



Introduction

This cooperative internship at T.C.C. Technology Co., Ltd. (TCCtech) focused on developing an Authentication and Authorization System to enhance security in user management. The project utilized Keycloak for identity management and integrated it using two approaches: a Go Fiber adaptor for seamless API authentication and a RESTful API for secure system communication. With Redis for efficient data handling, the system successfully improved access control and interoperability across company applications.

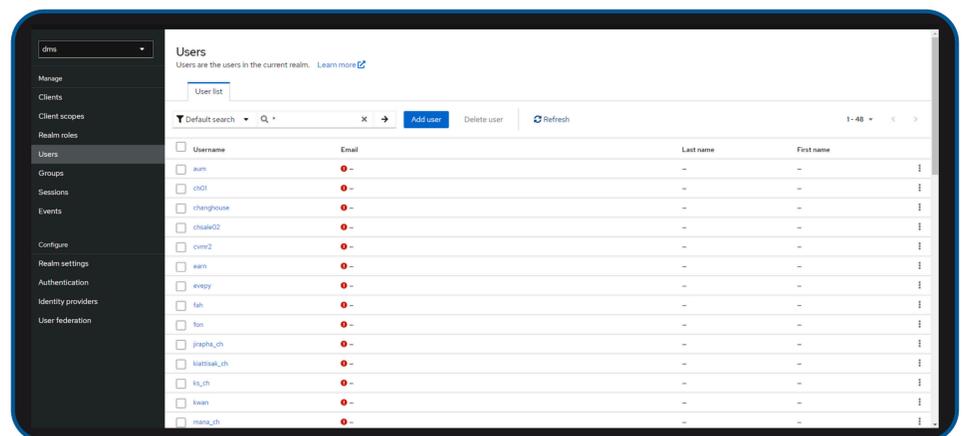
Abstract

The cooperative internship at T.C.C. Technology Co., Ltd. (TCCtech) involved a project developing an Authentication and Authorization system. The objective was to enhance the security of user management and access control across various systems used by the company. The developed system utilized Keycloak as the primary tool for managing user permissions, with two main development approaches for system integration. The first approach involved the development of a Go Fiber adaptor to connect Keycloak with the API system. This was implemented using the Go programming language, along with tools such as Postman, Redis, and MySQL to efficiently test and manage necessary data. The second approach was related to designing an API using Keycloak and Go Fiber to provide RESTful services. This approach ensured compatibility with other systems via HTTP connections and utilized Redis for quick data access and management. The development of both approaches was successfully completed according to the plan, and the system functions effectively in its intended environment.

Technology



Result



Keycloak User Manage Interface

Methodology



System Analysis and Design



Installing and Configuring Keycloak



Developing the Go Fiber Adaptor



System Testing



Deploying to Production

Conclusion

The development of the Authentication & Authorization Service using Keycloak as the core identity and role management tool enhances security and ensures scalability. The system architecture has been designed to support future expansion by integrating with external services via APIs and utilizing MySQL as the primary database. The system can generate authentication tokens and supports integration with Line Login. All developed functions have been thoroughly tested according to predefined test cases, ensuring that the system operates as planned.

Reference

Red Hat, Inc. (n.d.). Keycloak Documentation. Retrieved from <https://www.keycloak.org/documentation>
The Go Programming Language. (n.d.). Go Documentation. Retrieved from <https://go.dev/doc/>