LAB CHECKLIST – AD DC + JEA + GPO + OU + USERS/GROUPS + RDS

1. Base Environment Setup

Step	Task	Status
1.1	Install Windows Server 2019 on one machine (Server01)	
1.2	Install Windows 10 on three client machines (Client01, Client02, Client03)	
1.3	Assign static IP addresses to all machines in the same subnet	
1.4	Set proper hostnames for all machines	
1.5	Verify network connectivity (ping between all systems)	

---

2. Active Directory Domain Controller (AD DC)

Step	Task	Status
2.1	Install the Active Directory Domain Services (AD DS) role on Server01	
2.2	Promote Server01 to a Domain Controller (create new forest and domain, e.g., corp.local)	
2.3	Reboot and verify domain functionality	
2.4	Join all Windows 10 clients to the new domain	
2.5	Verify domain membership using whoami and echo %USERDOMAIN% on clients	

---

3. Organizational Units (OUs)

Step	Task	Status
3.1	Create main OU structure (e.g., Users, Groups, Computers, Servers, IT, HR)	
3.2	Move corresponding objects into each OU	
3.3	Create sub-OUs for department-level organization if needed	

---

4. Users and Groups

Step	Task	Status
4.1	Create user accounts (e.g., HRUser1, ITUser1, etc.)	
4.2	Create security and distribution groups	
4.3	Add users to groups based on roles or departments	
4.4	Verify logon using domain credentials from client machines	

---

5. Group Policy (GPO)

Step	Task	Status
5.1	Open Group Policy Management Console (GPMC)	
5.2	Create and link GPOs to specific OUs (e.g., password policy, desktop wallpaper, restricted access)	
5.3	Use gpupdate /force on clients to apply policies	
5.4	Verify GPO application using gpresult /r	

---

6. Just Enough Administration (JEA)

Step	Task	Status
6.1	Install Windows PowerShell 5.1+ (already included in Server 2019)	
6.2	Create a PowerShell session configuration file (using New-PSSessionConfigurationFile)	
6.3	Define Role Capabilities (restrict what commands can be run)	
6.4	Register the JEA endpoint using Register-PSSessionConfiguration	
6.5	Test limited access by connecting to the JEA endpoint from a non-admin account	

---

7. Remote Desktop Services (RDS)

Step	Task	Status
7.1	Install Remote Desktop Services role on the server	
7.2	Configure licensing mode (Per User or Per Device)	
7.3	Add domain users or groups allowed to access RDS	
7.4	Test Remote Desktop connection from Windows 10 clients	
7.5	Verify RDS access control and session policies	

---

8. Validation and Testing

Step	Task	Status
8.1	Log in from each Windows 10 client with domain credentials	
8.2	Test GPO policies (e.g., desktop restrictions, password policy)	
8.3	Test JEA access limitations	
8.4	Verify RDS login and session functionality	
8.5	Review event logs and system performance	

Environment:

- 1 × Windows Server 2019 (Main Server)
- 3 × Windows 10 Clients

---

1. ENVIRONMENT PREPARATION

Step 1: Install Windows Server 2019

- Install Windows Server 2019 (Standard or Datacenter).
- Set the computer name to **SRV-DC01**.
- Configure the server with a static IP (e.g., 192.168.10.10).
- Set the DNS server to itself (192.168.10.10).

Step 2: Install Windows 10 on three clients

- Names: CLIENT01, CLIENT02, CLIENT03.
- Assign IP addresses: 192.168.10.11, 192.168.10.12, 192.168.10.13.
- Set the preferred DNS on all clients to **192.168.10.10** (the DC).

Step 3: Test Connectivity

- From Server:
- ping 192.168.10.11
- ping 192.168.10.12
- ping 192.168.10.13
- From each client:
- ping 192.168.10.10
- All machines should reply successfully.

---

2. INSTALL AND CONFIGURE ACTIVE DIRECTORY DOMAIN CONTROLLER (AD DC)

Step 4: Install AD DS Role

- Open **Server Manager → Manage → Add Roles and Features**.
- Choose **Active Directory Domain Services**.
- Complete the wizard and click **Install**.

Step 5: Promote the server to a Domain Controller

- In Server Manager, click the yellow flag → **Promote this server to a domain controller**.
- Choose **Add a new forest**.
- Domain Name: **corp.local**.
- Set a DSRM password and proceed.
- Accept default paths and install.
- The server will automatically restart.

Step 6: Verify Domain Functionality

- Log in as **corp\administrator**.
- Open **Active Directory Users and Computers (ADUC)** → confirm **corp.local** is visible.
- Run:
- nltest /dsgetdc:corp.local

It should return details of the Domain Controller.

Step 7: Join Windows 10 Clients to the Domain

- On each client:
    1. Open **Settings → System → About → Rename this PC (advanced)**.
    2. Click **Change**, select **Domain**, and type corp.local.
    3. Enter the domain admin credentials.
    4. Reboot the client.

Step 8: Verify Domain Membership

- Log in on each client with a domain account.
- Run:
- whoami

It should return something like:

corp\username

---

3. CREATE ORGANIZATIONAL UNITS (OUs)

Step 9: Create OUs

- On the DC, open **Active Directory Users and Computers**.
- Right-click the domain → **New → Organizational Unit**.
- Create:
    - Users
    - Groups
    - Computers
    - IT
    - HR
    - Servers

Step 10: Move Objects

- Move computer objects (CLIENT01, etc.) into **Computers OU**.
- Move user accounts (once created) into their department OUs.

---

4. CREATE USERS AND GROUPS

Step 11: Create Users

- In ADUC, go to **Users OU → Right-click → New → User**.
- Example:
    - Name: **Ahmed HR**, Username: **ahmed.hr**

- Name: **Omar IT**, Username: **omar.it**

- Set a strong password and enable "Password never expires" (for lab).

Step 12: Create Groups

- In ADUC, create two groups:
  - **HR_Group** (Global, Security)
  - **IT_Group** (Global, Security)

Step 13: Add Users to Groups

- Add **ahmed.hr** to **HR_Group**.
- Add **omar.it** to **IT_Group**.

Step 14: Verify Membership

- Right-click user → **Properties → Member Of** → confirm correct groups.

---

5. CREATE AND APPLY GROUP POLICIES (GPO)

Step 15: Open Group Policy Management Console (GPMC)

- Run gpmc.msc.

Step 16: Create a New GPO

- Right-click the **IT OU** → **Create a GPO in this domain, and Link it here**.
- Name it: **IT Policy**.

Step 17: Edit GPO

- Right-click **IT Policy → Edit**.
- Example settings:
  - **User Configuration → Administrative Templates → Desktop → Desktop Wallpaper**
  - Set a specific wallpaper (e.g., C:\Windows\Web\Wallpaper\Windows\img0.jpg).

Step 18: Link GPOs to OUs

- Link **IT Policy** to the IT OU.

- (Optional) Create **HR Policy** for HR OU.

Step 19: Apply and Verify

- On CLIENT01 (domain-joined):
- gpupdate /force
- gpresult /r
- Confirm the correct GPO is applied.

---

6. CONFIGURE JUST ENOUGH ADMINISTRATION (JEA)

Step 20: Create Role Capability

- On the DC, create a folder for role capabilities:
- New-Item -Path 'C:\Program Files\WindowsPowerShell\Modules\JEA\RoleCapabilities' -ItemType Directory -Force
- Create a new file:
- New-PSRoleCapabilityFile -Path 'C:\Program Files\WindowsPowerShell\Modules\JEA\RoleCapabilities\LimitedAdmin.psrc'

Step 21: Edit Role Capability File

- Open the .psrc file and specify allowed commands:
- VisibleCmdlets = 'Get-Service', 'Restart-Service'

Step 22: Create Session Configuration

- Create session config file:
- New-PSSessionConfigurationFile -Path C:\JEAConfig.pssc -SessionType RestrictedRemoteServer -RoleDefinitions @{ 'corp\IT_Group' = @{ RoleCapabilities = 'LimitedAdmin' } }

Step 23: Register JEA Endpoint

Register-PSSessionConfiguration -Name 'JEASession' -Path 'C:\JEAConfig.pssc'

Step 24: Test JEA

- From CLIENT01:

- Enter-PSSession -ComputerName SRV-DC01 -ConfigurationName JEASession
- Try running Get-Service (should work) and New-LocalUser (should fail).

---

7. INSTALL AND CONFIGURE REMOTE DESKTOP SERVICES (RDS)

Step 25: Install RDS Role

- In Server Manager → **Add Roles and Features** → Select **Remote Desktop Services Installation**.
- Choose **Quick Start → Session-based desktop deployment**.
- Select **SRV-DC01** as the target server.
- Complete the wizard.

Step 26: Configure Licensing

- Open **Server Manager → Remote Desktop Services → Overview**.
- Set licensing mode to **Per User**.

Step 27: Allow Domain Users Access

- Add users or groups (e.g., **IT_Group**) to the **Remote Desktop Users** group.

Step 28: Test Remote Desktop

- From CLIENT01, open **mstsc.exe**.
- Enter SRV-DC01.corp.local.
- Log in with **omar.it** credentials.
- Verify successful connection.

---

8. VALIDATION AND TESTING

Step 29: Verify Domain Logins

- Confirm each client can log in using domain credentials.

Step 30: Verify GPO Application

- Ensure each OU receives its correct policy.

Step 31: Test JEA Restrictions

- Limited admins can only run permitted PowerShell commands.

Step 32: Test RDS Access

- Confirm users in **Remote Desktop Users** group can access the server.
- Verify session and logoff control.

Step 33: Review Logs

- Use **Event Viewer → Windows Logs → System / Security** to check for errors.