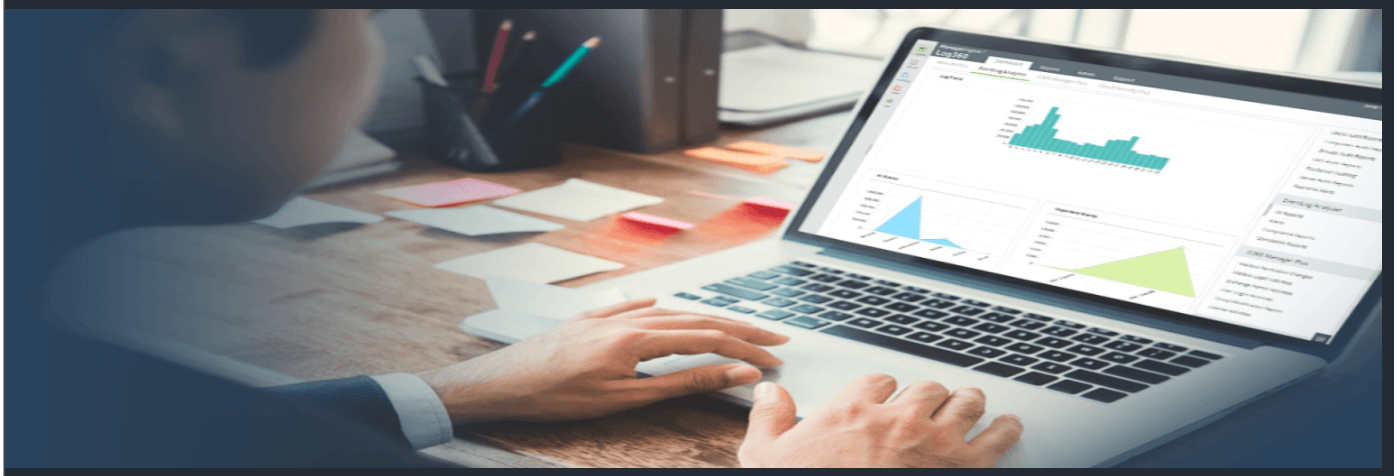
ZJTP20242282023



Log management, auditing,
and IT compliance management for SIEM

スタートアップガイド

ManageEngine
EventLog Analyzer

2024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**12400**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ホストや、Unixホスト・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へ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という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監視できます。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。

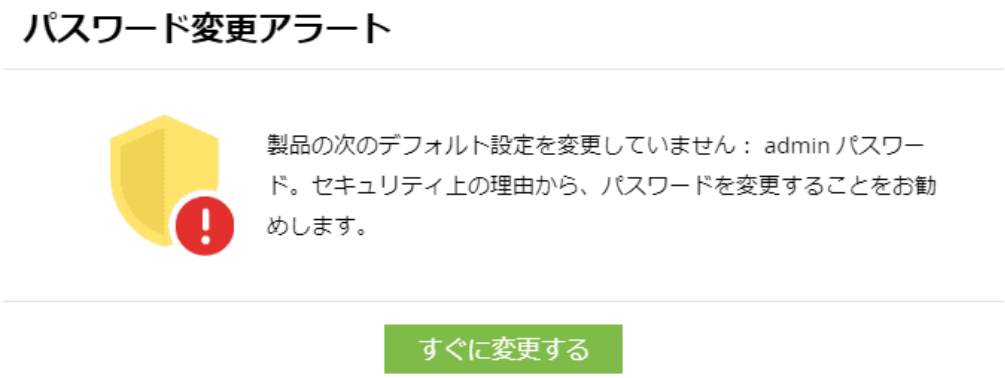
＊各エディションの機能比較は、こちらのページをご参照ください。
＊本ガイドでは、Premium Editionのインストール方法を紹介しております。
Distributed Editionの詳細はこちらのナレッジベース、設定方法はこちらのナレッジベースをご参照ください。

1-5 評価版からPremium Editionにアップグレードする方法

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

2. [ライセンスファイルを選択]の[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、ライセンスが適用されます。

4. ライセンスを適用後、製品のデフォルト管理者アカウント（admin）のパスワード変更を要求する通知が表示されますので、[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。
7. [パスワードの変更]をクリックします。

新しいパスワードを設定する際、満たす必要がある条件は以下のとおりです。

- 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**

2. システム要件

2-1 最小ハードウェア要件

- **CPU**：6 Core / 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

＊上記値はOS依存分を除きます。詳細なハードウェア要件はこちらのページをご参照ください。

2-2 サポートOS

- Windows 10 / 11
- Windows Server 2016 / 2019 / 2022
- CentOS 7
- Red Hat Enterprise Linux 7

＊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 サポートWebブラウザー

- 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。

2-4 解析可能なログレコード数

- Windowsイベントログ：3000/秒
- Syslog：20,000/秒

＊解析可能なログレコード数は、サーバーのスペックおよびネットワーク環境により変動します。したがいまして、ログ流量に対する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。

3. ポート要件

EventLog Analyzerは以下のポートを使用します。

通信方向	TCP/UDP	ポート番号	解説
inbound	TCP	8400 *変更可能	WebブラウザーでEventLog Analyzerに接続する際に使用します。
Local	UDP	5000-5002	収集したログを内部処理する際に使用します。
outbound	TCP	135 139 445	Windowsホストからログを収集する際に使用します。
inbound	TCP	49152-65534	Windowsホストからログを収集する際に使用します。
inbound	UDP	513 514 *変更可能	Syslogを受信する際に使用します。
inbound	TCP	514 *変更可能	Syslogを受信する際に使用します。
Local	TCP	33335 *変更可能	製品にバンドルされているPostgreSQLデータベースによって使用します。
Local	TCP	9300-9400	製品にバンドルされているElasticsearchによって使用します。
outbound	TCP	445	IISサイト監視の際に使用します。

outbound	TCP	446-449 8470-8476 9470-9476	IBM AS/400監視の際に使用します。
inbound	TCP	8400	エージェントとの通信に使用します。

＊変更可能なポート番号の変更手順はこちらのナレッジベースをご参照ください。

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。

ダウンロード時から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。なお、30日の評価期間が終了後、ライセンスを適用しない場合、自動的に無料版に移行します（無料版の可能監視対象数：5ホスト）。

＊監視対象数が5を超えていた場合、引き続き監視したいものを5つ選択した後に、利用開始可能です。

5. インストール手順

インストール手順を説明します。

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、EventLog Analyzerをインストールした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。**除外しない場合、スキャンまたはバックアップによってデータベースが破損する可能性があります。

- Windows版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できる統合ツール「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」の他、「Log360」「elasticsearch」および「ADAudit Plus」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。

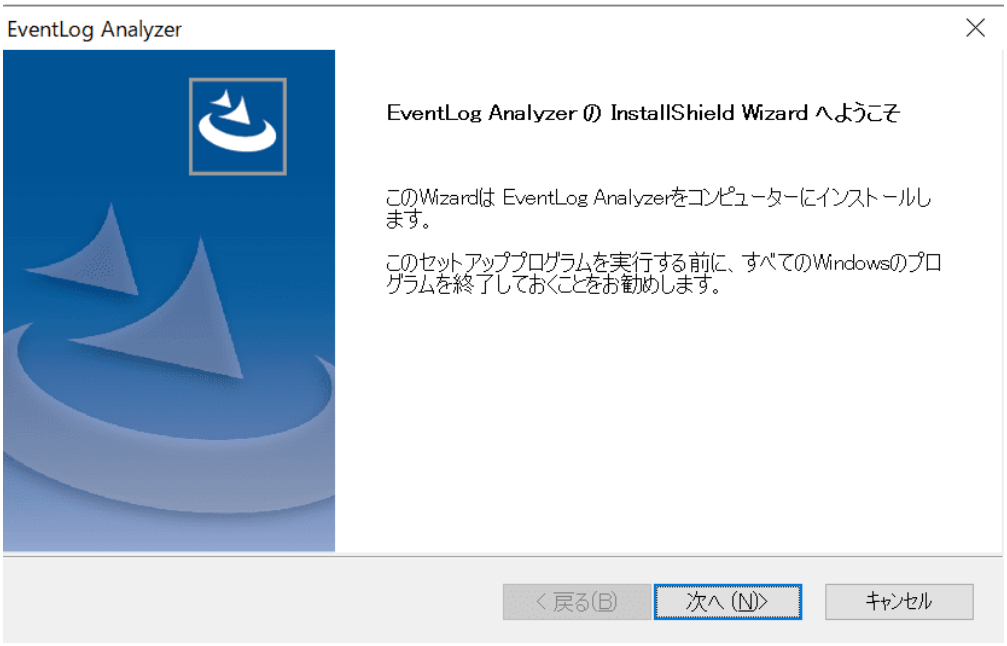
    - **ADAudit Plus**：Active Directory、Azure AD、およびファイルサーバー監査に特化したManageEngine製品
    - **Log360**：EventLog AnalyzerおよびADAudit Plusを1つのコンソール画面で管理できるManageEngine製品
    - **elasticsearch**： EventLog Analyzerがバンドルする検索エンジンデータベース

- **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」の利用をご希望のお客様は、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。**

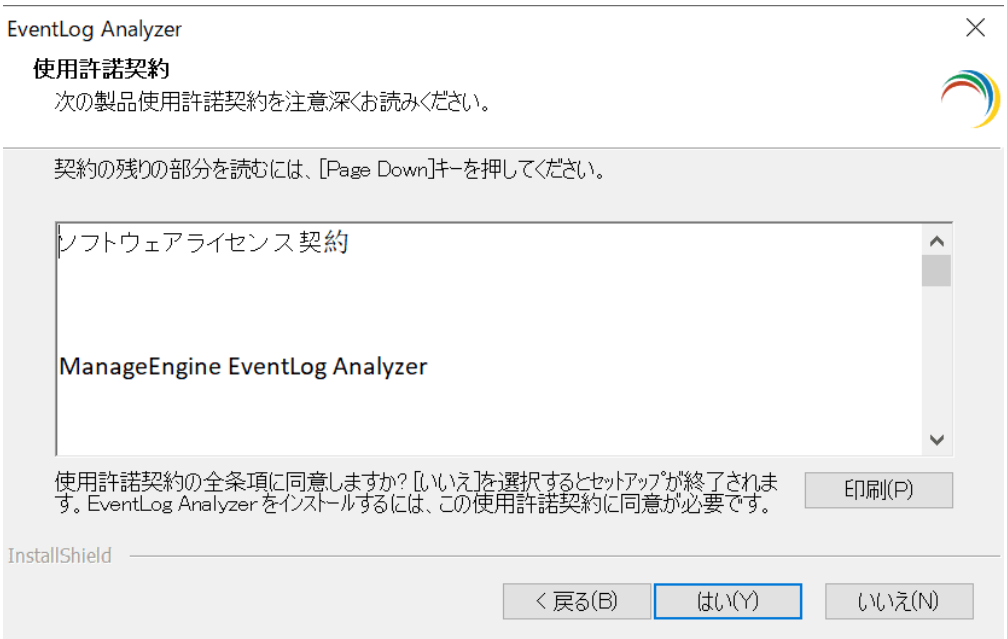
5-1 Windows環境でのインストール手順

1. "ManageEngine_EventLogAnalyzer_64bit.exe" を管理者権限で実行します。

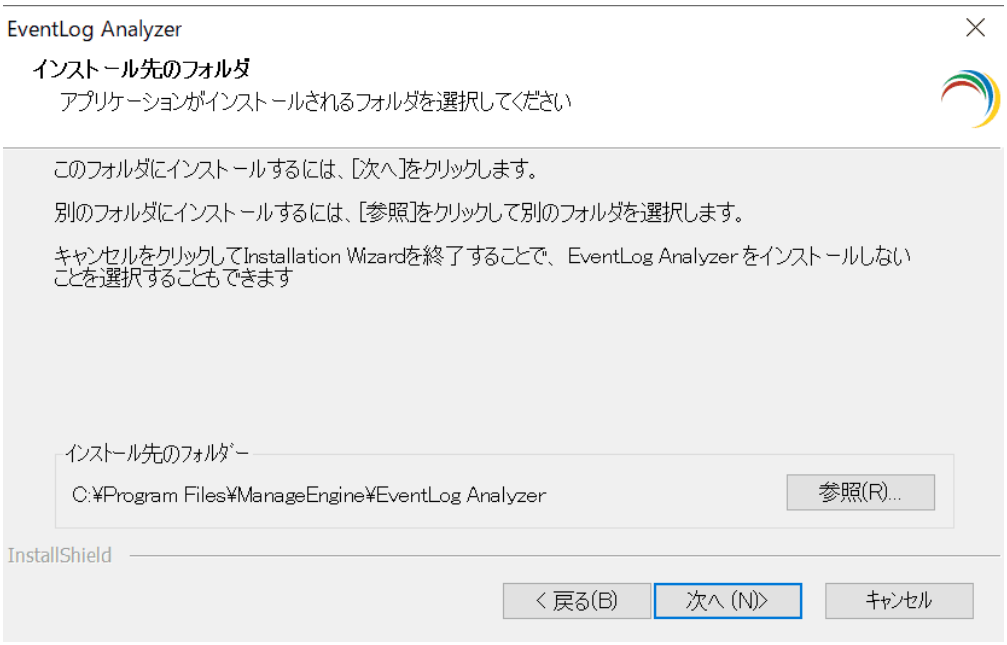
2. インストール画面が表示されるので、[次へ]をクリックします。



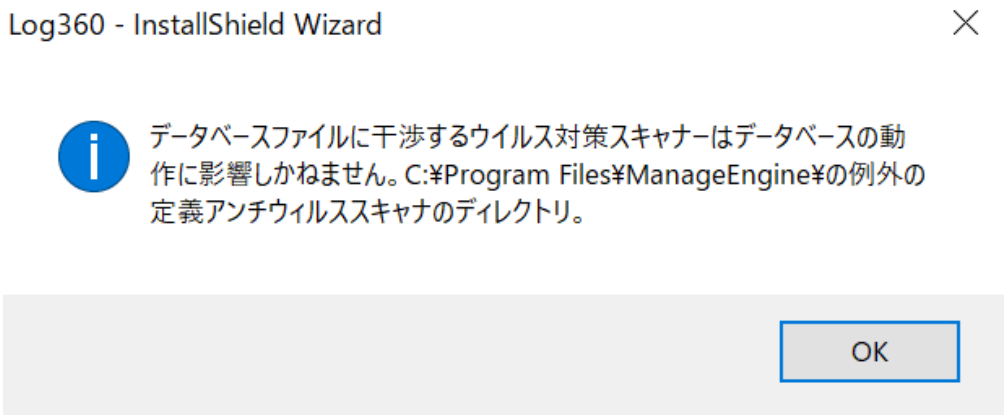
3. ライセンス条項を承諾後、[はい]をクリックします。



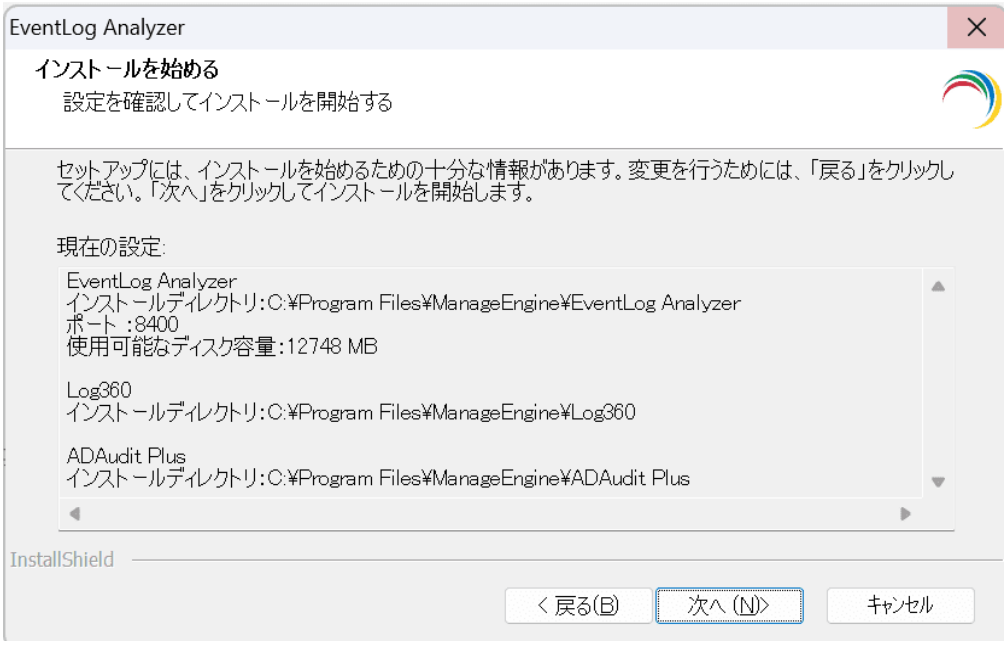
4. インストールディレクトリを選択します。デフォルトは"C:¥Program Files¥ManageEngine¥EventLog Analyzer"です。変更する場合は[参照...]をクリックします。設定後、[次へ]をクリックします。



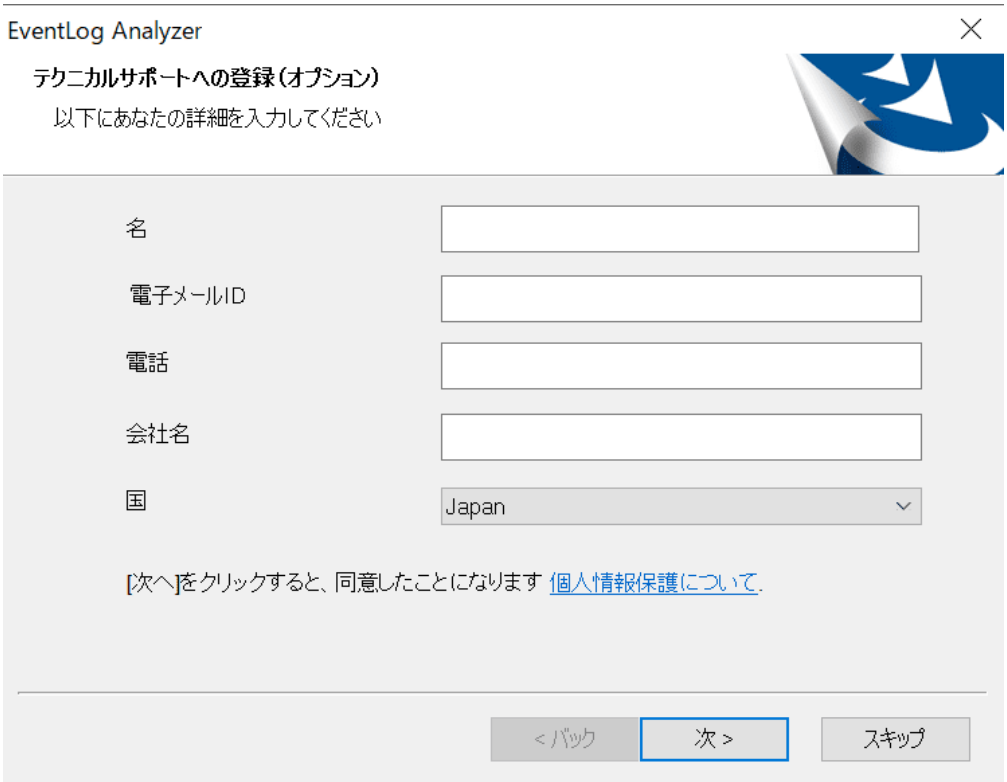
5. アンチウイルスソフトに関する警告画面が表示されますので、[OK]をクリックします。



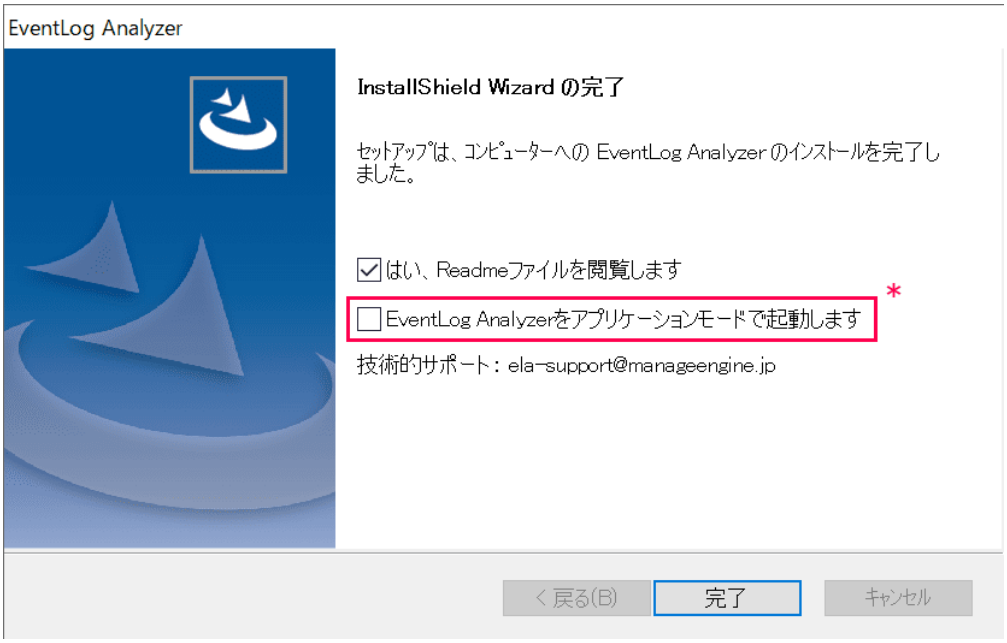
6. EventLog Analyzerをインストールするかの選択を行います。インストールを行う場合は、[次へ]をクリックします。インストールが開始します。



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について

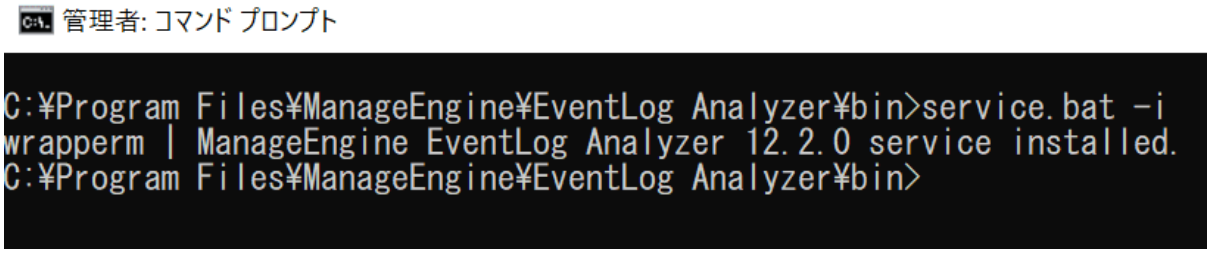
- [はい、Readmeファイルを閲覧します]：リリースノート情報を記載したページ（英語版）が開きます。
- [EventLog Analyzerをアプリケーションモードで起動します]：Eventlog Analyzerがアプリケーション（コンソールモード）として起動します。

＊製品の仕様上、EventLog Analyzerを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、以下[EventLog Analyzerサービスのインストール手順]のとおりです。

EventLog Analyzer サービスのインストール手順

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. "service.bat -i"を実行します。
4. EventLog Analyzerサービスがインストールされることを確認します。



EventLog Analyzerサービスの起動手順は[EventLog Analyzerサービスの起動手順]をご参照ください。

5-2 Linux環境でのインストール手順

1. "ManageEngine_EventLogAnalyzer_64bit.bin"ファイルを保存したパスに移動します。

2. "**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. "**./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できます。ライセンス条項を承諾する場合は"**y**"を押下します。

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

5. お客様情報を入力します（任意）。

```
Registration for Technical Support
------------------------------------------------------------
Name : dummy
Phone : xxxxxxxxxx
E-mail Id : dummy@dummy.com
Company Name : zoho
Country : Japan (116)
https;//www.manageengine.com/privacy.html
 -> 1- Next
    2- Skip
    3- Cancel
    4- Back
Select option to continue: 1
```

6. インストール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、ディレクトリを指定してください。

```
Where would you like to install?
   Default Install Folder: /opt/ManageEngine/EventLog
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: Enter
```

7. 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。変更しない場合は**Enterキー**を押下します。変更する場合はポート番号を入力してください。

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

8. 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** 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** を押下します。インストールしない場合は **2** を押下します。

```
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
```

9. 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。

```
Please Review the Following Before Continuing :
Product Name :
   ManageEngine EventlogAnalyzer
Install Folder :
   /opt/ManageEngine/EventLog
Disk Space Information ( for Installation Target ):
   Required:  692.13 MegaBytes
   Available: 143,187.43 MegaBytes
PRESS <ENTER> TO CONTINUE : Enter
```

10. 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。

```
InstallAnywhere is now ready to install ManageEngine EventlogAnalyzer onto your system at the following location :
   /opt/ManageEngine/EventLog
PRESS <ENTER> TO INSTALL : Enter
```

11. インストールが正しく行われたことを確認後、**Enterキー**を押下して終了します。

```
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

＊製品の仕様上、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

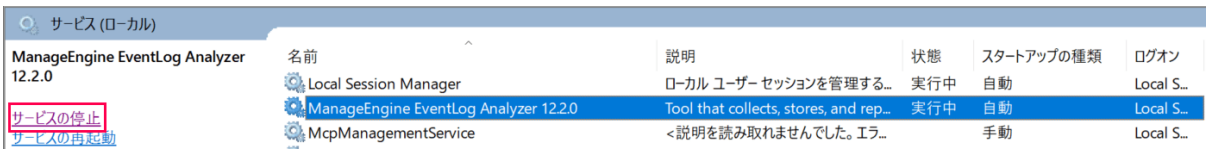
EventLog Analyzer サービスの起動手順

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]をご参照ください。

1. [スタート]→ [コントロールパネル] → [システムとセキュリティ] → [管理ツール] → [サービス]を開き、[ManageEngine EventLog Analyzer]を選択します。
2. [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

1. [スタート]→ [コントロールパネル] → [システムとセキュリティ] → [管理ツール] → [サービス]を開き、[ManageEngine EventLog Analyzer]を選択します。
2. [サービスの停止]をクリックします。

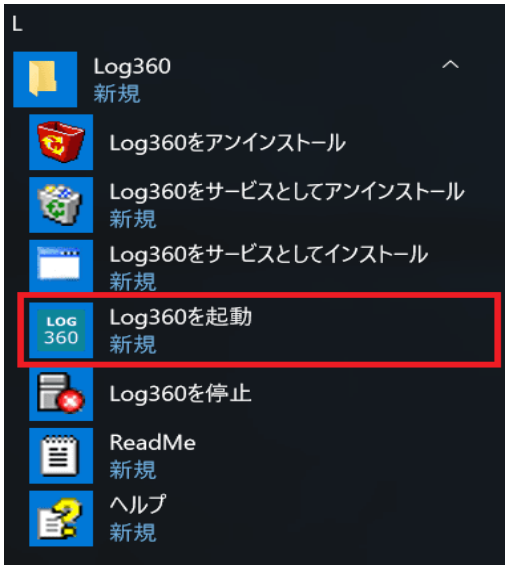


EventLog Analyzerアプリケーションの起動手順

＊製品の仕様上、サービスとして起動することを推奨します（手順はこちら）。

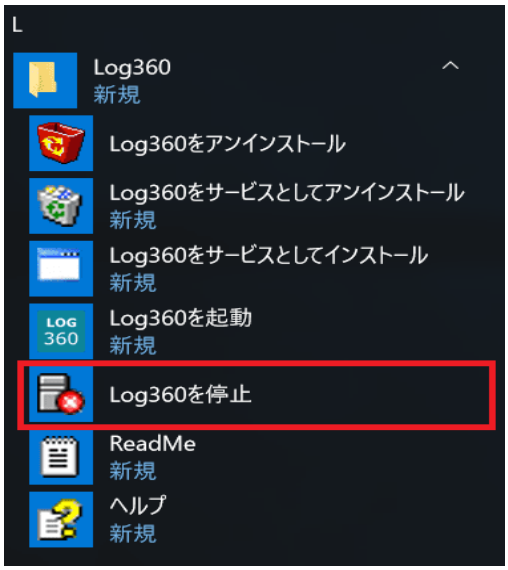
＊以下の手順を実施した場合、製品Log360の統合製品としてEventLog Analyzerが起動します。同時に起動するLog360はサポート対象外です。

[スタート] → [すべてのプログラム] → [Log360] → [Log360を起動]を選択します。
＊ショートカットからEventLog Analyzerを単体として起動できません。



EventLog Analyzerアプリケーションの停止手順

[スタート] → [すべてのプログラム] → [Log360] → [Log360を停止]を選択します。



6-3 Linux環境での起動/停止

EventLog Analyzerサービスの起動手順

EventLog Analyzerをサービスとしてインストールしていない場合、以下のコマンドを実行することで、サービスとしてインストールできます。
 # cd /opt/ManageEngine/EventLog/bin
 # sh configureAsService.sh -i

サービスを起動するためには、以下のコマンドを実行してください。
 # systemctl start eventloganalyzer

EventLog Analyzerサービスの停止手順

以下のコマンドを実行してください。
 # systemctl stop eventloganalyzer

EventLog Analyzerアプリケーションの起動手順

以下のコマンドを実行してください。
 # cd /opt/ManageEngine/EventLog/bin
 # sh run.sh

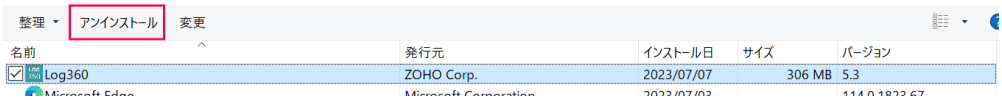
EventLog Analyzerアプリケーションの停止手順

以下のコマンドを実行してください。
 # 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. [スタート] → [コントロールパネル] → [プログラム] → [プログラムと機能]を開きます。
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]ボタンをクリックしてウィザードを閉じます。
6. EventLog Analyzerのインストールフォルダーを削除します。

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. 以下のコマンドを実行します。

 # cd /opt/ManageEngine/EventLog/_ManageEngine\ EventlogAnalyzer_installation
 # ./Change\ ManageEngine\ EventlogAnalyzer\ Installation

3. ウィザードに従って、アンインストールを実施します。
4. EventLog Analyzerのインストールフォルダーを削除します。

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]**と入力します。

- [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（デフォルトでは 8400）

  ＊SSLを有効化する設定を行った場合は、**https**://[host_name]:[port_number]と入力します。

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. 管理ホストの登録

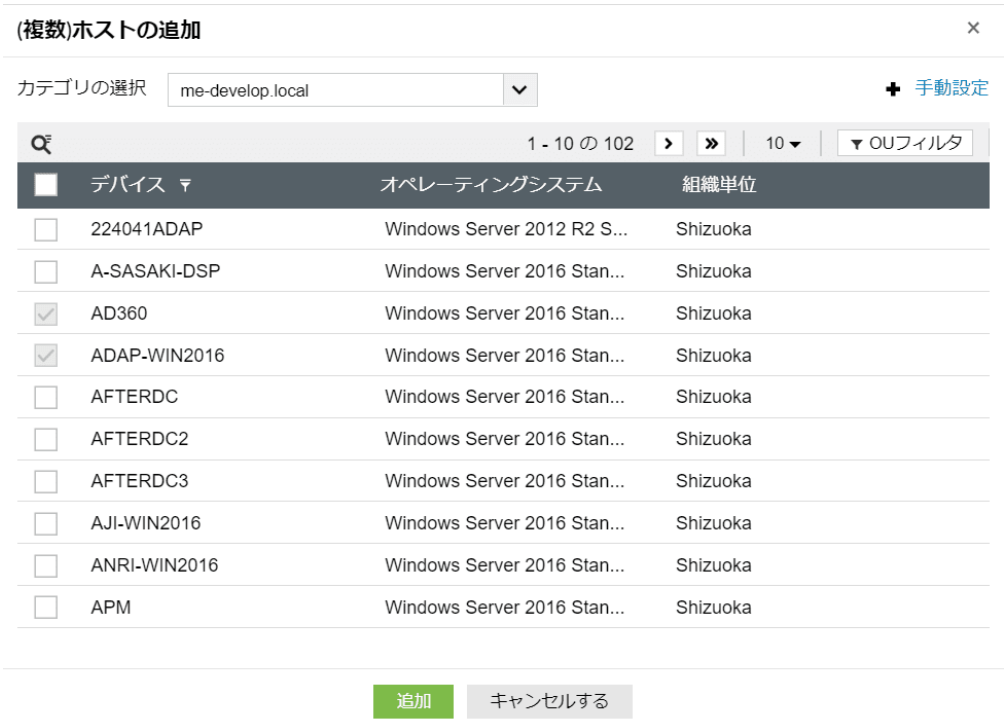
9-1 Windowsホストの登録手順

原則、**エージェント不要で**Windowsログを収集できます。エージェントを使用したログ収集の概要および手順は[こちらのナレッジベース]をご参照ください。

同じドメインに属したサーバーを登録する手順

1. 画面右上の[+追加] → [ホスト]をクリックします。

2. EventLog Analyzerが起動しているサーバーがドメインに属している場合、同一ドメインに属するWindowsサーバーが自動的に一覧表示されます。管理ホストとして登録したいサーバーにチェックを入れます。



3. [追加]をクリックします。

異なるドメインに属したサーバーを登録する手順

1. 異なるドメインに属するサーバーを追加する場合、対象ドメインをEventLog Analyzerに追加する必要があります。[設定]タブ → [管理者権限] → [ドメインとカウント] → [ドメインを構成する]タブから、[+新しいドメインの追加]をクリックします。

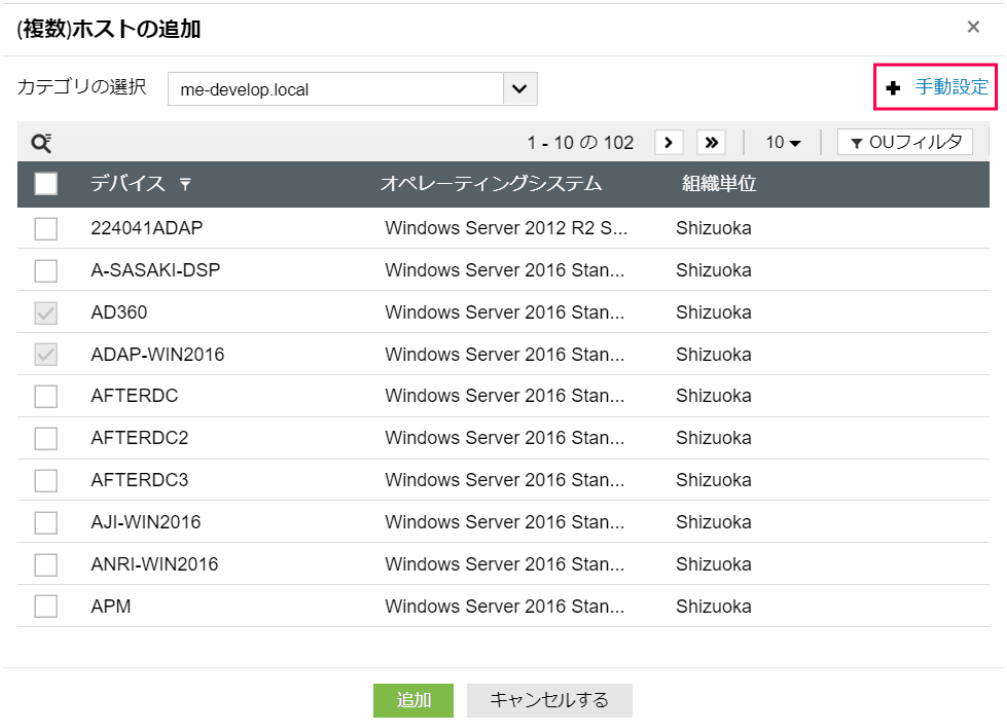
2. ドメイン名およびドメインコントローラーのホスト名またはIPアドレスを入力し、管理者権限（Domain Admins以上の権限）を持つユーザーの認証情報を入力します。

3. [追加]をクリックします。

ドメインに属さないワークグループのサーバーを登録する手順

1. 画面右上の[+追加] → [ホスト]をクリックします。

2. [+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]をクリックします。

9-2 Syslogホストの登録手順

EventLog Analyzerは、バンドルしているSyslogサーバーを使用してSyslogを受信します。そのため、Syslogホストとして登録したいデバイス側にて、EventLog AnalyzerにSyslogを転送する設定を実施する必要があります。EventLog AnalyzerがSyslogを受信後、自動的に管理ホストとして追加されます。

Syslogデバイス側でのSyslog転送設定手順

1. rootユーザーとしてログインします。
2. /etc/rsyslog.confをvi等で編集します。
3. 以下のパラメーターを追加します。

***.* @[EventLog Analyzerサーバー名 or IPアドレス]:[EventLog Analyzerがsyslog受信に使用するポート番号]**

パラメーター例）***.* @192.168.0.1:513**

[EventLog AnalyzerサーバーのIPアドレス]：**192.168.0.1**
[EventLog Analyzerが使用するポート番号]：**513**

4. 設定を保存します。
5. Syslogデーモンを再起動します。

10. システム設定

EventLog Analyzerを使用する際に必要となる設定手順を説明します。

10-1 EventLog Analyzerに接続する際のポート番号設定

EventLog Analyzerに接続する際に使用するポート番号は変更可能です（デフォルトは8400）。変更する場合は、以下の手順を実施してください。

ポート番号変更手順

1. [設定]タブ → [システム設定] → [接続設定] → [一般設定]タブをクリックします。
2. 「接続タイプ」にて、使用するプロトコルおよびポート番号を入力します。
3. LDAP SSLを任意で有効にします。
4. セッションの有効期限を任意で設定します。
5. [設定保存]をクリックします。
6. EventLog Analyzerサービスを再起動します。

10-2 メールサーバー設定

アラートメール通知の際などに使用するメールサーバーを設定します。

メールサーバー設定手順

1. [設定]タブ → [システム設定] → [通知設定] → [メール設定]タブをクリックします。
2. 「サーバー名/IPアドレス」に、メールサーバーの情報を入力します。
3. 「ポート」にメールサーバーが使用するポート番号を入力します。
4. 「送信元アドレス」に、メールの差出人となるメールアドレスを入力します。
5. 「管理者の電子メール アドレス」に、メールの宛先となるメールアドレスを入力します。
6. メールサーバーとの通信がSSLまたはTLS通信となる場合は、任意で「セキュア接続(SSL/TLS)」を選択します。
7. メールサーバーで認証を必要とする場合は、[承認が必要です]にチェックを入れ、「ユーザー名」と「パスワード」を入力します。
8. [設定保存]をクリックします。

10-3 製品ユーザー（技術者）のパスワード変更

こちらのナレッジベースをご参照ください。

10-4 ビジネス時間の設定

こちらのナレッジベースをご参照ください。

10-5 ログのアーカイブ設定

EventLog Analyzerは、収集したログをアーカイブファイルへ出力し、保存します。また、アーカイブファイルを定期的に圧縮することでディスク容量の節約につながり、ログを長期保管することが可能となります。アーカイブファイルの保持期間とログを圧縮する間隔は要望に合わせて設定可能です。以下、設定手順を説明します。

アーカイブの設定手順

1. [設定]タブ → [管理者権限] → [アーカイブ] → 画面右上の[設定]をクリックします。
2. 以下のページが表示されます。各項目を任意で設定後、[保存]をクリックします。

各項目の詳細

- **暗号データ**：アーカイブファイルを暗号化することができます。デフォルトでは無効です。暗号化を有効にすると、アーカイブファイルをテキストエディターで開いてもログ内容が確認できません。

- **アーカイブ保持期間**：アーカイブファイルの保持期間を選択します。デフォルトでは無期限です。設定した保持期間を過ぎたアーカイブファイルは自動的に削除されます。

- **アーカイブログの種類**：アーカイブファイルに含める情報を設定できます。デフォルトの設定値は解析済みフィールドを含む未処理ログです。未処理ログを設定した場合、解析したフィールドの情報が保存されないため、アーカイブファイルの容量が小さくなります。しかし、アーカイブファイルをロードする際に解析処理が実行されるため、ロードに時間を要します。

- **アーカイブ場所**：アーカイブファイルの保存パスを設定します。デフォルトの保存先パスは"C:\Program Files\ManageEngine\EventLog Analyzer\archive"です。＊保存先パスとして異なるデバイス上のパスを指定する場合、EventLog Analyzerサーバーと当該デバイス間のネットワーク接続が良好であることをご確認ください。

- **通知メールアドレス**：アーカイブ改ざん検知など、アーカイブファイルについてのアラートの通知先メールアドレスを設定します。

- **ロード保持期間**：アーカイブをロードした際に製品データベースに展開されるデータの保存期間を設定します。デフォルト設定では7日です。＊デフォルト設定ではアーカイブをロード後7日間、アーカイブデータをレポートタブや検索タブで使用できます。

- **ファイル作成間隔**：収集したログを1つのアーカイブファイルとして作成する間隔を設定します。デフォルトでは8時間です。＊デフォルト設定では8時間ごとに1アーカイブファイルが作成されます。

- **Zip作成間隔**：作成されたアーカイブファイルをgz圧縮する間隔を設定します。デフォルトでは1日です。＊デフォルト設定では1日間で作成されたアーカイブファイルをまとめてgz圧縮し、1つのgzファイルが作成されます。

- **アーカイブのタイムスタンプ**：アーカイブのタイムスタンプ機能を有効化することができます。デフォルトでは無効です。タイムスタンプ機能を有効にすると、アーカイブファイルの改ざんを検知することが可能です。

10-6 各種データの保存期間設定

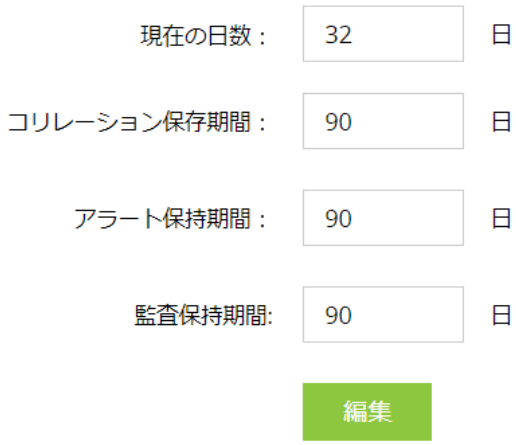
EventLog Analyzerが製品データベースに保存する各種データについて、それぞれ保存期間を設定することができます。

各種データの概要

- **インデックス処理されたログデータ**：レポートタブや検索タブにてログデータを表示する際に使用するデータ
- **コリレーションデータ**：コリレーション（相関）レポートの出力に使用するデータ
- **アラートデータ**：アラート情報の出力に使用するデータ
- **APIの監査データ**：APIの利用状況に関するデータ

各種データの保存期間設定手順

1. [設定]タブ → [管理者権限] → [保持設定]をクリックします。
2. 以下のページが表示されます。各項目について保存する日数を指定後、[編集]をクリックします。



各項目の詳細は以下のとおりです。

各項目の詳細

- [現在の日数]：インデックス処理されたログデータの保存期間を指定します。デフォルトは32日です。
- [コリレーション保存期間]：コリレーションデータの保存期間を指定します。デフォルトは90日です。

- [アラート保持期間]：アラートデータの保存期間を指定します。デフォルトは90日です。
- [監査保持期間]：APIの監査データの保存期間を指定します。デフォルトは90日です。

＊各保存期間に指定可能な最大値は9999日です。しかし、保存データ増加に伴うディスク容量の圧迫や、レポート出力と検索クエリ実行処理の増加に伴う動作遅延が発生するため、**特別な要件がない場合はデフォルト設定を推奨します。**
また、保存期間を経過したインデックス処理されたログデータは、アーカイブデータをロードすることで、データベースに再度展開することが可能です。データベースに再度展開することで、レポートタブや検索タブで当該ログデータの使用が可能となります。アーカイブデータをロードする方法については以下の手順をご参照ください。

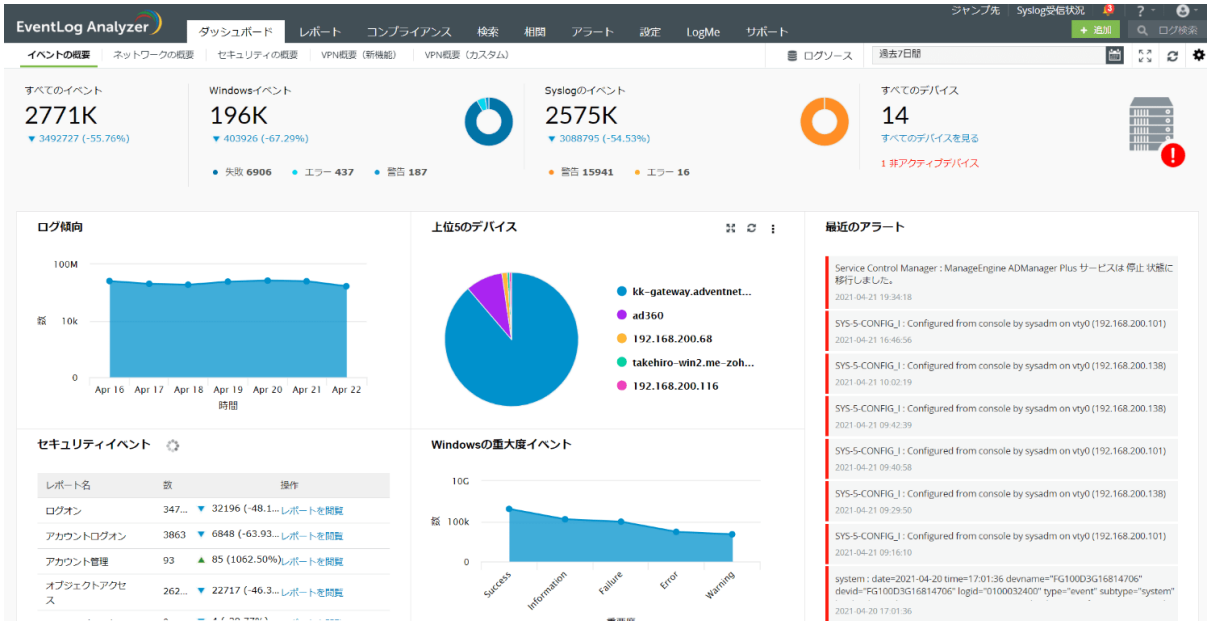
アーカイブデータをロードする手順

1. [設定]タブ → [管理者権限] → [アーカイブ]をクリックします。「ステータス」において、「ロードされていません」と表示されているアーカイブデータが、データベースに展開されていないデータです。当該アーカイブデータをロードしてデータベースに再度展開することで、レポートタブや検索タブで当該ログデータの参照が可能となります。
2. 対象のアーカイブデータのチェックボックスにチェックを入れます。
3. [アーカイブをロード]をクリックします。

11. 各タブの解説

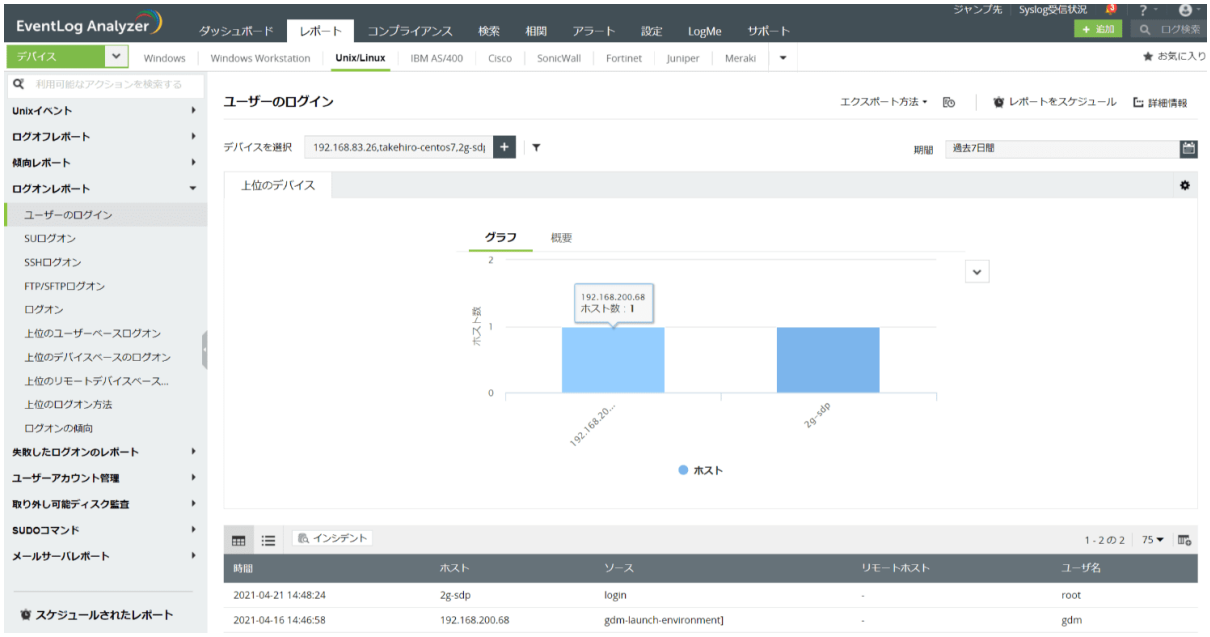
11-1 ダッシュボード

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。



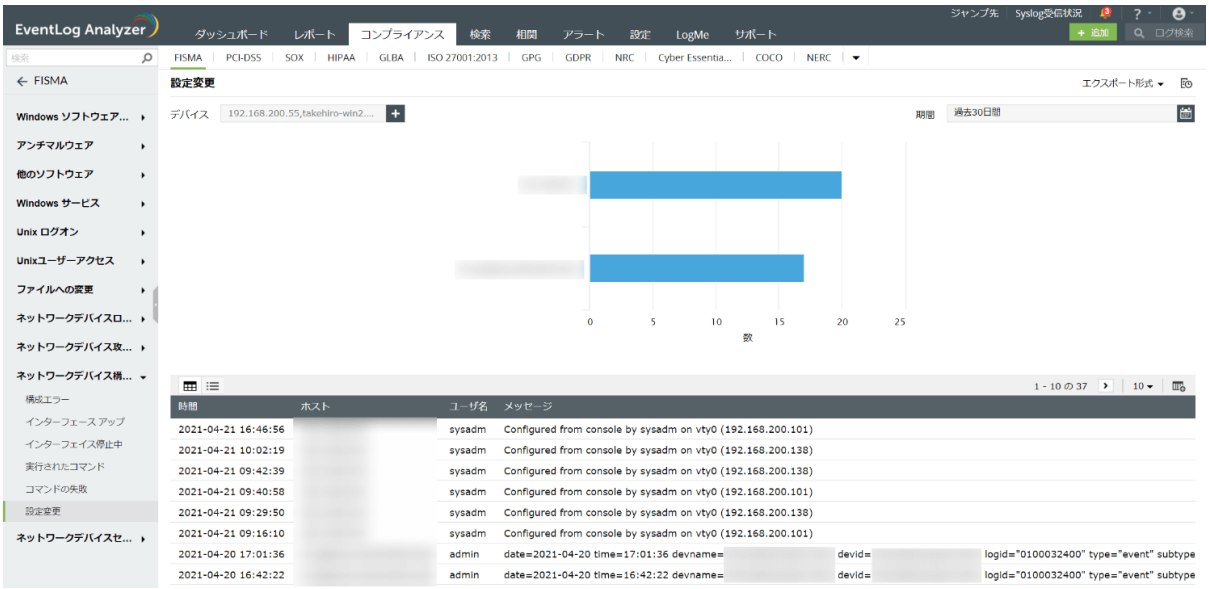
11-2 レポート

レポートタブでは、管理ホストに関する定義済みレポートが確認できます。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。また、日次や週次でスケジュールレポートを設定することで、定期的なレポート生成にも対応できます。カスタムレポートの設定方法はこちらのナレッジベース、スケジュールレポートの設定方法はこちらのナレッジベースをご参照ください。



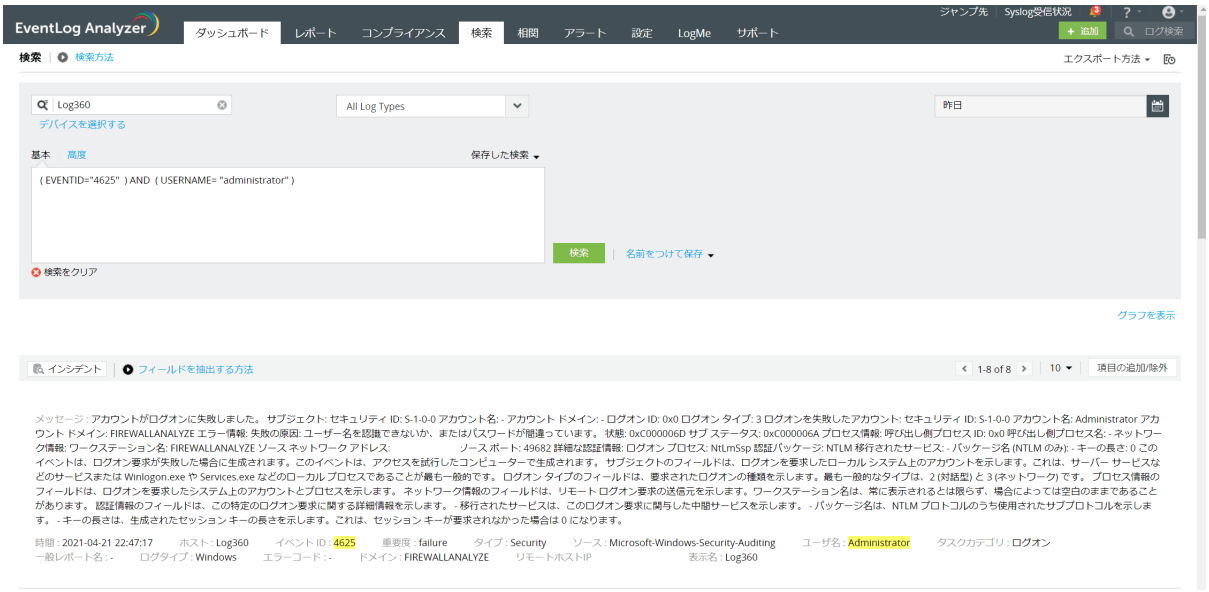
11-3 コンプライアンス

コンプライアンスタブでは、様々な規制法令に適合するコンプライアンス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。



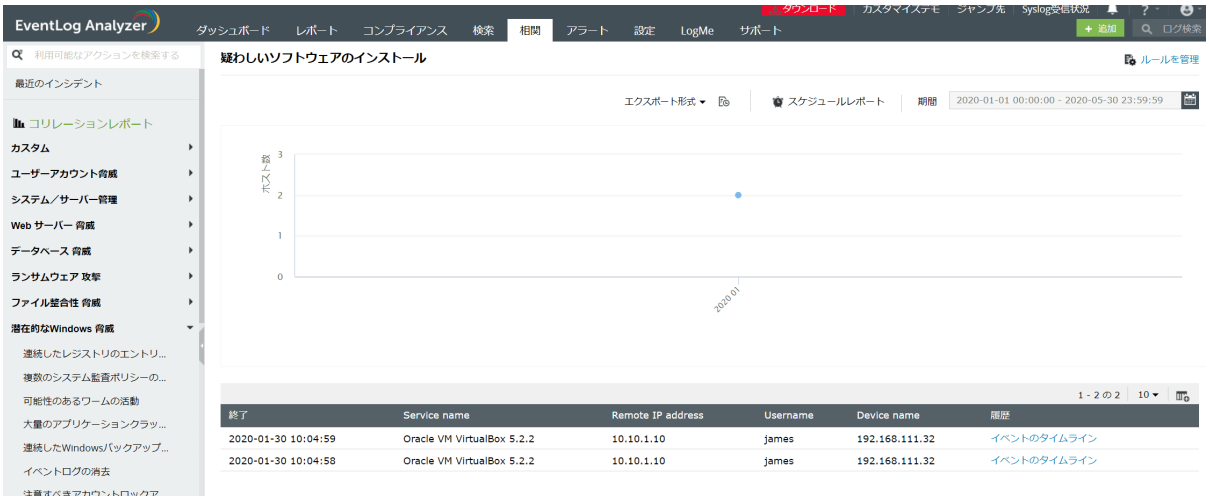
11-4 検索

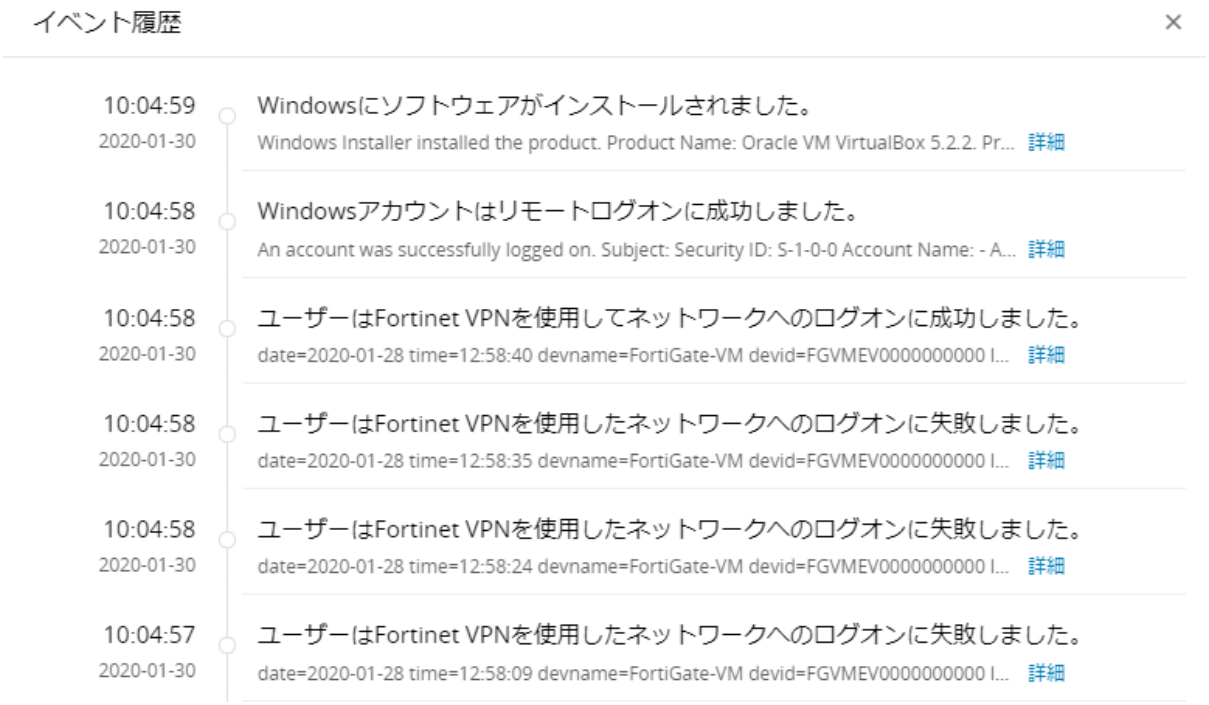
検索タブでは、日時や対象デバイス、特定の条件を設定して収集したログを検索できます。検索クエリに関する知識がなくても直感的に使用でき、インシデントの早期分析に役立ちます。検索機能の詳細はこちらのナレッジベースをご参照ください。



11-5 相関（コリレーション）

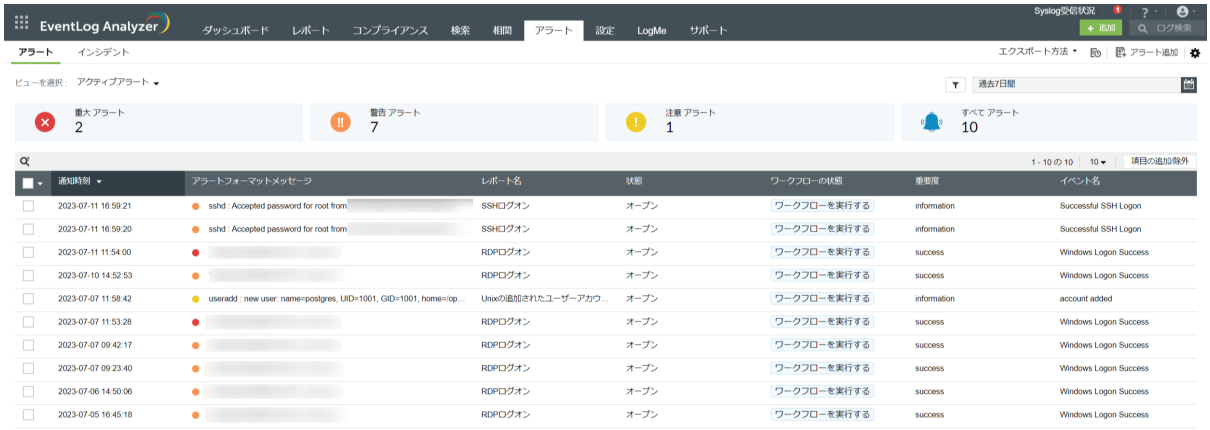
相関タブでは、異なるデバイスからログを相関的に分析して、ネットワーク間で発生している不審な挙動を検知できます。以下の画像例では、VPNデバイスから収集したVPNログオンに関するログおよびWindowsデバイスから収集したソフトウェアインストールに関するログを相関付けることで、発生したイベント（Windowsデバイス上でソフトウェアがインストールされた）の一連の流れを把握することができます。





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が収集された場合にアラートを生成することができ、管理者にメールを通知や指定したワークフローの実行が可能です。EventLog Analyzerでは、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。カスタムアラートの設定方法はこちらのナレッジベースをご参照ください。



12. トラブルシューティング

12-1. Windowsホスト登録に失敗する

こちらのナレッジベースをご確認ください。

12-2. Syslogホスト登録に失敗する

こちらのナレッジベースをご確認ください。

12-3. エージェントを使用したログ収集が失敗する

こちらのナレッジベースをご確認ください。

12-4 デフォルト管理者（admin）のパスワードを忘れた

サポートよりお問い合わせください。

13. 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/trail.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/