ALIBABA CLOUD

Alibaba Cloud

堡垒机

快速入门

文档版本：20220210

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.概览

本文指导您在开通V3.2版本堡垒机实例后，快速部署主机资产、堡垒机用户、运维规则，使用堡垒机实现主机运维，并通过堡垒机审计运维会话。

在使用V3.2版本堡垒机时，您可以按照以下步骤进行操作。

任务	描述
步骤1：同步阿里云ECS资产	在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中添加要管理的主机资产。在该任务中，管理员将在堡垒机实例中同步导入当前阿里云账号下的ECS资产并新建主机账户。
步骤2：导入阿里云RAM用户	在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中创建堡垒机用户。在该任务中，管理员在堡垒机实例中导入阿里云RAM用户（即阿里云子账号）作为堡垒机用户。
步骤3：创建运维规则	在使用堡垒机进行主机运维前，管理员需要创建运维规则，授权指定用户运维指定资产。在该任务中，管理员创建运维规则，授权指定用户运维指定主机和主机账户。
步骤4：主机运维	当管理员在堡垒机实例中完成主机资产、堡垒机用户、运维规则部署后，堡垒机用户可以通过CS运维方式访问已授权主机，进行运维操作。在该任务中，运维人员将了解CS运维的具体操作方法。
步骤5：审计运维会话	当运维人员通过SSH、RDP、SFTP协议方式登录堡垒机并对已授权服务器进行运维操作时，管理员可以在堡垒机Web管理页面查看用户会话的详细信息。在该任务中，管理员在堡垒机实例中进行审计查询和阻断高危会话操作。

更多堡垒机的功能，例如配置用户组、主机组实现批量操作，请参见用户指南（V3.2版本）。

2.启用堡垒机

购买堡垒机实例后，您需要启用堡垒机实例，才能使用堡垒机实例的服务。本文介绍如何启用堡垒机实例。

背景信息

新购买的堡垒机实例处于未初始化状态，需要启用后才能使用。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在堡垒机实例列表中，选择要启用的堡垒机实例，单击**启用**。

3. 在**启用**面板上，完成以下配置。

配置说明如下表。

配置项	说明
网络	选择堡垒机实例的专有网络和虚拟交换机。 **注意** ○ 专有网络和虚拟交换机在实例启用后无法修改。 ○ 为了确保内网连通，建议堡垒机实例最好与被运维的ECS使用同一个专有网络。 ○ 如果选择的交换机下资源已用完，则会导致堡垒机实例启用失败。如果出现选择交换机之后堡垒机实例启用失败的情况，请您更换一台交换机尝试。您也可以提前创建一个交换机，供堡垒机部署时选择。相关内容，请参见创建交换机。

配置项	说明
安全组	选择ECS对应的安全组。 **说明** ○ 堡垒机至少要加入一个普通安全组后才能启用，支持在启用后修改堡垒机所属安全组。堡垒机加入普通安全组后会自动生成访问规则，允许堡垒机访问该安全组内的ECS资产。 ○ 您也可以为堡垒机手动配置安全组访问规则。配置安全组访问规则后，堡垒机无须再加入安全组。配置安全组访问规则的具体操作，请参见添加安全组规则。 ○ 堡垒机不支持加入企业安全组，需手动配置企业安全组访问规则实现网络互通。配置安全组访问规则的具体操作，请参见添加安全组规则。

4. 单击**确定**。

   单击确定后，堡垒机实例会进入**初始化中**的状态。

   说明 初始化需要20分钟左右，请您耐心等待。初始化结束后，堡垒机实例会进入**运行中**的状态，表明该堡垒机实例已成功启用。

执行结果

成功启用堡垒机实例后，您可以在堡垒机实例列表中，单击**管理**，进入堡垒机控制台。

3.登录堡垒机系统

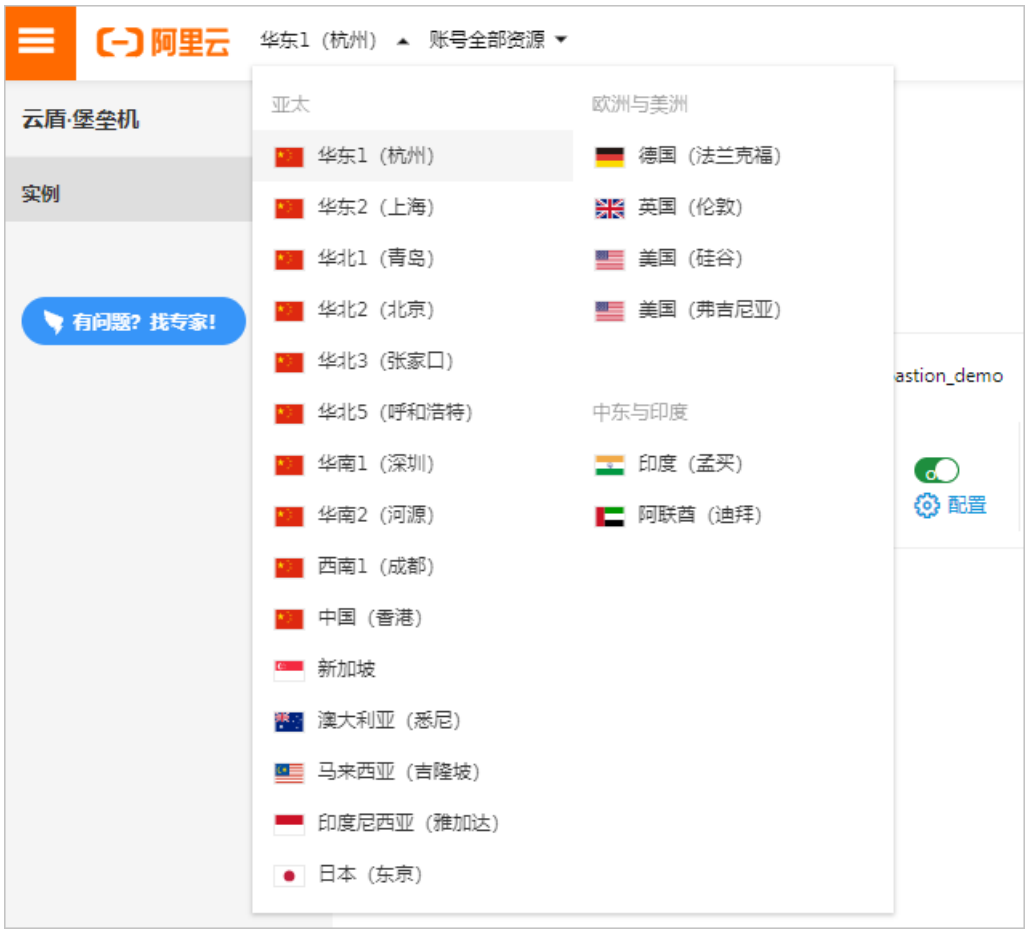
本文介绍了如何通过Web方式登录堡垒机系统。

背景信息

> **说明** 支持阿里云主账号和RAM账号登录堡垒机Web界面。

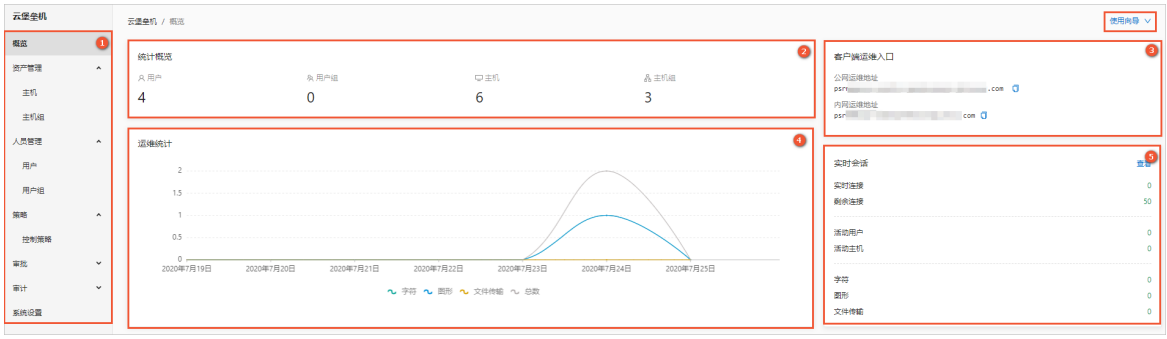
操作步骤

1. 登录云盾堡垒机控制台。
2. 在顶部区域下拉框中，选择堡垒机所在的地域。



3. 在堡垒机实例列表中，单击目标实例右侧的**管理**，进入堡垒机系统。

4. 选择接入方式，连接目标堡垒机Web 管理页面。



区域	说明
1	显示系统的功能菜单项。
2	统计用户、用户组、主机、主机组等信息。
3	运维的内网和外网口。
4	运维统计信息。
5	最近运维的概况信息。

4.步骤1：同步阿里云ECS资产

在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中添加要管理的主机资产和主机账户。本文指导管理员在堡垒机实例中导入当前阿里云账号下的ECS资产和添加主机账户。

背景信息

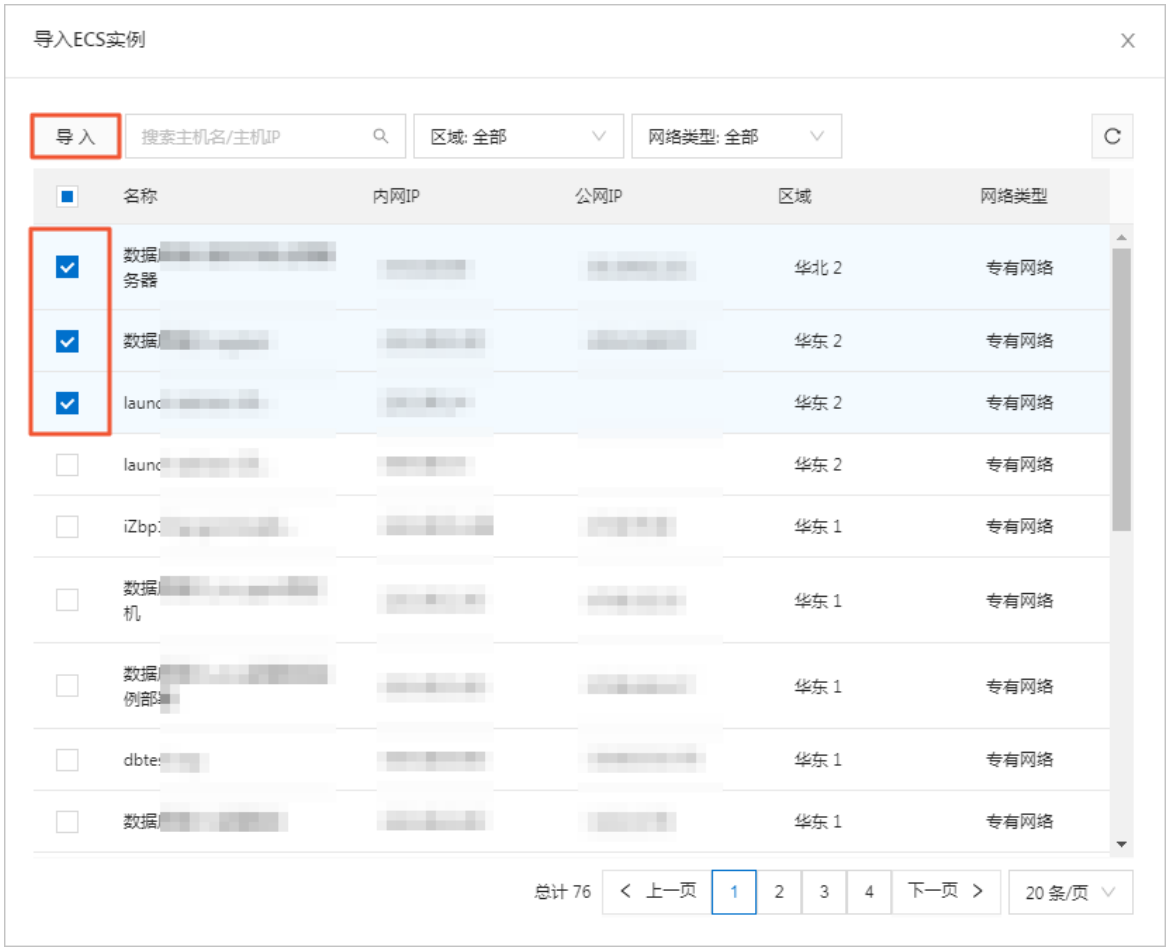
除了同步阿里云ECS资产，您还可以手动添加主机、从文件导入主机、导入RDS专有主机组。具体操作，请参见导入其他来源主机。

导入阿里云ECS实例

导入阿里云ECS实例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。具体参见以下步骤：

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**资产管理 > 主机**。
3. 在**主机**页面，单击**导入ECS实例**。
4. 在**选择区域**对话框中，选中需要同步的ECS实例所属的区域并单击**确定**。

5. 在**导入ECS实例**对话框中，选中需要导入的ECS并单击**导入**。



操作步骤

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**资产管理 > 主机**。
3. 在**主机**页面，为目标主机新建主机账户。
   - **为一个主机新建主机账户**
     a. 单击目标主机**操作**列的**新建主机账户**。

b. 在**新建主机账户**面板上，设置账户的**协议**、**登录名**和**认证类型**等参数。

c. 单击**验证密码**。

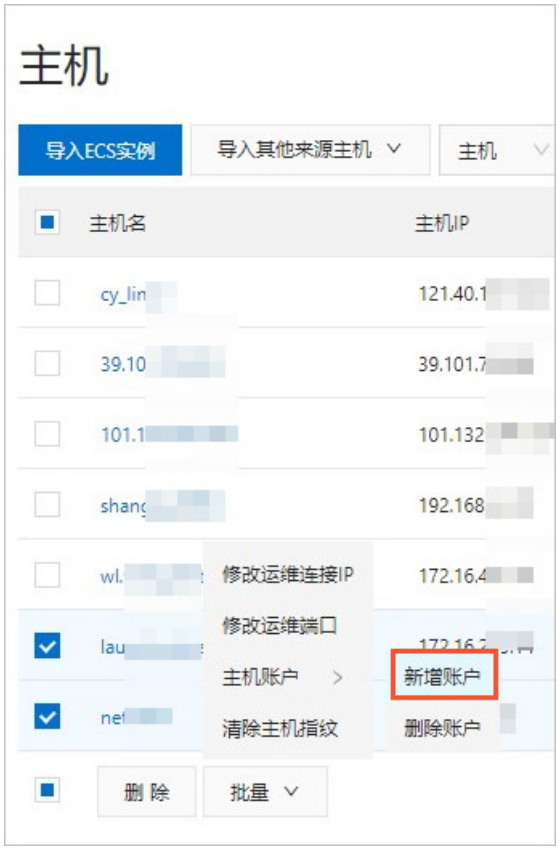
使用**验证密码**可以测试主机账户的用户名和密码是否正确。

d. 单击**创建**。

- **为多个主机新建主机账户**

a. 在主机列表中选中多个要新建主机账户的主机。

b. 在主机列表下方选择**批量 > 主机账户 > 新增账户**。



c. 在新增账户对话框中设置**认证类型**、**协议**、**登录名**等参数。

> **说明** 批量新增账户时，无需验证密码。

d. 单击下方**确定**。

5.步骤2：导入阿里云RAM用户

在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中创建堡垒机用户。本文将指导管理员在堡垒机实例中导入阿里云RAM用户（即阿里云子账号）作为堡垒机用户。

前提条件

- 开通堡垒机实例的阿里云账号下，已创建RAM用户。关于创建RAM用户的具体操作，请参见创建RAM用户。
- 要导入的阿里云RAM用户如果需要关联虚拟MFA设备，请参见为RAM用户启用多因素认证。

操作步骤

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**人员管理 > 用户**。
3. 在**用户**页面，单击**导入RAM用户**。
4. 在RAM用户列表中，选中需要导入的RAM用户。

   > **说明** 如果需要导入单个RAM用户，您可以直接在该用户的**操作**列中单击**导入**。

5. 单击**导入**。
   导入完成后，用户即可使用已导入的账号登录堡垒机。

6.步骤3：创建运维规则

在使用堡垒机进行主机运维前，管理员需要创建运维规则，授权指定用户运维指定主机和主机账户。本文将指导管理员创建运维规则。

授权主机

为用户授权主机，具体操作请参见以下步骤：

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**人员管理 > 用户**。
3. 在需要授权用户的**操作**列中，单击**授权主机**。

4. 在**已授权主机**页签下，单击**授权主机**。
5. 在授权主机面板上的主机列表中选中要授权的主机，单击**确定**。

授权主机账户

为用户授权单个主机的登录账户，具体操作请参见以下步骤：

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**人员管理 > 用户**。
3. 在需要授权用户的**操作**列中，单击**授权主机**。

4. 在**已授权主机**页签中，单击**已授权账户**列下的账户名称或**无已授权账户，点击授权账户**。

5. 选中主机账户并单击**更新**。

> **说明** 如果主机中没有账号，那么您可以单击**新建主机账户**创建主机账户。

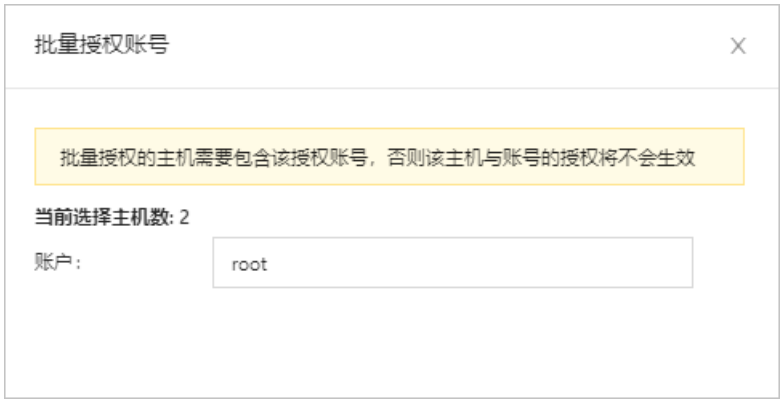
批量授权主机账户

为用户批量授权多个主机的登录账户，具体操作参见以下步骤：

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**人员管理 > 用户**。
3. 在需要授权用户的**操作**列中，单击**授权主机**。

4. 选中需要授权账户的主机并单击**批量 > 批量授权账号**。

5. 选中主机授权账户的**账户**名称。



> **说明** 批量授权主机账号时，只能选择一个主机账户进行授权。

6. 单击**更新**。

7.步骤4：主机运维

当管理员在堡垒机实例中完成主机资产、用户、运维规则部署后，堡垒机用户可以通过CS运维方式访问已授权主机，进行运维操作。本文将指导运维人员完成运维配置和登录。

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。该运维方式支持Windows和Mac操作系统。

- Windows操作系统
  - SSH协议运维
  - RDP协议运维
  - SFTP协议运维
- Mac操作系统
  - SSH协议运维
  - RDP协议运维
  - SFTP协议运维

8.步骤5：审计运维会话

当堡垒机用户通过SSH、RDP、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，管理员可以在云盾堡垒机**审计 > 实时监控**页面查看用户会话的详细信息。本文将指导管理员在堡垒机实例中进行审计查询和阻断高危会话。

搜索会话

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**审计 > 实时监控**。
3. 设置搜索条件。

您可以参考以下表格中的搜索项说明设置搜索条件。

搜索项	说明
协议	在下拉栏中选择会话的协议类型，支持**全部**、SSH、SFTP和RDP。
主机IP	输入会话中运维的目标主机IP。
主机名	输入会话中运维的目标主机名。
用户	输入会话的用户名。
登录名	输入会话中用户登录主机所使用的登录账号名称。
来源IP	输入会话的来源IP，即用户访问时使用的IP。
会话ID	输入会话ID。

4. （可选）单击**保存**，在**查询条件名称**中输入名称，单击**确定**，保存查询条件。

> **说明** 保存搜索条件后，下次如果需要设置相同的搜索条件，可以直接会话列表右上角的**默认条件**列表中选择该搜索条件。

5. 单击**搜索**。

实时监控页面阻断会话

1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。

2. 在左侧导航栏，选择**审计 > 实时监控**。
3. 在会话结果列表中，选中需要阻断的会话。

4. 单击**阻断会话**。