sumo logic

Log analysis: from days to 30 minutes

Results at a glance

- → Saved 30+ minutes per day by automating CloudOps engineering actions
- → Obtained strategic partner for multi-cloud environment analytics
- → Improved data intake cost-effectiveness
- → Empowered engineers to focus on high-value engineering functions
- → Optimized workflows to further automate reliability monitoring

AUTOMATION ANYWHERE
Go be great.

SUMO LOGIC PRODUCTS

Log Analytics

Application Observability (APM)

USE CASE

Digital Customer Experience

sumo

Challenge

With logs growing faster than ingest budgets, the company needed to ensure no data was lost and all reliability-critical analytics were maintained.

As the world embraces digital transformation, Automation Anywhere has grown rapidly, introducing new challenges. While Automation Anywhere engineers continuously build new features, their customers use their solutions at an accelerated rate. This results in an explosive amount of data coursing through their systems.

Ensuring observability and reliability throughout their tech stack is of the utmost importance for Automation Anywhere. Raj Desikavinayagompillai, US Cloud Operations lead for Automation Anywhere, shares that the main challenge is to ensure that all data is collected and searchable. However, ingest budgets are not growing as fast as the logs — a challenge for many organizations experiencing rapid growth. They must stay within their ingest budgets while ensuring that no data is lost, and all reliability-critical analytics are gleaned from the data.

Raj says that collecting logs is just the tip of the iceberg, "Logs are nothing but data for us. We want to do more with the data." Automation Anywhere needed a cost-effective solution to scale their cloud observability infrastructure that would allow them to collect all logs as well as make them useful and actionable for their teams.

AUTOMATION ANYWHERE
Go be great.

INDUSTRY

Software company

ABOUT

Founded in 2003, Automation Anywhere is an American global software company that builds products that empower people who make the companies they work for great. With millions of bots supporting their global clientele, Automation Anywhere's goal is to liberate people from mundane tasks so they can focus on high-value work, solving creative, higher-order business challenges.

"Logs are nothing but data for us. We want to do more with the data."

Raj Desikavinayagompillai
US Cloud Operations lead, Automation Anywhere

Solution

Automation Anywhere chose Sumo Logic as its strategic observability partner in ensuring the collection of all log data and extracting actionable insights while staying within budget.

Sumo Logic has helped Automation Anywhere dramatically increase efficiencies. Data Tier pricing allows Automation Anywhere to collect all logs as their data ingestion requirements grow. Dashboarding and alerting features enable Automation Anywhere to build workflows that have reduced time spent on analysis from days to less than 30 minutes.

Further, Sumo Logic provides the needed toolkit for Automation Anywhere to develop and refine their workflows to reduce manual engineering tasks, most notably through auto-remediation with the Shoreline and Sumo Logic integration. Other key tools used in this solution include Atlassian Opsgenie and Jira.

By the numbers

<30

minutes spent on analysis

Results

Raj, being in the industry for over two decades, is very familiar with the solutions available in the market. In his previous company, he worked with Splunk. Now at Automation Anywhere, he is the lead Sumo Logic evangelist, growing the strategic partnership.

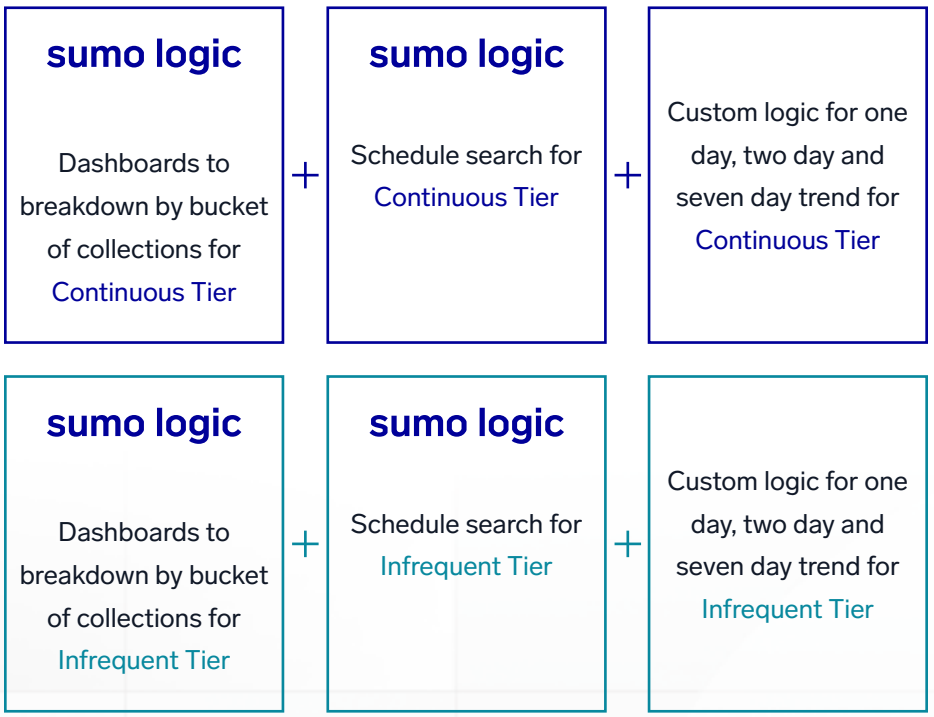
Automation Anywhere's engineers are continuously working with Sumo Logic to free up engineering hours by identifying ways to use Sumo Logic's features and integration capabilities to create workflows that simplify monitoring and ensure reliability.

Cost-effective, scalable data ingestion and monitoring through tier-based pricing

Automation Anywhere uses Sumo Logic's Continuous and Infrequent pricing tiers to ensure all their logs are ingested and monitored while staying within their ingestion budget. They currently use Sumo Logic to ingest and monitor data for their entire cloud environment on AWS and GCP — from their queue, Relational Database Service (RDS), frontend and application stacks.

Using Sumo Logic's scheduled search feature with custom logic set up for one-day, two-day, and seven-day trends for each tier on the collector level, the Automation Anywhere team can monitor their entire system and get alerted for any pattern changes that need to be addressed.

Automation Anywhere monitors their entire system across data tiers



Data tiers in use

- The Continuous Tier is for the data used to monitor and troubleshoot production applications and to ensure the security of applications.
- The Infrequent Tier is for data that is used to troubleshoot intermittent or hard-to-reproduce issues. For example, debugging logs, OS logs, thread dumps, etc. The Infrequent tier has a pay-per-search pricing model, and low ingestion cost.

Reduced log spike analysis time from days to 30 mins

A change in pattern, such as a log spike, triggers an Opsgenie alert which then kicks off a JIRA ticket. Automation Anywhere uses Sumo Logic's dashboards to group log data within buckets based on Kubernetes clusters, allowing them to focus on smaller pools of logs when responding to alerts, reducing mean time to repair (MTTR) — from triaging, analysis and debug time — from what used to be days to around 30 minutes.

For a company with a massive global footprint of around fourteen data centers, reducing time going through logs by categorizing them into smaller piles makes for faster analysis and time to action. "Every minute we waste is time which we can save to recover incidents quickly," shares Raj. Here's an example of a JIRA ticket that gets kicked off from this workflow which an on-call engineer then fixes in real time.

```
Description: Alert if spike in Kubernetes log ingestion(continuous-datatier)
Results:
[{"collector":"<eksclustername>","envtype":"largeEnv","gbytes":<SizeinGb>,"gbytes_1w":<Sizein
Gb>,"gbytes_2w":<SizeinGb>,"sendalerts":"True","spikegbytes_1w":<SizeinGb>,"spikegbytes_2
w":<SizeinGb>}]
```

Automated reliability monitoring and incident resolution through Sumo Logic and Shoreline integration

Sumo Logic ensures that all log data is monitored, and anything past set thresholds triggers an alert. From there, the Shoreline integration drives a self-healing workflow that takes runbooks already deployed in Op Packs and automatically applies quick fixes to known incidents.

This workflow has improved the MTTR for known incidents by eliminating the one to three manual actions on-call CloudOps engineers have to make each day, saving around 15-45 minutes of engineering time previously used manually going through incident runbooks and applying fixes. This doesn’t include the productivity loss eliminated from interruptions and task switching.

This is especially crucial when issues arise on the cluster level. When data ingestion is interrupted, issue resolution is further complicated and slowed down because not only is there a bug that needs to be identified, but there’s also a gap in the flow of real-time data required to monitor and troubleshoot clusters. Auto actions and auto-remediation with Sumo Logic and Shoreline reduce the time and data loss from these incidents. Moving forward, Automation Anywhere intends to build out this integration further.

Looking ahead

Automation Anywhere sees Sumo Logic as a strategic partner in building out their observability infrastructure. They aim to expand observability within their current stack, including AWS and traces, to paint an even more comprehensive picture of system and app insights, and identify security threats in real time.

Further building out the Shoreline integration with Sumo Logic is also in the pipeline. With Shoreline as the platform, the future state involves Sumo Logic as their observability solution to monitor their full tech stack using scheduled searches, invoking Shoreline actions in response to alerts, and Shoreline actions triggering a remediation script that could kick-off auto-remediation or auto action, freeing up CloudOps engineers from manual actions in the entire alert response workflow.

Learn more

Automation everywhere!
Using data to automate and accelerate cloud operations

WATCH THE FULL SESSION

305 Main Street, Redwood City, CA 94603