

Active Directory Implementation

Phour Global Limited

Windows Server Domain Controller Setup

Ibrahim Ayomide Fayomi

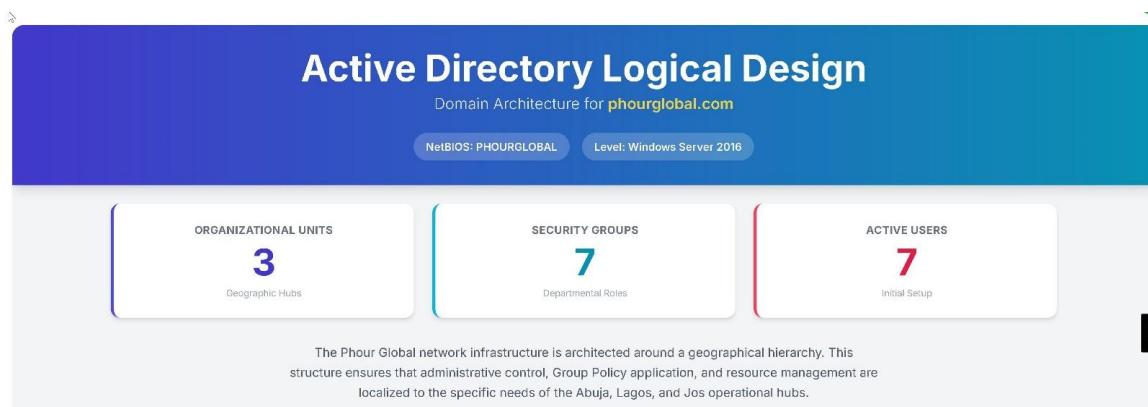
2026

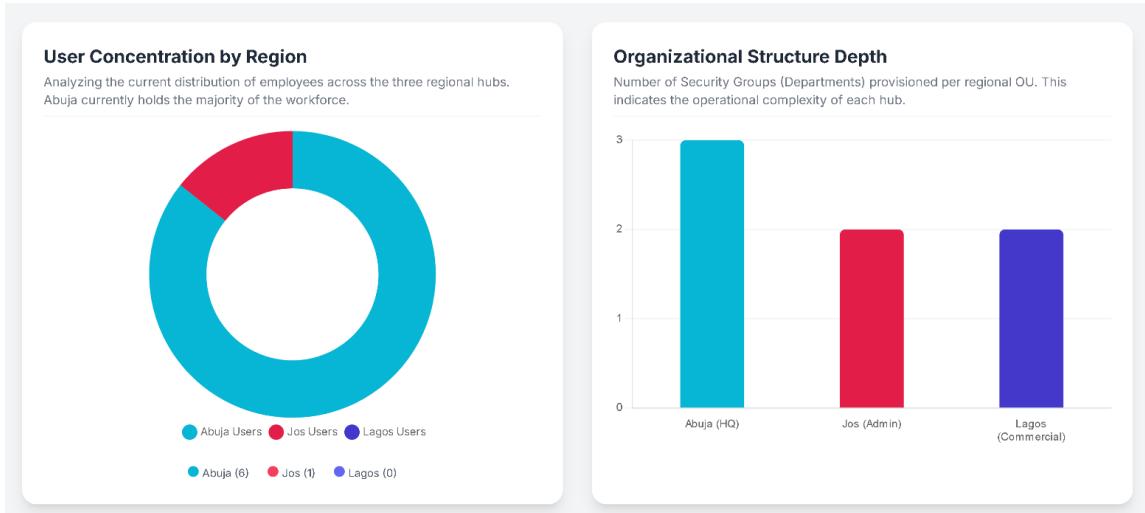
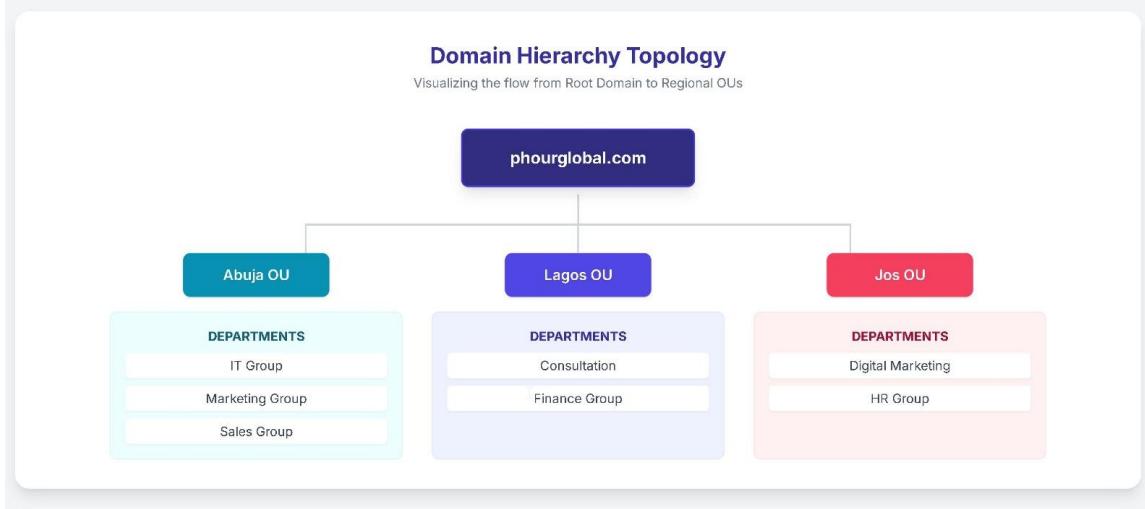
Project Overview

This project demonstrates the implementation of Active Directory Domain Services for Phour Global Limited, a cybersecurity services firm. The infrastructure includes a Windows Server 2012 domain controller managing user accounts, computers, and security policies across three office locations.

Network Infrastructure

The network consists of one Windows Server 2012 domain controller and two Windows 8 client machines connected through a switch. The domain controller handles authentication, DNS resolution, and group policy management for all domain members.





Detailed User Directory

A comprehensive breakdown of specific user assignments within the AD structure.

Abuja

IT Group

Akeem Ahmed
akeem_it@phourglobal.com

Mutiat Fayomi
mutiat_it@phourglobal.com

Marketing Group

Cara Ibrahim
cara_marketing@phourglobal.com

Samson Solanke
samson_marketing@phourglobal.com

Jos

HR Group

Ibrahim Fayomi
ibrahim_hr@phourglobal.com

Digital Marketing

No users currently provisioned.

Lagos

Consultation Group

No users currently provisioned.

Finance Group

No users currently provisioned.

Sales Group

2 Users

Hope Solanke

hope_sales@phourglobal.com

Rashidat Oyesile

rashidat_sales@phourglobal.com

Implementation Specifications

Naming Convention

Format: `first_department`
Example: `ibrahim_hr`
UPN Suffix: `@phourglobal.com`

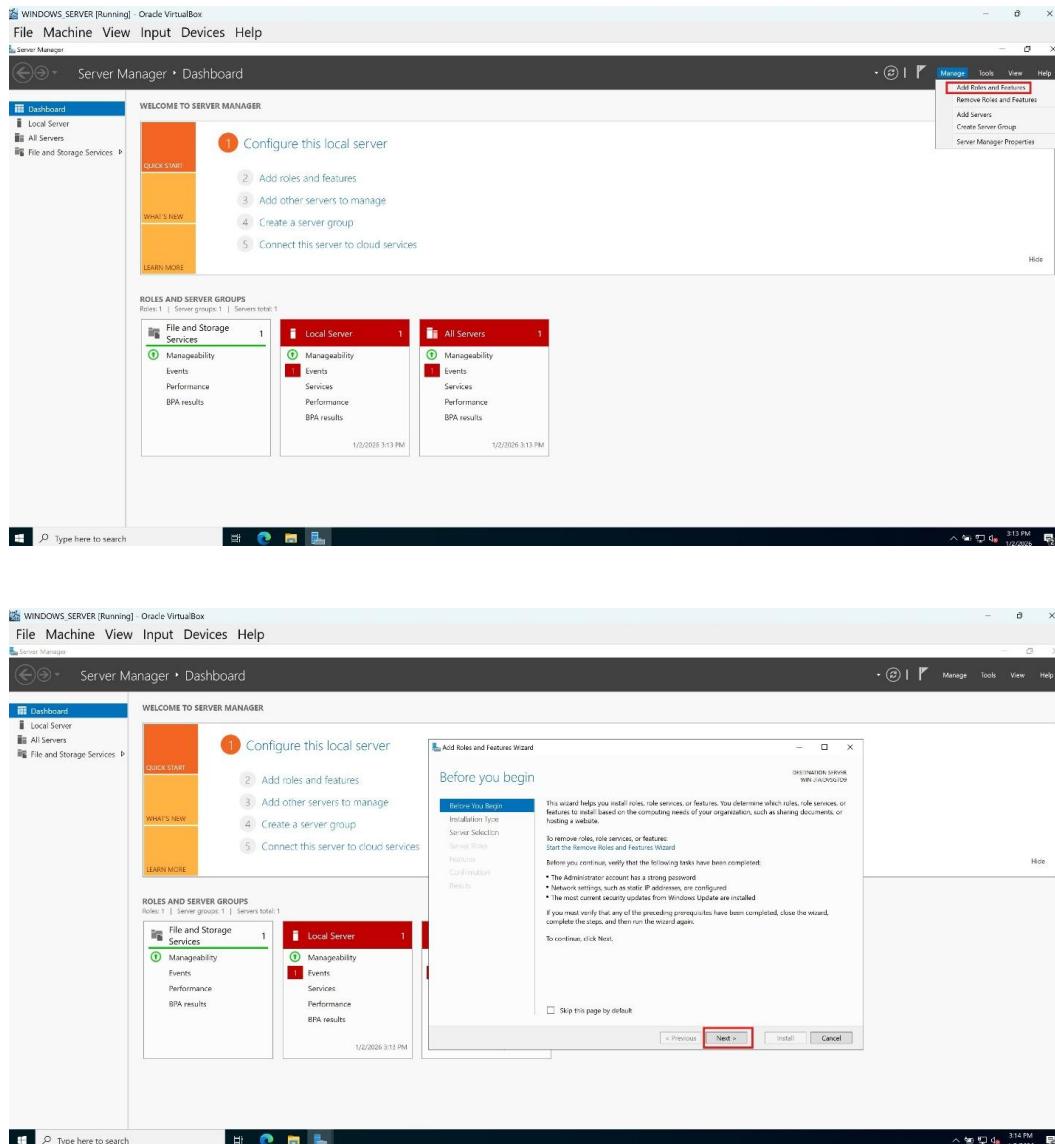
Delegation & Security

- Groups are configured as **Global Security Groups**.
- Consider delegating "*Password Reset*" rights to the Abuja IT Group for domain-wide support.

Phase 1: Domain Controller Setup

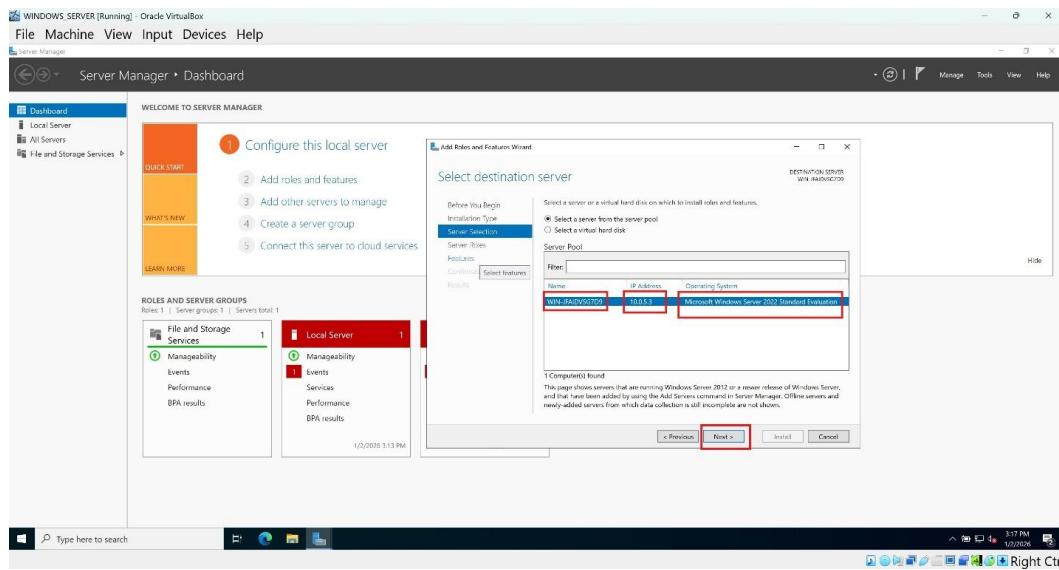
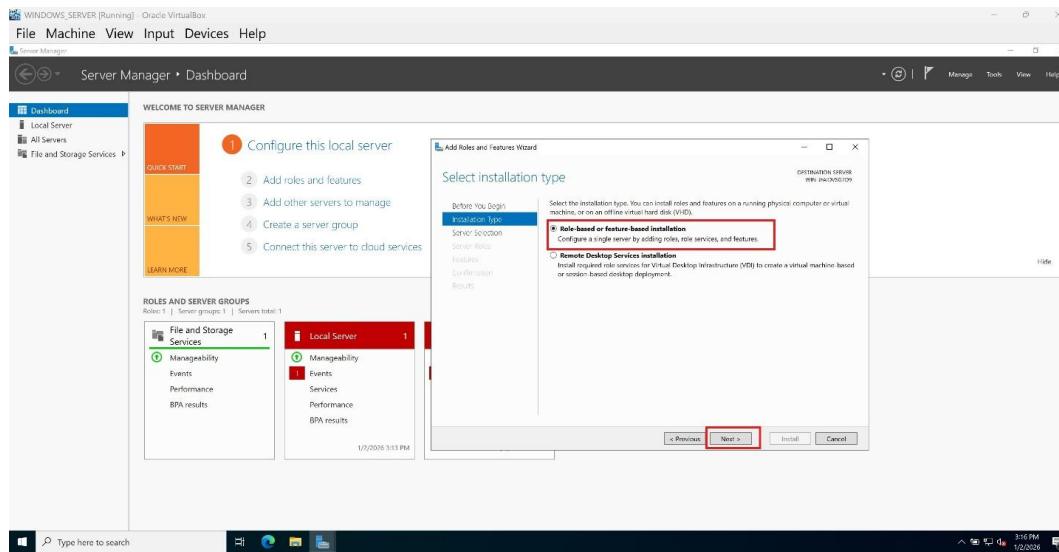
1. Adding Roles and Features

Begin by opening Server Manager, then select Add Roles and Features. This launches the wizard that will guide you through installing Active Directory Domain Services.



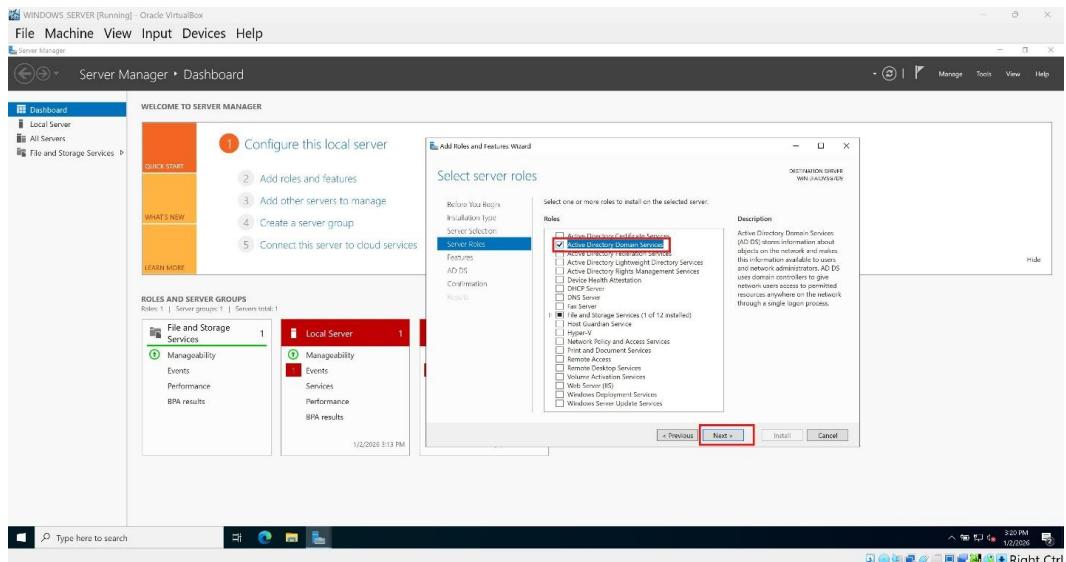
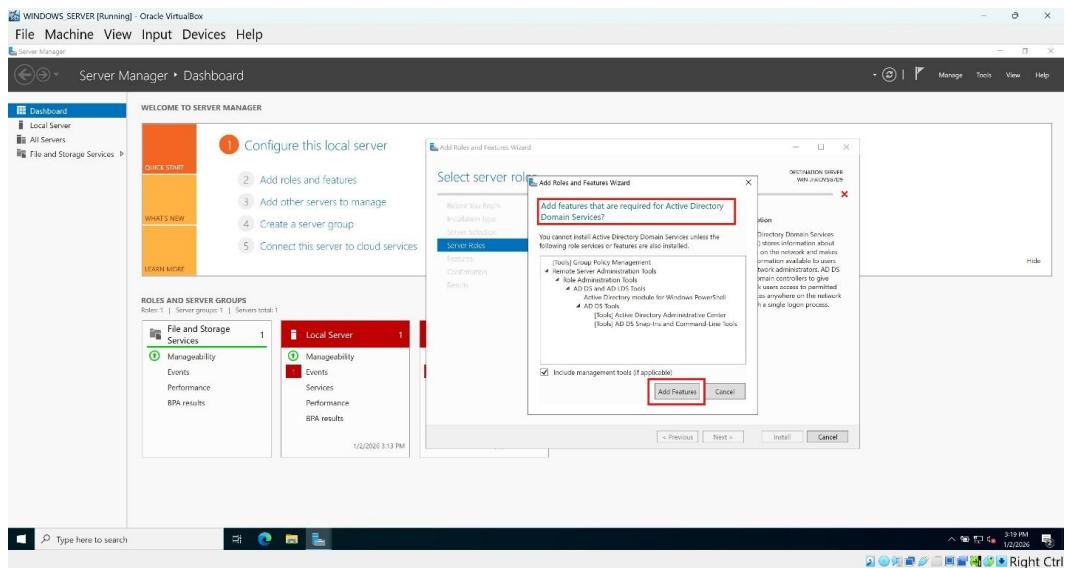
2. Role-Based Installation

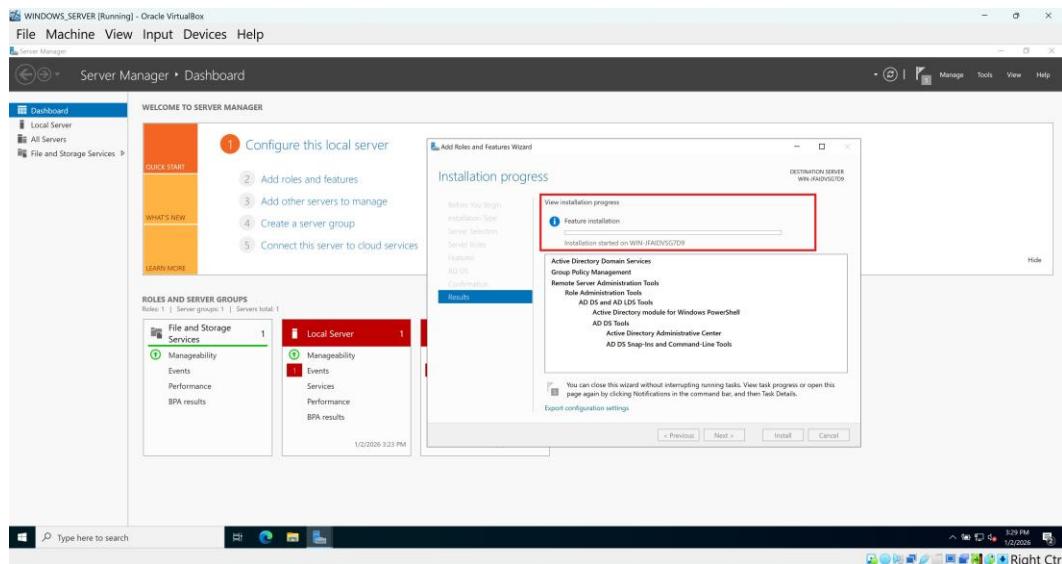
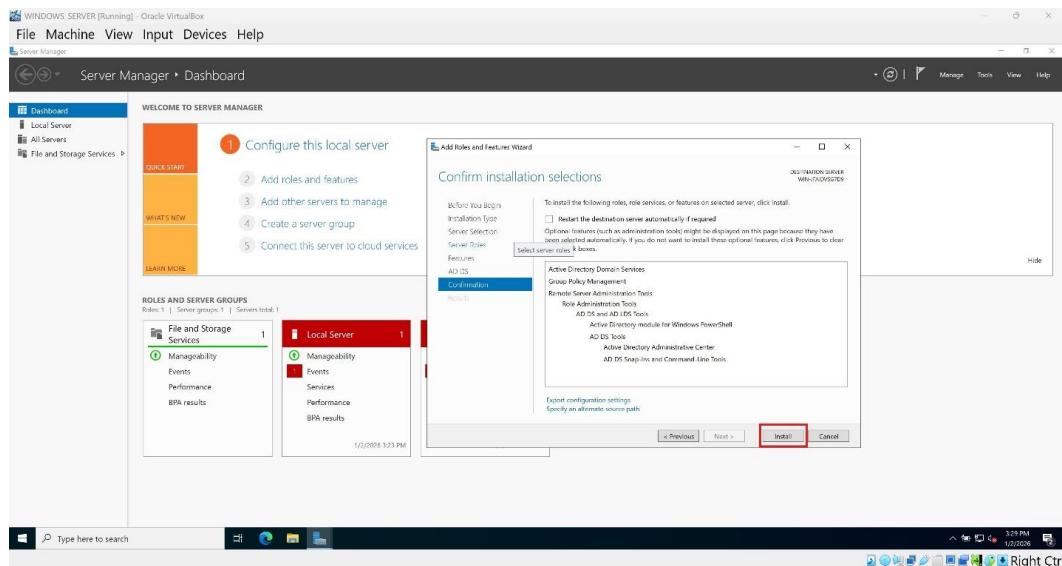
Choose Role-based or feature-based installation and select the local server from the server pool.

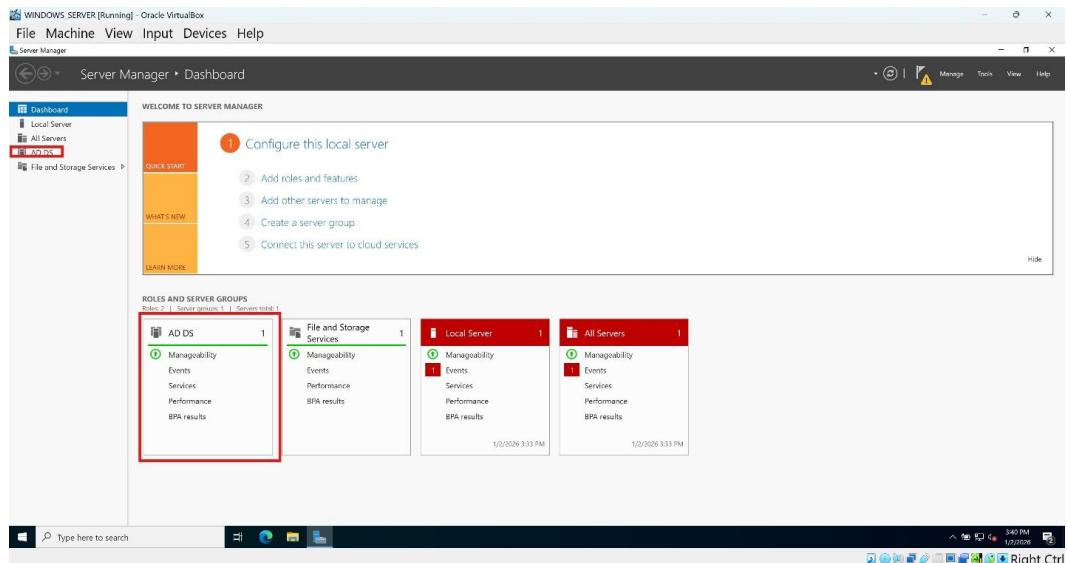
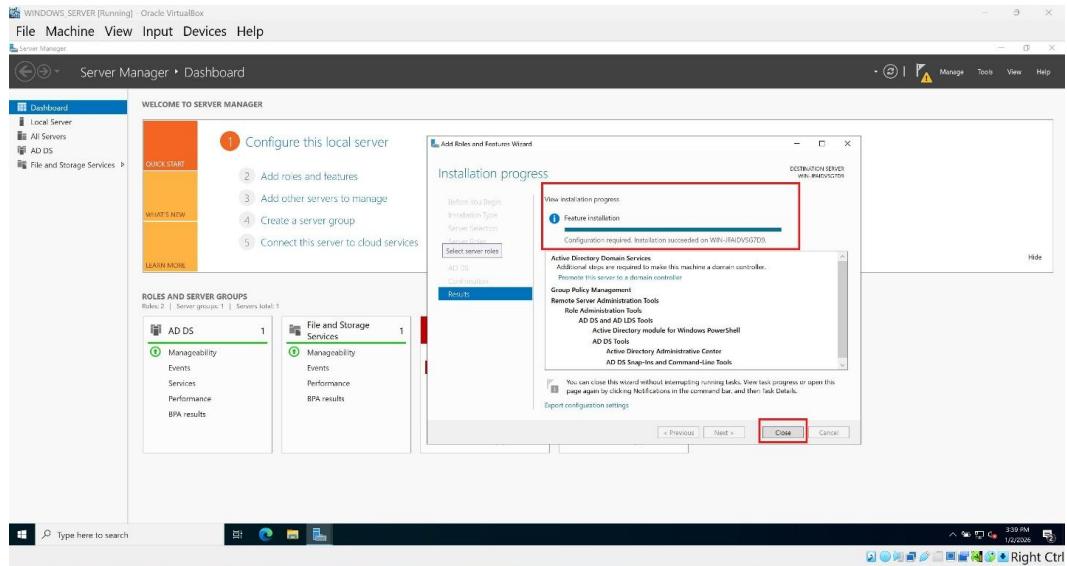


3. Installing Active Directory Domain Services

Select Active Directory Domain Services from the server roles list. The wizard will automatically include the required management tools.

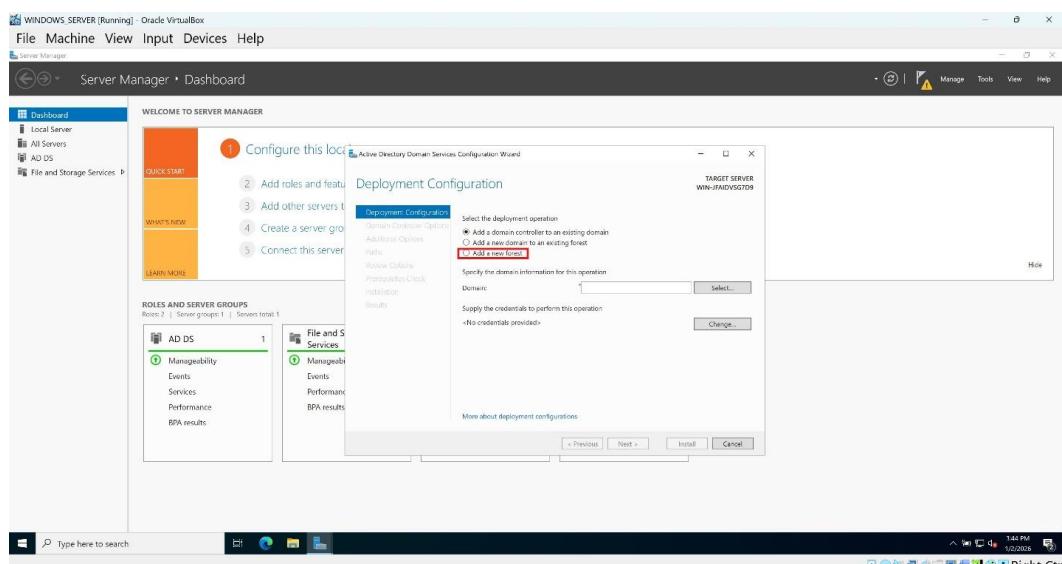
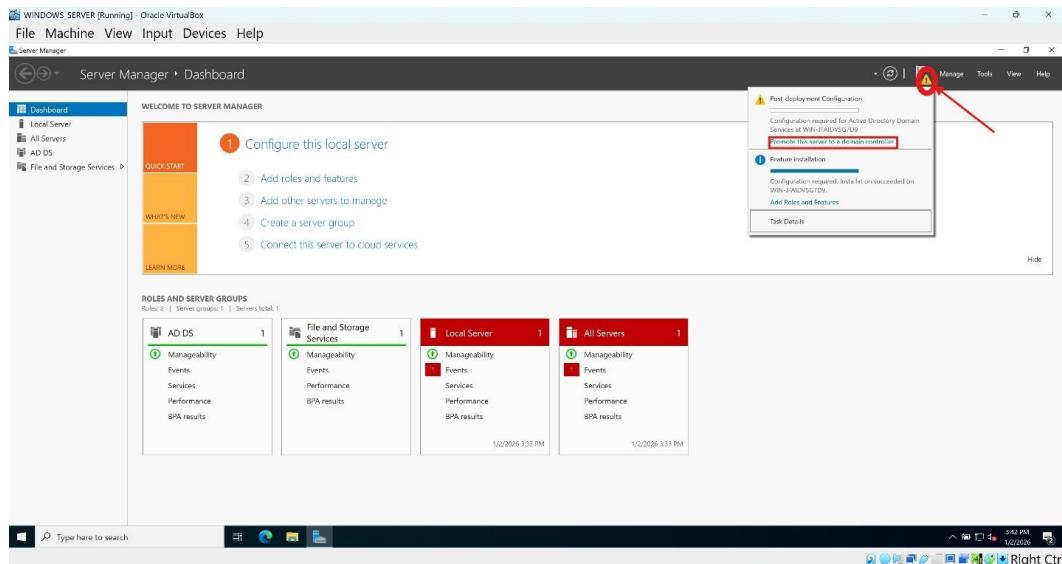






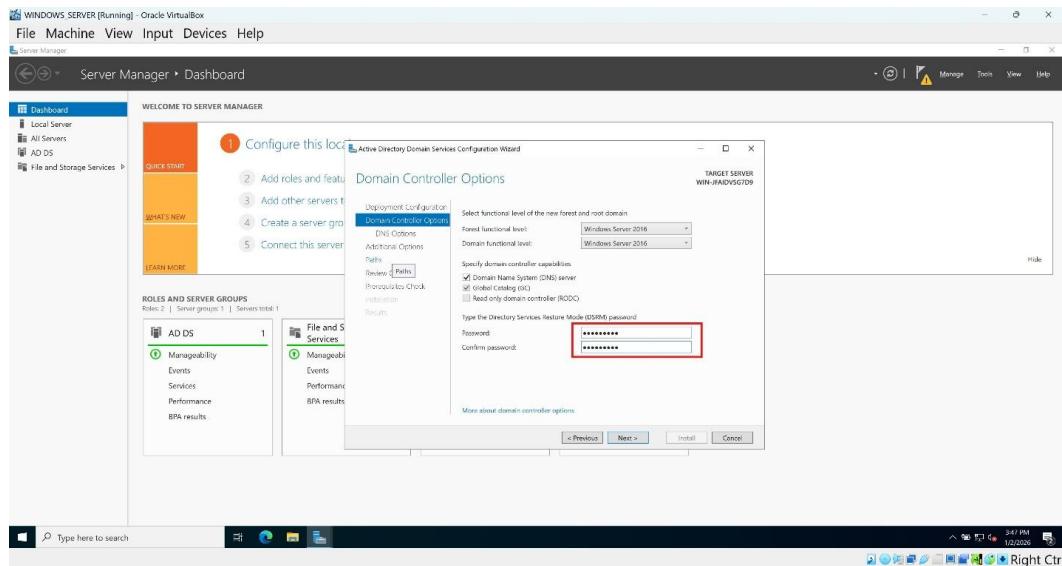
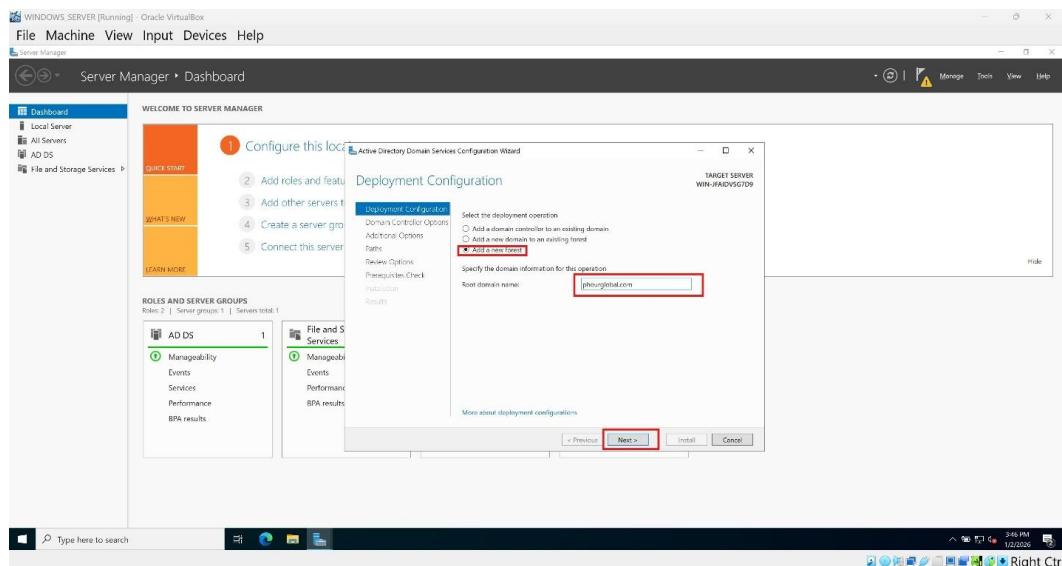
4. Promoting Server to Domain Controller

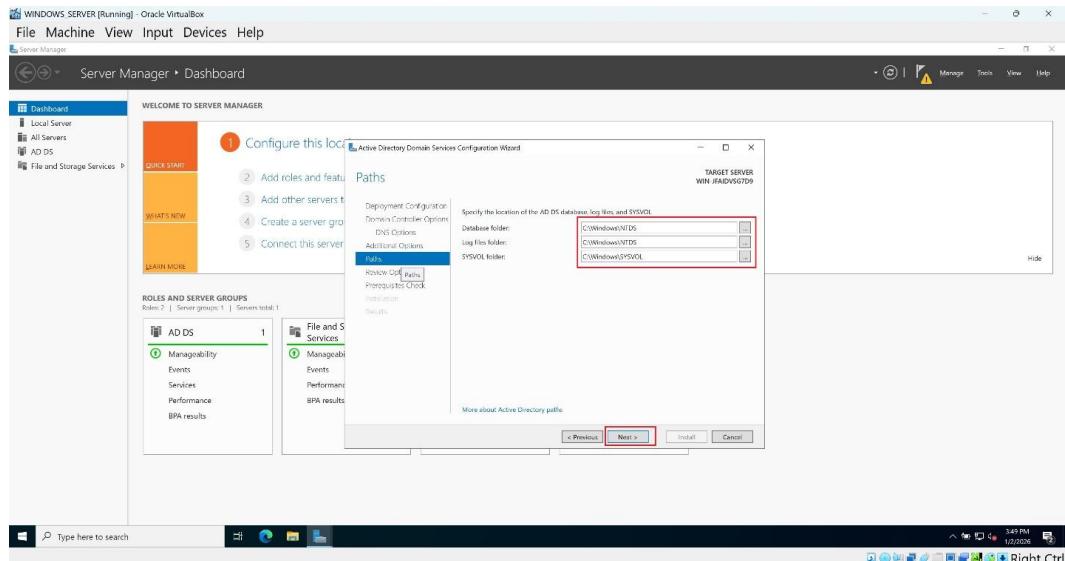
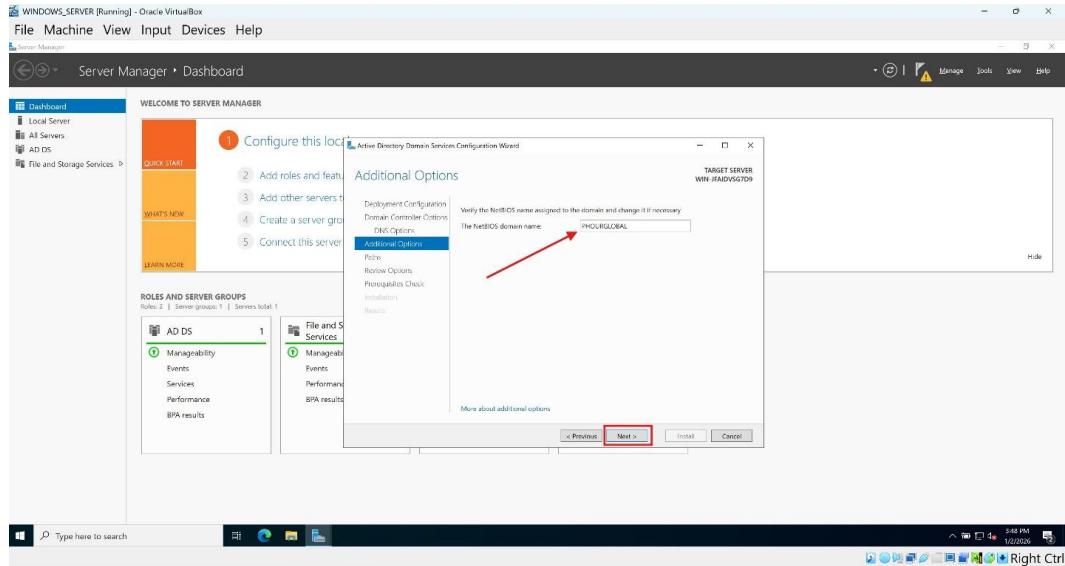
After the AD DS installation completes, click the notification flag in Server Manager and select "Promote this server to a domain controller". This begins the domain controller configuration wizard.



5. Creating New Forest and Domain

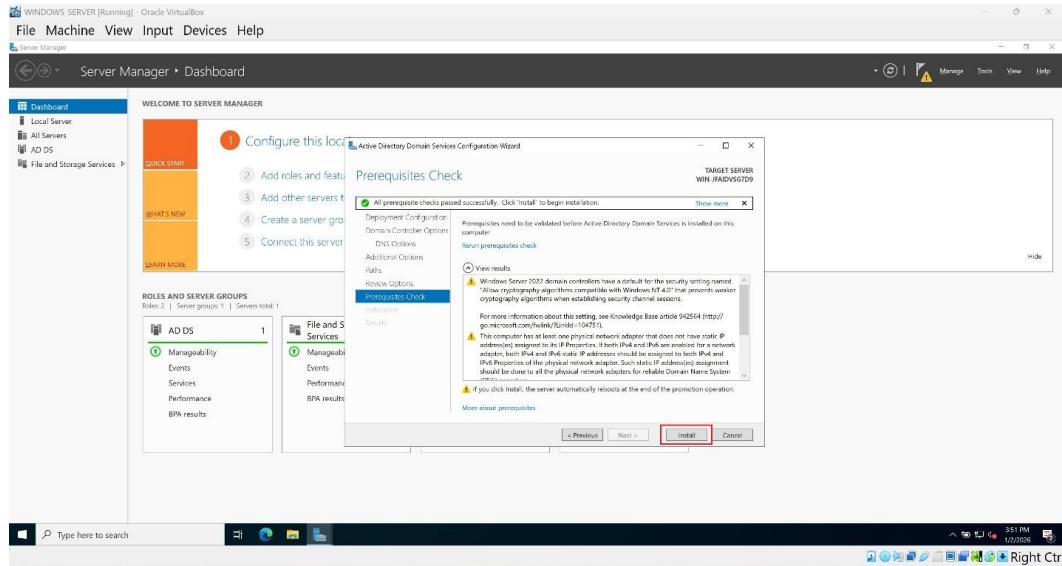
Select "Add a new forest" and enter the root domain name phourglobal.com. Set a strong password for Directory Services Restore Mode.





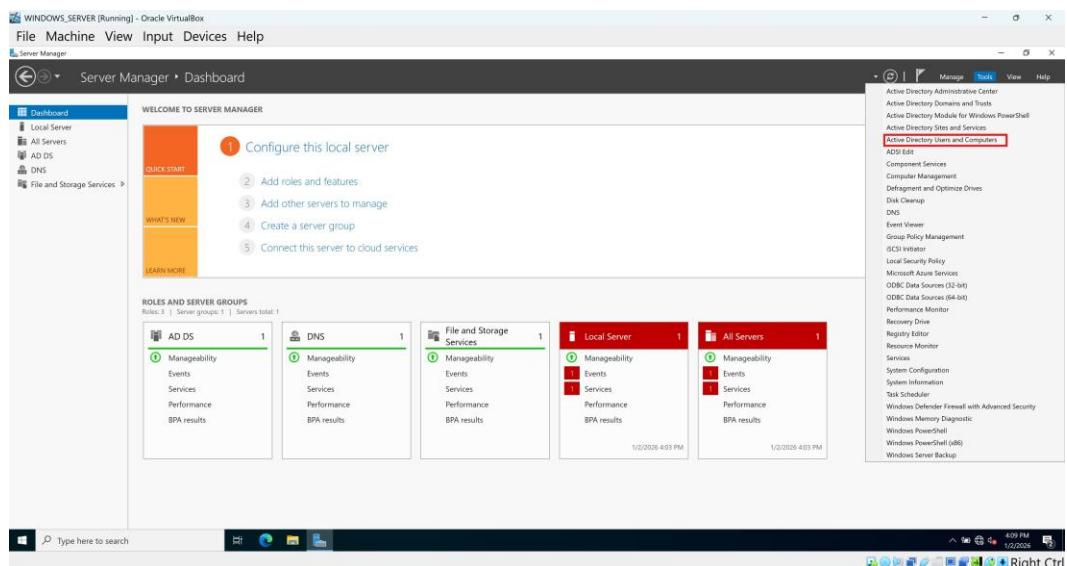
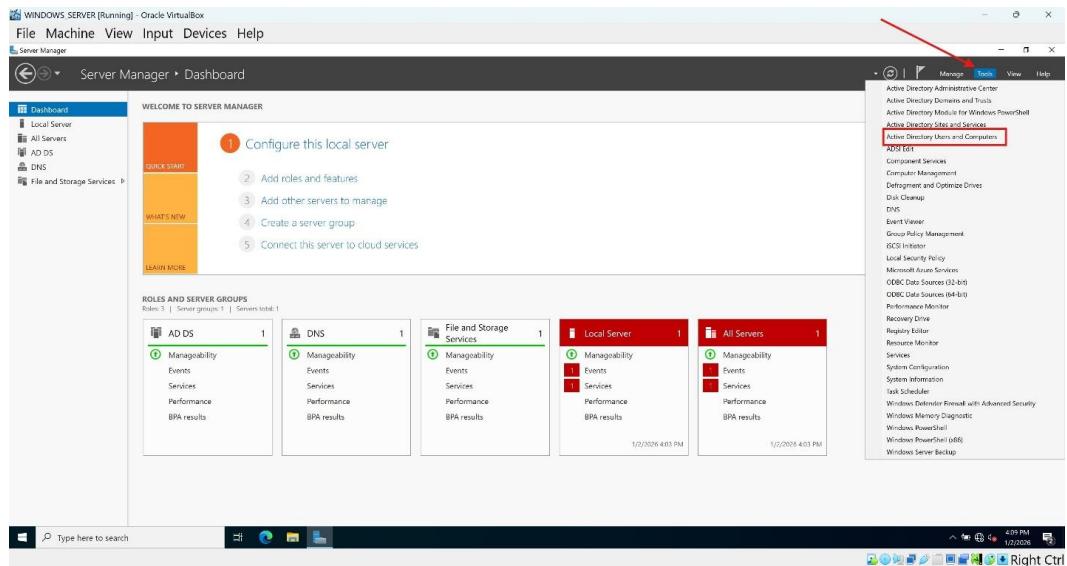
6. Prerequisites Check and Installation

The wizard verifies all prerequisites before installation. Once all checks pass, proceed with the installation. The server will automatically restart after completion.



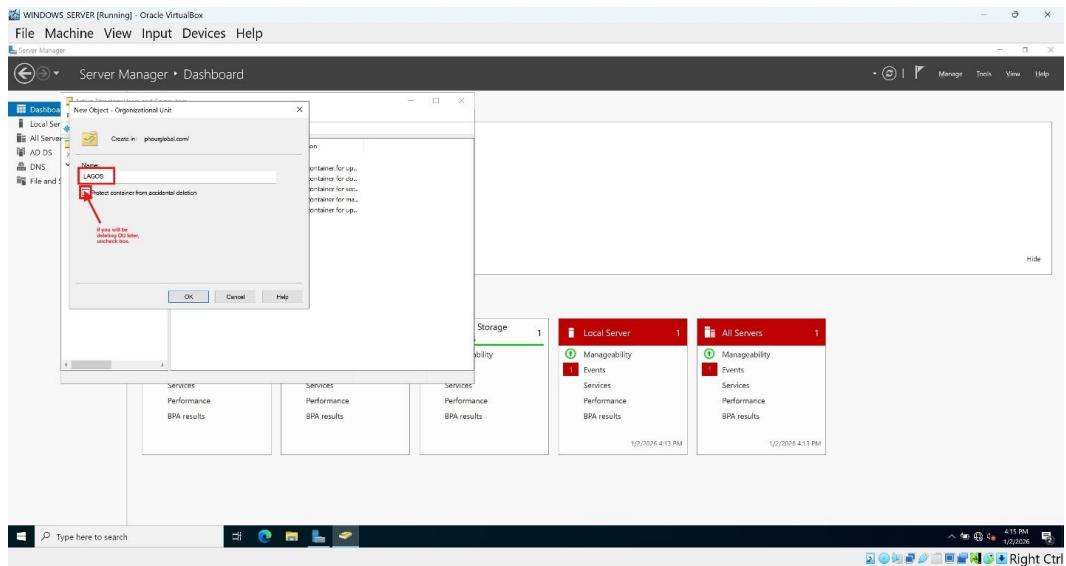
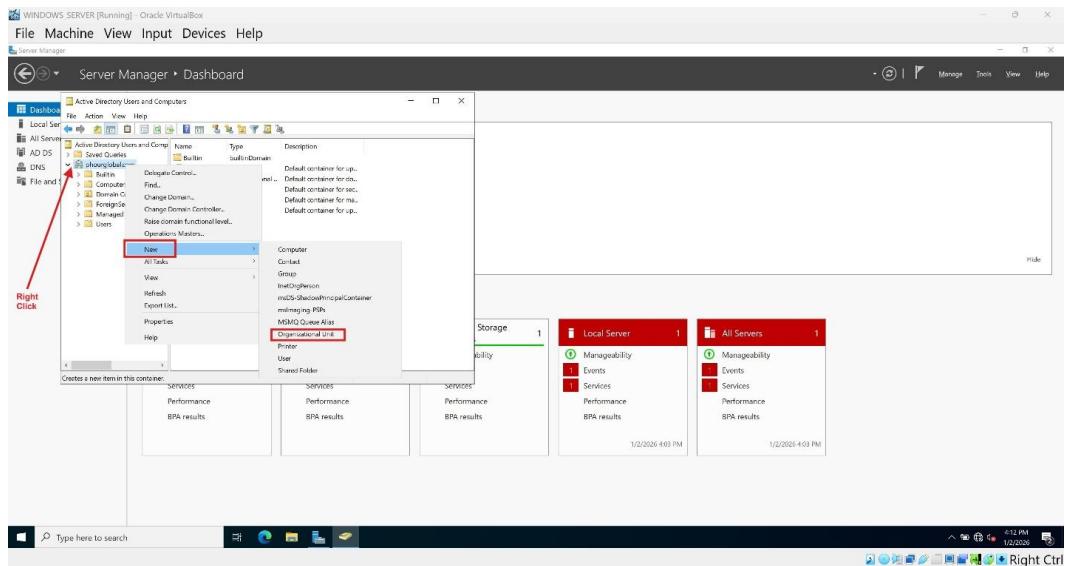
Phase 2: Creating Organizational Units

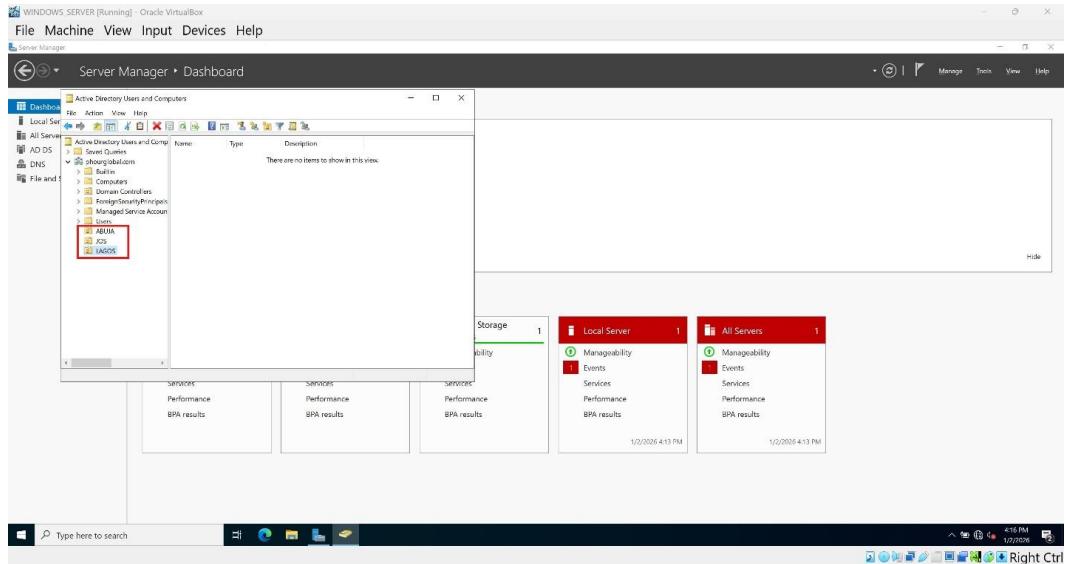
After logging back in as the domain administrator, open Active Directory Users and Computers from Server Manager tools. Organizational Units provide a way to organize users, groups, and computers by department or location.



1. Creating Location-Based OUs

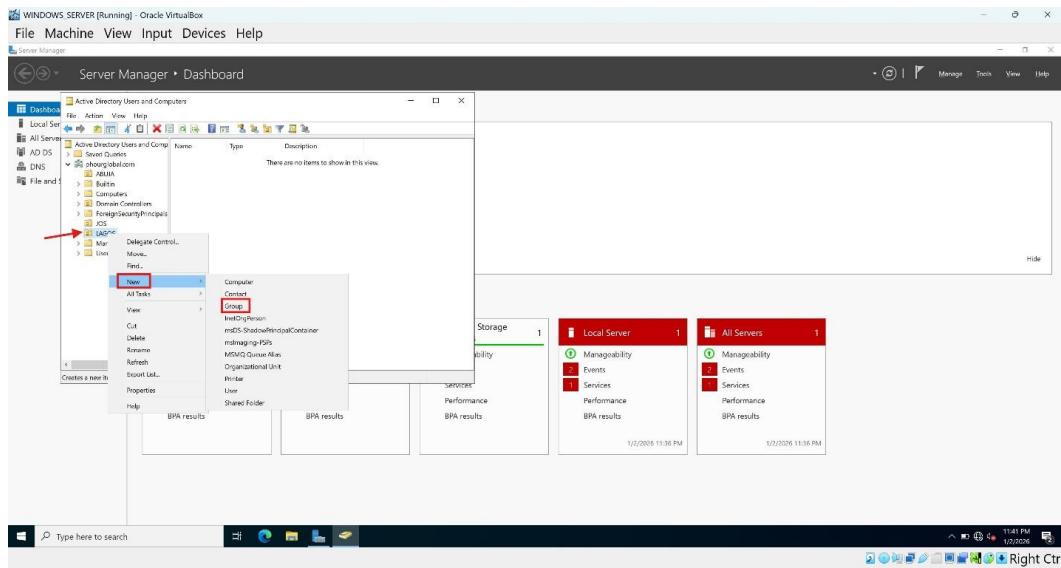
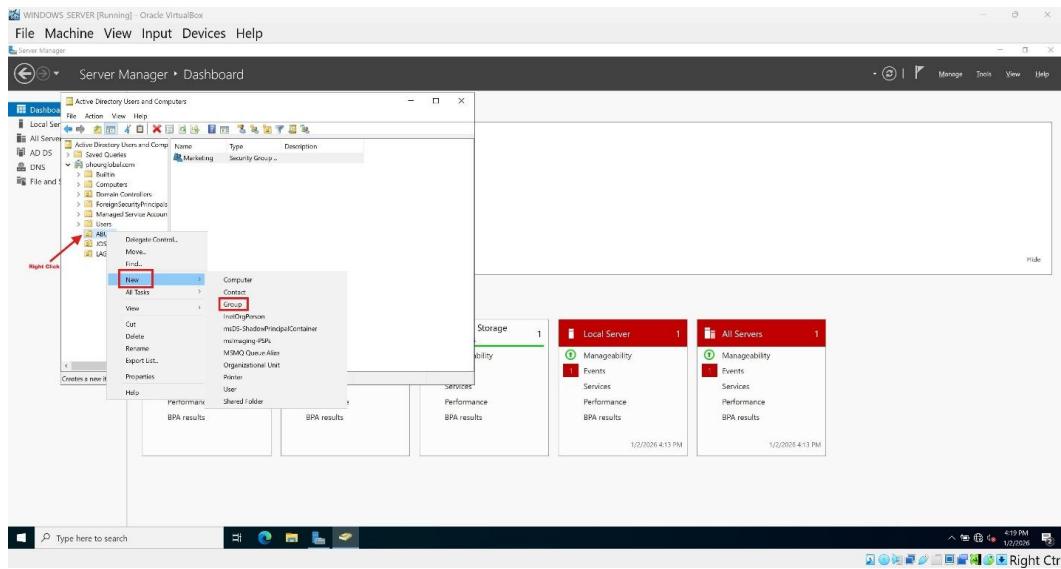
Right-click the domain name and select New, then Organizational Unit. Create three OUs representing the company locations: ABUJA, JOS, and LAGOS.

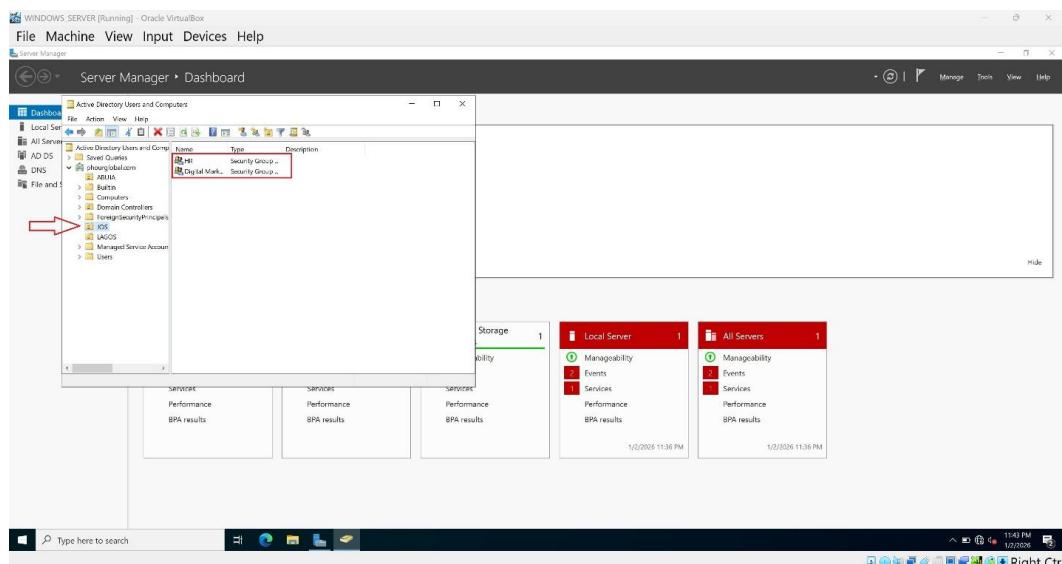
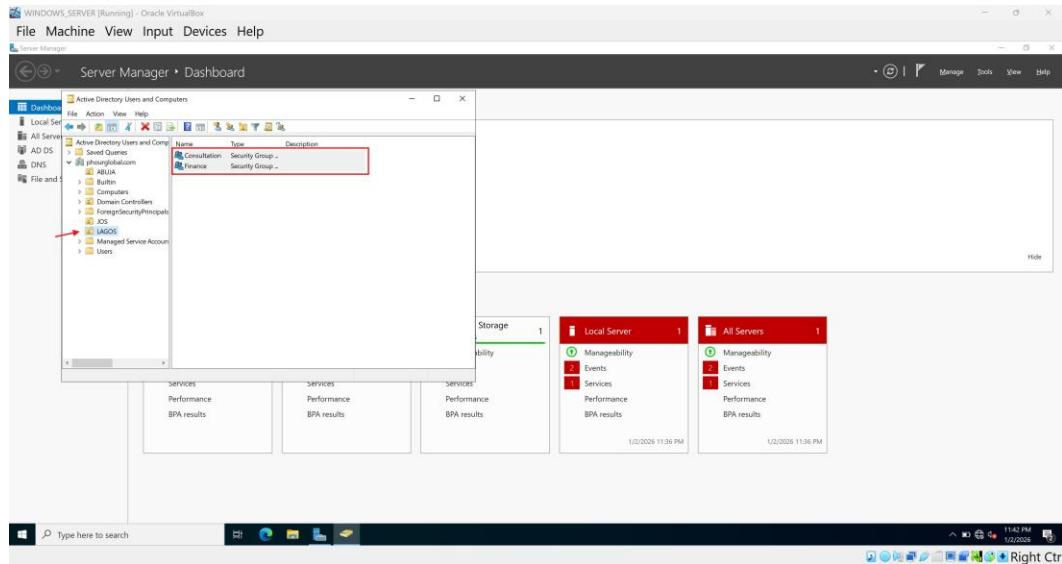


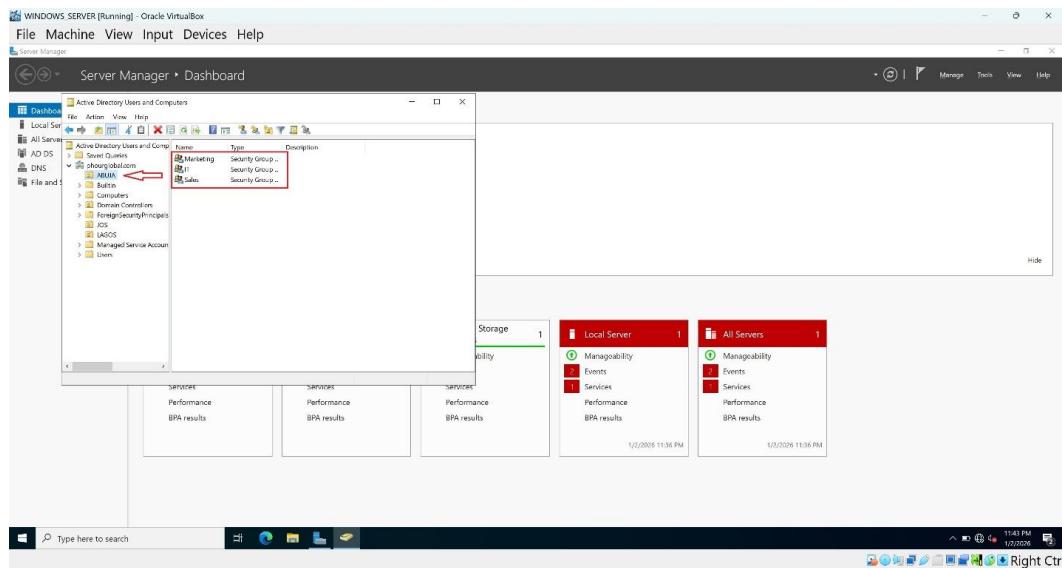


2. Creating Department Groups

Within each OU, create security groups for different departments. Right-click the OU, select New, then Group. Set the group type to Security and scope to Global.

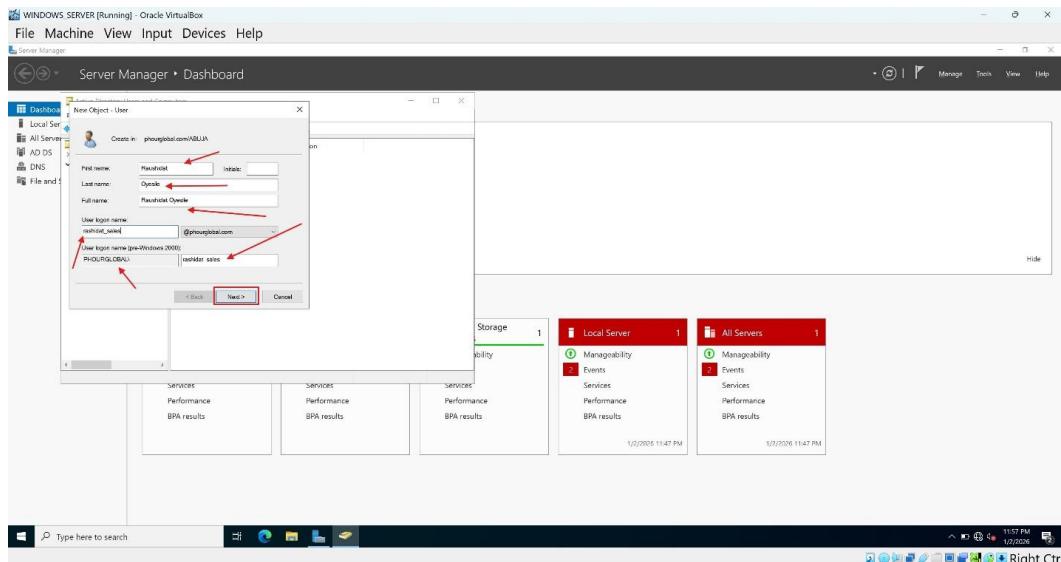
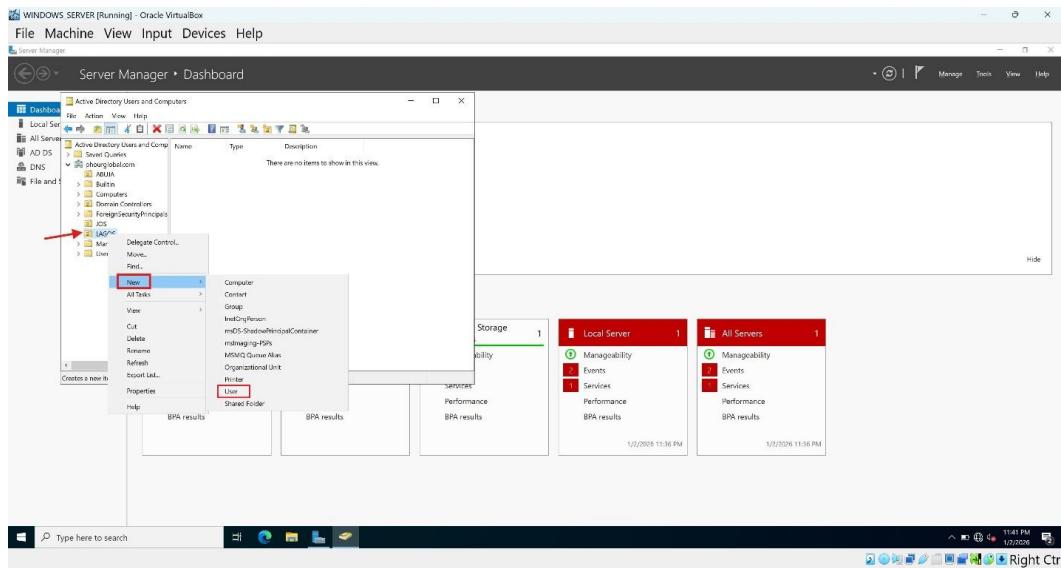


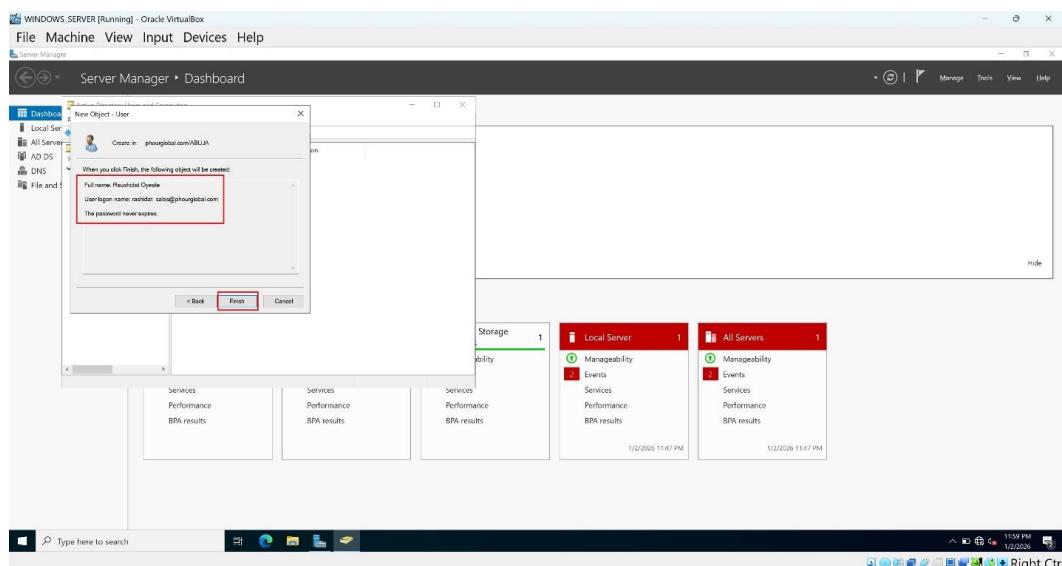
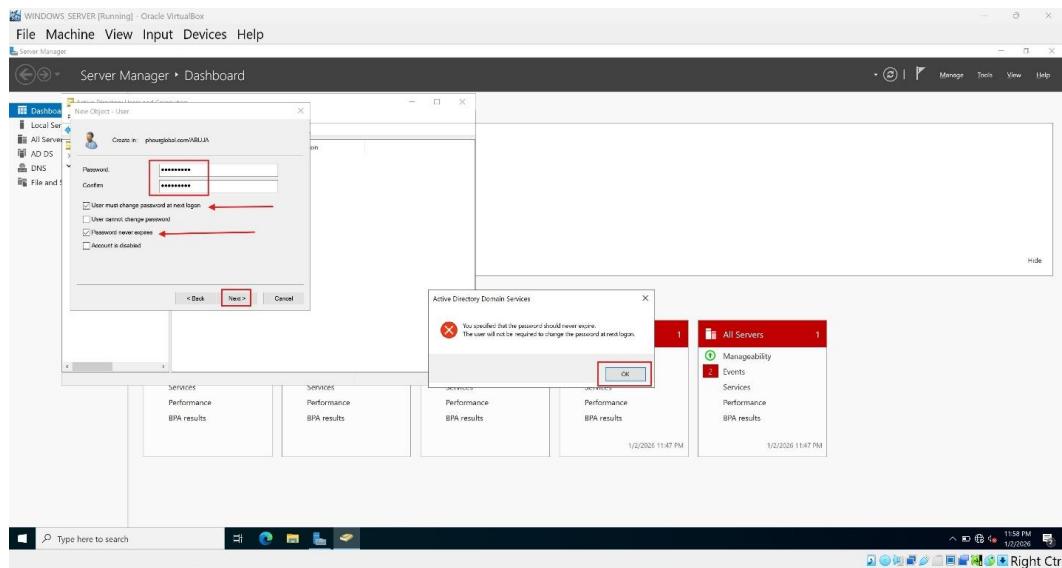


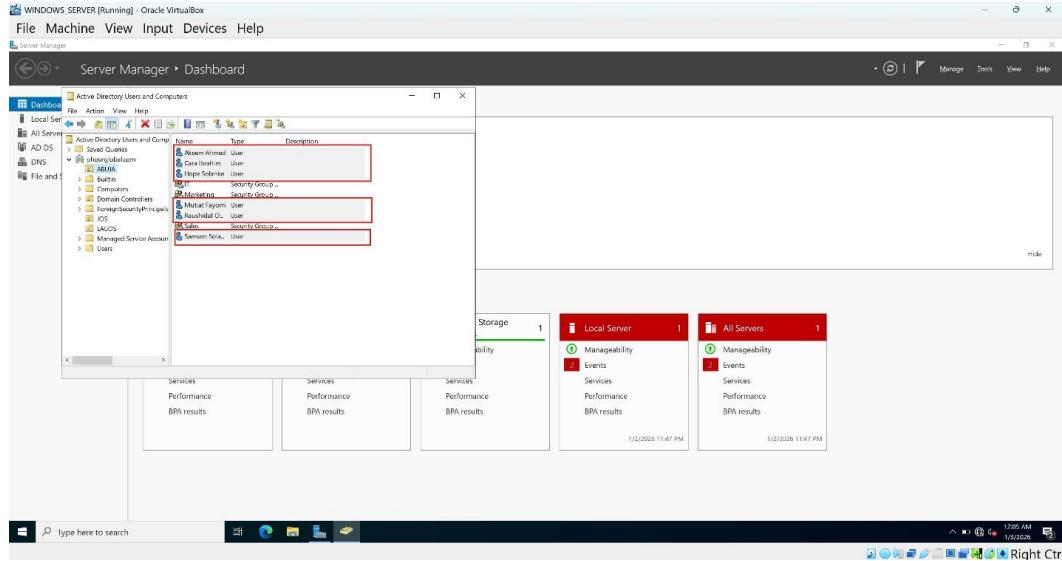


Phase 3: Creating User Accounts

User accounts are created within the appropriate department groups. Each user is assigned a unique username following the format `firstname_department` and added as a member of their department security group.

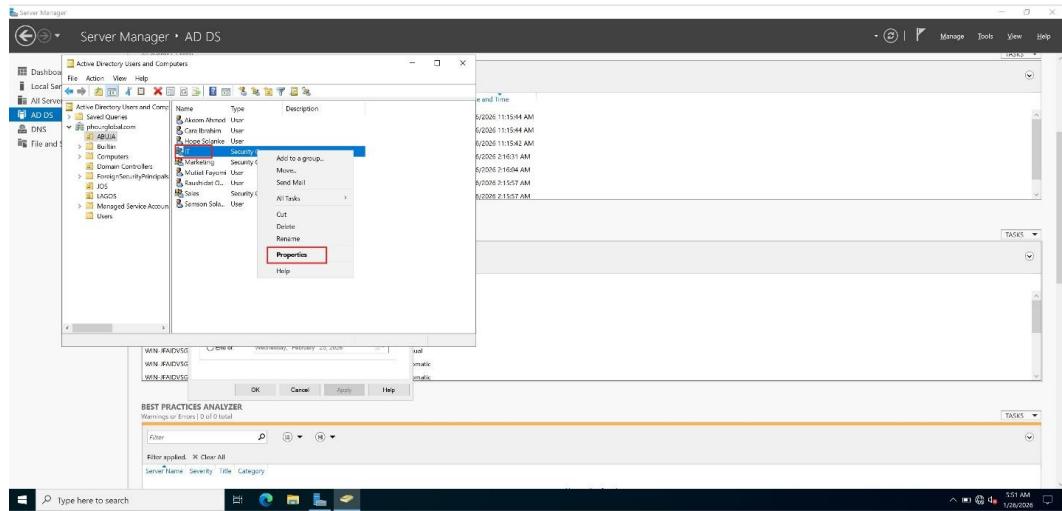


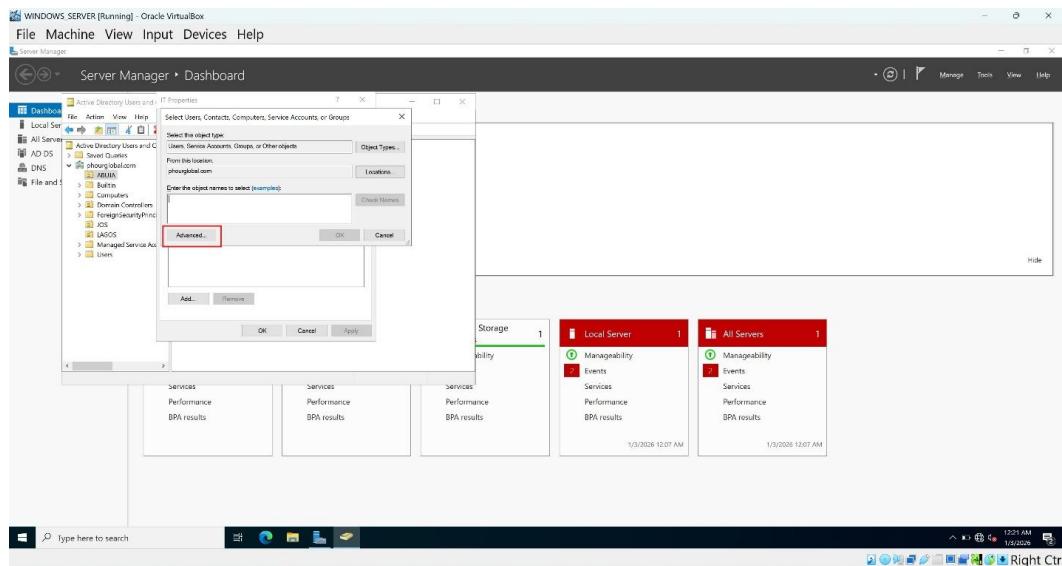
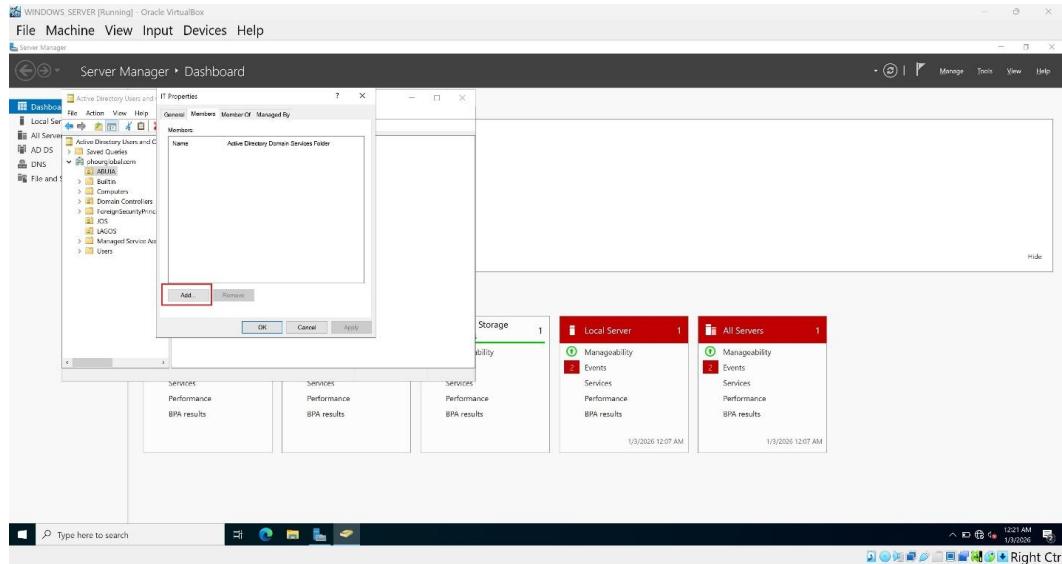


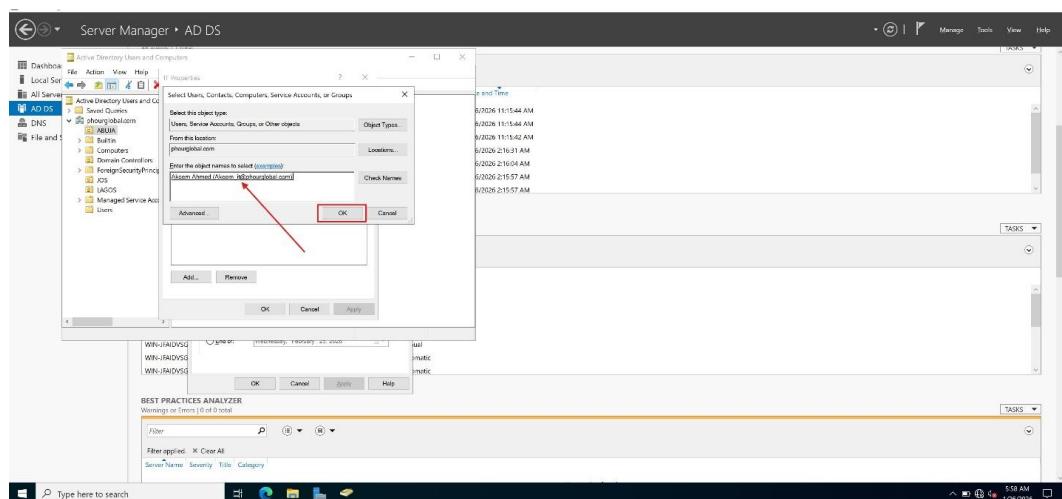
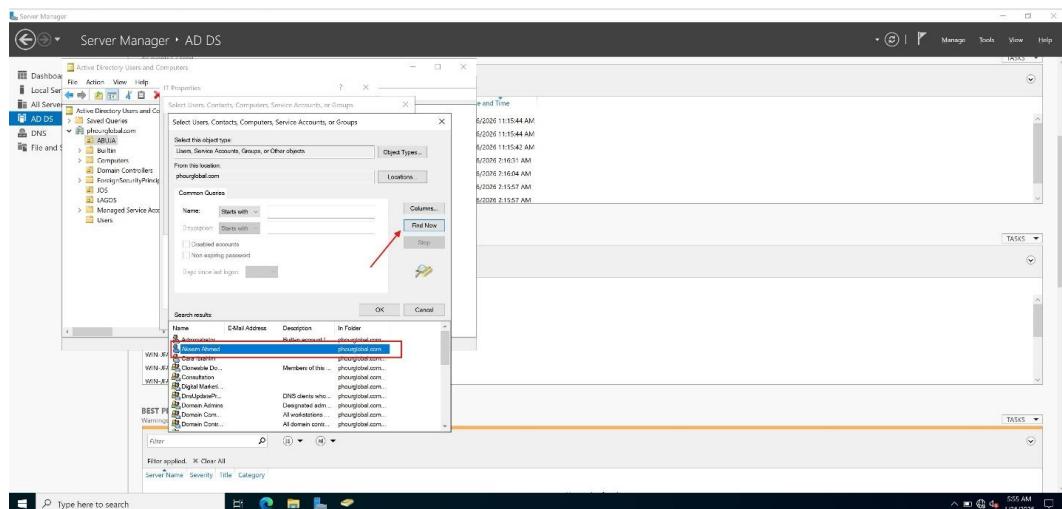
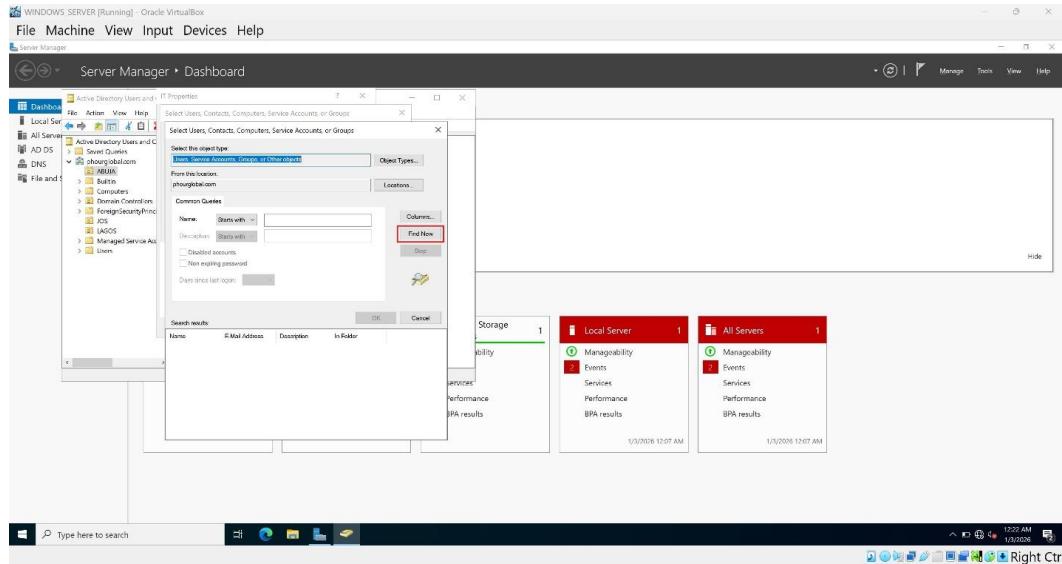


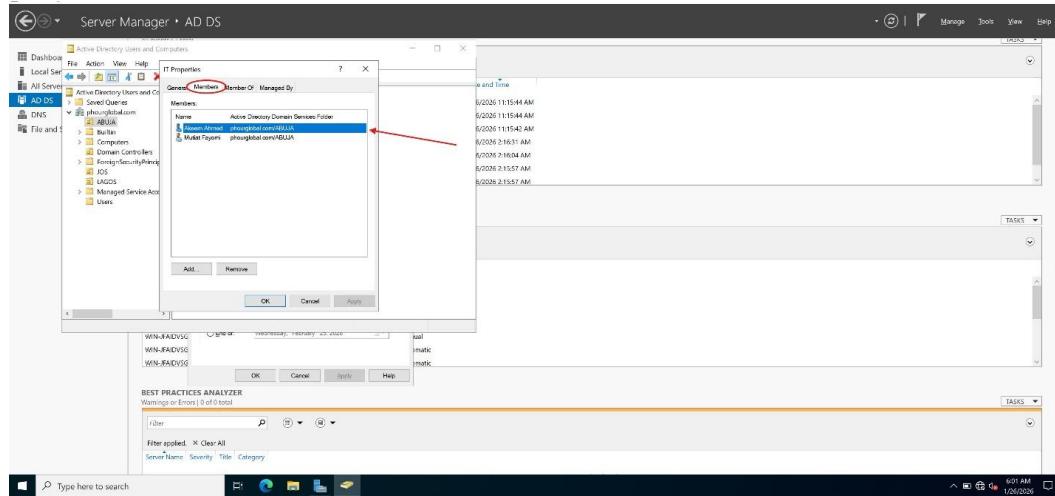
Adding Users to Groups

After creating users, add them to their respective security groups. Open the group properties, go to the Members tab, and add the appropriate users.



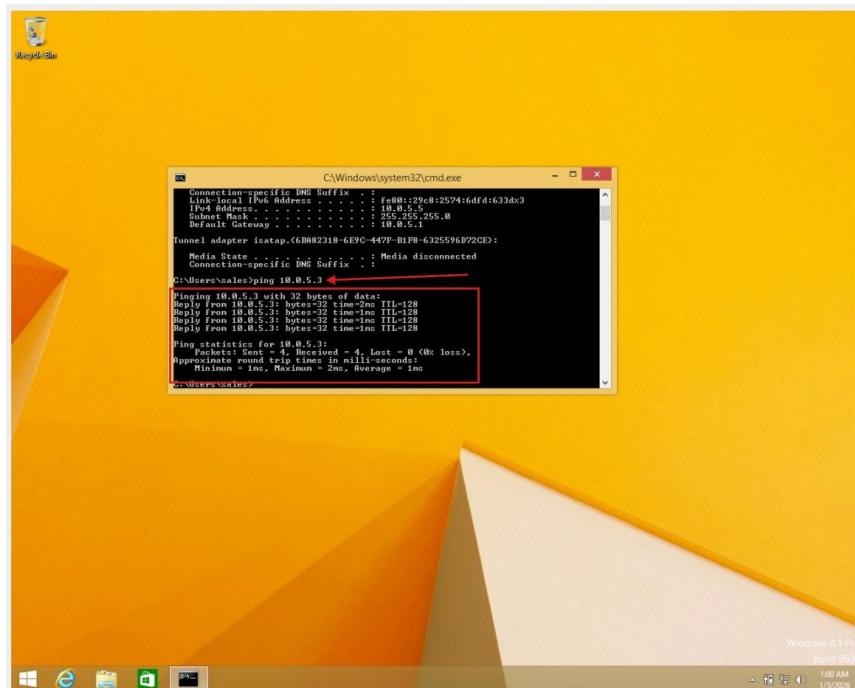
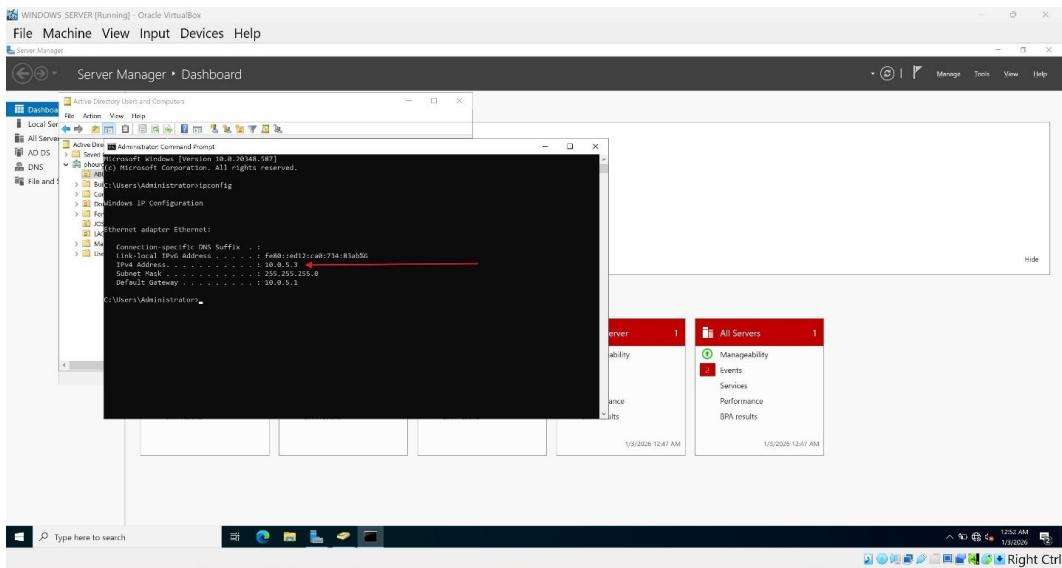


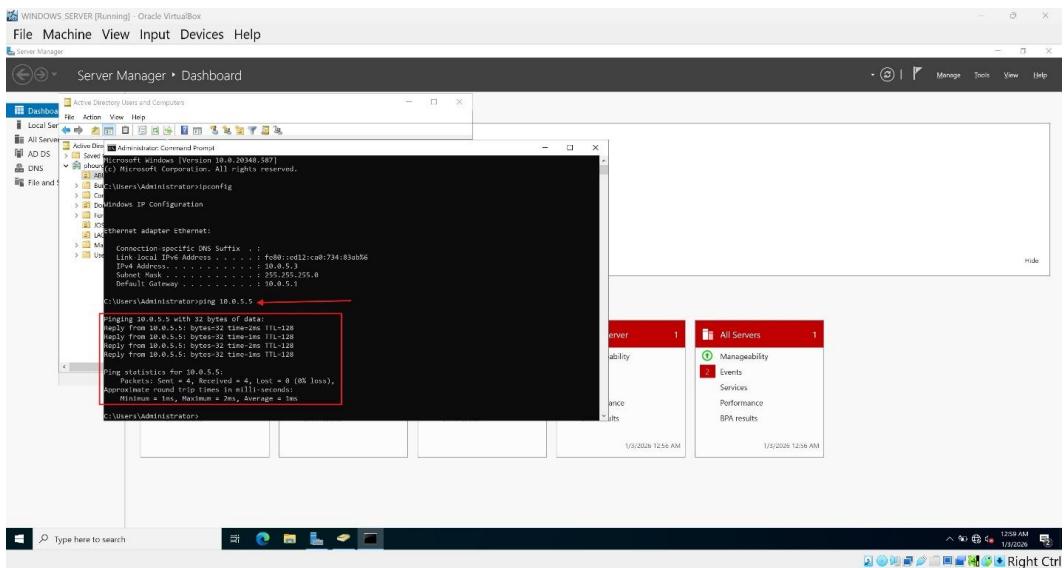




Phase 4: Client Network Configuration

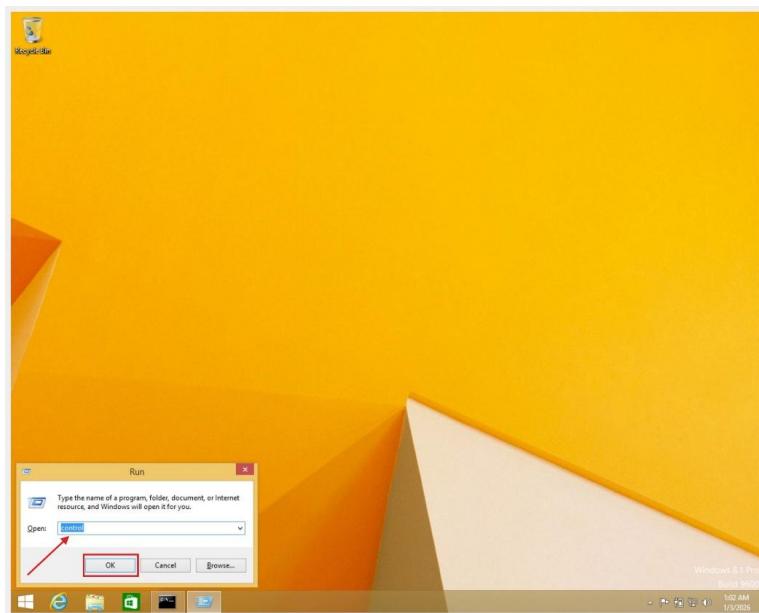
Before joining client computers to the domain, configure their network settings to use the domain controller as the DNS server. This allows the clients to resolve the domain name and locate domain resources.

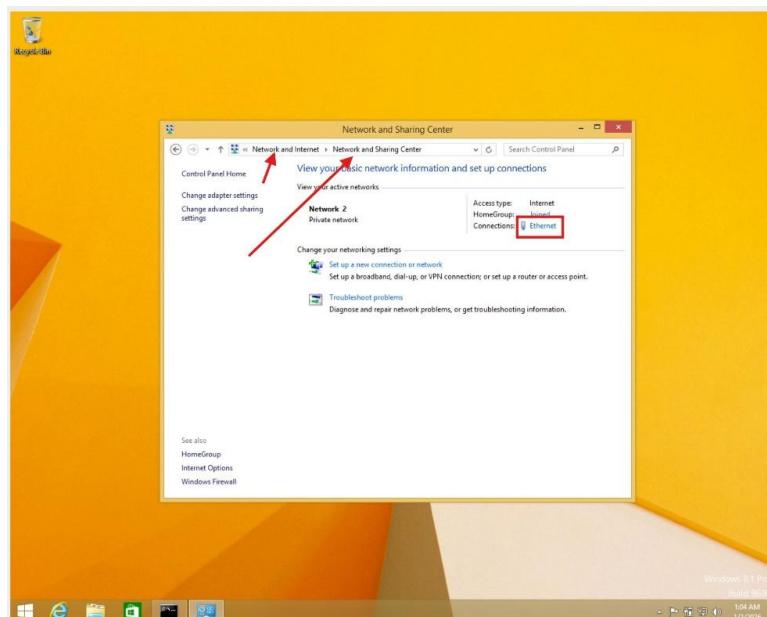
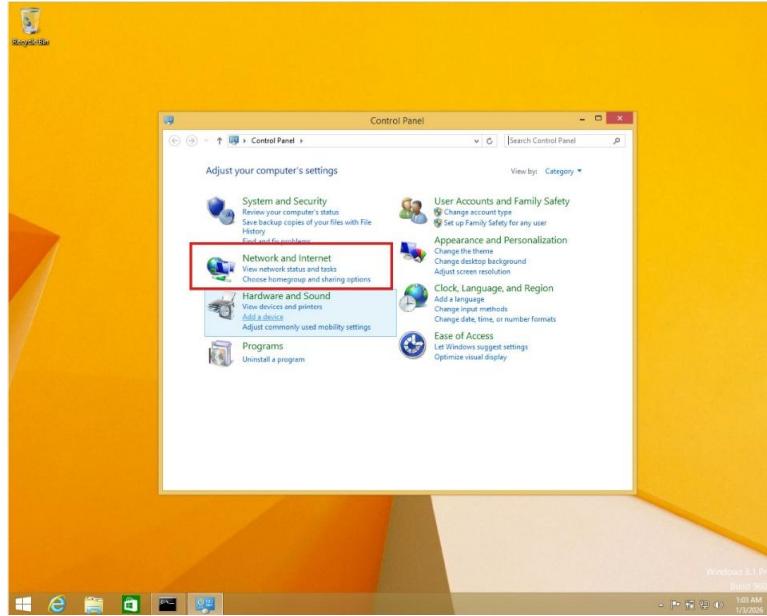


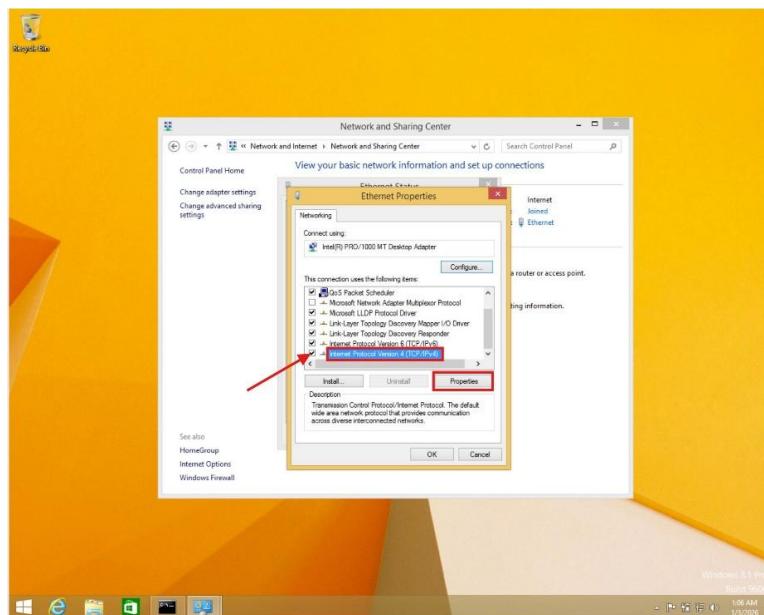
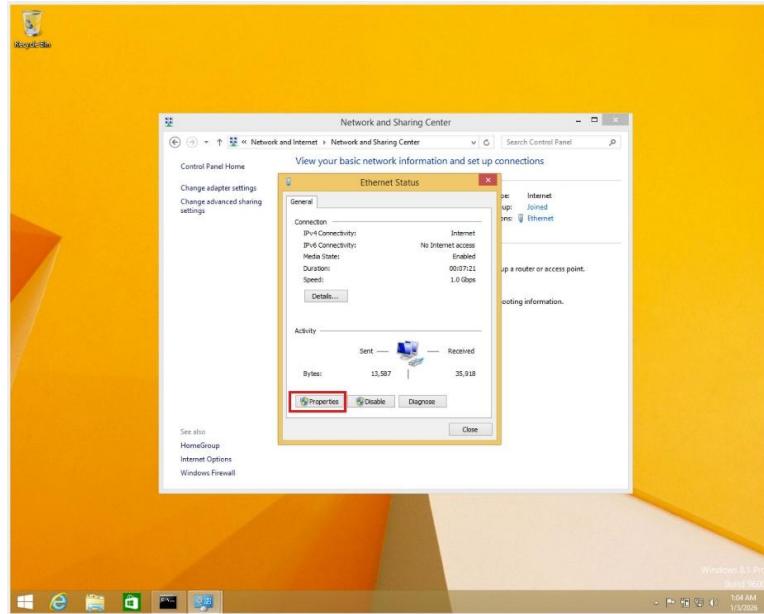


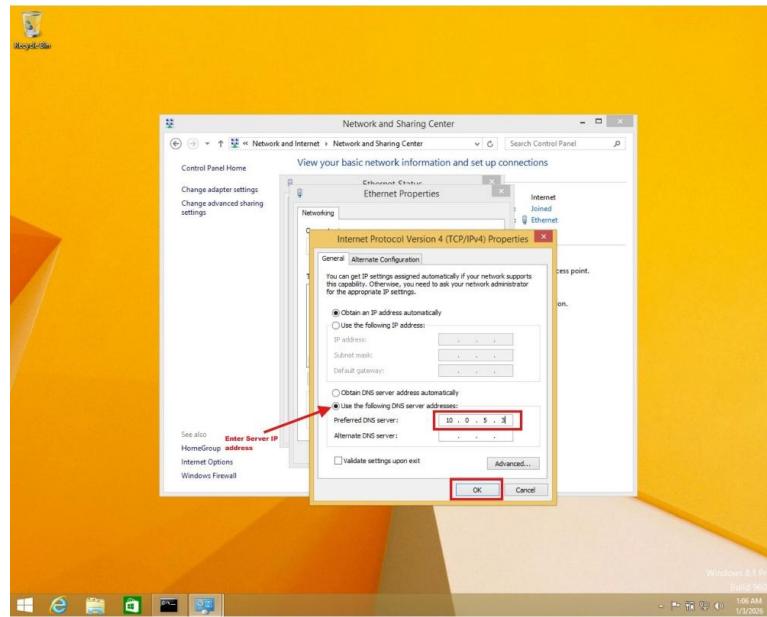
Network Adapter Configuration

Open Network and Sharing Center, click on the active connection, select Properties, then configure IPv4 settings. Set the preferred DNS server to 10.0.5.3 (the domain controller IP address).



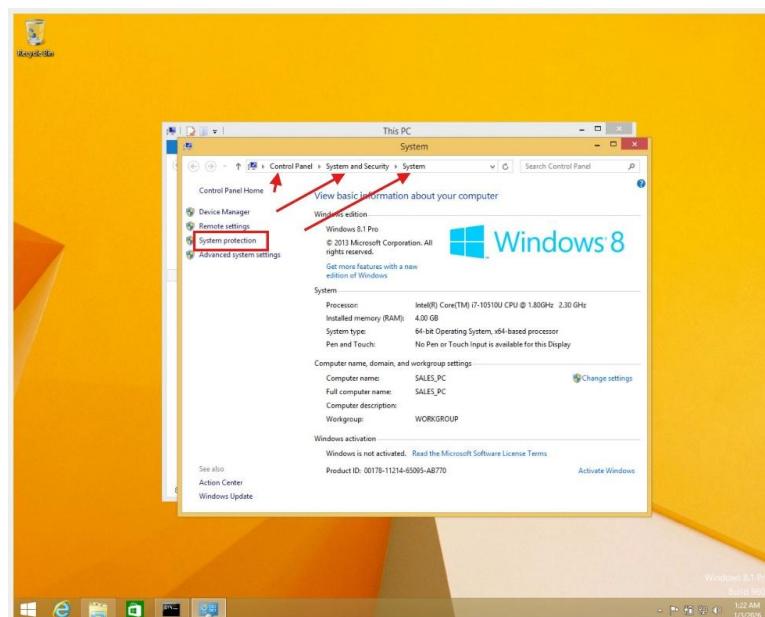
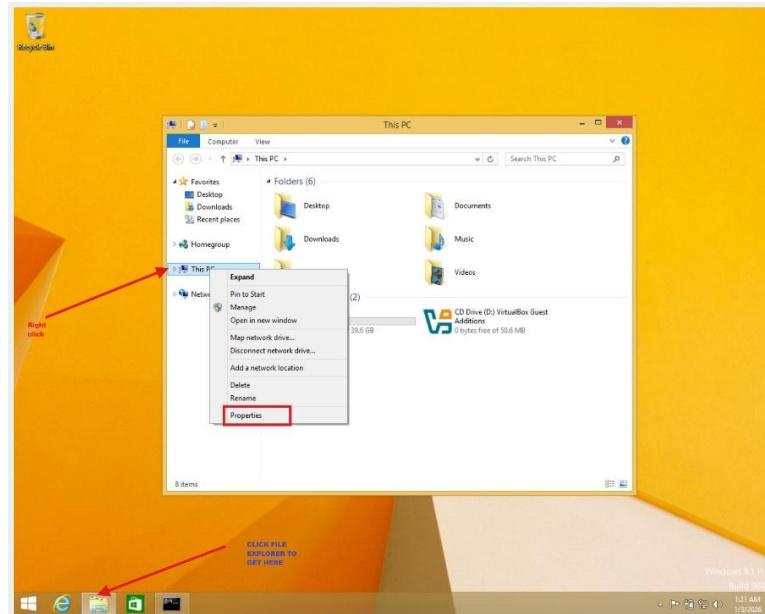


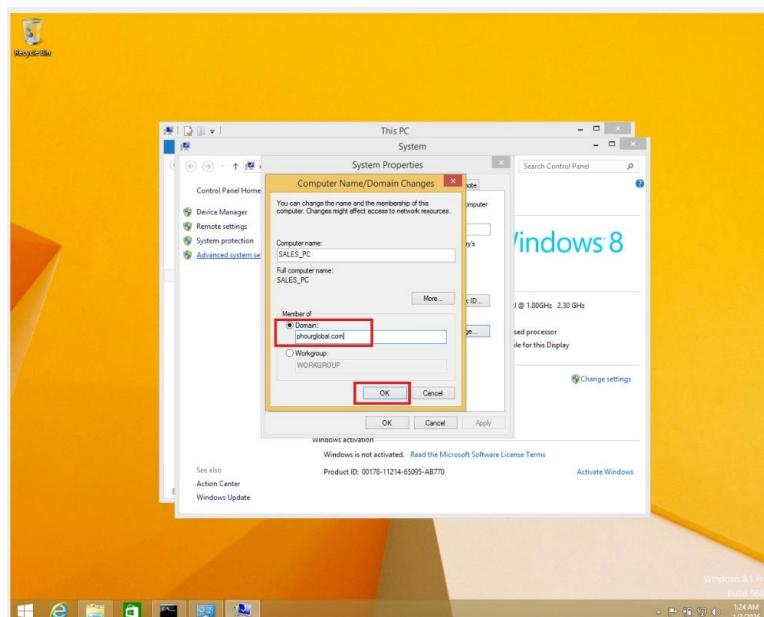
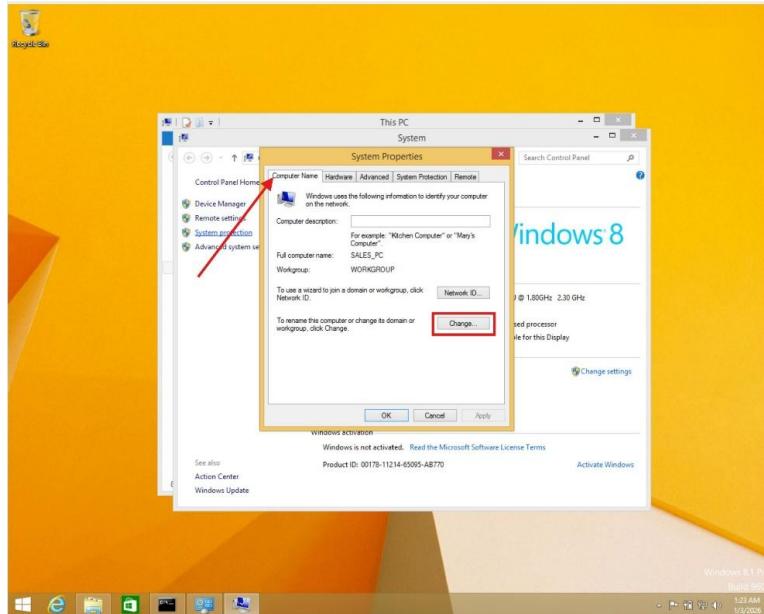


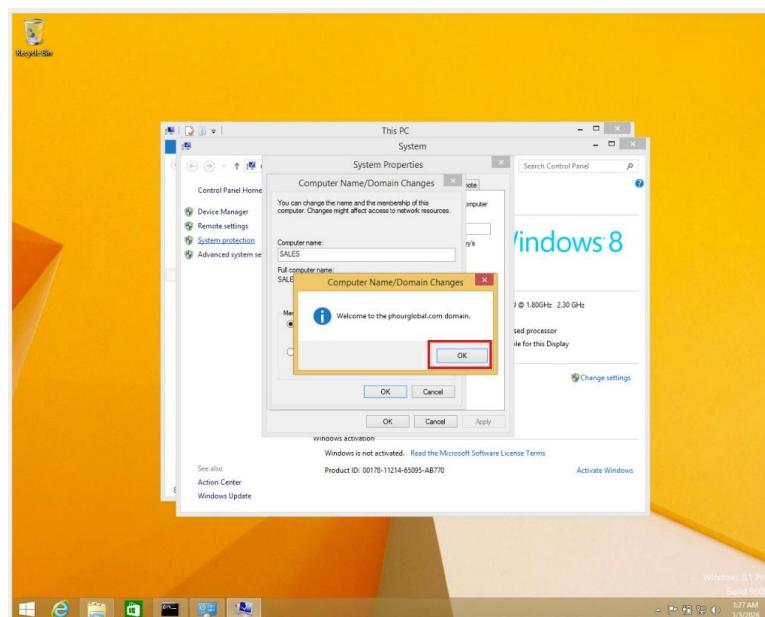
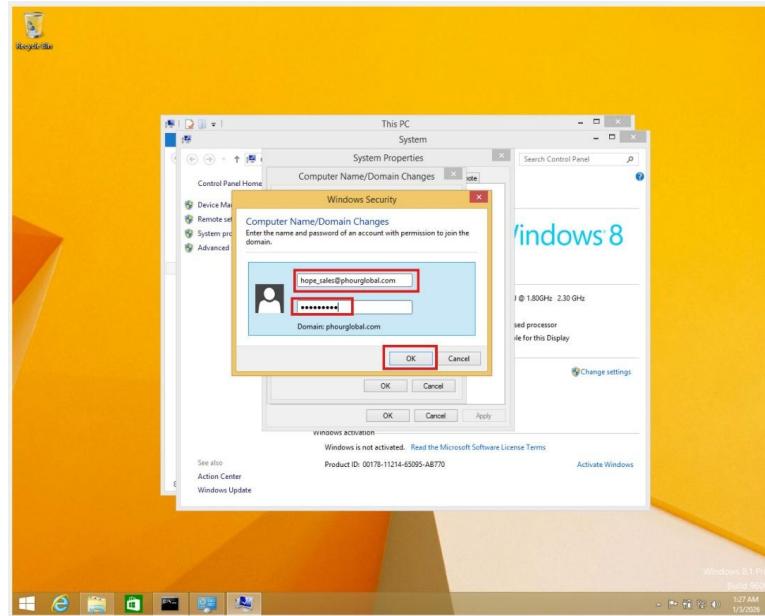


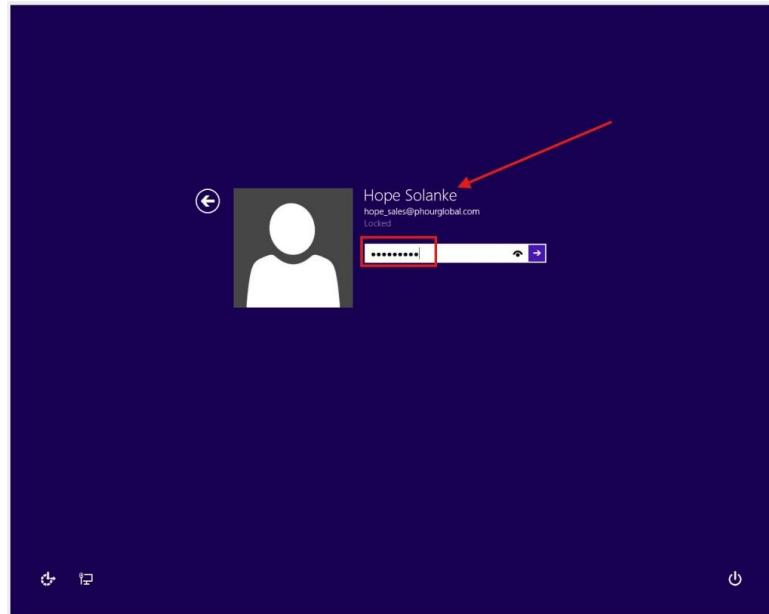
Phase 5: Joining Computers to Domain

With network settings configured, join the Windows 8 client computer to the phourglobal.com domain. This process establishes trust between the client and the domain controller.



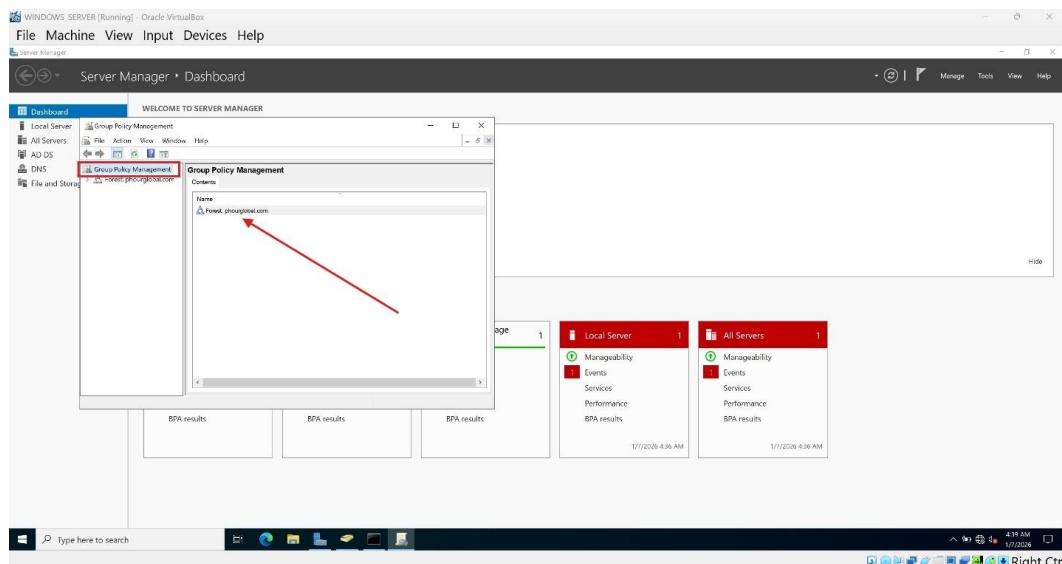
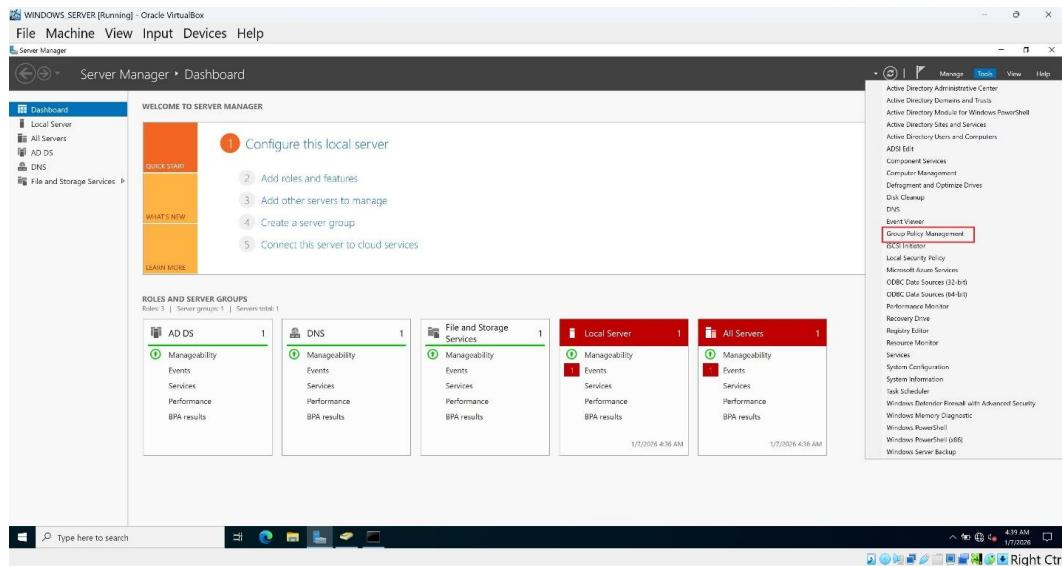


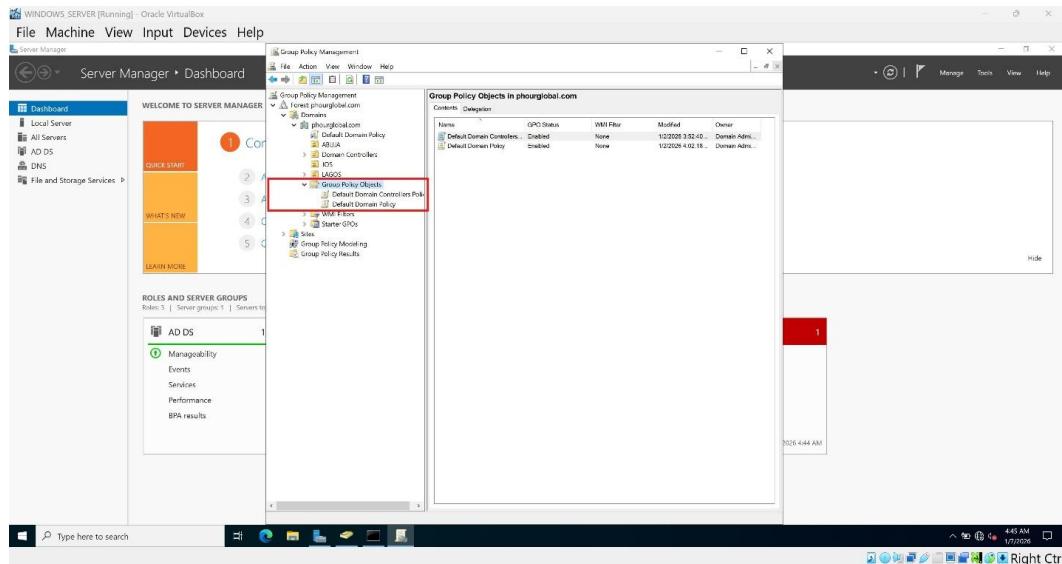
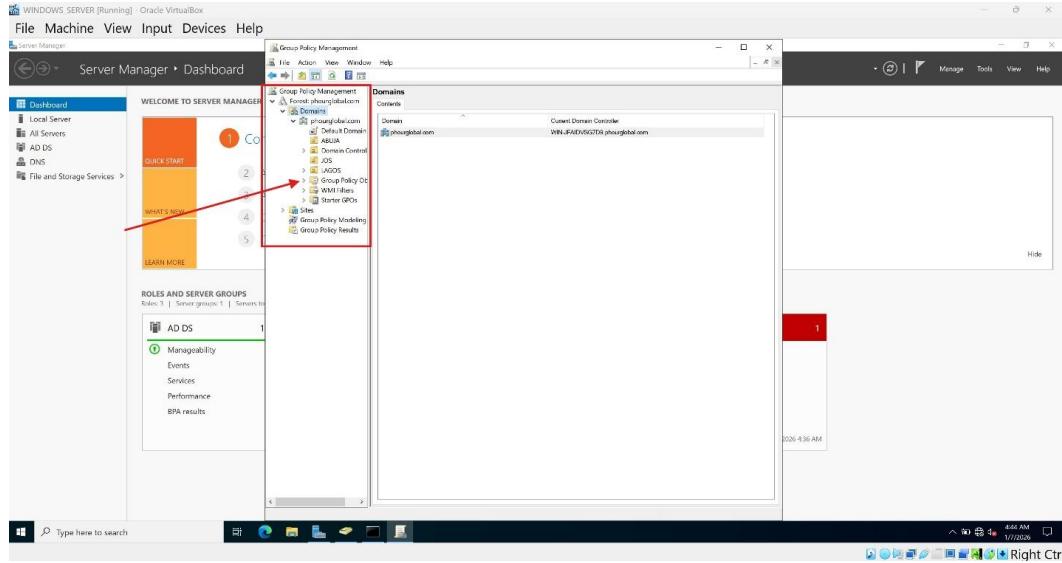


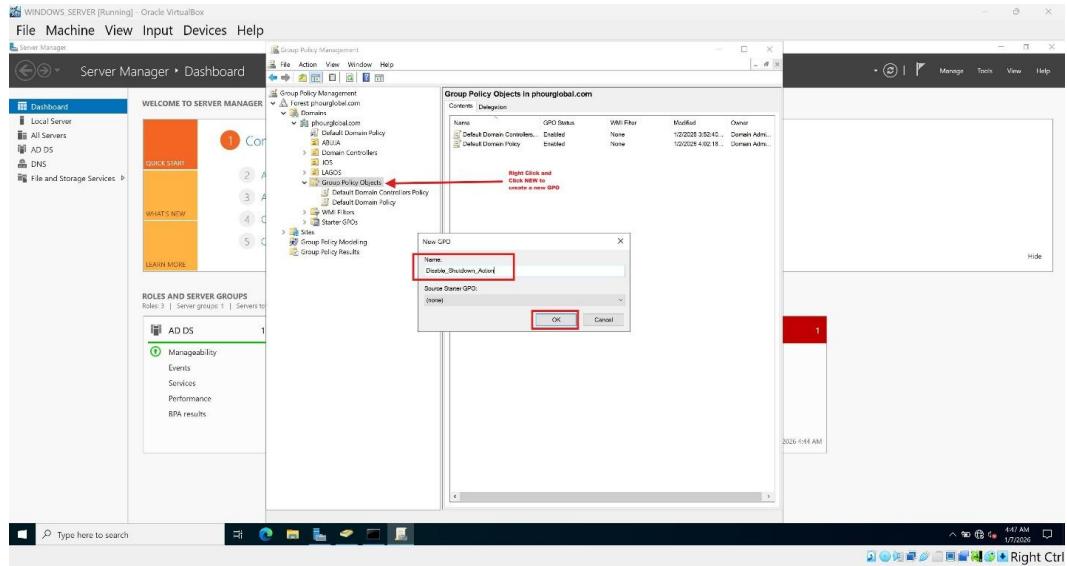


Phase 6: Group Policy Management

Group Policy allows centralized management of user and computer settings. This section demonstrates creating and applying a policy to restrict shutdown options for specific users.



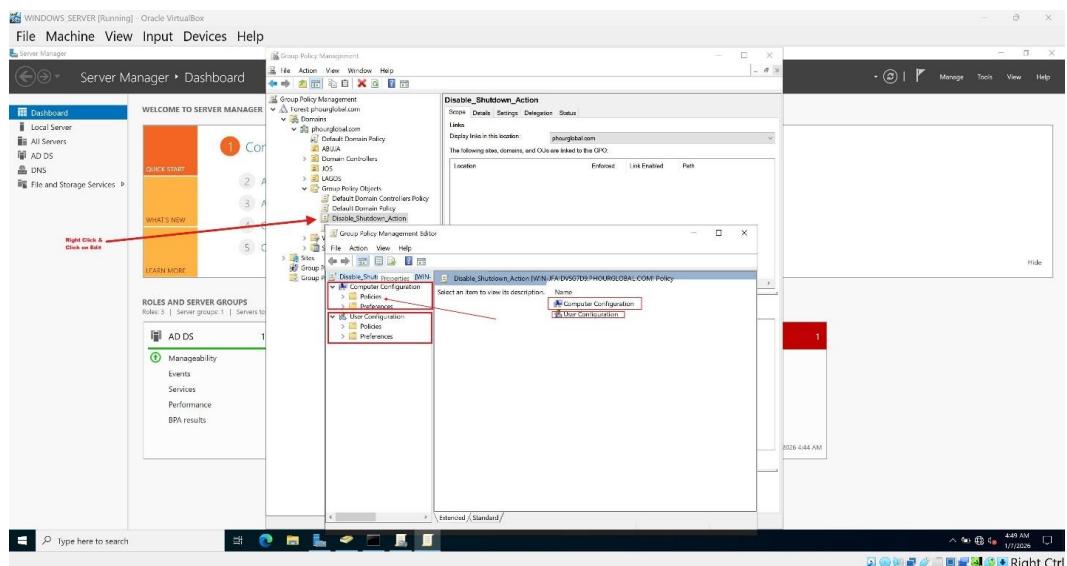


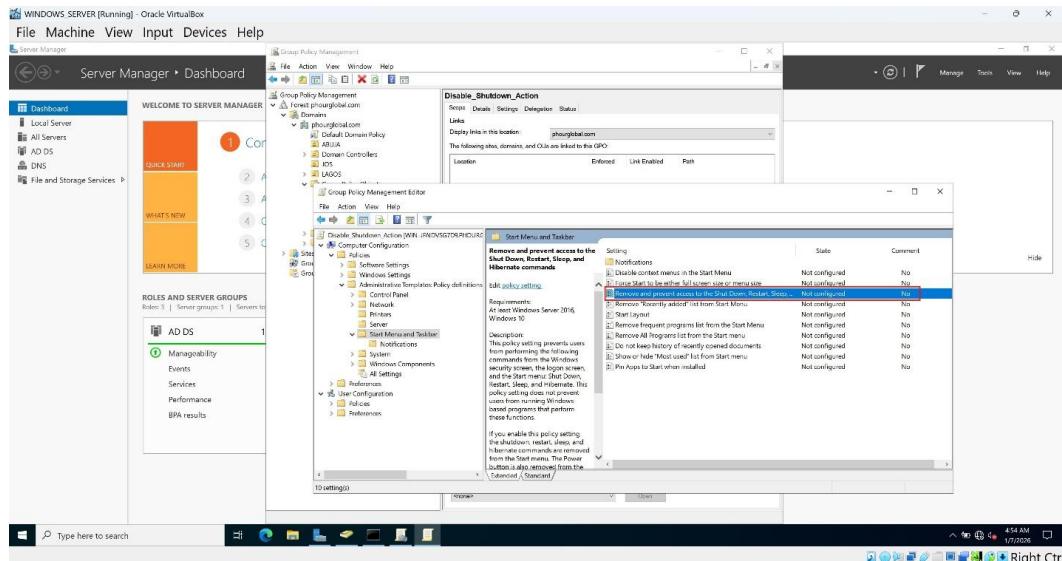
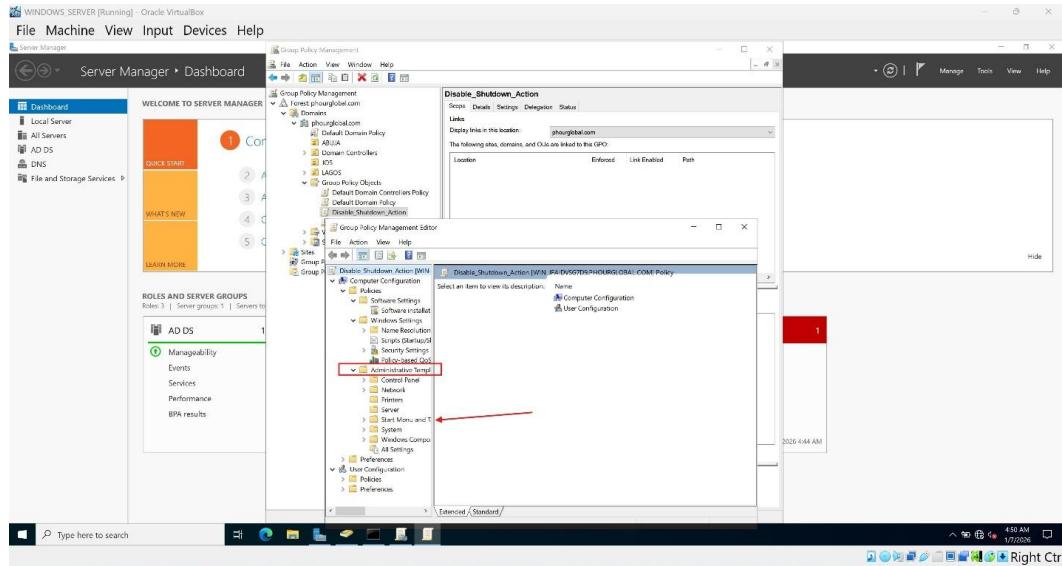


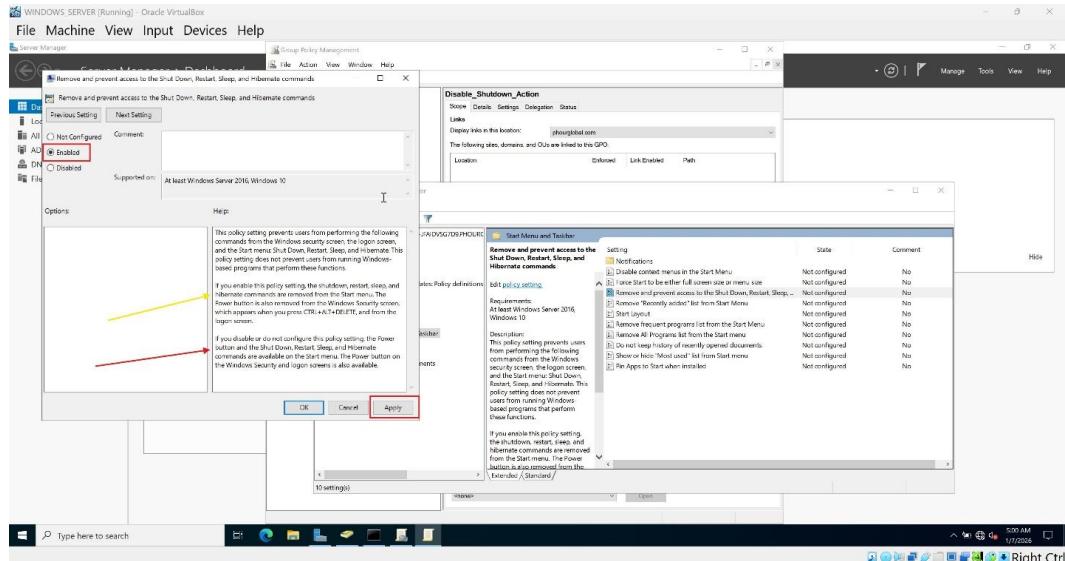
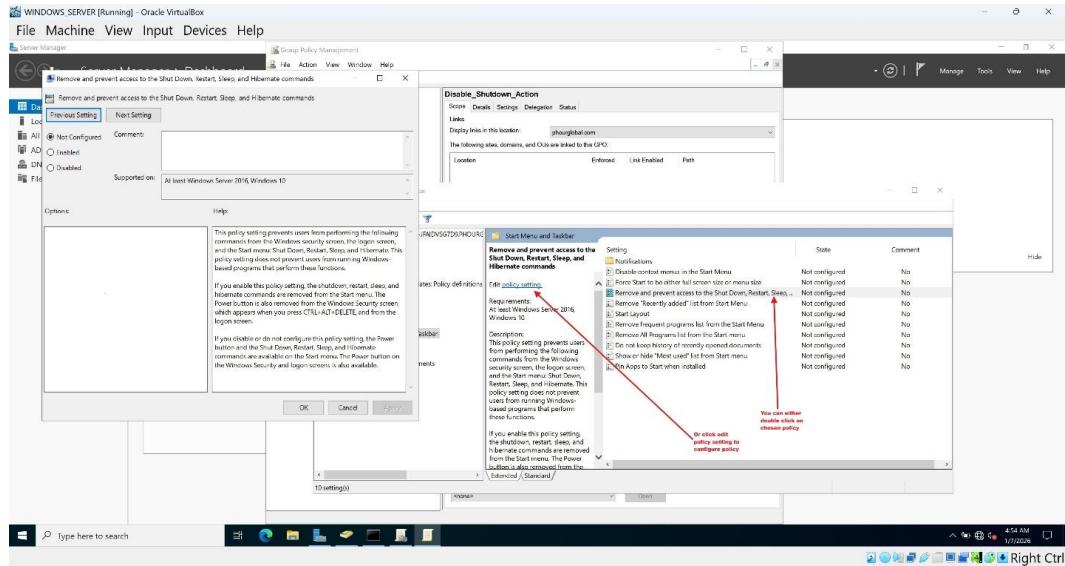
Configuring Shutdown Restriction Policy

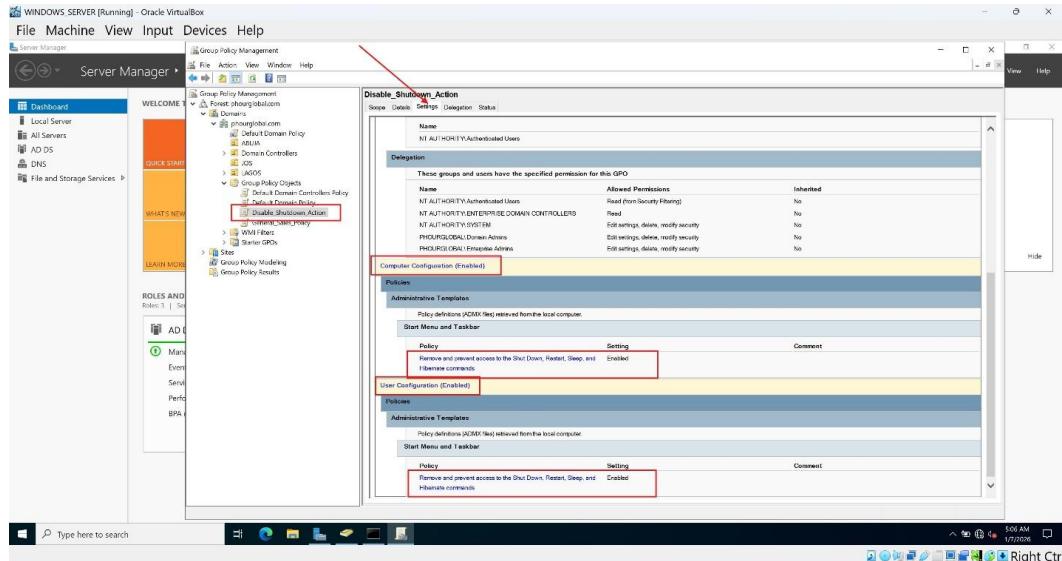
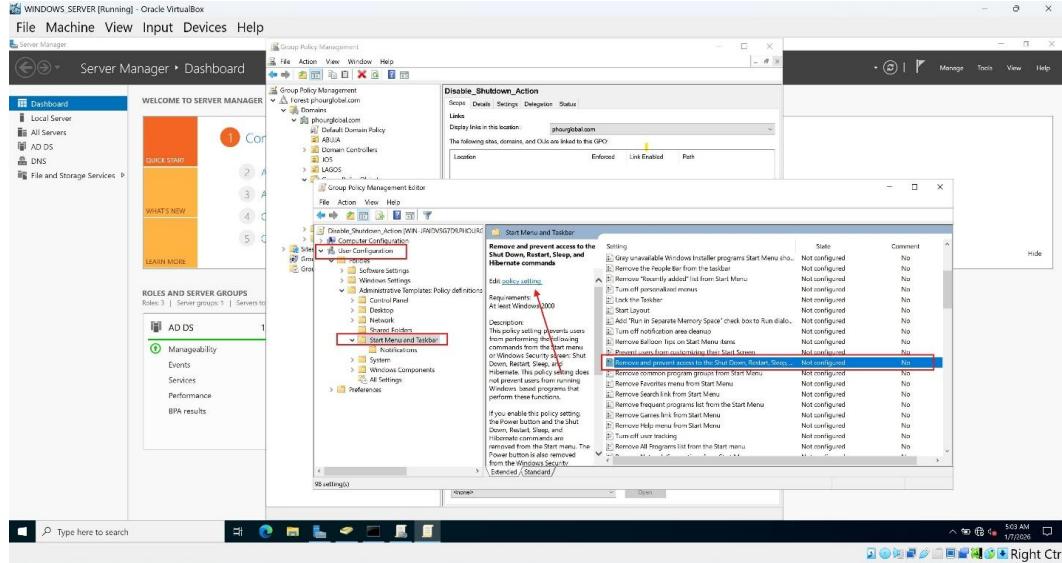
Navigate to User Configuration, Administrative Templates, then Start Menu and Taskbar.

Enable the policy "Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands".



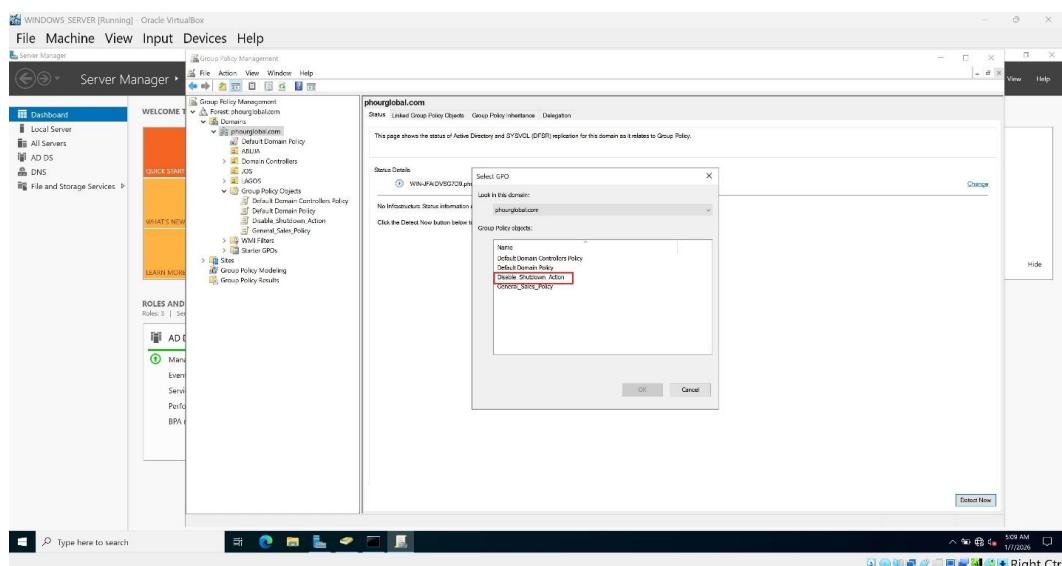
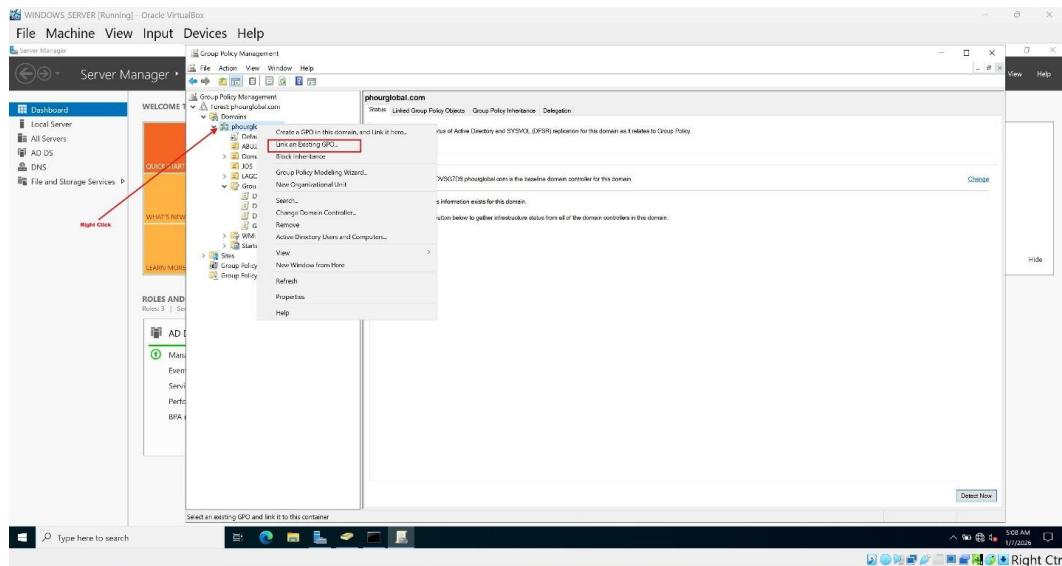


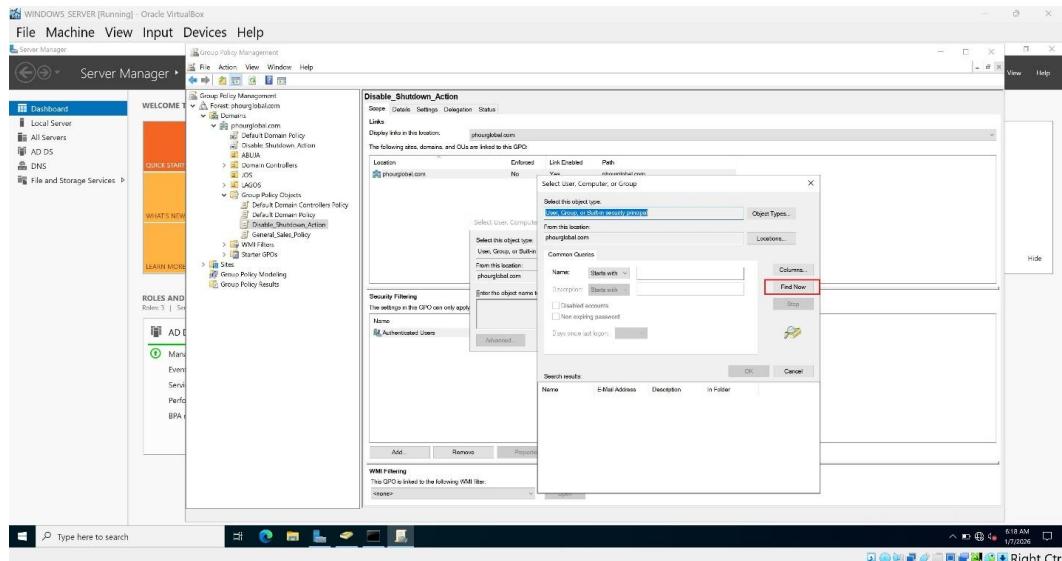
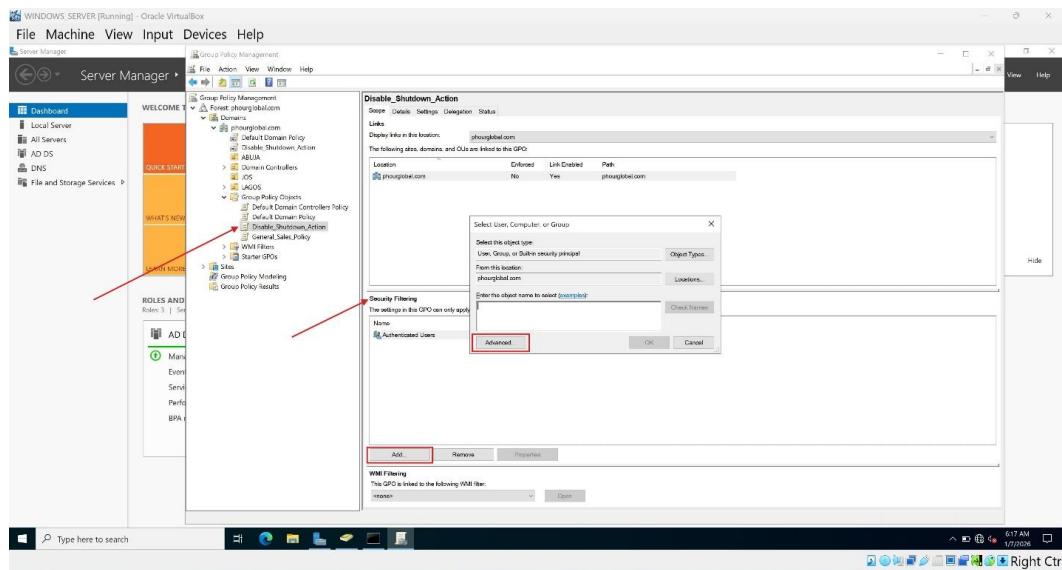


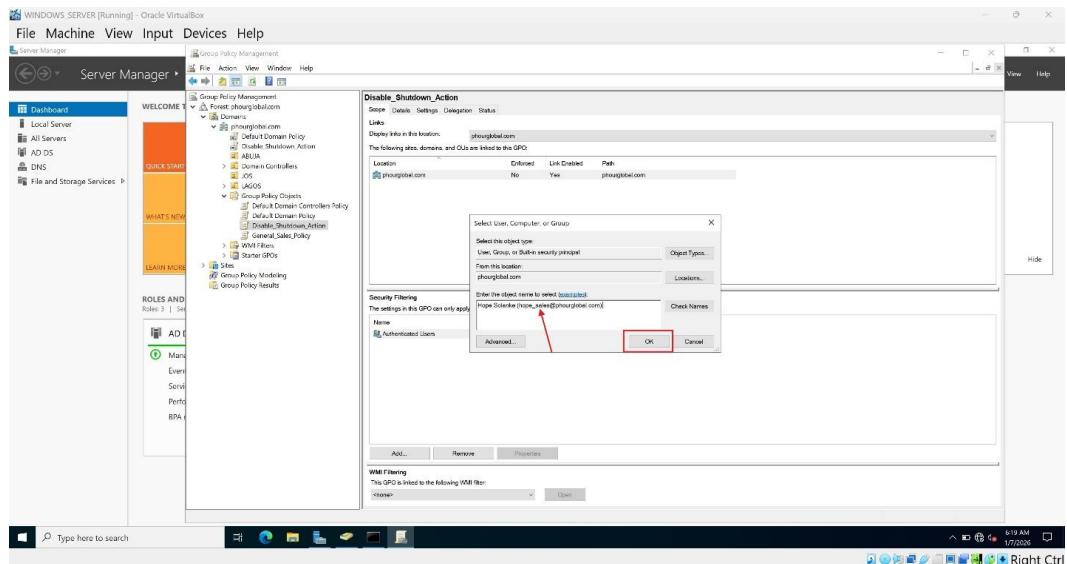
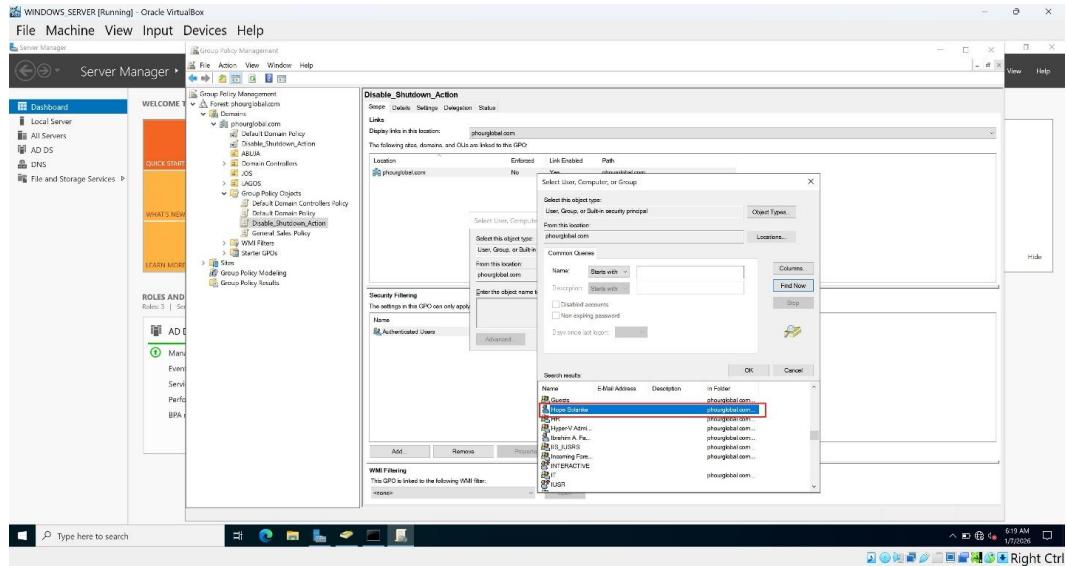


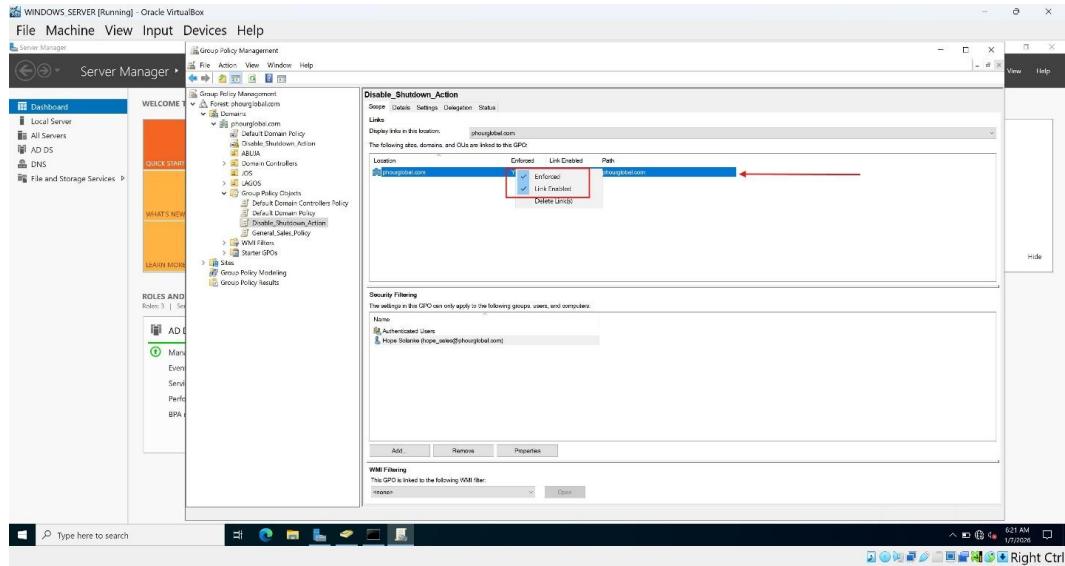
Linking and Applying GPO

Link the GPO to the ABUJA OU, then configure security filtering to apply the policy only to hope_sales@phourglobal.com. Remove Authenticated Users and add the specific user account.



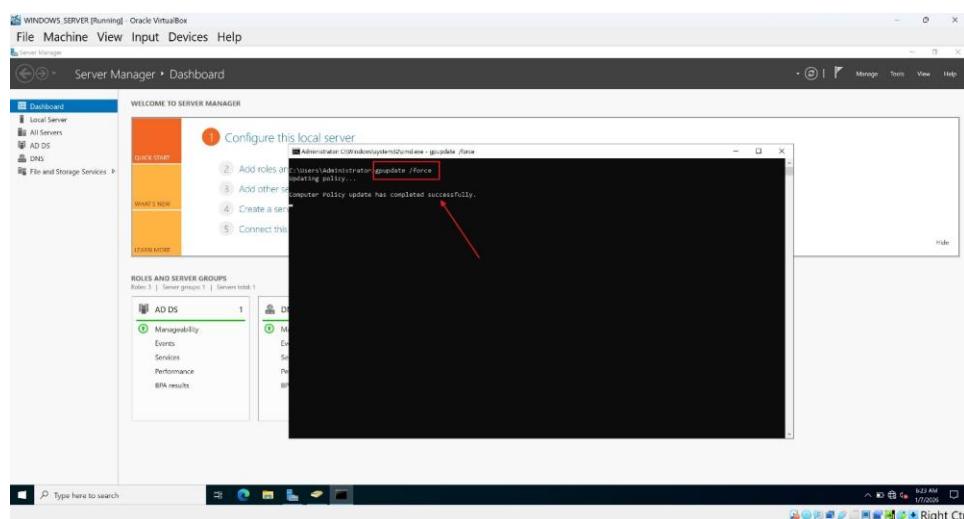
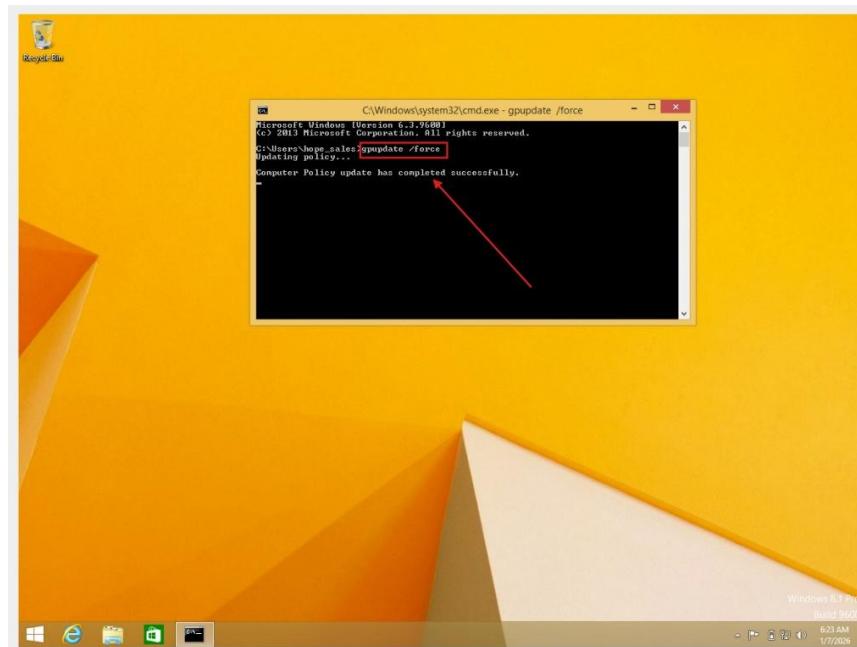


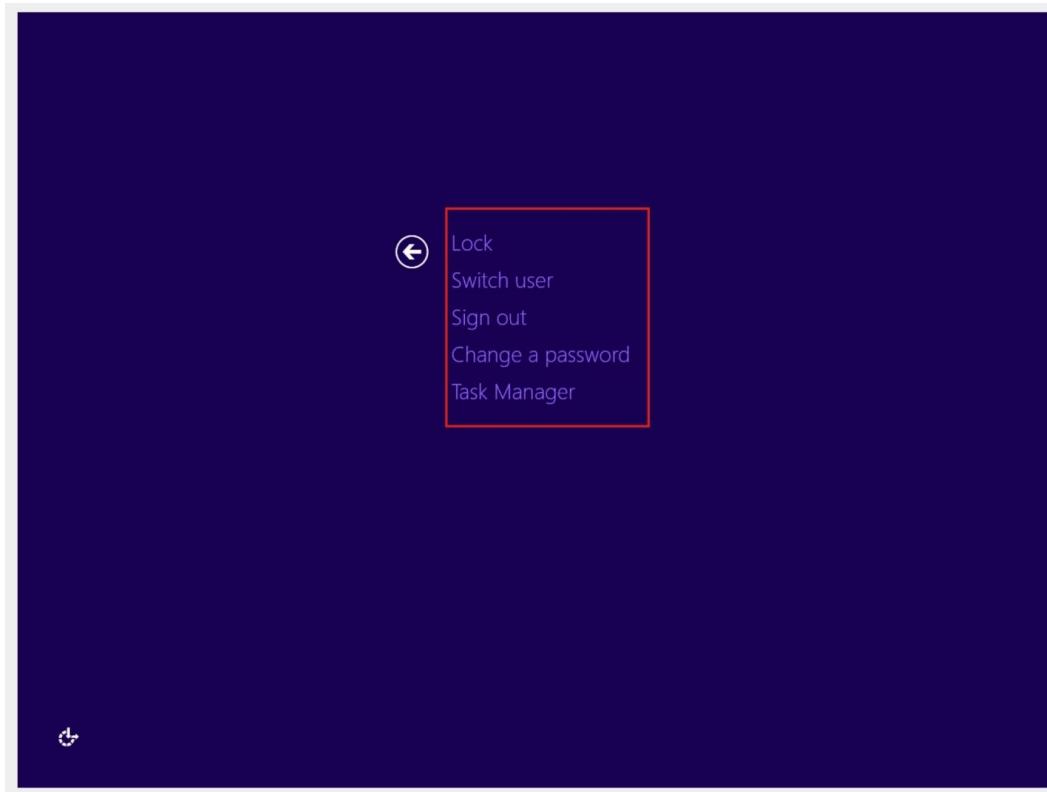
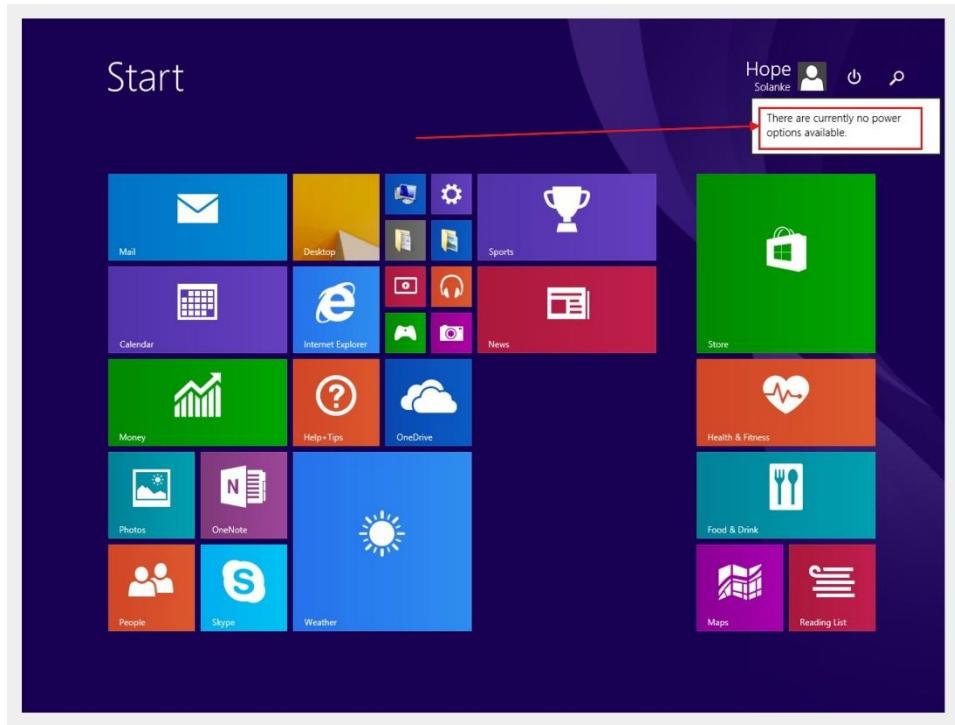




Policy Update and Verification

Run gpupdate /force on both the server and client machines to apply the new policy immediately. Log in as hope_sales and verify that shutdown options are no longer available in the Start menu or when pressing Ctrl+Alt+Delete.





Project Summary

This project successfully implemented a complete Active Directory infrastructure for Phour Global Limited. The environment includes a fully functional domain controller managing user authentication, DNS resolution, and centralized policy enforcement across multiple client computers.

Key Accomplishments

Configured Windows Server as the primary domain controller for phourglobal.com with integrated DNS services. Established a three-tier organizational unit structure representing company locations in Abuja, Jos, and Lagos. Created department-specific security groups and user accounts following standard naming conventions. Successfully joined Windows 8 client computers to the domain. Implemented and tested group policy for user-specific access control.

Skills Demonstrated

This project demonstrates proficiency in Windows Server administration, Active Directory design and implementation, DNS configuration, group policy management, and identity and access management principles. The implementation follows industry best practices for domain controller deployment and organizational unit design.

Future Enhancements

Additional improvements could include implementing DHCP services on the domain controller, configuring password policies and account lockout settings, establishing file server roles with shared folders, creating automated user provisioning scripts, and deploying a backup domain controller for redundancy.