Active Directory Deployment Documentation

Company Name: Nymous-Technologies

Domain Name: nymoustechnologies.local

Server Name: Nymous-Technologies

Operating Systems:

- Windows Server (Domain Controller)
- Windows 8 PC (HR Department)
- Windows 7 PC (IT Department)

1. Installing Active Directory Domain Services (AD DS)

Step 1: Install AD DS and DNS Roles

1. Open Server Manager (Windows Server).
2. Click Manage > Add Roles and Features.
3. In the wizard:
   - Select Role-based or feature-based installation.
   - Select the local server (Nymous-Technologies).
   - Choose the following roles:
     - Active Directory Domain Services
     - DNS Server
     - (Optionally) DHCP Server if dynamic IP assignment is needed.
4. Click Next until installation begins.
5. Reboot the server if prompted.

2. Promoting Server to a Domain Controller

Step 1: Promote via Server Manager

6. In Server Manager, click the notification flag and choose Promote this server to a domain controller.
7. Select:
   - Add a new forest
   - Root domain name: nymoustechnologies.local
8. Set Directory Services Restore Mode (DSRM) password.
9. Accept default selections for DNS and NetBIOS.
10. Review and click Install.
11. Server will reboot to complete the promotion.

3. Creating Organizational Units (OUs), Groups, and Users

Step 1: Open Active Directory Users and Computers (ADUC)

Go to Start > Administrative Tools > Active Directory Users and Computers.

Step 2: Create OUs

- Right-click on the domain nymoustechnologies.local and choose New > Organizational Unit:
- - Departments
  - HR
  - IT

Step 3: Create Security Groups

- Inside each department OU:
- - HR Group: HR_Users
  - IT Group: IT_Users

Step 4: Create User Accounts

- Under respective department OUs:
- - HR Department (Windows 8 PC): SegunAjani (SegunAjani.HR)
- - IT Department (Windows 7 PC): TobiAdio (TobiAdio.IT)

Right-click the OU > New > User, fill in username, password, and group membership.

4. Configuring User PCs to Join the Domain

Step 1: Network Configuration

- Ensure all PCs:
- - Are connected to the same network as the domain controller.
- - Have the DC IP address as their primary DNS server.

Example: DC IP: 192.168.1.10. On each PC, set 192.168.1.10 as DNS under IPv4 settings.

Step 2: Join Windows 8 PC (HR) to the Domain

12. Go to Control Panel > System > Change settings.
13. Click Change next to the computer name.
14. Select Domain, enter: nymoustechnologies.local.
15. Enter domain credentials (e.g., Administrator).
16. Restart when prompted.

Step 3: Join Windows 7 PC (IT) to the Domain

Follow the same steps as for Windows 8. Make sure DNS points to the DC.

5. Hardening the Domain Controller and Environment

A. Password and Account Policies

- Open Group Policy Management (gpmc.msc). Navigate to Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies:
- - Enforce password history: 24 passwords remembered
- - Maximum password age: 60 days
- - Minimum password length: 12 characters
- - Account lockout after 5 invalid attempts

B. Disable Guest Account

Use Local Security Policy or GPO to disable the guest account.

C. Enable Firewall and Anti-malware

Ensure Windows Defender or third-party antivirus is active and updated.

Use Windows Firewall with Advanced Security to allow only required inbound rules.

D. Audit Logging and Monitoring

- Enable auditing for the following:
- - Audit Account Logon Events
- - Audit Logon Events
- - Audit Policy Change

E. Limit Domain Admin Privileges

Use the Principle of Least Privilege.

Domain Admin account should be used only for administrative tasks.

Create separate standard accounts for daily usage.

F. Patch Management

Enable Windows Update.

Schedule weekly patch checks on the domain controller and user PCs.

G. Disable Unused Services and Ports

Use services.msc to disable unnecessary services (e.g., Telnet).

Use Windows Firewall or PowerShell to block unneeded ports.

6. Verification and Testing

- - Use ping and nslookup to verify name resolution.

- - Use gpresult /r to confirm GPOs are applied.
- - Log in from user PCs using domain credentials.