AWS re:Invent

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

ANT204

Dive Into Amazon OpenSearch Service

Singe Graham (He/Him)
Sr. Solutions Architect
AWS

Jon Handler (He/Him)
Sr. Principal Specialist SA
AWS

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

Agenda

- Access Event Engine
- Start your deployment
- Overview of OpenSearch
- Complete the lab guide
- Q&A and wrap up

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

Setup

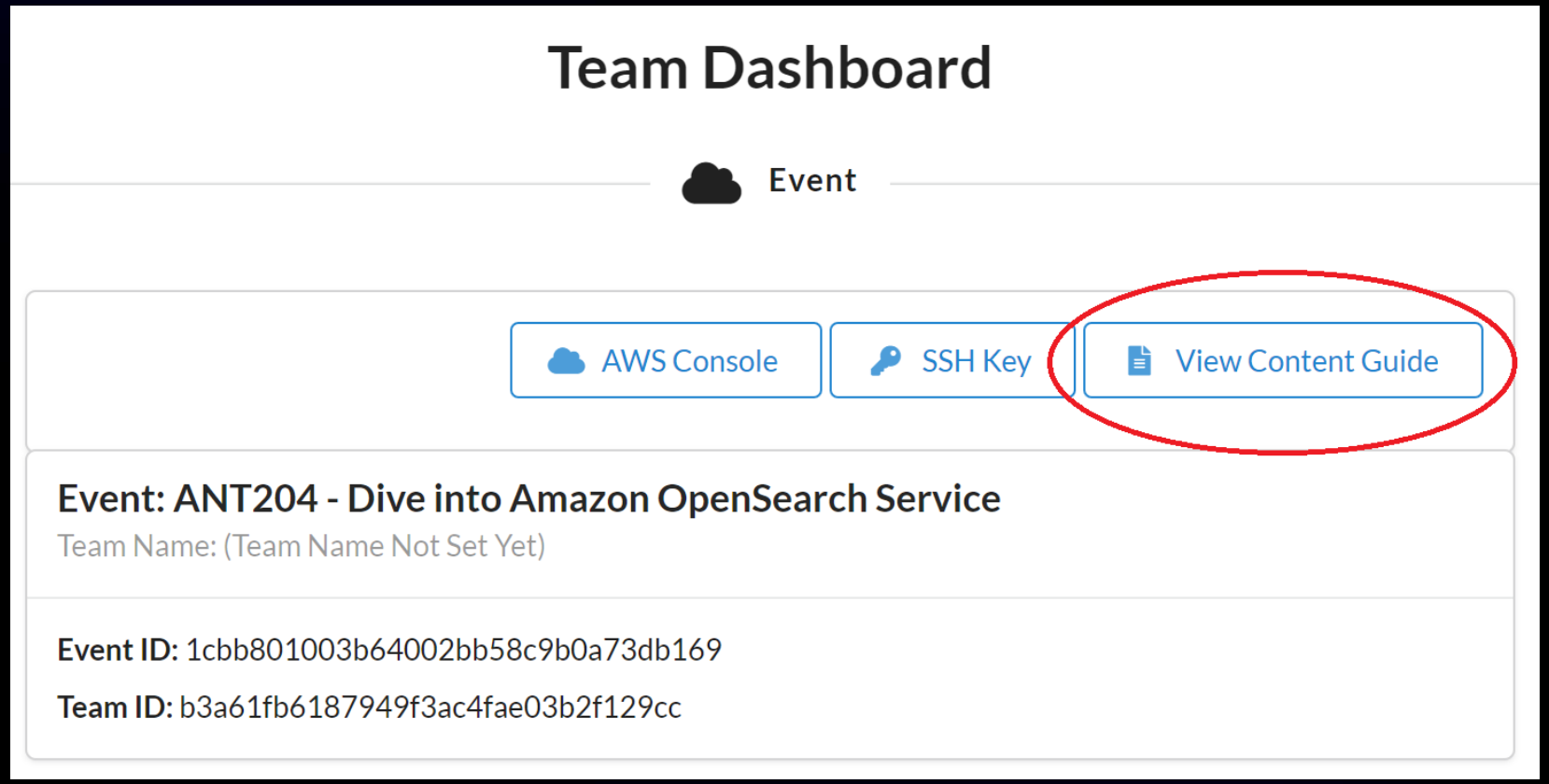
1. Navigate to https://dashboard.eventengine.run/

2. Use the event hash: **509f-19def81924-59**

3. Access the lab guide by clicking ‘View Content Guide’

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

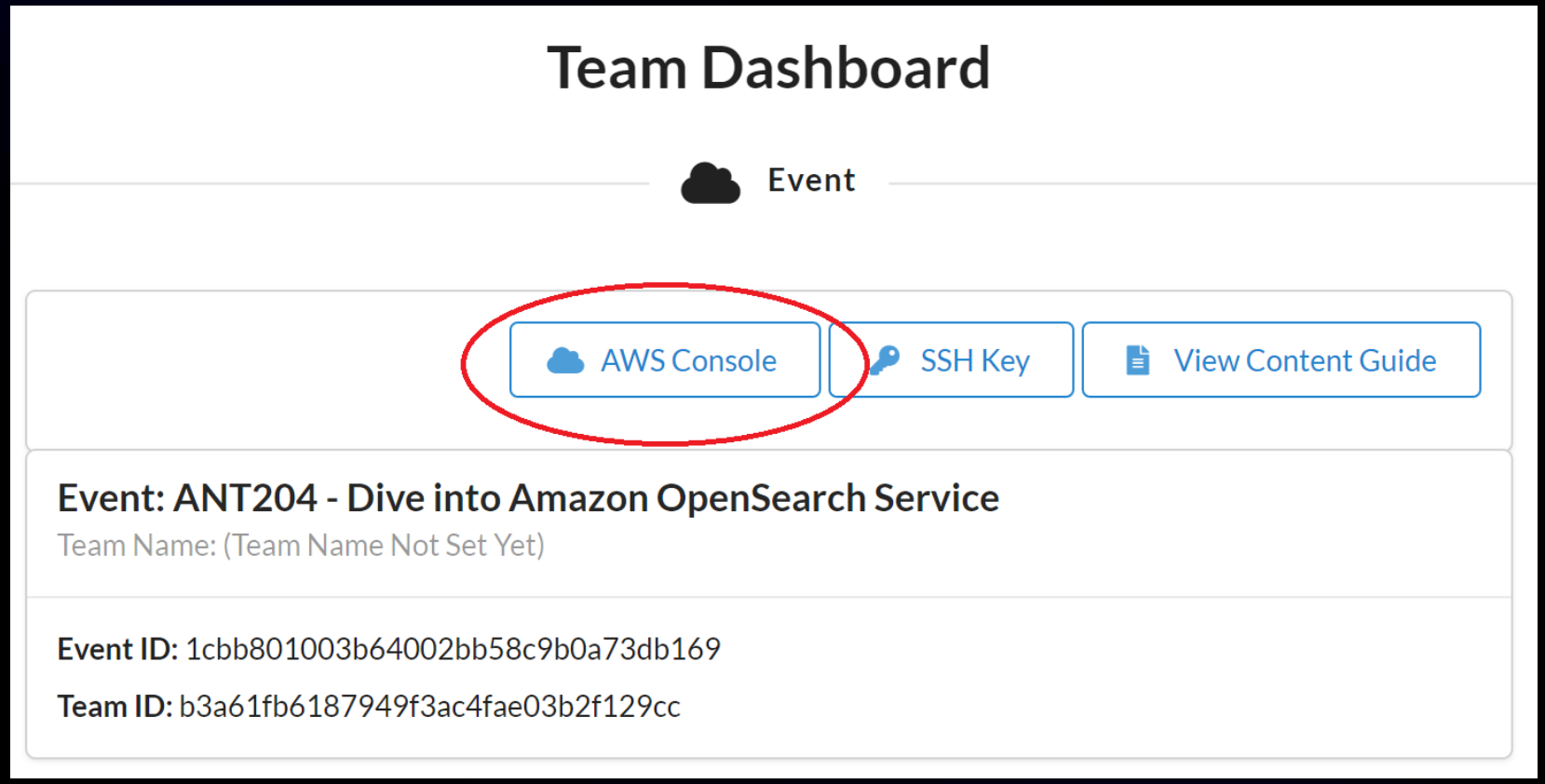
Open the Lab Guide



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

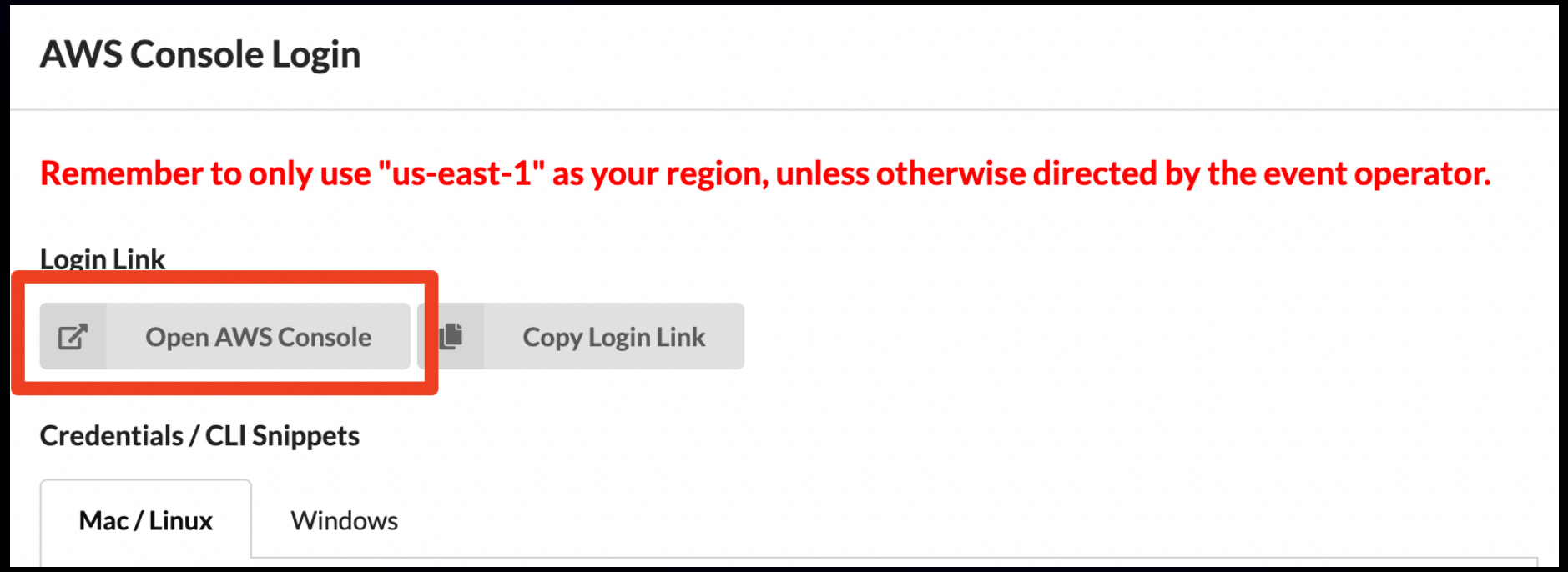
Navigate to the console



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

Navigate to the console



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

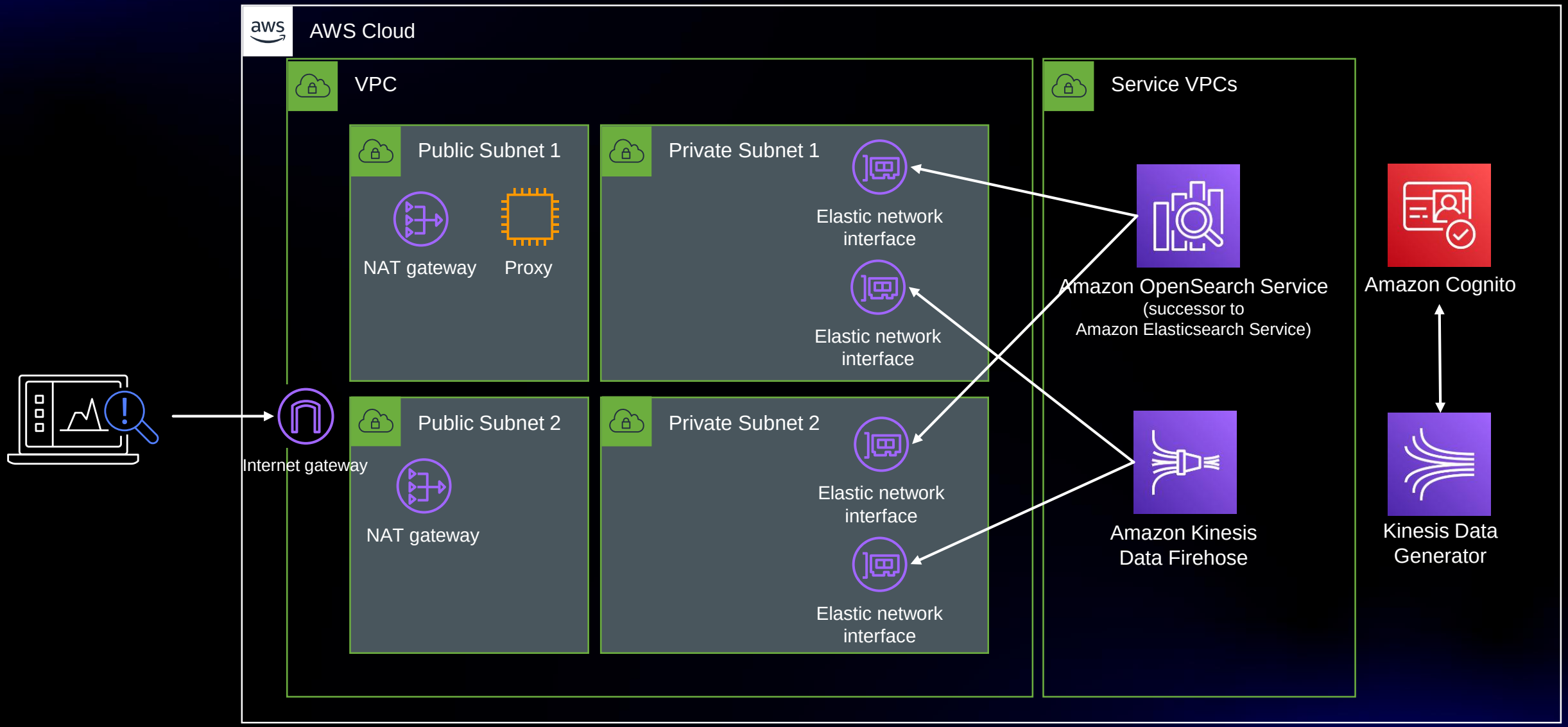
What's already deployed



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

When you complete the workshop



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

Setup

- Set up an Amazon OpenSearch Service domain
- Learn about the different features
- Explore best practices

https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

aws

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

Complete the ‘Setup’ section of the workshop

Time: 20 Minutes

https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

aws

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

Amazon OpenSearch Service

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

What is OpenSearch?



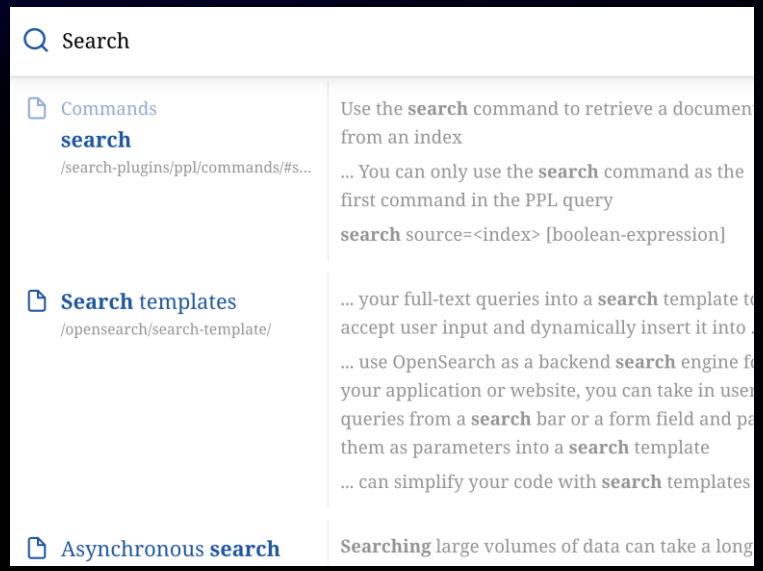
OpenSearch is a community-driven, open source search and analytics suite derived from Apache 2.0 licensed Elasticsearch 7.10.2 & Kibana 7.10.2.

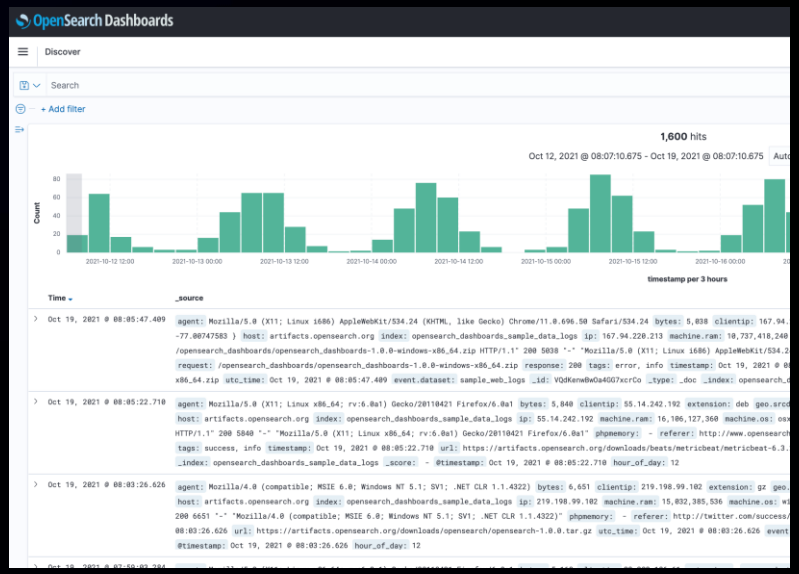
The OpenSearch Project comprises OpenSearch, a search engine daemon, OpenSearch Dashboards for visualization and user interface, and tools and plugins, providing additional functionality

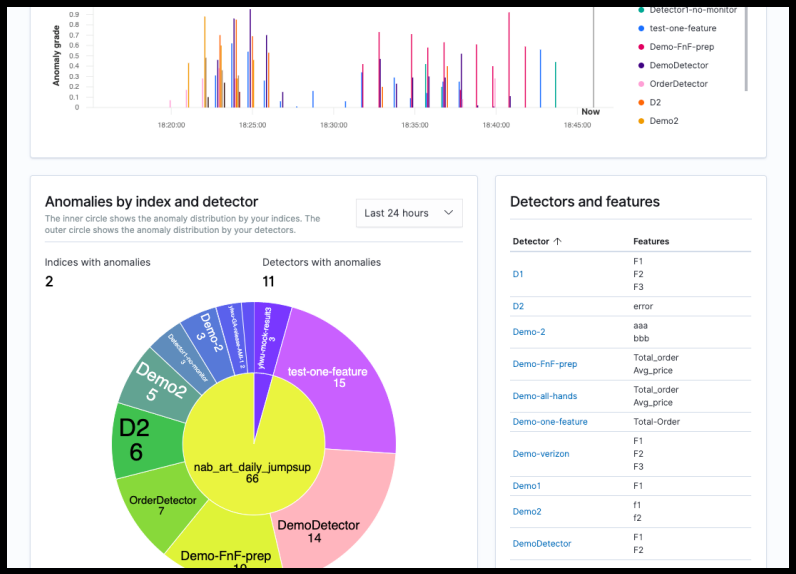
https://opensearch.org/

© 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.

Why should I use OpenSearch?

100% Open Source

- Use, Modify, Monetize
- Built in the open
- No CLA

Community Driven

- Your input matters
- Public roadmap
- Welcome contributions

Full Featured

- Full text search
- Visualization & Dashboards
- High performance
- Alerting
- Machine Learning
- Security

© 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-prem or in any other cloud

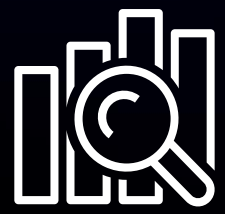
Compatible: No code changes required – including new universal language specific clients

Innovative: Dozens of new features in just first few releases including: *Cross-cluster replication, shard-level backpressure, notebooks, data streams, index transforms, bucket level alerting, and more*

aws

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

Amazon OpenSearch Service + OpenSearch



Amazon OpenSearch Service

+

OpenSearch

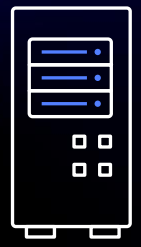
A great home for all of your Elasticsearch and OpenSearch workloads

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

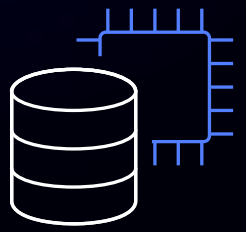
aws

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

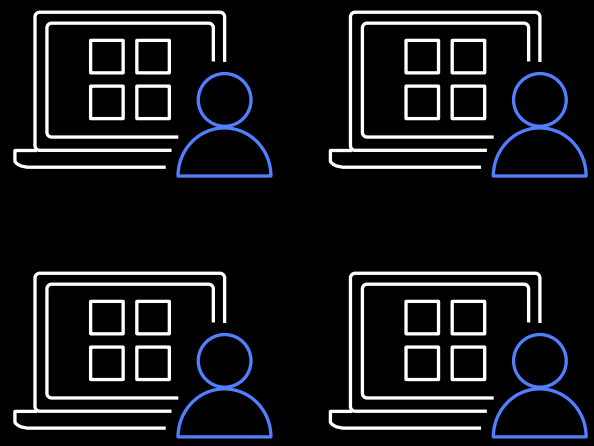
Interaction flow



Server, application, network, AWS, and other logs

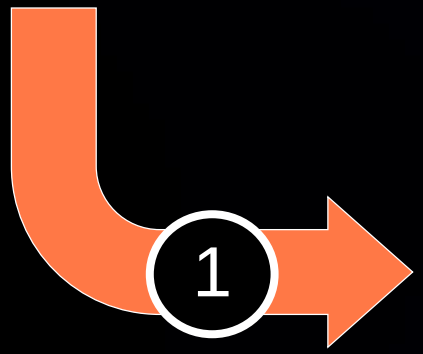


Application data

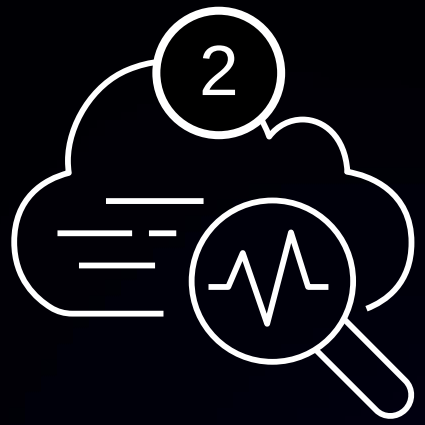


Application users, analysts, DevOps, and security

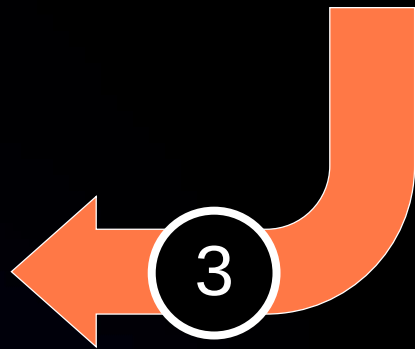
Indexed and instantly searchable



JSON documents



Amazon OpenSearch Service Domain

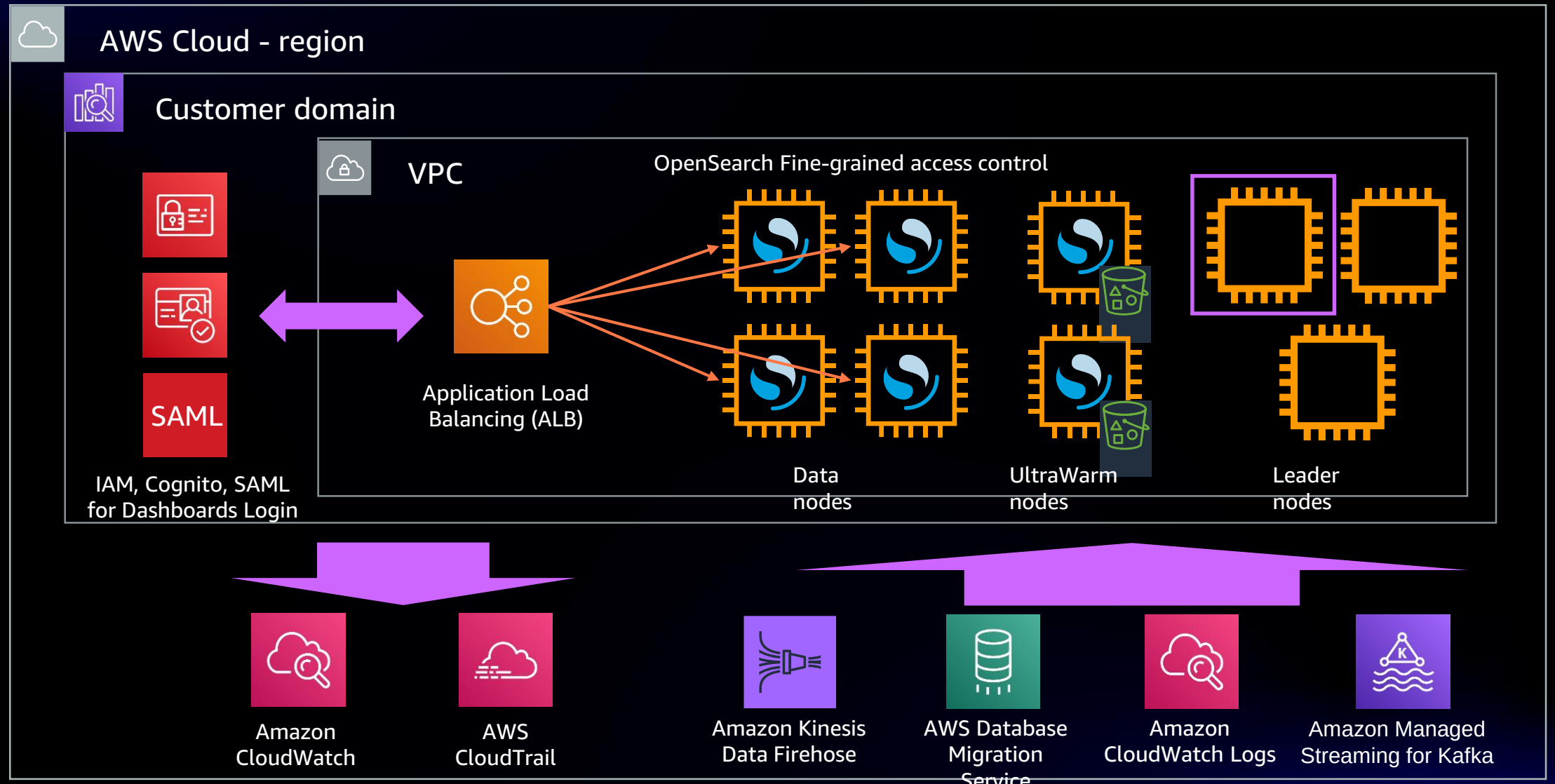


Rest APIs, clients, and OpenSearch Dashboards

aws

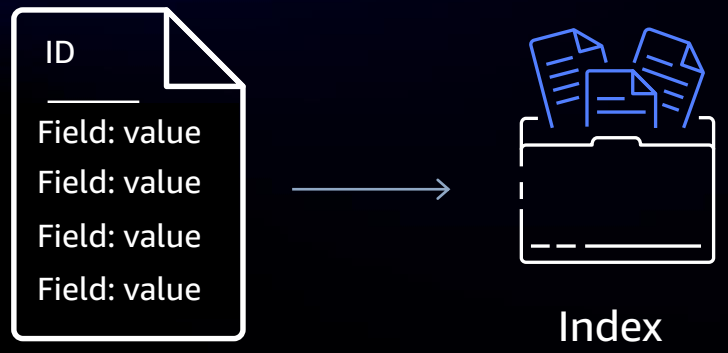
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service Architecture



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

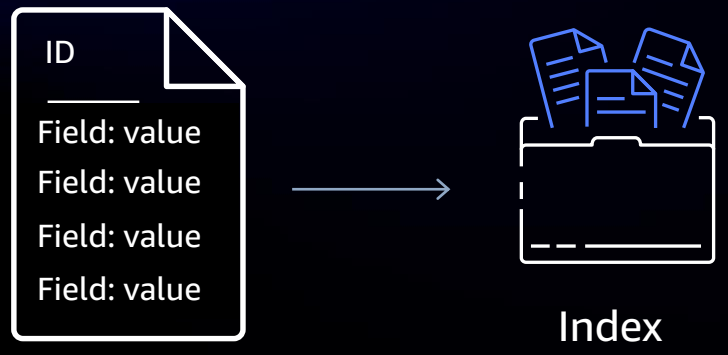
You send your data to an index



- An index is like a database table, fields are like columns, values are cells

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

You send your data to an index

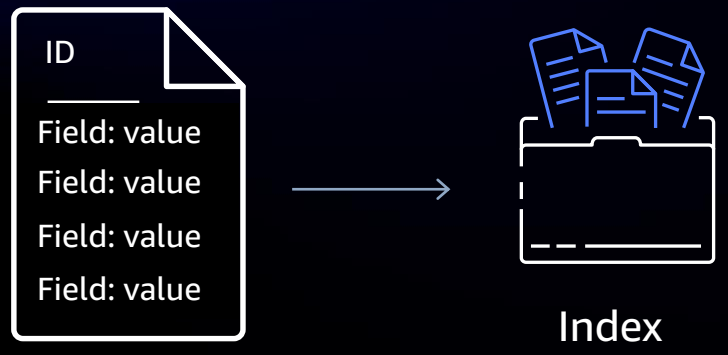


- An index is like a database table, fields are like columns, values are cells
- Interact via REST APIs

aws

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

You send your data to an index

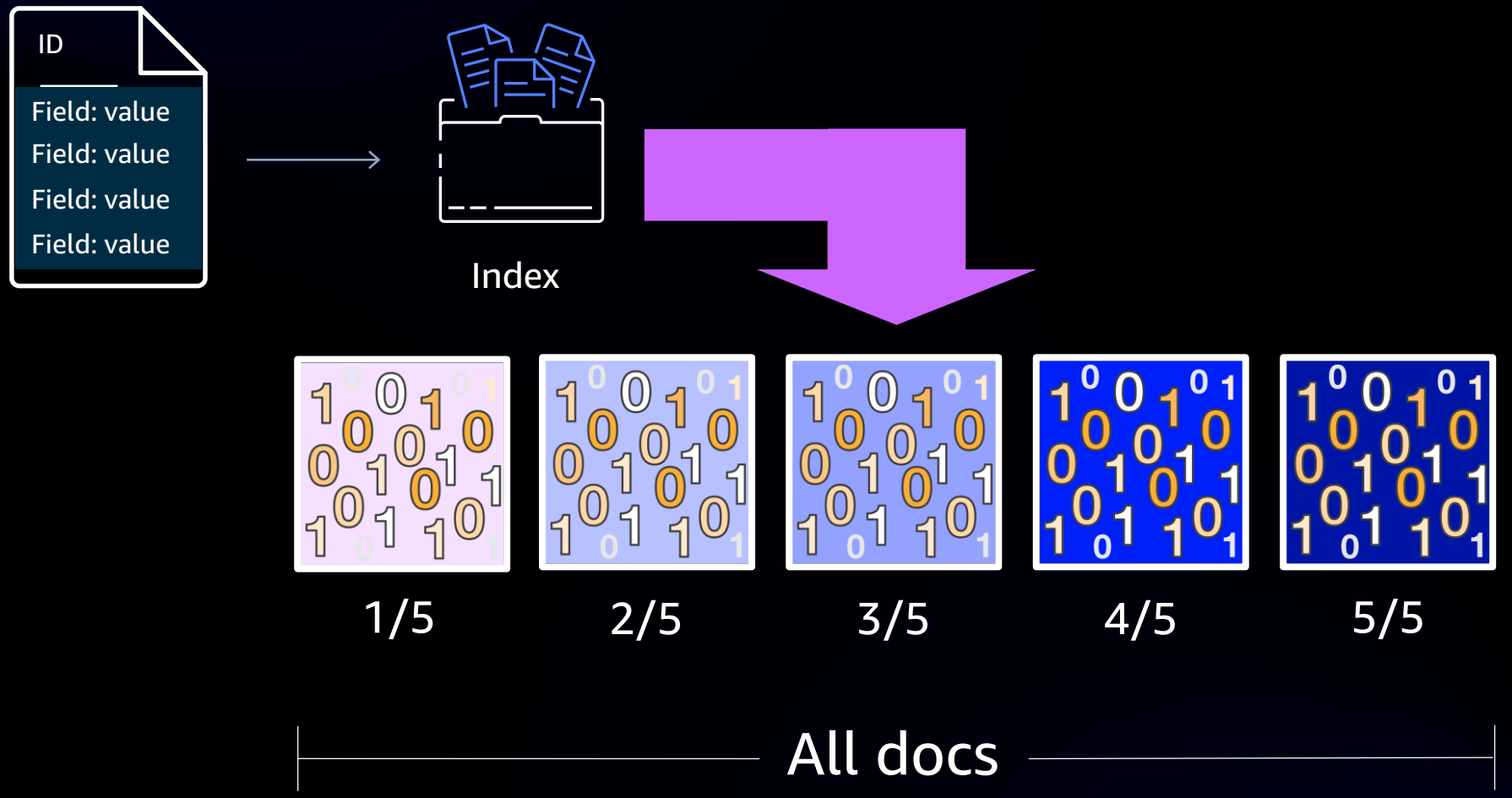


- An index is like a database table, fields are like columns, values are cells
- Interact via REST APIs
- Data is structured as fields/values in JSON

aws

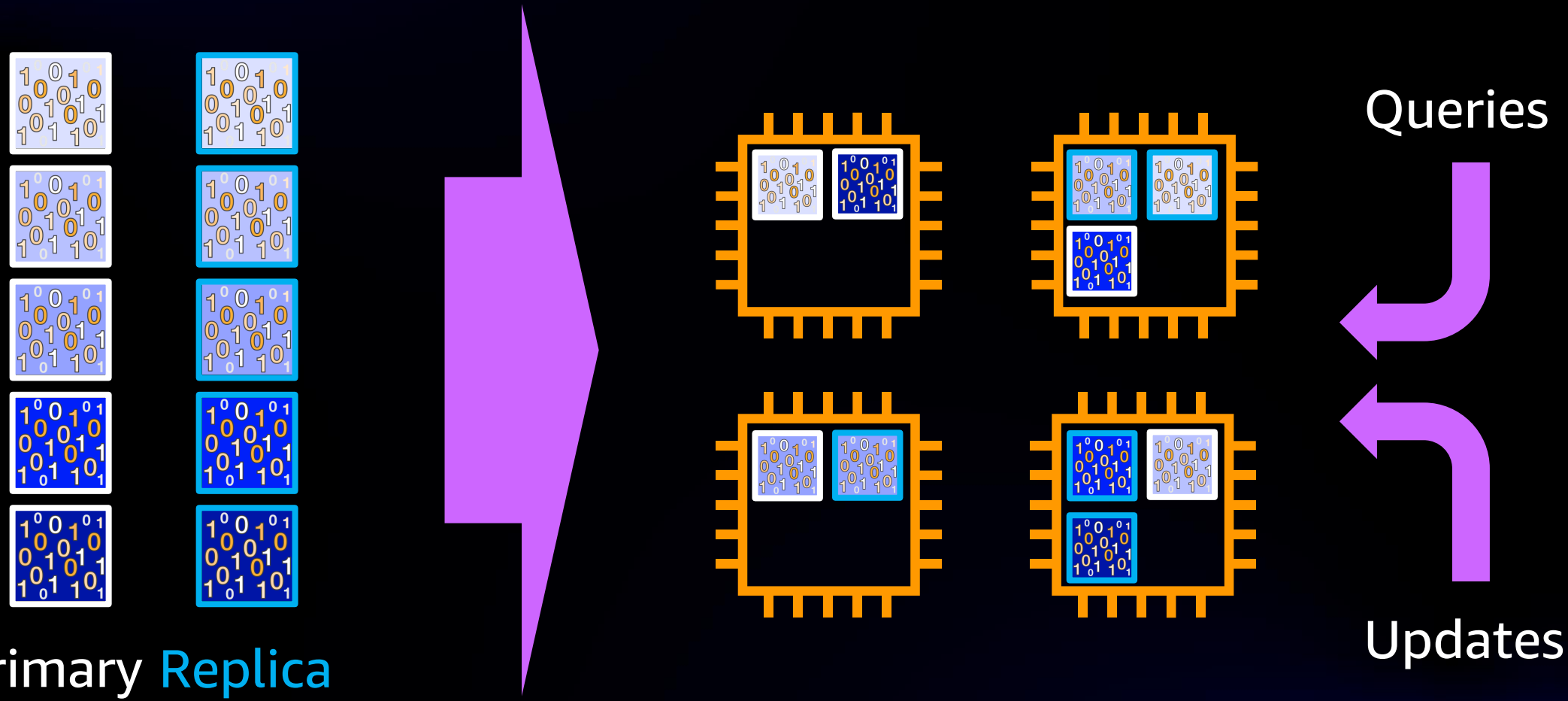
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Indices are comprised of shards



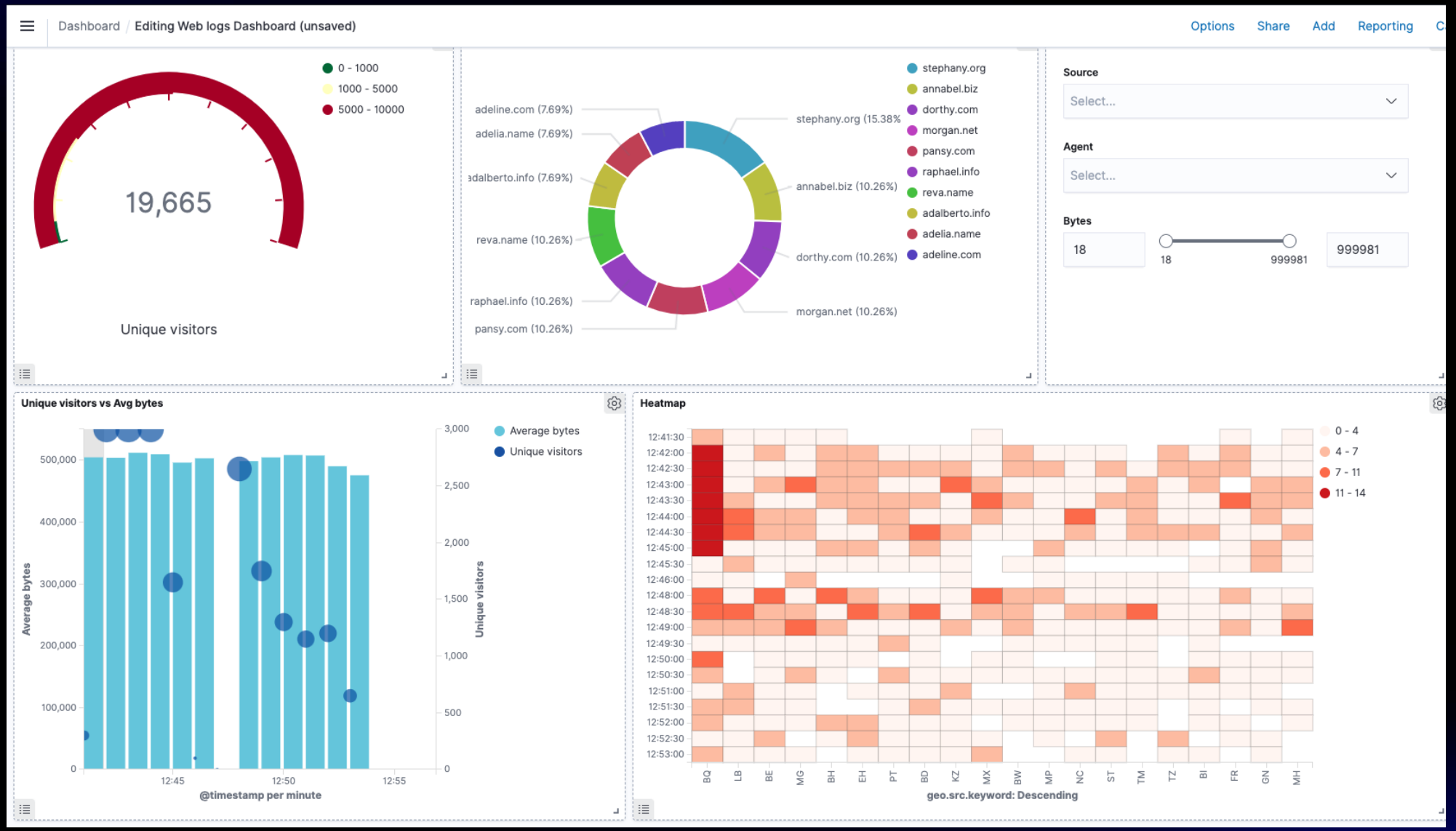
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OpenSearch distributes shards to data nodes



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

OpenSearch Dashboards is a lightweight, real-time visualization tool



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

Module 1: Search data flow

OpenSearch Dashboards reaches the proxy via public IP address

The proxy forwards to Amazon OpenSearch Service via an Elastic Network Interface that the service projects into your VPC

OpenSearch Dashboards Dev Tools tab is a handy way to interact with your domain



https://dashboard.eventengine.run // Event Hash: **40c7-19b78f2124-8a**

aws

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

Complete the ‘Module 1’ section of the workshop

Time: 30 Minutes

https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

aws

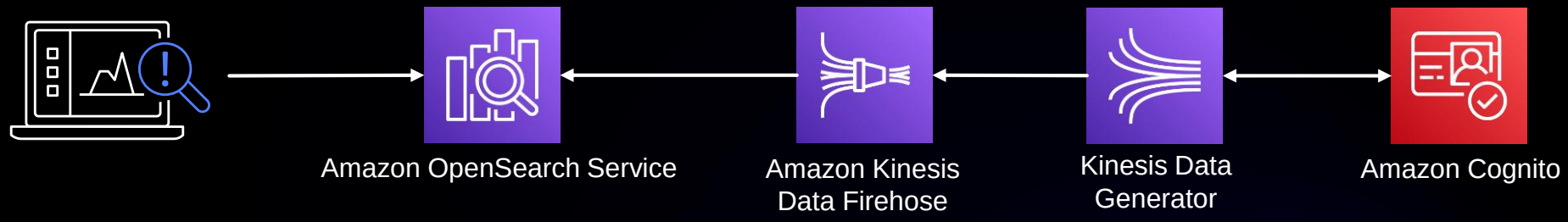
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 2: Log analytics data flow

Kinesis Data Generator (KDG)

OpenSearch Dashboards for visualization

Test streaming anomaly detection



https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

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

KDG template

Simulates Apache web logs

Time-based data

Randomized REST methods

Randomized status codes

Simulated geo information

```
{
    "host": "{{internet.domainName}}",
    "ident": "-",
    "auth": "-",
    "@timestamp": "{{date.utc("YYYY-MM-DDTHH:mm:ss")}}",
    "bytes": {{random.number(1000000)}},
    "verb": "{{random.weightedArrayElement(
        {
            "weights": [0.8,0.1,0.1],
            "data": ["GET","PUT","POST"]
        }
    )}}",
    "url": "{{internet.url}}",
    "http": "HTTP/1.1",
    "status": {{random.weightedArrayElement(
        {
            "weights": [0.9,0.05,0.05],
            "data": ["200","404","503"]
        }
    )}},
    "agent": "{{internet.userAgent}}",
    "clientip": "{{internet.ip}}",
    "geo": {
        "srcdest": "{{address.countryCode}}:{{address.countryCode}}",
        "src": "{{address.countryCode}}",
        "dest": "{{address.countryCode}}",
        "coordinates": {
            "lat": "{{address.latitude}}",
            "lon": "{{address.longitude}}"
        }
    }
}
```

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

Complete the ‘Module 2’ section of the workshop

Time: 30 Minutes

https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

aws

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

Complete the ‘Module 3’ section of the workshop

Time: 20 Minutes

https://dashboard.eventengine.run // Event Hash: **509f-19def81924-59**

aws

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

Thank you!

Singe Graham
ghrmgr@amazon.com

Jon Handler
handler@amazon.com

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