*LOGENTRIES INSIGHTS:*

# 10 Best Practices for Log Management & Analytics


***Trevor Parsons Ph.D***
*Co-founder & Chief Scientist*

logentries™

# Introduction

## Today's Log Management and Analytics Challenges

Within the last decade, the advancement of distributed systems has introduced new complexities in managing log data. Today's systems can include thousands of server instances or micro-service containers, each generating its own log data. With the rapid emergence and dominance of cloud-based systems, we have witnessed explosive growth in machine-generated log data. As a result, log management has become a staple in modern IT operations, supporting a number of use cases including debugging, production monitoring, performance monitoring, support and troubleshooting.

While distributed systems offer efficiency in terms of scalability, teams referring to log data can find themselves unsure of where to start or what level of effort would be required to even locate the needed log files. IT Administrators, devOps professionals and those closest to the systems producing logs are faced with the challenge of managing decentralized log files while adhering to security and compliance protocols. Developers and engineers who need to debug application-level issues can find themselves limited by their access to production-level log files. Operation, Devs, Data Scientists and Support teams who need insight into user-behavior for trend analysis and troubleshooting often lack the technical expertise sometimes required to leverage log data. Given these challenges, it's crucial to consider best practices when implementing a logging solution for your organization.

# 10 Best Practices for Log Management and Analytics

## 1. Set a Strategy

Don't log blindly. Instead, carefully consider what you are logging and why. Logging, like any significant IT component, needs to have a strategy. When structuring your DevOps setup or even when releasing a single new feature, be sure to include an organized logging plan. Without a well defined strategy, you could eventually find yourself manually managing an ever-growing set of log data, ultimately complicating the process of identifying important information.

When developing your logging strategy, consider what is most important from your perspective and what value you want from your logs. Your plan should include logging methods and tools, data hosting locations, and most importantly, an idea of the specific information you're looking for.

## 2. Structure Your Log Data

In addition developing a logging strategy, it's important to consider the format of your logs. Failing to understand effective logging formats makes it very difficult to identify and extract insights from your logs.

Log structures should be clear and understood from both a human and machine-readable perspective. Readable logs make troubleshooting easier and can sometimes enable log management services to further process log data, resulting in deeper insights and data visualizations. Two common log structuring formats are JSON and KVP (Key Value Pair). Both provide coherent log data for human understanding and allow logging software solutions to extract information from a semi-structured format.

> Failing to understand effective logging formats makes it difficult to identify and extract specific information.

## 3. Separate and Centralize your Log Data

Logs should always be automatically collected and shipped to a centralized location, separate from your production environment. Consolidating log data facilitates organized management and enriches analysis capabilities, enabling you to efficiently run cross analyses and identify correlations between different data sources. Centralizing log data also mitigates the risk of losing log data in an auto-scaling environment.

Forwarding log data to a centralized location enables system administrators to grant developer, QA and support teams access to log

data without giving them access to production environments. As a result, these teams can use log data to debug issues without risk of impacting the environment. Replicating and isolating log data also eliminates the risk of attackers deleting log data in an effort to hide security breaches. Even if your system is compromised, your logs remain intact.

> Forwarding log data to a centralized location enables system administrators to grant developer, QA and support teams access to log data without giving them access to production environments.

## 4. Practice End-to-End Logging

In order to overcome common troubleshooting complexities and achieve a more holistic view of your application and systems, you should monitor and log across all system components. Most people think about logging from server logs, such as Windows security logs. However, logging all relevant metrics and events from the underlying infrastructure, application layers and end user clients are equally as important.

End-to-end logging allows you to understand your systems' performance from an end user's point of view, taking things like network latency, database transaction delays and page loading times into account. This kind of visibility helps you to better deliver a seamless user experience.

## 5. Correlate Data Sources

End-to-end logging into a centralized location allows you to dynamically aggregate various streams of data from different sources - such as applications, servers, users and CDNs for correlation of key trends and metrics accordingly. Correlating data enables you to quickly and confidently identify and understand events that are causing system malfunctions. For example, discovering real-time correlations between infrastructure resource usage with application error rates can help you identify anomalies and react before end users are affected.

## 6. Use Unique Identifiers

Unique identifiers can be useful for debugging, support and analytics. Identifiers allow you to track particular user sessions and pinpoint actions taken by individual users. If you know a user's unique ID, you can you filter your search for all actions that user took over a specified period of time. With a breakdown of the user's activity, you can trace an entire transaction from first click to the database query that was executed.

## 7. Add Context

When using logs as data, it's important to consider the context of each data point. Knowing a user clicked a button may not be as useful as knowing a user specifically clicked the "purchase" button. Adding further context can reveal the type of purchase made. If the user's purchase resulted in an error, the available context will facilitate swifter resolution.

## 8. Perform Real-Time Monitoring

Service disruptions can lead to a host of unfortunate outcomes, including unhappy customers, lost purchases and missing data. When production-level issues arise, a real-time monitoring solution can be crucial when every second counts.

Beyond simple notifications, the ability to investigate issues and identify important information in real-time is just as important. Having "live tail" visibility into your log data can empower developers and administrators to analyze log events as users interact with their applications or systems. Live tail search and reporting can also enable support teams to investigate and solve customer issues as they come in.

## 9. Use Logs to Identify Key Trends

Troubleshooting and debugging only scratches the surface of what log data has to offer. Whereas logs were once considered a painful last resort for finding information, today's logging services can empower everyone from developers to data scientists to identify useful trends and key insights from their applications and systems.

Treating log events as data creates opportunities to apply statistical analysis to user events and system activities. Calculating average values helps you better identify anomalous values. Grouping event types and summing values enables you to compare events over time. This level of insight opens the door to make better informed business decisions based on data often unavailable outside of logs.

> "A log management & analytics service only accessible to highly technical teams severely limits your organization's opportunity to benefit from log data.

## 10. Empower the entire team

A log management & analytics service that is only accessible to a highly technical team severely limits your organization's opportunity to benefit from log data. A log management and analytics tool should give developers live-tail debugging, administrators real-time alerting, data-scientists aggregated data visualizations and support teams live search and filtering capabilities without requiring anyone to ever access the production environment.

# Now What? The Future of Log Management & Analytics

As applications and systems continue to grow in size and complexity, logging solutions are becoming a necessity across organizations of all sizes. As the practice of log management matures, logging tool features such as centralized logging, search, filters and real-time alerting are becoming requirements for modern-day Ops and Dev teams. As more organizations implement these solutions, the real business value will be realized by the insights that aggregated, real-time log data provides. Beyond traditional debugging and troubleshooting, the analysis of key trends across systems, applications and users will create opportunities for improved operations, decreased costs and new revenue opportunities. The data is all there - it's how organizations choose to leverage their data that will make the biggest impact to their business.

# About Logentries

Logentries is the leading real-time log management and analytics service built for the cloud, making business insights from machine-generated log data easily accessible to development, IT and business operations teams of all sizes. With the broadest platform support and an open API, Logentries brings the value of log-level data to any system, to any team member, and to a community of more than 35,000 worldwide users. While traditional log management and analytics solutions require advanced technical skills to use and are costly to set-up, Logentries provides an alternative designed for managing huge amounts of data, visualizing insights that matter, and automating in-depth analytics and reporting across its global user community. To sign up for the free Logentries service, visit logentries.com