
AWS
re:Invent

OPN207

The future of Elasticsearch: Open Distro for Elasticsearch

Kyle J. Davis
Senior Developer Advocate
Open Distro for Elasticsearch, AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

1. Project overview
2. Key features
3. Roadmap
4. Contributing and community



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Project overview

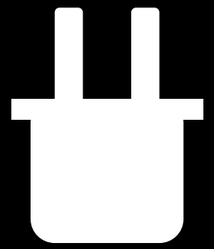


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are Elasticsearch and Kibana?

- TL;DRs
  - Elasticsearch is a distributed, full-text search engine built in Java using Lucene
  - Kibana is a UI and visualization platform for Elasticsearch built in Typescript using the Node.js runtime
- Both are open source - Apache 2.0
- Both are extensible via plugins

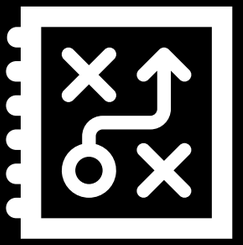
What is Open Distro for Elasticsearch?



A collection of Kibana and Elasticsearch plugins, all Apache 2.0 licensed



A handful of tools that interact with Kibana and Elasticsearch, all Apache 2.0 licensed



A multi-platform installer for the project components as well as Elasticsearch and Kibana

Why Open Distro for Elasticsearch?

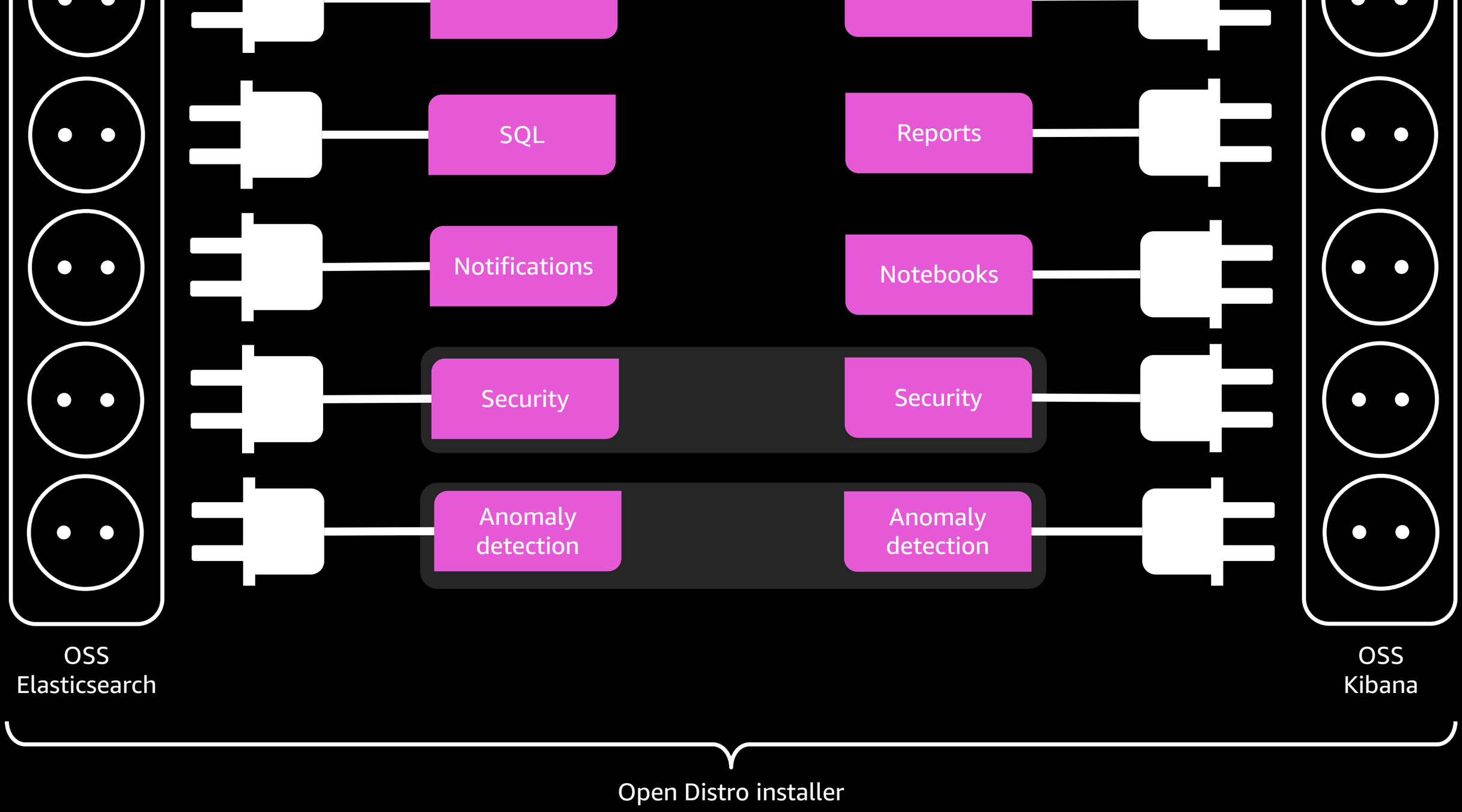
Because...

- We 😍 Elasticsearch
- Open source matters
- Users need more
- Open-source is positive for the community and users

Key features



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.


SQL
Reports
Notifications
Notebooks
Security
Security
Anomaly detection
Anomaly detection
OSS Elasticsearch
OSS Kibana
Open Distro installer

Security and access control

- Node-to-node encryption
- Authentication
  - HTTP Basic, Active Directory, LDAP, Kerberos, SAML, OpenID Connect
- Role-based access control
- Index-, document- & field-level access restriction
- Audit logging
- Kibana multi-tenancy

Query languages

- Elasticsearch Query DSL

```
{
    "_source" : ["name"],
    "query": { "range": { "RAM": { "gt": 16000 } } }
}
```

- Open Distro SQL (including ODBC, JDBC)

```
SELECT name FROM computers WHERE RAM > 16000
```

- Open Distro Piped Processing Language

```
source=computers | where RAM > 16000 | fields name
```

Alerting

1. Run a query on a schedule

    Run every 5 minutes (cron patterns)
2. Trigger an alert when a condition is met

    Example: *When n errors occur in a single hour*
3. Take an action on the alert

    Send a Slack message , fire a webhook, etc.

Anomaly detection

Unsupervised machine learning (RCF) to find outliers in your data

- Create a detector
- Add features to the detector
- Observe results
- Set up alerts
- Adjust model as needed
- Manage detectors

Other features

- *k*-nearest Neighbors (KNN)

  Find similarity for recommendation engines, fraud mitigation, etc.
- Index state management

  Automate and manage indices based on age, size, or document cardinality
- Notebooks

  Data stories using data queried from Elasticsearch along side text
- Trace analytics

  Distributing tracing that connects trace and log data to resolve performance issues in distributed applications

Roadmap 2021



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

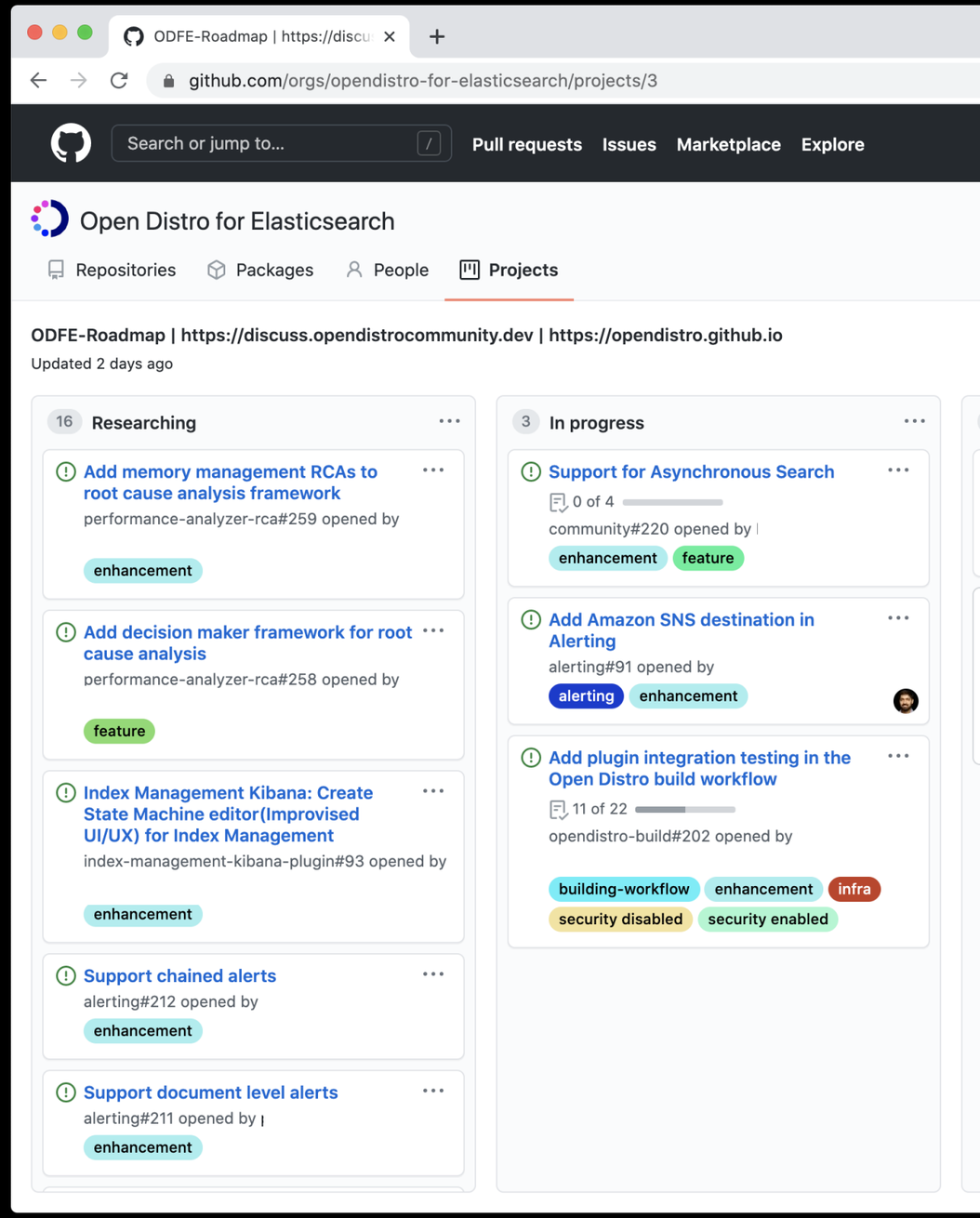
Focus areas for 2021

- Visualizations in Kibana
- Replication
- Ingest and transformation (Data Prepper)
- Deployment refinements (k8s operator)
- Geospatial enhancements
- Extensibility

Public active roadmap

We develop and plan publicly

opendistro.github.io/for-elasticsearch



Contributing and community



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to contribute

Elasticsearch plugins

- Kotlin: Alerting, Index State Management
- Java: all others

Kibana plugins

- Typescript

Tools

- Golang: odfe-cli
- Java: Performance Analyzer
- Python: sql-cli

Documentation

Website

Talk about us

Experience with k8s

Keep up-to-date and connected

Open Distro Community Meetings

- Hear from the team
- Live Q&A
- Connect with others

Open Distro Forums

- Ask and answer questions
- Find announcements

opendistro.github.io/for-elasticsearch/

Thank you!

Kyle J. Davis

@stockholmux
linkedin.com/in/kyle-davis-search/

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.