syslog-ng
by Quest

syslog-ng™ Premium Edition

Enterprise Class Log Management

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.

The **Premium Edition** of syslog-ng™ can **store** log messages **securely** in **encrypted**, **compressed**, and **timestamped** binary files.

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, ensuring that sensitive data is accessible only to authorized personnel with the appropriate encryption key.

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 all major Linux distributions with all features and dependencies included.
- Collecting Windows Event Logs without installing an agent
- Send log data directly to Apache Hadoop, Elasticsearch, Google Pub/Sub, Azure Sentinel, Splunk-HEC, MongoDB, Apache Kafka and others
- Easy self-monitoring with enterprise integration

Flexible Architecture

syslog-ng™ Client Mode

syslog-ng™ Relay Mode

syslog-ng™ Server Mode

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, such as 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, MongoDB, Apache Kafka, and Hadoop Distributed File System (HDFS) nodes. It can also use the Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) for other destinations.

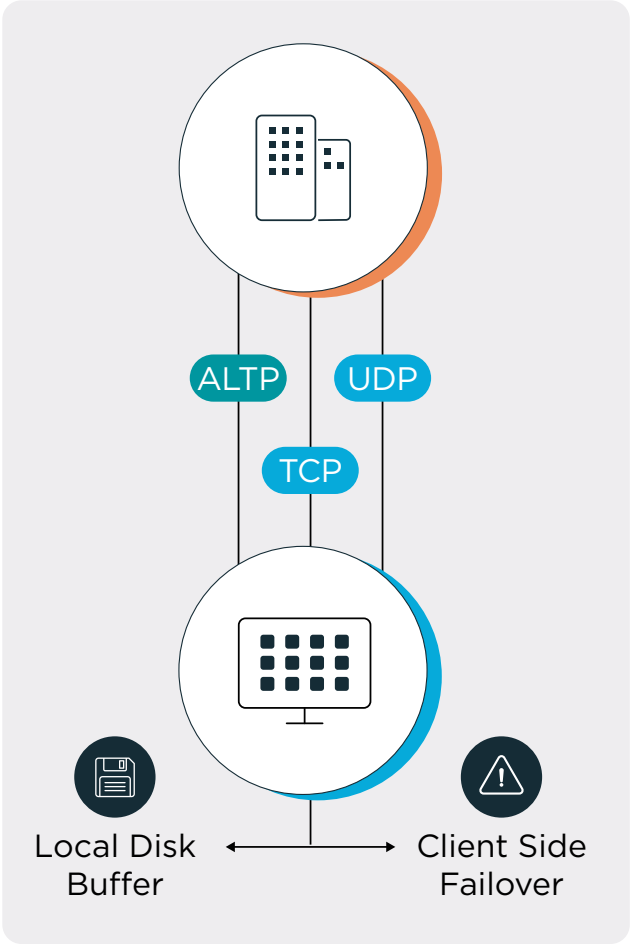
ONE IDENTITY by Quest

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 Advanced Log Transport Protocol (ALTP) 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.



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. Native binary syslog-ng Premium Edition installation packages are available for supported Linux platforms.

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.

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 supported server platforms. Product support – including 7x24 support – is available on an annual basis.

Learn more

- Read more about syslog-ng™ Premium Edition
- Request an evaluation
- Request a callback

About One Identity

One Identity delivers comprehensive cloud and on-premises identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to their business. Our Unified Identity Platform brings together best-in-class identity governance and administration (IGA), access management (AM), privileged access management (PAM) and Active Directory management (AD Mgmt) capabilities. This holistic approach enables organizations to increase the visibility, control and protection over all their identities. Proven and trusted on a global scale, One Identity manages more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

One Identity LLC
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

ONE IDENTITY by Quest