Coralogix

LOG MANAGEMENT & ANALYTICS

Generate Infinite Intelligence From Your Log Data

Centralize and analyze your logs without relying on indexing, and take full advantage of the wealth of information in your data with real-time alerting and monitoring that scales with your systems.

Integrate Using Open Source Agents & Shippers

- Ingest data from any source, in any format.
- Transform and enrich your data on the fly.
- Use any syntax, dashboard, and webhook endpoint to realize the full value of your data.
- Avoid vendor lock-in, streamline setup & improve user adoption.

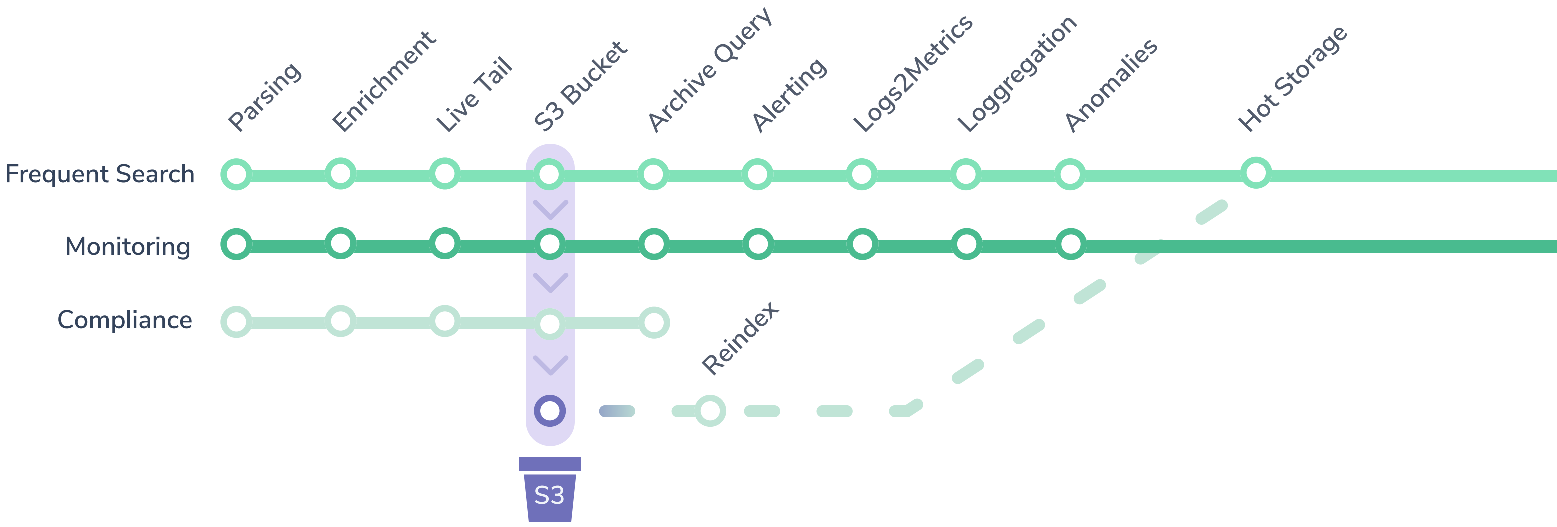
Transform & Enrich Your Data On the Fly

- Define parsing rules to easily transform your data and extract meaningful insights.
- Structure unstructured logs, mask or block fields, and more.
- Enrich your data with geo-location, IP reputation fields, or custom enrichment parameters.

Advanced TCO Optimization & Direct Archive Query

Leverage the proactive analytics of Streama© to route data to three different pipelines according to use case for advanced cost optimization. Data that is frequently searched can be selectively indexed for lightening-fast queries, while the rest can monitored for infinite insights and archived for compliance without ever being indexed.

All alerting, metric generation, and data clustering features can be leveraged on monitoring data for full coverage without any tradeoffs. Data written to your remote storage can be queried directly from the Coralogix platform at any time with no effect on daily quota or added compute costs.



Parsing
Enrichment
Live Tail
S3 Bucket
Archive Query
Alerting
Logs2Metrics
Loggregation
Anomalies
Hot Storage
Frequent Search
Monitoring
Compliance
Reindex
S3

Unlock More Value From Your Data

Our next-generation Streama© architecture is built — and priced — to help you extract infinite insights and make sense of ever-growing data as you scale.

Loggregation

Automatically cluster millions of individual logs into templates. With Loggregation, your log data is deduplicated for high-level analytics and streamlined investigation.

Logs2Metrics

Convert your log data into trackable metrics on the fly. Using the Logs2Metrics functionality, you can visualize these metrics with 12-month retention without indexing the raw log data.

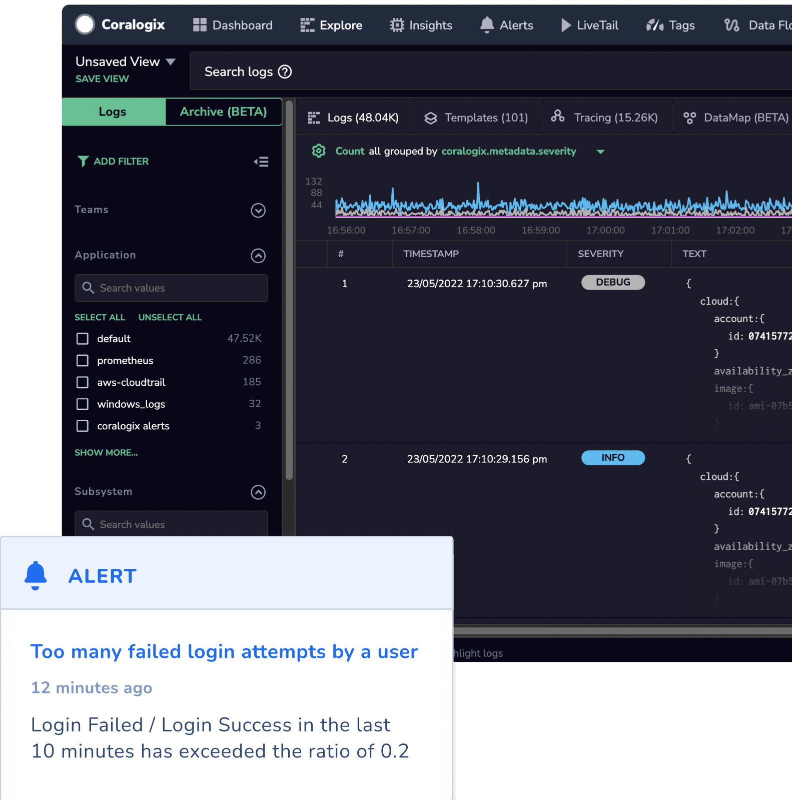
> *“We create metrics from our event data, and then we don’t need to index it. We archive the raw events and still see everything in real-time, and we can always query them later directly from the console.”*
>
> **Roi Amitay** - Head of DevOps

ARMIS

Anomaly Detection & Dynamic Alerting

With systems that generate massive amounts of logs every minute, you can’t rely on static thresholds to detect critical errors. Automatically detect unusual behavior, and use dynamic alerting to stay on top of critical events.

1. Error volume spike & flow anomalies
2. Dynamic alerting without reliance on static thresholds
3. New value, ratio between queries, time relative alerts & more



#	TIMESTAMP	SEVERITY	TEXT

1	23/05/2022 17:10:30.627 pm	DEBUG	{
			cloud:{
			account:{
			id: 07415772
			}
			availability_z
			image:{
			id: ami-07b5
			}

2	23/05/2022 17:10:29.156 pm	INFO	{
			cloud:{
			account:{
			id: 07415772
			}
			availability_z
			image:{
			id: ami-07b5
			}

ALERT

Too many failed login attempts by a user

12 minutes ago

Login Failed / Login Success in the last 10 minutes has exceeded the ratio of 0.2