老男孩教育-综合架构-jumpserver

```
1.跳板机
    2.跳板机的缺陷
    3.堡垒机
    4.堡垒机优势 4A能力
    5.jumpserver
    6.jumpserver安装
        手动
            理解各个组件:


        Docker
        脚本
        分布式
    7.jumpserver基本应用
    8.用户  ( 三类 )
        管理用户
        系统用户
        普通用户

    9.资产  ( 根据不同维度划分 )
        服务器
        网络设备
        数据应用

    10.权限
        将用户-->关联-->资产

    11.管理MySQL数据库应用

    12.审计
        1.不允许执行rm命令
        2.录屏回放 \  详细命令输出  \  批量执行

    13.安全
```

1. 跳板机

- 堡垒机,跳板机

2核心8G内存		

```

快速搭建使用.

#全自动
```

```
curl -sSL https://github.com/jumpserver/jumpserver/releases/download/v2.10.2/quick_start.sh | bash

#
[root@m02 ~]# tar xf jumpserver-installer-v2.10.2.tar.gz  -C /opt/
[root@m02 ~]# ln -s  /opt/jumpserver-installer-v2.10.2/  /opt/jumpserver
[root@m02 ~]# cd /opt/jumpserver
[root@m02 /opt/jumpserver]# ll
total 24
drwxrwxr-x 3 root root 4096 May 18 19:13 compose
-rw-rw-r-- 1 root root 1597 May 18 19:13 config-example.txt
drwxrwxr-x 7 root root   86 May 18 19:13 config_init
-rwxrwxr-x 1 root root 5503 May 18 19:13 jmsctl.sh
drwxrwxr-x 4 root root   29 May 18 19:13 locale
-rw-rw-r-- 1 root root 2593 May 18 19:13 README.md
drwxrwxr-x 2 root root  279 May 18 19:13 scripts
-rw-rw-r-- 1 root root   25 May 26 17:18 static.env
drwxrwxr-x 2 root root   41 May 18 19:13 utils
[root@m02 /opt/jumpserver]# cp config-example.txt  config/config.txt



[root@m02 /opt/jumpserver]# ./jmsctl.sh    #这一步显示命令格式 表示 config.txt配置ok
No such command:
JumpServer Deployment Management Script

Usage:
  ./jmsctl.sh [COMMAND] [ARGS...]
  ./jmsctl.sh --help

Installation Commands:
  install           Install JumpServer
  upgrade [version] Upgrade JumpServer
  check_update      Check for updates JumpServer
  reconfig          Reconfiguration JumpServer

Management Commands:
  start             Start   JumpServer
  stop              Stop    JumpServer
  close             Close   JumpServer
  restart           Restart JumpServer
  status            Check   JumpServer
  down              Offline JumpServer
  uninstall         Uninstall JumpServer

More Commands:
  load_image        Loading docker image
  python            Run python manage.py shell
  backup_db         Backup database
  restore_db [file] Data recovery through database backup file
  raw               Execute the original docker-compose command
  tail [service]    View log


#安装jumpserver
[root@m02 /opt/jumpserver]# ./jmsctl.sh install


       ██╗██╗   ██╗███╗   ███╗██████╗ ███████╗███████╗██████╗ ██╗   ██╗███████╗██████╗
       ██║██║   ██║████╗ ████║██╔══██╗██╔════╝██╔════╝██╔══██╗██║   ██║██╔════╝██╔══██╗
       ██║██║   ██║██╔████╔██║██████╔╝███████╗█████╗  ██████╔╝██║   ██║█████╗  ██████╔╝
  ██   ██║██║   ██║██║╚██╔╝██║██╔═══╝ ╚════██║██╔══╝  ██╔══██╗╚██╗ ██╔╝██╔══╝  ██╔══██╗
  ╚█████╔╝╚██████╔╝██║ ╚═╝ ██║██║     ███████║███████╗██║  ██║ ╚████╔╝ ███████╗██║  ██║
   ╚════╝  ╚═════╝ ╚═╝     ╚═╝╚═╝     ╚══════╝╚══════╝╚═╝  ╚═╝  ╚═══╝  ╚══════╝╚═╝  ╚═╝

                                   Version:  v2.10.2

语言 Language  (cn/en)  (default cn):
一直回车.
...

```

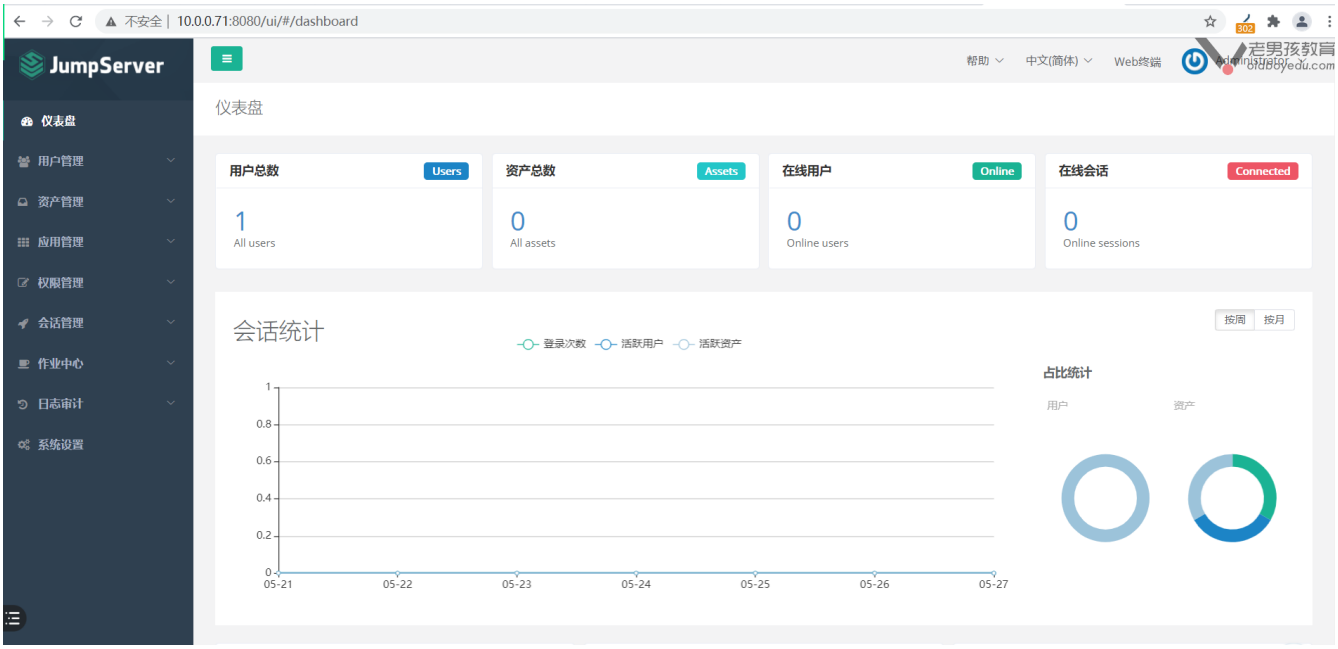
```
>>> 安装完成了
1. 可以使用如下命令启动，然后访问
./jmsctl.sh start   #docker 运行起来

2. 其它一些管理命令
./jmsctl.sh stop
./jmsctl.sh restart
./jmsctl.sh backup
./jmsctl.sh upgrade
更多还有一些命令，你可以 ./jmsctl.sh --help 来了解

3. Web 访问
http://10.0.0.71:8080
https://10.0.0.71:8443
默认用户：admin  默认密码：admin

4. SSH/SFTP 访问
ssh admin@10.0.0.71 -p2222
sftp -P2222 admin@10.0.0.71

5. 更多信息
我们的官网：https://www.jumpserver.org/
我们的文档：https://docs.jumpserver.org/
```



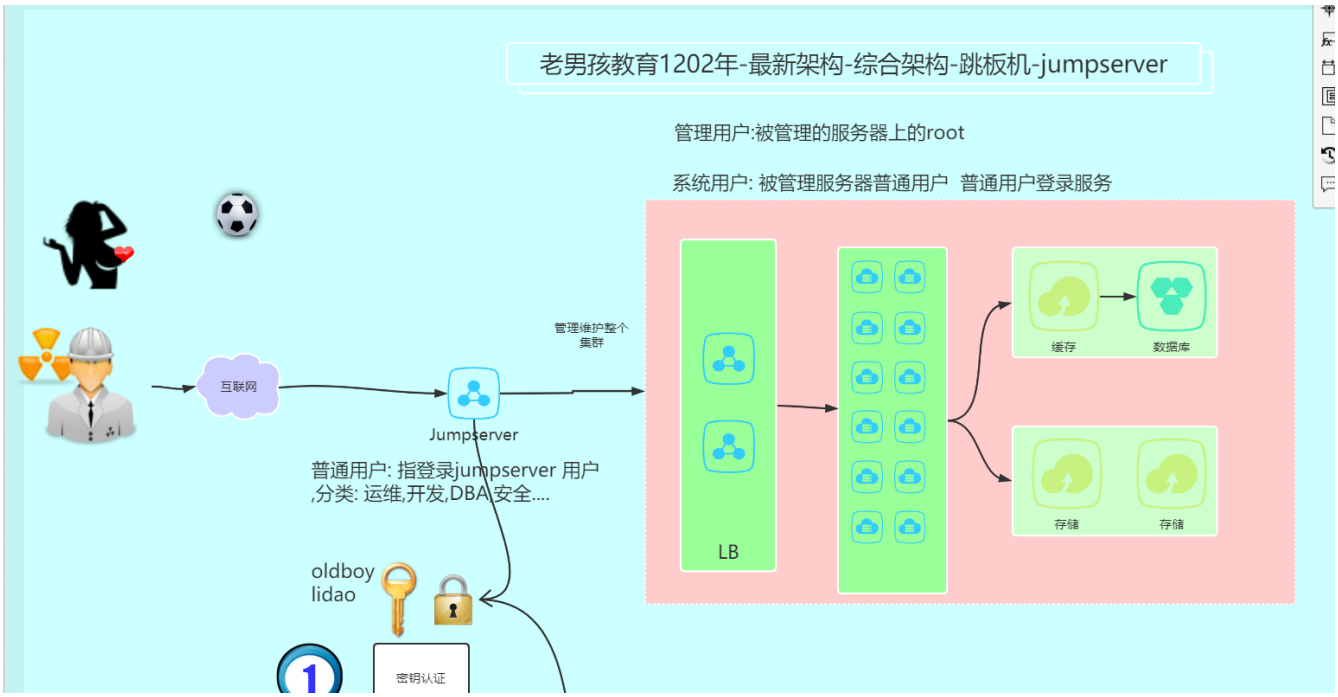
```
                Administrator,  欢迎使用JumpServer开源堡垒机系统

        1) 输入 部分IP, 主机名, 备注 进行搜索登录(如果唯一).
        2) 输入 / + IP, 主机名, 备注 进行搜索, 如: /192.168.
        3) 输入 p 进行显示您有权限的主机.
        4) 输入 g 进行显示您有权限的节点.
        5) 输入 d 进行显示您有权限的数据库.
        6) 输入 k 进行显示您有权限的Kubernetes.
        7) 输入 r 进行刷新最新的机器和节点信息.
        8) 输入 h 进行显示帮助.
        9) 输入 q 进行退出.
Opt>
```

2. 用户

管理用户	管理用户是资产（被控服务器）上的 **root**，或拥有 NOPASSWD: ALL sudo 权限的用户	
系统用户	系统用户是 JumpServer 跳转登录资产时使用的用户	
普通用户	普通用户: 指登录jumpserver 用户 ,分类: 运维,开发,DBA,安全....	

- 准备用户组(给用户组授权)
  - 运维
  - 开发
  - DBA
  - 安全



1. 添加普通用户（管理jms）

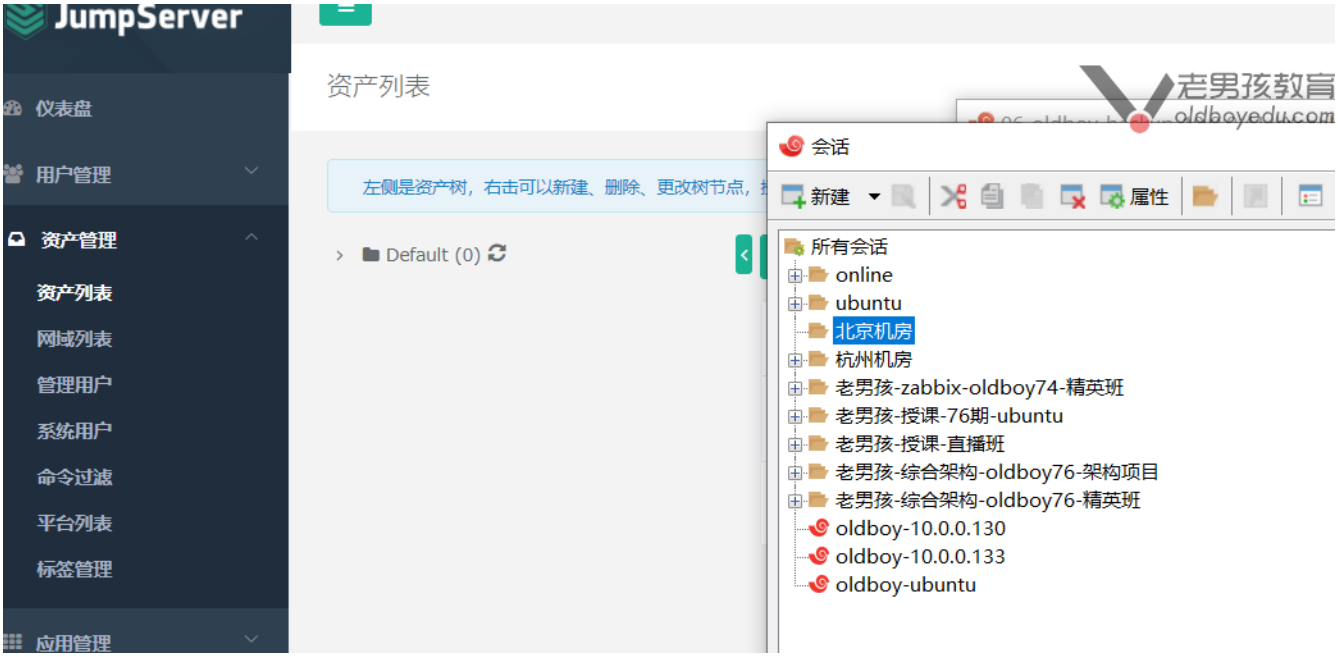
3. 资产

- 管理用户

- 添加主机-批量导入或手动添加

- 添加主机中使用的用户


JumpServer
仪表盘
用户管理
资产管理
资产列表
网域列表
管理用户
系统用户
命令过滤
平台列表
标签管理
应用管理
用户组
老男孩教育
oldboyedu.com
创建
更多操作
名称
DBA
开发
运维
Default
安全
1
2
3


JumpServer
仪表盘
用户管理
资产管理
资产列表
网域列表
管理用户
系统用户
命令过滤
平台列表
标签管理
应用管理
资产列表
老男孩教育
oldboyedu.com
左侧是资产树，右击可以新建、删除、更改树节点，
Default (0)
会话
新建
属性
所有会话
online
ubuntu
北京机房
杭州机房
老男孩-zabbix-oldboy74-精英班
老男孩-授课-76期-ubuntu
老男孩-授课-直播班
老男孩-综合架构-oldboy76-架构项目
老男孩-综合架构-oldboy76-精英班
oldboy-10.0.0.130
oldboy-10.0.0.133
oldboy-ubuntu

- 创建系统用户


基本
1
* 名称
zhuzhu
老男孩教育
oldboyedu.com
登录模
2
自动登录
手动登录
如果选择手动登录模式，用户名和密码可以不填写
用户名
用户名与用户相同
用户名是动态的，登录资产时使用当前用户的用户名登录
优先级
81
优先级可选范围为 1-100 (数值越小越优先)
* 协议
ssh
自动推送
3
自动推送
* Sudo
/bin/whoami
使用逗号分隔多个命令，如: /bin/whoami,/sbin/ifconfig
* Shell
/bin/bash
认证
自动生成密钥

4. 权限管理

-


仪表盘
用户管理
资产管理
应用管理
权限管理
资产授权
应用授权
资产授权
Default (8)
上海机房 (2)
北京机房 (2)
深圳机房 (2)
m01
nfs01
创建
更多操作
名称
老男孩教育
oldboyedu.com

- 添加授权


基本
* 名称
运维
老男孩教育
oldboyedu.com
用户
用户
请选择
用户组
运维
资产
资产
请选择
节点
/Default/北京机房/沙河机房
/Default
/Default/上海机房
/Default/北京机房
/Default/深圳机房
/Default/北京机房/大兴机房
* 系统用户
zhuzhu()
动作
权限
全部
剪切板权限控制目前仅支持 RDP/VNC 协议的连接

- 添加资产到可以批量管理流程
    - 添加用户组(用户)
    - 添加管理（特权）用户(root)
    - 添加系统用户：feilao web页面创建后，推送
    - 添加资产
    - 资产授权: 添加用户(jumpserver)与 资产关联()
    - 普通用户登录jumpserver管理

5. 数据库授权

-


JumpServer
仪表盘
用户管理
资产管理
资产列表
网域列表
管理用户
系统用户
命令过滤
平台列表
标签管理
应用管理
权限管理
会话管理
作业中心
日志审计
创建系统用户
老男孩教育
oldboyedu.com
基本
* 名称
all
登录模式
自动登录
手动登录
如果选择手动登录模式，用户名和密码可以不填写
* 用户名
all
优先级
81
优先级可选范围为 1-100 (数值越小越优先)
* 协议
mysql
认证
密码
密码或密钥密码

-


仪表盘
用户管理
资产管理
应用管理
数据库
Kubernetes
创建
搜索
老男孩教育
oldboyedu.com
名称
类型
主机
端口
数据库
备注
操作
数据库db01
MySQL
172.16.1.51
3306
172.16.1.51
更新
更多
共 1 条
15条/页
1

-

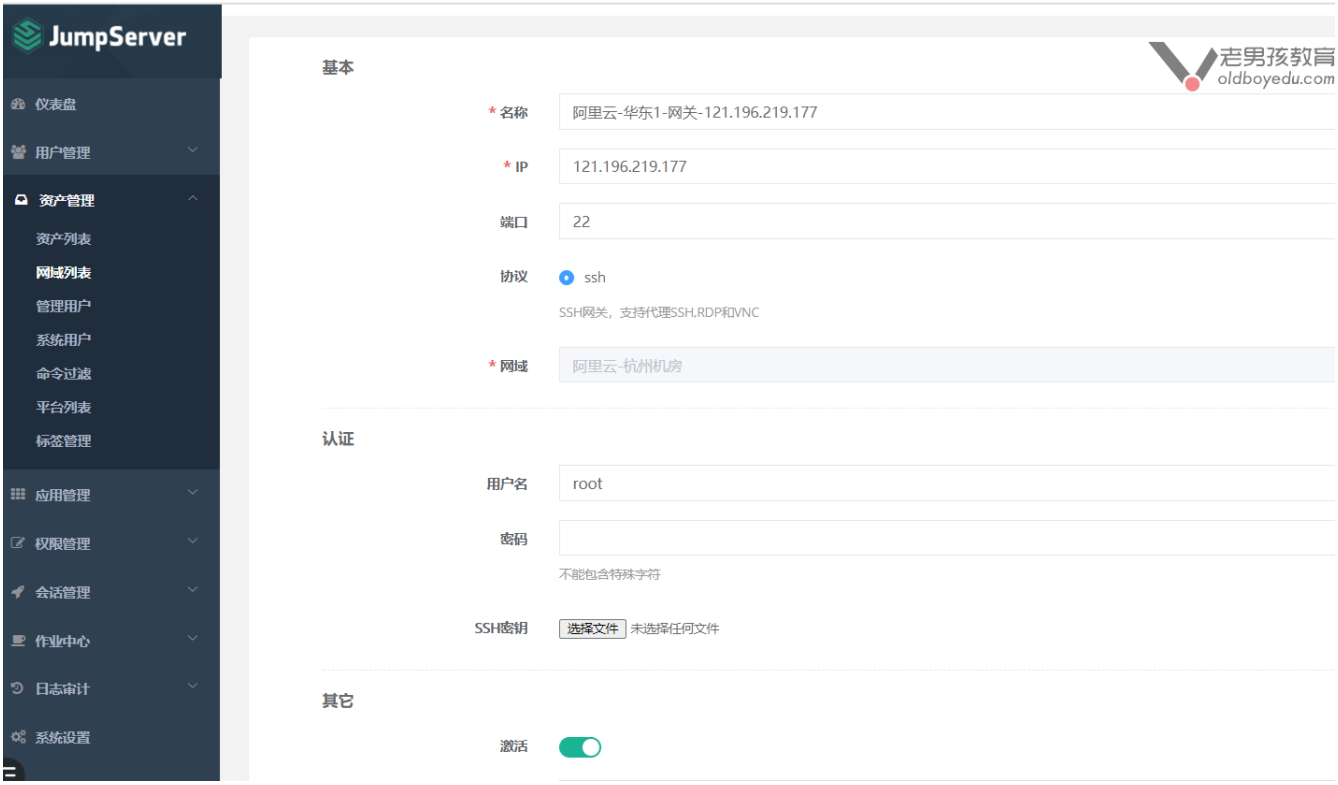
-

6. 多因子登录(二次验证)

- mfa 生成随机字符app
- jumpserver 谷歌登录验证器

7. 网域

- jumpserver批量关机多个地区机房
- JMS => 网域网关 => 目标资产
- 网域管理:

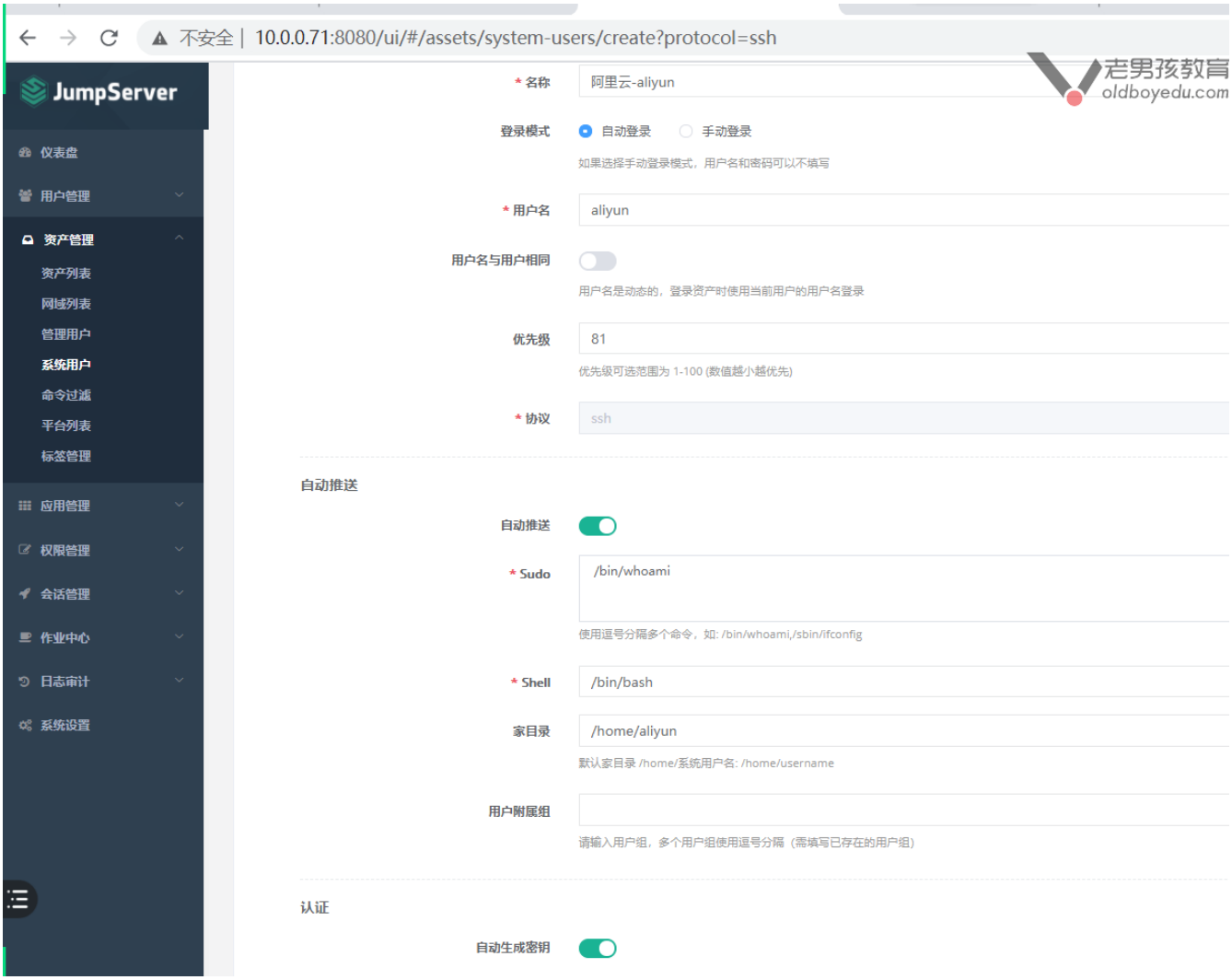


- 此处的秘钥是 跳板机到云服务器的私钥.

- 设置管理用户

- 秘钥是 云服务器(网关)与云服务内网服务器的 私钥

- 系统用户


不安全 | 10.0.0.71:8080/ui/#/assets/system-users/create?protocol=ssh
JumpServer
仪表盘
用户管理
资产管理
资产列表
网域列表
管理用户
系统用户
命令过滤
平台列表
标签管理
应用管理
权限管理
会话管理
作业中心
日志审计
系统设置
* 名称
阿里云-aliyun
登录模式
自动登录
手动登录
如果选择手动登录模式，用户名和密码可以不填写
* 用户名
aliyun
用户名与用户相同
用户名是动态的，登录资产时使用当前用户的用户名登录
优先级
81
优先级可选范围为 1-100 (数值越小越优先)
* 协议
ssh
自动推送
自动推送
* Sudo
/bin/whoami
使用逗号分隔多个命令，如: /bin/whoami,/sbin/ifconfig
* Shell
/bin/bash
家目录
/home/aliyun
默认家目录 /home/系统用户名: /home/username
用户附属组
请输入用户组，多个用户组使用逗号分隔（需填写已存在的用户组）
认证
自动生成密钥

- 添加资产

基本

* 主机名 172.16.1.81

* IP(域名) 172.16.1.81

* 系统平台 Linux

公网IP

网域 阿里云-杭州机房

协议组

协议组 ssh 22

认证

* 管理用户 阿里云-华东1-root用户(root)

节点

* 节点 /Default/阿里云-华东1(杭州))

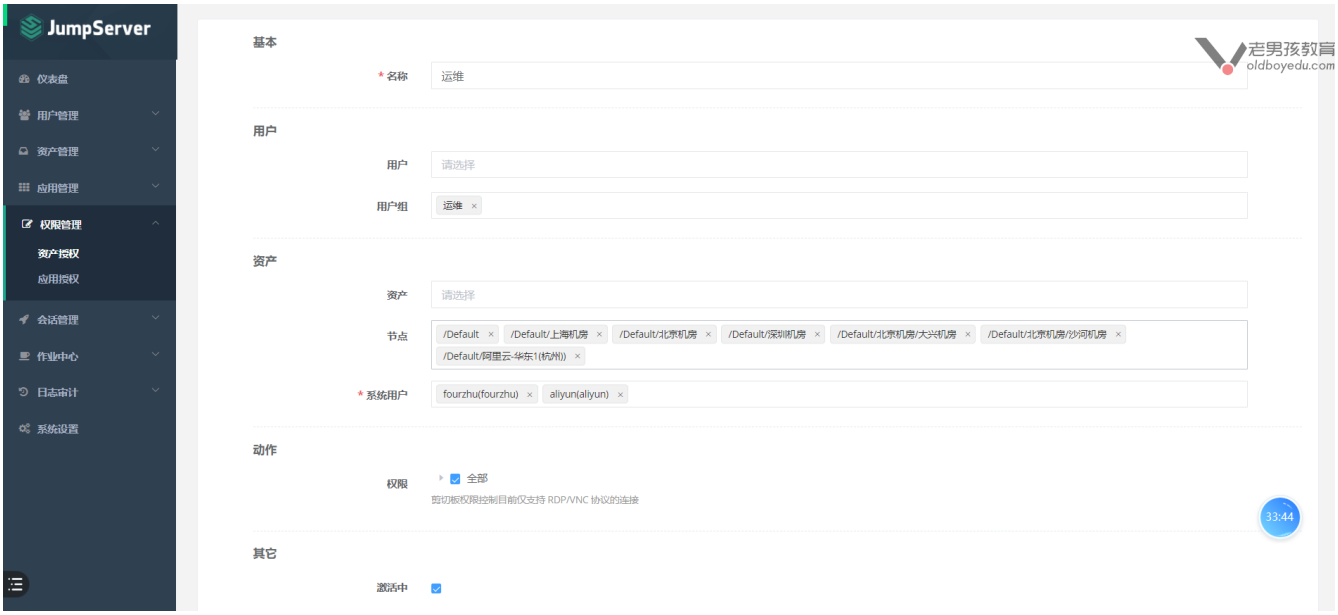
标签

标签管理 请选择

其它

激活

- 授权



8. LDAP oldboy oldboy123

- 域控
  - LDAP(OpenLDAP) linux
  - AD(域控) windows
- 公司有多个产品,各种产品都有不同的账号
  - 监控zabbix
  - 跳板机
  - 产品....
  -

9. 安全与优化

- 安全:
  - 用户--->vpn---->防火墙---->跳板机---->资产
  - https
- 优化:
  - 组件分离,手动部署