Netkiller LDAP 手札

netkiller Neo Chan

2009-11-16

文档出处: http://netkiller.sourceforge.net/ | http://netkiller.github.com

文档最近一次更新于 Thu Dec 1 12:51:21 UTC 2011

下面是我多年积累下来的经验总结，整理成文档供大家参考:

Netkiller Architect 手札	Netkiller Linux 手札	Netkiller Developer 手札	Netkiller Database 手札
Netkiller Debian 手札	Netkiller CentOS 手札	Netkiller FreeBSD 手札	Netkiller Shell 手札
Netkiller Web 手札	Netkiller Monitoring 手札	Netkiller Storage 手札	Netkiller Mail System 手札
Netkiller MySQL 手札	Netkiller LDAP 手札	Netkiller Security 手札	Netkiller Version 手札
Netkiller Intranet 手札	Netkiller Cisco IOS 手札	Netkiller Writer 手札	Netkiller Studio Linux 手札

目录

About author

1. 作者简介

1.1. 联系作者

1. OpenLDAP server (slapd)

1. Installation

1.1. CentOS/Redhat
1.2. Debian/Ubuntu

2. Configure
3. 基本操作

3.1. base-dn
3.2. Add
3.3. Search
3.4. Modify
3.5. Delete

3.6. Search
3.7. Organization Unit

2. Replication

1. Primary
2. Secondary

3. Backup and Restore
4. Active Directory
5. Outlook Address
6. Development

1. Python

范例清单

1.1. base-dn.ldif
1.2. ou.ldif

下一页
About author

About author

目录

1. 作者简介

1.1. 联系作者

1. 作者简介

主页地址：http://netkiller.sourceforge.net, http://netkiller.github.com/

陈景峰 (ㄔㄣˊ ㄐㄧㄥˇ ㄈㄥ)

Nickname：netkiller | English name: Neo chen | Nippon name: ちんけいほう (音訳) | Korean name: | Thailand name:

IT民工， UNIX like Evangelist, 业余无线电爱好者（呼号：BG7NYT）,户外运动以及摄影爱好者。

《PostgreSQL实用实例参考》，《Postfix 完整解决方案》，《Netkiller Linux 手札》的作者

2001年来深圳进城打工,成为一名外来务工者.

2002年我发现不能埋头苦干,埋头搞技术是不对的,还要学会"做人".

2003年这年最惨,公司拖欠工资16000元,打过两次官司2005才付清.

2004年开始加入分布式计算团队,目前成绩

2004-10月开始玩户外和摄影

2005-6月成为中国无线电运动协会会员

2006年单身生活了这么多年,终于找到归宿.

2007物价上涨,金融危机，休息了4个月（其实是找不到工作）

2008终于找到英文学习方法，，《Netkiller Developer 手札》，《Netkiller Document 手札》

2008-8-8 08:08:08 结婚,后全家迁居湖南省常德市

2009《Netkiller Database 手札》,年底拿到C1驾照

2010对电子打击乐产生兴趣，计划学习爵士鼓

2011 职业生涯路上继续打怪升级

1.1. 联系作者

Mobile: +86 13113668890

Tel: +86 755 2981-2080

Callsign: BG7NYT QTH: Shenzhen, China

注：请不要问我安装问题!

E-Mail: openunix@163.com
IRC irc.freenode.net #ubuntu / #ubuntu-cn

Yahoo: bg7nyt
ICQ: 101888222
AIM: bg7nyt

TM/QQ: 13721218
MSN: netkiller@msn.com
G Talk: 很少开
网易泡泡：很少开

写给火腿:

欢迎无线电爱好者和我QSO,我的QTH在深圳宝安区龙华镇溪山美地12B7CD,设备YAESU FT-50R,FT-60R,FT-7800 144-430双段机,拉杆天线/GP天线 Nagoya MAG-79EL-3W/Yagi

如果这篇文章对你有所帮助,请寄给我一张QSL卡片,qrz.cn or qrz.com or hamcall.net

Personal Amateur Radiostations of P.R.China

ZONE CQ24 ITU44 ShenZhen, China

Best Regards, VY 73! OP. BG7NYT

第 1 章 OpenLDAP server (slapd)

目录

1. Installation

1.1. CentOS/Redhat
1.2. Debian/Ubuntu

2. Configure
3. 基本操作

3.1. base-dn
3.2. Add
3.3. Search
3.4. Modify
3.5. Delete
3.6. Search
3.7. Organization Unit

1. Installation

1.1. CentOS/Redhat

Yum

```
[root@development ~]# yum -y install openldap-servers
[root@development ~]# yum -y install openldap-clients
```

Redhat AS4

```
[root@backup openldap]# rpm -aq |grep openldap
compat-openldap-2.1.30-6.4E
openldap-2.2.13-6.4E
openldap-devel-2.2.13-6.4E
openldap-clients-2.2.13-6.4E
openldap-servers-2.2.13-6.4E
openldap-servers-sql-2.2.13-6.4E
```

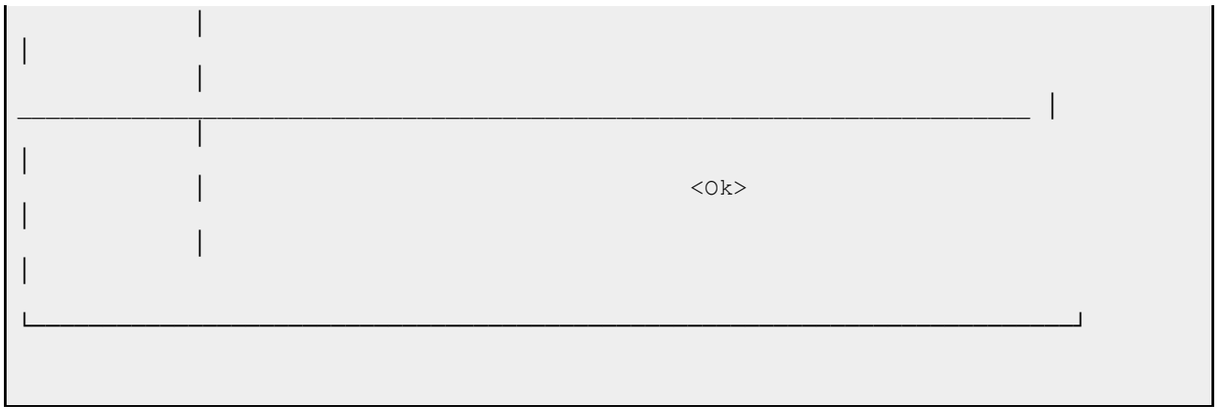
1.2. Debian/Ubuntu

$ sudo apt-get install slapd

```
$ sudo apt-get install slapd
$ sudo apt-get install ldap-utils
```

Admin password/Confirm password

```
                ┌──────────────────────────────┤  正在设定 slapd
├──────────────────────────────┐
                │  Please enter the password for the admin entry in your LDAP
directory.  │
                │
│
                │ Admin password:
│
```



上一页 下一页
About author 起始页 2. Configure

2. Configure

过程 1.1. Configure Openldap

1. 配置/etc/ldap.conf

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example, dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
HOST 127.0.0.1
BASE dc=bg7nyt,dc=cn
TLS_CACERTDIR /etc/openldap/cacerts
```

2. 配置/etc/slapd.conf

```
suffix          "dc=bg7nyt,dc=cn"
rootdn          "cn=Manager,dc=bg7nyt,dc=cn"
rootpw          {crypt}ijFYNcSNctBYg
```

rootpw 默认是 secret

crypt 密码产生很简单，很多语言里都有crypt(key,salt)函数，不过最简单的办法是，使用UNIX Shadow 密码，使用apache的htpasswd生成

如果你想使用更复杂的加密算法，可以参考我的另一篇文章《信息安全与加密》

3. ldap 脚本

service ldap {start|stop|restart|status|condrestart}

or

/etc/init.d/ldap {start|stop|restart|status|condrestart}

```
[root@backup openldap]# service ldap
Usage: /etc/init.d/ldap {start|stop|restart|status|condrestart}
[root@backup openldap]# service ldap start
Checking configuration files for : config file testing succeeded
Starting slapd:                                            [  OK  ]
[root@backup openldap]# service ldap restart
Stopping slapd:                                            [  OK  ]
Checking configuration files for slapd: config file testing succeeded
Starting slapd:                                            [  OK  ]
[root@backup openldap]# service ldap stop
Stopping slapd:                                            [  OK  ]
[root@backup openldap]#
```

reconfigure

```
sudo dpkg-reconfigure slapd
```

3. 基本操作

3.1. base-dn

建立基本DN

例 1.1. base-dn.ldif

```
dn: dc=bg7nyt,dc=cn
objectclass: dcObject
objectclass: organization
o:bg7nyt.net
dc: bg7nyt
description:Top level of directory

dn: cn=Manager,dc=bg7nyt,dc=cn
objectclass: organizationalRole
cn: Manager

dn: cn=admin,dc=bg7nyt,dc=cn
objectclass: organizationalRole
cn: admin

dn: cn=root,dc=bg7nyt,dc=cn
objectclass: organizationalRole
cn: root
```

ldapadd -x -D "cn=root,dc=bg7nyt,dc=cn" -W -f base-dn.ldif

3.2. Add

添加条目

```
[chenjingfeng@backup ldap]$ ldapadd -x -D "cn=root,dc=bg7nyt,dc=cn" -W -f base-
dn.ldif
Enter LDAP Password:
adding new entry "dc=bg7nyt,dc=cn"

adding new entry "cn=Manager,dc=bg7nyt,dc=cn"

adding new entry "cn=admin,dc=bg7nyt,dc=cn"

adding new entry "cn=root,dc=bg7nyt,dc=cn"
```

查看条目

```
[chenjingfeng@backup ldap]$ ldapsearch -x -b 'dc=bg7nyt,dc=cn' '(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=bg7nyt,dc=cn> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# bg7nyt.cn
dn: dc=bg7nyt,dc=cn
```

```
objectClass: dcObject
objectClass: organization
o: bg7nyt.net
dc: bg7nyt
description: Top level of directory

# Manager, bg7nyt.cn
dn: cn=Manager,dc=bg7nyt,dc=cn
objectClass: organizationalRole
cn: Manager

# admin, bg7nyt.cn
dn: cn=admin,dc=bg7nyt,dc=cn
objectClass: organizationalRole
cn: admin

# root, bg7nyt.cn
dn: cn=root,dc=bg7nyt,dc=cn
objectClass: organizationalRole
cn: root

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

3.3. Search

3.4. Modify

3.5. Delete

删除条目

```
ldapdelete -x -D "cn=root,dc=bg7nyt,dc=cn" -W "dc=bg7nyt,dc=cn"
```

3.6. Search

搜索条目

dn条目

```
ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
```

结果

```
# extended LDIF
#
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=bg7nyt,dc=cn

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
ldapsearch -x -b 'dc=bg7nyt,dc=cn'
```

3.7. Organization Unit

建立组织单元

例 1.2. ou.ldif

```
dn: ou=address,dc=bg7nyt,dc=cn
ou: address
objectClass: organizationalUnit

dn: cn=neo, ou=address, dc=bg7nyt,dc=cn
objectClass: person
cn: neo
sn: neo

dn: cn=netkiller, ou=address, dc=bg7nyt,dc=cn
objectClass: person
objectClass: inetOrgPerson
cn: netkiller
sn: netkiller
mail: openunix@163.com

dn: cn=bg7nyt, ou=address, dc=bg7nyt,dc=cn
objectClass: person
cn: bg7nyt
sn: bg7nyt
```

建立ou

```
[chenjingfeng@backup ldap]$ ldapadd -x -D "cn=root,dc=bg7nyt,dc=cn" -W -f ou.ldif
Enter LDAP Password:
adding new entry "ou=address,dc=bg7nyt,dc=cn"

adding new entry "cn=neo, ou=address, dc=bg7nyt,dc=cn"

adding new entry "cn=netkiller, ou=address, dc=bg7nyt,dc=cn"

adding new entry "cn=bg7nyt, ou=address, dc=bg7nyt,dc=cn"
```

删除ou

```
[chenjingfeng@backup ldap]$ ldapdelete -x -D "cn=root,dc=bg7nyt,dc=cn" -W
"ou=address,dc=bg7nyt,dc=cn"
Enter LDAP Password:
```

第 2 章 Replication

目录

1. Primary
2. Secondary

1. Primary

过程 2.1. Primary configure

1. installation

```
neo@master:~$ sudo apt-get install slapd ldap-utils
```

2. slapd.conf

```
neo@master:~$ vi /etc/ldap/slapd.conf
suffix          "dc=example,dc=org"
replogfile      /var/lib/ldap/replog
syncrepl        rid=001
                provider=ldap://192.168.245.131:389/
                binddn="cn=admin,dc=example,dc=org"
                bindmethod=simple
                credentials=chen
                searchbase="dc=example,dc=org"
                type=refreshAndPersist
                retry="5 5 300 5"
```

3. initial entries base dn

```
neo@master:~$ cat base-dn.ldif

dn: dc=example,dc=org
objectclass: dcObject
objectclass: organization
o:example.org
dc: example
description:Top level of directory

dn: cn=Manager,dc=example,dc=org
objectclass: organizationalRole
cn: Manager

dn: cn=admin,dc=example,dc=org
objectclass: organizationalRole
cn: admin

dn: cn=root,dc=example,dc=org
objectclass: organizationalRole
cn: root
```

Add initial entries to your directory.

```
neo@master:~$ ldapadd -x -D "cn=admin,dc=example,dc=org" -W -f base-dn.ldif
Enter LDAP Password:
adding new entry "dc=example,dc=org"

adding new entry "cn=Manager,dc=example,dc=org"
```

```
adding new entry "cn=admin,dc=example,dc=org"

adding new entry "cn=root,dc=example,dc=org"
```

check

```
neo@master:~$ ldapsearch -x -b 'dc=example,dc=org' '(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=org> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# example.org
dn: dc=example,dc=org
objectClass: dcObject
objectClass: organization
o: example.org
dc: example
description: Top level of directory

# Manager, example.org
dn: cn=Manager,dc=example,dc=org
objectClass: organizationalRole
cn: Manager

# admin, example.org
dn: cn=admin,dc=example,dc=org
objectClass: organizationalRole
cn: admin

# root, example.org
dn: cn=root,dc=example,dc=org
objectClass: organizationalRole
cn: root

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

4. Export the database of the master using slapcat. Then copy master.ldif to the slave using scp or other tools.

```
neo@master:~$ sudo slapcat -l master.ldif
```

2. Secondary

过程 2.2. Secondary configure

1. installation

```
neo@slave:~$ sudo apt-get install slapd ldap-utils
```

2. configure

```
neo@master:~$ vi /etc/ldap/slapd.conf
updatedn        cn=admin,dc=example,dc=org
updateref       ldap://master.example.org
```

3. Import the master.ldif using slapadd.

```
neo@slave:~$ sudo slapadd -c -l master.ldif
```

第 3 章 Backup and Restore

backup

```
cp -r /etc/openldap .
CURRENT_DATA=`date '+%m-%d-%y'`
slapcat -l backup_${CURRENT_DATA}_neo_chen.ldif
tar zcvf backup_ldap.tar.gz ldap/
md5sum backup_ldap.tar.gz > backup_ldap.tar.gz.md5
```

restore

ldapadd -x -D "cn=root,dc=bg7nyt,dc=cn" -W -f your.ldif

第 4 章 Active Directory

通过ldapsearch查询Windows Active Directory 是一件很有趣事情。

列出所有员工姓名

```
ldapsearch -x -H ldap://192.168.19.238 -D neo.chen@company.com -w 12345678 -b
'OU=china,DC=company,DC=com'
'(&(objectCategory=person)(objectClass=user)(company=*)(mail=*))'|grep '^name::' |
awk -F ' ' '{print $2}' |base64 --decode | sed 's/)/)\r\n/g'
```

统计员工数目

```
ldapsearch -x -H ldap://192.168.19.238 -D neo.chen@company.com -w 12345678 -b
'OU=china,DC=company,DC=com'
'(&(objectCategory=person)(objectClass=user)(company=*)(mail=*))'|grep '^name::' |
wc -l
```

制作通讯录,或导出邮件列表

```
ldapsearch -x -H ldap://192.168.19.238 -D neo.chen@company.com -w 12345678 -b
'OU=china,DC=company,DC=com'
'(&(objectCategory=person)(objectClass=user)(company=*)(mail=*))'|grep ^mail:|awk
-F ' ' '{print $2}'
```

列出 name mail mobile telephoneNumber

```
ldapsearch -x -H ldap://192.168.19.238 -D neo.chen@company.com -w 12345678 -b
'OU=china,DC=company,DC=com'
'(&(objectCategory=person)(objectClass=user)(name=*)(mail=*))' name mail mobile
telephoneNumber
```

第 5 章 Outlook Address

过程 5.1. Openldap for Outlook Address

1.
2.
3.
4.
5.

第 6 章 Development

目录

1. Python

1. Python

```
[root@development ~]# yum -y install python-ldap
```