Apica

DATA SHEET

Log Management for Modern Data Enterprises

Quick Summary

Apica's Log Management platform revolutionizes observability data management for organizations. It offers advanced log aggregation technology that enables seamless collection, optimization, analysis, and routing of log data across any scale. Apica provides a cost-effective, scalable, and feature-rich solution that ensures compliance, enhances security, and facilitates fast, efficient troubleshooting.

Key Benefits

Designed for cost-efficiency and scalable log management for organizations of any size.

Feature-rich and easily customizable to meet specific needs.

Ensures compliance, long-term retention, and security with PII masking.

AI-driven analytics for fast issue detection, complete coverage, and quick root cause analysis.

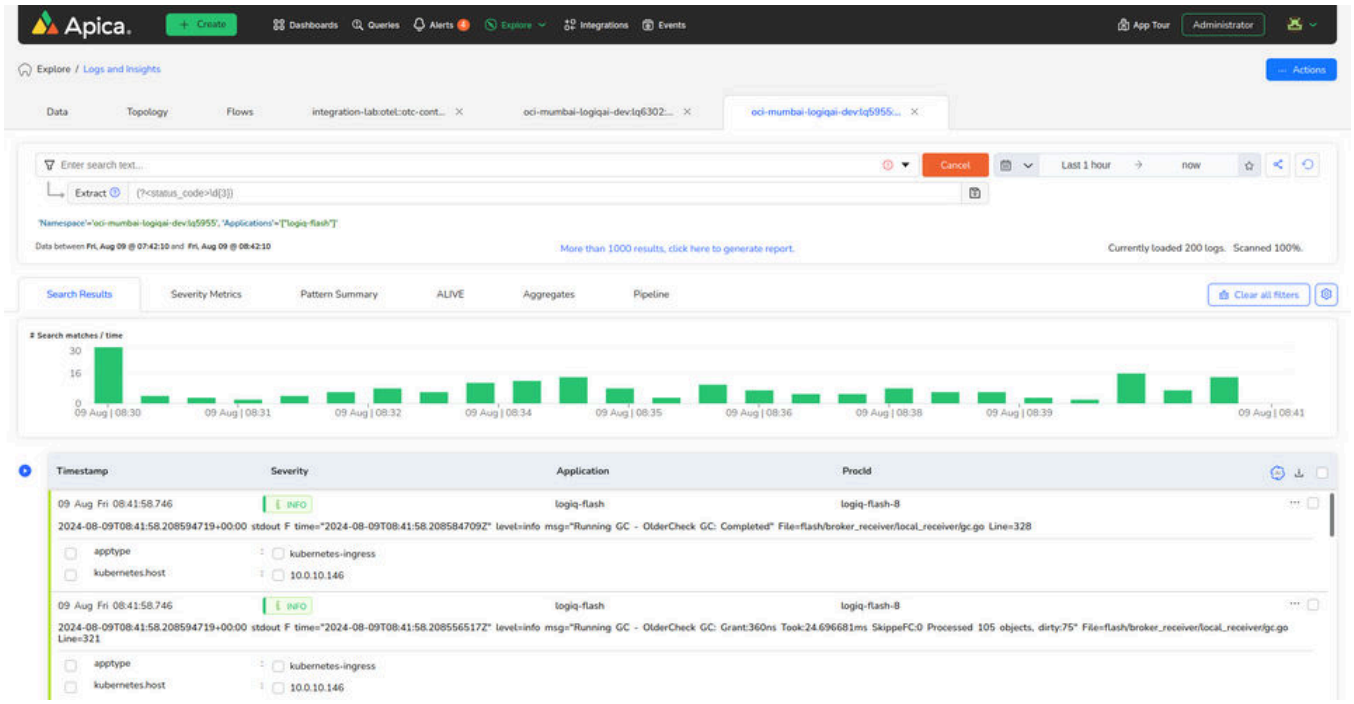
Provides full data ownership, flexible deployment (on-premises or cloud), and no vendor lock-in.

The Challenge

The exponential rise of connected devices and the shift to cloud environments have significantly increased the complexity of log management. Organizations face challenges in collecting, aggregating, and analyzing massive volumes of logs from diverse sources, each with its own format. Storing, retrieving, and making sense of this data requires robust, secure solutions that can handle the demands of modern IT infrastructures. Additionally, quick and effective troubleshooting is critical to maintaining system performance and operational efficiency.

Major Challenges

- **Centralization:** Consolidating diverse logs into a single, uniform format is crucial for effective analysis and insight.
- **Volume:** Managing and analyzing growing data volumes demands a robust system for timely insights.
- **Diversity:** Handling various log types, from event to threat logs, adds complexity to log management.
- **Resource & Time Intensive:** Manual log management is laborious; automation tools help reduce the burden.
- **Problem-Solving:** Effective troubleshooting requires well-managed, granular logs and skilled personnel.



Key Features

InstaStore

Convert raw log data into time series metrics with a single click, create custom indices, and set up alerts for key events.

Rule Packs & AI Detection

Utilize built-in Rule Packs for data optimization and AI to automatically detect patterns and reduce root cause analysis time.

Automated Topology

Quickly identify and resolve issues with real-time alerts, anomaly detection, and visualizations that map system components.

Live Log Streaming

Tail live log streams from the UI to swiftly detect production issues, supported by powerful search and filtering capabilities.

Comprehensive Storage

Store all log data in real-time, fully indexed, searchable, and replayable, ensuring no data is lost or overlooked.

MELT Data Enhancement

Integrate with OpenTelemetry for enhanced monitoring, logging, and tracing data (MELT).

Extensive Integration

Seamless integration with popular logging frameworks like Log4j and Syslog, and the ability to unify log data from any source

Architecture

- Run on any Kubernetes environment, on-premise, or on the public cloud.
- Built with a microservices architecture, and cloud-native principles.
- Scales from a laptop to 100's of nodes.
- 200+ data integrations via standardized protocols, push agents, pull integrations, and custom data collectors.
- Deployment options:
  - Available as a SaaS or self-hosted option.
  - OVA is available for virtualized infrastructure for small-scale deployments.
- Patented InstaStore technology for streaming data into any object storage for long-term retention and reverse ETL.
- Support for push data:
  - Open source agents such as OpenTelemetry, Fluentbit, Fluentd, Logstash, Filebeats, Vector
  - Syslog compatible push clients, Syslog-ng, and Rsyslog
  - Syslog RFC support for RFC3164, RFC5424, RFC5425, RFC 6587.
- Support for pulling data via built-in plugins such as Oracle Integration Pub/Sub, Kafka, and S3 compatible storage, among others.
- Ability to launch custom push/pull data integrations by launching user-created docker microservices in the telemetry pipeline.
- Live tailing of data for telemetry streams.
- Powerful rule engine for building the precise pipeline that meets your data needs.

Product Features

- Hierarchical log organization by Cluster ID, Namespaces, Applications, and Processes.
- Explore page for time machine view of application logs.
- Advanced search capabilities with complex expressions and filters.
- Log2Metrics for converting log data into real-time metrics.
- Custom indices for faster search experiences.
- Reporting functionality.
- Topology view for monitoring all incoming logs with a bird's eye view.
- Visualization tools for log data and metrics.
- Facet segregation for all the incoming logs.
- Real-time log tailing for immediate insights

Security and Compliance

- SSO via SAML and LDAP.
- Support for HTTPS and TLS connections.
- Zero-trust architecture for agent management means no host passwords are needed.
- Role-based access control for telemetry data access and management.
- SOC2 Type2 and ISO27001 compliant.

Working with Data

- Consumer-grade UI for working with streaming log data.
- Users can search data coming in the log stream, go back in time, and do advanced search expressions.
- Log2Metrics helps users convert incoming log streams into time series metrics, which can help monitor interesting events.
- Batch Report feature helps the users create reports over a long duration of time, and do aggregation on top of log data.
- Context logs help users see similar types of logs coming in that log stream.
- Rich set of rule types for data transformation, data filtering, and data management:
  - Filter: Filter noisy observability data.
  - Extract: Structure unstructured data.
  - Tag: Tag data for any interesting events.
  - Forward: Forward only what you want.
  - Stream: Send data into different flows and destinations.
  - Rewrite: Mask PII data coming in the data stream
  - Code (V8 Javascript): User can write complex JS functions to manipulate and manage their data.
- GenAI integration helps users to directly jump from the logline to the root cause.
- The severity metrics section lets users visualize the severity distribution across a time range.
- After enabling Pattern Signature in a log stream users can see the summary of the Patterns coming in the log stream.
- The pattern summary section helps users visualize and see a brief about all the patterns that have been recognized in the log stream.
- The ALIVE section can help users do complex data analysis on top of the data coming from the log streams.
- ALIVE has a sub-section for comparing patterns and the logs in that time duration or comparing patterns and logs from some other time duration.

Data Types

- Support for logs, metrics, and traces.
- Support for multiple log formats:
  - Syslog (RFC3164, RFC5424, RFC5425, RFC 6587), Syslog-NG, RELP or Rsyslog.
  - JSON-structured logs.
  - Plain text logs.
  - Logstash.
  - Lumberjack.
  - Logs embedded in open telemetry traces.
- Metrics data.
- Trace data.

- The aggregate section helps the user to visualize the data that is coming in the log stream. The UI is pretty straightforward with no code, drag and drop functionality.
- The pipeline section helps users visualize the pipeline of the log stream. Users can see how data is getting transformed by the rules. Also, users can see how much data savings or data replication has happened because of the applied rules.
- If the number of logs in the time frame is high, then the user can directly generate a report out of that search.

Open-Source Support

- Built-in support for OpenTelemetry collector, Fluent-bit, Telegraf, and other open-source agents.
- Extensible and compatible with a wide range of observability platforms, due to support for open-source protocols and technologies.

OpenTelemetry Support

- Ingest data from OpenTelemetry collector, compatible with OpenTracing for legacy compatibility.
- Both core and contrib OpenTelemetry collector distributions are supported.
- Support for custom collector builds.
- Open Agent Management Protocol (OpAMP) is a core technology for fleet management capabilities.

CLOUD NATIVE COMPUTING FOUNDATION

*__Contact us__ today to schedule a demo. Or reach out to **sales@apica.io***