Significance of Proficient Event Logs Archiving in prevailing over Compliance Worries

Whitepaper

2013

www.lepide.com

1. Introduction

Event logs archiving has gained immense significance in the light of numerous compliance requirements that have become inescapable for organizations. But before dwelling into what those requirements are, let’s try to understand what Event logs are and why they are important.

Event logs are historical records of all events happening on the computers and other devices in the network and are generated and stored locally. These Event Logs come in handy in all scenarios to find out what happened, Why and by Whom. As such, thousands of these are generated per day per machine (Removed the sentence here). And filtering hundreds of thousands of Logs spread across multiple machines for a piece of vital information is such a daunting task, and on top of that, not knowing how long you need to store these Event Logs (Event Log Archiving). A good strategy, in general, would be to keep track of as many events as possible in a centralized location without overburdening IT resources.

Event logs archiving deals with moving the generated logs from their source to another location for the purpose of long term storage either using native services or using commercially available software. Archiving event logs using native services comes with some inherent disadvantages, for example, you need to write complex scripts to implement archiving. Moreover, you cannot archive logs of all computer systems to a central location, which is the feature of most of the commercially available products; instead, you first need to create event logs backups locally and then move those backups to a central location.

Event logs archiving helps you to be compliant with various Organizational Standards, as different compliance standards stipulate different time duration for which you need to keep systems’ event logs. Apart from this, archiving also supports forensic analysis to investigate computer based crimes, planning etc.

2. Event Log Archiving Requirements for various Compliances

Various Compliance standards such as HIPAA, GLBA, PCI, SOX, FISMA etc, have different set of requirements when it comes to Event logs. However, related requirements such as forensic investigation etc. require you to archive and be able to recollect and analyze event logs for past as many years as you can, that should go well beyond the retention requirements of seven years as stated by SOX and HIPAA. Retention period notwithstanding, compliance requirements are most difficult to meet for any organization. Because, in this case you need to have demonstrable ability to answer all audit related questions such as who accessed what and when etc. on a continuous basis. On a fundamental level, you should be able to consolidate logs from different systems and correlate between them which in turn requires you to archive event logs from all systems in the network to a centralized location so that it can be processed to offer insights as per requirement. Imagine, using a simple Filter or a custom Report to get the needed data from hundreds of Gigs of Log data within a minute from the comfort of a centralized location (machine)

Health Insurance Portability and Accountability Act (HIPAA) is binding on those in the healthcare industry and transact patients' health information. In fact, patient's medical information cannot even be faxed, if so with certain hard limitations. Such organizations need to have sufficient internal control to regulate access, use, disclosure, modification, or interference with patients' data. In simple words, they should be able to store, report on and get instant information from logs that record access attempts made to IT resources. Monitoring Computer activities such as audit logs, access reports, security incident tracking, recording and examining activities of system that use healthcare information, managing passwords etc. are some of the requirements of HIPAA that are based around event logs analysis.

SOX compliance, which advocates proper internal control over financial reporting, is mandatory for all publicly traded US companies their international operations and also other overseas companies operating in US. Besides, many other nations have implemented similar compliances though they may call it by some other name. Basic requirements in the context of IT department are almost same – control, constant monitoring, evaluation of controls and ability to demonstrate such controls. Passing SOX compliance audits manually would be costly and inefficient; proper automation can, however, not only ensure successful auditing but at lower cost and effort.

PCI compliance needs to be sustained by all organizations that accept credit cards. Restricting access to card-holders data, tracking and evaluating all accesses made to resources that store or transact such data is mandatory as per PCI compliance. All computer logon activities must be tracked and analyzed, computer and server activities recorded with precise details, and provisions made to ensure unlimited and efficient storage of event logs for years with ability to retrieve any record are some of the requirements of PCI compliance.

Gramm-Leach-Bliley Act (GLBA) stipulates guidelines for security management aimed at protecting customer records for financial organizations. All customer records that are not supposed to be in the public domain need to be protected against attempted and successful access, modification and deletion by unauthorized users. This requires centralized archiving of all event logs so that reports and alerts can be generated at any time for required time frame that may extend for years.

Federal Information Systems Management Act (FISMA) requires federal agencies and contractors or other agencies that provide support to such agencies to create a cost-effective program to protect information systems that support operations and assets of the agency. This requires comprehensive event log tracking and archiving so that reports can be generated for specified period of time which could date back even 10 years or more, to investigate a security lapse or so.

3. How Event Log archiving assures compliance with various regulations?

Event logs archiving assures ready access to log data for any period of time to answer any audit question or to investigate cases of security lapse that might have occurred in the past. To generate reports for a particular time frame in the past, you first need to have event logs data for that period; the next step is to be able to segregate the requested data and then process it to present it in the required format. Now, depending on the time frame that you are looking at as part of your plan to archive event logs data, there could be a requirement of huge storage space. Chances of data redundancy may further push the resource requirement in case of inefficient archiving.

To deal with these issues and a host of other intricacies, organizations usually go for a centralized event logs archiving that is not only resource-efficient but also addresses a number of other concerns such as redundancy, security and accessibility. Having such centralized event logs archiving in place offers a number of benefits that includes successful compliance as well; let’s see how:

- Archiving event logs means you can get access to such logs for any time period in the past.
- Generate compliance-specific reports from a data pool and filter them by Computers/Process/Policy by which only required data can be presented to you.
- Event logs can be stored with efficient usage of memory space to accommodate more data.
- It can be secured against unauthorized access and data manipulation attempt to ensure that original logs are presented as and when required.

4. LELM and effective Event Log Archiving

Lepide Event Log Manager is a complete event log archiving and reporting solution that can take care of all your compliance worries. It collects and archives event logs and W3C logs in a centralized database to support specific auditing, long term reporting and efficient log management for entire network. You can employ agent-based and non-agent based event logs collection methods for efficient use of network capacity. Also, event logs collection rules can be configured for individual computers to collect only relevant logs from required computers while other logs can be discarded. Lepide Event Log Manager lets you archive and manage Windows and W3C events logs centrally with a number of benefits such as:

- Central repository for storing network-wide events from all machines in the Network.
- Collect only selected logs and maintain a lean archive of only relevant data.
- Archive event logs in a secured SQL server database to prevent data manipulation.
- Access archive data of any time frame with pre-defined and customized reports to support compliance.

About Lepide

Lepide Software offers cutting-edge software products that helps customer to excel in their businesses. It has a wide portfolio of products serving clients across verticals that have benefited largely from them. The company aims to be recognized as the best provider of business enhancement software tool. For more information, visit:

http://www.lepide.com

To know more about Lepide Event Log Manager, visit:

http://www.lepide.com/event-log-manager/

To try Lepide Event Log Manager, visit:

http://www.lepide.com/event-log-manager/download.html