OpenInfra Days Korea 2018

FreeIPA를 이용한 SSO

1일차 송상준 (LDAP)

FreeIPA & SSO

01 FreeIPA 구성

02 FreeIPA 이용방안

03 Kerberos 활용 SSO

04 Idp를 이용한 SSO

01 FreeIPA 구성

01 FreeIPA

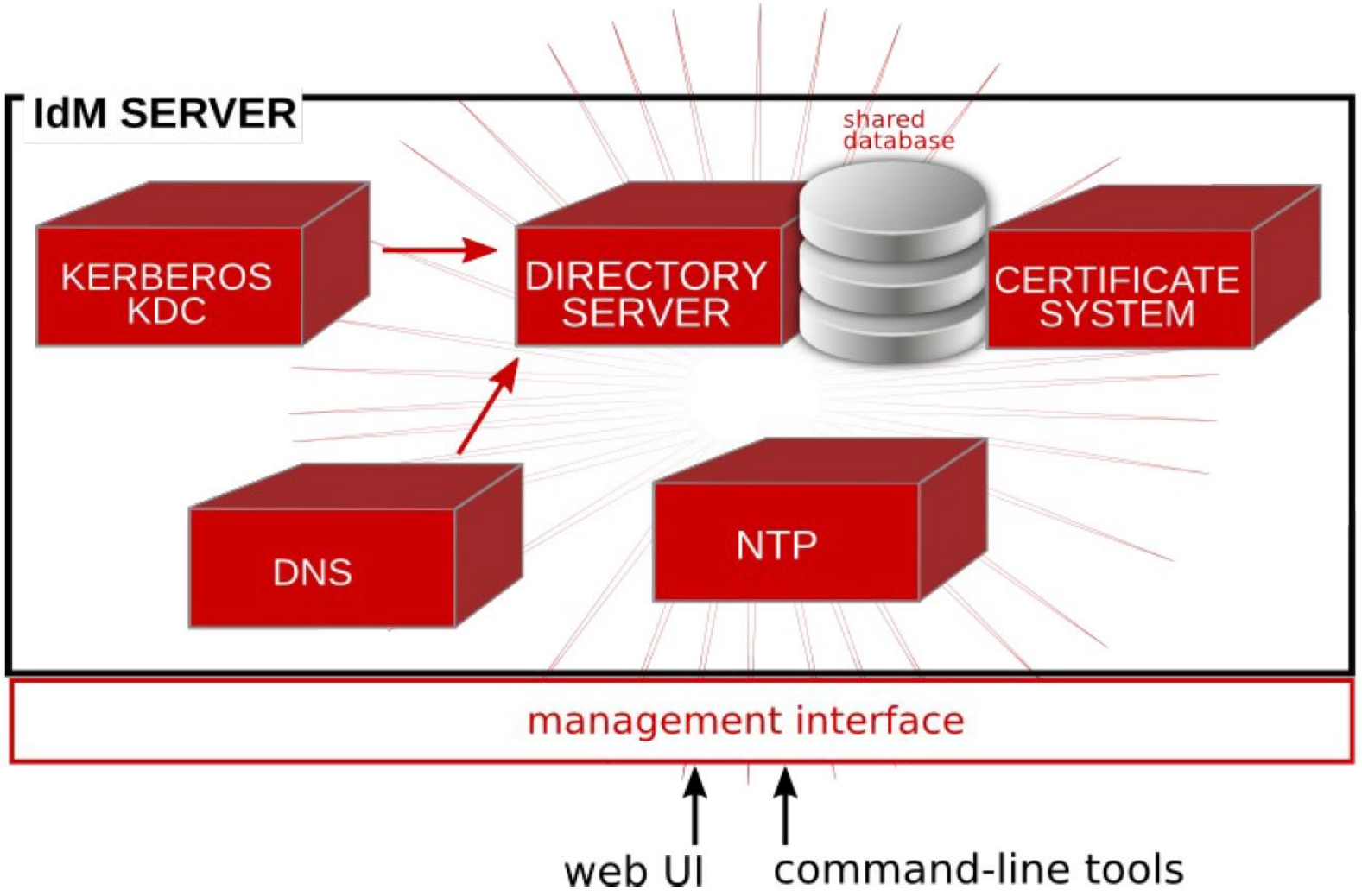
Identity, Policy, Audit

- **Identity** (machine, user, virtual machines, groups, authentication credentials)
- **Policy** (host based access control)
- **Audit** (이 부분은 아직 확정되지 않았음)

http://scribery.github.io/

01 FreeIPA 구성

FreeIPA는 크게 Directory Server, CA Server, Kerberos Server로 구성 됨



01 FreeIPA 구성

389 DIRECTORY SERVER

Directory Server

Kerberos KDC : MIT Kerberos

CA Server : Dogtag Server

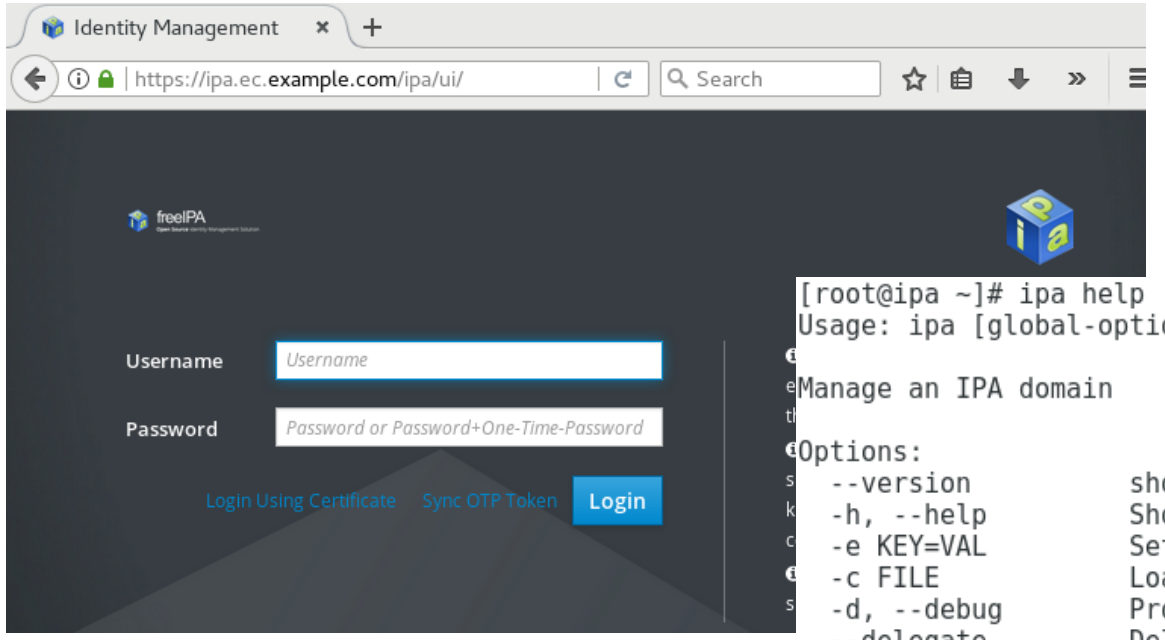
BIND

Berkeley Internet Domain Name

samba

01 FreeIPA 구성

WEB UI, Command Line Tools : IPA

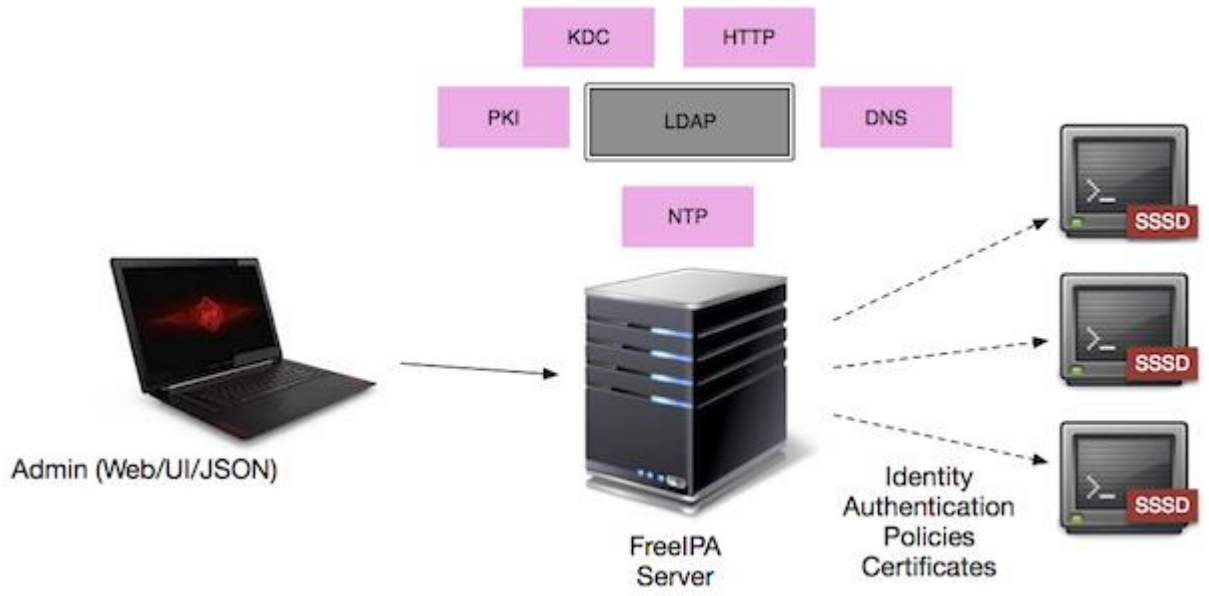



```
[root@ipa ~]# ipa help
Usage: ipa [global-options] COMMAND [command-options]

Manage an IPA domain

Options:
  --version           show program's version number and exit
  -h, --help          Show this help message and exit
  -e KEY=VAL          Set environment variable KEY to VAL
  -c FILE             Load configuration from FILE.
  -d, --debug         Produce full debuging output
  --delegate          Delegate the TGT to the IPA server
  -v, --verbose       Produce more verbose output. A second -v displays the
                      XML-RPC request
  -a, --prompt-all    Prompt for ALL values (even if optional)
  -n, --no-prompt     Prompt for NO values (even if required)
  -f, --no-fallback   Only use the server configured in /etc/ipa/default.conf

See "ipa help topics" for available help topics.
See "ipa help <TOPIC>" for more information on a specific topic.
See "ipa help commands" for the full list of commands.
See "ipa <COMMAND> --help" for more information on a specific command.
```

02 FreeIPA 이용 방안

02 FreeIPA 이용방안

OS 계정 통합



사용용도

1. Linux OS 계정통합

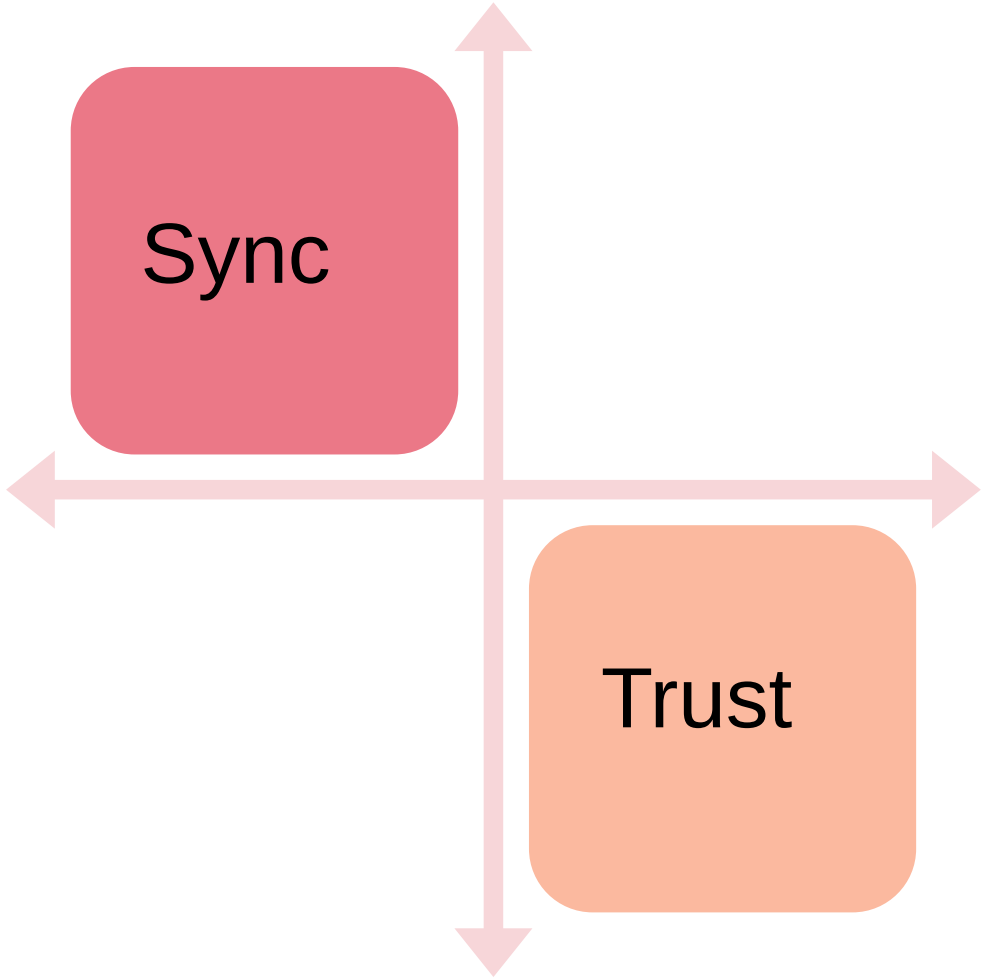
Linux의 OS계정을 통합이 가능하다.
단 ipa client 모듈을 설치해야 됨.

** IPA는 SSSD가 꼭 설치되어야 하므로 Linux OS버전에 따라 사용이 제한 5.x 6.x초반버전은 사용이 안될 수 있음

** ipa client모듈이 설치 없이 쓰기 위해서는 직접 설정을 하면 됨

02 FreeIPA 이용방안

Windows AD 연동 : Sync , Trust



Windows AD 연동

1. Sync
   AD -> IPA (389)
   IPA (389) -> AD

   계정동기화 가능 : AD -> IPA(389)일 경우
   AD DC에 모듈 설치 필요
2. Trust

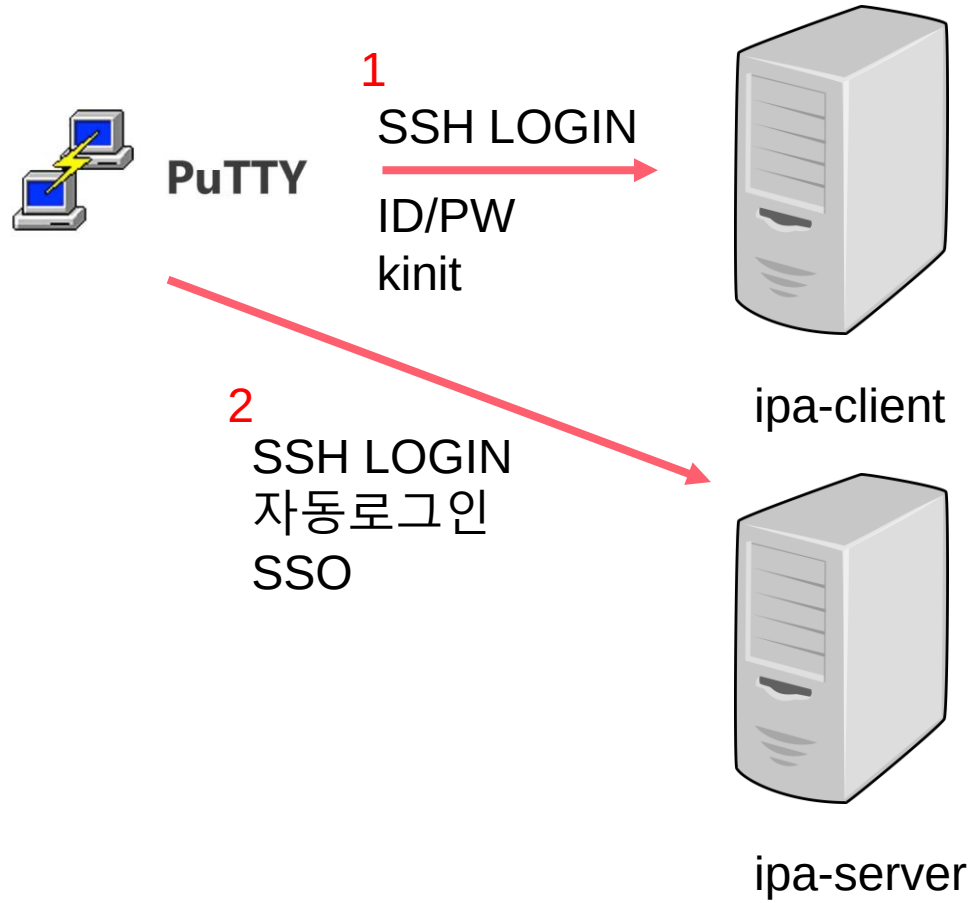
03 FreeIPA SSO

03 System Login SSO

Kerberos 이용한 사용자 로그인

1. ipa-client 로 첫 로그인 시도
   ID/PW로 로그인
   kinit으로 Kerberos 티켓 요청 및 획득
   (이부분을 Script를 통해 자동화 하면 좀 편함)

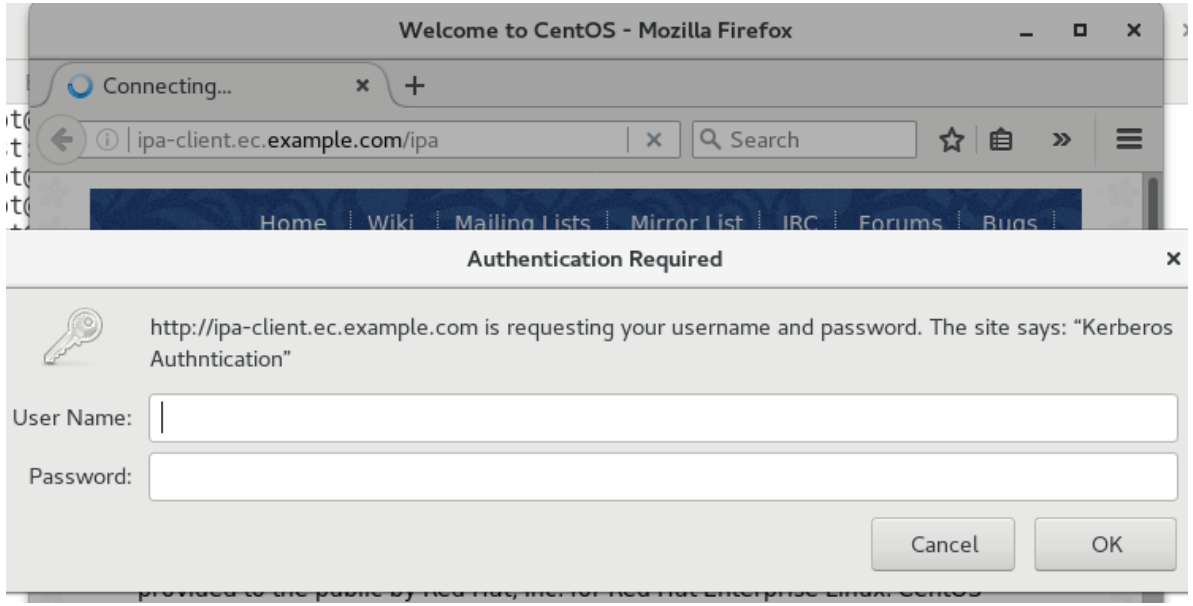
2. ipa-server로 두번째 로그인
   kerberos 티켓을 받은 상황이라 이후 로그인은 자동으로 로그인



03 Kerberos를 이용한 SSO

Apache Web Server SSO

```
[root@ipa-client ~]# klist
klist: Credentials cache keyring 'persistent:0:0' not found
```

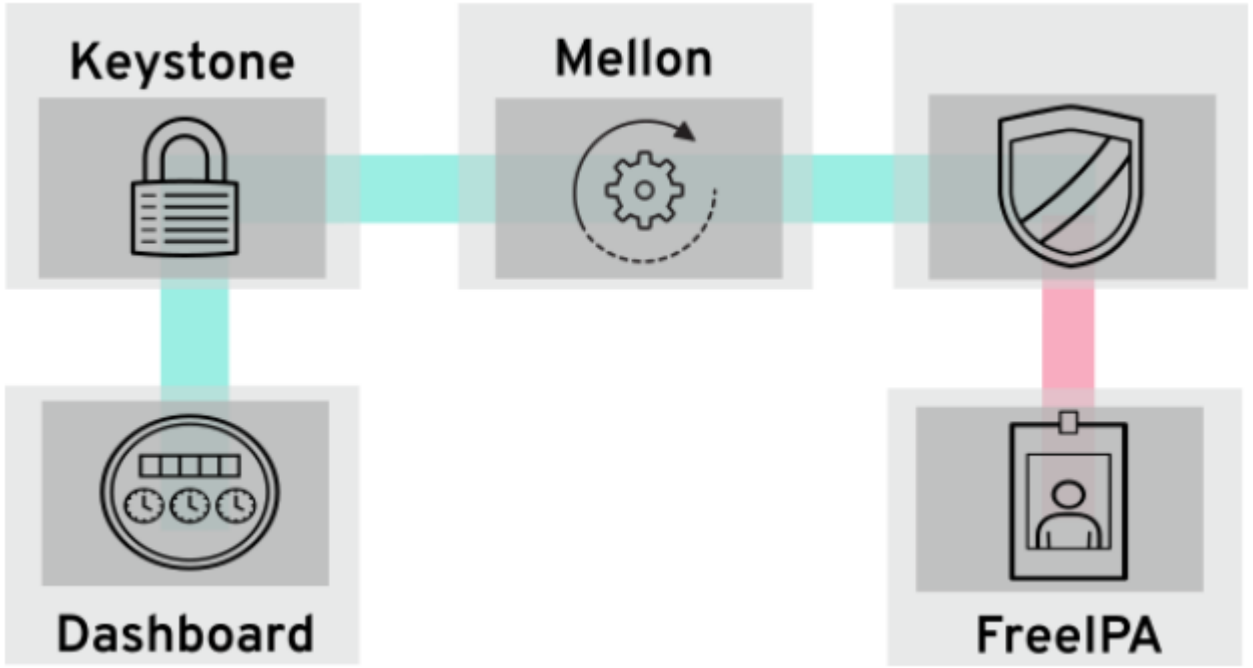


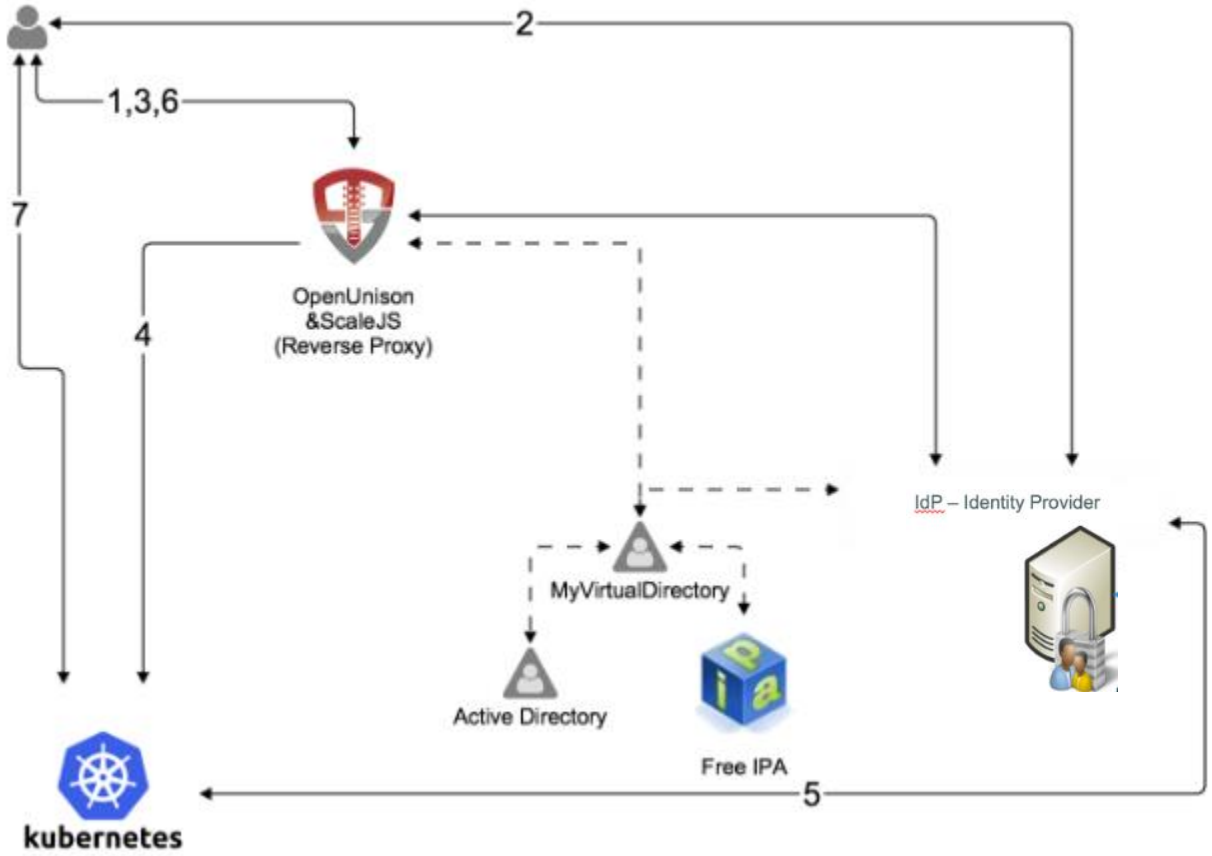

```
[root@ipa-client ~]# kinit sjsong
Password for sjsong@EC.EXAMPLE.COM:
```

04 Idp를 이용한 연동 방안

04 Idp를 이용한 연동 방안

FreeIPA ->Identity Provider(Idp)->Apache(mod_auth_mellon:SAML)





THANK YOU