开源跳板机(堡垒机)Jumpserver部署

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

QQ群：90122290

本文撰稿日期： 2015年01月11日

本站口号：开源、分享、共进

注解：任何想通过本平台分享文档的，可以随时联系，文档里面注明出稿人和邮箱，方便文档使用者同撰稿的兄弟技术咨询沟通和交流；

目录

1 说明 4

2 部署ldapserver 4

2.1 安装ldapserver 4

2.2 准备配置文件 4

2.3 修改配置文件 5

2.4 修改系统日志配置文件 5

2.5 启动slapd, 查看启动情况 5

2.6 导入ldif数据库框架和测试用户 6

3 testserver部署ldapclient 7

3.1 CentOS6设置 7

3.1.1 安装LDAP客户端 7

3.1.2 设置自动创建目录 7

3.1.3 备份原来authconfig,然后设置使用LDAP认证 7

3.2 CentOS5设置 7

3.2.1 安装LDAP客户端 7

3.2.2 设置自动创建目录 7

3.2.3 设置使用LDAP认证 8

3.3 从jumpserver连接ldapuser测试 8

4 LDAP负责sudo 8

4.1 拷贝sudo schema 8

4.2 修改文件导入schema 8

4.3 重新生成配置文件，重启slapd 8

4.4 导入sudo.ldif到ldapserver 9

4.5 在testserver设置sudo使用ldap 9

4.5.1 CentOS6 9

4.5.2 CentOS5 9

4.6 测试sudo 9

5 部署phpldapadmin管理ldap 10

5.1 安装phpldapadmin 10

6 部署jumpserver 10

6.1 安装mysql数据库，创建库 10

6.2 下载最新Jumpserver项目 10

6.3 安装Python2.7.6 11

6.4 安装setuptools 和 pip 11

6.5 安装依赖库 11

6.6 修改Jumpserver配置文件 11

6.7 修改logs目录权限 12

6.8 django sync db 到数据库 13

6.9 测试运行 13

6.10 初始化jumpserver浏览器打开 13

7 安装node.js 13

7.1 下载node.js 13

7.2 编译安装 14

7.3 设置path 14

7.4 安装项目依赖module 14

7.5 测试启动websocket 14

8 测试jumpserver 14

9 收尾 16

# 说明

此为国产开源包，项目信息如下,虽然bug多多，不过在此基础上二次开发也省了一些路子,此文章非原创，出自此开源项目作者自己的博客：

软件包：[http://pan.baidu.com/s/1i3kne6p](http://pan.baidu.com/s/1i3kne6p" \t "_blank)

论坛： [http://bbs.jumpserver.org](http://bbs.jumpserver.org/" \o "" \t "_blank)

项目地址：[https://github.com/ibuler/jumpserver](https://github.com/ibuler/jumpserver" \t "_blank)

博客地址： [http://laoguang.blog.51cto.com/](http://laoguang.blog.51cto.com/" \o "" \t "_blank)

部署步骤环境： centos6.6 mini安装 iptables selinux已经关闭

jumpserver**:** 192.168.231.224

testserver**:** 192.168.231.222

# 部署ldapserver

* 1. 安装ldapserver

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

* 1. 准备配置文件

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

 ## 该文件是slapd的配置文件

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

 ## 数据库的配置文件

* 1. 修改配置文件

# vim /etc/openldap/slapd.conf

**...**

loglevel        1

**...**

suffix          "dc=zhoufengjie,dc=cn"

rootdn          "cn=admin,dc=zhoufengjie,dc=cn"

rootpw          TyumenPassword

**...**

#说明：  loglevel：设置日志级别  suffix：其实就是BaseDN  rootdn**:** 超级管理员的dn  rootpw**:** 超级管理员的密码

* 1. 修改系统日志配置文件

# vim /etc/rsyslog.conf

local4**.\***          **/**var**/**log**/**ldap**.**log   # local7.\*下添加一行

# service rsyslog restart

* 1. 启动slapd, 查看启动情况

# service slapd start

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

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

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

# service slapd restart

# netstat -tulnp | grep slapd

#说明：第一次启动生会初始化ldap数据库，在/var/lib/ldap中，如果想删除ldap数据库就删除该目录，保留DB\_CONFIG配置文件。新版的ldap使用的是/etc/openldap/slapd.d 下的配置文件，删除原来的配置文件，slaptest是重新生成新的配置文件

* 1. 导入ldif数据库框架和测试用户

可以使用migrationtools导出框架,(也可以用我们的：http://download.zhoufengjie.cn/document/tools/jumpserver/jump.tar.gz)**.** base**.**ldif**,**group**.**ldif**,**passwd**.**ldif 将其中的dc**=**zhoufengjie**,**dc**=**cn替换成你的baseDN(sed -i ‘s/zhoufengjie/你的DN/g’ \*.ldif ; sed -i ‘s/dc=cn/dc=你的DN/g’ \*.ldif)**,**然后导入**,**密码是rootpw设置的密码

# ldapadd -x -W -D "cn=admin,dc=zhoufengjie,dc=cn" -f base.ldif

# ldapadd -x -W -D "cn=admin,dc=zhoufengjie,dc=cn" -f group.ldif

# ldapadd -x -W -D "cn=admin,dc=zhoufengjie,dc=cn" -f passwd.ldif

#说明：测试用户是ldapuser 密码是testuser123,可以用下面的命令查询ldap里面的内容：ldapsearch -x -D "cn=admin,dc=zhoufengjie,dc=cn" -w "TyumenPassword" -b "dc=zhoufengjie,dc=cn"

# testserver部署ldapclient

* 1. CentOS6设置
     1. 安装LDAP客户端

# yum -y install openldap openldap-clients nss-pam-ldapd pam\_ldap

* + 1. 设置自动创建目录

# echo "session required pam\_mkhomedir.so skel=/etc/skel umask=0077" >> /etc/pam.d/system-auth

* + 1. 备份原来authconfig,然后设置使用LDAP认证

# authconfig --savebackup=auth.bak

# authconfig --enableldap --enableldapauth --enablemkhomedir --enableforcelegacy --disablesssd --disablesssdauth --ldapserver=192.168.231.224 --ldapbasedn="dc=zhoufengjie,dc=cn" --update

* 1. CentOS5设置
     1. 安装LDAP客户端

# yum -y install openldap openldap-clients nss\_ldap

* + 1. 设置自动创建目录

# echo "session required pam\_mkhomedir.so skel=/etc/skel umask=0077" >> /etc/pam.d/system-auth

* + 1. 设置使用LDAP认证

# authconfig --enableldap --enableldapauth --enablemkhomedir --ldapserver=192.168.231.224 --ldapbasedn="dc=zhoufengjie,dc=cn" --update

* 1. 从jumpserver连接ldapuser测试

# ssh ldapuser@192.168.231.222

# 密码是testuser123如果连接成功则继续

# LDAP负责sudo

* 1. 拷贝sudo schema

在服务器端操作，centos版本不一样，可能sudo的版本不是1.8.6，其他的也可以，根据你的版本改对应的路径做copy；

# cp /usr/share/doc/sudo-1.8.6p3/schema.OpenLDAP /etc/openldap/schema/sudo.schema

* 1. 修改文件导入schema

# vim /etc/openldap/slapd.conf

 include         **/**etc**/**openldap**/**schema**/**sudo**.**schema

* 1. 重新生成配置文件，重启slapd

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

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

# chown -R ldap:ldap /etc/openldap/slapd.d/\*

# service slapd restart

* 1. 导入sudo.ldif到ldapserver

# ldapadd -x -W -D "cn=admin,dc=zhoufengjie,dc=cn" -f sudo.ldif

 #说明：将sudo.ldif中的dc=zhoufengjie,dc=cn换作你的baseDN

* 1. 在testserver设置sudo使用ldap

**说明: centos6上sudo-1.7.4p5的使用的ldap配置文件是 /etc/sudo-ldap.conf，sudo版本不同使用的配置文件可能也有所不同，sudo -V | grep 'ldap.conf' 查看**

**# sudo -V | grep 'ldap.conf'**

**...**

**ldap.conf path: /etc/sudo-ldap.conf**

**# 已知有的版本是 /etc/nslcd.conf，下面应该做出对应改变**

**...**

* + 1. CentOS6

# echo -e "uri ldap://192.168.231.224\nSudoers\_base ou=Sudoers,dc=zhoufengjie,dc=cn" > /etc/sudo-ldap.conf

# echo "Sudoers: files ldap" >>  /etc/nsswitch.conf

* + 1. CentOS5

# echo "Sudoers\_base ou=Sudoers,dc=zhoufengjie,dc=cn" >> /etc/ldap.conf

# echo "Sudoers: files ldap" >> /etc/nsswitch.conf

* 1. 测试sudo

# ssh ldapuser@192.168.231.222

# sudo su

#说明：密码是testuser123，sudo su如果不提示输入密码，则成功

# 部署phpldapadmin管理ldap

* 1. 安装phpldapadmin

最新的软件包的下载地址如下，这里不赘述，有需要通过界面管理的自己查看： http://sourceforge.net/projects/phpldapadmin/files/phpldapadmin-php5/1.2.3/phpldapadmin-1.2.3.zip/download

# 部署jumpserver

* 1. 安装mysql数据库，创建库

# yum -y install mysql mysql-server mysql-devel

# service mysqld start

# mysql

mysql**>** create database jumpserver charset**=**'utf8'**;**

mysql**>** grant all on jumpserver**.\*** to 'jumpserver'@'127.0.0.1' identified by 'mysqlTyumen'**;**

mysql**>** grant all on jumpserver**.\*** to 'jumpserver'@'localhost' identified by 'mysqlTyumen'**;**

* 1. 下载最新Jumpserver项目

# yum -y install git

# cd /opt

# git clone [https://github.com/ibuler/jumpserver.git](https://github.com/ibuler/jumpserver.git" \t "_blank)

# cd jumpserver

* 1. 安装Python2.7.6

# yum -y install xz gcc automake autoconf

# tar xvf Python-2.7.6.tar.xz && cd Python-2.7.6

#说明，在上面下载的压缩包里面包含了此python版本；

# ./configure && make && make install

# mv /usr/bin/python /usr/bin/python.default

# ln -s /usr/local/bin/python /usr/bin/python

# vim /usr/bin/yum

!/usr/bin/python.default

#说明：centos6下yum使用python2.6,centos5下yum使用python2.4，否则报错

* 1. 安装setuptools 和 pip

#  tar xvf pypa-setuptools-8e8c50925f18.tar.gz  && cd pypa-setuptools-8e8c50925f18 && python setup.py install

# tar xvf pip-1.5.6.tar.gz && cd pip-1.5.6 && python setup.py install

* 1. 安装依赖库

# cd /opt/jumpserver/scripts

# pip2.7 install -r requirements.txt -i http://pypi.douban.com/simple

 #说明：如果报错请手动安装每个模块

* 1. 修改Jumpserver配置文件

# cd ..

# vim jumpserver.conf

**[**db**]**

host **=** 127.0.0.1

port **=** 3306

user **=** jumpserver

password **=** mysqlTyumen

db **=** jumpserver

**[**jumpserver**]**

key **=** 88aaaf7ffe3c6c04

ldap\_host **=** ldap**://**127.0.0.1**:**389

ldap\_base\_dn **=** dc**=**zhoufengjie**,**dc=cn

admin\_cn **=** cn**=**admin**,**dc**=**zhoufengjie**,**dc=cn

admin\_pass **=** TyumenPassword

web\_socket\_host **=** 192.168.231.224**:**3000

# 说明：

# db里是数据库的设置，相信你看一眼就知道了

# jumpserver中

# key是加密时需要的字符，可以更改但需要是16位

# ldap\_host,ldap\_base\_dn,admin\_cn,admin\_pass都是与上面ldapserver设置的一致

# admin\_cn 对应ldap中的rootdn，必须一致

# admin\_pass是ldap的密码，对应ldap.conf中的 rootpw ，必须使用明文

# web\_socket\_host是websocket的url，把ip改为jumpserver的IP地址，需要修改，3000是默认端口

* 1. 修改logs目录权限

# chmod 777 logs

* 1. django sync db 到数据库

# cd /opt/jumpserver/webroot/AutoSa

# python manage.py syncdb

Would you like to create one now**?** **(**yes**/**no**):** no

* 1. 测试运行

# python manage.py runserver 0.0.0.0:80

# python log\_handler.py

#说明：两个窗口分别打开

* 1. 初始化jumpserver浏览器打开

http**://**192.168.231.224**/**install

显示安装成功测继续

# 安装node.js

为了实现实时监控，使用了node.js来完成websocket

* 1. 下载node.js

官方地址：http**://**www**.**nodejs**.**org**/**download**/**   或   使用压缩包提供的源码（node-v0.10.33.tar.gz）   或   使用压缩包编译好的rpm（node-0.10.33-1.x86\_64.rpm**,**适用于centos6 x86\_64**,**跳过编译安装和设置path,如果使用rpm包的话，就跳过下一个编译项目）

* 1. 编译安装

# ./configure --prefix=/opt/node/ && make && make install

* 1. 设置path

# vim /etc/profile.d/node.sh

export PATH**=**$PATH**:/**opt**/**node**/**bin

# source /etc/profile.d/node.sh

* 1. 安装项目依赖module

可以使用下载的包里面的软件,如果不用的话通过如下方式进行下载

# cd /opt/jumpserver/webroot/AutoSa/websocket

# npm install

# 可能下载需要几分钟，可以更省时

#说明：如果使用已经下载好的，将node\_modules.tar.bz2 移动到/opt/jumpserver/webroot/AutoSa/websocket

# tar xvf node\_modules.tar.bz2

* 1. 测试启动websocket

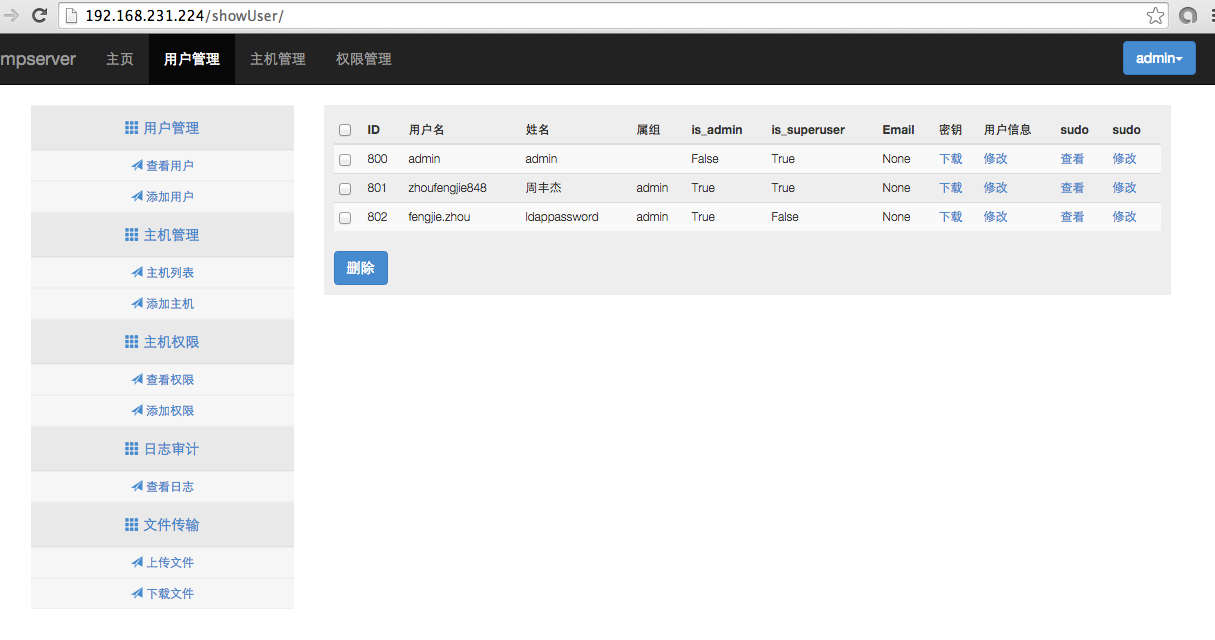
# node index.js

#说明：新窗口运行，如果开启了iptables确保放行3000端口

# 测试jumpserver

截图见原作者blog：**http://laoguang.blog.51cto.com/6013350/1576502**

6.1  登录 账号密码都是admin



6.2 添加属组

6.3 添加用户

6.4 添加IDC

6.5 添加主机

6.6 添加权限

6.7 查看权限

6.8 测试登录

6.9 下载key

6.10 导入key并登录xshell导入  Tools **-->** User Key Manager **-->** **import** **-->** 输入密码

6.11 登录

6.12 测试登录测试主机

# python /opt/jumpserver/jumpserver.py

#说明：p/P显示有权限主机ip E/e多主机执行命令 Q/q退出 输入ip或部分ip登录

6.13 显示有权限主机

6.14 多主机执行命令，逗号分隔     # 这里就一台主机



6.15 登录

6.16 查看sudo

6.17 修改sudo

6.18 测试sudo

6.19 测试监控  刷新，

6.20 结束session

6.21 查看统计日志  刷新，

6.22 用户测试上传下载

6.23 修改登录密码

# 收尾

如果一切没问题后，开始收尾

7.1 修改sshd配置，禁止密码登录

# vim /etc/sshd/sshd\_config

**...**

PasswordAuthentication no

**...**

# service sshd restart

7.2 让用户登录jumpserver自动运行系统

# cd /opt/jumpserver/scripts

# vim jumpserver.sh

**...**

**if** **[** $USER **==** 'guanghongwei' **];**then

# 修改特殊用户，结束后不退出

**...**

# cp jumpserver.sh /etc/profile.d/

7.3 正常运行jumpserver系统

# cd /opt/jumpserver/

# ./runserver#说明：如果想结束系统

# ./stopserver