

Active Directory and Group Policy Management Lab Report

Environment Overview :

Domain Controller: Windows Server 2008 R2 (hostname: WINSERVER2K8.Sci.dz).

Clients: Two Windows 10 virtual machines joined to the Sci.dz domain
Hypervisor: VMware Workstation.

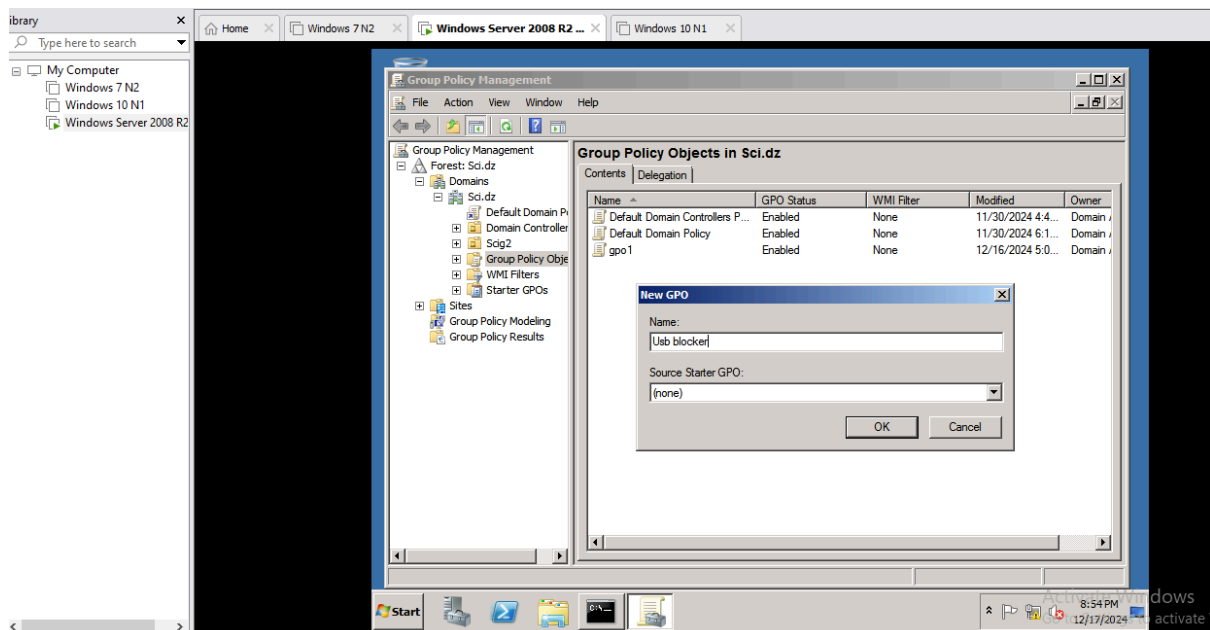
Domain: Sci.dz (Forest: Sci.dz).

Lab key focus : Policy Management.

After configuring the virtual endpoints and the server, we can apply various policies :

1. Group Policy to Block Removable Storage Access

A Group Policy Object (GPO) named “Usb blocker” was created and linked to the Sci.dz domain to enforce strict security control over removable media in order to prevent data exfiltration and internal payloads.



Configuration Path:

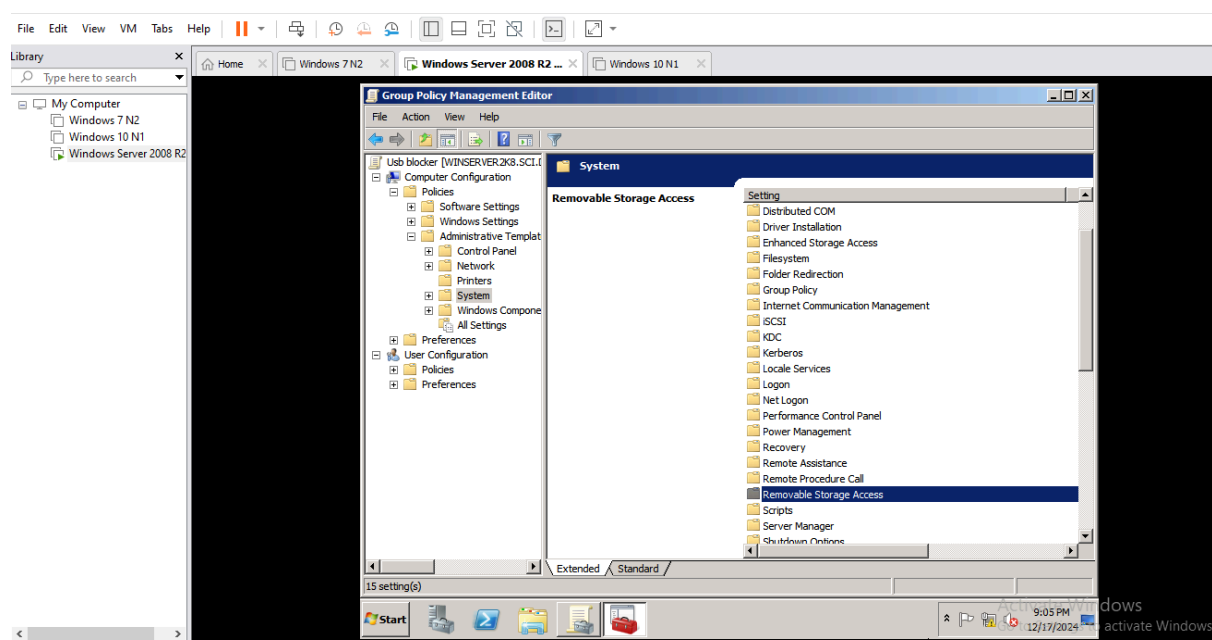
Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

Policy Applied:

All removable storage classes: Deny all access → Enabled

Effect:

All domain-joined machines are prohibited from reading from or writing to USB flash drives, external hard disks, CD/DVD drives, and other removable storage devices.

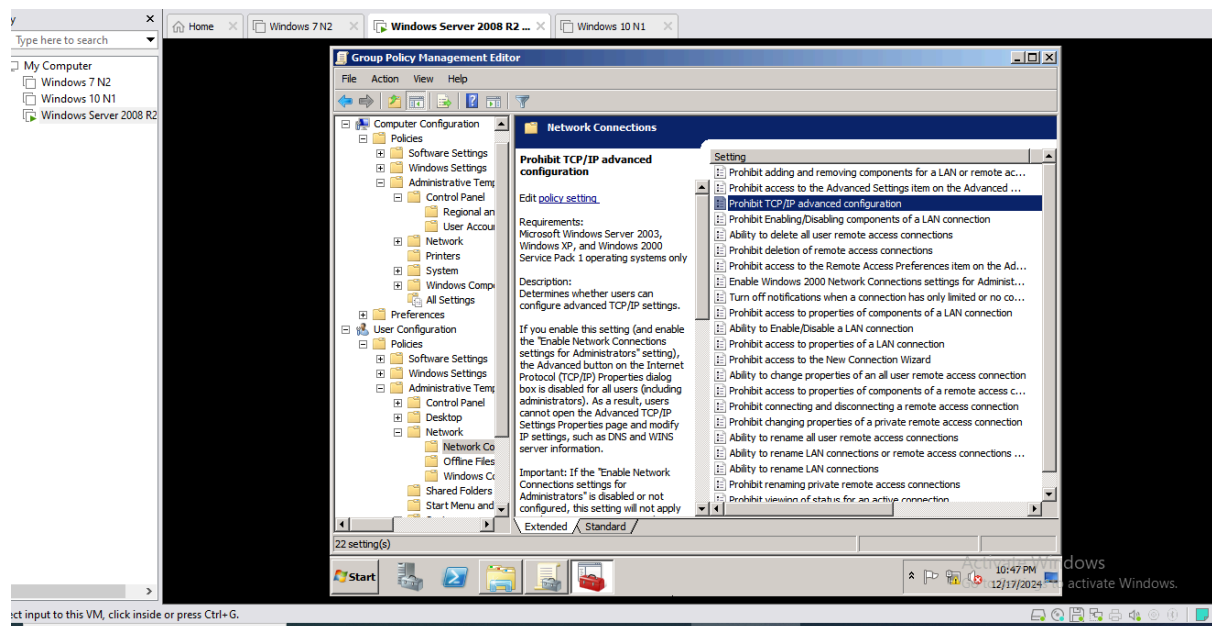


This way , external storage devices will not be granted access to our machines in the Sci.dz domain.

2. Group Policy to Restrict TCP/IP Configuration Changes

A GPO named “Tcp/IP settings block” was implemented to prevent users from modifying network settings.

Configuration Path: User Configuration → Policies → Administrative Templates → Network → Network Connections

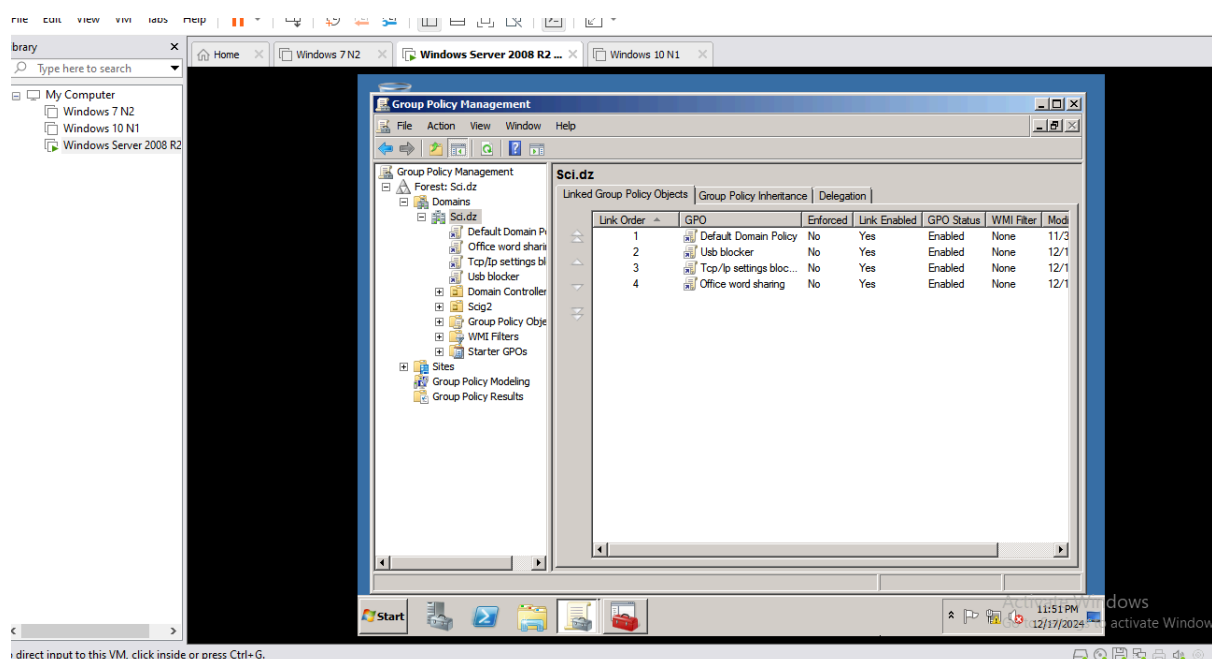


Policy Applied:

Prohibit TCP/IP advanced configuration → Enabled

Effect:

The Advanced button in the Internet Protocol Version 4 (TCP/IPv4) Properties dialog is disabled for all users (including administrators, when the companion “Enable Network Connections settings for Administrators” policy is disabled). This prevents modification of DNS, WINS, gateway, and other advanced IP settings.



3. Group Policy for Automated Microsoft Office Deployment

A GPO named “Office word sharing” was configured to automatically deploy Microsoft Office to all domain-joined workstations.

Steps Performed:

Downloaded the Microsoft Office installer (.exe format) on the domain controller.

Converted the .exe file to .msi format using a third-party packaging tool (I chose MSI Wrapper) to comply with Group Policy software installation requirements.

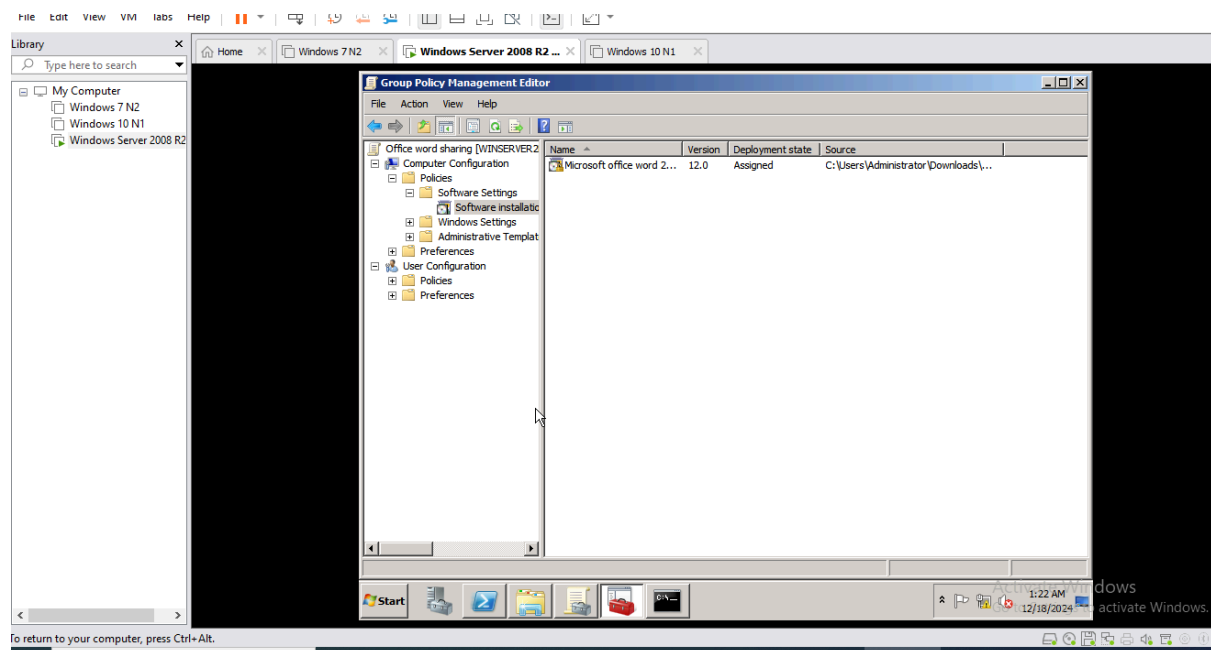
In Group Policy Editor, navigated to:

Computer Configuration → Policies → Software Settings → Software Installation

Right-clicked → New → Package, then selected the .msi file path.

Set deployment method to Assigned.

Linked the GPO to the Sci.dz domain.



Note :

It is essential to use command `gpupdate /force` in powershell after every modification in order to ensure a fast and reliable update to the group policy.

Policy Linking and Enforcement:

All GPOs were explicitly linked to the Sci.dz domain to ensure domain-wide application. The final GPO link order was:

Default Domain Policy :

Usb blocker : increase endpoint physical security and decrease internal threats.

Tcp/Ip settings block : improve network security

Office word sharing : automate software deployment for employees

Group Policy inheritance was verified using the Group Policy Management Console (GPMC).

Many additional policies can be made, including password policies such as length.

These policies can be explored and applied through their specific directories .