Estrategia de Pruebas para el Microservicio de Autenticación y Autorización

Objetivos de las Pruebas

Asegurar que el microservicio de Autenticación y Autorización funcione correctamente y cumpla con los requisitos de login y registro.

Identificar y corregir defectos antes de la implementación en producción.

Validar la seguridad, usabilidad y rendimiento del microservicio.

Enfoque de Pruebas

Pruebas Unitarias: Utilizar JUnit y Mockito para probar las funciones individuales de login y registro, asegurando que cada método cumpla con su propósito.

Pruebas de Integración: Implementar pruebas de integración con Postman o Spring Test para verificar que los procesos de autenticación y autorización interactúen correctamente con otros microservicios y bases de datos.

Pruebas de Carga: Usar herramientas como Apache JMeter o Gatling para simular múltiples intentos de login y registros simultáneos, evaluando el rendimiento bajo alta demanda.

Pruebas de Seguridad: Realizar pruebas de penetración y análisis de seguridad utilizando OWASP ZAP para identificar vulnerabilidades en el proceso de autenticación.

Pruebas de Usabilidad: Realizar pruebas con usuarios reales para obtener feedback sobre la experiencia de uso en los procesos de login y registro.

Pruebas de Regresión: Ejecutar un conjunto de pruebas automatizadas que se ejecuten con cada nueva implementación para garantizar que las funcionalidades de autenticación no se vean afectadas.

Herramientas de Pruebas

Pruebas Unitarias:

JUnit: Para realizar pruebas unitarias en el código Java.

Mockito: Para crear simulaciones y verificar interacciones entre componentes.

Pruebas de Integración:

Postman: Para pruebas de API y validación de respuestas de login y registro.

Spring Test: Para pruebas de contexto de la aplicación y simulación de escenarios.

Pruebas de Carga:

Apache JMeter: Para simular carga en el sistema durante los procesos de autenticación.

Gatling: Alternativa para pruebas de carga con un enfoque en simulaciones de usuarios.

Pruebas de Seguridad:

OWASP ZAP: Para realizar pruebas de seguridad y detectar vulnerabilidades en el microservicio.

Pruebas de Usabilidad:

Sesiones de prueba con usuarios: Evaluaciones de la facilidad de uso del login y registro.

Cronograma de Pruebas

Fase de Planificación: 1 semana

Definición de requisitos de prueba y preparación del entorno.

Desarrollo de Pruebas Unitarias: 2 semanas

Implementación de pruebas unitarias para los métodos de login y registro.

Desarrollo de Pruebas de Integración: 1 semana

Implementación de pruebas de integración para verificar el flujo de datos.

Ejecución de Pruebas de Carga: 1 semana

Configuración y ejecución de pruebas de carga en escenarios de alta demanda.

Pruebas de Seguridad: 1 semana

Realización de pruebas de seguridad y análisis de resultados.

Pruebas de Usabilidad: 1 semana

Reuniones de feedback con usuarios y ajustes según sea necesario.

Pruebas de Regresión: Continuas

Ejecución de pruebas de regresión en cada nueva implementación.

Recursos Necesarios

Equipo de Pruebas: Personal con habilidades en pruebas de software, conocimiento de las herramientas mencionadas y capacidad para analizar resultados.

Infraestructura: Entornos de prueba que simulen el entorno de producción, acceso a herramientas de pruebas y dispositivos para pruebas de usabilidad.

Documentación: Detallar todos los casos de prueba, resultados y defectos encontrados para asegurar una buena trazabilidad.

Criterios de Éxito

Todos los casos de prueba críticos deben ser exitosos, con una tasa de fallos aceptable (por ejemplo, menos del 5%).

Identificación y resolución de todos los defectos críticos en los procesos de login y registro antes de la implementación en producción.

Retroalimentación positiva de los usuarios sobre la usabilidad del proceso de autenticación.

Métricas de Pruebas

Tasa de éxito de pruebas unitarias: Porcentaje de pruebas unitarias que pasaron.

Tasa de fallos de integración: Porcentaje de pruebas de integración que pasaron.

Tiempo de respuesta bajo carga: Medir el tiempo que tarda el sistema en responder durante los procesos de autenticación bajo alta carga.

Número de defectos encontrados: Contar los defectos encontrados en cada fase de pruebas.