**统一登录部署**

# 总体部署架构



# 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

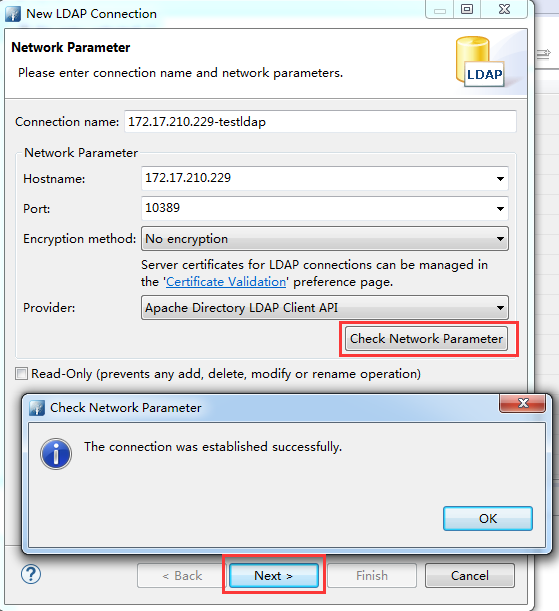
下载

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

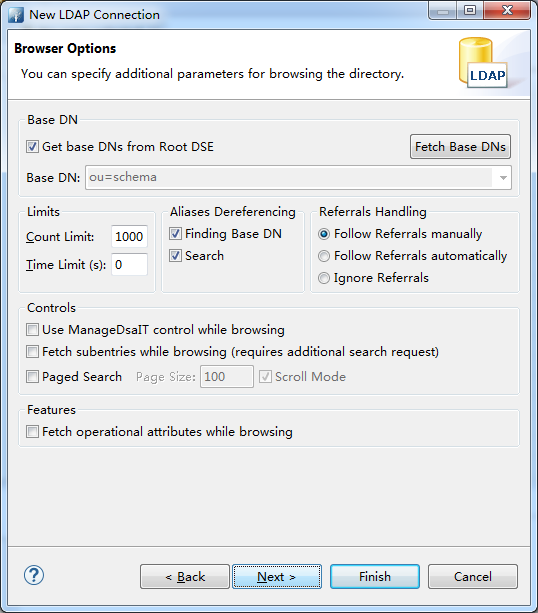
### New LDAP Connection

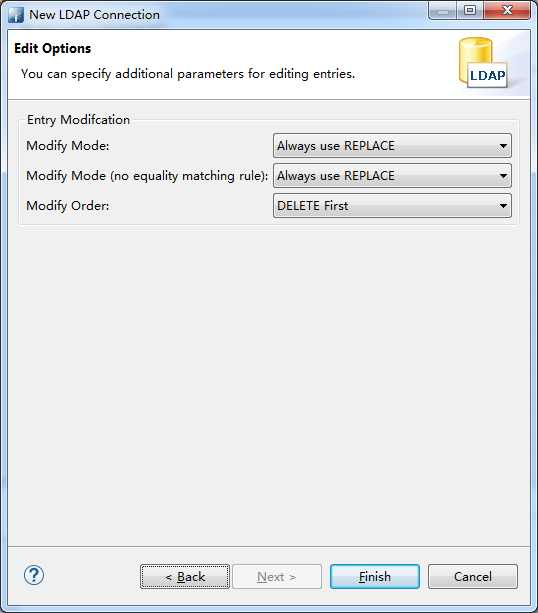
安装后连接服务端：

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

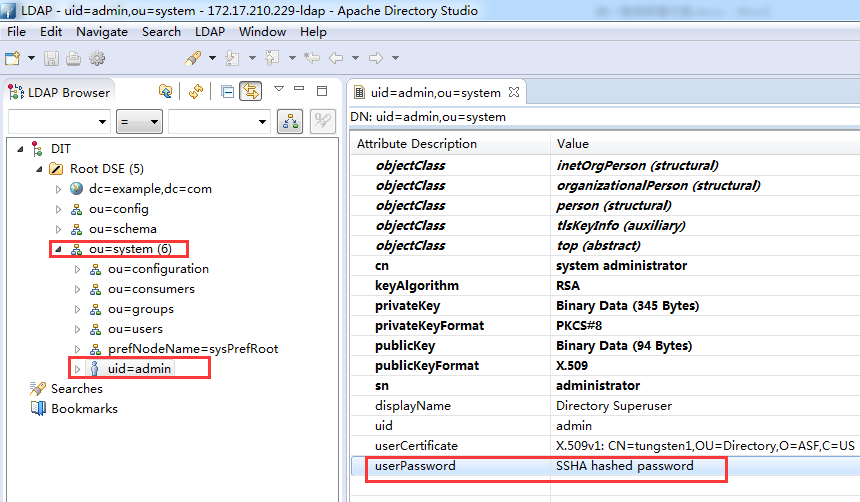


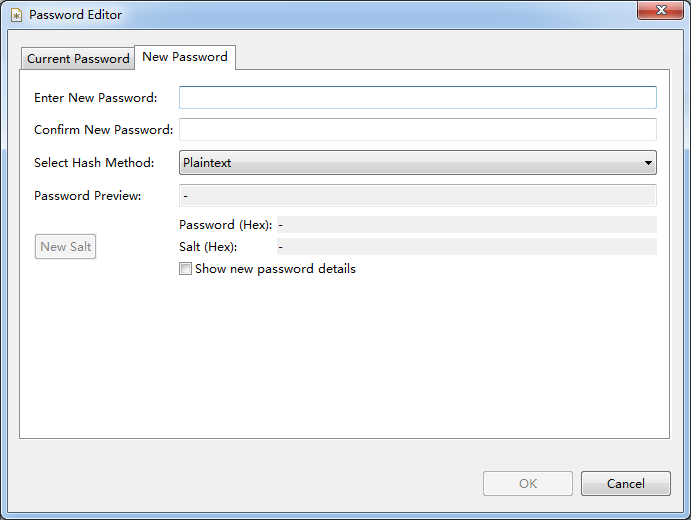
输入dn和password  
Dn：uid=admin,ou=system  
Password:secret





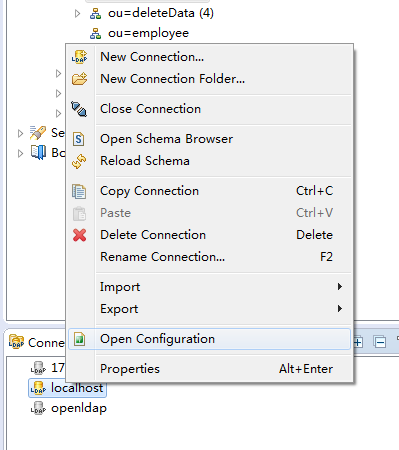
## 修改管理员密码



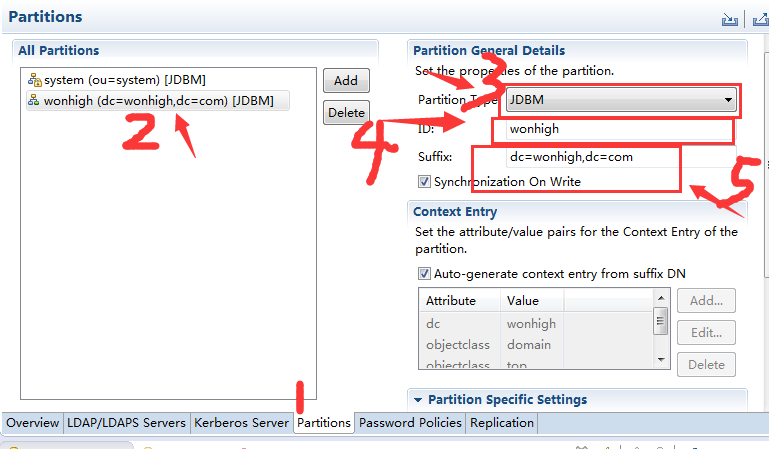


## Apacheds 新建wonhigh根节点

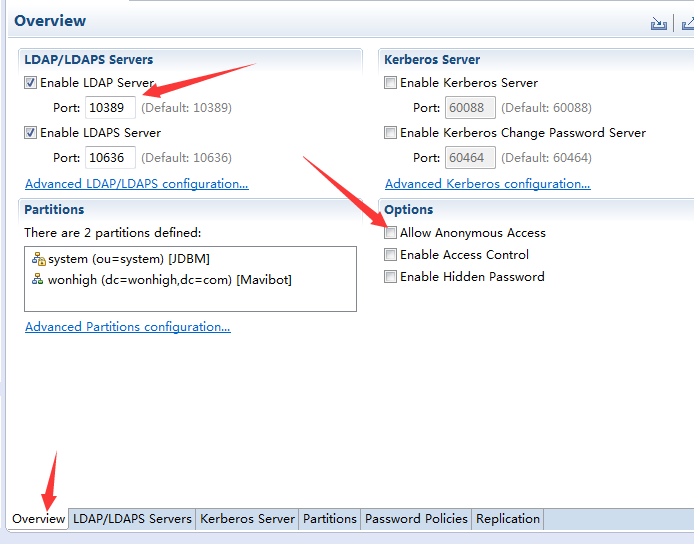
选择connection，右击选择open configuration



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



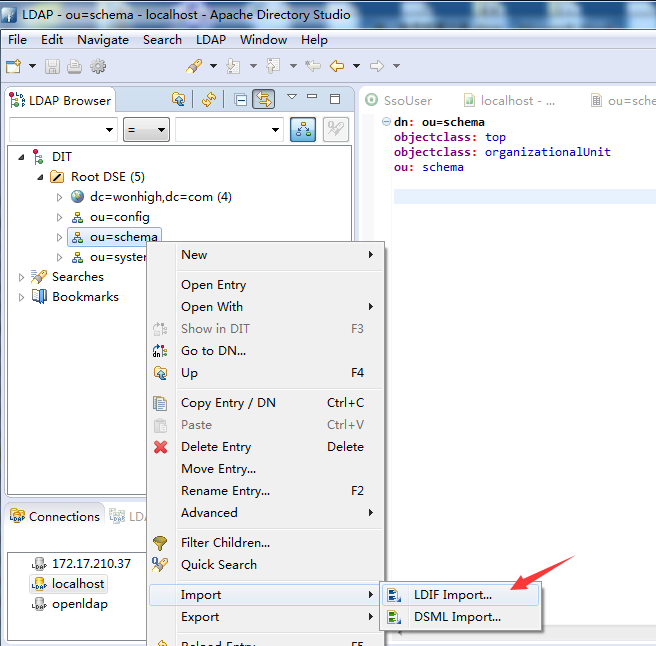
## Apacheds Schema导入

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。

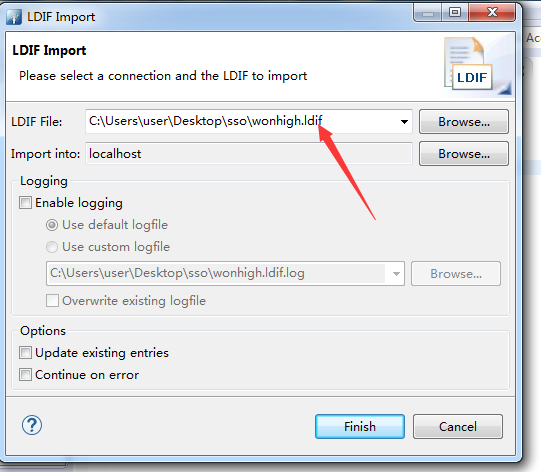
数据结构文件见附件。

### 通过Apache Diectory Studio导入

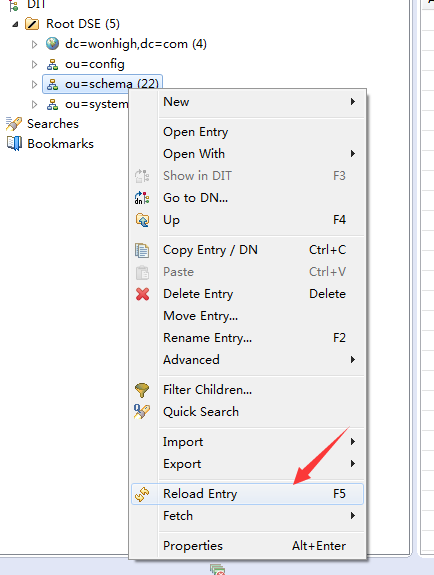
选择ou=schema节点，右键单击—>Import 🡪LDIF Import



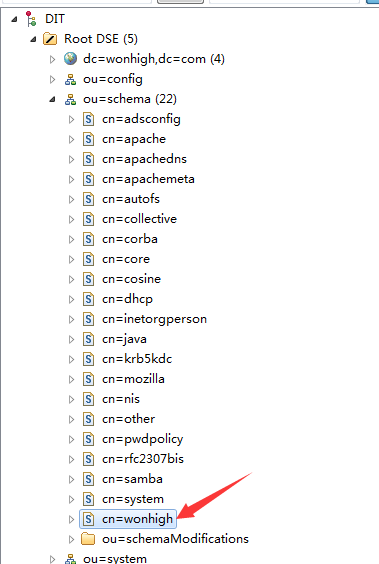
选择要导入的schema 文件

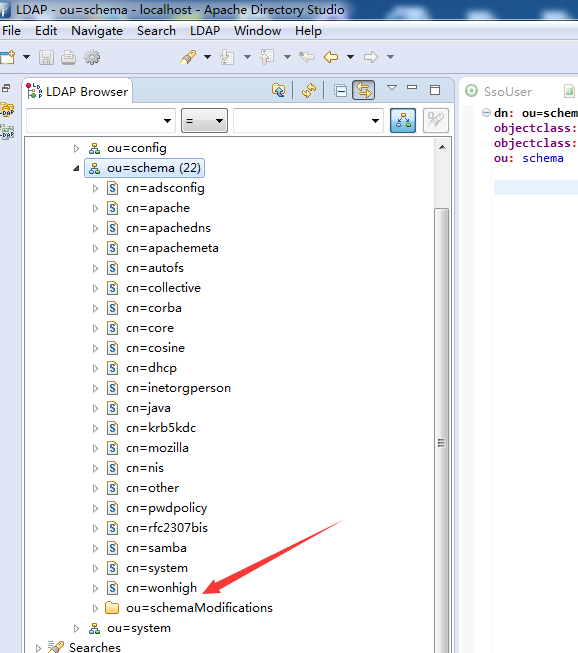


导入成功后，刷新ou=schema节点



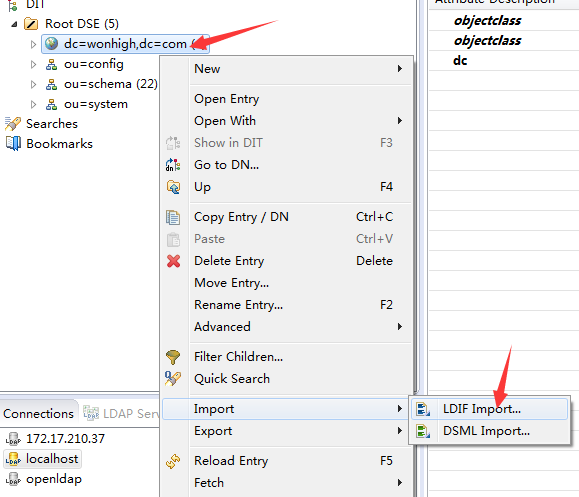
展开ou=schema节点 能够看到 wonhigh节点 表示导入成功。

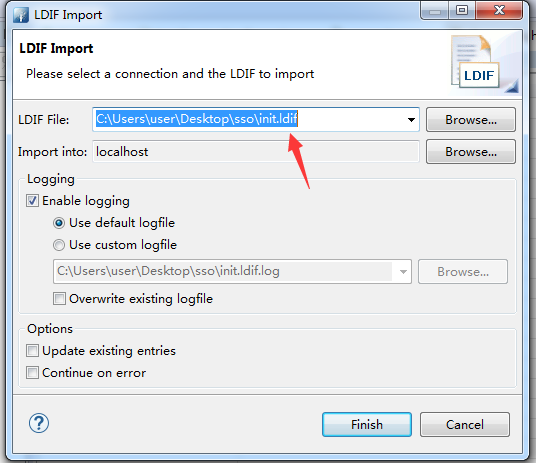


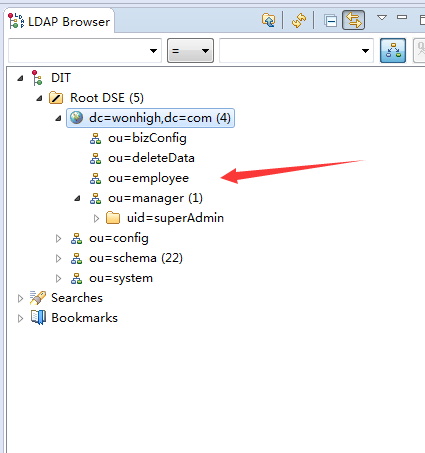


## Apacheds 初始化目录节点

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

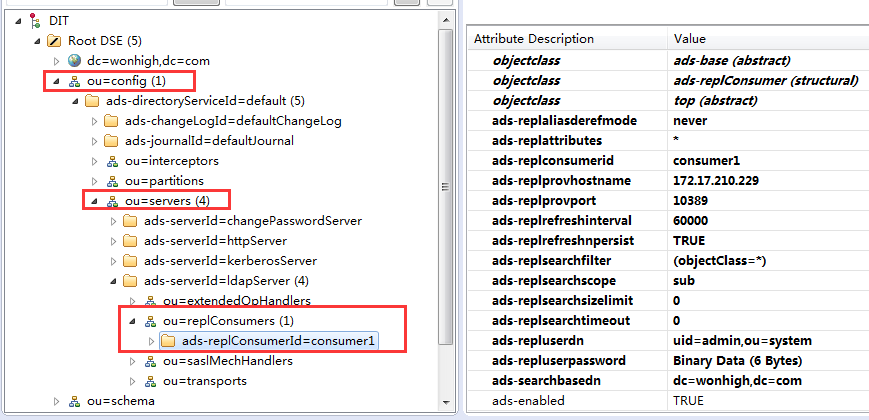
objectclass: ads-replConsumer

objectclass: ads-base

objectclass: top

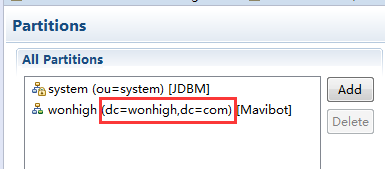
ads-replaliasderefmode: never

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/sso.sql

# 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 sso-cas

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=

## 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

## 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/platform-bs-sso -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**

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

static.url=http://localhost:6080

resources.version=0.2.0

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

**修改/etc/wonhighconf/sso-server-3100/platform-bs-sso/redis.config.properties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，devsso.belle.net.cn:cas域名，cas：项目路径名，login必须带是登录地址

cas.server.loginUrl=http://devsso.belle.net.cn/cas/login

#casPrefix地址，urlPrefix地址需要，cas域名:devsso.belle.net.cn:cas，cas项目路径名: cas(修改为cas部署的域名、路径名)

cas.server.urlPrefix=http://devsso.belle.net.cn/cas

#客户端地址，serverName地址需要，cas client域名：cas.client.serverName=http://devsso.belle.net.cn

###不需要修改，cas拦截器过滤地址配置(新增，必须配置)

cas.server.ignorePattern=/css/\*|/js/\*|/img/\*|/view/\*|/ignore/\*|/api/\*

## 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)

# SSO-Admin部署

## 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" 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://localhost:6080

resources.version=0.2.0

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

## 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>



