

Name: Truong Dang Truc Lam
ID: B2111933
Class: CT209H-M04

LAB 6

Exercise 1: Creating a Starter GPO

The first screenshot shows the 'Prohibit user configuration of Offline Files' Group Policy setting. It is configured to be 'Enabled'. The 'Supported on' field lists 'Windows Server 2003, Windows XP, and Windows 2000 only'. The second screenshot shows the 'Remove "Make Available Offline" command' Group Policy setting, also configured to be 'Enabled'. The 'Supported on' field lists 'At least Windows 2000'.

Create a Starter GPO to serve as a template

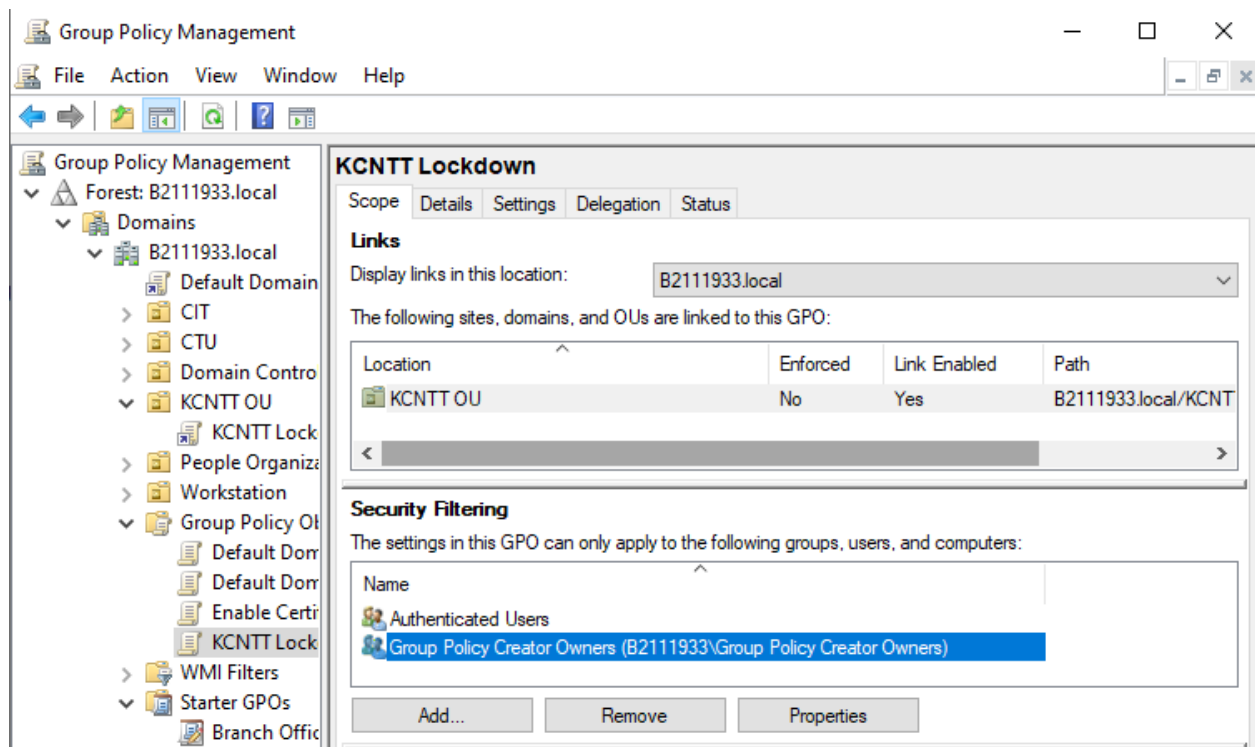
Exercise 2 Creating Group Policy Objects

The screenshot shows the Group Policy Management Editor. The left pane displays the 'Computer Configuration' tree, expanded to 'Policies'. The right pane shows a list of policies under the 'Policy Setting' column:

Policy Setting
Account lockout duration
30 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
30 minutes

Adjust the account lockout policies to prevent unauthorized access

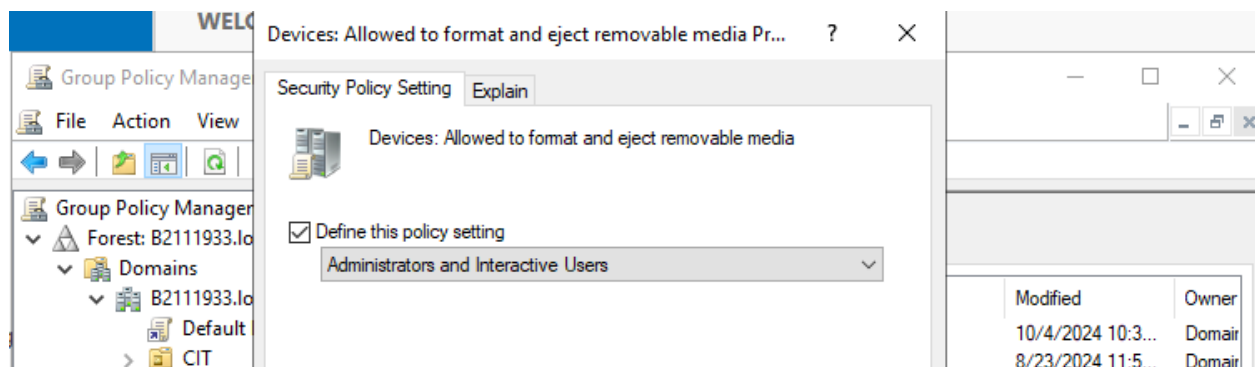
Exercise 3 Linking a Group Policy Object

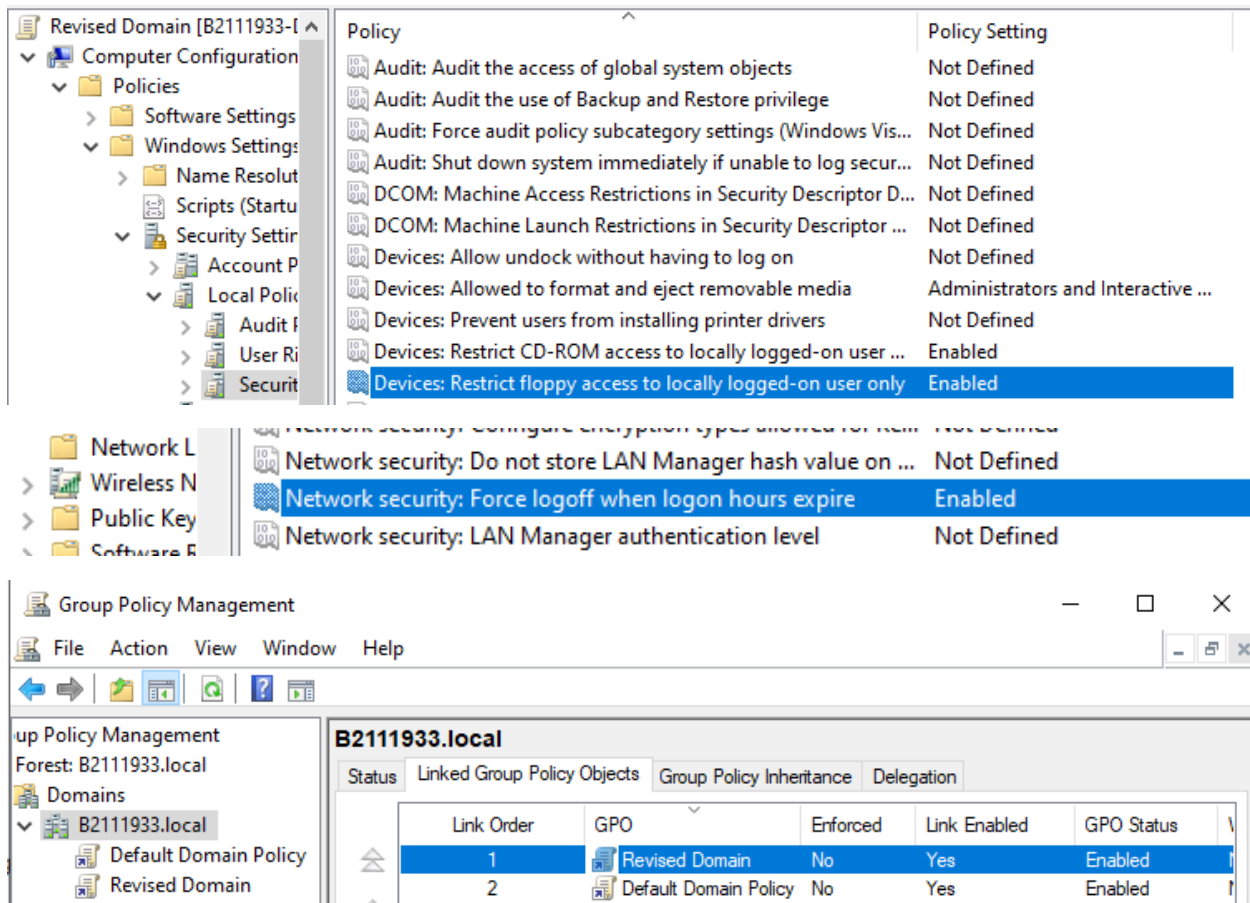


However, I cannot find any “Servers” object

Lab Challenge Confirming GPO Application

Exercise 4: Configuring Security Policies



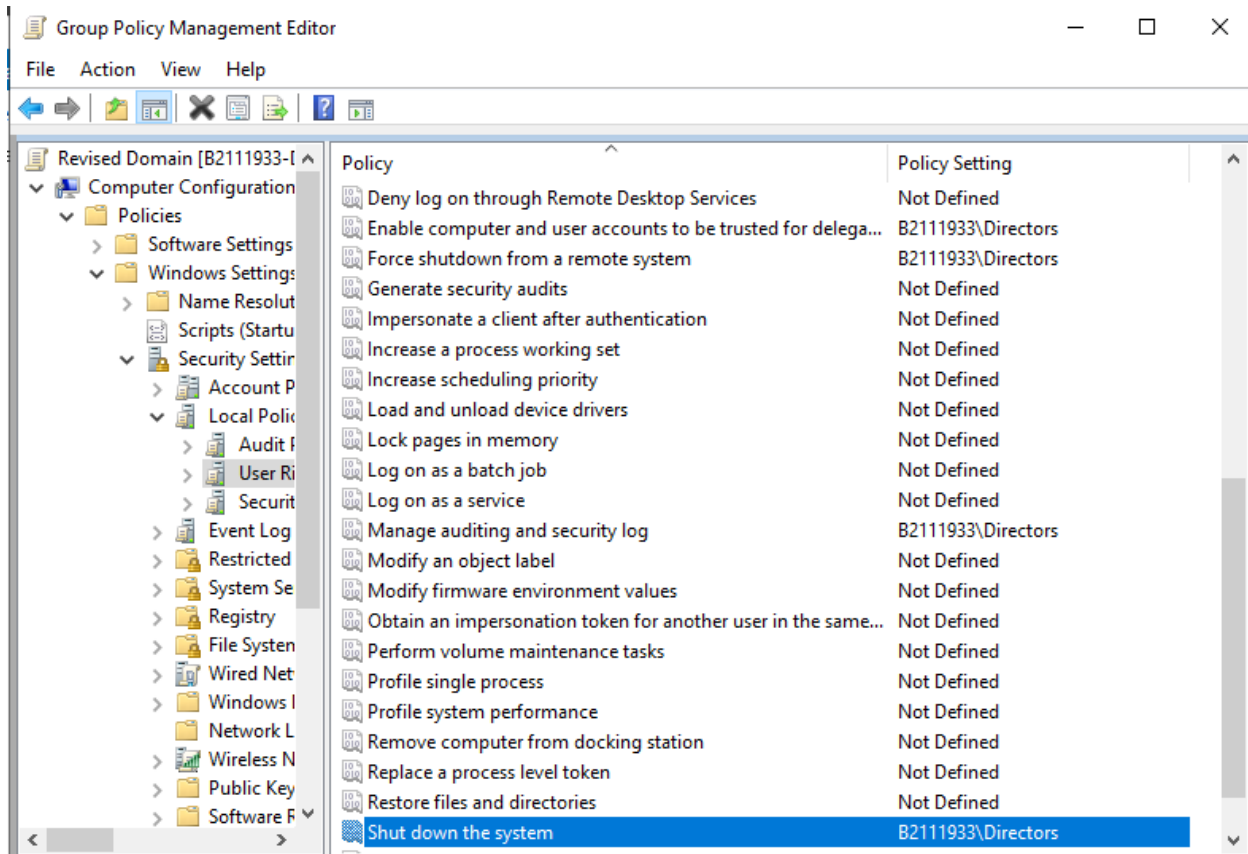
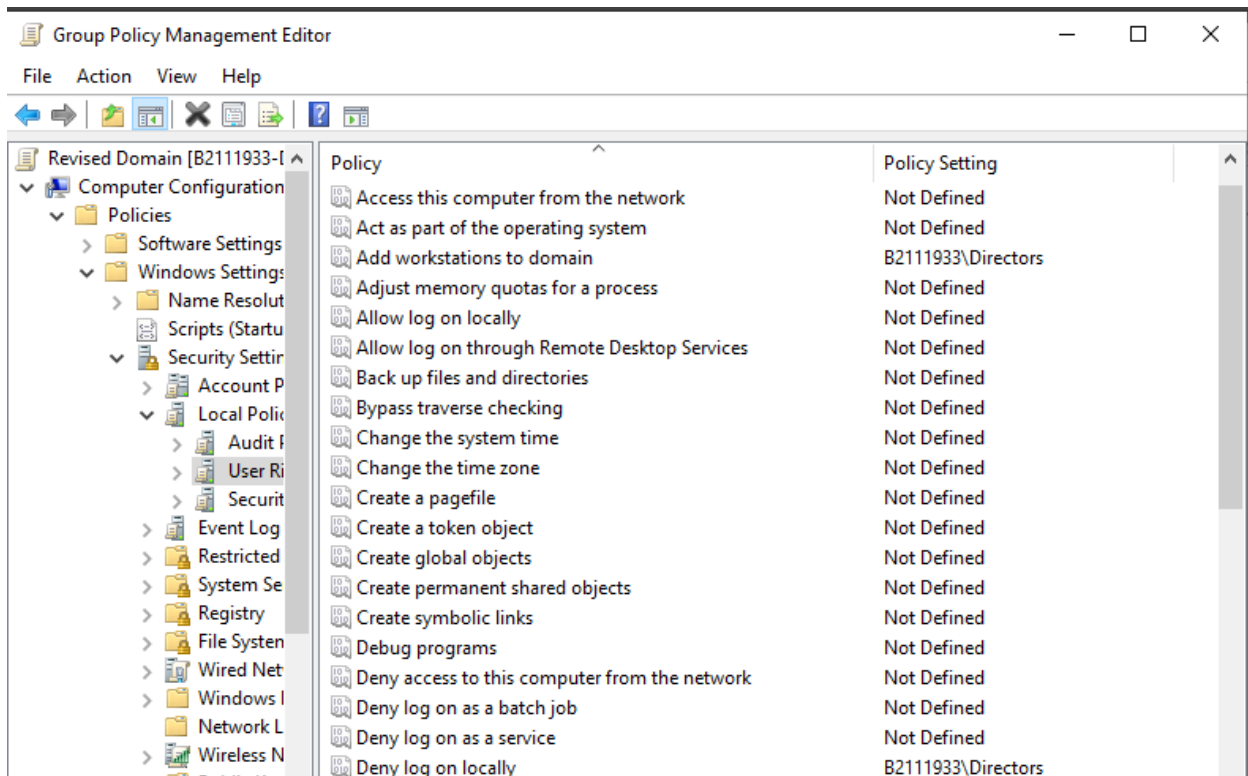


In Group Policy, the settings from higher-precedence GPOs will overwrite conflicting settings from those that have lower-precedence. By placing the Revised Options GPO first, its settings will take effect even if there are other GPOs linked to the domain that might have different configurations for the same policies.

Lab Challenge: Assigning User Rights

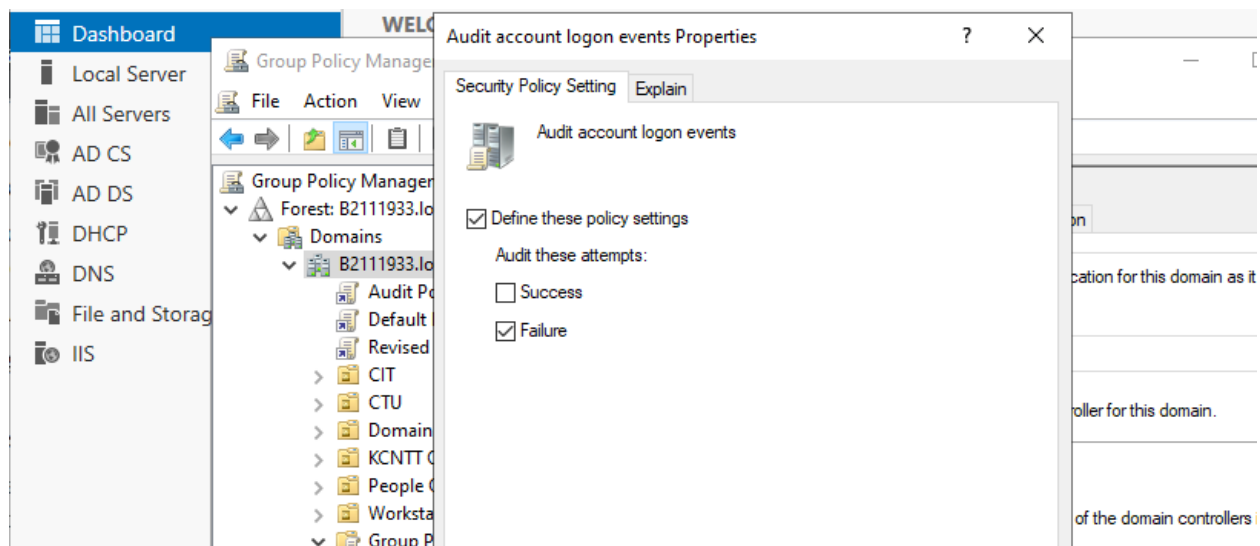
I have followed these steps:

1. Create the Directors Group
2. Add Users to the Directors Group
3. Assign User Rights to the Directors Group with Revised Domain Policy:
(Right click Revised Domain > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment)



Assign user rights to Directors group

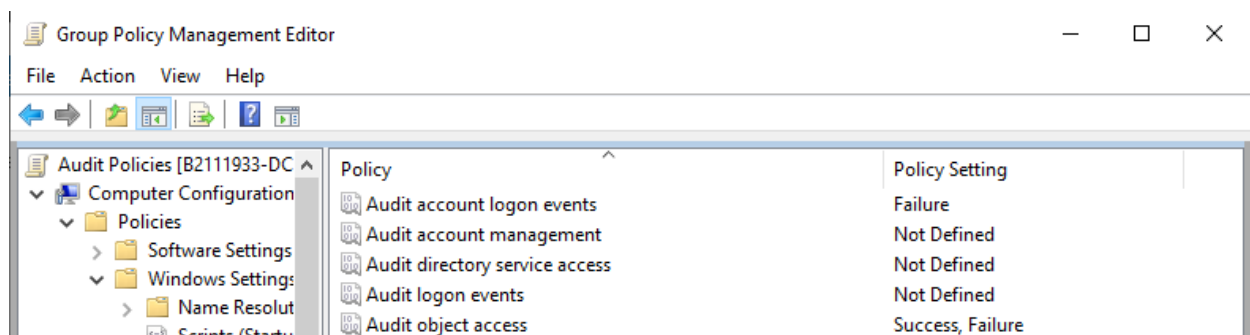
Exercise 5: Configuring Audit Policies



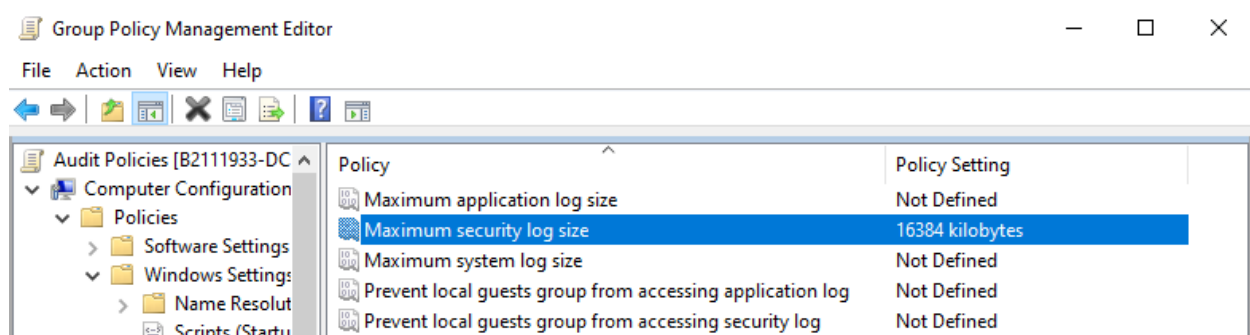
Configure Audit Policies for logon events

Why, in this case, is the auditing of event failures more useful than the auditing of successes?

Answer: Auditing event failures is more useful than auditing successes because it helps identify unauthorized attempts to log on to accounts or access specific objects.



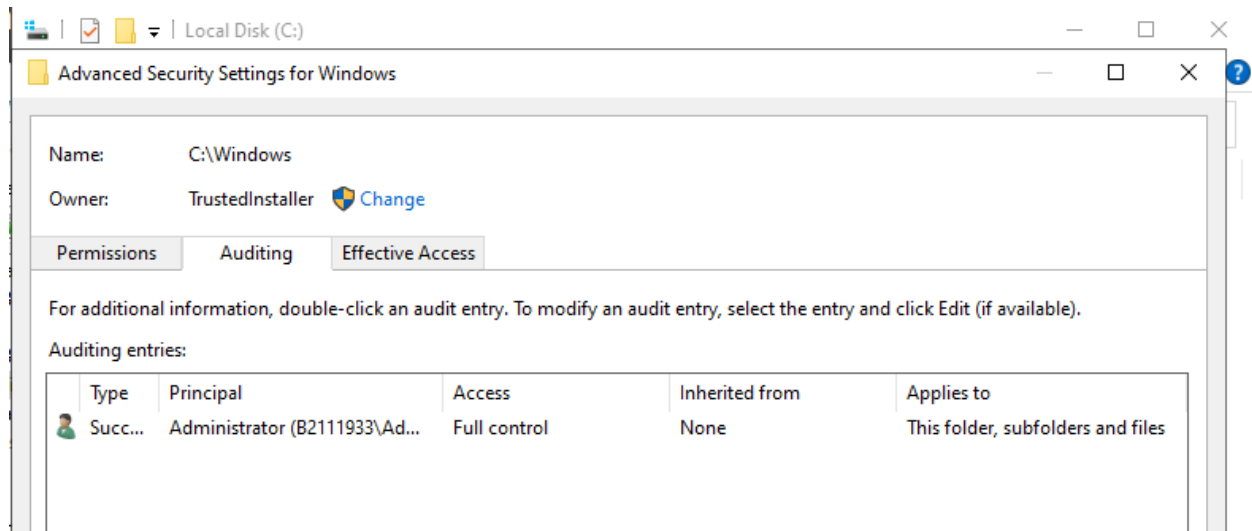
Configure Audit Policies for object access



Set Maximum security log size to 16384 kilobytes

Why is it prudent to limit the event log size when using auditing?

Limiting the event log size when using auditing is prudent to prevent the log from filling up and causing system performance issues. Additionally, it can help us focus on important events and avoid being overwhelmed by unnecessary information.



Configure auditing for the Administrator

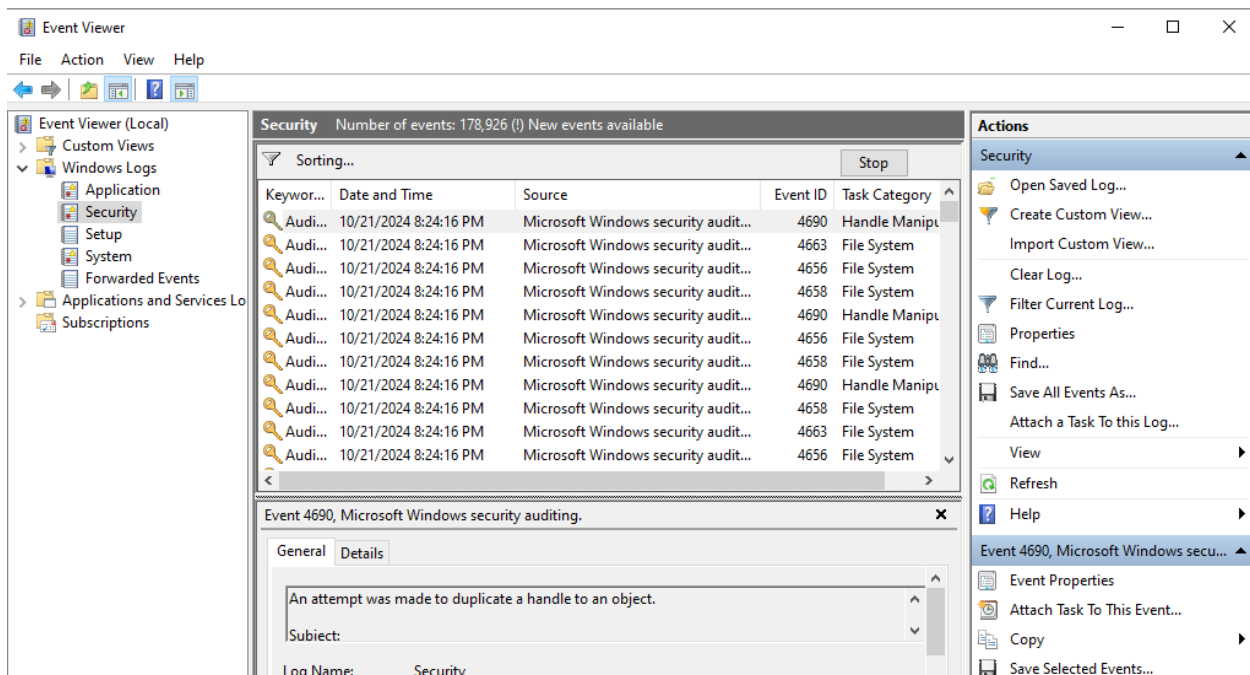
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

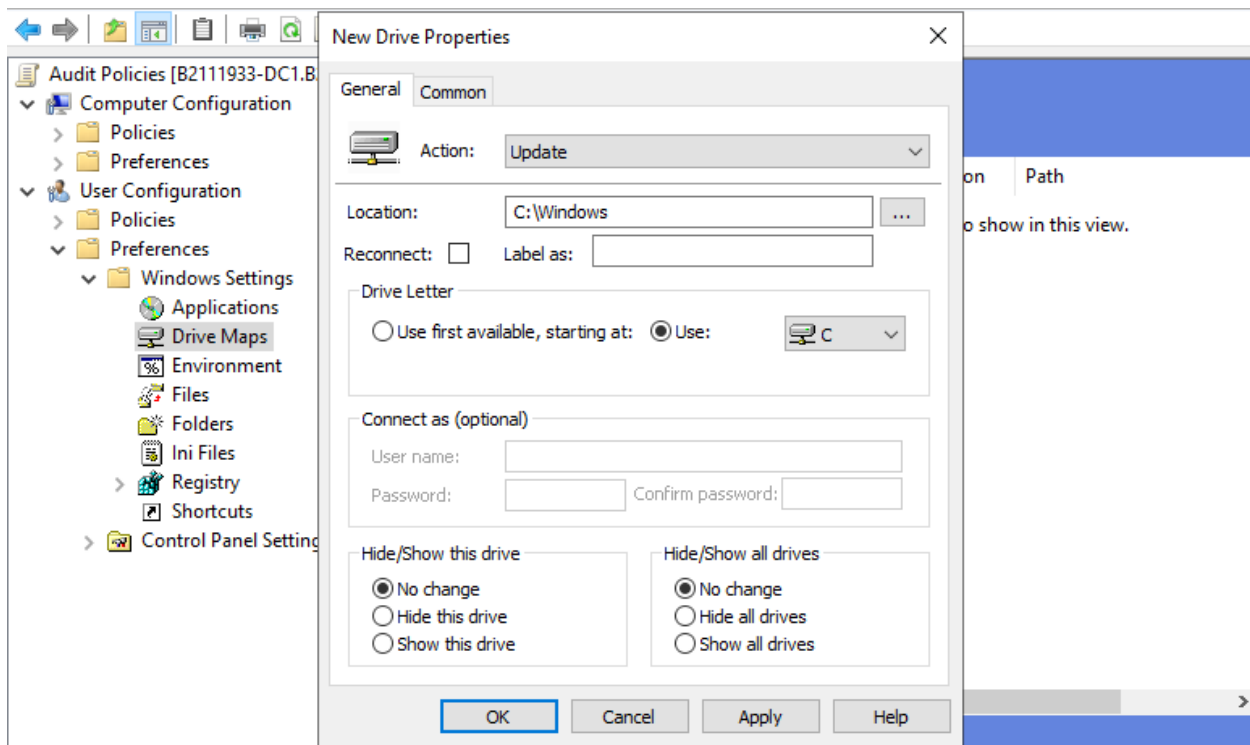
User Policy update completed

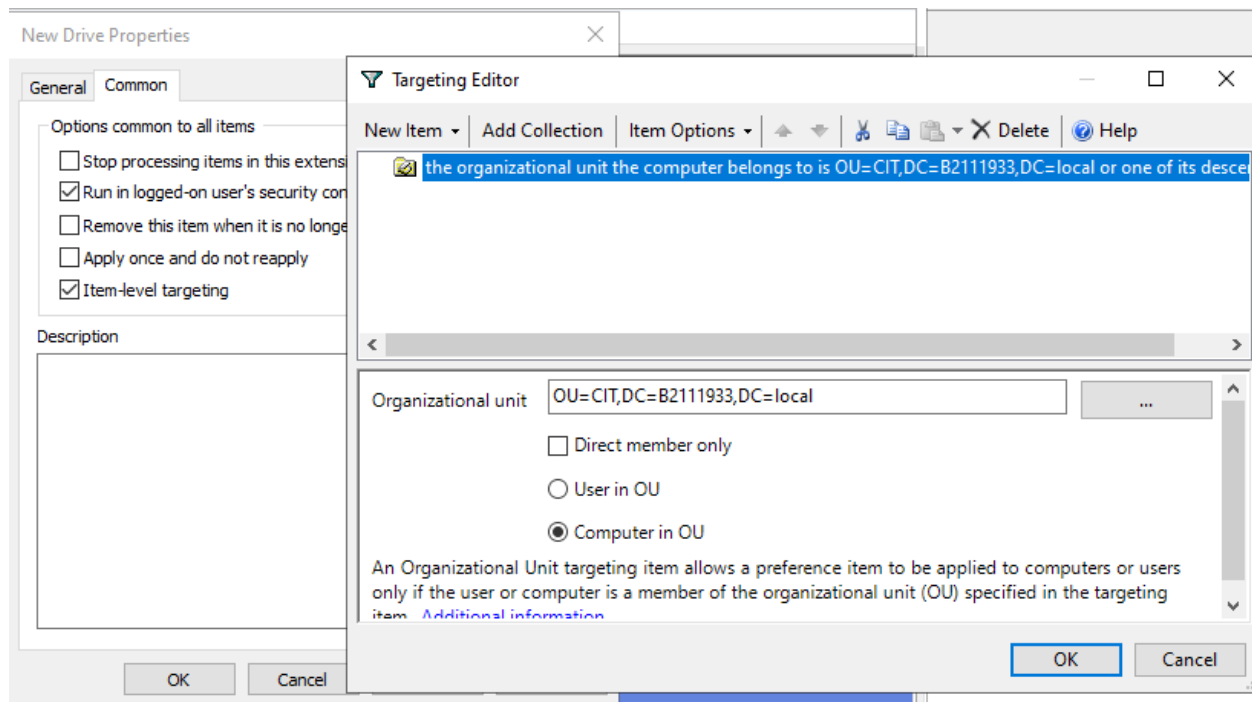
Lab Challenge: Viewing Auditing Data



Viewing auditing data

Lab 6: Configuring GPO to map A network drive





Configure GPO to map A network drive