Implementing file access auditing

You implement file access auditing when you want a record of when and how users access specific files and folders. You configure file access auditing by first enabling auditing in Group Policy and then configuring the items that you want to track so that they will be audited. You have two options when configuring group policy:

■■ You can audit object access generally by enabling the Audit Object Access policy located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy node. This will enable auditing for other objects as well as for file and folders.

■■ You can audit file and folder access specifically by enabling the Audit File System Policy located in the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access node. This only allows auditing of file and folders.

You should configure Global Object Access Auditing for your enterprise by using the security policy of a domain-based GPO. The two security policy settings that are required to enable global object access auditing are located in the following locations:

- Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy\Audit Policies \Object Access\Audit File System
- Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy\Audit Policy \Global Object Access Auditing\File System

Global Object Access Auditing includes a subcategory for file system and registry. All file access audit events also include the resource property values in the audit events so that you can use these values for advanced reporting such as “who accessed all finance data.” Do this by using tools such as Microsoft System Center to collect all the events in a central SQL database and produce reports based on these events