observIQ

SOLUTIONS BRIEF

observIQ Cloud

Log Management Made Simple

Businesses require a single cohesive view across all systems as they increasingly shift to running today's modern interconnected application stacks. Yet many of the largest organizations in the world are struggling to solve the challenge of collecting and monitoring massive log volumes across distributed systems. From exponential growth in log data to an ever-expanding list of log sources that organizations need to manage, log management is complicated and the tools to monitor logs haven't kept up.

Whether it's newer hosted DevOps and ITOps-focused log platforms or costly SIEM platforms that aren't optimized for operational log data, existing solutions are missing the mark. While some deliver a solid platform, the installation and configuration are too challenging for customers, and time to value is far too long.

At observIQ, we've created a dramatically simpler solution to managing logs for DevOps and ITOps teams, leveraging technology we developed for Google, VMware and others to address this problem.

observIQ Cloud is an intuitive log management platform addressing today's modern log management needs that DevOps teams can actually use.

Built upon observIQ's best-in-class open source log agent and using our highly-customized version of Kibana, observIQ Cloud allows customers to quickly and easily monitor multi and hybrid cloud environments so they can spend less time configuring and more time investigating.

With single-line installation, pre-built integrations, and fully automated remote agent management, deploying observIQ Cloud takes minutes, not hours or days. Dashboards are auto-installed for each integration so the instant you begin streaming logs, you have a curated view showing what's important. This provides customers the power to search, filter, and visualize events with ease, and get to a root cause far more quickly than other solutions.

observIQ Cloud reduces MTTR by automatically parsing and enriching logs with critical environment information, providing the context needed to easily trace events to the failing service. .

Popular customer use cases include:

- Rapid Incident Investigation
- Flexible Log Aggregation
- SIEM Cost Reduction

Simple to Set Up, Easy to Use

Regardless of the size of your company, you need a log management platform that addresses all of your needs via a reliable, secure, cost-effective method that's easy to implement and doesn't require specialized personnel to operate.

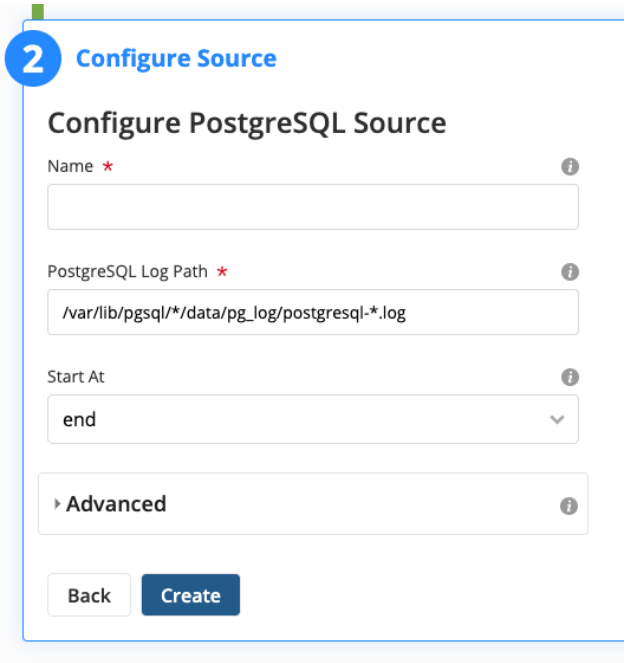
Engineers at observIQ understand the log management challenges that ITOps and DevOps face and have designed observIQ Cloud to free up developers to focus their time on developing new apps rather than worrying about managing event data.

With one-line agent installation commands, agents are installed and ready to manage within 30 seconds. And with guided remote configuration, and pre-built integrations, you can deploy end-to-end, modern log management ***in minutes*** with observIQ Cloud.

observIQ Cloud is easy to use right out of the box, providing support for 50+ of the most commonly used log sources and dashboards. Agents are auto-installed for each integration so you can see what's important the moment you begin streaming logs.

Customers also save time by updating all of their agents at once with one click thanks to fully automated remote agent management.

The team at observIQ has done the hard work for you so you can spend less time configuring, and more time investigating.



At observIQ, we're committed to helping customers get the best observability solutions for their needs as easily as possible - say goodbye to manual installation, configuration, and management.

Reduce MTTR with Rapid Incident Investigation

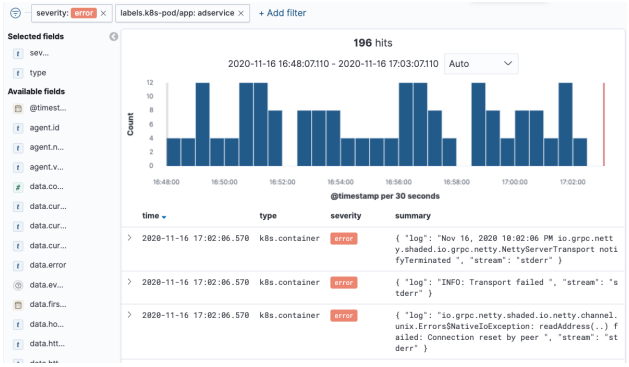
When you experience instability or an outage in your environment, you need to be able to quickly investigate and identify the source of the failure. Without the proper context, tracing an incident through your logs can be a slow and arduous process.

With observIQ Cloud, your logs are automatically parsed and enriched to provide the context needed to filter, search, visualize events with ease. Your logs can easily be tagged with custom labels as well, allowing you to specify data center, region or environment for complete traceability. With this robust context, you can identify the root cause of the issue quickly.

For example, if a service running on Kubernetes becomes unstable, the related, enriched logs will include useful information such as Deployment, Namespace, and Container, allowing you to easily trace an incident back to the failing service and correlate with other cluster-level events.

observIQ Cloud enables faster incident investigation so you can reduce MTTR and spend less time debugging and more time coding.

t resource.k8s_cluster_name	Hipster Store Prod
t resource.k8s_deployment_name	frontend
t resource.k8s_namespace_name	default
t resource.k8s_namespace_uid	b152e4b4-ac48-40c9-9813-a782f4e05822
t resource.k8s_node_name	kube-116-c1-w-0
t resource.k8s_pod_name	frontend-858d69d8dc-5bx48
t resource.k8s_pod_uid	927c5dbf-11e3-4baf-94e4-f1f66f485d9f
t resource.k8s_replicaset_name	frontend-858d69d8dc
t severity	error



If your SQL Server instance experiences an outage, deep and automatic parsing of Windows Event Log channels can guide you to a specific application and failure code.

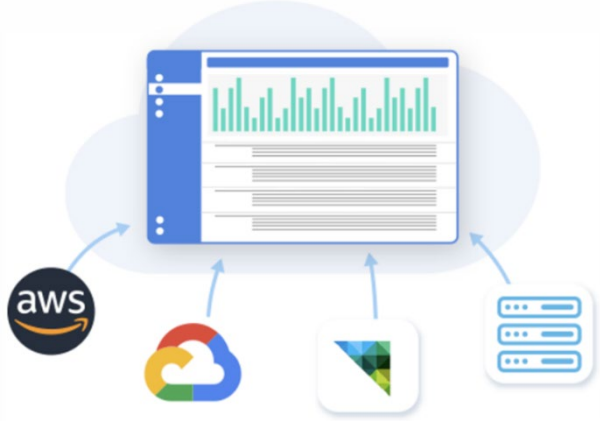
Aggregate All Your Logs – Wherever They Live

With newer applications residing across various hybrid cloud environments and legacy applications residing on-prem in data centers or field locations, retaining a legacy on-prem log solution can be costly due to increasing storage needs and specialized administration and deployment.

When different log aggregation tools are used for their different functionalities, it can make root cause analysis more difficult and time-consuming. Many struggle to find a single, cost-effective log collection tool that can aggregate all logs in a single location for analysis.

With observIQ Cloud's flexible log aggregation, you can collect all of your logs – wherever they live – via a reliable, secure, and cost-effective method that does not require specialized personnel to deploy and operate.

Efficiently and automatically aggregate logs from hybrid-cloud environments, containerized environments and microservice architectures into one log platform at scale with observIQ Cloud.



observIQ Cloud lowers the total-cost of ownership and mean time to value by making it as fast as possible for you to collect logs across multiple data centers, services, and clouds.

Reduce SIEM Costs

A typical enterprise may have hundreds of app teams collecting and processing countless log sources 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 they're not consistent with the needs of DevOps or ITOps.

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.

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.

Save your organization a significant amount of money by using a purpose-built log management platform.

Use observIQ Cloud for your IT operational logs and take advantage of simple and cost-effective consumption-based pricing.

- observIQ customers are saving over 50% by replacing costly $100K+ Splunk deployments with observIQ solutions
- Or use the observIQ Open Source Log Agent in building your own low-cost, high-performance log management solution

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.

Business value – observIQ Cloud

Rapid Incident Investigation

- Quickly understand what happened by easily tracing an incident back to the failing service
- Reduce MTTR with faster incident investigation and spend less time debugging, more time coding

Flexible Log Aggregation

- Minimize risk of missing critical events by gaining unified view of traditional and modern workloads plus guaranteed log delivery
- Save money by consolidating different tool sets that are no longer needed

SIEM Cost Reduction

- Save significant money by using a purpose-built log solution
- Save even more by freeing up advanced admin resources and data custodians required to manage SIEM platforms

Log Management Made Simple

Our users see value in minutes rather than days or weeks.

Why observIQ

At observIQ, our mission is to build the best open source observability solutions for DevOps and ITOps.

Scalable Observability. Intelligent Control.

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