



Windows Server: A Home Lab Guide to Active Directory, GPO, and Network File Sharing”

Hardware Requirements:

- **VMware Workstation Pro** - 1.2 GB Disk Space and 64-bit OS
- **Windows Server 2022**- 2GB Memory, 20GB Disk Space
- **Windows 10 Pro** - 2GB Memory, 20GB Disk Space (minimum)

Lab Setup

1. Set Up a Virtual Lab Environment:

- o Use virtualization software like **VMware Workstation**, **Hyper-V**, or **VirtualBox**.
- o Install **Windows Server** (preferably Windows Server 2019 or later) and configure it as a domain controller.
- o Install a couple of **Windows client machines** (e.g., Windows 10 or Windows 11 Enterprise or Pro) and join them to the domain.

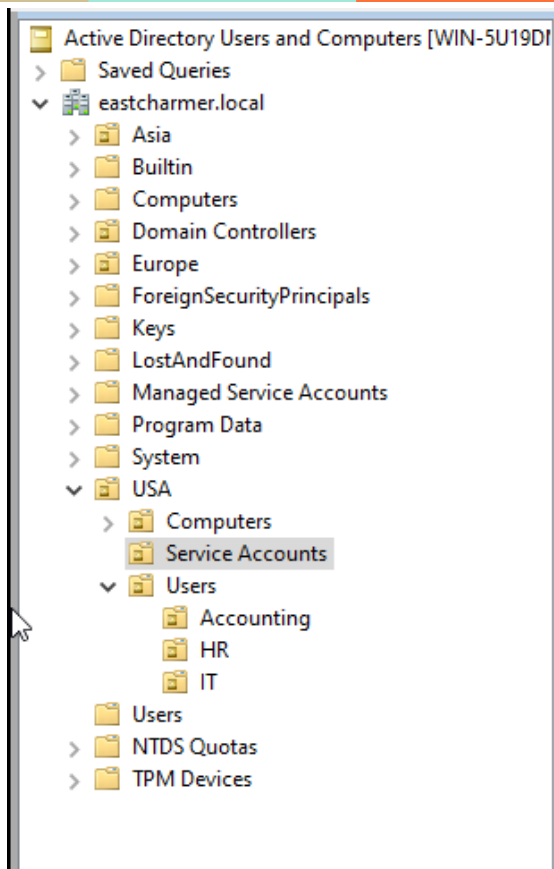
Hands-On Activities

1. Rename the server hostname

2. Install Active Directory Tools and Promote as DC

3. Creating Organizational Units (OUs)



- **Objective:** Organize the directory structure.
- 1. Open **Active Directory Users and Computers (ADUC)**.
- 2. Create OUs for Different Geographical Locations (e.g., **USA**, **Europe**, **Asia**)
 - Right-click the domain name and select **New > Organizational Unit**.
- 3. Create a nested OU inside the locations (e.g., **USA > Computers**, **Users**, **Service Accounts**)
- 4. Create a nested OU inside Computers (e.g., **IT > Servers**)
- 5. Create a nested OU inside Users (e.g., **Accounting**, **HR**, **IT**).



6.

2. Creating User Accounts




- **Objective:** Create user accounts with specific attributes.
1. Navigate to the appropriate OU (e.g., **HR**).
 2. Right-click the OU and select **New > User**.
 3. Fill in the user details:
 - First Name: John
 - Last Name: Doe
 - User Logon Name: jdoe
 4. Set a password and configure the account settings (e.g., password never expires).
 5. Set a Description for John Doe (e.g., **Recruiter**)
 6. Create more users for IT and Accounting OU following the steps above

Name	Type	Description
 John Doe	User	Recruiter
 Lacus Clyne	User	Senior HR Staff



3. Creating Groups

- **Objective:** Create security and distribution groups.
1. Navigate to an OU (e.g., **HR**).
 2. Right-click the OU and select **New > Group**.
 3. Name the group (e.g., **#HR_Department**).
 4. Select the group scope (e.g., Global) and type (e.g., Security).

Name	Type	Description
 John Doe	User	Recruiter
 Lacus Clyne	User	Senior HR Staff
 #HR_Department	Security Group...	

4. Adding Users to Groups

- **Objective:** Manage group memberships.
1. Open the properties of a user account (e.g., **jdoe**).
 2. Go to the **Member Of** tab.
 3. Click **Add** and select the group (e.g., **#HR_Department**).
 4. Verify the membership.
 5. Do the same for another user in the **HR** OU
 6. Add user in the OU **IT** to Domain Admins Group

5. Configure Network settings for the Server

1. Change the domain controller's IP address to static IP
2. Change DNS Servers to loopback and google DNS

6. Join Windows Client to the Domain

1. Change the DNS server of the computer to the DC IP and google DNS
2. Join the computer to the domain and move the computer to the appropriate OU
3. Login with the user created in Active Directory (e.g., **John Doe**)

7. Creating and Linking Group Policy Objects (GPOs)

- **Objective:** Create and link policies to OUs.
1. Open **Group Policy Management Console (GPMC)**.
 2. Right-click the domain or an OU and select **Create a GPO in this domain, and Link it here**.
 3. Name the GPO (e.g., **Password Policy**).
 4. Edit the GPO and configure settings (e.g., minimum password length, password complexity).
 5. Link the GPO to the desired OU.



6. Create more GPO to Restrict Control Panel Access, Block USB Drives and Set a default desktop wallpaper for all users

8. Configuring File Sharing and Permissions

- **Objective:** Set up file sharing within the AD environment
1. Create a network share (e.g., `\\ServerName\SHARED`). Create a folder named "SHARED" on the C: drive.
 2. Set Folder Properties
 - Right-click the folder and select "Properties."
 - Go to the "Sharing" tab
 3. Share the Folder
 - Click "Advanced Sharing."
 - Check "Share this folder" and provide a share name (e.g., "SharedFiles").
 - Click "Permissions" and set the share permissions (e.g., "Everyone" with "Read" access).
 4. Set NTFS Permissions
 - Go to the Security Tab. In the folder properties, go to the "Security" tab.
 - Edit Permissions
 - ❖ Click "Edit" to modify the NTFS permissions.
 - ❖ Add the appropriate users or groups and assign the necessary permissions (e.g., "Read & Execute," "Modify," etc.).

9. Map Network Drives via Group Policy

1. **Open Group Policy Management**
 - a. On the domain controller, open the Group Policy Management Console (GPMC).
2. **Create a GPO**
 - a. Create a new GPO (e.g., `Mapped Drive`).
3. **Configure Drive Mapping**
 - a. Navigate to User Configuration -> Preferences -> Windows Settings -> Drive Maps.
 - b. Right-click and select "New" -> "Mapped Drive."
 - c. Set the location (e.g., `\\ServerName\SHARED`) and choose a drive letter.
 - d. Configure additional settings as needed (e.g., "Reconnect," "Label as," etc.).
4. **Link the GPO**
 - Link the GPO to the appropriate Organizational Unit (OU) that contains the users who need access to the shared folder.
5. **Update Group Policy**
 - On the client computers, update the group policy by running `gpupdate /force` in the command prompt or simply restart the computers.



10. Creating Service Accounts

- **Objective:** Create and configure a service account.
- 1. Navigate to the appropriate OU (e.g., **Service Accounts**).
- 2. Right-click the OU and select **New > User**.
- 3. Fill in the service account details (e.g., **\$Autologin**) for name and set a Description.
- 4. Set a strong password and configure the account settings (e.g., password never expires, cannot change password).
- 5. Assign the necessary permissions to the service account on the relevant resources.
- 6. Set up with a client machine using Windows Autologon tool (sysinternals)

11. Configuring Account Lockout Policy

- **Objective:** Set up account lockout policies to enhance security.
- 1. Open **GPMC** and create a new GPO (e.g., **Account Lockout Policy**).
- 2. Edit the GPO:
 - Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**.
 - Configure the settings (e.g., Account lockout threshold, Account lockout duration, Reset account lockout counter after).
- 3. Link the GPO to the desired OU.

Testing and Verification

1. **Verify User Logon:** Log on to a client machine using one of the newly created user accounts.
2. **Check Group Membership:**
 - Open a Command Prompt and run **gpresult /r** to verify applied policies and group memberships.
3. **Test GPOs:**
 - Log on to a client machine with a user account that has GPOs configured and verify that the GPOs were applied.
4. **Test Network Drives:**
 - Log on to a client machine with a user account that has Drive Mapping GPO configured and verify that they can access the network folder.