

# 云匣子快速入门手册

## 数据融合与安全专家

深圳云安宝科技有限公司

文档版本：V3.2.8.0

2018年12月27日

# 目录

---

1. 信息完善与帐号创建.....	3
1.1. 完善管理员信息.....	3
1.2. 创建堡垒机用户帐号.....	4
2. 资源录入.....	5
2.1. 添加主机.....	5
2.2. 添加资源主机帐号.....	9
2.2.1. 手动登录帐号.....	9
2.2.2. 自动登录帐号.....	10
2.2.3. 提权登录.....	11
3. 授权.....	11
3.1. 访问策略.....	11

## 前言

云匣子\_堡垒机是租户连接云资源的安全管理工具，帮助云租户更加安全、精细的管理云上的虚拟机、数据库等资源。

# 1. 信息完善与帐号创建

## 1.1. 完善管理员信息

首次以 admin 帐号登录，在页面右上角，点击帐号右边的下拉按钮，进入 [个人中心/编辑]，显示当前个人帐号信息，在页面中可以编辑，如图 1-1-1、1-1-2 所示。

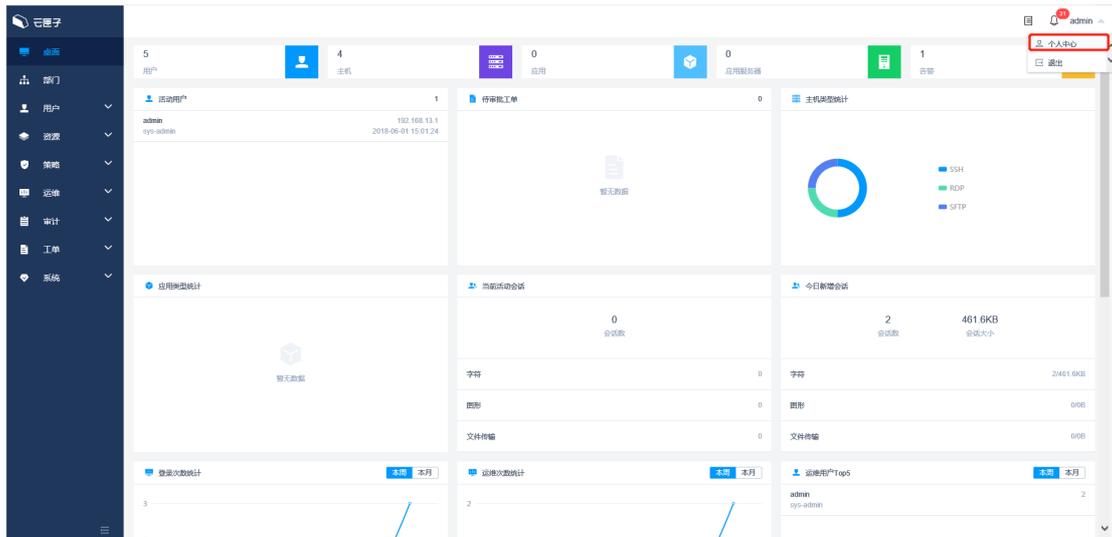


图 1-1-1

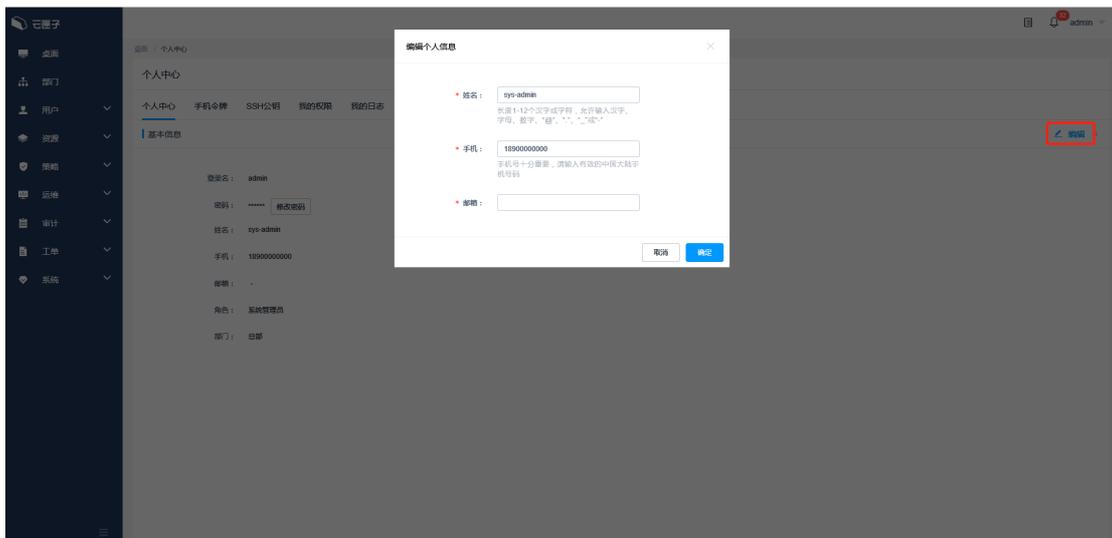


图 1-1-2

## 1.2. 创建堡垒机用户帐号

进入到[用户/用户管理]菜单栏，点击页面右边的“新建”，其中“\*”标记的红色部分为必填项，登录名、密码、姓名、手机、邮箱、请参考页面上提示信息填写，角色和部门以及认证类型根据实际情况进行选择。如图 1-2-1 所示。

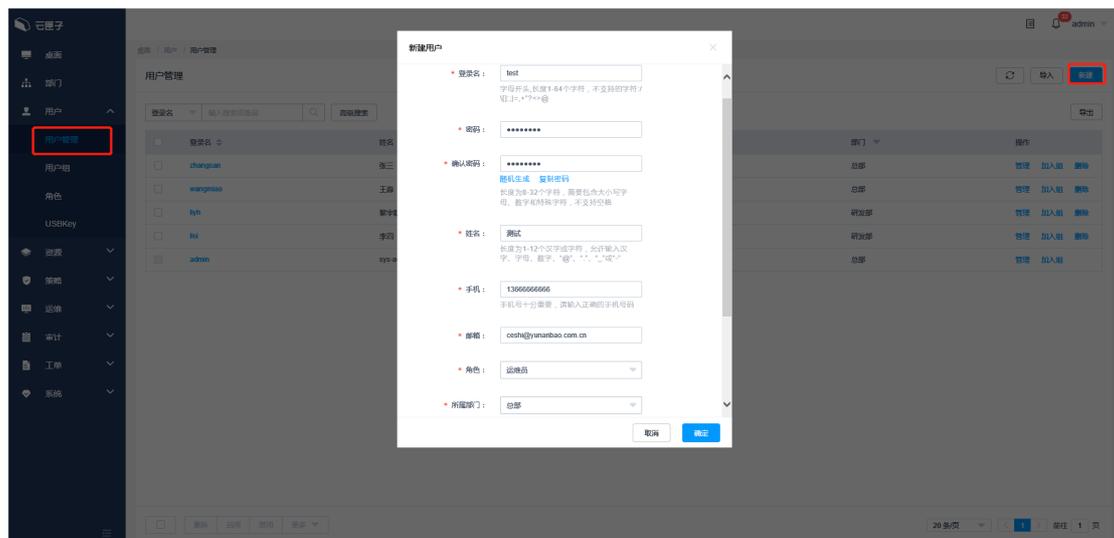


图 1-2- 1

## 2. 资源录入

### 2.1. 添加主机

进入到[资源/主机管理]菜单栏，录入主机信息分为单个录入与批量添加，批量添加又存在 2 种方法：一种为本地表格模版导入，另一种从云平台导入（适用于云主机）。

单台主机录入，点击页面右边的“新建”如图 2-1-1 所示。

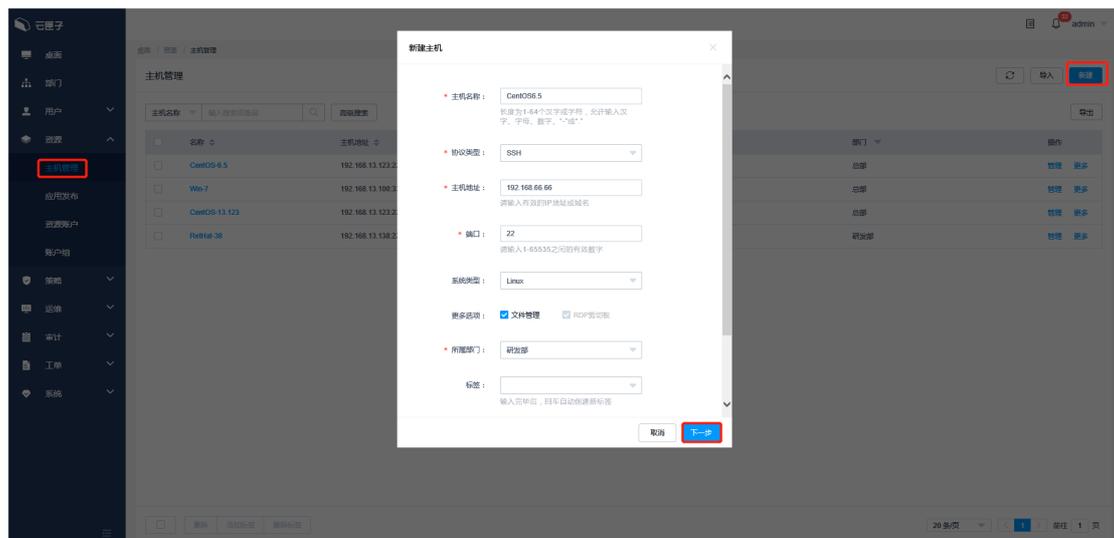


图 2-1-1

单台录入设备时, 会提示, 是否需要立即添加该资源主机上的系统帐号。如图 2-1-2 所示, 如若需要添加, 按照提示填写即可, 否则选择“以后添加”

### 新建主机 ×

添加账户： 立即添加  以后添加

\* 登录方式：

\* 主机账户：  
 特权账户

\* 密码：

SSH Key：  
填写之后将优先通过SSH Key登录

passphrase：

账户描述：  
描述最长128个汉字或字符

图 2-1-2

本地模版导入则点击页面右边的“导入”，提示需要下载模版，点击下载，模版如图 2-1-3-1、2-1-3-2 所示

名称 (IP地址/域名)	协议类型	端口	系统类型	所属部门 (标签)	主机描述	主机账户	登录方式 (自动登录)	特权账户 (密码)	SSH Key (SSPassphrase)	切换自 (输入/切换命令)	账户描述 (描述)
主机1 1.1.1.1	SSH	22	Cisco	总部, 部门1		root	自动登录	是	password		

图 2-1-3-1

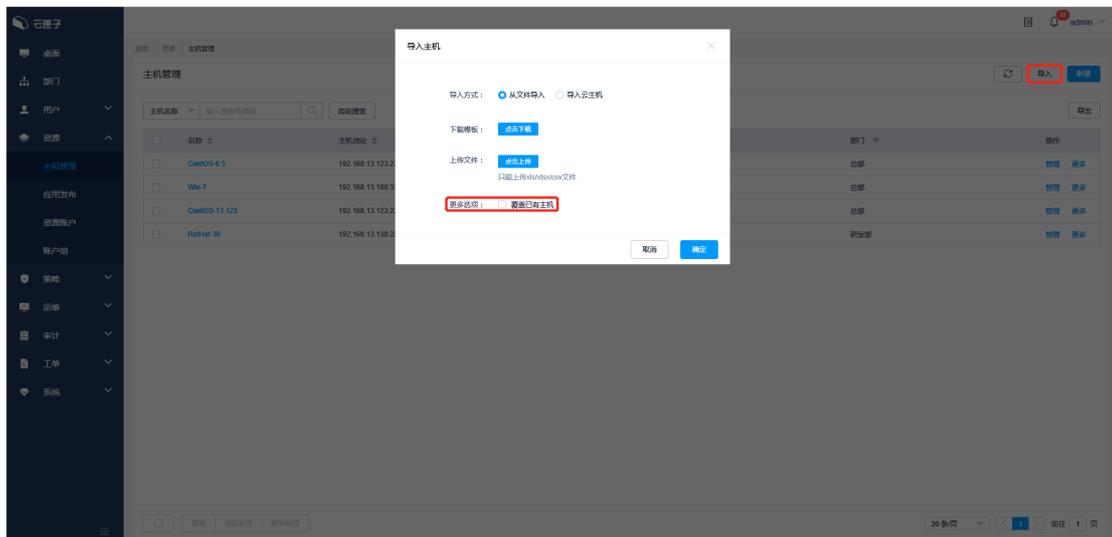


图 2-1-3-2

直接从云上导入主机，如图 2-1-4 所示。

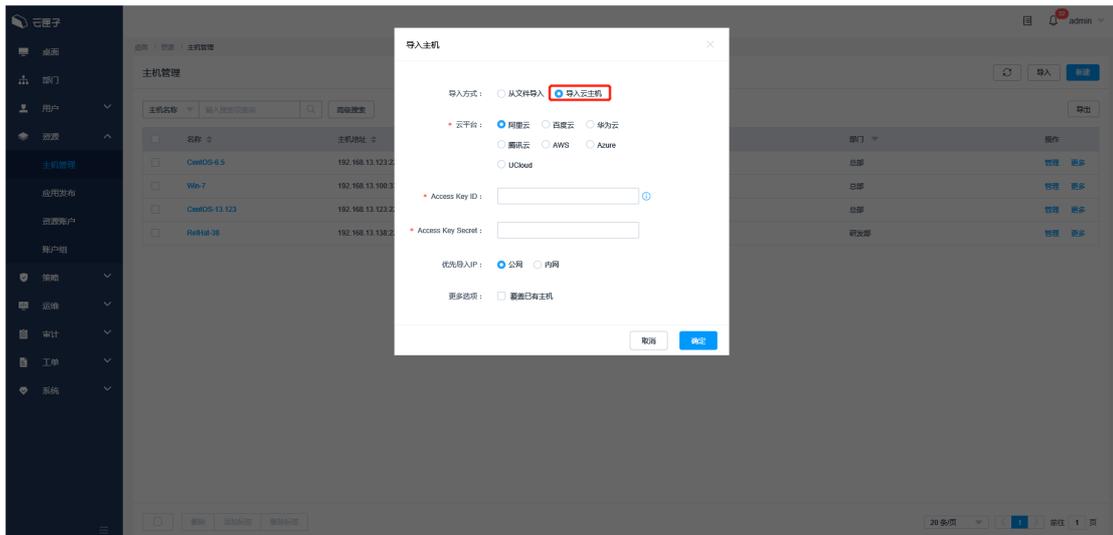


图 2-1-4

## 2.2. 添加资源主机帐号

### 2.2.1. 手动登录帐号

进入到[资源/资源帐号]菜单，点击页面右边的“新建”，出现编辑框，拉选登录方式为“手动登录”，关联相关的资源主机即可。需要注意的是，此时，资源账户这一栏并不是必填项，如果不填，添加的帐号为“Empty”，即手动登录，访问资源时需要手动输入账户名和密码。如果填写了资源帐号，添加的帐号为填写的帐号，访问资源时需要输入对应系统帐号的密码。

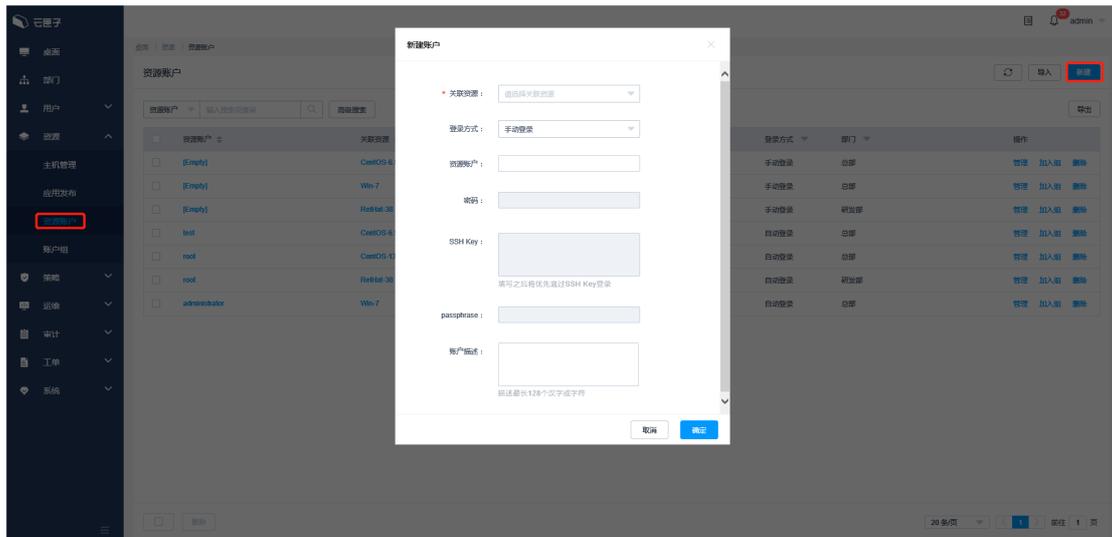


图 2-2-1

### 2.2.2. 自动登录帐号

自动登录帐号，其实就是已经把密码托管给了堡垒机的资源主机系统帐号，因此在访问资源主机时，堡垒机会将管理员托管进去的密码自动发给对应的资源主机，以实现无需人工手动输入密码的过程。

选择登录方式为“自动登录”，关联对应的资源主机，填写需要托管密码的系统帐号，然后将该帐号的密码托管给堡垒机，如图 2-2-2 所示。

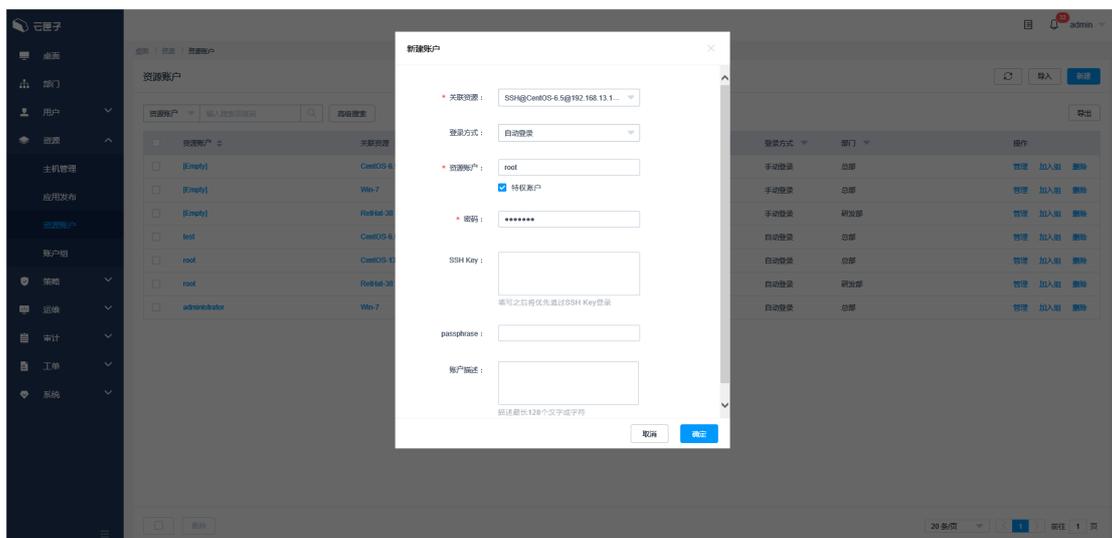


图 2-2-2

### 2.2.3. 提权登录

提权登录的概念为，当一个普通用户登录到目标资源主机上时，进行一次身份切换，登录到特权帐号。选择该方式时，需要先填写特权帐号密码，然后选取做切换的普通帐号。如图 2-2-3 所示。

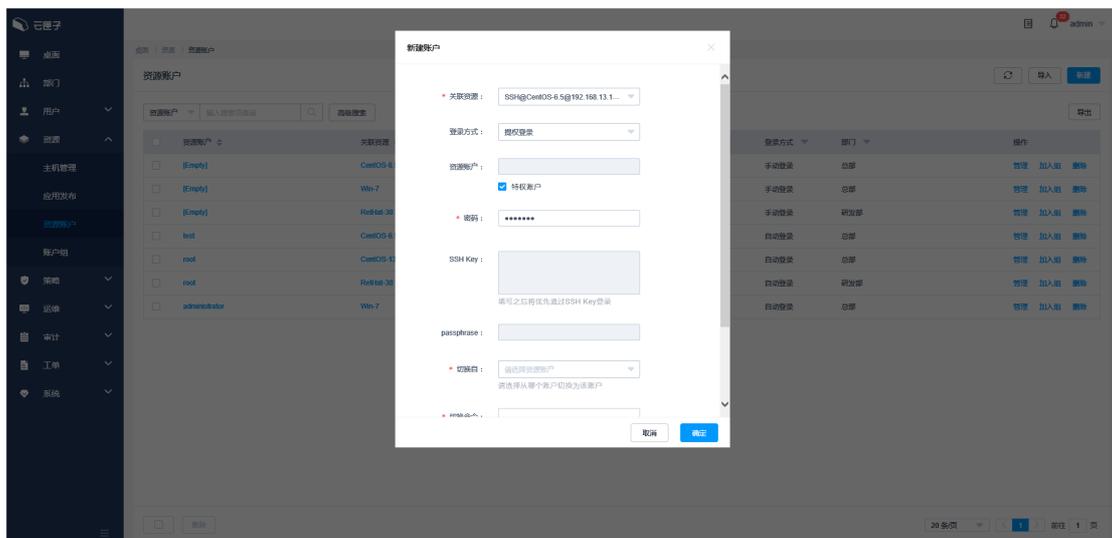


图 2-2-3

## 3. 授权

### 3.1. 访问策略

在创建完堡垒机用户以及将服务器资源信息纳入堡垒机之后，需要创建一条策略将对应的堡垒机用户与对应的资源主机进行关联起来。进入[策略/访问控制策略]，如图 3-1-1 所示，可以查看备份记录列表。

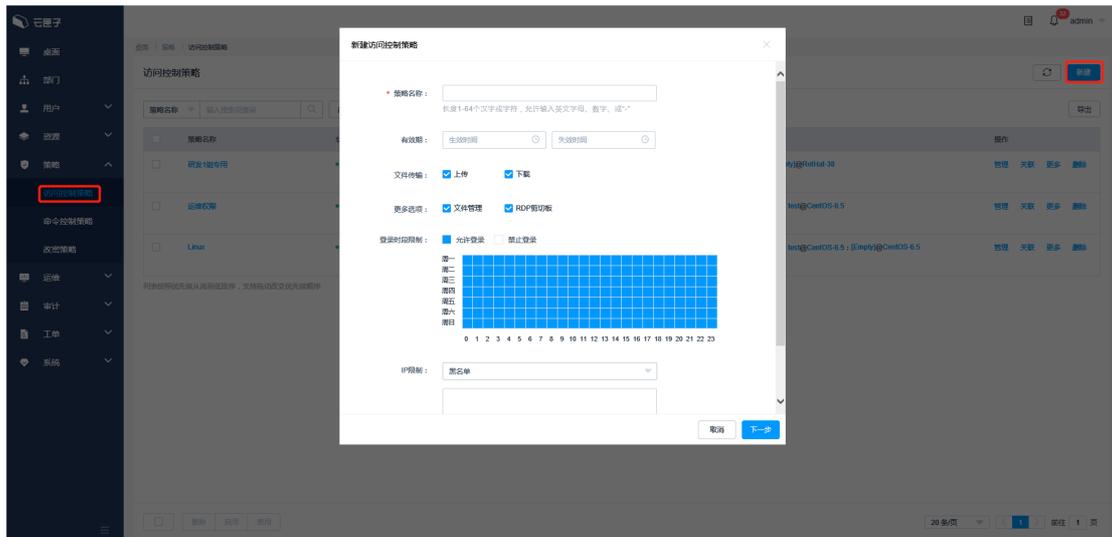


图 3-1-1

编辑创建[访问策略]对话框，先输入一个名称，然后可以设置该访问策略的有效期与生效时间，有效期不设置时为一直生效。限制文件的上传、下载以及文件管理、RDP 剪切板等功能，然后点击下一步，去关联对应的堡垒机用户和相关的资源主机与账户，支持直接关联组。如图 3-1-2-1 和 3-1-2-2 所示。



图 3-1- 2-1



图 3-1- 2-2

此时我们使用 test 帐号去登录堡垒机，可以看到，刚才我们配置的策略已经生效，如图 3-1-3，

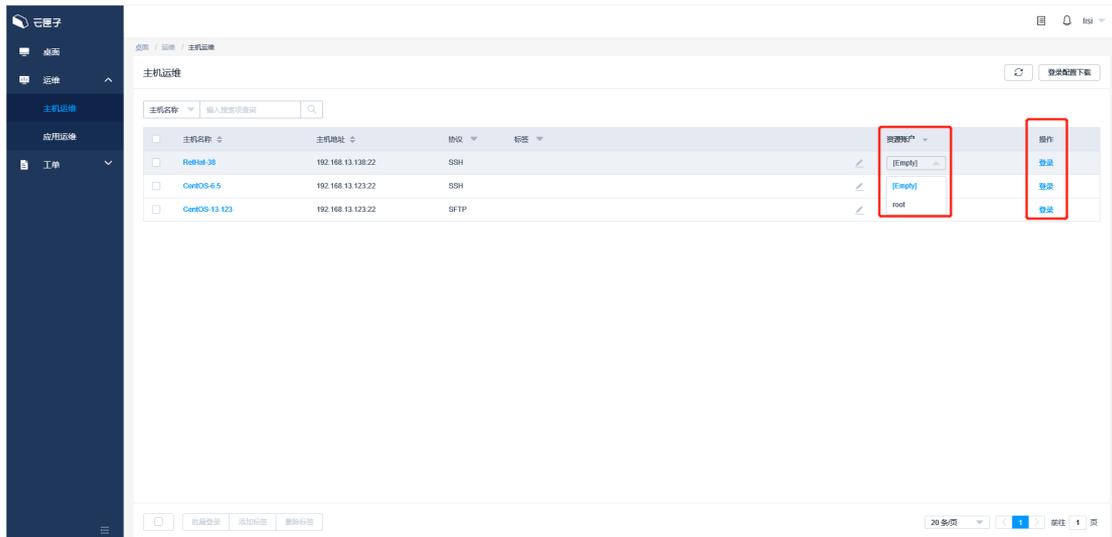


图 3-1-3

登录效果，如图 3-1-4



图 3-1-4

以上为堡垒机基础使用所需要满足的条件，简单来说分为 4 点：

- 1.堡垒机用户
- 2.资源主机
- 3.资源主机的系统帐号
- 4.访问策略

---

核心思路：通过访问策略控制指定的堡垒机用户能够在什么时候使用指定的系统帐号访问指定的资源主机。

更多配置相关，请参考《用户手册》。