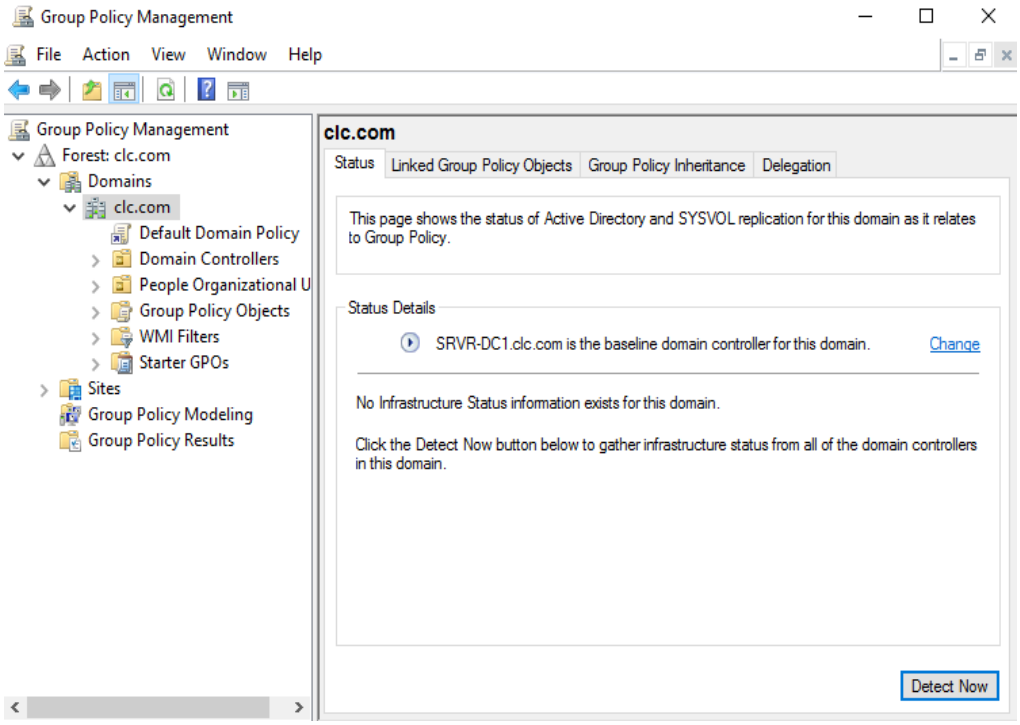
Lab 5

Creating and configuring Group Policy Objects

Exercise 1: Creating a Starter GPO

In this exercise, you create a new starter GPO containing settings that you want all your new GPOs to receive.

1. On Server, in Server Manager, click Tools > Group Policy Management. The Group Policy Management console appears.
2. In the left pane, expand the Forest: clc.com node, the Domains node, and the clc.com node

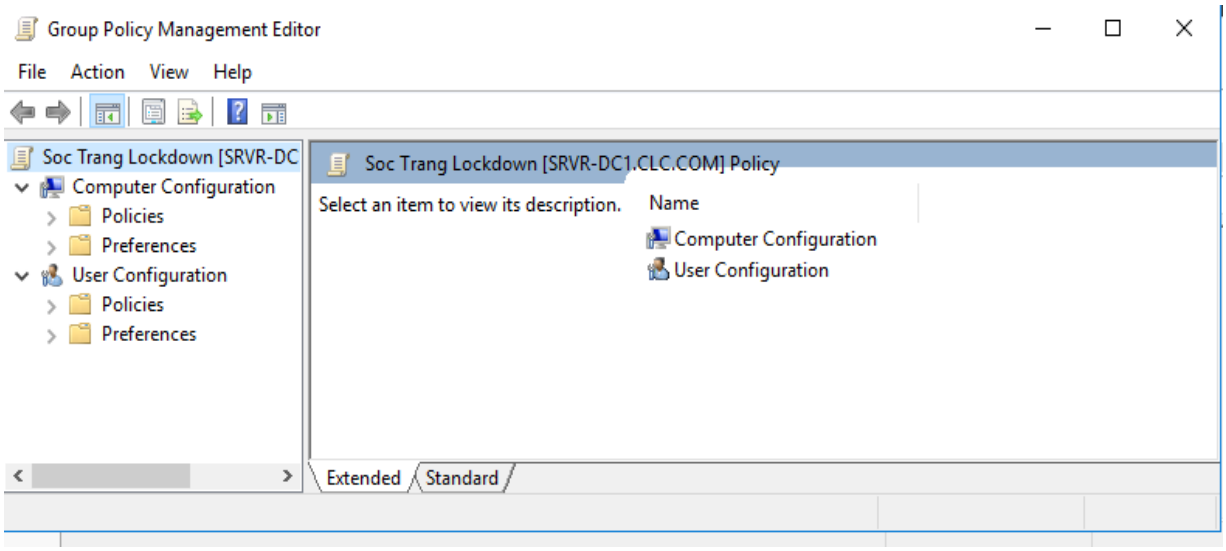


3. Right-click the Starter GPOs node and, from the context menu, click New. The New Starter GPO dialog box appears
4. In the Name text box, type Branch Office and click OK. The new starter GPO appears in the console.
5. Expand the Starter GPOs node, right-click the Branch Office GPO, and, from the context menu, select Edit. The Group Policy Starter GPO Editor console appears.
6. In the left pane, browse to the Computer Configuration > Administrative Templates > Network > Offline Files folder.
7. In the right pane, double-click the Prohibit user configuration of offline files policy. The Prohibit user configuration of offline files dialog box appears.

8. Select the Enabled option and click OK.
9. Open the Remove “Make Available Offline” Command dialog box and enable it as you did before, clicking OK when finished.
10. Close the Group Policy Starter GPO Editor console

Exercise 2 Creating Group Policy Objects

1. On sever, in the Group Policy Management console, right-click the Branch Office Starter GPO you created in Exercise 1, and, from the context menu, select New GPO from Starter GPO. The New GPO dialog box appears.
2. In the Name text box, type KCNTT Lockdown and click OK.
3. Expand the Group Policy Objects node. The new KCNTT Lockdown GPO appears.
4. Right-click the KCNTT Lockdown GPO and, from the context menu, select Edit. The Group Policy Management Editor console appears

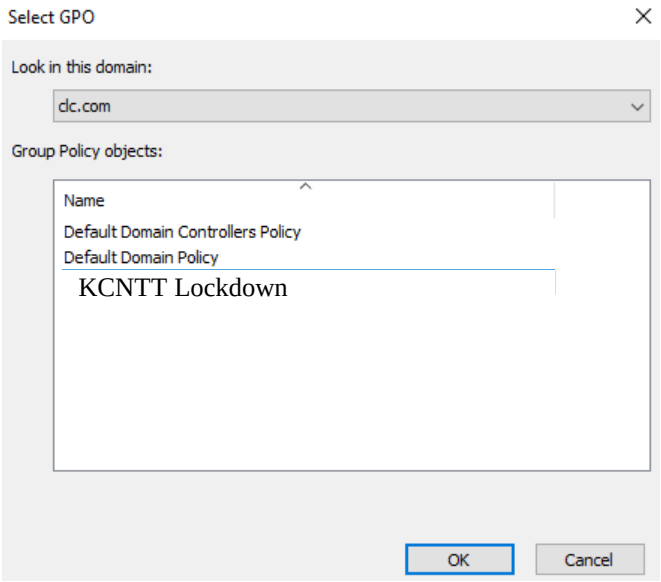


5. Now, browse to the Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy folder.
6. Open the following three policies, click the Define this policy setting check box, and configure them with the specified values:
    - Account lockout duration – 30 minutes
    - Account lockout threshold – 5 invalid Logon attempts
    - Reset account lockout after – 30 minutes
7. Close the Group Policy Management Editor console.

Exercise 3 Linking a Group Policy Object

To complete this exercise, you must apply the GPO you have made to an organizational unit, and control its application using security filtering.

1. On member sever, in the Group Policy Management console, right-click the KCNTT OU and, in the context menu, select Link an Existing GPO. The Select GPO dialog box appears
2. In the Group Policy Objects list, select KCNTT Lockdown and click OK. The GPO appears in the right pane, on the Linked Group Policy Objects tab of KCNTT OU.



3. Click the Group Policy Inheritance tab. The list of GPOs now contains the KCNTT Lockdown and the Default Domain Policy GPO.
4. In the Group Policy Objects node, select the KCNTT Lockdown GPO (click OK if a message appears) and, in the right pane, look at the Scope tab.
5. In the Security Filtering area, click Add. The Select User, Computer, or Group dialog box appears.
6. In the Enter the object name to select text box, type Servers and click OK. The Servers group appears in the Security Filtering list.
7. Select the Authenticated Users group and click Remove.
8. Click OK to confirm the removal.

Lab Challenge Confirming GPO Application

Demonstrate that the Group Policy settings you have created in the KCNTT Lockdown GPO have taken effect on other computer.

The client computer is located in the KCNTT OU, and is a member of the Servers group. It should, therefore, receive the settings you configured in the KCNTT Lockdown GPO.

Prove that this is the case by taking screen shots of the computer that demonstrate that the Account Lockout Threshold value has changed.

Exercise 4: Configuring Security Policies

In this exercise, you examine the default Security Policy settings for your domain and then create a GPO containing new and revised settings.

1. Log on to the server
2. In Server Manager, click Tools > Group Policy Management. The Group Policy Management console appears.
3. Browse to the Group Policy Objects folder.
4. Right-click the Group Policy Objects folder and, on the context menu, click New. The New GPO dialog box appears.
5. In the Name text box, type Revised Domain and click OK. A new Revised Domain GPO appears in the Group Policy Objects folder.
6. Right-click the Revised Domain GPO and, in the context menu, click Edit. The Group Policy Management Editor console appears.
7. In the Group Policy Management Editor console, browse to the Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options folder.
8. In the Security Options folder, double-click the Devices: Allowed to format and eject removable media policy.
9. Select the Define this policy setting check box, and in the drop-down list, select Administrators and Interactive Users. Then click OK.
10. Define and enable the following Security Options policies:
11. Devices: Restrict CD-ROM access to locally logged on user only policy
12. Devices: Restrict floppy access to locally logged on user only policy
13. Network Security: Force logoff when logon hours expire
14. Close the Group Policy Management Editor console.
15. In the Group Policy Management console, right-click the clc.com domain and, in the context menu, click Link an Existing GPO.
16. Select the Revised Domain GPO and click OK.
17. Select the clc.com domain and click the Linked Group Policy Objects tab in the right pane.
18. Select the Revised Domain GPO and click the Move link up arrow. The Revised Domain GPO now appears first in the list of linked GPOs.

Why is it necessary for the Revised Options GPO to appear first in the list?

Lab Challenge: Assigning User Rights

Your organization has created a new job role called the director, and your job is to provide the new directors with the domain controller user rights they need to perform their jobs. Creating group in the clc.com domain. To complete this challenge, you must create a group name Directors grant the Directors group the following user rights to all the domain controllers on the network, without interfering with any of the existing rights.

- Deny logon locally
- Add workstations to domain
- Force shutdown from a remote system
- Enable computer and user accounts to be trusted for delegation
- Manage auditing and security log
- Shut down the system

Write out the basic steps you have to perform to accomplish the challenge and then take a screen shot showing the user rights you configured

Exercise 5: Configuring Audit Policies

In this exercise, you configure the auditing policies to monitor account logons and access to specific objects.

1. On Log on to the server
2. In the Group Policy Management console, create a new GPO called Audit Policies and open it in the Group Policy Management Editor.
3. Browse to the Computer Configuration > Policies > Windows Settings > Security
4. Settings > Local Policies > Audit Policy node. The audit policies appear in the right pane.
5. Double-click the Audit account logon events policy. The Audit account logon events Properties sheet appears.
6. Select the Define these policy settings check box.
7. Select the Failure check box, clear the Success check box, and click OK.

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

8. Double-click the Audit object access policy. The Audit object access Properties sheet appears.
9. Select the Define these policy settings check box.

10. Select the Failure and the Success check boxes and click OK.
11. Under Security Settings, select the Event Log node.
12. In the right pane, double-click the Maximum security log size policy.
13. Select the Define this policy setting check box, leave the spinbox value at 16384 kilobytes, and click OK.

    Why is it prudent to limit the event log size when using auditing?
14. Close the Group Policy Management Editor console.
15. Link the Audit Policies GPO to the clc.com domain.
16. Click the File Explorer icon on the Taskbar. The File Explorer window appears.
17. In the left pane, browse to the C: drive on the local computer.
18. Right-click the C:\Windows folder and, in the context menu, click Properties. The Windows Properties sheet appears.
19. Click the Security tab.
20. Click Advanced. The Advanced Security Settings for Windows dialog box appears.
21. Click the Auditing tab
22. Click Add. The Auditing Entry for Windows dialog box appears.
23. Click Select a Principal. The Select User, Computer, Service Account, or Group dialog box appears.
24. In the Enter the object name to select text box, type Administrator and click OK.
25. Select the Full Control check box and click OK.
26. Click OK to close the Advanced Security Settings for Windows dialog box.
27. Click Continue to bypass error messages, if necessary. Click OK to close the Windows Properties sheet.
28. Open an administrative Command Prompt window and type gpupdate /force to update the system's Group Policy settings

Lab Challenge: Viewing Auditing Data

Demonstrate that your member server is actually gathering the auditing data you configured its policies to gather.

To complete this challenge, display the auditing data you configured your server to gather in Exercise 6 and take screen shot showing a sample of the data you gathered.

Lab 6: Configuring GPO to map A network drive

1. Edit one of the previous GPO
2. Navigate to User Configuration -> Preferences -> Windows Settings -> Drive Maps

3. Right Click Drive Maps, Select New – > Mapped Drive
4. Configure Drive Mapping Properties

General Tab Settings

In location put the path to the share/folder you want to map a drive to.

Select a drive letter

Choose Update for action

Label as: This is optional but may be beneficial for users.

Common Tab Settings

Select “Run in logged on users’s security context

Select Item-level Targeting

Click the Targeting Button

Select New Item

Select Organization Unit then select the OU you want to target

5. Verify that GPO works on a client machine