syslog-ng™
for Big Data

ONE IDENTITY™

Your data is important. No matter what problem you're trying to solve or question you need to answer, you need the right data at the right time. Whether that data is system logs, application logs, clickstream data, or metrics, delivering data from source to analytics tool is critical. For some problems, conventional data management tools are not enough. Distributed file systems, NoSQL databases and queuing systems are the backbone of today's big data deployments and syslog-ng™ delivers log data from a wide variety of sources directly to these data management tools.

Collect From a Wide Variety of Sources
syslog-ng™ can collect logs from legacy systems, web servers, SQL databases as well as any applications or devices generating JSON messages or text-based files.

Transform data in real-time
Using syslog-ng™'s Pattern Database you can classify, filter, parse, and re-write to transform disparate data types in real-time. You can turn unstructured text into key value pairs for processing by big data tools.

Flexibly Route Data
Data consumers have different needs and many organizations use a variety of data management and analysis tools, syslog-ng™ can flexibly route data from X sources to Y destinations.

Deliver Data with End-to-End Reliability
Data transfer over TCP and the Reliable Log Transfer Protocol (RLTP™), local disk buffering, client-side failover and other features ensure zero message loss, giving you confidence in your data.

Send to Hadoop
syslog-ng™ natively streams data to Hadoop Distributed File System as well as the MapR distributed file system. We have partnered with Hadoop pioneers Hortonworks and MapR to ensure seamless data transfer from syslog-ng™ to your Hadoop cluster.

Send to Elasticsearch
syslog-ng™ streams log data directly to Elasticsearch, one of the most popular enterprise search engines. syslog-ng™ delivers log data to Elasticsearch in JSON format where it can be searched.

Send to MongoDB
syslog-ng™ sends log data to MongoDB, a popular document NoSQL database. With its schema-free, document-oriented architecture, MongoDB is used as a backend to many websites and services.

Send to Apache Kafka
syslog-ng™ directly sends data messages to Apache Kafka, a messaging system designed for streaming data use cases with large amounts of data and low latency requirements. syslog-ng™ publishes log messages to Kafka where subscribers can access them.

syslog, event log, Journal, JSON, TXT, CSV → **syslog-ng** → SQL, Hadoop, Elasticsearch, MongoDB, Kafka

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™

syslog-ng.com