ManageEngine
EventLog Analyzer

EventLog Analyzer:

BEST PRACTICES GUIDE

Table of Contents

This guide details best practices which, if followed, ensure smooth operation and optimum performance of EventLog Analyzer.

System requirements

Hardware specifications

The minimum hardware requirements for the EventLog Analyzer server are a dual core processor and 2 GB RAM. Ideally, a quad core processor and 6 GB RAM would provide optimum performance. This is because the number of processor cores determines the indexing and search performance of the installation. More the number of cores, better the performance of the tool. Running Eventlog Analyzer in VMware is not recommended.

Event handling capacity

A standalone installation of EventLog Analyzer can handle an average log rate of 20,000 EPS (events per second) for syslogs and 2,000 EPS for event logs. To enhance the events handling capacity, a distributed EventLog Analyzer installation with multiple nodes can handle higher log volumes.

RAM allocation

To ensure optimal performance, it is recommended not to allocate more than 64 GB to a single instance of the ELA Server.

Optimizing hard disk space

The two main contributing factors to hard disk space are the database and archive files. The database (or index) files contain the most recent log data which can be reported on and searched, while the archive files contain the older, historic log data. Archive files need to be loaded into the product first before they can be searched or reported on.

Required hard disk space

The hard disk space required to store logs can be calculated by using the procedure detailed in the performance optimization guide in the EventLog Analyzer website

Manage database size

Log data is stored in the database and is periodically compressed and stored among the archive files. The longer the retention period in the database, the greater is the hard disk space needed and lower the database performance. The default retention period is 32 days and is configurable (Settings > Admin settings > DB retention settings). Minimize this value to obtain optimum performance.

Manage archive size

The archive files are retained for a specific period before being deleted permanently. As they can even be stored forever, the size of the archive folder could grow indefinitely. The archive retention period is forever and is configurable (Settings > Configuration settings > View archived files > Settings with Settings > Admin settings > View archived files > Settings). The archive folder size can also be managed by assigning a separate dedicated drive as the archive location, or manually transferring the contents to a tape drive or high capacity storage drive periodically.

Securing EventLog Analyzer

Installation configuration

The operating system user account used to install and run the product must be the same and must have permissions on all installed folders and subfolders. While it is not necessary for the root account to be used on a Linux system, on a Windows system, only the default administrator account must be used.

User configuration

It is best to change the default passwords for the admin and guest user accounts in the EventLog Analyzer web client (Settings > Admin settings > Manage technician)

SSL certification

EventLog Analyzer server-client communication can be secured using the SSL (Secure Sockets Layer) protocol. The SSL certification guide offers detailed steps on how to obtain SSL certification.

Database best practices

Secure database

For smooth and seamless installation, EventLog Analyzer makes use of the MySQL or PostgreSQL database default root/postgres user without password. It is recommended to assign a password to this account in order to further secure the database.

This is not needed in case of MS SQL, as a valid user account with credentials needs to be provided during installation itself.

Optimize PostgreSQL database performance

To optimize performance of the PostgreSQL database:

- Stop EventLog Analyzer.
- Navigate to <EventLog Analyzer home>/pgsql/data/directory.
- Open the file postgres_ext.txt.
- Replace the existing values of the parameters, with the values mentioned below.
- Save and restart EventLog Analyzer.

Parameter	Comment
shared_buffers=128 MB	Minimum requirement is 128 KB.
work_mem=12 MB	Minimum requirement is 64 KB.
maintenance_work_mem=100 MB	Minimum requirement is 1 MB.
checkpoint_segments=15	Logfile segments minimum 1 and 16 MB each.
checkpoint_timeout=11 minutes	Range: 30 seconds to 1 hour.
checkpoint_completion_target=0.9	checkpoint target duration is 0.0 - 1.0.
seq_page_cost=1.0	This parameter is measured in an arbitrary scale.
random_page_cost=2.0	This parameter is measured in same scale as above.
effective_cache_size=512MB	
synchronous_commit=off	

Optimize MySQL database performance

To optimize performance of the MySQL database:

- Stop EventLog Analyzer.
- Navigate to <EventLog Analyzer home>/bin.
- Open the file startDB.bat (startDB.sh in case of a Linux machine).
- Replace the existing value of the parameter "--innodb_buffer_pool_size", with a value suited to the RAM size of the machine, as given in the table below. For example, if the RAM size is 8 GB, the parameter should be "--innodb_buffer_pool_size=3000M".
- Save and restart EventLog Analyzer.

RAM Size	Value
1 GB	Default value (no need to replace)
2 GB	1200M
3 GB	1500M
4 GB	1500M
8 GB	3000M
16 GB	3000M

Back up database

It is recommended to back up the EventLog Analyzer database every fortnight, so that data is not lost in case of any disaster. The database files are located in the <EventLog Analyzer home>/mysql or <EventLog Analyzer home>/pgsql folder, as applicable to the build number. To back up the data, stop the EventLog Analyzer service, and take a copy of all files and folders in the location. This can be done manually or using any third party back up software. The procedure to back up MS SQL database data can be found in this link. It is also advisable to keep a backup of the archive files, found in <EventLog Analyzer>/archive. If restoring data from a backup, ensure that the build number of the product is the same as when the backup was taken.

Support best practices

Create Support Information File (SIF)

When support is required, creating a Support Information File (SIF) to send to the support team (eventloganalyzer-support@manageengine.com) would be helpful and time saving. To create a SIF from the web client, go to the Support tab of the product. Click on 'Create Support Information File', wait 30-40 seconds, and click on the Support tab again. Click on download and send the downloaded SIF to the support team, or click 'Upload to FTP Server', provide the required details and submit. If the server or web client is not working, zip the files found at <EventLog Analyzer Home>/server/default/log and upload the zip file in this FTP link.

About EventLog Analyzer

EventLog Analyzer is a comprehensive IT compliance and log management software for SIEM. It provides detailed insights into your machine logs in the form of reports to help mitigate threats in order to achieve complete network security. https://blogs.manageengine.com/eventloganalyzer

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.