阿里云
堡垒机

快速入门

文档版本：20181128

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。
斜体	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 限制说明

云盾堡垒机系统支持通过 SSH、SFTP、及 Windows 远程桌面等协议的方式代理接入授权的服务器，并实现全程录像。同时，支持使用标准客户端（如 Xshell、SecureCRT、PuTTY 等工具）对授权的服务器直接进行运维连接。

使用云盾堡垒机服务前需要注意以下内容：

- 所有接入堡垒机实例的 ECS 云服务器，需要正常开机并保持运行中状态。
- 堡垒机实例与要与接入的 ECS 云服务器属于一个相同的网络环境，且可以网络连通。例如，同属于一个安全组，或同属于一个 VPC 专有网络。

2 使用说明

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、审计人员、运维人员。

对象

云盾堡垒机有三种对象，分别是用户、主机、和凭据。

- 用户代表技术工程师，也就是自然人，登录堡垒机时用户名即为手机号码。
- 主机是您在阿里云上的ECS实例。
- 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。

授权组

授权组是将堡垒机中数个独立的对象个体联系在一起的概念，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主机的目的。假设您单位的运维模型如下：

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）

在此模型下，就可以按照如下策略配置授权关系：

个人账号	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改。
opsuser	APP1、APP2、DB1、DB2、M1、M2	ops	运维人员使用可以sudo权限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。

这样就可以通过授权组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；运维人员控制生产机；管理员则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。

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，现有规则表如下：

运维协议	端口号	四层协议
SSH	60022	TCP
Windows远程桌面	63389	TCP
SFTP	60022	TCP
FTP	60021	TCP
VNC	5900	TCP
Windows远程桌面网关	44300	TCP

您可以使用标准协议客户端如Xshell、SecureCRT、PuTTY、Windows远程桌面客户端直接连接上述端口号，并通过堡垒机用户名、密码登录，连接后根据提示进行下一步操作。详细的运维操作步骤，请参阅用户手册-运维手册。

审计

云盾堡垒机的审计分为两种，分别是实时监控和录像回放。实时审计专注于事中控制，可以通过云盾堡垒机管理平台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，主要用于已经结束的会话进行录像回放或命令检索，检索可以使用时间段、手机号、主机IP地址、ECS实例ID、协议类型等条件筛选结果，还可以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播放。

3 快速入门

本文介绍了如何配置、使用云盾堡垒机，帮助您快速熟悉产品。

在购买云盾堡垒机实例后，您需要进行如下配置操作：

1. 登录云盾云堡垒机控制台，选择您已购买的堡垒机实例，单击**启用** ，启用堡垒机，具体操作请参考网络配置。
2. 启用堡垒机实例后，单击管理。

3. 选择内网接入或公网接入，即通过内网还是公网连接云盾堡垒机 Web 管理页面。
4. 在云盾堡垒机Web管理页面中，定位到**资产 > 服务器**页面，单击页面右上角的**同步阿里云ECS**。

5. 在 **同步阿里云ECS** 对话框中，勾选您想要加入堡垒机实例进行管理的云服务器，单击 **加入云堡垒机**。

说明：

如果您的服务器使用的端口不是默认的端口（如 SSH 不是默认 22 端口，或 RDP 不是默认 3389 端口），或者您需要指定堡垒机实例连接的云服务器资产是通过公网 IP 还是内网 IP，您可通过以下两种方式进行配置：

- 定位到**资产 > 服务器**页面，勾选需要修改的服务器，单击服务器列表下方的**修改端口**及**配置连接IP**进行修改。

- 定位到**系统 > 系统设置**页面，进行运维端口及运维连接 IP 的全局设置，单击**保存**修改后生效。

说明：

如果您通过此方式进行全局设置，所有服务器都将使用该配置方式，且服务器单独的配置修改不生效。

6. 定位到资产 > 凭据页面，单击新建凭据。

7. 在新建凭据对话框中，输入名称、登录名、凭据类型、密码，单击确定。

> 说明：
>
> 关于凭据的作用，请参考术语介绍。

8. 定位到用户 > 用户管理页面，单击新建本地用户。

> 说明：

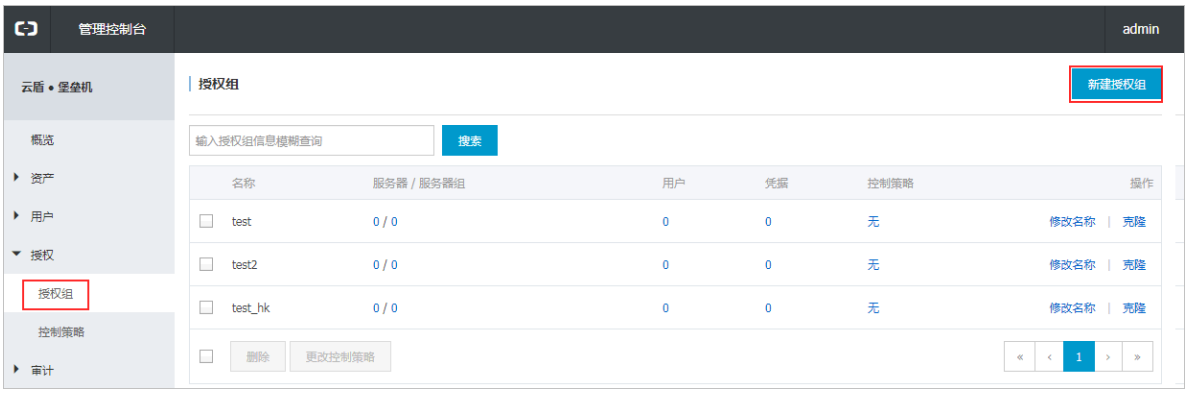
更多新建用户的操作，请参考用户管理。

9. 在新建用户对话框中，输入手机号码、密码、邮件、姓名，单击确定。

说明：

您输入的手机号码就是运维登录的用户名。

10. 定位到授权 > 授权组页面，单击右上角的新建授权组。在弹出的对话框中，输入授权组名称，单击确定。



11.单击已创建的授权组中**服务器/服务器组**、**用户**、**凭据** 、**控制策略**下方的文字，可将堡垒机的用户、服务器、凭据绑定在一起，并配置相应的控制策略。

说明：

其中服务器和凭据要对应，否则可能导致无法登录。

12.如果您希望堡垒机用户在通过 SSH 或 RDP 协议方式登录堡垒机时需要使用密码 + 短信验证码的双因子认证方式，可在**系统 > 系统设置**页面中勾选**双因子认证**选项，并单击**保存修改**。

审计查询操作

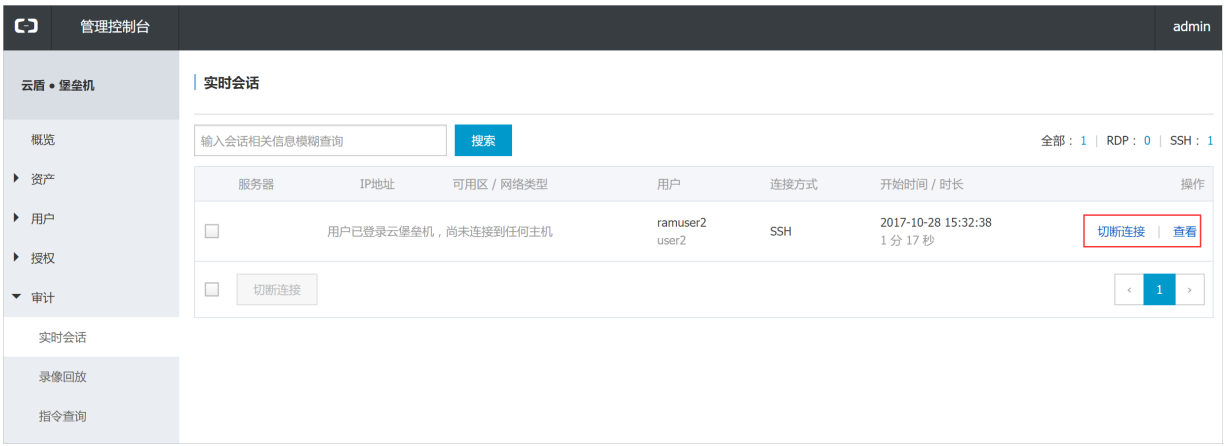
当用户以堡垒机用户的身份，通过 SSH、RDP、或 SFTP 协议方式登录云盾堡垒机并对已授权服务器进行运维操作时，您可在云盾堡垒机 Web 管理页面中查看该用户会话的详细信息。

> **说明：**
> 用户登录云盾堡垒机时，使用的用户名即为之前设定的用户手机号码。

关于如何登录堡垒机进行系统运维，请参考：

- *Mac*电脑运维
- *SSH*协议运维
- *SFTP*协议运维
- *RDP*协议运维

当用户登录堡垒机后对已授权服务器进行运维操作时，您可在**审计 > 实时会话**页面查看该用户的实时会话情况。单击**查看** 可以对该会话进行监控，也可以单击**切断连结**直接中断该实时会话。

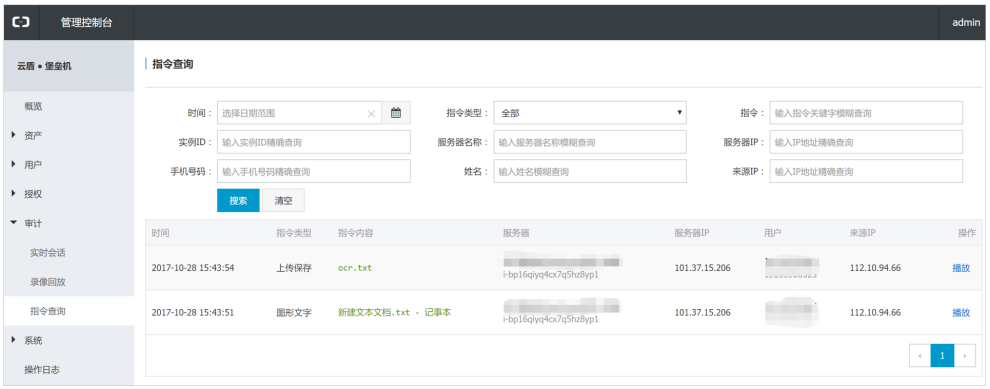


当用户的会话连接断开后，您可在**审计 > 录像回放**页面查看该用户的会话情况，单击**播放**查看该会话执行的操作。

您也可以在**审计 > 指令查询**页面，查看用户会话中输入并执行了哪些指令。

说明：

此功能仅针对已授权服务器上执行的命令行操作。



4 3.0.X版快速入门

登录云盾堡垒机系统

第一次登录时需要启用堡垒机实例。

1. 登录云盾堡垒机控制台。
2. 选择要操作的堡垒机实例，单击启用。

> 说明：
> 只有当实例状态为未初始化时，才会有启用操作。已初始化实例可以直接登录堡垒机系统。

3. 在启用对话框中，完成以下配置。
   a. 选择网络类型、已创建网络、交换机。

   > 说明：
   > - 网络类型和交换机在实例启用后无法修改。
   > - 若选择交换机后不可启用，是因为交换机下资源已用完。请更换一台交换机，或新建交换机供堡垒机部署选择。
   > - 若堡垒机是VPC类型，只要所选的VPC和ECS处于同一个VPC网络，交换机可任意选择（不会影响堡垒机和ECS内网相通）。

   b. 单击安全组ID，并选择ECS对应的安全组。

   > 说明：
   > 此操作允许堡垒机访问安全组内的ECS，可多选，支持启用后修改。

   c. 勾选公网访问控制类型。可选值：
      - 不对公网开放
      - 对公网白名单开放：勾选后，需进一步设置白名单IP。最多可填写30个IP或IP段。
      - 对公网全部开放
   d. 单击确定。等待启用生效。

启用堡垒机后，参照以下步骤登录堡垒机系统：

1. 登录云盾堡垒机控制台。
2. 选择要操作的堡垒机实例，单击管理。

3. 在管理对话框中，选择并单击接入方式：内网接入、公网接入。

进入云盾堡垒机系统。

步骤1：同步阿里云ECS资产

如果需要管理阿里云ECS以外的机器，请参考主机管理，手动创建主机或导入主机。

前提条件

- 授权堡垒机读取ECS列表信息。首次登录堡垒机控制台时会收到提示，需要您授权堡垒机读取ECS列表信息，以实现ECS快速接入。

  1. 登录云盾堡垒机控制台。
  2. 在页面上方提示中单击**授权**，完成授权。

  > **说明：**
  > 已完成授权时，不会出现该提示。

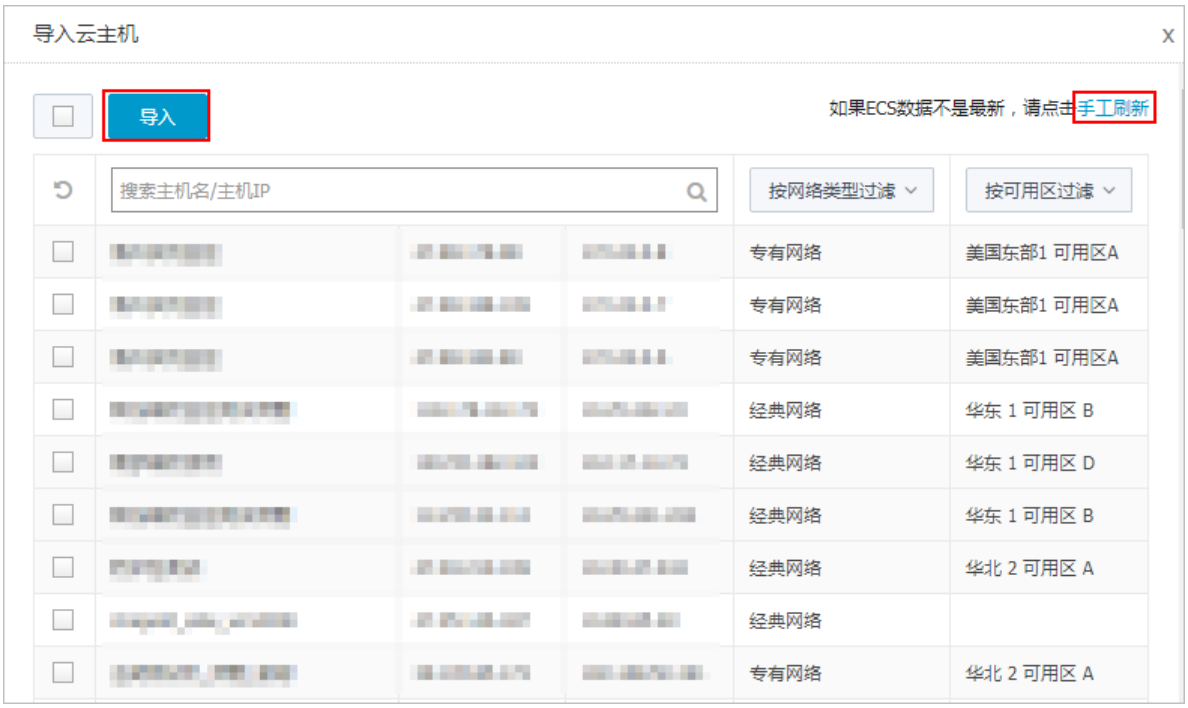
- 购买堡垒机的阿里云账号上有ECS实例。

操作步骤

1. 登录云盾堡垒机系统。
2. 前往资产 > 主机管理 页面，单击**ECS同步**页签。
3. 单击页面右上角的**同步阿里云ECS**。

4. 在导入云主机对话框中，勾选要导入的主机，并单击**导入**。

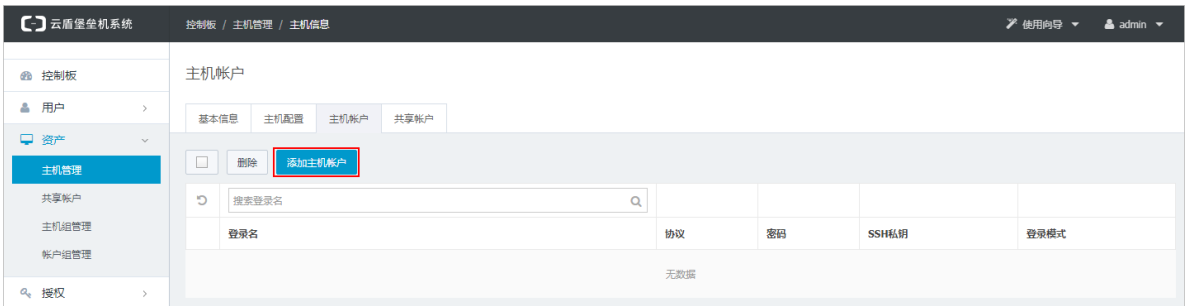
> **说明：**
> 如果ECS数据不是最新的，单击**手动刷新**重新检测。



成功导入ECS主机。

5. 在资产 > 主机管理页面主机列表中，单击要操作的主机IP，进入主机信息页面。

6. 单击主机帐户页签，然后单击添加主机帐户。



7. 在新建主机帐户对话框中，选择协议类型， 并填写有效的主机帐户登录名和密码（服务器上已经创建并存在的帐户和对应密码），单击创建主机帐户。

关于主机帐户选项的说明，请参考主机帐户选项说明。

成功创建主机帐户。

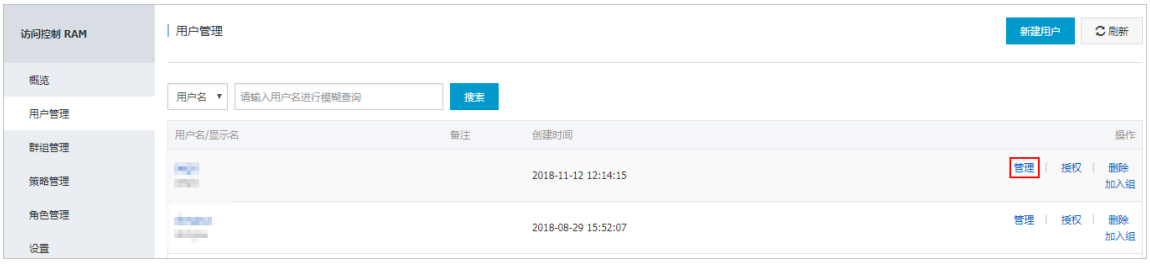
步骤2：导入阿里云子账号

如果需要新建本地用户，请参考用户管理。

前提条件

- 要导入的子账号需要关联虚拟MFA设备。

1. 登录阿里云访问控制*RAM*控制台。
2. 在用户管理页面，选择要操作的子账号，单击管理。



3. 在用户详情页面，单击启用虚拟**MFA**设备。


用户详情
用户授权策略
用户加入的组
基本信息
编辑基本信息
用户名
UID
创建时间 2018-11-12 12:14:15
显示名
aegis
手机
邮箱
备注 -
Web控制台登录管理
关闭控制台登录
重置密码
必须开启多因素认证
上次登录时间： 2018-11-12 12:16:14
下次登录必须重置密码：
多因素认证设备
类型
简介
启用状态
操作
虚拟MFA设备
遵循TOTP标准算法来产生6位数字验证码的应用程序
未启用
启用虚拟MFA设备

4. 在启用虚拟**MFA**设备页面，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。

5. 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。
6. 单击确定启用。

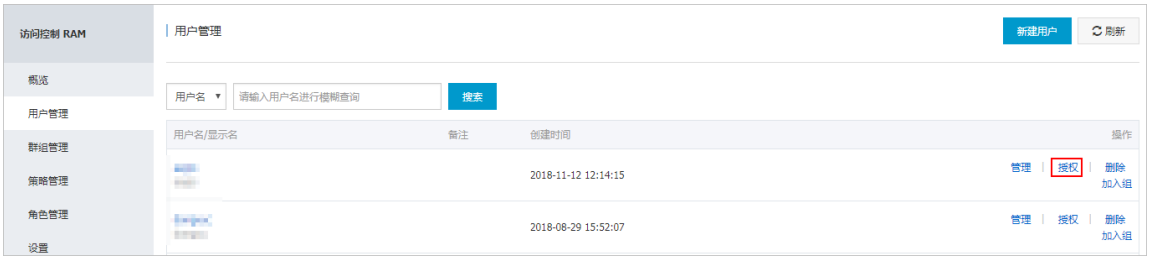
- 完成子账号授权。

堡垒机用户权限分为超级管理员（admin）和运维员两种。

- 阿里云主账号登录为admin权限，可以查看和管理所有数据。
- 子账号权限由主账号分配，可分配admin权限或者运维员权限。从限权角度，一般建议分配运维员权限。本地用户是运维员权限。

参照以下步骤为子账号授权：

1. 登录阿里云访问控制RAM控制台。
2. 在用户管理页面，选择要操作的子账号，单击授权。

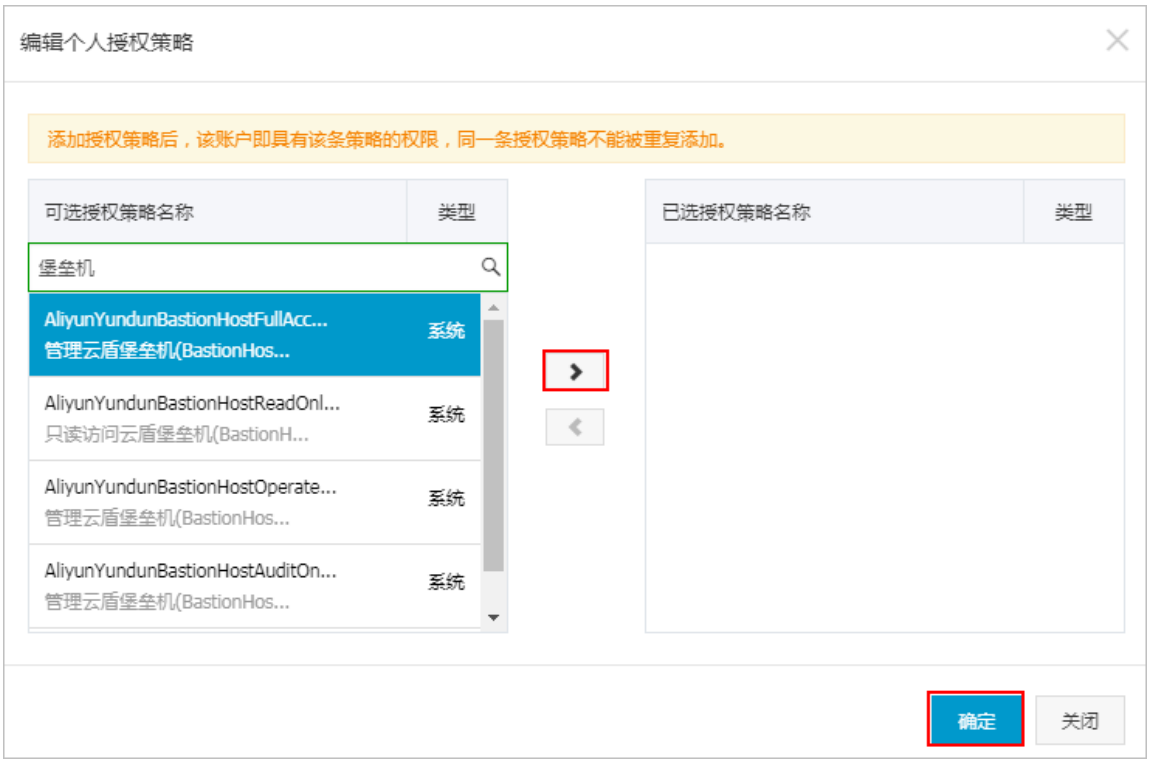


3. 在编辑个人授权策略对话框，可选授权策略名称下，输入“云盾堡垒机”搜索可用的系统策略。

   共有四个可用的系统策略：

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

   其中，FullAccess是管理员权限，其余三个是运维员权限，且无差别。



4. 选择要授予当前子账号的权限后，单击**确定**，完成授权。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在子账号管理页面，单击子账号列表下方的**刷新子账号数据**，从RAM获取最新的子账号数据。
3. 单击页面右上角的**导入子账号**。
4. 在导入阿里云子账号用户对话框中，勾选需要导入的子账号，并单击**导入子账号**。

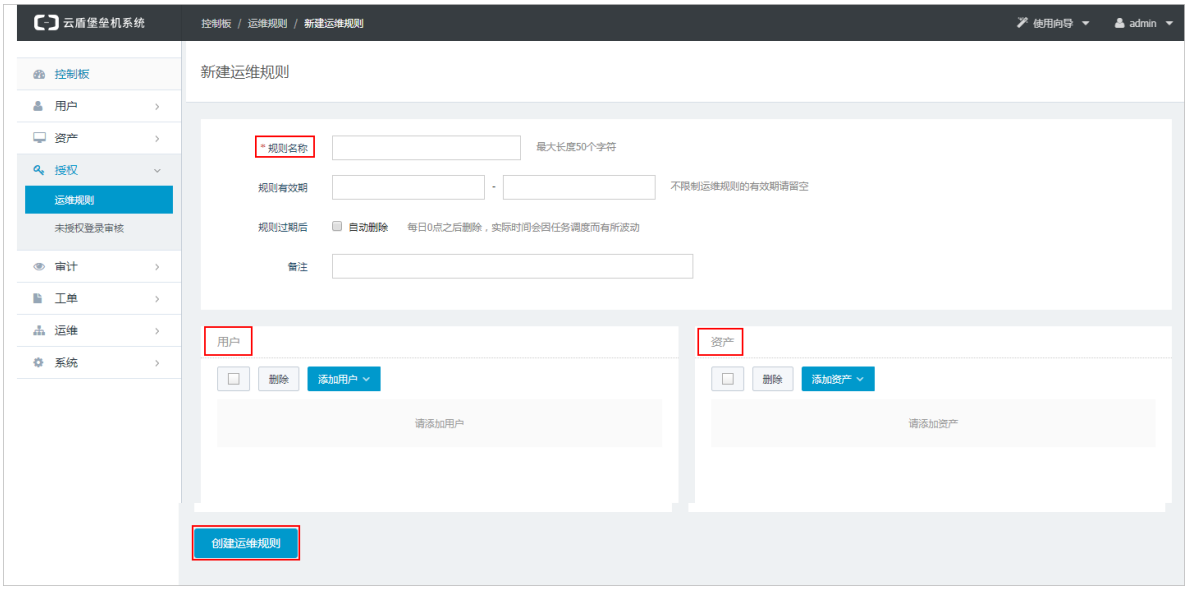
步骤3：创建运维规则

操作步骤

1. 登录云盾堡垒机系统。
2. 在**授权 > 运维规则**页面，单击**新建运维规则**。

3. 在新建运维规则页面，填写规则名称，选择授权用户和资产，并单击**创建**。

> **说明：**
> 您可以选择设置规则有效期。在规则过期后，用户和主机的运维授权关系即解除。



4. 成功创建规则后，您可以进一步编辑该规则，启用更多限制功能。例如，

   - 启用登录限制，限制允许/拒绝的访问来源IP，限制访问时间段等。
   - 启用命令控制，限制允许访问者使用的命令。
   - 启用协议控制，配置各个协议会话中的相关控制选项。

   具体请参考运维授权。

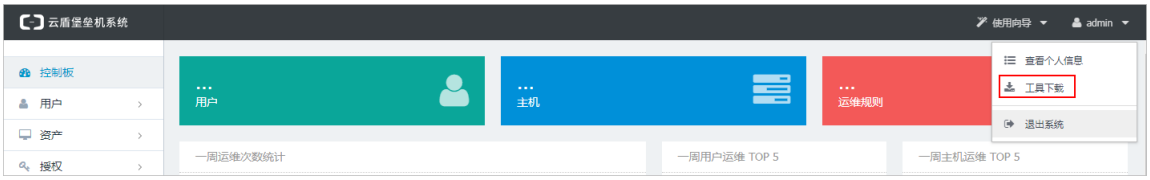
步骤4：主机运维

Windows客户端

分为BS运维和CS运维。CS运维请参考*SSH*协议运维。BS运维需满足以下前提条件：

- 下载安装单点登录器。

1. 登录云盾堡垒机系统。
2. 在右上角用户菜单下单击工具下载。



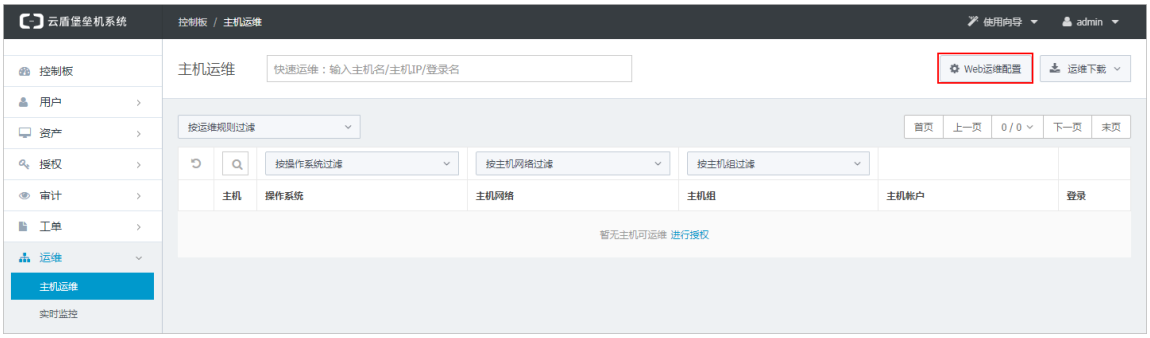
3. 下载并安装单点登录器。

说明：

请勿使用迅雷下载。使用浏览器下载，并安装在C盘；下载安装过程中关闭安全检测软件。

- 设置相应协议的运维配置。

1. 登录云盾堡垒机系统。
2. 在运维 > 主机运维页面，单击右上角的**Web运维配置**。



3. 在**Web运维配置**对话框中完成相应配置。具体请参考*BS*运维操作。

4. 单击保存，完成配置。

Mac客户端

因Mac环境和单点登录器不兼容，仅支持CS运维。具体请参考*SSH*协议运维。