Lab 7

Configuring Advanced Audit Policies

This lab contains the following exercises and activities:

|  |  |
| --- | --- |
| Exercise 7.1 | Implementing Auditing |
| Exercise 7.2 | Implementing Advanced Auditing |
| Exercise 7.3 | Using AuditPol.exe |
| Lab Challenge | Auditing Removable Devices |

BEFORE YOU BEGIN

The lab environment consists of student workstations connected to a local area network, along with a server that functions as the domain controller for a domain called *contoso.com*. The computers required for this lab are listed in Table 7-1.

Table 7-1

Computers Required for Lab 7

|  |  |  |
| --- | --- | --- |
| Computer | Operating System | Computer Name |
| Server (VM 1) | Windows Server 2012 | RWDC01 |
| Server (VM 2) | Windows Server 2012 | Server01 |

In addition to the computers, you also require the software listed in Table 7-2 to complete Lab 7.

Table 7-2

Software Required for Lab 7

|  |  |
| --- | --- |
| Software | Location |
| Lab 7 student worksheet | Lab07\_worksheet.rtf (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 Lab07\_worksheet.rtf. You will find these worksheets on the book companion site. 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 using WordPad, fill in the required information, and save the file to your flash drive.

After completing this lab, you will be able to:

* Configure standard audit policies
* Configure advanced audit policies
* Using AuditPol.exe to manage audit policies
* Audit removable devices

Estimated lab time: 60 minutes

|  |  |
| --- | --- |
| Exercise 7.1 | Implementing Auditing |
| Overview | During this exercise, you use standard Advanced Audit Policies to help keep track of who uses and attempts to use your network resources. |
| Completion time | 15 minutes |

**Mindset Question: Why is auditing important on today’s network?**

**1.** Log in to Server01 as **Contoso\Administrator** with the password of **Password01**.

**2.** On Server01, when the Server Manager opens, open the Tools menu and click Event Viewer. The Event Viewer console opens.

**3.** Expand Windows Logs and click Security.

|  |  |
| --- | --- |
| Question 1 | By looking at the current logs, what security events are being captured? |

**4.** Log in to RWDC01 as **Contoso\Administrator** with the password of **Password01**.

**5.** When Server Manger opens, click Local Server.

**6.** In the Properties pane, click On for *IE Enhanced Experience Improvement Program*.

**7.** When the *Internet Explorer Enhanced Security Configuration* dialog box opens, click Off for the Administratorsgroup.

**8.** Click OK to close the Enhanced Security Configuration dialog box.

**9.** Using Server Manager, open the Tools menu and click Group Policy Management. The Group Policy Management console opens.

**10.** Expand Forest:contoso.com > Domains > contoso.com and click Default Domain Policy. If a Group Policy Management Console dialog box opens, read the message and then click to select *Do not show this message again*, then click OK.

**11.** In the right-pane, click the Settings tab.

|  |  |
| --- | --- |
| Question 2 | Are there any audit policy settings configured for the Default Domain Policy? |

**12.** Expand the Domain Controllers node and click Default Domain Controllers Policy.

**13.** In the right-pane, click the Settings tab.

|  |  |
| --- | --- |
| Question 3 | Are there any audit policy settings configured for the Default Domain Controllers Policy? |

**14.** Right-click the contoso.com node and click *Create a GPO in this domain, and Link it here*. The New GPO dialog box opens.

**15.** For the name, type **Audit Policy** and click OK to close the New GPO dialog box.

**16.** Right-click the Audit Policy and click Edit. The Group Policy Management Editor opens.

**17.** Expand Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies, and click Audit Policy. The Policy settings show as shown in Figure 7-1.

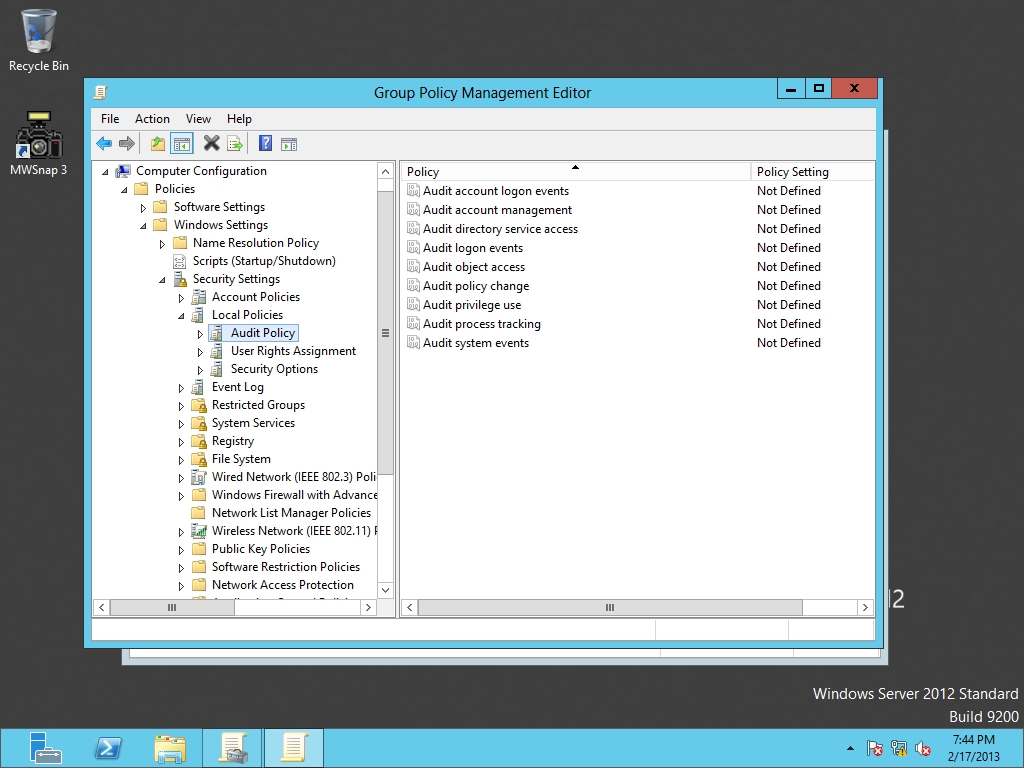


Figure 7-1

Configuring basic audit policies

**18.** Double-click Audit account logon events. The Audit account logon events Properties dialog box opens, as shown in Figure 7-2.

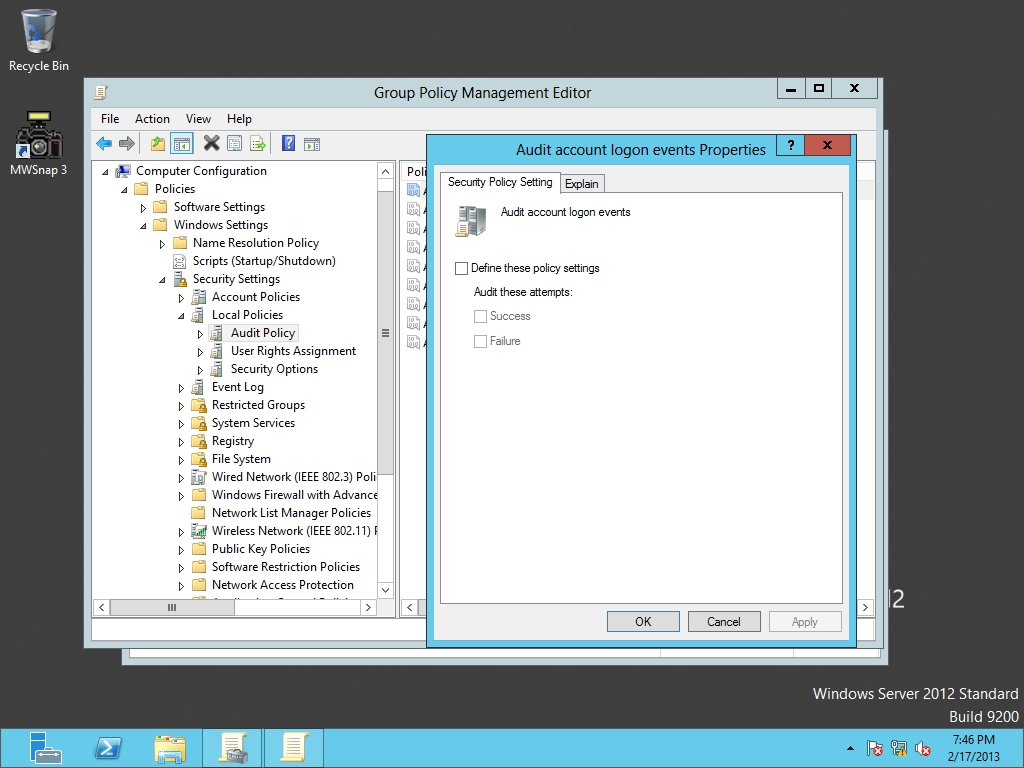


Figure 7-2

Enabling auditing of logon events

**19.** Click to select Define these policy settings and click to select both Success and Failure. Click OK to close the Audit account logon events Properties dialog box.

**20.** Double-click Audit Object access. The Audit object access Properties dialog box opens.

**21.** Click to select Define these policy settings and click to select both Success and Failure. Click OK to close the Audit object access Properties dialog box.

**22.** Go to Server01. With the Event Viewer open and Security highlighted, press F5 to refresh the Security logs.

**23.** Right-click the Start button and click Command Prompt (Admin). The Command Prompt opens.

**24.** Execute the following command:

gpupdate /force

**25.** Go back to the Event Viewer and refresh the Security logs again.

**26.** Take a screen shot of the Event Viewer window by pressing Alt+Prt Scr and then paste it into your Lab07\_worksheet file in the page provided by pressing Ctrl+V.

|  |  |
| --- | --- |
| Question 4 | What kind of events appears now? |

**27.** Go back to RWDC01. Open both Audit object access and Audit account logon events and uncheck the Define these policy settingscheck boxes.

**28.** Leave Group Policy Manager open for the next exercise.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 7.2 | Implementing Advanced Auditing |
| Overview | During this exercise, you use Advanced Audit Policies to help keep track of who uses and attempts to use your network resources. |
| Completion time | 20 minutes |

**Mindset Question: What advantage does advanced auditing have over standard auditing?**

**1.** On the RWDC01 server, if the Group Policy Management Editor is not open for the Audit Policy policy, right-click the Audit Policy and click Edit.

**2.** In the Group Policy Management Editor on RWDC01, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration and click Audit Policies, as shown in Figure 7-3.

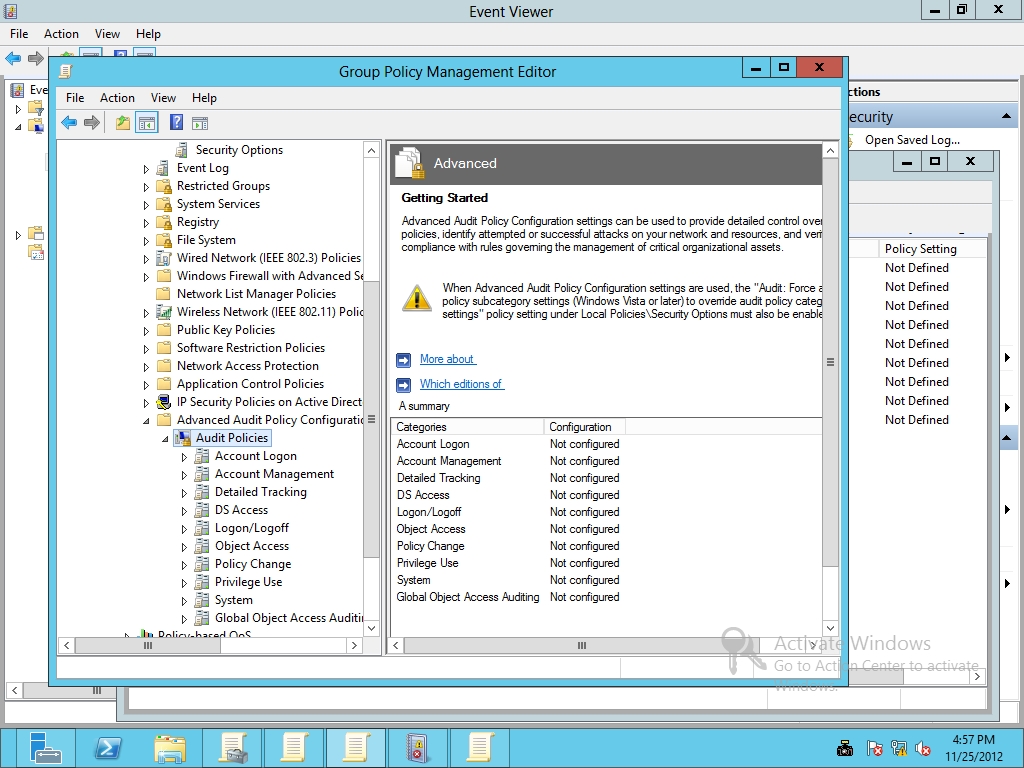


Figure 7-3

Configuring Advanced Audit Policy configuration settings

**3.** Under Audit Policies, double-click Logon/Logoff.

**4.** Double-click Audit Account Lockout. When the Audit Account Lockout Properties dialog box opens, click to select Configure the following audit events, and then select Success. Click OK to close Audit Lockout Properties.

**5.** Configure the following settings:

Audit Logoff Success

Audit Logon Success and Failure

**6.** Take a screen shot of the Group Policy Management Editor window by pressing Alt+Prt Scr and then paste it into your Lab07\_worksheet file in the page provided by pressing Ctrl+V.

**7.** Under Audit Policies, click Account Management and configure the following settings:

Audit Computer Account Management Success and Failure

Audit Security Group Management Success and Failure

Audit User Account Management Success and Failure

**8.** Under Audit Policies, click Object Access and configure the following settings:

Audit File Share Success and Failure

Audit File System Success and Failure

Audit Registry Success and Failure

Audit SAM Success and Failure

**9.** Click Privilege Use and configure the following settings:

Audit Sensitive Privilege Use Success and Failure

**10.** Click System and configure the following settings:

Audit Security State Change Success and Failure

**11.** Close the Group Policy Management Editor.

**12.** Go to Server01, open a Command prompt windows, and execute the gpupdate /force command.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 7.3 | Using AuditPol.exe |
| Overview | During this exercise, you use AuditPol.exe to manage auditing. |
| Completion time | 10 minutes |

**Mindset Question: What advantage does auditpol.exe have over standard and advanced audit policies?**

**1.** On the RWDC01 server, open a Command Prompt, and execute the following command to get a list of all Audit settings:

auditpol /get /category:\*

**2.** To see the audit policy set for Contoso\User1, execute the following command:

auditpol.exe /get /user:contoso\user1 /category:\*

**3.** Observe that there is no audit policy defined for Contoso\User1. To set the audit policy for User1 so that account management is audited for User1, execute the following command:

auditpol.exe /set /user:contoso\user1 /subcategory:"user account management" /success:enable /failure:enable

**4.** To display the settings for everyone again, run the following command:

auditpol /get /category:\*

**5.** To get the settings for user1, execute the following settings:

auditpol.exe /get /category:\* /user:user1

|  |  |
| --- | --- |
| Question 5 | Are the audit policies configured with Group Policies displayed when you specified a single user? |

**6.** Take a screen shot of the Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab07\_worksheet file in the page provided by pressing Ctrl+V.

**7.** To reset the settings for user1, execute the following settings:

auditpol /remove /user:contoso\user1

**8.** Verify that the per-user setting was removed by running the following command:

auditpol.exe /get /user:contoso\user1 /category:\*

LAB REVIEW QUESTIONS

|  |  |
| --- | --- |
| **Completion time** | **10 minutes** |

**1.** In Exercise 7.1, what is the location where you would find the standard auditing settings?

**2.** In Exercise 7.2, what is the location where you would find the advanced auditing settings?

**3.** In Exercise 7.2, which category would you use to enable auditing of the Registry?

**4.** In Exercise 7.3, what command did you use to configure a user-based audit policy?

|  |  |
| --- | --- |
| Lab Challenge | Auditing Removable Devices |
| Overview | To complete this challenge, you must demonstrate how to add audit removable devices by writing the steps to complete the tasks described in the scenerio. |
| Completion time | 5 minutes |

You need to determine when someone inserts a USB flash drive into a system in case it is being used to copy sensitive material. What can you do?

Write out the steps you performed to complete the challenge.

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.