**HCL Interview Questions**

1. **Which Spring boot version supports Java 8?**

Spring Boot 2.x versions support Java 8. [If you need to use Java 8 for your project, you should choose a version from the Spring Boot 2.x series, as Spring Boot 3.x and later require Java 11 or higher](https://www.onexception.dev/news/1238158/spring-boot-with-java-8)

1. **What is transient and volatile keyword?**

A screenshot of a computer

Description automatically generated

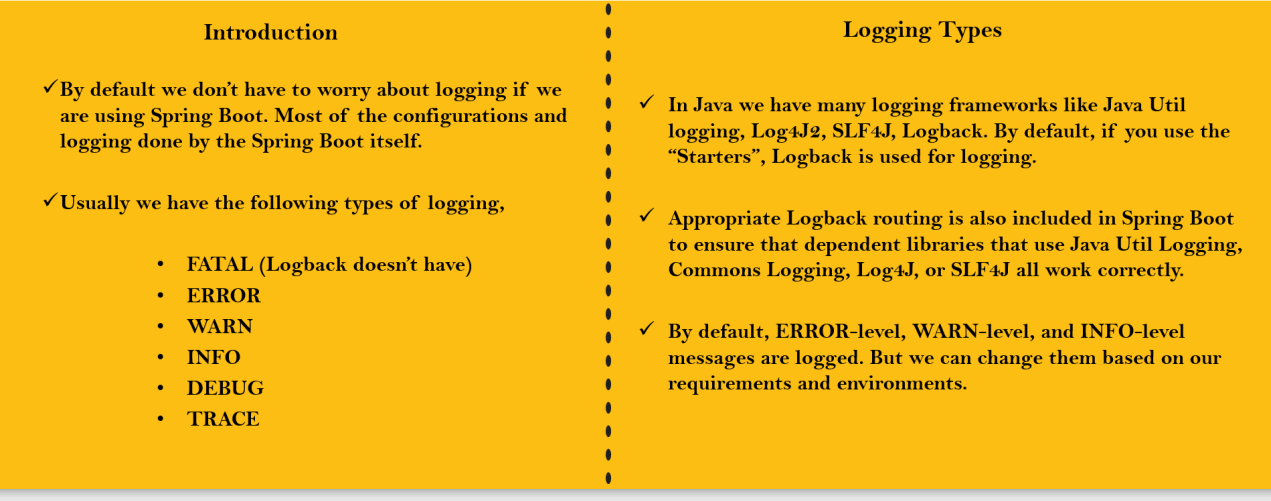
A screenshot of a computer program

Description automatically generated

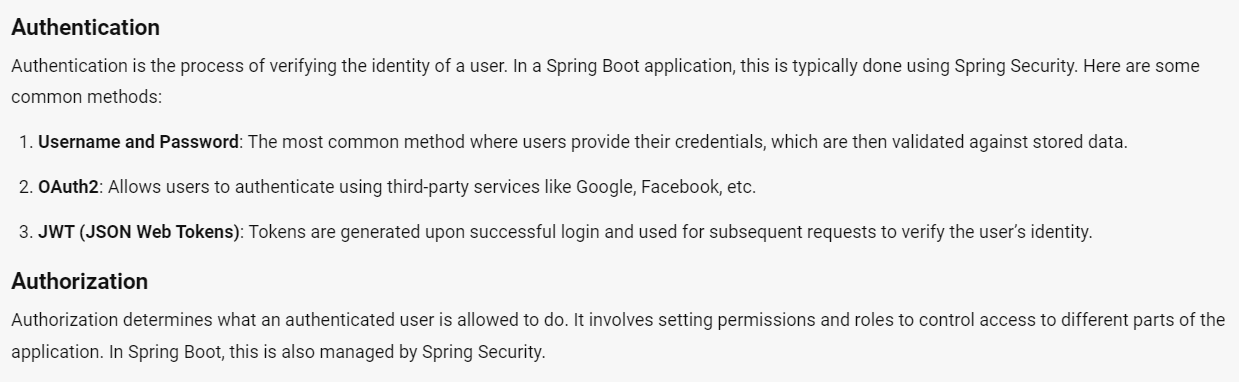
A close-up of a screen

Description automatically generated

1. **Springboot logging?**



1. **Authentication and Authorization**



1. **Find out a most repeating character in a string using streams?**

A screen shot of a computer code

Description automatically generated

1. JDK, JRE, JVM
2. Synchronized keyword
3. Git checkout command
4. How to change session timeout in spring security

We need add a property in application.properties file as below

server.servlet.session.timeout=20m(we can give only more than 120sec or 2m)

1. Merge two arrays and find duplicates

A screen shot of a computer program

Description automatically generated

Infosys:

1. **How to configure multiple databases in spring boot applications?**
2. **About Hikari?**

Hikari is Connection pooling vendor and it is the default implementation of spring boot applications.

We have c3po, DBCP2, tomcat, MySQL, oracle like we have multiple connection pooling vendors

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Internal working of hashing(SHA256)?**
2. **Can we use custom checked exceptions in our business logic?**

[not required] bcz our business logic throws an exceptions at runtime only right, if there are any checked expectations in business logic we can fix at compile time only, then why we need to create custom checked exception

1. **How do you provide estimates for a given task?**
2. **Dockerfile**
3. **How can a server communicate with the internet without allowing any inbound traffic from the outside in AWS?**

NAT gateway

1. **SAML vs OAUTH**

**SAML (Security Assertion Markup Language)**

* **Purpose**: Primarily used for authentication.
* **Use Case**: Commonly used in Single Sign-On (SSO) scenarios, especially in enterprise environments.
* **How It Works**: SAML allows users to log in once and gain access to multiple applications. It involves an identity provider (IdP) that authenticates the user and a service provider (SP) that provides the service.
* **Workflow**:
  1. User requests access to a service.
  2. The service provider redirects the user to the identity provider for authentication.
  3. The identity provider authenticates the user and sends a SAML assertion back to the service provider.
  4. The service provider grants access based on the assertion.
* **Example**: Logging into a corporate network and accessing various internal applications without re-entering credentials.

**OAuth (Open Authorization)**

* **Purpose**: Primarily used for authorization.
* **Use Case**: Commonly used to grant third-party applications limited access to user resources without exposing user credentials.
* **How It Works**: OAuth allows users to authorize third-party applications to access their resources on another service. It involves an authorization server and a resource server.
* **Workflow**:
  1. User initiates a request to access a resource.
  2. The application redirects the user to the authorization server.
  3. The user grants permission to the application.
  4. The authorization server issues an access token to the application.
  5. The application uses the access token to access the resource on the resource server.
* **Example**: Using your Google account to log into a third-party app like Hootsuite or SurveyMonkey.

**Key Differences**

* **Authentication vs. Authorization**: SAML is focused on authentication (verifying identity), while OAuth is focused on authorization (granting access to resources).
* **Tokens**: SAML uses XML-based tokens, while OAuth typically uses JSON Web Tokens (JWT).
* **Use Cases**: SAML is often used in enterprise SSO solutions, whereas OAuth is widely used for granting third-party applications access to user data.

**When to Use Each**

* **SAML**: Best for scenarios where you need to authenticate users across multiple applications within an organization.
* **OAuth**: Ideal for scenarios where you need to authorize third-party applications to access user data without sharing credentials.

1. **How you can make sure that your EC2 server is running**

In AWS ec2 dashboard, you can see if the status is **running**

By doing ping Test(ping ipaddr)

By doing SSH connection