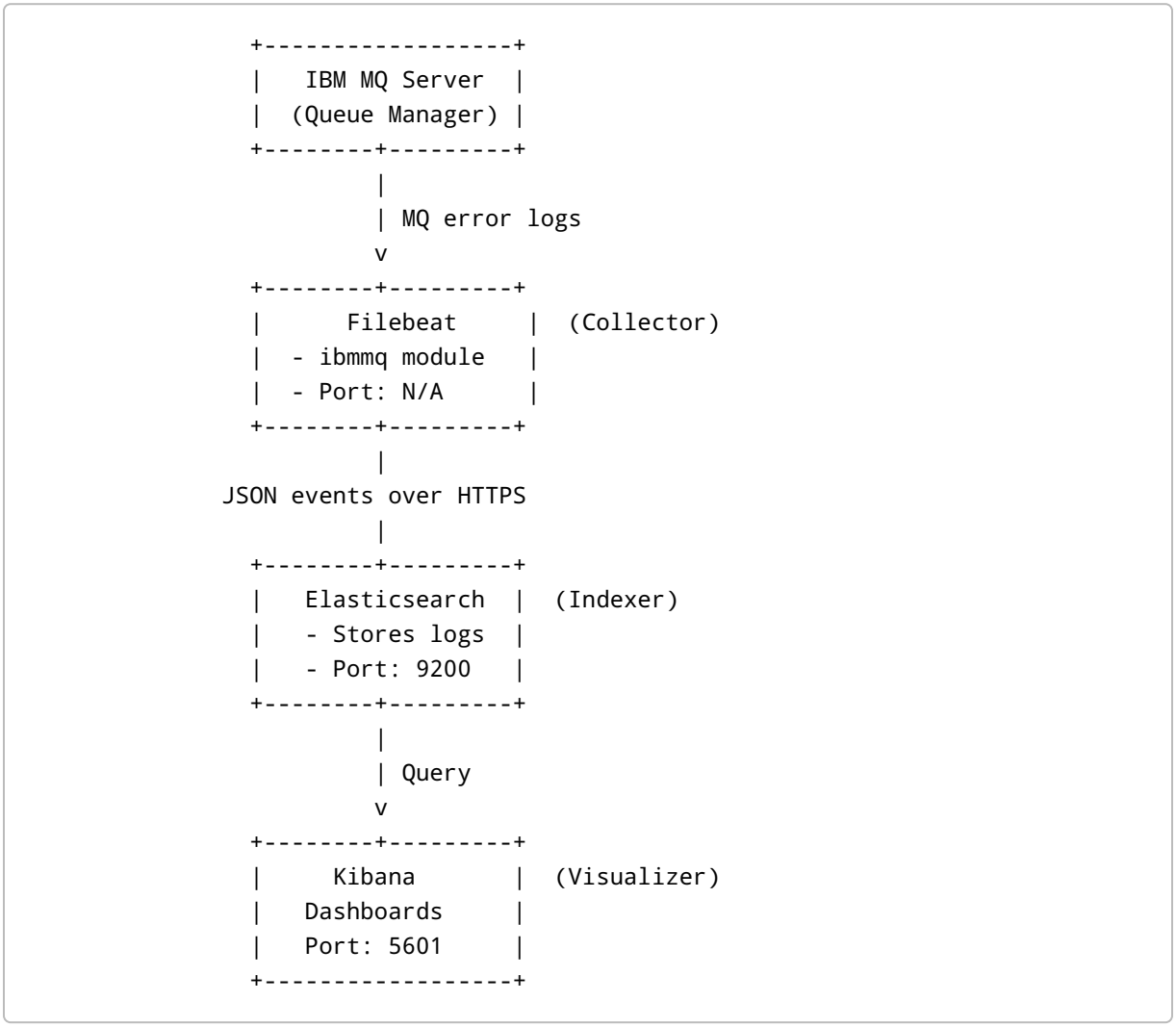
IBM MQ Log Monitoring Architecture with ELK Stack (Filebeat + Elasticsearch + Kibana)

📊Architecture Overview:



🕰️Component Details:

1. IBM MQ Server

- Generates logs like `AMQERR01.LOG`
- Path: `/var/mqm/qmgrs/<QMGR_NAME>/errors/`
- Port: Depends on queue manager listener (typically 1414)

2. Filebeat

- Installed on the same server as IBM MQ
- Uses `ibmmq` module to parse error logs
- Sends structured logs to Elasticsearch
- Port: N/A (acts as a client pushing logs)

Config Files:

- `/etc/filebeat/filebeat.yml`

```
filebeat.modules:
  - module: ibmmq
    error:
      enabled: true
      var.paths: ["/var/mqm/qmgrs/*/errors/AMQERR*.LOG"]

output.elasticsearch:
  hosts: ["https://localhost:9200"]
  username: "elastic"
  password: "<your_password>"
```

- Enable module:

```
sudo filebeat modules enable ibmmq
```

- Load dashboards & index template:

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

3. Elasticsearch

- Indexes and stores all MQ log data
- Accepts input from Filebeat
- Exposes data to Kibana
- Default Port: **9200**

Config File:

- `/etc/elasticsearch/elasticsearch.yml`

```
network.host: 0.0.0.0
http.port: 9200
cluster.name: elk-cluster
node.name: es-node-1
```

Check with:

```
curl -X GET "localhost:9200/_cat/indices?v"
```

4. Kibana

- Connects to Elasticsearch
- Visualizes `filebeat-*` index data
- Shows dashboards, e.g., error code distribution, queue manager errors
- Default Port: **5601**

Config File:

- `/etc/kibana/kibana.yml`

```
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.hosts: ["https://localhost:9200"]
elasticsearch.username: "elastic"
elasticsearch.password: "<your_password>"
```

Access: `http://<server-ip>:5601`

⚖️Service Start Order

1. **Elasticsearch**
2. **Kibana**
3. **Filebeat**

Start commands:

```
sudo systemctl start elasticsearch
sudo systemctl start kibana
sudo systemctl start filebeat
```

💡 Troubleshooting Tips

Component	Log File	Check Status	Default Port
Filebeat	`/var/log/filebeat/filebeat`	`journalctl -u filebeat`	N/A
Elasticsearch	`/var/log/elasticsearch/elasticsearch.log`	`curl localhost:9200/_cluster/health`	9200
Kibana	`/var/log/kibana/kibana.log`	`journalctl -u kibana`	5601

🔗 Notes:

- Logstash is **not needed** unless custom filtering is required.
- Ensure certificates are trusted if using HTTPS.
- Dashboards get created by `filebeat setup`.

Let me know if you want the same architecture as a PDF or image.