

1. Introduction to Logging

Importance of Logging

- **Purpose:** Logs provide insights into application behavior, help diagnose issues, and track performance.
- **Types of Logs:**
 - **Info:** General operational messages.
 - **Debug:** Detailed information for debugging.
 - **Warn:** Potential issues or unusual events.
 - **Error:** Errors that disrupt normal operations.

2. Spring Boot Logging Best Practices

Configuring Logging Levels

- Configuration in **application.properties**

```
logging.level.root=INFO
logging.file.name=app.log
logging.file.path=/path/to/logs
logging.pattern.console=%d{yyyy-MM-dd HH:mm:ss} - %msg%n
logging.pattern.file=%d{yyyy-MM-dd HH:mm:ss} - %msg%n
```

Structuring Log Messages

- **Include Key Information:** Timestamp, log level, message, and context.
- **Consistency:** Use a consistent format to make logs easier to read and analyze.

Log Rotation and Archival

- **Log Rotation:** Implement strategies to rotate logs to avoid large files.
- **Archival:** Archive old logs for historical analysis and compliance.

3. Introduction to ELK Stack

1. Overview of ELK Stack

- **Elasticsearch:** A distributed search and analytics engine used for storing and querying logs and other data.

- **Logstash:** A data processing pipeline that ingests logs, processes them, and forwards them to Elasticsearch.
- **Kibana:** A data visualization and exploration tool that provides powerful analytics and dashboard capabilities for data stored in Elasticsearch.

2. Setting Up Elasticsearch

- **Installation:** Install Elasticsearch following the official guide. Ensure it is running and accessible at <http://localhost:9200>.
- **Configuration:** Basic configuration involves setting up cluster name, network host, and port settings.

3. Integrating Kibana

- **Installation:** Install Kibana as per the official guide. Ensure it connects to the Elasticsearch instance.
- **Configuration:** Configure Kibana to use the Elasticsearch endpoint and set up index patterns to view the data.

4. Log Analysis with Kibana

- **Creating Visualizations:** Use Kibana's "Visualize" feature to create charts, graphs, and maps from your log data.
- **Building Dashboards:** Aggregate multiple visualizations into dashboards for comprehensive analysis.
- **Analyzing Data:** Leverage visualizations to identify trends, anomalies, and patterns in your log data.

Benefits of ELK Stack Integration

- **Centralized Logging:** Aggregates logs from various sources into a single system.
- **Advanced Search Capabilities:** Enables powerful search and query functionalities.
- **Customizable Visualizations:** Provides tools to create dashboards tailored to specific analysis needs.