ALIBABA CLOUD

阿里云

堡垒机

用户指南（V3.2版本）

文档版本：20201014

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. 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。
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。

1.2. 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。本文档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。
- 您使用的是阿里云主账号或拥有创建和删除服务关联角色权限的RAM账号。

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**删除RAM角色**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"
}
```

1.3. 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。

   编辑标签
3. 在标签设置页面，为实例添加或删除标签。

   添加标签

   - **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**确定**。

- **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。

  删除标签

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。

搜索标签

1.4. 主机管理

1.4.1. 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操作，在堡垒机中新建需要维护的主机。新建主机后，运维人员才可以通过堡垒机对该主机进行运维管理。

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. 在左侧导航栏单击**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**。

导入其他来源主机

您也可以通过**新建主机**、**导入RDS专有主机组**或**从文件导入主机**将需要运维管理的主机导入到堡垒机中，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. 在左侧导航栏单击**资产管理 > 主机**。
3. 在**导入其他来源主机**列表选择**新建主机**、**导入RDS专有主机组**或**从文件导入主机**中的一种方式导入主机。

   以下是**导入其他来源主机**支持的三种导入方式：

   - **新建主机**

     通过**新建主机**方式您可以手动添加主机。单击**新建主机**并填写主机的相关信息，包括操作系统类型、主机IP、主机名、主机组和备注信息。

   - **导入RDS专有主机组**

     通过**导入RDS专有主机组**方式您可以批量导入RDS专有主机组。单击**导入RDS专有主机组**。在**导入RDS专有主机组**对话框中选中需要导入的主机并单击**导入**。更多信息请参见通过堡垒机访问主机。

     > **说明** RDS专有主机组产品名称变更为云数据库专属集群MyBase。

   - **从文件导入主机**

     通过**从文件导入主机**方式您可以批量将主机导入堡垒机。单击**从文件导入主机**。在**导入主机**页面，单击**下载主机模板文件**并按照模板的要求完成主机信息的填写。完成填写后单击**点击上传**将主机信息导入。在**主机导入预览**页面选中需要导入的主机并单击**导入**。在**导入主机**页面单击**导入主机**批量将主机导入堡垒机。

     > **说明** 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。

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，具体请参见修改主机的服务端口。

1.4.2. 管理主机

如果堡垒机主机列表中的主机信息需要进行变更或主机不需要维护了，您可以修改主机信息或直接删除主机。本文介绍如何搜索主机、修改主机基本信息和管理主机。

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。

背景信息

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. 在左侧导航栏单击**资产管理 > 主机**。
3. 在**主机**页面，设置需要查看的主机的搜索条件。

   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. 在左侧导航栏单击**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。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。
4. 修改主机的**操作系统**、**主机IP**、**主机名称**、**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. 在左侧导航栏单击**资产管理 > 主机**。
3. 在**主机**页面，选中需要删除的主机并单击**删除**。

   > **说明** 如果只需要删除单个主机，您可以直接在**操作**列中单击**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。

1.4.3. 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. 在左侧导航栏单击**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. 在左侧导航栏单击**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**。

1.4.4. 新建主机账户

堡垒机需要使用对应的账户登录到需要进行运维的主机，本文档介绍如何在堡垒机中新建主机账户。

操作步骤

> **说明** 新建主机账户是指将您主机系统内存在的账号配置到堡垒机中，以便运维人员使用堡垒机登录主机。在堡垒机中新建的主机账号不会自动同步到您的主机系统内。

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**资产管理 > 主机**。
3. 在**主机**页面，定位到需要添加账户的主机并单击主机名称。
4. 单击**主机账户**页签。
5. 单击**新建主机账户**。

   新建主机账户

   如果需要为多个主机批量新建相同的账户，您可以选中需要批量添加账户的主机并在**批量**列表中单击**批量 > 新增账户**。

   

6. 在**新建主机账户**对话框中，设置账户的**协议**、**登录名**和**认证类型**等参数。

   

   如果您进行了批量添加用户操作，您需要在**新增账户**对话框中，设置账户的**认证类型**、**协议**、**登录名**和**密码**。

   

7. （可选）单击**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。

   > **说明** 批量新增账户时，无需验证密码。

8. 单击**创建**。

   > **说明** 批量新增账户时，单击**确定**。

1.4.5. 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。本文档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. 在左侧导航栏单击**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**对话框中，修改账户的**登录名**和**密码**。

   

7. （可选）单击**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。

   > **说明** 批量新增账户时，无需验证密码。

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. 在左侧导航栏单击**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并单击**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. 在左侧导航栏单击**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**页面，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**页面，输入密码。
   - **清除密码**

     定位到需要清除密码的登录名并单击**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. 在左侧导航栏单击**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并单击**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**。

1.4.6. 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. 在左侧导航栏单击**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**。

1.5. 主机组管理

1.5.1. 新建主机组

通过将多个主机加入到一个主机组，您可以集中管理这些主机，并进行批量授权。本文介绍如何新建主机组。

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. 在左侧导航栏单击**资产管理 > 主机组**。
3. 在**主机组**页面单击**新建主机组**。
4. 在**主机组名**文本框输入您的主机组名称。

> **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主机组名称，方便后续维护和识别。

5. 单击**新建主机组**。

后续步骤

添加完主机组后，您可以将主机添加到主机组中，具体请参见添加主机组成员。

1.5.2. 修改和删除主机组

您可以通过修改或删除功能，定期维护主机组列表。

修改主机组名称

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**资产管理 > 主机组**。
3. 在主机组列表中，单击需要修改的主机组的名称。
4. 单击**主机组设置**页签。

5. 在**主机组名**文本框输入新的主机组名称。
6. 单击**更新**。

删除主机组

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**资产管理 > 主机组**。
3. 在**主机组**页面，选中需要删除的主机组并单击**删除**。

> **说明** 如果需要删除单个主机组，您可以单击该主机组操作列的删除。

4. 在确认对话框中，单击**删除**。

1.5.3. 添加和移除主机组成员

您可以将多个主机加入到一个主机组，并对这些主机进行批量授权。本文介绍如何添加和移除主机组成员。

添加主机组成员

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**资产管理 > 主机组**。
3. 在主机组列表中，单击主机组的名称。

4. 在**主机组成员**页签中单击**添加主机成员**。

5. 在主机列表中，选择需要添加到主机组成员的主机并单击**添加**。

> **说明** 如果需要添加单个主机，您可以直接在**操作**列中单击**添加**。

移除主机组成员

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**资产管理 > 主机组**。
3. 在主机组列表中，单击主机组的名称。
4. 在主机组成员列表中，选中需要移除的主机组成员并单击**移除**。

> **说明** 如果需要移除单个主机组成员，您可以直接在该主机的**操作**列中单击**移除**。

1.6. 用户管理

1.6.1. 新建用户

堡垒机中的用户成员代表技术工程师，也就是自然人。堡垒机V3.2版本支持导入阿里云RAM用户、新建堡垒机本地用户、导入AD或LDAP认证用户。

导入RAM用户

如何导入已有RAM用户请参见以下步骤：

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**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**。

新建并导入RAM用户

新建并导入RAM用户的操作，具体请参见以下步骤：

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**人员管理 > 用户**。
3. 在**用户**页面单击**导入RAM用户**。

4. 单击**新建RAM用户 > RAM访问控制新建用户**。

5. 在**新建用户**页面设置新的RAM用户信息，并单击**确定**。您可以参考以下信息新建RAM用户：
   - 设置**登录名称**和**显示名称**。
   - 选中**控制台密码登录**。
   - 选中**要求开启MFA认证**。 建议您启用MFA认证。

   > **说明** 多因素认证MFA（Multi-factor authentication）是一种简单有效的最佳安全实践，在用户名和密码之外再增加一层安全保护。选中**要求开启MFA认证**，RAM用户登录时会直接进入多因素认证绑定流程，更多信息请参见**为RAM用户设置多因素认证**。

6. 新建RAM用户后，返回堡垒机**新建RAM用户**对话框，单击**新建完成**。
   新建完成后，在**导入RAM用户**的列表中，可以查看新建的RAM用户。
7. 在RAM用户列表中，选中新建的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**。

8. 单击**导入**。

新建本地账号

导入本地账号的操作，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. 在左侧导航栏单击**人员管理 > 用户**。
3. 在**导入其他来源用户**列表中单击**新增本地用户**或**从文件导入本地用户**。如果您只需要导入一个本地用户，建议您单击**新增本地用户**。如果您需要批量导入多个本地用户，建议您单击**从文件导入本地用户**。
4. 参照以下步骤完成本地用户导入操作。以下分别介绍**新增本地用户**和**从文件导入本地用户**的具体操作：
   - **新增本地用户**

     在**新增本地用户**页面配置账户的基本信息，包括用户名、密码、姓名、邮箱、手机号和用户组。配置完成后单击**创建**。

   - **从文件导入本地用户**

     单击**下载用户模板文件**，在下载的文件中输入您需要导入的用户信息。保存文件后，单击**点击上传**上传模板文件。在**导入用户预览**页面选中需要导入的用户并单击**导入**。单击**导入本地用户**完成本地用户的导入。

> 说明
>
> -
> -
> - 您填写的手机号码和邮箱仅用于接收验证码或告警信息，不用于其他用途。

导入AD认证用户

导入AD用户前需要配置AD认证。详细操作指导请参见配置AD认证。如何导入AD认证用户请参见以下步骤：

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**人员管理 > 用户**。
3. 在**导入其他来源用户**列表中单击**导入AD用户**。

   导入AD用户
4. 选中需要导入的AD用户并单击**导入**。

   导入AD用户

   您也可以单击某个AD用户操作列**导入**将该用户导入堡垒机中。

导入LDAP用户

导入LDAP用户前需要配置LDAP认证。详细操作指导请参见配置LDAP认证。如何导入LDAP认证用户请参见以下步骤：

1. 登录堡垒机系统，具体操作请参见登录堡垒机系统。
2. 在左侧导航栏单击**人员管理 > 用户**。
3. 在**导入其他来源用户**列表中单击**导入LDAP用户**。

   导入LDAP用户入口
4. 选中需要导入的AD用户并单击用户列表上方的**导入**。您也可以单击某个LDAP用户操作列**导入**将该用户导入堡垒机中。

1.6.2. 修改用户信息

如果用户的信息发生了变更，例如某个用户更换了手机号，您可以在堡垒机控制台上修改该用户的信息。本文介绍如何修改用户的信息。

背景信息

只支持修改本地用户的信息。不支持修改RAM用户、AD用户和LDAP用户的信息。

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**人员管理 > 用户**。
3. 定位到需要修改信息的用户并单击其用户名。
4. 在该用户的**基本信息**页签下，修改密码、手机号、邮箱和用户组信息。

> 说明
>
> - 如果开启双因子认证，请填写正确的用户手机号。本地用户在登录时，必须使用手机收到的验证码进行验证。
> - 堡垒机支持输入中国大陆、中国香港、俄罗斯、新加坡、马来西亚 、印度尼西亚、德国、澳洲、美东、美西、迪拜、东京、英国、印度地区的手机号码。

5. 单击**更新**。

1.6.3. 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。

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**人员管理 > 用户**。
3. 选中需要删除的用户。

4. 单击**删除**。

1.7. 用户组管理

1.7.1. 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. 在左侧导航栏单击**人员管理 > 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。

1.7.2. 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. 在左侧导航栏单击**人员管理 > 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. 在左侧导航栏单击**人员管理 > 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**。

1.7.3. 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. 在左侧导航栏单击**人员管理 > 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. 在左侧导航栏单击**人员管理 > 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**。

1.8. 认证设置

1.8.1. 安全配置

为了保障系统的安全，防止用户密码被暴力破解，您可以在安全配置中设置用户锁定配置。

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**安全配置**页面配置用户锁定的规则。

   您可以参考以下表格中的参数说明配置用户锁定规则。

参数	说明
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，如果设置为0，则不锁定账户。
锁定时长	用户锁定后，无法登录的时长。 取值范围：0~10080。默认值为30，如果设置为0，则锁定用户直到管理员解除。
重置计数器	登录尝试密码失败之后，将登录尝试失败计数器重置为0次所需要的时间。 取值范围：0~10080。默认值为5。

4. 单击**保存**。

1.8.2. 开启双因子认证

双因子认证在本地用户登录时发送短信口令，二次认证用户身份，可以有效降低账户泄露等情况带来的安全风险。本文介绍如何开启双因子认证。

背景信息

开启短信双因子认证后，未添加手机号的本地账号将不能进行运维操作。建议您在开启双因子认证前，为需要进行运维操作的本地账号添加手机号。

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. 选中**启用短信认证**。

5. 单击**保存**。

1.8.3. 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**。

1.8.4. 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**。

1.9. 授权主机

1.9.1. 按用户授权主机

授权主机是将堡垒机中的用户与主机资产联系在一起的概念，通过授权主机功能可以达到控制某个用户只能访问自己权限内主机的目的。该章节介绍按用户维度授权主机和主机账户，以及如何维护用户的主机和主机账户。

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. 在左侧导航栏单击**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**授权主机**。
5. 选中需要授权给该用户进行运维的主机并单击**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. 在左侧导航栏单击**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. 选中需要移除的已授权主机并单击**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. 在左侧导航栏单击**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. 在左侧导航栏单击**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. 在左侧导航栏单击**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**。

1.9.2. 按用户组授权主机

授权主机是将堡垒机中的用户与主机资产联系在一起的概念，按用户组授权主机可以控制某个用户组内的用户只能访问该用户组权限内的主机。该章节除了介绍按用户组维度授权主机和主机账户，同时还介绍后续如何维护用户组的主机和主机账户。

背景信息

按用户授权主机和按用户组授权主机的区别：

- 按用户授权主机：为单一用户授权主机和主机账户。
- 按用户组授权主机：用户组为多个用户的合集，为用户组授权相当于为用户组下的所有用户批量授权主机和主机账户。

授权主机

为用户组授权主机，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. 在左侧导航栏单击**人员管理 > 用户组**。
3. 在需要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**页签中，单击**授权主机**。
5. 在**授权主机**页面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，可以通过移除已授权主机操作，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. 在左侧导航栏单击**人员管理 > 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. 选中需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**。

授权主机账户

为用户组授权单个主机的登录账户，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. 在左侧导航栏单击**人员管理 > 用户组**。
3. 在需要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**页签中，单击**已授权账户**。

5. 选中主机账户，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. 在左侧导航栏单击**人员管理 > 用户组**。
3. 在需要授权主机的用户组的**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. 在左侧导航栏单击**人员管理 > 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**。

1.9.3. 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. 在左侧导航栏单击**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。

1.10. 授权主机组

1.10.1. 按用户授权主机组

主机组为多个主机的合集。通过授权主机组功能，用户可以控制主机组下面的所有主机和授权账户。该章节介绍按用户维度授权主机组和账户，以及如何维护用户的主机组和账户。

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. 在左侧导航栏单击**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，可以通过移除已授权主机组操作，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. 在左侧导航栏单击**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. 在左侧导航栏单击**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. 在左侧导航栏单击**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. 在左侧导航栏单击**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**。

1.10.2. 按用户组授权主机组

主机组为多个主机的合集。通过授权主机组功能，用户组可以控制主机组下面的所有主机和授权账户。本文介绍按用户组维度授权主机组和账户，以及如何维护用户组的主机组和账户。

背景信息

按用户授权主机组和按用户组授权主机组的区别：

- 按用户授权主机组：为单一用户授权主机组和账户。
- 按用户组授权主机组：用户组为多个用户的合集，为用户组授权相当于为用户组下的所有用户批量授权主机组和账户。

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. 在左侧导航栏单击**人员管理 > 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，可以通过移除已授权主机组操作，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. 在左侧导航栏单击**人员管理 > 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. 在左侧导航栏单击**人员管理 > 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. 在左侧导航栏单击**人员管理 > 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. 在左侧导航栏单击**人员管理 > 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**。

1.11. 控制策略

1.11.1. 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**策略 > 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**。

> **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**。 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**。 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、SSH协议控制策略并单击**下一步：访问控制**。 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。

1.11.2. 管理控制策略

如果您的业务场景发生变化，您可以编辑或删除已有的控制策略。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**策略 > 控制策略**。
3. 定位到需要修改的控制策略并单击操作列下的**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**策略 > 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**策略 > 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**。

1.12. 审批

1.12.1. 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**审批 > 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**。

1.13. 会话审计

1.13.1. 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审计，查看是否存在违规操作。

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. 在左侧导航栏单击**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。

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，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，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. 搜索目标会话，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。

1.14. 实时监控

1.14.1. 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. 在左侧导航栏单击**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**。

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. 在左侧导航栏单击**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. 在左侧导航栏单击**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。

1.14.2. 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. 在左侧导航栏单击**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**。

1.15. 操作日志

1.15.1. 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. 在左侧导航栏单击**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**

搜索项	说明
操作名称	在操作列表中选择需要查看的操作名称。例如：选择**添加主机组成员AddHostsToGroup**。
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。

1.16. 系统设置

1.16.1. 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。

2.运维使用手册

2.1. Windows系统运维

2.1.1. 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。

运维入口

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。

2.1.2. 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。

运维入口

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。

2.1.3. 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。

2.2. Mac系统运维

2.2.1. 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。

运维入口

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。

2.2.2. 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。

  运维入口

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。

   

2.2.3. 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。

  运维入口

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。