ALIBABA CLOUD

阿里云

堡垒机

用户指南（V3.2版本）

文档版本：20220608

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.管理员手册

1.1. 授权堡垒机访问云资源

首次使用堡垒机服务前，您需要先完成允许堡垒机访问云资源的授权。本文介绍如何进行云资源授权。

前提条件

- 您已购买堡垒机实例。更多信息，请参见购买堡垒机实例。
- 您使用的是阿里云账号或拥有创建和删除服务关联角色权限的RAM用户。

背景信息

首次使用堡垒机服务时，阿里云会自动创建堡垒机服务关联角色AliyunServiceRoleForBastionhost，授权堡垒机访问其他关联的云服务。服务关联角色无需您手动创建或做任何修改。相关内容，请参见服务关联角色。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在**欢迎使用堡垒机**对话框中，单击**确认创建**。

   您购买堡垒机实例后，首次登录堡垒机控制台时，堡垒机页面会提示您创建服务关联角色的流程。

   当您单击**确认创建**后，阿里云将自动为您创建堡垒机服务关联角色AliyunServiceRoleForBastionhost。您可以在RAM控制台的**RAM角色管理**页面查看阿里云为堡垒机自动创建的服务关联角色。只有创建服务关联角色AliyunServiceRoleForBastionhost后，您的堡垒机实例才能访问云服务器ECS、专有网络VPC等云服务的资源，对服务器进行运维审计等操作。

堡垒机服务关联角色介绍

通过堡垒机进行运维时，堡垒机需要访问云服务器ECS和专有网络VPC等云服务的资源，您可通过系统自动创建的堡垒机服务关联角色AliyunServiceRoleForBastionhost获取访问权限。

以下是堡垒机服务关联角色的介绍：

- 角色名称：AliyunServiceRoleForBastionhost
- 权限策略名称：AliyunServiceRolePolicyForBastionhost

  > **说明** 该权限策略为系统默认提供的策略，其策略名称和策略内容都不支持修改。

- 权限策略示例：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeImages",
                "ecs:DescribeZones",
                "ecs:DescribeRegions",
                "ecs:DescribeTags",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:AuthorizeSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupReferences",
                "ecs:CreateSecurityGroup",
                "ecs:RevokeSecurityGroup",
                "ecs:DeleteSecurityGroup",
                "ecs:ModifySecurityGroupAttribute",
                "ecs:ModifySecurityGroupPolicy",
                "ecs:ModifySecurityGroupRule",
                "ecs:CreateNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DescribeNetworkInterfacePermissions",
                "ecs:DeleteNetworkInterfacePermission",
                "ecs:DetachNetworkInterface",
                "ecs:AttachNetworkInterface"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcAttribute",
                "vpc:DescribeVSwitchAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "bastionhost.aliyuncs.com"
                }
            }
        }
    ]
}
```

删除服务关联角色

如果不再需要使用堡垒机服务，您可以删除堡垒机服务关联角色AliyunServiceRoleForBastionhost。在删除服务关联角色前您需要先释放已有的堡垒机实例。在释放已有的堡垒机实例后，您可以参考以下步骤在RAM控制台删除堡垒机服务关联角色。

1. 登录RAM控制台。
2. 在左侧导航栏中单击**RAM角色管理**。
3. 使用搜索功能定位到堡垒机服务关联角色AliyunServiceRoleForBastionhost，单击其操作列**删除**。
4. 在确认删除对话框中，单击**确定**。

相关问题

为什么我的RAM用户无法自动创建堡垒机服务关联角色AliyunServiceRoleForBastionhost？

您需要拥有指定的权限，才能自动创建或删除AliyunServiceRoleForBastionhost。因此，在RAM用户无法自动创建AliyunServiceRoleForBastionhost时，您需为RAM用户添加以下权限策略。详细操作步骤指导，请参见为RAM角色授权。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:主账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "bastionhost.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

1.2. 登录堡垒机系统

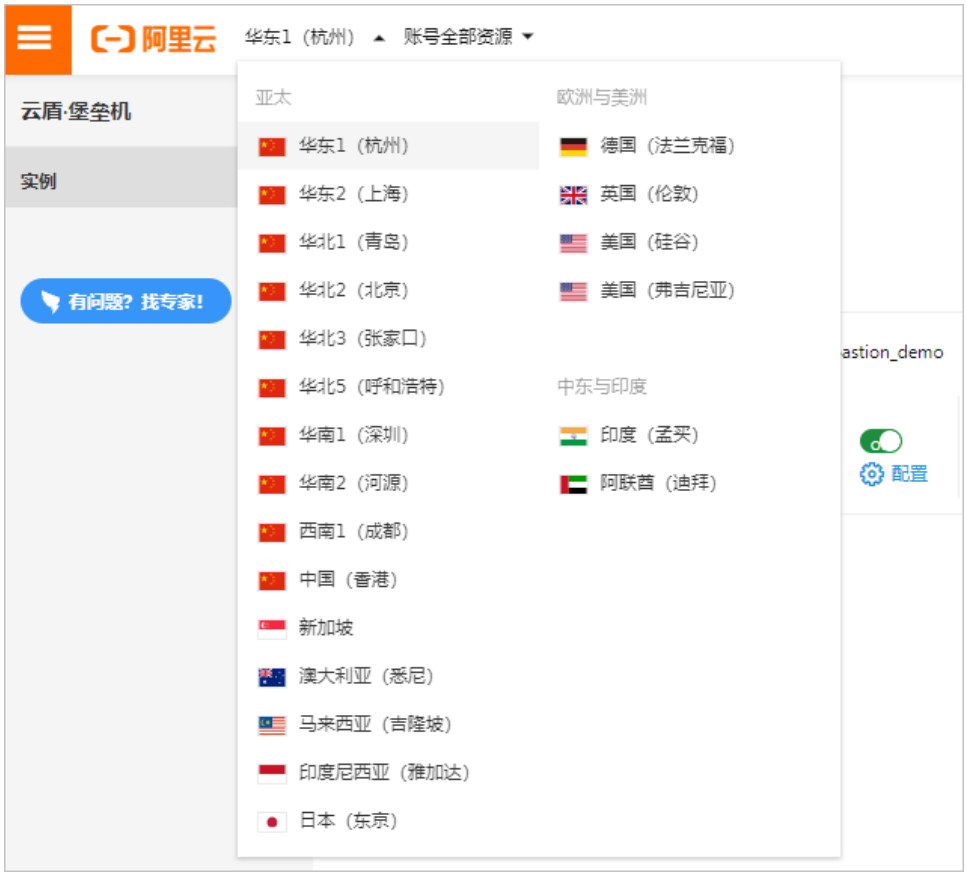
本文介绍了如何通过Web方式登录堡垒机系统。

背景信息

支持阿里云主账号和RAM账号登录堡垒机Web界面。

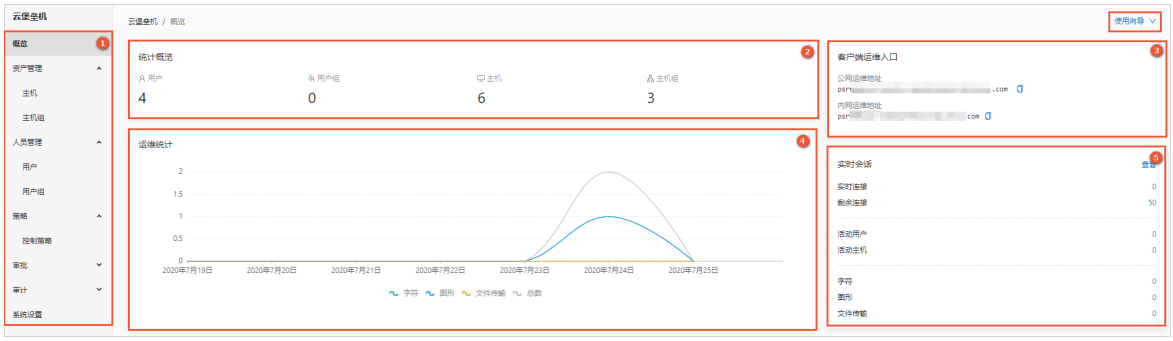
操作步骤

1. 登录云盾堡垒机控制台。
2. 在顶部菜单栏，选择堡垒机所在的地域。



3. 定位到需要访问的堡垒机实例，单击**管理**。

4. 在**云堡垒机**页面，查看堡垒机提供的**统计概览**、**运维入口**、**运维统计**和**实时会话**信息。



以下表格介绍了**云堡垒机**页面的各个区域。

区域	说明
①	堡垒机系统的功能菜单项。
②	用户、用户组、主机、主机组等信息的统计数据。
③	客户端运维的公网和内网入口。

区域	说明
④	运维统计信息。
⑤	最近运维的概况信息。

您可以单击右上角的**使用向导**，参考向导中提供的功能使用堡垒机进行运维。例如，您可以单击**导入ECS实例**跳转到**主机**页面，一键导入ECS实例。

1.3. 实例管理

1.3.1. 配置堡垒机

启用堡垒机实例后，如果您需要自定义或修改堡垒机实例的安全组、白名单、端口号，您可以在堡垒机列表中进行配置。本文介绍如何配置堡垒机实例。

配置安全组

通过配置安全组，可允许堡垒机访问该安全组内的服务器。

1. 登录云盾堡垒机控制台。
2. 在堡垒机实例列表中，单击**配置**。
3. 在**配置**的下拉列表中，单击**安全组**。

4. 在**网络设置**面板上，选择ECS对应的安全组。

> **说明** 支持选择多个安全组。

5. 配置完成后，单击**确定**。
   选择安全组后，堡垒机可以访问安全组内的ECS。

配置白名单

默认所有公网IP均可以登录堡垒机进行运维，如需限制可访问堡垒机的公网IP，可在白名单中配置可访问IP地址。

1. 登录云盾堡垒机控制台。
2. 在堡垒机实例列表中，单击**配置**。
3. 在**配置**的下拉列表中，单击**白名单**。

4. 在**网络设置**面板上，配置**公网白名单**。

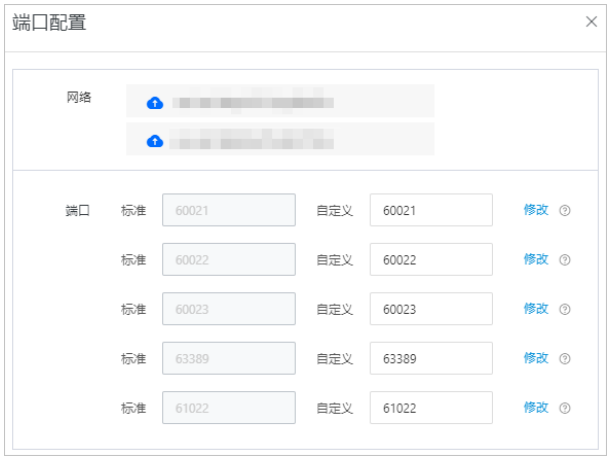
5. 配置完成后，单击**确定**。
   访问堡垒机的公网白名单配置成功。

配置端口号

如果您需要修改堡垒机的运维端口，您可以使用配置端口号功能进行修改。

1. 登录云盾堡垒机控制台。
2. 在堡垒机实例列表中，单击**配置**。
3. 在**配置**的下拉列表中，单击**端口号**。

4. 在**端口配置**面板上，配置**端口**。



> **说明** 1~1024端口为堡垒机的保留端口，建议您在配置端口号时，不要设置为此范围内的端口号。

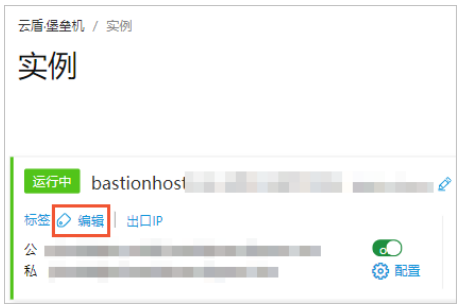
5. 配置完成后，单击**确定**。
   访问堡垒机的运维端口配置成功。

1.3.2. 管理堡垒机实例标签

堡垒机提供标签管理功能，方便您标记堡垒机实例资源，实现分类批量管理。本文介绍如何添加、删除标签和按标签搜索实例。

添加、删除标签

1. 登录云盾堡垒机控制台。
2. 在**实例**页面，鼠标移动到需要添加标签的实例**标签**处，并单击**编辑**。



3. 在**标签**面板上为实例添加或删除标签。
   - **添加标签**

     您可以为当前实例选择已有的标签，也可以为实例新建标签。

> **说明** 标签包含标签键和标签值（一对多的关系，即一个标签键可以包含多个标签值）。

- **选择已有的标签**

  在添加标签区域，分别选择标签键和标签值。

- **新建标签**

  在**新建标签**区域，输入新建标签的**键**和**值**，单击右侧**确认**。

- **删除标签**

  如果当前堡垒机不再需要使用某个标签，您可以单击该标签后的 图标，为当前堡垒机删除该标签。

设置完成后，在**标签**区域可以查看当前堡垒机的标签。

4. 单击**确定**。

按标签搜索实例

在**实例**页面，您可以在右上角的标签列表中选择需要查看的标签键和值，查看对应实例。

1.4. 资产管理

1.4.1. 主机管理

1.4.1.1. 新建主机

您可以通过进行导入阿里云ECS实例和导入其他来源主机方式，在堡垒机中新建需要维护的主机。导入或新建主机后，运维人员才可以通过堡垒机运维管理该主机。

导入阿里云ECS实例

您可以通过导入阿里云ECS实例方式批量导入当前阿里云账号中的ECS实例到堡垒机。使用该功能前，请确保您已经创建了ECS实例，具体操作，请参见连接方式概述。

> **说明** 该操作不会影响已导入的ECS实例的现有状态。

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

新建主机

您可以通过手动填写主机信息方式将需要运维管理的主机导入到堡垒机。

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**导入其他来源主机**列表，选择**新建主机**。
4. 输入主机的操作系统类型、主机IP、主机名等信息，然后单击**创建**。

导入云数据库专属集群

您可以通过导入云数据库专属集群方式批量将云数据库专属集群中的主机导入到堡垒机。

> **说明**
> - RDS专有主机组产品名称变更为云数据库专属集群MyBase。
> - 通过堡垒机访问云数据库专属集群主机的更多信息，请参见通过堡垒机访问主机（Linux）。

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**导入其他来源主机**列表，选择**导入云数据库专属集群**。
4. 在**导入云数据库专属集群**对话框，选中需要导入的主机，单击**导入**。

从文件导入主机

主机模板文件提供了*.xls*、*.csv*和*.xlsx*格式的模板，您可以选择其中一种格式的模板导入主机信息。您可以通过从文件导入主机方式批量将需要运维管理的主机导入到堡垒机。

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**导入其他来源主机**列表，选择**从文件导入主机**。
4. 在**导入主机**面板，单击**下载主机模板文件**，下载主机模板文件，按照模板格式要求填写主机信息并保存。
5. 在**导入主机**面板，单击**点击上传**，选择填写好主机信息的模板文件。
6. 在**主机导入预览**对话框，选择需要导入的主机，单击**导入**。
7. 在**导入主机**面板，确认主机信息，然后单击**导入主机**。

导入第三方资产源

您可以通过第三方资产源API和访问凭证导入其他云平台的主机。使用该功能前，请确保您已经创建了第三方资产源，具体操作，请参见管理第三方资产源。

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. 导入其他来源主机列表，选择需要导入的第三方资产源名称。
4. 在**导入第三方资产源**对话框，选择需要导入的主机，单击**导入**。

相关操作

- 在堡垒机中新建主机后，您还需要为主机创建对应的账户。具体操作，请参见新建主机账户。
- 如果目标主机中的运维协议（RDP、SSH）使用的不是默认端口，您需要修改服务端口。具体操作，请参见修改主机的服务端口。

1.4.1.2. 管理主机

本文介绍如何在主机列表中搜索目标主机、修改主机的基本信息和删除主机。

前提条件

已在堡垒机实例中新建了需要维护的主机。更多信息，请参见新建主机。

限制条件

仅支持修改手动新建或通过文件导入的主机的基本信息，不支持修改导入的ECS实例和RDS专有主机组的基本信息。

搜索主机

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，设置搜索条件搜索目标主机。

您可以通过以下搜索条件进行搜索：

- **搜索主机名或主机IP**：输入主机名或主机IP后，单击 图标，查看指定主机。主机名和主机IP支持模糊搜索。
- **选择操作系统类型**：选择操作系统类型，您可以选择**操作系统：全部**、Linux或Windows。
- **选择主机来源**：选择主机来源，您可以选择**主机来源：全部**、Local、ECS或RDS。
- **选择主机状态**：选择主机状态，您可以选择**主机状态：全部**、**正常**或**已释放**。堡垒机可以检测ECS主机和RDS专有主机组是否已被释放。如果ECS主机或RDS专有主机组已被释放，堡垒机会将该主机的**主机状态**置为**已释放**，否则将**主机状态**置为**正常**。您可以在搜索条件中选择**已释放**，筛选出所有被释放的主机，以便于您删除已被释放的主机。

> **说明** 如果您同时设置了多个搜索条件，堡垒机将展示同时满足您设置的所有搜索条件的主机。

修改主机基本信息

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，定位到需要修改的主机，单击其名称。

4. 修改主机的**操作系统**、**主机IP**、**主机名**、**网络域**、**备注**和**主机组**。

> **说明** 暂不支持修改ECS主机的主机IP和主机名。

5. 单击**更新**。
   完成主机信息修改后，修改内容会立即更新。

删除主机

如果您不再需要维护某个主机，可以在堡垒机的主机列表中删除该主机。

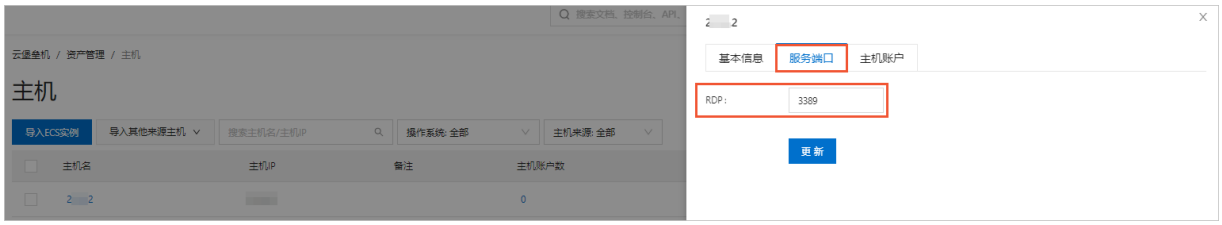
1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**资产管理 > 主机**。
3. 在**主机**页面删除主机。
   - **删除一个主机**：定位到要删除的主机，单击**操作**列的**删除**，也可单击主机列表下方的**删除**。
   - **删除多个主机**：选中要删除的多个主机，单击主机列表下方的**删除**。
4. 在**是否删除已选中主机**对话框中，单击**删除**。
   删除该主机后，该主机相关的所有授权会被同时删除。例如某用户已授权该主机，删除主机后，该授权关系会被同时删除。您将无法使用堡垒机登录该主机。

1.4.1.3. 修改主机的服务端口

目前堡垒机对于服务器的RDP和SSH协议使用的是默认端口（RDP协议默认使用3389端口，SSH协议默认使用22端口），如果您在主机中自定义了端口，需要在服务端口中做相应修改。 本文档介绍如何修改主机的服务端口。

前提条件

在您修改服务端口前，需要确认堡垒机修改的服务端口号和您主机中相应协议的端口一致，否则通过堡垒机运维时将无法登录主机。您可以在堡垒机控制台该主机的**服务端口**页面，查看当前堡垒机为该主机配置的协议和服务端口。



修改单个主机的服务端口

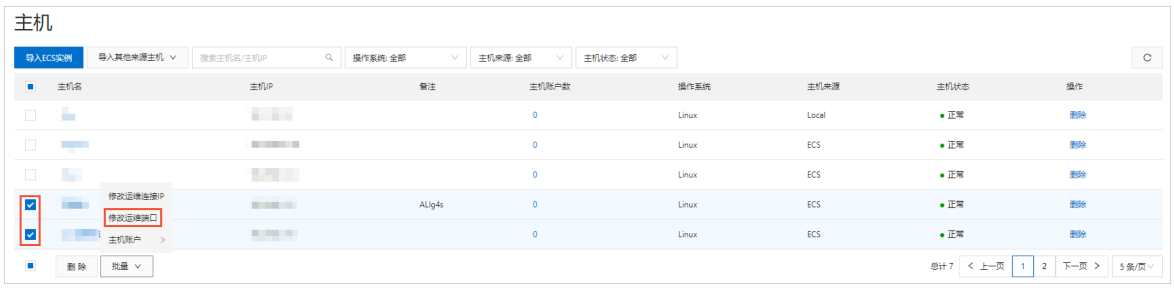
1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，选择**资产管理 > 主机**。
3. 在**主机**页面，定位到需要修改服务端口的主机并单击主机名称。
4. 在主机详情页面单击**服务端口**页签。
5. 根据主机实际情况，自定义**RDP**或**SSH**的端口号。

6. 单击**更新**。

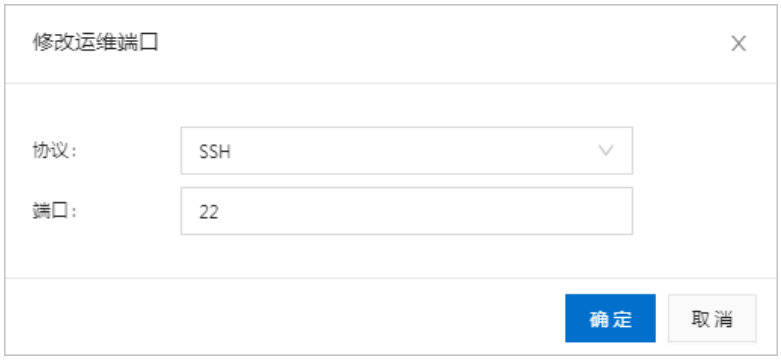
批量修改主机的服务端口

如果多个主机的同一协议使用的是相同的端口号，您可以通过以下步骤批量修改主机的服务端口：

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，选中需要批量修改服务端口的主机并在**批量**列表中单击**修改运维端口**。



4. 在**修改运维端口**对话框中，设置**协议**和**端口**。



5. 单击**确定**。

1.4.1.4. 新建主机账户

在新建主机后还需要为主机新建主机账户，即将主机的账户配置到堡垒机中，以便运维人员使用堡垒机登录主机进行运维。本文介绍如何在堡垒机中新建主机账户。

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**。

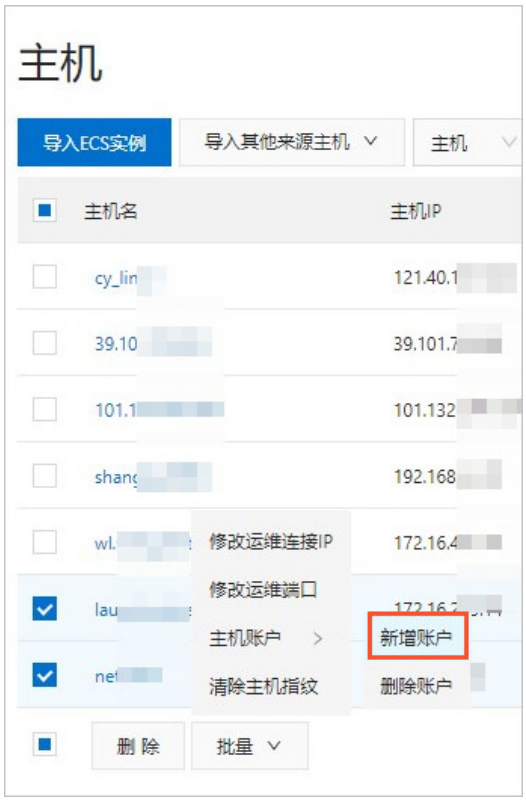
使用**验证密码**可以测试主机账户的用户名和密码是否正确。

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**。

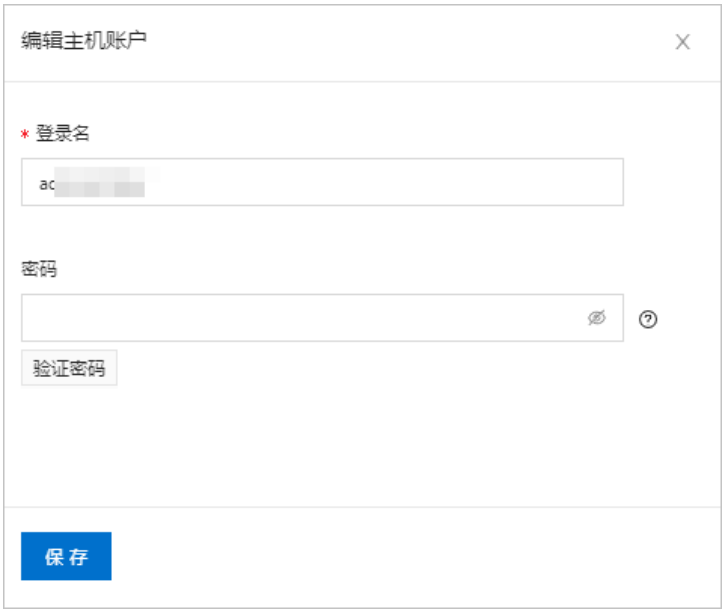
1.4.1.5. 配置主机账户

在堡垒机控制条完成主机账户的添加后，您可能需要进行修改主机账户、删除主机账户、设置账户的密码和私钥等操作。本文介绍如何在主机中配置对应的主机账户。

修改主机账户信息

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，定位到需要修改账户信息的主机并单击主机名称。
4. 单击**主机账户**页签。

5. 定位到需要修改的账户并单击其登录名。
6. 在**编辑主机账户**面板上，修改账户的**登录名**和**密码**。



7. 单击下方**验证密码**。

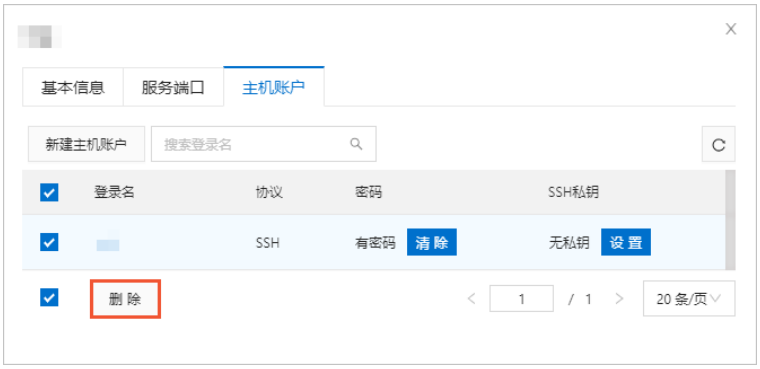
   使用**验证密码**可以测试账户的用户名和密码是否正确。
8. 单击**保存**。

删除主机账户

如果不需要使用某个主机账户，您可以参考以下步骤删除该账户：

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，定位到需要删除账户的主机并单击主机名称。
4. 单击**主机账户**页签。

5. 选中需要删除的账户，单击列表下方的**删除**。



6. 在确认提示处单击**删除**。

设置账户的密码

您可以在**主机账户**页签中新增、修改和删除账户的密码。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，定位到需要设置账户密码的主机并单击主机名称。
4. 单击**主机账户**页签。

5. 在**主机账户**页签下，您可以进行添加、修改或清除密码操作。

   以下是进行密码相关操作的说明：

   - **添加或修改密码**

单击登录名，在**编辑主机账户**面板上输入密码。

- **清除密码**

  定位到需要清除密码的登录名，单击**密码**列的**清除**。

设置账户的私钥

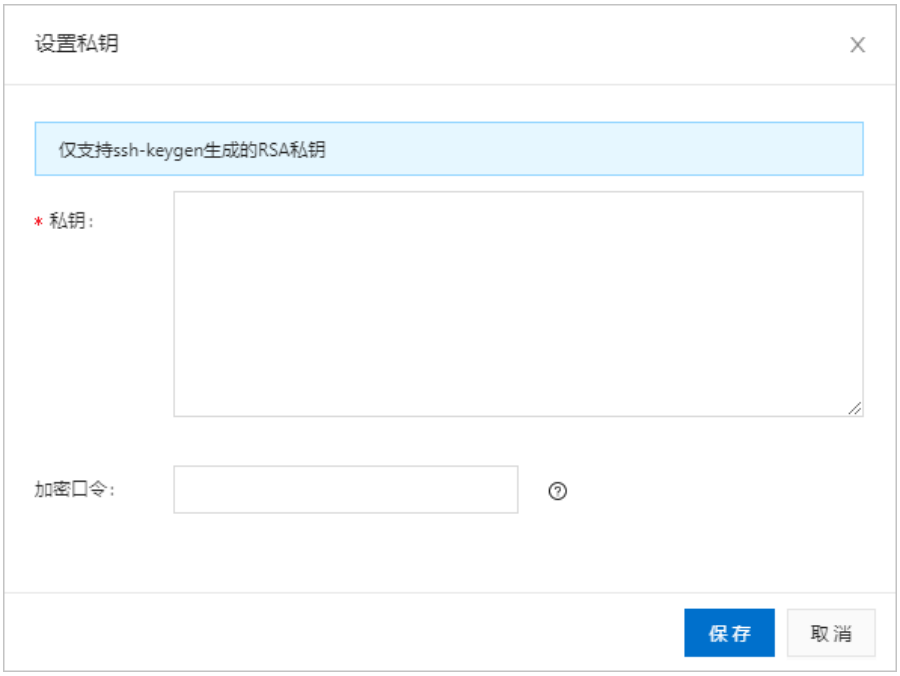
如果您运维的主机通过SSH密钥方式登录，则可以在主机账户中添加私钥。具体参见以下步骤：

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，定位到需要设置账户私钥的主机并单击主机名称。
4. 单击**主机账户**页签。

5. 定位到需要设置私钥的登录名，单击**SSH私钥**列的**设置**。

6. 在**设置私钥**对话框中，填入对应的私钥信息。

> **说明**
>
> - 堡垒机仅支持使用ssh-keygen命令生成的RSA私钥。
>
>   例如，您在Linux主机中使用ssh-keygen命令生成公钥和私钥，其中公钥存储在主机对应目录中，私钥导出到本地并在本步骤中输入私钥信息。
> - 如果主机设置密钥是免密登录，则**加密口令**可以为空。



7. 单击**保存**。
8. （可选）创建完成后，如果需要清除私钥，您可以在**SSH私钥**列单击**清除**。

1.4.1.6. 修改主机的运维连接IP

堡垒机支持设置运维连接IP为公网IP或内网IP。根据您的设置，堡垒机使用公网IP或内网IP连接主机。本文档介绍如何修改主机的运维连接IP。

背景信息

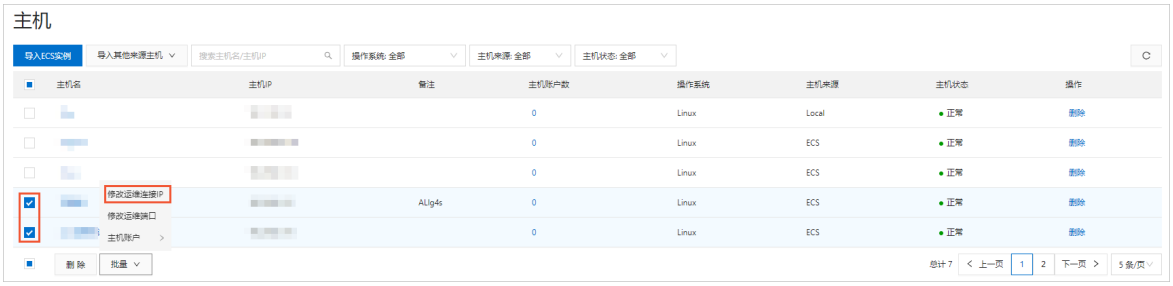
运维连接IP可设置为**内网IP**或**公网IP**。 以下是这两种连接方式的说明：

- 运维连接IP设置为**公网IP**，表示堡垒机通过公网IP连接到主机。
- 运维连接IP设置为**内网IP**，表示堡垒机通过内网IP连接到主机。

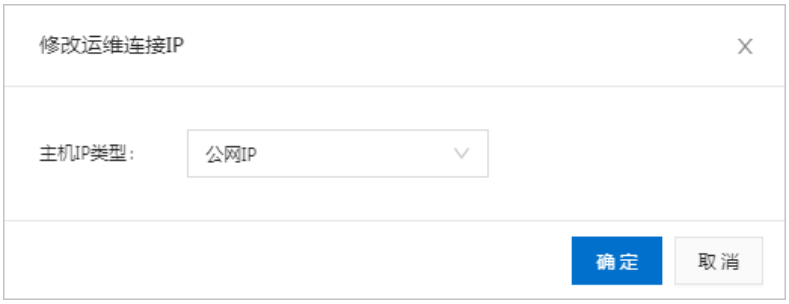
> **说明** 如果主机同时存在内网IP和公网IP，堡垒机默认使用内网IP连接主机。

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，选中需要修改运维连接IP的主机并单击**批量 > 修改运维连接IP**。



4. 在**修改运维连接IP**对话框中，选择**主机IP类型**。



- 选择**公网IP**，表示堡垒机通过公网IP连接到主机。
- 选择**内网IP**，表示堡垒机通过内网IP连接到主机。

5. 单击**确定**。

1.4.1.7. 清除主机指纹

主机指纹是堡垒机对使用SSH协议的Linux主机的唯一标识。堡垒机通过主机指纹对主机的访问权限进行安全检查，避免恶意用户通过重定向流量的方式获取未授权主机的访问权限。原主机指纹不适用时，您需要清除主机指纹，否则将无法进行正常运维。本文介绍清除主机指纹的具体操作。

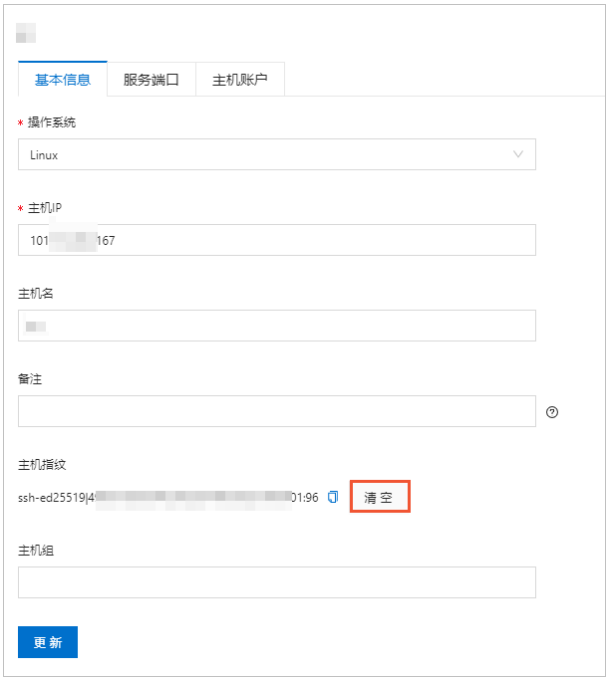
背景信息

堡垒机通过主机指纹可以唯一识别一台Linux主机。清空主机指纹不会对您的运维操作产生影响，再次运维该主机时，堡垒机会为该主机自动生成新的主机指纹。

清除单个主机指纹

如果需要清除单个主机的主机指纹，您可以参考以下步骤进行操作。

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏，选择**资产管理 > 主机**。
3. 定位到需要清除主机指纹的主机，单击其主机名。
4. 在该主机的**基本信息**页签下，单击主机指纹右侧的**清空**。



操作完成后，控制台会出现**主机指纹重置成功**的提示信息，并且主机指纹处会显示**暂无主机指纹**。

批量清除主机指纹

如果需要清除多台主机的主机指纹，您可以参考以下步骤进行操作。

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，选择需要清空主机指纹的主机，并选择**批量 > 清除主机指纹**。

4. 在**确认**对话框，单击**确定**。
   操作完成后，控制台会出现**主机指纹重置成功**的提示信息。

1.4.1.8. 一键导出主机列表

堡垒机提供一键导出主机详情列表功能，可供用户通过CSV本地文档格式对主机列表进行查看。本文介绍导出主机列表的具体操作。

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，单击主机列表右上角的**导出主机**。
   主机列表文件会以CSV格式下载到本地。

1.4.2. 管理资产组

您可以按照业务需要创建不同的资产组，然后将同一类型的主机添加到资产组，实现对主机的分类管理和批量操作。

添加资产组

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 > 资产组**。
3. 在**资产组**页面，单击**添加资产组**。
4. 在**新建资产组**面板，输入资产组名称和备注信息，单击**创建**。

   资产名称长度为1~128个字符，可以包含中英文字符、数字、半角句号（.）、下划线（_）、短划线（-）、反斜线（\）和空格，并且名称不能以特殊字符开头。

   > **说明** 建议您根据主机提供的服务、主机所属部门或主机所属地域等信息设置有意义的资产组名称，方便后续维护和识别。

添加主机成员

创建资产组后，您可以在资产组中添加主机成员，便于批量管理同一资产组的主机。添加主机成员前，请确保您已经在堡垒机中导入或新建主机，具体操作，请参见新建主机。

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 > 资产组**。
3. 在资产组列表，单击目标资产组名称。
4. 在**主机成员**页签，单击**添加主机成员**。
5. 在**添加主机成员**对话框的主机列表中，选中需要添加到资产组的主机，单击**添加**。

> **说明** 如果需要添加单个主机，您可以在主机的**操作**列单击**添加**。

相关操作

- 移除主机成员

  在**资产组**页面，单击目标资产组名称，在**主机成员**页签，选中需要移除的主机成员，然后单击**移除**，然后在弹出的对话框中再次单击**移除**。

- 修改资产组信息

  在**资产组**页面，单击目标资产组名称，在**资产组设置**页签，修改资产组名称和备注信息，然后单击**更新**。

- 删除资产组

  在**资产组**页面，找到目标资产组，在**操作**列单击**删除**，然后在弹出的对话框中再次单击**删除**。

1.4.3. 改密任务

堡垒机提供自动改密服务，可根据已配置的密码策略生成随机密码，自动轮转托管的主机账号密码。本文将介绍如何创建改密任务，如何执行改密任务以及其他相关操作。

背景信息

根据等级保护制度规定，服务器的密码需要定期更换。长期使用固定的主机账号密码存在安全隐患，定期人工维护主机账号密码的轮转是一项繁重且容易出错的工作。堡垒机提供自动改密服务。

限制条件

- 仅堡垒机高可用版实例支持使用改密任务功能。
- 仅支持为Linux主机账户修改密码，不支持为Windows主机账户修改密码。
- 改密任务仅支持SSH协议的主机账号，且主机账号必须是密码类型。

支持的操作系统

操作系统名称	版本
Alibaba Cloud Linux	• 3.2104 64位 • 2.1903 LTS 64位 • 2.1903 64位快速启动版
CentOS	支持所有版本
Ubuntu	支持所有版本
Debian	支持所有版本

操作系统名称	版本
Open SUSE	• 15.1 64位 • 15.2 64位 • 42.3 64位 说明 改密任务不支持修改root账号密码，仅支持修改普通账号密码。
SUSE Linux	• SUSE Linux Enterprise Server 15 SP2 64位 • SUSE Linux Enterprise Server 12 SP5 64位 • SUSE Linux Enterprise Server 11 SP4 64位
CoreOS	• 2303.4.0 64位 • 2247.6.0 64位 • 2023.4.0 64位 • 1745.7.0 64位

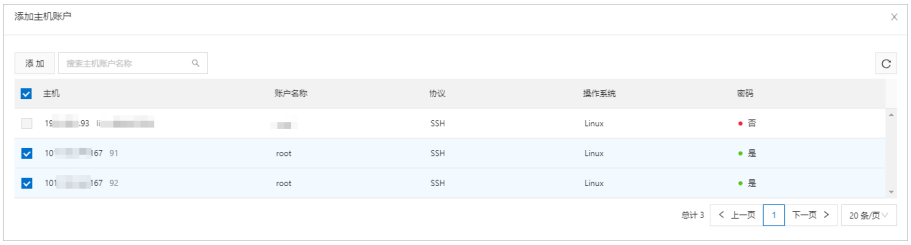
创建改密任务

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 > 改密任务**。
3. 在**改密任务**页面，单击**创建改密任务**。
4. 在**改密任务**面板，参考以下表格配置改密任务的参数。

参数	说明
任务名称	输入改密任务的名称。
执行方式	选择改密任务的执行方式。可选以下方式： ○ **周期执行**：需要设置执行时间和周期，执行时间至少应为当前时间5分钟后，周期最长支持设置365天。堡垒机会根据设置的执行时间和周期多次执行改密任务。 ○ **定时执行**：需要设置任务的执行时间（执行时间至少应为当前时间5分钟后）。到达设置的时间后，堡垒机会自动开始执行改密任务。
密码规则	设置修改后的密码的复杂度和密码长度。以下是相关说明： ○ **密码复杂度**：支持选择数字、小写字母、大写字母和其他字符。堡垒机会根据您选择的字符类型随机生成新密码。建议至少选择两种字符。 ○ **密码长度**：设置最小的密码长度。例如最小的密码长度设置为8时，会随机生成长度为8~32位的密码。
备注	输入改密任务的补充说明信息。

5. 单击**创建**。
   创建成功后控制台将显示创建改密任务成功的信息。
6. 单击**关联账户**。
7. 在**托管账户**页签下，单击**添加主机账户**。

8. 在**添加主机账户**对话框中，选择需要添加的主机账户并单击**添加**。



为改密任务添加主机账户有以下限制条件：

- 一个主机账户仅能添加到一个改密任务中。
- 主机账户使用协议为SSH且已设置密码。如果主机账户认证类型为SSH密钥或共享密钥，则无法添加到改密任务中。

操作成功后，您将收到**改密任务与主机账号关联成功**的提示信息。您可以在**改密任务**页面查看已创建的改密任务。

立即执行改密任务

创建改密任务后，改密任务会根据您设置的时间或周期自动执行。如果需要立即执行改密任务，您可以在**改密任务**页面选中需要执行的改密任务，单击**立即执行**。

> **说明**
>
> - 同时立即执行多个改密任务时，会依次执行。
> - 如果周期或定时执行任务的时间与立即执行的时间重合，则堡垒机仅执行一次改密任务。否则立即执行操作不会影响改密任务设置的执行时间和执行周期。立即执行改密任务后，到达改密任务设置的执行时间或执行周期时，改密任务仍会正常执行。

修改、启用、停止或删除改密任务

创建改密任务后，您可以在**改密任务**页面对已创建的改密任务进行修改、启用、停止、删除操作。

- **修改**

  堡垒机支持修改任务的基本信息和关联账户。在**改密任务**页面，单击需要修改的任务名称，在**任务详情**页签下修改该任务的基本信息，并单击**更新**。如果需要修改托管账户，您可以单击**托管账户**页签。在**托管账户**页签下，您可以添加主机账户或移除主机账户。

- **停止**

  如果在某段时间内无需使用某个或多个任务，您可以执行停止任务操作。在**改密任务**页面，选中需要停止的改密任务，单击**停止**。停止任务后，改密任务的状态将变更为**已取消**，该任务将不会再自动执行，您也无法立即执行该任务。

- **启用**

  如果需要再次启用某个或多个被停止的任务，您可以执行启用任务操作。在**改密任务**页面，选中需要启用的改密任务，单击**启用**。启用任务后，改密任务的状态将变更为**等待执行**，该任务将会按照您设置的执行时间和执行周期自动执行。

- **删除**

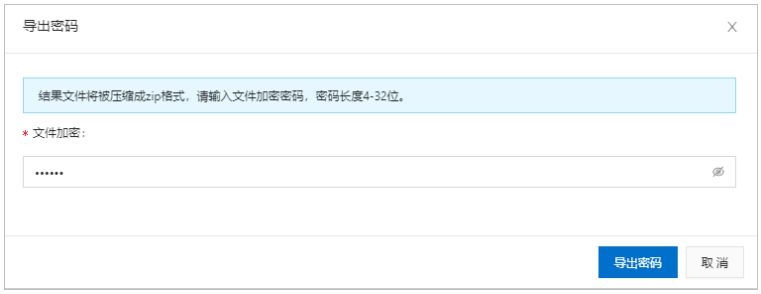
  如果确定无需再使用某个或多个任务，您可以执行删除任务操作。在**改密任务**页面，选中需要删除的改密任务，单击**删除**，并在提示信息框中再次单击**删除**。

  > **说明** 删除的改密任务无法再找回，建议您谨慎操作。

导出密码

改密任务执行成功后，您可以使用导出密码功能获取主机账户的当前密码。在**改密任务**页面，定位到需要导出密码的任务并单击其操作列**导出密码**，在**导出密码**对话框中输入4~32位的文件加密密码，并单击**导出密码**。主机账户的当前密码将被压缩为*.zip*文件并下载到您的本地电脑中。

> **说明** 您需要妥善保存在**导出密码**对话框中输入的文件加密密码，获取密码文件中的密码时需要输入该密码。



1.4.4. 密钥管理

堡垒机提供密钥管理功能。您可以创建密钥并将密钥批量关联到主机账户中，提高管理主机账户的效率。您也可以更改密钥的基本信息，增删关联主机账户，更好地满足运维需求。本文介绍如何创建和编辑密钥。

背景信息

如果您需要堡垒机帮您保存私钥，您可以在主机上部署好密钥对，然后使用堡垒机的密钥管理功能，创建共享密钥，以便关联到不同的主机账户。

创建密钥

您可以在堡垒机上创建密钥，并关联到主机账户。关联主机账户后，该密钥为已关联主机的共享密钥，运维主机时，将优先使用共享密钥登录。

步骤一：创建密钥

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 > 密钥管理**。
3. 在**密钥管理**页面，单击**创建密钥**。
4. 在**创建密钥**面板，输入**密钥名称**、**密钥**和**加密口令**。

   > **说明** **密钥**仅支持输入使用`ssh-keygen`命令生成的RSA密钥。

5. 单击**创建**。
   创建成功后，控制台密钥管理列表中将显示新创建的密钥。

步骤二：关联主机账户

> **说明**
> - 密钥管理功能仅支持关联SSH类型的主机账户。
> - 一个共享密钥可以关联多个主机账号，但一个主机账号只能绑定一个共享密钥。

1. 在**密钥管理**页面的密钥列表中，在新创建密钥的**操作**列，单击**关联主机账户**。
2. 在**关联主机账户**对话框中，选中需要关联的主机，然后单击左下角的或目标主机账户**操作**列的**关联**，并单

击**确认**。

编辑密钥

如果需要修改共享密钥的基础信息，或者需要增添或者解绑共享密钥关联的主机，您可以编辑密钥基本信息，或者增删密钥关联主机。

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 > 密钥管理**。
3. 在密钥列表中，找到需要修改的密钥，然后在目标密钥的**操作**列，单击**编辑**。在该密钥的详情面板，按需进行以下操作。
   - 在**基本信息**页签，修改**密钥名称**、**密钥**以及**加密口令**。修改完成后，单击**更新**。

     说明 密钥基本信息修改更新后，密钥列表中的**上次修改时间**会更新到最近一次修改密钥的时间。
   - 在**主机账户**页签，增删关联的主机。
     - 增加关联：单击**关联主机账户**，在**关联主机账户**对话框，选中需要关联的主机，然后单击左下角的或目标主机账户**操作**列的**关联**，并单击**确认**。
     - 解除关联：在待解除关联的主机账户的**操作**列，单击**解除关联**。

1.4.5. 网络域

如果您想统一运维分布在不同网络环境中或与堡垒机所在专有网络（VPC）网络不互通服务器，推荐使用堡垒机的网络域功能。您可以为这些服务器配置一台代理服务器，然后在堡垒机中创建网络域并成功连接到代理服务器，通过代理服务器运维其他服务器。本文介绍如何使用网络域功能。

背景信息

堡垒机的网络域功能为IDC、异构云、跨VPC等多混合云场景提供了最佳运维方案。通常情况下，企业的服务器资产分布在不同的区域且可能与堡垒机的网络不互通。在使用公网IP直接连接服务器所在网络会有安全风险，而使用专线连接服务器所在网络成本过高的场景下，可选用阿里云堡垒机高可用版提供的网络域代理方式，通过代理模式对线下IDC、异构云、跨VPC等不同网络环境下的服务器进行统一运维。

前提条件

已完成为处于同一网络环境下的服务器配置代理服务器。配置代理服务器，请参见如何将服务器配置为HTTP和SOCKS5代理服务器？。

限制条件

- 仅堡垒机的高可用版实例支持使用网络域代理方式。
- 网络域代理方式支持SSH代理、HTTP代理、SOCKS5代理。

新建网络域

要使用堡垒机运维网络域内的多台服务器，需要先在堡垒机中新建网络域并连接到代理服务器。具体操作步骤如下：

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，选择**资产管理 > 网络域**。
3. 在**网络域**页面，单击**新建网络域**。
4. 在**新建网络域**面板上，设置网络域的名称、备注信息，选择连接方式。

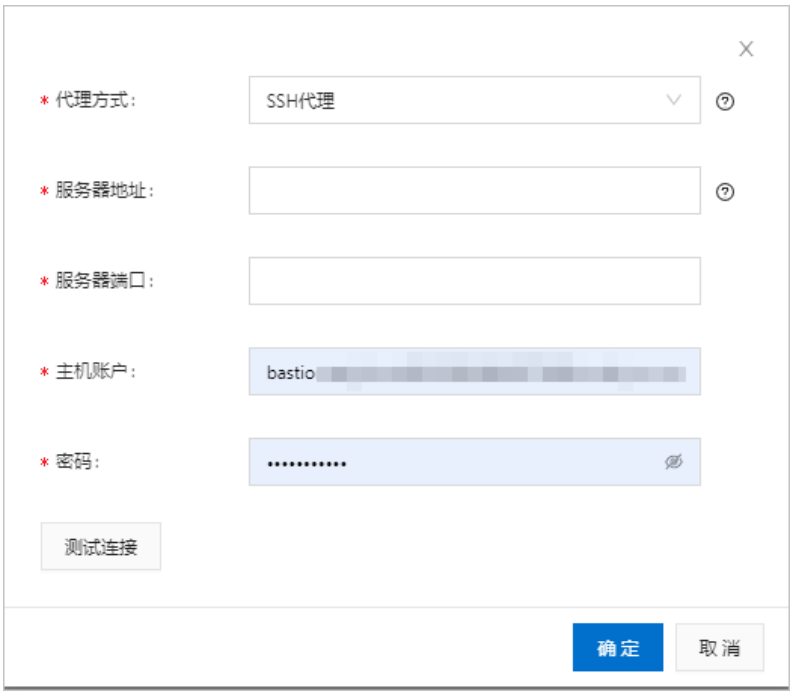
   连接方式支持**直连**和**代理**这两种方式。

> **说明** 堡垒机基础版和高可用版支持的连接方式不同。
>
> - 基础版仅支持直连。
> - 高可用版版支持直连、代理。

当您连接方式选择为**代理**时，您还需要配置代理服务器。备代理服务器配置的操作与主代理服务器相同，下文以配置主代理服务器为例，介绍配置代理服务器的具体操作：

i. 单击主代理服务器下方的**添加代理服务器**。

ii. 在弹出的对话框中配置主代理服务器。



配置项	描述
代理方式	选择代理方式。可选择的代理方式： ■ SSH代理 ■ HTTP代理 ■ SOCKS5代理
服务器地址	填写主代理服务器的地址。
服务器端口	填写主代理服务器的端口。
主机账户	填写主代理服务器的账户。
密码	填写主代理服务器账户的密码。

iii. （可选）按照配置主代理服务器的方式，配置备代理服务器。

> **说明** 网络域功能支持配置**主代理服务器**和**备代理服务器**两个代理服务器。当主代理服务器异常时，会自动切换使用备代理服务器。为了确保网络域使用更加稳定，建议您配置备代理服务器。

iv. 单击**测试连接**。

> **说明** 如果提示连接失败，请检查配置项信息是否填写正确。

v. 单击**确定**。

5. 单击**新建网络域**，进入新建网络域成功的页面。
   您可单击下方**关联主机**，将要运维的主机移入网络域。具体操作，请参见移入主机。

移入主机

新建网络域后，您可以将主机移入网络域。具体操作步骤如下：

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，选择**资产管理 > 网络域**。
3. 在**网络域**页面的网络域列表中，定位到要编辑的网络域。
4. 单击**移入主机**。
5. 在**移入主机**对话框的主机列表中，定位到您要移入的主机，单击右侧**移入主机**。
   您也可以在主机列表中，批量选中要移入网络域的主机，单击下方的**移入主机**，将主机批量移入网络域。

编辑网络域

您可以使用编辑功能修改网络域的基本信息、移入或删除主机。具体操作步骤如下：

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，选择**资产管理 > 网络域**。
3. 在**网络域**页面的网络域列表中，定位到要编辑的网络域。
4. 单击**编辑**。
5. 在网络域详情页面，编辑网络域的**基本信息**和**主机**。
   - **基本信息**：支持修改**网络域名称**、**连接方式**、**备注**、对主、备代理服务器进行**测试连接**和**编辑**。
   - **主机**：支持**移入主机**和**删除主机**。

后续步骤

通过网络域功能，成功连接堡垒机与网络域中的服务器后，您还需要完成授权主机，才可以使用堡垒机运维网络域中的服务器。

- 授权主机。具体操作，请参见按用户授权主机、按用户授权主机组。
- 运维服务器。具体操作，请参见主机运维。

网络域功能视频演示

1.5. 人员管理

1.5.1. 用户管理

1.5.1.1. 管理用户

管理员在堡垒机控制台上为运维员创建用户账号后，运维员可以使用账号登录堡垒机进行运维工作。本文介绍如何在堡垒机控制台新建用户、修改用户信息、锁定或解锁用户、托管用户公钥以及删除用户。

用户类型

堡垒机支持导入阿里云RAM用户、新建堡垒机本地用户、导入AD用户和导入LDAP认证用户。以下为您介绍堡垒机支持的用户类型及其使用场景。

用户类型	使用场景
RAM用户	为运维员创建阿里云RAM用户后，您可以通过导入RAM用户的方式一键导入RAM用户，作为登录堡垒机的账号。
堡垒机本地用户	您可以通过单个创建或批量从文件导入的方式，为运维员创建登录堡垒机的本地账号。
AD用户	您可以在堡垒机上配置AD认证，把AD用户同步到堡垒机后，将AD用户导入堡垒机作为运维员登录堡垒机的账号。 导入AD用户前，请确保您已经完成了AD认证。具体操作，请参见配置AD认证。
LDAP用户	您可通过在堡垒机上配置LDAP认证，把LDAP用户同步到堡垒机后，将LDAP用户导入堡垒机作为运维员登录堡垒机的账号。 导入LDAP用户前，请确保您已经完成了LDAP认证。具体操作，请参见配置LDAP认证。

新建用户

您可以根据业务场景，通过导入阿里云RAM用户、新建堡垒机本地用户、导入AD用户、导入LDAP认证用户方式，为运维员创建用于登录堡垒机的用户账号。

导入RAM用户

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. 如果您还未创建RAM用户，您可以在**导入RAM用户**页面，单击**新建RAM用户**，根据页面提示新建RAM用户。

   新建RAM用户的具体操作，请参见创建RAM用户。
5. 在**导入RAM用户**页面，在目标RAM用户的**操作**列单击**导入**，导入单个RAM用户；或者同时选中多个RAM用户后单击**导入**，批量导入多个RAM用户。

新建本地用户

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. 参考下表信息，单个新增本地用户或批量从文件导入本地用户。

适用场景	操作说明
单个新增本地用户	i. 选择**导入其他来源用户 > 新增本地用户**。 ii. 在**新增用户**面板，配置用户信息，单击**创建**。 配置用户信息时，除填写**姓名**、**密码**、**用户组**、**备注**等基础信息外，您还可以进行以下操作。 ■ 开启**本地用户在下次登录时必须重置密码**：勾选后，强制本地用户下一次登录时修改密码。该功能仅针对本地用户可用。 ■ 设置**有效期**：设置有效期限后，在用户列表的**状态**列，未在有效期内的用户状态会显示为**已过期**，且用户无法登录堡垒机进行运维操作。 ■ 配置**双因子认证方式**：开启后，用户登录堡垒机时，通过密码认证之后，还需要通过短信、邮件或钉钉工作消息通知发送动态验证码进行二次认证，降低安全风险。 **说明** ■ 开启双因子认证后，用户在登录时，必须使用手机号码或邮箱接收验证码进行验证，请确保填写的手机号码或邮箱地址无误。堡垒机短信双因子认证支持的国家和地区，请参见堡垒机短信双因子认证支持的国家和地区。 ■ 您填写的手机号和邮箱仅用于接收验证码或告警信息，不用于其他用途。 **双因子认证方式**包括以下两种类型： ■ 选择**全局配置**，表示当前用户采用全局的双因子认证方式，即您在**系统设置**中配置的双因子认证方式。具体操作，请参见开启双因子认证。 ■ 选择**单个用户配置**，表示您需要对当前用户单独设置双因子认证方式。堡垒机支持设置以下双因子认证方式： ■ **不开启双因子认证**：表示不开启双因子认证功能。 ■ **手机短信双因子认证**：表示使用当前用户的手机短信进行二次认证。此时您必须为该用户设置手机号码。 ■ **邮箱双因子认证**：表示使用当前用户的邮箱进行二次认证。此时您必须为该用户设置邮箱地址。 ■ **钉钉双因子认证**：表示使用当前用户的钉钉进行二次认证。此时您必须为该用户设置手机号码。 **说明** 如果您需要启用钉钉认证，请确保已符合以下要求： ■ 已为需要进行运维操作的用户账号添加手机号。为用户添加手机号的具体操作，请参见修改用户信息。 ■ 钉钉管理员已创建企业内部应用，并且为应用开通**根据手机号姓名获取成员信息的接口访问权限**。 ■ 已获取企业内部应用的AppKey、AppSecret、AgentId。

适用场景	操作说明
批量从文件导入本地用户	i. 选择**导入其他来源用户**列表中，选择**从文件导入本地用户**。 ii. 单击**下载用户模板文件**，下载用户模板文件到本地，在用户模板文件录入用户信息并保存。 iii. 在**导入本地用户**面板，单击**点击上传**，上传用户模板文件。 iv. 在**导入用户预览**对话框，选择需要导入的用户，单击**导入**。 v. 在**导入本地用户**面板，确认用户信息。 选中**本地用户在下次登录时必须重置密码**，表示导入的所有用户在下一次登录时都要重置密码。 vi. 单击**导入本地用户**。 **说明** 如果导入用户中存在与文件中用户或系统中已有用户的用户名重复的情况，用户名重复的用户将不会被导入。您可以在**导入本地用户**面板上单击**详情**，查看未被导入的用户。

导入AD认证用户

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. 选择**导入其他来源用户 > 导入AD用户**。
4. 在**导入AD用户**页面，在目标AD用户的**操作**列单击**导入**，导入单个AD用户；或者同时选中多个AD用户后单击**导入**，批量导入多个AD用户。

导入LDAP用户

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. 选择**导入其他来源用户 > 导入LDAP用户**。
4. 在**导入LDAP用户**页面，在目标LDAP用户的**操作**列单击**导入**，导入单个LDAP用户；或者同时选中多个LDAP用户后单击**导入**，批量导入多个LDAP用户。

修改用户信息

当用户手机号、邮箱等信息变更时，您需要及时到控制台修改，否则用户可能无法及时接收验证信息，继而导致用户无法登录控制台。例如，如果用户更换手机号码后没有在堡垒机上及时维护新手机号码，登录堡垒机时，验证码会发送到旧手机号，导致用户无法收到验证码，无法登录堡垒机进行运维。

说明 仅支持修改本地用户、AD认证用户、LDAP认证用户的信息，不支持修改RAM用户的信息。修改RAM用户的信息，具体操作，请参见修改RAM用户基本信息。

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. 定位到需要修改信息的用户，单击目标用户名。
4. 在该用户的**基本信息**页签下，修改用户信息，然后单击**更新**。

锁定或解锁用户

如果某个用户在一段时间内无需使用堡垒机进行运维，您可以在用户页面锁定该用户，被锁定的用户将无法登录服务器进行运维操作。如果已锁定的用户再次需要进行运维，您可以解锁该用户。

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，选中需要锁定或解锁的用户，然后单击**锁定**或**解锁**。

   > **注意** 锁定或解锁操作会即时生效，请您谨慎操作。

   以下是对锁定和解锁操作的说明。
   - **锁定**：锁定用户后，该用户无法登录已授权主机进行运维。在用户列表的**状态**列，已锁定用户的状态会从**正常**切换为**锁定**。锁定用户后，您仍可以修改该用户的基本信息、为该用户授权主机和主机组。
   - **解锁**：解锁成功后，您将收到**用户解锁成功**的提示信息。该用户即可正常登录已授权的主机进行运维。

托管用户公钥

如果需要堡垒机托管用户公钥，您可以在配置用户公钥后将公钥托管至堡垒机，用户即可使用私钥通过运维客户端登录堡垒机。

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. 在用户列表中，单击要配置用户公钥的用户名，并在**用户详情**页面，单击**用户公钥**页签，然后单击**添加SSH公钥**。
4. 在**添加SSH公钥**面板上，配置公钥的信息，包括**公钥名称**、用户**公钥**和**备注**。
5. 单击下方的**添加SSH公钥**。

   配置完成后，您可以在用户公钥列表中查看已托管的用户公钥。

删除用户

如果运维人员不再需要通过堡垒机运维主机，您可以删除对应的用户，降低安全风险。

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. 在用户列表中，选中需要删除的用户，然后单击**删除**。

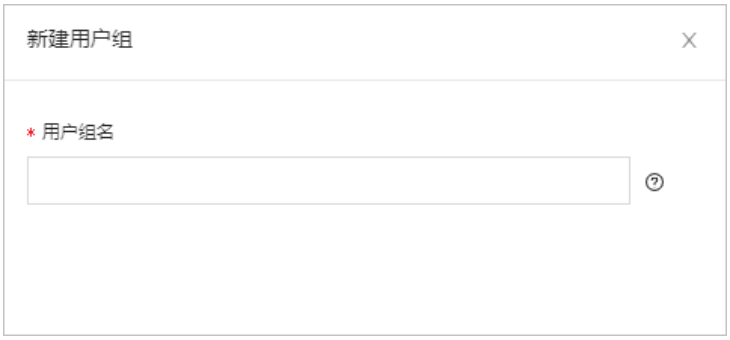
1.5.2. 用户组管理

1.5.2.1. 新建用户组

您可以使用用户组功能，对多个用户进行批量授权。本文介绍如何新建用户组。

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在**用户组**页面，单击**新建用户组**。
4. 在**用户组名**文本框输入您的用户组名称。



> **说明** 用户组名称建议使用能代表该用户组的信息，方便后续的管理和维护。

5. 单击**新建用户组**。

执行结果

创建成功后，您可以在用户组列表中查看新建的用户组。

后续步骤

用户组创建完成后，您可以将用户添加到用户组中，具体请参见添加和维护用户组成员。

1.5.2.2. 修改和删除用户组

当用户组信息需要变更或者不再需要用户组时，您可以修改或删除用户组。

修改用户组基本信息

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在用户组列表中，单击需要修改信息的用户组名称。

4. 在**用户组名**中，输入新的用户组名称。

5. 单击**更新用户组**。

删除用户组

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在用户组列表中，选中需要删除的用户组并单击**删除**。

1.5.2.3. 添加和维护用户组成员

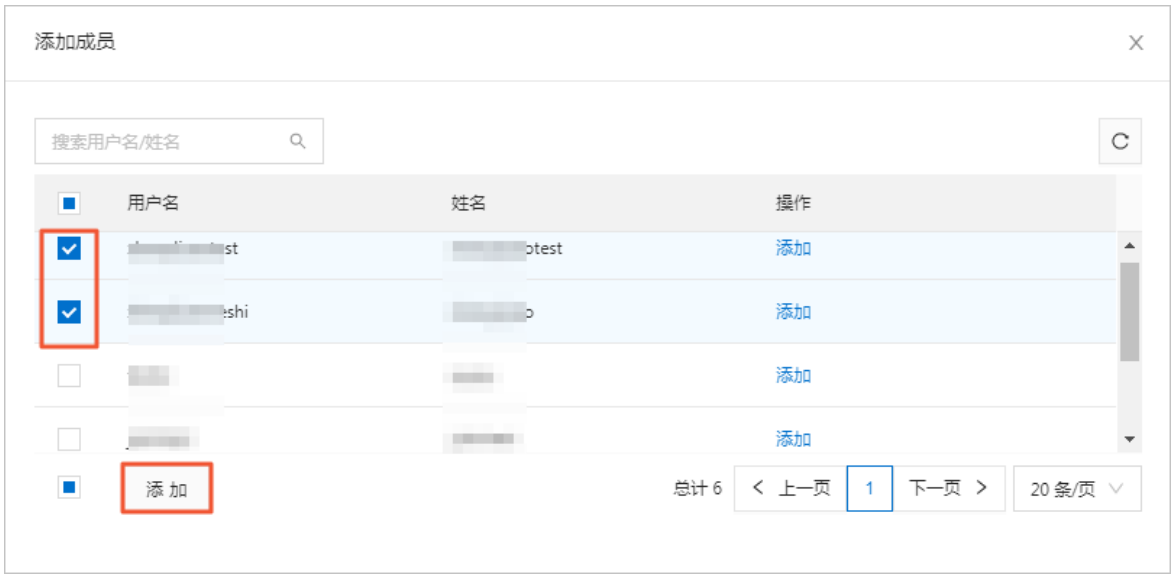
您可以将多个用户加入到一个用户组，并对这些用户进行批量授权。

添加用户组成员

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在用户组列表中，单击用户组名称。

4. 单击**用户组成员**页签。
5. 在**用户组成员**页签下单击**添加成员**。

6. 在**添加成员**对话框，选中需要添加的用户并单击**添加**。



> **说明** 如果只需要添加单个用户，您可以在该用户的**操作**列中单击**添加**。

移除用户组成员

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。

3. 在用户组列表中，单击用户组名称。

4. 单击**用户组成员**页签。
5. 在用户组成员列表中，选中需要移除的用户并单击**移除**。

> **说明** 如果只需要移除单个用户，您可以在该用户的**操作**列中单击**移除**。

1.5.3. 授权主机

1.5.3.1. 按用户授权主机

堡垒机提供按用户授权主机的功能。当您新建用户之后，您可以为该用户授权主机。授权后该用户即可使用堡垒机运维已授权的主机。本文介绍如何为用户授权主机。

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**。

移除已授权主机

根据最小授权原则，如果用户已经不需要维护某些主机，需要将这些主机从该用户的已授权主机列表中移除。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. 在需要移除授权主机的用户的**操作**列中，单击**授权主机**。

4. 在已授权主机列表中选中要移除的主机，单击**移除**。

5. 在确认对话框中，单击**移除**。

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。

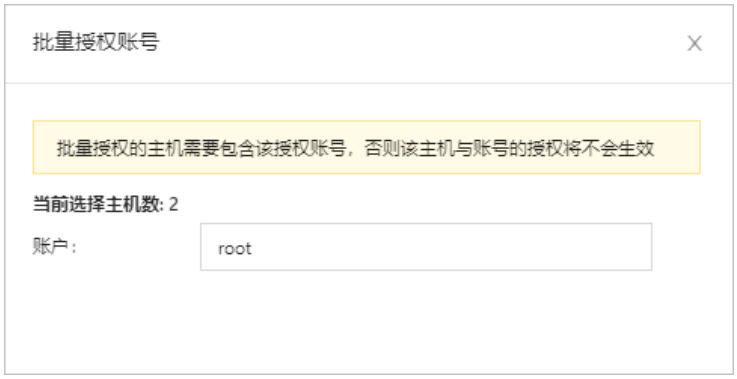
批量授权主机账户

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**。

批量移除已授权主机账户

为用户批量移除多个主机的已授权登录账户，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. 在需要移除授权主机账户的用户的**操作**列中，单击**授权主机**。

4. 在**已授权主机**页签，选中需要移除主机账户的主机。
5. 单击**批量 > 批量移除授权账号**。

6. 选中需要移除的主机授权账户名称。

> **说明** 批量移除已授权主机账号时，只能选择一个账户进行移除。

7. 单击**更新**。

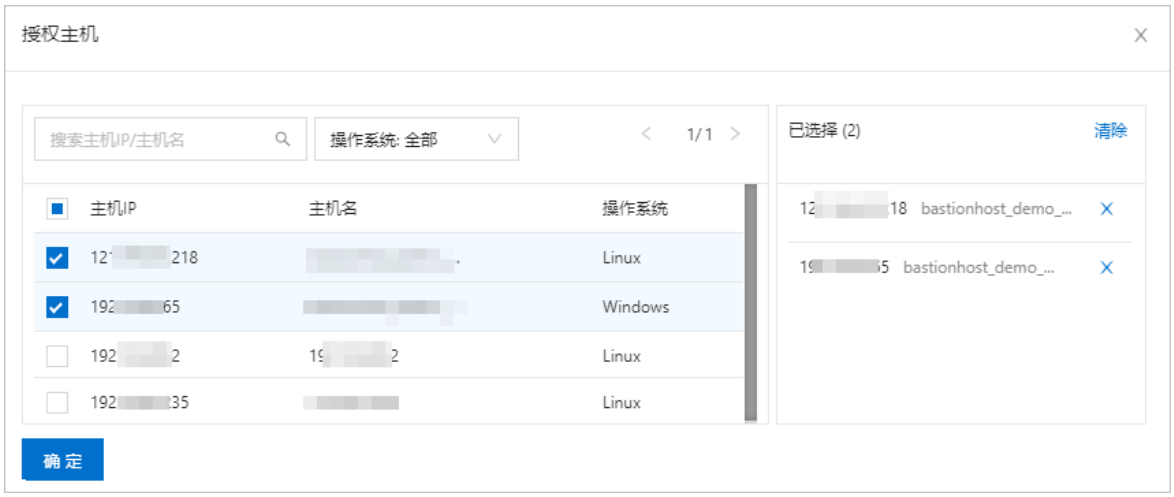
1.5.3.2. 按用户组授权主机

堡垒机提供按用户组授权主机的功能。当您新建用户组之后，您可以为该用户组授权主机。授权后用户组内的用户即可使用堡垒机运维已授权的主机。本文介绍如何为用户组授权主机。

授权主机

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在用户组列表中，单击需要授权主机的用户组的**操作**列的**授权主机**。

4. 在**已授权主机**页签中，单击**授权主机**。
5. 在**授权主机**面板上选中需要授权给该用户组进行运维的主机，并单击**确定**。



移除已授权主机

如果用户组已经不需要维护某些主机，可以移除已授权主机，实现最小授权原则。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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在需要移除授权主机的用户组的**操作**列中，单击**授权主机**。

4. 在**已授权主机**页签下，选中要移除的已授权主机并单击**移除**。

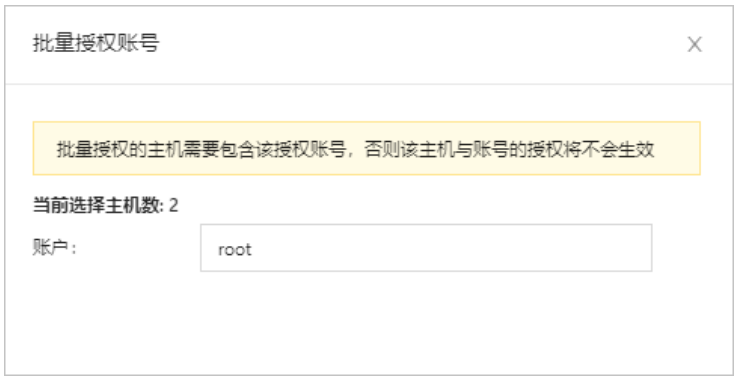
5. 在确认提示框中，单击**移除**。

批量授权主机账户

为用户组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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在用户组列表中，单击需要授权主机的用户组的**操作**列的**授权主机**。

4. 选中要授权账户的主机并单击下方的**批量 > 批量授权账号**。
5. 选择主机授权账户**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**。

批量移除已授权主机账户

为用户组批量移除多个主机的已授权登录账户，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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 在需要移除授权主机账户的用户组的**操作**列中，单击**授权主机**。

4. 在**已授权主机**页签，选中需要移除主机账户的主机并单击**批量 > 批量移除授权账号**。
5. 选择需要移除的主机授权账户**账户**名称。

> **说明** 批量移除已授权主机账号时，只能选择一个账户进行移除。

6. 单击**更新**。

1.5.3.3. 导出授权关系

堡垒机控制台提供导出授权关系的功能，通过导出授权规则，您可以查看所有用户和主机或主机组之间的授权关系。本文介绍如何导出用户和主机或主机组的授权关系。

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**导出授权关系**。

授权关系列表文件将以*.csv*格式导出到本地。

1.5.4. 授权主机组

1.5.4.1. 按用户授权主机组

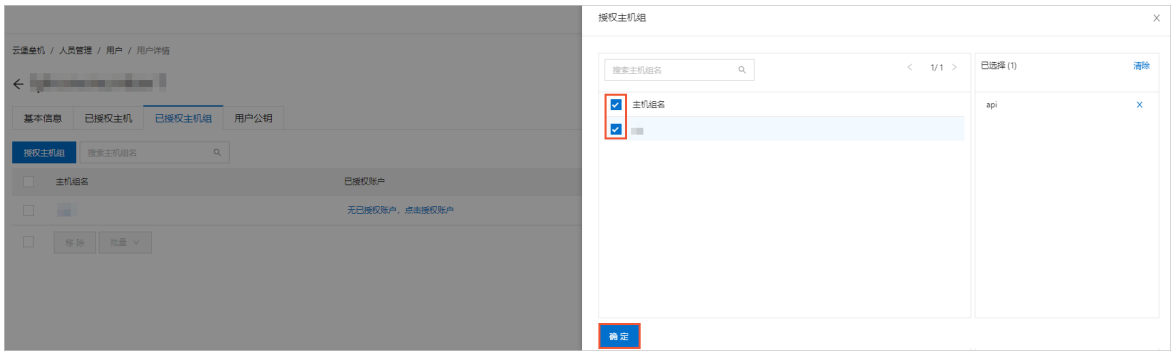
堡垒机提供按用户授权主机组的功能。当您新建用户之后，您可以为该用户授权主机组。授权后该用户即可使用堡垒机运维已授权的主机组内的主机。本文介绍如何为用户授权主机组。

授权主机组

为用户授权主机组，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**授权主机组**。

4. 在**已授权主机组**页签中，单击**授权主机组**。
5. 选中需要授权给该用户进行运维的主机组并单击**确定**。



移除已授权主机组

如果用户已经不需要维护某些主机组，可以移除已授权主机组，实现最小授权原则。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. 在需要移除授权主机组的用户的**操作**列中，单击**授权主机组**。
4. 选中需要移除的已授权主机组并单击**移除**。

5. 在确认提示框中，单击**移除**。

授权主机组账户

为用户授权单个主机组的登录账户，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**授权主机组**。

4. 在**已授权主机组**页签中，单击**无已授权账户，点击授权账户**。

> **说明** 如果主机组需要修改账户，您可以单击该主机组**已授权账户**下的账户名称，修改授权账户。

5. 在**账户**文本框输入您的账户名称。

6. 单击**更新**。

批量授权主机组账户

为用户批量授权多个主机组的登录账户，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**授权主机组**。

4. 选中需要授权账户的主机组并单击**批量 > 批量授权账号**。

5. 在**账户**文本框输入主机账户名称。

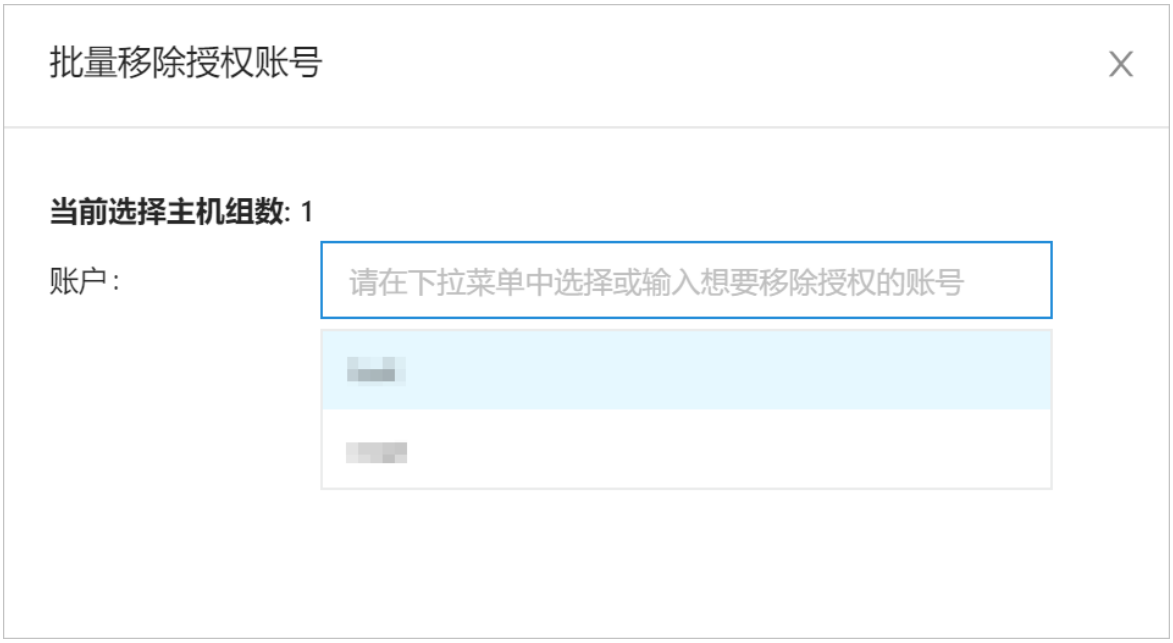
6. 单击**更新**

批量移除已授权主机组账户

为用户批量移除多个主机组的已授权登录账户，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. 在需要移除授权主机组账户的用户的**操作**列中，单击**授权主机组**。
4. 在**已授权主机组**页签，选中要移除账户的主机组并单击**批量 > 批量移除授权账号**。

5. 在**账户**列表选中需要移除的授权账户。



6. 单击**更新**。

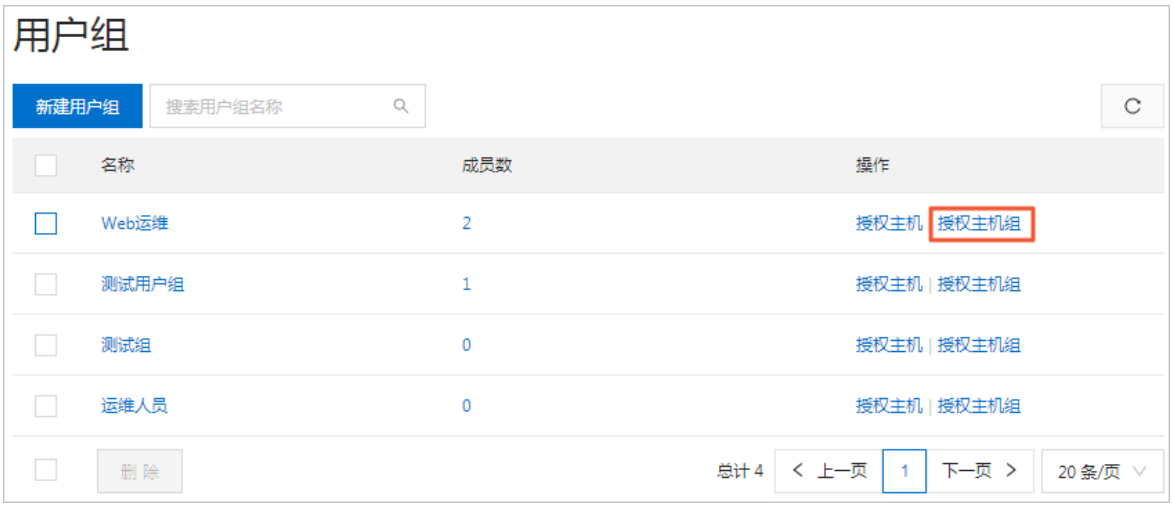
1.5.4.2. 按用户组授权主机组

堡垒机提供按用户组授权主机组的功能。当您新建用户组之后，您可以为该用户组授权主机组。授权后用户组内的用户即可使用堡垒机运维已授权的主机组内的主机。本文介绍如何为用户组授权主机组。

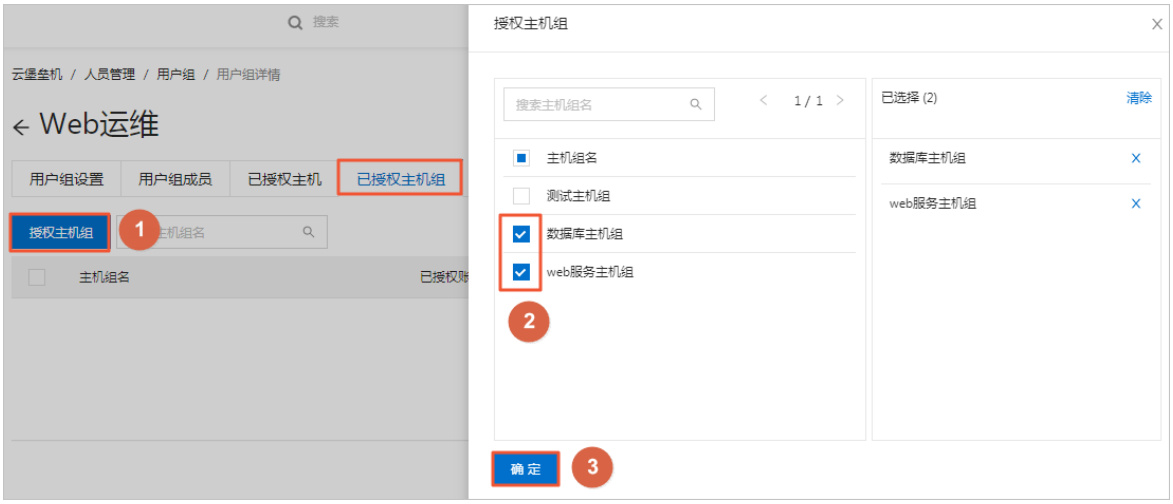
授权主机组

为用户组授权主机组，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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 定位到需要授权的用户组并单击**操作**的**授权主机组**。



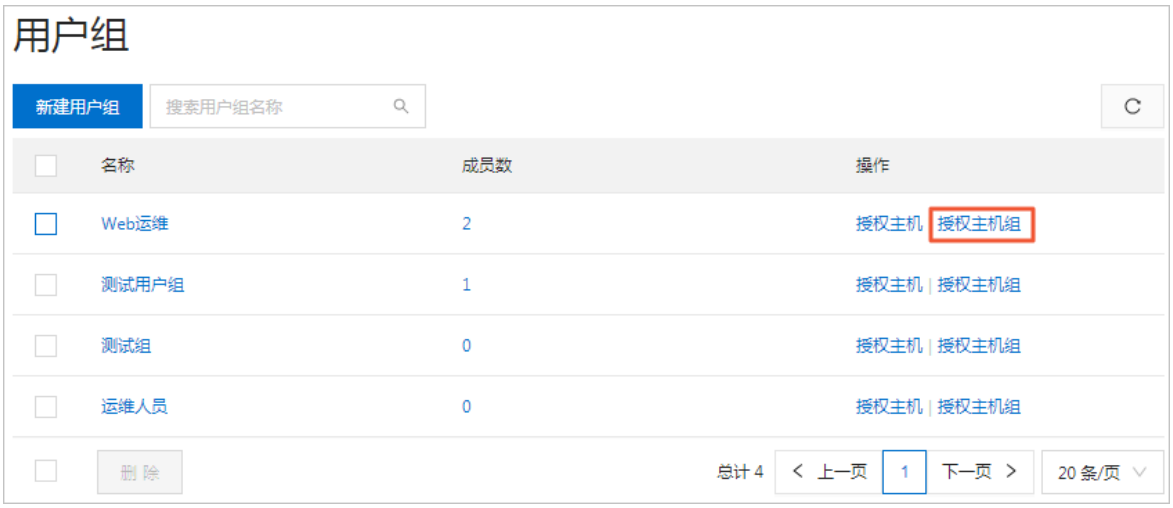
4. 在**已授权主机组**页签中，单击**授权主机组**。
5. 选中需要授权给该用户组进行运维的主机组并单击**确定**。



移除已授权主机组

如果用户组已经不需要维护某些主机组，可以移除已授权主机组，实现最小授权原则。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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 定位到需要移除授权主机组的用户组并单击**操作**列的**授权主机组**。



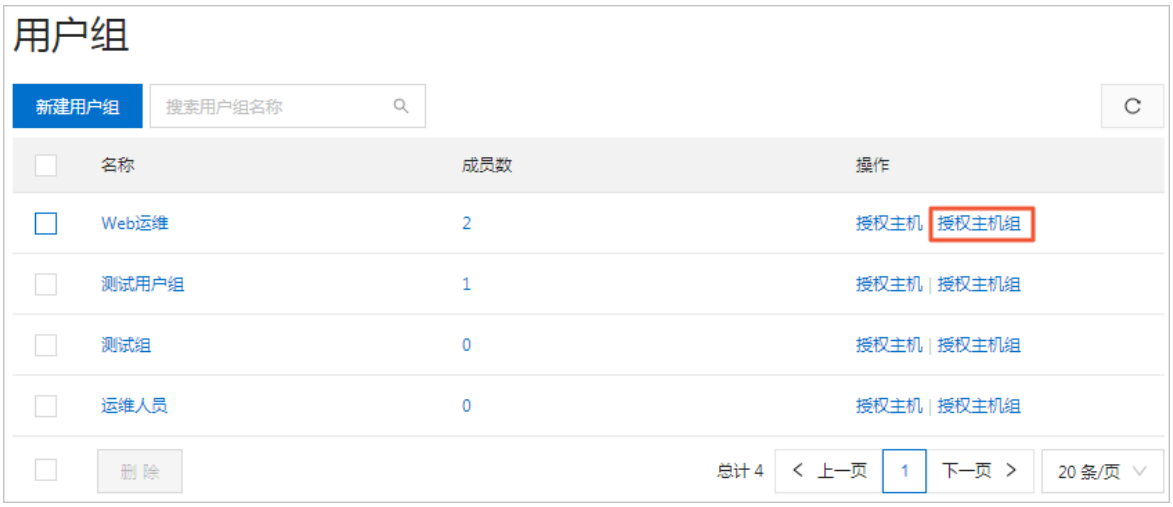
4. 选中需要移除的已授权主机组并单击**移除**。

5. 在确认提示框中，单击**移除**。

授权主机组账户

为用户组授权单个主机组的登录账户，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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 定位到需要授权的用户组并单击**操作**的**授权主机组**。



4. 在**已授权主机组**页签中，单击**无已授权账户，点击授权账户**。

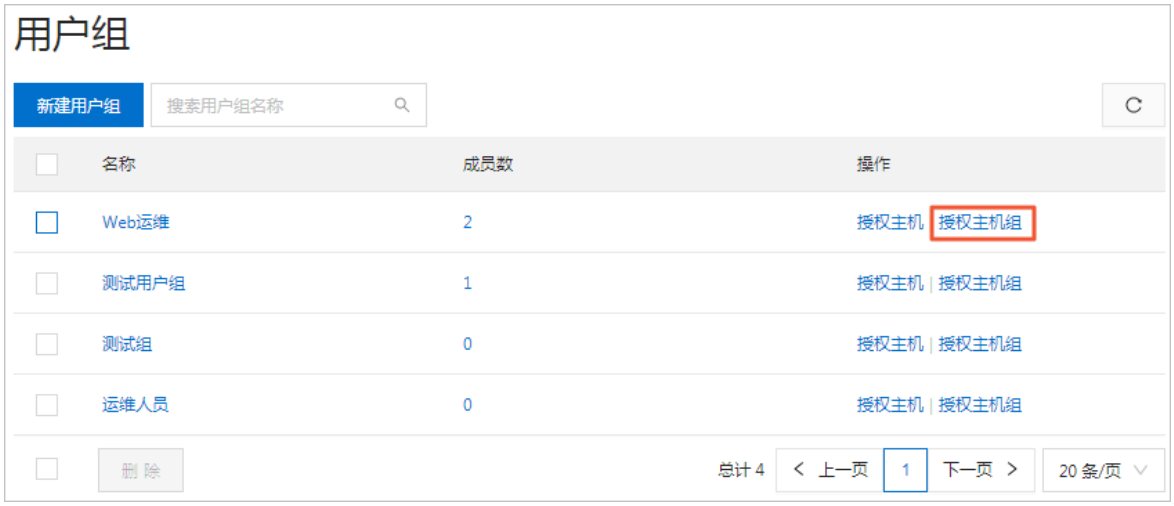
说明 如果主机组需要修改账户，您可以单击该主机组**已授权账户**下的账户名称，修改授权账户。

5. 在**账户**文本框输入账户名称。
6. 单击**更新**。

批量授权主机组账户

为用户组批量授权多个主机组的登录账户，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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 定位到需要授权的用户组并单击**操作**的**授权主机组**。



4. 选中需要授权账户的主机组并单击**批量 > 批量授权账号**。

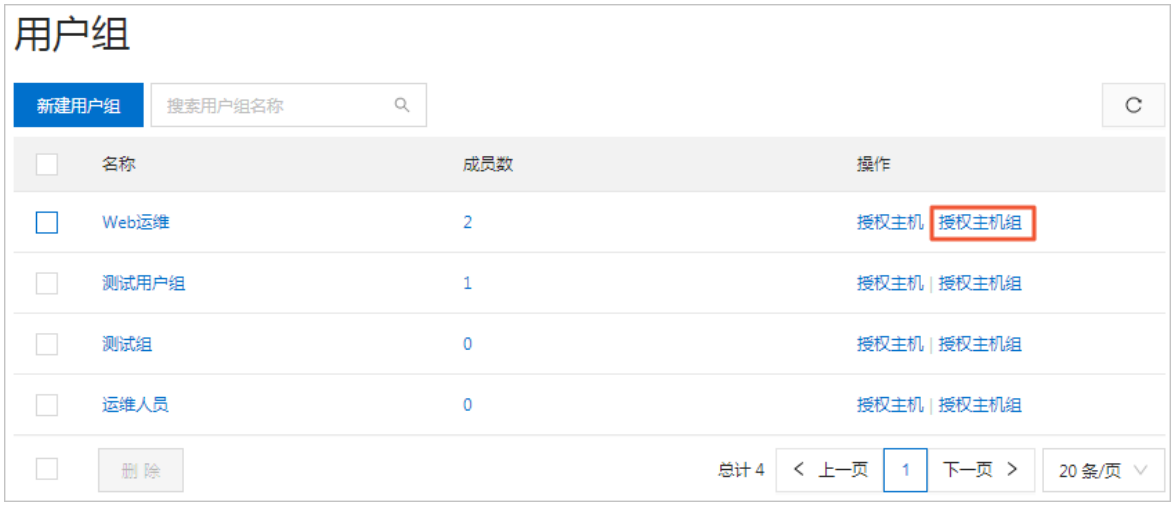
5. 在**账户**文本框输入账户名称。

6. 单击**更新**。

批量移除已授权主机组账户

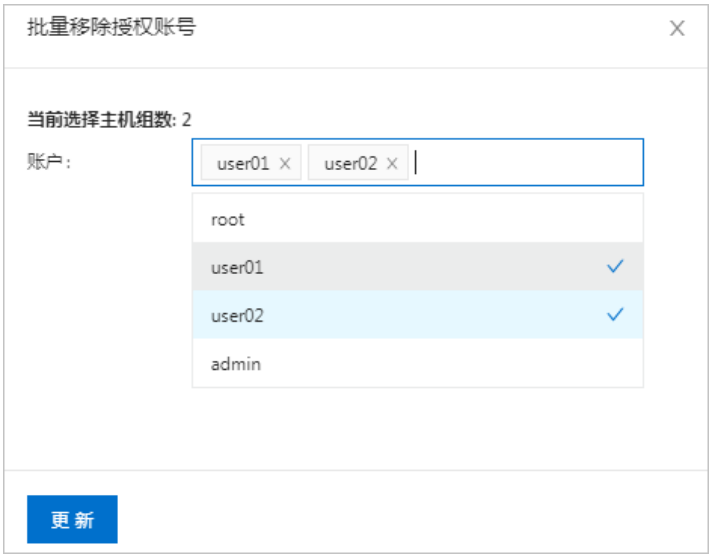
为用户组批量移除多个主机组的已授权登录账户，具体操作请参见以下步骤：

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 > 用户组**，然后在**用户组**页面，单击**新建用户组**。
3. 定位到需要移除账户的用户组并单击**操作**列的**授权主机组**。



4. 选中需要移除账户的主机组并单击**批量 > 批量移除授权账号**。

5. 在**账户**列表中选中需要移除的授权账户。



6. 单击**更新**。

1.6. 授权规则

1.6.1. 新建授权规则

堡垒机提供授权规则功能。您可以使用授权规则功能，按需求为多个用户批量授权资产，以及设置这些用户访问资产的有效期。授权规则功能不仅可以提升您管理用户和资产的效率，而且可以对用户访问资产的时间加以控制。本文介绍如何使用授权规则功能。

背景信息

堡垒机V3.2.22版本之前版本，仅支持为单个用户（或用户组）授权主机（或主机组），且不支持设置用户访问资产的有效期。如果您想使用授权规则功能，您需要将堡垒机实例升级至V3.2.22版本。

- 版本升级的时间，请参见【升级】堡垒机V3.2.22版本升级通知。
- 版本升级的具体操作，请参见版本升级配置指导。

操作步骤

1. 登录云盾堡垒机控制台。

2. 在左侧导航栏中，单击**授权规则**。
3. 在**授权规则**页面，单击**新建授权规则**。
4. 在**新建授权规则**面板上，对**授权规则名称**、**授权规则有效期**等进行配置。

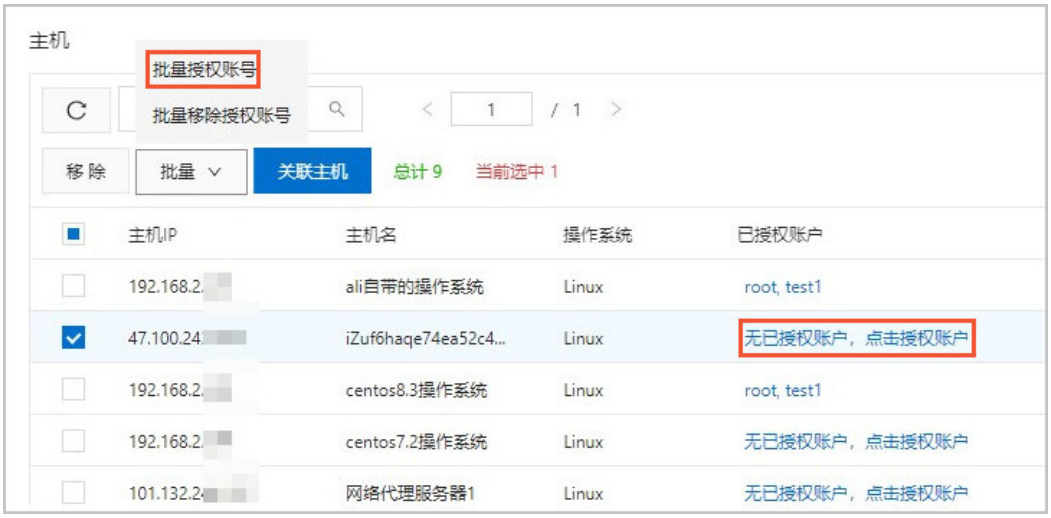
配置项	描述
授权规则名称	设置授权规则的名称。
授权规则有效期	设置授权规则的有效期。可按需要设置规则的开始、结束的日期及具体时间点。
备注	设置授权规则的备注信息。

5. 单击**新建授权规则**。
6. 在创建授权规则成功区域，单击**关联主机用户**。
7. 在**授权详情**页面，配置主机和用户。

i. **配置主机（主机组）**

- 如果您想该授权规则适用于所有主机，您可以选中**对所有主机生效**。
- 如果您想该授权规则只适用于部分主机，您可以选中**对已选择的主机生效**，然后按照以下步骤设置：
  a. 单击**关联主机（关联主机组）**。
  b. 在**关联主机（关联主机组）**面板的主机（主机组）列表中，选中您要关联的主机（主机组）。
  c. 单击**确定**。
  d. （可选）如果关联主机（主机组）后，在主机（主机组）列表中的**已授权账户**列显示**无已授权账户，点击授权账户**，请您单击**无已授权账户，点击授权账户**为该主机（主机组）完成账户授权。支持选中多个需要账户授权的主机（主机组）进行批量账户授权。

  如果您想批量移除授权账户，也可选中多个需要移除账户授权的主机（主机组），进行批量移除授权账户。



ii. **配置用户（用户组）**

- 如果您想该授权规则适用于所有用户，您可以在选中**对所有用户生效**。
- 如果您想该授权规则只适用于部分用户，您可以选中**对已选择的用户生效**，然后按照以下步骤设置：
  a. 单击**关联用户（关联用户组）**。
  b. 在**关联用户（关联用户组）**面板的用户（用户组）列表中，选中您要关联的用户（用户组）。
  c. 单击**确定**。

配置完成后，您可以在主机、主机组、用户以及用户组列表中看到您已关联的主机和用户。

执行结果

授权规则配置成功后，在该授权规则的**规则有效期**内，授权规则中关联的用户、用户组可以在设置的有效期内访问主机、主机组。

1.6.2. 管理授权规则

如果您需要修改某个授权规则的配置项或者该授权规则已过期不需要在维护了，您可以修改或者删除该授权规则。本文介绍如何修改、删除授权规则。

前提条件

已在堡垒机实例中创建了授权规则。具体操作，请参见新建授权规则。

修改授权规则

您可以修改已创建的授权规则的**基本信息**和**主机/用户**。

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，单击**授权规则**。
3. 在**授权规则**页面的授权规则列表中，定位到您要修改的授权规则。
4. 单击该授权规则操作列的**编辑**。
5. 在授权详情页面，修改授权规则的配置信息。
   - 修改**基本信息**。
     a. 修改**授权规则名称**、**授权规则有效期**及**备注**。
     b. 单击**更新**。
   - 修改**主机/用户**。
     您可以为该授权规则添加或删除主机和用户。修改主机、主机组、用户及用户组的操作相同。
     下文以修改主机为例，为您介绍如何修改已创建的授权规则中的主机。
     a. 单击**主机/用户**页签。
     b. 在主机区域，单击**关联主机**或者选中要删除的主机单击**移除**，为授权规则添加或删除主机。

   授权规则修改后，堡垒机将按照修改后的授权规则执行。

删除授权规则

如果某个授权规则已不再需要了，您可以删除该授权规则。

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，单击**授权规则**。
3. 在**授权规则**页面的授权规则列表中，定位到您要删除的授权规则。
4. 单击该授权规则操作列的**删除**。
5. 在弹出的确认对话框中单击**删除**。
   授权规则删除后，规则中为用户授权的资产及设置的访问资产的有效期等配置也会随之失效。

1.7. 控制策略

1.7.1. 添加控制策略

堡垒机提供控制策略功能。使用控制策略功能，您可以设置命令控制、命令审批、协议控制和访问控制策略来管理用户对主机的访问。本文介绍如何新建控制策略。

操作步骤

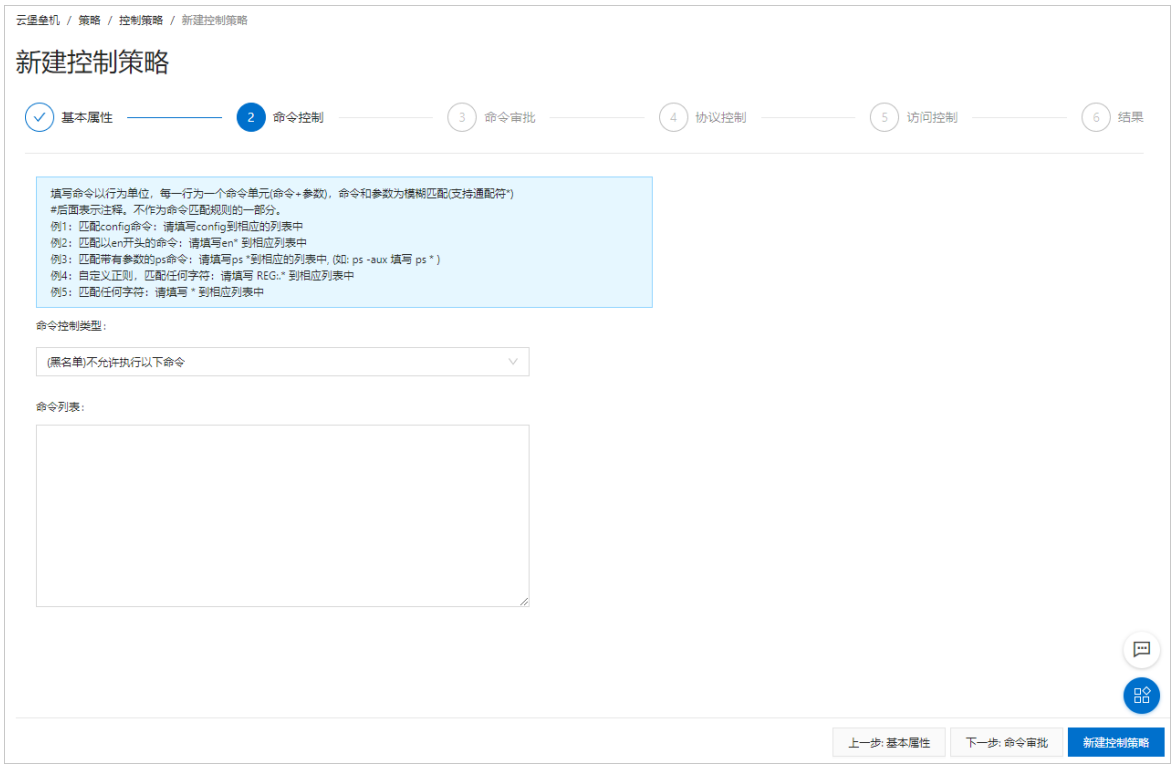
1. 登录堡垒机系统。具体操作，请参见登录堡垒机系统。
2. 在左侧导航栏，单击**控制策略**。
3. 在**控制策略**页面，单击**新建控制策略**。
4. 配置策略**名称**、**优先级**和**备注**并单击**下一步：命令控制（选填）**。

> **说明**
>
> - 优先级可设置范围：1~100。默认值为1，即最高优先级。
> - 不同控制策略可以设置相同的优先级。多个控制策略的优先级相同时，堡垒机会根据策略中具体的规则来确定策略生效顺序。命令相关规则优先级排序（从高到低）：拒绝、允许、审批。访问控制策略优先级排序：黑名单高于白名单。

5. 配置**命令控制类型**、**命令列表**并单击**下一步：命令审批（选填）**。

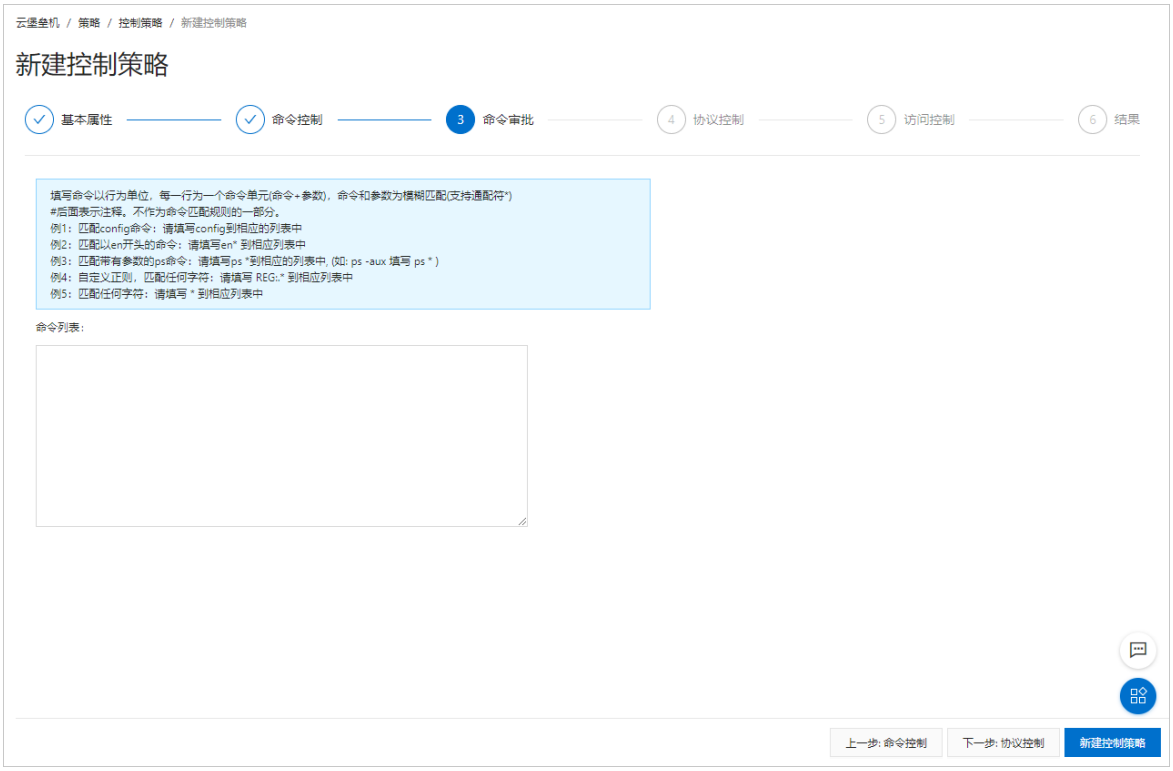
   命令控制类型分为**（白名单）只允许执行以下命令**和**（黑名单）不允许执行以下命令**：

   - **（白名单）只允许执行以下命令**：选择白名单后，命令列表为必填选项。在当前策略生效用户和主机中，只允许执行白名单命令列表中的命令。
   - **（黑名单）不允许执行以下命令**：选择黑名单后，命令控制列表可以为空。在当前策略生效用户和主机中，不允许执行黑名单命令列表中的命令。



6. 配置命令审批中的**命令列表**并单击**下一步：协议控制（选填）**。

   命令审批对命令控制（白名单或黑名单）以外的命令生效。命令控制策略生效的优先级高于命令审批。如果用户执行了已配置在命令审批命令列表中的命令，您可以在堡垒机控制台对该命令是否执行进行审批。审批允许后该命令会被执行，审批拒绝后该命令不生效。关于命令审批的更多信息请参见审批命令。



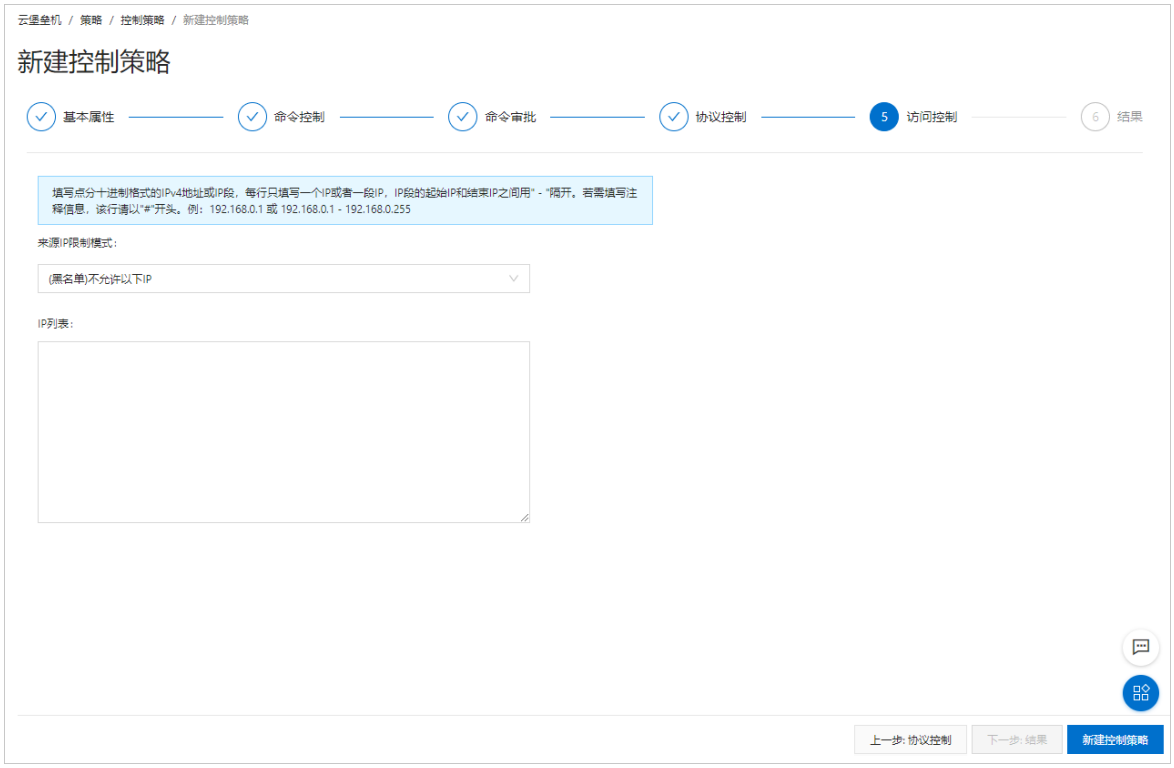
7. 配置**RDP选项**、**SSH选项**、**SFTP选项**，并单击**下一步：访问控制（选填）**。

   选中协议控制项表示允许该操作，未选中表示不允许进行相应操作。例如：选中文件上传，表示允许执行上传文件操作。

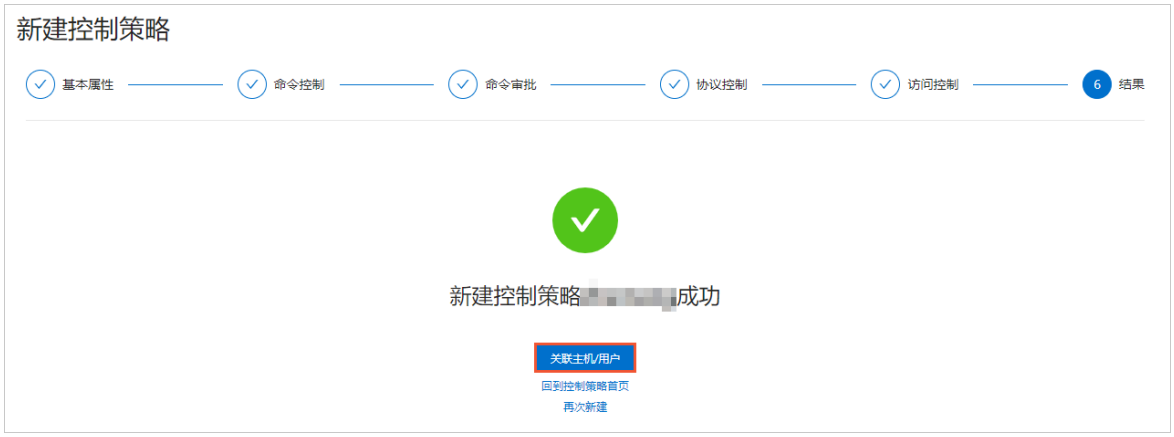
8. 设置允许访问主机的来源IP限制模式、IP列表并单击**新建控制策略**。

   您可以选择以下来源IP限制模式：

   - **（白名单）只允许以下IP**：如果选择白名单，IP列表为必填项。只允许白名单中的来源IP访问当前策略生效的主机。
   - **（黑名单）不允许以下IP**：如果选择黑名单，IP列表可以为空。不允许黑名单中的来源IP访问当前策略生效的主机。



9. （可选）单击**关联主机/用户**。



您可以为该策略关联用户或主机，使该策略在相应主机或用户上生效。更多信息请参见关联主机或用户。

控制策略功能视频演示

1.7.2. 管理控制策略

已添加的控制策略支持编辑和删除，您可以根据业务场景的变化对已有控制策略进行修改或者删除。本文介绍如何编辑、删除控制策略，以及如何为控制策略关联主机和用户。

编辑控制策略

如果您需要修改已有的控制策略，请参考以下步骤操作：

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，单击**控制策略**。
3. 在控制策略列表中定位到需要修改的控制策略，单击**操作**列的**编辑**。

您也可以单击控制策略名称进入**控制策略详情**页面。

4. 在**控制策略详情**页面，修改**控制策略设置**、**命令控制**、**命令审批**、**协议控制**、**访问控制**和**主机/用户**。

修改**控制策略设置**、**命令控制**、**命令审批**、**协议控制**和**访问控制**的详细信息，请参见添加控制策略。关联**主机/用户**的详细信息，请参见关联主机或用户。

5. 单击**更新控制策略**。

删除控制策略

如果您需要删除不再使用的控制策略，请参考以下步骤操作：

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，单击**控制策略**。
3. 定位到需要删除的控制策略并单击操作列下的**删除**。

如果需要删除多个控制策略，您可以选中需要删除的控制策略并单击控制策略列表下的**删除**。

4. 在确认删除提示框中单击**删除**。

关联主机或用户

如果您需要为新创建的控制策略关联用户和主机，或者修改已有控制策略关联的主机和用户，请参考以下步骤操作：

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，单击**控制策略**。
3. 定位到需要修改关联用户或主机的控制策略并单击**用户**、**用户组**、**主机**或**主机组**列下的数字。

您也可以单击需要修改关联用户或主机的控制策略名称或操作列下的**编辑**，并切换到**主机/用户**页签。

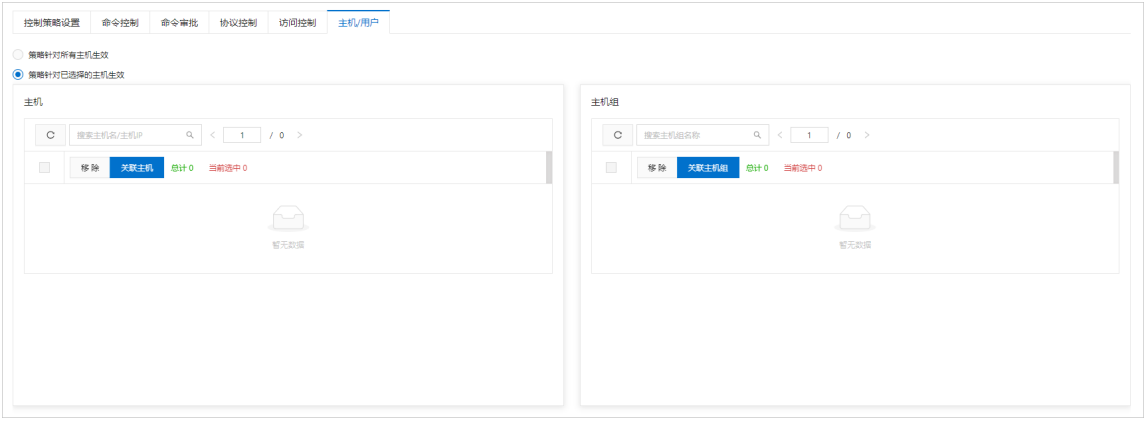
4. 设置关联主机和用户的生效策略。

> **说明** 主机或用户生效策略选择后会立即生效，建议您先确认需要设置的生效策略，再进行相应操作。

您可以根据以下信息选择合适的策略：

- 选择主机生效策略

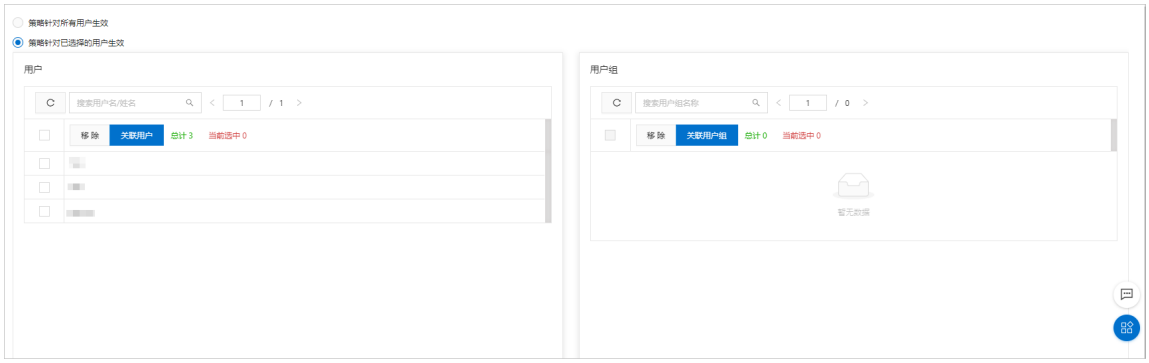
  您可以选择**策略针对所有主机生效**或**策略针对已选择的主机生效**。如果选择了**策略针对已选择的主机生效**，您需要设置策略关联的主机或主机组。设置关联主机或主机组后，该策略只对关联的主机或主机组生效。



> **说明** 如果多条优先级相同的控制策略对同一个主机同时生效，堡垒机会根据策略中具体的规则来确定策略生效顺序。命令相关规则优先级排序（从高到低）：拒绝、允许、审批。访问控制策略优先级排序：黑名单高于白名单。

- 设置用户生效策略

  您可以选择**策略针对所有用户生效**或**策略针对已选择的用户生效**。如果选择了**策略针对已选择的用户生效**，您需要设置策略关联的用户或用户组。设置关联用户或用户组后，该策略只对关联的用户或用户组生效。



如果某些主机或用户不再需要使用该策略，您可以将这些主机或用户从策略生效列表中移除。您可以选中需要移除的主机或用户，单击**移除**。

1.8. 命令审批

1.8.1. 审批命令

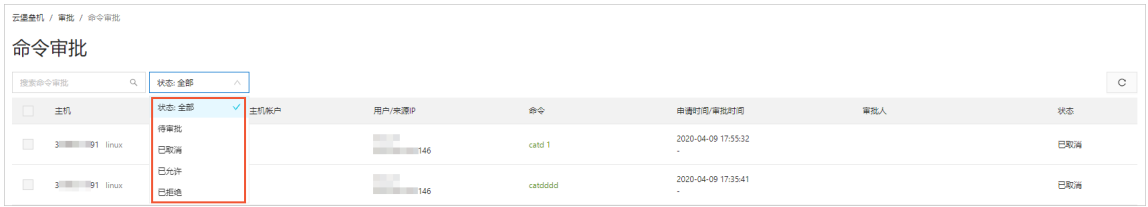
添加控制策略时配置了审批命令并关联了主机和用户后，如果关联的用户在关联的主机上执行了审批命令中的命令，管理员会在堡垒机控制台收到该命令的审批。管理员审批允许后该命令才会执行，审批拒绝后该命令不执行。命令控制列表中的命令无需审批。本文介绍管理员如何审批命令。

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，单击**命令审批**。
3. 在**命令审批**页面，您可以根据需要执行以下操作。
   - **查看命令详细信息**

     您可以在命令列表中查看命令的**主机**、**协议/主机帐户**、**用户/来源IP**、**命令**、**申请时间/审批时间**、**审批人**和**状态**。

您可以在**状态**列表中单击某个状态查看相应状态的命令。例如：单击**待审批**，可以查看待审批的命令列表。



支持选择以下命令状态：

- **全部**：所有状态的命令。
- **待审批**：等待审批的命令。
- **已取消**：已取消执行的命令。
- **已允许**：审批后允许执行的命令。

- **已拒绝**：审批后拒绝执行的命令。

- **允许命令**

  选中允许执行的命令并单击命令审批列表下方的**允许**。

- **拒绝命令**

  选中拒绝执行的命令并单击命令审批列表下方的**拒绝**。

1.9. 审计

1.9.1. 会话审计

1.9.1.1. 搜索和查看会话

运维人员每次通过堡垒机进行运维，都会生成一个会话记录运维操作。审计人员可以通过会话，查看运维人员在运维中是否存在违规操作。

前提条件

在播放会话录像前，需要确认浏览器已经安装Flash Player。

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 > 会话审计**。
3. 根据您需要进行搜索的会话类型，单击**所有会话**、**图像文字**、**字符命令**或**文件传输**页签。

图像文字、**字符命令**、**文件传输**这三种审计日志的详细说明如下：

- **图像文字**：可查看通过堡垒机RDP运维访问资产时的审计日志（仅支持Windows Server 2008及以下版本）。
- **字符命令**：可查看通过堡垒机SSH运维访问资产时的字符命令操作的审计日志。
- **文件传输**：可查看通过堡垒机运维访问资产时的文件上传、删除、更名等操作的审计日志。

4. 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
时间	设置搜索会话的时间范围，支持**全部**、**本日**、**本周**、**本月**和自定义时间段。
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。
删除状态	选择会话删除状态，支持选择以下状态： ○ **全部** ○ **未删除** ○ **已删除**

5. （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。

6. 单击**搜索**。

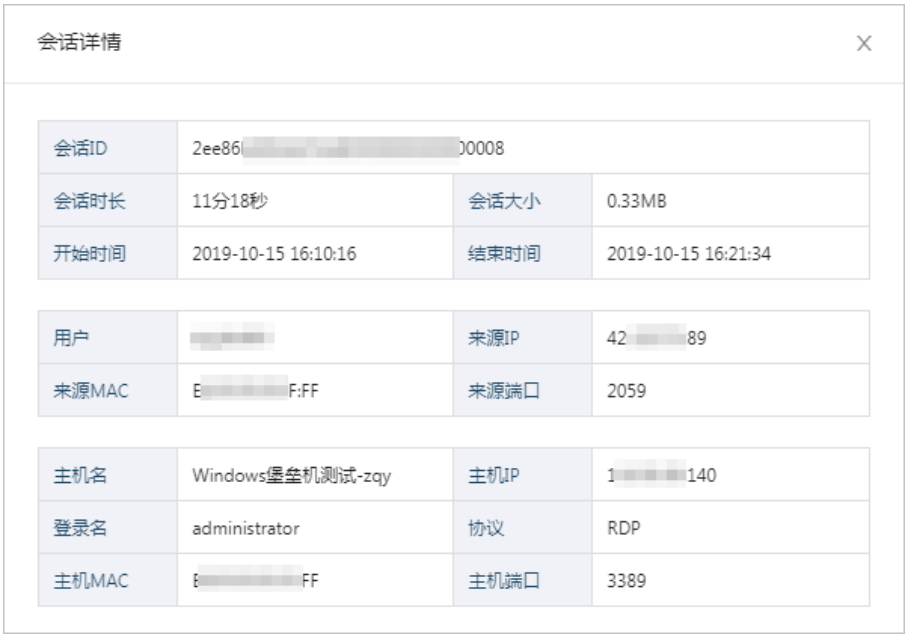
查看会话详情

1. 搜索目标会话。

   搜索目标会话的具体操作，请参见搜索会话。

2. 定位到目标会话，单击**会话操作详情**。

3. 在**会话详情**对话框中，查看会话基本信息、用户基本信息和主机基本信息。



播放会话录像

1. 搜索目标会话。

   搜索目标会话的具体操作，请参见搜索会话。

2. 定位到目标会话并单击**会话操作**列的**播放**，查看运维录像记录。

1.9.1.2. 归档审计日志到日志服务

堡垒机支持将审计日志（即运维记录）归档到日志服务（SLS）中。审计日志归档配置完成后，堡垒机在接收到运维记录时，会自动将日志转存到日志服务中。本文介绍如何将审计日志归档到日志服务中。

背景信息

审计日志即运维人员使用堡垒机进行运维的操作记录。堡垒机只提供180天的日志存储服务，如果需要长期保存审计日志，您可以将审计日志归档至日志服务。将审计日志归档到日志服务后，您可以在日志服务控制台自定义日志保存时间，并对审计日志进行查询和分析。更多信息，请参见查询概述和分析概述。

> **说明** 将审计日志归档到日志服务后，存储在堡垒机的审计日志不受影响，您仍可以在云盾堡垒机控制台**会话审计**页面，查看审计日志。更多信息，请参见搜索和查看会话。

操作步骤

1. 登录日志服务控制台。

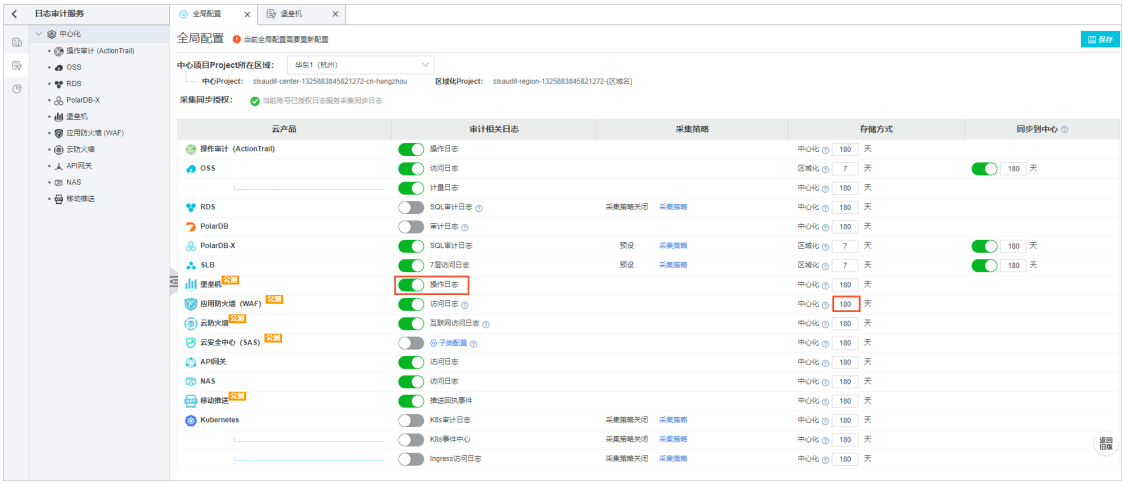
2. 根据页面提示，开通日志服务。
3. 在**日志应用**区域，单击**日志审计服务**。
4. 在**全局配置**页面，参考以下步骤配置审计信息。
   i. 在**中心项目Project所在区域**下拉列表中，选择日志中心化存储的目标地域。
   ii. 配置采集同步授权。

   日志审计服务支持手动授权和通过账号密钥辅助授权。您可以选择以下任一方式配置采集同步授权：

   - **通过账号密钥辅助授权**：输入账号的AccessKey和AccessSecret。

     AccessKey信息不会被保存，仅临时使用。此处AccessKey信息对应的RAM用户需具备RAM读写权限（例如已被授权AliyunRAMFullAccess策略）。
   - **手动授权**：具体操作，请参见自定义授权日志采集与同步。

   iii. 在云产品列表中，打开堡垒机**操作日志**开关并设置**存储方式**中的存储时间。



5. 查看堡垒机审计日志。
   i. 在左侧导航栏，单击 图标。
   ii. 在左侧**中心化**菜单下，单击**堡垒机**。
   iii. 在**堡垒机**页签，查看审计日志。

   操作日志的字段详情，请参见堡垒机日志字段详情。

1.9.1.3. 日志备份

堡垒机提供日志备份功能，帮助您更好地管理运维日志。运维日志会以自然月为单位备份为一个日志文件，您可按需下载。本文介绍如何使用日志备份功能。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，选择**审计 > 会话审计**。
3. 在**会话审计**页面，单击**日志备份**页签。
4. 在**日志备份**页签下，定位到您要下载的日志，单击其右侧的**下载**按钮。
   运维日志会以CSV格式下载到本地。

1.9.2. 实时监控

1.9.2.1. 搜索和查看实时监控会话

用户每次通过堡垒机进行运维，都会生成一个会话记录运维操作，审计人员可以通过实时监控，查看正在运维的会话是否存在违规操作。

前提条件

在播放会话录像前，需要确认浏览器已经安装Flash Player。

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。

搜索项	说明
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。

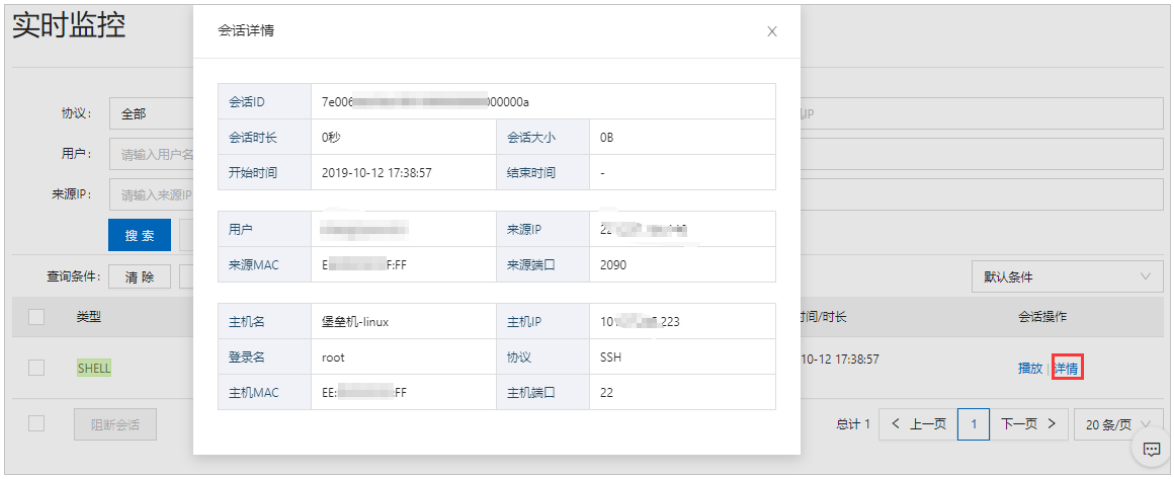
4. （可选）单击**保存**，在**查询条件名称**中输入名称，单击**确定**，保存查询条件。

> **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**。

查看会话详情

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. 定位到目标会话，并单击**会话操作**下的**详情**，查看会话详情。



在**会话详情**中，您可以查看会话基本信息、用户基本信息和主机基本信息。

播放会话录像

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. 定位到目标会话，并单击**会话操作**列下的**播放**，查看运维的实时录像。

1.9.2.2. 阻断会话

在实时监控中，如果您发现用户正在进行违规或者高危操作，可以通过阻断会话功能阻止该用户的连接。

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**。

1.9.3. 操作日志

1.9.3.1. 搜索和查看操作日志

堡垒机中所有的操作都会保存到操作日志中，您可以在操作日志中搜索和查看日志。

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**审计 > 操作日志**。
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
时间	设置日志的时间范围，支持**全部**、**本日**、**本周**、**本月**和自定义时间段。
结果	在下拉栏中选择用户操作是否成功的结果，支持选择以下结果： ○ **全部** ○ **成功** ○ **失败**
操作名称	在操作列表中选择需要查看的操作名称。
用户	输入日志的用户名。
来源IP	输入日志用户的来源IP，即用户访问时使用的IP。

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**，查询符合该搜索条件的日志结果。
6. 在日志列表中，查看日志信息。

时间	操作名称	用户	来源IP	结果
2020-04-29 19:17:32	AttachHostsToUserGroup	[redacted]	42[redacted]164	成功
2020-04-29 17:02:20	AddUsersToGroup	[redacted]	42[redacted]64	成功
2020-04-29 16:12:49	RemoveHostsFromGroup	[redacted]	42.[redacted]64	成功
2020-04-29 16:10:52	AddHostsToGroup	[redacted]	42.[redacted]164	成功

1.9.4. 运维报表

管理员可以通过运维报表，按时间范围查看运维的总体数据、会话大小、运维次数和运维时长。本文介绍如何查看运维报表。

报表说明

运维报表支持按**本日**、**昨天**、**本周**、**本月**和**自定义**五个时间范围查阅运维数据。五个时间范围的具体说明如下表：

页签	说明
本日	时间范围：今天的00:00:00~当前时间。
昨日	时间范围：昨天的00:00:00~24:00:00。
本周	时间范围：本周周一的00:00:00~当前时间。
本月	时间范围：本月1号的00:00:00~当前时间。
自定义	自定义时间范围，最大时间跨度为180天。

总览

总览界面以**总体**、**运维次数**、**运维时长**和**会话大小**四个模块，展示所选择时间范围内的运维数据。

会话大小

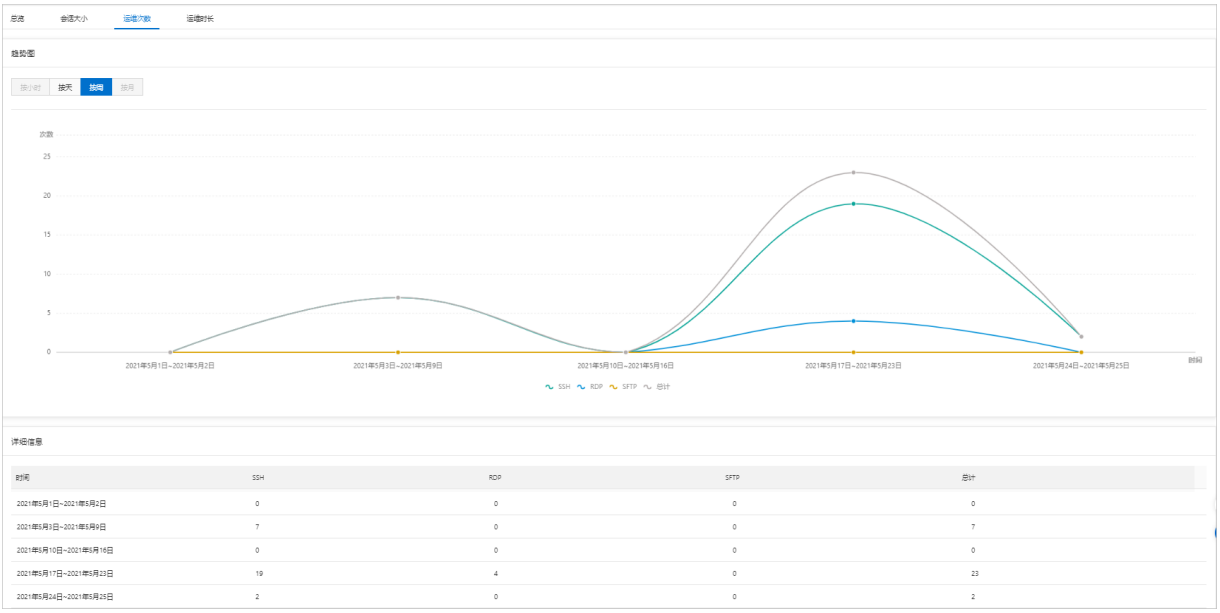
会话大小界面以**趋势图**和**详细信息**展示所选时间范围内的会话量趋势和详情。您还可以在**趋势图**上方的**按小时**、**按天**、**按周**、**按月**这四个页签中，选择更小的时间范围查看会话量的大小。

- **趋势图**：展示所选时间范围内会话量的趋势。
- **详细信息**：按照所选时间范围，从SSH、RDP、SFTP、**总计**四个维度来统计会话量的大小。

运维次数

运维次数界面以**趋势图**和**详细列表**展示所选时间范围的运维次数的趋势和详情。您还可以在**趋势图**上方的**按小时**、**按天**、**按周**、**按月**这四个页签中，选择更小的时间范围查看运维次数。

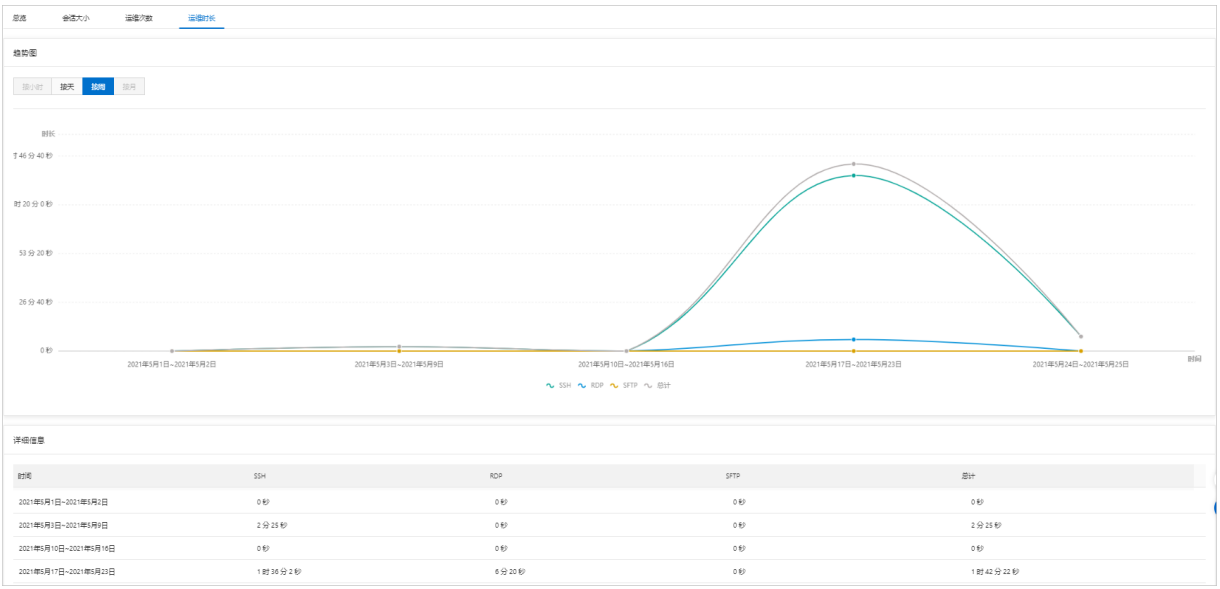
- **趋势图**：展示所选时间范围内运维次数的趋势。
- **详细信息**：按照所选时间范围，从SSH、RDP、SFTP和**总计**四个维度来统计运维次数。



运维时长

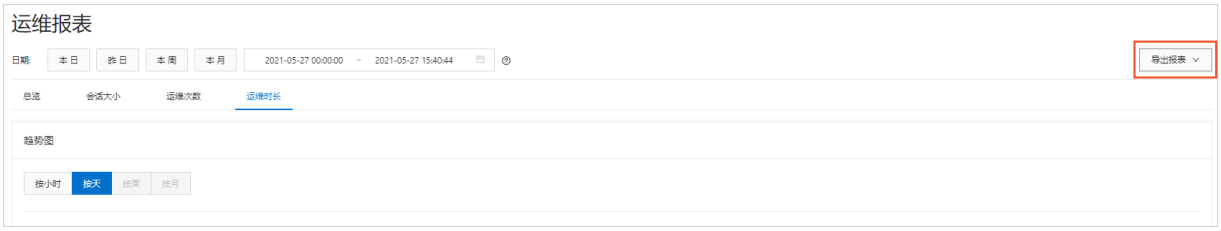
运维时长界面以**趋势图**和**详细列表**展示所选时间范围内的运维时长的趋势和详情。您还可以在**趋势图**上方的**按小时**、**按天**、**按周**、**按月**这四个页签中，选择更小的时间范围查看运维时长的数据。

- **趋势图**：展示所选时间范围内运维时长的趋势。
- **详细信息**：按照所选时间范围，从**SSH**、**RDP**、**SFTP**和**总计**四个维度来统计运维时长。



导出报表

在运维报表界面右上角，单击**导出报表**，可导出所选时间范围内的运维报表。支持导出报表的文件格式有WORD、PDF、HTML。



1.10. 主机运维

1.10.1. 主机运维

主机运维指普通用户以RAM用户身份登录堡垒机控制台并进入Web运维界面，无需通过SSH、RDP、SFTP客户端，可直接在Web端运维主机。本文介绍如何使用主机运维功能。

使用限制

- 仅堡垒机高可用版实例支持使用主机运维功能。
- 仅支持以RAM用户身份登录堡垒机控制台使用主机运维功能。

准备工作

1. 已完成新建并导入RAM用户。具体操作，请参见管理用户。

   > **说明** 如果您已新建RAM用户，请直接导入RAM用户。具体操作，请参见导入已有RAM用户。

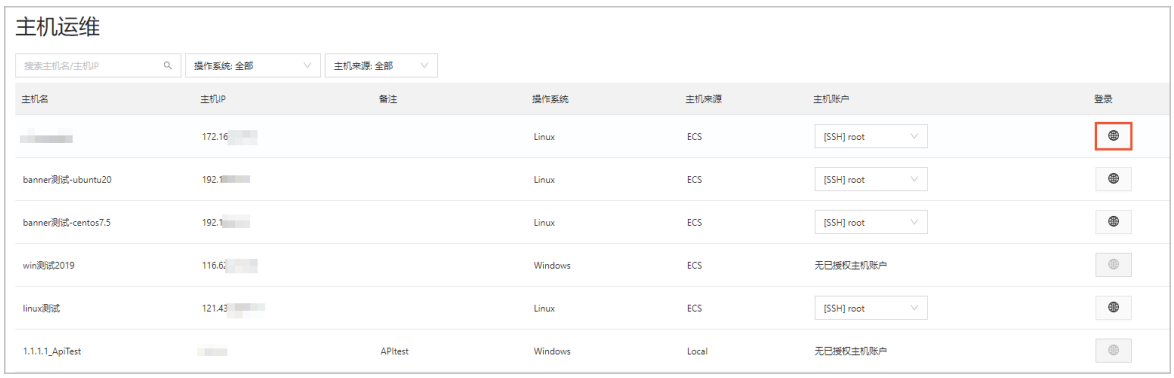
2. 已完成添加主机。具体操作，请参见新建主机。

   > **说明** 如果您想要托管主机账户，可以为主机创建账户。具体操作，请参见新建主机账户。

3. 已完成为用户和主机建立授权关系。具体操作，请参见按用户授权主机、按用户授权主机组。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏中，选择**运维 > 主机运维**。
3. 在**主机运维**页面的主机列表中，单击要运维的主机后面的 图标，即可进入主机运维页面。



如果主机列表中存在未授权的主机，在单击 图标后，会弹出**运维登录**对话框，请按照以下步骤进行配置操作：

i. 在**运维登录**对话框中，填写**登录名**和**密码**。

- **登录名**：登录主机的账户。
- **密码**：登录主机账户的密码。

> **说明** 协议为默认代选状态，您无需选择。

ii. 单击**确定**。

4. 进入Web运维界面，进行运维操作。

1.11. 系统设置

1.11.1. 用户配置

为了保障系统的安全，堡垒机提供用户锁定和用户状态配置功能。您可以通过配置用户密码的锁定策略，防止用户密码被暴力破解；通过配置用户状态，管理用户密码的有效期、标记长期未登录用户账号等。

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，单击**系统设置**。
3. 在**用户配置**页签，设置用户密码配置。

配置项		
用户锁定配置	**密码尝试次数**	用户连续错误登录的最大次数，超过最大次数，则锁定该用户。 取值范围：0~999，默认值为5。设置为**0**，表示不锁定账户。
	锁定时长	用户锁定后，无法登录的时长，单位：分钟。 取值范围：0~10080，默认值为30。设置为**0**，表示锁定用户直到管理员解除。
	重置计数器	密码错误尝试次数未超过设置的**密码尝试次数**时，重新开始计算密码尝试次数的时间，单位：分钟。 例如，**密码尝试次数**设置为5，**重置计数器**设置为5，当您在14:00:00第4次使用错误密码登录失败，并且您在14:00:00~14:05:00期间没有再次使用错误密码登录时，在当日14:05:00后，错误密码的尝试次数将从0开始计算。 取值范围：0~10080，默认值为5。
用户状态配置	**密码有效期**	密码的有效时长，超过有效时长后，需要重新设置密码。密码有效期只对本地用户生效。 取值范围：0~365，默认值为0，单位：天。设置为**0**，表示密码不会过期。
	用户长时间未登录	用户超过设置的时间未登录时，用户状态标记为长时间未登录，单位：天。 取值范围：0~365，默认值为0。设置为**0**，表示不标记状态。
	自动同步AD/LDAP用户状态	自动同步已导入堡垒机的AD/LDAP用户源中用户配置信息和状态的时间间隔，单位：分钟。 取值范围：15~14400，默认值为240。

4. 单击**保存**。

1.11.2. 开启双因子认证

登录堡垒机完成密码认证之后，您可以通过短信、邮件或钉钉工作消息通知发送动态验证码进行双因子认证，降低密码泄露风险。本文介绍如何开启双因子认证。

背景信息

- 堡垒机双因子认证功能仅针对堡垒机本地用户、AD认证用户和LDAP认证用户。
- 如果需要为RAM用户设置双因子认证，您可以登录RAM访问控制台，设置RAM用户的多因素认证MFA（Multi Factor Authentication）。具体操作，请参见为阿里云账号启用多因素认证。

前提条件

- 如果您需要启用短信认证，请确保已为需要进行运维操作的用户账号添加手机号，否则将无法接收到验证码。为用户添加手机号的具体操作，请参见修改用户信息。
- 如果您需要启用邮件认证，请确保已为需要进行运维操作的用户账号设置邮箱地址，否则将无法接收到验证码。为用户设置邮箱地址的具体操作，请参见修改用户信息。
- 如果您需要启用钉钉认证，请确保已符合以下要求：
  - 已为需要进行运维操作的用户账号添加手机号。为用户添加手机号的具体操作，请参见修改用户信息。
  - 钉钉管理员已创建企业内部应用，并且为应用开通**根据手机号姓名获取成员信息的接口访问权限**。
  - 已获取企业内部应用的**AppKey**、**AppSecret**、**AgentId**。

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，单击**系统设置**。
3. 在**系统设置**页面，单击**双因子认证**页签。
4. 打开**启用双因子认证**开关，设置认证信息，然后单击**保存**。

   如果**认证方式**选中**钉钉认证**，您需要输入企业内部应用的**AppKey**、**AppSecret**、**AgentId**。

1.11.3. 配置AD认证

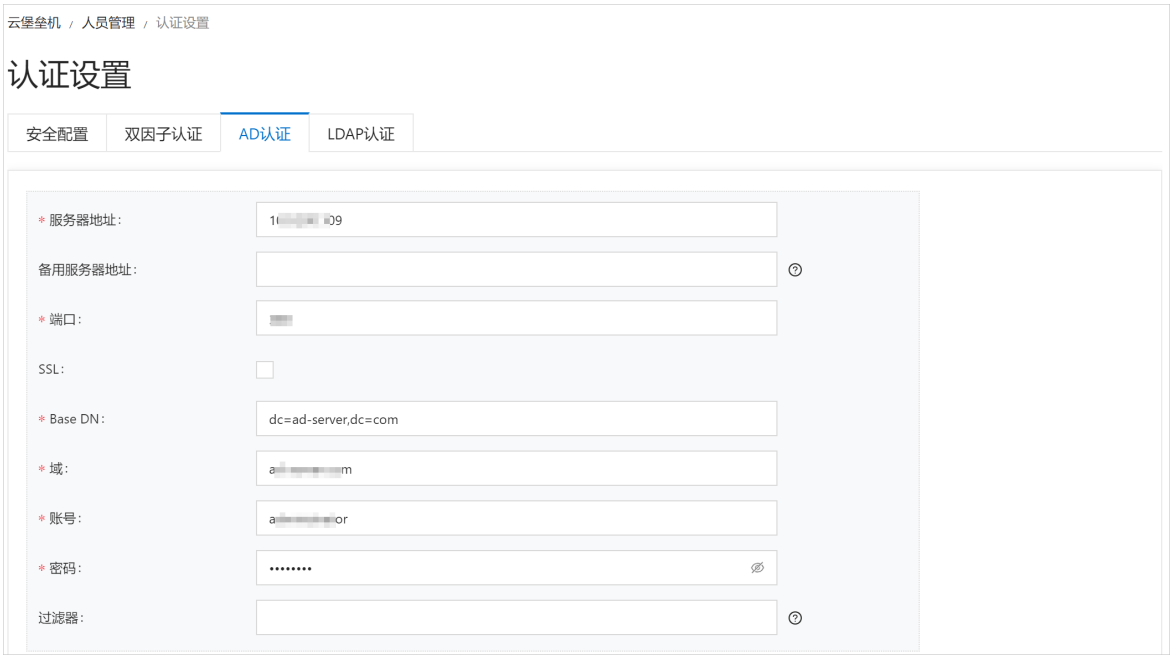
云盾堡垒机与AD服务器对接，可将AD服务器用户同步到堡垒机，作为堡垒机用户使用。同步AD服务器用户前，您需要在堡垒机控制台配置AD认证信息。本文介绍如何配置AD认证。

前提条件

配置AD认证前，您需要先部署好AD环境，并保证堡垒机可以正常访问AD服务器。

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，单击**系统设置**。
3. 在**系统设置**页面，单击**AD认证**页签。
4. 填写AD服务器地址、端口、Base DN、域名、账号、密码等信息。



5. 单击**测试连接**。
   测试连接成功时，会收到**AD认证连接测试成功**的提示信息。
6. 单击**更新配置**。

1.11.4. 配置LDAP认证

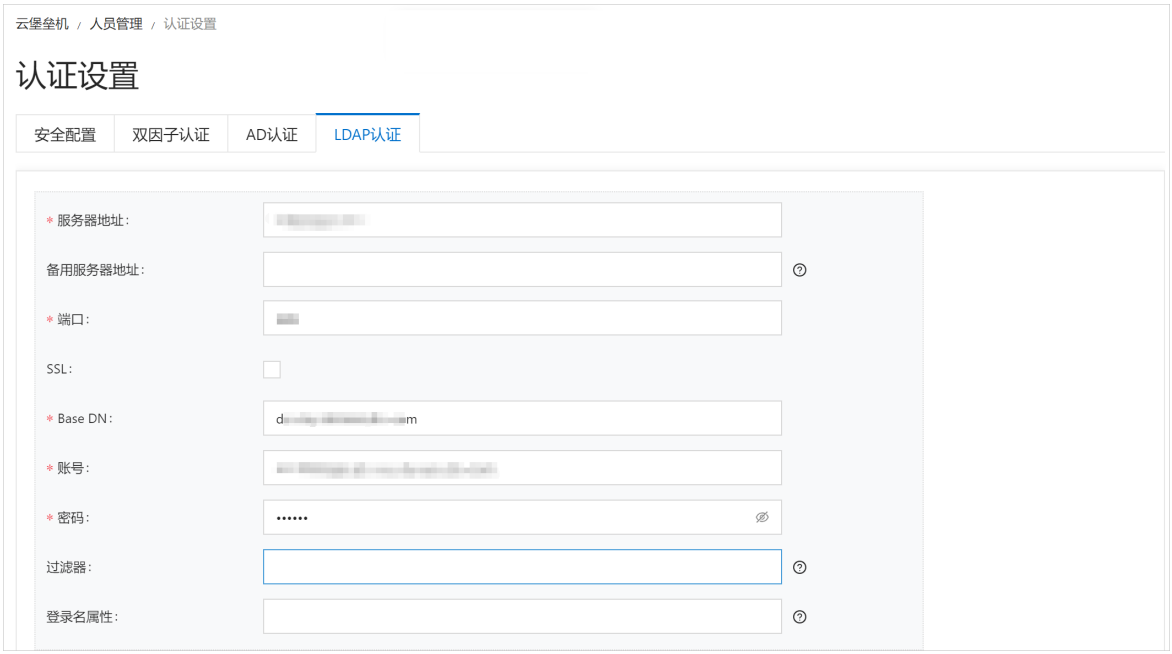
云盾堡垒机与LDAP服务器对接，可将LDAP服务器用户同步到堡垒机，作为堡垒机用户使用。同步LDAP服务器用户前，您需要在堡垒机控制台配置LDAP认证信息。本文介绍如何配置LDAP认证。

前提条件

配置LDAP认证前，您需要先部署好LDAP环境，并确保堡垒机可以正常访问LDAP服务器。

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，单击**系统设置**。
3. 在**系统设置**页面，单击**LDAP认证**页签。
4. 填写LDAP服务器地址、端口、Base DN、账号、密码等信息。



5. 单击**测试连接**。
   测试连接成功时，会收到**LDAP认证连接测试成功**的提示信息。
6. 单击**更新配置**。

1.11.5. 网络诊断

堡垒机系统设置页面为您提供了网络诊断功能，可以检测堡垒机到主机端口的网络是否连通。使用该功能可以帮助您确认网络的可达性，更高效地进行运维操作。本文介绍如何使用网络诊断功能。

背景信息

网络诊断功能支持检测IPv4地址和域名的连通性。

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，单击**系统设置**。
3. 在**系统设置**页面，单击**网络诊断**页签。
4. 输入**目标地址**和**端口**。

5. 单击**测试连接**。
   连通性测试成功时，您将收到**连通性测试成功**的提示。连通性测试失败时，您将收到**连通性测试失败**的提

示。排查和处理网络连接异常的方法请参见连接异常处理。

连接异常处理

网络连接测试失败时，您可以排查以下原因：

- 检查安全组规则是否允许堡垒机访问主机的端口。
- 检查主机是否已开启云防火墙，并且设置了允许堡垒机访问主机端口的访问策略。
- 检查主机是否已开启本地防火墙，并且设置了允许堡垒机访问主机端口的访问策略。

1.11.6. 运维配置

堡垒机提供运维配置功能，您可以更加精细化地配置运维条件，例如授权特殊用户访问主机账户、开启主机特殊配置，或者需要根据业务场景配置用户的运维总时长、运维空闲时长和阻断用户会话时长，避免主机资源浪费。本文介绍如何进行运维配置。

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，单击**系统设置**。
3. 在**系统设置**页面，单击**运维配置**页签。
4. 在**运维配置**区域，配置运维信息。

配置类型	配置项	说明
主机特殊账号	**允许用户使用堡垒机账户和密码访问主机**	设置是否允许用户使用堡垒机的账户和密码访问主机。 该配置适用于用户密码和主机密码同属AD、LDAP认证的场景。
	允许用户未授权主机账户访问主机	设置是否允许用户使用未授权主机账户访问主机。系统默认开启。 该配置只对用户未授权主机账户生效。 ○ 当用户未授权主机账户时，可使用empty账户，手动输入主机账户密码运维堡垒机。 ○ 当该配置关闭时，未授权主机账户的资产列表在运维时将不会显示。
主机特殊配置	**允许开启主机指纹**	系统默认开启。 主机指纹指堡垒机识别Linux主机的唯一标识，用于防止恶意用户通过重定向流量的方式获得未授权主机的访问权，不建议关闭主机配置。
	允许开启个性化桌面	系统默认关闭。 该配置只对Windows主机生效，勾选配置则允许用户使用Windows个性化桌面。 **说明** 个性化桌面会消耗大量带宽，请谨慎开启。

配置类型	配置项	说明
运维空闲时长限制		

配置类型	配置项	说明
运维总时长限制		

配置类型	配置项	说明

配置类型	配置项	说明
阻断会话抑制时长限制		

5. 配置完成后，单击**保存**。

1.11.7. 存储管理

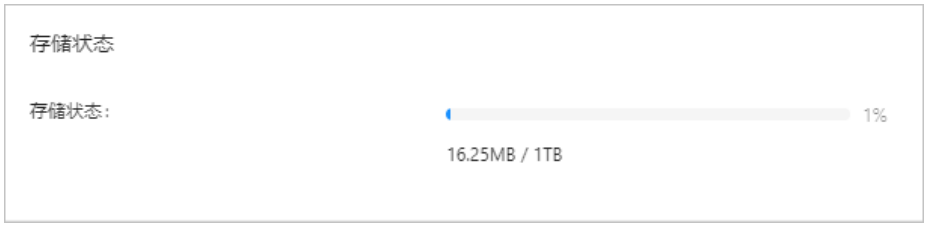
管理员可通过存储管理功能，查看审计会话数据的存储空间的使用情况，以及对存储时长进行配置。本文介绍如何使用存储管理功能。

背景信息

存储空间全部存满后，堡垒机会删除最早的审计会话数据。建议您根据业务需求，为审计会话数据设置合理的保存时长。

查看存储状态

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏，单击**系统设置**。
3. 在**系统设置**页面，单击**存储管理**页签。
4. 在**存储状态**区域，查看存储空间的使用情况。



设置自动删除会话数据

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，单击**系统设置**。
3. 在**自动删除**区域，选中**会话数据最大保存时长**复选框。

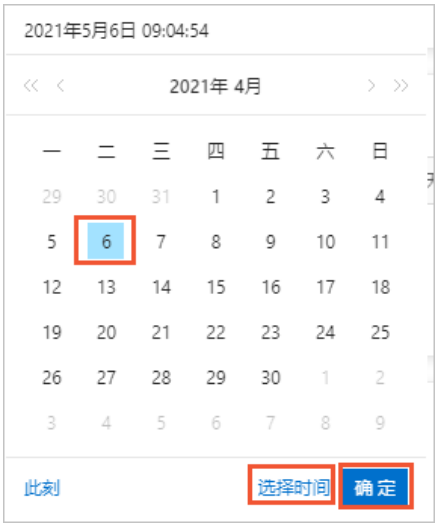
4. 单击**会话数据最大保存时长**后面的文本框，设置会话数据最大保存时长。

> **说明** 会话数据最大保存时长，有效值为1~9999，默认值为180天。当存储空间耗尽时，超过会话数据最大保存时长天数的数据将会被自动删除。
>
> - 如果删除数据后，剩余会话数据仍超过最大存储容量，堡垒机将自动删除最早的数据。
> - 如果没有开启自动删除规则，存储空间耗尽时，堡垒机将默认覆盖最早的数据。

5. 单击**保存**按钮。
   堡垒机将会按照您设置的会话数据最大保存时长，自动处理审计会话数据。

手动删除会话数据

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，单击**系统设置**。
3. 在**手动删除**区域，单击**请选择日期**文本框。
4. 在日历中，选择您要设置日期和时间，然后单击**确定**。



5. 单击**删除**按钮。
   堡垒机会根据您设置的时间点，删除该时间点之前的审计会话数据。

1.11.8. 消息通知

堡垒机提供消息通知功能，以站内信的形式发送消息通知，以便您及时了解业务情况，提高运维效率。消息通知功能支持的通知类型有命令告警通知、存储告警通知、自动化任务通知、运维报表通知、共享密钥到期提醒通知和网络域代理告警通知。本文介绍如何使用消息通知功能。

操作步骤

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏，单击**系统设置**。
3. 在**系统设置**页面，单击**消息通知**页签，然后在**消息通知**区域，进行以下配置。

> **说明** 消息通知中的配置项默认为关闭状态，需要您勾选或配置后，堡垒机才会以站内信的形式发送相关消息通知。

配置项	说明
命令告警通知	用户在运维时，如果触发了命令审批、命令阻断等控制策略，堡垒机会发送站内信通知。
存储告警通知	当存储容量即将耗尽（已消耗了85%的存储容量）时，堡垒机会通过站内信发送通知。 **说明** 存储剩余容量不增加的情况下，只发送一次通知。

配置项	说明
自动化任务通知	当自动改密任务执行完成后，堡垒机将通过站内信发送通知。 **说明** 在堡垒机中创建自动改密任务后，堡垒机会按照配置的密码策略周期或定时执行改密任务。堡垒机的改密任务功能可帮助您在满足等保合规要求的同时，避免定期人工维护主机账号密码轮转容易出错的问题。了解如何设置自动改密任务，请参见改密任务。
运维报表通知	堡垒机每周一的10:00-11:00期间，将通过站内信发送上一周的运维报表。
共享密钥到期提醒，到期提示时间	如果堡垒机管理员设置了共享密钥到期提醒时间，共享密钥即将到期前，堡垒机将通过站内信发送改密提醒通知。 **说明** 在堡垒机中创建共享密钥并将共享密钥关联到多个主机账户后，运维主机时，优先使用共享密钥登录，可以提高管理主机账户的效率。了解如何设置共享密钥，请参见密钥管理。
网络域代理告警通知	当网络域代理服务异常时，堡垒机将通过站内信发送通知。 **说明** 在堡垒机中创建网络域且使用代理的连接方式来添加代理服务器后，堡垒机会每五分钟检测一次代理服务器的连通性。有关创建代理网络域的详细信息，请参见网络域。

4. 单击**保存**。
   堡垒机将以站内信的形式，为您发送已配置的消息通知。您可以单击页面右上角的图标，进入**消息中心**页面查看消息通知。

1.11.9. 配置备份

堡垒机提供配置备份功能。配置备份功能可将堡垒机的现有配置快速复制到新购买的堡垒机中，为您免去重复的配置工作。本文介绍如何使用配置备份功能。

限制条件

- 支持低规格堡垒机实例的配置备份导入同规格或高规格堡垒机实例。例如，您可以将50资产的堡垒机实例的配置备份导入200资产的堡垒机实例，反之则不支持。
- 支持同版本实例的配置备份相互导入，如将基础版堡垒机实例的配置备份导入其他基础版实例。
- 支持低版本实例的配置备份导入高版本的实例，如将基础版堡垒机实例的配置备份导入高可用版堡垒机实例。
- 不支持将高可用版的配置备份导入到基础版。
- 改密任务的配置不支持导出，您需要在新够的堡垒机上重新配置改密任务。请您将旧堡垒机上的改密任务终止，妥善保管改密任务修改后的资产密码。

流程说明

当您新购堡垒机实例后，您可以将已有堡垒机的配置通过配置备份功能导出到本地，然后上传到新购的堡垒机中。导入配置备份数据总流程如下：

1. 为已有的堡垒机创建配置备份，导出配置备份。具体操作，请参见创建配置备份。
2. 将导出的配置备份上传到新购买的堡垒机实例中。具体操作，请参见上传配置备份。

创建配置备份

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏单击**系统设置**。
3. 在**系统设置**页面，单击**配置备份**页签。
4. 在**配置备份**页签下，单击**创建配置备份**。

   堡垒机的配置备份会以BH文件格式下载到本地。

上传配置备份

> **注意** 已有堡垒机的配置备份导入到新够的堡垒机后，您在新够的堡垒机上的配置将会被覆盖，请您谨慎操作。

1. 登录云盾堡垒机控制台。
2. 在左侧导航栏单击**系统设置**。
3. 在**系统设置**页面，单击**配置备份**页签。
4. 在**配置备份**页签下，单击**上传配置备份**。

   备份上传成功后，您可以在新购的堡垒机中查看并验证相关配置是否上传成功。

1.11.10. 管理第三方资产源

在堡垒机上维护第三方资产源信息后，堡垒机可以调用第三方接口获取该资产源账号下的主机列表，您可以将第三方资产源的主机导入第堡垒机进行运维管理。本文介绍如何管理第三方资产源。

前提条件

- 第三方厂商已创建资产源，并且已在资产源中添加主机。
- 您已经获取第三方资产源的访问凭证（Access Key ID、Secret Access Key），并且访问凭证已开通读取主机信息相关权限。具体操作，请查阅对应厂商的官方文档。

> **说明** 目前仅支持对接部分第三方厂商资产源，您可以提交工单咨询支持对接的厂商信息。

新建第三方资产源

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，单击**系统设置**。
3. 在**系统设置**页面，单击**第三方资产源**页签。
4. 在**第三方资产源**页签，单击**新建第三方资产源**。
5. 在**新建第三方资产源**面板，配置第三方资产源信息，然后单击**新建**。

配置项	说明
资产源名称	自定义资产源名称。 名称长度为1~128个字符，可以包含中英文字符、数字、半角句号（.）、下划线（_）、短划线（-）、反斜线（\）和空格，并且名称不能以特殊字符开头。

配置项	说明
资产源提供商	选择资产源所属的厂商。
Access Key ID	输入已获取的第三方资产源的Access Key ID。
Secret Access Key	输入已获取的第三方资产源的Secret Access Key。

后续操作

新建第三方资产源后，您可以导入第三方资产源下的主机，具体操作，请参见导入第三方资产源。

相关操作

- 同步第三方资产源：当第三方资产源更新时，您可以通过同步第三方资产源获取最新的主机信息。

  在**第三方资产源**页签，找到目标资产源，在**操作**列单击**同步**。
- 编辑第三方资产源信息：您可以修改第三方资产源的名称、提供商、Access Key ID和Secret Access Key。

  在**第三方资产源**页签的第三方资产源列表中，单击目标资产源名称，在**编辑第三方资产源**面板修改信息后，单击**编辑**。
- 删除第三方资产源：您可以删除不再使用的第三方资产源。

  在**第三方资产源**页签的第三方资产源列表中，找到目标资产源，在**操作**列单击**删除**后，在弹出的对话框中再次单击**删除**。

> **注意** 删除第三方资产源前，请确保已在堡垒机中删除该资产源下的所有主机，否则将无法删除第三方资产源。删除主机的具体操作，请参见删除主机。

2.运维使用手册

2.1. 运维概述

运维使用手册从运维人员的角度，介绍堡垒机支持的运维方式以及如何使用堡垒机运维服务器。堡垒机支持两种运维方式，分别为客户端运维和Web端运维。在日常的运维工作中，运维员可根据自己的实际情况，选择合适的运维方式运维服务器。

Web端运维

堡垒机支持Web端运维。您无需下载运维客户端软件，通过堡垒机控制台提供的主机运维功能，在Web端直接登录服务器进行运维。具体操作，请参见主机运维。

客户端运维

您可以根据您使用的电脑的操作系统，下载对应的运维客户端软件后，登录堡垒机运维服务器。

Windows客户端运维

- SSH协议运维
- RDP协议运维
- SFTP协议运维

Mac客户端运维

- SSH协议运维
- RDP协议运维
- SFTP协议运维

2.2. Windows客户端运维

2.2.1. SSH协议运维

运维人员需要通过本地的SSH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。本文以Xshell工具为例，介绍SSH协议的运维登录流程。

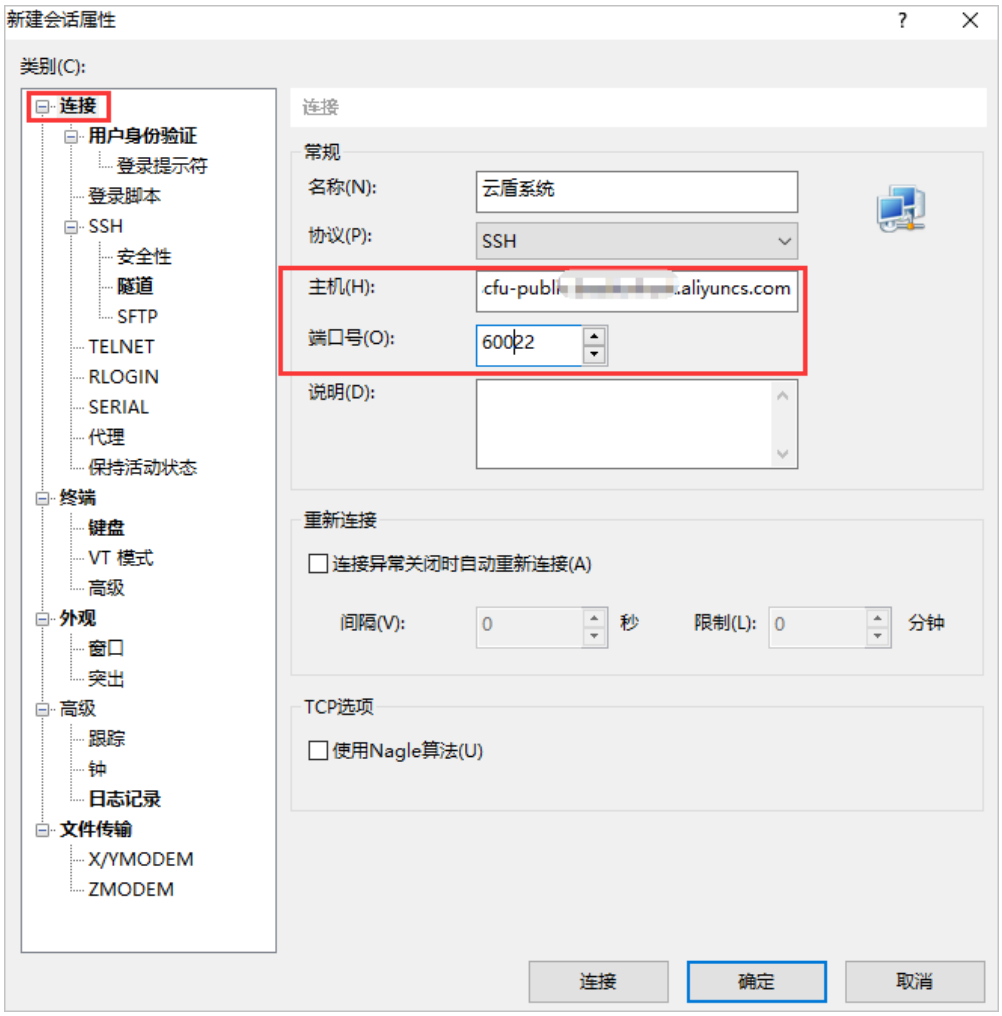
前提条件

- 请确认在本地主机已安装支持SSH协议的运维工具，例如： Xshell、SecureCRT、PuTTY等。
- 已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。

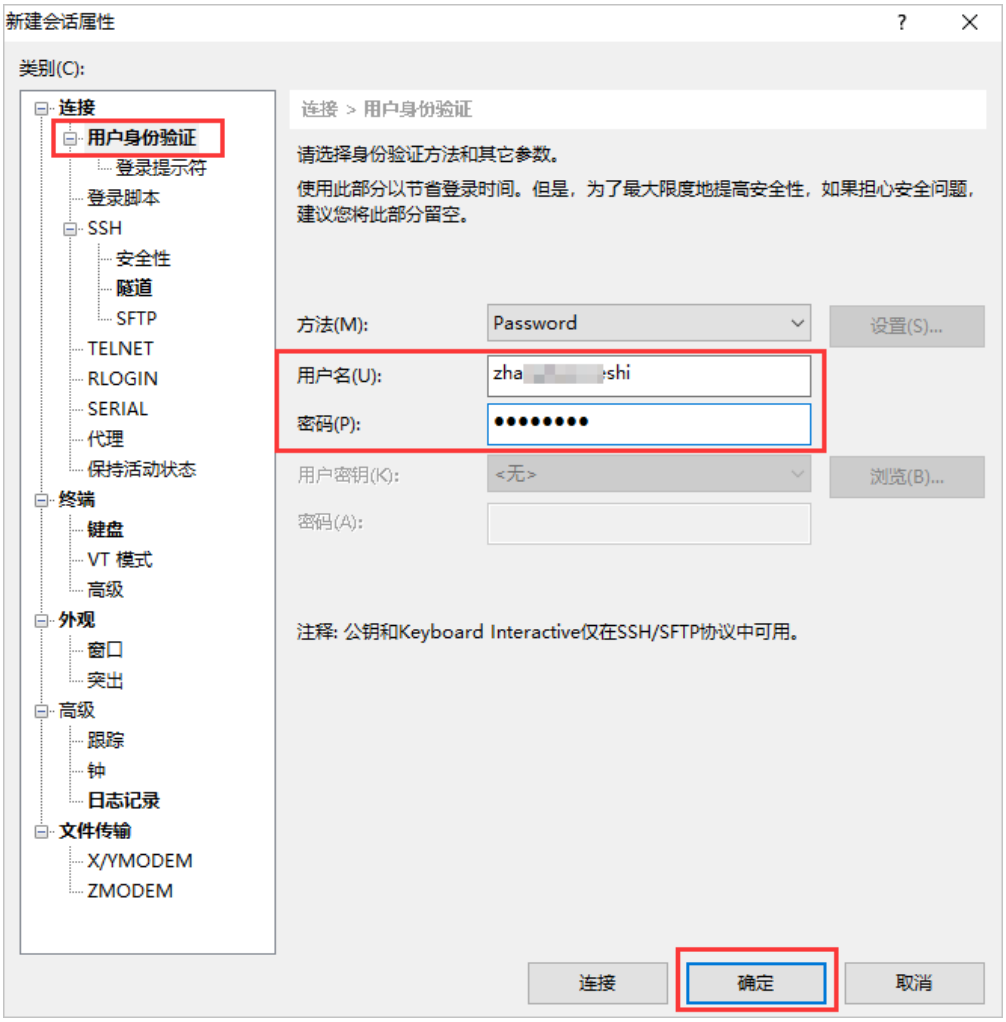
操作步骤

1. 打开Xshell工具，在**连接**设置中输入云盾堡垒机的运维地址和SSH端口号。

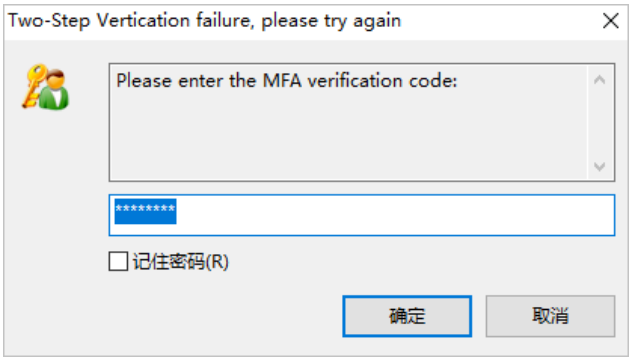
   SSH端口号默认为**60022**。



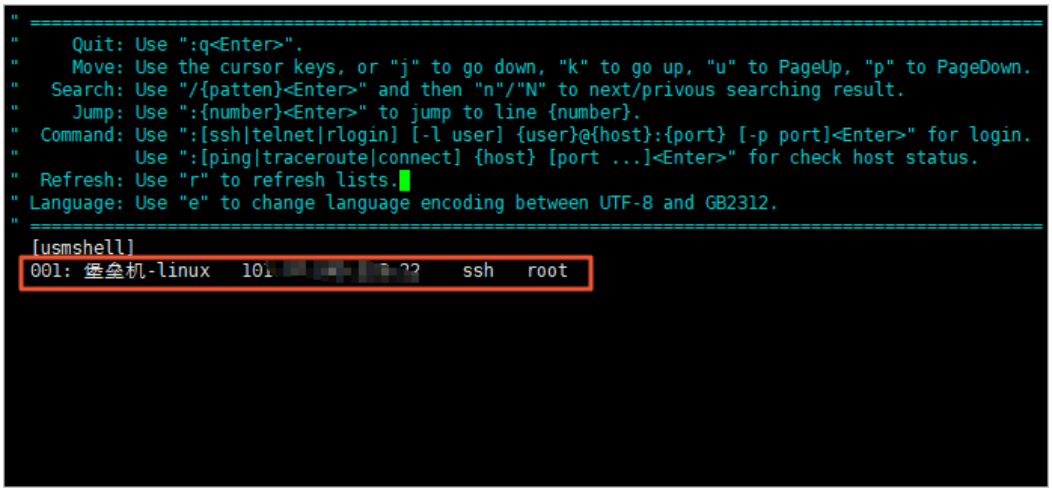
2. 在**用户身份验证**设置中输入云盾堡垒机的用户名和密码并单击**确定**。



3. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，单击**确定**。



4. 在资产管理界面，通过键盘上的上、下方向键选择您想要进行运维的服务器主机，按回车键（Enter），即可登录目标服务器主机进行运维操作。

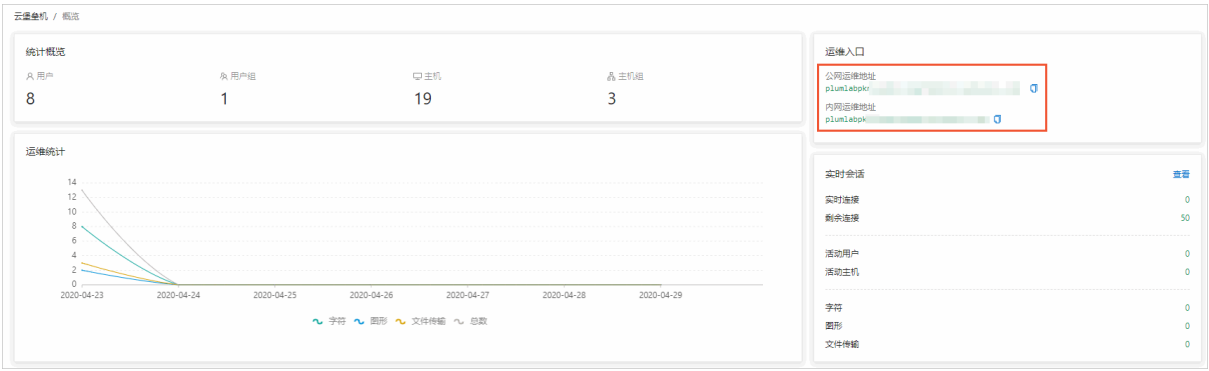


2.2.2. RDP协议运维

运维人员需要通过本地的RDP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。本章节以Windows系统自带的远程桌面连接工具（Mstsc）为例，介绍RDP协议的运维登录流程。

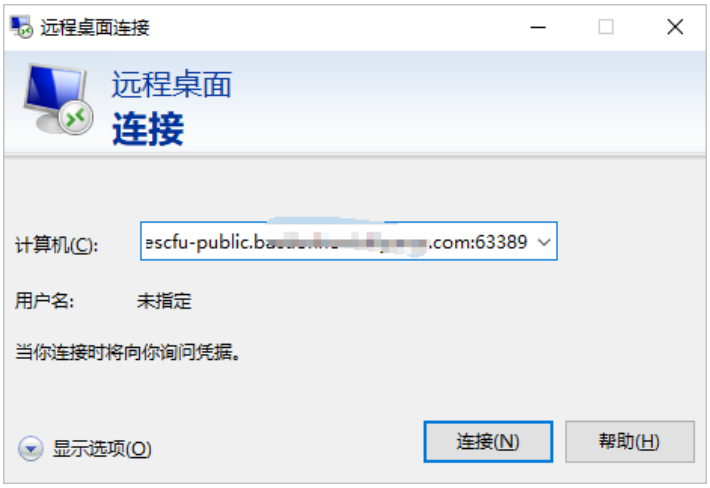
前提条件

已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。



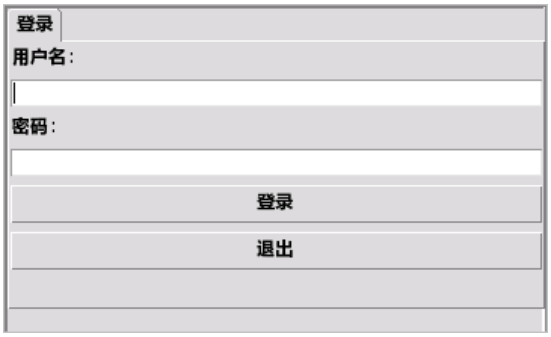
操作步骤

1. 在本地Windows系统主机中打开远程桌面连接工具（Mstsc）。
2. 输入 `<云盾堡垒机运维地址>:63389` ，并单击**连接**。



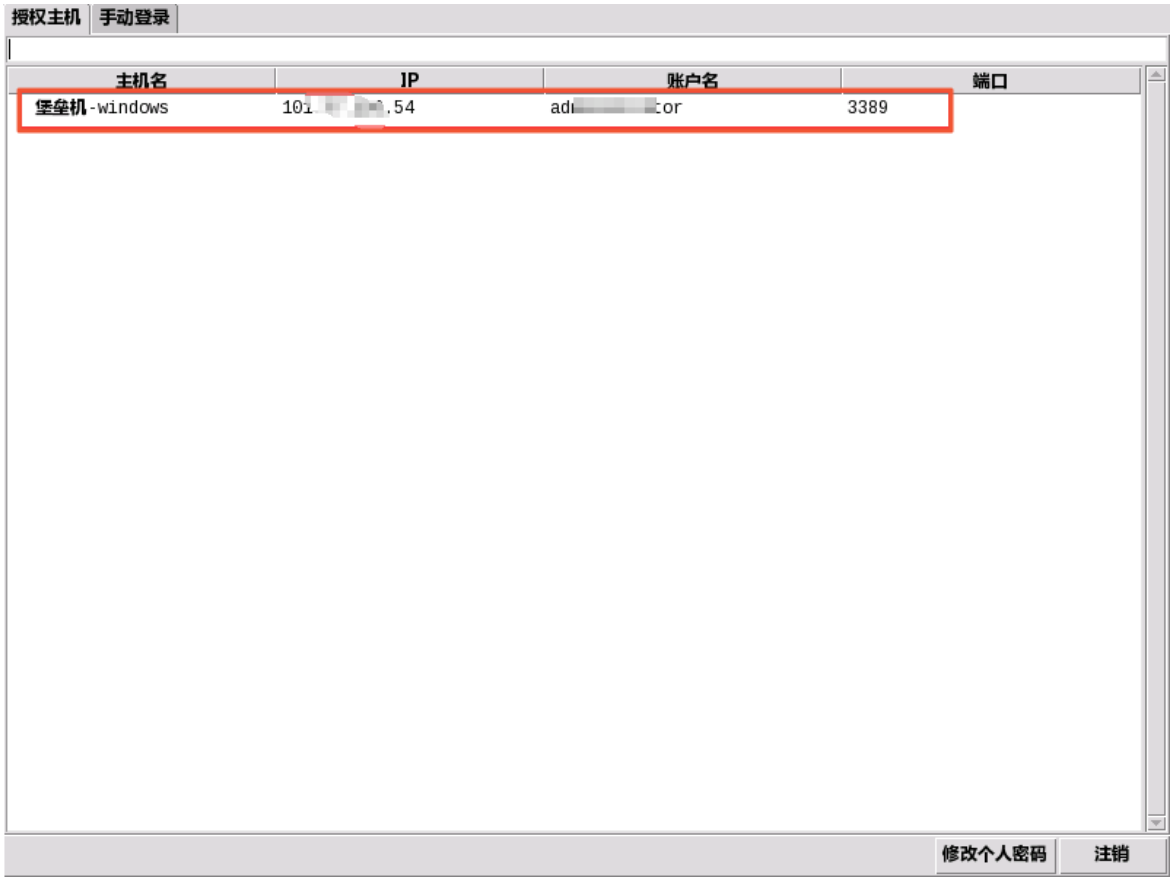
3. 在**远程桌面连接**提示框中，单击**是**。

4. 输入云盾堡垒机的用户名和密码，单击**登录**。



5. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，单击**确认**。

6. 在资产管理界面，双击您需要登录的已授权服务器主机，登录目标主机。



2.2.3. SFTP协议运维

运维人员需要通过本地的SFTP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。本章节以Xftp为例，介绍SFTP协议的运维登录流程。

前提条件

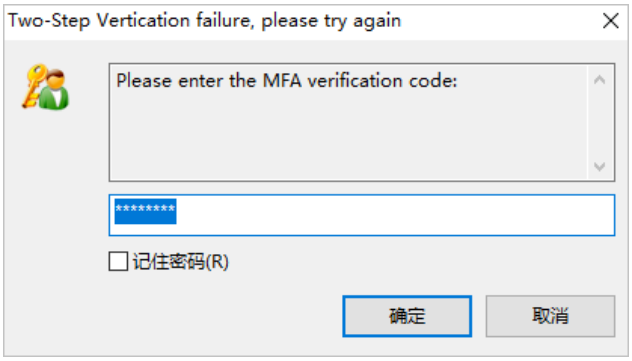
- 请确认在本地主机已安装支持SFTP协议的运维工具，如：Xftp、WinSCP等。

- 已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。

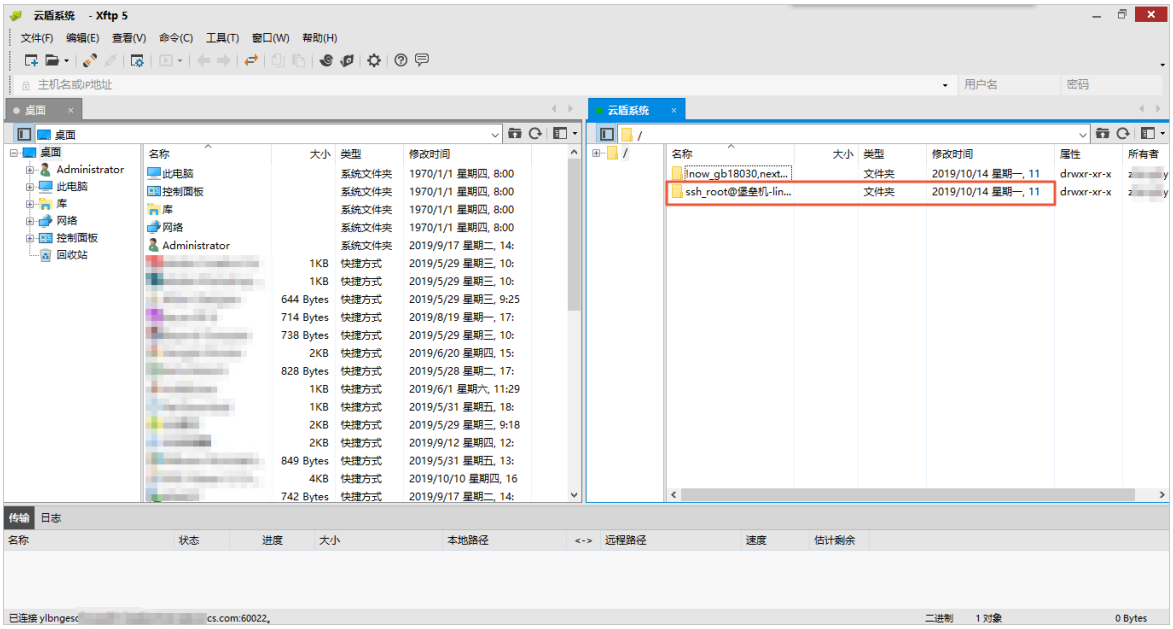
操作步骤

1. 打开Xftp工具，在登录窗口中输入云盾系统的运维地址、默认端口号60022、用户名和密码，并单击**确定**连接到云盾堡垒机。

2. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，单击**确定**。

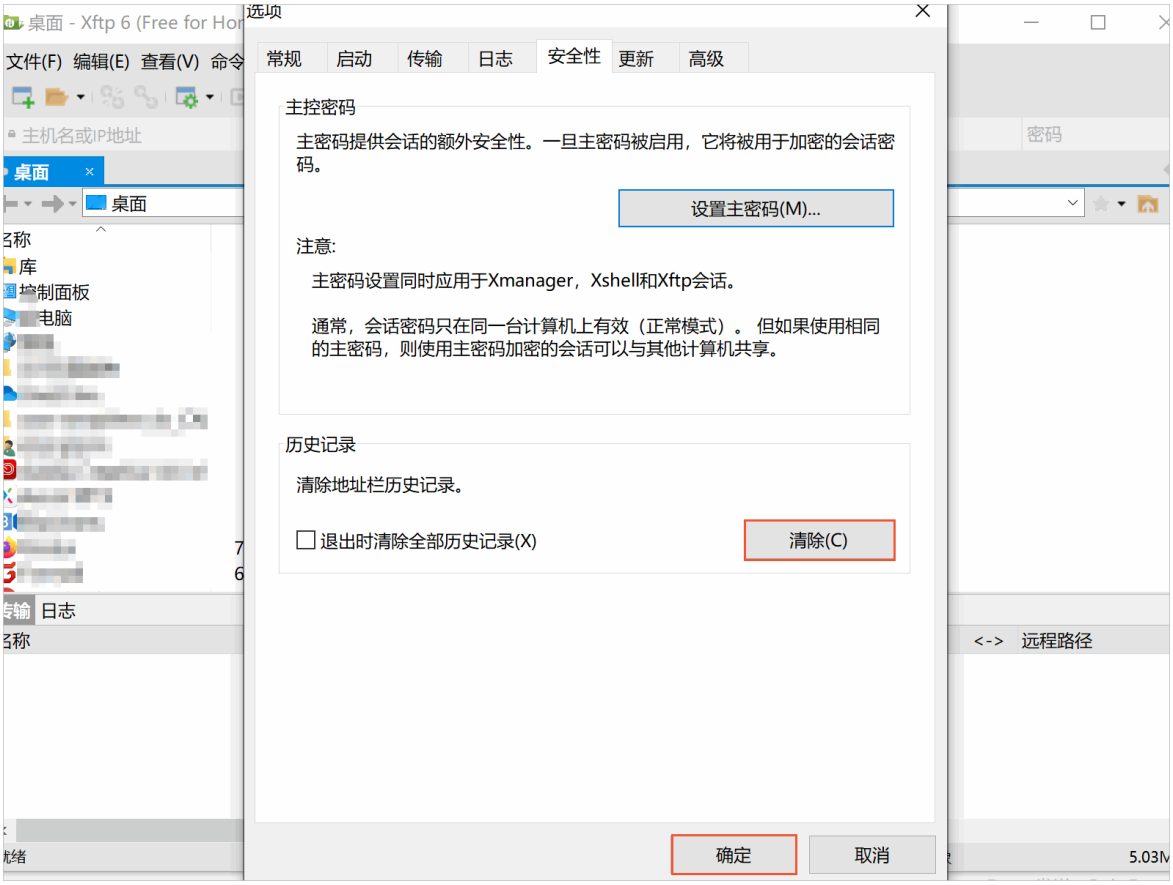


3. 成功登录云盾堡垒机后，在右侧可以查看已授权的服务器主机列表。



4. 双击需要运维的服务器主机，进入该服务器主机的目录，即可进行文件传输操作。

> **说明** 如果您无法进入服务器主机的目录，可尝试以下方法解决该问题：
>
> - 检查该主机的账户密码是否托管在堡垒机中。如果在堡垒机中未配置该主机的账户密码，请您配置该主机的账户密码。更多信息请参见新建主机账户。
> - 检查目录名称是否乱码。如果目录名称出现乱码，您可以双击转码目录并忽略报错信息，再右键选择刷新，进行转码。
> - 清理客户端的缓存。以Xftp 6为例，您可以在顶部菜单栏单击**选项**并选择**安全性**页签，在**历史记录**区域，单击**清除**。
>
> 如果以上方法都未解决您的问题，请您提交工单联系阿里云。



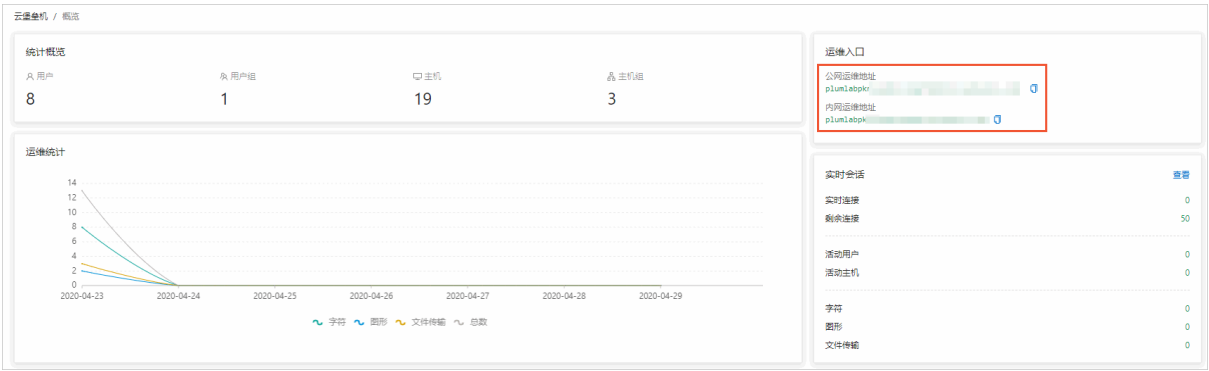
2.3. Mac客户端运维

2.3.1. SSH协议运维

运维人员需要通过SSH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。本章节以命令行终端工具为例，介绍SSH协议的运维登录流程。

前提条件

已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。



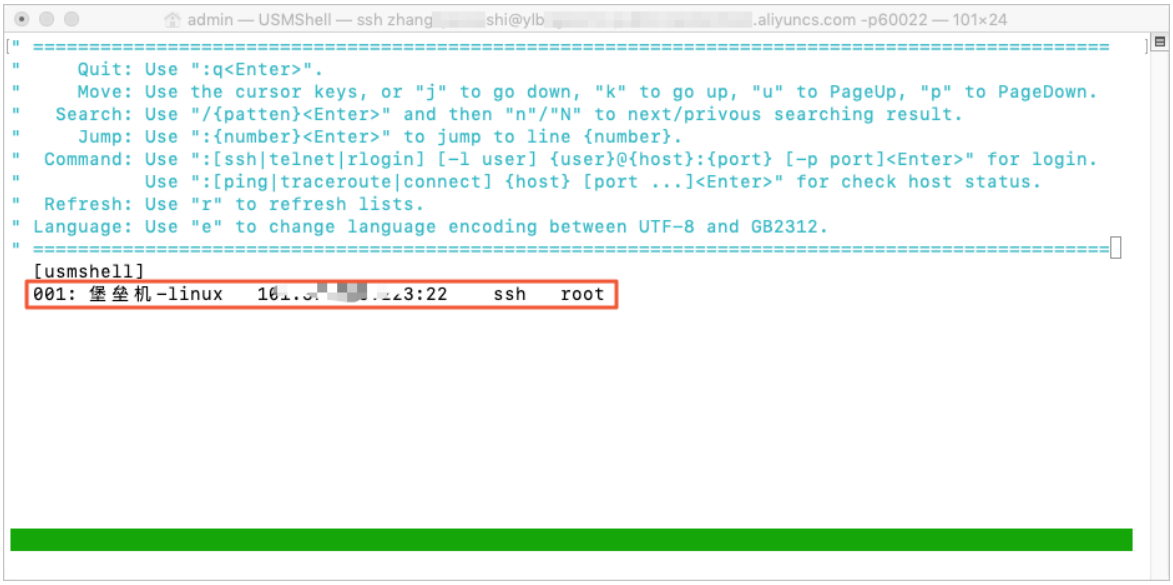
操作步骤

1. 打开命令行终端工具。

2. 输入登录堡垒机命令 `ssh <云盾堡垒机用户名>@<云盾堡垒机运维地址> -p60022` ，按回车键（Enter）。

3. 输入RAM用户的密码，按回车键（Enter）。
4. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，按回车键（Enter）。

5. 在资产管理界面，通过键盘上的上、下方向键选择您想要进行运维的服务器主机，按回车键（Enter），即可登录目标服务器主机进行运维操作。



2.3.2. RDP协议运维

运维人员需要通过本地的RDP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。本章节以Microsoft Remote Desktop工具为例，介绍RDP协议的运维登录流程。

前提条件

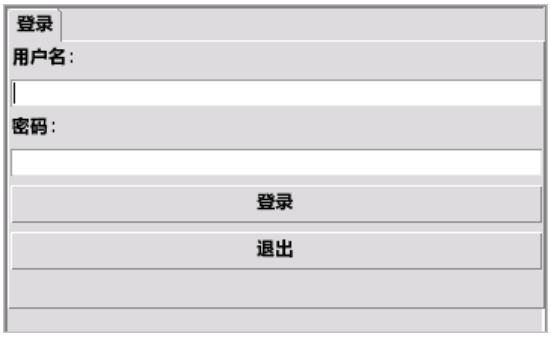
- 请确认已从应用商店安装RDP客户端，例如Microsoft Remote Desktop工具。

- 已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。

操作步骤

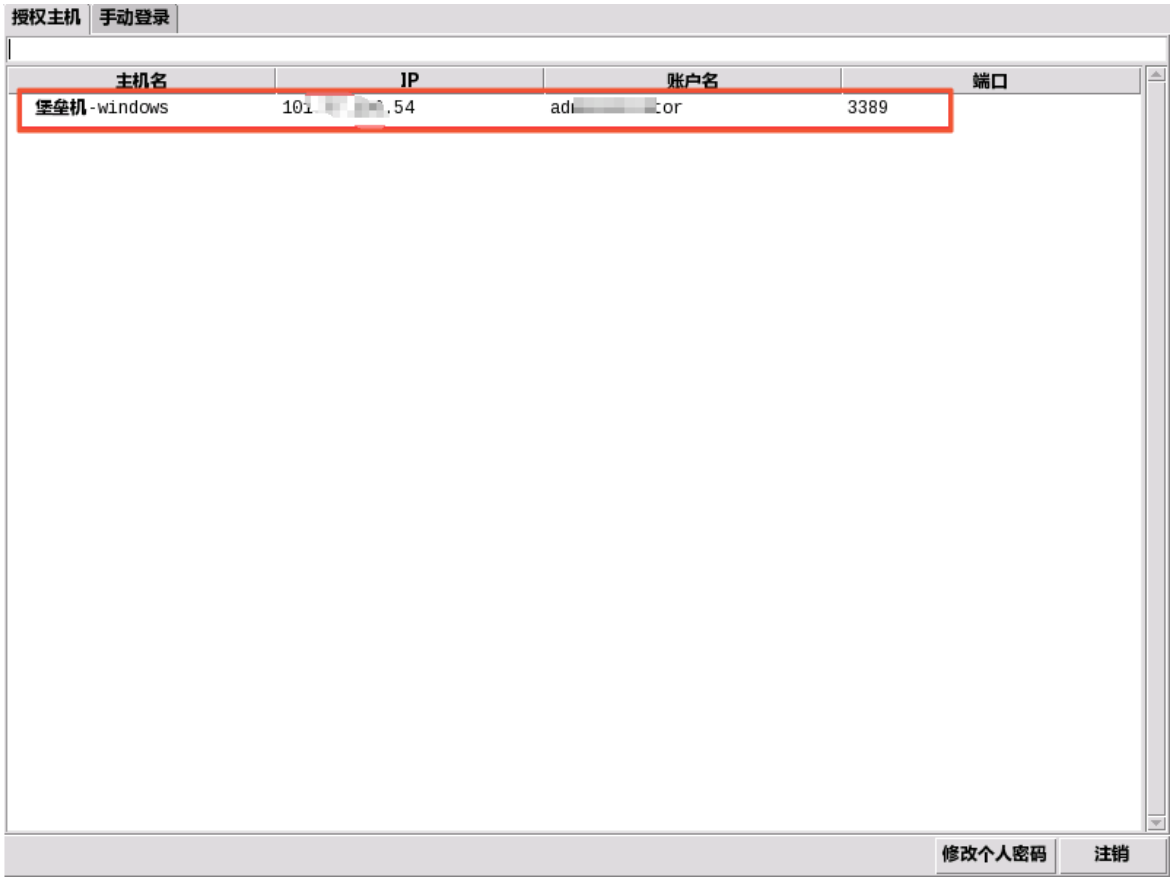
1. 打开Microsoft Remote Desktop工具。
2. 输入 `<云盾堡垒机运维地址>:63389` ，单击**连接**。

3. 输入云盾堡垒机的用户名和密码，单击**登录**。



4. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，单击**确认**。

5. 在资产管理界面，双击您需要登录的已授权服务器主机，登录目标主机。

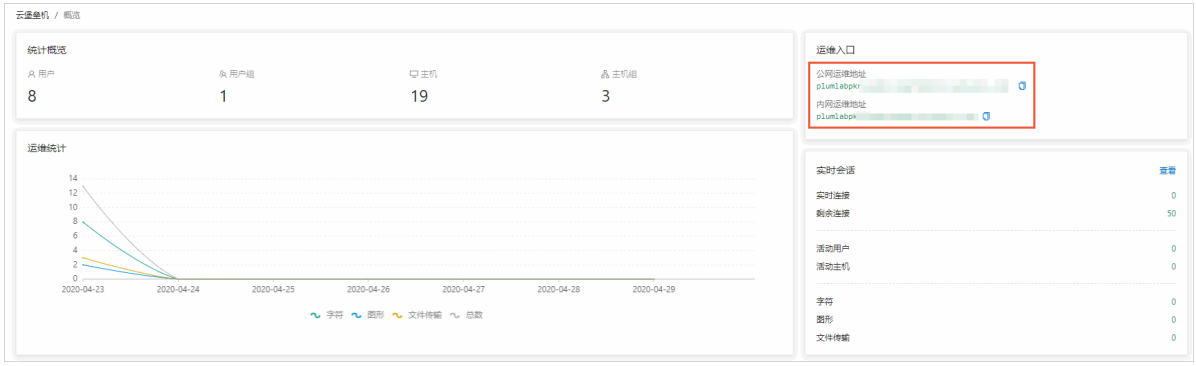


2.3.3. SFTP协议运维

运维人员需要通过本地的SFTP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。本章节以SecureFX为例，介绍SFTP协议的运维登录流程。

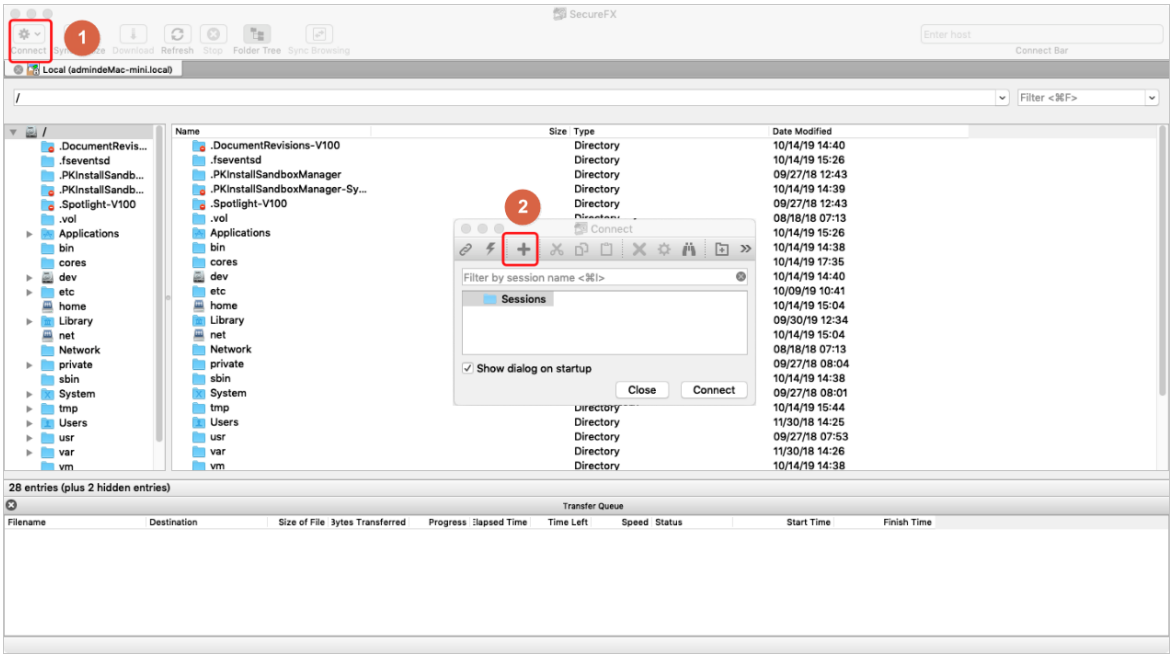
前提条件

- 请确认在本地主机已安装支持SFTP协议的运维工具，如：SecureFX等。
- 已获取堡垒机运维地址。您可以在堡垒机**概览**页面的**运维入口**区域获取运维地址。如何获取请参见登录堡垒机系统。

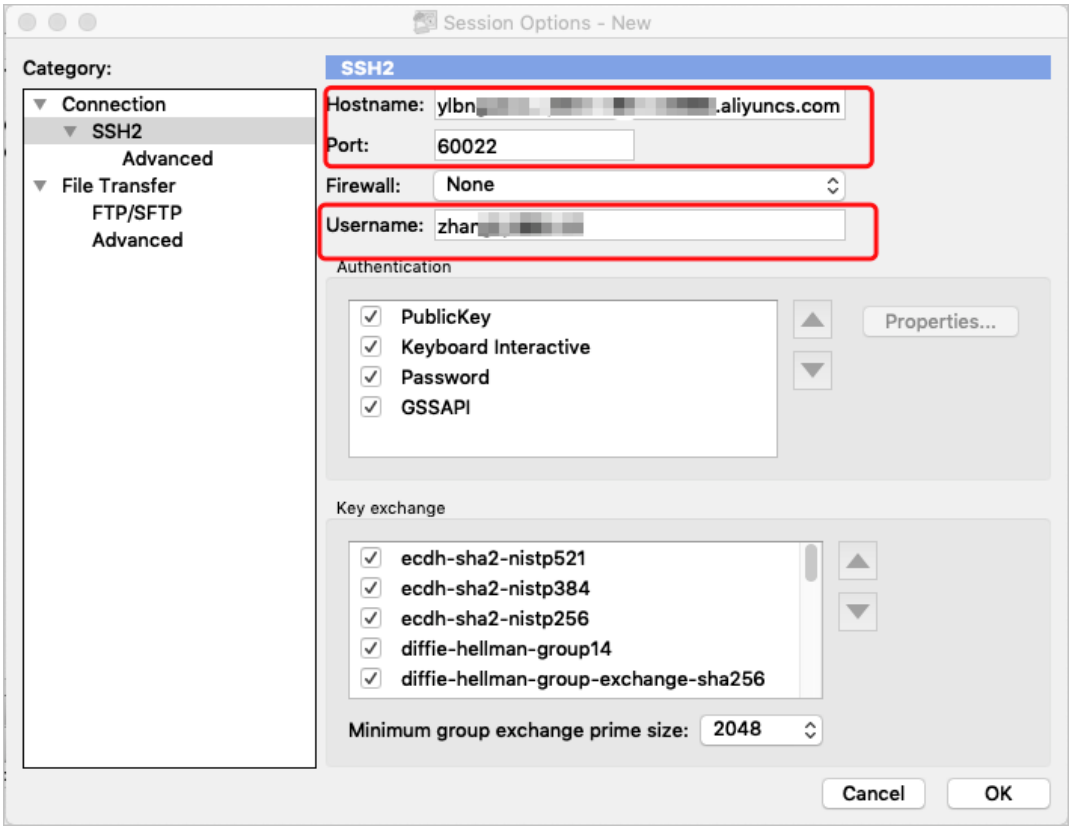


操作步骤

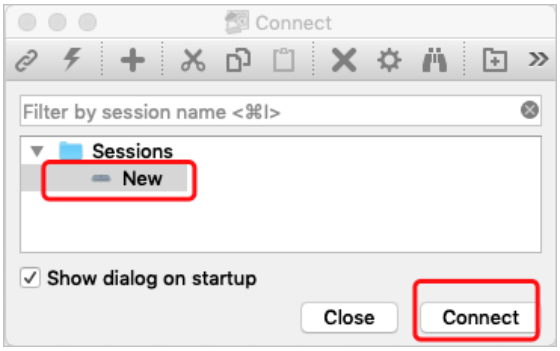
1. 打开SecureFX工具。
2. 单击左上角的**Connect**，在对话框中单击 + 图标。



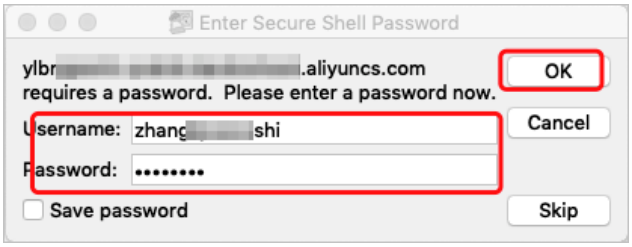
3. 输入堡垒机的运维地址、端口号（60022）和用户名，单击**OK**。



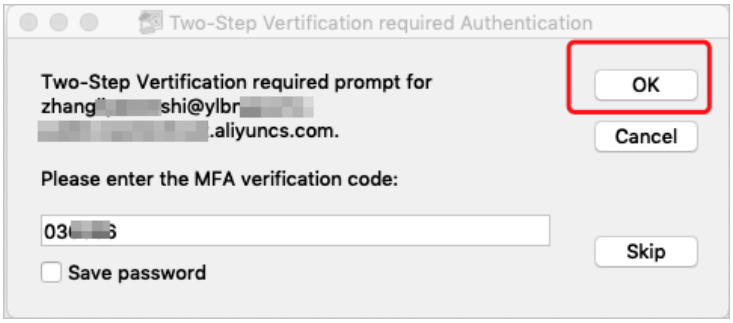
4. 选择刚刚新建的堡垒机，单击**Connect**。



5. 输入RAM用户名和密码，单击**OK**。

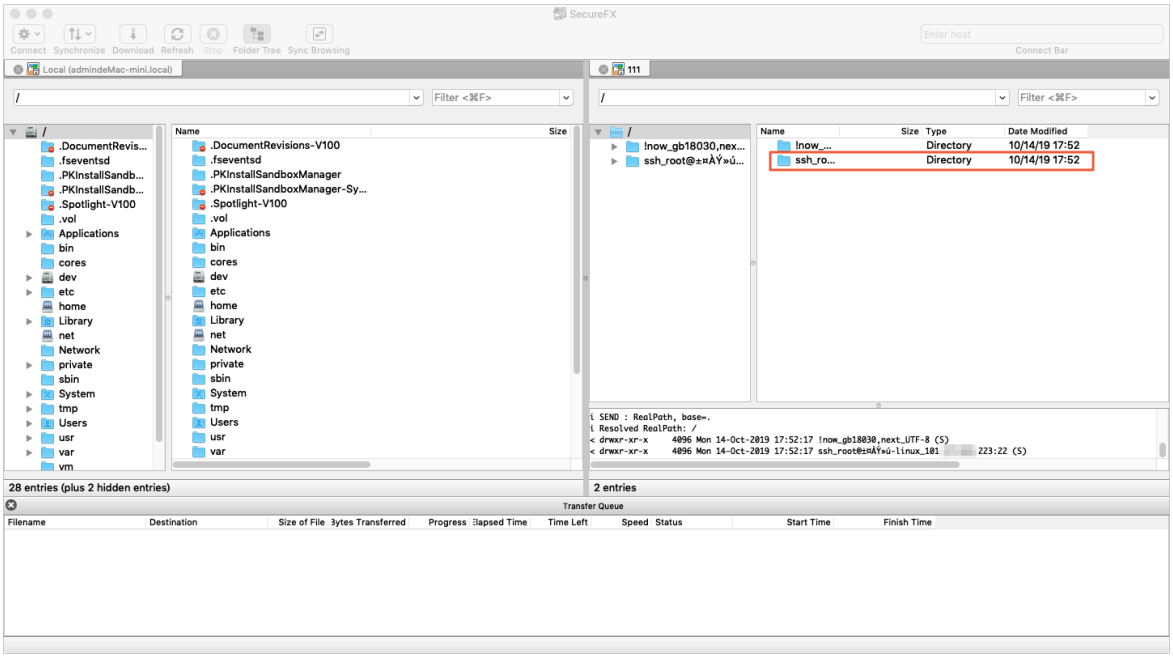


6. （可选）如果RAM用户开启了MFA二次验证，需要输入从已绑定的MFA设备（即阿里云App）中获取的安全码，单击**OK**。



7. 登录成功后，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** 如果您无法进入服务器主机的目录，可尝试以下方法解决该问题：
>
> - 检查该主机的账户密码是否托管在堡垒机中。如果在堡垒机中未配置该主机的账户密码，请您配置该主机的账户密码。更多信息请参见新建主机账户。
> - 检查目录名称是否乱码。如果目录名称出现乱码，您可以双击转码目录并忽略报错信息，再右键选择刷新，进行转码。
> - 清理登录客户端的缓存。
>
> 如果以上方法都未解决您的问题，请您提交工单联系阿里云。


SecureFX
Connect
Synchronize
Download
Refresh
Stop
Folder Tree
Sync Browsing
Enter host
Connect Bar
Local (admindeMac-mini.local)
111
Filter <⌘F>
Name
Size
Type
Date Modified
.DocumentRevisions-V100
.fseventsd
.PKInstallSandboxManager
.PKInstallSandboxManager-Sy...
.Spotlight-V100
.vol
Applications
bin
cores
dev
etc
home
Library
net
Network
private
sbin
System
tmp
Users
usr
var
!now_gb18030,nex...
ssh_root@±ÀÝ»ú...
!now_...
ssh_ro...
Directory
10/14/19 17:52
i SEND : RealPath, base=.
i Resolved RealPath: /
< drwxr-xr-x 4096 Mon 14-Oct-2019 17:52:17 !now_gb18030,next_UTF-8 (S)
< drwxr-xr-x 4096 Mon 14-Oct-2019 17:52:17 ssh_root@±ÀÝ»ú-linux_101 223:22 (S)
28 entries (plus 2 hidden entries)
2 entries
Transfer Queue
Filename
Destination
Size of File
Bytes Transferred
Progress
Elapsed Time
Time Left
Speed
Status
Start Time
Finish Time