Windows Server Configuration Lab

11.23.25

Alex Lutz
IT Support Specialist

Overview

I built a virtual homelab to deepen my understanding of enterprise-level network services and system administration. This project involved configuring a Windows Server to act as a domain controller and deploying core services like Active Directory, DHCP, and DNS. I also used an additional Windows client to simulate domain joining and group policy.

Objective

1. Gain practical experience in configuring and securing a Windows Server domain environment.
2. Exploring client-server interactions and basic network security principles.

Tools and Technology

- VirtualBox
- Windows Server (2022), Windows 11 ISO (2025)
- Active Directory Domain Services (AD DS)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Configuration Steps

I. Installing the Windows Server 2022 on Virtual Box

Virtual Box is installed to run both of these machines. Windows Server is downloaded along with the Windows 11 client. In the virtual box interface, these are the configurations for each in order to complete the lab.

Windows Server Configurations

- Type: Microsoft Windows
- Version: Windows 2022 (64-bit)
- Memory: 8192 MB
- Network Adapter: Internal Network (HomelabNet)
- Storage: Attach Windows Server 2022 ISO

Windows 11 Client Configurations

- Name: WIN11CLIENT01
- Type: Windows
- Version: Windows 11 (64-bit)
- Memory: 8192 MB
- Network Adapter: Internal Network (HomelabNet)
- Storage: Attach Ubuntu 22.04 ISO

II. Set a static IP address

- In network settings > IPv4 > properties, static IP is set to 192.168.1.10
- Set the IP address to 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

III. Rename the server

- Control panel > system > Rename this PC
- Change the computer name to DC01
- Restart the server to apply the changes

IV. Install Active Directory Domain Services (AD DS)

- Open Server Manager > Add Roles and Features
- Choose Role-based or Feature-based installation
- Select the local server (DC01)
- Under Server Roles, check Active Directory Domain Services
- Proceed through the Wizard and install required features

V. Promote the server to a Domain Controller

- Open Server Manager > Flag Icon > Promote server to a domain controller
- Add a new forest
- Specify the root domain name: homelab.net
- Set Directory Services Restore Mode (DSRM) password
- Complete the wizard and restart the server

VI. Configuring DHCP and DNS

- Open Server Manager > DHCP > Complete DHCP configuration
- Open Tools > DHCP > Add a new scope of IP addresses that will be assigned to devices on the network
- Set the parent domain and the server name

VII. Joining the Windows 11 Client to the Domain

- Power up the client
- Once prompted to connect to a network, hit shift + F10 to open command prompt
- Type the command “start ms-cxh:localonly” for local account creation
- Once the account is created, in the Start Menu search bar, type Rename this PC to change the hostname (WIN11CLIENT01), then restart
- Open Start > Settings > About > Advanced System Settings
- Under Computer Name > Change, then select Domain
- Enter the corresponding domain name (homelab.net)
- When prompted with login, use the Admin credentials established in AD DS

- Once logged in, you are now connected to the domain
- To test connections, in a command prompt type ping [IPv4 Address] of the Windows Server
- Type “ipconfig” to test DHCP automatically assigning an IP address to the client within the scope

Wrapping Up

This homelab project successfully demonstrated the process of building a functional Windows Server domain environment from the ground up. By configuring **Active Directory Domain Services (AD DS)**, **DNS**, and **DHCP**, the server was established as the central authority for identity, name resolution, and IP address management. The Windows 11 client was then joined to the domain, showcasing how enterprise endpoints interact with directory services and inherit policies through Group Policy.

Through these steps, I gained practical experience in:

- Setting up and promoting a server to a domain controller.
- Managing core infrastructure services that underpin enterprise networks.
- Understanding the client domain join process and authentication with AD DS.
- Exploring the foundation for centralized administration, security enforcement, and scalability.

This lab highlights the importance of **directory services and centralized management** in modern IT environments. Even in a small virtual setup, the same principles apply to enterprise networks: servers provide identity and resource control, while clients rely on them for secure access and consistent configuration.

Looking ahead, this environment can be expanded to include **Group Policy Objects (GPOs)** for enforcing security baselines, **WSUS** for patch management, and **role-based access control** to simulate real-world enterprise practices. By building this homelab, I’ve laid the groundwork for deeper exploration into **network security, automation, and hybrid cloud integration**, all of which are critical skills for future system administration.