How to Enable & Trackdown user actions concerning files and folders access

It is important to audit all user actions concerning files and folders access. In this article, the process of enabling files and folders auditing on Windows Server Systems have been explained.

On Windows Server Systems, auditing file and folder accesses consists of two parts:

1. Enable File and Folder auditing which can be done in two ways:

a) Through Group Policy (for Domains, Sites and Organizational Units)
b) Local Security policy (for single Servers)

2. Track-down Events for File and Folders

---

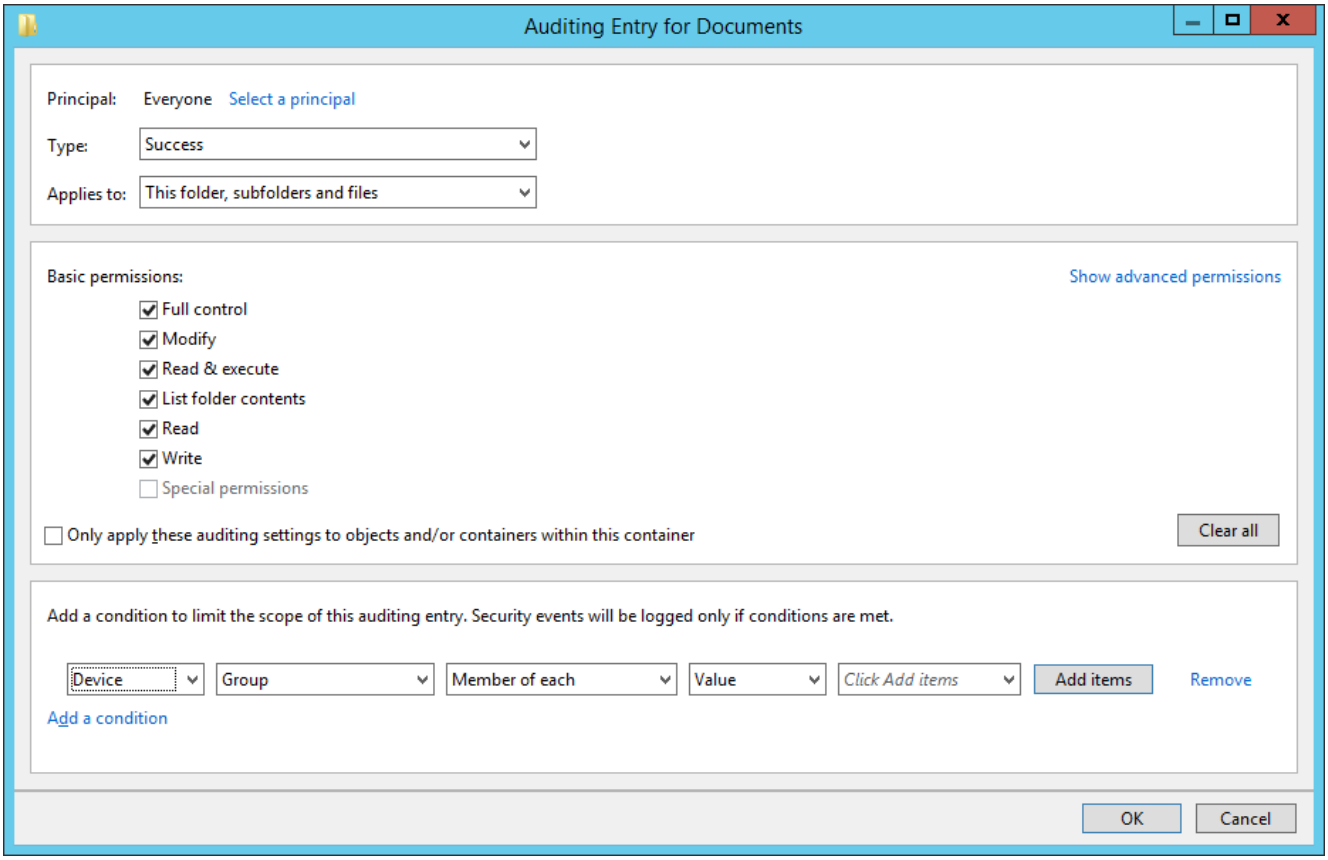
1 a. Enable Auditing through Group Policy

Run gpedit.msc, configure Default Domain Policy → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy → Audit object access → Define “Success and Failures”.
In the “Advanced Audit Policy Configuration” adjust Audit File System → Define “Success and Failures” and Audit Handle Manipulation → Define “Success and Failures”.

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

1 b. Enable Auditing of Specific Folder

Navigate to the file share, right-click it and select “Properties” → “Security” tab → “Advanced” button → “Auditing” tab → Click “Add” button Select Principal: “Everyone”; Select Type: “All”; Select Applies to: “This folder, subfolders and files”
Select the following “Advanced Permissions”: create files/write data, create folders/append data, write attributes, write extended attributes.



2. Trackdown Events for File and Folders

Event ID	Event Message
4656	A handle to an object was requested
4658	The handle to an object was closed
4660	An object was deleted
4663	An attempt was made to access an object
4685	The state of a transaction has changed
4985	The state of a transaction has changed