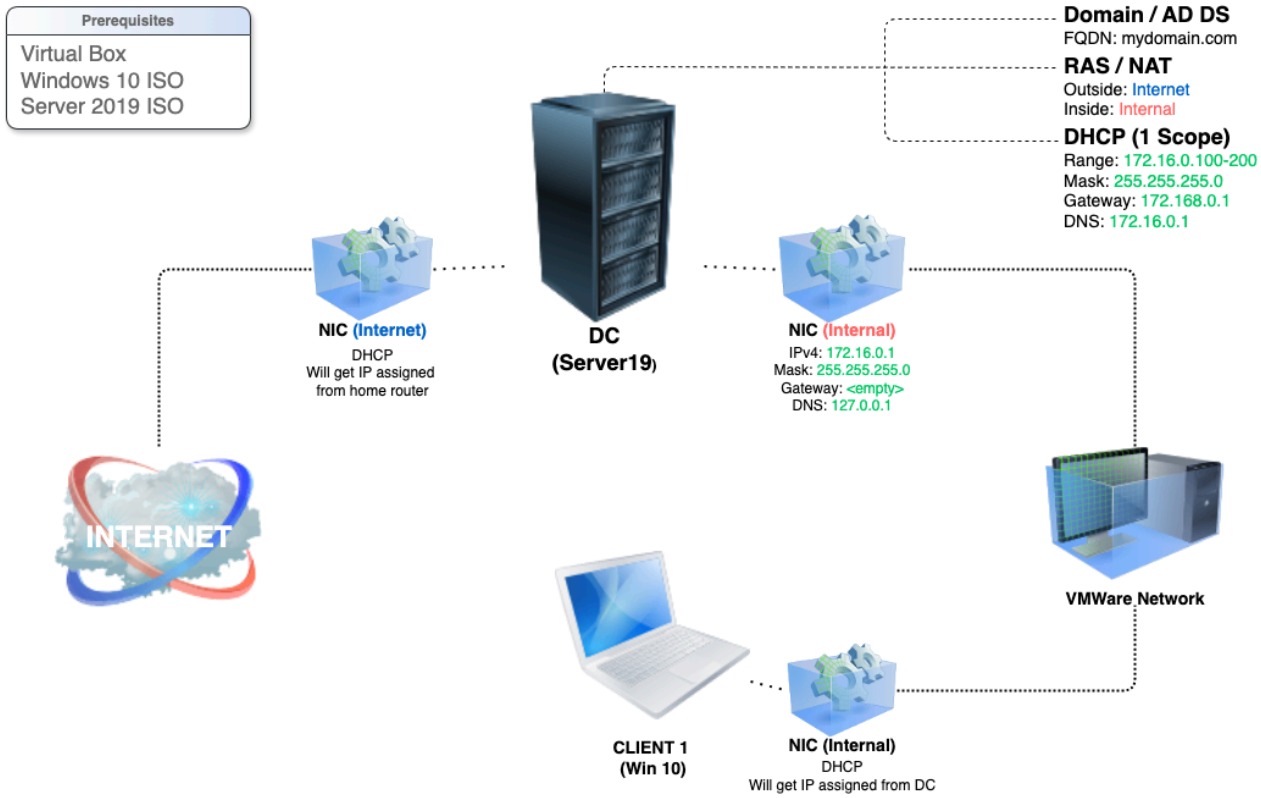
Active Directory Lab - Step by Step Guide



Introduction

This guide will walk you through setting up an Active Directory (AD) lab using Oracle VirtualBox, Windows Server 2019, and Windows 10. The lab will include a Domain Controller (DC), a Windows 10 client machine, and a configured network with DHCP, NAT, and Remote Access Service (RAS).

Step 1 - Preparation

Download Required Software:

- ★ Oracle VirtualBox: Download here
- ★ VirtualBox Extension Pack: Download here
- ★ Windows 10 ISO: Download here
- ★ Windows Server 2019 ISO: Download here

Overview:

Windows Server 2019 will function as the Domain Controller (DC) with Active Directory (AD) installed. It will have two network interfaces:

- ➔ One for Internet access
- ➔ One for internal network communication

Step 2 - Create Virtual Machine (Domain Controller)

- ➔ Open VirtualBox > Click New.
- ➔ Set the following:
  - ◆ Name: DC
  - ◆ Version: Other Windows (64-bit)
  - ◆ RAM: 2048MB
  - ◆ Processors: 1 or 2
  - ◆ Hard Disk: Create a virtual hard disk now > 20GB (25+ is recommended)
- ➔ Click Finish.

Configure Virtual Machine Settings:

- ➔ Settings > General > Advanced:
  - ◆ Shared Clipboard: Bidirectional
  - ◆ Drag and Drop: Bidirectional
- ➔ Settings > Network:
  - ◆ Adapter 1: NAT (default for internet access)
  - ◆ Adapter 2: Internal Network
- ➔ Click OK.

Install Windows Server 2019:

- ➔ Start the VM, select Windows Server 2019 ISO, and install:
  - ◆ Select Windows Server 2019 (Desktop Experience).
  - ◆ Choose Custom: Install Windows Only (Advanced).
  - ◆ Wait for the installation to complete.
  - ◆ Set an Administrator password.

Step 3 - Configure Domain Controller (DC)

Install VirtualBox Guest Additions (For better performance):

- ➔ Devices > Insert Guest Additions CD Image.
- ➔ Open This PC > CD Drive (D:) > VBoxWindowsAdditions-amd64.
- ➔ Run Install and restart.

Network Configuration:

- ➔ Rename Network Adapters:
  - ◆ Open Network Connections (ncpa.cpl)
  - ◆ Identify the internal adapter (APIPA 169.254.x.x address)
  - ◆ Rename it to _INTERNAL_
  - ◆ Rename the internet-facing adapter to _INTERNET_
- ➔ Assign Static IP (Internal Network Adapter):
  - ◆ IP Address: 172.16.0.1
  - ◆ Subnet Mask: 255.255.255.0
  - ◆ Gateway: (leave blank)
  - ◆ DNS: 127.0.0.1
- ➔ Rename the Server:
  - ◆ Settings > System > Rename this PC > DC > Restart.

Step 4 - Install and Configure Active Directory (AD DS)

- ➔ Server Manager > Add roles and features.
- ➔ Select Active Directory Domain Services (AD DS) > Add Features.
- ➔ Complete installation and click Promote this server to a domain controller.
- ➔ Create New Forest:
  - ◆ Root Domain Name: mydomain.com
  - ◆ Set DSRM Password: Password1
  - ◆ Click Install and restart.
- ➔ Login using:
  - ◆ User: MYDOMAIN\Administrator
  - ◆ Password: Password1

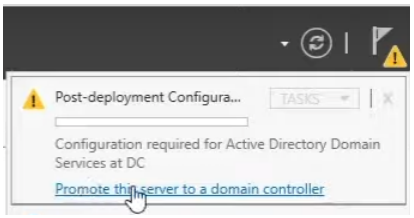
Step 5: Setup DHCP Server on DC

This will allow the client to automatically receive an IP address from the **Domain Controller (DC)** to connect to the network and access the internet.

Install the DHCP Role:

➔ Open Server Manager
- ◆ Go to Manage > Add Roles and Features
- ◆ Click Next until you reach Server Roles
- ◆ Select DHCP Server > Click Add Features when prompted
- ◆ Click Next > Next > Install

➔ Wait for the installation to complete, then click Close



Configure DHCP Server:

➔ In Server Manager, click the Notification Bell (top-right) > Complete DHCP Configuration

➔ Click Next > Use AD Credentials > Commit > Close

Create a New Scope:

➔ Open Server Manager > Go to Tools > DHCP
- ◆ Expand dc.mydomain.com > Right-click IPv4 > New Scope > Next
- ◆ Scope Name: 172.16.0.100-200 > Next
- ◆ Start IP Address: 172.16.0.100
- ◆ End IP Address: 172.16.0.200
- ◆ Subnet Mask: 255.255.255.0 (Length: 24) > Next
- ◆ Router (Default Gateway):
  - IP Address: 172.16.0.1
  - Click Add > Next

➔ DNS Settings: Ensure 172.16.0.1 is listed as the DNS Server > Next

➔ Activate Scope: Select Yes, activate now > Next > Finish

Authorize DHCP Server:

➔ In DHCP Console, right-click dc.mydomain.com > Authorize

➔ Right-click again > Refresh

➔ Expand IPv4 > Confirm the scope is Active

DHCP is now set up, and clients can receive IPs automatically.

Step 6: Install & Configure NAT for Internet Access

- ➔ Open Server Manager > Add Roles and Features
  - ◆ Select Remote Access > Routing > Install
  - ◆ Open Routing and Remote Access (Tools > Routing)
  - ◆ Right-click `DC (local)` > Configure & Enable
  - ◆ Select Remote Access > Next
- ➔ Select INTERNET interface > Finish

Step 7 - Create an Admin Account in AD

- ➔ Open Active Directory Users and Computers.
- ➔ Create a New User:
  - ◆ Name: AdminUser
  - ◆ Username: AdminUser
  - ◆ Password: Password1 (Change later!)
  - ◆ Set: Password never expires.
- ➔ Add to Administrators Group:
  - ◆ Right-click User > Properties > Member Of > Add.
  - ◆ Enter: Administrators > Apply.

Step 8 - Configure Windows 10 Client

- ➔ Create the VM:
- ➔ Open VirtualBox > Click New.
  - ◆ Name: Client
  - ◆ RAM: 2048MB
  - ◆ Network: Internal Network
  - ◆ Enable Drag & Drop and Shared Clipboard (Bidirectional).
- ➔ Install Windows 10:
  - ◆ Attach Windows 10 ISO and Start the VM.
  - ◆ Select Windows 10 Pro (Home edition cannot join a domain).
- ➔ Follow installation prompts, but choose:
  - ◆ Skip internet setup (use "Limited setup").
  - ◆ Username: User (No password).
- ➔ Open CMD (Win + R > cmd) & Run:
  - ◆ ipconfig
  - ◆ If no default gateway, check DHCP config on DC.
  - ◆ Ping 8.8.8.8 to test internet.

Join Domain:

- ➔ Right-click Start > System > Rename this PC (Advanced settings).
- ➔ Change Settings > Computer Name > Domain: mydomain.com.
- ➔ Enter AdminUser Credentials: MYDOMAIN\AdminUser.
- ➔ Restart & Login with Domain Account.

Step 8 - Troubleshooting

Common Issues:

- ★ No Default Gateway? Ensure DHCP is assigning 172.16.0.1 in Server Manager > DHCP.
- ★ Client Cannot Join Domain? Check DC's firewall settings and IP configuration.
- ★ No Internet on Internal Network? Ensure NAT & Routing are correctly set up in Routing and Remote Access.
- ★ Cannot Ping 8.8.8.8? Check Windows Firewall & NAT Rules.

Conclusion

This lab provides a fully functional Active Directory environment, allowing you to practice user management, group policies, and networking in a controlled virtualized setup.

Credits

Guide By Nicolas Cordischi

This lab was inspired by Josh Madakor's Active Directory series. You can check out his tutorials here:
Josh Madakor - Active Directory Lab

Big thanks to Josh for his detailed walkthroughs!