**统一登录部署**

# 总体部署架构



# OpenLDAP部署

**安装相关软件**

yum install openldap openldap-servers openldap-clients openldap-devel compat-openldap -y

**2、创建OpenLDAP的数据库配置文件**

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

cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

chown -R ldap.ldap /var/lib/ldap/

chown -R ldap.ldap /etc/openldap/

**3.修改LDAP的ldap.conf主配置文件**

cp /etc/openldap/ldap.conf /etc/openldap/ldap.conf.bak

vim /etc/openldap/ldap.conf

增加：

BASE dc=wonhigh,dc=com

URI ldap://172.17.210.75

**4、创建LDAP登录密码，修改LDAP的slapd.conf主配置文件。**

4.1 创建LDAP登录密码

slappasswd

输入密码

{SSHA}EuNl6ZK2hMeJ5g0veDP/tplP+DR4R1Jx

4.2 修改LDAP的slapd.conf

cp /etc/openldap/slapd.conf /etc/openldap/slapd.conf.bak

vim /etc/openldap/slapd.conf

by dn.exact="cn=Manager,dc=wonhigh,dc=com" read #第107行

suffix "dc=wonhigh,dc=com" #第115行

rootdn "cn=Manager,dc=wonhigh,dc=com" #第117行

rootpw {SSHA}EuNl6ZK2hMeJ5g0veDP/tplP+DR4R1Jx

**5、添加openLDAP日志功能**

vim /etc/openldap/slapd.conf

loglevel 296 #第5行

vim /etc/rsyslog.conf

local4.\* /data/logs/ldap.log #第15行

touch /data/logs/ldap.log

chown ldap.ldap /data/logs/ldap.log

**6、默认情况下，在/etc/openldap/slapd.d/目录下有很一些默认的配置文件，这里需要删除，重新建立，这一步很重要。**

rm -rf /etc/openldap/slapd.d/\*

chown ldap.ldap /var/lib/ldap/

/etc/init.d/slapd restart

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

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

**7、查看下slapd是否启动，使用netstat命令/ps命令**

ps -ef |grep slapd |grep -v grep #获取openldap进程的状态

netstat -ntplu |grep -i :389 #获取openldap默认监听的端口

**8.测试查找内容**

ldapsearch -LLL -W -x -H ldap:/// -D "cn=Manager,dc=wonhigh,dc=com"

**9.为ldap master初始化数据(如果不初始化，后面无法通过web界面管理)**

增加初始的入口(entries)

1) 创建LDIF文件

编辑一个LDIF格式文件：

cd /tmp

# vim base.ldif

dn: dc=wonhigh, dc=com

dc: wonhigh

objectClass: top

objectClass: domain

dn: ou=people, dc=wonhigh, dc=com

ou: people

objectClass: top

objectClass: organizationalUnit

dn: ou=group, dc=wonhigh, dc=com

ou: group

objectClass: top

objectClass: organizationalUnit

添加：

ldapadd -x -H ldap:/// -D "cn=Manager,dc=wonhigh,dc=com" -W -f /tmp/base.ldif

查询：

ldapsearch -x -LLL

安装migrationtools

yum install migrationtools -y

vim /usr/share/migrationtools/migrate\_common.ph

# Default DNS domain

$DEFAULT\_MAIL\_DOMAIN = "wonhigh.com";

# Default base

$DEFAULT\_BASE = "dc=wonhigh,dc=com";

/usr/share/migrationtools/migrate\_base.pl > /tmp/base.ldif

ldapadd -x -D "cn=Manager,dc=wonhigh,dc=com" -W -f /tmp/base.ldif

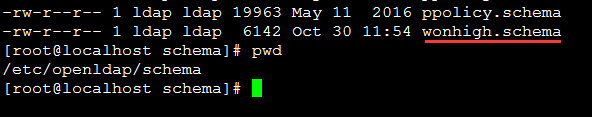
**二、openLDAP 自定义schema**

覆盖系统自带的schema文件：core.schema cosine.schema 见附件。

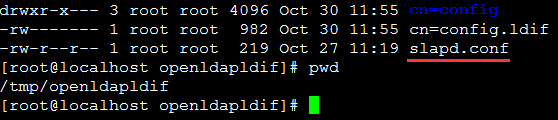
将两个文件导入目录 /etc/openldap/schema

从ApacheDS导出wonhigh.schema，见附件：wonhigh.schema

拷贝至openLDAP的如下路径：/etc/openldap/schema



在/tmp新建目录openldapldif，新建文件：slapd.conf



[root@localhost openldapldif]# vim slapd.conf

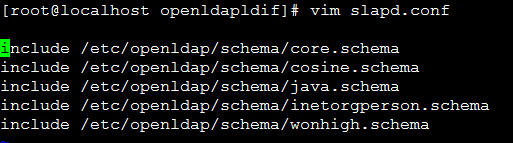
include /etc/openldap/schema/core.schema

include /etc/openldap/schema/cosine.schema

include /etc/openldap/schema/java.schema

include /etc/openldap/schema/inetorgperson.schema

include /etc/openldap/schema/wonhigh.schema



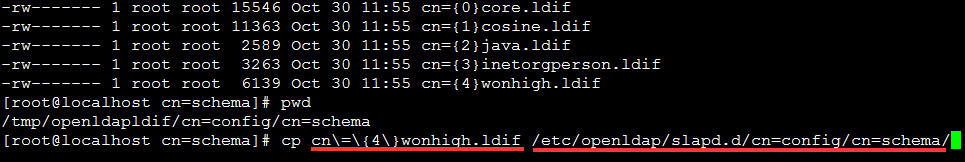
注：如果/tmp/openldapldif下有cn=config，则先删除。

之后运行，slapcat -f /tmp/openldapldif/slapd.conf -F /tmp/ -n0

把生成的的cn=config/cn=schema目录下对应的ldif文件去替换ldap中原先cn=config/cn=schema中的ldif文件。

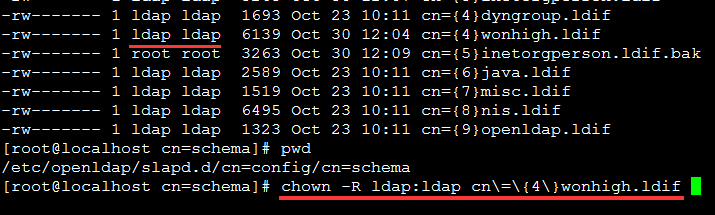
位置在：/etc/openldap/slapd.d/cn=config/cn=schema

cp cn\=\{4\}wonhigh.ldif /etc/openldap/slapd.d/cn=config/cn=schema



重启之前，对刚替换的ldif文件进行赋予权限。

chown -R ldap:ldap cn\=\{4\}wonhigh.ldif



重启服务器：/etc/init.d/slapd restart

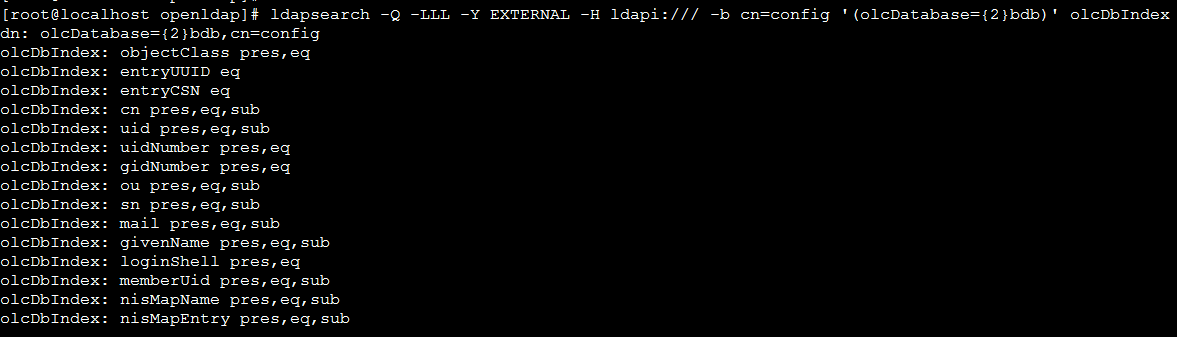
**三、openLDAP 查询、创建索引**

查询现有索引：

要创建索引具体步骤如下：

1.通过ldapsearch 命令查看当前olcDatabase={2}hdb 有哪些索引

ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcDatabase={2}bdb)' olcDbIndex



上述结果显示当前数据库文件没有关于“mobile pres,eq,sub”索引的信息。

2.创建一个ldif 文件，用于存放索引命令

cat >> hdb-index.ldif << EOF

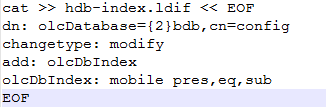
dn: olcDatabase={2}bdb,cn=config

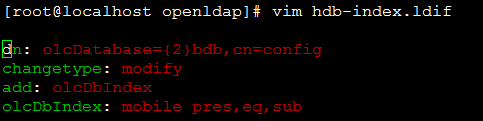
changetype: modify

add: olcDbIndex

olcDbIndex: mobile pres,eq,sub

EOF



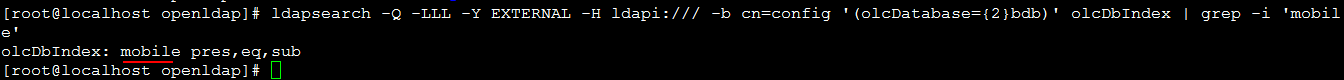


3.通过ldapmodify 命令创建olcDatabase={2}hdb 数据库相关索引条目

ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f hdb-index.ldif

4.通过ldapsearch 进行验证，是否“mobile pres，eq sub”添加成功

ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcDatabase={2}bdb)' olcDbIndex | grep -i 'mobile'



# ApacheDS部署

## Linux上部署ApacheDS

useradd apacheds

passwd apacheds

wget http://mirrors.hust.edu.cn/apache//directory/apacheds/dist/2.0.0-M24/apacheds-2.0.0-M24-64bit.bin

chmod a+x \*.bin

./apacheds-2.0.0-M24-64bit.bin

安装目录：

Where do you want to install ApacheDS? [Default: /opt/apacheds-2.0.0-M24]

/usr/local/apacheds-2.0.0-M24

Where do you want to install ApacheDS instances? [Default: /var/lib/apacheds-2.0.0-M24]

/data/apacheds-2.0.0-M24

其他都是默认回车

修改配置文件（执行以下脚本即可）：

sed -i 's/#wrapper.java.initmemory=1024/wrapper.java.initmemory=1024/g' /usr/local/apacheds-2.0.0-M24/conf/wrapper.conf

sed -i 's/#wrapper.java.maxmemory=2048/wrapper.java.maxmemory=2048/g' /usr/local/apacheds-2.0.0-M24/conf/wrapper.conf

sed -i 's/wrapper.logfile.maxsize=1m/wrapper.logfile.maxsize=100m/g' /usr/local/apacheds-2.0.0-M24/conf/wrapper.conf

sed -i 's/wrapper.logfile.maxfiles=5/wrapper.logfile.maxfiles=50/g' /usr/local/apacheds-2.0.0-M24/conf/wrapper.conf

启动：/etc/init.d/apacheds-2.0.0-M24-default start

## 安装客户端并测试连接

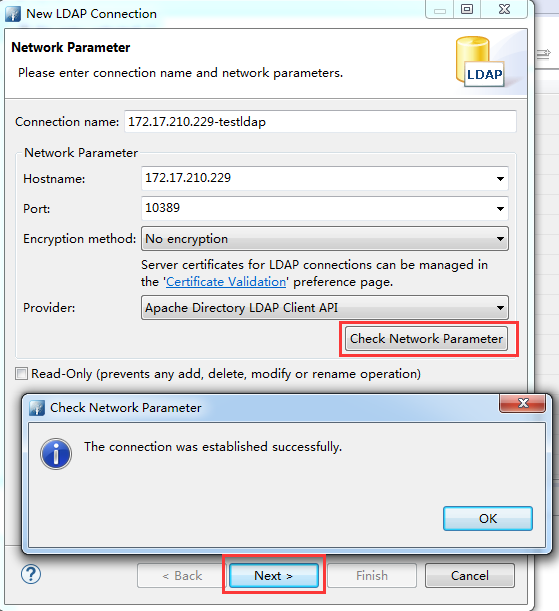
下载

<http://mirror.bit.edu.cn/apache/directory/studio/2.0.0.v20170904-M13/ApacheDirectoryStudio-2.0.0.v20170904-M13-win32.win32.x86_64.exe>

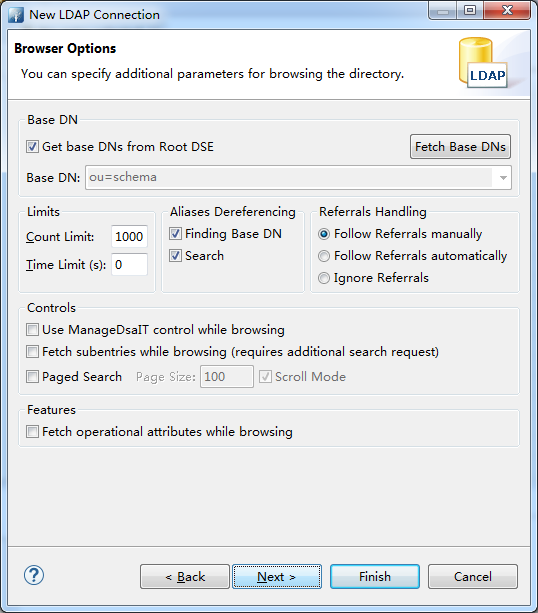
### New LDAP Connection

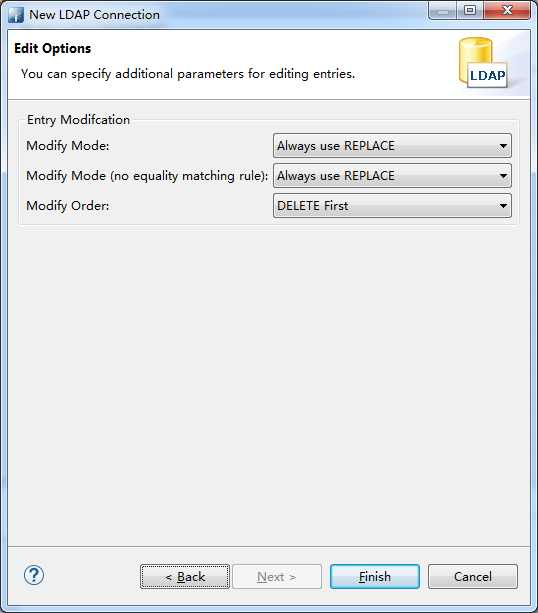
安装后连接服务端：

Hostname填写服务端ip，端口为10389（apacheds默认的端口）

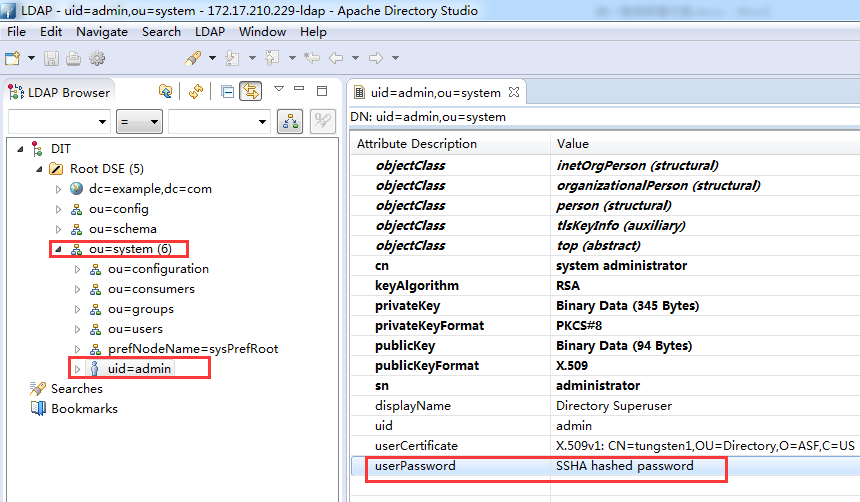


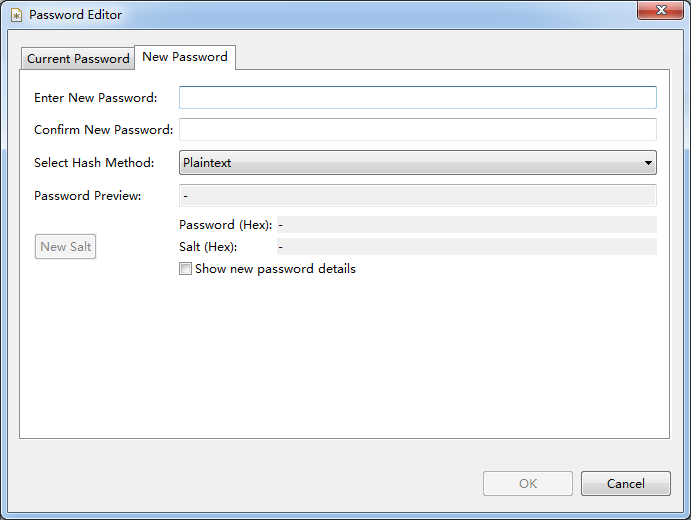
输入dn和password  
Dn：uid=admin,ou=system  
Password:secret





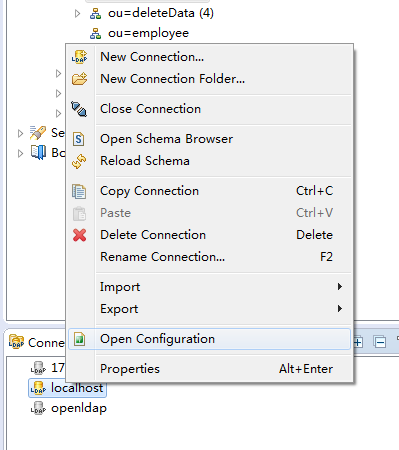
## 修改管理员密码



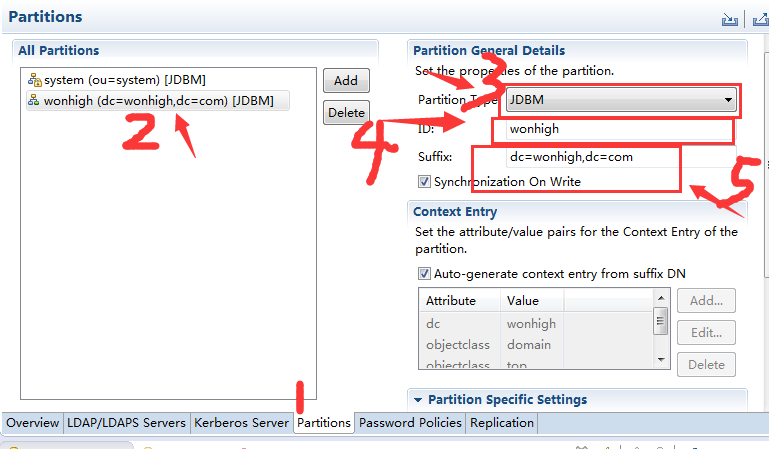


## Apacheds 新建wonhigh根节点

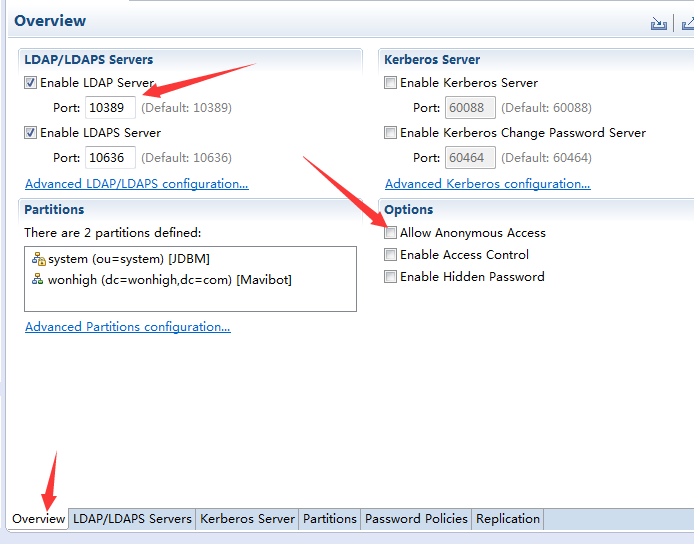
选择connection，右击选择open configuration



修改example节点名称为wonhigh，为确保成功，保存后重启ldap服务，再查看是否修改成功。



取消匿名访问和端口修改



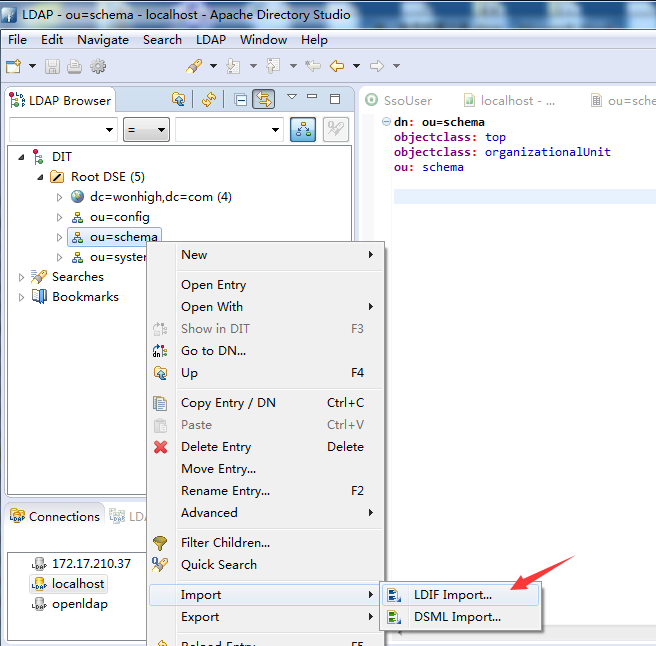
## Apacheds Schema导入

通过schema 来自定义数据结构，只有导入了数据结构文件后才能正常的读写ldap。

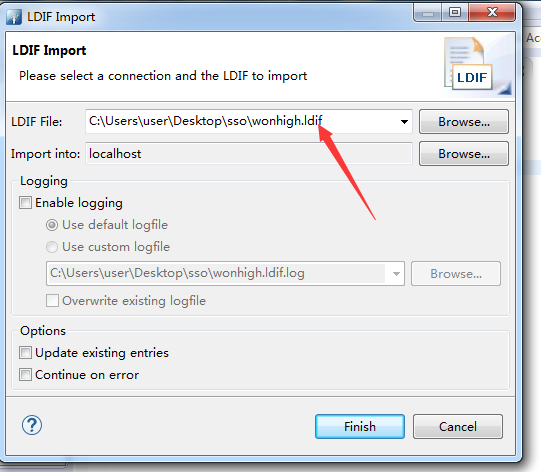
数据结构文件见附件。

### 通过Apache Diectory Studio导入

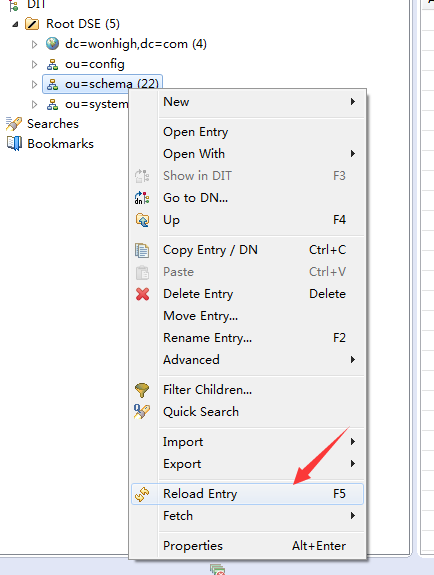
选择ou=schema节点，右键单击—>Import 🡪LDIF Import



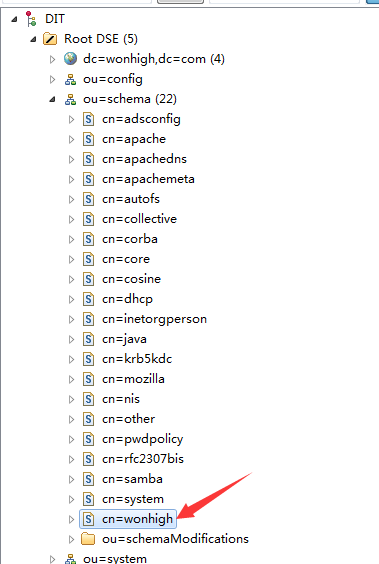
选择要导入的schema 文件

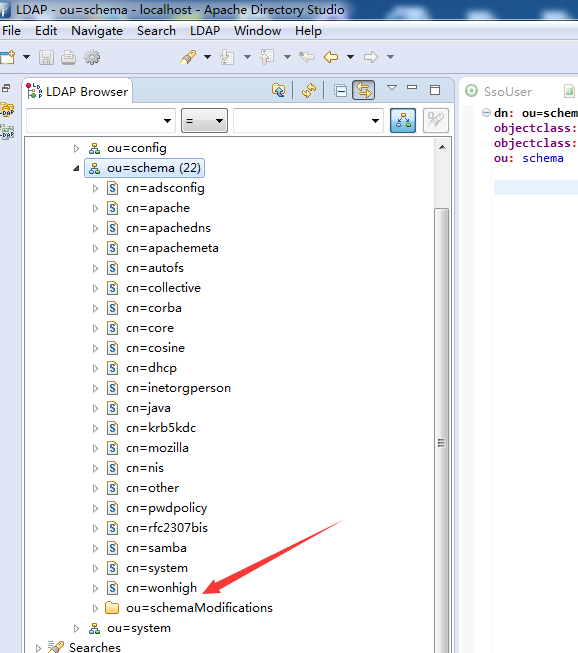


导入成功后，刷新ou=schema节点



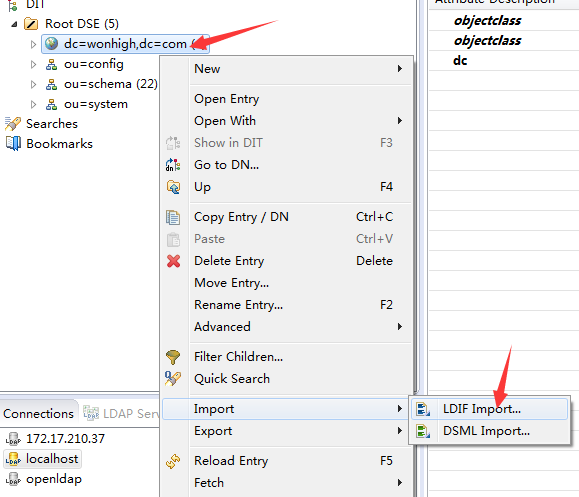
展开ou=schema节点 能够看到 wonhigh节点 表示导入成功。

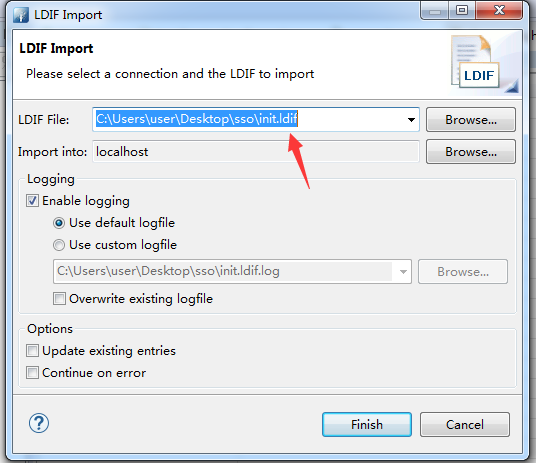


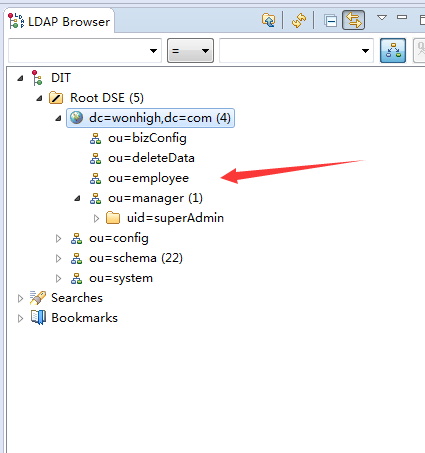


## Apacheds 初始化目录节点

选择 wonhigh 节点 导入init.ldif 数据







## 集群部署

### LDAP高可用与负载均衡部署架构



### LDAP Server主从配置

Slave上导入slave.ldif（在ou=config上导入）：

dn: ads-replConsumerId=consumer1,ou=replConsumers,ads-serverId=ldapServer,ou=servers,ads-directoryServiceId=default,ou=config

ads-replconsumerid: consumer1

ads-replstrictcertvalidation: FALSE

ads-replusetls: FALSE

ads-replsearchtimeout: 0

ads-replsearchfilter: (objectClass=\*)

ads-replsearchsizelimit: 0

ads-replattributes: \*

ads-replrefreshinterval: 60000

ads-repluserpassword: 123456

ads-repluserdn: uid=admin,ou=system

ads-replprovport: 10389

ads-replprovhostname: 172.17.210.229

ads-replrefreshnpersist: TRUE

ads-replsearchscope: sub

ads-searchbasedn: dc=wonhigh,dc=com

ads-enabled: TRUE

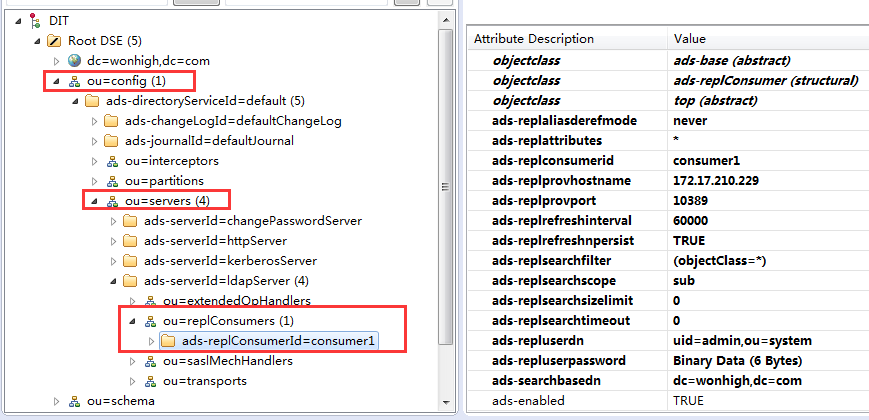
objectclass: ads-replConsumer

objectclass: ads-base

objectclass: top

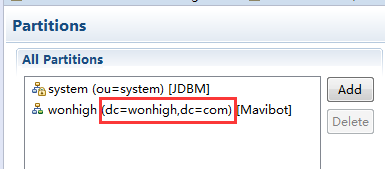
ads-replaliasderefmode: never

导入后的状态：



注意事项：

必须在主从上都提前建好partition。如本例中ads-searchbasedn: dc=wonhigh,dc=com，必须先建好partition，如下：



建好partition之后，若不生效，重启下apacheds服务端。

### LVS+keepalived配置

LVS、keepalived安装略。若需要把wiki上的搬过来

配置文件参考附件中keepalived.zip，realserver.sh

### 如何保证只在master上执行写操作？

写操作主要在SSO-ADMIN系统，写操作直连master

SSO-Server系统登录查询较多，通过vip连接LDAP server。

可以使用多数据源来支持读写分离。

# MySQL部署

## 单个mysql部署

Mysql使用5.7版本。

使用DBA提供的部署脚本一键安装。

## 主从配置

略。

## 数据初始化

**建立sso库**：

CREATE DATABASE IF NOT EXISTS sso default charset utf8 COLLATE utf8\_bin;

**导入初始化脚本**：

脚本在sso-admin的部署包中：platform-bs-sso-admin-web-xxx.yyyyMMddHHmm.zip/sql/

## 组织单元信息表同步

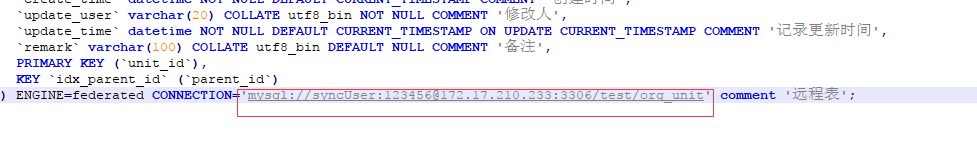
此功能是将HR系统数据库中的组织单元信息表的数据定时同步到SSO数据库中。需要操作的步骤如下

1. **在SSO数据库中，开启federated引擎和事件调度器**
   1. 在/etc/my.cnf文件的[mysqld]任意位置新增一行并插入“federated”
   2. 在/etc/my.cnf文件的[mysqld]任意位置新增一行并插入“event\_scheduler=1”
   3. 重启mysql
   4. 进入mysql执行“show engines;”发现“FEDERATED”的Support属性为“Yes”表示federated引擎开启成功
2. **在HR系统数据库中，给SSO数据库用户赋权，使SSO数据库用户能查询HR系统数据库中的组织单元信息表信息（org\_unit）。**

执行语句如下：

grant select on hrms.org\_unit to sso@'172.17.210.124' identified by '123456';

1. **在SSO数据库中，新建组织单元信息表结构，需要与HR系统数据库中组织单元信息表严格保持一致**
2. **在SSO数据库中，修改附件中的脚本create\_org\_unit\_temp.sql的参数并执行，来新建组织单元信息远程表org\_unit\_temp（表结构与组织单元信息表保持一致）**
3. 需要修改的部分如图：



需要修改的属性如下

CONNECTION='mysql://sso:123456@172.17.210.233:3306/ hrms/org\_unit'

1. 验证：

select count(\*) from org\_unit\_temp 就能看到HR系统数据库的数据了

1. **执行附件的produce\_and\_event.sql脚本，定义存储过程和事件**

手动调用call sp\_syncTable() 可测试同步功能

# SSO-CAS部署

## 单个SSO-CAS实例的部署

端口号：

部署路径：/usr/local/wonhigh/sso-cas-3200

日志路径：/data/logs/sso-cas-3200

配置文件路径：/etc/wonhighconf/sso-cas-3200

Tomcat路径：/usr/local/tomcat-x.x.x-3200(其中的x.x.x表示tomcat的版本号)

**部署步骤**：

1、Tomcat部署略。

mkdir -p /usr/local/wonhigh

mkdir -p /data/logs/sso-cas-3200

mkdir -p /etc/wonhighconf/sso-cas-3200

cd /usr/local/wonhigh

从ftp下载应用包放在/usr/local/wonhigh下

unzip cas-server-x.x.x-yyyyMMddHHmm.zip

mv cas-server sso-cas-3200

cp -fr conf/wonhighconf/cas-server/\* /etc/wonhighconf/sso-cas-3200

rm -fr /usr/local/wonhigh/conf

修改/usr/local/tomcat-x.x.x-3200/conf/server.xml,增加

<Context path="/cas" docBase="/usr/local/wonhigh/sso-cas-3200/cas-server" debug="0" reloadable="false"/>

修改tomcat端口：

sed -i 's/8080/3200/g' /usr/local/tomcat-x.x.x-3200/conf/server.xml

sed -i 's/8009/3209/g' /usr/local/tomcat-x.x.x-3200/conf/server.xml

sed -i 's/8005/3205/g' /usr/local/tomcat-x.x.x-3200/conf/server.xml

sed -i 's/8443/3203/g' /usr/local/tomcat-x.x.x-3200/conf/server.xml

touch /usr/local/tomcat-x.x.x-3200/bin/setenv.sh

vim /usr/local/tomcat-x.x.x-3200/bin/setenv.sh

增加：

#!/bin/bash

JAVA\_OPTS='-server -Xms2048m -Xmx2048m -XX:PermSize=128M -XX:MaxPermSize=128M -DSSO\_CAS\_WEB\_CONF=/etc/wonhighconf/sso-cas-3200 -Dlog4jpath=/data/logs/sso-cas-3200 '

**删除webapps下内容**：

rm -fr /usr/local/tomcat-x.x.x-3200/webapps/\*

**修改/etc/wonhighconf/sso-cas-3200/cas.properties**

#根据使用的域名而定，比如测试环境可以用http://testsso.belle.net.cn

server.name=http://sso.belle.net.cn

ldap.url=ldap://172.17.210.xx:10389

ldap.managerPassword=secret

**修改redis连接信息**：

vim /etc/wonhighconf/sso-cas-3200/redis-config.properties

redis.host=172.17.210.64

redis.port=6379

redis.password=

**修改/etc/wonhighconf/sso-cas-3200/cas-link.properties连接信息：**

#忘记密码地址  
cas.forgetPwd.url=http://devsso.belle.net.cn:8980/ignore/pwdindex\_rest  
  
#旧入口地址  
cas.orgLogin.url=http://test\_retail.belle.net.cn

## SSO-CAS集群部署

使用nginx+tomcat构建集群，详情见 [nginx代理服务器配置](#_Nginx代理服务器配置)

# SSO-Server部署

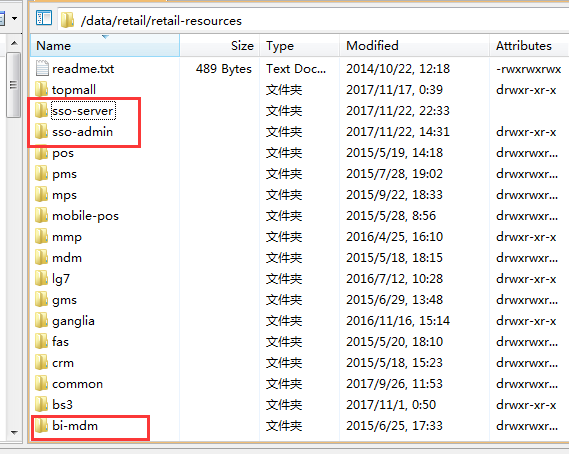
## 静态资源部署

ftp上取静态资源包（与web部署包在同一目录下），例如platform-bs-sso-server-resources. yyyyMMddhhmmsss.zip

部署到静态资源服务器上。

部署后访问路径测试：<http://s.belle.net.cn/sso-server/resources/js/index.js>

部署路径与pos、bi-mdm等的静态资源同级，如下图



## 单个SSO-Server实例的部署

端口号：

部署路径：/usr/local/wonhigh/sso-server-3100

日志路径：/data/logs/sso-server-3100

配置文件路径：/etc/wonhighconf/sso-server-3100

Tomcat路径：/usr/local/tomcat-x.x.x-3100(前面的x.x.x表示tomcat的版本号)

**部署步骤**：

Tomcat部署略。

mkdir -p /usr/local/wonhigh

mkdir -p /etc/wonhighconf/sso-server-3100

mkdir -p /data/logs/sso-server-3100

cd /usr/local/wonhigh

从ftp下载应用包放在/usr/local/wonhigh下

unzip platform-bs-sso-server-web-x.x.x.yyyyMMddHHmm.zip

cp -fr conf/wonhighconf/sso-server/\* /etc/wonhighconf/sso-server-3100

rm -fr /usr/local/wonhigh/conf

修改/usr/local/tomcat-x.x.x-3100/conf/server.xml,增加

<Context path="/" docBase="/usr/local/wonhigh/sso-sever" debug="0" reloadable="false"/>

修改tomcat端口：

sed -i 's/8080/3100/g' /usr/local/tomcat-x.x.x-3100/conf/server.xml

sed -i 's/8009/3109/g' /usr/local/tomcat-x.x.x-3100/conf/server.xml

sed -i 's/8005/3105/g' /usr/local/tomcat-x.x.x-3100/conf/server.xml

sed -i 's/8443/3103/g' /usr/local/tomcat-x.x.x-3100/conf/server.xml

touch /usr/local/tomcat-x.x.x-3100/bin/setenv.sh

vim /usr/local/tomcat-x.x.x-3100/bin/setenv.sh

增加：

#!/bin/bash

JAVA\_OPTS='-server -Xms2048m -Xmx2048m -XX:PermSize=128M -XX:MaxPermSize=128M -DSSO\_SERVER\_WEB\_CONF=/etc/wonhighconf/sso-server-3100-Dlog4jpath=/data/logs/sso-server-3100 '

**删除webapps下内容：**

rm -fr /usr/local/tomcat-x.x.x-3100/webapps/\*

**修改mysql连接信息：**

vim /etc/wonhighconf/sso-server-3100/platform-bs-sso/dal-db-config.properties

db.url=jdbc:mysql://172.17.210.180:3306/sso?useUnicode=true&characterEncoding=UTF-8&allowMultiQueries=true

db.username=sso

db.password=sso123

**修改ldap连接信息：（修改ip、密码）**

vim /etc/wonhighconf/sso-server-3100/platform-bs-sso/ldap.properties

sample.ldap.url=ldap://172.17.210.37:10389

sample.ldap.password=secret

**修改activemq连接信息：**

vim /etc/wonhighconf/sso-server-3100/platform-bs-sso/dal-activemq-config.properties

activemq.host=failover:(tcp://172.17.210.156:3046,tcp://172.17.210.157:3046,tcp://172.17.210.158:3046)?initialReconnectDelay=10000&amp;maxReconnectAttempts=-1

activemq.username=admin

activemq.password=admind

#多实例部署时activemq.listener.clientId要改成不相同，否则重复

activemq.listener.clientId=sso\_admin\_001

**修改/etc/wonhighconf/sso-server-3100/platform-bs-sso/platform-bs-sso-config.properties**

#EPP消息通知belletone\_dev ;belletone\_prod; belletone\_test  
EPP\_SOURCE\_PARAMETER=belletone\_dev  
  
domain.static= <http://s.belle.net.cn/sso-server>

##js版本，保持和项目版本一致（2017-12-17新增）

staticVersion=0.2.5  
  
common.domain.static=http://s.belle.net.cn

**修改redis连接信息：**

vim /etc/wonhighconf/sso-server-3100/platform-bs-sso/dal-redis-config.properties

redis.host=172.17.210.64

redis.port=6379

redis.pass=

**修改/etc/wonhighconf/sso-server-3100/platform-bs-sso/cas.client.properties连接信息：**

#cas登录地址  loginUrl地址需要cas域名：172.17.220.70，端口号：8085，cas项目名：cas-server，login必须带是登录地址  
cas.server.loginUrl=http://devsso.belle.net.cn:8980/cas/login  
  
#casPrefix地址，urlPrefix地址需要cas域名：172.17.220.70，端口号：8085，cas项目名：cas-server  
cas.server.urlPrefix=http://devsso.belle.net.cn:8980/cas  
  
#cas登出地址  loginUrl地址需要cas域名：172.17.220.70，端口号：8085，cas项目名：cas-server，logout必须带是登出地址  
cas.server.logoutUrl=http://devsso.belle.net.cn:8980/cas/logout  
  
#强制修改密码地址  
cas.server.forceEditPwdUrl=http://devsso.belle.net.cn:8980/ignore/pwd\_org  
  
#renew默认false  
cas.server.renew=false  
  
#gateway默认false  
cas.server.gateway=false   
  
#是否需要进行设备验证(只有零售需要设备验证：true, 其他系统为false)  
cas.client.deviceCheck=false

#cas.client编码集（2017-11-09新增）

cas.client.encoding=utf-8  
  
#客户端地址，serverName地址需要cas域名：172.17.220.70，端口号：8080  
cas.client.serverName=http://devsso.belle.net.cn:8980  
  
###不需要修改，cas拦截器过滤地址配置  
cas.server.ignorePattern=/css/\*|/js/\*|/img/\*|/view/\*|/ignore/\*|/api/\*

#cas.client业务系统分配Code，目的：拦截未绑定的业务系统

cas.client.bizCode=SSO-SERVER

#biz系统需要配置

sso.server.homeUrl=http:// devsso.belle.net.cn:8980/index

**修改sms-email-config.properties配置文件（2017-11-09新增）**

**sendSmsMsg.bussinessSysCode=22**

**#发送邮件地址** 2017-12-11 修改

[mail.username=platform.bs@belle.com.cn](mailto:mail.username=platform.bs@belle.com.cn)

mail.password=Bbl150604

#发送重置密码验证码模板 2017-12-11 新增   
########测试模板#######  
sendSmsMsg.content=测试内容：您正在重置一账通密码, 验证码:{code}, 请在15分钟内按页面提示提交验证码，切勿将验证码泄露他人。

#短信服务器地址（开发环境，不用修改）

sms.send.url=http://172.17.210.37:3250/o2o-ms/sendSms

#邮件服务地址（开发环境，不用修改）

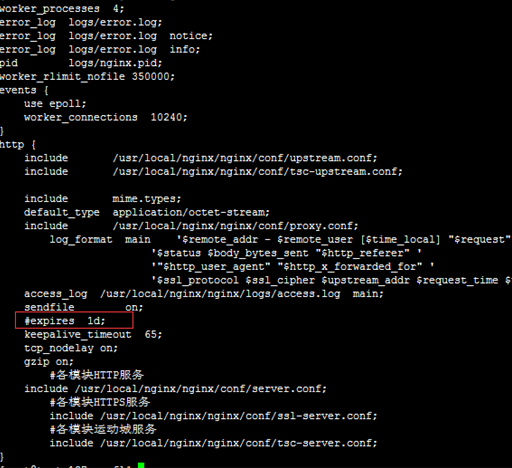
mail.send.url=http://172.17.210.37:3250/o2o-ms/sendEmail

## SSO-Server集群部署

使用nginx+tomcat构建集群，详情见 [nginx代理服务器配置](#_Nginx代理服务器配置)

备注：

1、配置ngnix时，需要注释expiress这项，否则跳转可能存在问题，比如: 请求登出接口，第二次会从cache中请求，存在找不到路径问题，导致无法登出。



2、nginx路由端口问题，主要是proxy\_set\_header Host $host:$server\_port; 这一句起作用否则端口号丢失了

非80端口的nginx代理问题，需要加入   
sso-server.conf  
#nginx非80端口处理  
proxy\_set\_header Host $host:$server\_port;  
#获取真实IP  
proxy\_set\_header X-Real-IP $remote\_addr;  
  
#获取代理者的真实ip  
proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

# SSO-Admin部署

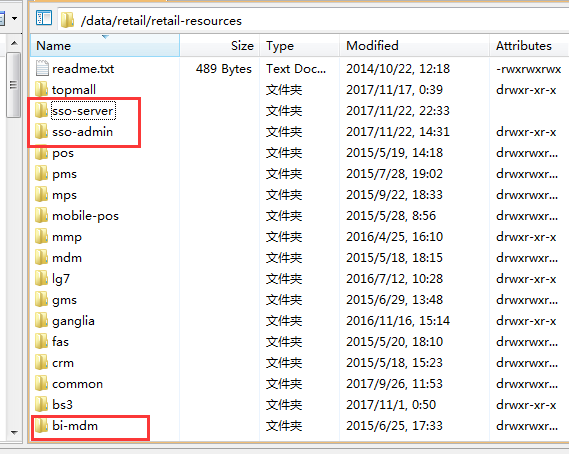
## 静态资源部署

ftp上取静态资源包（与web部署包在同一目录下），例如platform-bs-sso-admin-resources.yyyyMMddhhmmsss.zip

部署到静态资源服务器上。

部署后访问路径测试：<http://s.belle.net.cn/sso-admin/resources/js/tree.js>

部署路径与pos、bi-mdm等的静态资源同级，如下图



## 单个SSO-Admin实例的部署

端口号：

部署路径：/usr/local/wonhigh/sso-admin-3000

日志路径：/data/logs/sso-admin-3000

配置文件路径：/etc/wonhighconf/sso-admin-3000

Tomcat路径：/usr/local/tomcat-x.x.x-3000(前面的x.x.x表示tomcat的版本号)

**部署步骤**：

Tomcat部署略。

mkdir -p /usr/local/wonhigh

mkdir -p /data/logs/sso-admin-3000

mkdir -p /etc/wonhighconf/sso-admin-3000

cd /usr/local/wonhigh

从ftp下载应用包放在/usr/local/wonhigh下

unzip platform-bs-sso-admin-web-xxx.yyyyMMddHHmm.zip

cp -fr /usr/local/wonhigh/conf/wonhighconf/sso-admin/\* /etc/wonhighconf/sso-admin-3000

修改/usr/local/tomcat-x.x.x-3000/conf/server.xml,增加

<Context path="/admin" docBase="/usr/local/wonhigh/sso-admin-3000/sso-admin" debug="0" reloadable="false"/>

**修改tomcat端口：**

sed -i 's/8080/3000/g' /usr/local/tomcat-x.x.x-3000/conf/server.xml

sed -i 's/8009/3009/g' /usr/local/tomcat-x.x.x-3000/conf/server.xml

sed -i 's/8005/3005/g' /usr/local/tomcat-x.x.x-3000/conf/server.xml

sed -i 's/8443/3003/g' /usr/local/tomcat-x.x.x-3000/conf/server.xml

touch /usr/local/tomcat-x.x.x-3000/bin/setenv.sh

vim /usr/local/tomcat-x.x.x-3000/bin/setenv.sh

增加：

#!/bin/bash

JAVA\_OPTS='-server -Xms2048m -Xmx2048m -XX:PermSize=128M -XX:MaxPermSize=128M -DSSO\_ADMIN\_WEB\_CONF=/etc/wonhighconf/sso-admin-3000 -Dlog4jpath=/data/logs/sso-admin-3000 '

**删除webapps下内容：**

rm -fr /usr/local/tomcat-x.x.x-3000/webapps/\*

**修改mysql连接信息：**

vim /etc/wonhighconf/sso-admin-3000/platform-bs-sso/dal-db-config.properties

db.url=jdbc:mysql://172.17.210.180:3306/sso?useUnicode=true&characterEncoding=UTF-8&allowMultiQueries=true

db.username=sso

db.password=sso123

**修改ldap连接信息：（修改ip、密码）**

vim /etc/wonhighconf/sso-admin-3000/platform-bs-sso/ldap.properties

sample.ldap.url=ldap://172.17.210.37:10389

sample.ldap.password=secret

**修改activemq连接信息：**

vim /etc/wonhighconf/sso-admin-3000/platform-bs-sso/dal-activemq-config.properties

activemq.host=failover:(tcp://172.17.210.156:3046,tcp://172.17.210.157:3046,tcp://172.17.210.158:3046)?initialReconnectDelay=10000&amp;maxReconnectAttempts=-1

activemq.username=admin

activemq.password=admind

#多实例部署时activemq.listener.clientId要改成不相同，否则重复

activemq.listener.clientId=sso\_admin\_001

**修改/etc/wonhighconf/sso-admin-3000/platform-bs-sso/platform-bs-sso-config.properties**

common.static.url=http://s.belle.net.cn/

static.url=http://s.belle.net.cn /sso-admin/

##js版本，保持和项目版本一致（2017-12-17新增）

staticVersion=0.2.5

syncHR.cron=0 0 0 \* \* ? \*

#通知epp api source参数（2017-11-22新增） 生产：belletone\_prod 开发：belletone\_dev 测#试：belletone\_test

EPP\_SOURCE\_PARAMETER=belletone\_test

concurrent.semaphore.number=5

concurrent.export.max.size.per.request=10000

**修改sms-email-config.properties配置文件（2017-11-09新增）**

#短信邮件参数

sms.business.system.code=22

#新建账号模板

sms.create.new.account.msg=您的一账通账号注册成功，账号：{account}，初始密码：{password}

#修改密码模板

sms.update.password.msg=您的一账通账号{account}密码修改成功，新密码：{password}

## SSO-Server集群部署

使用nginx+tomcat构建集群，详情见 [nginx代理服务器配置](#_Nginx代理服务器配置)

# 部署后访问方式

|  |  |  |
| --- | --- | --- |
| **子系统** | **访问url** | **备注** |
| SSO-Admin | http://sso.belle.net.cn/admin | 开发测试环境配置本地hosts 开发环境域名建议： devsso.belle.net.cn 测试环境域名建议： testsso.belle.net.cn |
| SSO-Server | http://sso.belle.net.cn |
| SSO-CAS | http://sso.belle.net.cn/cas |

# Nginx代理服务器配置

Nginx配置文件见附件nginx-proxy.zip

# 附件

\\172.17.221.250\share\public\soft\ldap

<http://directory.apache.org/studio/download/download-windows.html>

