EventLog Analyzer
Training

ManageEngine EventLog Analyzer Training

This training is designed to equip users with the knowledge to work with EventLog Analyzer. In this training, you will learn about the best practices that helps you get started with EventLog Analyzer.

The duration of the course depends on the scope of work and is subject to consultation and implementation needs if any.

- Course Objectives
- Who Should Attend
- Course Agenda

Course Objective

EventLog Analyzer training shortens the learning cycle and makes your network staff manage your network more productively right away. At the end of this course you will be able to use EventLog Analyzer to:

- Centrally collect, archive, analyze, machine generated logs from heterogeneous systems, network devices and applications

- Generate user activity monitoring reports (PUMA reports), IT security and regulatory compliance reports (SOX, PCI, HIPAA, FISMA, GLBA, etc.)

- Make accurate capacity planning decisions, enforce security policies, perform compliance auditing and forensic investigation

Course Audience

If you are an IT Manager, Security Manager, System Administrator, Managed Security Service Provider (MSSP) and you want to deploy EventLog Analyzer in your environment for log monitoring. Basic knowledge about the event logs and syslogs is required.

Course Agenda

Introduction

- Description of the product
- Main features of the product
- Address the user problem

Install the software

- Check the minimum hardware requirement
- Supported operating systems for deployment
- Supported browsers for user interface
- Ports required for the software's use
- Procedure to install the software
- Install the software as service, application

Get Started

- Start the EventLog Analyzer
- Connect to EventLog Analyzer
- Configure hosts to send logs in real time
- Import application logs to process
- Import logs (syslog and event log) to process

Deployment Setup

- Configure users and access levels
- How to setup log collection filters
- Configure Mail, SMS server

Reports

- Types of reports - top, user activity, compliance, and trend
- Creating custom reports
- Customize existing reports
- Convert the search result as reports
- How to schedule report generation
- How to receive reports via email in various formats
- How to pin your customized reports to the dashboard for easy analysis

Compliance Reports

- PCI-DSS
- HIPAA
- FISMA
- SOX
- GLBA etc.,
- How to schedule compliance reports

Advanced Reports

- User activity reports
- Application reports
- IBM iSeries (AS/400) reports

Alerts

- Create alert profiles
- Get alerts notified via email, SMS
- Run program/ script on alert generation

Search

- Simple search
- Advanced search for forensic analysis

MSSP Setup

- Set up for MSSP - Rebranding
- Customize the dashboard

System Setup

- Group hosts for easy management
- Configure compliance reports
- Import archived log files to process
- Configure working hours for trending

Admin Setup

- Configure archive settings
- Enable external user authentication
- Email alert when the EventLog Analyzer stops collecting log data
- Access Eventlog Analyzer database
- View Eventlog Analyzer server details

Miscellaneous

- Calculate archive and index storage size and plan
- Configuring MS SQL database
- How to migrate PGSQL to MSSQL
- How to export and import report, alert, and filter profiles
- How/ When to use trouble shooting tools in EventLog Analyzer
- Backup and Maintenance tips
- Best Practices

Check out our Online KB pages and explore our Paid Training Programs.

Our Products

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus | DataSecurity Plus | SharePoint Manager Plus

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

$ Get Quote   ⬇ Download