OSS를 이용한
ZTNA 인증 서비스 개발

Contents

프레젠테이션 목차 안내

Contents 01

개발 동기 및 목표

Contents 02

구성 환경

Contents 03

서비스 기능

Contents 04

기대 효과 및 일정

Project target

프로젝트 수행 동기

권한 관리 취약점의 대두

SK쉴더스 보안관리 보고서에 따르면, 국내 대기업 권한과 관련된 보안 취약점이 증가하고 있는 추세이다. 권한, 즉 인증 인가와 관련된 중요성이 증가하고 있다.

Problem

미인증 사용자의 접근에 따른 취약점 발생

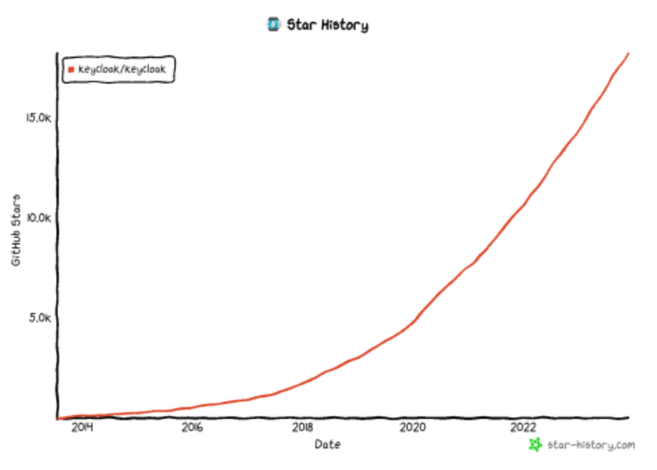
OWASP TOP10에 따르면, Access Broken과 같이 사용자의 접근 제어가 제대로 이루어지지 않아 발생하는 취약점이 많음을 언급함.

Solution

인증 인가가 필요한 여러 IT 비즈니스 업체에서 쉽게 발생할 수 있는 인증 인가 관련된 취약점을 보완할 수 있는 솔루션 개발 진행한다. 또한, 해당 솔루션을 통하여 권한과 관련된 보안 문제를 해결하고자 한다.

Project target

프로젝트 수행 목적



Total Star

21,206

인증에 대한 중앙 통제가 가능한 인증 인가 전담 오픈소스 Keycloak 선택

Ranking

585

사용자가 원하는 모듈을 쉽게 커스텀 할 수 있다는 장점으로 다양한 인증 인가 모듈 제공 가능

Project target

ZTNA와 Keycloak과의 연계를 통해 인증 인가를 전담할 수 있는 고도화된 솔루션을 제공하며 동시에 해당 솔루션을 이용해 접근 통제 및 User 검증 모듈을 손쉽게 사용할 수 있도록 한다.

Development

프로젝트 개발 솔루션

Solution 01 인증 인가 모듈 허가된 사용자만 서비스를 이용할 수 있도록 인증 및 인가 모듈 개발

Solution 02 USER 관리 기능 허가된 사용자를 분류할 수 있는 USER 관리 솔루션 개발

Solution 03 자동 인프라 구축 손쉽게 KEYCLOAK 인프라를 구축할 수 있도록 자동화 솔루션 개발

Infra

서비스 구성 환경 개요

Docker & K8S

KeyCloak

기존의 KeyCloak의 경우 helm chart를 이용해 쿠버네티스 환경을 만들 수 있도록 클라우드 환경의 서비스 지원

Container Service

실제로 현재 컨테이너 기술은 전체 IT 회사의 96%가 사용하고 있는 만큼 클라우드 및 컨테이너 환경의 서비스 구축

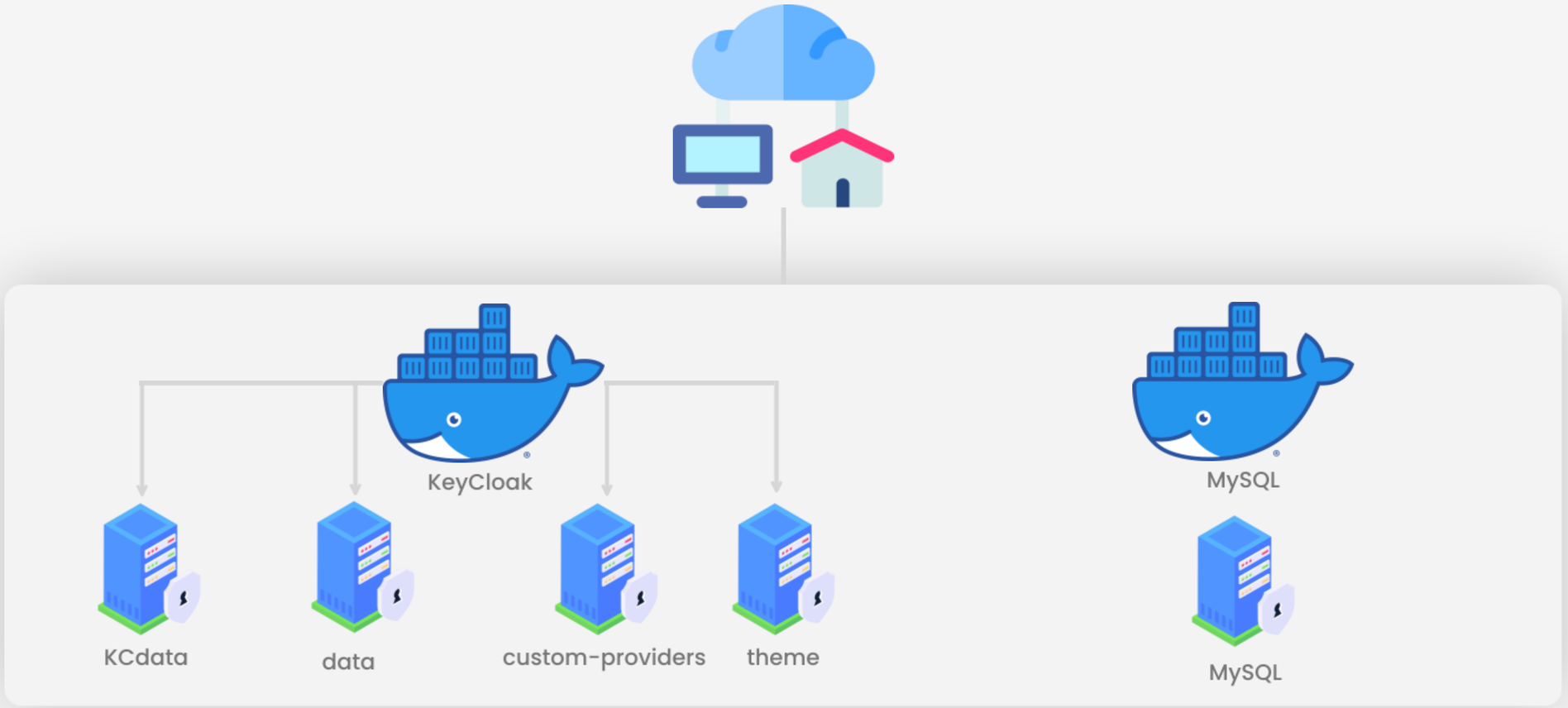
Effect

컨테이너 기술을 활용하는 다양한 회사 측에서 손쉽게 인증 인가 관리를 할 수 있도록 한다

Infra: docker

서비스 구성 환경 : docker

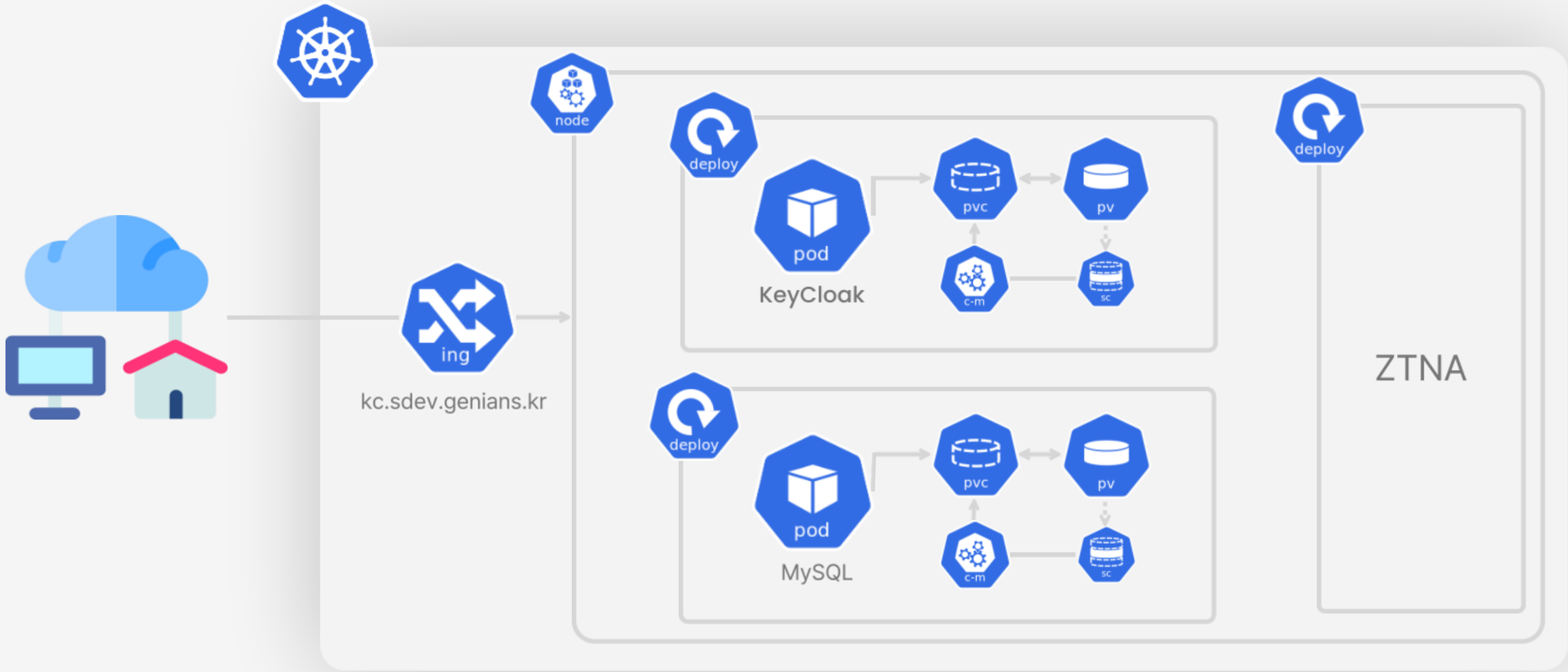
- Cloud Service : AWS
- Docker Version : 24.0.5 community Version
- OS : Ubuntu 20.04.6 LTS



Infra: kubernetes

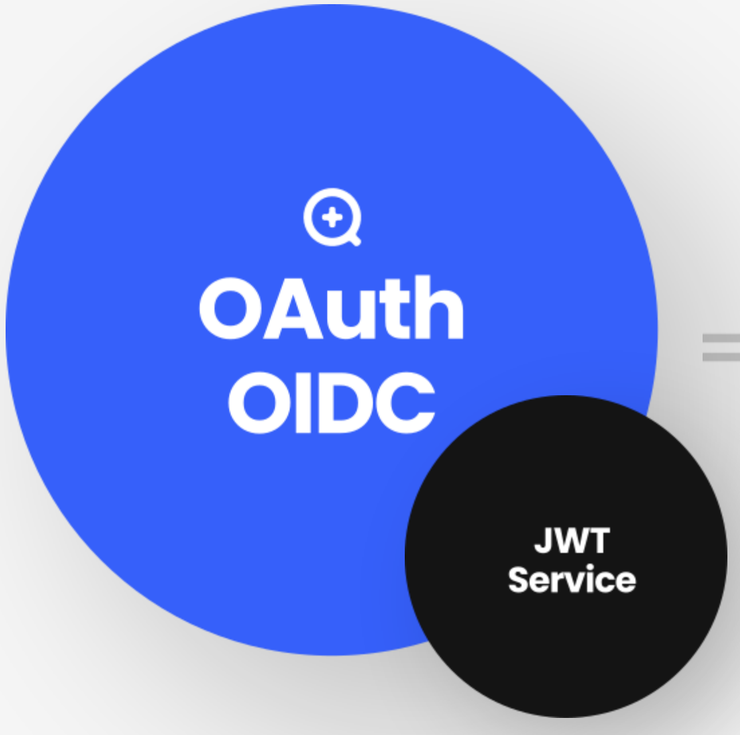
- Cloud Service : AWS EKS
- Docker Version : 24.0.5 community Version
- OS : Ubuntu 20.04.6 LTS

서비스 구성 환경 : kubernetes



OAuth & OIDC

KeyCloak을 이용한 외부 인증 연동 통합 관리



Problem	서비스 제공 측에서 부적절한 방법으로 데이터를 저장할 경우 보안성 측면에서 위험 존재
Solution	OAuth & OIDC 솔루션을 활용하여 구글 및 카카오 로그인을 통해 인증된 사용자만 서비스를 사용할 수 있도록 솔루션 개발
Effect	서비스 제공 자사 측에서 해킹을 당하더라도 USER와 관련된 정보의 탈취 위험을 줄일 수 있다.

Custum Plugin

User Federation : MySQL DB 연동

DB Federation

외부 DB 연동이 가능하도록 연동을 할 수 있는 기능 개발
이후 MySQL 외에도 다른 플러그인까지 이용할 수 있도록
확장 예정

Custum User Management

ID, EMAIL로 USER를 찾을 수 있도록
USER 관련된 기능 구현
USER 및 EMAIL 검증 기능 구현

Custum Plugin

Event Listener

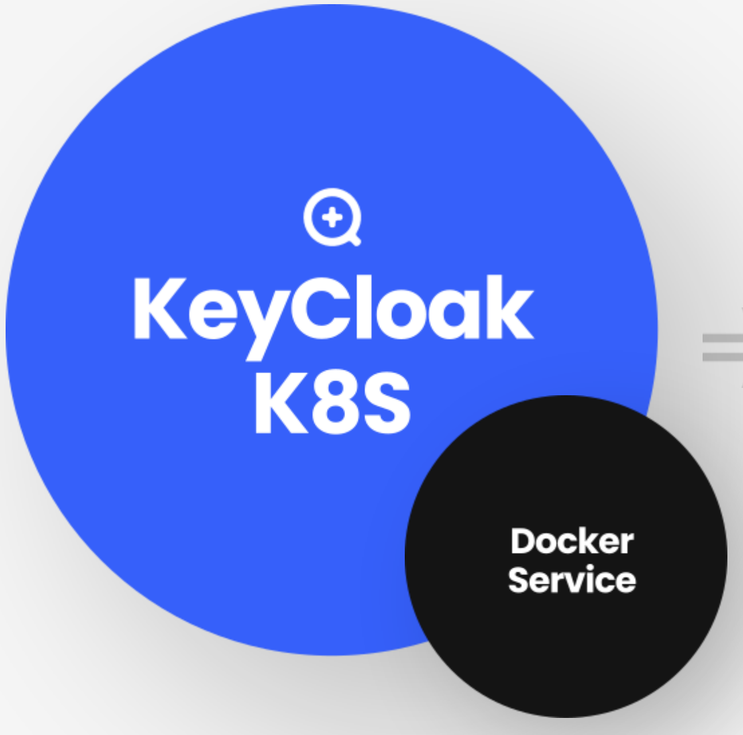
로그인 시 IP 및 타임스탬프를 추출하는 기능 구현
비정상 로그 탐지로 추후 연결 가능

Custum theme

사용자가 원하는 방식의 다양한 테마를 사용할 수 있도록
theme 기능 구현

Infra Automation

KeyCloak 설정 및 구성 자동화 솔루션 개발



Problem

기존 KeyCloak 서비스 사용의 어려움 존재
Helm Chart 등 사용에서 인증서와 같이 누락된 부분의 존재

Solution

K8S 및 Docker 환경에서 KeyCloak을 자유롭게 사용할 수 있도록 인프라 자동화 솔루션 개발

Effect

다양한 추가 모듈 개발 시 손쉬운 적용 가능 및 여러 서비스와 KeyCloak의 결합으로 인증 인가 보안성 보장 가능

Project Results

프로젝트 기대 효과

인증 절차에 대한 보안성 향상

Keycloak 어플리케이션의 사용으로
JWT, 공개키 교환 및 인증 인가 등 각각의 절차의
도입으로 여러 어플리케이션의 보안성을 향상한다.

식별 가능한 개별 **application** 권한 부여

여러 Application이 연동될 때 각각의
User별 권한을 부여하여 효율적인 인증 및 인가
관리가 가능하게 된다.

Key Keywords

기존 모듈과의 연동 프로세스 일원화

여러 서비스를 사용하는 다양한 상황에서도
인증 인가 서비스를 쉽게 사용할 수 있도록
프로세스 일원화 진행

향후 추가 연동 및 기능 개발 시 확장성 용이

ELK를 통한 각종 로그분석으로 인증 인가 관련 기능 확장
MSA 아키텍쳐 분리로 여러 기능을 추가하게 되더라도
확장이 용이하게 된다.

Solution

솔루션 판매 대상 및 차별화

	Community	Pro	Enterprise
사용 대상	인증 인가 서비스 사용자	인증 인가 서비스 사용자	Keycloak으로 인증 인가를 하고자 하는 기업
인프라 기능	Docker 인프라 자동화 서비스	Docker 인프라 자동화 서비스 Kubernetes 인프라 자동화 서비스	Docker 인프라 자동화 서비스 Kubernetes 인프라 자동화 서비스
KEYCLOAK 기능	KeyCloak 기본 서비스 기능	KeyCloak 기본 서비스 기능 KeyCloak Custom 확장 기능	KeyCloak 기본 서비스 기능 KeyCloak Custom 확장 기능 KeyCloak 모니터링 기능(예정)

schedule

프로젝트 추진 일정

구분	내용	7-10	7-17	7-24	7-31	8-7	8-14	8-21	8-28	9-4	9-11	9-18	9-25	10-2	10-9	10-16	10-23	10-30	11-6	11-13	11-20	11-27	12-4
(1) ZTNA 교육	ZTNA 기본 교육																						
(2) 개발환경 & K8S	개발에 필요한 배경지식 점검																						
(3) 네트워크 보안 OSS	Online Meetup																						
(4) ZTNA & SWG	상세 구조의 이해																						
(5) 프로젝트 Setup	개발 방향 & 기획안 도출																						
(1) DevOps의 이해																							
(2) GitHub Action, AWS Cloud, Terraform																							
(3) Github Actions + Terraform + AWS																							
(4) Kubernetes 에서 Wordpress 구동하기																							
(5) K8s helloworld 서비스 생성																							
KeyCloak 적용 실습	docker 내 keycloak 설치 및 기본 테스트																						
	keycloak 이벤트 리스너 생성 및 전달																						
	keycloak jwt 토큰 생성 및 응답 수신																						
	keycloak user federation 예제 작성 및 테스트																						
Keycloak 개별 업무분장	User Federation DB 설정																						
	User Federation Custum DB Plugin 제작																						
	KeyCloak Custum Event Listener 제작																						
	외부 인증 연동 통합 관리																						
	외부 인증 연동 통합 테스트																						
	Application 접속 권한 부여																						
	NginX와 연동한 Application 접속 권한 테스트																						
	K8S 환경 구축 및 ZTNA 모듈 연동																						
	KeyCloak Custum 테마 제작																						
	KeyCloak Test용 User Form UI 제작																						

Thank you.