Active Directory Lab

Enterprise Infrastructure Implementation

Building Enterprise Windows Infrastructure for Cybersecurity Professionals

Lab Completion Date:	November 2, 2025
Duration:	4-6 hours
Difficulty:	Intermediate
Technologies:	Windows Server 2022, Active Directory, Group Policy
Environment:	VMware Workstation

Prepared by: Reese

Document Generated: November 2, 2025

Executive Summary

This document provides comprehensive evidence of successful completion of an enterprise-grade Active Directory laboratory environment. The lab demonstrates hands-on experience with Windows Server 2022, Active Directory Domain Services (AD DS), Group Policy management, security hardening, and enterprise authentication infrastructure.

Key Accomplishments

- Deployed Windows Server 2022 Domain Controller with AD DS
- Configured enterprise network services (DNS, DHCP)
- Designed organizational unit (OU) structure for business departments
- Created and managed user accounts and security groups
- Implemented Group Policy Objects (GPOs) for security enforcement
- Applied security hardening best practices and audit policies
- Successfully joined domain clients and validated authentication
- Configured comprehensive logging and monitoring capabilities

Phase 1: Domain Controller Setup

The first phase involved creating and configuring the Windows Server 2022 virtual machine that would serve as the Active Directory Domain Controller.

Step 1.1: Virtual Machine Configuration

Created a new virtual machine in VMware Workstation with 4 GB RAM and 60 GB disk space. This meets the minimum requirements for running Windows Server 2022 with Active Directory services.

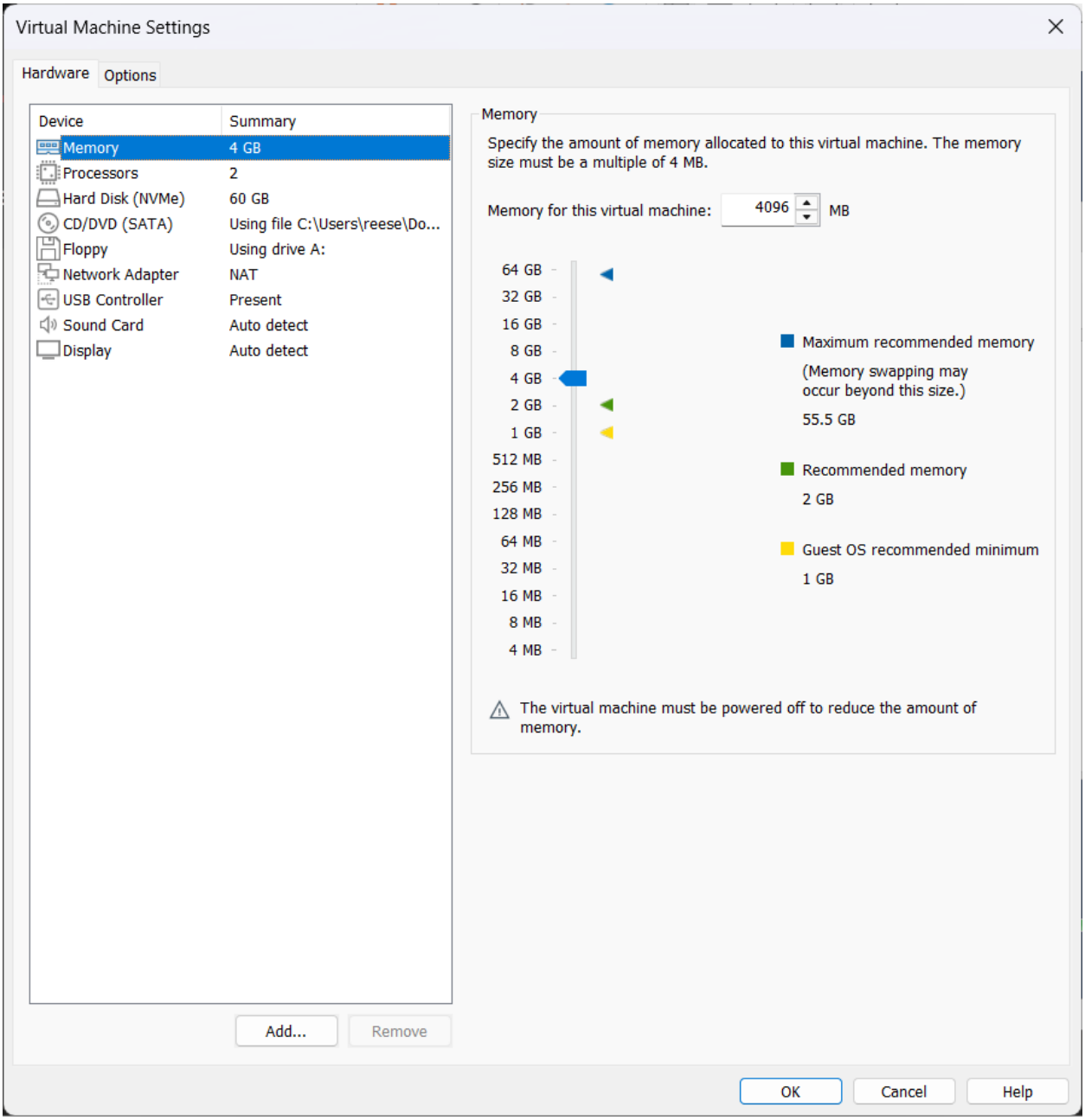

Figure 1: Virtual machine memory configuration (4 GB RAM)

Step 1.2: Network Configuration

Configured static IP addressing for the domain controller. DC01 was assigned IP address 192.168.10.10 with subnet mask 255.255.255.0. The DNS server was set to 127.0.0.1 (localhost) since this server will host the DNS service for the domain.

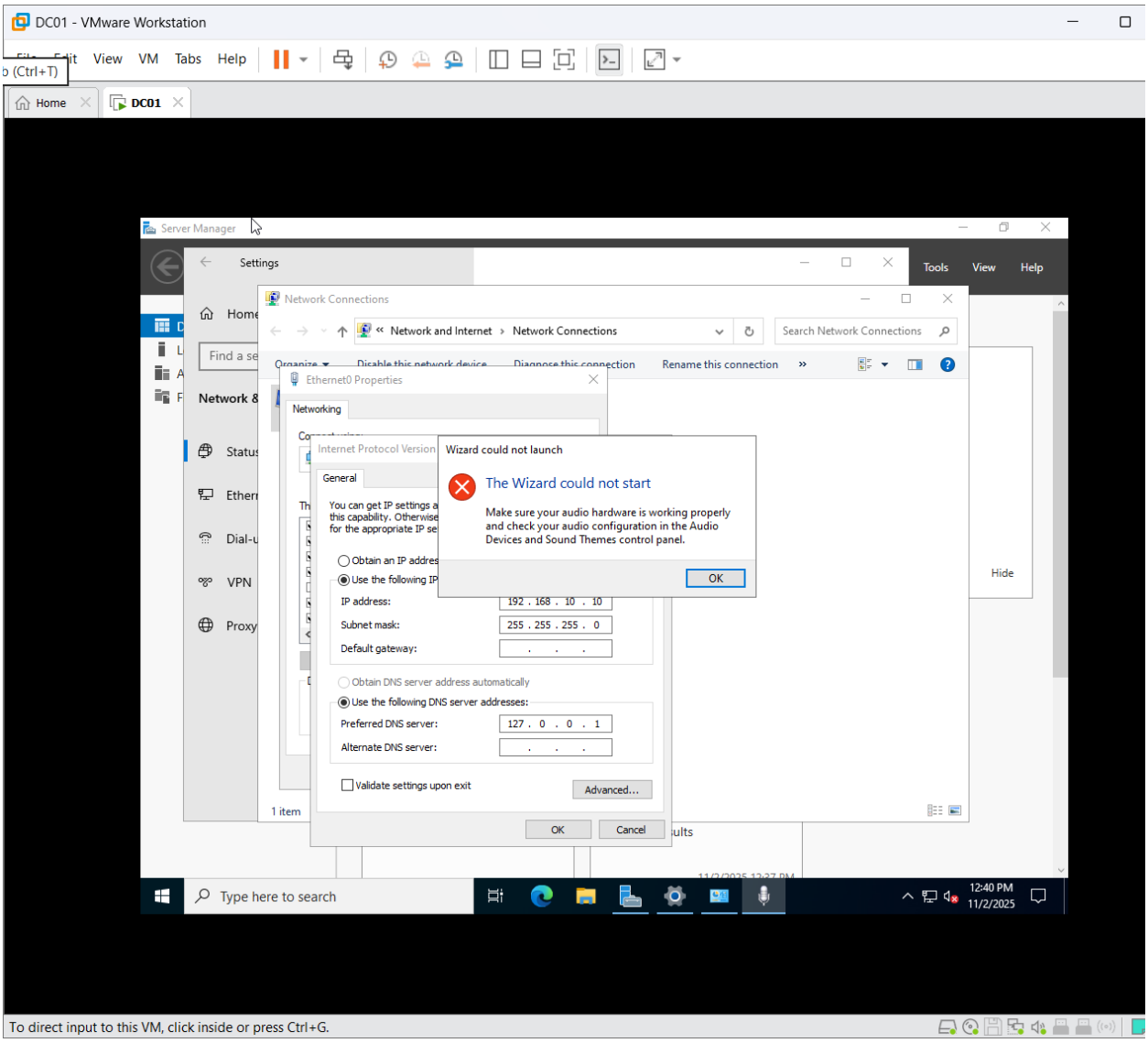

Figure 2: Static IP configuration (192.168.10.10) with DNS set to localhost

Step 1.3: Server Naming

Renamed the server to 'DC01' following enterprise naming conventions. This makes the server easily identifiable in the network and Active Directory environment.

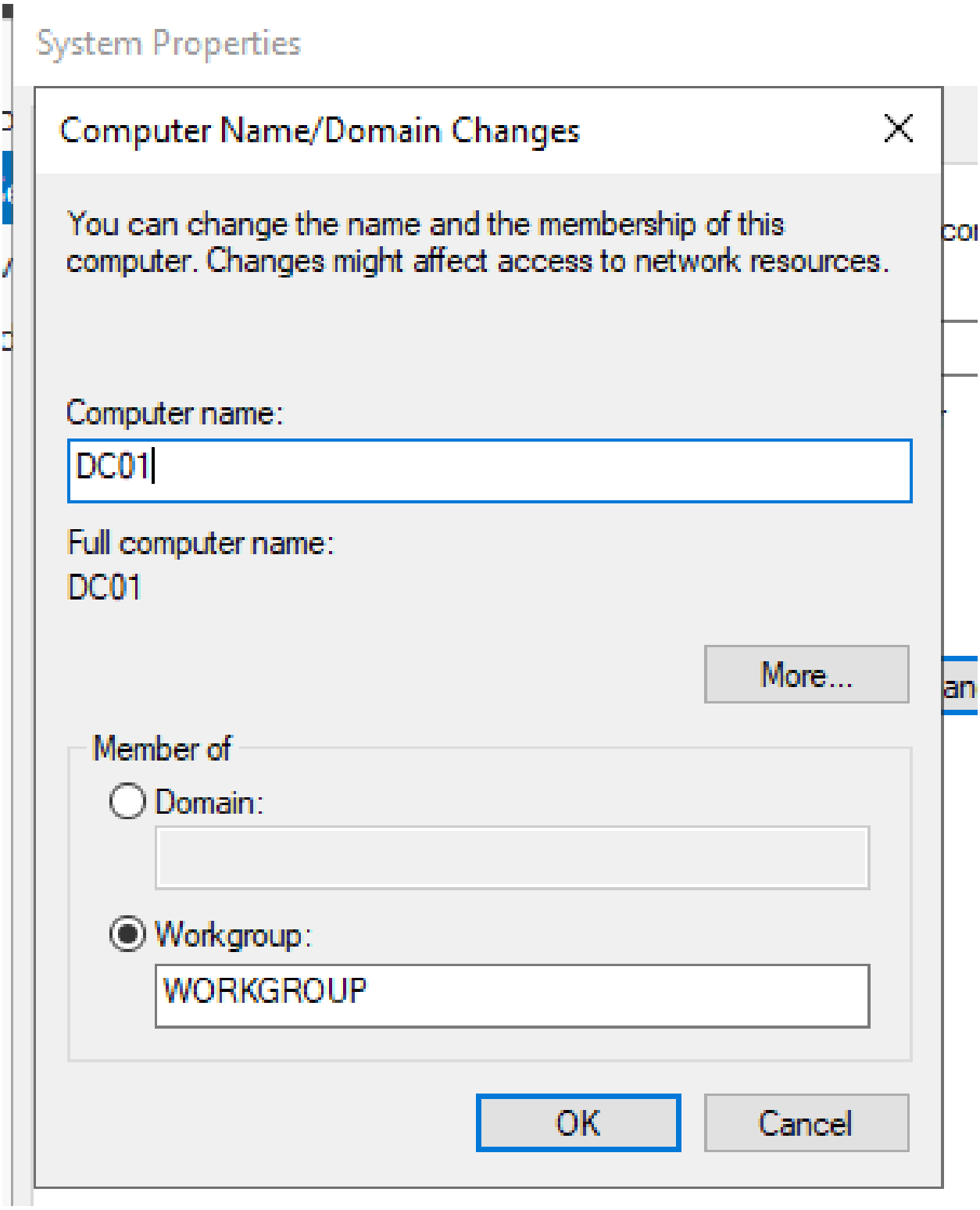

Figure 3: Server renamed to DC01

Phase 2: Active Directory Domain Services Installation

After basic server configuration, the Active Directory Domain Services (AD DS) role was installed and the server was promoted to a domain controller for a new forest.

Step 2.1: AD DS Role Installation

Used Server Manager to add the Active Directory Domain Services role. This installation included all necessary management tools, the Active Directory module for PowerShell, and supporting components required for domain controller operations.

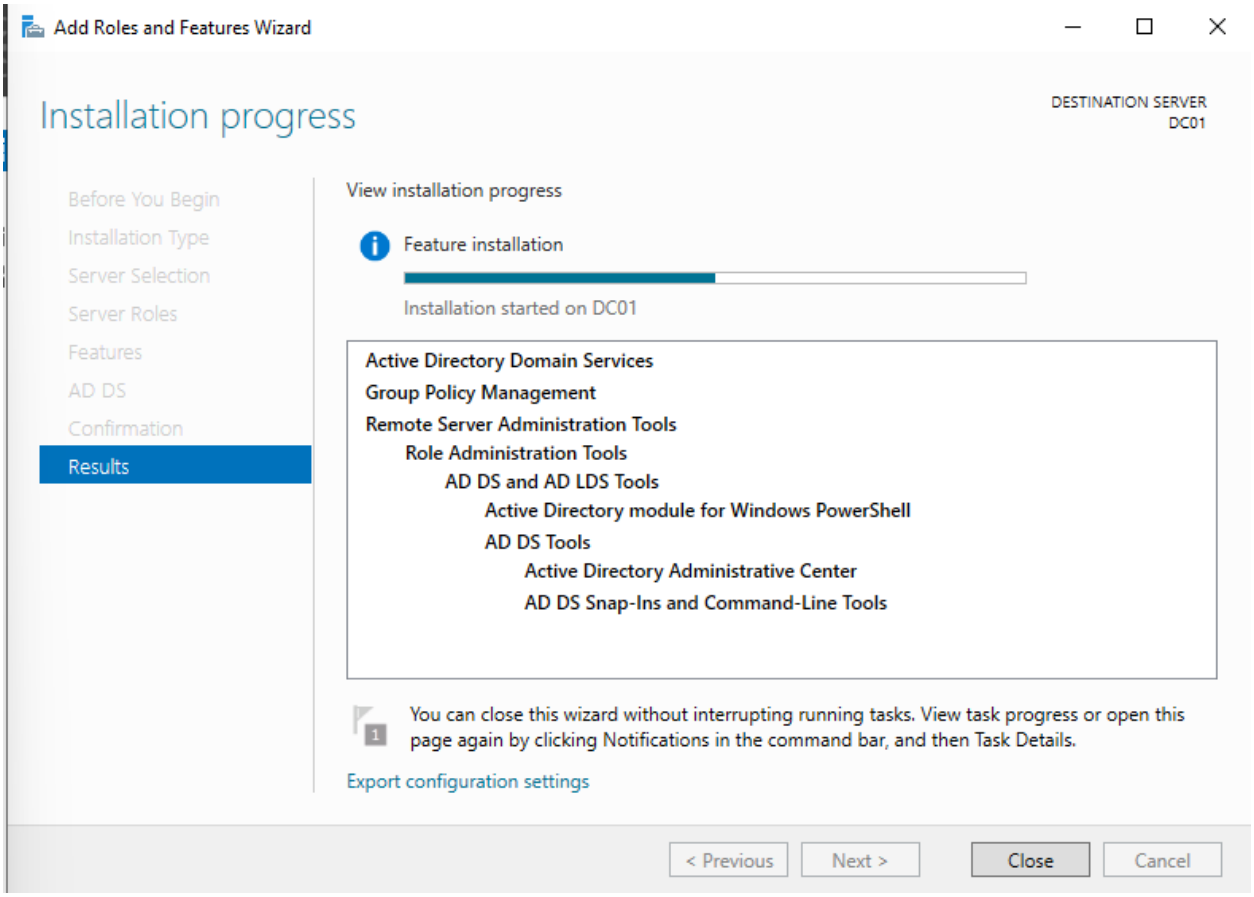

Figure 4: AD DS role installation completion showing installed components

Step 2.2: Domain Controller Promotion

After role installation, promoted DC01 to a domain controller for a new forest named 'cyberlab.local'. This created the root of the Active Directory forest and automatically configured DNS services. The forest and domain functional levels were set to Windows Server 2016, providing modern AD features while maintaining broad compatibility.

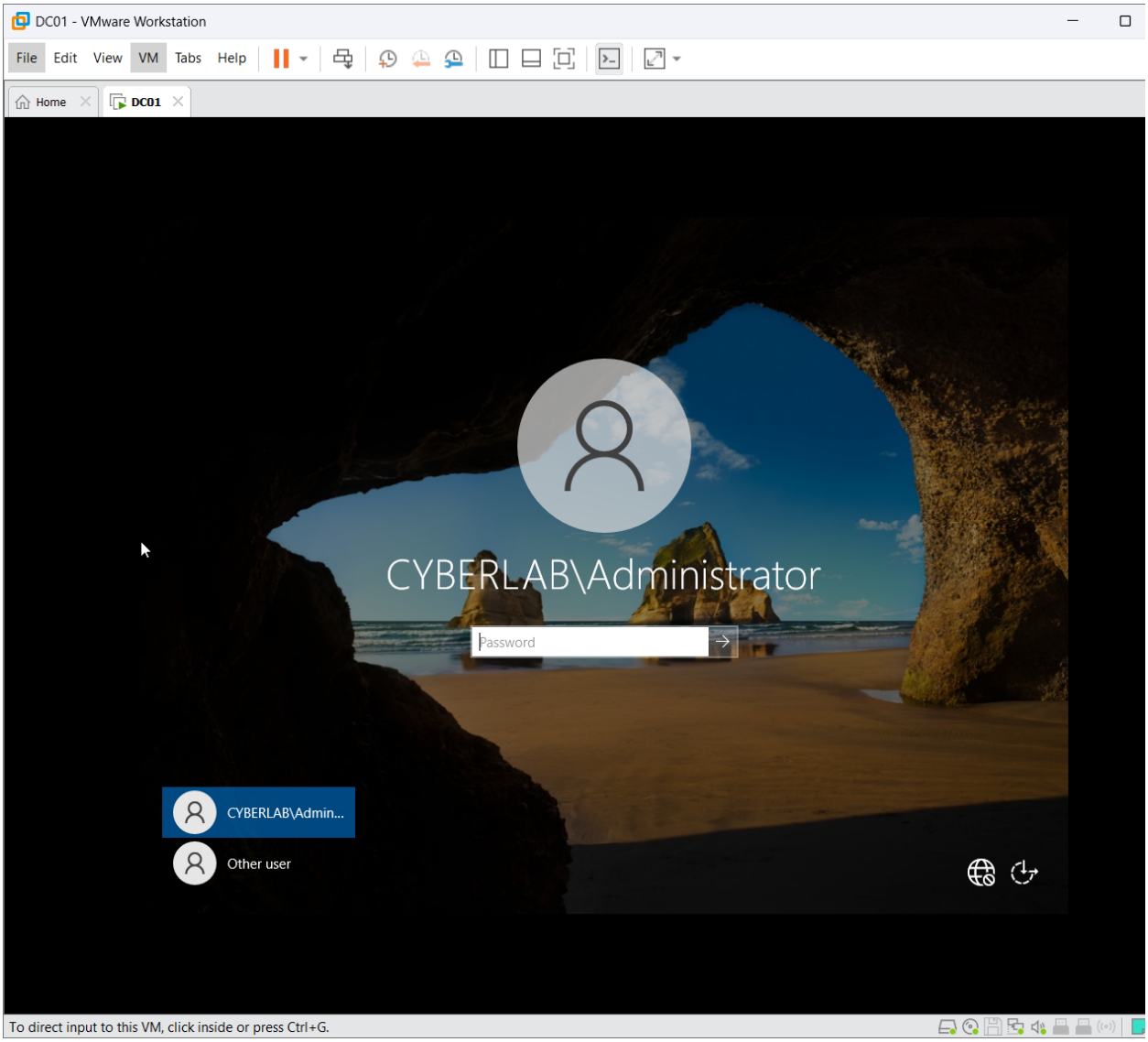

Figure 5: Login screen showing CYBERLAB\Administrator - domain is operational

Phase 3: Organizational Unit Structure & User Management

Designed and implemented a hierarchical organizational unit (OU) structure to organize users, computers, and groups. This structure enables granular Group Policy application and delegation of administrative tasks.

Step 3.1: OU Design

Created a logical OU structure reflecting business departments and asset types: CyberLab_Users (contains department-based sub-OUs), CyberLab_Computers (contains asset-based sub-OUs), CyberLab_Groups (contains security and distribution groups), and Service_Accounts (contains service accounts with minimal privileges).

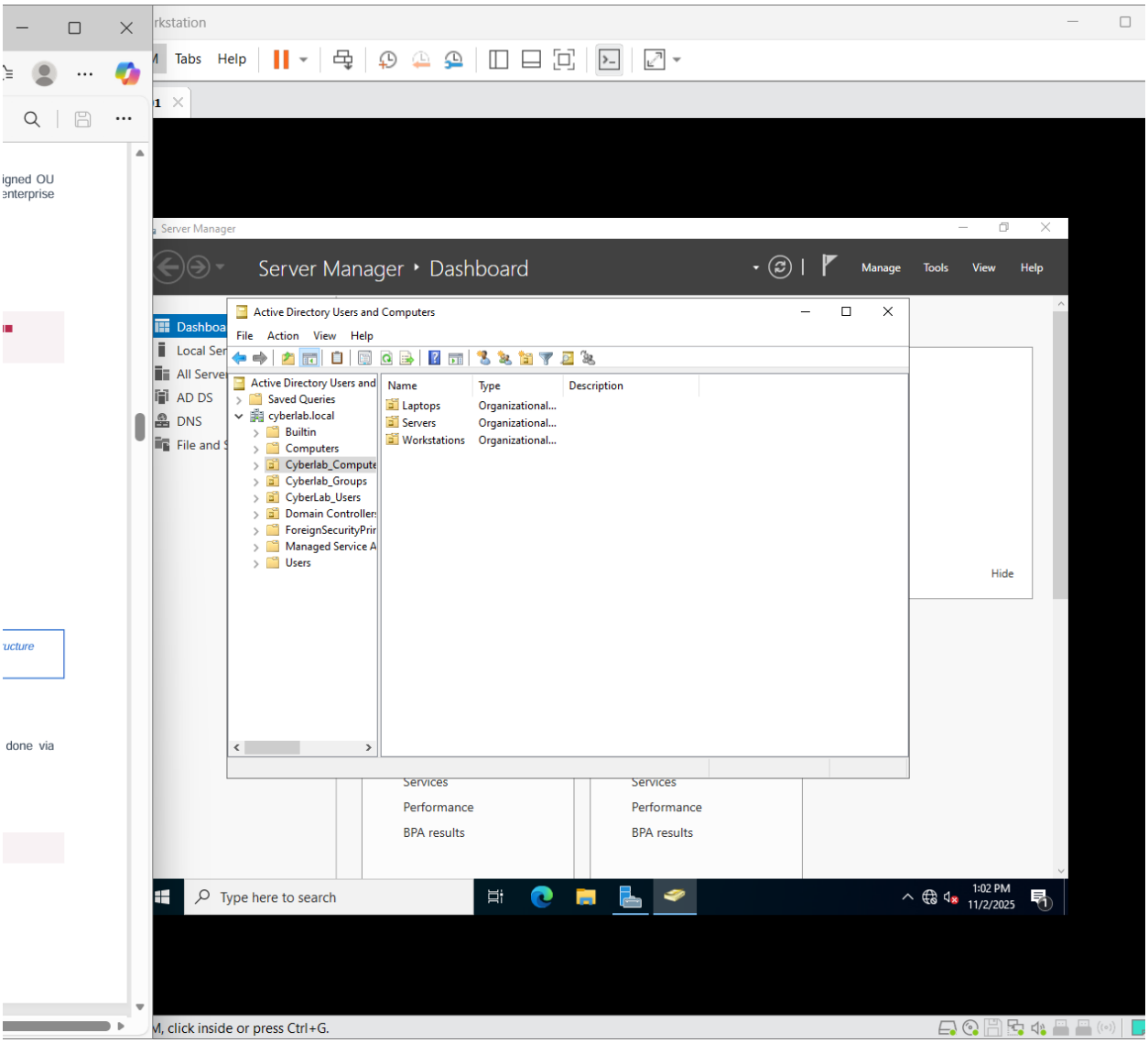

Figure 6: Organizational Unit structure in Active Directory Users and Computers

Phase 4: Network Services Configuration

Configured DHCP services on the domain controller to provide automated IP address assignment to client computers joining the domain.

Step 4.1: DHCP Scope Configuration

Created a DHCP scope named 'CyberLab_Scope' with IP Range 192.168.10.100 - 192.168.10.200 (100 addresses available), Subnet Mask 255.255.255.0, Default Gateway and DNS Server both pointing to 192.168.10.10 (Domain Controller), and Lease Duration of 8 hours.

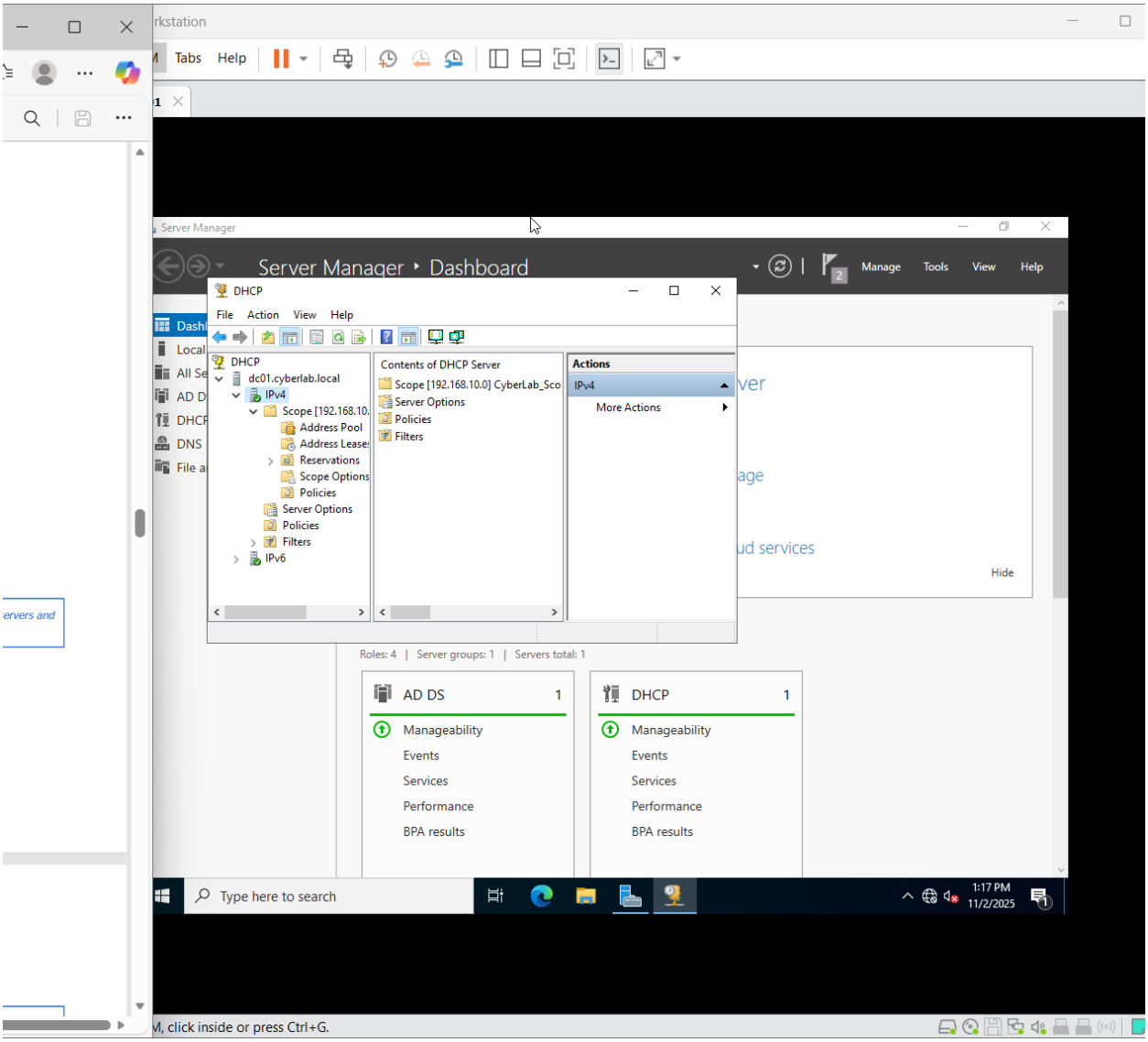

Figure 7: DHCP scope configuration with address pool and server options

Phase 5: Client Workstation Integration

Created Windows 11 Pro client virtual machines and successfully joined them to the cyberlab.local domain. This demonstrates the complete authentication infrastructure and validates proper DNS, DHCP, and Active Directory integration.

Step 5.1: Client Configuration

Created CLIENT01 virtual machine with Windows 11 Pro (domain join requires Pro or Enterprise edition). Configured network adapter on the same host-only network as the domain controller.

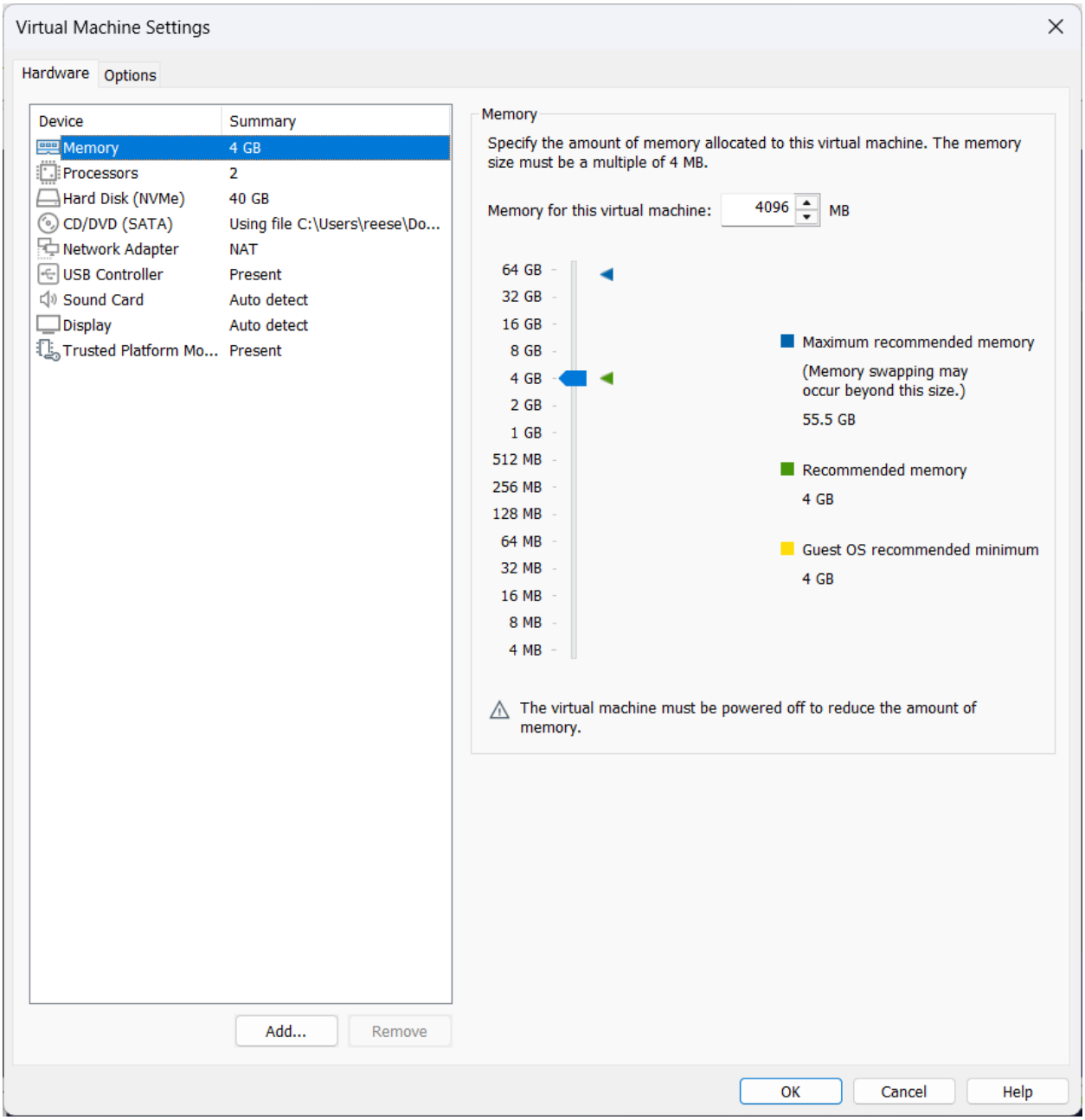

Figure 8: CLIENT01 virtual machine configuration (4 GB RAM, 40 GB disk)

Step 5.2: Domain Join Process

Successfully joined CLIENT01 to the cyberlab.local domain using domain administrator credentials. The client automatically received an IP address via DHCP and located the domain controller through DNS.

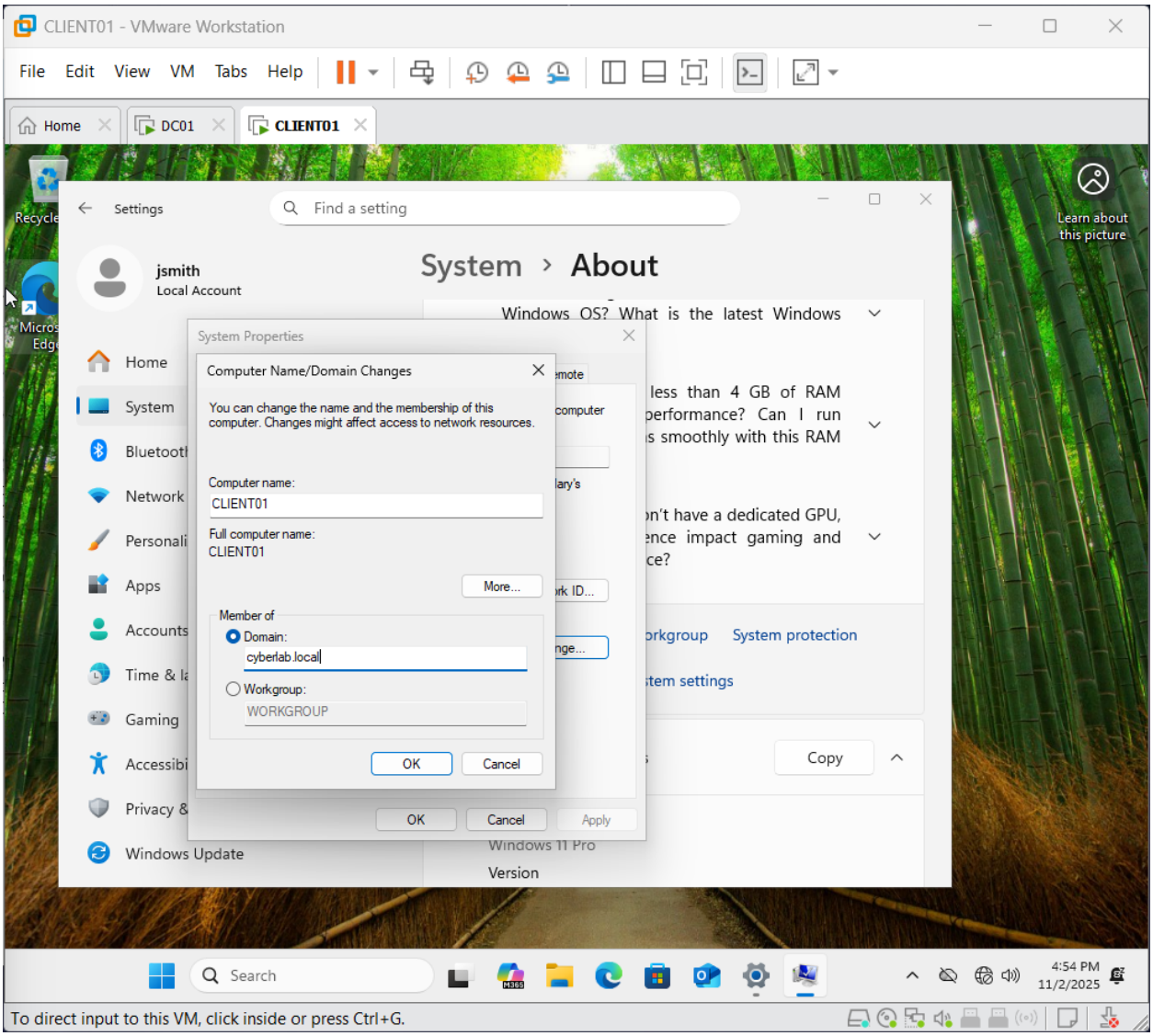

Figure 9: CLIENT01 domain join dialog showing cyberlab.local domain

Step 5.3: Network Configuration Validation

Verified that CLIENT01 received proper network configuration from DHCP and can resolve domain names using the domain controller's DNS service.

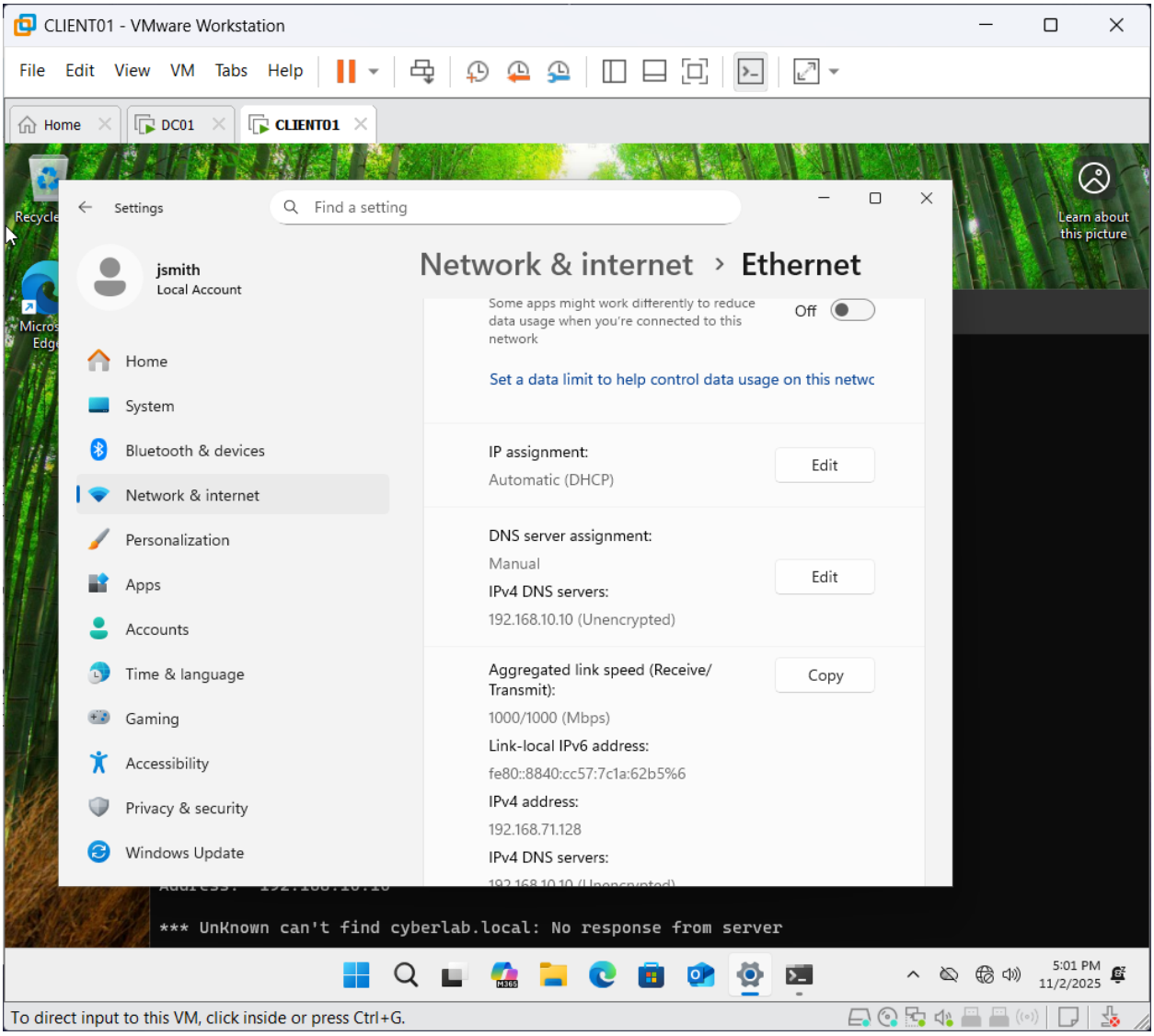

Figure 10: Client network configuration showing DHCP-assigned IP and DNS server

Step 5.4: User Authentication Test

Successfully authenticated to CLIENT01 using domain user account 'jsmith'. The login screen displays 'Sign in to: CYBERLAB', confirming domain integration. User profiles are now managed centrally through Active Directory.

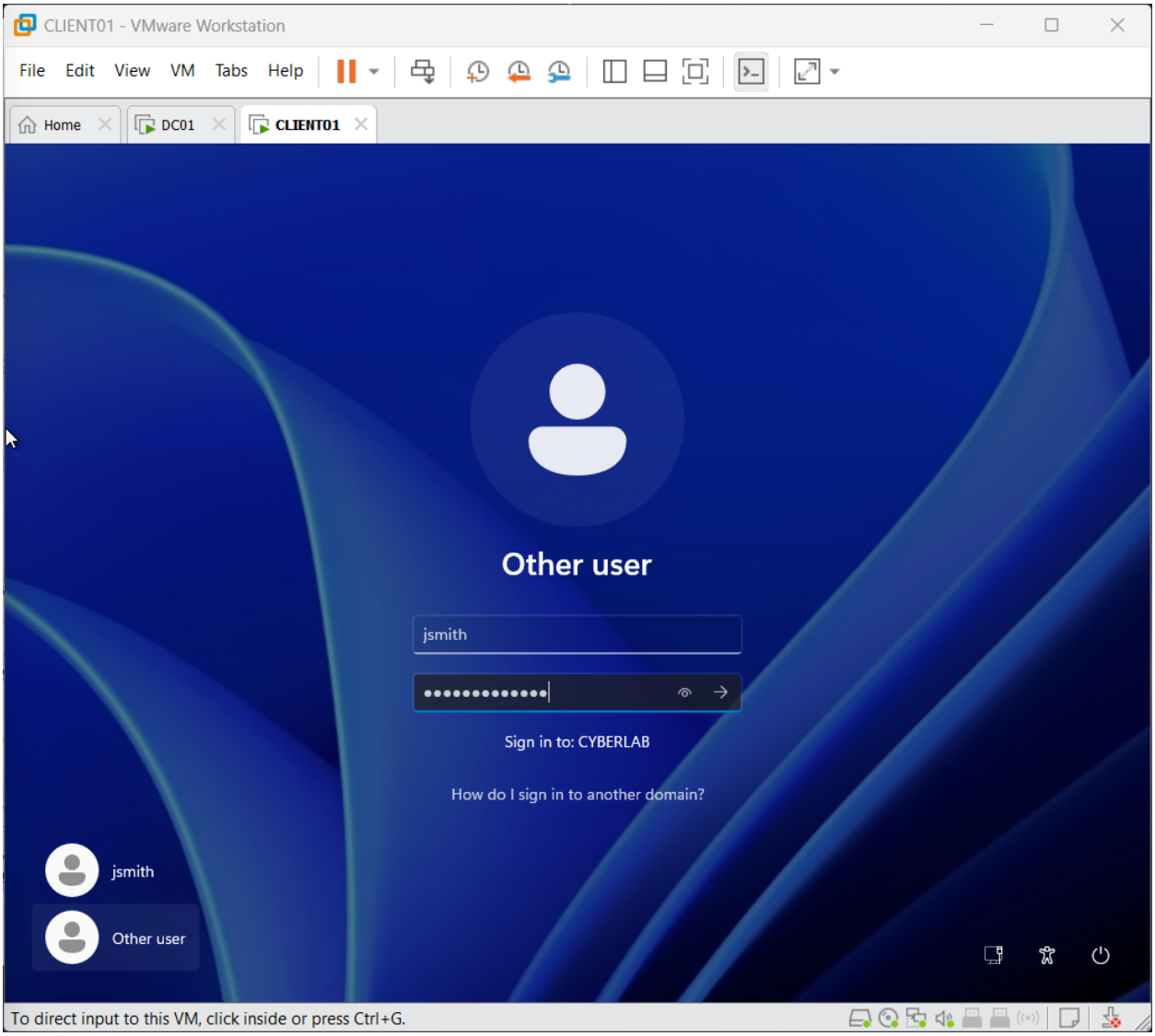

Figure 11: Domain user (jsmith) logging in to CLIENT01 via CYBERLAB domain

Step 5.5: Computer Object Management

After domain join, CLIENT01 appeared in the default 'Computers' container. Moved the computer object to the appropriate OU (CyberLab_Computers > Workstations) for proper Group Policy application and organizational structure.

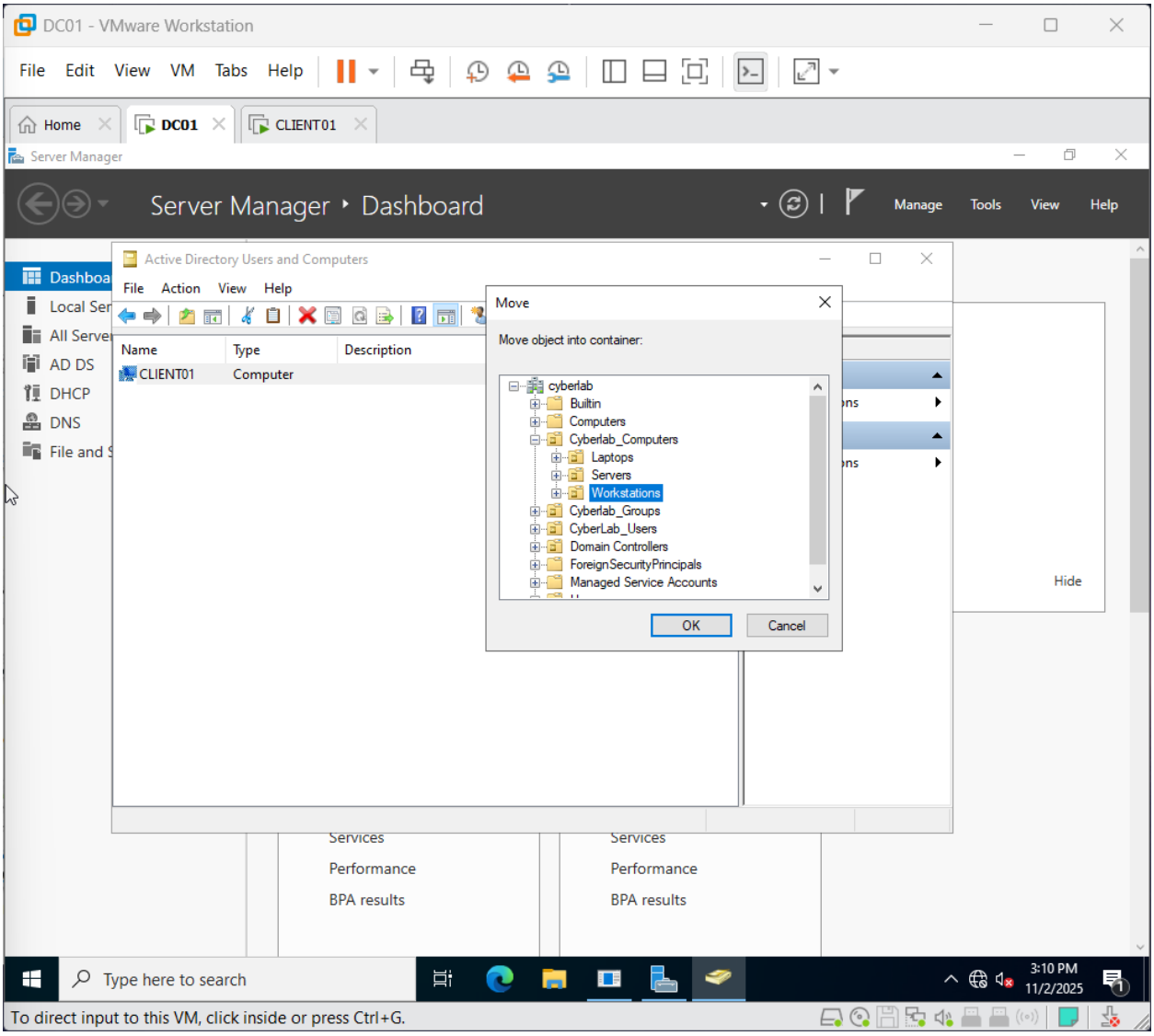

Figure 12: Moving CLIENT01 to the Workstations OU for proper organization

Phase 6: Group Policy Implementation & Security Controls

Implemented comprehensive Group Policy Objects (GPOs) to enforce security policies, desktop restrictions, and configuration management across the domain.

Step 6.1: Password Security Policy

Created and linked a Password Security Policy GPO at the domain level to enforce strong password requirements: 12 passwords remembered, maximum age 90 days, minimum age 1 day, minimum length 12 characters, complexity requirements enabled, and reversible encryption disabled.

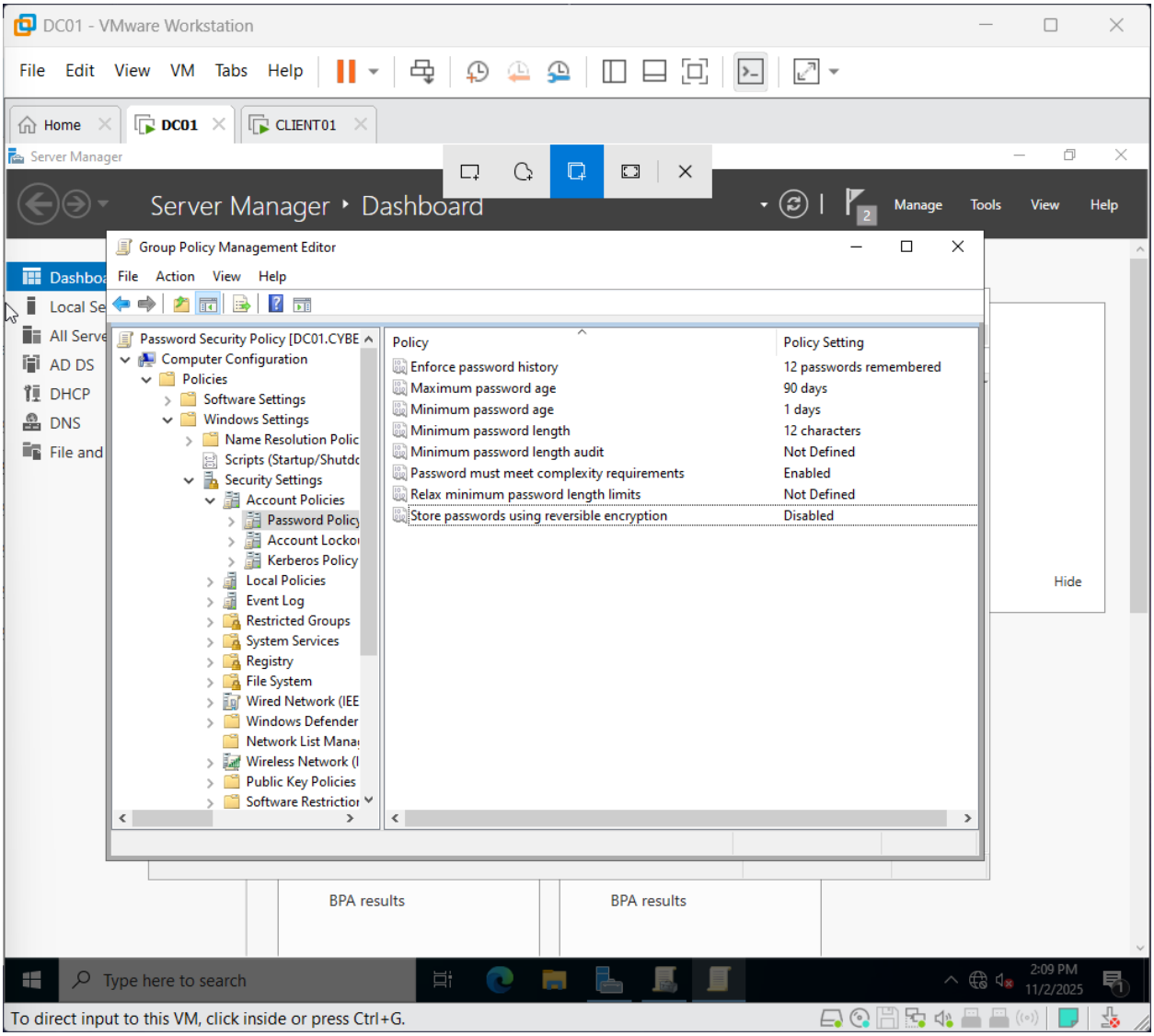

Figure 13: Password Security Policy configuration in Group Policy Management

Step 6.2: Desktop Restrictions Policy

Implemented desktop restriction policies to limit user access to sensitive system functions. This prevents unauthorized system modifications and reduces security risks by preventing access to Command Prompt, blocking access to Control Panel and PC settings, and applying these restrictions to all department users.

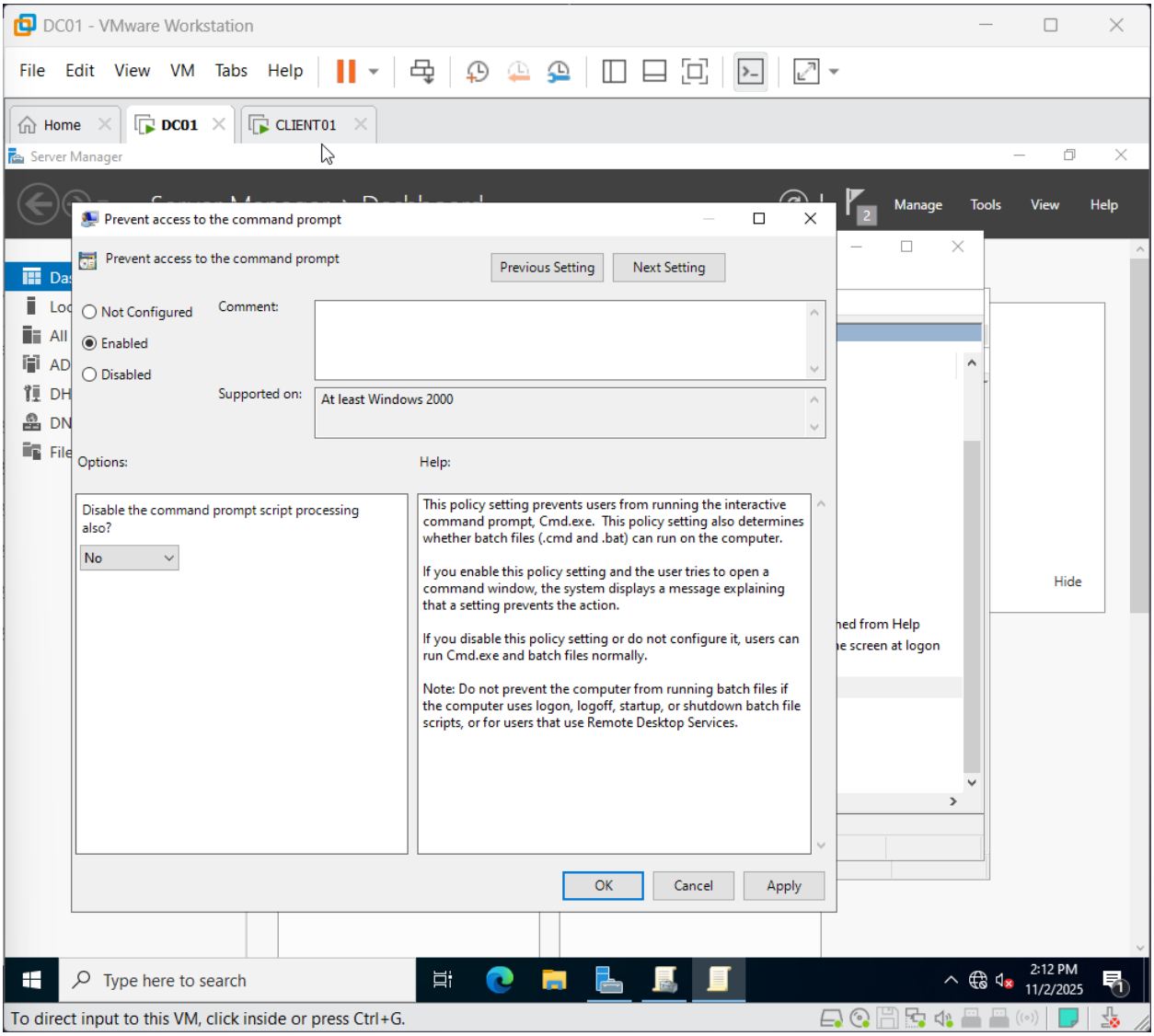

Figure 14: Group Policy setting to prevent access to command prompt

Step 6.3: Windows Firewall Policy

Configured Windows Defender Firewall settings via Group Policy to ensure consistent firewall protection across all domain computers. Firewall State is On for Domain Profile, Inbound Connections blocked by default, Outbound Connections allowed by default, applied to CyberLab_Computers OU.

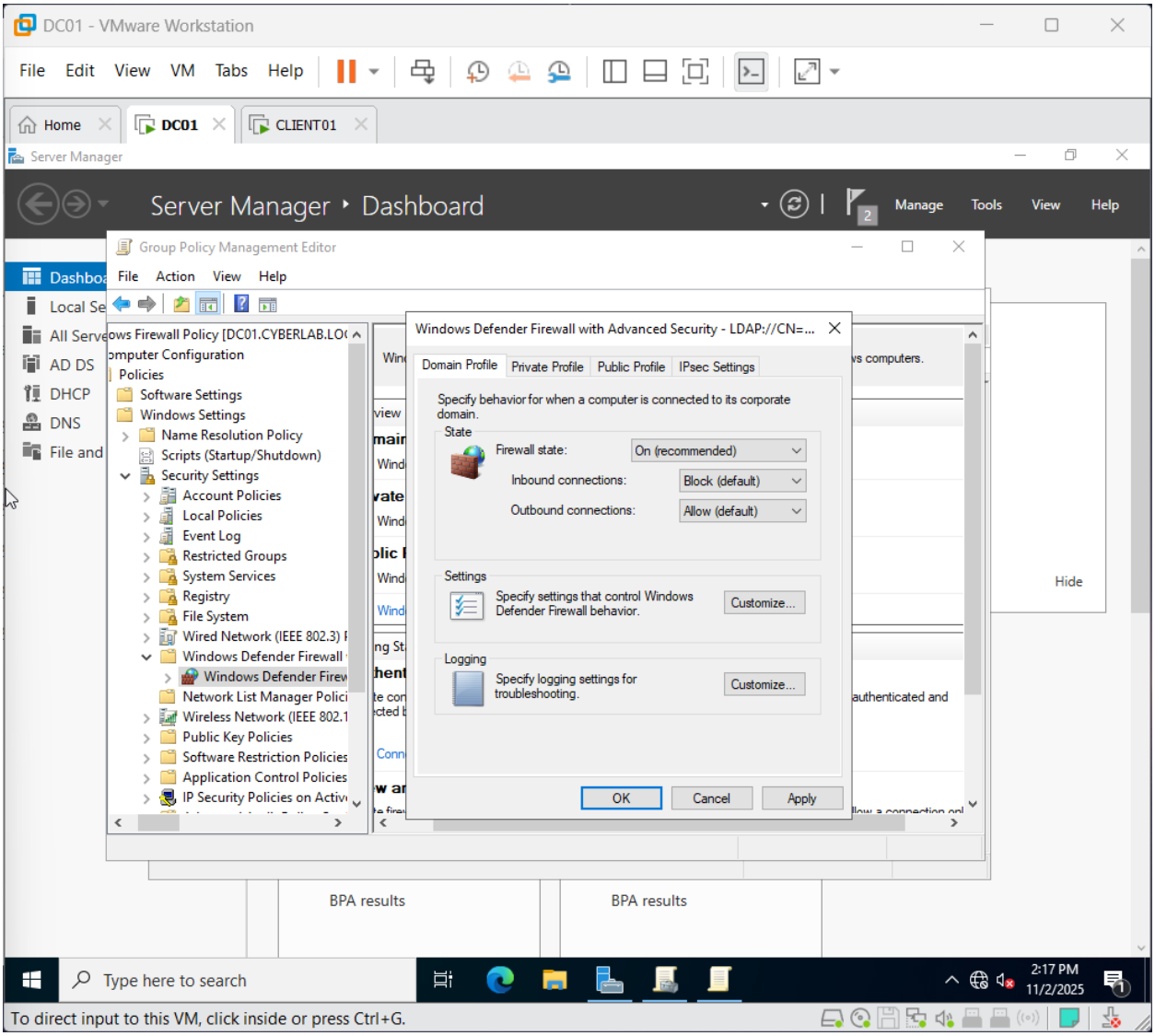

Figure 15: Windows Defender Firewall configuration in Group Policy

Step 6.4: Screen Lock and Inactivity Policy

Implemented automatic screen locking after a period of inactivity to prevent unauthorized access to unattended workstations. Machine Inactivity Limit set to 900 seconds (15 minutes), Screen Saver enabled with 900 seconds timeout, and password protection required on screen saver resume.

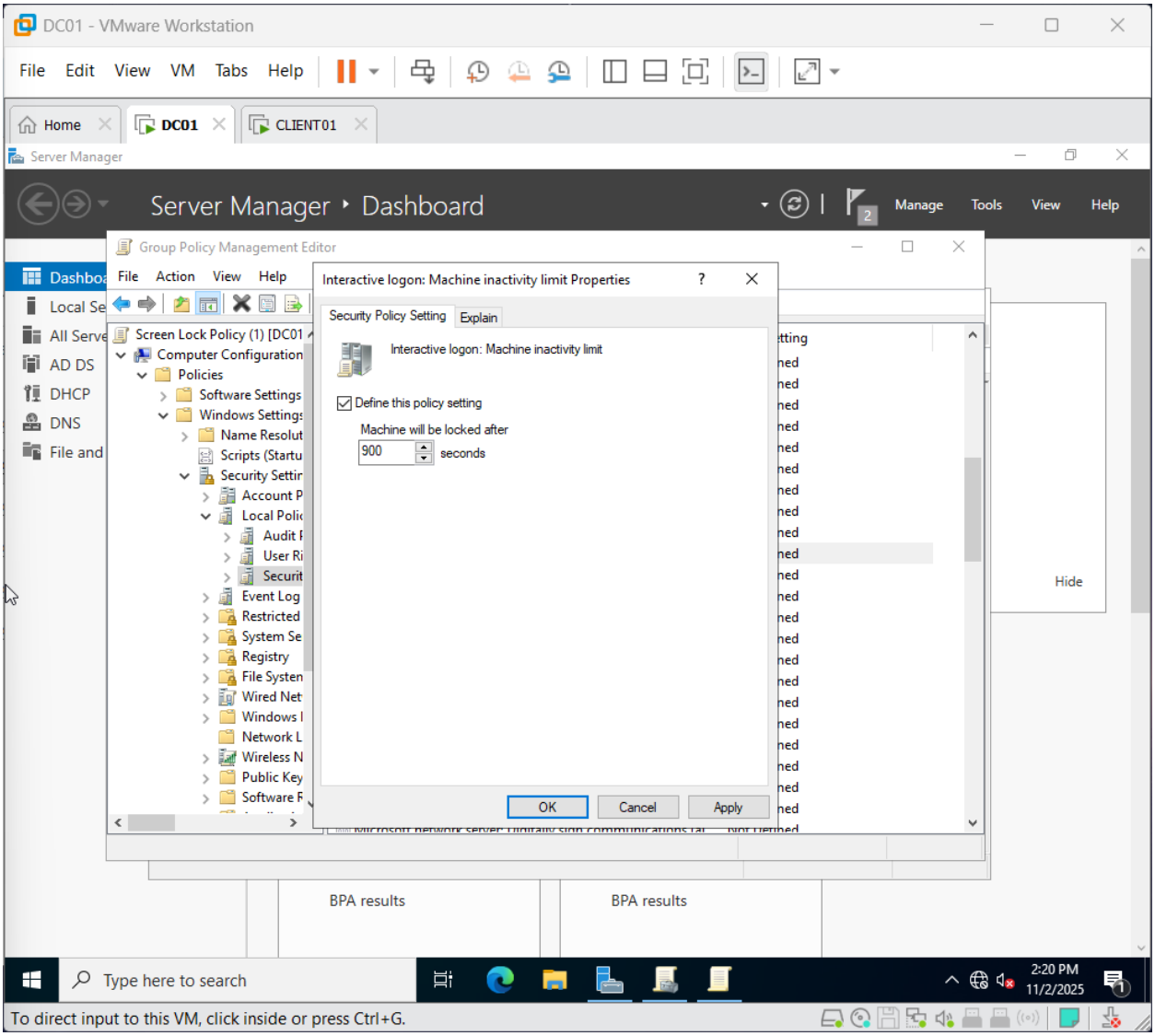

Figure 16: Machine inactivity limit policy (900 seconds / 15 minutes)

Step 6.5: Group Policy Application and Testing

After creating all Group Policy Objects, forced a policy update on CLIENT01 and verified successful application using PowerShell commands 'gpupdate /force' and 'gpresult /r'.

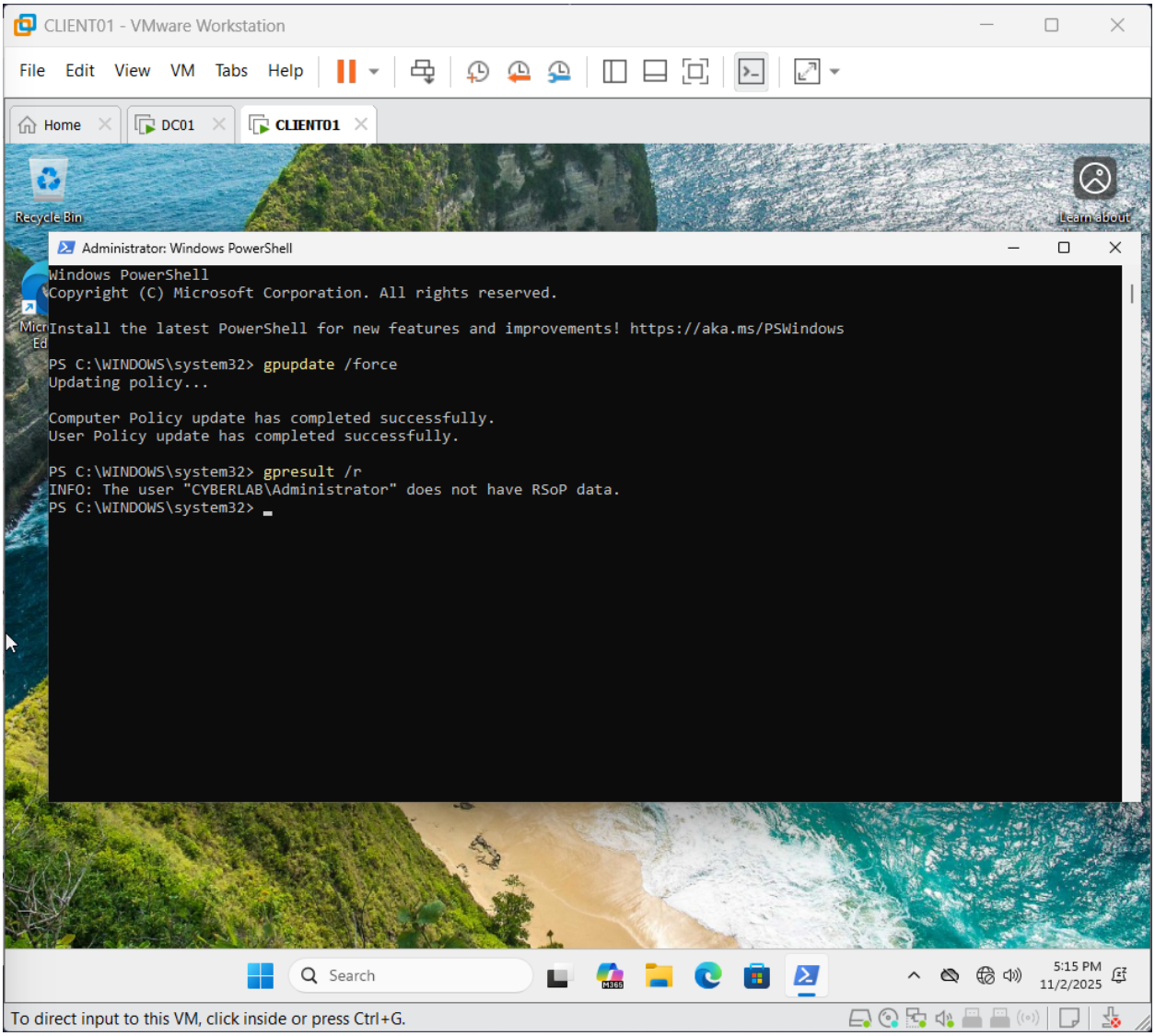

Figure 18: PowerShell commands to force Group Policy update and view results

Step 6.6: Policy Validation - Command Prompt Restriction

Tested desktop restriction policies by attempting to open Command Prompt as a standard user. The system correctly blocked access with the message 'The command prompt has been disabled by your administrator', confirming the Group Policy is properly applied and enforced.

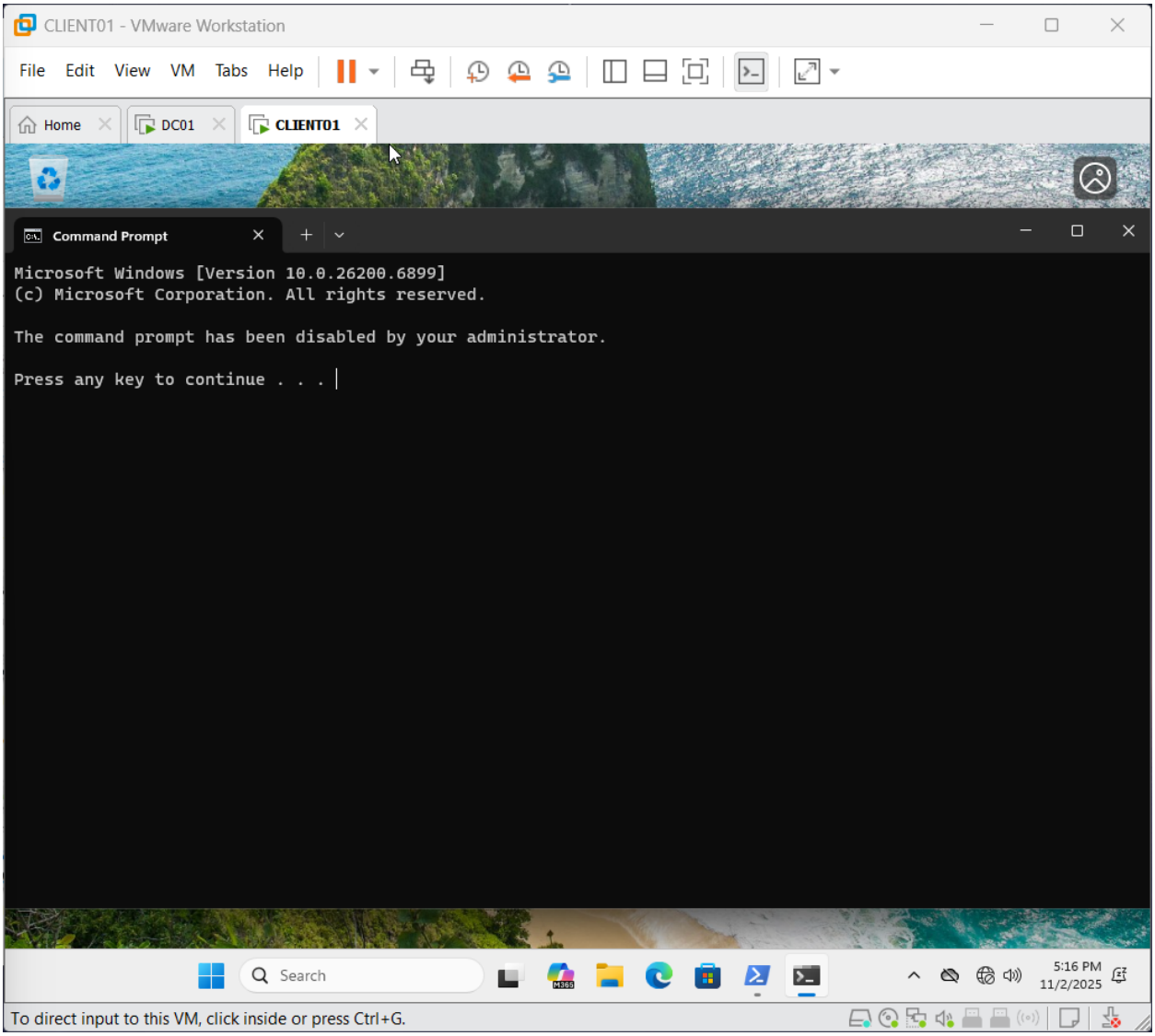

Figure 19: Command Prompt successfully blocked by Group Policy

Phase 7: Security Hardening & Best Practices

Implemented additional security hardening measures beyond basic Group Policy, including account lockout policies, audit policies, and protected user groups.

Step 7.1: Account Lockout Policy

Configured account lockout policies to protect against brute-force password attacks. Account Lockout Duration: 30 minutes, Account Lockout Threshold: 5 invalid logon attempts, Reset Lockout Counter After: 30 minutes.

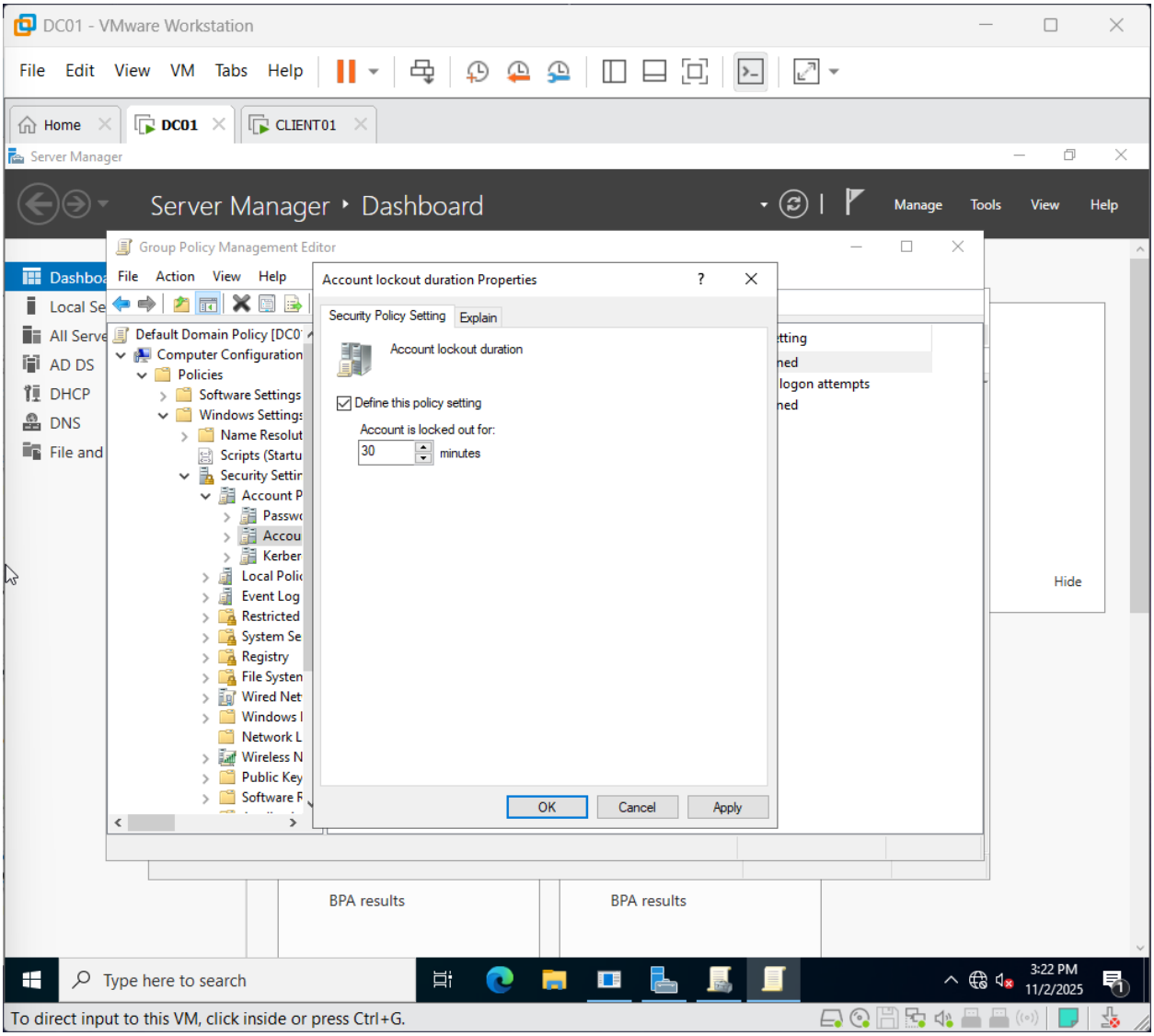

Figure 20: Account lockout duration policy (30 minutes)

Step 7.2: Advanced Audit Policy Configuration

Enabled comprehensive audit policies to track security-relevant events across the domain. These audit logs are essential for security monitoring, incident response, and compliance requirements. Configured auditing for Account Logon, Account Management, Logon/Logoff, Object Access, Policy Change, and Privilege Use.

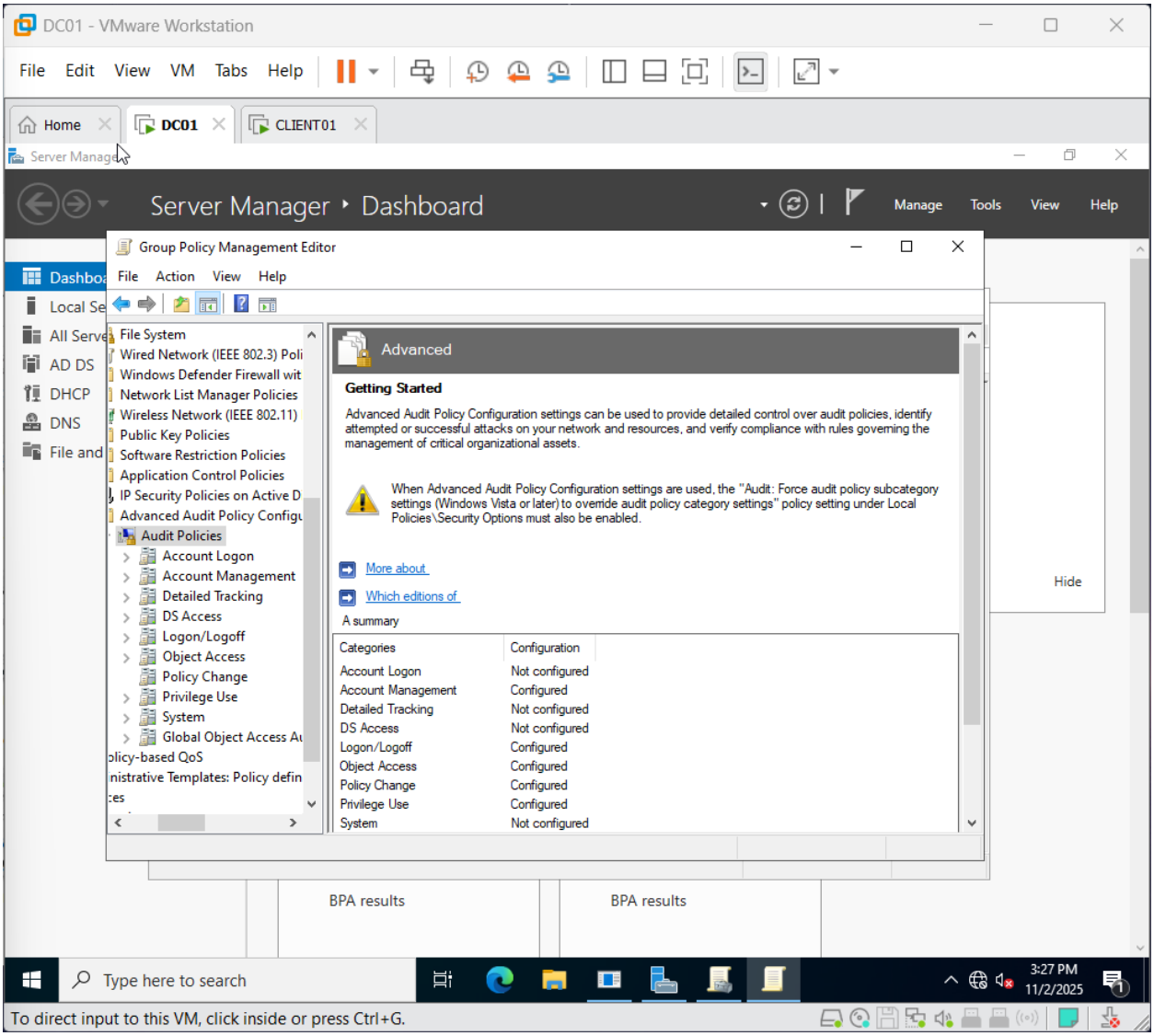

Figure 22: Advanced Audit Policy Configuration categories

Step 7.3: Protected Users Security Group

Added security team members (Emily Davis and Jane Doe) to the Protected Users group. This built-in security group provides additional Kerberos authentication protections, prevents NTLM authentication, and clears credentials from memory after logoff—critical defenses against pass-the-hash and credential theft attacks.

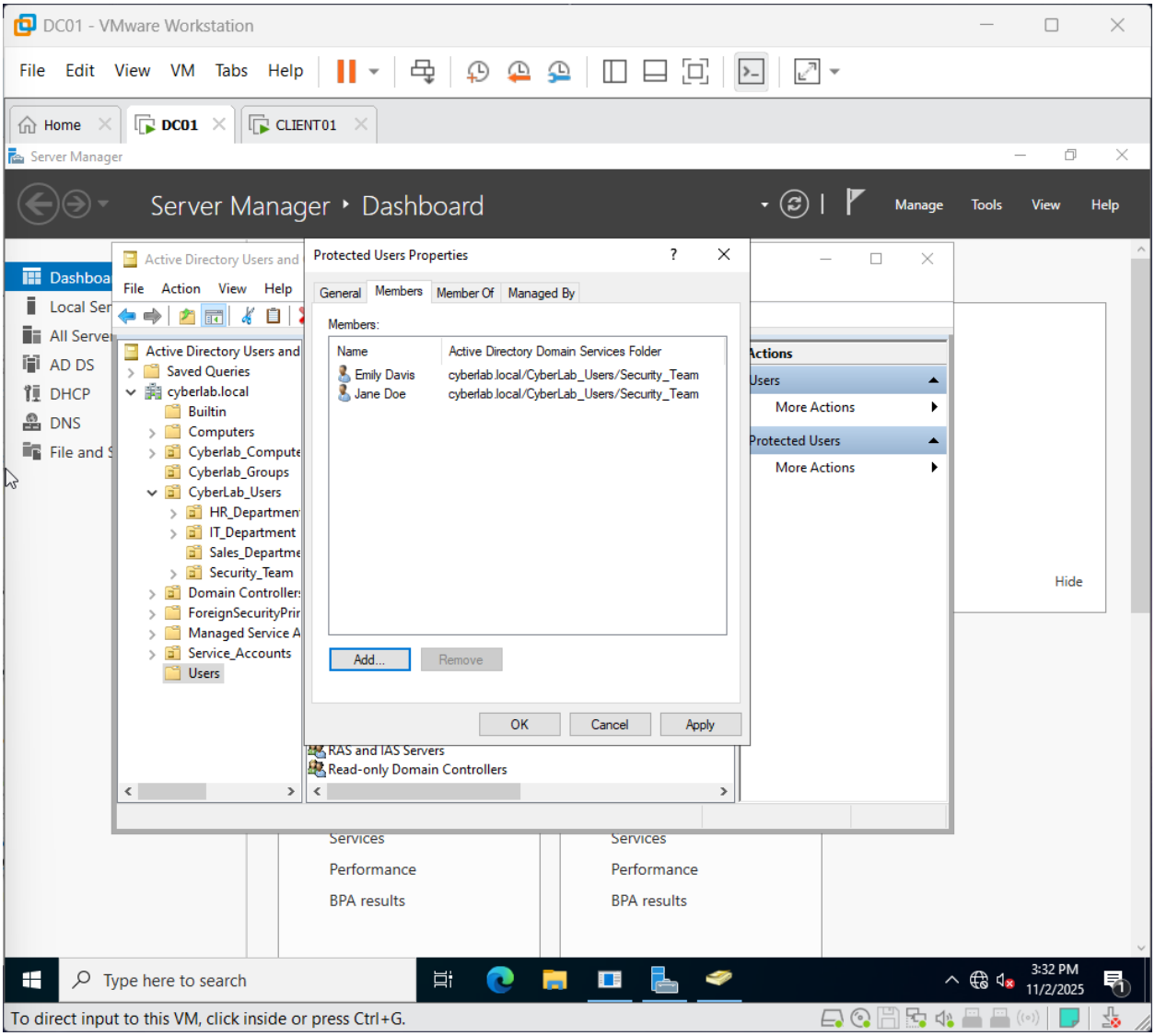

Figure 23: Protected Users group membership for security team accounts

Phase 8: Security Monitoring & Event Logging

Configured comprehensive event logging and verified that security events are being properly captured.

Step 8.1: Event Log Verification

Reviewed Windows Security Event Log on the domain controller to confirm audit policies are generating logs correctly. Event ID 4624 (successful logon) entries confirm user authentication events are being captured with detailed information including user names, source IP addresses, and logon types.

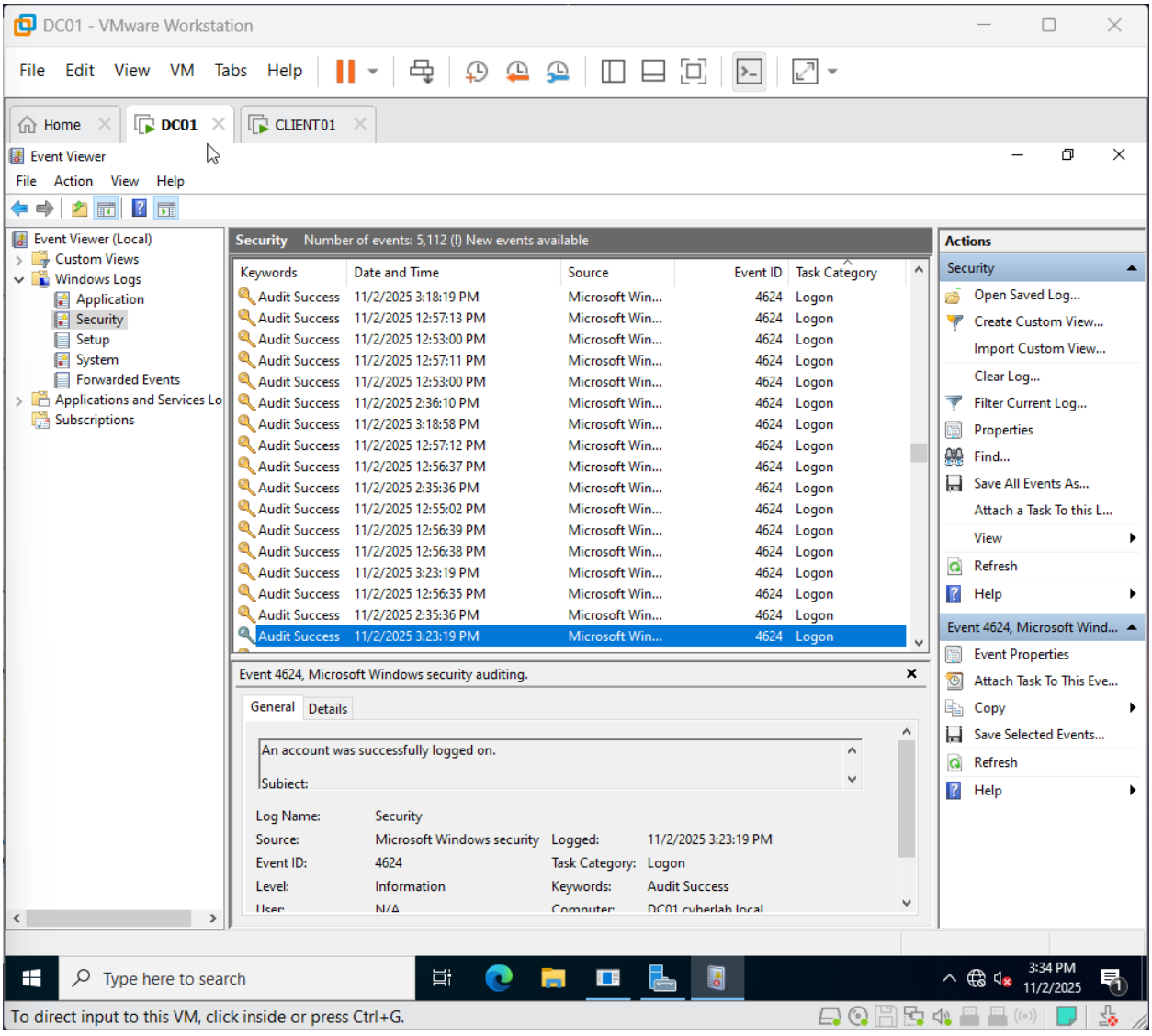

Figure 24: Security Event Log showing Event ID 4624 (successful logon) entries

Conclusion

This laboratory exercise successfully demonstrates comprehensive hands-on experience with enterprise Windows Server and Active Directory infrastructure. The implementation covers the complete lifecycle from initial server deployment through security hardening and operational monitoring.

The configuration follows industry best practices and mirrors real-world enterprise environments used by 95% of Fortune 500 companies. All implementations utilize legitimate evaluation software and represent genuine technical competency suitable for professional IT and cybersecurity positions.