sysdig cloud

CASE STUDY

INTRO

The Brigham Young University (BYU) Department of Chemistry and Biochemistry is one of the leading research departments at BYU, focused on research that includes calorimetry, macrocycles, cancer therapy, and chromatography. Like most modern higher education institutions, the faculty and students in BYU's chemistry department routinely access online systems that provide access to research and provide a way to submit assignments and coursework. Keeping these systems up and running is of the utmost importance for the Department, as downtime and slow performance directly inhibit their ability to drive innovation.

LIFE BEFORE SYSDIG CLOUD

Garrett Hyde, System Administrator at BYU's Department of Chemistry and Biochemistry, was using the open source solution Nagios but was looking for a better way to monitor their internal systems. He found that Nagios did a satisfactory job of giving him the status of his servers, but failed to provide insights into why a particular incident occurred and wasn't able to provide visibility into the interactions and dependencies between the different components of his environment. This led to many hours of retroactive, manual troubleshooting involving combing through logs, reviewing kernel dumps, and using top to monitor the server manually, waiting for the issue to happen again. Oftentimes Garrett was forced to guess what the root cause of a particular issue was and hope that he had diagnosed the issue correctly. One particularly frustrating memory-related issue involved a web server crashing repeatedly. This type of problem would typically take over a day to diagnose and fix with Garrett's existing toolset, and he never was able to know for certain whether his actions resolved the issue or if it simply disappeared for the time being. There needed to be a better way.

CHOOSING SYSDIG CLOUD

When evaluating Nagios replacements, Garrett had four key requirements in mind.

1. PROCESS-LEVEL VISIBILITY

Getting deep visibility into what was going on at any given moment inside his system was hugely important to Garrett. Nagios didn't do a great job of uncovering root cause, so any solution that he chose needed to have drill down capabilities to streamline his troubleshooting efforts and show exactly which processes were being run inside his environment.

2. REAL-TIME METRICS STREAM

It was important to Garrett to have an up to the second view of all the metrics being collected in his environment. This would allow Garrett to detect and investigate performance bottlenecks immediately and reduce unplanned downtime.

3. PROACTIVE ALERTING

Garrett wanted to be the first to know when system performance started degrading. It wasn't enough to know what servers were up or down, Garrett needed insights into the performance of his system over time and to be automatically alerted when abnormal performance was observed.

WHY SYSDIG CLOUD?

- One-second granularity live data streaming
- Historical replay
- Process-level visibility
- Automatic correlation of metrics across the environment
- Easy setup and maintenance

KEY BENEFITS

- More efficient troubleshooting
- Proactive performance management
- Holistic view of environment

> *"Sysdig Cloud pinpoints actual truth as opposed to hunches and guesses. It makes troubleshooting problems much faster and easier."*

4. HISTORICAL REPLAY

Finally, Garrett needed to analyze historical data to enable retroactive system troubleshooting and analysis. Being able to examine system health in the past is an important component of any monitoring strategy.

Garrett installed Sysdig Cloud to evaluate how it could address his requirements and he found the deployment process very fast and straightforward. "Easiness [of the install] would probably be a nine out of ten… with ten being I didn't have to do it," said Garrett, "It was magical." The total deployment time across all servers was 15 minutes, which allowed him to realize value right away.

LIFE AFTER PURCHASING SYSDIG CLOUD

Sysdig Cloud has given Garrett the information he needs to proactively manage the performance of his environment. Garrett appreciates the way the data is displayed in Sysdig Cloud because it automatically surfaces information that he can immediately take action on.

The one-second granularity data streaming from Sysdig Cloud provides Garrett a simple way to observe what's happening at any given moment inside his infrastructure. He's pinned the key statistics he's tracking to custom dashboards in order to track them more effectively. Garrett can also pause the data stream and move backward in time with the same one-second granularity, enabling retroactive troubleshooting to discover what system activity contributed to particular bottlenecks. The intelligent alerting triggers notifications the second abnormal behavior is detected in the environment, ensuring Garrett is the first to know about degradations.

Once Garrett identifies bottlenecks it's very easy for him to drill down to a particular area of interest within his environment. Iterating from a high level view of system health down to specific activity inside a component gives Garrett the drill down capabilities he needs to rapidly isolate root cause. "If Apache crashes, I can look at that machine's metrics like Memory and Disk I/O and analyze the processes that led to that crash," said Garrett.

Sysdig Cloud also automatically correlates all system metrics together so Garrett can quickly spot patterns and trends over time using the powerful built-in views and explore any metric and visualize it as a time series, a top 10 chart, a map, or a data table. By allowing Garrett to slice and dice his server, application, network, and database metrics in a number of different ways all in the same view, Sysdig Cloud lets him easily uncover the data he needs to solve performance problems fast.

By leveraging these capabilities, Garrett's monitoring and troubleshooting process has become significantly more efficient. "Sysdig Cloud pinpoints actual truth as opposed to hunches and guesses," Garrett said, "It makes troubleshooting problems much faster and easier." That memory issue that was crashing his web server and would typically take over a day to resolve? Sysdig Cloud provided him the information he needed to isolate the issue and fix the problem in under 5 minutes, a whopping 99% reduction in mean-time-to-resolution (MTTR). Since purchasing Sysdig Cloud, this particular issue hasn't reappeared in his environment due to Garrett being notified ahead of server crashes the instant memory spikes outside of what's expected and having the ability to validate his remediation actions in real-time.

Garrett also values how easy Sysdig Cloud is to maintain. In the past, Garrett would routinely spend hours configuring his Nagios deployment, Sysdig Cloud has enabled him to virtually eliminate that configuration requirement altogether. "Just a periodic agent update and that's it," Garrett stated.

Try Sysdig Cloud for free today at sysdigcloud.com