TESTING ELASTICSEARCH ALERTS LOCALLY: A LOCALSTACK APPROACH

How many of you have spent hours debugging production alerts only to realize they could have been caught earlier in the development cycle?

STORY TIME

Migration from Slack to MS Teams alerts

elasticsearch

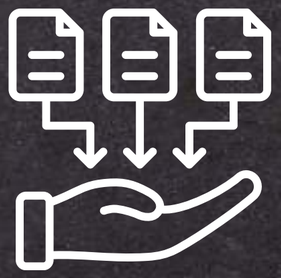
A DISTRIBUTED, RESTFUL SEARCH AND ANALYTICS ENGINE USED FOR A WIDE VARIETY OF USE CASES, INCLUDING LOGGING, METRICS ANALYSIS, AND SEARCH ENGINES

ELASTICSEARCH IN AWS

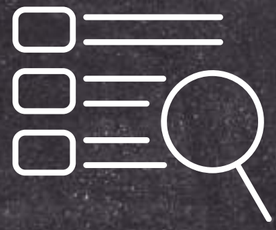
AWS provides a managed service called Amazon ElasticSearch Service, which simplifies the setup and management of ElasticSearch clusters

HOW ITS HELP?

COLLECTING

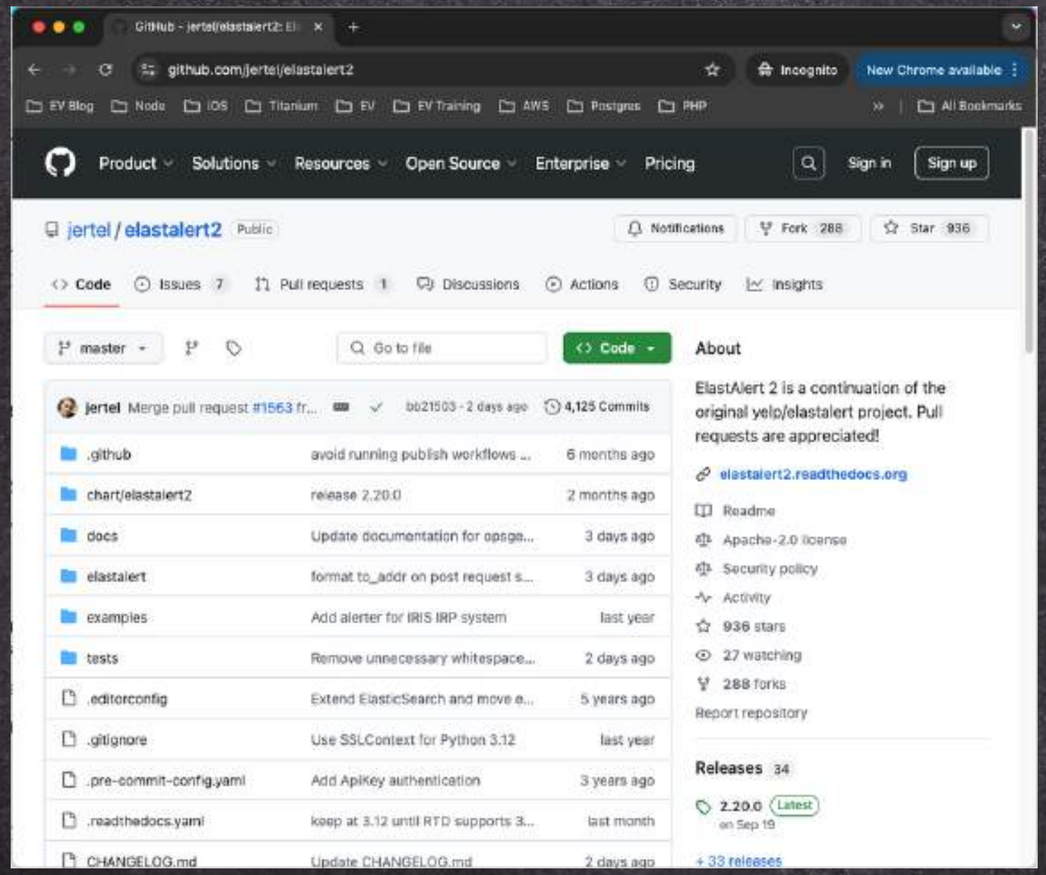


INDEXING



ANALYZING

ELASTALERT?



- ElastAlert is an alerting framework built on top of Elasticsearch
- Alerts can be configured based on queries and thresholds and can send notifications to Slack, email, or other communication platforms

ALERT TYPE

1. Threshold-based alerts (e.g., trigger when error rate exceeds a certain limit).

2. Missing data alerts (e.g., trigger if a specific log is missing).

3. Time-based alerts (e.g., trigger when no data is received in a specific timeframe).

WHY LOCAL TESTING WITH LOCALSTACK?

COST-EFFICIENT

You don't need to use AWS resources during local testing.

FASTER DEVELOPMENT CYCLE

LocalStack allows you to test and iterate quickly without the need to deploy to the cloud each time

SAFE TESTING

You can simulate and test alerts without risking production data

LOCALSTACK VS. AWS CLOUD TESTING

TESTING LOCALLY ALLOWS YOU TO CATCH ISSUES EARLY IN THE DEVELOPMENT CYCLE AND ENSURES SMOOTHER DEPLOYMENT WHEN MIGRATING TO AWS

SHOW TIME

ENOUGH OF THEORY

CONCLUSION

his setup is ideal for development and testing environments where you can validate your alerting rules before deploying them to production

REFERENCES

- https://www.internetkatta.com/how-to-test-elastalert-locally-using-localstack-a-step-by-step-guide
- https://elastalert.readthedocs.io/en/latest/index.html

Thank You

Connect with me

avinashdalvi.com

@AvinashDalvi_

@LearnWithAvinashDalvi