УДК 004.41
Дегодюк І. – ст. гр. СП-31, Бармак Р. – ст. гр. СП-41
Тернопільський національний технічний університет імені Івана Пулюя

ІНТЕГРАЦІЯ ДЕТАЛІЗОВАНИХ ДОЗВОЛІВ KEYCLOAK У ПРОЦЕС АВТОРИЗАЦІЇ КОРИСТУВАЧІВ СИСТЕМИ

Науковий керівник: PhD Бревус В. М.

Dehodiuk I., Barmak R.
Ternopil Ivan Puluj National Technical University

INTEGRATION OF KEYCLOAK FINE-GRAINED PERMISSIONS INTO USER AUTHENTICATION FLOW

Supervisor: PhD Brevus V. M.
Ключові слова: Аутентифікація Користувачів, Деталізовані Дозволи, Keycloak.
Keywords: User Authentication, Fine-Grained Permissions, Keycloak.

Вступ. Процес аутентифікації користувачів у системі відповідає за розподіл дозволів для конкретного користувача. На поточний момент, у цього процесу немає стандарту, що забезпечуватиме гнучкість та безпеку системи. Це призводить до зловживання користувачів власними правами, навіть, у додатках світового значення.

Мета роботи — дослідження підходів для інтеграції деталізованих дозволів Keycloak у мікросервісну систему. Ознайомлення із доступними програмними інтерфейсами та пошук оптимального рівня делегації логіки процесу аутентифікації.

Основна частина. Починаючи з версії 26.2.0, Keycloak дозволяє налаштовувати деталізовані дозволи для клієнтських застосунків. Дозвіл складається із декількох незалежних компонентів [1]:

1. Ресурс: об’єкт системи, доступ до якого повинен бути обмеженим. Keycloak не обмежує формат ресусу, тому він може бути представлений будь-яким чином. Опційно, ресурс може оголошувати сфери застосування, для більш детального контролю дозволу.

2. Політика: визначає умову необхідну для отримання доступу. Умова може перевіряти певну властивість користувача, наявність атрибутів. Додатково, умови можуть бути тимчасовими.

3. Дозвіл: сутність об’єднує одну, або більше, політику із ресурсом та його сферами застосування. Keycloak реалізовує програмний інтерфейс із трьома режимами роботи, який дозволяє регулювати рівень делегації логіки [2]. Режим визначається за допомогою параметру response_mode, що приймає 3 значення: 1. Decision: повна делегація авторизації, Keycloak самостійно приймає рішення щодо доступу користувача. 2. Permissions: Keycloak поверне список дозволених дій для поточного користувача. Програма повинна обробити їх та прийняти рішення самостійно. 3. Параметр відсутній: Keycloak поверне RPT токен, що містить дозволи та додаткові дані про користувача. Підхід забезпечує найнижчий рівень делегації. Токен може обмінюватись між різними мікросервісами.

Повноцінна система вимагає великої кількості дозволів та чіткої стратегії для їхньої організації [3]. Деталізовані дозволи Keycloak можуть бути налаштовані за допомогою Terraform провайдеру, що спрощує процес управління та забезпечує версійність.

На рисунку 1 представлена високорівнева структура системи після інтеграції деталізованих дозволів Keycloak за допомогою описаних підходів. Залежно від рівня делегації, роль виконавця політик (PEP) може виконувати, або API Gateway, або сервіс що опрацьовує запит.

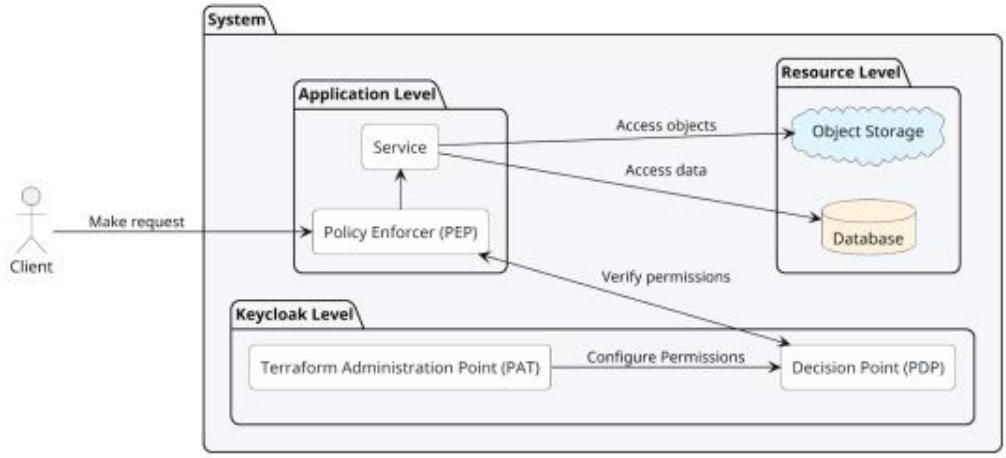

Рисунок 1 — Структурна діаграма системи

Результати. Досліджені підходи для інтеграції деталізованих дозволів Keycloak із інтеграцією Terraform провайдеру дозволяють:

- Централізувати та стандартизувати процес авторизації користувачів.
- Налаштовувати рівні доступу користувачів без змін у програмному коді.
- Відслідковувати історію змін конфігурації.
- Відновити створену конфігурацію у випадку критичних збоїв системи.

Висновки. Досліджені підходи інтеграції деталізованих дозволів Keycloak забезпечують низку переваг та значно спрощують процес авторизації користувачів системи. Можливість регулювання рівня делегації робить процес гнучким та уможливлює його застосування у різноманітних системах. Використання Terraform забезпечує версійність та відновлюваність конфігурації, підвищуючи надійність усього потоку авторизації.

Список джерел.

[1] K. M and N. Kumaresh, "Implementation of Dynamic Role Based Access Control in Multi-Tenant Cloud". Accessed: Mar. 23, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11234495

[2] Gamayanto, Indra, Michael Christ Kurniawan, and Gabriello Klavin Sanyoto. "Security Evaluation of Keycloak-Based Role-Based Access Control in Microservice Architectures Using the OWASP ASVS Framework". Accessed: Mar. 23, 2026. [Online]. Available: https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/11604

[3] V. Voicu, D. Petreuş, E. Cebuc and S. B. Marcu, "University Identity and Access Management Infrastructure with Keycloak: Lessons Learned". Accessed: Mar. 23, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10722517/metrics#metrics