Active Directory with Group Policy (GPO)

Prepared by: Junior Kalomba

Date: July 25, 2025

Active Directory with Group Policy (GPO)

Junior Kalomba Systems Administrator

IT Infrastructure | Systems Administration

Windows Server, Active Directory, GPO

Project overview

This project demonstrates the deployment of Active Directory and Group Policy Objects (GPO) in a Windows Server 2022 environment. The aim is to build a secure, central identity management system for improved user and resource control via group policies.

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. File Server with Permissions: Implemented shared folders with NTFS and share-level permissions based on group membership (e.g., HR, IT, Sales).
3. 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 in case Windows 11

Project Goals

- Install and configure Active Directory Domain Services (AD DS)-
- Promote the server to a domain controller- Create Organizational Units (OUs)-
- Add users and groups into OUs
- Configure and link Group Policy Objects (GPOs)
- Enforce security settings and restrictions via GPO

Step-by-Step Setup

1. Install Windows Server 2022 and configure a static IP.
2. Install the 'Active Directory Domain Services' role via Server Manager.
3. Promote the server to a Domain Controller and create a new forest (e.g., lab.local or Kalomba.local (in my case)).

4. Use Active Directory Users and Computers to create Organizational Units such as IT, HR, and Sales.
5. Add test users and security groups into each OU.
6. Open Group Policy Management, create GPOs (e.g., disable Control Panel), and link them to appropriate OUs.
7. Test the policies by logging in with a user account and verifying restrictions are applied.

Skills:

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

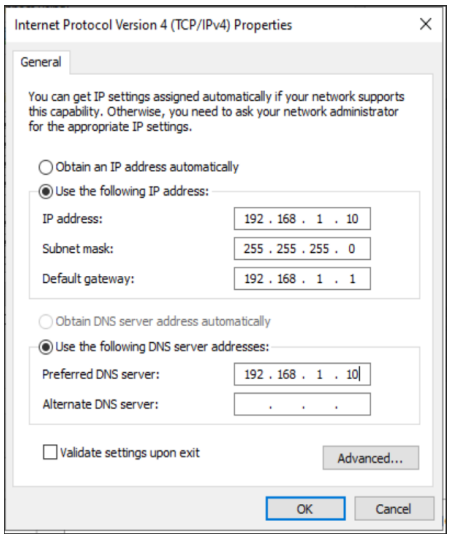
Active Directory Domain with Group Policies

---

1. **Set Static IP Address**

Steps:

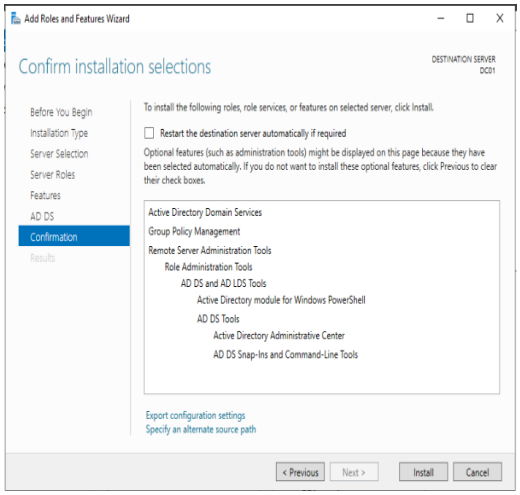
1. **Open Network and Sharing Center**
2. **Click Change adapter settings**
3. **Right-click Ethernet > Properties**
4. **Select Internet Protocol Version 4 (TCP/IPv4) > Properties**
5. **Use these settings:**
    - **IP: 192.168.1.10**
    - **Subnet: 255.255.255.0**
    - **Gateway: 192.168.1.1**
    - **DNS: 192.168.1.10 (pointing to itself)**

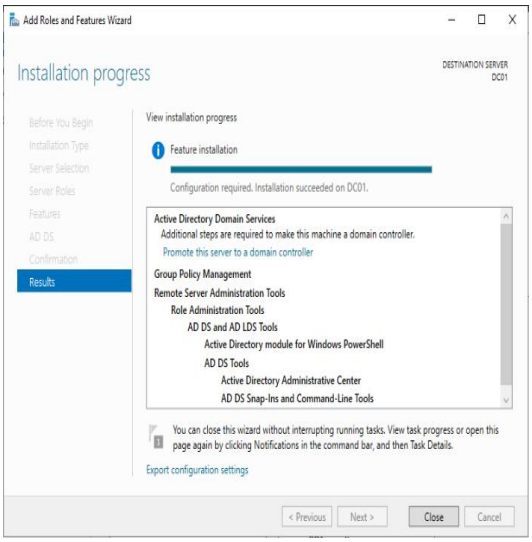


2. **Install AD DS Role**

Steps:

1. **Open Server Manager**
2. **Click Add roles and features**
3. **Choose:**
    - **Role-based or feature-based installation**
    - **Select your local server**
4. **Check Active Directory Domain Services**
5. **Accept defaults and install**





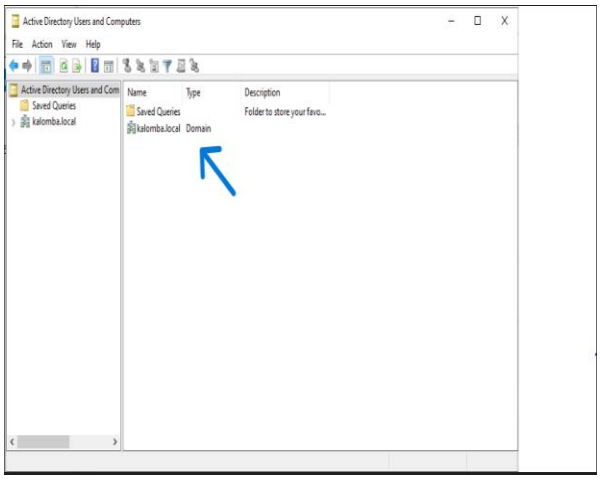
3. **Promote Server to Domain Controller**

Steps:

1. **After install, click the yellow flag ⚠ > "Promote this server to a domain controller"**
2. **Choose:**
   - **Add a new forest**
   - **Root domain: lab.local for my case I used “kalomba.local”**
3. **Set a DSRM password**
4. **Keep default settings (DNS and GC)**
5. **Complete the wizard and restart when prompted**

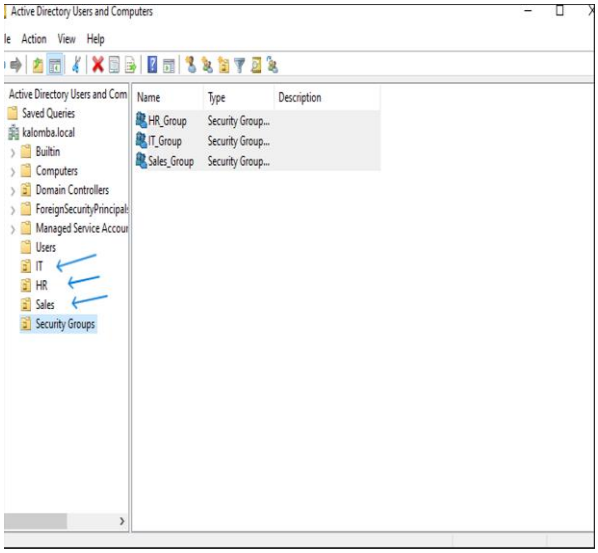
4. **Create Organizational Units (OUs)**

1. **Open Active Directory Users and Computers**
2. **In the left pane, expand your domain (lab.local for me I used” kalomba.local”)**
3. **Right-click kalomba.local > New > Organizational Unit**



4. **Create the following OUs:**

- **IT**
- **HR**
- **Finance or sales**



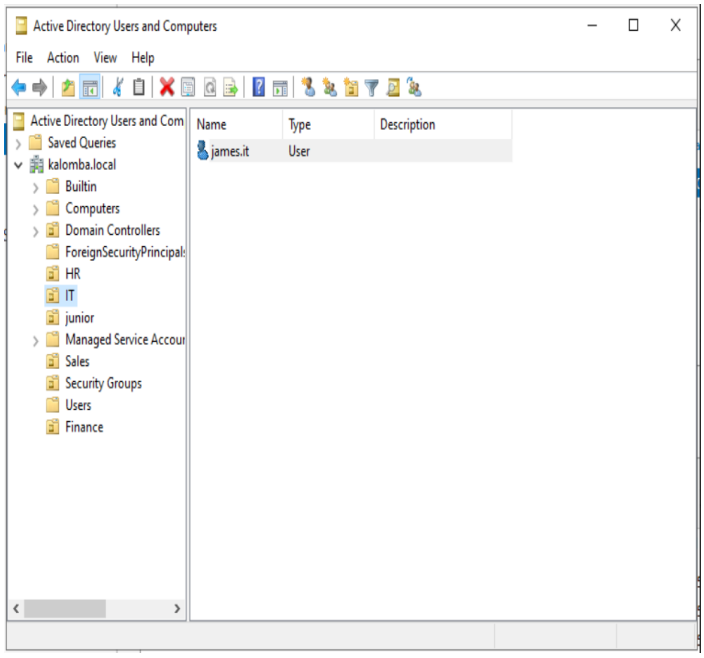
5. **Create Users and Groups**

1. Open "Active Directory Users and Computers"

2. For Each OU:

- **Right-click > New > User**
  - **IT OU:**
    - **User: james.it**

        - **Logon name: james.it@kalomba.local**
    - **For HR OU:**
        - **User: lucy.hr**
        - **Logon name: lucy.hr@kalomba.local**
    - **For Sales OU:**
        - **User: david.sales**
        - **Logon name: david.sales@kalomba.local**
    - **Set a password and check "User must change password at next logon" if desired**



Conclusion

This project successfully demonstrates how to deploy Active Directory and enforce policies through Group Policy in a Windows Server environment. Key components such as domain controller setup, OU creation, user/group management, and GPO configuration were implemented. The project reflects real-world system administration practices and provides a solid foundation for managing enterprise IT infrastructure.