sysdig

CASE STUDY

LogDNA Delivers Higher Uptime and Improved Customer Experience

COMPANY DETAILS:
The LogDNA log management solution enables DevOps teams to aggregate all of their system and application logs into a single platform.

BUSINESS NEEDS:

- Deliver Kubernetes logging capability to customers
- Transition the entire stack to run as microservices on Kubernetes

CHALLENGES:

- Managing Prometheus servers was time consuming
- No audit trails for debugging and troubleshooting
- Lack of alerting before an event impacted customer experience

BUSINESS IMPACT OF SYSDIG:
Improved customer experience by reducing time to resolve performance issues. Improved efficiency for compliance and audit processes.

SYSDIG PLATFORM BENEFITS:

- Quick insight to address security issues pre-production
- Dashboards help to understand what is going on in the environment
- Audit trails for efficient troubleshooting and compliance reporting
- Fast ramp with dashboard and alert creation across all environments
- Minimal maintenance effort

INFRASTRUCTURE: Amazon Web Services

ORCHESTRATION: Elastic Kubernetes Service (EKS)

logdna

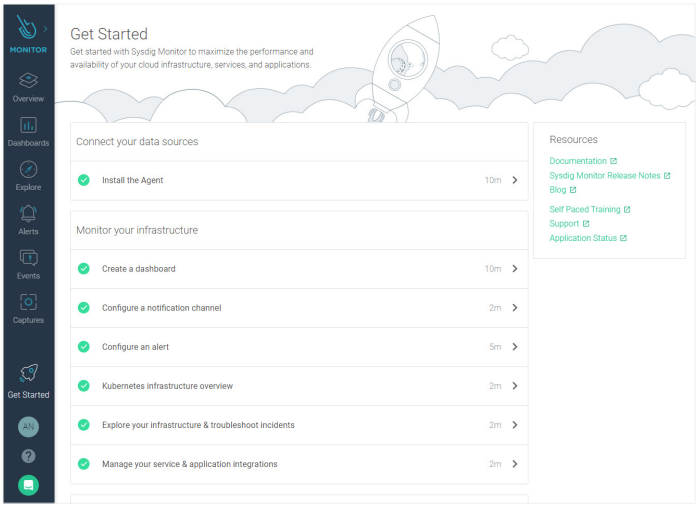
Overview

LogDNA is a centralized log management solution that empowers DevOps teams with the tools that they need to develop and debug their applications with ease. They help thousands of companies, from startups to large enterprises, take control of their data and gain valuable insights from their logs.

As Kubernetes has matured over the last few years, LogDNA found that a growing number of customers wanted a Kubernetes logging solution. To meet the market need and to take advantage of consistency, scalability, and repeatability, the company made the decision to transition its entire stack to run as microservices on Kubernetes.

According to Ryan Staatz, Systems Architect at LogDNA, “Microservices make things a lot more interesting. There are a lot of things running at the same time. One of the cloud environments we use is Amazon EKS and we really enjoy the fact that it is a managed service. We don’t have to focus on managing the Kubernetes masters and we can just do what we do best, which is running our application stack in Kubernetes.”

By building their environment on Kubernetes, LogDNA became first-hand Kubernetes experts for their customers, which includes understanding the tooling options available to them. The log management company runs more than two dozen Kubernetes clusters, containing over 1,000 workers and 21,000 pods, with a mixture of stateful and stateless applications.



Challenge

Being in the data business, LogDNA understands the value of good data. They realized they needed better visibility and security for their AWS environment. Staatz explained, “If someone has access to a privileged container with the right settings, they can access and change the underlying node’s OS and aspects of it. Being able to monitor this is really important. Containers aren’t just free. They're not just magically secured. And that’s just one reason you need monitoring.”

After initially building monitoring tooling alongside Prometheus, the LogDNA DevOps team realized the resource drain of scaling Prometheus. Staatz related, “We started trying to manage our own alerts and we found that it was somewhat unwieldy, at least at the time. Having to consistently manage Prometheus over more than a dozen deployments was an operational burden. Using Sysdig to monitor Kubernetes metrics and security allows us to focus on logging.”

After evaluating solutions, LogDNA chose Sysdig. According to Staatz, "Sysdig is our go-to metrics provider for Kubernetes, there is no better choice than Sysdig to meet our monitoring and security needs. Sysdig reports on our entire AWS infrastructure, including infrastructure and application events."

> “Sysdig is our go-to metrics provider for Kubernetes, there is no better choice than Sysdig to meet our monitoring and security needs.”
>
> - Ryan Staatz
> Systems Architect, LogDNA

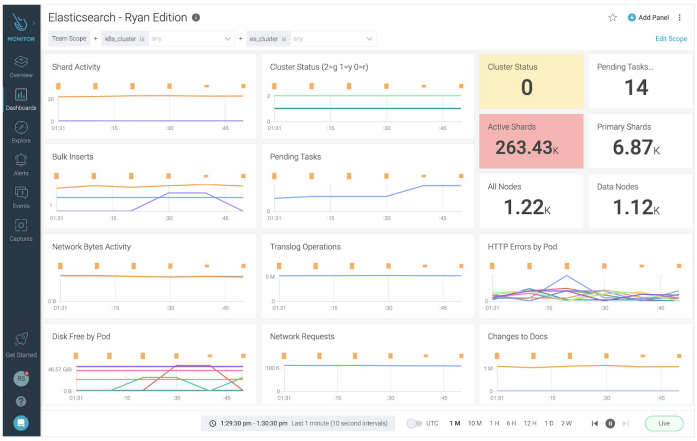
Catching customer-impacting events 98% of the time

LogDNA takes full advantage of the Sysdig alerting feature. As Staatz explained, “One of the really cool features of Sysdig is that it continuously scans container images and it alerts when there is a problem. For example, if the developers are alerted to a vulnerability in our version of Lodash, they know that they need to check it out before that code goes to production. These proactive notifications really help our developers that are focused on making updates quickly. With Sysdig, we know if

there's an issue almost immediately after our CI or CD pipeline builds an image that is being shipped into the container registry. Every time we update a dependency, there's obviously a risk of there being a vulnerability. So we use Sysdig all the time to find these vulnerabilities and alert us."

> "With Sysdig, we're able to resolve incidents faster. We're able to get insights faster. We're able to tell when there are performance problems faster. And so as a result, we're able to deliver a consistent and better customer experience that we otherwise would not be able to without Sysdig."
>
> - Ryan Staatz
> Systems Architect, LogDNA

"The detection and alerting has been super valuable for not just us, but also our end customers because we get those alerts quickly. It has moved us to be able to identify customer impacting events before customers, easily 98% of the time. We pinpoint the cause quickly. For example, it could be a resource contention, maybe it's a security concern, or perhaps it's just somebody resolving incidents in some way. In general, at the end of the day, the measure to our business value is how effective we are at enabling a better experience for our customer. With Sysdig, we're able to resolve incidents faster. We're able to get insights faster. We're able to tell when there are performance problems faster. And as a result, we're able to deliver a consistent and better customer experience that we otherwise would not be able to without Sysdig."



"There's no end to all the things you can do with Sysdig"

LogDNA finds a lot of value in the dashboards. As Staatz said, "The segmented line panels and the ability to scope variables make pivoting really helpful. One unexpected feature that I use heavily is the ability to choose whether to override the dashboard scope so context can be provided across multiple segments."

Sysdig provides out-of-the-box dashboards to help organizations get started quickly and point novice users to what they should focus on. The platform also enables companies to build their own dashboards as their operations mature.

"We really appreciate the ability to set up dashboards that are custom-tailored to what we want to look at," said Staatz. I recently made a dashboard to track disk usage across mounts for a particular set of pods. Some graphs segment on Kubernetes cluster, others segment on mount point.

The scope allows selecting for specific clusters, but you can easily compare the cluster-specific graphs with the segmented per cluster graphs for context if you need that."

"I also like being able to see alerts overlaid onto these dashboards. This enables us to see if there's a correlation between alerts and certain activity. This is something I use all the time with networking issues, CPU contention, memory, or even for something simple, like if I discover that there are too many pending tasks in ElasticSearch. It's all in one place and super wonderful for us to use. There's no end to all the things you can do with Sysdig."

> **"I was amazed by the amount of data collected by default by Sysdig. We don't have to do much at all. It's already there. We just have to make the dashboards that we want, and even then they have canned ones which is really cool."**
>
> **- Ryan Staatz**
> **Systems Architect, LogDNA**

Fast ramp and minimal effort to maintain

Speaking on the set up and maintenance of Sysdig, Staatz said, "Set up is really simple. You put in some configurations. They run and deploy a daemonset, and you're good to go. Just like that, and all of these metrics are automatically shipped to Sysdig and you can see them in this wonderful UI. And it's not just regular performance metrics or application metrics that you can see, but you can also observe insights around security as well. I was amazed by the amount of data collected by default by Sysdig. We don't have to do much at all. It's already there. We just have to make the dashboards that we want, and even then they have canned ones which is really cool."

Staatz went on to explain, "The fact that Sysdig is immediately compatible with Kubernetes was a big draw for us. A lot of the security around Kubernetes is new and it's kind of hard to grapple with it at first. Sysdig helps with a lot of that and we don't have to do a lot of managing the Sysdig stack, which ultimately makes our lives easier so we can focus on debugging our own stack."

Sysdig Captures makes compliance audits easier

Sysdig provides a feature called Sysdig Captures, which records audit trails in the event of anomalous behavior to help with post-event investigations and troubleshooting. Staatz explained, "A Sysdig Capture is a TCP dump-style of information saved, should there be a targeted area you want to look at. It includes information on the connections being made, things happening, and events."

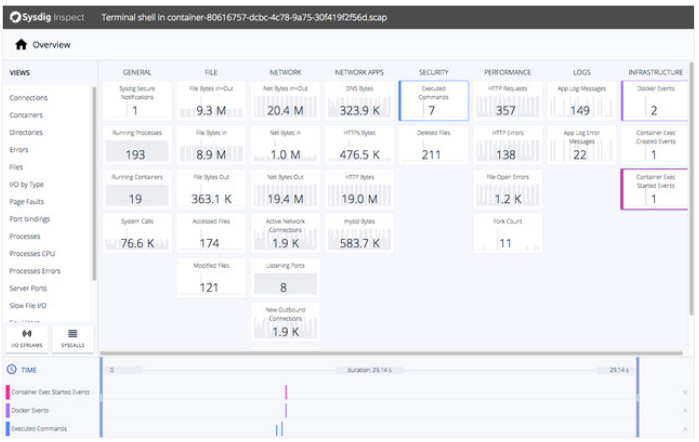
With the Sysdig single source of truth, LogDNA has access to a massive amount of granular data that can be cut and analyzed from any perspective. Sysdig Captures is unique to Sysdig and on top of the audit file it provides; the deep data can't be matched. As Staatz said, "We get all sorts of information – at host, node, and pod level. Anything you'd ever want to know about the policy event can be logged – and our security team very much appreciates having this in place – especially around compliance and audits and things like that."

Sysdig helps troubleshoot tough issues, faster

Sysdig Captures also provides an audit trail that helps LogDNA when there is anomalous behavior but the container has been killed. “In addition to seeing and alerting on access, with Sysdig, you can also put custom policies in place that will do things,” said Staaz. “For example, we have policies that capture specific information if a certain thing happens so we have the file later to troubleshoot from.”

Speaking about troubleshooting, Staatz explained, “If you exec into a container shell and you start executing commands, Sysdig records that session for you. It’ll alert you so you can proactively know what's happening immediately. Even when it's something as innocuous as an SRE going in and doing something to help resolve an incident, you can at least know what's happening because there is an audit of all of the different connections made to containers.”

The deep data Sysdig gets means there is more data to use when understanding an issue. “We used Sysdig to debug and track down the harder issues we’ve experienced,” said Staaz. “For example, we once had TCP errors between external load balancers and our pods that receive that traffic. Sysdig was instrumental in figuring out where that problem was. We've seen things like CPU contention where on the end-of-the-line node there was no high CPU but we saw performance issues for the pods running on it. When we looked closer, the load was sky high, for example. And so we were able to get those sorts of insights just by having Sysdig dashboards and pivoting on those pieces of information.”



For LogDNA, the insight gained from using a single security, compliance, and visibility platform tailored for Kuberenetes has made it easier for its security and DevOps teams to solve issues faster. The efficiencies gained from using Sysdig help LogDNA ensure their time and efforts are spent on executing strategic initiatives to better serve its customers and continue to grow its business.

Learn more at www.sysdig.com

CS-LOGDNA Rev. A 9/20