**Active Directory & LDAP Implementation – Step-by-Step Guide**

**Table of Contents**

1. Introduction
2. Setting Up a Virtual Machine
3. Installing Windows Server
4. Deploying & Configuring Active Directory (AD)
5. Enabling Remote Desktop (RDP)
6. Setting Up Group Policies
7. Securing AD for Public Access
8. Configuring Networking for Remote Access
9. Setting Up LDAP & Integration
10. Troubleshooting Guide

**1. Introduction**

This guide walks you through setting up a Windows Server with Active Directory (AD), configuring Remote Desktop (RDP), enforcing security policies, enabling LDAP authentication, and securing remote access in the easiest way possible.

**System Requirements**

* **Windows Server:** 2022
* **Virtualization Software:** VirtualBox
* **Hardware:** Minimum 4GB RAM & 2 CPU cores
* **Administrator Access:** Required for security configurations

**2. Setting Up a Virtual Machine**

**Step 1: Create a Virtual Machine (VM)**

1. Open VirtualBox, VMware, or Hyper-V.
2. Click **New** and name the VM (e.g., Active\_dir\_env).
3. Choose **Windows Server 2019/2022** as the OS type.
4. Assign **4GB RAM** and **2 CPU cores**.
5. Create a **50GB+ virtual hard disk**.
6. Attach the Windows Server ISO file and boot the VM.

**3. Installing Windows Server**

**Step 1: Installation**

1. Boot from the Windows Server ISO.
2. Choose your **language, time zone, and keyboard settings**.
3. Click **Install Now**.
4. Select **Windows Server Standard (with GUI)**.
5. Partition the disk and complete the installation.
6. Set an **Administrator password**.

**Step 2: Basic Configurations**

1. Log in as Administrator.
2. Open **Server Manager**.
3. Set a **static IP address**.
4. Rename the computer (e.g., Domain-Controller).
5. Enable **Remote Desktop (RDP)**.
6. Restart the server.

**4. Deploying & Configuring Active Directory (AD)**

**Step 1: Install AD DS (Active Directory Domain Services)**

1. Open **Server Manager > Add Roles and Features**.
2. Choose **Role-based Installation**.
3. Select **Active Directory Domain Services (AD DS)**.
4. Install **DNS & Group Policy** (required features).
5. After installation, click **Promote this server to a domain controller**.

**Step 2: Configure the Domain Controller**

1. Choose **Add a new forest** (e.g., test.local).
2. Set **Forest Functional Level** to Windows Server 2016/2019.
3. Configure a **Directory Services Restore Mode (DSRM) password**.
4. Allow **DNS installation & replication settings**.
5. Complete configuration and **restart the server**.

**Step 3: Verify AD Installation**

1. Open **Active Directory Users and Computers (ADUC)**.
2. Confirm the **domain controller** is listed (DC=test,DC=local).
3. Test using Command Prompt:
4. nslookup test.local

**5. Enabling Remote Desktop (RDP)**

**Step 1: Enable RDP**

1. Open **System Properties (sysdm.cpl) or can also be accessed in server manager**.
2. Navigate to **Remote > Allow Remote Connections**.
3. Open **Windows Firewall** and allow RDP (port **3389**).

**Step 2: Test RDP Connection**

1. From a client machine, open **Remote Desktop (mstsc or mstsc.exe)**.
2. Enter the **AD-Server’s IP/Hostname(**domain-controller.test.local)
3. Log in using Administrator credentials.

**6. Setting Up Group Policies (GPOs)**

**Step 1: Create & Configure GPOs**

1. Open **Group Policy Management** in Server Manager.
2. Right-click your domain (test.local) and create a new GPO (e.g., SecurityPolicy).
3. Edit the GPO to enforce password policies, firewall rules, and restrictions.

**Step 2: Apply Security Settings**

1. Open **GPO Editor**.
2. Navigate to **Computer Configuration > Windows Settings > Security Settings**.
3. Modify **Password Policy, User Rights Assignment, and Firewall Rules**.
4. Link the GPO to **Organizational Units (OUs) that I have create and which is called employees**.
5. Apply changes

**7. Securing AD for Public Access**

**Step 1: Disable Anonymous Access in LDAP configuration**

**Step 2: Enforce Secure Authentication (LDAPS)**

1. Install an **SSL certificate** on the domain controller.
2. Enable **LDAPS (port 636)** for secure queries.
3. Restrict **public access** to sensitive AD objects.

**8. Configuring Networking for Remote Access**

**Step 1: Set Static IP for AD Server**

1. Open **Network & Internet Settings**.
2. Assign **Static IP (e.g., 192.168.1.10)**.
3. Set **DNS Server** to **127.0.0.1** (self-reference) or 192.168.1.10.

**Step 2: Configure Firewall Rules**

1. Open **Windows Firewall > Inbound Rules**.
2. Allow connections on:
   * **RDP (3389)**
   * **LDAPS (636)**
   * **LDAP (389)**

**9. Setting Up LDAP & Integration**

**Step 1: Verify LDAP Service**

Test if LDAP is running:

netstat -an | findstr ":389"

**Step 2: Enable LDAPS (LDAP over SSL)**

1. Install **Active Directory Certificate Services (AD CS)**.
2. Generate an **SSL Certificate** for LDAP.
3. Verify LDAPS:
4. netstat -an | findstr ":636"

**Step 3: Configure LDAP Authentication**

* **LDAP Server URL:** ldap://192.168.1.10:389
* **Base DN:** DC=test,DC=local
* **Bind DN:** CN=Administrator,CN=Users,DC=test,DC=local

**Step 4: Test LDAP Connection**

Using LDP.exe:

1. Open **LDP.exe**.
2. Connect to the **server IP on port 389/636**.
3. Authenticate using **Administrator credentials**.

Using PowerShell:

Test-NetConnection -ComputerName domain-controller.test.local -Port 389

**10. Troubleshooting Guide**

| **Issue** | **Cause** | **Solution** |
| --- | --- | --- |
| Cannot connect via LDAP | Firewall blocking port 389/636 | Open necessary ports |
| LDAPS not working | SSL certificate missing | Install a valid SSL certificate |
| Users cannot log in via LDAP | Incorrect Bind DN | Verify credentials in LDAP settings |
| Remote Desktop not connecting | RDP disabled | Enable RDP and allow firewall access |

**Checking Event Logs for Errors**

1. Open **Event Viewer**.
2. Navigate to **Applications and Services Logs > Directory Service**.
3. Look for **LDAP or AD-related errors**.

**Conclusion**

This guide covers everything I needed to set up Active Directory, configure security settings, and enable LDAP authentication. By following these steps, I ensure a **secure, well-managed, and efficient** AD environment.

Note that all of these steps has screenshots and detailed videos of the connection of the User **Nils** through RDP with another vm hosting windows 10 pro and connected to the same internal network as the AD server that it uses as a dhcp server to assign an Ip address to itself, the configuration step for the dhcp server is detailed in the screenshots.

**PROBLEMS**:

Could not create a second server for a new AD environment because of lack of resources also Hyper-V enabling could not work because the server was on a virtual machine and accessing the BIOS to enable it was no possible, I tried the parallel solution directly through the vm with no success as you can see in the images down

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.