Setting Up Your Active Directory Lab Environment: Detailed Guide

Step 1: Virtual Machine Setup for Domain Controller

Launch Hyper-V Manager

1. Open Start menu and search for "Hyper-V Manager"
2. Click to open the management console

Create a Virtual Switch

1. Select "Virtual Switch Manager" from the Actions panel
2. Click "New virtual network switch"
3. Choose "External" and click "Create Virtual Switch"
4. Name it "External Network" and select your physical network adapter
5. Click "Apply"
6. Create a second switch, choose "Internal" type
7. Name it "Domain Network" and click "OK"

Create the Domain Controller VM

1. Click "New" → "Virtual Machine" in the Actions panel
2. Name your VM "DC01" and choose to store it on your NVMe SSD
3. Select "Generation 2" for better performance
4. Allocate RAM:
    - Set 4GB (4096MB)
    - Check "Use Dynamic Memory" to optimize your host's RAM usage
5. Configure Networking:
    - For the first connection, select your "External Network" switch
6. Create Virtual Hard Disk:
    - Location: Your NVMe SSD
    - Size: 60GB (plenty for a DC with room for growth)
7. Installation Options:
    - Select "Install an operating system from a bootable image file"
    - Browse to your Windows Server ISO file

8. Click "Finish" to create the VM

Configure VM Settings

1. Right-click the newly created VM and select "Settings"
2. Under Processor, set 2 virtual processors (your i7-10510U has 4 cores/8 threads)
3. Add a second network adapter:
    - Click "Add Hardware"
    - Select "Network Adapter"
    - Connect it to your "Domain Network" switch
4. Under "Firmware," ensure your boot order is:
    - DVD Drive
    - Hard Drive
    - Network Adapter
5. Click "OK" to apply settings

Step 2: Windows Server Installation

Start the Installation

1. Right-click the VM and select "Connect"
2. Click "Start" in the VM console
3. The VM will boot from the ISO into Windows Setup
4. Select your language and keyboard layout, click "Next"
5. Click "Install now"

Operating System Selection

1. Select "Windows Server 2022 Standard (Desktop Experience)"
    - The Desktop Experience includes GUI management tools
2. Accept the license terms
3. Choose "Custom: Install Windows only"
4. Select the 60GB drive and click "Next"
5. Wait for installation to complete (15-20 minutes on your NVMe SSD)

Initial Configuration

1. When prompted, set a strong administrator password
2. Press Ctrl+Alt+Delete (in Hyper-V, use the "Action" menu or Ctrl+Alt+End)
3. Log in with your administrator credentials
4. When Server Manager opens, close any initial setup wizards

Step 3: Configure Network Settings

Identify Network Adapters

1. Right-click Start and select "Network Connections"
2. Identify which adapter connects to the internet (External) and which is for your domain network (Internal)
   - You can rename them for clarity (e.g., "External" and "Domain")

Configure Domain Network Adapter

1. Right-click on the Domain adapter and select "Properties"
2. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties"
3. Select "Use the following IP address"
4. Enter:
   - IP address: 192.168.1.10
   - Subnet mask: 255.255.255.0
   - Default gateway: (leave blank)
   - Preferred DNS server: 127.0.0.1 (this will be replaced with your own DNS once it's set up)
5. Click "OK" to apply settings

Configure External Network Adapter

1. Right-click the External adapter and select "Properties"
2. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties"
3. Keep "Obtain an IP address automatically" selected if your home network has DHCP
4. Click "OK"

Step 4: Configure Server Identity

Rename the Server

1. Open Server Manager if not already open
2. Click "Local Server" in the left navigation
3. Click on the current computer name (to the right of "Computer name")
4. In the System Properties dialog, click "Change"
5. Enter "DC01" as the computer name
6. Click "OK" and "OK" again
7. Restart when prompted

Step 5: Install Windows Updates

Update the Server

1. After restart, log back in
2. Press Win+I to open Settings
3. Go to Update & Security → Windows Update
4. Click "Check for updates"
5. Download and install all available updates
6. Restart if required
7. Repeat until no more updates are available

Step 6: Install Active Directory Domain Services

Add the AD DS Role

1. Open Server Manager
2. Click "Manage" in the top-right, then "Add Roles and Features"
3. Click "Next" until you reach "Server Roles"
4. Check "Active Directory Domain Services"
5. When prompted to add required features, click "Add Features"
6. Click "Next" until you reach "Confirmation"
7. Check "Restart the destination server automatically if required"
8. Click "Install"
9. Wait for installation to complete

Step 7: Promote Server to Domain Controller

Configure Active Directory

1. After installation completes, click the notification flag in Server Manager
2. Click "Promote this server to a domain controller"
3. Select "Add a new forest"
4. Enter your root domain name: "contoso.local" (or your preferred name)
5. Click "Next"
6. On the Domain Controller Options screen:
   - Forest functional level: Windows Server 2016 (for compatibility)
   - Domain functional level: Windows Server 2016
   - Ensure "Domain Name System (DNS) server" is checked
   - Ensure "Global Catalog (GC)" is checked
   - Enter and confirm a Directory Services Restore Mode (DSRM) password
7. Click "Next"

DNS Delegation

1. You'll likely see a warning about DNS delegation - this is normal for a lab
2. Click "Next"

Additional Options

1. Verify the NetBIOS domain name (should be "CONTOSO" if your domain is contoso.local)
2. Click "Next"

Paths

1. Keep the default paths for the database, log files, and SYSVOL
   - These will be stored on your VM's virtual hard disk on the NVMe SSD
2. Click "Next"

Review and Install

1. Review your selections
2. Click "Next"
3. The prerequisite check will run - resolve any critical issues

4. Click "Install"
5. The server will automatically restart after AD DS installation

Step 8: Verification

Verify Active Directory Installation

1. After restart, log in with your administrator credentials
2. Open Server Manager
3. Click "Tools" → "Active Directory Users and Computers"
4. Verify that your domain (contoso.local) appears in the left pane
5. Expand it to see default containers (Users, Computers, etc.)
6. Open "Server Manager" → "Tools" → "DNS"
7. Expand your server and verify that forward and reverse lookup zones exist

Step 2: Creating Domain Structure and Objects in Active Directory - Detailed Guide

Organizational Unit (OU) Structure

Opening Active Directory Users and Computers

1. Log into your Domain Controller server with administrator privileges
2. Open Server Manager by clicking on the Server Manager icon in the taskbar or from the Start menu
3. From Server Manager, click on "Tools" in the top-right corner
4. Select "Active Directory Users and Computers" from the dropdown menu
    - Alternatively, you can press Win+R, type "dsa.msc" and press Enter

Creating the Base OU Structure

1. In the Active Directory Users and Computers console, locate your domain name in the left navigation pane
2. Right-click on your domain name (e.g., contoso.local) and select "New" → "Organizational Unit"
3. A dialog box will appear to create the new OU
4. Type "Departments" as the name and uncheck "Protect container from accidental deletion" if you want to allow deletion during your lab setup
5. Click "OK" to create the OU

Creating Department-Specific OUs

1. Right-click on your domain name again and create two more base OUs following the same process:
    - "Resources"
    - "Administration"
2. Now create department-specific OUs:
    - Right-click on the "Departments" OU
    - Select "New" → "Organizational Unit"
    - Create the following sub-OUs one by one:
        - IT
        - HR
        - Finance
        - Marketing
3. For the "Resources" OU, create the following sub-OUs:
    - Computers
    - Servers
    - Groups
4. For the "Administration" OU, create the following sub-OUs:
    - Admin Accounts
    - Service Accounts

Your OU structure should now resemble a hierarchical tree with these organizational units properly nested.

User Account Creation

Creating Standard User Accounts

1. First, decide which departments your test users will belong to (distribute them across IT, HR, Finance, and Marketing)
2. For each user:
    - Right-click on the appropriate department OU (e.g., Departments > IT)
    - Select "New" → "User"

- In the New Object - User dialog box, enter:
  - First name (e.g., "John")
  - Last name (e.g., "Smith")
  - Full name will auto-populate (e.g., "John Smith")
  - User logon name (e.g., "john.smith" or "jsmith")
  - For the domain suffix, use your domain name (e.g., "@contoso.local")
- Click "Next"

3. On the password screen:
   - Enter an initial password (e.g., "P@ssw0rd123!")
   - Configure password options:
     - Uncheck "User must change password at next logon" for lab purposes (in production, you would typically leave this checked)
     - Check "Password never expires" for lab convenience (not recommended in production)
     - Leave "User cannot change password" unchecked
     - Leave "Account is disabled" unchecked
   - Click "Next"
4. Review the settings and click "Finish" to create the user
5. Repeat this process to create at least 10 users distributed across your departments. Example users:
   - IT: John Smith, Sarah Jones, Michael Chen
   - HR: Emily Davis, Robert Johnson
   - Finance: David Wilson, Amanda Garcia
   - Marketing: Thomas Brown, Jessica Miller, Lisa Taylor

Creating Administrator Accounts

1. Right-click on the "Admin Accounts" OU under "Administration"
2. Select "New" → "User"

3. Create administrative accounts with naming conventions that identify them as admin accounts:
    - Example: "admin-jsmith" for John Smith's admin account
    - Set stronger passwords for these accounts (e.g., longer, more complex)
4. For department administrators, create accounts like:
    - IT-Admin
    - HR-Admin
    - Finance-Admin
    - Marketing-Admin
5. For service-specific administrators, consider:
    - Exchange-Admin (if you're running Exchange)
    - SQL-Admin (if you're running SQL Server)
    - Backup-Admin

Security Groups

Creating Global Security Groups for Departments

1. Right-click on the "Groups" OU under "Resources"
2. Select "New" → "Group"
3. In the New Object - Group dialog:
    - Enter Group name (e.g., "IT-Staff")
    - Group scope: Select "Global"
    - Group type: Select "Security"
    - Click "OK"
4. Repeat to create the following global security groups:
    - IT-Staff
    - HR-Staff
    - Finance-Staff
    - Marketing-Staff

Creating Domain Local Groups for Resource Access

1. Right-click on the "Groups" OU again
2. Select "New" → "Group"
3. Create domain local groups for resource permissions:
    - Group name: "FileServer-Read"
    - Group scope: "Domain Local"
    - Group type: "Security"
    - Click "OK"
4. Repeat to create additional domain local groups:
    - FileServer-Modify
    - FileServer-FullControl
    - PrinterAccess
    - RemoteDesktopUsers

Adding Users to Groups - Method 1: Via User Properties

1. Navigate to a specific OU containing users (e.g., Departments > IT)
2. Double-click on a user (e.g., John Smith)
3. In the user properties dialog, click on the "Member Of" tab
4. Click "Add" button
5. In the "Select Groups" dialog:
    - Type the name of the group (e.g., "IT-Staff")
    - Click "Check Names" to validate
    - The name should become underlined if found
    - Click "OK"
6. The group now appears in the "Member Of" list
7. Click "Apply" then "OK" to save changes

Adding Users to Groups - Method 2: Via Group Properties

1. Navigate to the Groups OU under Resources
2. Double-click on a group (e.g., "IT-Staff")
3. In the group properties dialog, click on the "Members" tab

4. Click "Add" button
5. In the "Select Users, Contacts, Computers, Service Accounts, or Groups" dialog:
    - Type names of users to add, separated by semicolons (e.g., "John Smith; Sarah Jones")
    - Click "Check Names" to validate
    - Names should become underlined if found
    - Click "OK"
6. The users now appear in the "Members" list
7. Click "Apply" then "OK" to save changes

Creating Nested Groups

1. Open the properties of a domain local group (e.g., "FileServer-Read")
2. Click on the "Members" tab
3. Click "Add"
4. Type the name of a global group (e.g., "IT-Staff")
5. Click "Check Names" and then "OK" when validated
6. The global group is now a member of the domain local group
7. Add other relevant global groups to this domain local group:
    - For example, add "IT-Staff" and "HR-Staff" to "FileServer-Read"
    - Add only "IT-Staff" to "FileServer-FullControl"
    - Add all department groups to "PrinterAccess"

Group Policy Objects Implementation Guide

Basic Group Policy Configuration

Opening Group Policy Management

1. Log into your Domain Controller as a Domain Administrator
2. Access Group Policy Management in one of these ways:
    - From Server Manager: Click "Tools" in the upper right corner, then select "Group Policy Management"
    - From Administrative Tools: Navigate to Start > Windows Administrative Tools > Group Policy Management

- Run gpmc.msc from the Run dialog (Win+R)

Creating the Default Domain Password Policy GPO

1. In Group Policy Management, expand your forest, then Domains, and locate your domain
2. Right-click on your domain name and select "Create a GPO in this domain, and Link it here"
3. Name it "Default Domain Password Policy" and click OK
4. Right-click the new GPO and select "Edit" to open Group Policy Management Editor
5. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
6. Configure the following settings:
   - Enforce password history: 24 passwords remembered (prevents reuse of recent passwords)
   - Maximum password age: 90 days (forces regular password changes)
   - Minimum password age: 1 day (prevents rapid cycling of passwords)
   - Minimum password length: 12 characters
   - Password must meet complexity requirements: Enabled
   - Store passwords using reversible encryption: Disabled (more secure)
7. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy
8. Configure these settings:
   - Account lockout duration: 30 minutes
   - Account lockout threshold: 5 invalid logon attempts
   - Reset account lockout counter after: 30 minutes
9. Click "OK" to save changes and close the editor

Important: Since this is your domain password policy, it will affect all users in the domain. Consider your organization's specific needs when setting these values.

Desktop Environment Settings

Creating the Corporate Desktop Settings GPO

1. In Group Policy Management, right-click on "Group Policy Objects" and select "New"
2. Name the GPO "Corporate Desktop Settings" and click OK
3. Right-click the new GPO and select "Edit"

Configuring Desktop Background

1. Navigate to: User Configuration > Policies > Administrative Templates > Desktop > Desktop
2. Double-click "Desktop Wallpaper"
3. Select "Enabled"
4. Specify the path to your wallpaper file (e.g., \\domainname\NETLOGON\Wallpapers\corporate.jpg)
5. Set "Wallpaper Style" to "Fill" for best appearance on most displays

Setting Power Management Options

1. Navigate to: Computer Configuration > Policies > Administrative Templates > System > Power Management
2. Configure settings such as:
   - Power Management > Sleep Settings > "Specify the system sleep timeout" (Enabled, set to 30 minutes)
   - Power Management > Power Button Settings > "Select the Power button action" (Enabled, set to "Sleep")
   - Power Management > Hard Disk Settings > "Turn off hard disk after" (Enabled, set to 20 minutes)

Adding Desktop Shortcuts

1. Navigate to: User Configuration > Preferences > Windows Settings > Shortcuts
2. Right-click in the right pane and select "New > Shortcut"
3. Configure shortcuts to common applications:
   - For each shortcut, set:
     - Action: Create
     - Name: [Application Name]
     - Target type: File System Object

        - Location: Desktop
        - Target path: Path to the application (e.g., C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE)
    - Repeat for each required application

Restricting Control Panel Access

1. Navigate to: User Configuration > Policies > Administrative Templates > Control Panel
2. To disable the entire Control Panel, double-click "Prohibit access to Control Panel and PC settings" and set to "Enabled"
3. For more granular control, navigate to: User Configuration > Policies > Administrative Templates > Control Panel > specific applet folder
4. Configure settings for specific Control Panel items you want to restrict

Linking the Corporate Desktop Settings GPO

1. Back in Group Policy Management, expand your domain and locate the Department OU
2. Right-click on the Department OU and select "Link an Existing GPO"
3. Select "Corporate Desktop Settings" GPO from the list and click OK

Security Baselines

Creating the Security Baseline GPO

1. In Group Policy Management, right-click on "Group Policy Objects" and select "New"
2. Name the GPO "Security Baseline" and click OK
3. Right-click the new GPO and select "Edit"

Configuring Windows Firewall Settings

1. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security
2. Right-click on "Windows Defender Firewall with Advanced Security" and select "Properties"
3. Configure each profile (Domain, Private, Public):
    - Firewall state: On (recommended)

   - Inbound connections: Block (default)
   - Outbound connections: Allow (default)
4. For specific application rules, right-click on "Inbound Rules" and select "New Rule"
5. Follow the wizard to create rules for necessary applications or services

Enabling Audit Policies

1. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies
2. Configure these key audit policies:
   - Account Logon > Audit Credential Validation: Success and Failure
   - Account Management > Audit User Account Management: Success and Failure
   - Logon/Logoff > Audit Logon: Success and Failure
   - Logon/Logoff > Audit Logoff: Success

Restricting Local Administrator Rights

1. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment
2. Configure "Allow log on locally" to include only necessary groups
3. Configure "Access this computer from the network" to restrict remote access
4. Configure "Back up files and directories" and "Restore files and directories" as needed

Disabling Unnecessary Services

1. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > System Services
2. Review the list of services and for each unnecessary service:
   - Double-click the service
   - Select "Define this policy setting"
   - Set startup mode to "Disabled"
   - Common services to consider disabling:
     - Print Spooler (if no printing is needed)

        - Remote Registry (security risk)
        - Secondary Logon
        - Xbox Services (on business computers)

Linking and Testing the Security Baseline GPO

1. In Group Policy Management, locate the appropriate OUs for applying the security baseline
2. Right-click each target OU and select "Link an Existing GPO"
3. Select "Security Baseline" GPO from the list and click OK

Setting Up Exceptions for Specific Groups

1. In Group Policy Management, right-click on the "Security Baseline" GPO and select "Properties"
2. Click the "Security Filtering" tab
3. By default, "Authenticated Users" will be listed
4. To apply exceptions:
    - Remove "Authenticated Users" if you want very targeted application
    - Add specific security groups that need exceptions
    - For each group, adjust the "Apply Group Policy" permission as needed

Testing and Verification

After implementing these GPOs, it's essential to test them:

1. Run gpupdate /force on a test computer to apply the policies immediately
2. Use the Group Policy Results wizard (in Group Policy Management) to verify application
3. Create test user accounts in different OUs to ensure policies are applied correctly
4. Document any unintended consequences or conflicts

Remember that GPOs are processed in this order: Local, Site, Domain, OU - with the most specific policy (OU) taking precedence if there are conflicts.