## File Integrity Monitoring (FIM) – via Windows Auditing

|  |  |
| --- | --- |
| **Section** | **Description** |
| **Description** | When it comes to Windows we have two methods available to use to watch for changed files – OSSEC syscheck and Windows Auditing. If the host you are watching is Windows and you need to know WHO changed files (for instance, when watching application deployments on a server for change management purposes), then using Windows Auditing coupled with OSSEC email alerting will be the best option. That’s what this section is about.  However, if you only need to know that files were changed/added/deleted and don’t care WHO did it, or if your host is a Linux box, skip to the next section **FIM – via OSSEC Syscheck.** |
| **Overview** | To enable FIM using Windows Auditing, the high-level steps involved are as follows:   1. Enable Windows Audit Policy for File System Objects 2. Configure the audit policy appropriately for the files and/or directories that need to be watched 3. Configure custom rules in OSSEC to trigger on file add/change/delete events |
| **Step 1:**  **Enable Audit Policy for File System Objects** | To have Windows watch for file changes and report such activity in the event log, we need to enable the **Audit File System** audit setting.   1. Enable the **Advanced Audit Configuration** for “Audit File System” and set it to **Success** only.    1. In GPO, this is found under ***Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Object Access > Audit File System*** 2. Apply the GPO to the appropriate server(s) 3. Logon to the server you want to apply this policy to and execute **CMD**: **gpupdate** 4. From an elevated **CMD** prompt, verify **Object Access > File System** is set to **Success** by executing:  **auditpol /get /category:"Object Access"** |
| **Step 2:**  **Configure Files / Directories to be Monitored** | 1. Logon to the server where you want files to be watched 2. Open **File Explorer** and navigate to the directory you want to watch 3. In the directory **Properties**, go into **Security > Advanced > Auditing** and **Add** the auditing you want to perform. To watch for the same add/delete/modify changes as OSSEC’s syscheck, you would choose the **Show advanced permissions** and select the following four permissions:    1. **Create files / write data**    2. **Create folders / append data**    3. **Delete subfolders and files**    4. **Delete** 4. These four permissions will cover all the necessary bases, without firing off events every time someone simply reads a file or traverses the directory.   **NOTE:**  *Windows audits certain directories/files by default, which will in turn potentially trigger excessive and/or unnecessary alerting after enabling . If so, you may find that you need to create multiple custom exceptions in your rules to minimize that noise. You can use various tools to determine what directories are being audited already – such as this simple free tool:* [*http://www.cjwdev.co.uk/Software/CheckAuditGUI/CheckAuditGUI.zip*](http://www.cjwdev.co.uk/Software/CheckAuditGUI/CheckAuditGUI.zip)  *In addition, there’s some suggestion that audit entries are created with some backup application that utilize the archive flag on files.* |
| **Step 3:**  **Configure OSSEC Rules** | The final step is to configure the appropriate rules on the OSSEC server. By default rule #18104 detects audit successes and simply discards them (level =”0”). We want to use those 18104 events for our FIM.  Edit your local\_rules.xml and first create a rule that will disregard many temporary type files. We’ll use a custom group named “noise” for this activity:  <rule id="100200" level="0">  <if\_sid>18104</if\_sid>  <id>^4659$|^4663$</id>  <regex>Object Name:\.\*.tmp|</regex>  <regex>Object Name:\.\*.log|</regex>  <regex>Object Name:\.\*\\~\$</regex>  <group>noise,syscheck</group>  <description>FIM: Ignore temporary and log files like .log .tmp and \~$ from most editing applications</description>  </rule>  Next, we can set a lower alert level or simply disregard some other areas that have a lot of changes when it comes to things like Windows patching. In this case we’ll still log these but not send any email alerts:  <rule id="100202" level="7">  <if\_sid>18104</if\_sid>  <id>^4659$|^4663$</id>  <regex>Object Name:\.\*C:\\Windows\\WinSxS|</regex>  <regex>Object Name:\.\*:\\Windows\\rescache|</regex>  <regex>Object Name:\.\*:\\Windows\\Microsoft.NET|</regex>  <regex>Object Name:\.\*:\\Windows\\SYSVOL\_DFSR|</regex>  <regex>Object Name:\.\*:\\System Volume Information</regex>  <options>no\_email\_alert</options>  <group>syscheck,</group>  <description>FIM: Changes that don't need email alerts but are still logged</description>  </rule>  Now we can set rules to detect and alert on file changes and deletes. Since OSSEC can’t translate the Windows Event Log field codes to human readable text, it will only see the %%xxxx field code (see ***Appendix H*** for a full list of known field codes).  <!-- General Servers -->  <rule id="100220" level="7">  <if\_sid>18104</if\_sid>  <id>^4659$|^4663$</id>  <regex>Access Request Information:\.\*Accesses:\s\*\t\*%%4417|</regex>  <info>%%4417 maps to "WriteData or AddFile"</info>  <regex>Access Request Information:\.\*Accesses:\s\*\t\*%%4418|</regex>  <info>%%4418 maps to "AppendData or AddSubDirectory"</info>  <description>FIM: Audited file has been CHANGED or a new file/directory ADDED.</description>  <group>syscheck,</group>  </rule>  <rule id="100221" level="7">  <if\_sid>18104</if\_sid>  <id>^4659$|^4663$</id>  <regex>Access Request Information:\.\*Accesses:\s\*\t\*%%1537</regex>  <info>%%1537 maps to "DELETE"</info>  <description>FIM: Audited file has been DELETED.</description>  <group>syscheck,</group>  </rule> |

## Appendix: Mapping of Event Log Codes

Mapping of some event log codes to human-readable text access rights:

**High level Generic Codes**

1537 DELETE

1538 READ\_CONTROL

1539 WRITE\_DAC

1540 WRITE\_OWNER

1541 SYNCHRONIZE

1542 ACCESS\_SYS\_SEC

**File codes**

4416 ReadData

4417 WriteData

4418 AppendData

4419 ReadEA

4420 WriteEA

4421 Execute/Traverse

4422

4423 ReadAttributes

4424 WriteAttributes

**Registry Codes**

4432 Query Key Value

4433 Set Key Value

4434 Create Sub Key

4435 Enumerate sub-keys

4436 Notify about changes to keys

4437 Create Link

Here is the complete list (from msobj.dll) in Windows XP. Values like "undefined" have been stripped out. *NOTE: Newer Windows version added many more values.*

ACCESS\_EVENT\_ID = {

1536 : 'Unused message ID',

1537 : 'DELETE',

1538 : 'READ\_CONTROL',

1539 : 'WRITE\_DAC',

1540 : 'WRITE\_OWNER',

1541 : 'SYNCHRONIZE',

1542 : 'ACCESS\_SYS\_SEC',

1543 : 'MAX\_ALLOWED',

1601 : 'Not used',

1603 : 'Assign Primary Token Privilege',

1604 : 'Lock Memory Privilege',

1605 : 'Increase Memory Quota Privilege',

1606 : 'Unsolicited Input Privilege',

1607 : 'Trusted Computer Base Privilege',

1608 : 'Security Privilege',

1609 : 'Take Ownership Privilege',

1610 : 'Load/Unload Driver Privilege',

1611 : 'Profile System Privilege',

1612 : 'Set System Time Privilege',

1613 : 'Profile Single Process Privilege',

1614 : 'Increment Base Priority Privilege',

1615 : 'Create Pagefile Privilege',

1616 : 'Create Permanent Object Privilege',

1617 : 'Backup Privilege',

1618 : 'Restore From Backup Privilege',

1619 : 'Shutdown System Privilege',

1620 : 'Debug Privilege',

1621 : 'View or Change Audit Log Privilege',

1622 : 'Change Hardware Environment Privilege',

1623 : 'Change Notify (and Traverse) Privilege',

1624 : 'Remotely Shut System Down Privilege',

4352 : 'Device Access Bit 0',

4353 : 'Device Access Bit 1',

4354 : 'Device Access Bit 2',

4355 : 'Device Access Bit 3',

4356 : 'Device Access Bit 4',

4357 : 'Device Access Bit 5',

4358 : 'Device Access Bit 6',

4359 : 'Device Access Bit 7',

4360 : 'Device Access Bit 8',

4368 : 'Query directory',

4369 : 'Traverse',

4370 : 'Create object in directory',

4371 : 'Create sub-directory',

4384 : 'Query event state',

4385 : 'Modify event state',

4416 : 'ReadData (or ListDirectory)',

4417 : 'WriteData (or AddFile)',

4418 : 'AppendData (or AddSubdirectory or CreatePipeInstance)',

4419 : 'ReadEA',

4420 : 'WriteEA',

4421 : 'Execute/Traverse',

4422 : 'DeleteChild',

4423 : 'ReadAttributes',

4424 : 'WriteAttributes',

4432 : 'Query key value',

4433 : 'Set key value',

4434 : 'Create sub-key',

4435 : 'Enumerate sub-keys',

4436 : 'Notify about changes to keys',

4437 : 'Create Link',

4448 : 'Query mutant state',

4464 : 'Communicate using port',

4480 : 'Force process termination',

4481 : 'Create new thread in process',

4483 : 'Perform virtual memory operation',

4484 : 'Read from process memory',

4485 : 'Write to process memory',

4486 : 'Duplicate handle into or out of process',

4487 : 'Create a subprocess of process',

4488 : 'Set process quotas',

4489 : 'Set process information',

4490 : 'Query process information',

4491 : 'Set process termination port',

4496 : 'Control profile',

4512 : 'Query section state',

4513 : 'Map section for write',

4514 : 'Map section for read',

4515 : 'Map section for execute',

4516 : 'Extend size',

4528 : 'Query semaphore state',

4529 : 'Modify semaphore state',

4544 : 'Use symbolic link',

4560 : 'Force thread termination',

4561 : 'Suspend or resume thread',

4562 : 'Send an alert to thread',

4563 : 'Get thread context',

4564 : 'Set thread context',

4565 : 'Set thread information',

4566 : 'Query thread information',

4567 : 'Assign a token to the thread',

4568 : 'Cause thread to directly impersonate another thread',

4569 : 'Directly impersonate this thread',

4576 : 'Query timer state',

4577 : 'Modify timer state',

4592 : 'AssignAsPrimary',

4593 : 'Duplicate',

4594 : 'Impersonate',

4595 : 'Query',

4596 : 'QuerySource',

4597 : 'AdjustPrivileges',

4598 : 'AdjustGroups',

4599 : 'AdjustDefaultDacl',

4608 : 'Create instance of object type',

4864 : 'Query State',

4865 : 'Modify State',

5120 : 'Channel read message',

5121 : 'Channel write message',

5122 : 'Channel query information',

5123 : 'Channel set information',

5136 : 'Assign process',

5137 : 'Set Attributes',

5138 : 'Query Attributes',

5139 : 'Terminate Job',

5140 : 'Set Security Attributes',

5376 : 'ConnectToServer',

5377 : 'ShutdownServer',

5378 : 'InitializeServer',

5379 : 'CreateDomain',

5380 : 'EnumerateDomains',

5381 : 'LookupDomain',

5392 : 'ReadPasswordParameters',

5393 : 'WritePasswordParameters',

5394 : 'ReadOtherParameters',

5395 : 'WriteOtherParameters',

5396 : 'CreateUser',

5397 : 'CreateGlobalGroup',

5398 : 'CreateLocalGroup',

5399 : 'GetLocalGroupMembership',

5400 : 'ListAccounts',

5401 : 'LookupIDs',

5402 : 'AdministerServer',

5408 : 'ReadInformation',

5409 : 'WriteAccount',

5410 : 'AddMember',

5411 : 'RemoveMember',

5412 : 'ListMembers',

5424 : 'AddMember',

5425 : 'RemoveMember',

5426 : 'ListMembers',

5427 : 'ReadInformation',

5428 : 'WriteAccount',

5440 : 'ReadGeneralInformation',

5441 : 'ReadPreferences',

5442 : 'WritePreferences',

5443 : 'ReadLogon',

5444 : 'ReadAccount',

5445 : 'WriteAccount',

5446 : 'ChangePassword (with knowledge of old password)',

5447 : 'SetPassword (without knowledge of old password)',

5448 : 'ListGroups',

5449 : 'ReadGroupMembership',

5450 : 'ChangeGroupMembership',

5632 : 'View non-sensitive policy information',

5633 : 'View system audit requirements',

5634 : 'Get sensitive policy information',

5635 : 'Modify domain trust relationships',

5636 : 'Create special accounts (for assignment of user rights)',

5637 : 'Create a secret object',

5638 : 'Create a privilege',

5639 : 'Set default quota limits',

5640 : 'Change system audit requirements',

5641 : 'Administer audit log attributes',

5642 : 'Enable/Disable LSA',

5643 : 'Lookup Names/SIDs',

5648 : 'Change secret value',

5649 : 'Query secret value',

5664 : 'Query trusted domain name/SID',

5665 : 'Retrieve the controllers in the trusted domain',

5666 : 'Change the controllers in the trusted domain',

5667 : 'Query the Posix ID offset assigned to the trusted domain',

5668 : 'Change the Posix ID offset assigned to the trusted domain',

5680 : 'Query account information',

5681 : 'Change privileges assigned to account',

5682 : 'Change quotas assigned to account',

5683 : 'Change logon capabilities assigned to account',

6656 : 'Enumerate desktops',

6657 : 'Read attributes',

6658 : 'Access Clipboard',

6659 : 'Create desktop',

6660 : 'Write attributes',

6661 : 'Access global atoms',

6662 : 'Exit windows',

6663 : 'Unused Access Flag',

6664 : 'Include this window station in enumerations',

6665 : 'Read screen',

6672 : 'Read Objects',

6673 : 'Create window',

6674 : 'Create menu',

6675 : 'Hook control',

6676 : 'Journal (record)',

6677 : 'Journal (playback)',

6678 : 'Include this desktop in enumerations',

6679 : 'Write objects',

6680 : 'Switch to this desktop',

6912 : 'Administer print server',

6913 : 'Enumerate printers',

6930 : 'Full Control',

6931 : 'Print',

6948 : 'Administer Document',

7168 : 'Connect to service controller',

7169 : 'Create a new service',

7170 : 'Enumerate services',

7171 : 'Lock service database for exclusive access',

7172 : 'Query service database lock state',

7173 : 'Set last-known-good state of service database',

7184 : 'Query service configuration information',

7185 : 'Set service configuration information',

7186 : 'Query status of service',

7187 : 'Enumerate dependencies of service',

7188 : 'Start the service',

7189 : 'Stop the service',

7190 : 'Pause or continue the service',

7191 : 'Query information from service',

7192 : 'Issue service-specific control commands',

7424 : 'DDE Share Read',

7425 : 'DDE Share Write',

7426 : 'DDE Share Initiate Static',

7427 : 'DDE Share Initiate Link',

7428 : 'DDE Share Request',

7429 : 'DDE Share Advise',

7430 : 'DDE Share Poke',

7431 : 'DDE Share Execute',

7432 : 'DDE Share Add Items',

7433 : 'DDE Share List Items',

7680 : 'Create Child',

7681 : 'Delete Child',

7682 : 'List Contents',

7683 : 'Write Self',

7684 : 'Read Property',

7685 : 'Write Property',

7686 : 'Delete Tree',

7687 : 'List Object',

7688 : 'Control Access'

}