observIQ

PRODUCT 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. Many of the largest organizations in the world are struggling to collect and monitor massive volumes of log data across distributed systems. Smaller organizations are struggling with the complexity of the current solutions. From the exponential growth in log data resulting from an ever-expanding list of log sources, to the difficulty in achieving an acceptable time to value, log management is complicated and the tools 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 a 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 automatically installed for integrations 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, and get to a root cause far more quickly than other solutions.

observIQ Cloud also 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

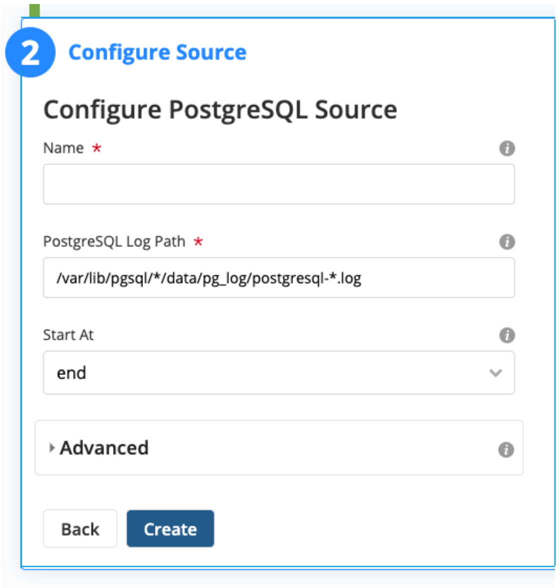
Simple To Set Up And Use

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 teams 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, combined with over 40 pre-built integrations and dashboards that are automatically installed, you can deploy end-to-end modern log management ***in minutes*** with observIQ Cloud.

Utilizing fully automated remote management capabilities, customers can save time by updating their entire fleet of agents with a single click.



2 Configure Source

Configure PostgreSQL Source

Name *

PostgreSQL Log Path *

/var/lib/pgsql/*/data/pg_log/postgresql-*.log

Start At

end

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

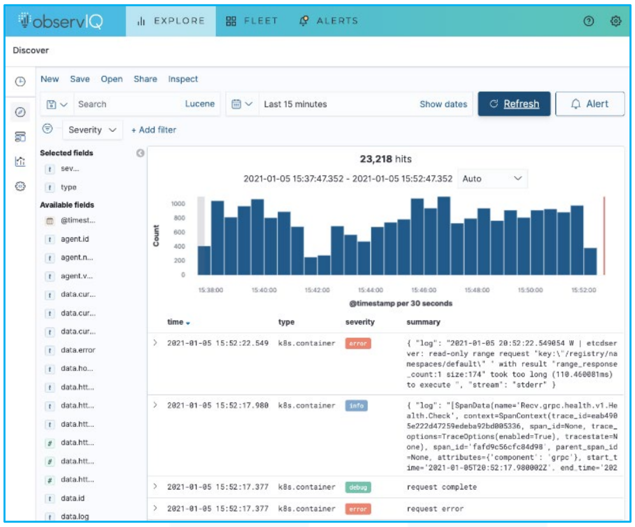
Reduced MTTR With Rapid Incident Investigation

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.

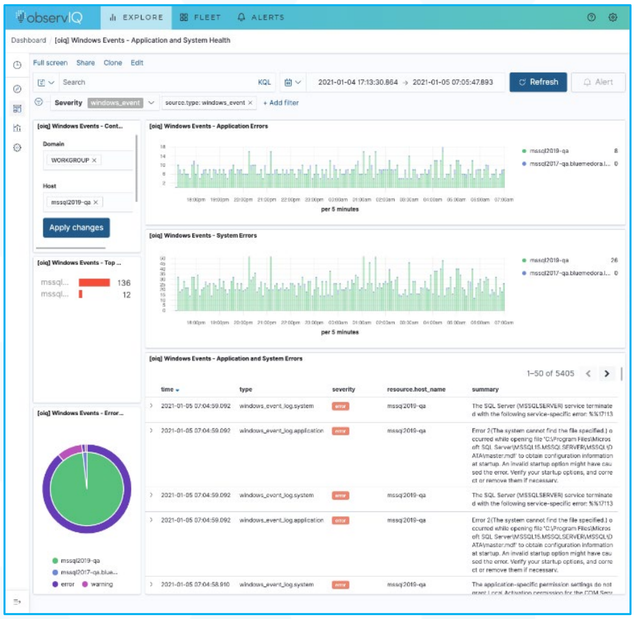
With observIQ Cloud, your logs are automatically parsed and enriched to provide the context needed to filter, search, visualize events with ease. Your logs can easily be tagged with custom labels as well, allowing you to specify data center, region or environment for complete traceability. With this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

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.



time	type	severity	summary
2021-01-05 15:52:22.549	k8s.container	error	{ "log": "2021-01-05 20:52:22.549054 W | etcdserver: read-only range request 'key:\"/registry/namespaces/default\" ' with result 'range_response_count:1 size:174' took too long (110.460081ms) to execute ", "stream": "stderr" }
2021-01-05 15:52:17.980	k8s.container	info	{ "log": "[SpanData(name='Recv.grpc.health.v1.Health.Check', context=SpanContext(trace_id=eab4905e222d47259edeba92bd005336, span_id=None, trace_options=TraceOptions(enabled=True), tracestate=None), span_id='fafd9c56cfc84d98', parent_span_id=None, attributes={'component': 'grpc'}, start_time='2021-01-05T20:52:17.980002Z', end_time='202
2021-01-05 15:52:17.377	k8s.container	debug	request complete
2021-01-05 15:52:17.377	k8s.container	error	request error



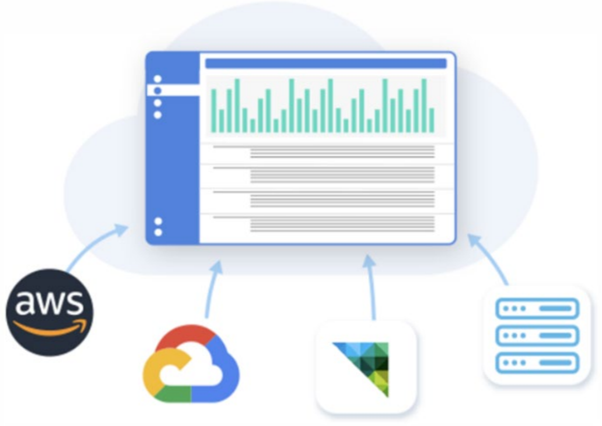
time	type	severity	resource.host_name	summary
2021-01-05 07:04:59.092	windows_event_log.system	error	mssql2019-qa	The SQL Server (MSSQLSERVER) service terminated with the following service-specific error: %%17113
2021-01-05 07:04:59.092	windows_event_log.application	error	mssql2019-qa	Error 2(The system cannot find the file specified.) occurred while opening file 'C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\master.mdf' to obtain configuration information at startup. An invalid startup option might have caused the error. Verify your startup options, and correct or remove them if necessary.
2021-01-05 07:04:59.092	windows_event_log.system	error	mssql2019-qa	The SQL Server (MSSQLSERVER) service terminated with the following service-specific error: %%17113
2021-01-05 07:04:59.092	windows_event_log.application	error	mssql2019-qa	Error 2(The system cannot find the file specified.) occurred while opening file 'C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\master.mdf' to obtain configuration information at startup. An invalid startup option might have caused the error. Verify your startup options, and correct or remove them if necessary.
2021-01-05 07:04:58.910	windows_event_log.system	error	mssql2019-qa	The application-specific permission settings do not grant Local Activation permission for the COM Serv

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 specialized capabilities, 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.



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. Others may be hesitant to make the investment in SIEM given the setup and total cost of ownership that traditionally have come along with these deployments. In reality, these security-focused incident and event management solutions aren't built for operational types of logs. Not only is the cost of using SIEM solutions 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 SIEM tools, but face difficult tradeoffs because their proprietary models lock customers in and makes it difficult to switch. 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, DevOps and ITOps professionals can move operational logs to a more cost effective, purpose-built log platform like observIQ Cloud.

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.

observIQ Cloud Business Value

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

Why observIQ

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

Scalable Observability. Intelligent Control.

observIQ

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