LDAP用户与用户组管理

# 1 导入系统用户

与系统用户相关的文件有/etc/passwd,/etc/shadow,/etc/group，其中

* 1. /etc/passwd: 存储有关本地用户的信息，其中的域给出了用户名、加密口令和用户的其他信息
  2. /etc/shadow，存储用户的密码信息，将/etc/passwd文件的加密口令移动到/etc/shadow中，该文件只对超级用户可读
  3. /etc/group，存储了用户组的信息

可以从这几个文件中生成ldif更新ldap数据库，这需要用到migrationtools工具，安装命令如下：

yum -y install migrationtoools

1）导入Linux系统base设置

利用迁移工具生成模板，修改默认的配置，更改DEFAULT\_BASE DN：

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

# Default DNS domain

$DEFAULT\_MAIL\_DOMAIN = "hadoop.org";

# Default base

$DEFAULT\_BASE = "dc=hadoop ,dc=org";

生成模板文件：

/usr/share/migrationtools/migrate\_base.pl > base.ldif

执行导入命令

ldapadd -x -D "cn=Manager,dc=hadoop,dc=org" -W -f base.ldif

2）导入用户

将当前用户导入到LDAP中，可以选择导入指定用户，从/etc/passwd中查找到用户，然后使用migrationtools，生成用户文件，例如导入用户hadoop：

$grep -E "hadoop" /etc/passwd > passwd.txt

$/usr/share/migrationtools/migrate\_passwd.pl passwd.txt passwd.ldif

ldapadd -x -D "cn=Manager,dc=hadoop ,dc=org" -W -f passwd.ldif

3）导入用户组

从/etc/group中获取用户组，生成用户组ldif文件，然后导入到ldap中

$grep -E "hadoop" /etc/group > group.txt

$/usr/share/migrationtools/migrate\_group.pl group.txt group.ldif

ldapadd -x -D "cn=Manager,dc=hadoop,dc=org" -W -f group.ldif

# 2查询用户

查询新添加的"hadoop"用户

ldapsearch -LLL -x -D "cn=Manager,dc=hadoop,dc=org" -W -b "dc=hadoop,dc=org" 'uid=hadoop'

查询结果



可以看到指定'uid=hadoop'，只查询这个用户的数据，这个查询条件叫做filter。在LDAP+Hadoop中，根据用户User查询group值需要指定这个filter。

例如，根据hadoop用户查询到hadoop群组，命令如下：

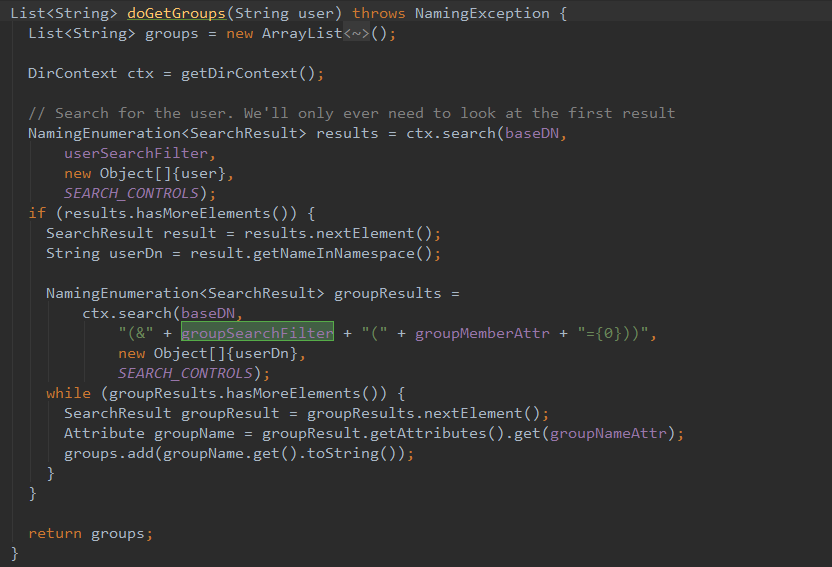
ldapsearch -x -D "cn=Manager,dc=hadoop,dc=org" -W -b "dc=hadoop,dc=org" '(& (objectclass=posixAccount)(cn=com))'

这条命名查询到用户名为com的用户，下面的命令根据查询到的信息查询到用户组

ldapsearch -x -D "cn=Manager,dc=hadoop,dc=org" -W -b "dc=hadoop,dc=org" '(&(objectclass=posixGroup)(gidNumber=1025))'

# 3.Hadoop用户账户管理

Hadoop中，LdapGroupsMapping中doGetGroups源码如下：



其中，Ldap查询所使用的查询条件分别如下：

用户：(&(objectclass=person(objectclass=applicationProcess))(cn={0}))

用户组：(objectclass=groupOfNames)(member={0})

与导入的Linux用户的Object class不同，因此需要改代码，patch在目录中