

Kakao

Fossid 적용

후기

이민정 yally.next

Kakao

오픈소스기술파트

Fossil Overview

Fossid

Fossid

- **2016**년 설립
- 오픈소스 식별 솔루션 전문 기업
- 스웨덴, 루마니아, 핀란드, 대만 및 일본에 지사
- **2020**년 **2**월 **OSBC**에서 한국 총판 계약. (이전 **PROTEX** 총판 업체)

Snyk

- **Security** 전문 업체
- **2020.4**월 오픈소스 라이선스 컴플라이언스 기능까지 추가한 일반 사용자 서비스 제공.
- **Snyk**에서 **2021.05**년 **FOSSID** 인수.



방대한 데이터 수집

AI/머신러닝 기반 소스코드 수집 기술을 통해, 전 세계 오픈소스 저장소로부터 약 2,048Terabytes 이상의 데이터 수집합니다.



AI를 통한 효율성 향상

FOSSID만의 자체 인공지능을 활용해 오탐결과를 자동 제거하고, 수동 리소스를 최소화해 분석작업에 필요한 시간과 비용을 절약할 수 있습니다.



사용자 중심의 손쉬운 작업

FOSSID는 웹 어플리케이션 및 CLI를 통해 코드의 스캔 및 식별이 가능합니다. 사용자는 소스코드를 손쉽게 스캔, 검증할 수 있으며 이밖에 다양한 리포트 생성이 가능합니다.



빠르고 정확한 검색엔진

FOSSID만의 혁신적인 검색엔진으로 초당 약 70개 이상의 파일 분석이 가능합니다.



프로그램 연동/통합의 용이성

FOSSID는 경량 클라이언트 프로그램을 제공해 기업의 개발 프로세스 어디에든 부담없이 연동 및 설치가 가능합니다.

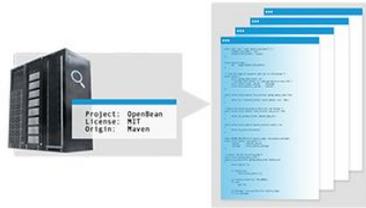


소스코드의 완벽 보안

FOSSID는 자체 보유한 보안기술을 통해, 소스코드 내 디지털 시그니처 만을 추출해 오픈소스를 탐지합니다.

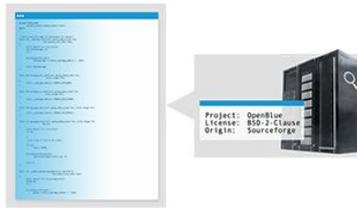
FOSSID는 모든 형태의 오픈소스를 식별합니다.

Entire Components



FOSSID는 폴더, 라이브러리, 아카이브, 바이너리 등 파일 형식에 관계 없이 모든 컴포넌트를 빠르게 스캔해 분석 시간을 줄이고 정확성을 높여줍니다.

Full Files



FOSSID의 혁신적인 검색 알고리즘은 변경/편집된 파일도 손쉽게 찾아내 분석이 가능합니다.

Code Snippets



FOSSID는 웹에서 붙여넣기한 소스코드 검증도 가능합니다. 스니펫 코드의 식별 및 분석은 오픈소스 검증 효율성을 크게 높여줄 수 있습니다.

FOSSID는 사용자 중심의 유연한 활용 환경을 제공합니다.

- 2가지 방식의 실행환경 -



FOSSID CLI

FOSSID CLI는 대부분의 운영체제(Windows, Linux 등)에서 실행 가능합니다. 또한 기업의 개발 프로세스 및 Tool chain과 연동이 용이해, 반복적 또는 대량 작업의 자동화를 가능하게 만들어줍니다.



FOSSID Webapp

FOSSID 웹 응용프로그램은 사용자가 검증을 포함한 오픈소스 컴플라이언스 및 보안활동을 손쉽게 수행할 수 있는 직관적인 UI를 제공합니다.

FOSSID는 클라우드 서비스와 온프레미스 서비스를 각각 제공합니다.
기업은 FOSSID 온프레미스 버전을 통해, 자체 네트워크 내에 FOSSID 솔루션을 배치할 수 있습니다.



정기 업데이트 버전

FOSSID 도구를 로컬상에 설치한 뒤,
클라우드 기반 기술자료를 이용해 오픈소스 검증을 수행합니다.
스캔 시, 소스코드가 FOSSID의 클라우드로 전송되지 않으므로
최대한의 프라이버시를 보장합니다.

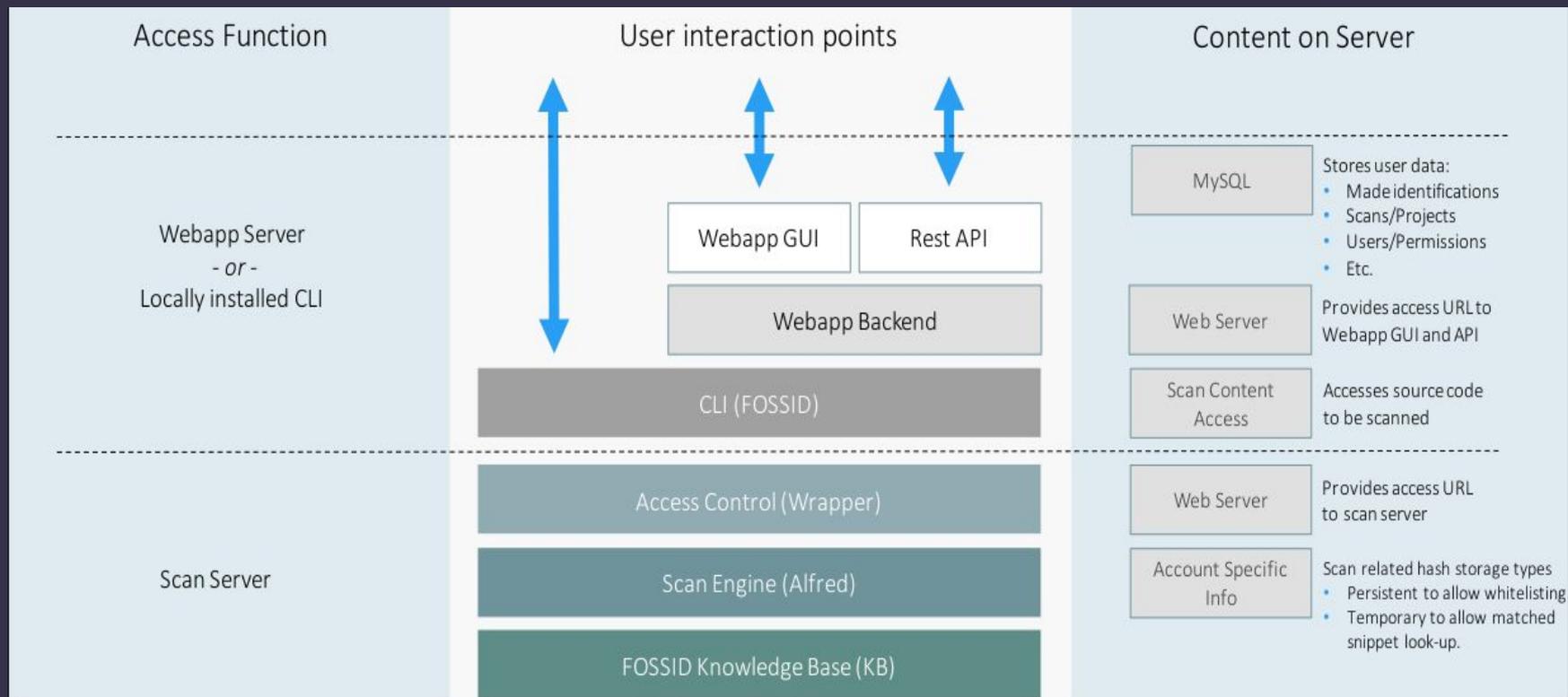


오프라인 설치 버전

오프라인 설치 버전의 경우, FOSSID 데이터 사본을 기업 네트워크에
설치합니다. 이에 따라, 오픈소스 검증을 수행하는 데 있어, 어떠한
외부 종속성이나 기업 네트워크를 제외한 외부 네트워크 트래픽이
포함되지 않습니다.

Fossil System

Fossid System : Architecture



Fossid System : Webapp Server

OS

- **CentOS-7 and 8**
- **RedHat Enterprise Linux 7 and 8**
- **RedHat Enterprise Linux Server 7**
- **Debian 9 and 10 (Stretch/Buster)**
- **Ubuntu 18.04, Ubuntu 20.04**

Application

- **PHP 7.3 or late**
- **NginX (default 7.3)**
- **MySQL Server 5.7 or late / MariaDB 5.5 or late**
 - **Remote 지원**

Fossid System : Webapp GUI

FOSSID part of snyk

Projects Scans Components Licenses Tools Users System Utils Help

 **Documentation**

Search documentation

 **Getting Started**
Get started with FossID

 **Web Application**
Get Help with FossID Web Application

 **Command Line Interface**
Get Help with FossID Command line interface

 **Blind Audit**
Get Help with FossID Blind Audits

 **Vulnerabilities**
Get Help with vulnerabilities

 **Dependency Analysis**
Learn about analyzing dependencies

 **WebApp API**
Get help with FossID Webapp restful API

Tip of the day
Scans can be configured to only look for full file matches or to also look for code snippet matches
[Next tip](#)

Start Scanning
Get started with a FossID scan
[New Scan](#)

Create Project
Create a project and start adding scans to it
[Create Project](#)

Snippet Search
Copy-paste a snippet into a text box and run an instantaneous scan
[Snippet Search](#)

Latest projects

rogers-test_864	rogers-test	2022-04-25 17:29:04						
olive_729	khaili	2022-04-21 12:38:24						
olive_805	graphql-kotlin	2022-04-14 11:42:49						
raintest_861	raintest	2022-04-14 16:49:34						
yallytest_858	yallytest	2022-04-13 14:12:56						

[Go to projects](#) [Create new project](#)

Latest scans

olive_12_1njAoTgeBH	olive_1njAoTgeBH	2022-04-26 11:20:26			
olive_12_1njAoJGzRv	olive_1njAoJGzRv	2022-04-26 11:20:15			
olive_12_1nj9B2uXUz	olive_1nj9B2uXUz	2022-04-26 09:35:37			
olive_12_1nj9B1d3Dy	olive_1nj9B1d3Dy	2022-04-26 09:35:36			
olive_12_1nj9AKLQf2	olive_1nj9AKLQf2	2022-04-26 09:34:52			

[Go to scans](#) [Create new scan](#)

Previous 2 3 4 5 ... 181 Next

Fossid System : Webapp Rest API

- requires a FossID WebApp user account and an API key

```
{
  "group": "projects",
  "action": "create",
  "data": {
    "username": "username",
    "key": "user_key",
    "project_code": "My project code",
    "project_name": "My first project",
    "limit_date": "2017-12-31",
    "product_code": "My product code",
    "product_name": "My first product",
    "description": "This is my first project created from REST API",
    "comment": "No comments",
    "jira_project_key": "My JIRA Project Key"
  }
}
```

Fossid System : System Utils

Manage backups

Create DB backup

Create files backup

Refresh list

Available backups

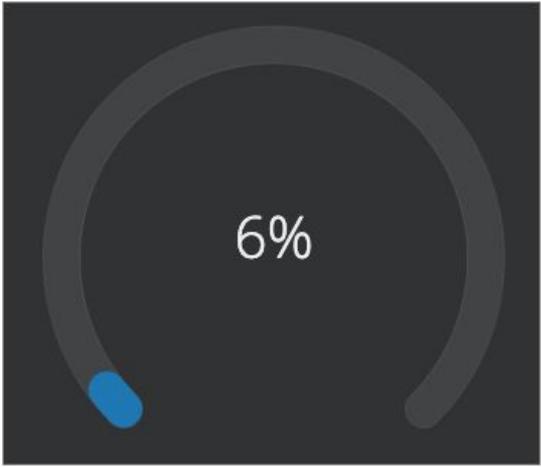
Show entries Search:

Name	Restore	Delete
2022_03_16.sql		
2022_03_16.tar.gz		
db.2022.01.25.sql		
file.2022.01.25.tar.gz		

Showing 1 to 4 of 4 entries Previous Next

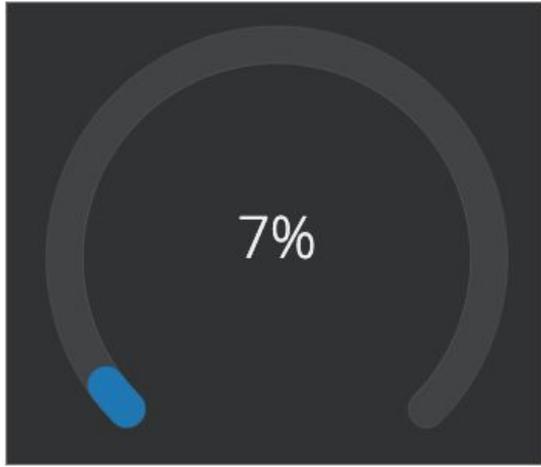
System Monitoring

Disc Information



6%

Memory Information



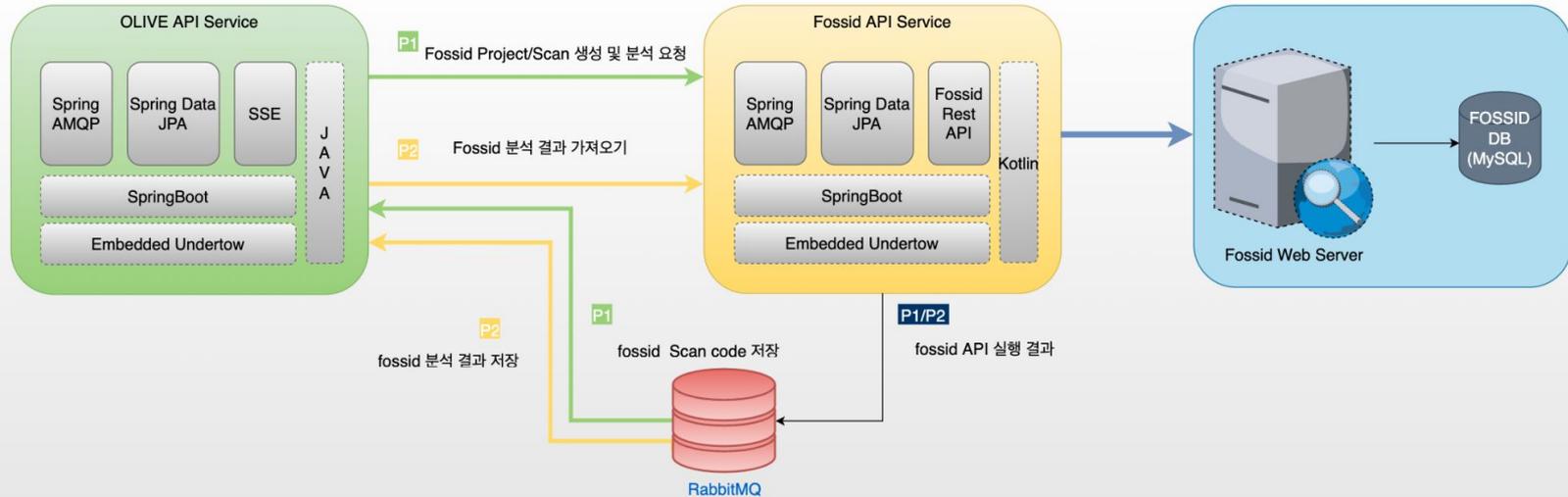
7%

Kakao 적용

Kakao : BMT

	Protex	Fossid
업데이트	자동. 웹 클릭 or 스케줄 지정 업데이트가 무겁고 느림. 업데이트 후 장애 발생	수동. 파일을 다운 받아서 서버에서 실행 Knowledgebase 가 제외되어 가볍고 빠름
연동	SOAP API. Java 6 기반 코드 SDK 업데이트가 거의 이루어 지지 않음	Rest API. 실제 WAS 에서 동작 테스트 가능
기술지원	최소한의 유지보수. 안정적인 배포버전	활발한 개발 및 릴리즈
서버	Knowledgebase 로 인해 고사양 스펙 요구	일반 시스템 서버
Scan	3 개의 스캔 동시 수행. 서버 다운.	3 개의 스캔 동시 수행. 1 시간 소요
Component	컴포넌트 목록 제공	전체 컴포넌트 목록 제공하지 않음
License	총돌 및 의무사항에 대한 정보 제공	총돌 및 의무사항에 대한 정보 제공하지 않음
비밀관리	개발팀에 의해 관리	운영팀에 의해 관리

Kakao : system



- **Ubuntu 20.04.3**
- **Mysql 8.0.19**
- **Php 8.0.13**
- **Nginx 1.18.0**

Kakao : migration

- 사용중인 서비스의 가장 마지막 검증만 마이그레이션
- 310개의 project
- 1st Scan : 6시간
 - Spdx import
 - 관련 api가 있지만 동작하지 않음
 - 별도 스크립트 + api로 처리
- 2nd Scan : 13시간
 - 해당 검증 시점의 소스코드를 업로드
 - 1st Scan의 검증내역을 반영하여 소스코드 분석
 - api을 이용하여 일괄 스캔하는 운영메뉴 추가 개발
- 1st VS 2nd
 - diff을 확인할수 있는 내부 운영메뉴 추가 개발
 - 301개 프로젝트에 대하여 diff 체크
 - 52개 프로젝트에서 발생.
 - 프로젝트당 1~2개의 누락 발생
 - 동일파일에 1개 이상의 컴포넌트가 체크된 케이스

Kakao : customizing

- **SPDX import** 일부 실패
 - **Protext spdx** 포맷 중 일부 파싱 오류
 - **fossid** 서버 **spdx.php** 자체 수정
- **SPDX import** 로 스캔 생성 이후 컴포넌트 중복 이슈
 - **fossid-api**에서 중복 제거 로직 추가
- **SPDX import**로 스캔 생성 이후 **component url** 미등록 이슈
 - **fossid** 서버 **spdx.php** 자체 수정
- **Git Tag** 연동
 - **branch**만 지원
 - **fossid** 서버 **scan.php** 자체 수정
- **Git clone --depth=1** 적용
 - 기존에는 **fetch && checkout** 명령을 내부 사용
 - 특정 프로젝트의 경우 **3G -> 800M, 17분 -> 3분**으로 개선
 - **fossid** 서버 **scan.php** 자체 수정
- 소스 디렉토리 이름에 공백이 존재하는 케이스 다운로드 실패
 - **fossid** 서버 **scan.php** 자체 수정

Kakao : bugfix

- **Fossid-21.2.4** 릴리즈 반영
 - 전체 스캔에 적용되는 **Global** 정책 등록이 되지 않는 버그
 - 비밀번호 변경이 되지 않는 버그
 - **Git Tag** 지원
- **Fossid-22.1** 릴리즈 예정
 - **SPDX import API**
 - **SPDX import** 로 스캔 생성 이후 컴포넌트 중복 이슈
 - **SPDX import** 일부 실패 케이스
 - **SPDX import**로 스캔 생성 이후 **component url** 미등록 이슈
 - 특정 **json** 분석 오류
- 개선 요청
 - **Git clone --depth=1** 적용
 - 사용자 등록 컴포넌트의 **Full File Match** 이외에 추가 지원
 - 소스 디렉토리 이름에 공백이 존재하는 케이스 다운로드 실패

Kakao : s/w update

- **fossid-21.2.3 -> fossid-21.2.4**
- 작업 내역
 - **DB/File** 백업 진행 : **Webapp** 메뉴 이용
 - 업데이트 버전 다운로드 : 설치파일 + 가이드 문서
 - 설치 파일을 서버로 이동
 - 패키지 설치
 - **DB** 유효성 체크 **php** 실행
 - **DB** 업데이트 **php** 실행
- **1.5시간** 소요

Kakao : review

- 장점
 - 인프라
 - 기존의 고사양 서버가 더 이상 필요하지 않아서 비용 절감
 - 확장성
 - **SPDX, ORT** 등 오픈소스와 연동이 활발하고 적극적
 - **code** 취약성 체크(**Dependency** 미지원) 기능
 - **code** 불력을 입력하여 실시간으로 **snippet search** 기능
 - 품질
 - 빠른 스캔 속도와 안정적인 분석
 - 릴리즈를 기다리지 않고 직접 **php**수정을 통한 자체 패치가 가능
 - 발전성
 - 빠른 업그레이드, 활발한 버그 패치 및 개선 등의 지원
- 단점
 - **UX** : 사용자 편의성이 부족하고 검증 작업에 많은 클릭이 필요함
 - 안정성 : 릴리즈에 따른 기존 기능 오동작

Link

- <https://fossid.com/>
- https://osbc.co.kr/page/oss_fossid_intro
- <https://www.youtube.com/channel/UCDAxa8U4ipQ.64XJocf721jg>
 - 리포트 생성 : <https://youtu.be/ch-MODgWHFg>
 - 오픈소스 식별 : <https://youtu.be/cFMA4ZP4iOU>
 - 코드스니펫 확인 : <https://youtu.be/9AbMoBdSUTI>

Thanks!



kakao |  OPENCHAIN