ManageEngine
EventLog Analyzer

File integrity monitoring with EventLog Analyzer

Introduction

Enterprises most commonly use file-based systems to organize, store, and process information, and file integrity monitoring (FIM) is a change monitoring technique that helps you ensure the security of data stored in critical files and folders. A comprehensive FIM technique continuously monitors files and folders for unexpected or unauthorized changes, and it instantly collects important contextual information, including who made the change, when, and from where.

Importance of FIM

FIM is used to audit changes made to your most critical files and folders, such as:

- Binary files of important system software—including operating systems, compilers, assemblers, and drivers.
- Configurations, settings, and other important application files.
- Business-critical files that contain sensitive data such as customer information.
- Log files related to network activity.

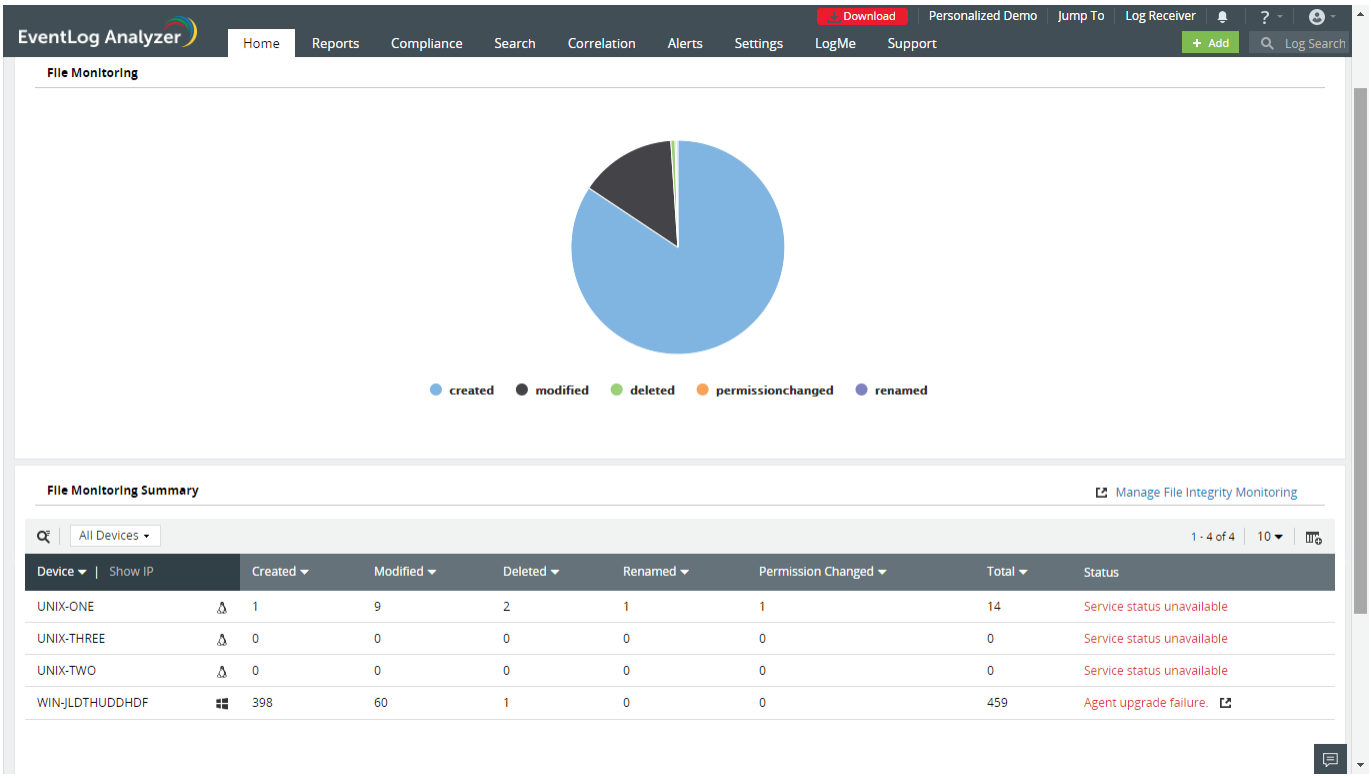
These files are the very foundation upon which your network and business run. The files and their various configurations dictate how your systems operate; they store your business data, determine how various business activities are carried out, and log all network activity.

The ripple effects caused by modifications to these files can be disastrous. A deleted log file could cause you to completely miss a security incident while attackers siphon off your business data. It could also hinder your forensic investigation after you discover the incident and could potentially lead to serious charges against your company for non-compliance.

A single corrupted system file may cause a critical server to crash, resulting in downtime your business can't afford. Furthermore, changes made to the folders where sensitive data are stored can also become cause for concern. For example, malware inserted at critical locations may aid attackers in their efforts to take over your network.

Additionally, disastrous file changes may sometimes be solely the result of error or oversight. Apart from monitoring your files and folders for suspicious changes, FIM helps you track accidental file changes as well. Plus, it helps you remain compliant with important regulatory policies such as PCI DSS and HIPAA.

Highlights of FIM with EventLog Analyzer



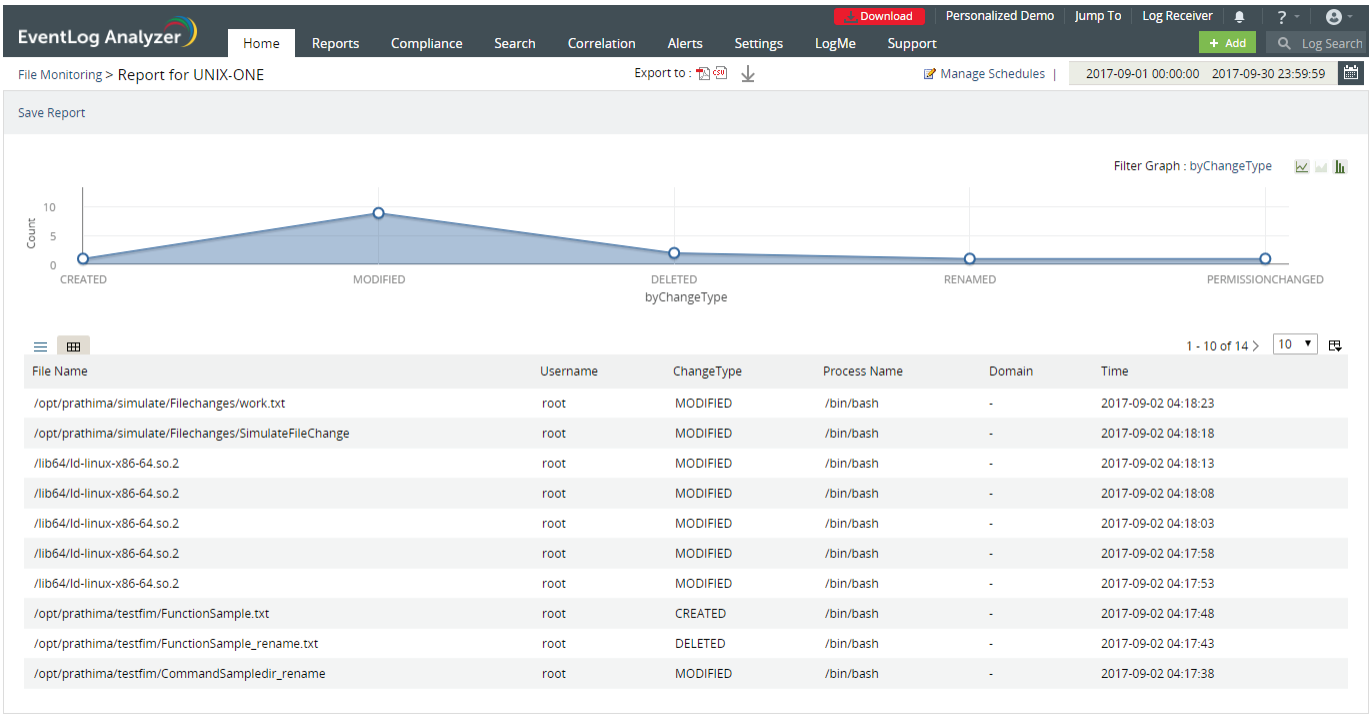
EventLog Analyzer's FIM module monitors critical data on your Windows and Linux systems for changes. This module is easy to use, and it allows you to review changes made to files across your network from a centralized console. Here are some of the highlights:

- **Easy configuration.** Setting up FIM using EventLog Analyzer requires minimal user effort. You can configure multiple devices simultaneously, and the required FIM agents will be automatically installed on these devices. All necessary audit policies, agent updates, and SACL settings are automatically updated.

- **High degree of control.** You can exercise control over the files and folders you wish to monitor. The following features provide you with granular control:

    - **Templates.** Create templates to group the file and folder locations you want to monitor, and apply them to as many devices as needed. By modifying these templates once, you can apply the change to all devices, even those previously configured using that template. Predefined templates are also provided for common critical files and folders.

    - **Filters.** You can choose to include or exclude subfolders, specific files, or file types.



- **In-depth reports and alerts.** The FIM dashboard gives you an overview of all changes made to files and folders you're monitoring. Reports and alerts are also available for each independent device being monitored. These reports give you details on the following changes:

  - **Creations.** Know when files are created or copied into critical folders. This helps you identify and stop the spread of malware.
  - **Modifications.** Track changes to important files and prevent malicious changes from corrupting sensitive data.
  - **Deletions.** Protect yourself from data loss by identifying sensitive files that have been deleted, so you can immediately restore them from a backup.
  - **Renames.** Identify files which have been moved or renamed. Several applications depend on specific files, and an erroneous file move or rename can hinder smooth business operations.
  - **Permission changes.** Track permission changes and ensure that nobody gains unauthorized access to critical files.

- **Compliance.** Generate predefined compliance reports for various policies, including PCI DSS, FISMA, HIPAA, and the GDPR while providing details about various file operations as mandated.

Conclusion

Whether you're dealing with confidential business information, network settings, or configurations, files store a lot of data that's vital to the smooth functioning of your network and business. FIM is an essential process that every organization must follow in order to preserve data integrity and protect your network from attacks. With EventLog Analyzer's FIM capability, you can monitor files across Windows and Linux platforms with ease, ensuring they stay secure.