阿里云
堡垒机

用户指南（V3版本）

文档版本：20190830

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *{stand | slave}*

目录

1 管理员手册

1.1 登录系统

本文介绍了如何通过Web方式登录堡垒机系统。

背景信息

> **说明:**
> 只有阿里云主账号和RAM账号可以通过以下方法登录堡垒机Web界面。本地帐户、AD/LDAP账号无法登录堡垒机Web界面，只能通过CS方式运维。

操作步骤

1. 登录云盾堡垒机控制台。
2. 选择要操作的堡垒机实例，单击其操作列下的管理。
3. 选择接入方式，连接目标堡垒机Web 管理页面。

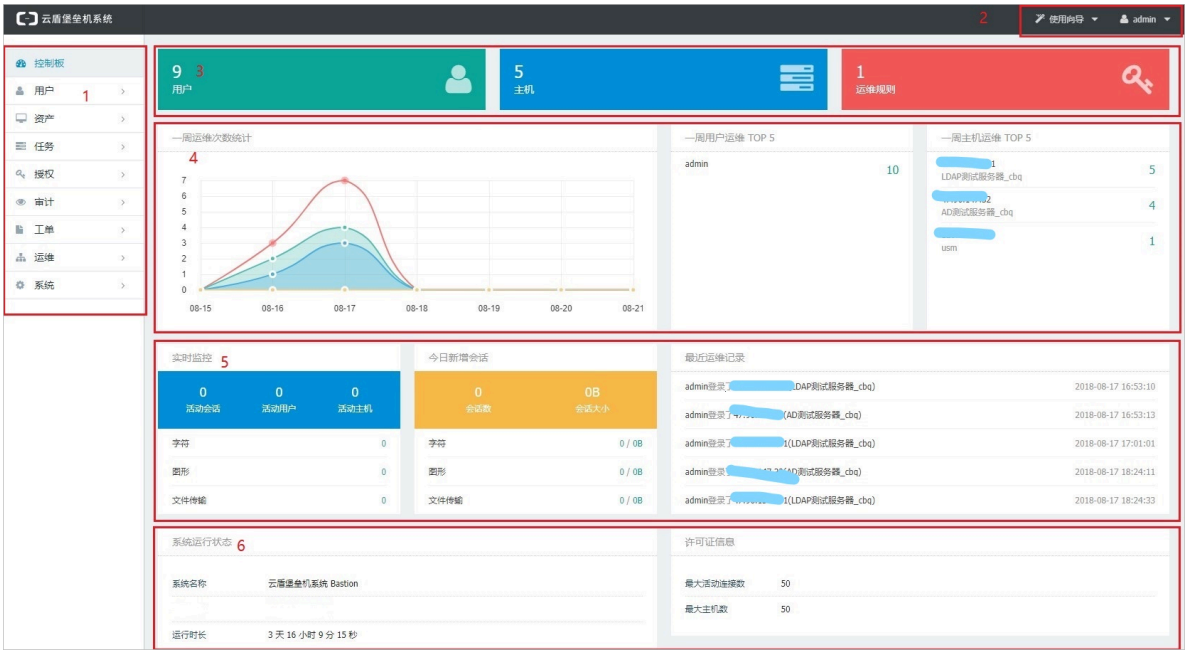


表 1-1: 系统首页说明

区域编号	区域页面介绍
1	显示系统的功能菜单项：控制板、用户、资产、任务、授权、审计、工单、运维和系统。
2	使用向导、用户功能菜单项。

3	从左往右分别是用户管理下的用户数量、主机数量和运维授权关系数量。
4	从左往右依次为一周运维次数统计、一周运维次数用户排名和一周运维次数主机排名。
5	从左往右依次为实时监控统计、新增会话记录和最近运维记录。
6	从左往右依次为系统运行状态（系统名称、运行时长）和许可证信息（最大活动连接数、最大主机数）。

1.2 控制板说明

控制板用于显示系统的常用功能、系统运行状态、最近运维会话、系统许可信息等。

控制板显示以下信息：

- 用户和资产：显示了能够管理的用户数量、主机数量和授权关系数量。单击图标可进入对应的管理界面。
- 一周运维次数统计：根据会话类型统计出一周内每天的运维次数。
- 一周用户运维 TOP 5：根据一周运维次数对用户进行排名，显示排名前五的用户及其运维次数。
- 一周主机运维 TOP 5：根据一周运维次数对主机进行排名，显示排名前五的主机及其运维次数。
- 实时监控：显示当前活动的会话数量、活动的用户数量和主机数量。
- 今日新增会话：显示今天产生的运维会话数量和会话大小。
- 最近运维记录：显示最近五条具体运维记录。
- 系统运行状态：显示系统名称和系统运行的时长。
- 许可证信息：包括最大活动连接数和最大主机数。

1.3 用户

1.3.1 用户管理

用户管理支持多种用户维护及配置操作，包括创建/删除用户、导入/导出用户、锁定/解锁用户、编辑用户基本/配置信息、搜索用户、配置SSH公钥/私钥，以及查看授权给用户的主机等。

创建用户

用户成员代表技术工程师，也就是自然人。云盾堡垒机的用户类型有本地用户、云子账号用户、AD/LDAP用户。

您可以在用户管理页面创建用户，创建方式包括：手动创建、导入RAM子账号、从本地文件中导入。

- 手动创建：单击新建用户进入配置页，按页面要求填写用户信息（标*为必填项），完成后单击创建用户。
- 导入RAM子账号：单击导入RAM子账号，在弹窗中选择需要导入的子账号。
- 从本地文件导入：选择更多操作 > 从文件导入。您可以直接上传由本系统导出的用户文件；或先下载模板文件，根据文件格式填写完成后再上传到本系统。

操作步骤

参照以下步骤创建用户：

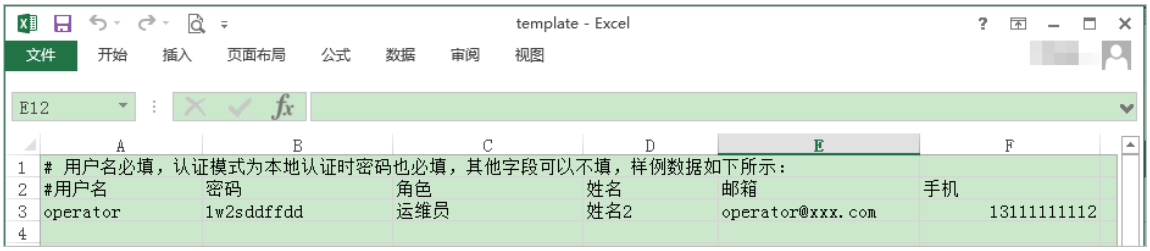
1. 进入用户 > 用户管理页。
2. （可选）手动创建用户。
   a. 单击新建用户，进入配置页。
   b. 输入用户名、密码、姓名，选择角色，并根据需要补充联系信息。
   c. 单击创建用户。

3. （可选）导入用户。

   a. 选择更多操作 > 导入用户。

   b. 在导入用户页，单击下载模板文件。

   c. 解压下载的模板文件，在用户表格中编辑用户信息。



   d. 在导入用户页，单击上传文件，并上传已编辑的用户表格。

   e. 单击导入用户即可成功导入。

导出用户

参照以下步骤导出用户：

1. 进入用户 > 用户管理页。
2. 在用户列表右下角单击导出用户，即可查看用户表信息。

删除用户

参照以下步骤删除用户：

1. 进入用户 > 用户管理页。
2. 在用户列表中勾选需要删除的用户，单击删除。

锁定用户

用户被锁定之后将不能登录堡垒机，直到管理员将其解锁为止。

参照以下步骤锁定用户：

1. 进入用户 > 用户管理页。
2. 在用户列表中单击需要锁定的用户。

3. 在用户配置页勾选锁定这个用户。

> 说明:
> 您也可以在用户列表勾选相应用户后，单击锁定。

解锁用户

参照以下步骤解锁用户：

1. 进入用户 > 用户管理页。
2. 在用户列表中单击需要解锁的用户。
3. 在用户配置页取消勾选锁定这个用户。

> 说明:
> 您也可以用户列表勾选相应用户后，单击解锁。

搜索用户

参照以下步骤搜索用户：

1. 进入用户 > 用户管理页。
2. 在搜索框中输入用户名进行搜索。您也可以通过用户角色和认证方式过滤用户列表。

编辑用户基本信息

参照以下步骤编辑用户基本信息：

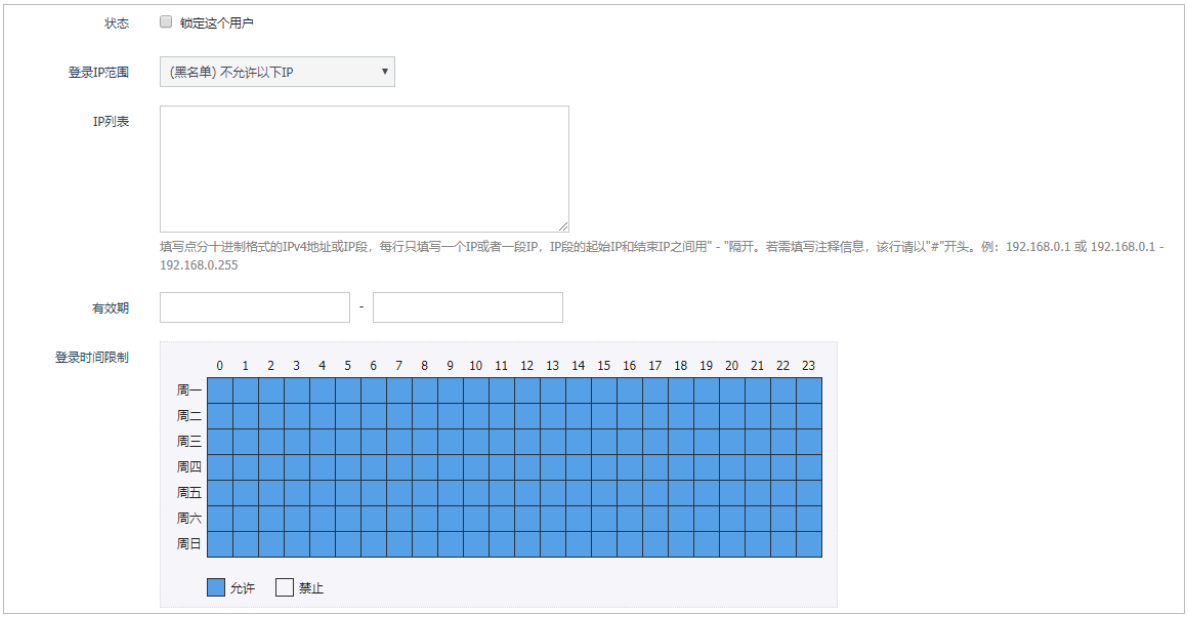
1. 进入用户 > 用户管理页。
2. 单击要操作的用户名。
3. 前往基本信息页，根据需要编辑相关信息。

编辑用户配置

参照以下步骤编辑用户配置：

1. 进入用户 > 用户管理页。
2. 单击要操作的用户名。

3. 前往用户配置页，根据需要锁定/解锁用户、限制用户登录IP范围、设置用户登录有效期和登录时间。



管理SSH公钥

SSH公钥适用于使用SSH协议登录堡垒机系统的用户。

参照以下步骤添加SSH公钥：

1. 进入用户 > 用户管理页。
2. 单击要操作的用户名。
3. 前往SSH公钥页，并单击添加SSH公钥。

4. 在配置窗口中添加公钥名称和公钥内容后保存。

设置SSH私钥

SSH私钥用于使用SSH协议登录主机。

参照以下步骤设置SSH私钥：

1. 进入用户 > 用户管理页。
2. 单击要操作的用户名。

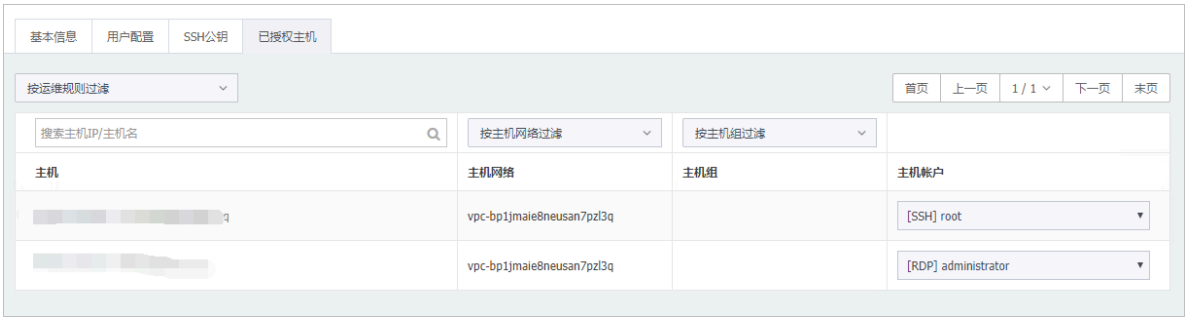
3. 在页面右上角个人信息下选择SSH私钥。

4. 输入SSH私钥，并单击保存私钥。

查看已授权的主机

参照以下步骤查看已授权的主机：

1. 进入用户 > 用户管理页。
2. 单击要操作的用户名。
3. 前往已授权主机页，查看所有授权给当前用户的主机。



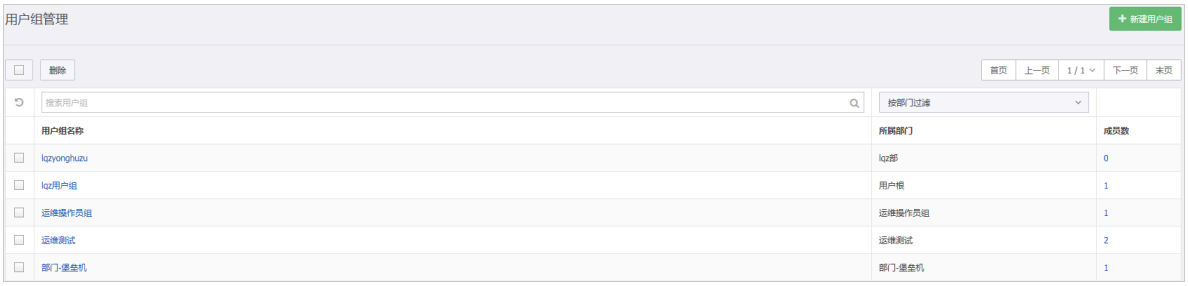
1.3.2 用户组管理

您可以将多个用户加入到一个用户组，并对这些用户进行批量授权。用户组管理支持创建、编辑、删除用户组，以及维护用户组成员。

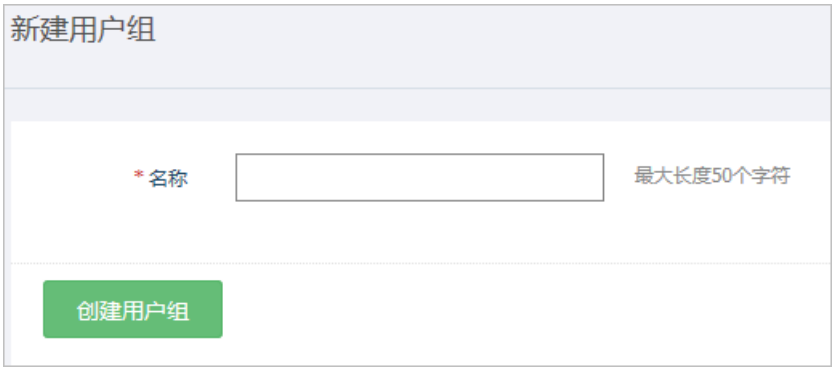
新建用户组

参照以下步骤新建用户组：

1. 进入用户 > 用户组管理页。



2. 单击新建用户组进入配置页。



3. 在新建用户组页，填写用户组名称，然后单击创建用户组。

   成功创建用户组后，单击用户组名称可前往编辑页面，添加、删除用户组成员。

删除用户组

参照以下步骤删除用户组：

1. 进入用户 > 用户组管理页。
2. 勾选要删除的用户组，单击删除。

搜索用户组

参照以下步骤搜索用户组：

1. 进入用户 > 用户组管理页。
2. 在搜索框中输入用户组名称进行搜索。

修改用户组名称

参照以下步骤修改用户组名称：

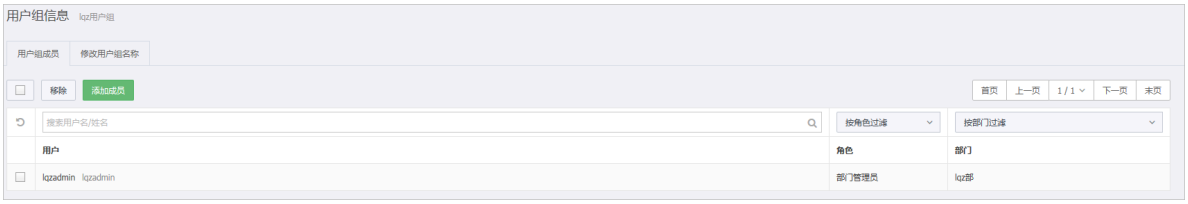
1. 进入用户 > 用户组管理页。
2. 单击要操作的用户组名称。

3. 前往修改用户组名称页，输入新的用户组名称，并单击保存更改。

为用户组添加成员

参照以下步骤为用户组添加成员：

1. 进入用户 > 用户组管理页。
2. 单击要操作的用户组名称。
3. 前往用户组成员页，单击添加成员。

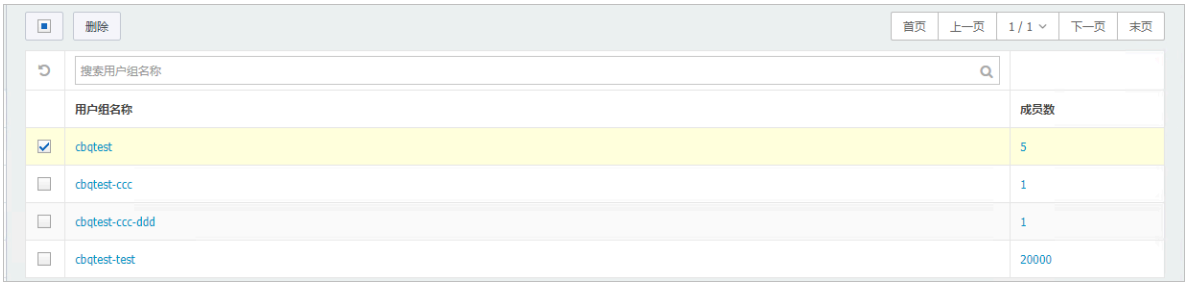


4. 在选择用户对话框中勾选需要添加到当前用户组的成员。
5. 单击添加即可成功添加并自动返回配置页。

从用户组移除成员

参照以下步骤从用户组中移除成员：

1. 进入用户 > 用户组管理页。
2. 单击要操作的用户组名称。
3. 前往用户组成员页，勾选要移除的用户，并单击移除。



1.3.3 添加阿里云子账号到堡垒机账户系统

本文介绍如何在阿里云访问控制（RAM）中创建用于堡垒机管理和运维的阿里云子账号（即RAM用户），以及如何导入阿里云子账号到堡垒机账户系统。

操作步骤

1. 新建阿里云子账号。

   a) 使用阿里云主账号登录访问控制控制台。

   b) 在人员管理 > 用户页面，单击新建用户。

   c) 在新建用户页面，设置用户登录名称和显示名称，并选择访问方式。

   d) 单击确定完成用户创建。

2. 为阿里云子账号启多因素认证（MFA）登录。

a) 使用阿里云主账号登录访问控制控制台。

b) 在人员管理 > 用户页面，单击新创建的用户登录名。

c) 在用户详情页，单击启用虚拟MFA设备。

d) 在启用虚拟MFA设备页面，（阿里云子账号使用者）使用阿里云App（或其他MFA应用程序）扫码添加账号。

成功添加账号后，在阿里云App的虚拟MFA页面会显示已关联账号和每60s自动刷新生成的安全码。

e) **在启用虚拟MFA设备页面的第一组安全码和第二组安全码中输入阿里云App中连续获取的两组安全码，然后单击确定启用。**

成功启用MFA设备后，每次使用子账号登录时，都要输入从已绑定的MFA设备（即阿里云App）中获取的安全码。

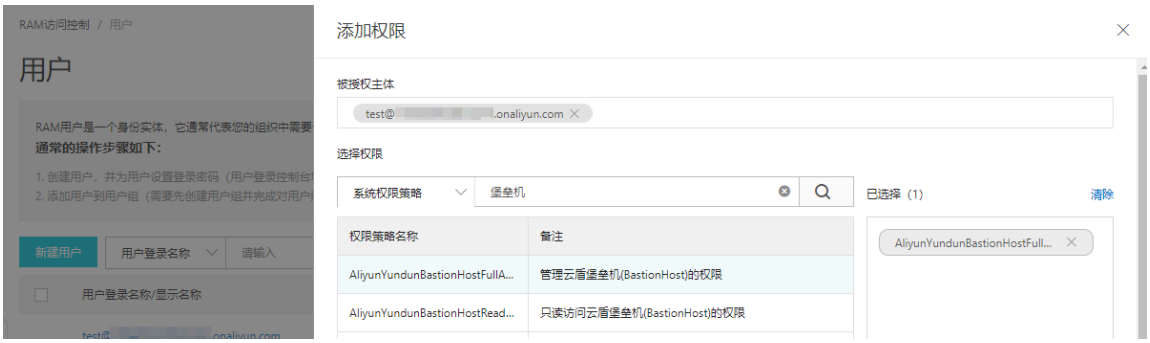
3. 向阿里云子账号授权。

a) 使用阿里云主账号登录访问控制控制台。

b) 在人员管理 > 用户页面，选择要操作的子账号，单击添加权限。

c) 在添加权限页面，搜索以下系统授权策略，并选择要授权给当前子账号的权限：

- AliyunYundunBastionHostFullAccess（管理员权限）
- AliyunYundunBastionHostReadOnlyAccess（运维员权限）



d) 选择要授予当前子账号的权限后，单击确定完成授权。

被授予权限的子账号可用来执行相应操作。

4. 添加阿里云子账号到堡垒机账户系统。

   a) 登录云盾堡垒机控制台。

   b) 在账户页面，单击右上角的添加子账号。

   c) 在添加子账号对话框，单击刷新子账号，获取当前阿里云账号的子账号信息；然后勾选要导入的子账号，单击导入子账号。

   勾选的子账号被导入到账户列表中。

后续步骤

已添加到堡垒机账户系统的阿里云子账号能够进一步被导入到具体的堡垒机实例，作为堡垒机的用户。更多信息，请参见导入阿里云子账号作为堡垒机用户。

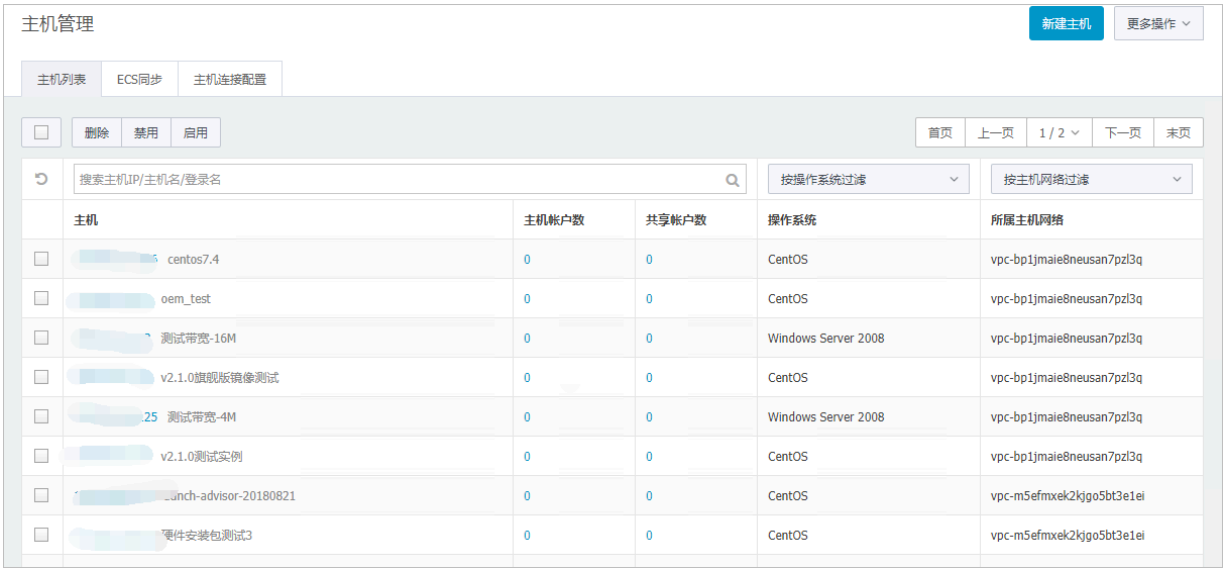
1.4 资产

1.4.1 主机管理

主机管理用于管理目标主机的IP、名称、协议、控制策略、添加、导入、导出、编辑等功能。

新建主机

您可以在资产 > 主机管理页面创建主机，创建方式包括：手动创建、同步阿里云ECS、从本地文件导入。



- 手动创建：单击新建主机，进入新建主机页，然后按要求填写主机信息后即可创建。
- 同步阿里云ECS：在ECS同步页，单击同步阿里云ECS，在弹窗中选择需要同步的ECS后即可导入。
- 从本地文件导入：在主机列表，选择更多操作 > 从文件导入。您可以直接上传由本系统导出的主机文件，或先下载模板文件，根据文件格式填写主机信息后再上传到本系统。

> **说明:**
> 通过此方式可以将主机帐户一同导入，当需要添加大量主机资产时，推荐您使用此方式。

操作步骤

参照以下步骤新建主机：

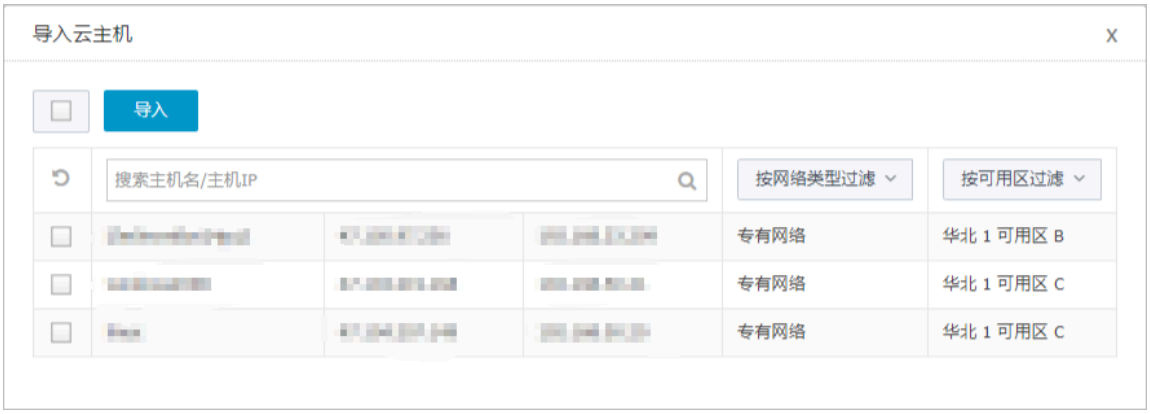
1. 进入资产 > 主机管理页。
2. （可选）手动创建主机。
   a. 单击新建主机。
   b. 在新建主机页，填写主机IP、主机名称、操作系统、所属网络等，并单击创建主机。

      创建成功后，单击主机IP进入相关页面，可编辑主机基本信息、主机配置信息、主机帐户信息、共享帐户。

3. （可选）同步阿里云ECS。

   a. 前往阿里云ECS页，单击页面右上角的同步阿里云ECS。

   b. 勾选要导入堡垒机的ECS实例，并单击导入。



4. （可选）导入主机。

   a. 在主机列表右上方，选择更多操作 > 导入主机。

   b. 在导入主机页，单击下载模板文件，将文件下载至本地并解压缩。

   c. 编辑并保存主机表格。

# 各个字段的值必须满足本系统的输入规则						
# 若该主机的帐户密码字段为空，则登录模式为手动，反之为自动						
# 样例数据如下：						
#主机IP	主机名称	操作系统	帐户登录名	帐户密码	协议:端口	主机组名称
192.168.50.112	主机名称	CentOS	root		TELNET	主机组1
192.168.50.112	主机名称	CentOS	xxx		SSH:10022	
192.168.50.113	主机名称	Windows Server 2012	yyy		FTP:10021	主机组2
192.168.50.113	主机名称	Windows Server 2012	zzz		SFTP	主机组3
192.168.50.113	主机名称	Windows Server 2012	www		RDP	主机组3
192.168.50.114	主机名称	Other Linux	2:yyy		VNC	主机组3
192.168.50.115	主机名称	Cisco IOS Device				

说明:

第一列为主机IP（必填）、第二列为主机名称、第三列为操作系统、第四列为帐户名称，第五列为帐户密码，第六列为协议及端口号，第七列为主机组名称。网络协议的格式为协

议:端口号（中间用英文冒号隔开），如SSH:22；如果存在多个协议及端口号，可参考TELNET:23,FTP:21（中间用英文逗号隔开）。

d. 在导入主机页，单击上传文件。

e. 在打开文件对话框中选择并导入已编辑的主机表格。

f. 单击导入主机后即可成功导入。

5. （可选）创建主机后，您可以在主机连接配置页设置主机网络下的主机通过公网IP连接还是内网IP连接。

创建主机帐户

主机帐户是用于登录目标主机及应用的管理帐户。本系统支持7种协议的帐户：SSH、TELNET、FTP、SFTP、RDP、VNC、Rlogin。

参照以下步骤创建主机帐户：

1. 进入资产 > 主机管理页。
2. 选择主机帐户 > 添加主机帐户。
3. 在新建主机帐户页，选择协议、登录模式、帐户和密码是否代填、验证是否连通。

说明:

关于主机帐户选项的说明，请参考主机账户选项说明。

4. 单击共享帐户选项卡，为主机关联或移除共享帐户。

导出主机

通过导出主机，您可以导出以下信息：主机IP、主机名称、操作系统、主机帐户登录名、帐户密码、协议:端口、主机组、主机网络。

导出的主机文件可直接导入堡垒机。因此，您可以通过此方式对主机和主机帐户进行批量修改。

参照以下步骤导出主机：

1. 进入资产 > 主机管理页。
2. 单击页面右下角的导出主机即可完成导出。

删除主机

参照以下步骤删除主机：

1. 进入资产 > 主机管理页。
2. 勾选要删除的主机，单击删除即可成功删除。

禁用主机

通过禁用主机，您可以限制用户对被禁用主机的访问。

参照以下步骤禁用主机：

1. 进入资产 > 主机管理页。
2. 单击要禁用的主机，进入主机配置页。
3. 在主机配置页，勾选禁用这台主机，并单击保存更改。

启用主机

参照以下步骤启用主机：

1. 进入资产 > 主机管理页。
2. 单击要启用的主机，进入主机配置页。
3. 在主机配置页，取消勾选禁用这台主机，并单击保存更改。

搜索主机

参照以下步骤搜索主机：

1. 进入资产 > 主机管理页。
2. 在搜索框中输入主机名IP、主机名、或登录名进行搜索。您也可以通过操作系统或主机网络过滤主机列表。

编辑主机

参照以下步骤编辑主机：

1. 进入资产 > 主机管理页。
2. 单击要操作的主机IP。

3. 前往基本信息页，编辑主机信息和配置协议端口，完成后单击保存更改。

说明:

此处的协议端口指目标主机上该协议对应的端口号。出于安全考虑，您的主机一般不用常见的端口号，但是在托管到堡垒机时需要在此处将协议端口号设置为真实的端口。

4. 前往主机配置页，进行详细配置。

说明:

- 主机配置选项与运维规则中协议控制都是相同的选项内容。当运维规则中的协议控制为启用状态时，系统将忽略主机配置选项，否则系统将采用主机配置选项。

- **关于主机配置选项的说明，请参考主机配置选项说明。**


主机配置
基本信息
主机配置
主机帐户
共享帐户
主机配置
状态
禁用这台主机
会话选项
开启会话二次审批
开启会话备注
开启历史会话审计
开启实时会话监控
RDP选项
启用键盘记录
允许打印机/驱动器映射
允许使用剪贴板下载
允许使用剪贴板上传
SSH选项
允许X11转发
允许打开SFTP通道
允许请求exec
禁止文件上传
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
FTP选项
禁止文件上传
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
文件审计
生成文件SHA1
保存文件
保存下载文件
保存上传文件
启用文件压缩
不保存超过 30 KB 的文件
单个会话保存的文件超过 100 MB 时停止保存
保存更改

5. 编辑完成后单击保存更改。

1.4.2 主机选项说明

主机选项包括主机帐户选项和主机配置选项。

主机帐户选项说明

表 1-2: RDP主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-3: SSH主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录（二次登录）和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录（二次登录）	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-4: TELNET主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录（二次登录）和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录（二次登录）	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-5: FTP主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-6: SFTP主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。

手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-7: VNC主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机帐号（X:帐户名）和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	须设置帐户名称X:root（X表示桌面号，从0开始）、密码留空即可；运维人员登录目标主机时需要输入VNC主机的密码才能登录成功。
X:root	表示VNC的帐户。如果VNC服务器只启用了一个5900端口，那就是0:root；如果VNC服务器同时启用了8个桌面号（即5901-5908），那就是1:root-8:root。 如果主机是unix类平台，则帐户名称的格式为X:帐户名（X表示桌面号，从0开始）。 如果主机是windows平台，则帐户名称的格式为X:root（X表示桌面号，从0开始），目前仅支持VNC服务端的“VNC password”模式。 “X”是为了实现VNC服务会启动多个桌面，且用户之间互不干扰地使用各自的桌面；所以VNC服务使用的端口号与桌面号相关，VNC服务使用的端口从5900开始，例如桌面号是“:1”，则使用的端口是5901；桌面号是“:2”，则使用的端口是5902，依次类推；基于Java的VNC客户程序Web服务端口从5800开始，它也与桌面号相关。
验证	如需验证主机的账户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

表 1-8: Rlogin主机帐户选项

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机帐号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击验证。 · 提示验证成功代表帐户和密码正确。 · 提示验证失败代表帐户或密码错误。 · 提示验证超时代表网络或协议不通。

主机配置选项说明

选项	功能	解释
会话选项	开启会话二次审批	登录主机时，需要管理员对此次登录行为进行审核后，才可登录。
	开启会话备注	登录主机时需要写明登录主机的原因或目的才可登录，便于事后审计。
	开启历史会话审计	表示允许堡垒机对运维会话内容进行审计，关闭后会产生会话记录，但没有具体内容。
	开启实时会话监控	表示管理员可以对主机进行实时监控，关闭后管理员可看到实时会话记录，但无法得知会话内容。
RDP选项	启用键盘记录	表示记录RDP主机的键盘符操作记录。
	允许打印机/驱动器映射	在运维RDP主机时，可以映射本地打印和本地磁盘。
	允许使用剪切板下载	表示运维RDP主机时，可以使用复制-粘贴功能从主机下载。
	允许使用剪贴板上传	表示运维RDP主机时，可以使用复制-粘贴功能上传至主机。
SSH选项	允许X11转发	表示在运维时可以通过SSH方式转发X11协议。
	允许打开SFTP通道	表示在运维时可以使用SSH的客户工具直接打开SFTP协议。
	允许请求exec	表示可以直接使用exec指令。

	禁止文件上传	表示可以禁止通过sftp、scp、rzsz命令进行文件上传。
	禁止文件下载	表示可以禁止通过sftp、scp、rzsz命令进行文件下载。
	禁止文件删除	表示可以禁止通过sftp进行文件删除操作。
	禁止重命名	表示可以禁止通过sftp进行重命名操作。
	禁止目录创建	表示可以禁止通过sftp进行目录创建操作。
	禁止目录删除	表示可以禁止通过sftp进行目录删除操作。
文件审计	生成文件SHA1	表示可以对SFTP/FTP传输的文件进行sha1签名，确保文件的唯一性与不重复。
	保存文件	表示可以对SFTP/FTP传输的文件进行保存在运维审计系统中，审计时可下载下来对文件内容进行审计，查看是否有违规文件。
	保存下载文件	表示可以保存下载的文件。
	保存上传文件	表示可以保存上传的文件。
	启用文件压缩	表示可以对传输的文件进行压缩，节省堡垒机空间。
	不保存超过多少KB的文件	表示可以根据单个文件的大小进行保存。
	单个会话保存的文件总大小超过多少MB时停止保存	表示可以控制单个会话保存的文件大小。

1.4.3 共享帐户

当多个主机的管理帐户的登录名、密码/密钥相同时，通过关联共享帐户可以节约配置时间。

新建共享帐户

参照以下步骤新建共享帐户：

1. 进入资产 > 共享帐户页。

2. 单击新建共享帐户。
3. 在新建共享帐户对话框，输入帐户名称、登录名和密码，并选择协议，完成创建共享帐户。

   创建完成后，单击关联主机，通过添加主机，将此帐户关联到主机中。

编辑共享帐户

参照以下步骤编辑共享帐户信息：

1. 进入资产 > 共享帐户页。
2. 选择要操作的帐户，单击编辑。
3. 在编辑共享帐户页，输入帐户信息，单击保存，完成对帐户的修改。

删除共享帐户

参照以下步骤删除共享帐户：

1. 进入资产 > 共享帐户页。
2. 勾选要删除的帐户，单击删除即可将共享帐户删除。

搜索共享帐户

参照以下步骤搜索共享帐户：

1. 进入资产 > 共享帐户页。
2. 在搜索框中输入帐户名或登录名进行搜索。您也可以通过协议或者认证类型过滤共享帐户列表。

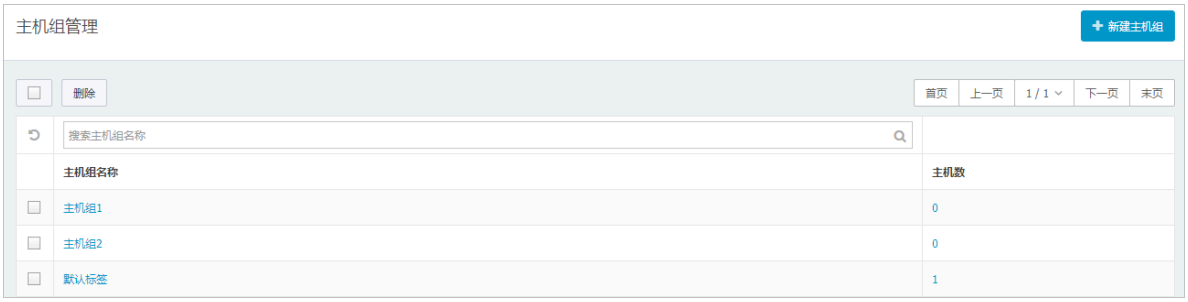
1.4.4 主机组管理

您可以将多个主机加入到一个主机组，并对这些主机进行批量授权。

新建主机组

参照以下步骤新建主机组：

1. 进入资产 > 主机组管理页。



2. 单击新建主机组。
3. 在新建主机组页，输入主机组名称，单击创建主机组，即可成功创建主机组并返回主机组管理页。
4. 单击新创建的主机组名称。
5. 在主机组配置页，选择主机组成员选项，单击页面中的添加主机。
6. 在选择主机对话框，勾选要添加到当前主机组的主机，并单击添加。

修改主机组名称

1. 进入资产 > 主机组管理页。
2. 单击要操作的主机组的名称。
3. 前往修改主机组名称页，输入新的主机组名称，单击保存更改即可成功修改主机组名称。

删除主机组

1. 进入资产 > 主机组管理页。
2. 勾选要删除的主机组，单击删除即可删除主机组。

搜索主机组

1. 进入资产 > 主机组管理页。
2. 在搜索框中输入主机组名称进行搜索。

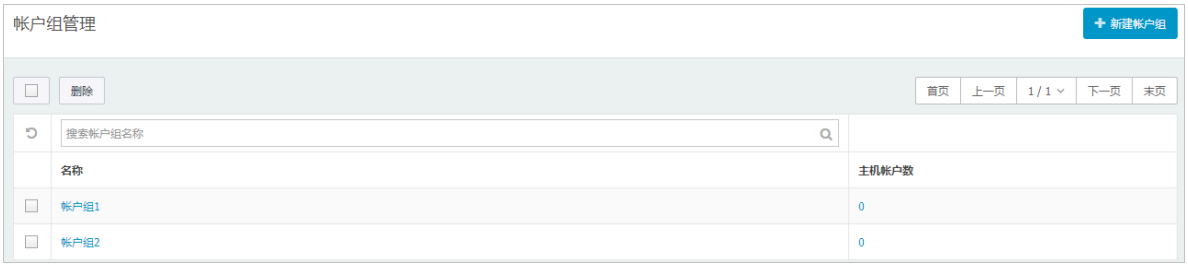
1.4.5 帐户组管理

您可以将多个帐户加入到一个帐户组，并对这些帐户进行批量授权。

新建帐户组

参照以下步骤新建帐户组：

1. 进入资产 > 帐户管理页。



2. 单击新建帐户组。
3. 在新建帐户组对话框中，输入帐户组名称，并单击创建帐户组。

   成功创建后，单击帐户组名称，可以进入帐户组编辑页面。

编辑帐户组

参照以下步骤维护帐户组成员及编辑帐户组名称：

1. 进入资产 > 帐户管理页。
2. 单击要操作的帐户组名称。
3. 前往主机帐户页，添加或删除帐户组成员。

4. 前往修改帐户组名称页，编辑帐户组名称，并单击保存修改。

删除帐户组

参照以下步骤删除帐户组：

1. 进入资产 > 帐户管理页。
2. 勾选要删除的帐户组，单击删除。

搜索帐户组

1. 进入资产 > 帐户管理页。

2. 在搜索框中输入帐户组名称进行搜索。

1.5 授权

1.5.1 运维授权

运维授权是指将某部分主机帐户的运维权限赋予某部分用户。

运维授权是将堡垒机中的用户与主机资产联系在一起的概念，通过运维授权功能可以达到控制某个用户只能访问他权限内主机的目的。

运维授权的关系类型有：

- 帐户组授权给用户组
- 单个主机帐户授权给用户组
- 主机组授权给用户组
- 帐户组授权给单个用户
- 单个主机帐户授权给单个用户
- 主机组授权给单个用户

您可以在授权 > 运维规则页查看所有运维规则。

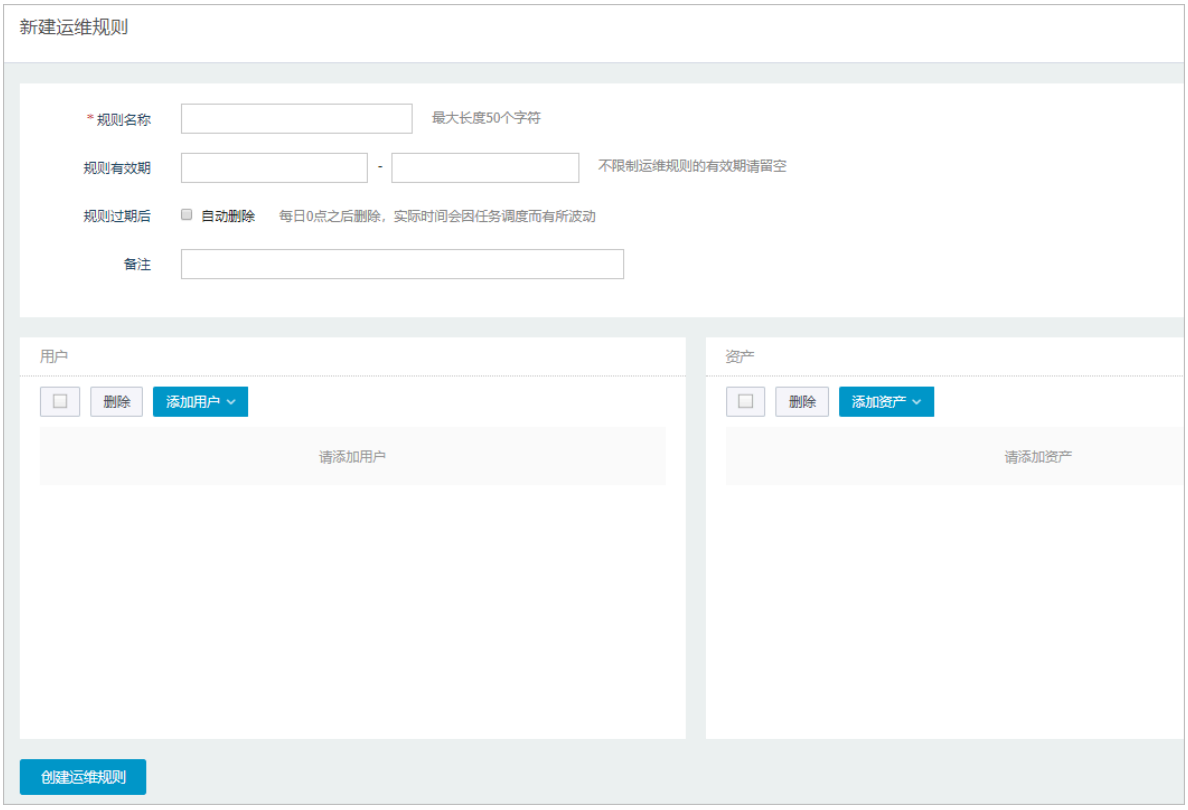
新建运维授权

以“主机账户授权给用户”为例，参照以下步骤新建运维规则：

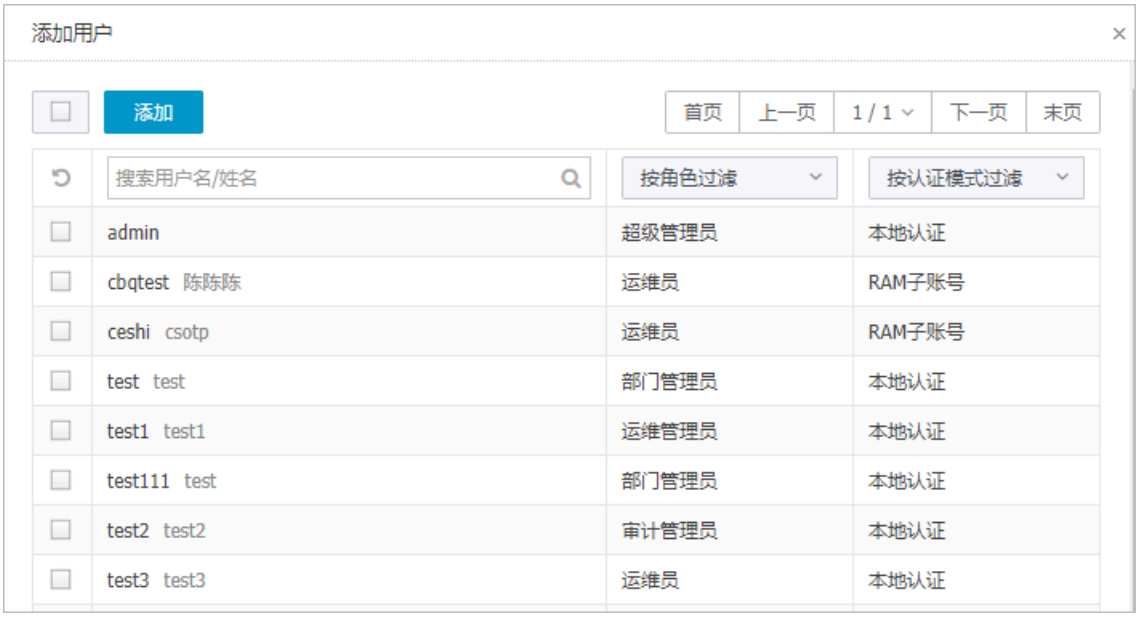
1. 登录云盾堡垒机Web管理页。
2. 进入授权 > 运维授权页。
3. 单击新建运维规则。
4. 在新建运维规则页，填写规则名称。按实际需求设置规则有效期以及规则过期后是否自动删除。

说明：

若勾选了规则过期后自动删除，则过期后此运维规则中的授权关系不会在运维页面中出现。

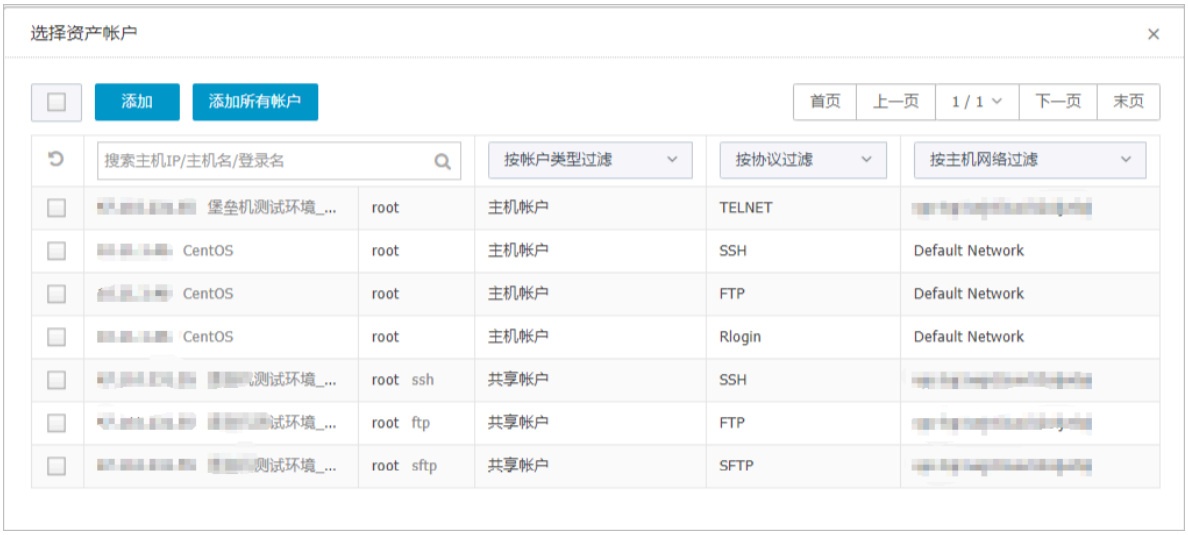


5. **在新建运维规则页，单击添加用户/用户。**
6. **在添加用户对话框中，选择要添加的用户，并单击添加。**



7. **在新建运维规则页，单击添加资产/主机帐户。**

8. 在选择主机帐户对话框中，选择要添加的主机帐户，并单击添加。



9. 设置用户和资产之后，在新建运维规则页单击创建运维规则即可完成授权。

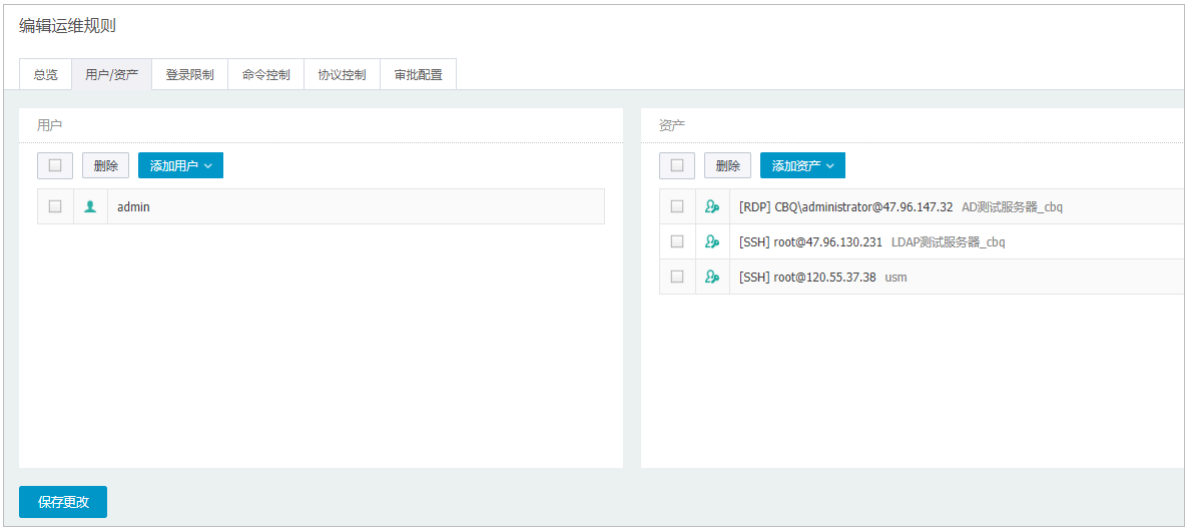
编辑运维规则

在运维规则页，单击运维规则名称或者单击编辑规则可以对运维规则进行修改。

参照以下步骤修改运维规则：

1. 进入授权 > 运维授权页。
2. 选择要操作的规则，单击运维规则名称或者单击编辑规则进入运维规则总览页，在此页面可以修改规则名称、规则有效期等信息。

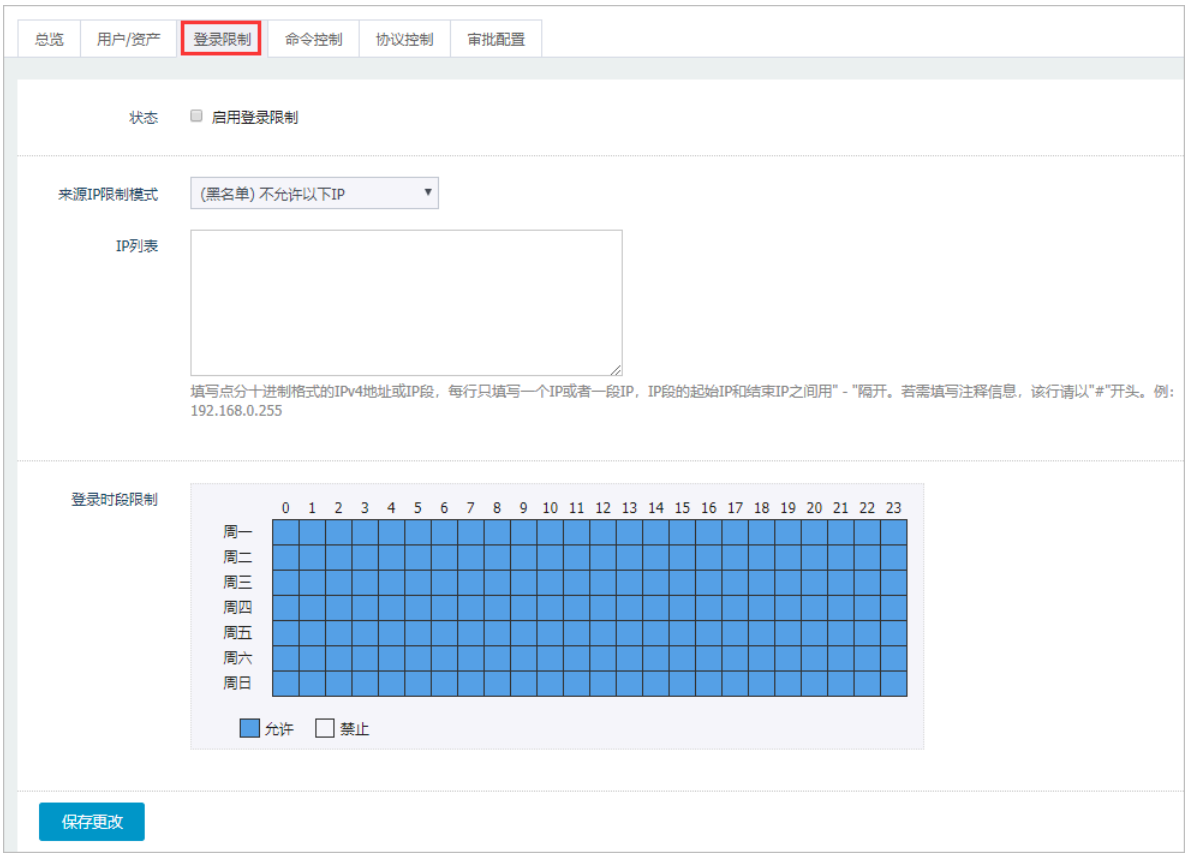
3. 前往用户/资产页，修改用户和资产间关联关系。



4. 前往登录限制页，编辑源IP的黑白名单列表及登录时段限制。编辑完成后勾选启用登录限制并单击保存更改。

说明:

若不勾选启用登录限制，则登录限制页的设置不会生效。



5. 前往命令控制页，启用命令控制，并配置命令阻断，命令审批和命令黑白名单。

> **说明:**
> 若不勾选启用命令控制，则命令控制页的设置不会生效。

6. 前往协议控制页，配置各个协议会话中的相关控制选项。

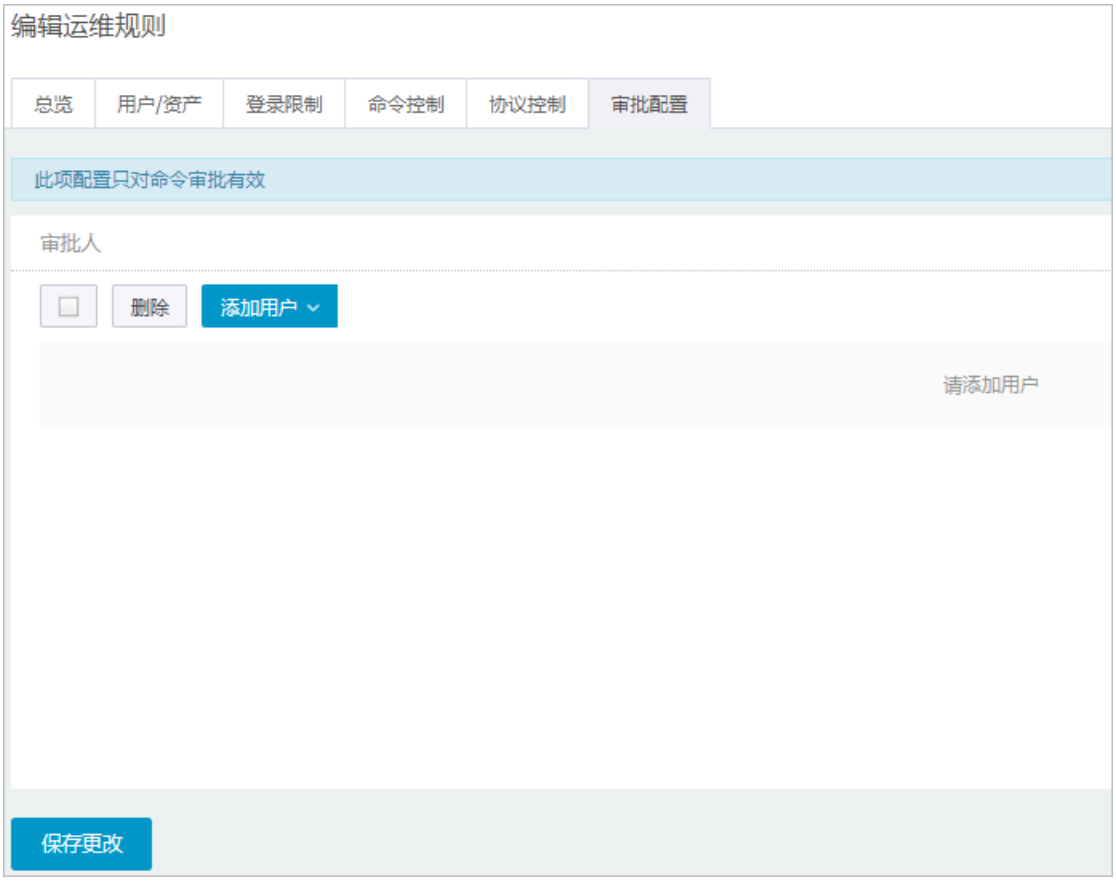
> **说明:**
> 此处的协议控制选项作用与主机配置中的协议控制选项相同，但优先级高于主机配置。勾选启用协议控制后，在此运维规则的授权关系中所采用的是此处的协议控制设置，否则将采用主机

配置中的协议控制设置。此处设置主要用于同一主机账户授权给不同用户时需要对不同用户设置不同权限的场景。


编辑运维规则
总览
用户/资产
登录限制
命令控制
协议控制
审批配置
状态
启用协议控制
会话选项
开启会话二次审批
开启会话备注
开启历史会话审计
开启实时会话监控
RDP选项
启用键盘记录
允许打印机/驱动器映射
允许使用剪贴板下载
允许使用剪贴板上传
SSH选项
允许X11转发
允许打开SFTP通道
允许请求exec
禁止文件上传
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
FTP选项
禁止文件上传
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
文件审计
生成文件SHA1
保存文件
保存下载文件
保存上传文件
启用文件压缩
不保存超过 30 KB 的文件
单个会话保存的文件超过 100 MB 时停止保存
保存更改

7. 前往审批配置页，设置命令审批人。

> **说明:**
> 此项配置只对命令审批有效。



删除、禁用或启用运维规则

参照以下步骤管理运维规则：

1. 进入授权 > 运维授权页。
2. 勾选相应的运维规则，单击删除、禁用或启用可对规则执行相应操作。

查看运维分组

参照以下步骤查看运维分组：

1. 进入授权 > 运维授权页。
2. 在搜索框输入用户名、主机帐户、帐户组和应用进行搜索。您也可以按用户类型、资产类型、IP范围限制和部门过滤授权规则，快速查找授权关系。

1.5.2 未授权登录审核

未授权登录审核用于对开启了允许未授权登录功能后，用户通过未授权登录方式运维未授权过的主机而产生的临时规则进行授权与否的操作。

未授权审核指对未授权的主机-用户关系进行授权审核。对主机-用户关系进行授权相当于创建一条固定的运维规则，授权后用户在运维该主机时无需输入主机信息。

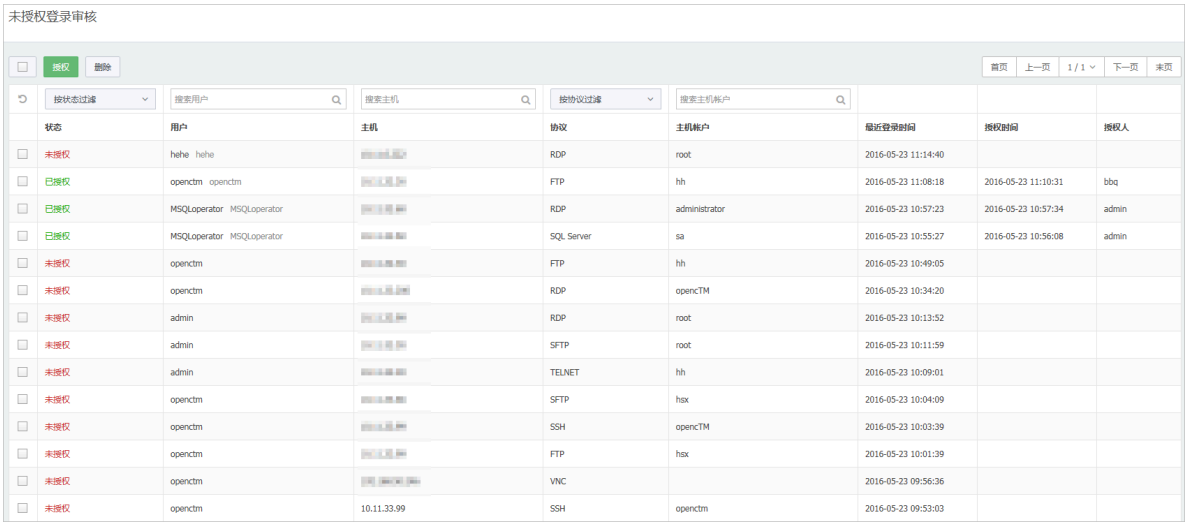
> 说明:
> 此功能需要在系统配置 > 运维配置页面中设置收集未授权登录。

授权审核条目

授权审核指对未授权登录的用户-主机关系进行审核，决定授权与否。

参照以下步骤进行授权审核操作：

1. 进入授权 > 授权审核页。
2. 勾选相应未授权条目，单击授权。



删除审核条目

参照以下步骤删除审核条目：

1. 进入授权 > 授权审核页。
2. 勾选要删除的条目，单击删除。

搜索审核条目

参照以下步骤搜索审核条目：

1. 进入授权 > 授权审核页。

2. 在搜索框中输入主机名、用户名或主机账户进行模糊搜索。您也可以根据协议和授权状态过滤列表。

1.6 审计

1.6.1 会话审计

会话审计用于审计运维人员对主机操作过程的会话日志。管理员可通过审计会话定位故障及追溯故障根源。会话支持在线播放以及下载离线播放两种查看方式。

审计用于审计运维人员对主机的访问操作日志，多角度记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。会话审计专注于事后审计，主要用于对已经结束的会话进行录像回放或命令检索。

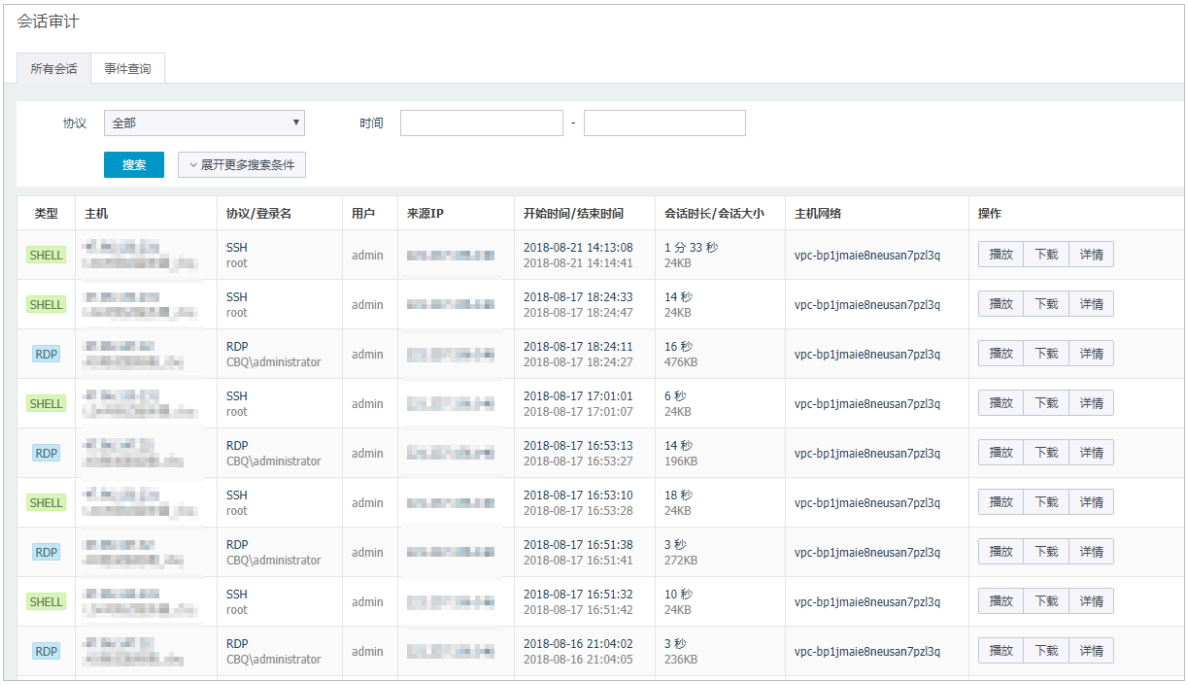
会话审计支持通过时间段、主机网络、来源IP、协议类型等条件进行筛选，还支持通过曾经执行过的命令进行全局检索，并自动跳转到执行这条命令的会话和时间段进行回放。

查看所有会话

参照以下步骤查看会话：

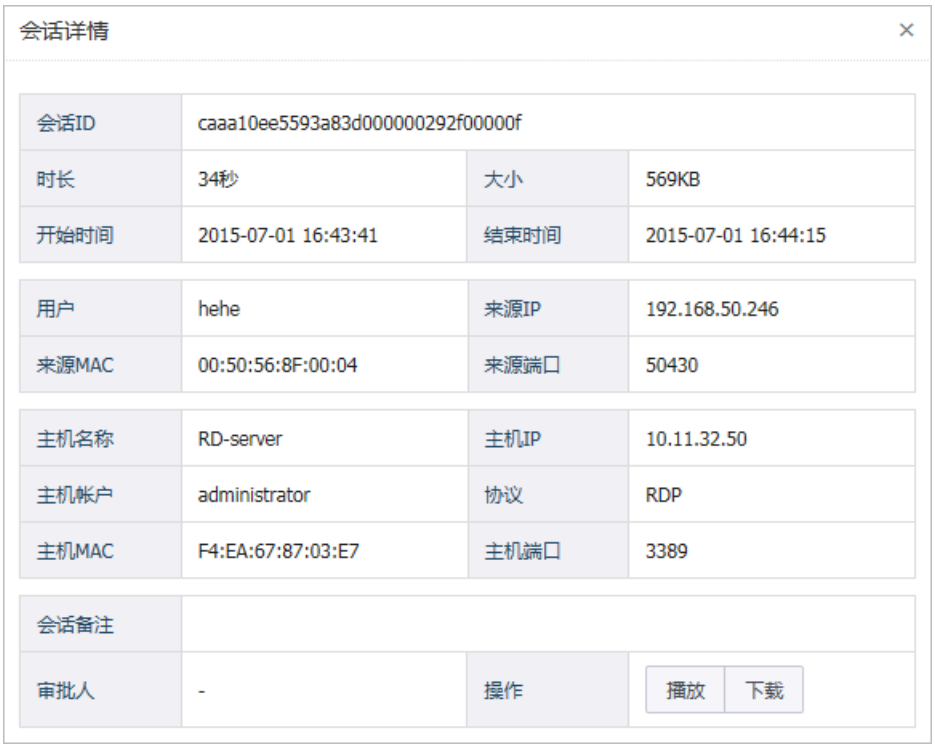
1. 进入审计 > 会话审计页。

在会话审计页可以查看字符、图形、文件、应用类型的会话审计日志。



2. 在会话审计页，单击详情后弹出相应会话详情。

   在会话详情页可以查看到详细的会话信息。



3. 单击关闭即可返回管理页面。
4. 在会话审计页，单击下载可下载会话文件，并通过离线播放器查看。

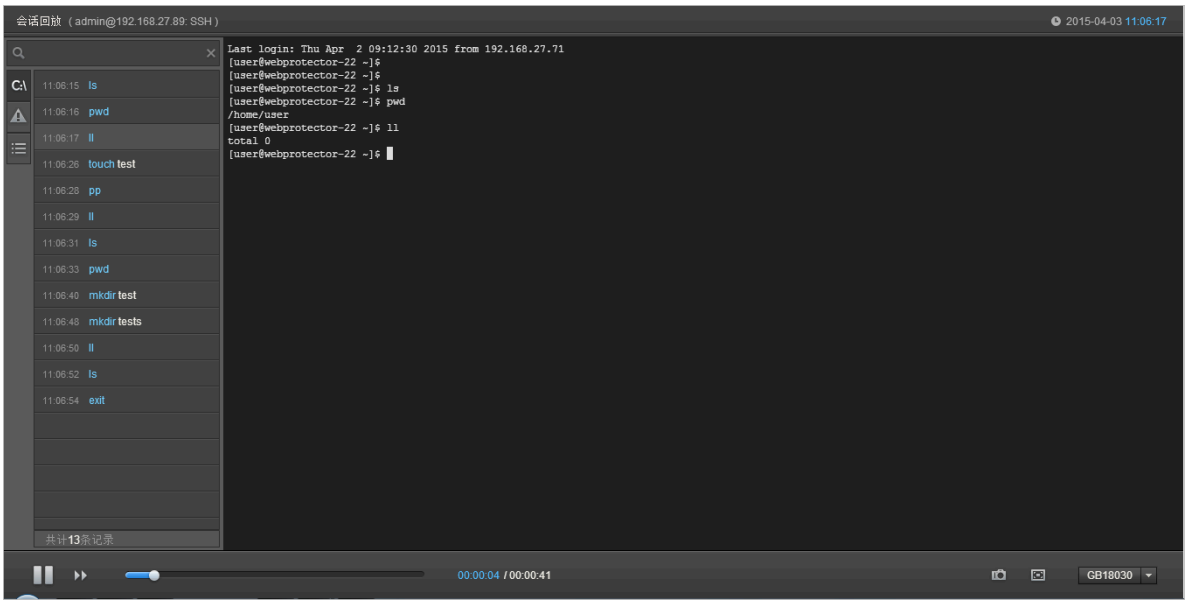
   说明:

   关于离线播放器，请在工具下载页面中下载并安装至本地。具体操作请参考工具下载。

5. 在会话审计页面，单击播放即可通过web方式查看会话审计。可以查看日志回放、命令记录、搜索等。

   说明:

要使用Web方式查看会话审计，则必须在本地安装Flash Player。如果未安装Flash Player，请在工具下载页面中下载并安装至本地。具体操作请参考工具下载。



6. 查看完成后，关闭Web页面。

搜索审计会话

参照以下步骤搜索审计会话：

1. 进入审计 > 会话审计 > 所有会话页。
2. 单击展开更多搜索条件，并使用组合条件搜索要查看的审计会话。

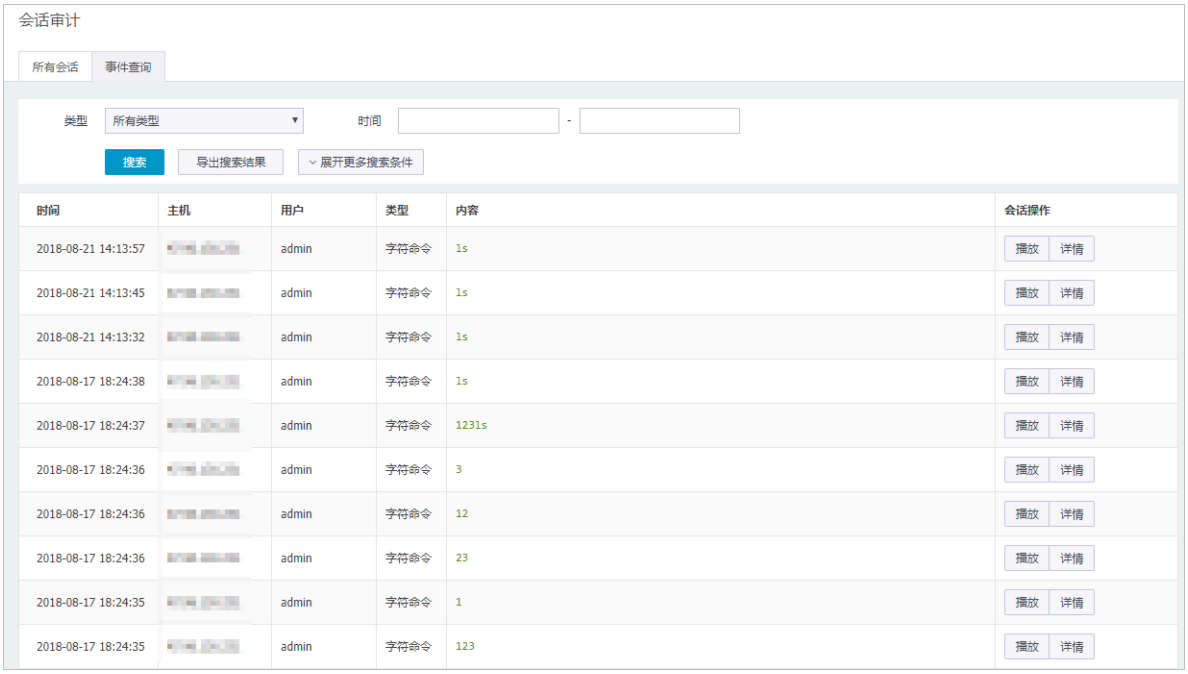
3. 单击搜索查看结果。

事件查询

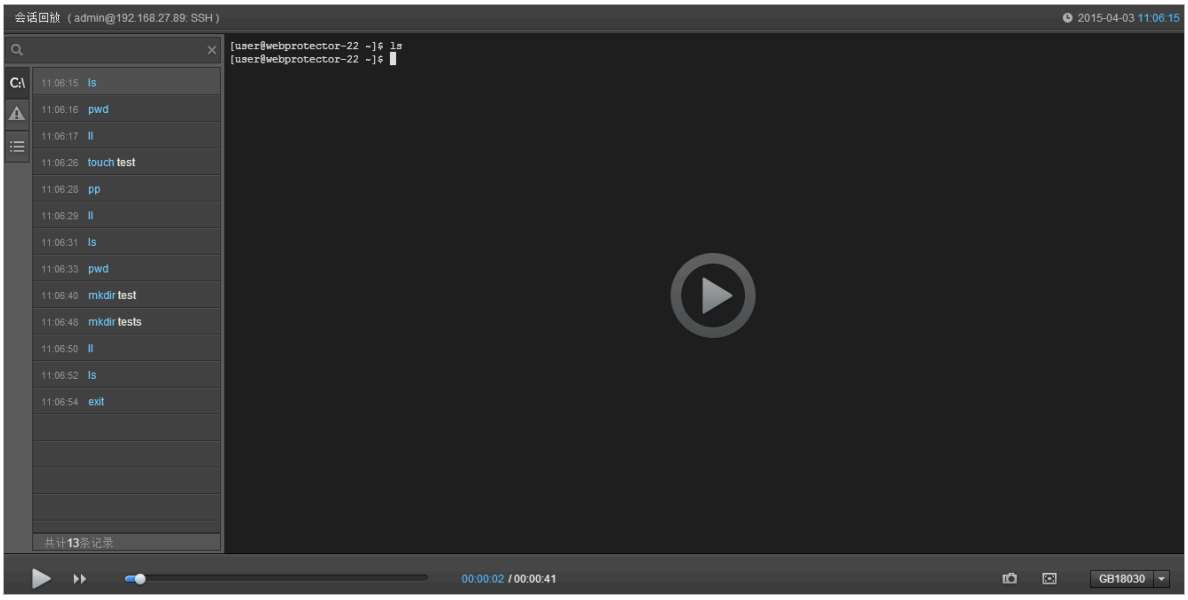
事件查询用于通过曾经执行过的命令进行全局检索，并自动跳转到这条命令的会话和时间段进行播放。

参照以下步骤查询事件：

1. 进入审计 > 会话审计 > 事件查询页。



2. 单击详情，在弹出窗口中查看会话的详细信息。
3. 单击播放即可通过web方式播放会话审计。



4. 查看完成后，关闭Web页面。

搜索事件

参照以下步骤搜索事件：

1. 进入审计 > 会话审计 > 事件查询页。
2. 单击展开更多搜索条件，使用组合条件进行搜索。

导出搜索结果

参照以下步骤导出搜索结果：

1. 进入审计 > 会话审计 > 事件查询页。
2. 按照条件搜索，然后单击导出搜索结果。
3. 设置起始偏移量和导出总条目数后，单击导出即可将过滤后的搜索结果导出。

1.7 工单

当运维人员需要运维授权关系以外的主机，且管理员并没有开启未授权登录时，运维人员可以通过工单向管理员申请运维这些资产。管理员批准工单后系统将自动创建工单中的授权关系。

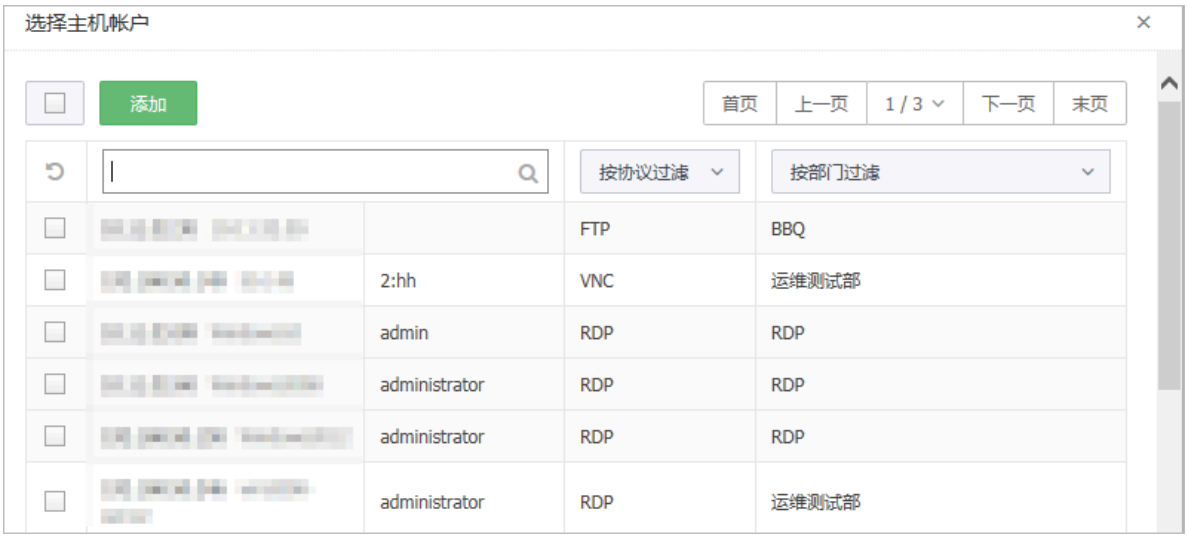
新建工单

运维人员可以参照以下步骤新建工单申请运维资产：

1. 进入工单 > 我的工单页。

2. 单击新建工单进入新建工单页面。填写授权有效期以及备注（可选）。

3. 在新建工单页，单击选择资产，选择并添加主机账户或应用。



4. 添加资产后，在新建工单页单击创建工单。

   在我的工单页会显示新添加的主机，此时工单处于待审批的状态。

工单处于待审批状态时，运维人员想要修改工单信息或者取消工单申请，只需单击工单号或工单后的详情即可对工单进行修改；勾选相应的工单条目，单击取消即可取消工单申请。

> 说明：
> 已审批的工单不能取消或修改。

工单审批

仅管理员具有工单审批权限。运维人员申请工单后，管理员需要对工单进行审批。

管理员可参照以下步骤进行审批操作：

1. 进入工单 > 工单审批页。

2. （可选）勾选工单申请条目，单击批准，通过审批。

> 说明：
> 工单处于待审批状态时，管理员可单击工单号或工单后的详情对运维人员申请的工单进行修改。

   审批通过后，申请人可以在运维界面登录申请的主机。

3. （可选）勾选工单申请条目，单击拒绝，不予批准工单。

1.8 运维

1.8.1 工具下载

工具下载用于运维人员在登录主机前下载需要用到的运维工具以及管理员下载审计需要用到的工具。

下载单点登录器

说明:

在使用Web方式调用运维客户端工具时，必须安装单点登录器。

参照以下步骤下载单点登录器：

1. 在页面右上方的用户菜单下，选择工具下载。
2. 在工具下载页，下载单点登录器，并安装到本地。

下载离线播放器与Adobe AIR

离线播放器与Adobe ATR用于离线查看会话审计中导出的日志。

参照以下步骤下载离线播放器和Adobe AIR：

1. 前往运维 > 工具下载页。
2. 在工具下载页，下载离线播放器和Adobe ATR，并安装在本地。

下载Flash Player

Flash Player用于通过Web方式查看会话审计的日志。

参照以下步骤下载Flash Player：

1. 前往运维 > 工具下载页。
2. 在工具下载页，下载Flash Player，并安装在本地。

下载Chrome

参照以下步骤，下载Chrome：

1. 前往运维 > 工具下载页。
2. 在工具下载页，下载Chrome浏览器，并安装在本地。

下载字符客户端

字符客户端工具用于连接SSH、Telnet协议的主机。

参照以下步骤下载字符客户端：

1. 前往运维 > 工具下载页。
2. 在工具下载页，下载支持SSH和Telnet协议的客户端工具，并安装在本地。

下载图形客户端

图形客户端工具用于连接Windows服务器、VNC服务器。

参照以下步骤下载图形客户端：

1. 前往运维 > 工具下载页。
2. 在工具下载页，下载支持RDP和VNC协议的客户端工具，并安装在本地。

下载文件传输客户端

文件传输客户端工具用于连接SFTP/FTP服务器。

参照以下步骤下载文件传输客户端：

1. 前往运维 > 工具下载页。
2. 在工具下载页面，下载支持SFTP和FTP协议的客户端工具，并安装在本地。

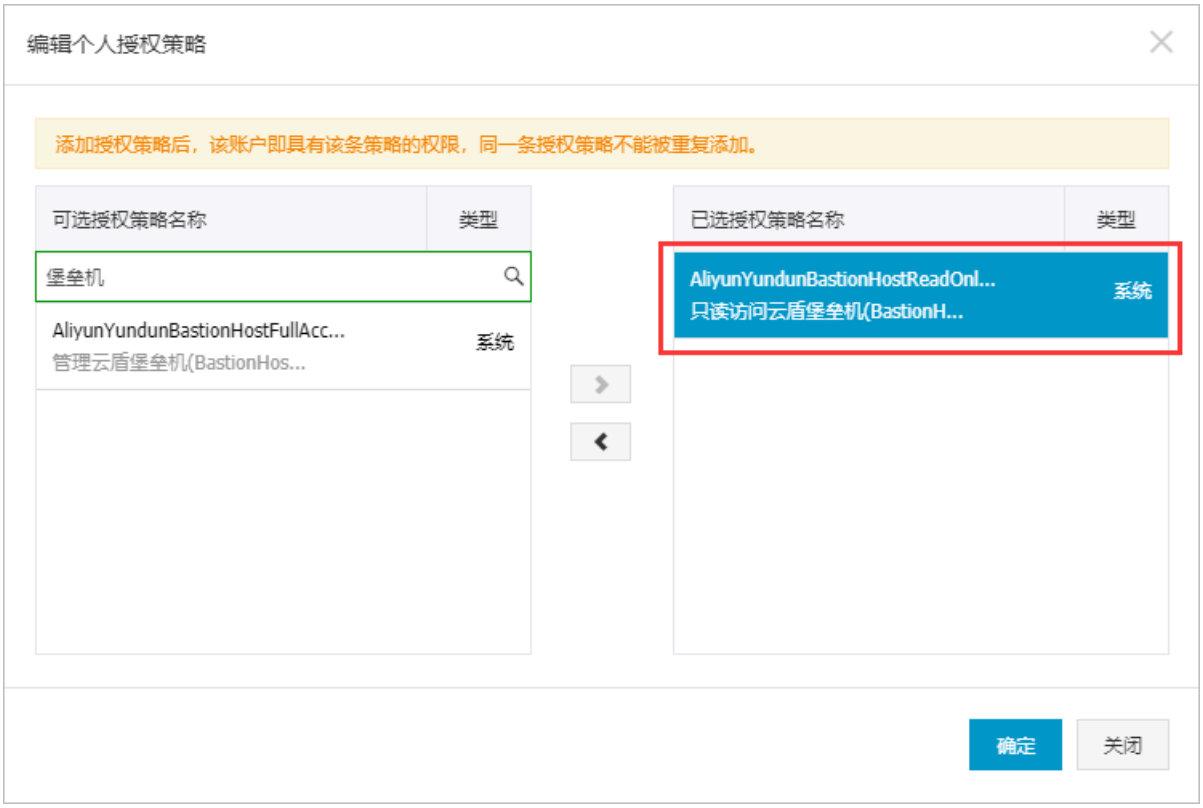
1.8.2 BS运维操作

BS运维指普通运维用户以RAM子账号身份登录堡垒机控制台并进入Web运维界面，调用本地客户端，单点登录ECS进行运维。该运维方式仅支持RAM子账号用户以及主账号使用，可以在Windows和MAC环境下使用。

与BS运维方式相对的CS运维，指运维人员通过本地客户端工具登录云盾堡垒机，访问目标服务器主机进行运维操作。本文主要介绍BS运维的操作方法。

RAM子账号登录

在进行BS运维前，请根据需求设置好RAM子账号权限。您可以使用主账号登录访问控制RAM-用户管理，给需要运维的RAM子账号授权。建议赋予子账号只读权限，只允许使用运维，避免子账号进入管理页面，发生越权操作。



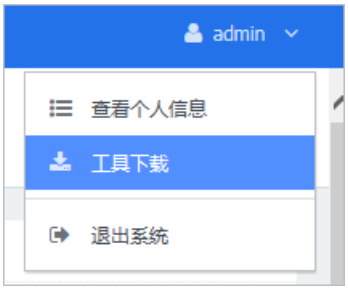
参照以下步骤使用RAM子账号登录运维页面：

1. **通过RAM子账号登录界面，登录云盾堡垒机控制台。**
2. **选择要操作的实例，单击运维，进入Web运维界面。**

配置单点登录

参照以下步骤配置单点登录：

1. **在系统页面的右上角单击用户名，在下拉菜单中单击工具下载。**



2. 在工具下载页面，选择下载单点登录器。

3. 安装单点登录器到本地。

4. 配置各协议的单点登录所用客户端。

5. 配置完成后退出。

Web运维配置

参照以下步骤进行Web运维配置：

1. **进入运维 > 主机运维页。**

2. **单击页面右上角的WEB运维配置。**
3. **在RDP子页，设置分辨率、连接模式、本地设备和资源、本地驱动器后，单击保存。**

说明:

本地驱动器只需勾选要映射的盘符即可。请勿勾选全部盘符，否则该设置无效。

4. 前往SSH & TELNET & Rlogin页，选择客户端程序、终端类型、编码格式后，单击保存。

5. 前往FTP页，选择对应的客户端程序后，单击保存。

6. 参照步骤5，分别在SFTP和VNC页，设置SFTP和VNC参数。

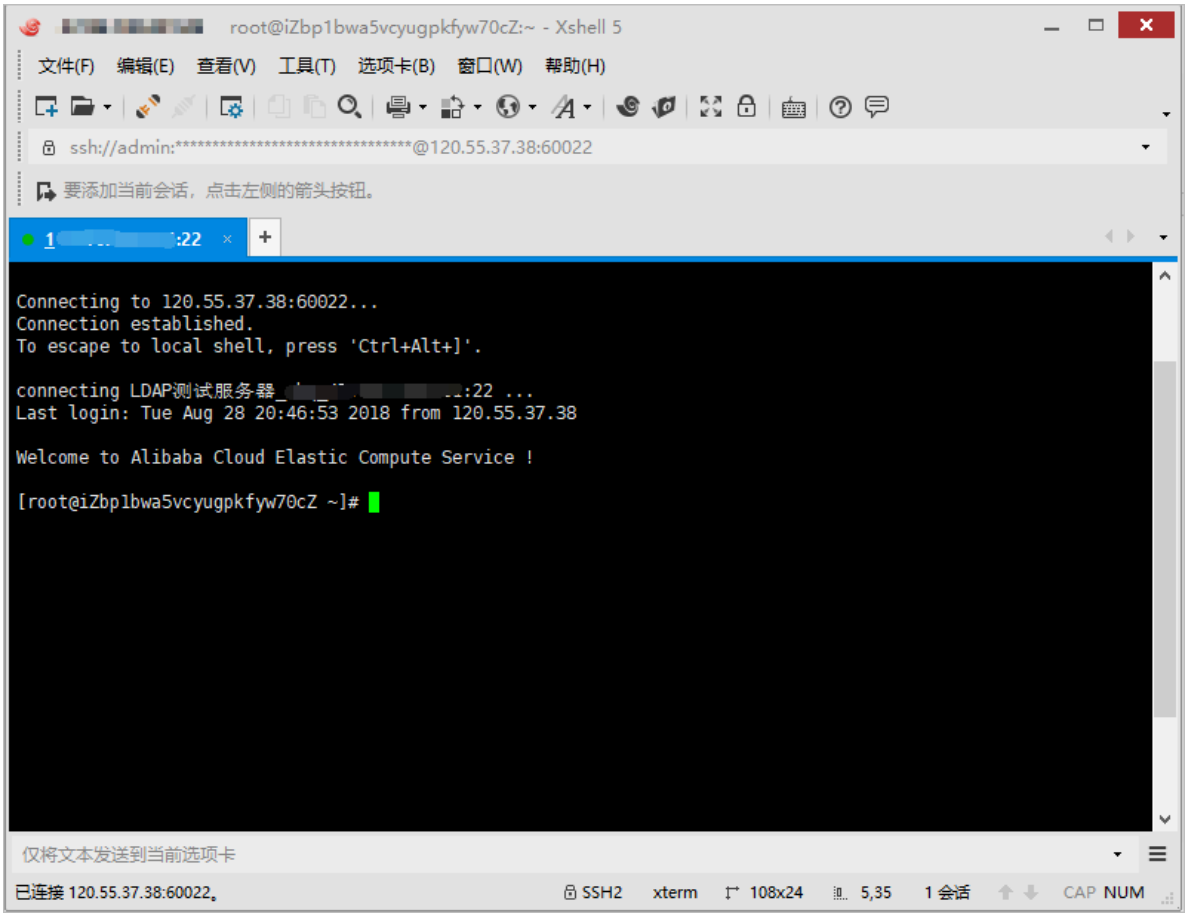
主机登录

在主机运维列表中，单击相应主机条目的登录图标框，会自动弹出配置好的客户端，登录主机进行操作。

以SSH运维为例，参照以下步骤登录主机：

1. 进入运维 > 主机运维页。
2. 在主机运维列表中，选择需要登录的服务器，单击右侧登录图标框，自动调用所配置的SSH客户端。

3. 自动登入服务器，进行运维操作。



快速运维

通过快速运维可快速找到最近多次登录的目标主机进行运维。快速运维主要用于需要频繁登录某些主机账户进行运维的场景。

参照以下步骤进行快速运维：

1. 进入运维 > 主机运维页。
2. 单击搜索框，将自动显示最近运维的主机账户。在搜索框中输入主机IP/主机名/账户名、或关键信息，系统会自动过滤出与目标主机有关的信息。

3. 单击需要登录的目标主机及帐户后，即可成功登录。

搜索主机

参照以下步骤搜索主机：

1. 进入运维 > 主机运维页。
2. 在搜索框中输入主机名称或主机IP实现模糊搜索。您也可以通过主机协议过滤列表。

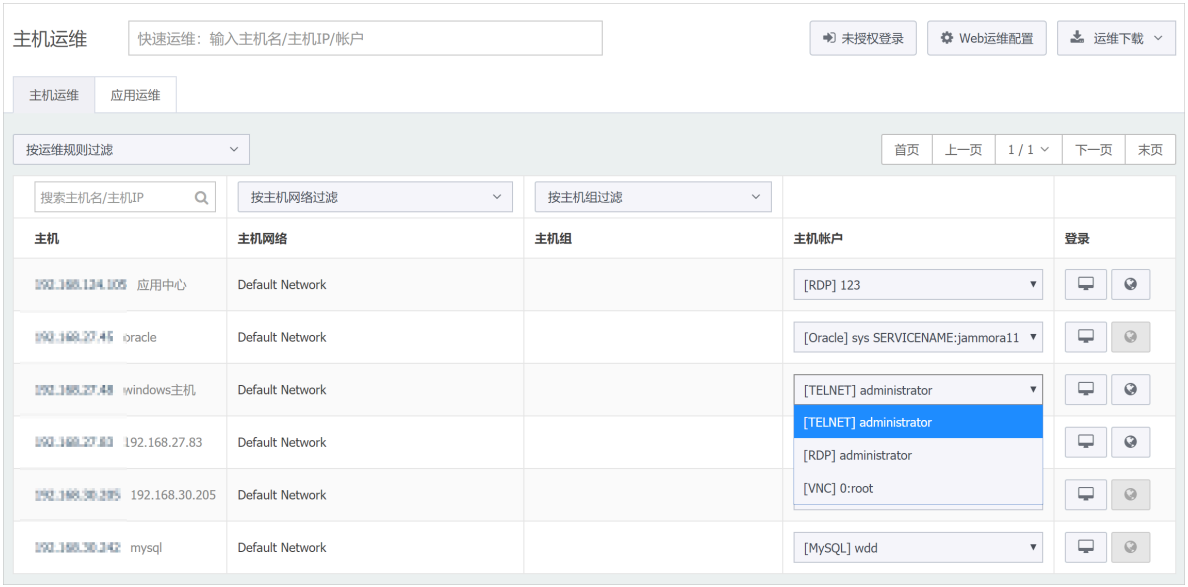
合并重复IP

主机运维中的重复IP合并将相同主机IP地址的不同主机账户全部整合在相应主机IP地址下，方便查看。

参照以下步骤合并重复IP：

1. 进入运维 > 主机运维页。

2. 单击主机IP地址对应的主机账户即可查看。



1.8.3 未授权登录

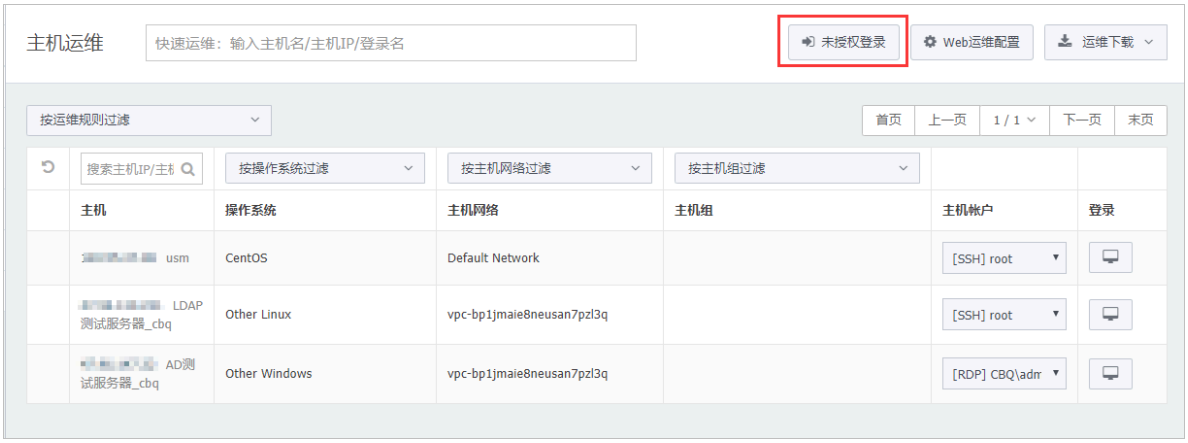
当运维人员想访问某主机并且知道该主机的IP、账户和密码，但该主机没有被授权，没有在运维列表中显示。这种情况下，运维人员可以使用未授权登录。

前提条件

此功能需要在系统 > 系统配置 > 运维配置中勾选允许未授权登录。

操作步骤

1. 进入运维 > 主机运维页。
2. 单击未授权登录。



3. 在登录对话框中输入主机IP、端口、协议、登录名、密码，选择登录方式，即可登录。

1.8.4 实时监控

实时监控专注于事中控制，可以通过堡垒机管理平台随时切入某个运维会话查看现场操作，管理正在运维主机的会话，进行命令审批或会话阻断等操作。

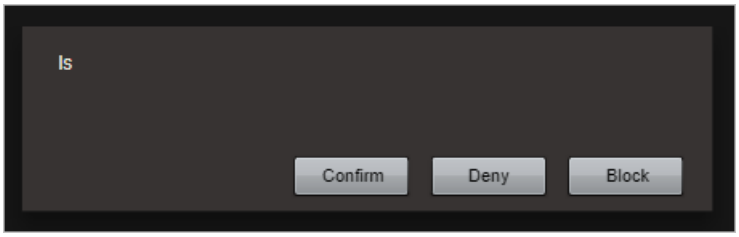
命令审批

参照以下步骤进行命令审批：

1. 管理员登录系统后，进入运维 > 实时监控页。

   所有会话显示了正在运维的会话，需要命令审批显示了需要进行命令审批的会话。

2. 前往需要命令审批页，单击会话条目右侧的播放，进入运维窗口监控页面，可以实时查看运维会话的操作情况。
3. 如果有命令需要审批，监控页面会弹出命令审批对话框，根据实际需求进行处理。



阻断会话

管理员对会话进行阻断操作后，将会断开客户端与主机之间的连接，运维员不能再进行运维操作。

参照以下步骤阻断会话：

1. 进入运维 > 实时监控页。
2. 勾选要阻断的会话，单击阻断会话。

1.8.5 命令审批

当运维员有命令需要审批时，审批人可以在运维 > 命令审批页进行审批操作。

背景信息

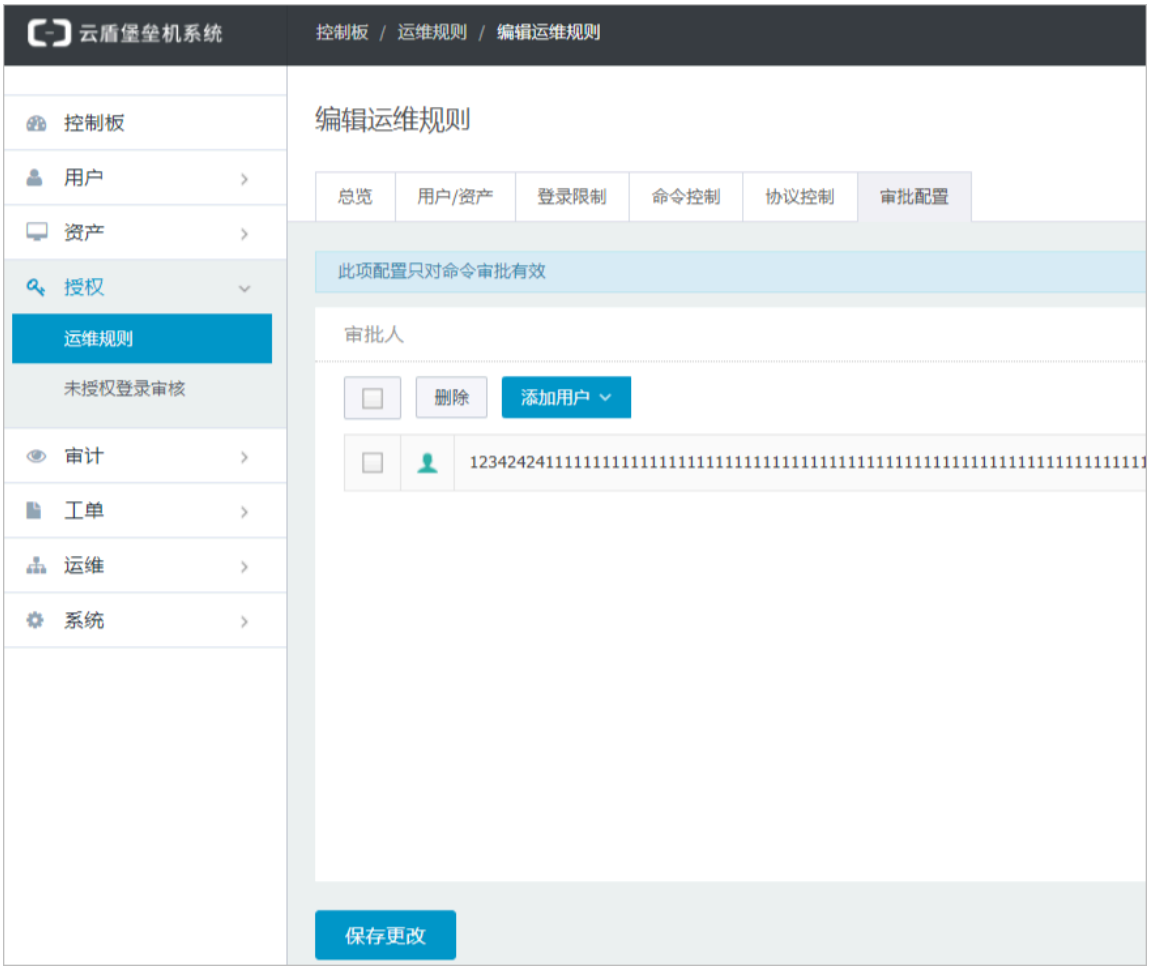
命令审批主要用于某些运维员需要有命令审批权限的场景。可参照以下步骤进行操作。

操作步骤

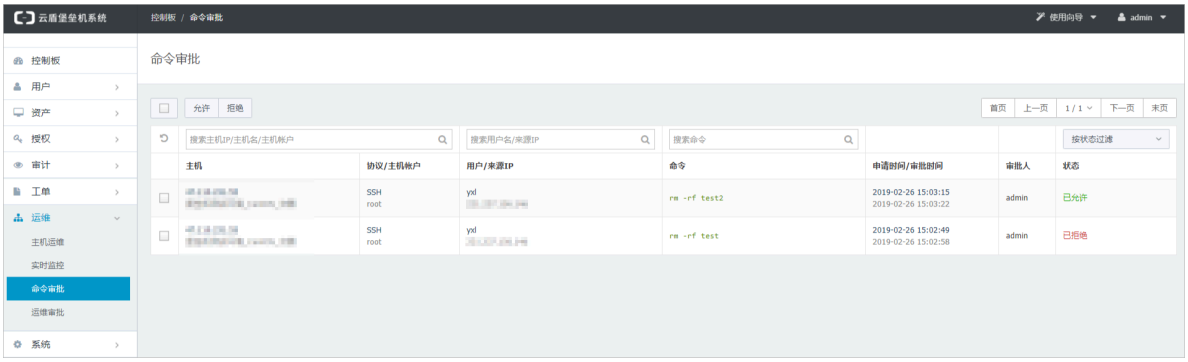
1. 审批配置。管理员在进行授权运维规则时应事先设置命令审批人。

   a) 前往授权 > 运维规则 > 审批配置页。

   b) 单击添加用户，设置审批人并保存。



2. 命令审批。运维员进行运维时，若输入了需要审批的命令，审批人可前往运维 > 命令审批页进行审批。



1.8.6 运维审批

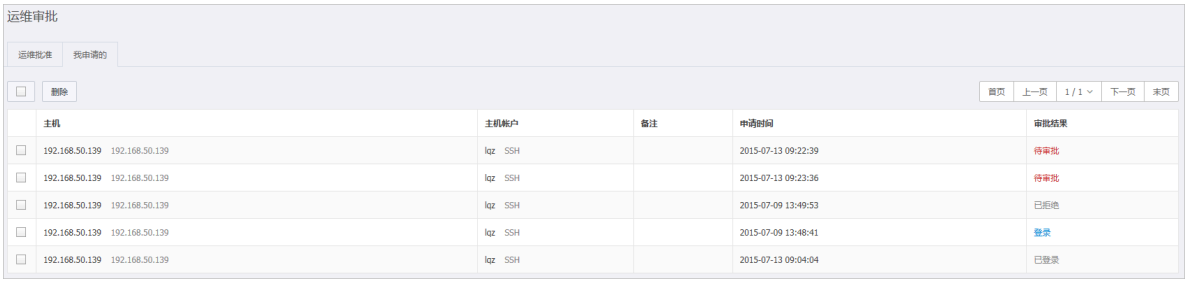
维审批即二次审批，对于设置了二次审批的主机，即使经过授权，运维人员也不能直接登录成功，系统会自动生成运维申请，必须由管理员审批通过之后，才能进行运维。

操作步骤

1. 设置二次审批。管理员前往资产 > 主机管理页，单击需要设置的主机，在配置界面中勾选开启会话二次审批并保存。

运维人员在运维页面登录设置过二次审批的主机时，系统会提示“运维申请已创建，等待批准”。

2. 运维申请。运维人员前往运维 > 运维审批 > 我申请的页面查看到主机的审批情况。



说明:

对于已批准的运维申请，对应主机会显示登录字样，单击该字样，可以运维对应的主机。

3. 运维批准。管理员在运维 > 运维审批 > 我申请的 > 运维批准页面查看运维人员的运维申请，勾选相应的运维申请条目，并单击批准，在弹出的运维审批对话框中填写审批有效期，即可完成运维批准。

1.9 系统

1.9.1 认证管理

您可以在认证管理下设置安全配置、远程认证、和双因子认证。

安全配置

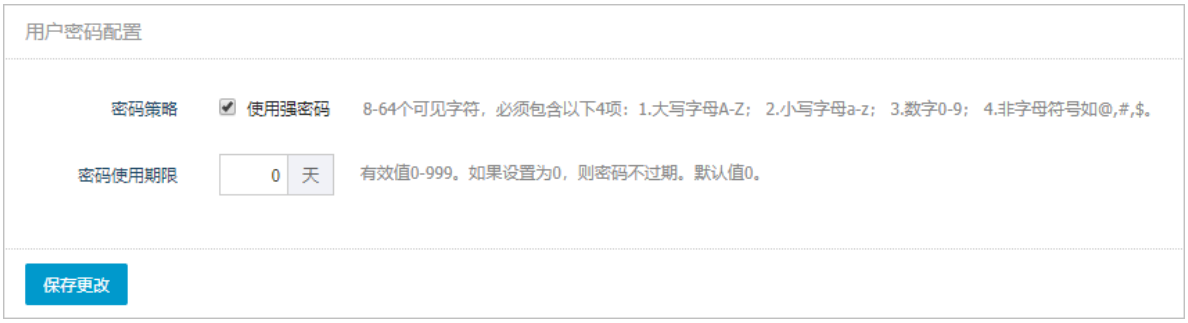
参照以下步骤进行安全配置：

1. 进入系统 > 认证管理 > 安全配置页。

2. 在登录配置下，编辑登录超时时间以及验证码过期时间，完成后单击保存更改。

3. 在用户锁定下，编辑尝试密码次数、锁定时长、重置计数器时长，完成后单击保存更改。

4. 在用户密码配置下，配置是否使用强密码和密码使用期限，完成后单击保存更改。



远程认证

当设置认证状态为关闭时，相应认证类型的用户便无法登录堡垒机。

通过设置本地认证状态来控制本地用户是否可以登录堡垒机。

云盾堡垒机与AD/LDAP服务器对接，可将AD/LDAP服务器用户同步进堡垒机，作为堡垒机用户使用。 此功能需具有部署好的AD/LDAP环境，且保证堡垒机至服务器网络可达。

参照以下步骤配置远程认证：

1. 进入系统 > 认证管理 > 远程认证页。
2. 启用远程认证，选择认证方式，并完成相关配置。
3. （可选）选择AD域认证模式。

   a. 填写服务器地址、端口号、Base DN、域名，填写一个AD服务器中的账户和密码。

   b. 单击测试连接，测试与服务器的联通性及该账户是否可用。

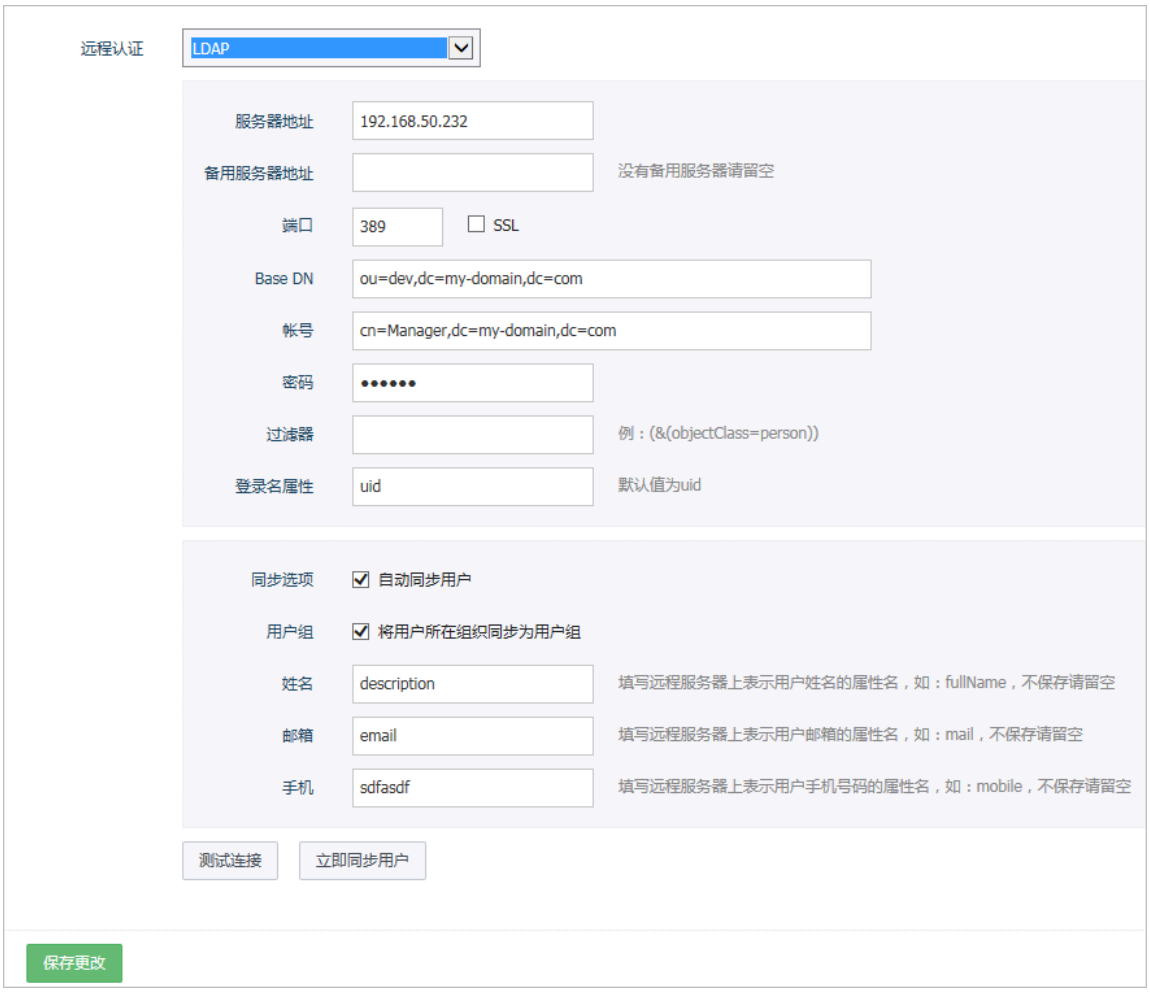
   c. 同步AD用户，单击立即同步用户或勾选自动同步用户。

> **说明:**
> 自动同步周期为30分钟。

   d. 单击保存更改。

4. 选择LDAP认证模式。

   a. 填写服务器地址、端口号、Base DN、域名，填写一个LDAP服务器中的账户和密码。



   b. 单击测试连接，测试与服务器的联通性及该账户是否可用。

   c. 同步LDAP用户，单击立即同步用户或勾选自动同步用户。

> **说明:**
> 自动同步周期为30分钟。

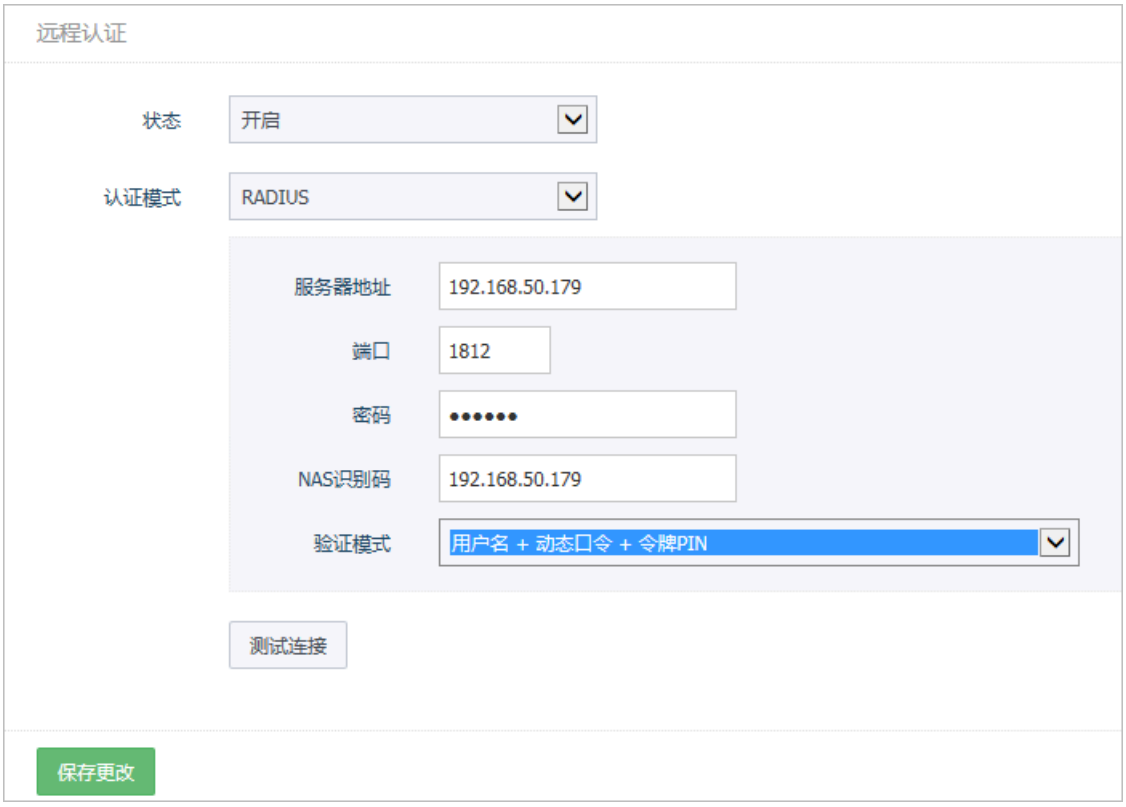
   d. 单击保存更改。

5. 选择RADIUS认证模式。

   a. 输入远程RADIUS服务器的IP地址、服务端口号、服务器密码、NAS识别码，选择验证模式。

> **说明:**

RADIUS验证模式有三种：选择用户名和密码时，使用用户名和密码验证；选择用户名和动态口令时，可以使用用户名、密码或者动态口令验证；选择用户名、令牌PIN和动态口令时，可以使用用户名、密码验证，也可以使用用户名、令牌PIN和动态口令验证。



b. 单击测试连接测试与服务器连通性。

c. 同步LDAP用户，单击立即同步用户或勾选自动同步用户。

说明:
自动同步周期为30分钟。

d. 单击保存更改。

双因子认证

引入双因子认证机制，通过短信认证、动态令牌等技术，控制账号密码泄露风险，防止运维人员身份冒用和复用。开启双因子认证之后，运维人员登录堡垒机时，需要先输入用户密码，密码验证正确之后，需要输入动态口令/短信口令才能登录成功。

参照以下步骤配置双因子认证：

1. 管理员通过云盾堡垒机控制台登录堡垒机。
2. 进入系统 > 认证管理 > 双因子认证页。

3. 按需勾选要启用的认证方式：密码、短信口令。

> **说明:**
> 当勾选了密码时，将优先采用密码认证方式。运维人员登录堡垒机时输入用户密码即可登录成功。仅勾选短信口令未勾选密码时，运维人员登录堡垒机时，需要先输入用户密码，密码验证正确之后，需要输入短信口令才能登录成功。

4. 单击保存更改。

1.9.2 系统配置

您可以在系统配置中设置运维配置、告警配置、和界面语言。

运维配置

运维配置包括未授权登录，运维登录和运维时长限制配置。

- 运维授权配置主要是对未授权登录进行相关配置，若允许未授权登录，则运维人员可以在运维页面通过未授权登录运维自身授权关系以外的资产。
- 运维登录指允许用户使用堡垒账户登录主机，主要适用于用户和账户同属于AD/LDAP的场景。
- 运维时长限制指当协议连接上的空闲时长限制，超过该限制时，网络连接会自动断开。

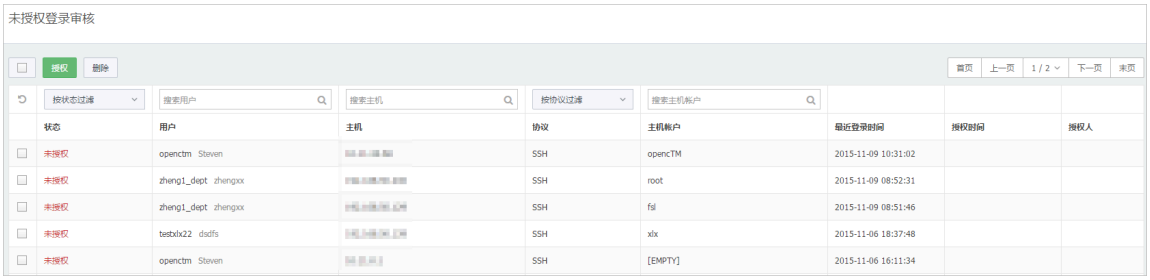
操作步骤

参照以下步骤进行运维配置：

1. 进入系统 > 配置 > 运维配置页。

2. 在未授权登录下，勾选并应用相关选项。

- 允许未授权登录：运维人员可以在运维页面通过未授权登录运维自身授权关系以外的资产。
- 收集授权关系：用户进行未授权登录后，系统会自动收集用户和主机的授权对应关系，并支持在未授权登录审核页面查看。



- 收集主机账户和密码：用户进行未授权登录后，系统会自动收集用户所登录主机的账户和密码。
- 自动授权：系统检测到未授权登录的事件发生后，会自动创建相应授权关系，不需要管理员进行手动授权。

3. 在运维登录下，勾选并应用相关选项。

   - 允许使用用户密码登录主机：允许用户使用堡垒账户登录主机。勾选此项后，在运维界面的账户列表中会有相关项。如下图所示，选用[SYSDEF][SELF]账户，即可使用堡垒账户登录主机。主要适用于用户和账户同属于AD/LDAP的场景。

   - 允许使用SSH私钥登录主机：勾选此项后，堡垒将允许用户无需输入主机账户的密码，使用已经添加过的SSH私钥登录主机运维。
   - 允许使用SSH-agent-forwarding方式登录SSH服务器：勾选此项后，堡垒将支持SSH-agent-forwarding 特性，适用于登录堡垒机和登录SSH服务器使用同样私钥的场景。

4. 在SSH登录下，勾选并应用相关选项。

   - 允许使用公钥登录：勾选此项后，用户可以使用SSH公钥登录运维审计系统。
   - 允许使用密码登录：勾选此项后，用户将通过密码登录运维审计系统。
   - 允许发送环境变量：勾选此项后，用户可以选择允许发送运维用户信息和运维来源IP。
   - Usmshell使用命令行方式：勾选此项后，将通过命令行方式登录堡垒主机。

5. 在运维时长限制下，设置时长限制。当协议连接上的空闲时长超过此限制，网络连接会自动断开。

   说明:

   各协议空闲时长定义如下：

   - rdp、vnc：客户端无数据发送时。
   - ftp：命令通道和数据通道均无数据发送时。
   - ssh、telnet、sftp、mysql、sqlserver、oracle：客户端和服务端均无数据发送时。

告警配置

参照以下步骤进行告警配置：

1. 进入系统 > 系统配置 > 告警配置页。

2. 邮件方式告警。

   a. 在邮件配置下，配置邮件的地址、端口、账号、密码、收件人邮箱。

   b. 单击发送测试邮件测试邮件配置成功后，单击保存更改。

3. Syslog方式告警。

   a. 在Syslog配置下，配置发送标识、服务器IP、端口。

   b. 单击发送测试数据测试已连通后，单击保存更改。

4. 在操作日志告警下，开启告警，根据需要勾选系统邮件告警等级和Syslog告警等级，完成后单击保存更改。

语言设置

参照以下步骤进行语言设置：

1. 进入系统 > 系统配置 > 语言设置页。
2. 选择要使用的界面显示语言，然后单击保存更改。系统支持三种界面显示语言：简体中文、繁体中文和英文。

1.9.3 存储管理

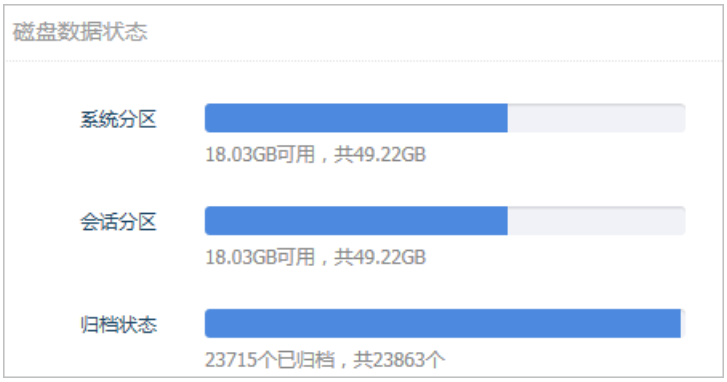
通过存储管理可以查看堡垒机磁盘数据状态和管理堡垒机中的数据信息。

数据归档

参照以下步骤使用数据归档：

1. 进入系统 > 存储管理 > 数据归档页。

2. 在磁盘数据状态下，查看磁盘空间使用量。



3. 在录像归档下，开启或关闭录像归档功能。您可以使用FTP或SFTP方式将归档数据发送到目标服务器。

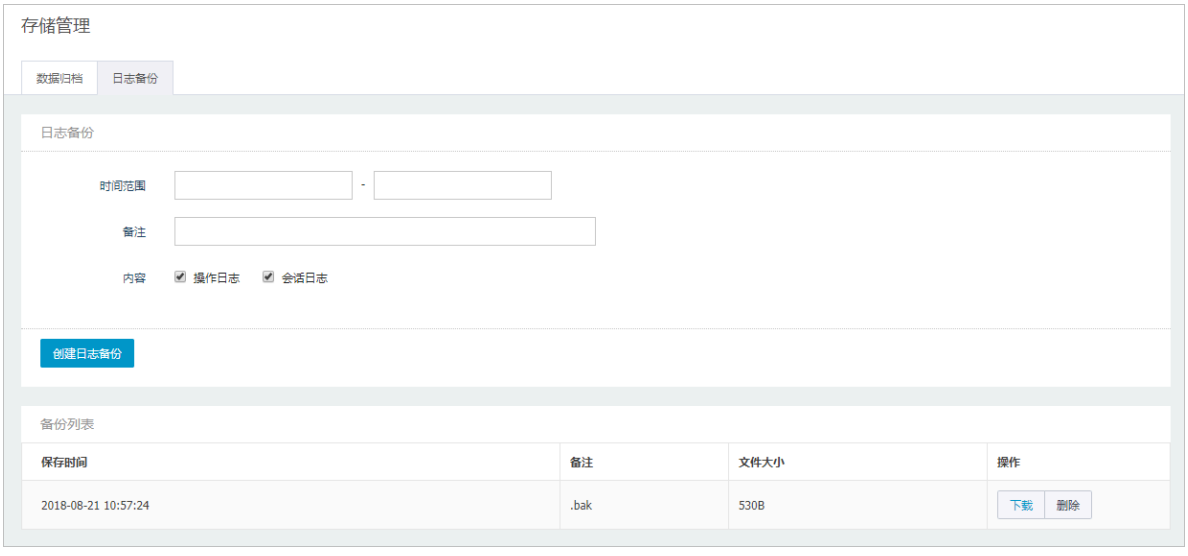
4. （可选）在自动删除下，设置自动删除多少天之前的数据。

5. （可选）在手动删除下，根据数据类型和日期删除不需要的数据。

日志备份

参照以下步骤使用日志备份：

1. 进入系统 > 存储管理 > 日志备份页。
2. 选择时间范围，编辑备注，并选择需要导出的内容（操作日志、会话日志）。



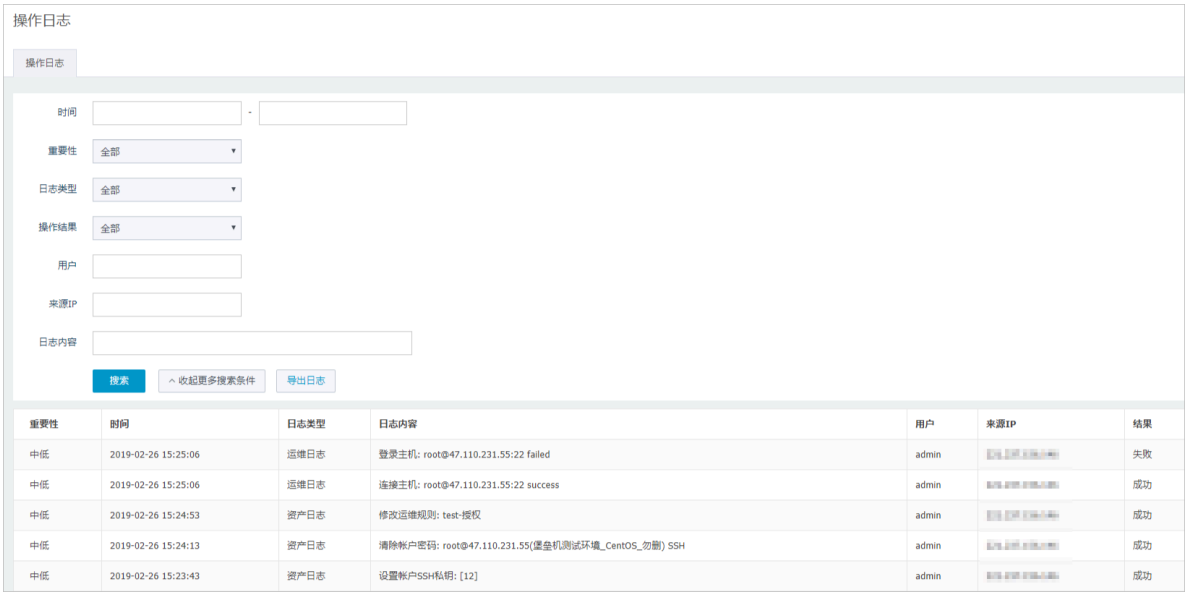
3. 单击创建日志备份即可生成备份文件。
4. （可选）在备份列表单击下载可将文件下载至本地查看。
5. （可选）在备份列表单击删除可将备份文件删除。

1.9.4 操作日志

操作日志是指用户操作、配置云盾堡垒机本身时所产生的日志。您可以在云盾堡垒机Web管理页面查看所有操作日志，或使用多种过滤条件查询特定的日志记录。

操作步骤

1. 进入系统 > 操作日志页。
2. 在操作日志子页，搜索或导出相关日志。



1.9.5 本机维护

您可以在本机维护中设置系统管理、系统备份、系统配置推送和接收、网络诊断工具、以及系统诊断工具。

系统管理

管理员可以在系统管理中设置系统时间。

参照以下步骤进行设置：

1. 进入系统 > 本机维护 > 系统管理页。

2. 在系统时间下，设置时间服务器，开启/关闭自动同步功能。您可以单击同步服务器时间或同步浏览器时间直接同步时间数据。

系统备份

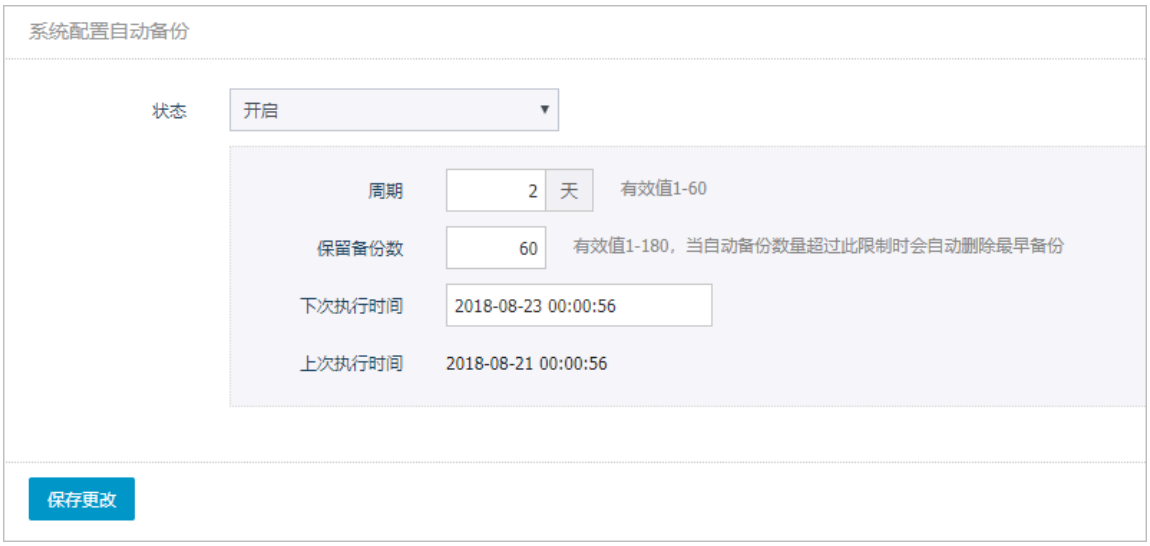
参照以下步骤使用系统备份：

1. 进入系统 > 本机维护 > 系统备份页。

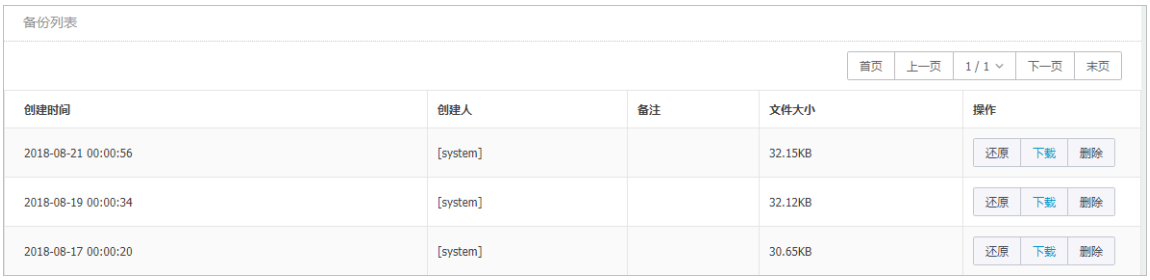
2. 根据需要执行以下操作：

- 在系统备份手动备份下，编辑备注信息，然后单击创建系统配置备份即可在备份列表中新增新增备份信息。

- 在系统备份自动备份下，将状态设置为开启，并填写备份周期和保留备份数，完成后单击保存更改。



- 在备份列表下，选择要操作的备份，单击下载，可下载备份文件至本地。



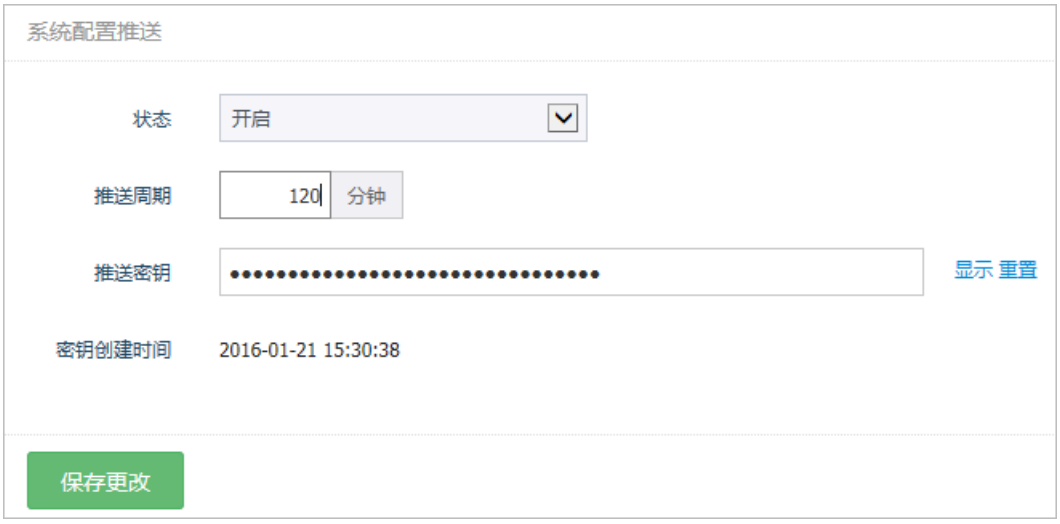
- 在备份列表下，选择要操作的备份，单击还原，可将备份文件恢复还原至系统中。
- 在备份列表下，选择要操作的备份，单击删除，可将备份文件从系统中删除。
- 在系统配置还原下，单击上传系统配置文件，可将系统配置备份的文件恢复还原至系统中。

系统配置推送

开启系统配置推送后，系统将按照设定的推送周期向目标设备推送本设备的系统配置。增加目标设备IP之后，需要在目标设备的系统配置接收选项里填写本设备的推送密钥。

参照以下步骤开启系统配置推送：

1. 进入系统 > 本机维护 > 系统配置推送页。
2. 开启推送功能，并设置推送周期和推送密钥。

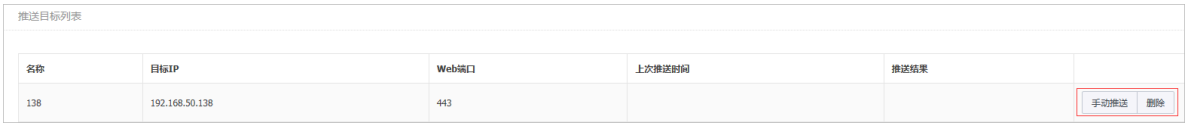


说明：

单击上图的重置可设置推送密钥。在接收设备上设置接收配置时需要提供该推送密钥。

3. 添加推送目标，即接收设备。

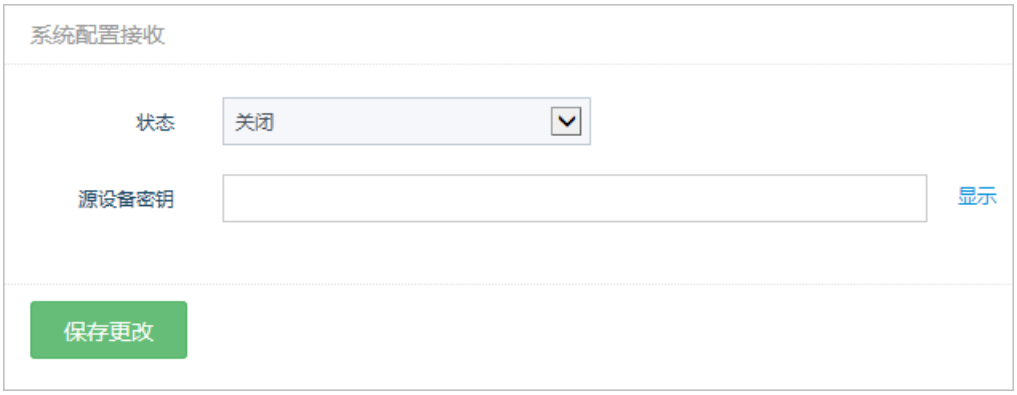
4. 添加完成后，在推送目标列表中可查看所有推送目标，也可以操作手动推送配置和删除推送目标。



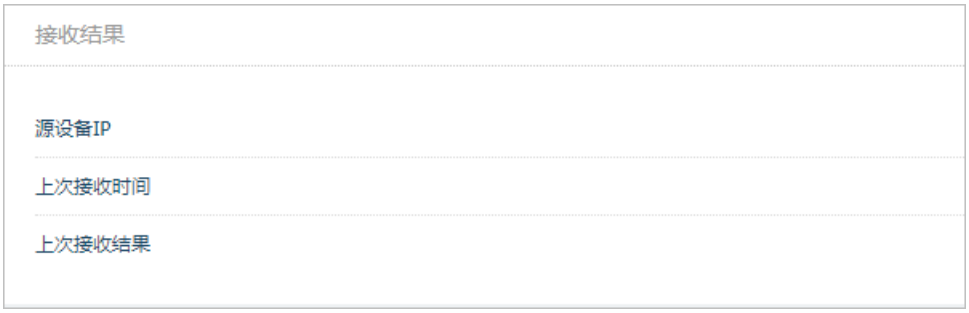
系统配置接收

参照以下步骤查看系统配置接收结果：

1. 在接收设备上设置源设备密钥（即推送设备上设置的密钥），并开启接收功能即可接收推送设备推送的系统配置。



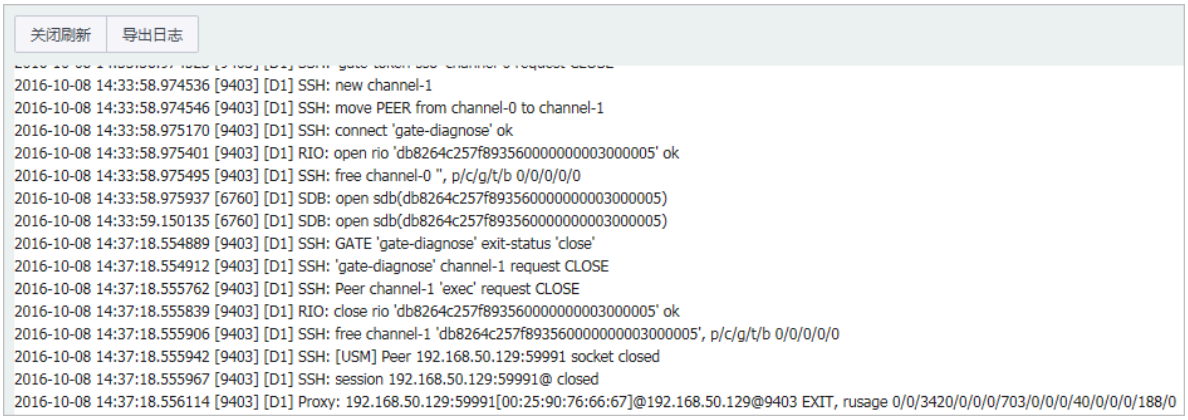
2. 在接收结果页面可看到上次接收的时间、结果等信息。



调试日志

参照以下步骤使用调试日志：

1. 进入系统 > 本机维护 > 调试日志页。



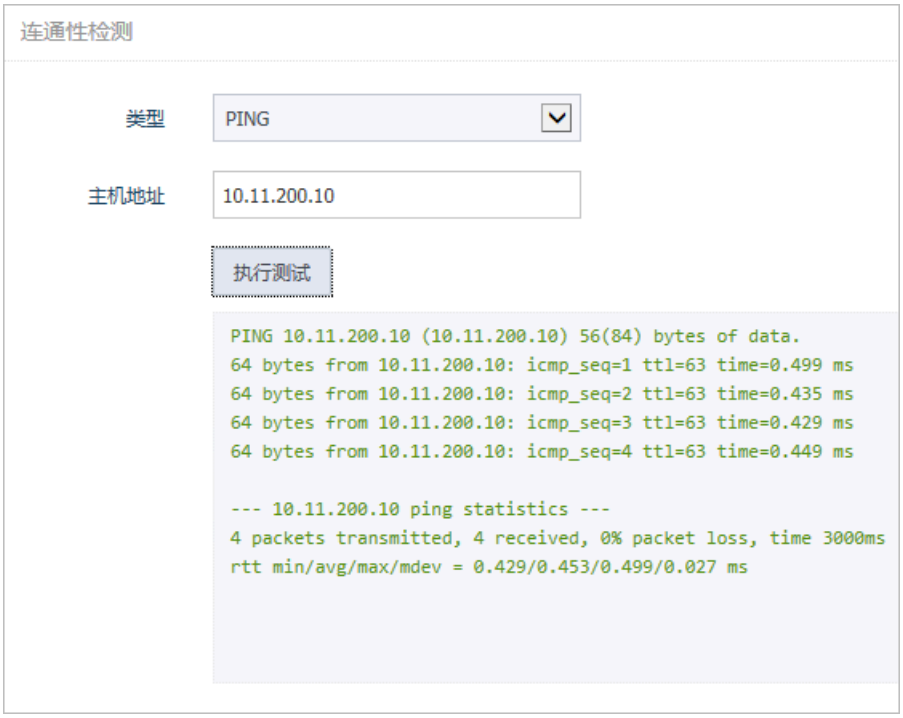
2. 单击关闭刷新可暂停调试日志的更新。
3. 单击导出日志可将调试日志导出查看。

网络诊断

使用网络诊断工具可以检测主机IP、TCP端口、UDP端口是否连通，路由是否可达。

参照以下步骤进行网络诊断：

1. 进入系统 > 系统维护 > 网络诊断页。
2. 在连通性检测下，选择检测类型，并输入主机地址。



说明:

支持检测主机的IP或端口是否连通、路由是否可达、TCP端口、UDP端口。

3. 单击执行测试即可自动检测出主机的ip是否连通。

系统诊断

参照以下步骤进行系统诊断：

1. **进入系统 > 本机维护 > 系统诊断工具页。**
2. **查看系统各设备信息和前十个进程。**

2 运维使用手册

2.1 SSH协议运维

本文受众范围：运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。

运维人员需要通过本地的客户端工具登录云盾堡垒机，再访问目标服务器主机进行运维操作。

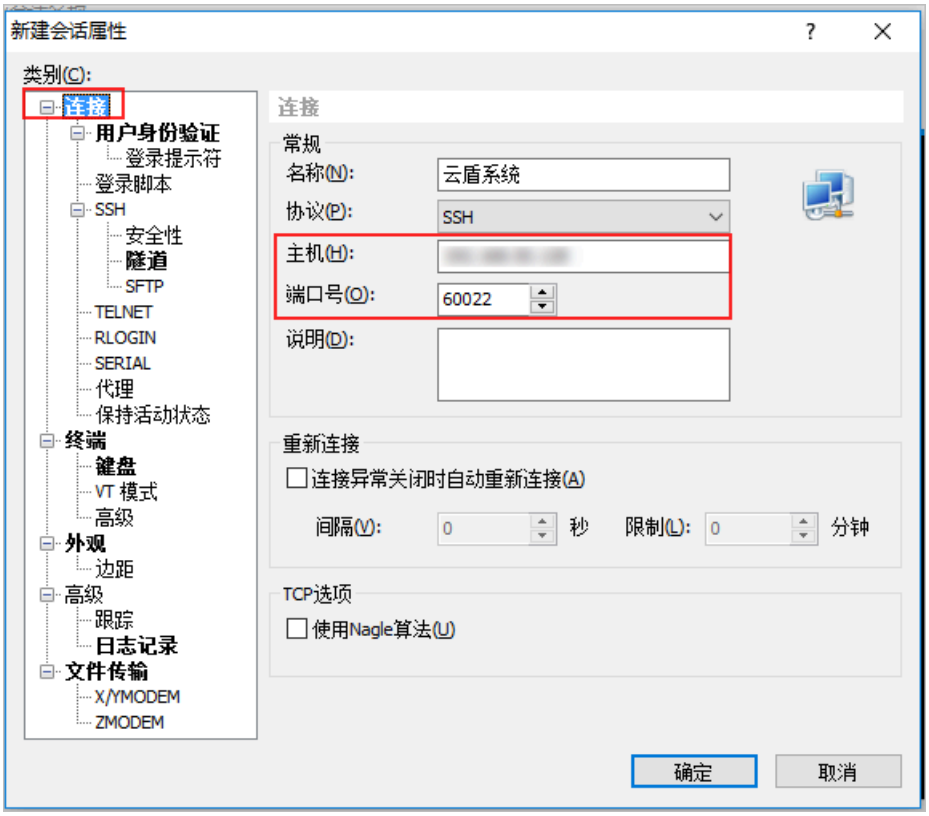
说明:

请确认在本地主机已安装支持 SSH 协议的运维工具，如 Xshell、SecureCRT、PuTTY 等工具。

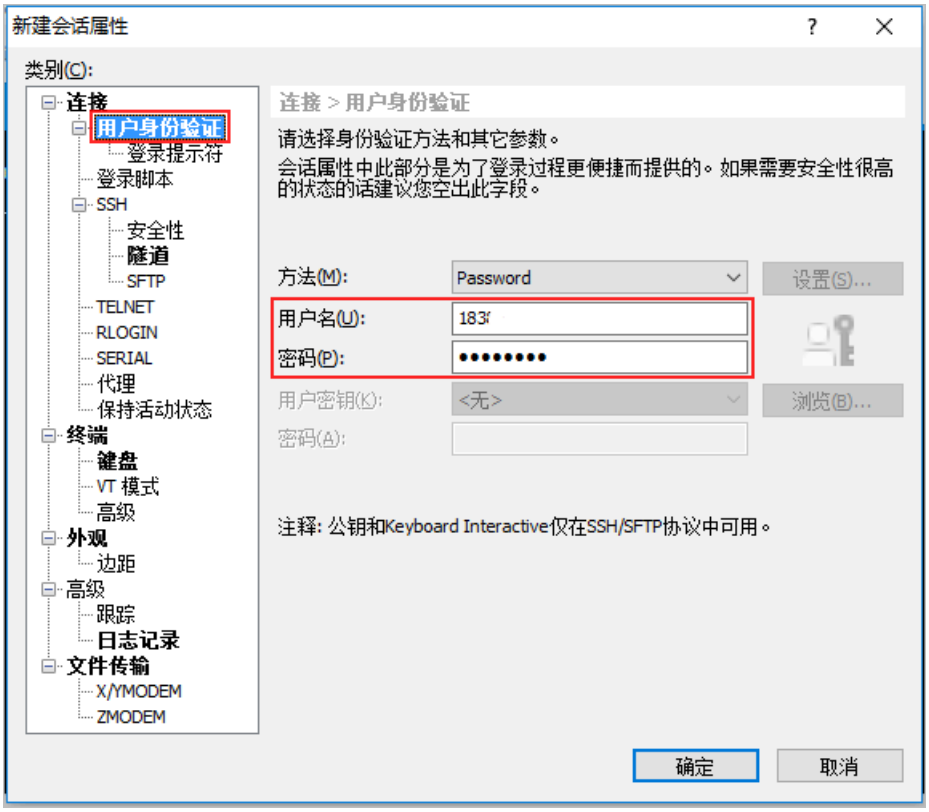
Xshell

下文以Xshell工具为例，介绍运维登录流程：

1. 打开Xshell工具，在连接设置中输入云盾堡垒机的IP和SSH端口号（SSH端口号默认为60022）。

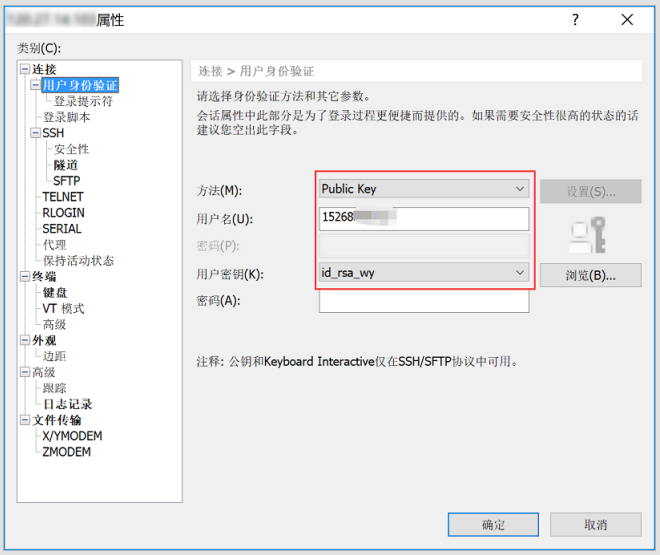


2. 在用户身份验证设置中输入云盾堡垒机的用户名和密码。



说明:

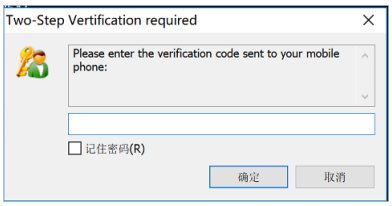
如果管理员在云盾堡垒机中配置了用户公钥，则用户可以通过公私密钥对的方式登录，无需输入密码。在用户身份验证设置中，选择Public Key，输入云盾堡垒机用户名，选择对应的私钥。



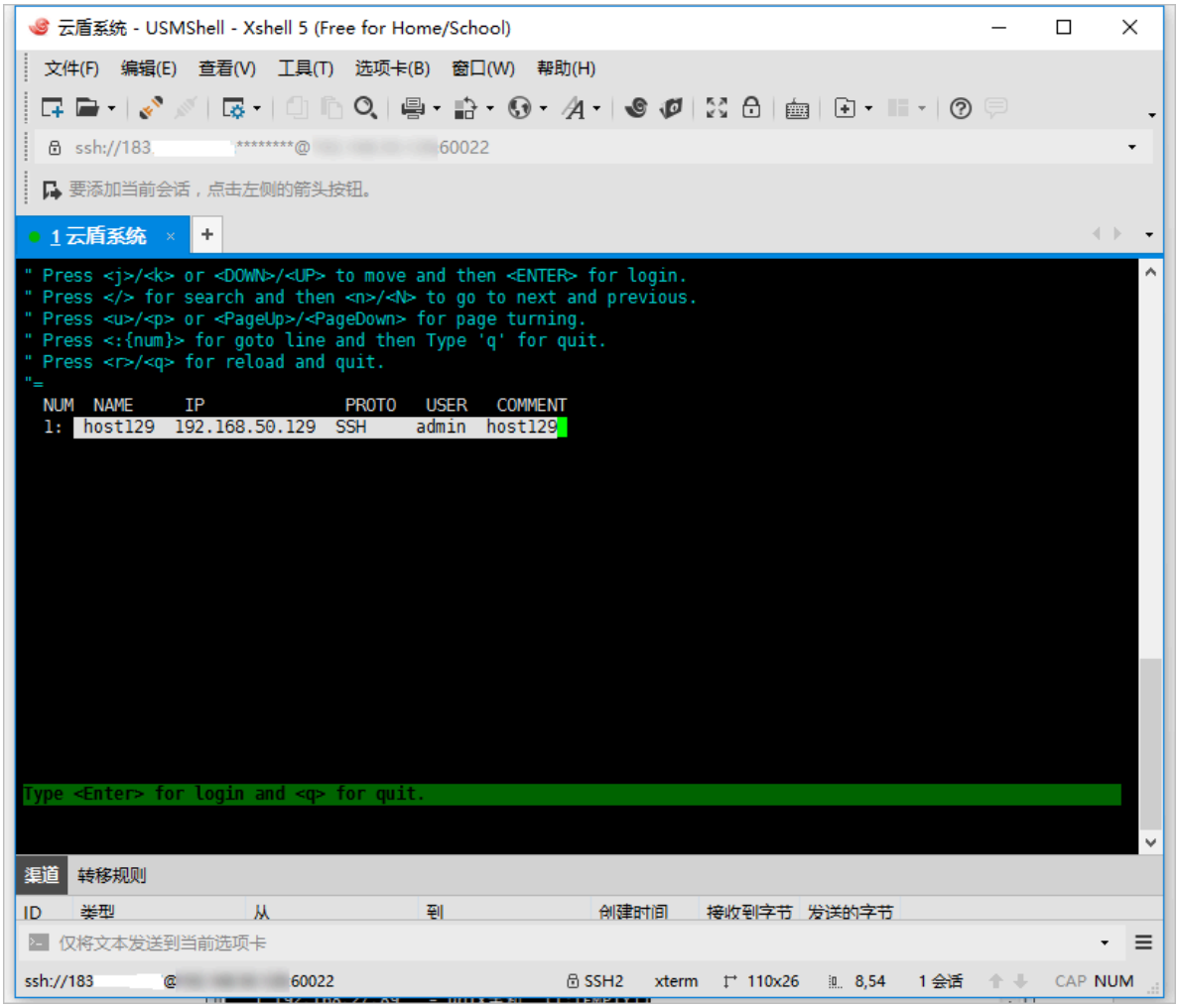
3. 单击确定，连接云盾堡垒机。

4. （可选）如果管理员启用了双因子认证登录，将会弹出双因子口令对话框，请输入您手机上收到的6位数字。

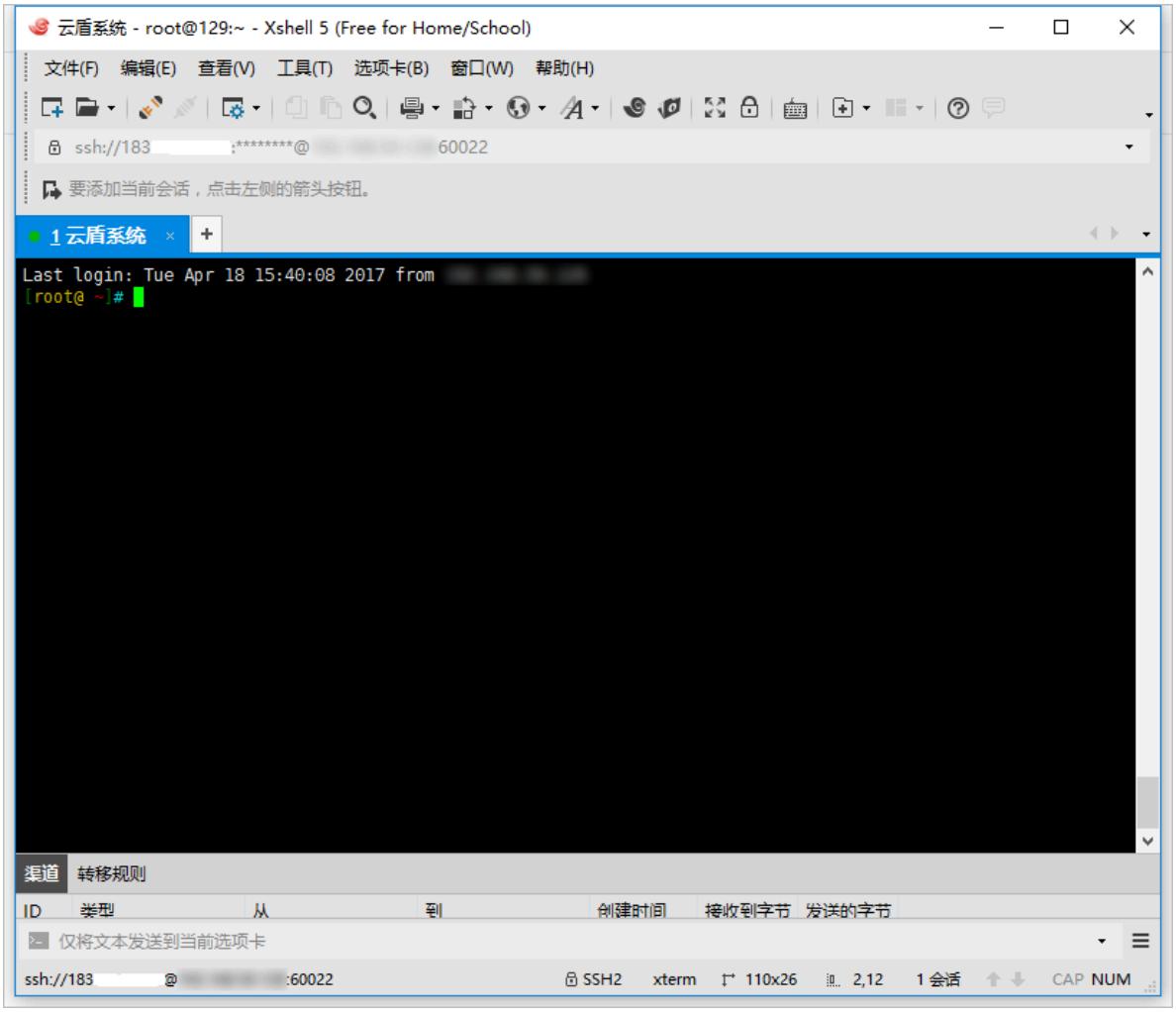
> **说明:**
> 云子账号账户使用MFA进行二次验证。



5. 成功登录云盾堡垒机后，进入资产管理界面。通过键盘上的上、下箭头选择您想要进行运维的服务器主机。



6. 按 Enter 键即可登录目标服务器主机进行运维操作。

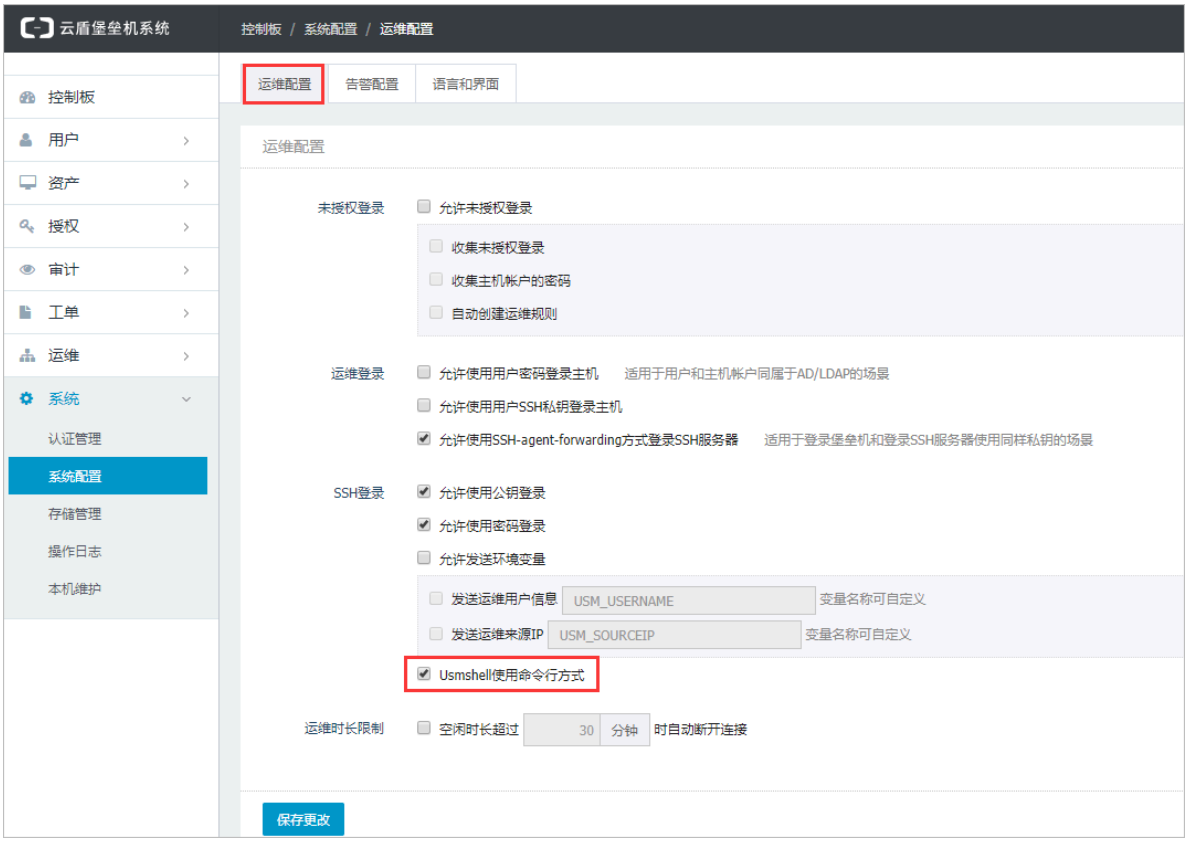


Usmshell使用说明

参照以下步骤开启Usmshell使用命令行方式：

1. 进入系统 > 系统配置 > 运维配置页。

2. 在SSH登录选项中勾选Usmshell使用命令行方式。



3. 打开SSH协议客户端，使用CS运维方式登录堡垒机。输入`help`查看usmshell使用帮助。

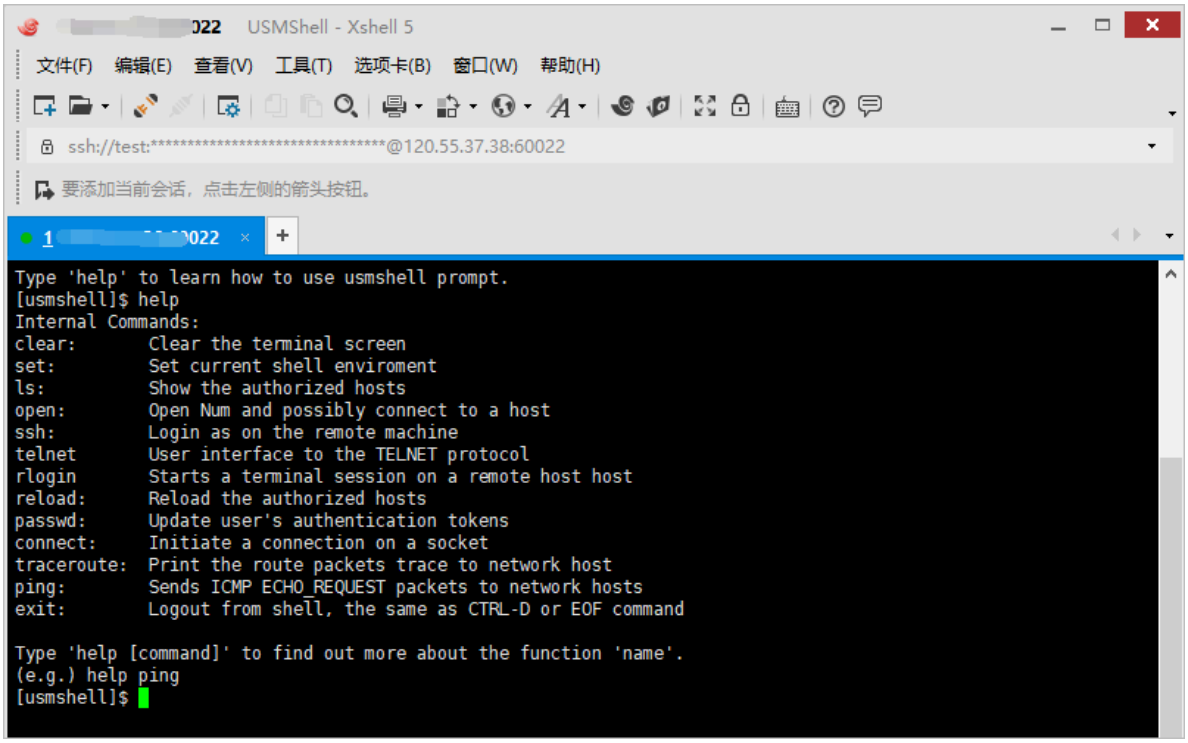


表 2-1: 命令描述

命令	描述

clear	清屏。
set	设置当前shell环境。
ls	列出可运维的资产列表。
open	按编号连接可运维列表中的资产。
ssh	连接ssh协议资产。
telnet	连接telnet协议资产。
rlogin	连接rlogin协议资产。
reload	重连。
passwd	修改用户密码。
connect	连接主机某个端口。
traceroute	将路由数据包跟踪打印到主机。
ping	检查连通性。
exit	退出登录。

说明:

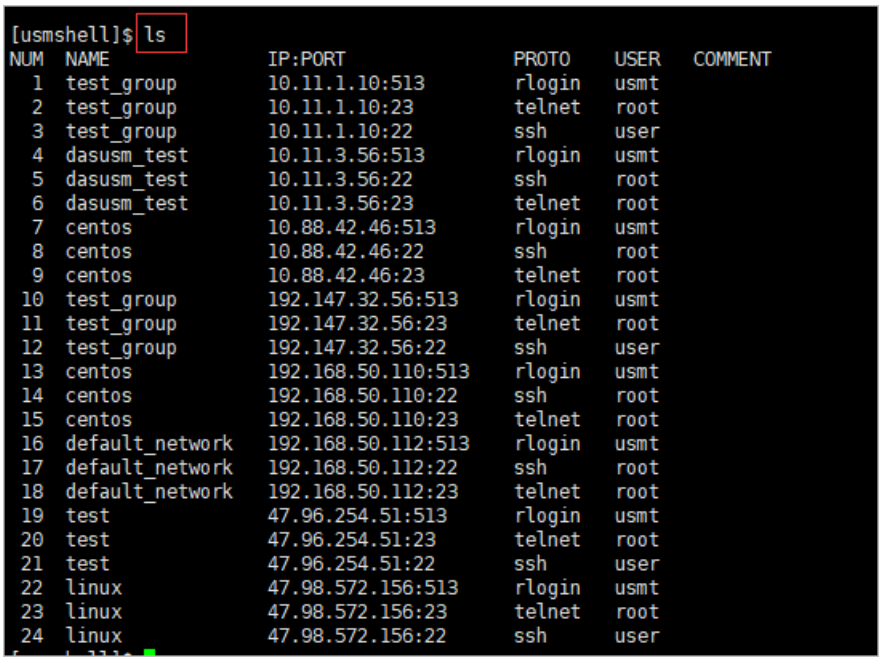
输入`help [command]`查看更详细的使用帮助。

以ls、open、ssh、passwd命令为例详细介绍其使用方法。

- ls

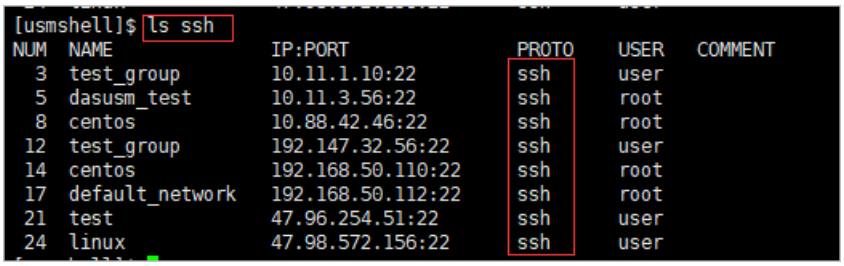
  ls命令支持通过协议、用户名、主机名和主机IP过滤资产并列出资产，且支持模糊匹配功能。

  - 输入`ls`，列出所有可运维资产。



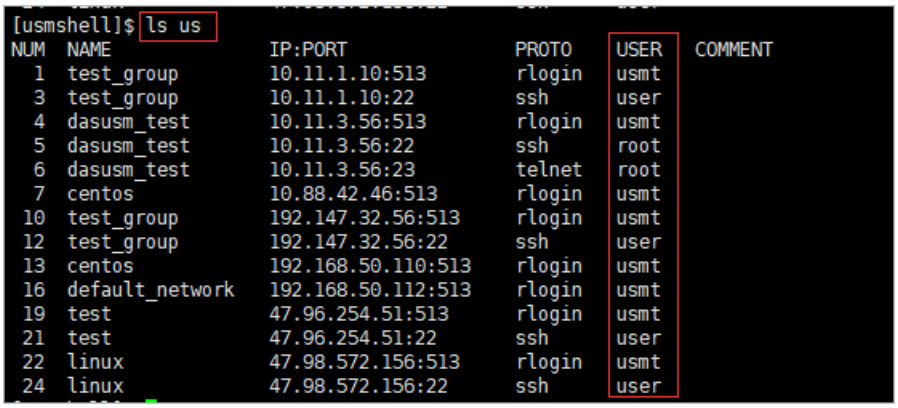
```
[usmshell]$ ls
NUM  NAME              IP:PORT              PROTO    USER   COMMENT
  1  test_group        10.11.1.10:513       rlogin   usmt
  2  test_group        10.11.1.10:23        telnet   root
  3  test_group        10.11.1.10:22        ssh      user
  4  dasusm_test       10.11.3.56:513       rlogin   usmt
  5  dasusm_test       10.11.3.56:22        ssh      root
  6  dasusm_test       10.11.3.56:23        telnet   root
  7  centos            10.88.42.46:513      rlogin   usmt
  8  centos            10.88.42.46:22       ssh      root
  9  centos            10.88.42.46:23       telnet   root
 10  test_group        192.147.32.56:513    rlogin   usmt
 11  test_group        192.147.32.56:23     telnet   root
 12  test_group        192.147.32.56:22     ssh      user
 13  centos            192.168.50.110:513   rlogin   usmt
 14  centos            192.168.50.110:22    ssh      root
 15  centos            192.168.50.110:23    telnet   root
 16  default_network   192.168.50.112:513   rlogin   usmt
 17  default_network   192.168.50.112:22    ssh      root
 18  default_network   192.168.50.112:23    telnet   root
 19  test              47.96.254.51:513     rlogin   usmt
 20  test              47.96.254.51:23      telnet   root
 21  test              47.96.254.51:22      ssh      user
 22  linux             47.98.572.156:513    rlogin   usmt
 23  linux             47.98.572.156:23     telnet   root
 24  linux             47.98.572.156:22     ssh      user
```

  - 输入`ls [protocol]`，列出通过协议过滤后的资产，支持模糊匹配。



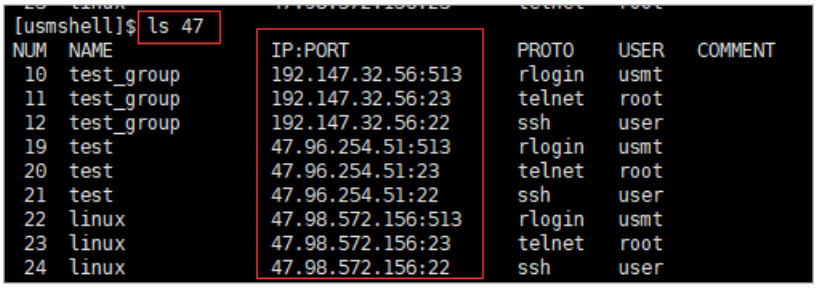
```
[usmshell]$ ls ssh
NUM  NAME              IP:PORT              PROTO    USER   COMMENT
  3  test_group        10.11.1.10:22        ssh      user
  5  dasusm_test       10.11.3.56:22        ssh      root
  8  centos            10.88.42.46:22       ssh      root
 12  test_group        192.147.32.56:22     ssh      user
 14  centos            192.168.50.110:22    ssh      root
 17  default_network   192.168.50.112:22    ssh      root
 21  test              47.96.254.51:22      ssh      user
 24  linux             47.98.572.156:22     ssh      user
```

  - 输入`ls [user]`，列出通过用户名过滤后的资产，支持模糊匹配。

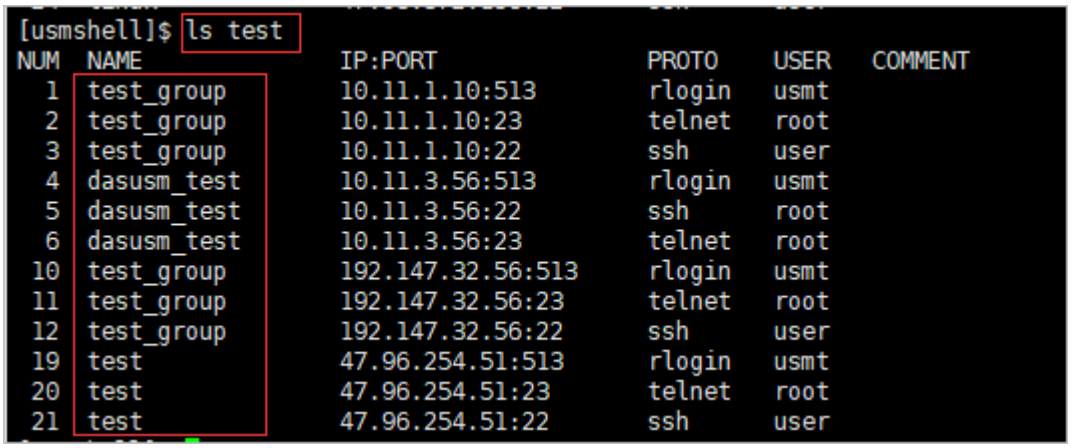


```
[usmshell]$ ls us
NUM  NAME              IP:PORT              PROTO    USER   COMMENT
  1  test_group        10.11.1.10:513       rlogin   usmt
  3  test_group        10.11.1.10:22        ssh      user
  4  dasusm_test       10.11.3.56:513       rlogin   usmt
  5  dasusm_test       10.11.3.56:22        ssh      root
  6  dasusm_test       10.11.3.56:23        telnet   root
  7  centos            10.88.42.46:513      rlogin   usmt
 10  test_group        192.147.32.56:513    rlogin   usmt
 12  test_group        192.147.32.56:22     ssh      user
 13  centos            192.168.50.110:513   rlogin   usmt
 16  default_network   192.168.50.112:513   rlogin   usmt
 19  test              47.96.254.51:513     rlogin   usmt
 21  test              47.96.254.51:22      ssh      user
 22  linux             47.98.572.156:513    rlogin   usmt
 24  linux             47.98.572.156:22     ssh      user
```

  - 输入`ls [ip]`，列出通过主机IP过滤后的资产，支持模糊匹配。

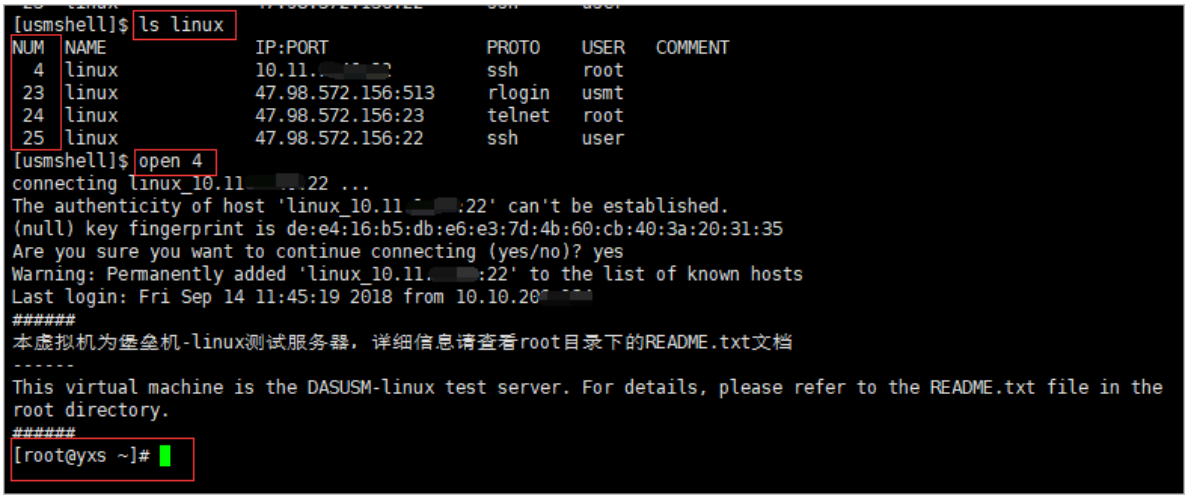


- 输入`ls [name]`，列出通过主机名过滤后的资产，支持模糊匹配。



- open

使用open命令可以按编号连接可运维列表中的资产，先输入ls命令获取资产列表，再通过open命令连接资产。

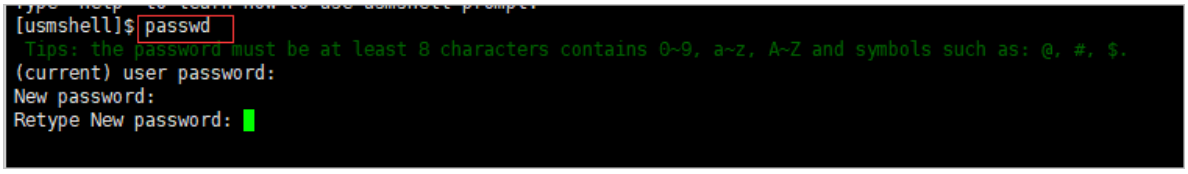


- ssh

  通过ssh协议登录资产。前提是所登录资产的ssh账户已被授权。

- passwd

  通过passwd命令修改堡垒机用户密码。登录堡垒机后，输入passwd命令并按Enter键。根据提示依次输入当前用户密码、新密码、重复新密码，并按 Enter 键。



2.2 RDP协议运维

本文受众范围：运维工程师、云盾堡垒机管理员、持有阿里云帐号的管理员。

背景信息

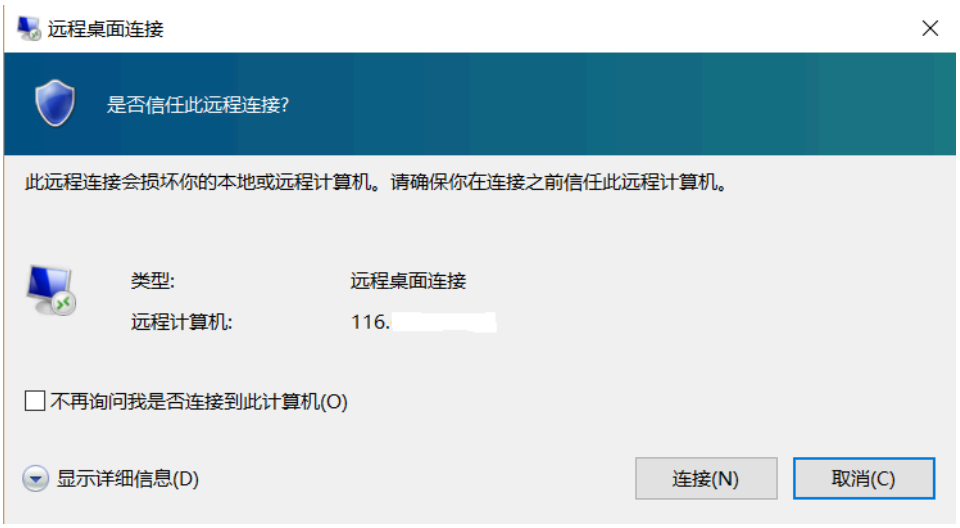
运维人员需要通过本地的客户端工具登录云盾堡垒机，再访问目标服务器主机进行运维操作。下文以 Windows 系统自带的 远程桌面连接工具（Mstsc）为例说明运维登录流程：

操作步骤

1. 在本地 Windows 系统主机中打开远程桌面连接工具（Mstsc）。

2. 输入云盾堡垒机的 IP 和 RDP 端口号（RDP 端口号默认为 63389）：`< IP >:63389`，单击连接。

3. 在是否信任此远程连接？对话框中，单击连接。



4. 在无法验证次远程计算机的身份。是否仍要连接？对话框中，单击是。

5. 在云盾堡垒机登录窗口中，输入云盾堡垒机的用户名和密码。

6. 单击登录，登录云盾堡垒机。

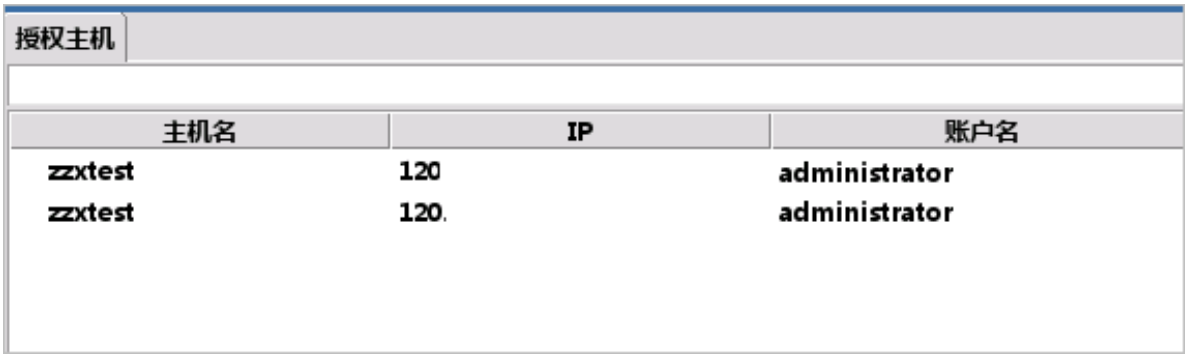
说明:

**如果管理员启用了双因子认证登录，将会弹出双因子口令对话框，请输入您手机上收到的6位数字。

说明:

云子帐号使用MFA进行二次验证。

7. 成功登录云盾堡垒机后，进入资产管理界面，双击您需要登录的已授权服务器主机进行登录。



8. 进入目标服务器主机的登录界面，输入主机的账户和密码。

说明:

若已在堡垒机中添加凭据，且该凭据添加到该用户的授权组中，则无需输入主机账户密码可直接登录主机。

9. 按Enter键即可登录服务器主机进行运维操作。

2.3 SFTP协议运维

运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。

背景信息

运维员通过本地的客户端工具登录云盾堡垒机，再访问目标主机。

说明:
您必须先在本地安装好支持SFTP协议的运维工具，如：Xftp、WinSCP、FlashFXP等。

下文以Xftp为例介绍运维登录流程：

操作步骤

1. 打开Xftp工具，在登录窗口中输入云盾系统的IP、端口号60022、用户名、密码。

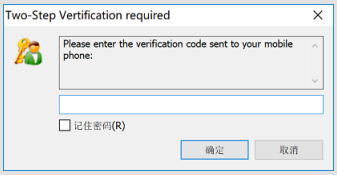
说明:

如果管理员在云盾堡垒机中配置了用户公钥，则用户可以通过公私密钥对的方式登录，无需输入密码。 在用户身份验证设置中，选择Public Key，输入云盾堡垒机用户名，选择对应的私钥。

2. 单击 确定，连接云盾堡垒机。

说明:

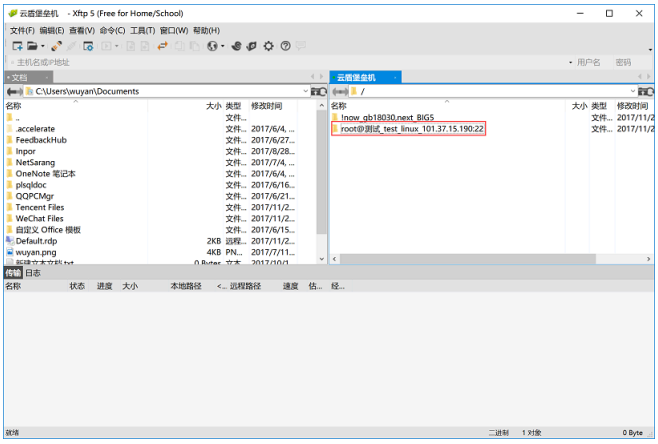
如果管理员启用了双因子登录，将会弹出双因子口令对话框，请输入您手机上收到的6位数字。



说明:

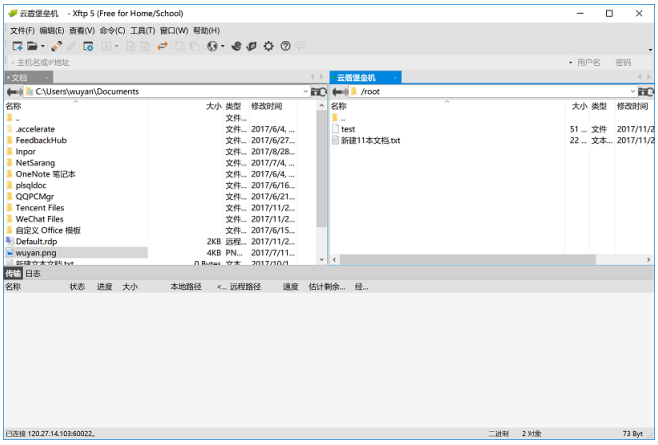
云子帐号账户使用MFA进行二次验证。

3. 成功登录云盾堡垒机后，在右侧可以看到已授权的服务器主机列表。



4. 双击需要操作的服务器，进入该服务器主机的目录，即可进行文件传输操作。

> **说明:**
> SFTP运维必须将有效凭据添加到相应授权组，否则无法登入ECS。



> **说明:**
> 主机列表中第一个目录是为了转码使用，如果主机列表编码有问题，可双击第一个目录后刷新进行转码。

2.4 Mac系统运维

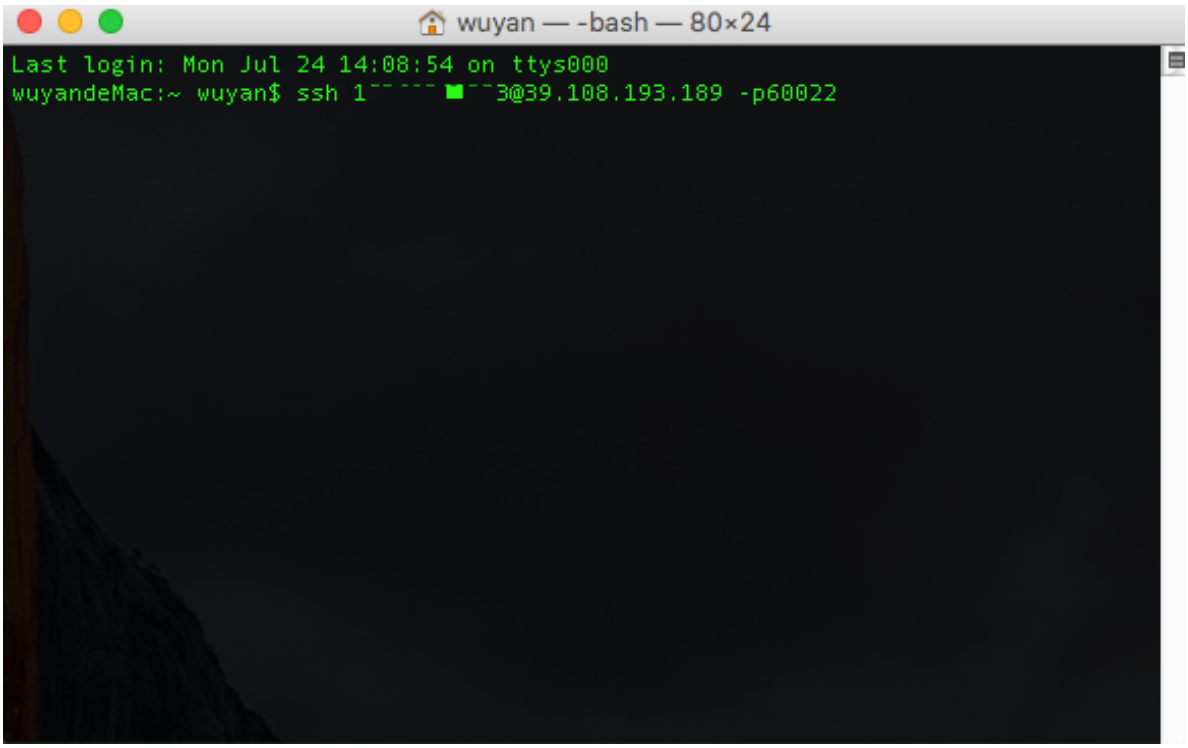
本文受众范围：运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。适用于使用Mac电脑通过本地客户端工具登录云盾堡垒机，再访问目标主机的运维工程师。

SSH协议运维

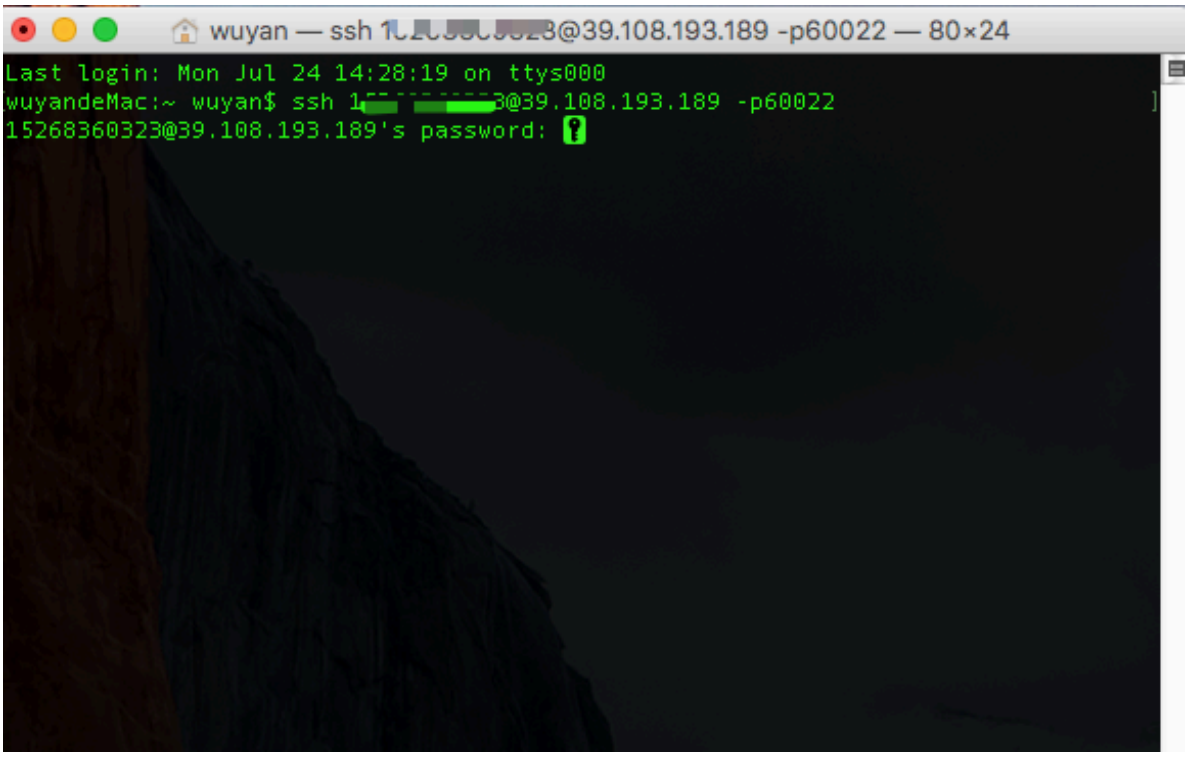
以MAC自带的命令行终端APP为例：

1. 打开命令行终端APP。

2. 输入以下命令：`ssh 云盾堡垒机用户名@云盾堡垒机IP -p60022`

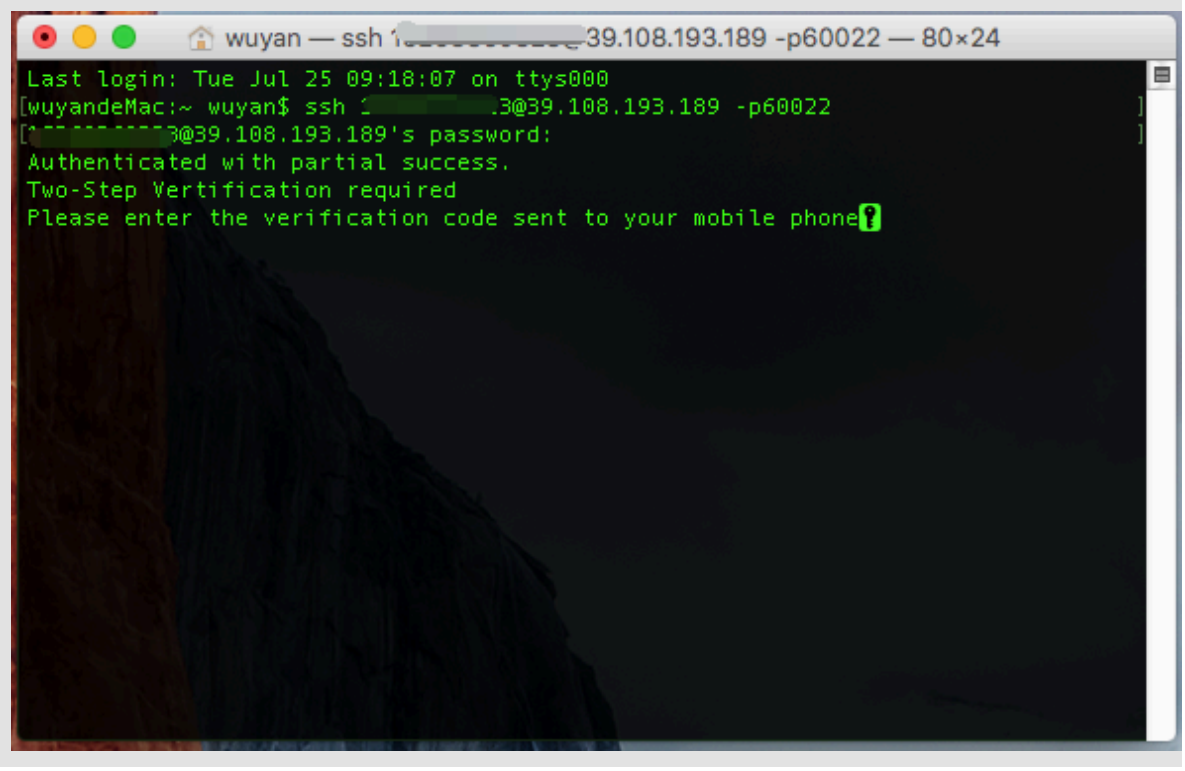


3. 输入云盾堡垒机密码。

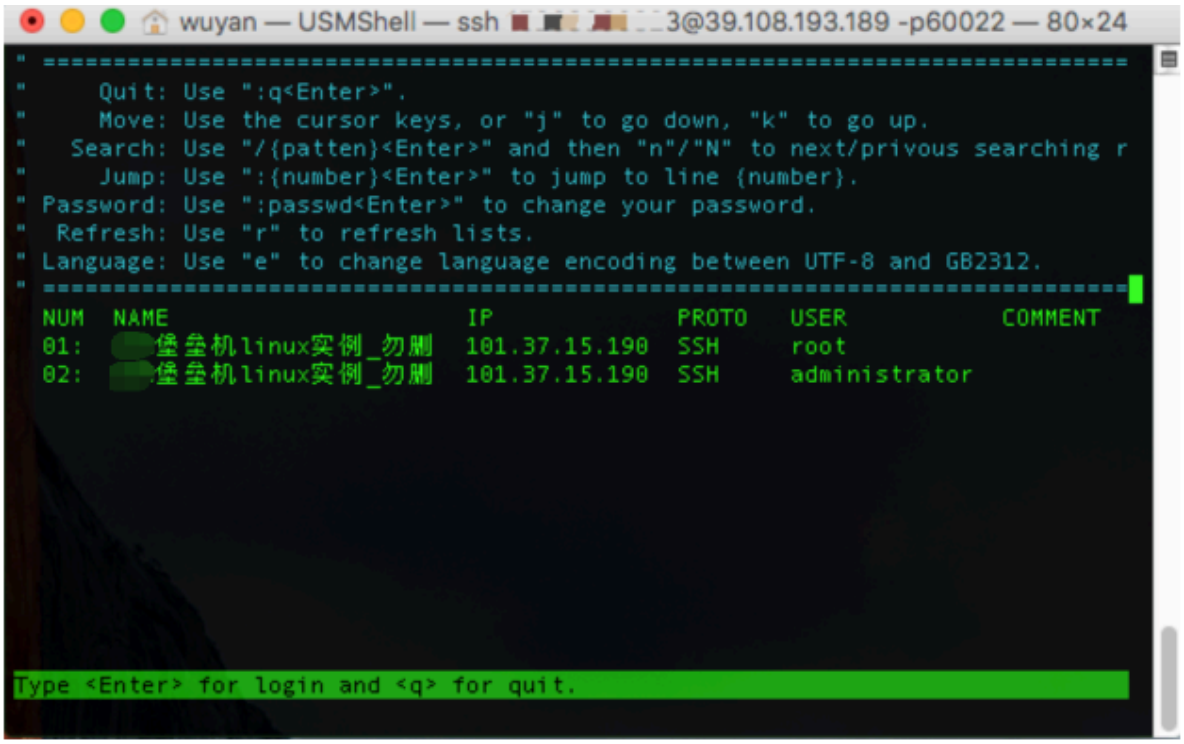


说明:

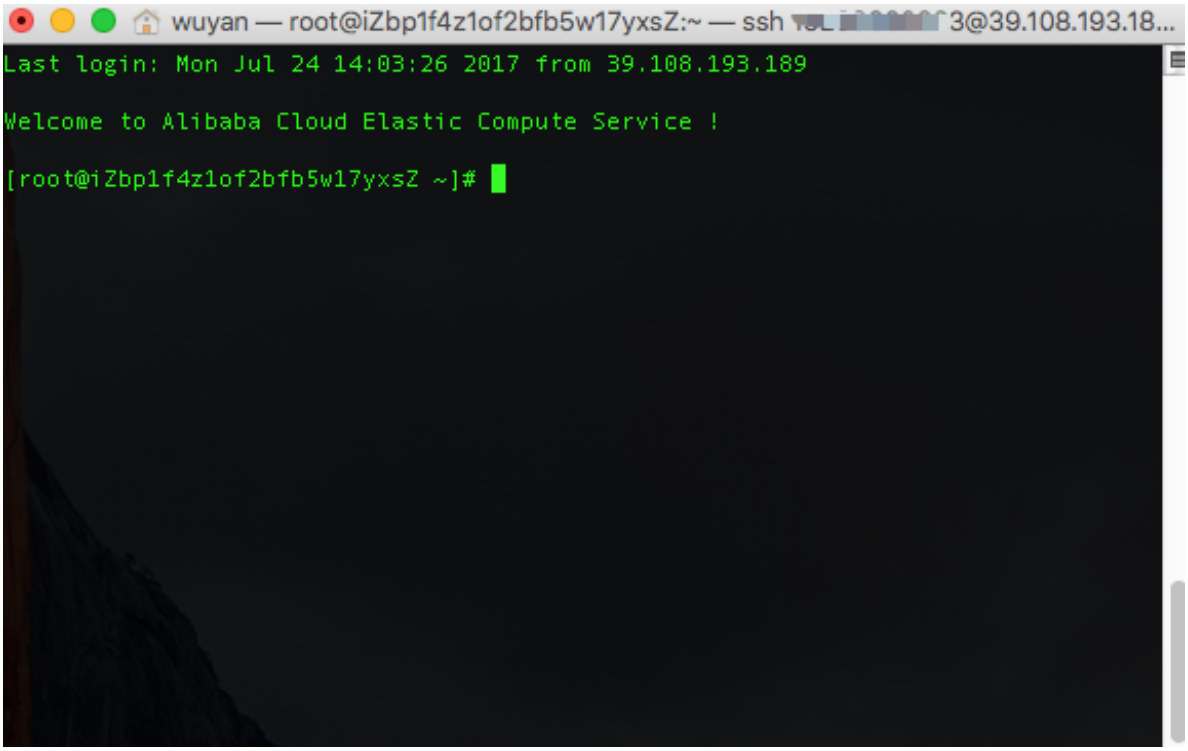
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。



4. 回车后进入资产管理界面，用上下键选择已授权的资产。



5. 回车后进入目标主机界面，进行运维操作。

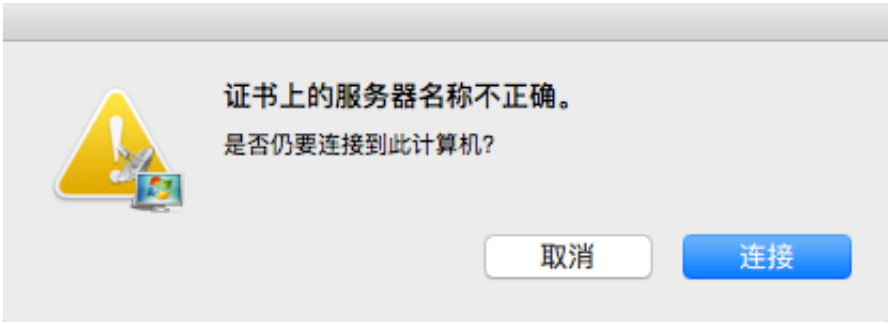


RDP协议运维

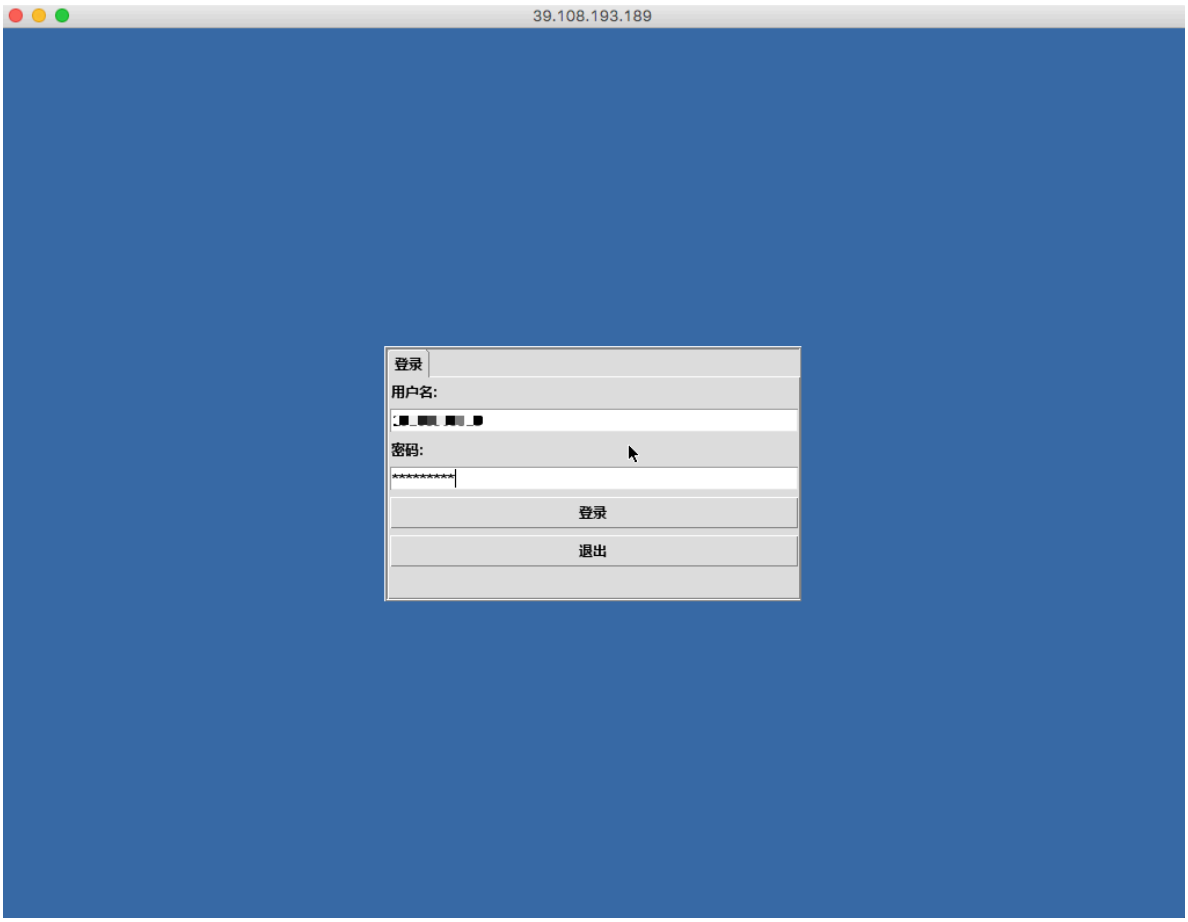
以远程桌面连接APP为例：

1. 打开命令行终端APP。
2. 输入云堡垒机的IP：`63389`

3. 单击连接后，弹出是否仍要连接此计算机？

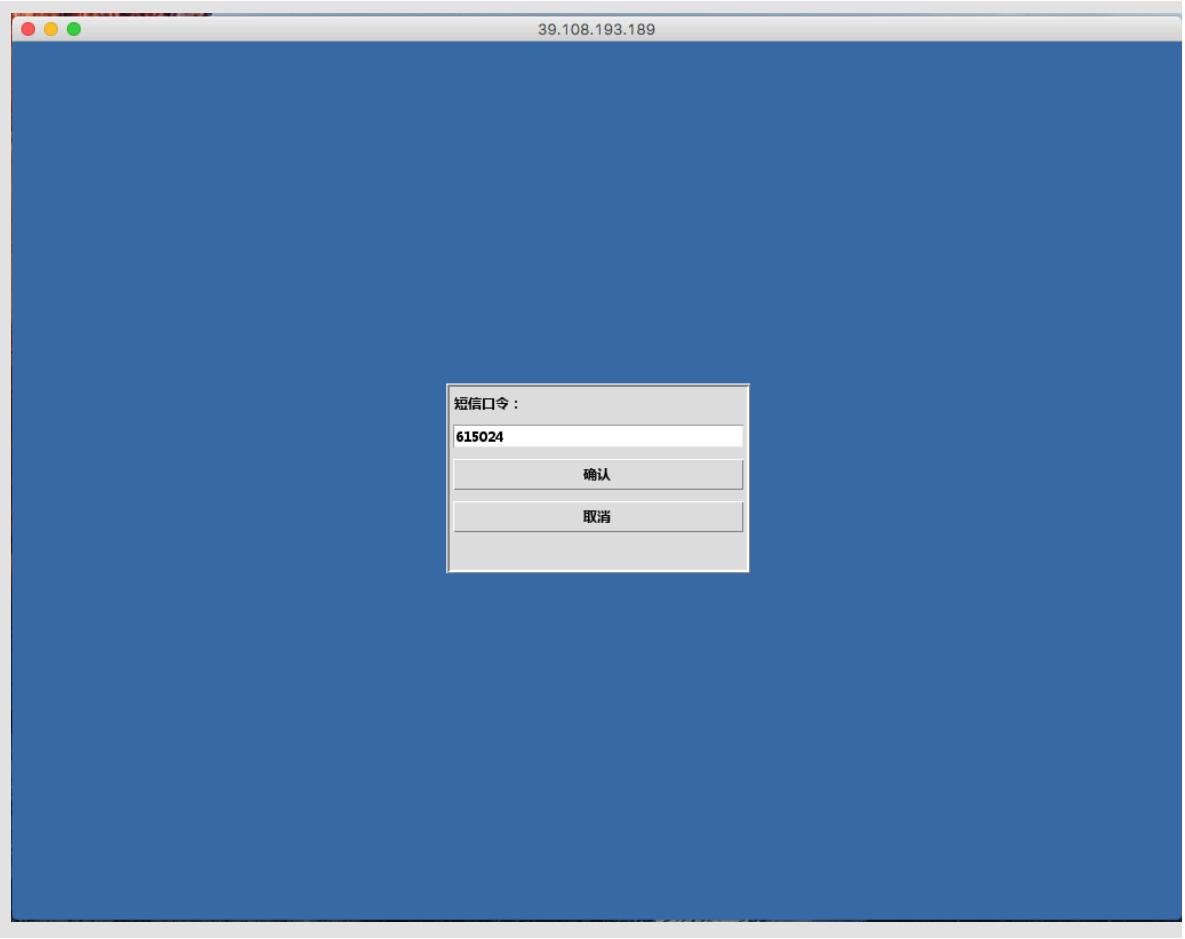


4. 单击连接后，进入云堡垒机登录窗口，输入：云堡垒机的用户名和密码

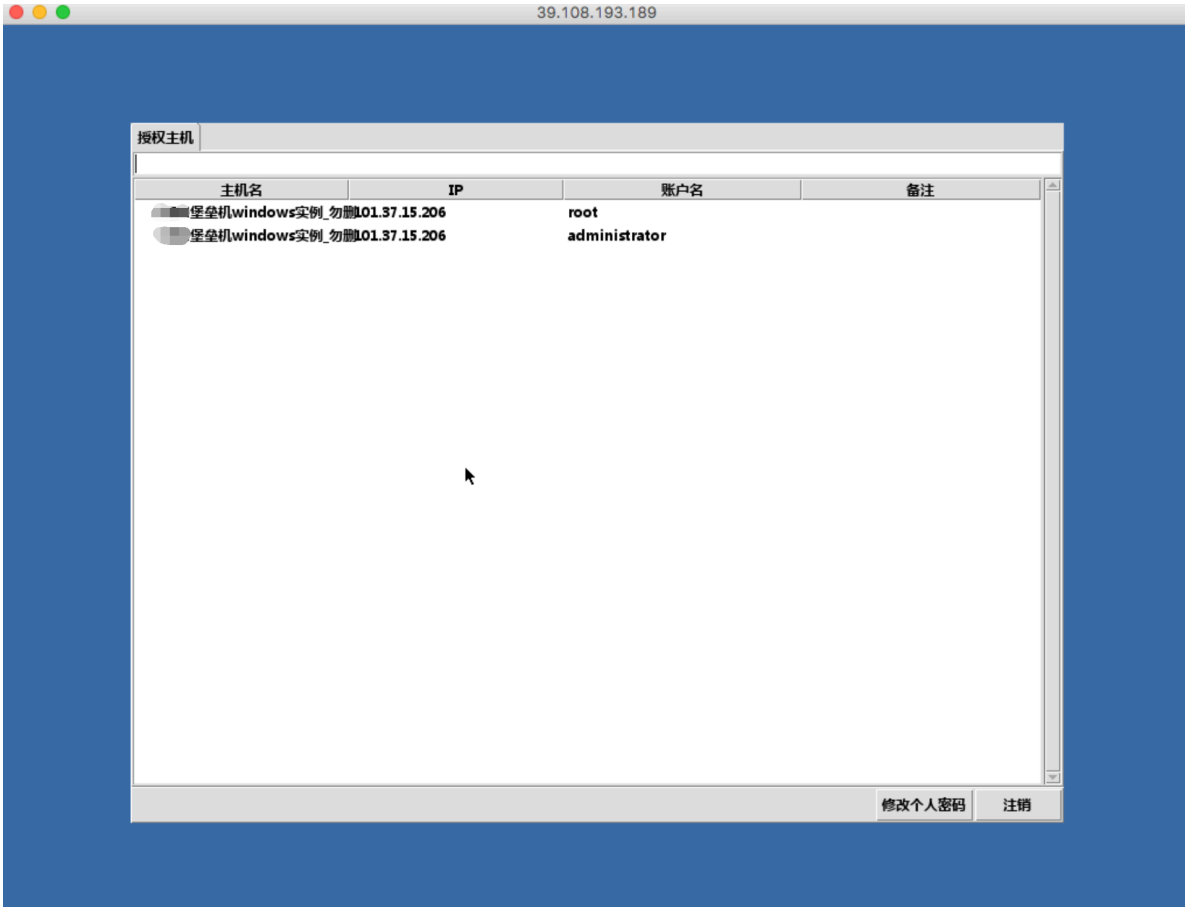


说明:

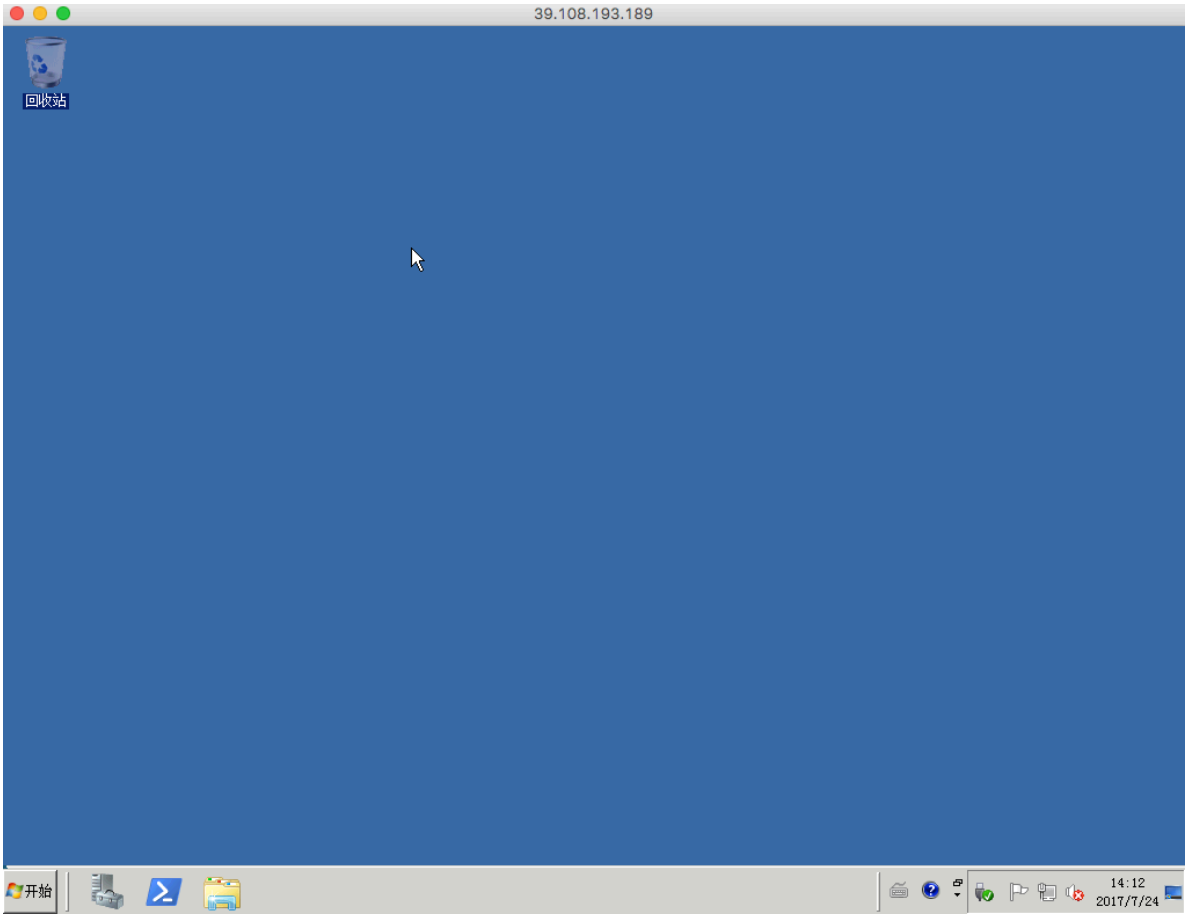
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。


39.108.193.189
短信口令：
615024
确认
取消

5. 单击登录后进入资产管理界面：用鼠标选择已授权的资产，或者通过搜索框搜索主机信息。



6. 双击之后即可进入目标主机进行运维操作。



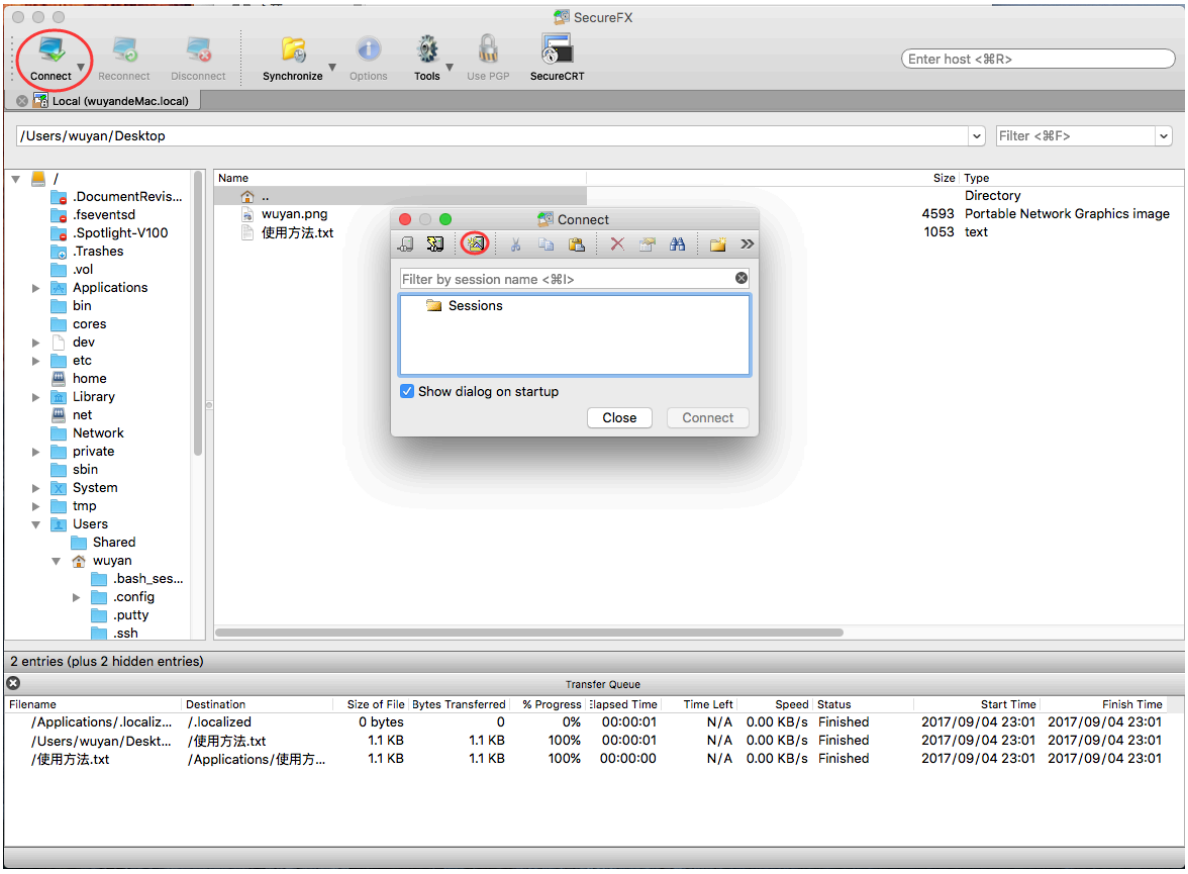
文件传输运维

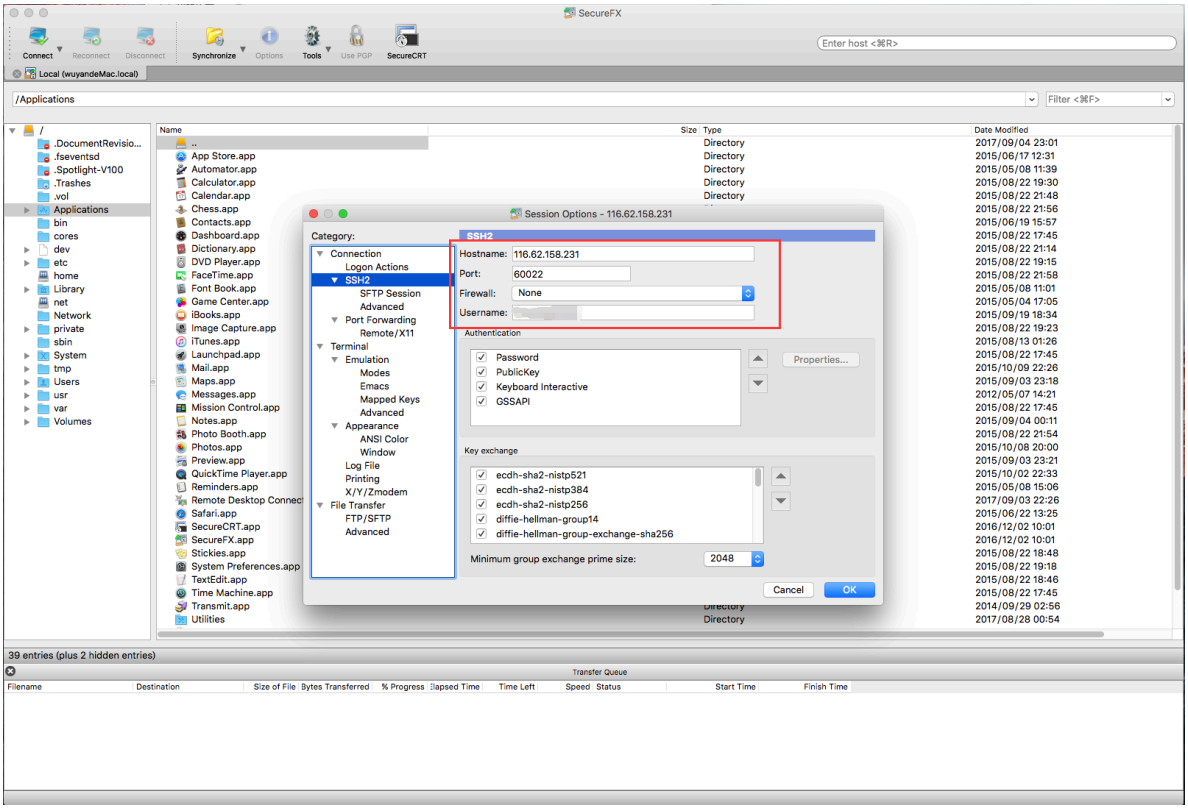
客户端访问堡垒机，再选择ECS方式运维

以SecureFX工具为例：

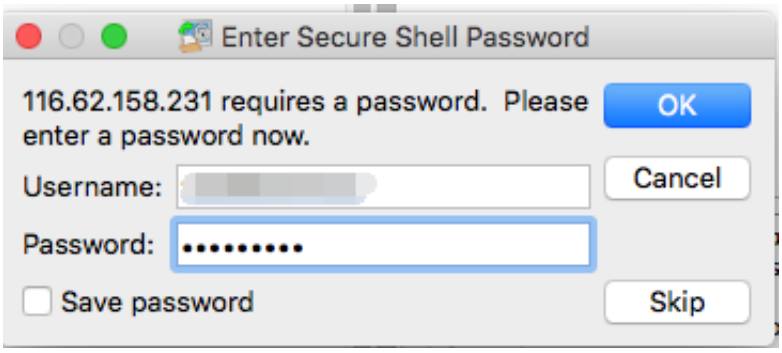
1. 打开SecureFX工具。

2. 新建连接，输入云堡垒机IP，端口60022，账户信息。



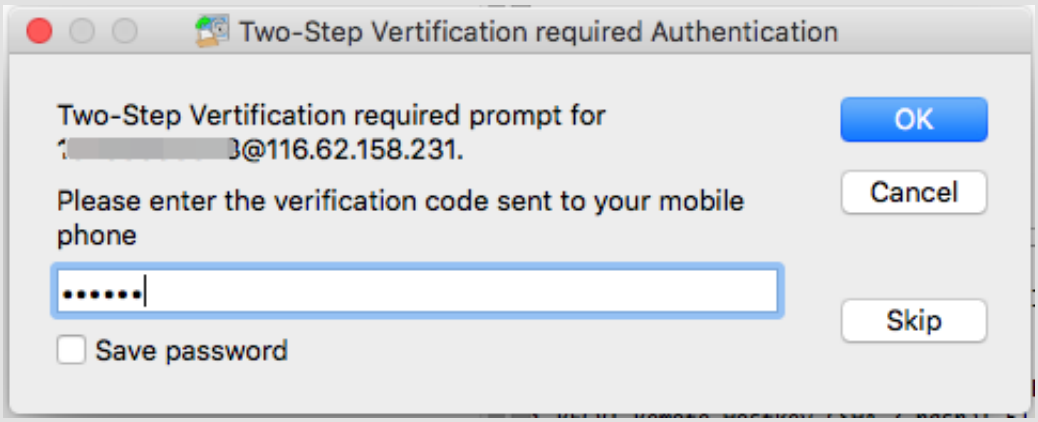


3. 单击连接后，按提示输入堡垒机密码。



说明:

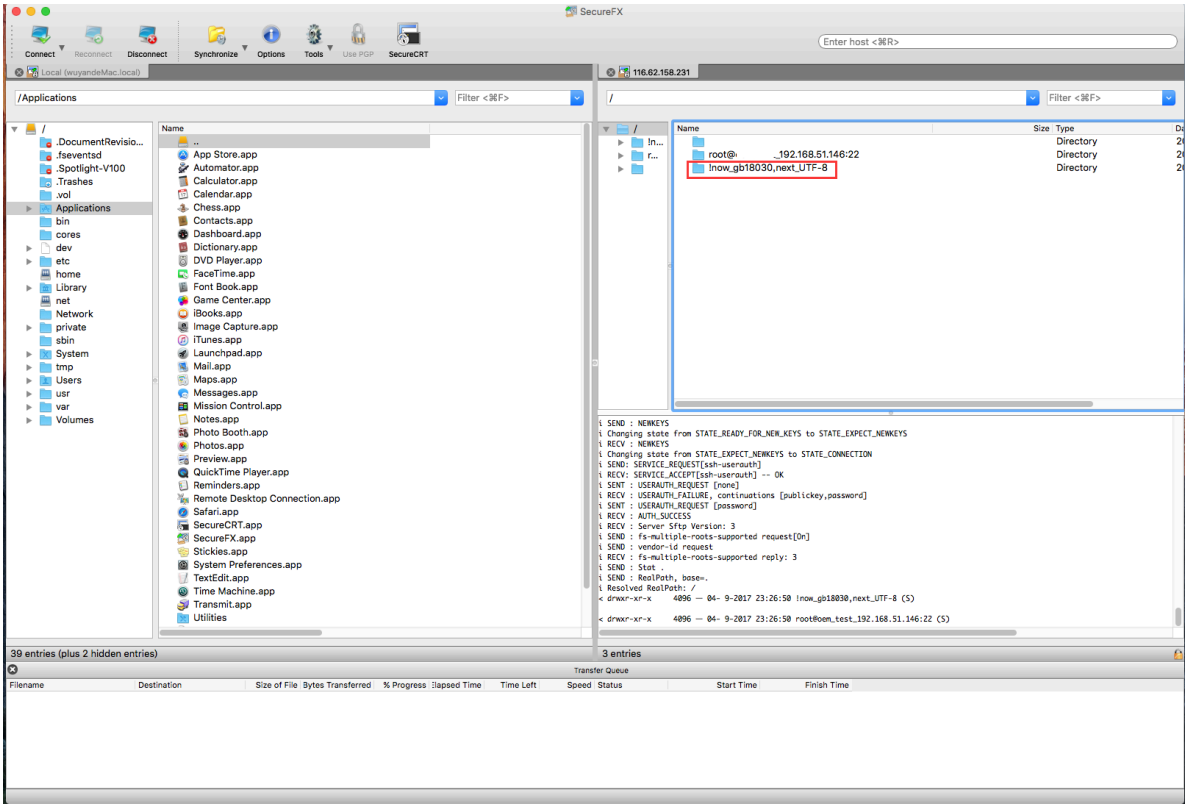
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。

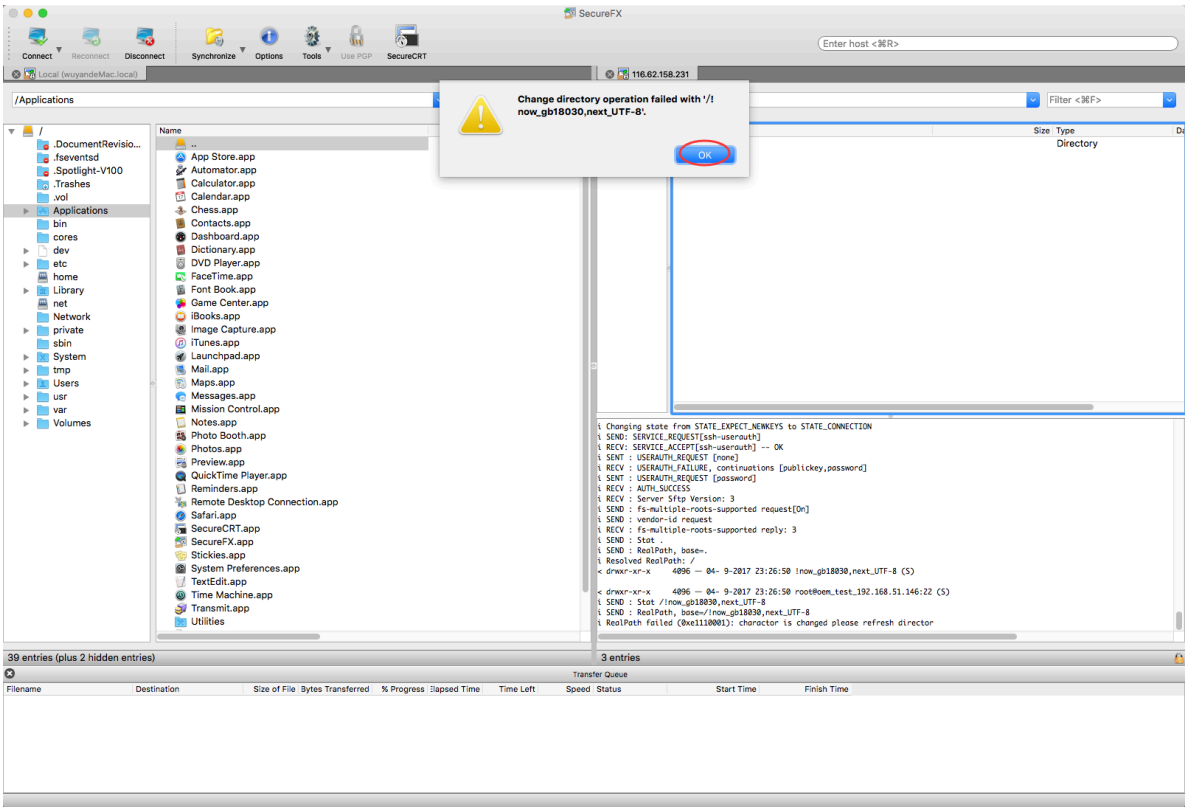


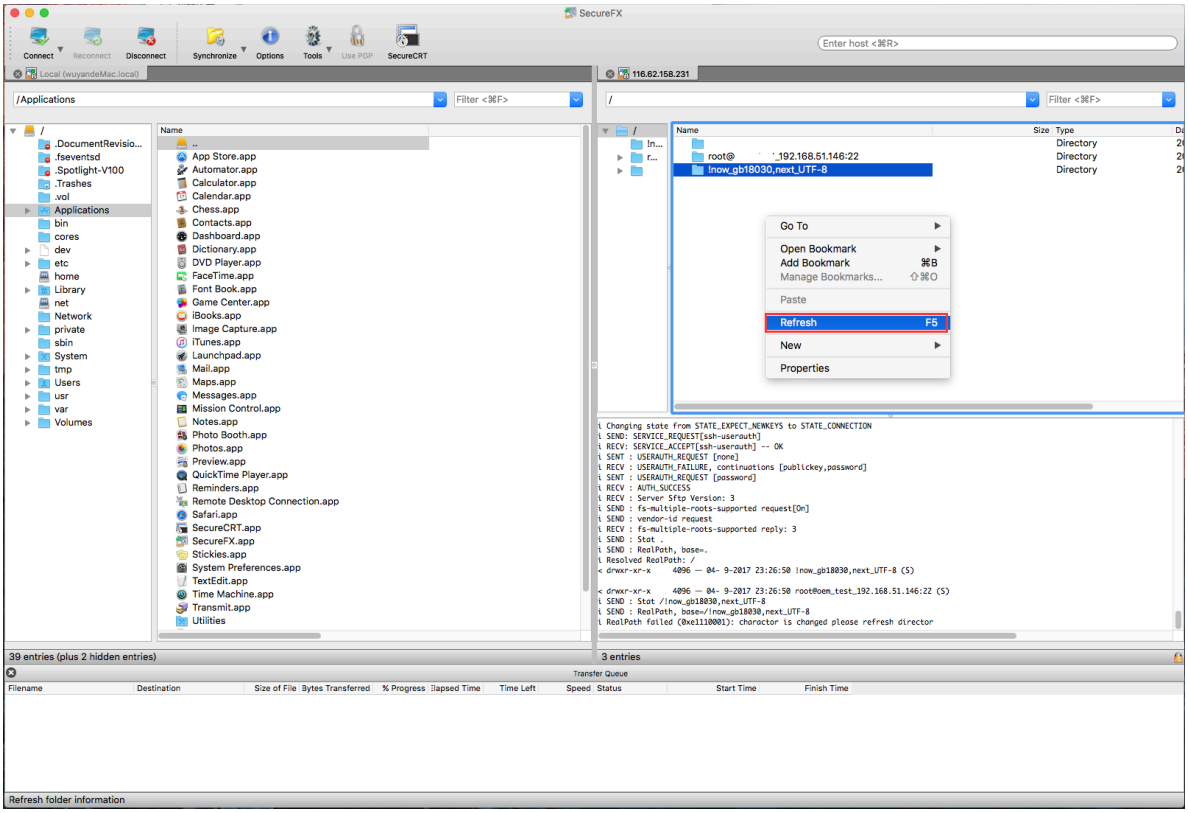
说明:

云子账号使用MFA进行二次验证。

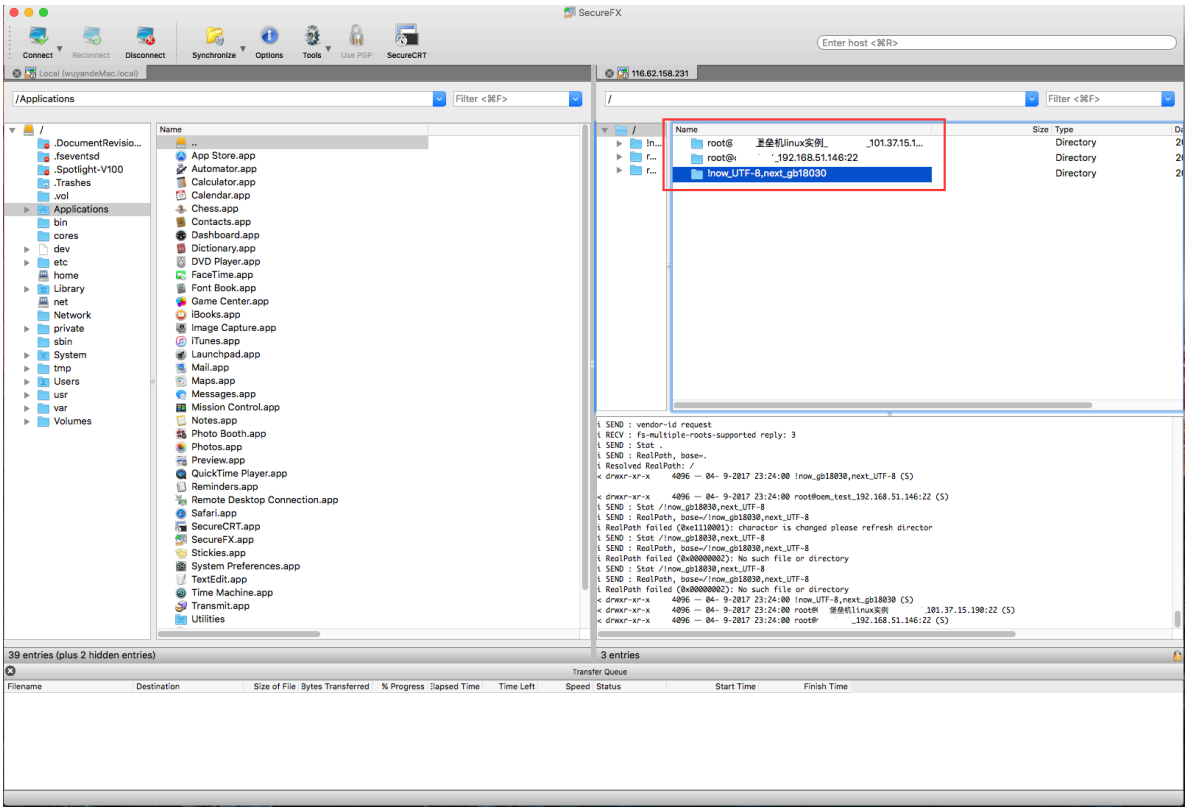
4. 单击<登录>后进入资产管理界面，请双击选择转码目录（忽略报错信息），再右键选择刷新，进行转码。



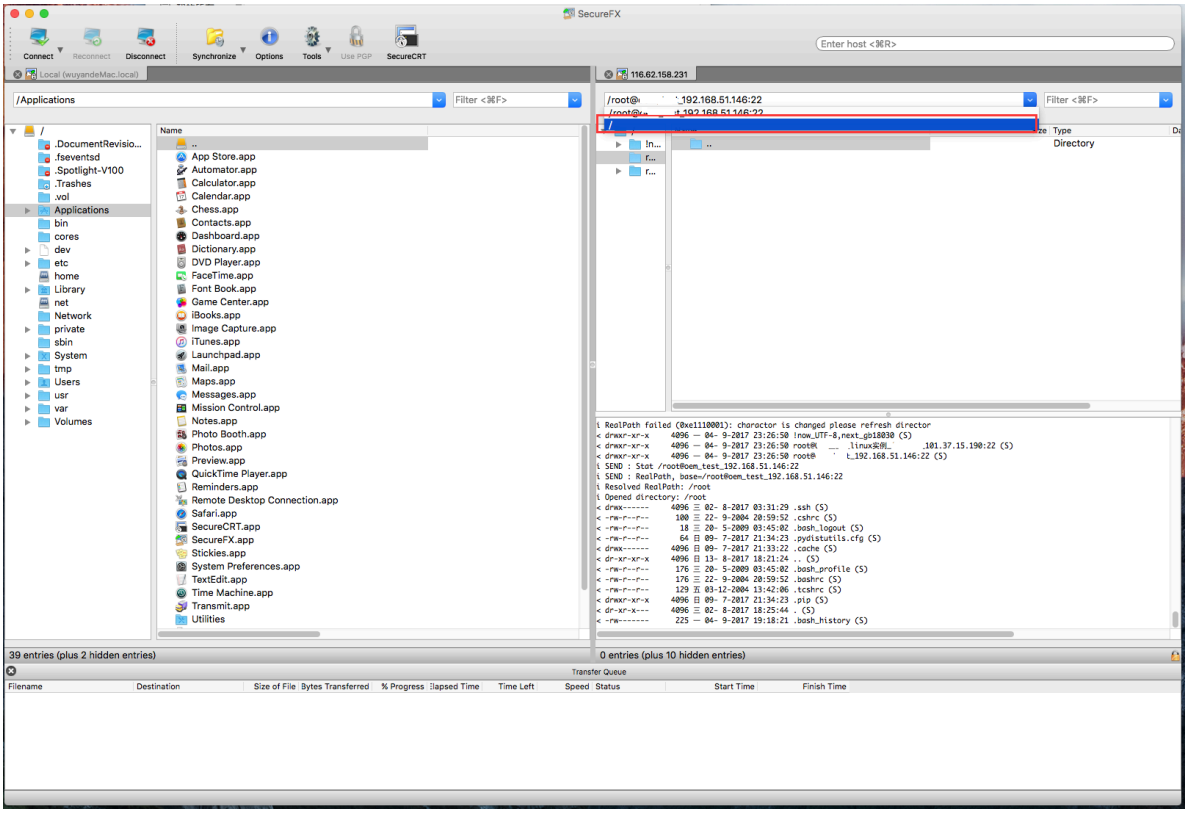


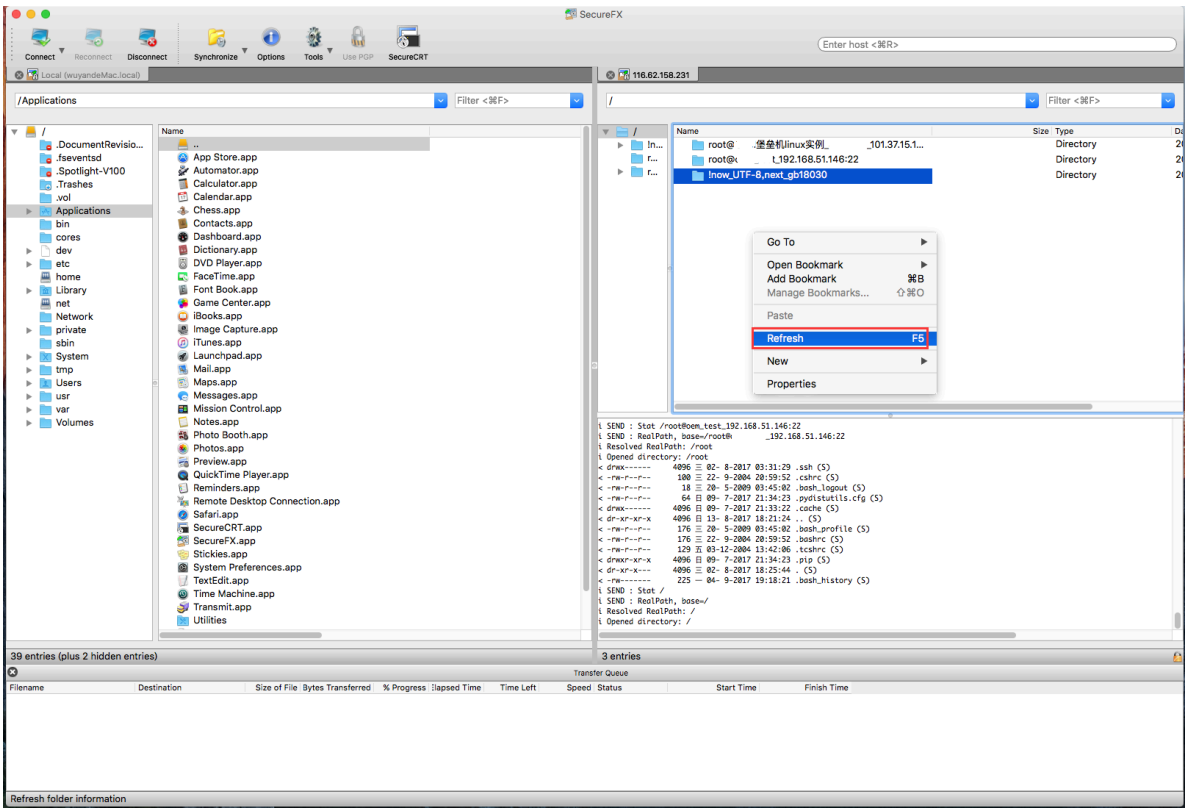


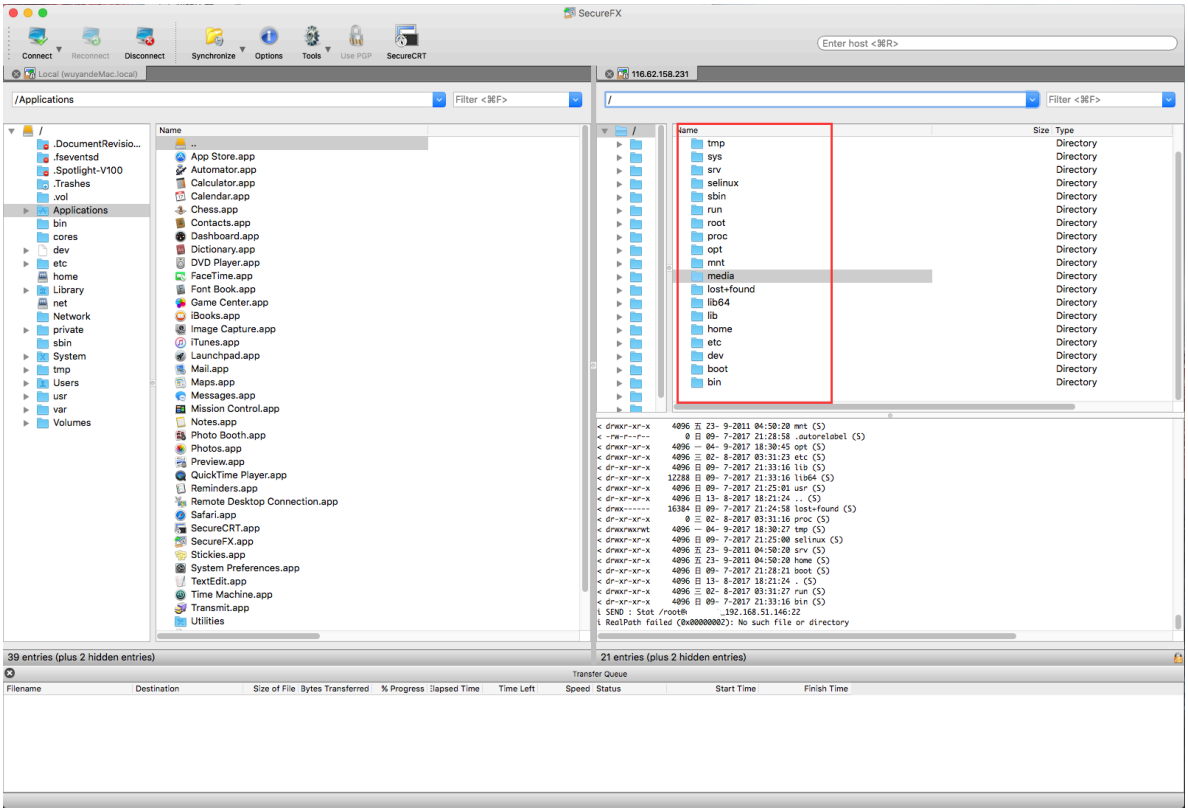
5. 转码后资产列表显示正常。



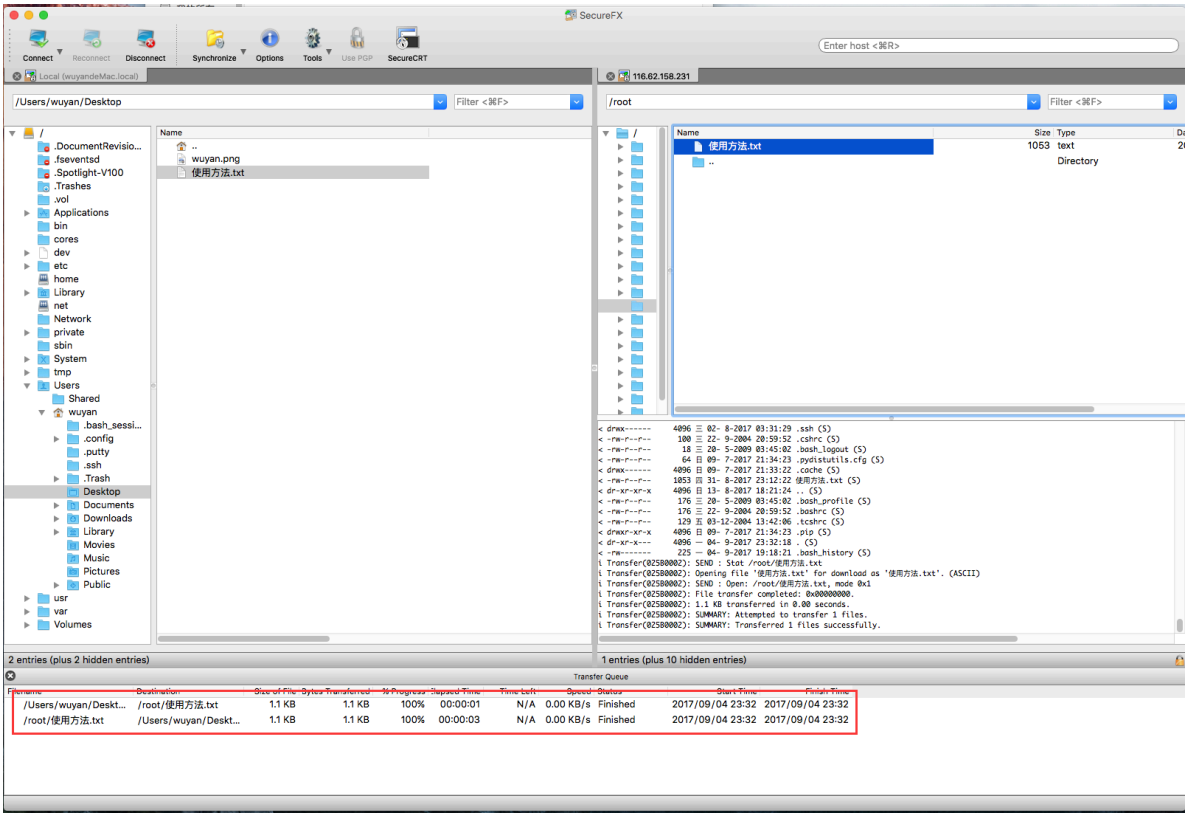
6. 选择目录主机双击进入后，需要先退回到根目录，再右键选择刷新后，进入主机，即可进行运维操作。







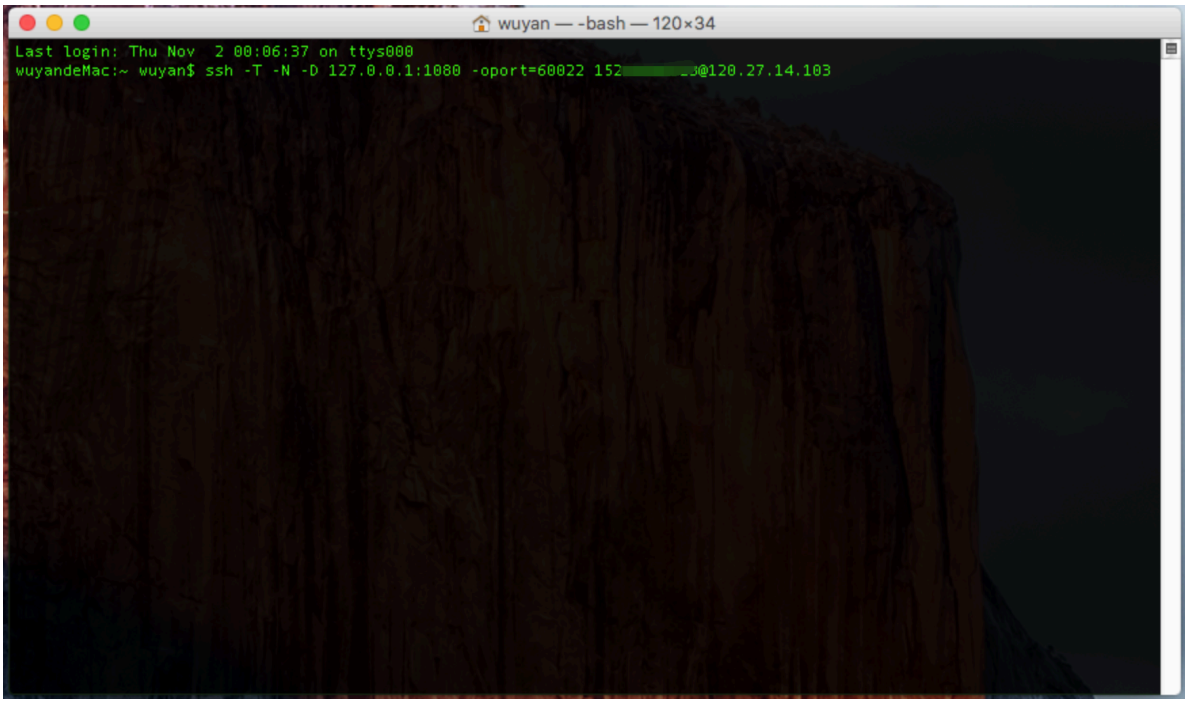
7. 可正常进行上传下载操作。



SSH网关+filezilla直连ECS方式运维

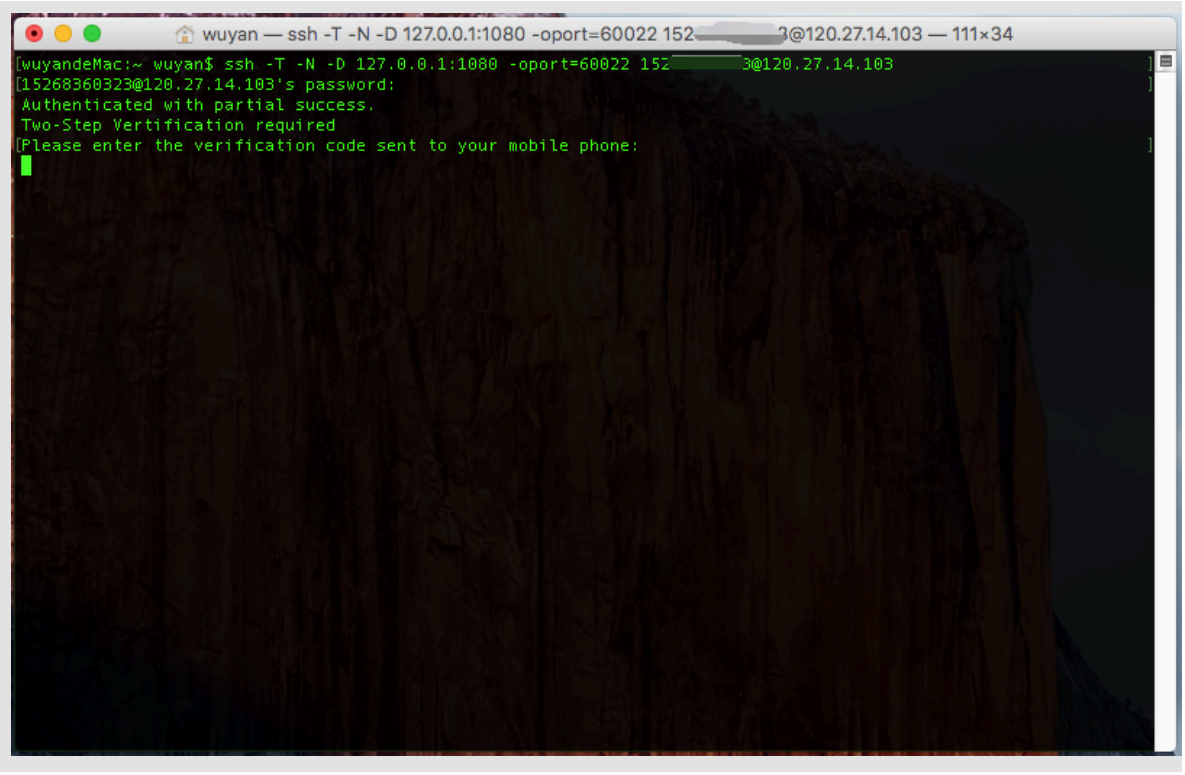
1. 打开命令行终端APP。

2. 输入`ssh -T -N -D 127.0.0.1:1080 -oport=60022 用户名@堡垒机IP`，按Enter键。



3. 输入云盾堡垒机密码，按Enter键连接到堡垒机，不要关闭该窗口。

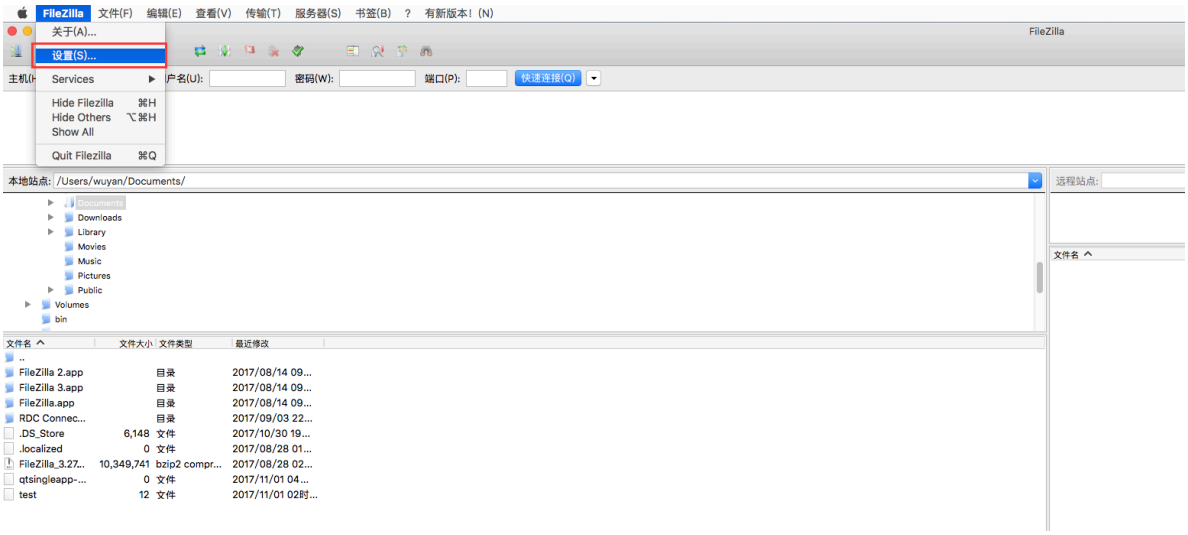
> **说明:**
> 如果管理员启用了双因子认证登录，将会提示输入双因子口令，请输入您手机上收到的6位数字。



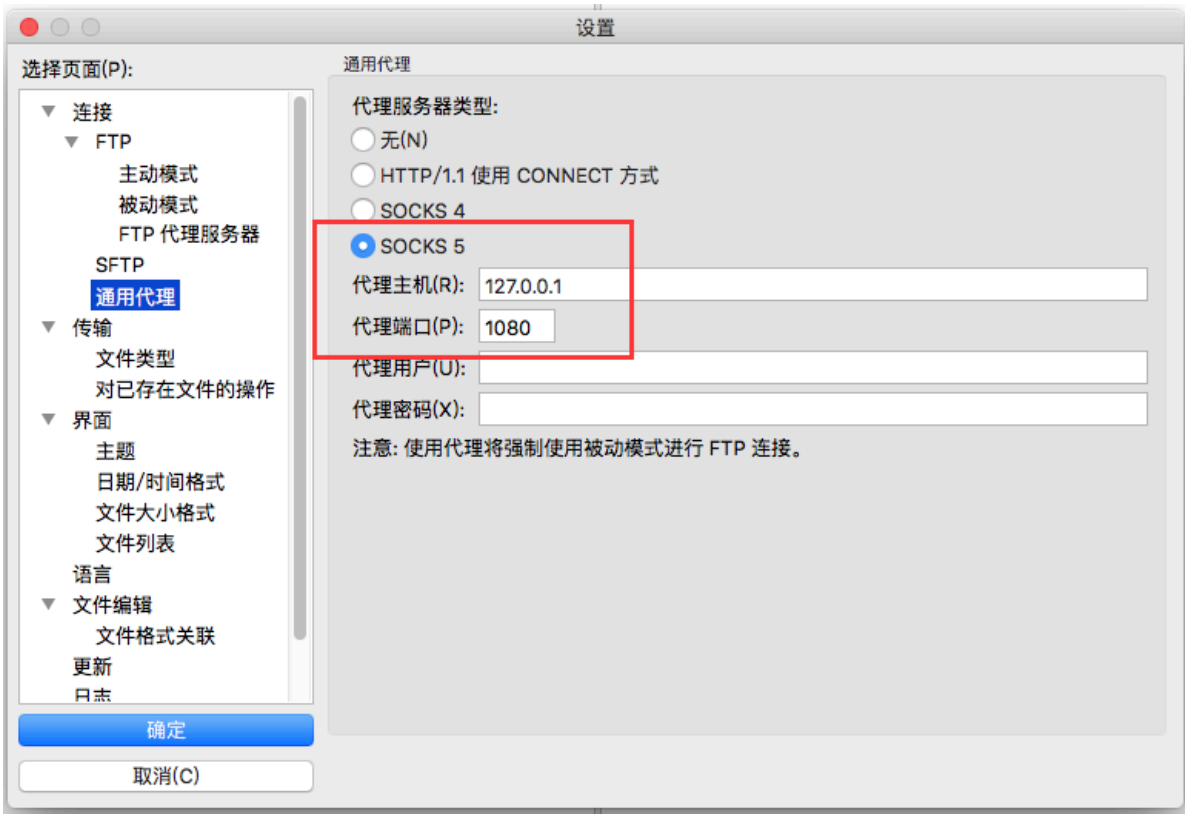
说明:

云子账号使用MFA进行二次验证。

4. **打开filezilla客户端，进入设置页面。**



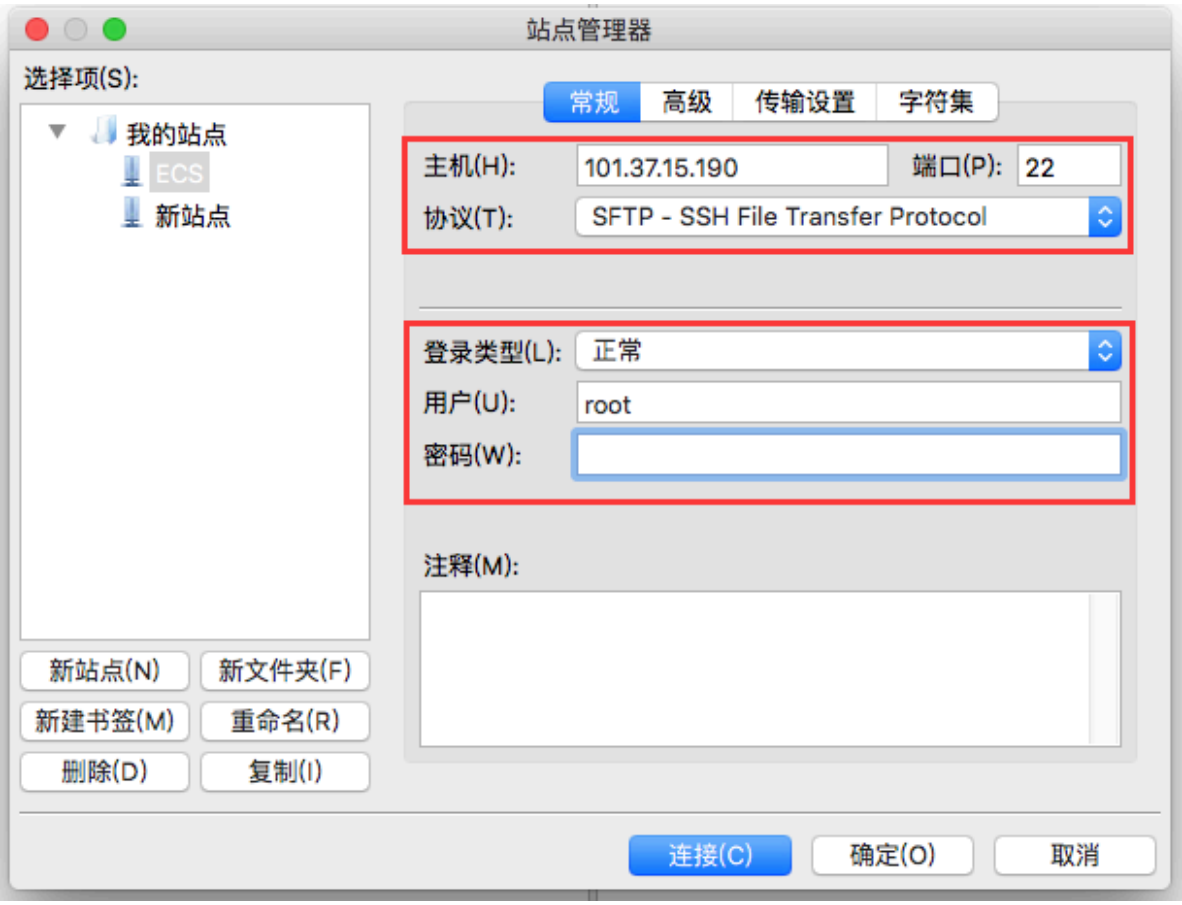
5. 单击通用代理，选择 SOCKS5，设置代理主机：127.0.0.1，端口：1080，单击确定。



6. 打开站点管理器，输入需要连接运维的服务器IP，设置端口：22；登录类型：正常；输入服务器用户名、密码。

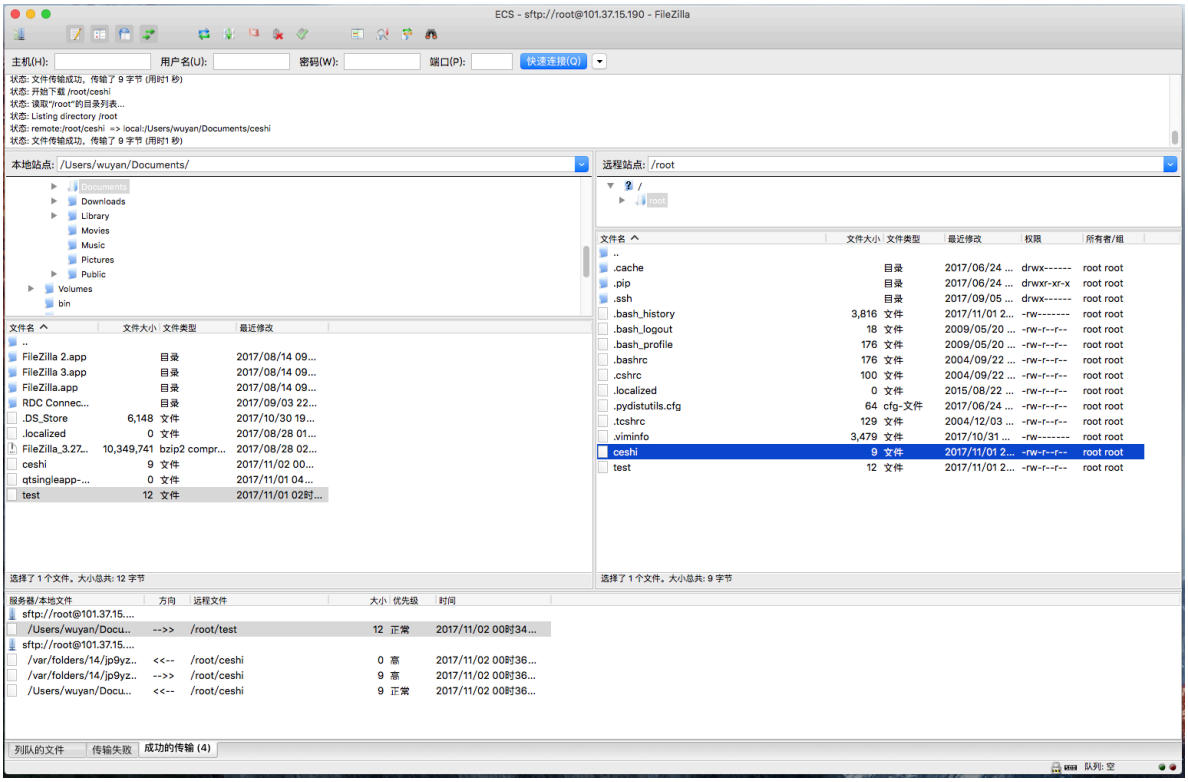
说明:

若相关授权组中已添加正确凭据，则无需输入密码。



7. **单击连接，弹出窗口选择确定。**

8. 进入远程服务器后，即可进行文件传输运维，堡垒机可正常审计。



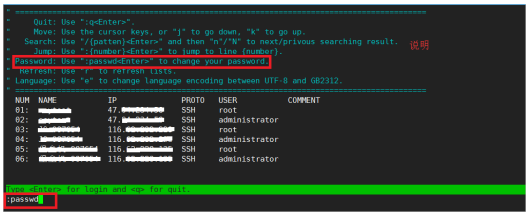
2.5 用户修改密码

本文中的修改密码指的是修改堡垒机用户密码，用户指的是通过堡垒机用户页面所创建的用户。本文中的操作步骤无法修改服务器密码与阿里云账号密码。

SSH 协议运维人员修改密码

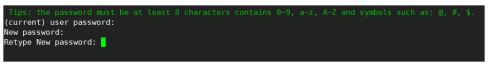
运维人员请参考SSH协议运维中的操作步骤登录云盾堡垒机后，进行以下操作进行密码修改：

1. 登录云盾堡垒机后，参考菜单界面的说明，输入：passwd命令并按 Enter 键。



2. 根据提示依次输入当前用户密码、新密码、重复新密码，并按 Enter 键。

> **说明:**
>
> 云盾堡垒机密码至少八位，且必须包含以下四项字符：大写字母、写字母、数字、非字母符号（如 @，#，$ 等）。



3. 云盾堡垒机用户密码修改成功。

RDP 协议运维人员修改密码

运维人员请参考RDP协议运维中的操作步骤登录云盾堡垒机后，进行以下操作进行密码修改：

1. 登录云盾堡垒机后，单击菜单栏下方的修改个人密码。
2. 在弹出的对话框中，依次输入当前用户密码、新密码、重复新密码，单击保存更改。

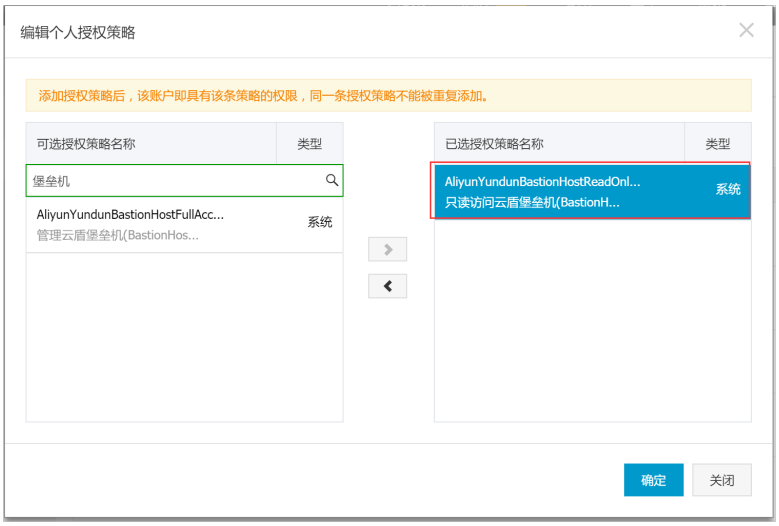
> **说明:**
> 云盾堡垒机密码至少八位，且必须包含以下四项字符：大写字母、写字母、数字、非字母符号（如 @，#，$ 等）。

3. 云盾堡垒机用户密码修改成功。

2.6 BS运维

BS运维指普通运维用户以RAM子账号身份登录堡垒机控制台并进入Web运维界面，调用本地客户端，单点登录ECS运维。该运维方式仅支持RAM子账号用户使用，可以在Windows环境下使用。

在进行BS运维前，请根据需求设置好RAM子账号权限。您可以使用主账号登录访问控制RAM-用户管理，给需要运维的RAM子账号授权。建议赋予子账号只读权限，只允许使用运维，避免子账号进入管理页面，发生越权操作。



RAM子账号登录

参照以下步骤，使用RAM子账号登录运维页面：

1. 通过RAM子账号登录界面，登录云盾堡垒机控制台。

2. 选择要操作的实例，单击运维，进入Web运维界面。

> **说明:**
> RAM子账号需要先导入堡垒机，否则可能无法看到运维按钮，导入方法参见用户管理。

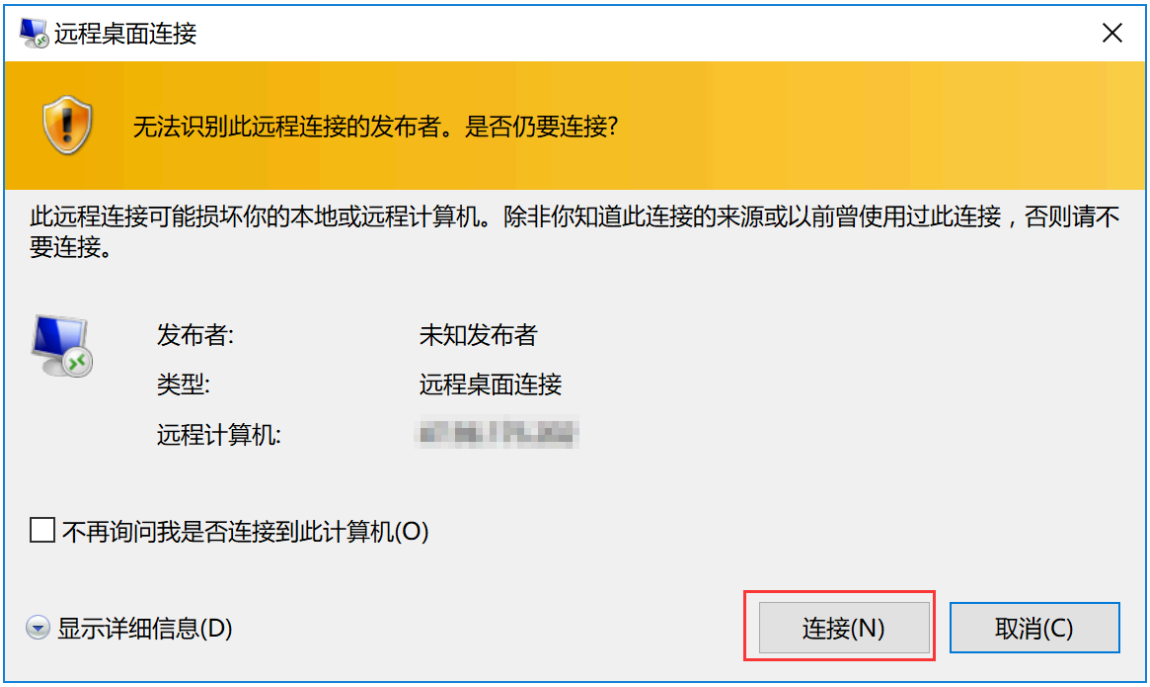
BS运维操作

使用RAM子账号登录云盾堡垒机运维页面后，可以看到该账号可以访问的服务器信息。

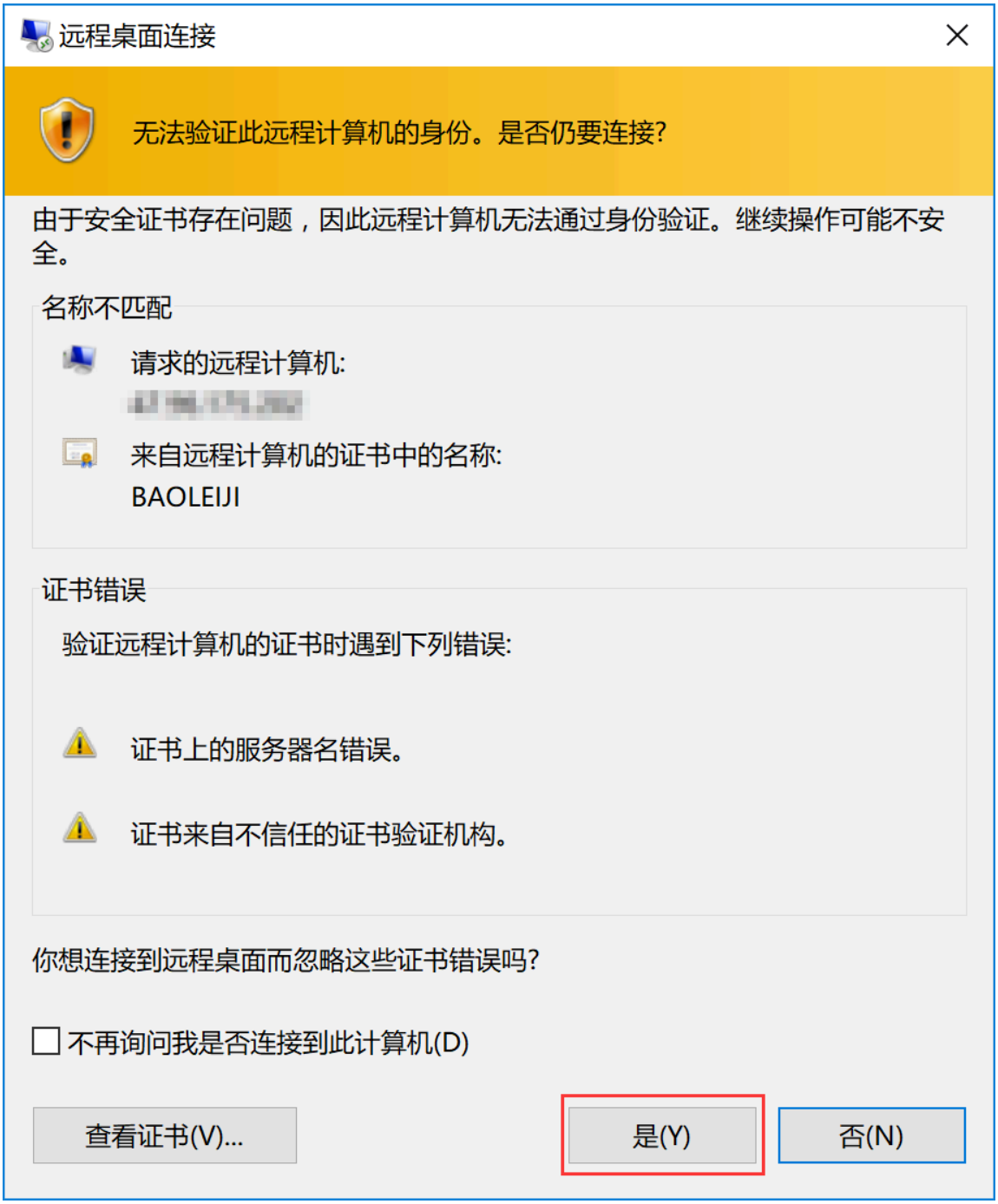
> **说明:**
> 管理员必须给RAM子账号授权相应的服务器，否则无法看到服务器信息。

- **RDP运维**

1. **选择需要登录的服务器，单击右侧RDP登录，自动调用mstsc客户端。**
2. **在弹出界面，单击连接 。**



3. **在弹出界面，单击是，成功登录服务器。**

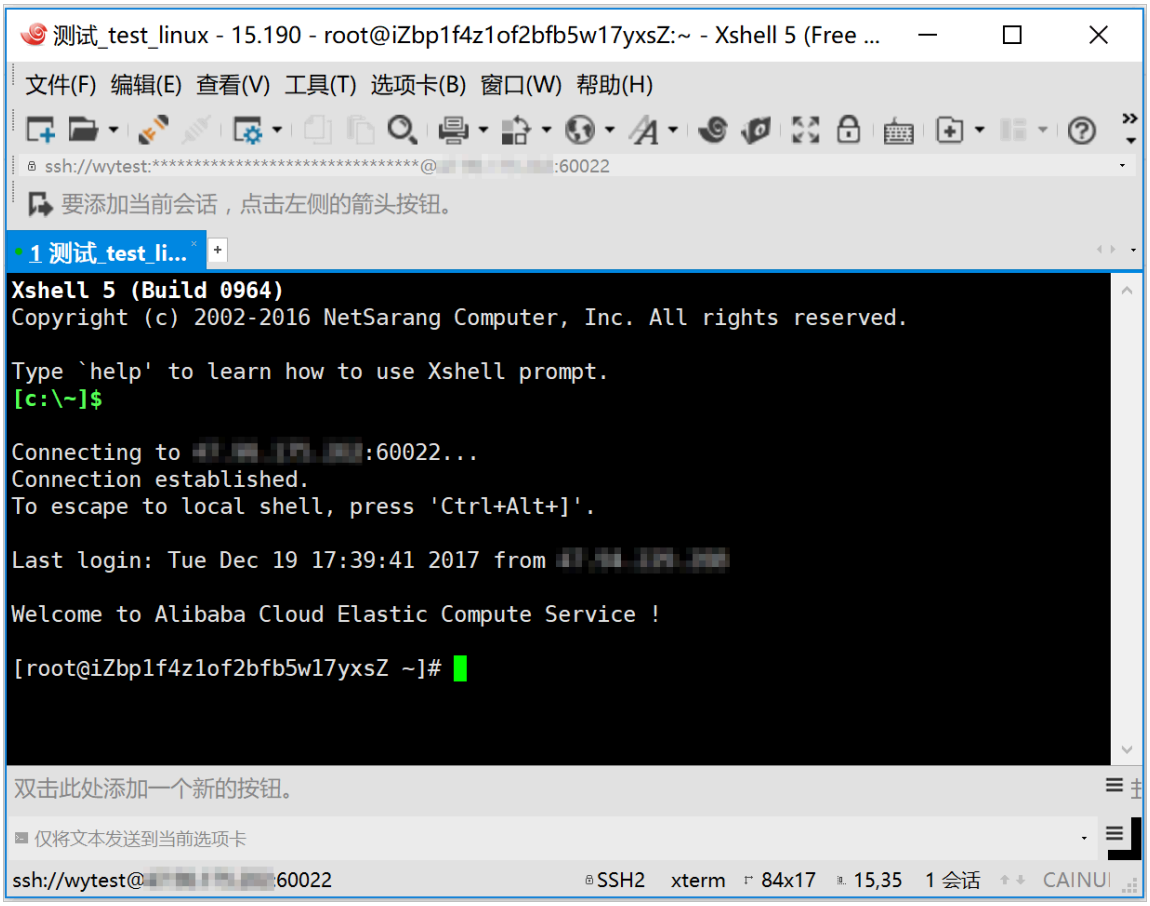


说明:

MAC环境下RDP客户端不支持自动登入服务器，您在调用RDP客户端后，需要人工选择运维的服务器，然后双击后连接进入。

- SSH运维

1. 选择需要登录的服务器，单击右侧SSH登录，自动调用所配置的SSH客户端。
2. 自动登入服务器，进行运维操作。



- SFTP运维

1. 选择需要登录的服务器，单击右侧SFTP登录，自动调用所配置的SFTP客户端。
2. 自动登入服务器，进行运维操作。