EventLog Analyzer - Training

OEM: ManageEngine • Code: ME-EVENTLOGANALYZER

COURSE DESCRIPTION

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.

AUDIENCE PROFILE

- 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.

PREREQUISITES

- Basic knowledge about the event logs and syslogs is required.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- 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 OUTLINE

Module 1: Introduction

- Description of the product
- Main features of the product

- Address the user problem

Module 2: 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

Module 3: 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

Module 4: Deployment Setup

- Configure users and access levels
- Filter events to store into database
- Configure Mail, SMS server

Module 5: Search

- Simple search
- Advanced search for forensic analysis

Module 6: 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
- Use Ask ME to get routine customized reports

Module 7: Compliance Reports

- PCI-DSS
- HIPAA
- FISMA
- SOX

- GLBA

Module 8: Advanced Reports

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

Module 9: Alerts

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

Module 10: MSSP Setup

- Set up for MSSP - Rebranding
- Customize the dashboard

Module 11: System Setup

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

Module 12: 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

Module 13: Miscellaneous

- MySQL performance tuning
- Calculate archive and index storage size and plan
- Configuring MS SQL database
- How to migrate from MySQL to MS SQL database and vice versa

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