Active Directory Lab

Complete Step-by-Step Guide

Building Enterprise Windows Infrastructure for Cybersecurity Professionals

Lab Duration:	4-6 hours
Difficulty:	Intermediate
Prerequisites:	Basic networking knowledge
Resume Value:	High - Enterprise Windows Administration

Created: November 2025

Table of Contents

1. Introduction & Lab Overview

This comprehensive Active Directory lab will teach you enterprise Windows Server administration and directory services - critical skills for cybersecurity roles, system administration, and IT infrastructure positions. By completing this lab, you'll gain hands-on experience with technologies used by 95% of Fortune 500 companies.

What You'll Learn

- Windows Server 2022 installation and configuration
- Active Directory Domain Services (AD DS) deployment
- User and group management at enterprise scale
- Organizational Unit (OU) design and implementation
- Group Policy Object (GPO) creation and application
- Domain Name System (DNS) configuration for AD
- Dynamic Host Configuration Protocol (DHCP) integration
- Security hardening and baseline configurations
- Event log monitoring and security auditing
- PowerShell automation for AD administration

Why This Lab Matters for Your Career

Active Directory is the backbone of enterprise IT infrastructure. Understanding AD is essential for:

- **Cybersecurity Roles:** SOC analysts, incident responders, and security engineers must understand AD to detect attacks, respond to breaches, and implement security controls
- **System Administration:** Managing users, computers, and policies across hundreds or thousands of devices
- **IT Support:** Troubleshooting authentication, permissions, and access issues
- **Cloud Transition:** Understanding on-premises AD prepares you for Azure AD and hybrid environments

> ***NOTE:*** *This lab uses freely available evaluation versions of Windows Server. Everything you build here is legitimate experience that belongs on your resume.*

2. Lab Architecture & Requirements

Lab Network Diagram

Our lab environment consists of three virtual machines on an isolated network:

<b>VM Name</b>	<b>Role</b>	<b>OS</b>	<b>RAM</b>	<b>IP Address</b>
DC01	Domain Controller	Windows Server 2022	4 GB	192.168.10.10
CLIENT01	Windows Workstation	Windows 10/11	4 GB	192.168.10.20 (DHCP)
CLIENT02	Windows Workstation	Windows 10/11	2 GB	192.168.10.21 (DHCP)

Required Software & Downloads

All software used in this lab is freely available for evaluation or educational use:

- **Virtualization Platform:** VMware Workstation Player (Free), VirtualBox (Free), or VMware Fusion (Mac)
- **Windows Server 2022:** 180-day evaluation ISO from Microsoft Evaluation Center
- **Windows 10/11:** Free development VMs from Microsoft or personal Windows installation
- **Disk Space:** Minimum 80 GB free space (100 GB recommended)

Download Links

Visit these official Microsoft links to download:

```
Windows Server 2022 Evaluation:
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022 Windows 10
Development Environment:
https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/ VMware
Workstation Player (Windows/Linux):
https://www.vmware.com/products/workstation-player.html VirtualBox (All Platforms):
https://www.virtualbox.org/wiki/Downloads
```

IMPORTANT: Evaluation versions are fully functional for 180 days. This gives you plenty of time to complete the lab and include it on your resume before expiration.

3. Phase 1: Domain Controller Setup

The Domain Controller (DC) is the heart of your Active Directory environment. It handles authentication, authorization, and provides directory services to all domain members.

Step 3.1: Create Domain Controller VM

1. Open your virtualization software (VMware or VirtualBox)
2. Create new virtual machine named 'DC01'
3. Select Windows Server 2022 ISO as installation media
4. Allocate 4 GB RAM (minimum 2 GB)
5. Create 60 GB virtual hard disk
6. Configure network adapter as 'Host-Only' or 'Internal Network'
7. Start the VM and begin Windows Server installation

Step 3.2: Install Windows Server 2022

During installation, choose **Windows Server 2022 Standard Evaluation (Desktop Experience)** to get the GUI interface. The Desktop Experience option is crucial for learning - it provides the familiar Windows interface.

1. Boot from Windows Server 2022 ISO
2. Select language, time, and keyboard preferences
3. Click 'Install Now'
4. Choose 'Windows Server 2022 Standard Evaluation (Desktop Experience)'
5. Accept license terms
6. Select 'Custom: Install Windows only (advanced)'
7. Choose the virtual disk and click Next
8. Wait for installation to complete (10-15 minutes)
9. Set Administrator password when prompted (use a strong password you'll remember)

ADMINISTRATOR PASSWORD: Choose something secure but memorable for this lab environment. Example: P@ssw0rd2024Lab (Do NOT use this in production!)

Step 3.3: Initial Server Configuration

After logging in for the first time, Server Manager will launch automatically. We need to configure basic settings before promoting this server to a Domain Controller.

Configure Static IP Address:

1. Click Start > Settings > Network & Internet
2. Click 'Change adapter options'

3. Right-click your network adapter > Properties
4. Select 'Internet Protocol Version 4 (TCP/IPv4)' > Properties
5. Select 'Use the following IP address' and enter:

```
IP Address: 192.168.10.10 Subnet Mask: 255.255.255.0 Default Gateway: (leave blank for
isolated lab) Preferred DNS: 127.0.0.1 Alternate DNS: (leave blank)
```

6. Click OK to apply settings

Rename the Server:

1. In Server Manager, click on the computer name under 'Properties'
2. Click 'Change' button
3. Enter 'DC01' as the computer name
4. Click OK, then restart when prompted

> ***✓ CHECKPOINT:*** *At this point, you should have a Windows Server 2022 machine named DC01 with IP address 192.168.10.10. The server should restart and you'll log back in as Administrator.*

4. Phase 2: Active Directory Domain Services

Now we'll install Active Directory Domain Services and promote our server to a Domain Controller. This is where your Windows Server becomes the authentication hub for your entire network.

Step 4.1: Install AD DS Role

1. Open Server Manager (should open automatically)
2. Click 'Add roles and features'
3. Click 'Next' on the Before You Begin page
4. Select 'Role-based or feature-based installation' > Next
5. Select your server (DC01) > Next
6. Check the box for 'Active Directory Domain Services'
7. In the popup, click 'Add Features' to include management tools
8. Click Next through Features, AD DS, and Confirmation pages
9. Click 'Install' and wait for completion (5-10 minutes)
10. Click 'Close' when installation completes

Step 4.2: Promote Server to Domain Controller

Installing the AD DS role only adds the software - now we need to configure it and create our domain.

1. In Server Manager, click the yellow notification flag (top right)
2. Click 'Promote this server to a domain controller'
3. Select 'Add a new forest'
4. Enter 'cyberlab.local' as the Root domain name
5. Click Next

> ***DOMAIN NAME CHOICE:*** *We use 'cyberlab.local' as our domain name. The .local TLD is traditional for internal networks. You could also use cyber.lab or security.internal - just stay consistent throughout the lab.*

Domain Controller Options:

1. Leave 'Forest functional level' as 'Windows Server 2016'
2. Leave 'Domain functional level' as 'Windows Server 2016'
3. Ensure 'Domain Name System (DNS) server' is checked
4. Ensure 'Global Catalog (GC)' is checked
5. Enter Directory Services Restore Mode (DSRM) password
6. (Use the same password as Administrator for this lab)
7. Click Next

Continue the Wizard:

1. DNS Options page: Click Next (NetBIOS name will be CYBERLAB)
2. Paths page: Accept default paths > Next
3. Review Options: Click Next
4. Prerequisites Check: Wait for validation (ignore DNS warnings)
5. Click 'Install' to begin promotion
6. Server will restart automatically after 10-15 minutes

AFTER RESTART: *Your login screen will now show 'CYBERLAB\Administrator' instead of just 'Administrator'. This confirms your domain is active! Use the same password to log in.*

Step 4.3: Verify Active Directory Installation

Let's confirm everything is working correctly:

1. Open Server Manager
2. Click Tools > Active Directory Users and Computers
3. Expand 'cyberlab.local' in the left pane
4. You should see default containers: Computers, Domain Controllers, Users, etc.
5. Click on 'Domain Controllers' - you should see DC01 listed
6. Click on 'Users' - you should see Administrator and other built-in accounts

✓ CHECKPOINT: *Congratulations! You now have a functioning Active Directory domain called cyberlab.local with one Domain Controller (DC01). This is enterprise-grade infrastructure!*

5. Phase 3: Organizational Structure Design

Organizational Units (OUs) are containers that organize users, computers, and groups. A well-designed OU structure makes it easier to apply Group Policies and delegate administrative tasks - critical for enterprise environments.

Step 5.1: Create Organizational Unit Structure

We'll create a realistic OU structure mimicking a small business:

```
cyberlab.local/ ■■■ CyberLab_Computers ■ ■■■ Workstations ■ ■■■ Laptops ■ ■■■
Servers ■■■ CyberLab_Users ■ ■■■ IT_Department ■ ■■■ Security_Team ■ ■■■
HR_Department ■ ■■■ Sales_Department ■■■ CyberLab_Groups
```

Creating OUs in Active Directory:

1. Open Server Manager > Tools > Active Directory Users and Computers
2. Right-click on 'cyberlab.local' > New > Organizational Unit
3. Name it 'CyberLab_Users' > OK
4. Repeat to create 'CyberLab_Computers' and 'CyberLab_Groups'

Creating Sub-OUs:

1. Right-click 'CyberLab_Users' > New > Organizational Unit
2. Create: IT_Department, Security_Team, HR_Department, Sales_Department
3. Right-click 'CyberLab_Computers' > New > Organizational Unit
4. Create: Workstations, Laptops, Servers

OU DESIGN TIP: *In real environments, OUs are often organized by location, department, or function. This structure allows granular control over security policies and administrative delegation.*

Step 5.2: Create User Accounts

Now we'll populate our directory with users. In enterprise environments, this would typically be done via PowerShell or automated imports, but we'll start manually to understand the process.

1. Navigate to CyberLab_Users > IT_Department
2. Right-click in the right pane > New > User
3. Fill in the form:

```
First name: John Last name: Smith User logon name: jsmith
```

4. Click Next
5. Enter password (example: CyberLab2024!)
6. Uncheck 'User must change password at next logon'

7. Check 'Password never expires' (for lab purposes only!)
8. Click Next > Finish

Create Additional Users:

Repeat the process to create these additional users in their respective departments:

<b>Name</b>	<b>Username</b>	<b>Department OU</b>
Jane Doe	jdoe	Security_Team
Mike Johnson	mjohnson	IT_Department
Sarah Williams	swilliams	HR_Department
Tom Brown	tbrown	Sales_Department
Emily Davis	edavis	Security_Team

Step 5.3: Create Security Groups

Security groups simplify permission management. Instead of assigning rights to individual users, we assign them to groups and add users as members.

1. Navigate to CyberLab_Groups
2. Right-click in the right pane > New > Group
3. Group name: IT_Admins
4. Group scope: Global
5. Group type: Security
6. Click OK

Create These Additional Groups:

- Security_Analysts (in CyberLab_Groups)
- HR_Staff (in CyberLab_Groups)
- Sales_Team (in CyberLab_Groups)
- Remote_Workers (in CyberLab_Groups)

Add Users to Groups:

1. Right-click the 'IT_Admins' group > Properties
2. Click the Members tab > Add button
3. Type 'jsmith' and click Check Names
4. Click OK to add John Smith
5. Repeat to add 'mjohnson' (Mike Johnson)
6. Click OK to save

Complete these group memberships:

- Security_Analysts: jdoe, edavis
- HR_Staff: swilliams
- Sales_Team: tbrown

✓ ***CHECKPOINT:*** *You now have a properly structured Active Directory with OUs, user accounts, and security groups. This mirrors real enterprise design!*

6. Phase 4: Client Workstation Integration

Now we'll create Windows 10/11 client machines and join them to the domain. This demonstrates how end-user devices integrate into an Active Directory environment.

Step 6.1: Configure DHCP on Domain Controller

First, let's set up DHCP so our client machines get IP addresses automatically:

1. On DC01, open Server Manager
2. Click 'Add roles and features'
3. Next through to Server Roles
4. Check 'DHCP Server'
5. Add Features > Next > Next > Next > Install
6. After installation, click 'Complete DHCP configuration'
7. Click Commit > Close

Create DHCP Scope:

1. Server Manager > Tools > DHCP
2. Expand DC01 > Right-click IPv4 > New Scope
3. Name: CyberLab_Scope > Next
4. Start IP: 192.168.10.100
5. End IP: 192.168.10.200
6. Subnet mask: 255.255.255.0 > Next
7. Add no exclusions > Next
8. Lease duration: 8 hours (default) > Next
9. Select 'Yes, I want to configure these options now' > Next
10. Router (Default Gateway): 192.168.10.10 > Add > Next
11. Parent Domain: cyberlab.local (already filled) > Next
12. WINS Servers: Skip > Next
13. Activate scope now: Yes > Next > Finish

> ***DHCP CONFIGURATION:*** *Our scope provides IPs from .100-.200, leaving .1-.99 for static assignments like servers and network devices. The DC acts as both DNS server and default gateway in our lab.*

Step 6.2: Create Windows Client VMs

1. Create new VM named 'CLIENT01' in your hypervisor
2. Allocate 4 GB RAM, 40 GB disk
3. Use same network adapter type as DC01 (Host-Only/Internal)
4. Install Windows 10 or Windows 11

5. Complete the Windows setup wizard
6. Skip Microsoft account creation (use local account)
7. Username: 'localadmin', strong password

WINDOWS VERSION: *Use Windows 10/11 Pro or Enterprise for domain-join capability. Home editions cannot join domains.*

Step 6.3: Join Client to Domain

1. On CLIENT01, click Start > Settings
2. Go to System > About
3. Click 'Rename this PC (advanced)'
4. Click 'Change' button
5. Computer name: CLIENT01
6. Select 'Domain' radio button
7. Enter: cyberlab.local
8. Click OK

Authentication Prompt: You'll be asked to provide credentials with permission to join the domain:

```
Username: CYBERLAB\Administrator Password: [Your Administrator password]
```

9. Click OK
10. You'll see 'Welcome to the cyberlab domain'
11. Click OK > OK
12. Restart the computer when prompted

Step 6.4: Verify Domain Join

1. After restart, click 'Other user' at login screen
2. Login as: jsmith
3. Password: CyberLab2024!
4. Domain should auto-fill as CYBERLAB

Verify on Domain Controller:

1. On DC01, open Active Directory Users and Computers
2. Navigate to Computers container (or CyberLab_Computers > Workstations)
3. You should see CLIENT01 listed
4. Move CLIENT01 to CyberLab_Computers > Workstations OU (drag and drop)

Optional: Create CLIENT02

Repeat steps 6.2-6.4 to create CLIENT02 for a more realistic multi-workstation environment. This is optional but helps demonstrate Group Policy application across multiple machines.

> ✓ ***CHECKPOINT:*** *You now have domain-joined Windows clients! Users can log in from any domain computer using their Active Directory credentials - this is the power of centralized authentication.*

7. Phase 5: Group Policy Implementation

Group Policy Objects (GPOs) are one of Active Directory's most powerful features. They allow centralized configuration management across all domain computers and users. This is where security policies, desktop settings, and software deployments are controlled.

Step 7.1: Create Password Policy GPO

Let's create a Group Policy to enforce strong password requirements:

1. On DC01, open Server Manager > Tools > Group Policy Management
2. Expand Forest > Domains > cyberlab.local
3. Right-click on cyberlab.local > Create a GPO in this domain, and Link it here
4. Name: Password Security Policy
5. Click OK

Configure Password Settings:

1. Right-click 'Password Security Policy' > Edit
2. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
3. Configure these settings:

```
Enforce password history: 12 passwords remembered Maximum password age: 90 days Minimum
password age: 1 day Minimum password length: 12 characters Password must meet complexity
requirements: Enabled Store passwords using reversible encryption: Disabled
```

4. Close the Group Policy Management Editor

Step 7.2: Create Desktop Restriction GPO

This GPO will restrict users from accessing Control Panel and Command Prompt:

1. In Group Policy Management, right-click CyberLab_Users > Create a GPO in this OU, and Link it here
2. Name: Desktop Restrictions
3. Right-click the new GPO > Edit
4. Navigate to: User Configuration > Policies > Administrative Templates > Control Panel
5. Double-click 'Prohibit access to Control Panel and PC settings'
6. Select 'Enabled' > OK
7. Navigate to: User Configuration > Policies > Administrative Templates > System
8. Double-click 'Prevent access to the command prompt'
9. Select 'Enabled' > OK
10. Close the editor

Step 7.3: Create Windows Firewall GPO

1. Create a new GPO linked to CyberLab_Computers: Windows Firewall Policy
2. Edit the GPO
3. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security
4. Right-click 'Windows Defender Firewall' > Properties
5. Domain Profile tab: Firewall state = On
6. Inbound connections = Block (default)
7. Outbound connections = Allow (default)
8. Click OK
9. Close the editor

Step 7.4: Create Screen Lock GPO

This enforces automatic screen locking after inactivity:

1. Create new GPO linked to cyberlab.local: Screen Lock Policy
2. Edit the GPO
3. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
4. Find 'Interactive logon: Machine inactivity limit'
5. Set to 900 seconds (15 minutes)
6. Navigate to: User Configuration > Policies > Administrative Templates > Control Panel > Personalization
7. Enable 'Enable screen saver' = Enabled
8. Set 'Screen saver timeout' = 900 seconds
9. Enable 'Password protect the screen saver' = Enabled

Step 7.5: Test Group Policy Application

On CLIENT01, force Group Policy update and verify settings:

1. On CLIENT01, log in as jsmith
2. Open PowerShell as Administrator
3. Run: gpupdate /force
4. Wait for completion
5. Run: gpresult /r to see applied policies
6. Restart CLIENT01 to apply all computer-based policies

Verify Policy Application:

1. Try to open Command Prompt - should be blocked
2. Try to open Control Panel - should be blocked

3. Check that Windows Firewall is enabled (Windows Security > Firewall)
4. Wait 15 minutes of inactivity - screen should lock

TROUBLESHOOTING GPOs: *If policies don't apply: • Run 'gpupdate /force' on the client • Ensure the computer is in the correct OU • Check GPO links in Group Policy Management • Review Event Viewer > Applications and Services Logs > Microsoft > Windows > GroupPolicy for errors*

✓ CHECKPOINT: *You've implemented enterprise-grade security controls using Group Policy! These policies enforce password requirements, desktop restrictions, firewall settings, and automatic screen locking across your entire domain.*

8. Phase 6: Security Hardening & Best Practices

Now we'll implement security hardening measures that demonstrate understanding of enterprise security principles. These configurations are critical in production Active Directory environments.

Step 8.1: Disable Guest Account

1. Open Active Directory Users and Computers
2. Click on Users container
3. Right-click 'Guest' account > Properties
4. Check 'Account is disabled'
5. Click OK

Step 8.2: Rename Administrator Account

Renaming the default Administrator account makes it harder for attackers to target:

1. In Active Directory Users and Computers
2. Right-click Administrator > Rename
3. Change to: Admin_CyberLab
4. Press Enter

Step 8.3: Create Least-Privilege Service Accounts

Service accounts should have minimal permissions:

1. Create new OU: Service_Accounts (under cyberlab.local)
2. Create new user: svc_backup
3. Set strong password
4. Check 'Password never expires' and 'User cannot change password'
5. Add description: 'Backup Service Account'
6. Do NOT add to Domain Admins or other privileged groups

Step 8.4: Configure Account Lockout Policy

1. Open Group Policy Management
2. Edit Default Domain Policy
3. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy
4. Configure:

```
Account lockout duration: 30 minutes Account lockout threshold: 5 invalid logon
attempts Reset account lockout counter after: 30 minutes
```

Step 8.5: Enable Audit Policies

Audit policies generate security event logs critical for incident response:

1. In Group Policy Management, edit Default Domain Policy
2. Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies
3. Configure these audit settings to 'Success and Failure':

- Account Logon > Audit Credential Validation
- Account Management > Audit Security Group Management
- Account Management > Audit User Account Management
- Logon/Logoff > Audit Logon
- Logon/Logoff > Audit Logoff
- Object Access > Audit File Share
- Policy Change > Audit Audit Policy Change
- Privilege Use > Audit Sensitive Privilege Use

Step 8.6: Implement Time-Based Access Control

Restrict when accounts can log in (useful for preventing after-hours unauthorized access):

1. In Active Directory Users and Computers
2. Right-click user 'tbrown' (Sales) > Properties
3. Go to Account tab
4. Click 'Logon Hours' button
5. By default, all hours are permitted
6. Select weekend hours (Saturday-Sunday) and click 'Logon Denied'
7. Select weekday hours before 8 AM and after 6 PM, click 'Logon Denied'
8. Click OK > OK

Step 8.7: Create Protected Users Group

The Protected Users group provides additional Kerberos protections:

1. In Active Directory Users and Computers
2. Navigate to Users container
3. Find the built-in 'Protected Users' group
4. Right-click > Properties > Members tab
5. Add your Security_Analysts group members (jdoe, edavis)
6. Click OK

PROTECTED USERS: *This group enforces strong Kerberos encryption, prevents NTLM authentication, and clears credentials from memory when users log off - critical protections against pass-the-hash attacks.*

✓ ***CHECKPOINT:*** *Your Active Directory is now hardened with industry best practices: disabled guest access, renamed admin account, account lockout policies, comprehensive auditing, time-based access controls, and protected user groups.*

9. Phase 7: Monitoring, Logging & PowerShell

Effective monitoring is crucial for detecting security incidents. We'll explore Event Viewer, configure logging, and use PowerShell for administrative automation - skills that directly apply to SOC analyst and security engineer roles.

Step 9.1: Explore Security Event Logs

1. On DC01, open Server Manager > Tools > Event Viewer
2. Expand Windows Logs > Security
3. Look for Event ID 4624 (successful logon)
4. Look for Event ID 4625 (failed logon)
5. Look for Event ID 4672 (special privileges assigned to new logon)
6. Double-click events to see details

<b>Event ID</b>	<b>Description</b>	<b>Security Significance</b>
4624	Successful Logon	Track user authentication
4625	Failed Logon	Detect brute force attempts
4720	User Account Created	Monitor unauthorized accounts
4722	User Account Enabled	Track account modifications
4738	User Account Changed	Detect permission escalation
4740	Account Lockout	Identify attack attempts

Step 9.2: PowerShell for AD Administration

PowerShell is the primary tool for Active Directory automation. Let's learn essential commands:

Basic AD PowerShell Commands:

```
# List all AD users Get-ADUser -Filter * | Select-Object Name, SamAccountName, Enabled #
List all computers in the domain Get-ADComputer -Filter * | Select-Object Name,
OperatingSystem # List all groups Get-ADGroup -Filter * | Select-Object Name,
GroupCategory # Get members of a group Get-ADGroupMember -Identity "IT_Admins" # Find
disabled user accounts Get-ADUser -Filter {Enabled -eq $false} | Select-Object Name,
SamAccountName # Search for users by name Get-ADUser -Filter {Name -like "*Smith*"}
```

Try These PowerShell Tasks:

1. Open PowerShell ISE on DC01
2. Import the Active Directory module: Import-Module ActiveDirectory
3. List all users in the IT_Department OU
4. Find all computers that haven't logged in for 30 days
5. Create a new user using New-ADUser

6. Export all user data to CSV using Export-Csv

Step 9.3: Create PowerShell Scripts

Create a script to generate a user report:

```
# AD User Report Script # File: UserReport.ps1 Import-Module ActiveDirectory $Users =
Get-ADUser -Filter * -Properties LastLogonDate, PasswordLastSet, Enabled ` |
Select-Object Name, SamAccountName, Enabled, LastLogonDate, PasswordLastSet $ReportPath
= "C:\Reports\AD_User_Report_$(Get-Date -Format 'yyyyMMdd').csv" $Users | Export-Csv
-Path $ReportPath -NoTypeInformation Write-Host "Report generated: $ReportPath"
Write-Host "Total users: $($Users.Count)"
```

Save and Run the Script:

1. Create C:\Reports directory on DC01
2. Open PowerShell ISE
3. Copy the script above
4. Save as C:\Scripts\UserReport.ps1
5. Run: Set-ExecutionPolicy RemoteSigned (if needed)
6. Execute: C:\Scripts\UserReport.ps1
7. Check C:\Reports for the generated CSV file

Step 9.4: Monitor Failed Logon Attempts

```
# Failed Logon Monitor Script # File: FailedLogonMonitor.ps1 $StartTime =
(Get-Date).AddHours(-24) $FailedLogons = Get-EventLog -LogName Security -After
$StartTime ` | Where-Object {$_.EventID -eq 4625} Write-Host "Failed logon attempts in
last 24 hours: $($FailedLogons.Count)" $FailedLogons | Select-Object TimeGenerated,
Message ` | Format-Table -AutoSize
```

✓ ***CHECKPOINT:*** *You can now monitor Active Directory through Event Viewer, use PowerShell for administration and reporting, and create automated scripts for security monitoring - essential skills for cybersecurity roles!*

10. Testing & Validation Scenarios

Let's validate your Active Directory configuration with realistic security testing scenarios. These tests demonstrate your understanding and provide talking points for interviews.

Test 1: Password Policy Enforcement

1. On CLIENT01, try to change jsmith's password to 'Password1'
2. Should fail - doesn't meet 12-character requirement
3. Try 'Pass1234567!' - should fail (too simple)
4. Try 'Cyb3rL@b!2024Secure' - should succeed
5. Verify in Event Viewer (Security log, Event ID 4723)

Test 2: Account Lockout Protection

1. On CLIENT01, log out
2. At login screen, enter wrong password for jsmith 5 times
3. Account should be locked after 5th failed attempt
4. On DC01, check Event Viewer for Event ID 4740 (account lockout)
5. In AD Users and Computers, verify jsmith account shows locked status
6. Wait 30 minutes or manually unlock the account

Test 3: Group Policy Application

1. Log into CLIENT01 as jsmith
2. Try to open Command Prompt - should be blocked
3. Try to access Control Panel - should be blocked
4. Check Windows Firewall status - should be enabled
5. Run 'gpresult /h C:\gpreport.html' in PowerShell
6. Open the HTML report to see all applied policies

Test 4: Time-Based Access Control

1. Temporarily change system time on CLIENT01 to Saturday
2. Try to log in as tbrown
3. Should be denied (we configured no weekend access)
4. Change time back to weekday outside 8 AM-6 PM
5. Login should still be denied
6. Change time to weekday, 2 PM - login should work

Test 5: Security Group Permissions

1. Create a shared folder on DC01: C:\SharedData
2. Right-click > Properties > Sharing > Share
3. Add 'IT_Admins' group with Full Control
4. Add 'Security_Analysts' group with Read access
5. Log into CLIENT01 as jsmith (IT_Admins member)
6. Access \\DC01\SharedData - should have full access
7. Log in as swilliams (not in either group)
8. Access should be denied

VALIDATION COMPLETE: *By completing these tests, you've verified that all security controls are functioning: • Password policies enforcing complexity • Account lockout protecting against brute force • Group Policies applying desktop restrictions • Time-based access controls working • Security group permissions properly configured • Audit logging capturing security events*

11. Resume Enhancement Guide

Now that you've built this Active Directory lab, let's translate it into resume-worthy content that stands out to hiring managers and passes ATS (Applicant Tracking Systems).

How to Add This Lab to Your Resume

Option 1: Technical Projects Section

Active Directory Enterprise Lab | Personal Project • Designed and deployed Windows Server 2022 Active Directory environment managing 6 user accounts across 4 departmental OUs with centralized authentication and directory services • Implemented Group Policy Objects (GPOs) enforcing password complexity (12+ characters), account lockout policies (5 attempt threshold), desktop restrictions, and Windows Firewall configurations across domain-joined workstations • Configured DHCP and DNS services supporting automated IP allocation and name resolution for domain infrastructure • Developed PowerShell automation scripts for user management, security auditing, and compliance reporting, reducing manual administrative tasks • Enabled comprehensive security audit logging (Event IDs 4624, 4625, 4720) for authentication monitoring and incident response capabilities • Applied enterprise security hardening including disabled guest accounts, renamed default administrator, Protected Users group, and time-based access controls

Option 2: Skills Section Keywords

Add these keywords to your technical skills section:

- Windows Server 2022 Administration
- Active Directory Domain Services (AD DS)
- Group Policy Object (GPO) Management
- PowerShell Scripting & Automation
- DHCP/DNS Configuration
- Security Auditing & Event Log Analysis
- Organizational Unit (OU) Design
- User & Group Management
- Windows Firewall Policy Implementation
- Enterprise Security Hardening

Interview Talking Points

When discussing this project in interviews, use the STAR method (Situation, Task, Action, Result):

Example Answer: "I built a production-grade Active Directory lab to understand enterprise identity management. The environment included a Windows Server 2022 Domain Controller, multiple client workstations, and implemented security controls you'd find in real businesses. The challenge was balancing usability with security - I needed users to be productive but also protected. I implemented Group Policies that enforced 12-character passwords, locked accounts after 5 failed attempts, and automatically enabled firewalls. I also configured time-based access controls so employees could only log in during business hours. One thing I learned was the importance of audit logging. I enabled security event monitoring across the domain, which generates logs for every authentication attempt, account change, and privilege escalation. This is exactly what a SOC analyst needs to detect suspicious activity. The result was a fully functional enterprise directory that gave me hands-on experience with technologies used by 95% of Fortune 500 companies. I documented the entire process and can demonstrate the configuration if you'd like."

Linking Lab to Job Requirements

Here's how this lab maps to common job requirements:

<b>Job Requirement</b>	<b>Your Lab Experience</b>
Windows Server Administration	Installed, configured, and maintained Windows Server 2022 Domain Controller
Active Directory Experience	Designed OU structure, managed users/groups, implemented AD DS
Group Policy Management	Created and deployed 4 GPOs for security and configuration management
PowerShell Scripting	Developed scripts for user reporting and security monitoring
Security Hardening	Implemented baseline security controls and audit policies
Troubleshooting Skills	Validated all configurations, tested security controls, resolved issues

Next Steps & Continued Learning

- **Expand the Lab:** Add a second domain controller for high availability and disaster recovery practice
- **Integrate Azure AD:** Set up hybrid identity with Azure AD Connect (free Azure trial)
- **Add Certificate Services:** Deploy AD Certificate Services (AD CS) for PKI infrastructure
- **Implement SIEM:** Forward AD logs to your Splunk lab for security monitoring integration
- **Test Attack Scenarios:** Use Mimikatz or BloodHound to understand AD security vulnerabilities
- **Backup & Recovery:** Practice Active Directory backup and disaster recovery procedures
- **Document Everything:** Create a GitHub repository with your PowerShell scripts and documentation

CONGRATULATIONS! *You've successfully built an enterprise Active Directory environment from scratch. This lab demonstrates real-world IT infrastructure skills that are in high demand across cybersecurity, system administration, and IT support roles. Remember: Hiring managers value candidates who take initiative to learn on their own. This lab proves you can independently research, build, and troubleshoot complex Windows environments - exactly what employers are looking for!*

Additional Resources

- **Microsoft Learn:** https://learn.microsoft.com/en-us/windows-server/
- **PowerShell Documentation:** https://learn.microsoft.com/en-us/powershell/

- **Active Directory Security Blog:** https://adsecurity.org/
- **AD Attack & Defense:** https://attack.mitre.org/ (search for 'Active Directory')
- **Group Policy Reference:** https://admx.help/