OpenLdap 安装配置

1.准备工作

1)节点1:192.168.149.150 做服务器； 节点2:192.168.149.155 做客户端

2)挂载系统盘

2.安装 LDAP 服务:

1)安装ldap服务端软件

yum install openldap-servers.x86_64

2)配置sldap.conf

cp -a /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf # 主配置文件

cp -a /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG

3)生成密码

[root@rhev ~]# slappasswd -s ZR123.com

{SSHA}R8TK0liZzbrWT0xR4ctoIGiHNccXVJIi

4)配置主文件dc

114 database bdb

115 suffix "dc=racher,dc=com"

116 checkpoint 1024 15

117 rootdn "cn=admin,dc=racher,dc=com"

118 # Cleartext passwords, especially for the rootdn, should

119 # be avoided. See slappasswd(8) and slapd.conf(5) for details.

120 # Use of strong authentication encouraged.

121 # rootpw secret

122 # rootpw {crypt}ijFYNcSNctBYg

123 rootpw {SSHA}R8TK0liZzbrWT0xR4ctoIGiHNccXVJIi

5)删除原始文件

rm -rf slapd.d/* # 删除原始的文件

slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/ # 重新生成一下，这里很重要

config file testing succeeded

6)修改文件权限

chown -R ldap:ldap /etc/openldap/slapd.d/

chown -R ldap:ldap /var/lib/ldap/

6)端口检查

netstat -ntplu | grep slapd # ldap监听端口为tcp: 389

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

3.安装配置migrationtools 并创建ldpa测试账号

1)安装migrationtools

yum install migrationtools -y

2)创建用户

cd /usr/share/migrationtools/

mkdir /ldaphome

[root@rhev tmp]# useradd -d /ldaphome/ldapuser2 ldapuser2

[root@rhev tmp]# echo 'ldapuser2' | passwd ldapuser2 --stdin

3)编辑文件/usr/share/migrationtools/migrate_common.ph

70 # Default DNS domain
71 $DEFAULT_MAIL_DOMAIN = "racher.com";
72
73 # Default base
74 $DEFAULT_BASE = "dc=racher,dc=com";

4)利用pl脚本将/etc/passwd 和/etc/shadow生成LDAP能读懂的文件格式，保存在/tmp/下

./migrate_base.pl > /tmp/base.ldif # 生成三个文件: base.ldif、passwd.ldif、group.ldif

grep ldapuser1 /etc/passwd > /tmp/passwd.in
./migrate_passwd.pl /tmp/passwd.in > /tmp/passwd.ldif

grep ldapuser1 /etc/group > /tmp/group.in
./migrate_group.pl /tmp/group.in > /tmp/group.ldif

5)编辑 /tmp/base.ldif

1 dn: dc=racher,dc=com
2 dc: racher
3 objectClass: top
4 objectClass: domain

36 dn: ou=People,dc=racher,dc=com
37 ou: People
38 objectClass: top
39 objectClass: organizationalUnit

41 dn: ou=Group,dc=racher,dc=com
42 ou: Group
43 objectClass: top
44 objectClass: organizationalUnit

6)编辑 /tmp/passwd.ldif

dn: uid=ldapuser1,ou=People,dc=racher,dc=com
uid: ldapuser1
cn: ldapuser1
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:
{crypt}6GyDAJ2r2$3lZ1FlwCAbktNpd5SwEl/wtLQuDFVsDJojyTc9dYdETgJaBKUleoGb5qnpkS18inwVffnhQVxFM.vJeL1CQic1
shadowLastChange: 17105
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 502
gidNumber: 502

homeDirectory: /ldaphome/ldapuser1

7)编辑 /tmp/group.ldif

dn: cn=ldapuser1,ou=Group,dc=racher,dc=com
objectClass: posixGroup
objectClass: top
cn: ldapuser1
userPassword: {crypt}x
gidNumber: 502

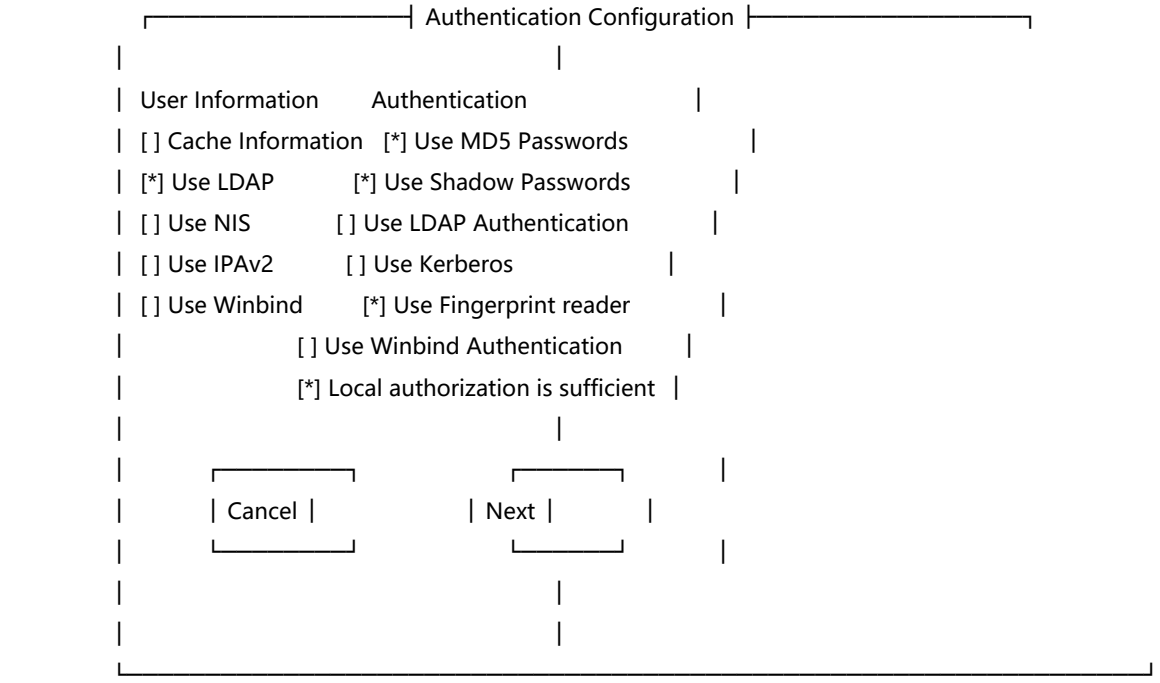
8)把这三个文件导入到LDAP，这样LDAP的数据库里就有了我们想要的用户

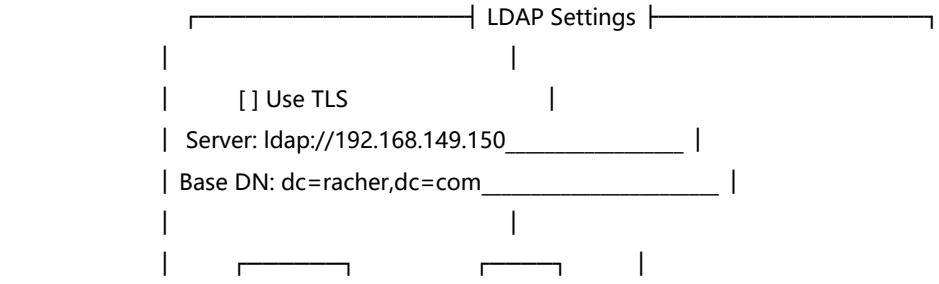
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/base.ldif
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/passwd.ldif
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/group.ldif

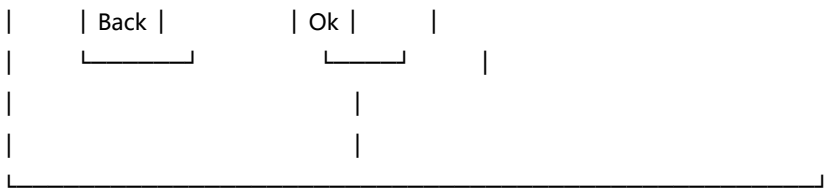
至此 已配置完一个 ldapuser1 用户为 ldap 用户。

4.ldap 客户端配置

1)配置 setup neirong ，没有此工具，可以 yum -y install setuptool 安装







2) 安装nfs-utils 使用showmount 查看服务器共享目录

yum install nfs-utils -y

//查看已经挂载上了共享目录

[root@cldap etc]# showmount -e 192.168.149.150

Export list for 192.168.149.150:

/ldaphome 192.168.149.0/24

3)安装autofs包

yum install autofs -y

4)添加挂载规则

vim /etc/auto.master

/ldaphome /etc/auto.nfs   # 添加一条新的规则

vim /etc/auto.nfs   # 添加自动挂载的规则

* -fstype=nfs,rw,async 192.168.118.14:/ldaphome/&   # 挂载192.168.118.14:/ldaphome/到本地的/ldaphome

4)直接测试

[root@cldap etc]# su - ldapuser1

[ldapuser1@cldap ~]$ pwd

/ldaphome/ldapuser1

[ldapuser1@cldap ~]$

[ldapuser1@cldap ~]$ df

Filesystem   1K-blocks   Used Available Use% Mounted on

、、、

192.168.149.150:/ldaphome/ldapuser1

59862528 9865216 46956544 18% /ldaphome/ldapuser1

[root@rhev tmp]# useradd -d /ldaphome/ldapuser2 ldapuser2

[root@rhev tmp]# echo 'ldapuser2' | passwd ldapuser2 --stdin

service rpcbind start

Starting rpcbind: [OK]

service nfs start

参考:

http://blog.csdn.net/u013080248/article/details/17516425

http://www.linuxidc.com/Linux/2015-04/116536.htm
http://blog.csdn.net/hitabc141592/article/details/22931179

http://blog.csdn.net/u013080248/article/details/17516425

http://mt.sohu.com/20160618/n455072025.shtml

http://www.cnblogs.com/hukey/p/5779069.html