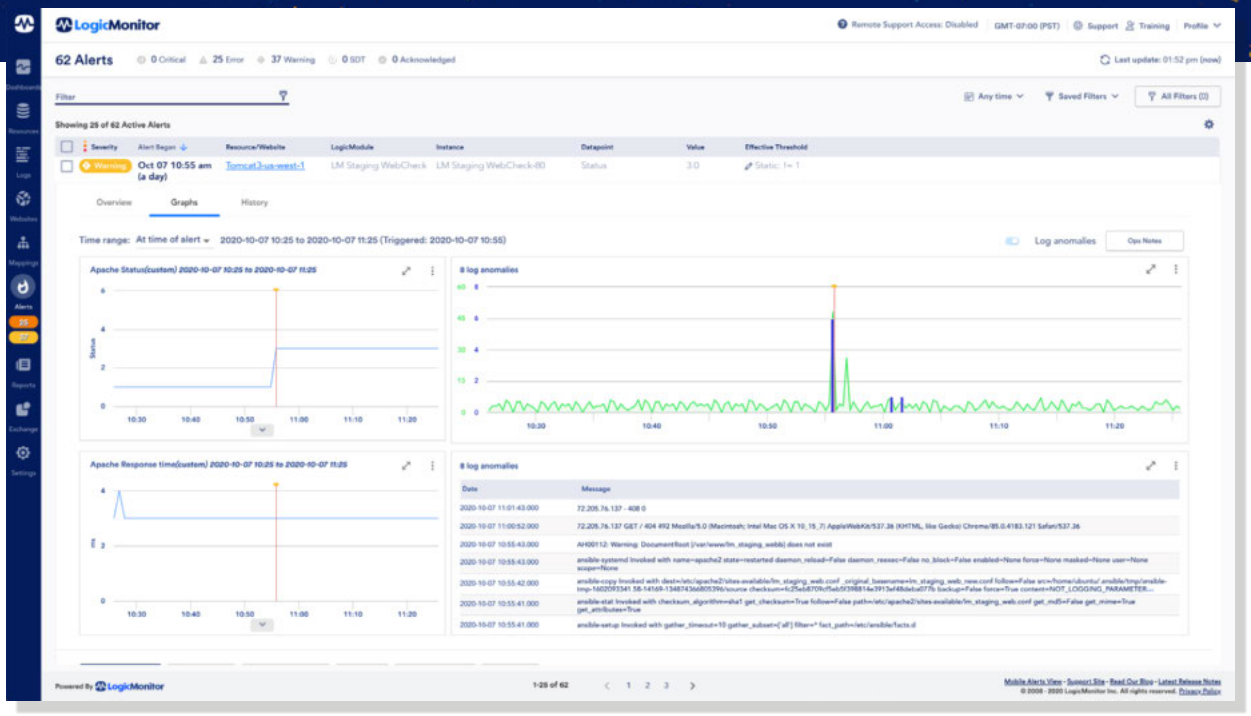
DATASHEET

LogicMonitor

LM Logs

Automatically analyzes 100% of your log data, to uncover root-causes of raised performance monitoring alerts and exposes unknown issues proactively.



Logs now are embedded in alerts to enrich the context.

LogicMonitor

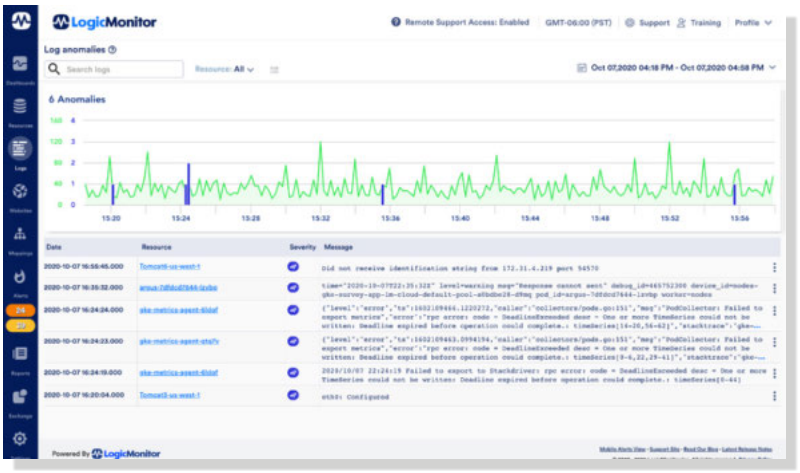
LM Logs is the only solution for IT Operations, DevOps, and SRE teams that automatically analyzes 100% of your log data, to uncover root causes of raised performance monitoring alerts and exposes unknown issues proactively. All of this rich data, combined with infrastructure performance metrics, improve operational efficiency and service delivery in a single pane of glass.

LM Logs intelligently analyzes millions of log lines to highlight events that signify anomalous changes within infrastructure. By narrowing the focus from millions of logs to the key events representing new behavior or activity, IT teams can reduce time spent troubleshooting and hunting for the root causes of incidents and alerts.

Anomalous log events are automatically correlated with metric-based alerts in LogicMonitor's existing intelligent IT infrastructure monitoring platform. This provides more in-depth insight beyond simple notification and helps customers quickly understand why alerts have triggered. LM Logs also enhances LogicMonitor's existing AIOps Early Warning System capabilities to help IT teams reduce mean-time-to-repair (MTTR) and proactively prevent widespread business impact.

High Context Alerting.

LogicMonitor automatically correlates relevant log anomalies with alerts that have been triggered by LogicMonitor's performance-metric based alerts. This provides IT teams with immediate answers as to why incidents have occurred, thereby providing them with the necessary information to quickly restore intended performance.



View all log anomalies under the new Logs tab.

Anomaly Detection.

With these new in-system algorithms, LogicMonitor will immediately detect log events representing change and anomalies across entire environments. Never miss a new NullPointerException that is introduced into an application. Bubble up those rare service restarts that could lead to bigger problems down the road. Capture the failed connections to your sensitive devices. This allows IT teams to focus on the right information at the right time without spending valuable time searching through massive volumes of logs..

Log and Metric Data in One, Unified Platform.

LM Logs provides out-of-the-box coverage for Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), Syslog, Fluentd, and an API that can accept logs from any system. This means that IT teams can achieve full visibility into their infrastructure and application logs in a single platform. Presenting logs together with metrics on the same platform improves operational efficiency.

Benefits

- Reduce MTTR by surfacing key log information at the time of critical alerts.
- Correlate metrics, configuration changes, and logs in one platform and avoid context switching among various tools.
- Proactively identify and fix problems before they cause disruption.

Features

Seamless On-boarding

- New logs page available with simple instructions for getting started
- Utilize existing collectors

Unified Observability Experience

- Logs are correlated automatically with monitored resources, configuration sources, and metrics
- Users can seamlessly navigate from any performance-metric graph to relevant logs for more intelligent and relevant context
- Users can drill down into the resource from a log found in the new Logs tab for faster triaging of issues
- LogicMonitor displays log anomalies in the context of alerts -- Allowing customers to quickly go from “what” is wrong, as indicated by the metric, to “where” the issue is occurring, as characterized by topology, to “why” it has happened, as noted in the logs

Comprehensive and Extensible Log Collection

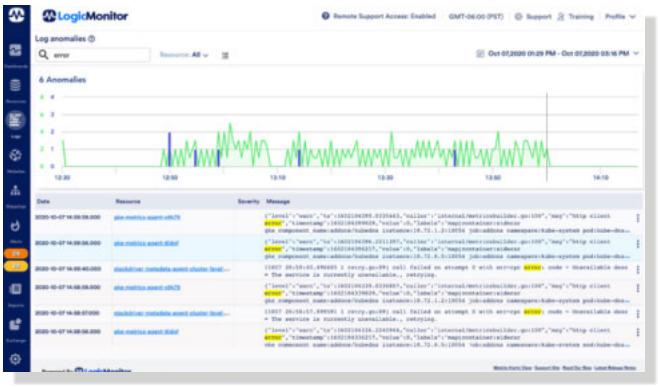
- LM Logs out-of-the-box integrations with AWS, Azure, GCP, Syslog, and Fluentd make it easy to send logs to LogicMonitor
- Send it and forget it: logs are matched automatically to monitored resources, and anomalies are automatically detected and contextually displayed
- A robust API enables users to customize log collection and send any logs to LogicMonitor

AIOps-based Log Anomaly Detection

- LM Logs learns the normal log patterns for monitored resources and identifies deviations from these normal patterns
- Anomaly detection surfaces log events that haven’t occurred before and represent change -- these events often explain “why” issues are occurring
- Additional algorithms will come in 2021 to identify more types of anomalies

Logs Alerting (coming soon)

- Users can define alert conditions as a part of Log Pipelines to ensure alerts are triggered and send out notifications when known issues arise
- Users can easily create alert conditions from existing anomalies or log events and test to see how many events the conditions would match
- Users can see log alerts alongside metric alerts within their existing workflows on LogicMonitor's alerts page



Use the search bar for faster and easier filtering of logs.

Highlight and zoom in on a specific time range to filter the view.

Keyword Search and Filtering

- LM Logs supports keyword search, so users can quickly search for log events containing specific keywords
- Users can easily filter logs (raw logs and anomalies) based on the resource or resource group they relate to
- Users can toggle between all raw logs and anomalies logs view by clicking the Raw Logs button
- Users can quickly filter displayed logs based on time range, either by configuring a specific time range or zooming in on specific ranges within the overview graph