一、ldap完整部署（已验证）

主要以centos7.5 为基础系统进行讲解，包括服务端的安装以及客户端

****yum 安装为主****

常用的属性名如下：

|  |
| --- |
| openlda: OpenLDAP服务端和客户端用的库文件 openldap-servers:  服务端程序 openldap-clients:  客户端程序 openldap-devel:  开发包，可选 openldap-servers-sql: 支持sql模块，可选 migrationtools: 实现OpenLDAP用户及用户组的添加，导入系统账户，可选 compat-openldap:  OpenLDAP 兼容性库 |

### **安装OpenLDAP**

|  |
| --- |
| yum -y install openldap \  compat-openldap \  openldap-clients \  openldap-servers \  openldap-servers-sql \  openldap-devel migrationtools  yum clean all && yum makecache |

查看OpenLDAP版本，使用如下命令：

|  |
| --- |
| slapd -VV |

### **2、配置OpenLDAP**

OpenLDAP安装完毕后，接下来我们开始配置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。

生成openldap的管理加密密钥（记下来，下面将用到）

|  |
| --- |
| slappasswd -s admin  {SSHA}YadJTuYz5nk/Pl4keLa60p5JEe85AOiw |

复制 slapd.ldif 到 /etc/openldap 下面

|  |
| --- |
| /bin/cp /usr/share/openldap-servers/slapd.ldif /etc/openldap |

在第83行左右 corba.ldif 下面添加以下内容:

|  |
| --- |
| vim /etc/openldap/slapd.ldif  include: file:///etc/openldap/schema/collective.ldif  include: file:///etc/openldap/schema/corba.ldif  include: file:///etc/openldap/schema/cosine.ldif  include: file:///etc/openldap/schema/duaconf.ldif  include: file:///etc/openldap/schema/dyngroup.ldif  include: file:///etc/openldap/schema/inetorgperson.ldif  include: file:///etc/openldap/schema/java.ldif  include: file:///etc/openldap/schema/misc.ldif  include: file:///etc/openldap/schema/nis.ldif  include: file:///etc/openldap/schema/openldap.ldif  include: file:///etc/openldap/schema/pmi.ldif  include: [file:///etc/openldap/schema/ppolicy.ldif](file://etc\\openldap\\schema\\ppolicy.ldif) |

### **3、或者使用 Schemas 命令导入（要先开启slapd）**

systemctl start slapd

systemctl enable slapd

systemctl status slapd

|  |
| --- |
| ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/collective.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/corba.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/cosine.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/duaconf.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/dyngroup.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/inetorgperson.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/java.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/misc.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/nis.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/openldap.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/pmi.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f /etc/openldap/schema/ppolicy.ldif |

### **4. 修改 /etc/openldap/slapd.ldif文件 Server status monitoring 下面相关内容,在139行**

|  |
| --- |
| olcAccess: to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,c  n=auth" read by dn.base="cn=goodadmin,dc=good,dc=com" read by \* none |

### **5. 修改 /etc/openldap/slapd.ldif文件Backend database definitions 下面为以下内容,在149行**

|  |
| --- |
| olcSuffix: dc=good,dc=com #找到olcSuffix，修改为你的dc  olcRootDN: cn=goodadmin,dc=good,dc=com #找到olcRootDN, 修改为你的用户名  olcRootPW: {SSHA}YadJTuYz5nk/Pl4keLa60p5JEe85AOiw #在文件末尾添加此行，设置是刚才的密码 |

### **6. 查看配置文件目录**

|  |
| --- |
| cd /etc/openldap && tree slapd.d/ |

### **7. 备份配置文件**

|  |
| --- |
| cd /etc/openldap && /bin/mv slapd.d slapd.d.bak  mkdir -p slapd.d |

### **8. 配置配置文件权限**

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

### **9. 初始化生成配置文件**

* -n: 代表写入那个数据库,-n 0 是写在0号这个数据库里
* -F: 指定配置成位置, -F slapd.d 生成在 slapd.d 目录里
* -l: 指定生成哪个slapd.ldif文件

|  |
| --- |
| cd /etc/openldap/  slapadd -n 0 -F slapd.d -l slapd.ldif |

### **10. 复制数据库配置文件到数据库目录里**

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

### **11. 配置数据库目录权限**

|  |
| --- |
| chown -R ldap:ldap /var/lib/ldap /etc/openldap/slapd.d |

### **12. 启动slapd服务区**

|  |
| --- |
| systemctl start slapd |

### **13. slapd服务状态**

|  |
| --- |
| systemctl status slapd |

### **14. 开机启动slapd**

|  |
| --- |
| systemctl enable slapd |

### **15. 查看启动端口**

|  |
| --- |
| ss -tunlp|grep 389 |

### **16、日志配置**

|  |
| --- |
| **日志切割（以下配置不能包含注释）**  # cat > /etc/logrotate.d/slapd <<EOF  /var/log/slapd/slapd.log {  daily  rotate 7  copytruncate  nocompress  dateext  missingok  }  EOF  daily         #每天轮询一次日志      rotate 5      #存储5个日志，超过该数目后的日志将被删除      copytruncate  #复制原日志内容后，将原日志清空，而不创建新文件      nocompress    #切割时不压缩      dateext       #切割时文件名带有日期      missingok     #如果指定的目录不存在，logrotate会报错，此项用来关闭报错    ****测试配置是否有问题****  logrotate -f /etc/logrotate.d/slapd    # mkdir /var/log/slapd  # cat >> /etc/rsyslog.conf << EOF  local4.\* /var/log/slapd/slapd.log  EOF  # systemctl restart rsyslog  # cat > /root/loglevel.ldif << EOF  dn: cn=config  changetype: modify  replace: olcLogLevel  olcLogLevel: stats  EOF  # ldapmodify -Y EXTERNAL -H ldapi:/// -f /root/loglevel.ldif  # systemctl restart slapd |

参考url:

<https://blog.csdn.net/rockstics/article/details/112861652>

### **17. 配置基本域修改为下面值**

|  |
| --- |
| /bin/cp /usr/share/migrationtools/migrate\_common.ph{,\_bak}  vim /usr/share/migrationtools/migrate\_common.ph  $DEFAULT\_MAIL\_DOMAIN = "ldap.good.com"; #71行  $DEFAULT\_BASE = "dc=good,dc=com"; #74行  $EXTENDED\_SCHEMA = 1; #90行 |

### **18. 生成ldif文件**

|  |
| --- |
| mkdir -p /etc/openldap/ldif  /usr/share/migrationtools/migrate\_base.pl > /etc/openldap/ldif/basedomain.ldif |

### **19. 导入数据**

|  |
| --- |
| ldapadd -x -D cn=goodadmin,dc=good,dc=com -W -f /etc/openldap/ldif/basedomain.ldif |

### **20. 使用工具LdapAdmin管理添加一个连接如图**

|  |
| --- |
| **然后我们全部删除手动建一个**   tee /etc/openldap/ldif/config\_init.ldif <<-EOF  dn: dc=good,dc=com  objectclass: dcObject  objectclass: organization  o: https://www.good.com  dc: good  EOF **导入数据** #ldapadd -x -D "cn=goodadmin,dc=good,dc=com" -W -f /etc/openldap/ldif/config\_init.ldif  Enter LDAP Password:  adding new entry "dc=good,dc=com" **查询所有 objectClass=\*** ldapsearch -x -b 'dc=good,dc=com' '(objectClass=\*)'  ldapsearch -H ldapi:/// -Y EXTERNAL -b "cn=config" -LLL –Q  ldapsearch -x -b "dc=good,dc=com" -H ldap://127.0.0.1      **参考url:**  <https://www.fooher.com/20201222_346.html> |

1. **配置 TLS SSL 认证**

OpenLDAP软件设计用于在各种计算环境中运行，从严格控制的封闭网络到全球Internet。因此，OpenLDAP软件支持许多不同的安全机制。

****默认情况下：****

* ldap监听在 389/tcp 端口
* ldaps监听在 636/tcp 端口

#### 1. 配置TLS/SSL创建CA证书

|  |
| --- |
| #yum -y install openssl  #cd /etc/pki/CA  #(umask 077;openssl genrsa -out private/cakey.pem 2048)    #openssl req -new -x509 -key private/cakey.pem -out cacert.pem -days 36500 \  -subj "/C=CN/ST=FJ/L=XM/O=ops/OU=IT/CN=ldap.good.com/emailAddress=Service@good.com"    解决办法：  cd /root && openssl rand -writerand .rnd  #touch index.txt  #echo "01" > serial |

#### 2. ldap服务器端创建证书请求

|  |
| --- |
| #cd /etc/openldap/certs/  #(umask 077;openssl genrsa -out openldapkey236.pem 2048)  这里 -subj 后面内容要和上面一致不然有警告提示  #openssl req -new -key openldapkey236.pem -out openldap236.csr -days 36500 -subj "/C=CN/ST=FJ/L=XM/O=ops/OU=IT/CN=ldap.good.com/emailAddress=Service@good.com" |

#### 3. CA证书服务器签发证书

|  |
| --- |
| #cd /etc/pki/CA  #openssl ca -in /etc/openldap/certs/openldap236.csr -out /etc/pki/CA/certs/openldapcert236.pem -days 36500   显示上面错误,请修改 openssl.cnf 文件,在第42行和330行 **dir = ./demoCA 改为 dir = /etc/pki/CA**  vim /usr/local/openssl/ssl/openssl.cnf      ========================================  最终结果如下：  openssl ca -in /etc/openldap/certs/openldap236.csr -out /etc/pki/CA/certs/openldapcert236.pem -days 36500 |

#### 4. 配置 openldap 证书

|  |
| --- |
| #cd /etc/pki/CA  #/bin/cp /etc/pki/CA/certs/openldapcert236.pem /etc/pki/CA/cacert.pem /etc/openldap/certs/  #chown -R ldap:ldap /etc/openldap/certs  这里执行权限时千万不要把 certs 文件夹设成 0400  chmod -R 0400 /etc/openldap/certs/{openldapcert236.pem,cacert.pem,openldapkey236.pem}  注意:不要有空行,修改下面内容  vim /etc/openldap/slapd.ldif  olcTLSCACertificatePath: /etc/openldap/certs  olcTLSCertificateFile: "OpenLDAP Server"  olcTLSCertificateKeyFile: /etc/openldap/certs/password  改为  olcTLSCertificateFile: /etc/openldap/certs/openldapcert236.pem  olcTLSCertificateKeyFile: /etc/openldap/certs/openldapkey236.pem  olcTLSCACertificateFile: /etc/openldap/certs/cacert.pem  olcTLSVerifyClient: never  注意:在生产环境中重新生成配置文件一定要备份 "/etc/openldap/slapd.d" 这个目录,  防止 slapd.ldif 文件里的配置和 slapd.d 里的配置不一致,不然会导致有的配置不生效或者丢失掉,这里千万要注意.  #systemctl stop slapd  #/bin/mv /etc/openldap/slapd.d /etc/openldap/slapd.d\_bak\_$(date +%Y%m%d%H)  #cd /etc/openldap/ && mkdir -p slapd.d  #chown -R ldap:ldap /etc/openldap/slapd.d  #vim /etc/sysconfig/slapd  修改下面的一行  SLAPD\_URLS="ldapi:/// ldap:///"  改为:  SLAPD\_URLS="ldapi:/// ldap:/// ldaps:///"  **或者修改OpenLDAP默认监听389端口 本实例修改端口配置**  SLAPD\_URLS="ldapi:/// ldap:/// ldaps://0.0.0.0:5973/"  SLAPD\_URLS="ldapi://0.0.0.0:5972/ ldap://0.0.0.0:5972/ ldaps://0.0.0.0:5973/" #**此方法phpldapadmin无法编辑sudo策略**  重启OpenLDAP服务，如下:  #systemctl daemon-reload  #systemctl start slapd.service 此时启动会报错，执行第5步骤的脚本后才能正常启动服务，可以先忽略    #netstat -tunlp |

#### 5. 删除配置文件，重新生成，删除前请备份 使用shell脚本,自动添加配置参数

|  |
| --- |
| cat > /etc/openldap/ldif/config\_init.sh << EOF  #!/bin/bash  export PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin  rm -rf /etc/openldap/slapd.d/\*  slapadd -n -0 -F /etc/openldap/slapd.d -l /etc/openldap/slapd.ldif  chown -R ldap:ldap /etc/openldap/slapd.d  systemctl restart slapd  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/ldif/log.ldif #没有log.ldif可以忽略此条  echo -e "\033[34m 查看配置文件是否添加成功,这里要在全局里找 \033[0m"  cat /etc/openldap/slapd.d/cn\=config.ldif  netstat -tunlp  EOF  #sh /etc/openldap/ldif/config\_init.sh    **验证**  openssl verify -CAfile /etc/openldap/certs/cacert.pem /etc/openldap/certs/openldapcert236.pem |

现在可以通过 LDAP admin 客户端连接 ssl 636 端口 tls测试是否正常，记得要把防火墙636端口要放行.  
注意：如果无法启动ssl,检查证书文件权限,这里没有导入 cacert.pem 证书,状态下会显示 "无法找到该证书的颁发者"

|  |
| --- |
| 开始导出 cacert.pem 证书,用 sz 命令保存到你指定的位置 cd /etc/openldap/certs  sz cacert.pem  然后使用谷哥浏览器在地址栏里输入 "chrome://settings/security" 找到 "管理证书 管理 HTTPS/SSL 证书和设置" 点击进去,选择 "受信任的根证书颁发机构" 最后导入   也可以用使用 快捷键 "Win+R" 运行命令 "certmgr.msc" 进行查看   **参考url:**  <https://www.fooher.com/20210426_365.html> |

1. 安装phpldapadmin

|  |
| --- |
| # yum安装时，会自动安装apache和php的依赖。  # 注意： phpldapadmin很多没更新了，只支持php5，如果你服务器的环境是php7，则会有问题，页面会有各种报错  yum install -y phpldapadmin    # 修改apache的phpldapadmin配置文件  # 修改如下内容，放开外网访问，这里只改了2.4版本的配置，因为centos7 默认安装的apache为2.4版本。所以只需要改2.4版本的配置就可以了  # 如果不知道自己apache版本，执行 rpm -qa|grep httpd 查看apache版本    vim /etc/httpd/conf.d/phpldapadmin.conf  -----------------------------------------------------------------  <IfModule mod\_authz\_core.c>  # Apache 2.4  Require all granted //修改这行就行，其他的不用管  </IfModule>  -----------------------------------------------------------------      # 修改配置用DN登录ldap  vim /etc/phpldapadmin/config.php  # 301行，修改连接ldap的端口（在端口已经修改的情况下）  // $servers->setValue('server','port',389); 去掉注释，修改端口  $servers->setValue('server','port',5972);  注意：修改端口后。此方法无法编辑sudo策略。  # 398行，默认是使用uid进行登录，我这里改为dn.  $servers->setValue('login','attr','dn');    这一行的注释去掉   // $servers->setValue('login','attr','uid');  这一行注释掉    # 460行，关闭匿名登录，否则任何人都可以直接匿名登录查看所有人的信息  $servers->setValue('login','anon\_bind',false); //ture改成false    # 519行，设置用户属性的唯一性，这里我将cn,sn加上了，以确保用户名的唯一性  $servers->setValue('unique','attrs',array('mail','uid','uidNumber','cn','sn'));  -----------------------------------------------------------------      # 启动apache  systemctl restart httpd  systemctl enable httpd |

**登录phpldapadmin界面**

|  |
| --- |
| 在浏览器上访问: http://ip/ldapadmin ，然后使用上面定义的用户，进行登录,如本例用户admin,密码也是admin.      参考url:  <https://blog.csdn.net/weixin_41004350/article/details/89521170> |

1. phpldapadmin 进行增加用户

|  |
| --- |
|  |

# 五、配置SUDO和SSH，为LDAP用户添加SUDO权限

## **查找系统安装的SUDO包中带来的SCHEMA.OPENLDAP文件**

|  |
| --- |
| #rpm -qal | grep sudo | grep -i OpenLDAP |



**2.拷贝该档案到LDAP SCHEMA中**

|  |
| --- |
| #cp /usr/share/doc/sudo-1.8.23/schema.OpenLDAP /etc/openldap/schema/sudo.schema |

**3.再配置SSH部分**

OpenLDAP支持ssh验证需要openssh-dalp包提供

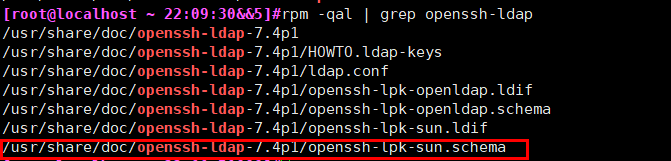
|  |
| --- |
| # yum -y install openssh-ldap |

查找openssh-ldap提供的schema模型

|  |
| --- |
| #rpm -qal | grep openssh-ldap |

我们需要的是openssh-lpk-openldap.schema，将该模型拷贝到openldap的schema中

|  |
| --- |
| #cp /usr/share/doc/openssh-ldap-7.4p1/openssh-lpk-openldap.schema /etc/openldap/schema/ |



**4.导入SUDO.SCHEMA和OPENSSH-LPK-OPENLDAP.SCHEMA**

删除原模型中的配置文件

|  |
| --- |
| # rm -rf /etc/openldap/slapd.d/cn\=config/cn\=schema/\* |

编辑新的模型需求文件

vim /etc/openldap/schema.conf

|  |
| --- |
| include /etc/openldap/schema/core.schema  include /etc/openldap/schema/cosine.schema  include /etc/openldap/schema/inetorgperson.schema  include /etc/openldap/schema/nis.schema  include /etc/openldap/schema/collective.schema  include /etc/openldap/schema/sudo.schema  include /etc/openldap/schema/openssh-lpk-openldap.schema |

注意：*导入的模型可以根据自己的需求自定义要导入哪些模型*

​ *导入一定要注意以上顺序*

​ 重新导入新的LDAP模型

|  |
| --- |
| # slaptest -f /etc/openldap/schema.conf -F /etc/openldap/slapd.d/  # chown -R ldap.ldap /etc/openldap/slapd.d/  # systemctl restart slapd  # systemctl status slapd |

​ 然后我们可以在看到重新生成的模型文件

|  |
| --- |
| # ll /etc/openldap/slapd.d/cn\=config/cn\=schema |

注意：*cn={5}与cn={6}即配置sudo与ssh需要的模型*

​ 最后更改所有模型文件的权限并重启服务

**5.导入SUDO策略模板**

|  |
| --- |
| Phpldapadmin默认不支持sudo策略配置，需要前往一下网址抓取sudo策略template [http://phpldapadmin.sourceforge.net/wiki/index.php/TemplatesContributed:Sudo](http://phpldapadmin.sourceforge.net/wiki/index.php/TemplatesContributed:Sudo" \t "https://www.freesion.com/article/16551246271/_blank)  导入的sudo策略template有两个，  /usr/share/phpldapadmin/templates/creation/sudo.xml  /usr/share/phpldapadmin/templates/modification/sudo.xml |

**6.在PHPLDAPADMIN中配置SUDOERS策略**

先创建sudoers组用来存储sudo策略(创建的OU必须名为sudoers)

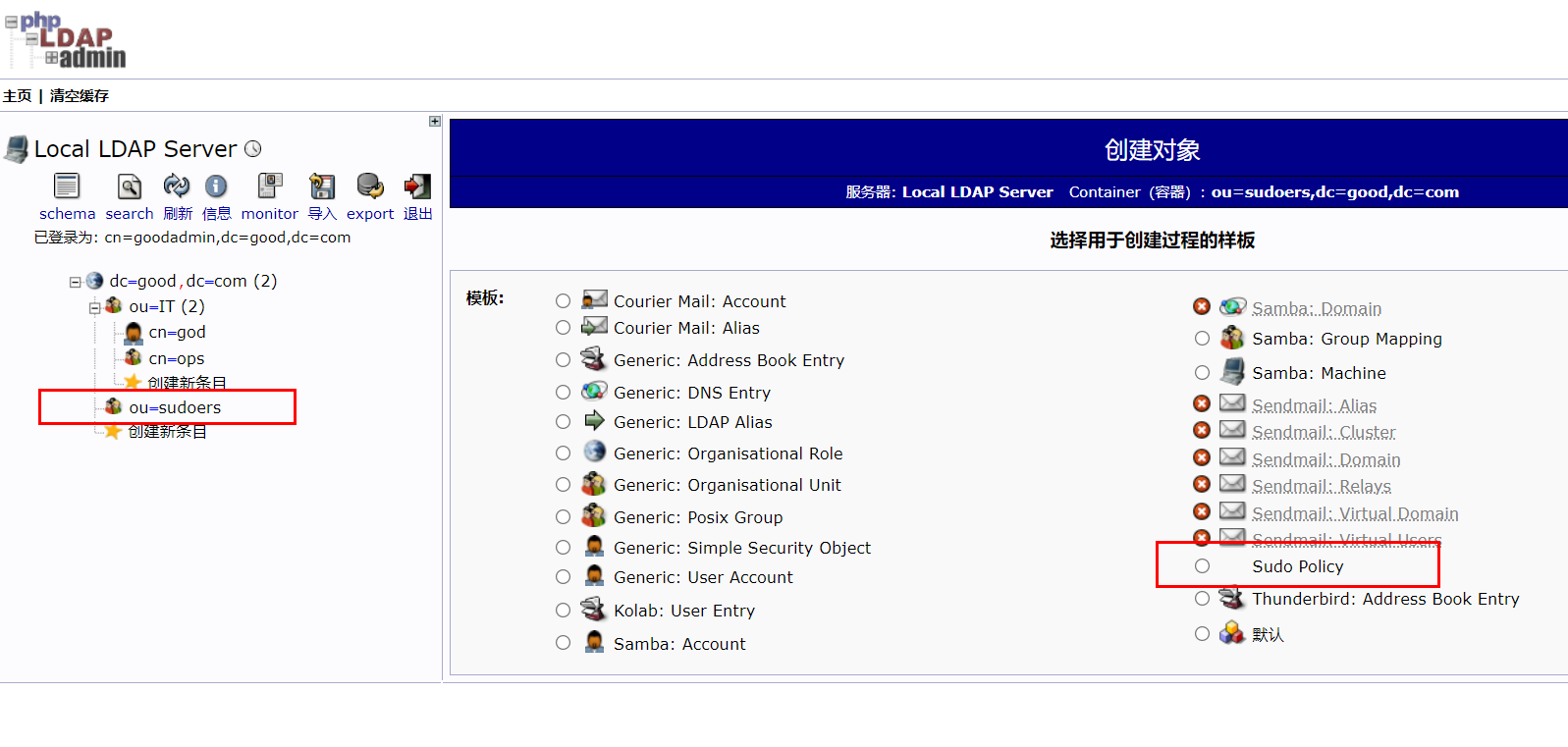


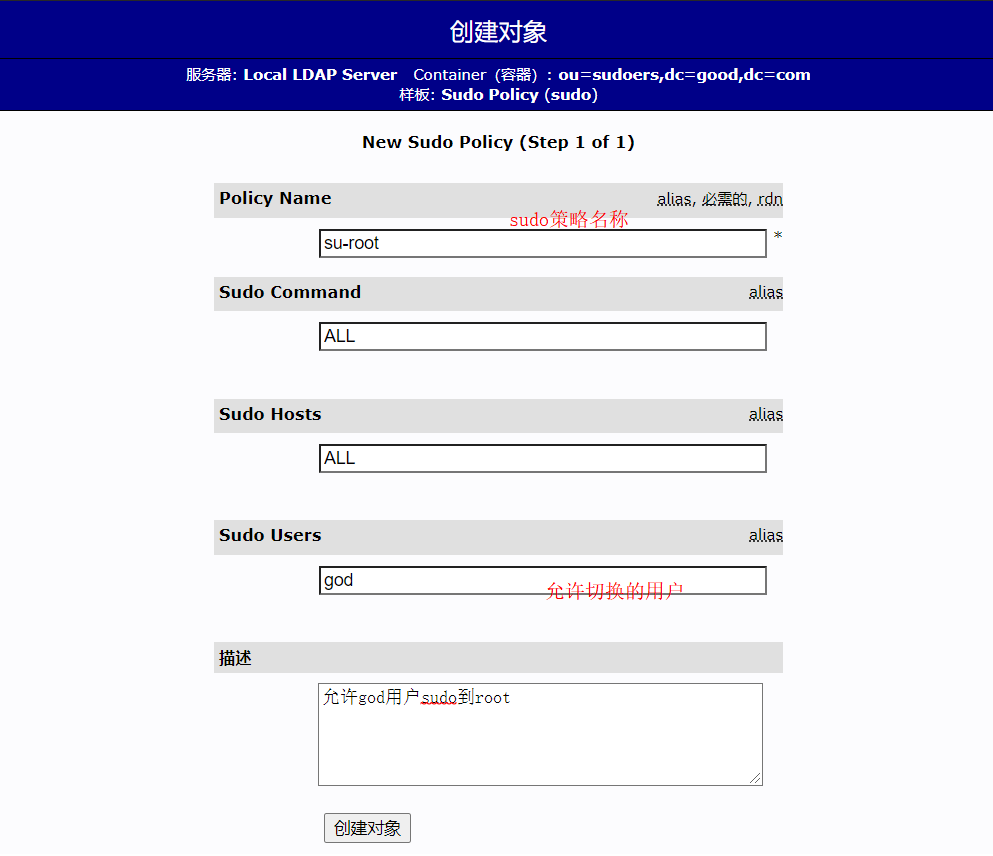


**可能还需要退出重新登录才能看到sudo Policy**

**7.在sudoers组中创建sudo策略**

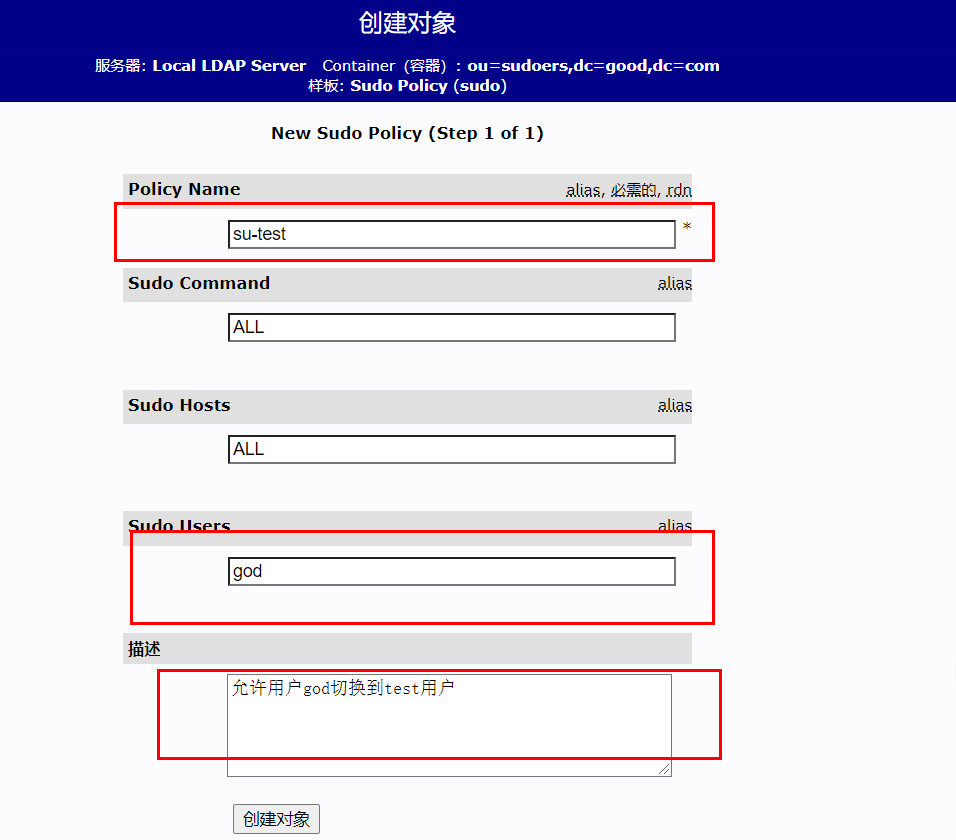
**例一 sudo到root**





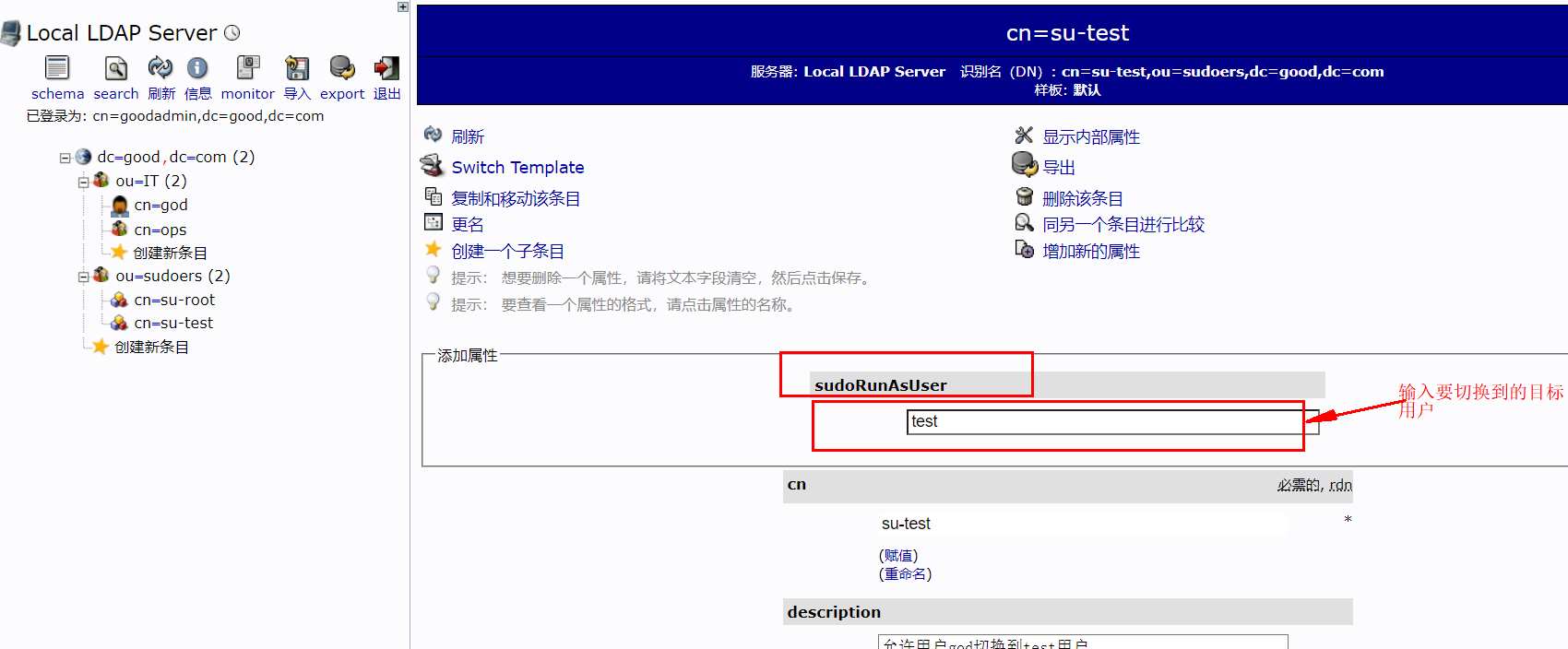
**例二 sudo到 test普通用户 （在要登录的服务器上创建test用户）**







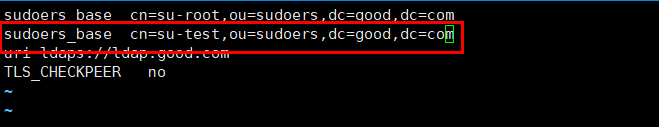
下拉框选择**[sudoRunAsUser](http://192.168.91.11/ldapadmin/cmd.php?cmd=schema&server_id=1&view=attributes&viewvalue=sudorunasuser" \o "Click to view the schema definition for attribute type: sudoRunAsUser)**





[root@localhost ~ 22:52:33&&5]#vim /etc/sudo-ldap.conf

添加：sudoers\_base cn=su-test,ou=sudoers,dc=good,dc=com



1. **登录测试验证:**

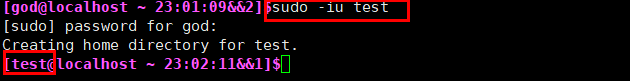
**首先使用安装脚本安装openldap客户端，安装完毕需要重启服务器(不重启服务器，登陆验证很慢需要20几秒的时间。避免踩坑)**

****

普通用户切换到root用户：sudo -i

普通用户切换到普通用户：sudo -iu 用户名

#sudo -iu test



参考url: <https://www.freesion.com/article/16551246271/>

# **六、自助修改密码系统self-service-password**

## 1、配置yum源文件

|  |
| --- |
| # vi /etc/yum.repos.d/ltb-project.repo  [ltb-project-noarch]  name=LTB project packages (noarch)  baseurl=https://ltb-project.org/rpm/$releasever/noarch  enabled=1  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-LTB-project |

## 2、导入库密钥:

|  |
| --- |
| # rpm --import https://ltb-project.org/wiki/lib/RPM-GPG-KEY-LTB-project |

## 3、安装self-service-password

|  |
| --- |
| # yum install self-service-password  升级php5到php7  yum install <http://rpms.remirepo.net/enterprise/remi-release-7.rpm>  yum --enablerepo=remi-php73 install php |

## 4、查看self-service-password安装文件及目录

|  |
| --- |
| # rpm -ql self-service-password |

## 5、修改Apache配置

|  |
| --- |
| ****Apache配置文件所在路径是：/etc/httpd/conf.d/self-service-password.conf**** 只需要修改其中****ServerName****为自己所用域名即可，其他配置无需修改。  # vi /etc/httpd/conf.d/self-service-password.conf |

## 6、修改Self-Service-Password配置

****Self-Service-Password配置文件所在路径是：/usr/share/self-service-password/conf/config.inc.php****

****6.1、**配置LDAP相关信息**

|  |
| --- |
| # vi /usr/share/self-service-password/conf/config.inc.php  # LDAP  $ldap\_url = "ldap://192.168.91.11:389";  $ldap\_starttls = false;  $ldap\_binddn = "cn=goodadmin,dc=good,dc=com";  $ldap\_bindpw = 'admin';  $ldap\_base = "dc=good,dc=com";  $ldap\_login\_attribute = "uid";  $ldap\_fullname\_attribute = "cn";  $ldap\_filter = "(&(objectClass=person)($ldap\_login\_attribute={login}))";  $ldap\_use\_exop\_passwd = false;  $ldap\_use\_ppolicy\_control = false;  $pwd\_min\_length = 8; 　　　 #密码最低8位数  $pwd\_complexity = 3;　　　　　　　　　 #密码复杂度最少为3种字符  $keyphrase = "good";　　　　　　　　　　 #默认是secret，必须改一个其他的字符串  $who\_change\_password = "manager"; #定义使用什么账户来修改密码，如选用manager请确保binddn用户有修改用户密码的权限（建议域管理员身份）  $ad\_options['change\_expired\_password'] = true; #允许用户更改密码，如果密码过期  **注意：本例为了验证方便，密码复杂度按默认设置。如pwd\_min\_length，pwd\_complexity 都设置为0，生产要严格设置。** |

**6.2、配置邮件服务信息**

**邮件**

在密码忘记的时候，可以通过点击此处，服务会给LDAP账号绑定的邮箱发一个重置密码的链接，点击后直接重置密码，无需输入旧密码。注意，此处输入的是LDAP用户名，所以创建用户的时候必须配置用户的邮箱信息，否则收不到邮件。

|  |
| --- |
| ## Mail  # LDAP mail attribute  $mail\_attribute = "mail";  # Get mail address directly from LDAP (only first mail entry)  # and hide mail input field  # default = false  $mail\_address\_use\_ldap = true; #注意此处配置为true，这样重制密码的收信息的邮箱就是用户LDAP上配置的邮箱信息，用户重置密码的时候就不能自己随意输入邮箱，以免违规更改他人密码。  # Who the email should come from  $mail\_from = "751536336@qq.com";  $mail\_from\_name = "DevOps运维组";  $mail\_signature = "";  # Notify users anytime their password is changed  $notify\_on\_change = false;  # PHPMailer configuration (see https://github.com/PHPMailer/PHPMailer)  $mail\_sendmailpath = '/usr/sbin/sendmail'; #yum安装 yum install -y sendmail  $mail\_protocol = 'smtp';  $mail\_smtp\_debug = 0;  $mail\_debug\_format = 'html';  $mail\_smtp\_host = 'smtp.qq.com';  $mail\_smtp\_auth = true;  $mail\_smtp\_user = '751536336@qq.com';  $mail\_smtp\_pass = 'jjueigohmavibcbi'; #这个需要登陆QQ邮箱网页去生成授权码  $mail\_smtp\_port = 465;  $mail\_smtp\_timeout = 30;  $mail\_smtp\_keepalive = false;  $mail\_smtp\_secure = 'ssl'; #注意这里ssl不是tls，tls 会导致邮件发不出去  $mail\_smtp\_autotls = true;  $mail\_smtp\_options = array();  $mail\_contenttype = 'text/plain';  $mail\_wordwrap = 0;  $mail\_charset = 'utf-8';  $mail\_priority = 3; |

参考url: <https://www.cnblogs.com/fanggege/p/14252813.html>

登录验证是否能打开。

|  |
| --- |
|  |

**6.3、QQ邮箱授权码生成**

|  |
| --- |
| 1. 登录网页版QQ邮箱 2>设置 3>账户 4>生成授权码 （在第三方客户端的密码框里面输入16位授权码进行验证）         官方设置步骤url：  <https://service.mail.qq.com/cgi-bin/help?subtype=1&&no=1001256&&id=28> |

**6.4 发送邮箱验证**

|  |
| --- |
| 1. 选择邮件修改     由于mail\_address\_use\_ldap = true 设置为true,所以只需输入用户名。  2 发送成功    3、到自己所在邮箱查看，此时已收到修改密码的邮件。 |

遇到的问题

|  |
| --- |
| **1、Token encryption requires a random string in keyphrase setting**    $keyphrase = "secret";  随意修改，只要不是默认的值就行，否则会报错  2、密码被LDAP服务器拒绝    who\_change\_password 修改为manager //定义使用什么账户来修改密码 |