Adiscon IT-Solutions GmbH

Windowsイベントログ収集・監視ツール

EventReporter

使いやすく低コストで効果的
重要イベントを検出し、管理者に通知

Adiscon EventReporter は、1997 年に世界初の「Windows イベントログ収集管理と Syslog 転送」製品として開発されました。監査ログを収集管理することで必要なポリシーに準拠することができます。スタンドアローン製品としても、WinSyslog と連携しても利用できます。

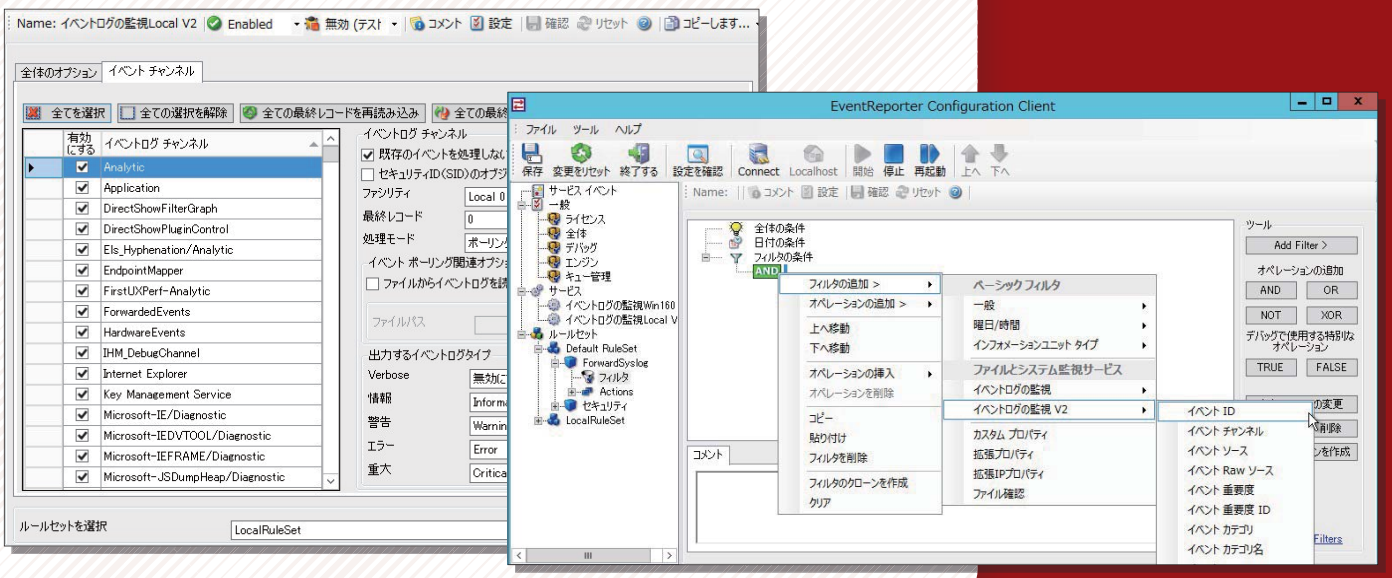
◆ 製品概要

Windowsイベントログ収集・監視が簡単！
重要なログを見逃さない

- 1 秒当たり 200 イベント以上の収集処理能力
- イベントログのメッセージをすべてプロパティごと (イベント ID, イベントユーザー , イベントタイプ等) に切り分けて保存しフィルターとして使用可能
- 多彩なフィルターによりログの絞り込みが可能
- 収集したイベントログをカスタムフォーマット、複数の文字エンコードで テキストファイルやデータベースに保存
- 既存ログサーバーに Syslog 転送、メール通知等、豊富なアクション機能
- リモート端末のイベントログもエージェントレスで収集可能 （監視端末 1 台につき 1 ライセンス必要）
- WinSyslog と連携することでログの互換性の高い集中管理が可能
- **SETP 転送機能**により、イベントログ独自のプロパティ情報も全て WinSyslog に転送可能（WinSyslog Enterprise 版のみ）

【SETP（Simple Event Transfer Protocol）とは】
Adiscon 社により開発された同社製品間の通信をより確実にするためのプロトコルです。

【SETP 転送するメリット】
Syslog 転送の場合、イベントログの内容はすべてメッセージプロパティに統合されて転送されますが、SETP 転送の場合は、EventReporter が保存したプロパティ情報（イベント ID, チャンネル等）がそのまま転送されます。これにより WinSyslog 側でもプロパティ値を使ったフィルタリングや、出力するフィールドのカスタマイズが可能となります。



ジュピターテクノロジー

◆ EventReporterの活用例

注視すべきイベント（システムやネットワークにおけるセキュリティ上の問題や障害イベントなど）をリアルタイムに検知して E メール通知し、把握

認証/監査ログのIDのみ抽出して特定フォルダにファイリング

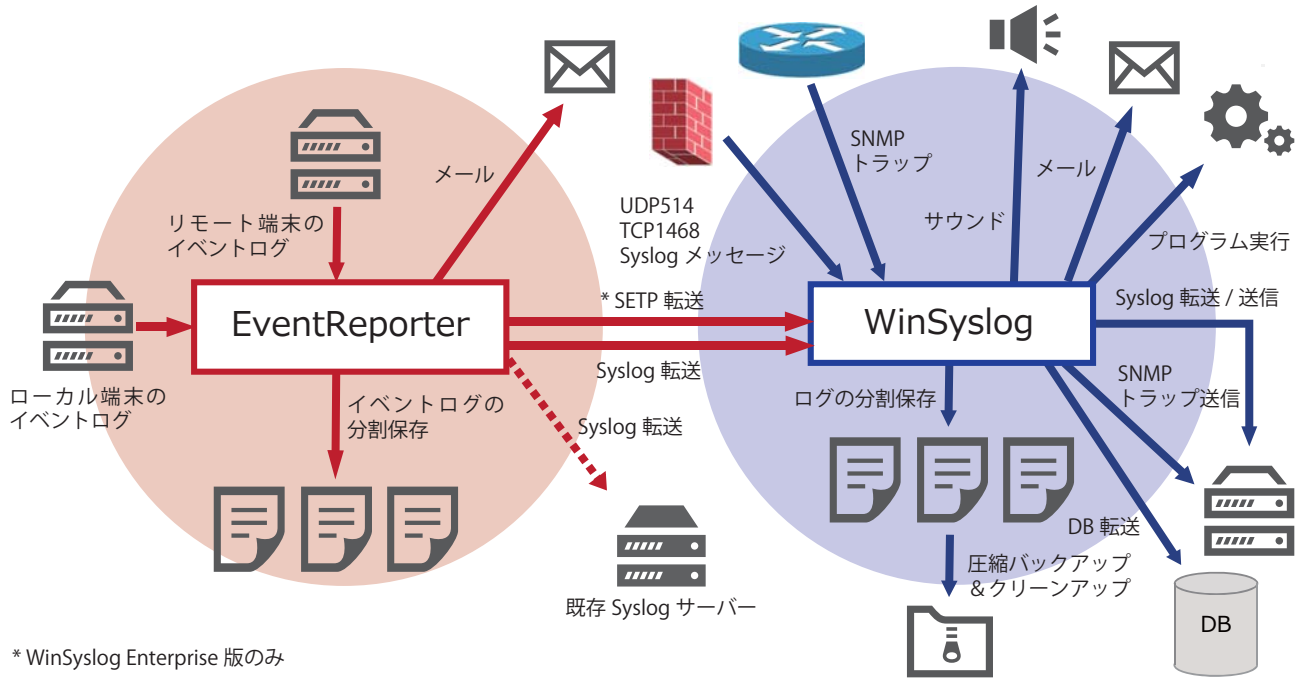
特定のイベントを抽出しSyslogもしくはSETP転送

解析用にフォーマットをカスタマイズして出力

脅威のイベント発生時に外部プログラムを実行

EventReporter と WinSyslog との連携イメージ

EventReporter と WinSyslog を連携利用することで、ログの集中管理が可能です。EventReporter で収集したイベントログを、WinSyslog に SETP プロトコルで転送します。受信したログは圧縮、暗号化することが可能で、アーカイブやバックアップもサポートされます。



◆ システム要件

Windows Server 2016、Windows 10、Windows 2012 R2、Windows 2012、Windows 8、Windows 7、Windows 2008、Windows 2008 R2、Windows Vista、Windows 2003、Windows XP、Windows 2000

H29.8.3

ジュピターテクノロジー
【本社】〒183-0023 東京都府中市宮町2-15-13 第15三ツ木ビル8F
TEL:042-358-1250　FAX:042-360-6221
【大阪営業所】〒530-0001 大阪府大阪市北区梅田1-1-3
大阪駅前第3ビル11F
TEL:06-6131-8471　FAX:06-6131-8472
【URL】http://www.jtc-i.co.jp/