BALASYS

One Identity syslog-ng Premium Edition

Enterprise Class Log Management

BENEFITS

- High performance collection
- Zero message loss transfer
- Real-time filtering, parsing, rewriting, normalization
- Pattern-matching and correlation
- Data enrichment with key-value pairs from an external database
- Write your own parsers and templates in Python
- Secure transfer using TLS
- Tamper-proof, encrypted storage
- Installation packages for more than 50 server platforms, including Windows
- Send log data directly to Apache Hadoop, Elasticsearch, MongoDB, and Apache Kafka
- Central configuration management with Puppet
- Easy self-monitoring with enterprise integration

INTRODUCTION

The syslog-ng Premium Edition delivers the log data critical to understanding what is happening in your IT environment. Whether it's user activity, performance metrics, network traffic, or any other log data, syslog-ng can collect and centralize it. You can remove data silos and gain full-stack visibility of your IT environment.

Scale up your log management

Depending on its configuration, one syslog-ng server can collect more than half a million log message per second from thousands of log sources. A single central server can collect log messages from more than 5,000 log source hosts. When deployed in a client relay configuration, a single syslog-ng log server can collect logs from tens of thousands of log sources.

Secure your log data

Encrypted transfer and storage ensure logs cannot be tampered with, preserving the digital chain of custody. TLS encryption prevents 3rd parties from accessing log data. The Premium Edition of syslog-ng can store log messages securely in encrypted, compressed, and timestamped binary files, so any sensitive data is available only for authorized personnel who have the appropriate encryption key.

Hortonworks Certified HDP

MAPR Certified Technology Partner

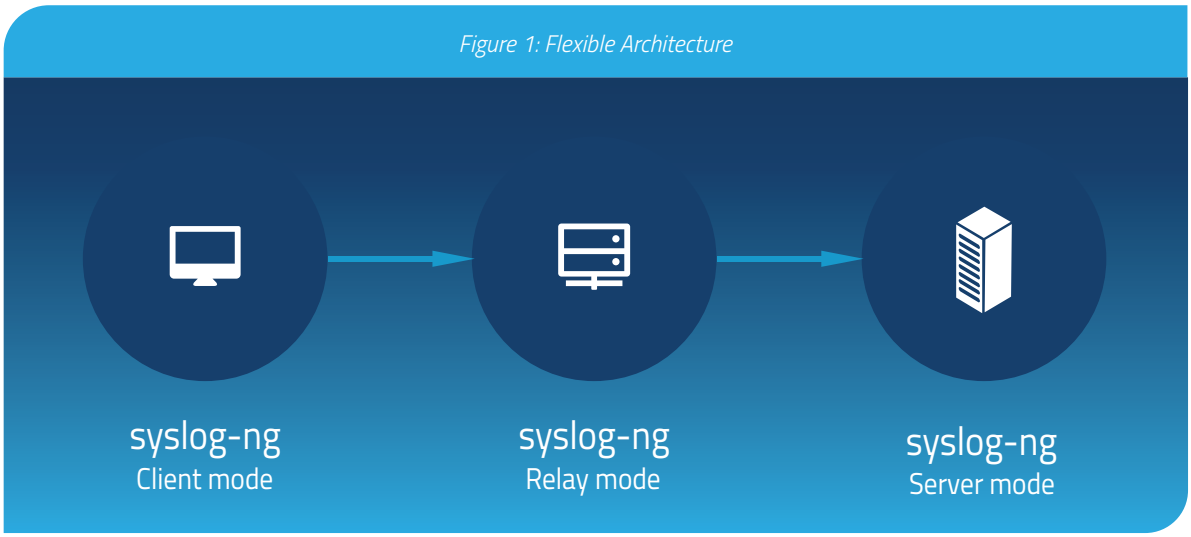

Figure 1: Flexible Architecture

Have confidence in the data underlying your analytics, forensics, and compliance efforts

Using local disk buffering, client-side failover, and application layer acknowledgement, syslog-ng can transfer logs with zero message loss.

Syslog-ng stores messages on the local hard disk if the central log server or the network connection becomes unavailable. The syslog-ng application automatically sends the stored messages to the server when the connection is reestablished in the same order the messages were received.

The syslog-ng Premium Edition supports the Reliable Log Transfer Protocol (RLTP™) which enables application level acknowledgement of message receipt. The syslog-ng application residing on the server acknowledges receipt of log messages from the syslog-ng application on the client, ensuring that messages are not lost in the event of a transport layer fault.

Optimize your analytic tools

With powerful filtering, parsing, re-writing and classification options, syslog-ng can transform logs on remote hosts, reducing the amount and complexity of log data forwarded to analytic tools like SIEM, reducing their total cost of ownership.

The PatternDB™ feature can correlate log data in real-time, comparing log message content with predefined patterns. The flexible configuration language allows users to construct powerful, complex log processing systems on remote hosts with simple rules.

Flexibly route logs

syslog-ng can collect log messages from a wide variety of sources and flexibly route them to multiple destinations.

syslog-ng Premium Edition can natively collect and process log messages from any device sending logs via the syslog protocol, SQL databases, Microsoft Windows platforms as well as JSON formatted messages or plain text files. It can also process multiline log messages, for example, Apache Tomcat messages.

Many large organizations need to send their logs to multiple log analysis tools. Most log analysis and SIEM solutions can receive syslog messages. The syslog-ng application can send logs directly to SQL databases, Elasticsearch including support for Shield enabled secure deployments, MongoDB, Apache Kafka, and Hadoop Distributed File System (HDFS) nodes, or use the Standard Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) for other destinations.

Reduce maintenance and deployment costs with universal log collection

syslog-ng can be deployed as an agent on a wide variety of hosts and flexibly route logs to multiple analytic tools or databases, eliminating the need to deploy multiple agents on servers. Tested binary files for the syslog-ng Premium Edition are available for more than 50 server platforms reducing the time required for installation and maintenance.

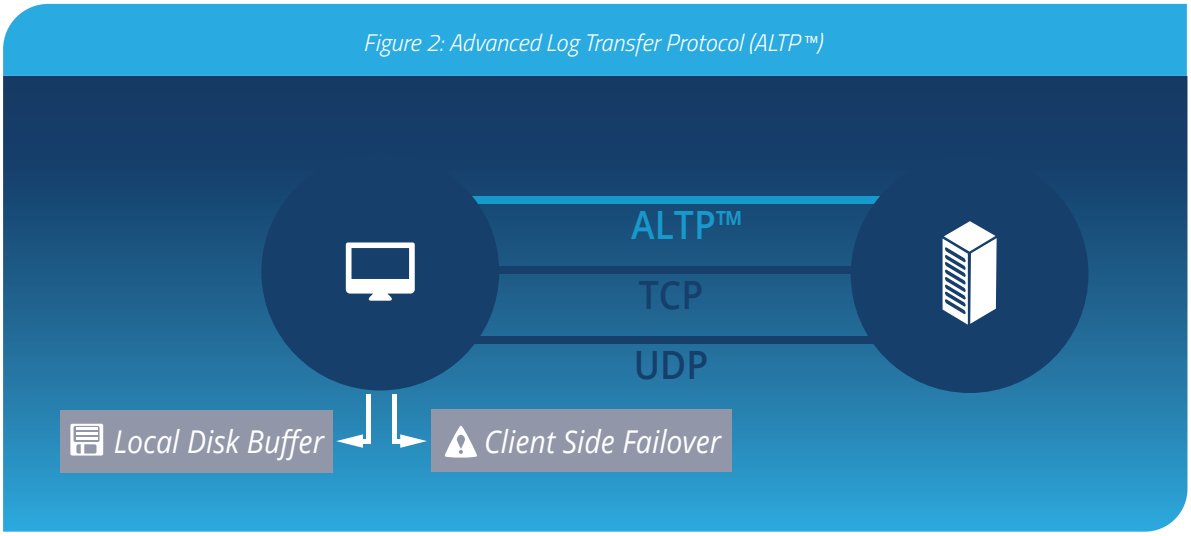

Figure 2: Advanced Log Transfer Protocol (ALTP™)

Centralized configuration management

syslog-ng supports the Puppet configuration management software enabling you to install syslog-ng from a package repository, upgrade syslog-ng to a newer version, delete syslog-ng from a host, update the syslog-ng PE configuration file on remote hosts from a central repository, and create backup of your syslog-ng configuration files, and perform a rollback if needed.

Licensing and support

Licensing is based on the number of Log Source Hosts (LSH). There are no license limits on the amount or rate of data processed or stored, making project budgeting easy. Purchasing syslog-ng Premium Edition entitles you to access binary installation files for more than 50 server platforms. Product support – including 7x24 support – is available on an annual basis.

ONE IDENTITY™

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.

Balasys IT Ltd. | Alíz Street 4. H-1117 Budapest | Phone: +36 1 646 4740 | sales@balasys.hu