Lesson 7: Configure Advanced Audit Policies
Overview

• Exam Objective 2.4: Configure Advanced Audit Policies
• Enabling and Configuring Auditing
Enabling and Configuring Auditing

Lesson 7: Configure Advanced Audit Policies
Enabling and Configuring Auditing

Enable auditing so you have a record of:

• Who has successfully logged in
• Who has attempted to log in but failed
• Who has made changes to accounts in Active Directory
• Who has accessed or changed certain files
• Who has used a certain printer
• Who restarted a system
• Who has made system changes
Implementing Auditing Using Group Policies

To enable auditing, specify what types of system events to audit using one of the following:

• Group Policy

• The local security policy (Computer Settings\Policies\Security Settings\Local Policies\Audit Policy)
Implementing Auditing Using Group Policies

When you enable auditing, select only what you need because:

• High levels of auditing can affect the performance of the computer that you audit.
• When you search through the security logs, you will find far too many events, which can make it more difficult for you to find the potential problems you need to find.
• The logs quickly fill up, replacing older events with newer events.
## Audit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Explanation</th>
<th>Default Settings Defined for Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account logon</td>
<td>Determines whether the operating system (OS) audits each time the computer validates an account’s credentials, such as account logon. Account logon events are generated when a domain user account is authenticated on a domain controller.</td>
<td>Successful account logons</td>
</tr>
<tr>
<td>Account management</td>
<td>Determines whether to audit each event of account management on a computer including changing passwords and creating or deleting user accounts.</td>
<td>Successful account management activities</td>
</tr>
<tr>
<td>Directory service access</td>
<td>Determines whether the OS audits user attempts to access Active Directory objects, the previous change value, and the new assigned value.</td>
<td></td>
</tr>
</tbody>
</table>
## Audit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Explanation</th>
<th>Default Settings Defined for Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon</td>
<td>Determines where the OS audits each instance of a user attempting to log on to or log off his or her computer. Logon events are generated when a domain user interactively logs on to a domain controller or a network logon to a domain controller is performed to retrieve logon scripts and policies.</td>
<td>Successful logons</td>
</tr>
<tr>
<td>Object access</td>
<td>Determines whether the OS audits user attempts to access non-Active Directory objects including NT File System (NTFS) files, folders, and printers.</td>
<td></td>
</tr>
<tr>
<td>Policy change</td>
<td>Determines whether the OS audits each instance of an attempt to change user rights assignments, auditing policies, account policies, or trust policies.</td>
<td>Successful policy changes</td>
</tr>
</tbody>
</table>
# Audit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Explanation</th>
<th>Default Settings Defined for Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege use</td>
<td>Determines whether to audit each instance of a user exercising a user right.</td>
<td></td>
</tr>
<tr>
<td>Process tracking</td>
<td>Determines whether the OS audits process-related events such as process creation, process termination, handle duplication, and indirect object access. This is usually used for troubleshooting, because enabling the auditing of process tracking can affect performance.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Determines whether the OS audits if the system time is changed, if the system is started or shut down, if there is an attempt to load extensible authentication components, if there is a loss of auditing events due to auditing system failure, and if the security log exceeds a configurable warning threshold level.</td>
<td>Successful system events</td>
</tr>
</tbody>
</table>
Implementing Auditing Using Group Policies

• After you enable logging, open the Event Viewer security logs to view the security events.

• Most major Active Directory events are already audited although there is not a group policy that includes these settings.
Implementing an Audit Policy

Enabling auditing using group policies
Object Access Auditing Using Group Policies

Auditing NTFS files, NTFS folders, and printers is a two-step process:
1. Enable object access using Group Policy.
2. Specify which objects you want to audit.
Audit Files and Folders

Viewing the Security tab
Audit Files and Folders

Displaying the Advanced Security Settings for Updates dialog box
Audit Files and Folders

Using the Auditing tab

<table>
<thead>
<tr>
<th>Name:</th>
<th>C:\Pics\Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner:</td>
<td>Administrators (CONTOSO\Administrators)</td>
</tr>
</tbody>
</table>

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
</table>

[Add]  [Remove]  [View]

[Disable inheritance]

Replace all child object auditing entries with inheritable auditing entries from this object

[OK]  [Cancel]  [Apply]
Audit Files and Folders

Displaying the Auditing Entry for Updates dialog box
Audit Files and Folders

Opening the Select User, Computer, Service Account, or Group dialog box
Audit Printer Events

Selecting the Security tab in the Printer Properties dialog box
Audit Printer Events

Opening the Advanced Security Settings for Microsoft XPS Document Writer dialog box

© 2013 John Wiley & Sons, Inc.
Audit Printer Events

Selecting the Auditing tab
Audit Printer Events

Opening the Auditing Entry for Microsoft XPS Document Writer dialog box
Advanced Audit Policy Settings—Group Policies

To access a new policy, open **Group Policy Editor** for a group policy and go to **Configuration\Policies \Windows Settings\Security Settings\Advanced Audit Policy Configuration**.
Implementing Auditing Using AuditPol.exe

The syntax for AuditPol.exe includes:

• `/get`: Displays the current audit policy.
• `/set`: Sets the audit policy.
• `/list`: Displays selectable policy elements.
• `/backup`: Saves the audit policy to a file.
• `/restore`: Restores the audit policy from a file that was previously created by using auditpol /backup.
Implementing Auditing Using AuditPol.exe

The syntax for AuditPol.exe includes (continued):

- `/clear`: Clears the audit policy.
- `/remove`: Removes all per-user audit policy settings and disables all system audit policy settings.
- `/resourceSACL`: Configures global resource SACLs.
- `/?`: Displays help at the command prompt.
Auditpol.exe

Subcommands

- /user:<username>
- /category:<name>
- /subcategory:<name>
- /success:enable
- /success:disable
- /failure:enable
- /failure:disable
- /file
Auditpol.exe Examples

• To configure auditing for user account management for successful and failed attempts:

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

• To remove the per-user audit policy for the jsmith account:

  auditpol.exe /remove /user:jsmith
Viewing Audit Events

Opening security logs in the Event Viewer
Viewing Audit Events

Filtering security events
Creating Expression-Based Audit Policies

• **Global Object Access Auditing** lets you define computer-wide system access control lists for either the file system or registry.

• Is an alternative to manually altering and maintaining SACLs.
Displaying the Global Object Access Auditing settings
Define Global Object Access Auditing

Displaying the File system Properties dialog box
Define Global Object Access Auditing

Displaying the Auditing Entry for Global File SACL dialog box
Define Global Object Access Auditing

Adding a condition
Define Global Object Access Auditing

Specifying the conditions
Removable Storage Access Policy

• Earlier versions of the Windows and Windows Server operating systems didn't enable administrators to track the use of removable storage devices.

• Posed a security liability.

• Use the **Removable Storage Access policy** to limit or deny users the ability to use removable storage devices.
Configure the Monitoring of Removable Storage Devices

Opening the Audit Removable Storage Properties dialog box
Configure the Monitoring of Removable Storage Devices

Displaying a 4663 Event

<table>
<thead>
<tr>
<th>Log Name:</th>
<th>Security:</th>
<th>Source:</th>
<th>Logged:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID:</td>
<td>4663</td>
<td>Microsoft Windows security</td>
<td>8/19/2012 9:04:05 PM</td>
</tr>
<tr>
<td>Level:</td>
<td>Information</td>
<td>Task Category: Removable Storage</td>
<td></td>
</tr>
<tr>
<td>User:</td>
<td>N/A</td>
<td>Keywords: Audit Success</td>
<td></td>
</tr>
<tr>
<td>More Information:</td>
<td>Event Log Online Help</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An attempt was made to access an object.
Subject: Security ID: SYSTEM, Account Name: WIN2012SRV\$, Account Domain: CONTOSO, Logon ID: 0:3E7
Lesson Summary

• Enable auditing so that you can have a record of the users who have logged in, what the user accessed or tried to access, and what action a user has performed such as rebooting or shutting down a computer or accessing a file.

• To enable auditing, specify what types of system events to audit using Group Policy or the local security policy (Computer Settings\Policies\Security Settings\Local Policies\Audit Policy).

• Auditing NTFS files, NTFS folders, and printers is a two-step process. You must first enable Object Access using Group Policy. Then you must specify which objects you want to audit.

• Advanced Security Audit Policy Settings give you more control over what events get recorded by using 56 new settings instead of the traditional nine basic audit settings.
Lesson Summary

• It is not recommended you use both basic audit policy settings and Advanced Audit Policy Configuration because they can cause unexpected results.
• The AuditPol.exe command displays information about and performs functions to manipulate audit policies.
• The audit events can be viewed by opening the security logs in the Event Viewer.
• Global Object Access Auditing lets you define computer-wide system access control lists for either the file system or registry.
• Organizations can limit or deny users the ability to use removable storage devices by using the Removable Storage Access policy.
Copyright 2013 John Wiley & Sons, Inc.
All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.