

## 系统集成

### 1. 安装 LDAP

参考文档：<https://www.cnblogs.com/mascot1/p/10498392.html>

#### 1.1 先决条件

```
#关闭 SELINUX
vim /etc/sysconfig/selinux    # SELINUX=disabled
setenforce 0
```

```
#关闭防火墙
systemctl stop firewalld
systemctl disable firewalld
```

#### 1.2 安装 ldap

```
#安装了 ldap 工具
yum install -y openldap-servers openldap-clients migrationtools
slappasswd    #据提示输入密码会返回加密的密码字符串，保存好这个字符串
```

```
#配置数据库缓存
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown -R ldap:ldap /var/lib/ldap/
```

```
#测试配置文件
slaptest -u    #出现 configfile testing succeeded 说明成功了
```

```
#启动 ldap
systemctl start slapd.service
systemctl enable slapd.service
```

```
#导入模板
ls /etc/openldap/schema/*.ldif | xargs -l {} sudo ldapadd -Y EXTERNAL -H ldapi:/// -f {}
```

### 2. 安装 LDAP 控制台

#### 2.1 先决条件

```
#安装 apache
yum -y install httpd
```

```
#修改配置文件
vim /etc/httpd/conf/httpd.conf #AllowOverride all

#启动服务测试
systemctl start httpd
systemctl enable httpd
curl 127.0.0.1
```

## 2.2 安装 phpldapadmin

```
#安装 phpldapadmin
cat /etc/yum.repos.d/epel.repo
[epel]
name=Extra Packages for Enterprise Linux 7 - $basearch
baseurl=https://mirrors.tuna.tsinghua.edu.cn/epel/7Server/x86_64/
enabled=1
gpgcheck=0

yum install phpldapadmin
```

## 2.3 更改配置文件

```
#修改配置文件
vim /etc/phpldapadmin/config.php
$servers->setValue('server','host','127.0.0.1');
$servers->setValue('server','port',389);
$servers->setValue('server','base',array('dc=my-domain,dc=com'));
$servers->setValue('login','auth_type','session');
$servers->setValue('login','attr','dn');

$servers->setValue('login','attr','dn'); #注释掉

#修改 httpd 配置文件
vim /etc/httpd/conf.d/phpldapadmin.conf
Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>
    <IfModule mod_authz_core.c>
        # Apache 2.4
        Require local
        Require ip 192.168.0
    </IfModule>
    <IfModule !mod_authz_core.c>
```

```
# Apache 2.2
Order Deny,Allow
Deny from all
Allow from 127.0.0.1
Allow from ::1
</IfModule>
</Directory>

#创建基础目录
vim /etc/openldap/base.ldif
dn: dc=my-domain,dc=com
o: ldap
objectclass: dcObject
objectclass: organization
dc: my-domain
```

## 2.4 访问测试

```
#重启 httpd 服务
service restart httpd
#访问测试
http://192.168.0.41/phpldapadmin
```

## 3. LDAP 创建组织

参考文档：<https://www.cnblogs.com/mascot1/p/10498460.html>

### 3.1 创建 OU



选择 Organisational unit 组织单元

创建对象

服务器: Local LDAP Server Container (容器): dc=my-domain,dc=com

选择用于创建过程的样板

模板:

☐ Courier Mail: Account  
☐ Courier Mail: Alias  
☐ Generic: Address Book Entry  
☐ Generic: DNS Entry  
☐ Generic: LDAP Alias  
☐ Generic: Organisational Role  
☒ Generic: Organisational Unit  
☐ Generic: Posix Group

☒ Samba: Domain  
☐ Samba: Group Mapping  
☐ Samba: Machine  
☒ Sendmail: Alias  
☒ Sendmail: Cluster  
☒ Sendmail: Domain  
☒ Sendmail: Relays  
☒ Sendmail: Virtual Domain

输入 OU 名称

创建对象

服务器: Local LDAP Server Container (容器): dc=my-domain,dc=com  
样板: Generic: Organisational Unit (ou)

New Organisational Unit (Step 1 of 1)

组织化单元(Organizational Unit)

alias, 必需的, rdn, 提示

jenkins

创建对象

提交信息

Create LDAP Entry

服务器: Local LDAP Server Container (容器): dc=my-domain,dc=com

Do you want to create this entry?

属性	新值	跳过
ou=jenkins,dc=my-domain,dc=com		
Organisational Unit	jenkins	<input type="checkbox"/>
objectClass	organizationalUnit	<input type="checkbox"/>

提交 取消

查看结果

Local LDAP Server

schema search 刷新 信息 monitor 导入 export 退出

已登录为: cn=Manager,dc=my-domain,dc=com

dc=my-domain,dc=com (2)

ou=devops (1)

ou=jenkins

创建新条目

ou=jenkins

服务器: Local LDAP Server 识别名 (DN): ou=jenkins,dc=my-domain,dc=com 样板: 默认

刷新

Switch Template

复制和移动该条目

更名

创建一个子条目

提示: 想要删除一个属性, 请将文本字段清空, 然后点击保存。

提示: 要查看一个属性的格式, 请点击属性的名称。

显示内部属性

导出

删除该条目

同另一个条目进行!

增加新的属性

objectClass

## 3.2 创建人员

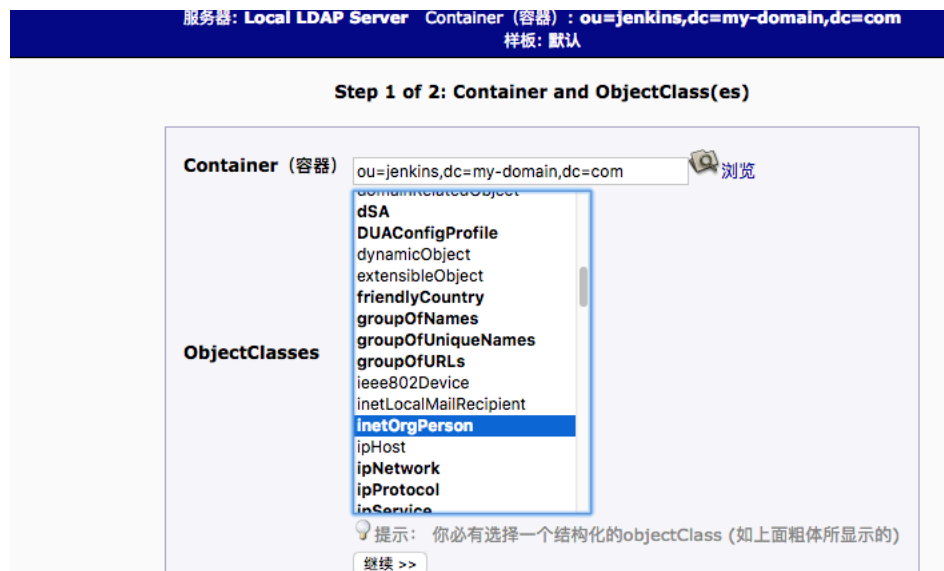
选择 OU->选择新建子条目



选择默认模板



选择 inetorgperson



填写并提交信息

服务器: Local LDAP Server Container (容器) : ou=jenkins,dc=my-domain,dc=com

Do you want to create this entry?

属性	新值	跳过
<b>cn=test2,ou=jenkins,dc=my-domain,dc=com</b>		
cn	test2	<input type="checkbox"/>
objectClass	inetOrgPerson	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
sn	test2	<input type="checkbox"/>

用户创建完成

**Local LDAP Server**

schema search 刷新 信息 monitor 导入 export 退出

已登录为: cn=Manager,dc=my-domain,dc=com

- dc=my-domain,dc=com (2)
  - ou=devops (1)
    - cn=test1
    - 创建新条目
  - ou=jenkins (1+)
    - cn=test2
    - 创建新条目

**创建条目**

Creation successful! DN: **cn=test2,ou=jenkins,dc=**

服务器: Local LDAP Server 识别

刷新

Switch Template

复制和移动该条目

更名

创建一个子条目

提示: 想要删除一个属性, 请将文本字段清空, 然后点击保

提示: 要查看一个属性的格式, 请点击属性的名称。

## 4. Jenkins 集成 LDAP

参考文档: <https://www.cnblogs.com/mascot1/p/10498513.html>

### 4.1 先决条件

- 1.准备一个 adminDN 账号用于查询用户。 cn=Manager,dc=my-domain,dc=com
- 2.将访问 Jenkins 的用户放到一个 OU 中。 ou=jenkins,dc=my-domain,dc=com
- 3.提供 ldap 服务器地址。 ldap://192.168.0.41:389

### 4.2 Jenkins 配置

安装 ldap 插件

Filter:

Enabled	Name ↓	Version	Previously installed version	Uninstall
<input checked="" type="checkbox"/>	<a href="#">bouncycastle API Plugin</a> This plugin provides an stable API to Bouncy Castle related tasks.	<a href="#">2.17</a>		<input type="button" value="Uninstall"/>
<input checked="" type="checkbox"/>	<a href="#">Command Agent Launcher Plugin</a> Allows agents to be launched using a specified command.	<a href="#">1.3</a>		<input type="button" value="Uninstall"/>
<input checked="" type="checkbox"/>	<a href="#">JDK Tool Plugin</a> Allows the JDK tool to be installed via download from Oracle's website.	<a href="#">1.2</a>		<input type="button" value="Uninstall"/>
<input checked="" type="checkbox"/>	<a href="#">LDAP Plugin</a> Adds LDAP authentication to Jenkins	<a href="#">1.20</a>		<input type="button" value="Uninstall"/>
<input checked="" type="checkbox"/>	<a href="#">Mailer Plugin</a> This plugin allows you to configure email notifications for build results	<a href="#">1.23</a>		<input type="button" value="Uninstall"/>

# 全局安全配置

Access Control

Security Realm

Jenkins专有用户数据库

LDAP

服务器

Server

ldap://192.168.0.41:389

root DN

Allow blank rootDN

User search base

ou=jenkins,dc=my-domain,dc=com

User search filter

cn={0}

Group search base

ou=jenkins,dc=my-domain,dc=com

Group search filter

Group membership

Parse user attribute for list of LDAP groups

Search for LDAP groups containing user

Group membership filter

Manager DN

cn=Manager,dc=my-domain,dc=com

Manager Password

.....

Display Name LDAP attribute

displayName

Email Address LDAP attribute

mail

Environment Properties

Add

Ignore if Unavailable

Add Server

Delete

Test LDAP settings

Advanced Configuration...

Servlet容器代理

Authorization

任何用户可以做任何事(没有任何限制)

Save

Apply

选择账号测试，出现一下信息集成完毕

Add Server

Test LDAP settings

Login

✓ **Authentication: successful**  
✓ **User ID: test2**  
✓ **User Dn: cn=test2,ou=jenkins,dc=my-domain,dc=com**  
No display name specified for user!  
Is the LDAP attribute name "displayname" correct?  
Available LDAP attributes are:

- ⚠
- userPassword
  - objectClass
  - sn
  - cn

No email address specified for user!  
Is the LDAP attribute name "mail" correct?  
Available LDAP attributes are:

- ⚠
- userPassword
  - objectClass
  - sn
  - cn

No LDAP group membership reported.  
⚠ If the user is a member of some LDAP groups then the group membership settings are probably configured incorrectly.

Lookup

✓ **User lookup: successful**  
✓ **User groups consistent (login and lookup)**  
⚠ LDAP Group lookup: could not verify.  
Please try with a user that is a member of at least one LDAP group.

Advanced Configuration...