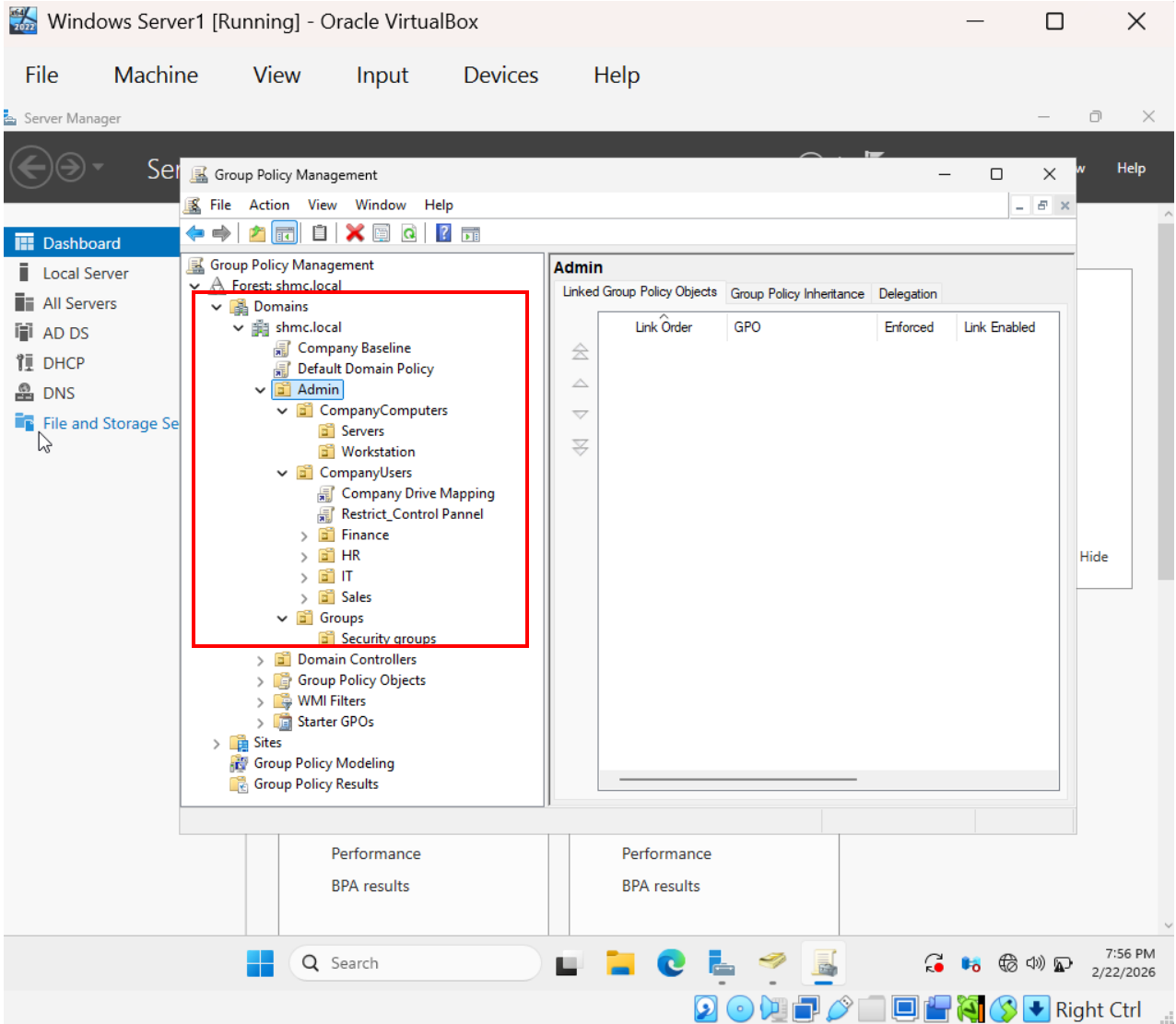


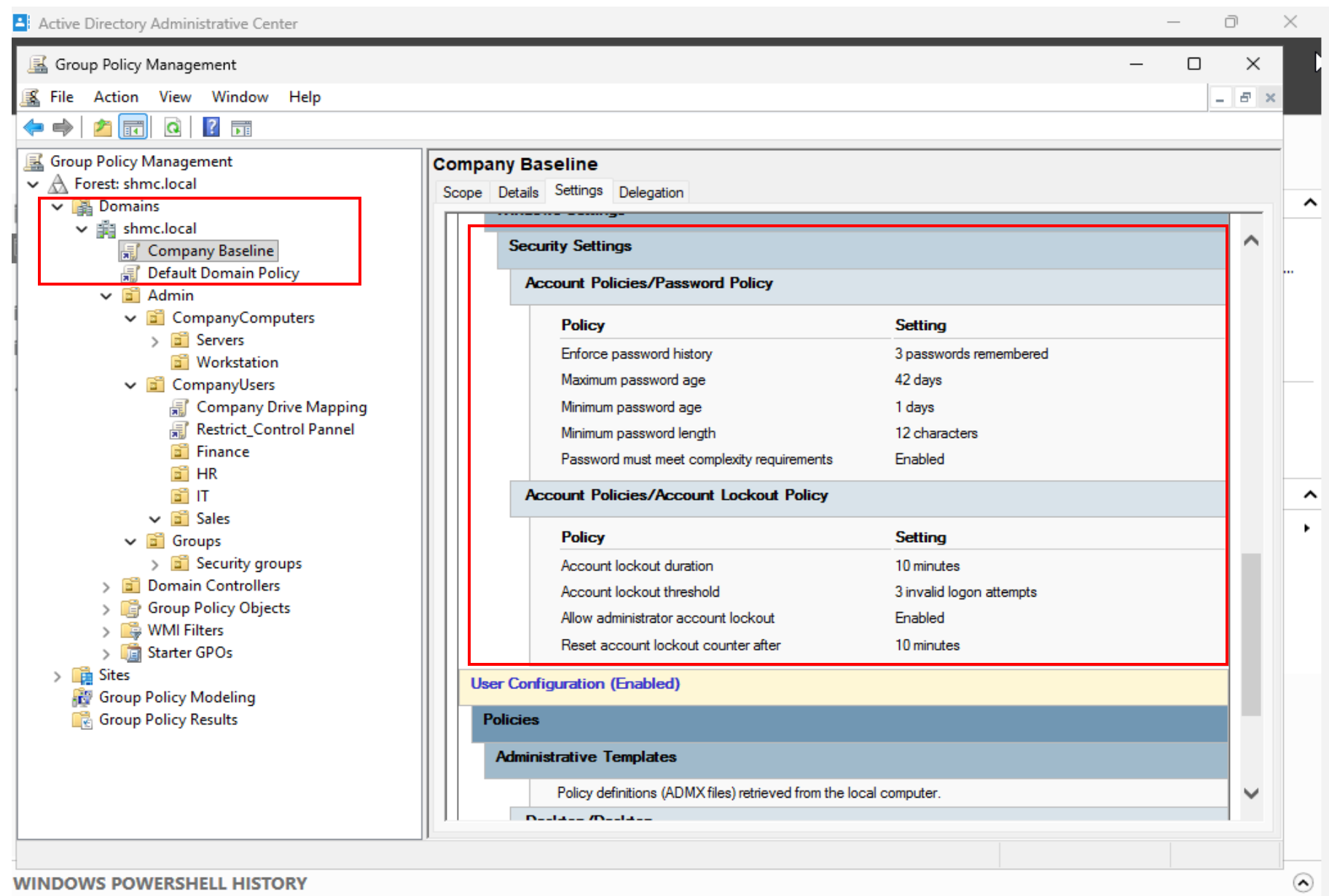
Windows Environment Design & Core Services

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.

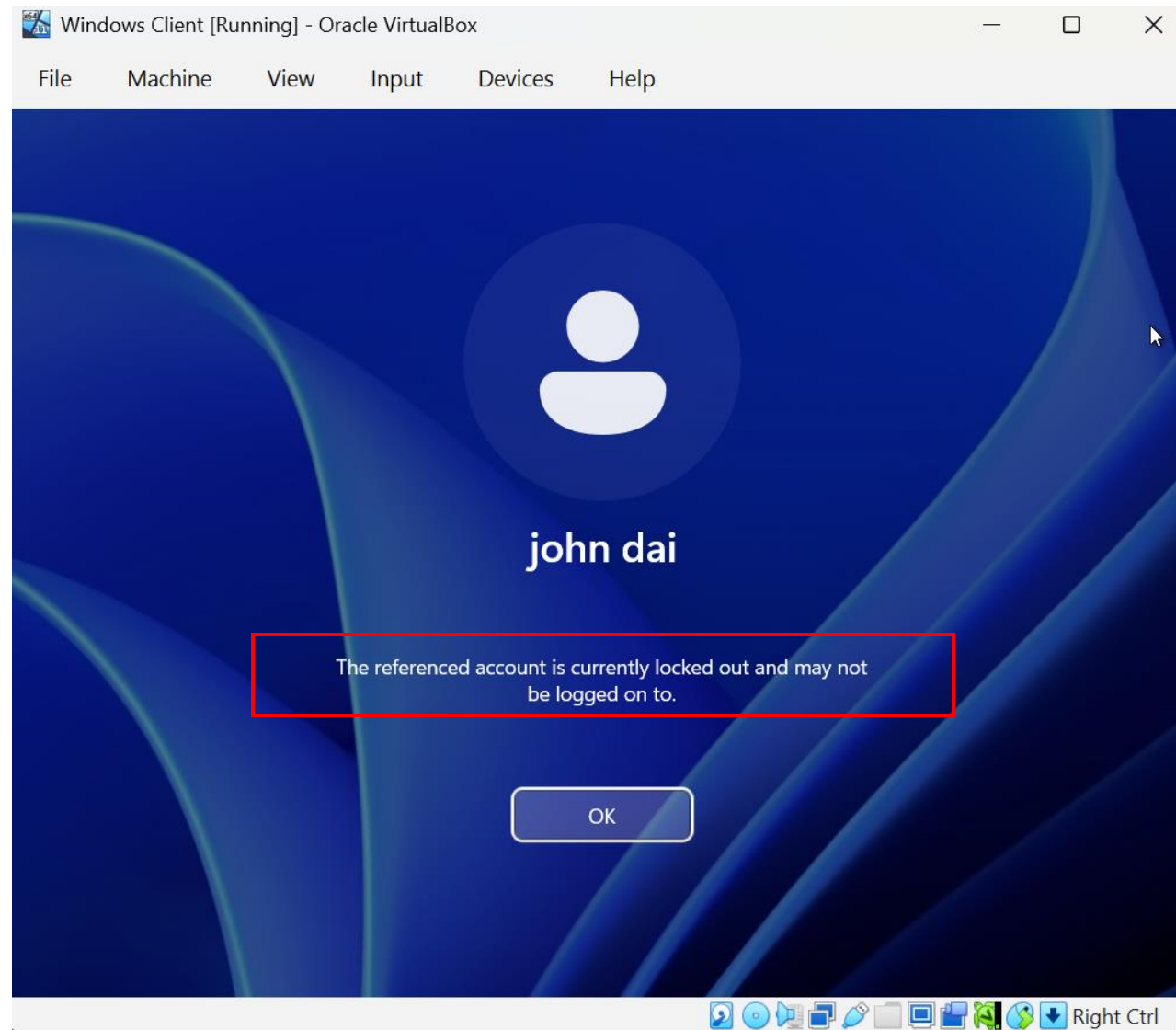
Designed and managed Group Policy Objects (GPOs) within a structured OU framework to support role-based administration and departmental policy control. Demonstrated policy scoping, inheritance planning, and security segmentation for users and computers in a domain environment.



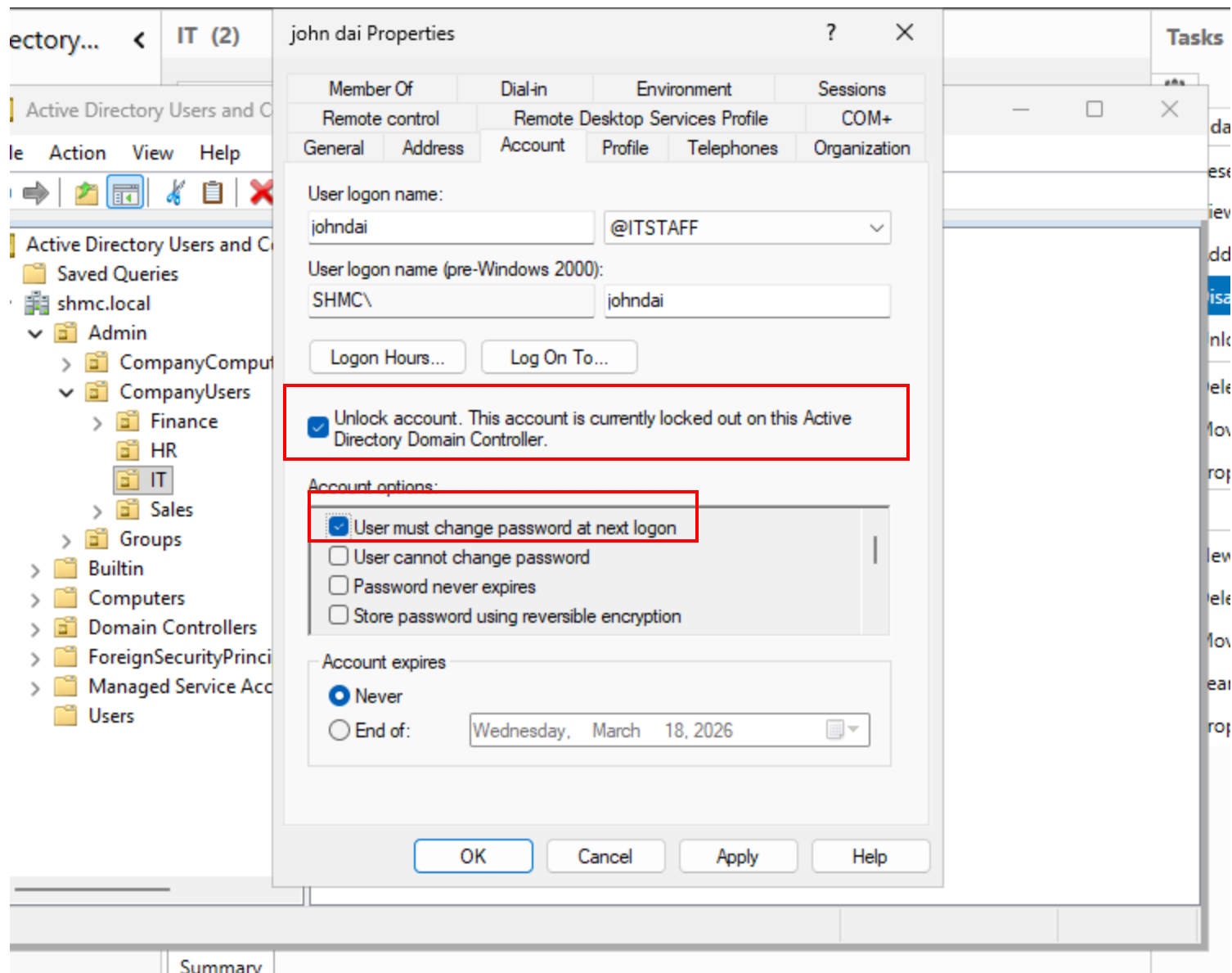
Configured Account Lockout Policy to protect against brute-force authentication attempts.



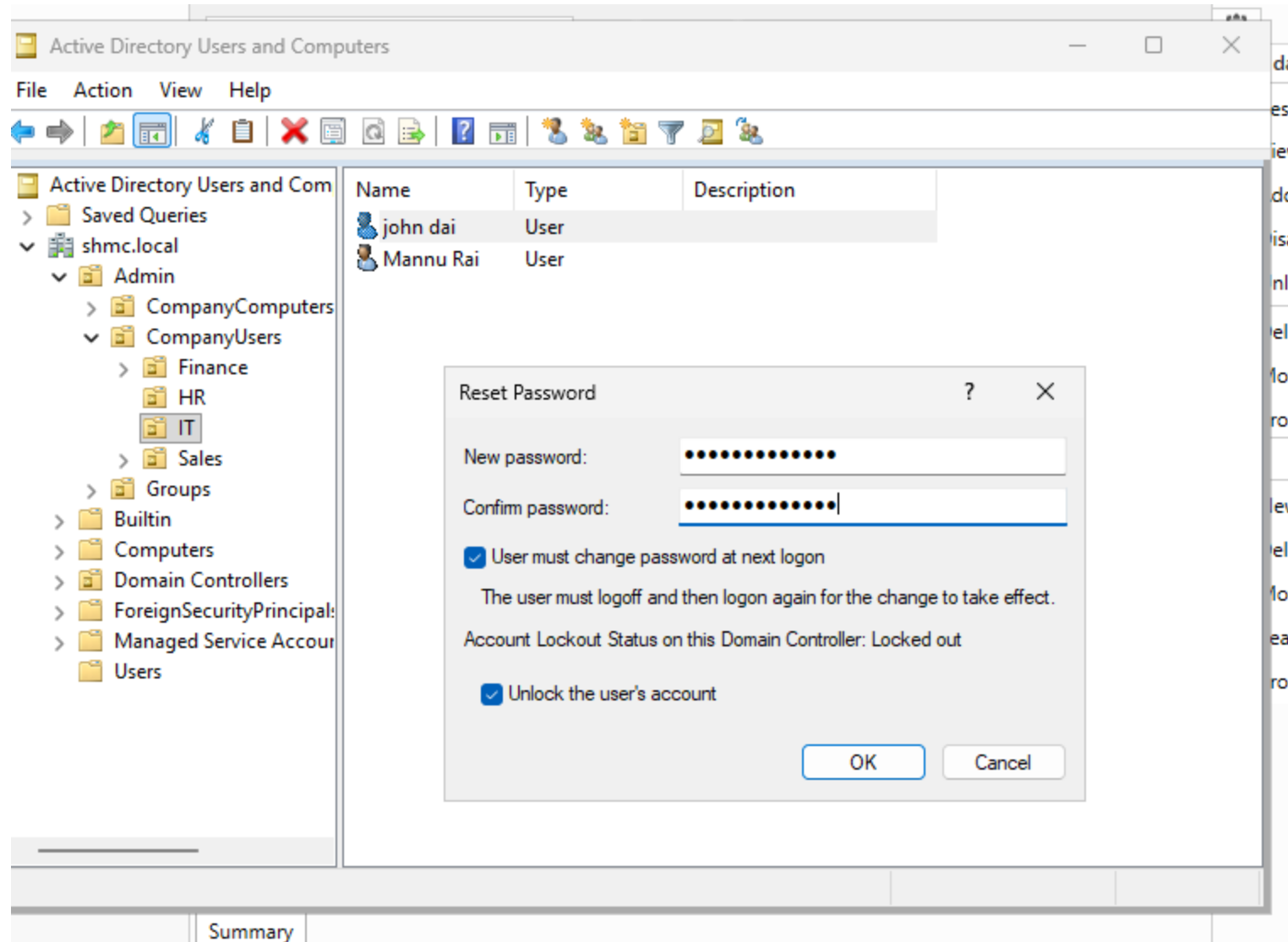
Demonstrated workings of the Account lockout GPO where a User Account has been disabled as a result of invalid password attempts.



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

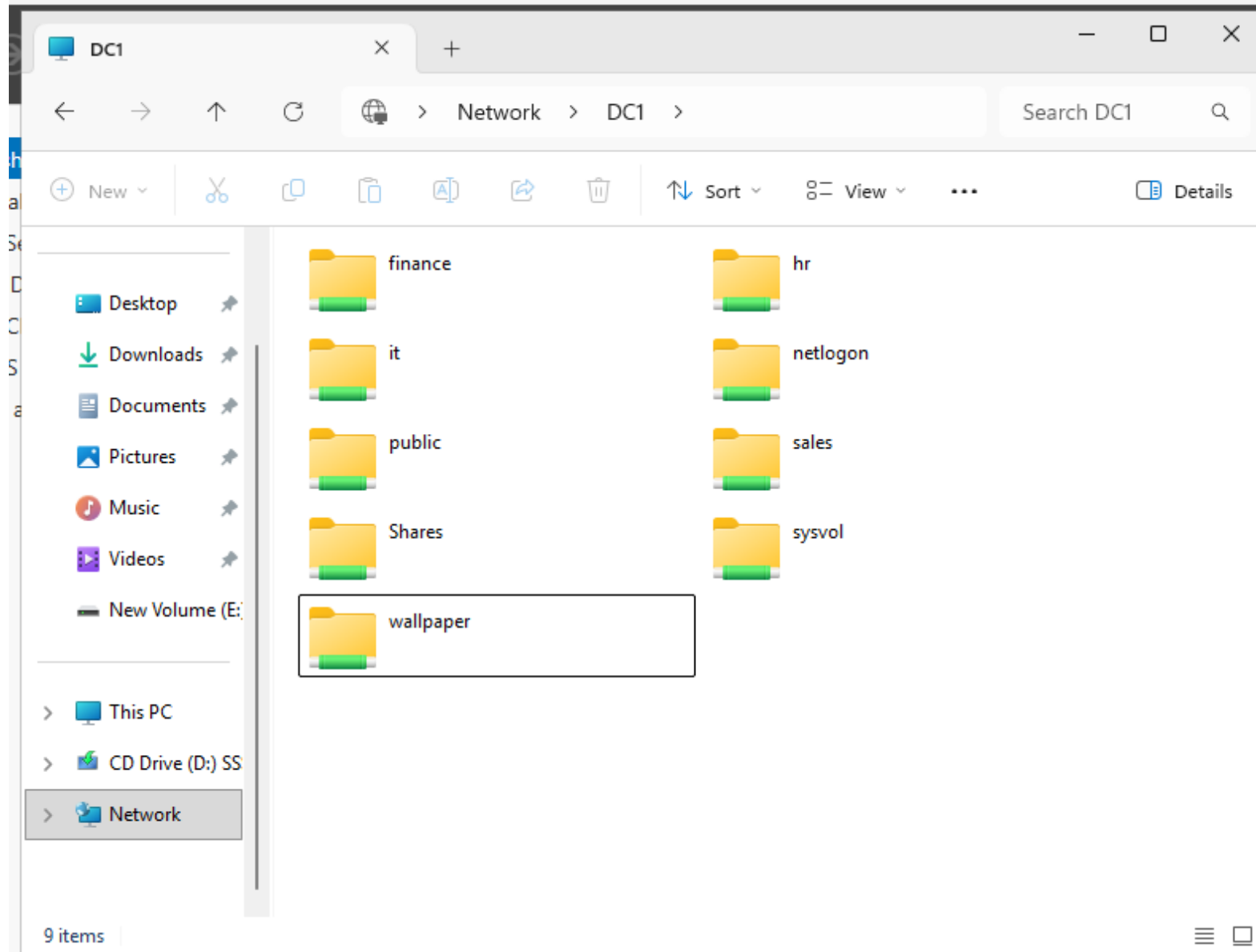


Demonstrating a password reset situation.



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

The screenshot displays the Group Policy Management console. In the left-hand tree, the hierarchy is: Forest: shmc.local > Domains > shmc.local > Admin > CompanyComputers > Workstation > CompanyUsers. The 'Company Drive Mapping' GPO is selected under the CompanyUsers OU.

The main pane shows the configuration for 'Company Drive Mapping' with tabs for Scope, Details, Settings, and Delegation. The 'Details' tab is active, showing the 'Drive Map (Drive: B)' configuration.

Drive Map (Drive: B)

B: (Order: 1)

General

Action	Update
Letter	B
Location	\\dc1\shares\it
Reconnect	Disabled
Label as	IT
Use first available	Disabled
Hide/Show this drive	Show
Hide/Show all drives	No change

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Item-level targeting: Security Group

Attribute	Value
bool	AND
not	0
name	SHMC\IT
sid	S-1-5-21-1488034608-2913169338-1601791521-1123

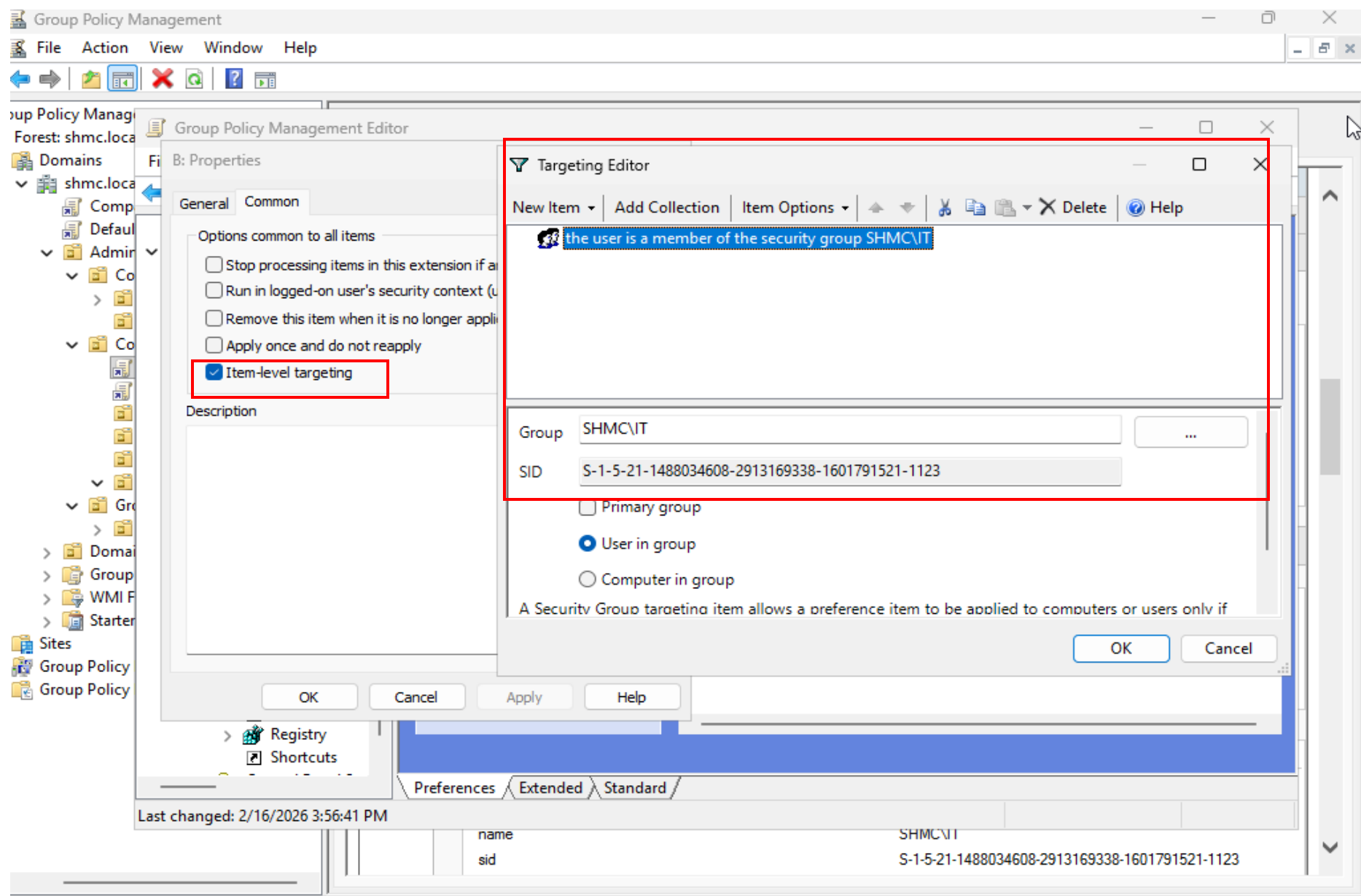
Created a GPO with Drive mappings, Assigned appropriate drive letter for each Department.

The screenshot displays the Group Policy Management Editor window. The left-hand navigation pane shows the hierarchy: Group Policy Management > Forest: shmc.local > Domains > shmc.local > Administrative Templates > Control Panel > Desktop > Network > Shared Folders > Start Menu and Taskbar > System > Windows Components > All Settings > Preferences > Windows Settings > Drive Maps. The main pane is titled 'Drive Maps' and contains a table with the following data:

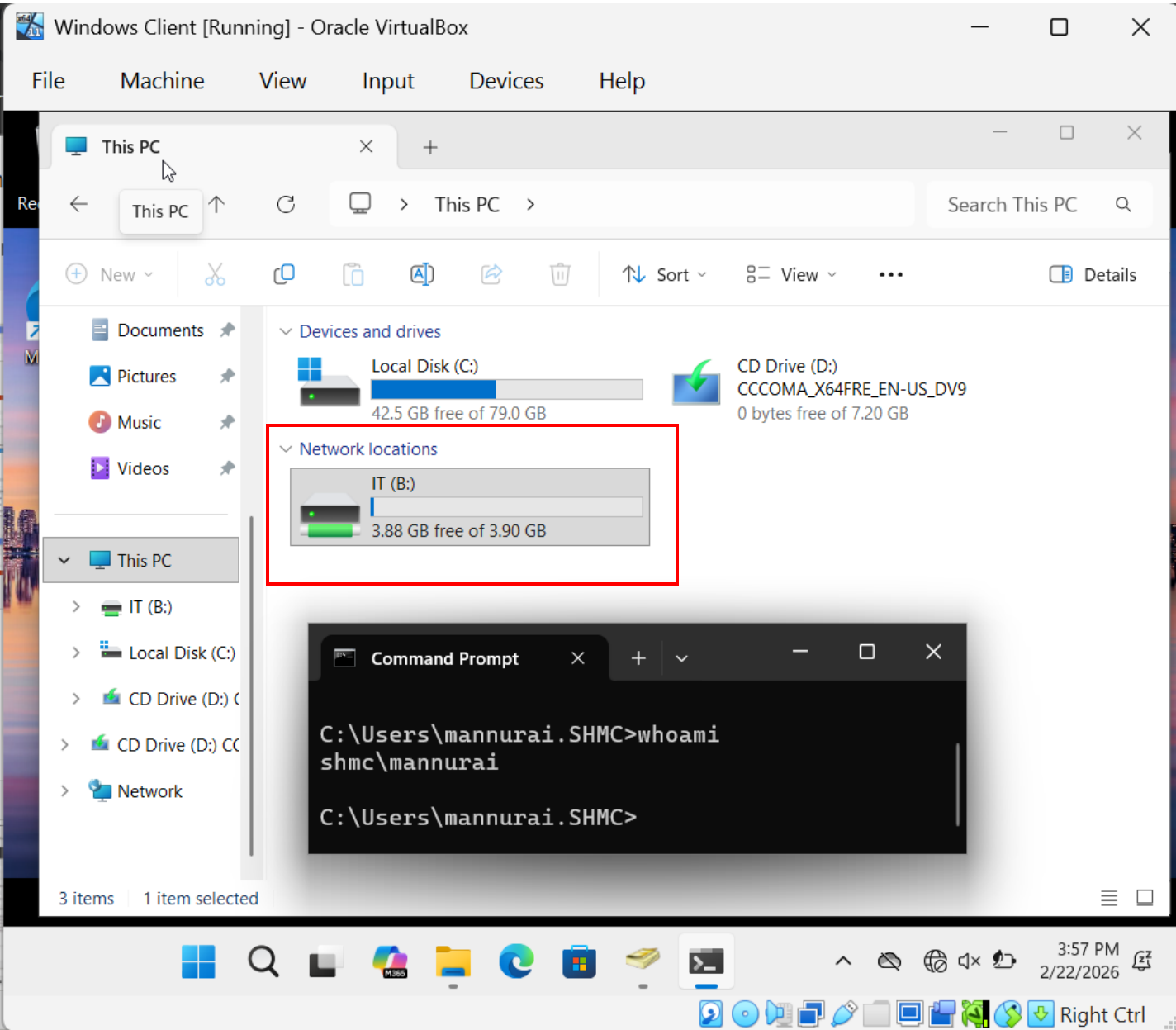
Name	Order	Action	Path	Reconnect
B:	1	Update	\\dc1\shares\it	No
E:	2	Update	\\dc1\shares\hr	No
F:	3	Update	\\dc1\shares\finance	No
G:	4	Update	\\dc1\shares\sales	No

Below the table, there is a 'Description' section with the text 'No policies selected'. At the bottom of the window, the 'Drive Maps' tab is selected, and the 'name' and 'sid' fields are visible, showing the name 'SHMCVT' and the SID 'S-1-5-21-1488034608-2913169338-1601791521-1123'.

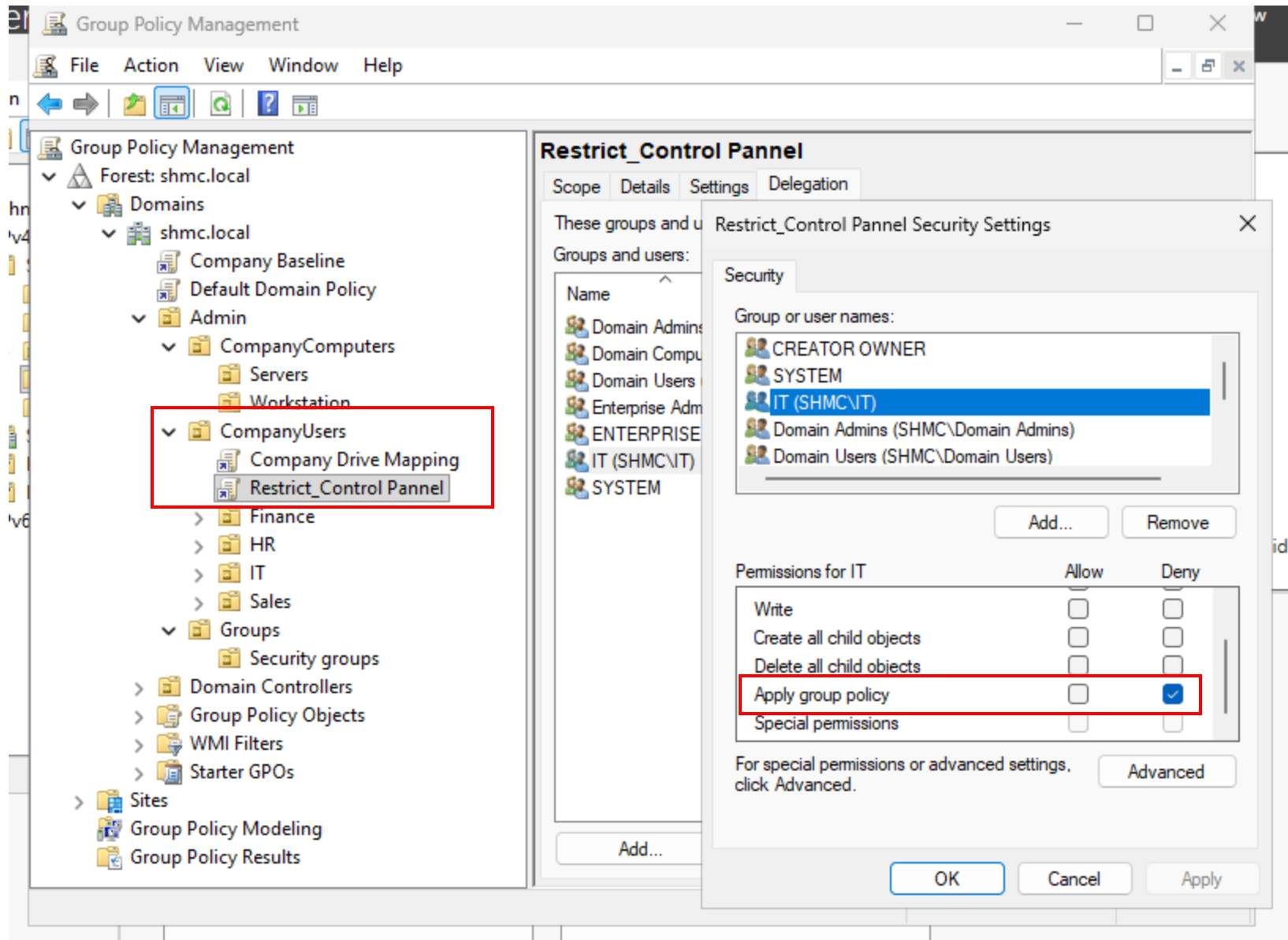
Item level Targetting for each drive maps, ensuring users from different departments are directed towards their appropriate share.



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



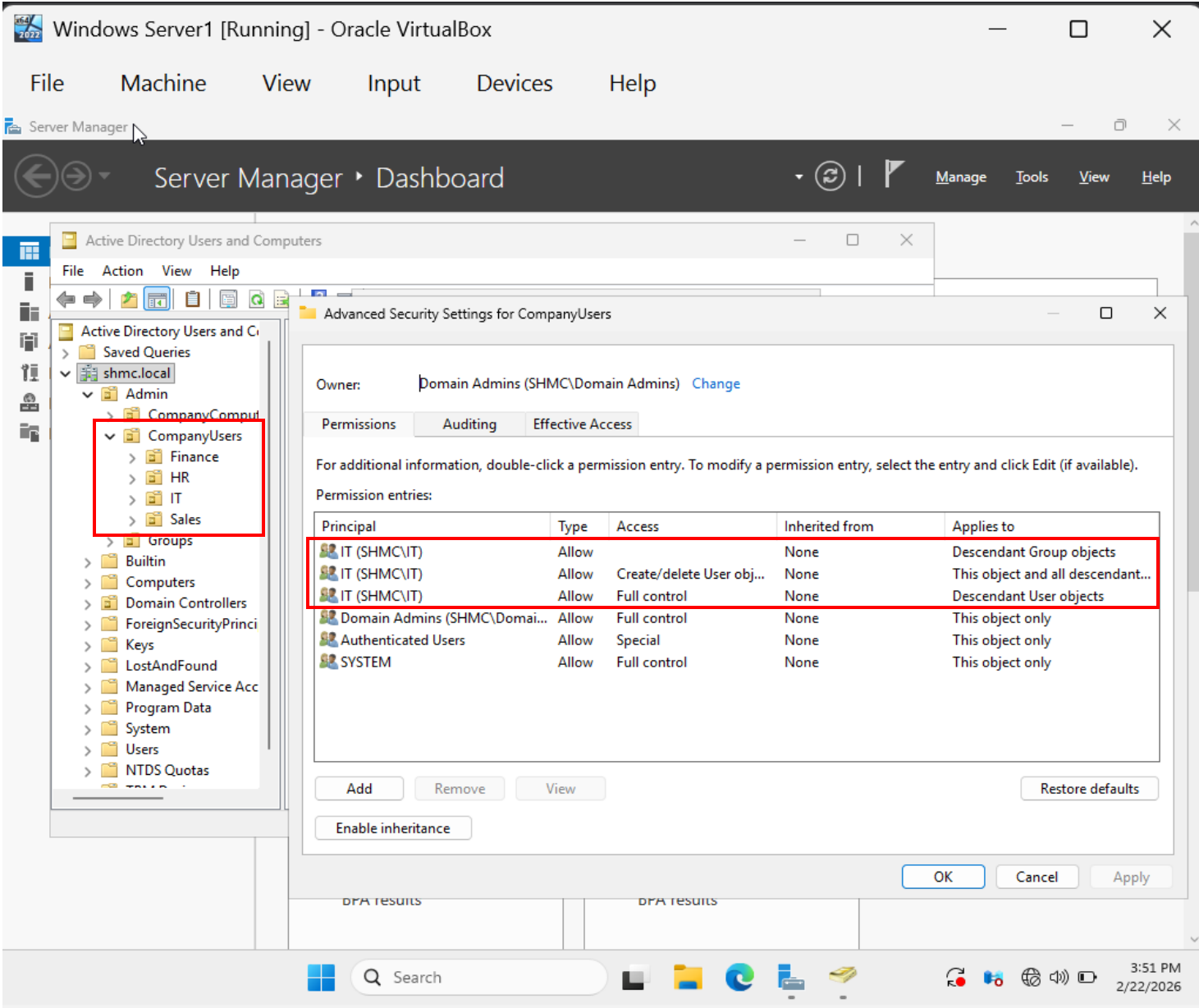
Created a GPO that restrict company users from accessing Control panel and Sensitive computer setting, Excluded IT security group for control and basic troubleshooting.



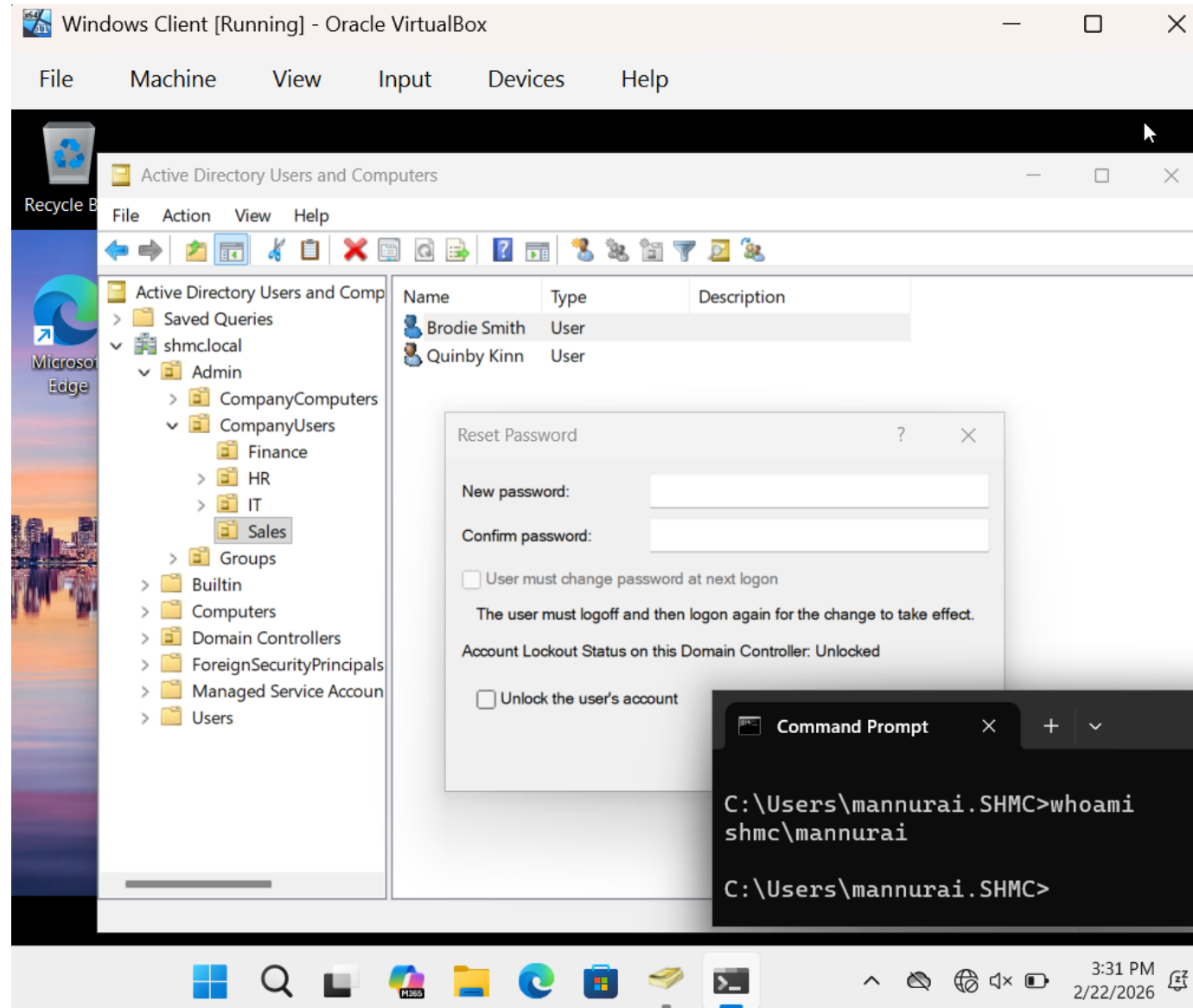
Delegation of Control

- 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.

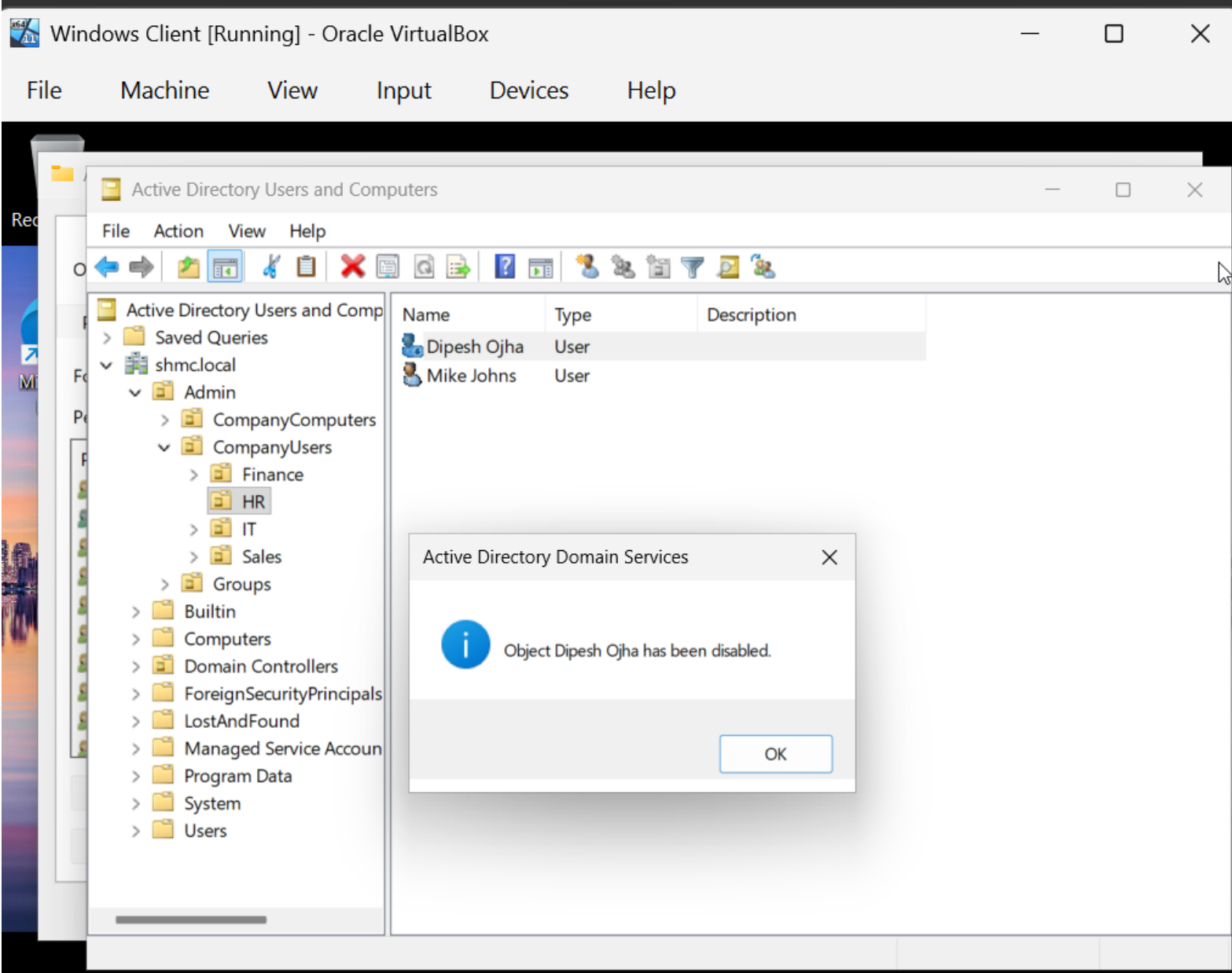
Delegating IT Security group basic management controller over Company Users OU, Any users that have issues with password, account, group membership can report to IT team member for a resolution.



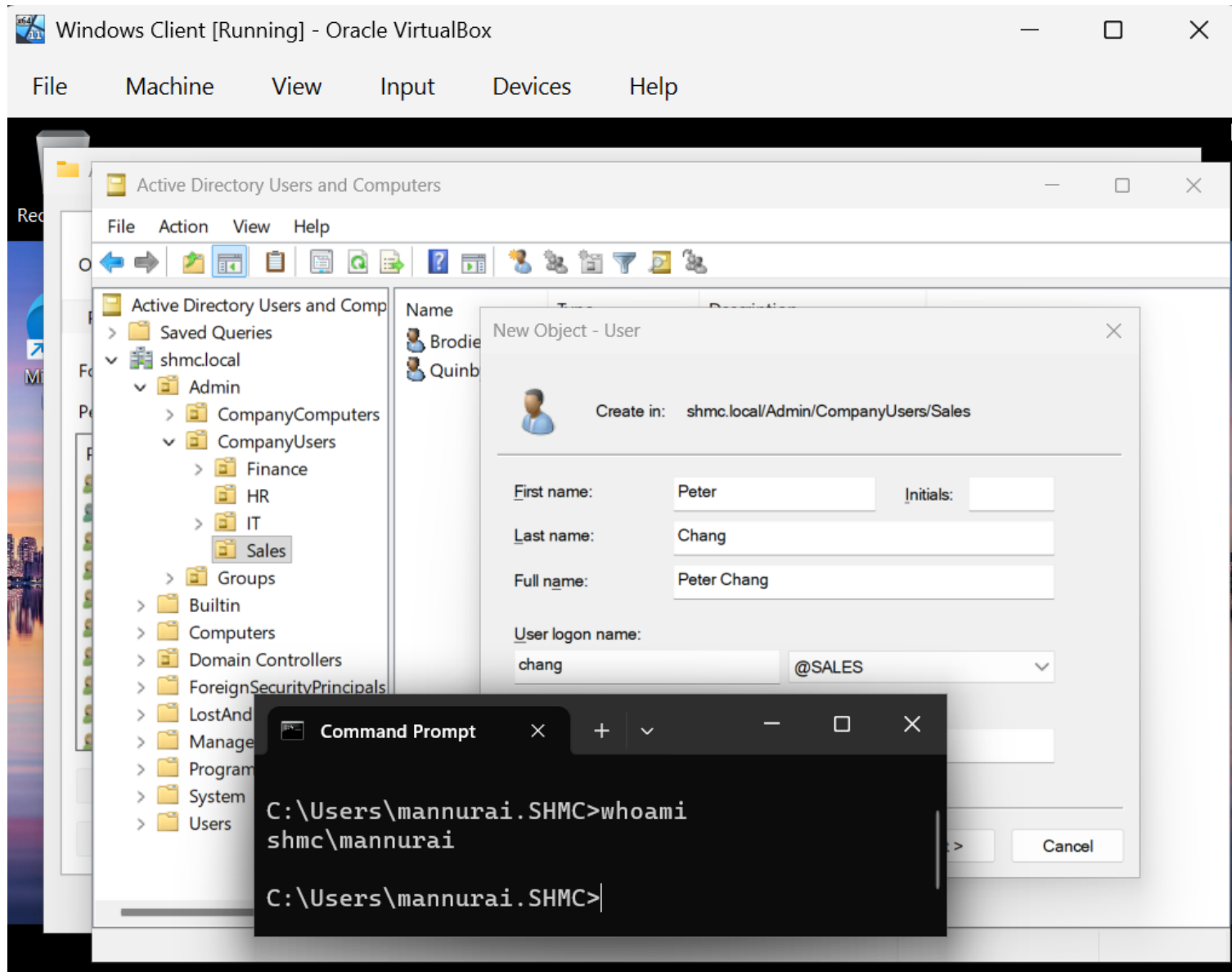
Administrating Active directory Users and Computers from member of IT security group, Mannurai a member of IT Security Group can solve issues related to users and groups using RSAT on the Client machine.



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.

