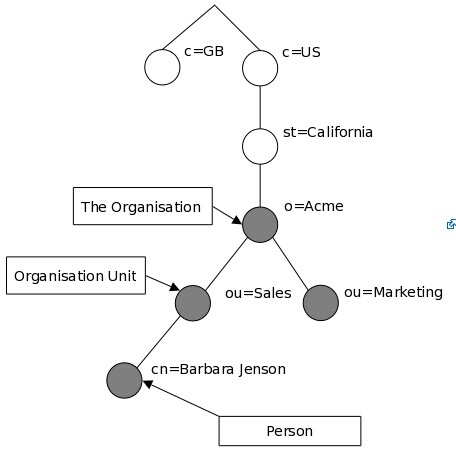
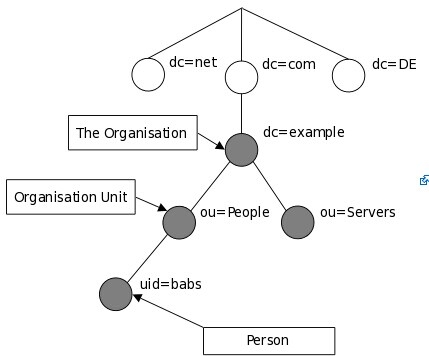
LDAP权限认证与实现

# 什么是LDAP

## 1、LDAP目录结构

[](http://s3.51cto.com/wyfs02/M00/3E/99/wKioL1PHexCiFLkzAACx6mZ_OZI194.jpg)

  此图为树形目录结构，我将此跳过去了，因为这个是按照“国家这种结构来划分的”。如果你喜欢这样看更好，如下还有一种：

[](http://s3.51cto.com/wyfs02/M02/3E/99/wKioL1PHe5TDP0w8AACgqGGzxhU812.jpg)

树也可以根据互联网域名组主。这种命名方式正越来越受欢迎，因为它允许使用DNS为目录服务定位 。这个LDAP目录树中使用基于域的命名。比较适合我的应用场景（从域名-->部门-->个人）。

## 2、条目（Entry）

  条目（Entry）就是目录管理的对象，他是LDAP中最基本的颗粒，就像字典中的词条，或者是数据库中的记录。通常对LDAP的添加、删除、更改、检索都是以条目为基本对象的。

  每一个条目都有一个唯一的标识名（distinguished Name ，DN），比如（1.1中图2互联网域名树形图）：cn=doubao,ou=Ops,dc=shuyun,dc=com。DN在语法上是由多个相对的标识名（distinguished Name ，DN）组成的，他们之间由逗号分隔。如果把DN看做对象的全路径，那么RDN就是其中的每一段路径。通过DN的层次型语法结构，可以方便地表示出条目在LDAP树中的位置。有时在不一致引起歧义的情况下，RDN也特指DN中最靠前的一段，而剩余的部分称为父标识（Parent DN,PDN）。此处不再举例。RDN本身也可以由多个值构成，比如OU=Tech+CN=doubao,dc=shuyun,dc=com中的RDN为OU=Tech+CN=doubao，由2个值OU=Tech和CN=doubao组成，他们之间由加好隔开。

  如果DN中含有一些特殊字符，比如：,=+<>;\"，他们需要转转义符(\)来帮助表述。

## 3、属性（Attribute）

  每个条目都可以有很多属性（Attribute），比如常见的人都有姓名、地址、电话等属性。每个属性都有名称及对应的值，属性值可以有单个、多个。比如你有多个电话。

  LDAP为人员组织机构中常见的对象都设计了属性(比如commonName，surname)。下面有一些常用的别名(表1-3-1)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性 | 别名 | 语法 | 描述 | 值(举例) |
| commonName | cn | Directory String | 姓名 | doubao |
| surname | sn | Directory String | 姓 | Chen |
| organizationalUnitName | ou | Directory String | 单位（部门）名称 | Tech |
| organization | o | Directory String | 组织（公司）名称 | shuyun |
| telephoneNumber |  | Telephone Number | 电话号码 | 110 |
| owner |  | DN | 该条目的拥有者 | cn=doubao,ou=ops,dc=shuyun |
| jpegPhoto |  | Binary | JPEG照片 | .. |

## 4、属性类型（AttributeType）

  每个属性都有唯一的属性类型（AttributeType），属性类型约定属性值的数据格式和语法类型（Syntax）。比如，属性cellPhone的类型为telephoneNumber，它规定了电话号码是由数字组成的，其中允许插入一些分隔符，如连接符、括号、空格等。

  属性类型也约定了属性值是否可以有多少个，多值属性类型也可以使人员信息的组织变得更加灵活并接近现实情况，比如：人员的手机、地址、邮箱等属性都可以有多个值。这样，用ldap组织的信息会比简单的表结构更加理想。

  类型也规定了属性查询时的匹配规则、排序顺序、大小写敏感等。

## 5、对象类（ObjectClass）

  对象类（ObjectClass）是属性的集合，LDAP预想了很多人员组织机构中常见的对象，并将其封装成对象类。比如人员（person）含有姓（sn）、名（cn）、电话(telephoneNumber)、密码(userPassword)等属性，单位职工(organizationalPerson)是人员(person)的继承类，除了上述属性之外还含有职务（title）、邮政编码（postalCode）、通信地址(postalAddress)等属性。

  通过对象类可以方便的定义条目类型。每个条目可以直接继承多个对象类，这样就继承了各种属性。如果2个对象类中有相同的属性，则条目继承后只会保留1个属性。对象类同时也规定了那些属性是基本信息，必须含有(Must 活Required，必要属性)：哪些属性是扩展信息，可以含有（May或Optional，可选属性）。

  对象类有三种类型：结构类型（Structural）、抽象类型(Abstract)和辅助类型（Auxiliary）。结构类型是最基本的类型，它规定了对象尸体的基本属性，每个条目属于且仅属于一个结构型对象类。抽象类型可以是结构类型或其他抽象类型父类，它公国将对象属性中共性的部分组织在一起，称为其他类的模板，条目不能直接集成抽象型对象类。辅助类型规定了对象实体的扩展属性。虽然每个条米只属于一个结构型对象类，但可以同时属于多个辅助型对象类。

  对象类本身是可以相互继承的，所以对象类的根类是top抽象型对象类。以常用的人员类型为例，他们的继承关系如图1-5-1：

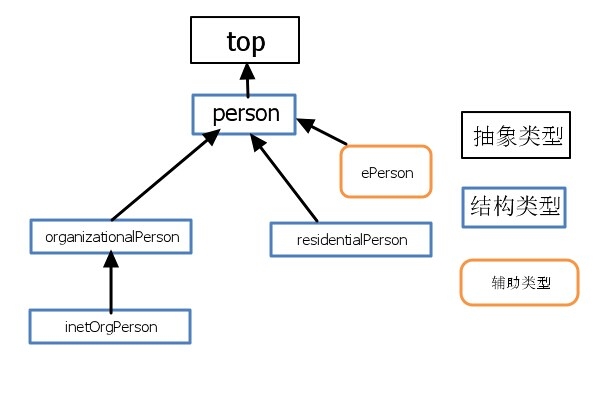
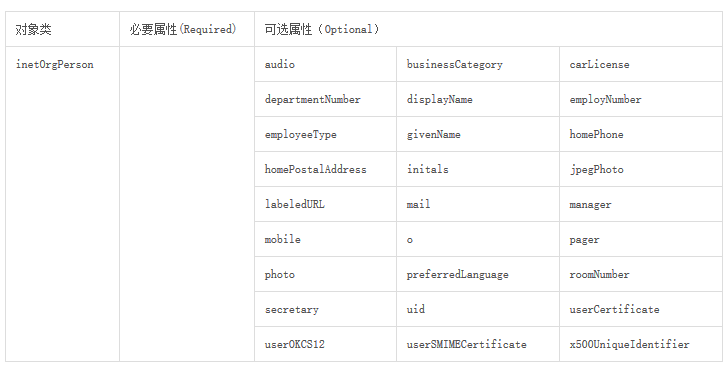
[](http://s3.51cto.com/wyfs02/M02/3E/AF/wKioL1PHmHLycKa4AADp74iLi5M845.jpg)

图1-5-1

 如果将其中一支 top-->person-->organizationalPerson-->inetOrgPerson的必要属性和可选属性列表（表1-5-2），就会发现这种设计还是非常合理的。我们可以从任何一个对象派生出自己的对象类，比如organizationalPerson派生出职工(employee)对象类，那么它可以含有工号(employeeNumber)、工种(employeeType)等属性。注意，对象类继承的时候会把属性是必须(Must)还是可选（May）的特性也一并继承。也就是说person有cn和sn两个Must属性，organizationalPerson和inetOrgPerson由于直接或间接继承了person，也会有这两个Must属性。

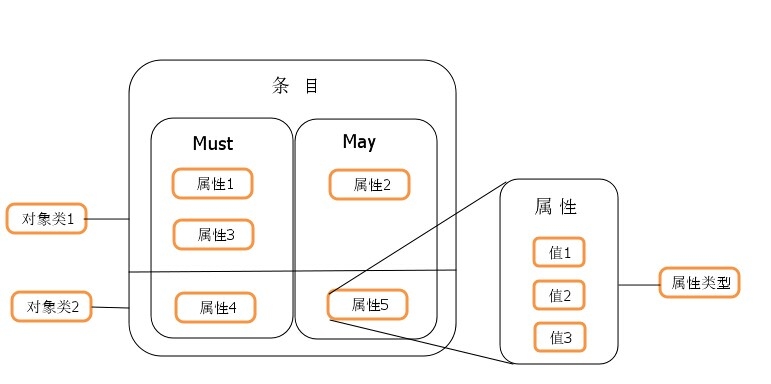
表1-5-2





## 6、模式（Schema）

  对象类（ObjectClass）、属性类型（AttributeType）、语法（Syntax）分别约定了条目、属性、值，他们之间的关系如下图所示。所以这些构成了模式(Schema)，模式中的每一个元素都有唯一的OID编号，如2.5.4.41.条目数据在导入时通常需要接受模式检查，它确保了目录中所有的条目数据结构都是一致的。

[](http://s3.51cto.com/wyfs02/M01/3E/B8/wKiom1PHoRbxZBZ-AAECq9r2G9Y162.jpg)

# Openldap安装

选一个节点安装即可，该节点即为ldap服务端

1. 安装openldap软件包

yum install openldap openldap-clients openldap-servers migrationtools

1. 生成根节点（manager）密码



通过slappasswd生成加密的密码，直接复制生成的加密密码，拷贝到slapd.conf文件中的rootpw行，具体为：rootpw {SSHA}RUBsqwKON0NLg3V1U+AwFBBq4LzIMbtO

如不进行上述slappasswd操作，则可直接在slapd.conf的rootpw行使用明文密码

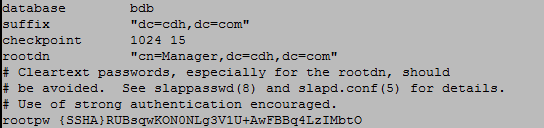
1. 修改配置文件
2. 拷贝配置文件

cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

cp /usr/share/openldap-servers/DB\_CONFIG.example /etc/openldap/DB\_CONFIG

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

1. 修改 slapd.conf



需要配置的是

suffix "dc=cdh,dc=com" //配置dc,根据自己需求进行设置

rootdn "cn=Manager,dc=cdh,dc=com" //配置cn，dc，根据需求进行配置

rootpw {SSHA}RUBsqwKON0NLg3V1U+AwFBBq4LzIMbtO //上一步生产的密码，可以使用明文

1. 重新生成配置数据

rm /etc/openldap/slapd.d/\* -rf

slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d

chown -R ldap:ldap /var/lib/ldap /etc/openldap/\*

这一步可能会提示相关文件夹不存在，那么可以手动创建，或者先进行1.3.4启动服务再进行此步，然后再进行1.3.4进行restart服务

1. 启动sladp服务

service slapd start

service slapd status

service slapd restart

1. 修改ldif生成工具：

vim /usr/share/migrationtools/migrate\_common.ph

#line 71 defalut DNS domain

$DEFAULT\_MAIL\_DOMAIN = "cdh.com";

#line 74 defalut base

$DEFAULT\_BASE = "dc=cdh,dc=com";

1. 添加根节点条目
2. 创建文件 top.ldif，写入：

dn:dc=cdh,dc=com

objectclass:dcObject

objectclass:organization

o:Cdh,Inc.

dc:cdh

dn:ou=People,dc=cdh,dc=com

objectclass:organizationalRole

cn:Manager

note:中间有一空行

1. 添加条目到系统中

ldapadd -x -W -D "cn=Manager,dc=cdh,dc=com" -f top.ldif

1. 添加用户条目
   1. 在 Shell下添加 Linux用户yangqi

useradd yangqi

passwd yangqi

* 1. 生成 LDIF文件

grep hive /etc/passwd >hive.in

/usr/share/migrationtools/migrate\_passwd.pl hive.in hive.ldif

* 1. 更新 LDIF文件

dn: uid=yangqi,ou=People,dc=cdh,dc=com

uid: yangqi

cn: yangqi

objectClass: account

objectClass: posixAccount

objectClass: top

objectClass: shadowAccount

userPassword: {crypt}$6$9jYjTtL3$PLI9jTwHCDyUnN8jizbv11pfXg6twOnjscqyo9IzlqQF5Mzsvz26nCLraSd8Jr3/X.OIpb0QjdoNKN7pPuEhk0

shadowLastChange: 16854

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

loginShell: /bin/bash

uidNumber: 503

gidNumber: 503

homeDirectory: /home/yangqi

* 1. 添加用户条目到 LDAP 中

ldapadd -x -D "cn=Manager,dc=cdh,dc=com" -W -f yangqi.ldif



* 1. Ldap修改用户密码

ldappasswd -x -D “cn=Manger,dc=cdh,dc=com” -w adminPasswd "uid=hive,ou=People,dc=cdh,dc=com" –S

强制修改用户密码

ldappasswd -H ldap://Server\_IP -x -D "cn=Manager,dc=cdh,dc=com" -W -S "uid=UserName,ou=People,dc=163,dc=com"

* 1. ldap删除用户

ldapdelete -x -w 123456 -D “cn=Manager,dc=cdh,dc=com” "uid=test,ou=people,dc=cdh,dc=com"

* 1. ldap查询用户

ldapsearch -LLL -x -D “cn=Manger,dc=cdh,dc=com” -w 123456 -b “ou=people,dc=cdh,dc=com” “uid=test”

# LDAP的HIVE配置

## 配置hive的ldap权限控制

1. 启用cdh上hive的ldap 服务：需要在Hive Metastore Server和HiveServer2节点上

Impala集成LDAP（使用CM配置）：CM访问：<http://ip:7180/>

对于cdh5.2及以前的版本，需要使用配置文件来开启ldap,如下：

<property>

<name>hive.server2.authentication</name>

<value>LDAP</value>

</property>

<property>

<name>hive.server2.authentication.ldap.url</name>

<value>ldap://cloud192</value>

</property>

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>ou=People,dc=cdh,dc=com</value>

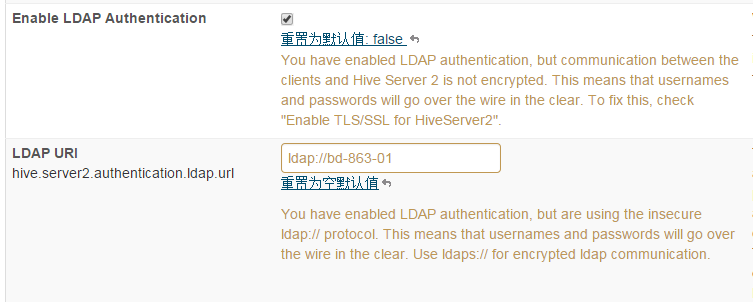
</property>

如图：



对于5.3及以上版本，需要进行一下开关操作

进入hive→配置→服务范围→安全性：按照如下配置





baseDN为ou=People,dc=cdh,dc=com

1. 配置完成后重启hive的相关服务。即可使用beeline输入用户名和密码的形式来登录hive