Active Directory Domain Environment Deployment and Permission Management Report

Basic Information

Name	Gaoyuan Zhang
Date	October 26, 2025
Environment	Oracle VirtualBox + Windows Server 2022 + Windows 11
Objective	Build a complete Active Directory (AD) domain environment in a virtualized lab, enabling user management, group policy deployment, and file-sharing permission control.
File Name	AD_Lab_Deployment_Report_EN_Full_GaoyuanZhang_B00961366.docx

1. Project Overview

This project combines Active Directory automation and domain management within a Windows Server 2022 environment.
It demonstrates the configuration of AD DS, DNS, Group Policy, centralized access control, and department-based file permissions.
PowerShell scripting is used to automate user provisioning and group assignments, while GPOs enforce company-wide settings such as wallpaper and drive mapping.

2. Environment Setup

- Windows Server 2022 as Domain Controller (WIN-LH5SMGL3A3H.lab.local)
- Domain: lab.local
- Organizational Units (OUs): Halifax, Departments, Users, Computers
- Security Groups: Employee, IT, Admin
- DNS configured for internal name resolution
- File sharing and Remote Desktop enabled
- Centralized Group Policy for wallpaper and access control

OU Structure:

lab.local
├ Halifax

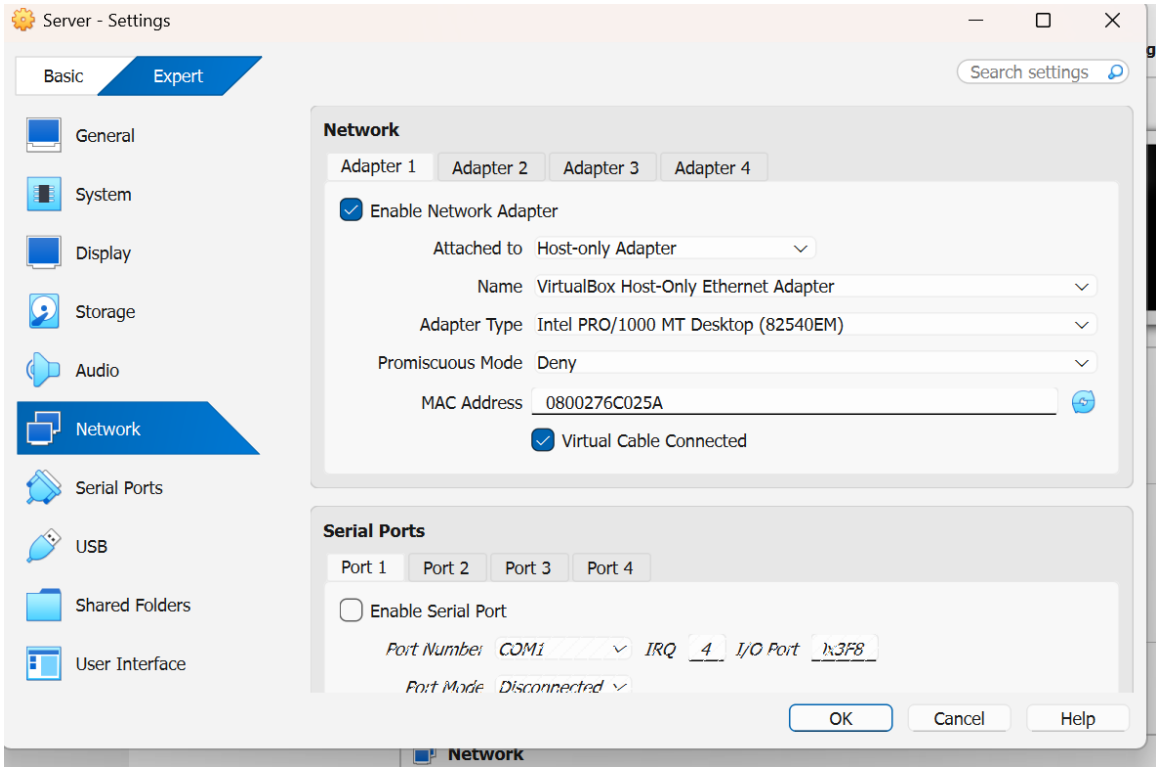
```
|  ├ Departments
|  |  ├ Admin
|  |  ├ Employee
|  |  └ IT
|  ├ Users
|  └ Computers
```

Experiment Steps and Results

Step 0: Prepare Virtual Machines and ISO Images

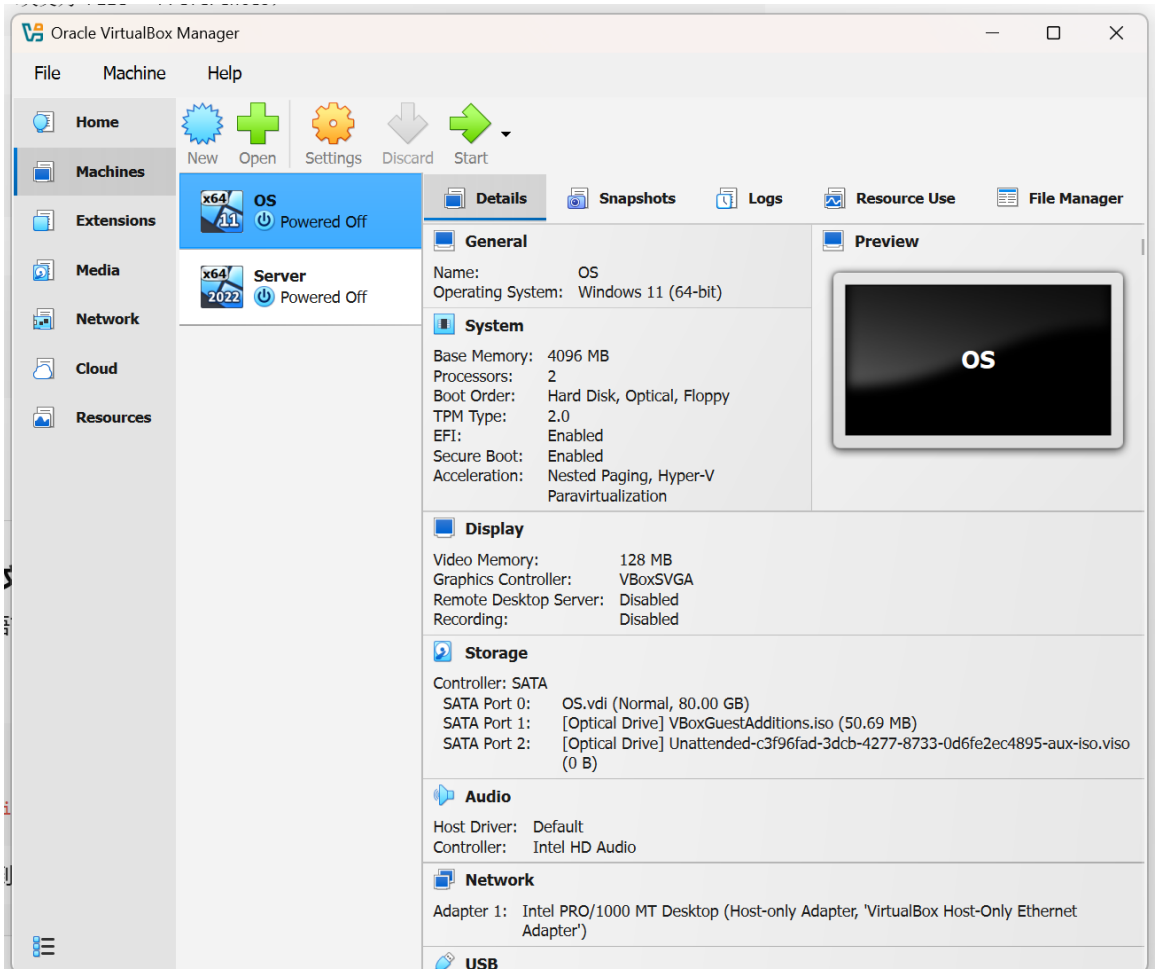
Description: Two virtual machines were created in Oracle VirtualBox — one for Windows Server 2022 and another for Windows 11. WIN-LH5SMGL3A3H was configured with 4–8GB RAM, 60GB+ disk, and two CPUs. The Windows 11 client had 4GB RAM and 40GB+ disk. Installation ISO files for both systems were attached for setup.

Step 1: Configure VirtualBox Network Settings



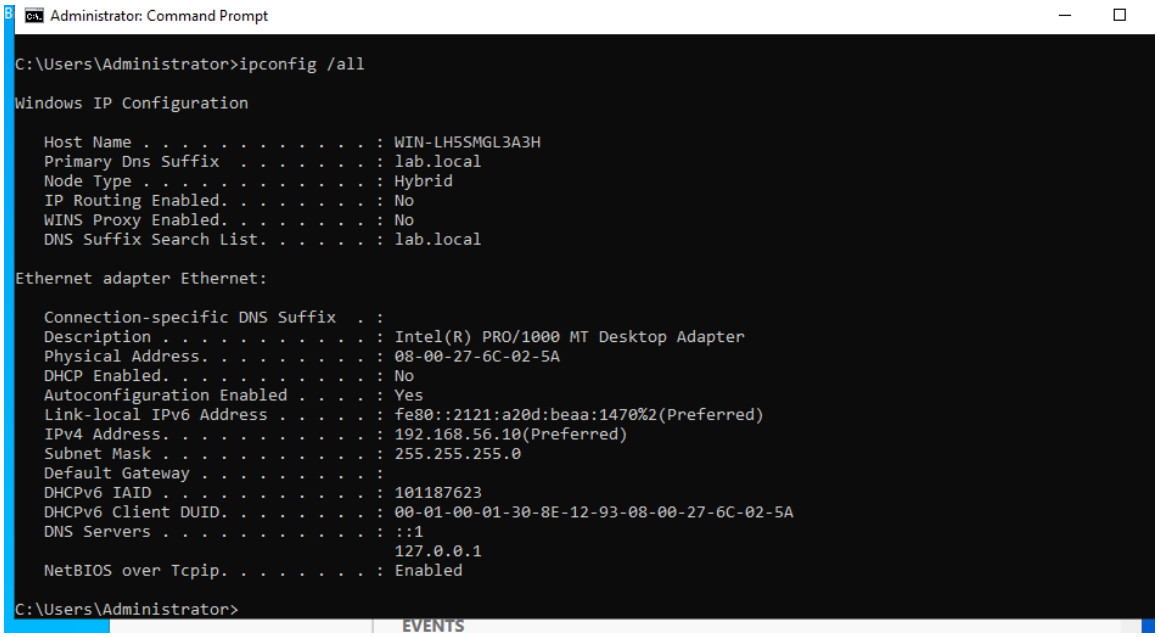
Description: Both virtual machines were configured with two network adapters: Adapter 1 (Host-Only) for internal domain communication.

Step 2: Install Windows Server (Domain Controller)



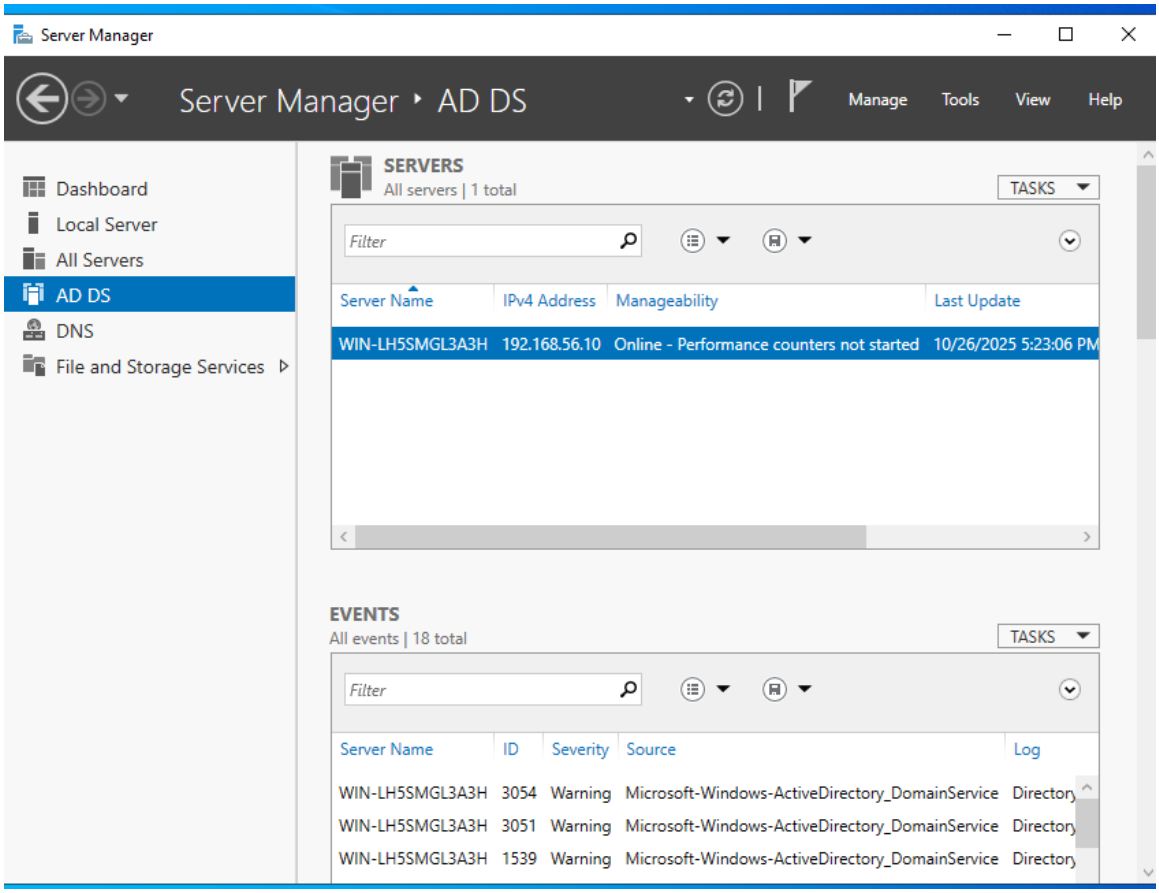
Description: Installed Windows Server 2022 Standard (Desktop Experience). After installation, the hostname was changed to WIN-LH5SMGL3A3H and the system was rebooted. This server will act as the domain controller for the lab environment.

Step 3: Configure Static IP for Domain Controller



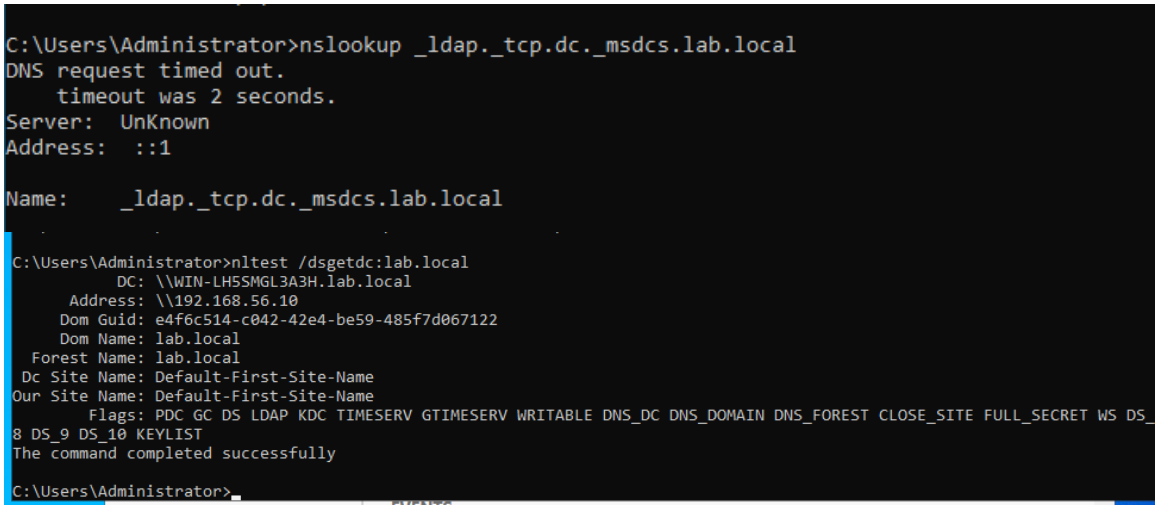
Description: In Network Connections (ncpa.cpl), the Host-Only adapter was assigned a static IP of 192.168.56.10 with subnet mask 255.255.255.0. DNS was set to 192.168.56.10 (self-reference). The NAT adapter remained on DHCP for internet connectivity. Verified connectivity using ping and ipconfig.

Step 4: Install AD DS + DNS and Promote to Domain Controller



Description: Through Server Manager → Add Roles and Features, installed Active Directory Domain Services (AD DS) and DNS Server roles. Promoted WIN-LH5SMGL3A3H to a new forest with the root domain name lab.local. Set DSRM password, completed the wizard, and rebooted. Login now appears as LAB\Administrator.

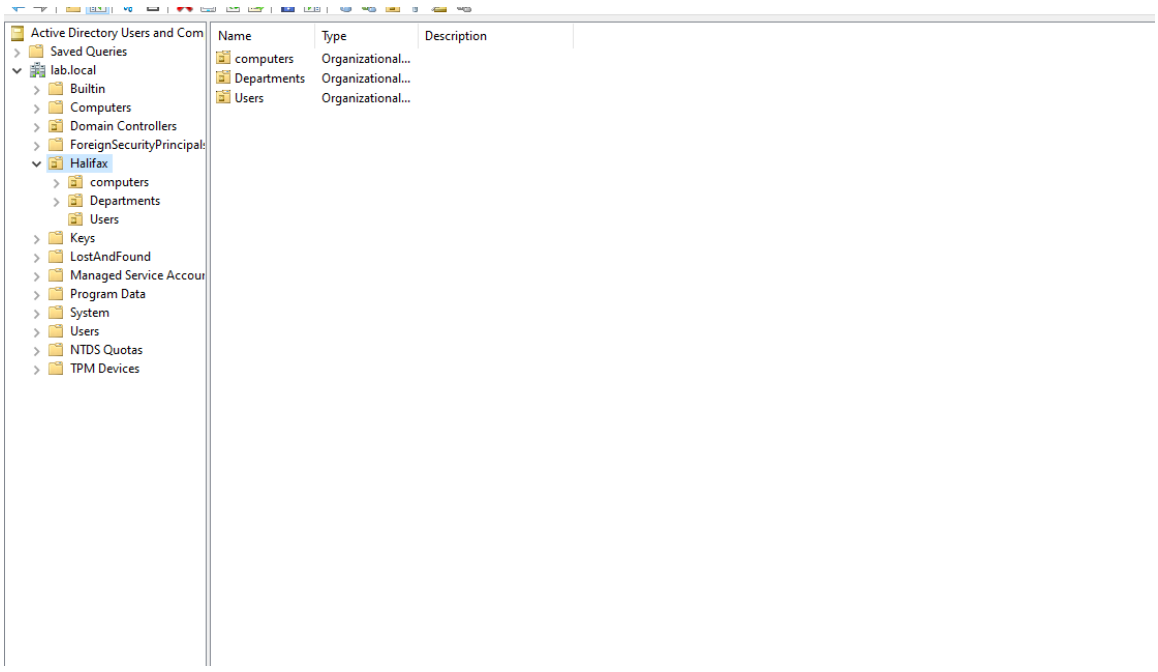
Step 5: Verify Domain Controller Health

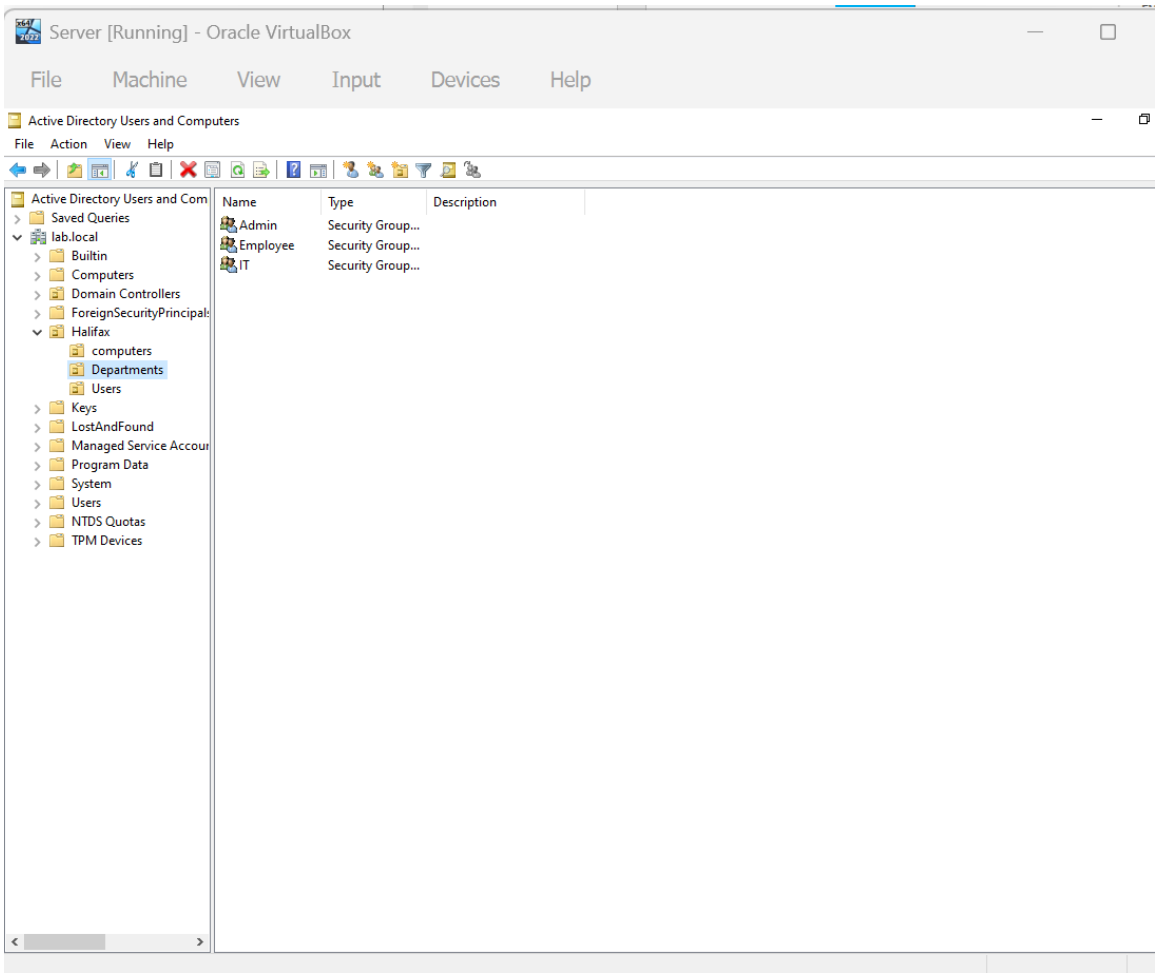


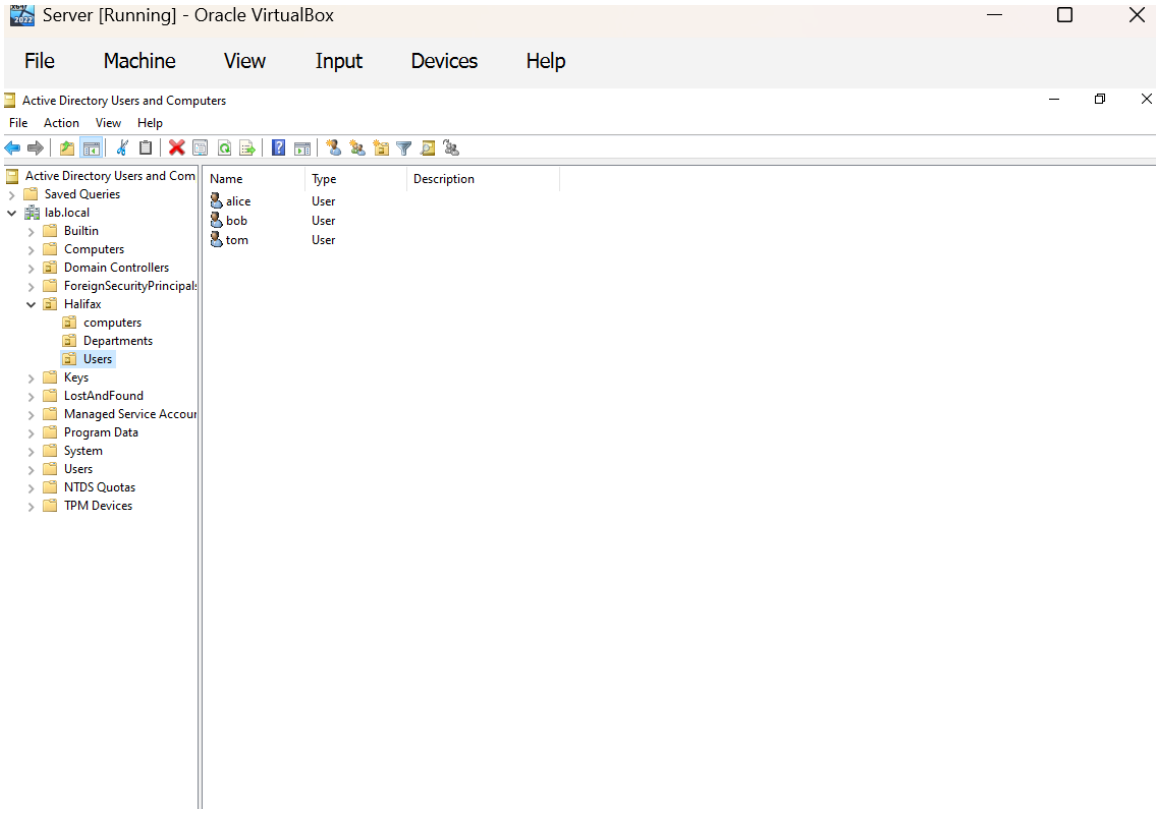
Description: Verified the AD installation using diagnostic commands: nslookup _ldap._tcp.dc._msdcs.lab.local and nltest /dsgetdc:lab.local confirmed proper domain resolution. Opened AD tools (gpmc.msc, dsa.msc) to ensure AD DS and DNS services were running correctly.

Step 6: Create Organizational Units (OU) and Users

📸 Screenshot Placeholder (Insert screenshot for this step).




Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Halifax
computers
Departments
Users
Keys
LostAndFound
Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Description
Admin
Security Group...
Employee
Security Group...
IT
Security Group...



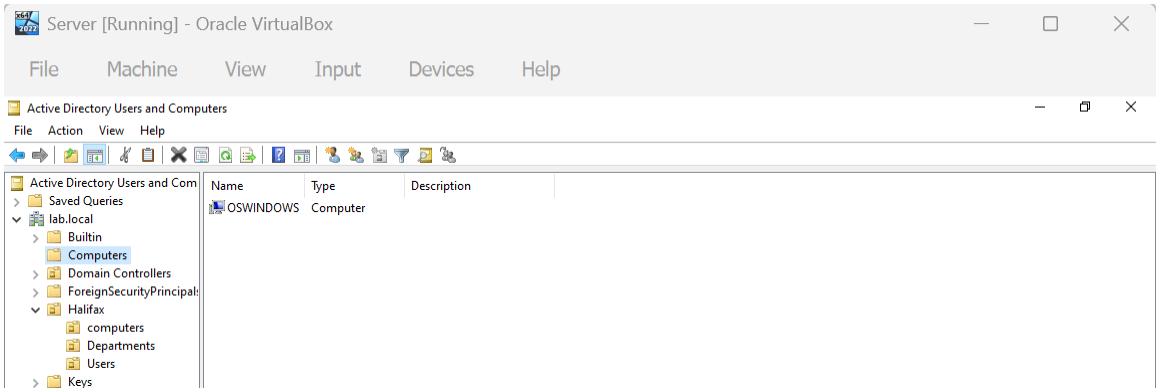
Description: In Active Directory Users and Computers (dsa.msc), created OUs for Departments, Users, and Computers. Under Departments, created IT, Employee, and Admin OUs. Created users alice (Admin) and bob (Employee), and added them to corresponding security groups.

Step 7: Configure Client Static IP

📸 Screenshot Placeholder (Insert screenshot for this step).

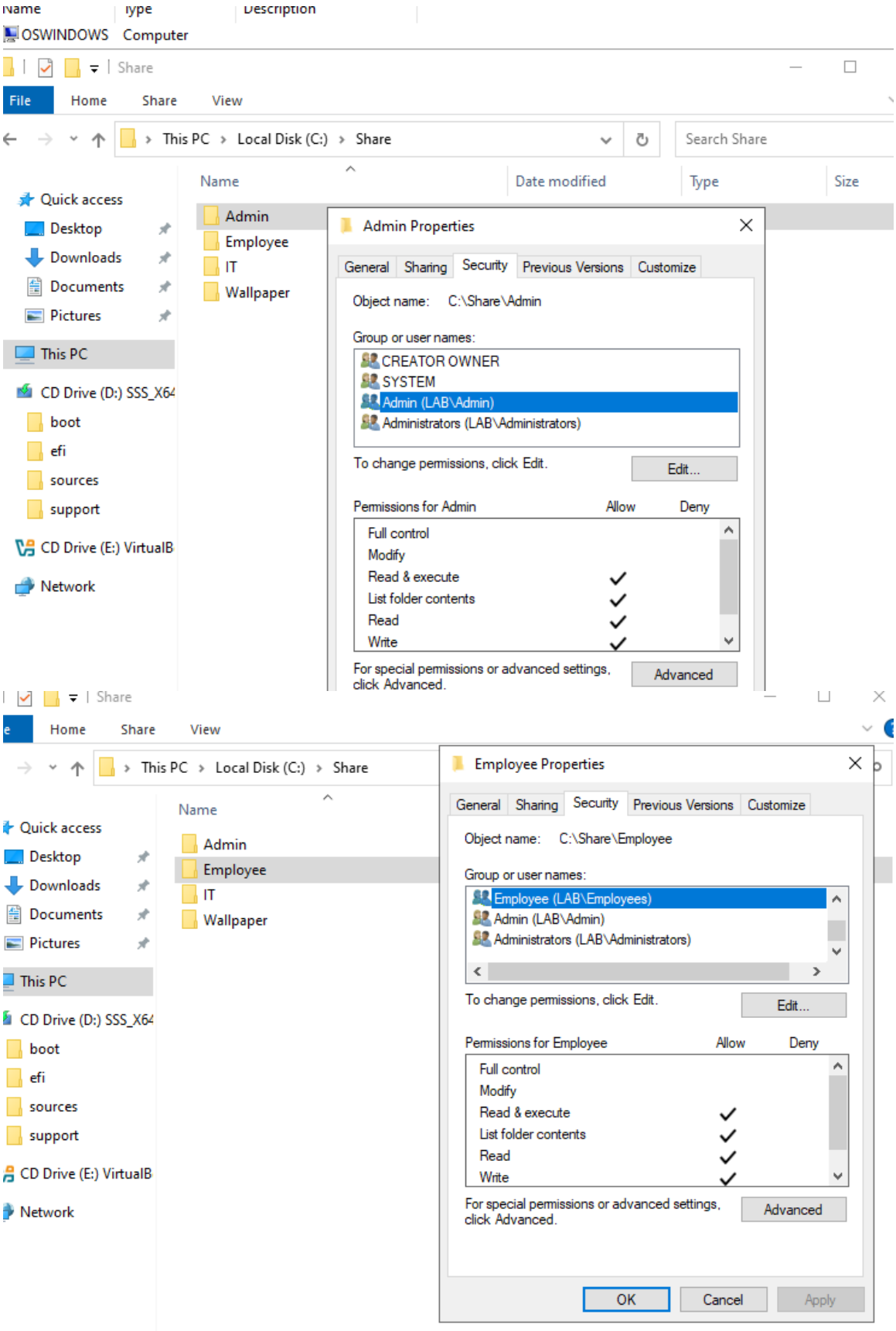
Description: Configured the Windows 11 client (WIN11) with Host-Only IP 192.168.56.20, subnet mask 255.255.255.0, and DNS 192.168.56.10. This allows the client to communicate with WIN-LH5SMGL3A3H and resolve lab.local through the domain controller.

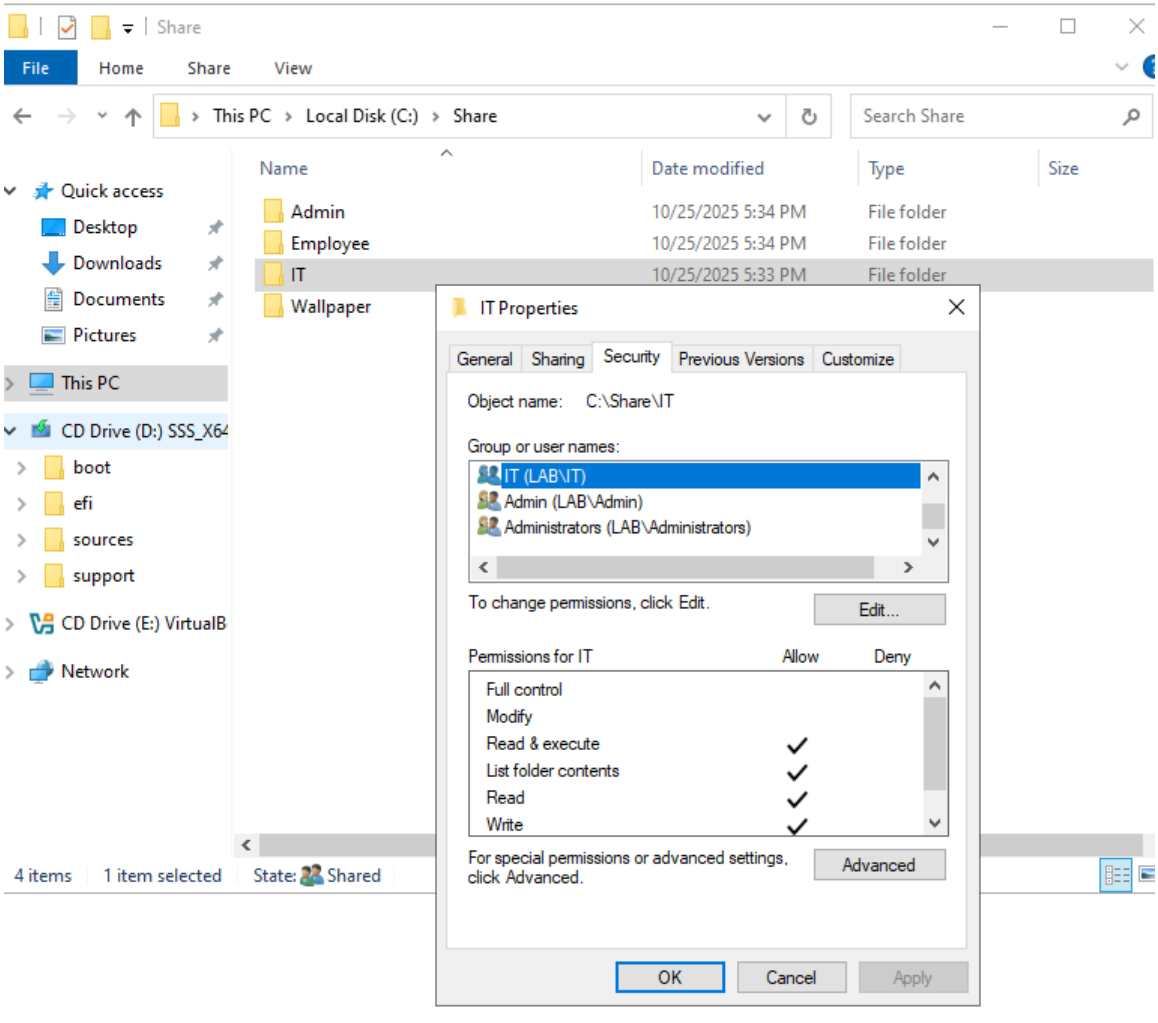
Step 8: Join Client to Domain

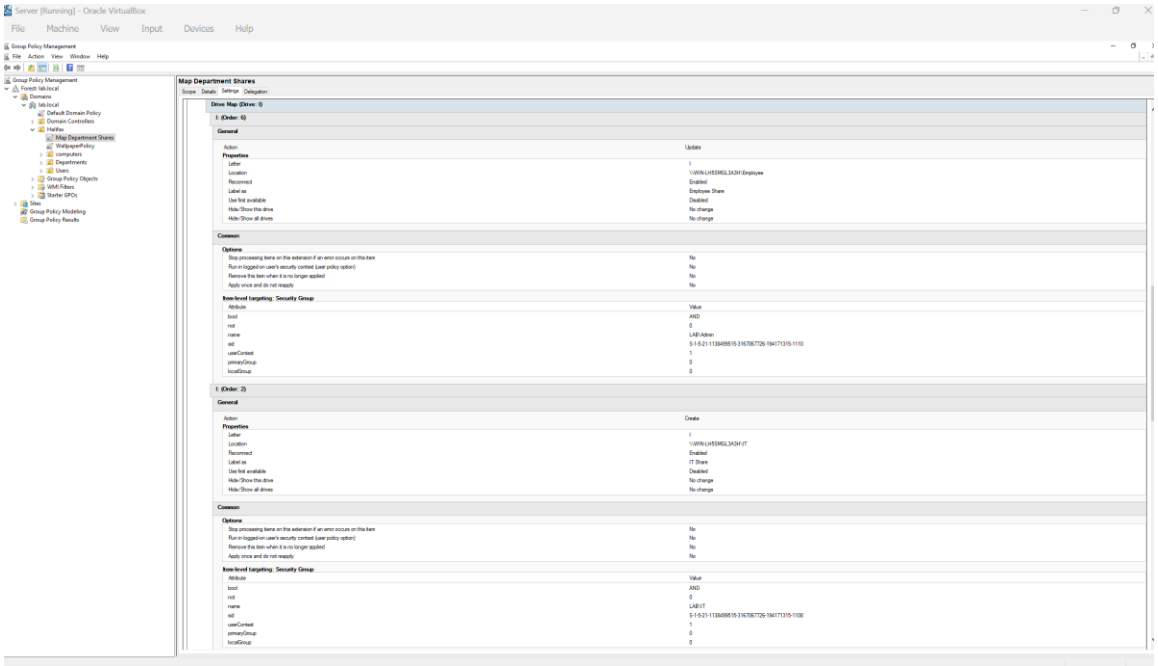


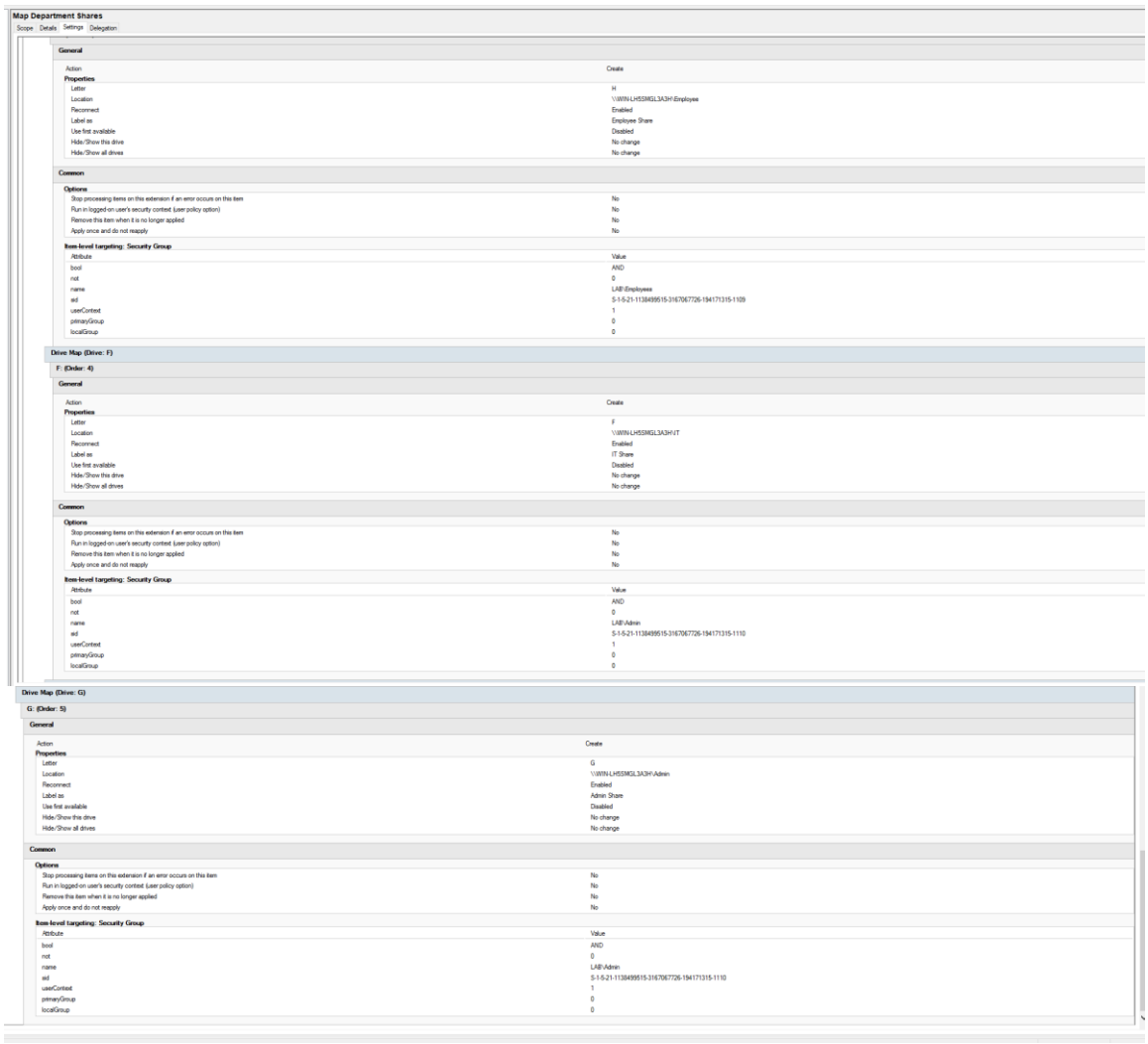
Description: On the Windows 11 client, changed the system domain to lab.local under System → About → Rename this PC (Advanced). Entered domain credentials LAB\Administrator. After rebooting, verified domain login with LAB\alice credentials.

Step 9: Set Up Shared Folders and Verify Permissions


Name
Type
Description
OSWINDOWS
Computer
Share
File
Home
Share
View
This PC
Local Disk (C:)
Share
Search Share
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) SSS_X64
boot
efi
sources
support
CD Drive (E:) VirtualB
Network
Name
Date modified
Type
Size
Admin
Employee
IT
Wallpaper
Admin Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Share\Admin
Group or user names:
CREATOR OWNER
SYSTEM
Admin (LAB\Admin)
Administrators (LAB\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Admin
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Employee Properties
Object name: C:\Share\Employee
Employee (LAB\Employees)
Admin (LAB\Admin)
Administrators (LAB\Administrators)
Permissions for Employee
OK
Cancel
Apply

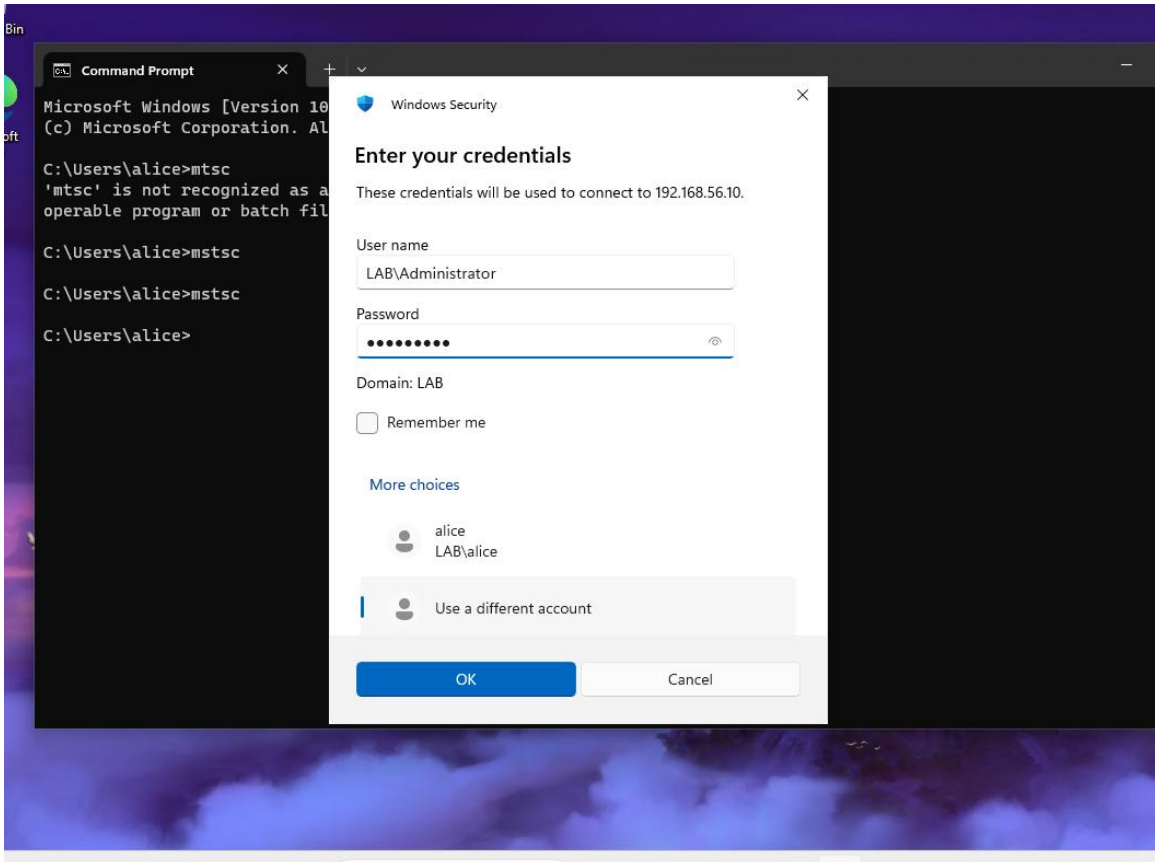

Share
File
Home
Share
View
This PC
Local Disk (C:)
Share
Search Share
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) SSS_X64
boot
efi
sources
support
CD Drive (E:) VirtualB
Network
Name
Date modified
Type
Size
Admin
10/25/2025 5:34 PM
File folder
Employee
10/25/2025 5:34 PM
File folder
IT
10/25/2025 5:33 PM
File folder
Wallpaper
4 items
1 item selected
State: Shared
IT Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Share\IT
Group or user names:
IT (LAB\IT)
Admin (LAB\Admin)
Administrators (LAB\Administrators)
To change permissions, click Edit.
Edit...
Permissions for IT
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

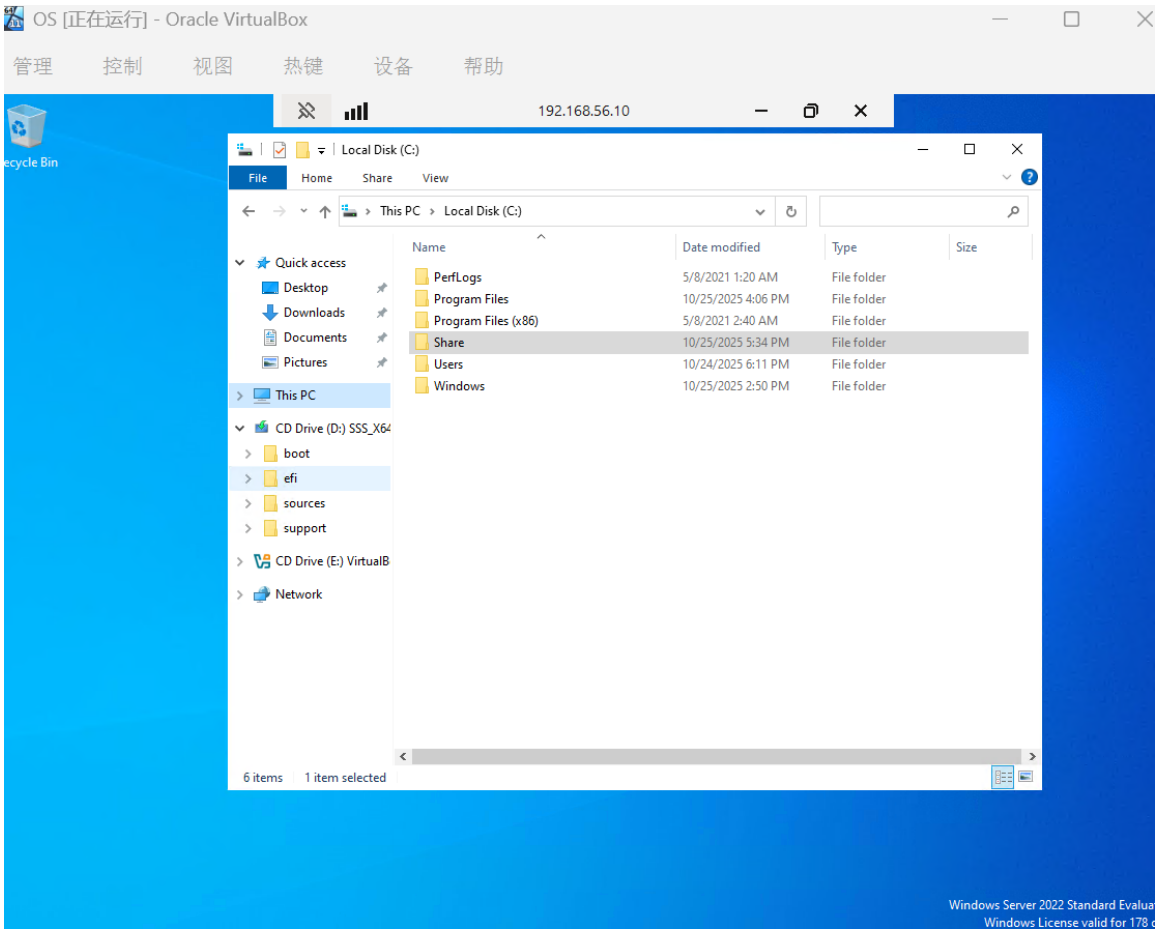




Description: Created shared folders D:\Share\IT and D:\Share\HR on DC. Configured Share and NTFS permissions — IT folder accessible only to IT group and Admin group, Employee folder accessible only to Employee group and Admin group, Admin folder only to Admin group. On the client, \ WIN-LH5SMGL3A3H \IT, \ WIN-LH5SMGL3A3H \Admin, and \ WIN-LH5SMGL3A3H \Employee verified correct access isolation between groups.

Step 10: Enable Remote Desktop Access





Description: Enabled Remote Desktop under System → Remote Desktop → Allow remote connections to this computer. Firewall automatically opened TCP port 3389. Verified service status using netstat -an | find "3389". From the host or client machine, connected to DC via mstsc using LAB\Administrator credentials.

Step 11. PowerShell Automation

A PowerShell script automates new employee onboarding by creating users in the appropriate OU,
assigning them to department-specific security groups, and integrating with a centralized GPO that maps network drives automatically based on role.

Example role configuration snippet:

```
$RoleConfig = @{
  "Employee" = @{
    OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
    Group  = "Employee"
  }
```

```
    "IT" = @{
        OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
        Group  = "IT"
    }
    "Admin" = @{
        OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
        Group  = "Admin"
    }
}
```

```
<#
.SYNOPSIS
Creates new Active Directory users under OU=Halifax/Users
and assigns them to corresponding security groups under OU=Halifax/Departments.
Designed for centralized GPO drive mapping in lab.local.
#>

# ----------------------------
# Global Configuration
# ----------------------------
$domain = "lab.local"
# Default password for all new users (users will change at first login)
<#
.SYNOPSIS
Creates new Active Directory users under OU=Halifax/Users
and assigns them to corresponding security groups under OU=Halifax/Departments.
Designed for centralized GPO drive mapping in lab.local.
#>

# ----------------------------
# Global Configuration
# ----------------------------
$domain = "lab.local"
$defaultPassword = ConvertTo-SecureString "P@ssword123" -AsPlainText -Force

# ----------------------------
# User List
# ----------------------------
$Users = @(
    @{ Name="User1"; Username="u1"; Role="Employee" },
    @{ Name="User2"; Username="u2"; Role="IT" },
    @{ Name="User3"; Username="u3"; Role="Admin" }
)

# ----------------------------
# Role Configuration Table
# ----------------------------
$RoleConfig = @{
    "Employee" = @{
        OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
        Group  = "Employee"
    }
    "IT" = @{
        OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
        Group  = "IT"
```

```
    }
    "Admin" = @{
        OUPath = "OU=Users,OU=Halifax,DC=lab,DC=local"
        Group  = "Admin"
    }
}

# ---------------------------
# Main Execution Loop
# ---------------------------
foreach ($user in $Users) {
    $name = $user.Name
    $username = $user.Username
    $role = $user.Role
    $OUPath = $RoleConfig[$role].OUPath
    $GroupName = $RoleConfig[$role].Group

    Write-Host "`nCreating user: $name ($role)..."

    # Step 1: Create AD user account
    New-ADUser `
        -Name $name `
        -SamAccountName $username `
        -DisplayName $name `
        -Path $OUPath `
        -AccountPassword $defaultPassword `
        -Enabled $true `
        -ChangePasswordAtLogon $true `
        -Description "$role Role"

    # Step 2: Add user to the correct security group
    $GroupPath = "CN=Employee,OU=Departments,OU=Halifax,DC=lab,DC=local"
    if ($role -eq "Employee") {
        Add-ADGroupMember -Identity $GroupPath -Members $username
    } elseif ($role -eq "IT") {
        Add-ADGroupMember -Identity "CN=IT,OU=Departments,OU=Halifax,DC=lab,DC=local" -Members $username
    } elseif ($role -eq "Admin") {
        Add-ADGroupMember -Identity "CN=Admin,OU=Departments,OU=Halifax,DC=lab,DC=local" -Members $username
    }


    Write-Host "$username created in $OUPath and added to group $GroupName"
}

Write-Host "`nAll users have been created successfully under OU=Halifax/Users."
```

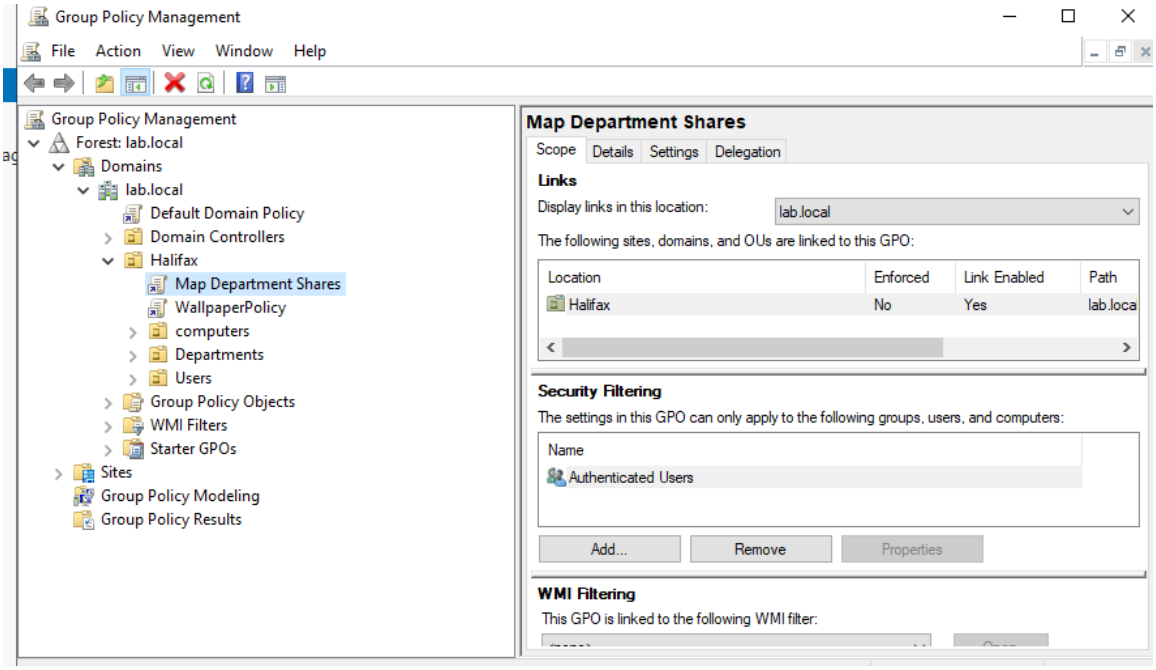
```
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> .\Create-ADUsers.ps1

Creating user: User1 (Employee)...
u1 created in OU=Users,OU=Halifax,DC=lab,DC=local and added to group Employee

Creating user: User2 (IT)...
u2 created in OU=Users,OU=Halifax,DC=lab,DC=local and added to group IT

Creating user: User3 (Admin)...
u3 created in OU=Users,OU=Halifax,DC=lab,DC=local and added to group Admin

All users have been created successfully under OU=Halifax/Users.
PS C:\Users\Administrator\Desktop>
```

4. Group Policy Integration

A centralized Group Policy Object (GPO) linked to the Halifax OU handles user environment settings,
such as automatic network drive mapping, wallpaper configuration, and remote desktop permissions.
Drive mappings are filtered by security group membership (Item-level targeting).

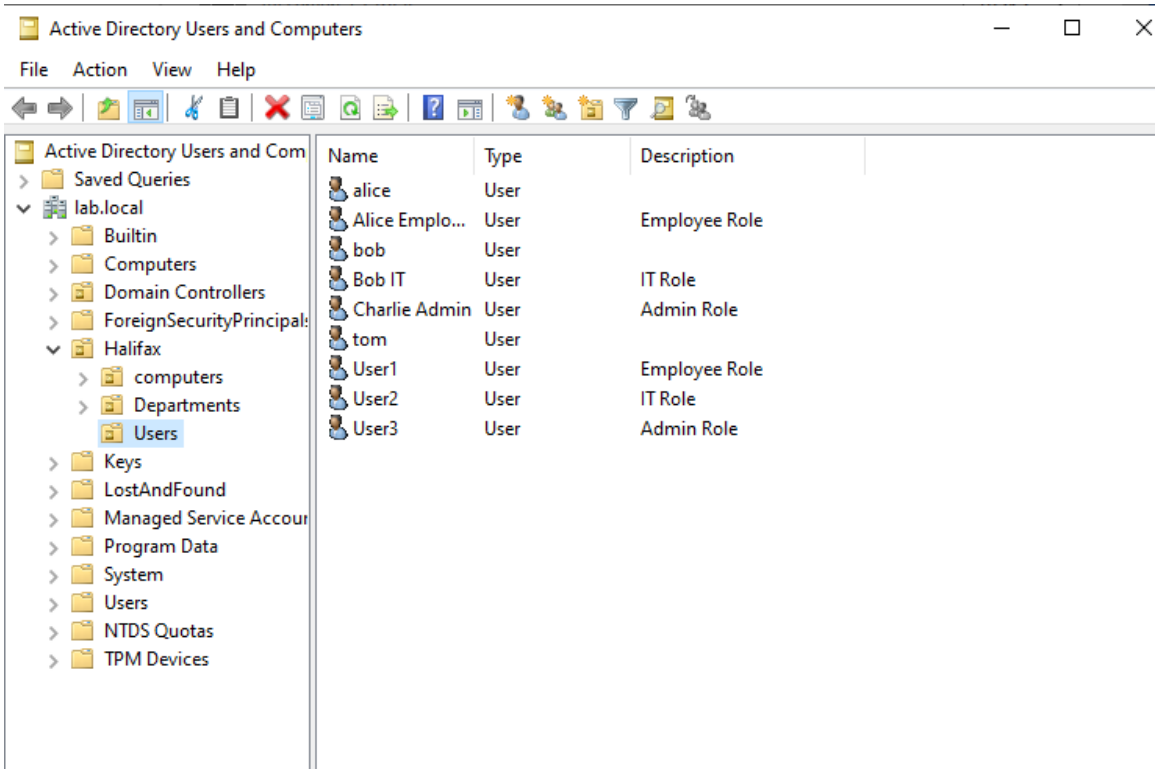
Drive Mapping Rules:
Z: → \\WIN-LH5SMGL3A3H\EmployeeShare → Employee group

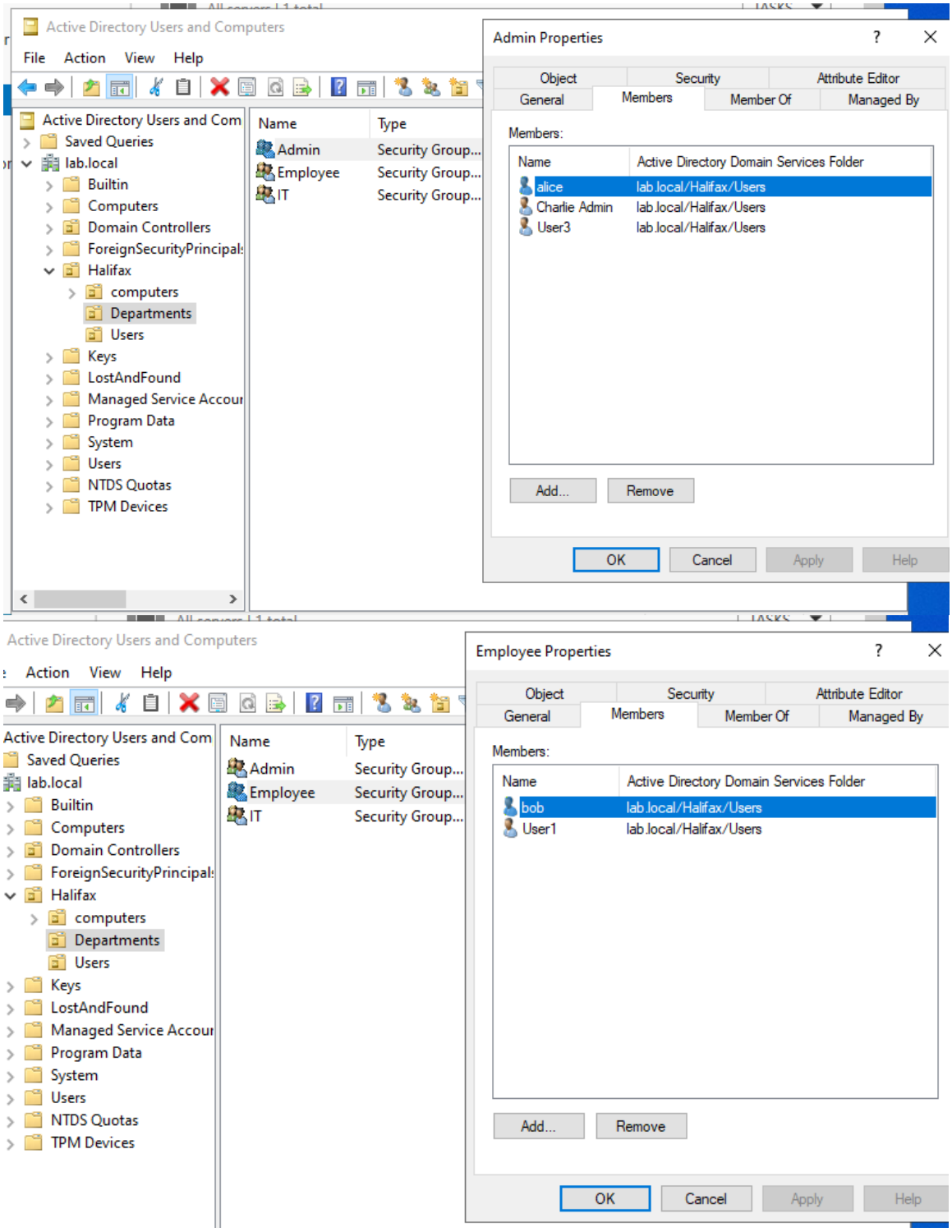
Y: → \WIN-LH5SMGL3A3H\ITShare → IT group
X: → \WIN-LH5SMGL3A3H\AdminShare → Admin group

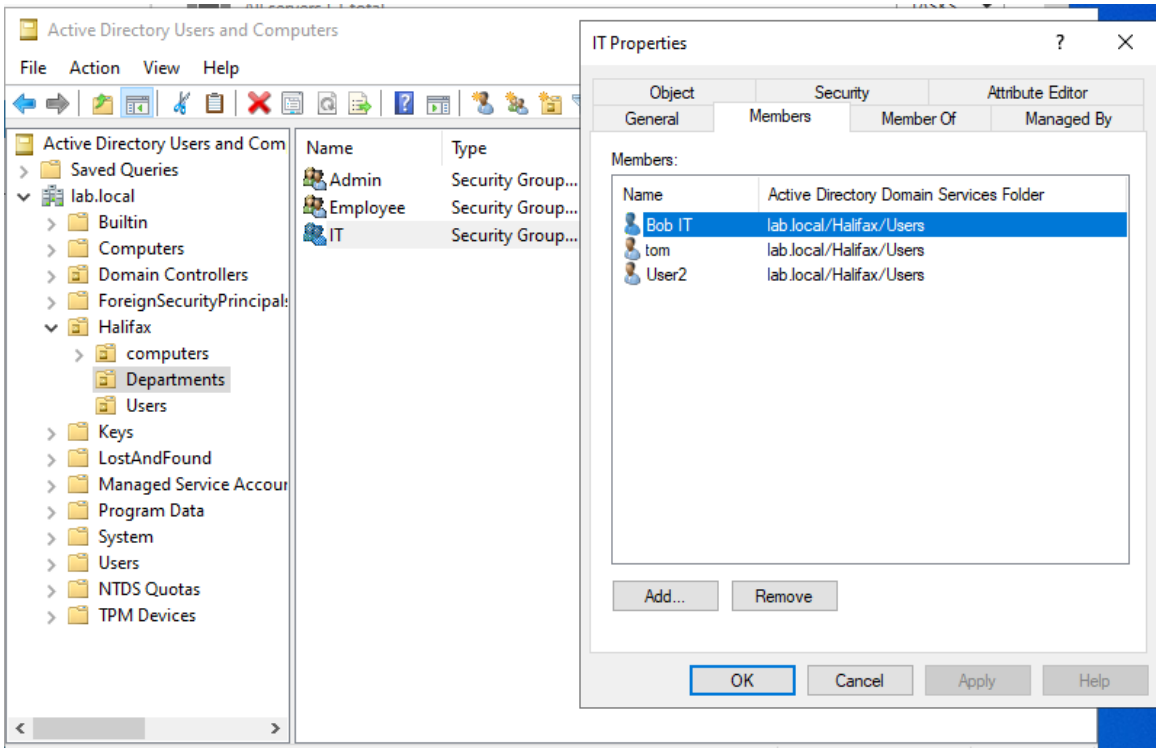


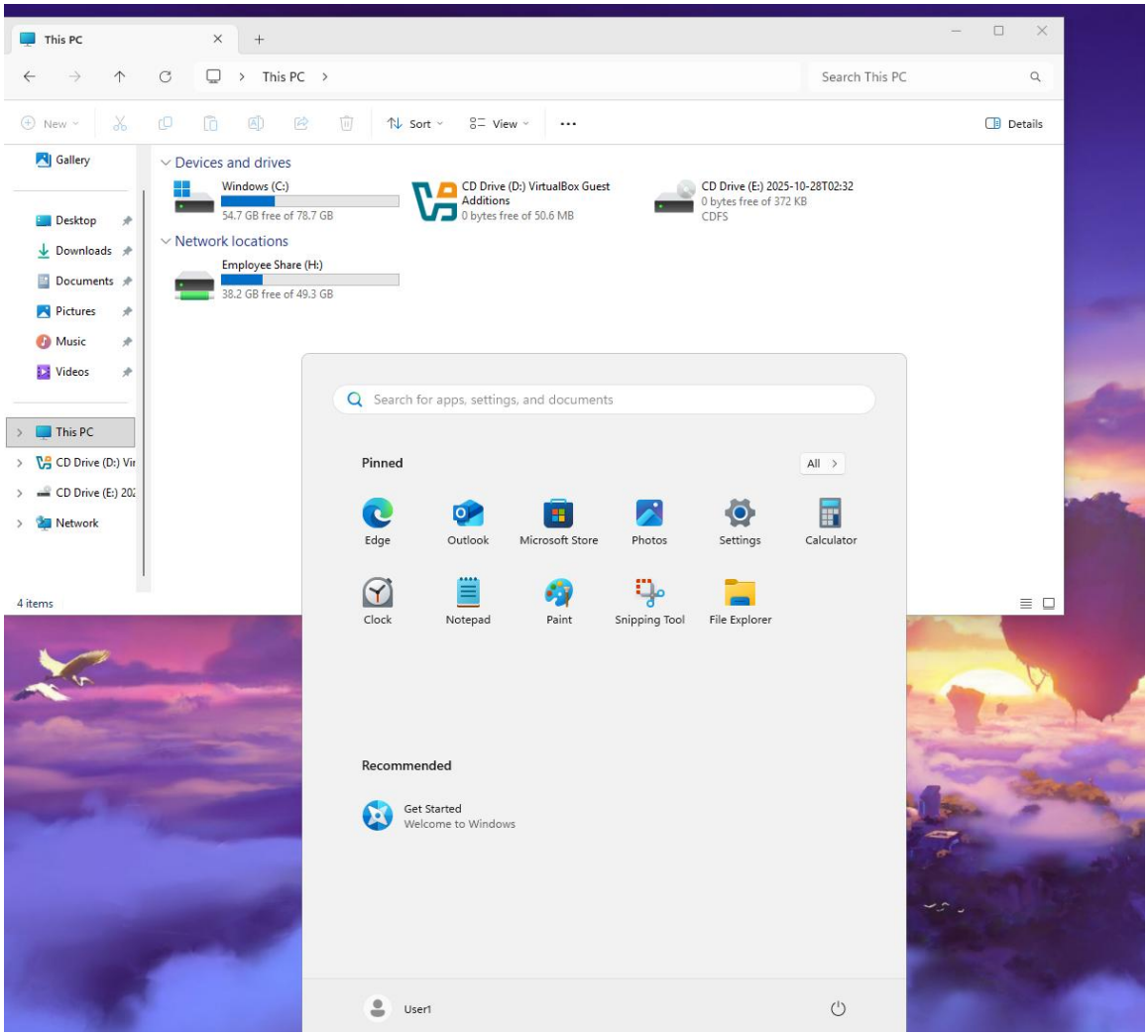
5. Verification and Results

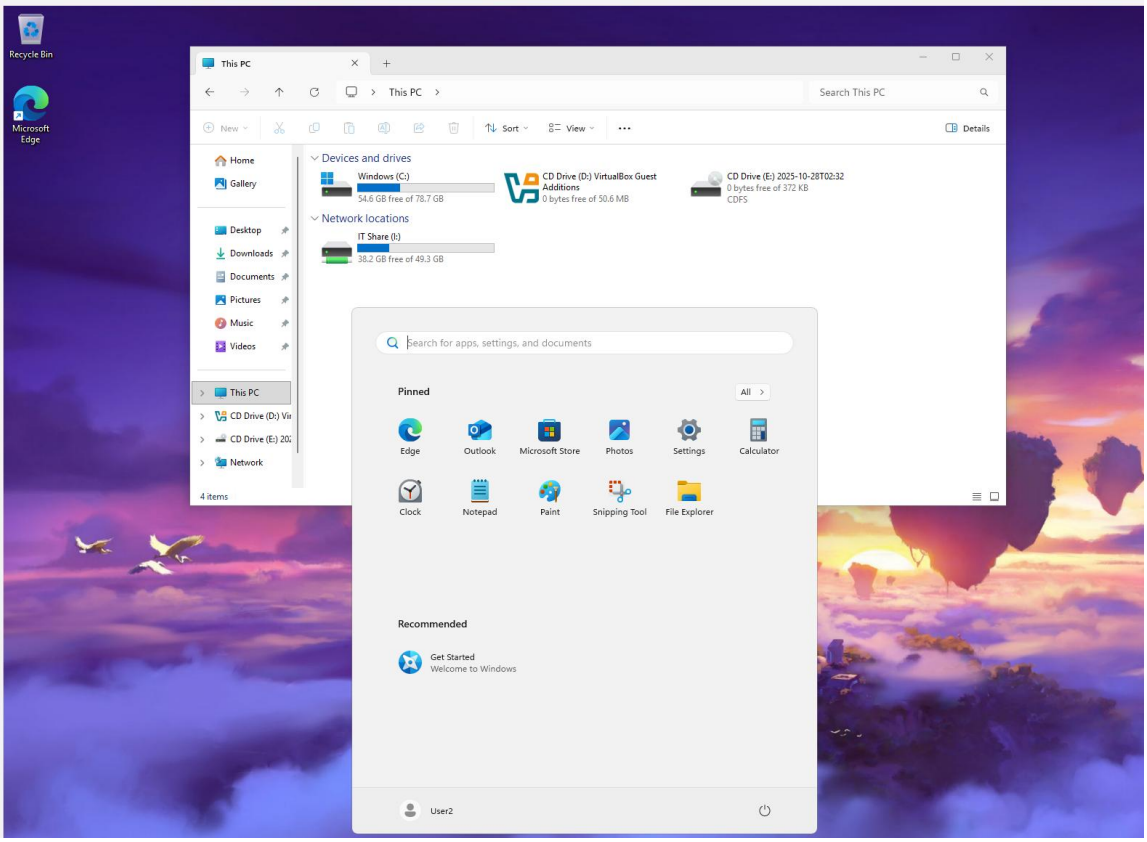
After running the PowerShell script, users were automatically created under OU=Halifax/Users and added to their respective groups.
The GPO correctly mapped network drives and applied desktop settings according to group membership.

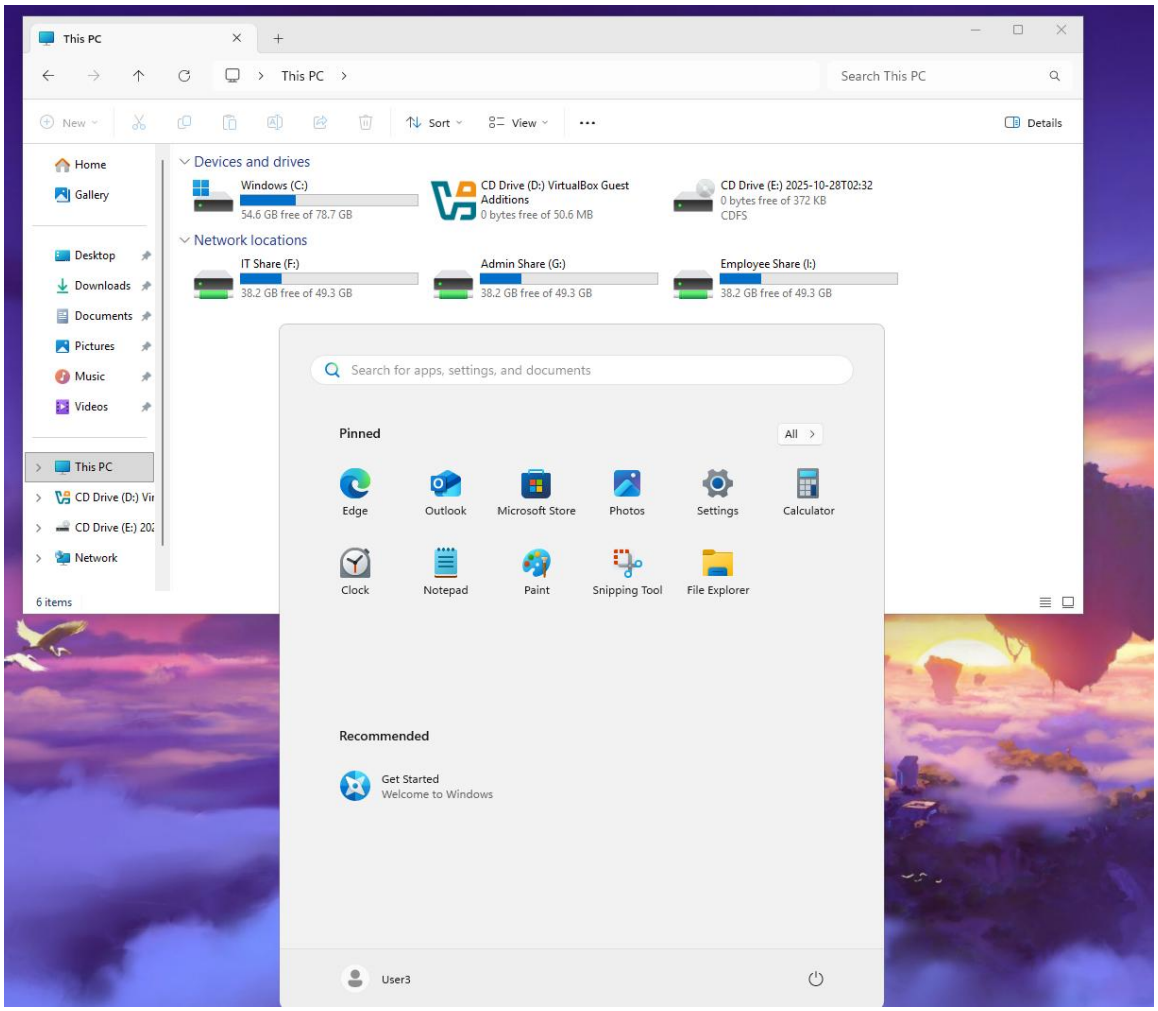

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Halifax
computers
Departments
Users
Keys
LostAndFound
Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Description
alice
User
Alice Emplo...
User
Employee Role
bob
User
Bob IT
User
IT Role
Charlie Admin
User
Admin Role
tom
User
User1
User
Employee Role
User2
User
IT Role
User3
User
Admin Role


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Halifax
computers
Departments
Users
Keys
LostAndFound
Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Admin
Security Group...
Employee
Security Group...
IT
Security Group...
Admin Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
alice
lab.local/Halifax/Users
Charlie Admin
lab.local/Halifax/Users
User3
lab.local/Halifax/Users
Add...
Remove
OK
Cancel
Apply
Help
Active Directory Users and Computers
Action View Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Halifax
computers
Departments
Users
Keys
LostAndFound
Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Admin
Security Group...
Employee
Security Group...
IT
Security Group...
Employee Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
bob
lab.local/Halifax/Users
User1
lab.local/Halifax/Users
Add...
Remove
OK
Cancel
Apply
Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Halifax
computers
Departments
Users
Keys
LostAndFound
Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Admin
Security Group...
Employee
Security Group...
IT
Security Group...
IT Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Bob IT
lab.local/Halifax/Users
tom
lab.local/Halifax/Users
User2
lab.local/Halifax/Users
Add...
Remove
OK
Cancel
Apply
Help


This PC
This PC
Search This PC
New
Sort
View
Details
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
CD Drive (D:) Vir
CD Drive (E:) 202
Network
Devices and drives
Windows (C:)
54.7 GB free of 78.7 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 50.6 MB
CD Drive (E:) 2025-10-28T02:32
0 bytes free of 372 KB
CDFS
Network locations
Employee Share (H:)
38.2 GB free of 49.3 GB
4 items
Search for apps, settings, and documents
Pinned
All
Edge
Outlook
Microsoft Store
Photos
Settings
Calculator
Clock
Notepad
Paint
Snipping Tool
File Explorer
Recommended
Get Started
Welcome to Windows
User1


Recycle Bin
Microsoft Edge
This PC
Search This PC
New
Sort
View
Details
Home
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
4 items
Devices and drives
Windows (C:)
54.6 GB free of 78.7 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 50.6 MB
CD Drive (E:) 2025-10-28T02:32
0 bytes free of 372 KB
CDFS
Network locations
IT Share (I:)
38.2 GB free of 49.3 GB
Search for apps, settings, and documents
Pinned
All
Edge
Outlook
Microsoft Store
Photos
Settings
Calculator
Clock
Notepad
Paint
Snipping Tool
File Explorer
Recommended
Get Started
Welcome to Windows
User2



6. Troubleshooting Notes

Common issues encountered and their solutions:

- Error: Cannot find object 'Employee' → Use full DistinguishedName (CN=Employee,...)
- Script blocked → Set-ExecutionPolicy RemoteSigned -Force
- GPO not applied → Verify OU link and permissions
- Duplicate group names → Check for objects with identical CNs

7. Conclusion

This lab successfully implemented a Windows Server 2022 domain with automated AD user provisioning,
centralized group policies, and secure file-sharing access control.
It simulates a real-world IT environment, demonstrating practical knowledge of Active Directory, PowerShell automation, and enterprise system administration.

Appendix A: Command Summary

Command	Description
ipconfig /all	Display all network configuration details.
ping 192.168.56.10	Test connectivity with the domain controller.
nslookup lab.local	Verify DNS resolution for the domain.
nltest /dsgetdc:lab.local	Retrieve information about the domain controller.
gpupdate /force	Force immediate Group Policy update.
net use	List all mapped network drives.
netstat -an | find "3389"	Check if Remote Desktop (RDP) service is listening.

Appendix B: Summary and Reflection

- ✅ Successfully deployed a Windows Server 2022 Active Directory domain environment.
- ✅ Client successfully joined the domain and authenticated with domain credentials.
- ✅ Group Policy Objects (GPOs) were successfully applied and verified.
- ✅ File sharing permissions were properly configured and enforced per department.
- ✅ Remote Desktop access to the domain controller was successfully enabled.

Through this lab, I gained hands-on experience in setting up and managing a Windows domain environment. I learned how to integrate DNS, AD DS, Group Policy, and file-sharing permissions within an enterprise network. This exercise demonstrated how to securely manage users and systems within an organizational infrastructure.