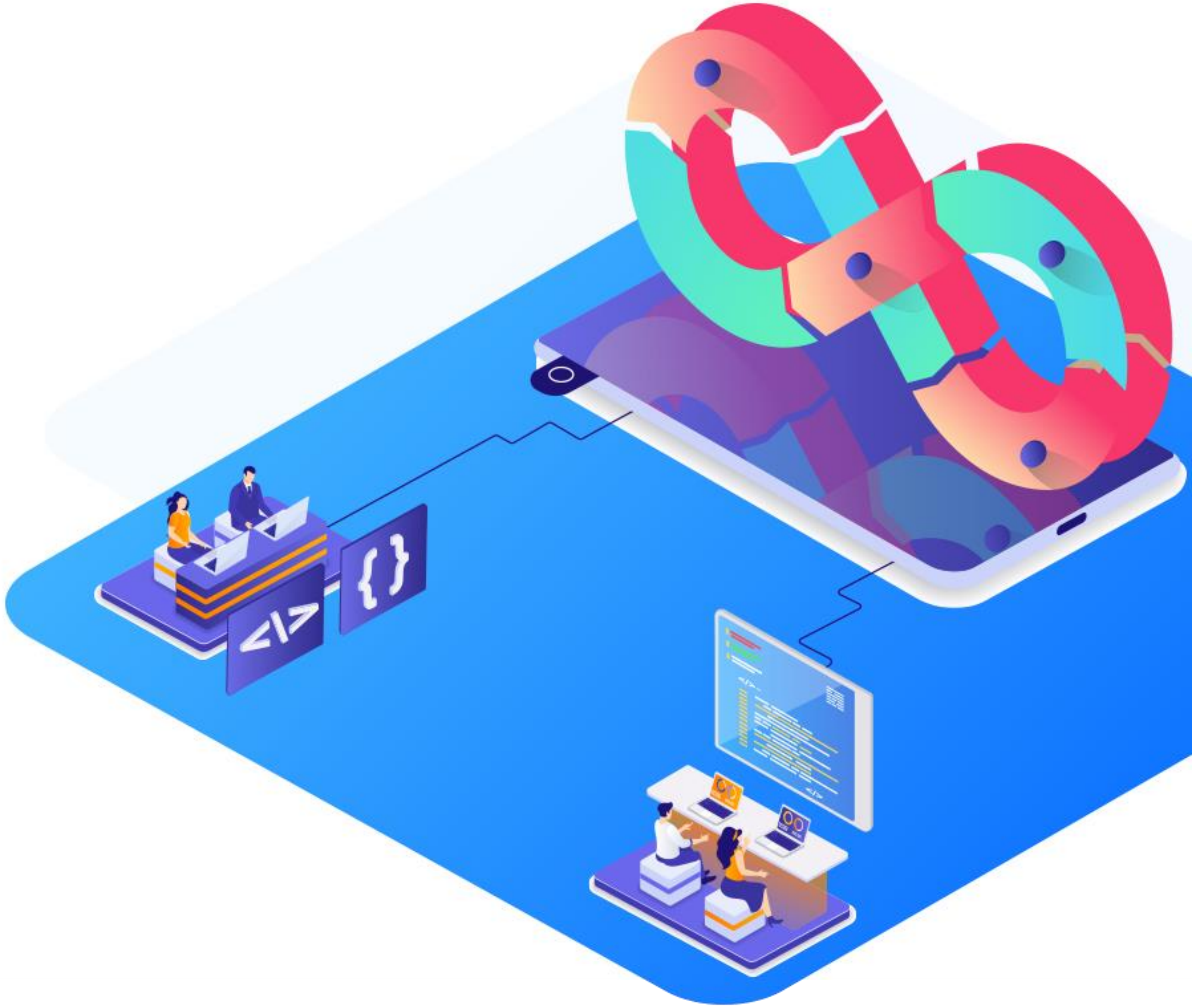
Monitoring and Logging



Course-End Project

Publishing Application Logs Directly to ELK Stack

Objective

To automate application log monitoring across environments using the ELK stack and a NodeJS application. This streamlines log collection, processing, and visualization with Elasticsearch, Logstash, and Kibana. The goal is to create dashboards and alerts for faster, high-quality software delivery.

Problem Statement and Motivation

Real-time scenario:

General Insurance, a leading global insurance provider based in the US, offers various products such as home, health, car, and life insurance. The company is transitioning to a DevOps architecture and aims to automate continuous monitoring across its environments.

To achieve this, they have adopted the ELK stack as their application monitoring tool. ELK stack will collect and process application logs using Logstash. However, to support the microservices architecture running on Docker containers, logs will be sent directly to the ELK stack.

By using ELK Stack and Docker, the company aims to provide continuous feedback to developers, speeding up software delivery, improving quality, and reducing the feedback loop between developers and testers.

Industry Relevance

The following tools used in this project serve specific purposes within the industry:

1. **NodeJS**: It is a JavaScript runtime built on Chrome's V8 engine, enabling server-side execution of JavaScript. It excels in building scalable, event-driven, and real-time applications.

2. **Elasticsearch**: It is a distributed search and analytics engine designed for scalability and speed. It is commonly used for log and data analysis, enabling fast searches, filtering, and real-time insights.

3. **Kibana**: It is a data visualization and exploration tool used with Elasticsearch. It enables users to create real-time dashboards, graphs, and reports to analyze and visualize data stored in Elasticsearch.

4. **Logstash**: It is a server-side data processing pipeline that ingests, filters, and transforms data from multiple sources. It works with Elasticsearch to process and analyze logs and events in real time.

Tasks

The following tasks outline the process of publishing application logs directly to ELK Stack:

1. Install Elasticsearch and Logstash components on the Linux terminal

2. Configure NodeJS application to publish application logs to ELK stack using Filebeat directly

3. Configure Kibana visualization tool to visualize application logs

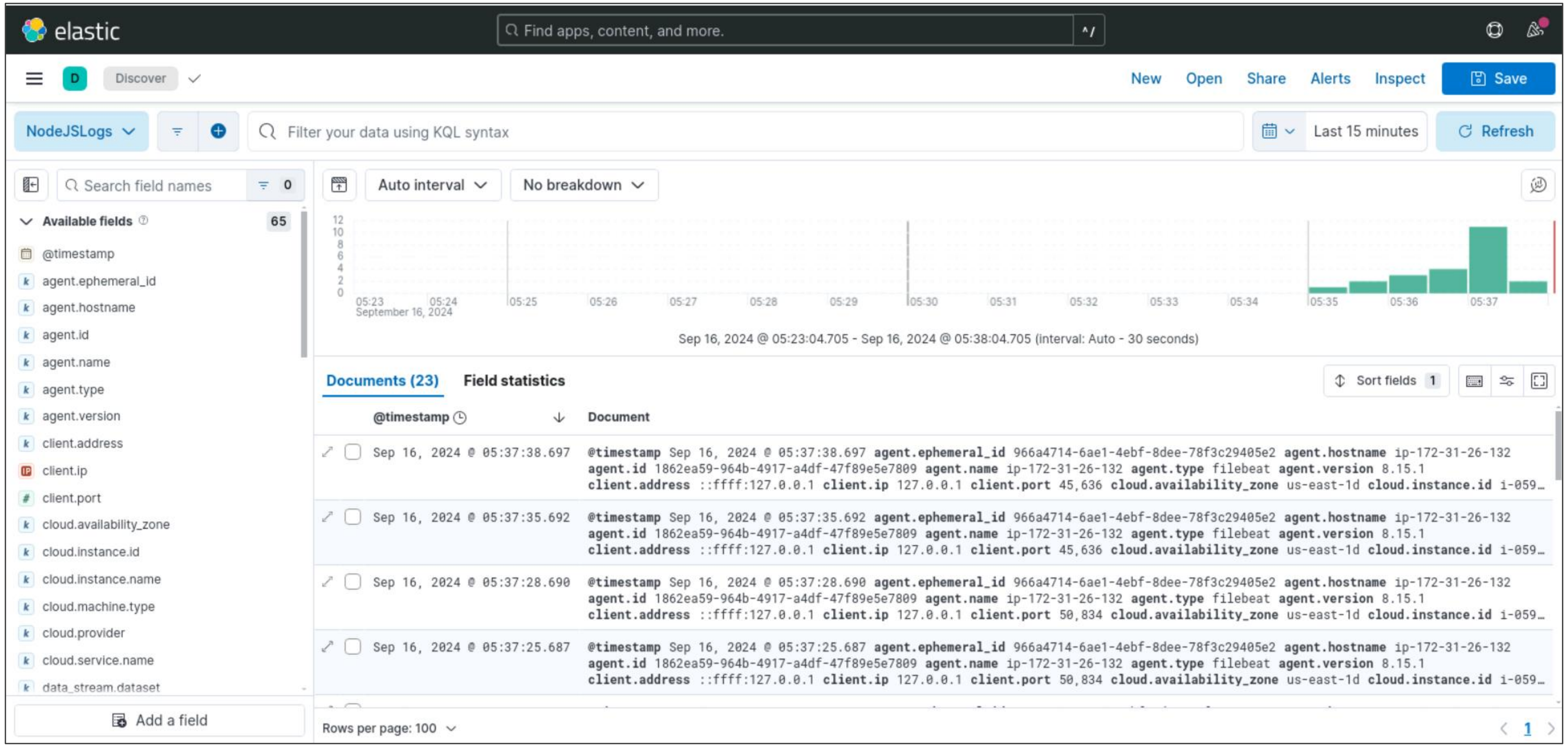
4. Create application logs dashboard

Project References

- **Task 1**: Lesson 05
- **Task 2**: Lesson 05
- **Task 3**: Lesson 05
- **Task 4**: Lesson 05

Output Screenshots

Kibana log data exploration page:



Available fields 65

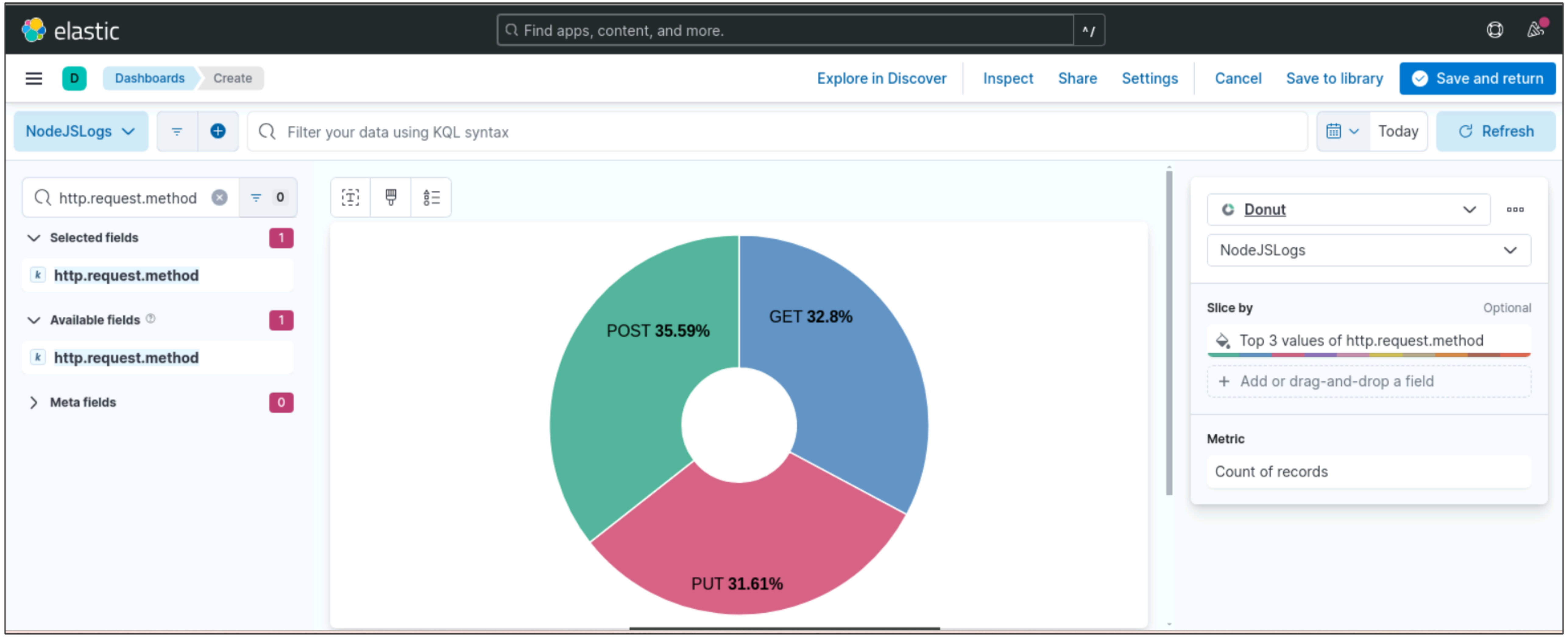
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- client.address
- client.ip
- client.port
- cloud.availability_zone
- cloud.instance.id
- cloud.instance.name
- cloud.machine.type
- cloud.provider
- cloud.service.name
- data_stream.dataset

Sep 16, 2024 @ 05:23:04.705 - Sep 16, 2024 @ 05:38:04.705 (interval: Auto - 30 seconds)

```
@timestamp                  Document
Sep 16, 2024 @ 05:37:38.697 @timestamp Sep 16, 2024 @ 05:37:38.697 agent.ephemeral_id 966a4714-6ae1-4ebf-8dee-78f3c29405e2 agent.hostname ip-172-31-26-132
                            agent.id 1862ea59-964b-4917-a4df-47f89e5e7809 agent.name ip-172-31-26-132 agent.type filebeat agent.version 8.15.1
                            client.address ::ffff:127.0.0.1 client.ip 127.0.0.1 client.port 45,636 cloud.availability_zone us-east-1d cloud.instance.id i-059…
Sep 16, 2024 @ 05:37:35.692 @timestamp Sep 16, 2024 @ 05:37:35.692 agent.ephemeral_id 966a4714-6ae1-4ebf-8dee-78f3c29405e2 agent.hostname ip-172-31-26-132
                            agent.id 1862ea59-964b-4917-a4df-47f89e5e7809 agent.name ip-172-31-26-132 agent.type filebeat agent.version 8.15.1
                            client.address ::ffff:127.0.0.1 client.ip 127.0.0.1 client.port 45,636 cloud.availability_zone us-east-1d cloud.instance.id i-059…
Sep 16, 2024 @ 05:37:28.690 @timestamp Sep 16, 2024 @ 05:37:28.690 agent.ephemeral_id 966a4714-6ae1-4ebf-8dee-78f3c29405e2 agent.hostname ip-172-31-26-132
                            agent.id 1862ea59-964b-4917-a4df-47f89e5e7809 agent.name ip-172-31-26-132 agent.type filebeat agent.version 8.15.1
                            client.address ::ffff:127.0.0.1 client.ip 127.0.0.1 client.port 50,834 cloud.availability_zone us-east-1d cloud.instance.id i-059…
Sep 16, 2024 @ 05:37:25.687 @timestamp Sep 16, 2024 @ 05:37:25.687 agent.ephemeral_id 966a4714-6ae1-4ebf-8dee-78f3c29405e2 agent.hostname ip-172-31-26-132
                            agent.id 1862ea59-964b-4917-a4df-47f89e5e7809 agent.name ip-172-31-26-132 agent.type filebeat agent.version 8.15.1
                            client.address ::ffff:127.0.0.1 client.ip 127.0.0.1 client.port 50,834 cloud.availability_zone us-east-1d cloud.instance.id i-059…
```

Output Screenshots

Kibana dashboard visualization creation page:



Thank you