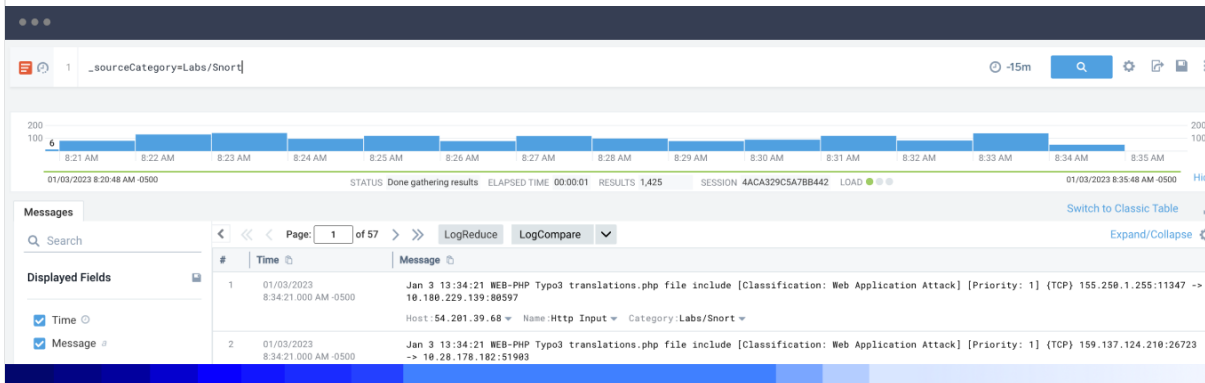


Why log management is essential to the success of cloud-first companies

sumo logic



The ultimate guide



Cloud powers business

03

Log management

05

Log management process

09

Log analytics

11

Best practices

13

Tool features

15

Conclusion

16

CLOUD POWERS BUSINESS:

Organizations increasingly rely on cloud solutions to power their business.

[Gartner](#) estimates that by 2025, over half of IT spending in the application software, business process services, infrastructure software and system infrastructure markets will shift to public cloud solutions.

This change offers cloud-native SaaS organizations — and those undergoing digital transformation — an exciting opportunity to drive conversions and growth. Competition will be stiff, with the SaaS industry expected to grow at a compound annual growth rate (CAGR) of 11.7% between 2020 and 2026. For cloud-based SaaS organizations, these numbers present a few challenges:

Reliability

How to ensure a highly reliable and secure digital experience?

Security

How to prevent attacks and respond quickly when they inevitably happen?

Optimization

How to reduce the effort to monitor, secure and optimize your applications in real-time?

Troubleshooting

How to troubleshoot errors and reduce mean time to repair (MTTR) to maximize customer satisfaction and minimize potential churn?

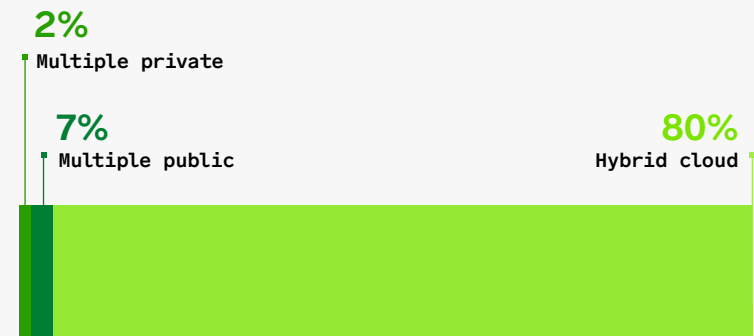
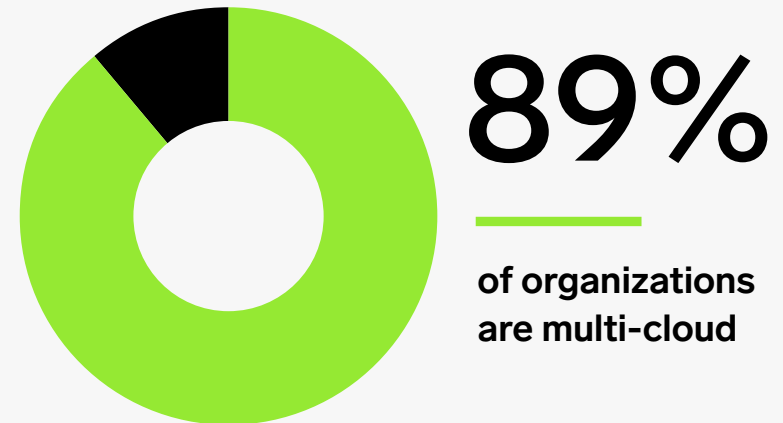
Data insights

How to leverage data to strengthen performance and improve your security posture?

Log management is a critical piece of the solution.

In this ultimate guide to log management, we explore:

- What is meant by terms like log management and centralized logging?
- How can log management improve reliability and security?
- What is log analytics, and how can it superpower your operations?
- What are logging and monitoring best practices?
- What capabilities do the best log management and analytics tools have?



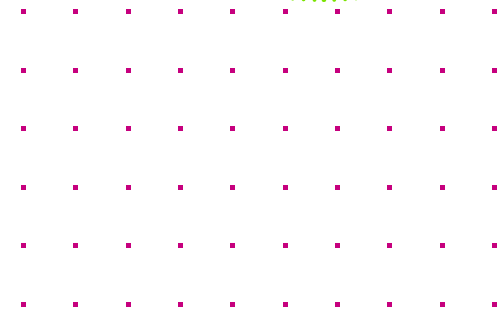
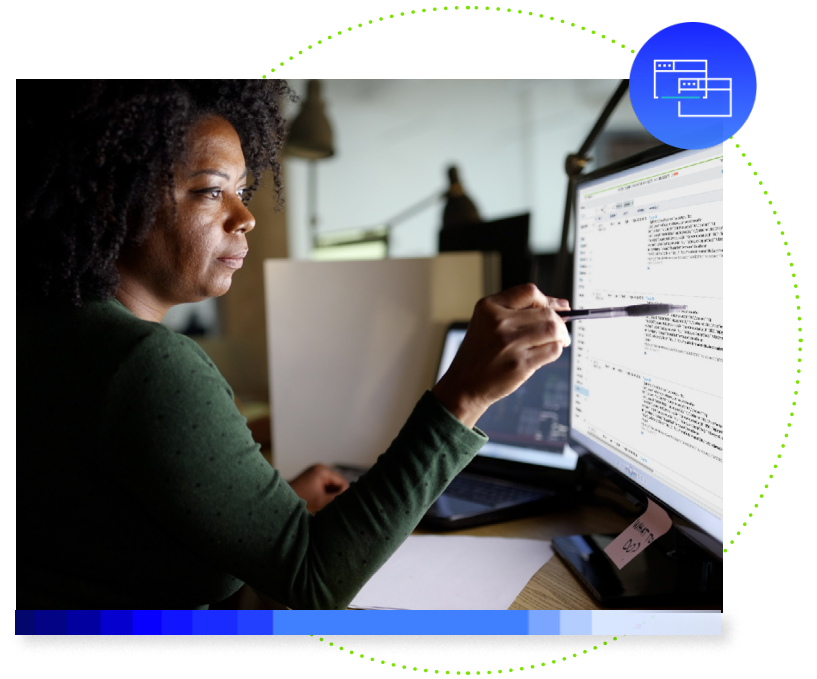
■ Multi-cloud environments create challenges in visibility, making it difficult to spot or address issues fast if data stays in silos.

N=753

Source: Flexera 2022 State of the Cloud Report

What exactly does it mean in today's digital world?

[Log management](#) refers to a system or practice that allows organizations to process the massive amounts of computer-generated log events (or logs) created daily. These log files play a critical role in telling DevOps and security teams whether systems are performing as expected or were compromised and what might be causing the issues that occurred.



Let's start with the very basics: What are logs?

Logs are time-stamped digital records of actions and events that occur within a technology stack or IT infrastructure. They are generated from:

- Applications
- Application infrastructure
- Cloud infrastructure
- Containers
- Load balancers
- Message bus (Kafka)
- Networks
- Servers

The data logs hold provide visibility into how an application behaves at any moment. They include data points like:

- Timestamp
- Host name
- Process type
- Application
- Action
- TCP (Transmission Control Protocol) socket status

Imagine receiving a security or outage alert without any additional context.

Without logs, organizations don't have the information they need to understand the chain of events that transpired, which could spell disaster.

```
metadata                                     keywords
├── _sourceCategory=Labs/Apache/Access and "Mozilla"
└──
parse  ── [ parse "GET * HTTP/1.1\" * " as url,status_code
filter  ── [ where status_code matches "5*"
aggregate ── [ count by status_code
format  ── [ sort by _count
         ── [ limit 3
```

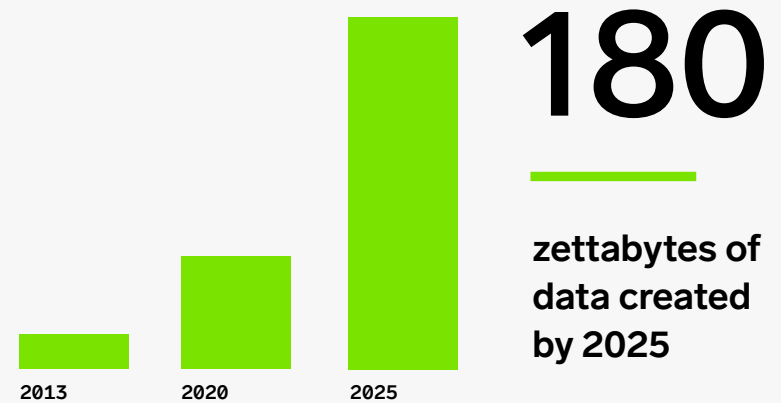
■ The query syntax of data analytics consists of keywords and operators, separated by pipes, that build on top of each other.

Next up: Why does **log management matter?**

Log management allows teams to monitor and improve system performance, quickly identify issues and bugs and bolster security across an enterprise's entire system. Logs and log data are the foundation of effective troubleshooting for service reliability and security.

Some corporations are now dealing with petabytes of log files, not to mention all of their other data. Some estimates indicate that globally, data is expected to [more than double](#) between 2022 and 2026. A robust log management practice is the best way to store and analyze logs, ensuring optimal network and application observability and security.

A log management tool is the software or platform that assists teams in doing some or all of their log management processes and procedures. Log management tools are increasingly important — especially for businesses building and/or running modern applications in the cloud — due to the huge increase in log data volume and the sheer number of applications and tools in an organization's tech stack.



Data continues to explode. A robust log management and analytics platform helps organizations draw insights from their machine data.

Source:

Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth

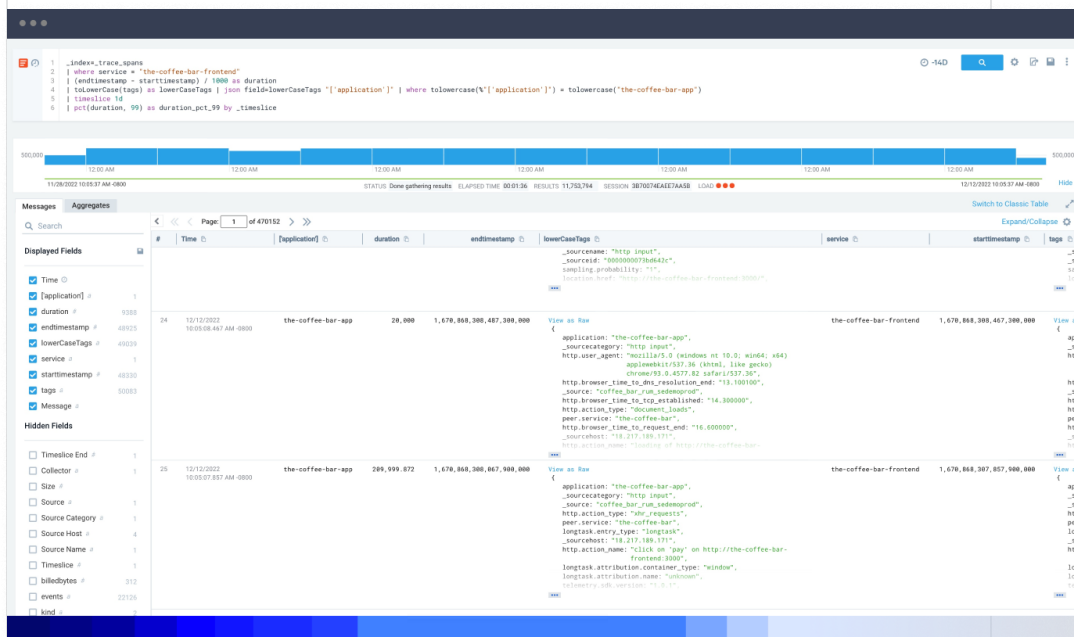
All your data in one place.

The advantages of centralized logging.

Centralized logging is a process that organizations use to collect and aggregate all of their logs from disparate systems and tools into a single location. Before the cloud, organizations typically stored and managed their data in data centers or on-premises servers.

With centralized logging tools, organizations can improve operational efficiency by eliminating potential data silos and relying on cloud principles to offer increased scalability and accessibility.

The best log management tools cover the entire log management process from start to finish, eliminating data silos and the need for duplicative monitoring tools. What's more, with a solution like [Sumo Logic](#), which provides log management and analytics for both reliability and security use cases, organizations can operate from a single source of truth on one platform.



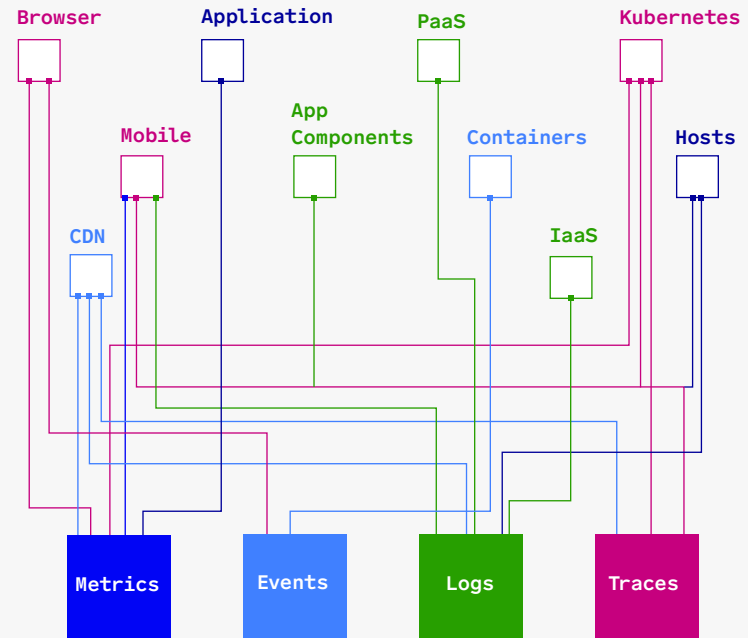
LOG MANAGEMENT PROCESS:

The five essential steps

1. Instrument and collect

A log collector allows you to ingest data from disparate locations throughout your tech stack. This process can be performed by a Syslog or applications writing the logs into the log management system via hypertext transfer protocol (HTTP).

Once the data is collected, it may require parsing. Log parsing means extracting templates and parameters to interpret the logs. Log management and analytics solutions like Sumo Logic allow you to extract fields from log messages, regardless of their format.



OpenTelemetry is a collection of tools, APIs, and SDKs that you can use to instrument, generate, collect, and export all machine data. It is becoming the gold standard to collect machine data. [Learn more.](#)

FIVE ESSENTIAL STEPS CONTINUED...

2. Centralize and index

In the second step, you will aggregate, normalize and index your logs into a single location to increase access and visibility across the entire application environment and IT infrastructure. Because organizations — especially those that operate in cloud environments — deploy a large number of applications and other infrastructure, having logs centralized in a single location is critical to security, operations and reliability.

At Sumo Logic, our cloud-native SaaS analytics platform provides top-tier [log aggregation](#) and log parsing capabilities, with the ability to collect logs from almost any source, offering end-to-end log management and analytics functionality.

3. Search/query and analyze

Once aggregation is complete, DevOps teams, developers and security analysts can access, search and analyze the log data. This is where the magic happens. With cloud-native log management and analytics solutions like Sumo Logic, you can integrate with several environments using IIS web servers, NGINX and others to improve the log analysis process.

4. Monitor and alert

Along with analytics, monitoring is another vital component that benefits from a proper log management process. As we touched on previously, information from log files is used in a variety of ways. One such way is to monitor system performance for errors, anomalies or security breaches, which helps ensure greater reliability and security for your users.

Using the data collected and analyzed, IT teams can develop rules and alerts for various occurrences to notify the right people immediately if an issue arises, significantly increasing operational efficiency.

5. Report and dashboard

Finally, any organization knows that the ability to visualize and report data points and metrics for operational needs to business stakeholders and key decision-makers is critical. Not only does this ensure that everyone—including individuals inside and outside the IT team—is on the same page regarding data and performance, it also empowers better business decisions at every stage.

Making sense of the data you collect

At a high level, log analytics helps teams review, interpret and understand logs. [Log analytics](#) is critical for monitoring, troubleshooting and investigating reliability and security issues. It gets down to the root cause of why that issue occurred. Using analysis to make sense of all that data is just plain smart.

Log management and log analytics are related, but they refer to different aspects of working with log data.

Log management

Log management refers to the processes and tools used to collect, store and manage log data.

Log analytics

Log analytics refers to the process of analyzing log data to extract insights and generate useful information. The goal of log analytics is to use log data to improve the efficiency and effectiveness of an organization, identify and troubleshoot problems, and monitor the health and performance of systems.



Five benefits from log analytics for every organization

- 1 Improves application reliability with a framework for troubleshooting and root cause analysis to speed incident resolution and reduce MTTR.
- 2 Allows organizations to better monitor their cyber security posture and make their assets more secure. Logs can act as a red flag for bad actors, providing information like IP addresses, HTTP status codes, client/server requests and more.
- 3 Helps organizations maintain compliance with audits, security policies, or regulatory requirements. Organizations operating in certain industries may be required to comply with PCI, HIPAA, GDPR, FISMA, SOC, ISO, COBIT and others. Regular collection and analysis of log data provides organizations with information they need to comply with these bodies and assist with potential audit requirements.

- 4 Log analytics drive product analytics and user analytics that feed business and adoption insights. Logs provide data about how customers use a product, what's working and areas of a product that may have performance issues.
- 5 Empowers organizations to take a more proactive approach to business. Trend data provides information about traffic loads or spikes to inform teams about how to improve website performance or even when to release a new version or update.

BEST PRACTICES:

Get the most out of log management and analytics

Whether you select a new log management and analytics system or revamp your current system, maintaining log management best practices help you get the most out of your chosen solution.



Develop a log management policy

A log management policy helps ensure everyone follows set protocols. What information will your logs capture? How long should you store your logs? Are there regulatory or auditing requirements you must keep in mind?



Centralize your logs

Aggregating your logs is the best way to achieve an end-to-end experience where you can track your log data in a single platform. This best practice eliminates data silos and reduces duplicative efforts.



Use structured logging

Writing logs in formats like JSON or XML makes them easier to parse, query and analyze. This cuts down on time spent parsing and simplifies analysis.



Create meaningful log messages

Like most kinds of communication, the best log messages convey information clearly. Include context — in addition to fields like timestamps, user request identifiers and unique identifiers.

BEST PRACTICES CONTINUED:



Avoid logging sensitive or proprietary data

While logging more information is almost always better, this isn't necessarily the case with sensitive or proprietary data. Avoid logging application source codes, proprietary data, or any personally identifiable information (PII) to ensure compliance with data privacy standards.



Implement real-time monitoring

To ensure both reliability and an excellent user experience, monitor your logs in real time, leading to decreased downtimes and outages and catching potential security incidents.



Use data tiers

[Data tiers](#) sort your data into low-touch and high-touch logs. At Sumo Logic, our data tiering also helps you minimize costs, based on how often you plan to access the data you ingest.



Create analytics from logs

Log analytics is critical for troubleshooting and forensics investigations. Functions and methods, such as normalization, pattern recognition powered by machine learning, classification and tagging, correlation analysis and more, means you can manipulate log data to extract the performance, security and business information needed for IT teams and key stakeholders.



Use a cloud-native log management platform

Cloud-native log management companies understand the unique pain points and requirements that cloud-based SaaS companies face. As a cloud-native company ourselves, Sumo Logic understands how crucial reliability and security are—we require them both to maintain our own platform.

TOOL FEATURES:

What is the best logging tool?

As you begin your search for a log management and analytics solution, look for the following key features and functionalities.



Integrated, full-stack capabilities

The right [log management solution](#) will aggregate your data from cloud and on-premises infrastructure, eliminating silos to improve troubleshooting and security.



Tool consolidation

Tech stacks have gotten massive, and the best solutions support [tool consolidation](#). Sumo Logic, consolidates log data across both observability and security, providing you a single source of truth for all your data.



Cloud-native architecture

The right solution will make it quick and easy to manage your log data, security and digital transformation. Cloud-native architecture provides the scale and elasticity you need.



Machine learning analytics

The best log management tools empower teams to ingest and analyze any type of data, including structured, semi-structured and unstructured.



Tiered analytics and credit licensing

The best log aggregation tools offer cost-effective data tiered pricing and credit licensing to help meet your budgetary requirements.



Out-of-the-box auditing and compliance

[Compliance](#) and regulatory requirements are crucial components of the work you do every day. Look for a solution that offers cloud-native security and configuration analytics for rapid, continuous compliance.



Scale without compromising on reliability

The best log management tools offer you the flexibility to ingest data as it grows and scales without compromising on the performance.

CONCLUSION:

Ensure reliability and security with Sumo Logic

In today's increasingly digital world, customer satisfaction means providing a solution that's reliable and secure.

With Sumo Logic's log management and analytics solution, cloud-first companies can:

- Collect all your logs in one place
- Break down data silos between teams, systems and cloud providers
- Improve application performance and reliability with greater visibility
- Increase security and support compliance
- Gain business insights across your entire organization
- Lower costs

Explore our [full log management and analytics solution](#) or our [case studies](#) to find out how organizations like yours are excelling with Sumo Logic. When you're ready, take the next step and [start a free trial](#) to discover the Sumo Logic difference.

About Sumo Logic

Sumo Logic, Inc. (NASDAQ: SUMO) empowers the people who power modern, digital business. Through its SaaS analytics platform, Sumo Logic enables customers to deliver reliable and secure cloud-native applications. The Sumo Logic Continuous Intelligence Platform™ helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers around the world rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications. For more information, visit: SUMOLOGIC.COM

sumo logic

**s u
m o**