Lesson 7: Configure Advanced Audit Policies

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

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

Event	***Explanation***	***Default Settings Defined for Domain Controllers***
Account logon	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.	Successful account logons
Account management	Determines whether to audit each event of account management on a computer including changing passwords and creating or deleting user accounts.	Successful account management activities
Directory service access	Determines whether the OS audits user attempts to access Active Directory objects, the previous change value, and the new assigned value.	

Audit Events

Event	***Explanation***	***Default Settings Defined for Domain Controllers***
Logon	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.	Successful logons
Object access	Determines whether the OS audits user attempts to access non-Active Directory objects including NT File System (NTFS) files, folders, and printers.	
Policy change	Determines whether the OS audits each instance of an attempt to change user rights assignments, auditing policies, account policies, or trust policies.	Successful policy changes

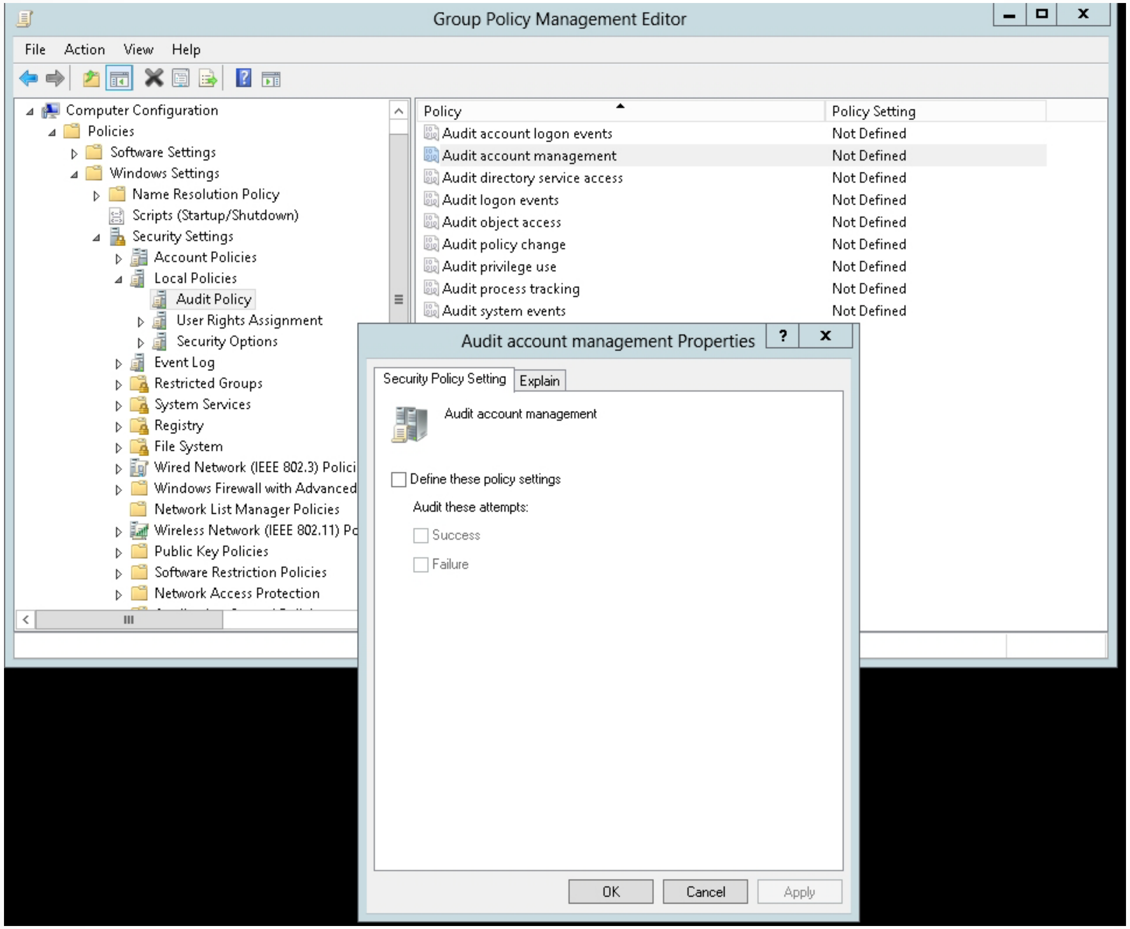
Audit Events

Event	***Explanation***	***Default Settings Defined for Domain Controllers***
Privilege use	Determines whether to audit each instance of a user exercising a user right.	
Process tracking	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.	
System	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.	Successful system events

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



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Polici
        - Windows Firewall with Advanced
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Po
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection

Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Audit account management

□ Define these policy settings

Audit these attempts:

□ Success

□ Failure

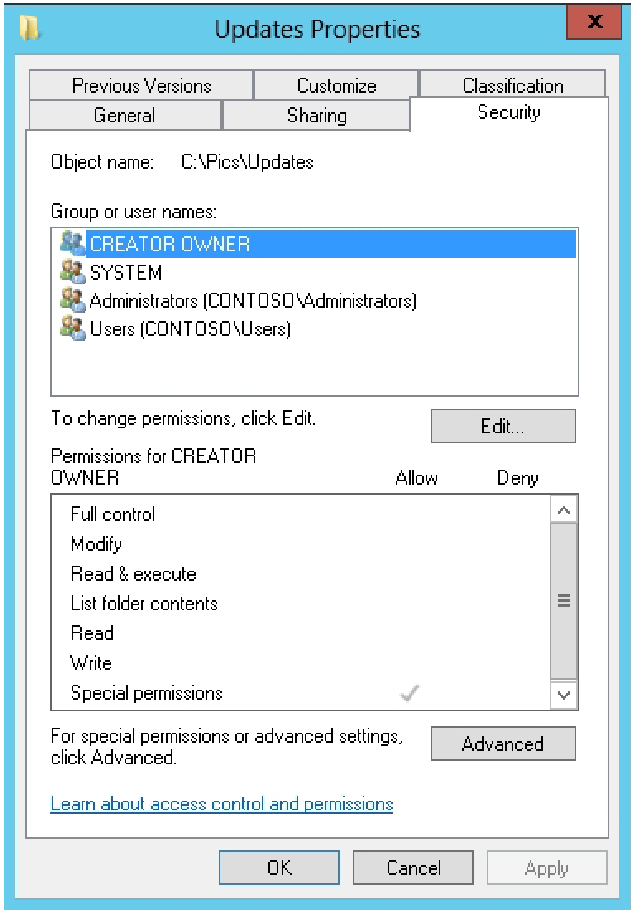
Enabling auditing using group policies

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



Object name: C:\Pics\Updates

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (CONTOSO\Administrators)
- Users (CONTOSO\Users)

To change permissions, click Edit.

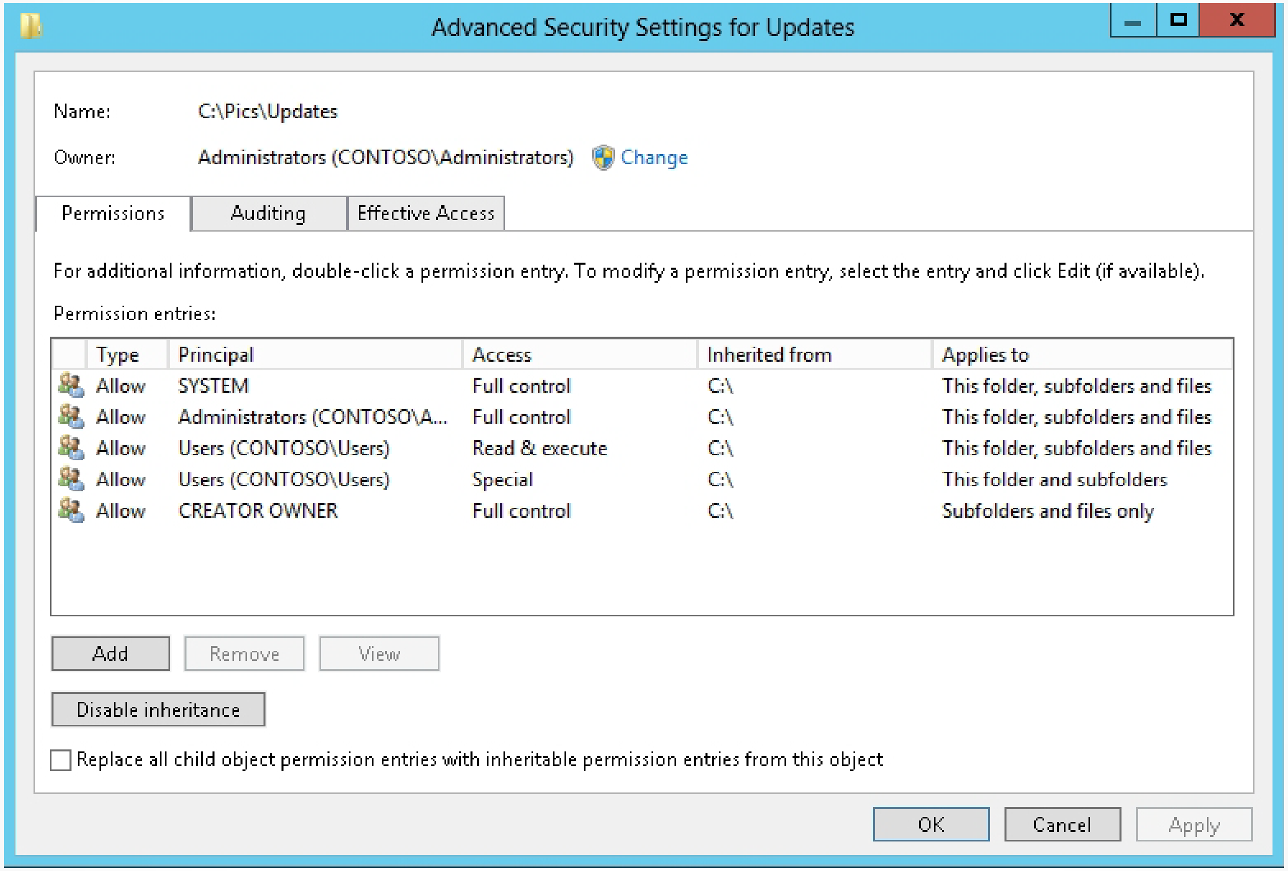
Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Viewing the Security tab

Audit Files and Folders



Advanced Security Settings for Updates

Name: C:\Pics\Updates

Owner: Administrators (CONTOSO\Administrators) Change

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

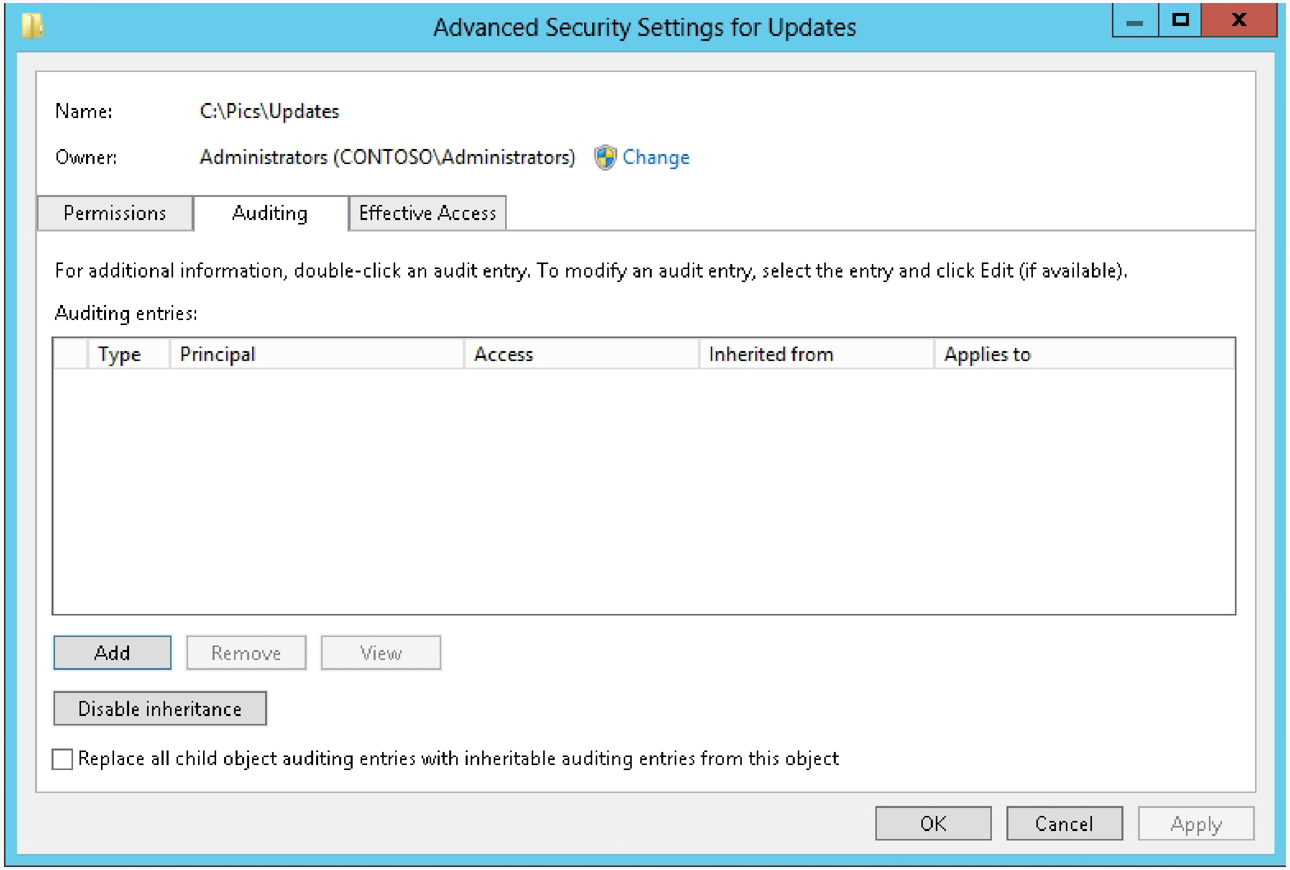
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (CONTOSO\A...	Full control	C:\	This folder, subfolders and files
Allow	Users (CONTOSO\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (CONTOSO\Users)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

□ Replace all child object permission entries with inheritable permission entries from this object

Displaying the Advanced Security Settings for Updates dialog box

Audit Files and Folders



Advanced Security Settings for Updates

Name: C:\Pics\Updates

Owner: Administrators (CONTOSO\Administrators) Change

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

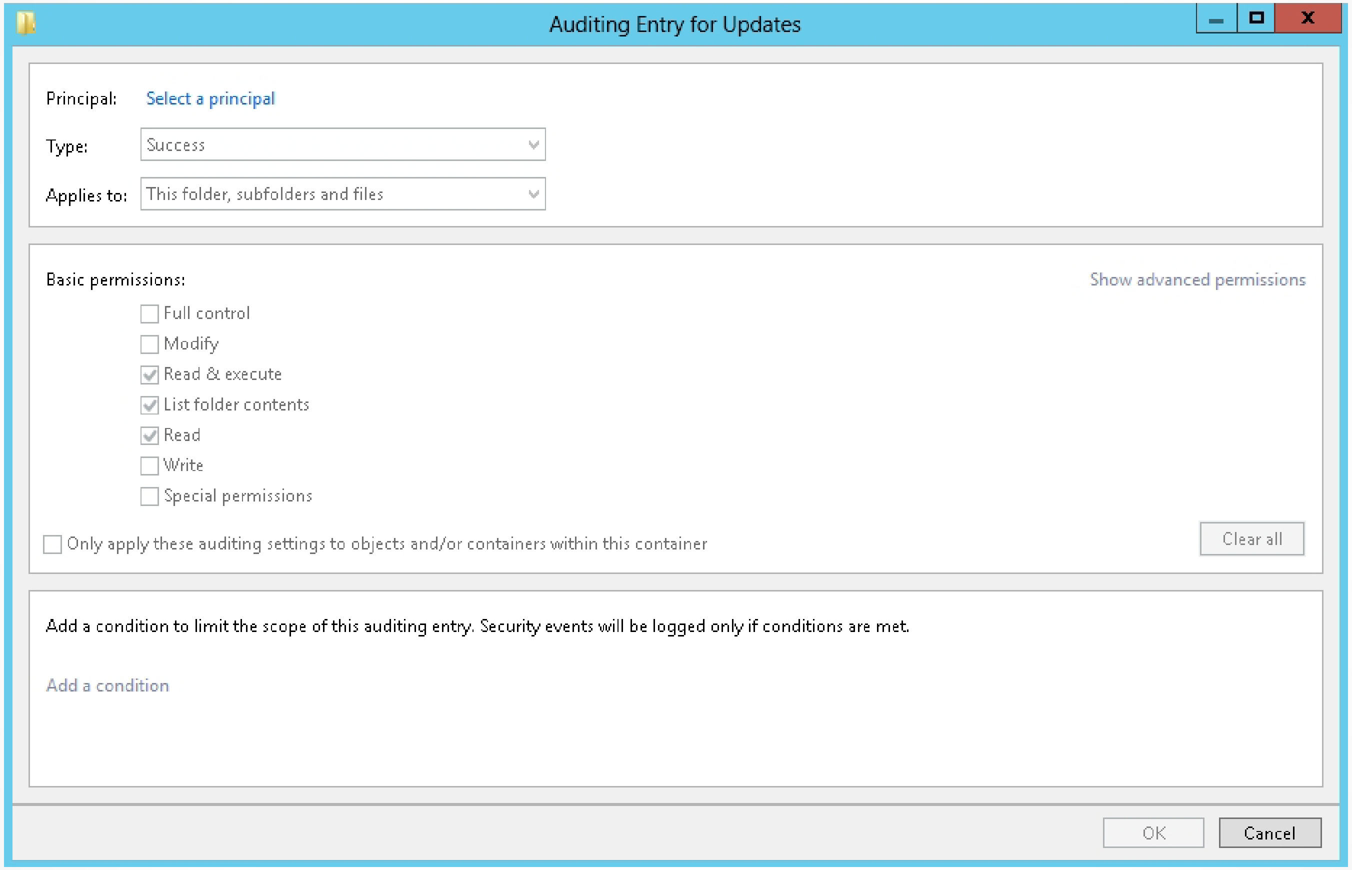
Auditing entries:

Type	Principal	Access	Inherited from	Applies to

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

Using the Auditing tab

Audit Files and Folders



Auditing Entry for Updates

Principal: Select a principal

Type: Success

Applies to: This folder, subfolders and files

Basic permissions:

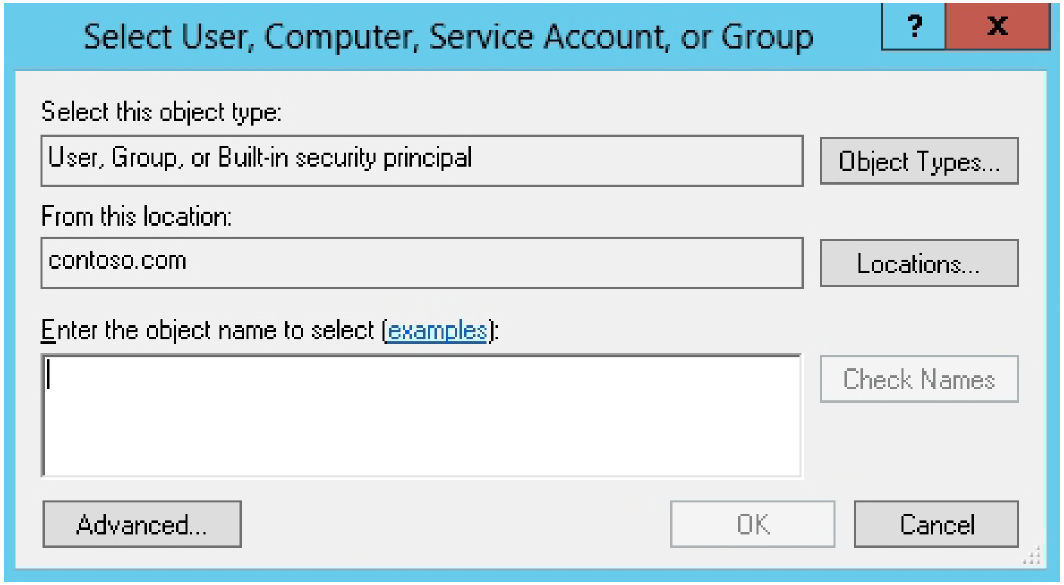
- □ Full control
- □ Modify
- ☑ Read & execute
- ☑ List folder contents
- ☑ Read
- □ Write
- □ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Displaying the Auditing Entry for Updates dialog box

Audit Files and Folders



Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

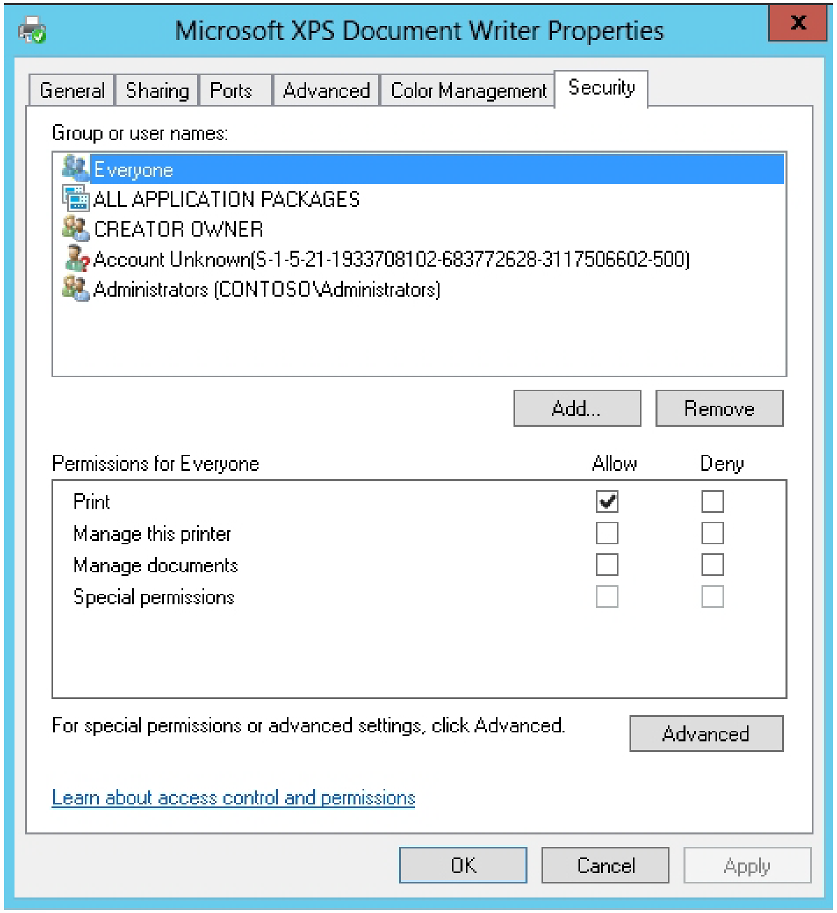
From this location:

contoso.com

Enter the object name to select (examples):

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

Audit Printer Events



Microsoft XPS Document Writer Properties

Group or user names:

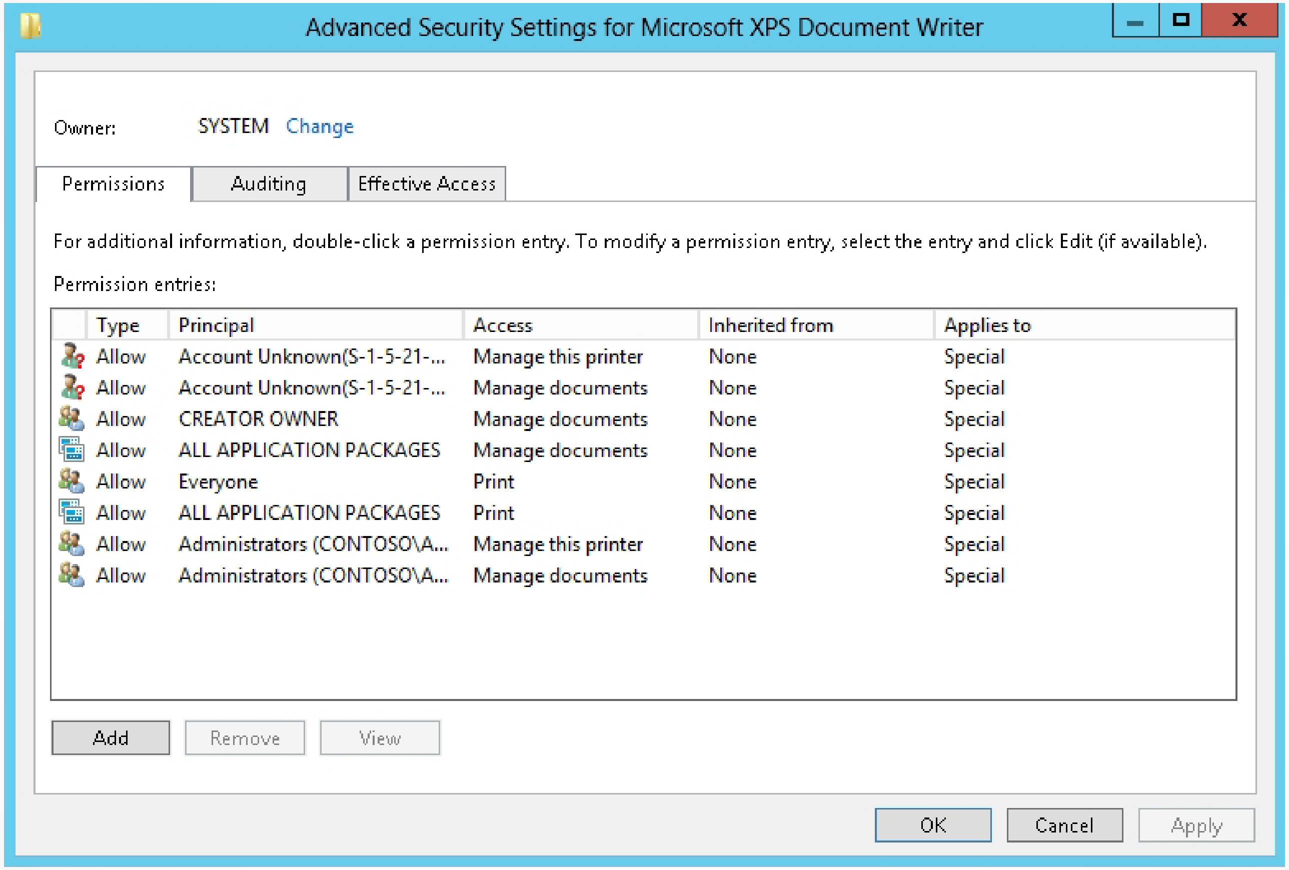
- Everyone
- ALL APPLICATION PACKAGES
- CREATOR OWNER
- Account Unknown(S-1-5-21-1933708102-683772628-3117506602-500)
- Administrators (CONTOSO\Administrators)

Permissions for Everyone	Allow	Deny
Print	☑	□
Manage this printer	□	□
Manage documents	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Selecting the Security tab in the Printer Properties dialog box

Audit Printer Events



Advanced Security Settings for Microsoft XPS Document Writer

Owner: SYSTEM

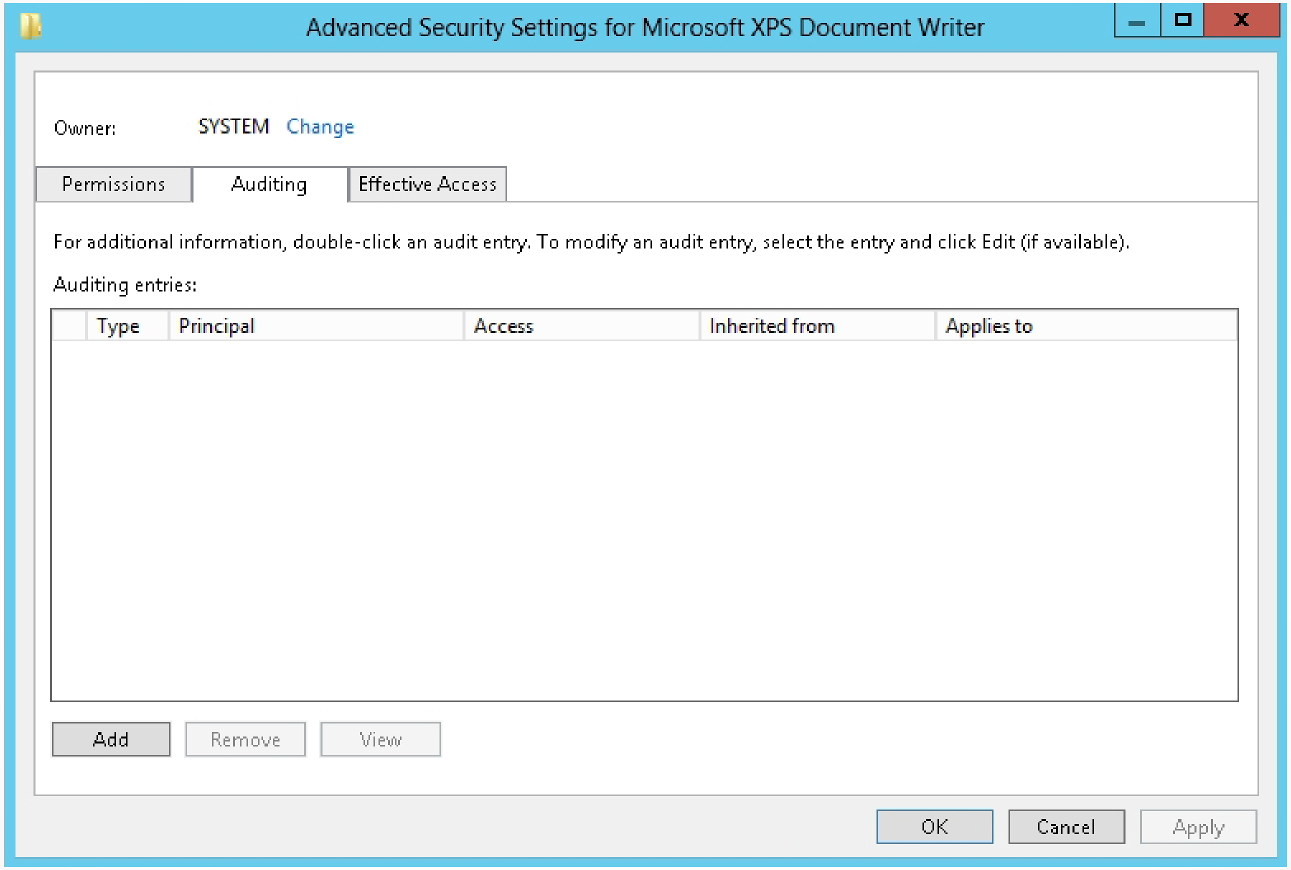
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Account Unknown(S-1-5-21-...	Manage this printer	None	Special
Allow	Account Unknown(S-1-5-21-...	Manage documents	None	Special
Allow	CREATOR OWNER	Manage documents	None	Special
Allow	ALL APPLICATION PACKAGES	Manage documents	None	Special
Allow	Everyone	Print	None	Special
Allow	ALL APPLICATION PACKAGES	Print	None	Special
Allow	Administrators (CONTOSO\A...	Manage this printer	None	Special
Allow	Administrators (CONTOSO\A...	Manage documents	None	Special

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

Audit Printer Events


Advanced Security Settings for Microsoft XPS Document Writer

Owner: SYSTEM Change

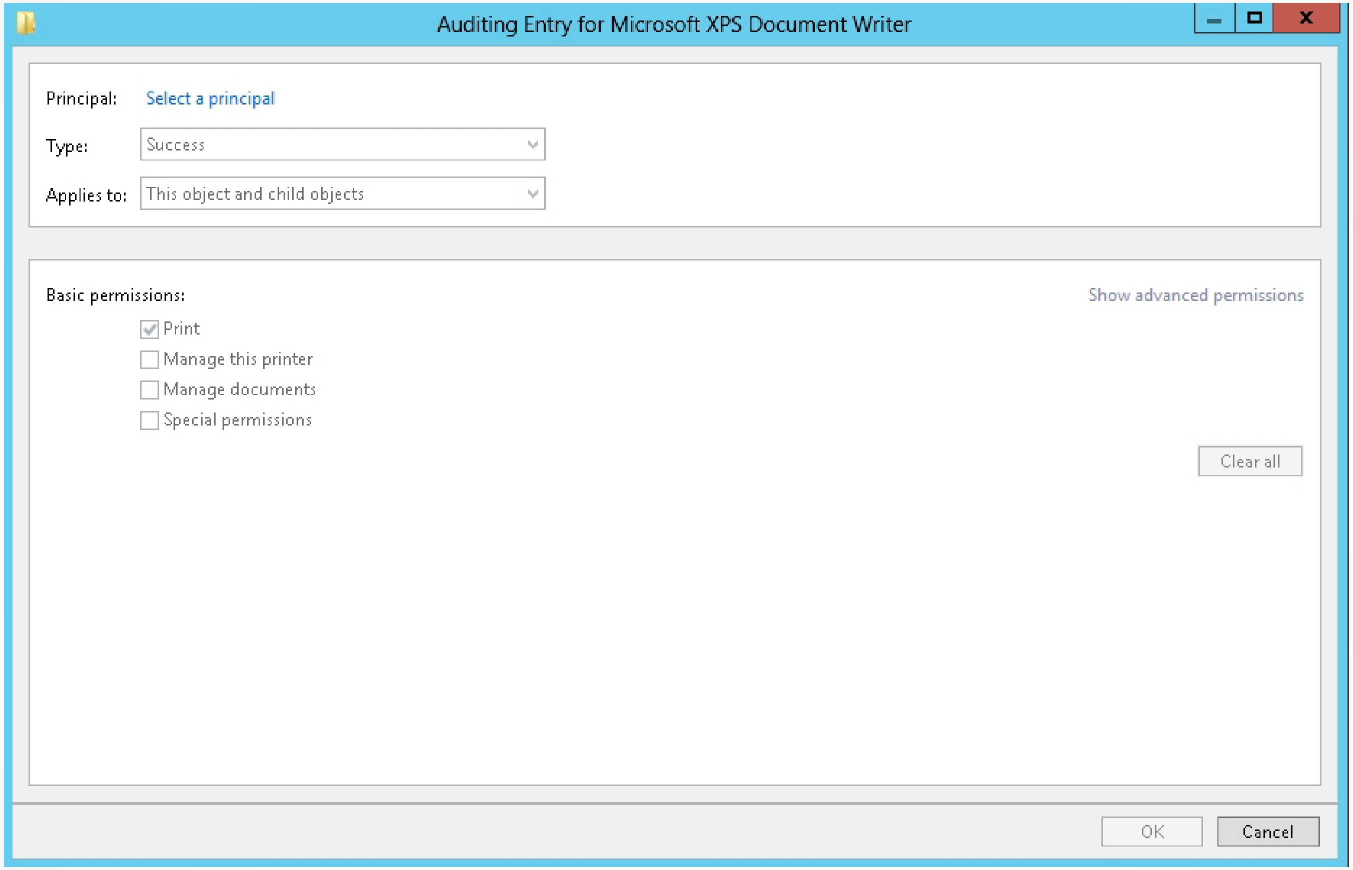
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

	Type	Principal	Access	Inherited from	Applies to

Selecting the Auditing tab

Audit Printer Events



Auditing Entry for Microsoft XPS Document Writer

Principal: Select a principal

Type: Success

Applies to: This object and child objects

Basic permissions:

☑ Print

□ Manage this printer

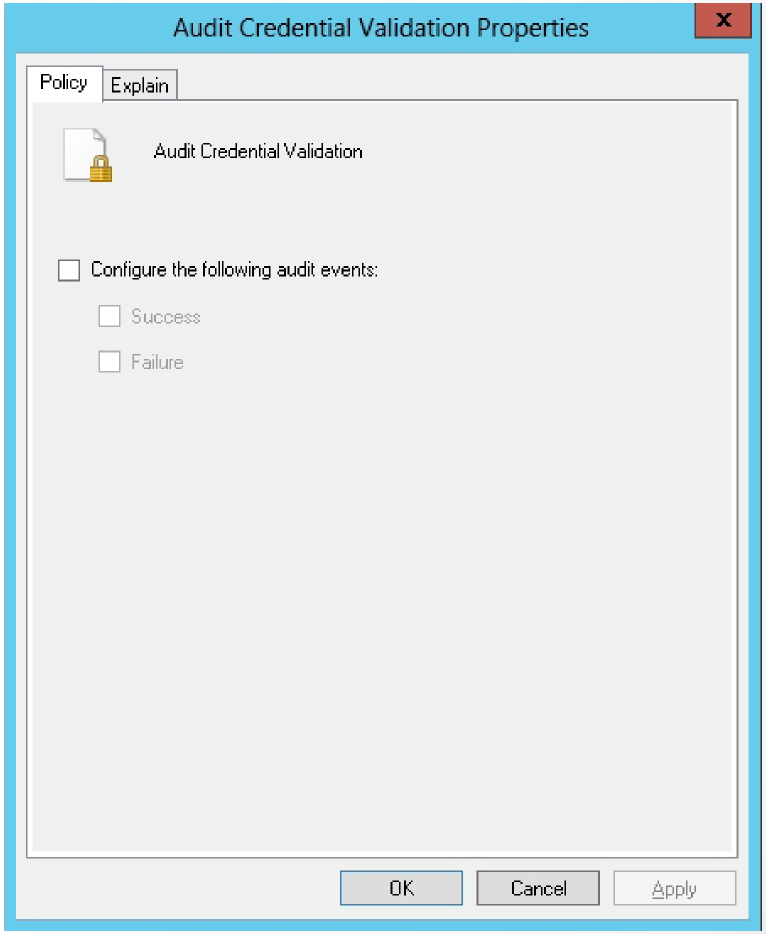
□ Manage documents

□ Special permissions

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.*


Audit Credential Validation Properties

Audit Credential Validation

□ Configure the following audit events:

□ Success

□ Failure

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

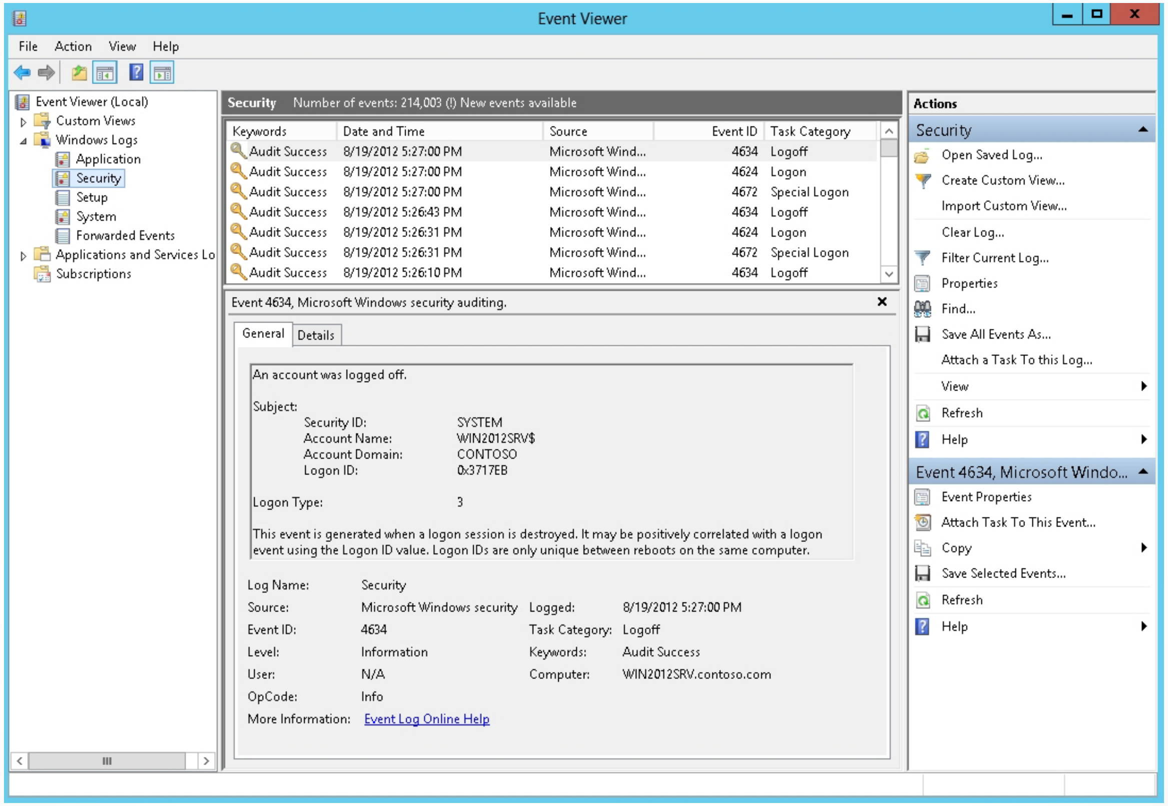
- To configure auditing for user account management for successful and failed attempts:

```
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



Security Number of events: 214,003 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/19/2012 5:27:00 PM	Microsoft Wind...	4634	Logoff
Audit Success	8/19/2012 5:27:00 PM	Microsoft Wind...	4624	Logon
Audit Success	8/19/2012 5:27:00 PM	Microsoft Wind...	4672	Special Logon
Audit Success	8/19/2012 5:26:43 PM	Microsoft Wind...	4634	Logoff
Audit Success	8/19/2012 5:26:31 PM	Microsoft Wind...	4624	Logon
Audit Success	8/19/2012 5:26:31 PM	Microsoft Wind...	4672	Special Logon
Audit Success	8/19/2012 5:26:10 PM	Microsoft Wind...	4634	Logoff

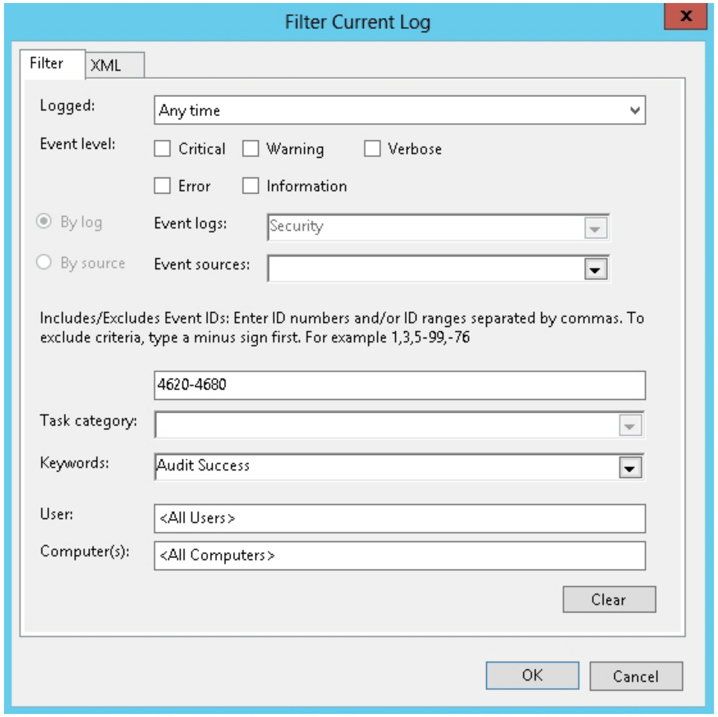
Event 4634, Microsoft Windows security auditing.

```
An account was logged off.

Subject:
        Security ID:            SYSTEM
        Account Name:           WIN2012SRV$
        Account Domain:         CONTOSO
        Logon ID:               0x3717EB

Logon Type:                     3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon
event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8/19/2012 5:27:00 PM
Event ID:          4634                         Task Category:   Logoff
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN2012SRV.contoso.com
OpCode:            Info
More Information:  Event Log Online Help
```

Opening security logs in the Event Viewer

Viewing Audit Events



Filter Current Log

Logged: Any time

Event level: □ Critical □ Warning □ Verbose

□ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4620-4680

Task category:

Keywords: Audit Success

User: <All Users>

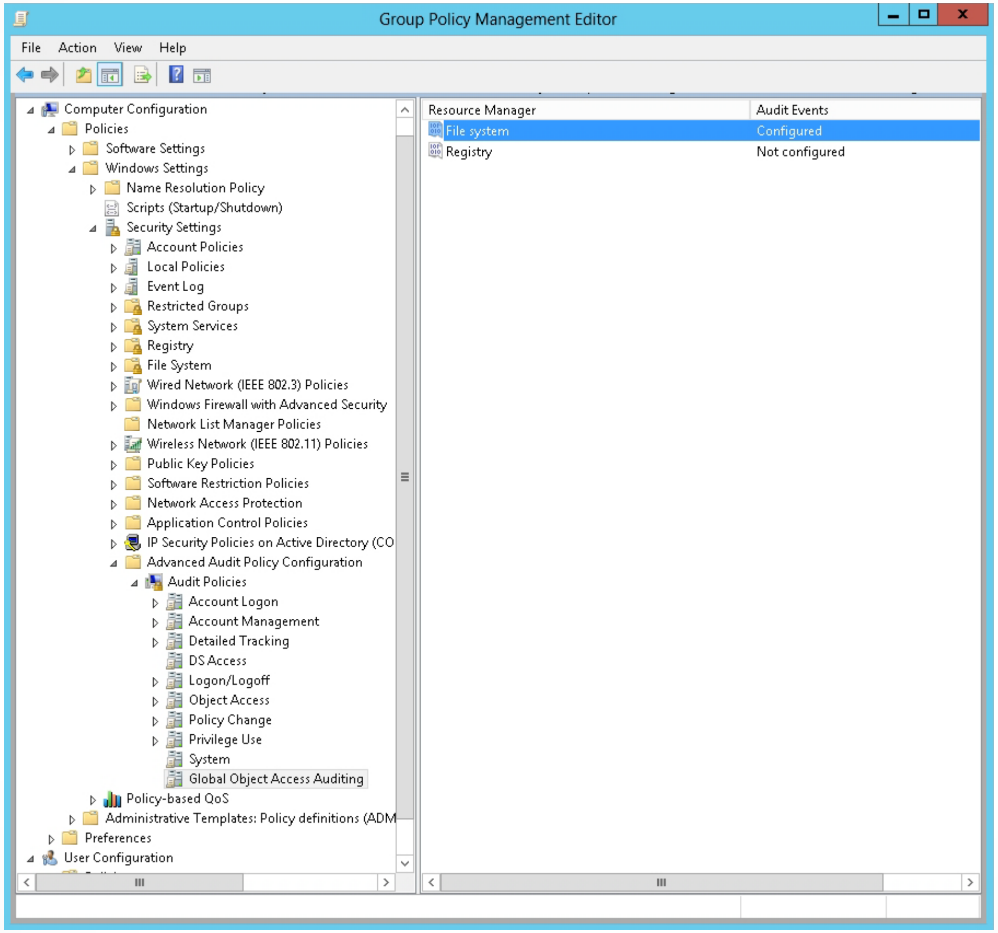
Computer(s): <All Computers>

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.

Define Global Object Access Auditing

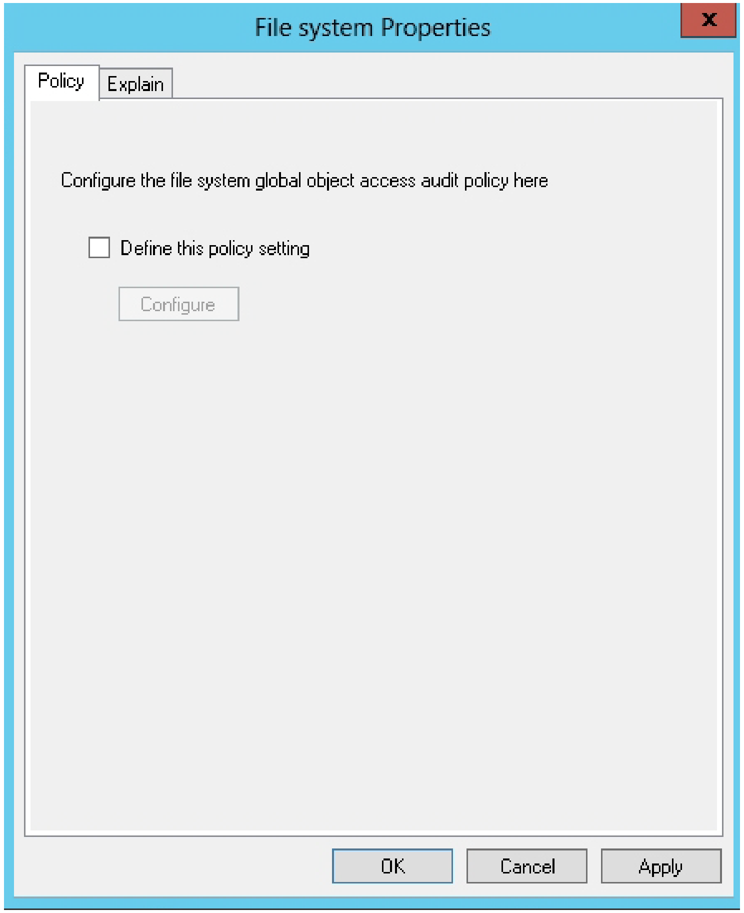


- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - Application Control Policies
        - IP Security Policies on Active Directory (CO
        - Advanced Audit Policy Configuration
          - Audit Policies
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System
            - Global Object Access Auditing
      - Policy-based QoS
    - Administrative Templates: Policy definitions (ADM
  - Preferences
- User Configuration

Resource Manager	Audit Events
File system	Configured
Registry	Not configured

Displaying the Global Object Access Auditing settings

Define Global Object Access Auditing

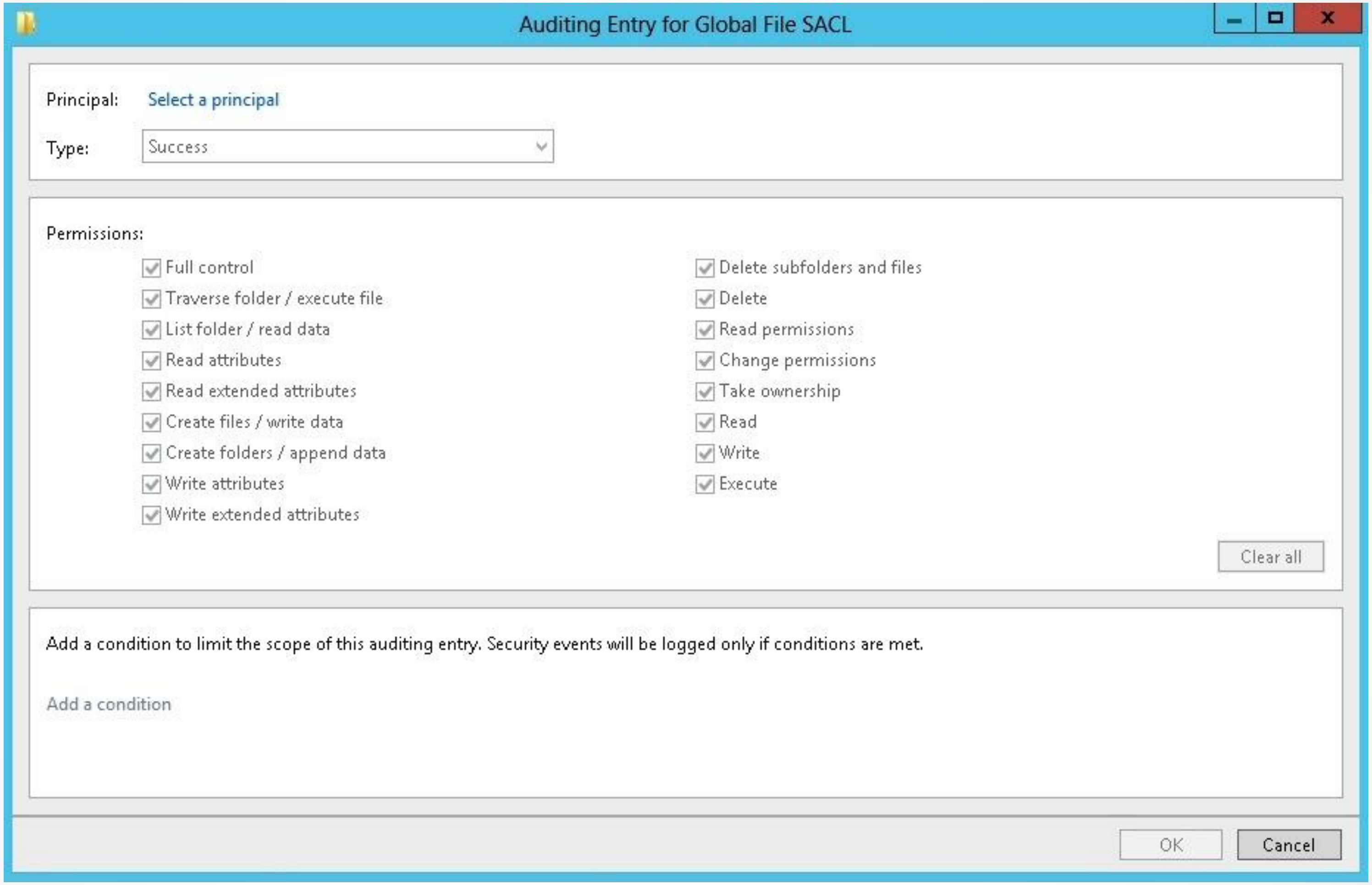


Configure the file system global object access audit policy here

☐ Define this policy setting

Displaying the File system Properties dialog box

Define Global Object Access Auditing



Principal: Select a principal

Type: Success

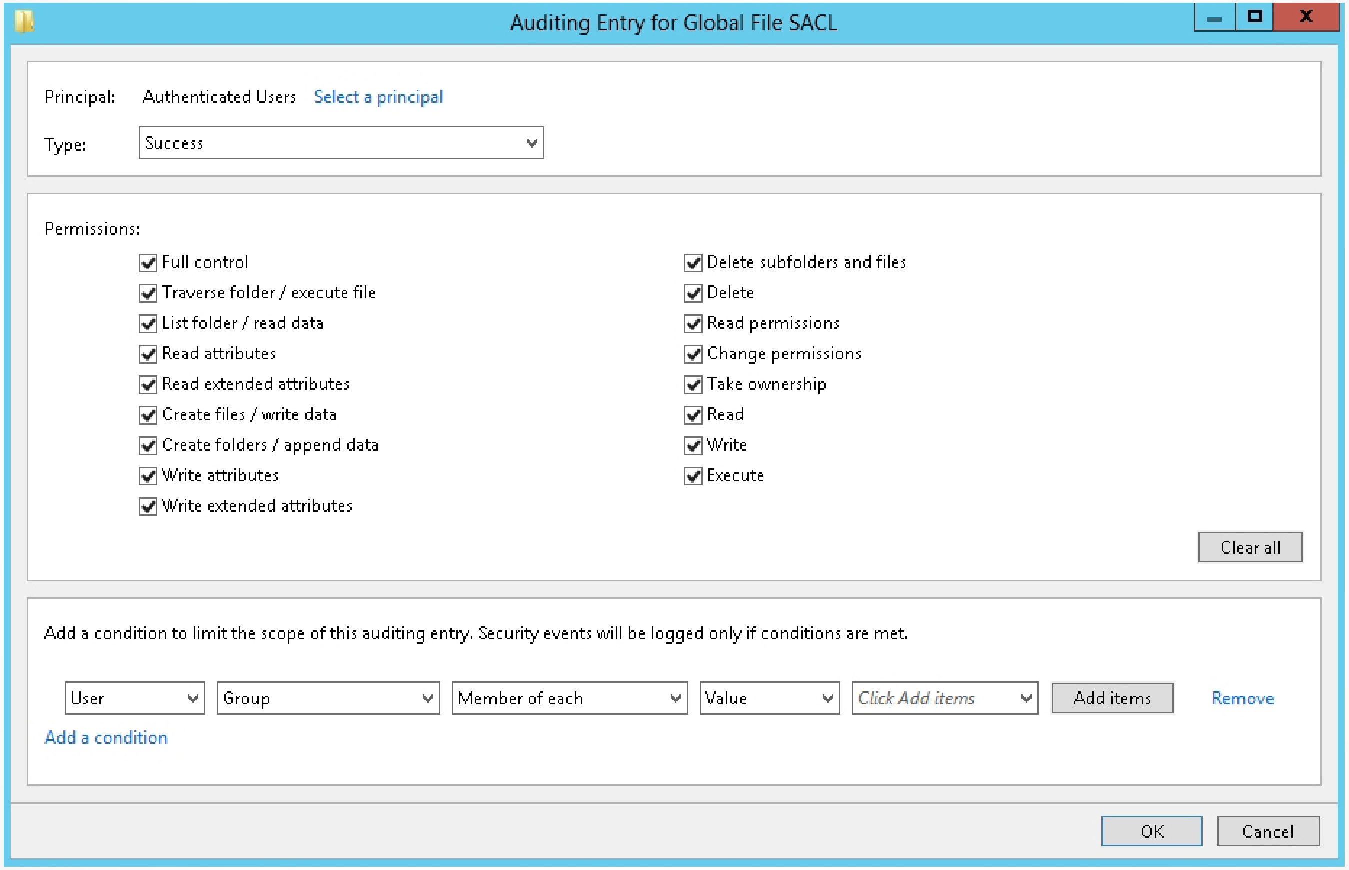
Permissions:

- ☑ Full control
- ☑ Traverse folder / execute file
- ☑ List folder / read data
- ☑ Read attributes
- ☑ Read extended attributes
- ☑ Create files / write data
- ☑ Create folders / append data
- ☑ Write attributes
- ☑ Write extended attributes
- ☑ Delete subfolders and files
- ☑ Delete
- ☑ Read permissions
- ☑ Change permissions
- ☑ Take ownership
- ☑ Read
- ☑ Write
- ☑ Execute

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Displaying the Auditing Entry for Global File SACL dialog box

Define Global Object Access Auditing



Principal: Authenticated Users Select a principal

Type: Success

Permissions:

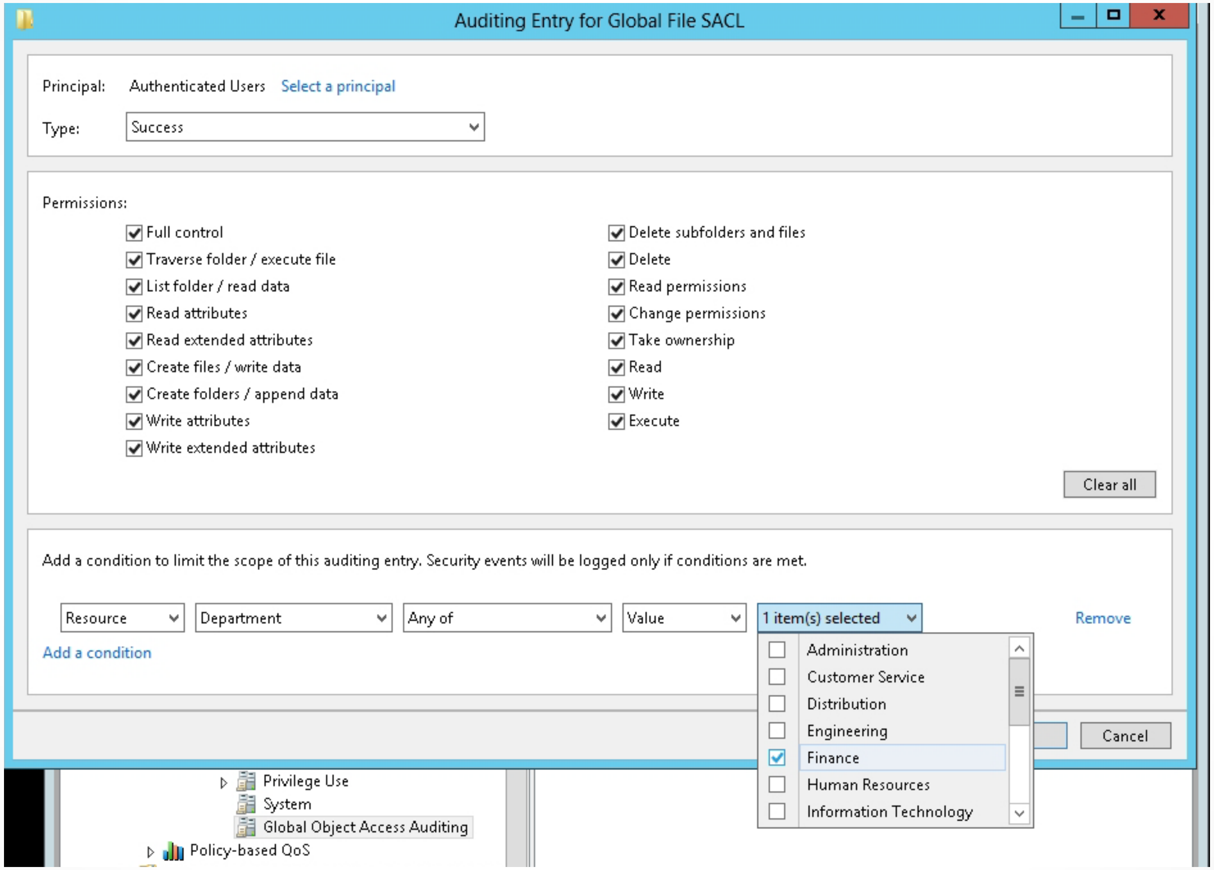
- ☑ Full control
- ☑ Traverse folder / execute file
- ☑ List folder / read data
- ☑ Read attributes
- ☑ Read extended attributes
- ☑ Create files / write data
- ☑ Create folders / append data
- ☑ Write attributes
- ☑ Write extended attributes
- ☑ Delete subfolders and files
- ☑ Delete
- ☑ Read permissions
- ☑ Change permissions
- ☑ Take ownership
- ☑ Read
- ☑ Write
- ☑ Execute

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

User | Group | Member of each | Value | Click Add items

Adding a condition

Define Global Object Access Auditing



Auditing Entry for Global File SACL

Principal: Authenticated Users Select a principal

Type: Success

Permissions:

- ☑ Full control
- ☑ Traverse folder / execute file
- ☑ List folder / read data
- ☑ Read attributes
- ☑ Read extended attributes
- ☑ Create files / write data
- ☑ Create folders / append data
- ☑ Write attributes
- ☑ Write extended attributes
- ☑ Delete subfolders and files
- ☑ Delete
- ☑ Read permissions
- ☑ Change permissions
- ☑ Take ownership
- ☑ Read
- ☑ Write
- ☑ Execute

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Resource | Department | Any of | Value | 1 item(s) selected

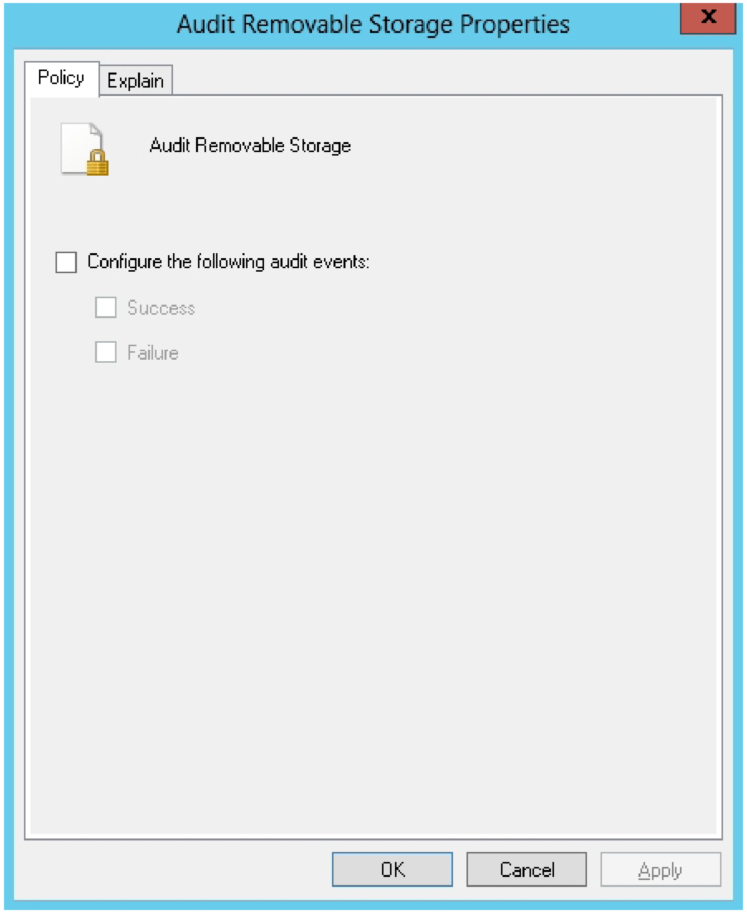
- □ Administration
- □ Customer Service
- □ Distribution
- □ Engineering
- ☑ Finance
- □ Human Resources
- □ Information Technology

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


Audit Removable Storage Properties

Audit Removable Storage

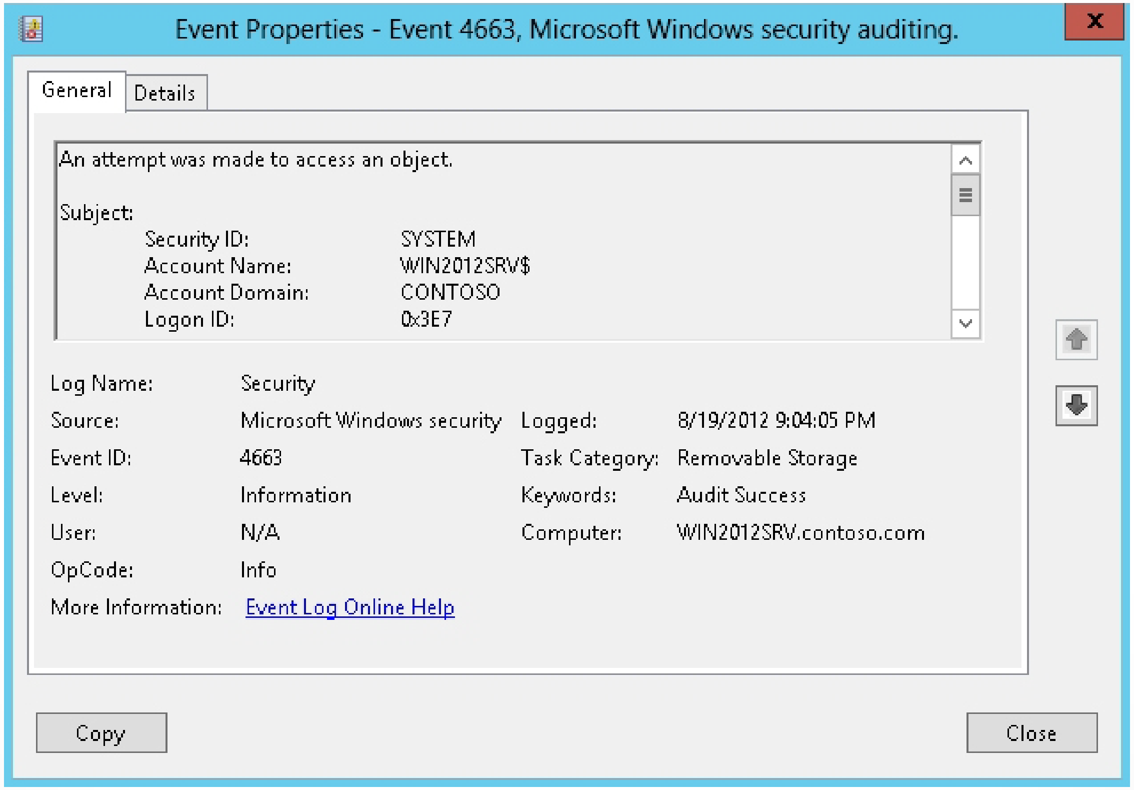
□ Configure the following audit events:

□ Success

□ Failure

Opening the Audit Removable Storage Properties dialog box

Configure the Monitoring of Removable Storage Devices



Event Properties - Event 4663, Microsoft Windows security auditing.
General
Details

An attempt was made to access an object.

```
Subject:
        Security ID:            SYSTEM
        Account Name:           WIN2012SRV$
        Account Domain:         CONTOSO
        Logon ID:               0x3E7
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/19/2012 9:04:05 PM
Event ID:	4663	Task Category:	Removable Storage
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN2012SRV.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

Displaying a 4663 Event

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.