

# Computer Audit Trails



- An *audit trail* is a series of records of computer events, about an operating system, an application, or user activities.
- A computer system may have several audit trails, each devoted to a particular type of activity.

**Source:** Computer Security Resource Center, NIST

<https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul1997-03.txt>

# Audits Logs Provide Nonrepudiation

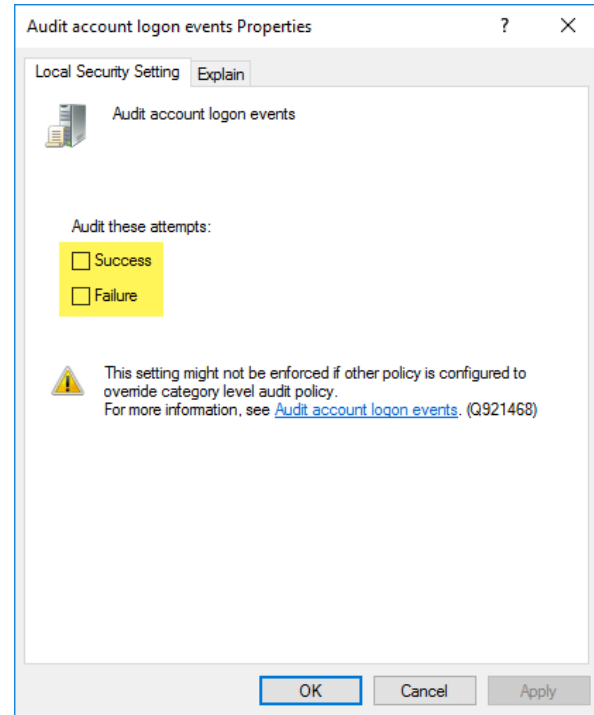


- **Nonrepudiation** is the assurance that someone cannot deny something.
- Logging events into audit logs provides nonrepudiation.

# Types of Audits



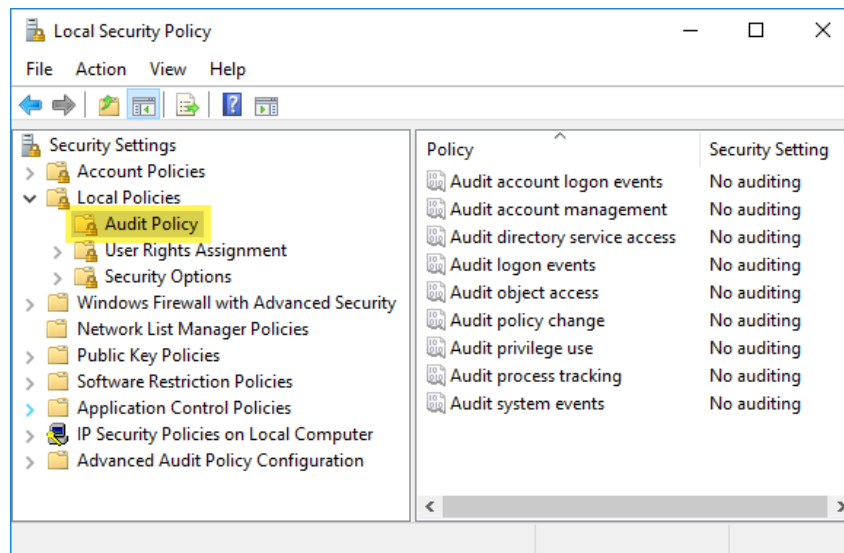
- We can audit the “success” or “failure” of an event.
- For example:
  - User Login Success
  - File Access Failure



# What Can Be Audited?



- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy Change
- Privilege Use
- Process Tracking
- Audit System Events



# Configuring Audits



## Local Security Policy

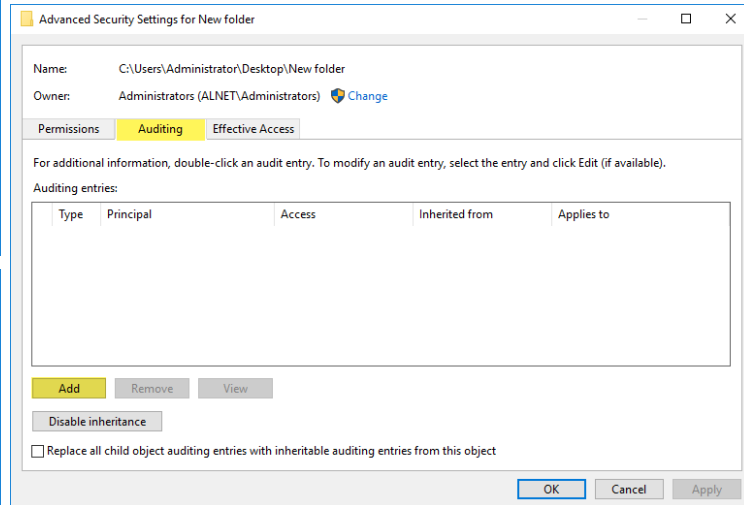
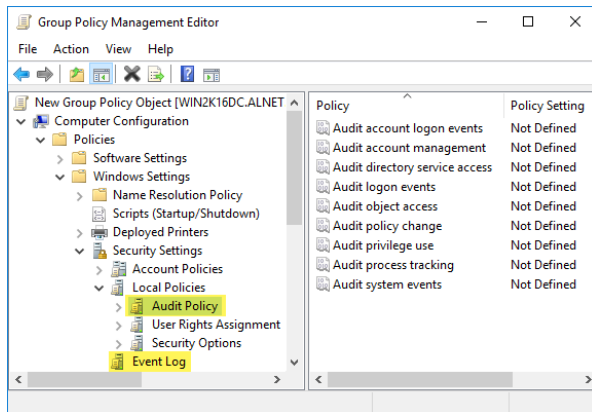
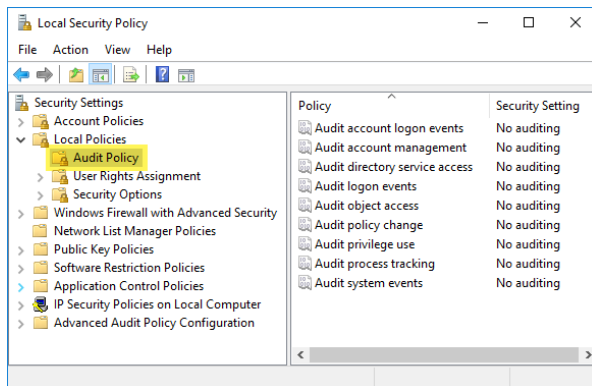
- Individual PCs

## Group Policy Management Editor

- AD Domain

## NTFS Advance Security Settings

- Individual Objects (files, folders, OUs, etc.)



# Viewing Audit Logs



The screenshot shows the Windows Event Viewer application. The left pane displays the navigation tree with 'Security' selected under 'Windows Logs'. The main pane shows a list of events with columns for Keywords, Date and Time, Source, Event ID, and Task Category. The right pane shows the 'Actions' menu with 'Event Properties' selected.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/28/2018 7:04:43 PM	Security-Auditing	4624	Special Logon
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management
Audit Success	12/28/2018 7:04:29 PM	Security-Auditing	4798	User Account Management

**Event 4672, Security-Auditing**

General Details

Special privileges assigned to new logon.

Subject:

Log Name: Security  
Source: Security-Auditing  
Event ID: 4672  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 12/28/2018 7:04:43 PM  
Task Category: Special Logon  
Keywords: Audit Success  
Computer: DESKTOP-4LBG7UF