Active Directory

活動目錄 AD & 羽量級 LDAP

Table of Contents

What is AD, Active Directory?

It is originated from DS, Directory Service, an organized and ACL-functional system with storage.

One directory maps itself to key/val pair, maybe the name and attribute.

And this system is aim at providing service to File System.

DS (Directory Service) Schema applies everywhere

Below Phone Directory, DNS, FS, and so on are Object, and the info about the Object is stored as Attribute. User with certificates will be allowed to access to the Object and to r/w the Attribute.

If we want to design a complicate directory service, the info (or called attributes hereby) may include: UserID, SSL certificate, Devices, Apps Config, those authority is setup to access the Object to R/W its Info.

Phone Directory: Name, mobile phone number

DNS: domain name, IP address

OS: printer, users accounts whitelist

FS: directory node name, child node (can be sub-directory or files)

How to create AD?

To create AD using ADSI, Active Directory Service Interface. Developer can create AD by connecting & accessing ADSI, we can think this interface is a DB, it has schema, and can execute CRUD operations.

By using freeware LDAP client tool software to create LDAP:

OpenDJ (cross-platform)

Active Directory Explorer (micosoft)

LDAP Admin(micosoft)

NetTools(micosoft)

OpenLDAP (cross-platform)

Apache Directory Server/Studio(cross-platform)

Links: https://en.wikipedia.org/wiki/List_of_LDAP_software

LDAP Client

384/TCP,UDP	一個遠端網路伺服器系統	官方
387/TCP,UDP	AURP, AppleTalk 升級用路由協定	官方
389/TCP,UDP	輕型目錄存取協定 LDAP	官方
401/TCP,UDP	不間斷電源，不間斷電源供應系統	官方
411/TCP	Direct Connect Hub 埠	非官方
412/TCP	Direct Connect 用戶端—用戶端 埠	非官方

LDAP Node.js

> Search users on OpenLDAP server using ldapjs and express.

Working with LDAP on dev environment isn't an easy thing, and especially when it comes to configuring an OpenLDAP only for development. So this project contains a simple implementation for users search feature from LDAP, and a docker environment for development based only on docker-compose, so there's no docker file.

The docker-compose has two services:

- dev: lunches the express application using nodemon by running the script `dev` into package.js.
- ldap: starts the OpenLdap server, adds the groups and users from `./ldif/directory.ldif`.

Both services working on the same network `ldap` network. So the ldapjs client on `dev` has access to ldap through this config:

```
const client = ldap.createClient({
  url: "ldap://ldap:389"
});
```

Starting the dev environment

To make thing more pleasant, I created a make file, so need to remember all docker commands to start your project. first of all, you necessitate to install the dependencies and start the dev server via docker-compose up, by typing:

```
make install
make dev
```

Hola! now you can request the user's search thought out the Rest API, via:

OpenDJ

.ldif (LDAP filename extension)

The **LDAP Data Interchange Format** (**LDIF**) is a standard plain text data interchange format for representing LDAP (Lightweight Directory Access Protocol) directory content and update requests.

LDIF conveys directory content as a set of records, one record for each object (or entry). It also represents update requests, such as (CRUD) Add, Modify, Delete, and Rename, as a set of records, one record for each update request.

LDAP, Lightweight Directory Access Protocol

Key is entry, value is attribute, it consists of a k/v pair as one schema.

Apple Open Directory (using LDAP)

Apple Open Directory is a fork of OpenLDAP.

A lightweight DS software that store info about user and resource (ACL).

p.s.

With the release of osX 10.5, Apple chose to move away from using the Netinfo directory service which had been used by default for all local accounts and groups in every release of osX 10.0 ~ 10.4. Mac OS X 10.5.

Local accounts are now registered in the Local Plugin, which uses XML property list (plist) files stored in /var/db/dslocal/nodes/Default/ as its backing storage.

Features in DS

IAM

Cerificate

Difference between Duplica & Deployment

Duplica

For LB-purposed.

Deploy

For Decentralized-purposed.

Other Applications

SAP solution Manager

IBM Tivoli Directory Server

Apple Open Directory (macOS)

Apache Directory Server