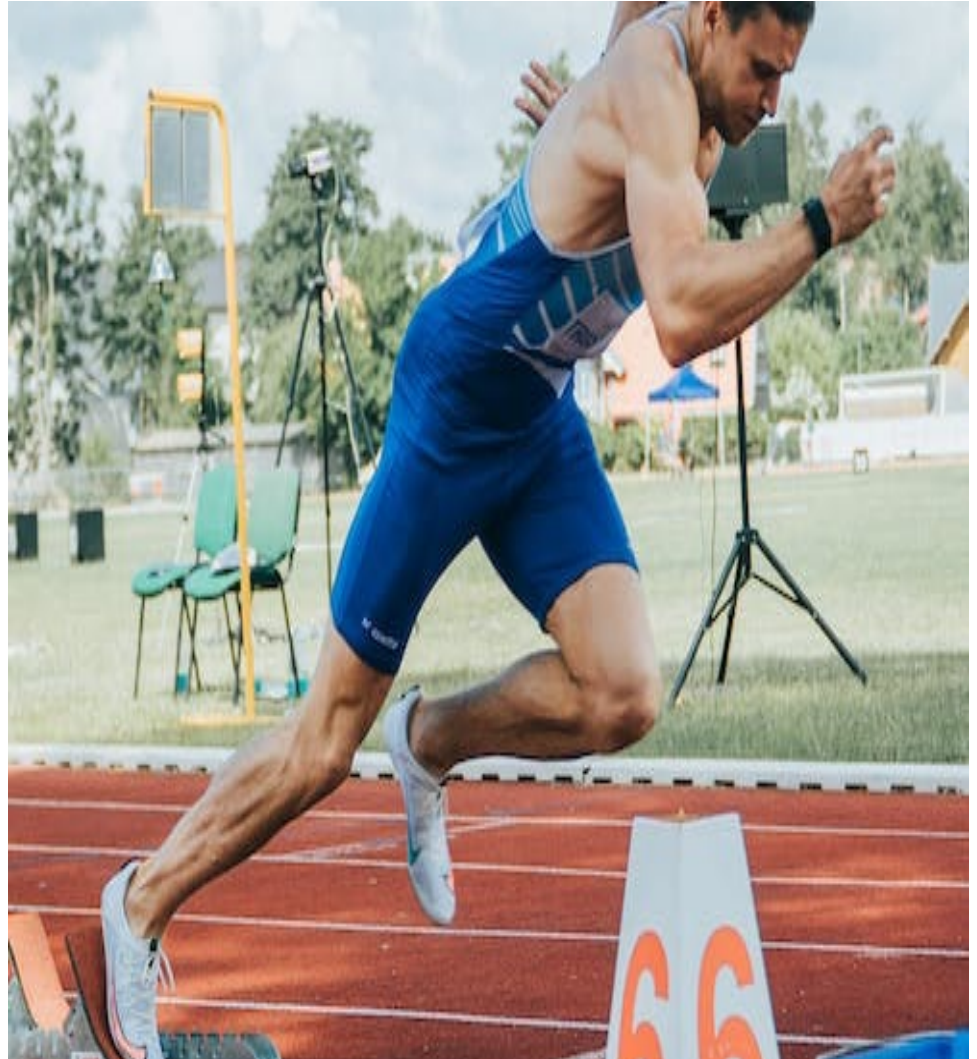


오픈소스를 활용한 web 보안정책



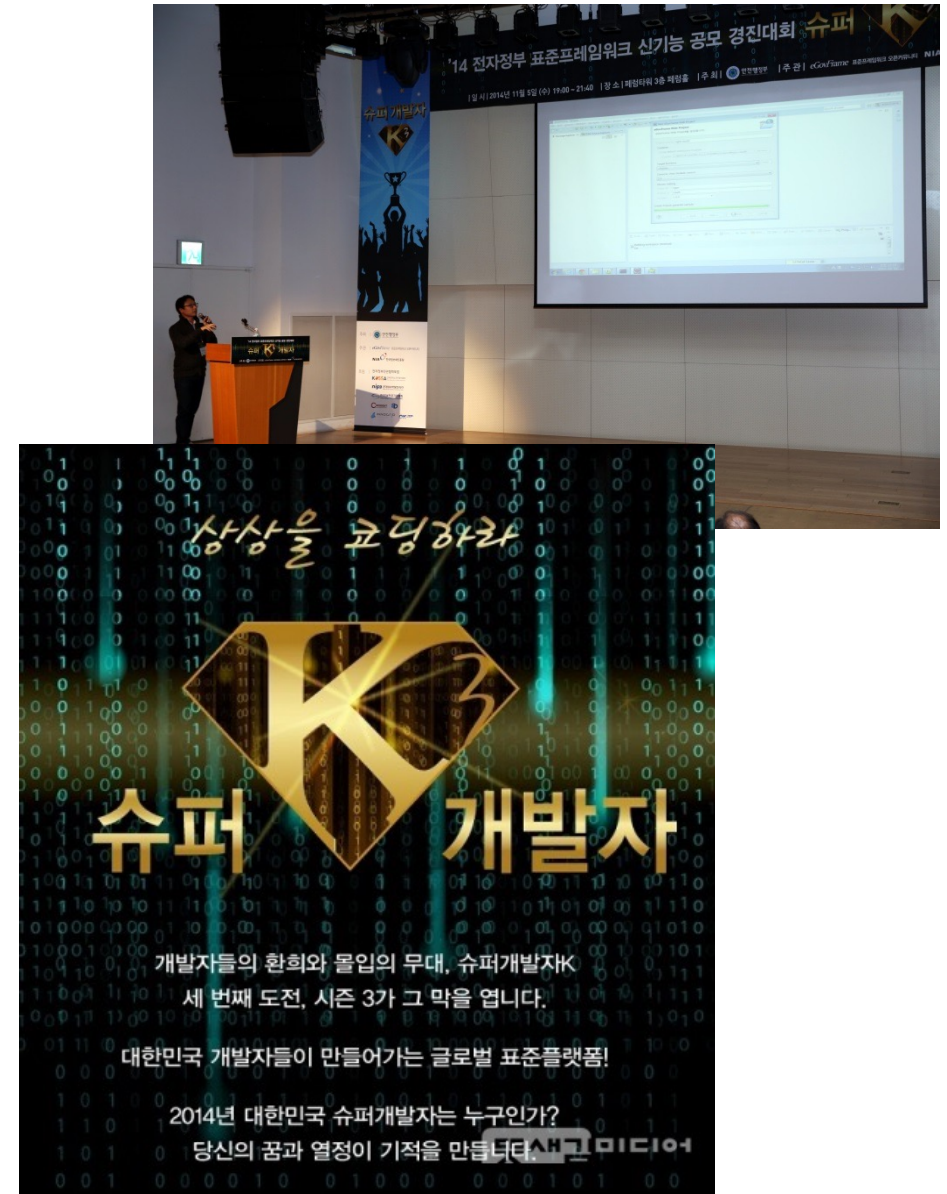
목 차

1. 발표자 소개
2. 용어 설명
3. OpenSource
4. 개발 목표
5. 개발 구현
6. 개발 시연
7. 개발 환경
8. 참고



1. 발표자 소개

- ❑ 現한화시스템 ICT부문(2021~)
 - Cloud Native BigData Platform Engineer
- ❑ 前SK주식회사 C&C(2012 ~ 2021)
 - Cloud 프로젝트 다수 구축(2017 ~ 2020)
 - 사내 강의 다수
 - 사내 개발자 대회 다수 분야 3등(2018)
- ❑ 〈나도 해보자! 시리즈〉 오픈커뮤니티 세미나 발표
 - 나도 해보자! 표준프레임워크 개발환경 구축
 - 나도 해보자! Cloud Project with Kubernetes 등
- ❑ 오픈플랫폼(PaaS) 전문가과정 강의(2016)
- ❑ 행정안전부장관 표창 수상(2021)
- ❑ 슈퍼개발자K 시즌3 동상 수상(2014)
- ❑ 現OPDC 리더(2015 ~)
- ❑ 前T-Hub(SK그룹 기술커뮤니티)
 - DevOps Master(2020~2021)



2. 용어 설명

❑ 인증(Authentication)

- 사용자(예: 유저, 시스템, 디바이스)를 확인하는 행위

❑ 인가(Authorization)

- 사용자(예: 유저, 시스템, 디바이스)가 권한이 있는지 확인하는 행위

❑ OAuth(Open Authorization)

- 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할 수 있는 공통적인 수단으로서 사용되는, 접근 위임을 위한 개방형 표준
- 이 매커니즘은 여러 기업들에 의해 사용되는데, 이를테면 아마존, 구글, 페이스북, 마이크로소프트, 트위터가 있으며 사용자들이 타사 애플리케이션이나 웹사이트의 계정에 관한 정보를 공유할 수 있게 허용함

❑ OpenID

- 비영리 재단인 OpenID 재단(OpenID Foundation)에서 관리하는 인증 수단

❑ OIDC(OpenID Connect)

- OAuth 2.0 프로토콜을 사용하여 빌드된 개방형 표준 및 단순 ID 프로토콜

2. 용어 설명

□ 통합 인증(SSO: Single Sign-On)

- 한 번의 인증 과정으로 여러 컴퓨터 상의 자원을 이용 가능하게 하는 인증 기능
- **싱글 사인온, 단일 계정 로그인, 단일 인증**
- 예를 들어 어느 컴퓨터에 로그인한 후 그룹웨어 등의 응용 프로그램을 사용할 때에 또 로그인, 다른 서버상의 응용 프로그램을 사용할 때에도 다시 로그인이 필요한 상황이라면, 사용자는 여러 개의 아이디와 비밀번호를 관리해야 한다.
- 통합인증을 도입한 환경에서는 사용자는 하나의 아이디와 비밀번호로 모든 기능을 사용 가능

□ Istio



- 기존 분산 애플리케이션에 투명하게 계층화되는 오픈 소스 서비스 메시
- Istio의 강력한 기능은 서비스를 보호, 연결 및 모니터링하는 일관되고 보다 효율적인 방법을 제공
- Istio는 서비스 코드 변경이 거의 또는 전혀 없는 로드 밸런싱, 서비스 간 인증 및 모니터링을 위한 경로

□ Keycloak



- 현대의 애플리케이션과 서비스에 초점을 둔 아이덴티티 및 접근 관리(Identity and Access Management)에 통합 인증(SSO)을 허용하는 오픈 소스 소프트웨어

2. 용어 설명

❑ LDAP (Lightweight Directory Access Protocol)

- TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜
- 디렉터리는 논리, 계급 방식 속에서 조직화된, 비슷한 특성을 가진 객체들의 모임
- 가장 일반적인 예로는 전화 번호부(telephone directory)가 있는데 가나다 순의 일련의 이름을 가지고 있고, 이름마다 전화 번호와 주소가 포함
- 이러한 기본 설계 때문에 LDAP는 인증을 위한 다른 서비스에 의해 자주 사용

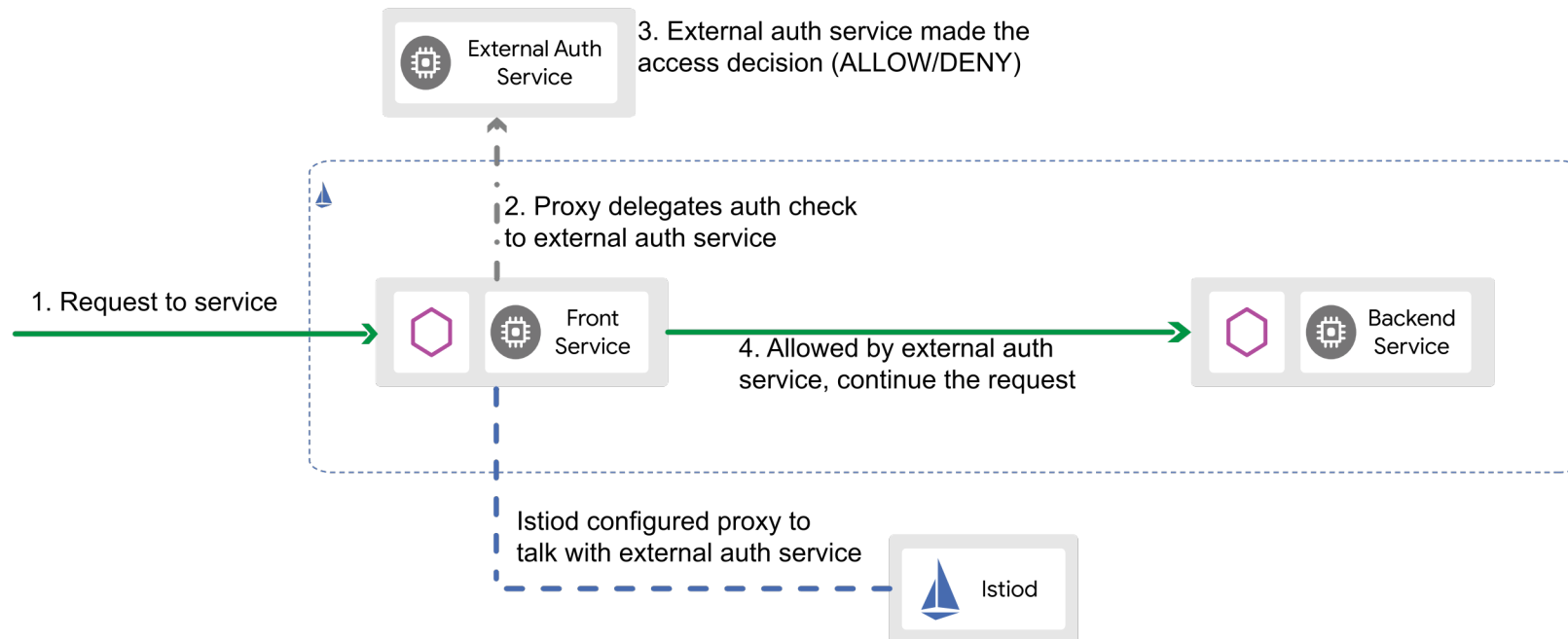
❑ OpenLDAP

- OpenLDAP 프로젝트가 개발한 LDAP의 자유 오픈 소스 구현체

3. OpenSource

❑ Istio

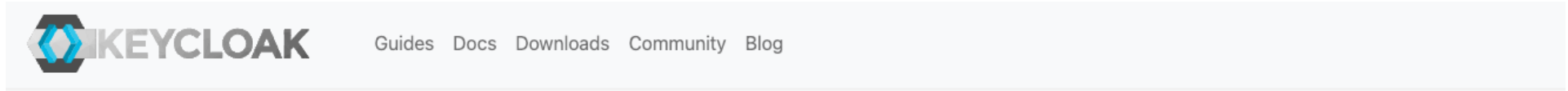
- External Authorization
- 이 태스크는 액세스 제어를 외부 인증 시스템에 위임하기 위해 작업 필드 CUSTOM의 새 값을 사용하여 Istio 인증 정책을 설정하는 방법을 보여줌
- OPA 인증, oauth2-proxy, 사용자 지정 외부 인증 서버 등과 통합하는 데 사용 가능
출처: <https://istio.io/latest/docs/tasks/security/authorization/authz-custom/>



이미지 출처: <https://istio.io/latest/blog/2021/better-external-authz/>

3. OpenSource

❑ Keycloak Gatekeeper 지원 종료



Sunsetting Louketo Project

August 21 2020 by Bruno Oliveira

This post is more than one year old. The contents within the blog is likely to be out of date.

After careful consideration, we have decided to pull the plug on Louketo and start the EOL procedure. The plan is during the next 3 months to fix only critical bugs and security issues. Everyone interested in capabilities provided by Louketo Proxy should look at [OAuth2 Proxy](#) project which is providing a similar set of capabilities and has a healthy and active community.

A few months ago, the Keycloak team started Louketo — a joint effort to build a generic OAuth2 Proxy and possibly also begin an umbrella project for a set of OIDC related integration libraries. The initial set of goals has not worked out. Keycloak Gatekeeper and OAuth2 Proxy projects hoped to merge and join efforts but for various reasons, this has not worked out.

With Louketo and OAuth2 proxy providing similar features, OAuth Proxy being a more popular project with a bigger community we reached a conclusion there's no reason to put more effort into Louketo, when we can just contribute there.

What does it mean in practice?

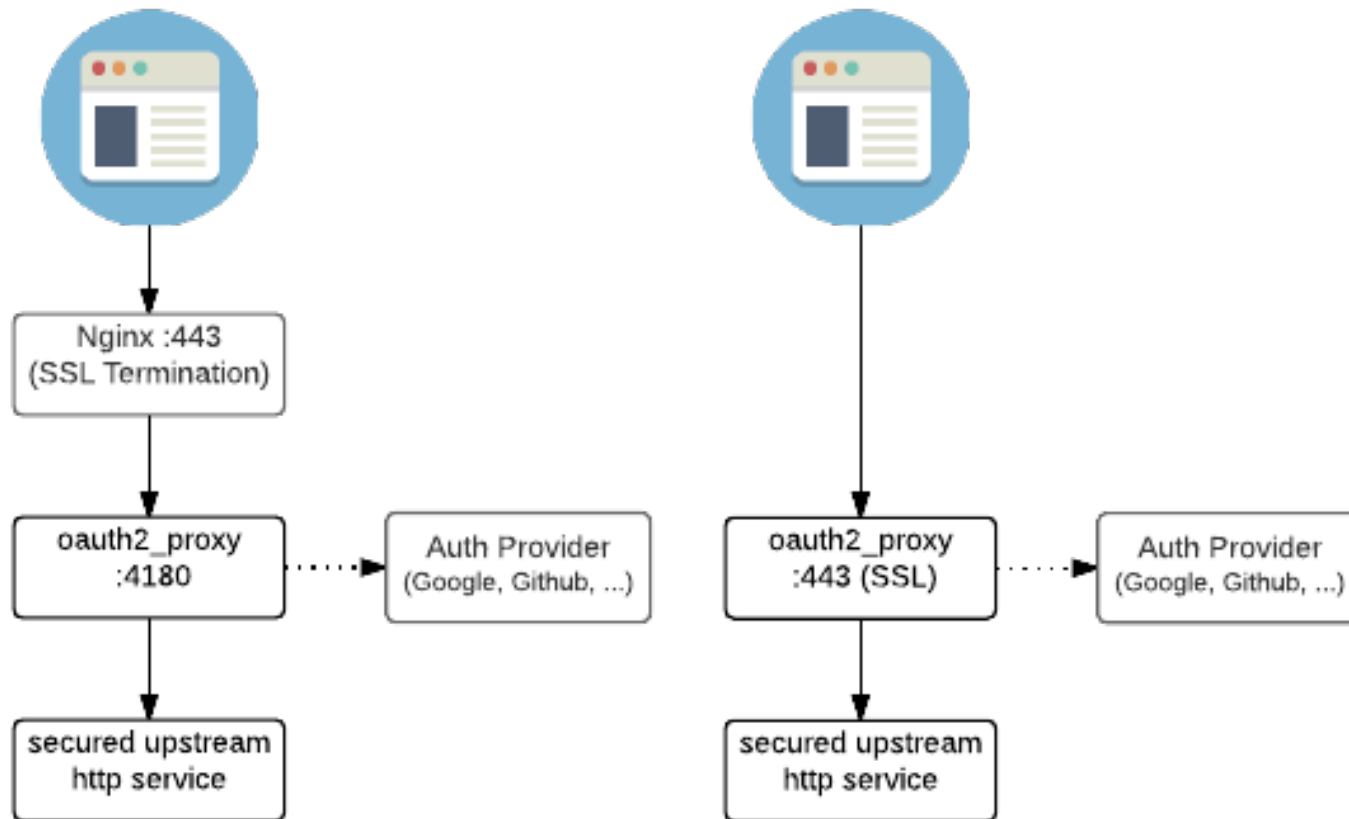
이미지 출처: <https://www.keycloak.org/2020/08/sunsetting-louketo-project.adoc>

3. OpenSource

❑ OAuth2-proxy

- 이메일, 도메인 또는 그룹별로 계정을 검증하기 위해 공급자(Google, GitHub 등)를 사용하여 인증을 제공하는 역방향 프록시 및 정적 파일 서버입니다.

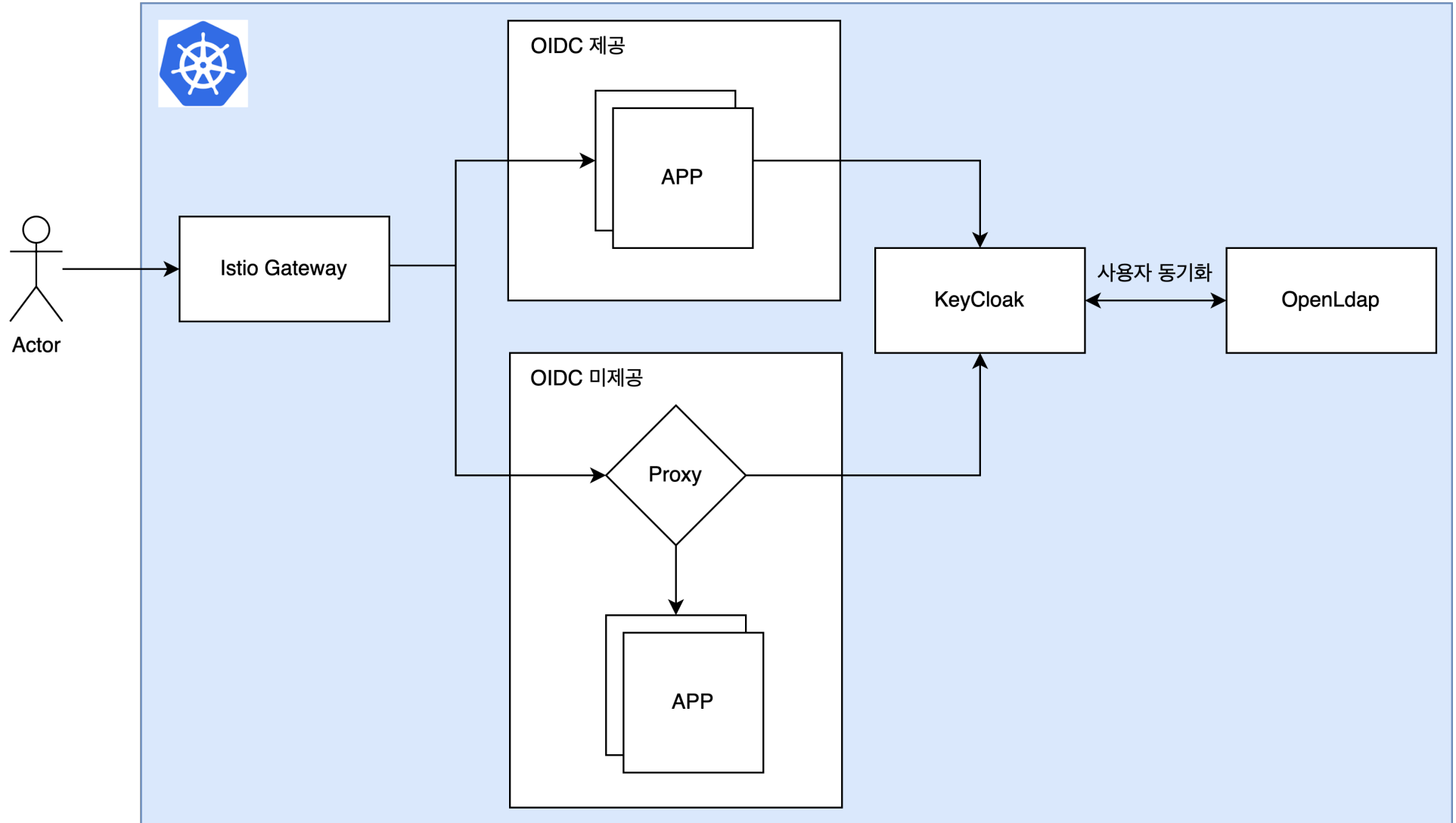
- **Architecture**



이미지 출처: <https://oauth2-proxy.github.io/oauth2-proxy/>

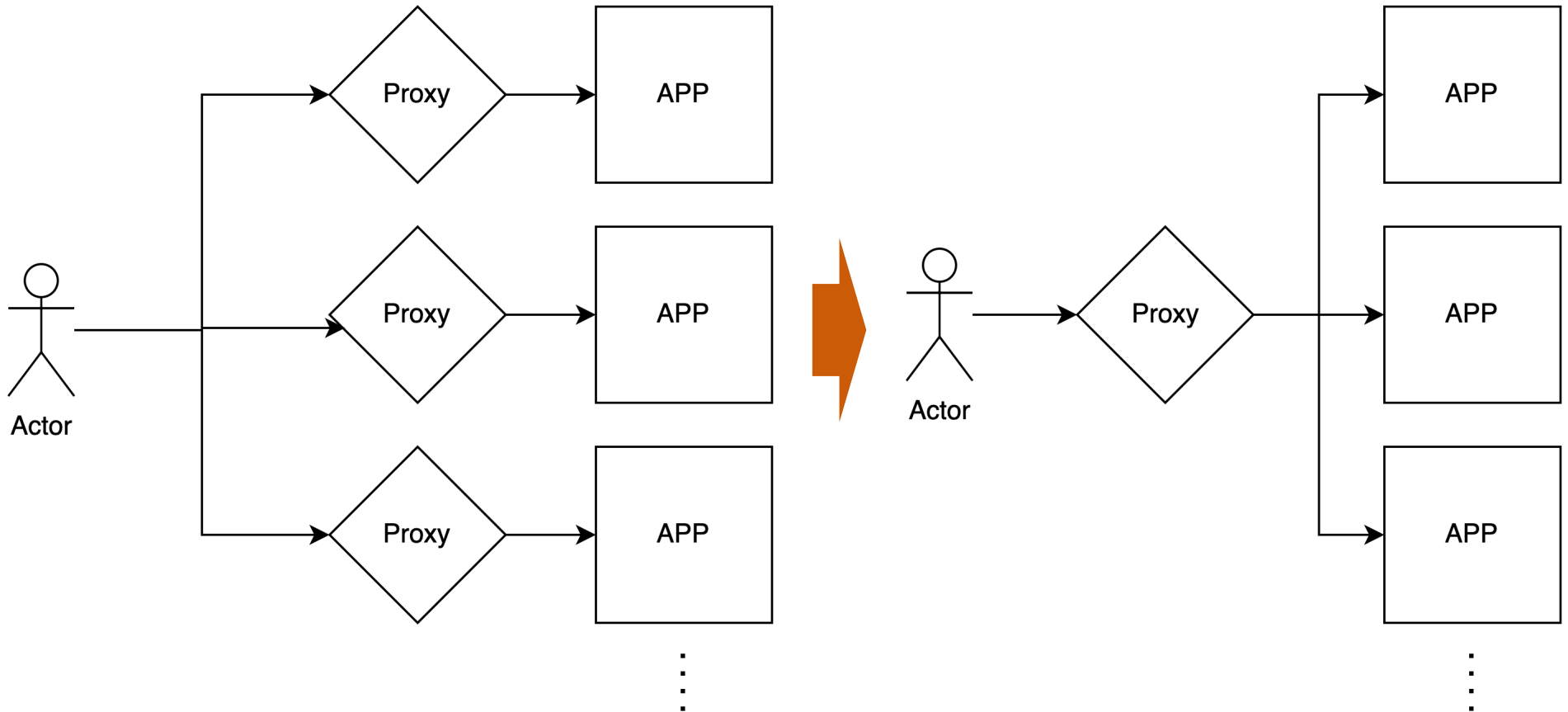
4. 개발 목표

□ Architecture



4. 개발 목표

□ Proxy Architecture



5. 개발 구현

예제 소스

```
openInfra_community_2023 ~/Documents/IdeaPro
├── .idea
├── certificate
│   ├── _openinfra.io
│   ├── certificate.sh
│   ├── minica.pem
│   └── minica-key.pem
├── istio
│   ├── local-authorizationpolicy_keycloak_dev.yaml
│   ├── local-gateway.yaml
│   ├── localhost-vs.yaml
│   ├── values-gateway-local.yaml
│   └── values-istiod-local.yaml
├── keycloak
│   ├── dev-realm-export.json
│   └── values-keycloak.yaml
├── kube-prometheus-stack
│   └── values-kube-prometheus-stack-local.yaml
├── oauth2-proxy
│   └── values-oauth2-proxy-local.yaml
├── openldap-stack-ha
│   ├── openldap-vs.yaml
│   └── values-openldap-stack-ha-local.yaml
└── install.sh
```

```
#!/usr/bin/env bash
```

```
# helm setting
```

```
# helm repo
```

```
helm repo add istio https://istio-release.storage.googleapis.com/charts
```

```
helm repo add helm-openldap https://jp-gouin.github.io/helm-openldap/
```

```
helm repo add oauth2-proxy https://oauth2-proxy.github.io/manifests
```

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

```
# helm update
```

```
helm repo update istio
```

```
helm repo update helm-openldap
```

```
helm repo update oauth2-proxy
```

```
helm repo update bitnami
```

```
# certificate
```

```
brew install minica
```

```
minica -domains '*.openinfra.io' -ip-addresses xx.xxx.xx.xx
```

```
kubectrl create secret tls tls-secret --cert=./certificate/minica.pem --key=./certificate/minica-key.pem -n istio-ingress
```

```
# istio
```

```
helm upgrade --install istio-base istio/base -n istio-system --version 1.18.0 --create-namespace
```

```
helm upgrade --install istiod istio/istiod -f ./istio/values-istiod-local.yaml -n istio-system --version 1.18.0 --create-namespace
```

```
helm upgrade --install istio-ingress istio/gateway -f ./istio/values-gateway-local.yaml -n istio-ingress --version 1.18.0 --create-namespace
```

```
# istio ingress-gateway
```

```
kubectrl apply -f ./istio/local-gateway.yaml
```

```
# istio virtual service
```

```
kubectrl apply -f ./istio/localhost-vs.yaml
```

```
# istio
```

```
kubectrl apply -f ./istio/local-authorizationpolicy_keycloak_dev.yaml
```

```
# openldap
```

```
helm upgrade --install openldap-stack-ha -f ./openldap-stack-ha/values-openldap-stack-ha-local.yaml helm-openldap/openldap-stack-ha
```

```
-n openldap --version 4.1.1 --create-namespace
```

```
kubectrl apply -f ./openldap-stack-ha/openldap-vs.yaml
```

```
# keycloak
```

```
helm upgrade --install keycloak -f ./keycloak/values-keycloak.yaml bitnami/keycloak --version 15.1.4 -n keycloak --create-namespace
```

```
# kube-prometheus-stack
```

```
helm upgrade --install ps -f ./kube-prometheus-stack/values-kube-prometheus-stack-local.yaml prometheus-community/kube-prometheus-stack
```

```
--version 41.6.0 -n ps --create-namespace
```

```
# oauth2-proxy
```

```
helm upgrade --install dev -f ./oauth2-proxy/values-oauth2-proxy-local.yaml oauth2-proxy/oauth2-proxy --version 6.13.1
```

```
-n oauth2-proxy --create-namespace
```

```
kubectrl apply -f ./oauth2-proxy/openldap-vs.yaml
```

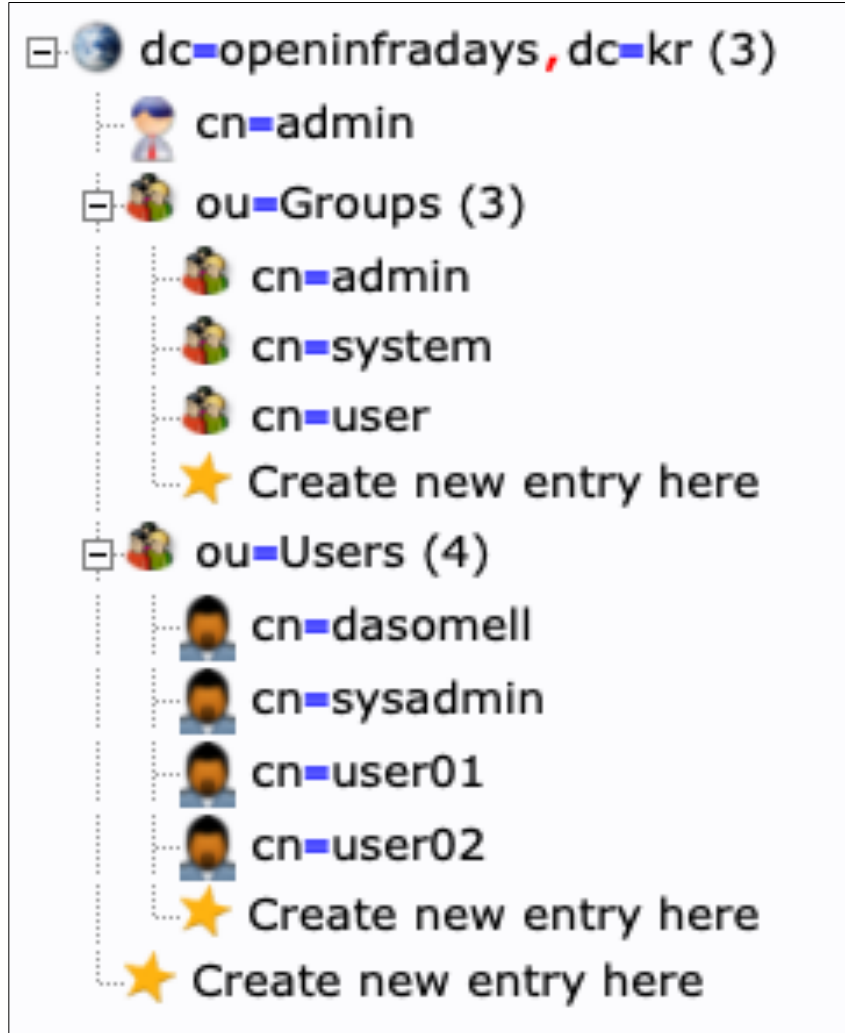
5. 개발 구현

□ 권한 설정

설명	app	URI	구현방식	App 세부권한	ldap group	비고
사용자 관리	openldap	openldap.openinfra.io	oauth2-proxy	N/A	admin	인가 후 id/pw 로그인
메트릭/ 로그 시각화	grafana	dev.openinfra.io /grafana	helm 설정	Admin	admin	대시보드, 사용자 및 팀을 포함한 모든 조직 리소스에 액세스
				Editor	system	대시보드, 폴더 및 재생 목록을 보고 편집
				Viewer	user	대시보드 및 재생 목록을 볼 수 있음
Infra 메트릭 수집 시스템	prometheus	dev.openinfra.io /prometheus	oauth2-proxy	N/A	admin, system	app 자체 로그인 안함
Infra 메트릭 알람	alertmanager	dev.openinfra.io /alertmanager	oauth2-proxy	N/A	admin, system	app 자체 로그인 안함

6. 개발 시연

❑ User 연동



OpenLDAP

User	Group	비고
dasomell	admin	관리자
sysadmin	system	시스템
user01	user	일반사용자01
user02	user	일반사용자02

Users				
Users are the users in the current realm. Learn more				
User list				
Q *	x	→	Add user	Delete user
1 - 4 < >				
<input type="checkbox"/>	Username	Email	Last name	First name
<input type="checkbox"/>	dasomell	dasomell@gmail.com	이기하	—
<input type="checkbox"/>	sysadmin	sysadmin@openinfra.ai	시스템	—
<input type="checkbox"/>	user01	user01@openinfra.ai	일반사용자01	—
<input type="checkbox"/>	user02	user02@openinfra.ai	일반사용자02	—

Keycloak

6. 개발 시연

□ Group 연동

openldap-stack-ha.openldap

schema search refresh info monitor import export logout

Logged in as: cn=admin

dc=openinfra-days, dc=kr (3)

- cn=admin
- ou=Groups (3)
 - cn=admin
 - cn=system
 - cn=user
- Create new entry here
- ou=Users (4)
 - cn=dasomell
 - cn=sysadmin
 - cn=user01
 - cn=user02
- Create new entry here
- Create new entry here

cn=admin

Server: openldap-stack-ha.openldap Distinguished Name: cn=admin, ou=Groups, dc=openinfra-days, dc=kr Template: Default

Refresh Switch Template Copy or move this entry Rename Create a child entry Show internal attributes Export Delete this entry Compare with another entry Add new attribute

Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.

cn admin required, rdn

member required

cn=dasomell, ou=Users, dc=openinfra-days, dc=kr

objectClass

- groupOfNames

Update Object

OpenLDAP

Groups > Group details

admin

Child groups Members Attributes Role mapping

Add member Include sub-group users 1-1

Name	Email	First name	Last name	Membersh...
<input type="checkbox"/> dasomell	dasomell@gmail.com	-	이기하	/admin

Keycloak

6. 개발 시연

□ Group 연동

openldap-stack-ha.openldap

Server: openldap-stack-ha.openldap Distinguished Name: cn=system,ou=Groups,dc=openinfra,dc=kr Template: Default

Refresh Switch Template Copy or move this entry Rename Create a child entry Show internal attributes Export Delete this entry Compare with another entry Add new attribute

Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.

cn (required, rdn)
system
(add value)
(rename)

member (required)
cn=sysadmin,ou=Users,dc=openinfra,dc=kr
(add value)
(modify group members)

objectClass
groupOfNames
(add value)

Update Object

OpenLDAP

Groups > Group details

system

Child groups Members Attributes Role mapping

Add member ☐ Include sub-group users 1-1

<input type="checkbox"/>	Name	Email	First name	Last name	Members...
<input type="checkbox"/>	sysadmin	sysadmin@openinfra.ai	-	시스템	/system

1-1

Keycloak

6. 개발 시연

□ Group 연동

The image illustrates the integration between OpenLDAP and Keycloak. On the left, the OpenLDAP interface shows a tree structure with a group 'cn=user' highlighted. This group is linked to the 'user' group in Keycloak, which is shown on the right. The 'user' group in Keycloak has two members: 'user02' and 'user01'.

OpenLDAP

Server: openldap-stack-ha.openldap Distinguished Name: cn=user,ou=Groups,dc=openinfra,dc=kr Template: Default

Attributes:

- cn: user (required, rdn)
- member: cn=user01,ou=Users,dc=openinfra,dc=kr; cn=user02,ou=Users,dc=openinfra,dc=kr (required)
- objectClass: groupOfNames (add value)

Keycloak

Groups > Group details

user

Members

Name	Email	First name	Last name	Members...
user02	user02@openinfra.ai	-	일반사용자02	/user
user01	user01@openinfra.ai	-	일반사용자01	/user

6. 개발 시연

❑ OIDC 제공되는 APP

- [로그인] 최초접속

<https://dev.openinfra.io/grafana/>



<https://dev.openinfra.io/grafana/login>



https://dev.openinfra.io/grafana/login/generic_oauth



https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/auth?access_type=online&client_id=grafana&redirect_uri=https%3A%2F%2Fdev.openinfra.io%2Fgrafana%2Flogin%2Fgeneric_oauth&response_type=code&scope=openid+profile+email+groups&state=Hj2xwnZWmQLwuzcdBCM_s8Maykz282kEroCKWpEjsIO%3D



OPENINFRA COMMUNITY DAYS KOREA 2023

Sign in to your account

Username or email

Password

[Sign In](#)

grafana/	302	document	기타	251 B	2...	
login	307	document	/grafana/	134 B	2...	
generic_oauth	302	document	/grafana/login	698 B	1...	
auth?access_type=online&client_id=grafana&...	200	document	/grafana/login/generi...	4.5 kB	7...	

6. 개발 시연

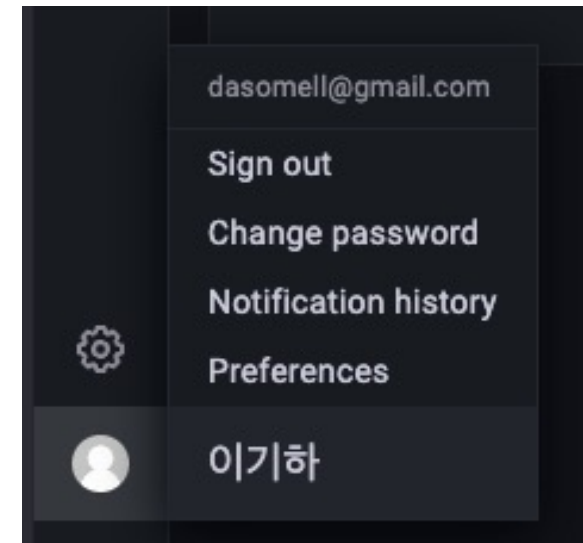
❑ OIDC 제공되는 APP

- [로그인] 관리자

https://dev.openinfra.io/keycloak/realms/dev/login-actions/authenticate?session_code=_tOHhFU_79bdFgLv2KY0luCxtI983OSHchc9Z-K99Gg&execution=b2e292e2-802d-44a4-9491-67bc9e88d0d5&client_id=grafana&tab_id=U4TLxCUBNX0

https://dev.openinfra.io/grafana/login/generic_oauth?state=qJf9YxRx26tZ5rlcz3GhYB0FV_6Y61qVdJuTeBw5o9E%3D&session_state=be4c8787-8468-48c4-8532-df7ab348c7b9&code=fd814df8-7cec-421d-9d71-9f1615010637.be4c8787-8468-48c4-8532-df7ab348c7b9.c45cdb3d-c4d4-4530-a581-9c5c4aa8d6dd

<https://dev.openinfra.io/grafana/>



authenticate?session_code=_tOHhFU_79bdF...	302	document...	기타	2.0 kB	4...	
generic_oauth?state=qJf9YxRx26tZ5rlcz3Gh...	302	document...	/keycloak/realms/de...	295 B	8...	
grafana/	200	document	/grafana/login/generi...	40.5 kB	1...	

6. 개발 시연

❑ OIDC 제공되는 APP

- [로그인] 관리자

Sessions						Action
Sessions are sessions of users in this realm and the clients that they access within the session. Learn more						
All session types		Search session		1-1		
User	Type	Started	Last access	IP address	Clients	
dasomell	REGULAR	7/2/2023, 11:50:07 AM	7/2/2023, 11:50:07 AM	10.211.55.20	grafana	

Configuration					
Organization: Main Org.					
Data sources Users Teams Plugins Preferences API keys Service accounts					
Search user by login, email or name					
Invite					
Login	Email	Name	Seen	Role	
admin	admin@localhost		18 minutes	Admin	
dasomell@gmail.com	dasomell@gmail.com	이기하	1 minute	Admin	

6. 개발 시연

❑ OIDC 제공되는 APP


- [로그인] 시스템관리자

Sessions Action ▾

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)




⌵ All session types ▾ 🔍 Search session → 1-2 ▾ < >

User	Type	Started	Last access	IP address	Clients
dasomell	REGULAR	7/2/2023, 11:50:07 AM	7/2/2023, 11:50:07 AM	10.211.55.20	grafana ⋮
sysadmin	REGULAR	7/2/2023, 11:52:57 AM	7/2/2023, 11:53:14 AM	10.211.55.20	grafana ⋮

 **Configuration**
Organization: Main Org.

📄 Data sources 👤 **Users** 👥 Teams ⚙️ Plugins ⚙️ Preferences 🔑 API keys 🗝️ Service accounts

🔍 Search user by login, email or name Invite

Login	Email	Name	Seen	Role
 admin	admin@localhost		21 minutes	Admin ▾
 dasomell@gmail.com	dasomell@gmail.com	이기하	4 minutes	Admin ▾
 sysadmin@openinfra.ai	sysadmin@openinfra.ai	시스템	1 minute	Editor ▾


sysadmin@openinfra.ai

Sign out

Change password

Notification history

Preferences

 시스템

6. 개발 시연

❑ OIDC 제공되는 APP

- [로그인] 일반사용자01

Sessions Action ▾

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)

⌵ All session types ▾ 🔍 Search session → 1 - 3 < >

User	Type	Started	Last access	IP address	Clients
dasomell	REGULAR	7/2/2023, 11:50:07 AM	7/2/2023, 11:50:07 AM	10.211.55.20	grafana ⋮
sysadmin	REGULAR	7/2/2023, 11:52:57 AM	7/2/2023, 11:53:14 AM	10.211.55.20	grafana ⋮
user01	REGULAR	7/2/2023, 11:56:06 AM	7/2/2023, 11:56:22 AM	10.211.55.20	grafana ⋮

Configuration
Organization: Main Org.

Data sources **Users** Teams Plugins Preferences API keys Service accounts

🔍 Search user by login, email or name Invite

Login	Email	Name	Seen	Role
admin	admin@localhost		25 minutes	Admin ▾
dasomell@gmail.com	dasomell@gmail.com	이기하	2 minutes	Admin ▾
sysadmin@openinfra.ai	sysadmin@openinfra.ai	시스템	4 minutes	Editor ▾
user01@openinfra.ai	user01@openinfra.ai	일반사용자01	< 1 minute	Viewer ▾

user01@openinfra.ai

Sign out

Change password

Notification history

Preferences

일반사용자01

6. 개발 시연

❑ OIDC 제공되는 APP

- Grafana 설정

```
grafana:
  defaultDashboardsTimezone: Asia/Seoul
  adminPassword: xxxx
  grafana.ini:
    grafana_net:
      url: https://dev.openinfra.io/grafana
    server:
      domain: dev.openinfra.io
      root_url: https://dev.openinfra.io/grafana
      serve_from_sub_path: true
    auth.generic_oauth:
      enabled: true
      tls_skip_verify_insecure: true
      name: "Keycloak"
      allow_sign_up: true
      client_id: "grafana"
      client_secret: "bquuaPKNixHsKm0umP...v"
      scopes: "openid profile email groups"
      email_attribute_name: email
      auth_url: "https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/auth"
      token_url: "https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/token"
      api_url: "https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/userinfo"
      oauth_auto_login: true
      role_attribute_path: "contains(groups[*], '/admin') && 'Admin' || contains(groups[*], '/system') && 'editor' || 'Viewer'"
```

자동 로그인 설정

권한 설정

자동 로그인 로그

```
logger=context userId=0 orgId=0 uname= t=2023-07-02T02:56:22.23928962Z level=info
msg="OAuth auto login enabled. Redirecting to /grafana/login/generic_oauth"
```

6. 개발 시연

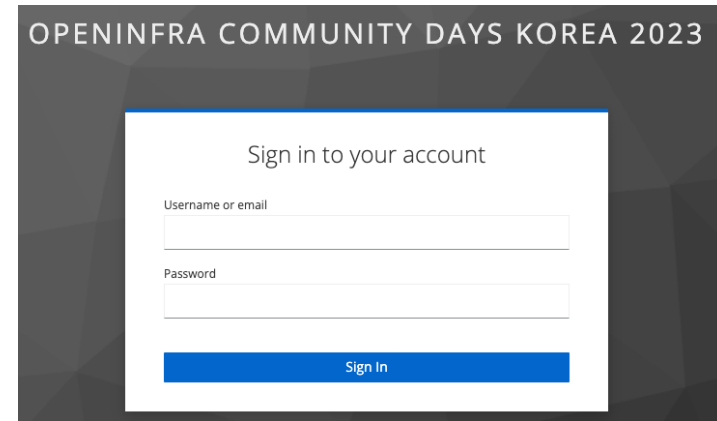
❑ OIDC 미제공 되는 APP





- [로그인] 최초접속

`http://openldap.openinfra.io/`



`https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/auth?client_id=oauth2-proxy&nonce=vSK4l5ciEIU92GdTbUDLPIjFpNzHzr1QxIAwEUMGTyM&redirect_uri=http%3A%2F%2Fopenldap.openinfra.io%2Foauth2%2Fcallback&response_type=code&scope=openid+email+profile+groups&state=00TuGOyLBWqFnPj8aZwOk3iwFRBzjzBxqCN8E9DMOuU%3Ahttps%3A%2F%2Fopenldap.openinfra.io%2F`



 openldap.openinfra.io	302	documen...	기타	812 B	7...	
 auth?client_id=oauth2-proxy&nonce=vSK4l...	200	document	openldap.openinfra...	4.3 kB	2...	

6. 개발 시연

❑ OIDC 미제공 되는 APP

- [로그인] 관리자

https://dev.openinfra.io/keycloak/realms/dev/login-actions/authenticate?session_code=XqQawDNXrhhknVw4hdk17hnAmy2wMROzS9T0G2hpMY&execution=b2e292e2-802d-44a4-9491-67bc9e88d0d5&client_id=oauth2-proxy&tab_id=sR_rTHb3JNc



http://openldap.openinfra.io/oauth2/callback?state=0OTuGOyLBWqFnPj8aZwOk3iwFRBzjzBxqCN8E9DMOuU%3Ahttps%3A%2F%2Fopenldap.openinfra.io%2F&session_state=e8f8f10e-0ef3-4e28-814e-0154871b8998&code=66a0d750-bcc8-4c02-bb5d-b0088049444d.e8f8f10e-0ef3-4e28-814e-0154871b8998.29593503-a23c-4a2c-9cee-112e247b70eb



https://openldap.openinfra.io/oauth2/callback?state=0OTuGOyLBWqFnPj8aZwOk3iwFRBzjzBxqCN8E9DMOuU%3Ahttps%3A%2F%2Fopenldap.openinfra.io%2F&session_state=e8f8f10e-0ef3-4e28-814e-0154871b8998&code=66a0d750-bcc8-4c02-bb5d-b0088049444d.e8f8f10e-0ef3-4e28-814e-0154871b8998.29593503-a23c-4a2c-9cee-112e247b70eb



<https://openldap.openinfra.io/>

authenticate?session_code=XqQawDNXrhh...	302	document...	기타	2.1 kB	4...	
callback?state=0OTuGOyLBWqFnPj8aZwO...	301	document...	dev.openinfra.io/ke...	426 B	3...	
callback?state=0OTuGOyLBWqFnPj8aZwO...	302	document...	/oauth2/callback?st...	3.5 kB	2...	
openldap.openinfra.io	200	document	/oauth2/callback?st...	1.7 kB	6...	

6. 개발 시연

❑ OIDC 미제공 되는 APP

- [로그인] 관리자

Sessions						Action ▾
Sessions are sessions of users in this realm and the clients that they access within the session. Learn more						
All session types ▾		Search session →		1-1 ▾		< >
User	Type	Started	Last access	IP address	Clients	
dasomell	REGULAR	7/2/2023, 12:24:42 PM	7/2/2023, 12:24:42 PM	10.211.55.20	oauth2-proxy	⋮

6. 개발 시연

❑ OIDC 미제공 되는 APP

- [로그인] 일반사용자01

`https://dev.openinfra.io/keycloak/realms/dev/login-actions/authenticate?session_code=J-4w9U8mK20CtyNiJv9XxP2xMwgmOjc4Z9z-bRRl2k&execution=b2e292e2-802d-44a4-9491-67bc9e88d0d5&client_id=oauth2-proxy&tab_id=R1yDRLiOnaQ`



`http://openldap.openinfra.io/oauth2/callback?state=WN1o2MZZ0H9c5MQKYbpdzZUjJCl6a6YhIU-4sOi-bs%3Ahttps%3A%2F%2Fopenldap.openinfra.io%2F&session_state=3d5fa479-55ea-415b-a5ec-d947a60779e4&code=5bde83ef-19dc-419b-8937-2bcf7b6e6a73.3d5fa479-55ea-415b-a5ec-d947a60779e4.29593503-a23c-4a2c-9cee-112e247b70eb`



`https://openldap.openinfra.io/oauth2/callback?state=WN1o2MZZ0H9c5MQKYbpdzZUjJCl6a6YhIU-4sOi-bs%3Ahttps%3A%2F%2Fopenldap.openinfra.io%2F&session_state=3d5fa479-55ea-415b-a5ec-d947a60779e4&code=5bde83ef-19dc-419b-8937-2bcf7b6e6a73.3d5fa479-55ea-415b-a5ec-d947a60779e4.29593503-a23c-4a2c-9cee-112e247b70eb`

<code>authenticate?session_code=J-4w9U8mK20...</code>	302	document...	기타	2.1 kB	4...	
<code>callback?state=WN1o2MZZ0H9c5MQKYbp...</code>	301	document...	<code>dev.openinfra.io/ke...</code>	426 B	3...	
<code>callback?state=WN1o2MZZ0H9c5MQKYbp...</code>	403	document	<code>/oauth2/callback?st...</code>	3.0 kB	2...	

6. 개발 시연

❑ OIDC 미제공 되는 APP

- [로그인] 일반사용자01

Sessions

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)

All session types

Search session

→

1 - 2

User	Type	Started	Last access	IP address	Clients
dasomell	REGULAR	7/2/2023, 12:24:42 PM	7/2/2023, 12:24:42 PM	10.211.55.20	oauth2-proxy
user01	REGULAR	7/2/2023, 12:27:03 PM	7/2/2023, 12:27:03 PM	10.211.55.20	oauth2-proxy

403

Forbidden

More Info

Invalid session: unauthorized

Request ID: 948a3bf4-ed7d-45a3-8932-c508445a9896

Go back

Sign in

6. 개발 시연

❑ OIDC 미제공 되는 APP

- OAuth2-proxy 설정

```
alphaConfig:  
  enabled: true  
  configData:  
    providers:  
      - id: oidc-istio  
        clientID: oauth2-proxy  
        clientSecret: zddgG9jiOp3  
        provider: keycloak-oidc  
        loginURL: https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/auth  
        redeemURL: https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/token  
        profileURL: https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/userinfo  
        validateURL: https://dev.openinfra.io/keycloak/realms/dev/protocol/openid-connect/userinfo  
        scope: "openid email profile groups"  
    allowedGroups:  
      - /admin  
      - /system
```

인가 허용 그룹

7. 개발 환경

❑ Kubernetes Pod

- Kubectl get pod -A

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
istio-ingress	istio-ingress-54464bcb87-nz9wh	1/1	Running	0	18h
istio-system	istiod-68757f57b4-6rzt6	1/1	Running	0	16h
keycloak	keycloak-0	2/2	Running	1 (9h ago)	20h
keycloak	keycloak-postgresql-0	2/2	Running	5 (7h35m ago)	20h
kube-system	calico-kube-controllers-84c476996d-bdpb	1/1	Running	5 (7h46m ago)	173d
kube-system	calico-node-hb4ks	1/1	Running	1 (27h ago)	173d
kube-system	coredns-57575c5f89-2wdmh	1/1	Running	1 (27h ago)	173d
kube-system	coredns-57575c5f89-5tl8r	1/1	Running	1 (27h ago)	173d
kube-system	etcd-h	1/1	Running	1 (27h ago)	173d
kube-system	kube-apiserver-h	1/1	Running	5 (7h46m ago)	173d
kube-system	kube-controller-manager-h	1/1	Running	66 (7h35m ago)	173d
kube-system	kube-proxy-zqscp	1/1	Running	1 (27h ago)	173d
kube-system	kube-scheduler-h	1/1	Running	63 (7h36m ago)	173d
kube-system	nfs-provisioner-nfs-subdir-external-provisioner-76d878d9d8kc29m	1/1	Running	61 (7h37m ago)	27h
oauth2-proxy	dev-oauth2-proxy-85f685c54d-pb9gh	2/2	Running	1 (16h ago)	16h
openldap	openldap-stack-ha-0	1/1	Running	1 (27h ago)	27h
openldap	openldap-stack-ha-1	1/1	Running	1 (27h ago)	27h
openldap	openldap-stack-ha-2	1/1	Running	1 (27h ago)	27h
openldap	openldap-stack-ha-phpldapadmin-59997cfd4f-52676	1/1	Running	0	27h
ps	alertmanager-ps-kube-prometheus-stack-alertmanager-0	2/2	Running	1 (27h ago)	27h
ps	prometheus-ps-kube-prometheus-stack-prometheus-0	2/2	Running	15 (7h35m ago)	27h
ps	ps-grafana-78644c545c-vk4rb	4/4	Running	0	6h7m
ps	ps-kube-prometheus-stack-operator-9cd4499fb-x6kk4	1/1	Running	0	27h
ps	ps-kube-state-metrics-5d98878b6f-49wxp	1/1	Running	0	27h
ps	ps-prometheus-node-exporter-97jcg	1/1	Running	76 (7h37m ago)	27h

8. 참고

설명	app	URI	구현방식	App 세부권한	비고
데이터 파이프라인 관리	airflow	airflow.openinfra.io	flask	Admin	다른 사용자의 권한 부여 또는 취소를 포함하여 가능한 모든 권한
				Public	권한이 없음
				Viewer	제한된 뷰어 권한
				User	Viewer권한과 추가 사용자 권한
				Op	User권한과 추가 운영 권한
BI 시각화 및 Query 툴	superset	superset.openinfra.io	flask	Admin	다른 사용자의 권한 부여 또는 취소, 다른 사람의 슬라이스 및 대시보드 변경을 포함하여 가능한 모든 권한
				Public	권한이 없음
				Alpha	모든 데이터 소스에 액세스할 수 있지만 다른 사용자의 액세스 권한을 부여하거나 취소 불가 자신이 소유한 객체를 변경하는 것으로 제한 Alpha 사용자는 데이터 소스를 추가하고 변경 가능
				Gamma	액세스가 제한 그들은 다른 보안 역할을 통해 액세스 권한이 부여된 데이터 소스에서 오는 데이터만 사용 액세스 권한이 있는 데이터 원본에서 만든 슬라이스 및 대시보드를 볼 수 있는 액세스 권한만 있음 데이터 소스를 변경하거나 추가할 수 없음 슬라이스와 대시보드를 만들 수 있지만 대부분 콘텐츠 소비자라고 가정합니다. Gamma 사용자가 대시보드와 조각 목록 보기를 볼 때 액세스 권한이 있는 개체만 표시
				sql_lab	SQL Lab에 대한 액세스 권한을 부여
Image Repository	harbor	harbor.openinfra.io	app 설정 (OIDC)	Limited Guest	프로젝트에 대한 전체 읽기 권한이 없음 이미지를 끌어올 수는 있지만 푸시할 수는 없으며, 로그인 프로젝트의 다른 멤버를 볼 수 없음
				Guest	지정된 프로젝트에 대한 읽기 전용 권한 이미지를 끌어오고 태그를 다시 지정할 수 있지만 푸시는 할 수 없음
				Developer	프로젝트에 대한 읽기 및 쓰기 권한
				Maintainer	이미지 스캔, 복제 작업 보기, 이미지 및 헬름 차트 삭제 등의 기능을 포함하여 '개발자' 이상의 권한
				ProjectAdmin	새 프로젝트를 만들 때 프로젝트에 "ProjectAdmin" 역할이 할당 읽기/쓰기 권한 외에도 "ProjectAdmin"에는 멤버 추가 및 제거, 취약점 스캔 시작과 같은 일부 관리 권한

8. 참고

설명	app	URI	구현방식	App 세부권한	비고
Object Storage	minio	minio.openinfra.io	helm 설정	consoleAdmin	관리자
				diagnostics	MinIO 진단 기능 접근 권한
				readonly	읽기 전용
				readwrite	읽기/쓰기 가능
				writeonly	쓰기 전용
사용자 관리	openldap	openldap.openinfra.io	oauth2-proxy	N/A	인가 후 id/pw 로그인
메트릭/ 로그 시각화	grafana	dev.openinfra.io /grafana	helm 설정	Admin	대시보드, 사용자 및 팀을 포함한 모든 조직 리소스에 액세스
				Editor	대시보드, 폴더 및 재생 목록을 보고 편집
				Viewer	대시보드 및 재생 목록을 볼 수 있음
Infra 메트릭 수집 시스템	prometheus	dev.openinfra.io /prometheus	oauth2-proxy	N/A	app 자체 로그인 안함
Infra 메트릭 알람	alertmanager	dev.openinfra.io /alertmanager	oauth2-proxy	N/A	app 자체 로그인 안함
라이브러리 저장소 관리	nexus	dev.openinfra.io /nexus	oauth2-proxy / app 설정(LDAP)	nx-admin	관리자
				nx-anonymous	익명사용자



Questions
Answers



감사합니다