

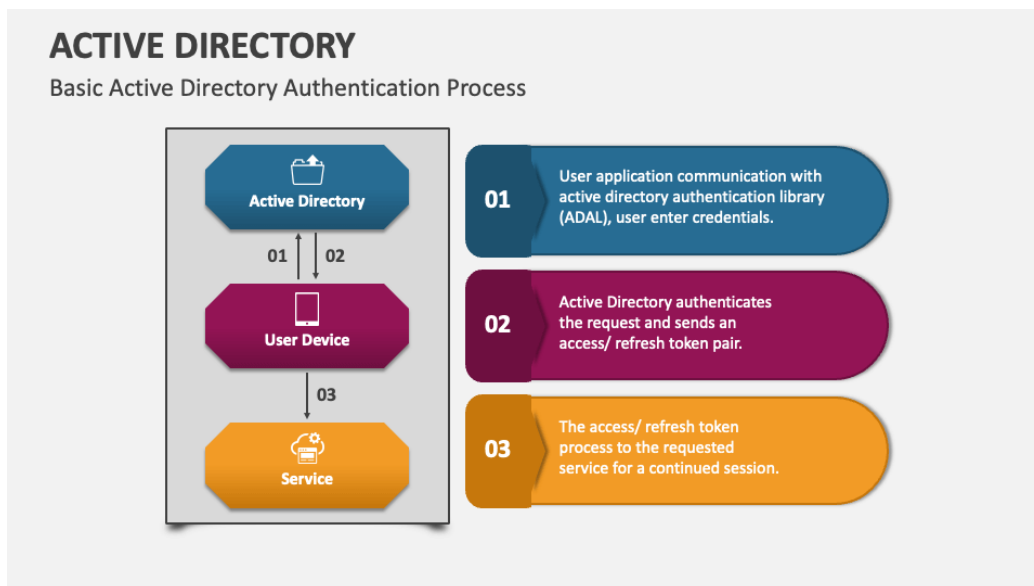
Active Directory Lab Implementation Documentation

1 Introduction – What is Active Directory?

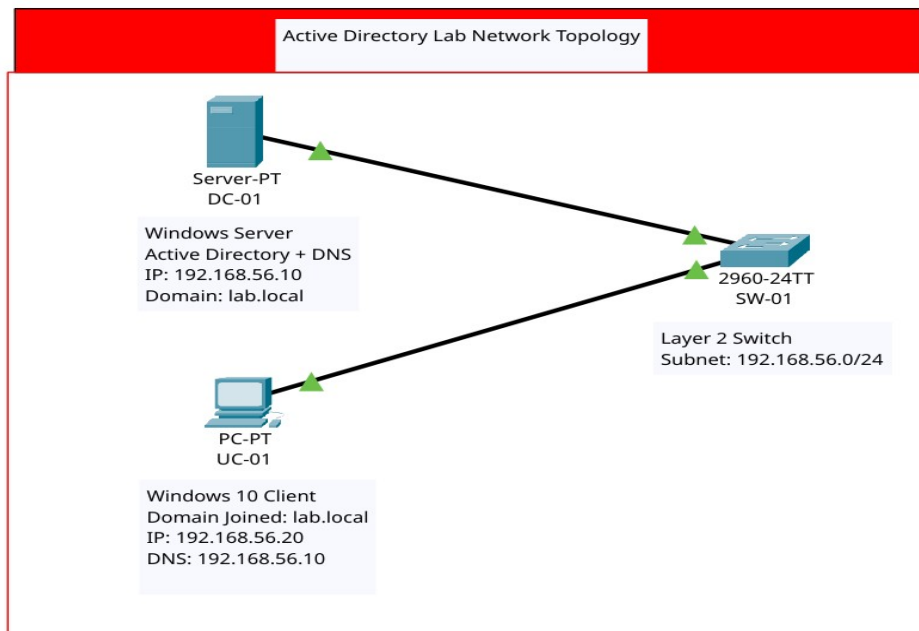
Active Directory (AD) is a directory service developed by Microsoft that enables centralized management of users, computers, and security policies within a Windows domain environment.

It allows:

- User authentication
- Authorization
- Centralized password management
- Device management
- Domain-based login



2 Lab Environment Setup



Virtualization Platform:

- Oracle VirtualBox
- Operating Systems Used:
- Windows Server (Domain Controller)
- Windows 10 Pro (Client Machine)

Network Configuration:

- Both machines configured on the same Host-Only network
- Same subnet (192.168.56.0/24)

3 Domain Controller Configuration

Server Setup Steps:

- Installed Windows Server
- Renamed server to: **DC-01**
- Promoted server to Domain Controller
- Created domain: **lab.local**

(In a company environment, this would reflect the company's real domain name.)

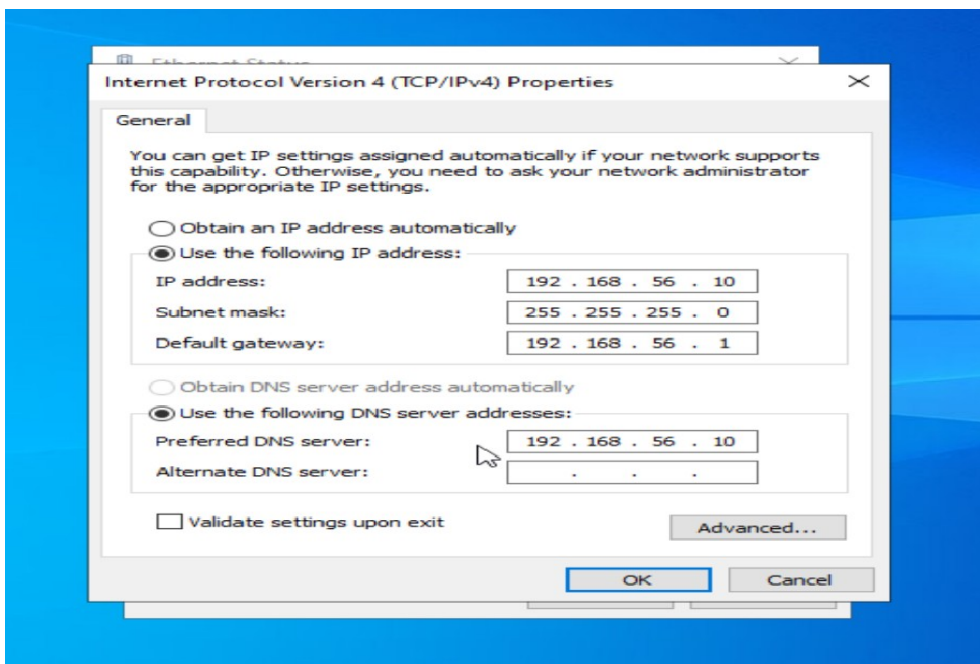
4 Static IP Configuration (Important Concept)

A static IP was configured on the Domain Controller:

IP Address: 192.168.56.10s
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.56.1
Preferred DNS: 192.168.56.10

Reason: Clients must use a stable DNS server to locate the Domain Controller.

Without static IP, domain join fails because DNS records may change on DHCP IP configuration settings.



5 User Creation in Active Directory

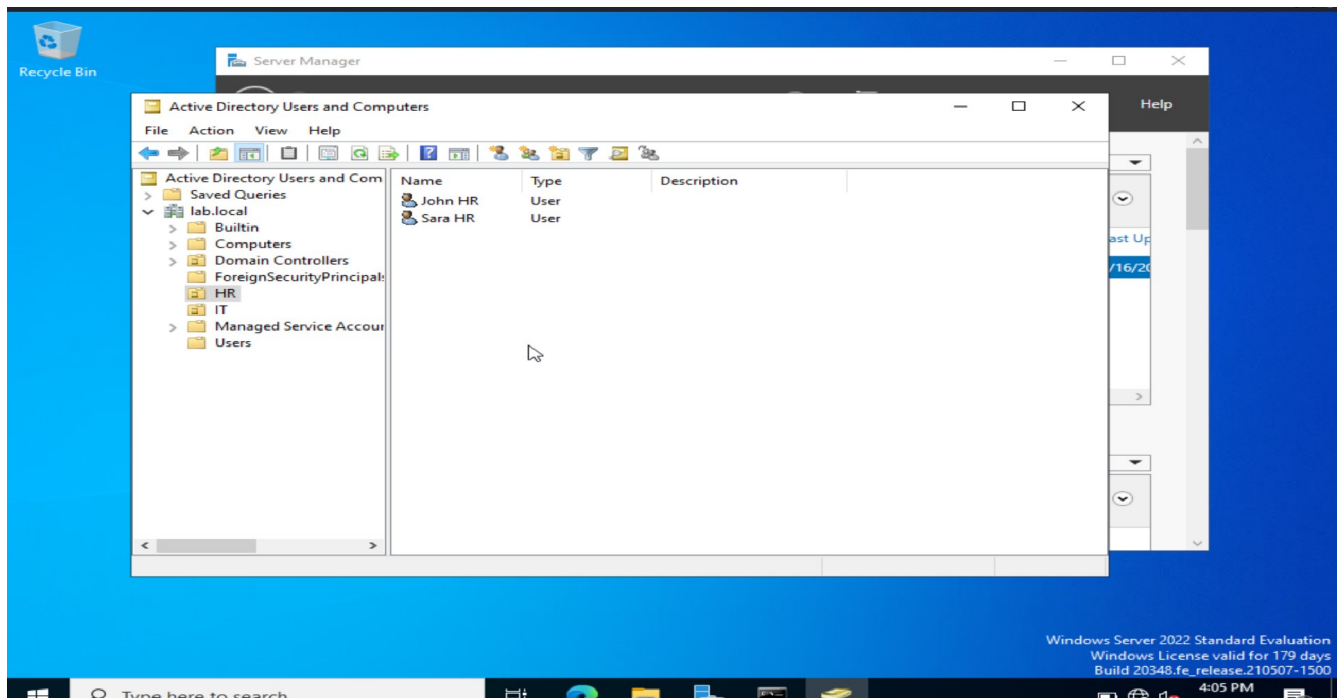
Using Active Directory Users and Computers:

Created users such as:

- Ahmed.it
- Sara.hr

Password policy considerations:

- Strong password format
- Minimum complexity
- Following basic IT security best practices (SOP mindset)



6 Client Machine Configuration (Windows 10)

Steps Performed:

- Renamed computer to: UC-01
- Configured network settings
- Set Preferred DNS to: 192.168.56.10
- Verified connectivity using:

```
C:\Windows\system32\cmd.exe

C:\Users\suhai>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\suhai>nslookup lab.local
DNS request timed out.
    timeout was 2 seconds.
Server:      Unknown
Address:     192.168.56.10

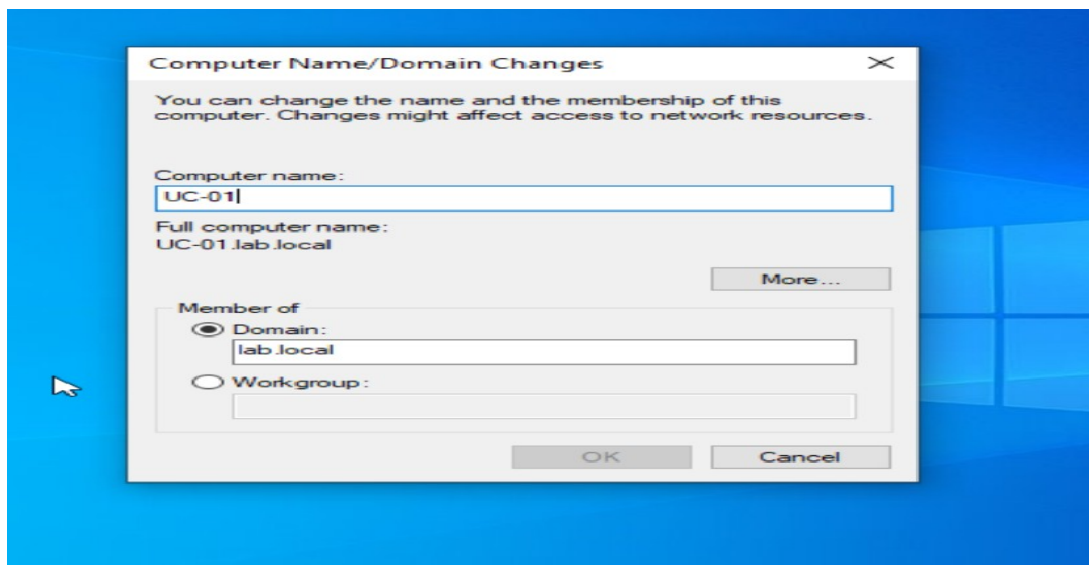
Name:       lab.local
Address:    192.168.56.10

C:\Users\suhai>
```

ping 192.168.56.10 server, connectivity successful.

7 Domain Join Process

- Opened Advanced Settings on Client Machine
- Selected "Computer Name Properties"
- Joined domain: lab.local
- Entered Domain Administrator credentials

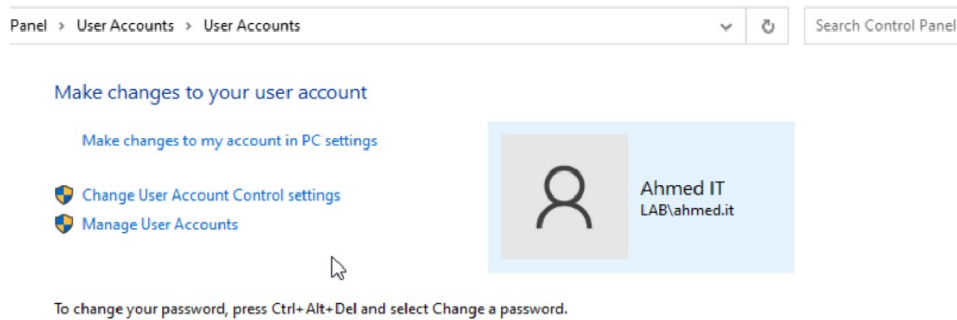


- Restarted machine

After restart:

Successfully logged in using:

lab\Ahmed.it
lab\Sara.hr



8 Account Management & Security Testing

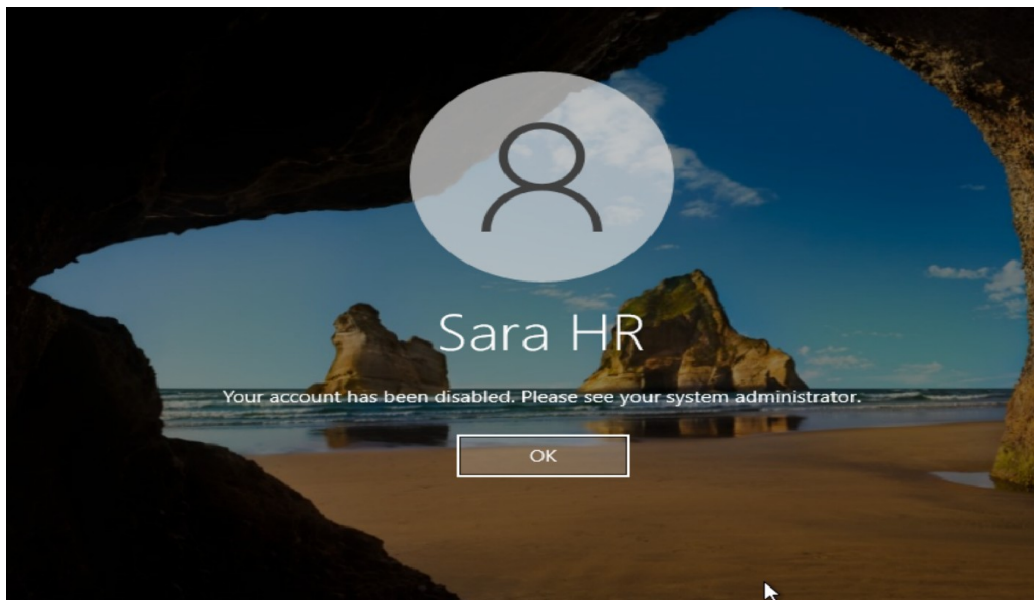
Test: Disable User Account Sara

Objective:

Verify that disabling a user account in Active Directory prevents authentication.

Steps Performed:

1. Logged in as lab\Sara.hr on Windows 10.
2. On Domain Controller (DC-01), opened Active Directory Users and Computers.
3. Right-clicked user Sara → Selected **Disable Account**.
4. Logged out from Windows 10.
5. Attempted login again using lab\Sara.hr.

**Result:**

System returned error:

“The account has been disabled. Please see your system administrator.”
