# Active Directory Lab Documentation - Security+ Portfolio Project

This lab simulates a real-world deployment of a Windows Active Directory (AD) environment using virtual machines. The goal is to demonstrate foundational enterprise skills in system administration, user management, Group Policy control, and basic network security—aligning directly with Security+ exam objectives.

The environment is built across two macOS-based devices using both **Parallels** and **UTM** as hypervisors to host **Windows Server 2022 Standard** and **Windows 11 Pro** clients. One machine acts as the **Domain Controller (DC1)**, while another serves as the **domain-joined workstation**.

#### **Objectives:**

- Deploy a Domain Controller (DC) using Windows Server 2022 Standard
- Join a Windows 11 client machine to AD
- Showcase domain administration tasks (remote management and Group policy)
- Configure AD components (adding users, groups, OUs & DNS)
- Document each step for clarity and portfolio demonstration

#### Tools & Environment

<u>Component</u>	<u>Platform</u>
Machines	Mac Mini M4
Hypervisors	UTM, Parallels
Server OS	Windows Server 2022 Standard
Client OS	Windows 11 Pro

🔴 🔵 🌒 🖑 🗏 🍕 Windows Server			3	
🚘 Server Manager				– 0 ×
	Server		🔹 🧭   🚩 Manage Tools	View Help
- ~ ~		System Properties	Computer Name/Domain Changes	×
🔛 Dashboard	For WIN-T	Computer Name	You can change the name and the membership computer. Changes might affect access to netwo	of this ork resources.
Local Server	outer name	Window on the r		
File and Storage Services ▷	Igroup	Computer descript	Computer name: DC1	
	psoft Defender Fir	Full computer nam	Full computer name: DC1	
	ote management ote Desktop	Workgroup:		More
	eaming net	To rename this co workgroup, click (	Domain:	
			Workgroup:     WORKGROUP	
	ating system vers			
	ware information		ОК	Cancel
	<			>
	EVENTS		OK Cancel	Apply
	All events   742 to	tal		TASKS 🔻 🗸
🖶 🔎 🗄 💽 🖡	. 占 🥺		토 4×	11:41 AM 6/4/2025
		Process	<u>s:</u>	

Step 1. Prepped for Domain Controller (Windows Server 2022 VM on UTM)

Deployed a Windows Server 2022 VM using UTM on a MacBook Pro. Installed the OS and completed the basic configuration. Performed initial server updates and renamed the machine to DC1 to act as the primary domain controller.

<u>Purpose:</u>

Renaming the server gives us a clear hostname that reflects its role in the network. Leaving the server with a default name can make network management and troubleshooting a hassle.

Ethernet Properties	Internet Protocol \	/ersion 4 (TCP/IPv4	l) Properties	×
Networking	General	13		
Connect using:	You can get IP se this capability. Ot for the appropria	ttings assigned auto herwise, you need t te IP settings.	omatically if your network supports to ask your network administrator	
This connection uses the following items:	Obtain an IF Use the follo	address automatica	ally	
<ul> <li>✓</li></ul>	IP address: Subnet mask:		192.168.64.10         255.255.255.0	
Microsoft Network Adapter Multiplexor Prot     Microsoft LLDP Protocol Driver     Internet Protocol Version 6 (TCP/IPv6)	Obtain DNS	ay: server address auto	192 . 168 . 64 . 1	
<	Use the following the follo	wing DNS server ad	dresses:	
Install Uninstall	Preferred DNS	server:	127.0.0.1	
Transmission Control Protocol/Internet Protocol.	Alternate DNS	server:		
across diverse interconnected networks.	Validate set	ttings upon exit	Advanced	
ОК			OK Cancel	

#### Step 2. Configure Static IP Address on DC1



Configured a static IP and DNS address via the server's network adapter settings to ensure consistent domain resolution. Set the DNS to point to the server's own IP for internal name resolution.

#### Purpose:

A Domain controller must have a fixed IP address to reliably provide services like DNS and Active Directories. Here, I manually set a static IP based on my current network range. Below you can see me conduct a ping test to confirm the IP and gateway worked correctly.

🚔 Add Roles and Features Wizard		_		$\times$
Installation progre	SS	DESTINA	ATION SER	VER DC1
Before You Begin	View installation progress			
Installation Type	1 Starting installation			
Server Selection				
Server Roles				
Features	Active Directory Domain Services			
AD DS	Group Policy Management			
Confirmation	Remote Server Administration Tools			
Results	Role Administration Tools			
	Active Directory module for Windows PowerShell			
	AD DS Tools			
	Active Directory Administrative Center			
	AD DS Snap-Ins and Command-Line Tools	€3		
	You can close this wizard without interrupting running tasks. View task page again by clicking Notifications in the command bar, and then Task Export configuration settings	progress or c Details.	open thi	5

## Step 3 Install Active Directory Domain Services (AD DS)

#### <u>Purpose:</u>

AD DS is required for creating and managing domains, users, security groups and other policies. This prepares DC1 to be the first domain controller in my lab network.

Active Directory Domain Service	s Configuration Wizard —		×
Review Options	1	arget sei	RVER DC1
Deployment Configuration	Review your selections:		
Domain Controller Options	Configure this server as the first Active Directory domain controller in a new forest.		^
DNS Options	The new domain name is "plaines.local". This is also the name of the new forest.		
Additional Options	The NetBIOS name of the domain: PLAINES		
Paths	Ferent Europhianal Laurah Windows Service 2016		
Review Options	Forest Functional Level: Windows Server 2010		
Prerequisites Check	Domain Functional Level: Windows Server 2016		
	Additional Options:		
	Global catalog: Yes		
	DNS Server: Yes		
	Create DNS Delegation: No		~

#### 📥 Active Directory Domain Services Configuration Wizard TARGET SERVER Installation DC Progress Creating directory partition: CN=Configuration, DC=plaines, DC=local; 111 objects remaining Niew detailed operation results A Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions. For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?LinkId=104751). 🔥 A delegation for this DNS server cannot be created because the authoritative parent zone Installation cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "plaines.local". Otherwise, no action is required.

## Process:

Installed Active Directory Domain Services (AD DS) and promoted the server to a domain controller for the newly created forest plaines.local. Set a Directory Services Restore Mode (DSRM) password and rebooted to complete configuration.

#### Purpose:

This step promoted DC1 to an actual domain controller and created *plaines.local* AD forest. It correctly installs and configures the DNS, Global Catalog, and initial directory partitions.

Create in: plaines.local/	
	tion
Name: LabUser	rs in this group c rs of this group rs of this group t
Protect container from accidental deletion	rs in this group c ministrators Gro
	ents who are per ted administrato
	ain controllers i ain guests
	ain users ted administrato
OK Cancel Help	rs of this group rs of this group
Guest User B	Built-in account for gue

## Step 5: Create OU - LabUsers

Create 1 OU, *LabUsers*, to logically separate users and devices. Moved the Lab User machine into their respective OUs to support scoped GPO targeting.

### <u>Purpose:</u>

OUs provide structure in Active Directory. They allow for more granular management of users, computers, and policies. Here, I create an OU for isolating all lab client machines.

	Active Directory User	a and Communi						 		~
2	New Object - User	2 and Lombur	arr			×				^
C F										
- 4										
	Create in:	plaines.local.	Users							
							ion			
		1.1					s in this group c			
	Hirst name:	Lab		Initials:			s of this group			
	Last name:	User					s of this group t			
	Edamo	Lab User			_		s in this group c			
	rui name.						nts who are per			
	User logon name:						ed administrato			
	LabUser		@plaines.lo	cal	~		stations and ser			
							ain controllers i			
	User logon name (pre	-Windows 2000	):				ain guests			
	PLAINES\		LabUser				ain users			
					ed administrato					
							s of this group			
			< Back	Next >	Car	ncel	s of this group			
			Cont			n de la	s in this group c			
			ig Guest Landen Die	User		Built-In	n account for gue			
			Key Admir	nies Oser Ins Security	Group	Membe	ers of this group			
			Protected	Us Security	Group	Memb	ers of this group			
		8	RAS and IA	S Security	Group	Servers	in this group can			
<		> 4	Read-only	D Security	Group	Memb	ers of this group			
			~						1	

#### Step 6 - Create Domain User

#### Process:

Created a standard domain user (Lab User) in ADUC to simulate a non-privileged user. This account was used to test user-level policy enforcement in later steps.

#### Purpose:

Creating a test domain user allows us to validate domain join, and user-level permissions from a windows 11 client system. Below you can see the new user with the non-admin privileges.

Sector 1	* * *	
🏪 Guest	User	Built-in account for gue
📥 Jorden Plaines	User	Built-in account for ad
🧟 Key Admins	Security Group	Members of this group
📥 Lab User	User	
💐 Protected Us	Security Group	Members of this group

← Settings		- 🗆 X
Lab User labuser@plaines.local	Network & internet > Ethernet	
Find a setting Q	Tal No internet	^
A Home	Authentication settings	Edit
<ul> <li>System</li> <li>Bluetooth &amp; devices</li> </ul>	Metered connection Some apps might work differently to reduce data usage when you're connected to this network	Off
Network & internet	Set a data limit to help control data usage on this network	
<ul> <li>Personalization</li> <li>Apps</li> <li>Accounts</li> </ul>	IP assignment:         Manual           IPv4 address:         192.168.64.11           IPv4 mask:         255.255.255.0           IPv4 gateway:         192.168.64.1	Edit
<ul> <li>Time &amp; language</li> <li>Gaming</li> </ul>	DNS server assignment: Manual IPv4 DNS servers: 192.168.64.10 (Unencrypted) 8.8.8.8 (Unencrypted)	Edit

#### Step 7: Join Client to Domain & Log in

Process:

On a Windows 11 VM running in Parallels (Mac Mini), configured a static IP and DNS, renamed the computer, and joined it to the plaines.local domain. Restarted the system and verified domain connectivity.

<u>Purpose:</u>

The goal was to enable the client to communicate with the DC and become a domain-joined device, allowing centralized management through AD.



Step 8: Move Domain-Joined Client to LabComputers OU

Purpose:

To prepare for applying specific Group Policy Objects (GPOs), we moved the Windows 11 client into the LabComputers OU.

Group Policy Management	v Help	
✓ Group Policy Management ✓ Group Policy Management ✓ Group Domains ✓ Plaines.local ✓ Domain Contro > © Domain Contro > © Demain Contro > © LabUers > © LabUers > © LabUers > © Statte GPOs > © State Ø Group Policy Madeling © Group Policy Results	Group Policy Management Conterts  Name  New GPO  Source Stater GPO:  (pone)  OK  Cancel	ation 0 days
🔳 A 🖽 💽	E <u> &lt; </u>	C 4 20548.7€_Telease.210507-1500

Step 9: Create and Link a GPO to the LabUsers OU

Process:

Opened Group Policy Management Console (GPMC) and created a GPO titled LabUsers -Basic Restrictions. Linked it to the LabUsers OU to begin applying user-based policies.

## <u>Purpose:</u>

Implementing a Group Policy Object (GPO) linked to the LabUsers Organizational Unit allows for the application of custom restrictions to standard domain users. By disabling access to Control Panel, Command Prompt, and registry editing tools, this GPO enforces fundamental security measures. These restrictions serve to hinder unauthorized configuration modifications and emulate typical limitations imposed on non-administrative users in corporate settings.

I I Vindows Server					
📠 Group Policy Management		- 🗆 🗙			
🛋 File Action View Window Help –					
Group Policy Management	LabUsers - Basic Restrictions				
A Forest: plaines.local	Scope Details Settings Delegation Status				
Bomains     Bomains     Bomaines local	Administrative Translater				
🗊 Default Domain Poli	Administrative remplates	$\sim$			
> 📓 Domain Controllers	Policy definitions (ADMX files) retrieved from the local computer.				
> E LabComputers	Control Panel				
<ul> <li>Group Policy Object</li> </ul>	Policy Setting Comment				
📑 Default Domain	Prohibit access to Control Enabled				
E LabUsers - Basic	Panel and PC settings				
👺 WMI Filters	System				
Starter GPOs	Policy Setting Comment				
Group Policy Modeling	Prevent access to registry Enabled				
Group Policy Results	editing tools				
	Disable regedit from running silently? Yes				
	Policy Setting Comment				
	Prevent access to the Enabled				
	command prompt	× 1			
< >>		iation			
	Puile	days			
		4:27 AM			
		€ 48 6/7/2025			

## Step 10: Configure LabUsers GPO

## Process:

Edited the GPO to disable access to the Control Panel, Registry Editor, and Command Prompt. Applied these restrictions under User Configuration > Administrative Templates. Verified GPO application by logging in as Lab User and observing blocked features.

## <u>Purpose:</u>

To create a secure, locked-down environment similar to enterprise settings, the LabUsers Organizational Unit (OU) will have specific restrictions enforced via a linked Group Policy Object (GPO). This configuration prevents standard users (like "Lab User") from making unauthorized changes or causing misconfigurations during testing or normal use.

## **Applied Security Policies:**

• **Control Panel and PC Settings Access Disabled:** Restricts users from modifying system configurations or personalization options.

- **Registry Editing Tools Access Blocked:** Prevents unauthorized alterations to critical registry settings.
  - Silent execution of regedit is specifically disabled: Enabled.
- **Command Prompt Access Restricted:** Blocks users from running commands that could impact system stability or security.

These policies ensure users adhere to predefined boundaries and maintain system integrity. Login to the domain-joined Windows 11 client as Lab User was successful, with all configured restrictions effectively implemented. As seen in the provided screenshot, policy enforcement successfully blocked access to restricted tools such as the Control Panel and CMD.



#### Step 11: Test GPO Enforcement

## Process:

Logged into the client as Lab User to test the policy configuration. Confirmed the Command Prompt, Control Panel, and Registry Editor were successfully restricted. Took screenshots of blocked attempts for documentation.

## <u>Purpose:</u>

To validate that the LabUsers - Basic Restrictions GPO is correctly applied to standard user accounts. This step ensures that domain users placed in the LabUsers OU experience the intended restrictions—such as being blocked from accessing the Command Prompt, Control Panel, and Registry Editor—when logging into a domain-joined machine.

## Active Directory Lab Project Summary

This project involved the comprehensive deployment of a domain-based Windows network environment using virtual machines. It successfully established a working Active Directory infrastructure, including domain controller setup, organizational unit creation, client machine integration, and the enforcement of specific Group Policy Objects.

## Key Steps and Configurations:

- Deployed a Windows Server 2022 Domain Controller utilizing the "plaines.local" domain.
- Configured essential network services: DNS, static IP addressing, and Active Directory Domain Services (AD DS).
- Structured Active Directory by creating "LabUsers" and "LabComputers" Organizational Units (OUs) for targeted policy implementation.
- Successfully joined a Windows 11 client virtual machine to the domain.
- Provisioned domain users, including a standard, non-administrative account for testing purposes.
- Implemented and confirmed user-level restrictions via GPOs, such as disabling the Control Panel, Command Prompt, and Registry Editor for standard users.
- Applied and verified computer-level GPOs to enforce Microsoft Defender real-time protection settings.

## **Demonstrated Technical Proficiencies:**

- Active Directory administration expertise.
- Configuration of DNS and IP addressing within domain-based networks.
- Proficiency in Group Policy Management for both user and computer scopes.
- Implementation of Windows security hardening and environment lockdowns.
- Effective network troubleshooting and system configuration abilities.

## **Future Applications:**

This lab environment provides a foundation for advanced enterprise-level testing. It can be further utilized for security baselining, incident detection exercises, and future integrations with tools like PowerShell, Sysmon, or SIEM platforms.

# Post Project Summary

## <u>Key Takeaways</u>

- Successfully built and managed a Windows Active Directory environment from scratch using virtualization tools.
- Verified proper OU design and GPO targeting, ensuring users and computers received scoped policies.
- Demonstrated user-level restrictions like disabling the Command Prompt, Registry Editor, and Control Panel.
- Used essential tools like *gpupdate, gpresult*, and *ipconfig* to validate configurations and troubleshoot issues.
- Reinforced concepts covered in the Security+ (SY0-701) certification, especially around identity, access control, and security baselines.

# Troubleshooting Highlights

- DNS resolution issues were resolved by manually configuring static IPs and ensuring the client pointed to the domain controller as its DNS server.
- Bridged networking had to be correctly configured in Parallels and UTM to allow domain joining and IP-level communication.
- Password policy enforcement required adjustments when creating test users, highlighting the importance of understanding group policy settings.
- GPO application troubleshooting was performed using OU placement verification and the *gpupdate /force* + *gpresult /r* workflow.

# Next Steps

- Set up a secondary domain controller (DC2) to explore replication and fault tolerance.
- Implement audit logging with Windows Event Viewer or integrate with a lightweight SIEM like Wazuh or Graylog.
- Explore PowerShell scripting to automate user account creation and OU assignment.
- Introduce a Linux client or server to simulate cross-platform AD integration.
- Simulate security incidents (e.g., failed logon attempts, privilege escalation) for Blue Team/IR testing.

## **Final Reflection**

This lab project mirrors real-world enterprise operations and serves as a foundation for more advanced testing and development. It not only reinforces theoretical knowledge from the Security+ curriculum but also proves capability in configuring, securing, and troubleshooting Windows-based infrastructures.

The result is a functional domain environment that can be reused and extended for incident response, endpoint detection, and network monitoring practice, paving the way toward a career in **cybersecurity operations**, **GRC**, or **security automation**.