Creating, Editing, and Auditing a File in the "data1" Folder

This guide will walk you through the process of creating a file, editing it, and enabling auditing to track who accessed or modified the file in the "data1" folder.

# Step 1: Create the Folder "data1"

1. Open File Explorer.  
2. Navigate to the location where you want to create the folder (e.g., C:\).  
3. Right-click in the folder and select New > Folder.  
4. Name the folder "data1".

# Step 2: Create a File in the "data1" Folder

1. Navigate to the "data1" folder you created.  
2. Right-click inside the folder and select New > Text Document.  
3. Name the file "testfile.txt".  
4. Double-click "testfile.txt" to open it in Notepad.  
5. Type some content, such as:  
 This is a test file to monitor access and modifications.  
6. Save and close the file.

# Step 3: Enable Auditing for the "data1" Folder

1. Right-click on the "data1" folder and select Properties.  
2. Go to the Security tab and click Advanced.  
3. Click the Auditing tab, then click Add.  
4. Click Select a Principal, type Everyone (or specific users like Hirwa and Paddy), and click OK.  
5. Under Type, select Success and Failure.  
6. Check the following permissions to audit:  
 - Read (for access tracking)  
 - Write (for modification tracking)  
 - Delete (for deletion tracking)  
7. Click Apply and OK.

# Step 4: Edit the "testfile.txt" File

1. Right-click on testfile.txt and select Open.  
2. Modify the content of the file. For example:  
 This file has been modified to track access and modifications.  
3. Save and close the file.

# Step 5: Refresh Group Policy

To apply auditing policies, use one of the following methods:  
  
Method 1: Refresh via Group Policy Management Console (GPMC)  
1. Go to Group Policy Management.  
2. Right-click your domain (e.g., YourDomainName).  
3. Click Group Policy Update and confirm by clicking Yes.  
  
Method 2: Restart the Server  
1. Click Start Menu > Power > Restart.  
2. The policy changes will apply automatically after the server restarts.

# Step 6: View Audit Logs in Event Viewer

1. Open Server Manager.  
2. Click Tools and select Event Viewer.  
3. In Event Viewer, navigate to:  
 Windows Logs > Security  
4. Look for the following Event IDs:  
 - 4624 → Successful login  
 - 4625 → Failed login attempt (this is crucial for auditing failed login attempts)  
 - 4663 → File or folder accessed (this will show when the file was accessed or modified)  
 - 4670 → Permission changes  
  
5. Example of Failed Login Audit:  
 - If a user attempts to log in but fails, you will see Event ID 4625.  
 - To locate this event:  
 1. In the Security log, filter by Event ID 4625.  
 2. This will show details such as the user account name, failure reason, and time of the attempt.  
  
 Sample Event Details for a Failed Login:  
 - Event ID: 4625  
 - Account Name: Hirwa  
 - Failure Reason: Unknown user name or bad password  
 - Date and Time: 3/31/2025 10:15:22 AM  
  
6. Click on an event to view the details:  
 - Who accessed or modified the file  
 - What action was taken (read, write, delete)  
 - Date and time of the action

# Conclusion

By following these steps, you have successfully created a file, edited it, and configured auditing to track any access and modifications to the "data1" folder and its contents. Using Event Viewer, you can monitor who interacted with the file, what actions were taken, and when they occurred.