AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

ANT203

What's new in Amazon OpenSearch Service

Mehul A. Shah (he/him)
GM: OpenSearch, CloudSearch, Lake Formation
Amazon Web Services

Wei Zhu (he/him)
Staff Software Engineer Observability
Pinterest

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Amazon OpenSearch Service

The OpenSearch project

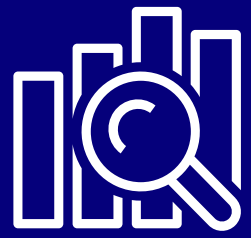
Cost at scale

Machine learning in the open

The road ahead

Pinterest: Logsearch at Pinterest

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



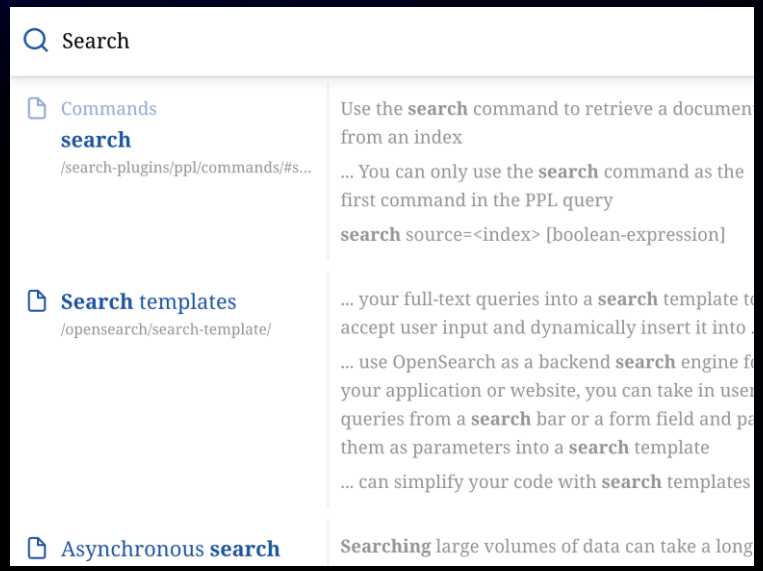
Amazon OpenSearch Service

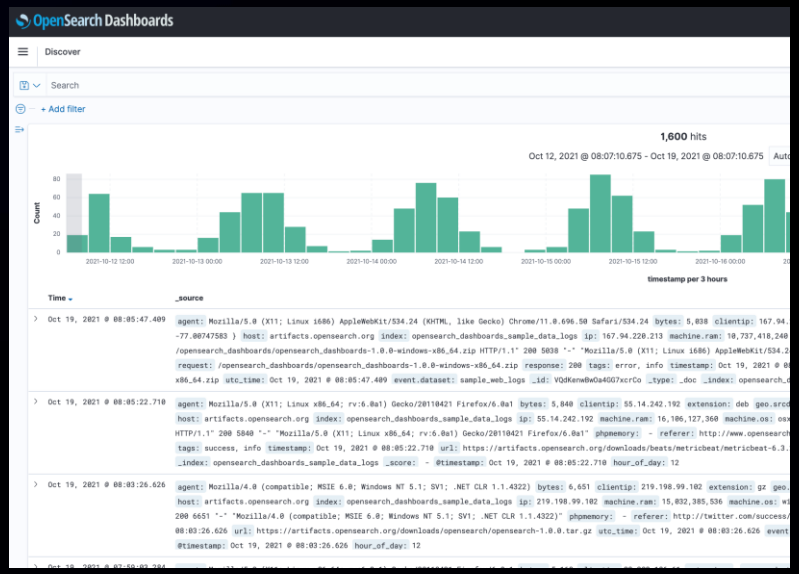
Amazon OpenSearch Service
(successor to Amazon Elasticsearch Service)

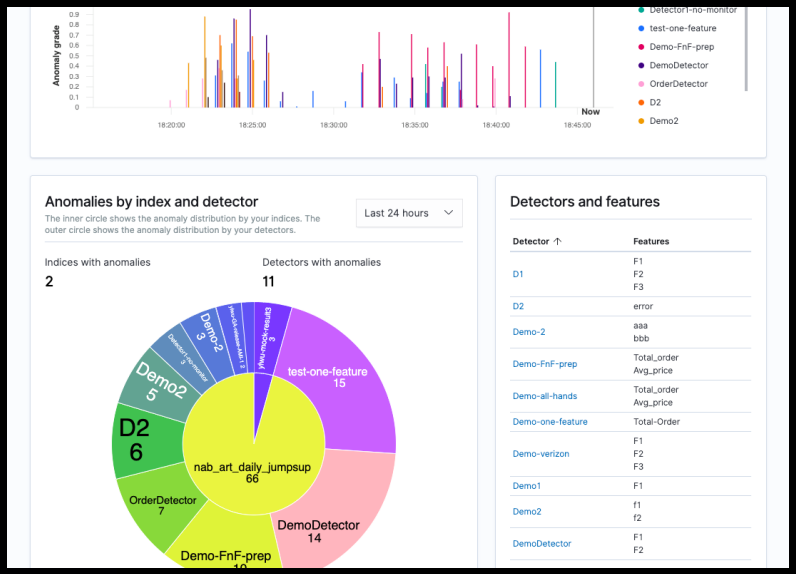
A managed service that makes it easy to **deploy**, **operate**, and **scale OpenSearch** and legacy Elasticsearch clusters on the AWS Cloud

© 2021, 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

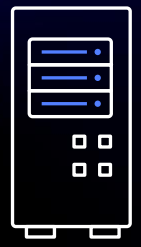
Analysis

Time-based visualizations

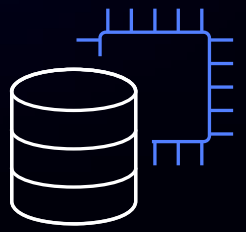
Nestable statistics

Time series tools

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Server, application, network, AWS, and other logs

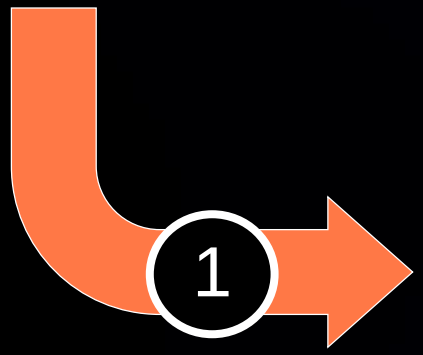


Application data

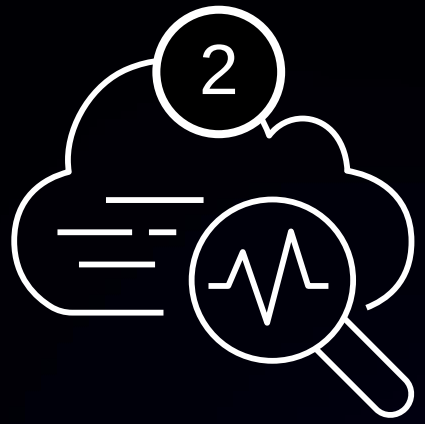


Application users, analysts, DevOps, and security

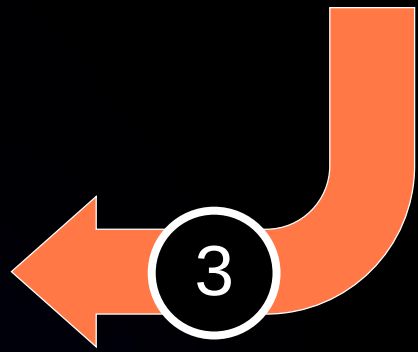
Indexed and instantly searchable



JSON documents



Amazon OpenSearch Service domain



Rest APIs, clients, and OpenSearch Dashboards

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Search, analyze, and visualize log data



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service customers

Software and internet

Adobe · IAC · AUTODESK

Education technology

McGraw Hill Education · INSTRUCTURE · Blackboard

BioTech and pharma

MONSANTO · Bristol-Myers Squibb

Financial services

THOMSON REUTERS · stripe · KICKSTARTER

Media and entertainment

mlbam · NETFLIX · FOX

Social media

Pinterest · ancestry · Nextdoor

Telecommunications

Jio · COMCAST · T-Mobile

Travel and transportation

lyft · Expedia · UBER

Real estate

Zillow · move

Logistics and operations

here · elementum · infor

Publishing

FT FINANCIAL TIMES · ELSEVIER · The Washington Post

Other

Canon · SAMSUNG · British Gas

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We've been busy …

Remote reindex support

Data Prepper

Cross-cluster replication

Data streams

Lucene 8.9

k-NN with Hamming distance

SAML/ADFS auth

Random Cut Forest 2

High cardinality anomaly detection

Output plugin for Logstash

Bucket-level alerting

JavaScript client

Piped Processing Language

Historical data analysis for anomaly detection

Asia Pacific (Osaka) Region

Python client

Upgrade tool

Service notifications via Amazon EventBridge

Gantt visualizations

Arm 64/AWS Graviton2

Asynchronous search

Dashboards reports

PPL auto-complete

Tag-based auth

Trace Analytics

Microsoft Power BI integra

Unified notifications

Auto-Tune for memory management

Custom dashboard branding

Africa (Cape Town) Region

Encryption on existing domains

Shard-level indexing back pressure

Elasticsearch 7.10

Custom domain names

Alerting on HTTP inputs

Grafana – OpenSearch plug-in

Overallocated shard prevention

Unified anomaly detection UI

k-NN with FAISS

Elasticsearch 7.9

Index rollups

Europe (Stockholm) Region

50+ features since re:Invent 2020

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OpenSearch Project



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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why OpenSearch?

Community-driven

AWS is the steward

Made with your input

Public roadmap

Welcome contributions

Co-maintainers

100% open source

Apache License, Version 2.0

Use, modify, monetize

Built in the open

No contributor
license agreement

Full featured

Wire-compatible with
Elasticsearch 7.10.2

Full text search

Analytics

Fast ingest

Machine learning

Security

… and more

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What does it mean for you?



A path forward: open-source Elasticsearch users can keep advancing

No lock in: the same software you get from us can be run on-premises or in the cloud

Compatible: no code changes required – including new universal language-specific clients

Innovative: dozens of new features in just first few releases, including: *cross-cluster replication, shard-level back pressure, notebooks, data streams, index transforms, bucket-level alerting, and more*

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service + OpenSearch



Amazon OpenSearch Service

+

OpenSearch

A great home for all of your Elasticsearch and OpenSearch workloads

- Eliminate operational overhead and reduce costs
- Comprehensive integrated security and compliance
- Provided by the stewards of the open-source software

Open source: OpenSearch 1.0–1.2
Amazon OpenSearch Service: OpenSearch 1.0, 1.1 (coming soon – Dec. 2021)

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cost at scale

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecture and scaling

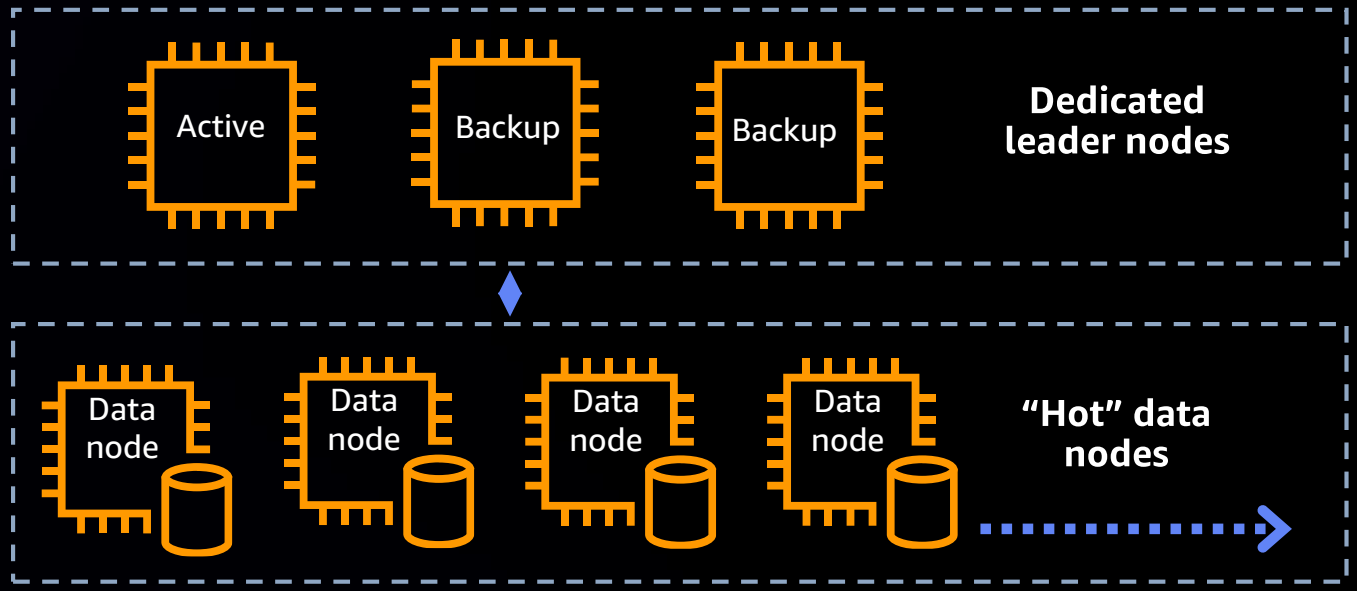
Cluster of Amazon EC2 instances

- Leaders: cluster management
- “Hot” data nodes: store data and handle indexing and search requests

Compute and storage coupling

- High cost at scale

Maximum cluster size: **3 PB**



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

UltraWarm low-cost storage tier

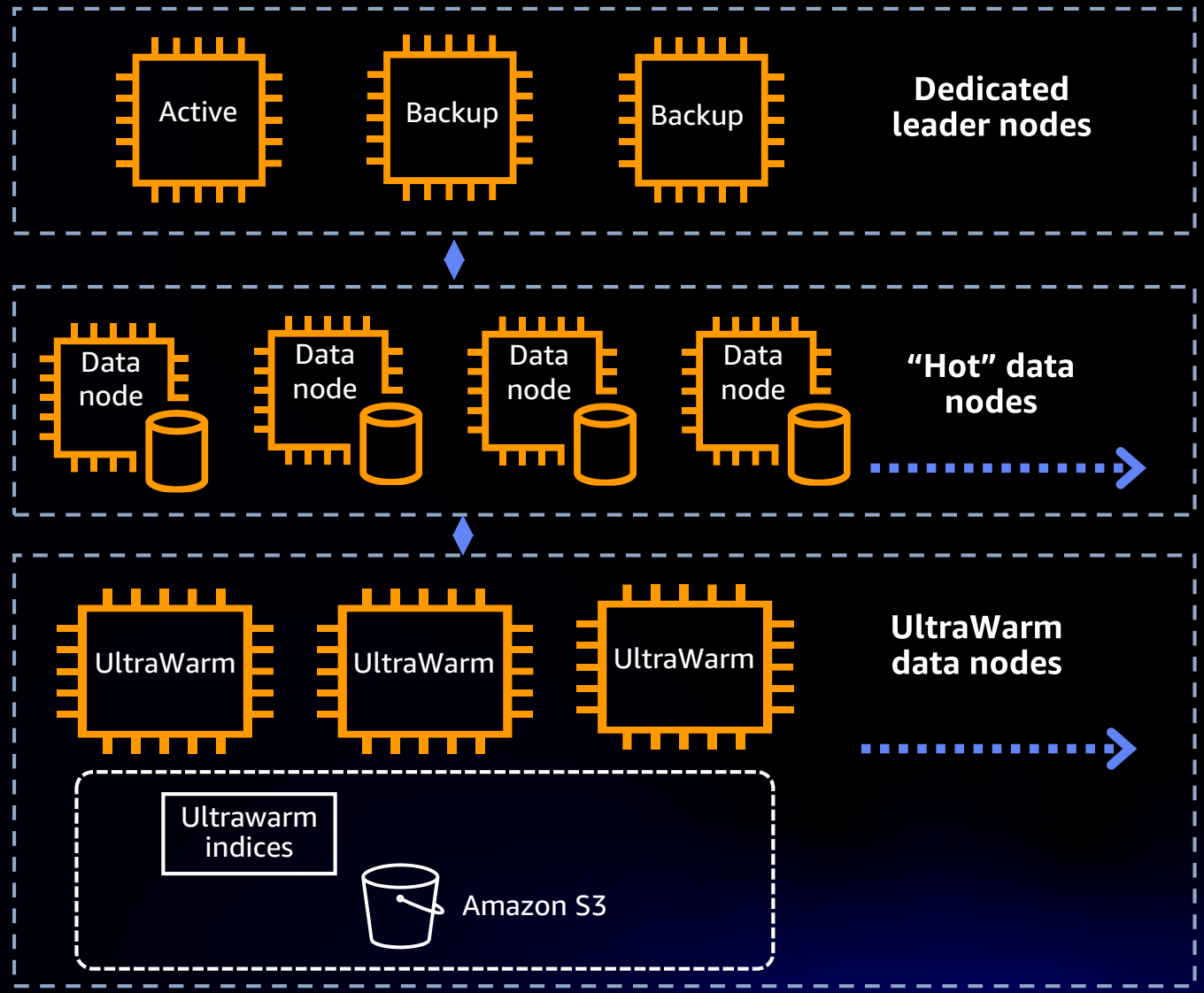
UltraWarm (May 2020) allows you to store older, less frequently accessed data at 90% less cost

UltraWarm data nodes are optimized caching and query nodes for indexes stored in Amazon S3

Fast enough for interactive log analytics and visualization

Maximum cluster size remains **3 PB** as metadata management in leader limits cluster scale

Tradeoff: data in UltraWarm is immutable



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

UltraWarm at Asurion

"We are really excited that **UltraWarm** removes the operational overhead, and reduces cost significantly. We were able to easily migrate our data from the hot nodes to UltraWarm nodes, and use our existing dashboards, without the need to make any changes."

Shyam Rayaprolu, Principal Architect

asurion

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cold storage

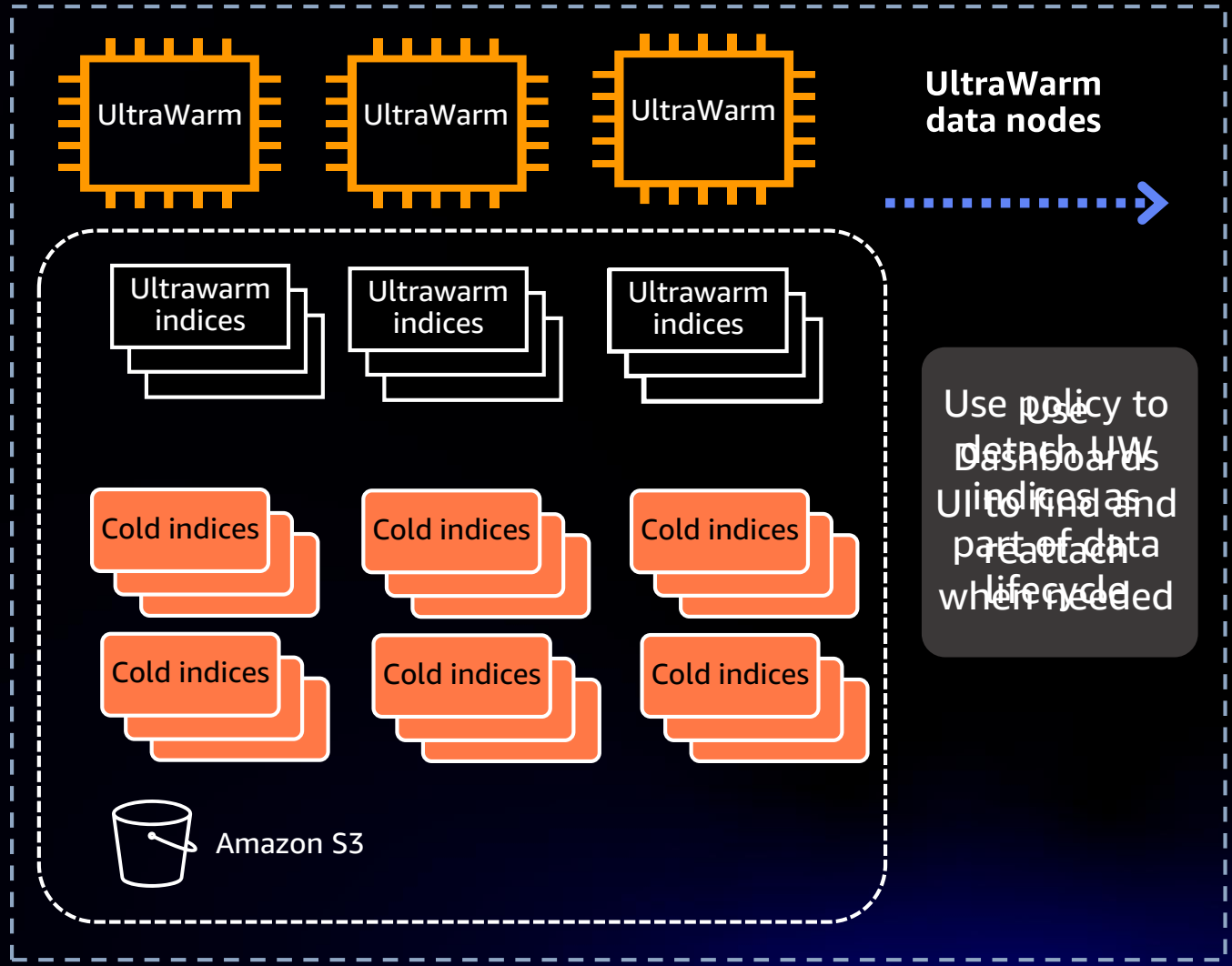
LOWEST COST TIER FOR PERIODICALLY ACCESSED DATA

Cold storage (May 2021) fully decouples/detaches UltraWarm indices from UltraWarm data nodes

Provides a virtually unlimited online archive for your cluster at near S3 prices

Simple discovery UI enables users to find and attach cold indices in seconds

Tradeoff: data is not directly queryable and must be attached before being analyzed



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cold storage at Verizon

"**Cold storage** helps us to increase our log retention timeframe at a much lower cost. Integration is simple and seamless to use, has no additional operational overhead, and helps our team self-serve their requests without compromising query performance."

Raghu Chandran, Sr. Systems Engineer

verizon

aws

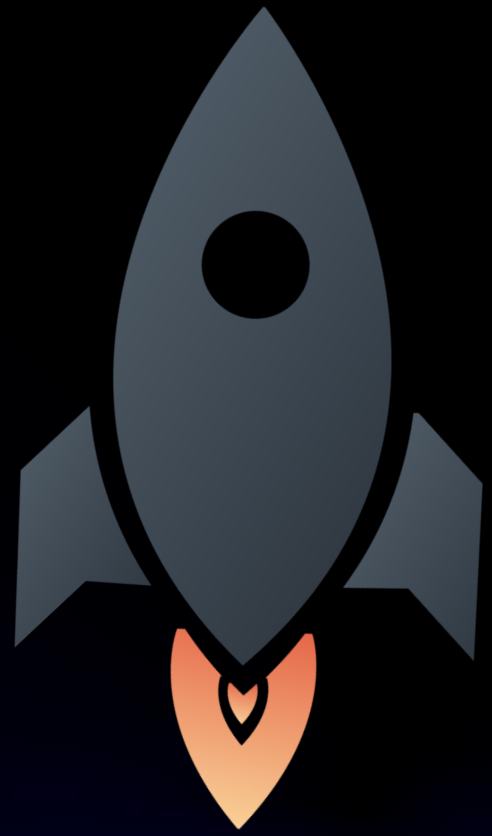
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service auto-tuning

Distributed system complexity can stifle performance

Dependency on workload and data makes tuning difficult

Auto-tuning: continuously monitors, learns, and adjusts to optimize cost and performance

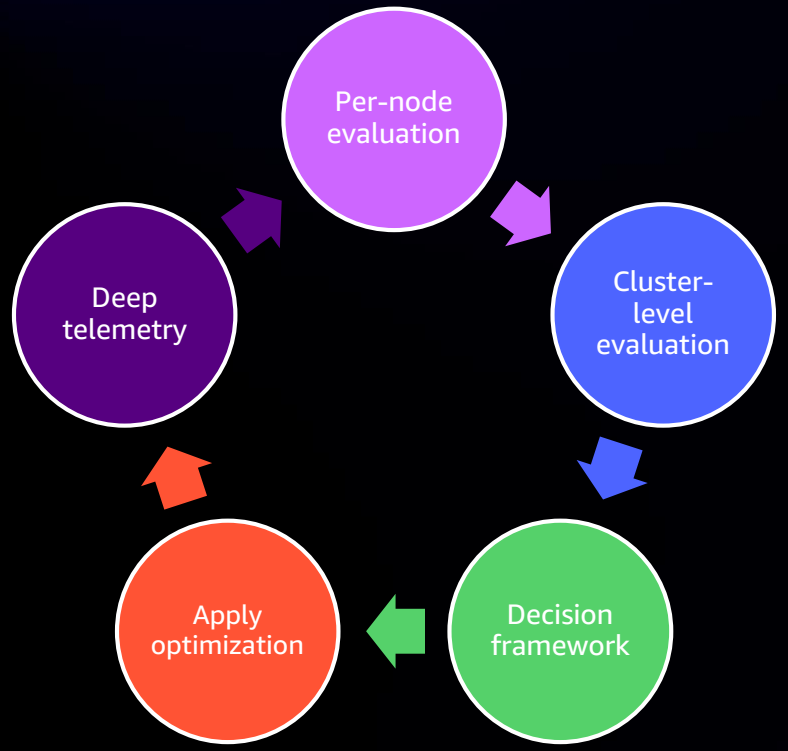


aws

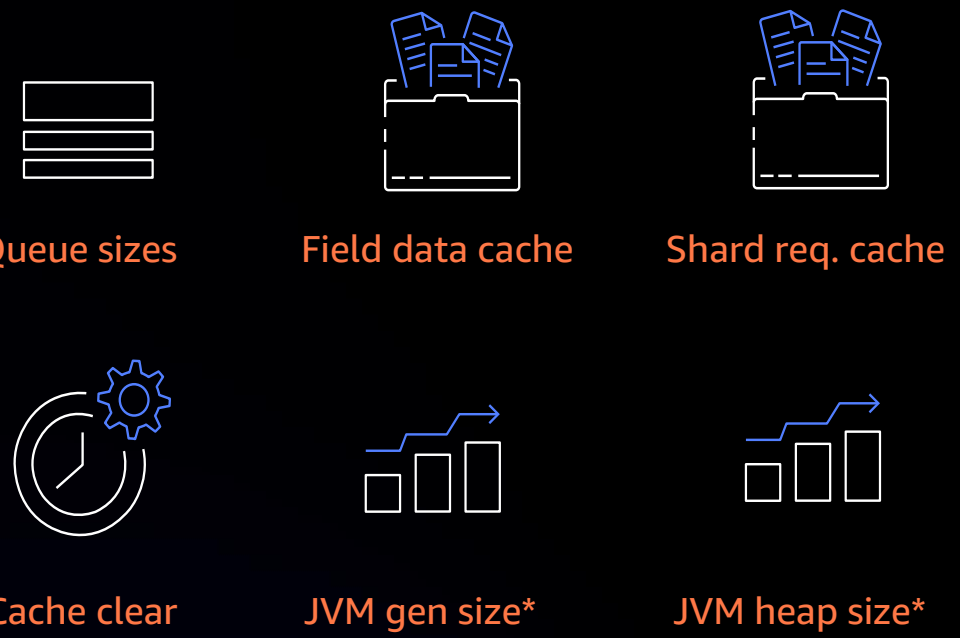
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Auto-Tune

AUTOMATICALLY MAXIMIZES EFFICIENCY AND PERFORMANCE



Virtuous cycle



Parameters tuned

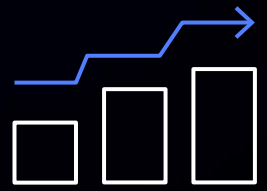
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Auto-Tune customer use case



Use case

Fintech company
2 billion+ business events
Ingest of 2–3 TB / day



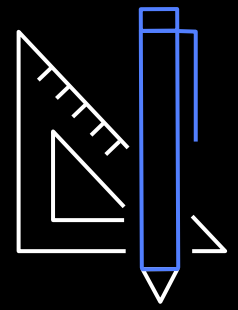
Problem

High JVM memory pressure (JVMMP)
Frequent GC
Indexing and query errors



Auto-Tune

Bulk queue size = 5x
Search queue size = 2x
Heap = 128 G
Enable G1GC



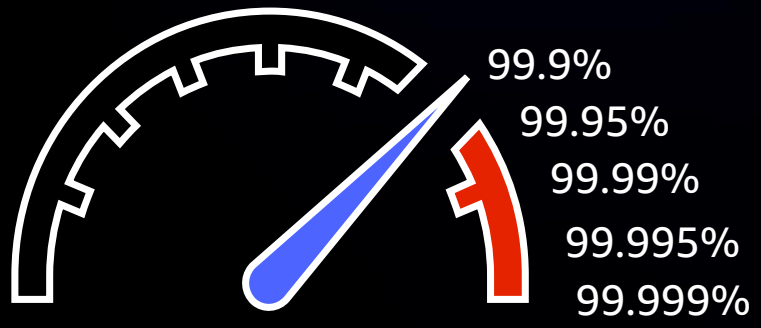
Results

JVMMP down 90%
Throughput ~2X
Error rates 0%

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Achieving high availability



Critical apps need 24x7 operation

Each step in availability is increasingly harder

Sometimes you need more than one cluster

- Dealing with disasters
- Getting closer to your users

Synchronizing can be a challenge

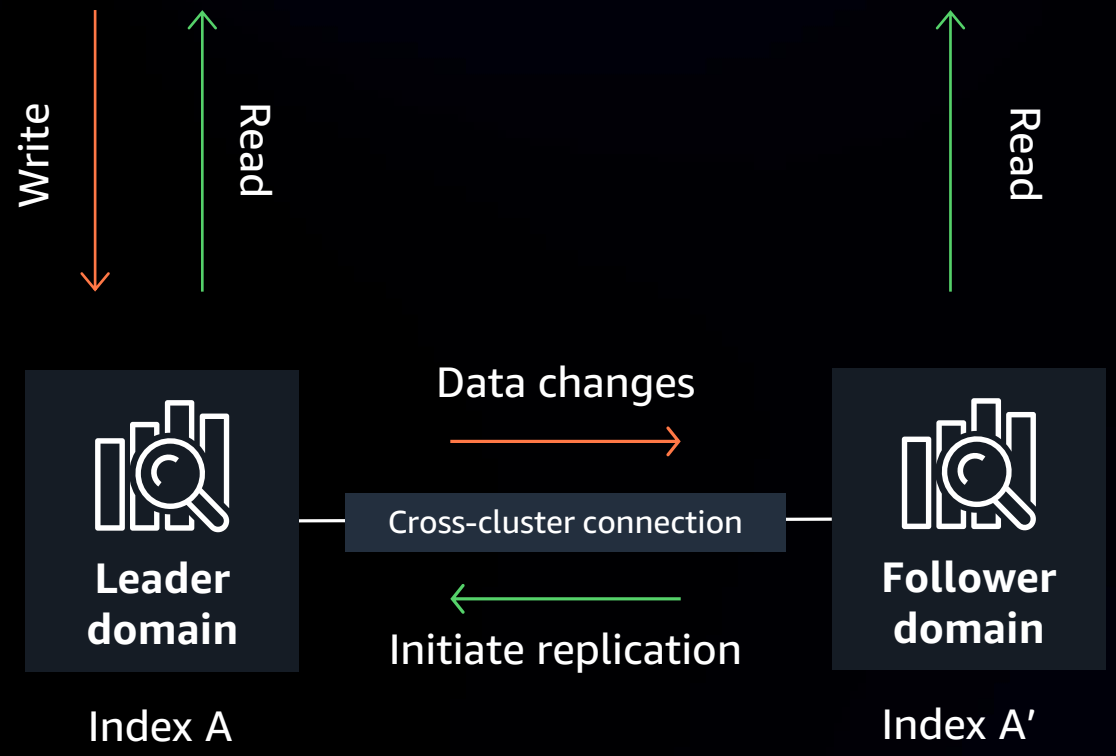
Availability %	Downtime per year	Downtime per month
99.9% ("three nines")	8.77 hours	**43.83 minutes**
99.95% ("three and ½ nines")	4.38 hours	21.92 minutes
99.99% ("four nines")	52.60 minutes	4.38 minutes
99.995% ("four ½ nines")	26.30 minutes	2.19 minutes
99.999% (“five nines”)	5.26 minutes	26.30 seconds

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-cluster replication

HIGH AVAILABILITY, DISASTER RECOVERY, AND DATA PROXIMITY



Elasticsearch 7.10 (available now)

OpenSearch 1.1
(available in open source; coming soon to managed service – Dec. 2021)

Active-passive replication

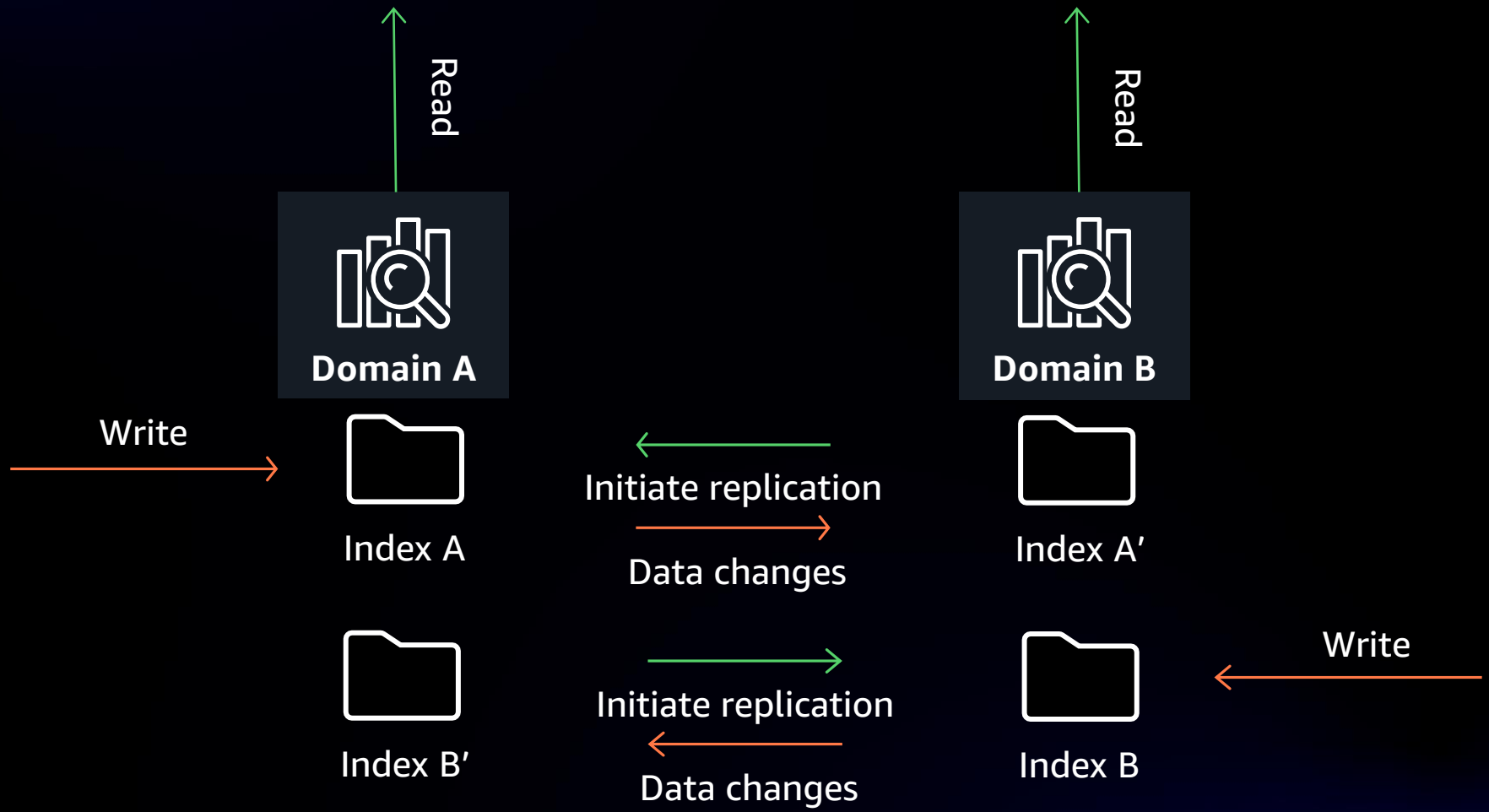
Cross-account and cross-Region support

Sequential consistency and subminute global replication

Granular control at index level — set up many configurations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-cluster replication topologies



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-cluster replication topologies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Machine learning in the open

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Trending use cases for OpenSearch

Time series



Fraud detection

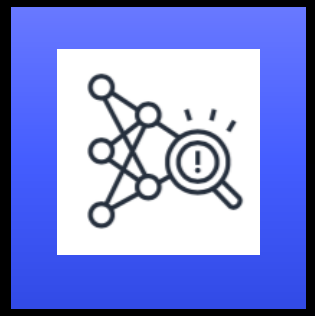


Intrusion detection

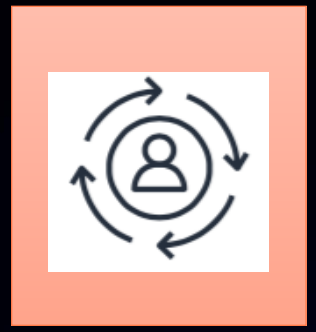


System health monitoring

Search



Product recommendations



Personalization



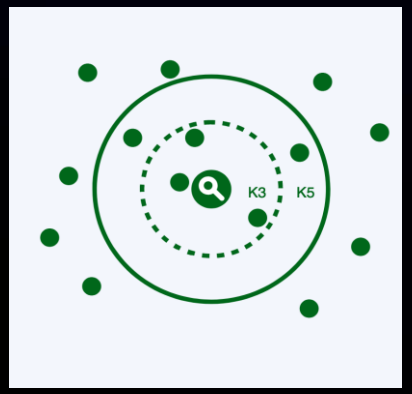
Image search

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Machine learning innovations in OpenSearch

K-Nearest Neighbor (k-NN) for search



Find nearest matches in vectorized space in milliseconds

Updates in real time

Range of distance techniques including: Euclidean, cosine similarity, Hamming distance, FAISS

NOVARTIS

Powers procurement system using OpenSearch k-NN

Help select equipment from 2 million+ items – vendor, price, properties, etc.

Incorporates natural language to match on lexical meaning and search context

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Machine learning innovations in OpenSearch

Anomaly detection for time series

Detect and mitigate issues faster with anomaly detection

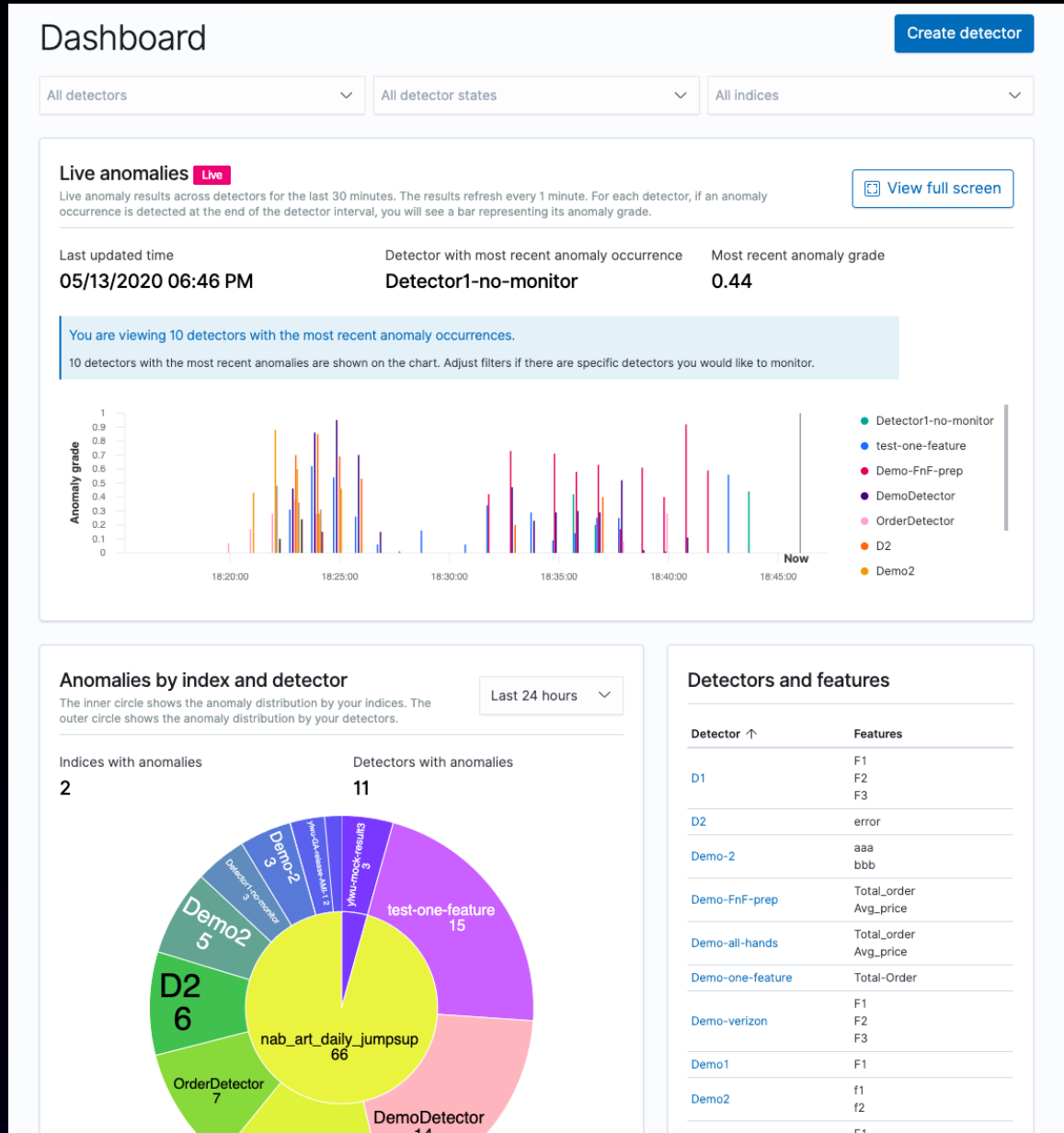
Performant at scale

Machine learning models are distributed and processed across nodes

Easy to use

No machine learning expertise required

Based on Random Cut Forest (RCF)*



*Guha, Mishra, Roy, Schrijvers, ICML 2016

Anomaly detection at Mobilewalla

"We integrate with hundreds of our customers using Amazon S3 API for data exchange, and we monitor their traffic patterns by analyzing S3 access logs in Amazon OpenSearch Service. **Anomaly detection** has helped us detect changes in traffic patterns without configuring complex rules for each customer. This has enabled us to respond to those changes in a timely manner, ensuring security and reliability of our platform."

Harikrishnan Chandrasekaran, Principal Cloud Architect

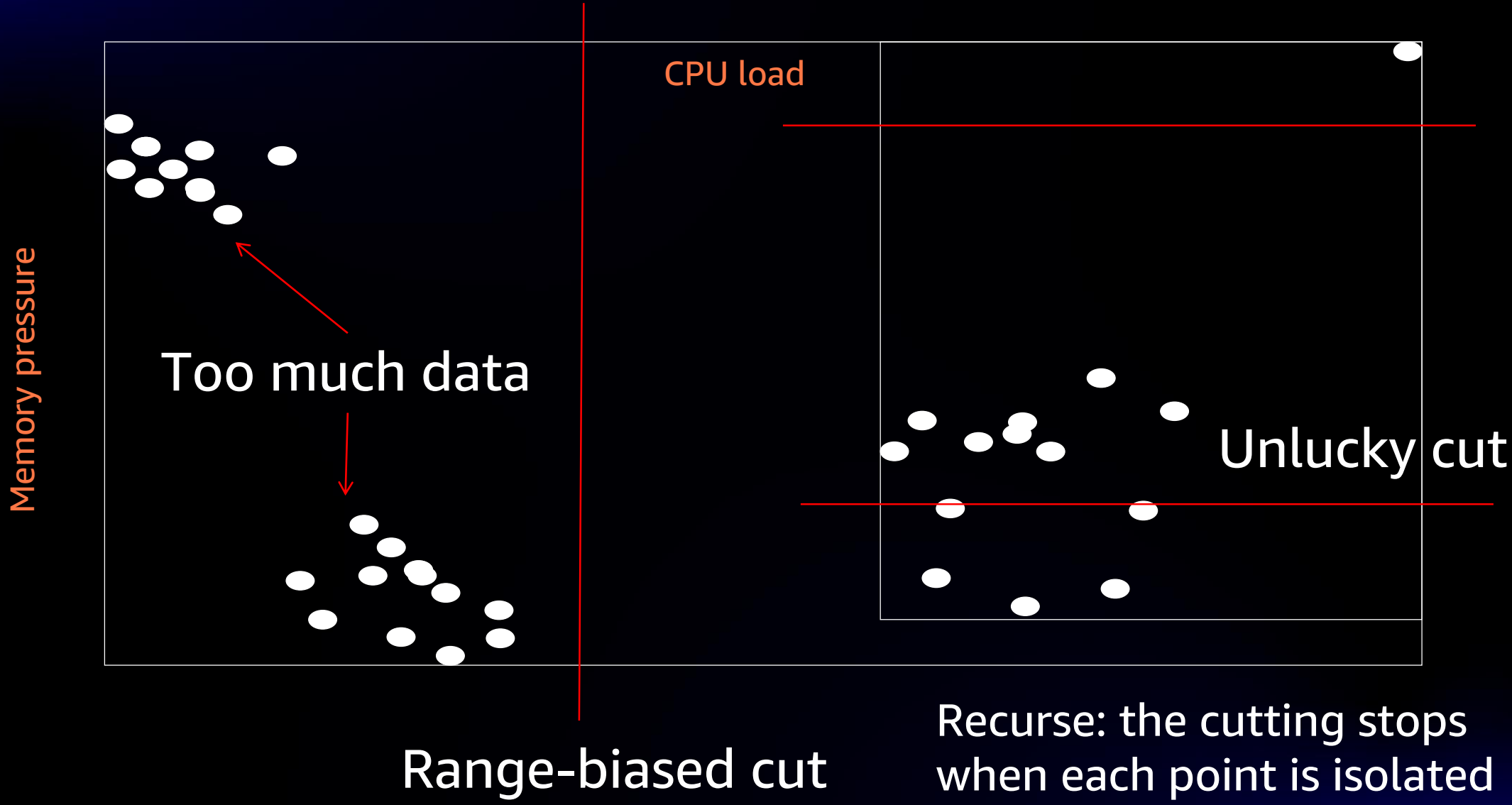


mobilewalla

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Random Cut Tree: A sketch

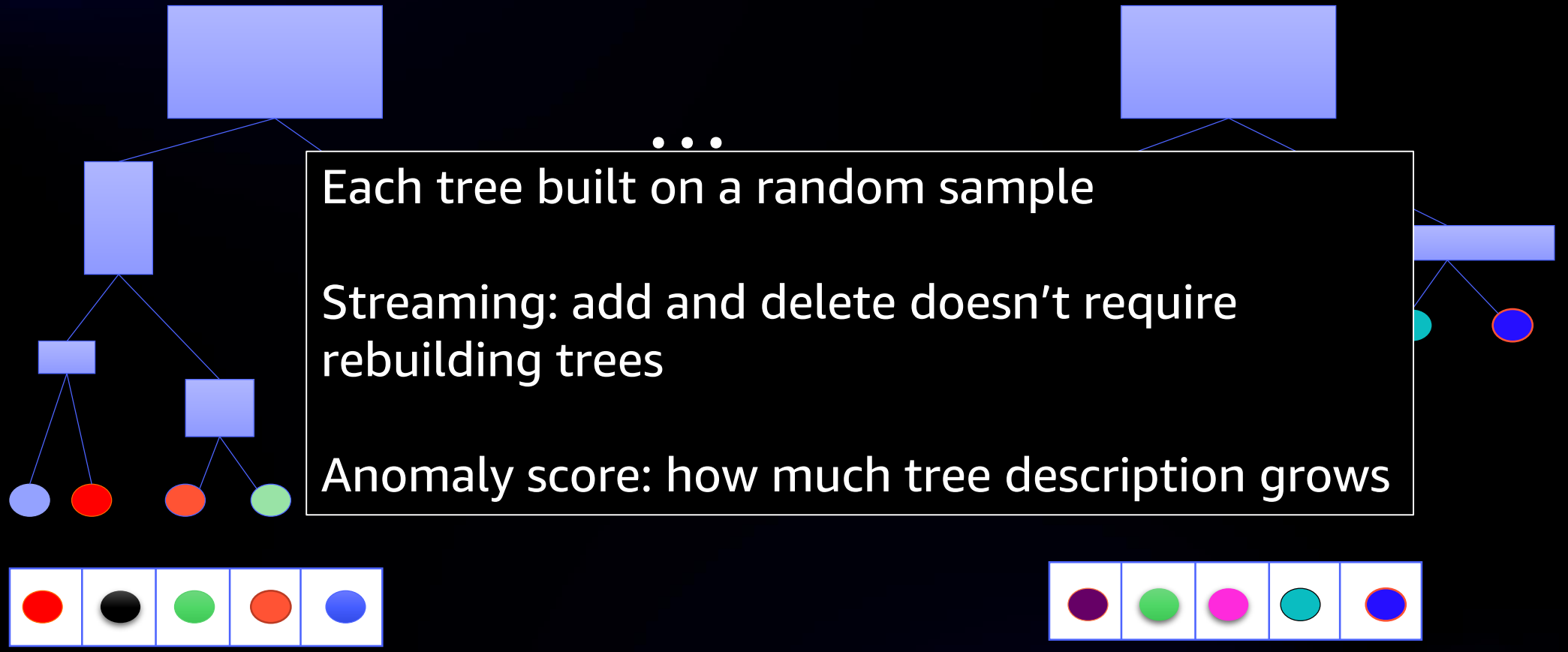


Recurse: the cutting stops when each point is isolated

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Random Cut Forest (RCF)



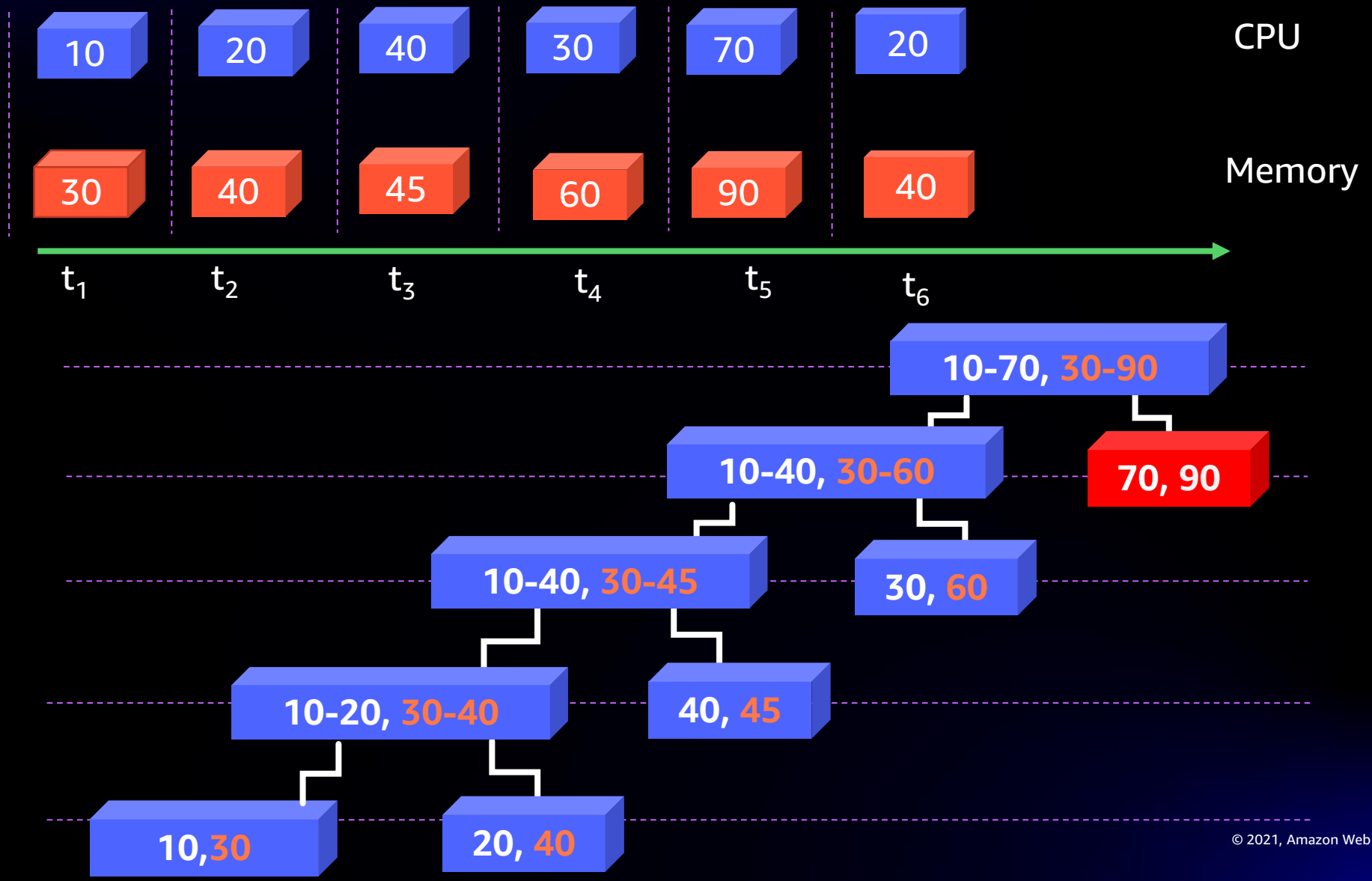
Each tree built on a random sample

Streaming: add and delete doesn't require rebuilding trees

Anomaly score: how much tree description grows

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-dimensional RCT



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Real-time anomaly detection

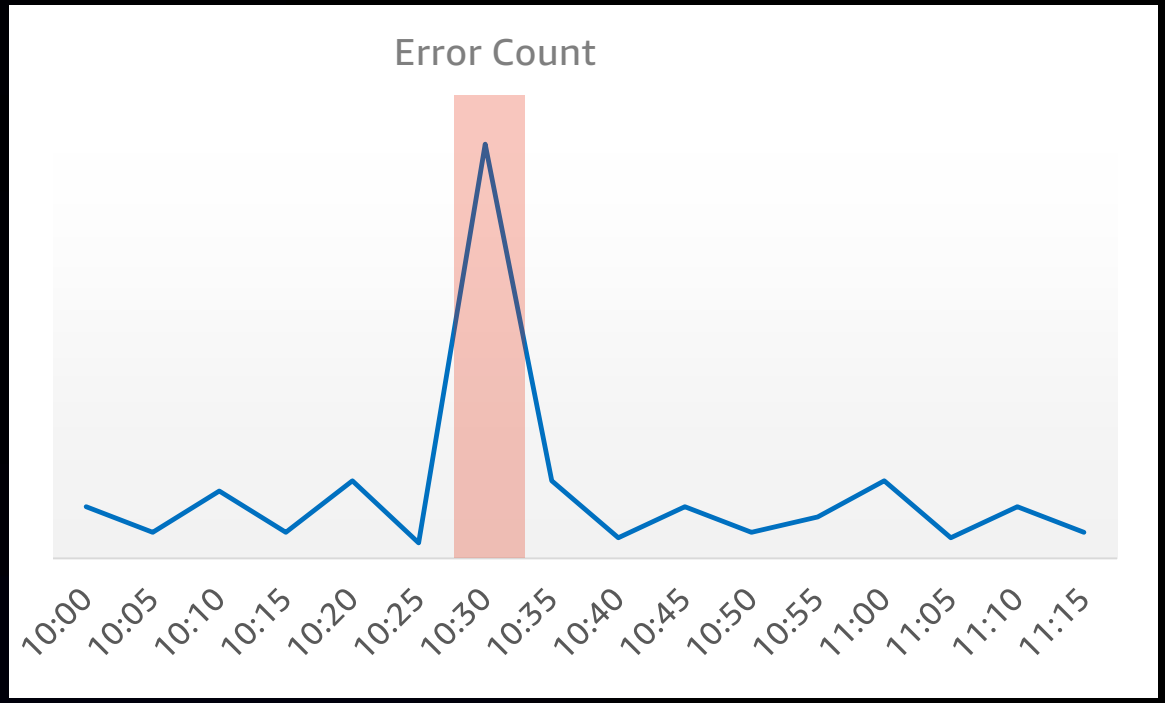
Released April 2020

Dynamically detects anomalies in near real time on streaming data

Detector supports up to five dimensions
For example: CPU, memory, disk storage, latency

Integrated with OpenSearch alerting, providing real-time notifications on anomalies

Use cases: increases in error rates, unusual data downloads, spikes in CPU and IO usage, increases in network traffic rejections



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High cardinality anomaly detection

Released November 2020

Detects anomalies on entities by **group-by** category

One model per entity
(e.g., host id where host id = host1, host2)

Surfaces individual entities with anomalous patterns

Use cases: identifying individual hosts or services with high error rates, isolating suspicious users, and detecting outliers in sales by Region

Only scaled to support ~1,000 unique entities



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High cardinality anomaly detection

OpenSearch 1.1 (coming soon – Dec. 2021)

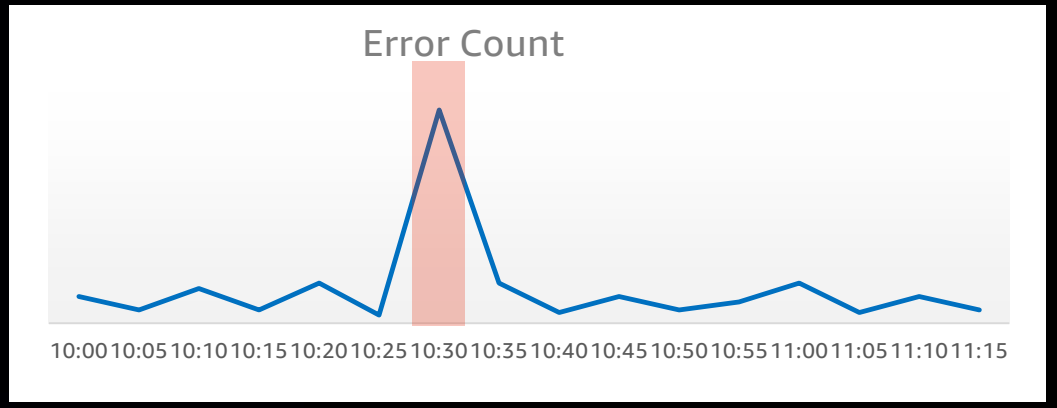
Support for **1 million** entities

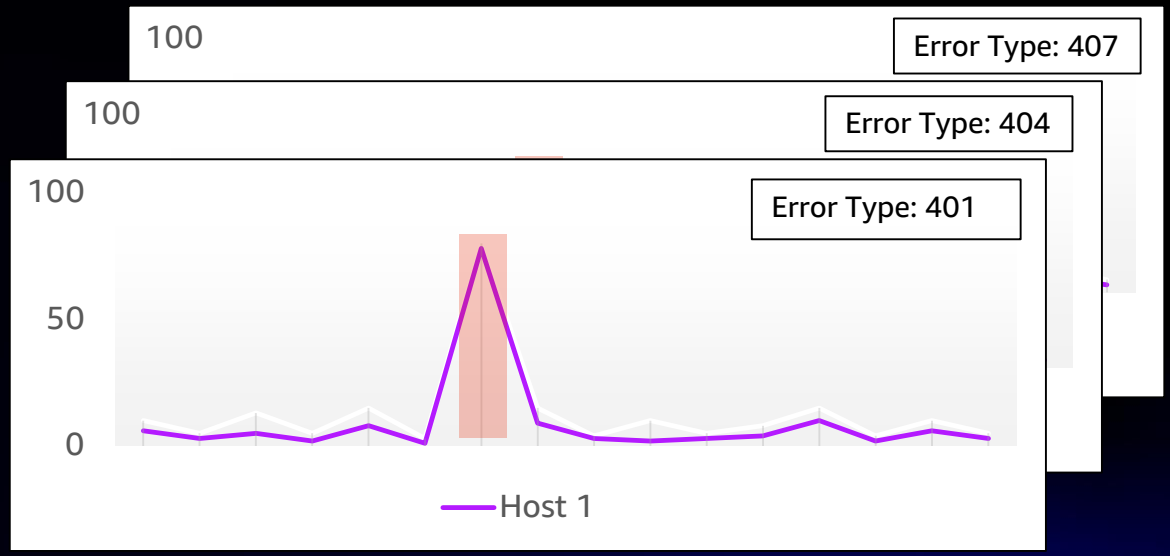
Underpinned by improved RCF algorithm (RCF 2.0)

Supports an additional **group-by** category

One model per entity
(e.g., entity = host id * error type)

Use cases: identifying individual hosts with high error count by error types, isolating suspicious users accessing sensitive information by S3 buckets





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

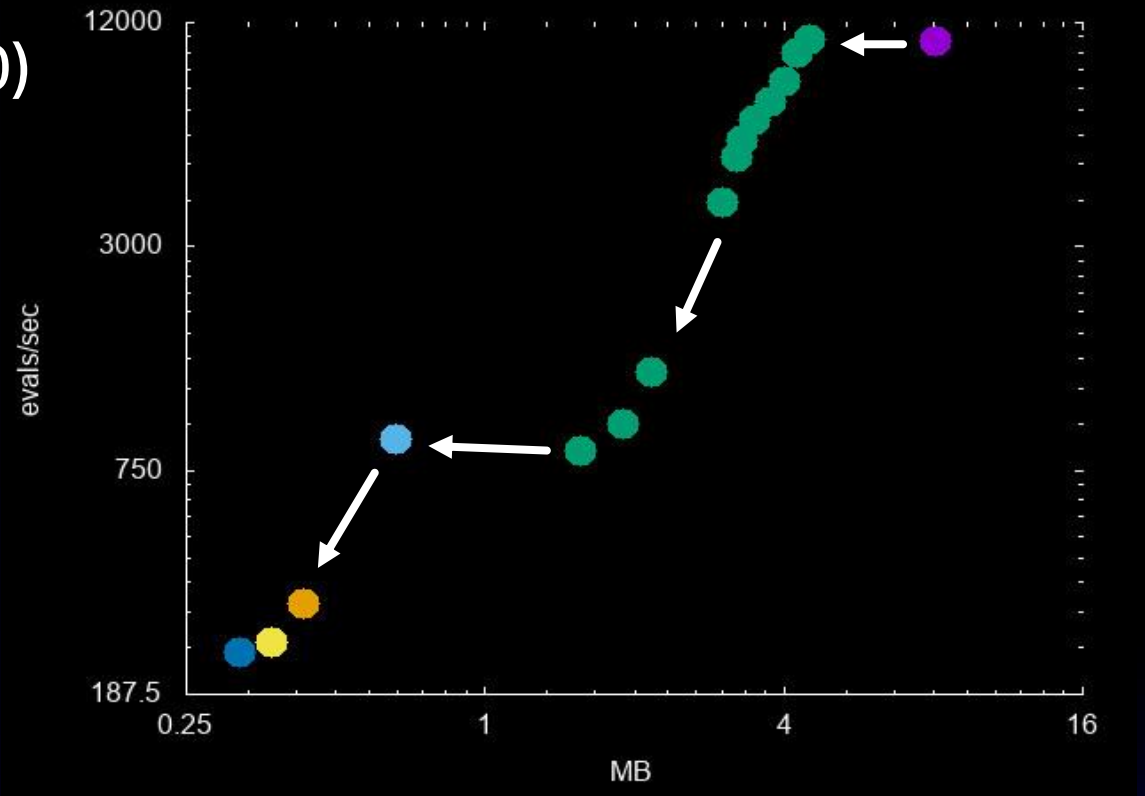
RCF 2.0: Enabling ML at scale

Smaller, more compact models

Memory: 8 MB (RCF 1.0) → 300 KB (RCF 2.0)

Enhancements driving improvements

- Recomputing bounding boxes/ intervals on the fly
- Efficient management of shingles/patterns
- Representing trees as sequences
- Columnar compression



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The road ahead

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enhancing core OpenSearch

Higher availability and resiliency

e.g., cross-cluster replication, index-level throttle, skew avoidance during failures

Improve performance

e.g., k-NN FAISS, RCF 2.0, Lucene 8.9

Drive down cost



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

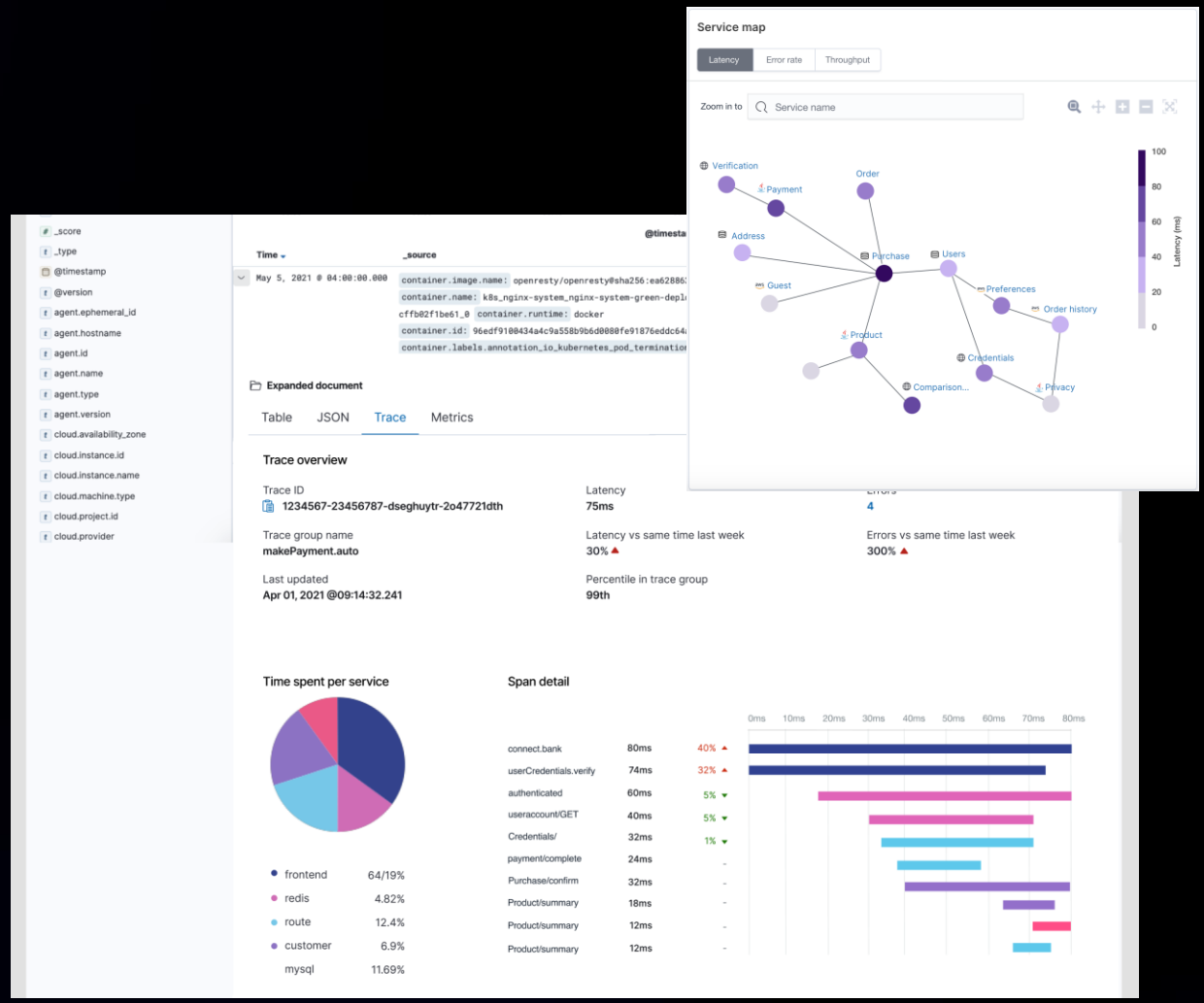
Observability

OpenSearch Trace Analytics

CNCF OpenTelemetry
Open Distro for Elasticsearch 1.12 (ES 7.9)

Correlate logs, traces, and metrics

Out-of-the-box operational analytics



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recap

Same great service, same flexibility

OpenSearch is fully open source

Apache License V2, backward compatible, no lock in

Cutting-edge features: open source and service

Cold storage, Auto-Tune, replication, ML, Trace Analytics, Data Prepper, and more

Innovation at the pace you expect



Feedback: searchservices-pm@amazon.com

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logsearch at Pinterest

Wei Zhu (he/him)

Staff Software Engineer Observability
Pinterest

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Overview

- Services are ingesting (mainly exception) logs to OpenSearch clusters
- Use OpenSearch Dashboard to visualize the logs in near real time, which is a main tool for root cause analysis
- Monitor performance stats and detect degradation using access log and mobile client log
- Generate metrics from logs by calling OpenSearch API
  - The metrics are ingested to Pinterest metrics pipeline
  - The metrics are used for generic alerting
  - The metrics are part of automated canary analysis

aws

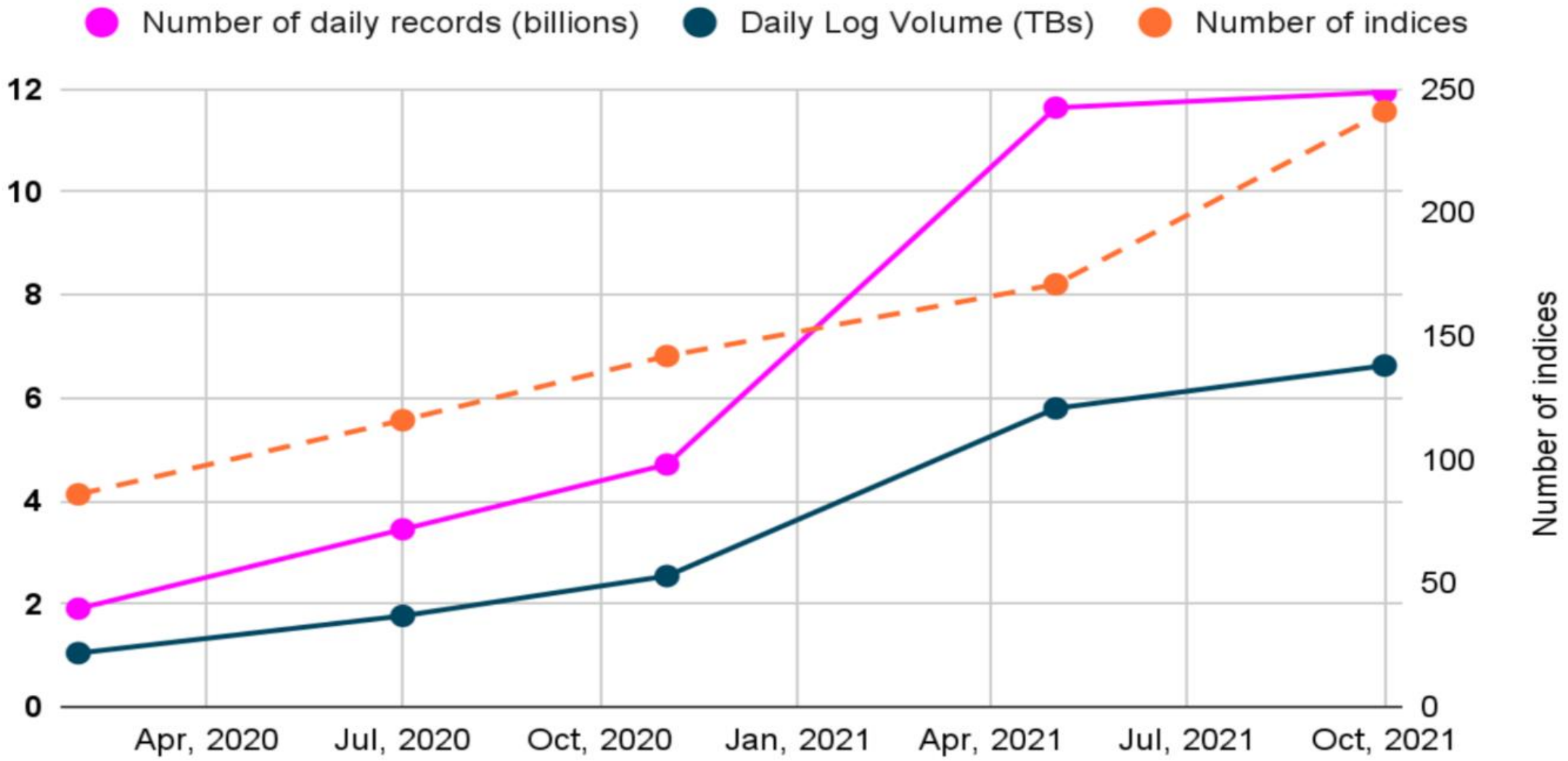
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Journey to Amazon OpenSearch Service

- Before 2017
  - Self-hosted Elasticsearch cluster, too much operational overhead
- 2017 to 2020
  - SaaS vendor, cost too much, poor performance
  - Proprietary query language
- 2020 to now
  - Amazon OpenSearch Service
  - 7 clusters, total of almost 200 nodes
  - 240 log streams
  - 12 billion daily records
  - 6.6 TB daily volume
  - <0.5 FTE to keep the lights on

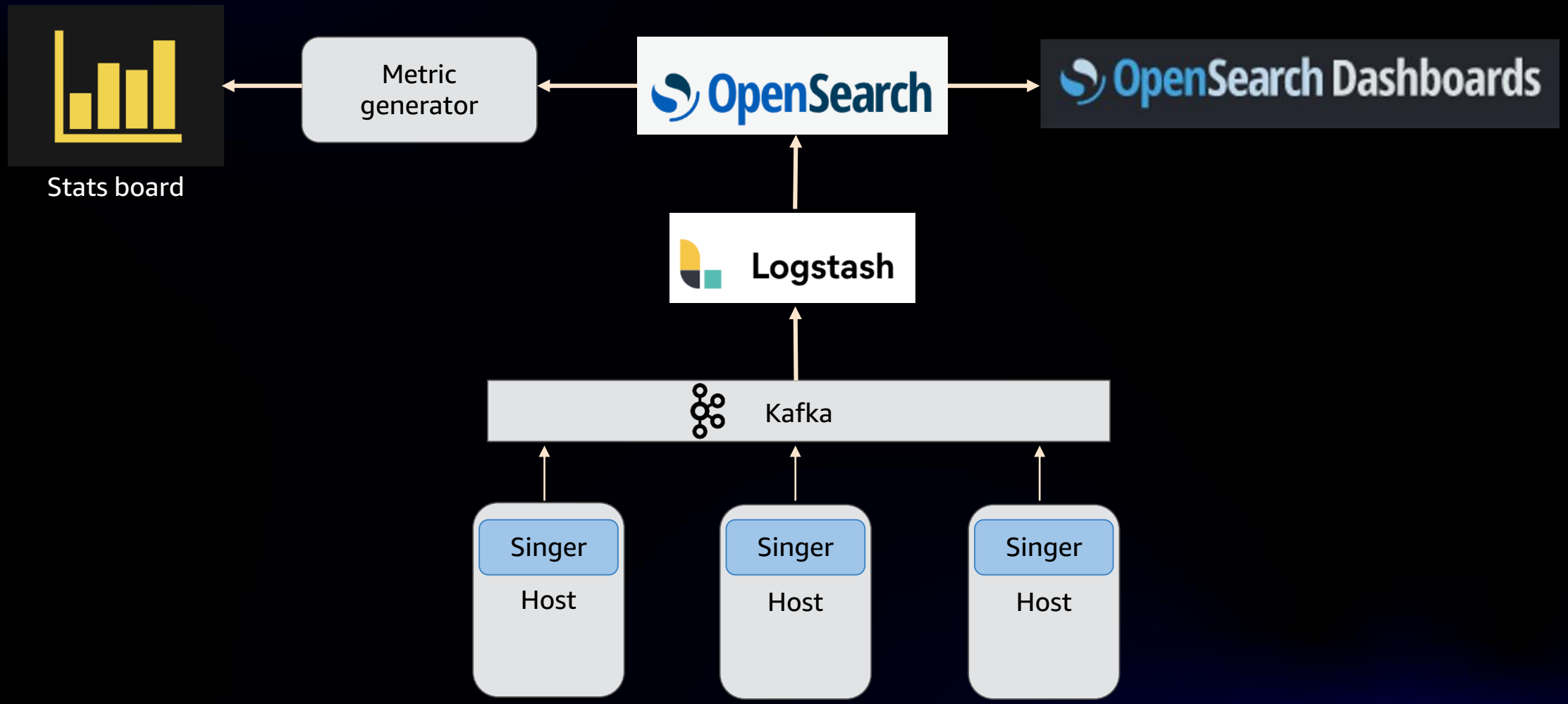
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logsearch



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logsearch architecture



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New features adoption

UltraWarm, cold storage

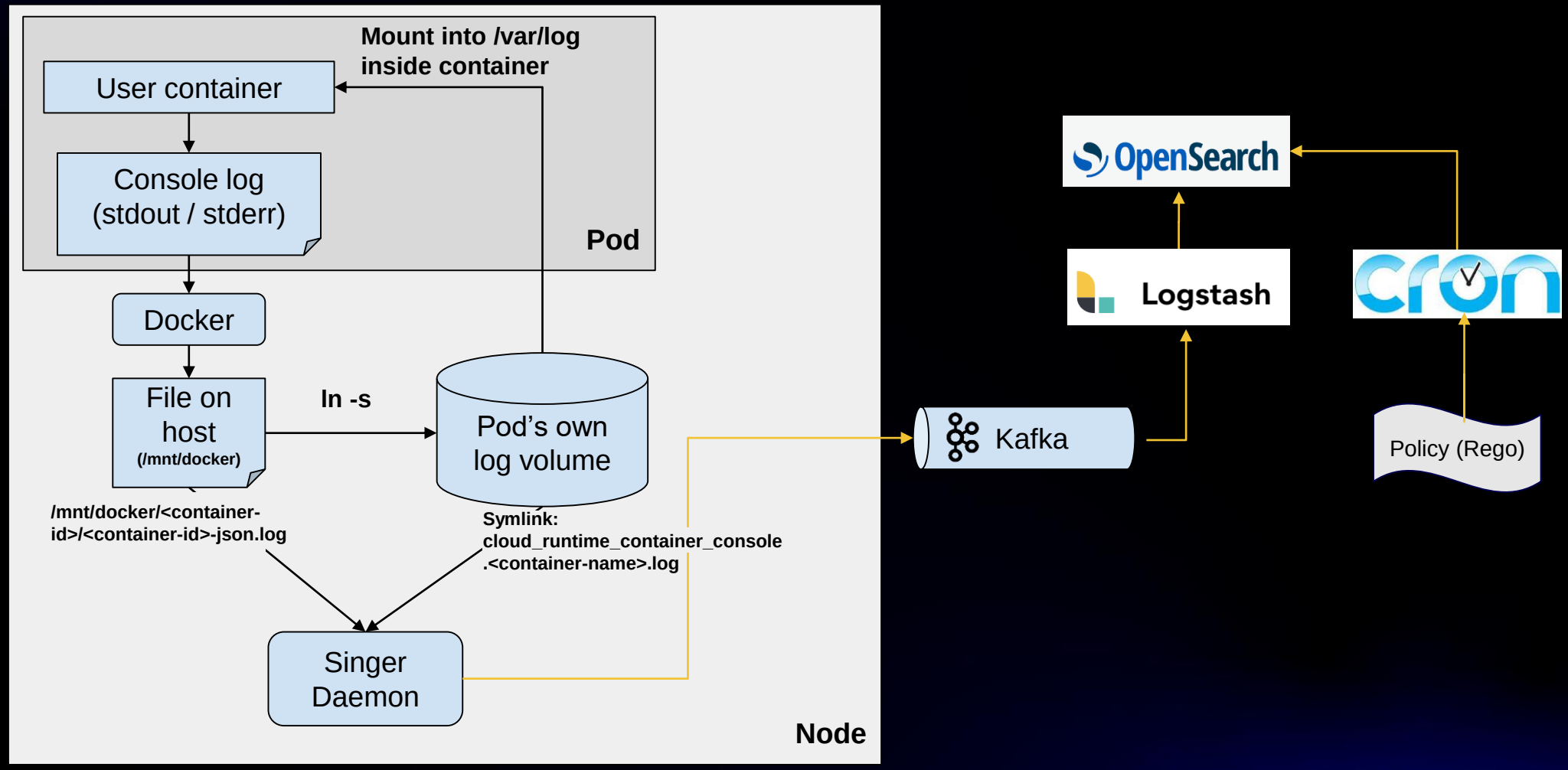
- Keep logs longer with less cost
- 35% cost reduction, which is more than $500K annual savings
- More use cases possible
  - Hadoop logs: daily volume of 2 TB
  - Mobile logs: keep logs for 2 years

Security features

- SAML integration with Okta
  - Integration with Amazon Cognito was hard to manage
- FGAC
  - Role-based access control
  - Security at the index, document, and field level
  - OpenSearch Dashboards multi-tenancy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case: K8s console logs



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case: K8s console logs

- Logs are persisted in Amazon OpenSearch Service, even after the pods are terminated
- Logs from 70+ different workloads are ingested to OpenSearch, and the whole process is fully automated
- Use the same Rego policy file to control the k8s resources and OpenSearch indices
  - Rego is a high-level declarative language to describe Open Policy Agent policies; it’s the standard security policy language we use in Pinterest
  - Cron job to sync the Rego policy with OpenSearch FGAC configuration using OpenSearch API

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

- Scales to fit use cases
- Low cost of maintenance with Amazon OpenSearch Service
- Cost savings with UltraWarm and cold storage tier
- Advanced security features

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Feedback: searchservices-pm@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.