MÔ HÌNH THỰC THỂ LDAP

EGOV PLATFORM

TÀI LIỆU KĨ THUẬT

Version 1.0

LỊCH SỬ PHIÊN BẢN

Phiên bản	Ngày phát hành	Mô tả
1.0	08/28/2014	Mô tả sơ lược mô hình thực thể LDAP

GIỚI THIỆU

Đây là tài liệu mô tả mô hình thực thể LDAP được tích hợp đăng nhập 1 lần (SSO) vào hệ thống nền tảng mở openegovplatform. Tài liệu sẽ không đi sâu vào phần tích LDAP mà chỉ nhằm giới thiệu cơ bản về cấu trúc và chỉ mục được sử dụng trong nền tảng này. Để tìm hiểu kĩ hơn các bạn có thể tìm tài liệu chuyên sâu về LDAP.

Tài liệu sẽ gồm 2 phần cơ bản: 1 phần là mô hình cây thực thể và 2 là phần giải thích các thuộc tính được sử dụng trong nền tảng mở openegovplatform.

MỤC LỤC

Thuật ngữ viết tắt

SSO	Single Sign On
LDAP	Lightweight Directory Access Protocol
DN	Distinguished Name
DC	Domain Component
OU	Organization Unit
CN	Common Name
Mail	E-mail address
SN	Surname
UID	User Identification

1. Giới thiệu LDAP

Thư mục LDAP là một tập hợp dữ liệu về người dùng hay nhóm người dùng. LDAP (Lightweight Directory Access Protocol) là giao thức internet mà qua đó các ứng dụng web có thể sử dụng để truy cập và tìm kiếm thông tin người dùng hay nhóm người dùng từ máy chủ LDAP.

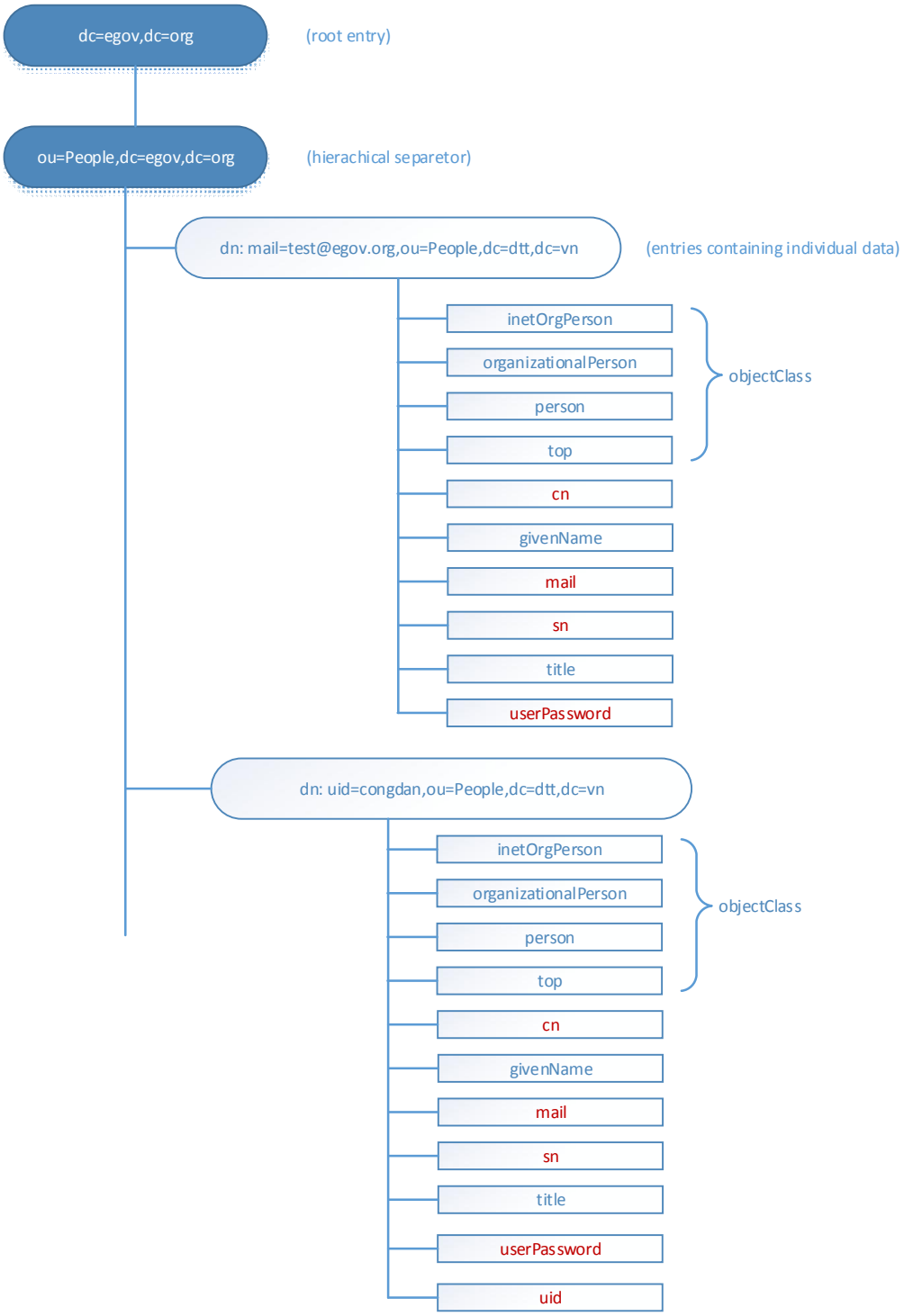
Máy chủ LDAP hiện có rất nhiều loại phổ biến như sau:

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- OpenLDAP Using Posix Schema
- Posix Schema for LDAP
- Sun Directory Server Enterprise Edition (DSEE)
- A generic LDAP directory server.

Trong nền tảng nguồn mở, chúng tôi sử dụng hệ thống OpenLDAP server cho hệ thống openegovplatform. Để tìm hiểu chi tiết, các bạn có thể vào trang web: www.openldap.org

2. Mô hình thực thể

Mô hình thực thể tổng quan về LDAP



Mô hình 1: Mô hình cây LDAP

Đây là thực thể của LDAP gồm các thuộc tính cơ bản cần có trong LDAP để hệ thống openegovplatform sử dụng để SSO qua các ứng dụng hay các hệ thống khác nhau sử dụng nền tảng này.

2.1 Thư mục gốc

Đây là thư mục gốc của một cấu trúc thư mục cây của LDAP cũng là nơi khởi nguồn hay bắt đầu của việc rẽ nhánh cây thực mục. Nhánh này có thể là quốc gia(country) hay tên miền cần định danh.

2.2 Thư mục rẽ nhánh cấp tổ chức

Đây là nơi định nghĩa tổ chức, đơn vị của tổ chức, phòng ban, nhóm người dùng.

2.3 Thực thể của LDAP

Đây là nơi lưu trữ thông tin cá nhân người dùng gồm các thuộc tính như email, tên, tuổi, mô tả,...

2.3.1 DN (Distinguished Name) với mail làm thuộc tính chính

Tên định danh duy nhất để phân biệt trong thực thể LDAP và không trùng với bất cứ DN nào. Trong DN này có một số thuộc tính cơ bản và một số thuộc tính bôi đỏ là không được phép để trống trong hệ thống nền tảng mở openegovplatform. Trong phần DN này ta lấy DN với thuộc tính `mail` làm khai báo trong hệ thống LDAP.

Ví dụ:

```
dn: mail=test@egov.org,ou=People,dc=egov,dc=org
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Test Test
givenName: Test
mail: test@egov.org
sn: Test
title: test
userPassword:: YWJjQDEyMw==
```

Diễn giải ví dụ trên như sau: DN lấy `mail`làm tính năng duy nhất để phân biệt, trong đó có thuộc tính cơ bản của người dùng là các `objectClass`để khai báo. Bên cạnh đó hệ thống có các thuộc tính ràng buộc là `cn`, `sn`, `mail`, `userPassword`vàthuộc tính bổ sunglà `givenName, title.`

2.3.2 DN (Distinguished Name) với uid làm thuộc tính chính

Khác với phần định danh ở trên là lấy thuộc tính `mail` làm định danh thì ta có thể lấy thêm thuộc tính là `uid` làm định danh. Tất nhiên định danh uid này là duy nhất và không bị trùng lặp trong `ou` của cây thư mục thực thể phụ thuộc.

Ví dụ:

```
dn: uid=congdan,ou=People,dc=egov,dc=org
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
cn:congdan
givenName:: WSB04bq/
mail: congdan@egov.org
sn: congdan
title:: UXXhuqNuIHRy4buLIGjhu4cgdGjhu5FuZw==
uid: congdan
userPassword:: NDMyMQ==
```

Diễn giải ví dụ trên như sau: DN lấy `uid`làm tính năng duy nhất để phân biệt, trong đó có thuộc tính cơ bản của người dùng là các `objectClass`để khai báo. Bên cạnh đó hệ thống có các thuộc tínhràng buộc là `uid`, `cn`, `sn`, `mail`, `userPassword`vàcác thuộc tínhbổ sung là `givenName`, `title`.

2.3.3 Kết luận

Trong nền tảng mở openegovplatform ta có thể sử dụng song song cả hai DN trên cho khả chuyển mà không bị bó buộc. Ta có thể thấy nó khác với một số hệ thống LDAP thương mại khác. Tùy các hệ thống khác nhau hỗ trợ giao thức LDAP là ta có thể tích hợp được với nền tảng này.