IBM MQ Log Monitoring with ELK Stack

Architecture Overview

```
[IBM MQ Queue Manager Logs]
        ->
     Filebeat (ibmmq module, harvester)
        ->
Ingest Pipeline in Elasticsearch
        ->
  Elasticsearch Indices
        ->
       Kibana (Dashboards)
```

Component Details

1. Filebeat (Log Forwarder)

- Installed on MQ host to monitor /var/mqm/qmgrs/*/errors/*.LOG

- Parses multiline MQ logs using ibmmq module

- Sends logs to Elasticsearch

2. Ingest Pipeline in Elasticsearch

- Created using `filebeat setup`

- Parses logs into ECS fields (ibmmq.errorlog.qmgr, .code, .explanation, etc.)

3. Elasticsearch Indices & ILM

- Logs stored in indices like filebeat-8.x-ibmmq-errorlog-*

- ILM manages rollover and retention

4. Kibana (UI)

- Visualize structured MQ logs using dashboards

Setup and Configuration Steps

```
1. Enable Filebeat ibmmq module:
   sudo filebeat modules enable ibmmq

2. Configure ibmmq log path in /etc/filebeat/modules.d/ibmmq.yml:
   - module: ibmmq
     errorlog:
       enabled: true
       var.paths: ["/var/mqm/qmgrs/*/errors/*.LOG"]
```

```
3. Edit /etc/filebeat/filebeat.yml paths:
   path.config: /etc/filebeat
   path.data: /var/lib/filebeat
   path.logs: /var/log/filebeat

4. Deploy pipelines and dashboards:
   sudo filebeat setup -E output.elasticsearch.hosts=["https://localhost:9200"] \
     -E output.elasticsearch.username=elastic \
     -E output.elasticsearch.password="your_password"

5. Restart Filebeat:
   sudo systemctl restart filebeat
```

Log Paths and Service Commands

```
- Filebeat logs: /var/log/filebeat/filebeat.log
- Elasticsearch logs: /var/log/elasticsearch/elasticsearch.log
- Kibana logs: /var/log/kibana.log

Service Commands:
- systemctl status|restart filebeat|elasticsearch|kibana
- journalctl -u filebeat -f
```

Common Troubleshooting

```
- Check Filebeat ingestion: tail -f /var/log/filebeat/filebeat.log
- Elasticsearch indices: curl -s localhost:9200/_cat/indices?v | grep filebeat
- Pipelines: curl -s localhost:9200/_ingest/pipeline/ibmmq*
- Reset Filebeat registry:
  sudo systemctl stop filebeat
  sudo rm -f /var/lib/filebeat/registry/*
  sudo systemctl start filebeat
```