

Lab Assignment 2 (Part II) - GPO

Lab Objective

This lab is designed to **configure and test advanced Group Policy Objects (GPOs)** in a domain environment. Students will work with Administrative Templates, security policies, folder redirection, software installation, and scripts.

The lab will focus on implementing these configurations, linking them to appropriate OUs, and verifying their impact.

Lab Environment Requirements

- **DC1XX:** Domain Controller with Active Directory, DNS, and Group Policy Management installed.
 - **ClientXX:** Windows 11 client machine joined the domain.
 - **DC3XX:** File Server for folder sharing.
-

Tasks

Task 1: Creating a Central Store for Administrative Templates

- Create a **central store** for Administrative Templates on **DC1XX**.
 - Copy all **ADMX** and **ADML** files to this Central store.
 - Verify that **Group Policy Management Console (GPMC)** loads templates from the **central store**.
-

Task 2: Managing and Configuring Administrative Templates

- Download and install **Microsoft Office Administrative Templates** (*You will need to **add the NAT NIC** to download this package. Remove it after completing the download*).
- Create a new GPO named **RestrictTeamsStarting**.
- Use **Filter Options** for **User Configuration** to locate **Microsoft Teams settings**.
- Enable **Prevent Microsoft Teams from starting automatically after installation**.

- Add a **comment** to document this setting.
 - Link to **Engineering OU** (*to be tested in **Task 8 Managing Software Installation** task*).
 - Run **gpupdate /force** to apply changes.
-

Task 3: Managing Account Policies

- Modify **password policies** in the **Default Domain Policy** GPO:
 - Minimum password length: **12 characters**.
 - Password complexity: **Enabled**.
 - Password expiration: **60 days**.
 - Apply **Account Lockout Policy**:
 - Lock account after **2 failed login attempts**.
 - Lockout duration: **2 minutes**.
 - Run **gpupdate /force** to apply changes.
 - From **ClientXX**, test with **Emma Petit** by attempting password modification and simulating an account lockout.
-

Task 4: Implementing Fine-Grained Password Policies

- Create a new **Fine-Grained Password** Policy named **IT_FGPPolicy**.
- Modify password settings:
 - Minimum password length: **10 characters**.
 - Password complexity: **Disabled**.
 - Password expiration: **Never**.
- Directly apply it to the **IT Group**.
- Run **gpupdate /force** to apply changes.
- From **ClientXX**, test with a **user from the IT group** by attempting password modification.

Task 5: Managing Audit Authentication

- Modify **Default Domain Policy GPO** to enable **Audit Logon Events (Success and Failure)**.
 - Restart the **ClientXX**
 - Test by failing and successfully logging in with any user on **ClientXX**.
 - Open **Event Viewer** on **DC1XX** and verify **Security Logs**.
-

Task 6: Managing Security Templates

- Create a security template named **OpenSSH_Auth**.
 - In this template, modify **OpenSSH Authentication Agent** under **System Services** to start **automatically**.
 - Import this **new template** into a new GPO named **OpenSSHAAuth**.
 - Link the GPO to **DomainControllers OU**.
 - Run **gpupdate /force** on **DC1XX** to apply changes.
 - Restart **DC1XX** and verify in **Services** that **OpenSSH Authentication Agent** has started.
-

Task 7: Configuring Folder Redirection

- Use **DC3XX** as the file server.
 - Create a shared folder: **\\DC3XX\UserData** to the **HR** Group (r & w).
 - Create a new **GPO** named **SharedUserData**
 - Use **Basic redirection** to **Create a Folder for Each User Under the Root Path**.
 - Redirect **Documents** and **Desktop** to the user's respective folder under **\\DC3XX\UserData**.
 - Link GPO to **HR OU**,
 - Run **gpupdate /force** to apply changes.
 - Test with **a user** from the **HR OU**.
-

Task 8: Managing Software Installation

- Create a network share: **\\DC3XX\Software**.
 - Download the **Microsoft Teams MSI package** *(You will need to **add the NAT NIC** to download this package. Remove it after completing the download).*
<https://learn.microsoft.com/en-us/microsoftteams/msi-deployment#msi-files>
 - Create a new GPO named **DC3XX_Teams_Installation**.
 - Assign the **Teams MSI package** installation to the **Engineering OU**.
 - Run **gpupdate /force** to apply changes.
 - Restart **ClientX**, log in with a user from **Engineering OU**, and verify that Microsoft Teams is installed.
 - Confirm that Teams do **not** start automatically after installation (to test GPO **RestrictTeamsStarting**, created in Task 2).
-

Task 9: Managing Scripts with GPO

- Create a shared folder on **\\DC3XX\Public** and share it with **Everyone (read and write)**.
 - Create a **logon script (MapDrive.bat)** to map this shared network drive. Add this text in this file: **net use Z: \\DC3XX\Public**
 - Store the script in **\\DC1XX\NETLOGON**.
 - Create a new GPO named **Public_Share**.
 - Add this new logon script to **User Configuration Scripts → Logon**.
 - Link GPO to the **Domain**.
 - Run **gpupdate /force** to apply changes.
 - Test with any by logging into **ClientX** and verifying the drive mapping.
 - Try to create files and folders in this drive.
-

Lab Assignment Deliverables

You should submit a **lab report** in **PDF** including **screenshots** covering your work.