Rapport de Projet : Intégration de Keycloak avec Spring Boot et Surveillance avec ELK

Résumé Exécutif

Ce projet a porté sur l'intégration de Keycloak pour la gestion de l'authentification et des autorisations au sein d'une application Spring Boot, ainsi que sur la mise en place d'un système de surveillance des logs avec la pile ELK. Les objectifs étaient de renforcer la sécurité de l'application, d'améliorer la gestion des utilisateurs et de fournir une visibilité claire sur les opérations de l'application via les logs. Les technologies utilisées ont apporté des solutions robustes et évolutives, répondant aux besoins modernes de sécurité et de surveillance des applications.

Introduction

Contexte du Projet

Dans le contexte actuel, où la sécurité des applications web est primordiale, l'entreprise a reconnu la nécessité de mettre en œuvre une solution d'authentification et de gestion des autorisations robuste et fiable. La nécessité d'une surveillance approfondie des opérations de l'application pour une maintenance proactive et réactive était également un point clé.

Objectifs

Les principaux objectifs étaient de:

- Intégrer Keycloak avec une application Spring Boot pour gérer l'authentification et l'autorisation.

- Mettre en place un système de logs centralisé avec ELK pour la surveillance et l'analyse des événements de l'application.
- Assurer une expérience utilisateur fluide et sécurisée.

Portée du Projet

Le projet couvre la conception, le développement et la mise en œuvre d'un système d'authentification avec Keycloak, la sécurisation des endpoints, et la configuration d'une pile ELK pour collecter et visualiser les logs. Il ne couvre pas la mise en œuvre de fonctionnalités au-delà de l'authentification et de la surveillance des logs.

Technologies Utilisées

Spring Boot

Spring Boot a été choisi pour le développement d'applications autonomes basées sur Spring, en minimisant la configuration requise.

Keycloak

Keycloak est utilisé comme serveur d'authentification et de gestion des identités, permettant la centralisation des processus d'authentification et des politiques d'accès.

ELK Stack (Elasticsearch, Logstash, Kibana)

Elasticsearch est un moteur de recherche et d'analyse distribué. Logstash est utilisé pour le traitement des logs, et Kibana est une interface utilisateur qui permet la visualisation des données Elasticsearch.

Configuration de l'Environnement de Développement

Paramètres du Serveur

Les paramètres du serveur ont été configurés pour supporter les applications de haute disponibilité, avec des considérations pour la charge et la performance.

Configuration des Outils de Développement

Des environnements de développement locaux ont été configurés, y compris des IDE, des outils de gestion de versions et des outils de CI/CD.

Configuration de l'Environnement Keycloak

Keycloak a été déployé et configuré pour travailler avec l'application Spring Boot, avec des rôles et des politiques d'accès définis pour les utilisateurs.

Configuration de la Pile ELK

La pile ELK a été configurée pour recueillir les logs de l'application, les indexer dans Elasticsearch et les visualiser via Kibana.

Développement de l'Application

Authentification et Autorisation avec Keycloak

Le flux d'authentification a été mis en place pour permettre aux utilisateurs de s'authentifier via Keycloak et d'accéder à l'application en fonction de leurs rôles.

Gestion des Rôles et des Permissions

Les rôles ont été créés et gérés dans Keycloak, permettant des permissions granulaires au niveau des endpoints API.

Sécurité de l'API

Les API ont été sécurisées en utilisant des jetons JWT pour s'assurer que seuls les utilisateurs authentifiés avec les bons rôles puissent accéder aux ressources.

Intégration avec le Frontend

Une interface utilisateur réactive a été développée pour interagir avec l'API backend de manière sécurisée.

Interactions Utilisateur

Les interactions des utilisateurs avec l'application ont été conçues pour être intuitives, avec des réponses immédiates aux actions d'authentification.

Surveillance avec ELK

Configuration d'Elasticsearch

Elasticsearch a été configuré pour stocker et indexer efficacement les logs générés par l'application et Keycloak.

Intégration de Logstash

Logstash a été utilisé pour traiter et acheminer les logs vers Elasticsearch depuis différentes sources.

Visualisation avec Kibana

Des dashboards personnalisés ont été créés dans Kibana pour permettre une surveillance en temps réel et une analyse approfondie des événements de l'application.

Tests et Validation

Stratégies de Tests

Des stratégies de tests comprenant des tests unitaires, d'intégration et de performance ont été mises en œuvre.

Cas de Tests

Des scénarios de tests ont été définis pour couvrir les fonctionnalités et les flux de données de logs.

Résultats des Tests

Les résultats ont montré une forte adhérence aux exigences et une performance élevée des fonctionnalités testées.

Conclusion

Le projet a réussi à mettre en œuvre une authentification robuste avec Keycloak et à établir une surveillance efficace avec ELK.

L'application bénéficie maintenant d'une meilleure sécurité, d'une meilleure gestion des utilisateurs, et d'une visibilité complète sur les opérations grâce aux logs.