jumpserver应用

一、jumpserver介绍

堡垒机、跳板机

基于python开发

JumpServer 现已支持管理 SSH、 Telnet、 RDP、 VNC 协议资产

1、jumpserver核心组件

1) jumpserver　核心组件

2) Luna　提供web管理界面

3) Koko　提供ssh服务

4) Guacamole 提供对windows服务器支持

二、jumpserver安装部署

1、安装MySQL， redis

```
[root@jumpserver ~]# yum install -y epel-release
[root@jumpserver ~]# yum install -y mariadb-server redis

[root@jumpserver ~]# vim /etc/redis.conf
bind 192.168.183.10

[root@jumpserver ~]# systemctl start mariadb redis
[root@jumpserver ~]# systemctl enable mariadb redis
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/redis.service to /usr/lib/systemd/system/redis.service.
[root@jumpserver ~]#
[root@jumpserver ~]# netstat -antp | grep -E "mysql|redis"
tcp 0 0 192.168.183.10:6379 0.0.0.0:* LISTEN 1314/redis-server 1
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 1559/mysqld
```

2、创建jumpserver数据库，授权用户

```
MariaDB [(none)]> create database jumpserver charset utf8 collate utf8_bi
n;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all on jumpserver.* to 'jumpuser'@'localhost' ide
ntified by 'redhat';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

3、编译安装python 3.6.12

```
[root@jumpserver ~]# yum install -y openssl-devel
[root@jumpserver ~]# tar xf Python-3.6.12.tar.xz
[root@jumpserver ~]# cd Python-3.6.12/
[root@jumpserver Python-3.6.12]# ./configure && make && make install

[root@jumpserver ~]# python3
Python 3.6.12 (default, Oct 20 2020, 09:42:42)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>>
>>> exit()
```

4、创建jumpserver项目对应的虚拟环境

```
//创建虚拟环境
[root@jumpserver ~]# cd /opt/
[root@jumpserver opt]# python3 -m venv jumpserver_venv

//进入虚拟环境
[root@jumpserver opt]# source jumpserver_venv/bin/activate

退出虚拟环境
```

```
(jumpserver_venv) [root@jumpserver /]# deactivate
```

5、下载安装jumpserver组件

```
(jumpserver_venv) [root@jumpserver ~]# tar xf jumpserver-v2.3.1.tar.gz
(jumpserver_venv) [root@jumpserver ~]# mv jumpserver-v2.3.1 /opt/jumpserver
```

6、安装jumpserver需要的python模块

```
(jumpserver_venv) [root@jumpserver ~]# yum install -y $(cat /opt/jumpserver/requirements/rpm_requirements.txt)
(jumpserver_venv) [root@jumpserver ~]# pip3 install -r /opt/jumpserver/requirements/requirements.txt
```

7、编辑修改jumpserver的配置文件

```
[root@jumpserver ~]# cp /opt/jumpserver/config_example.yml /opt/jumpserver/config.yml
[root@jumpserver ~]# vim /opt/jumpserver/config.yml
SECRET_KEY: cisTgGO75QWy0Ss2QOyHsDzaCz0TJI6Or3i959hMopXv5fDMW
BOOTSTRAP_TOKEN: 39a0419bac0c2a437384
LOG_LEVEL: ERROR
LOG_DIR: /var/log/jumpserver.log

DB_ENGINE: mysql
DB_HOST: localhost
 DB_PORT: 3306
 DB_USER: jumpuser
 DB_PASSWORD: redhat
 DB_NAME: jumpserver

 REDIS_HOST: 192.168.183.10
 REDIS_PORT: 6379
```

8、启动jumpserver

```
(jumpserver_venv) [root@jumpserver jumpserver]# ./jms start

(jumpserver_venv) [root@jumpserver jumpserver]# netstat -antp | grep 8080
tcp 0 0 0.0.0.0:8080 0.0.0.0:* LISTEN 32815/python3
```

9、安装koko组件，提供SSH服务

```
(jumpserver_venv) [root@jumpserver ~]# tar xf koko-v2.4.0-linux-amd64.tar.gz
(jumpserver_venv) [root@jumpserver ~]# mv koko-v2.4.0-linux-amd64 /opt/koko
(jumpserver_venv) [root@jumpserver ~]# chown -R root.root /opt/koko

(jumpserver_venv) [root@jumpserver ~]# cp /opt/koko/config_example.yml /opt/koko/config.yml
(jumpserver_venv) [root@jumpserver ~]# vim /opt/koko/config.yml
BOOTSTRAP_TOKEN: 39a0419bac0c2a437384

(jumpserver_venv) [root@jumpserver koko]# ./koko -d
(jumpserver_venv) [root@jumpserver koko]# netstat -antp | grep 2222
tcp6 0 0 :::2222 :::* LISTEN 2413/./koko
```

10、安装lina组件，提供web ui界面

```
(jumpserver_venv) [root@jumpserver ~]# tar xf lina-v2.4.0.tar.gz
(jumpserver_venv) [root@jumpserver ~]# mv lina-v2.4.0 /opt/lina
(jumpserver_venv) [root@jumpserver ~]# chown -R nginx.nginx /opt/lina
```

11、安装luna组件, 提供web终端管理

```
(jumpserver_venv) [root@jumpserver ~]# tar xf luna-v2.4.0.tar.gz
(jumpserver_venv) [root@jumpserver ~]# mv luna-v2.4.0 /opt/luna
(jumpserver_venv) [root@jumpserver ~]# chown -R nginx.nginx /opt/luna
```

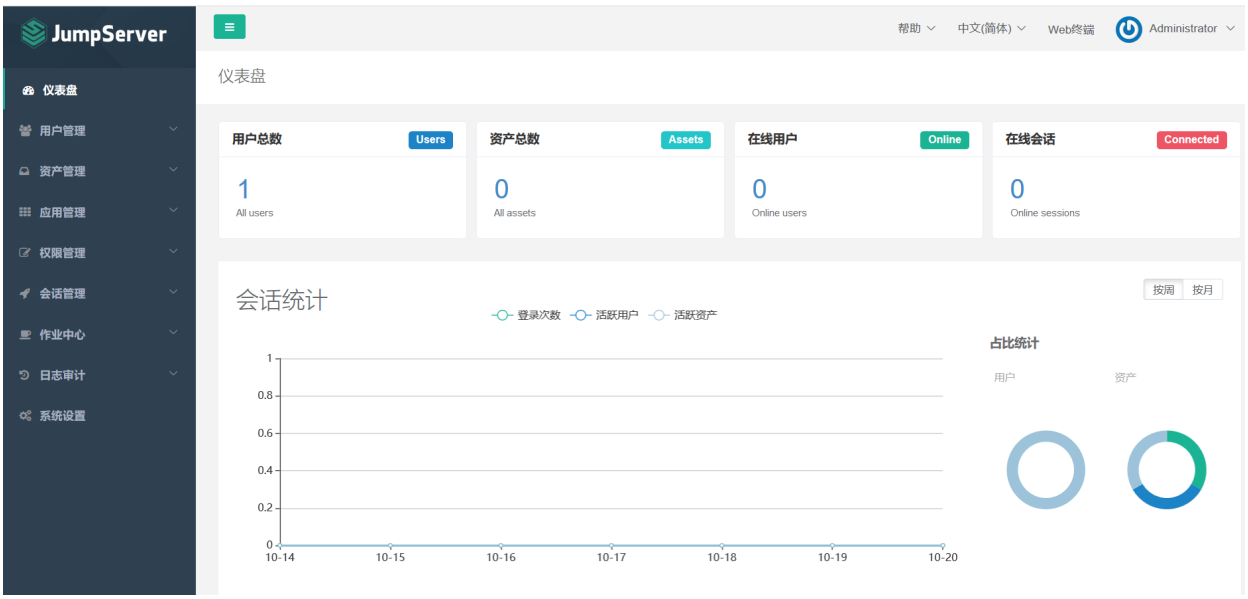
12、安装nginx，整合所有组件

```
(jumpserver_venv) [root@jumpserver ~]# yum install -y nginx
(jumpserver_venv) [root@jumpserver ~]# vim /etc/nginx/nginx.conf
 <复制官网nginx配置>
(jumpserver_venv) [root@jumpserver ~]# systemctl start nginx
(jumpserver_venv) [root@jumpserver ~]# systemctl enable nginx
(jumpserver_venv) [root@jumpserver ~]# netstat -antp | grep nginx
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 2627/nginx: master
(jumpserver_venv) [root@jumpserver ~]#
```

13、访问jumpserver的登录界面

```
http://192.168.183.10
```

默认用户名admin，密码admin



三、jumpserver的使用

1、创建用户

运维人员连接登录堡垒机的账号

2、创建资产

1) 创建管理用户

获取硬件配置信息、推送系统用户

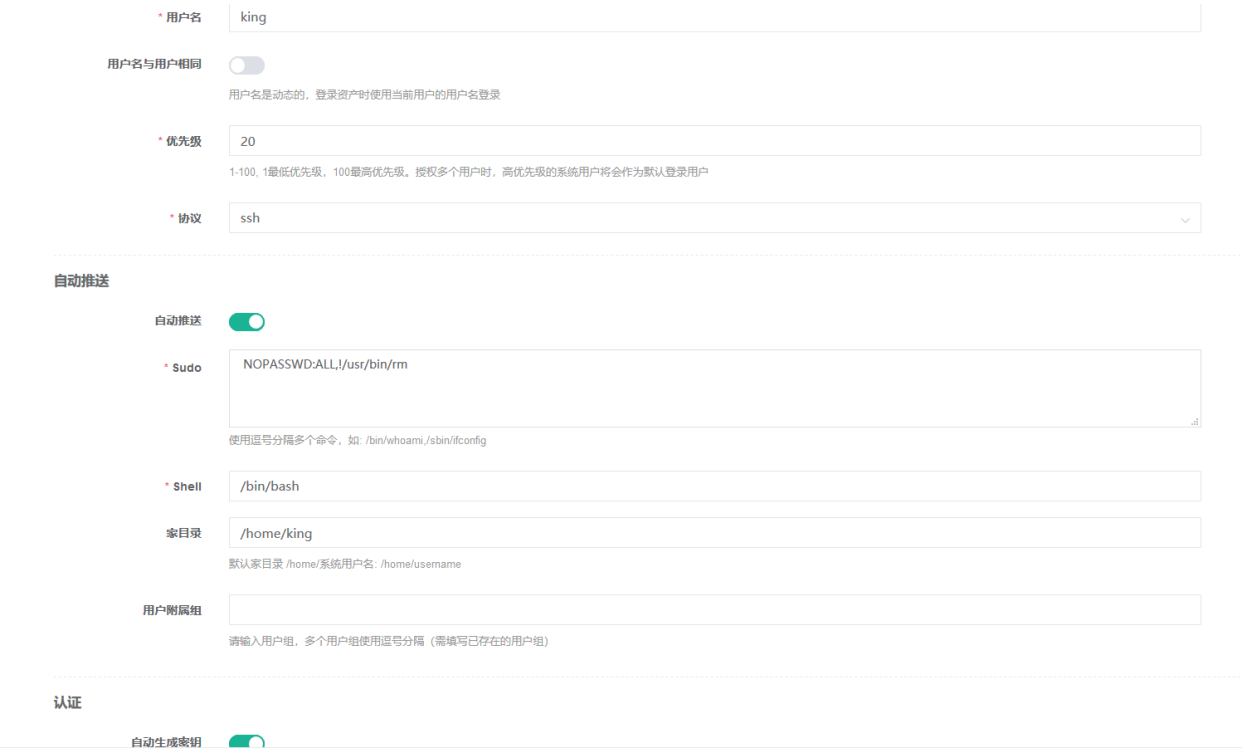
后端服务器真实存在root用户、普通用户(NOPASSWD:ALL)

2) 创建资产

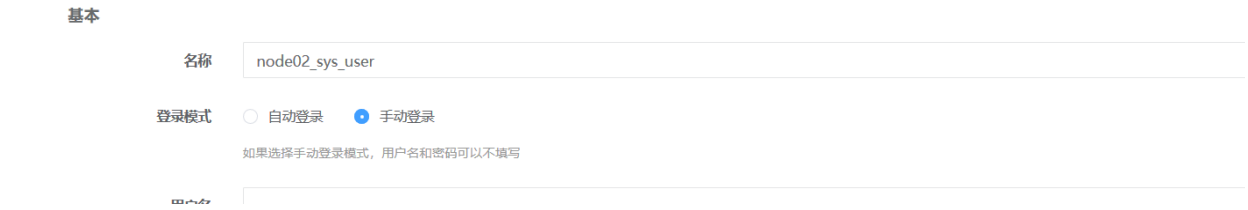
3、创建系统用户

用于堡垒机连接资产服务器

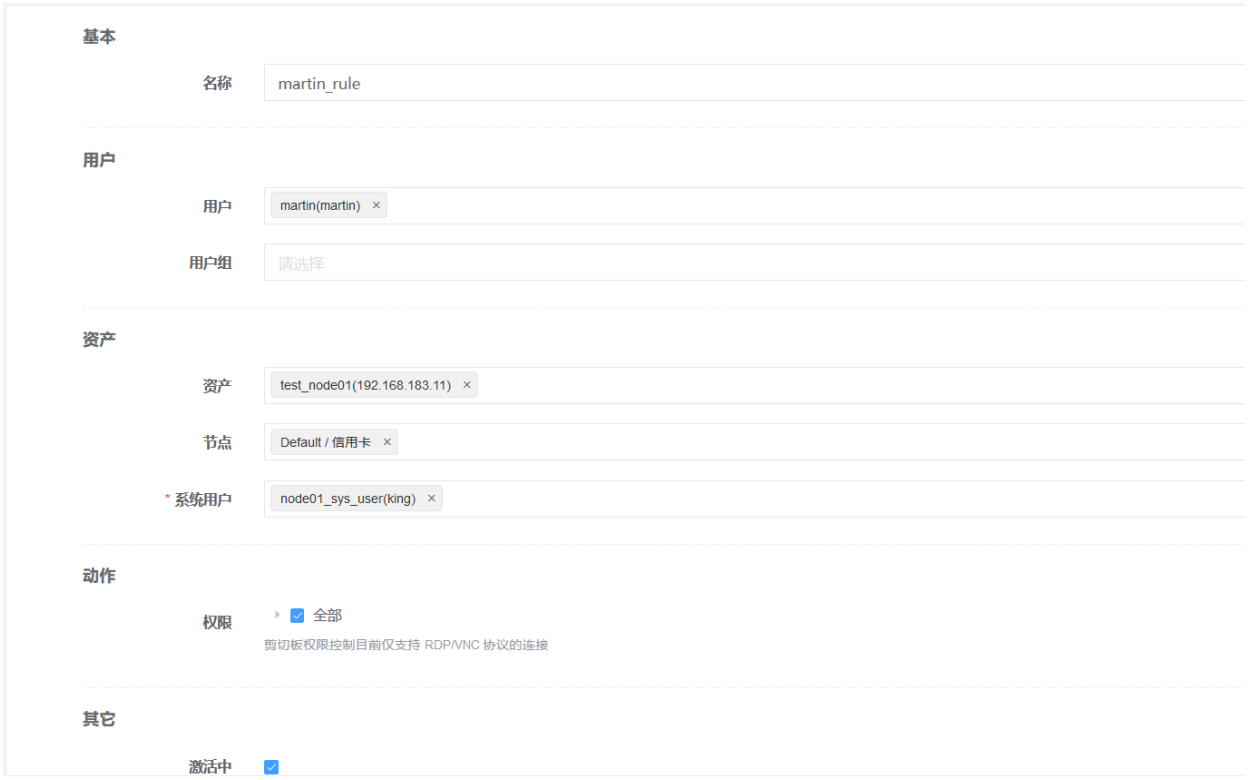
1) 自动登录用户



2) 手动登录



4、创建资产授权



创建资产授权规则

基本

名称: robin_rule

用户

用户: robin(robin) ×

用户组: 请选择

资产

资产: test_node02(192.168.183.12) ×

节点: Default / 手机银行 ×

* 系统用户: node02_sys_user() ×

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