Tech Modernisation for Internal Application with Containerisation, OIDC, Zero Trust, and RBAC

Ranveer Chaudhary (2110993886)

Problem Statement:

One of my firm's application runs on traditional server infrastructure and relies on Kerberos for authentication. This setup lacks flexibility, fine-grained access control, and modern security measures. The system is not easily scalable or portable and does not align with current best practices in cloud-native development or cybersecurity. The scope of my internship is to transition to containerisation, a modern authentication system using OIDC and OAuth 2.0, and the adoption of Zero Trust security principles along with RBAC to enforce least-privilege access.

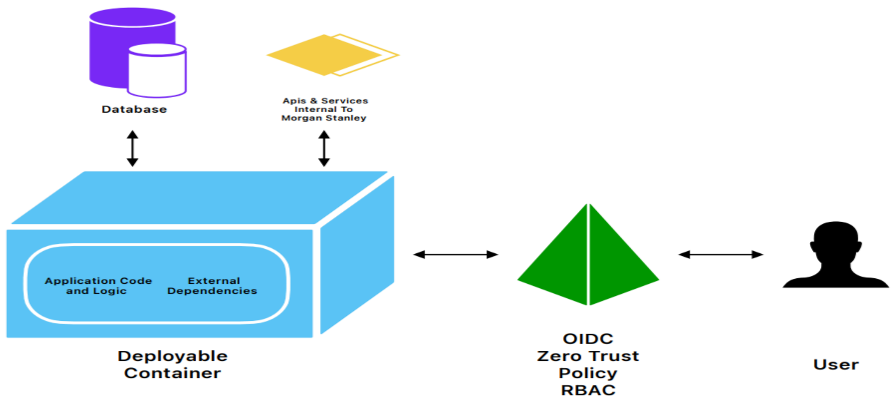
Introduction:

This project focuses on modernising an internal application by moving away from legacy server-bound architecture and outdated authentication mechanisms. The goal is to containerized the application, replace Kerberos with OpenID Connect (OIDC) and OAuth 2.0, and implement a Zero Trust security model. Role-Based Access Control (RBAC) will also be introduced to ensure only authorised users can access specific resources based on their roles. This transformation will enhance security, scalability, portability, and compliance with modern enterprise standards.

Technology:

- Backend: Python and Java-based Spring boot services
- Build System: Gradle a modern Java build tool
- Database: SQL-based relational database
- Docker Like service

Flowchart


Database
Apis & Services Internal To Morgan Stanley
Application Code and Logic
External Dependencies
Deployable Container
OIDC Zero Trust Policy RBAC
User

References

- [OpenID Connect Core Specification]
- [OAuth 2.0 Authorization Framework – RFC 6749]
- [What is Containerization? – Red Hat]