

WELCOME TO | WILLKOMMEN ZU



EUROPE | BERLIN 2024

Conference Keynote

**Delivering the Next Wave of
Innovation with OpenSearch**





Mukul Karnik

General Manager, OpenSearch



Search is the foundation

OpenSearch is an information retrieval system

Delivers the most relevant results

Text search, faceting, geospatial, auto-complete, fuzzy matching

Helps finds patterns in logs

Unlocks the latest AI/ML technologies



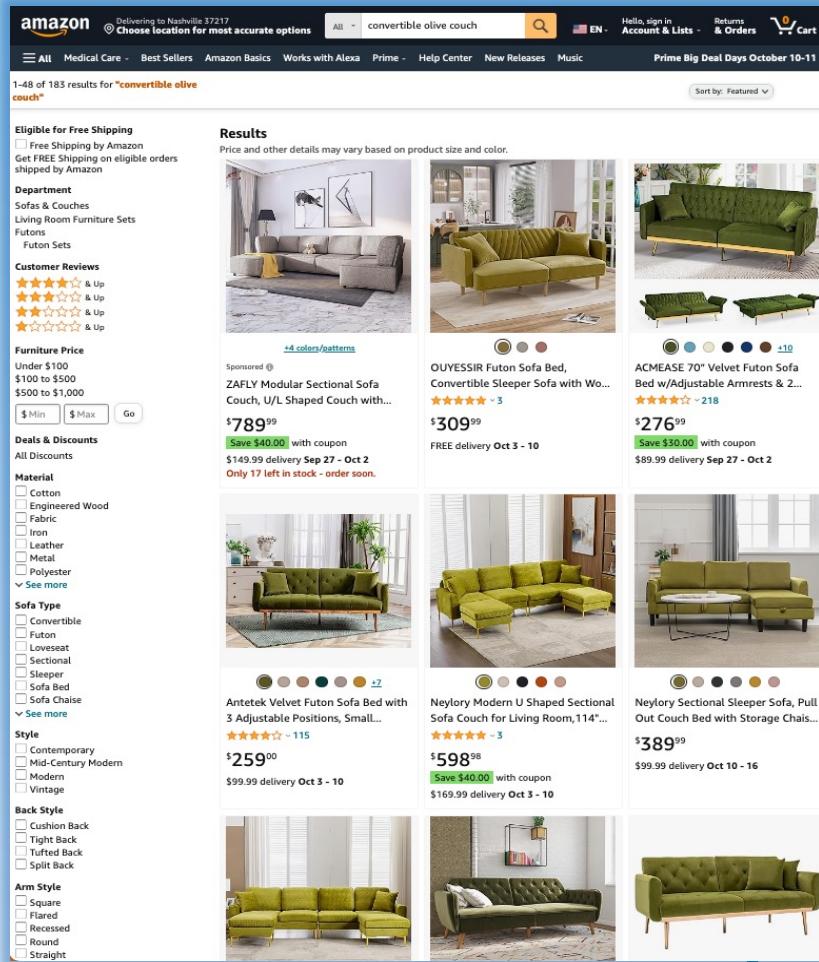
Text search

Search engines match terms to objects in a catalog

Match free text or structured data

Relevance determines sort order

Facets let users drill into the search results to narrow by attribute value



The boom in AI/ML

Large language models (LLMs)
providing good baseline NLP

ChatBots hit the public's
awareness

“Semantic” capabilities are directly
relevant for search workloads

Other AI/ML techniques are highly
relevant for search as well

OpenSearch enables working with
vector embeddings



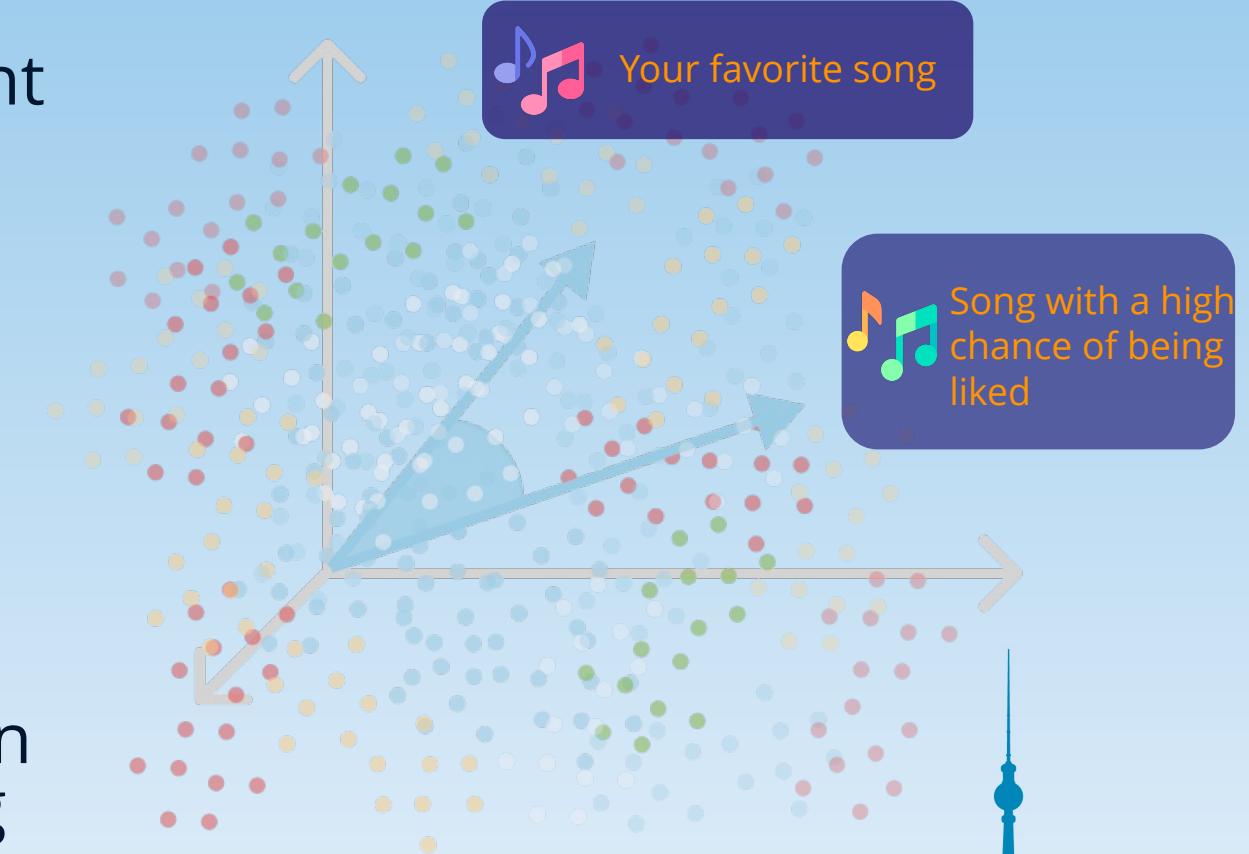
Vector similarity search

Generative AI models represent unstructured data as vector embeddings

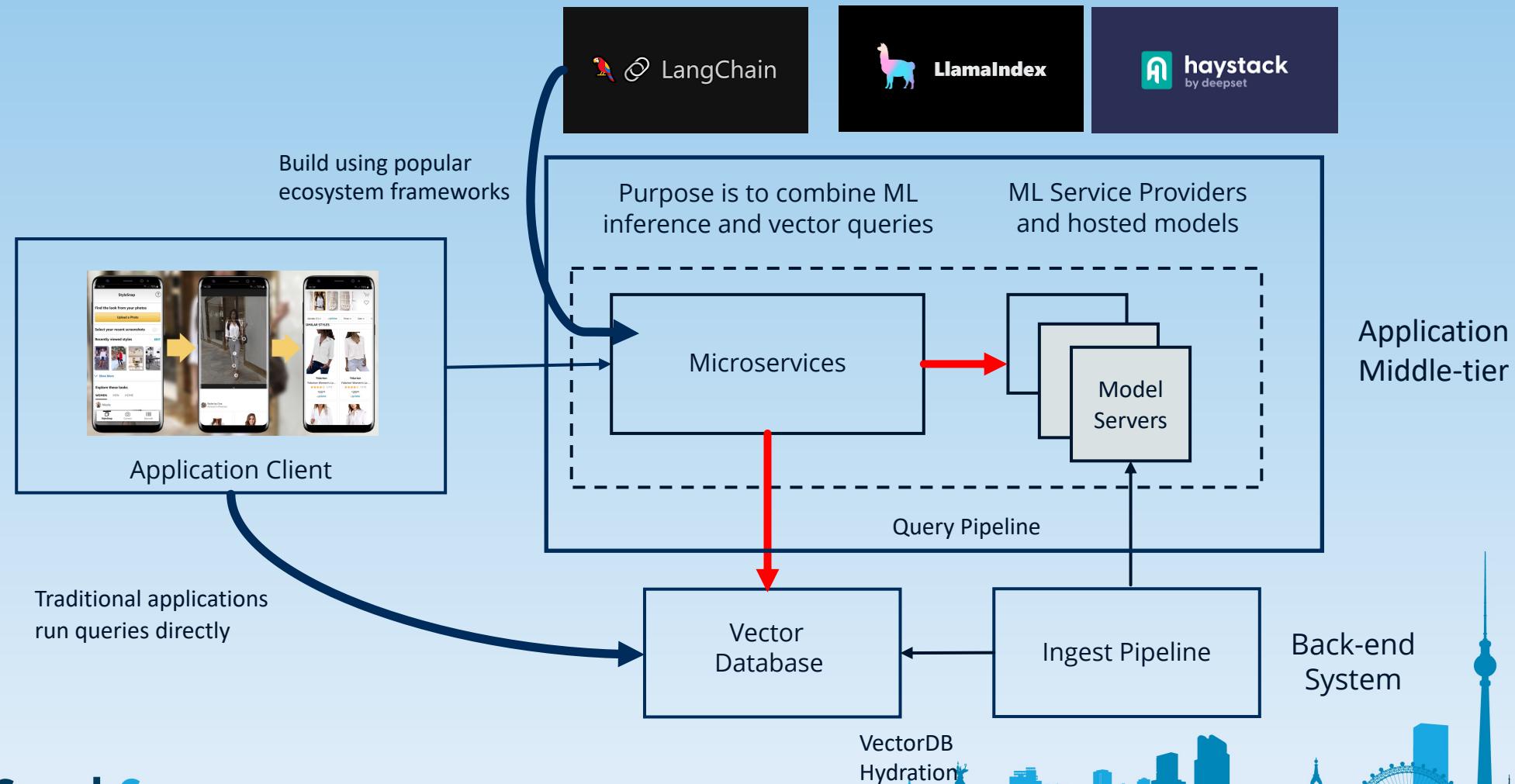
Embeddings capture semantic meaning and content relationships

Similar vectors = similar meaning and context

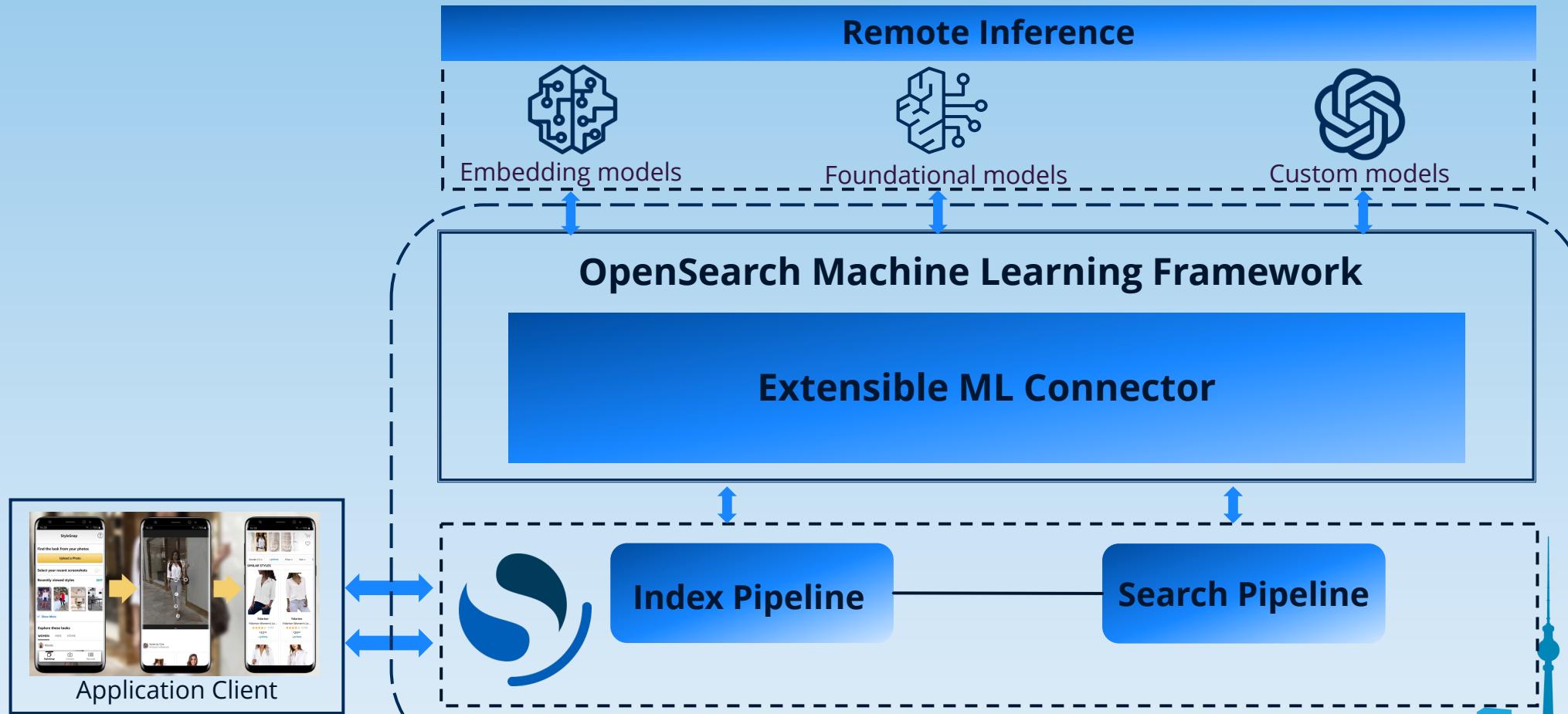
Deliver search results based on vector proximity by comparing vector distances



Vector search architecture



Build with neural search



Integrated semantic and hybrid search

Hybrid search

Fine-tuned models

Sparse vector retrieval

Multimodal search

The screenshot shows the OpenSearch Dashboards interface with the title 'Compare search results'. It is described as an 'Experimental Feature' for comparing search results using the same search text with different queries. The interface has two main sections: 'Query 1' and 'Query 2'. Both sections have an 'Index' dropdown set to 'flickr2_demo' and a 'Query' text area containing OpenSearch Query DSL code. The 'Query 1' code is:

```
1 "query": {  
2     "match": {  
3         "image_description_text": "%SearchText%"  
4     }  
5 },  
6     "_source": ["image_id", "image_description_text"]  
7 }  
8 }  
9 }
```

The 'Query 2' code is:

```
1 "image_description_embedding_custom": {  
2     "query_text": "%SearchText%",  
3     "model_id": "f0fbeyQBJ_MROKKh0gnC"  
4 }  
5 },  
6     "_source": ["image_description_text", "image_id"]  
7 }  
8 }  
9 },  
10 }  
11 }
```

Below the queries, there is a placeholder text: 'Enter a query in OpenSearch Query DSL. Use %SearchText% to refer to the text in the search bar.' At the bottom center, it says 'Add queries to compare search results.'

Conversational search

The screenshot shows a web-based application for managing PDF documents and performing conversational search. On the left, a sidebar titled "Your documents" allows users to upload PDF files by dragging them or using a "Browse files" button. Two files are listed: "OpenSearchFA..." (0.7MB) and "Operational be..." (491.6KB). A "Process" button is available for these files. A green message at the bottom of the sidebar says, "you can start searching on your PDF(s)". The main area is titled "Chat with your PDF using OpenSearch" and includes a "Clear Chat" button. A text input field is provided for asking questions. A message at the top of this area states, "You are talking to the uploaded PDF, ask any question." The background features a silhouette of the Berlin skyline.

Observability with OpenSearch

Rich log analytics capabilities

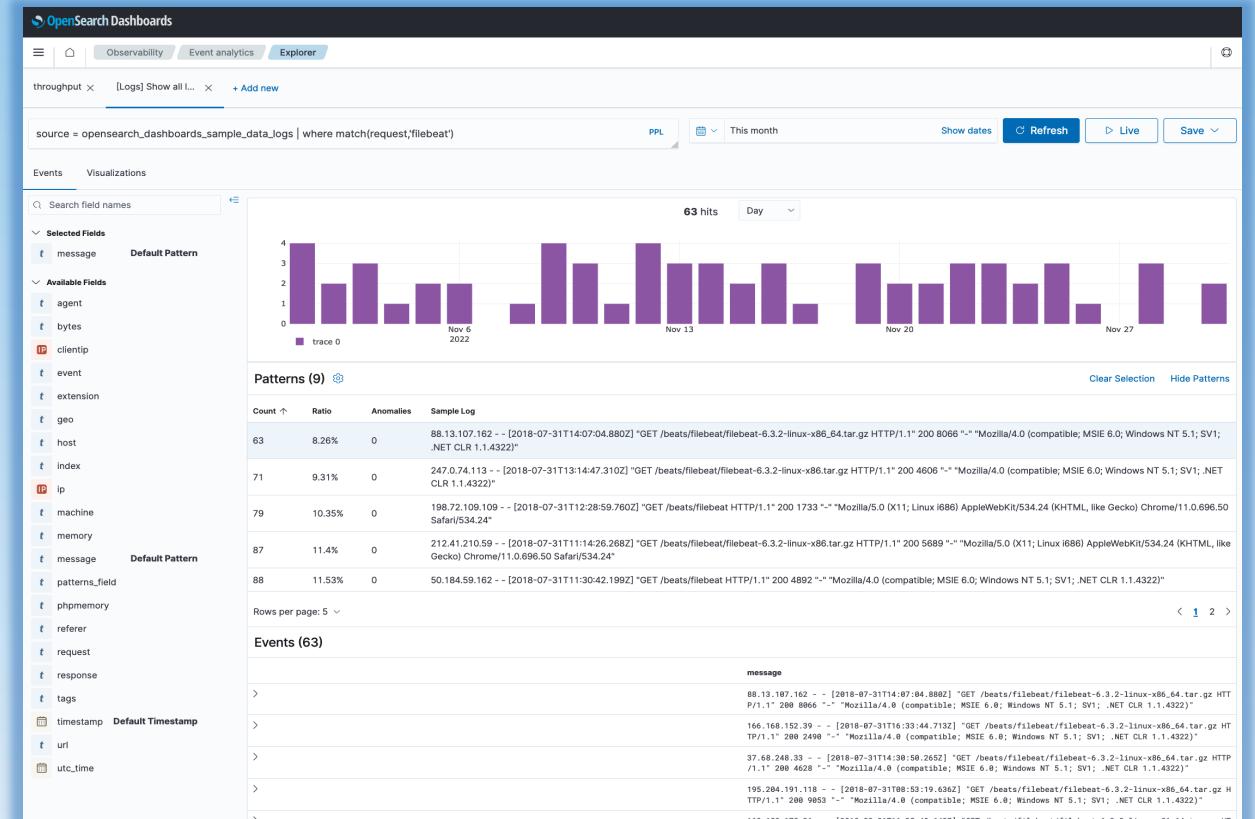
- Built-in anomaly detection & alerts
- Support for OpenTelemetry data
- Log patterns, tailing, surround, and more
- PPL query language

Extend tracing with Jaeger

- Spans, trace groups, and service maps

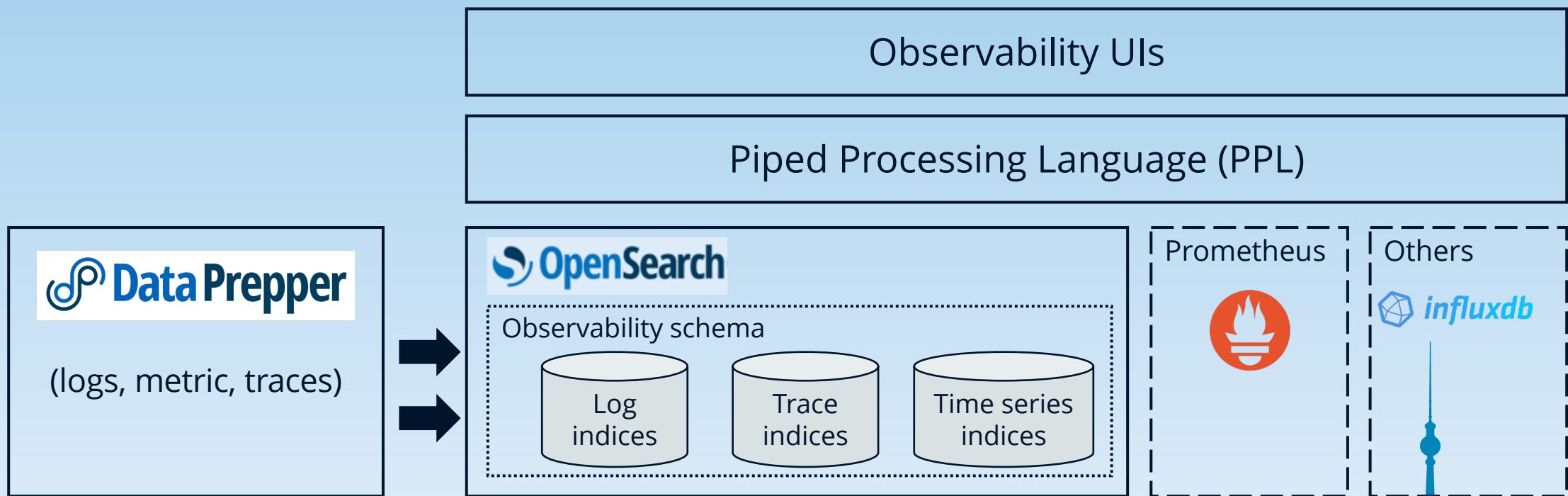
Metric Analysis

- Metric extraction from logs



Observability architecture

Open source | Open standards | Customizable



Anomaly Detection

Detect and mitigate issues faster with anomaly detection

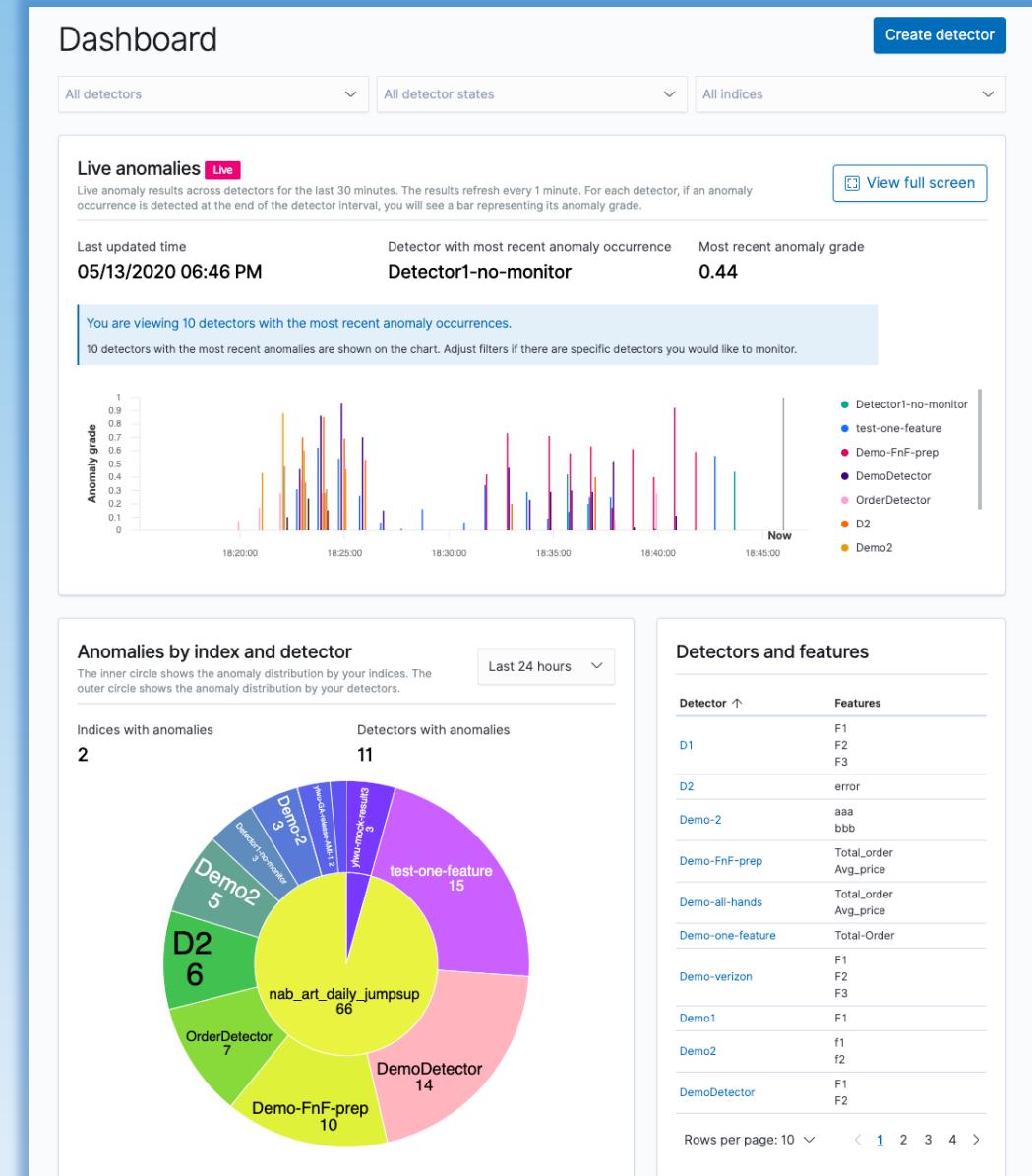
Performant at scale

- Machine learning models are distributed and processed across nodes

Easy to use

- No machine learning expertise required

Based on Random Cut Forest (RCF)



The OpenSearch Assistant

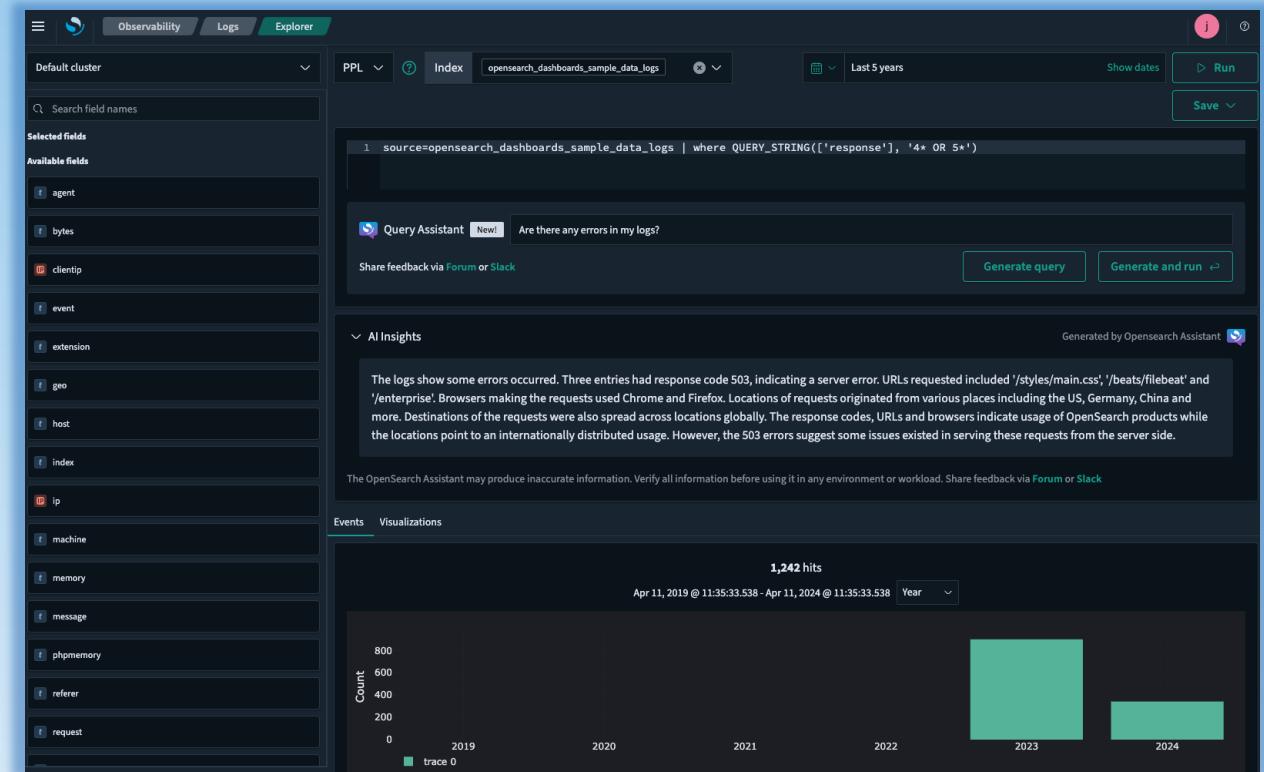
Interact using natural language

Open-source customizable toolkit

Simplified and rich insights

Implement your own skills

Connect to your preferred model



Security Analytics with OpenSearch

Decrease time to response

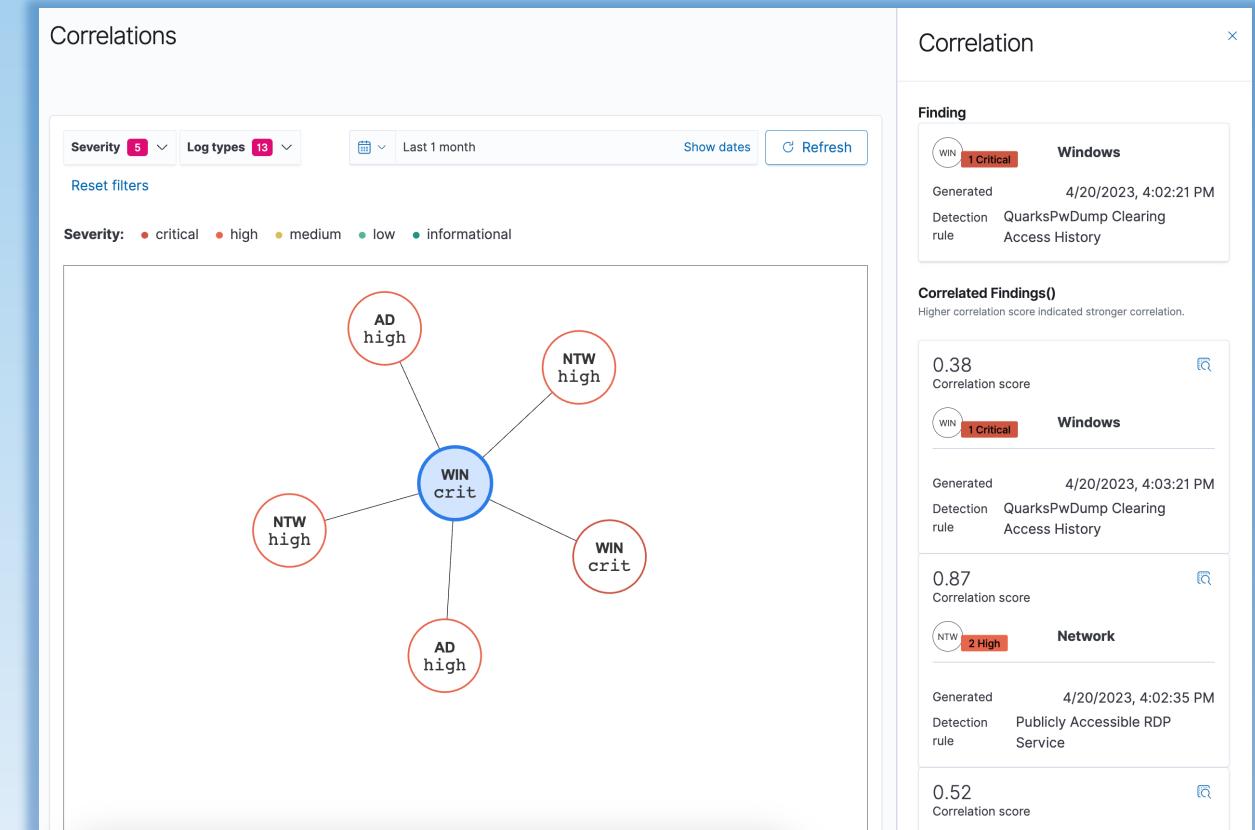
Detect potential threats quickly

2000+ security rules built-in

25+ log sources supported

Alert stakeholders

[New v 2.9] Correlation Engine



Performance Improvements



Performance Improvements from 1.0 to 2.12

Indexing

25%

throughput increase

Query

15-129%

latency reduction

Storage

15-30%

disk space reduction

Range queries

50-70%

latency reduction

Zstandard compression

15-30%

storage reduction

Full-text queries

129%

latency reduction

Match_all queries

85%

latency reduction

Vector search

30%

latency reduction

Sort improvements

926%

latency reduction

Date histogram

1434%

latency reduction

Remote-backed storage

Durability

increase

Segment replication

25%

throughput increase

Introducing...



Hariharan Gandhi

Product Owner, SAP

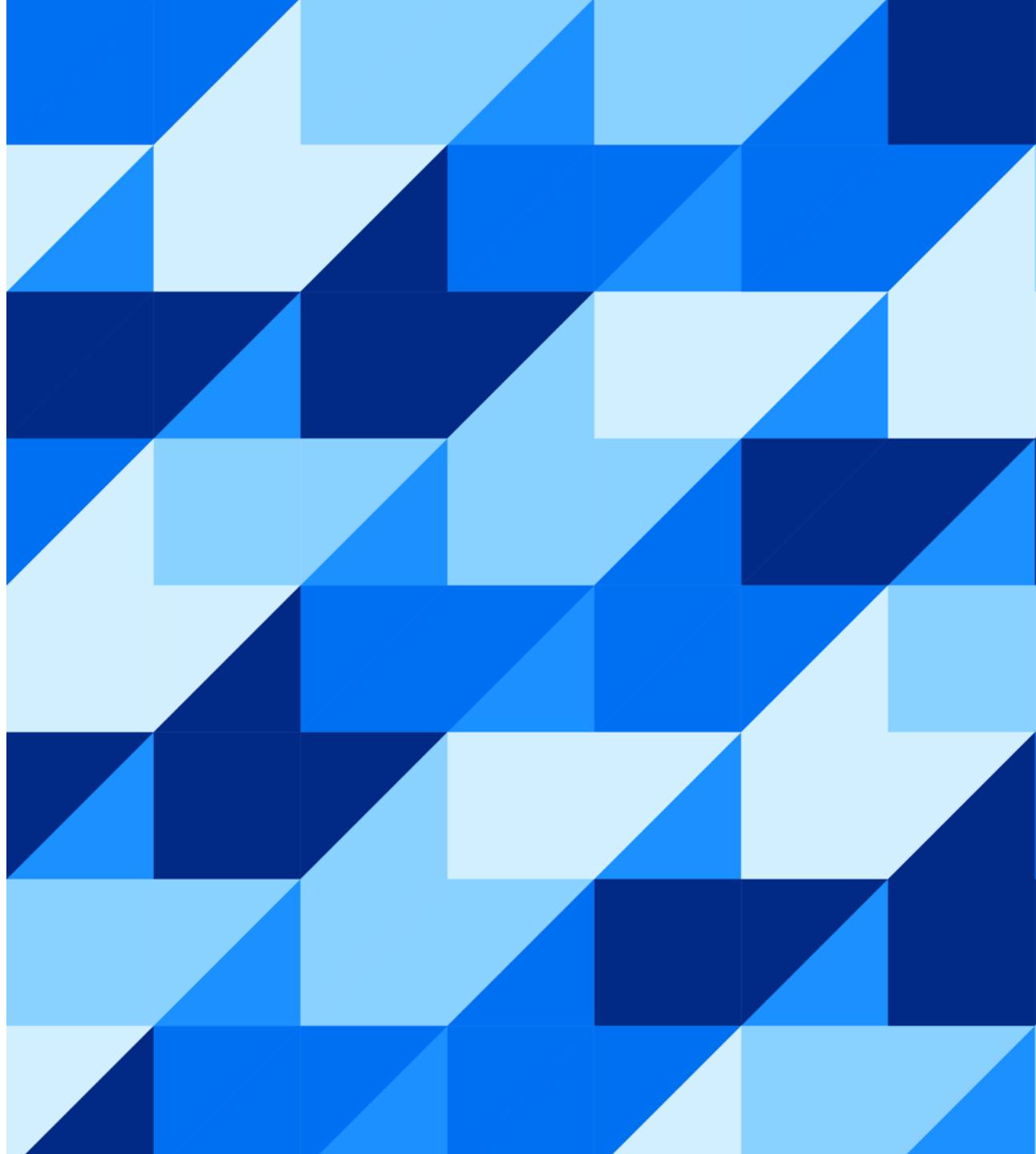




OpenSearch @ SAP BTP Logging Service

Hariharan Gandhi, SAP
May 07, 2024

Public



OpenSearch @SAP BTP Logging service

SAP's Business Technology Platform (BTP)

- PaaS Runtimes –  **Kyma**
- Services
- Customers building Business apps



SAP Service Teams

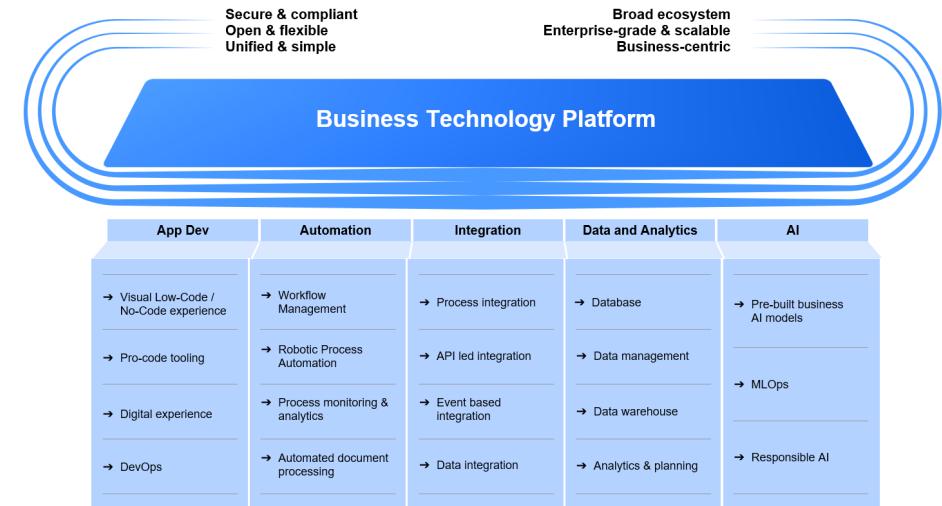


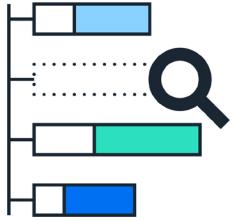
External Customer



SAP Platform Teams

SAP BTP Cloud Capabilities





Need: Hosted Observability solution

- Reduced Operational Overhead
- Pre-defined contents tailored for SAP BTP runtimes – CF & Kyma
- Compliance needs: Retention, encryption, privacy etc.

Our team: **BTP Logging service**

- Offers hosted observability as a services
- Consumed by the platform's runtimes and services
- Consumed by customers of BTP
- OTel shared semantics beyond BTP

Powered by  **OpenSearch**

Product Owner - Logging Service @ SAP's Business Technology Platform (BTP)

Distributed Systems Engineer (M.Sc. Technical University of Darmstadt)

Over 11 years of experience in the Software Industry, with a steadfast focus on SAP's logging/observability needs for the past 8 years

In his previous role as an Architect, Hariharan spearheaded the replatforming of OpenSearch-based logging services to Kubernetes at scale



Hariharan Gandhi
Product Owner
Logging Service

Agenda



Our OpenSearch Setup



Use cases

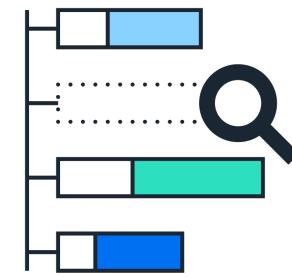
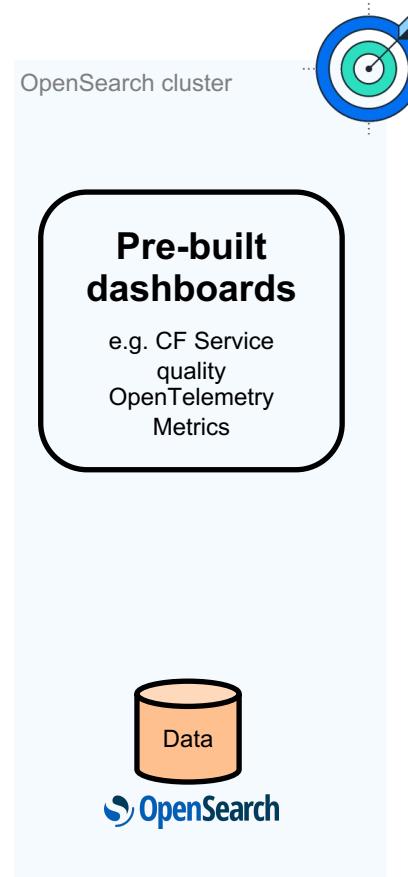
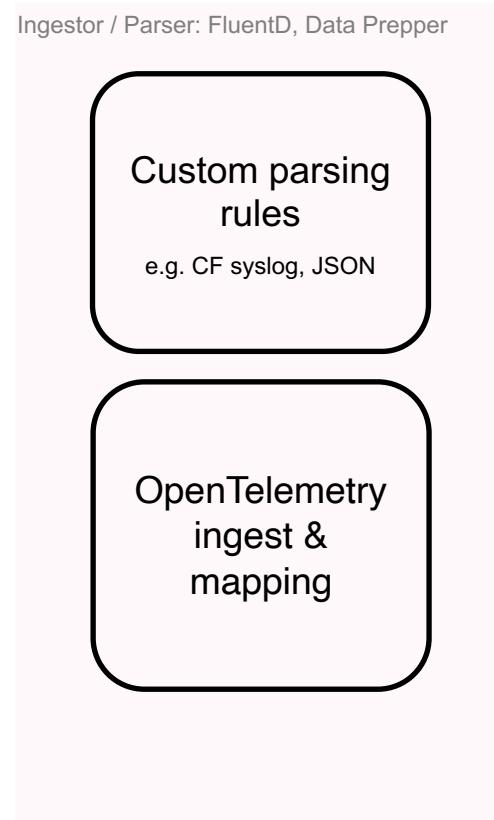
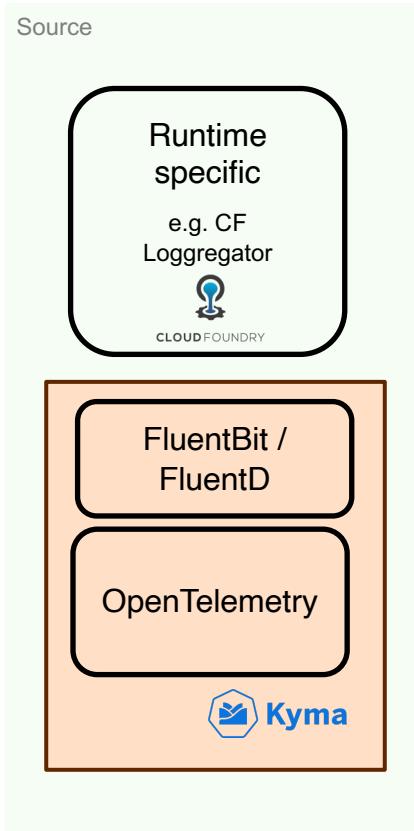


Challenges

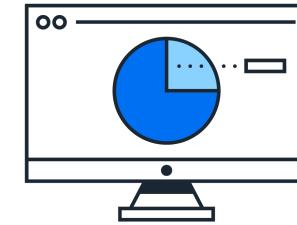


Team & OS Community

OpenSearch Setup



SAP specific correlation



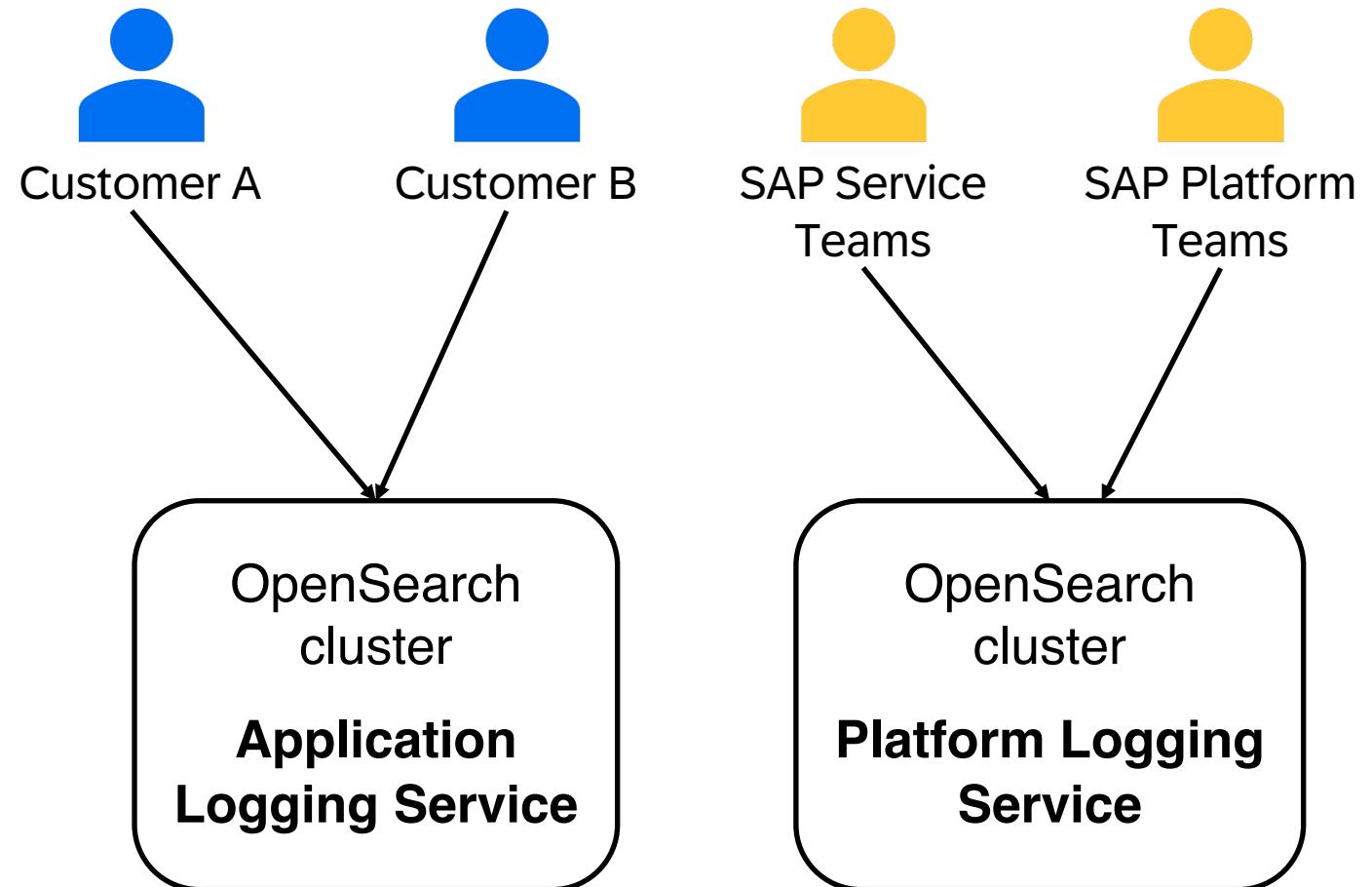
Pre-defined contents

OpenSearch Setup 1

Large central clusters on VMs

Shared stack ☀️

Multi-tenancy on top



OpenSearch Setup 1: Large central clusters on VMs



 **50+ Global**

Both for runtimes and end
use application logs

200k - 1Mi

Events per seconds

~100 Billion

Events: logs & metrics stored
for 14 days

~1k

CPUs on Largest Cluster –
Data Nodes

~1.5TB

Memory on Largest Cluster
– Data Nodes

 **0.5PB**

60-70% usage. Retention 14
days



OpenSearch Setup 1: Large central clusters on VMs

Shared stack

⌚ 50+ Global

Both for runtimes and end user application logs

200k - 1Mi

Events per seconds

~100 Billion

Events: logs & metrics stored for 14 days

~1k

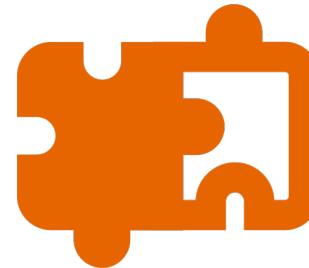
CPU on Largest Cluster – Data Nodes

~1.5TB

Memory on Largest Cluster – Data Nodes

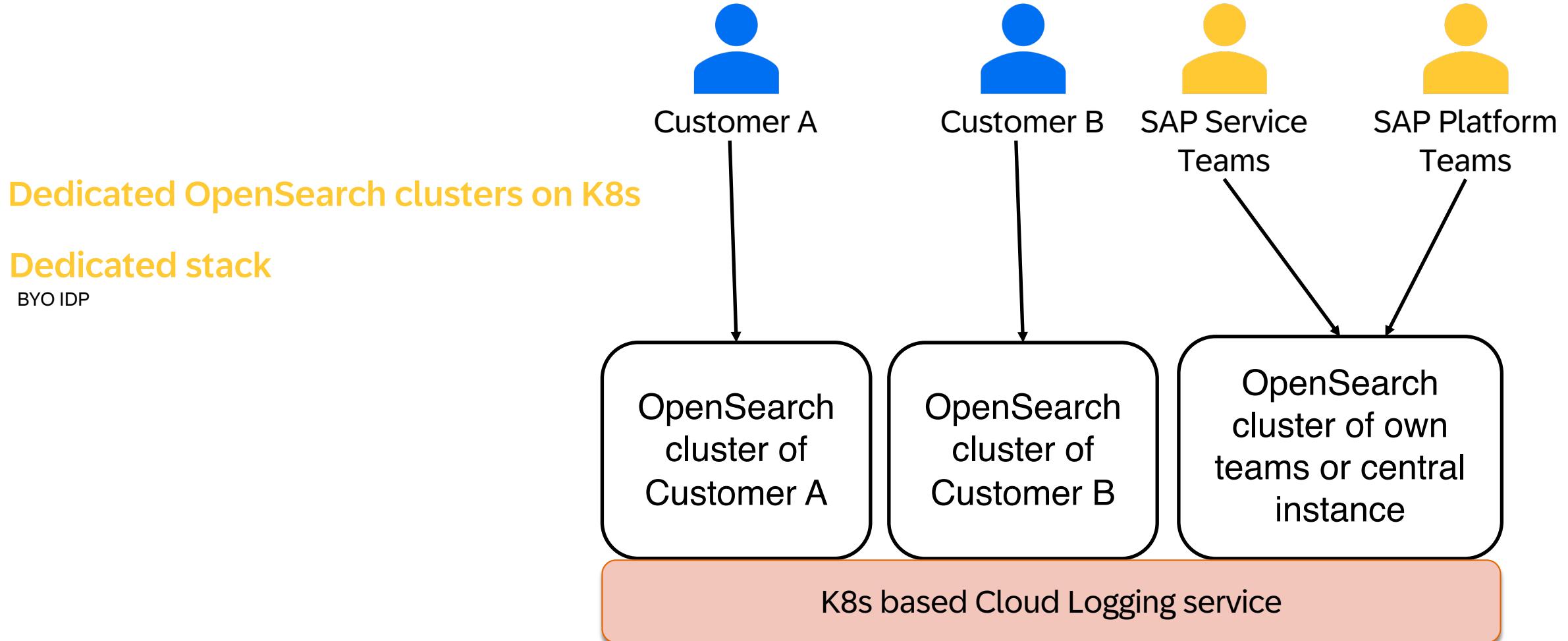
0.5PB

60-70% usage. Retention 14 days



- Complex Multitenancy setup
- Limited exposure of OpenSearch features
- No flexibility in config: retention, dashboards etc

OpenSearch Setup 2



OpenSearch Setup 2: Dedicated clusters on K8s

>7400

OpenSearch Clusters

50000

Persistent Volumes

>3PB Storage

(Hot) With Auto-Scaling

 **>1700 EC2**

Spread equally across 3 Zones

50K CPU / 220 TB of Memory

35 K8s

Clusters using Gardener

 **10 Global**

Deployments



OpenSearch Setup 2: Dedicated clusters on K8s

>7400

OpenSearch Clusters

50000

Persistent Volumes

>3PB Storage

With Auto-Scaling

⌚ >1700 EC2

Spread equally across 3 Zones

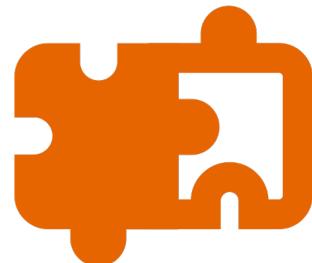
50K CPU / 220 TB of Memory

35 K8s

Clusters using Gardener

⌚ 10 Global

Deployments



- Complex operational setup

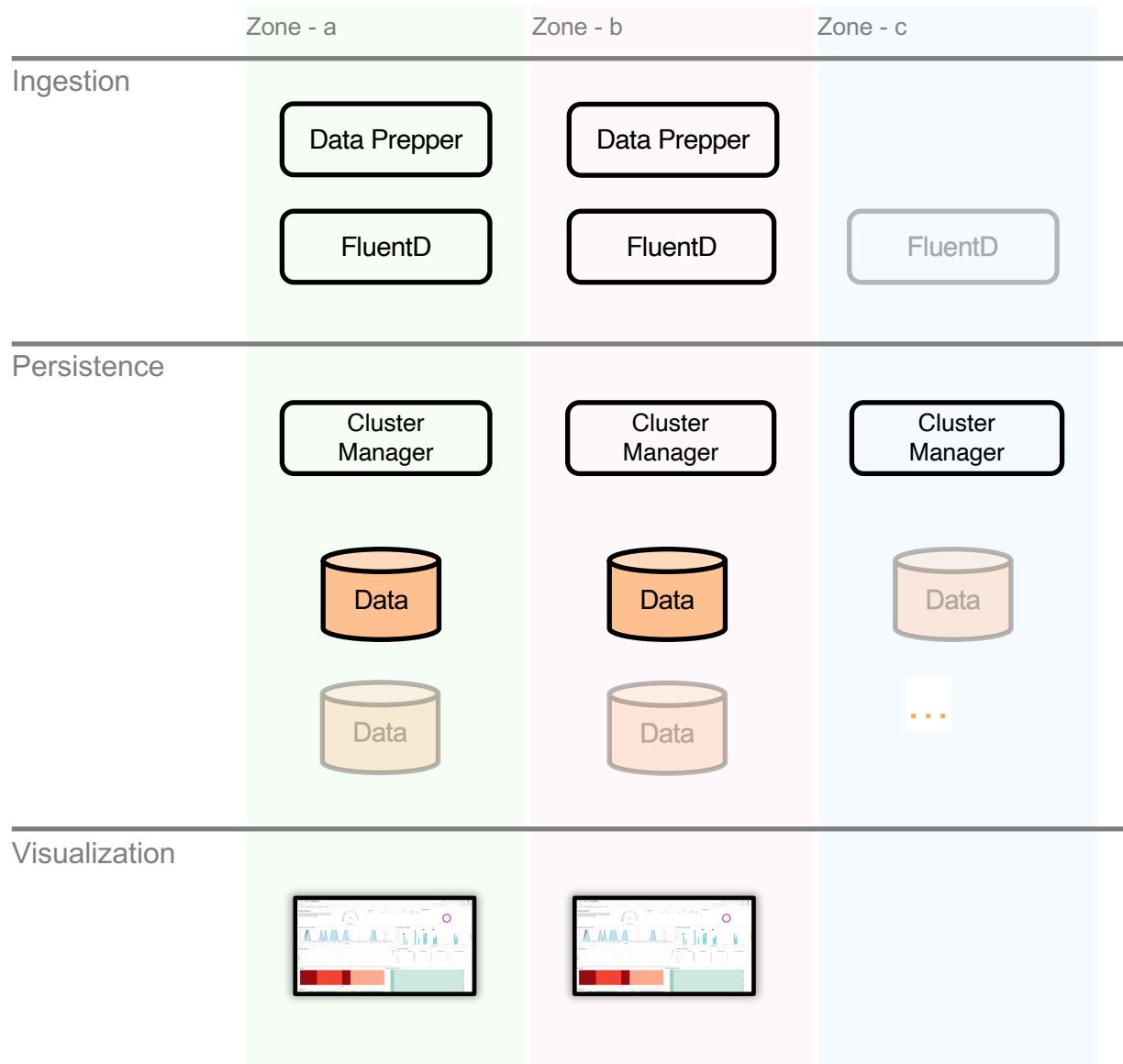
OpenSearch Setup 2



Control Components



Monitoring Components



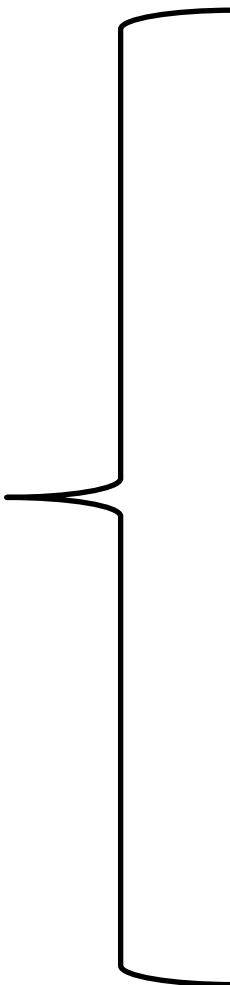
OpenSearch Setup 2



Control Components

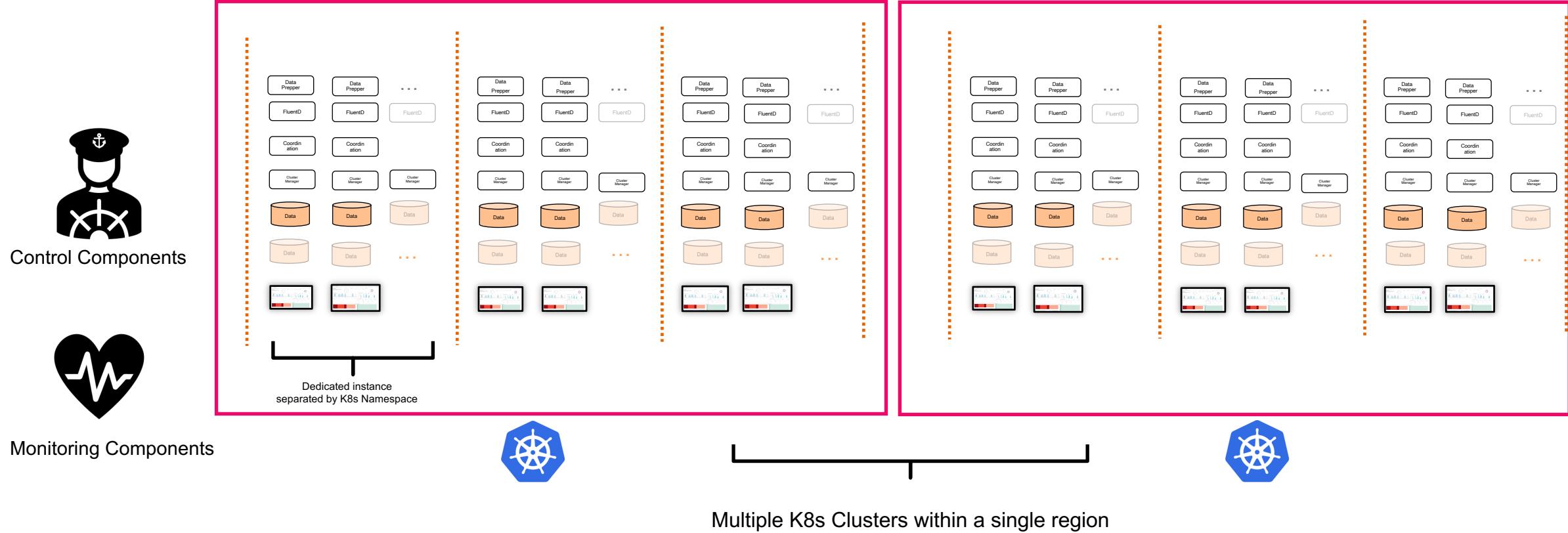


Monitoring Components

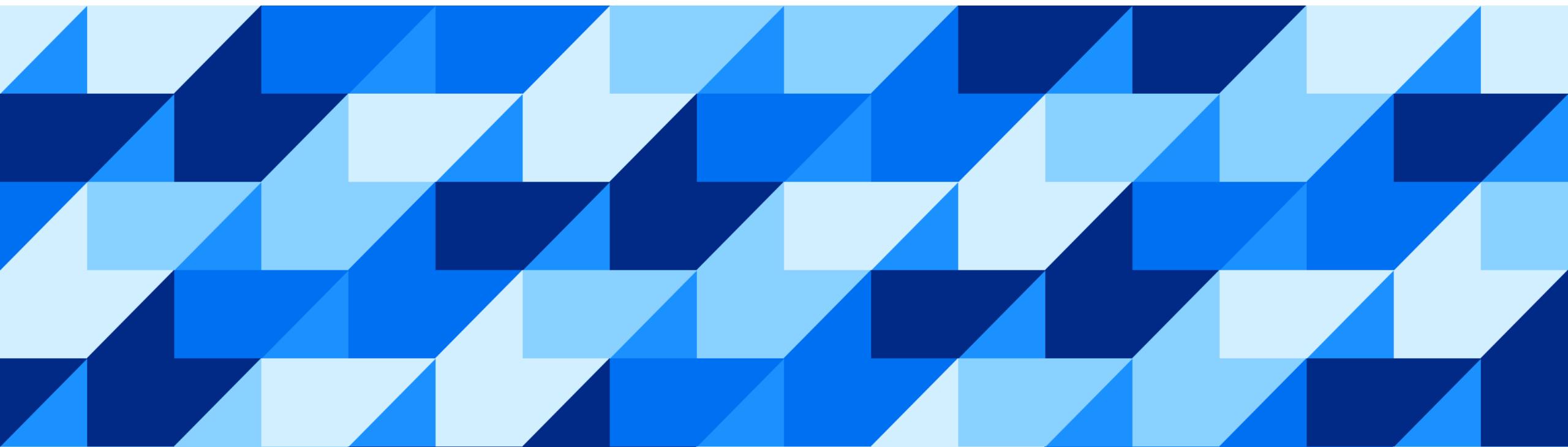


- Instance Lifecycle: **Provisioning**, Binding, Configuration
- **Auto Scaling** based on Disk usage w/ safe draining
- Troubleshooting / Self Healing
- Contents (dashboards, alerts) Manager
- **Backup and Restore** of user contents
- Certificate and Credential Rotation
- Metering / usage reporting
- Health:
 - Availability reporting
 - Self Monitoring
 - Alerting

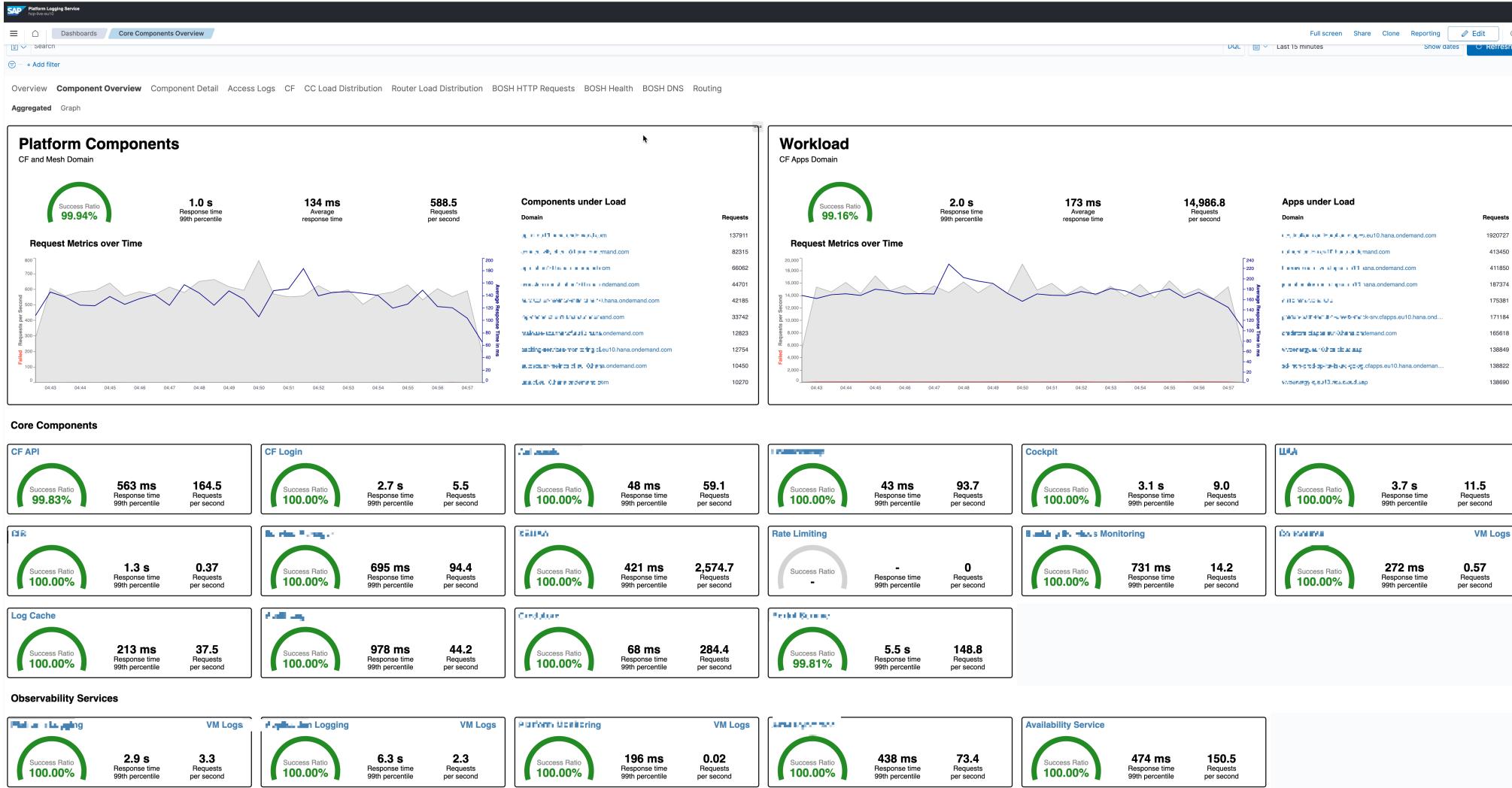
OpenSearch Setup 2: single instance to complete landscape



Use Cases



Log Analytics Use cases: RCA



Log Analytics Use cases: RCA

SAP Platform Logging Service

haproxyAccessLogsDashboard

Search: NOT-3XX x NOT-4XX x NOT-5XX x Contains Hostname x NGF-1XX x NOT CF Application x + Add filter

Full screen Share Clone Reporting Edit Last 15 minutes Show dates Refresh

Navigation: Overview Component Overview Component Detail Access Logs CF CC Load Distribution Router Load Distribution BOSH HTTP Requests BOSH Health BOSH DNS Routing

haproxyAccessLogsDomains

message_host: Descending	Count
sgw-100001.svc.cluster.local	434,101
www-100001.svc.cluster.local	262,023
www-100002.svc.cluster.local	138,792
www-100003.svc.cluster.local	103,833
www-100004.svc.cluster.local	67,885
www-100005.svc.cluster.local	41,951
www-100006.svc.cluster.local	27,624
www-100007.svc.cluster.local	24,819
www-100008.svc.cluster.local	20,917
www-100009.svc.cluster.local	18,048
www-100010.svc.cluster.local	15,912
www-100011.svc.cluster.local	12,086
www-100012.svc.cluster.local	8,617
www-100013.svc.cluster.local	7,932
www-100014.svc.cluster.local	7,495
www-100015.svc.cluster.local	7,063
www-100016.svc.cluster.local	6,451
www-100017.svc.cluster.local	5,924
www-100018.svc.cluster.local	5,713
www-100019.svc.cluster.local	4,698

haproxyAccessLogsStatusCodes

message_code: Descending	Count
200	994,118
401	333,322
404	61,689
400	57,736
304	17,355
202	10,768
302	7,408
503	6,495
301	1,460
201	1,338
204	408
307	399
429	395
403	385
422	183
409	127
500	112
303	81
502	52
415	30

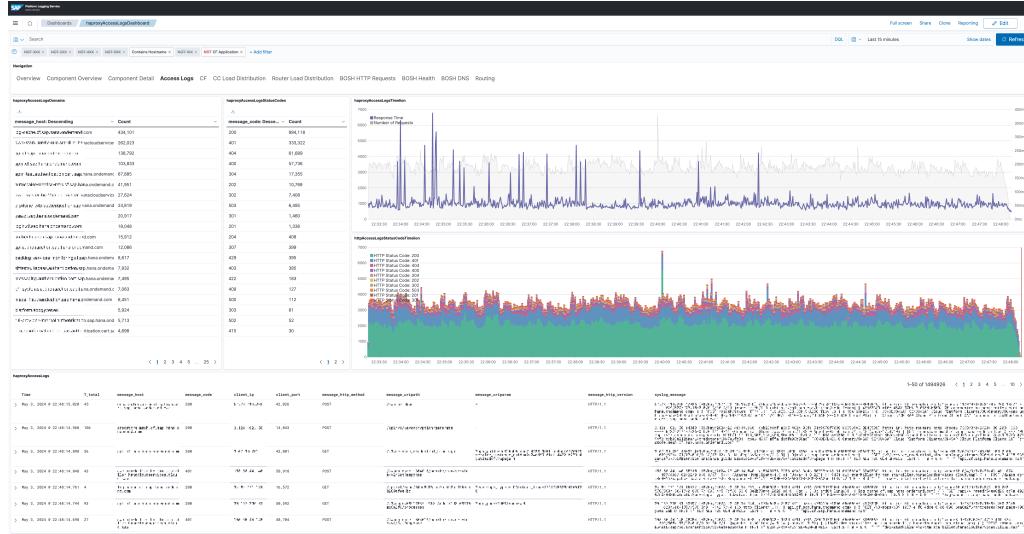
haproxyAccessLogTimeline

httpAccessLogsStatusCodeTimeline

haproxyAccessLogs

Time	T_total	message_host	message_code	client_ip	client_port	message_http_method	message_uripath	message_uriparam	message_http_version	syslog_message
May 3, 2024 02:48:15.828	45	sgw-100001.svc.cluster.local	200	192.168.1.24	42,826	POST	/api/v1/namespaces/default/pods	-	HTTP/1.1	1.12.1.24 - [1002] 2019-05-03T02:48:15.828Z GET /api/v1/namespaces/default/pods [200] 1.12.1.24 - [1002] 2019-05-03T02:48:15.828Z GET /api/v1/namespaces/default/pods [200]
May 3, 2024 02:48:14.968	186	sgw-100001.svc.cluster.local	200	3.121.12.12	14,943	POST	/api/v1/namespaces/default/pods	-	HTTP/1.1	3.121.12.12 - [1002] 2019-05-03T02:48:14.968Z GET /api/v1/namespaces/default/pods [200] 3.121.12.12 - [1002] 2019-05-03T02:48:14.968Z GET /api/v1/namespaces/default/pods [200]
May 3, 2024 02:48:14.898	56	sgw-100001.svc.cluster.local	200	3.121.12.29	43,881	GET	/api/v1/namespaces/default/pods	-	HTTP/1.1	3.121.12.29 - [1002] 2019-05-03T02:48:14.898Z GET /api/v1/namespaces/default/pods [200] 3.121.12.29 - [1002] 2019-05-03T02:48:14.898Z GET /api/v1/namespaces/default/pods [200]
May 3, 2024 02:48:14.848	43	sgw-100001.svc.cluster.local	401	192.168.1.24	58,918	POST	/api/v1/namespaces/default/pods	-	HTTP/1.1	192.168.1.24 - [1002] 2019-05-03T02:48:14.848Z POST /api/v1/namespaces/default/pods [401] 192.168.1.24 - [1002] 2019-05-03T02:48:14.848Z POST /api/v1/namespaces/default/pods [401]
May 3, 2024 02:48:14.761	4	sgw-100001.svc.cluster.local	200	3.121.12.29	16,572	GET	/api/v1/namespaces/default/pods	-	HTTP/1.1	3.121.12.29 - [1002] 2019-05-03T02:48:14.761Z GET /api/v1/namespaces/default/pods [200] 3.121.12.29 - [1002] 2019-05-03T02:48:14.761Z GET /api/v1/namespaces/default/pods [200]
May 3, 2024 02:48:14.744	93	sgw-100001.svc.cluster.local	200	3.121.12.29	58,592	GET	/api/v1/namespaces/default/pods	-	HTTP/1.1	3.121.12.29 - [1002] 2019-05-03T02:48:14.744Z GET /api/v1/namespaces/default/pods [200] 3.121.12.29 - [1002] 2019-05-03T02:48:14.744Z GET /api/v1/namespaces/default/pods [200]
May 3, 2024 02:48:14.698	27	sgw-100001.svc.cluster.local	401	192.168.1.24	48,784	POST	/api/v1/namespaces/default/pods	-	HTTP/1.1	192.168.1.24 - [1002] 2019-05-03T02:48:14.698Z POST /api/v1/namespaces/default/pods [401] 192.168.1.24 - [1002] 2019-05-03T02:48:14.698Z POST /api/v1/namespaces/default/pods [401]

Log Analytics Use cases: RCA



> Apr 10, 2024 @ 05:08:32.284 finance-prod [/var/vcap/packages/whitelist-plugin]: 2024/04/10 05:13:18 [INFO] Attempted access to forbidden resource POST /api/finance/value/. [request_id: 8b19e78a-3894-25f5-8efe-20bb0c4f19f0]

> Apr 10, 2024 @ 05:08:31.516 frontend-proxy-blue [/var/vcap/packages/plugin]: 2024/04/10 05:08:31 [INFO] Time taken to fetch scopes user '5bc53f10-a47a-36ae-b898-858586c6bc34' 2.33876ms. [request_id: 8b19e78a-3894-25f5-8efe-20bb0c4f19f0]





SAP Service
Teams



External
Customer

Use cases: Service Performance / Quality

SAP Application Logging Service

Overview Four Golden Signals Usage Performance and Quality Requests and Logs Statistics Help Legacy

All Signals Latency Traffic Errors Saturation

Latency (view details)

Successful Requests

Average Responsetime **126.77 ms**

Failed Requests

Average Responsetime **536.18 ms**

Errors (view details)

Errors / Not Found

Error percentage (Status > 400) **16.658%**

Drill Down

Organizations

Name	Count
SPS-120	273,622
SPS-120-1234567890	3,761
SPS-120-1234567890-1234567890	3,503,976
SPS-120-1234567890-1234567890-1234567890	36,256,594

Spaces

Name	Count
SPS-120	71,925,854
SPS-120-1234567890	38,256,476
SPS-120-1234567890-1234567890	8,860,017
SPS-120-1234567890-1234567890-1234567890	6,532,376
SPS-120-1234567890-1234567890-1234567890-1234567890	4,288,333

Traffic (view details)

Requests per Second

SAP Application Logging Service

Overview Four Golden Signals Usage Performance and Quality Requests and Logs Statistics Help Legacy

All Signals Latency Traffic Errors Saturation

CPU load

Average CPU **8.713%**

Max CPU **1,373.997%**

Container Memory Usage

Average Memory **25.533%**

Max Memory **96.656%**

Disk Load

Average Disk **24.841%**

Max Disk **100%**

Drill Down

Organizations

Name	Count
SPS-120	273,605

Spaces

Name	Count
prod	71,767,632

Components

Name	Count
SPS-120-1234567890-1234567890-1234567890-1234567890	36,074,881

Instances

Name	Count
[1, "2"]	1

Traffic (view details)

Network Traffic per Second

SAP Application Logging Service

Overview Four Golden Signals Usage Performance and Quality Requests and Logs Statistics Help Legacy

All Signals Latency Traffic Errors Saturation

CPU usage per component

Max CPU usage by component

component	Used CPU Percent
SPS-120-1234567890-1234567890-1234567890-1234567890	1,373.997%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890	933.008%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	919.382%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	878.582%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	841.887%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	834.739%
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	740.389%

Memory usage per component

Max Memory usage by component

component	Memory usage in percent	Memory usage absolute	Memory Quota
SPS-120-1234567890-1234567890-1234567890-1234567890	96.656%	123.7MB	10GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890	95.237%	243.8MB	25GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	69.826%	3.6GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	88.922%	3.6GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	84.488%	3.4GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	81.599%	3.3GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	79.076%	3.7GB	4GB

Disk usage per component

Max Disk usage by component

component	Disk usage in percent	Disk usage absolute	Disk Quota
SPS-120-1234567890-1234567890-1234567890-1234567890	100%	500MB	2GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890	83.527%	3.3GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	83.527%	3.3GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	83.072%	3.3GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	79.076%	1.2GB	4GB
SPS-120-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890-1234567890	79.076%	1.2GB	4GB

Use cases w/ Open Telemetry: Logs, Metrics, Traces

SAP Cloud Logging cls
?

☰ Dashboard / [OTel] K8s Container Metrics
 Full screen Share Clone Reporting Edit

Namespace Name	#Pods
kyma-system	23
example	20
istio-system	3
test	1
47	

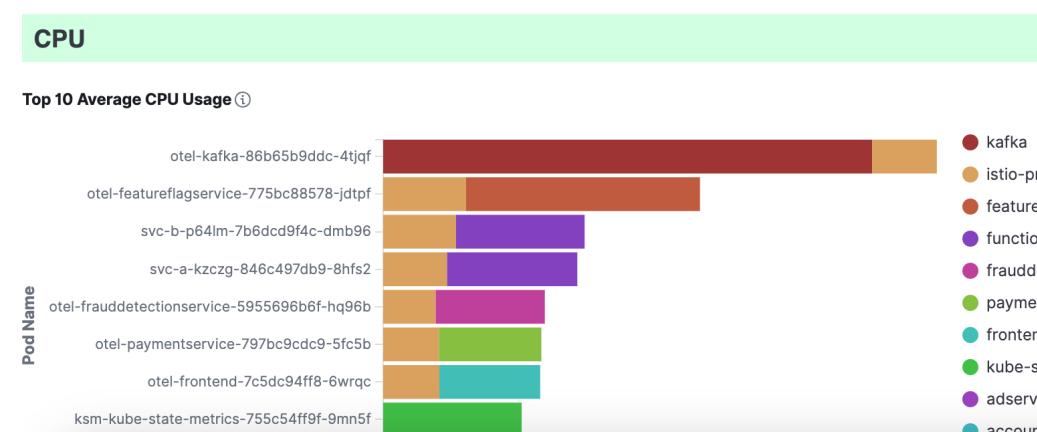
Pod Name	#Containers
otel-accountingservice-6f86dcf4b6-872kr	2
otel-adservice-7bd4c79675-wfml9	2
otel-cartservice-55447ff54f-cd2dr	2
otel-checkoutservice-5b8df4cccd-m85wv	2
otel-currencyervice-c9dbd8b6f-thcj7	2
otel-emailservice-7795877686-r2lrl	2
otel-featureflagservice-775bc88578-jdtpf	2
otel-ffspostgres-6dff6c5f65-kq4v8	2
otel-frauddetectionservice-5955696b6f-hq96b	2
otel-frontend-7c5dc94ff8-6wrqc	2
51	

Container Name	#Metrics
istio-proxy	20
accountingservice	11
adservice	11
cartservice	11
checkoutservice	11
currencyervice	11
emailservice	11
featureflagservice	11
ffspostgres	11
frauddetectionservice	11
240	

Export: [Raw](#) [Formatted](#)

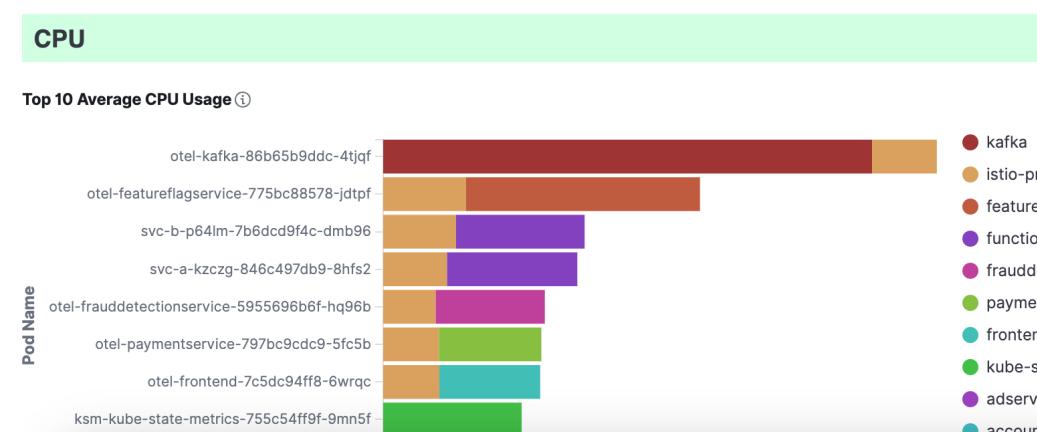
CPU

Top 10 Average CPU Usage ⓘ



Pod Name	Avg CPU Usage
otel-kafka-86b65b9ddc-4tjqf	~0.95
otel-featureflagservice-775bc88578-jdtpf	~0.75
svc-b-p64lm-7b6dc9f4c-dmb96	~0.65
svc-a-kzcwg-846c497db9-8hfs2	~0.65
otel-frauddetectionservice-5955696b6f-hq96b	~0.60
otel-paymentservice-797bc9cdc9-5fc5b	~0.55
otel-frontend-7c5dc94ff8-6wrqc	~0.50
ksm-kube-state-metrics-755c54ff9f-9mn5f	~0.45

Top 3 Pods Container CPU Time ⓘ



Pod Name	Container Name	CPU Time
otel-kafka-86b65b9ddc-4tjqf	kafka	~0.85
otel-ffspostgres-6dff6c5f65-kq4v8	istio-proxy	~0.15
otel-adservice-7bd4c79675-wfml9	featureflagservice	~0.10

Export: [Raw](#) [Formatted](#)

1 2 3 4 »

1 2 3 »

40

Use cases w/ Open Telemetry: Logs, Metrics, Traces

SAP Cloud Logging TravelAgency

Dashboard / OTEL Spans and Logs

traceld: 5605bfe2b67b34ad96c2a8280b1419d + Add filter

Spans and Logs Metrics

Server Spans

Time	serviceName	traceld	name	span.attributes.http@status_code	durationInNanos
> Apr 29, 2024 @ 13:06:52.815448935	sflight-srv	5605bfe2b67b34ad96c2a8280b1419d	POST /processor/**	-	166,941,619

1-1 of 1 < >

Details

Log Events by Traceld ⓘ

traceld: Descending ⓘ Count ⓘ

5605bfe2b67b34ad96c2a8280b1419d 7

Export: Raw ⓘ Formatted ⓘ

SAP Cloud Logging TravelAgency

Dashboard / [OTel] JVM Metrics

Logs

Garbage Collection

Time	serviceName	traceld	severityText	instrumentatio
> Apr 29, 2024 @ 13:06:52.944000000	sflight-srv	5605bfe2b67b34ad96c2a8280b1419d	INFO	com.sap.cap.sfl
> Apr 29, 2024 @ 13:06:52.944000000	sflight-srv	5605bfe2b67b34ad96c2a8280b1419d	INFO	com.sap.cap.sfl
> Apr 29, 2024 @ 13:06:52.944000000	sflight-srv	5605bfe2b67b34ad96c2a8280b1419d	INFO	com.sap.cap.sfl
> Apr 29, 2024 @ 13:06:52.944000000	sflight-srv	5605bfe2b67b34ad96c2a8280b1419d	INFO	com.sap.cap.sfl

GC Counts by GC Name

Copy 2
MarkSweepCompact 0

GC Rate per Second by GC Name

per 60 seconds

GC Time Slice per Second by GC Name

per 60 seconds

CPU

JVM CPU Time Slice per Second

per 60 seconds

Classes

Total Class Count

per 60 seconds

Classes Loaded

per 60 seconds

Classes Unloaded

per 60 seconds

Known Challenges



Parallel update of 7000+ clusters



Shard count/sizing during autoscaling



Size based curation for log index via ISM

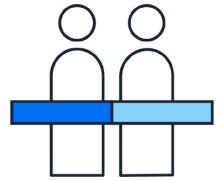
- Currently implemented externally



Data Prepper enhancements



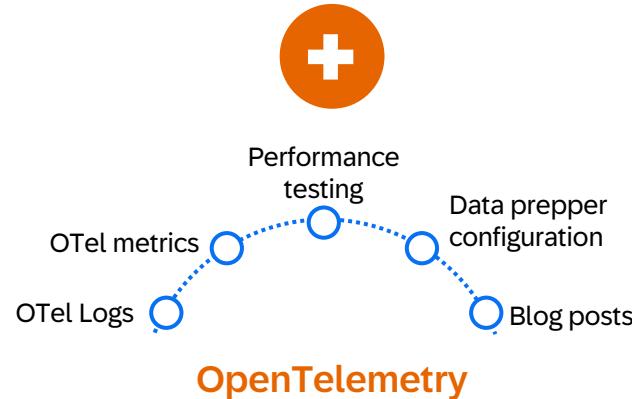
Handling customer misconfiguration



SAP Cloud Logging team + OpenSearch community

SAP customers expect a unified, business-centric and open SAP Business Technology Platform. Our observability strategy uses Elasticsearch as a major enabler. OpenSearch provides a true open source path and community-driven approach to move this forward.

JAN SCHAFFNER
SVP AND HEAD OF BTP FOUNDATIONAL PLANE
SAP



Tech Talk: [How SAP analyzes OpenTelemetry signals using Data Prepper](#)



[Maintainer for Data Prepper](#)

Merged divenable merged 2 commits into opensearch-project:main from divenable:maintainers-KarstenSchnitter 3 weeks ago

Conversation 3 Commits 2 Checks 49 Files changed 2

divenable commented last month Member

Description

Adding @KarstenSchnitter as voted upon by the existing Data Prepper maintainers per the [maintainer guidelines](#). Karsten has lead efforts at SAP to introduce new features into Data Prepper. In particular, his contributions provided support for OTel Metrics and OTel Logs.

Some PRs where he is listed as an author or co-author:

- g24 Update Armeria Version #1507
- Support OpenTelemetry Logs #1372
- Support remaining OpenTelemetry Metrics proto spec features #1154
- Support OpenTelemetry Metrics #1154
- Select require_alias for OS bulk inserts from ISM Policy #3560
- Add Support for OTel Log SeverityText #3280 #3281

By submitting this pull request, I confirm that my contribution is made under the terms of the Apache 2.0 license. For more information on following Developer Certificate of Origin and signing off your commits, please check [here](#).

Thank you

Contact information:

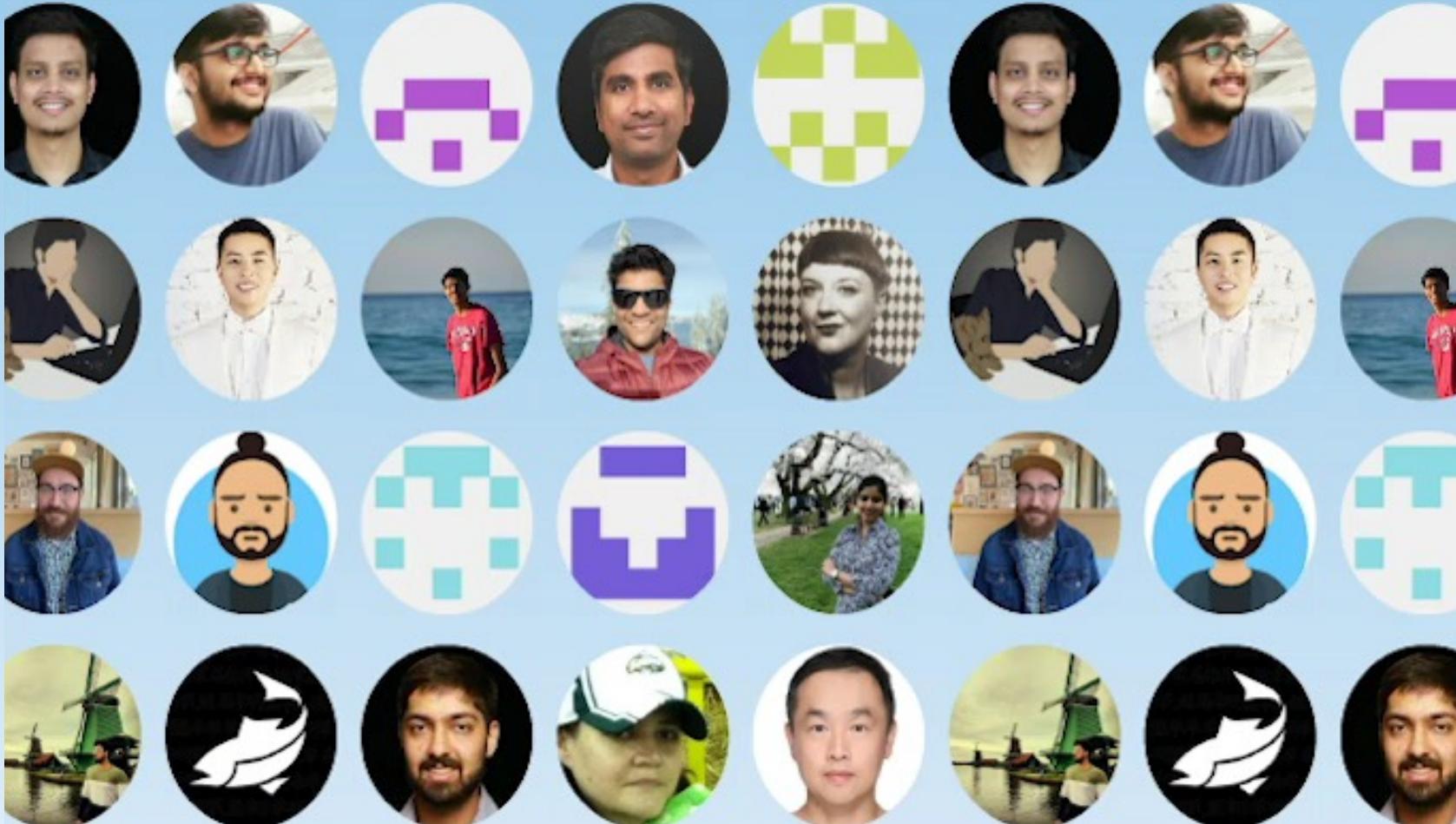
Hariharan Gandhi

hariharan.gandhi@sap.com

 [@hariharangandhi](https://www.linkedin.com/in/hariharangandhi)

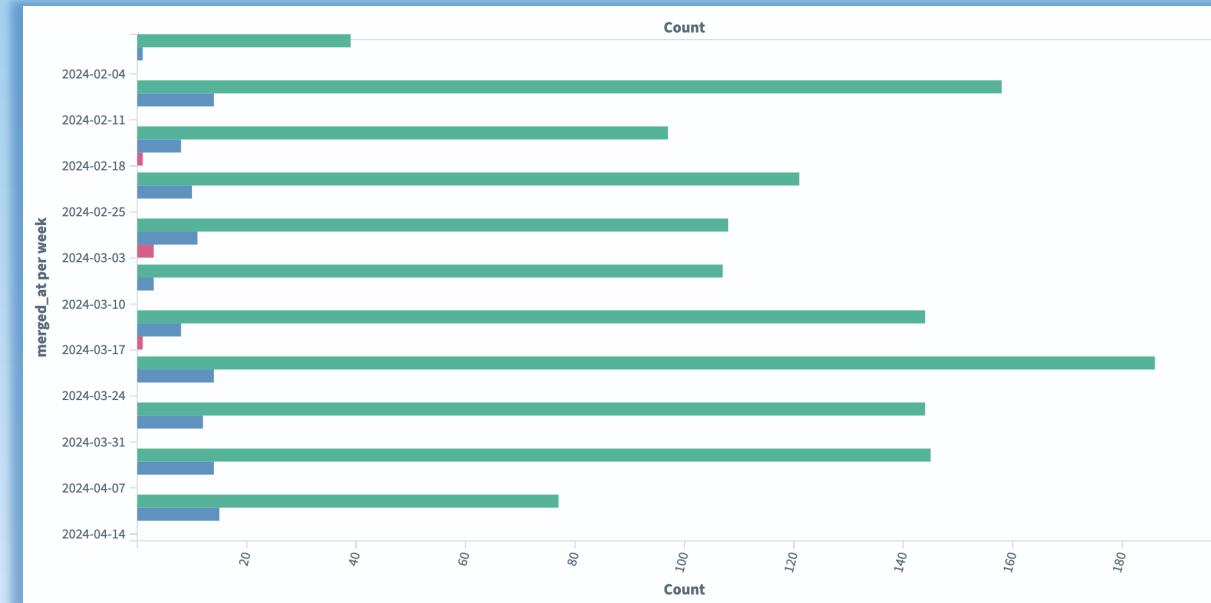


Community-powered innovation

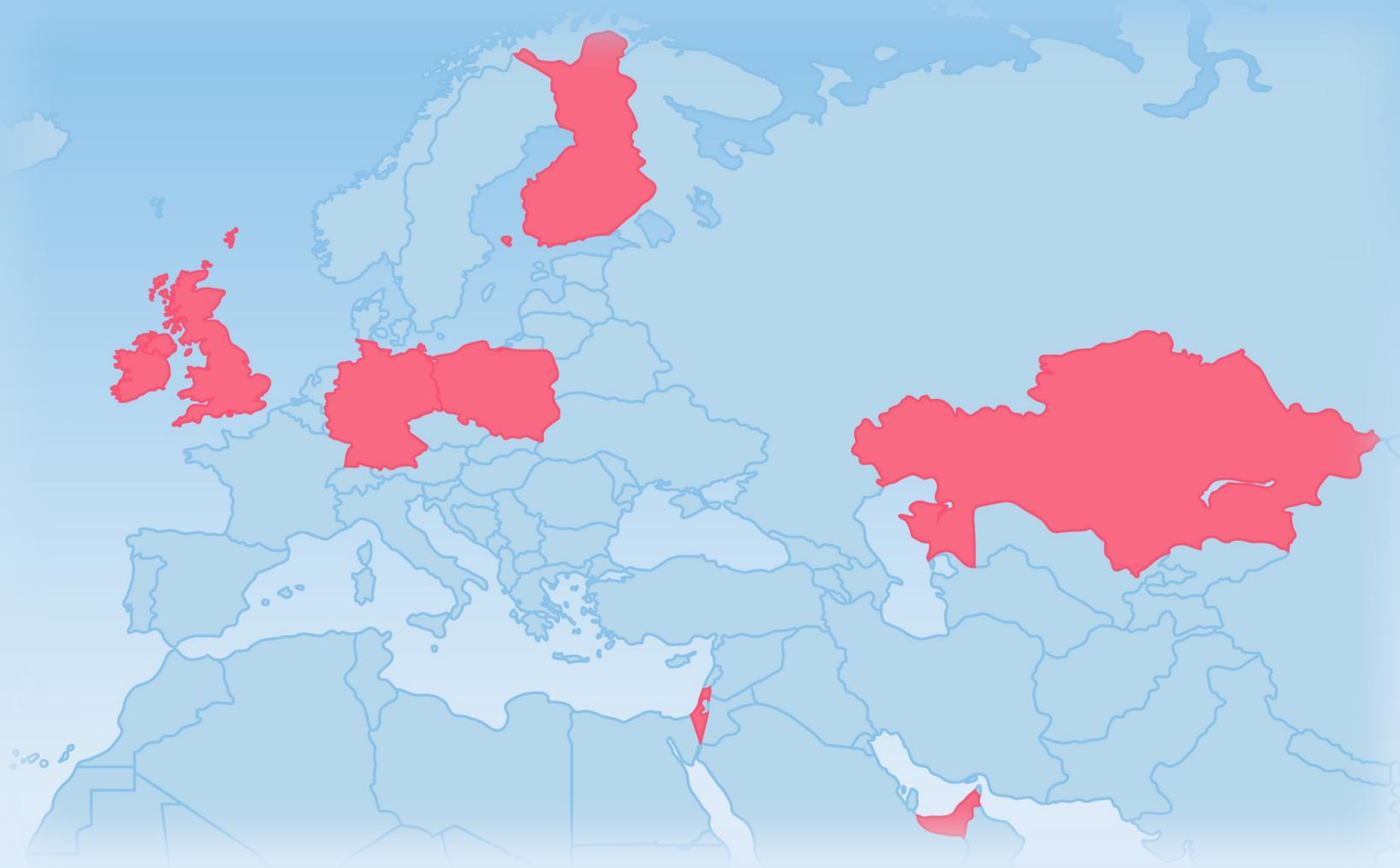


Community contributions

- 2000+ Contributors outside of AWS
 - *Oracle, Aiven, Aryn, ByteDance, SAP, Intel, IBM, and more*
- Weekly average of 100+ contributions



Community contributions



Community-led dialogue

The screenshot shows a Slack channel interface with a dark theme. On the left, there's a sidebar with a list of channels, including "# security-analytics" which is currently selected and highlighted in blue. The main area displays a conversation in the "# security-analytics" channel.

Shawn Houston 10:38 AM
Not sure if this is a bug so I am going to ask here:
image.png

A modal window titled "Data source" is open, showing a dropdown menu labeled "Select or input source indexes or index patterns". The dropdown is set to "Indices" and lists several indices:

- nqt-inventory-static
- metrics-v2.4.0-20240423
- nqt-activity-20240424
- nqt-activity-20240425
- metrics-v2.4.0-20240425
- metrics-v2.4.0-20240424

That drop down has indices as a list - should there also be a list of index patterns in that drop down?

Kevin Garcia 1:48 PM
Index patterns are dashboards saved objects. The backend has no awareness of index patterns. I would say this is a UI bug cc: [@Xenia Tupitsyna](#) -- The field label should be [Select or input source indexes](#), and the helper text underneath the input should clarify that you can enter * as a wildcard pattern to match multiple indexes. -- try typing `nqt-activity*` and hitting return, and see if that gives you what you need (edited)

Xenia Tupitsyna 3:06 PM
@Shawn Houston Please feel free to add more context here: [#995 \[BUG\]](https://github.com/opensearch-project/security-analytics-dashboards-plugin/issues/995)
What is the bug?
The "Indexes" field in "Create threat detector" flow gives a wrong impression that user can use frontend index patterns as a source for threat detection.
https://playground.opensearch.org/app/opensearch_security_analytics_dashboards#/create-detector
Screenshot 2024-04-25 at 3 02 30 PM
What is the expected behavior?
To clarify the meaning of the field, the field label should be [Select or input source indexes or aliases](#), and the helper text underneath the input should clarify that user can enter * as a wildcard pattern to match multiple indexes as [Use * as a wildcard pattern to match multiple sources](#).

Screenshot 2024-04-25 at 3 04 08 PM
Labels

Global gatherings

 OpenSearchCon

EUROPE | Berlin 2024



 OpenSearchCon

INDIA | Bengaluru 2024



 OpenSearchCon

NORTH AMERICA | San Francisco 2024



 OpenSearchCon

EUROPE | Berlin 2024

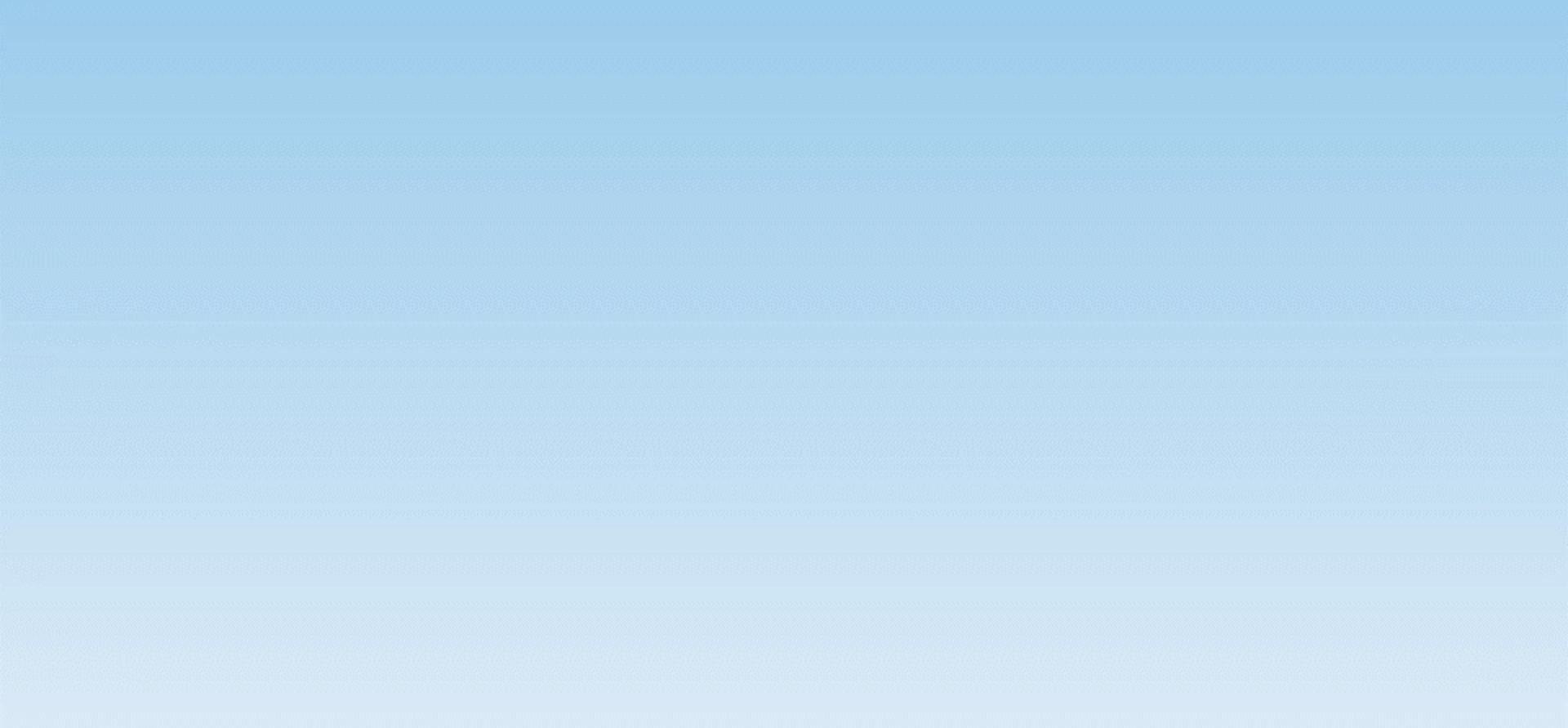


Downloads to date

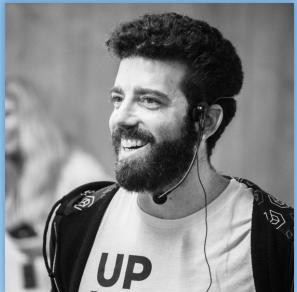
0 0 0 0 0 0 0 0 0



70+ Partners and Counting



A more open OpenSearch



Amitai Stern



Anandhi Bumstead



Andriy Redko



Charlotte Henkle



Eli Fisher



Grant Ingersoll



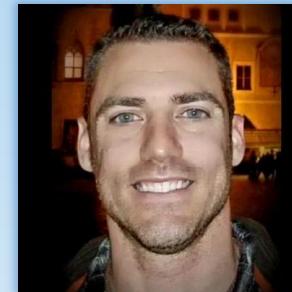
Jonah Kowall



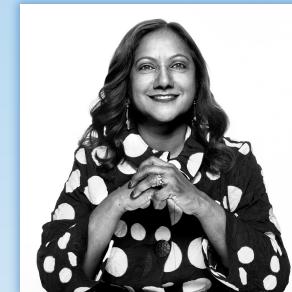
Kris Freedain



Mehul A. Shah



Nick Knize



Nithya Ruff



Samuel Herman



THANK YOU | DANKE



EUROPE | BERLIN 2024