On-Premises Identity & Access Management W/ Active Directory Lab

Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Oracle VirtualBox, Windows Server 2025, Windows 10 Pro VM |
PORTFOLIO WEBSITE: https://www.saintmaiden.site/

EXECUTIVE SUMMARY:

PROBLEM:	SOLUTION:	IMPACT:
A growing financial firm requires a centralized identity management infrastructure to support 20 new employees across 5 departments while enforcing strict compliance, folder segmentation, and endpoint protection against unauthorized media.	Designed and deployed an isolated Windows 2025 Server Active Domain Directory Services (corp.local) environment with segmented Organizational Units (OUs), Role-Based Access Controls (RBACs) via security groups, and Baseline Group Policy Objects (GPOs).	Established centralized identity governance, enforced the Principle of Least Privilege (PoLP) across confidential department data, and hardened network endpoints against physical USB threat vectors.

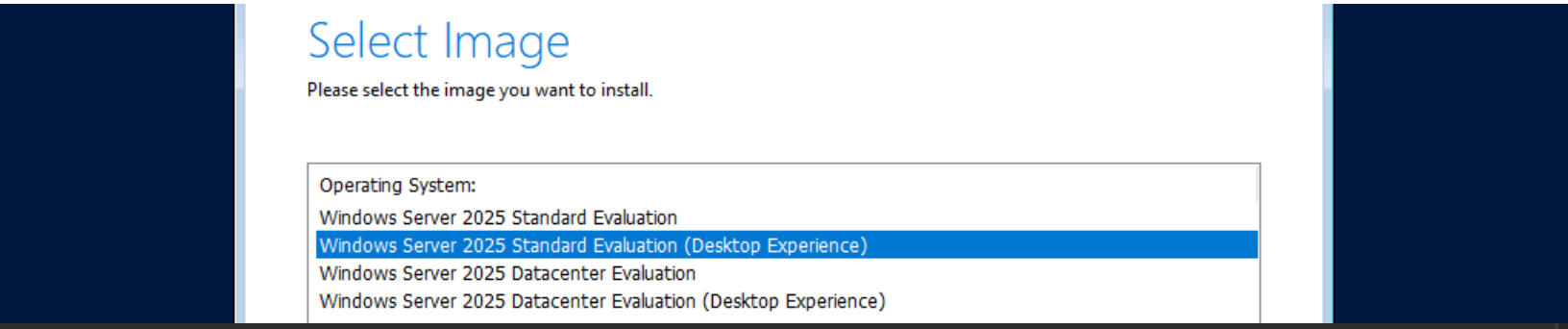
TECHNICAL TOPOLOGY/SPECIFICATIONS:

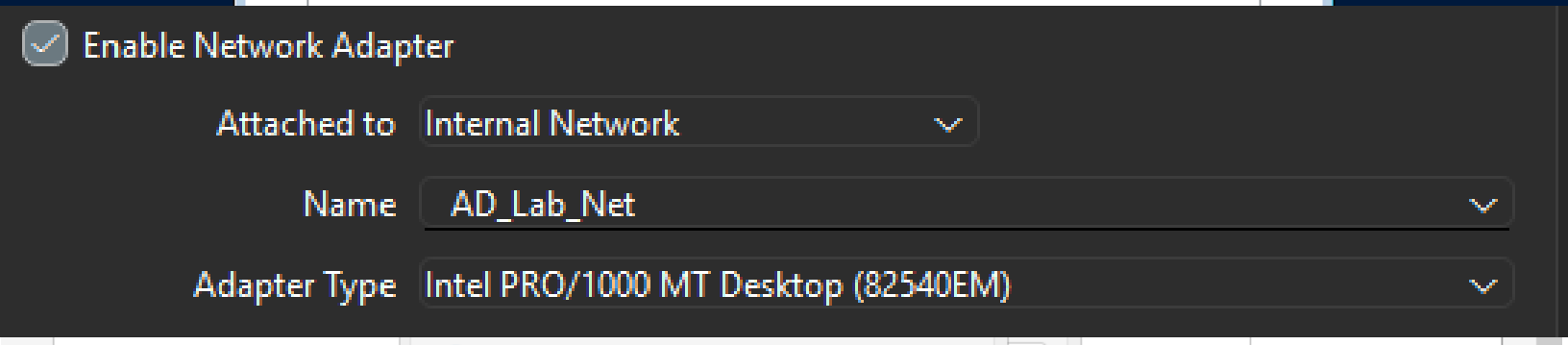
COMPONENT/ROLE	SYSTEM/HOST NAME	NETWORK MODE & IP ADDRESS	SUBNET MASK/DNS SETTINGS	SERVICES & ROLES
Domain Controller	WINSERV555 (Windows Server 2025	Internal Network (AD_Lab_Net)/192.168.10.10 (Static)	Subnet: 255.255.255.0/DNS: 192.168.10.10	AD DS, DNS SERVER, SHARED FILES, NTDS DATABASE
Client Workstation	WINCLIENT555 (Windows 10 Pro)	Internal Network (AD_Lab_Net)/192.168.10.50 (Dynamic/Static)	Preferred DNS: 192.168.10.10	Windows 10 Pro Domain Member

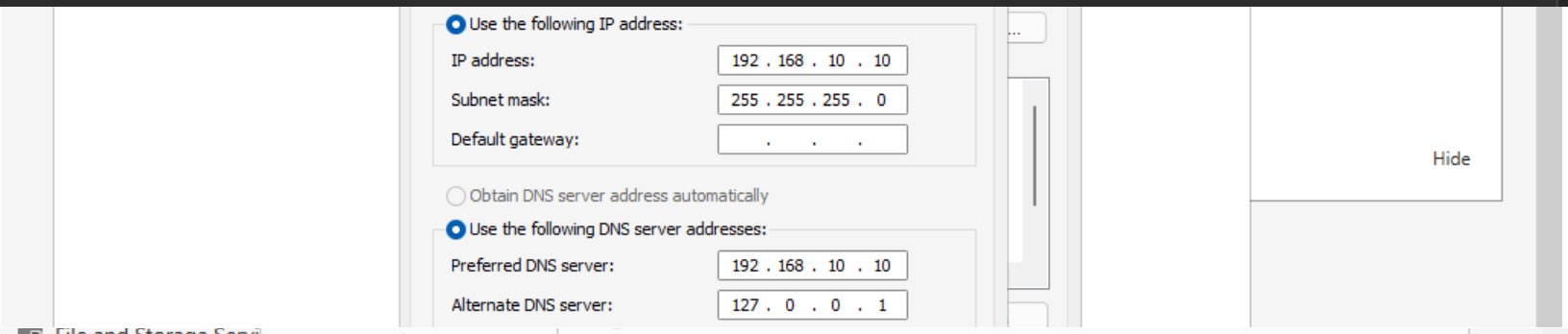
PHASE 1: VIRTUAL INFRASTRUCTURE AND DOMAIN PROMOTION

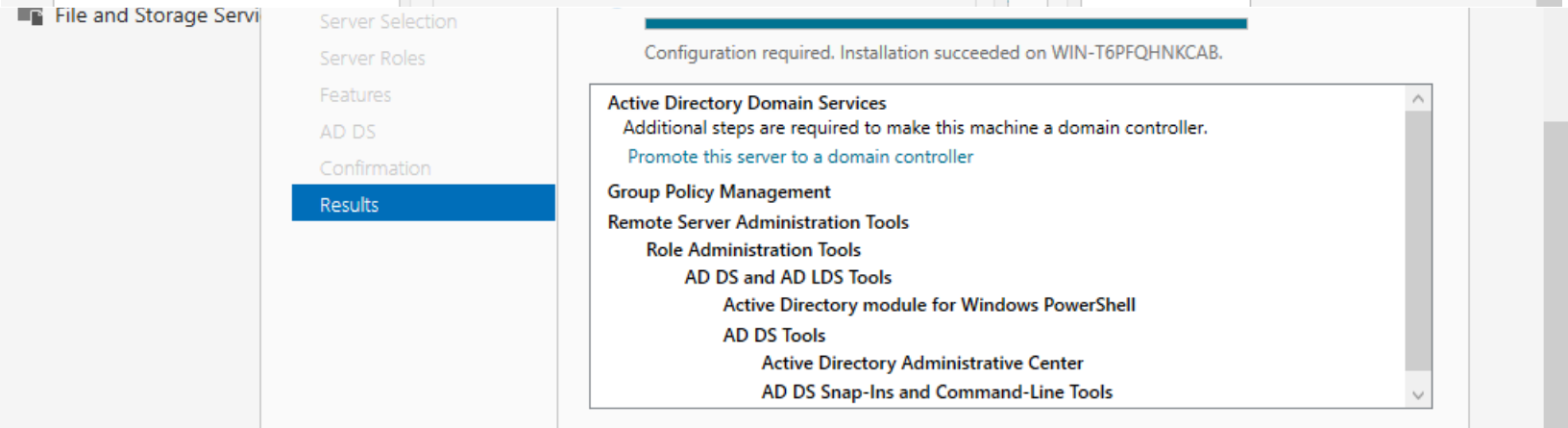
ACTION: Deployed an isolated VirtualBox host-only internal network (AD_Lab_Net), configured IPv4/DNS parameters, installed Active Directory Domain Services on the Windows Server 2025, and promoted it to Domain Controller for the Forest Root Domain "corp.local".

WHY?: Virtualization isolates domain configuration from host networks to save costs, while Static DNS configurations ensure that clients can discover and join the server with no hassle.



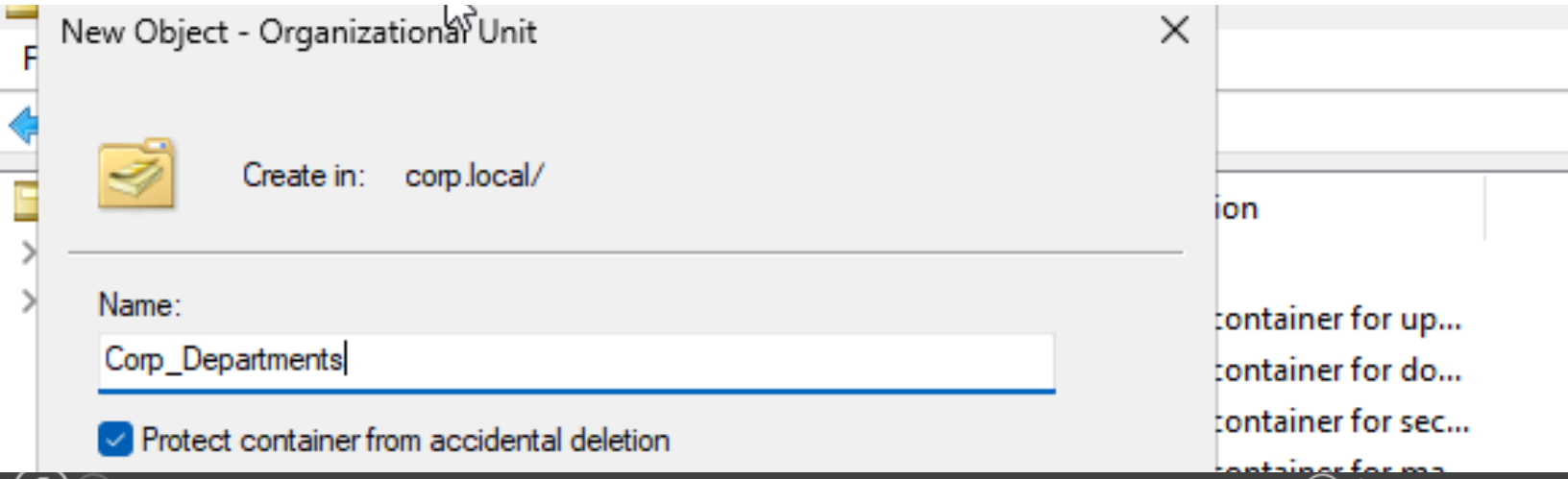


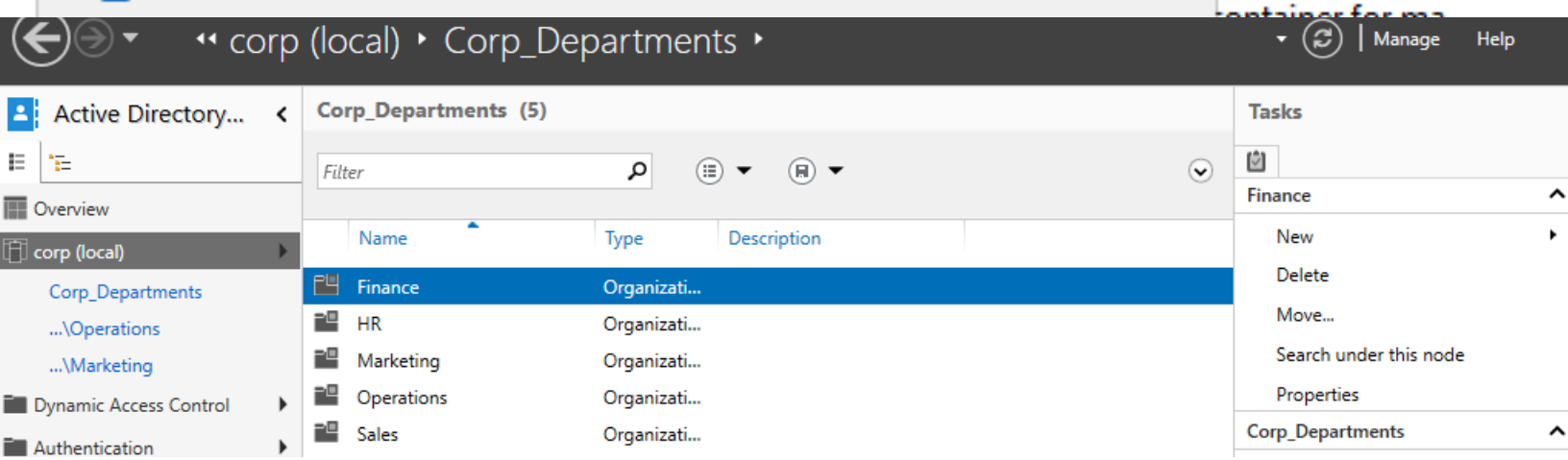


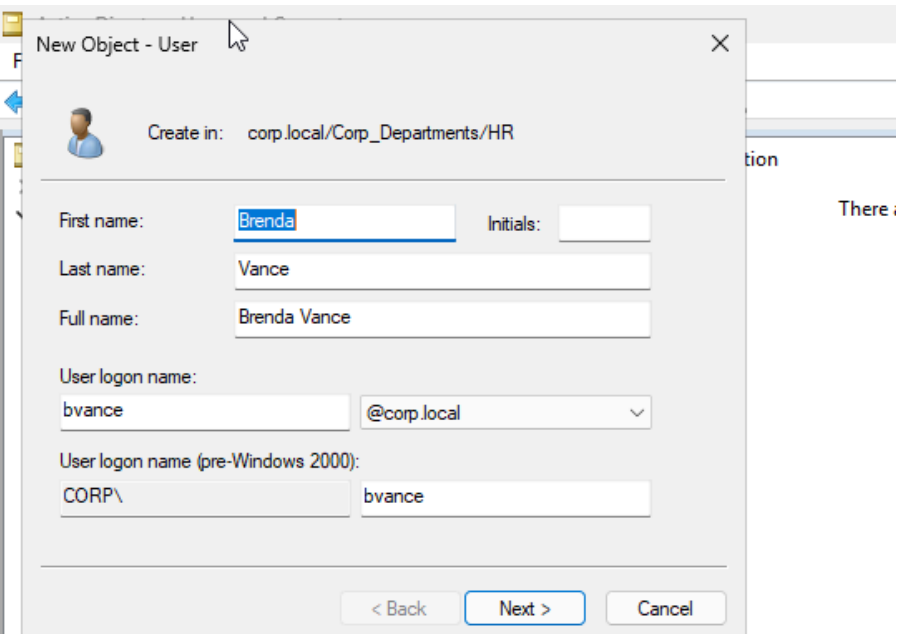


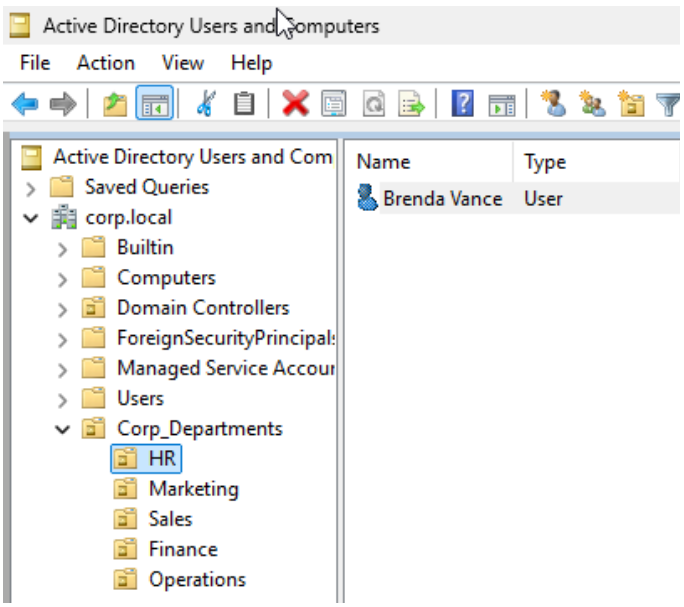
PHASE 2: OU HIERARCHY & BULK USER PROVISIONING:

ACTION: Constructed a top-level Organizational Unit (Corp_Departments) containing Sub-OUs for Finance, Operations, HR, Marketing, and Sales, followed by provisioning 20 initial user accounts using Active Directory Administrative Center.
WHY?: Segmenting directory objects by department streamlines policy targeted delivery (GPO Scope) and simplifies administrative access control across the domain.



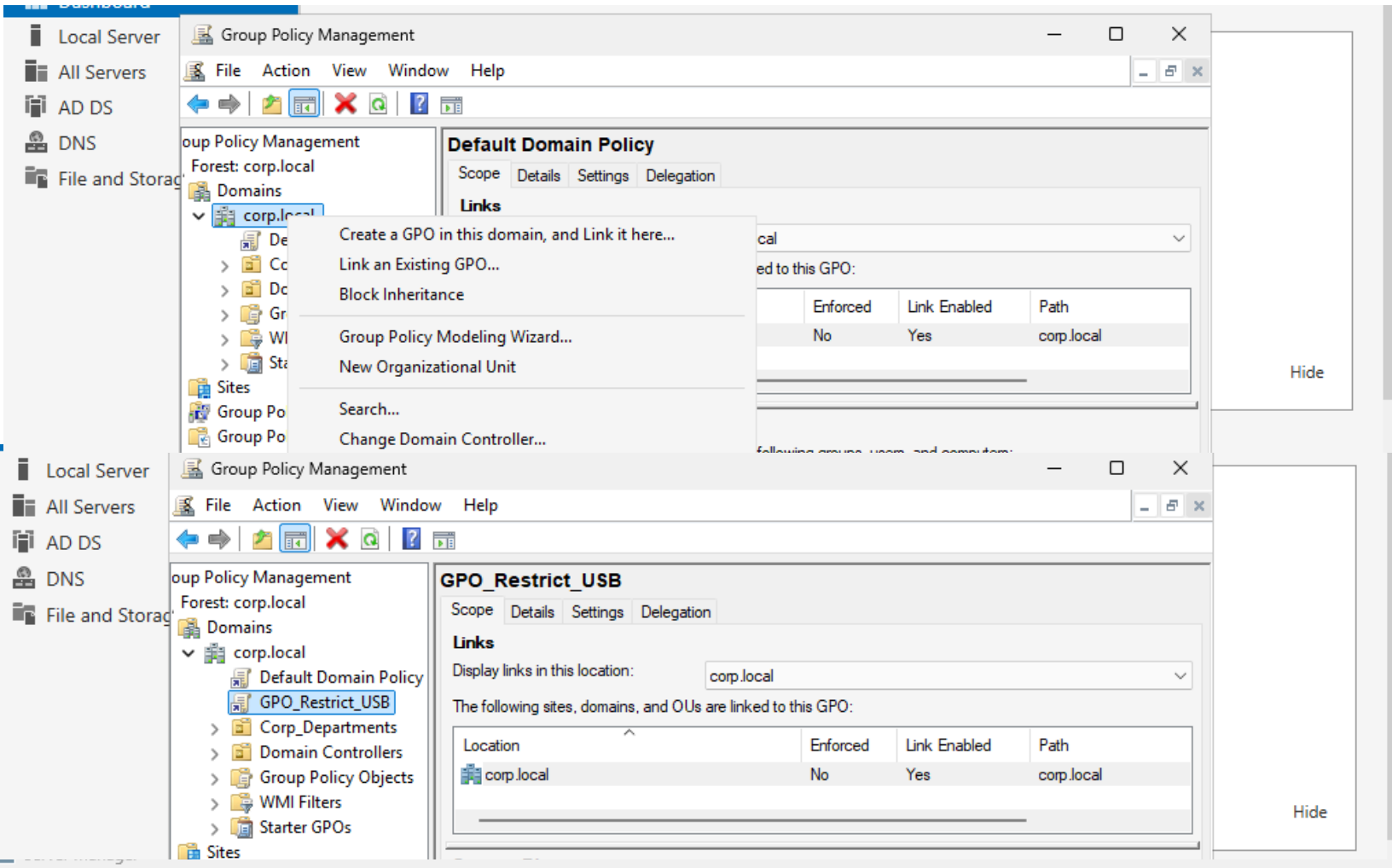


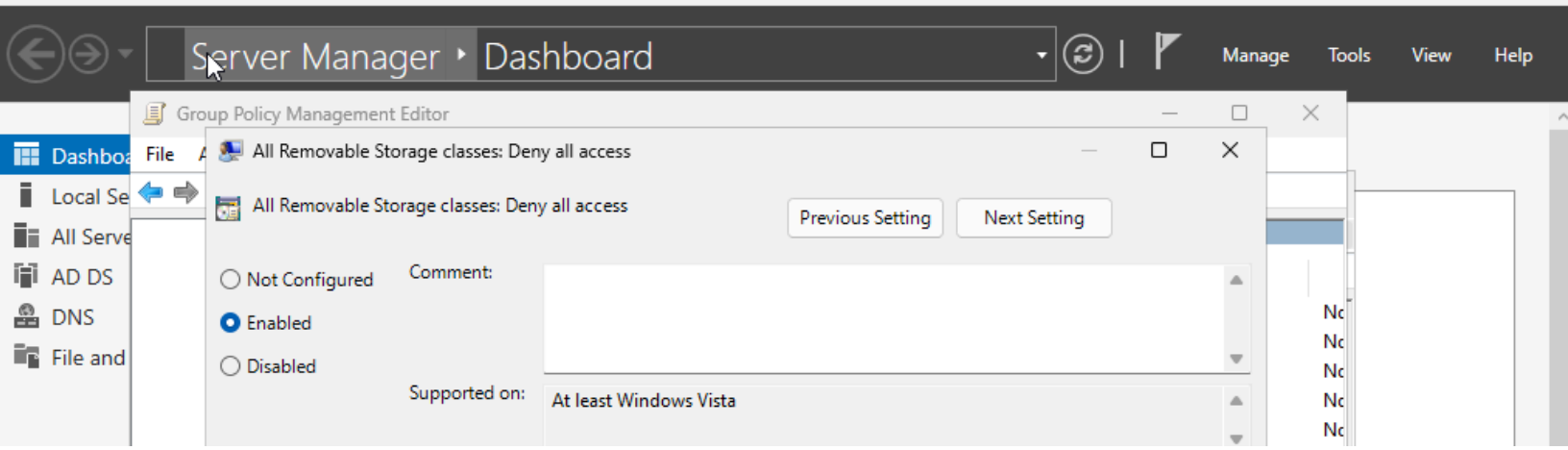




PHASE 3: ENDPOINT HARDENING & BASELINE SECURITY (GPO)

ACTION: Created and linked the `GPO_Restrict_USB` Group Policy Object to the `corp.local` domain root, enabling *All Removable Storage classes: Deny all access.*
WHY?: Mitigates physical attack vectors and rogue hardware incidents (e.g., untrusted USB malware/ransomware delivery) by enforcing a strict security baseline across all workstation endpoints.

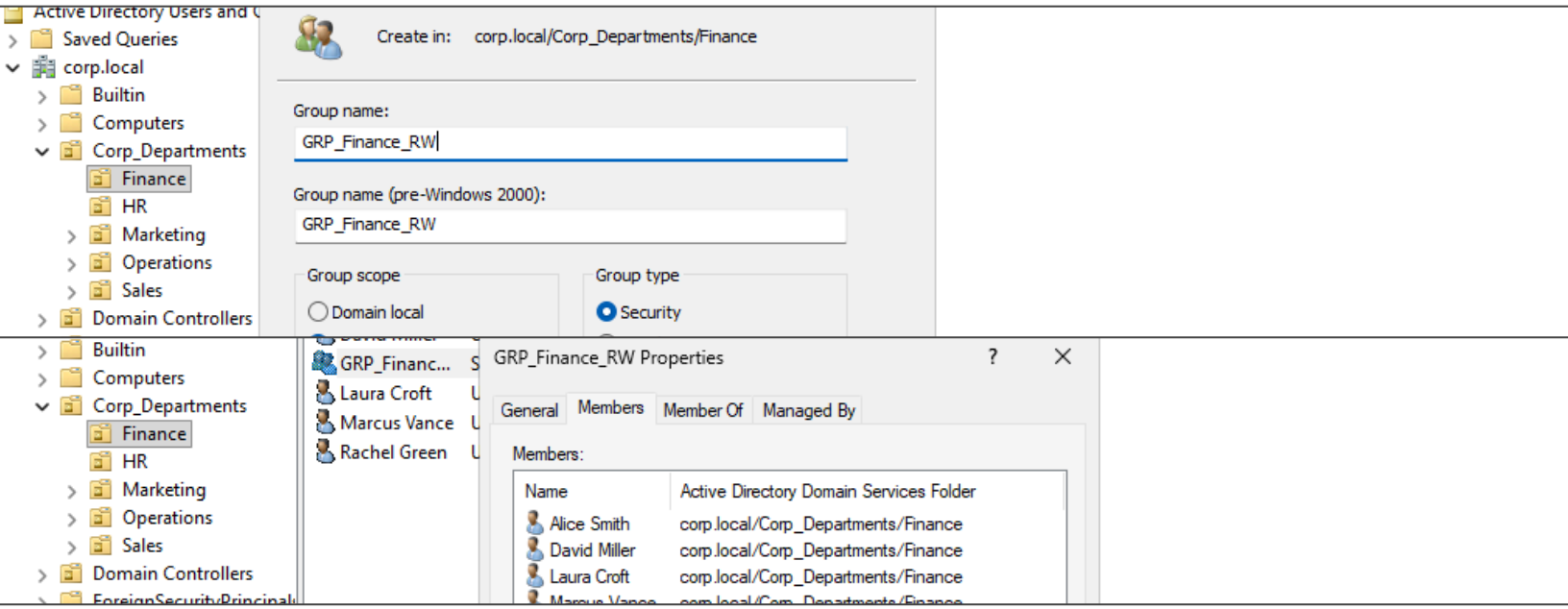


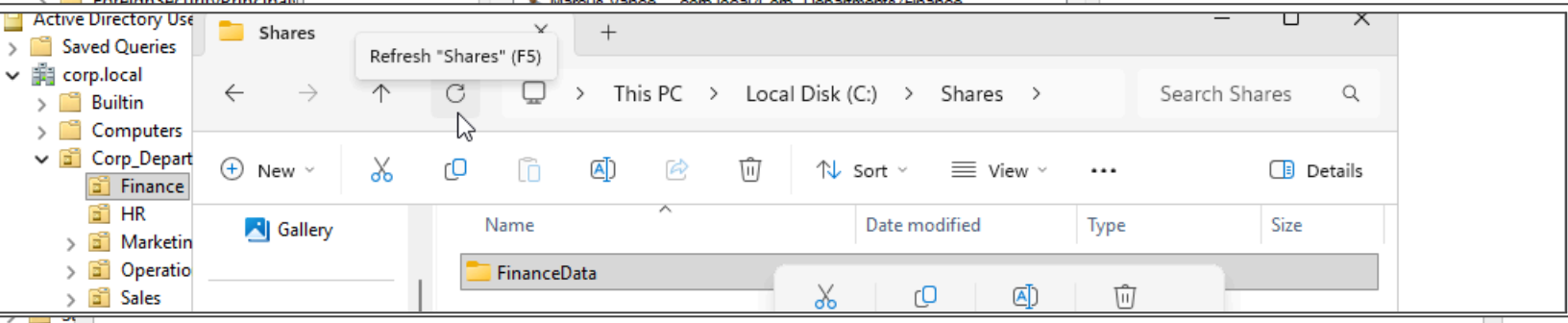


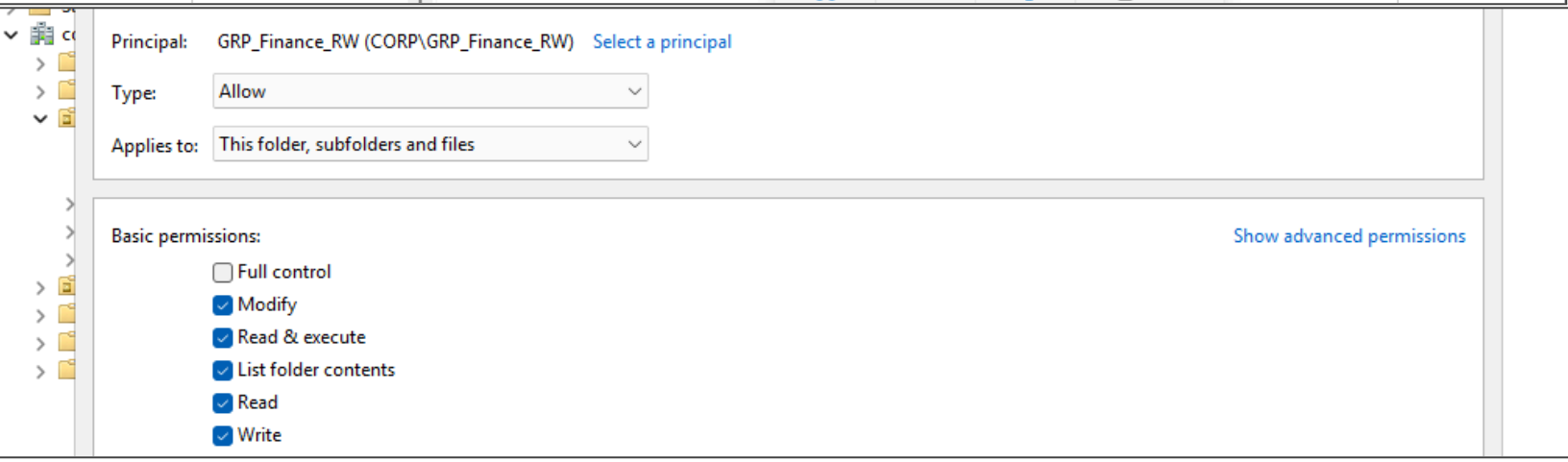
PHASE 4: ROLE-BASED ACCESS CONTROL (RBAC) & DATA SEGREGATION

ACTION: **Configured security group `GRP_Finance_RW`, added Finance department users, created path `C:\Shares\FinanceData`, disabled NTFS permission inheritance, and granted explicit Read/Write/Execute permissions to `GRP_Finance_RW`.**

WHY?: **Prevents cross-departmental data leakage ("prying eyes") and strictly enforces Least Privilege by managing access at the security group level rather than assigning explicit individual permissions.**



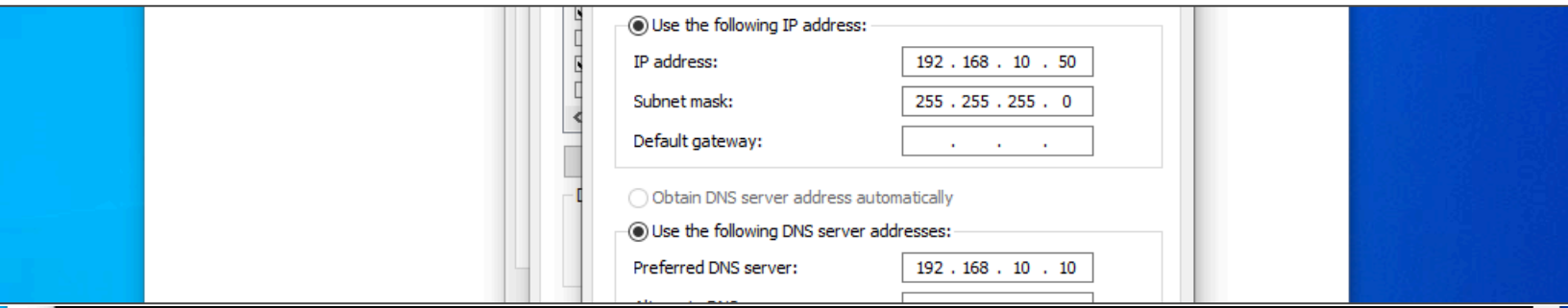


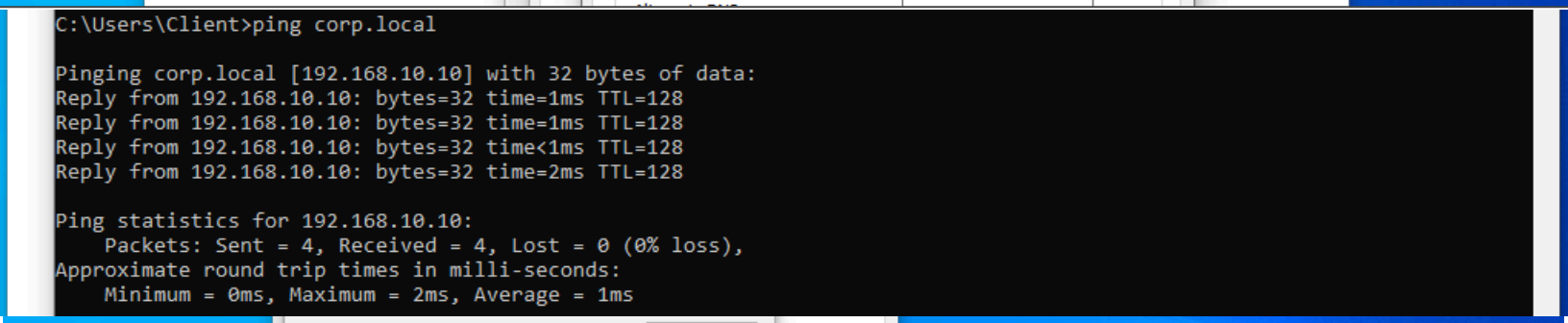


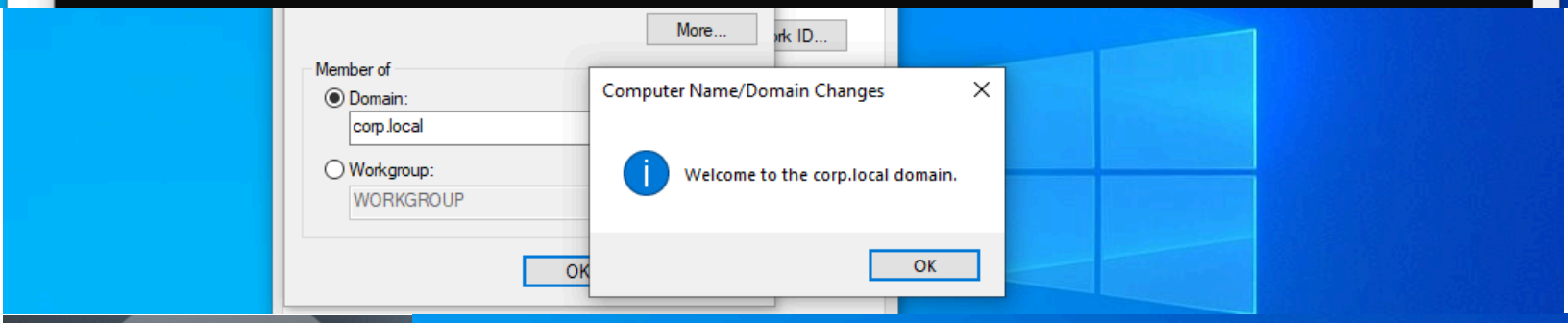
PHASE 5: END-TO-END VERIFICATION AND DOMAIN JOIN

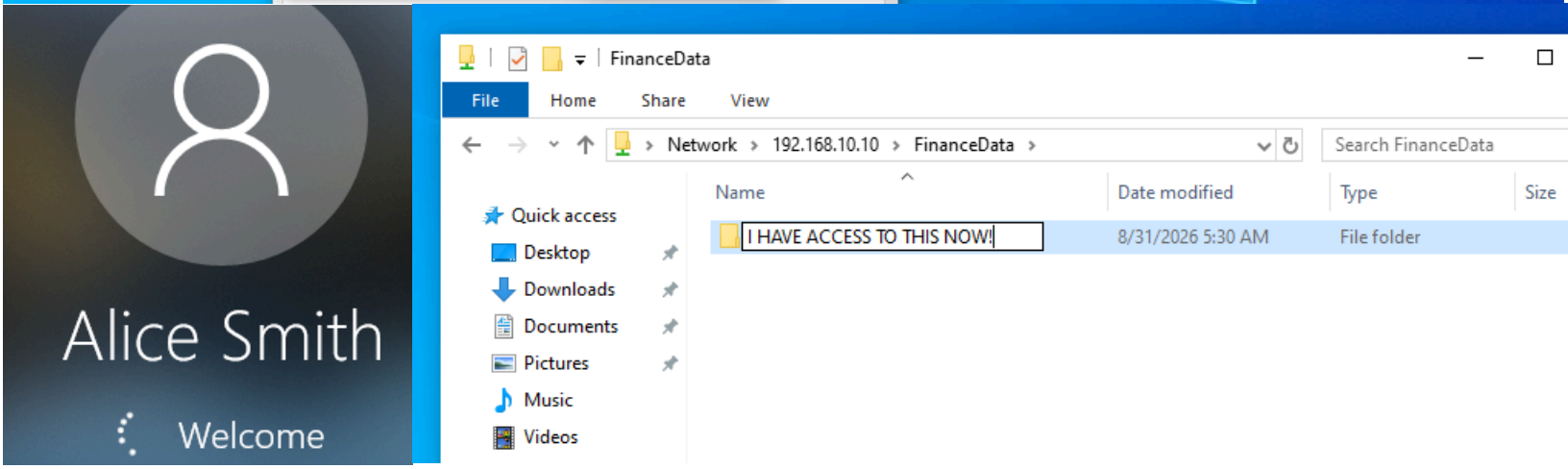
ACTION: **Configure client IP/DNS settings on `WINCLIENT555`, verified ICMP connectivity (`ping corp.local`), completed domain join to `corp.local`, and authenticated as user `Alice Smith (asmith)` to test file share permissions (\\192.168.10.10\FinanceData)**

WHY?: **This will validate Active Directory authentication, DNS resolution, and verifies that NTFS/SMB share permissions function as expected for authorized end users.**









TECHNICAL SUMMARY:

SECURITY DOMAIN	TECH & CONTROLS CONFIGURED
DIRECTORY INFRASTRUCTURE	AD DS Domain Controller Promotion, Root Forest setup (corp.local), NTDS Database
IDENTITY GOVERNANCE	Organizational Unit Structure (Corp_Departments), Bulk User Provisioning
ACCESS CONTROL & LEAST PRIVILEGE	Security Group RBAC (GRP_Finance_RW), Explicit NTFS/Share Permission Inheritance Override
ENDPOINT SECURITY & POLICY	Group Policy Object Deployment (GPO_Restrict_USB), Removable Storage Prevention Baseline
VIRTUAL NETWORKING	Isolated Internal Virtual Switch, Static IPv4/DNS Resolution, Workstation Domain Join Verification

RESULT & BUSINESS IMPACT:

- **CENTRALIZED IDENTITY GOVERNANCE:** Established structured OU management and streamlined directory object administration for scalable user onboarding.
- **HARDENED ENDPOINT SECURITY BASELINE:** Prevented physical rogue hardware risks by enforcing domain-wide USB execution restrictions via GPO.
- **ENFORCED PRINCIPLE OF LEAST PRIVILEGE:** Secured sensitive departmental shares using group-based RBAC, ensuring confidential data remains isolated from unauthorized personnel.
- **VERIFIED PRODUCTION READINESS:** Completed domain authentication and resource validation via client workstation testing to ensure operational readiness

Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Oracle VirtualBox, Windows Server 2025, Windows 10 Pro VM | **PORTFOLIO WEBSITE:** https://www.saintmaiden.site/