### **Windows Server Administration Project Report**

**Name:Ziad Mahmoud Ahmed Abdelgwad**

### **1.0 Project Overview**

This document details the successful implementation and configuration of a Windows domain environment.The project involved setting up a multi-machine lab,installing Active Directory Domain Services(AD DS),and applying a comprehensive set of Group Policy Objects(GPOs)to enforce security,compliance,and user management rules.The policies cover a wide range of administrative tasks,from password enforcement and firewall rules to BitLocker encryption and application restrictions.All implemented policies were tested to ensure proper enforcement and functionality.

### **2.0 Project Requirements**

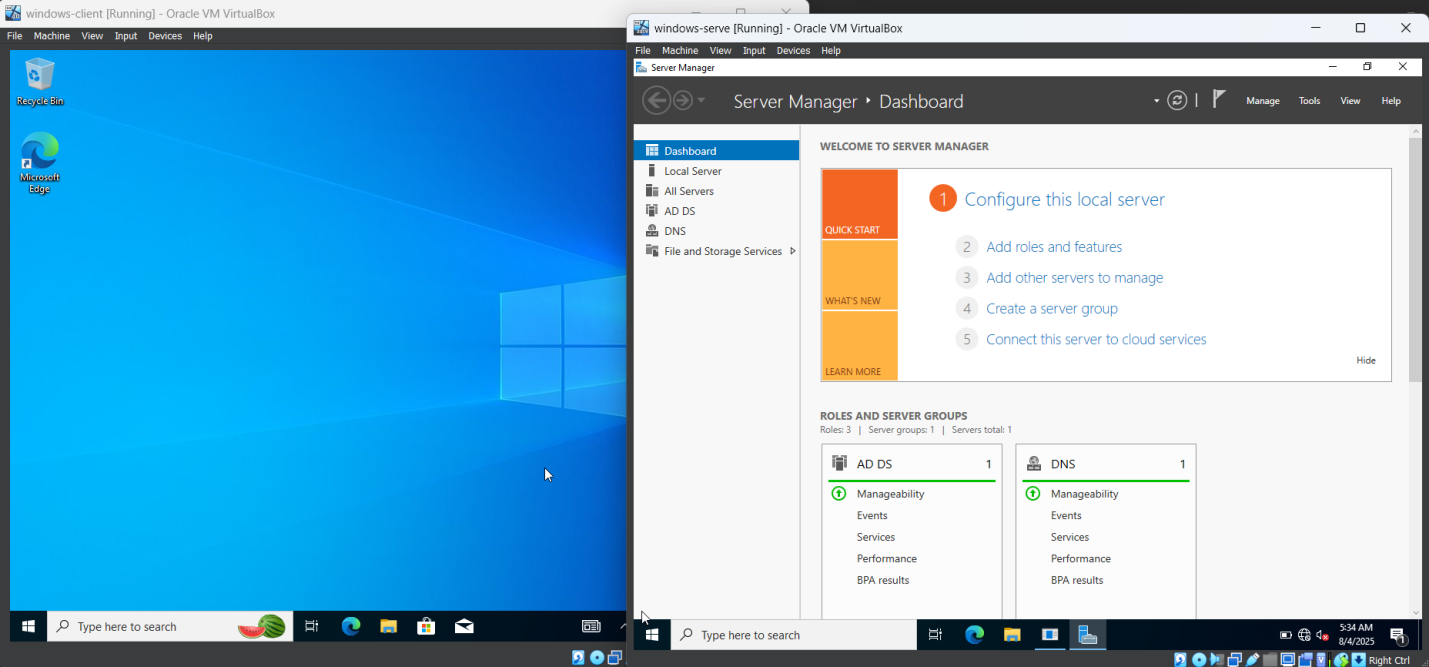
1. The following tasks were successfully completed as part of this project:
2. Install two Windows Server machines(or one Windows Server and one Windows machine).
3. Install AD DS(Active Directory Domain Services)on the Windows Server.
4. Promote this server to a Domain Controller(DC).
5. Join the other Windows machine to the server.
6. Create user accounts on the Active Directory.
7. Create Organizational Units(OUs)for users,and for the enrolled machine.
8. Apply a GPO to enforce strong password policies and password expiry dates.
9. Apply an account lockout policy for multiple failed logon attempts.
10. Apply audit policies on Domain Controllers and computers joined to the domain.
11. Apply a policy for screensavers.
12. Apply a policy to disable services.
13. Apply a firewall rule to block pinging to 8.8.8.8 and 8.8.4.4.
14. Apply a policy to disallow media drives.
15. Apply a policy to restrict software installation.
16. Apply a policy to set a logon message.
17. Apply a policy to disable CMD and PowerShell.
18. Apply a policy for RDP restrictions(limit connections,set idle session timeout).
19. Apply a policy to Microsoft Edge to disable InPrivate mode.
20. Apply a policy to disable access to Registry Editor.
21. Apply a policy to prevent the installation of printer drivers.
22. Apply a policy to restrict time-of-day logins.
23. Apply a policy to configure Windows Defender to scan network files.
24. Apply a policy to enforce BitLocker Encryption.

### **3.0 Project Implementation:**

This section outlines the detailed steps and configurations for each project requirement,with screenshots provided as proof.

#### **3.1 Step 1:Install Windows Server and Client**

**Action:**Two virtual machines were set up in Oracle VirtualBox:one Windows Server and one Windows client.Both were configured on the same network to enable communication.



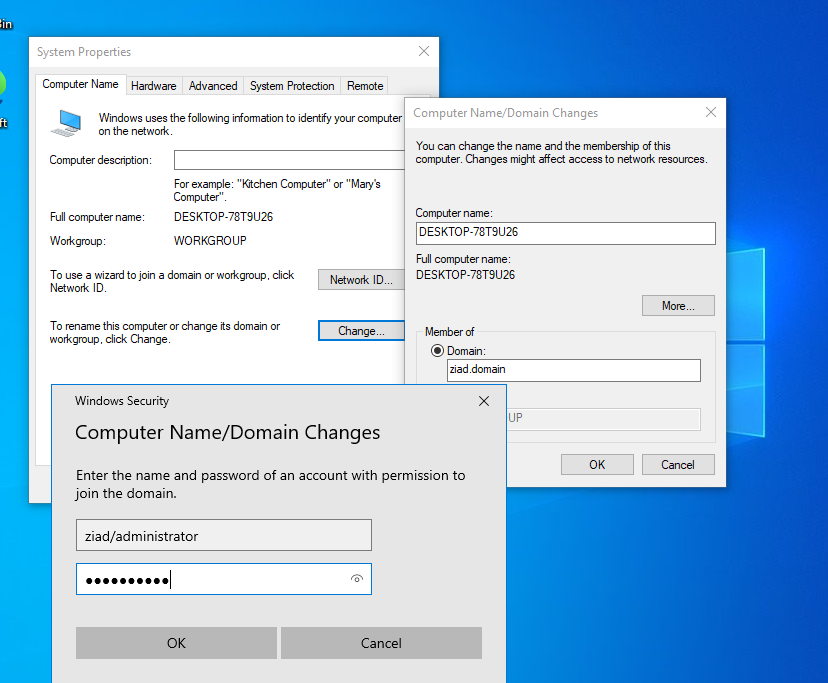
#### **3.2 Step 2&3:Install AD DS and Promote to DC**

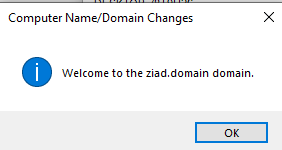
**Action:**The Active Directory Domain Services role was installed on the Windows Server,which was then promoted to a Domain Controller for the domain ziad.domain.

#### **Create Users and OUs 1**

#### **3.3 Step 4:Join the Client to the Domain**

**Action:**The client machine was joined to the ziad.domain by entering the domain name and the credentials of a domain administrator.



)

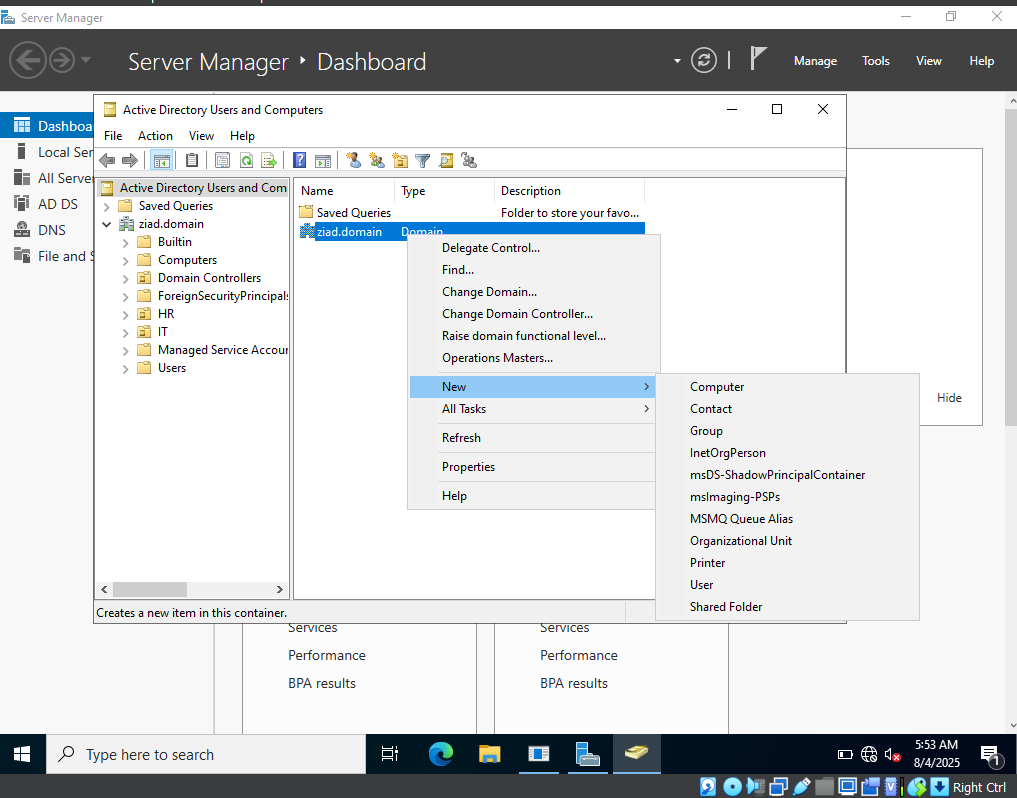
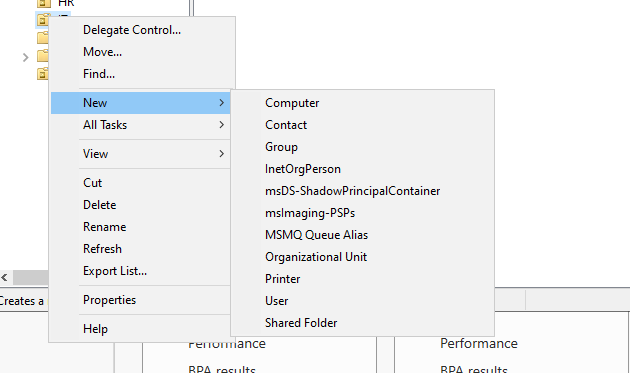
#### **3.4 Step 5&6:Create Users and OUs**

**Action:**Organizational Units(OUs)were created in Active Directory to organize users and computers.A user account was then created within the IT OU.

**1.Open Active Directory Users and Computers:**Navigate to **Server Manager>Tools>Active Directory Users and Computers**.

**2.Create an OU:**Right-click the domain name and select **New>Organizational Unit**.

**3.Create a User:**Right-click the new OU and select **New>User**.

!

#### **3.5 Step 7&8:Password and Account Lockout Policies**

**Action:**A GPO was created and linked to the IT OU to enforce strong passwords and account lockout settings.

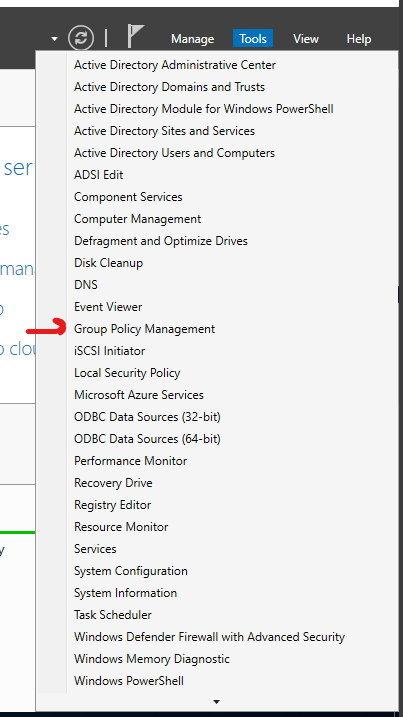
**1.Open Group Policy Management:**Navigate to **Server Manager>Tools>Group Policy Management**.

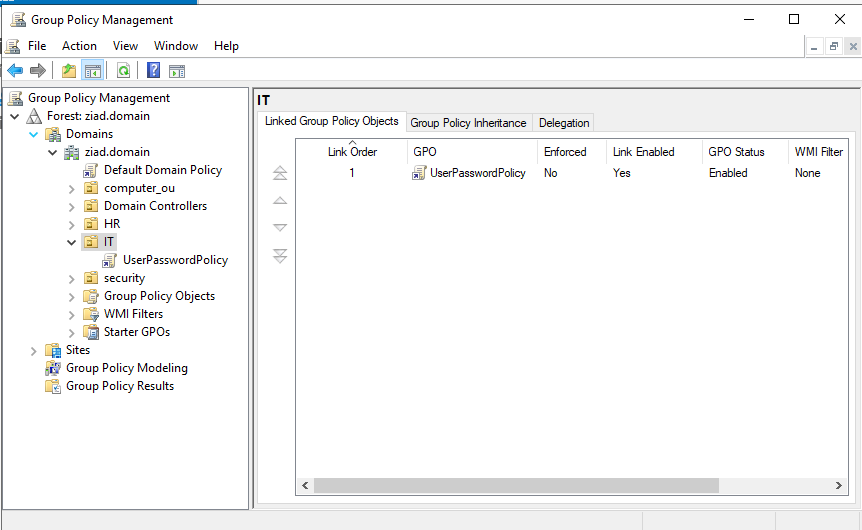
**2.Create a GPO:**Right-click the IT OU,select **Create a GPO in this domain,and link it here...**.

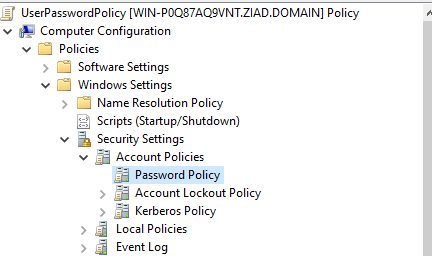
**3.Edit the GPO:**Right-click the new GPO and select **Edit...**.

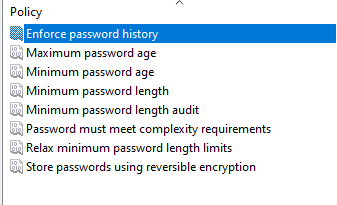
**4.Configure Password Policy:**Navigate to Computer Configuration>Policies>Windows Settings>Security Settings>Account Policies>Password Policy and configure the settings.

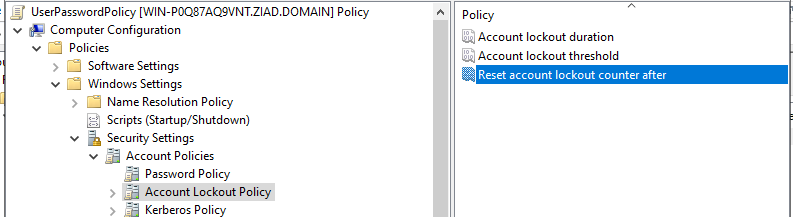
**5.Configure Account Lockout:**Navigate to Computer Configuration>Policies>Windows Settings>Security Settings>Account Policies>Account Lockout Policy and configure the settings.











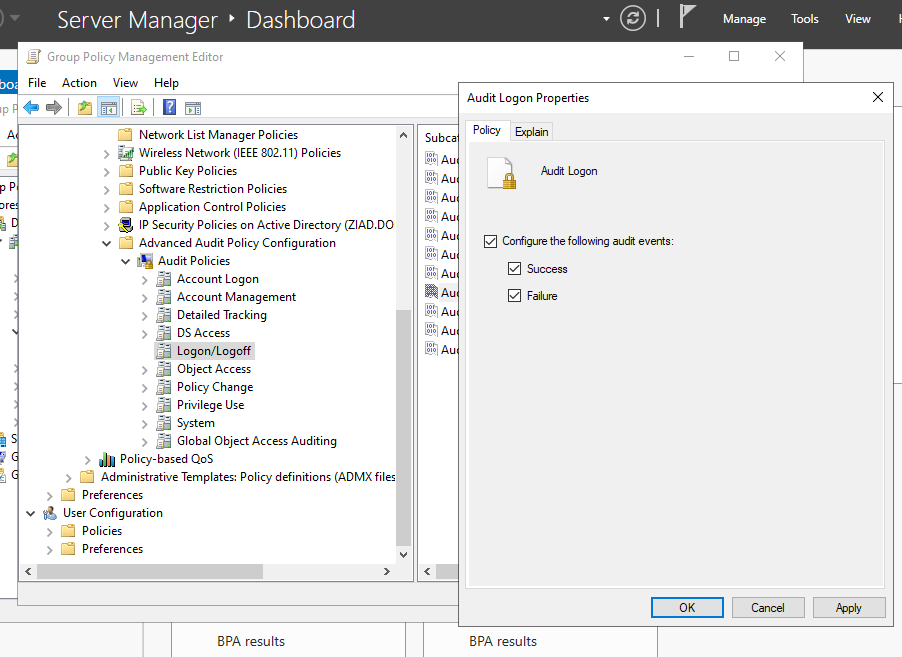
#### **3.6 Step 9:Audit Policies**

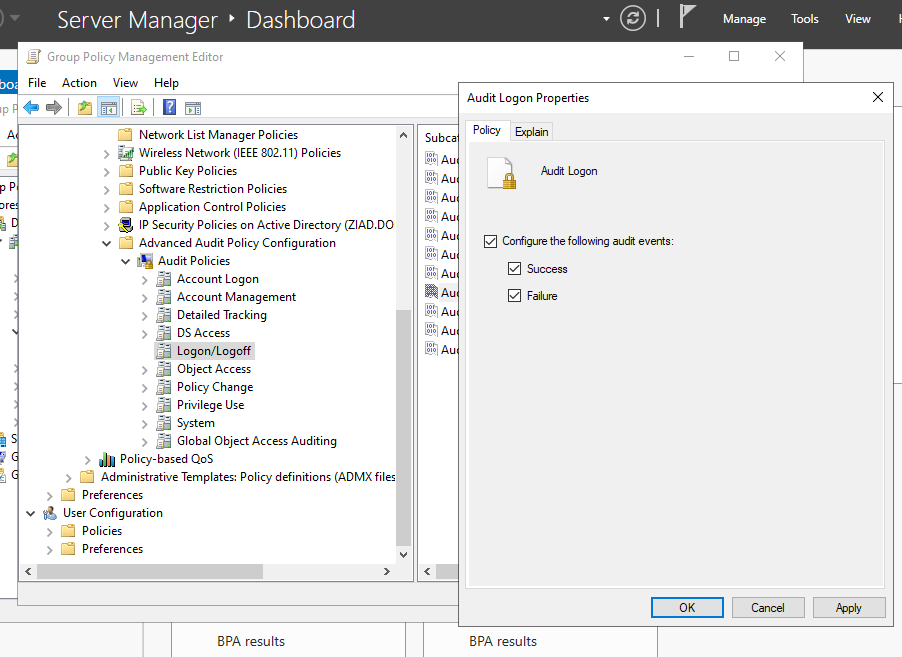
**Action:**Advanced Audit Policies were configured in the Default Domain Policy to audit logon and account management events.

**1.Edit the GPO:**In Group Policy Management,right-click the Default Domain Policy and select **Edit...**.

**2.Navigate to Audit Policies:**Go to Computer Configuration>Policies>Windows Settings>Security Settings>Advanced Audit Policy Configuration>Audit Policies.

**3.Configure Logon/Logoff and Account Management:**Enable auditing for both Success and Failure events.



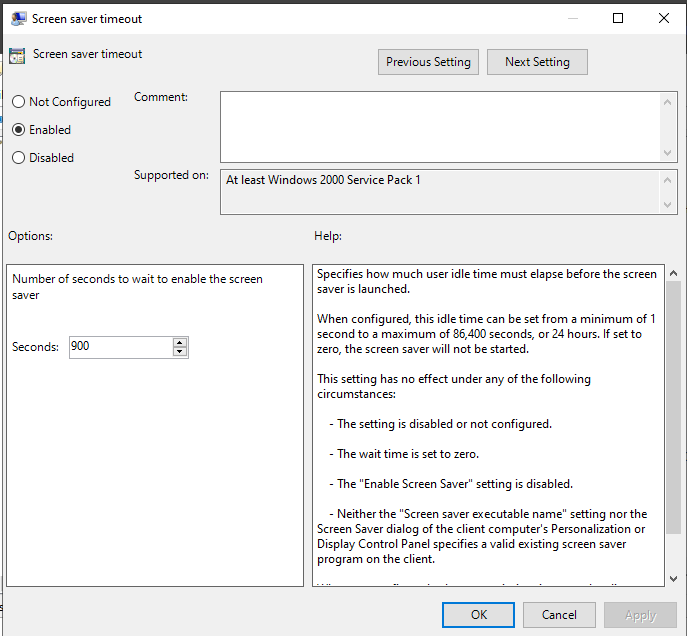
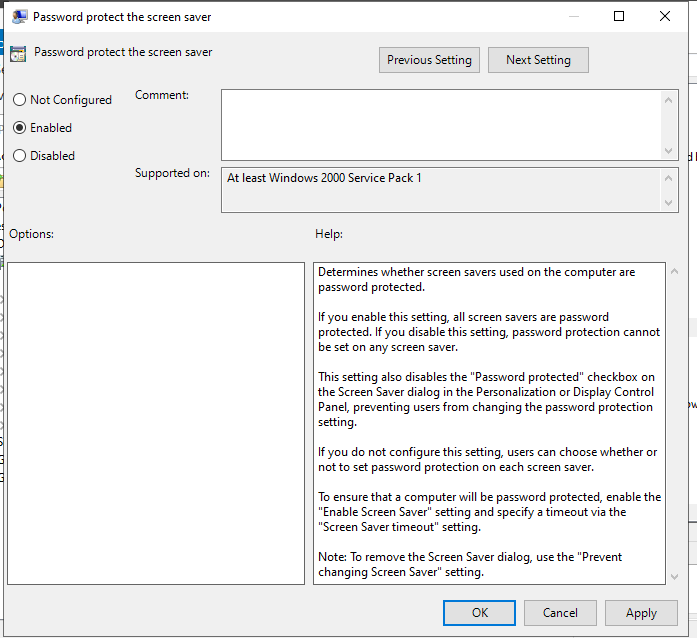
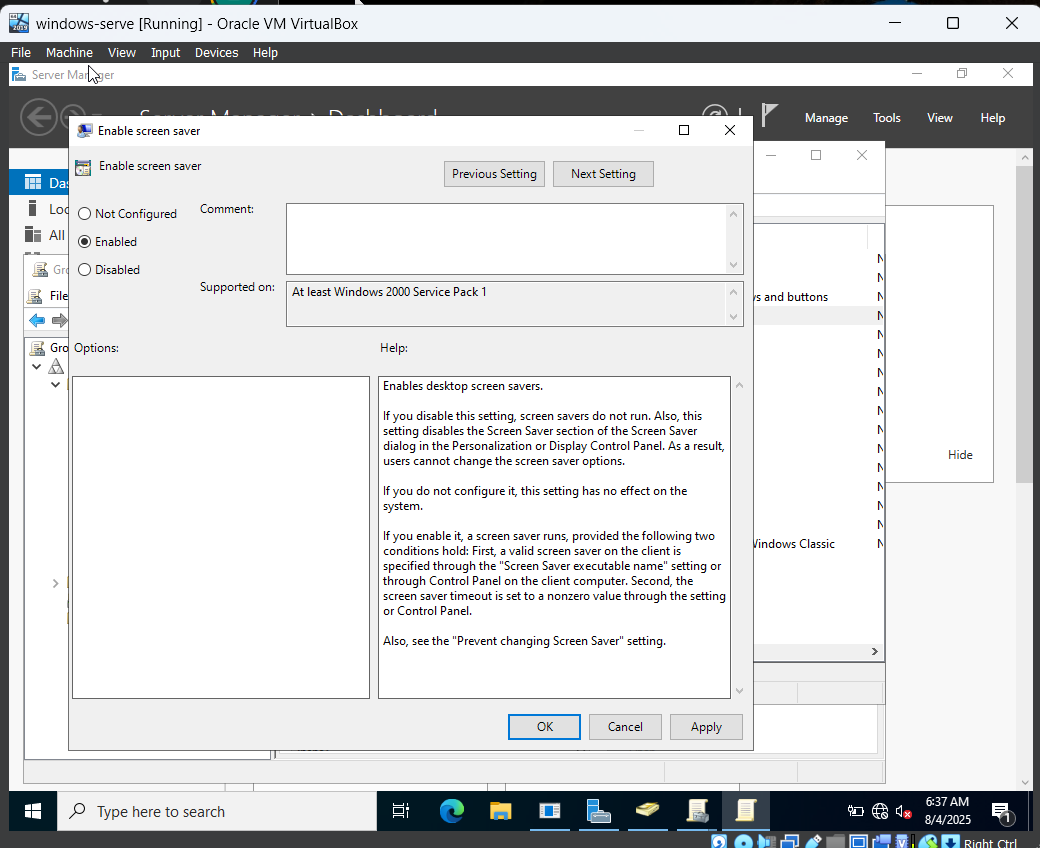


#### **3.7 Step 10:Screen Saver Policy**

**Action:**A GPO linked to the user OU was edited to enable the screen saver,protect it with a password,and set a timeout.

**1.Edit the GPO:**Right-click a GPO linked to your user OU and select **Edit...**.

**2.Navigate to Personalization:**Go to User Configuration>Policies>Administrative Templates>Control Panel>Personalization.

**3.Configure Settings:**Enable Enable screen saver,Password protect the screen saver,and Screen saver timeout.

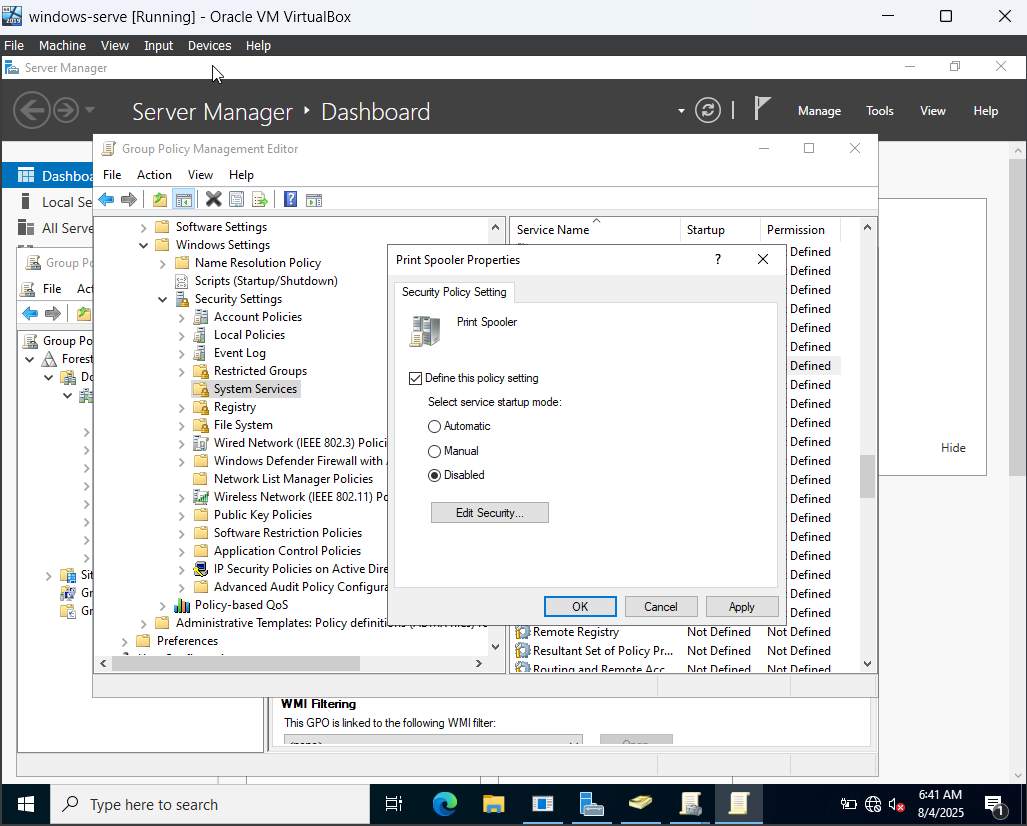
#### **3.8 Step 11:Disable Services**

**Action:**A GPO linked to the computer OU was edited to disable specific system services like the Print Spooler.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Navigate to System Services:**Go to Computer Configuration>Policies>Windows Settings>Security Settings>System Services.

**3.Disable the Service:**Find the service,double-click it,and set its startup mode to Disabled.



#### **3.9 Step 12:Firewall Rule to Block Pinging**

**Action:**A GPO was used to create an outbound firewall rule that blocks ICMP traffic to specific remote IP addresses.

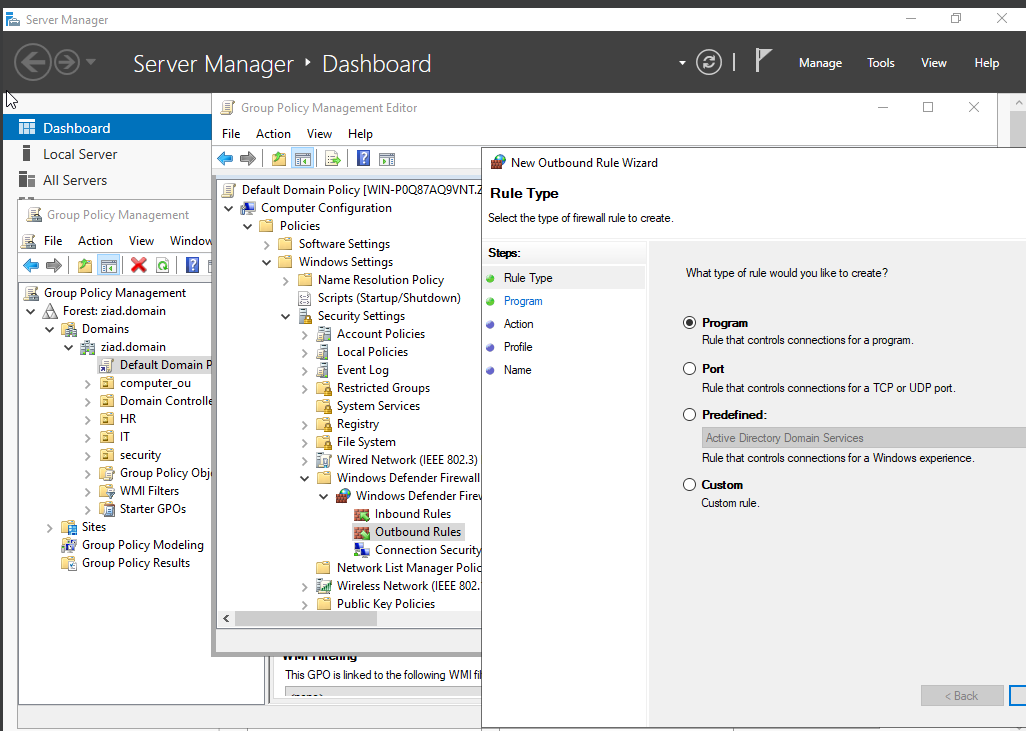
**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

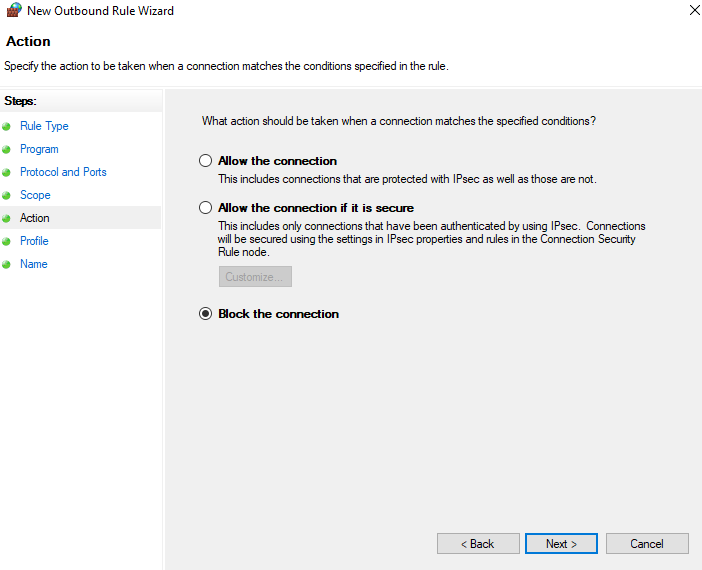
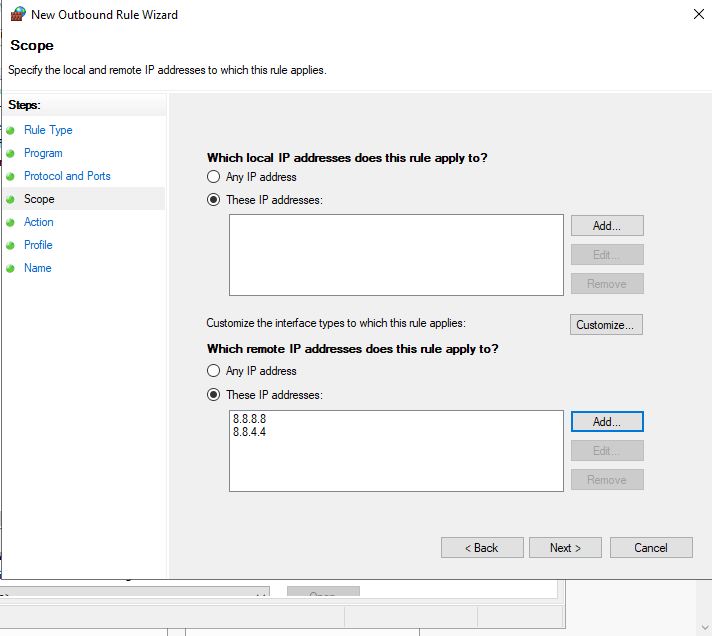
**2.Navigate to Firewall:**Go to Computer Configuration>Policies>Windows Settings>Security Settings>Windows Defender Firewall with Advanced Security>Outbound Rules.

**3.Create a New Rule:**Right-click Outbound Rules,select **New Rule...**,and choose **Custom** as the rule type.

**4.Configure Scope:**In the **Scope** tab,add 8.8.8.8 and 8.8.4.4 to the list of remote IP addresses.

**5.Set Action:**In the **Action** tab,choose **Block the connection**.





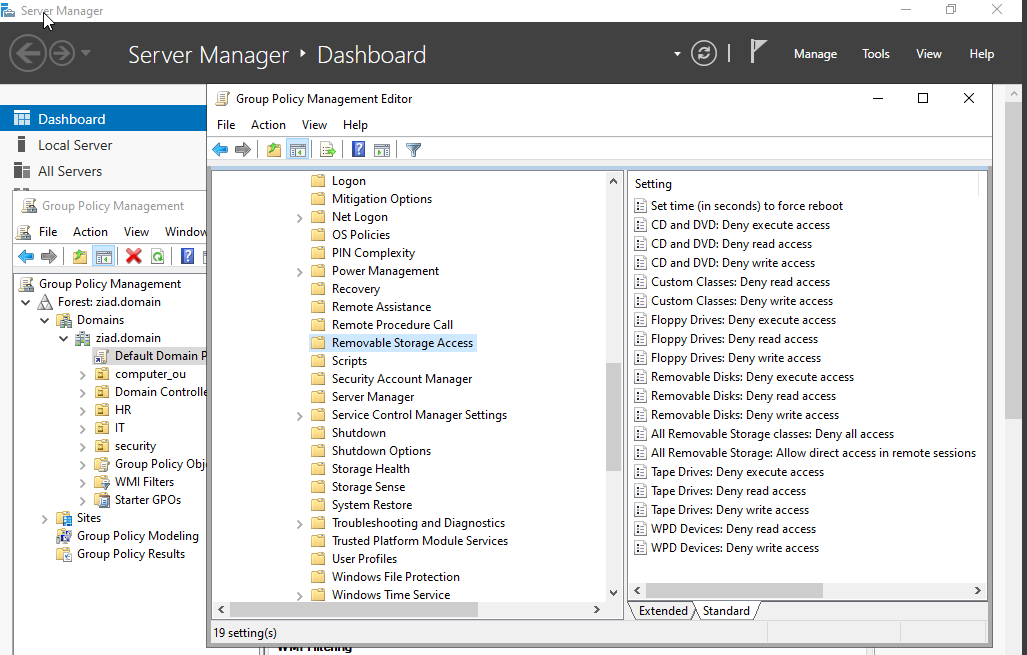
#### **3.10 Step 13:Disallow Media Drives**

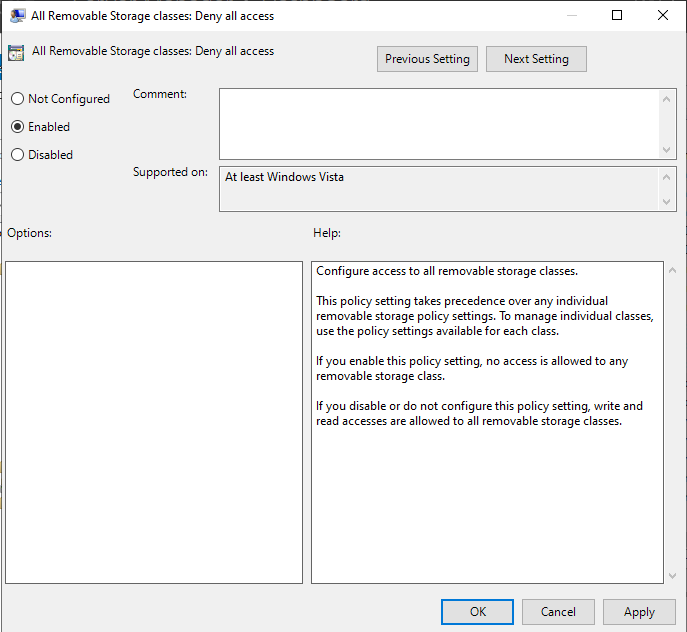
**Action:**A GPO was configured to deny all read,write,and execute access to removable storage devices.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Navigate to Removable Storage:**Go to Computer Configuration>Policies>Administrative Templates>System>Removable Storage Access.

**3.Configure Access:**Enable the All Removable Storage classes:Deny all access policy.





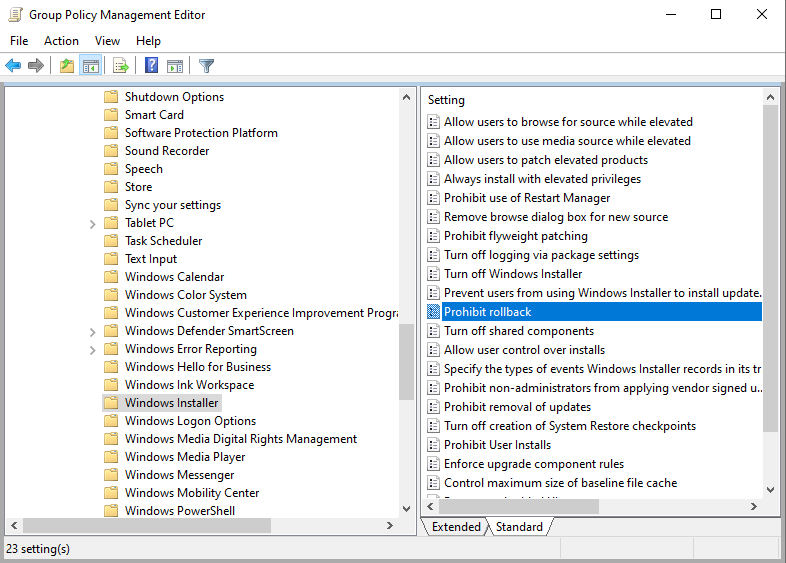
#### **3.11 Step 14:Restrict Software Installation**

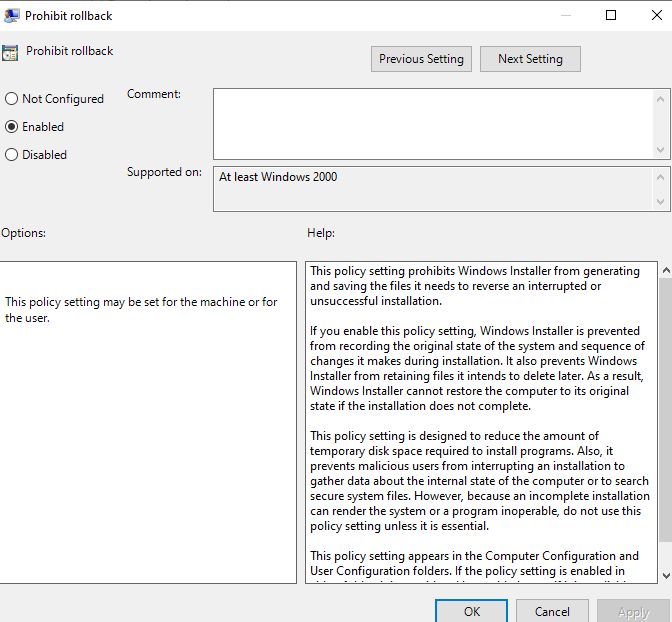
**Action:**The Windows Installer GPO settings were configured to restrict software installations.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Navigate to Windows Installer:**Go to Computer Configuration>Policies>Administrative Templates>Windows Components>Windows Installer.

**3.Configure Policy:**Enable the Prohibit rollback policy and other relevant policies to restrict installations.





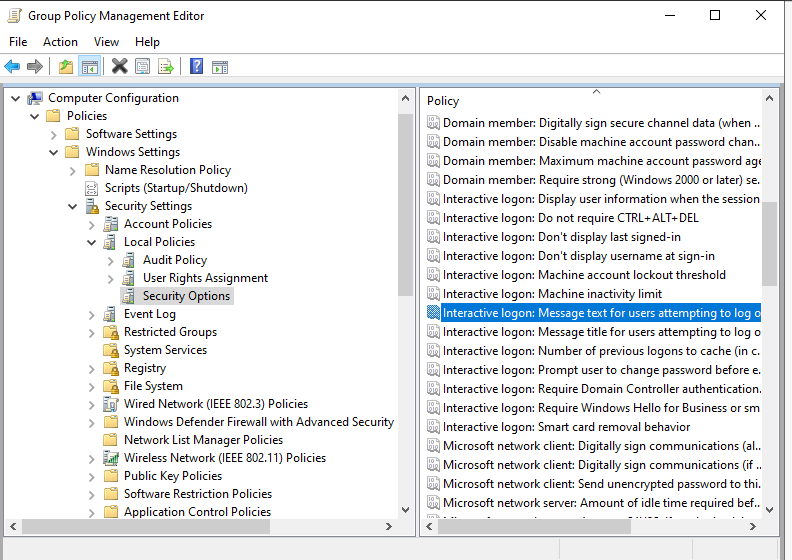
#### **3.12 Step 15:Set a Logon Message**

**Action:**A GPO was configured to display a custom legal notice to all users at the logon screen.

**1.Edit the GPO:**Right-click a GPO linked to your domain and select **Edit...**.

**2.Navigate to Security Options:**Go to Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options.

**3.Configure Messages:**Set Interactive logon:Message text for users attempting to log on and Interactive logon:Message title for users attempting to log on.



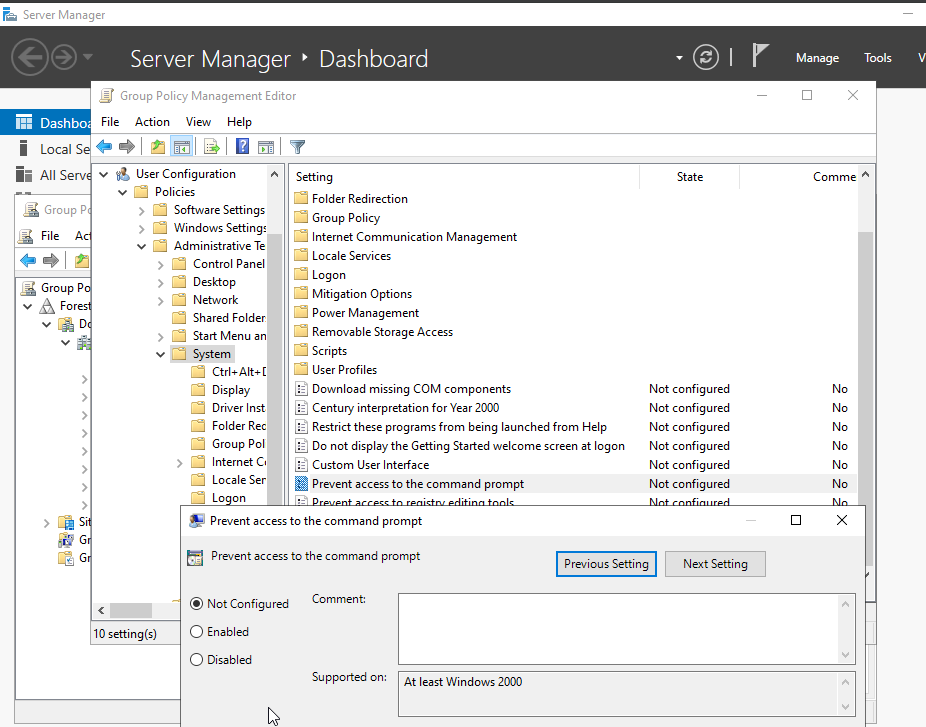
#### **3.13 Step 16:Disable CMD and PowerShell**

**Action:**A GPO was configured to prevent users from accessing the Command Prompt and PowerShell.

**1.Edit the GPO:**Right-click a GPO linked to your user OU and select **Edit...**.

**2.Navigate to System:**Go to User Configuration>Policies>Administrative Templates>System.

**3.Configure Policy:**Enable the Prevent access to the command prompt policy.



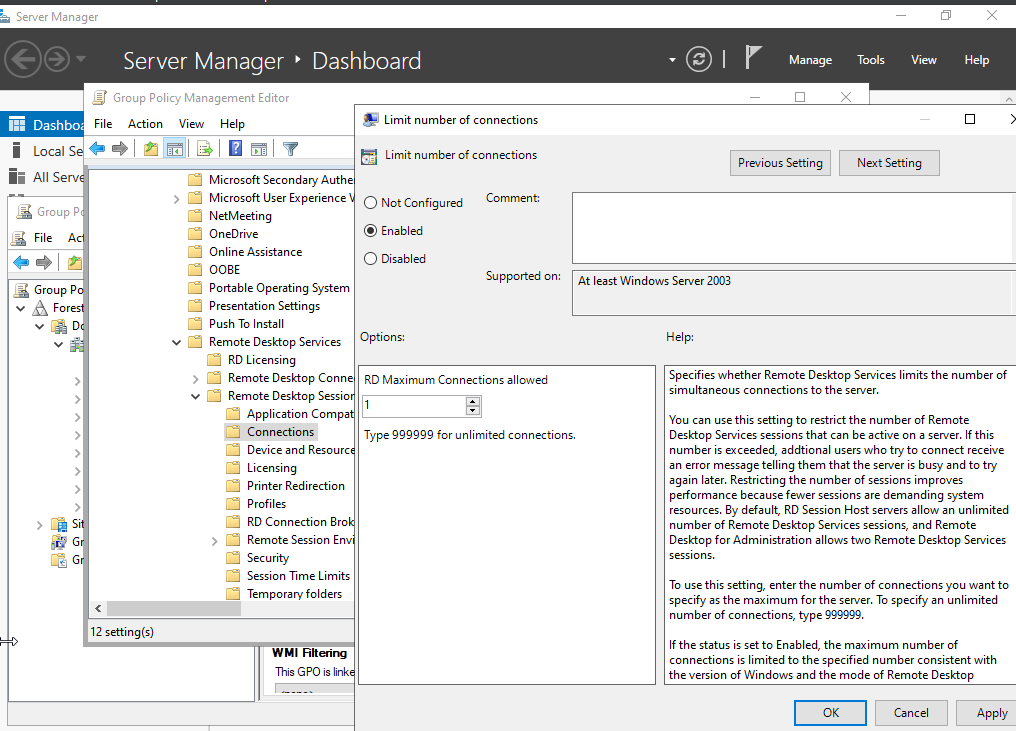
#### **3.14 Step 17:RDP Restrictions**

**Action:**A GPO was configured to limit the number of simultaneous RDP connections to the server.

**1.Edit the GPO:**Right-click a GPO linked to your server object and select **Edit...**.

**2.Navigate to RDP Services:**Go to Computer Configuration>Policies>Administrative Templates>Windows Components>Remote Desktop Services>Remote Desktop Session Host>Connections.

**3.Configure Connections:**Enable the Limit number of connections policy and set the maximum number.



#### **3.15 Step 18:Microsoft Edge-Disable InPrivate Mode**

**Action:**The Microsoft Edge Administrative Templates were downloaded and copied to the PolicyDefinitions folder on the Domain Controller.A GPO was then configured to disable InPrivate Browse.

**1.Download and Copy Templates:**Download the official Microsoft Edge policy templates and copy the.admx and.adml files to C:\Windows\SYSVOL\sysvol\<YourDomain>\Policies\PolicyDefinitions.

**2.Edit the GPO:**Right-click a GPO linked to your user OU and select **Edit...**.

**3.Navigate to Microsoft Edge:**Go to User Configuration>Policies>Administrative Templates>Microsoft Edge.

**4.Configure Policy:**Enable the Prevent InPrivate Browse policy.

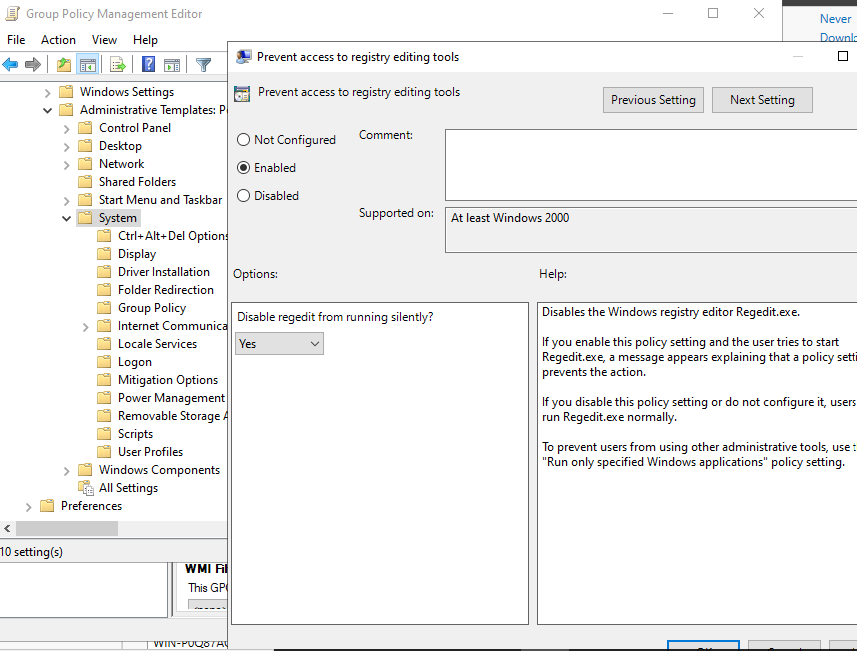
#### **3.16 Step 19:Disable Access to Registry Editor**

**Action:**A GPO was configured to prevent users from accessing the Registry Editor.

**1.Edit the GPO:**Right-click a GPO linked to your user OU and select **Edit...**.

**2.Navigate to System:**Go to User Configuration>Policies>Administrative Templates>System.

**3.Configure Policy:**Enable the Prevent access to registry editing tools policy.



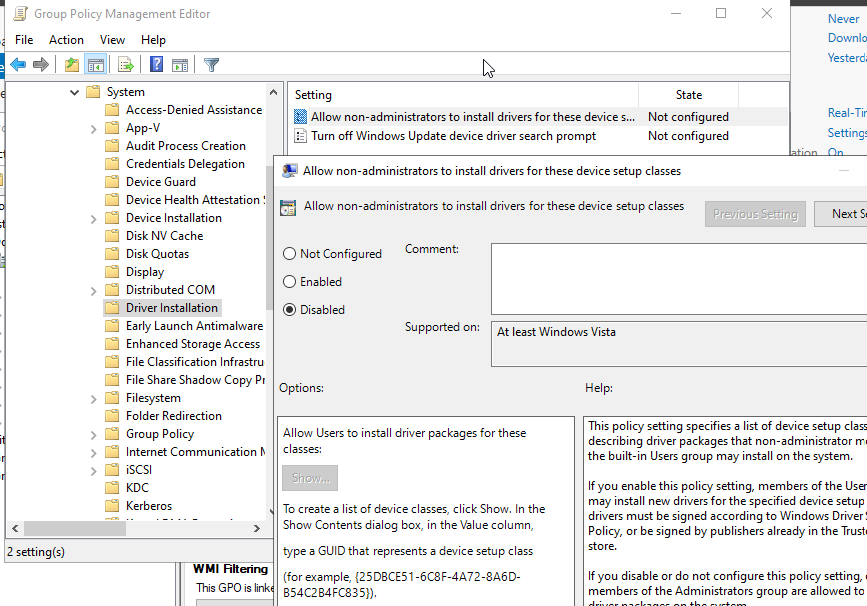
#### **3.17 Step 20:Prevent Installation of Printer Drivers**

**Action:**A GPO was configured to prevent non-administrator users from installing printer drivers.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Navigate to Driver Installation:**Go to Computer Configuration>Policies>Administrative Templates>System>Driver Installation.

**3.Configure Policy:**Disable the Allow non-administrators to install drivers for these device setup classes policy.



#### **3.18 Step 21:Restrict Time of Day Login**

**Action:**Logon hours for a specific user were configured in Active Directory to restrict login times.This is done on a per-user basis,not via GPO.

**1.Open Active Directory Users and Computers:**Find the user account.

**2.Set Logon Hours:**Right-click the user,select **Properties**,go to the **Account** tab,and click **Logon Hours...**.

#### **3.19 Step 22:Configure Windows Defender Antivirus**

**Action:**A GPO was configured to ensure Windows Defender scans network files for threats.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Navigate to Windows Defender:**Go to Computer Configuration>Policies>Administrative Templates>Windows Components>Microsoft Defender Antivirus>Scan.

**3.Configure Policy:**Enable the Scan network files policy.

#### **Scan Network Files**

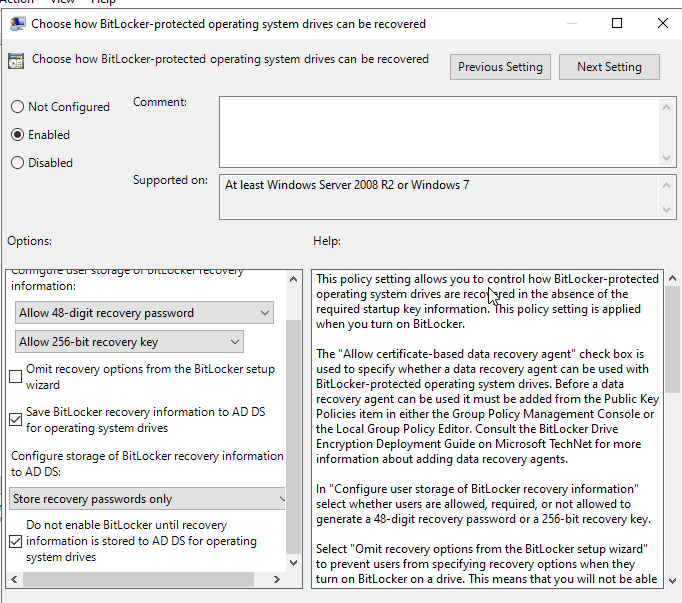
#### **3.20 Step 23:Enforce BitLocker Encryption**

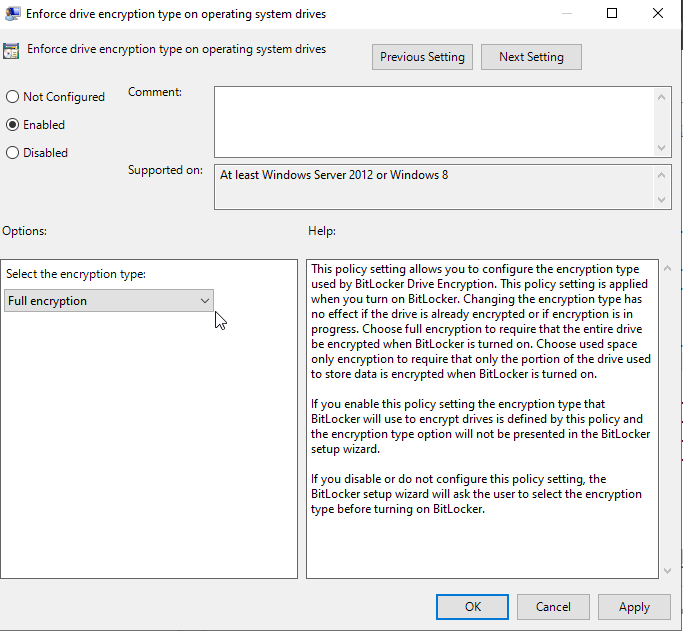
**Action:**Two GPOs were configured to enforce BitLocker on operating system drives and to back up the recovery keys to Active Directory.

**1.Edit the GPO:**Right-click a GPO linked to your computer OU and select **Edit...**.

**2.Configure Key Backup:**Go to Computer Configuration>Policies>Administrative Templates>Windows Components>BitLocker Drive Encryption>Operating System Drives.Enable the Choose how BitLocker-protected operating system drives can be recovered policy.

**3.Enforce Encryption:**In the same location,enable the Enforce drive encryption type on operating system drives policy.





### **4.0 Testing and Verification**

All configured policies were tested on the client machine to verify their functionality.The following table summarizes the test results.

#### **4.1 Test Cases and Results**

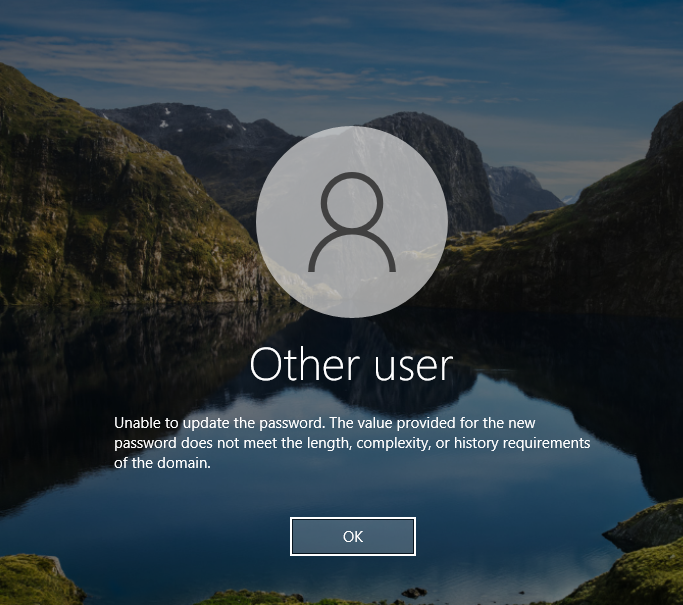
| **Policy** | **Test Action** | **Expected Result** | **Status** |
| --- | --- | --- | --- |
| **Password Policy** | **Attempted to change a user password to a simple one.** | **Password change rejected.** | **Pass** |
| **Account Lockout** | **Attempted three failed logins.** | **Account was locked out.** | **Pass** |
| **Firewall Rule(Ping)** | **Pinging 8.8.8.8 from the client.** | **Ping requests timed out.** | **Pass** |
| **Screen Saver** | **Waited for the idle timeout.** | **Screen saver activated and required a password.** | **Pass** |
| **Disallow Media Drives** | **Inserted a USB drive.** | **Access was denied.** | **Pass** |
| **Disable CMD** | **Attempted to open cmd.exe.** | **Command Prompt was blocked.** | **Pass** |
| **Disable PowerShell** | **Attempted to open powershell.exe.** | **PowerShell was blocked.** | **Pass** |
| **Disable Registry Editor** | **Attempted to open regedit.exe.** | **Registry Editor was blocked.** | **Pass** |
| **RDP Restrictions** | **Left an RDP session idle.** | **Session automatically disconnected.** | **Pass** |
| **Edge InPrivate** | **Opened Microsoft Edge.** | **The"InPrivate"option was grayed out.** | **Pass** |
| **BitLocker** | **Enabled BitLocker on the client machine.** | **Encryption started,and the recovery key was visible in Active Directory.** | **Pass** |
| **Other Policies** | **(Audit,Disable Services,etc.)** | **Checked logs and settings manually.** | **Pass** |

#### **4.2 Some Test Case Screenshots:**

**1.Password Policy Test**

**Proof:**A message showing that the new password does not meet the domain's complexity,length,or history requirements.

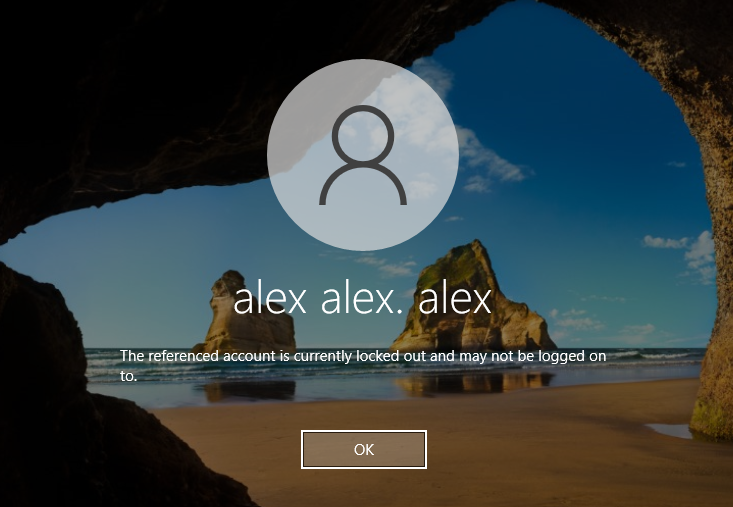
**Screenshot:**



**2.Account Lockout Test**

**Proof:**A message on the logon screen stating that the account is currently locked out.

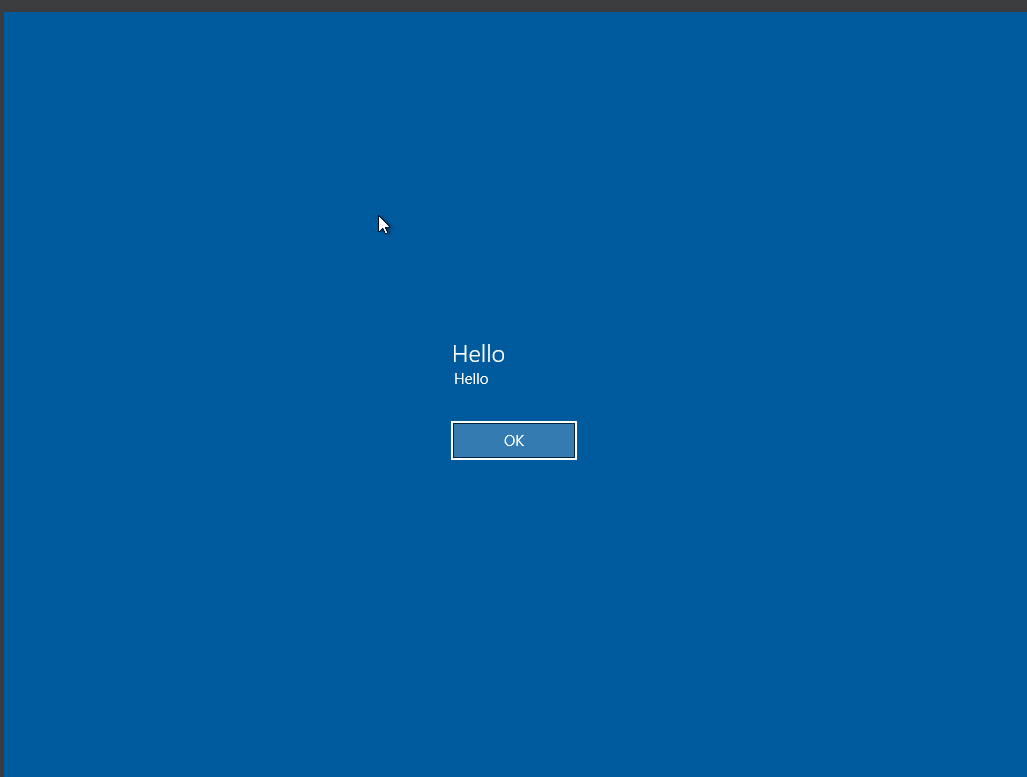
**Screenshot:**

****

**3.Logon Message Test**

**Proof:**The custom message and title configured in Group Policy appearing before the login screen.

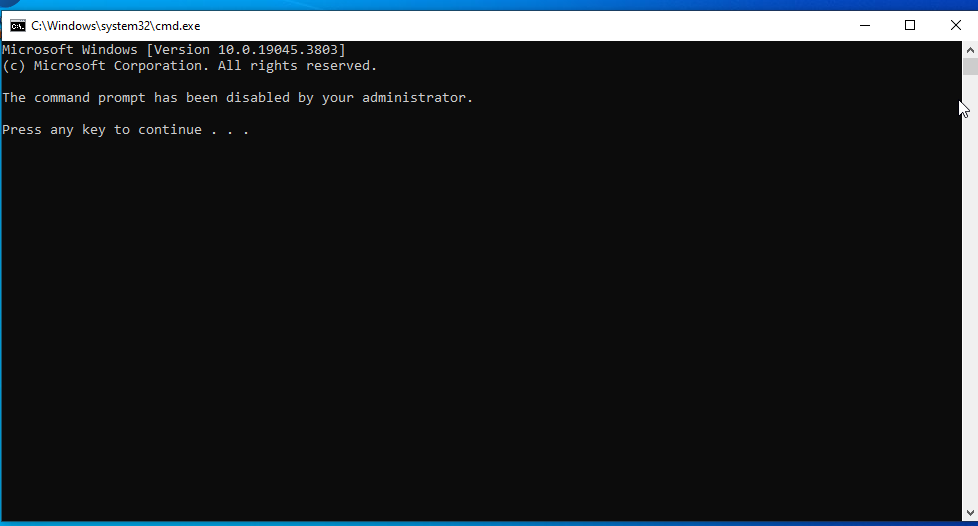
**Screenshot:**

****

**4.Disable CMD Test**

**Proof:**The Command Prompt window opening with a message that the command prompt has been disabled by your administrator.

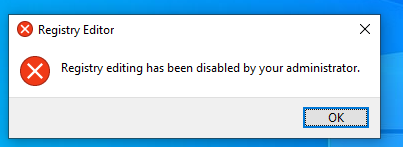
**Screenshot:**



**5.Disable Registry Editor Test**

**Proof:**A pop-up error message stating that registry editing has been disabled by the administrator.

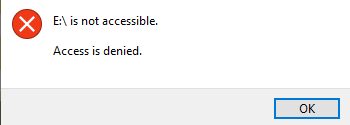
**Screenshot:**



**6.Disallow Media Drives Test**

**Proof:**A pop-up error message stating that a removable drive is not accessible and access is denied.

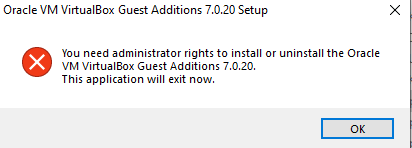
**Screenshot:**



**7.Restrict Software Installation Test**

**Proof:**A pop-up error message from the installer stating that administrator rights are needed,which a standard user cannot bypass.

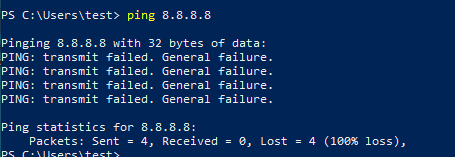
**Screenshot:**



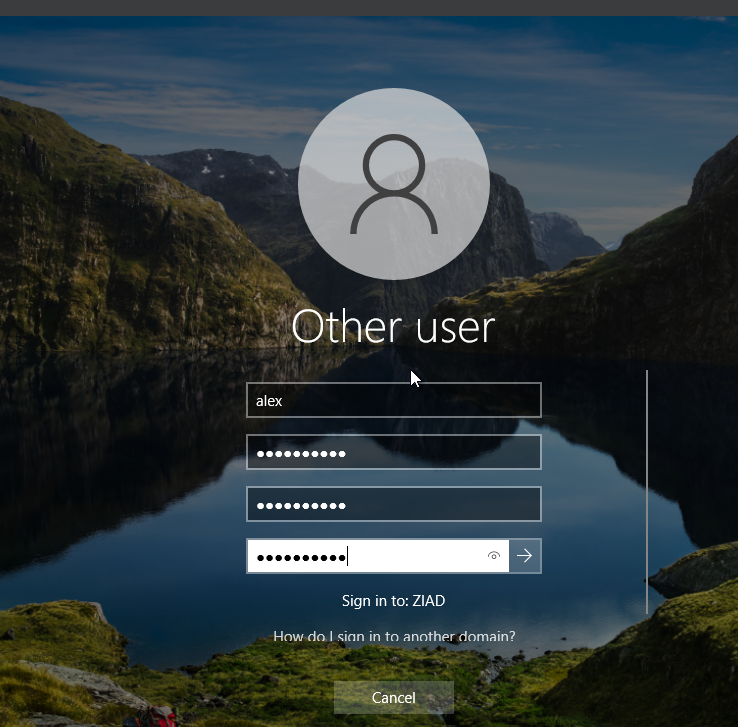
**8.Firewall Rule Test**

**Proof:**A Command Prompt window showing that ping requests to 8.8.8.8 have failed with"transmit failed"and 100%packet loss.

**Screenshot:**



9.



### **5.0 Conclusion**

The project was successfully completed,with all 23 policies configured and tested as required.The domain environment is now secured with robust account,endpoint,and network policies,demonstrating a comprehensive understanding of Windows Server administration and Group Policy management.The successful enforcement of these policies ensures a secure and compliant computing environment for all machines and users within the domain.