SERVERLESS OBSERVABILITY: A CASE STUDY OF SLOs

DIANA TODEA - SRE

MONITORAMA JUNE 11th 2024

DIANA TODEA - OBSERVABILITY SRE

https://www.linkedin.com/in/diana-todea-b2a79968

https://github.com/didiViking/Conferences_Talks

UNSPLASH Juan Puyo

elastic

CONTEXT

- Transition to serverless
- Pro-active insights across multiple CSP, multiple regions
- Federated search queries across all the configured remote clusters (CCS)
- Focus on efficient aggregations with better cache results

SLA
Service Level Agreement

Promise

User Agreement when breached can cause loss/penalty

Sales & Users

SLO
Service Level Objective

Goal

Service provider goal to defend SLA and achieve happy users

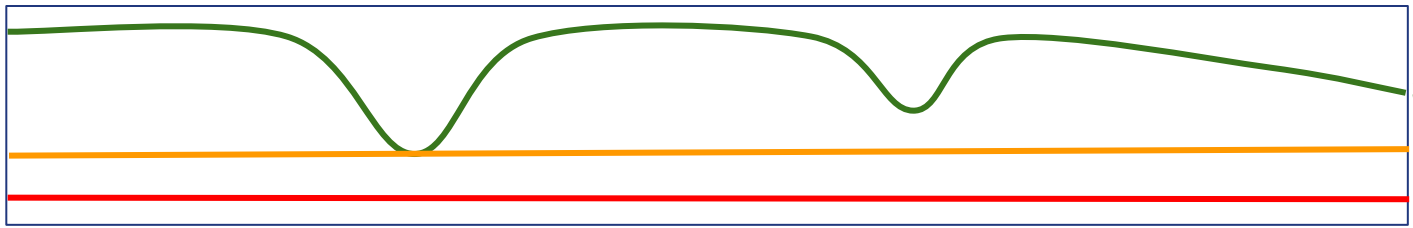
SREs & Product

SLI
Service Level Indicator

Measurement

Metric used to measure performance

Devs & SREs



elastic

BURN RATE

The rate at which we are burning the error budget over a defined period of time.
Very useful for alerting before exhausting the error budget.

ERROR BUDGET

Defined as 100% minus the SLO.
Quantity of errors that is tolerated.

Source: Google SRE Book

deprecated

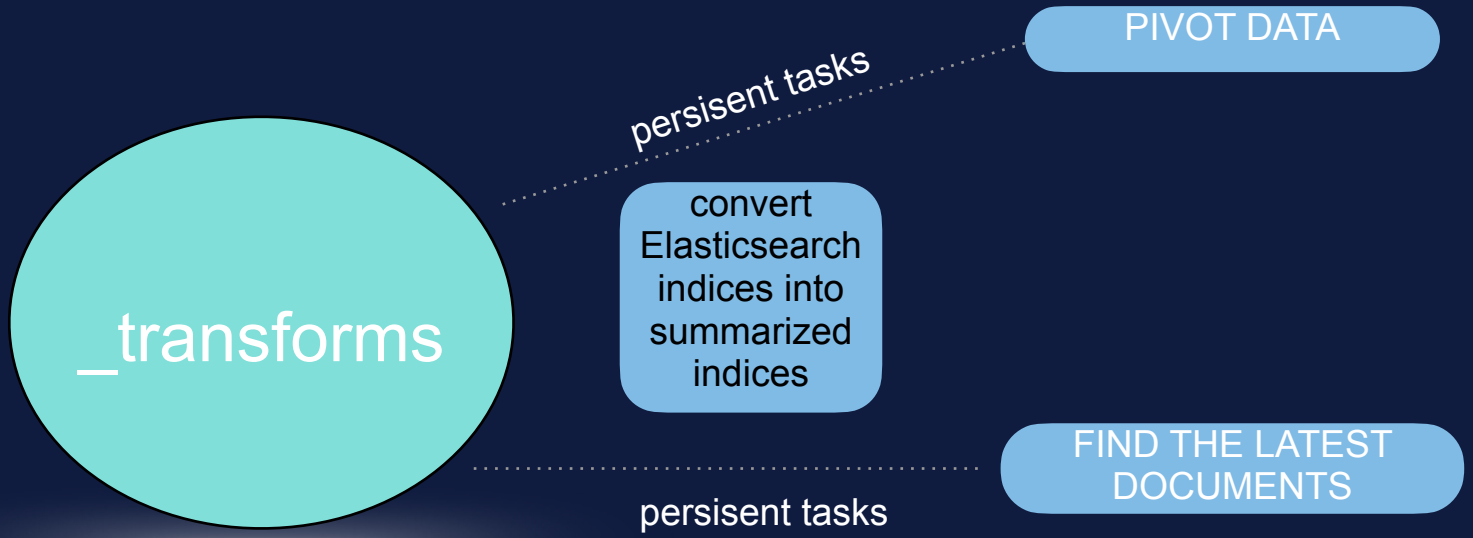
ROLLUP HISTORICAL DATA

Unsplash@stenslens

Unsplash@markuswinkler

TRANSFORMS

elastic


_transforms
persisent tasks
PIVOT DATA
convert Elasticsearch indices into summarized indices
persisent tasks
FIND THE LATEST DOCUMENTS

WHEN YOU WANT TO CREATE **SUMMARY TABLES** TO OPTIMIZE QUERIES.

WHEN YOU NEED A COMPLETE **FEATURE INDEX** RATHER THAN A TOP-N SET OF ITEMS.

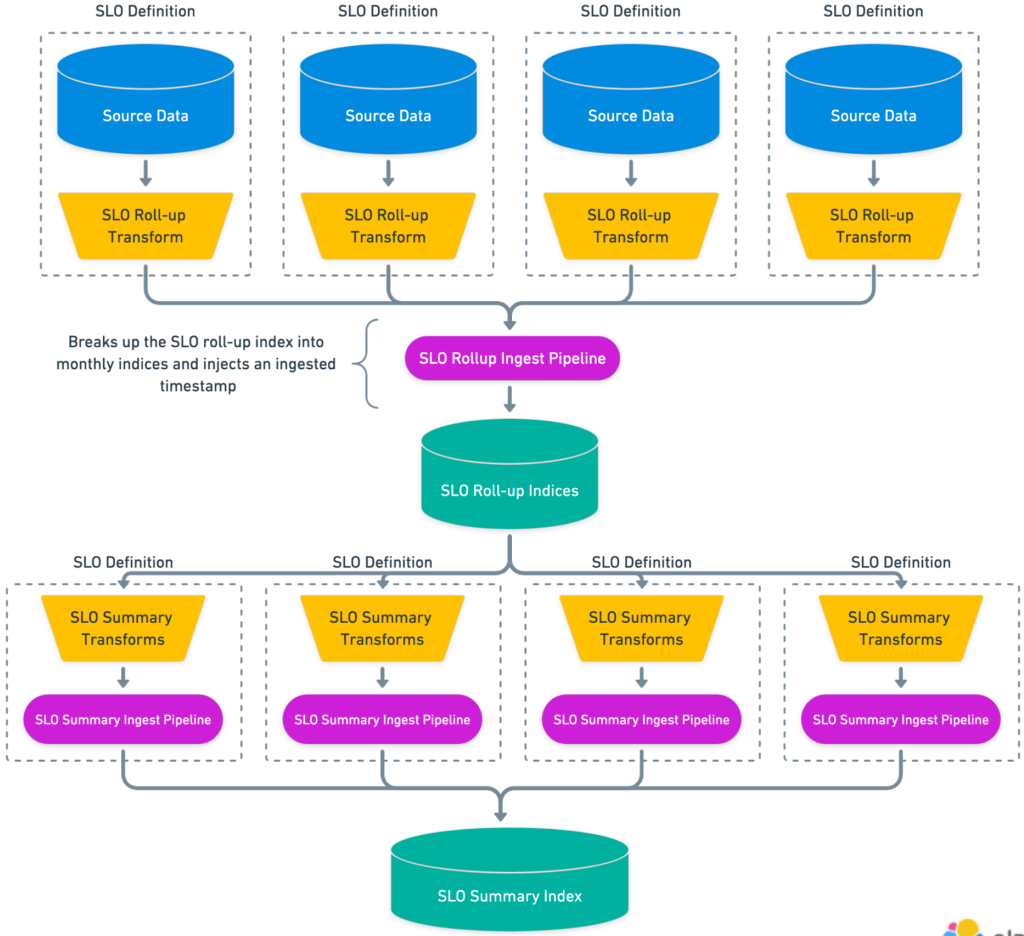
WHEN YOU NEED TO SORT AGRREGATION RESULTS BY A **PIPELINE AGGREGATION**.

elastic

SLO Architecture

SLOs relies on the Transform service to roll-up the source data into roll-up indices.

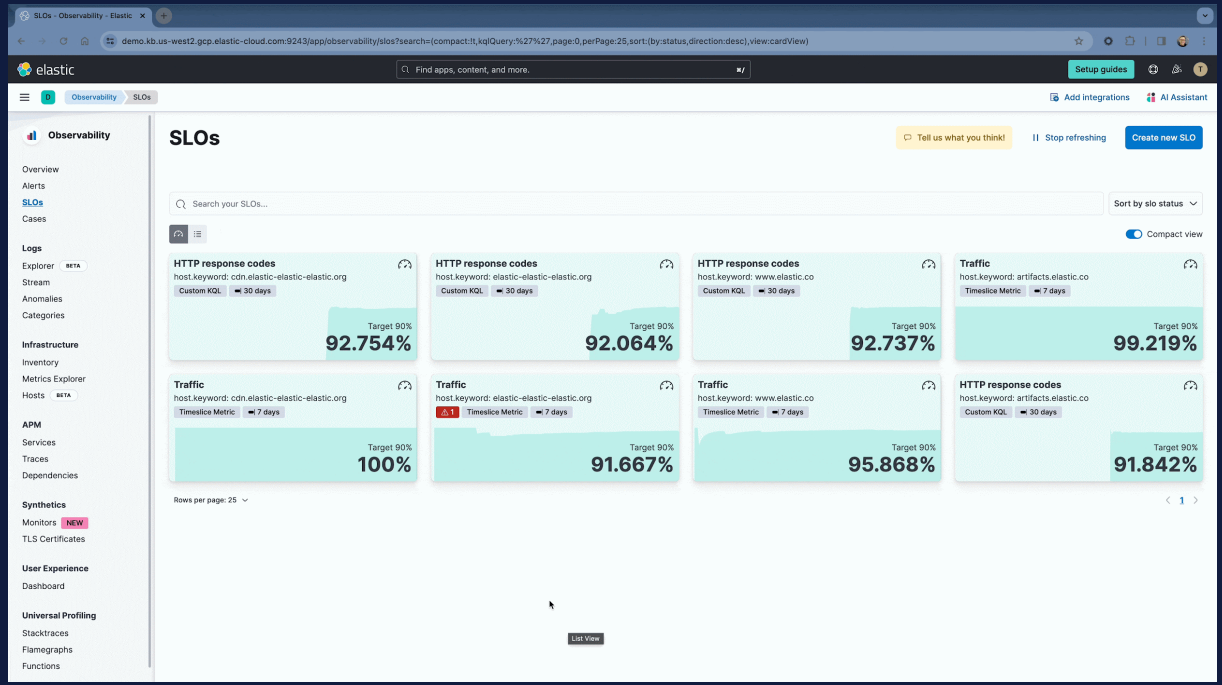
The SLO service rolls up your data to a single document every minute and then computes a summary document based on the SLO definition and these roll up documents. By using an intermediary layer and not relying on the raw data, we can compute the SLO data faster with less storage.



elastic

SLO Overview for Observability

- Proactive and strategic approach to monitor and maintain Service Level Objectives (SLOs).
- Focused on the SRE use cases.
- Provides baseline metrics and highlight how changes affect those measurements.
- Acts as a communication layer with common language to align across teams and business goals.



elastic

Unsplash@carsonmasterson

VS.

Unsplash@miteneva

elastic

Four Golden Signals of Observability

Latency

Is my service fast enough?

Traffic

Is my service available?

Error Rate

Is my service accurate?

Saturation

Is my service at capacity?

elastic

Service Level Indicator types

APM Latency & Availability

Custom Metrics

Histogram

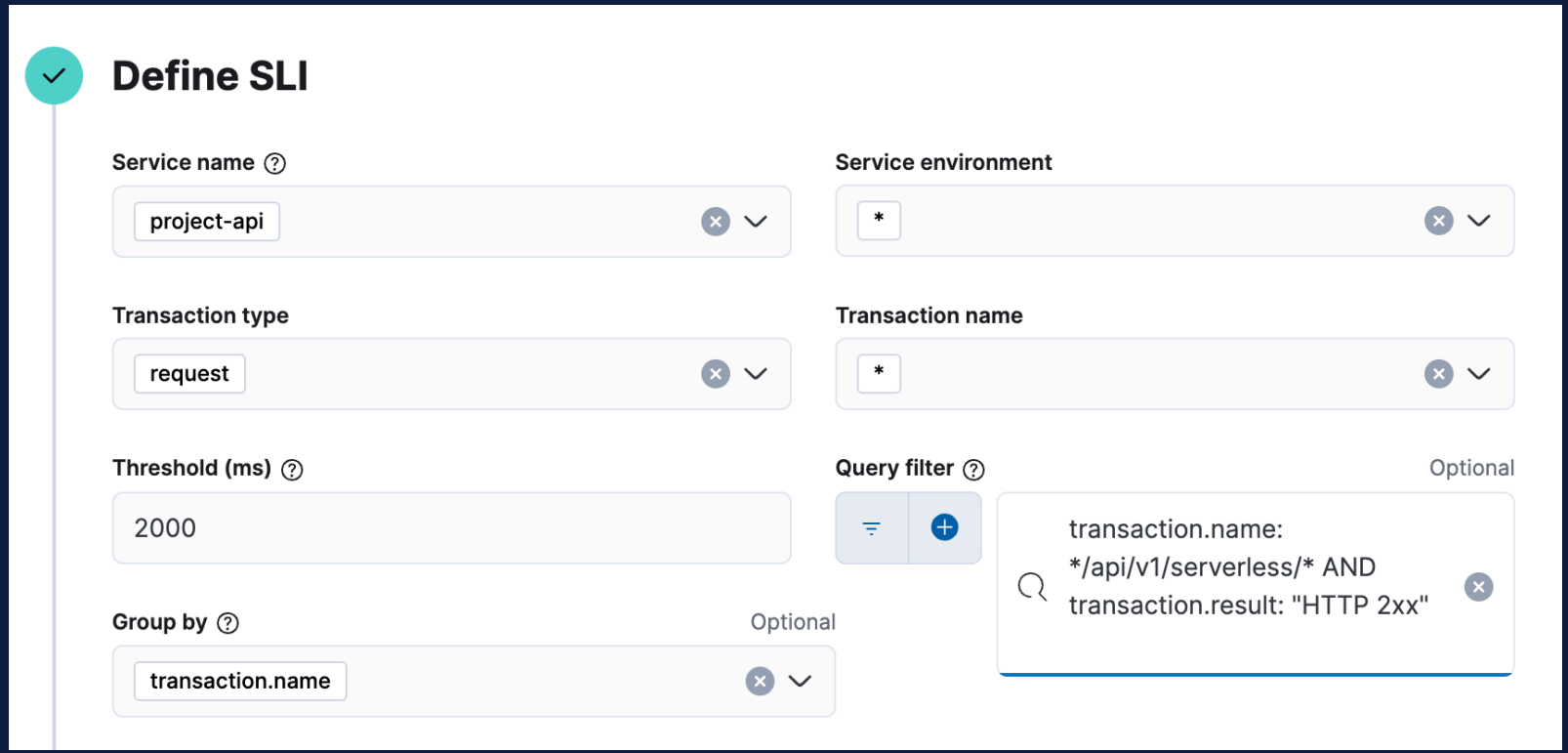
Synthetics

Custom Query

Time Slice Metrics

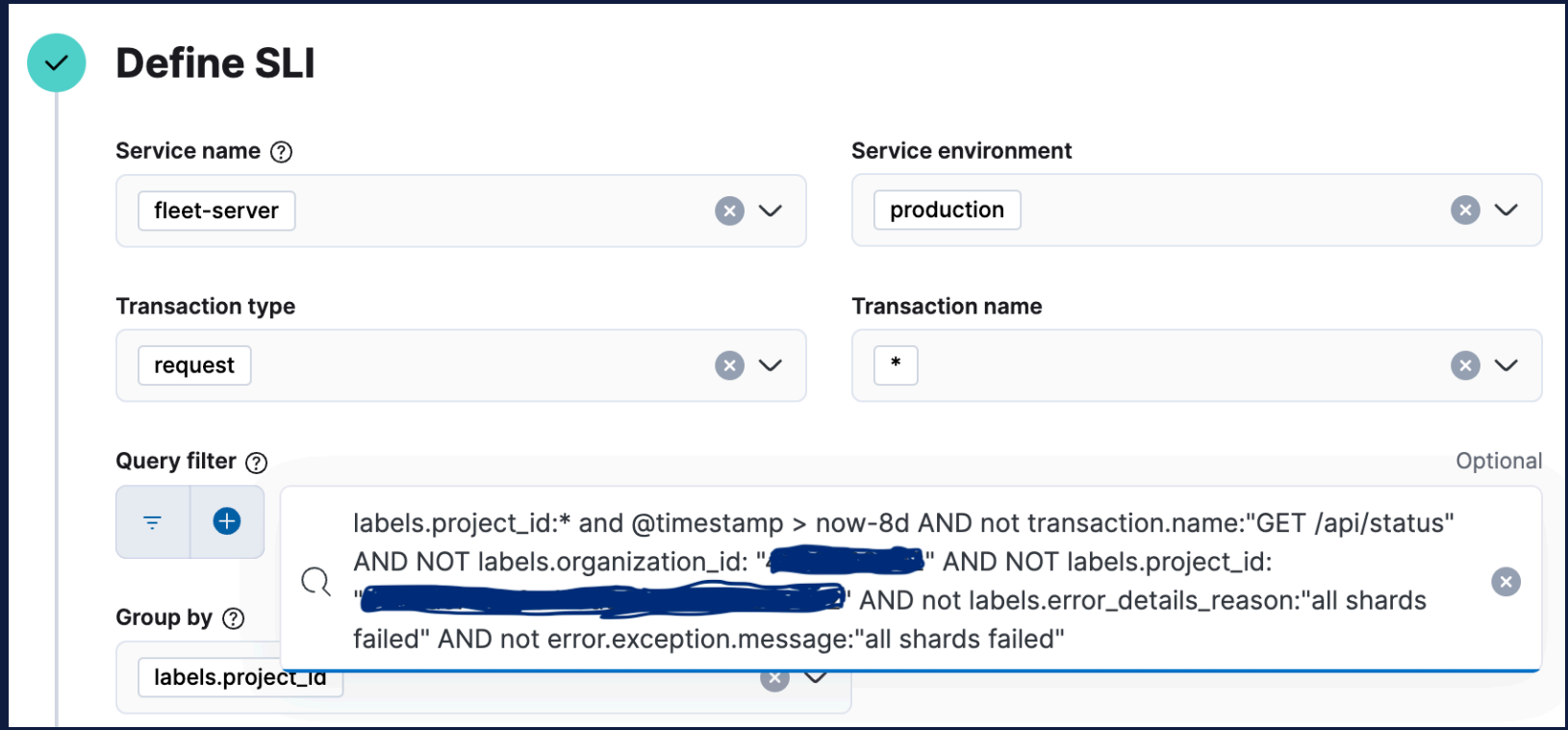
elastic

APM LATENCY SLI

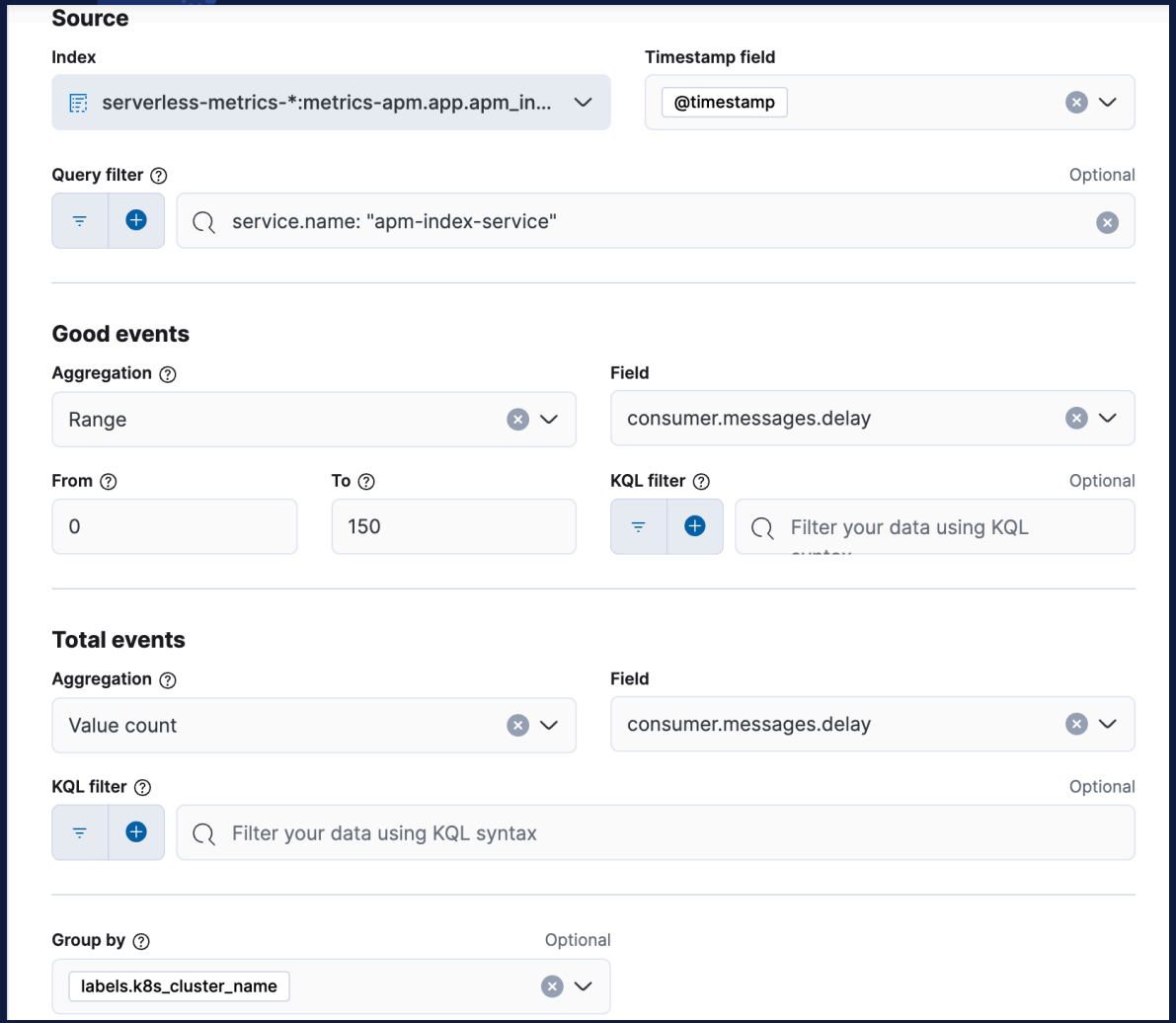


elastic

APM AVAILABILITY SLI

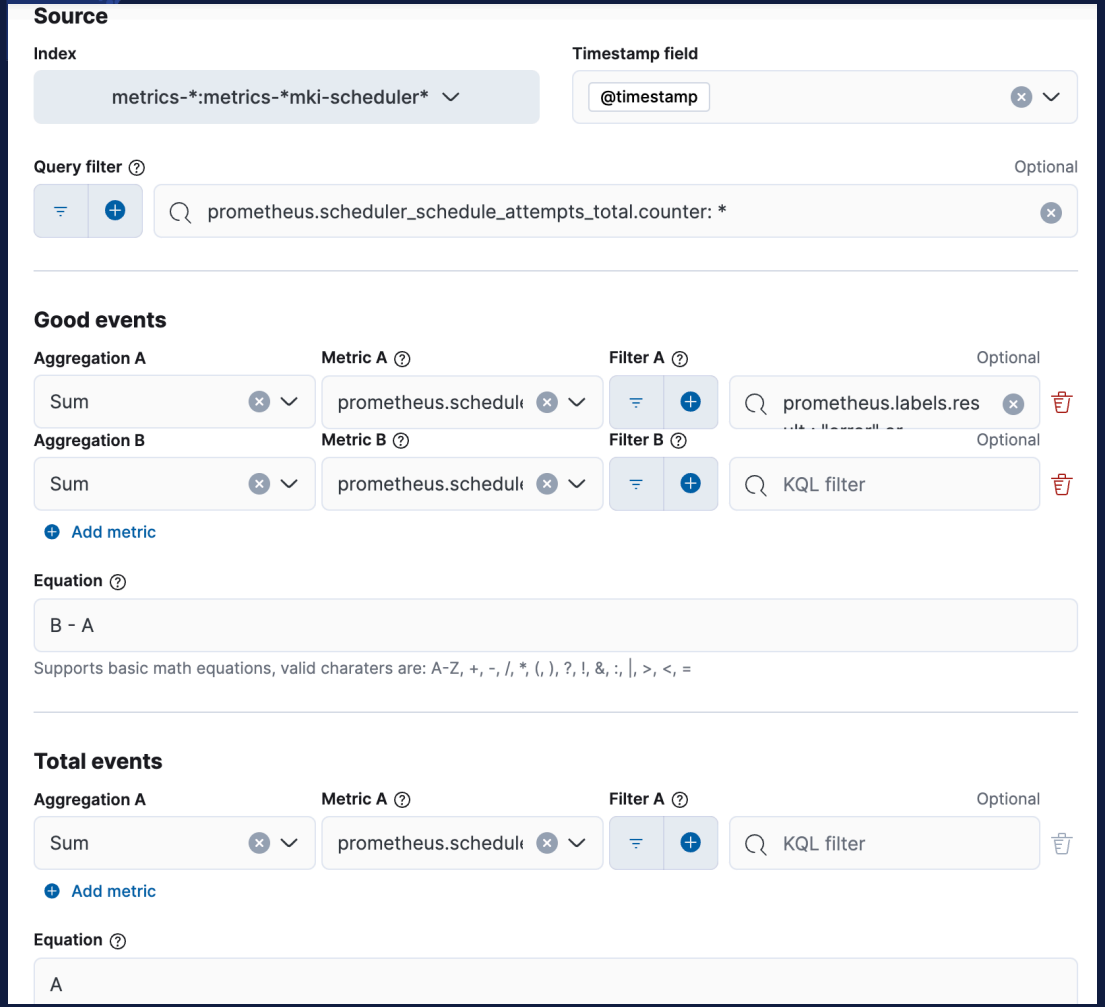


elastic



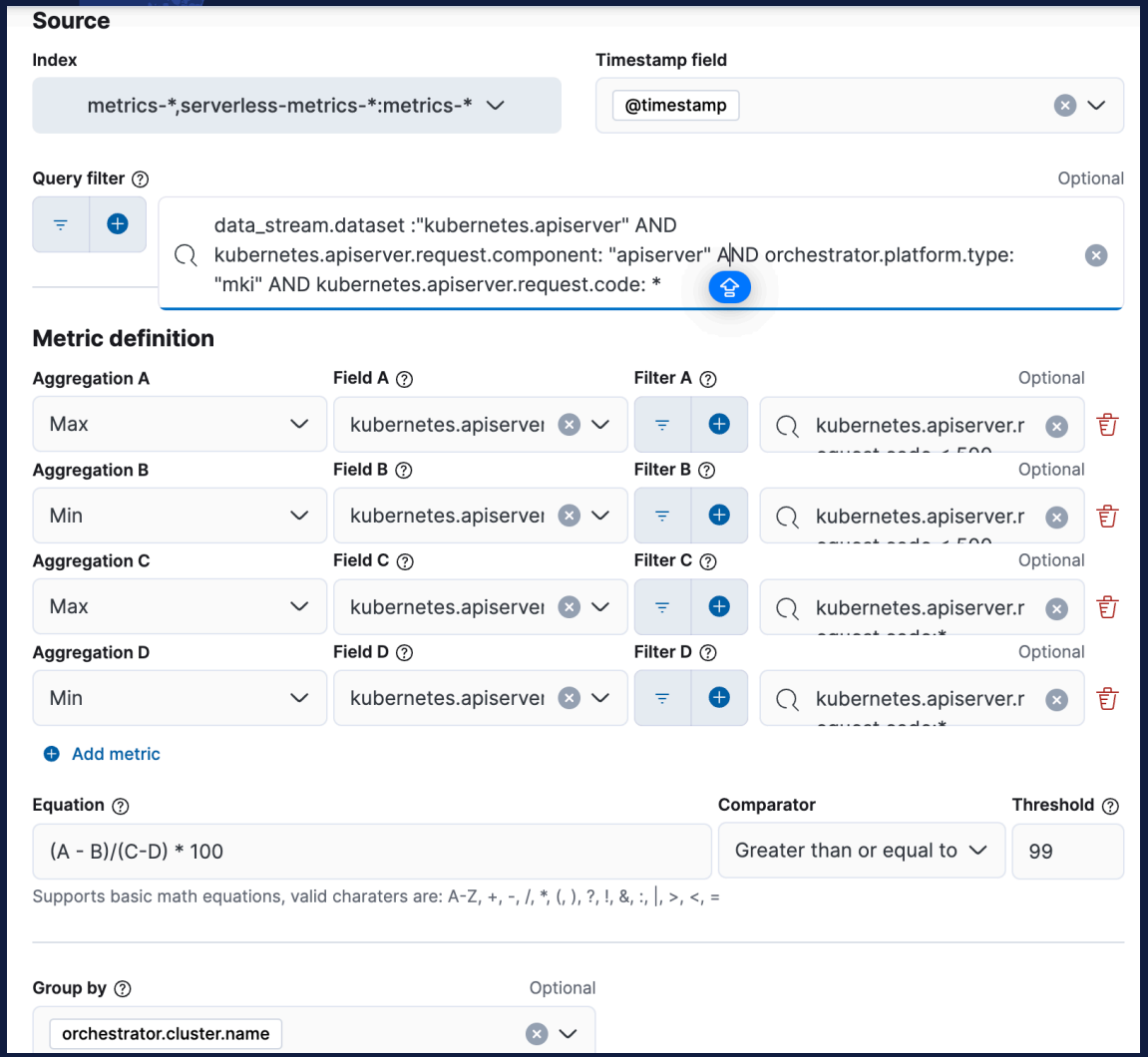
HISTOGRAM METRIC SLI

elastic



CUSTOM METRIC SLI

elastic

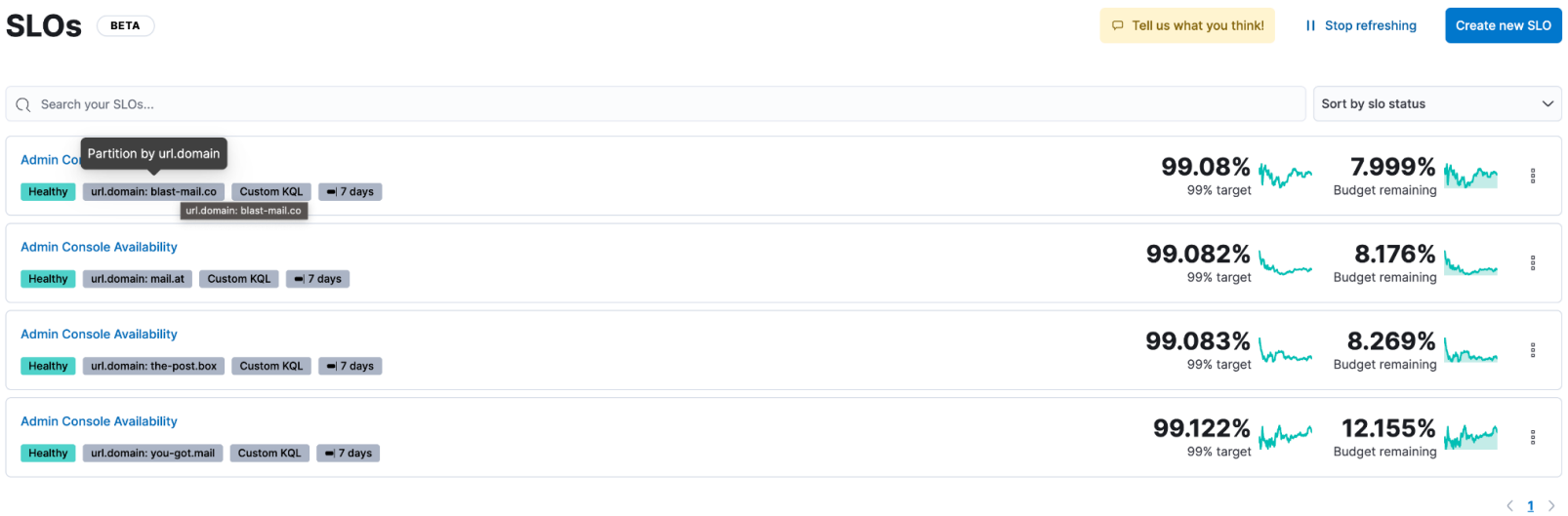


TIMESLICE METRIC SLI

elastic

Grouping SLOs by a field

With SLOs, you can choose a field to group the data by. This will create multiple SLOs using a single definition. The number of SLOs created will depend on the cardinality of the field used for the group by.



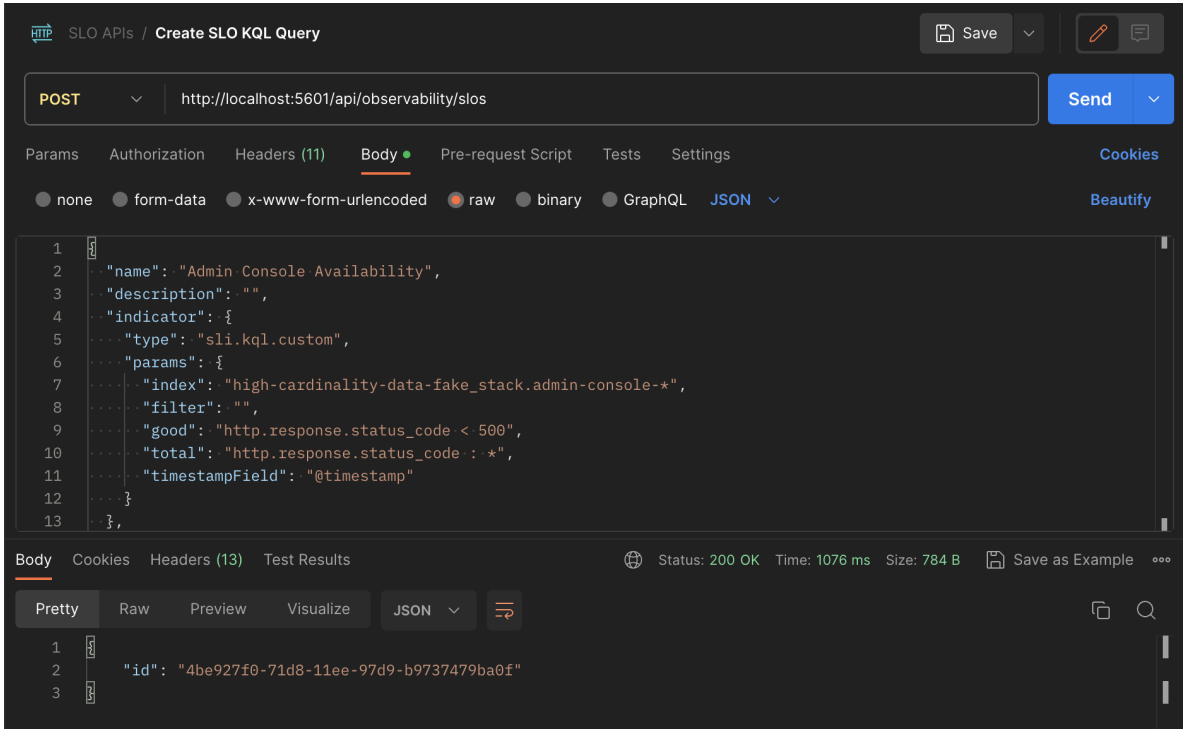
elastic

SLO API is a First Class Citizen

We built the API first, inspired by OpenSLO standard

We provide OpenAPI documentation to enable developers.

```
GET /_transforms/_all
GET /s/{spaceId}/api/observability/slos/{sloId}
```



BURN RATE ALERTING

calculates the rate at which SLOs are failing over multiple windows of time.

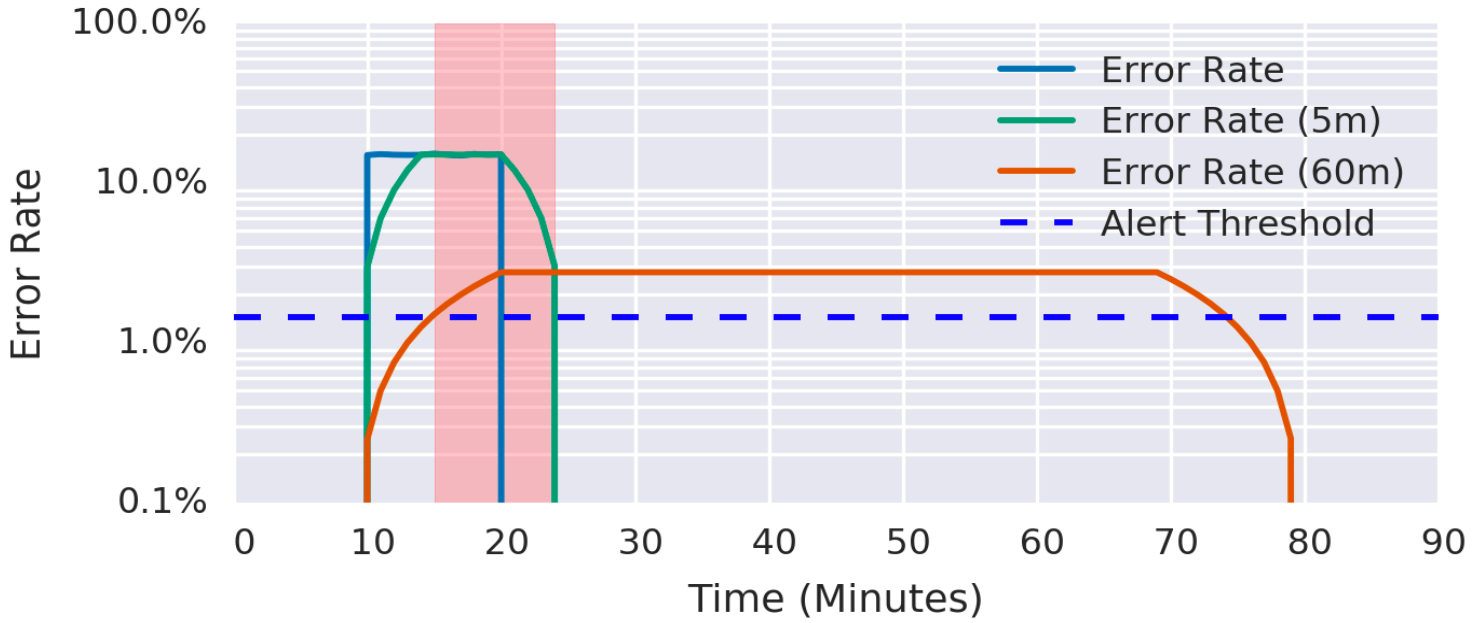
is less sensitive to short term fluctuations by focusing on **sustained deviations**.

gives an indication of how severly the service is **degrading** and it helps **prioritize** multiple issues at the same time.

elastic

Burn rate alerting with multiple windows

For each severity, there are two windows, a short and long; the short window is 1/12 the long window. When the burn rate for both windows exceeds the threshold, the alert is triggered.



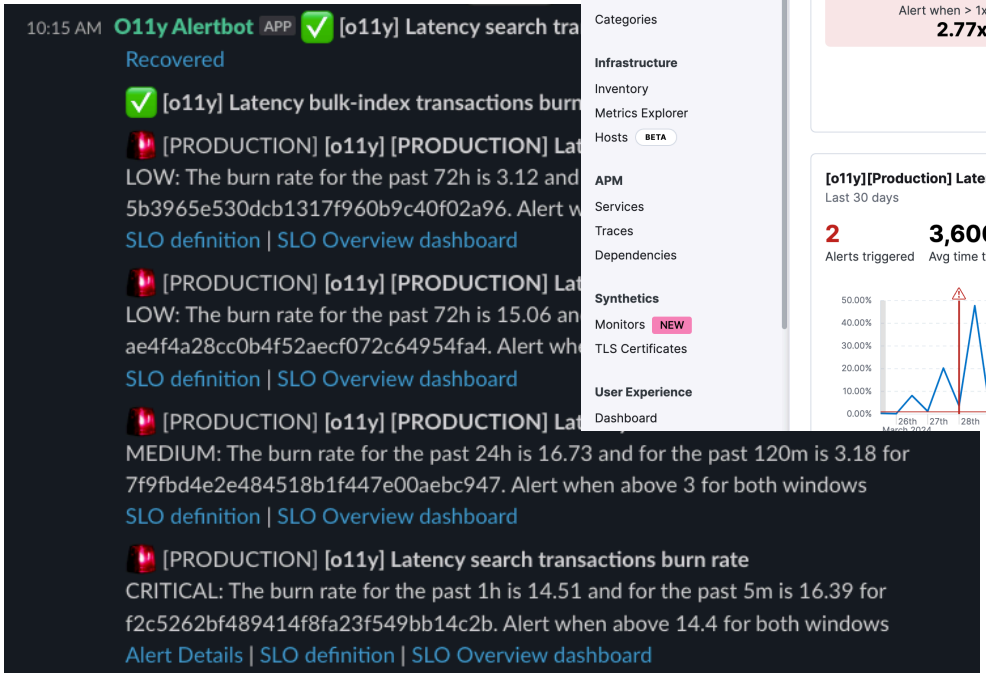
elastic

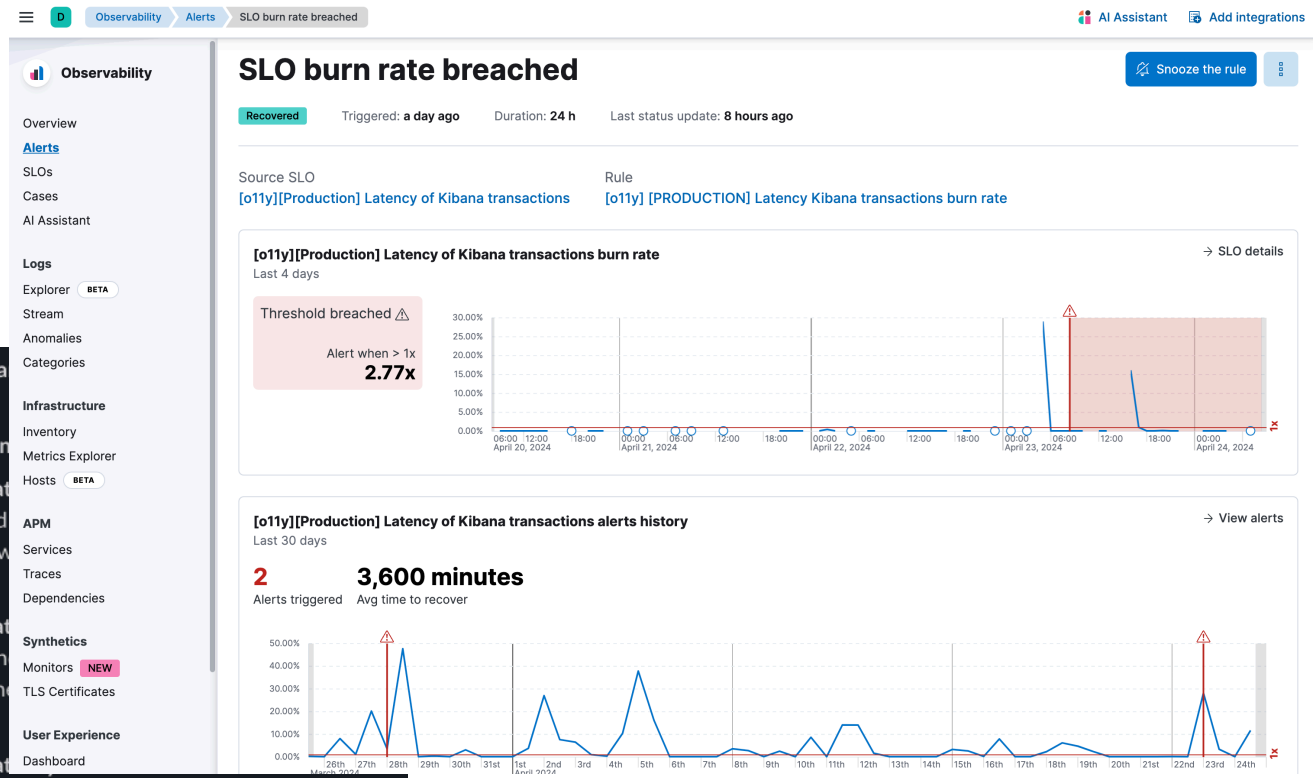
Multi-window, multi-burn rates

You can define multiple sets of windows depending on your notification strategy and how quickly you need to respond to defend the SLO.

Severity	Windows	Burn Rate	Budget consumed before alert
Critical	5m & 1h	14.4x	2%
High	30m & 6h	6x	5%
Medium	2h & 24h	3x	10%
Low	6h & 3d	1x	10%

Based on a 30 day SLO with a 99% target


10:15 AM O11y Alertbot APP [o11y] Latency search tra
Recovered
[o11y] Latency bulk-index transactions burn
[PRODUCTION] [o11y] [PRODUCTION] Lat
LOW: The burn rate for the past 72h is 3.12 and
5b3965e530dcb1317f960b9c40f02a96. Alert w
SLO definition | SLO Overview dashboard
[PRODUCTION] [o11y] [PRODUCTION] Lat
LOW: The burn rate for the past 72h is 15.06 an
ae4f4a28cc0b4f52aecf072c64954fa4. Alert wh
SLO definition | SLO Overview dashboard
[PRODUCTION] [o11y] [PRODUCTION] Lat
MEDIUM: The burn rate for the past 24h is 16.73 and for the past 120m is 3.18 for
7f9fbd4e2e484518b1f447e00aebc947. Alert when above 3 for both windows
SLO definition | SLO Overview dashboard
[PRODUCTION] [o11y] Latency search transactions burn rate
CRITICAL: The burn rate for the past 1h is 14.51 and for the past 5m is 16.39 for
f2c5262bf489414f8fa23f549bb14c2b. Alert when above 14.4 for both windows
Alert Details | SLO definition | SLO Overview dashboard


D
Observability
Alerts
SLO burn rate breached
AI Assistant
Add integrations
Observability
Overview
Alerts
SLOs
Cases
AI Assistant
Logs
Explorer BETA
Stream
Anomalies
Categories
Infrastructure
Inventory
Metrics Explorer
Hosts BETA
APM
Services
Traces
Dependencies
Synthetics
Monitors NEW
TLS Certificates
User Experience
Dashboard
SLO burn rate breached
Snooze the rule
Recovered
Triggered: a day ago
Duration: 24 h
Last status update: 8 hours ago
Source SLO
[o11y][Production] Latency of Kibana transactions
Rule
[o11y] [PRODUCTION] Latency Kibana transactions burn rate
[o11y][Production] Latency of Kibana transactions burn rate
Last 4 days
SLO details
Threshold breached
Alert when > 1x
2.77x
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
April 20, 2024
April 21, 2024
April 22, 2024
April 23, 2024
April 24, 2024
1x
[o11y][Production] Latency of Kibana transactions alerts history
Last 30 days
View alerts
2
Alerts triggered
3,600 minutes
Avg time to recover
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
1x

DEMO

elastic

Management

Ingest
Ingest Pipelines
Logstash Pipelines

Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Cross-Cluster Replication
Remote Clusters

Alerts and Insights
Rules
Cases
Connectors
Reporting
Machine Learning
Watcher
Maintenance Windows

Security
Users
Roles
API keys
Role Mappings

Kibana

Transforms

Transform docs

Use transforms to pivot existing Elasticsearch indices into summarized entity-centric indices or to create an indexed view of the latest documents for fast access.

Total transforms: **155** Batch: **0** Continuous: **155** Failed: **3** Started: **143** Nodes: **6**

Search...

Status | Mode | Health | Reload | Create a transform

ID	Description	Type	Status	Mode	Progress	Health	Actions
endpoint.metadata_current-default-8.11.1 Managed	Latest Endpoint metadata document per host	latest	started	continuous		Healthy	
endpoint.metadata_current-default-8.6.1 Managed	Latest Endpoint metadata document per host	latest	started	continuous		Healthy	
endpoint.metadata_current-default-8.8.0 Managed	Latest Endpoint metadata document per host	latest	started	continuous		Healthy	
endpoint.metadata_united-default-8.11.1 Managed	Merges latest Endpoint and Agent metadata documents	pivot	started	continuous		Healthy	
endpoint.metadata_united-default-8.6.1 Managed	Merges latest Endpoint and Agent metadata documents	pivot	failed	continuous		Unavailable	
endpoint.metadata_united-default-8.8.0 Managed	Merges latest Endpoint and Agent metadata documents	pivot	failed	continuous		Unavailable	
slo-210dcca0-8f67-11ee-a205-47d75dde5ded-4 Manag	Rolled-up SLI data for SLO: [EA] 99% of the Artifactory GET requests should be completed in under 500ms within a 30d period	pivot	started	continuous		Healthy	
slo-323a9b60-8f63-11ee-8cd7-23f418d34c67-4 Manag	Rolled-up SLI data for SLO: [EA] 99% of the Container Library GET requests should be completed in under 20s within a 30d period	pivot	started	continuous		Healthy	
slo-36964160-92a5-11ee-950c-15c94e977f88-1 Mana	Rolled-up SLI data for SLO: [Copy] [Serverless] Kibana UI Node Uptime	pivot	started	continuous		Healthy	

Scalable, Flexible, and deployable for the SRE use case

SLOs Scaled for Large Enterprise

- Large Enterprise
- 100K+ of Services
- 100K+ users using those services
- 100s of users of SLO UIs
- Multi-clusters using CCS

Multiple SLO user roles

SREs, DevOps, and developers have unique perspective and focus, but share common deployment, notifications and troubleshooting.

o11y Integrations

Logs/Discover, Dashboards, Kibana Alerting, APM

API first & Config as Code

JSON & Terraform configuration settings

elastic

RESOURCES

1. https://www.elastic.co/guide/en/observability/current/slo.html
2. https://www.elastic.co/guide/en/observability/current/slo-create.html
3. https://www.elastic.co/guide/en/elasticsearch/reference/current/transforms.html
4. https://www.elastic.co/guide/en/elasticsearch/reference/current/transform-apis.html
5. https://docs.elastic.co/api-reference/observability/findslosop
6. https://www.elastic.co/guide/en/elasticsearch/reference/current/transform-scale.html
7. https://www.elastic.co/guide/en/elasticsearch/reference/current/transform-examples.html
8. https://www.elastic.co/guide/en/observability/current/slo-burn-rate-alert.html
9. https://www.elastic.co/guide/en/observability/current/observability-introduction.html
10. https://openapi.tools/

elastic

QUESTIONS?

THANK YOU!

elastic