ZJTP20265253475

ZOHO

ManageEngine
a division of Zoho Corp.

スタートアップガイド

Log management, auditing,
and IT compliance management for SIEM

ManageEngine
EventLog Analyzer

2026年 改訂

■著作権について
本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。

■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

■商標一覧
OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。
ManageEngineは、ZOHO Corporation Pvt.Ltd社の登録商標です。
なお、本ガイドでは、(R)、TM表記を省略しています。

目次

1. はじめに

1-1. 本ガイドについて

本ガイドではEventLog Analyzer Premium Editionのインストール方法、製品機能の概要、製品内の設定手順について説明しています。本ガイドは「**ビルド12581**」をもとに作成しています。

1-2. 対象読者

本ガイドは、製品を導入するシステム管理者を対象としています。

1-3. EventLog Analyzerの概要

ManageEngine EventLog Analyzerは、ネットワークイベントを監視・管理するWebベースのログ管理ツールです。ネットワーク内のWindowsデバイスや、Unixデバイス・ルーター・スイッチなどのSyslogを出力する機器からログデータをエージェントレスで収集します。収集したログデータは、レポートとしてWebブラウザーに表示されます。また、特定のログを受信した際に、あらかじめ定義した条件に基づき管理者に対するメール通知やスクリプトの実行、チケット管理システムとの連携などを設定することが可能です。

1-4. エディションの種類

EventLog Analyzerには、Premium EditionおよびDistributed Editionの2種類のエディション（Edition）があります。

- **Premium Edition**
  1つのEventLog Analyzerサーバーがログを収集する単一サーバー構成です。

- **Distributed Edition**
  複数のManagedサーバーと1つのAdminサーバーから成る2層構成です。Managedサーバーは、データの収集・解析を行い、Adminサーバーは、Managedサーバーが収集したログを参照することで、すべてのログデータを統合管理できます。ログ流量が多い場合や、異なる拠点のログを収集する場合に適した構成です。

＊各エディションの機能比較は、こちらのページをご参照ください。
＊本ガイドでは、Premium Editionのインストール方法を紹介しております。
Distributed Editionの設定方法は、こちらのナレッジをご参照ください。

2. システム要件

2-1. 最小ハードウェア要件

- **CPU：**6コア / 64bit
- **メモリー（RAM）：**16 GB 以上
- **ディスク空き容量：**1.2 TB 以上
- **ディスクタイプ：**HDD / SSD
- **IOPS：**150 以上
- **ネットワークカード通信速度：**1GB/s 以上

＊必要なサーバースペックは、収集するログの種類や量、製品設定により変動します。したがいまして、サーバースペックが充分であるか、必ず評価版にてご検証ください。ハードウェア要件の詳細については、動作環境ページをご参照ください。

2-2. オペレーティングシステム要件

- Windows 11
- Windows Server 2016 / 2019 / 2022 /2025
- Ubuntu 14 以降
- Red Hat Enterprise Linux 7 以降
- CentOS 7 以降

＊クライアントOSは評価目的でのみ利用可能です。本番環境にはサーバーOSをご利用ください。

2-3. データベース要件

- PostgreSQL
- Microsoft SQL Server

＊EventLog Analyzerには、デフォルトでPostgreSQLがバンドルされています。

2-4. Webブラウザー要件

- Google Chrome
- Mozilla Firefox
- Microsoft Edge（Chromium版）

＊各ブラウザーの最新バージョンの利用を推奨します。

3. ポート要件

EventLog Analyzerが使用するポートの詳細は、こちらのドキュメントをご参照ください。

4. 評価版インストーラーをダウンロード

評価版インストーラーは、こちらのページよりダウンロードできます。

インストール後30日間は、評価版としてPremium Editionのすべての機能が利用できます。また、評価期間中は、無料の技術サポートが提供されます。

30日の評価期間が終了した後にライセンスを適用しない場合、製品は自動的に無料版に移行します（無料版で管理可能なデバイス数：5台）。

＊評価版/無料版の詳細は、こちらのページをご参照ください。

なお、評価版または無料版にライセンスを適用することで、Premium Edition（製品版）に製品を移行できます。ライセンスの適用方法は、「9. ライセンスの適用方法」をご参照ください。

〇製品購入後の場合

製品購入後は、お客様専用サイト「ManageEngine Community」より、購入した製品のインストーラーをダウンロードできます。

ManageEngine Communityに保守ユーザーとしてログイン後、「購入済みの製品」タブの「インストーラー/サービスパック一覧」からインストーラーをダウンロードしてください。「購入済みの製品」タブの詳細は、こちらのマニュアルをご参照ください。

＊インストーラーをダウンロードするためには「保守ユーザー」としてログインする必要があります。ManageEngine Communityのユーザー登録（納品メール受領後の初回登録）方法の詳細は、こちらのマニュアルをご参照ください。2人目以降の保守ユーザーを追加で登録する場合は、こちらのマニュアルをご参照ください。

ManageEngine Communityに関するお問い合わせは、以下の窓口にご連絡ください。
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ゾーホージャパン株式会社
ManageEngine事業部　営業部　ライセンス担当
メール：jp-license@zohocorp.com
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

5. インストール手順

EventLog Analyzerのインストール手順を説明します。

- Windows環境でのインストール手順
- Linux環境でのインストール手順

5-1. 注意事項

- **アンチウイルスソフトやバックアップツールなどをインストールしている場合、こちらのドキュメントに記載のフォルダーをスキャン対象またはバックアップ対象から必ず除外してください。**スキャンまたはバックアップによりデータベースや重要ファイルが破損する可能性があるためです。

- Windows版のEventLog Analyzerをインストールすると、「ADAudit Plus」および「EventLog Analyzer」を1つのコンソール画面で管理可能な統合ツール「Log360」としてインストールされます。そのため、指定したインストールディレクトリに、「EventLog Analyzer」フォルダーの他に「Log360」フォルダー、「ADAudit Plus」フォルダー、「elasticsearch」フォルダーが作成されます。各フォルダーの詳細は、以下のとおりです。

    - **Log360：**EventLog AnalyzerおよびADAudit Plusを1つのコンソール画面で管理できるManageEngine製品
    - **ADAudit Plus：**Active Directory、Microsoft Entra ID、およびファイルサーバー監査に特化したManageEngine製品
    - **elasticsearch：**EventLog Analyzerがバンドルする検索エンジンデータベース

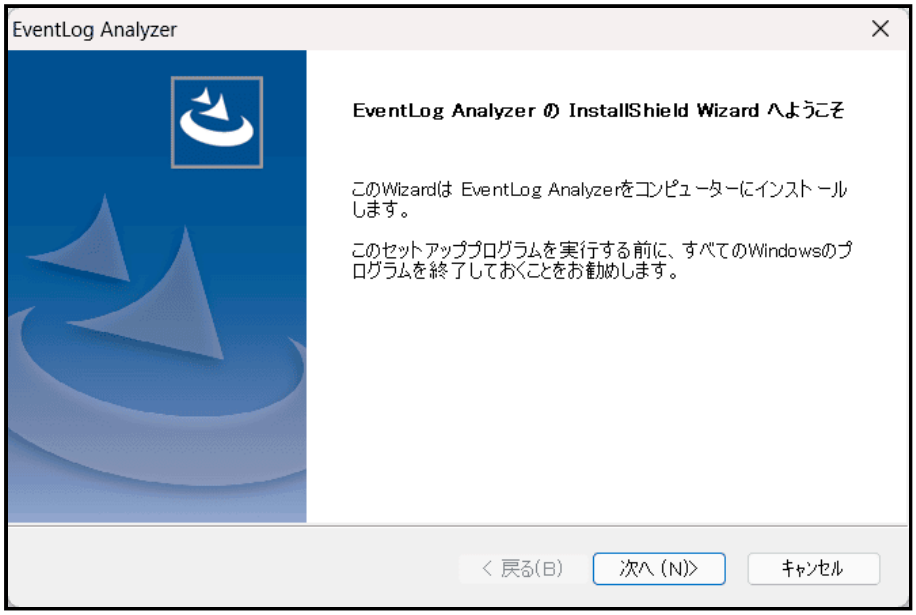
- **EventLog Analyzerのインストーラーを使用してインストールした「Log360」および「ADAudit Plus」はサポート対象外となります。**「Log360」または「ADAudit Plus」の利用をご希望の場合は、該当製品のインストーラーを使用して製品をインストールしてください。また、Log360およびADAudit Plusのアンインストールをご希望の場合は、弊社サポートまでお問い合わせください。

- Windows版とLinux版の機能差異の詳細は、こちらのドキュメントをご参照ください。

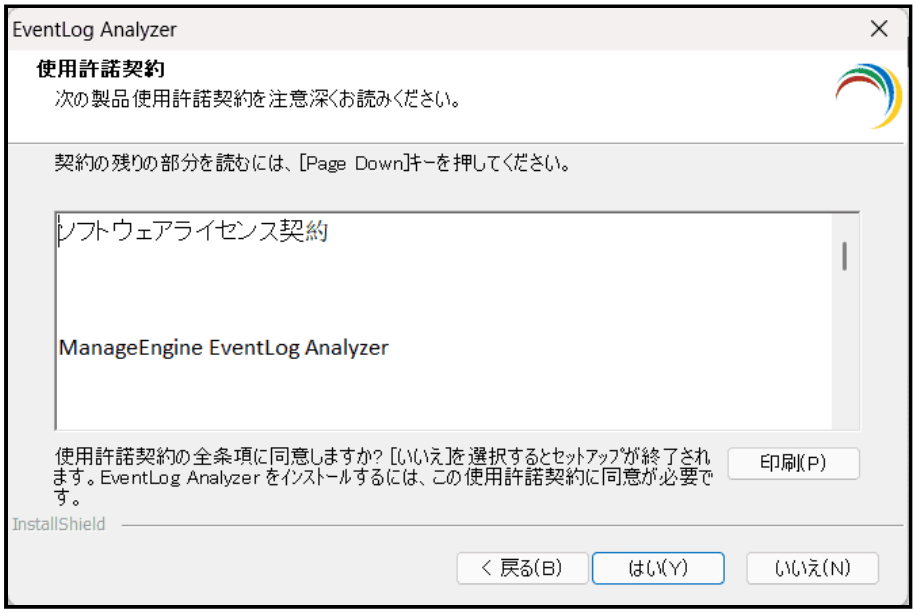
5-2. Windows環境でのインストール手順

1. インストーラー「ManageEngine_EventLogAnalyzer_64bit.exe」を管理者権限で実行します。

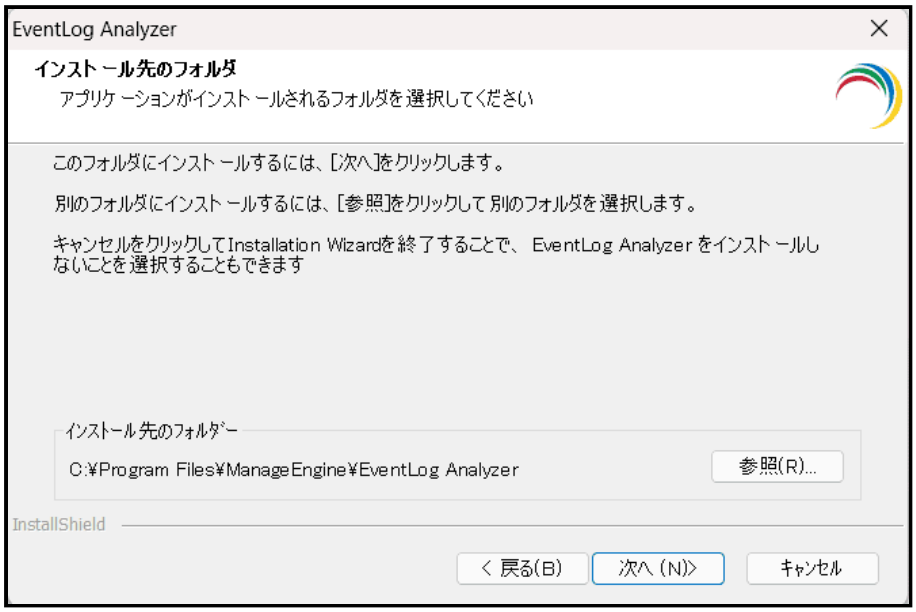
2. インストール画面が表示されるため、［次へ (N)>］をクリックします。



3. ライセンス条項を承諾後、［はい (Y)］をクリックします。

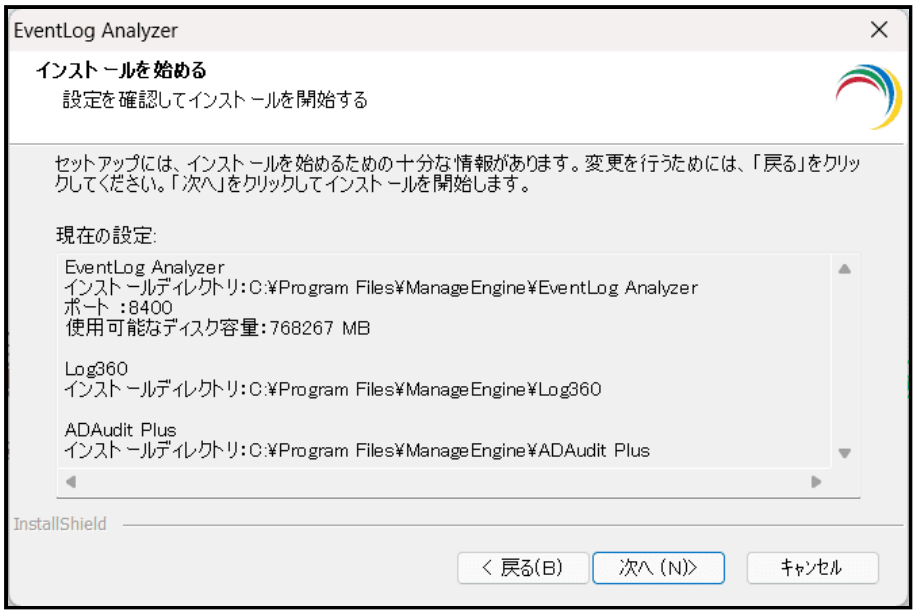


4. EventLog Analyzerをインストールするフォルダーを指定します。デフォルトは「C:¥Program Files¥ManageEngine¥EventLog Analyzer」です。変更する場合は［参照(R)...］をクリックします。設定後、［次へ (N)>］をクリックします。



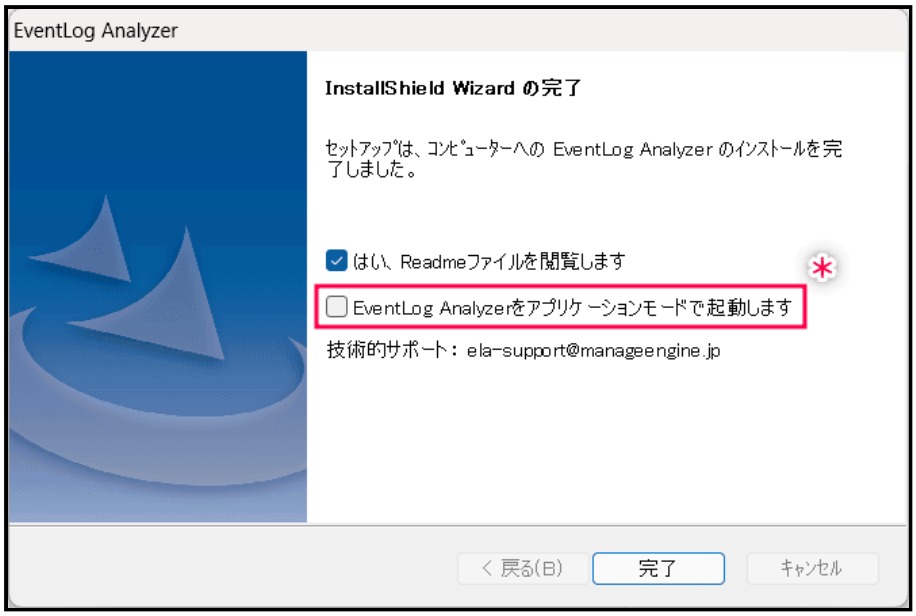
5. アンチウイルスソフトに関する警告画面が表示されるため、［OK］をクリックします。

6. EventLog Analyzerをインストールするかの選択を行います。インストールを行う場合は、［次へ (N)>］をクリックします。インストールが開始します。



7. 任意でお客様情報を入力後、［次 >］をクリックします。入力しない場合は［スキップ］をクリックします。

8. インストールの完了です。**各チェックボックスの詳細は以下に記載しています。**必要に応じて各チェックを外した後、［完了］をクリックします。



各チェックボックスの詳細

- **はい、Readmeファイルを閲覧します：**リリースノート情報を記載したページ（英語）が開きます。
- **EventLog Analyzerをアプリケーションモードで起動します：**Eventlog Analyzerがアプリケーション（コンソールモード）として起動します。

＊製品の性質上、バックグラウンドで常に起動することを推奨するため、アプリケーションではなく、サービスとして起動することを推奨します。サービスとして製品を起動する場合、［EventLog Analyzerをアプリケーションモードで起動します］のチェックを外した後に［完了］をクリックしてください。EventLog Analyzerをサービスとしてインストールする手順は、「EventLog Analyzerサービスのインストール手順（Windows環境）」をご参照ください。

5-3. Linux環境でのインストール手順

1. インストーラー「ManageEngine_EventLogAnalyzer_64bit.bin」を保存したパスに移動します。

2. コマンド「chmod u+x ManageEngine_EventLogAnalyzer_64bit.bin」を実行することで、ファイル実行権限を付与します。

3. コマンド「./ManageEngine_EventLogAnalyzer_64bit.bin -i console」を実行します。

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...
===============================================================================
ManageEngine EventlogAnalyzer                (created with InstallAnywhere)
-------------------------------------------------------------------------------
```

4. Enterキーを押下することでライセンス条項を確認します。

```
===============================================================================
Introduction
------------

InstallAnywhere will guide you through the installation of ManageEngine
EventlogAnalyzer.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation. If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE : Enter

===============================================================================
```

5. ライセンス条項を承諾する場合は「Y」を入力後、Enterキーを押下します。

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N) : Y
```

6. お客様情報を入力します。入力は任意です。入力しない場合は「N」を入力後、Enterキーを押下します。

```
Do you want to register for technical support?(Y/N) (Default: Y): N
```

7. EventLog Analyzerをインストールするディレクトリを指定します。デフォルトは「/opt/ManageEngine/EventLog」です。変更しない場合は、Enterキーを押下します。変更する場合は、インストール先の絶対パスを指定します。

```
===============================================================================
Choose Install Folder
---------------------

Where would you like to install?

    Default Install Folder: /opt/ManageEngine/EventLog

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: Enter
```

8. EventLog AnalyzerのWebポート番号を指定します。デフォルトでは「8400」を使用します。デフォルトのWebポート番号を使用する場合は、Enterキーを押下します。変更する場合は、ポート番号を入力後、Enterキーを押下します。

```
===============================================================================
Server Port Configuration
-------------------------

Server Port Configuration

Enter the EventLog Analyzer Web Server Port (Default: 8400): Enter
```

9. EventLog Analyzerをサービスとしてインストールするかどうか選択します。デフォルトでは「2」（サービスとしてインストールしない）が選択されているため、サービスとしてインストールする場合は「1」を入力、Enterキーを押下します。サービスとしてインストールしない場合は、何も入力せずにEnterキーを押下します。
＊製品の性質上、サービスとしてインストールすることを推奨します。
＊サービスは後からでもインストール可能です。サービスのインストール手順は、「EventLog Analyzerサービスのインストール手順（Linux環境）」をご参照ください。

```
================================================================================
Install As Service
------------------

Enter requested information

   1- Install EventLog Analyzer as Service
 ->2- Do not install EventLog Analyzer as a service

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED
CHOICES, OR
 PRESS <ENTER> TO ACCEPT THE DEFAULT: 1
```

10. インストール情報が表示されます。設定情報に問題がなければ、Enterキーを押下します。

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
   ManageEngine EventlogAnalyzer

Install Folder:
   /opt/ManageEngine/EventLog

Disk Space Information (for Installation Target):
   Required:  861.89 MegaBytes
   Available: 142,030 MegaBytes

PRESS <ENTER> TO CONTINUE: Enter
```

11. 以下のようにメッセージが表示されたら、Enterキーを押下してインストールを開始します。

```
===============================================================================
Ready To Install
----------------

InstallAnywhere is now ready to install ManageEngine EventlogAnalyzer onto
your system at the following location:

  /opt/ManageEngine/EventLog

PRESS <ENTER> TO INSTALL:  Enter
```

12. インストールが正しく行われたことを確認後、Enterキーを押下してインストーラーを終了します。

```
===============================================================================
Installation Complete
---------------------

Congratulations. ManageEngine EventlogAnalyzer has been successfully installed
to:

  /opt/ManageEngine/EventLog

PRESS <ENTER> TO EXIT THE INSTALLER: Enter
```

6. 起動と停止

EventLog Analyzerを起動する方法は、以下の2通りです。

- サービスとして起動する
- アプリケーションとして起動する

＊製品の性質上、バックグラウンドで常に起動することを推奨するため、アプリケーションではなく、サービスとして起動することを推奨します。

6-1. Windows環境での起動/停止

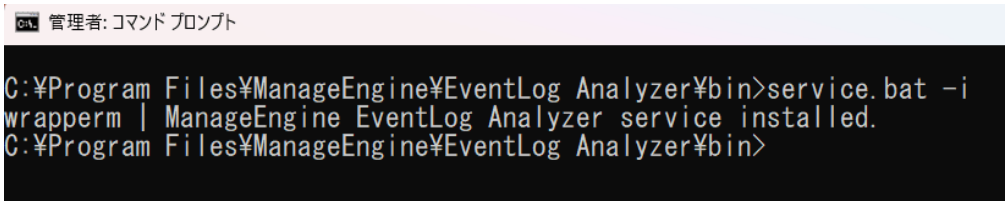
Windows環境でのサービスのインストール、起動、停止方法を説明します。

- EventLog Analyzerサービスのインストール手順（Windows環境）
- EventLog Analyzerサービスの起動手順（Windows環境）
- EventLog Analyzerサービスの停止手順（Windows環境）
- EventLog Analyzerアプリケーションの起動手順（Windows環境）
- EventLog Analyzerアプリケーションの停止手順（Windows環境）

EventLog Analyzerサービスのインストール手順（Windows環境）

EventLog Analyzerをサービスとしてインストールする手順は、以下のとおりです。

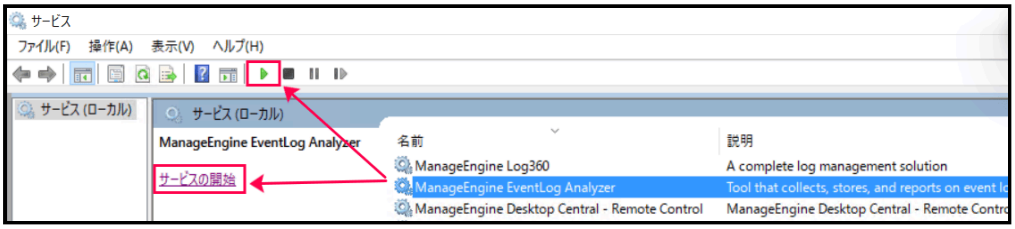
1. 管理者権限でコマンドプロンプトを起動します。
2. 「<EventLog Analyzer_インストールフォルダー>\bin」へ移動します。
3. コマンド「service.bat -i」を実行します。



EventLog Analyzerサービスの起動手順（Windows環境）

EventLog Analyzerサービスを起動する手順は、以下のとおりです。

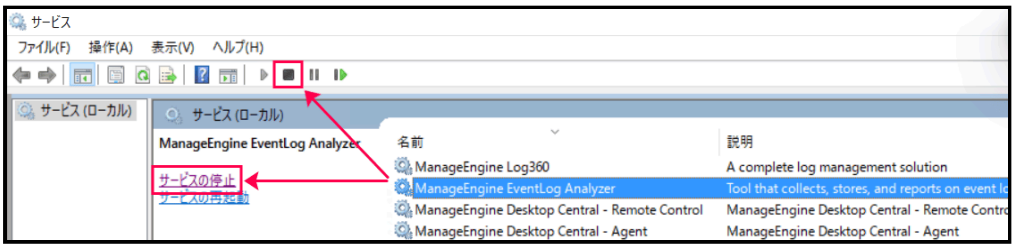
1. ファイル名を指定して実行（Windows + R）を開きます。
2. サービスを開くために「services.msc」を入力後、［OK］をクリックします。
3. サービス一覧から「ManageEngine EventLog Analyzer」を選択します。
4. 画面上部の開始アイコンまたは［サービスの開始］をクリックします。



EventLog Analyzerサービスの停止手順（Windows環境）

EventLog Analyzerサービスを停止する手順は、以下のとおりです。

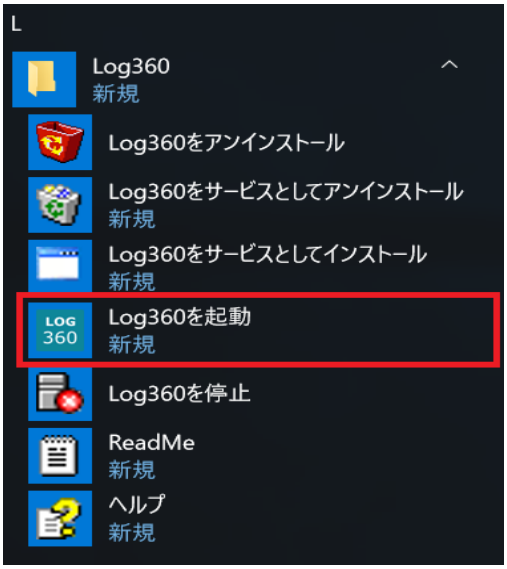
1. ファイル名を指定して実行（Windows + R）を開きます。
2. サービスを開くために「services.msc」を入力後、［OK］をクリックします。
3. サービス一覧から「ManageEngine EventLog Analyzer」を選択します。
4. 画面上部の停止アイコンまたは［サービスの停止］をクリックします。



EventLog Analyzerアプリケーションの起動手順（Windows環境）

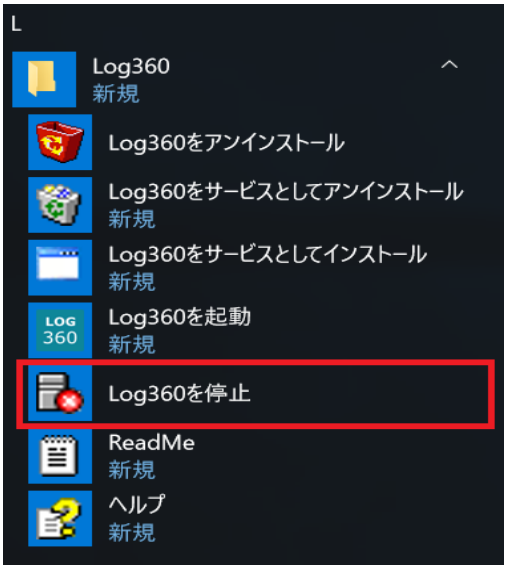
＊製品の性質上、サービスとして起動することを推奨します。
＊以下の手順を実施した場合、Log360の統合製品としてEventLog Analyzerが起動します。同時に起動するLog360はサポート対象外です。

［スタート］ → ［すべてのプログラム］ → ［Log360］ → ［Log360を起動］をクリックします。



EventLog Analyzerアプリケーションの停止手順（Windows環境）

［スタート］ → ［すべてのプログラム］ → ［Log360］ → ［Log360を停止］をクリックします。



6-2. Linux環境での起動/停止

Linux環境でのサービスのインストール、起動、停止方法を説明します。

EventLog Analyzerサービスのインストール手順（Linux環境）

EventLog Analyzerをサービスとしてインストールするためには、「<EventLog Analyzer_インストールフォルダー>/bin」へ移動し、以下のコマンドを実行します。

```
sh configureAsService.sh -i
```

例）
cd /opt/ManageEngine/EventLog/bin
sh configureAsService.sh -i

EventLog Analyzerサービスの起動手順（Linux環境）

EventLog Analyzerサービスを起動するためには、以下コマンドを実行します。

```
「systemctl start eventloganalyzer」または「service eventloganalyzer start」
```

EventLog Analyzerサービスの停止手順（Linux環境）

EventLog Analyzerサービスを停止するためには、以下コマンドを実行します。

```
「systemctl stop eventloganalyzer」または「service eventloganalyzer stop」
```

EventLog Analyzerアプリケーションの起動手順（Linux環境）

＊製品の性質上、サービスとして起動することを推奨します。

EventLog Analyzerをアプリケーションとして起動するためには、「<EventLog Analyzer_インストールフォルダー>/bin」へ移動し、以下のコマンドを実行します。

```
sh run.sh
```

例）
cd /opt/ManageEngine/EventLog/bin
sh run.sh

EventLog Analyzerアプリケーションの停止手順（Linux環境）

EventLog Analyzerアプリケーションを停止するためには、「<EventLog Analyzer_インストールフォルダー>/bin」へ移動し、以下のコマンドを実行します。

```
sh shutdown.sh
```

例）
cd /opt/ManageEngine/EventLog/bin
sh shutdown.sh

7. アンインストール手順

7-1. Windows環境でのアンインストール手順

1. EventLog Analyzerを停止します。

2. コントロールパネルを開き、［プログラム］ → ［プログラムと機能］に移動します。

3. ［Log360］を選択し、［アンインストール］をクリックします。

4. 表示されるウィザードにて、［EventLog Analyzerを削除します。］および［ADAudit Plusを削除します。］にチェックを入れ、［アンインストール］をクリックします。

5. アンインストール完了後、［完了］をクリックします。

6. インストールフォルダーが残っている場合、手動で削除します。

7-2. Linux環境でのアンインストール手順

1. EventLog Analyzerを停止します。
2. 「<EventLog Analyzer_インストールフォルダー>/_ManageEngine\ EventlogAnalyzer_installation」に移動します。

   例）
   cd /opt/ManageEngine/EventLog/_ManageEngine\ EventlogAnalyzer_installation

3. 以下のコマンドを実行します。

   ./Change\ ManageEngine\ EventlogAnalyzer\ Installation

4. ウィザードに従って、アンインストールを実施します。
5. インストールフォルダーが残っている場合、手動で削除します。

8. ログイン方法

1. JavaScriptの実行を許可した状態で、Google ChromeやMozilla FirefoxなどのWebブラウザーを起動します。

2. アドレスバーに「**http://<host_name>:<port_number>**」を入力します。

   - **<host_name>：**EventLog Analyzerが起動しているマシンのホスト名またはIPアドレス
   - **<port_number>：**EventLog AnalyzerのWebサーバーが使用するポート番号（デフォルト：8400）

   例）
   http://eventloganalyzer-server:8400

   ＊SSLを有効化している場合は、「**https**:/<host_name>:<port_number>」を入力します。

3. ユーザー名とパスワードを入力してログインをクリックします（デフォルトのユーザー名とパスワードはともに「admin」です）。

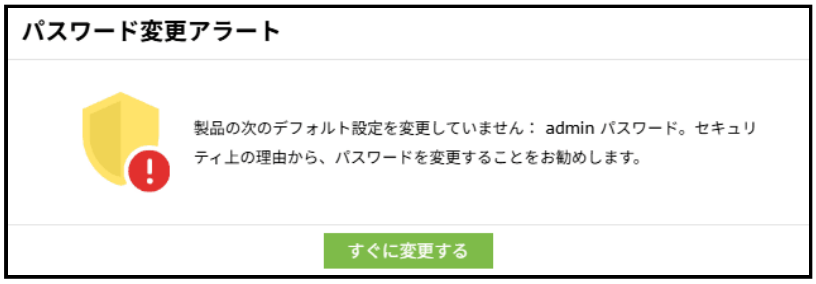
9. ライセンスの適用方法

1. EventLog Analyzerにログイン後、画面右上にある［?］→［ライセンス］をクリックします。

2. ［参照する］をクリックして、購入したライセンスファイルを選択します。

3. ［アップグレード］をクリックすることで、ライセンスを適用します。

4. 製品のデフォルト管理者アカウント（admin）のパスワードを変更していない場合、ライセンス適用後に［ライセンス詳細］画面を閉じるとパスワード変更を要求する通知が表示されるため、通知画面の［すぐに変更する］をクリックします。



5. ［現在のパスワード］に「admin」と入力します。

6. ［新しいパスワード］および「パスワードを確認する」に任意のパスワードを入力します。

   ＊新しいパスワードは、以下の条件を満たす必要があります。

   - 最大文字数：20
   - 最小文字数：8
   - 数字/英語小文字/英語大文字/特殊文字：それぞれ1つ以上

7. ［パスワードの変更］をクリックします。

10. 管理対象デバイスの追加方法

本ガイドでは、Windowsデバイスおよび Syslogデバイスの追加方法を説明します。その他の管理対象デバイス（ログソース）の設定方法は、ヘルプドキュメントをご参照ください。

10-1. Windowsデバイスの追加方法

Windowsデバイスの追加方法として、以下の3パターンを説明します。

- ドメイン/ワークグループからデバイスを追加する方法（Windows版）
- デバイスを手動で追加する方法（Windows版）
- Linux版のEventLog AnalyzerでWindowsデバイスを追加する方法

＊Windows版のEventLog Analyzerをインストールした場合、EventLog Analyzerは EventLog Analyzerをインストールしたサーバーや検出したドメインコントローラーなどのWindowsデバイスを製品の初回起動時に自動的に追加する場合があります。

ドメイン/ワークグループからデバイスを追加する方法（Windows版）

EventLog Analyzerにドメインまたはワークグループを追加すると、ドメインまたはワークグループに所属するデバイスを簡単に追加できるようになります。

1. ドメインの追加方法

1. ［設定］タブ →［管理者権限］→［ドメインとアカウント］に移動します。

2. ［ドメインを構成する］タブで画面右上の［+新しいドメインの追加］をクリックします。

   ＊ドメインに所属するサーバーにEventLog Analyzerをインストールした場合、該当ドメインが自動的に検出され、［ドメインを構成する］タブに追加されます。ドメインが既に追加されている場合は、ドメインの編集（鉛筆）アイコンをクリックし、正しくドメインコントローラーが検出されていることをご確認ください。ドメインコントローラーが正しく検出されている場合は、手順5以降を実施します。ドメインコントローラーが正しく検出されていない場合は、手順4以降を実施します。

3. ［ドメイン名］にドメイン名を入力します。

4. ドメインコントローラーのホスト名を入力するか、［ディスカバリー］をクリックすることでドメインコントローラーを追加します。

5. ［認証］にチェックを入れ、管理者権限（Domain Admins以上の権限）を持つユーザーの認証情報を入力します。管理者権限の認証情報を提供できない場合は、こちらのドキュメントに記載の手順で最小権限を持つユーザーを作成し、認証情報を入力します。

6. ［追加］または［編集］をクリックすることで、ドメインを追加します。

7. ドメインを追加後は、「3. デバイスの追加方法」を実施します。

2. ワークグループの追加方法

＊ドメインに所属するサーバーにEventLog Analyzerをインストールした場合、ワークグループを追加することはできません。ワークグループのデバイスを追加したい場合は、「デバイスを手動で追加する方法（Windows版）」をご参照ください。

1. ［設定］タブ →［管理者権限］→［ドメインとアカウント］に移動します。

2. ワークグループに所属するサーバーにEventLog Analyzerをインストールした場合、該当ワークグループが自動的に検出され、［ワークグループを構成する］タブに表示されます。

3. ワークグループの編集（鉛筆）アイコンをクリックし、［認証］にチェックを入れ、管理者権限を持つユーザーの認証情報を入力します。管理者権限の認証情報を提供できない場合は、こちらのドキュメントに記載の手順で最小権限を持つユーザーを作成し、認証情報を入力します。

4. ［編集］をクリックすることで、ワークグループの情報を更新します。

5. ワークグループを追加後は、「3. デバイスの追加方法」を実施します。

3. デバイスの追加方法

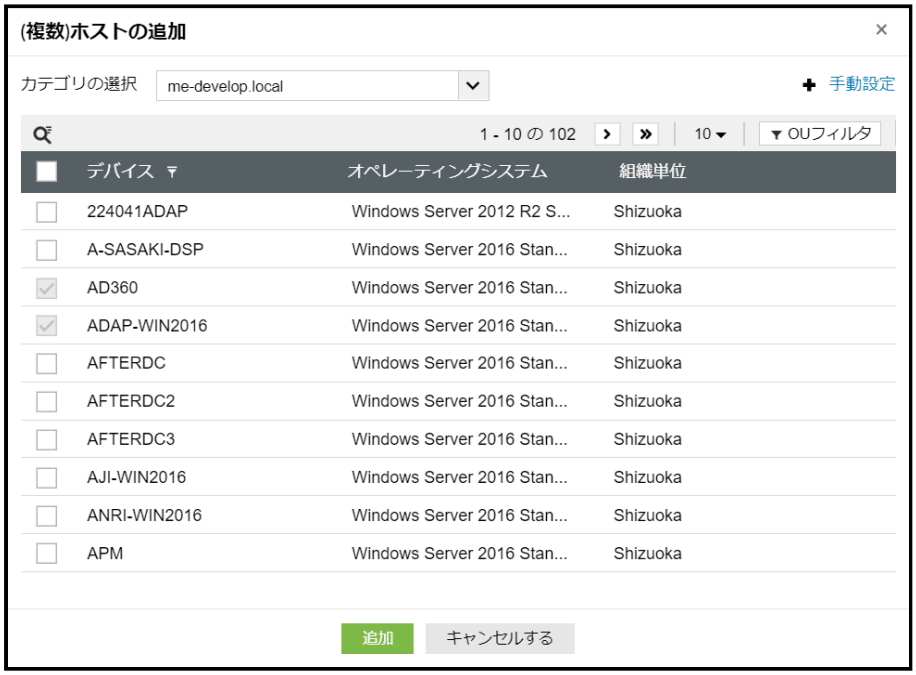
＊本ガイドでは、エージェントレスでのログ収集の設定方法を説明しています。
エージェントベースのログ収集を設定する方法は、こちらのドキュメントをご参照ください。

1. 以下のいずれかの方法でデバイスの追加画面に移動します。

   - 画面右上の［+追加］→［ホスト］をクリック
   - ［設定］タブ →［ログソースの構成］→［デバイスを管理］→［Windowsホスト］タブに移動し、画面右上の［+ (複数)ホストの追加］をクリック

2. ［カテゴリの選択］のドロップダウンメニューから管理対象として追加したいWindowsデバイスが所属するドメインまたはワークグループを選択します。

3. 選択したドメインまたはワークグループに所属するWindowsデバイスが一覧表示されるため、追加するデバイスにチェックを入れます。



8. ［追加］をクリックします。

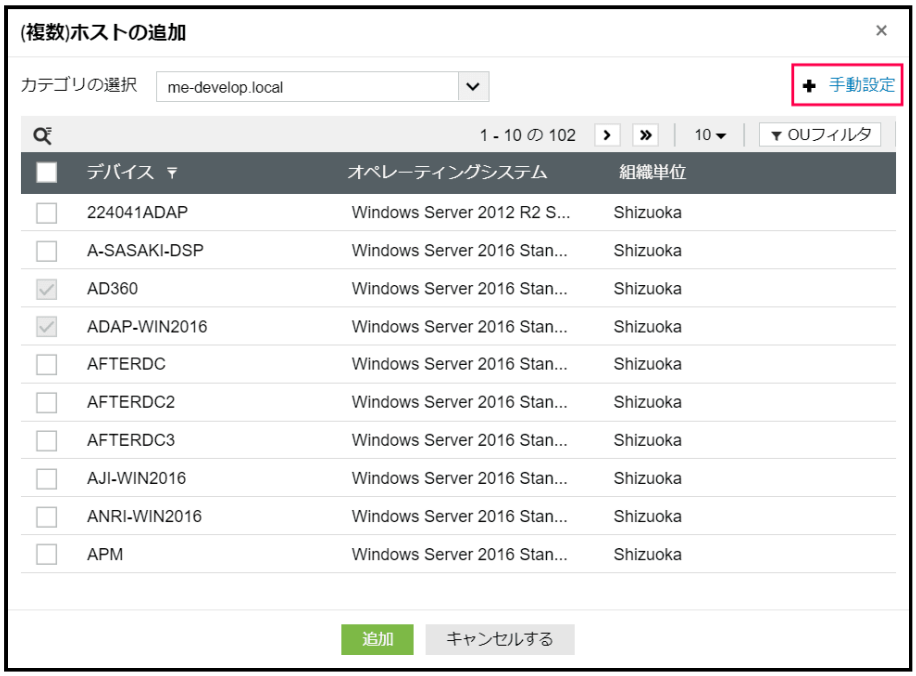
デバイスを手動で追加する方法（Windows版）

ドメインまたはワークグループを追加できない場合やデバイスを手動で追加したい場合は、以下の手順を実施します。

1. 以下のいずれかの方法でデバイスの追加画面に移動します。

   - 画面右上の［+追加］→［ホスト］をクリック
   - ［設定］タブ →［ログソースの構成］→［デバイスを管理］→［Windowsホスト］タブに移動し、画面右上の［+ (複数)ホストの追加］をクリック

2. 画面右上の［+手動設定］をクリックします。



3. 追加したいサーバーのホスト名またはIPアドレスを入力後、管理者権限を持つユーザーの認証情報を入力します。

4. ［追加］または［追加して閉じる］をクリックします。

Linux版のEventLog AnalyzerでWindowsデバイスを追加する方法

Linux環境にEventLog Analyzerをインストールした場合、Windowsデバイスからイベントログを収集するためには、Windowsデバイスにエージェントを手動でインストールする必要があります。管理対象のWindowsデバイスにエージェントをインストールすると、［設定］タブ →［ログソースの構成］→［デバイスを管理］→［Windowsホスト］タブに表示されます。エージェントを手動でインストールする方法は、こちらのドキュメントをご参照ください。

10-2. Syslogデバイスの追加方法

EventLog Analyzerは、バンドルしているSyslogサーバーを使用してSyslogを受信し収集します。そのため、追加したいSyslogデバイス側にて、SyslogをEventLog Analyzerサーバーに転送する設定を実施する必要があります。EventLog Analyzerは Syslogを受信後、該当Syslogデバイスを自動的に管理対象デバイスとして追加し、ログ収集を開始します。（EventLog AnalyzerのUI画面上でデバイスを手動で追加する必要はありません。）

Syslogデバイス側でのSyslog転送設定手順

＊本手順では、rsyslogでの設定手順（UDPで転送する場合）を解説しています。
rsyslog以外での転送設定手順は、各ベンダー様へお問合せください。

1. rootユーザーとしてSyslogデバイスにログインします。

2. vi等のテキストエディターで「/etc/rsyslog.conf」を編集します。

3. 以下のパラメーターを追加します。
   ＊「*.*」と「@」の間にはスペースを空けてください。

   ```
   *.* @<EventLog Analyzerサーバー名/IPアドレス>:<EventLog Analyzerが syslog受信に使用するポート番号>
   ```

   以下、EventLog AnalyzerサーバーのIPアドレスが192.168.0.1、使用するポート番号が514の場合の記述例です。

   ```
   例）
   *.* @192.168.0.1:514
   ```

4. 設定ファイル（rsyslog.conf）を保存します。

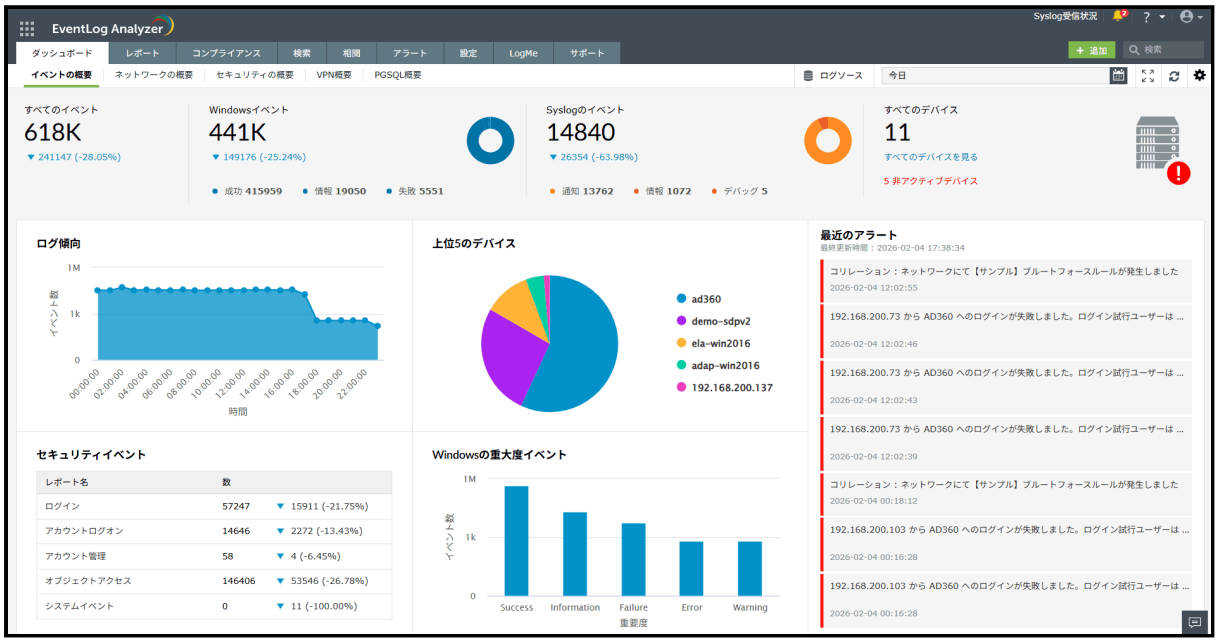
5. 設定変更を反映させるため、rsyslogを再起動します。

Syslogデバイスが自動追加されると、［設定］タブ →［ログソースの構成］→ ［デバイスを管理］→［Syslogデバイス］タブに表示されます。

11. 各タブの概要

11-1. ダッシュボード

ダッシュボードタブでは、収集した監査ログの概要がスナップショットとして表示されます。各種ログの流量に関する情報や、発生しているアラートを即座に確認することが可能です。また、表示する内容は環境に合わせてカスタマイズできます。



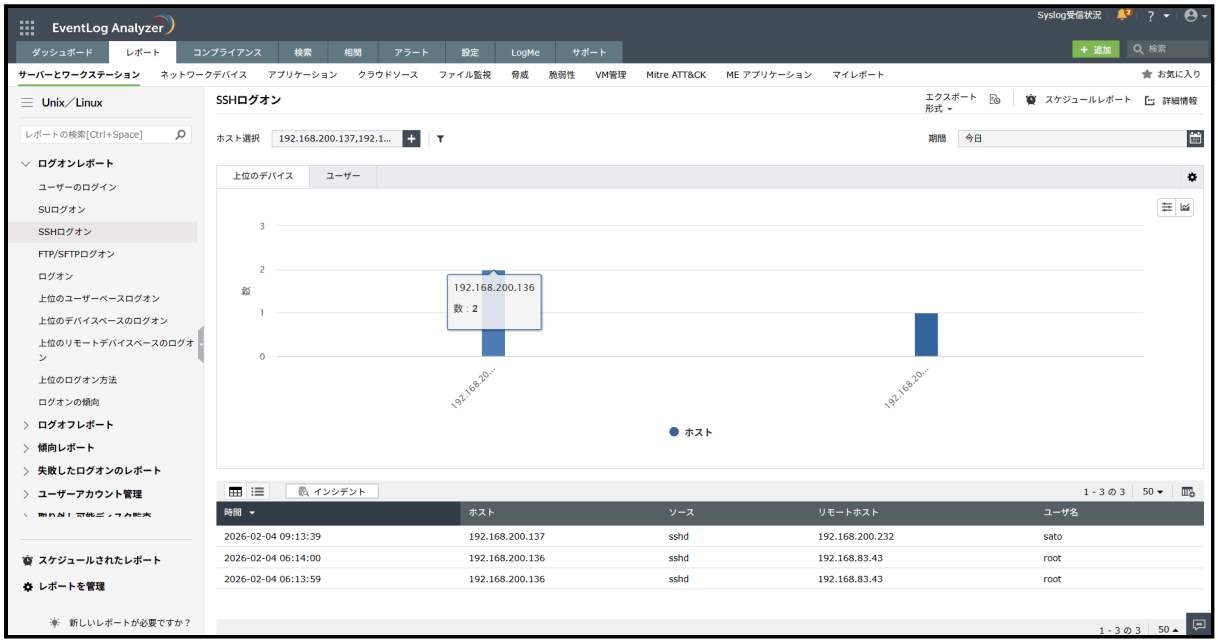
ダッシュボードタブの詳細は、以下のドキュメントをご参照ください。

- タブ
- ダッシュボード
- ダッシュボードのカスタマイズ

11-2. レポート

レポートタブでは、管理対象デバイスに関する定義済みレポートを確認できます。Windowsデバイス、Unix/Linuxデバイス、ネットワークデバイス、アプリケーションログに対して多くのレポートを用意しており、ワンクリックで状況を把握することができます。デフォルトで用意されているレポート以外のイベントを確認したい場合は、任意の条件でカスタムレポートを作成することも可能です。

また、日次や週次でレポートを自動的に出力し、管理者にメール通知するようスケジュールを設定することで、定期的なレポート生成にも対応できます。



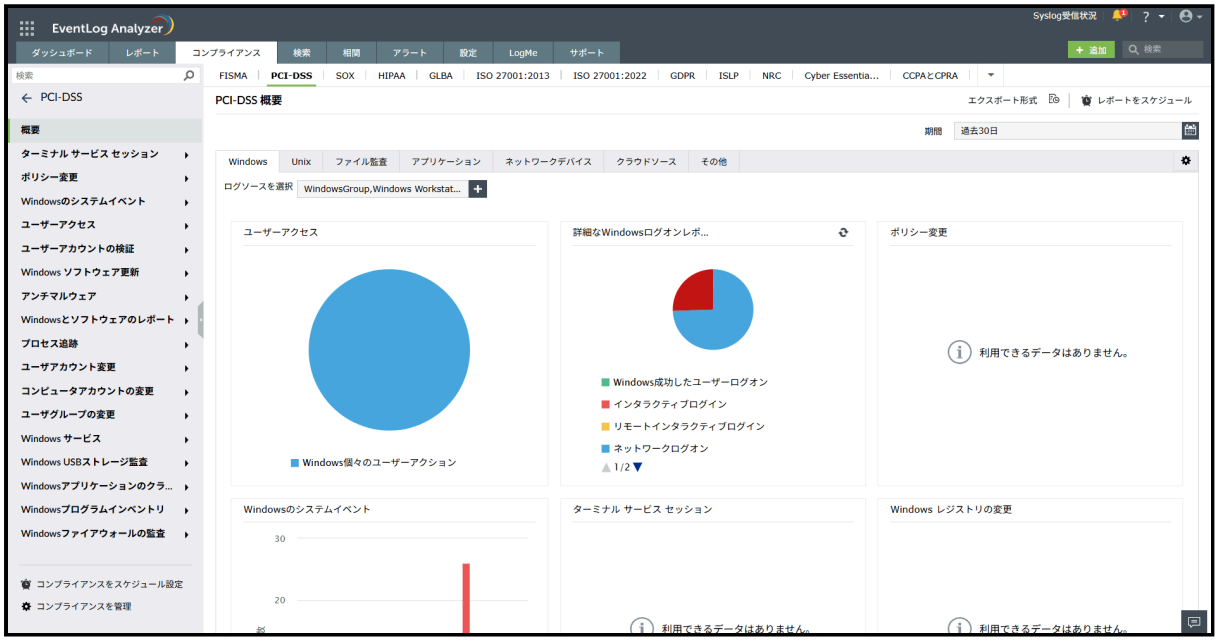
レポートタブの詳細は、以下のドキュメントをご参照ください。

- レポートの概要
- カスタムレポート
- レポートのスケジュール

11-3. コンプライアンス

コンプライアンスタブでは、様々なコンプライアンス要件への準拠に役立つレポートを生成できます。コンプライアンスレポートを生成することで、ネットワークのセキュリティポリシーに反した操作や挙動を容易に把握でき、コンプライアンス監査への対応をスムーズに行えます。

また、SQL Serverを管理対象としている場合、SQL Serverのセキュリティ設定がベストプラクティスに沿って設定されているかを確認できるセキュリティ状況機能も利用できます。

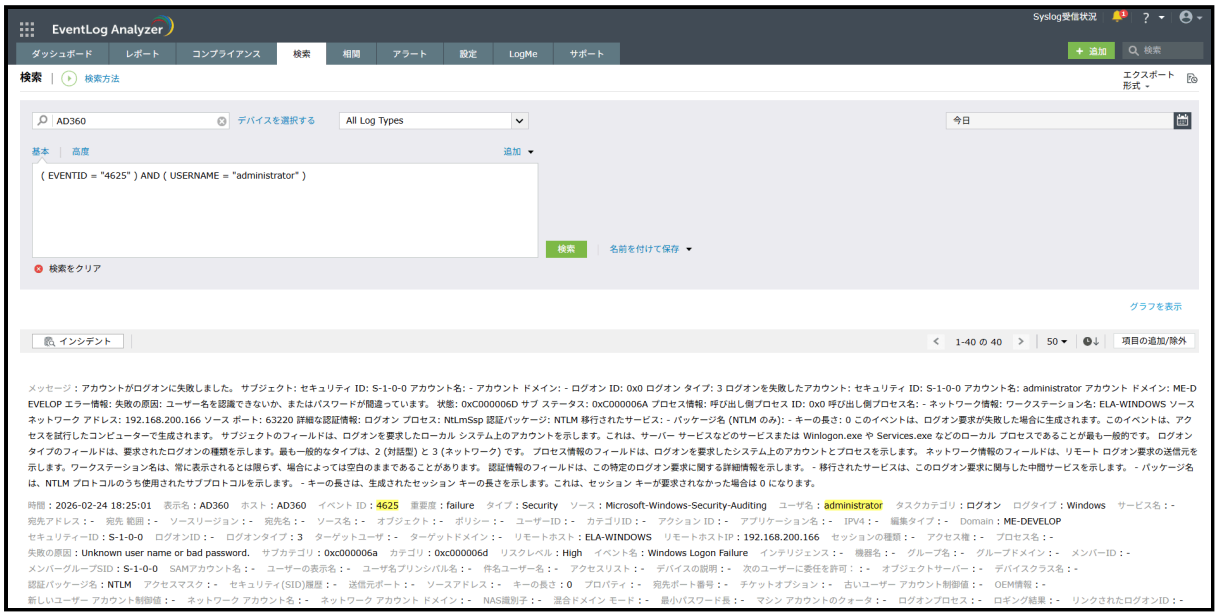


コンプライアンスタブの詳細は、以下のドキュメントをご参照ください。

- コンプライアンスレポート
- セキュリティ状況

11-4. 検索

検索タブでは、日時や対象デバイス、特定の条件を設定して収集したログを検索できます。検索クエリに関する知識がなくても直感的に使用でき、ログの詳細確認やインシデントの早期分析に役立ちます。



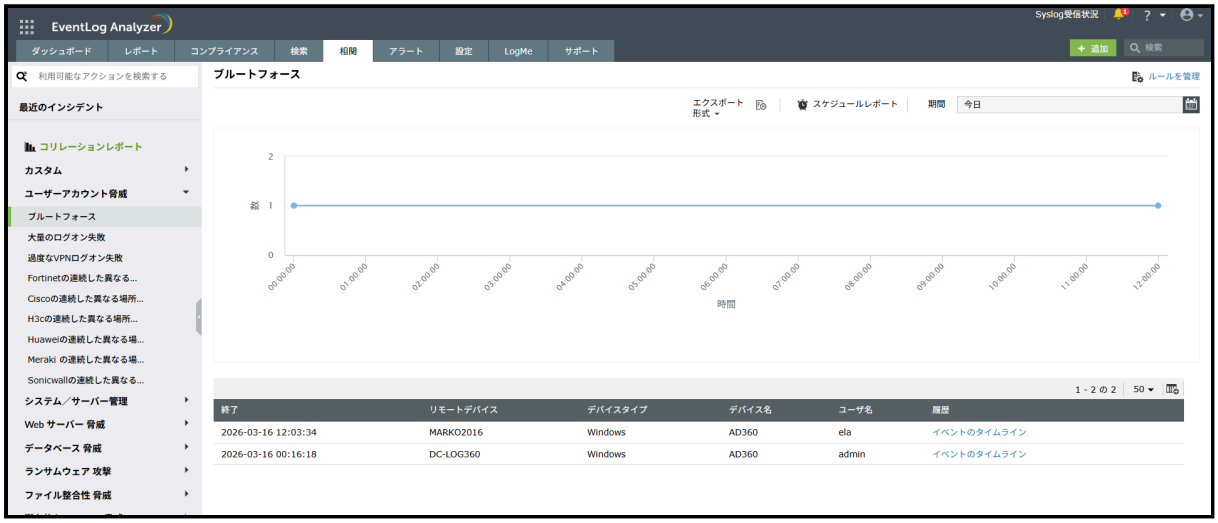
検索タブの詳細は、以下のドキュメントをご参照ください。

- ログの検索
- 検索の保存とエクスポート

11-5. 相関（コリレーション）

相関タブでは、異なるデバイスや異なるログタイプのログを相関的に分析して、ネットワーク内で発生している不審な挙動を検知できます。

例えば、VPNデバイスから収集したVPNログオンに関するログおよびWindowsデバイスから収集したソフトウェアインストールに関するログを相関付け、発生したイベント（VPN接続後にWindowsデバイス上でソフトウェアがインストールされた）の一連の流れを把握することができます。



相関タブの詳細は、以下のドキュメントをご参照ください。

- コリレーションの概要
- コリレーションレポート
- コリレーションルールの作成
- コリレーションルールの管理

11-6. アラート

アラートタブでは、あらかじめ設定した条件に合致するログを収集した際にアラートを生成することができます。アラート生成時には、管理者へのメール通知やワークフロー（2次アクション）の実行、連携したチケット管理ツールへのチケット起票を実行することも可能です。

EventLog Analyzerは、デフォルトで多くのアラートプロファイルを備えているため、簡単にアラートを設定できます。また、要望に合わせたカスタムアラートを設定することもできます。

アラートタブの詳細は、以下のドキュメントをご参照ください。

- アラートの概要
- アラートの表示
- アラートプロファイルの作成
- アラートプロファイルの管理
- ワークフロー
- チケット管理ツールとの連携

11-7. 設定

設定タブでは、ログ収集対象の管理や製品設定の変更など、さまざまな設定をカスタマイズできます。

以下、製品活用に役立つおすすめの製品設定を紹介します。詳細に関しては、各項目にリンクされているドキュメントをご参照ください。

- メールサーバー設定：EventLog Analyzerにメールサーバーを設定すると、アラートやスケジュールレポートなどの各種メール通知を受け取れるようになります。

- 接続設定：接続設定では、EventLog Analyzerに接続する際に使用するポート番号（デフォルト：8400）を変更できます。また、EventLog AnalyzerサーバーとWebブラウザー間の通信をHTTPSで暗号化するよう設定したり、Active DirectoryへのLDAP接続にSSLを使用するよう設定（LDAPSを有効化）することも可能です。

- ログ収集アラート：ログ収集アラートを設定すると、管理対象デバイスからのログ収集が停止している場合にメール通知を受け取ることができます。

- ログ収集フィルター：EventLog Analyzerでは、ログ収集フィルターを活用し、特定のログのみを収集対象としたり、特定のログを収集対象外とすることができます。ノイズとなるイベントや収集不要なイベントを収集対象外とすることで、ディスク容量の節約や製品パフォーマンスの向上が見込めます。

- ビジネス時間設定：EventLog Analyzer内でビジネス時間（業務時間）を設定すると、ビジネス時間内外に絞ったレポート出力やログ検索、アラート検知が可能になります。

- 技術者と役割：EventLog Analyzerでは、技術者（製品ユーザー）の役割（アクセス権限）を柔軟に設定できます。EventLog Analyzerを複数人で運用する場合は、適切な権限を持つアカウントを各担当者に割り振ることができます。

- ログイン設定：EventLog Analyzerでは、ログイン時のセキュリティ強化のために、技術者のパスワードポリシーを変更したり、CAPTCHAや二段階認証を設定することができます。

12. ログの保存期間に関する設定

EventLog Analyzerで効率的にログを長期保管するために必要な設定を紹介します。

12-1. 前提知識

EventLog Analyzerは、Windowsデバイスや Syslogデバイスからログを収集した後、収集したログに対して「インデックスデータ」と「アーカイブデータ」の2種類のデータを生成します。各データの詳細は、以下のとおりです。

- **インデックスデータ：**UI画面上（レポートタブや検索タブ）でログを参照するために必要なデータです。

- **アーカイブデータ：**ログの長期保管用に生成するデータです。アーカイブデータが書き込まれるファイル（フラットファイル）は、定期的にgz形式で圧縮されます。

インデックスデータとアーカイブデータには、それぞれ個別の保存期間が設定されており、保存期間を経過すると対象のデータが自動的に削除されます。EventLog Analyzerで効率的にログを長期保管するためには、各データにそれぞれ設定されている保存期間を適切に設定する必要があります。

インデックスデータの保存期間には参照頻度の高い直近のログの保存期間（ログを即座に参照する必要がある期間）を指定し、アーカイブデータの保存期間にはログを保管する必要がある期間を指定します。例えば、ログを1年間保管する必要があり、直近3か月のログは即座に参照する必要がある（頻繁に参照する）場合は、インデックスデータの保存期間を3か月、アーカイブデータの保存期間を1年に設定します。これにより、参照頻度の高い直近のログはいつでも即座に確認できる状態を維持しつつ、参照頻度の低い過去のログは圧縮した状態でディスク消費量を抑えながら長期保管することが可能となります。

また、インデックスデータの保存期間が経過し（インデックスデータが削除され）、UI画面上でログを参照できなくなった場合でも、アーカイブデータが存在する場合は「アーカイブをロード」を実施することで、アーカイブデータからインデックスデータを復元（再生成）できます。「アーカイブをロード」を実施することで、ログをUI画面上で参照可能な状態に戻せるため、インデックスデータの保存期間経過後もアーカイブデータの保存期間内であればログの可用性は担保されています。

12-2. ログデータの保存期間の設定方法

インデックスデータとアーカイブデータの保存期間の設定方法を説明します。

○インデックスデータの保存期間設定

インデックスデータの保存期間は［保持設定］画面から設定可能です。

1. ［設定］タブ → ［管理者権限］ → ［保持設定］に移動します。
2. ［現在の日数］の設定値（デフォルト：32日）を変更します。
3. ［編集］をクリックします。
4. 表示されるポップアップ画面にて、［承認］をクリックします。

＊インデックスデータはアーカイブデータに比べてデータサイズが大きく、保存期間を延ばした場合、レポート出力や検索クエリ実行処理の増加に伴う動作遅延や、保存データ量の増加に伴うディスク容量の圧迫が発生する可能性があります。そのため、**特別な要件がない場合はデフォルト設定（32日）の利用を推奨します。**アーカイブデータが存在する場合は「アーカイブをロード」を実施し、簡単にインデックスデータを復元できるため、不必要にインデックスデータの保存期間を延ばすのではなく、必要に応じてインデックスデータを復元（アーカイブをロード）する運用を推奨します。

保持設定画面では、インデックスデータの保存期間以外にも、アラートタブや相関タブで表示されるデータの保存期間も設定可能です。保持設定画面の各設定の詳細は、こちらのドキュメントをご参照ください。

○アーカイブデータの保存期間設定

アーカイブデータの保存期間は［アーカイブの設定］画面から設定可能です。

1. ［設定］タブ → ［管理者権限］ → ［アーカイブ］に移動します。
2. 画面右上の［設定］をクリックします。
3. ［アーカイブ保持期間］の設定値（デフォルト：無期限）を変更します。
4. ［保存］をクリックします。

アーカイブの設定画面では、アーカイブデータの保存期間以外にも、アーカイブの保存場所の変更や暗号化の有無の設定など、アーカイブデータに関する様々な設定を変更できます。アーカイブ関連の設定の詳細は、こちらのドキュメントをご参照ください。

12-3. アーカイブをロードする方法

インデックスデータの保存期間が経過したログを再度UI画面上から参照したい場合は「アーカイブをロード」を実施し、アーカイブデータからインデックスデータ復元する必要があります。

アーカイブをロードする方法は、以下のとおりです。

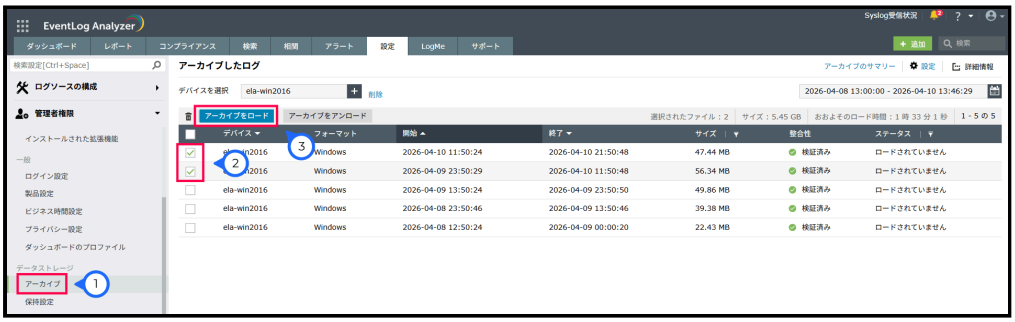
1. ［設定］タブ → ［管理者権限］ → ［アーカイブ］に移動します。

2. 対象のアーカイブのチェックボックスにチェックを入れます。

   ＊画面左上の［デバイスを選択］や画面右上のカレンダーアイコンから、対象のアーカイブをフィルタリングできます。

   ＊参照するためにロードが必要なアーカイブには、［ステータス］列に「ロードされていません」または「データの一部が利用可能です。」と表示されています。「データの一部が利用可能です。」と表示されているアーカイブは、一部のインデックスデータが既に存在することを意味します。ロードを実施すると、UI画面上に表示されるログが重複する可能性があります。

3. ［アーカイブをロード］をクリックします。



ロードが完了すると、［ステータス］列の表示が「ロード済み」に変わり、レポートタブや検索タブでログを参照できるようになります。

ロードしたデータは、アーカイブの設定画面のロード保持期間（デフォルト：7日）を経過すると自動的にアンロードされます（ロードにより復元したインデックスデータが削除されます）。ロード保持期間を経過する前に復元したインデックスデータが不要となった場合は［アーカイブをロード］の隣に表示される［アーカイブをアンロード］をクリックし、手動でアンロードすることも可能です。

13. トラブルシューティング、FAQ

トラブルシューティング

こちらのヘルプドキュメントをご参照ください。

FAQ

こちらのヘルプドキュメントをご参照ください。

Windowsデバイスの登録が失敗する

こちらのナレッジをご参照ください。

Syslogデバイスの登録が失敗する

こちらのナレッジをご参照ください。

エージェントを使用したログ収集が失敗する

こちらのナレッジをご参照ください。

デフォルト管理者（admin）のパスワードを忘れた

サポート窓口までお問い合わせください。

14. お問い合わせ

価格、お見積りなど営業に関するお問い合わせ

https://www.manageengine.jp/purchase/

評価版ご利用中のお客様向け技術サポート

https://www.manageengine.jp/support/trial.html

保守サポート契約締結のお客様向け技術サポート

https://www.manageengine.jp/support/purchased.html

その他製品に関するお問い合わせ

https://www.manageengine.jp/contact.html

会社情報

ゾーホージャパン株式会社 ManageEngine 事業部
〒220-0012 神奈川県横浜市西区みなとみらい3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/