ELK Stack — Real-Time Log Monitoring on AWS EC2:

Project: Real-Time Log Monitoring using ELK (**Elasticsearch, Logstash**, **Kibana**) deployed on AWS EC2.

1. Project Overview

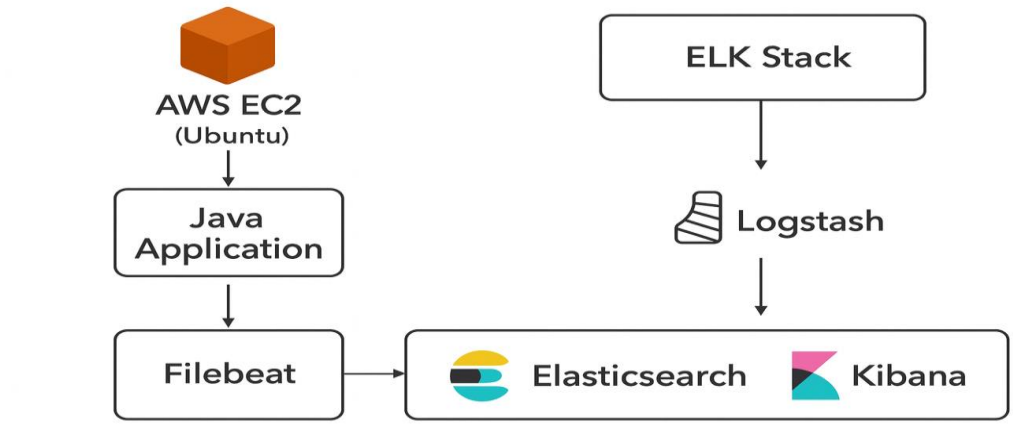
This project builds a scalable, real-time log monitoring solution for applications running on AWS EC2 using the ELK stack. Logs from application and system services are shipped by Filebeat to Logstash for parsing and enrichment, indexed into Elasticsearch for search and analytics, and visualized with Kibana dashboards for live monitoring, alerting, and troubleshooting.

Primary goals:

- Centralize logs from multiple servers and applications
- Provide real-time searching and visualization

2. Tech Stack Used

- **Cloud / Infrastructure:** AWS EC2 (Ubuntu 22.04)
- **Log collection:** Filebeat (Beats)
- **Log processing:** Logstash
- **Storage & Search:** Elasticsearch (single-node for demo / clustered for prod)
- **Visualization:** Kibana
- **Java spring boot application**
- **Grok filters**
- **Linux Terminal(ubuntu)**



ELK Stack

The **ELK Stack** consists of:

- **Elasticsearch** → Stores and indexes logs.
- **Logstash** → Processes and transforms logs before storing them in Elasticsearch.
- **Kibana** → Provides visualization and analysis of logs.
- **Filebeat** → Forwards logs from the application to Logstash.

3. Step-by-Step Installation

Step 1: Install & Configure Elasticsearch (ELK Server)

1.1 Install Java (Required for Elasticsearch & Logstash)

sudo apt update && sudo apt install openjdk-17-jre-headless -y

1.2 Install Elasticsearch

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add - echo "deb

https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list sudo

apt update

sudo apt install elasticsearch -y

1.3 Configure Elasticsearch

sudo vi /etc/elasticsearch/elasticsearch.yml Modify:

network.host: 0.0.0.0

cluster.name: my-cluster

node.name: node-1

discovery.type: single-node

1.4 Start & Enable Elasticsearch

sudo systemctl start elasticsearch sudo

systemctl enable elasticsearch sudo

systemctl status elasticsearch

1.5 Verify Elasticsearch

```
curl -X GET "http://localhost:9200"
```

Step 2: Install & Configure Logstash (ELK Server)

2.1 Install Logstash

```
sudo apt install logstash -y
```

2.2 Configure Logstash to Accept Logs

sudo vi /etc/logstash/conf.d/logstash.conf Add:

```
input    {
  beats {
    port => 5044
  }

}


filter {
  grok {
    match => { "message" => "%{TIMESTAMP_ISO8601:log_timestamp} %{LOGLEVEL:log_level}
%{GREEDYDATA:log_message}"  }
  }

}



output {
elasticsearch {
    hosts => ["http://localhost:9200"] index
    => "logs-%{+YYYY.MM.dd}"
  }

  stdout { codec => rubydebug }
}
```

2.3 Start & Enable Logstash

```
sudo systemctl start logstash

sudo systemctl enable logstash

sudo systemctl status logstash
```

2.4 Allow Traffic on Port 5044

sudo ufw allow 5044/tcp

Step 3: Install & Configure Kibana (ELK Server)

3.1 Install Kibana

sudo apt install kibana -y

3.2 Configure Kibana

sudo vi /etc/kibana/kibana.yml

Modify:

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://localhost:9200"]

3.3 Start & Enable Kibana

sudo systemctl start kibana sudo

systemctl enable kibana sudo

systemctl status kibana

3.4 Allow Traffic on Port 5601

sudo ufw allow 5601/tcp

3.5 Access Kibana Dashboard

Open a browser and go to:

http://<ELK_Server_Public_IP>:5601\

Step 4: Install & Configure Filebeat (Client Machine)

4.1 Install Filebeat

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add - echo "deb

https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list sudo

apt update

sudo apt install filebeat -y

4.2 Configure Filebeat to Send Logs to Logstash

sudo vi /etc/filebeat/filebeat.yml

Modify:

```
filebeat.inputs:
  - type: log
    enabled: true
    paths:
      - /home/ubuntu/Boardgame/target/app.log

output.logstash:
  hosts: ["<ELK_Server_Private_IP>:5044"]
```

4.3 Start & Enable Filebeat

sudo systemctl start filebeat sudo

systemctl enable filebeat sudo

systemctl status filebeat

4.4 Verify Filebeat is Sending Logs

sudo filebeat test output

Step 5: Deploy Java Application & Generate Logs

5.1 Install Java (If Not Installed)

sudo apt install openjdk-17-jre-headless -y

5.2 Download & Run Sample Java App

wget https://repo1.maven.org/maven2/org/springframework/boot/spring-boot-sample-simple/1.4.2.RELEASE/spring-boot-sample-simple-1.4.2.RELEASE.jar -O app.jar

nohup java -jar app.jar > /home/ubuntu/Boardgame/target/app.log 2>&1 &

5.3 Verify Java Application is Running

5.4 Generate Logs for Testing

echo "Test log entry $(date)" >> /home/ubuntu/Boardgame/target/app.log

Step 6: View & Analyze Logs in Kibana

6.1 Open Kibana Discover

1. Go to **Kibana → Discover**.
2. Select log* index.
3. Search for:

log.file.path: "/home/ubuntu/Boardgame/target/app.log"

4. View structured fields (log_timestamp, log_level, log_message).

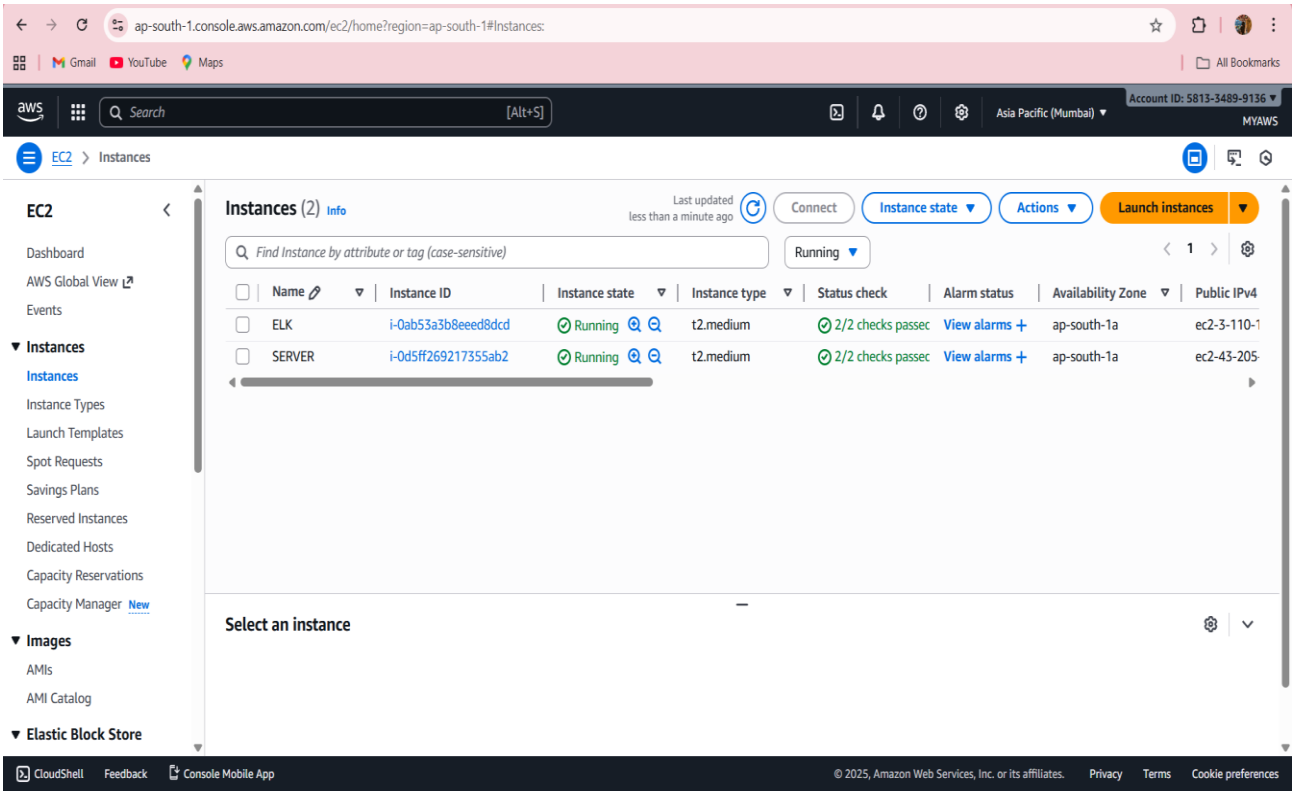
6.2 Create Kibana Visualizations

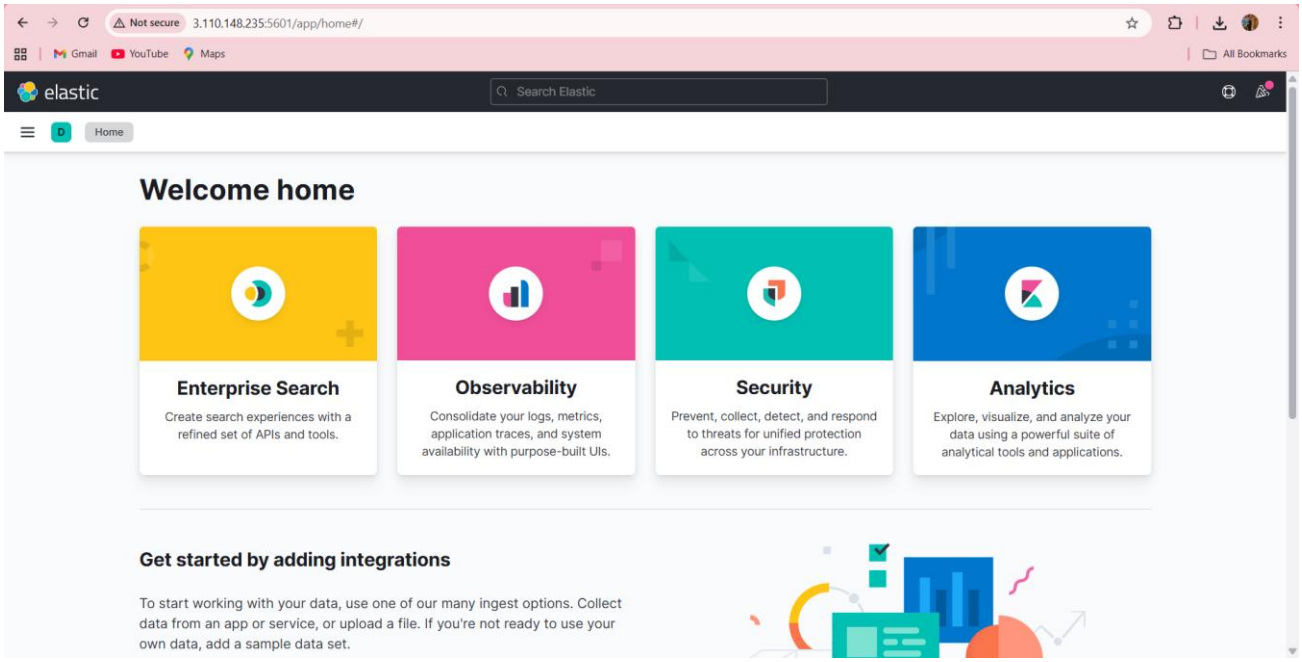
1. **Pie Chart** → Log level distribution.
2. **Line Chart** → Logs over time.
3. **Data Table** → Structured log table.

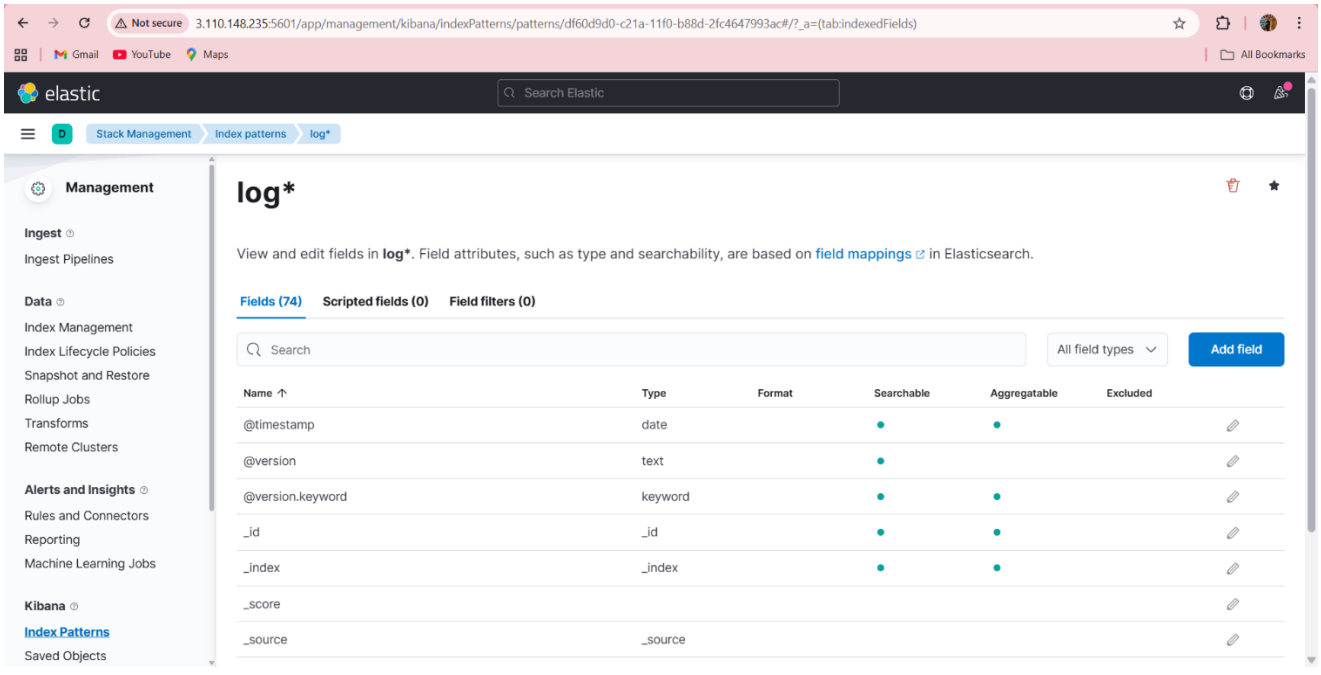
6.3 Create a Kibana Dashboard

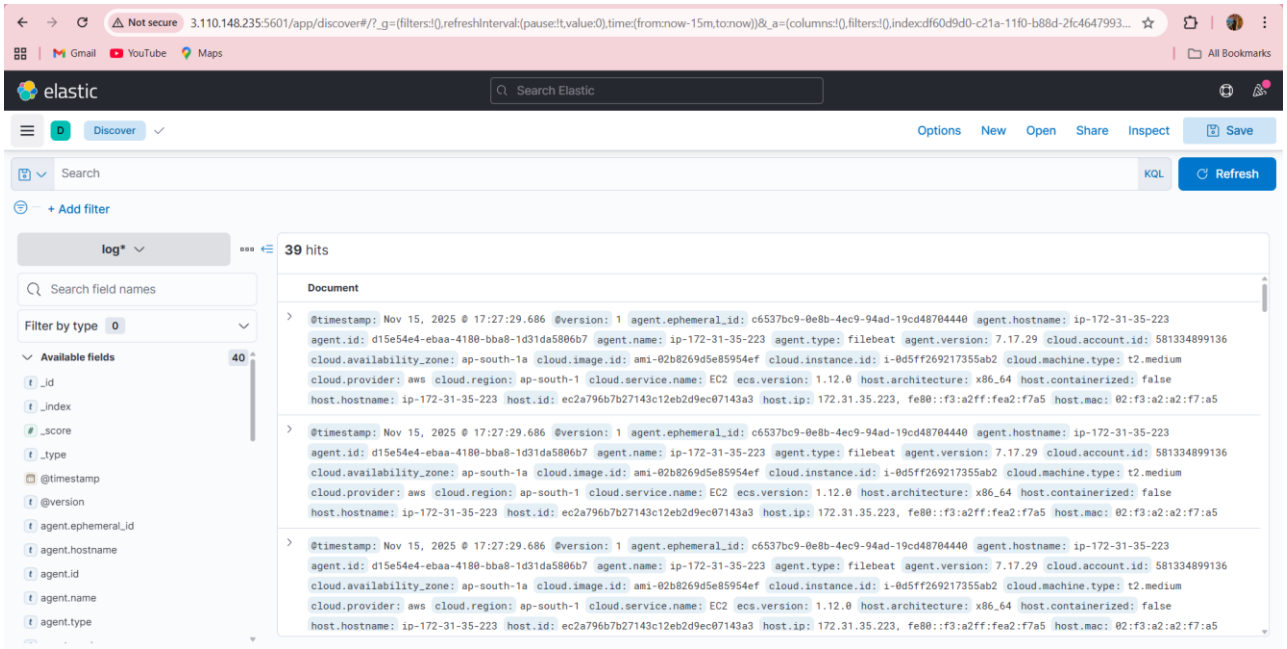
1. **Go to Kibana → Dashboard → Create Dashboard**.
2. Add **Pie Chart, Line Chart, Data Table**.
3. Save as "Java Application Log Monitoring".

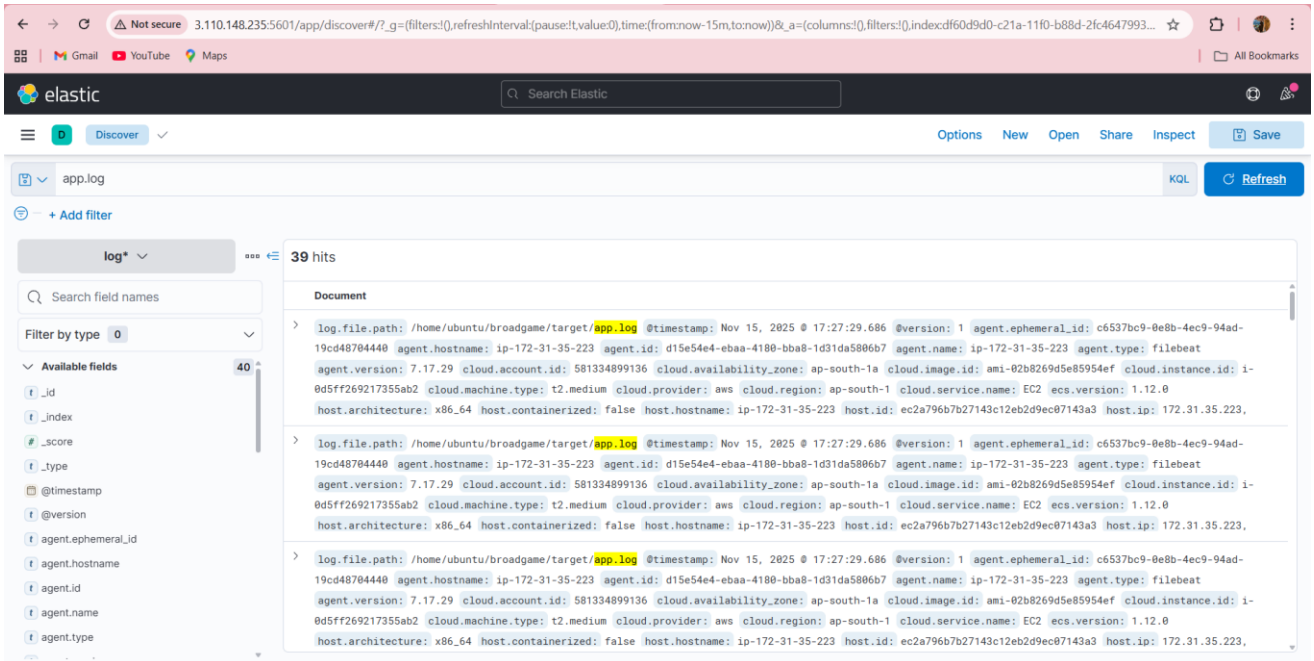
4. Screenshot & output

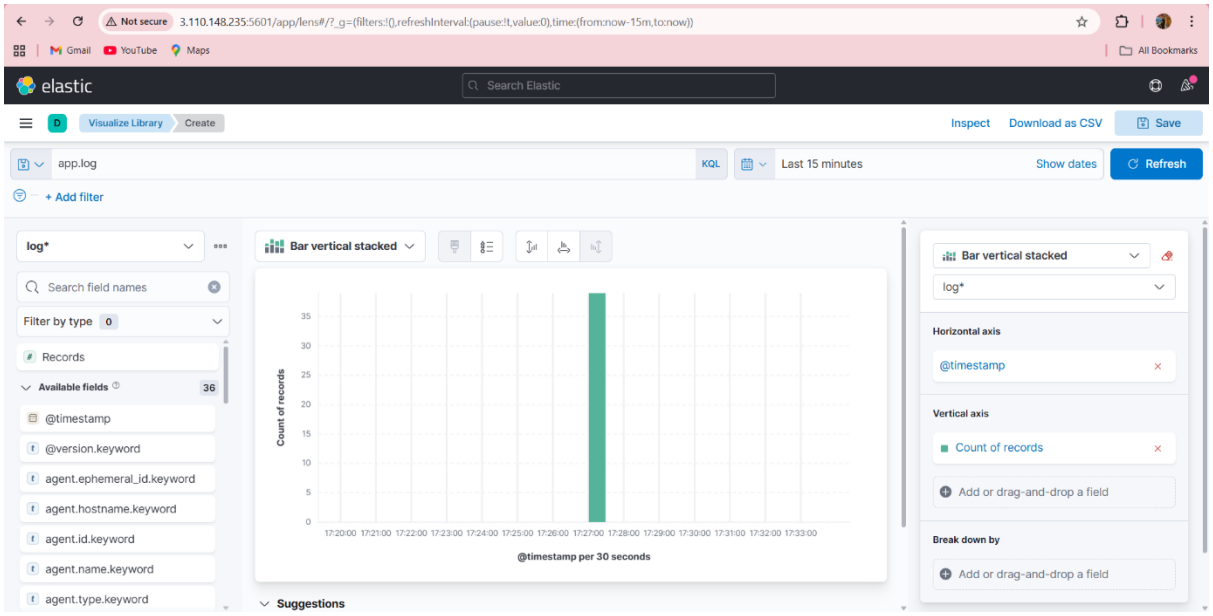


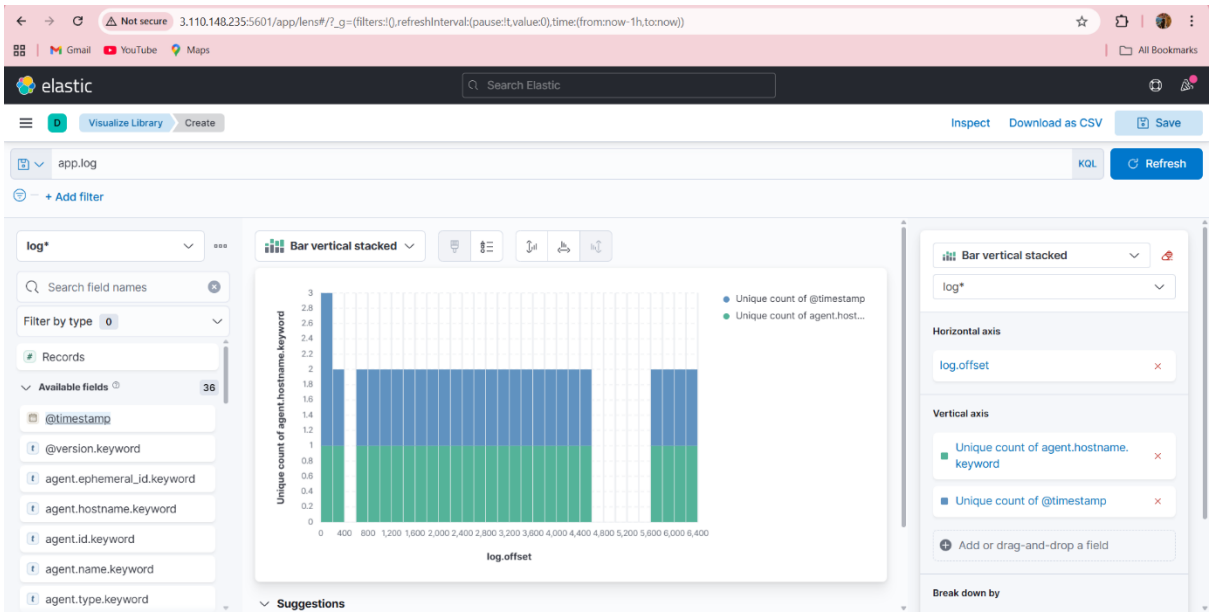

Not secure 3.110.148.235:5601/app/home#/
Gmail YouTube Maps
All Bookmarks
elastic
Search Elastic
D Home
Welcome home
Enterprise Search
Create search experiences with a refined set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
Get started by adding integrations
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.


Not secure 3.110.148.235:5601/app/management/kibana/indexPatterns/patterns/df60d9d0-c21a-11f0-b88d-2fc4647993ac#/?_a=(tab:indexedFields)
Gmail YouTube Maps
All Bookmarks
elastic
Search Elastic
D Stack Management Index patterns log*
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
log*
View and edit fields in log*. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (74) Scripted fields (0) Field filters (0)
Search
All field types
Add field
Name ↑ Type Format Searchable Aggregatable Excluded
@timestamp date
@version text
@version.keyword keyword
_id _id
_index _index
_score
_source _source


Not secure 3.110.148.235:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!(),index:df60d9d0-c21a-11f0-b88d-2fc4647993...
Gmail YouTube Maps All Bookmarks
elastic Search Elastic
Discover Options New Open Share Inspect Save
Search KQL Refresh
+ Add filter
log* 39 hits
Search field names
Filter by type 0
Available fields 40
_id _index _score _type @timestamp @version agent.ephemeral_id agent.hostname agent.id agent.name agent.type
Document
@timestamp: Nov 15, 2025 @ 17:27:29.686 @version: 1 agent.ephemeral_id: c6537bc9-0e8b-4ec9-94ad-19cd48704440 agent.hostname: ip-172-31-35-223 agent.id: d15e54e4-ebaa-4180-bba8-1d31da5806b7 agent.name: ip-172-31-35-223 agent.type: filebeat agent.version: 7.17.29 cloud.account.id: 581334899136 cloud.availability_zone: ap-south-1a cloud.image.id: ami-02b8269d5e85954ef cloud.instance.id: i-0d5ff269217355ab2 cloud.machine.type: t2.medium cloud.provider: aws cloud.region: ap-south-1 cloud.service.name: EC2 ecs.version: 1.12.0 host.architecture: x86_64 host.containerized: false host.hostname: ip-172-31-35-223 host.id: ec2a796b7b27143c12eb2d9ec07143a3 host.ip: 172.31.35.223, fe80::f3:a2ff:fea2:f7a5 host.mac: 02:f3:a2:a2:f7:a5


Not secure 3.110.148.235:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!(),index:df60d9d0-c21a-11f0-b88d-2fc4647993...
Gmail YouTube Maps All Bookmarks
elastic Search Elastic
Discover Options New Open Share Inspect Save
app.log KQL Refresh
+ Add filter
log* 39 hits
Search field names
Filter by type 0
Available fields 40
_id _index _score _type @timestamp @version agent.ephemeral_id agent.hostname agent.id agent.name agent.type
Document
log.file.path: /home/ubuntu/broadgame/target/app.log @timestamp: Nov 15, 2025 @ 17:27:29.686 @version: 1 agent.ephemeral_id: c6537bc9-0e8b-4ec9-94ad-19cd48704440 agent.hostname: ip-172-31-35-223 agent.id: d15e54e4-ebaa-4180-bba8-1d31da5806b7 agent.name: ip-172-31-35-223 agent.type: filebeat agent.version: 7.17.29 cloud.account.id: 581334899136 cloud.availability_zone: ap-south-1a cloud.image.id: ami-02b8269d5e85954ef cloud.instance.id: i-0d5ff269217355ab2 cloud.machine.type: t2.medium cloud.provider: aws cloud.region: ap-south-1 cloud.service.name: EC2 ecs.version: 1.12.0 host.architecture: x86_64 host.containerized: false host.hostname: ip-172-31-35-223 host.id: ec2a796b7b27143c12eb2d9ec07143a3 host.ip: 172.31.35.223,


Not secure 3.110.148.235:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))
elastic
Search Elastic
Visualize Library
Create
Inspect
Download as CSV
Save
app.log
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
log*
Search field names
Filter by type 0
Records
Available fields 36
@timestamp
@version.keyword
agent.ephemeral_id.keyword
agent.hostname.keyword
agent.id.keyword
agent.name.keyword
agent.type.keyword
Bar vertical stacked
Count of records
@timestamp per 30 seconds
Suggestions
Bar vertical stacked
log*
Horizontal axis
@timestamp
Vertical axis
Count of records
Add or drag-and-drop a field
Break down by
Add or drag-and-drop a field


Not secure 3.110.148.235:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-1h,to:now))
elastic
Search Elastic
Visualize Library
Create
Inspect
Download as CSV
Save
app.log
KQL
Refresh
+ Add filter
log*
Search field names
Filter by type 0
Records
Available fields 36
@timestamp
@version.keyword
agent.ephemeral_id.keyword
agent.hostname.keyword
agent.id.keyword
agent.name.keyword
agent.type.keyword
Bar vertical stacked
Unique count of agent.hostname.keyword
log.offset
Unique count of @timestamp
Unique count of agent.host...
Suggestions
Bar vertical stacked
log*
Horizontal axis
log.offset
Vertical axis
Unique count of agent.hostname.keyword
Unique count of @timestamp
Add or drag-and-drop a field
Break down by

5. Key Learnings & DevOps Relevance

Technical learnings:

- How beats (Filebeat) efficiently harvest logs and forward them to centralized pipelines.
- Using Logstash filters to parse, enrich, and normalize heterogeneous logs (grok, json, date, mutate).
- Elasticsearch index lifecycle basics, index patterns, and searching using Kibana.
- Designing dashboards for operational visibility and rapid troubleshooting.

Conclusion

You have successfully:

- Installed **Elasticsearch, Logstash, Kibana, and Filebeat**
- Set up a **Java application to generate logs**
- Parsed logs into **structured fields using Grok**
- Created a **real-time Kibana dashboard for log monitoring**