

# Active Directory Domain Environment Deployment and Permission Management Report

---

## Basic Information

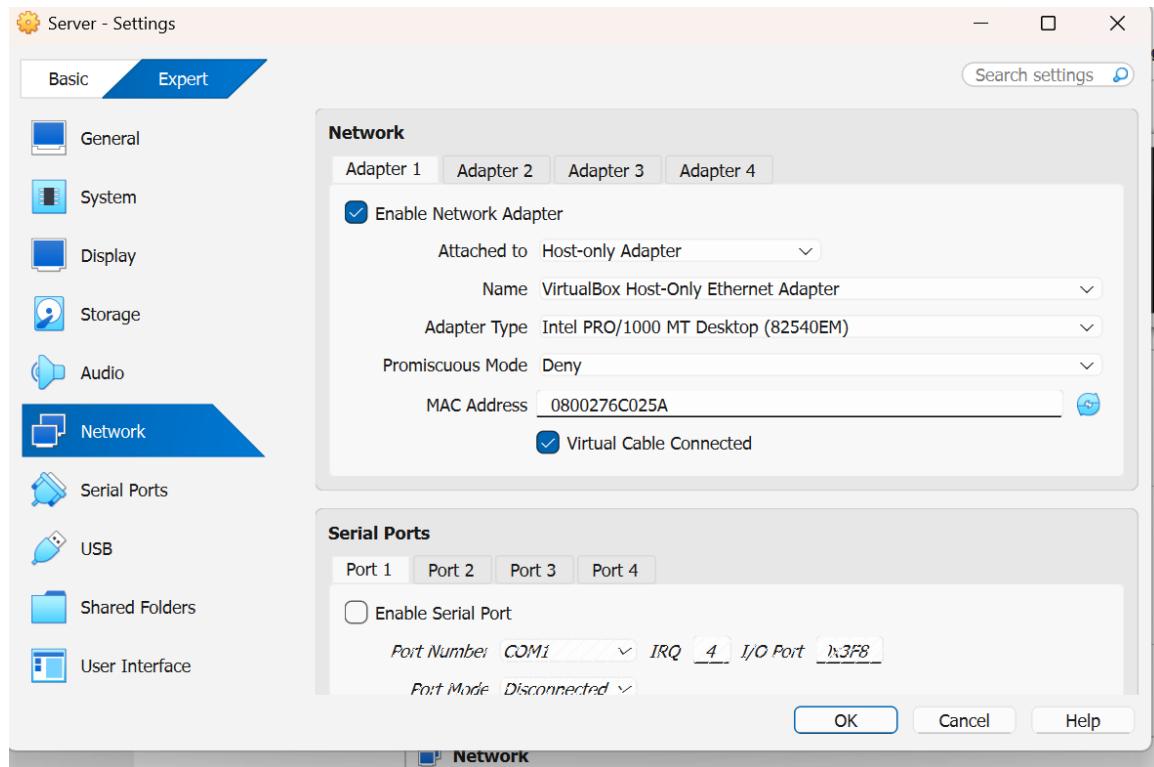
Name	Gaoyuan Zhang
Student ID	B00961366
Date	October 26, 2025
Environment	Oracle VirtualBox + Windows Server 2022 + Windows 11
Objective	Build a complete Active Directory (AD) domain environment in a virtualized lab, enabling user management, group policy deployment, and file-sharing permission control.
File Name	AD_Lab_Deployment_Report_EN_Full_GaoyuanZhang_B00961366.docx

## Experiment Steps and Results

### Step 0: Prepare Virtual Machines and ISO Images

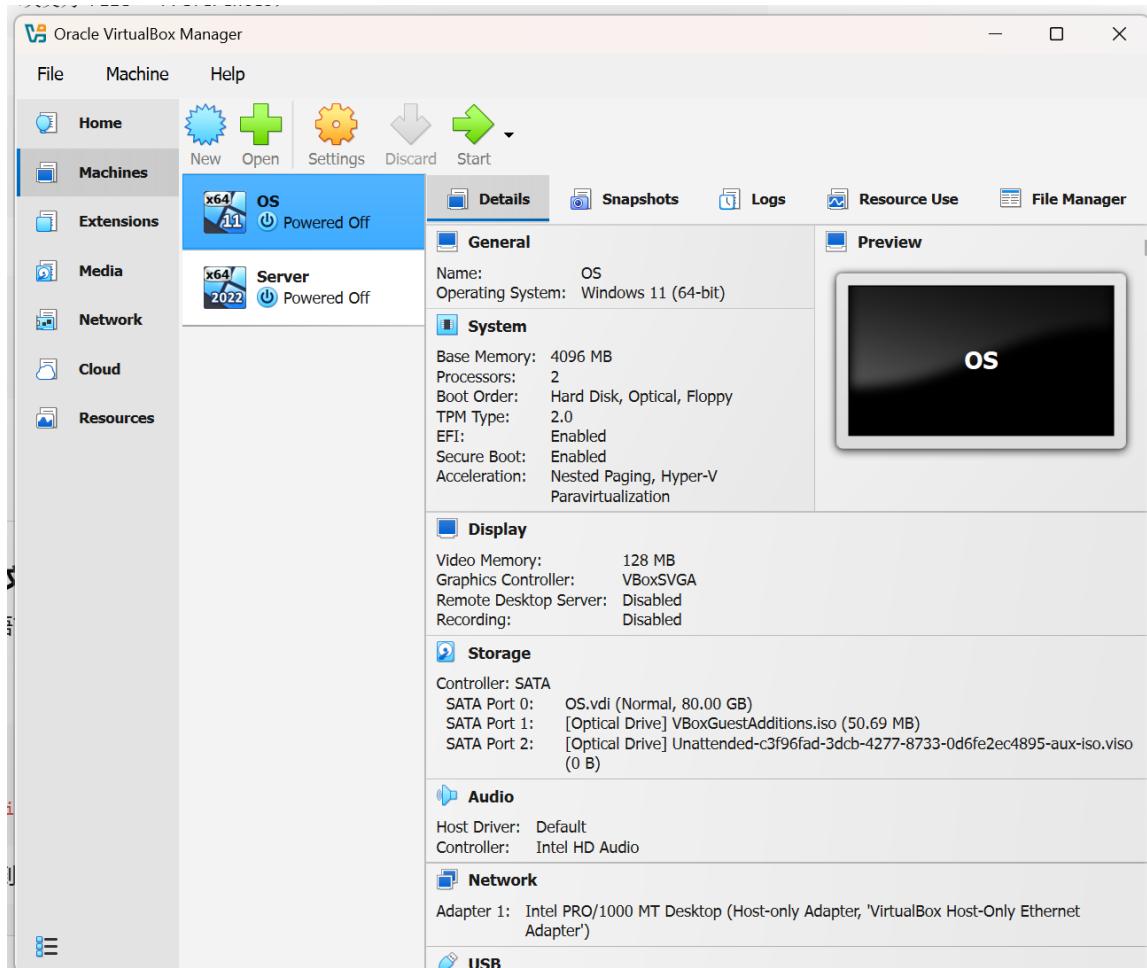
Description: Two virtual machines were created in Oracle VirtualBox — one for Windows Server 2022 and another for Windows 11. Server01 was configured with 4–8GB RAM, 60GB+ disk, and two CPUs. The Windows 11 client had 4GB RAM and 40GB+ disk. Installation ISO files for both systems were attached for setup.

### 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)



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

Administrator: Command Prompt  
 C:\Users\Administrator>ipconfig /all  
 Windows IP Configuration  
 Host Name . . . . . : WIN-LH55MGL3A3H  
 Primary Dns Suffix . . . . . : lab.local  
 Node Type . . . . . : Hybrid  
 IP Routing Enabled. . . . . : No  
 WINS Proxy Enabled. . . . . : No  
 DNS Suffix Search List. . . . . : lab.local  
 Ethernet adapter Ethernet:  
 Connection-specific DNS Suffix . . . :  
 Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter  
 Physical Address . . . . . : 08-00-27-6C-02-5A  
 DHCP Enabled. . . . . : No  
 Autoconfiguration Enabled . . . . . : Yes  
 Link-local IPv6 Address . . . . . : fe80::2121:a20d:beaa:1470%2(Preferred)  
 IPv4 Address . . . . . : 192.168.56.10(Preferred)  
 Subnet Mask . . . . . : 255.255.255.0  
 Default Gateway . . . . . :  
 DHCPv6 IAID . . . . . : 101187623  
 DHCPv6 Client DUID . . . . . : 00-01-00-01-30-8E-12-93-08-00-27-6C-02-5A  
 DNS Servers . . . . . : ::1  
 127.0.0.1  
 NetBIOS over Tcpip. . . . . : Enabled  
 C:\Users\Administrator>

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

The screenshot shows the Windows Server Manager interface. The left navigation pane is collapsed, and the main content area displays two sections: 'SERVERS' and 'EVENTS'.

**SERVERS**  
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update
WIN-LH5SMGL3A3H	192.168.56.10	Online - Performance counters not started	10/26/2025 5:23:06 PM

**EVENTS**  
All events | 18 total

Server Name	ID	Severity	Source	Log
WIN-LH5SMGL3A3H	3054	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory
WIN-LH5SMGL3A3H	3051	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory
WIN-LH5SMGL3A3H	1539	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory

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

```
C:\Users\Administrator>nslookup _ldap._tcp.dc._msdcs.lab.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:      _ldap._tcp.dc._msdcs.lab.local

C:\Users\Administrator>nlttest /dsgetdc:lab.local
DC: \\WIN-LH5SMGL3A3H.lab.local
Address: \\192.168.56.10
Dom Guid: e4f6c514-c042-42e4-be59-485f7d067122
Dom Name: lab.local
Forest Name: lab.local
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10 KEYLIST
The command completed successfully

C:\Users\Administrator>
```

Description: Verified the AD installation using diagnostic commands: nslookup \_ldap.\_tcp.dc.\_msdcs.lab.local and nlttest /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).

Name	Type	Description
computers	Organizational...	
Departments	Organizational...	
Users	Organizational...	

Server [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Active Directory Users and Computers

File Action View Help

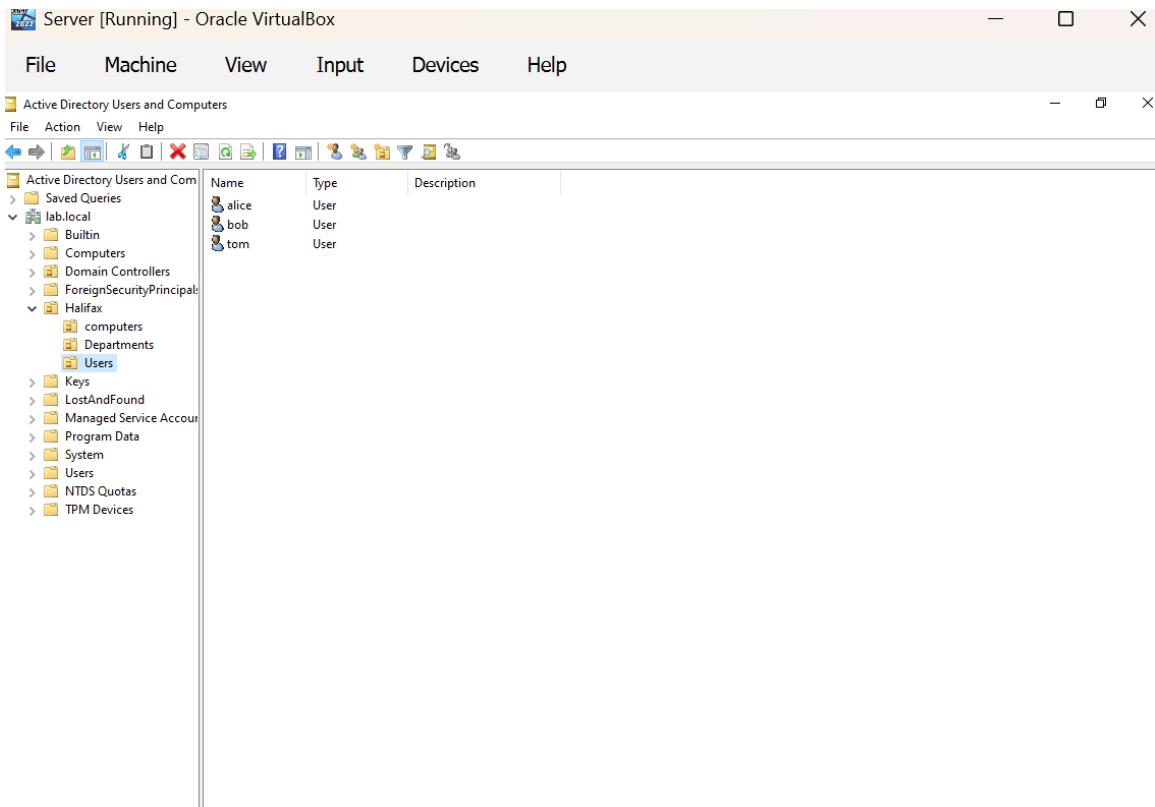
Active Directory Users and Computers

Name Type Description

Name	Type	Description
Admin	Security Group...	
Employee	Security Group...	
IT	Security Group...	

Saved Queries  
lab.local  
Builtin  
Computers  
Domain Controllers  
ForeignSecurityPrincipals  
Halifax  
computers  
Departments  
Users  
Keys  
LostAndFound  
Managed Service Account  
Program Data  
System  
Users  
NTDS Quotas  
TPM Devices

< >



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

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

Windows IP Configuration

Host Name . . . . . : OSWindows
Primary Dns Suffix . . . . . : lab.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : lab.local

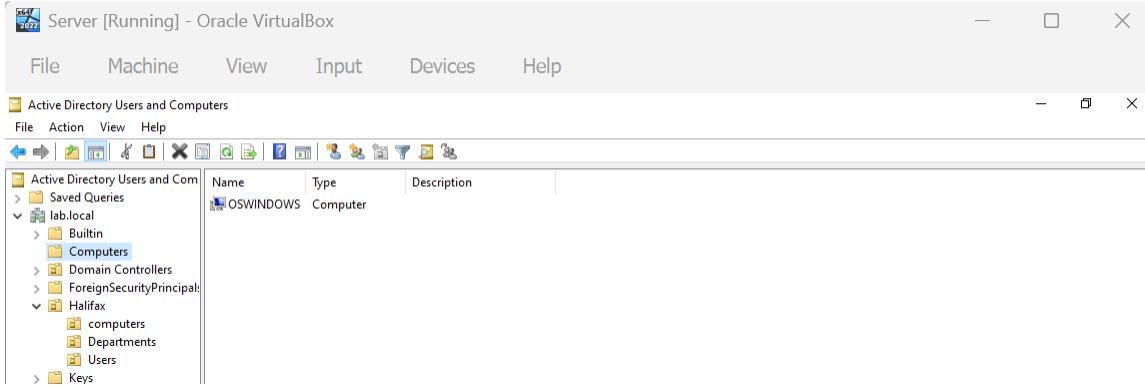
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-77-8C-9D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f03b:fc9e:b54a:748f%7(Preferred)
IPv4 Address . . . . . : 192.168.56.20(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-8D-E9-05-08-00-27-77-8C-9D
DNS Servers . . . . . : 192.168.56.10
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\alice>
```

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

The screenshot shows the Group Policy Management Editor. The left pane displays the GPO structure: Scope (WallpaperPolicy), Details (General tab), Links (Link tab), Security Filtering (Security Filtering tab), Delegation (Delegation tab), Computer Configuration (Computer Configuration tab), User Configuration (User Configuration tab), Policies (Administrative Templates tab), and Desktop/Display (Desktop/Display tab). The General tab shows the GPO name is WallpaperPolicy, created by LAB\Domain Admins on 10/25/2025 at 12:37:38 PM, and is linked to the lab.local domain. The Security Filtering tab specifies NT AUTHORITY\Authenticated Users as the target. The Delegation tab lists specific permissions for various security principals. The Computer Configuration tab contains a single policy named 'Desktop Wallpapers' with the setting 'Enabled'. The User Configuration tab and Policies tab are empty. The Desktop/Display tab also contains a single policy named 'Desktop Wallpapers' with the setting 'Enabled'.

### 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

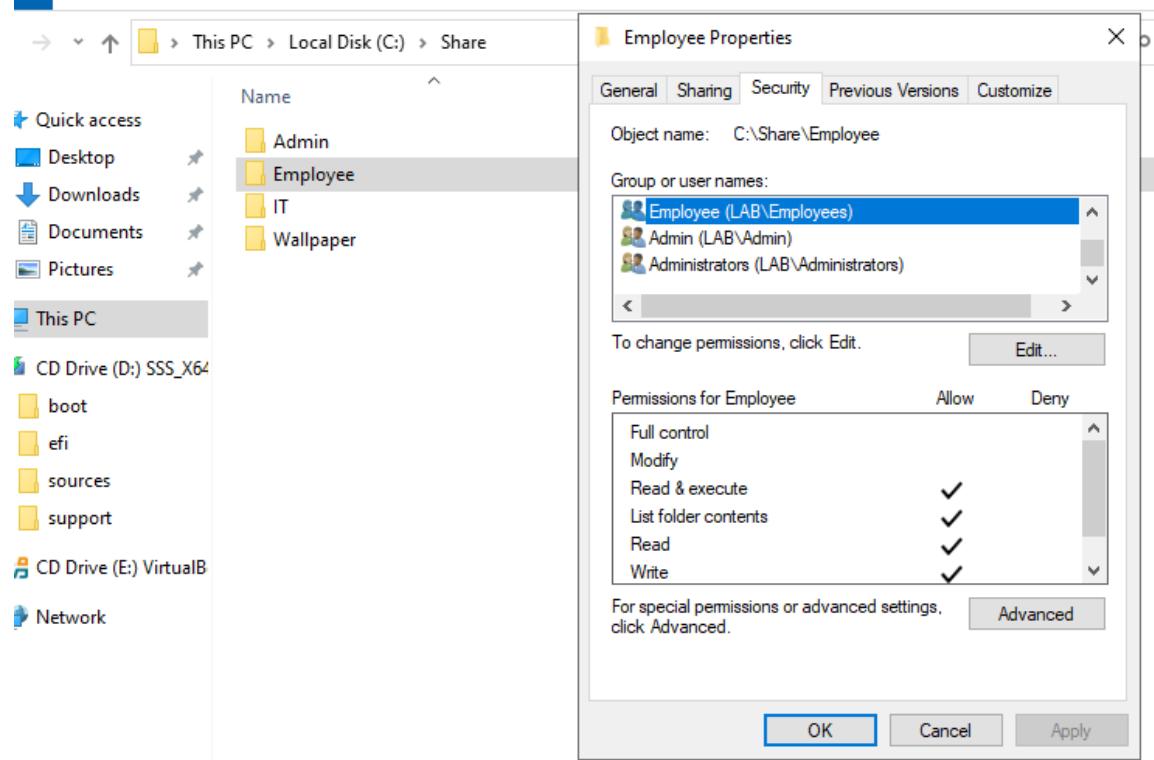
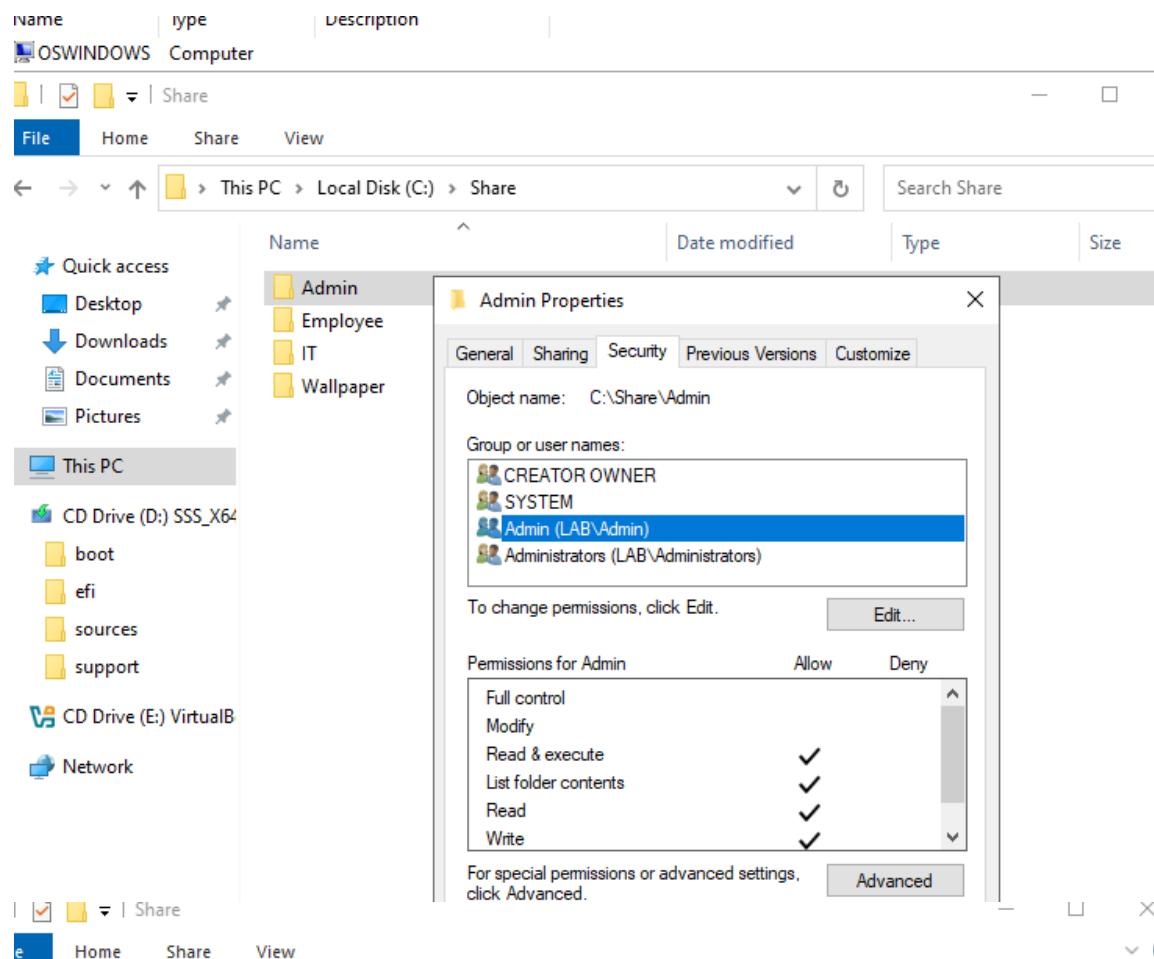
The wallpaper path was set to:

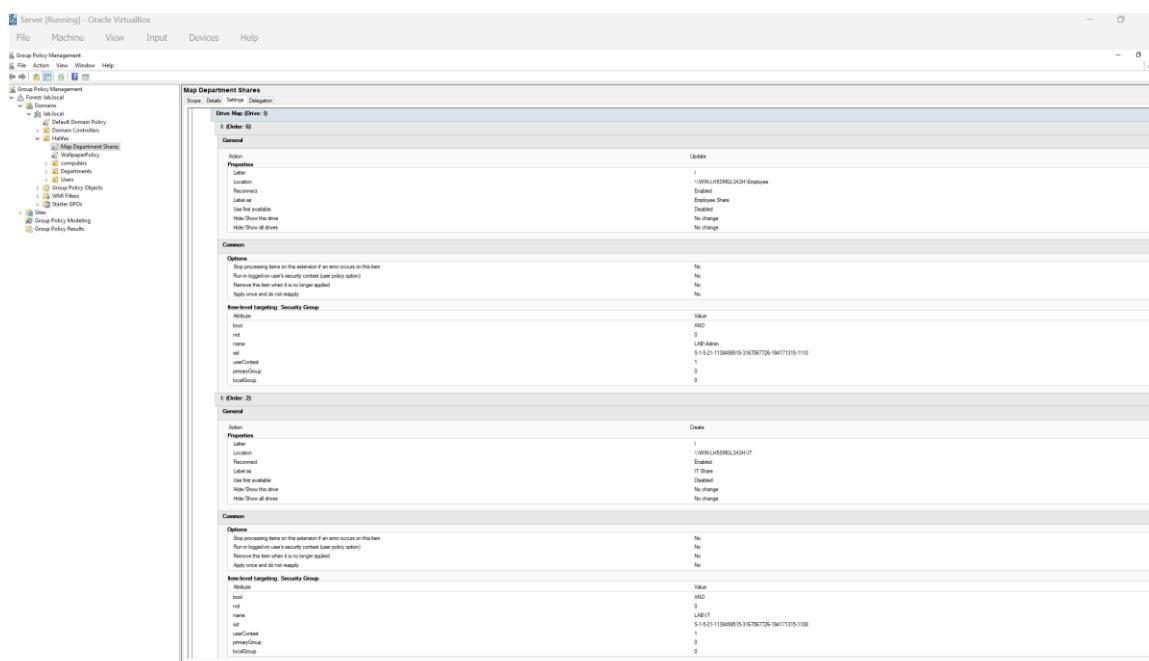
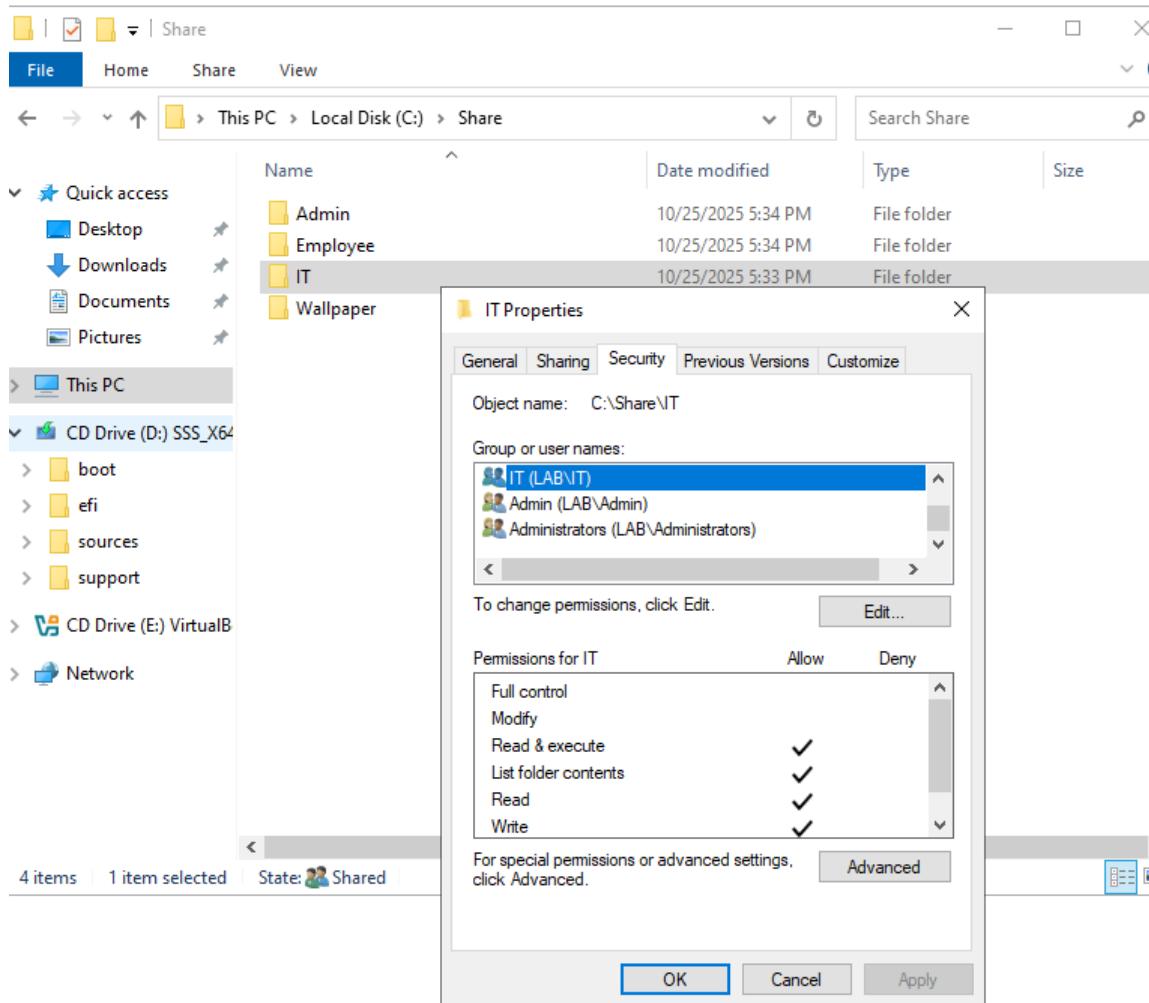
\\ WIN-LH5SMGL3A3H \Wallpaper\background.jpg

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**





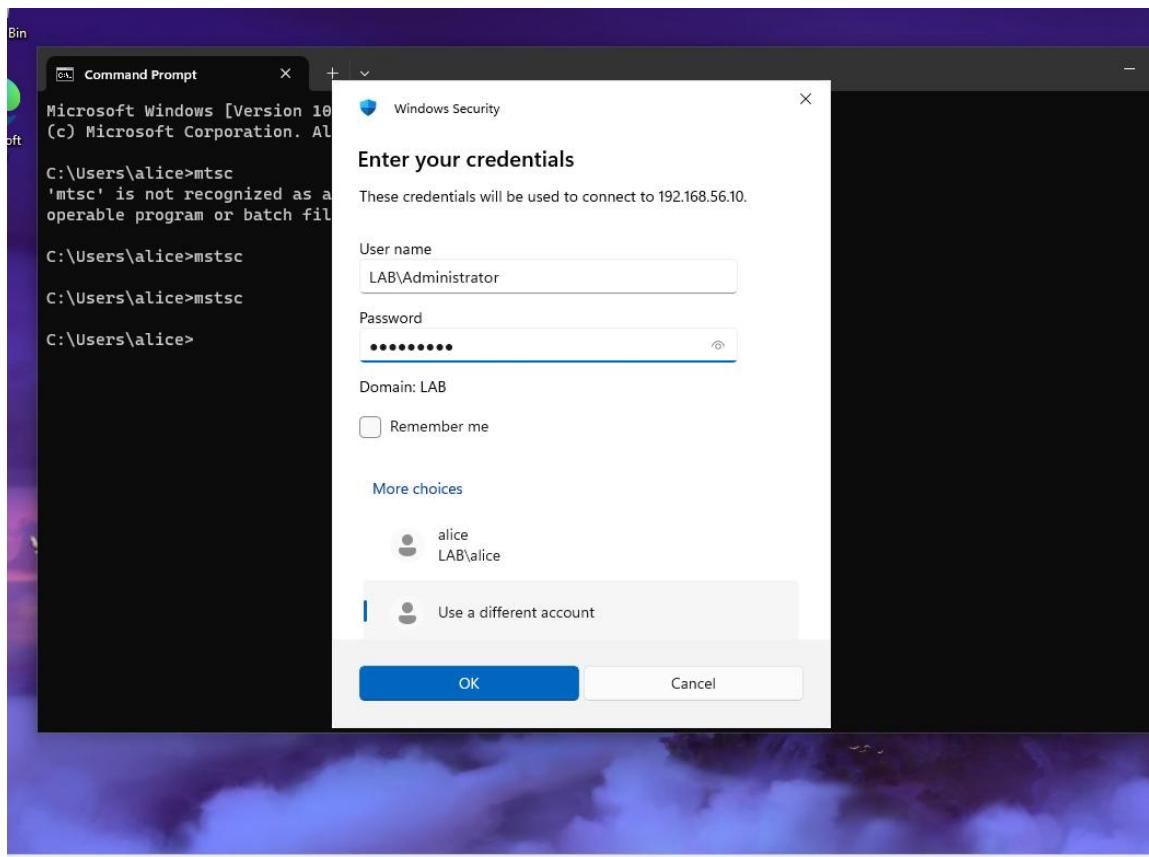
**Map Department Shares**

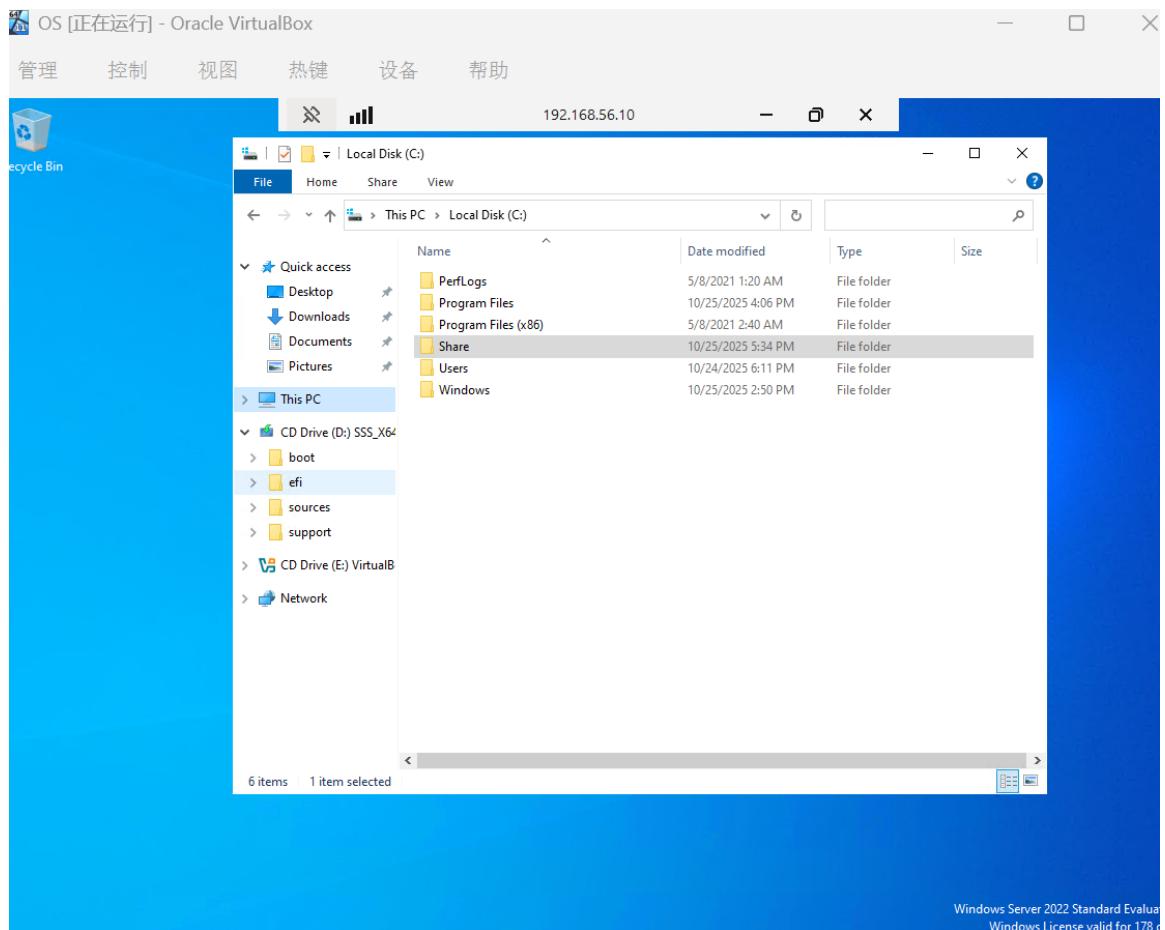
Scope: Details Settings Delegation

<b>General</b>	
Action	Create
Properties	Letter: H Location: \\WIN-LH5SMGL3A3H\Employee Recurred: No Label as: Employee Share Use first available: Disabled Hide/Show this drive: No change Hide/Show all drives: No change
<b>Common</b>	
Options	Stop processing items on this extension if an error occurs on this item: No Run in logged-on user's security context (User policy option): No Remove this item when it is no longer applied: No Apply once and do not reapply: No
Item-level targeting: Security Group	Attribute: Value bool: AND not: 0 name: LAB\Admin ad: S-1-5-21-1138499515-3167067726-194171315-1110 useContext: 1 parentGroup: 0 localGroup: 0
<b>Drive Map (Drive: F)</b>	
<b>F (Order: 4)</b>	
<b>General</b>	
Action	Create
Properties	Letter: F Location: \\WIN-LH5SMGL3A3H\IT Recurred: No Label as: IT Share Use first available: Disabled Hide/Show this drive: No change Hide/Show all drives: No change
<b>Common</b>	
Options	Stop processing items on this extension if an error occurs on this item: No Run in logged-on user's security context (User policy option): No Remove this item when it is no longer applied: No Apply once and do not reapply: No
Item-level targeting: Security Group	Attribute: Value bool: AND not: 0 name: LAB\Admin ad: S-1-5-21-1138499515-3167067726-194171315-1110 useContext: 1 parentGroup: 0 localGroup: 0
<b>Drive Map (Drive: G)</b>	
<b>G (Order: 5)</b>	
<b>General</b>	
Action	Create
Properties	Letter: G Location: \\WIN-LH5SMGL3A3H\Admin Recurred: No Label as: Admin Share Use first available: Disabled Hide/Show this drive: No change Hide/Show all drives: No change
<b>Common</b>	
Options	Stop processing items on this extension if an error occurs on this item: No Run in logged-on user's security context (User policy option): No Remove this item when it is no longer applied: No Apply once and do not reapply: No
Item-level targeting: Security Group	Attribute: Value bool: AND not: 0 name: LAB\Admin ad: S-1-5-21-1138499515-3167067726-194171315-1110 useContext: 1 parentGroup: 0 localGroup: 0

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.