Auditing policy in Win server

You can apply audit policies to individual files and folders on your computer by setting the permission type to record successful access attempts or failed access attempts in the security log.

To complete this procedure, you must be signed in as a member of the built-in Administrators group or have **Manage auditing and security log** rights.

To apply or modify auditing policy settings for a local file or folder

1. Select and hold (or right-click) the file or folder that you want to audit, select **Properties**, and then select the **Security** tab.
2. Select **Advanced**.
3. In the **Advanced Security Settings** dialog box, select the **Auditing** tab, and then select **Continue**.
4. Do one of the following tasks:
    - To set up auditing for a new user or group, select **Add**. Select **Select a principal**, type the name of the user or group that you want, and then select **OK**.
    - To remove auditing for an existing group or user, select the group or user name, select **Remove**, select **OK**, and then skip the rest of this procedure.
    - To view or change auditing for an existing group or user, select its name, and then select **Edit.**
5. In the **Type** box, indicate what actions you want to audit by selecting the appropriate check boxes:
    - To audit successful events, select **Success.**
    - To audit failure events, select **Fail.**
    - To audit all events, select **All.**
6. In the **Applies to** box, select the object(s) to which the audit of events will apply. These objects include:
    - **This folder only**
    - **This folder, subfolders and files**
    - **This folder and subfolders**
    - **This folder and files**
    - **Subfolders and files only**
    - **Subfolders only**
    - **Files only**

7. By default, the selected **Basic Permissions** to audit are the following:
    - **Read and execute**
    - **List folder contents**
    - **Read**
    - Additionally, with your selected audit combination, you can select any combination of the following permissions:
        - **Full control**
        - **Modify**
        - **Write**