ManageEngine

EventLog Analyzer

Object Access Auditing Simplified with EventLog Analyzer

Solution Brief

Object Access Auditing Simplified with EventLog Analyzer

Most administrators face the challenge of knowing what actually happened to their files and folders – who accessed them, deleted them, edited them, moved them, where the files and folders went, etc. Object access auditing can help administrators to meet this challenge head-on.

Object access auditing is a critical requirement for organizations and helps network administrators to secure their enterprise network. With Object access auditing, organizations can secure their business critical data, such as employee data, accounting records, intellectual property, patient data, financial data, etc. One of the key goals of object access audits is regulatory compliance.

Industry standards such as Sarbanes Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Payment Card Industry (PCI) require organizations to adhere to strict set of rules related to data security and privacy. Unauthorized access, accidental access, files/folders deletion, changes in files/folders, or permissions opens the door for data thefts and can result in getting your organization a non-compliant status which not only is a costly affair but will also tarnish your company's brand value.

To enable windows auditing for Object access, first activate audits of successful object access attempts and Failure access attempts via the local or domain security policy settings.

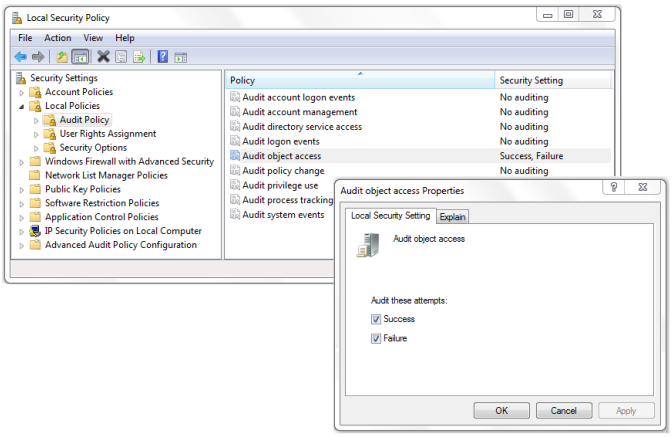


Figure 1: Enabling Object Access Audit in Windows

If you do not enable the above setting, you will have no record when a file or folder was accessed. Most administrators would like to know only the failure attempts when someone tries to access the file or folder but failed because of improper permission. But it is highly recommended to enable both – failure attempts and success attempts. The reason for enabling success attempts is that sometimes hackers can use administrator privilege and gain access to confidential files and folders.

Your enterprise will have crucial data stored in files and folders such as financial data, employee data, patient records, bank account data, etc. The next step is to go to such files and folders to enable auditing on them. Each file / folder's auditing settings must be modified to include those users you wish to audit.

These are enabled in Properties->Security->Advanced->Auditing. If you want to audit all access events by everyone, add everyone group, and select Success>Full Control.

(**See Screen Shot Below**)

Note:

Select the attributes based on your requirement. Delete and Modify attributes are most recommended.

Enabling all the attributes to users will flood the event viewer in few seconds, and consume more bandwidth. So judiciously select the attributes required for your auditing needs.

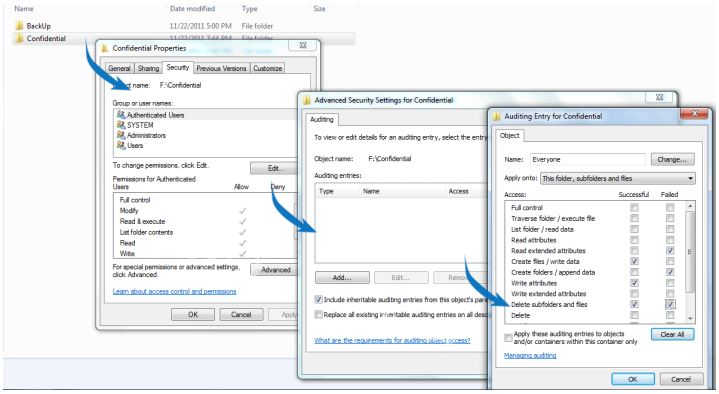


Figure 2: Object Access Auditing Configuration on Files and Folders

Please refer the following links to configure object access to a specified folder/file for various Windows operating systems:

For XP:

http://support.microsoft.com/?kbid=310399

For Windows 2000:

http://support.microsoft.com/kb/314955

For Windows 2003:

http://support.microsoft.com/kb/814595

For Windows 2008:

http://technet.microsoft.com/enus/library/cc731607(WS.10).aspx

There are no objects configured to be audited by default. Once this auditing setting for an object is configured, log entries on access attempts (Successful and Failed) start getting recorded and you will be able to view the object access related events in the security log in Event Viewer. (**See Screen Shot Below**)

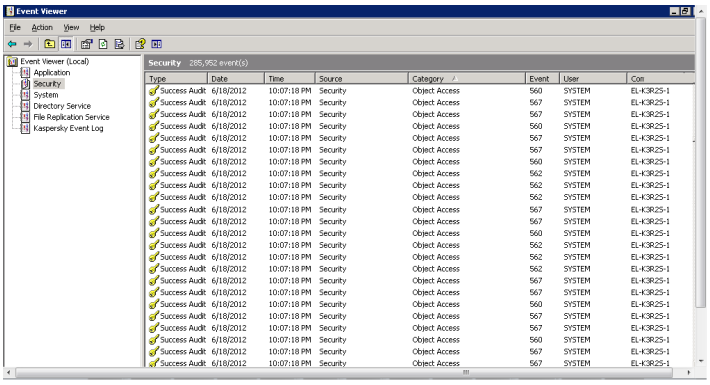


Figure 3: Windows Event Viewer

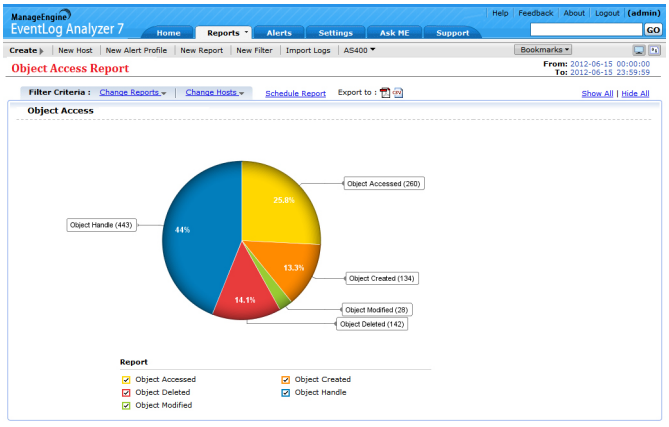
The events must be opened up individually to inspect their contents, which is a painful process and is totally impossible in an IT enterprise network. Manually collecting, archiving and analyzing object access log data is cumbersome and a time consuming task. Automated log management solutions like EventLog Analyzer willhelp network administrators to automatically collect, archive and analyze object access log data at a centralized location from all your machines present in your network.

Object Access Auditing with EventLog Analyzer

Using EventLog Analyzer you can collect all your object access audit logs at a centralized location and manage your object access audit logs effectively. This log management software can track success and failure access attempts on folders and files in your enterprise.

EventLog Analyzer provides object access reports in user friendly formats (PDF and CSV) and sends alerts when your sensitive files / folders are accessed by unauthorized people in real-time via sms or email. With EventLog Analyzer you get precise information of object access such as which user performed the action, what was the result of the action, on which server it happened and tracks down the user workstation/network device from where the action was triggered.

The EventLog Analyzer Object Access Report dashboard is intuitively designed and it shows the object access audit data in a graphical and tabular format. (**See Screen Shot Below**).



Object Access (1007 events)

Object Accessed (260 events)

HostName	Count
ADCluster	55
ADServer	46
DHCPServer	48
Domain-Controller	60
ExchangeServer	51

Object Created (134 events)

HostName	Count
ADCluster	31
ADServer	30
DHCPServer	23
Domain-Controller	25
ExchangeServer	25

Object Modified (28 events)

HostName	Count
ADCluster	3
ADServer	10
DHCPServer	4
Domain-Controller	6
ExchangeServer	5

Object Deleted (142 events)

HostName	Count
ADCluster	29
ADServer	30
DHCPServer	20
Domain-Controller	33
ExchangeServer	30

Object Handle (443 events)

HostName	Count	Handle Allocated	Handle Closed
ADCluster	80	0%	100%
ADServer	79	0%	100%
DHCPServer	93	0%	100%
Domain-Controller	101	0%	100%
ExchangeServer	90	0%	100%

Figure 4: Object Access Auditing Dashboard in EventLog Analyzer

The EventLog Analyzer dashboard and reports cover all the aspects of object access auditing in detail. You can drill down on the event data available on the object access dashboard and reports to get more precise information such as Username, Domain, Severity, Event ID, Object name, Object type and time. (**See Screen Shot Below**)

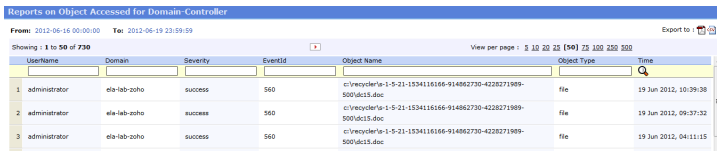


Figure 5: Object Access Analysis in EventLog Analyzer

Create Reports and Alerts using Object Access Audit Event ID's

EventLog Analyzer allows you to create reports and alerts using Object Access Audit event ID's. In simple words, these Event Id's give detailed information on Object Accessed, Object Created, Object Modified, Object Deleted and Object Handle. Read more on event ids used for Object access auditing.

Object Access Event Id's for Windows Operating Systems

560, 562, 563, 564, 565, 566, 567 and 568

- Windows 2000
- Windows Xp
- Windows 2003

4656, 4658, 4659, 4660, 4661, 4662, 4663 and 4664

- Windows Vista,
- Windows 7
- Windows 2008 & Windows 2008 R2

EventLog Analyzer allows you to create Object access audit reports using the above mentioned event Id's. (**See Screen Shot Below**)

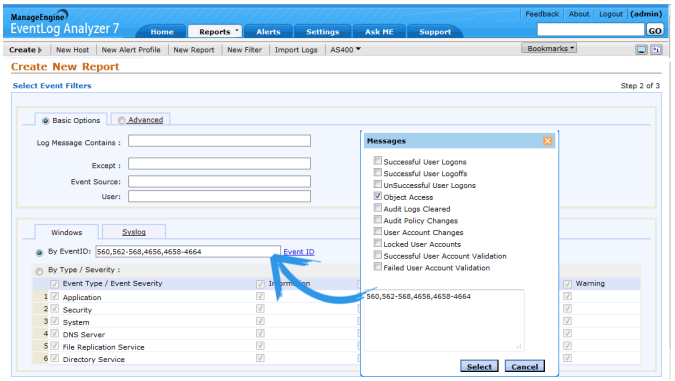


Figure 6: Object Access Auditing Reports using Object Access EventID's

Similarly, EventLog Analyzer allows you to create Object access audit alerts using the above mentioned Object access Event Id's.

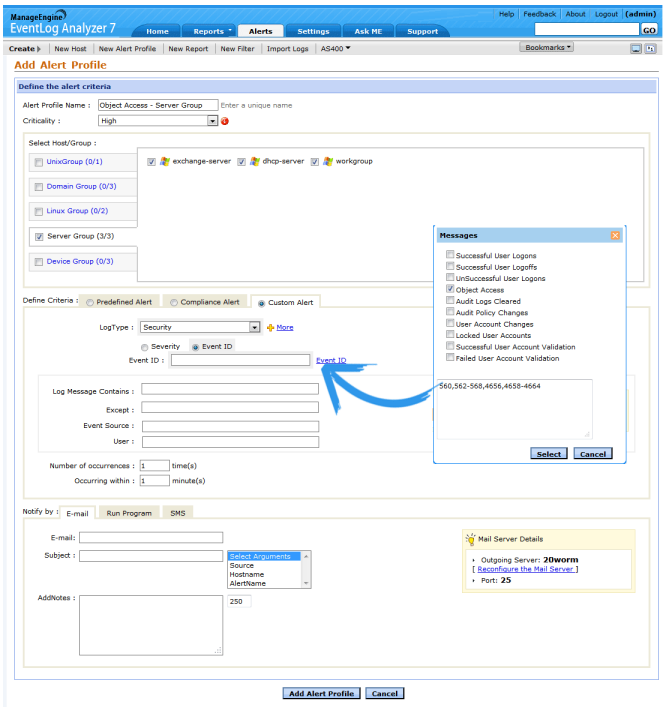


Figure 7: Object Access Auditing Alert Configuration

With EventLog Analyzer you can now detect anomalous behavior in real-time, mitigate loopholes in network security, and thereby prevent data breaches by creating a trail of user activity that happened on your files and folders. You can also use this user activity trail for log forensic analysis using EventLog Analyzer.

About EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less (optional agent available), event log and application log monitoring and management software. EventLog Analyzer helps monitoring internal threats to the enterprise IT resources and tighten security policies in the enterprise.

http://blogs.eventloganalyzer.com/ www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.