CASE STUDY

LogDNA is the Key to Kubernetes Observability

Quick Summary

INDUSTRY

Software

REQUIREMENTS

- Aggregated logging
- Kubernetes support
- Performance at scale
- Compliant logging
- Archiving

LOGDNA SOLUTIONS

- Centralizes logs from all sources
- Kubernetes Agent and Kubernetes Enrichment
- Supports 50TB of logs per month
- Compliant with SOC 2 Type 2, PCI-DSS Level 1, HIPAA, GDPR, Privacy Shield, and CCPA
- Automatic Archiving to S3

BUSINESS IMPACT

- Teams have holistic visibility into all of their systems and applications
- Users see logs 80% faster with LogDNA, improving MTTD
- Logs are now accessible and actionable across teams
- Compliant and secure

When you develop security software for containers, Kubernetes, and cloud services, as Sysdig does, you have an especially keen appreciation of what it takes to build an effective observability stack. You are also in a strong position to appreciate the efficiency that comes with modern observability tools that work seamlessly with next-generation platforms, such as Kubernetes.

Both of these factors contributed to Sysdig's decision to adopt LogDNA for gaining operational observability into its internal IT infrastructure. We recently spoke to Mark Breitung, a senior member of the DevOps team at Sysdig, about why the company chose LogDNA, and how the solution enables the holistic, contextualized observability that his team needs to keep the Sysdig platform running smoothly.

Searching for a Better Observability Solution

Sysdig, which builds security software for DevOps, initially relied on a custom-built observability solution to manage and analyze logs. The company's DevOps team used syslog to aggregate logs into an S3 bucket hosted in the Amazon cloud. Then, the team deployed Athena, an Amazon cloud service, to process log data.

This approach was an effective way to collect logs and store them in the cloud. However, it fell far short of delivering full observability. The Sysdig team's ability to query log data using Athena was limited, and there was no efficient way to customize queries for different types of logs, such as server logs and Kubernetes logs. The solution was also unwieldy to manage. It was "crazy town," according to Breitung, because it relied on a mishmash of open source tooling and Amazon cloud services, which made it difficult for the team to track down critical information quickly and gain holistic visibility into its systems.

Worst of all, the logs that the team aggregated into S3 buckets were difficult for most team members to access. Although in theory the logs were accessible to anyone, the tools necessary to process and analyze them were too difficult for the team to use efficiently in practice. The custom-built solution "got us a check box telling us that our logs were there, but I don't think anyone actually used it," Breitung explained.

The Switch to LogDNA

Shortcomings of the initial logging solution used by Sysdig pushed the team to search for a better solution, which it found in LogDNA.

For Sysdig, LogDNA offered an array of benefits. Most obviously, LogDNA allowed the DevOps team to replace its complex log management stack with a unified solution that provides log aggregation, processing, and management through a single tool while still allowing the team to keep its log data in the cloud.

But LogDNA did much more than simplify the logging solution stack. Another critical point of value is LogDNA's Kubernetes Enrichment feature, which provides native, out-of-the-box support for displaying Kubernetes events and metrics data alongside log data. That means that the Sysdig team can gain visibility into its Kubernetes clusters without writing extensive custom queries or managing Kubernetes metrics separately from other observability data.

LogDNA's built-in alerting features are also important. They enable the Sysdig team to write nuanced alerts that trigger notifications based not merely on simplistic metrics and thresholds but also on contextual data. "We can say in LogDNA, 'Send me an alert if X thing happens more than five times in a minute,'" Breitung said. "This is helpful when our backend doesn't have a metric yet," but the team nonetheless wants to configure alerts for certain types of events or patterns.

The graphing tools within LogDNA, too, stood out to the Sysdig team. With graphing, DevOps engineers can create rich visualizations to help them interpret log data, using whichever method suits them best: A line graph, a histogram, or a pie graph.

LogDNA's archiving features also help Sysdig manage its historical log data efficiently. With LogDNA, the Sysdig team can still archive log data in the Amazon cloud using S3, as it did with its original logging solution. The archiving experience in LogDNA, however, is simpler to manage and easier to automate. It also ensures that archived logs remain searchable, even if they are housed on a low-cost cloud storage service.

Finally and most importantly, LogDNA simplifies log access. With LogDNA, anyone with a Sysdig email address can easily access and interact with log data, Breitung said. He added that there is no need to manage complex user identities in the Amazon cloud, as there was when working with Athena.

Ultimately, LogDNA helped the Sysdig team to achieve an 80 percent improvement in the time it takes to access and use log data. By extension, the team has significantly reduced its Mean Time to Resolution (MTTR), ensuring that it can quickly and efficiently troubleshoot problems in production systems.

> *"LogDNA helped the Sysdig team to achieve an 80 percent improvement in the time it takes to access and use log data."*

Conclusion: LogDNA Delivers Easier, Kubernetes-Friendly Visibility

For the Sysdig DevOps team, LogDNA has greatly simplified log management and delivered critical observability into complex systems like Kubernetes, which few other log management solutions support natively. At the same time, LogDNA ensures that everyone on the Sysdig team can access visibility insights whenever they need to. That helps the Sysdig team achieve the same level of operational observability into its systems that Sysdig provides to its customers through its security observability solutions.

About LogDNA

At LogDNA, everything starts with our mission: To help developers be more productive so they can focus on what they love. We are a mission-driven, developer-first company. This mission is simple, but bold. We focus on logging because logs are the lifeblood for developers — it is the core atomic unit for how modern engineering teams understand what's going on with their systems, monitor what they are doing, and get information they need to troubleshoot. Simply put, everything rests on your logs.

Sign up for a fully-featured 14-day trial and optimize your logging workflow or reach out to our sales team to create a plan tailored to your needs at outreach@logdna.com today.

logdna

Thank You

Sales Contact:	outreach@logdna.com
Support Contact:	support@logdna.com
Media Inquiries:	press@logdna.com