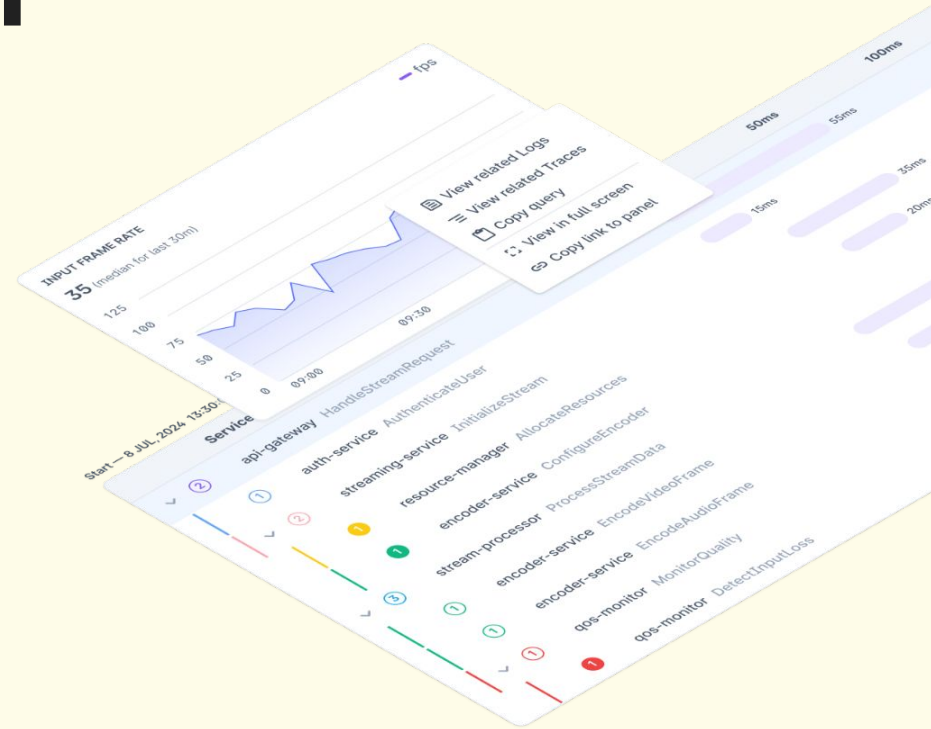
Last9

OpenTelemetry with ClickHouse

Battle tested lessons from Last9



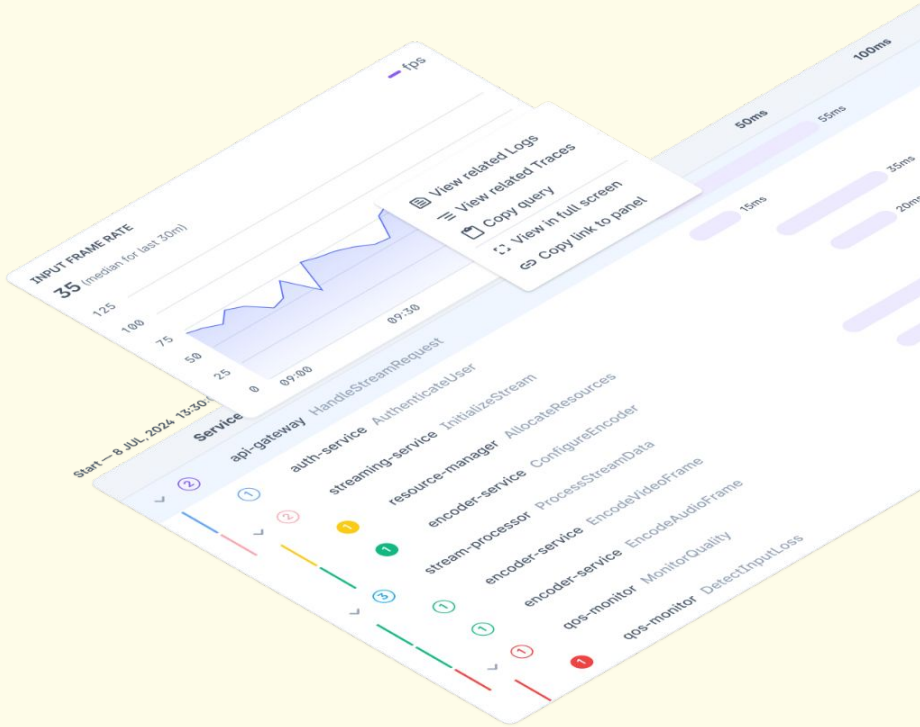
Prathamesh Sonpatki
Developer Evangelist, Last9

Last9

Less War, More Room

Confessions of a Reformed Alert Hoarder

Prathamesh Sonpatki
Developer Evangelist, Last9



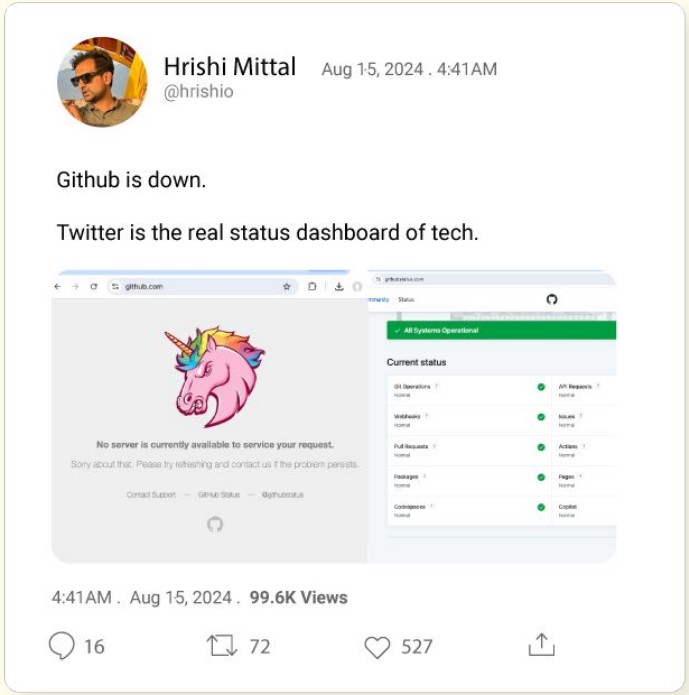
>_ ~/prathamesh

```ruby
# who_am_i.rb

def initialize
@loves = ['Cricket', 'Books', 'Programming', 'Stickers']
@claims_to_fame = ['Top-30 Rails Contributor',
'Developer Evangelist @Last9']
@writes_at = 'srestories.dev'
@tweets_at = '@prathamesh2'
end

def current_status
'Building observability tools while collecting stickers'
end
```

3AM War Room Bingo



3:00 AM — It's probably just a blip. Noisy alert!

Let's wait 5 minutes to see if it self-resolves

3:10 AM — What changed?

Restart all the things

3:20 AM — Does anyone have access to that machine?

`grep -r "error" /var/log/* | less`

3:30 AM — Users are still seeing errors

5 people on the war room by now

Patal Log!

Log Everything

Helps future you debug at 3 AM.

- → Structured, consistent logging across services
- → High-cardinality data that adds context
- → Events that tell a story about system behavior

Log Anything

Future you curses past you at 3 AM.

- → Random console.log("here") sprinkled like confetti
- → Unstructured text that's a pain to parse
- → Non-thoughtful severity levels.

Observability in an ideal world

- → Structured data
- → Best tool for the job
- → Instrumentation changes on demand
- → Find correlated information easily
- → High fidelity data without worrying about performance and cost

OpenTelemetry

- → OpenTelemetry is gaining wild attention and adoption is 🚀.
- → Brings standardization.
- → Vendor neutrality.
- → Signal correlation.
- → Support for more languages and SDKs for Otel metrics.
- → Native support for OpenTelemetry Metrics in Prometheus.

ClickHouse

- One of the best performance / $
- Fast in the absolute sense
- Engines and data modelling for logs metrics traces and events
- SQL access

ClickHouse + OpenTelemetry

- Out of the box exporter https://github.com/open-telemetry/opentelemetry-collector-contrib/tree/main/exporter/clickhouseexporter
- Default schema for logs metrics traces
- Engines for logs metrics traces
- Grafana data source for ClickHouse
- Read/Write isolation
- Make sure your batch sizes are high*

```
clickhouse/logs:
  endpoint: ${logs_endpoint}
  ttl_days: 14
  logs_table_name: ${logs_table_name}
  timeout: 50s
  database: ${logs_database_name}
  username: ${logs_writer_username}
  password: "${logs_writer_password}"
  retry_on_failure:
    enabled: true
    initial_interval: 5s
    max_interval: 30s
    max_elapsed_time: 300s
```

On the ground challenges

- → Lack of Structured Data
- → Data Silos
- → Service specific needs
- → Alert thresholds
- → Too much data, far less insights
- → Too much noise
- → Legacy code

Last9

Observability for rest of us..

What do we need?

What we have today?

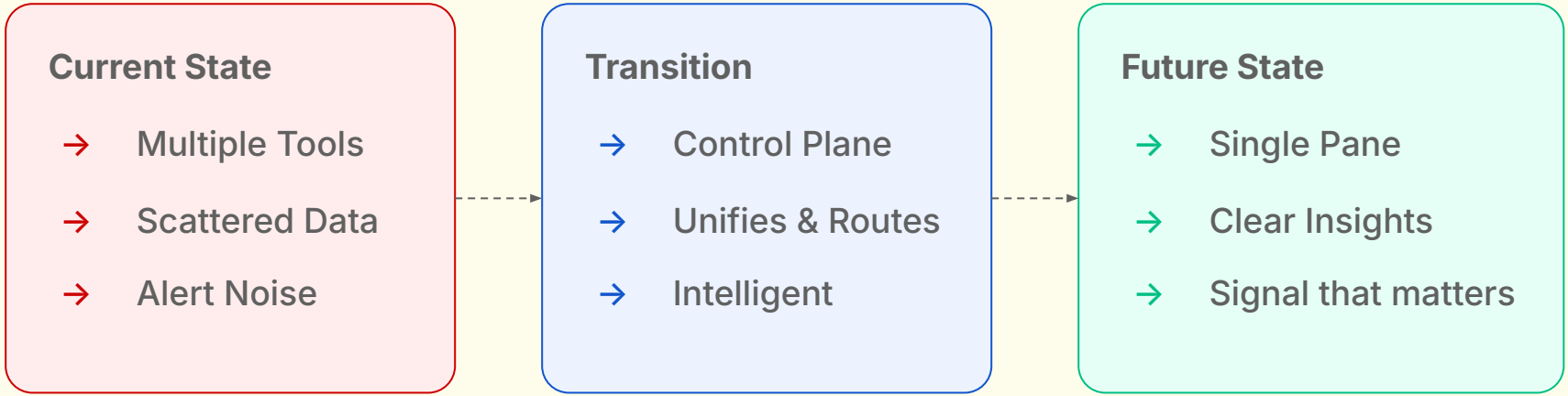
- → Multiple dashboards
- → Scattered telemetry data
- → Configuration sprawl
- → Alert fatigue
- → Constant Instrumentation changes

What we need?

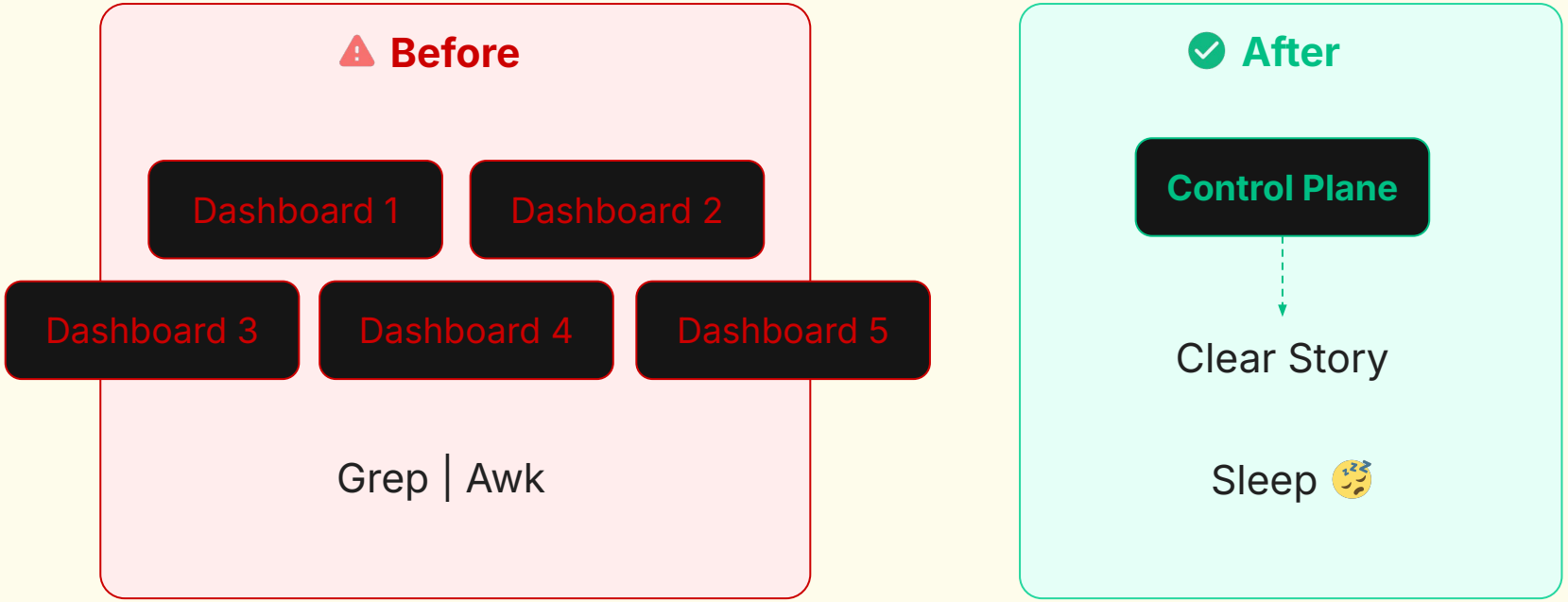
- → Single source of truth
- → Unified telemetry
- → Centralized control
- → Signal vs Noise

Observability for Rest of us..

Migration Path:



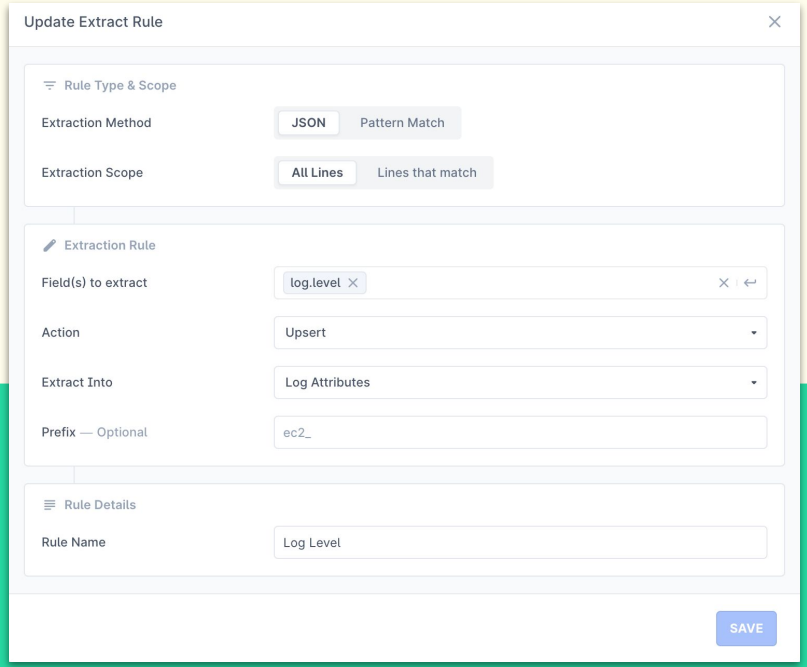
Observability for Rest of us..

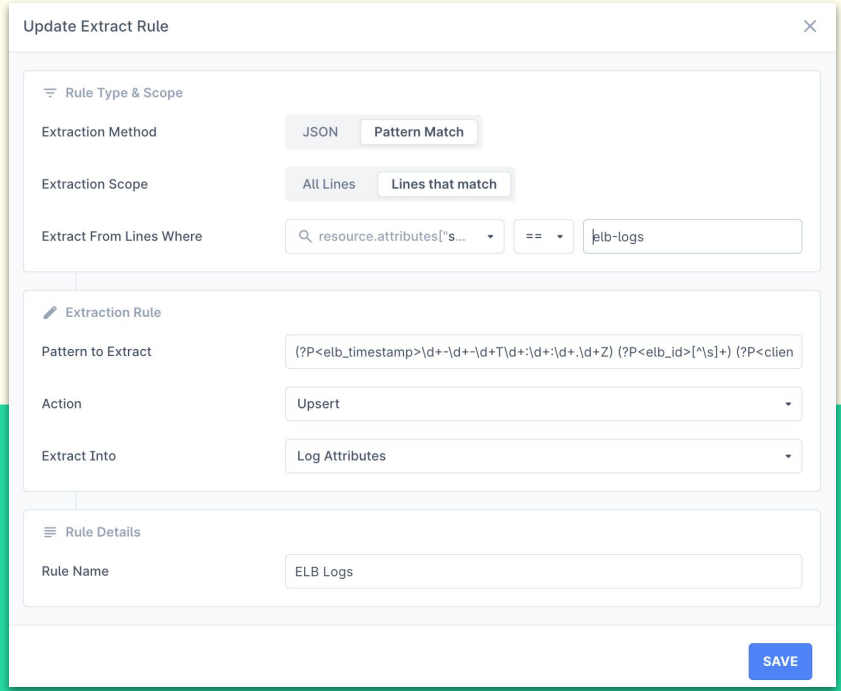


Last9

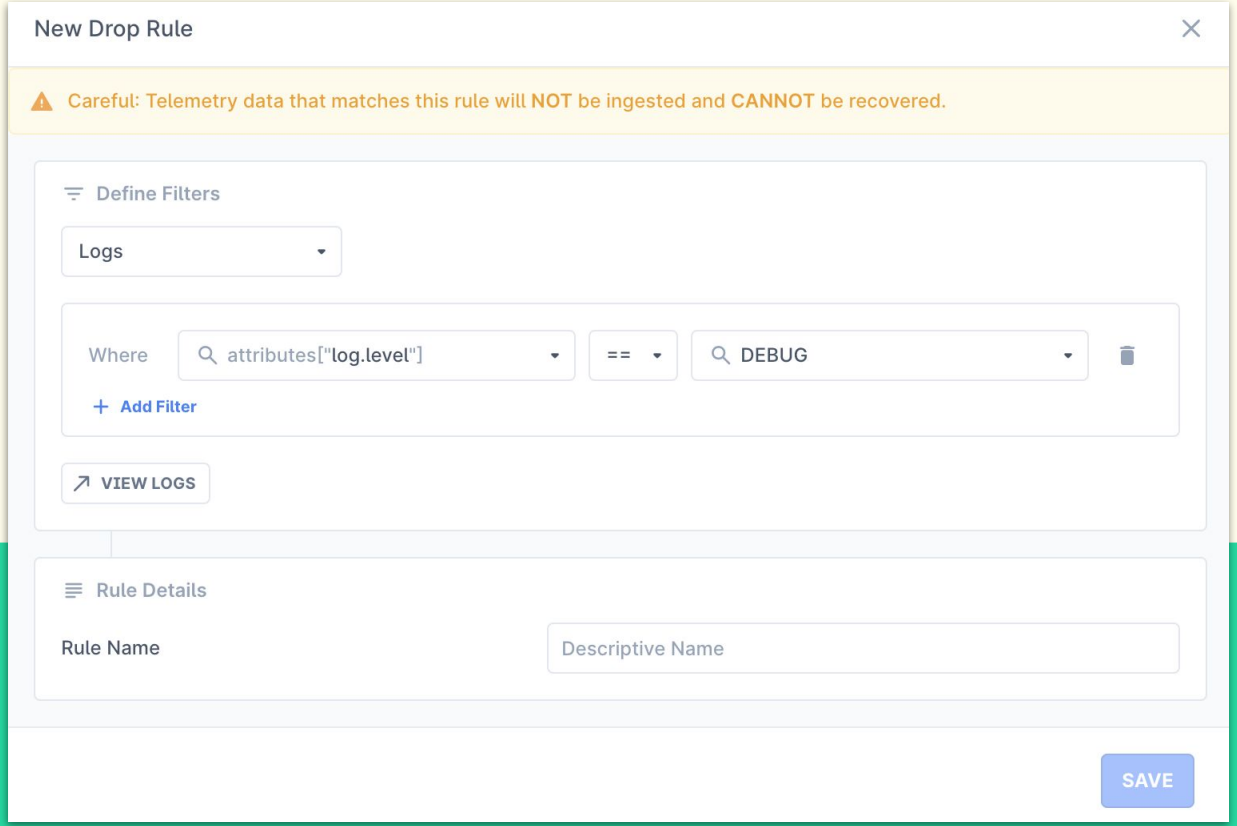
Control Plane

Extract / Remap

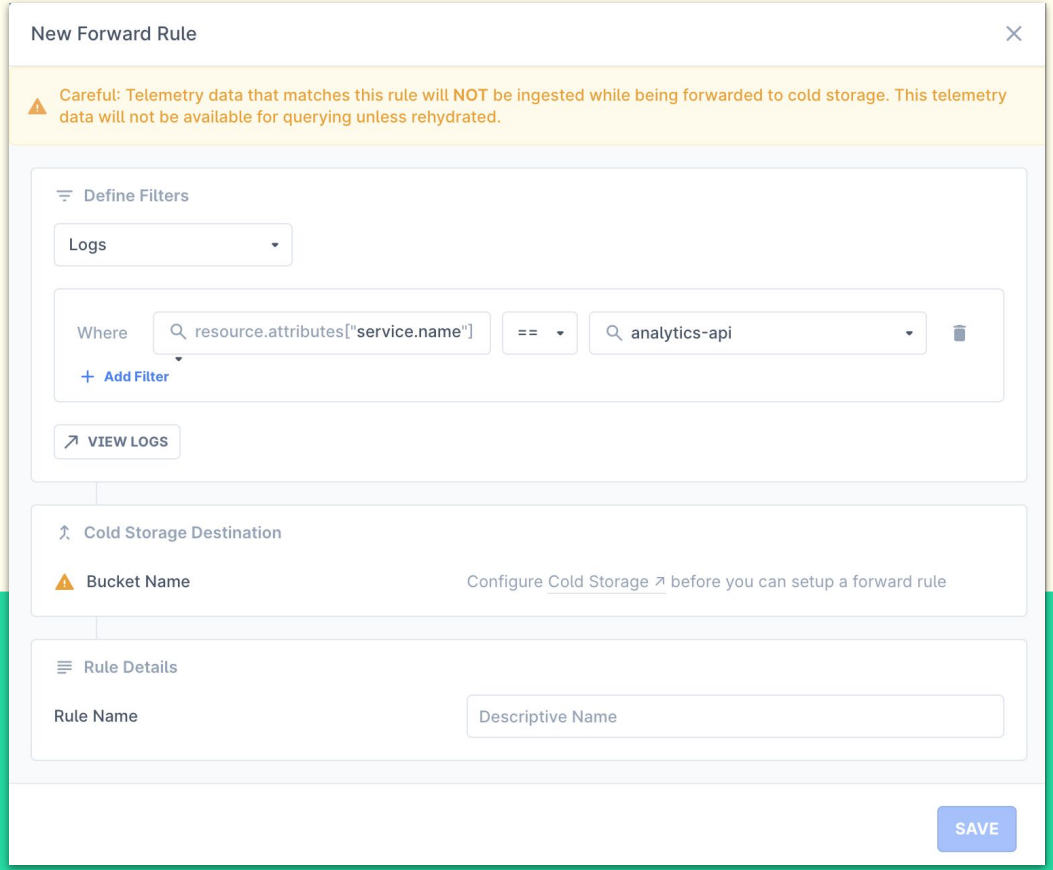




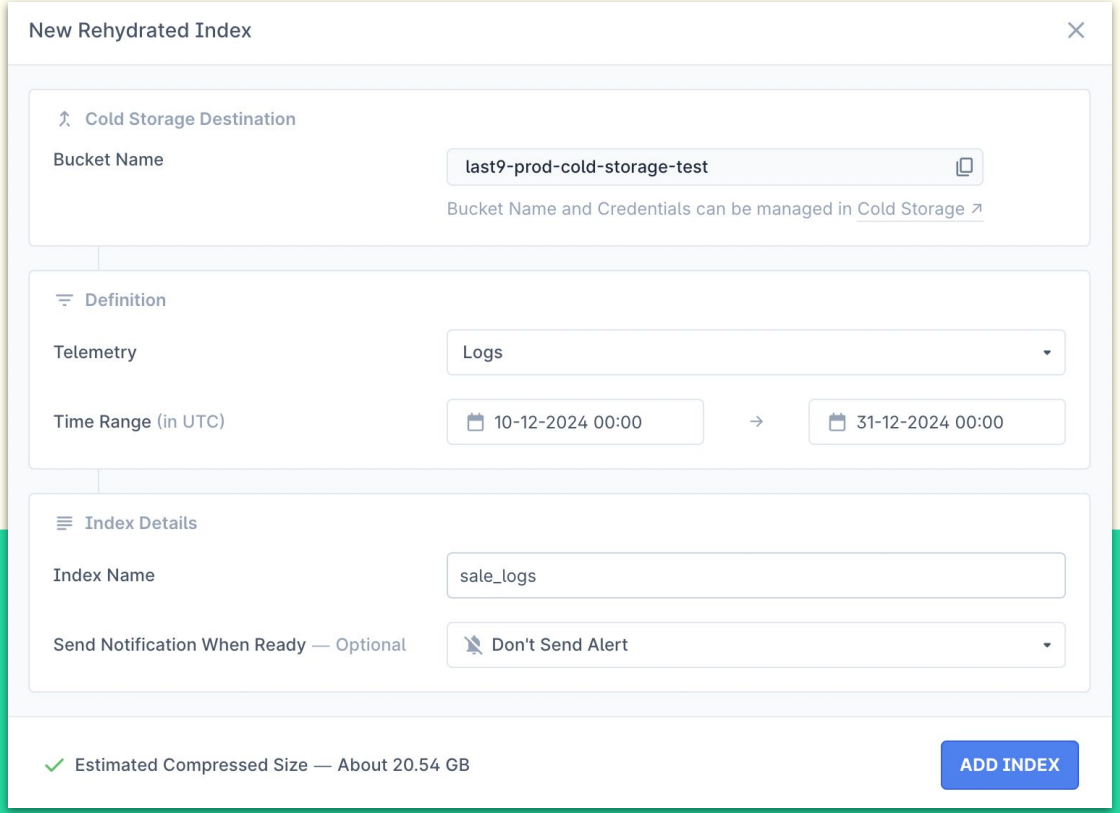
Drop


New Drop Rule
Careful: Telemetry data that matches this rule will NOT be ingested and CANNOT be recovered.
Define Filters
Logs
Where
attributes["log.level"]
==
DEBUG
Add Filter
VIEW LOGS
Rule Details
Rule Name
Descriptive Name
SAVE

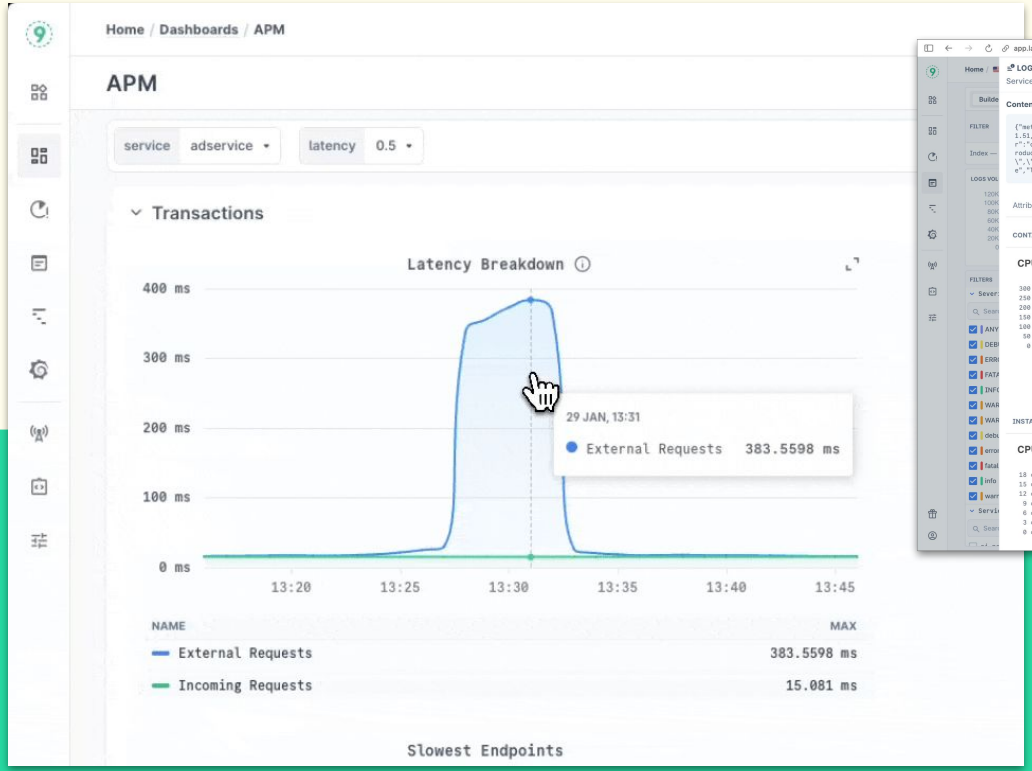
Forward

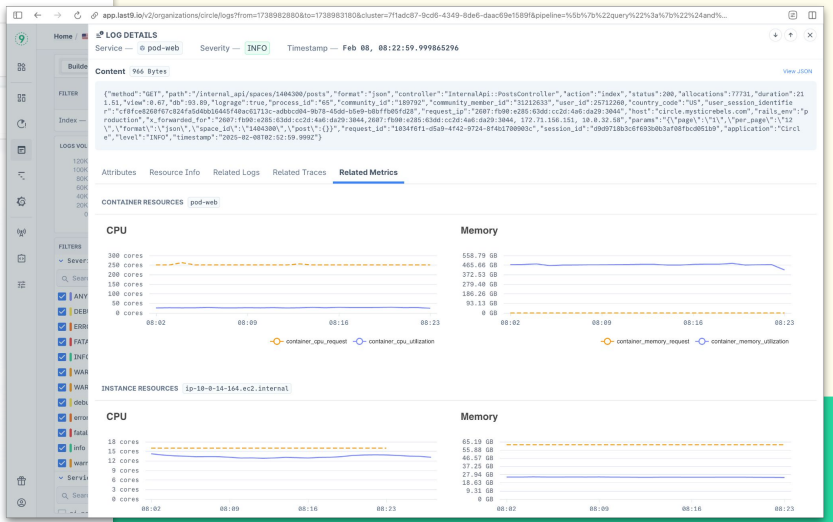

New Forward Rule
Careful: Telemetry data that matches this rule will NOT be ingested while being forwarded to cold storage. This telemetry data will not be available for querying unless rehydrated.
Define Filters
Logs
Where
resource.attributes["service.name"]
==
analytics-api
Add Filter
VIEW LOGS
Cold Storage Destination
Bucket Name
Configure Cold Storage ↗ before you can setup a forward rule
Rule Details
Rule Name
Descriptive Name
SAVE

Rehydrate

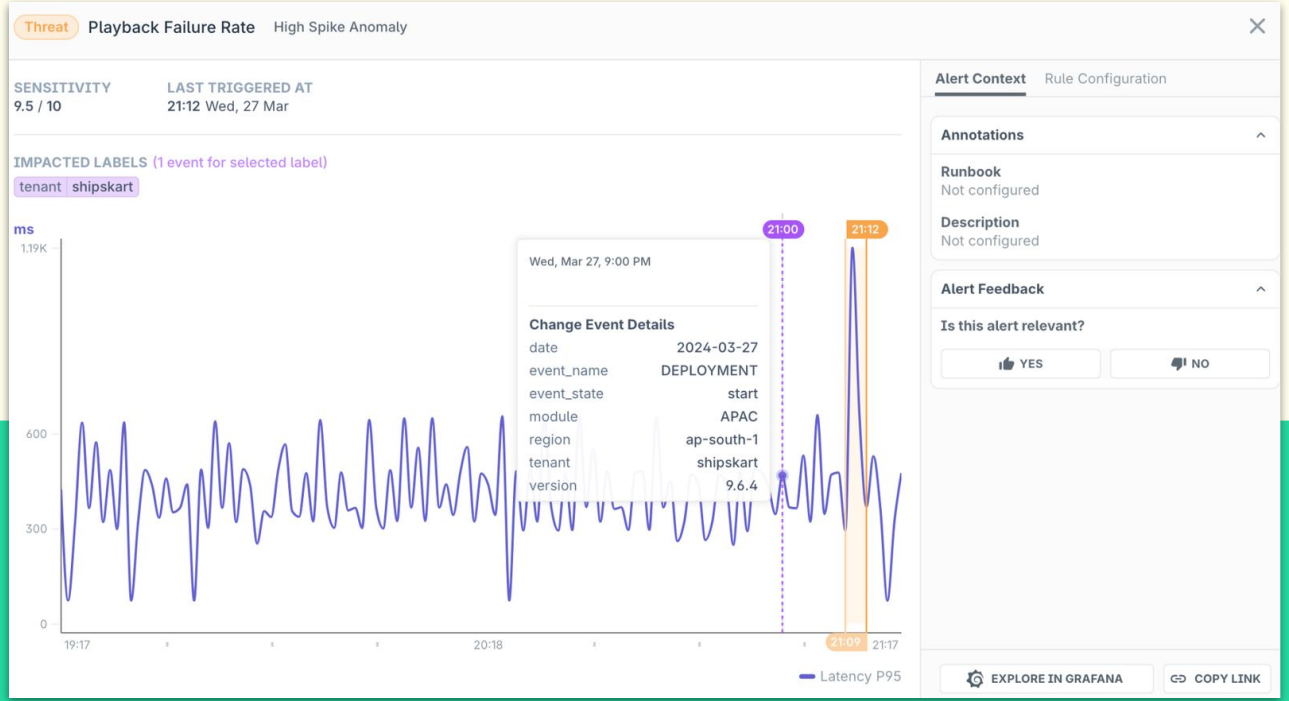

New Rehydrated Index
Cold Storage Destination
Bucket Name
last9-prod-cold-storage-test
Bucket Name and Credentials can be managed in Cold Storage
Definition
Telemetry
Logs
Time Range (in UTC)
10-12-2024 00:00
31-12-2024 00:00
Index Details
Index Name
sale_logs
Send Notification When Ready — Optional
Don't Send Alert
Estimated Compressed Size — About 20.54 GB
ADD INDEX

Single Pane of Glass





What Changed



Flexibility

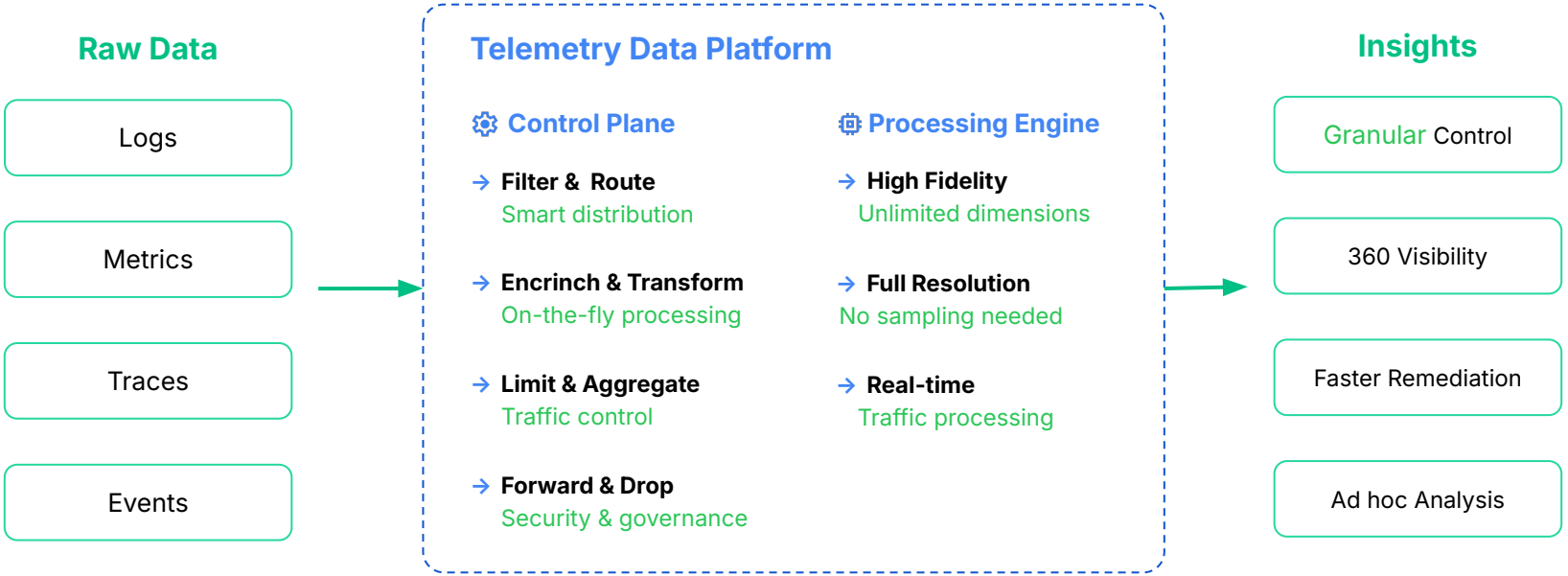
- Grafana
- Native UI
- LogQL
- PromQL
- TraceQL
- SQL

Last9

Let’s meet where you are...

Last9

Last9: Telemetry Data Platform



1M+
samples/second

100ms
Query Latency

20M+
Dimensions

360°
Visibility

And that is it!

THANK YOU.

Let’s keep the conversation going.
Reach out at prathamesh@last9.io :)

Last9 Blog