IBM MQ Monitoring with ELK - Setup and Troubleshooting

Setup Steps

1. Installed and started Elasticsearch and Kibana.
2. Verified Elasticsearch on https://localhost:9200.
3. Logged into Kibana UI using default credentials (elastic + generated password).
4. Installed Filebeat and enabled the 'ibmmq' module.
5. Configured Filebeat to forward logs to Elasticsearch securely (TLS enabled).
6. Verified Filebeat connection to Elasticsearch with 'filebeat test output'.
7. Checked Filebeat logs using 'journalctl -u filebeat -f' to ensure input/output work.
8. Verified index creation using curl and _cat/indices API.
9. Created a data view in Kibana using the pattern 'filebeat-*'.
10. Loaded IBM MQ Filebeat dashboards using 'filebeat setup --dashboards'.
11. Opened dashboards like:
    - [Filebeat IBM MQ] Overview of error log overview
    - Overview of IBM MQ

Troubleshooting Summary

1. Issue: Filebeat unable to talk to Elasticsearch (EOF error)
   Cause: Using HTTP instead of HTTPS while Elasticsearch was secured.
   Solution: Changed the output URL to https://localhost:9200 in filebeat.yml.

2. Issue: Kibana "No results match your search criteria"
   Cause: Index not setup or time filter mismatch.
   Solution: Verified data ingestion using curl, created data view 'filebeat-*', adjusted time range.

3. Issue: Dashboards not showing expected panels after selecting IBM MQ overview
   Cause: Dashboard created manually instead of importing existing.
   Solution: Used Filebeat's built-in dashboards via 'filebeat setup --dashboards', then accessed them through Kibana > Dashboard.

4. Warnings seen:
   - SSL/TLS verifications disabled in Filebeat logs
   - Alerting and notification APIs disabled in Kibana logs
   These are informational/warnings due to default or non-configured features, no impact on log ingestion.

Result: IBM MQ error logs are successfully forwarded from Filebeat to Elasticsearch and visualized in Kibana.