Active Directory Domain Environment Deployment and Permission Management Report

# Basic Information

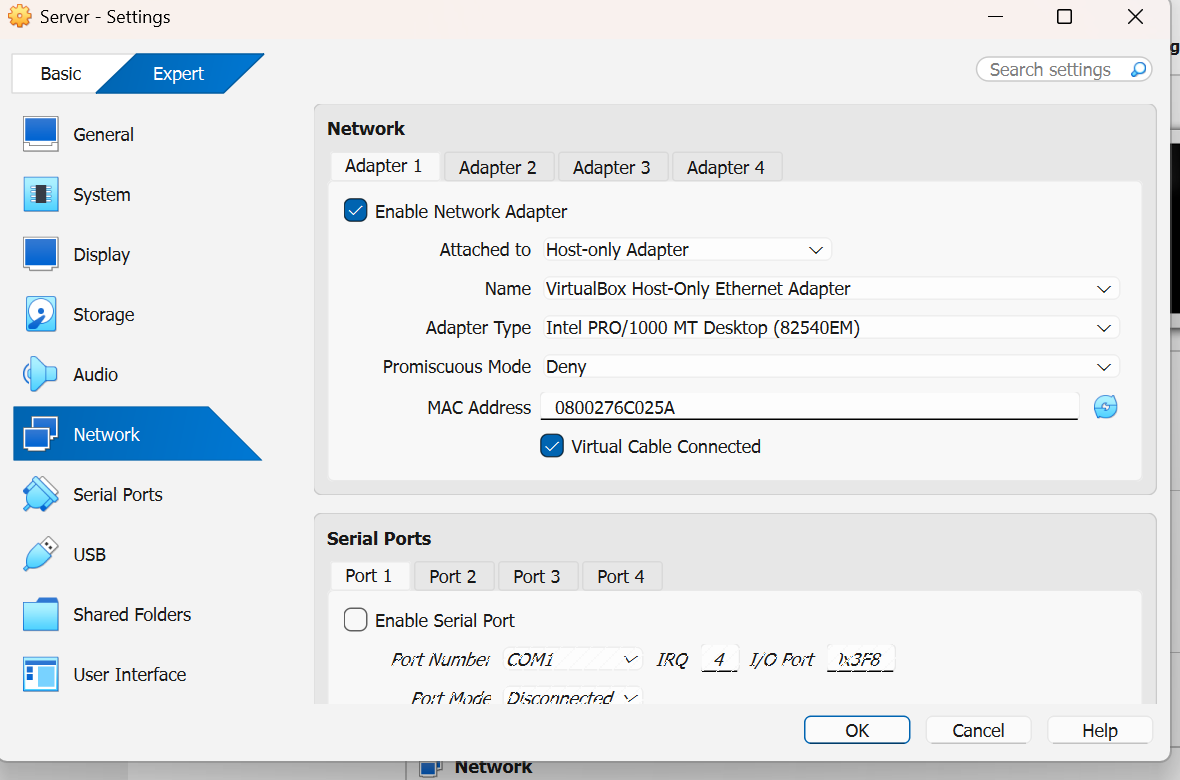
|  |  |
| --- | --- |
| Name | Gaoyuan Zhang |
| Student ID | B00961366 |
| Date | October 26, 2025 |
| Environment | Oracle VirtualBox + Windows Server 2022 + Windows 11 |
| Objective | Build a complete Active Directory (AD) domain environment in a virtualized lab, enabling user management, group policy deployment, and file-sharing permission control. |
| File Name | AD\_Lab\_Deployment\_Report\_EN\_Full\_GaoyuanZhang\_B00961366.docx |

# 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. Server01 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.

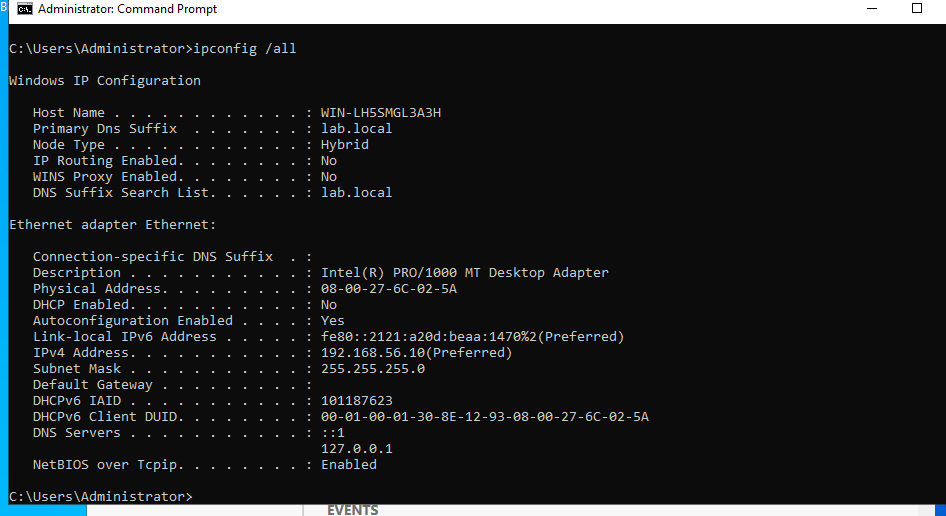
## Step 2: Install Windows Server (Domain Controller)

图形用户界面, 应用程序

AI 生成的内容可能不正确。

Description: Installed Windows Server 2022 Standard (Desktop Experience). After installation, the hostname was changed to SERVER01 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.

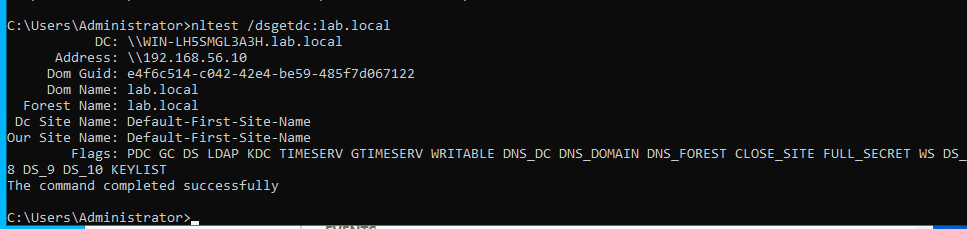
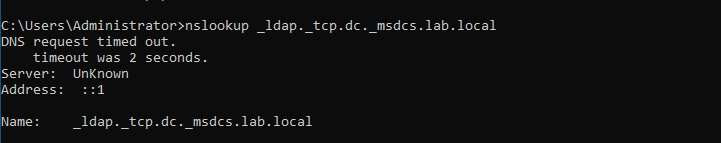
## Step 4: Install AD DS + DNS and Promote to Domain Controller

图形用户界面, 文本, 应用程序, 电子邮件

AI 生成的内容可能不正确。

Description: Through Server Manager → Add Roles and Features, installed Active Directory Domain Services (AD DS) and DNS Server roles. Promoted SERVER01 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.

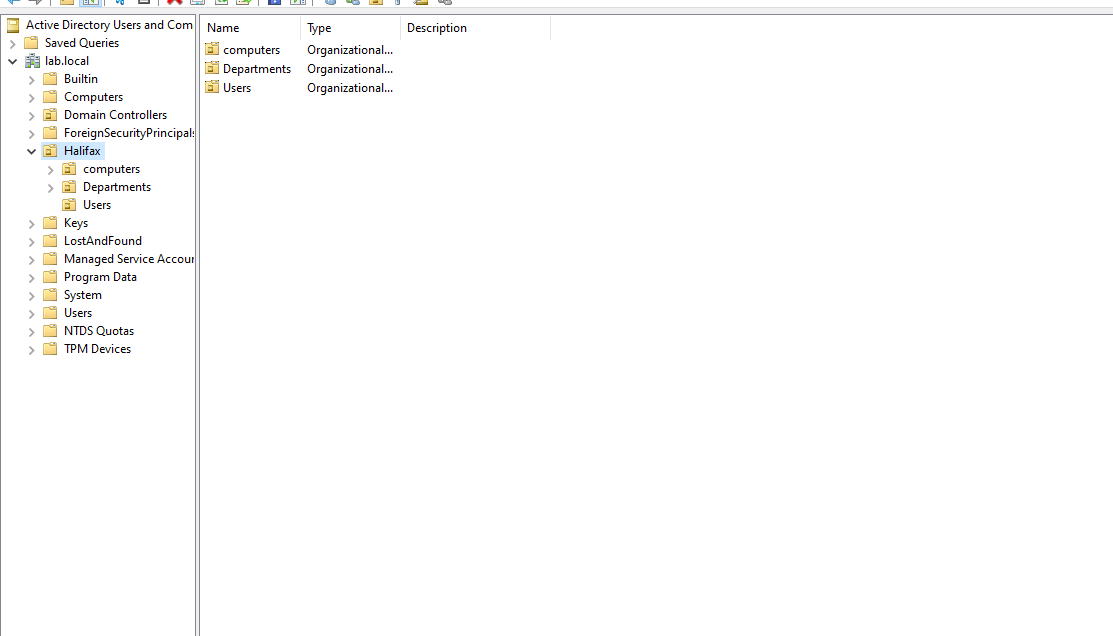
## Step 5: Verify Domain Controller Health

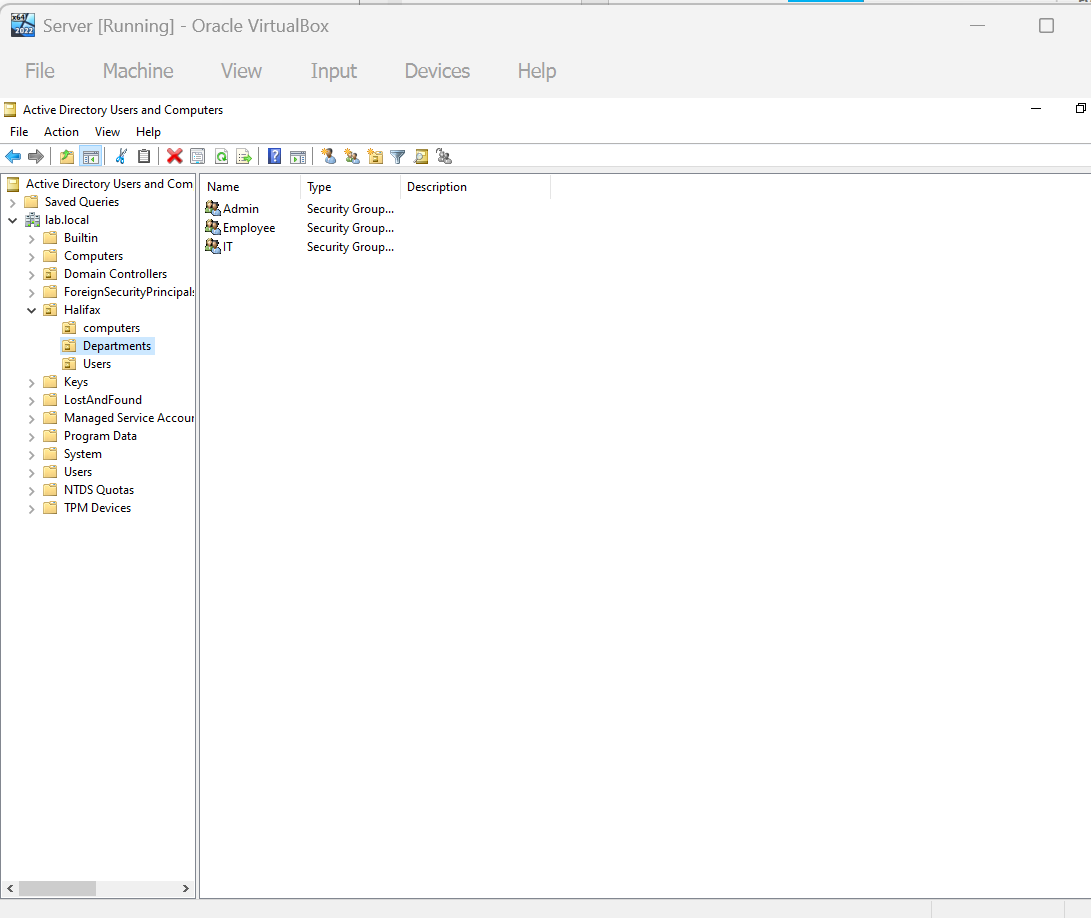


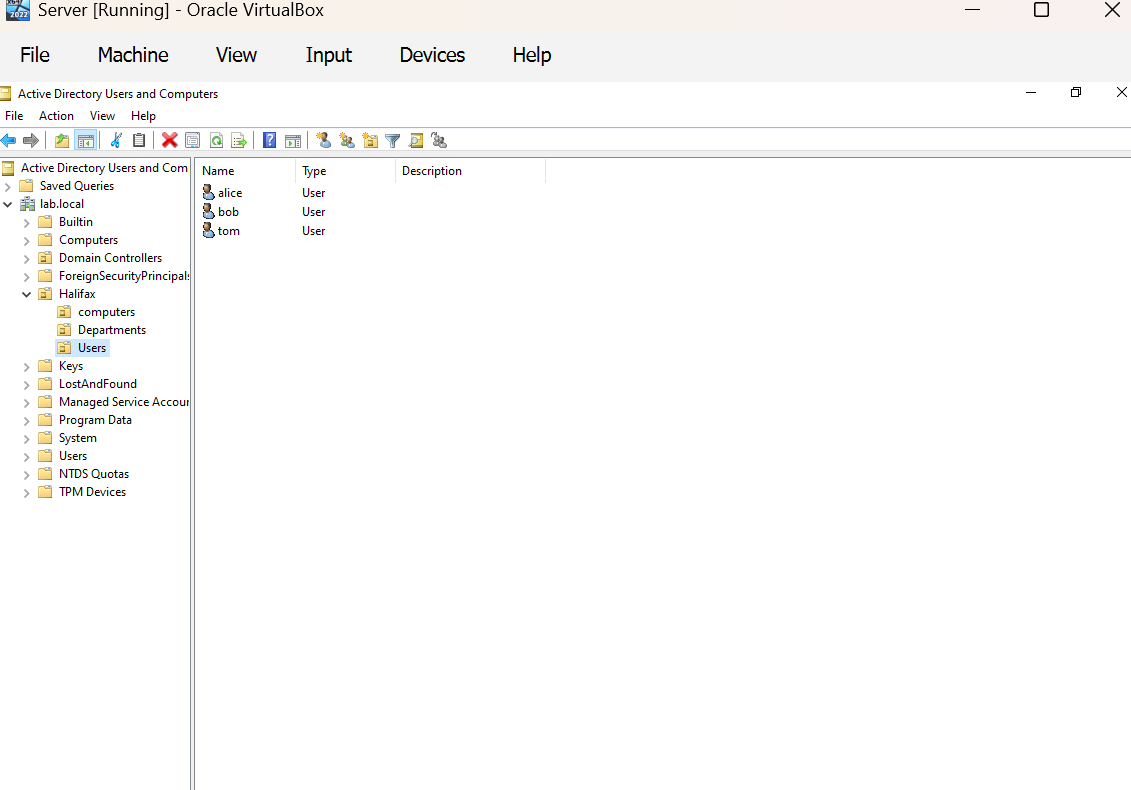
Description: Verified the AD installation using diagnostic commands: nslookup \_ldap.\_tcp.dc.\_msdcs.lab.local and nltest /dsgetdc:lab.local confirmed proper domain resolution. Opened AD tools (gpmc.msc, dsa.msc) to ensure AD DS and DNS services were running correctly.

## Step 6: Create Organizational Units (OU) and Users

📸 Screenshot Placeholder (Insert screenshot for this step).







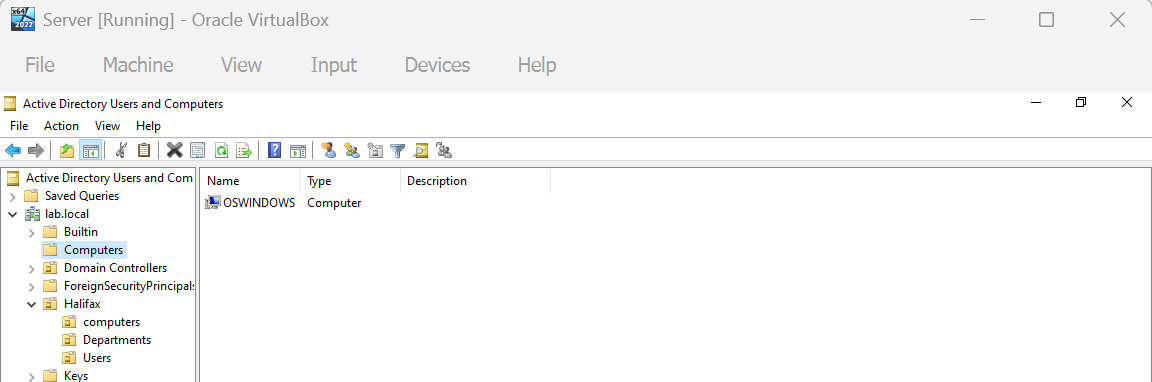
Description: In Active Directory Users and Computers (dsa.msc), created OUs for Departments, Users, and Computers. Under Departments, created IT, Employee, and Admin OUs. Created users alice (Admin) and bob (Employee), and added them to corresponding security groups.

## Step 7: Configure Client Static IP

📸 Screenshot Placeholder (Insert screenshot for this step).

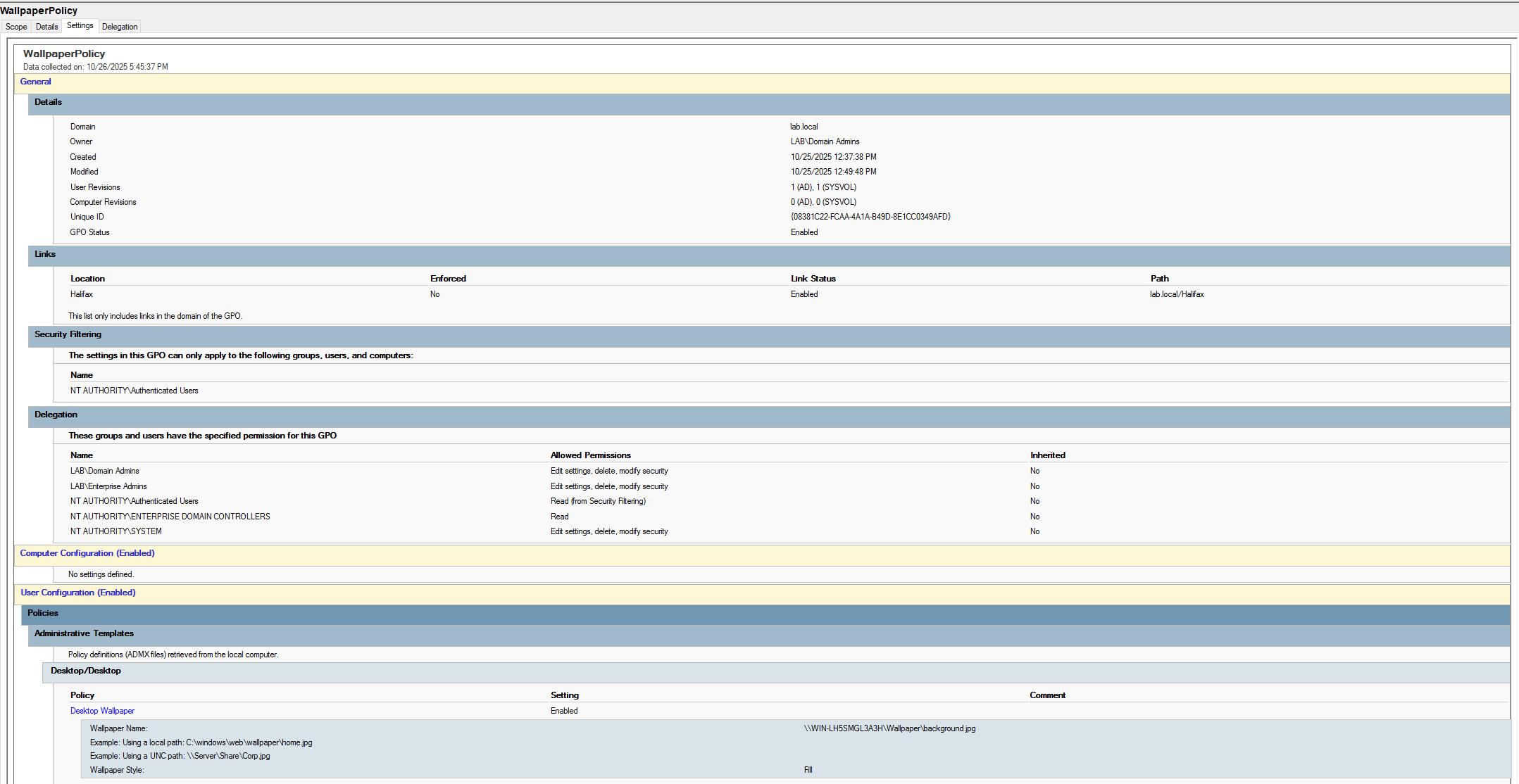
Description: Configured the Windows 11 client (WIN11) with Host-Only IP 192.168.56.20, subnet mask 255.255.255.0, and DNS 192.168.56.10. This allows the client to communicate with SERVER01 and resolve lab.local through the domain controller.

## 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: Deploy a Unified Wallpaper Policy via GPO



**Description:**  
A new Group Policy Object (GPO) named **WallpaperPolicy** was created under the domain *lab.local*.  
This policy enforces a unified desktop wallpaper for all domain users to maintain a consistent corporate appearance.

In **Group Policy Management Editor**, the following configuration was applied:

User Configuration → Administrative Templates → Desktop → Desktop → Desktop Wallpaper

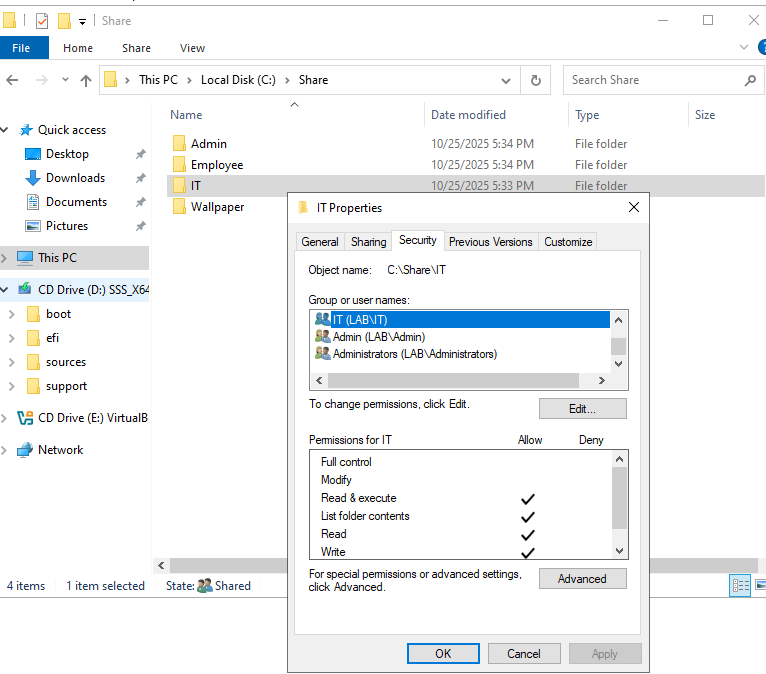
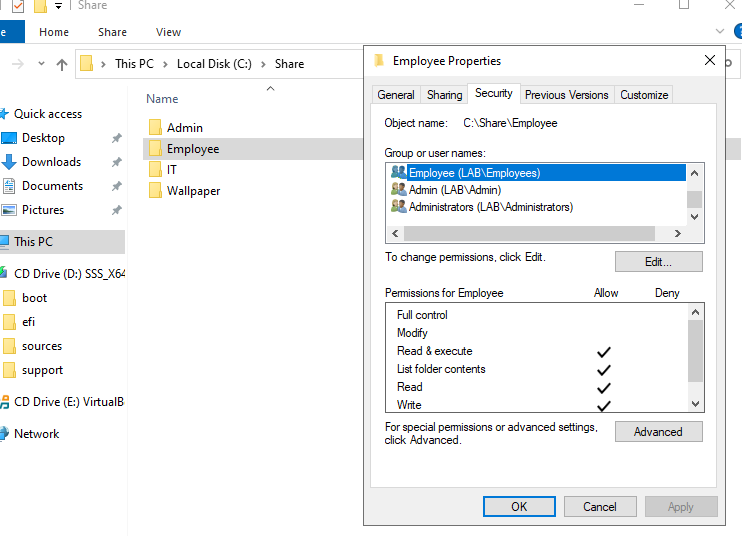
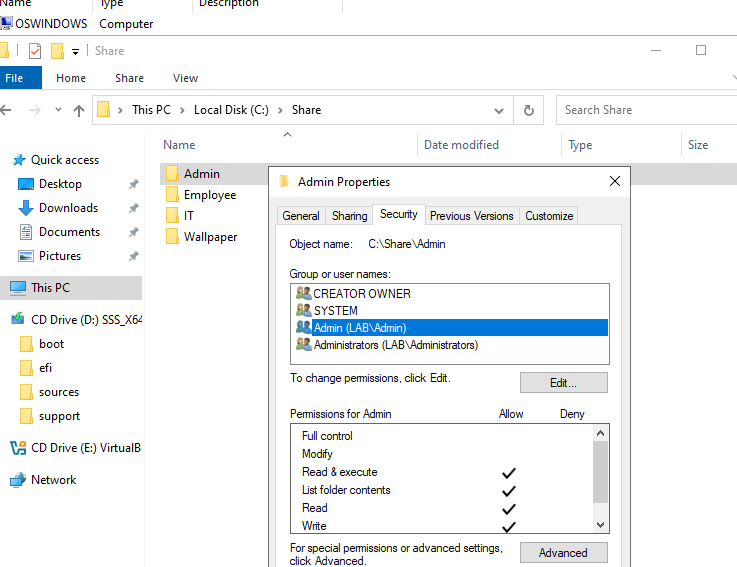
The wallpaper path was set to:

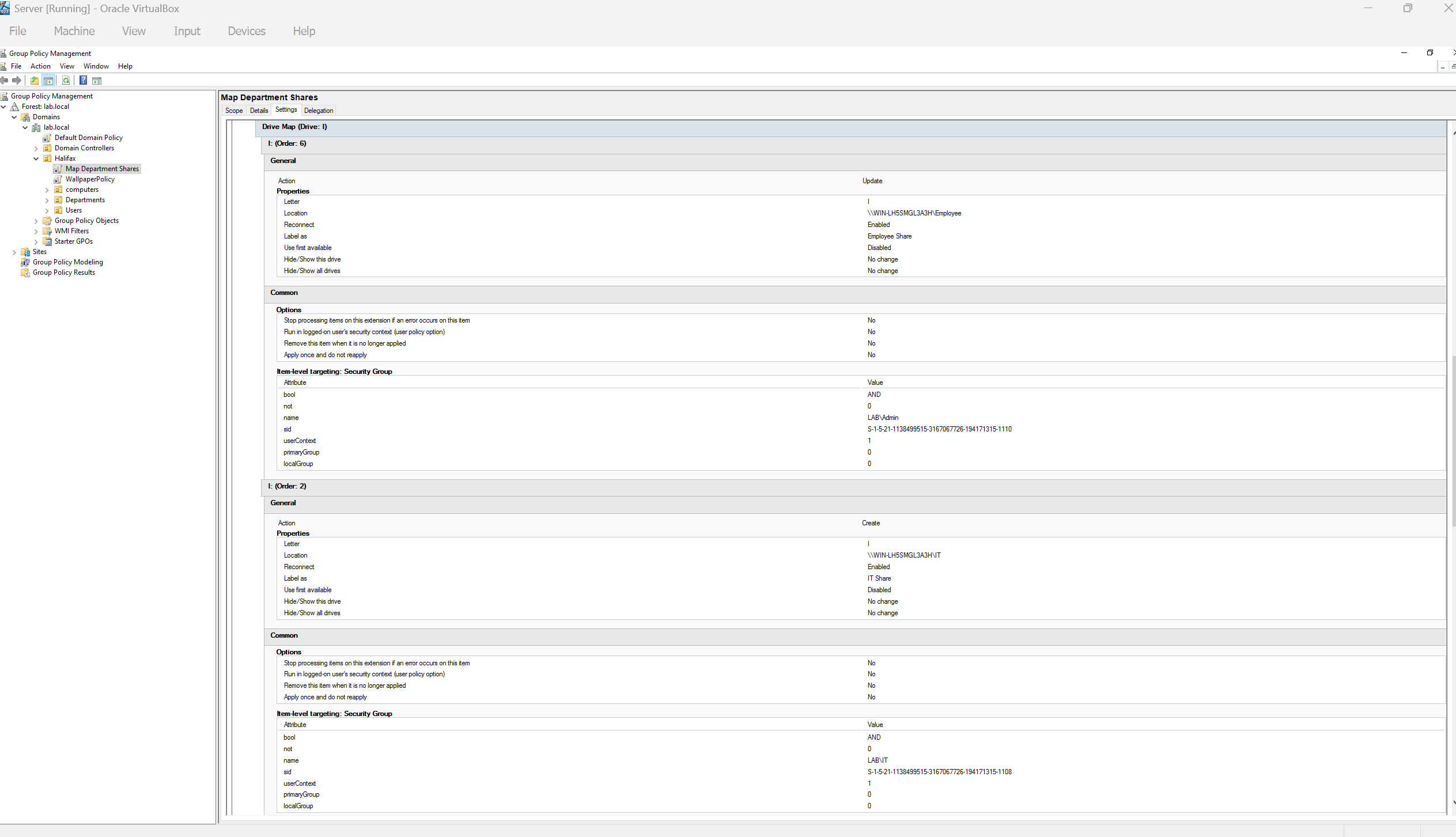
\\SERVER01\Wallpaper\background.jpg

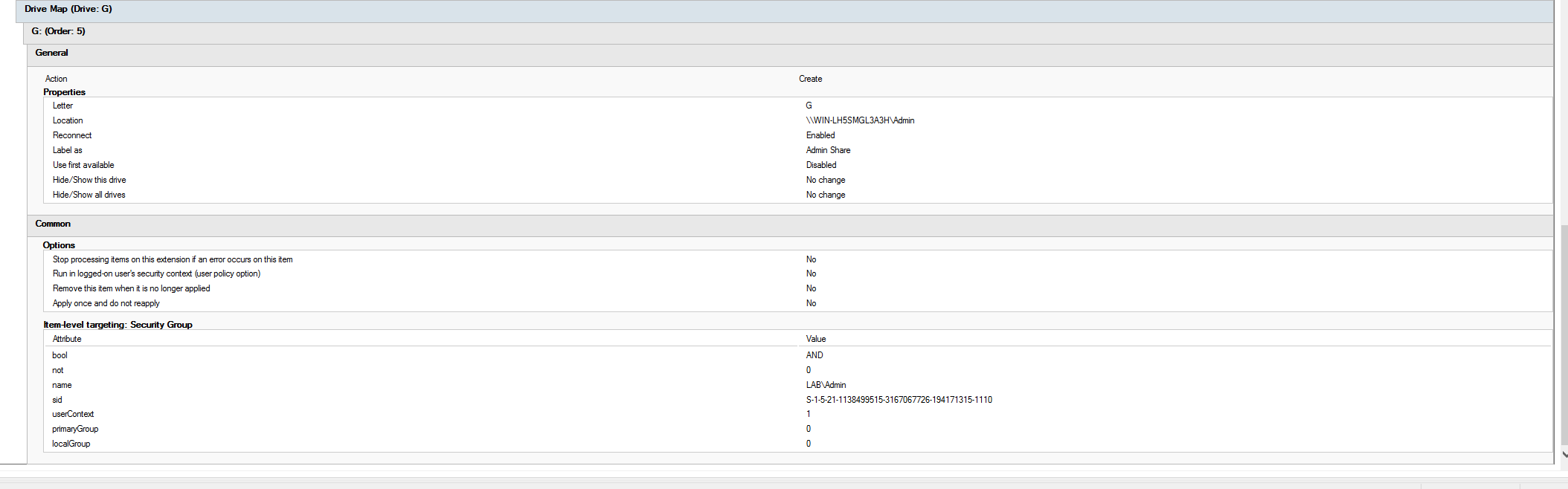
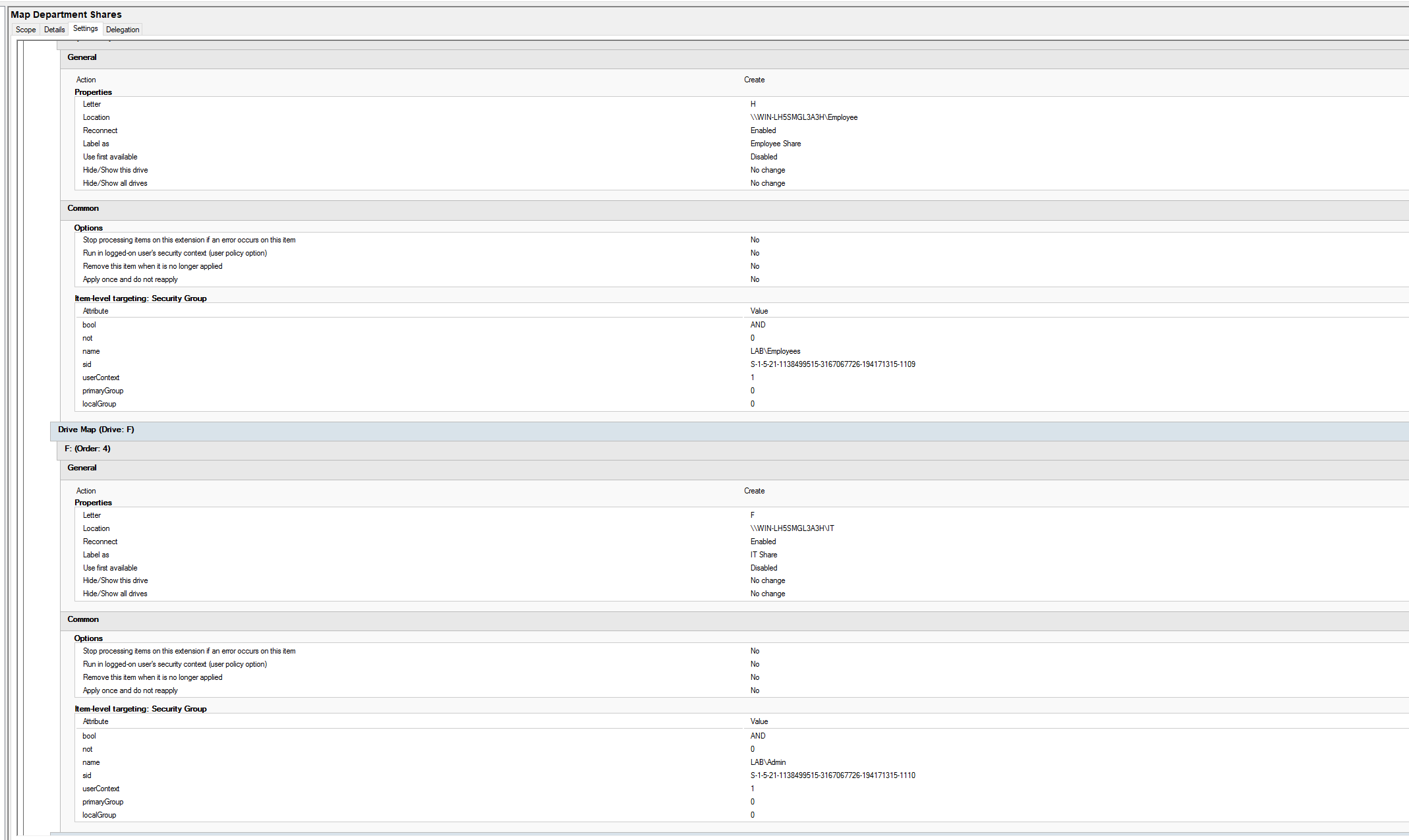
and the wallpaper style was set to **Fill**.

After running gpupdate /force on the client and re-logging in,  
all domain users’ desktops displayed the same background, confirming successful policy deployment.

## Step 10: Set Up Shared Folders and Verify Permissions

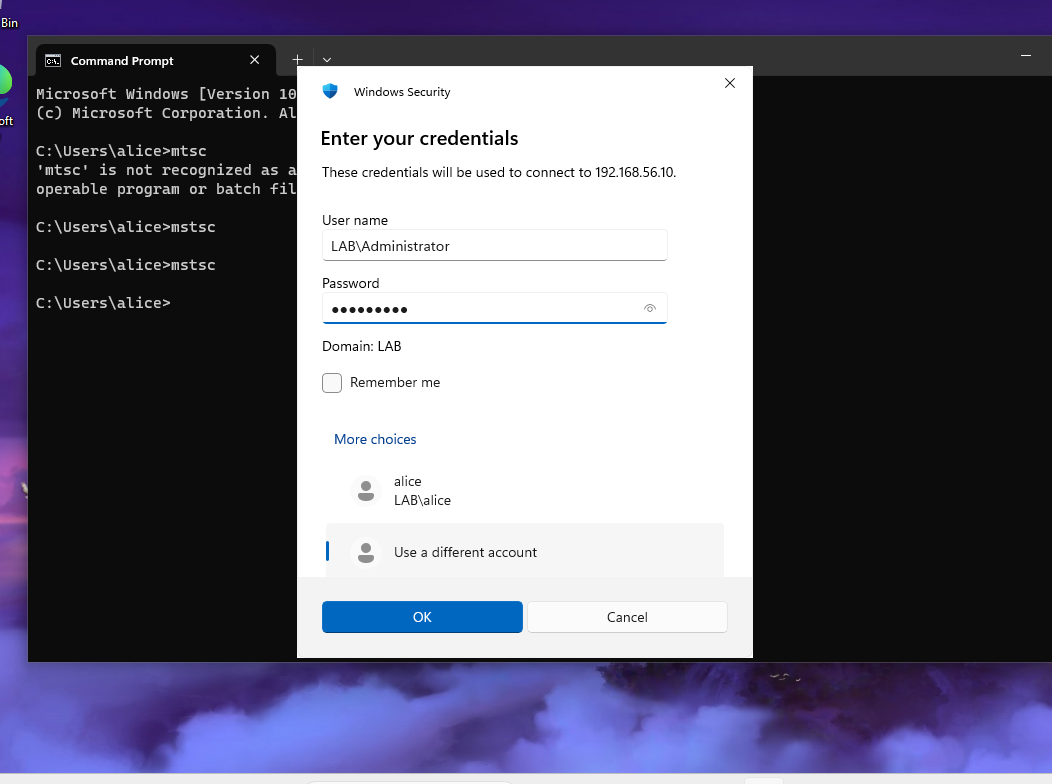


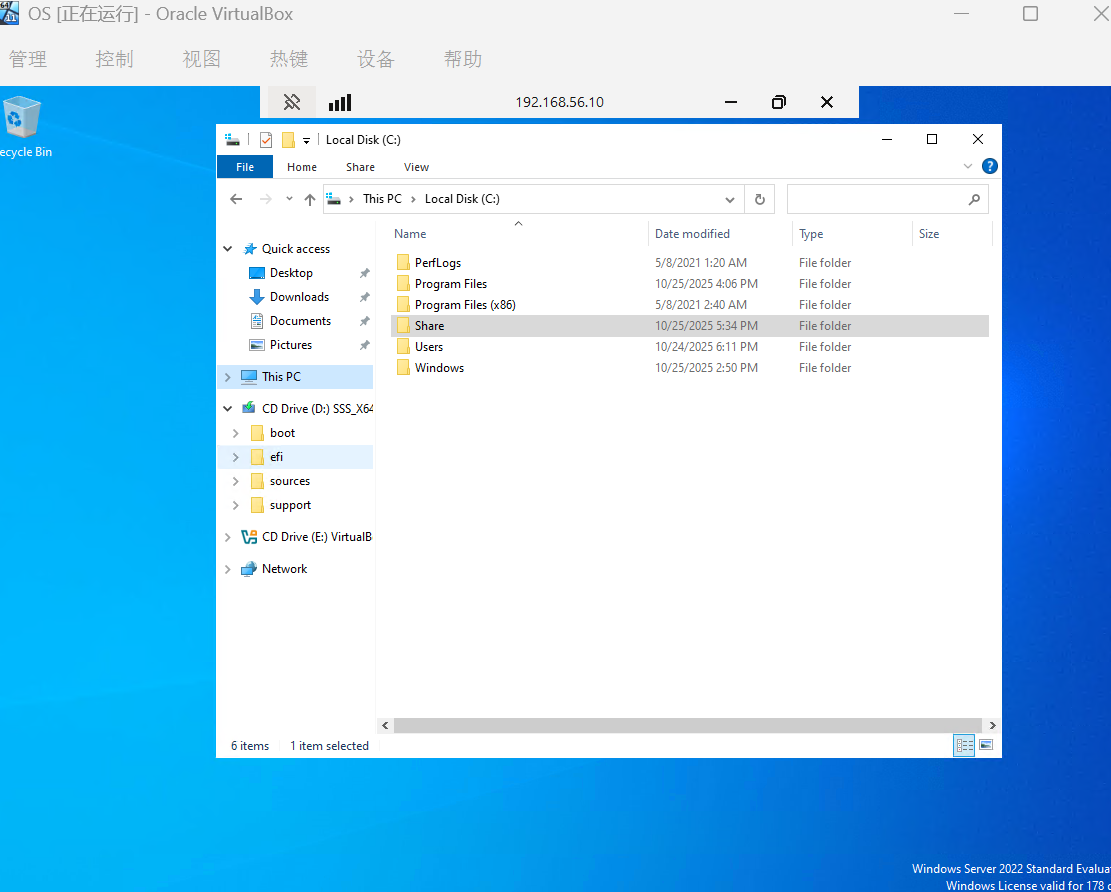




Description: Created shared folders D:\Share\IT and D:\Share\HR on DC. Configured Share and NTFS permissions — IT folder accessible only to IT group and Admin group, Employee folder accessible only to Employee group and Admin group, Admin folder only to Admin group. On the client, \ WIN-LH5SMGL3A3H \IT,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

## Step 11: 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 SERVER01 via mstsc using LAB\Administrator credentials.

# 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.