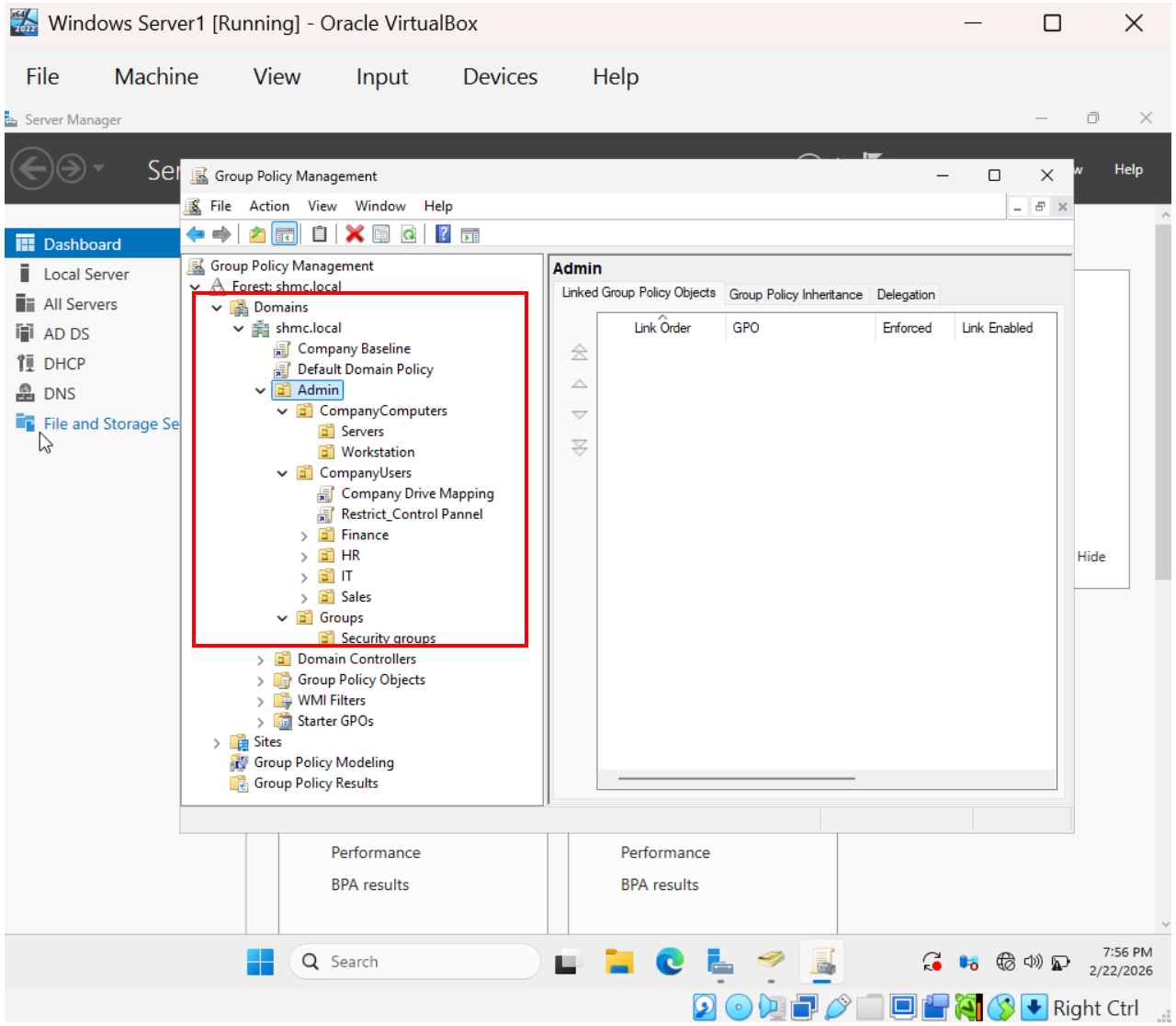
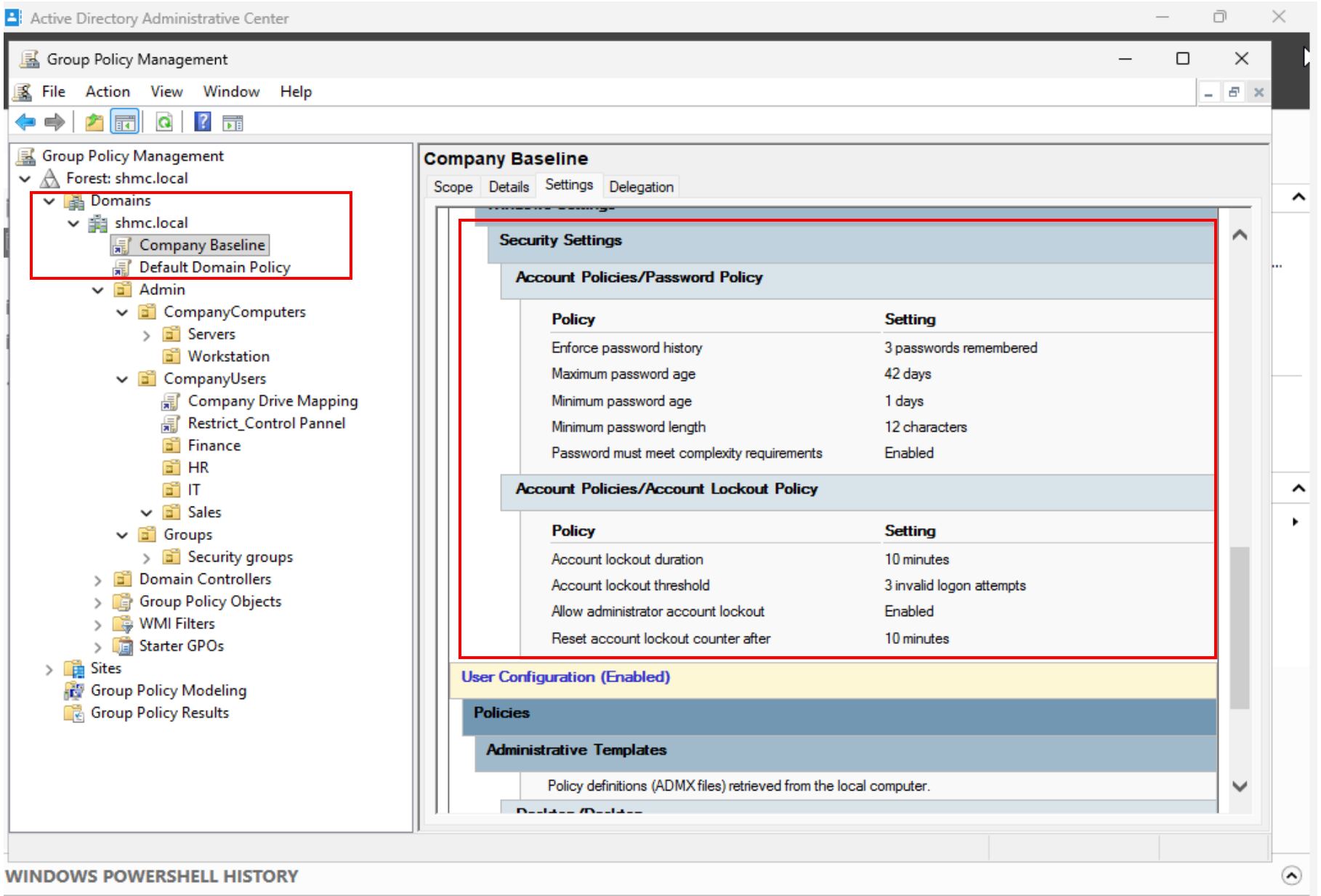
# Windows  Environment Design & Core Services

Built a functional enterprise-style Active Directory lab environment including organizational units (OUs), users, security groups, and Group Policy Objects (GPOs). Configured foundational network services such as DHCP and DNS to simulate real-world domain operations and centralized management.

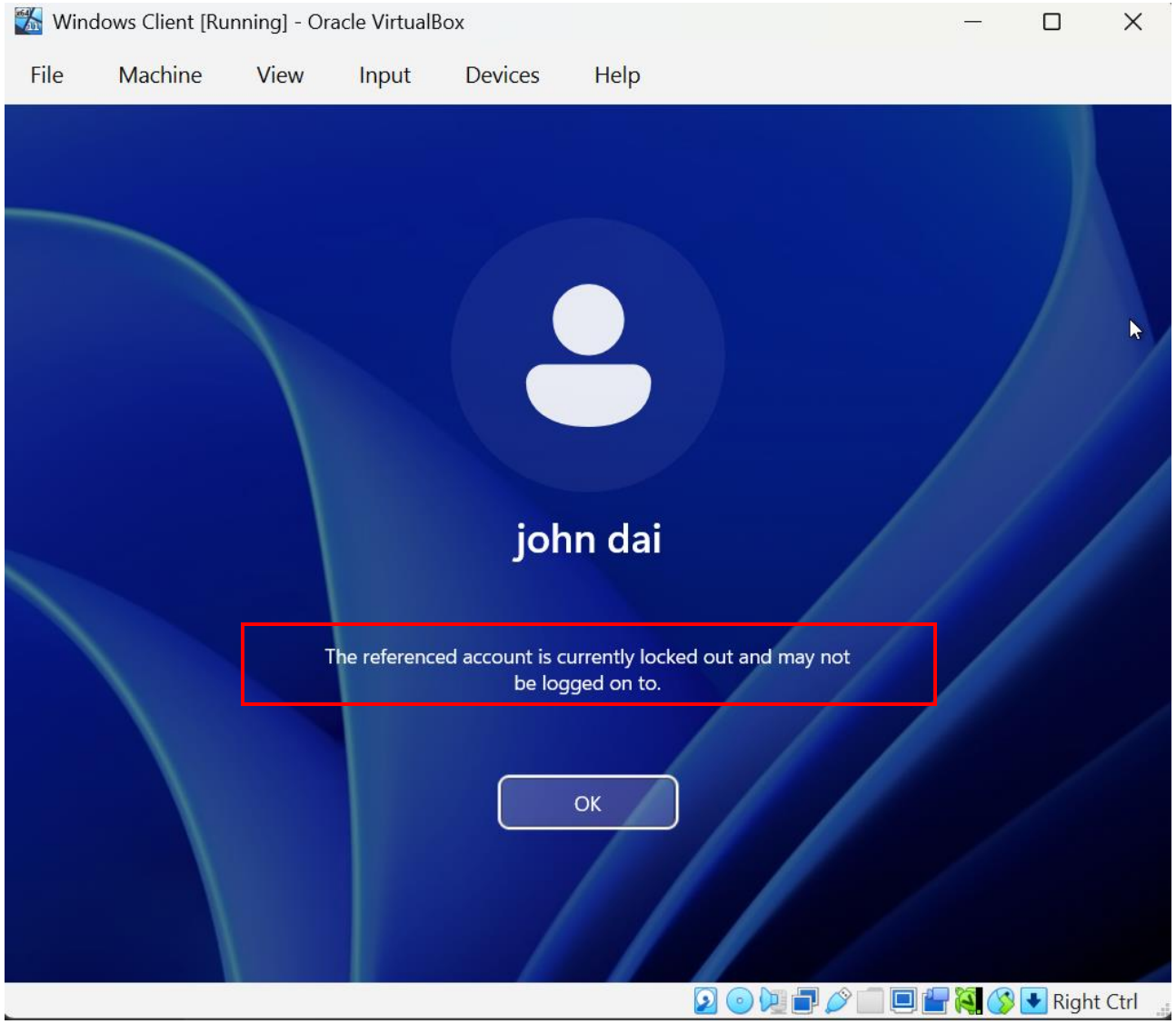
Designed and managed Group Policy Objects (GPOs) within a structured OU framework to support role-based administration and departmental policy control. Demonstrated policy scoping, inheritance planning, and security segmentation for users and computers in a domain environment.



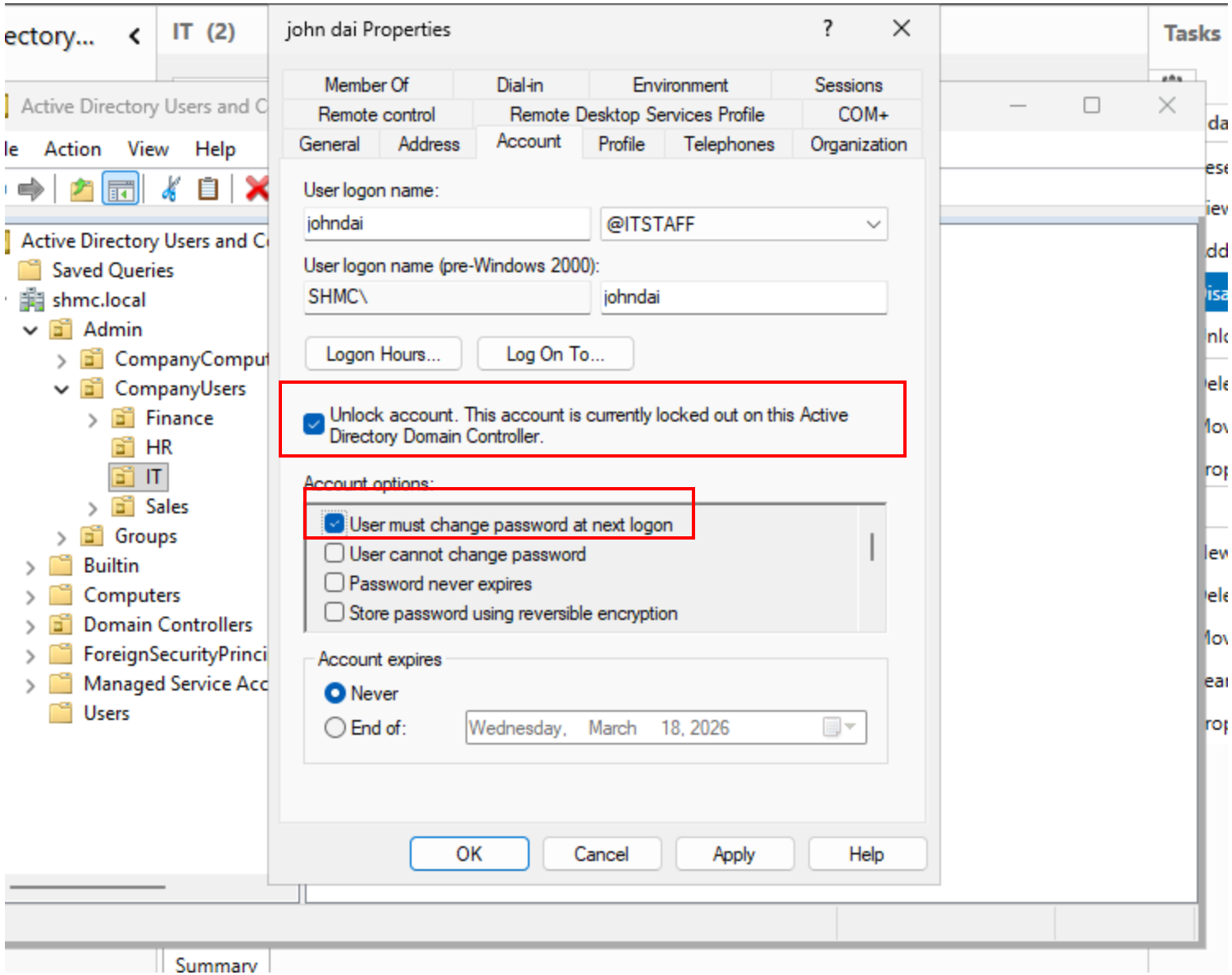
Configured Account Lockout Policy to protect against brute-force authentication attempts.



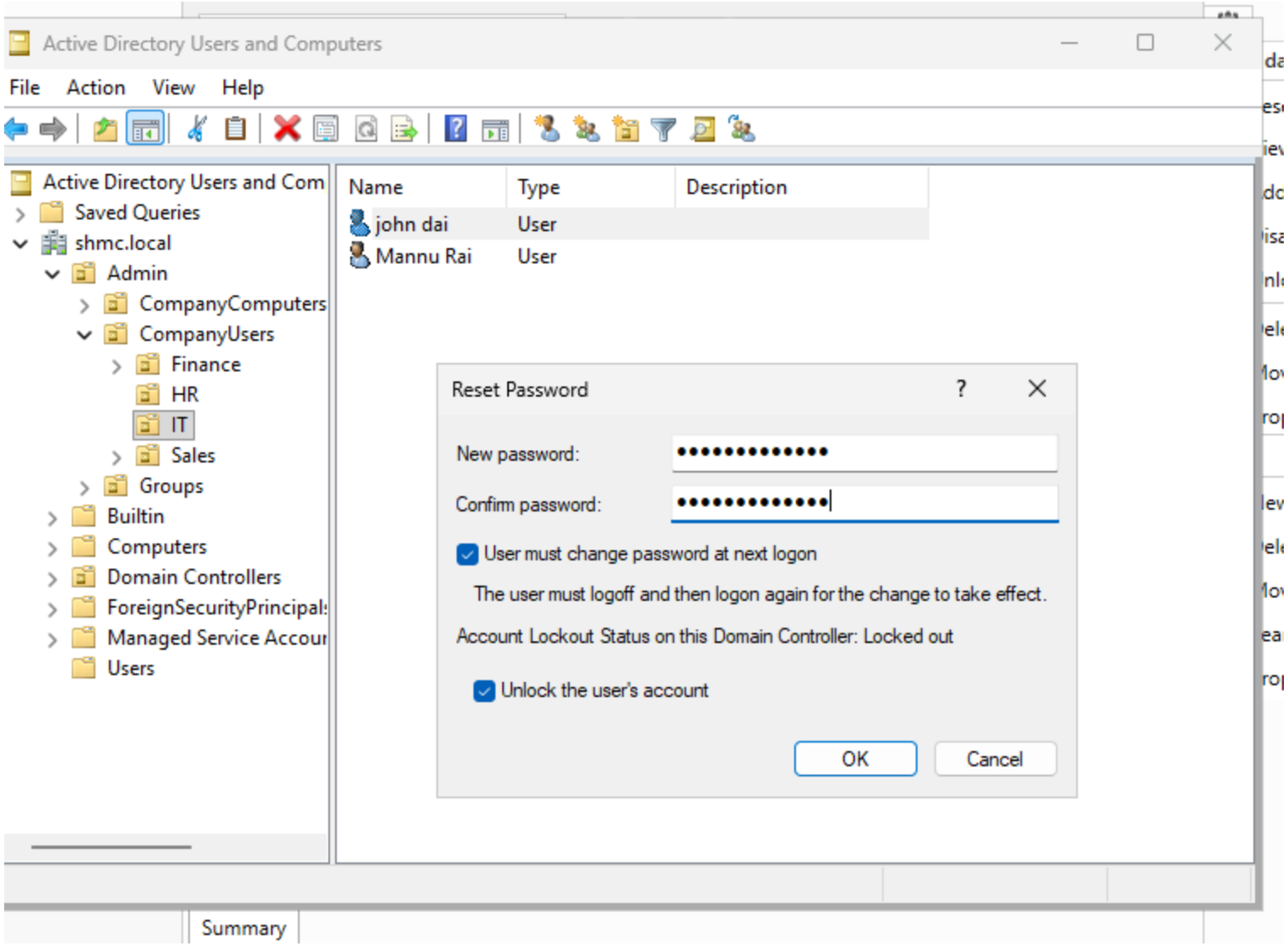
Demonstrated workings of the Account lockout GPO where a User Account has been disabled as a result of invalid password attempts.



User reports to IT about the issue, IT unlocks the account and enforces password change at next logon.

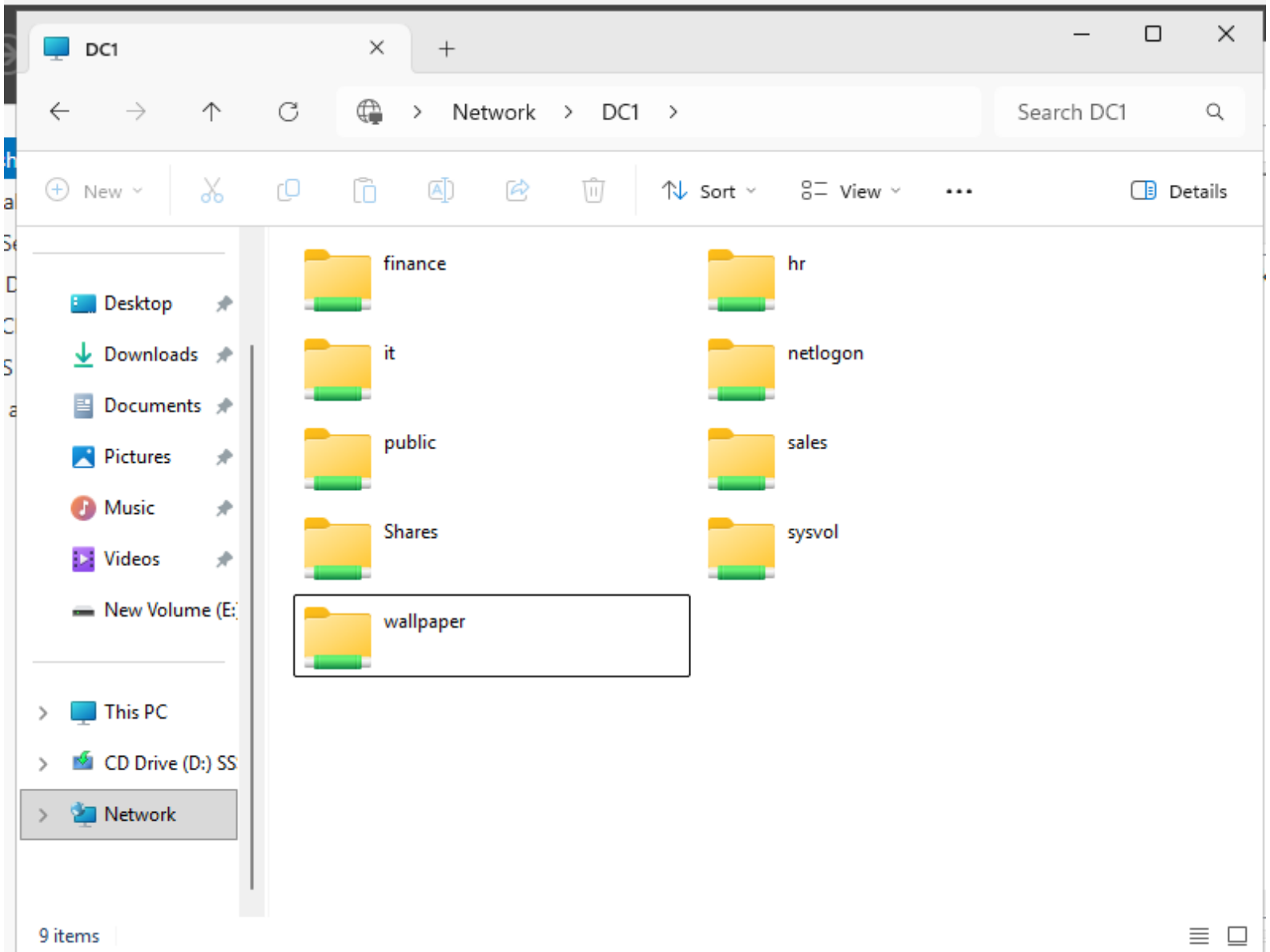


Demonstrating a password reset situation.

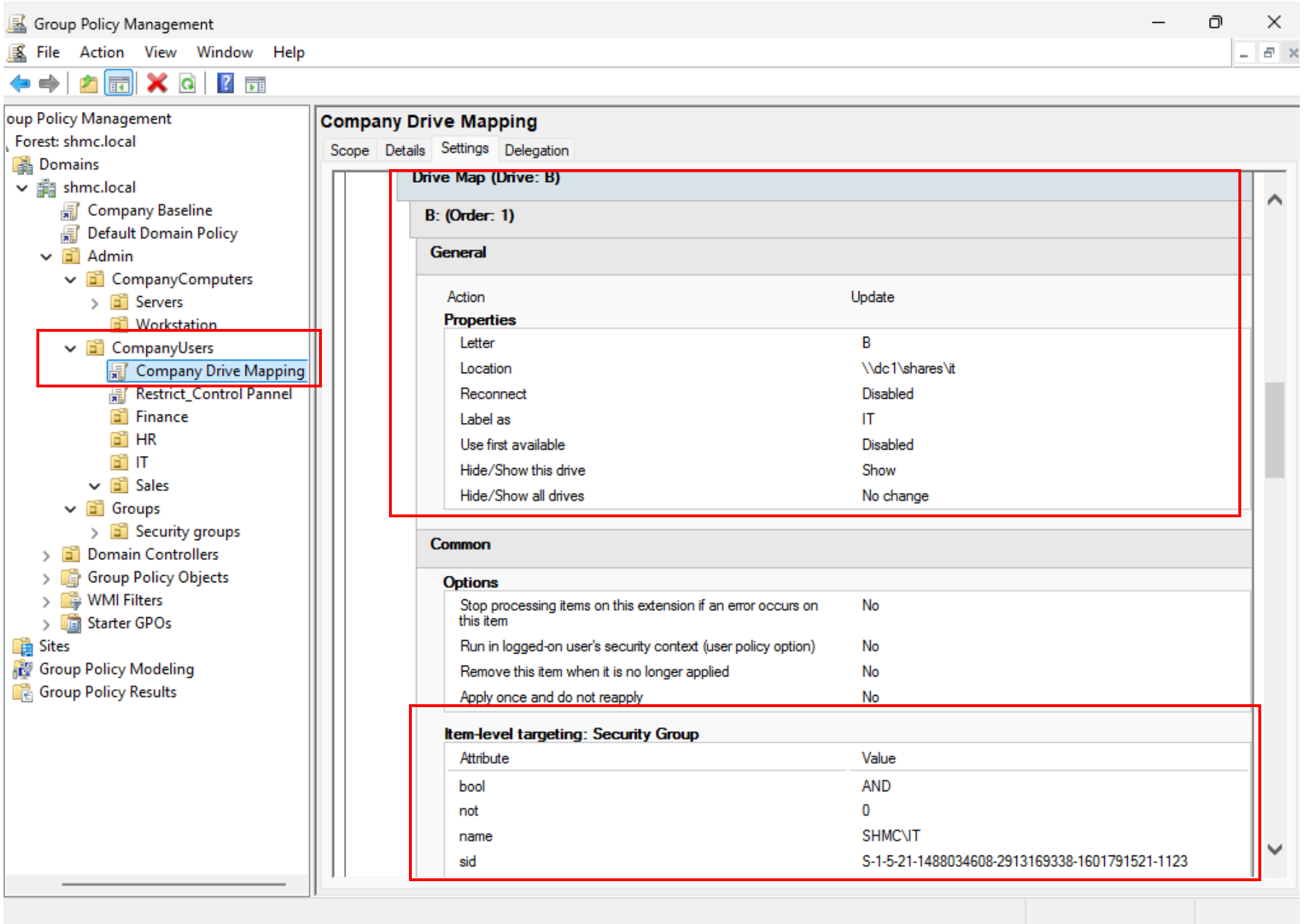


# Network Shares and Drive mappings

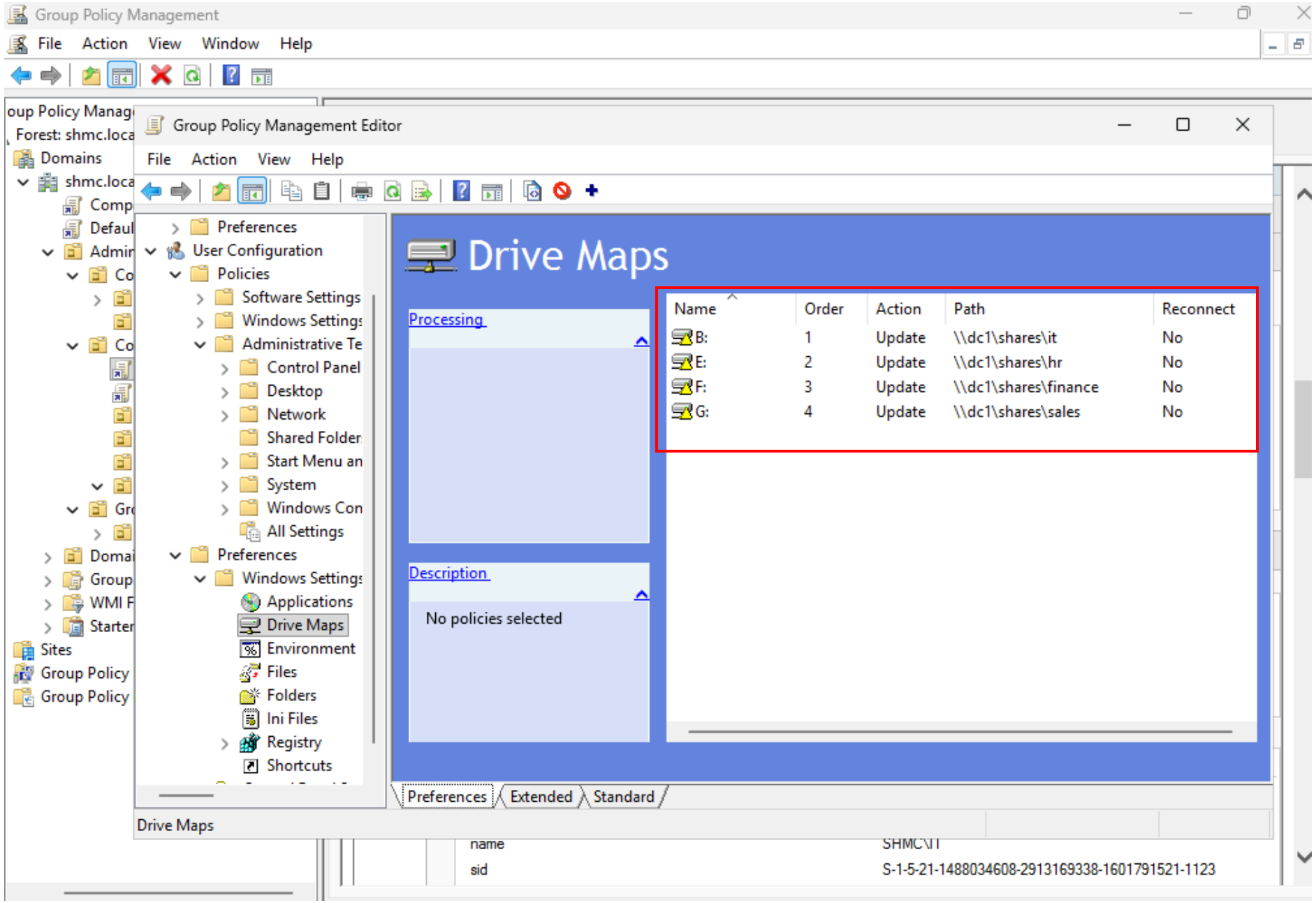
- Created a Centralized File Server (DC1 In this Lab) and shared Folders over the network.
- Created a GPO that maps Drive letter for each department to the appropriate Network shares.



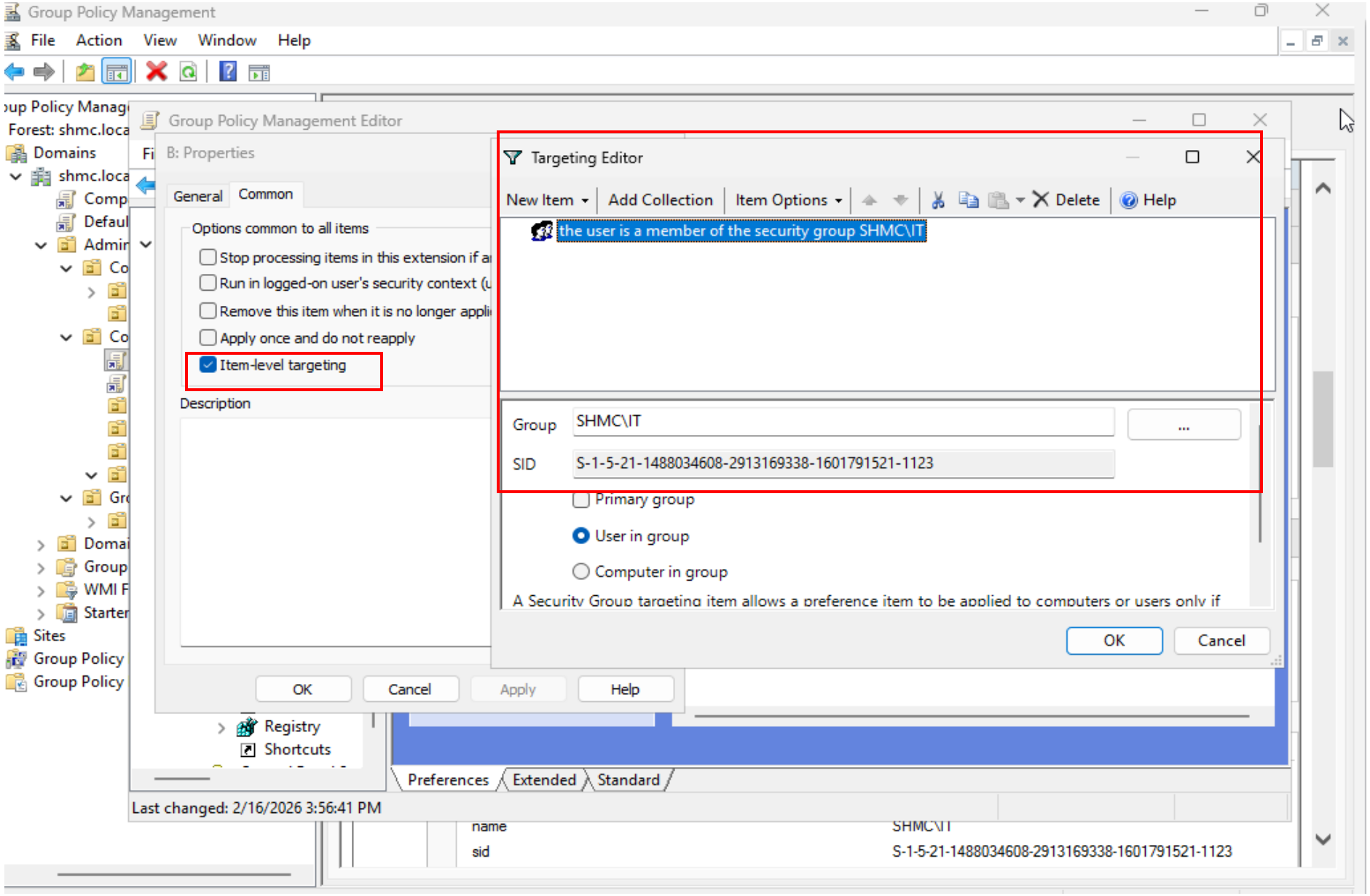
# Drive Mapping GPO linked to Company Users OU



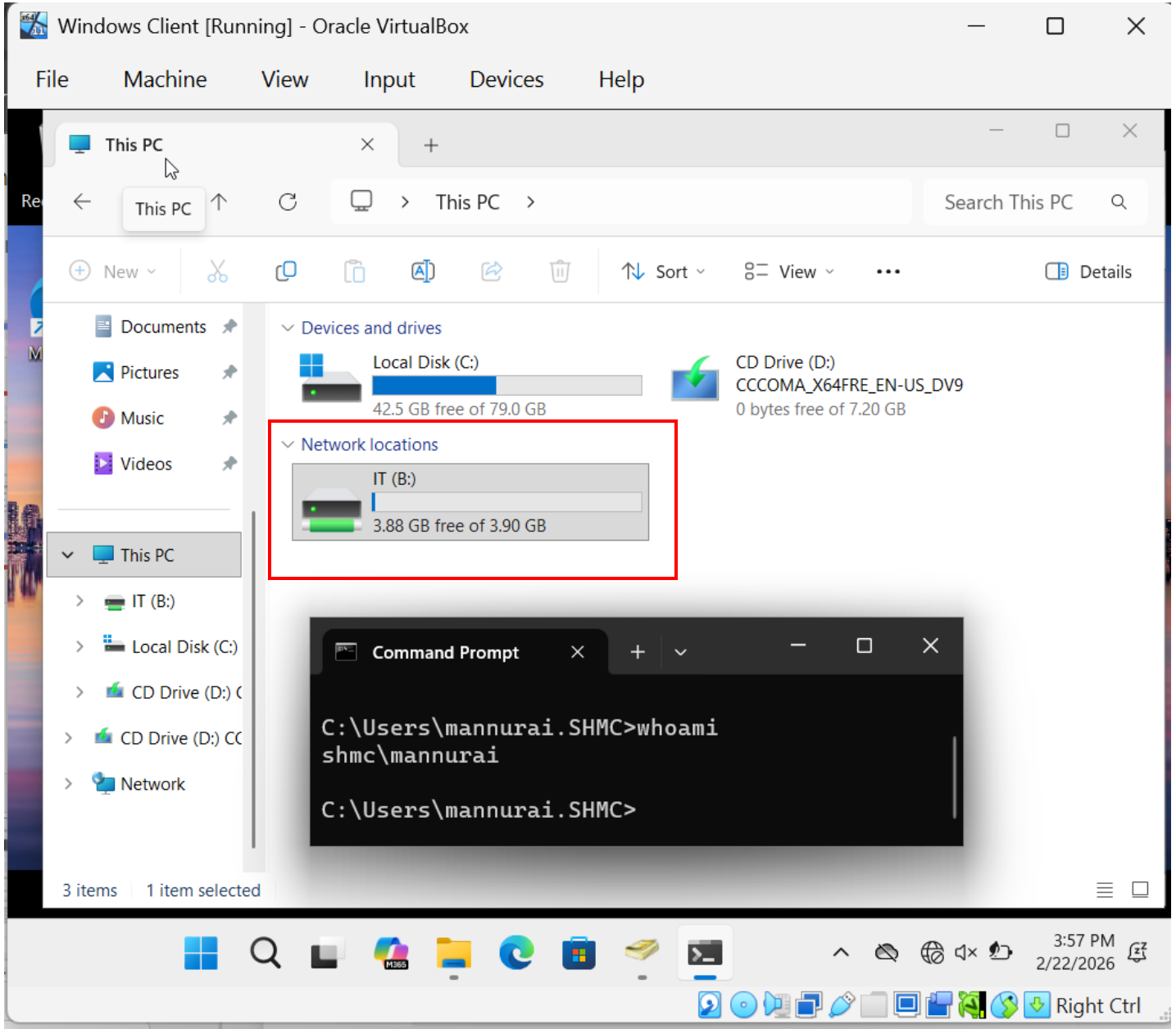
Created a GPO with Drive mappings, Assigned appropriate drive letter for each Department.



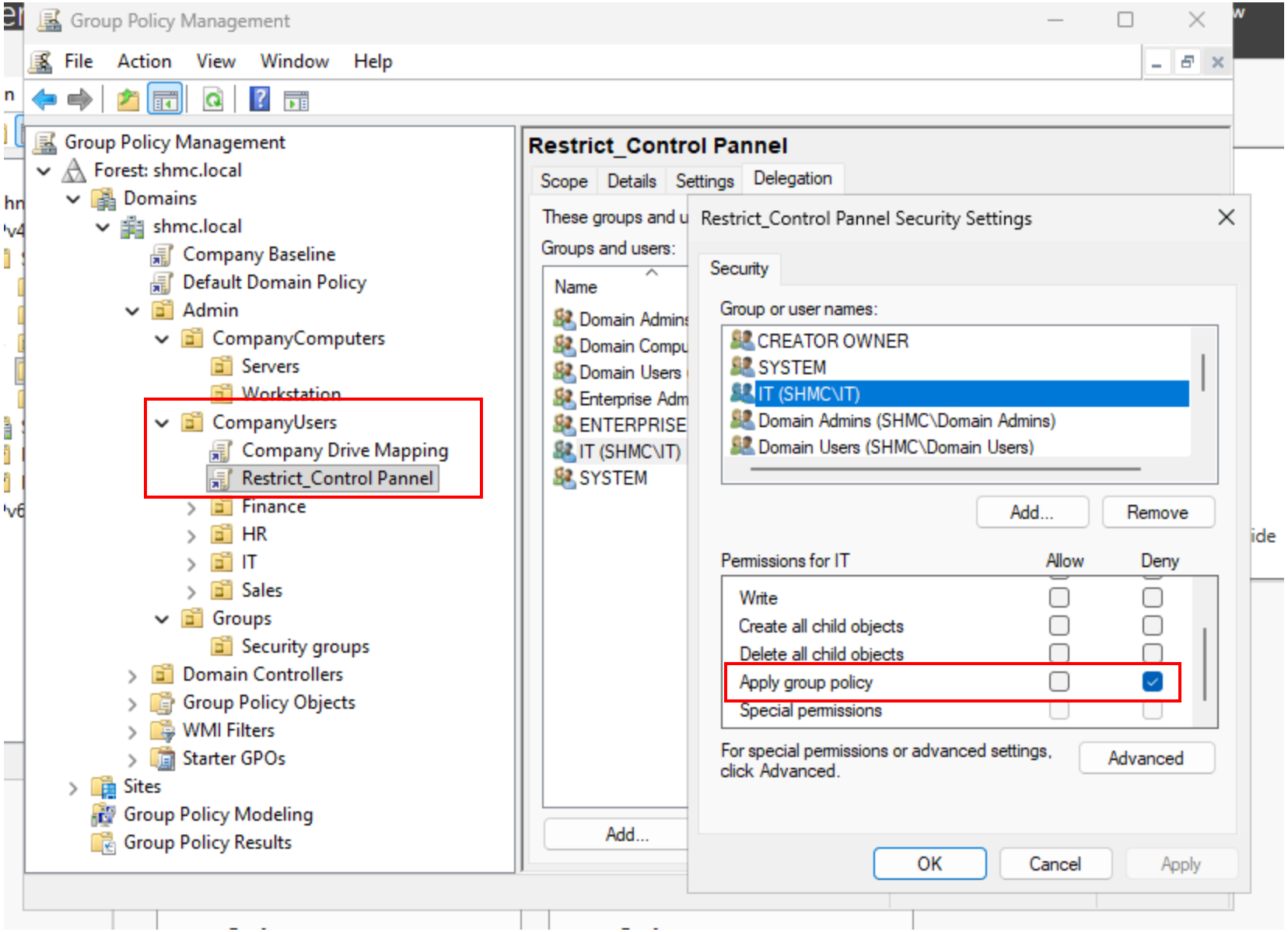
Item level Targetting for each drive maps, ensuring users from different departments are directed towards their appropriate share.



IT user logs in and finds the share using a friendly drive letter.



Created a GPO that restrict company users from accessing Control pannel and Sensitive computer setting, Excluded IT security group for controll and basic troubleshooting.

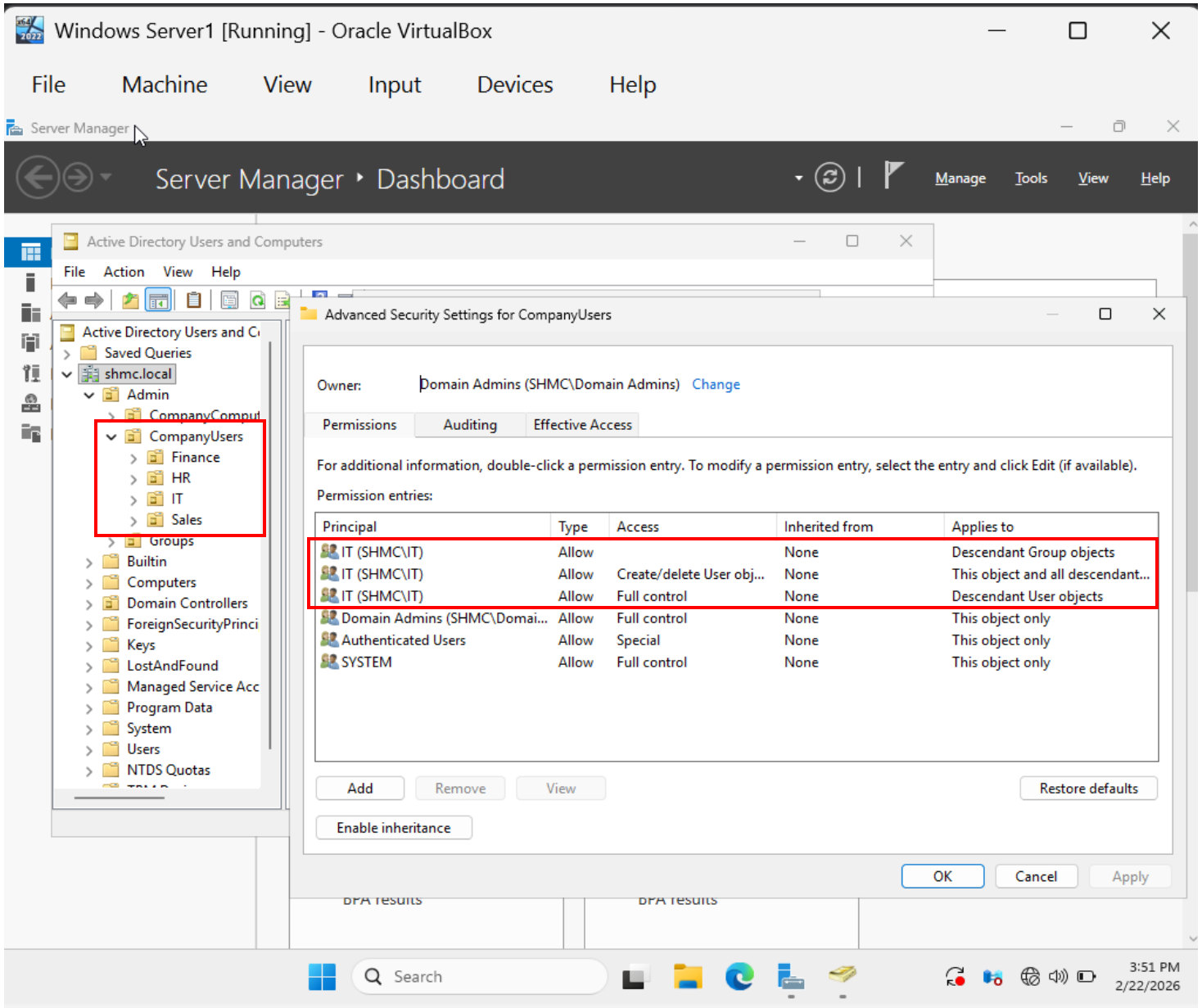


# Delegation of Control

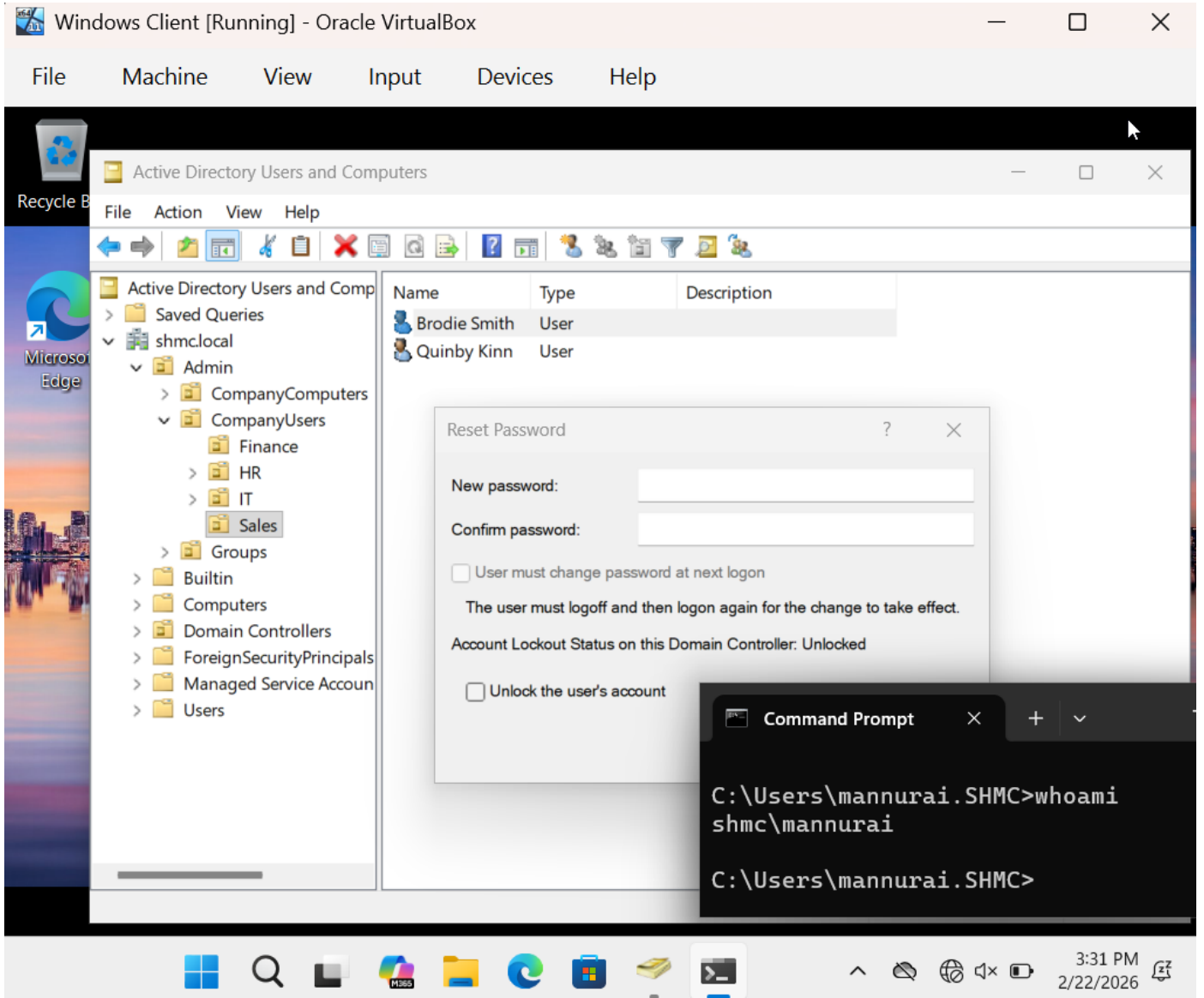
- Delegated appropriate permissions to the IT Security group over the *Company Users* OU to support routine help desk operations. Allowed tasks include user account creation/deletion, password resets, account unlock/disable actions, and group membership management. This delegation model follows least-privilege principles and reflects typical Tier 1 / help desk responsibilities in an enterprise domain environment.

- Configured least-privilege delegation for the IT Security group to perform standard help desk functions, including managing user accounts, resetting passwords, unlocking/ disabling accounts, and modifying group memberships.

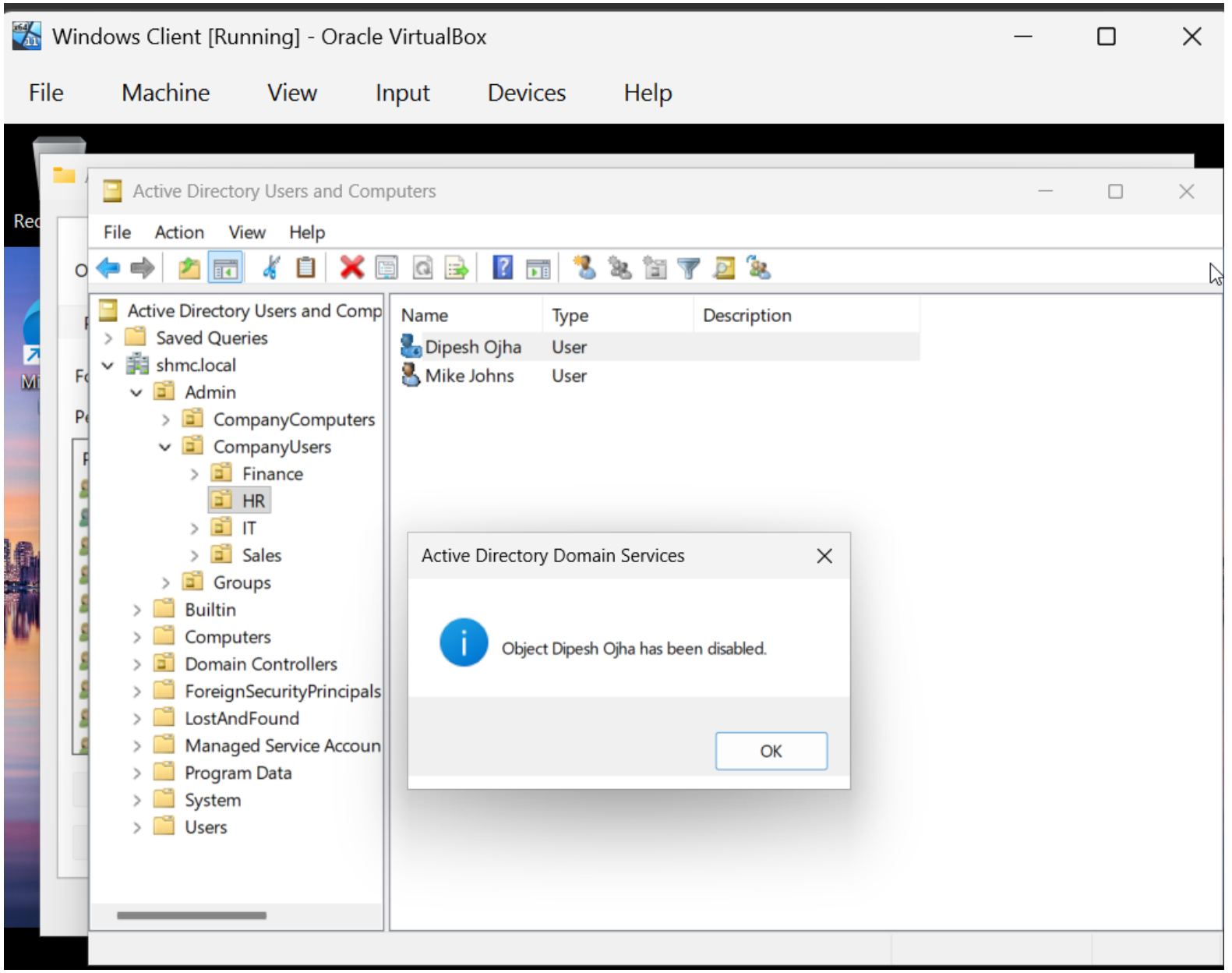
Delegating IT Security group basic management controller over Company Users OU, Any users that have issues with password, account, group membership can report to IT team member for a resolution.



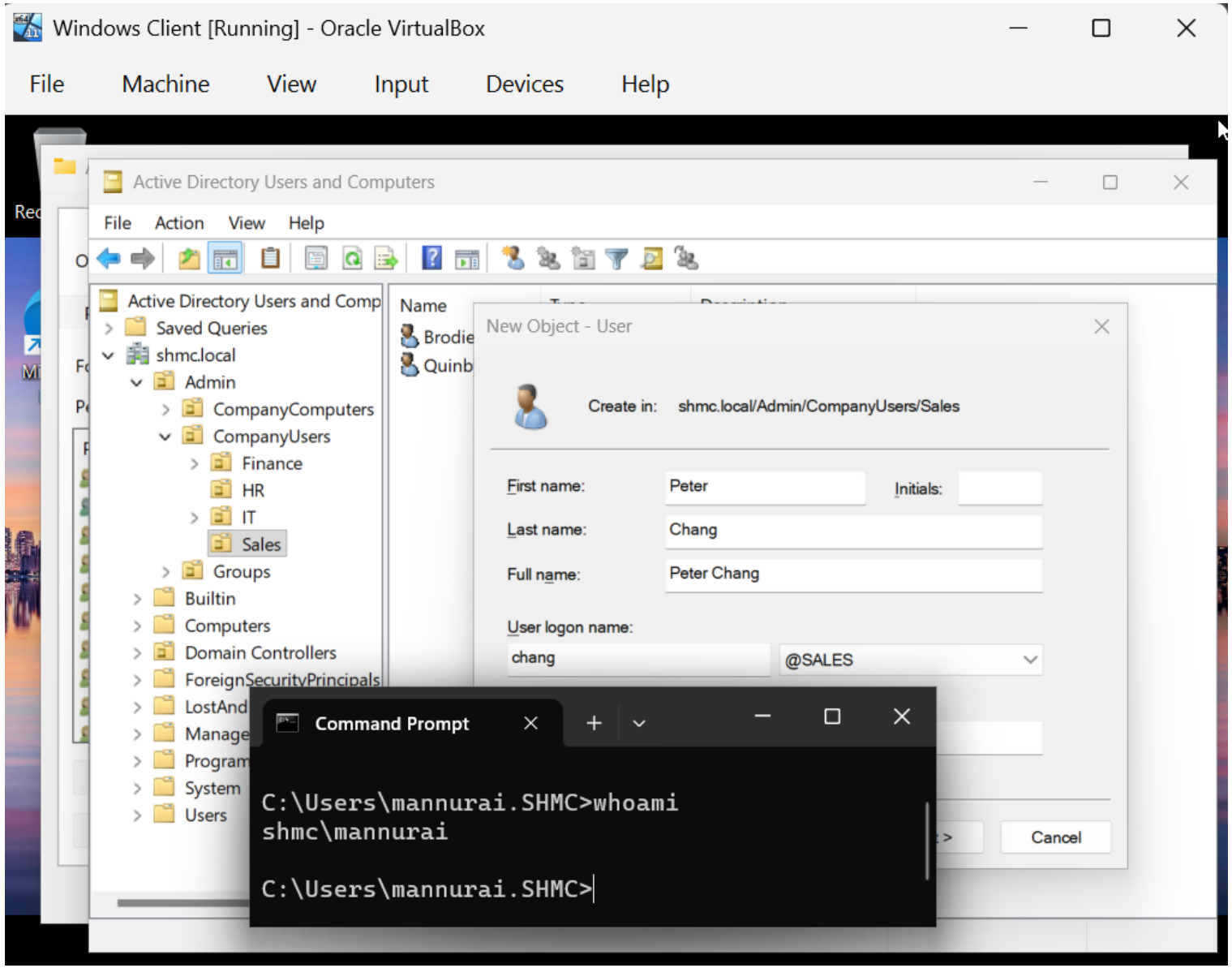
Administrating Active directory Users and Computers from member of IT security group, Mannurai a member of IT Security Group can solve issues related to users and groups using RSAT on the Client machine.



Demonstrating basic functions from IT Security group users using RSAT.



Creating a User from mannurai which belongs to IT security group.



Basic DHCP Configuration with different options such as Default gateway, DNS server and domain name.