ManageEngine
EventLog Analyzer

ManageEngine EventLog Analyzer

Quick Start Guide

14 November 2012

Version 1.0

Contents

Install and Start EventLog Analyzer

- Download the product from the download page
- Check the installation requirements

Install the product

Upon starting the installation you will be provided with two options:

- One Click Install
- Advanced Install

Choose **One Click Install** option to install the product in a single step. This means you agree to the product licensing terms. By default, the product will be installed in *C:\ManageEngine\EventLog* folder (/root/ManageEngine/EventLog/ in Linux). It will use port number 8400 for web server. It will be installed as a service.
Choose **Advanced Install** option to customize your product installation. The wizard screens will guide you through the installation.

Quick view of Advanced Installation

- Agree to the terms and conditions of the license agreement. You may get it printed and keep it for your offline reference
- Choose the **Standalone** edition to install. The editions available are, **Standalone, Distributed, and Free**
- Select the folder to install the product. Use the **Browse** option. The default installation location will be *C:\ManageEngine\EventLog* folder. If the new folder or the default folder does not exist, it will be created and the product will be installed.
- Enter the web server port. The default port number will be 8400. Ensure that the default port or the port you have selected is not occupied by some other application.
  Choose the language (Simplified Chinese, Traditional Chinese, English, Japanese, Others). Ensure that the browser supports the selected language.
  Choose the web protocol (HTTP/HTTPS). Use HTTP for unsecured and HTTPS for secured communication.
- Select **Install EventLog Analyzer as service** option to install the product as Windows service. By default this option is selected. Unselect this option to install as an application. You can install as application and later convert the same as service. ManageEngine recommends you to install it as service.
- Enter the folder name in which the product will be shown in the Program Folder. By default it will be **ManageEngine EventLog Analyzer <version number>** folder.
- Enter your personal details to get assistance.

At the end of the procedure, you can view the ReadMe file and start the EventLog Analyzer server. With this the EventLog Analyzer product installation is complete.

- Ensure the pre-requisites are met
- Run the product as a service or an application

Connect Web Client

If EventLog Analyzer is installed as a service, the Web Client is launched automatically. Or else you can open a new browser instance and connect to EventLog Analyzer by typing the hostname and port number

1. Open a supported web browser window
2. Type the URL address as ***http://<hostname>:8400*** (where *<hostname>* is the name of the machine on which EventLog Analyzer is running, and *8400* is the default web server port)
3. Log in to EventLog Analyzer using the default username/password combination of **admin/admin**.

Add Hosts

Add Windows host

In all Windows hosts, that you would like to monitor using EventLog Analyzer, ensure that WMI, DCOM are enabled; logging is enabled for respective module/ object.

1. Select the host type as Windows.
2. Enter the host name(s). Enter multiple host names separated by comma.
3. If you have logged in with Administrator rights, you will see the **Pick Hosts** option. Use the **Pick Host**s link to select one or multiple hosts from the Windows workgroups and domains and all the hosts of a workgroup or domain
4. Select the host group. For Windows host type, **Windows Group** will be the default selection.
5. The **Domain Name** field is optional only if the host machine is in the local workgroup. Ensure to manually type-in the domain name of the host(s). If **Pick Hosts** menu is used, **Domain Name** field will be filled automatically
6. Enter the **Login Name** (refers to user name) and **Password** to access the configured host(s). The user account should have admin privileges to fetch the logs. Use the **Verify Login** link to validate the credentials. If multiple hosts are selected, ensure that the credentials are valid for all the hosts
7. Enter the **Monitor Interval** to configure the frequency at which EventLog Analyzer should fetch the log from the hosts. By default, 10 minutes is the minimum monitor interval.
8. Click **Save** button to add the host(s). Use **Save & Add More** button to add more hosts

Note: If EventLog Analyzer has been installed on a UNIX machine, it cannot collect event logs from Windows hosts. However, third party applications like SNARE can be used to convert the Windows event logs to Syslog and forward it to EventLog Analyzer.

Add UNIX/ Linux hosts

UNIX/ Linux hosts configured to send Syslog data to the EventLog Analyzer on either of the default Syslog ports (**513** & **514**) need not be added as UNIX hosts in EventLog Analyzer and they will be automatically added to the list of hosts.

Import Application Logs

Application logs have to be imported into EventLog Analyzer. But in the case of Oracle, Print Server, and IBM iSeries applications logs can be fetched in real-time also. The software can import the application logs automatically at regular interval.

1. Use the **Local Host** option to import the log files from the local machine, from where you are accessing EventLog Analyzer over the web. The maximum log file size for import from local host is 1 GB.
2. Use the **Remote Host** option to import the log files from remote machines. The maximum log file size for import from remote host is 2 GB
3. Choose the log format you want to import. Choose the Windows Event Log format.
4. Click the **Import** button to start the file import operation

To import **Windows event log** format

Import Once from Local Host and Import Periodically

a. The time interval at which the log file should be imported is listed. It could be one time import or every hour or every day or every <xxx> minutes.
b. If you have selected **Local Host**, then the one time import (**Time Interval** : **Import Once**) option allows you to import the log file from the local machine/host EventLog Analyzer client.
c. Periodical import of log files (**Time Interval** - every hour or every day or every <xxx> minutes) is only possible if the log files are present in the EventLog Analyzer server machine.

Import Log from Remote Host

If you have selected **Remote Host,** to import the log file from the remote machines, for all **Time Interval** options manually type-in the location of the file or folder containing the log files in the remote machine. Alternatively, use the **Select Remote File** link to get the location of the file or folder

a. Use the '**Want to Specify Time Criteria**' option, if you want the import logs of a particular time period. Enter the time frame using the '**From**' and '**To**' fields. This option is applicable only for importing Windows event logs.
b. For *Windows Event Log* format, choose the **Log Type** from the list. The options are **Application, Security, System, DNS Server, File Replication Service, and Directory Service**
c. Use the **Create Throw Away Reports** option, if you want to import the log file for ad-hoc report generation. The imported log file will be retained only for two days and after that it will be purged

View Canned Reports

EventLog Analyzer offers a rich set of canned reports that help in analyzing network's internal security and audit the activities of internal users. The reports are displayed in the **Reports** tab of the UI. The event counts shown in the reports can be drilled down to get the raw logs. The logs can be filtered based on various log fields.

Description of reports

My Reports - The custom reports created will be listed in this section.
Top N Reports - The top network activities can be viewed with these reports. The top hosts accessed by most number of users, top users with most logins both successful and failed, top login results like successful, failed etc., and event severity wise top hosts and top processes are displayed in these reports.
User Activity Reports - These reports present the overview of user activities and user based activity. It can be filtered for hosts, users, and reports
Trend Reports - The event severity, event category and alert trend reports are available in this section. Reports are displayed in both graph and table formats. Reports can be configured for working and non-working hours and can be filtered for individual severity and category
Detailed Application Reports - The application reports display specific number of events for each application. The applications are, MS IIS W3C Web Server, MS IIS W3C FTP Server, Apache Web Server, DHCP Windows Server, DHCP Linux Server, Print Server, IBM Maximo Server, MS SQL Database Server, and Oracle Database Server
Detailed Host Reports - The detailed host reports display the number of events of each type that have been generated by that host in a selected time period.

- **Important Events** - EventLog Analyzer considers events such as user logon/logoff, user account changes, and server-specific events as important events, and shows them under the Important Events tab.
- **All Events** - All the events generated by the host, are classified by process (event type) and displayed under this tab.

Create Custom Reports

The custom reports created will be listed in the My Reports section. New reports can be added; existing report can be edited or deleted. Unscheduled reports can be scheduled. Refer the Create Custom Reports topic in the help document.

Search the Logs

EventLog Analyzer's Log search functionality is very easy and allows you to do a free form search. When a user enters a search criterion in the search bar, EventLog Analyzer rapidly drills down into the raw logs and retrieves the results for your search query. The results can be saved as report profiles.

- Refer the How to Search topic for explanation about search. You can carry out two types of searches: **Basic Search** and **Advanced Search**
- Refer the How to Extract Additional Fields topic for explanation about how to extract fields interactively

Create Alert Profiles

EventLog Analyzer can generate alert for occurrence of a specific security event and specific compliance event. Alert profiles can be created using pre-defined alert criteria, custom alert criteria, and compliance alert criteria. Refer the Create Alert Profiles topic in the help document.

Configure Email, SMS Settings

1. Ensure that you configure the **'Mail Server Settings'** to send the Email alert notification and distribute the scheduled reports generated
2. Configure the **SMS Settings**, if required. You need to configure the SMS Setting, in order to receive alert notifications in your mobile phone. You need to connect a physical device with a SIM card from service provider to send SMS alert notification.

Advanced Configurations

- EventLog Analyzer supports **MS SQL** as back end database. This is apart from the MySQL database bundled with the product. If you have MS SQL already in your enterprise, you can utilize the same with a simple migration procedure. Refer the procedure in the help document
- EventLog Analyzer archives the log files periodically for internal, forensic and compliance audits. The archival interval and retention period is configurable. The **archive** file can be encrypted and time-stamped to make it secure and tamper-proof.
- EventLog Analyzer retains the log data in the database for a limited period to process. After the period is over, the data is purged from the database. You can set the **database storage size**.
- Configure **'Log Collection Alert'** under Settings tab, so that you would receive an alert, if the EventLog Analyzer does not receive logs from the hosts for a span of more than 15 minutes

For more startup information refer the following topics:

- Frequently Asked Question (FAQ)
- Troubleshooting Tips