

# Windows Domain Environment Setup Documentation (Full Project)

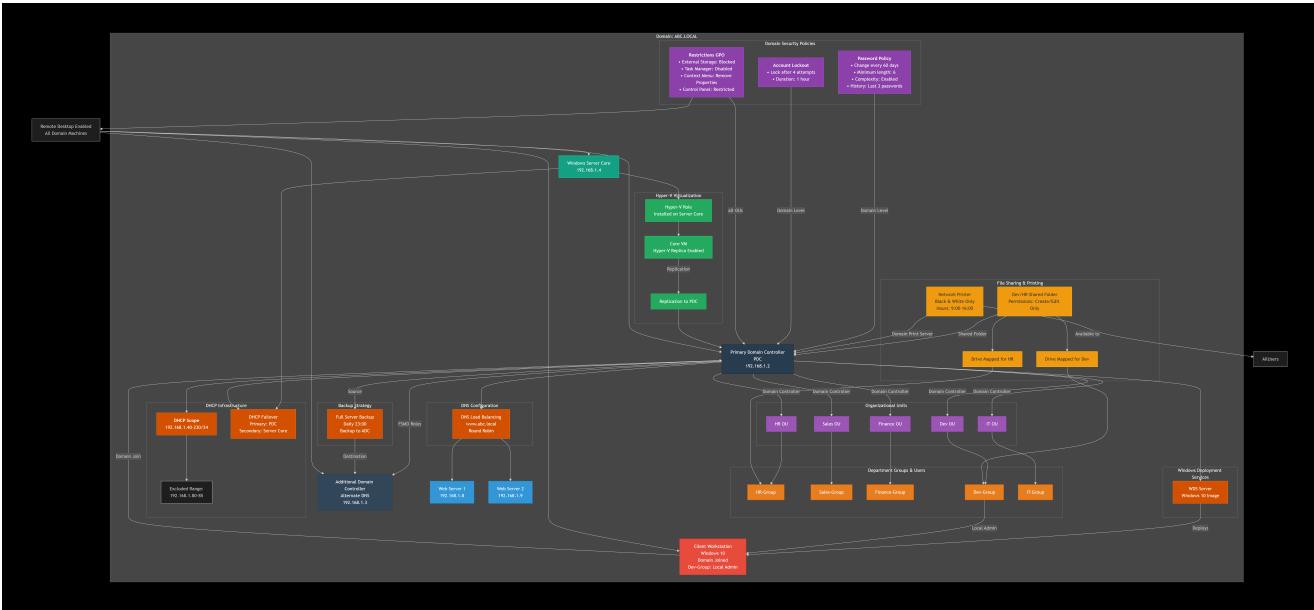
---

## The Project Task

### Windows Server Full LAB

- Create a domain environment with domain name (ABC.LOCAL) on a server with PDC as a computer name.
- Create separate OU for each department (HR, Sales, Finance, Dev, IT)
- Create users in each department, create separate groups for each department and add users to the department group.
- Configure password policy must change every 60 days, minimum length 6 digits with complex password and remember last 3 password.
- Force account lock for 1 hour after entering wrong password 4 times.
- Enable remote desktop connection for all machines in the domain.
- Prohibit access to all external storage, task manager, remove manage and properties from computer context menu and Control Panel.
- Create DHCP with scope start 192.168.1.40 to 192.168.1.230 /24 – also exclude range from IP address 80 to 85.
- Using DNS create a load balancing for [www.abc.local](http://www.abc.local) on two IP Addresses 192.168.1.8 and 192.168.1.9.
- Configure DHCP failover on windows server core.
- Install Hyper-V role on Windows Server Core and create a Core VM and configure Hyper-V replica with the PDC server.
- Install Windows 10 for the client through WDS.
- Join this machine to domain and add Dev group as a local administrator.
- Create a folder shared for Dev and HR can create, edit but can't delete.
- Create a MAP network drive for Dev and HR department.
- Add Printer for all domain users with black and white printing only and they can use the printer from 9:00 am to 4:00 pm only.
- Make an Additional Domain Controller with an alternate DNS.
- Create a full server backup every day at 11:00 pm for the main server and the backup on the ADC.

## The Project Diagram



## Project Overview

### 1. Create Domain abc.local on PDC

1. Set static IP: **192.168.1.2 /24**, Preferred DNS **127.0.0.1** or **192.168.1.2**
2. Rename computer → **PDC** → reboot
3. Server Manager → Add roles → **Active Directory Domain Services** → install
4. Promote this server to domain controller → **Add a new forest** → Root domain name: **abc.local**
5. Set DSRM password → Install → reboot

### 2. Create OUs, Groups & Users

Open **Active Directory Users and Computers** (dsa.msc)

- Right-click **abc.local** → New → Organizational Unit → create:
  - **HR**
  - **Sales**
  - **Finance**
  - **Dev**
  - **IT**
- In each OU → New → Group (Global, Security):
  - **HR-Group, Sales-Group, Finance-Group, Dev-Group, IT-Group**
- Create users (example logon names; set complex passwords):
  - OU HR: hruser1, hruser2 → add to **HR-Group**
  - OU Sales: salesuser1, salesuser2 → **Sales-Group**
  - OU Finance: finuser1, finuser2 → **Finance-Group**
  - OU Dev: devuser1, devuser2 → **Dev-Group**
  - OU IT: ituser1, ituser2 → **IT-Group**

### 3. Domain-wide Password & Lockout Policy

Group Policy Management → **Default Domain Policy** → Edit

- Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies
  - **Password Policy**
    - Enforce password history: **24** passwords remembered
    - Maximum password age: **60** days
    - Minimum password length: **6** characters
    - Password must meet complexity requirements: **Enabled**
  - **Account Lockout Policy**
    - Account lockout threshold: **4** invalid logon attempts
    - Account lockout duration: **60** minutes (1 hour)
    - Reset account lockout counter after: **60** minutes

Run `gpupdate /force` on PDC

### 4. Enable Remote Desktop (RDP) Domain-wide

Default Domain Policy → Edit

- Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections
  - Allow users to connect remotely... → **Enabled**
- User Rights Assignment → Allow log on through Remote Desktop Services → Add **Administrators + Remote Desktop Users**

(Optional) Disable NLA for easier lab access.

### 5. Prohibit External Storage, Task Manager, Control Panel / Properties Access

New GPO (or edit Default) linked to domain → name "Restrict User Access"

- **User Configuration** → Policies → Administrative Templates
  - System → **Prevent access to the command prompt** → Enabled (if needed)
  - System → **Remove Task Manager** → Enabled
  - Control Panel → **Prohibit access to Control Panel and PC settings** → Enabled
  - Desktop → **Hide and disable all items on the desktop** (optional) or use **Prohibit access to properties of Components**
- **Computer Configuration** → Policies → Administrative Templates → System → Removable Storage Access

- All Removable Storage classes: Deny all access → **Enabled**

Link GPO to domain or specific OUs (exclude admins if needed via WMI/Delegation).

## 6. DHCP Scope + DNS Round-Robin (on PDC or separate server)

Install **DHCP Server** role on PDC (or preferred server)

- DHCP console → IPv4 → New Scope
  - Range: **192.168.1.40 – 192.168.1.230**
  - Exclusion: **192.168.1.80 – 192.168.1.85**
  - DNS: **192.168.1.2**
- DNS Manager → abc.local → New Host (A)
  - Name: **www**
  - IP: **192.168.1.8** → Add Host
  - Same again → IP: **192.168.1.9** → Add Host

Round-robin is automatic (verify Advanced tab → Enable round robin).

## 7. Windows Server Core + DHCP Role + Hyper-V + Replica

1. Create new VM → install Windows Server Core
2. Set static IP, join domain abc.local
3. PowerShell commands:

text

```
Install-WindowsFeature DHCP -IncludeManagementTools
Install-WindowsFeature Hyper-V -IncludeManagementTools
```

4. Authorize DHCP in AD (from GUI server: DHCP console → right-click server → Authorize)
5. Create scope same as above (or use failover later)
6. Configure Hyper-V Replica:
  - On PDC (Hyper-V host): Enable replication → Hyper-V Settings → Replication Configuration → Enable
  - On Core: same
  - Create VM on Core → Enable replication to PDC

## 8. WDS – Deploy Windows 10 Client

On PDC (or dedicated server):

1. Add role **Windows Deployment Services** → both Deployment + Transport
2. Configure WDS → choose location for images
3. Add Boot image & Install image from Windows 10 ISO

4. Boot client VM → PXE boot → select image → install Win10
5. After install → join domain **abc.local**
6. Move computer object to **Dev** OU

Add **Dev-Group** as local admin on client:

- Local → lusrmgr.msc → Administrators → Add **abc\Dev-Group**
- Or use Restricted Groups GPO linked to Dev OU

## 9. Shared Folders (Dev & HR – no delete)

On file server (PDC):

- **C:\DevShare** → Share name **Dev**
  - Share perm: **Dev-Group** = Change
  - NTFS: **Dev-Group** = Modify → Advanced → uncheck **Delete + Delete subfolders/files**
- Same for **C:\HRShare** → **HR** share → **HR-Group**

## 10. Map Drives (GPO)

New GPO linked to Dev OU → "Map Dev Drive"

- User Config → Preferences → Drive Maps → New → **Z:** → \PDC\Dev

Same for HR OU → **Y:** → \PDC\HR

## 11. Printer – All users, Black/White only, 9:00–16:00

1. Install **Print Server** role
2. Add printer (network/local)
3. Printer Properties → **Advanced** tab
  - Printing Defaults → set driver to **Grayscale** / Black & White
  - Available from: **9:00** to **16:00**

Deploy via GPO (Printers preference) or let users add manually.

## 12. Additional Domain Controller + Alternate DNS

1. New server → IP e.g. **192.168.1.3**, DNS = 192.168.1.2
2. Install **AD DS** → Promote → Additional DC in abc.local
3. DHCP scope options → 006 DNS Servers → add **192.168.1.3**

## 13. Daily Full Backup – 23:00 on PDC & ADC

On both servers:

1. Add feature **Windows Server Backup**
2. wbadmin → Backup Schedule → Full server → Daily → 23:00
  - Destination: local disk or share

## Final Tests

- Password policy / lockout
- RDP from client
- No USB / Task Manager / Control Panel for restricted users
- DHCP leases in range
- [www.abc.local] rotates IPs
- Drives map correctly, cannot delete in shares
- Printer only B&W and only during time window
- Backup runs at 23:00