Windows Security Log File Access Auditing Deep Dive

Sponsored by

solarwinds

Thanks to

- Made possible by

solarwinds

LOG & EVENT MANAGER

www.solarwinds.com

Travis Fenton, Sr. Engineer

Nicole Pauls, Product Manager

© 2014 Monterey Technology Group Inc.

Preview of Key Points

- Enabling file auditing at the system level
- Configuring folder/file level auditing
  - Allowed/denied
  - Which users/groups
  - Which permissions
- Watching for the appropriate events
- Interpreting the details of the events

System level auditing

- Enable security option: "Audit: force audit subcategory"
- Enable Advanced Audit Policy\Object Access
  - File Access
  - Handle Manipulation?
- Related categories
  - Removable Storage
  - Detailed File Share

Folder level auditing

- Who?
- Allow or Deny?
- Which permissions?
- Folders or just Files?
- Propagate to child objects?

What is being logged?

- Not user actions
  - Application interaction with file system
    - Open file (request handle) with X permissions
    - Perform operations on file via handle
    - Close the handle
- Not file i/o
  - Successful/failed request of permissions to files and folders at the time object is opened
  - Successful use of any of those permissions for the first time while object opened
  - Closure of handle to the object

Event IDs

- 4656 – Handle to an object was requested
  - Success/failure
  - Only logged if Handle Manipulation enabled along with "File System"
- 4663 – An attempt was made to access an object
  - Success
- 4658 – The handle to an object was closed
  - Success
  - Only logged if Handle Manipulation also enabled

Caveats

- Successful file open (4656) don't tell you permissions where actually **used** – just successfully requested
- To get failure audits – must enable Handle Manipulation
  - Triples quantity of events
- How long file open?
  - Use file close event
  - But remember that it reflects when the application closed the file – may not match user experience

Caveats

- Audit scenarios
  - Failed access attempts
    - Enable handle manipulation
    - 3x the events
  - File read
    - Be aware of things like Explorer's thumbnail processing
  - File write
    - Be aware of applications like MS Office that modify a file even if user doesn't modify the document
  - Deletion

Other events

- 4659 A handle to an object was requested with intent to delete
  - Unobserved in testing
  - For when files flagged for deletion at next OS restart: patching
- 4660 An object was deleted
  - File name omitted use 4663 instead
- 4664 An attempt was made to create a hard link
  - Make a given file show up in another folder but with different permissions
- 4670 Permissions on an object were changed
  - Need to be auditing Change Permissions permission
  - Shows before and after ACL

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Audit scenarios

- Attempts to look at unauthorized files
- Audit trail of information access
- Audit trail of modifications
- File/Folder creation
- File/Folder deletion
- Permission changes

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Bottom line

- Auditing file access
  - Be very careful with audit policy
    - Understand difference between file/folder permissions
    - Apply inheritance correctly
    - Don't enable Handle Manipulation unless tracking Failed access
  - Get ready for a lot of noise
  - No wildcard auditing
  - No centralized control
    - Folder level auditing
    - Collection and Analysis of events
- Solution: SolarWinds Log and Event Manager
  - Agent based auditing to the rescue
  - Support for native file access auditing
  - Events from both sources normalized!

SolarWinds' Vision

The POWER to Manage IT, Anywhere

Regardless of…

- Location of IT resources
- Where management resource needs to be located
- Size of company or complexity of environment

solarwinds

File Integrity Monitoring

- Monitor files and registry for changes in real-time
- FIM for Systems Monitoring
  - Assists with spotting issues like unintentional deletion, unexpected changes to system files/keys
- FIM for Security Monitoring
  - Detect threats that AV and other tools may not pick up by monitoring at the file/registry level
  - Track potential insider abuse (too much access, unexpected changes)
  - Aids in compliance with many regulatory initiatives (PCI, HIPAA, SOX, and more)
- Included as an out of the box feature with SolarWinds Log & Event Manager

solarwinds

FIM + SIEM Is Even Better!

- Benefits of LEM – supplements Windows File Auditing with FIM+SIEM
  - Centralized mass configuration without relying on group policy
  - Easier to configure in a single console, rather than accessing many directories/files individually
- Correlate file activity with other log and system activity
  - Combine FIM with USB-Defender to track file and process activity on both systems and USB devices
  - See file events in scope with other server change events, anti-virus events, traditional Windows Event Log events, and more, to identify source and scope of potential issues and reduce false positives from tracking files alone
- Use active response to mitigate potential issues in real-time
  - Remove privileges, disable computer/user accounts, and more, automatically or with the push of a button

solarwinds

DEMO

solarwinds

Q&A

- Monthly Live Demo of SolarWinds Log & Event Manager
- Upcoming Topics
  - August 8: Intrusion Detection & Malware Protection
  - September 12: Workstation Security & Endpoint Protection
- Sign up at http://go.solarwinds.com/lem/livedemo/2014

solarwinds