



# The Sumo Logic Solution: Application Management

## Introduction

The most critical and demanding responsibility facing CIOs, IT operations managers and system administrators on a daily basis is to keep their customer-facing production applications up and running. Today's business critical applications are distributed, large-scale, and rely on in-house developed software, open-source and 3rd-party components, making them difficult to manage, monitor and troubleshoot. This degree of difficulty is further compounded by a combination of physical, virtual and cloud (PVC) computing infrastructures where these applications are being deployed by modern enterprises.

---

“Agility and speed really matter when you’re running production systems. With Sumo Logic, the most recent log data is available instantly so that you can investigate and analyze network, system and user behavior immediately.”

As the volume and complexity of unstructured application log data generated by applications has increased dramatically, troubleshooting and root cause analysis have become orders of magnitude more difficult. Home-grown tools or aging on-premise log management systems, which were never architected to address complexities and scale of today’s distributed applications, simply can’t keep pace. Unable to manage and analyze the extraordinary volume of unstructured log data being generated by production applications and supporting infrastructure, these systems have become business liabilities.

### **Sumo Logic’s Log Management and Analytics Service**

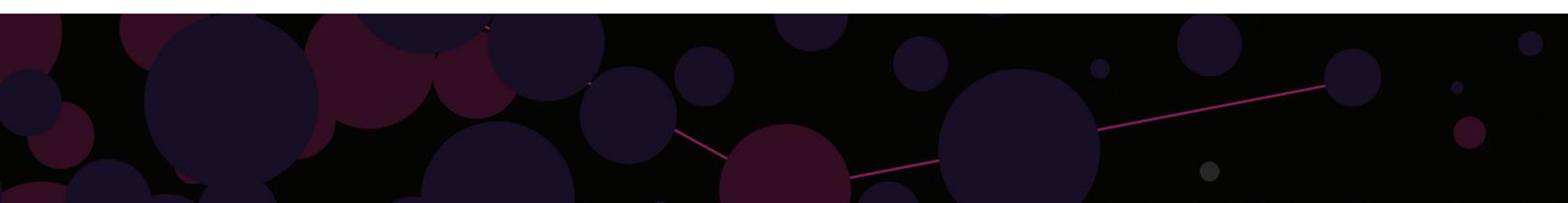
Sumo Logic’s next-generation log management and analytics service changes this equation, delivering actionable insights into application and infrastructure operations while dramatically reducing complexity and cost.

As a massively scalable, multi-tenant service, Sumo Logic performs log data collection, processing, storage and analysis within a centralized and highly secure cloud-based platform. It effortlessly handles all of your log data, regardless of volume, type or location, enabling IT teams to uncover operational insights buried under terabytes of logs in seconds. As a result, log data is emerging as one of the most strategic business assets within the enterprise.

Sumo Logic is designed from the ground up to handle Big Data-scale environments. Among Sumo Logic’s breakthroughs is its near-zero latency Real-Time Forensics engine that delivers real-time search results from petabytes of log data. Real-Time Forensics makes critical new events occurring within IT infrastructure instantly available for analysis. Anomalous conditions can be spotted as they occur, enabling operations teams to respond immediately to prevent network outages, eliminate system downtime, resolve application issues and improve SLAs. In short, Sumo Logic reduces mean-time-to-investigation and mean-time-to-resolution dramatically.

Sumo Logic also scales to support orders of magnitude more data than legacy premise-based log management systems. Its patented Elastic Log Processing engine scales each component of the service independently to meet every customer’s compute, storage and data processing requirements on demand.

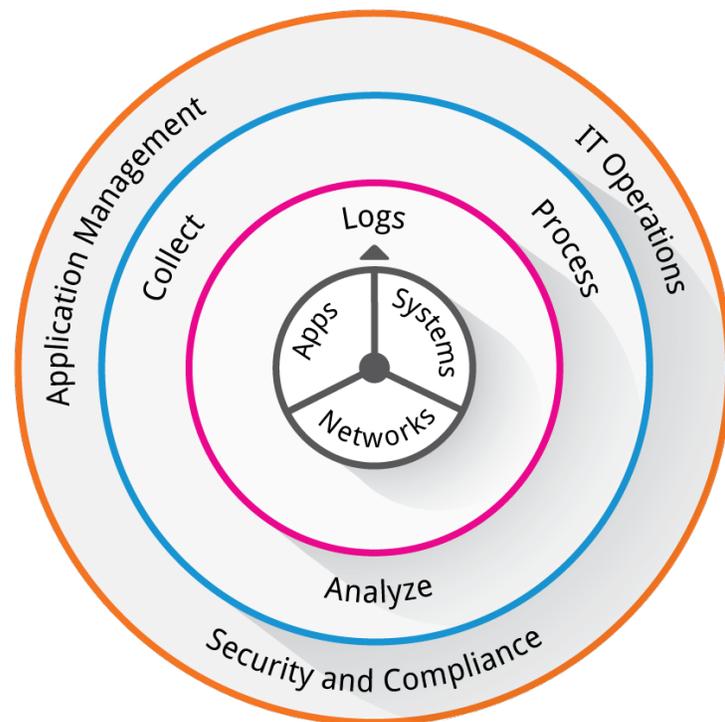
Sumo Logic also takes a unique approach to log data collection. Data is securely and reliably collected through either local collection (via Sumo Logic Collectors) or through hosted collection (via https or directly from Amazon S3). All data is collected in raw, or unstructured format with no need to parse or understand



the data upfront; all data processing and parsing is handled in the cloud. By separating collection from processing and parsing, which occur entirely in the Sumo Logic service, there is no need to update complex parsing logic. Consequently performance is significantly improved and management overhead significantly reduced.

To help enterprises manage exploding volumes of log data, Sumo Logic is built around a globally distributed data retention architecture featuring built-in data redundancy. Sumo Logic eliminates the need for costly SAN and NAS infrastructures and removes the complexity of data archiving, backups and restores.

Another major breakthrough is Sumo Logic's patent-pending LogReduce technology that eliminates the time-consuming and tedious tasks of manually reading log records, writing scripts and handcrafting queries. LogReduce reduces millions of log lines into a handful of human digestible patterns that enable IT teams to get to insights without having to manually writing queries to slice and dice the data. This enables our customers to quickly find important and emerging system and application behavior patterns that would otherwise require days of analysis. Sumo Logic's patent-pending Push Analytics leverages LogReduce technology to automatically uncover insights; it then pushes those insights proactively to IT teams in order to facilitate immediate investigations.



Sumo Logic's next-generation log management and analytics service delivers actionable insights into application and infrastructure operations while dramatically reducing complexity and cost.

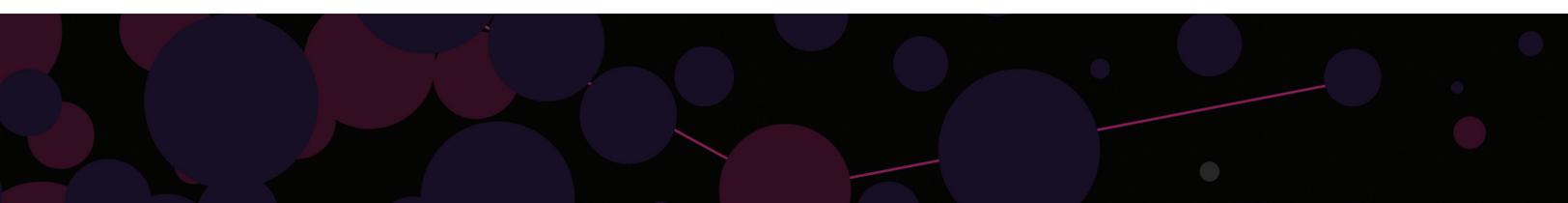
### Sumo Logic At Work

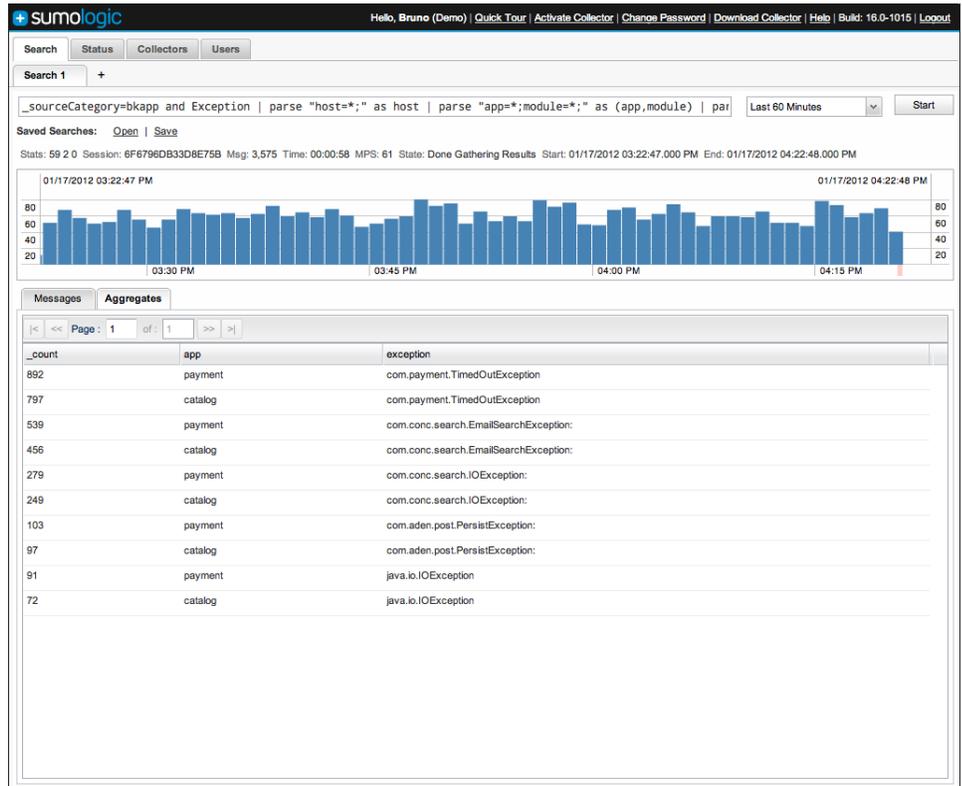
In the context of application management, Sumo Logic plays a key role in ensuring customer-facing production applications achieve optimal uptime, performance, and SLAs. In addition, the service delivers application analytics that help enterprises better understand how their distributed applications behave, how users interact with those applications, providing immediate invaluable insights to operations, development, and other business functions.

**Application Troubleshooting and Root Cause Analysis:** When something goes wrong in a distributed production application running across multiple data centers or in the cloud, conducting root cause analysis and troubleshooting in seconds is critical. The ability to quickly isolate the application node, module, or even line of code where the root cause of the problem hides dramatically reduces mean-time to investigation and mean-time to resolution.

Take the case of an online retail site timing out connections when it tries to reach its payment system and generating "failure, please try again later" messages. Every second this condition persists is causes not only lost revenue but also a decrease in customer satisfaction and loyalty.

Determining the root cause of application failure requires the ability to collect, index and analyze the most up-to-date log data from application nodes, underlying infrastructure and networks. By quickly identifying new patterns that are causing application failures and bringing them to the surface in real-time, Sumo Logic expedites the problem resolution process. Equally importantly, Sumo Logic can apply its advanced data collection, indexing, real time forensics and push analytics to monitor how the application behaves after modifications are made or new versions are released to production. By operating in real-time, the impact of application changes can be observed instantly.





Sumo Logic's LogReduce™ delivers real-time results and uncovers new behavior patterns that cause failures within critical applications.

**Application Analytics:** Above and beyond troubleshooting and root cause analysis, Sumo Logic enables organizations to analyze their application behavior.

Especially valuable for customer facing and revenue generating applications is the ability of teams developing, operating, marketing, and selling them to glean insights into what new features are driving customer engagement, where the usage dropoffs are, how the applications performs for end users, and what the overall user experience is. Similar is true for internal mission-critical applications used by employees in important job functions such as sales, customer support, supply chain, etc.

Sumo Logic's real-time data collection, forensics and analysis capabilities reveal new application and user behaviors immediately so developers and operators can tune applications in order to achieve optimal impact, productivity and user experience.

---

“One of the key benefits of Sumo Logic is that their scaling model can easily accommodate our growing volume of log data.”

“We’re using Sumo Logic for more than just shaving a few dollars here and there; they’re actually improving our ability to innovate.”

The Roblox logo is written in a stylized, red, blocky font with a white outline and a slight shadow effect.

In the case of organizations operating online social networking and gaming sites, there is a growing need to continuously measure interactions with site visitors. Not only do these organizations want to track what features and capabilities site visitors are using, but also how effective those features are, how well they perform, and what the ultimate impact of those new features are on site and gaming traffic. For example, if log data shows that connection time between users is trending up, operations managers may need to deploy additional servers or faster network gear in order to facilitate higher performance to positively impact the user experience. Failure to quickly gather and recognize key trending patterns could result in customer attrition. With Sumo Logic, application analytics are delivered with near-zero latency resulting in real impact to the bottom line.

**Performance Monitoring:** Sumo Logic enables operations management to continuously monitor application performance to ensure SLAs are meeting commitment levels. Because Sumo Logic performs real-time log data collection, forensics and analysis, changes in performance characteristics that could impact SLAs can be spotted and corrected well before they become a problem. This is imperative for modern enterprises, SaaS, managed service providers, and cloud-computing providers alike whose customers rely on them to deliver business critical services and applications.

### Summary

Sumo Logic’s next generation log management and analytics enables IT and DevOps teams to develop, manage, and operate their applications and underlying infrastructure by accelerating troubleshooting and root cause analysis, improving application performance monitoring, and dramatically improving visibility into application and user behavior. This helps modern enterprises get more value out of their critical business applications while at the same time minimizing the cost of dealing with massive volumes of log data those applications generate.