

ALIBABA CLOUD

阿里云

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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

- 1.概览 ----- 05
- 2.启用堡垒机 ----- 06
- 3.登录堡垒机系统 ----- 08
- 4.步骤1：同步阿里云ECS资产 ----- 10
- 5.步骤2：导入阿里云RAM用户 ----- 14
- 6.步骤3：创建运维规则 ----- 15
- 7.步骤4：主机运维 ----- 18
- 8.步骤5：审计运维会话 ----- 19
- 9.V3.1版本 ----- 21
 - 9.1. 概览 ----- 21
 - 9.2. 登录实例 ----- 21
 - 9.3. 步骤1：同步阿里云ECS资产 ----- 24
 - 9.4. 步骤2：导入阿里云子账号 ----- 26
 - 9.5. 步骤3：创建运维规则 ----- 28
 - 9.6. 步骤4：主机运维 ----- 30

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）](#)。

您还可以通过观看以下视频，快速了解使用堡垒机的基本操作。

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

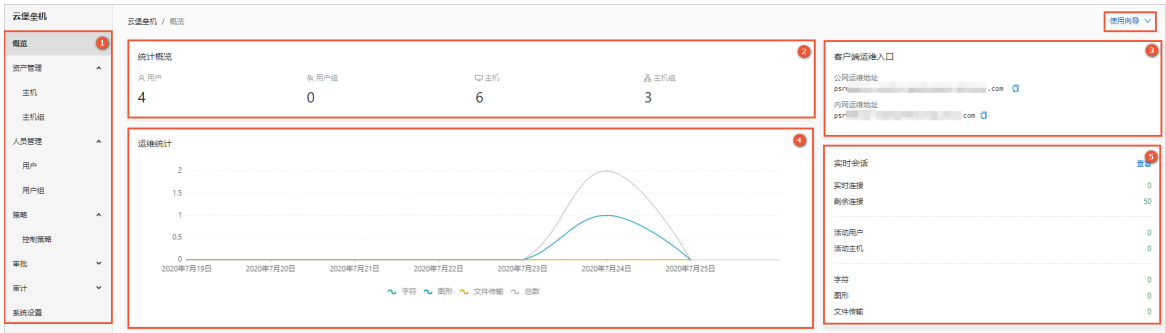
1. 登录云盾堡垒机控制台。
2. 在顶部区域下拉框中，选择堡垒机所在的地域。



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。

选择区域

亚太

华北 1	华北 2	华北 3	华北 5
华东 1	华东 2	华南 1	西南1 (成都)
香港	亚太东北 1 (东京)	亚太东南 1 (新加坡)	亚太东南 2 (悉尼)
亚太东南 3 (吉隆坡)	亚太东南 5 (雅加达)		

欧洲与美洲

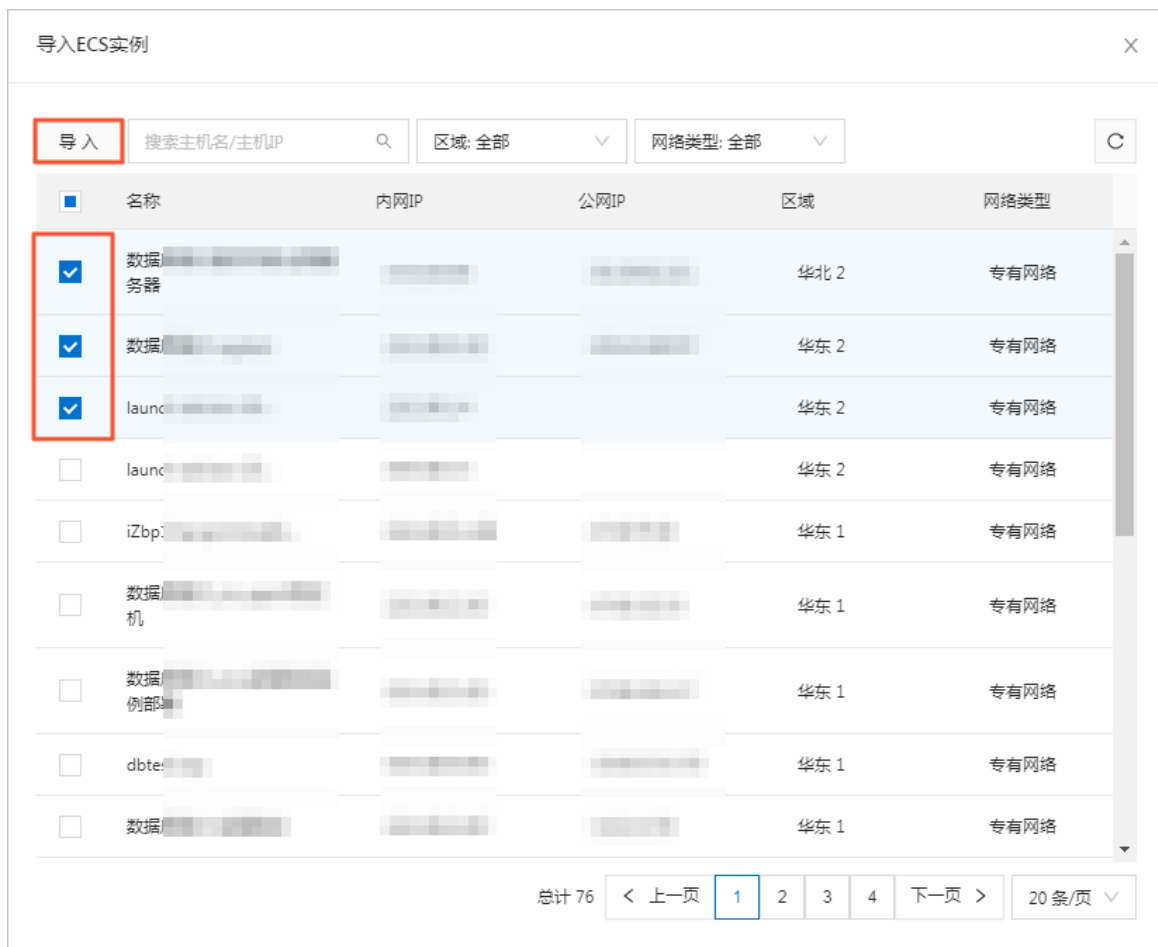
美国东部 1 (弗吉尼亚)	美国西部 1 (硅谷)	英国 (伦敦)	欧洲中部 1 (法兰克福)
---------------	-------------	---------	---------------

中东与印度

亚太南部 1 (孟买)	中东东部 1 (迪拜)
-------------	-------------

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。

新建主机账户

×

请确认主机或ECS实例上已经创建了对应的操作系统账户，堡垒机不会将主机账户同步到主机或ECS实例。

* 协议

SSH

▼

* 登录名

bastion_ onaliyun.com

认证类型

密码

▼

密码

.....

🔑

?

验证密码

c. 单击验证密码。

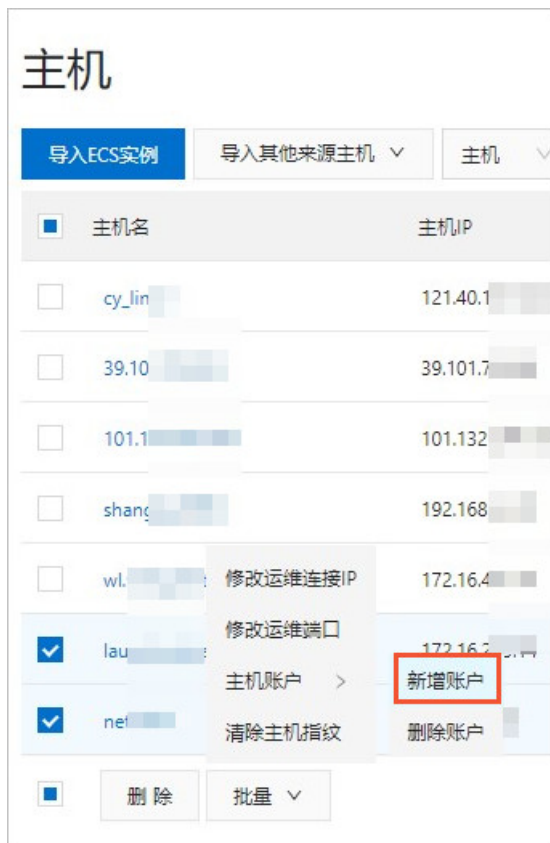
使用验证密码可以测试主机账户的用户名和密码是否正确。

d. 单击创建。

o 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。

② 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定要授权的主机，单击确定。

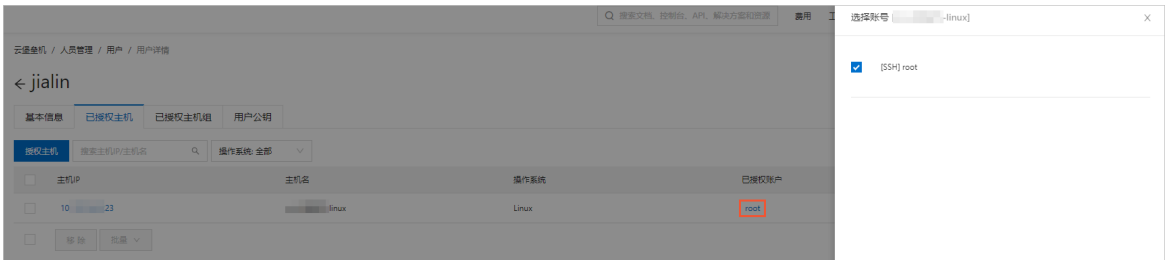
授权主机账户

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：

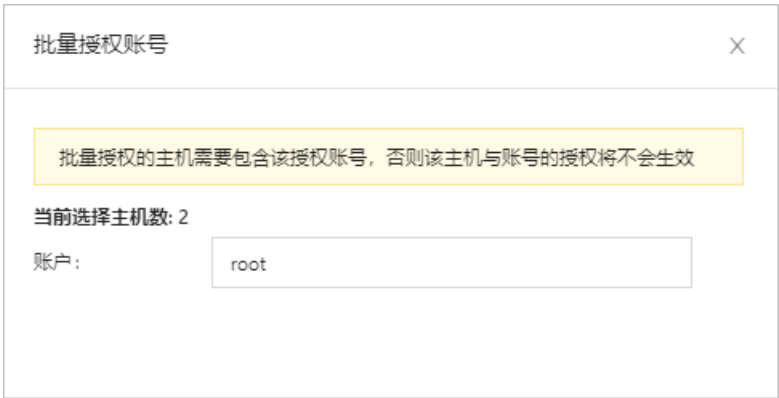
- 1. 登录堡垒机系统。具体操作，请参见[登录堡垒机系统](#)。
- 2. 在左侧导航栏，选择人员管理 > 用户。
- 3. 在需要授权用户的操作列中，单击授权主机。



- 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。

云堡垒机 / 审计 / 实时监控

实时监控

协议：

全部

主机IP：

请输入主机IP

主机名：

请输入主机名

用户：

请输入用户名

登录名：

请输入登录名

来源IP：

请输入来源IP

会话ID：

请输入会话ID

搜索

重置

查询条件：

清除

保存

默认条件

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。

实时监控

协议：

全部

主机：

请输入主机名/主机IP

用户：

请输入用户名

登录名：

请输入登录名

来源IP：

请输入来源IP

会话ID：

请输入会话ID

搜索

重置

查询条件：

清除

保存

默认条件

☒	类型	主机	协议/登录名	用户/来源IP	开始时间/时长	会话操作
☒	SHELL	10.10.10.223 堡垒机	SSH root	zhangsan@10.10.10.223 22	2019-10-12 17:38:57 4分17秒	播放 详情

☒ 阻断会话

总计 1

< 上一页

1

下一页 >

20 条/页

4. 单击阻断会话。

9.V3.1 版本

9.1. 概览

本文将指导您在开通V3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，并使用堡垒机实现主机运维。

在使用V3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。
步骤2：导入阿里云子账号	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，管理员将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，管理员将创建运维规则。
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BS运维或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BS运维和CS运维的具体操作方法。

9.2. 登录实例

开通云盾堡垒机实例后，您需要启用并登录实例，才能使用指定实例下的服务。

操作步骤

1. 登录[云盾堡垒机控制台](#)。
2. 如果您已经启用过实例，请直接前往下一步；否则，请参照以下步骤启用实例：
 - i. 选择要启用的堡垒机实例，单击启用。

 说明 只有当实例状态为未初始化时，才会出现启用操作。

云盾 • 堡垒机	未初始化  未命名				
实例	香港	版本	规格	到期时间	
账户	未初始化	V3.1.0	堡垒机_50资产授权	2019年4月27日	

- ii. 在启用对话框中，完成以下配置。

配置项	说明
-----	----

配置项	说明
网络	选择虚拟机实例的专有网络和虚拟交换机。  说明 ■ 专有网络和虚拟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）。
安全组	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。
公网访问控制	选择公网访问控制类型。可选值： ■ 公开模式 0.0.0.0/0：允许所有公网地址访问。 ■ 白名单访问模式：允许10.0.0.0/8，172.16.0.0/12，192.168.0.0/16和配置在白名单地址访问。选择后，需进一步配置白名单。最多可添加30个IP地址或地址段。 ■ 内网访问模式：只允许10.0.0.0/8，172.16.0.0/12，192.168.0.0/16地址访问。

启用 (VPC)

网络

请选择专有网络

请选择虚拟交换机

安全组

请选择

选择后，允许堡垒机访问安全组内的ECS

堡垒机

ECS

公网访问控制

公开模式 0.0.0.0/0

公网

内网

堡垒机

确定

取消

iii. 单击确定，等待启用生效。

3. 选择要登录的堡垒机实例，单击管理。

云盾 • 堡垒机	全部状态	全部地区
实例	运行中	未命名
账户	华东2（上海）	版本 V3.1.0 新版本
	规格 堡垒机_20资产授权	到期时间 2019年5月3日
	配置	管理

4. 在管理对话框中，选择一种接入方式：内网接入、公网接入。

管理

请选择以私网还是公网连接方式访问堡垒机控制台：

内网接入

公网接入

取消

执行结果

成功登录指定的云盾堡垒机实例。

9.3. 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。本文将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。

前提条件

开通堡垒机实例的阿里云账号下开通有ECS实例。关于如何开通ECS实例，请参见[创建ECS实例](#)。

背景信息

除了导入阿里云ECS作为堡垒机资产外，您还可以手动添加或批量导入非阿里云主机作为堡垒机资产。更多信息，请参见[主机管理](#)。

操作步骤

1. （可选）授权堡垒机读取ECS列表信息。

首次登录堡垒机控制台时，您会收到提示，需要授权堡垒机读取ECS列表信息，以实现ECS快速接入。您可以参照以下步骤进行授权：

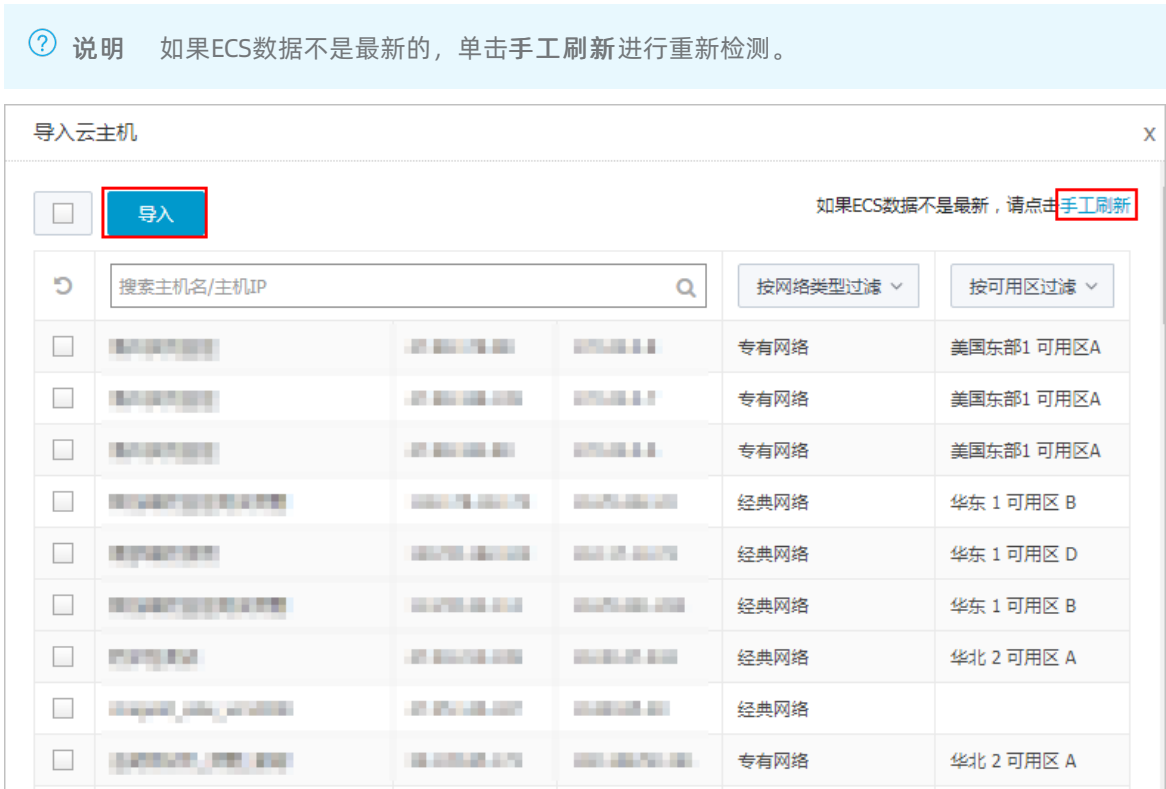
- i. 登录[云盾堡垒机控制台](#)。
- ii. 在页面上方提示中单击[授权](#)，完成授权。



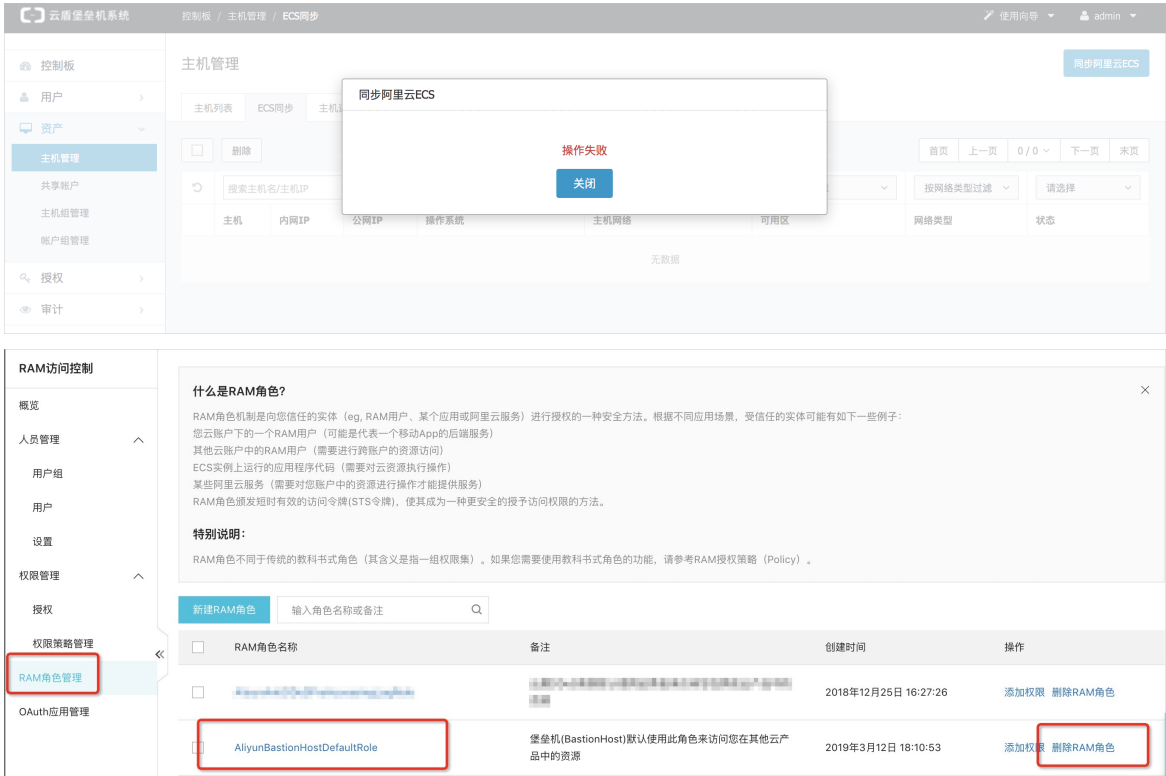
2. 登录[云盾堡垒机实例](#)。
3. 前往[资产 > 主机管理](#) 页面，并打开ECS同步页签。
4. 单击页面右上角的同步阿里云ECS。



5. 在导入云主机对话框中，勾选要导入的主机，并单击导入。



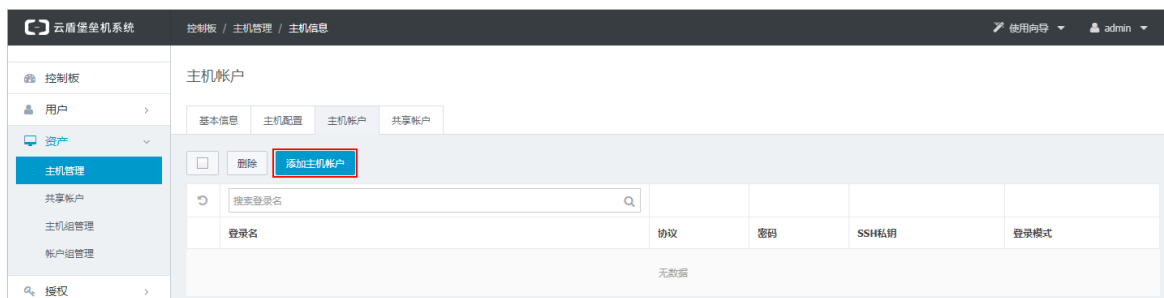
成功导入ECS主机。您需要进一步为已导入的主机添加主机帐户信息。
如果提示操作失败，建议您前往RAM访问控制控制台的[RAM角色管理](#)页面，删除AliyunBastionHostDefaultRole角色，并参照步骤1重新完成授权。完成授权后，堡垒机默认使用上述角色访问其他云产品的资源。若该角色失效，则可能导致操作失败；通过重新授权，可以修复该问题。重新授权后，请重新执行步骤2~步骤5，同步阿里云ECS。



6. 在资产 > 主机管理页面，打开主机列表页签，并单击要操作的主机IP。



7. 打开主机帐户页签，单击添加主机帐户。



8. 在新建主机帐户对话框中，选择协议类型，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），并单击创建主机帐户。



成功创建主机帐户，完成阿里云ECS资产同步。

后续步骤

步骤2：导入阿里云子账号

9.4. 步骤2：导入阿里云子账号

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。本文介绍如何在堡垒机实例中导入阿里云RAM用户（即阿里云子账号）。

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](#)

户。

- 要导入的阿里云子账号需要关联虚拟MFA设备。关于为子账号关联虚拟MFA设备的具体操作，请参见[为RAM用户启用多因素认证](#)。

说明 对于3.1.3及以上版本的堡垒机，如果您不需要子账号进行双因子认证，可以不做子账号的MFA关联。

- 要导入的子账号拥有堡垒机关联权限。

堡垒机用户权限分为超级管理员（admin）和运维员两种，对应阿里云访问控制的系统权限策略分别是AliyunYundunBastionHostFullAccess和AliyunYundunBastionHostOperateOnlyAccess。

- 阿里云主账号拥有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，可被分配admin权限或者运维员权限。从限权角度，一般建议您为子账号分配运维员权限。直接在堡垒机实例中创建的本地用户拥有运维员权限。

关于为子账号授权的具体操作，请参见[为RAM用户授权](#)。

背景信息

除了导入阿里云子账号作为堡垒机用户外，您还可以手动创建本地用户或者导入AD、LDAP用户作为堡垒机用户。更多信息，请参见[用户管理](#)。

要导入阿里云子账号作为堡垒机用户，您必须依次完成两次导入操作：

- 导入阿里云子账号到堡垒机账户系统，见下文步骤3。
- （从堡垒机账户系统中）导入RAM子账号到具体堡垒机实例，见下文步骤7。

操作步骤

- 登录[云盾堡垒机控制台](#)。
- 在账户页面，单击添加子账号。



- 在添加子账号对话框中，单击刷新子账号，获取当前阿里云账号的RAM子账号信息；然后选中要导入的子账号并单击导入子账号。



成功将RAM子账号导入到堡垒机，已导入堡垒机的子账号支持进一步导入到具体的堡垒机实例中。

- 4. 登录云盾堡垒机实例。
- 5. 在左侧导航栏单击用户 > 用户管理。
- 6. 在用户管理页面，单击导入RAM子账号。



- 7. 在导入RAM子账号对话框中，选择要导入到实例中的RAM子账号，并单击导入。

说明 只有已经通过步骤3成功导入堡垒机的RAM子账号，才会显示在RAM子账号列表中。若列表为空，请先通过步骤3将子账号导入到堡垒机。



成功将阿里云子账号导入到指定的堡垒机实例。

后续步骤

步骤3：创建运维规则

9.5. 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。本文将指导管理员创建运维规则。

背景信息

除了创建授权规则，明确具体用户的可运维主机范围外，云盾堡垒机还支持开启未授权登录。开启未授权登录后，用户在登录未授权主机时需要通过临时授权审核。更多信息，请参见[未授权登录审核](#)。

操作步骤

1. [登录云盾堡垒机实例](#)。
2. 前往[授权 > 运维规则](#)页面，单击[新建运维规则](#)。



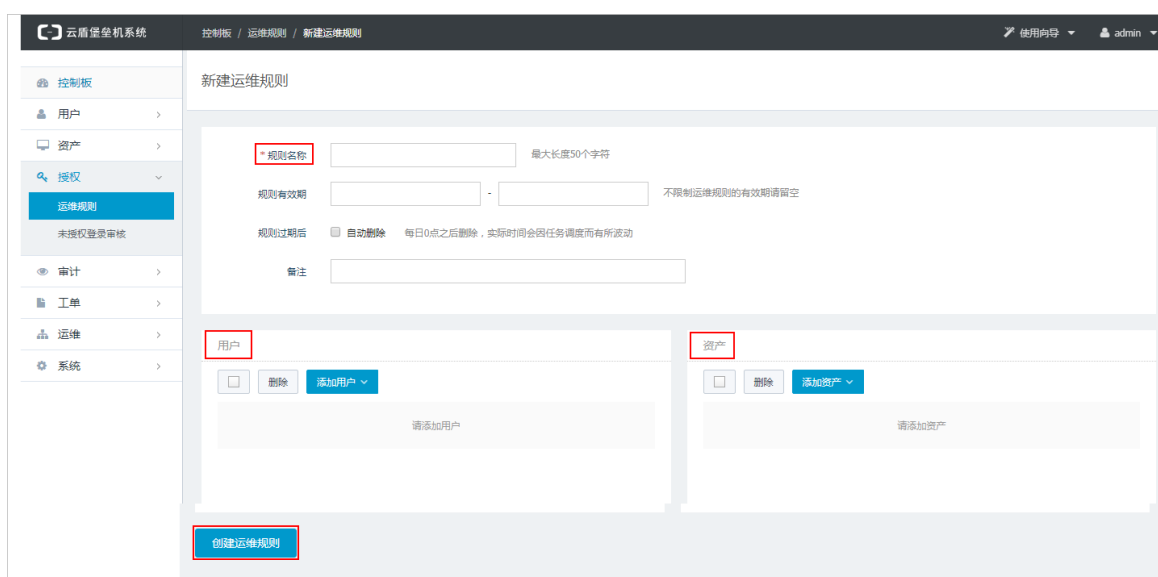
3. 在[新建运维规则](#)页面，填写规则名称，选择授权用户和资产，并单击[创建](#)。

说明

- 添加资产时，建议您选择添加资产帐户。在主机详情里面创建的主机帐户即对应此处的资产帐户。



- 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自动解除。



成功创建运维规则。针对已创建的运维规则，您可以进一步编辑其内容，启用更多限制功能。支持配置

的功能包括：

- 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。

具体操作，请参见[运维授权](#)。

后续步骤

步骤4：主机运维

9.6. 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BS运维或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。

管理员监控和审计运维

针对运维人员的主机运维，管理员可以进行实时监控和会话审计。

- 实时监控：实时监控专注于事中控制，管理员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。更多信息，请参见[实时监控](#)。
- 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。更多信息，请参见[会话审计](#)。

BS运维

BS运维指运维人员以RAM用户身份登录堡垒机控制台，进入Web运维页面；然后调用本地客户端，单点登录ECS进行运维。

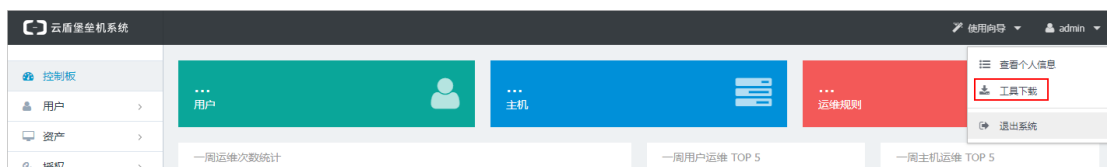
该运维方式仅支持RAM用户账号使用，且仅支持Windows环境。在使用BS运维时，您需要安装单点登录器并完成Web运维配置。

操作步骤

1. 使用RAM用户账号，通过RAM用户登录地址登录云盾堡垒机控制台。

 **说明** RAM用户登录地址和RAM用户账号由管理员向您提供；其中，RAM用户登录地址可以在访问控制控制台概览页查看，RAM用户账号必须已导入堡垒机（参见[步骤2：导入阿里云子账号](#)）。

2. 选择要操作的实例，单击[运维](#)，进入Web运维页面。
3. 如果您已经安装单点登录器，请直接前往下一步；否则，请参照以下步骤安装单点登录器：
 - i. 打开页面右上角的用户菜单，并单击[工具下载](#)。



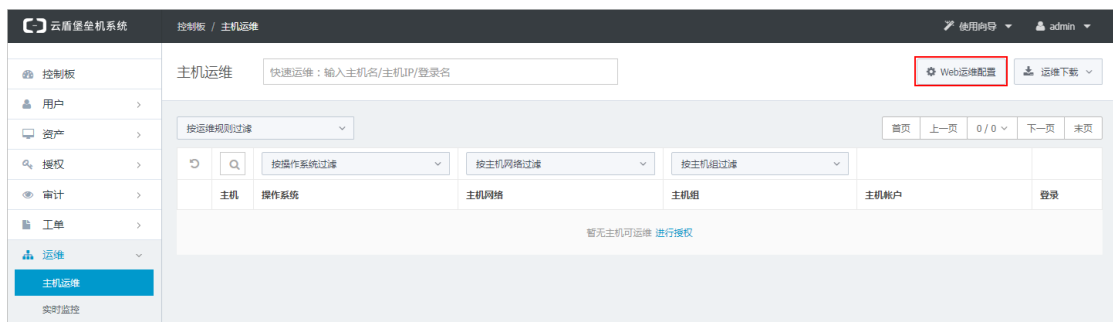
ii. 下载并安装单点登录器。

② 说明 请勿使用迅雷下载。使用浏览器下载，并安装在C盘；下载安装过程中请关闭安全检测软件。



4. 如果您已经完成Web运维配置，请直接前往下一步；否则，请参照以下步骤进行Web运维配置：

i. 前往运维 > 主机运维页面，单击页面右上角的Web运维配置。



ii. 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](#)。



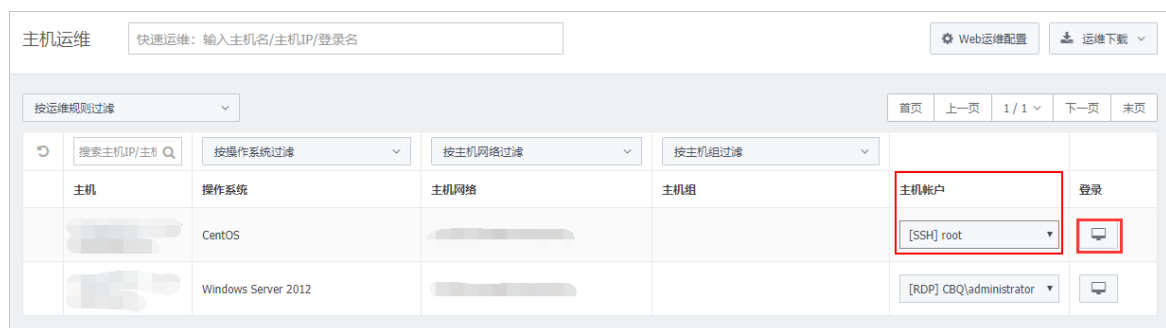
Web运维配置对话框包含以下配置项：

- RDP**：分辨率 默认
- SSH & TELNET & Rlogin**：连接模式 ☐ 连接到管理会话
- 本地设备和资源**：
 - ☒ 打印机
 - ☒ 剪贴板
 - ☒ 智能卡
 - ☒ 端口
 - ☒ 其他支持的即插即用(PnP)设备
 - ☒ 将我的所有监视器用于远程会话
- 本地驱动器**：
 - ☐ 全部
 - ☐ C: ☐ D: ☐ E: ☐ F: ☐ G:
 - ☐ H: ☐ I: ☐ J: ☐ K: ☐ L:
 - ☐ M: ☐ N: ☐ O: ☐ P: ☐ Q:
 - ☐ R: ☐ S: ☐ T: ☐ U: ☐ V:
 - ☐ W: ☐ X: ☐ Y: ☐ Z: ☐ A:

底部有 **保存** 按钮。

iii. 单击保存，完成配置。

5. 前往[运维 > 主机运维](#)页面，定位到要登录的主机，选择要登录的主机账户，并单击登录图标。



主机运维页面显示主机列表，包含以下列：主机、操作系统、主机网络、主机组、主机账户、登录。

主机	操作系统	主机网络	主机组	主机账户	登录
[模糊]	CentOS	[模糊]		[SSH] root	[登录图标]
[模糊]	Windows Server 2012	[模糊]		[RDP] CBQ\administrator	[登录图标]

红色框标注了主机账户和登录图标。

堡垒机将调用本地客户端直接登录目标主机；登录成功后，即可进行运维。

CS运维

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。该运维方式支持所有账号类型使用，且支持Windows和Mac操作系统。

关于不同协议的具体登录方式，请参见以下文档：

- [SSH协议运维](#)
- [RDP协议运维](#)
- [SFTP协议运维](#)
- [Mac系统运维](#)