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**.

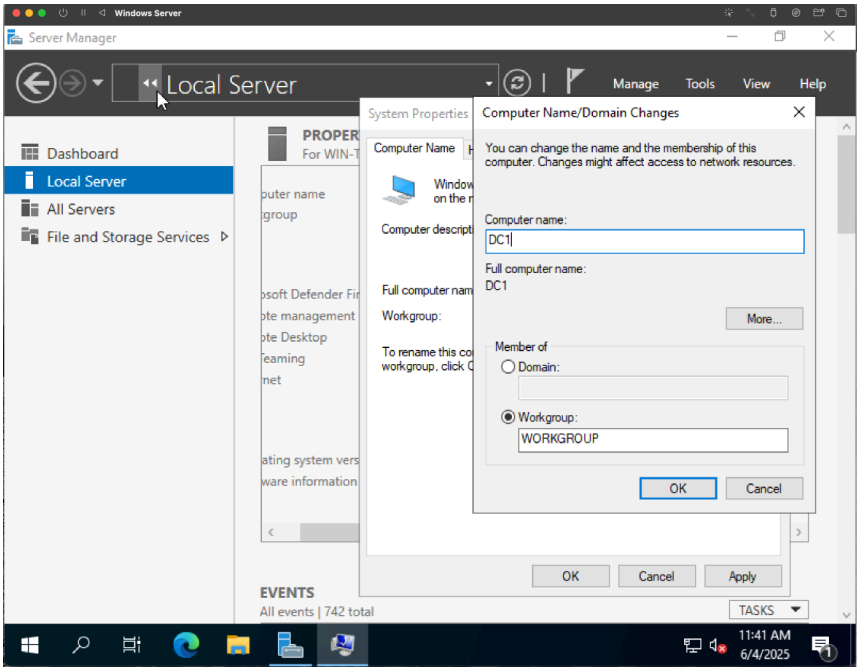
Objectives:

- 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

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

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



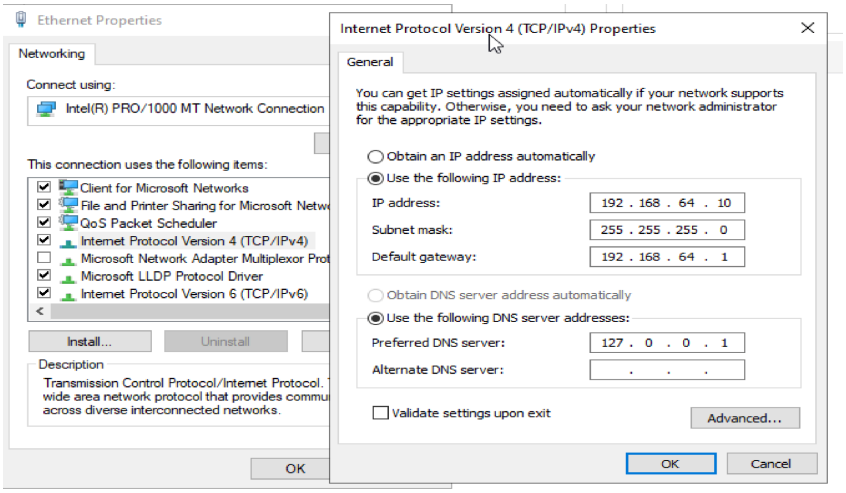
Process:

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.

Purpose:

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.

Step 2. Configure Static IP Address on DC1



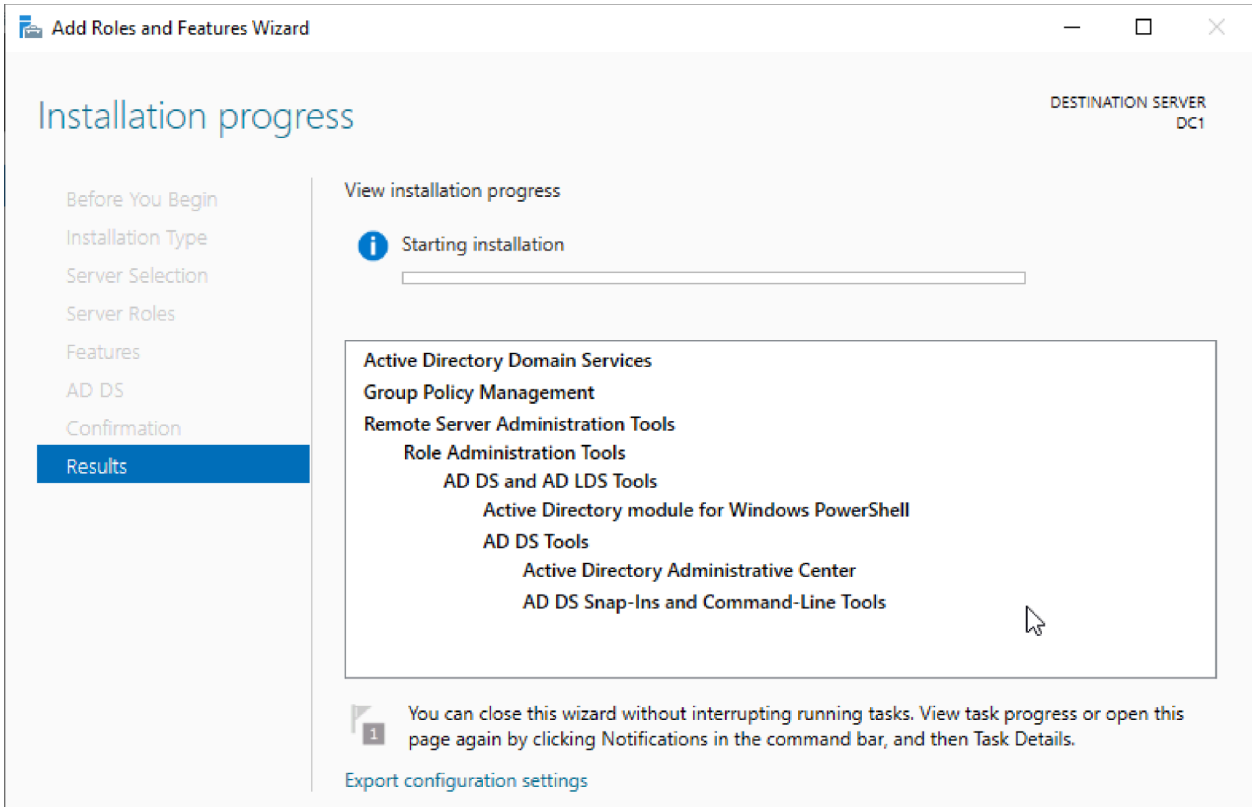
Process:

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.

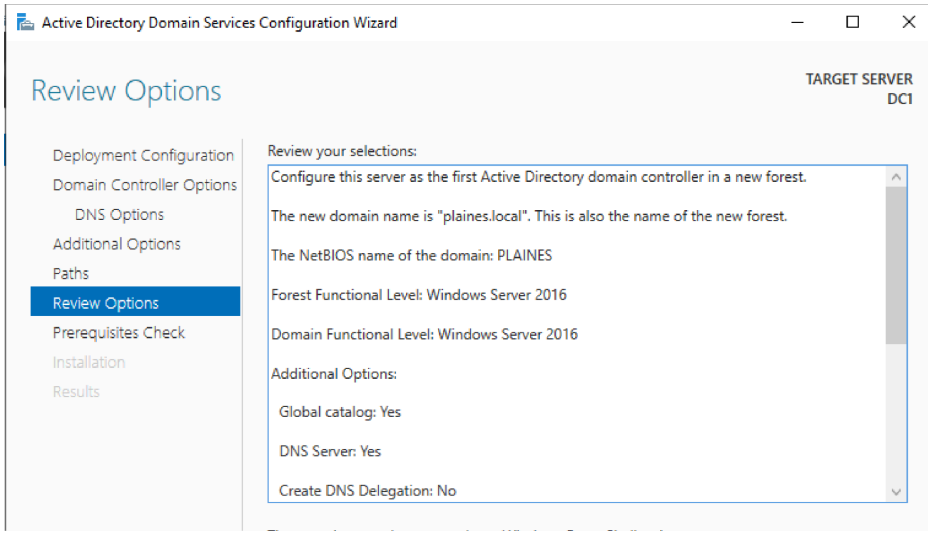
Step 3 Install Active Directory Domain Services (AD DS)

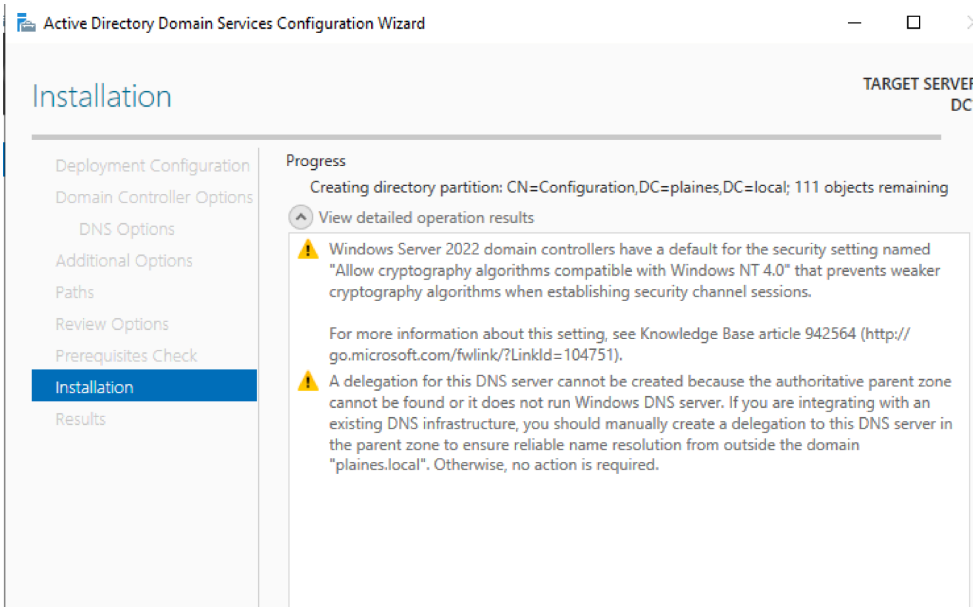


Purpose:

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.

Step 4. Promote Server to DC





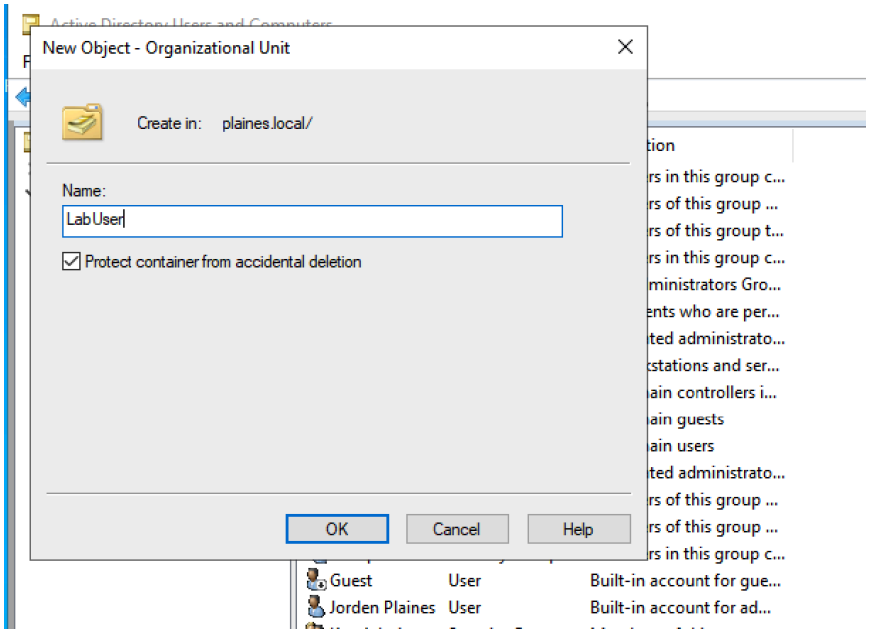
Process:

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.

Step 5: Create OU - *LabUsers*



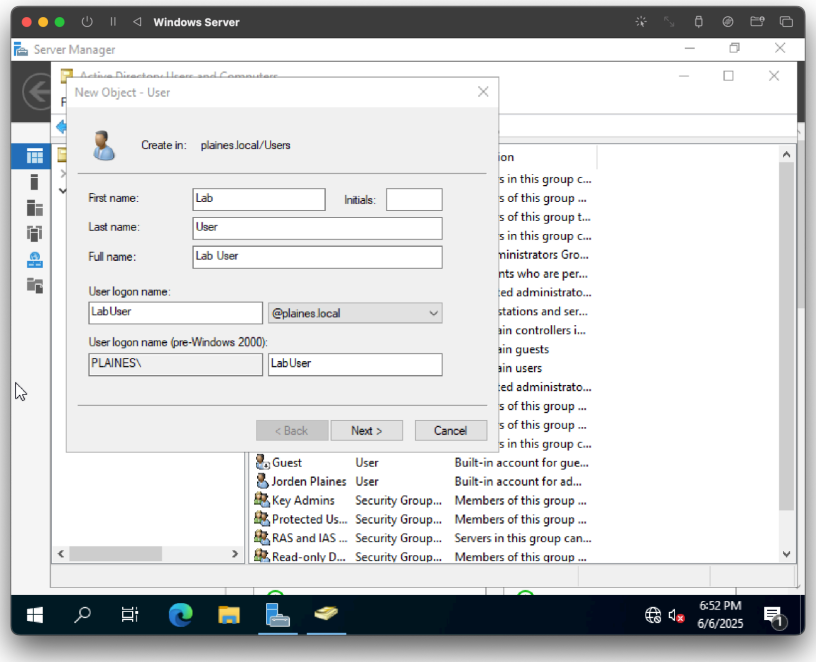
Process:

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

Purpose:

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.

Step 6 - Create Domain User

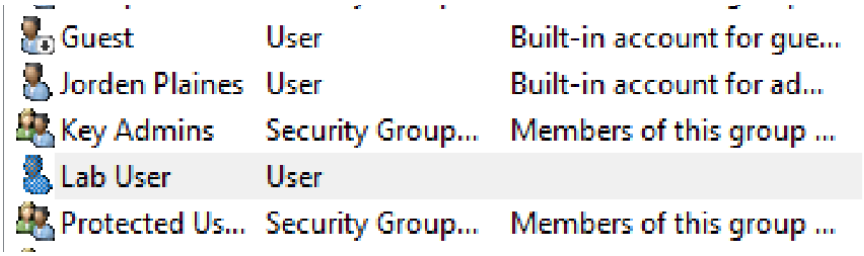


Process:

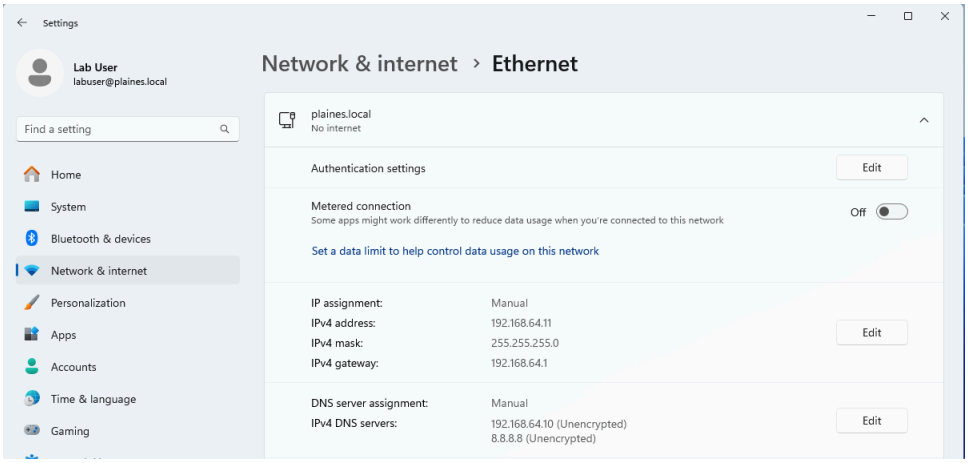
Created a standard domain user (Lab User) in ADUC to simulate a non-privileged user. This account was used to test user-level policy enforcement in later steps.

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.



Step 7: Join Client to Domain & Log in



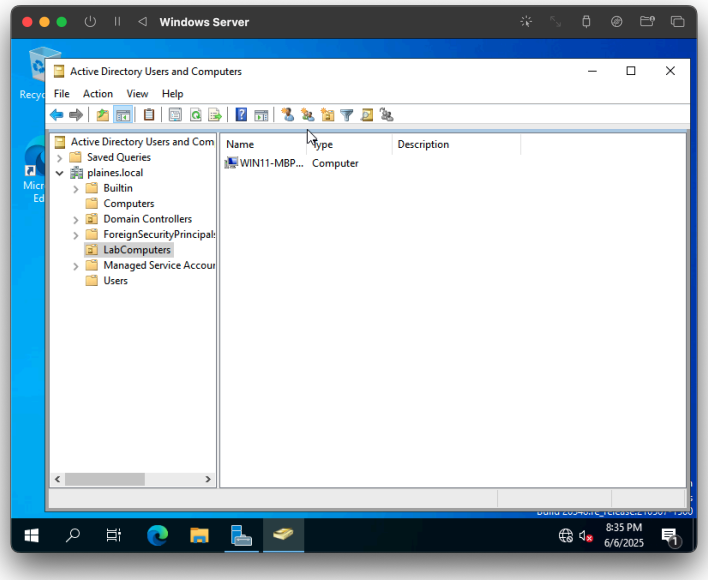
Process:

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.

Purpose:

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

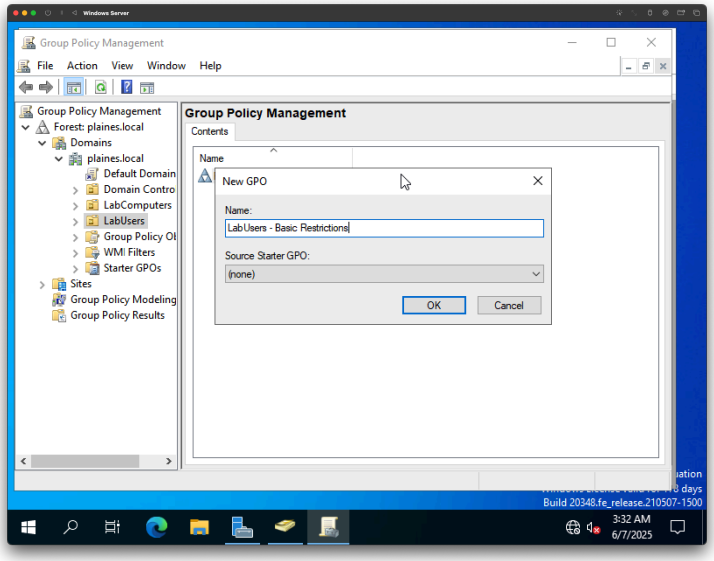
Step 8: Move Domain-Joined Client to LabComputers OU



Purpose:

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

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



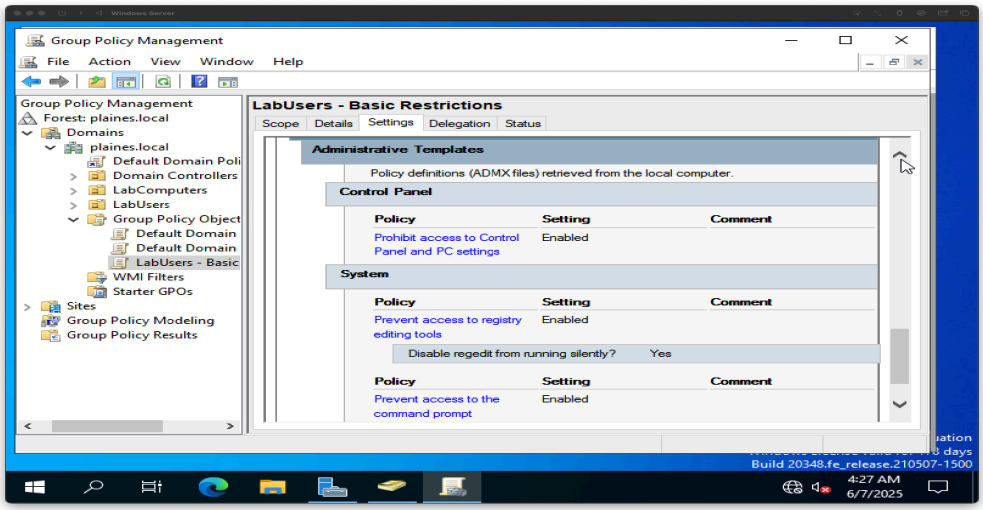
Process:

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.

Purpose:

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.

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.

Purpose:

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.

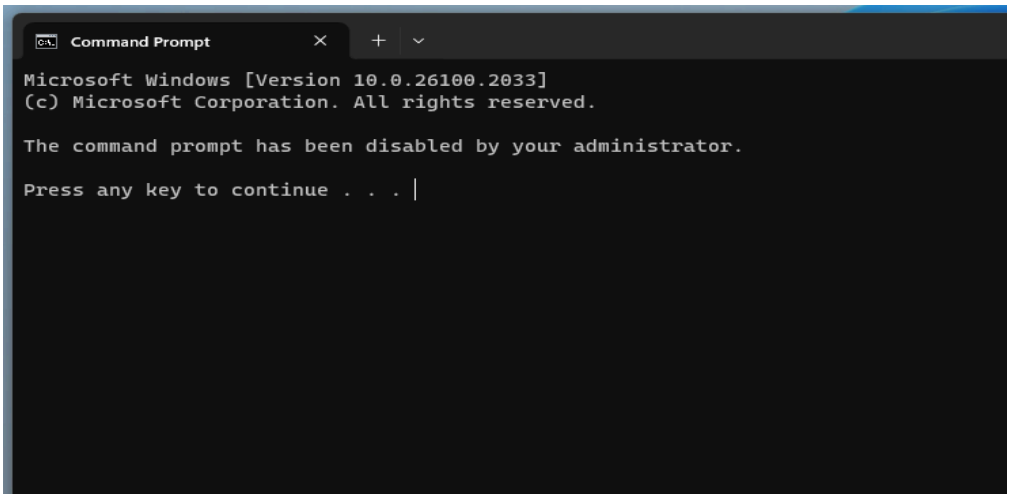
Applied Security Policies:

- **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.

Purpose:

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

Key Takeaways

- 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**.