

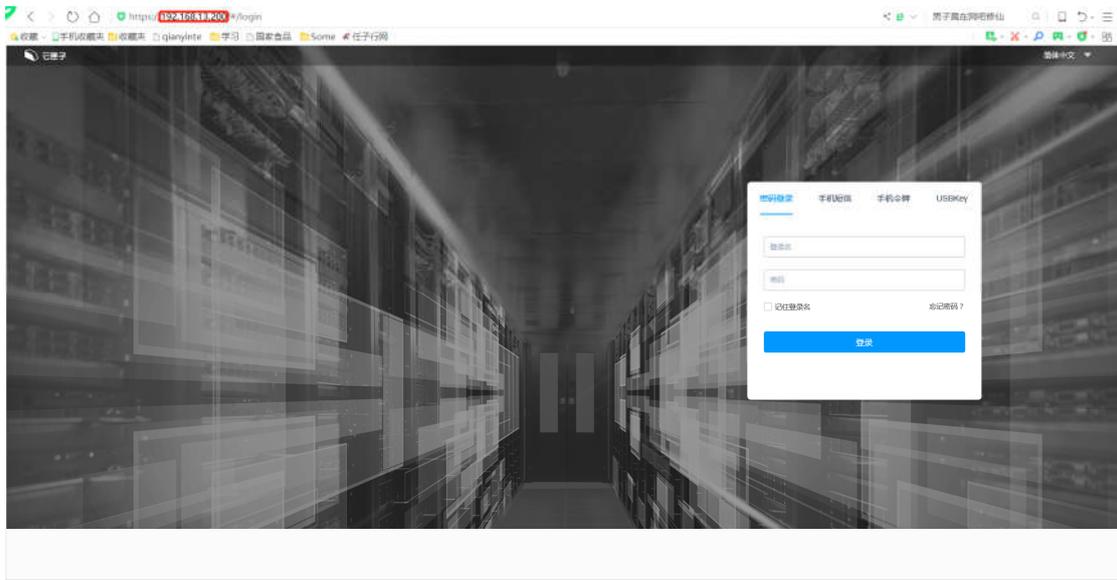
云安宝云匣子 运维员操作手册

云涌起 安有宝

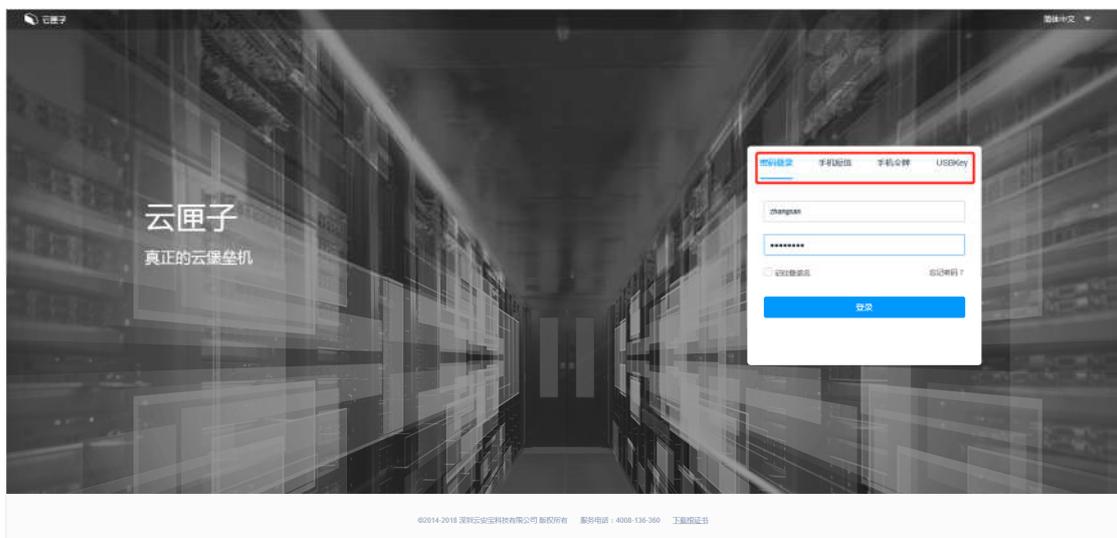
登录堡垒机

访问方式：

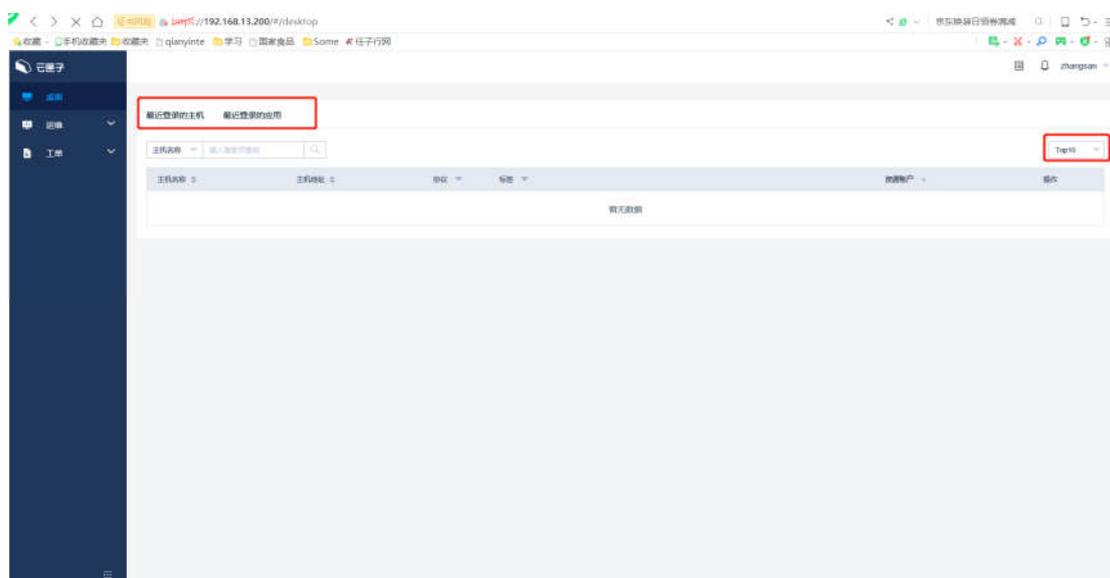
打开浏览器，在地址栏输入 ip 地址即可，如果能够访问，会进行自用的协议跳转。



用户根据自己的认证方式选择相应的认证类型，例如此处为静态密码

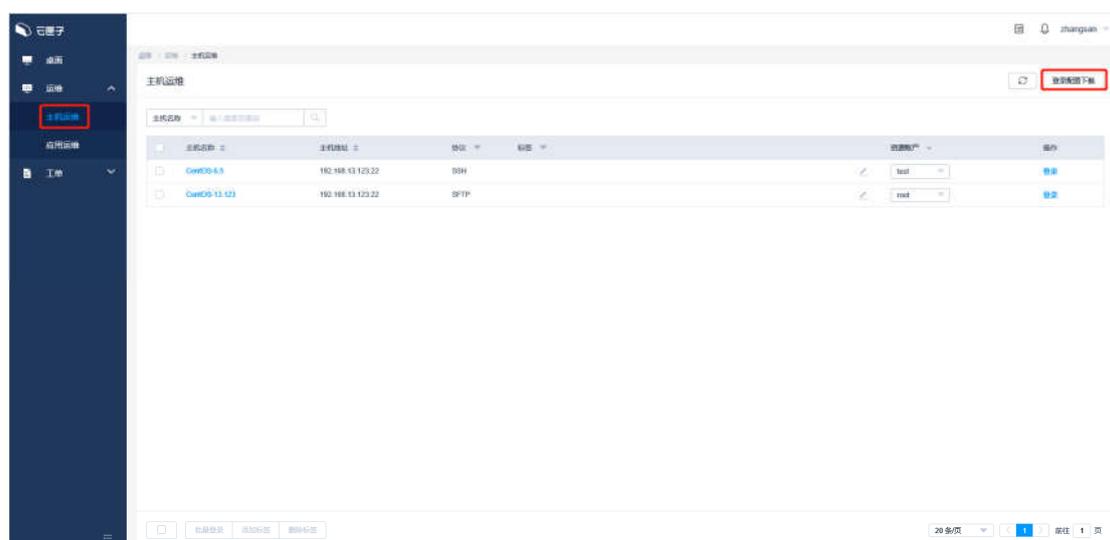


登录之后，页面会跳转到“桌面”，在这里可以看到“最近登录的主机”，“最近登录的应用”，右边还支持对登录次数最多的机器做排序。



运维

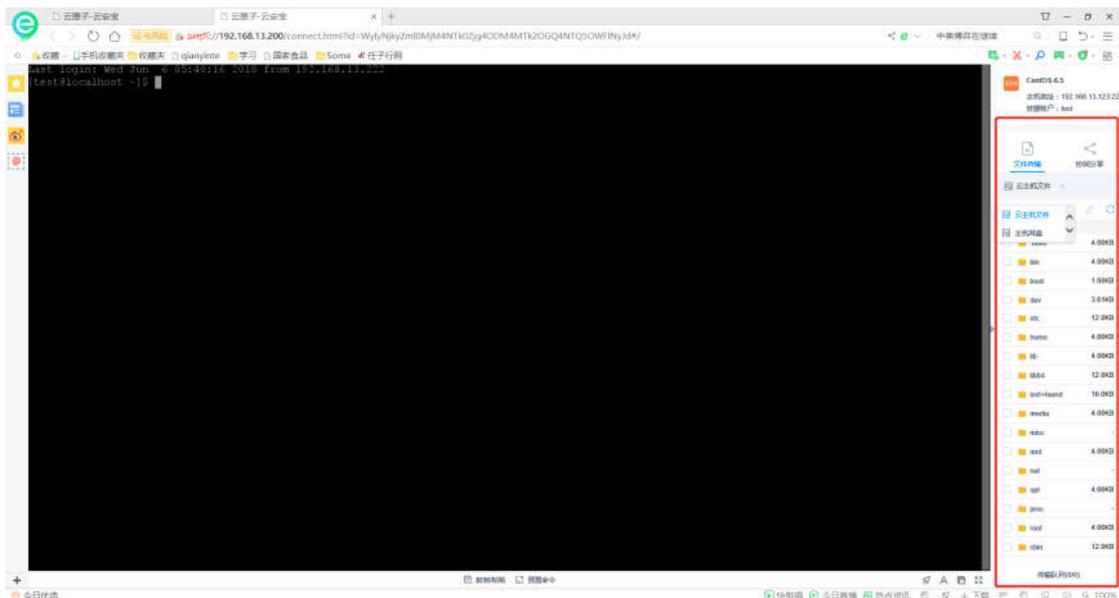
在左侧的菜单中，“运维”中可以看到，堡垒机管理员给定义该堡垒机运维员能访问的机器与应用。



对于字符类设备，支持通过第三方工具直接登录，例如 X-shell、SecureCRT。

堡垒机支持直接将能访问的字符类设备做一个 session，点击右上角“登录配置下载”即可下载到本地，双击即可打开，如果做了密码托管的设备，则直接就能访问过去。

通过 Web 页面直接访问，以此处的 Linux 设备为例。



登录上去之后，可以看到左边的界面和远程 ssh 目标服务器一模一样，右边可以看到两个功能选项，分别是“文件传输”、“协同分享”

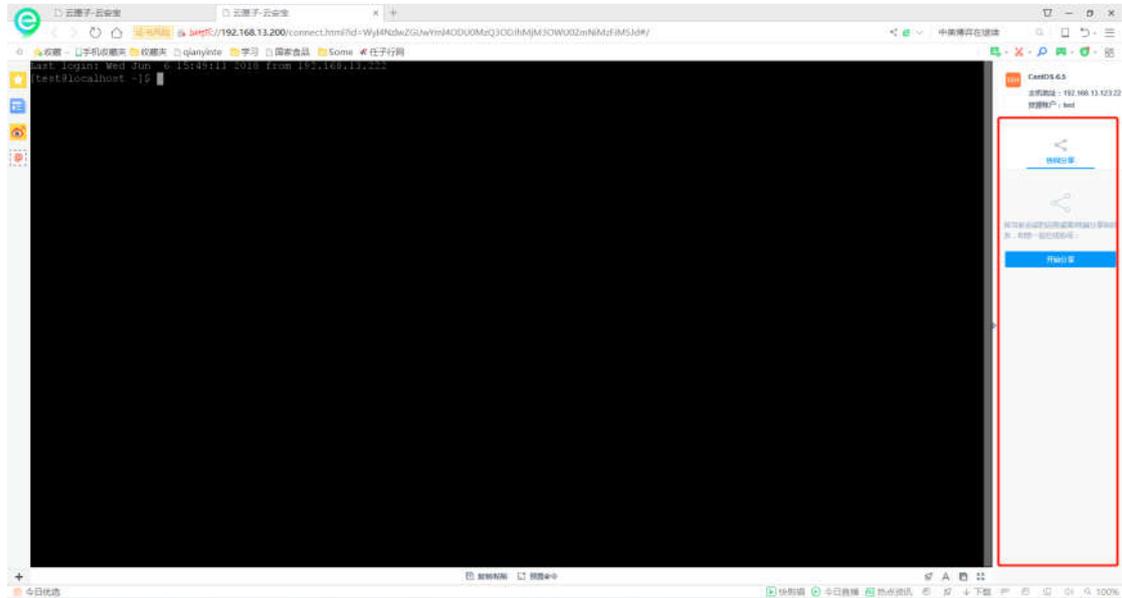
文件传输：云匣子特色功能之一，每个堡垒机用户在堡垒机上都有自己的个人网盘空间。

所有堡垒机用户，访问策略中给允许了“文件管理”权限，就能够在本地客户端、堡垒机、目标服务器之间进行文件传输。

如果某用户的访问策略中给了“文件管理”权限，但是没有给“上传、下载”权限，那么实际上能看得到，下载东西会提示能够开始，但是

内容是空白，或者是下载任务会一直持续（实际上做了控制，是无法进行上传下载的）。

而如果没有给予“文件管理”权限，则如图。



协同分享：实现多人共同访问一个会话。

在实际场景中，有时候工作上遇到一些问题可能需要同事的帮助，一些不是很重要的事情也可能需要跑一趟，云匣子的会话协同分享可以实现两个人对于会话的共同分享，远程协作，工作流程与 QQ 远程差不多。唯一的区别在于发起人点击“开始分享”后，会出现一个带有链接的对话框，将链接发给协同者，协同者将链接输入到浏览器中，即可加入会话。

来张效果图看一下：

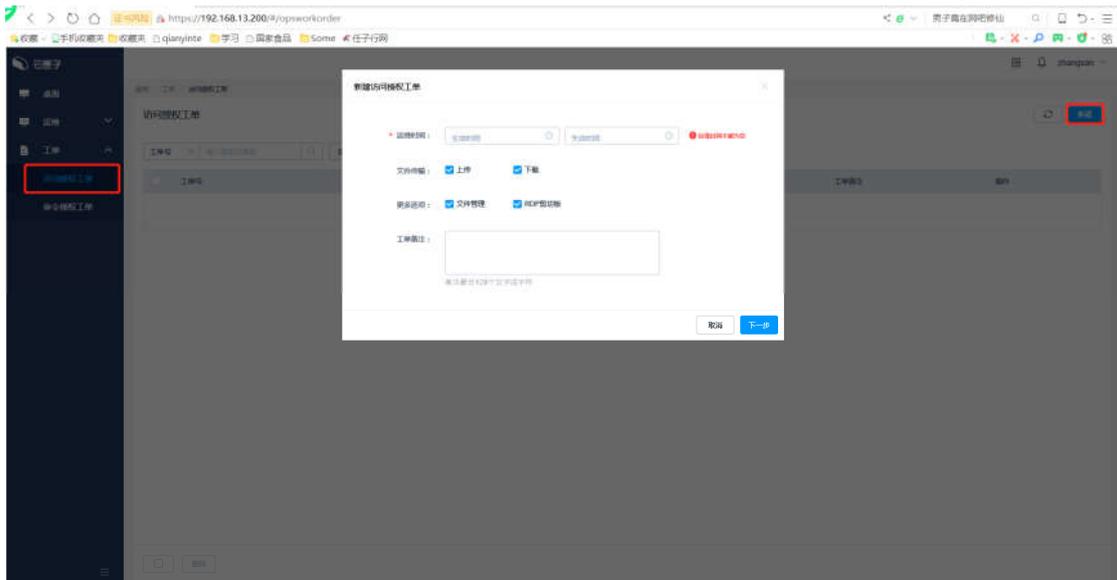


对于这台机器，可能只有 A 用户才能访问，但是其发起会话共享之后，原来无法访问的 B 用户也能访问了，需要注意的是，协同者也需要有堡垒机的帐号。在会话的审计记录里，也是会记录协同操作者的，因此其在堡垒机中也需要一个真实有效身份。

工单

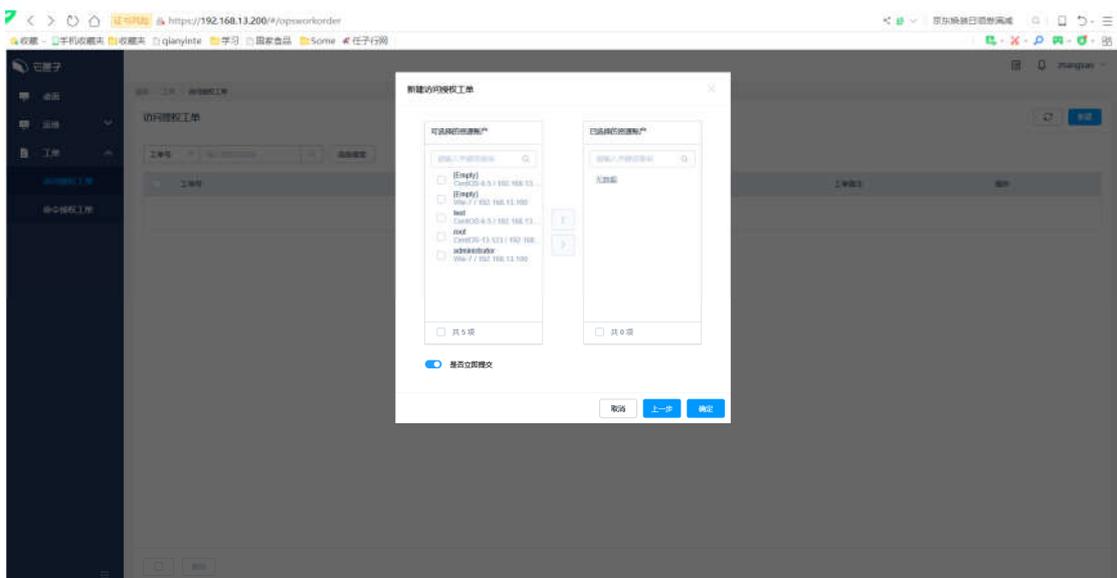
一般情况下，堡垒机管理员会给运维员授权（授权：设置访问控制策略）经常需要访问的资源主机，对于不常用的主机，可以通过“工单”功能进行申请，如图，存在两种类型的工单：

1. 访问授权工单：用来申请设备进行访问运维，。
2. 命令授权工单：适用于字符类型设备，不可手动创建，只有当堡垒机管理员给某用户设置“命令控制策略”，且触发命令后执行的操作作为“动态执行”时，才会自动在该列表生成对应的工单。然后再提交。



如图，创建访问控制策略时，需要填写一下相关信息，需要多久的使用时间、是否需要“上传、下载、文件管理”的权限，如果有 Windows 会话，是否需要 RDP 剪切板，如果有需要，进行相应的勾选。最后在备注写上此次操作的大概目的，例如，进行升级维护、修改 xx、xx 等服务，升级某 xx 的版本等等。

然后就是勾选需要的资源。

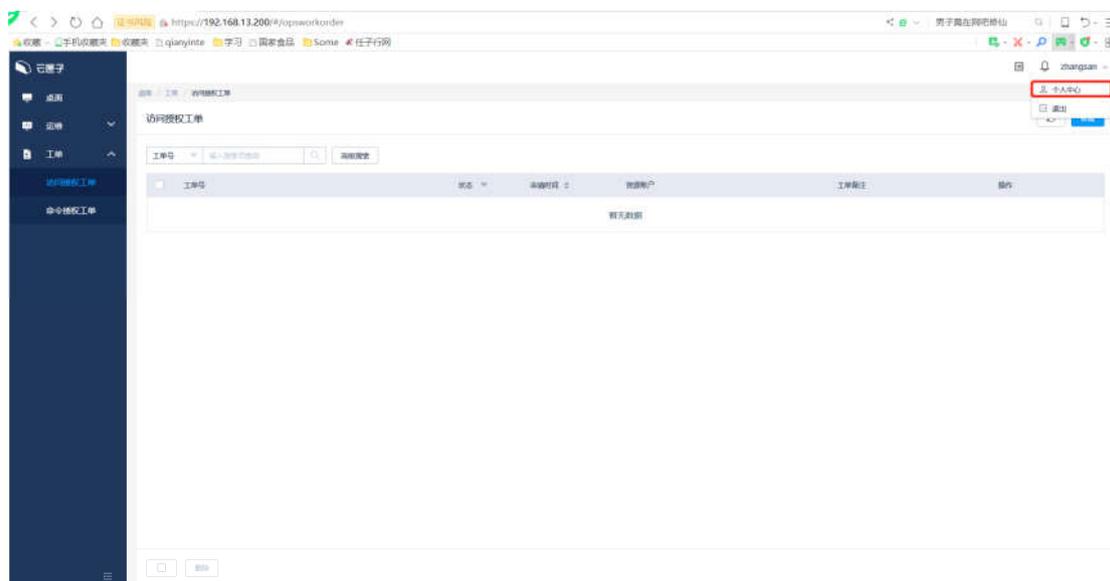


创建完成之后，选择是否立即提交，等待管理员批准之后，申请的资

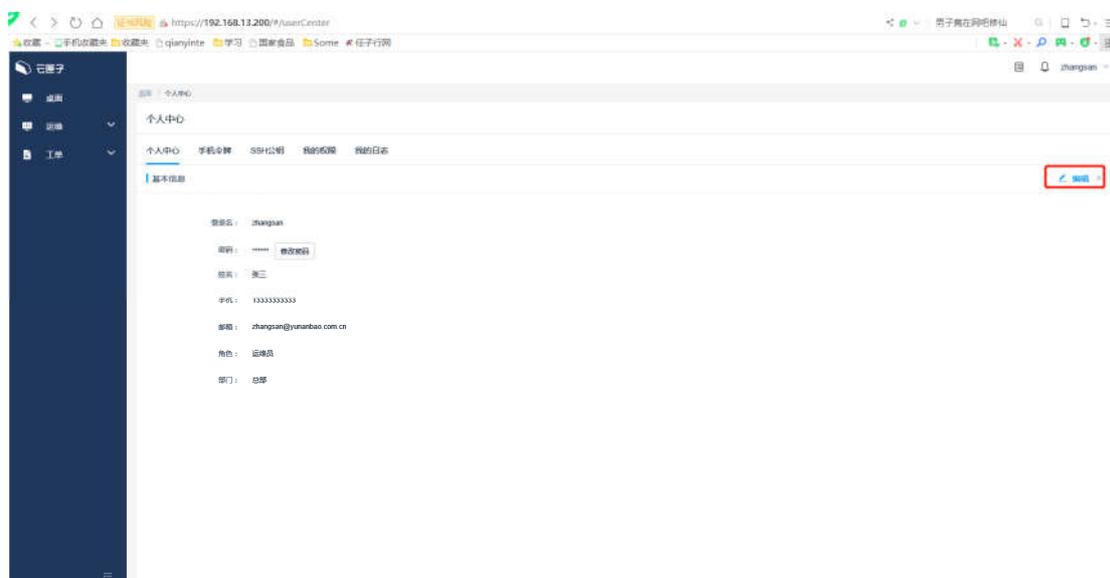
源就会出现在“运维”里头。

个人中心

除了左侧功能菜单的内容之外，每个用户还有自己的“个人中心”。



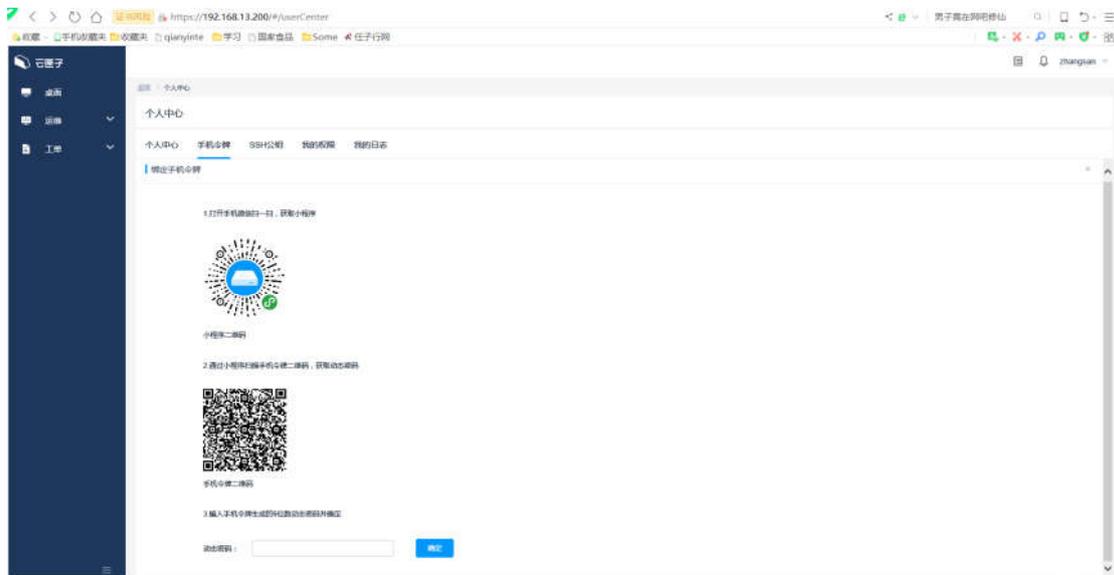
进入之后，可以修改个人信息，例如登录密码、邮箱、电话等。



如果管理员需要给某用户设置“手机令牌”，则需要实现在这里进行绑定。

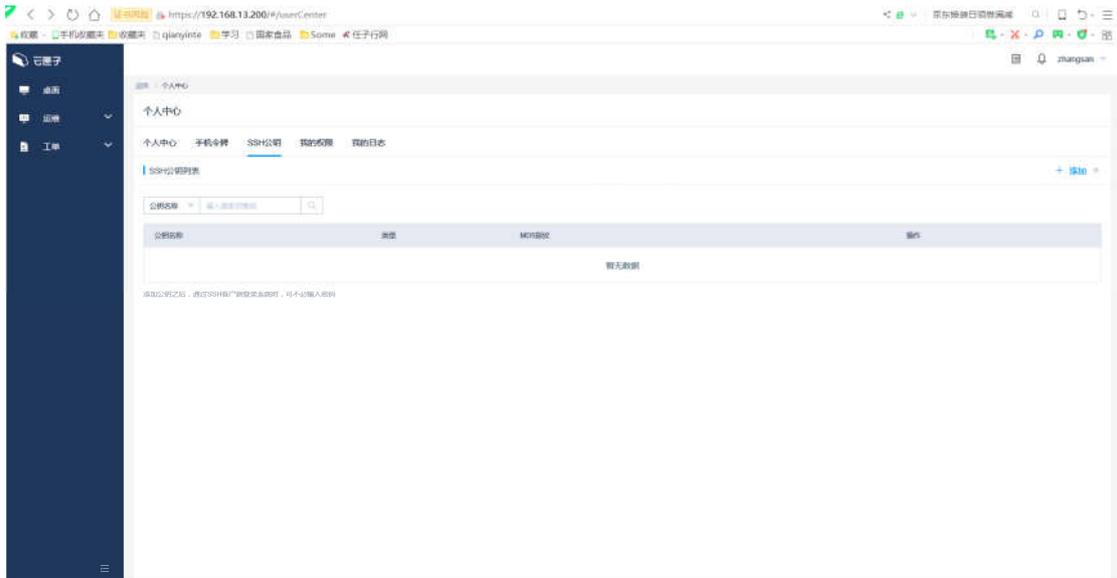
方法步骤如下：

1. 打开手机微信，扫一扫，第一个图标，关联相关微信小程序。
2. 打开的小程序打开后页面就有一个扫一扫，点击扫一扫，扫下面这个方形的二维码，此时会出现一行信息，其中会包括堡垒机用户名、以及一个6位数的动态码（30s一个），将首次出现的动态数字填入到下面的“动态密码”框，点击“确定”进行绑定。如果堡垒机系统时间和手机上的时间相差不大的话，即可绑定成功。

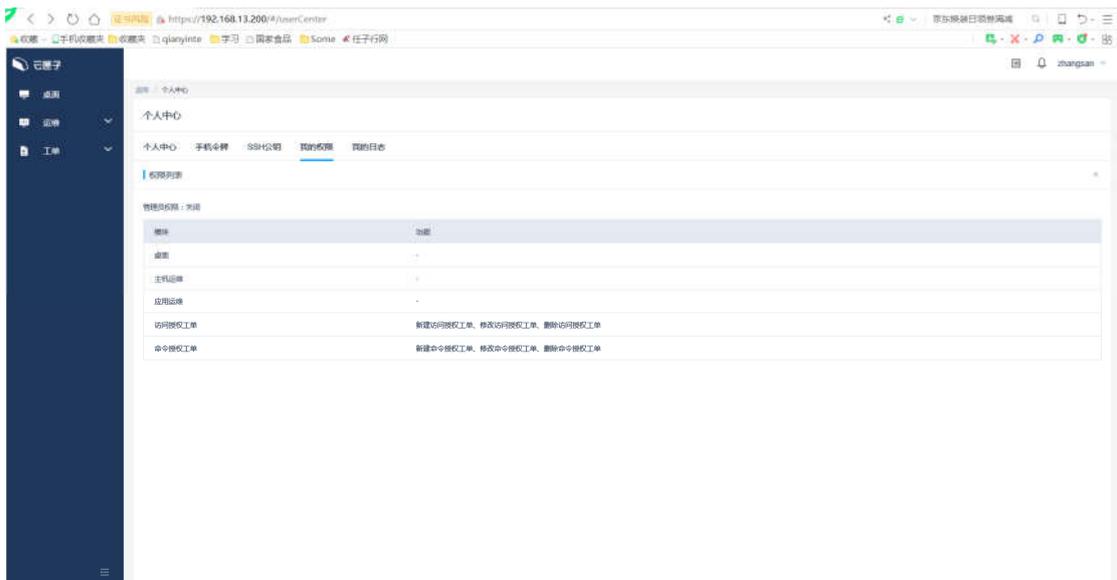


需要注意的是：开启双因子认证（静态密码+动态密码）后，将无法再直接使用静态密码登录。

如果管理的字符类设备比较多，使用的又是密钥对认证登录，可以在个人中心中进行添加，集中管理。



还可以看到自己所处的角色在堡垒机中拥有的权限。



以及个人操作记录，对于记性不大好的人，也挺有帮助的

浏览器地址: https://192.168.13.200/#/userCenter

个人中心

个人中心 手机令牌 SSH公钥 我的权限 我的日志

系统登录日志列表

日志内容

时间	来源IP	登录方式	日志内容	结果	备注
2018-06-06 19:08:04	192.168.13.1	Web页面	登录系统	成功	登录系统
2018-06-06 18:01:07	192.168.13.1	Web页面	退出系统	成功	退出系统
2018-06-06 18:01:00	192.168.13.1	Web页面	登录系统	成功	登录系统

20条/页 1/1 前往 1/1 页

系统操作日志列表

日志内容

时间	用户	来源IP	模块	日志内容	结果	备注
2018-06-06 19:26:28	zhangsan	192.168.13.1	运维	使用浏览器用户登录主机[CentOS-6.5]	成功	-
2018-06-06 19:15:03	zhangsan	192.168.13.1	运维	使用浏览器用户登录主机[CentOS-6.5]	成功	-

20条/页 1/1 前往 1/1 页