**快速安装**

建议使用 centos 6 mini环境快速安装，安装过一些软件后，其中可能会安装一些不兼容的python库，如pycrypto, django, 会影响快速安装

**环境**

CentOS 6.x x86\_64 mini

iptables stop

selinux disable

**开始**

**1. 安装依赖rpm**

yum -y install epel-release

yum -y install git python-pip mysql-devel gcc automake autoconf python-devel vim sshpass lrzsz

**2. 下载jumpserver**

cd /data

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

**3. 执行快速安装脚本**

cd jumpserver/install && pip install -r requirements.txt

python install.py

*根据提示输入相关信息，完成安装，完成安装后，请访问web，继续查看后续文档*

*4,修改配置文件*

vim */data/jumpserver/ jumpserver.conf*

*[base]*

*url = http://172.16.51.171*

*key = vri80l3td79o5rpf*

*log = debug*

*[db]*

*host = 172.16.51.13*

*port = 3306*

*user = jumpserver*

*password = jjjr@2015*

*database = jumpserver3*

*[ldap]*

*ldap\_enable = 1*

*host\_url = ldap://172.16.51.170:389*

*base\_dn = dc=openldap,dc=17money,dc=com*

*root\_dn = cn=Manager,dc=openldap,dc=17money,dc=com*

*root\_pw = {SSHA}kI4ox1W5BK20oj/eAGGfCJrKU1JzrCIb*

*[websocket]*

*web\_socket\_host = 172.16.51.171:3000*

*[mail]*

*mail\_enable = 1*

*email\_host = mail.17money.com*

*email\_port = 25*

*email\_host\_user = weixin@17money.com*

*email\_host\_password = jjjr@2015*

*email\_use\_tls = True*

*如果启动失败，请返回上层目录，手动运行 ./service.sh restart启动*

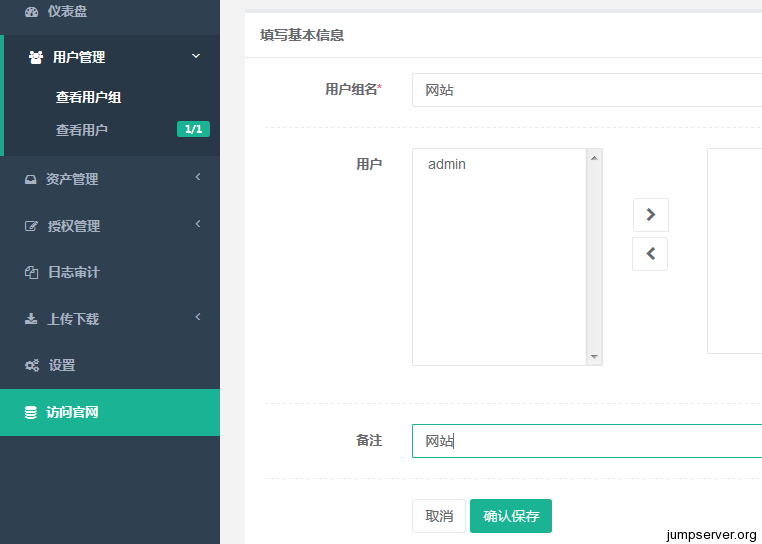
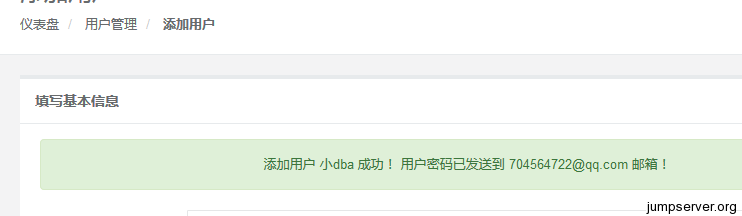
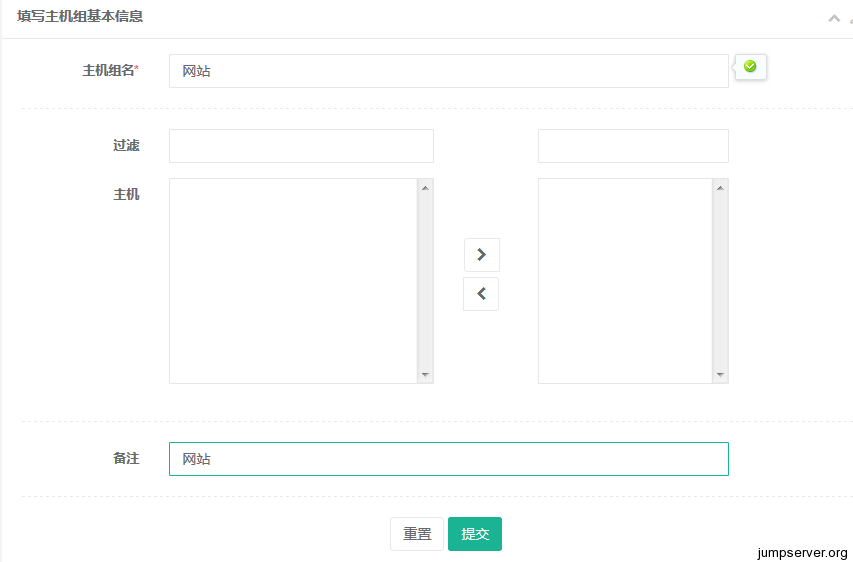
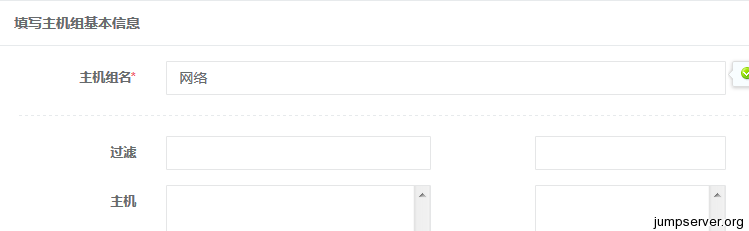
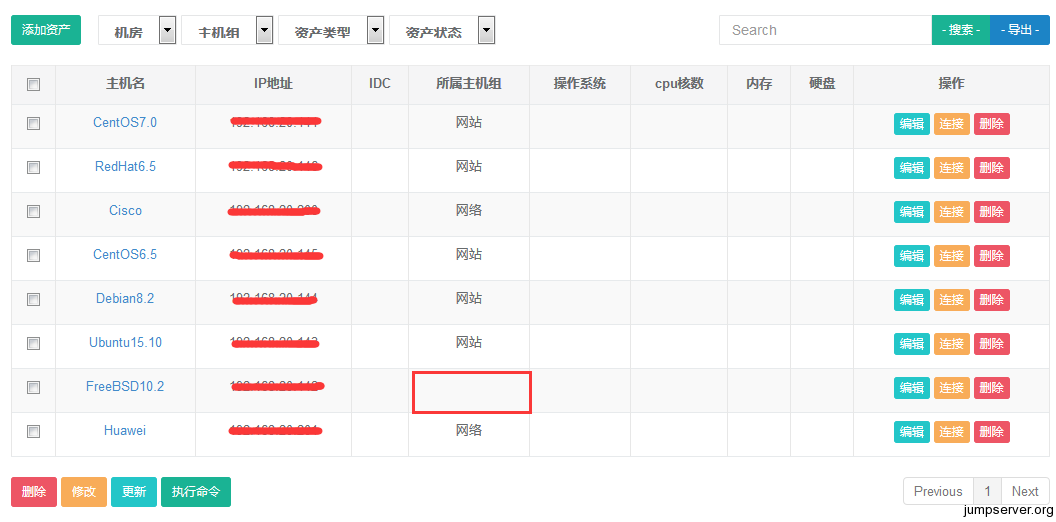
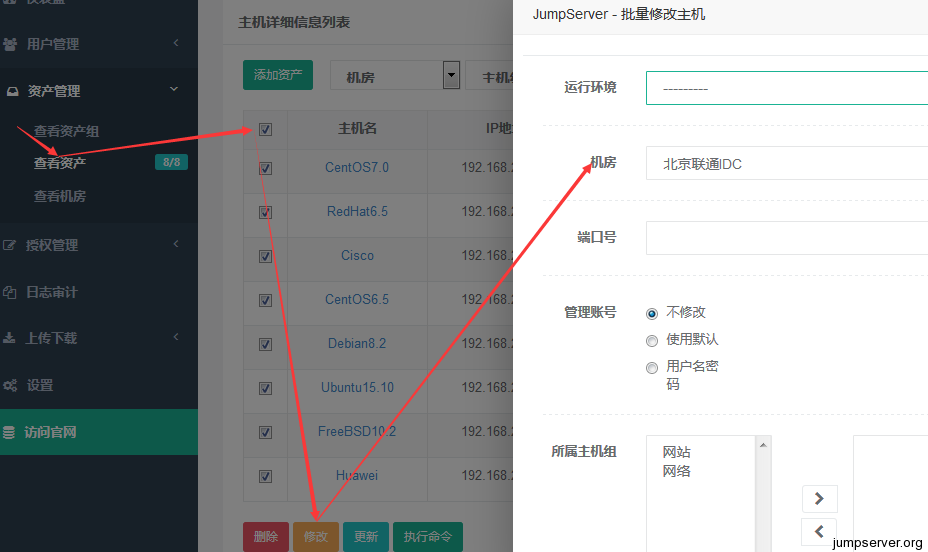
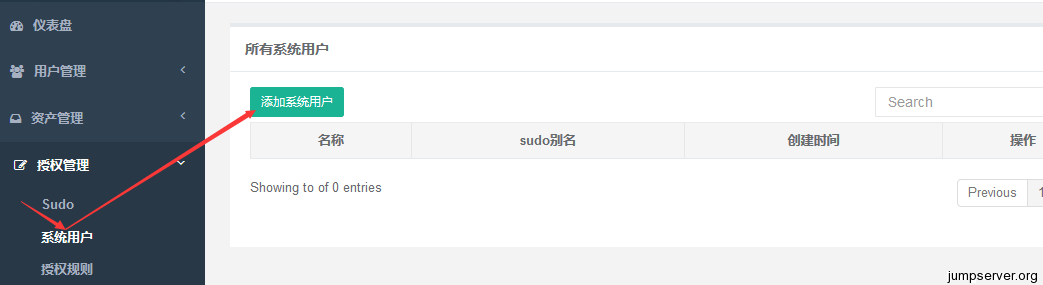
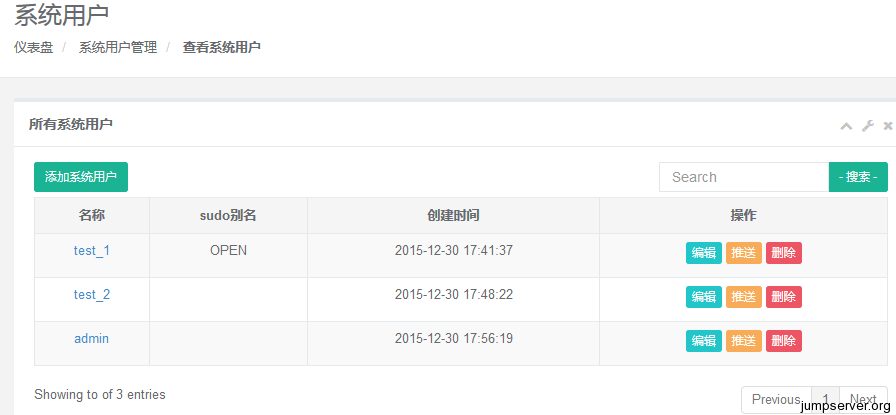
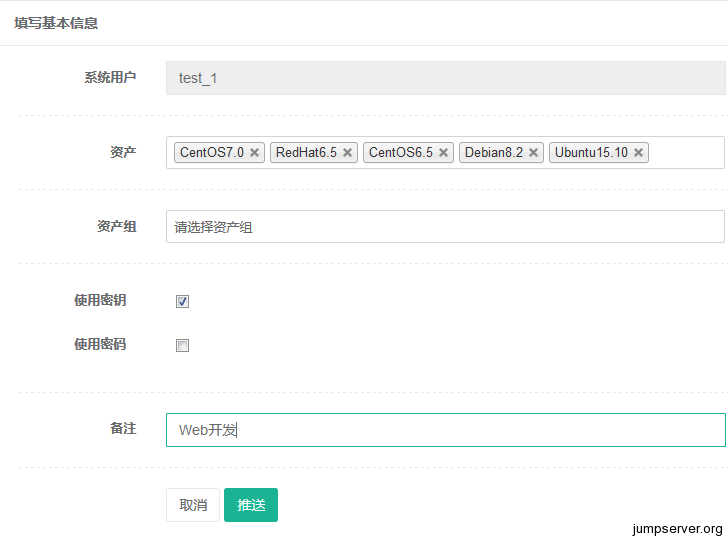
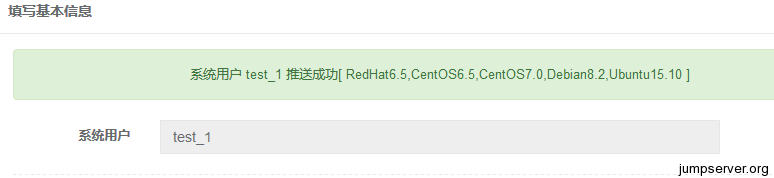
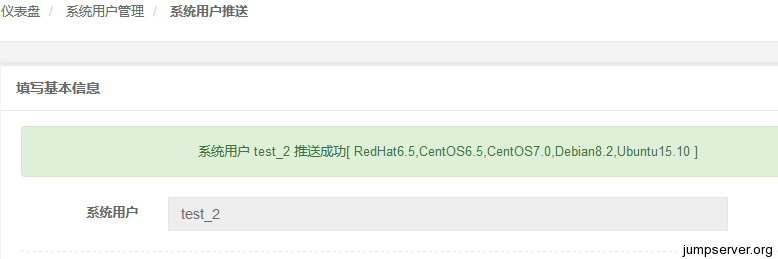
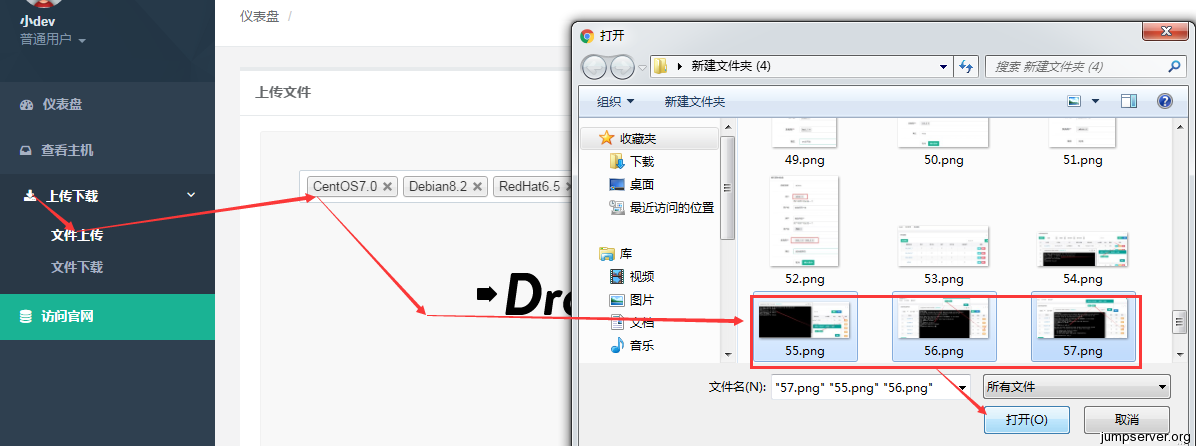
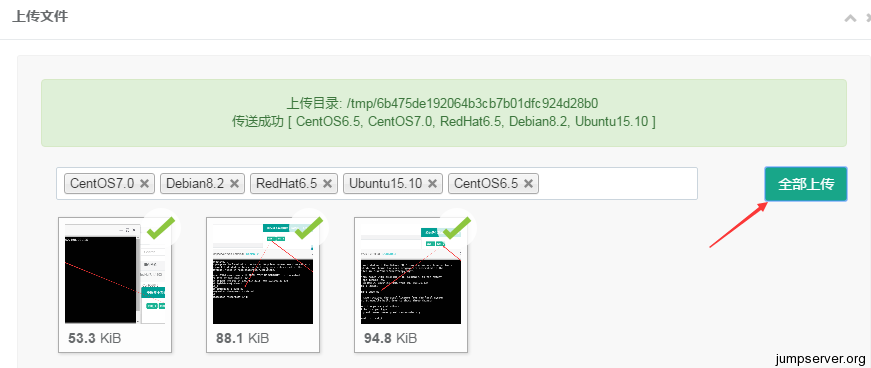
\*默认账号密码 admin 5Lov@wife

**注意**

1. 后端服务器需要有python环境才能使用推送用户，批量命令等功能

2. 后端服务器如果开启了selinux，请安装 libselinux-python

**配置篇**

**一、修改信息**   
   
  
**二、用户管理**   
**2.1.添加用户组   
用户组 ：**多个用户可以组合成用户组，为了方便进行授权，可以将一个部门或几个用户 组建成用户组，   
在授权中使用组授权，该组中的用户拥有所有授权的主机权限   
   
  
2.1.1  添加一个网站组   
   
  
2.1.2 添加一个网络组   
   
2.1.3 查看组   
   
  
**2.2.添加用户**   
**用户：** 用户是授权和登陆的主体，将来为每个员工建立一个账户，用来登录跳板机，将资产授权给该用户，   
查看用户登陆记录命令历史等   
   
  
2.2.1 创建第一个普通用户为dev，选网站组   
   
  
2.2.2 这里不选发送邮件，但用户邮箱是必填的   
  
   
  
2.2.3 确认保存   
   
  
2.2.4 创建第二个普通用户为dba，选网络组   
   
  
2.2.5 这里选发送邮件   
   
  
2.2.6 确认保存   
   
  
2.2.7 查看用户   
   
  
**三、设置默认管理帐号**   
**默认设置：**设置默认管理账号信息，包括账号密码密钥，默认信息为了方便添加资产而设计，   
添加资产时如果选择使用默认管理账号，则会使用这里设置的信息，端口是资产的ssh端口，添加资产时，默认会使用该端口   
  
默认管理用户用root 默认密码123456 ，默认管理帐号是Client端（后端服务器）真实存在的   
   
  
**四、资产管理**   
**4.1.添加主机组**   
**主机组：**同用户组，是资产组成的集合，为了方便授权   
   
  
4.1.1 添加一个网站组   
   
  
4.1.2 添加一个网络组   
   
  
4.1.3 查看资产组   
   
  
**4.2.添加资产**   
**资产：** 资产通常是我们的服务器、网络设备等，将资产授权给用户，用户则会有权限登 录资产，执行命令等   
   
  
**管理账户：** 添加资产时需要添加一个管理账户，该账户是该资产上已有的有管理权限的用户，   
如root，或者有 NOPASSWD: ALL sudo权限的用户，该管理账户用来向资产推送系统用户， 为系统用户添加sudo，   
获取资产的一些硬件信息   
  
4.2.1 单台添加，使用默认管理帐号，选网站组，如果默认管理帐号没设置，可选框会是禁选的，这里第三步已设   
  
  
4.2.2 单台添加，不使用默认管理帐号,选网站组，管理帐号是后端服务器真实存在的   
   
  
4.2.3 单台添加，选网络组，不使用默认管理帐号，网络设备已配置了ssh登录帐号：admin 密码：123456   
   
  
**4.3.批量添加**   
4.3.1 先下载模板   
   
  
4.3.2 填写资产在模板上的对应信息   
   
  
4.3.3 上传asset.xlsx文件   
   
  
4.3.4 查看资产   
注：asset.xlsx文件中FreeBSD 是数据库组，刚才并没有创建这个组，上传后这里为空，也就是说不会自动帮你创建组。   
   
  
**4.4.添加机房**   
   
  
4.4.1 添加IDC   
   
  
4.4.2 查看机房   
   
  
**4.5.批量修改**   
4.5.1 给主机添加一个IDC   
注：这里批量修改功能只能加不能减，如主机属于网站组，这里修改不能把主机从网站组中移除   
   
  
  
**五、授权管理**   
**5.1 添加别名**   
**Sudo：** 这里的sudo其实是Linux中的sudo命令别名，一个sudo别名包含多个命令， 系统用户关联sudo就代表该系统用户有权限sudo执行这些命令   
   
  
5.1.2 添加一个叫open别名   
注：系统命令格式，如果系统命令要用ALL，一定要大写 的ALL   
   
  
5.1.3 查看别名   
   
  
   
  
**5.2 添加系统用户**   
**系统用户：** 系统用户是服务器上建立的一些真实存在的可以ssh登陆的用户,如 dev, sa, dba等，   
系统用户可使用jumpserver推送到服务器上，也可以利用自己公司 的工具进行推送，   
授权时将用户、资产、系统用户关联起来则表明用户有权限登陆该资产的 这个系统用户   
如：用户 **小明**以 **dev** 系统用户登录 **172.16.1.1**资产, 简单理解就是 将某个资产上的某个系统用户映射给这个用户登录   
  
****  
5.2.1 添加用户test\_1，关联sudo:open   
   
  
5.2.2 添加用户test\_2，不关联sudo:open   
   
  
5.2.3 添加用户：admin，密码：123456，不关联sudo:open   
   
  
5.2.4 查看系统用户   
   
  
**5.3.推送**   
**推送系统用户：** 添加完系统用户，需要推送，推送操作是使用ansible，把添加的系统 用户和系统用户管理的sudo，   
推送到资产上，具体体现是在资产上useradd该系统用户，设置它的key,然后设置它的sudo，为了让用户可以登录它   
注：   
1. 后端服务器需要有python,sudo 环境才能使用推送用户，批量命令等功能   
2. 后端服务器如果开启了selinux，请安装 libselinux-python   
   
  
5.3.1 推送系统用户test\_1,资产单个添加，使用密钥   
   
  
5.3.2 推送成功   
   
  
5.3.3 推送系统用户test\_2,资产组添加，使用密码   
   
   
5.3.4 推送成功   
   
  
5.3.5 推送系统用户admin,网络设备主要是模拟推送一下，所以复选框不选使用密钥和密码   
   
  
5.3.4 推送成功   
   
  
**5.4.添加授权规则**   
**授权规则：** 授权规则是将 **资产** **系统用户** 和 **用户** 关联起来，用来完成授权。   
这样用户就可以以某个系统用户账号登陆资产。大家对这好像不是很理解，其实也是对系统用户， 用户这里没有搞清楚。   
我们可以把用户当做虚拟的用户，而系统用户是真实再服务器上存在的用户， 系统用户可以使用jumpserver推送，也可以自己手动建立，   
但是推送的过程一定要有，哪怕是模拟 推送（不选择秘钥和密码推送，如网络设备），因为添加授权规则会检查推送记录。   
为了简化理解， 我们暂时 以 **用户** **资产** **系统用户** 来理解，暂时不考虑组，添加这样的规则意思是 授权 用户 在这个资产上 以这个系统用户来登陆,   
系统用户是一组具有通用性，具有sudo的用户， 不同的用户授权不同的 系统用户，比如 dba可能有用数据库的sudo权限   
  
   
  
5.4.1 添加一个规则名称为dev\_test\_1,授权方式：用户对资产组   
   
  
5.4.2 添加一个规则名称为dev\_test\_2，授权方式：用户对资产   
   
  
5.4.3 添加一个规则名称为dba\_admin，授权方式：用户对资产   
   
  
5.4.3 添加一个规则名称为admin，超级管理员admin要想web terminal和web端批量命令也是要授权的   
   
  
  
5.4.4  查看规则   
   
   
**八、 上传下载**   
**8.1.文件上传**   
8.1.1 主机和文件可以多对多批量上传   
   
  
8.1.2 全部上传成功   
   
  
**8.2.文件下载**   
8.2.1 文件和主机只能一对多批量下载，下载的文件会分别放在以主机名创建对应的文件夹里   
 