Have you ever had difficulties while troubleshooting a problem because of lost or missing log messages?

Do you have to handle sensitive log data?

Are you having problems with the performance of your logging system?

Do you need to forward your logs for further analysis?

- Open Source
- Encrypted message transport using TLS
- Direct Database Access
- Easy to extend in C or Java/Lua/Perl/Python
- A large variety of sources and destinations
- Real-time message classification
- High-performance multi-thread processing
- Filter, parse, rewrite

The syslog-ng™ solution collects log messages from a wide variety of devices and applications, and can transfer them to a central log server in an encrypted channel. You can process the messages with parsers to extract important information into key-value pairs, and normalize data to simplify further analysis and processing. You can remove or modify sensitive data, such as credit card numbers or IP addresses for legal or compliance purposes. Finally, you can store your logs in files or databases, or forward them to a wide variety of NoSQL, key-value store, alerting and visualization systems. You can use JSON formatting to preserve structured data from messages. The syslog-ng™ Open Source Edition is complemented with the syslog-ng™ incubator project, offering experimental features like ZeroMQ support, a Kafka destination, and bindings to popular programming languages, like Python or Java.

Secure log transfer

The syslog-ng™ application enables you to send log messages of your hosts to a central logserver using the latest syslog protocol standards. Using mutually-authenticated and TLS-encrypted channels maintains the confidentiality of the transferred information.

Open Source

Released under a combination of the GNU General Public License (GPL) and Lesser General Public License (LGPL) - you can tweak it, extend it, customize it the way you want. Developed in the open: code, issues, mailing list all available!

http://syslog-ng.org

Easy to extend in C or Java/Lua/Perl/Python

The core of syslog-ng™ is written in C, making it lightning fast. Most modules are also written in C, but modules in the syslog-ng™ incubator make it possible to extend syslog-ng™ with destinations written in Java, Lua, Perl or Python. These applications run inside syslog-ng™ and receive all the message data (like name-value pairs) from syslog-ng™. The ElasticSearch destination was created this way, and it's now easy to do custom log processing or connect to systems not yet directly supported by syslog-ng™.

Direct database access

Storing log messages in a database allows you to easily search and query the messages and interoperate with log analysis applications.

Filter, parse and rewrite

The syslog-ng™ application can sort the incoming log messages based on their content and various parameters like the source host, application, and priority. It can also separate parts of log messages to named fields or columns, and modify the values of these fields, for example, to remove sensitive data. Complex filtering using regular expressions and boolean operators offers almost unlimited flexibility to forward only the important log messages to the selected destinations.

Classify messages

The syslog-ng™ application can classify messages using the Pattern DB™ feature. Identified messages can be tagged and filtered based on their content. Message classification is done real-time. The message patterns can be easily extended and customized to cover additional applications.

Scale to the largest environments

With multi-thread processing the syslog-ng™ Open Source Edition delivers unparalleled performance. Depending on its exact configuration, it can process over 650,000 messages per second real-time, and over 300 GB raw logs per hour on standard server hardware.

A large variety of destinations

Send your log messages to:

- NoSQL databases (like MongoDB)
- key-value stores (like Redis)
- alerting systems (like Riemann)
- visualization tools (like Graphite)
- message queuing (like ZeroMQ)

If something is not yet supported, it's easy to extend syslog-ng™ in C or other programming languages.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com

ONE IDENTITY™