

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

```
1 [root@jumpserver ~]# yum install -y epel-release
2 [root@jumpserver ~]# yum install -y mariadb-server redis
3
4 [root@jumpserver ~]# vim /etc/redis.conf
5 bind 192.168.183.10
6
7 [root@jumpserver ~]# systemctl start mariadb redis
8 [root@jumpserver ~]# systemctl enable mariadb redis
9 Created symlink from /etc/systemd/system/multi-
  user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.servic
  e.
10 Created symlink from /etc/systemd/system/multi-user.target.wants/redis.s
  ervice to /usr/lib/systemd/system/redis.service.
11 [root@jumpserver ~]#
12 [root@jumpserver ~]# netstat -antp | grep -E "mysql|redis"
13 tcp 0 0 192.168.183.10:6379 0.0.0.0:* LISTEN 1314/redis-server 1
14 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

```
1 MariaDB [(none)]> create database jumpserver charset utf8 collate utf8_bin;
2 Query OK, 1 row affected (0.00 sec)
3
4 MariaDB [(none)]> grant all on jumpserver.* to 'jumpuser'@'localhost' identified by 'redhat';
5 Query OK, 0 rows affected (0.00 sec)
6
7 MariaDB [(none)]> flush privileges;
8 Query OK, 0 rows affected (0.00 sec)
```

3、编译安装python 3.6.12

```
1 [root@jumpserver ~]# yum install -y openssl-devel
2 [root@jumpserver ~]# tar xf Python-3.6.12.tar.xz
3 [root@jumpserver ~]# cd Python-3.6.12/
4 [root@jumpserver Python-3.6.12]# ./configure && make && make install
5
6 [root@jumpserver ~]# python3
7 Python 3.6.12 (default, Oct 20 2020, 09:42:42)
8 [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux
9 Type "help", "copyright", "credits" or "license" for more information.
10 >>>
11 >>>
12 >>> exit()
```

4、创建jumpserver项目对应的虚拟环境

```
1 //创建虚拟环境
2 [root@jumpserver ~]# cd /opt/
3 [root@jumpserver opt]# python3 -m venv jumpserver_venv
4
5 //进入虚拟环境
6 [root@jumpserver opt]# source jumpserver_venv/bin/activate
7
8 退出虚拟环境
```

```
9 (jumpserver_venv) [root@jumpserver ~]# deactivate
```

5、下载安装jumpserver组件

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

6、安装jumpserver需要的python模块

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

7、编辑修改jumpserver的配置文件

```
1 [root@jumpserver ~]# cp /opt/jumpserver/config_example.yml /opt/jumpserver/config.yml
2 [root@jumpserver ~]# vim /opt/jumpserver/config.yml
3 SECRET_KEY: cisTgG075QWy0Ss2Q0yHsDzaCz0TJI60r3i959hMopXv5fDMW
4 BOOTSTRAP_TOKEN: 39a0419bac0c2a437384
5 LOG_LEVEL: ERROR
6 LOG_DIR: /var/log/jumpserver.log
7
8 DB_ENGINE: mysql
9 DB_HOST: localhost
10 DB_PORT: 3306
11 DB_USER: jumpuser
12 DB_PASSWORD: redhat
13 DB_NAME: jumpserver
14
15 REDIS_HOST: 192.168.183.10
16 REDIS_PORT: 6379
```

8、启动jumpserver

```
1 (jumpserver_venv) [root@jumpserver jumpserver]# ./jms start
2
3 (jumpserver_venv) [root@jumpserver jumpserver]# netstat -antp | grep 8080
4 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

```
1 (jumpserver_venv) [root@jumpserver ~]# tar xf koko-v2.4.0-linux-  
amd64.tar.gz  
2 (jumpserver_venv) [root@jumpserver ~]# mv koko-v2.4.0-linux-amd64 /opt/koko  
3 (jumpserver_venv) [root@jumpserver ~]# chown -R root.root /opt/koko  
4  
5 (jumpserver_venv) [root@jumpserver ~]# cp /opt/koko/config_example.yml /o  
pt/koko/config.yml  
6 (jumpserver_venv) [root@jumpserver ~]# vim /opt/koko/config.yml  
7 BOOTSTRAP_TOKEN: 39a0419bac0c2a437384  
8  
9 (jumpserver_venv) [root@jumpserver koko]# ./koko -d  
10 (jumpserver_venv) [root@jumpserver koko]# netstat -antp | grep 2222  
11 tcp6 0 0 :::2222 :::* LISTEN 2413/./koko
```

10、安装lina组件, 提供web ui界面

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

11、安装luna组件, 提供web终端管理

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

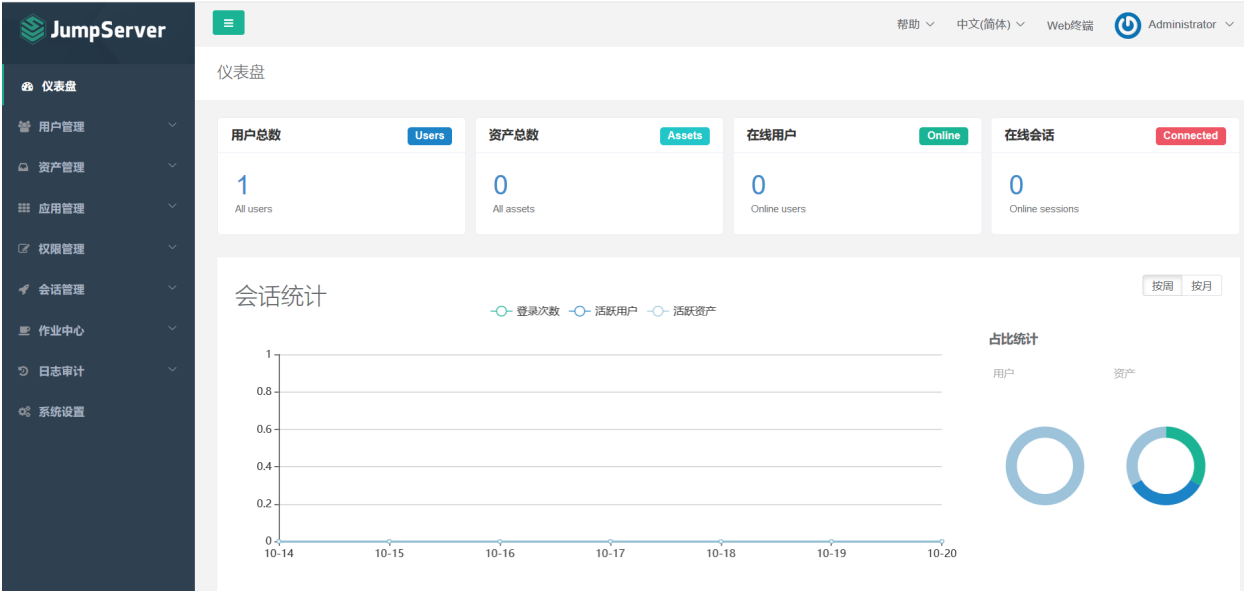
12、安装nginx, 整合所有组件

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

13、访问jumpserver的登录界面

```
1 http://192.168.183.10
```

默认用户名admin，密码admin



```
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.
```

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

* 用户名 king

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 20

1-100, 1最低优先级, 100最高优先级。授权多个用户时，高优先级的系统用户将会作为默认登录用户

* 协议 ssh

自动推送

自动推送 ☒

* Sudo NOPASSWD:ALL, /usr/bin/rm

使用逗号分隔多个命令，如: /bin/whoami,/sbin/ifconfig

* Shell /bin/bash

家目录 /home/king

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 ☒

2) 手动登录

基本

名称	node02_sys_user
登录模式	<input type="radio"/> 自动登录 <input checked="" type="radio"/> 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	
密码	

4、创建资产授权

基本

名称	martin_rule
----	-------------

用户

用户	martin(martin) ×
用户组	请选择

资产

资产	test_node01(192.168.183.11) ×
节点	Default / 信用卡 ×
* 系统用户	node01_sys_user(king) ×

动作

权限	<input checked="" type="checkbox"/> 全部
剪切板权限控制目前仅支持 RDP/VNC 协议的连接	

其它

激活中	<input checked="" type="checkbox"/>
-----	-------------------------------------

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