LAB 16
CREATING GROUP POLICY OBJECTS

Dr. Rendong Bai

This lab contains the following exercises and activities:

Exercise 16.1	Installing Group Policy Management
Exercise 16.2	Creating a Starter GPO
Exercise 16.3	Creating Group Policy Objects
Exercise 16.4	Linking a Group Policy Object
Lab Challenge	Confirming GPO Application

BEFORE YOU BEGIN

The lab environment consists of three servers connected to a local area network, one of which is configured to function as the domain controller for a domain called *adatum.com*. The computers required for this lab are listed in Table 16-1.

Table 16-1
Computers Required for Lab 16

Computer	*Operating System*	*Computer Name*
Domain controller 1	Windows Server 2016	SERVERA
Member server 2	Windows Server 2016	SERVERB
Member server 3	Windows Server 2016	SERVERC

In addition to the computers, you also require the software listed in Table 16-2 to complete Lab 16.

Table 16-2
Software Required for Lab 16

Software	***Location***
Lab 16 student worksheet	Lab16_worksheet.docx (provided by instructor)

Working with Lab Worksheets

Each lab in this manual requires that you answer questions, take screen shots, and perform other activities that you will document in a worksheet named for the lab, such as Lab16_worksheet.docx. It is recommended that you use a USB flash drive to store your worksheets, so you can submit them to your instructor for review. As you perform the exercises in each lab, open the appropriate worksheet file, fill in the required information, and save the file to your flash drive.

After completing this lab, you will be able to:

- Create a starter GPO
- Create new GPOs
- Link GPOs to organizational units
- Confirm GPO application to OU

Estimated lab time: 55 minutes

Exercise 16.1	Installing Group Policy Management
Overview	In this exercise, you install the Group Policy Management tools that enable you to create and manage GPOs from a member server.
Mindset	What is the most convenient location to manage your enterprise Group Policy strategy?
Completion time	10 minutes

1. Log on to the **SERVERB** computer as domain administrator and then, in Server Manager, click **Manage** > **Add Roles and Features**. The Add Roles and Features Wizard appears, displaying the *Before you begin* page.
2. Click Next. The *Select installation type* page appears.
3. Click Next. The *Select destination server* page appears.
4. Click Next. The *Select server roles* page appears.

5. Click Next. The ***Select features*** page appears.

6. Scroll down and select the **Group Policy Management** check box.

   If the **Group Policy Management** feature has been installed, click Cancel and move to step 10.

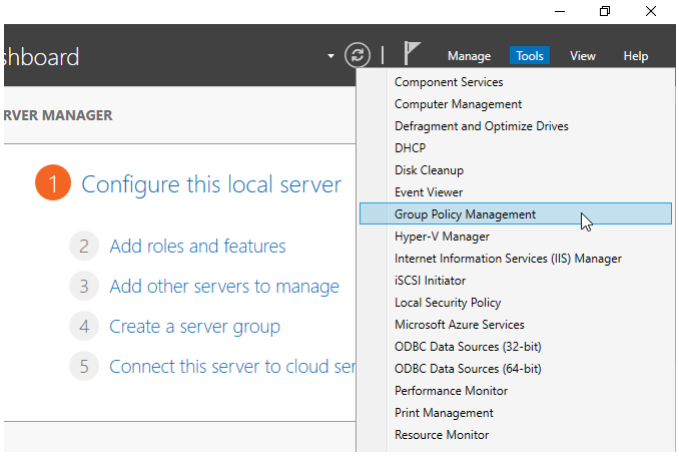
7. Click Next. The *Confirm installation selections* page appears.

8. Click Install. The *Installation progress* page appears as the wizard installs the selected features.

9. Click Close. The wizard closes.

10. Click Tools. The Tools menu appears, which now contains the **Group Policy Management** console.

11. **[SCREEN SHOT 1]** Press Alt+Prt Scr to take a screen shot of the Tools menu. Press Ctrl+V to paste the image on the page provided in the Lab 16 worksheet file.



End of exercise. Leave all windows open for the next exercise.

Exercise 16.2	Creating a Starter GPO
Overview	In this exercise, you create a new starter GPO containing settings that you want all your new GPOs to receive.
Mindset	How do I avoid configuring the same settings in many GPOs?
Completion time	10 minutes

1. On **SERVERB**, in Server Manager, click Tools > **Group Policy Management**. The Group Policy Management console appears.

2. In the left pane, expand the **Forest: adatum.com** node, the **Domains** node, and the **adatum.com** node (see Figure 16-1).

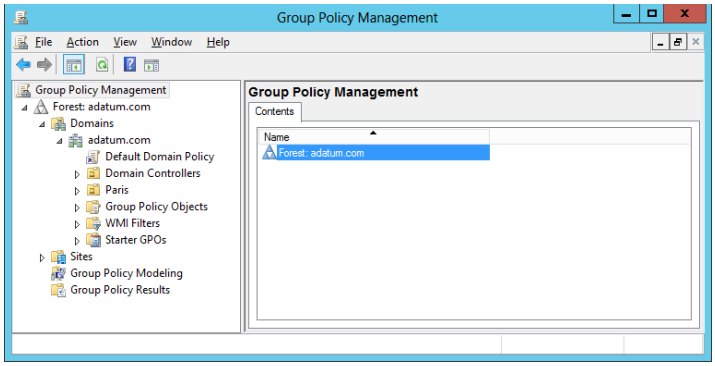


Figure 16-1
The Group Policy Management console

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.

   It seems the following part is not in Server 2016. If you didn't see "Show…", just ignore and continue.

   Under Options and Files and Folders, click "Show…", **Show Contents** dialog box appears.

   Click Value name box, enter "\\SERVERB\Users\student\Documents", click OK to close Show Contents dialog box.

Click OK to close ***Remove "Make Available Offline"*** dialog box.

10. **[SCREEN SHOT 2]** Press Alt+Prt Scr to take a screen shot of the Group Policy Starter GPO Editor console, showing the two policies you configured. Press Ctrl+V to paste the image on the page provided in the Lab 16 worksheet file.

11. Close the Group Policy Starter GPO Editor console.

End of exercise. Leave all windows open for the next exercise.

Exercise 16.3	Creating Group Policy Objects
Overview	To complete this exercise, you use the starter GPO you created previously to create a new GPO with additional settings.
Mindset	How do I use a starter GPO to create additional GPOs?
Completion time	10 minutes

1. On **SERVERB**, in the Group Policy Management console, right-click the **Branch Office** Starter GPO you created in Exercise 16.2, and, from the context menu, select **New GPO from Starter GPO**. The New GPO dialog box appears.

2. In the Name text box, type **Prague Lockdown** and then click OK.

3. Expand the **Group Policy Objects** node. The new Prague Lockdown GPO appears.

4. Right-click the **Prague Lockdown** GPO and, from the context menu, select **Edit**. The Group Policy Management Editor console appears (see Figure 16-2).

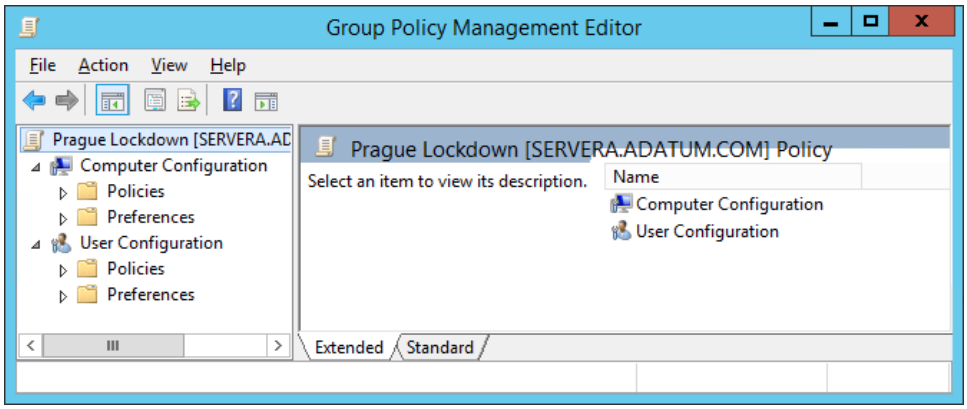


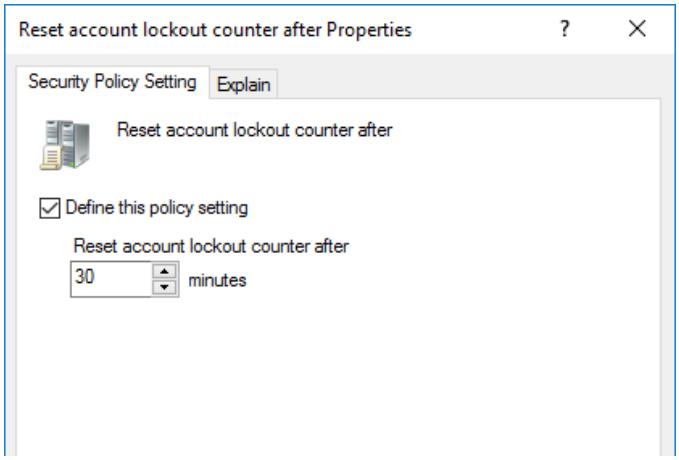
Figure 16-2
The Group Policy Management Editor console

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. **[SCREEN SHOT 3]** Press Alt+Prt Scr to take a screen shot of the *Reset account lockout after Properties* sheet, showing the changes you made to its configuration. Press Ctrl+V to paste the image on the page provided in the Lab 16 worksheet file.



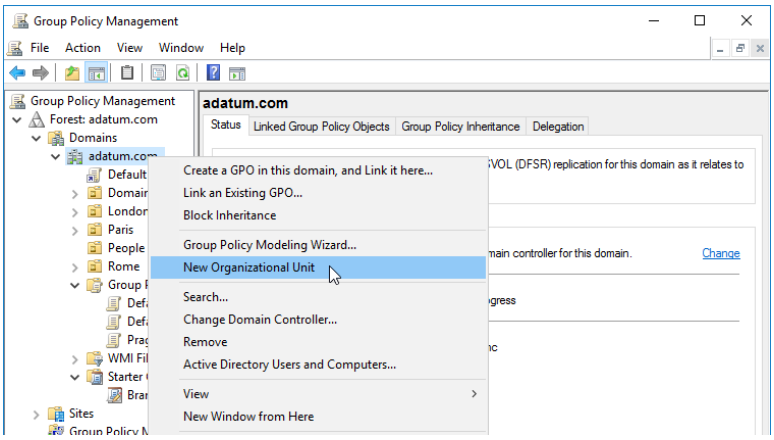
8. Close the Group Policy Management Editor console.

End of exercise. Leave all windows open for the next exercise.

Exercise 16.4	Linking a Group Policy Object
Overview	To complete this exercise, you must apply the GPO you have made to an organizational unit, and control its application using security filtering.
Mindset	How do you control which computers receive the settings in a specific GPO?
Completion time	10 minutes

1. Log on to **SERVERA** as Adatum\administrator using the password **Pa$$W0rd.**
2. On Server Manager select Tools > **Active Directory Users and Computers**.
3. Under the adatum.com node, right click the **Users** OU and select **New** > **Group**.
4. In the *New Object – Group* window create a ***Global Security group*** named **Directors**.
5. Select OK and then close Active Directory Uses and Computers.

6. On **SERVERB**, in the Group Policy Management console, right-click adatum.com, click “New Organizational Unit”



7. Enter **Prague** and click OK.

8. Right-click the Prague OU and, in the context menu, select "Link an Existing GPO". The Select GPO dialog box appears (see Figure 16-3).

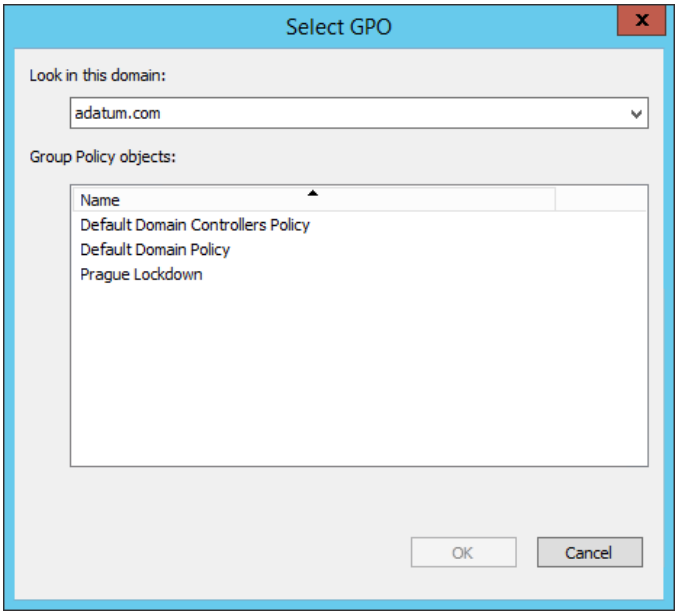


Figure 16-3
The Select GPO dialog box

9. In the Group Policy objects list, select **Prague Lockdown** and click OK. The GPO appears in the right pane, on the Linked Group Policy Objects tab of Prague OU.

10. Click the Group Policy Inheritance tab. The list of GPOs now contains the Prague Lockdown and the Default Doman Policy GPO.

Question 1	*What causes the Default Domain Policy GPO to appear here, even though it is not directly linked to the Prague OU?*

Question 2	*In the Default Domain Policy GPO, the value assigned to the Account Lockout Threshold policy is 0. In the Prague Lockout GPO, the same policy has a value of 5. Which of these values will a computer in the Prague OU use after processing all its Group Policy settings?*

11. In the "Group Policy Objects" node, select the **Prague Lockdown** GPO (click OK if a message appears) and, in the right pane, look at the **Scope** tab.

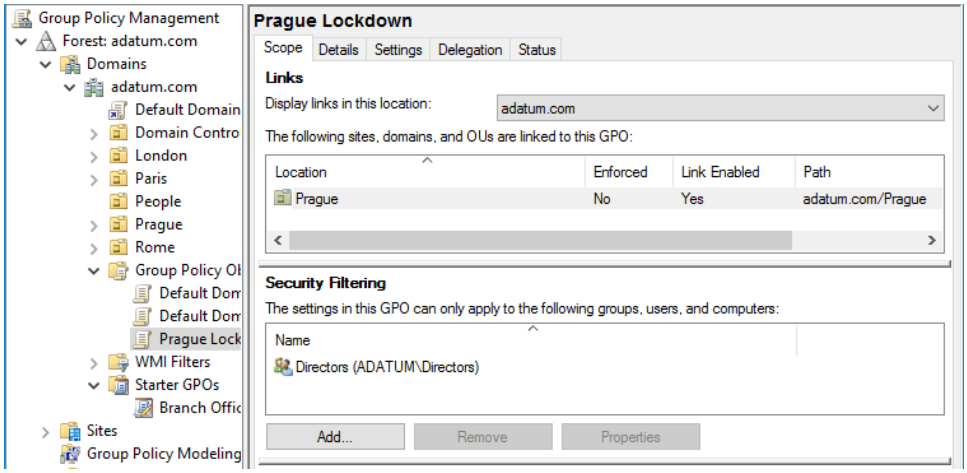
12. In the "Security Filtering" area, click **Add**. The Select User, Computer, or Group dialog box appears.

13. In the *Enter the object name to select* text box, type **Directors** and click OK. The **Directors** group appears in the Security Filtering list.

14. Select the **Authenticated Users** group and click **Remove**.

15. Click OK to confirm the removal.

16. **[SCREEN SHOT 4]** Press Alt+Prt Scr to take a screen shot of the Group Policy Management console, showing the changes you made to the Security Filtering configuration. Press Ctrl+V to paste the image on the page provided in the Lab 16 worksheet file.



End of exercise. Leave all windows open for the next exercise.

Lab Challenge	Confirming GPO Application
Overview	To complete this challenge, you must demonstrate that the Group Policy settings you have created in the Prague Lockdown GPO have taken effect on SERVERC.
Mindset	How can you tell when Group Policy settings are active?
Completion time	15 minutes

The SERVERC computer is located in the Prague OU, and is a member of the Server group. It should, therefore, receive the settings you configured in the Prague 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.

NOTE	*Before you begin working on SERVERC, open an administrative command prompt and run the **gpupdate /force** command to refresh the computer's Group Policy settings.*

End of lab. You can log off or start a different lab. If you want to restart this lab, you'll need to click the End Lab button in order for the lab to be reset.