原创

centos7搭建openldap+phpldapadmin

羊草

2018-01-27 12:58:09 4197人阅读 4人评论

> 参考：https://www.cnblogs.com/bigbrotherer/p/7251372.html
> https://www.ilanni.com/?p=13775
> openldap-server的数据必须用原配的Berkeley DB，不能使用mysql作为后端数据库
> openldap的操作语法比较复杂，推荐使用phpldapadmin管理配置，同时也可以用windows下ldapadmin程序进行配置

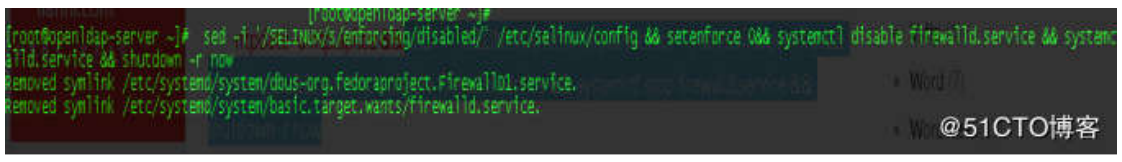
1.初始化准备

系统centos7 64位
配置yum源

```
wget http://mirrors.aliyun.com/repo/Centos-7.repo
    cp Centos-7.repo /etc/yum.repos.d/
    cd /etc/yum.repos.d/
    mv CentOS-Base.repo CentOS-Base.repo.bak
    mv Centos-7.repo CentOS-Base.repo
    yum clean all
    yum makecache
```

关闭selinux和防火墙

```
&& systemctl disable firewalld.service && systemctl stop firewalld.service && shutdown -r now
```

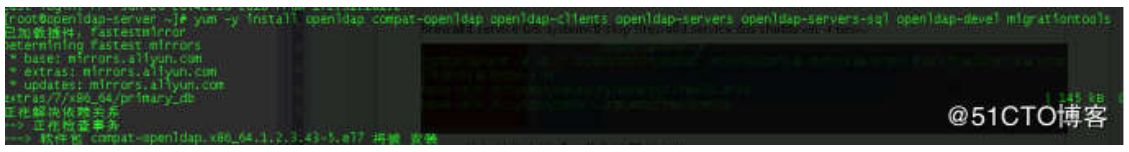


环境初始化完毕后，我们就可以安装OpenLDAP。

2.安装OpenLDAP

使用如下命令安装OpenLDAP：

```
-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel migrationtools
```



查看OpenLDAP版本，使用如下命令：

```
slapd -VV
```

OpenLDAP安装完毕后，接下来我们开始配置OpenLDAP。

3.配置OpenLDAP

OpenLDAP配置比较复杂牵涉到的内容比较多，接下来我们一步一步对其相关的配置进行介绍。
注意:从OpenLDAP2.4.23版本开始所有配置数据都保存在/etc/openldap/slapd.d/中，建议不再使用slapd.conf作为配置文件。

设置OpenLDAP的管理员密码:

```
slappasswd -s ******
```

上述加密后的字段保存下，等会我们在配置文件中会使用到。

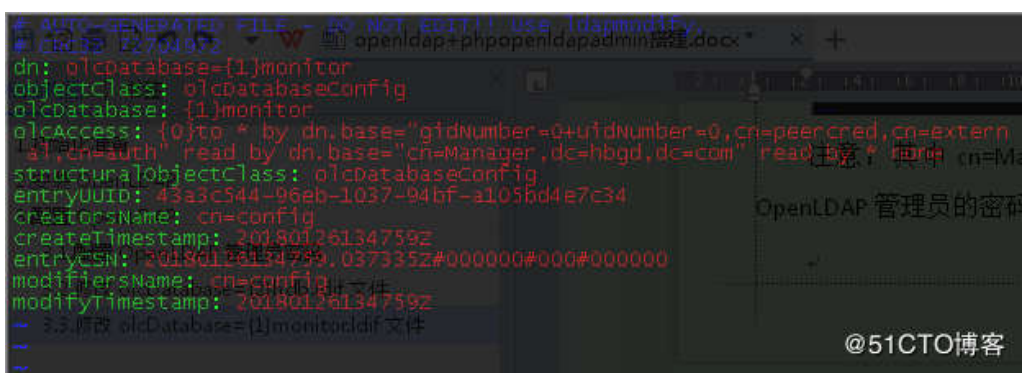
3.2.修改olcDatabase={2}hdb.ldif文件

```
Vim /etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif
修改olcDatabase={2}hdb.ldif文件,对于该文件增加一行
olcRootPW: {SSHA}o1bqtofUr95dkEDdXbAMAVPFSnNDU3+2，然后修改域信息：
olcSuffix: dc=hbgd,dc=com
olcRootDN: cn=Manager,dc=hbgd,dc=com
```

注意：其中cn=Manager中的Manager表示OpenLDAP管理员的用户名，而olcRootPW表示OpenLDAP管理员的密码。

3.3.修改olcDatabase={1}monitor.ldif文件

```
修改olcDatabase={1}monitor.ldif文件，如下：
vim /etc/openldap/slapd.d/cn=config/olcDatabase\=\{1\}monitor.ldif
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=hbgd,dc=com" read by * none
```



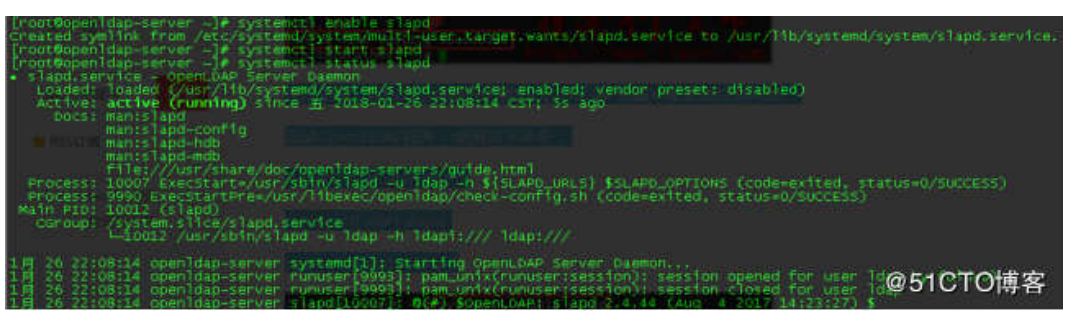
注意：该修改中的dn.base是修改OpenLDAP的管理员的相关信息的。

验证OpenLDAP的基本配置，使用如下命令：

```
slaptest -u
```

通过上图，我们可以很明显的看出OpenLDAP的基本配置是没有问题。
启动OpenLDAP服务，使用如下命令：

```
systemctl enable slapd
systemctl start slapd
systemctl status slapd
```



OpenLDAP默认监听的端口是389，下面我们来看下是不是389端口，如下：

```
netstat -antup | grep 389
```

0 4 羊草

通过上图，我们可以很明显的看出OpenLDAP确实是监听的是389端口。

3.4.配置OpenLDAP数据库

OpenLDAP默认使用的数据库是BerkeleyDB，现在来开始配置OpenLDAP数据库，使用如下命令：

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap:ldap -R /var/lib/ldap
chmod 700 -R /var/lib/ldap
ll /var/lib/ldap/
```

注意：/var/lib/ldap/就是BerkeleyDB数据库默认存储的路径。

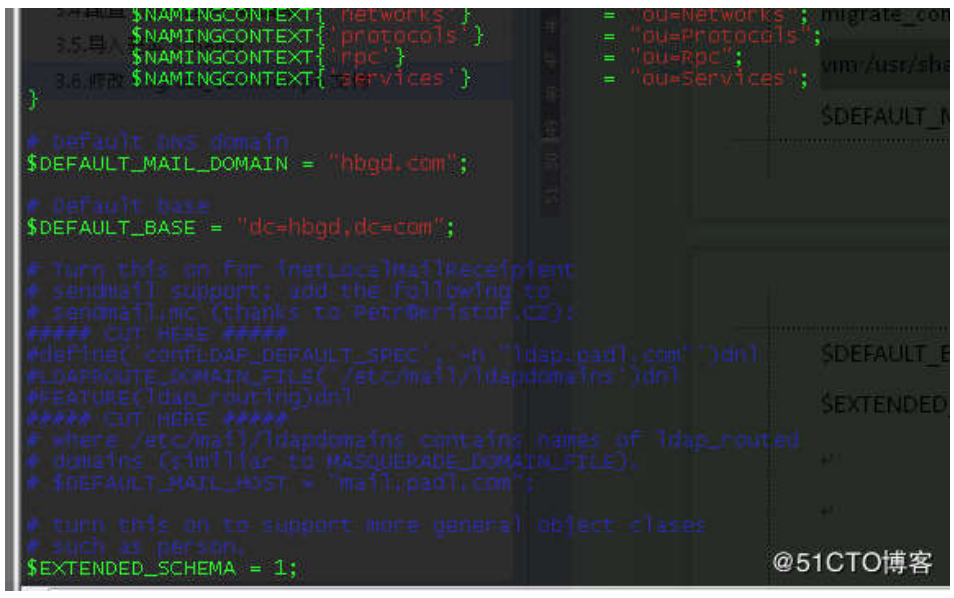
3.5.导入基本Schema

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

3.6.修改migrate_common.ph文件

migrate_common.ph文件主要是用于生成ldif文件使用，修改migrate_common.ph文件，如下：

```
vim /usr/share/migrationtools/migrate_common.ph +71
$DEFAULT_MAIL_DOMAIN = “hbgd.com”;
$DEFAULT_BASE = “dc=hbgd,dc=com”;
$EXTENDED_SCHEMA = 1;
```



到此OpenLDAP的配置就已经全部完毕，下面我们来开始添加用户到OpenLDAP中。

4.添加用户及用户组

默认情况下OpenLDAP是没有普通用户的，但是有一个管理员用户。管理用户就是前面我们刚刚配置的root。
现在我们把系统中的用户，添加到OpenLDAP中。为了进行区分，我们现在新加两个用户ldapuser1和ldapuser2，和两个用户组ldapgroup1和ldapgroup2，如下：
添加用户组，使用如下命令：

```
groupadd ldapgroup1
groupadd ldapgroup2
```

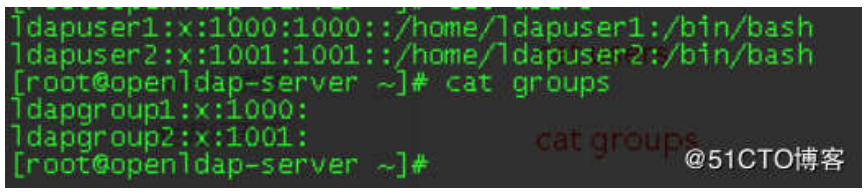
添加用户并设置密码，使用如下命令

```
useradd -g ldapgroup1 ldapuser1
```

0 4 羊草

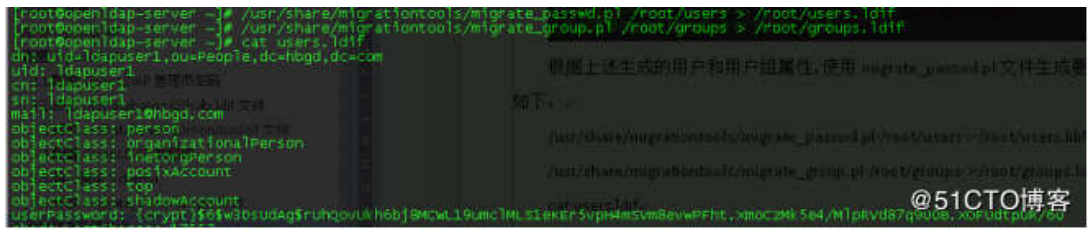
把刚刚添加的用户和用户组提取出来，这包括该用户的密码和其他相关属性，如下

```
grep “:10[0-9][0-9]” /etc/passwd > /root/users
grep “:10[0-9][0-9]” /etc/group > /root/groups
```



根据上述生成的用户和用户组属性，使用migrate_passwd.pl文件生成要添加用户和用户组的ldif，如下：

```
/usr/share/migrationtools/migrate_passwd.pl /root/users > /root/users.ldif
/usr/share/migrationtools/migrate_group.pl /root/groups > /root/groups.ldif
cat users.ldif
cat groups.ldif
```



注意：后续如果要新加用户到OpenLDAP中的话，我们可以直接修改users.ldif文件即可。

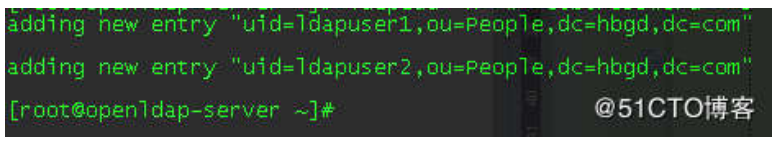
5.导入用户及用户组到OpenLDAP数据库

配置openldap基础的数据库，如下：

```
cat > /root/base.ldif << EOF
dn: dc=hbgd,dc=com
o: hbgd com
dc: hbgd
objectClass: top
objectClass: dcObject
objectclass: organization
dn: cn=Manager,dc=hbgd,dc=com
cn: Manager
objectClass: organizationalRole
description: Directory Manager
dn: ou=People,dc=hbgd,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
dn: ou=Group,dc=hbgd,dc=com
ou: Group
objectClass: top
objectClass: organizationalUnit
EOF
```

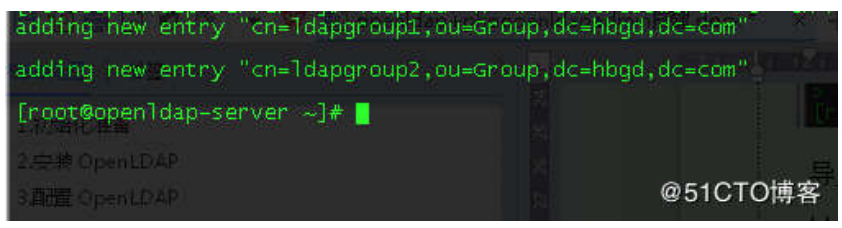
导入基础数据库，使用如下命令：

```
ldapadd -x -w “xxxxxx” -D “cn=Manager,dc=hbgd,dc=com” -f /root/base.ldif
```



导入用户组到数据库，使用如下命令

```
ldapadd -x -w “xxxxx” -D “cn=Manager,dc=hbgd,dc=com” -f /root/groups.ldif
```



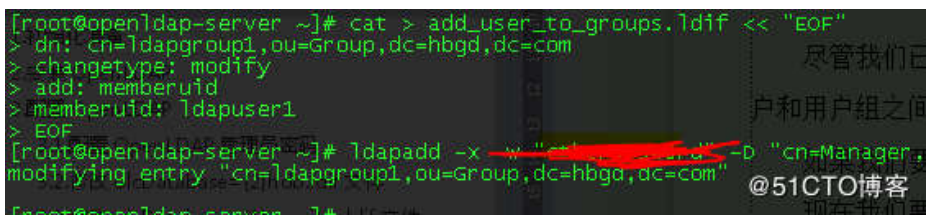
6.把OpenLDAP用户加入到用户组

尽管我们已经把用户和用户组信息，导入到OpenLDAP数据库中了。但实际上目前OpenLDAP用户和用户组之间是没有任何关联的。
如果我们要把OpenLDAP数据库中的用户和用户组关联起来的话，我们还需要做另外单独的配置。
现在我们要把ldapuser1用户加入到ldapgroup1用户组，需要新建添加用户到用户组的ldif文件，如下：

```
cat > add_user_to_groups.ldif << “EOF”
dn: cn=ldapgroup1,ou=Group,dc=hbgd,dc=com
changetype: modify
add: memberuid
memberuid: ldapuser1
EOF
```

执行如下命令：

```
ldapadd -x -w “xxxxxx” -D “cn=Manager,dc=hbgd,dc=com” -f /root/add_user_to_groups.ldif
```



查询添加的OpenLDAP用户组信息，如下：

```
ldapsearch -LLL -x -D ‘cn=Manager,dc=hbgd,dc=com’ -w “xxxxx” -b ‘dc=hbgd,dc=com’ ‘cn=ldapgroup1
```

通过上图，我们可以很明显的看出ldapuser1用户已经加入到ldapgroup1用户组了。

7.开启OpenLDAP日志访问功能

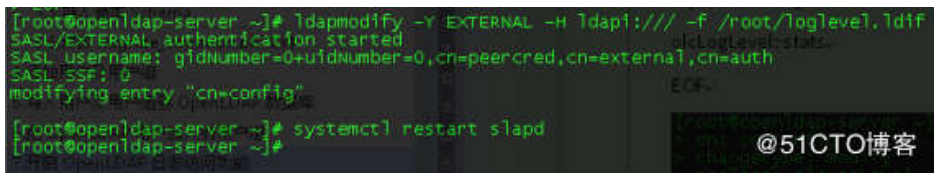
默认情况下OpenLDAP是没有启用日志记录功能的，但是在实际使用过程中，我们为了定位问题需要使用到OpenLDAP日志。
新建日志配置ldif文件，如下：

```
cat > /root/loglevel.ldif << “EOF”
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
EOF
```

导入到OpenLDAP中，并重启OpenLDAP服务，如下：

0 4 羊草

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f /root/loglevel.ldif
systemctl restart slapd
```

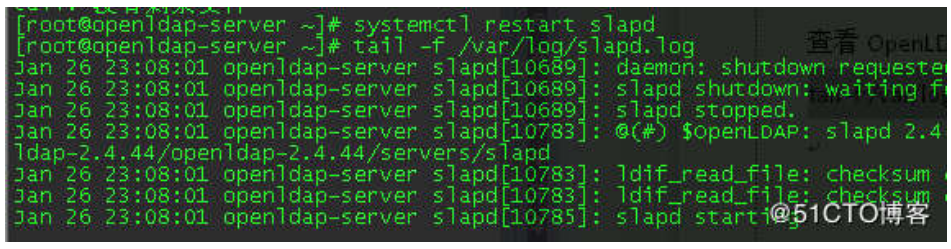


修改rsyslog配置文件，并重启rsyslog服务，如下：

```
cat >> /etc/rsyslog.conf << “EOF”
local4.* /var/log/slapd.log
EOF
systemctl restart rsyslog
```

查看OpenLDAP日志，如下：

```
tail -f /var/log/slapd.log
```



8..安装和配置LDAP管理工具PHPldapadmin

首先安装Apache和PHP：

```
[root@localhost ~]# yum -y install httpd php php-ldap php-gd php-mbstring php-pear php-bcmath php-xml
```

然后安装phpldapadmin：

```
[root@localhost ~]# yum -y install epel-release
[root@localhost ~]# yum --enablerepo=epel -y install phpldapadmin
```

分享

修改配置文件

```
[root@localhost ~]# vim /etc/phpldapadmin/config.php
#397行取消注释，398行添加注释
$servers->setValue('login','attr','dn');
// $servers->setValue('login','attr','uid');

[root@localhost ~]# vim /etc/httpd/conf.d/phpldapadmin.conf

// 修改配置
<IfModule mod_authz_core.c>
# Apache 2.4
Require local
#添加一行内容，指定可访问的ip段（虽然我也不知道为什么，但不填不能运行这个管理工具，我就直接写的本地ip）
Require ip 172.31.101.110
</IfModule>
```

设置开机自启并启动Apache：

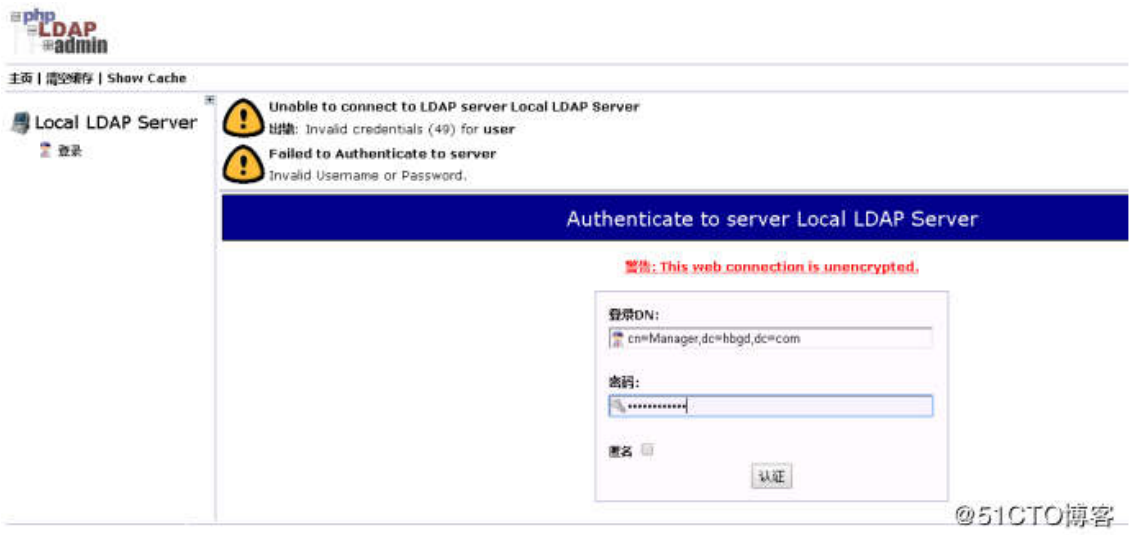
```
[root@localhost ~]# systemctl enable httpd
[root@localhost ~]# systemctl start httpd
```

浏览器访问phpldapadmin：

http://(localhost或服务器地址)/phpldapadmin/

用户名：cn=Manager,dc=hbgd,dc=com

密码：设定的管理员密码



openldap 搭建 linux&zabbix

0 收藏 分享

上一篇：OSPF邻接关系建立 下一篇：网络工程师软件solarwind...

羊草
119篇文章，28W+人气，0粉丝
年轻人，少吐槽，多搬砖

提问和评论都可以，用心的回复会被更多人看到和认可

Ctrl+Enter 发布 取消 发布

4条评论 按时间正序 | 按时间倒序

tokyohuang123
1楼 2018-07-10 20:09:56 1

php没安装成功怎么回事

作者 羊草:@tokyohuang123
报啥错

2018-07-10 21:16:13 回复

血印之风
2楼 2018-07-17 15:18:59 1

请问一下为什么不能用mysql作为数据库啊

作者 羊草:@血印之风
测试mysql，不能正常使用

推荐专栏

基于Kubernetes企业级容器云平台落地与…

容器私有云平台实践之路

共15章 | 李振良OK

订阅

￥51.00 **70人订阅**

VMware vSAN中小企业应用案例

掌握主流虚拟化技术

共42章 | 王春海

订阅

￥51.00 **37人订阅**

负载均衡高手炼成记

高并发架构之路

共15章 | sery

订阅

￥51.00 **150人订阅**

老司机网络运维干货集锦（含路由交换安全…

新西兰资深网工运维之道

共16章 | 姜汁啤酒

订阅

￥51.00 **450人订阅**

带你玩转高可用

前百度高级工程师的架构高可用实战

共15章 | 曹林华

订阅

￥51.00 **237人订阅**

猜你喜欢

linux学习-将seafile启动脚本设置为开机启动服务

用Kibana和logstash快速搭建实时日志查询、收集与分…

企业邮件系统搭建-关于不能往yahoo,sina，hotmail地址…

metricbeat部署及监控linux系统指标汇总

linux工具-journalctl

Java线程：创建与启动

超详细CentOS6.5配置rsync+inotify实现同步

Magent + Keepalived实现Memcached高可用群集

0 4 羊草