阿里云
堡垒机

用户指南（V2版本）

文档版本：20190530

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 术语介绍

基本对象

云盾堡垒机有五种对象，分别是用户、服务器、服务器组、凭据、控制策略。

- 用户：代表技术工程师，也就是自然人，云盾堡垒机目前有本地用户、云子账号用户、 AD/LDAP用户。
- 服务器：是您在阿里云上的ECS实例。
- 服务器组：是多个服务器的组合，方便归类管理，统一授权。
- 凭据：是用于登录ECS实例的用户名、密码或用户密钥。其中，
  - 凭据名称用于辨识不同的凭据。
  - 登录名为要登录的ECS上的用户名（例如administrator、root）。
  - 密码或密钥为该用户的密码或密钥。
- 控制策略：用于对运维操作行为做策略控制。云盾堡垒机支持RDP协议上传下载控制、来源IP控制、访问时间段控制、SSH命令控制。

授权组

授权组是将堡垒机中数个独立的对象联系在一起的概念，通过授权组功能可以达到控制某个用户只能访问他权限内服务器的目的。

以下通过示例帮助您更好地理解授权组的概念：

您在阿里云上共10个ECS实例，其中：

- 应用服务器2个（APP1、APP2）
- 数据库服务器2个（DB1、DB2）
- 中间件服务器2个（M1、M2）
- 开发测试服务器4个（TEST1-4）

您单位共有三类工作人员：

- 开发人员（devuser）：负责开发产品原型以及测试
- 运维人员（opsuser）：负责维护线上服务器和应用系统
- 管理员（adminuser）：全面协调公司内部技术人员工作，并定期进行审计

您在ECS实例中使用三种主机账号：

- dev（不能sudo）
- ops（可以sudo）

- shadow_r00t（可以sudo）

在这样的情况下，您可以按照如下策略配置授权关系：

云盾账号	ECS主机	主机账号	说明
devuser	TEST1-4	dev	开发人员只能使用开发机，且使用不能sudo的账号防止基础系统配置被篡改。
opsuser	APP1、APP2、DB1、DB2、M1、M2	ops	运维人员使用可以sudo的账号维护主机基础系统配置。
adminuser	所有	shadow_r00t	管理员使用可以sudo的账号登录系统。

根据这样的授权关系配置进行授权组配置就可以实现职责明晰的技术管理策略：

- 开发人员对开发测试服务器有完全的控制权限。
- 运维人员控制生产服务器。
- 管理员可以访问所有设备，并通过云盾堡垒机Web管理页面进行审计。

关于详细授权组操作步骤，请参考授权组管理。

运维

云盾堡垒机的运维操作可以通过连接协议代理端口实现。

默认链接协议规则如下表：

运维协议	端口号	四层协议
SSH	60022	TCP
Windows远程桌面	63389	TCP
SFTP	60022	TCP

您可以使用标准协议客户端（如 Xshell、SecureCRT、PuTTY、及Windows 远程桌面客户端等工具）直接连接规则表中的端口号，并使用堡垒机用户名、密码进行登录。成功登录堡垒机后，根据提示即可对授权服务器进行相关运维操作。

关于登录堡垒机进行运维的详细操作步骤，请参考：

- MAC电脑运维
- SSH协议运维

- SFTP协议运维
- RDP协议运维

审计

云盾堡垒机的审计分为两种：实时监控和录像回放。

- 实时审计：专注于事中控制，您可以通过云盾堡垒机Web管理页面随时切入某个运维会话查看现场操作。
- 录像回放：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。支持通过时间段、手机号、服务器 IP、ECS 实例 ID、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。

关于审计相关的详细操作步骤，请参考：

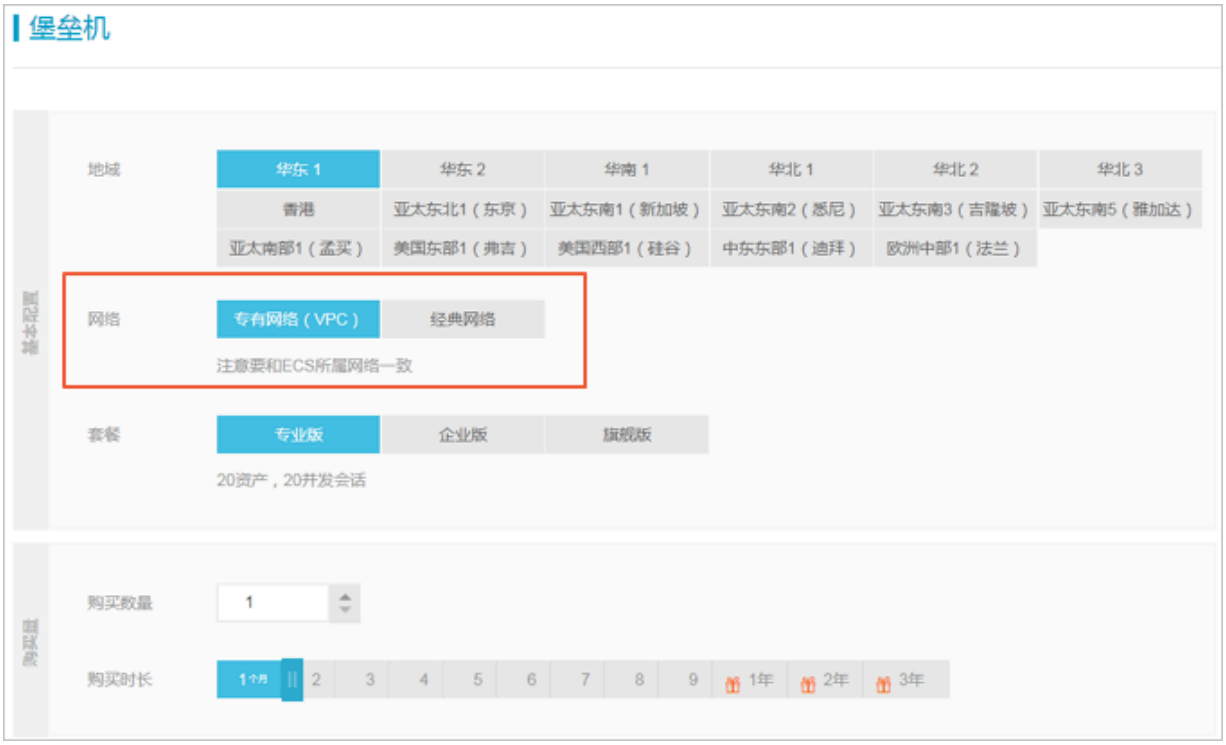
- 实时会话
- 录像回放
- 指令查询

2 管理员手册

2.1 网络配置

选择网络类型

在购买云盾堡垒机实例时，除了选择地域、套餐、购买时长外，您还需要选择云盾堡垒机实例所使用的网络类型。



建议您选择与所需接入堡垒机系统进行运维的ECS服务器相同的网络类型：

- 如果ECS服务器都处于专有网络环境，堡垒机实例的网络应选择专有网络（VPC）。
- 如果ECS服务器都处于经典网络环境，堡垒机实例的网络应选择经典网络。
- 如果需要接入ECS服务器既有专有网络环境也有经典网络环境，建议您的堡垒机实例的网络选择专有网络（VPC）。

购买云盾堡垒机实例后，您需要在云盾堡垒机管理控制台中启用该实例，然后才能登录云盾堡垒机系统。

启用专有网络（VPC）类型的堡垒机实例

参考以下操作步骤，启用您已购买的专有网络类型的堡垒机实例：

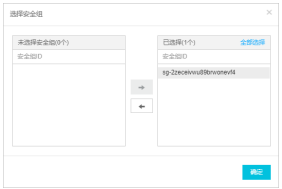
1. 在云盾堡垒机管理控制台中，选择已购买的云盾堡垒机实例，单击启用。

2. 选择专有网络和交换机。

> **说明:**
> 建议您选择与所需运维的ECS实例相同的专有网络。这样，堡垒机系统即可通过内网访问同一专有网络VPC环境中的ECS实例。

> **说明:**
> 如果收到以下错误提示，则表示该交换机所在的可用区已无可启用实例。建议在其它可用区新建一个虚拟交换机，重新启用堡垒机实例。

3. 单击选择安全组，选择经典网络环境中已有的安全组，单击确定。



> **说明:**
> 选择安全组后，系统会自动在对应的安全组中创建一条访问控制规则，允许堡垒机系统访问该安全组中的ECS实例。

> **说明:**
> 系统并不是将堡垒机实例直接添加至进所选择的安全组中，而是在安全组中添加以下规则允许堡垒机实例访问安全组中的ECS实例。

说明:

请勿删除该安全组规则。

4. 设置公网访问控制，单击确定，堡垒机实例的状态变为初始化中。

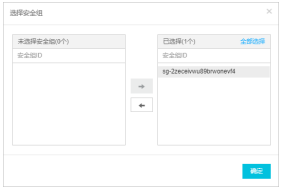
10分钟后，刷新云盾堡垒机管理控制台页面查看堡垒机实例状态，如状态变更为有效，则堡垒机实例启用成功。

启用经典网络类型的堡垒机实例

参考以下操作步骤，启用您已购买的经典网络类型的堡垒机实例：

1. 在云盾堡垒机管理控制台中，选择已购买的云盾堡垒机实例，单击启用。

2. 单击选择安全组，选择经典网络环境中已有的安全组，单击确定。



说明:

选择安全组后，系统会自动在对应的安全组中创建一条访问控制规则，允许堡垒机系统访问该安全组中的ECS实例。

说明:

系统并不是将堡垒机实例直接添加至进所选择的安全组中，而是在安全组中添加以下规则允许堡垒机实例访问安全组中的ECS实例。

说明:

请勿删除该安全组规则。

3. 设置堡垒机系统的网络访问控制。

说明:

堡垒机实例启用后，您可以单击网络配置修改访问控制策略。

- 内网访问控制：此处添加的为堡垒机系统的登录白名单，即只有添加在内网访问控制框中的内网IP可访问堡垒机。例如，您可以在此处添加VPN服务器的内网IP。

  说明:

  不添加内网IP则表示堡垒机系统对内网访问无限制。
- 公网访问控制：此处可对堡垒机系统的公网访问进行控制。

4. 单击确定后，堡垒机实例的状态变为初始化中。

10分钟后，刷新云盾堡垒机管理控制台页面查看堡垒机实例状态，如状态变更为有效，则堡垒机实例启用成功。

网络配置FAQ

无法通过公网IP登录堡垒机系统

请检查堡垒机实例网络配置中的公网访问控制选项，确认公网访问方式已启用，或者您用于登录的IP已添加至公网白名单中。

说明:

华东1地域的金融云用户无法通过公网IP登录堡垒机系统。

无法通过内网IP登录堡垒机系统

请检查你的客户端是否可以与堡垒机系统处于同一专有网络VPC环境中的其他ECS服务器。

- 如果无法连通，请检查VPN服务器状态。
- 如果可以连通，请尝试通过同一专有网络VPC环境中的其它ECS服务器登录堡垒机系统。如果登录成功，则请检查VPN服务器。

说明:

如果堡垒机实例的网络类型为经典网络，请检查网络配置中的内网访问控制是否存在相关限制。

通过堡垒机系统登录ECS服务器的公网IP失败

请尝试不通过堡垒机系统直接访问该ECS服务器的公网IP。

- 如果无法登录，请检查该ECS服务器的状态。
- 如果可以登录，请检查该ECS服务器的安全组中是否有堡垒机系统自动添加的规则。如果没有相关安全组规则，您需要在堡垒机实例的网络配置中重新添加一次相关的安全组。

说明:

部分金融云账号默认禁止使用公网IP登录ECS服务器，您必须通过内网IP登录ECS服务器。

通过堡垒机系统登录ECS服务器的内网IP失败

请检查堡垒机实例与目标ECS服务器是否在同一专有网络VPC环境或经典网络环境。

- 如果目标ECS服务器与堡垒机不在同一网络环境，则无法通过内网连通，您必须通过公网IP登录该ECS服务器。
- 如果目标ECS服务器与堡垒机处于同一网络环境，请检查该ECS服务器所在的安全组，确认已对堡垒机系统开放访问相关运维端口的权限。

2.2 服务器管理

在云盾堡垒机的Web管理页面，您可以执行以下服务器相关的操作：添加、启用/禁用、修改、移除。

添加服务器

您可以使用三种方式来添加服务器：同步阿里云ECS、手动添加、和批量添加。

同步阿里云ECS

同步ECS云服务器指将您阿里云账号中的ECS实例列表同步到云盾堡垒机系统中。该操作不会影响您阿里云账号中的 ECS 实例的现有状态。参照以下步骤同步阿里云ECS：

1. 登录到云盾堡垒机Web管理页面。
2. 定位到资产 > 服务器页面，单击页面右上角的同步阿里云ECS。

说明:

若需要将ECS按ECS标签分别添加到不同的服务器组，请在系统 > 系统配置中勾选同步ECS标签。

3. 在同步阿里云ECS对话框中，单击手工刷新以获取最新ECS信息。

说明:

如果堡垒机无法正常获取您云账号中的ECS云服务器列表，请确认您已在云盾堡垒机管理控制台中的实例列表页面授权堡垒机系统读取ECS列表信息。

4. 勾选所需添加的云服务器，单击加入云堡垒机。

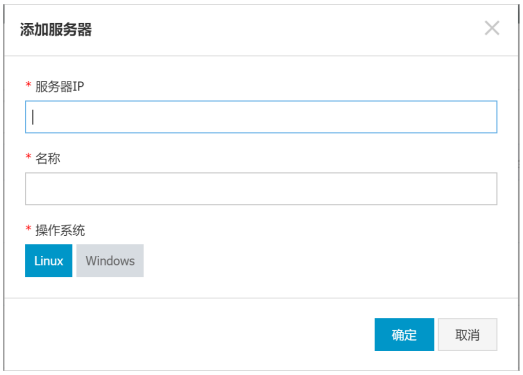
手动添加服务器

参照以下步骤手动添加服务器：

1. 登录到云盾堡垒机Web管理页面。
2. 定位到资产 > 服务器页面，单击页面右上角的 添加服务器。

说明:

手动添加服务器可以是外部主机，确保该主机与堡垒机网络互通即可。

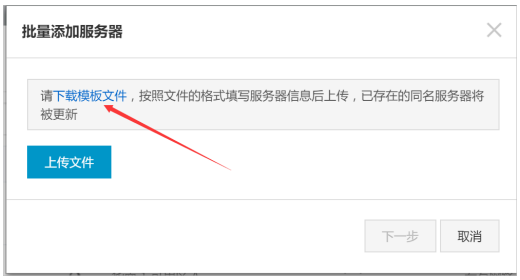


3. 在添加服务器对话框中，填写服务器信息后，单击确定完成添加。

批量添加服务器

参照以下步骤手动添加服务器：

1. 登录到云盾堡垒机Web管理页面。
2. 定位到资产 > 服务器页面，单击页面右上角的 批量添加服务器。
3. 在批量添加服务器对话框中，单击下载模板文件将模板文件下载到本地。



4. 根据模板文件格式要求填写服务器信息后，单击上传文件，将服务器信息文件上传，单击下一步。
5. 确认添加的服务器信息无误后，单击确定完成批量添加。

启用/禁用服务器

参照以下步骤启用/禁用服务器：

1. 登录到云盾堡垒机Web管理页面。
2. 定位到资产 > 服务器页面，勾选您想要启用或禁用的服务器，单击列表下方的启用或禁用。

说明：

您可以单击列表最下方单选框全选本页全部服务器，再选择启用或禁用，则可以启用/禁用本页全部服务器。

操作完成后，查看该服务器右侧对应状态是否为启用/禁用，检验操作是否成功

修改服务器

登录到云盾堡垒机Web管理页面，定位到资产 > 服务器，您可对已添加的服务器进行修改。

- 勾选您想要修改的服务器，单击修改端口。您可在弹出的对话框中根据您服务器的实际情况更改 SSH 和 RDP 协议端口的相关配置。

- 勾选您想要修改的服务器，单击配置连接IP。您可在弹出的对话框中根据需要更改连接 IP 的相关配置。

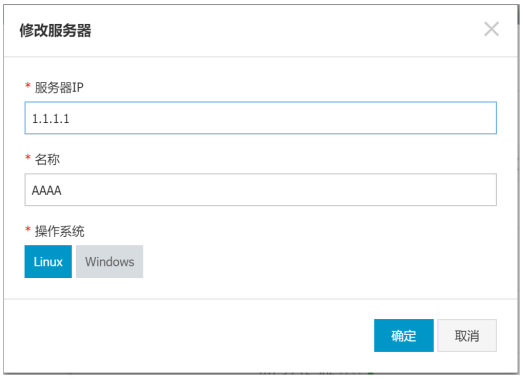
说明:

连接 IP 配置只对拥有公网 IP 和内网 IP 的阿里云ECS云服务器生效。

- 选择您想要修改的服务器，单击右侧的编辑。您可在弹出的对话框中修改普通服务器的信息。

说明:

编辑功能只适用于通过手动方式或批量方式添加的服务器。



移除服务器

移除服务器是指从云盾堡垒机列表中将服务器移除，该操作不会影响您帐号中的ECS实例及其他服务器。参照以下步骤移除服务器：

1. 登录到云盾堡垒机Web管理页面。
2. 定位到资产 > 服务器页面，勾选您想要移除的服务器，单击列表下方的移除。

> **说明：**
> 您可以单击列表最下方单选框全选本页全部服务器，再选择移除，则可以移除本页全部服务器。

3. 确认无误后，在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

2.3 授权组管理

在云盾堡垒机Web管理页面，您可以执行以下授权组相关操作：新建、修改、克隆、删除。

新建授权组

参照以下步骤新建授权组：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权组，单击新建授权组。
3. 在弹出的对话框中填写新授权组的名称，单击确定。

4. 配置已创建的授权组的基本对象。

- 服务器/服务器组

a. 选择已创建的授权组，单击服务器/服务器组栏中的数字。

b. 在授权组：服务器/服务器组对话框中，勾选一个或多个服务器/服务器组，单击加入授权组。

- 用户

a. 选择已创建的授权组，单击用户栏中的数字。

b. 在授权组：用户对话框中，选择一个或多个用户，单击加入授权组。

- 凭据

a. 选择已创建的授权组，单击凭据栏中的数字。

b. 在授权组：凭据对话框中，勾选一个或多个凭据，单击加入授权组。

- 控制策略

a. 选择已创建的授权组，单击控制策略栏中的文字。

b. 在更改控制策略对话框中，选择一个控制策略，单击加入授权组。

修改授权组

参照以下步骤修改授权组：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权组，选择您需要修改的授权组，单击右侧的修改名称。

3. 在弹出的对黄框中修改授权组名，单击确定。

克隆授权组

参照以下步骤克隆授权组：

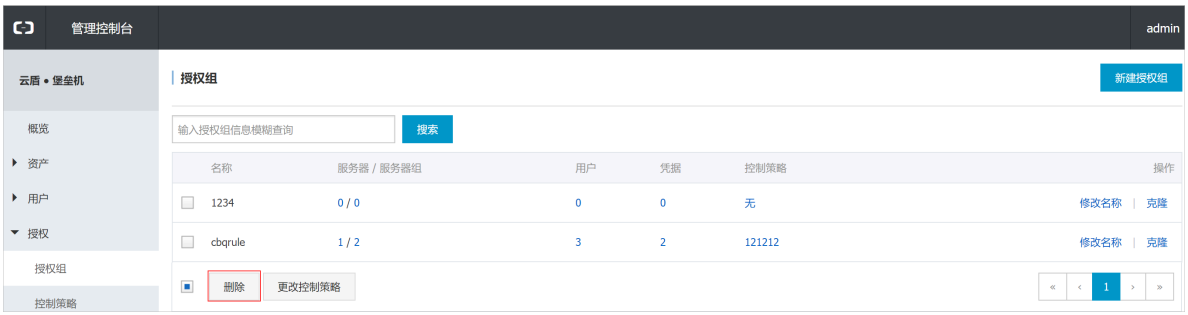
1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权组，选择您需要克隆的授权组，单击右侧的克隆。

3. 在弹出的对话框中填写通过克隆创建的授权组名称，单击确定。

删除授权组

参照以下步骤删除授权组：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权组，勾选您需要删除的授权组，单击列表下方的删除。



3. 在弹出的对话框中，单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

2.4 双因子认证

开启双因子认证之后，运维人员登录云服务器时，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/MFA）才能登录成功。

背景信息

双因子认证有如下几种情况：

- 使用密码运维登录
  - 本地用户和AD/LDAP用户要使用手机验证码进行二次验证。
  - 云子帐号无论是否勾选此项都需要使用MFA进行二次验证。
- 使用公钥运维登录
  - 本地用户和AD/LDAP用户要使用手机验证码进行二次验证。
  - 云子帐号在勾选此项后需要使用MFA进行二次验证。

参照以下步骤启用/禁用双因子认证：

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。
4. 定位到 系统 > 系统设置页面，在双因子认证下勾选或取消勾选对应功能选项。

5. 单击保存设置，刷新页面查看操作是否成功。

2.5 操作日志管理

操作日志是指管理员操作、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。

背景信息

参照以下步骤查看和查询操作日志：

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。
4. 定位到操作日志页面，查看所有操作日志，您可以选择以下搜索方式进行查询：

说明：

支持设置多个搜索条件，单击清空可清空已设置的条件。

- 按照操作日期搜索：单击操作日期文本框并设置日期范围，单击搜索。

- 按日志类型搜索：单击日志类型文本框并选择日志类型（资产、用户、授权组、运维、其他），单击搜索。

- 按操作结果搜索：单击操作结果文本框并选择成功或失败，单击搜索。
- 按日志内容搜索：在日志内容文本框中输入要在日志内容中搜索的关键字，单击搜索。

2.6 AD/LADP配置

本文受众范围：云盾堡垒机管理员、持有阿里云账号的管理员。

云堡垒机与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。

AD域设置

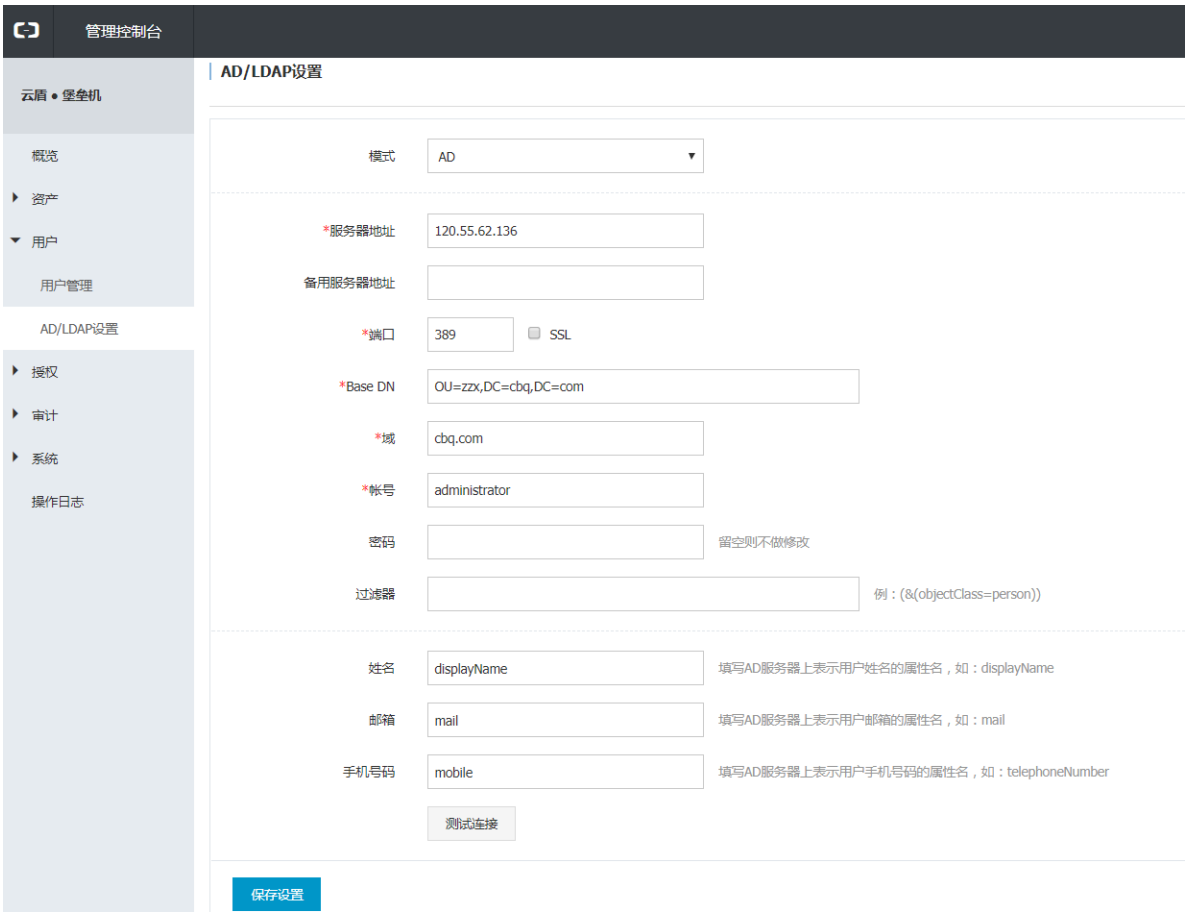
1. 登录堡垒机Web管理页面，进入用户AD/LDAP设置，将模式调整为AD 。
2. 在页面内依次填入AD服务器IP、端口、要同步的用户所在的组织、域名、域用户账号、密码，以及姓名、邮箱、手机号码等属性字段名称（带*为必填项）。

说明:

需保证填入的用户账号有权限访问Base DN 。

说明:

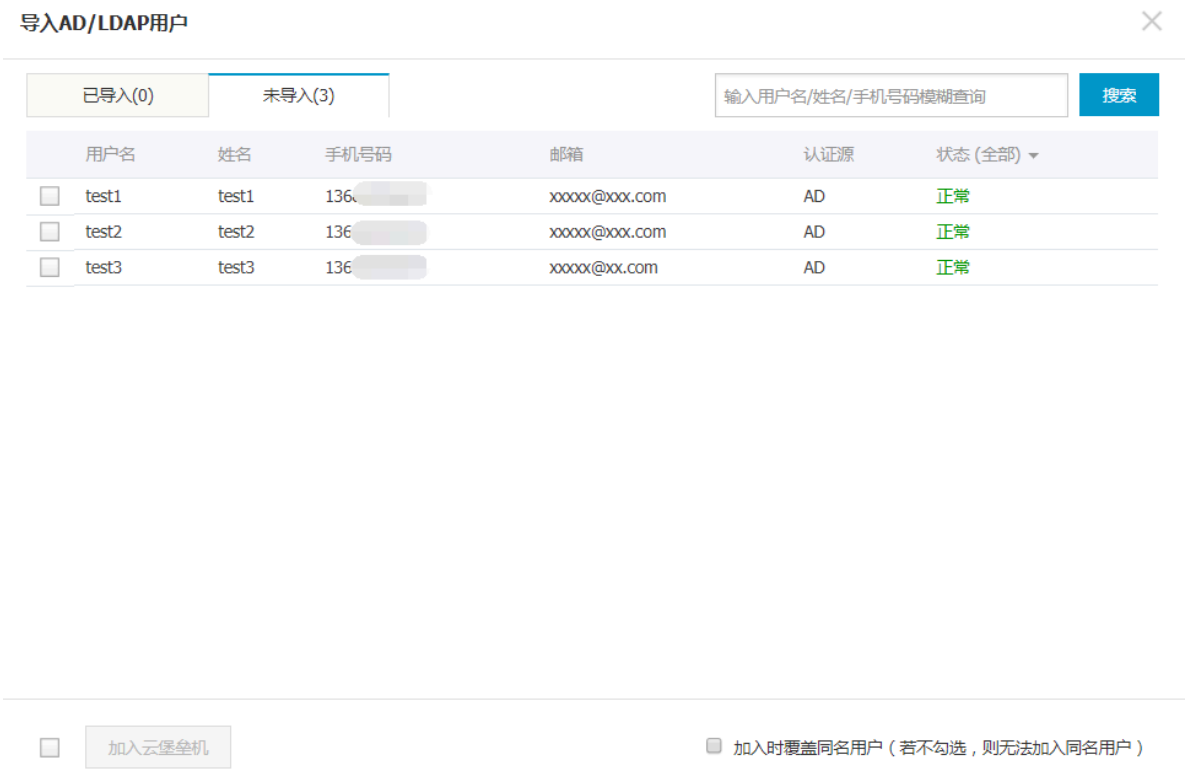
若拉取的用户无手机号码属性，或内容为空，同步下来的用户手机号字段将置空，若打开设置中的二次认证选项，同步的用户将无法登录堡垒机 。



3. 配置完成后，单击页面下方测试连接，若结果如图所示，单击保存设置。

若结果如下图所示，则证明堡垒机与AD服务器之间网络或端口不通，需对网络进行排查。

4. 配置完成后，进入堡垒机用户 > 用户管理菜单，单击右上方导入AD/LDAP用户，可将Base DN中的用户加入至堡垒机。

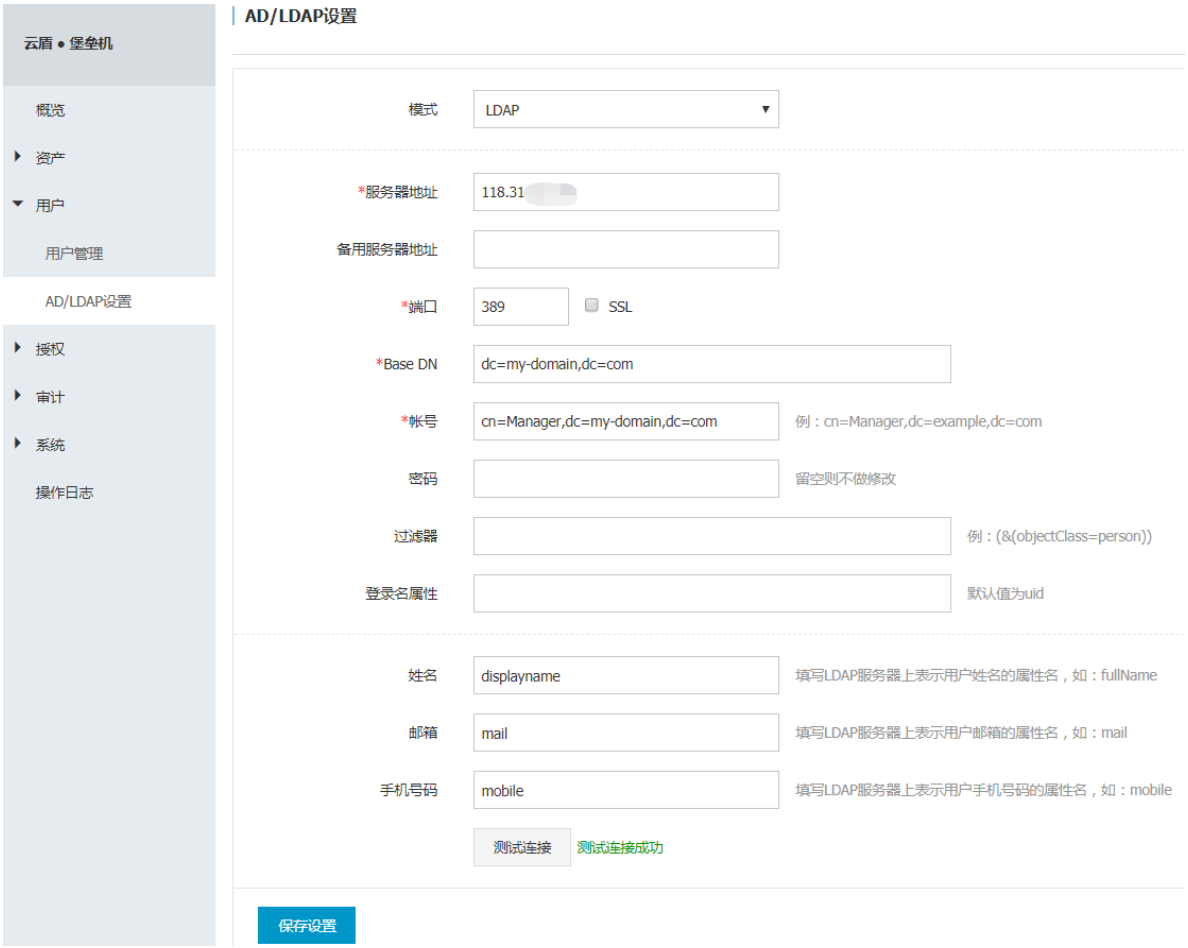


5. 用户加入堡垒机后，可以运维登录操作。

LDAP设置

1. 登录堡垒机Web管理页面，进入用户 > AD/LDAP设置菜单，将模式调整为LDAP。

2. 在页面依次填入LDAP服务器信息。



3. 测试连接通过后，保存设置。

4. 参考AD域设置，导入用户，并使用LDAP用户进行认证登录。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

2.7 配置备份管理

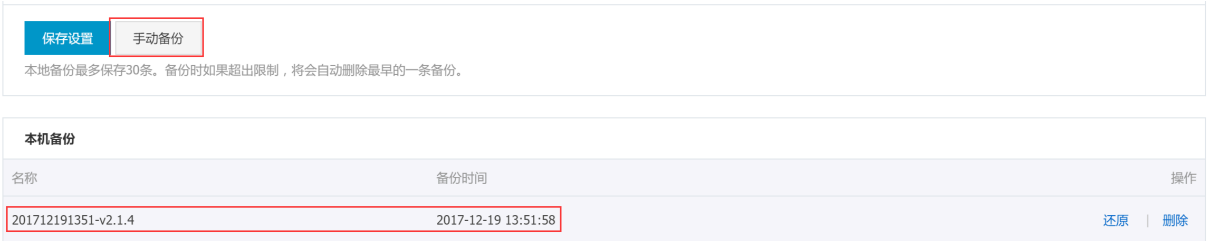
本文受众范围：云盾堡垒机管理员、持有阿里云账号的管理员。堡垒机配置包含所有配置数据，如用户、资产、授权、系统等配置数据，不包含审计日志。

自动配置备份

登录云盾堡垒机Web管理页面，定位到系统 > 配置备份管理，选择启用自动备份，设置备份周期，单击保存设置 。

手动配置备份

登录云盾堡垒机Web管理页面，定位到系统 > 系统备份管理，单击手动备份，自动生成一条备份记录。

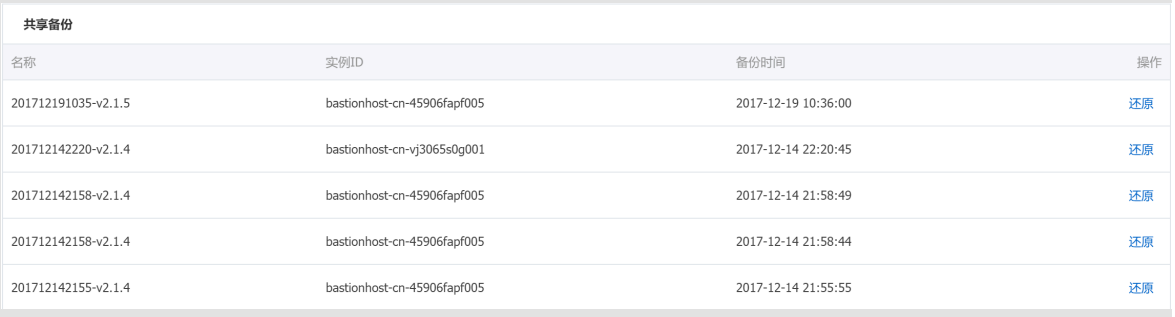


共享备份

1. 登录云盾堡垒机Web管理页面，定位到系统 > 配置备份管理，选择勾选下图选项，单击保存设置。

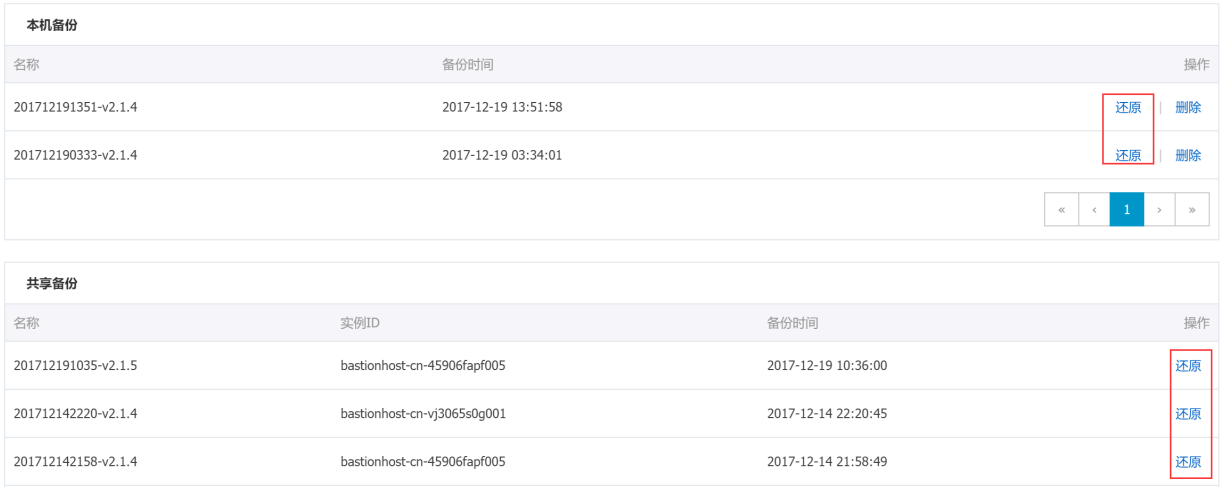
2. 使用该账号下其他堡垒机登录堡垒机Web管理页面，定位到系统 > 配置备份管理，共享备份将出现上面堡垒机配置备份数据。

> **说明：**
> 共享账号只能在同一个账号下不同堡垒机之间使用。



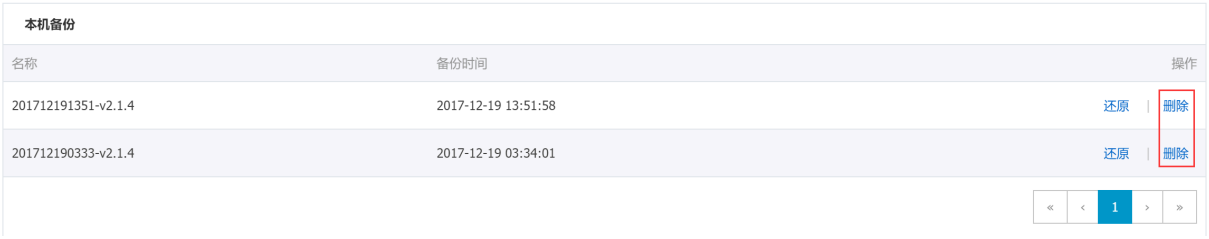
还原备份

登录云盾堡垒机Web管理页面，定位到系统 > 配置备份管理，在本机备份或共享备份列表中，选择一条记录，单击还原，自动还原该备份数据。



删除备份

登录云盾堡垒机Web管理页面，，定位到系统 > 配置备份管理，在本机备份列表中，选择一条记录，单击删除，自动删除该备份数据。



如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

2.8 控制策略管理

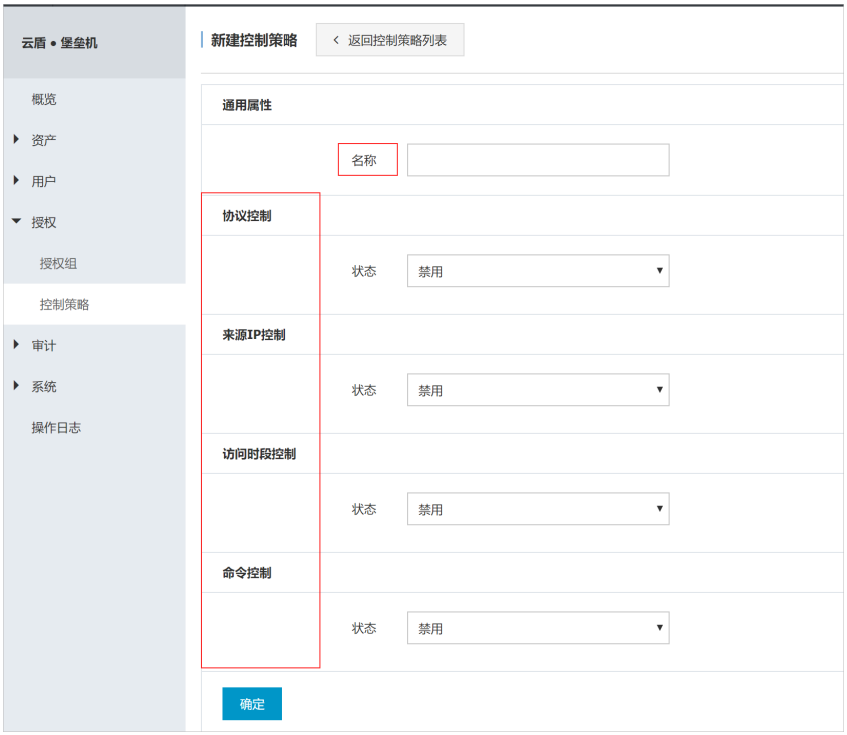
在云盾堡垒机Web管理界面，您可以执行以下与控制策略相关的操作：新建、编辑、克隆、删除。

新建控制策略

参照以下步骤新建控制策略：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权策略，单击新建控制策略。

3. 在新建控制策略页面，填入控制策略名称，选择启用并编辑需要的控制策略。您可以选择启用的控制策略包括：



- 协议控制：选择启用，展开协议控制选项，根据自身需求勾选需要控制的项目。

- 来源IP控制：选择启用 ，展开来源IP控制输入框，填入允许访问的IP或IP段。

- 访问时间段控制：选择启用，展开访问时间控制选项，选择编辑允许访问的时间段。

- 命令控制：选择启用，展开命令控制输入框（只针对SSH字符命令有效），填入需要禁止的命令。

4. 全部策略编辑完成后，单击确定，返回控制策略列表可看到新建的控制策略。

编辑控制策略

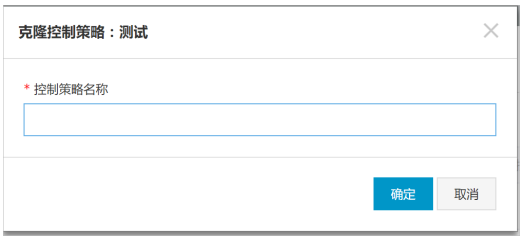
参照以下步骤编辑控制策略：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权策略，选择您需要编辑的控制策略，单击右侧的编辑。
3. 在进入编辑页面后，进行相应的修改编辑，修改完成后单击确定。

克隆控制策略

参照以下步骤克隆控制策略：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权策略，选择您需要编辑的控制策略，单击右侧的克隆。
3. 在弹出的对话框中填写通过克隆创建的控制策略名称，单击确定。



删除控制策略

参照以下步骤删除控制策略：

1. 登录云盾堡垒机Web管理页面。
2. 定位到授权 > 授权策略，勾选您需要删除的控制策略，单击删除。

3. 确认无误后，在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

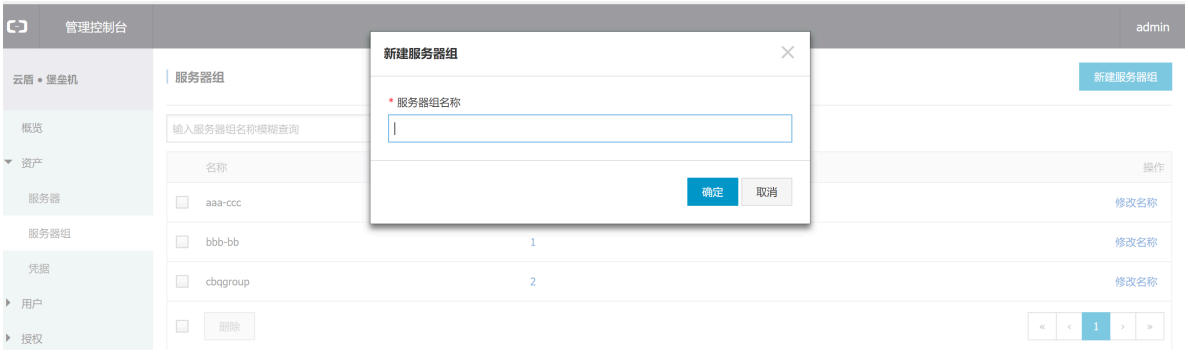
2.9 服务器组管理

本文受众范围：云盾堡垒机管理员、持有阿里云账号的管理员。

新建服务器组

1. 登录云盾堡垒机Web管理页面，定位到资产 > 服务器组，单击页面右上角的新建服务器组。

2. 在新建服务器组窗口中，填写服务器组名称后，单击确定。



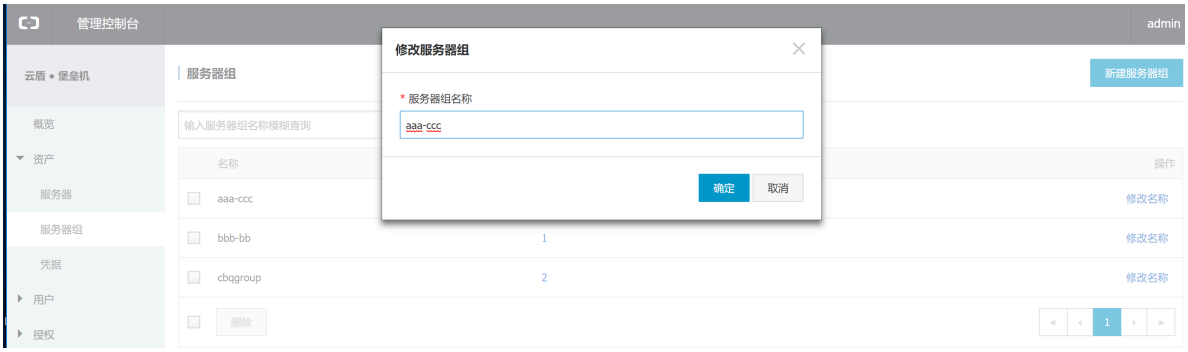
修改服务器组名称

1. 登录云盾堡垒机Web管理页面，定位到资产 > 服务器组，单击修改名称。

2. 在修改服务器组窗口中，修改服务器组名称后，单击确定。

说明:

修改由ECS标签同步过来的服务器组名称，不会影响ECS标签信息。



删除服务器组

1. 登录云盾堡垒机Web管理页面，定位到资产 > 服务器组，勾选您想要移除的服务器，单击列表下方的删除。

2. 确认无误后，在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

2.10 用户管理

在云盾堡垒机Web管理页面，您可以执行以下与用户相关的操作：新建本地用户、新建/导入云子账号、导入AD/LDAP用户、修改用户、配置公钥、搜索用户、删除用户。

新建本地用户

参照以下步骤新建本地用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，单击新建本地用户。

3. 在新建本地用户对话框中填写以下用户信息：

- 手机号码：必填，填写11位真实手机号。
- 密码：必填，由8到64个字符组成，必须同时包含大小写字母、数字、和特殊符号（@#$）。
- 邮箱：选填，如果填写则必需使用真实且符合规范的邮箱地址。
- 姓名：选填。

新建云子账号

参照以下步骤新建云子账号：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，单击新建云子账号。

3. 在子账号管理页面，您可以执行以下操作：

- 导入子账号

  a. 单击导入子账号，直接导入RAM子账号信息。

  b. 在导入阿里云子账号用户对话框，勾选需要导入的子账号，单击导入子账号。

- 新建子账号

  a. 单击新建子账号，页面跳转至访问控制 RAM的用户管理页面。

  b. 在RAM用户管理页面新建RAM子账号，具体操作见用户管理。

- 编辑子账号

  a. 选择要修改的子账号，单击其操作列下的编辑，页面跳转至访问控制 RAM的用户管理页面。

  b. 在RAM用户管理页面修改目标子账号信息，具体操作见用户管理。

- 移除子账号：选择要删除的子账号，单击其操作列下的移除，将其从云盾堡垒机子账号列表中移除。

  说明：
  该操作不会影响访问控制 RAM中的子账号信息。

- 解锁子账号：选择要解锁的子账号，单击其操作列下的解锁，将其锁定状态解除。

  说明：
  使用子账号登录时，如果在一小时内密码错误4次，则子账号会被锁定。

- 刷新子账号数据：单击列表下方刷新子账号数据，可以从访问控制 RAM 同步RAM子账号信息到堡垒机子账号管理。

导入云子账号

参照以下步骤导入云子账号：

1. 登录云盾堡垒机Web管理页面。

2. 定位到用户 > 用户管理，单击导入云子账号。
3. 当堡垒机自动获取云子账号信息后，在弹出的对话框中勾选所需添加的云子账号，单击加入云堡垒机。

导入AD/LDAP用户

参照以下步骤导入AD/LDAP用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，单击导入AD/LDAP用户。

> **说明：**
> 您必须先在用户 > AD/LDAP设置页面配置好AD/LDAP服务器器信息。

3. 当堡垒机自动获取AD/LDAP用户信息后，在弹出的对话框中勾选所需添加的用户，单击加入云堡垒机。

修改用户

参照以下步骤修改用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，选择您想要修改的本地用户，单击右侧的修改。

> **说明：**
> 修改操作只针对本地用户，其他用户无法修改。

3. 在修改用户对话框中，修改用户信息，单击确定。

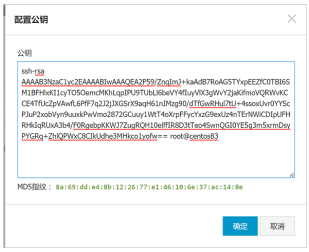
配置公钥

参照以下步骤配置公钥：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，选择您想要配置公钥的本地用户，单击右侧的配置公钥。

> **说明：**
> 用户配置公钥后，SSH协议运维操作就可以通过公私密钥对的方式登录堡垒机。

3. 在配置公钥对话框中，配置用户公钥信息，单击确定。



搜索用户

参照以下步骤搜索用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，在用户列表上方的搜索框中填写姓名、手机号码、或邮箱，单击搜索，即可对填写的字段进行模糊查询。

删除用户

参照以下步骤删除用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，勾选您需要删除的用户，单击用户列表下方的删除。

> **说明：**
> 您也可以单击用户列表下方的单选框勾选本页所有用户，然后单击删除。

3. 确认无误后，在弹出的对话框中单击确定。

启用/禁用用户

参照以下步骤删除用户：

1. 登录云盾堡垒机Web管理页面。
2. 定位到用户 > 用户管理，勾选您想要禁用或启用的用户，单击列表下方的启用或禁用。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面：

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。

3 运维使用手册

3.1 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

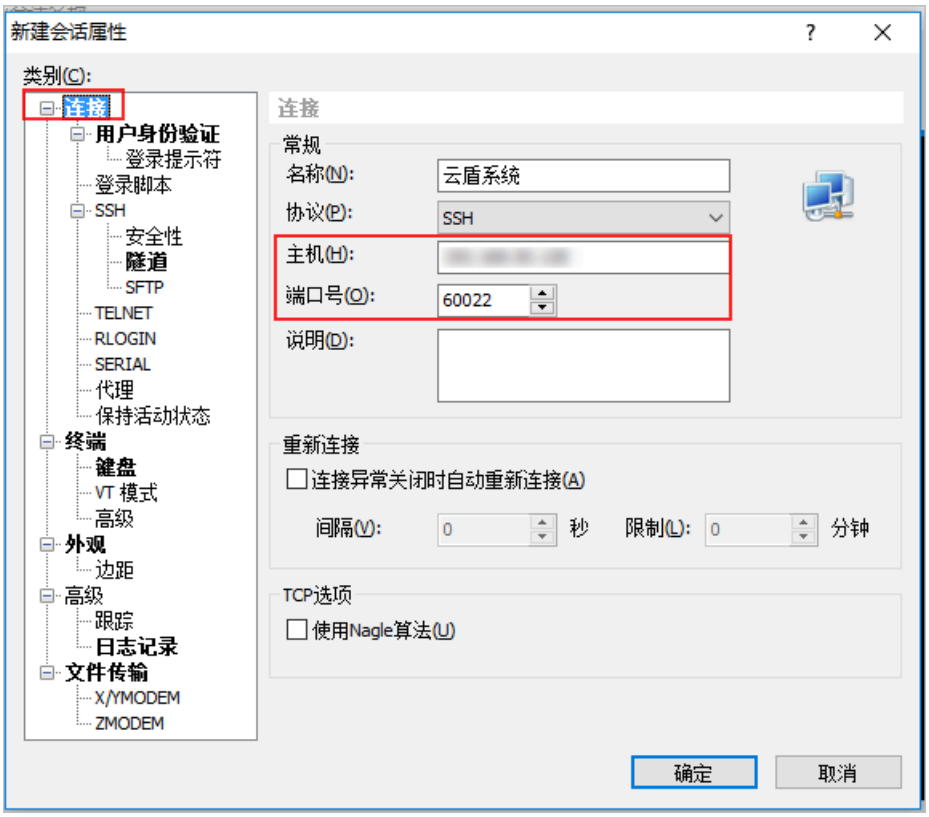
运维人员需要通过本地的客户端工具登录云盾堡垒机，再访问目标服务器主机进行运维操作。

> **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。

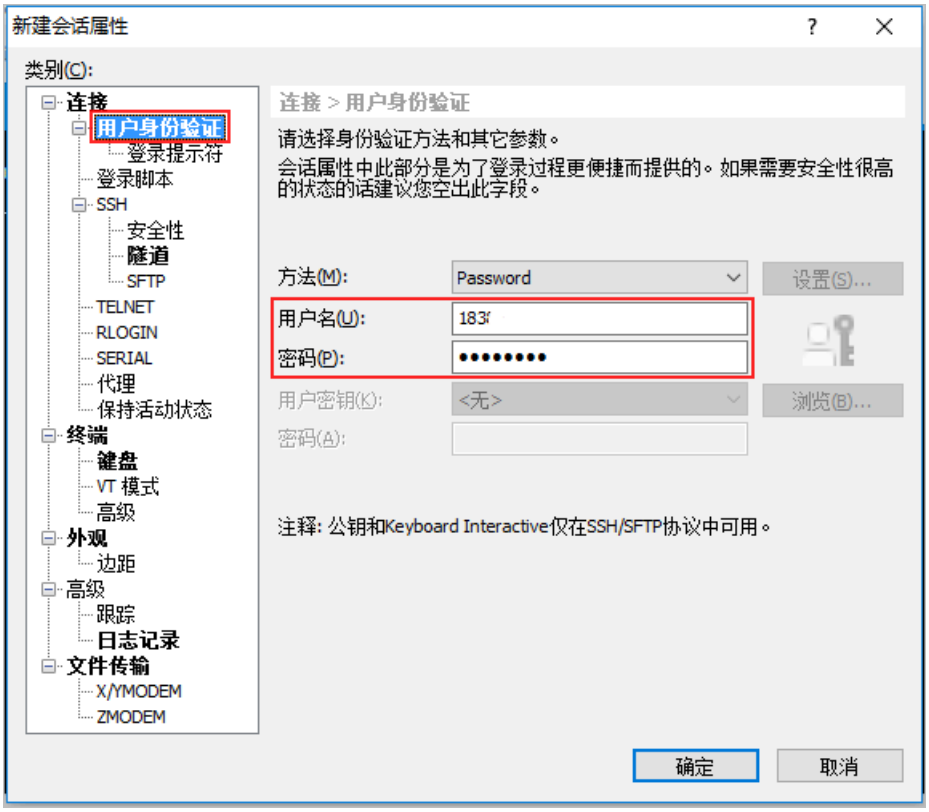
下文以Xshell工具为例，介绍运维登录流程：

操作步骤

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）。

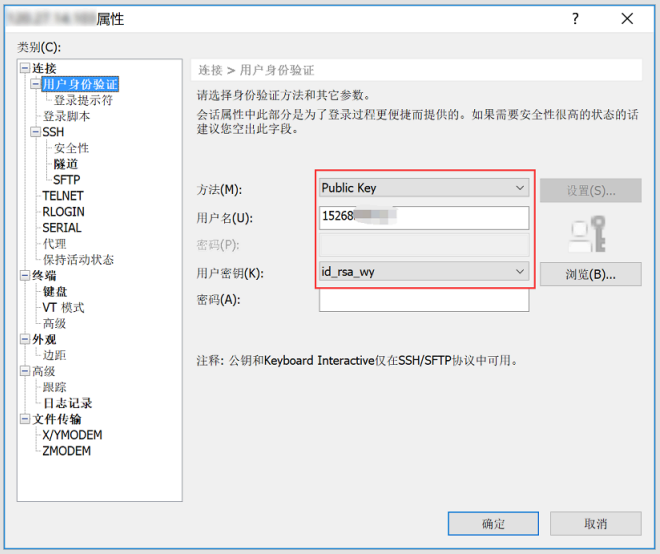


2. 在用户身份验证设置中输入云盾堡垒机的用户名和密码。



说明:

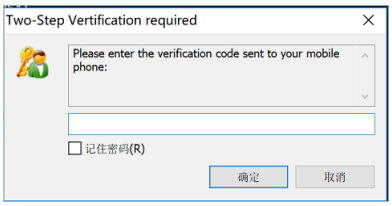
如果管理员在云盾堡垒机中配置了用户公钥，则用户可以通过公私密钥对的方式登录，无需输入密码。在用户身份验证设置中，选择Public Key，输入云盾堡垒机用户名，选择对应的私钥。



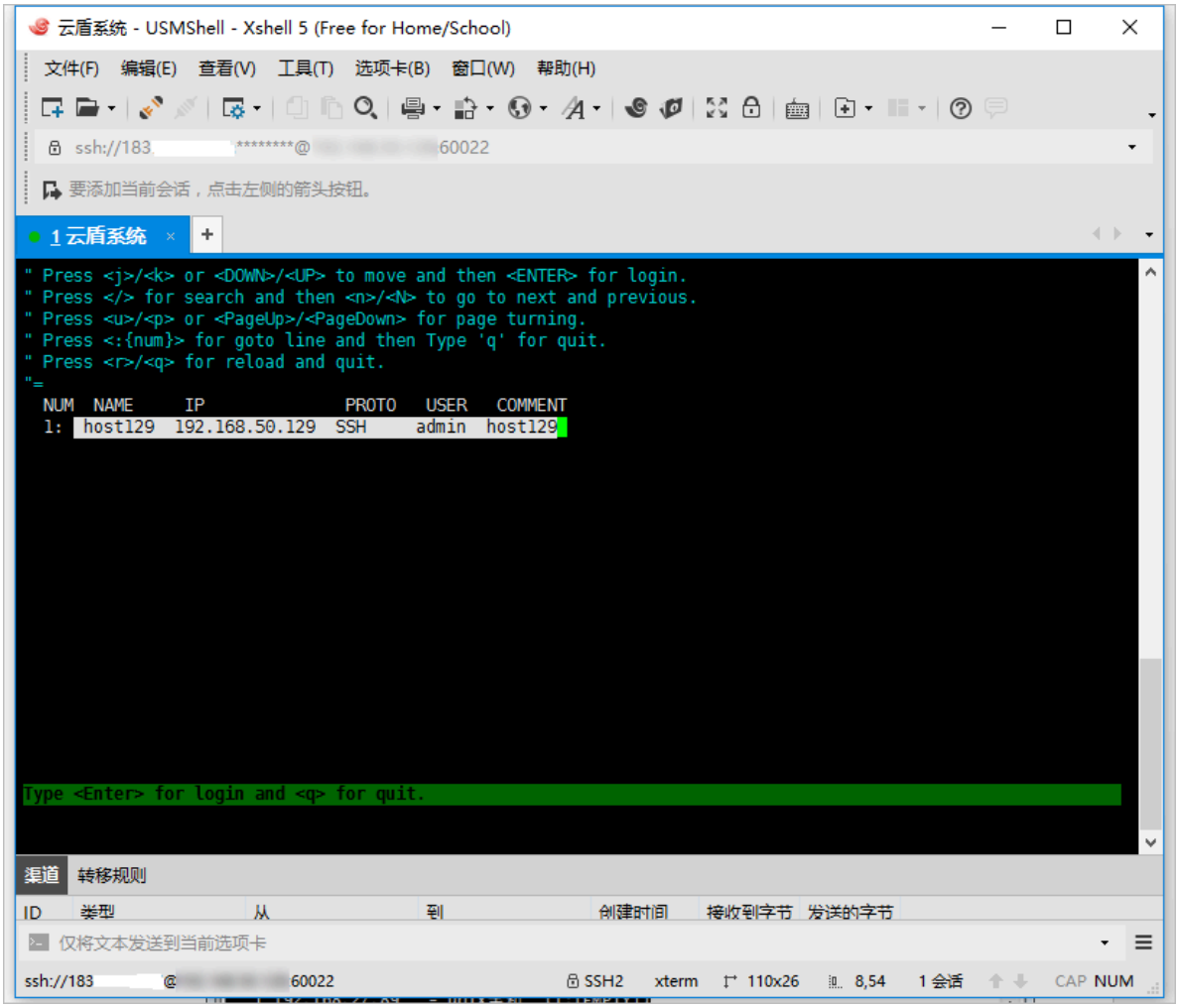
3. 单击确定，连接云盾堡垒机。

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。

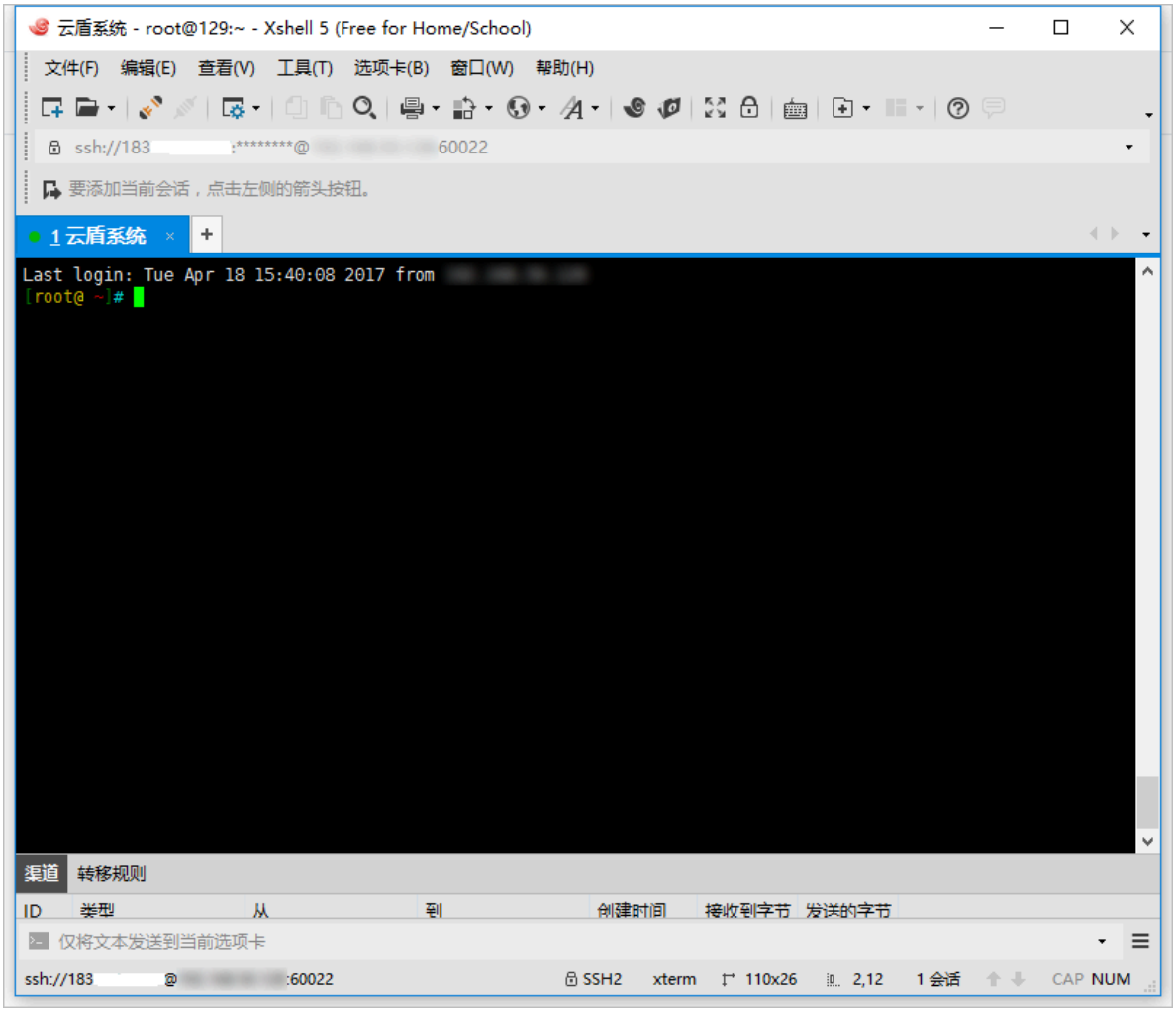
> **说明:**
> 云子帐号账户使用MFA进行二次验证。



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。



3.2 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

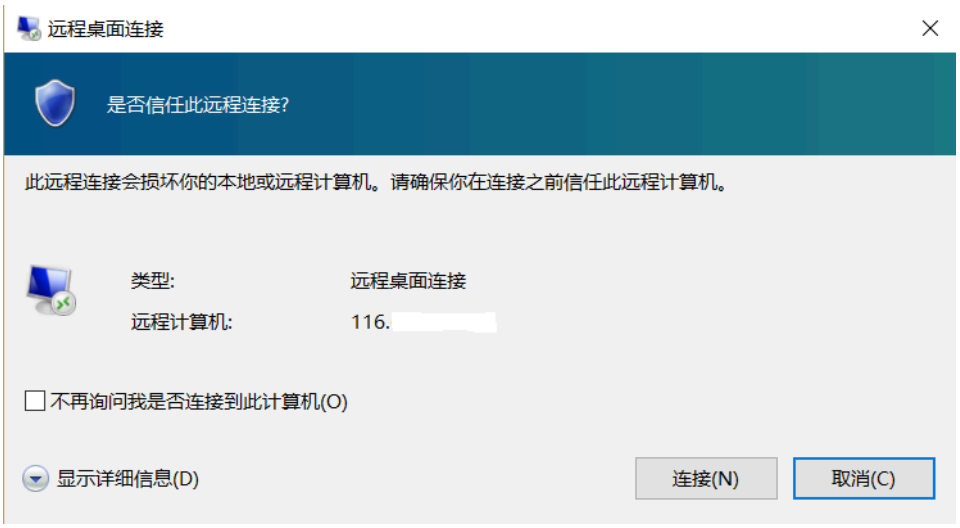
运维人员需要通过本地的客户端工具登录云盾堡垒机，再访问目标服务器主机进行运维操作。下文以 Windows 系统自带的 远程桌面连接工具（Mstsc）为例说明运维登录流程：

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。

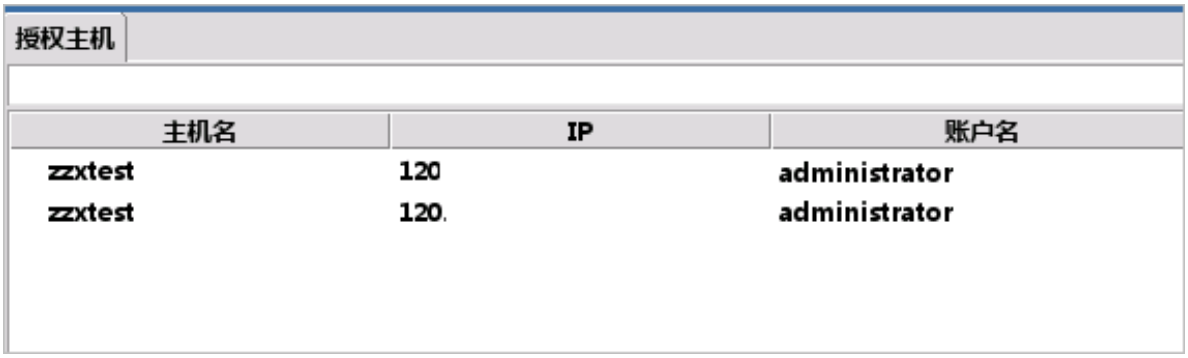
说明:

**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。

3.3 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。

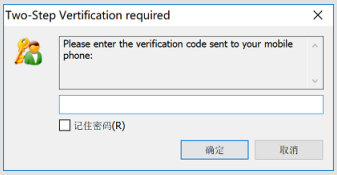
说明:

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:

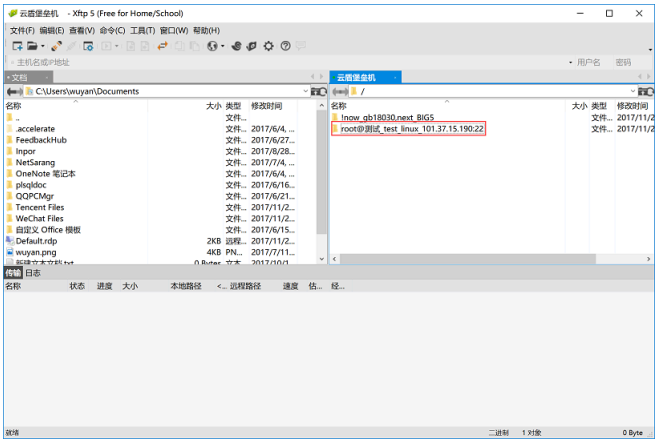
如果管理员启用了双因子登录，将会弹出双因子口令对话框，请输入您手机上收到的6位数字。



说明:

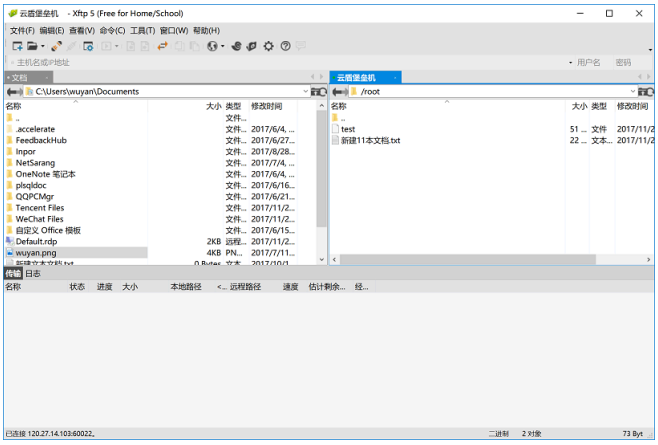
云子帐号账户使用MFA进行二次验证。

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。

3.4 Mac系统运维

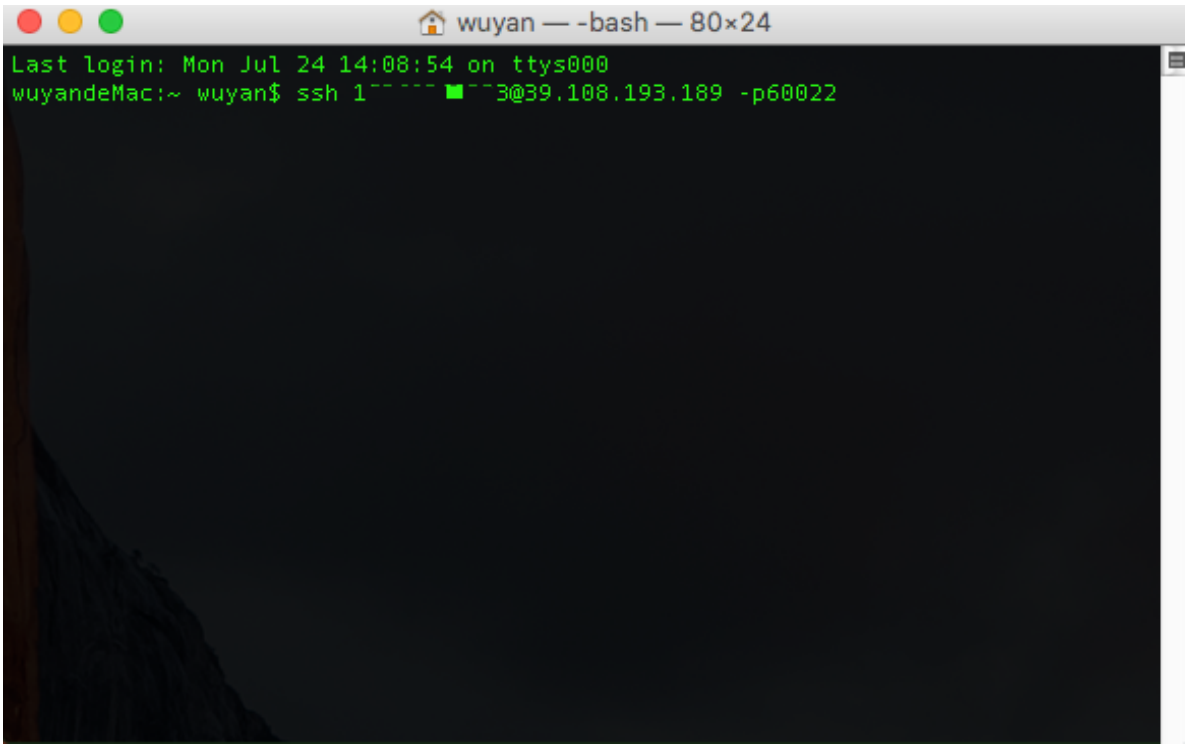
本文受众范围：运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。适用于使用Mac电脑通过本地客户端工具登录云盾堡垒机，再访问目标主机的运维工程师。

SSH协议运维

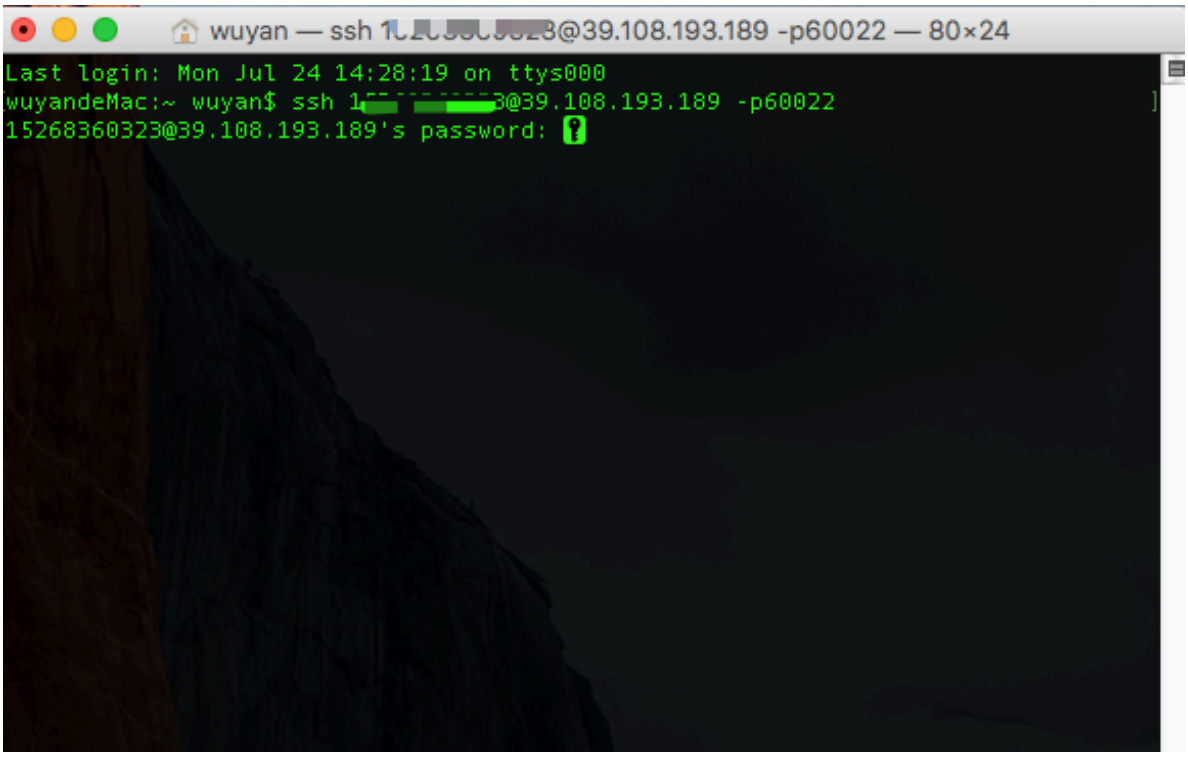
以MAC自带的命令行终端APP为例：

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`

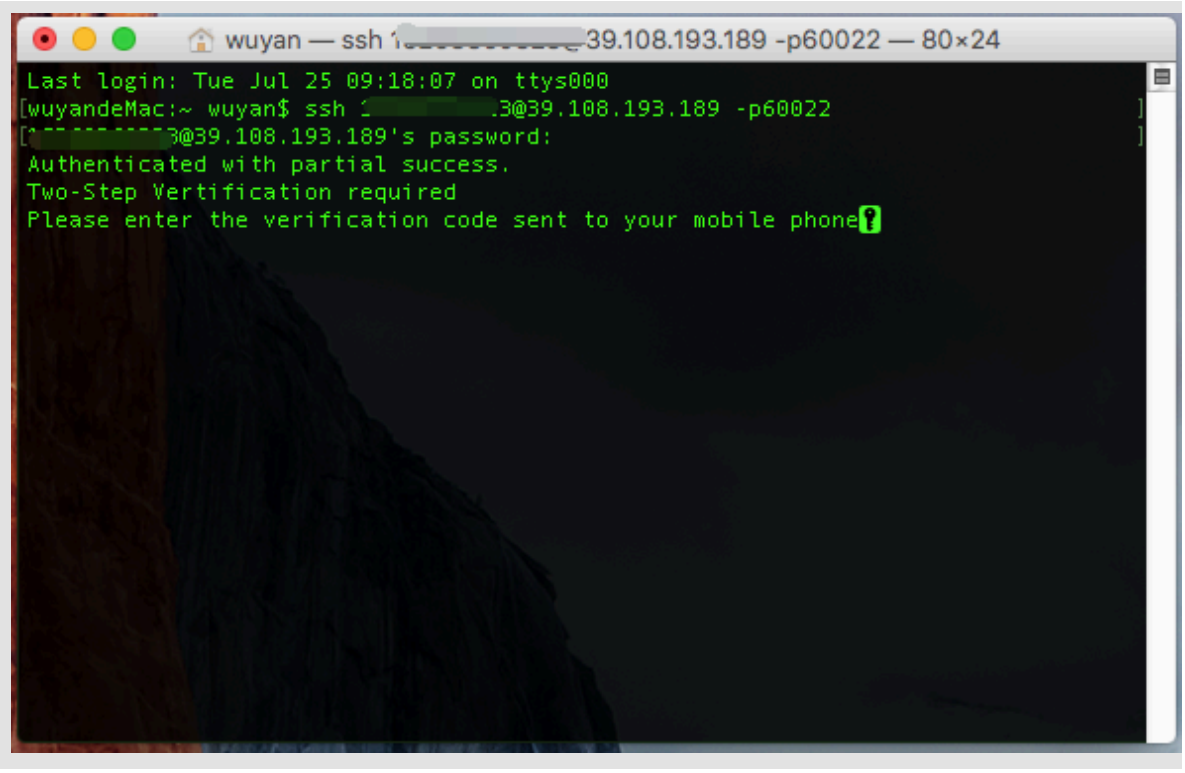


3. 输入云盾堡垒机密码。

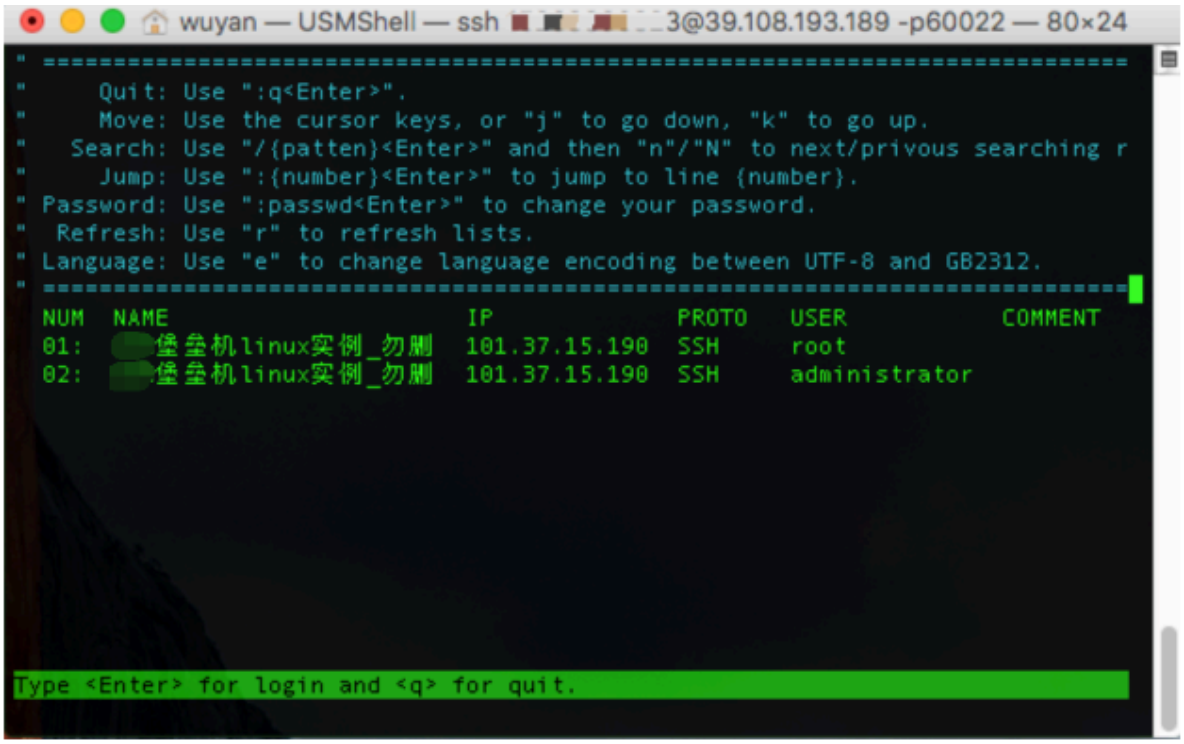


说明:

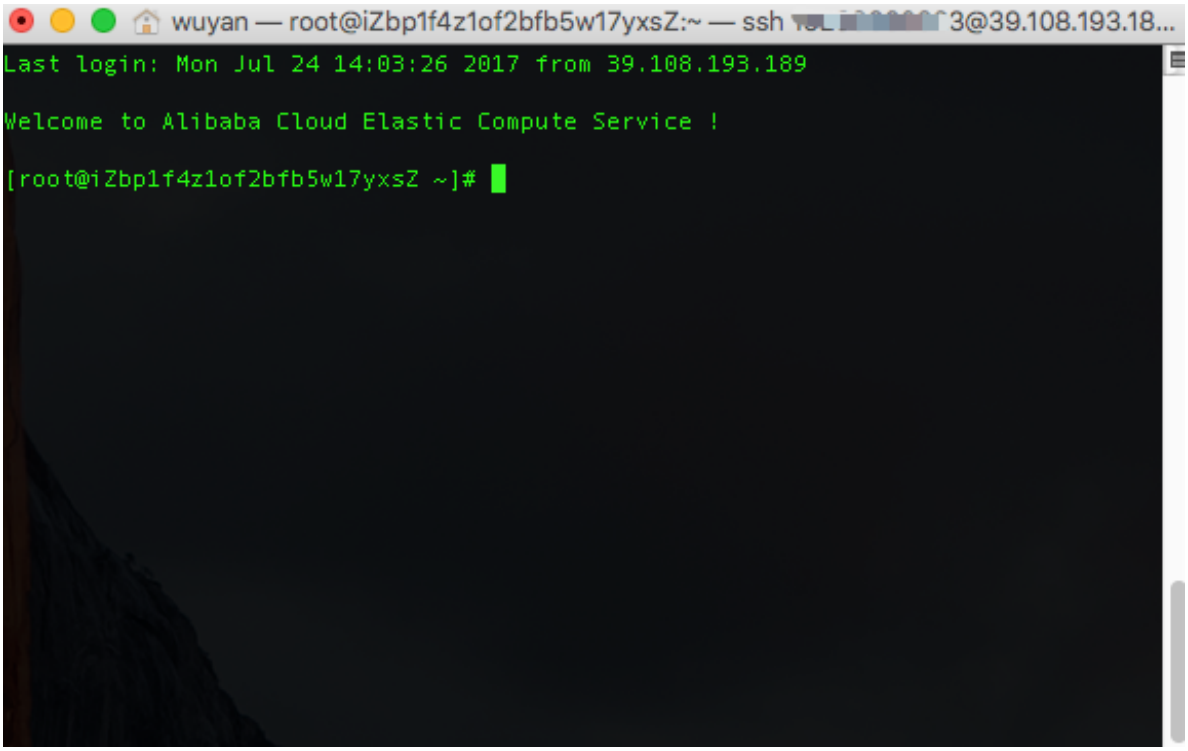
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。



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。

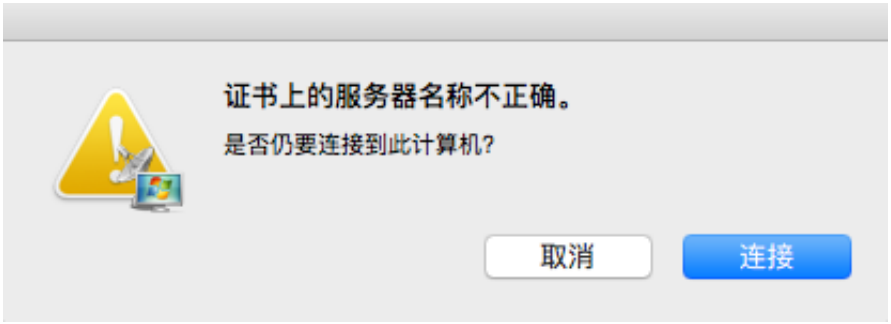


RDP协议运维

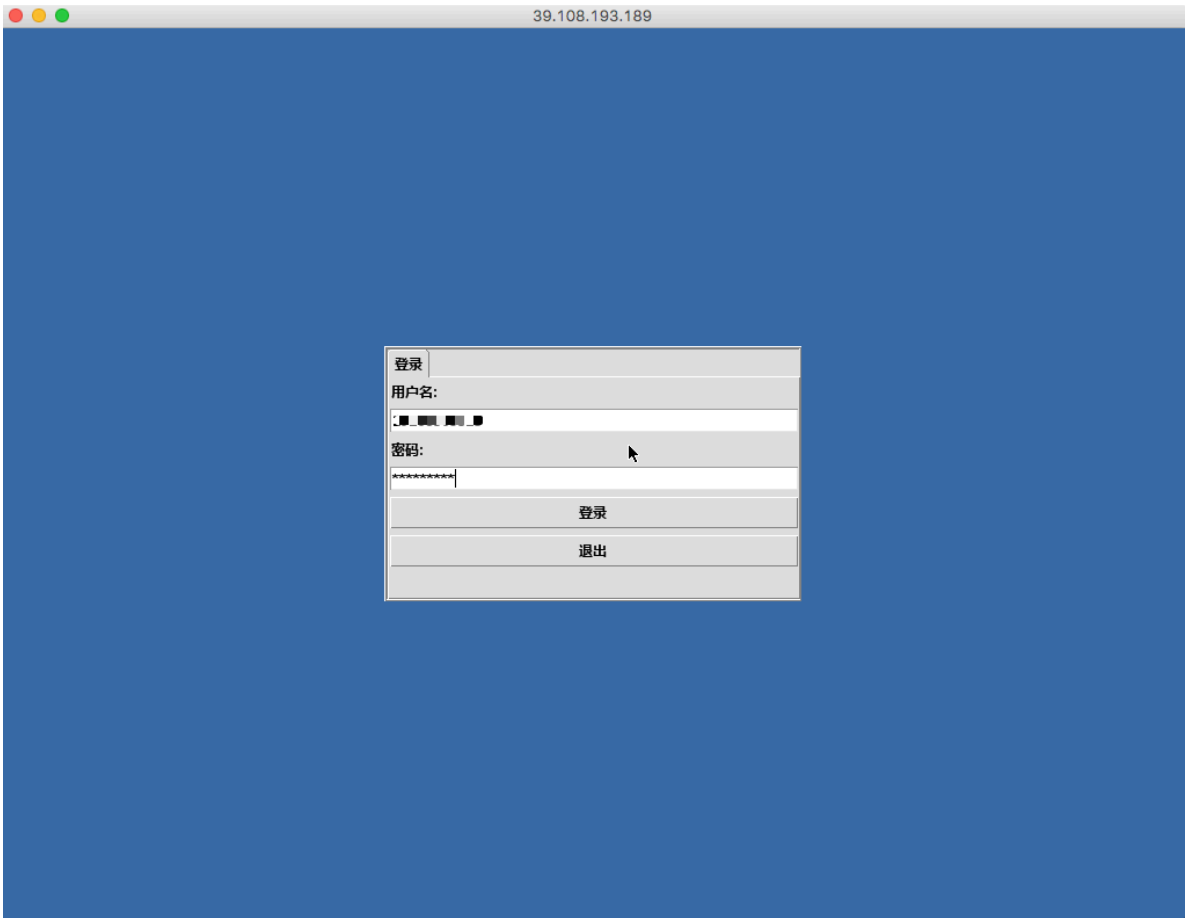
以远程桌面连接APP为例：

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？

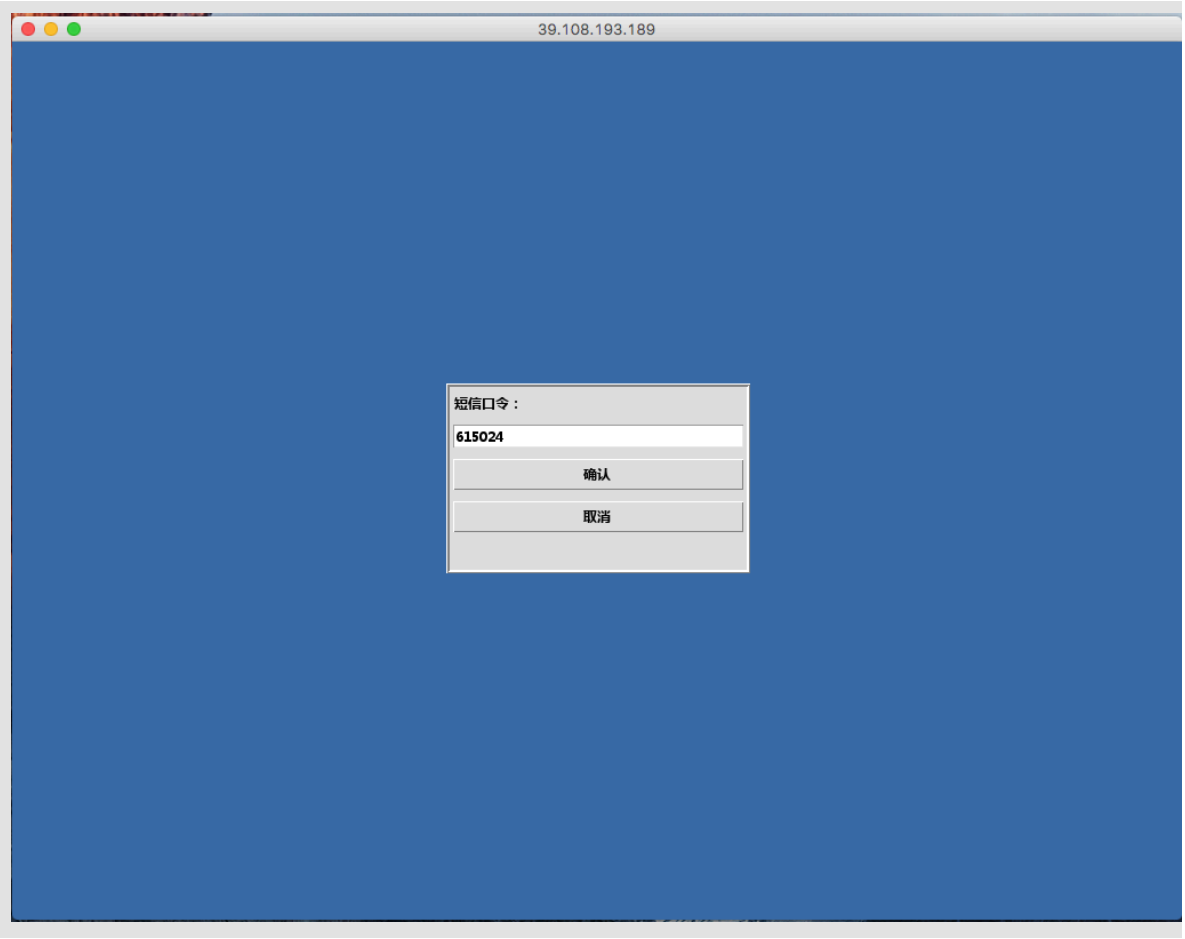


4. 单击连接后，进入云堡垒机登录窗口，输入：云堡垒机的用户名和密码

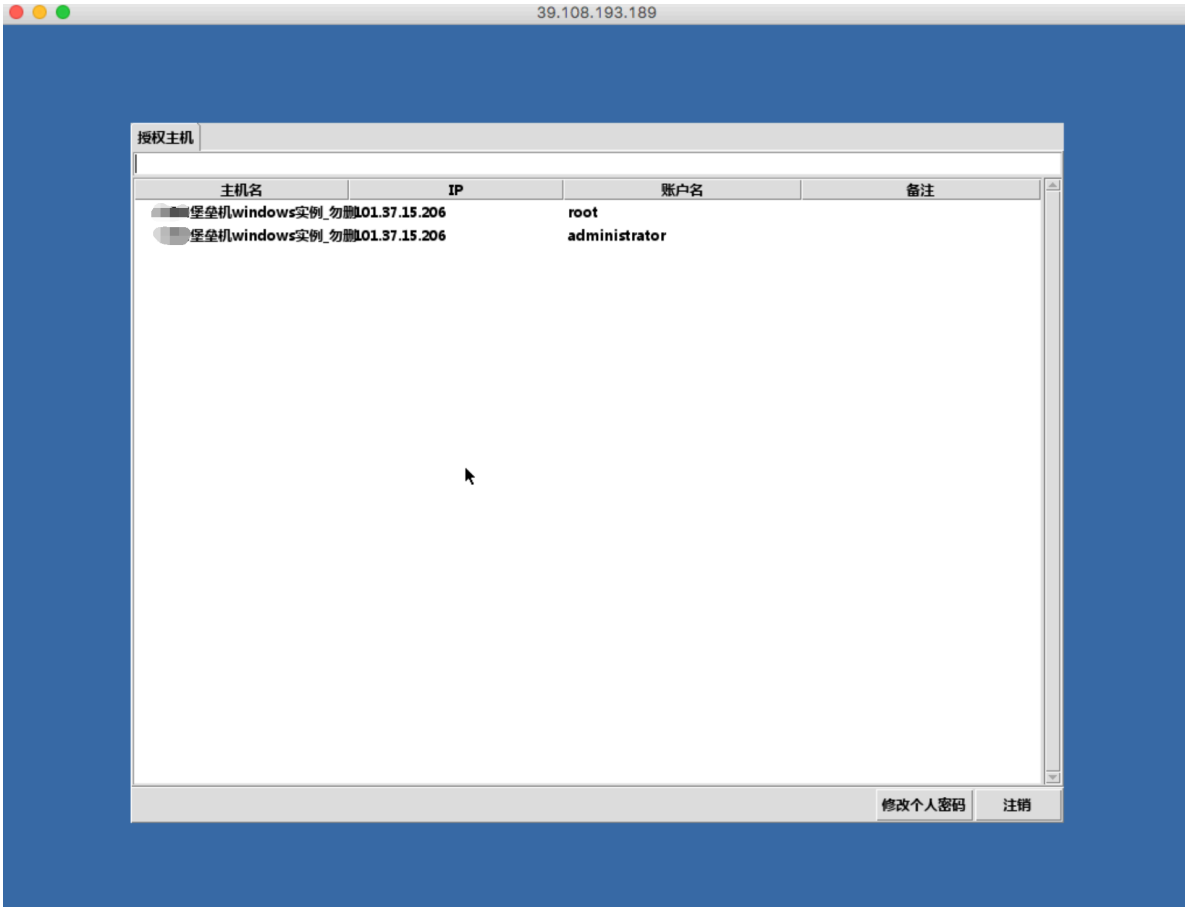


说明:

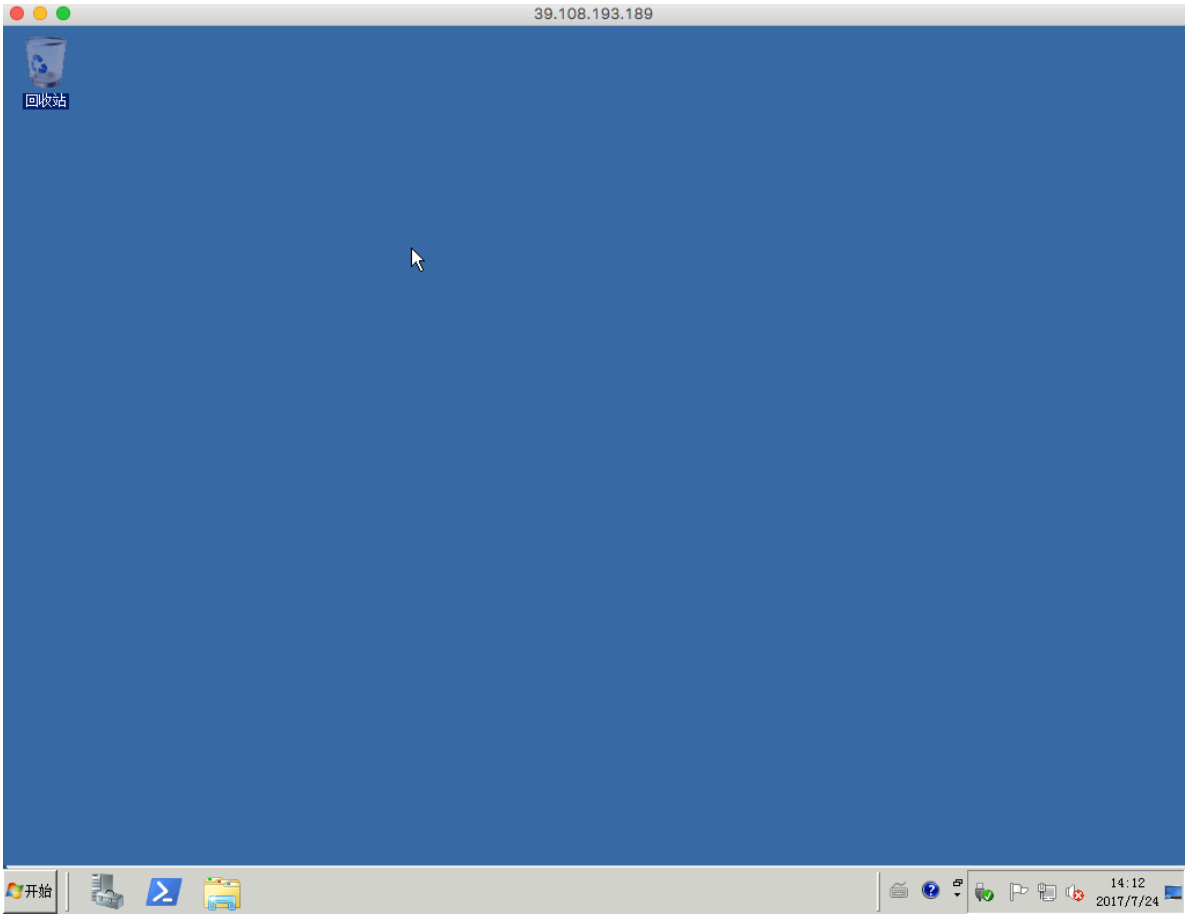
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。


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。



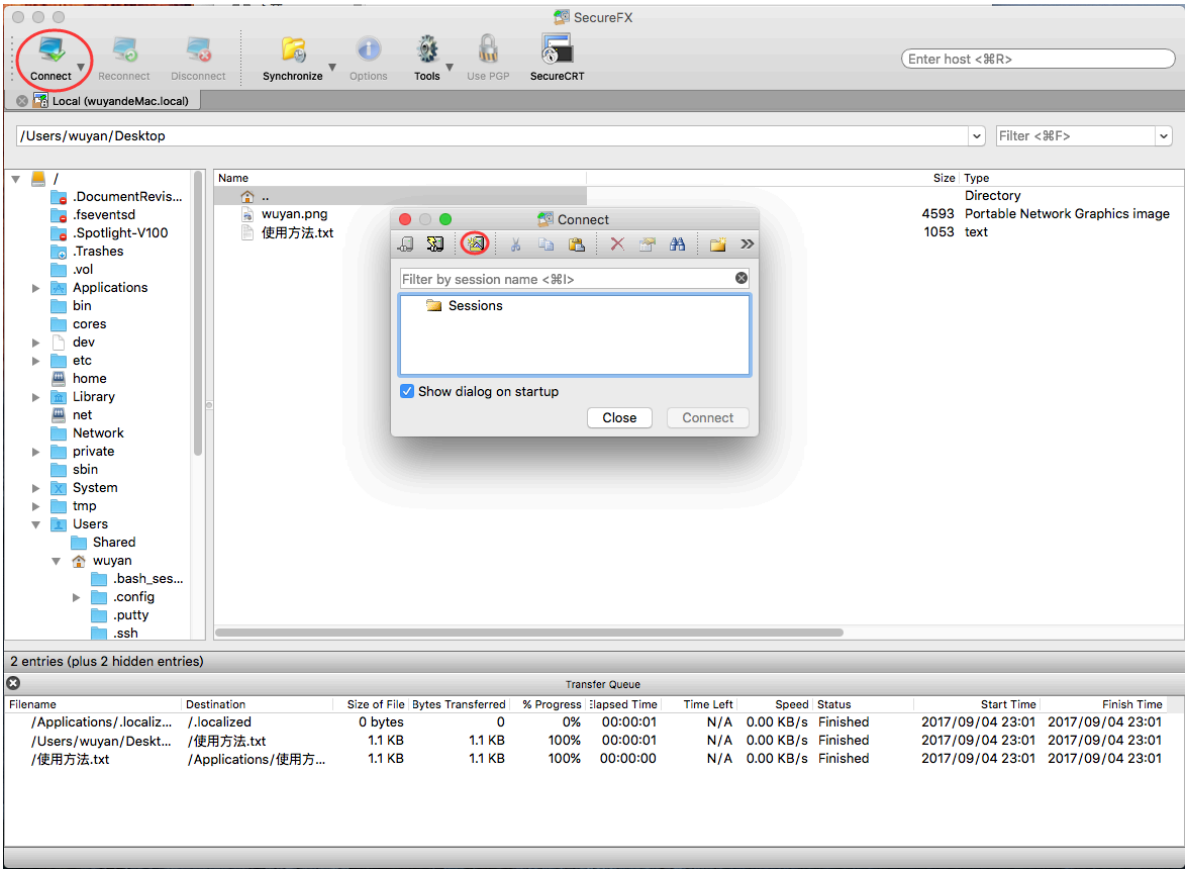
文件传输运维

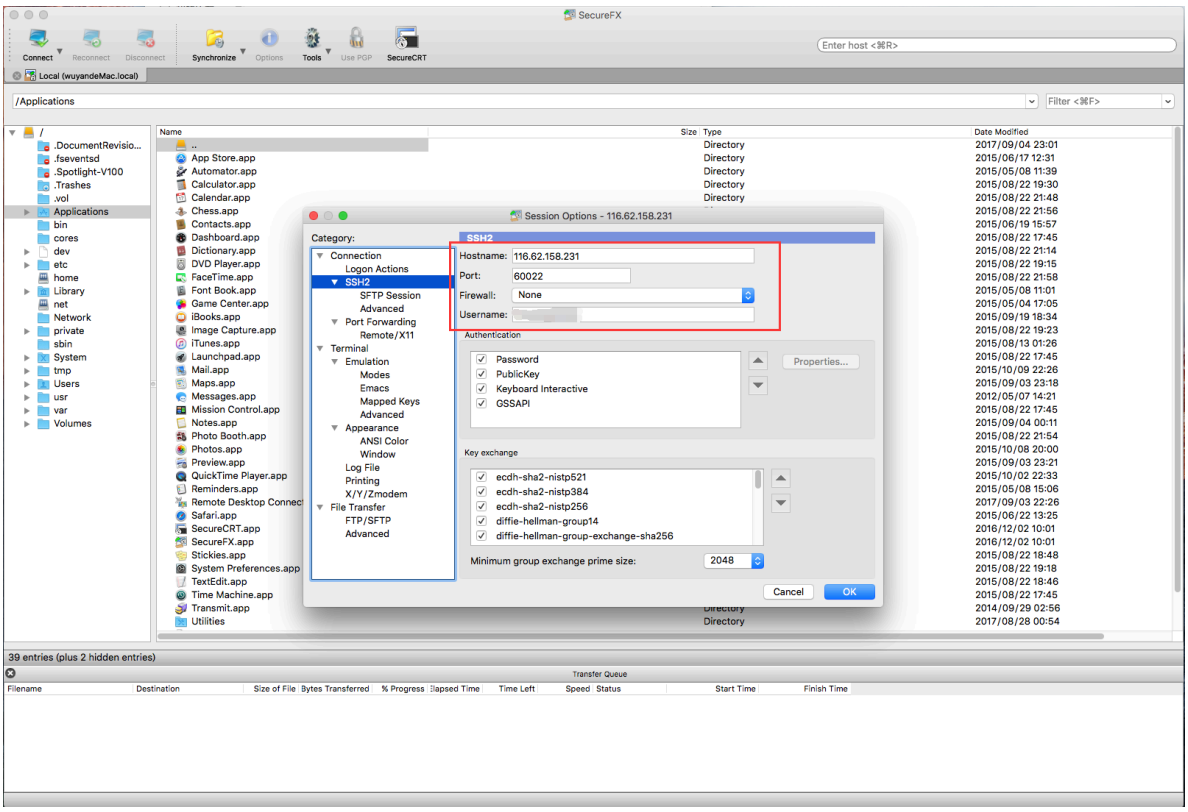
客户端访问堡垒机，再选择ECS方式运维

以SecureFX工具为例：

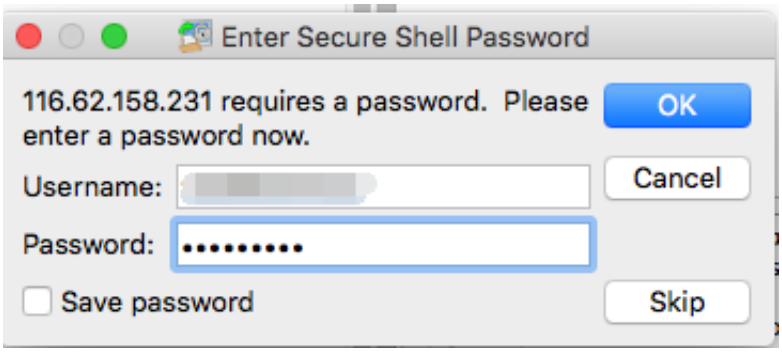
1. 打开SecureFX工具。

2. 新建连接，输入云堡垒机IP，端口60022，账户信息。



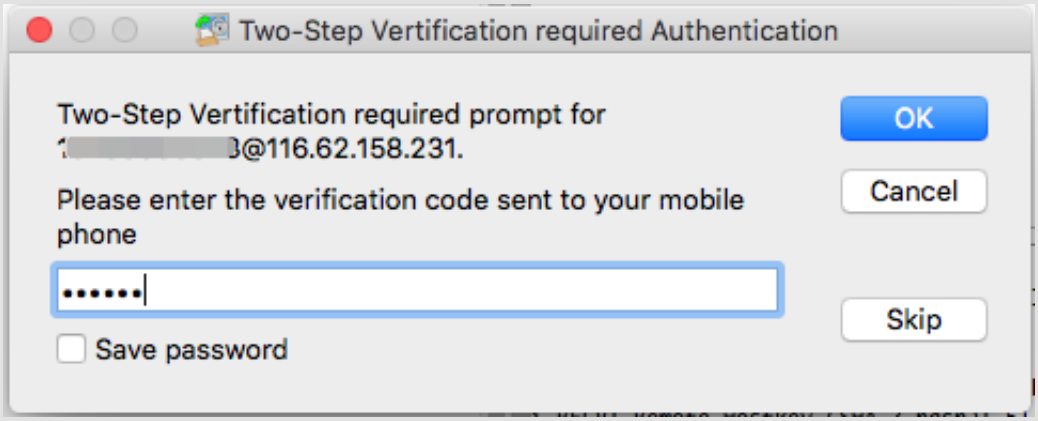


3. 单击连接后，按提示输入堡垒机密码。



说明:

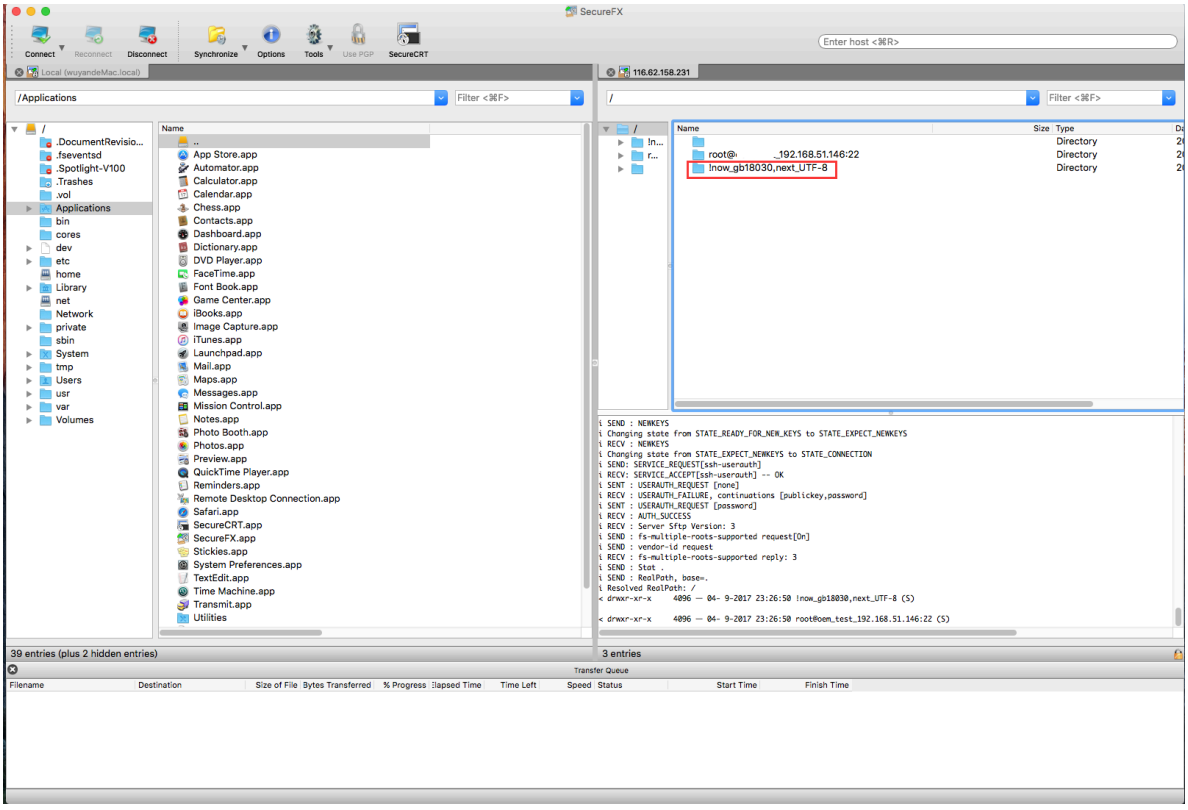
如果管理员启用了双因子登录，将会弹出短信口令对话框，请输入您手机上收到的6位数字。

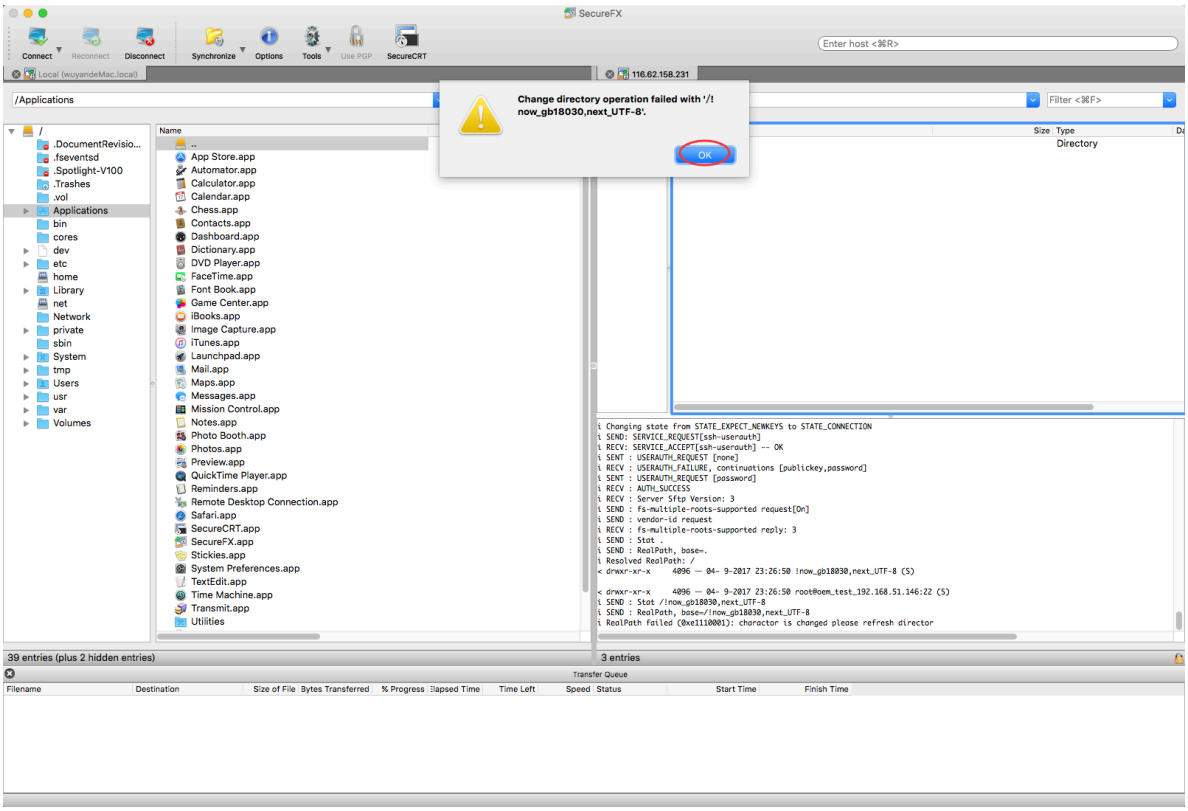


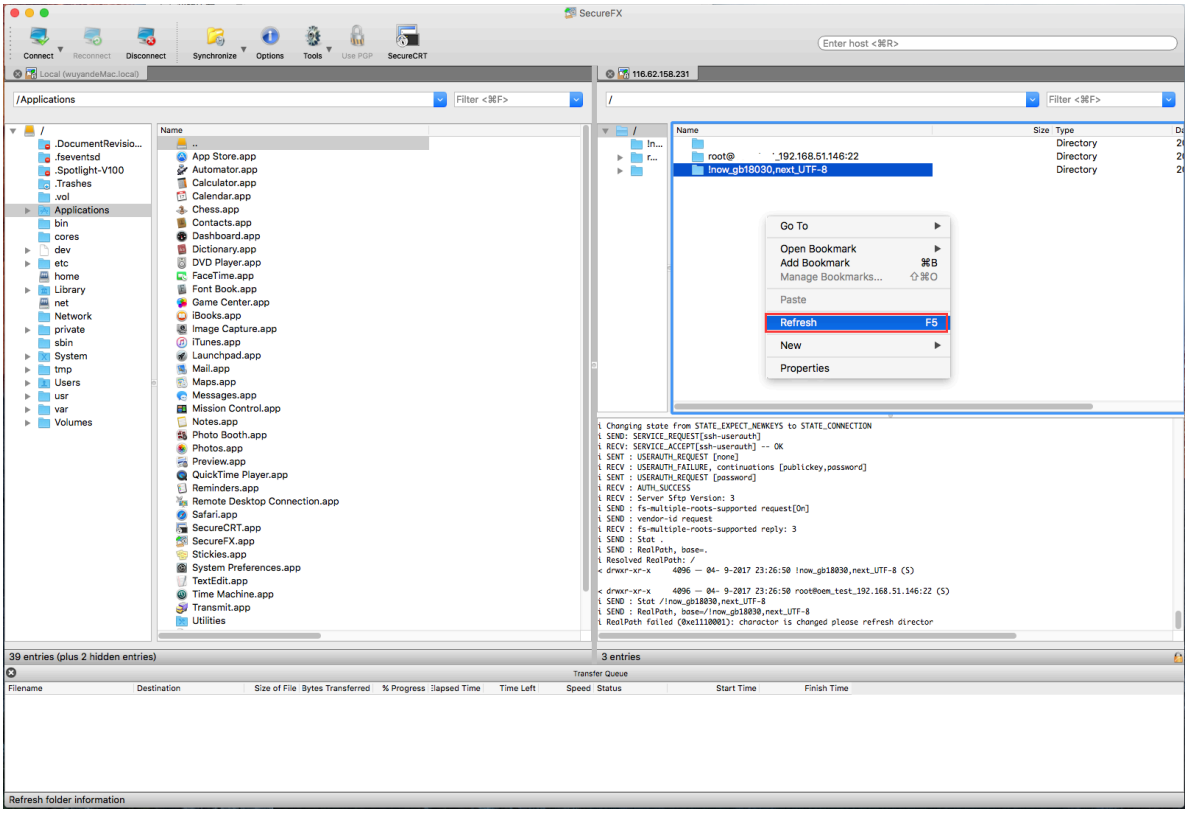
说明:

云子账号使用MFA进行二次验证。

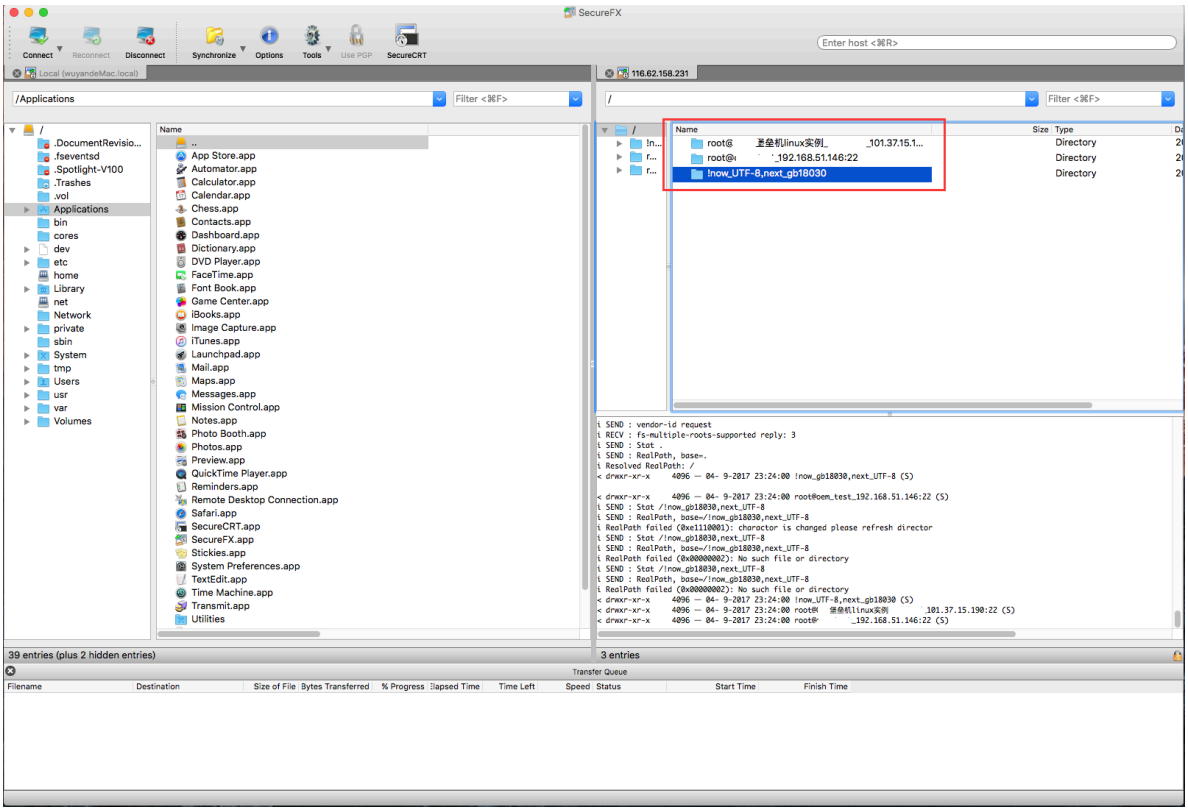
4. 单击<登录>后进入资产管理界面，请双击选择转码目录（忽略报错信息），再右键选择刷新，进行转码。



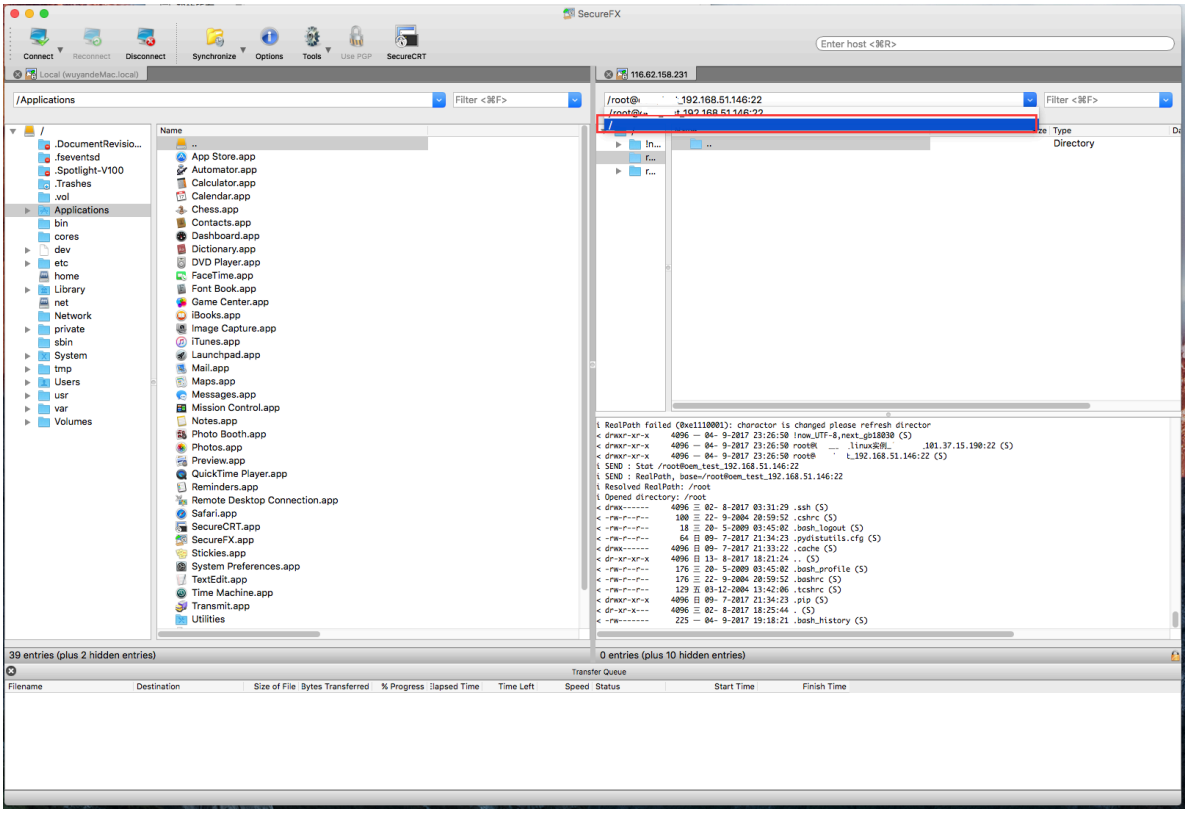


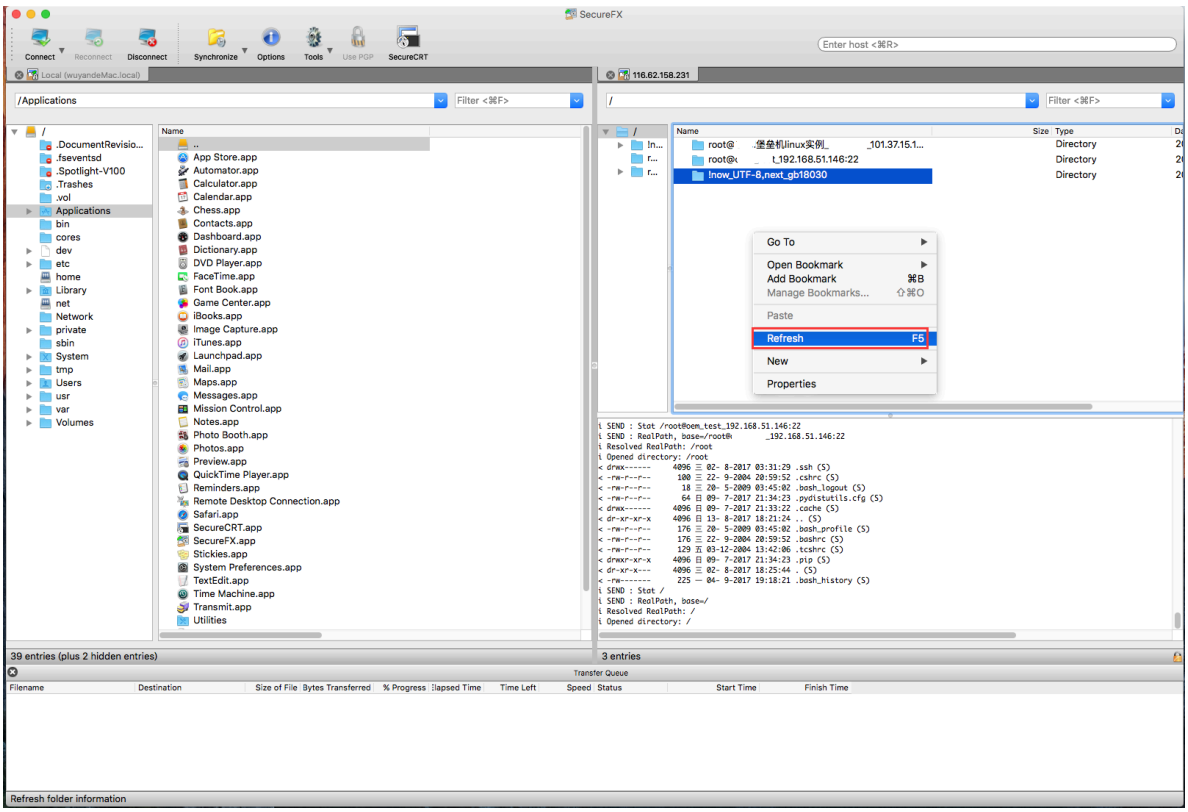


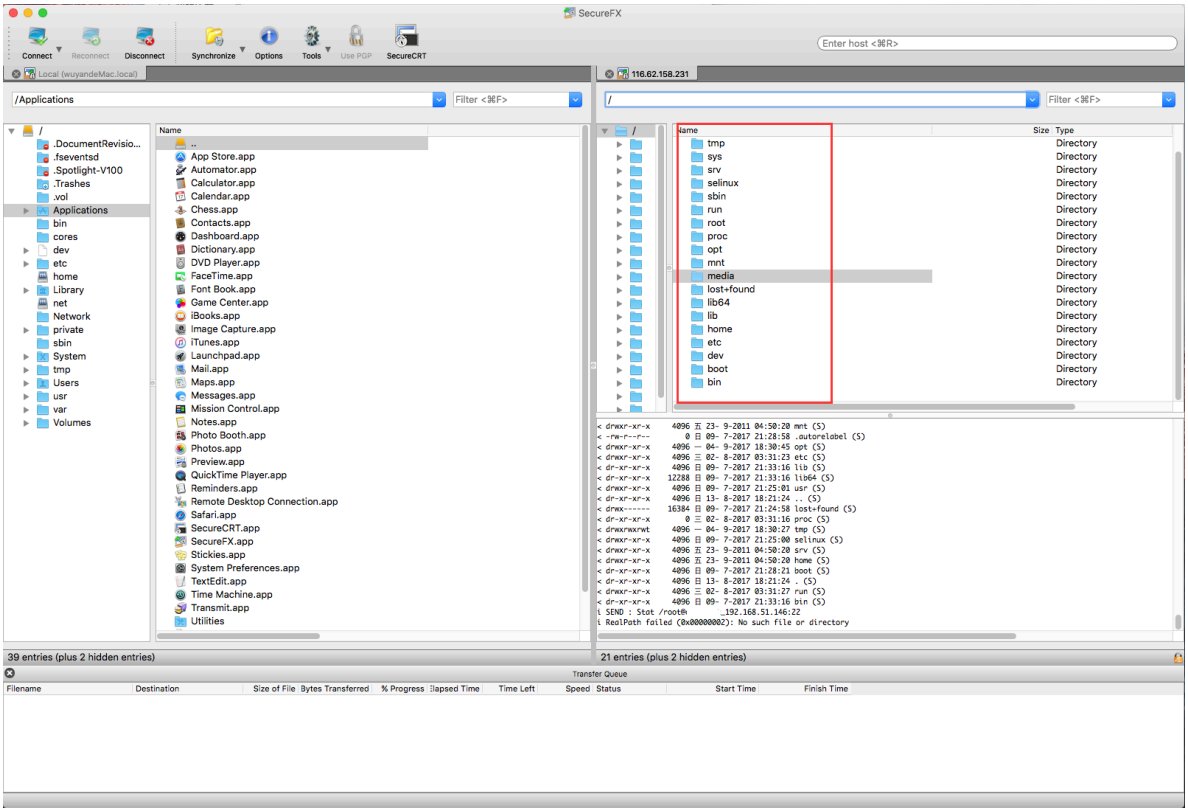
5. 转码后资产列表显示正常。



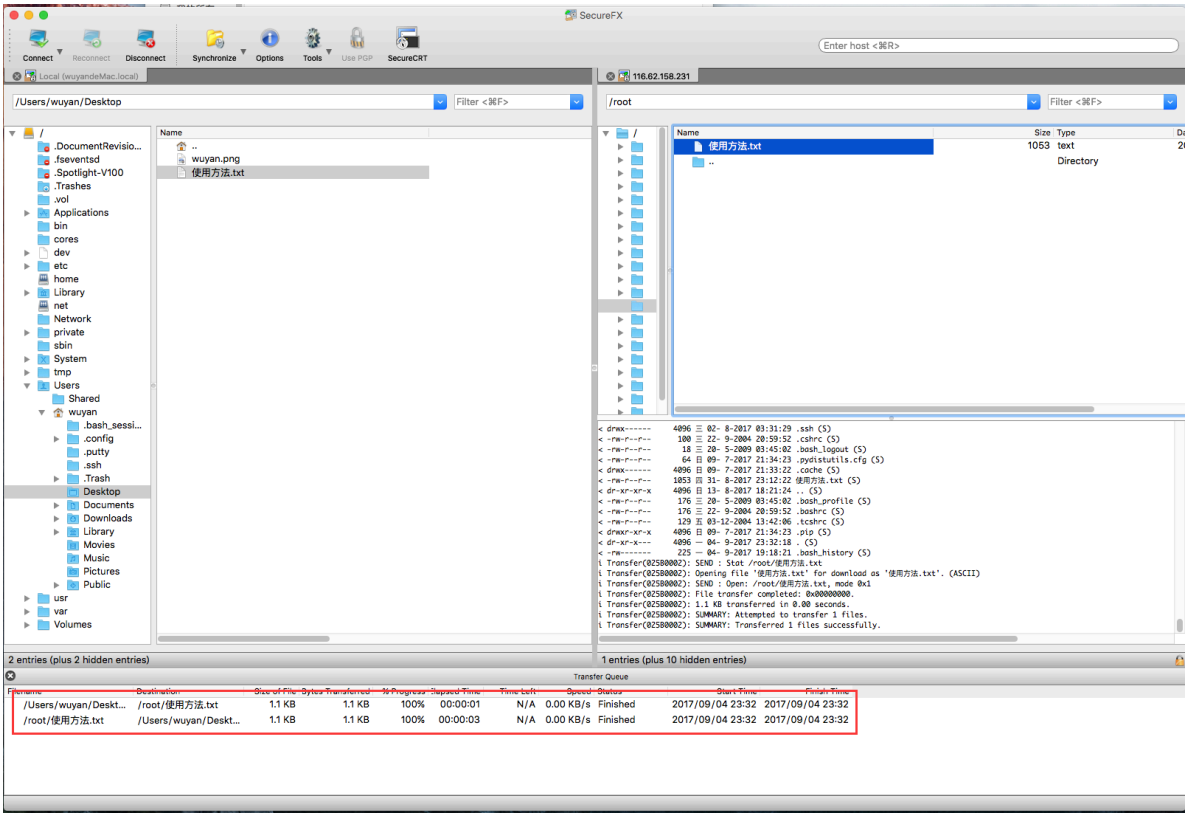
6. 选择目录主机双击进入后，需要先退回到根目录，再右键选择刷新后，进入主机，即可进行运维操作。







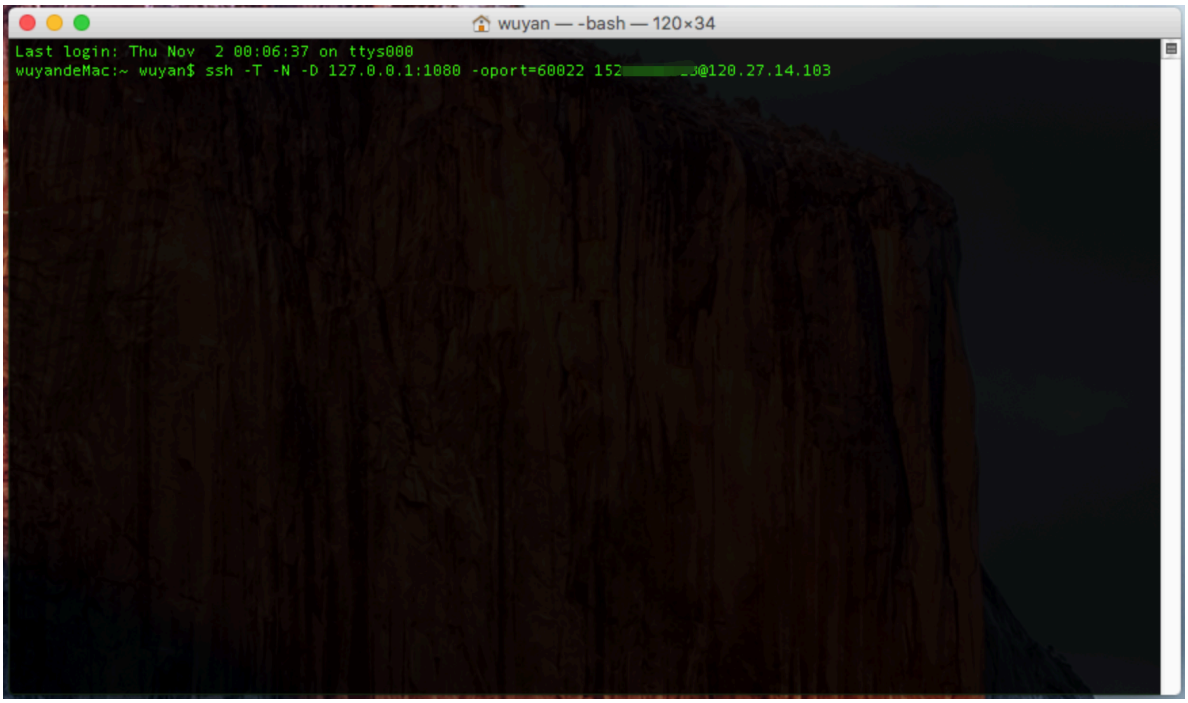
7. 可正常进行上传下载操作。



SSH网关+filezilla直连ECS方式运维

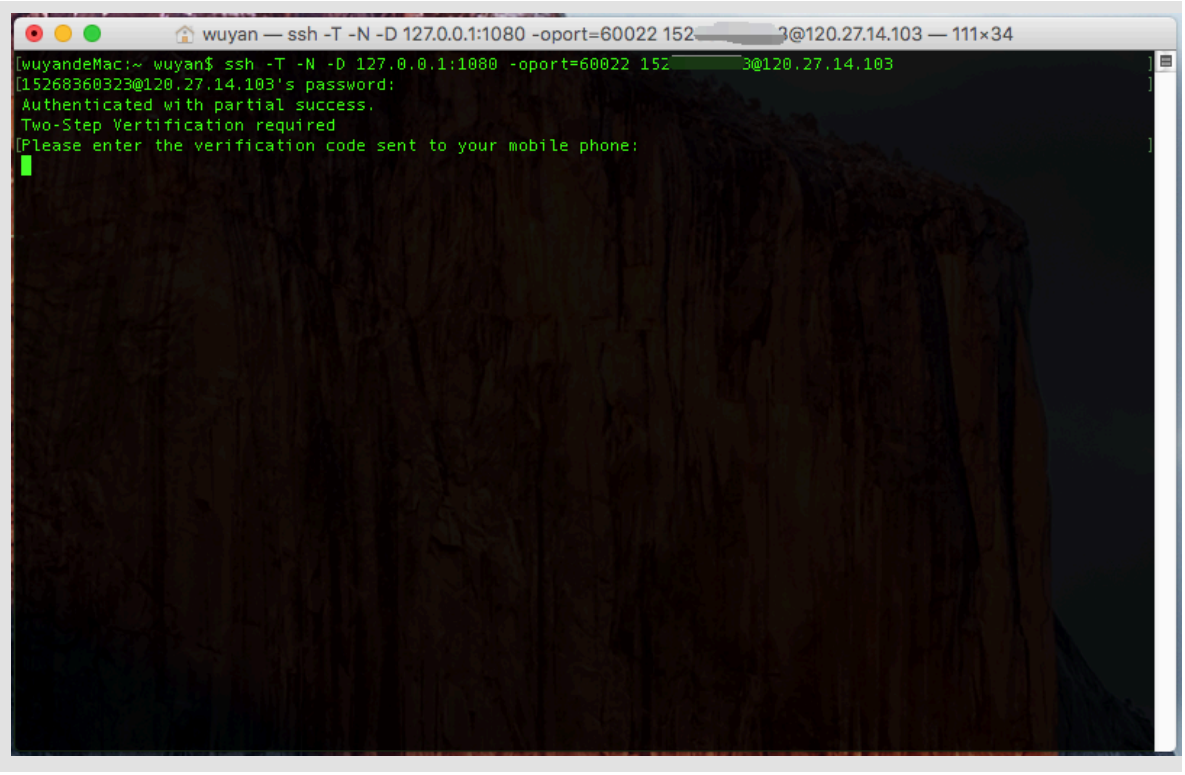
1. 打开命令行终端APP。

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。

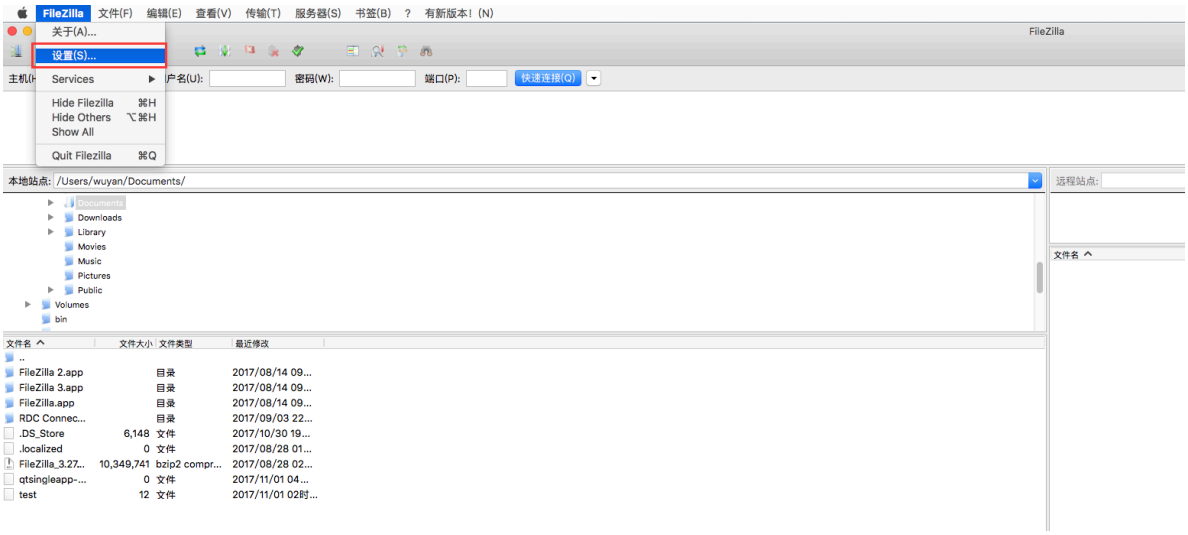
> **说明:**
> 如果管理员启用了双因子认证登录，将会提示输入双因子口令，请输入您手机上收到的6位数字。



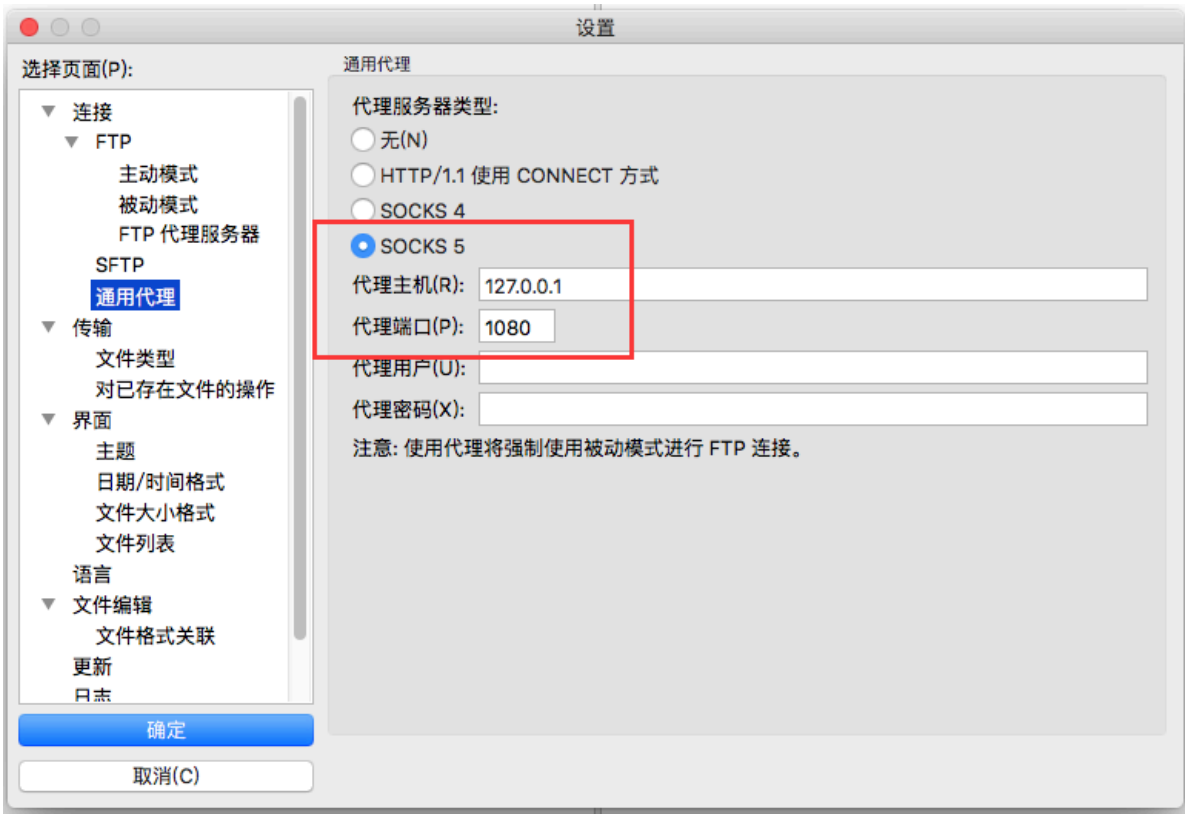
说明:

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。**



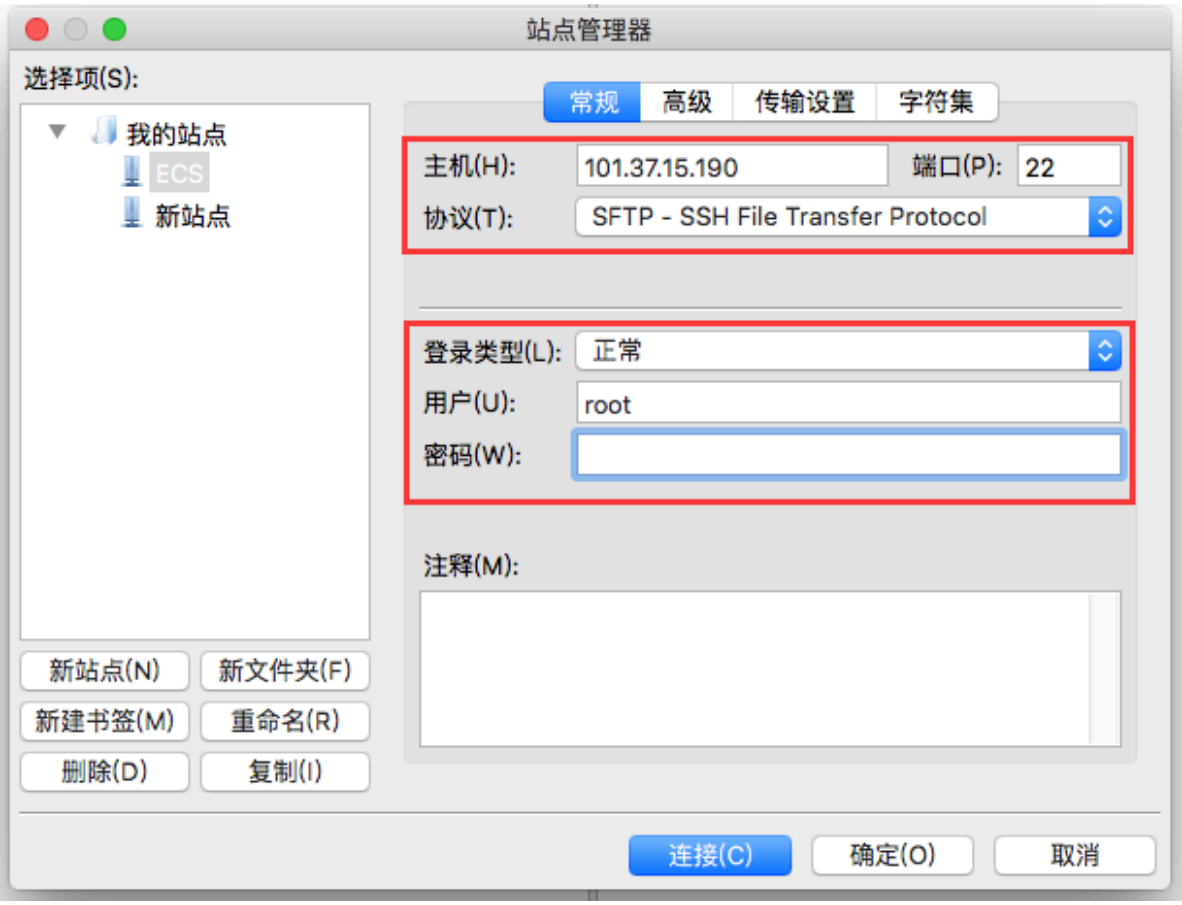
5. 单击通用代理，选择 SOCKS5，设置代理主机：127.0.0.1，端口：1080，单击确定。



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。

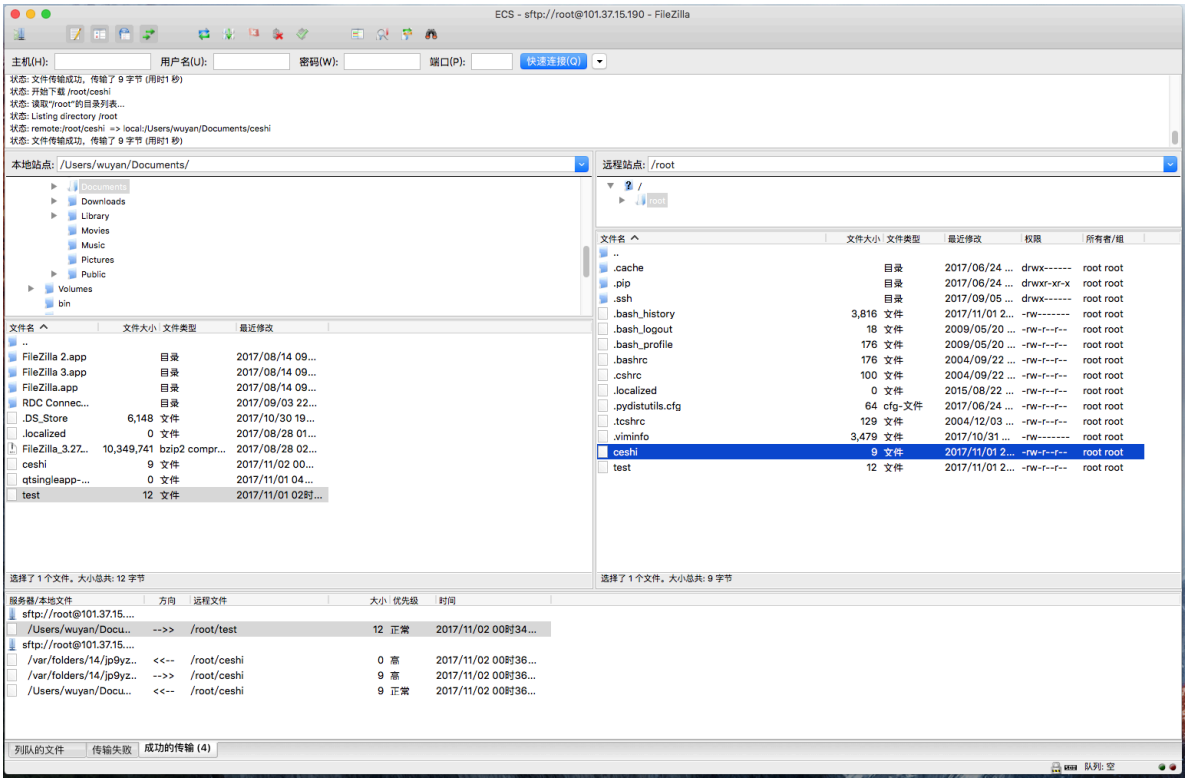
说明:

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。



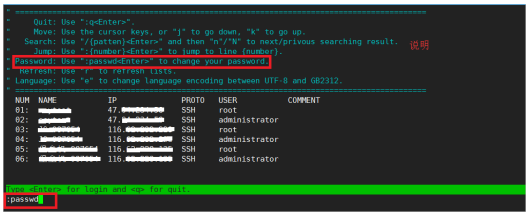
3.5 用户修改密码

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。

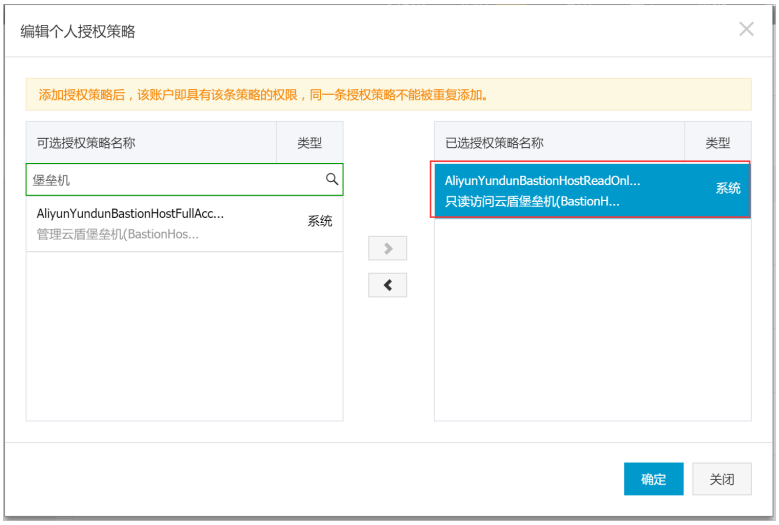
> 说明:
> 云盾堡垒机密码至少八位，且必须包含以下四项字符：大写字母、写字母、数字、非字母符号（如 @，#，$ 等）。

3. 云盾堡垒机用户密码修改成功。

3.6 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和MAC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

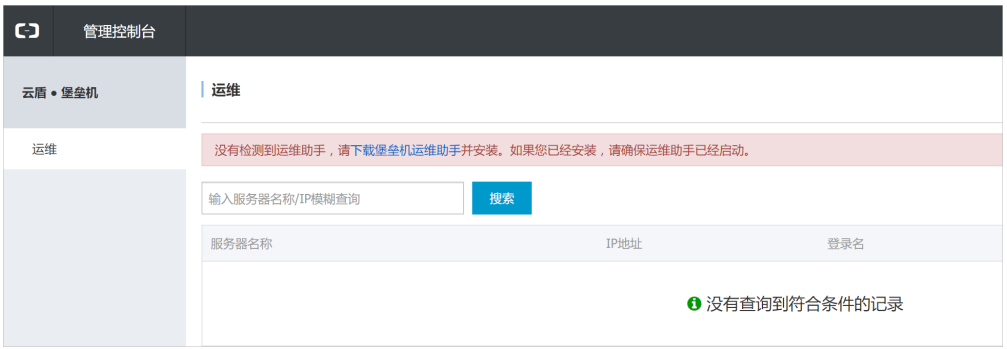
参照以下步骤，使用RAM子账号登录运维页面：

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。

3. 单击下载堡垒机运维助手按钮，下载后进行安装。

> **说明：**
> 使用BS运维功能前，确保堡垒机运维助手启用。

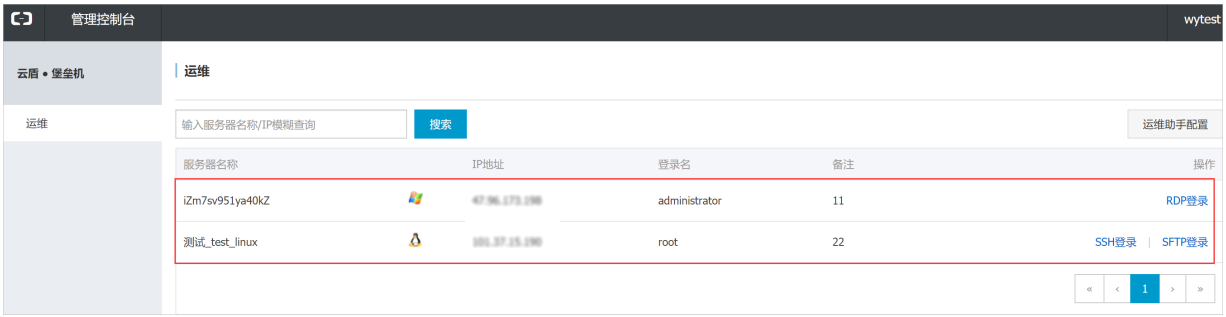


4. 安装完成后，刷新运维页面，不再提示未检测到堡垒机运维助手。
5. 单击运维助手配置，进入运维助手配置界面。
6. 分别对所需使用的SSH客户端、RDP客户端、SFTP客户端进行配置。以SFTP为例，步骤如下：

BS运维操作

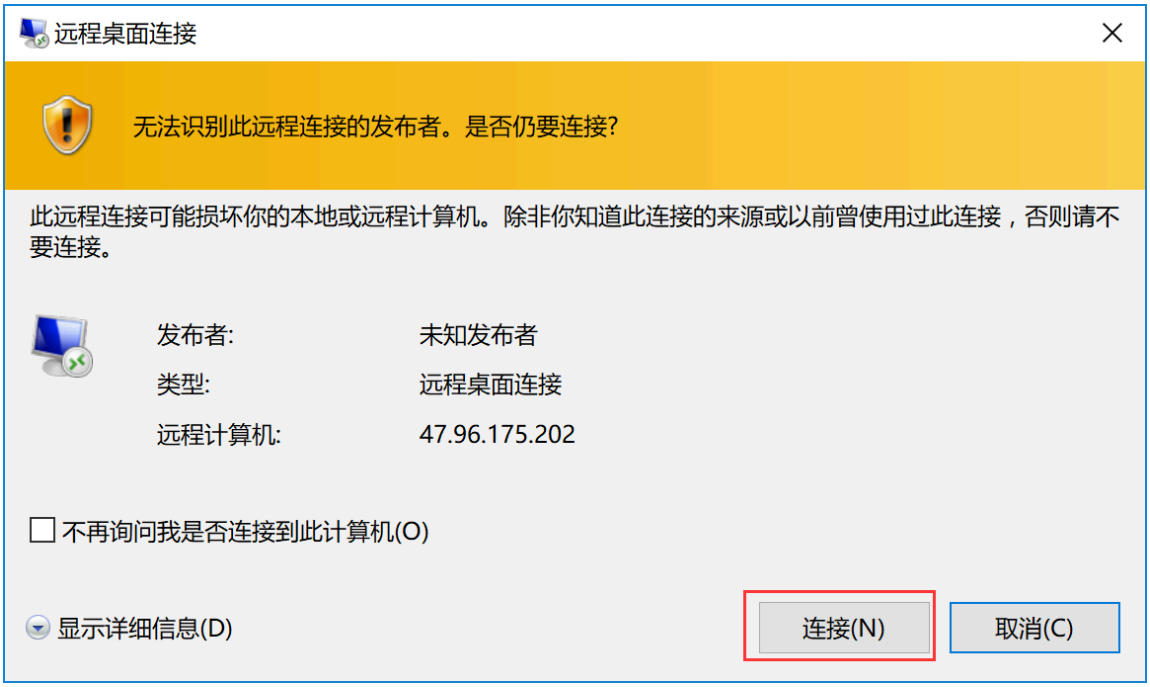
使用RAM子账号登录云盾堡垒机运维页面后，可以看到该账号可以访问的服务器信息。

> **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 。**



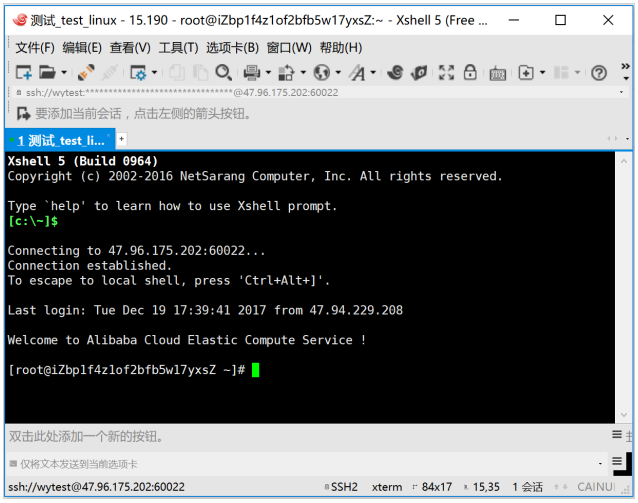
3. **在弹出界面，单击是，成功登录服务器。**

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。