SEOJIN DSA

오픈 소스(Directory Server(LDAP))를 이용한 Identity관리

Enterprise LDAP Team

2015.10.28.

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

00 목차

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

01 발표자 소개 및 회사 소개

발표자 : 송상준

2000년부터 LDAP 디렉토리서버 구축 및 컨설팅 시작

삼성관련 Project
- 삼성SDS Openstack Project – LDAP구축&컨설팅
- 삼성전자 LDAP 계정통합 – 구축 및 기술지원
- 삼성전자 Mobile 부분 – LDAP관련 교육 지원

OpenLDAP	389 directory server (redhat)	ORACLE	OpenDS	OpenDJ	UnboundID	Apache
OpenLDAP Public License	MPL/LGPL/GPL	Proprietary	CDDL 1.0	CDDL 1.0	Proprietary	Apache License 2.0
C	C	C	Java	Java	Java	Java

열린 with SeojinDSA OpenDJ

ca technologies

hp UX

IBM

CentOS

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

2007년부터 2년마다 개최
- 개최는 대부분 유럽에서 함
- 2015년은 5번째 LDAPCON EDINBURCH에서 개최
- 대부분 오픈소스 디렉토리 관련된 내용

- *DBIS: Directory-Based Information Services* – Mark Bannister
- *Samba4 with OpenLDAP backend* – Nadezhda Ivanova
- *Introducing a Security Access Control Engine that resides in OpenLDAP* – Shawn McKinney
- *The Open Source Identity Ecosystem* – Shawn McKinney
- *The OpenID Connect protocol* – Clément Oudot
- *LDAP Monitoring using open source* – Sangjun Song
- *Complete Open Source IAM Solution* – Radovan Semančik
- *Monitoring OpenLDAP* – Michael Ströder
- *Æ-DIR*: Yet another LDAP user and systems management – Michael Ströder
- *An asynchronous meta backend for OpenLDAP* – Nadezhda Ivanova
- *Improvements of LDAP protocol and transaction protocol* – Christian Hollstein
- *Innovative replication management in FreeIPA* – Ludwig Krispenz, Petr Vobornik
- *WiredTiger Backend for OpenLDAP* – HAMANO Tsukasa
- *2-factor Authentication with OpenLDAP, OATH-HOTP and Yubikey* – Axel Hoffmann

1. (LDAP) Lightweight Directory Access Protocol
2. X.500의 DAP에서 기원
3. TCP/IP 상에서 디렉터리서버에 연결하여 데이터를 저장, 삭제, 수정, 검색을 할 수 있는 Protocol
4. LDAP 모델

Information Model

LDAP: Directory Information Models [RFC4512]
Describes the structure of information (Schema)

Naming Model

LDAP: String Representation of Distinguished Names [RFC4514]
How information is organized and referenced

Functional Model

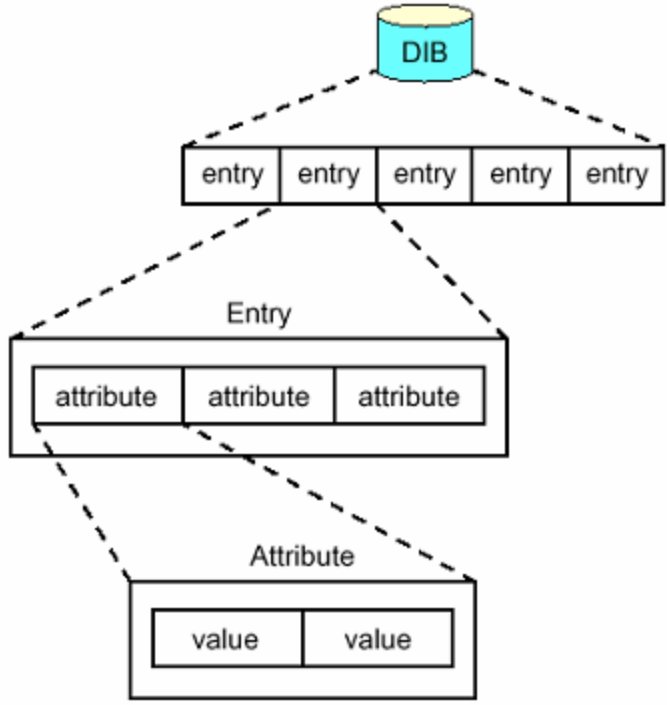
LDAP: Directory Information Models [RFC4512]
What can be done with the information

Security Model

LDAP: Authentication Methods and Security Mechanisms [RFC4513], ACL, PasswordPolicy

Information Model

Describes the structure of information (Schema)
디렉토리 저장소에 데이터를 어떠한 형태로 저장할 것인가를 정의하는 모델이다.



LDAP정보모델은 3가지의 기본 구성요소로 구성되어 있다.

논리적 데이터	물리적 데이터
1) ObjectClass	Entry
2) Attribute	Attribute
3) Syntax	

스키마 구성 순서

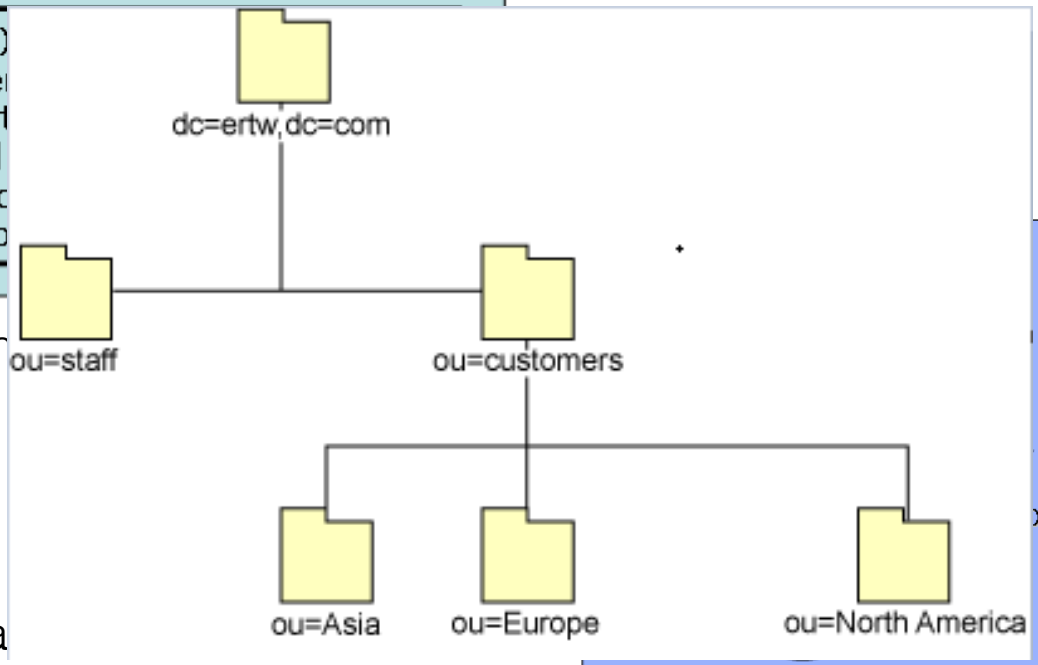
Attribute (Syntax포함) -> Objectclass

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

Object : 직원(employee)
이름(name) : 홍길동 필수
나이(age) : 30

직위(job)
이메일(e
부서(part
부서장이
방번호(ro
층수(floo

Attribute는 **필수 와 옵션으로 구분**
필수 값이 없으면 Entry가 생성되지 않음



Attribute 선언 시 Syn
를 정의해 주어야 함

형식(Type)
단일 값(Single value)
다중 값(Multi value)
ory Attribute)

스키마

옵션속성(Optional Attribute)

OpenLDAP 예제

```
olcObjectClasses: (
  DESC 'RFC2256: a
  SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber
$ seeAlso $ description ) )
```


SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

Naming Model

How information is organized and referenced

RDN (Relative Distinguished Name)

```
dn: uid=hacker,ou=People,dc=my-domain,dc=com
uid: hacker
cn: Sergio
sn: Hacker
objectClass: person
objectClass: top
# objectClass: organizationalRole
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
uidNumber: 1561
gidNumber: 10037
gecos: Undergrad
homeDirectory: /home/hacker
mail: info@matear.eu
telephoneNumber: 402-640-2560
o: UNL-City
ou: Arts & Sciences
l: Comp Sci
shadowLastChange: 14333
shadowMax: 99999
shadowWarning: 7
userPassword: OneTwo2012
```

RDN: 작성 방법
<rdn> :== <rdncomp> | <rdncomp>
<rdn>
<rdncomp> :== <attr> '=' <value>
<attr> :== an LDAP attribute type (cn, dc, …)
<value> :== an LDAP attribute value

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

Functional Model

What can be done with the information

종류	연산자
인증(Authentication)	Open, Bind, Unbind
질의(Interrogation)	Search, Compare
수정(Update)	Add, Delete, Modify, ModifyRDN
기타	Abandon, Extened, Control

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr

엔터프라이즈 레벨의 중앙 집중화된 계정 관리 오픈소스

DESIGNED LINUX 시스템에 특화

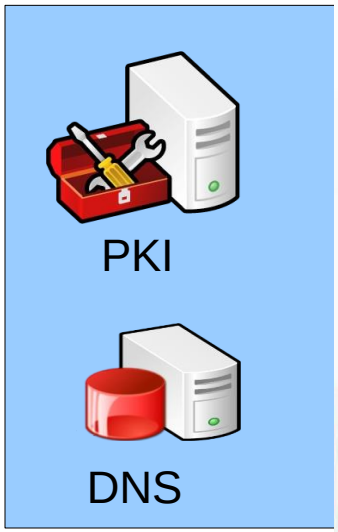
SIMPLE 사용자, 그룹, 시스템, 서비스 관리 SIMPLE

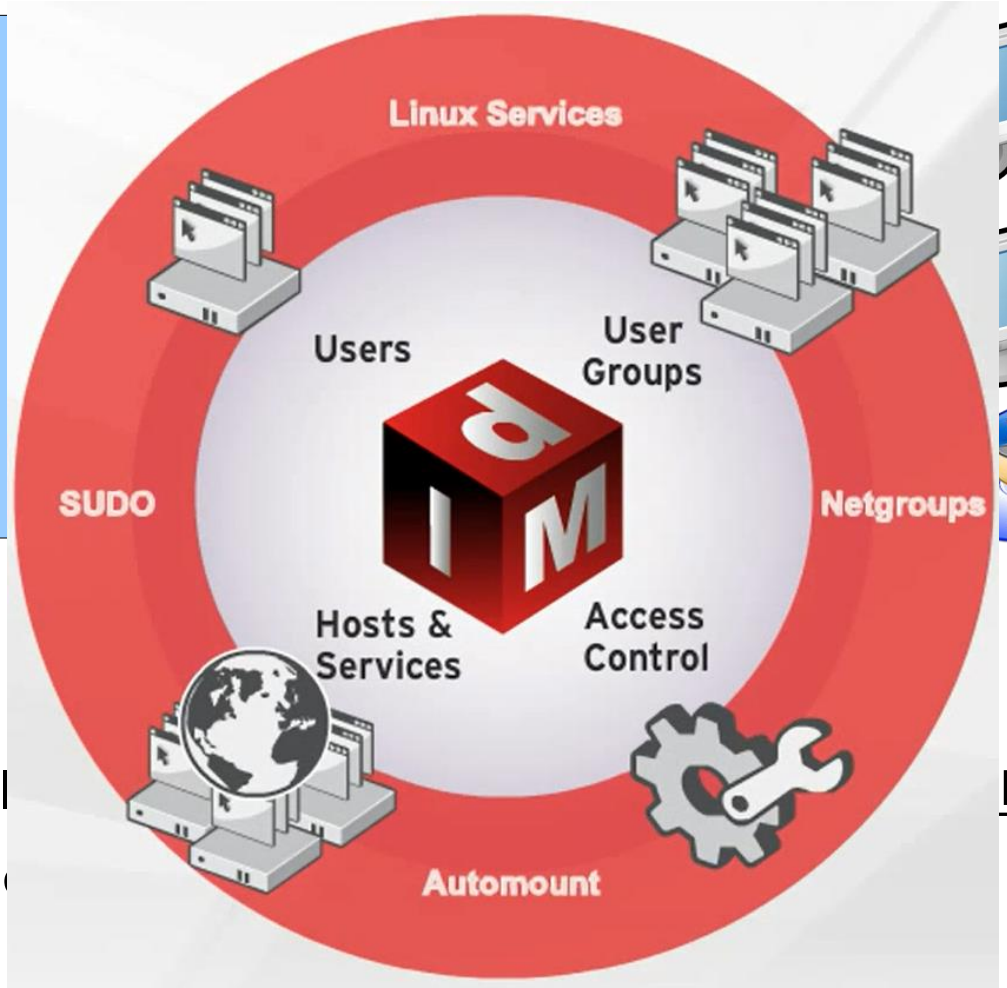
REDUCE 관리작업의 OVERHEAD 감소

STREANLINE 기존 IDM 솔루션의 provisioning의 부하 감소

IMPROVE 보안 부분 기능 향상 (HOST BASE ACCESS)

SEOJIN DSA
2 Floor, 288-25, Sungnae-Dong,Gangdong-Gu Seoul, Korea
T 82 10 9780 6746 | F 82 2 470 7689 | www.seojindsa.kr





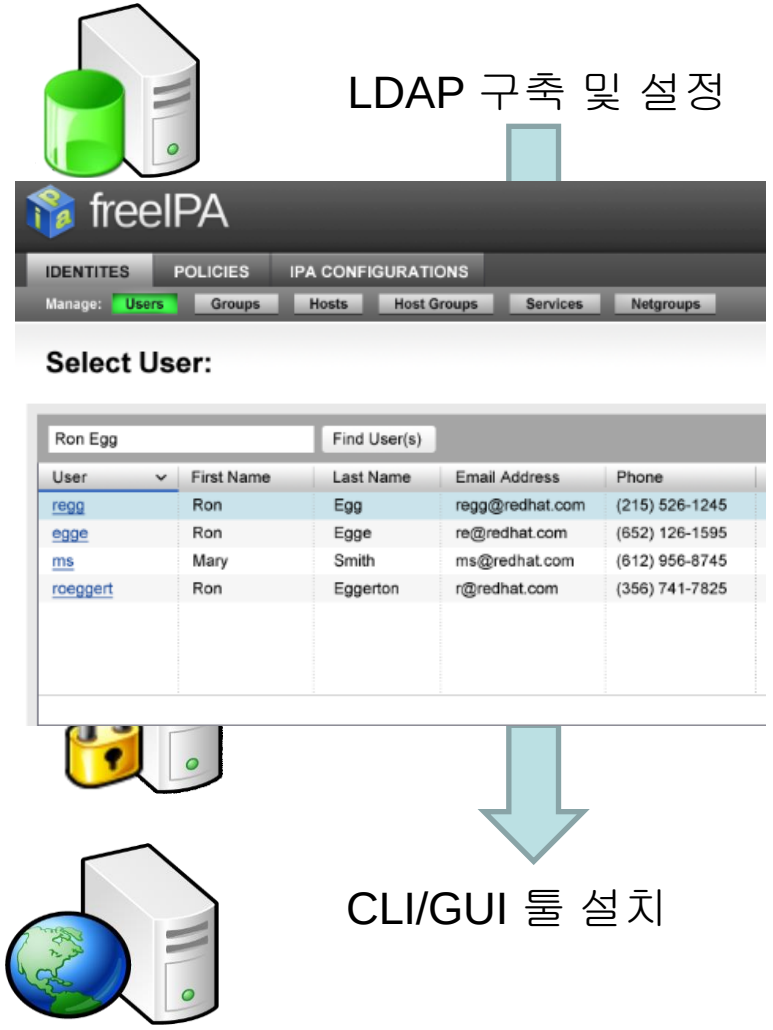
Unix/Linux Clients

Admin

- **Integrated**
- **Standard -**
- **Manageabl** 인터페이스
- **Open -** Fre

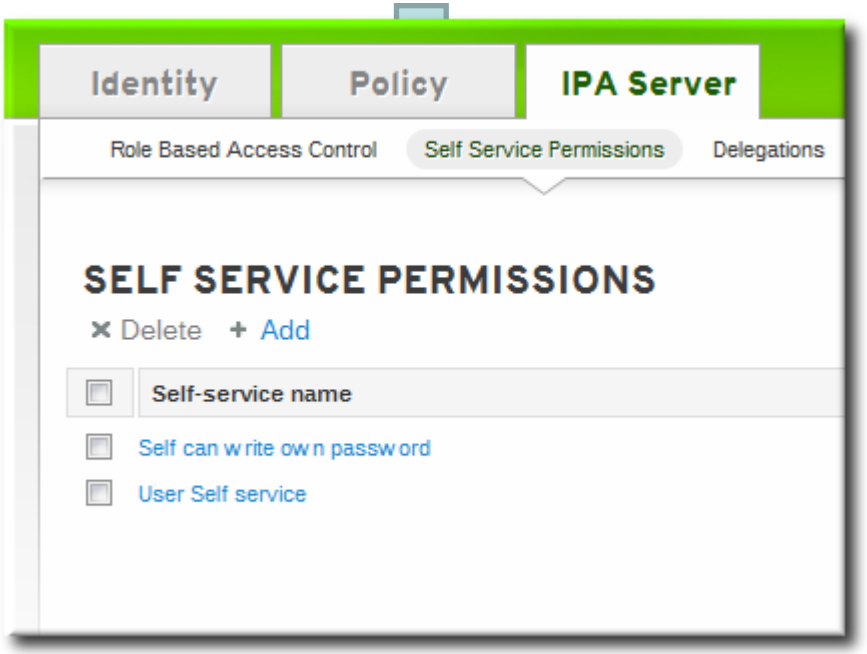
05 LDAP 구축과정 vs FreeIPA 구축과정

일반적인 LDAP 계정관리 구축



FreeIPA 계정관리 구축

yum install freeipa-server




VIEW OUR
DEMO

Windows Client LOGIN

Kerberos LOGIN