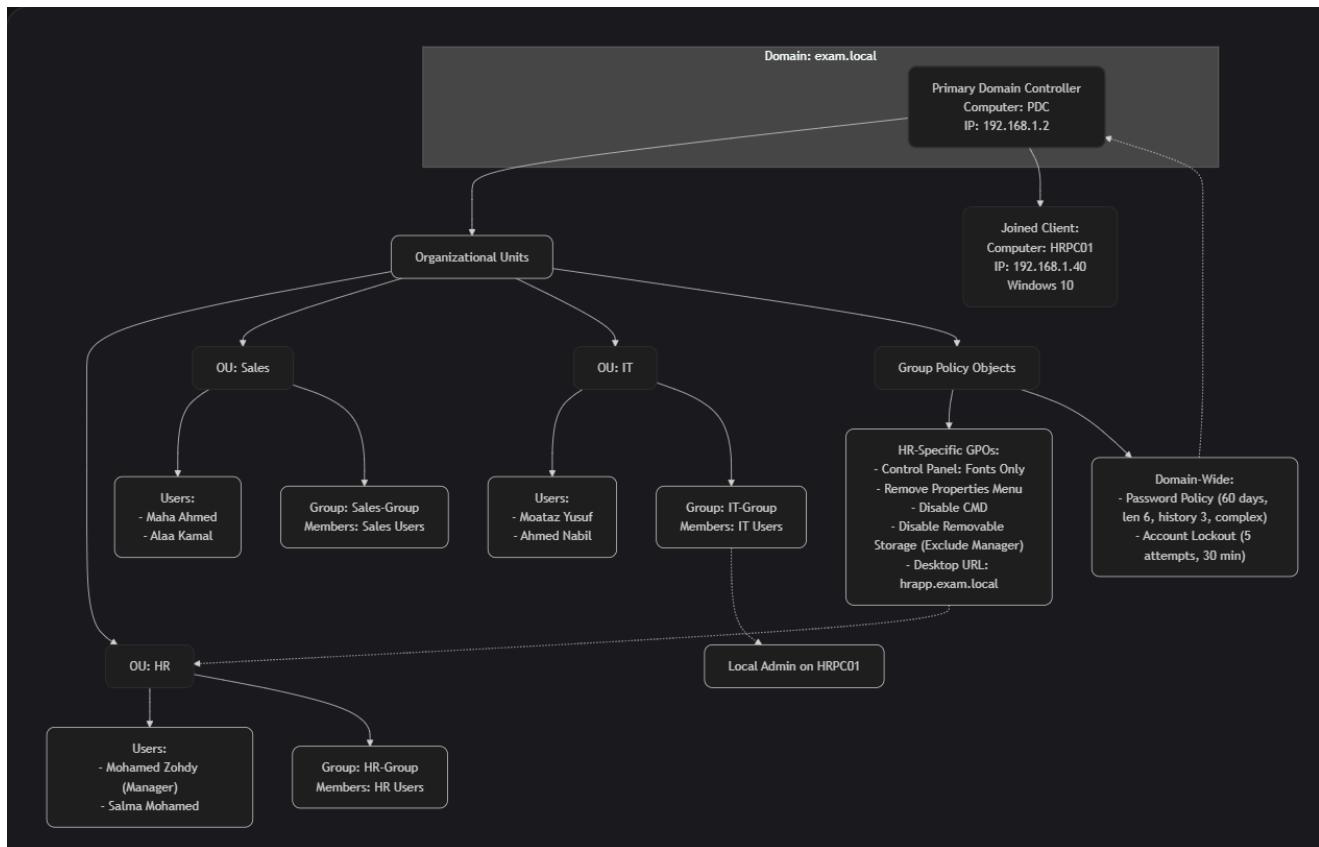


Windows Domain Environment Setup Documentation (Project 1)

The project Task

- Create a domain environment with domain name (exam.local) on a server with the following :
 - Computer name : PDC
 - IP Address : 192.168.1.2
- Create separate OU for each department (HR, Sales, IT)
- Create 2 users in each department.
 - HR : Mohamed Zohdy , Salma Mohamed
 - Sales : Maha Ahmed , Alaa Kamal
 - IT : Moataz Yusuf , Ahmed Nabil
- Create separate groups for each department and add users to the department group.
- Join windows 10 machine with computer name (HRPC01) and IP Address (192.168.1.40)
- Add domain group IT-Group as a Local Administrator
- Show only fonts in Control panel for HR.
- Remove properties from This PC context menu.
- Disable Command Line for HR.
- Disable External Storage for HR Users and exclude the HR manager user account (Mohamed Zohdy)
- Configure password policy must change every 60 days, minimum length 6 digits with complex password and remember last 3 password.
- Force account lock for 30 min after entering wrong password 5 times.
- Create HR URL for all HR Users on their desktop (hrapp.exam.local).

The project Diagram



Project Overview

This documentation outlines the setup of a Windows domain environment for a fictional organization named "Exam". The domain is configured on a server acting as the Primary Domain Controller (PDC) with specific IP addressing, organizational units (OUs), users, groups, and a joined client machine. Additionally, Group Policy Objects (GPOs) are applied to enforce security policies, restrictions, and customizations, particularly targeting the HR department for compliance and access control.

The project simulates a small enterprise network with departments (HR, Sales, IT), user management, and policy enforcement using Active Directory Domain Services (AD DS). All configurations are performed on Windows Server (assumed version 2019 or 2022) and Windows 10 client.

Objectives

- Establish a domain for centralized user and resource management.
- Organize users and groups by department.
- Join a client machine to the domain.
- Apply targeted policies for security, access restrictions, and user experience customizations.

Assumptions and Prerequisites

- Hardware: One server machine for PDC, one Windows 10 client machine.

- Software: Windows Server with AD DS role installed; Windows 10 Pro/Enterprise for domain join.
- Network: Static IP assignments; basic LAN connectivity.
- Administrator access on all machines.
- No production environment; this is for testing/educational purposes.

Step-by-Step Configuration

1. Create Domain Environment

Goal: Set up the domain "exam.local" on the server.

- Install Windows Server on the machine.
- Assign static IP: 192.168.1.2 (subnet mask 255.255.255.0, gateway/DNS as needed).
- Set computer name to "PDC" via System Properties > Computer Name > Change.
- Install Active Directory Domain Services role:
 - Open Server Manager > Add Roles and Features > Select "Active Directory Domain Services".
 - Promote to Domain Controller: Run dcpromo or use Server Manager > Promote this server to a domain controller > Add a new forest > Root domain name: exam.local.
- Complete the wizard, set DSRM password, and reboot.
- Verify: Open Active Directory Users and Computers (dsa.msc) to see the domain.

2. Create Organizational Units (OUs)

Goal: Create separate OUs for departments to organize objects and apply targeted policies.

- Open Active Directory Users and Computers (dsa.msc).
- Right-click the domain (exam.local) > New > Organizational Unit.
- Create OUs:
 - Name: HR
 - Name: Sales
 - Name: IT
- Verify OUs appear under the domain root.

3. Create Users

Goal: Add two users per department in their respective OUs.

- In dsa.msc, navigate to each OU.
- Right-click OU > New > User.
- Configure users (first name, last name, user logon name as [firstname.lastname@exam.local], set initial password, enable "User must change password at next logon"):
 - HR OU:

- Mohamed Zohdy (HR Manager)
- Salma Mohamed
- Sales OU:
 - Maha Ahmed
 - Alaa Kamal
- IT OU:
 - Moataz Yusuf
 - Ahmed Nabil
- Verify users in their OUs.

4. Create Groups and Add Users

Goal: Create department-specific groups and add users for role-based access.

- In dsa.msc, right-click domain or appropriate OU > New > Group.
- Create Domain Local or Global Security groups:
 - HR-Group
 - Sales-Group
 - IT-Group
- For each group:
 - Right-click group > Properties > Members tab > Add > Select users from the same department.
- Add users:
 - HR-Group: Mohamed Zohdy, Salma Mohamed
 - Sales-Group: Maha Ahmed, Alaa Kamal
 - IT-Group: Moataz Yusuf, Ahmed Nabil
- Verify membership.

5. Join Windows 10 Machine to Domain

Goal: Join client machine HRPC01 to the domain.

- On the Windows 10 machine:
 - Assign static IP: 192.168.1.40 (subnet 255.255.255.0, DNS: 192.168.1.2).
 - Set computer name to HRPC01 via System > About > Rename this PC.
 - Join domain: System > About > Join a domain > Enter "exam.local" > Provide domain admin credentials.
- Reboot and log in with domain user.
- Verify: Command Prompt > whoami shows domain\username.

6. Add Domain Group as Local Administrator

Goal: Grant IT-Group local admin rights on HRPC01.

- On HRPC01, open Computer Management (compmgmt.msc) or lusrmgr.msc.
- Navigate to Local Users and Groups > Groups > Administrators > Add.
- Add "exam\IT-Group".
- Verify: Members list shows the group.

7. Show Only Fonts in Control Panel for HR

Goal: Restrict Control Panel to show only Fonts applet for HR users via GPO.

- Open Group Policy Management (gpmc.msc) on PDC.
- Create new GPO: Right-click HR OU > Create a GPO in this domain, and Link it here > Name: HR-ControlPanel-Restrict.
- Edit GPO: User Configuration > Policies > Administrative Templates > Control Panel > Show only specified Control Panel items > Enable > Add "Microsoft.Fonts" (canonical name for Fonts).
- Link to HR OU.
- Apply: On client, run gpupdate /force.
- Verify: Log in as HR user; Control Panel shows only Fonts.

8. Remove Properties from This PC Context Menu

Goal: Hide "Properties" option from This PC right-click menu via GPO.

- In gpmc.msc, create/edit GPO linked to HR OU (e.g., HR-ContextMenu).
- User Configuration > Policies > Administrative Templates > Windows Components > File Explorer > Remove "Properties" from the Computer context menu > Enable.
- Apply gpupdate /force.
- Verify: Right-click This PC; no Properties option.

9. Disable Command Line for HR

Goal: Prevent HR users from accessing Command Prompt via GPO.

- In gpmc.msc, create/edit GPO for HR OU (e.g., HR-DisableCMD).
- User Configuration > Policies > Administrative Templates > System > Prevent access to the command prompt > Enable > Set "Disable command prompt script processing" to Yes.
- Apply gpupdate /force.
- Verify: HR user tries to run cmd.exe; access denied.

10. Disable External Storage for HR Users (Exclude HR Manager)

Goal: Block removable storage for HR users except Mohamed Zohdy via GPO.

- In gpmc.msc, create GPO: HR-RemovableStorage-Disable, link to HR OU.

- User Configuration > Policies > Administrative Templates > System > Removable Storage Access > All Removable Storage classes: Deny all access > Enable.
- To exclude HR Manager: Edit GPO > Delegation tab > Advanced > Add "exam\Mohamed Zohdy" > Deny "Apply Group Policy".
- Apply gpupdate /force.
- Verify: HR users (except Zohdy) can't access USB drives; Zohdy can.

11. Configure Password Policy

Goal: Set domain-wide password requirements.

- In gpmc.msc, edit Default Domain Policy (linked to domain root).
- Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy:
 - Maximum password age: 60 days
 - Minimum password length: 6 characters
 - Enforce password history: 3 passwords remembered
 - Password must meet complexity requirements: Enable
- Apply gpupdate /force.
- Verify: Attempt to set simple/short password; fails.

12. Force Account Lockout

Goal: Lock accounts after 5 failed logons for 30 minutes.

- In Default Domain Policy > Account Policies > Account Lockout Policy:
 - Account lockout threshold: 5 invalid logon attempts
 - Account lockout duration: 30 minutes
 - Reset account lockout counter after: 30 minutes (optional, but recommended).
- Apply gpupdate /force.
- Verify: Simulate 5 bad logons; account locks for 30 min.

13. Create HR URL on Desktop for HR Users

Goal: Place a shortcut to hrapp.exam.local on HR desktops via GPO.

- In gpmc.msc, create GPO: HR-DesktopShortcut, link to HR OU.
- User Configuration > Preferences > Windows Settings > Shortcuts > New > Shortcut:
 - Action: Create
 - Name: HR App
 - Target type: URL
 - Target URL: [http://hrapp.exam.local] (or https if applicable)
 - Location: All Users Desktop
- Apply gpupdate /force.

- Verify: Log in as HR user; shortcut appears on desktop.

Testing and Verification

- Log in as various users on HRPC01 to test restrictions.
- Use Event Viewer to monitor policy applications (e.g., Event ID 5136 for directory changes).
- Run gpresult /r on client to verify applied GPOs.

Potential Issues and Troubleshooting

- GPO not applying: Check linking, security filtering, WMI filters; run gpupdate /force.
- Domain join fails: Verify DN
- S resolution to PDC.
- Policy conflicts: Ensure no overriding GPOs at higher levels.