Active Directory Home Lab: Creation & Security Hardening

Domain: mopetech.ai

Environment: Oracle VirtualBox

Operating Systems: Windows Server 2022 (DC), Windows 8.1 (Client)

📖 Overview

This project demonstrates the deployment of a Windows-based network infrastructure. The primary focus was implementing the Principle of Least Privilege (PoLP) through structured Organizational Units (OUs) and restrictive Group Policy Objects (GPOs).

🛠️ Step 1: Domain Controller & Forest Setup

I promoted a Windows Server 2022 instance to a primary domain controller for the forest **(mopetech.ai).**

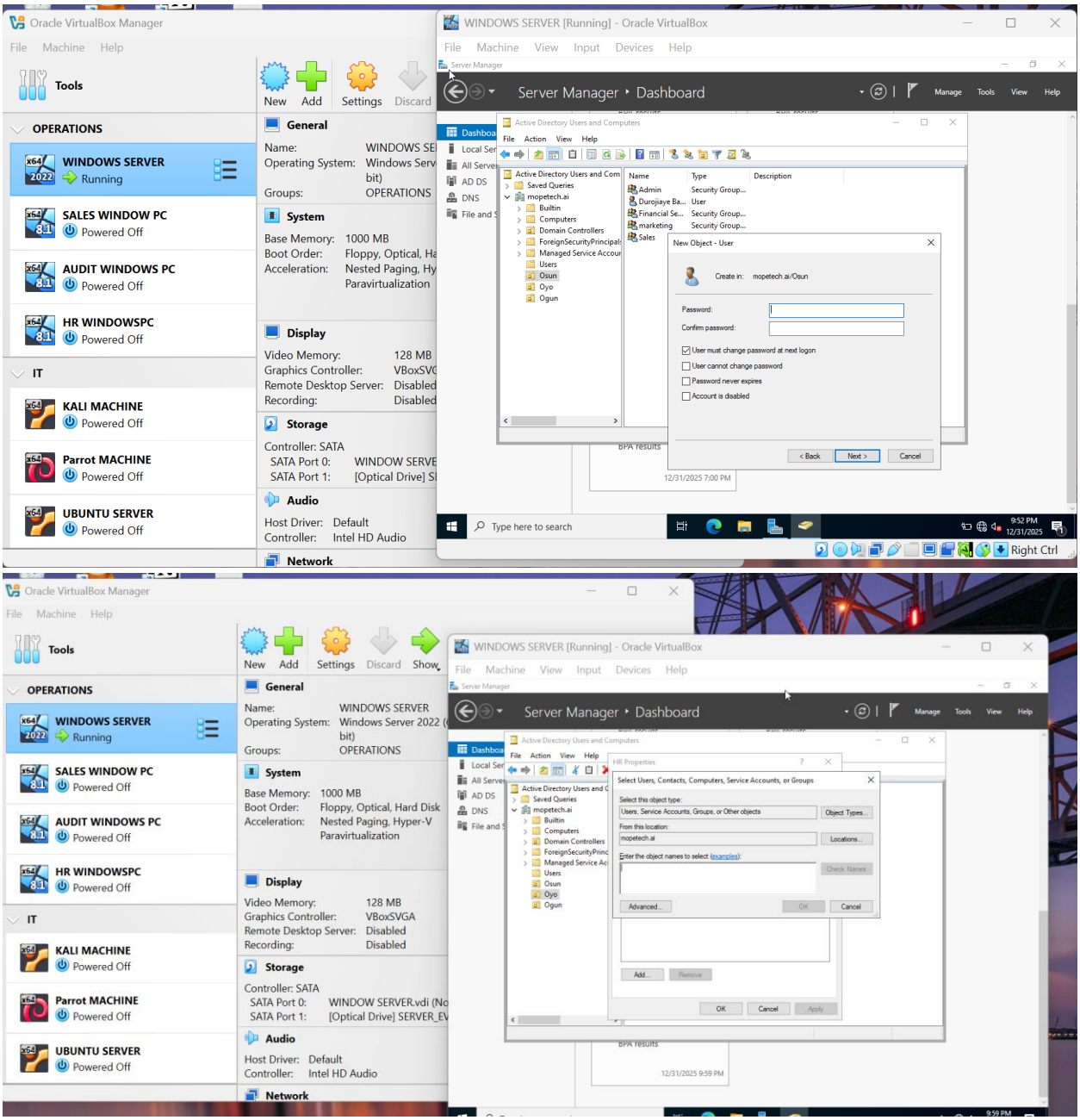
- **Role Installation:** Configured Active Directory Domain Services (AD DS) and DNS.
- **Infrastructure:** Set up the server with 1000 MB Base Memory and VBoxSVGA graphics for stable virtualization.

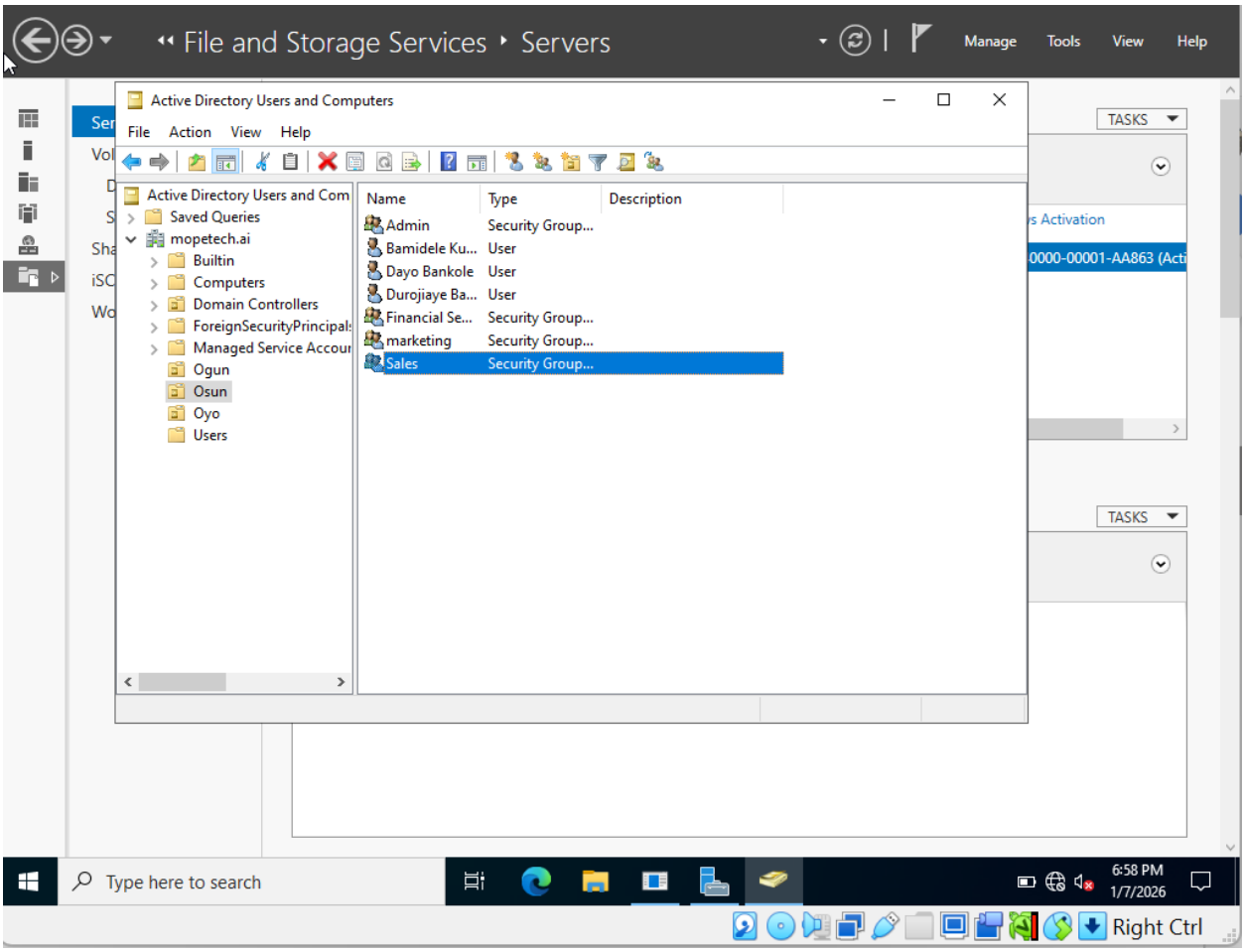
📂 Step 2: Directory Organization (OU Structure)

Following best practices, I moved away from a "flat" directory. I created regional Organisational Units (OU) to manage users and resources efficiently:

- **OUs Created:** Ogun, Osun, Oyo.
- **Administrative Groups:** These security groups were created: Sales, HR, Consultation, Finance, Booking, and Support handle Role-Based Access Control (RBAC).

- Users: Bamidele.Kurode, Durojaiye.Bande, Dayo Bankole, Rasaq Lawal, Dara Gbemi, Kunle Sean, Funmi Kosope.

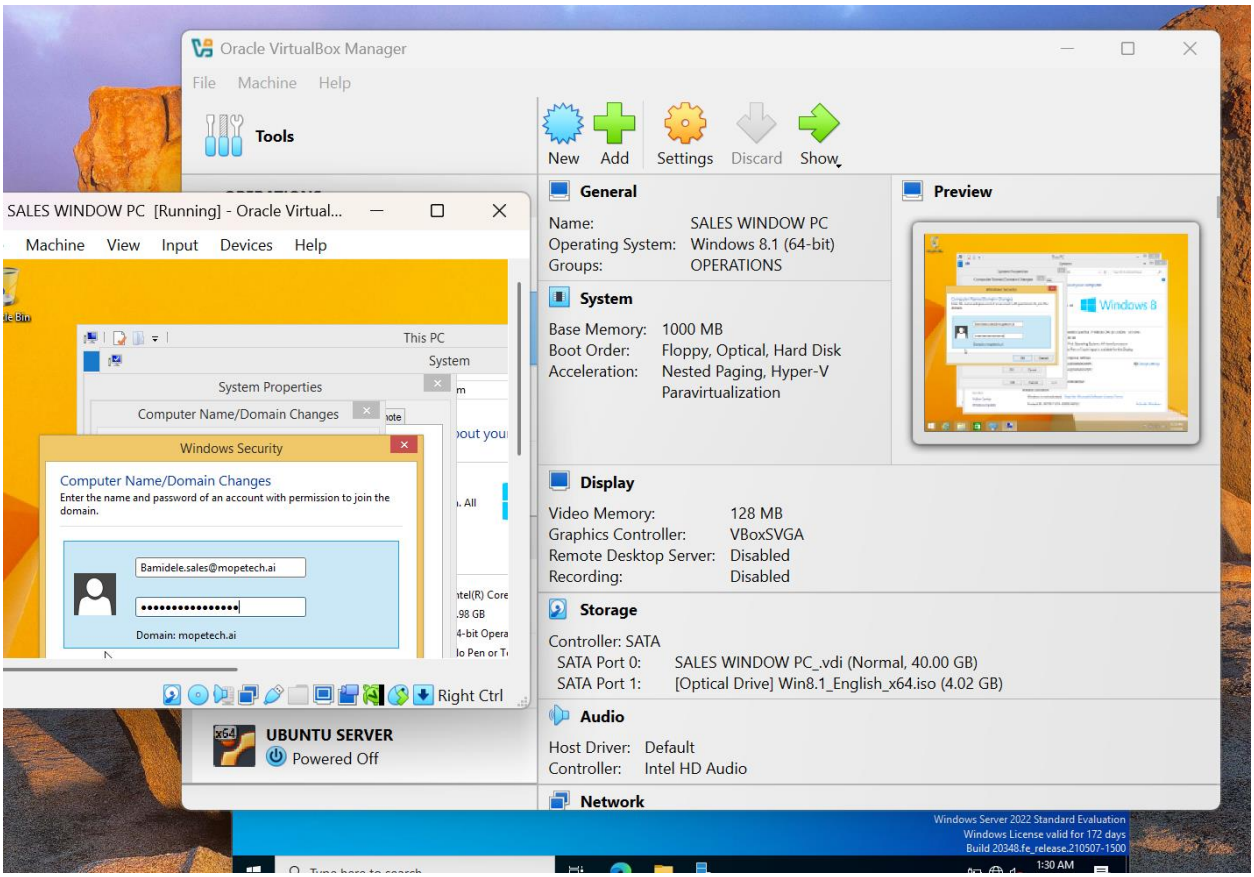

Oracle VirtualBox Manager
File Machine Help
Tools
OPERATIONS
WINDOWS SERVER
Running
SALES WINDOW PC
Powered Off
AUDIT WINDOWS PC
Powered Off
HR WINDOWSPC
Powered Off
IT
KALI MACHINE
Powered Off
Parrot MACHINE
Powered Off
UBUNTU SERVER
Powered Off
New Add Settings Discard
General
Name: WINDOWS SE
Operating System: Windows Serv
bit)
Groups: OPERATIONS
System
Base Memory: 1000 MB
Boot Order: Floppy, Optical, Ha
Acceleration: Nested Paging, Hy
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVG
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: WINDOW SERVE
SATA Port 1: [Optical Drive] S
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
WINDOWS SERVER [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
mopetech.ai
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Osun
Oyo
Ogun
Name Type Description
Admin Security Group...
Durojiaye Ba... User
Financial Se... Security Group...
marketing Security Group...
Sales
New Object - User
Create in: mopetech.ai/Osun
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back Next > Cancel
BPA results
12/31/2025 7:00 PM
Type here to search
9:52 PM
12/31/2025
Right Ctrl
Oracle VirtualBox Manager
File Machine Help
Tools
OPERATIONS
WINDOWS SERVER
Running
SALES WINDOW PC
Powered Off
AUDIT WINDOWS PC
Powered Off
HR WINDOWSPC
Powered Off
IT
KALI MACHINE
Powered Off
Parrot MACHINE
Powered Off
UBUNTU SERVER
Powered Off
New Add Settings Discard Show
General
Name: WINDOWS SERVER
Operating System: Windows Server 2022 (
bit)
Groups: OPERATIONS
System
Base Memory: 1000 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: WINDOW SERVER.vdi (No
SATA Port 1: [Optical Drive] SERVER_EV
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
WINDOWS SERVER [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and Computers
File Action View Help
HR Properties
Select Users, Contacts, Computers, Service Accounts, or Groups
Select this object type:
Users, Service Accounts, Groups, or Other objects
Object Types...
From this location:
mopetech.ai
Locations...
Enter the object names to select (examples):
Check Names
Advanced... OK Cancel
Add... Remove
OK Cancel Apply
BPA results
12/31/2025 9:59 PM
9:59 PM



Step 3: Client Integration

I successfully joined a Windows 8.1 workstation (SALES WINDOW PC) to the mopetech.ai domain.

- **Authentication:** Verified domain connectivity by logging in with a delegated user account (Bamidele.sales@mopetech.ai).
- **Verification:** Confirmed the "Welcome to the mopetech.ai domain" status via System Properties.



Step 4: Network Configuration & Client Integration

To establish a functional link between the **Windows Server 2022 (DC)** and the **Windows 8.1 (Client)**, I performed a manual network alignment and domain join.

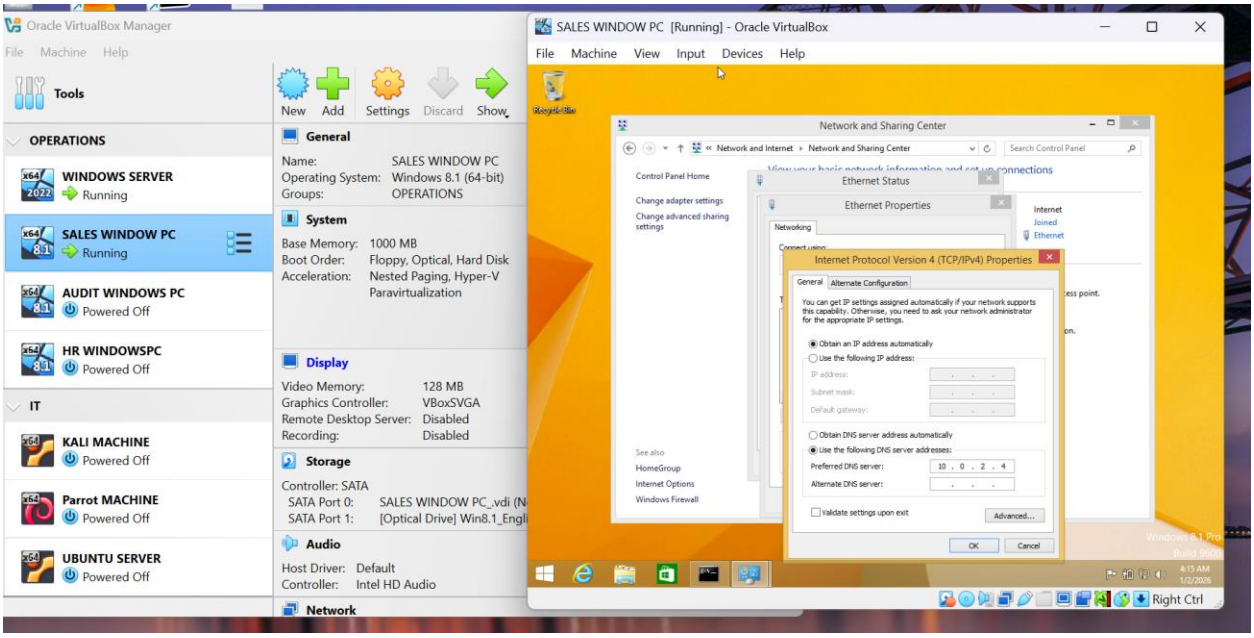
4.1. IP Addressing Schema

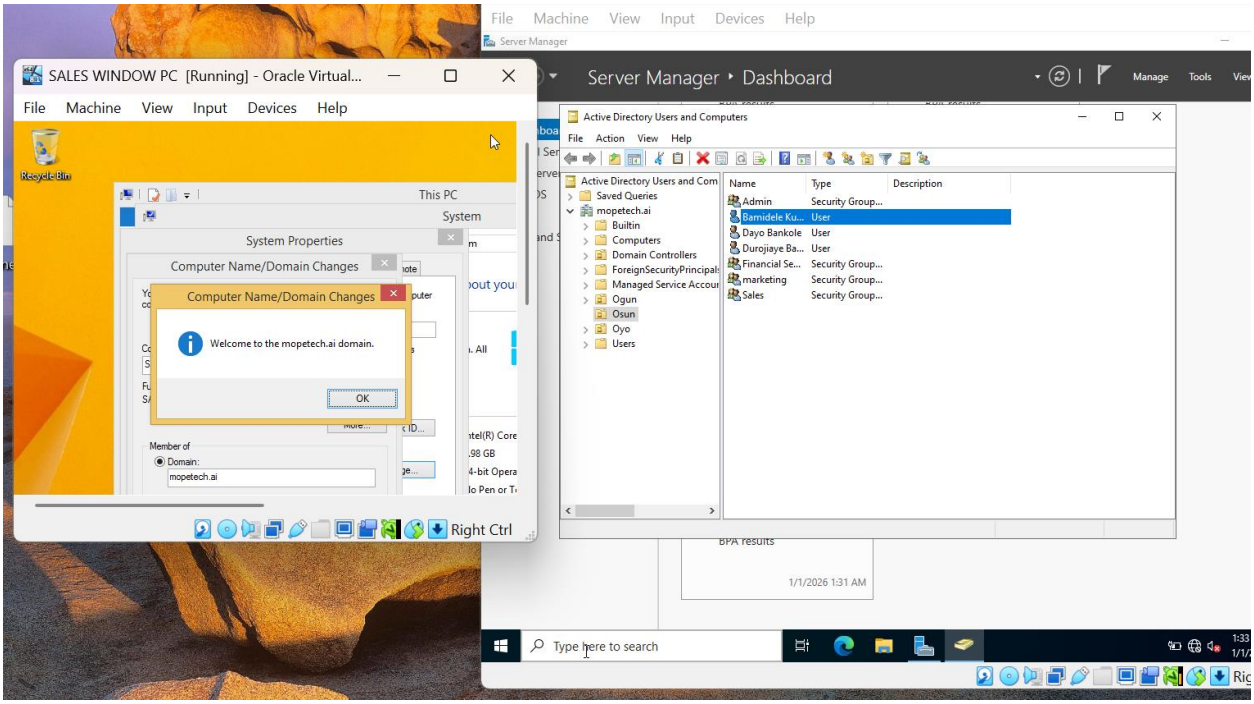
I assigned static IP addresses to ensure persistent connectivity within the virtual network:

Machine	Role	IP Address	DNS Server
Windows Server	Domain Controller	`10.0.2.4`	`127.0.0.1` (Self)
Sales Window PC	Client Workstation	`10.0.2.5`	`10.0.2.4` (DC)

The integration was confirmed successful when the client displayed the **"Welcome to the mopetech.ai domain"** notification.

- **Active Directory Update:** The SALES WINDOW PC object now automatically appears in the **Computers** container within the Active Directory Users and Computers (ADUC) console on the server.



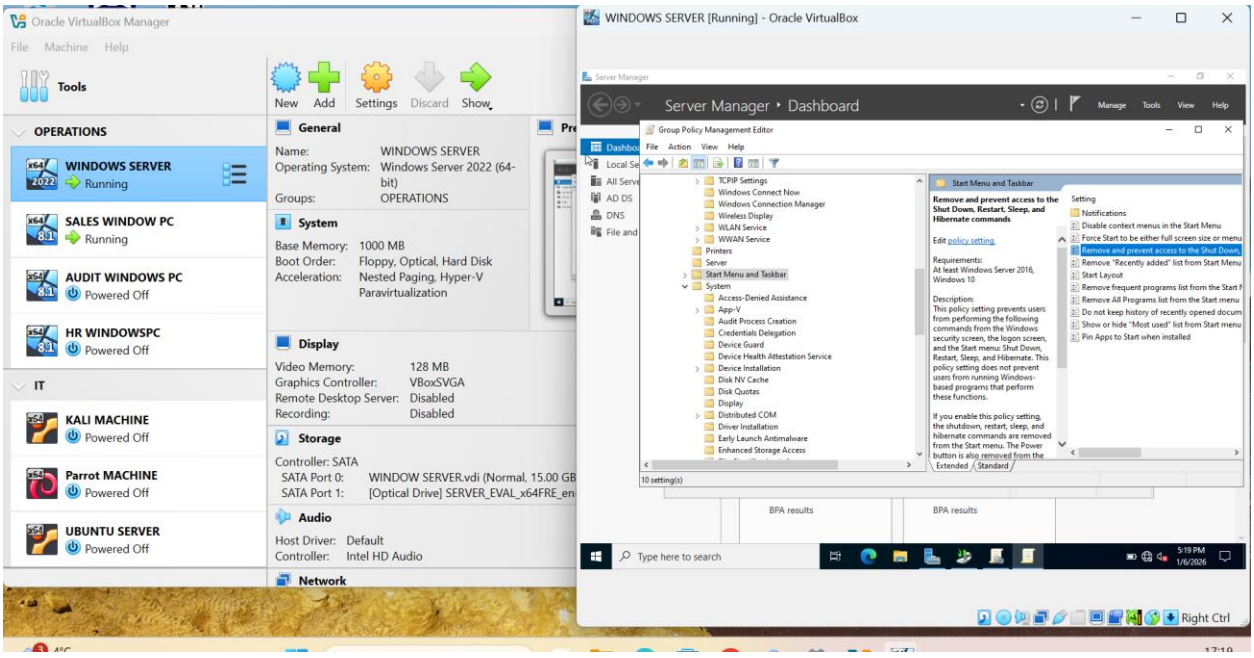


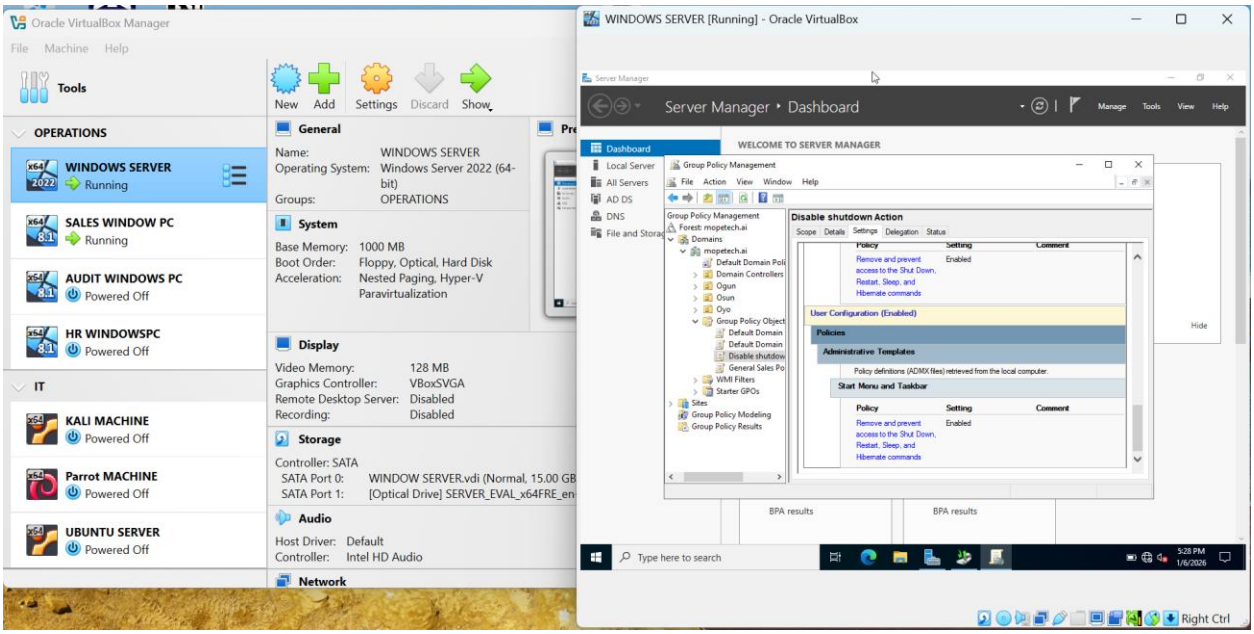
Step 4: Security Hardening (Group Policy)

To enforce the **Principle of Least Privilege**, I configured and deployed specific GPOs to restrict standard user capabilities:

Key Policies Implemented:

1. **Disable Shutdown Action:** Prevented non-admin users from shutting down or restarting the server/workstations via the Start Menu.
2. **Remove Access to Shut Down/Restart:** Enabled the "Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands" policy under *User Configuration > Administrative Templates > Start Menu and Taskbar*.
3. **Firewall Management:** Ensured Inbound Rules were active and monitored via Windows Firewall with Advanced Security.


Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
OPERATIONS
WINDOWS SERVER
Running
SALES WINDOW PC
Running
AUDIT WINDOWS PC
Powered Off
HR WINDOWSPC
Powered Off
IT
KALI MACHINE
Powered Off
Parrot MACHINE
Powered Off
UBUNTU SERVER
Powered Off
General
Name: WINDOWS SERVER
Operating System: Windows Server 2022 (64-bit)
Groups: OPERATIONS
System
Base Memory: 1000 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: WINDOW SERVER.vdi (Normal, 15.00 GB
SATA Port 1: [Optical Drive] SERVER_EVAL_x64FRE_en
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
WINDOWS SERVER [Running] - Oracle VirtualBox
Server Manager • Dashboard
Group Policy Management Editor
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands
BPA results
Type here to search
Right Ctrl

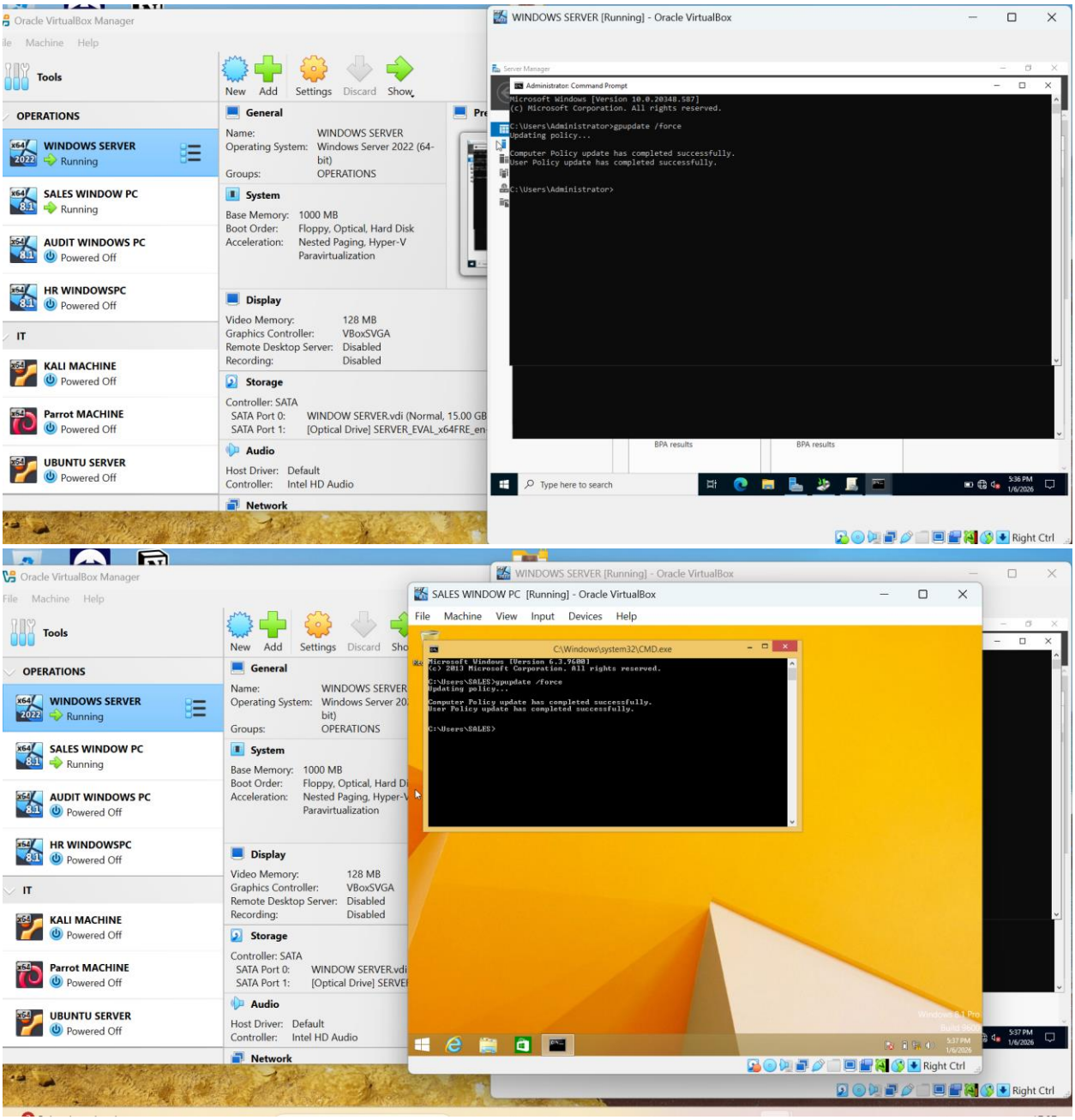

Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
OPERATIONS
WINDOWS SERVER
Running
SALES WINDOW PC
Running
AUDIT WINDOWS PC
Powered Off
HR WINDOWSPC
Powered Off
IT
KALI MACHINE
Powered Off
Parrot MACHINE
Powered Off
UBUNTU SERVER
Powered Off
General
Name: WINDOWS SERVER
Operating System: Windows Server 2022 (64-bit)
Groups: OPERATIONS
System
Base Memory: 1000 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: WINDOW SERVER.vdi (Normal, 15.00 GB
SATA Port 1: [Optical Drive] SERVER_EVAL_x64FRE_en
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
WINDOWS SERVER [Running] - Oracle VirtualBox
Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Group Policy Management
Disable shutdown Action
User Configuration (Enabled)
Policies
Administrative Templates
Start Menu and Taskbar
BPA results
Type here to search
Right Ctrl

Step 5.0 Policy Enforcement:

I used the command line to force immediate application of these security settings across the domain:

DOS

gpupdate */force*



🚫 Step 5: Proof of Principle (Least Privilege)

To validate the security model, I attempted to access restricted system settings using a standard user account.

- **Result:** The system successfully blocked the action with a **"Restrictions"** error: *"This operation has been cancelled due to restrictions in effect on this computer."*
- **Conclusion:** This confirms that the PoLP is successfully preventing unauthorized configuration changes by domain users.