Oracle Management Cloud: Log Analytics

Oracle Log Analytics Cloud Service is a software-as-a-service solution that monitors, aggregates, indexes, and analyzes all log data from your all your applications and infrastructure (running on-premises or in the cloud). It enables users to search, explore, and use machine learning to correlate log data to troubleshoot problems faster and derive operational insights to make better decisions.

Log Analytics relies on key capabilities to help users accelerate troubleshooting. It enriches logs with application topology and error categorization. Powerful machine learning capabilities help users rapidly analyze large volumes of log data to identify patterns and anomalies. Finally, built on a uniform platform, it integrates with Monitoring services (application and infrastructure) to provide a comprehensive operational view in a single Dashboard.
LIGHT TOUCH LOG AGGREGATION

Oracle Log Analytics can monitor, aggregate, index, and analyze log data from a wide variety of Oracle and non-Oracle log sources. Simple configuration of data collectors can rapidly enable log data monitoring from ANY log file (including Syslog sources) and securely transport this data to the Oracle Log Analytics service. The data collectors can significantly compress the log data (10:1) and transport the compressed data over a secure communication protocol (HTTPS).

TOPLOGY AWARE LOG EXPLORATION

Troubleshooting problems in today’s distributed applications (that now span enterprise data centers, private clouds, and public clouds) has become increasingly complex. While developers, IT Ops, and DevOps teams rely heavily on application and infrastructure logs for troubleshooting, modern applications are elastic and have a dynamic topology. Oracle Log Analytics understands and uses the current application topology to provide an accurate picture of which platform and infrastructure components make up your application and then it enables you to explore logs relevant to the application at the time the problem occurred. Exploring logs relevant to the application makes the troubleshooting process more accurate as it enables users to focus on the right log data in the context of the problem.

Figure 1. Topology-Aware Log Exploration

MACHINE LEARNING BASED PATTERN AND ANOMALY DETECTION

IT Operations and DevOps organizations are inundated with the volume of log data that needs to be analyzed to troubleshoot problems. This is exacerbated by the fact that modern applications are developed and deployed in an agile manner making it difficult to troubleshoot problems by relying purely on domain knowledge and rules. Oracle Log Analytics relies on machine learning to rapidly identify “Interesting” log entries in your log data. These could include patterns or anomalies that exist in your log data. Working with patterns and anomalies makes log exploration more efficient and can help get to the root cause of the problem faster.
Dashboards provide operational insight for IT and Business. Stakeholders can get visibility into the health and availability of applications and monitor critical events from one central place using out-of-box and custom dashboards. The rich set of predefined widgets, charts and controls enable extraction of critical operational information from logs and are used to build dashboards that expose critical business metrics. When problems occur, users can drill into the Log Visual Analyzer for troubleshooting. The big-data platform common to all Oracle Management Cloud services enables aggregation of widgets from across the services to get a 360-degree view of end-user experience (from APM), events, critical errors, business metrics (from Logs), and resource/capacity availability (from IT Analytics) across all your applications and services.

APM INTEGRATION

Troubleshooting modern web applications requires looking at a variety of data including end-user experience, transaction performance, workload and resource performance metrics and logs from across all software and hardware components. Users can analyze and correlate this wide variety of data by seamlessly navigating from the APM service and the application issue they are working on into Oracle Log Analytics and explore the logs related to the application server, database, and hosts in the context of the workload. Expanding troubleshooting efforts from the APM view into the application and infrastructure logs in the application context and request flows helps accelerate the problem troubleshooting process.