

# Jumpserver v0.5.0 开源堡垒机使用详解

Jumpserver 是一款由 python 编写开源的跳板机(堡垒机)系统，是全球首款完全开源的堡垒机，是符合 4A 的专业运维审计系统。实现了跳板机应有的功能。基于 ssh 协议来管理，客户端无需安装 agent。

Jumpserver 使用 Python / Django 进行开发，遵循 Web 2.0 规范，配备了业界领先的 Web Terminal 解决方案，交互界面美观、用户体验好。

Jumpserver 采纳分布式架构，支持多机房跨区域部署，中心节点提供 API，各机房部署登录节点，可横向扩展、无并发限制。

支持常见系统：

- 1.RedHat Linux 和 CentOS
- 2.Debian
- 3.SUSE Linux 和 Ubuntu
- 4.FreeBSD
- 5.其他 ssh 协议硬件设备

## 1.1.1 一. Jumpserver 启动 Python: 版本 3.6

### 1.1 启动 Jumpserver

先进入 Python 虚拟环境

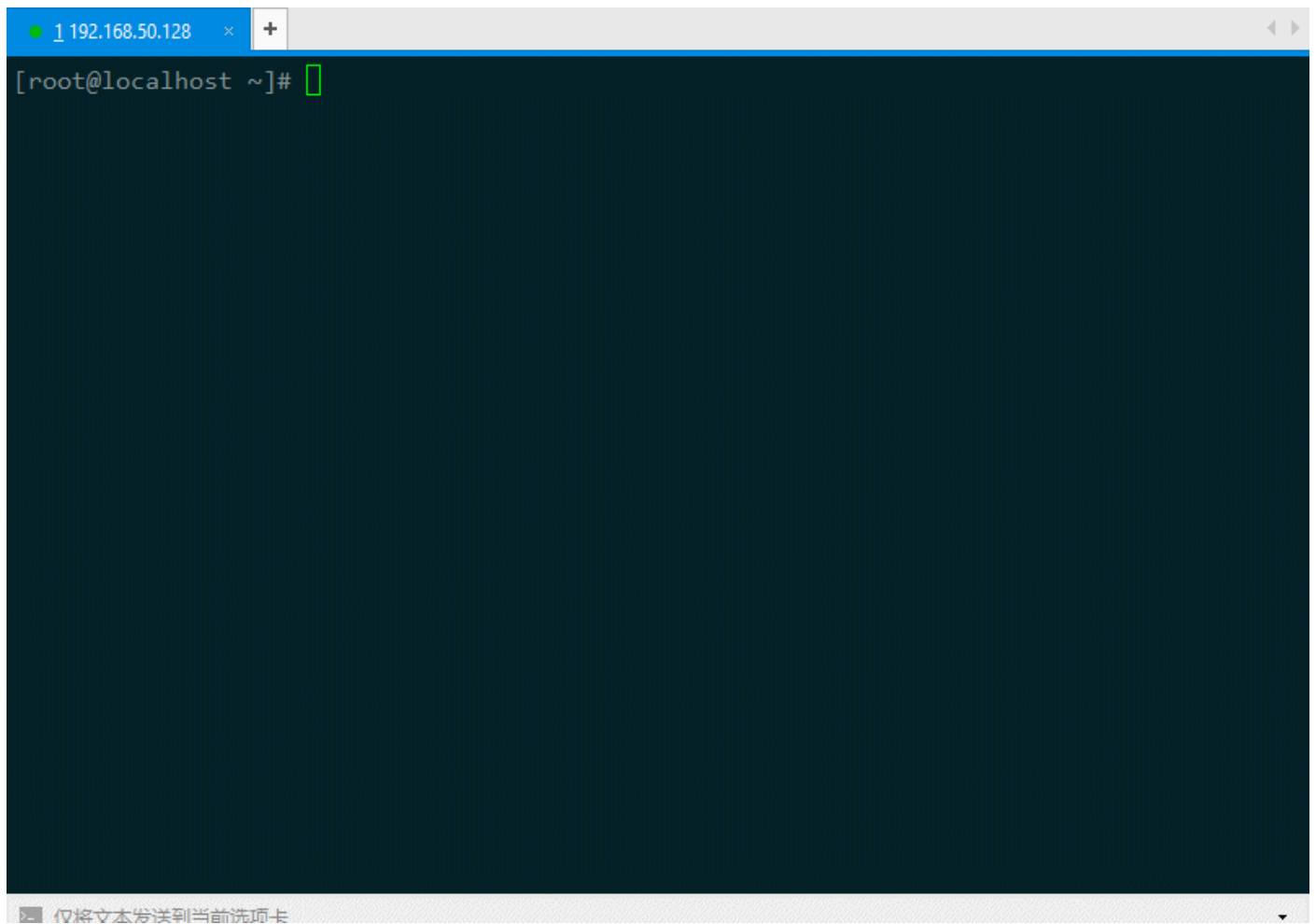
```
[root@localhost ~]# source /opt/py3/bin/activate
```

```
(py3) [root@localhost ~]# service redis start
Redirecting to /bin/systemctl start redis.service
```

```
(py3) [root@localhost ~]# cd /opt/jumpserver/
```

```
(py3) [root@localhost jumpserver]# sh nginx.sh start
Starting nginx: [ OK ]
```

```
(py3) [root@localhost jumpserver]# python run_server.py all
Sun Jan 28 21:19:21 2018
Jumpserver version 0.5.0, more see https://www.jumpserver.org
Quit the server with CONTROL-C.
- Start Gunicorn WSGI HTTP Server
Check database change, make migrations
2018-01-28 21:19:23 [signals_handler DEBUG] Receive django ready signal
....
```



## 1.2 启动 coco

先进入 Python 虚拟环境

```
[root@localhost ~]# source /opt/py3/bin/activate
```

```
(py3) [root@localhost ~]# cd /opt/coco/
```

```
(py3) [root@localhost coco]# python run_server.py
```

```
2018-01-28 22:06:47 [service DEBUG] Initial app service
```

```
2018-01-28 22:06:47 [service DEBUG] Load access key
```

```
2018-01-28 22:06:47 [service INFO] No access key found, register it
```

```
2018-01-28 22:06:47 [service INFO] "Terminal was not accepted yet"
```

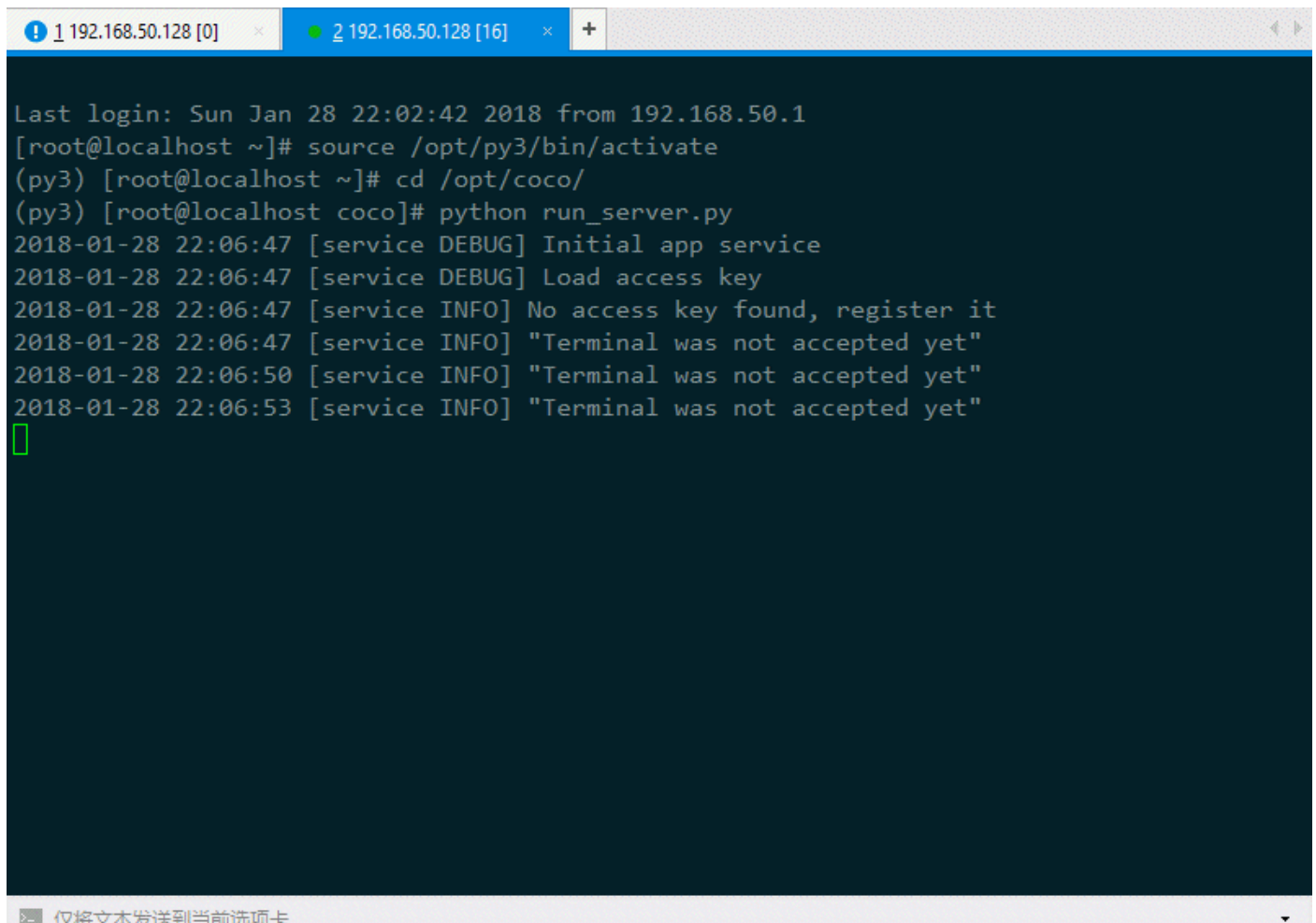
```
2018-01-28 22:06:50 [service INFO] "Terminal was not accepted yet"
```

```
...
```

```
1 192.168.50.128 x +
127.0.0.1 [28/Jan/2018:21:37:33 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
127.0.0.1 [28/Jan/2018:21:37:39 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
127.0.0.1 [28/Jan/2018:21:37:45 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
127.0.0.1 [28/Jan/2018:21:37:51 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
127.0.0.1 [28/Jan/2018:21:37:58 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
beat: Synchronizing schedule...
Writing entries...
beat: Waking up in 1.00 minute.
127.0.0.1 [28/Jan/2018:21:38:04 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
201 2
127.0.0.1 [28/Jan/2018:21:38:07 +0800] "DELETE /api/terminal/v1/terminal/f6c3562e-bdd1-4
215-bf14-5ee34d92cade/ HTTP/1.0" 204 -
127.0.0.1 [28/Jan/2018:21:38:10 +0800] "POST /api/terminal/v1/terminal/status/ HTTP/1.1"
403 31
127.0.0.1 [28/Jan/2018:21:38:11 +0800] "GET /users/logout HTTP/1.0" 200 2886
127.0.0.1 [28/Jan/2018:21:38:13 +0800] "GET /users/login HTTP/1.0" 200 4678
127.0.0.1 [28/Jan/2018:21:38:14 +0800] "GET /captcha/image/1112e1e446713a9980a6ff8459ac9
6ceaab96e25/ HTTP/1.0" 200 4266
beat: Waking up in 1.00 minute.
█
仅将文本发送到当前选项卡
```

1.3 访问 jumpserver 管理后台接受 coco 的注册

http://ip 账号密码: admin admin



A terminal window with a dark blue background and white text. The window has two tabs at the top: the first tab is labeled '1 192.168.50.128 [0]' and the second tab is labeled '2 192.168.50.128 [16]'. The terminal output shows the following sequence of commands and messages:

```
Last login: Sun Jan 28 22:02:42 2018 from 192.168.50.1
[root@localhost ~]# source /opt/py3/bin/activate
(py3) [root@localhost ~]# cd /opt/coco/
(py3) [root@localhost coco]# python run_server.py
2018-01-28 22:06:47 [service DEBUG] Initial app service
2018-01-28 22:06:47 [service DEBUG] Load access key
2018-01-28 22:06:47 [service INFO] No access key found, register it
2018-01-28 22:06:47 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:50 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:53 [service INFO] "Terminal was not accepted yet"
█
```

At the bottom of the terminal window, there is a status bar with a small icon and the text '仅将文本发送到当前选项卡'.

## 1.4 系统设置

### 1.4.1 基本设置

→ ↺ 192.168.50.128/settings/

Jumpserver

仪表盘

用户管理

资产管理

限管理

活

作业中心

系统设置

公社  
linux  
www.linuxidc.com

≡

仪表盘 / 系统设置 / 基本设置

您的ssh秘钥没有设置或已失效，请点击 [链接](#) 更新

基本设置

邮件设置

LDAP设置

当前站点URL

http://192.168.50.128  
http://jumpserver.abc.com:8080

用户向导URL

http://192.168.50.128  
用户第一次登录，修改profile后重

Email主题前缀

[Jumpserver]

重置

提交

1.4.2 邮件设置

→ ↻ 不安全 | 192.168.50.128/settings/email/

Jumpserver

仪表盘

用户管理

资产管理

权限管理

会话

作业中心

系统设置

仪表盘 / 系统设置 / 邮件设置

您的ssh秘钥没有设置或已失效, 请点击 [链接](#) 更新

基本设置

邮件设置

LDAP设置

终端

SMTP主机

smtp.exmail.qq.com

SMTP端口

465

SMTP账号

\*\*\*\*\*

SMTP密码

\*\*\*\*\*

一些邮件提供商需要输入的是Token

使用SSL

☒

如果SMTP端口是465,

使用TLS

☐

如果SMTP端口是587,

测试连接

重置


提交

## 1.5 创建用户并登录

创建用户会发送邮件，需要设置密码，登录

### 1.5.1. 创建用户

→ 192.168.50.128/users/user

 Jumpserver

仪表盘

用户管理

用户

用户组

登录日志

资产管理

权限管理

会话

作业中心

系统设置

仪表盘 / 用户管理 / 用户列表


您的ssh密钥没有设置或已失效, 请点击 [链接](#) 更新

用户列表

创建用户

|                          |               |   |
|--------------------------|---------------|---|
| <input type="checkbox"/> | 名称            | ↕ |
| <input type="checkbox"/> | Administrator |   |

批量删除 提交

  
www.linuxidc.com

1.5.2. 创建用户jms

→ ↺

🛡️ 不安全 | 192.168.50.128/users/user/create

🏠 仪表盘

👤 用户管理

👤 用户

👤 用户组

📅 登录日志

💼 资产管理

🔑 权限管理

💬 会话

📋 作业中心

⚙️ 系统设置

仪表盘 / 用户管理 / 创建用户

您的ssh秘钥没有设置或已失效，请点击 [链接](#) 更新

创建用户

账户

名称

jumpserver

\* required

用户名

jms

\* required

邮件

704564722@qq.com

\* required

用户组

× Default |

认证

密码

生成重置密码连接，通过邮件发送给用户

角色安全

角色

用户

失效日期

📅

2088-01-12

公社

linux

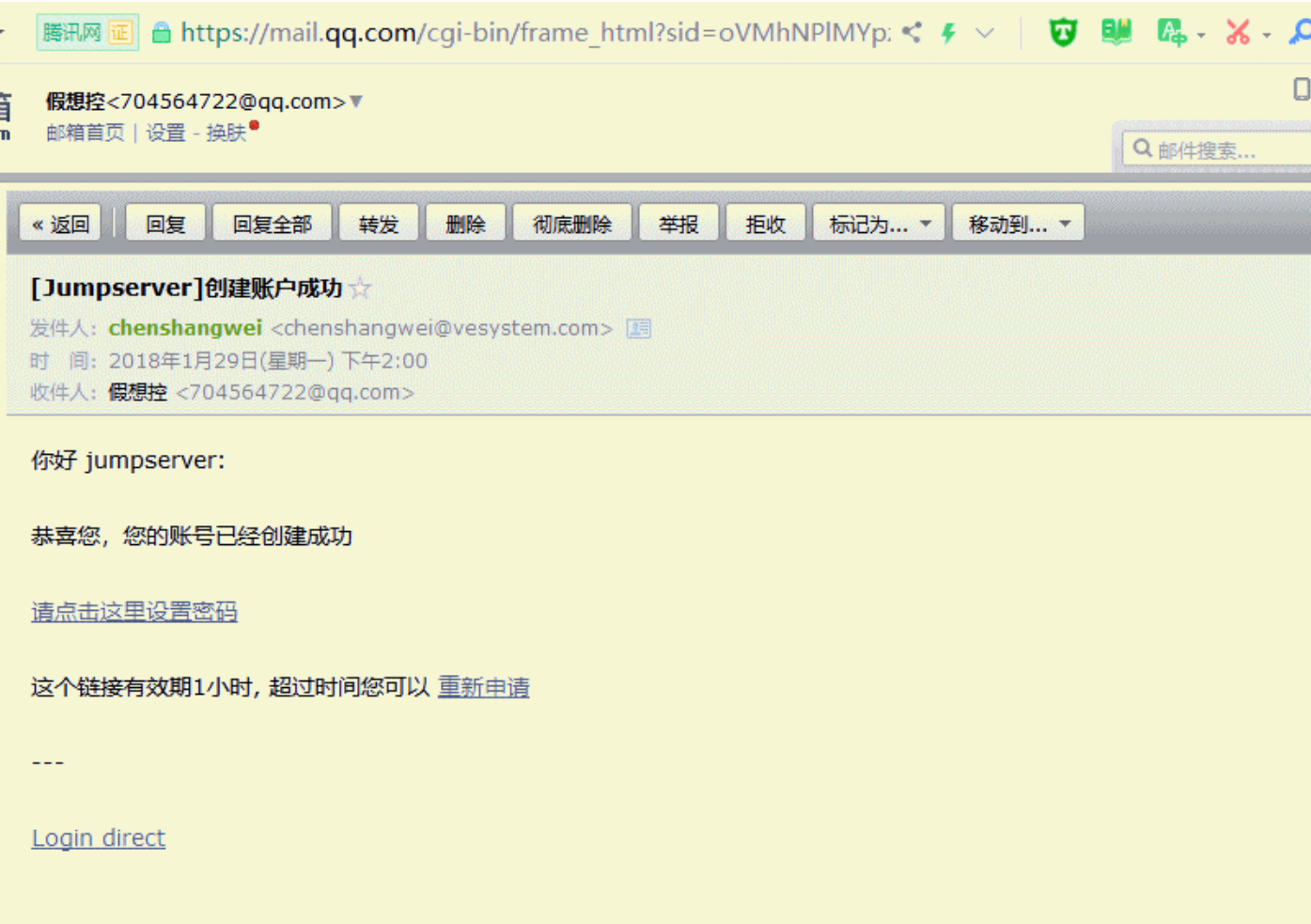
www.linuxidc.com

1.5.3. 发送邮件创建帐户成功





1.5.4. 打开邮件点设置密码 登录用户 jms



1.6 创建管理用户

创建一个管理用户, 创建资产时需要关联

1.6.1. 创建管理用户



1.6.2. 管理用户为root

仪表盘

用户管理

资产管理

资产

资产组

集群

管理用户

系统用户

标签管理

权限管理

会话

作业中心

系统设置

仪表盘 / 资产管理 / 创建管理用户

您的ssh私钥没有设置或已失效，请点击 [链接](#) 更新

### 创建管理用户

名称

root

\* required

用户名

root

\* required

密码

.....

密码或密钥密码

ssh私钥

[选择文件](#) id\_rsa

备注

备注



[www.linuxidc.com](http://www.linuxidc.com)

重置

提交

您的ssh秘钥没有设置或已失效，请点击 [链接](#) 更新

root 创建成功

管理用户是 服务器上已存在的特权用户，Jumpserver使用该用户来“推送系统用户”、“获取资产硬件信息”等。可以设置主机级别管理用户，也设置集群级别管理用户，这样资产可以不用再单独设置

管理用户列表

创建管理用户

|                          | 名称   | 用户名  | 资产 | 可连接 | 不可达 | 比例 | 备注 | 动作                                    |
|--------------------------|------|------|----|-----|-----|----|----|---------------------------------------|
| <input type="checkbox"/> | root | root | 0  | 0   | 0   | 0% |    | <a href="#">更新</a> <a href="#">删除</a> |

显示第 1 至 1 项结果, 总共 1 项

1.7 创建资产

创建一个资产,关联刚创建的管理用户

1.7.1. 创建资产

192.168.50.128/assets/asset/

Jumpserver

仪表盘

用户管理

资产管理

资产

资产组

集群

管理用户

创建资产

仪表盘 / 资产管理 / 资产列表

您的ssh秘钥没有设置或已失效，请点击 [链接](#) 更新

资产列表

|  | 主机名 | IP |
|--|-----|----|
|--|-----|----|

1.7.2. 添加资产并关联管理用户

## 基本

主机名

CentOS 7.2

\* required

IP

192.168.50.129

\* required

端口

22

\* required

集群

Default

\* required

公网IP

公网IP

系统类型

物理机

资产环境

生产环境

## 认证

管理用户

root

主机级别管理用户，如果没有设置则默认使用集群级别管理用户

## 组

资产组

× Default

您的ssh密钥没有设置或已失效, 请点击 [链接](#) 更新

资产列表

创建资产

每页 15 搜索 标签 导入 导出

|                          | 主机名        | IP             | 端口 | 集群      | 硬件                    | 激活中 | 可连接 | 动作                                    |
|--------------------------|------------|----------------|----|---------|-----------------------|-----|-----|---------------------------------------|
| <input type="checkbox"/> | CentOS 7.2 | 192.168.50.129 | 22 | Default | 1 Core 977.0 M 20.0 G | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |
| <input type="checkbox"/> | RedHat 6.5 | 192.168.50.138 | 22 | Default | 1 Core 980.0 M 20.0 G | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |
| <input type="checkbox"/> | Ubuntu 15  | 192.168.50.140 | 22 | Default | 1 Core 975.0 M 20.0 G | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |
| <input type="checkbox"/> | FreeBSD    | 192.168.50.142 | 22 | Default | 1 Core 973.0 M 0.0 K  | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |
| <input type="checkbox"/> | Fedora 23  | 192.168.50.139 | 22 | Default | 1 Core 976.0 M 20.0 G | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |
| <input type="checkbox"/> | Debian 8.2 | 192.168.50.141 | 22 | Default | 1 Core 228.0 M 20.0 G | ✓   | ●   | <a href="#">更新</a> <a href="#">删除</a> |

批量删除 提交

显示第 1 至 6 项结果, 总共 6 项

< 1 >

## 1.8 创建系统用户

系统用户是用来登录资产的，授权时需要

### 1.8.1. 创建系统用户

192.168.50.128/assets/system-user/

Jumpserver

仪表盘

用户管理

资产管理

资产

资产组

集群

管理用户

系统用户

标签管理

权限管理

仪表盘 / 资产管理 / 系统用户列表

您的ssh密钥没有设置或已失效, 请点击 [链接](#) 更新

系统用户是 用户登录资产(服务器)时使用的用户, 如 web, sa, dba等具有密码。

系统用户列表

创建系统用户

|  | 名称 | 用户名 |
|--|----|-----|
|--|----|-----|

### 1.8.2. 创建系统用户为Dev

|     |                          |
|-----|--------------------------|
| 名称  | dev                      |
|     | * required               |
| 用户名 | dev                      |
|     | * required               |
| 优先级 | 10                       |
|     | 高优先级的系统用户将会作为默认登录用户      |
| 协议  | ssh                      |
| 集群  | <div>× Default</div>     |
|     | 如果选择了自动推送，系统用户将会创建在集群资产上 |

认证

|        |                                     |
|--------|-------------------------------------|
| 自动生成密钥 | <input checked="" type="checkbox"/> |
| 自动推送   | <input checked="" type="checkbox"/> |

其它

|       |                |
|-------|----------------|
| Sudo  | /sbin/ifconfig |
| Shell | /bin/bash      |
| 备注    | 备注             |



1.8.3. 创建完成

dev 创建成功

系统用户是 用户登录资产(服务器)时使用的用户, 如 web, sa, dba等具有特殊功能的用户, 系统用户创建时, 如果选择了自动推送, Jumpserver会使用ansible自动推送到系统用户所在集群的资产中, 如果资产(交换机)不支持ansible, 请手动填写资产ID。

系统用户列表

创建系统用户

每页 15 搜索

| <input type="checkbox"/> | 名称  | 用户名 | 资产 | 可连接 | 不可达 | 比例 | 备注 | 动作                                    |
|--------------------------|-----|-----|----|-----|-----|----|----|---------------------------------------|
| <input type="checkbox"/> | dev | dev | 6  | 0   | 0   | 0% |    | <a href="#">更新</a> <a href="#">删除</a> |

显示第 1 至 1 项结果, 总共 1 项

< 1 >

公社  
linux  
www.linuxidc.com

1.9 创建授权规则

授权规则 关联用户，资产，系统用户 形成授权规则，授权的系统用户会自动推送到资产上

1.9.1. 创建授权规则

192.168.50.128/perms/asset-permission

Jumpserver

仪表盘

用户管理

资产管理

权限管理

资产授权

会话

作业中心

系统设置

仪表盘 / 权限管理 / 资产授权列表

您的ssh秘钥没有设置或已失效, 请点击 [链接](#) 更新

提前规划好集群中的系统用户, 授权时选择的资产(组内资产)必须存在该系

资产授权列表

创建授权规则

| <input type="checkbox"/> | 名称 | 用户 | 用 |
|--------------------------|----|----|---|
|--------------------------|----|----|---|

公社  
linux  
www.linuxidc.com

1.9.2. 创建授权规则jms\_Dev



## 创建资产权限

### 名称

名称 jms\_dev

\* required

### 用户

用户 × admin × jms

用户组 × Default

### 资产

资产 × CentOS 7.2 × RedHat 6.5 × Ubuntu 15 × FreeBSD × Fedora 23 × Debian 8.2

资产组 × Default

系统用户 × dev

\* required

### 其它

激活中 ☒

失效日期 2088-01-12



Copyright 北京堆栈科技有限公司 © 2014-2018

### 1.9.3. 完成创建授权规则

jms\_dev 创建成功

提前规划好集群中的系统用户，授权对选择的资产(组内资产)必须存在该系统用户，否则可能无法成功登录

资产授权列表

| 名称      | 用户 | 用户组 | 资产 | 资产组 | 系统用户 | 有效                                  | 动作                  |
|---------|----|-----|----|-----|------|-------------------------------------|---------------------|
| jms_dev | 2  | 1   | 6  | 1   | 1    | <input checked="" type="checkbox"/> | <button>删除</button> |

显示第 1 至 1 项结果, 总共 1 项

### 1.10 SSH连接终端

```
$ ssh -p2222 admin@192.168.244.144
```

密码: admin

如果是用在windows下，Xshell terminal登录语法如下

```
$ssh admin@192.168.244.144 2222
```

密码: admin

```
1 192.168.50.128 [0] × 2 192.168.50.128 [16] × +
Last login: Sun Jan 28 22:02:42 2018 from 192.168.50.1
[root@localhost ~]# source /opt/py3/bin/activate
(py3) [root@localhost ~]# cd /opt/coco/
(py3) [root@localhost coco]# python run_server.py
2018-01-28 22:06:47 [service DEBUG] Initial app service
2018-01-28 22:06:47 [service DEBUG] Load access key
2018-01-28 22:06:47 [service INFO] No access key found, register it
2018-01-28 22:06:47 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:50 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:53 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:56 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:06:59 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:02 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:05 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:08 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:11 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:14 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:17 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:20 [service INFO] "Terminal was not accepted yet"
2018-01-28 22:07:23 [service DEBUG] Set app service auth: 5b5f47cd-35cd-476a-ae93-b14b60e47c4a:9f176c01-ab2d-4429-bc3d-8f2171ad2b83
2018-01-28 22:07:23 [service DEBUG] Service http auth: <jms.auth.AccessKeyAuth object at 0x7fc247a74550>
2018-01-28 22:07:23 [app DEBUG] Loading config from server: {"COMMAND_STORAGE": {"TYPE":
```

```
仅将文本发送到当前选项卡
1 192.168.50.128 [0] × 2 192.168.50.128 [1] × 3 192.168.50.128:2222 × +
jumpserver, 欢迎使用Jumpserver开源跳板机系统

1) 输入 ID 直接登录 或 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 or 备注 搜索. 如: /ip
3) 输入 P/p 显示您有权限的主机.
4) 输入 G/g 显示您有权限的主机组.
5) 输入 G/g + 组ID 显示该组下主机. 如: g1
6) 输入 H/h 帮助.
0) 输入 Q/q 退出.

Opt> █
```

仅将文本发送到当前选项卡

## 1.11 WEB连接终端

administrator 先切换到用户界面

帮助

Administrator ▾

⚙️ 个人信息

⇄ 用户页面

🚪 注销登录

用户

Online

在线会话

Connected

ine user

0

Online sessions



www.linuxidc.com

Jumpserver

x

← → ↻ ⓘ 192.168.50.128/assets/user-asset/

Jumpserver



🏠 我的资产

👤 个人信息

🖥️ Web终端

仪表盘 / 资产管理 / 资产列表

您的ssh密钥没有设置或已失效, 请点击 [链接](#) 更新

资产列表

| <input type="checkbox"/> | 主机名 <small>↑↓</small> | IP <small>↑↓</small> | 端口 <small>↑↓</small> | 类型 <small>↑↓</small> |
|--------------------------|-----------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | CentOS 7.2            | 192.168.50.129       | 22                   | 物理机                  |
| <input type="checkbox"/> | RedHat 6.5            | 192.168.50.138       | 22                   | 物理机                  |
| <input type="checkbox"/> | Ubuntu 15             | 192.168.50.140       | 22                   | 物理机                  |
| <input type="checkbox"/> | FreeBSD               | 192.168.50.142       | 22                   | 物理机                  |
| <input type="checkbox"/> | Fedora 23             | 192.168.50.139       | 22                   | 物理机                  |
| <input type="checkbox"/> | Debian 8.2            | 192.168.50.141       | 22                   | 物理机                  |

官方网址: <https://github.com/jumpserver/jumpserver>

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com)网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

**Linux公社** 主站网址：[www.linuxidc.com](http://www.linuxidc.com)

**Linux公社资源站**网址：[linux.linuxidc.com](http://linux.linuxidc.com)

**Linux公社手机站**网址：[m.linuxidc.com](http://m.linuxidc.com)

旗下网站：[www.linuxidc.net](http://www.linuxidc.net)

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#)  
[RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)



Linux 公社微信公众号：[linuxidc\\_com](#)



微信扫一扫

[Linuxidc.com](http://Linuxidc.com)

订阅专业的最新Linux资讯及开源技术教程。

搜索微信公众号：[linuxidc\\_com](#)