ZJTM171229101

ManageEngine
EventLog Analyzer

EventLog Analyzer

エージェントベースのログ収集について

2017 年 12 月 29 日　発行

目次

1. はじめに 3
2. エージェントベースのログ収集 3
3. エージェントベースにおけるログ収集の流れ 4
4. エージェントベースのログ収集に必要な設定 4
5. エージェントの管理 6
6. セキュアなログ収集 6

1. はじめに

本ガイドでは、エージェントの使用が想定されるシナリオ、およびエージェントを使用した場合のログ収集の流れ等についてご案内します。

EventLog Analyzer(Windows 版)が Windows イベントログを取得する方法は、以下の 2 つです。

- **エージェントを使用しない(エージェントレスの)ログ取得**
- **エージェントを使用したログ取得**

企業様の機能要件、通信要件により適するログ取得方法が異なるため、本ガイドをご参照の上、エージェント利用をご判断ください。

2. エージェントベースのログ収集

EventLog Analyzer では、ファイアウォールや WAN をまたいだログ収集を行う場合など、監視対象のサーバーにエージェントをインストールすることでログの収集が可能です。

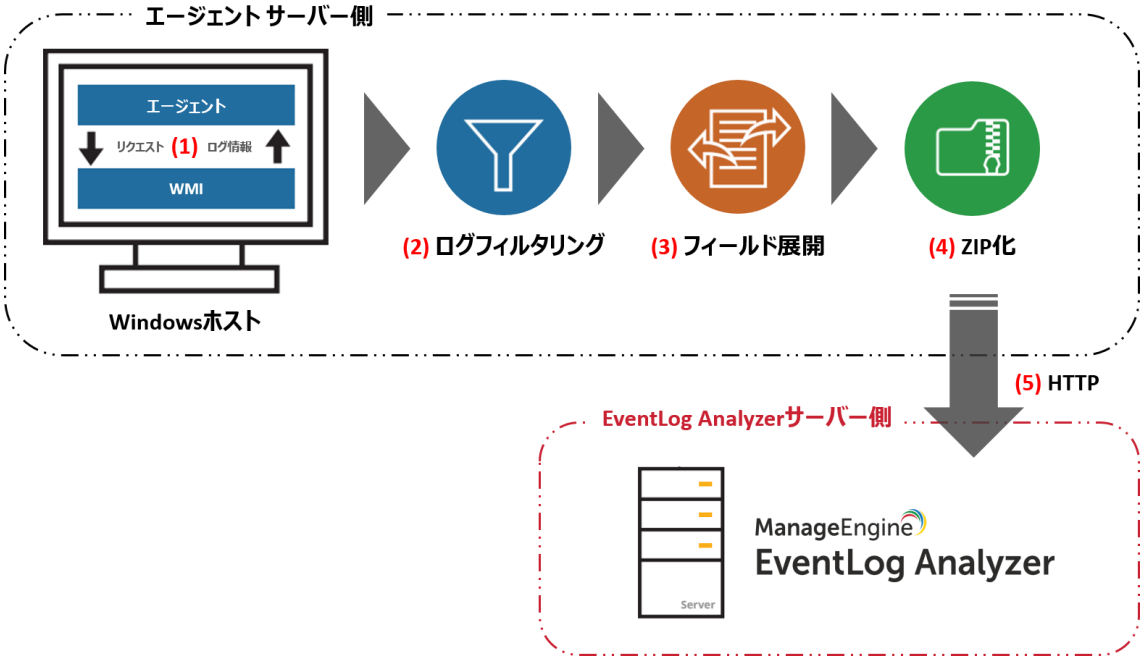
なお、エージェントの使用が想定されるシナリオとしては、以下が挙げられます。

- **組織の IT ポリシー上、Windows ホストにおいて WMI/DCOM の通信ポートを許可することができない場合（※Windows ホストとは、サーバー、ワークステーション、ドメインコントローラーを指しています）**
- **EventLog Analyzer サーバーとログ収集対象デバイス間でネットワーク接続の確立ができない場合**
- **ファイアウォールや WAN をまたいだログ収集を行う場合**
- **Windows のファイル監視を行う場合**

3. エージェントベースにおけるログ収集の流れ

エージェントベースの場合、以下の流れでログの取得が行われます。

(1) 自身がインストールされているサーバーへ WMI 接続を行い、ログデータを取得
(2) 取得したログに対してフィルタリングを実施
(3) ソースごとに定義されているフィールドの展開処理を実施
(4) ログデータを ZIP 化して保存
(5) HTTP プロトコルを使用して、EventLog Analyzer サーバーにログデータを転送



4. エージェントベースのログ収集に必要な設定

EventLog Analyzer は、デフォルトでエージェントレスのログ収集を行います。また、エージェントベースのログ収集を行っていた場合でも、エージェントがアンインストールされた際には、自動的にエージェントレスでのログ取得に切り替え、処理を継続します。以下では、エージェントベースでログ収集を行うために必要な、エージェントのインストール手順についてご案内します。

■ エージェントのインストール手順

1) 設定 > 管理者権限 > エージェントの管理 > **エージェントのインストール** をクリック

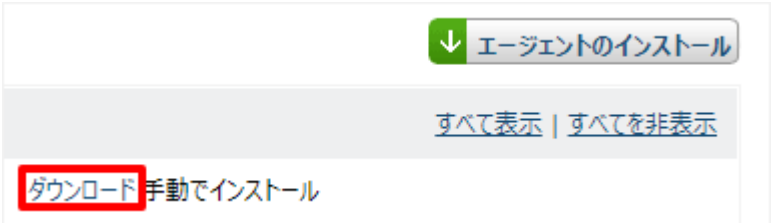
2) [エージェント名]に監視対象サーバーのホスト名/IP アドレスを入力
※複数のホストを同時に登録する場合は、[ホストスキャン]をクリックします。

3) [ドメイン名]にドメイン名を入力
※ドメインユーザーの認証情報を使用しない場合は、空白のままとします。

4) [ログオン名][パスワード]に管理者権限をもつアカウントの認証情報を入力
※入力した認証情報が正しいかを確認するためには、[ログイン情報の検証]をクリックします。

NOTE

ネットワーク接続の問題などにより、エージェントの自動インストールに失敗する場合は、インストーラーをダウンロードして、エージェントを手動インストールすることも可能です。なお、インストーラーは、「手動でインストール」という文字の左隣にある、[ダウンロード]リンクからダウンロードします。



5. エージェントの管理

エージェントは、設定 > 管理者権限 > **エージェントの管理** ページから簡単に管理を行うことが可能です。

このページでは、追加されているエージェントの一覧、サービスのステータスを確認することができ、更にサービスの再起動や停止を行うことが可能です。また、エージェントの編集やアンインストールをリモートから実行することが可能です。

NOTE

エージェントの編集はアンインストールといった操作を実行するためには、エージェントと EventLog Analyzer サーバー間が通信可能な状態である必要があります。

6. セキュアなログ収集

EventLog Analyzer はエージェントからのログ収集を安全に行うため、エージェントサーバーと EventLog Analyzer サーバー間のデータ転送の際、DES アルゴリズムを使用して暗号化を行っています。また、同様に TLS1.2 を使用した暗号通信にも対応しています。

■ お問い合わせ先 ■
ゾーホージャパン株式会社
〒222-0012 神奈川県横浜市西区みなとみらい三丁目 6 番 1 号 みなとみらいセンタービル 13 階
ホームページ：https://www.manageengine.jp/
EventLog Analyzer 製品ページ：https://www.manageengine.jp/products/EventLog_Analyzer/