ZJML130522101

ManageEngine EventLog Analyzer 8.5

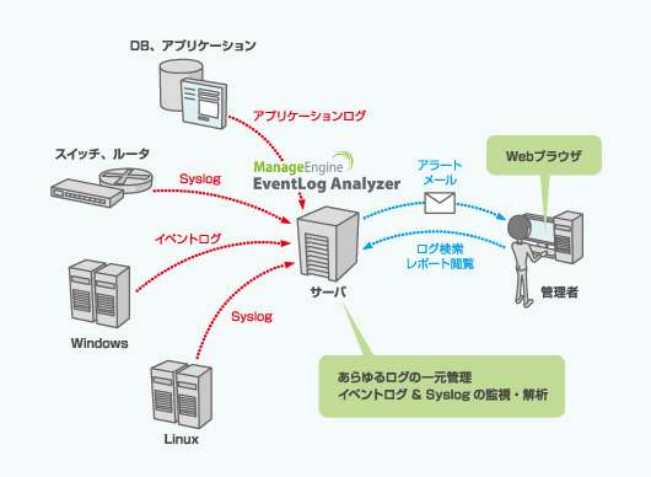
イベントログ・Syslog 対応 統合ログ管理ツール

製品概要

イベントログ、Syslog をはじめ、あらゆるログを収集、監視、解析する統合ログ管理ツール

ManageEngine EventLog Analyzer（マネージエンジン イベントログアナライザ、以下、EventLog Analyzer）は、世界 3,500 ユーザの導入実績を誇るログ管理ツールです。国内では、一般企業をはじめ、自治体、金融、大学、研究機関といった幅広い分野で利用されています。

EventLog Analyzer は、ネットワーク内の Windows ホストから出力されるイベントログや、Unix ホスト、ルータ、スイッチなどのネットワーク機器から出力される Syslog を収集し、ログデータをレポートとして生成することで、イベントの状況把握を可能にします。また、指定の条件に合致するログを受信した際にメールで通知し、24 時間いつでも、どこでも、システムやネットワークの問題を把握することが可能です。さらに、ネットワーク内のあらゆるログのインポートと検索に対応し、ログの一元管理を容易に実現します。

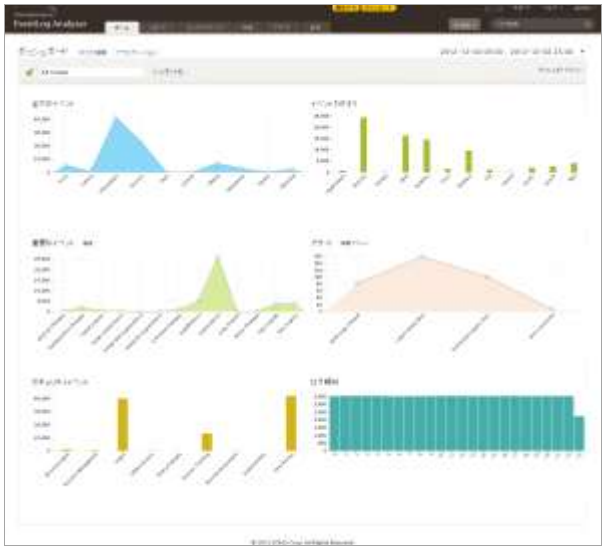


[EventLog Analyzer 利用環境イメージ]

特長

わかりやすいレポート画面

わかりやすい GUI デザインで、直観的に操作できます。



[EventLog Analyzer ダッシュボード画面]

イベント状況を即座に把握

収集したログを即座に解析し、レポート表示します。特定のホストやイベント単位でログを検索できます。設定した条件に合致するログを受信した際にアラート通知が可能です。

あらゆるログのインポートに対応

ミドルウェア、ソフトウェア等から出力される、任意形式のログのインポートに対応し、検索が可能です（暗号化されたログや、日本語を含むログには対応していません）。

[インポートしたログの一覧表示画面]

新機能

ファイル監視機能を追加【新機能】

Windows 環境において、特定のファイルやフォルダに対する操作を監視し、変更を検出した場合にログを生成して、即座に専用のタブでサマリをレポート表示します（日本語名が含まれるフォルダ/ファイルを監視対象とした場合、詳細レポートに反映されません）。すべての変更を取得し、監査証跡として一括管理できるので、データセキュリティの監査が容易になり、不正アクセス防止などのキュリティ対策に役立てることができます。

また、エージェントをインストールしてログ収集を行うため、ログのプレフォーマット処理を同時に行うことができ、収集性能が向上しています。

[ファイル監視の詳細レポート画面]

主な機能

ログ監視

（アラートの生成）

イベントの種類やメッセージのキーワード、イベントIDなど、任意の条件に当てはまるイベントが発生した時にアラートを生成し、管理者にログの異常を知らせます。指定したメールアドレスへのアラート通知だけでなく、スクリプトの実行も可能です。

（Syslog ビューアー）

ネットワーク機器等の各Syslogデバイスから送信されるSyslogをビューアーでタイムリーに確認できます。トラブルシューティング時の送信確認などに活用できます。

ログ管理

（ログの収集）

エージェントレス、またはリモートエージェントを使用して、Windows イベントログや Syslog を収集、管理します。WMI によるイベントログの取得、Syslog の受信が可能です。

（ログのインポート）

既存の Windows イベントログファイル(.evt/.evtx 形式)や Syslog ファイル、任意形式のログファイルを、ローカルから、またはFTP/SFTPを使用してリモートからインポートできます。定期インポート設定も可能です。

（ログのアーカイブ）

収集したログデータをファイル化し、ZIP 形式でアーカイブして自動的に保管します。アーカイブファイルを暗号化し、保管されたログの改ざんを検出します。

ログ解析

（レポートの生成）

収集したログを即座に解析し、レポートを表示します。イベント発生数の多いホストやユーザの一覧表示、ユーザごとの操作イベントのグラフ表示など、多様なレポートを生成します。米国 SOX 法、PCI DSS 等の規制法令に適合するコンプライアンスレポートも生成できます。また、組織のニーズに合わせたレポートのカスタマイズ、レポートの定期自動配信、CSV/PDF 形式でのエクスポートも可能です。

（ログの検索）

Web ブラウザ上で収集したログを特定のホストやイベント単位で検索できます。必要に応じて、生ログを用いた詳細な検索も可能です。

［ログ検索画面］

Edition と価格

機能比較	Professional Edition	Premium Edition	Distributed Edition
Windows イベントログ/Syslog の収集、ログ収集のスケジュール化	○	○	○
ログのアーカイブ(ZIP 化)/暗号化、アラート生成、レポート生成	○	○	○
Windows イベントログファイルのインポート	○	○	○
Syslog ファイル / 任意形式のログファイルのインポート	×	○	○
MS SQL Server （バックエンドデータベースとして利用）	×	○	○
Active Directory ベース認証	×	○	○
リモートエージェント(Windows 32bit/64bit 環境)	×	○	○
ファイル監視(Windows 32bit/64bit 環境)【NEW】	×	○	×
監視ホスト/アプリケーション数	10～500	10～500	200～5000
構成	単一サーバ	単一サーバ	2 階層分散サーバ
年間ライセンス料金 （消費税別、年間保守サポート付き）	¥68,000～	¥136,000～	¥1,062,000～
通常ライセンス料金 （消費税別、初年度保守サポート付き）	¥196,000～	¥490,000～	¥3,264,000～

動作環境

OS（32bit / 64bit）		CPU	メモリ	ディスク	ブラウザ
Windows	Server2003/2008/2008R2/2012、XP/Vista/7	32bit： 1GHz Pentium Dual Core Processor 64bit： 2.8GHz Xeon LV Processor 以上	2GB 以上	5GB 以上	Internet Explorer7.0 以上 Firefox 2.0 以上
Linux	Red Hat Enterprise Linux 4 以上				

主なログ解析対象			
OS	Windows - XP/ Vista/ 7、Server 2003/ 2008/ 2008R2/ 2012	Linux - Red Hat、Debian など	UNIX - Solaris、HP-UX など
ネットワーク機器	スイッチ・ルータ など、SNARE for Windows、IBM AS/400 - V5R1/ V5R2 / V5R3 / V5R4 / V5R5 / V6R1		
アプリケーション	Oracle、MS IIS W3C Web / FTP Server、MS SQL Server、DHCP Windows / Linux、VMWare、Apache Access、Print サーバなど		

☞ **無料で製品を評価できます！** EventLog Analyzer ダウンロード 検索

●このリーフレットの記載内容は、2013 年 5 月現在のものです。記載されている内容は事前の予告なしに変更する場合があります。
●製品に関するご質問、ご購入は、下記までお問い合わせください。

製品提供元
ゾーホージャパン株式会社
神奈川県横浜市神奈川区金港町 6-3 横浜金港町ビル 6 階
Tel:045-444-3881（ManageEngine 営業担当）
http://www.manageengine.jp/
E-mail: jp-mesales@zohocorp.com

お問い合わせ先

販売元