
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

OPN401-R

Observing logs and traces with OpenSearch

Muthu Pitchaimani (he/him)

Sr. Analytics Specialist Solutions Architect
Amazon Web Services

Aish Gunasekar (she/her)

Sr. Analytics Specialist Solutions Architect
Amazon Web Services

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modern information system challenges

- Increasing number of enterprise applications and types
- Increasing need to accommodate emerging technologies in analytics, AI, and ML
- Modern applications and infrastructure are increasing in complexity
- Machine-generated data is ever growing
  - 45 zettabytes and growing at 400 exabytes per day*

*The World Economic Forum

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logs are ubiquitous



Applications and infrastructure

Services/microservices

Web applications

Business applications

APIs



IT and DevOps

Databases

Load balancers

Networking

Servers



IoT and wireless

Automotive

Home devices

Manufacturing

Mobile applications

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Turning logs into insights



Business insights

What content/products are my users interested in?

Which features are used most or least?

What users are most active and why?



Security monitoring

Is there any suspicious authentication activity?

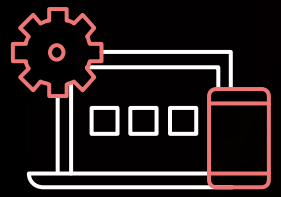
What data was accessed by this IP address?

Are there instances of fraud?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Turning logs into signals



Application troubleshooting

Is my infrastructure working?

What is the latency and error rate?

What caused my application issue?

Monitoring more than failures

Is it behaving as expected?

What is the usage?

What is the business impact?

$42,000 per hour

Average hourly cost of downtime per year

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Downtime costs money (and stress)



87 hours per year

Of downtime per year*

- **$42K** per hour avg hourly cost
- Opportunity loss, cost of **not doing business**
- **Penalties** of not meeting SLAs
- **Brand** alienation
- **Interruptions** to business

*Gartner

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



OpenSearch

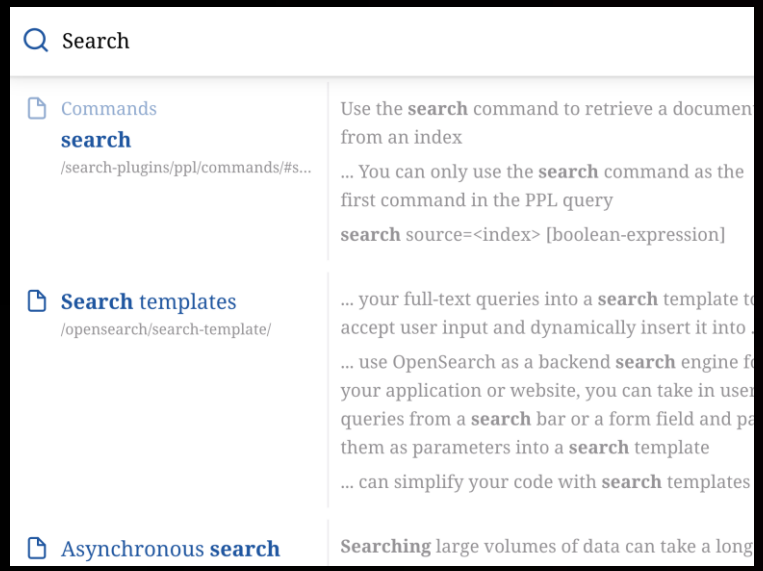
Community-driven, open-source search and analytics suite derived from Apache 2.0 licensed Elasticsearch 7.10.2 & Kibana 7.10.2

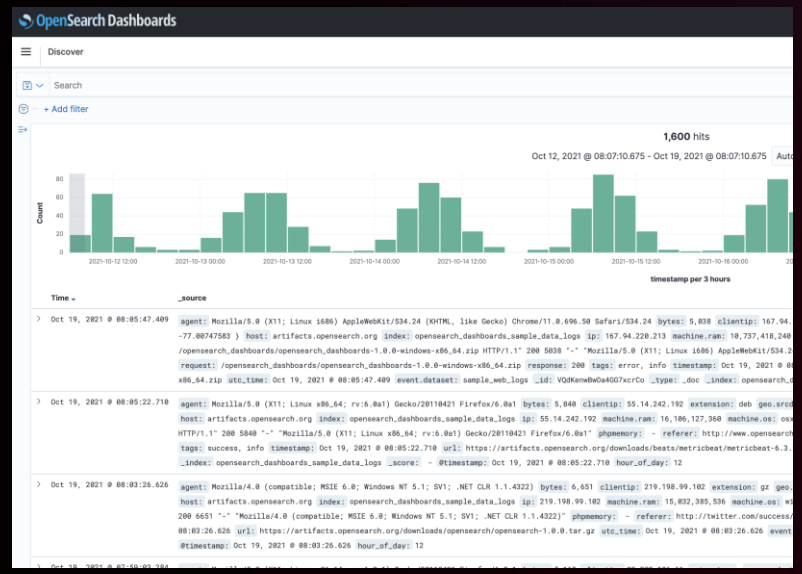
Consists of a search engine, OpenSearch, and a visualization user interface, OpenSearch Dashboards, as well as a series functionality adding tools and plugins

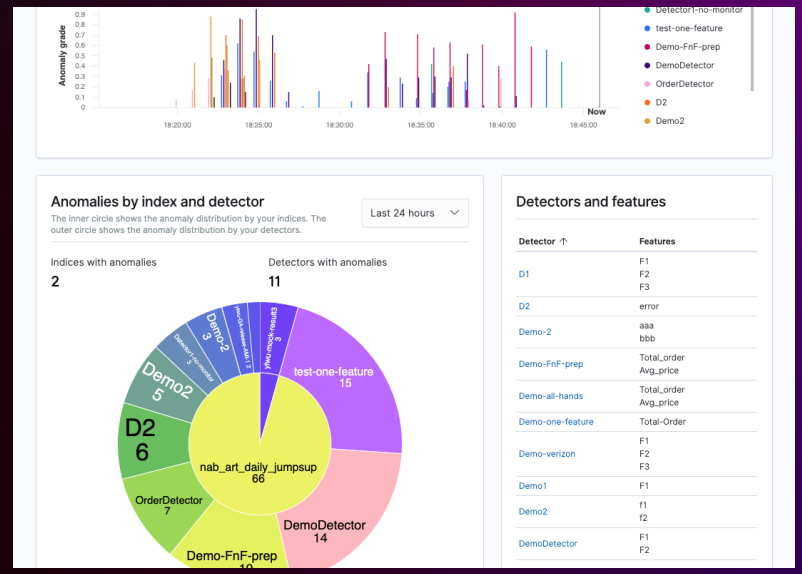
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OpenSearch







Text search

Natural language

Boolean queries

Relevance

Streaming data

High-volume ingest

Near real time

Distributed storage

Analysis

Time-based visualizations

Nestable statistics

Time series tools

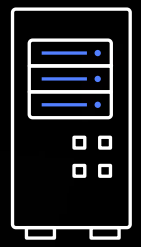
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Search, analyze, and visualize log data

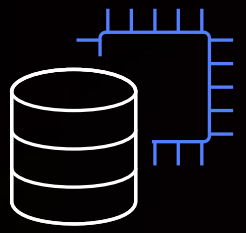


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

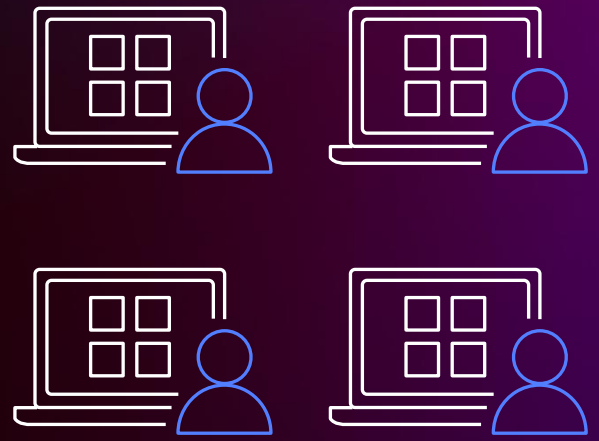
How does it work?



Server, application, network, AWS, and other logs



Application data



Application users, analysts, DevOps, and security

Indexed and instantly searchable

1

JSON documents



Amazon OpenSearch Service domain

3

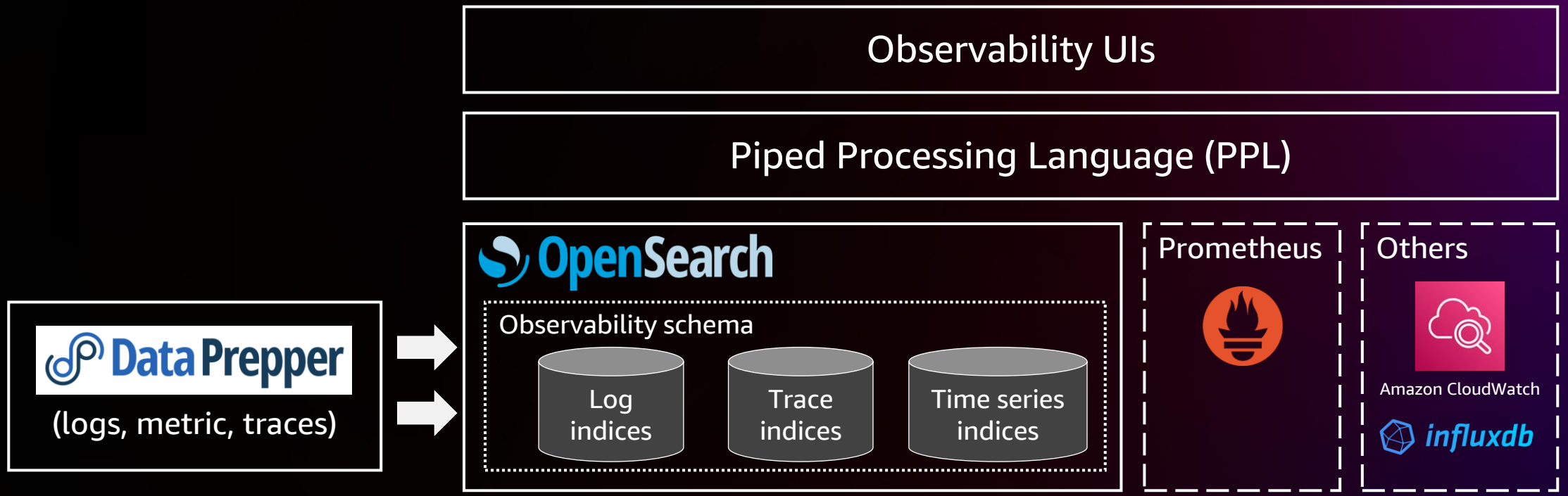
Rest APIs, clients, and OpenSearch Dashboards

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Observability implementation overview

Open source | Logs | Metrics | Traces

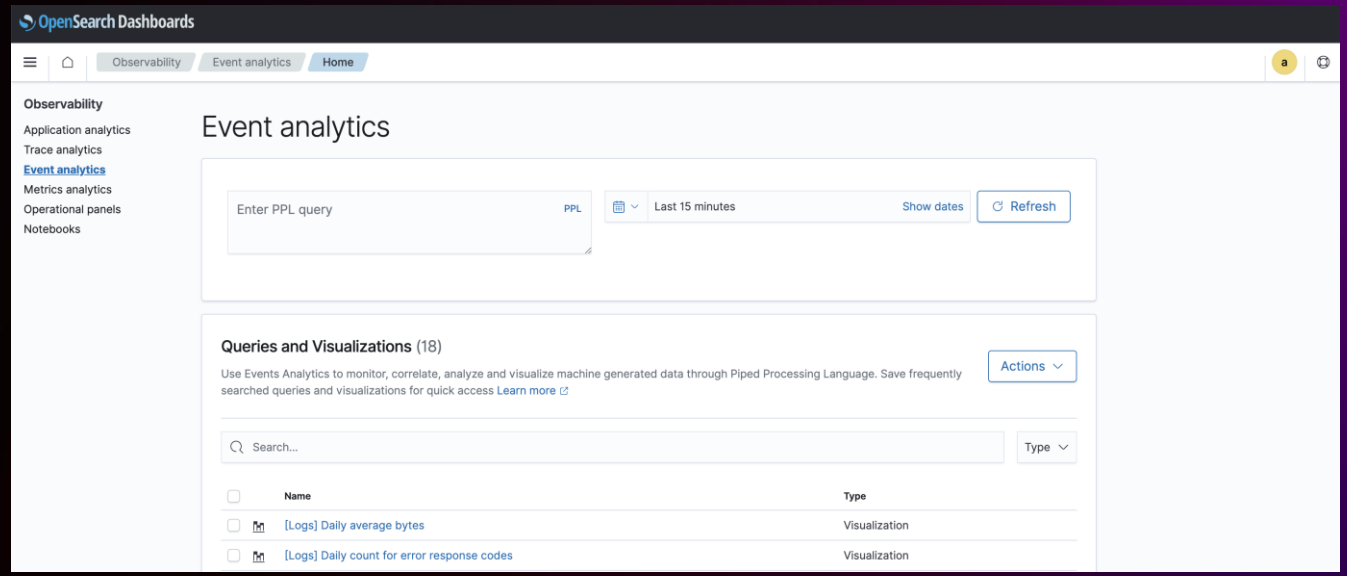


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Observability with OpenSearch

Log monitoring, event analytics

- Expanded log analytics capabilities
- PPL parse commands support



Distributed tracing: Trace analytics

APM: Application analytics to correlate logs, traces, and metrics

Out-of-the-box operational analytics

(Coming soon: metric extraction, alerting, anomaly detection, Prometheus integration)

aws

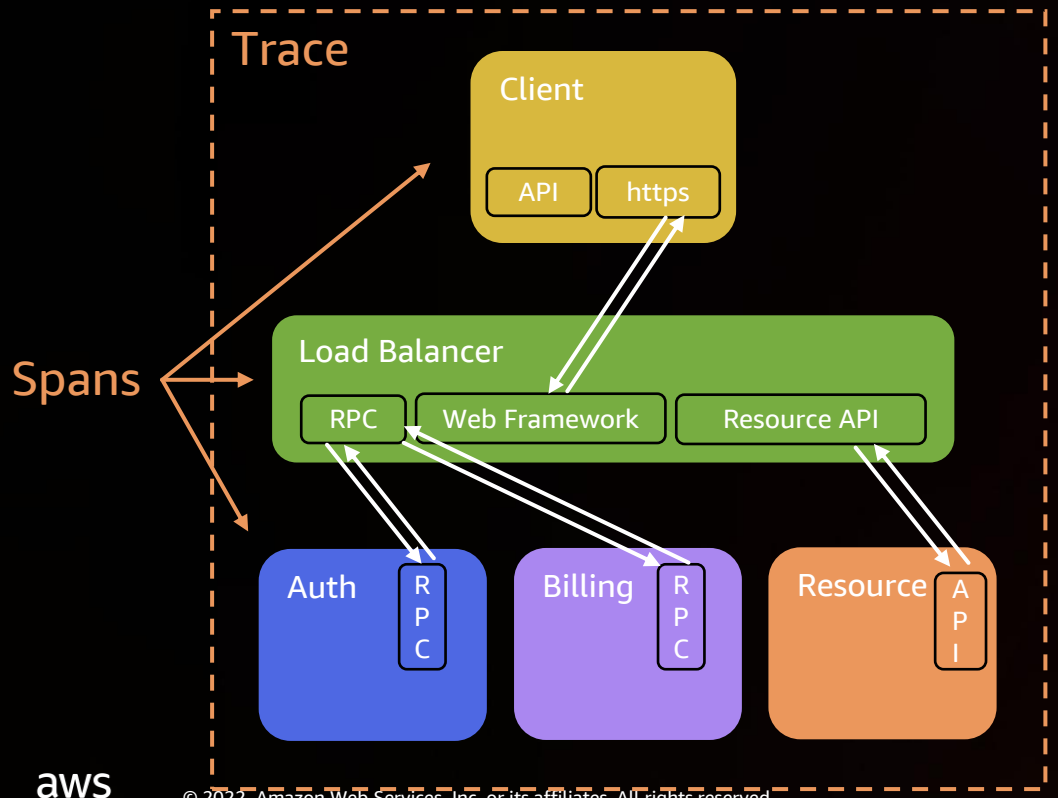
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

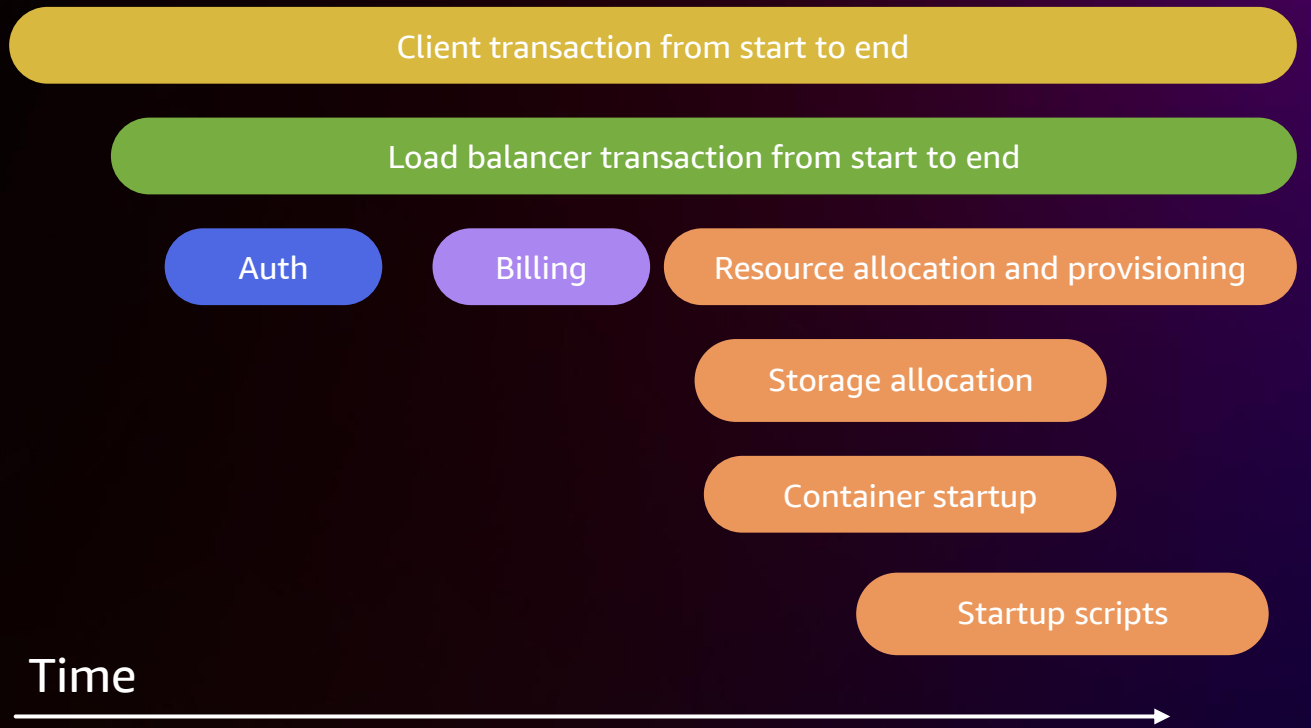
What is distributed tracing?

IDENTIFYING PROBLEMS IN CLOUD APPLICATIONS

A method of observing requests as they propagate through distributed systems

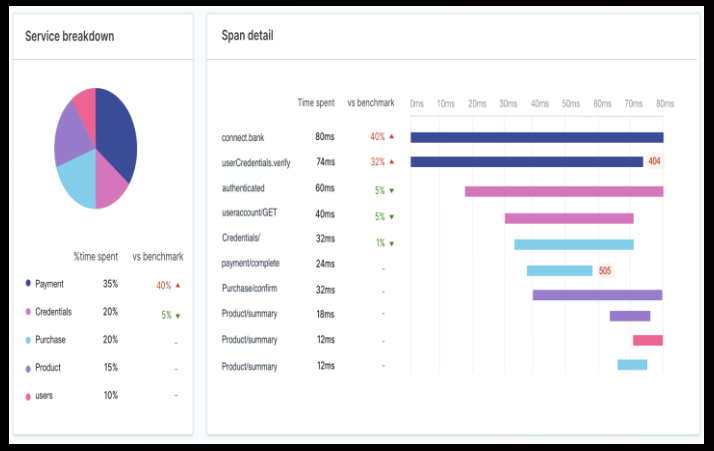
Trace: Hierarchical, end-to-end record of processing a request

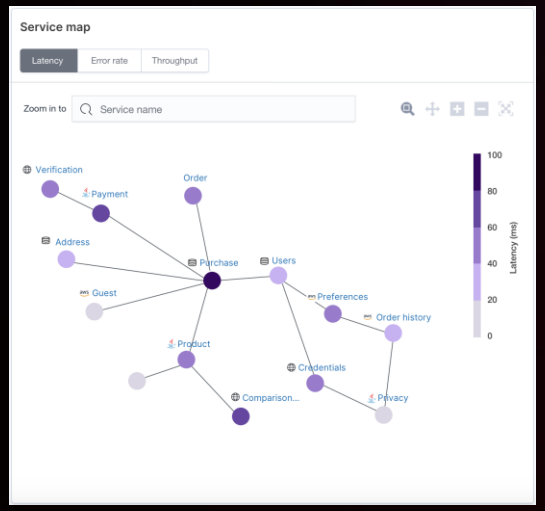


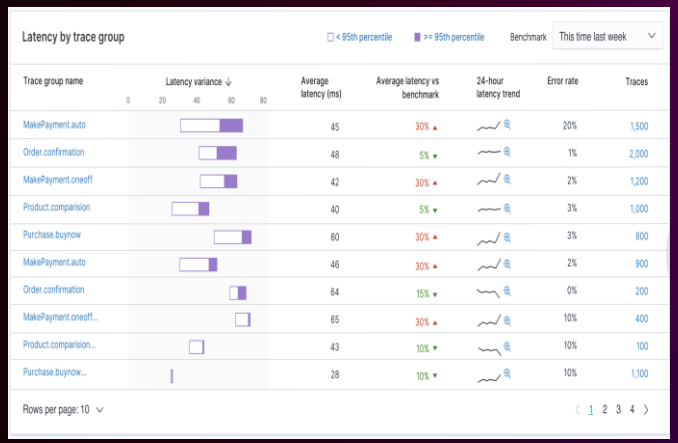


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Trace analytics







Trace-span details

- Single request performance
- Diagnose root cause

Service maps

- End-to-end view
- Isolate issues to services

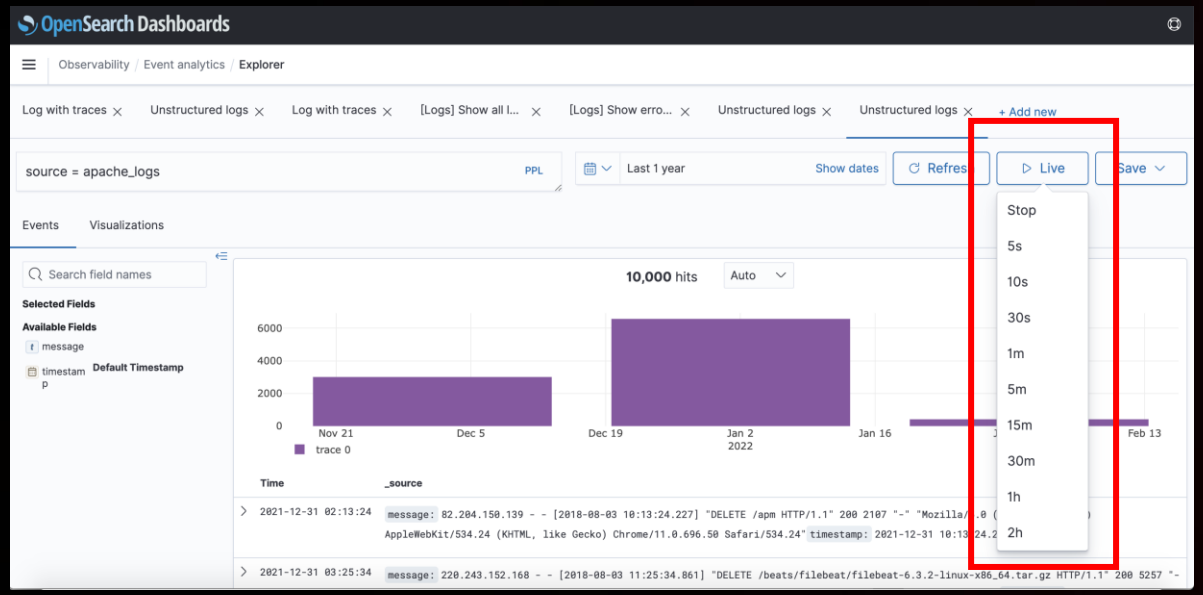
Trace groups

- Monitor performance
- Identify issues early

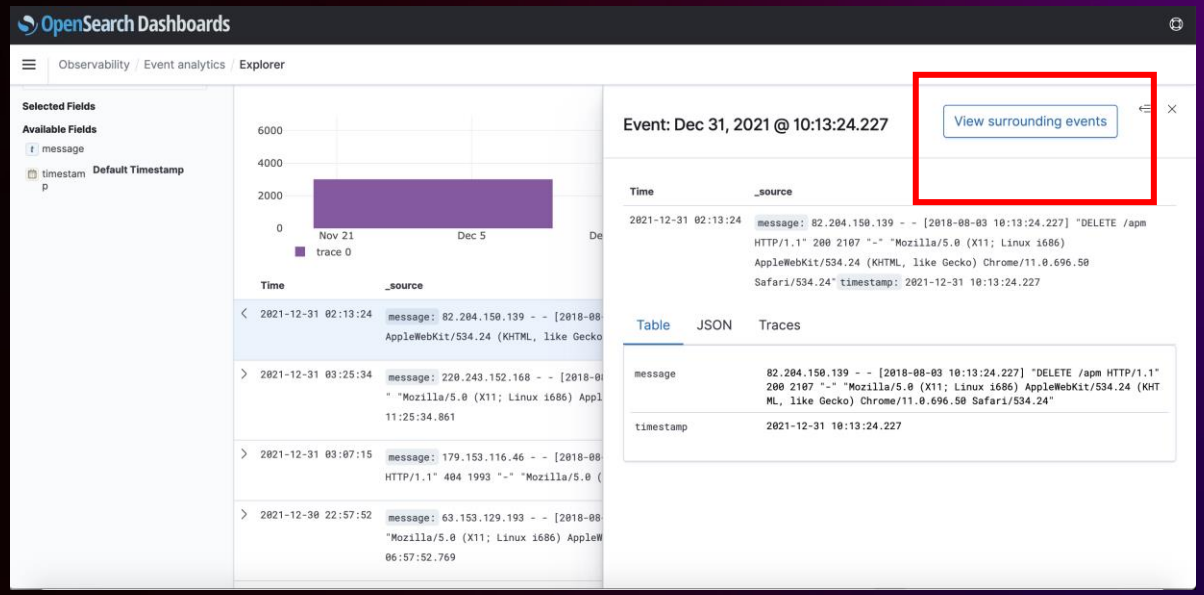
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Log monitoring

Live Tail



Log Surround

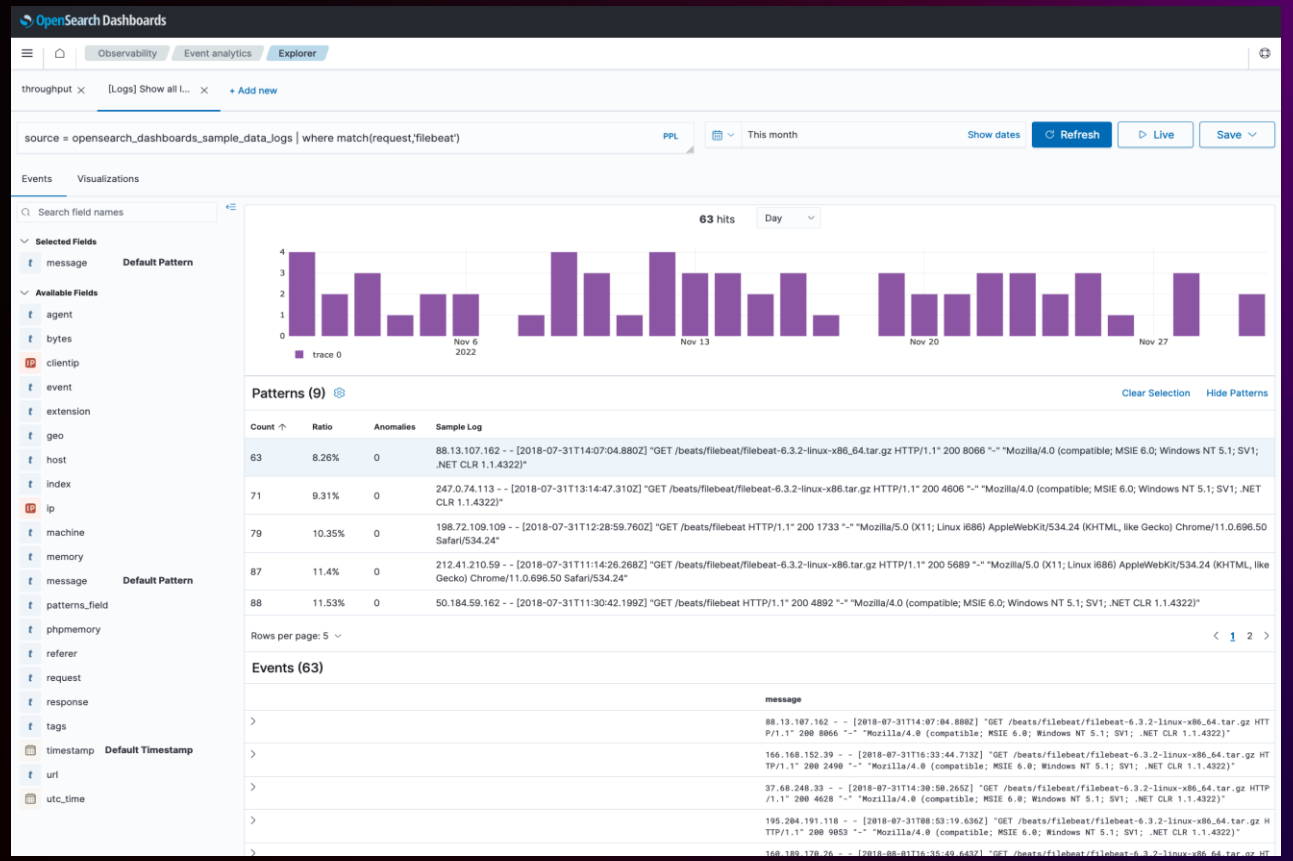


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Log patterns

GET AUTOMATIC INSIGHTS INTO MOUNTAINS OF LOG DATA

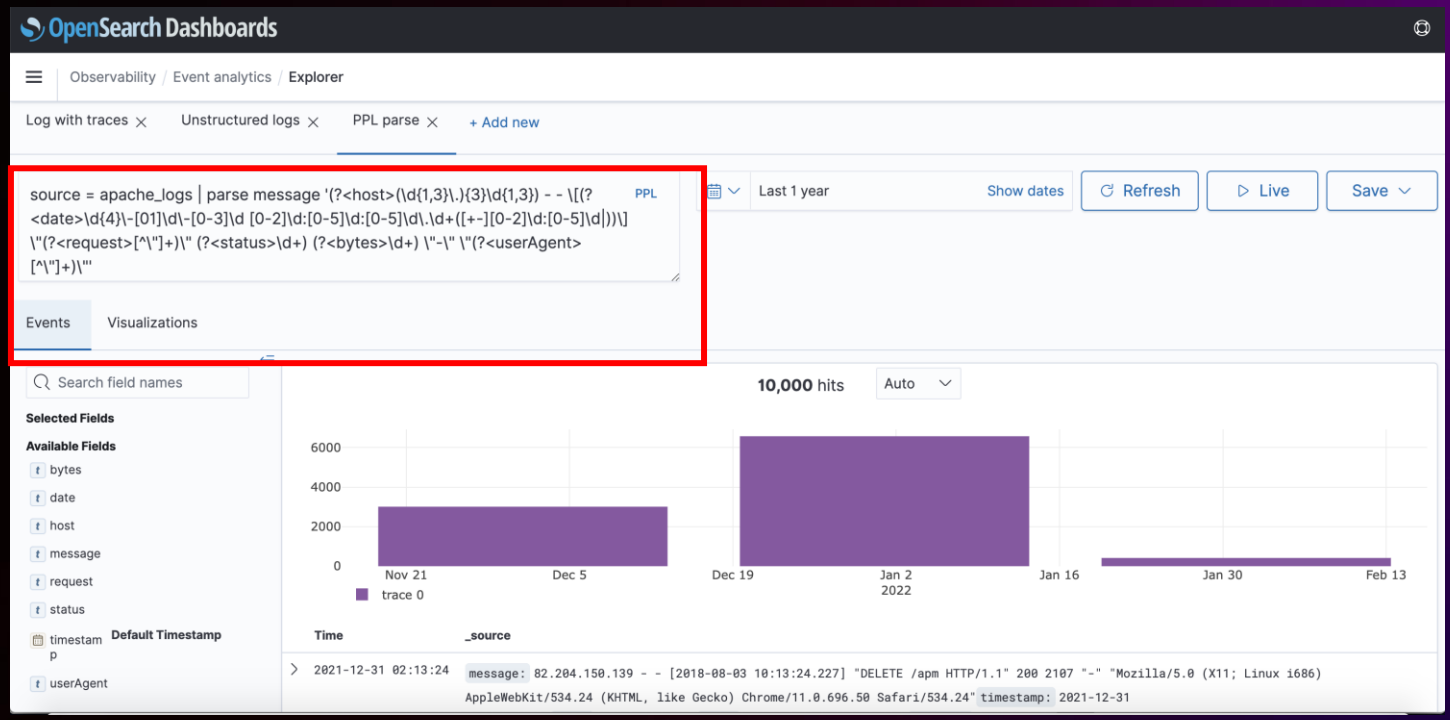
- Detect unexpected outliers
- Detect common “non-interesting” patterns for drop filters
- Patterns based on recurrence of event signatures
- Builds on log tailing, log surround, capabilities



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Piped Processing Language (PPL) query layer

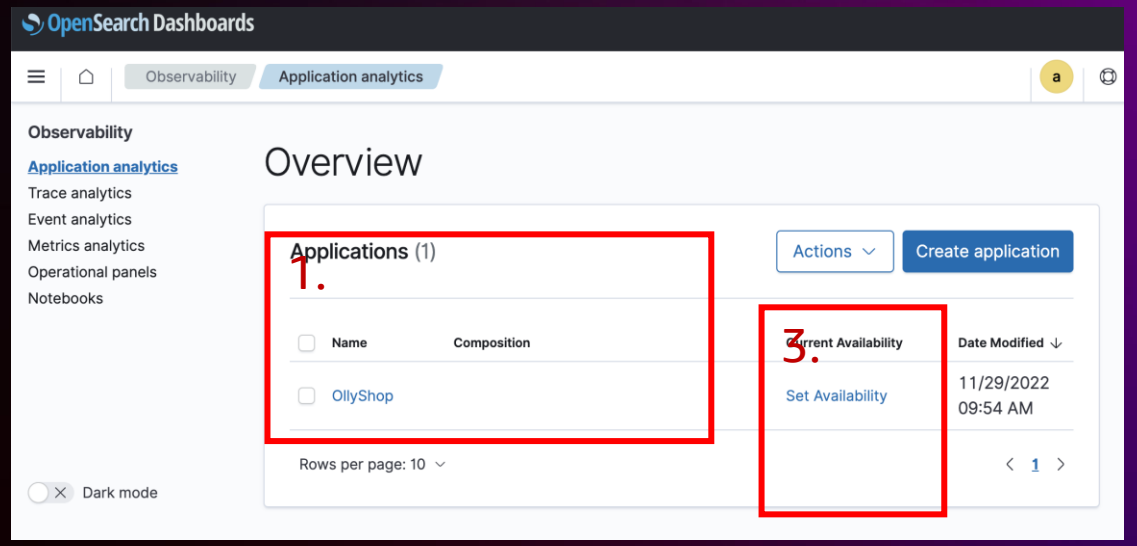
- Interactively explore, discover, and visualize data using a set of commands delimited by pipes (|)
- Visualization driven by “stats” command
- New “parse” command – parse a text field using regular expressions and pipe into other commands or search results

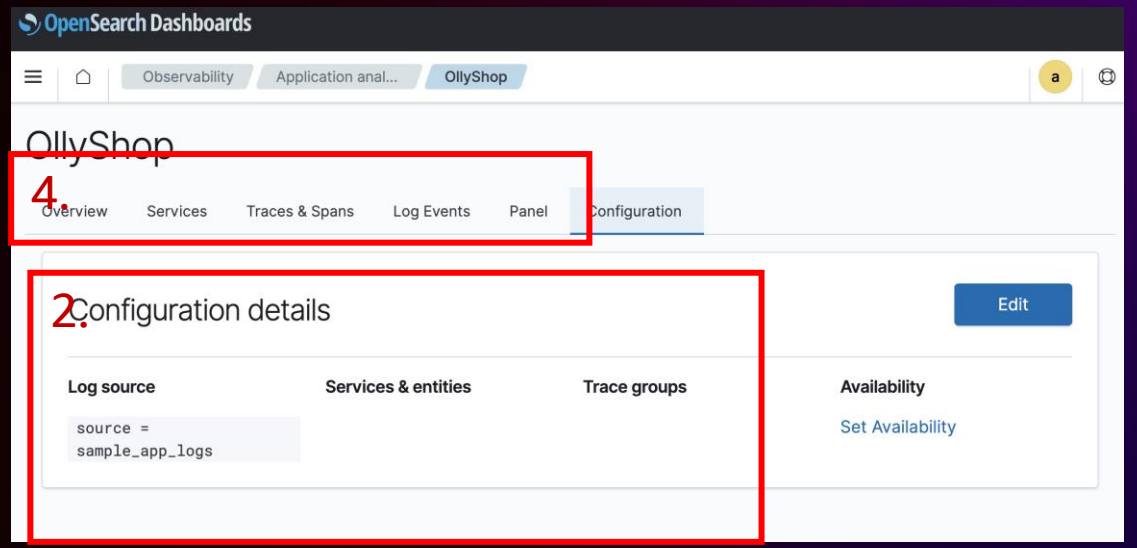


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application analytics

1. Build multiple application views into collected signal data
2. Select log sources, trace groups, or services to be part of each application
3. Monitor application availability
4. Drill into detailed view of traces, services, and logs
5. Easily trace and log events using span-id and trace-id embedded within log events and span details





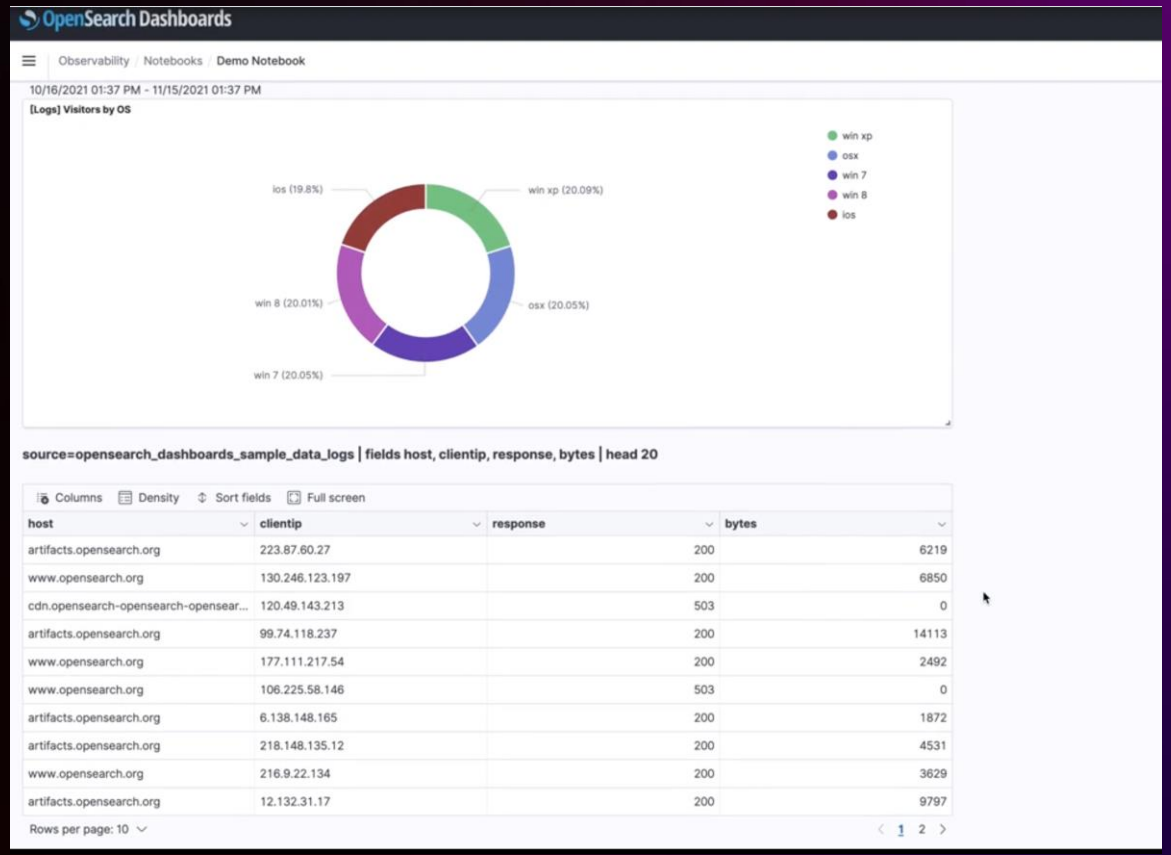
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Storytelling with notebooks

A notebook is a document made up of cells or paragraphs that can combine Markdown, SQL/PPL queries, and visualizations

Support for multi-timelines so that users can easily tell a story

Can be shared as an OpenSearch Dashboards link, PDF, or PNG



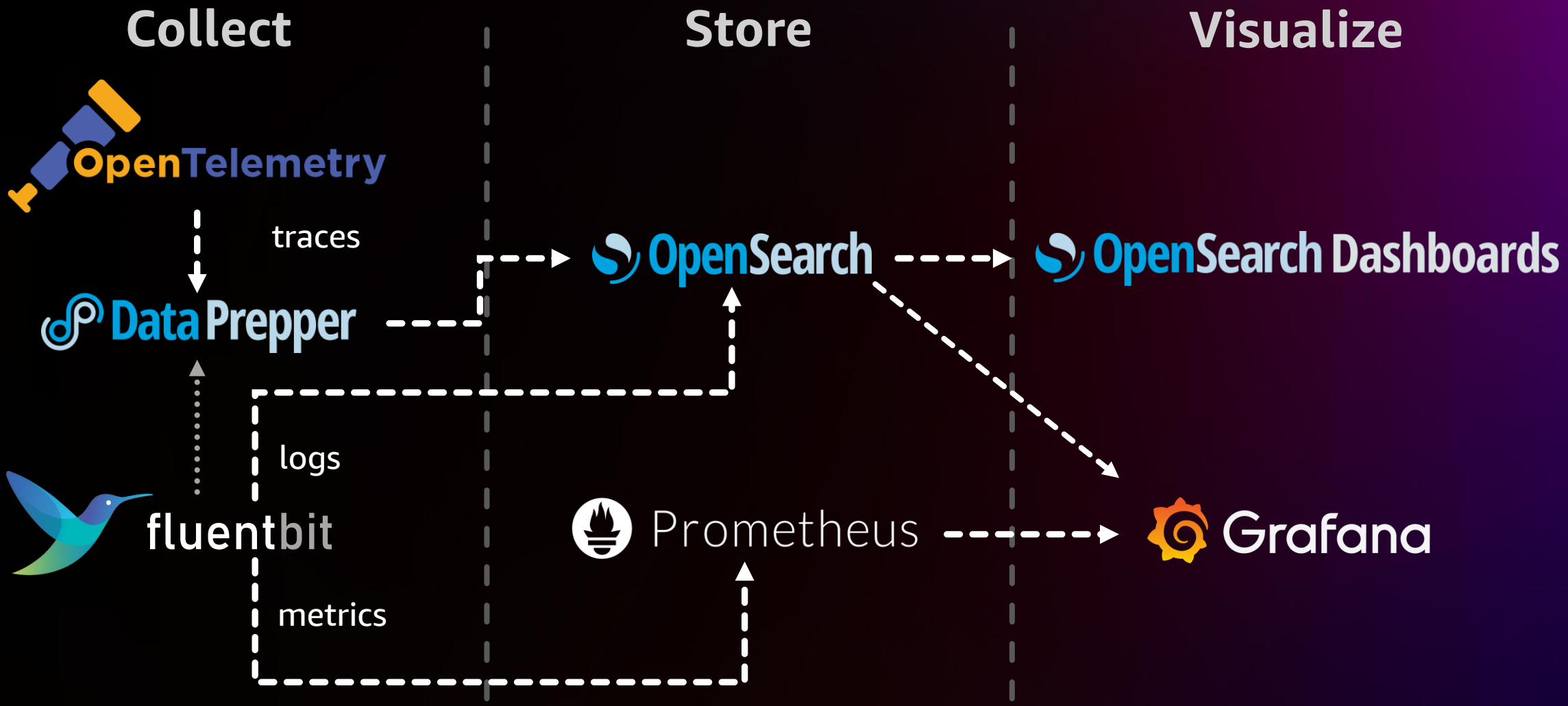
- Common use cases include creating postmortem reports, designing run books, building live infrastructure reports, and even documentation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OpenSearch observability architecture

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Open-source observability architecture



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.