LDAP (轻量级目录访问协议) 介绍

王旭

Wireless Tech Innovation (WTI) Institute,
Beijing University of Posts and Telecommunications (BUPT)

Slides are manipulated by LaTeX 2ε & Beamer.

大纲

1. LDAP 简介
2. LDAP 的用途
3. LDAP 相关概念
4. LDAP 的使用

LDAP 的历史云云

- 起源于 X.500 目录
- 由 University of Michigan 开发, 被 IETF 接纳为标准
- LDAP 是一个轻量级的目录访问协议
  - 一个访问目录的网络协议，而不是数据库/目录
  - 用于访问 X.500 目录
  - 简单直接的操作，去除了不常用的功能
  - ASN.1
- LDAP 拥有很多大公司的产品的支持，当然，也不乏开源的支持。

LDAP 与数据库

LDAP 是一种网络协议而不是数据库，而且...

- LDAP 的目录不是关系型的，没有 RDBMS 那么复杂
- LDAP 不支持数据库的 Transaction 机制，纯粹的无状态、请求-响应的工作模式
- LDAP 不能存储 BLOB
- LDAP 的读写操作是非对称的，读非常方便，写比较麻烦
- LDAP 支持复杂的查询过滤器 (filter)，可以完成很多类似数据库的查询功能
- LDAP 使用树状结构，接近于公司组织结构、文件目录结构、域名结构等我们耳熟能详的东东
- LDAP 使用简单、接口标准，并支持 SSL 访问

LDAP 与 NIS

回顾一下，啥叫 NIS

就是 Yellow Page, SUN 最早开发出来的东西，UNIX 普遍支持，用于在一群 UNIX主机之间共享配置信息。

和 NIS 相比，LDAP...

- LDAP 是标准的、跨平台的，在 Windows 下也能支持
- LDAP 支持非匿名的访问，而且有比较复杂的访问控制机制 (如 ACL)，安全性似乎更好一些
- LDAP 支持很多复杂的查询方式
- LDAP 的用途较 NIS 更为广泛，各种服务都可以和 LDAP 挂钩

各种 LDAP 的用途

网络服务

- DNS 服务

认证服务

- Linux PAM (ssh, login, cvs...)
- Apache 访问控制
- 各种服务登录 (ftpd, php based, perl based, python based...)

其它服务

- 个人信息类，如地址簿
- 服务器信息，如帐号管理、邮件服务等

LDAP 相关产品

主要的 LDAP 服务器

- OpenLDAP: http://www.openldap.org
- Microsoft Active Directory
- Netscape LDAP SDK

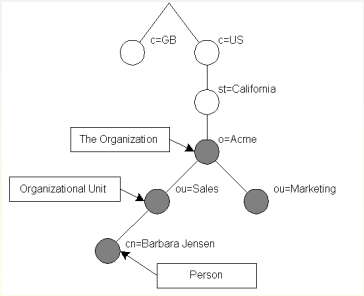
常见的利用 LDAP 的服务器

- WWW: Apache authnz-ldap (For apache 2.2), ldap-userdir
- FTP: Proftpd-ldap, Pure-ftpd-ldap
- Mail: Postfix, Qmail, Courier

LDAP 的树状目录

下图是一个典型的 LDAP 目录

- 这是一个树状结构
- 没有根节点
- 每个节点都是一个目录项，不论是否是叶子节点
- 每个节点的的名字 (DN)，都表明了它在树上的位置 (从根出发)



ObjectClass, Attribute 与 Schema

如何描述一个节点

- 一个节点属于某个 ObjectClass:
  - 表征一个节点所属的类型
  - 一个节点可能同时是多个 ObjectClass
- 一种 ObjectClass 的节点具有一系列的 Attribute:
  - Attribute 是一些属性，这些属性的对应值表征了每个对象的与众不同之处
  - ObjectClass 之中，有些属性是必须的，有些则不是
- ObjectClass 和 Attribute 由一些 Schema 文件来规定
  - Schema 文件使用 ASN.1 描述
  - Schema 文件规范 ObjectClass 的构成、继承关系，Attribute 的格式等

LDAP URL

```
ldap://host:port/basedn?attribute?scope?filter
```

各个字段的含义:

- host, port: 这两个不用解释了
- basedn, 选择了哪个树枝，比如
  dn: uid=wangxu,ou=users,ou=stl,o=cg.com.cn
- attribute: 要提取哪个字段，比如，认证的时候一般是 uid
- scope: one or subtree
- 这个是复合搜索字符串，用以筛选搜索结果
- 上述四个，不都是必须的，看情况选择

LDAP 搜索过滤

- Filter 极大扩展了 LDAP 使用的灵活性和便利性，可以用来过滤 LDAP 搜索结果的节点的各个属性
- Filter 应该放在圆括号里面
- Filter 用目录中节点的属性来进行过滤，如

```
(objectClass=posixAccount)
(sn=w*)
```

- 可以同时使用多个过滤条件，进行一些逻辑运算，这就需要用前缀表达式了:

```
(&(objectClass=posixAccount)(sn=w*))
(|(sn=w*)(sn=l*))
```

LDAP 数据交换格式: LDIF

LDAP 的数据交换都是使用这种文本格式的

- 下面这个是我的真实情况的案例:

```
dn: uid=wangxu,ou=user,ou=stl,dc=cg,dc=com,dc=cn
uid: wangxu
cn: Wang Xu
sn: Wang
mail: wangxu@cg.com.cn
accountStatus: active
mailMessageStore: /var/mail/wangxu/
uidNumber: 1101
gidNumber: 1101
homeDirectory: /home/lusers/wangxu
loginShell: /bin/bash
objectClass: organizationalPerson
objectClass: person
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: qmailUser
objectClass: top
```

OpenLDAP 服务器

服务器工具

- 服务器守护程序: slapd (stand-alone ldap daemon)
- 服务器配置文件: /etc/ldap/slapd.conf
- 存放 schema 的位置: /etc/ldap/schema
- 常用维护工具: slapcat, slapadd, slapindex
  - 需要停下服务器才能使用
  - 必须在服务器本机运行
  - slapcat 可以用来备份
  - slapadd 和 slapindex 可以用来初始化或恢复 LDAP 目录
  - 还有一些其他的工具，都是 slap 开头的
- 多服务器协同工具: slurpd

LDAP 命令行工具

LDAP-UTILS 的使用

- 配置 /etc/ldap/ldap.conf 指定 LDAP 服务器
- ldapsearch 是最常用的工具了，如

```
gnawux@spirit:~$ ldapsearch -x uid=wangxu|grep
"sn"
sn:  Wang
```

- ldapadd, ldapmodify 可以用来添加、修改目录项，使用的信息格式就是 LDIF
- ldapdelete 可以用来删除目录项
- 上面这些修改目录的命令一般都需要通过认证

使用 LDAP 控制各种登录

- 前提一: 系统使用 PAM 并且安装了 libpam-ldap
- 前提二: 用户信息在 LDAP 里面以 posixAccount 类型存储
- 首先配置 /etc/pam_ldap.conf 和 pam_ldap.secret
- PAM 的配置文件位于 /etc/pam.d/ 目录下，修改相应程序的登录设置，如，鉴权:

```
auth sufficient pam_unix.so nullok_secure
auth sufficient pam_ldap.so
```

  这样，本机或 LDAP 帐户都能通过鉴权了，同理，还要修改 account, password 和 session 部分。
- 如果涉及本机登录，要修改 /etc/nssswitch.conf 的内容:

```
passwd:  files ldap
group:  files ldap
shadow:  files ldap
```

  并重启 nscd

Apache2.2 使用 LDAP 进行访问控制

这是一个例子:

```
AuthName "Test Authentiaction with authnz_ldap"
AuthType Basic
AuthBasicProvider ldap
AuthLDAPURL ldap://127.0.0.1/dc=cg,dc=com,dc=cn

require ldap-user wangxu liyinong tangxiaosheng
```

- 当然，这需要先启用 Authnz_ldap 模块
- 除了上面的一种授权方式之外，还可以通过 require ldap-group, require valid-user 或 require ldap-filter 授权

谢 谢！

2007年3月