

第1章 jumpserver介绍

1.什么是堡垒机/跳板机

- 1 堡垒机就是统一设备运维入口口，支持管理Linux、Windows、Unix、MacOS等设备资源，实现对服务器资源操作管理的集中认证，集中控制，集中审计。提升运维管理水平。

2.为什么要用堡垒机/跳板机

- 1 现在互联网企业，往往都拥有大量量服务器器，如何安全并高效的管理这些服务器是每个系统运维或安全运维人员必要工作。
- 2 现在比较常见的方案是搭建堡垒机环境作为线上服务器的入口口，所有服务器只能通过堡垒机进行行行登陆访问。
- 3 说句句大大白话：就是监控运维人员、开发人员对服务器的命令操作。出了事故能找到具体责任人。

3.跳板机的特性

- 1.精细化的资源与功能授权，让运维人员各司其职。
- 2.体系化的指令审计规则，让运维操作安全可控。
- 3.支持多重身份认证，让非法访问无所遁形。
- 4.主机账号统一管理，SSH密钥对一键批量下发。

第2章 jumpserver安装

1.方法1 docker安装

- 1 docker pull docker.io/jumpserver/jms_all
- 2 docker run --name Jumpserver -d -p 80:80 -p 2222:2222 docker.io/jumpserver/jms_all:latest

进入容器修改配置

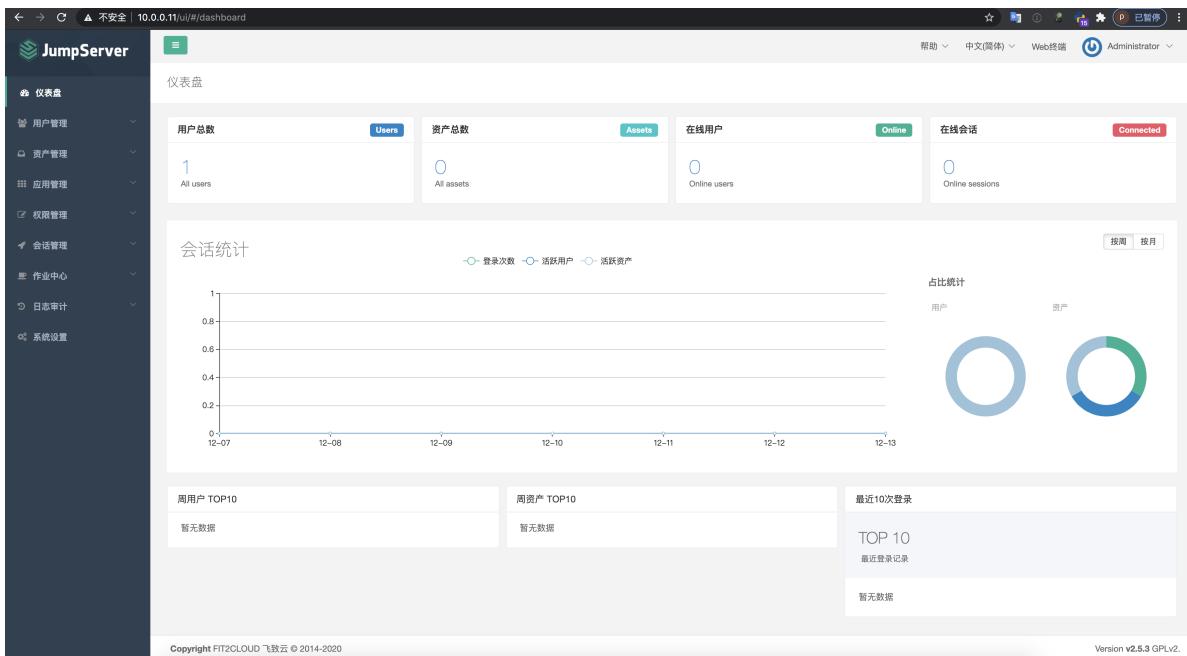
- 1 docker exec -it Jumpserver /bin/bash
- 2 docker restart Jumpserver

2.方法2 官网脚本安装

- 1 curl -SSL https://github.com/jumpserver/jumpserver/releases/download/v2.5.3/quick_start.sh | sh

第3章 jumpserver应用

1.启动访问



2. 配置邮箱

The screenshot shows the '邮件设置' (Email Settings) page under '系统设置' (System Settings). The '基本信息' (Basic Information) section includes:

- SMTP主机 (SMTP Host): smtp.qq.com
- SMTP端口 (SMTP Port): 465
- SMTP账号 (SMTP Account): 526195417@qq.com
- SMTP密码 (SMTP Password): **QQ邮箱的授权码** (Authorization code for QQ Mailbox)
- 发送账号 (Send Account): 526195417@qq.com
- 测试收件人 (Test Recipient): 526195417@qq.com
- 使用SSL (Use SSL):
- 使用TLS (Use TLS):

底部有 测试连接 (Test Connection), 重置 (Reset) 和 提交 (Submit) 按钮。

3. 创建用户组

The screenshot shows the '创建用户组' (Create User Group) page under '用户管理' (User Management). The '基本' (Basic) section includes:

- 名称 (Name): 运维组
- 用户 (User): 请选择 (Select User)
- 备注 (Remarks): 运维账户

底部有 保存并继续添加 (Save and Add Another) 和 提交 (Submit) 按钮。

JumpServer					
用户组					
操作		名称	用户	备注	操作
<input type="checkbox"/>	开发组	0	开发账户		<button>更新</button> <button>更多</button>
<input type="checkbox"/>	测试组	0	测试账户		<button>更新</button> <button>更多</button>
<input type="checkbox"/>	运维组	0	运维账户		<button>更新</button> <button>更多</button>

4. 创建用户

账户					
* 名称	<input type="text" value="张亚"/>				
* 用户名	<input type="text" value="zhangya"/>				
* 邮件	<input type="text" value="526195417@qq.com"/>				
用户组	<input type="text" value="运维组"/>				
认证					
密码策略	<input checked="" type="radio"/> 生成重置密码链接，通过邮件发送给用户	<input type="radio"/> 设置密码			
多因子认证	<input checked="" type="radio"/> 禁用	<input type="radio"/> 启用	<input type="radio"/> 强制启用		
用户来源	<input type="text" value="数据库"/>				
安全					
系统角色	<input checked="" type="radio"/> 系统管理员	<input type="radio"/> 系统审计员			
失效日期	<input type="text" value="2120-11-20 06:44:34"/>				
其它					
手机	<input type="text" value="15321312624"/>				
微信	<input type="text" value="jijiaozhangya"/>				
备注	<input type="text" value="运维老大"/>				
	<button>保存并继续添加</button>	<button>提交</button>			

用户列表					
操作		用户名	用户组名	角色	用户来源
<input type="checkbox"/>	<input type="checkbox"/>	Administrator		系统管理员 组织管理员	数据库 <input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	zhangya	运维组	系统管理员 组织管理员	数据库 <input checked="" type="checkbox"/>

密码会通过邮件发送到邮箱里

创建账户成功☆

发件人: 张亚 <526195417@qq.com> 
时 间: 2020年12月14日 (星期一) 上午6:46
收件人: 张亚 <526195417@qq.com>

您好 张亚:

您的账户已创建成功

用户名: zhangya

密码: [请点击这里设置密码](#) (这个链接有效期1小时, 超过时间您可以[重新申请](#))

[直接登录](#)



欢迎使用JumpServer开源堡垒机

全球首款完全开源的堡垒机，使用GNU GPL v2.0开源协议，是符合 4A 的专业运维审计系统。

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。

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、无并发访问限制。

改变世界，从一点点开始。

登录

zhangya

.....

登录

忘记密码?

首次登录

完善个人信息

账户

用户名: zhangya
名称: 张亚
邮件: 526195417@qq.com

认证

多因子认证: 禁用 启用
启用多因子认证，使账号更加安全。启用之后您将在下次登录时进入多因子认证绑定流程；您也可以在「个人信息->快速修改-更改多因子设置」中直接绑定。

其它

手机: 15321312624
微信: jiujiao_zhangya

条款和条件

* 我同意

为了保护您和公司的安全，请妥善保管您的账户、密码和密钥等重要敏感信息：(如：设置复杂密码，并启用多因子认证)

重置 提交

4.资产管理

The screenshot shows the JumpServer web interface at the URL 10.0.0.11/ui/#/assets/assets. The left sidebar is titled '资产管理' (Asset Management) and includes sections for Asset List, Network List, User Management, Application Management, and more. The 'Asset List' section is currently selected. On the right, there is a tree view under 'Default (0)' with options like 'Create Node', 'Rename Node', 'Delete Node', 'Add Asset to Node', 'Move Asset to Node', 'Update Asset Node Hardware Information', 'Test Asset Node Connectivity', 'Show Only Current Node Assets', 'Show All Sub-node Assets', and 'Show Node Details'. Below the tree view is a table with columns for '主机名' (Host Name), 'IP', '硬件信息' (Hardware Information), '可连接' (Connectable), and '操作' (Operations). The table displays '暂无数据' (No data available) and has a page size of 15 items per page.

5. 用户管理

1 | 注意：

- 2 1. 创建管理用用户使用用root用户名
- 3 2. 创建系统用用户：运维组,开发组,总监组各创建一个
- 4 3. 只有运维组的系统用用户的sudo权限是/bin/su,其他组的系统用用户使用用默认

创建管理用户

创建管理用户

基本

- 名称: 超级管理员
- 用户名: root
- 密码: *****
- SSH密钥: [选择文件] 未选择任何文件

其它

- 备注:

保存并继续添加 **提交**

创建系统用户

基本

- 名称: 运维
- 登录模式: 自动登录 手动登录
- 用户名: ops
- 用户名与用户相同:
- 优先级: 20
- 协议: ssh

自动推送

- 自动推送:
- Sudo: /bin/su 允许使用的 sudo 命令
- Shell: /bin/bash

系统用户

系统用户是JumpServer 跳转登录资产时使用的用户，可以理解为登录资产用户，如 web, sa, dba ('ssh web@some-host')，而不是使用某个用户的用户名登录服务器 ('ssh xiaoming@some-host')；简单来说是用户使用自己的用户名登录 JumpServer，JumpServer 使用系统用户登录资产。系统用户创建时，如果选择了自动推送，JumpServer 会使用 Ansible 自动推送系统用户到资产中，如果资产（交换机）不支持 Ansible，请手动填写账号密码。

创建	搜索	导出	刷新			
名称	用户名	协议	登录模式	资产	备注	动作
开发	dev	ssh	自动登录	0		更新 删除
测试	qa	ssh	自动登录	0		更新 删除
运维	ops	ssh	自动登录	0		更新 删除

共 3 条 15条/页 < 1 >

6.资产管理

创建资产

The screenshot shows the 'Create Asset' form in the JumpServer web interface. The left sidebar shows the navigation menu. The main form has several sections:

- 基本**: Fields for Host Name (web01), IP (172.16.1.12), and System Platform (Linux). The IP field is highlighted with a red box.
- 协议组**: A protocol group named 'ssh' on port 22.
- 认证**: Authentication method set to '超级管理员(root)'.
- 节点**: Node path set to '/Default/web前端'.
- 标签**: Tag management dropdown.
- 其它**: An '激活' (Activation) toggle switch, which is highlighted with a red box.

The screenshot shows the 'Asset List' interface in the JumpServer web interface. The left sidebar shows the navigation menu. The main area displays a hierarchical asset tree on the left and a detailed table on the right:

主机名	IP	硬件信息	可连接	操作
db01	172.16.1.13	1 Core 1.98 G 40.0 G	✓	[更新] [更多]
web01	172.16.1.12	1 Core 1.98 G 40.0 G	✓	[更新] [更多]

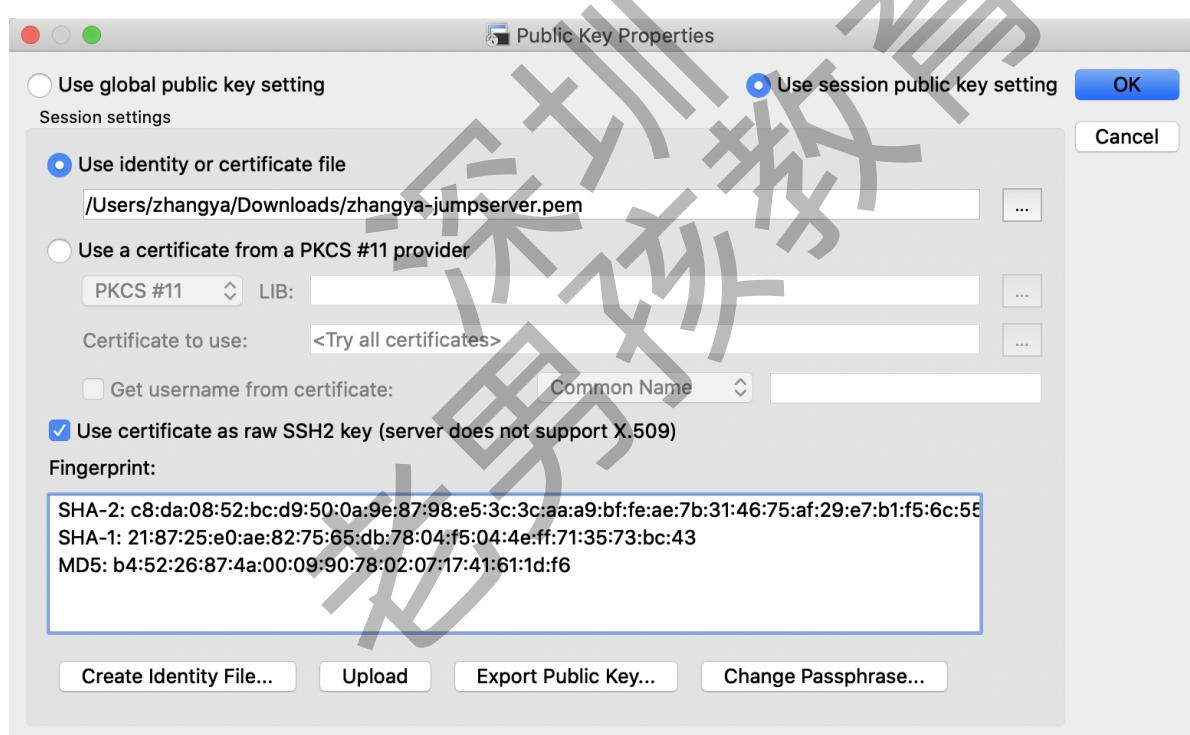
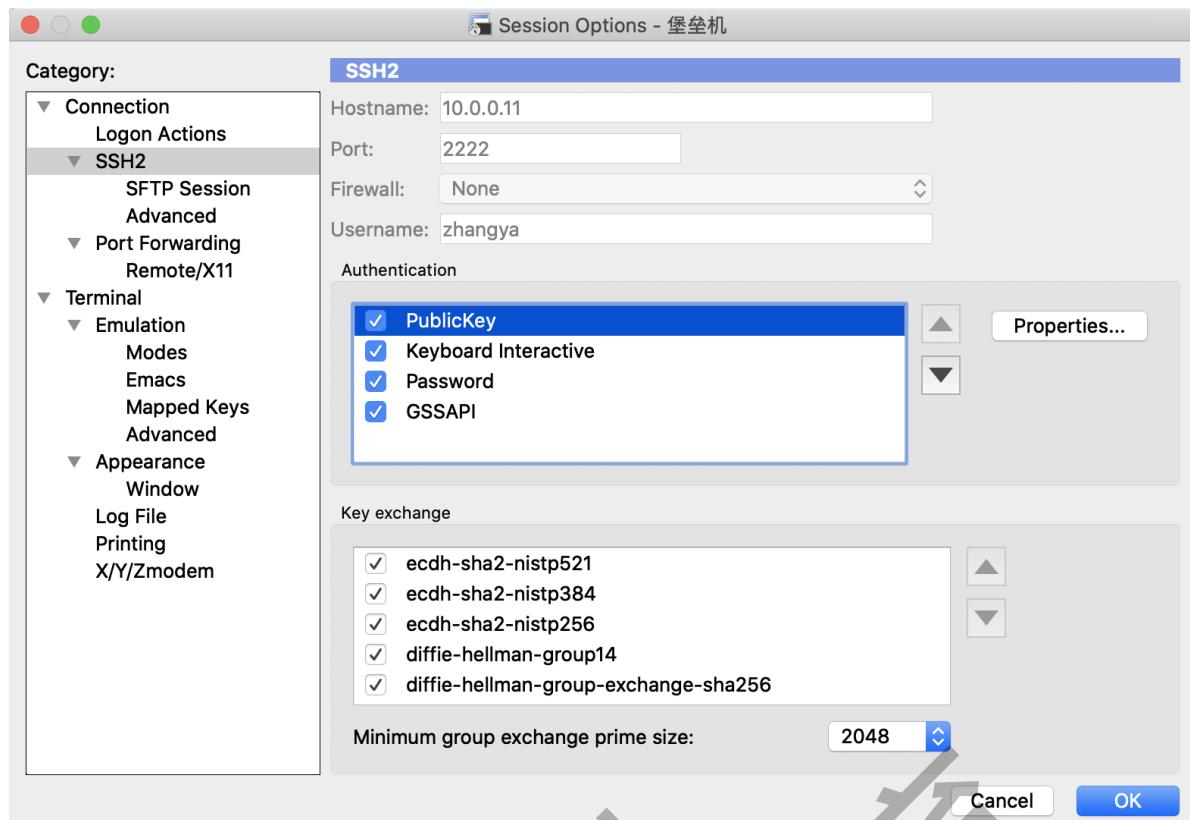
Text above the table: 左侧是资产树，右击可以新建、删除、更改树节点，授权资产也是以节点方式组织的，右侧是属于该节点下的资产。

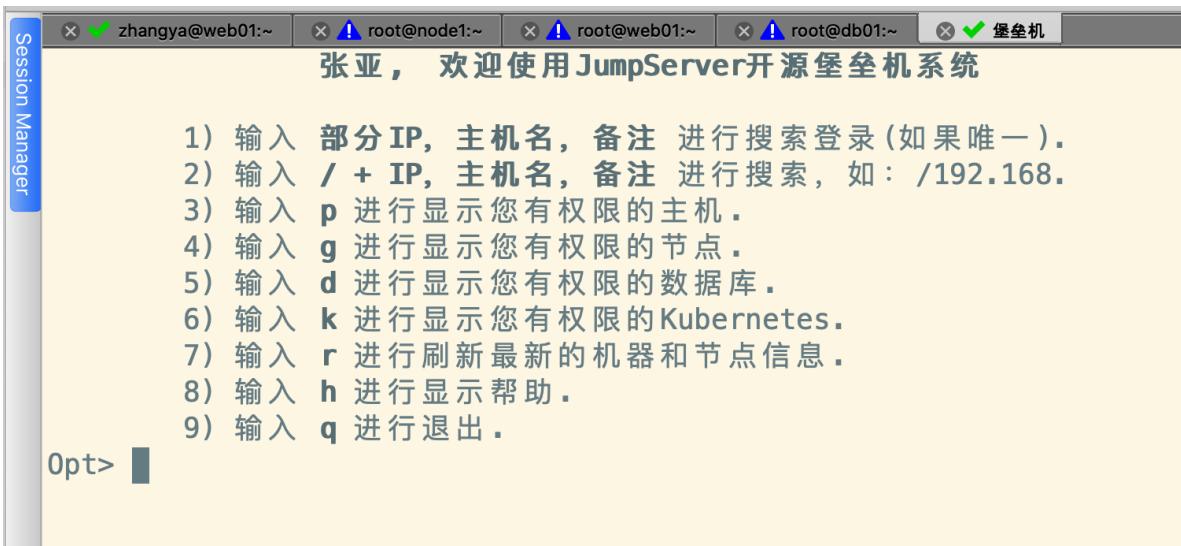
7.权限管理

创建授权规则

8.配置终端登陆

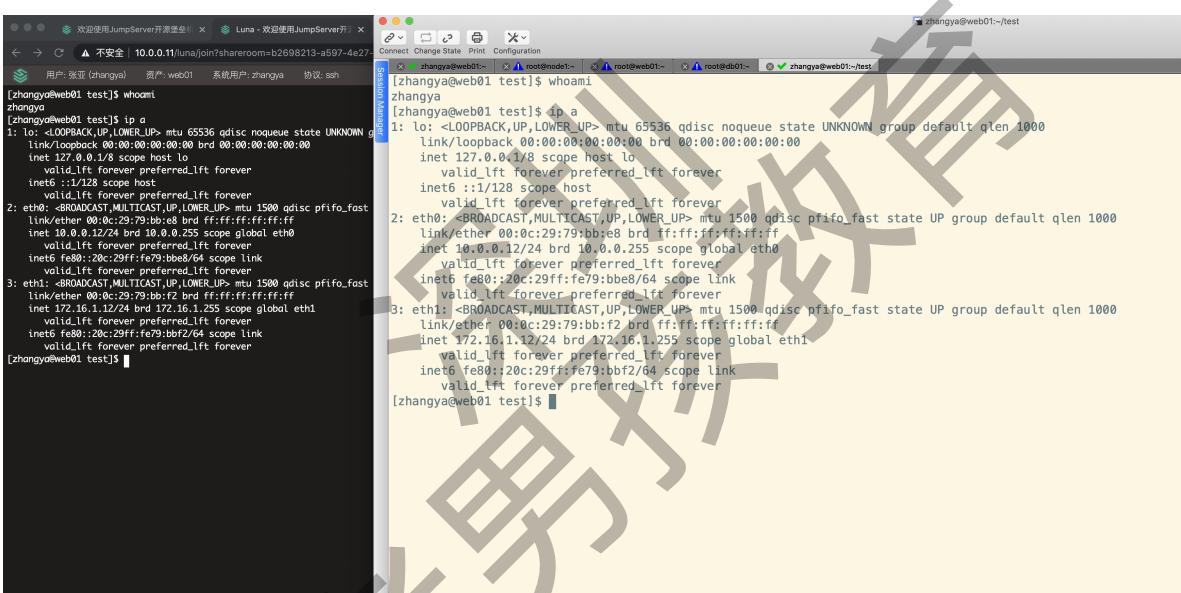
ssh-rsa
AAAAE3NzaC1IwzEAAAQABAAQABQD9RAc5BpdFOodRhmRF3GFh0HmgHE/EOlOTbjdYHR+yJgS8RtBDuh7Gw8xfoH15KKpl0DrWDYjzG5um0zInK1TGxOmoMUp9905Sm1t0BCelubm6GjrsG14KPTGH2hPFSSjn+B/h76BZx0HNJM+f39jD1/bbe64MuJGrul2Qbx4oOGmTbKTqhrO3JRvynZwtJA-51ZFDg02NbPm2wSiSKBiKdjURG2+20)U+4zTPMFnogIV0aUxwRaXaBKcCTc9vP2fk/lu3lnFF03rMpqInO0yyKKl/ONWtzeCU/mf0f1a+q9sg9iwWWSQmQ+dKkYQbf0heqilHP9LCTre5 root@im01





9.会话管理

- 1 | 会话管理可以看到当前有哪些正在连接的会话并且可以实时的同步监控会话内容，也可以随时断开会话



10.命令记录

- 1 | 历史会话里里面面记录了了哪个用用户在什么时间用用什么系统用用户登录了了哪台主机，执行行行了多少条命令，以及操作的视频都记录了了下来。
2 | 这样操作人人员操作了了什么，事后都能清清楚楚的知道。
3 | 也可以说，谁想对系统做破坏，都有证据找到责任人。

JumpServer

命令记录

命令	风险等级	用户	资产	系统用户	会话	日期
ls	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:35:18
rm -rf /opt/*	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:35:17
touch /opt/123.txt	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:34:48
ll /opt/	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:34:39
shutdown	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:34:30
touch 123.txt	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:34:19
cd test/	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:34:00
mkfile test	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:33:59
ip a	普通	张亚 (zhangya)	web01	zhangya	转到	2020/12/14 07:29:15
whoami	普通	张亚 (zhangya)	db01	zhangya	转到	2020/12/14 07:21:46
ip a	普通	张亚 (zhangya)	db01	zhangya	转到	2020/12/14 07:19:55
su - root	普通	张亚 (zhangya)	db01	zhangya	转到	2020/12/14 07:19:32

共 12 条 15条/页 1 / 1

老男孩教育