LDAP

可以通过以下三句话快速的认识一下LDAP：

1. LDAP：Lightweight Directory Access Protocol，轻量目录访问协议。
2. LDAP服务是一个为只读（查询，浏览，搜索）访问而优化的非关系型数据库，呈树状结构组织数据。
3. LDAP主要用作用户信息查询（如邮箱，电话等）或对各种服务访问做后台认证以及用户数据权限管控。

LDAP的定位

使用LDAP类似于人们使用图书馆卡或电话簿的方式。当任务需要“一次写入/更新，多次读取/查询”时，可以考虑使用LDAP。LDAP旨在为大规模数据集提供极快的读取/查询性能。每个条目(Entry)只存储一小部分信息。与读取/查询相比，添加/删除/更新性能相对较慢，因为假设不经常进行“更新”。

如果只使用数据库，当大量请求需要用户验证，数据库的性能会成为瓶颈。

LDAP是数据库之外的另一个优化层，用于提高性能，而不是替换数据库。

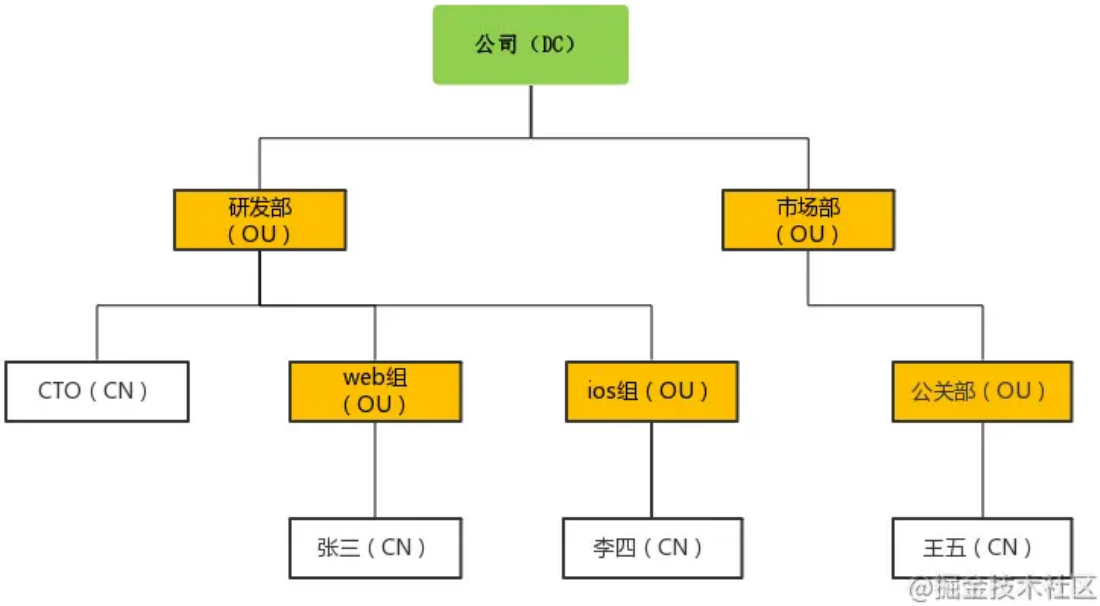
LDAP不仅用于用户验证，任何具有一下属性的任务对于LDAP都是一个很好的用例：

1. 需要频繁并快速地定位一个数据。
2. 不在乎不同数据之间的逻辑和关系。
3. 不会经常更新，添加或删除数据。
4. 每个数据条目很小。
5. 不介意将所有的条目放在一个集中的位置。

名词解释

- DC：domain component 一般为公司名，例如：dc=163，dc=com
- OU：organization unit 为组织单元，最多可以有四级，每级最长32个字符，可以为中文
- CN：common name 为用户名或者服务器名，最长可以到80个字符，可以为中文
- DN：distinguished name 为一条LDAP记录项的名字，有唯一性，例如：dn:"cn=admin,ou=developer,dc=163,dc=com"

组织架构



OpenLDAP

上边介绍了LDAP只是一个协议，基于这个协议实现服务器端程序有OpenLDAP、Active Directory(微软的域控制器)等等

部署OpenLDAP

部署环境：Debian 8.4

1.安装OpenLDAP,OpenLDAP服务端程序叫slapd

```
# apt-get install -y slapd
```

2.安装完成之后，会自动生成一个OpenLDAP的系统账号

```
# cat /etc/passwd
openldap:x:110:115:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
```

3.生成OpenLDAP管理员账号的密码（后边修改配置文件需要使用）

```
# slappasswd
New password:
Re-enter new password:
{SSHA}TpWoSebaT5gKy2Y3EHmZh+WcOhJaFp7y
```

4.新建OpenLDAP配置文件

```
# cp /usr/share/slapd/slapd.conf /etc/ldap/
# 配置文件中有很多@xxx@的配置替换为真实配置

# slaptest -f /etc/ldap/slapd.conf
5ad9b19d /etc/ldap/slapd.conf: line 105: rootdn is always granted unlimited
privileges.
5ad9b19d /etc/ldap/slapd.conf: line 122: rootdn is always granted unlimited
privileges.
config file testing succeeded
```

配置文件重要参数说明（需要自己修改的，其他未提到的可以不修改）：

- `database bdb`：定义使用的后端数据存储格式，数据库默认采用了berkeley db，其后可以跟的值有bdb、ldbm、passwd、shell。bdb指使用Berkley DB 4数据库
- `suffix "dc=163,dc=com"`：suffix是"LDAP基准名"，它是LDAP名字空间在这里的根。设置想要创建的子树的根DN
- `rootdn "cn=admin,dc=163,dc=com"`：设置管理LDAP目录的超级用户的DN。这个用户名不要出现在/etc/passwd文件里
- `rootpw {SSHA}TpWoSebaT5gKy2Y3EHmZh+WcOhJaFp7y`：设置这个数据库的超级用户的口令验证方式。也就是上边rootdn设置的用户的密码。一定要用加密的口令存储，可以使用的加密方式有：CRYPT、MD5、SMD5、SHA和SSHA，**就是我们第三部生成的密码**
- `directory /var/lib/ldap`：设置LDAP数据库和索引文件所在的目录
- `access to`：权限配置下边详细说明

5.删除原配置，生成新配置

```
# rm -rf /etc/ldap/slapd.d/*
# slaptest -f /etc/ldap/slapd.conf -F /etc/ldap/slapd.d/

# 给新生成的配置文件赋予openldap的权限
# chown -R openldap.openldap /etc/ldap/slapd.d/
```

6.重启openldap

```
# /etc/init.d/slapd restart
```

ACL权限控制

ACL访问指令的格式：

```
access to [what]
    by [who] [control]
```

简单解释：通过access to约束我们访问的范围（what），通过by设定哪个用户（who）有什么权限（control）

ACL的详细配置还是比较复杂的，可以看下下边参考文档的第三篇，写的比较详细，这里都不再赘述。

线上ACL控制配置解析

为了用户能够自主修改密码，部署了lam给用户使用（见下文lam介绍）。希望能达到的效果是：

1. 管理员能够有全部权限，包含新建用户，修改用户属性，充值用户密码等
2. 普通用户只能修改自己的密码，别的权限都没有

配置如下：

```
# access to attrs=userPassword通过属性找到访问范围密码，
# 超级管理员也就是我们ldap配置文件里写的rootdn："cn=admin,dc=163,dc=com"有写(write)权限；
# 由于管理员可能不止一个，我创建了个管理员组"ou=Admin,dc=163,dc=com"把管理员统一都放到这个组下，管理员组下的所有用户（dn.children）有写权限；
# 匿名用户(anonymous)要通过验证(auth)；
# 自己(self)有对自己密码的写（write）权限，其他人(*)都没有权限(none).
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=163,dc=com" write
        by dn.children="ou=Admin,dc=163,dc=com" write
        by anonymous auth
        by self write
        by * none

# access to * 所有其他属性，
# 超级管理员rootdn："cn=admin,dc=163,dc=com"有写(write)权限；
# 管理员"ou=Admin,dc=163,dc=com"成员有写(write)权限；
# 其他人(*)只有读(read)权限
access to *
        by dn="cn=admin,dc=163,dc=com" write
        by dn.children="ou=Admin,dc=163,dc=com" write
        by * read
```

备份和还原

备份

```
# ldapsearch -x -b "dc=163,dc=com" -D "uid=authz,ou=Public,dc=163,dc=com" -w "AzdfD863M4" > ldap.20180626.ldif
```

参数说明：

- `-x`：进行简单的验证
- `-D`：用来绑定服务器的DN
- `-w`：绑定DN的密码
- `-b`：要查询的根节点 authz账号要有`"dc=163,dc=com"`的查询权限

还原

```
# ldapadd -x -c -D "cn=admin,dc=163,dc=com" -w "smile" -f ldap.20180626.ldif
```

参数说明：

- `-c`：出错后继续执行程序不终止，默认出错即停止
- `-f`：从文件内读取信息还原，而不是标准输入 还原的DN最好为管理员账号，至少也要有要LDAP的写入权限

web管理工具

用了phpldapadmin和ldap-account-management(简称lam)两款web管理工具，强烈推荐lam，所以这里就不介绍其他的了

ldap-account-manager

安装

1.安装ldap-account-management

```
# apt-get install ldap-account-manager
```

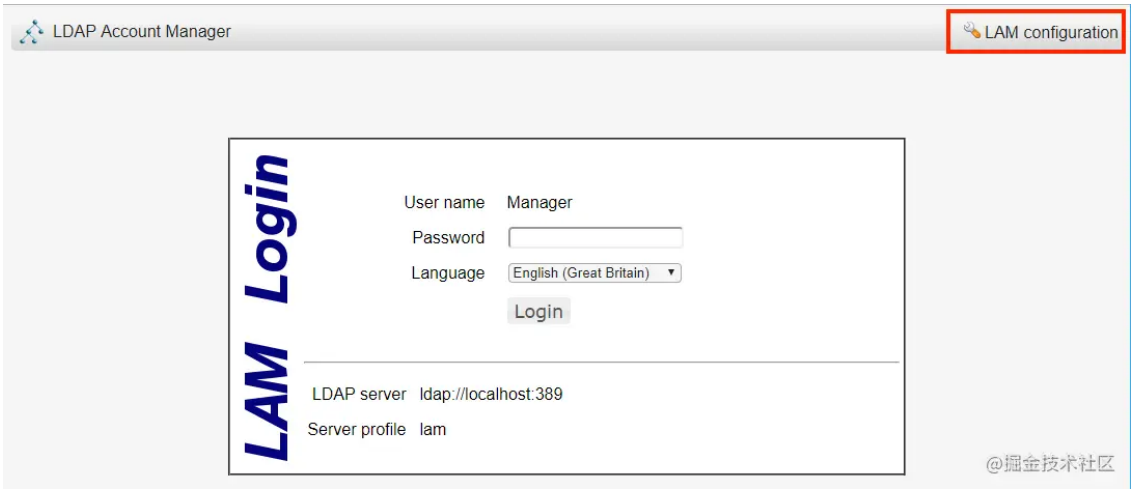
2.浏览器访问

```
http://ip/lam
```

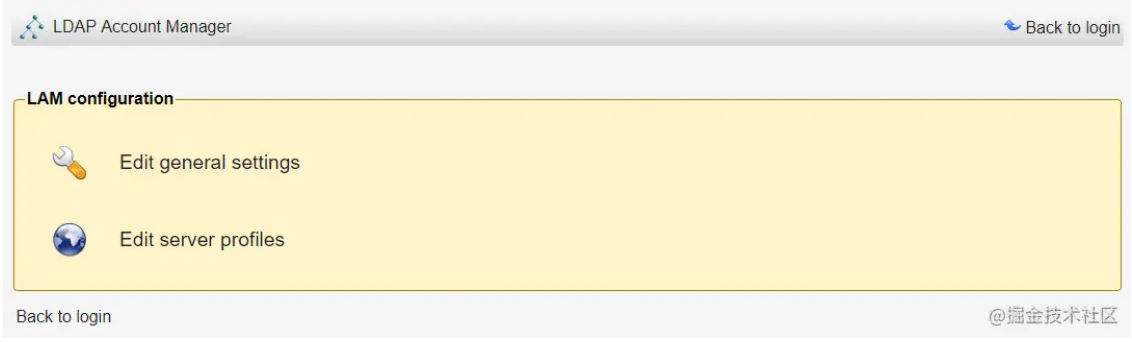
配置

lam的所有配置都可以在web端配置，不需要去服务器上修改一行代码，这个太好用了。

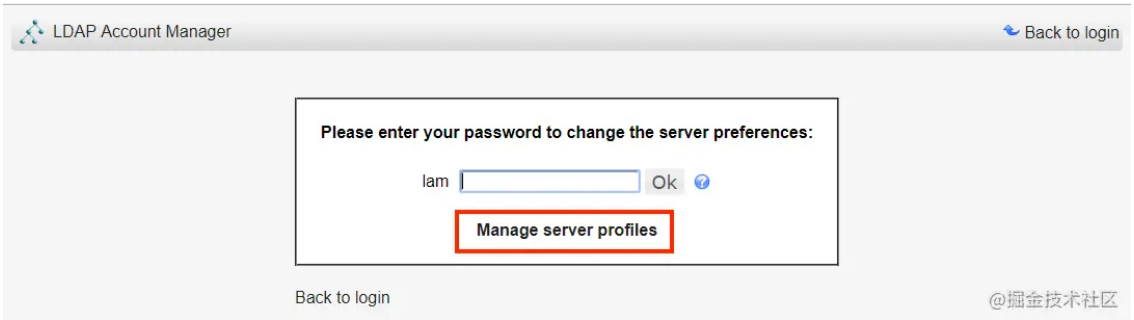
1. 浏览器访问后进入登录页面，我们点击右上角"LAM configuratrion"来在线编辑配置文件



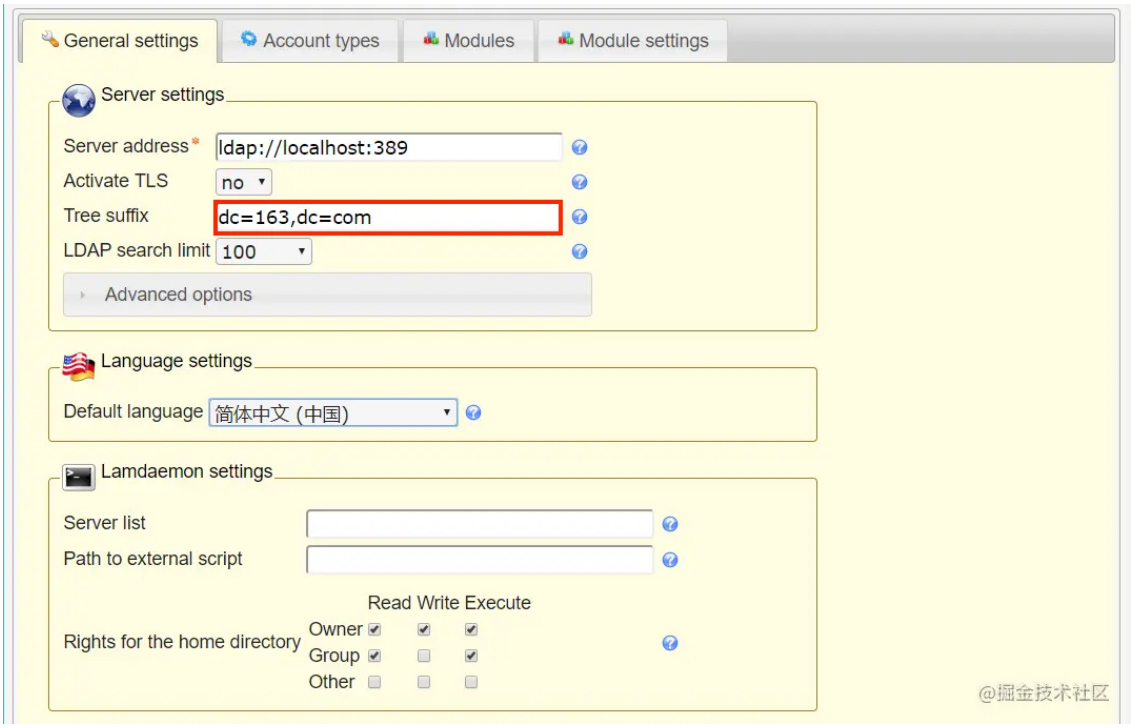
2. 看到如下页面有两个选项："Edit general settings"来编辑通用配置，默认密码lam，进入之后能配置密码策略、日志、管理员密码，最重要的是更新掉管理员密码，这个在后边"Manage server profiles"管理的时候需要提供；"Edit server profiles"来编辑服务器配置，我们先来编辑服务器配置



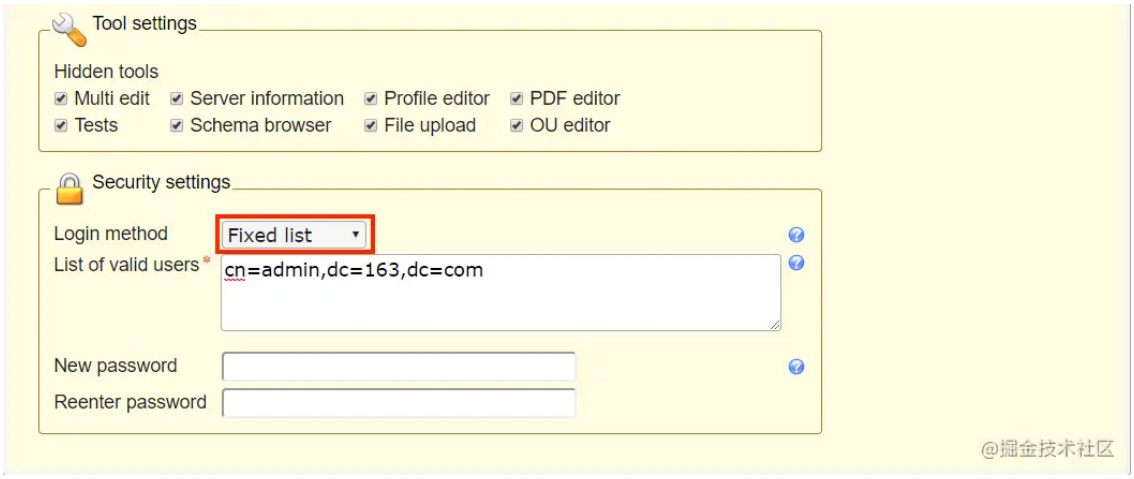
3. 进入如下页面，输入默认密码lam即可编辑配置，这里要说明一下的是红框标注的"Manage server profiles"可以对服务器的配置文件进行配置，例如增加、删除配置文件、配置文件重命名，最重要的是可以设置配置文件密码（也就是我们刚输入的密码lam，但修改密码需要管理员密码，后边配置）



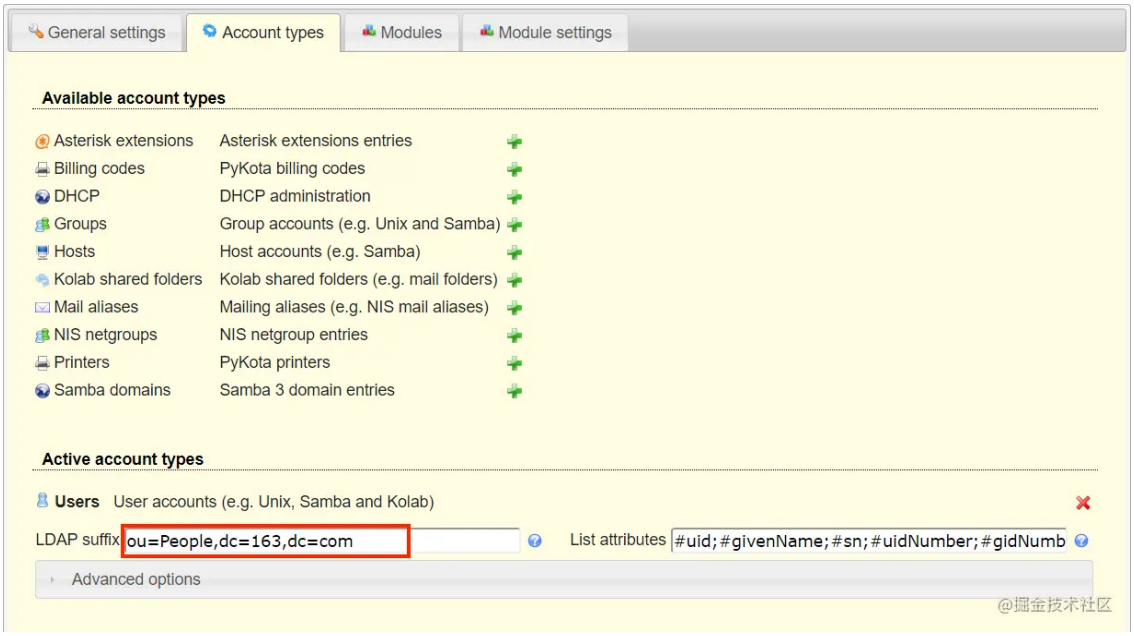
4. 输入密码lam后就正式进入服务器配置页，看到第一个标签"General setting"，（可以先改下语言简体中文保存，整站就给汉化啦，英文渣渣看起来就非常方便了），基本配置都看的很清晰了，主要是Tree suffix配置为自己的DC可以了



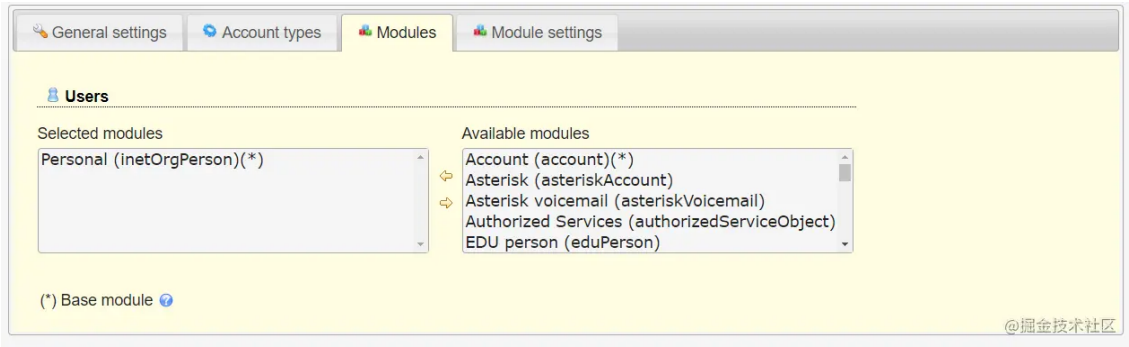
5. 接着来看这个页面，"security settings"非常重要，配置以何种方式登录web控制台，默认为Fixed list模式，就是下边列表里配置的dn可以登录，我们ldap里还没有任何一个账号（当我们创建了账号之后可以选择"LDAP serch"的模式，让普通账号也能登录以修改自己的密码），这里要选择fixed list模式并配置为我们ldap的rootdn，设置一个密码登录之后创建账号等操作



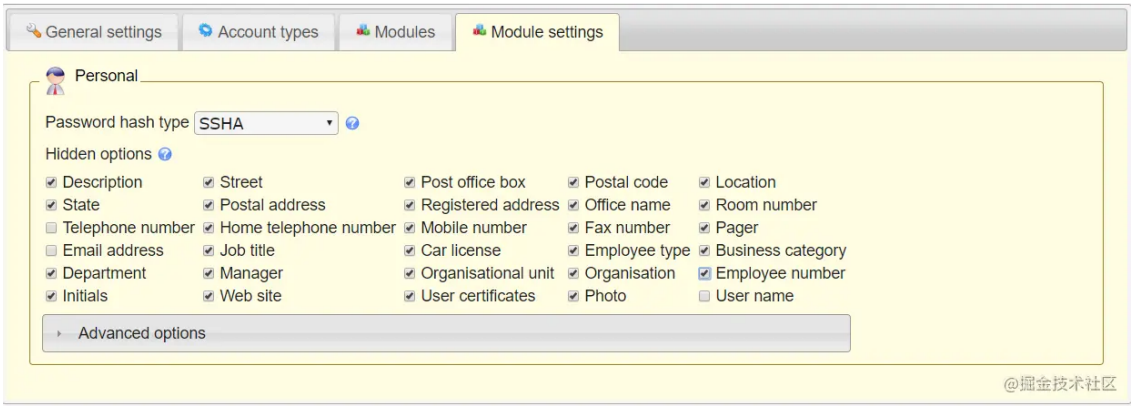
6. 接下来就是"Account types"标签页的配置，这里配置我们登录web控制显示的标签，我这里只需要他显示用户，就把Group之类的都删除了，保留了User



7. "Modules"页面配置上一个具体每个account type显示的模块



8. "Models setting"页面配置models具体要显示的内容，不得不说配置非常详细



9. 经过上边的配置就可以进入控制台新建账号了，新建账号之前一个有用的操作是修改用户的默认RDN标致为uid，更高位置在登录web控制台后右上角配置文件编辑器里边

10. 基本配置完成，可以开始使用了，中文界面比较清晰，无需过多解释啦。

参考文档

参考了太多网上优秀的文章，向他们致敬，下边列出的可能不全

- www.ibm.com/developerwo...
- www.cnblogs.com/qiuxiangmuy...
- blog.csdn.net/Dolphin_h/a...