Monitor and Control Windows File Access in Real-Time

Background

It is always very important to protect your company's confidential and sensitive data, although you can apply the NTFS security and firewall policies, it might not provide enough information to you , you still want to know who accesses the files, including the user name and process name, and you also want to know which file was accessed and when this file was accessed. If a file was modified, you also want to know who modified it and what content was changed. You want to get the alert for any unauthorized file access in real-time. The Windows File System Filter Driver can create a secure file access environment, protecting data from unauthorized access and distribution, and create the change auditor for Windows File Servers proactively tracks, audits, reports and alerts on vital changes in real time and without the overhead of native auditing. You will instantly know who made what change, and get the original and current values for fast troubleshooting.

Windows File System Filter Driver

A file system filter driver intercepts requests targeted at a file system or another file system filter driver. By intercepting the request before it reaches its intended target, the filter driver can extend or replace functionality provided by the original target of the request. File system filtering services are available through the filter manager in Windows. The Filter Manager provides a framework for developing File Systems and File System Filter Drivers without having to manage all the complexities of file I/O. The Filter Manager simplifies the development of third-party filter drivers and solves many of the problems with the existing legacy filter driver model, such as the ability to control load order through an assigned altitude. A filter driver developed to the Filter Manager model is called a minifilter. Every minifilter driver has an assigned altitude, which is a unique identifier that determines where the minifilter is loaded relative to other minifilters in the I/O stack. Altitudes are allocated and managed by Microsoft.

How to Monitor and Control Windows File Access

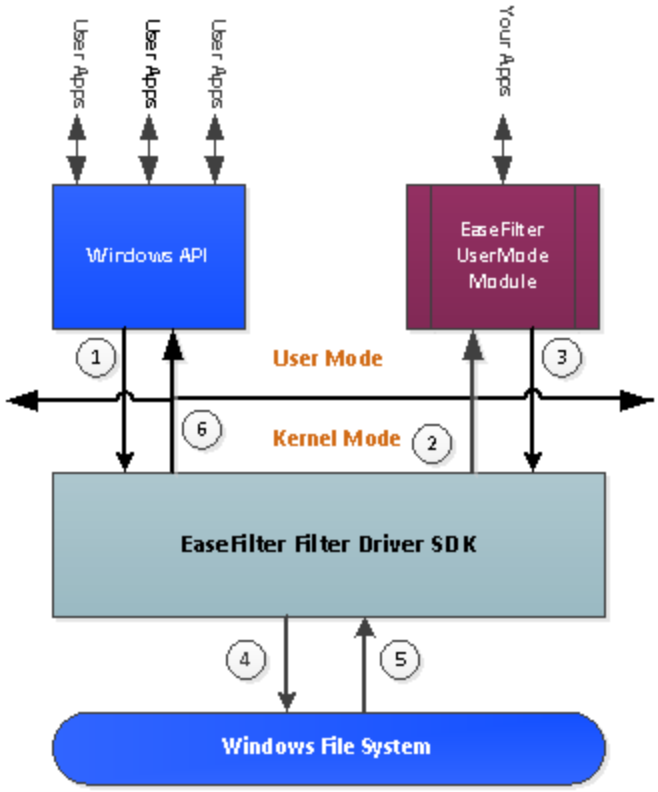
What is the file access? The file access is an I/O operation to a file, there are two types of file access: read access and write access, read access will not change the file, write access will change the file data, file information or file security. To access a windows file, you have to invoke the Win32 API which was exported by Windows subsystems service, the most frequently used Windows API to a file is ”CreateFile”, “ReadFile”, “WriteFile”, “MoveFile”. “DeleteFile”. In this section, we will explain how to monitor and control these APIs with windows file system filter driver in detail.

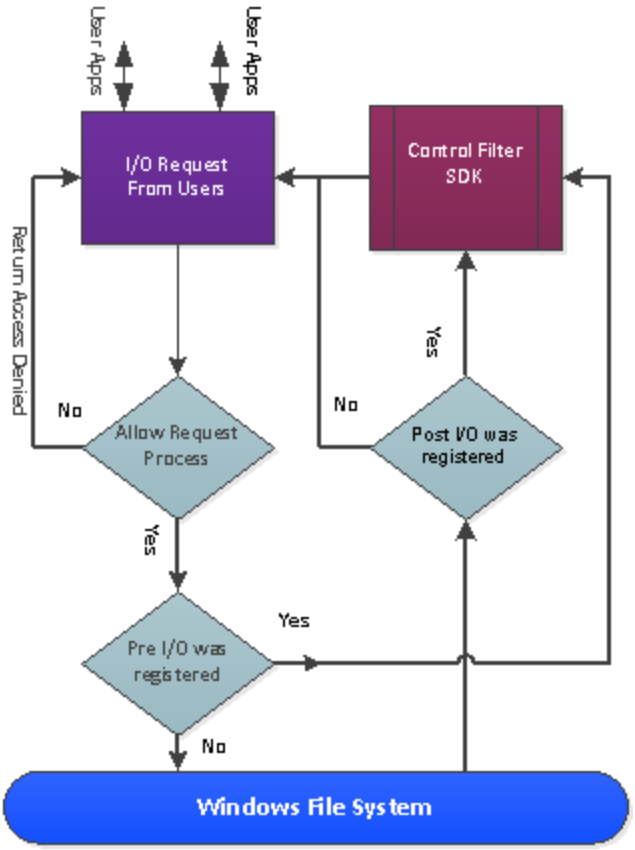
I/O operations are layered, when a user application invokes a Win32 API, the I/O manager intercepts this call, sets up one or more I/O request packets (IRPs), and routes them through possibly layered drivers to physical devices, if a file system filter driver was installed and registered with the volume which the file was located, it can intercept this I/O, then the filter driver can pass through this I/O to next layer driver or complete this I/O. If the filter driver passes through this I/O, the filter driver can intercept this I/O request which comes back from the Windows file system if the post I/O operation was registered. If the filter driver completes this I/O, the request will not pass down to the Windows file system, the filter driver can return your won status and appropriate data to the user application.

The filter driver can register a preoperation callback routine, a postoperation callback routine, or both. When the filter driver intercepts the I/O request, it can get the caller's process name, user's SID (Security Identifier) which it can decode the user name, domain name, the filter driver also can get the current I/O information, the I/O type (create, read, write, rename, delete…), the file name and the file information (file size, file time, file attributes…). If the filter driver only wants to monitor this I/O request, it can send those informations to the user, if the filter driver wants to control this I/O request, it can denied this I/O request, or modify the I/O data and return status.

The below figure shows how the EaseFilter driver monitors and controls the Windows file access, the EaseFilter SDK includes two parts, one part is the filter driver running in the Windows kernel, the other part is the user mode monitor and control module. Here is the steps for specific File_Create I/O request, normally most of the I/O requests start with a File_Create request to open or create a file first, then follow with other requests(read,write,delete…).

1) The user application initiates an I/O request, the I/O request was transferred to the I/O manager, the I/O manager passes down this request to the lower layer drivers.
2) The EaseFilter filter driver will intercept this request, if the file is not located in the managed folder of the EaseFilter, the filter driver passes through this request, or the filter driver will create a file context to track all the following I/O request, then the filter driver will check if this request preoperation was registered, if yes, the EaseFilter filter driver will send the request information to the user mode module, or it will go to step 4.
3) The EaseFilter user mode module can monitor or modify the I/O request and send it back to the EaseFilter filter driver, the EaseFilter filter driver will complete this request if the user mode send back the complete request, or it will pass down to the lower layer drivers.
4) The EaseFitler filter driver passes down this request to the lower layer drivers.
5) The EaseFilter filter driver intercepts the postoperation I/O request if this postoperation I/O request was registered.
6) The EaseFilter filter driver sends this postoperation I/O request information to the user application.





The Applications To Use File System Filter Driver

1. **Audit File Access and Change in Windows in Real-Time**

   One of the bigger problems that we come across is auditing of file systems – specifically, you want to know who read, modified, deleted or created files in a shared area. Get comprehensive control and visibility over users and data by tracking and monitoring all the user & file activities, permission changes, storage capacity and generate real-time audit reports.

   With file system monitor filter you can monitor the file activities on file system level, captures file open, create, overwrite, read, write, query file information, set file information, query security information, set security information, file rename, file delete, directory browsing and file close I/O requests.You can create the file access log, you will know who, when, what files were accessed.

2. **File Access Control System**

With the file system filter driver, you can control the file access with whatever you want as following:

1) Allow or deny the file open or create with the specific access right for some users and processes.
2) Reparse the specific file open to another location.
3) Hide and change the display file names for the specific folders.
4) Replace the read or write data with your own content for specific files.
5) Allow or deny the file rename, delete or modification for the specific users and processes.

EaseFilter File System Filter Driver SDK Framework

To develop file systems and file system filter drivers, use the Windows Driver Kit (WDK),which is provided by Microsoft. Even with the resources available in the Windows Driver Kit (WDK) developing file systems is certainly a challenge. To simplify your development and to provide you with a robust and well-tested file system filter driver that works with all versions and patch releases of the Windows operating systems supported by Microsoft, EaseFilter Inc. offers the file system filter driver SDK which provides a complete, modular environment for building active file system filters in your application. With the EaseFilter file system filter driver SDK, you can develop your own filter driver application with c++/c# or other languages.

EaseFilter File System Filter Driver SDK is a mature commercial product. It provides a complete modular framework to the developers even without driver development experience to build the filter driver within a day. The SDK includes the modules from code design to the product installation, it includes all the basic features you need to build a filter driver:

1. The communication module.

   It demonstrates how to set up the communication channel between the filter driver and your user mode application, send and receive the messages between them.

2. The debug and trace module.

   You can print or trace the debug message with WPP trace module, and you also can use the system event log to log the information from the filter driver.

3. The configuration module.

   This module shows how to manage the configuration setting for the filter driver, includes the managed folders.

4. The file context module.

   This module demonstrate how to trace every file I/O request, with the user information, process information and file information.

5. The I/O request packet handler module.

   This is the most important module, the SDK demonstrates how to intercept the I/O requests, modify the I/O data. It means you can build your own custom filter driver easily based on the SDK.

About EaseFilter Inc.

EaseFilter Inc. is a company who specializes in windows file system filter driver development. It can provide architect, implement and test file system filter drivers for a wide range of functionalities. It also can offer several levels of assistance to meet your specific needs: Provide consulting service for your existing file system filter driver; Customize the SDK to meet your requirement; Create your own filter driver with SDK source code.

For more information please go to the website: www.easefilter.com

You can download the demo binary and example projects here:
http://www.easefilter.com/download/easefilter.zip