Log Analytics v1.0

Assure service performance and security to maximize customer satisfaction.

Benefits

- Provides a fully tested and vendor-supported distribution of the industry-leading search data engine from Elastic™
- High-performance, vendor agnostic, and closed loop to the control system.
- Bundled open source pipeline approach yields an end to end data stack in a single delivery package.
- Docker container run time environment enables a hardware agnostic solution supporting bare metal or virtual hosting on private or public clouds.
- Real-time contextual message indexing using an XML based pattern definition template and expression-based matching.
- DevPack add-ons deliver out of the box templates to support managed products with no additional development.
- High speed REST northbound API with cluster-wide search and egress message bus delivery.

Use Cases

- Secuirty Visibility
- Mobile Edge Visibility
- OpenStack Visibility
- ONAP DCAE Visibility

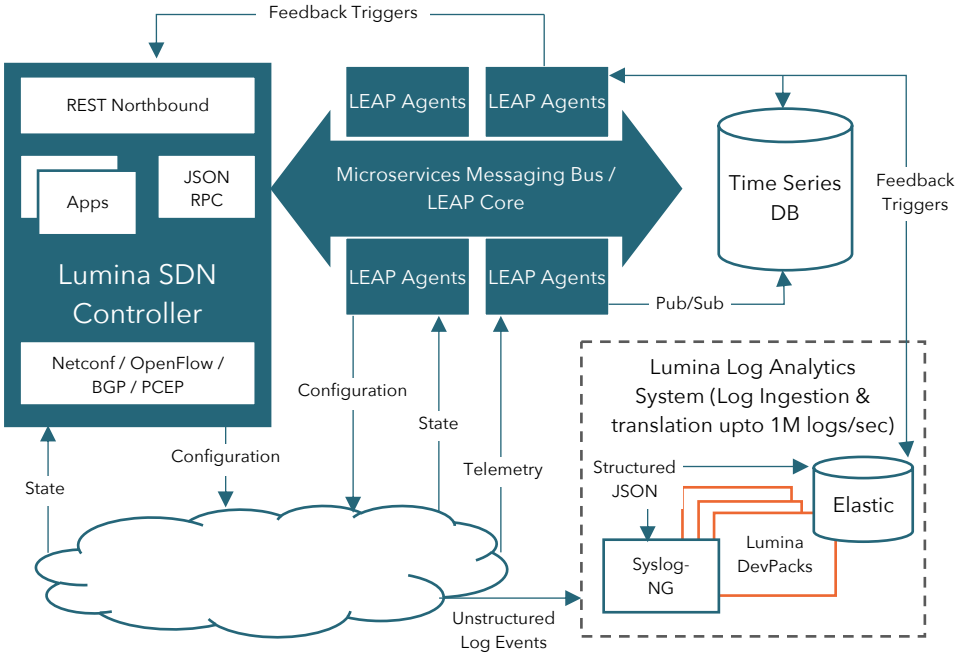
At a Glance

Delivering on a primary objective to ingest, process, organize and retain security log message streams, OLS enables efficient open access of indexed message data by backend security analytics and threat detection platforms, unlocking deep visibility into firewall performance and traffic behavior.

The OLS approach is based on community driven projects, stitched together and abstracted into a common open-source process pipeline. The resulting data stack is quality assured, scale tested and packaged with traditional commercial software support, mitigating Lifecyle risk and providing ongoing capital protection.

Offered with an unlimited volume pricing model and able to handle extreme message rate while requiring only minimal resource expense, OLS is a must-have function for a modern security OSS architecture, shown to quickly return customer business value.

Solution Architecture



Specifications

Ingestion & Processing

- Maximum single instance message rate of 100K log messages per second.
- Load balancing function to distribute a single incoming stream to pools of listeners using either UDP or TCP inside connections
- Maximum cluster message rate of upto 1M logs/sec
- Scalable concurrent listeners, ingesting, indexing and inserting optimized message date into the date engine
- Support for standard syslog UDP/TCP message and IPFix binary stream message, over either IPv4 and IPv6
- Pre-processing ability to take accept or drop action based on message property matches

Data Organization

- An user extensible XML template with pattern matching to define indexed key value pairs
- Message content substitution, driven by a lookup against an external mapping table
- High performance multi-threaded query engine, supports filtering on key value pairs and returns matching log messages with or without extended detail
- Single cluster query interface, to run the same query across multiple data engine instances returning results into a common message bus topic

Data Retention

- Uncompressed data is stored for 72 hours to optimize performance of short-term results.
- After 72 hours, data will be compressed and stored for 14 days.
- After 14 days, compressed data will be moved offline for up to 180 days.

Open Access

- High performance REST API to drive backend integration and provide directional query interface.
- “Raw” message bus provides data buffering improving data reliability and outside system access.
- “Cluster” message bus aggregates data engine instance output stream and provides asyncronous status information.