IBM MQ Integration with ELK (Elasticsearch, Logstash, Kibana) Stack

This document contains the **complete steps**, **configurations**, and **troubleshooting** actions performed during the setup of IBM MQ monitoring using **Filebeat** and **ELK stack**.

✅Prerequisites

- RHEL Server with root access
- IBM MQ installed and running
- ELK stack:
- Elasticsearch (8.18.3)
- Kibana
- Filebeat (8.18.3)
- Internet access or proper repositories

✔️Step-by-Step Setup

1. Install Elasticsearch

```
sudo rpm --install elasticsearch.rpm
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
```

> If TLS is enabled, remember to retrieve and store the generated password from installation logs or `/etc/elasticsearch/elasticsearch.keystore`

2. Verify Elasticsearch

```
curl -k https://localhost:9200
# Should return security_exception unless auth is provided

curl -k -u elastic:<password> https://localhost:9200
```

3. Install Kibana

```
sudo rpm -ivh kibana.rpm
sudo systemctl enable kibana
sudo systemctl start kibana
```

- Access Kibana at: `http://<host>:5601`
- Login using `elastic` user and password from Elasticsearch setup

4. Install Filebeat

```
sudo rpm -ivh filebeat.rpm
```

5. Enable IBM MQ Filebeat Module

```
sudo filebeat modules enable ibmmq
```

6. Edit Filebeat Configuration

File: `/etc/filebeat/filebeat.yml`

```
output.elasticsearch:
  hosts: ["https://localhost:9200"]
  username: "elastic"
  password: "<password>"
  ssl.verification_mode: none
```

7. Test Filebeat Configuration

```
sudo filebeat test config
sudo filebeat test output
```

Ensure `connection` and `TLS handshake` show OK

8. Start Filebeat

```
sudo systemctl start filebeat
sudo systemctl enable filebeat
```

9. Setup Filebeat Index Management and Dashboards

```
sudo filebeat setup --index-management \
  -E output.elasticsearch.hosts=["https://localhost:9200"] \
  -E output.elasticsearch.username=elastic \
  -E output.elasticsearch.password="<password>"

sudo filebeat setup --dashboards
```

10. Verify Indexes Created

```
curl -k -u elastic:<password> https://localhost:9200/_cat/indices?v | grep
filebeat
```

🈂️Kibana Dashboard Configuration

1. Create Data View in Kibana

- Navigate to: `Stack Management > Data Views`
- Create view:
- Index pattern: `filebeat-*`
- Timestamp field: `@timestamp`

2. Verify Dashboards

- Navigate to: `Kibana > Dashboard`
- Look for:
- **Filebeat IBM MQ** Overview of error log overview
- **Overview of IBM MQ**

If not present:

```
sudo filebeat setup --dashboards
```

✡️Troubleshooting Summary

❌Filebeat Not Sending Data to Elasticsearch

Error: `ERROR Get "http://localhost:9200": EOF`

- **Solution:**

- Ensure Elasticsearch is running: `systemctl status elasticsearch`
- Update Filebeat to use HTTPS and correct credentials
- Update `filebeat.yml` to:

```
output.elasticsearch:
  hosts: ["https://localhost:9200"]
  username: "elastic"
  password: "<password>"
  ssl.verification_mode: none
```

❌No logs in Kibana Discover View

- **Reason:** Data view not created or index not matched
- **Fix:**
- Create data view: `filebeat-*`
- Set time range to `Last 24 hours` or `Last 7 days`

❌Kibana Dashboard is Empty After Click

- **Cause:** You clicked on create dashboard instead of opening pre-loaded ones
- **Fix:**
- Go to `Dashboard`
- Search `IBM MQ`
- Click on `[Filebeat IBM MQ] Overview of error log overview`

❌Journalctl Shows Filebeat Cannot Connect

- **Fix:**
- Check credentials and `filebeat.yml`
- Restart filebeat and monitor logs

```
sudo systemctl restart filebeat
sudo journalctl -u filebeat -f
```

✅Outcome

You now have:

- IBM MQ error logs (/var/mqm/qmgrs//*errors/AMQERR*.LOG) shipping via Filebeat
- Data indexed into Elasticsearch securely
- Visual dashboards in Kibana under `Filebeat IBM MQ`

🚫 Optional Security Enhancements

- Replace `ssl.verification_mode: none` with valid CA
- Use service account for Filebeat access

🟡 Reference Links

- IBM MQ Filebeat Module Docs: https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-ibmmq.html
- Elastic Stack Security Guide: https://www.elastic.co/guide/en/elasticsearch/reference/current/configuring-stack-security.html