observIQ

SOLUTION BRIEF

Splunk Alternative For Operational Logs

Using A Purpose-Built Log Management Platform Is A Cost Effective Splunk Alternative For DevOps And ITOps Teams

The Problem

Many organizations use expensive SIEM solutions like Splunk to monitor ALL of their logs. However, operational logs have different requirements, and expensive SIEM tools are not necessarily the right tool for the job.

Splunk Is Not Made For Monitoring Operational Logs

A typical large enterprise may have hundreds of app teams collecting and processing logs from countless sources such as Apache, Tomcat, Kubernetes, and others via SIEM tools such as Splunk, while in reality, these security-focused incident and event management solutions aren't built for those types of logs. Not only is the cost of using SIEM products as log aggregation tools prohibitively expensive, but products such as Splunk are purpose-built - and exceptionally well-built - for the security use case, adeptly handling trend analysis, anomaly detection, and a host of other functions that security teams focus on.

But that's not consistent with the needs of DevOps or ITops teams. The $100,000 Porsche Taycan is an outstanding performance car, but it's not much help when you need to take the family to the beach for the week. Using SIEM products for all log aggregation drives throughput, and therefore cost. Moreover, SIEM tools require advanced administration resources and data custodians to manage the solution, adding even more expense to organizations that rely on them.

In today's environment, there's no need to conflate operational log aggregation and security log analysis. Organizations can have the best of both worlds, and the associated cost savings as well. Using Splunk and other SIEM tools for security alongside purpose-built operational log aggregation tools is not only feasible but rapidly becoming an accepted best practice.

The Challenge

Although SIEM tools are overly expensive, and open source solutions require extensive time, effort and expertise, there have not been effective alternatives for enterprise grade log management.

Vendor Lock-In

Many companies are looking for ways to either scale back or move off of SIEM tools, and particularly Splunk, but face difficult tradeoffs because their proprietary models lock customers in and makes it difficult to switch. And, up until recently, the alternatives haven't been able to fully address the specific log management challenges DevOps and ITOps teams confront daily in increasingly dynamic multi and hybrid cloud environments.

Build Your Own Vs. Buy

Smaller shops may find it appealing to build their own log management systems using open source log agents such as Fluentd, Fluentbit or Logstash, as part of an Open Source Log Management Platform.

However, the time and effort required to build a logging stack - plus maintaining and upgrading it on a regular basis - is an untenable burden for most companies. Furthermore, while these deployments can

work well on a small scale, they require considerable administrator attention to adequately support the high-throughput needs of enterprise log data collection and observability use-cases.

Increasingly, organizations are finding that they need flexible, commercially-supported log management solutions with enterprise grade features that scale as their businesses grow, and work seamlessly across multi and hybrid cloud environments.

The Solution

DevOps/ITOps logs do not need to be monitored in the same system as security logs. Avoiding costly SIEM tools and utilizing a purpose-built log management platform can save organizations a significant amount of money. Using the observIQ Cloud log management platform, which is built on observIQ's ultra-low-resource-consuming, high-performance Open Source Log Agent, users can easily extract IT operational logs from the SecOps environment as a low-cost, Splunk alternative.

Move To A Purpose-Built Solution

By reducing data ingestion and storage in costly security-focused platforms like Splunk, DevOps and ITOps professionals can move operational logs to a more cost effective, purpose-built log platform like observIQ Cloud.

observIQ Cloud is a powerful, full stack SaaS log management platform built on a best-of-breed log management agent and the Kibana visualization tool customers are already familiar with. The observIQ Cloud platform is scalable, reduces network load, and stores data more efficiently and with more reliable and faster log-to-platform delivery than legacy log collection agents.

A core element of observIQ Cloud is the observIQ open source log agent, Stanza. Not only does Stanza provide out-of-the-box support for more than 50 of the most common log sources - including

custom parsing and formatting for each, intelligent defaults, and predefined configuration - it has unmatched technical performance, using up to 10 times less CPU and memory than legacy log agents.

Move to an open, industry-leading solution and stop investing significant time and effort learning SPL or becoming a SIEM ninja in a proprietary ecosystem.

Moving operational log collection from SIEM products to a purpose-built, intelligent log aggregation platform not only reduces raw throughput costs, but also places log collection decisions in the hands of the professionals who know best what's required: the DevOps and ITOps teams themselves. With the ability to intelligently collect logs, the operational teams can accelerate collection when issues are spotted without the need to ship everything up front and decide what's valuable later...after unnecessary throughput money has already been spent.

Move To The Cutting Edge and Stay There - All While Eliminating Vendor Lock-In

Imagine if, regardless of the platform you ultimately sent the data to, you could instrument your code with the same libraries, the same agents, and a single set of binaries and libraries. It would dramatically simplify the deployment process, internal training, and make it trivial to change or add analytics platforms as needed.

This is the promise of the OpenTelemetry project which is supported by nearly all the largest monitoring and cloud vendors and was officially started in May 2019. It's a Cloud Native Computing Foundation sandbox project and resulted from the merger of the OpenCensus and OpenTracing projects. They've since expanded their objective to include not only application tracing and code instrumentation, but also metric and log collection, essentially covering all the critical telemetry points in a system or application.

Through the OpenTelemetry working group, observIQ technology remains compatible with these latest standards. Always be on the cutting edge of monitoring instrumentation and observability with observIQ.

Powerful And Easy To Use With Unmatched Performance

With observIQ Cloud, customers can sort, search, visualize and manage all of their log data in real time, and easily create their own custom log parsers and plugins. Additionally, customers will be able to update and configure agents remotely, change log levels and parsing on the fly, and know when log messages fail to send. For larger environments, customers can update all their log agent configurations at once with fleet management capabilities.

Not only does observIQ's open source log agent, Stanza, process log data up to 10x faster than FluentD and Logstash, but it is resilient in the face of massive log volumes that cause these existing agents to fail. Stanza provides guaranteed log delivery, alert storm mitigation and an extensive log plugin catalog as well. It automatically aggregates log signals from any source – including microservice architectures, containerized environments, and hybrid cloud logs – into a single platform.

About observIQ

observIQ's mission is to build the best open source observability solutions for DevOps and ITOps. Built by engineers for engineers, observIQ has a specific focus on developing the latest next-generation agent technologies as part of its modern observability platform.

Scalable Observability.
Intelligent Control.

3225 N. Evergreen Drive NE,
Suite 103
Grand Rapids, MI 49525
(616) 719-4550
observIQLabs.com

©2020 observIQLabs. All rights reserved.