Active Directory User Provisioning – Lab Demonstration

Summary

This lab demonstrates my ability to provision, modify, and deprovision user accounts in an Active Directory environment. The tasks performed align with core Identity & Access Management (IAM) responsibilities, including user onboarding, role-based access control (RBAC), least privilege enforcement, and secure offboarding.Completed using the TestOut Security Pro 8.0 lab environment.

Environment & Tools

• CompTIA Security+ training platform

• Windows Server environment

• Active Directory Users and Computers (ADUC)

Skills Demonstrated:

• User creation & identity lifecycle management

• Role-based access assignment

• Least privilege implementation

• Account disablement/deprovisioning

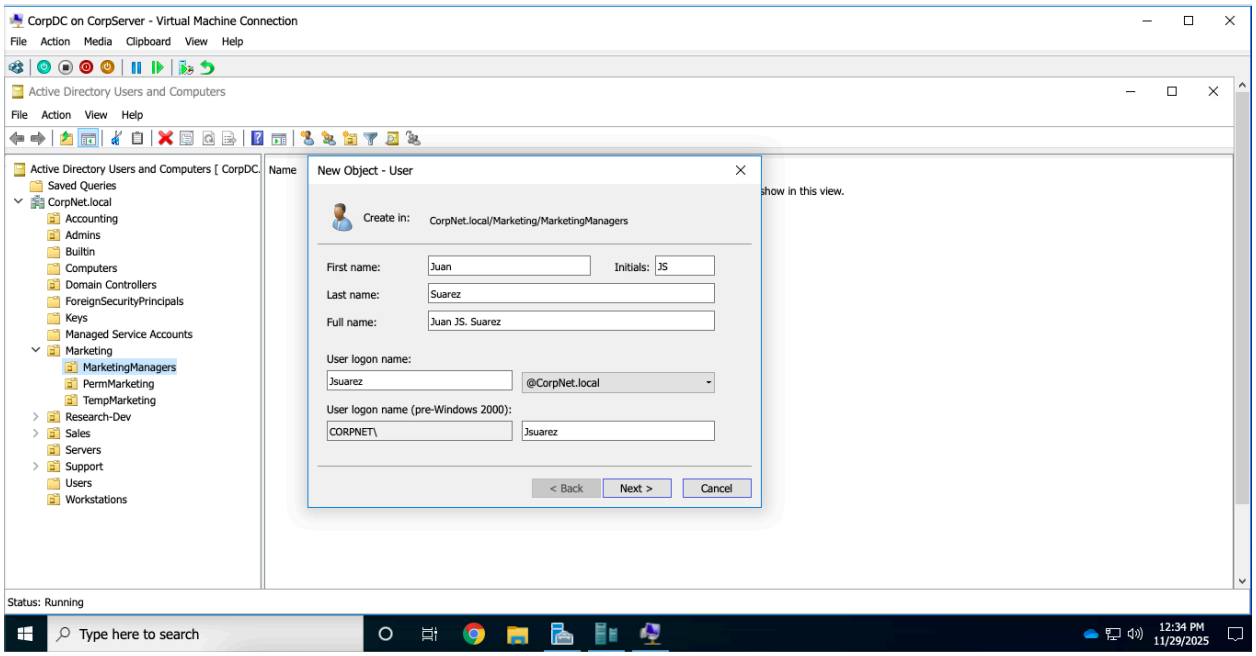
• Group-based permissions (RBAC)

Step-by-Step Implementation

Step 1 — Create a New User Account

Actions Performed:- Created a new AD user within the appropriate Organizational Unit (OU).- Assigned username, display name, and logon details.- Configured 'User must change password at next logon.'

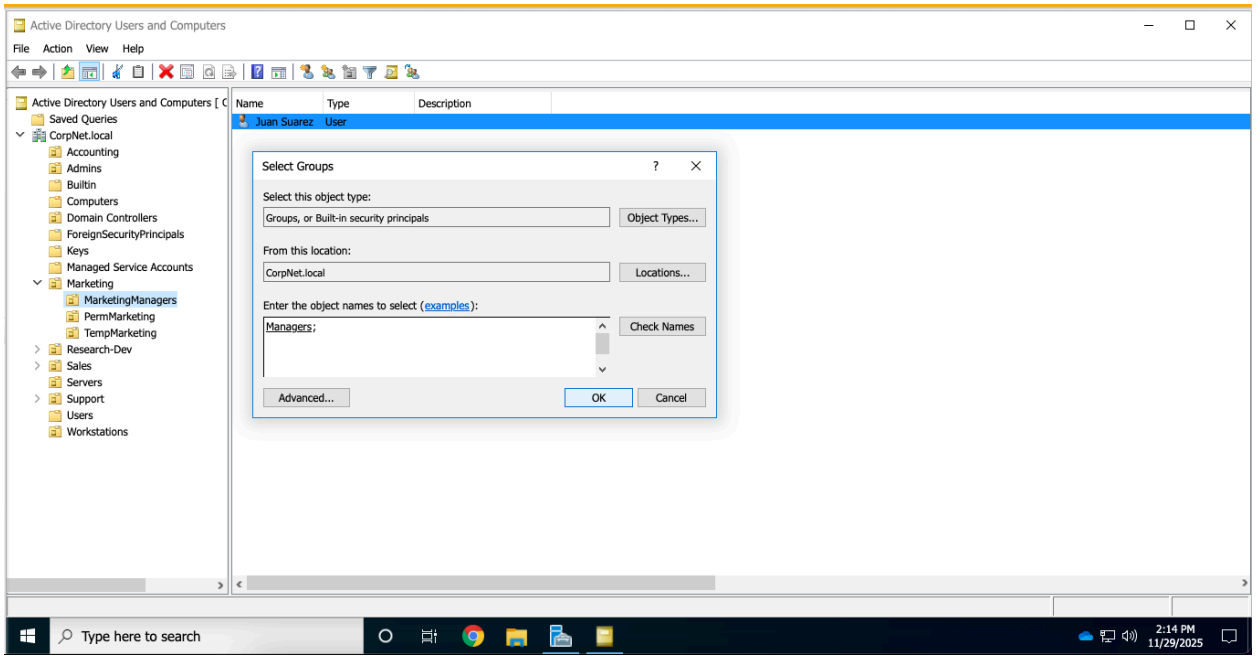
Why It Matters:Provisioning ensures correct identity setup and traceability.



Step 2 — Assign Security Groups (RBAC)

Actions Performed:- Added the user to job-role-appropriate security groups.- Ensured least privilege by avoiding direct folder permissions.

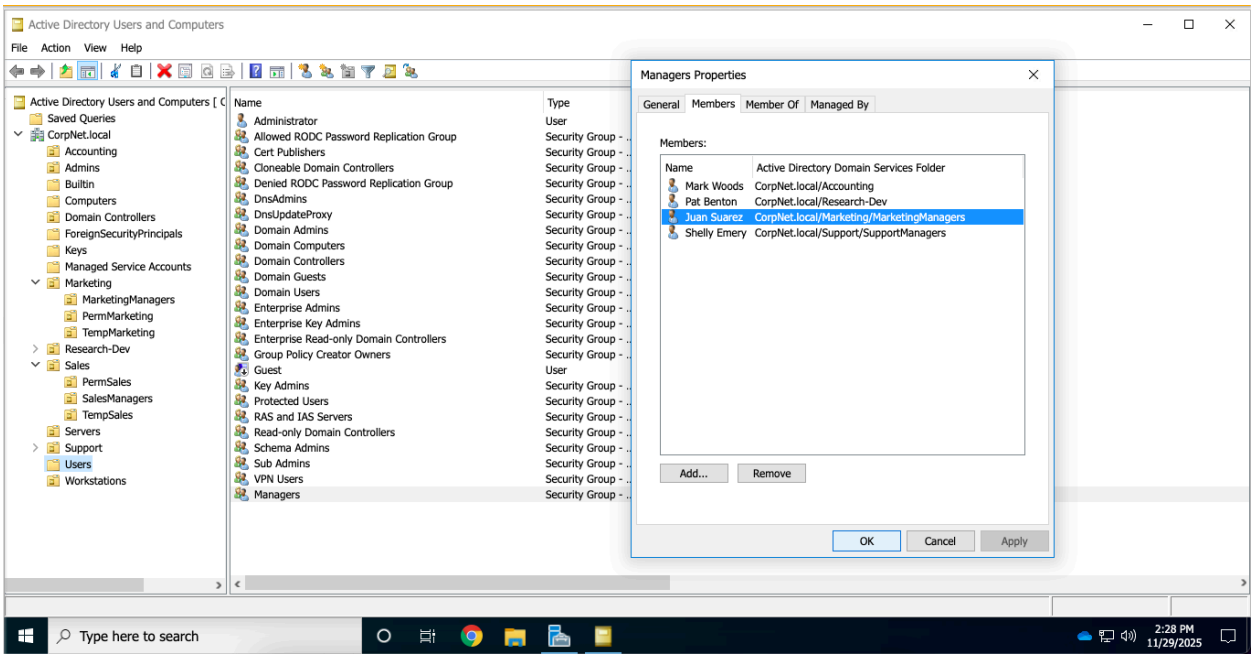
Why It Matters:RBAC ensures consistent, scalable authorization control.



Step 3 — Apply Permissions Using Groups (Least Privilege)

Actions Performed:- Verified access to relevant shared folders was controlled via group membership.- Ensured the user did not inherit unnecessary permissions.

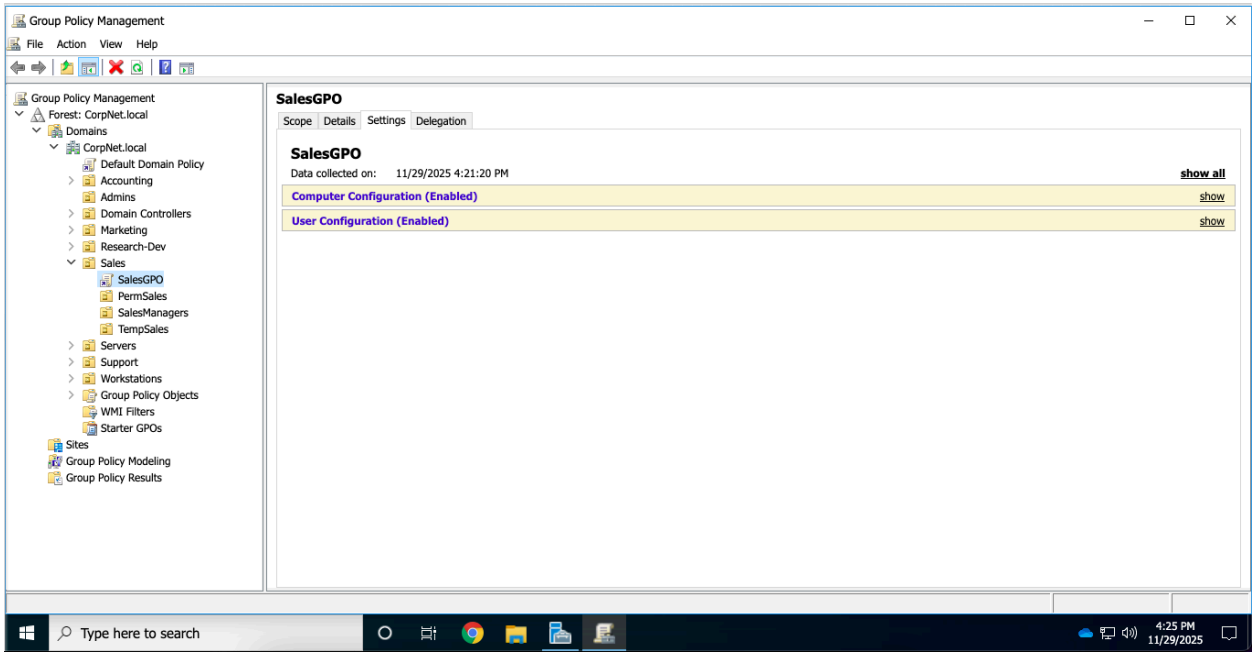
Why It Matters:Least privilege minimizes attack surface and reduces data exposure.



Step 4 — Validate Access

Actions Performed:- Logged in as the provisioned user (or used TestOut verifier).- Confirmed that authentication and access behaved as expected.

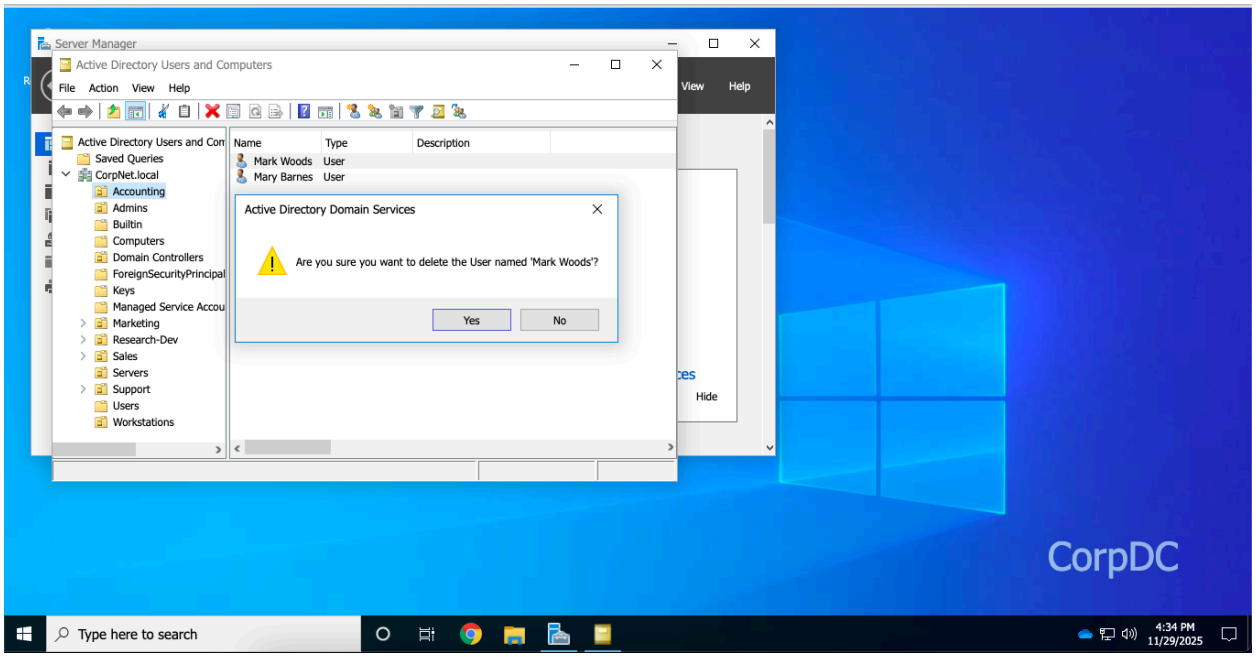
Why It Matters:Validating ensures provisioning was successful and compliant.



Step 5 — Disable User Account (Offboarding)

Actions Performed:- Located and disabled the user account.- Verified the account displayed as 'Disabled.'- (Optional) Removed unnecessary group memberships.

Why It Matters:Proper offboarding prevents unauthorized access from orphaned accounts.



IAM Concepts Demonstrated

• Identity Lifecycle Management: onboarding, modification, offboarding.• Role-Based Access Control (RBAC): consistent access assignment.• Least Privilege: minimized permissions.• Auditability: all actions traceable and documentable.

Final Summary

This demonstration shows my ability to manage user identities in AD, apply least privilege principles, validate permissions, and securely offboard accounts.