Windows Server Infrastructure Deployment

by Junior Kalomba

Systems Administrator

Date: July 21, 2025

Windows server Infrastructure Project Deployment

Junior Kalomba Systems Administrator

IT Infrastructure | Systems Administration

Windows Server, Active Directory, DNS, DHCP, File Server, GPO

Project Overview:

This project demonstrates the setup and configuration of a complete Windows Server infrastructure in a simulated business environment. It includes the deployment of Active Directory for centralized identity management, DNS and DHCP for name resolution and IP distribution, a secured File Server with permission-based access control, and the use of Group Policy Objects (GPOs) to enforce system policies and automate configurations across the network.

Key Components:

1. Active Directory Domain Services (AD DS): Configured a domain controller with user and group management, Organizational Units (OUs), and login policies.
2. DNS & DHCP Server: Set up internal DNS for name resolution and DHCP for automatic IP assignment across the network.
3. File Server with Permissions: Implemented shared folders with NTFS and share-level permissions based on group membership (e.g., HR, IT, Sales).
4. Group Policy (GPO): Created and linked policies to enforce security settings (e.g., password policies, desktop restrictions, folder redirection).

Tools & Technologies:

- VMware Workstation
- Windows Server 2022
- Windows 10/11

Project Objectives Achieved:

- Centralized user authentication and authorization
- Secure and structured file sharing based on departments
- Automated configuration and restriction enforcement using GPO
- Functional DNS and DHCP services supporting domain clients

Skills:

- Windows Server Administration
- Network Services Configuration
- Security Policies via Group Policy
- IT Infrastructure Design

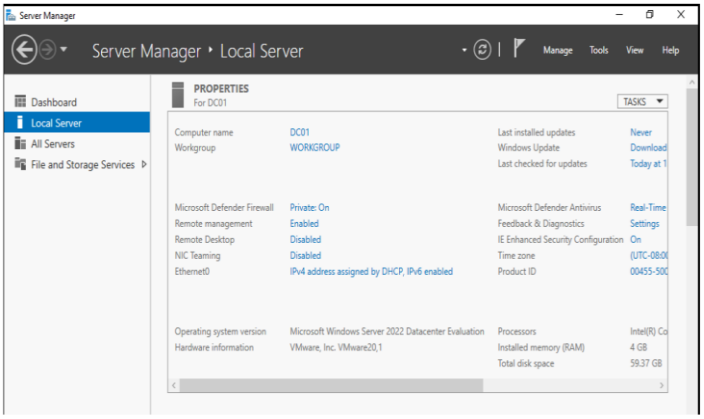
Windows Server 2022 Setup and Configuration Project

This document provides a step-by-step breakdown of setting up a Windows Server 2022 environment, including configuring Active Directory, DHCP, Group Policy, and role-based access using screenshots for better understanding.

Project breakdown

Step 1: Rename the Server

1. Open Server Manager.
2. Go to **Local Server** tab.
3. Click on the **Computer Name** ("WIN-XXXXXXX").
4. Click **Change.**
5. Rename it to: DC01 (for Domain Controller)
6. Restart the server when prompted.

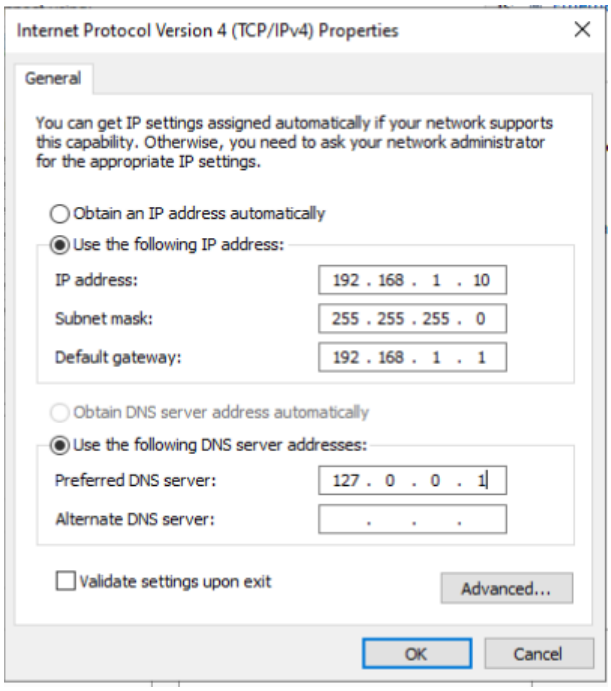


Step 2: Set a Static IP Address

1. **Open Control Panel > Network and Sharing Center**
2. **Click Ethernet > Properties**

3. **Select Internet Protocol Version 4 (TCP/IPv4) > Properties**
4. **Use the following example settings:**

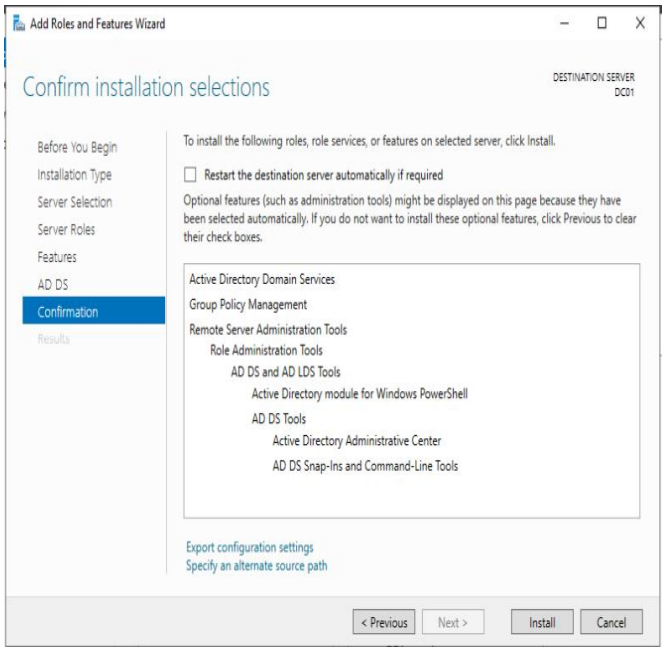
    - **IP address:** 192.168.1.10
    - **Subnet mask:** 255.255.255.0
    - **Default gateway:** 192.168.1.1
    - **Preferred DNS server:** 127.0.0.1 *(points to self)*



Configured a static IP address for the server to ensure reliable DNS and DHCP functionality.

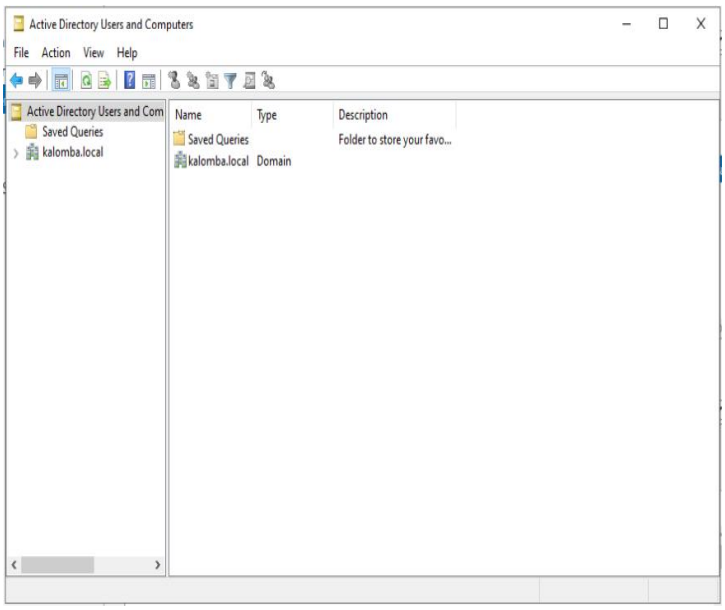
Step 3: Install Active Directory Domain Services (AD DS)

1. Open Server Manager
2. Click Add roles and features
3. On the Before you begin page → Click Next
4. On Installation Type → Select Role-based or feature-based installation → Click Next
5. On Server Selection → Keep default server selected → Click Next
6. On Server Roles:
    - Check **Active Directory Domain Services**
    - Click **Add Features** when prompted
    - Click **Next** until you reach **Confirmation**
7. Click Install



Step 4: Promote Server to Domain Controller

1. In Server Manager click the yellow flag notification → Click **Promote this server to a domain controller**
2. Choose:
    - **Add a new forest**
    - **Root domain name: kalomba. local (You can use your name)**
3. Set a DSRM password (Directory Services Restore Mode)
4. Click Next through the rest (leave defaults) and Review and Click **Install**
5. Go to Server Manager > Tools > Active Directory Users and Computers
6. Expand your domain: kalomba.local

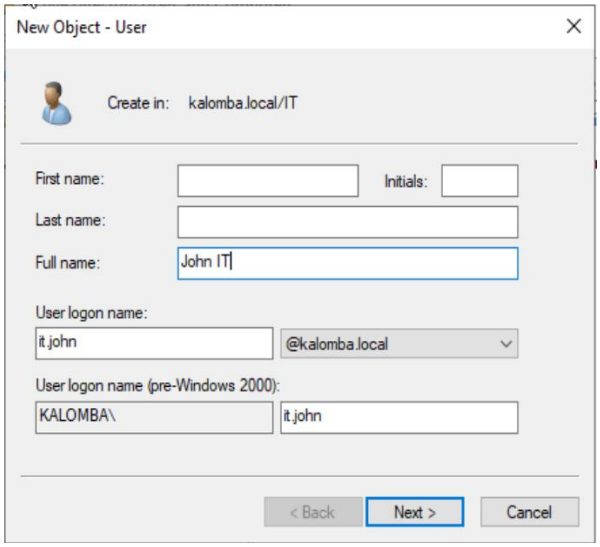


Opened Active Directory Users and Computers to manage the domain kalomba.local.

Step 5: Create Organizational Units (OUs)

1. Right-click your domain → **New > Organizational Unit**
2. Create the following OUs:
    - **IT**
    - **HR**
    - **Sales**
    - **Security Groups (for group-based permission control)**
3. Right-click each OU → New > User
4. Create one user per department

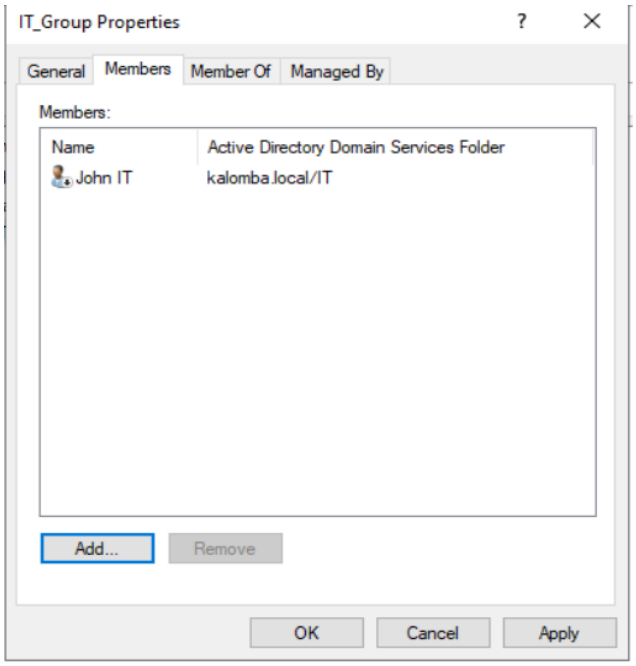
OU	Username	Full Name	Password
IT	it.john	John IT	P@ssw0rd1!
HR	hr.jane	Jane HR	P@ssw0rd1!
Sales	sales.mike	Mike Sales	P@ssw0rd1!



Step 6 : Create Security Groups

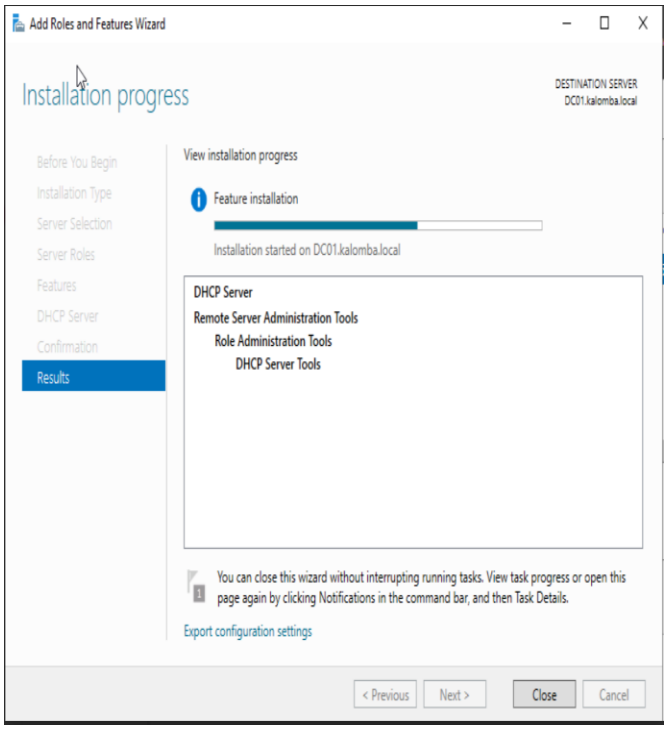
1. **Go to Security Groups OU**
2. **Right-click > New > Group**
3. **Create:**
    - **HR_Group**
    - **Sales_Group**
    - **IT_Group**

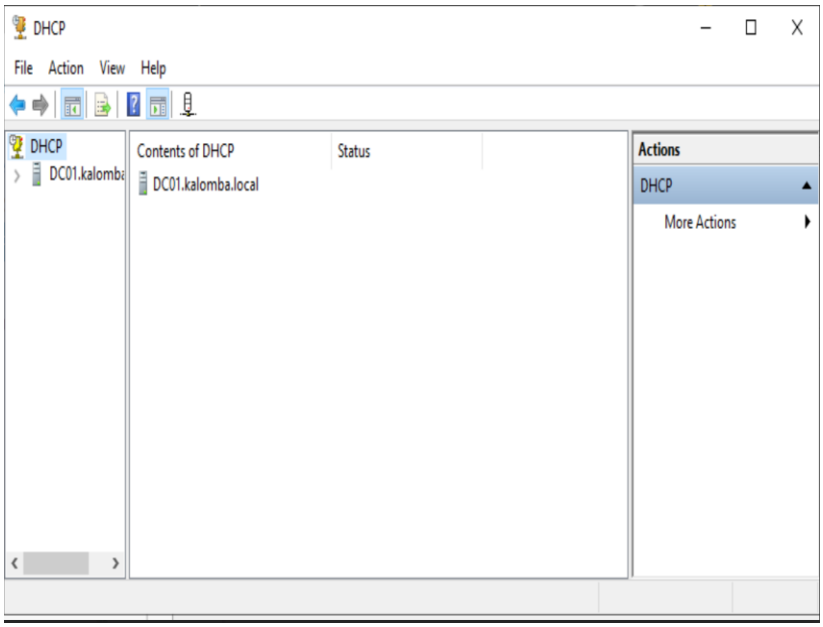
4. Set **Group scope: Global**, **Type: Security**
5. Add respective users to each group



Step 6 : Install DHCP Role

1. **Open Server Manager**
2. **Click Add Roles and Features**
3. **Select:**
    - **DHCP**
4. **Click Add Features if prompted**
5. **Continue → Click Install**

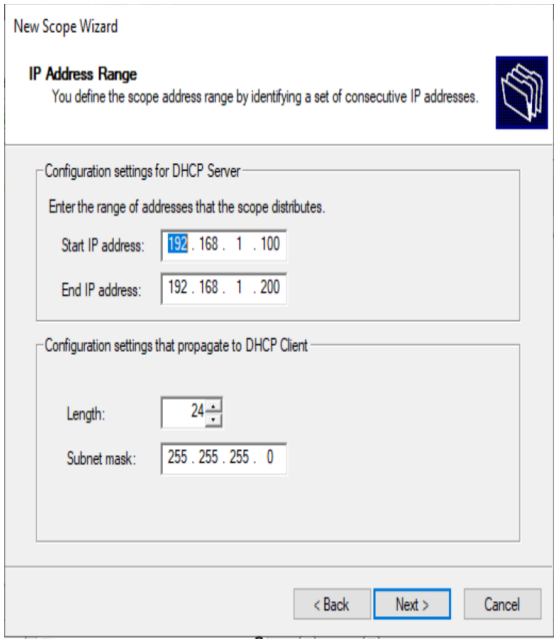




Verified that a client machine received an IP address from the DHCP server.

Step 7: Authorize DHCP & Create a Scope

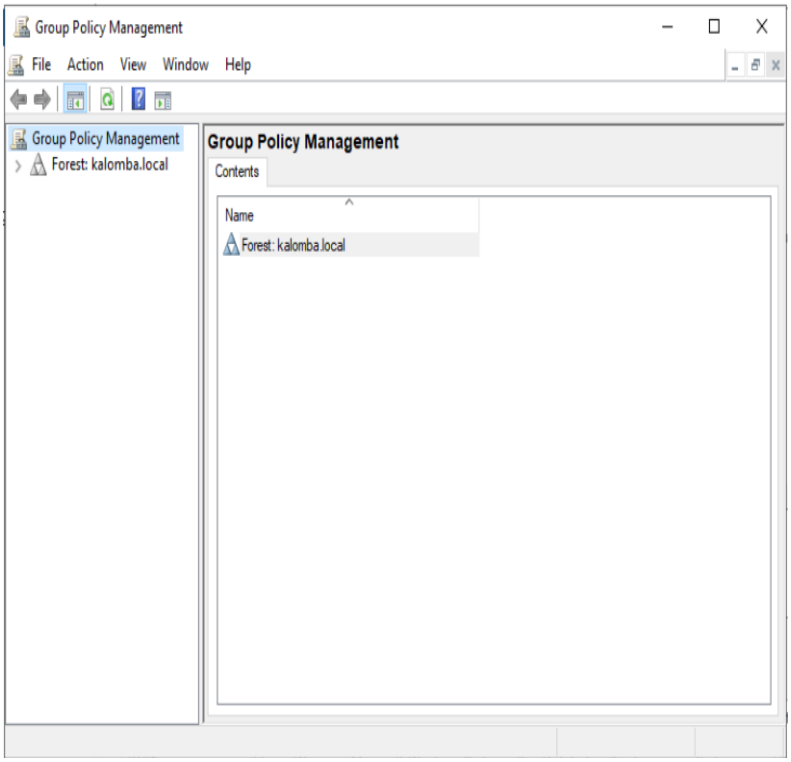
- Open DHCP Console via Server Manager > Tools > DHCP
- Expand your server → Right-click IPv4 > New Scope
- Name the scope: InternalLAN
- Set scope range:
  1. **Start IP:** 192.168.1.100
  2. **End IP:** 192.168.1.200
  3. **Subnet Mask:** 255.255.255.0
- Set default gateway: 192.168.1.1
- DNS: 192.168.1.10 (your DC)



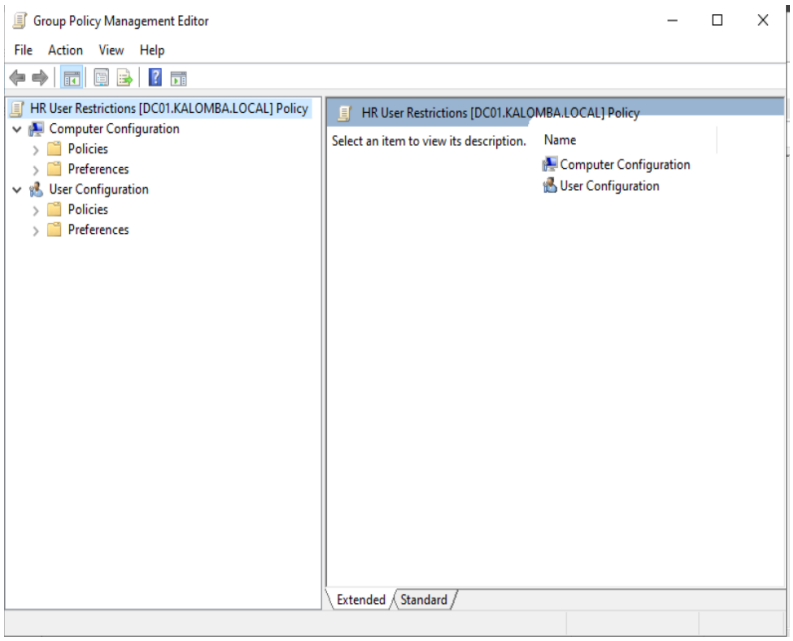
Configured the DHCP server and added a new scope to automatically assign IP addresses to clients.

Step 8: Create a New GPO

- Right-click your domain or an OU → **Create a GPO in this domain, and link it here**
- Name it: HR User Restrictions
- Right-click the new GPO → **Edit**



Launched Group Policy Management Console to manage policies across the domain.

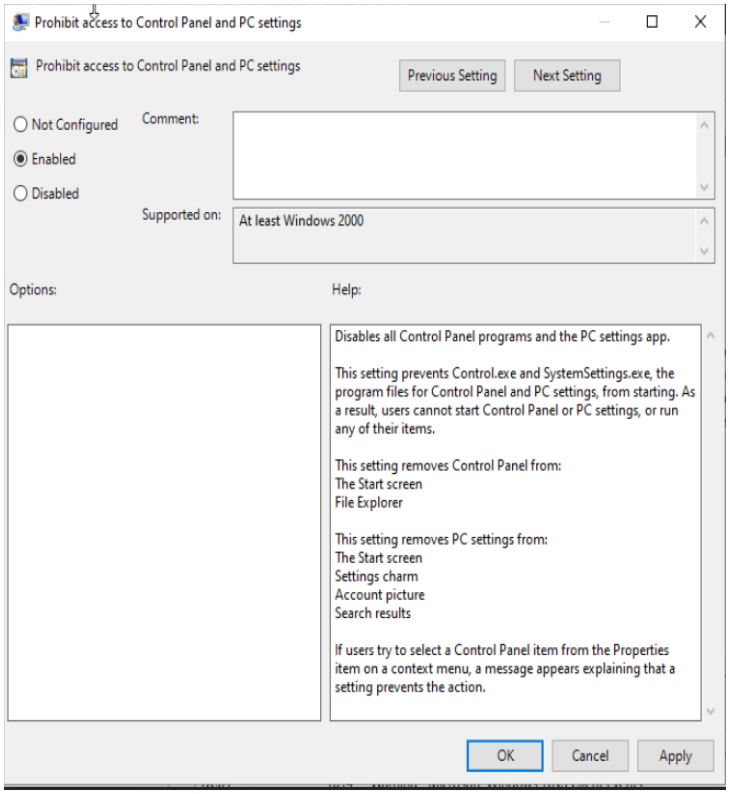


Created and linked a new GPO for user-level or computer-level settings.

In the **Group Policy Management Editor**:

Path:
User Configuration > Policies > Administrative Templates > Control Panel

- Double-click **Prohibit access to Control Panel and PC settings**
- Set it to **Enabled** → Click **OK**



Password Policy

⏪ Conclusion

This project successfully demonstrates the deployment and configuration of a complete Windows Server 2022 environment, simulating a real-world business network. By implementing Active Directory, DNS, DHCP, Group Policy. I showcased key skills in infrastructure setup, user management, and access control. This hands-on experience reinforces my ability to design and manage scalable and secure Windows-based networks.


Windows
Server
DNS