**16️⃣ Active Directory Federation Services (ADFS)**

**📥 Install ADFS Role**

1. Open **Server Manager > Add Roles and Features**.
2. Select **Active Directory Federation Services**.
3. Complete installation and **Configure ADFS**.

**⚙️ Configure ADFS**

1. Choose **Create the first federation server**.
2. Provide credentials with domain admin rights.
3. Specify SSL certificate (you must pre-install).
4. Choose Federation Service Name: fs.vlab.local.
5. Specify a Service Account (Group Managed Service Account recommended).
6. Review and complete configuration.

**☁️ 17️⃣ Azure AD Connect (Hybrid Identity)**

**🔄 Sync On-Prem AD to Azure AD**

1. Download [Azure AD Connect](https://www.microsoft.com/en-us/download/details.aspx?id=47594).
2. Launch the installer and select **Custom installation**.
3. Use **Express Settings** for lab or **Custom** for selective sync.
4. Enter credentials for:
   * Azure Global Administrator
   * On-prem Domain Admin
5. Choose sync options: **Password Hash Sync**, **Pass-through Authentication**, or **Federation with ADFS**.
6. Configure OU filtering and optional features.
7. Finish setup and confirm first sync.

🔁 To force sync:

Start-ADSyncSyncCycle -PolicyType Delta

**📊 18️⃣ Monitoring & Health Checks**

**🧪 Tools**

* **Event Viewer** (AD DS, DNS, ADFS logs)
* **dcdiag** – Domain controller diagnostics
* **repadmin** – Replication monitoring
* **Server Manager > Performance Monitor**
* **Azure AD Connect Health** (for hybrid)

**🔍 Example Health Checks**

# Test replication health

repadmin /replsummary

# Check DC diagnostics

Dcdiag /v

# DNS test

nltest /dsgetdc:vlab.local

**💻 19️⃣ PowerShell Automation**

**⚙️ Useful Cmdlets**

# Create AD User

New-ADUser -Name "John Doe" -GivenName John -Surname Doe -SamAccountName jdoe -UserPrincipalName jdoe@vlab.local -AccountPassword (ConvertTo-SecureString 'P@ssw0rd!' -AsPlainText -Force) -Enabled $true

# Add to Group

Add-ADGroupMember -Identity "Domain Admins" -Members jdoe

# Create OU

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

# Create GPO

New-GPO -Name "Disable USB Storage"

# Link GPO

New-GPLink -Name "Disable USB Storage" -Target "OU=TechDept,DC=vlab,DC=local"

**🧠 Scripts to Automate**

* Bulk user creation from CSV
* User deprovisioning (disable, move, archive mailbox)
* GPO export/import
* Audit report generation
* Scheduled backups