



**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	5
1-1 本ガイドについて	5
1-2 対象読者	5
1-3 EventLog Analyzer の概要	5
1-4 エディションの種類	5
1-5 評価版からPremium Editionにアップグレードする方法	6
2. システム要件	8
2-1 最小ハードウェア要件	8
2-2 サポートOS	8
2-3 サポートWebブラウザ	8
2-4 解析可能なログレコード数	8
3. ポート要件	10
4. 評価版インストーラーをダウンロード	12
5. インストール手順	13
5-1 Windows環境でのインストール手順	14
5-2 Linux環境でのインストール手順	19
6. 起動と停止	22
6-1 Windows環境での起動/停止	22
6-3 Linux環境での起動/停止	24
7. アンインストール手順	25
7-1 Windows環境でのアンインストール手順	25
7-2 Linux環境でのアンインストール手順	26
8. ログイン方法	27
9. 管理ホストの登録	28
9-1 Windowsホストの登録手順	28
9-2 Syslogホストの登録手順	31
10. システム設定	32
10-1 EventLog Analyzerに接続する際のポート番号設定	32
10-2 メールサーバー設定	32
10-3 製品ユーザー（技術者）のパスワード変更	33
10-4 ビジネス時間の設定	33
10-5 ログのアーカイブ設定	34
10-6 各種データの保存期間設定	36
11. 各タブの解説	38
11-1 ダッシュボード	38
11-2 レポート	39
11-3 コンプライアンス	40
11-4 検索	41
11-5 相関（コリレーション）	42
11-6 アラート	43
12. トラブルシューティング	44
12-1. Windowsホスト登録に失敗する	44
12-2. Syslogホスト登録に失敗する	44

12-3. エージェントを使用したログ収集が失敗する.....	44
12-4 デフォルト管理者（admin）のパスワードを忘れた.....	44
13. お問い合わせ.....	45

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。

ライセンス詳細 ×

 **製品のセキュリティ強化 - 20%** 推奨されるセキュリティ設定を構成することにより、EventLog Analyzer 展開のセキュリティを向上させます。 [すぐに変更する](#)

ライセンスタイプ	評価エディション - トライアルバージョン
製品名	ManageEngine EventLog Analyzer
製品バージョン	12.4.0
ビルド番号	12400
サブスクリプションの期限切れまで	2024-03-30
使用中	
Windowsサーバー数	4
デバイス数	0
アプリケーションの数	0

 [今すぐ購入](#) [お見積り](#) | [価格の詳細](#)

ライセンスファイルの入力 [参照する](#) [アップグレード](#)

Eventlog Analyzerを更新またはアップグレードして、管理対象のデバイスまたはアプリケーションを増やすためには、Zoho Corp.から取得した有効なライセンスファイルを入力してください。

DID : +1-408-916-9393 jp-mesales@zohocorp.com
フリーダイヤル : +1-844-649-7766 ela-support@manageengine.jp

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。

パスワード変更アラート



製品の次のデフォルト設定を変更していません： admin パスワード。セキュリティ上の理由から、パスワードを変更することをお勧めします。

すぐに変更する

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。

パスワード変更

次のパスワードを変更する： admin

* 現在のパスワード

.....

* 新しいパスワード

.....

* パスワードを確認する

- ✓ 最大文字数：20
- ✓ 最小文字数：8
- ✓ 少なくとも1件の数字を含めてください。
- ✓ 少なくとも1文字の小文字を含めてください。
- ✓ 少なくとも1件の大文字を含めてください。
- 少なくとも1件の特殊文字を含めてください。

上位5のデバイス

最近の

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

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

*各ブラウザ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。したがって、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

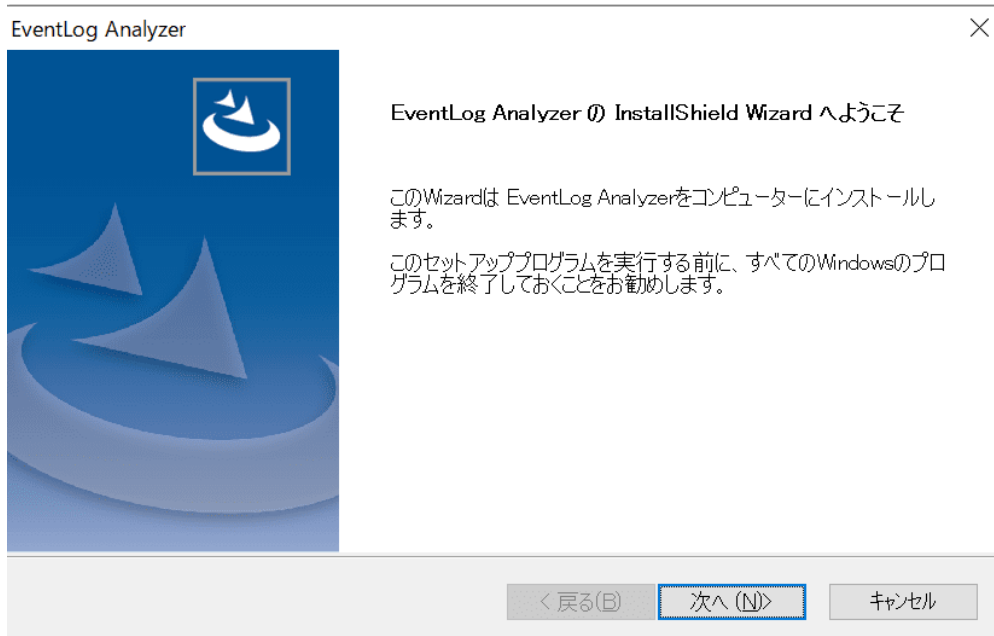
インストール手順を説明します。

注意事項

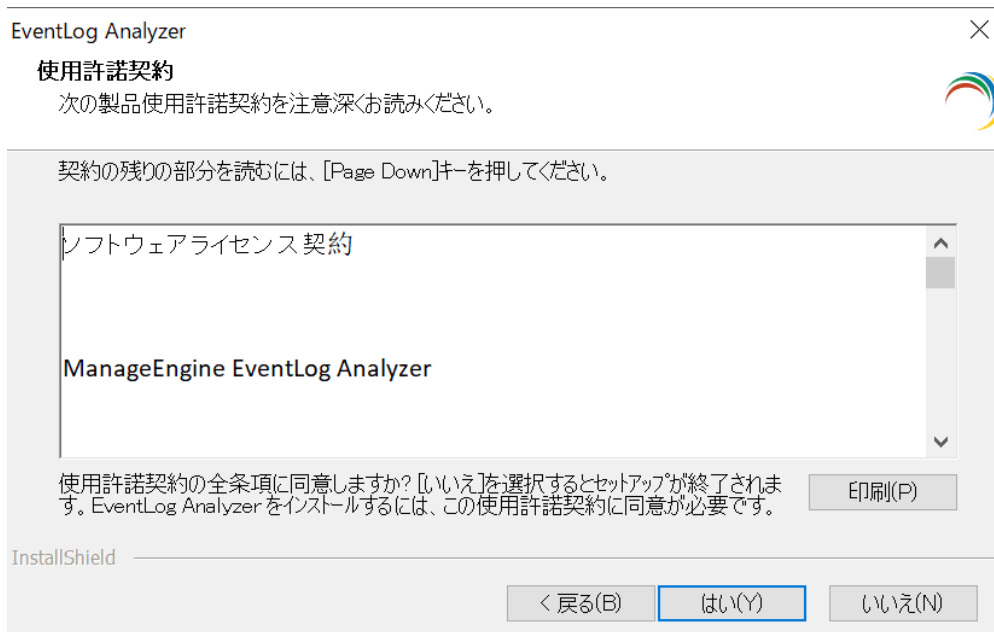
- **アンチウイルスソフトやバックアップツールなどをインストールしている場合、EventLog Analyzerをインストールしたフォルダーをスキャン対象またはバックアップ対象から必ず除外してください。**除外しない場合、スキャンまたはバックアップによってデータベースが破損する可能性があります。
- Windows版EventLog Analyzerをインストールすると、「ADAudit Plus」および「EventLog Analyzer」を1つのコンソール画面で管理できる統合ツール「Log360」としてインストールされます。そのため、指定したインストールディレクトリに「EventLog Analyzer」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

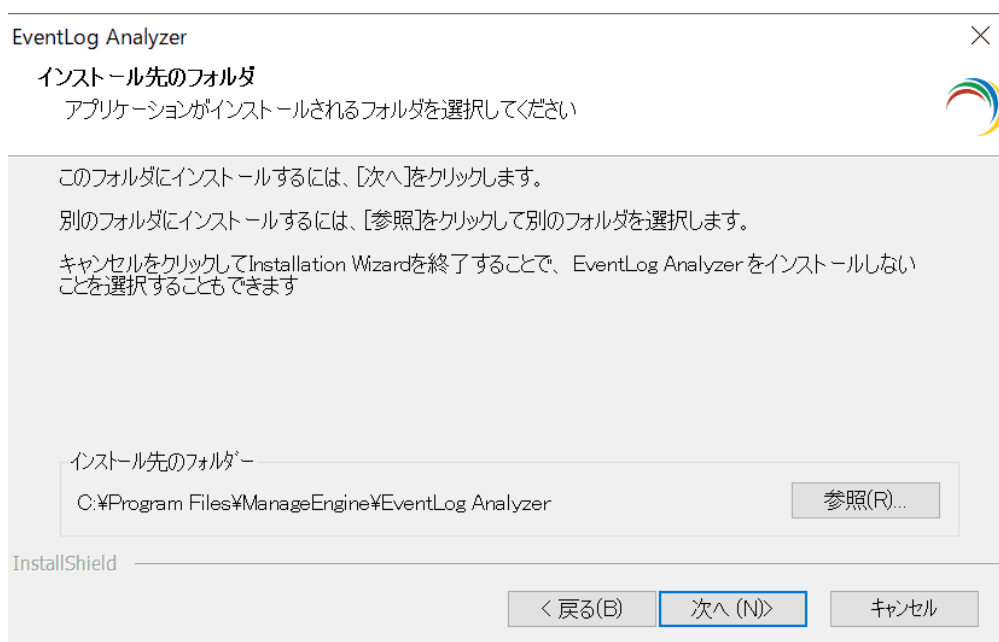
1. "ManageEngine_EventLogAnalyzer_64bit.exe" を管理者権限で実行します。
2. インストール画面が表示されるので、[次へ]をクリックします。



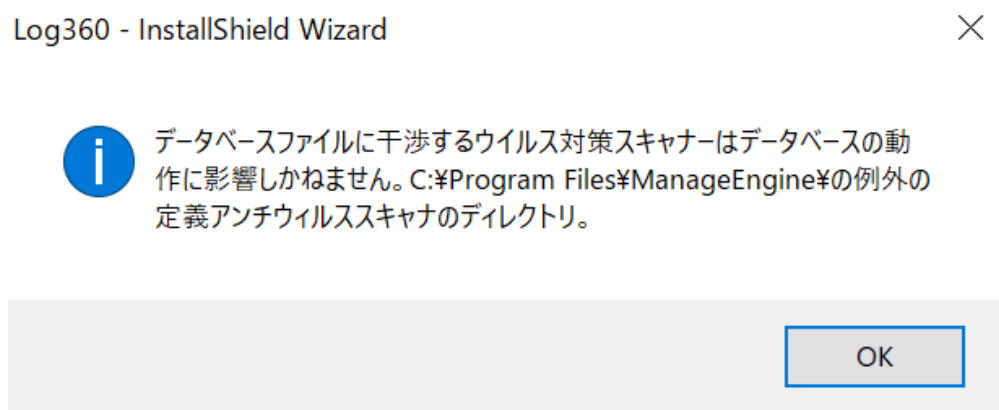
3. ライセンス条項を承諾後、[はい]をクリックします。



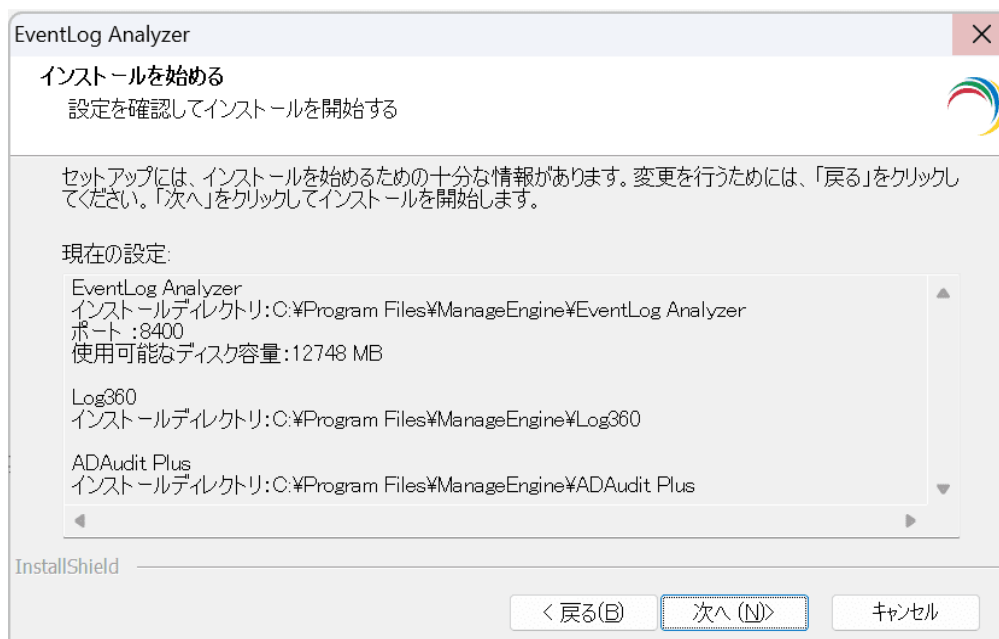
4. インストールディレクトリを選択します。デフォルトは "C:¥Program Files¥ManageEngine¥EventLog Analyzer"です。変更する場合は [参照...]をクリックします。設定後、[次へ]をクリックします。



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。

EventLog Analyzer

テクニカルサポートへの登録 (オプション)
以下にあなたの詳細を入力してください

名

電子メールID

電話

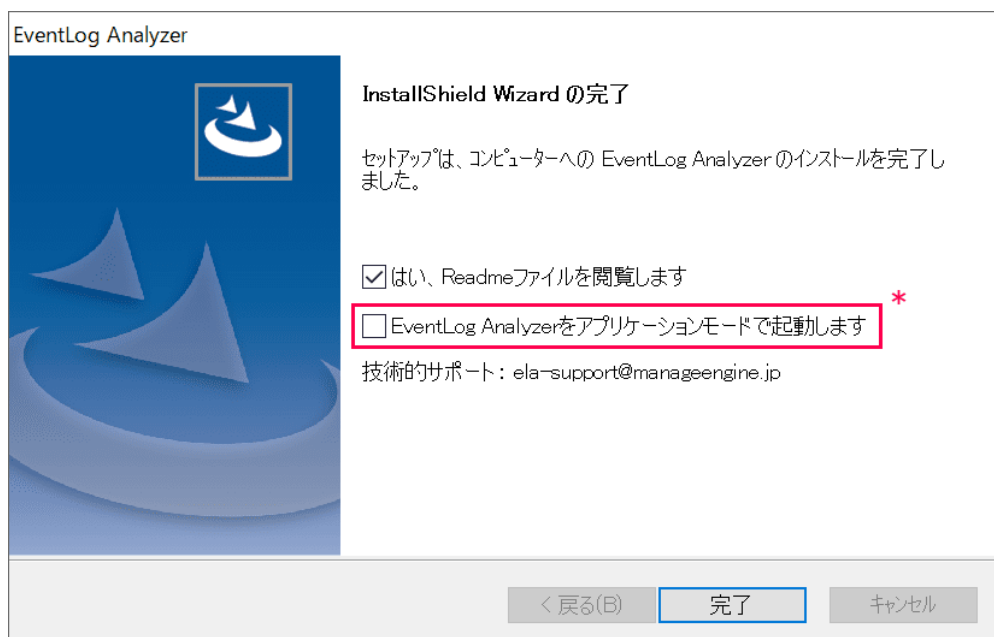
会社名

国

[次へ]をクリックすると、同意したことになります [個人情報保護について](#).

< バック 次 > スキップ

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ファイルを開覧します]：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。

 管理者: コマンド プロンプト

```
C:\Program Files\ManageEngine\EventLog Analyzer\bin>service.bat -i  
wrapperm | ManageEngine EventLog Analyzer 12.2.0 service installed.  
C:\Program Files\ManageEngine\EventLog Analyzer\bin>
```

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 : xxxxxxxxxxxx

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

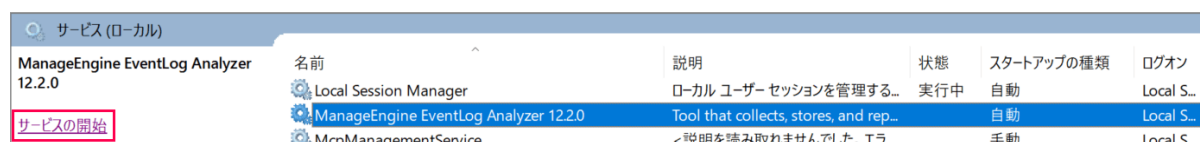
***製品の仕様上、サービスとして起動することを推奨します。**

6-1 Windows環境での起動/停止

EventLog Analyzer サービスの起動手順

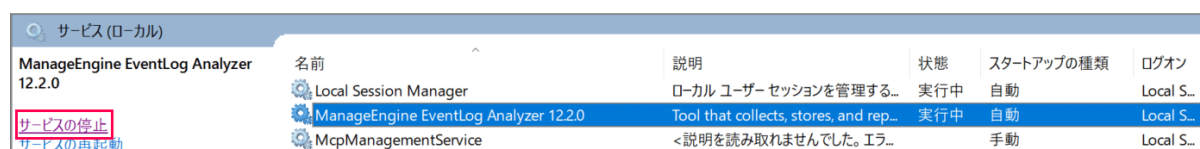
EventLog Analyzerをサービスとしてインストールする手順は、[\[EventLog Analyzer サービスのインストール手順\]](#)をご参照ください。

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。

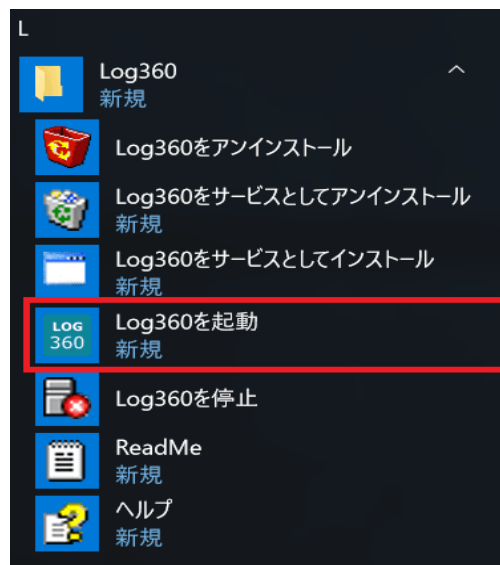


EventLog Analyzer アプリケーションの起動手順

*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](#)）。

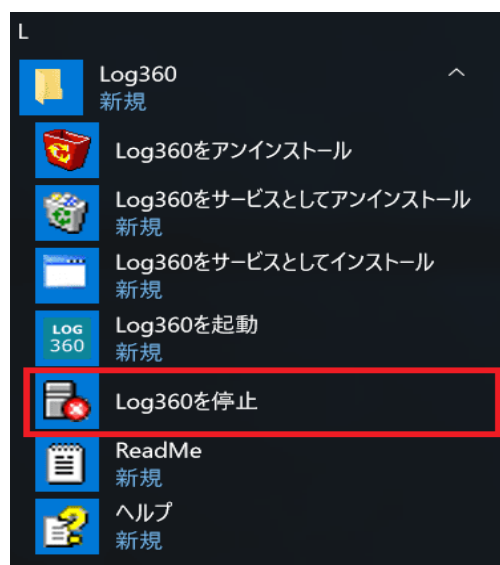
*以下の手順を実施した場合、製品Log360の統合製品としてEventLog Analyzerが起動します。同時に起動するLog360はサポート対象外です。

[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

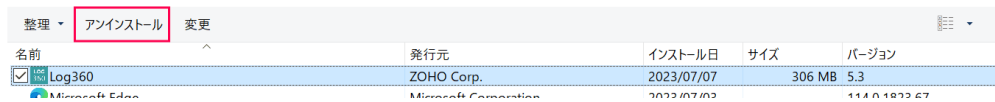
以下のコマンドを実行してください。

```
# cd /opt/ManageEngine/EventLog/bin  
# sh shutdown.sh
```

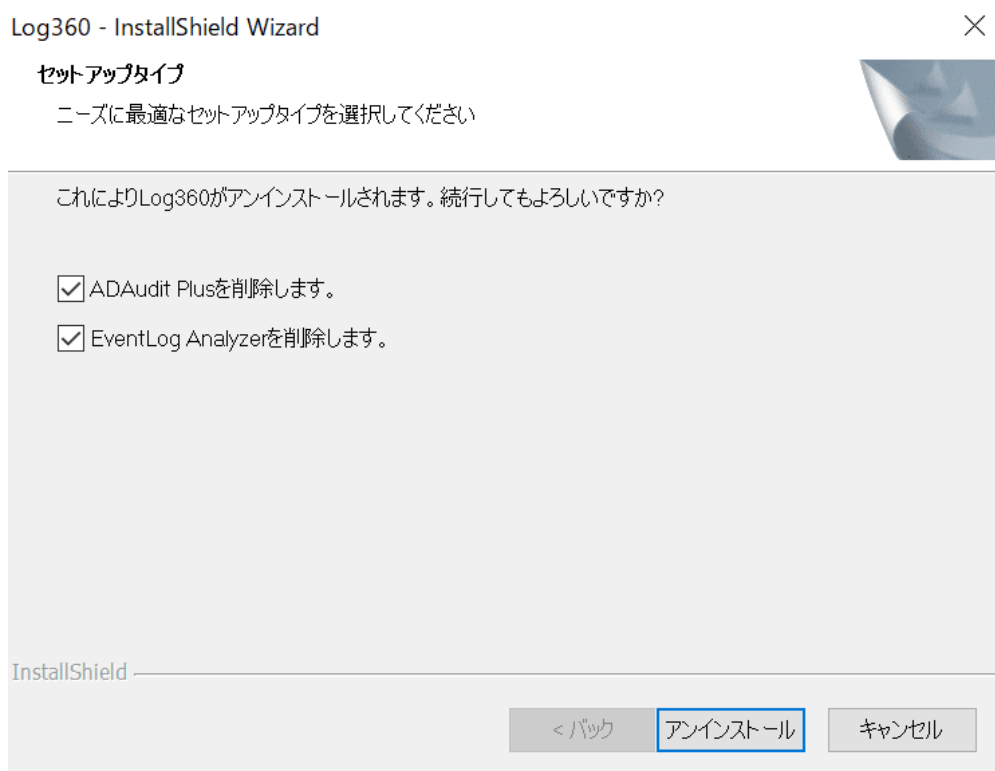

7. アンインストール手順

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

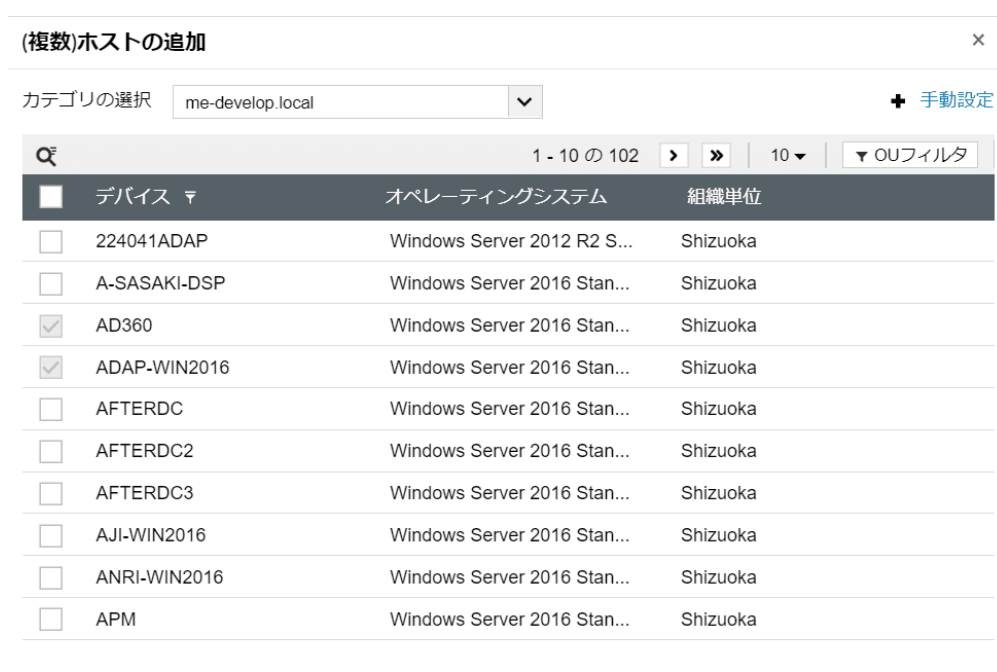
原則、エージェント不要でWindowsログを収集できます。エージェントを使用したログ収集の概要および手順は[こちらのナレッジベース](#)をご参照ください。

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

- 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。
- 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。

新しいドメインの追加

ドメイン名 me-develop.local

ドメインコントローラー AD360 ディスカバリー

複数のホストを追加するには半角カンマで区切ってください。

認証
認証情報を指定しない場合、マシンのローカル認証情報が使用されます。

ユーザー名 me-develop\administrator

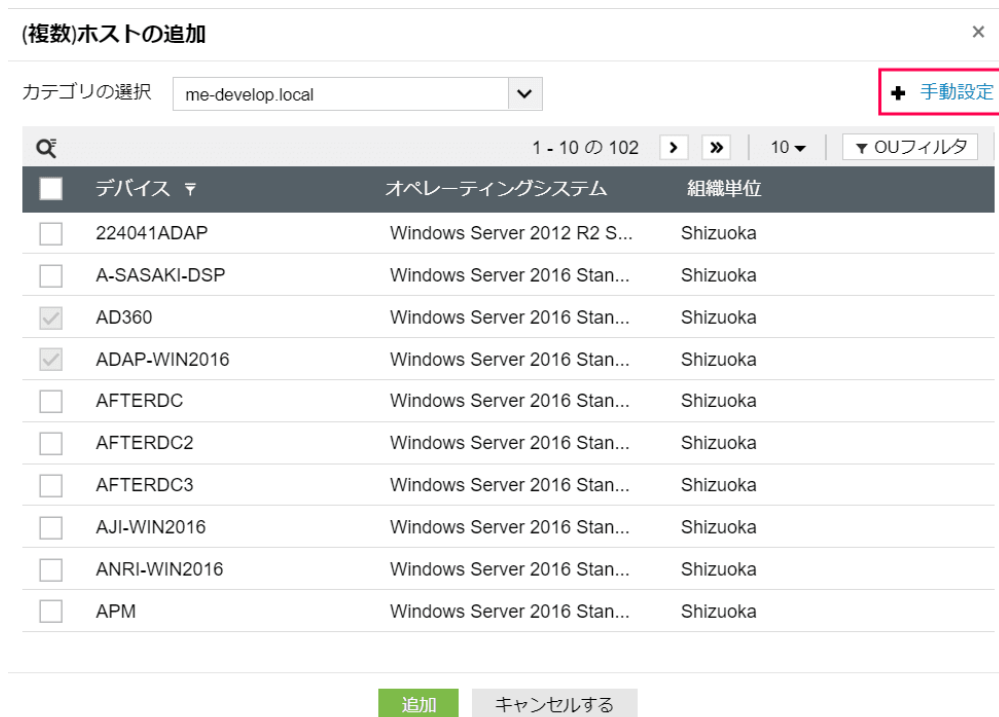
パスワード

追加 閉じる

- [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。

アーカイブの設定 ?

アーカイブ化を有効にする

暗号データ ▼

アーカイブ保持期間 ▼

アーカイブログの種類 ▼ ?

アーカイブ場所

通知メールアドレス ? [メールサーバーの再設定](#)

ロード保持期間 ▼

詳細 ▼

ファイル作成間隔 時

Zip作成間隔 ▼ [今すぐZip作成](#)

アーカイブのタイムスタンプ ▼

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。

現在の日数：	<input type="text" value="32"/>	日
コリレーション保存期間：	<input type="text" value="90"/>	日
アラート保持期間：	<input type="text" value="90"/>	日
監査保持期間：	<input type="text" value="90"/>	日

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。

アーカイブしたログ 設定

デバイスを選択 ログソースを選択 クリックして日付範囲を選択します。

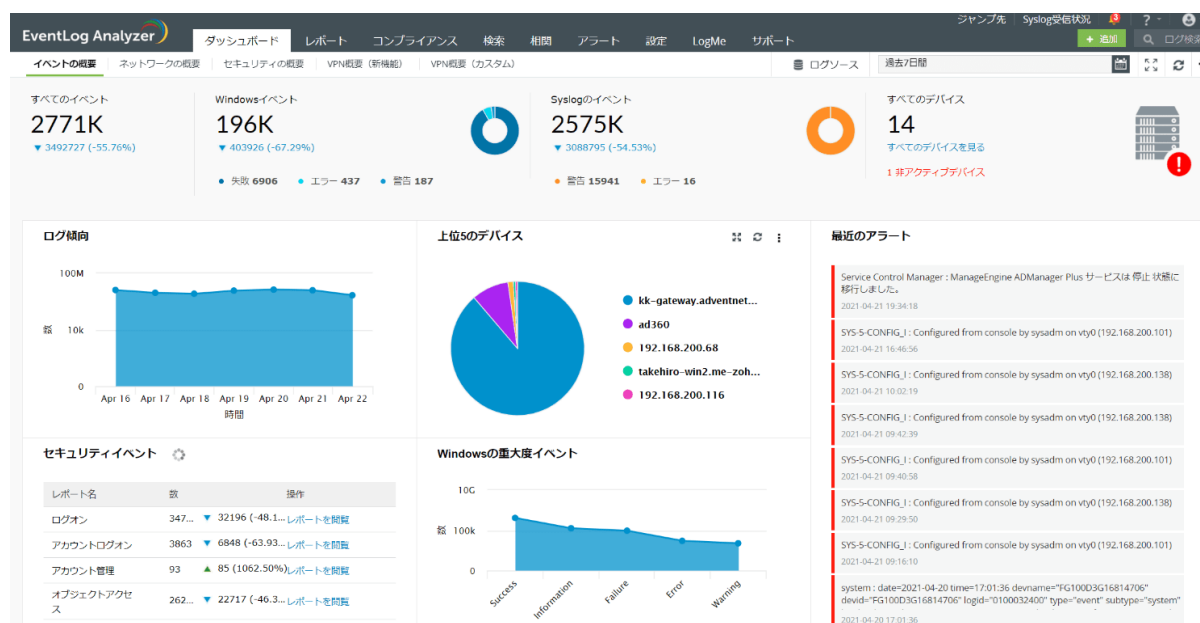
アーカイブをロード アーカイブをアンロード 選択されたファイル: 1 サイズ: 57.82 MB おおよそのロード時間: 58 秒 1-90 の 90

<input type="checkbox"/>	デバイス	フォーマット	開始	終了	サイズ	整合性	ステータス
<input checked="" type="checkbox"/>	ELA-WIN2016	Windows	2023-06-10 23:49:21	2023-06-11 23:49:26	43.90 MB	検証済み	ロードされていません

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。



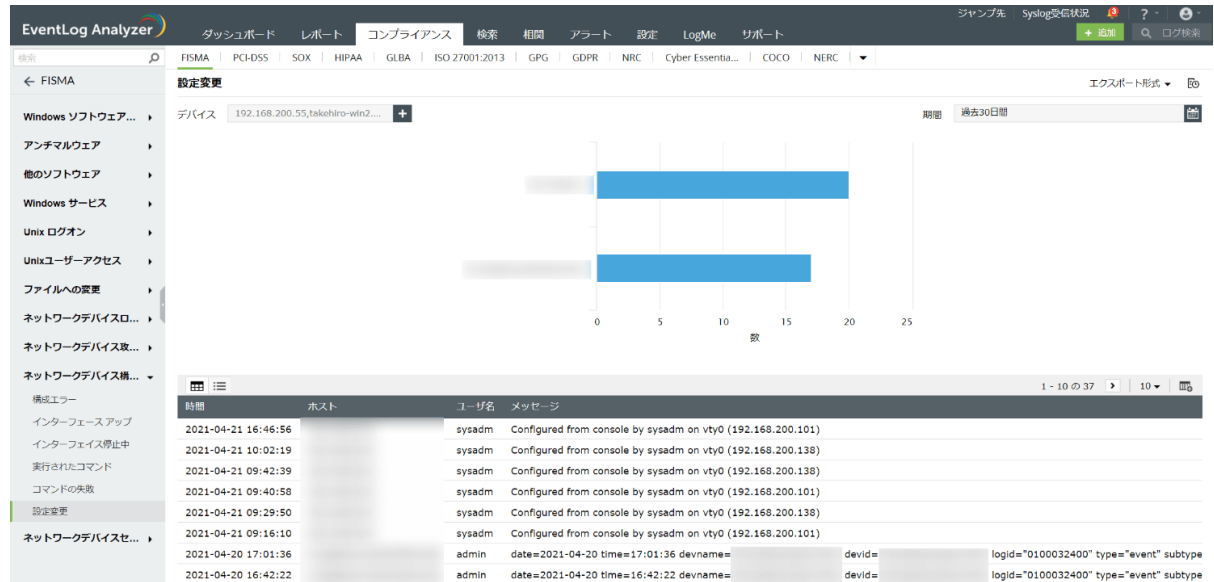
11-2 レポート

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。

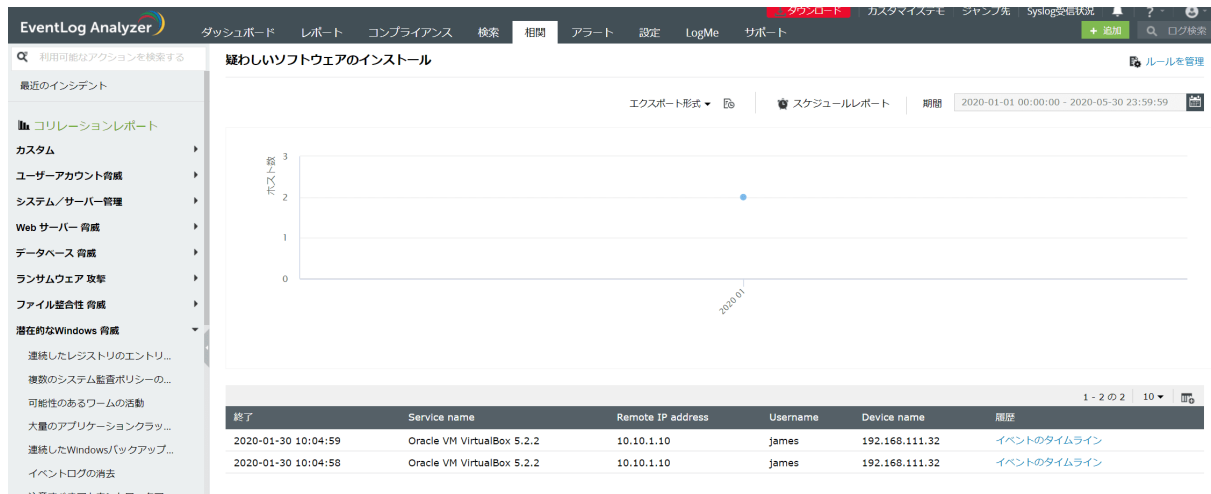
The screenshot shows the EventLog Analyzer search interface. The search bar contains the query `(EVENTID=4625) AND (USERNAME="administrator")`. Below the search bar, there is a detailed log entry for a failed login attempt. The entry includes a message in Japanese, a timestamp of 2021-04-21 22:47:17, and various fields such as Host, Event ID, Severity, Type, Source, User Name, and Task Category.

メッセージ: アカウントがログオンに失敗しました。 サブジェクト: セキュリティ ID: S-1-0-0 アカウント名: - アカントドメイン: ログオン ID: 0x0 ログオンタイプ: 3 ログオンを失敗したアカウント: セキュリティ ID: S-1-0-0 アカウント名: Administrator アカントドメイン: FIREWALLANALYZE エラー情報: 失敗の原因: ユーザー名を認識できないか、またはパスワードが間違っています。 状態: 0xc000006d サブ ステータス: 0xc000006a プロセス情報: 呼び出し側プロセス ID: 0x0 呼び出し側プロセス名: ネットワーク情報: ワークステーション名: FIREWALLANALYZE ソース: ネットワークアドレス: ユーザー名: 4662 詳細な認証情報: ログオン プロセス: NtLmSsp 認証パッケージ: NTLM 移行されたサービス: パッケージ名: NTLM のみ: キーの長さ: 0 このイベントは、ログオン要求が失敗した場合に生成されます。 このイベントは、アクセスを試行したコンピューターで生成されます。 サブジェクトのフィールドは、ログオンを要求したローカルシステム上のアカウントを示します。これは、サーバーサービスなどのサービスまたは Winlogon.exe や Services.exe などのローカル プロセスであることが最も一般的です。 ログオンタイプのフィールドは、要求されたログオンの種類を示します。最も一般的なタイプは、2 (対話型) と 3 (ネットワーク) です。 プロセス情報のフィールドは、ログオンを要求したシステム上のアカウントとプロセスを示します。 ネットワーク情報のフィールドは、リモート ログオン要求の送信元を示します。 ワークステーション名は、常に表示されるとは限らず、場合によっては空白のままであることがあります。 認証情報のフィールドは、この特定のログオン要求に関する詳細情報を示します。 - 移行されたサービスは、このログオン要求に関連した中間サービスを示します。 - パッケージ名は、NTLM プロトコルのうち使用されたサブプロトコルを示します。 - キーの長さは、生成されたセッション キーの長さを示します。これは、セッション キーが要求されなかった場合は 0 になります。

日時: 2021-04-21 22:47:17 ホスト: Log360 イベント ID: 4625 重要度: failure タイプ: Security ソース: Microsoft Windows Security Auditing ユーザー名: Administrator タスクカテゴリ: ログオン
一般レポート名: - ログタイプ: Windows エラーコード: - ドメイン: FIREWALLANALYZE リモートホスト IP: 表示名: Log360

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。



イベント履歴

- 10:04:59**
2020-01-30
Windowsにソフトウェアがインストールされました。
Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Pr... [詳細](#)
- 10:04:58**
2020-01-30
Windowsアカウントはリモートログオンに成功しました。
An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - A... [詳細](#)
- 10:04:58**
2020-01-30
ユーザーはFortinet VPNを使用してネットワークへのログオンに成功しました。
date=2020-01-28 time=12:58:40 devname=FortiGate-VM devid=FGVMEV0000000000 I... [詳細](#)
- 10:04:58**
2020-01-30
ユーザーはFortinet VPNを使用したネットワークへのログオンに失敗しました。
date=2020-01-28 time=12:58:35 devname=FortiGate-VM devid=FGVMEV0000000000 I... [詳細](#)
- 10:04:58**
2020-01-30
ユーザーはFortinet VPNを使用したネットワークへのログオンに失敗しました。
date=2020-01-28 time=12:58:24 devname=FortiGate-VM devid=FGVMEV0000000000 I... [詳細](#)
- 10:04:57**
2020-01-30
ユーザーはFortinet VPNを使用したネットワークへのログオンに失敗しました。
date=2020-01-28 time=12:58:09 devname=FortiGate-VM devid=FGVMEV0000000000 I... [詳細](#)

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。



通知時刻	アラートフォーマットメッセージ	レポート名	状態	ワークフローの状態	重要度	イベント名
2023-07-11 16:59:21	sshd: Accepted password for root from [redacted]	SSHログイン	オープン	ワークフローを実行する	information	Successful SSH Login
2023-07-11 16:59:20	sshd: Accepted password for root from [redacted]	SSHログイン	オープン	ワークフローを実行する	information	Successful SSH Login
2023-07-11 11:54:00	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-10 14:52:53	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-07 11:58:42	useradd: new user: name=postgres, UID=1001, GID=1001, home=/opt...	Unixの追加されたユーザーアカウ...	オープン	ワークフローを実行する	information	account added
2023-07-07 11:53:28	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-07 09:42:17	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-07 09:23:40	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-06 14:50:06	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success
2023-07-05 16:45:18	[redacted]	RDPログイン	オープン	ワークフローを実行する	success	Windows Logon Success

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/