ManageEngine®

EventLog Analyzer

Best Practices Document

Table of Contents

System Requirements

CPU and RAM Requirements

The CPU (Processor & Speed) and RAM size requirements depend on net log rate, the average log record size, and the number of hosts sending log information sent to the EventLog Analyzer.

Hard Disk Space Requirements

The hard disk space requirement depends on the log volume, per day, to be archived by EventLog Analyzer.

Up to 50 hosts

Log Rate	Speed, CPU Specification	RAM	Log Volume	Hard Disk Space
100/sec	1 GHz, Pentium 4 processor	512 MB	1.5 GB/day	150 GB
300/sec	1 GHz, Pentium 4 processor dedicated machine	1 GB	4.5 GB/day	450 GB
500/sec	1.5 GHz, Pentium Dual Core dedicated machine	2 GB	7 GB/day	720 GB

Up to 100 hosts

Log Rate	Speed, CPU Specification	RAM	Log Volume	Hard Disk Space
100/sec	1 GHz, Pentium 4 processor dedicated machine	1 GB	3 GB/day	300 GB
300/sec	1.5 GHz, Pentium Dual Core dedicated machine	2 GB	9 GB/day	900 GB
500/sec	1.5 GHz, Pentium Dual Core dedicated machine	4 GB	15 GB/day	1500 GB

Up to 200 hosts

Log Rate	Speed, CPU Specification	RAM	Log Volume	Hard Disk Space
100/sec	1.5 GHz, Pentium Dual Core dedicated machine	2 GB	6 GB/day	600 GB
300/sec	1.5 GHz, Pentium Dual Core dedicated machine	4 GB	18 GB/day	1800 GB
500/sec	2 GHz, Pentium Quad Core dedicated machine	8 GB	30 GB/day	3000 GB

Note: For 200 hosts and log rate exceeding 300/sec, EventLog Analyzer technical team recommends you to use MS SQL as back end database.

Up to 500 hosts

Log Rate	Speed, CPU Specification	RAM	Log Volume	Hard Disk Space
100/sec	1.5 GHz, Pentium Dual Core dedicated machine	4 GB	15 GB/day	1500 GB
300/sec	2 GHz, Pentium Quad Core dedicated machine	8 GB	45 GB/day	4500 GB
500/sec	2 GHz, Pentium Quad Core dedicated machine	16 GB	75 GB/day	7500 GB

Above 500 hosts

If your deployment involves more than 500 hosts, please consult our technical team for exact requirements.

Note:

- The above given requirement calculation is based on approximation of an average log record size of 350 bytes.
- The Hard Disk space requirement projected is for one month. If you need to archive the logs for more number of months, multiply the above requirements with the number of months based on your requirement.

Optimizing Hard Disc Space

Controlling hard disk space growth

EventLog Analyzer has two main data sources that consume hard disc space. One is database and the other is archive file storage. The log data, for MySQL database, is stored in the *<EventLog Analyzer Home>/mysql* directory and the archive files are stored in the *<EventLog Analyzer Home>/archive* directory.

Optimize database hard disk space

EventLog Analyzer stores the log data in the database to analyze and generate reports. But the logs cannot be kept stored in the database forever. This will not only increases the hard disk space consumption, but also downgrade the database performance. The log data in the database is periodically stored in the archive. The time duration to retain the data in the database is configurable. Default value is 32 days. Change the value to optimize the storage.

Optimize archive hard disk space

EventLog Analyzer stores the copy of the log files collected from all the configured hosts in the archive directory, hence the size of this archive folder will grow indefinitely.

You can control the hard disk space growth by following the practices given below:

- Changing the archive folder to another location. Use the *Settings* > *Archived Files* > *Archive Settings* menu in EventLog Analyzer web-client.
- You can keep two locations for archiving and keep swapping locations periodically. Transfer the contents of the dormant archive to tape drive or high capacity storage, so that you can store them for longer period.
- You can assign separate dedicated drive(s) to archive log files and overcome the disk space limitation.

Securing EventLog Analyzer

Installation configuration

- It is recommended to install EventLog Analyzer as service. When it is installed as service, any time you boot the system, the EventLog Analyzer service will start automatically without your manual intervention. In one click installation, by default EventLog Analyzer will be installed as service. Even if you have installed EventLog Analyzer as application, you can convert it to service by a simple procedure.
- The OS user account needs full permissions on all folders and subfolders in the installation folder of EventLog Analyzer only.
- It is NOT necessary to install EventLog Analyzer in root (in Linux) user account. But, it is necessary to install EventLog Analyzer in Administrator (in Windows) user account. Ensure that the whole installation is done using the same OS user account.
- For installation and running of the application/service, same OS user account should be used. Installing the application using *root* and running it using an *OS user* account will fail.

Precautions for EventLog Analyzer Installation Directory

- Exclude the EventLog Analyzer installation directory ‘AdventNet’ (it could be in C:\AdventNet or D:\AdventNet) from both the System Backup and Anti-Virus Scan, since it may corrupt the MySQL tables.

User configuration

- Make sure you change the password for the default **admin** and **guest** web client users within EventLog Analyzer.

Securing Server-Client communication

If you want to secure the EventLog Analyzer server-client communication, you can implement Secured Socket Layer (SSL).

Refer the Help documents for the detailed procedure to configure SSL for EventLog Analyzer Server-Client communication given in the below link:

http://www.manageengine.com/products/eventlog/help/appendix/eventflow_ssl_support.html

Best database practices

Securing MySQL database installation

For smooth and seamless installation, EventLog Analyzer uses the MySQL database default '**root**' user without password. You can secure MySQL database installation harder, by assigning password to the '**root**' user.
It is recommended to assign password to default **root** user.

Refer the Frequently Asked Questions for the detailed procedure to assign/change MySQL Database password given in the below link.

http://www.manageengine.com/products/eventlog/faq.html#17_2

Securing MS SQL database installation

For MS SQL database, there is no requirement to assign password, because during installation of the product itself you have to provide, a valid MS SQL user account with credentials, apart from other parameters.

Optimizing MySQL database performance

For better performance, you can configure the existing MySQL parameters with the corresponding changes to the EventLog Analyzer servers RAM Size.

Refer the Help documents for the detailed procedure to configure the MySQL parameters given in the below link:

http://www.manageengine.com/products/eventlog/system_requirement.html#mysql

Separating MySQL database installation to optimize performance

EventLog Analyzer server and MySQL database can be installed in separate machines, in case of higher log rate with low-end CPU machines.

Data backup practices

Backup the EventLog Analyzer data

It is recommended to backup the EventLog Analyzer data in database every fortnight, so that data is not lost in case of any disaster.

Before taking backup of the EventLog Analyzer data, please shutdown the EventLog Analyzer server/service.

MySQL

Take the copy of the following folder and files manually or use any third party backup software.

<EventLog Analyzer Home>/mysql/

Note: Please take the complete backup of folder including the files and sub folders.

MS SQL

For the procedure to take backup of MS SQL database, refer the link given below:

http://support.microsoft.com/kb/930615

We would also suggest you to take a copy of the Archive folder, located under *<EventLog Analyzer Home>/archive/*, if you would like to clear some space on HDD.

You can do the above steps once every fortnight and restore it if there is any issue.

Note: Please make sure that the build number is same while restoring, if not, get back to us. We will consider automating the backup process in our future releases.

Best support practices

Procedure to create a Support Information File (SIF) and send the SIF to EventLog Analyzer support

We would recommend the user to create a Support Information File (SIF) and send the SIF to eventloganalyzer-support@manageengine.com

The instructions for creating the SIF is as follows:

- Login to the Web-client and click the 'Support' tab.
- Click the 'Create Support Information File' link show in that page.
- Wait for 30-40 Secs and again click the 'Support' tab.
- Now you will find new links 'Download' and 'Upload to FTPServer'.
- You can either download the SIF by clicking on the “Download’ link and then send the downloaded SIF to eventloganalyzer-support@manageengine.com or click the 'Upload to FTP Server' and provide the details asked and upload the file.

Procedure to create SIF and send the file to ZOHO Corp., if the EventLog Analyzer server or web client is not working

If you are unable to create a SIF from the web client UI, you can zip the files under '**log**' folder, which is located in *<EventLog Analyzer Home>\server\default\log* (default path) and send the zip file by upload it in the following ftp link:

http://bonitas.adventnet.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com