目录

[一 权限集中管理-日志审计 2](#_Toc450659903)

[1.1公司问题现状 2](#_Toc450659904)

[1.2 项目要求 2](#_Toc450659905)

[1.3 具体实现 3](#_Toc450659906)

[二 JumpServer安装 3](#_Toc450659907)

[2.1 安装准备工作 3](#_Toc450659908)

[2.1.1 部署LdapServer环境 3](#_Toc450659909)

[2.1.2 准备配置文件 4](#_Toc450659910)

[2.1.3修改openldap配置文件 4](#_Toc450659911)

[2.1.4修改系统日志配置文件 4](#_Toc450659912)

[2.1.5启动slapd，查看启动情况 5](#_Toc450659913)

[2.1.6导入ldif数据库框架和测试用户 5](#_Toc450659914)

[2.1.7 部署ldapclient 7](#_Toc450659915)

[2.1.8 LDAP负责sudo 8](#_Toc450659916)

[2.1.9修改文件导入schema 8](#_Toc450659917)

[2.2.0导入sudo.idif到ldapserver 9](#_Toc450659918)

[2.2.1 testserver设置sudo使用ldap 9](#_Toc450659919)

[2.2.2 测试sudo 10](#_Toc450659920)

[2.2.3 删除测试用户 10](#_Toc450659921)

[三 安装mysql数据库 11](#_Toc450659922)

[3.1 安装数据库，授权 11](#_Toc450659923)

[3.2 下载最新项目 11](#_Toc450659924)

[3.3安装依赖模块 12](#_Toc450659925)

[3.4 修改jumpserver配置文件 12](#_Toc450659926)

[3.5建立logs目录并且修改权限 13](#_Toc450659927)

[四 启动jumpserver 14](#_Toc450659928)

[4.1 测试运行 14](#_Toc450659929)

[4.2 安装node.js 15](#_Toc450659930)

[五 信息采集 15](#_Toc450659931)

[5.1.1 人员信息采集表 15](#_Toc450659932)

[5.1.2 用户截图 17](#_Toc450659933)

[六 权限规划 18](#_Toc450659934)

[6.1.1 运维组 18](#_Toc450659935)

[6.1.2 开发组 19](#_Toc450659936)

[6.1.3 dba组 19](#_Toc450659937)

[6.1.4 架构组 19](#_Toc450659938)

[6.1.5 安全组 20](#_Toc450659939)

[七 jumpserver 20](#_Toc450659940)

[7.1.1 首页截图 20](#_Toc450659941)

[7.1.2 日志审计截图 21](#_Toc450659942)

[7.1.3 通过xshell使用秘钥登录 21](#_Toc450659943)

[7.1.4 登录成功的连接方法 22](#_Toc450659944)

[7.1.5通过web登录 22](#_Toc450659945)

[7.1.6登录成功如下界面 23](#_Toc450659946)

[八 登录方式 23](#_Toc450659947)

[8.1.1 管理员登录 23](#_Toc450659948)

[8.1.2 流程说明 23](#_Toc450659949)

# 一 权限集中管理-日志审计

## 1.1公司问题现状

当前我们公司里服务器有上百台，各个服务器上的管理人员很多（开发+运维+DBA），在大家登陆使用linux服务器时，不同职能的员工水平不同，因此导致操作很不规范，root权限泛滥，经常导致文件莫名其妙的丢失，等等，这样使得公司服务器安全存在很大的不稳定性，及操作的安全隐患，据调查企业服务器环境，50%以上的安全问题都来自于内容，而不是外部，为了解决以上问题，单个用户管理权限过大现状，以及日志审计（记录所有操作人员在服务器上的键盘操作并且可回放，也方便以后事故责任制）现提出针对linux服务器用户权限集中管理

## 1.2 项目要求

我们既希望超级用户root密码掌握在少数或唯一的管理员手中，又希望多个系统管理员或相关有权限的人员，能够完成更多更复杂的自身职能相关的工作，又不至于越权操作导致系统安全隐患

**最小化：1）安装软件最小化。2）目录文件权限最小化。3）用户权限最小化。4）程序运行权限最小化……………………….**

## 1.3 具体实现

针对公司不同部门，根据员工的具体工作职能（例如：开发，运维，数据库管理员），分等级，分层次的实现对linux服务器管理的权限最小化，规范化，这样既减少了运维管理成本，消除安全隐患，又提高了工作效率，实现了高质量的，快速化的完成项目进度，以及日常系统维护

# 二 JumpServer安装

## 2.1 安装准备工作

[root@localhost ~]# /etc/init.d/iptables stop

[root@localhost ~]# setenforce 0

[root@localhost ~]# cat /etc/redhat-release

CentOS release 6.7 (Final)

## 2.1.1 部署LdapServer环境

#安装基本环境，后面依赖

rpm-ivhhttp://dl.fedoraproject.org/pub/epel/6/x86\_64/epel-release-6-8.noarch.r

yum install -y vim automake autoconf gcc xz ncurses-devel \

patch python-devel git python-pip gcc-c++

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

## 2.1.2 准备配置文件

#该文件是slapd的配置文件

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

#数据库的配置文件

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

## 2.1.3修改openldap配置文件

vim /etc/openldap/slapd.conf

argsfile /var/run/openldap/slapd.args

loglevel 1

suffix "dc=jumpserver,dc=org"

rootdn "cn=admin,dc=jumpserver,dc=org"

rootpw secret234

#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

## 2.1.4修改系统日志配置文件

vim /etc/rsyslog.conf

#在local7.\*下面添加

local4.\* /var/log/ldap.log

service rsyslog restart #重启rsyslog

## 2.1.5启动slapd，查看启动情况

/etc/init.d/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/\*

/etc/init.d/slapd restart

netstat -lntup |grep slapd

netstat -lntup |grep slapd

tcp 0 0 0.0.0.0:389 0.0.0.0:\*

 #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

## 2.1.6导入ldif数据库框架和测试用户

ldapadd -x -W -D "cn=admin,dc=jumpserver,dc=org" -f base.ldif

Enter LDAP Password:

adding new entry "dc=jumpserver,dc=org"

adding new entry "ou=Hosts,dc=jumpserver,dc=org"

adding new entry "ou=Rpc,dc=jumpserver,dc=org"

adding new entry "ou=Services,dc=jumpserver,dc=org"

adding new entry "nisMapName=netgroup.byuser,dc=jumpserver,dc=org"

adding new entry "ou=Mounts,dc=jumpserver,dc=org"

adding new entry "ou=Networks,dc=jumpserver,dc=org"

adding new entry "ou=People,dc=jumpserver,dc=org"

adding new entry "ou=Group,dc=jumpserver,dc=org"

adding new entry "ou=Netgroup,dc=jumpserver,dc=org"

adding new entry "ou=Protocols,dc=jumpserver,dc=org"

adding new entry "ou=Aliases,dc=jumpserver,dc=org"

adding new entry "nisMapName=netgroup.byhost,dc=jumpserver,dc=org"

[root@localhost ~]# ldapadd -x -W -D "cn=admin,dc=jumpserver,dc=org" -f group.ldif

Enter LDAP Password:

adding new entry "cn=testuser,ou=Group,dc=jumpserver,dc=org"

[root@localhost ~]# echo $?

0

[root@localhost ~]# ldapadd -x -W -D "cn=admin,dc=jumpserver,dc=org" -f passwd.ldif

Enter LDAP Password:

adding new entry "uid=testuser,ou=People,dc=jumpserver,dc=org"

可以使用migrationtools导出框架，导入好的

base.ldif,group.ldif,passwd.ldif 将其中的dc=jumpserver,dc=org替换成你的baseDN,然后导入,密码是rootpw设置的 secret234  这些文件百度云中下载  http://pan.baidu.com/s/1i3kne6p

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

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

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

下载链接:http://pan.baidu.com/s/1i3ken6p

## 2.1.7 部署ldapclient

---centos6设置-----

2.1.1安装LDAP客户端

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

2.2.2 设置自动创建目录

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

2.2.3 备份原来authconfig，然后设置使用LDAP认证

authconfig --savebackup=auth.bak #备份

authconfig --enableldap --enableldapauth --enablemkhomedir --enableforcelegacy --disablesssd --disablesssdauth --ldapserver=10.1.208.112 --ldapbasedn="dc=jumpserver,dc=org" --update

测试 在服务端

[root@localhost ~]# ssh testuser@10.1.208.111

testuser@10.1.208.111's password:

Creating directory '/home/testuser'.

--- CentOS5设置 ---

2.1 安装LDAP客户端

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

2.2 设置自动创建目录# echo "session required pam\_mkhomedir.so skel=/etc/skel umask=0077" >> /etc/pam.d/system-auth

2.3 设置使用LDAP认证

# authconfig --enableldap --enableldapauth --enablemkhomedir --ldapserver=ip --ldapbasedn="dc=jumpserver,dc=org" –update

## 2.1.8 LDAP负责sudo

拷贝sudo schema，centos版本不一样，可能sudo的版本不是1.8.6，其他的也可以

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

## 2.1.9修改文件导入schema

vim /etc/openldap/slapd.conf

include /etc/openldap/schema/sudo.schema

3.3.3 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

config file testing succeeded

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

service slapd restart

正在启动 slapd： [确定]

## 2.2.0导入sudo.idif到ldapserver

ldapadd -x -W -D "cn=admin,dc=jumpserver,dc=org" -f sudo.ldif

Enter LDAP Password:

adding new entry "ou=Sudoers,dc=jumpserver,dc=org"

adding new entry "cn=defaults,ou=Sudoers,dc=jumpserver,dc=org"

adding new entry "cn=testuser,ou=Sudoers,dc=jumpserver,dc=org"

#说明：将sudo.ldif中的dc=jumpserver,dc=org换作你的baseDN

## 2.2.1 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' 查看使用使用什么配置文件

#配置客户端，注意在客户端操作

echo -e "uri ldap://10.1.208.112\nSudoers\_base ou=Sudoers,dc=jumpserver,dc=org" > /etc/sudo-ldap.conf

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

--- CentOS5 ---

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

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

## 2.2.2 测试sudo

# ssh testuser@192.168.20.131 #服务端

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

sudo ifconfig

eth0 Link encap:Ethernet HWaddr 00:0C:29:5B:B4:5D

inet addr:10.1.208.111 Bcast:10.1.255.255 Mask:255.255.192.0

inet6 addr: fe80::20c:29ff:fe5b:b45d/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:56585 errors:0 dropped:0 overruns:0 frame:0

TX packets:18063 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:42897268 (40.9 MiB) TX bytes:1629933 (1.5 MiB)

## 2.2.3 删除测试用户

# ldapdelete -x -D "cn=admin,dc=jumpserver,dc=org" -w secret234 "uid=testuser,ou=People,dc=jumpserver,dc=org"

# ldapdelete -x -D "cn=admin,dc=jumpserver,dc=org" -w secret234 "cn=testuser,ou=Sudoers,dc=jumpserver,dc=org"

#暂时可以不操作

# 三 安装mysql数据库

## 3.1 安装数据库，授权

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

/etc/init.d/mysql start

mysqladmin -uroot -p password 1q2w3e4r

mysql -uroot -p

mysql> create database jumpserver charset='utf8';

Query OK, 1 row affected (0.00 sec)

mysql> grant all on jumpserver.\* to 'jumpserver'@'127.0.0.1' identified by 'mysql234';

Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;

Query OK, 0 rows affected (0.00 sec)

## 3.2 下载最新项目

cd /opt

git clone https://github.com/ibuler/jumpserver.git

cd jumpserver

## 3.3安装依赖模块

cd /opt/jumpserver/docs/

pip 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修改Jumpserver配置文件

## 3.4 修改jumpserver配置文件

cat jumpserver.conf

[base]

ip = 10.1.208.112

port = 80

key = 88aaaf7ffe3c6c04

[db]

host = 127.0.0.1

port = 3306

user = jumpserver

password = mysql234

database = jumpserver

[ldap]

ldap\_enable = 1

host\_url = ldap://127.0.0.1:389

base\_dn = dc=jumpserver, dc=org

root\_dn = cn=admin,dc=jumpserver,dc=org

root\_pw = secret234

[websocket]

web\_socket\_host = 10.1.208.112:3000

[mail]

email\_host = smtp.qq.com

email\_port = 25

email\_host\_user = 593597557@qq.com

email\_host\_password = 123qweASD12

email\_use\_tls = False

说明：

[base] ip, port是访问web的ip和端口号, key是用来加密的随机字符串，如果更改请确保是16位

[db]里是数据库的设置

[ldap] ldap\_enable启用ldap, host\_url是ldapserver的地址， base\_dn root\_dn root\_pw与前面配置的ldapserver保持一致

[websocket] websocket的地址，是允许node index.js程序的服务器地址，通常和web运行在一起，端口号默认是 3000

[mail] 配置mail服务器，用来发送邮件，本版本添加用户会自动发邮件给用户的email

## 3.5建立logs目录并且修改权限

cd /opt/jumpserver/

mkdir logs;chmod 777 logs

4.6 导入数据库 django sync db

python manage.py sync db

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

如果失败请升级pip python 参考5.1.1

# 四 启动jumpserver

## 4.1 测试运行

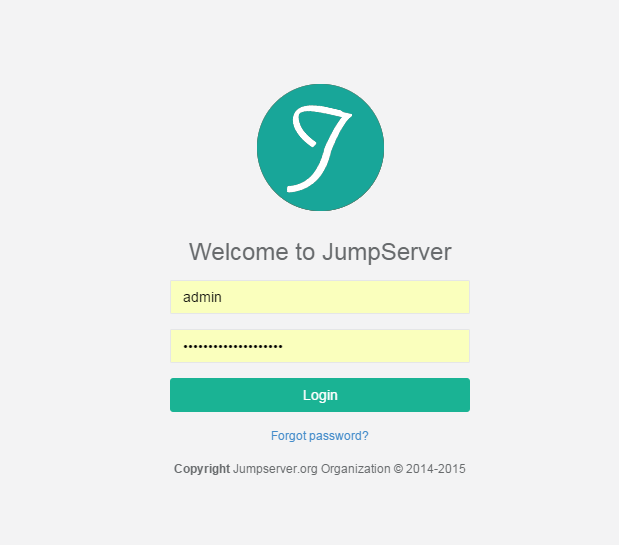
测试运行

python manage.py runserver 0.0.0.0:80

cd /opt/jumpserver/

python log\_handler.py  #说明：两个窗口分别打开

4.8 初始化jumpserver浏览器打开 http://ip/install



## 4.2 安装node.js

为了实现实时监控，使用了node.js来完成websocket

6.1.1 yum安装node.js

yum -y install nodejs npm

cd websocket

npm install  #说明：可能下载需要几分钟，也可以使用我已经下载好的模块，将node\_modules.tar.bz2 移websocket目录解压即可  # tar xvf node\_modules.tar.bz2 # 如果运行上面的install可以不解压提供的模块

6.2.2 测试启动websocket

cd /opt/jumpserver/websocket

node index.js

# 五 信息采集

## 5.1.1 人员信息采集表

|  |  |  |  |
| --- | --- | --- | --- |
| 人员名单 | 职位 | 负责的业务 | 对应服务器权限 |
| 赵成强 | 开发 | 未采集 | 未采集 |
| 许高明 | 开发 | 营销 | 未采集 |
| 张庄 | 开发 | 未采集 | 未采集 |
| 崔冬青 | 运维总监 | ALL | ALL |
| 丁成华 | 开发 | 未采集 | 未采集 |
| 耿磊 | 运维 | 未采集 | 未采集 |
| 梁玉洁 | 开发 | 未采集 | 未采集 |
| 齐宁 | 运维 | 预生产-代码发布 | 未采集 |
| 沈慧 | 开发 | 未采集 | 未采集 |
| 王昌双 | 运维 | 线上业务 | 未采集 |
| 王亮 | 开发 | 未采集 | 未采集 |
| 王宣琨 | 开发 | 点晶 | 未采集 |
| 具体权限需要相关人员配合，合理规划权限和人员的对应配置 | | | |

## 5.1.2 用户截图



# 六 权限规划

## 6.1.1 运维组

**运维组**

|  |  |
| --- | --- |
| 级别 | 权限 |
| 初级运维 | 查看系统信息，查看网络状态  /usr/bin/free,/usr/bin/iostat,/usr/bin/top,/bin/hostname,/sbin/ifconfig /bin/netstat /sbin/route |
| 高级运维 | 查看系统信息，查看和修改网络配置，进程管理，软件包管理，储蓄管理  /usr/bin/free,/usr/bin/iostat,/usr/bin/top,/etc/init.d/network,/bin/nice /bin/kill,/usr/bin/kill,/usr/bin/killall,/bin/rpm,/usr/bin/up2date,/usr/bin/yum /sbin/fdisk,/sbin/sfdisk,/sbin/parted,/sbin/partprobe,/bin/mount,/bin/umount /usr/bin/chattr,/usr/bin/lsattr,/usr/sbin/useradd,/usr/sbin/userdel,/usr/sbin/group,/usr/sbin/groupdel,/usr/bin/passwd |
| 运维经理 | 超级用户权限  ALL |

## 6.1.2 开发组

**开发组**

|  |  |
| --- | --- |
| 级别 | 权限 |
| 初级开发 | root,查看权限，对应服务查看日志的权限  /usr/bin/tail /app/log\*,/bi/grep/app/log\*,/bin/cat,/bin/ls |
| 高级开发 | root的查看权限，对应服务查看日志的权限，重启对应服务的权限  /sbin/service,/sbin/chkconfig,tail/app/log\*,grep/app/log\*,/bin/cat,/bin/ls |
| 开发经理 | 未定义 |

## 6.1.3 dba组

**dba组**

|  |  |
| --- | --- |
| 级别 | 权限 |
| 初级dba | 普通用户权限  不加入sudo列表 |
| 高级dba | 项目所在数据服务器的ALL权限 |

## 6.1.4 架构组

**架构组**

|  |  |
| --- | --- |
| 级别 | 权限 |
| 架构工程师 | 普通用户的权限  不加入sudo列表 |

## 6.1.5 安全组

**安全组**

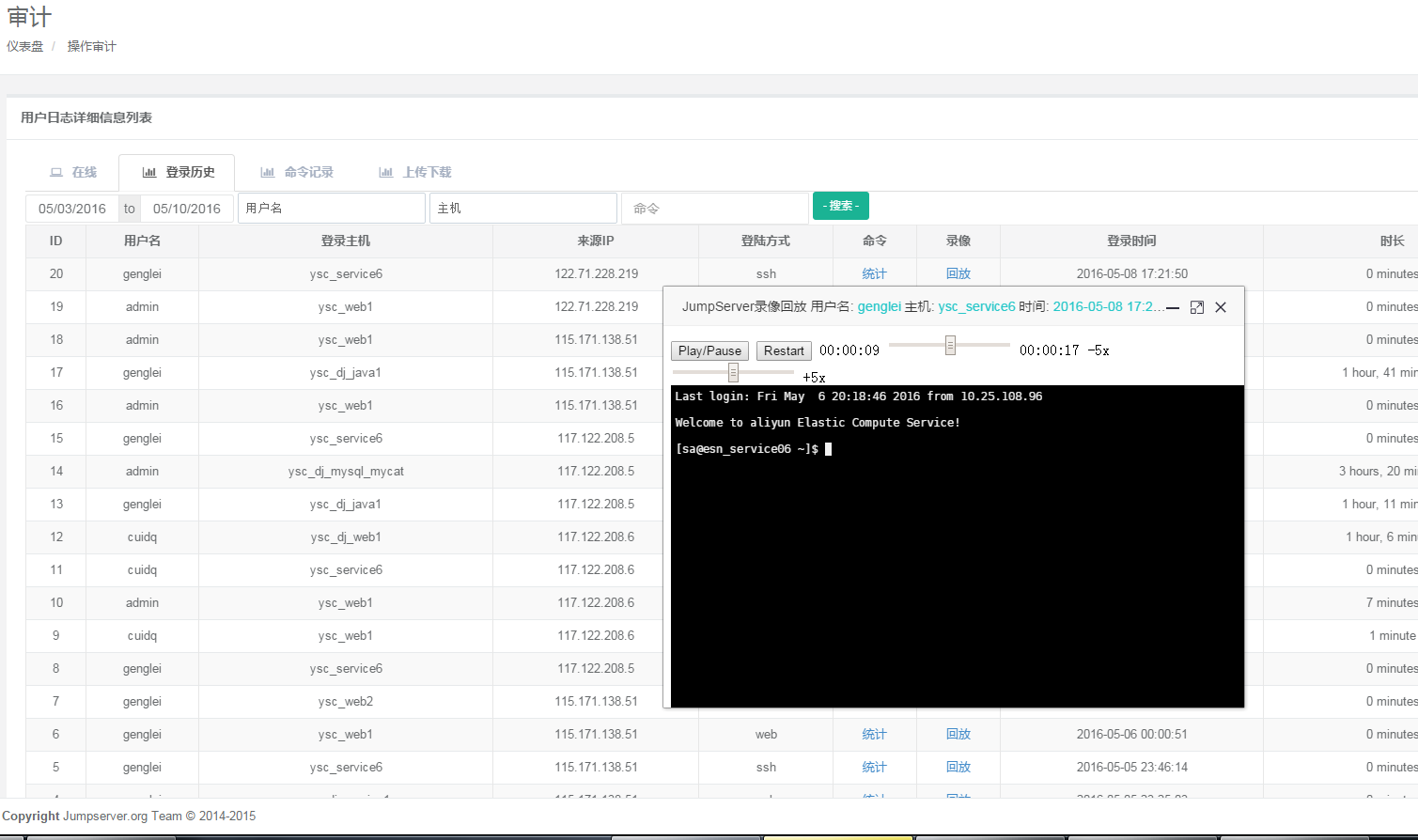
|  |  |
| --- | --- |
| 级别 | 权限 |
| 初级安全工程师 | 普通用户权限  不加入sudo列表 |
| 高级安全工程师 | 服务器网络方面的ALL权限  /sbin/route /sbin/ifconfig /bin/ping /sbin/dhclient /usr/bin/net /sbin/iptables /sbin/iwconfig /sbin/mii-tool /bin/cat /var/log/\* |

# 七 jumpserver

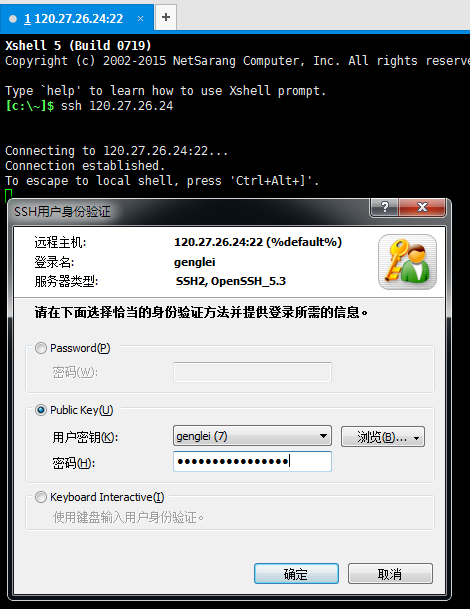
## 7.1.1 首页截图



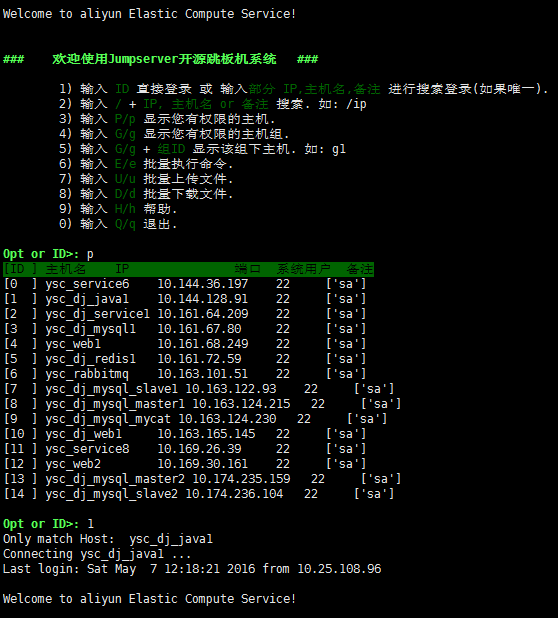
## 7.1.2 日志审计截图



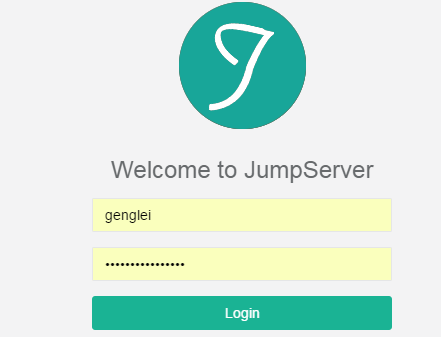
## 7.1.3 通过xshell使用秘钥登录



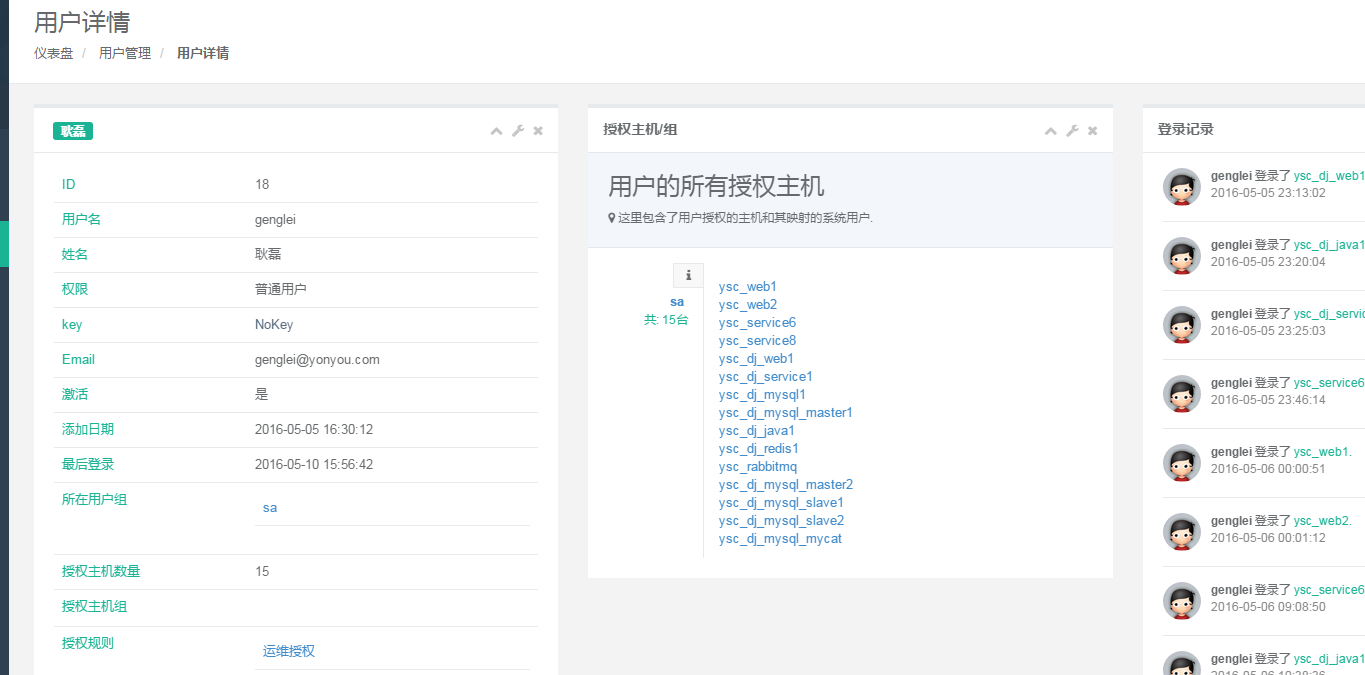
## 7.1.4 登录成功的连接方法



## 7.1.5通过web登录



## 7.1.6登录成功如下界面



# 八 登录方式

## 8.1.1 管理员登录

|  |  |
| --- | --- |
| <http://120.27.26.24:50077/> | |
| 用户：admin | 密码：JuiuCHvvwBPcsKCqtSBl |

## 8.1.2 流程说明

权限方案一旦实施后，所有员工必须通过《员工Linux服务器管理权限申请表》来申请对应的权限，确定审批流程，规范管理