**🛠️ Active Directory Setup — vlab.local**

**👥 Lab Environment**

|  |  |
| --- | --- |
| **Component** | **Details** |
| Domain Name | vlab.local |
| Subnet | 172.16.1.0/24 |
| Domain Controller | 172.16.1.10 |
| DNS Server | Same as DC |
| Client Machine | 172.16.1.100+ |
| OS Version | Windows Server 2019/2022 |

**1️⃣ Install and Configure Active Directory Domain Services**

**🔌 Set Static IP Address**

New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.1.10 -PrefixLength 24 -DefaultGateway 172.16.1.1

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 172.16.1.10

**🖊️ Rename Computer**

Rename-Computer -NewName "HQ-DC01" -Restart

**🕐 Set Time Zone**

Set-TimeZone -Name "Arab Standard Time"

**🗓️ Install AD DS Role**

1. Open **Server Manager** → click **Add Roles and Features** → click **Next**.
2. Select **Role-based or feature-based installation** → click **Next**.
3. Select **this server** from the server pool → click **Next**.
4. Select **Active Directory Domain Services**.
5. When prompted, click **Add Features** → click **Next** until **Confirmation**.
6. Click **Install**. Wait for completion, then click **Close**.

**🏗️ Configure Domain Controller**

1. Click the **flag notification** in Server Manager → **Promote this server to a domain controller**.
2. Choose **Add a new forest** → enter vlab.local as domain name → click **Next**.
3. Set **DSRM password** → click **Next**.
4. Ignore DNS delegation warnings → click **Next**.
5. Confirm NetBIOS domain name is VLAB → click **Next**.
6. Accept default locations for database, log, and SYSVOL folders → click **Next**.
7. Review settings → click **Next**, run prerequisites check, and then **Install**.

The server will reboot automatically.

**✅ Verify Domain Setup**

Get-ADDomain

Get-ADForest

**🌐 Configure DNS Forwarders**

Add-DnsServerForwarder -IPAddress 8.8.8.8

**2️⃣ Create Service Accounts**

**👤 Add Service Accounts**

1. Open **Active Directory Users and Computers** → go to vlab.local → **Users** container.
2. Right-click → **New → User** and add:
   * **ra-service** → set password → mark as "Password never expires"
   * **autoenrollmentbind** → set password → mark as "Password never expires"

**👥 Group Membership**

* Add autoenrollmentbind to **Cert Publishers** group.

⚠️ *Tip*: You may use a single account for all services for simplicity, but **do not** add it to the **Protected Users** group to avoid LDAP Bind failures.

**3️⃣ Add Hosts to DNS Service**

1. Open **DNS Manager** from **Server Manager → Tools → DNS**.
2. Expand your server → Forward Lookup Zones → vlab.local.
3. Right-click → **New Host (A or AAAA)**:
   * Add entries for **EJBCA** and other servers.
4. Update the **SOA serial number**.

**4️⃣ Install Active Directory Certificate Services Tools**

1. From **Server Manager** → **Manage → Add Roles and Features**.
2. Click **Next** until **Features**.
3. Expand **Remote Server Administration Tools** → **Role Administration Tools**.
4. Check **AD Certificate Services Tools** → click **Next** → click **Install**.

Wait for installation to complete, then click **Close**.

**5️⃣ Add a Client to the Domain**

On a client machine (e.g. 172.16.1.100):

1. Set DNS to 172.16.1.10
2. Rename to CLIENT01
3. Join domain:

Add-Computer -DomainName "vlab.local" -Credential vlab\administrator -Restart

**6️⃣ Create OU and First User**

New-ADOrganizationalUnit -Name "IT" -Path "DC=vlab,DC=local"

New-ADUser -Name "Mohamed Nada" \

-SamAccountName "mnada" \

-UserPrincipalName "mnada@vlab.local" \

-AccountPassword (ConvertTo-SecureString "P@ssw0rd123" -AsPlainText -Force) \

-Enabled $true \

-Path "OU=IT,DC=vlab,DC=local"

**7️⃣ Health Checks**

dcdiag

repadmin /replsummary

✅ AD setup complete for vlab.local. Next: GPO, Delegation, Trusts, and Advanced Configs.