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.

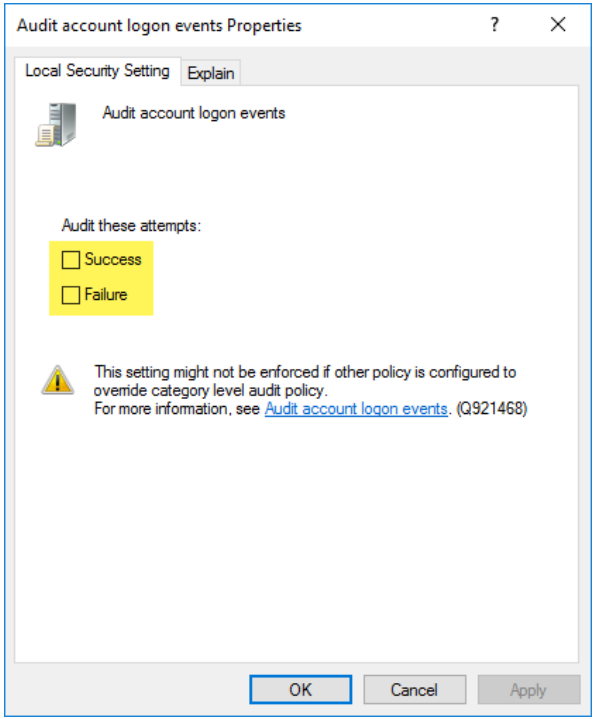
Source: Computer Security Resource Center, NIST
https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul1997-03.txt

Audits Logs Provide Nonrepudiation

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

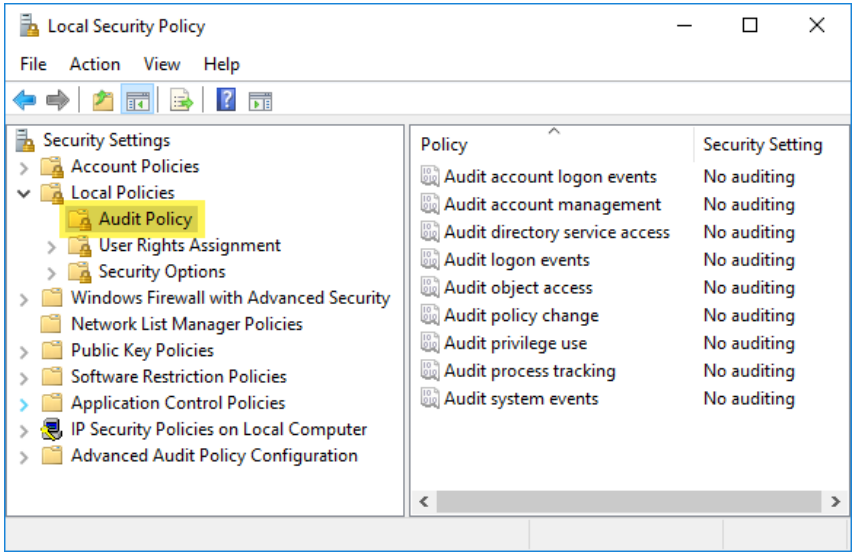
Types of Audits

- 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

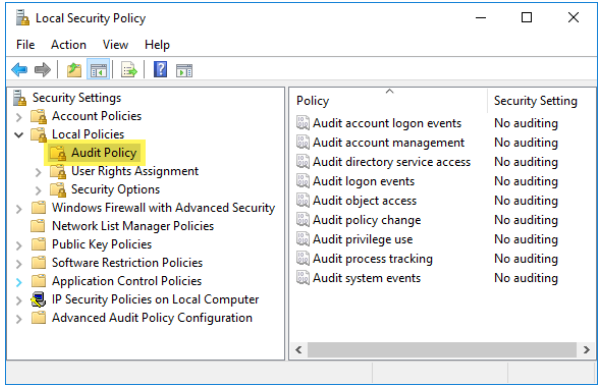


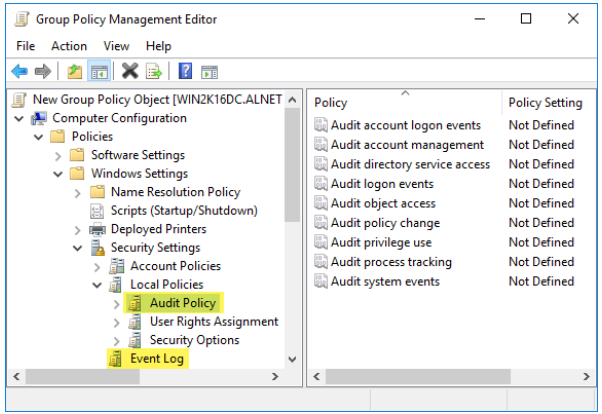
Configuring Audits

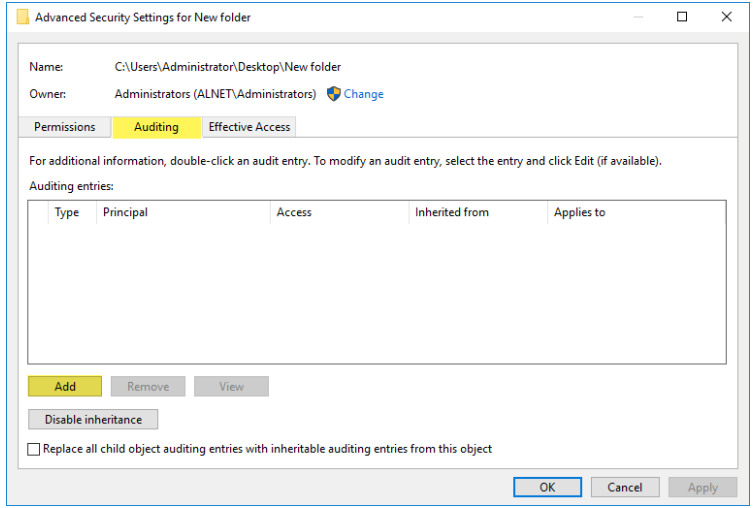
Local Security Policy
- Individual PCs

Group Policy Management Editor
- AD Domain

NTFS Advance Security Settings
- Individual Objects (files, folders, OUs, etc.)







Viewing Audit Logs