Alibaba Cloud

堡垒机 用户指南(V3.2版本)

文档版本: 20220608



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。

- 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。
- 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。
- 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。	大意 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 <i>,</i> 不是 用户必须了解的内容。	⑦ 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 listinstanceid
[] 或者 [alb]	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 {act ive st and}

目录

1.管理员手册	07
1.1. 授权堡垒机访问云资源	07
1.2. 登录堡垒机系统	09
1.3. 实例管理	10
1.3.1. 配置堡垒机	10
1.3.2. 管理堡垒机实例标签	12
1.4. 资产管理	14
1.4.1. 主机管理	14
1.4.1.1. 新建主机	14
1.4.1.2. 管理主机	15
1.4.1.3. 修改主机的服务端口	17
1.4.1.4. 新建主机账户	19
1.4.1.5. 配置主机账户	20
1.4.1.6. 修改主机的运维连接IP	24
1.4.1.7. 清除主机指纹	25
1.4.1.8. 一键导出主机列表	26
1.4.2. 管理资产组	26
1.4.3. 改密任务	27
1.4.4. 密钥管理	30
1.5. 人员管理	31
1.5.1. 用户管理	31
1.5.1.1. 管理用户	31
1.5.2. 用户组管理	35
1.5.2.1. 新建用户组	35
1.5.2.2. 修改和删除用户组	35
1.5.2.3. 添加和维护用户组成员	36

1.5.3. 授权主机	38
1.5.3.1. 按用户授权主机	38
1.5.3.2. 按用户组授权主机	42
1.5.3.3. 导出授权关系	45
1.5.4. 授权主机组	46
1.5.4.1. 按用户授权主机组	46
1.5.4.2. 按用户组授权主机组	50
1.6. 授权规则	55
1.6.1. 新建授权规则	55
1.6.2. 管理授权规则	57
1.7. 控制策略	58
1.7.1. 管理控制策略	58
1.8. 命令审批	61
1.8.1. 审批命令	61
1.9. 审计	62
1.9.1. 会话审计	62
1.9.1.1. 搜索和查看会话	62
1.9.1.2. 归档审计日志到日志服务	64
1.9.1.3. 日志备份	65
1.9.2. 实时监控	66
1.9.2.1. 搜索和查看实时监控会话	66
1.9.2.2. 阻断会话	68
1.9.3. 操作日志	68
1.9.3.1. 搜索和查看操作日志	68
1.9.4. 运维报表	69
1.10. 主机运维	72
1.10.1. 主机运维	72
1.11. 系统设置	73

1.11.1. 用户配置	73
1.11.2. 开启双因子认证	74
1.11.3. 配置AD认证	74
1.11.4. 配置LDAP认证	75
1.11.5. 网络诊断	76
1.11.6. 运维配置	77
1.11.7. 存储管理	81
1.11.8. 消息通知	83
1.11.9. 配置备份	84
1.11.10. 管理第三方资产源	85
2.运维使用手册	87
2.1. 运维概述	87
2.2. Windows客户端运维	87
2.2.1. SSH协议运维	87
2.2.2. RDP协议运维	90
2.2.3. SFTP协议运维	92
2.3. Mac客户端运维	95
2.3.1. SSH协议运维	95
2.3.2. RDP协议运维	96
2.3.3. SFTP协议运维	98

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<mark>服务关联角色</mark>。

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

⑦ 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:

用户指南(V3.2版本)·管理员手册

```
{
   "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。

运行中 bastionhost				
华东1(杭州)				會理
标签	版本	规格	到期时间	EXT.
	10. T	79010	EN LOUIS	
	企业版	50资产 企 升配	2019年11月16日 👔 续费	



以下表格介绍了云堡垒机页面的各个区域。

区域	说明
0	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。
6	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。

创建主机 创建用户 运维授权 主机运维 ●				使用向导 >
トレニシング トレニシング トレニシング トレニシング トレニシング トレニシング 日戸建度授权 医生机运推端口 SSH: 60022 RDP: 63389 本地客户端公网运進入口 SSH: 60022 RDP: 63389 本地客户端公网运進入口 アメロシング 中地客户端公の送進入口 アメロシング 中地客户端公内运進入口 アメロシング 本地客户端公内运進入口 アメロシング 本地客户端公内运進入口 アメロシング 本地客户端へ内运進入口 アメロシング 本地客户端内内运進入口 アメロシング 本地客户端内内运進入口 Psrmamcqcr-public.bastionho ① 文持水は、csv、xlsx格式批量导入 人文件导入本地用户 文持水は、csv、xlsx格式批量导入 人文件导入本地用户 アメロシング 本地客户端内内运進入口 Psrmamcqcr.bastionhost.aliyu ①	创建主机	创建用户	运维授权	主机运维
新建主机 新増本地用户 访问主机时可使用的凭据。 本地客户端公网运维入口 手动添加单个主机 本地用户双因子认证采用短信验证 psrmamcqcr-public.bastionho ① 从文件导入主机 码 本地客户端内网运维入口 支持xls、csv、xlsx格式批量导入 人文件导入本地用户 支持xls、csv、xlsx格式批量导入 文持xls、csv、xlsx格式批量导入	■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	<mark>导入RAM用户</mark> RAM子账户双因子采用MFA认证	用户维度授权 为用户添加主机的访问权限,以及	叠垒机运维端口 SSH: 60022 RDP: 63389
	新建主机 手动添加单个主机 从文件导入主机 支持xls、csv、xlsx梢式批量导入	新增本地用户 本地用户双因子认证采用短信验证 码 从文件导入本地用户 支持xls、csv、xlsx格式批量导入	访问主机时可使用的凭握。	本地客户端公网运维入口 psrmamcqcr-public.bastionho ① 本地客户端内网运维入口 psrmamcqcr.bastionhost.aliyu ①

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。

标签 🖉 编辑 🗌 出口IP		
公网	on)	
私网	☆ 配置 V3.2.18 (新版本)	①升纲
	<u>又主知</u> 古夕首	

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。

网络设置		×
网络	 vpc-t vsw-t 	
安全组	bastionho × × 选择后,允许堡垒机访问安全组内的ECS 通 ● ● 量 量 量 量 量 ECS	

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。

运行中	and the second s
标签 🕢 编辑 🗌 出口IP	版本
私网	段 配置 V3.2.18 新版本 ① 并
	安全组
	日名単 第日号

4. 在网络设置面板上, 配置公网白名单。

×	网络设置
	网络
	公网白名单 请输入IP地址,以英文,分开,最多30个
	公网白名单 请输入IP地址,以英文,分开,最多30个

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。

运行中	-	100.00
标签 ⑦ 編編 │ 出口IP 公网 私网	on 动配置	版本 V3.2.18 新版本 ①升级
	安全组 白名単 靖口号	

4. 在端口配置面板上, 配置端口。

端口配置						×
网络	0					
	•					
端口	标准	60021	自定义	60021	修改	0
	标准	60022	自定义	60022	修改	0
	标准	60023	自定义	60023	修改	0
	标准	63389	自定义	63389	修改	0
	标准	61022	自定义	61022	修改	0

⑦ 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。

云盾 ^{堡垒机 / 实例} 实例	
2477中 bastionhost 标签 ② 编辑 出口IP 公	 ○ ○ ○ ○ ○

- 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。

⑦ 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。

标签设置		\times
标签	11: 22 🗵	

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。

	产品	手册	购买堡垒机
请选择	^	全部状态	\sim
全部标签	22		
11 >			
			管理
		、上页	1 下一页 >

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。

⑦ 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AP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。

主机										
导入ECS实例导入其他来源	験主机 > 主机 > 投索目	E机名/主机IP Q	操作系统: 全部	✓ 主机来源:全部 ✓ 主机	〕状态:全部 ∨				导出主机	С
主机名	主机IP	晉注	主机账户数	网络域	攝作系统	主机来源	主机状态	搵作		
cylin	192.168.0		0	Direct Network	Linux	ECS	 正常 	新建主机账户 删除	k	
39.101	39.101.		1	Direct Network	Windows	Local	 正常 	新建主机账户 删除	k	
101.132	101.132.		1	Direct Network	Linux	Local	 正常 	新建主机账户 删除	k	
shangha	192.16		1	shanghaicy	Linux	Local	 正常 	新建主机账户 删除	k	
wl.w	172.16		0	Direct Network	Linux	ECS	 正常 	新建主机账户 删除	k	

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 Q 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。
 - ⑦ 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。

基本信息	服务端口	主机账户		
* 操作系统				
Windows				
* 主机IP				
39.101.				
主机名				
30.101				

Direct Network (直连)	~
計	
日本	

⑦ 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。

					Q 搜索文档、 拍	潮台、API、	2 2				х
云堡垒机 / 资产管理	里 / 主机						基本信息	服务端口	主机账户		
主机							RDP :	3389			
导入ECS实例	导入其他来源主机 >		操作系统:全部		主机来源: 全部	\vee					
主机名		主机IP	备注	主机	账户数			更新			
2 2				0							

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。

·W	indows	
基本信息	服务端口	主机账户
RDP:	3389	
	更新	

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。

主机	l								
导入B	CS\$200	导入其他来源主机 >	搜索主机名/主机IP Q	操作系统:全部 · · 3	初来源:全部 ソ 主机状态:	:全部 ∨			С
	主机名		主机IP	曾注	主机账户数	操作系统	主机来源	主机状态	攝作
	14		1000		0	Linux	Local	• 正常	删除
					0	Linux	ECS	• 正常	删除
			1211		0	Linux	ECS	• 正常	那 時
		修改运输连接 IP	A	ALIg4s	0	Linux	ECS	• 正常	劃除
		主机账户 >	1.000		0	Linux	ECS	• 正常	把 的
	删除	批量 ∨						息计7 < 上一页	1 2 下一页 > 5条/页>

4. 在修改运维端口对话框中,设置协议和端口。

修改运维端口			×
协议:	SSH	~	
端口:	22		
		确定	取消

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。

新建主机账户				
请确认主机或ECS案 户同步到主机或ECS	:例上已经创建了对应 实例。	立的操作系统账户,	堡垒机不会将主	E机账
* 协议				
SSH			\sim	
bastion. 认证 选 刑		onaliyun.com		
wuyyyu 密码			~	
密码				
			Æ	0
验证密码				

c. 单击验证密码。

使用验证密码可以测试主机账户的用户名和密码是否正确。

- d. 单击**创建**。
- 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。

主机		
导入ECS实例	导入其他来源主机	しゃ 主机 く
■ 主机名		主机IP
cy_lin		121.40.1
39.10		39.101.7
101.1	-	101.132
shang		192.168
wl.	修改运维连接IP	172.16.4
🖌 lau	修改运维端口 主机账户 >	172.162 。 新増账户
nef 🔤	清除主机指纹	删除账户
	余 批量 ∨	

c. 在新增账户对话框中设置认证类型、协议、登录名等参数。

⑦ 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。

-windows			:	×
基本信息 服务端口	主机账户			
新建主机账户 搜索登录	洺	Q	С	
登录名	协议	密码	SSH私钥	
	RDP	无密码 设置	无私钥 设置	
删除			< 1 / 1 > 20条/页>	

- 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。

编辑主机账户	×
* 登录名	
ac	
密码	
ø	0
验证密码	
保存	

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。

-	windows)
基本信息	服务端口	主机账户			
新建主机则	(户) 搜索登录	Ä	٩		С
登	灵名	协议	密码	SSH私钥	
		RDP	无密码 设置	无私钥 设置	
	删 除			< 1 / 1 > 20条/页	~

5. 选中需要删除的账户, 单击列表下方的删除。

10				х
基本信息	服务端口	主机账户		
新建主机账户	搜索登录谷	7	Q	С
✓ 登录名		协议	密码	SSH私钥
		SSH	有密码清	除 无私钥 设置
✔ 删除				〈 1 / 1 〉 20条/页 \/

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。

-W	indows			×
基本信息	服务端口	主机账户		
新建主机账户	• 搜索登录	Š.	Q	С
登录	名	协议	密码	SSH私钥
		RDP	无密码 设	置 无私钥 设置
册	除			< 1 / 1 > 20条/页 >

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。

-wi	indows				×
基本信息	服务端口	主机账户			
新建主机账户	搜索登录谷	3	Q		С
登录	名	协议	密码	SSH私钥	
		RDP	无密码 设置	置 无私钥 设置	
755	除			< 1 / 1 > 2	20条/页∨

5. 定位到需要设置私钥的登录名,单击SSH私钥列的设置。

m wi	ndows					×
基本信息	服务端口	主机账户				
新建主机账户	搜索登录	Л	٩			С
登录	ž	协议	密码		SSH私钥	
a	or	RDP	无密码	设置	无私钥 设置	
		RDP	有密码	清除	无私钥 设置	
删	除			<	1 / 1 > 20)条/页∨

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。

设置私钥				×
仅支持ssh-ke	ygen生成的RSA私钥			
★ 私钥:				
加爽口会。		0		//
		U	保存	取消

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。

⑦ 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。

王初									
导入的	CS\$\$2(0)	导入其他来源主机 ∨	搜索主机名/主机IP Q	提作系统: 全部 V	主机来源: 全部 🛛 🗸 主机状态: 🕯	286 V			С
	主机名		主机IP	备注	主机账户数	操作系统	主机来源	主机状态	操作
	14		1000		0	Linux	Local	• 正常	删除
					0	Linux	ECS	• 正常	删除
			1000		0	Linux	ECS	• 正常	删除
		修改运進连接IP	A 1999 - 1	ALIg4s	0	Linux	ECS	• 正常	删除
		主机账户 >	1.000		0	Linux	ECS	• 正常	1990 :
	删除	批量 ~						息计7 < 上一页	1 2 下一页 > 5条/页 >

4. 在修改运维连接IP对话框中,选择主机IP类型。

修改运维连接IP	1			×
主机IP类型:	公网IP	~		
			确定	取消

- 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。

基本信息	服务端口	主机账户			
* 操作系统					
Linux					\sim
* 主机IP					
101 16	7				
主机名					
备注					
					0
主机指纹				_	
ssh-ed25519 4		D1:	96 🗊 清空		
主机组					
更新					

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。

 主机器 	主的JP	養注	主机联合数	操作系统	主机来源	主机状态	操作
ch-bp1	192 62	dhg-60k16828	4	Linux	云数旗库专雕原制	• 正常	新建主机联冲 数除
	101 167		1	Linux	Local	• 正常	新建主机账户 勤除
	101 167		1.	Linux	Local	 正常 	新建主机联合 数除
	19; 12		0	Windows	ECS	• 正常	新建主机联冲 動除
A 律改运建连接IP	192 13		0	Linux	ECS	• 正常	新建主机账户 勤除
(学校)画(教)日	19. 93		4	Linux	BCS	 已释放 	新建主机联合 数除
清除主机器纹	192 6		0	Linux	Local	• 正常	新建主机联冲 動除
■ 創除 找量 ¥							息计7 く 上一页 1 下一页 > 20 条/页 >

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。
- 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。

主机													
导入ECS实例	导入其他来源主机 ×	主机・ソー	搜索主机名/主机P	۹ 1	操作系统: 全部		主机来源:全部	主机状态: 全部				导出主机	С
主机名		主机IP		留	注	3	主机账户数	操作系统	主机来源	主机状态	操作		
		10	167				1	Linux	Local	• 正常	新建主机账户 删除		
		101	67				1	Linux	Local	• 正常	新建主机账户 删除		

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。

⑦ 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。

⑦ 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
Cent OS	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
	⑦ 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。

添加主机账户					×
添加 捜索主机账户名称 Q					С
✓ 主机	账户名称	协议	操作系统	南码	
19 .93 li		SSH	Linux	• 否	<u>^</u>
✓ 10 167 91	root	SSH	Linux	• 是	
✓ 101 167 92	root	SSH	Linux	• 是	-
				息计 3 < 上一页 1 下一页 > 20	条/页∨

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**。

⑦ 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。

⑦ 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。

导出密码	Х
结果文件将被压缩成zip格式,请输入文件加密密码,密码长度4-32位。	
* 文件加密:	
	ø
	密码 取消

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。

⑦ 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。

⑦ 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。

1.5. 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 <mark>配置AD认证</mark> 。
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 <mark>配置LDAP认证</mark> 。

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。
- 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
适用场景	操作说明
单个新增太地用户	

适用场景	■ 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 操作说明 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。
	 ⑦ 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
	 Ⅰ 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。
	⑦ 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。
	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。
	v. 在 导入本地用户 面板,确认用户信息。
批量从文件导入本地 用户	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 。
	⑦ 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。
- 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。

② 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。

新建用户组	×
* 用户组名	0

⑦ 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。

用户组		
新建用户组 搜索用户组名称 Q.		С
名称	成员数	操作
Web运维	0	授权主机丨授权主机组
测试用户组	1	授权主机丨授权主机组
测试组	0	授权主机丨授权主机组
运维人员	0	授权主机丨授权主机组
割除		总计4 く 上一页 1 下一页 > 20 条/页 >

4. 在用户组名中, 输入新的用户组名称。

← Web运维							
用户组设置	用户组成员	已授权主机	已授权主机组				
* 用户组名							
Web运维							
更新用户组							

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。

用户组							
新建用	户组 搜索用户组名称 Q			С			
	名称	成员数	操作				
	Web运维	0	授权主机 授权主机组				
	测试用户组	1	授权主机 授权主机组				
	测试组	0	授权主机 授权主机组				
	运维人员	0	授权主机 授权主机组				
	删除		总计4 < 上一页 1 下一页 > 20 组	ዷ/页 ∨			

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。

用户组		
新建用户组 搜索用户组名称 Q、		C
名称	成员数	操作
Web运维	0	授权主机 授权主机组
测试用户组	1	授权主机 授权主机组
测试组	0	授权主机 授权主机组
运维人员	0	授权主机 授权主机组
删除	总计 4 < _	上一页

- 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。

云堡垒机 / 人员管理 / 用户组 / 用户组详情								
← network								
用户组设置	用户组成员	已授权主机	已授权主机组					
添加成员	搜索用户名/姓名	Q						
用户名								

6. 在添加成员对话框,选中需要添加的用户并单击添加。

添加成员			×
搜索用户名/姓名 Q、			С
■ 用户名	姓名	握作	
I i i st	otest	添加	•
✓	o	添加	
		添加	- 1
	10000	添加	-
■ 添加		总计6 〈 上一页 】 下一页 〉 :	20条/页 >

⑦ 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。

用户组		
新建用户组 搜索用户组名称 Q		C
名称	成员数	操作
Web运维	0	授权主机 授权主机组
测试用户组	1	授权主机 授权主机组
测试组	0	授权主机 授权主机组
运维人员	0	授权主机 授权主机组
□ 删除	总计 4	く 上一页 1 下一页 > 20 条/页 ∨

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。

\leftarrow network					
用户组设置用户组成员	已授权主机	已授权主机组			
添加成员 搜索用户名/姓名	ç Q				С
■ 用户名			姓名	操作	
			100	移除	
			-	移除	
■移除				总计 2 〈 上一页 1 下一页 〉 20	条/页∨

⑦ 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。

云堡垒机 / 人	员管理 / 用户				
用户					
导入RAM用F	➡ 导入其他来源用户 ∨	搜索用户名/姓名 Q	认证源:全部 🛛 🗸		导出授权关系 C
用户	9名	姓名	认证源	操作	
		100	RAM用户	授权主机 授权主机组	
			本地认证	授权主机 授权主机组	

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。

云堡垒机	/ 人员管理	/ 用户						
用户	1							
导入R/	AM用户	导入其他来源用户 🗸	搜索用户名/姓名	へ 认证源:全部	\vee		导出授权关系	С
	用户名		姓名	i	认证源	操作		
				I	RAM用户	授权主机 授权主机组		
				;	本地认证	授权主机 授权主机组		

4. 在已授权主机列表中选中要移除的主机,单击移除。

云堡垒机 / 人员管理 / 用户 / 用户详情				
÷.				
基本信息 已授权主机 已授权主机	机组 用户公钥			
授权主机 搜索主机IP/主机名 C	入 操作系统:全部 🗸			С
主切IP	主机名	操作系统	已授权账户	
1 23	-linux	Linux	root	
▼ 移除 批量 >				总计 1 く 上一页 1 下一页 > 20 条/页 >

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。

_{云堡垒机} 用户	/ 人员管理 / 用户					
导入RA	M用户 导入其他来源用户 >	搜索用户名/姓名 Q	认证源:全部 ∨		导出授权关系	С
	用户名	姓名	认证源	操作		
		100	RAM用户	授权主机 授权主机组		
			本地认证	授权主机 授权主机组		

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。

			Q 搜索文档、控制台、API、解决方	anter 1	恵用 エ	选择账号 -linux]	×
云堡垒机 / 人员管理 / 用户 / 用户洋街							
← jialin						[394] 1001	
基本信息 已授权主机 已授权主机组 用户公钥							
授权主机 控索主机 い主机名 9、 操作系统:全部							
主机P	主机名	操作系统		已授权账户			
10 23	linux	Linux		root			
□ 移 除 就量 ∨							

5. 选中主机账户并单击更新。

⑦ 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。

云堡垒机 / 人员管理	2 / 用户					
用户						
导入RAM用户	导入其他来源用户 > 搜索用户名/约	名 9、 认证源:全部	×		导出授权关系	С
用户名		姓名	认证源	操作		
		100	RAM用户	授权主机 授权主机组		
			本地认证	授权主机 授权主机组		

4. 选中需要授权账户的主机并单击批量 > 批量授权账号。

云堡垒机 / 人長	云堡垒机 / 人员管理 / 用户 / 用户详情							
÷								
基本信息	已授权主机	已授权主机组	用户公钥					
授权主机	搜索主机IP/主机名	ç Q	操作系统: 全部	V				
 主机 	,IP 批母培权M	K=		主机名				
1	批量移除排	《 受权账号		linux				
✓ 移	3除 批量 >							

5. 选中主机授权账户的账户名称。

批量授权账号		×
批量授权的主机需	暑要包含该授权账号,否则该主机与账号的授权将不会生效	
当前选择主机数: 2 账户:	root	
? 说明 批量	授权主机账号时,只能选择一个主机账户进行	亍授权

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。

云堡垒机 / 人员管理	/ 用户					
用户						
导入RAM用户	导入其他来源用户 ∨ 搜索用户名/姓名	Q 认证源: 全部	\sim		导出授权关系	С
用户名	姓名	认	证源	作		
		RA	AM用户 援	叙主机 授权主机组		
		本	地认证 摄	叙主机 授权主机组		

- 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。

云堡垒机 / 人	云堡垒机 / 人员管理 / 用户 / 用户详情				
÷.					
基本信息	已授权主机	已授权主机组	用户公钥		
授权主机	搜索主机IP/主机名	g Q	操作系统: 全部	~	
之 主材	JIP 批量授权II	K₽		主机名	
10	批量移除批	受权账号		linux	
✔ 私	8 除 批量 ∨				

6. 选中需要移除的主机授权账户名称。

批量移除授权账	'문	×		
当前选择主机数: 6	; 			
账户:				
	user			
	root			
? 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	深。

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。

用户组		
新建用户组 搜索用户组名称 Q.		С
名称	成员数	操作
Web运维	2	授权主机 授权主机组
测试用户组	1	授权主机丨授权主机组
测试组	0	授权主机丨授权主机组
运维人员	0	授权主机丨授权主机组
		总计4 < 上一页 1 下一页 > 20 条/页 ∨

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。

搜索主机IP/主机名	♀ 操作系统:全部 ∨	< 1/1 >	已选择 (2)	清晰
■ 主机IP	主机名	操作系统	12 18 bastionhost_demo	x
✓ 12 ⁻ 218		Linux	19 5 bastionhost_demo	×
✓ 192 65		Windows		
192 2	19 2	Linux		
192 35		Linux		

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。

用户约	组		
新建用户	组 搜索用户组名称 Q		С
	名称	成员数	操作
	Web运维	2	授权主机 授权主机组
	测试用户组	1	授权主机 授权主机组
	测试组	0	授权主机 授权主机组
	运维人员	0	授权主机 授权主机组
	删除	总计,	4 く 上一页 1 下一页 > 20 条/页 ∨

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。

< Webì	运维						
用户组设置	用户组成员	已授权主机	已授权主机组				
授权主机	搜索主机IP/主机名	٩	操作系统:全部	/			С
■ 主机	р	主机名		操作系统	已授权账户	à	
1		堡垒机_勿	册1	Linux	0		
1	23	堡垒机-lin	iux	Linux	0		
	73	Bastion_A	ssets2	Linux	0		
■ 移	除 批量 >				总计 3 🔸	く 上一页 1 下一页	> 20条/页 ∨

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。

用户约	且			
新建用户	組 捜索用户组名称 Q			С
- 4	名称	成员数	操作	
	Web运维	2	授权主机 授权主机组	
	测试用户组	1	授权主机 授权主机组	
	则试组	0	授权主机 授权主机组	
j j	运维人员	0	授权主机 授权主机组	
			总计4 < 上一页 1 下一页 >	20条/页 >

- 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。

批量授权账号		×
批量授权的主机器	需要包含该授权账号,否则该主机与账号的授权将不会生效	
当前选择主机数: 2 账户:	root	
? 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。

用户编	且			
新建用户	组 搜索用户组名称 Q			С
	名称	成员数	操作	
	Web运维	2	授权主机 授权主机组	
i	测试用户组	1	授权主机 授权主机组	
i	测试组	0	授权主机 授权主机组	
i j	运维人员	0	授权主机 授权主机组	
	删除		总计 4 く 上一页 1 下一页 > 20 条/	页 ~

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。

批量移除授权账号	ţ	×
当前选择主机数 : 6		
火大/一:	user	
	root	
⑦ 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。

云堡垒机 / 人员管	理 / 用户			
用户				
导入RAM用户	局入其他来源用户 ∨	○ 认证源:全部 ∨		导出授权关系 C
用户名	姓名	认证源	操作	
	100	本地认证	授权主机 授权主机组	
	1.12	本地认证	授权主机 授权主机组	
解發	删 除			总计2 < 上一页 1 下一页 > 20 魚/页∨

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。

云堡垒机 / 人员管理 / 用户				
用户				
导入RAM用户 与入其他来源用户 ∨				导出授权关系 C
用户名	姓名	认证源	操作	
		本地认证	授权主机 授权主机组	
		本地认证	授权主机 授权主机组	
解锁副除				总计2 く 上一页 1 下一页 > 20 象/页 >

- 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。

		授权主机组				×
云遥金帆 / 人员管理 / 用户 / 用户详病		推卖主机组名	٩	< 1/1 >	已选择 (1)	清除
		✓ ±0/38名✓			арі	×
±1/88	已接权账户 无已接权账户、点由接权账户					
. <u>98 18 -</u>						
		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。

云堡垒机 / 人员管理 / 用户 ·	/ 用户详情		
基本信息 已授权主机	已授权主机组	用户公钥	
授权主机组 搜索主机组	名 Q		C
✓ 主机组名		已授权账户	
		root	
✔ 移除 批量	~		总计1 く 上一页 1 下一页 > 20 条/页 >

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。

云堡垒机 / 人员管理 / 用户				
用户				
导入RAM用户 导入其他来源用户 ∨	援索用户名/姓名 Q. 以证源:金部			导出授权关系 C
用户名	姓名	认证源	摄作	
	10	本地认证	授权主机 授权主机组	
•		本地认证	授权主机 授权主机组	
解 惊 劉 除				总计 2 く 上一页 1 下一页 > 20 奥/页 ∨

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。

÷	1.0	1		
基本信息	已授权主机	已授权主机组	用户公钥	
授权主机组	搜索主机组名	Q		
主机	组名			已授权账户
				无已授权账户,点击授权账户
移	除 批量 >			
\sim				

⑦ 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。

选择账号 [1]	×
账户:	请输入想要授权的账号	

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。

云逶垒机 / 人员管理 / 用户				
用户				
导入RAM用户 导入其他来源用户 ∨	援派用户名/姓名 Q 以证源:全部 > >			导出授权关系 C
用户名	姓名	认证源	操作	
	10	本地认证	授权主机 授权主机组	
		本地认证	授权主机 授权主机组	
解锁 删除				总计2 < 上一页 1 下一页 > 20 魚/页∨

4. 选中需要授权账户的主机组并单击批量 > 批量授权账号。

基本信息	已授权主机	已授权主机组	用户公钥	
授权主机组	搜索主机组名	Q		
主机线	且名 批·母抵权1	K 🗠		已授权账户
~	批量移除批	受权账号		无已授权账户,点击授权账户
✔ 移	除 批量 >	1		

5. 在账户文本框输入主机账户名称。

批量授权账号	×
当前选择主机组数: 2 账户: user01 × user0	12 ×
更新	

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。

÷				
基本信息	已授权主机	已授权主机组	用户公钥	
授权主机组	搜索主机组名	Q		
✓ 主机	组名 批母培权[К П		已授权账户
	批量移除排	受权账号		root
✓ 移	除 批量 >]		

5. 在账户列表选中需要移除的授权账户。

批量移除授权账号		X
当前选择主机组数 : 1		
账户:	请在下拉菜单中选择或输入想要移除授权的账号	
	1000	

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。

用户组		
新建用户组 搜索用户组名称 Q		C
名称	成员数	操作
Web运维	2	授权主机 授权主机组
测试用户组	1	授权主机 授权主机组
测试组	0	授权主机 授权主机组
运维人员	0	授权主机 授权主机组
副除		总计 4 く 上一页 1 下一页 > 20 条/页 >

- 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。

Q 搜索	授权主机组	X
云堡垒机 / 人员管理 / 用户组 / 用户组详情 ← Webi云维		已选择 (2) 清除
用户组设置 用户组成员 已援权主机 已授权主机组	 主机组名 测试主机组 	数据库主机组 × web服务主机组 ×
	 次馮库主初組 web服务主机组 	
	2	
	· 通定 3	

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:

- 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。

用户组		
新建用户组 搜索用户组名称 Q		С
名称	成员数	擬(乍
Web运维	2	授权主机 授权主机组
测试用户组	1	授权主机 授权主机组
测试组	0	授权主机 授权主机组
运维人员	0	授权主机 授权主机组
制除		总计 4 く 上一页 1 下一页 > 20 条/页 >

4. 选中需要移除的已授权主机组并单击移除。

 ← Operation Group 					
用户组设置	用户组成员	已授权主机	已授权主机组		
授权主机组	搜索主机组名	Q			
■ 主机组	名			已授权账户	
				无已授权账户,点击授权账户	
				root	
■移員	€ 批量 ∨				

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。

用户	组		
新建用	户组 搜索用户组名称 Q		С
	名称	成员数	攝作
	Web运维	2	授权主机 授权主机组
	测试用户组	1	授权主机 授权主机组
	测试组	0	授权主机 授权主机组
	运维人员	0	授权主机 授权主机组
	制除		总计 4 く 上一页 1 下一页 > 20 条/页 ∨

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。

< Oper	ation Gro	up		
用户组设置	用户组成员	已授权主机	已授权主机组	
授权主机组	搜索主机组名	Q		
■ 主机	组名			已授权账户
test				无已授权账户,点击授权账户
арі				root
移	除 批量 >			

⑦ 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。

用户组			
新建用户组	搜索用户组名称 Q		С
名称		成员数	攝作
Webìź	5维	2	授权主机 授权主机组
测试用	户组	1	授权主机 授权主机组
测试组	1	0	授权主机 授权主机组
运维人	员	0	授权主机 授权主机组
册			总计 4 く 上一页 1 下一页 > 20 条/页 >

4. 选中需要授权账户的主机组并单击批量 > 批量授权账号。

← Operation Group						
用户组设置	用户组成员	已授权主机	已授权主机组			
授权主机组	搜索主机组名	Q				
■ 主机组	名			已授权账户		
	北母塔权所有	1		无已授权账户,点击授权账户		
	批量移除授机	2016号		root		
■移員	余 批量 ∨					

5. 在**账户**文本框输入账户名称。

批量授权账号		Х
当前选择主机组数: 1		
账户:	请输入想要授权的账号	

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。

用户组	8		
新建用户组	且 搜索用户组名称 Q		С
2	S称	成员数	攝作
□ w	Veb运维	2	授权主机授权主机组
测	则试用户组	1	授权主机 授权主机组
测	则试组	0	授权主机 授权主机组
i iz	医维人员	0	授权主机 授权主机组
			总计 4 く 上一页 1 下一页 > 20 条/页 >

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。

← Operation Group						
用户组设置	用户组成员	已授权主机	已授权主机组			
授权主机组	搜索主机组名	Q				
■ 主机组	招			已授权账户		
	米母塔拉呢	1		无已授权账户,点击授权账户		
	批量移除授权	。 2账号		root		
■移	除 批量 >					

5. 在账户列表中选中需要移除的授权账户。

批量移除授权账号	<u>a</u>		Х
当前选择主机组数: 2	2		
账户:	user01 × user02 ×		
	root		
	user01	~	
	user02	\checkmark	
	admin		
更新			

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。

* 授权规则名称: 	新建授权	规则				
授权规则有效期: 开始日期 ~ 结束日期 日 留注:	* 授权规则	名称:				
授权规则有效期:						0
开始日期 ~ 结束日期 芭 备注:	授权规则有	夏效期:				
备注:		开始日期	~	结束日期	Ē	
	备注:					
						0

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。

主机	批量授权账号			
С	批量移除授权账号	Q, < 1	/ 1 >	
移除	批量 > 关系	关主机 总计 9 当前选·	⊉ 1	
	主机IP	主机名	操作系统	已授权账户
	192.168.2	ali自带的操作系统	Linux	root, test1
	47.100.24	iZuf6haqe74ea52c4	Linux	无已授权账户,点击授权账户
	192.168.2.	centos8.3操作系统	Linux	root, test1
	192.168.2.	centos7.2操作系统	Linux	无已授权账户,点击授权账户
	101.132.2	网络代理服务器1	Linux	无已授权账户,点击授权账户

- 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

- 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. 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。

云遥垒机 / 策略 / 控制策略							
控制策略							
新建拉制策略 提素拉制策略名称 Q							С
名称	用户	用户组	主机	主机组	优先级	摄作	
	2	0	所有	所有	2	編輯 删除	
	3	0	1	0	3	编辑 删除	
	1	1	1	0	4	编辑 删除	
劃除						息计 3 < 上一页 1 下一页 >	20 条/页 \/

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。

云堡垒机 / 策略 / 控制策略 / 控制策略详情								
控制策略详情								
<								
控制策略设置	命令控制	命令审批	协议控制	访问控制	主机/用户			
* 名称								
					0			
优先级								
2					0			
备注								
				/				

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。

云堡垒机 / 策略 / 拉制策略							
控制策略							
新建控制策略 搜索控制策略名称 Q							С
名称	用户	用户组	主机	主机组	优先级	攝作	
	2	0	所有	所有	2	编辑 自動除	
	3	0	1	0	3	編輯 删除	
	1	1	1	0	4	編輯 删除	
一 胞 除						息计3 < 上一页 1 下一页 >	20 条/页 \

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。

云堡垒机	/ 策略 / 控制策略							
控制	策略							
新建的	制策略 提案控制策略名称 Q、							С
	名称	用户	用户组	主机	主机组	优先级	操作	
		2	0	所有	所有	2	編輯 删除	
		3	0	1	0	3	編輯 删除	
	1.0	1	1	1	0	4	編輯 删除	
	刑 除						总计3 < 上一页 1 下一页 > 20	姜/页∨

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。

⑦ 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。

控制策略设置 命令控制 命令审批 协议控制 访问控制 主机/用户	
 ○ 病職+1次將有主机生效 ● 病職+17已恐得的主机生效 	
主机	主机组
C 搜索主机名/主机P Q < 1 / 0 >	C 撤票主机组合称 Q_ <
移 除	
57.80A	19元0月

⑦ 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。

	用户组	
C 搜索用户名/姓名 Q < 1 / 1 >	C 撤宽用户组合称 Q < 1 / 0 >	
移除 关联用户 总计3 当前选中0	修除 关联用户组 总计 0 当前四十 0	
SI		
	· · · · · · · · · · · · · · · · · · ·	

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。

云堡垒机 / 审批 / 命令审批						
命令审批						
捜索命令审批 へ 状态:全部						С
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	状态
39 91 linux	SSH root	146	catd 1	2020-04-09 17:55:32		已取消
3 91 linux	SSH root	146	catdddd	2020-04-09 17:35:41		已取满
91 linux	SSH root	146	catd	2020-04-09 17:34:59		已取満

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。

云堡垒机 / 审批 / 命令审批								
命令审批								
捜索命令审批 Q	状态:全部 ^]					С	
□ 主机	状态: 全部 🗸 🗸	主机帐户	用户/来源即	#\$	申请时间/审批时间	軍批人	状态	
3 91 linux	得审批 已取消		146	catd 1	2020-04-09 17:55:32		已取消	
3 91 linux	已允许 已拒绝		146	catdddd	2020-04-09 17:35:41		已取消	

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。

云堡垒机 / 审议	+ / 会话审计			
会话审	计			
所有会话	图像文字 字符命令 文件传输			
时间:	全部 本目 本周 开始日期	~	结束日期	明
协议:	全部	\sim	主机IP:	请输入主机IP
主机名:	请输入主机名		用户:	请输入用户名
登录名:	请输入登录名		来源IP:	请输入来源IP
会话ID:	请输入会活ID		删除状态:	全部 🗸
	搜索 重置			
查询条件:	清除保存			默认条件 🗸 🗸

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。

⑦ 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。

类型	主机	协议/登录名	用户/来源IP	开始时间/结束时间	会话时长/会话大小	会话操作
RDP	1	RDP administrator	****	2019-10-15 16:10:16 2019-10-15 16:21:34	11分18秒 0.33MB	播放详情
SHELL	1 c	SSH root	225.	2019-10-08 10:52:13 2019-10-08 11:24:32	32分19秒 1.31KB	播放详情
RDP	1	RDP administrator	225.	2019-10-08 10:46:49 2019-10-08 10:51:23	4分34秒 0.34MB	播放详情
RDP	1	RDP administrator	1000	2019-10-08 10:45:24 2019-10-08 10:46:17	53秒 2.78MB	播放详情

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。

会话详情			×
会话ID	2ee86	20008	
会话时长	11分18秒	会话大小	0.33MB
开始时间	2019-10-15 16:10:16	结束时间	2019-10-15 16:21:34
用户	10,000	来源IP	42 89
来源MAC	E F:FF	来源端口	2059
主机名	Windows堡垒机测试-zqy	主机IP	1 140
登录名	administrator	协议	RDP
主机MAC	FF	主机端口	3389

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。

类型	主机	协议/登录名	用户/来源IP	开始时间/结束时间	会话时长/会话大小	会话操作
RDP		RDP administrator	****	2019-10-15 16:10:16 2019-10-15 16:21:34	11分18秒 0.33MB	播放详情
SHELL	1 c	SSH root	25%	2019-10-08 10:52:13 2019-10-08 11:24:32	32分19秒 1.31KB	播放 详情
RDP	1	RDP administrator	225.	2019-10-08 10:46:49 2019-10-08 10:51:23	4分34秒 0.34MB	播放详情
RDP	1	RDP administrator	100	2019-10-08 10:45:24 2019-10-08 10:46:17	53秒 2.78MB	播放详情

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。

⑦ 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。

<	日志审计服务	③ 全局配置 × □ 温金机 ×											
(D)	∨ 會 申ù化	全局配置 9 半航全局配置需要重新配置				田 保存							
GD	• 🛞 攝作审计 (ActionTrail)												
B	• 👩 OSS	中心项目Project所在区域: 华东1 (杭州)	~										
(9	• 🐨 RDS	← Φ-OProject: sisaudt-conter-1325883845821272-cn-hangzhou ElifeProject: sisaudt-region-1325883845821272-(Elife;E)											
	• 😞 PolarDB-X	深集编章操程: ② 點前期等已變成日告聽對系集局的日志											
	 曲 堡垒机 												
	• 🔞 应用防火増 (WAF)	云产品	审计相关日志	采集策略	存储方式	同步到中心 ⑦							
	* (m) 云防火堤	💮 操作审计 (ActionTrail)	● 操作日志		中心化 () 180 天								
	• 🗼 API网关	0\$\$	() 访问日志		区域化 🕤 7 天	180 天							
	* (2) NAS		- () 计量日志		中心化 ③ 180 天								
	 ·	😍 RDS	SQL#HEE 💿	采集箱暗关闭 采集箱略	中心化 ③ 180 天								
		PolarDB	() 第计日志 ()		中心化 ① 180 天								
		🛞 PolarDB-X	SQL單计日志	预设 采集策略	区域化 ⑦ 7 天	180 天							
		🙏 SLB	7层访问日志	要设 采集箱略	区城化 🕥 7 天	180 天							
			操作日志		中心化 ① 180 天								
		🧑 应用防火墙 (WAF)	(1) 访问日志 (1)		中心化 ① 180 天								
		(意) 云筋火境	互联网访问日志 ()		中心化 ① 180 天								
		🧭 云安全中心 (SAS) 📉	() © 7#101 0		中心化 ⑦ 180 天								
		API阅关	10月1日志		中心化 ⑦ 180 天								
		🐻 NAS	访问日本		中心化 🕥 180 天								
		🔤 移动推送	推送回执事件		中心化 ③ 180 天								
		Kubernetes	K8s审计日志	采集策略关闭 采集策略	中心化 ⑦ 180 天								
			- K8s事件中心	采集策略关闭 采集策略	中心化 ⑦ 180 天	· 返田 日報							
			_ Ingress访问日志	尿樂策略关闭 尿樂策略	中心化 () 180 天								

- 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。

所有会话 图像文字 字符命令 文件传输 日志备份 名称 文件大小 开始备份时间 备份结束时间 操作 2021-04.csv 22.06KB 2021年4月28日 08:00:00 2021年4月29日 08:00:00 下戦 K 22.06KB 2021年4月28日 08:00:00 企業 20.14年月29日 08:00:00 「大戦	云堡垒机 / 审计	/ 会话审计						使用向导 >
所有会话 图像文字 字符命令 文件传输 日志备份 名称 文(十) 开始备份时间 备份结束时间 操作 2021-04.csv 22.06KB 2021年4月28日 08:00:00 2021年4月29日 08:00:00 下载 KUT 大山、一页 1 下一页 > 20.96/07	会话审证	, †						
名称 文件大小 开始备份时间 备份结束时间 操作 操作 2021-04.csv 22.06KB 2021年月28日 08.00.00 2021年月29日 08.00.00 下或 1 下の、 20.9.07	所有会话	图像文字	字符命令	文件传输	日志备份			
2021-04.csv 22.06KB 2021年4月28日 08:00:00 2021年4月29日 08:00:00 下載 <	名称		文件	#大小	开始备份时间	备份结束时间	操作	
总计 1 く 上一页 1 下一页 > 20 条/页	2021-04.csv		22.0	06KB	2021年4月28日 08:00:00	2021年4月29日 08:00:00	下载	
							总计1 〈 上一页 】 下一页 〉	20条/页

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。

云堡垒机 / 审计 / 突时监控										
实时监控										
协议:	全部 🗸	主机IP:	请输入主机P							
主机名:	请输入主机名	用户:	请输入用户名							
登录名:	请输入登录名	来源IP:	请输入来源IP							
会话ID:	请输入会活ID									
	搜索重置									
查询条件:	清除保存		默认条件 🗸							

您可以参考以下表格中的搜索项说明设置搜索条件。

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

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。

⑦ **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。

实时监持	空	会话详情				×			
	_								
协议:	全部	会话ID	7e006)00000a			LIP		
		会话时长	0秒	会话大小	OB				
用户:	请输入用户省	开始时间	2019-10-12 17:38:57	结束时间	-				
来源IP:	请输入来源IP								
	搜索	用户		来源IP	2.				
查询条件:	清除	来源MAC	E F:FF	来源端口	2090			默认条件	\vee
类型		主机名	堡垒机-linux	主机IP	10. 223		1间/时长	会话操作	
SHEL	L	登录名	root	协议	SSH		10-12 17:38:57	播放 洋情	
		主机MAC	EE: FF	主机端口	22				
	断会话						总计1 < 上一页	1 下一页 > 20	条/页 🗸
									÷

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。

实时监控											
协议:	全部			\sim	主机:	请输入主机	治/主机IP				
用户:	请输入用户名				登录名:	请输入登录名					
来源IP:	请输入来源IP				会话ID:	请输入会语					
	搜索	重置									
查询条件:	<mark>清</mark> 除	保存							默认条件	\sim	
- 类型		主机	协议/登录名	用户/	′来源IP		开始时间/时长		会话操作		
SHE	LL	堡垒机-linux	SSH root	2	eshi 146		2019-10-12 17:38:57 1分8秒		播 放 详情		
	断会话						总计 1	< 上一页	1 下一页 > 2	20 条/页	

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。

实时监持	空					
(4)公	◆ #8		~	主 机 ·	法给λ 士机么/土机D	
用户:	请输入用户名			登录名:	请输入登录名	
来源IP:	请输入来源IP			会话ID:	请输入会活ID	
	搜索重置					
查询条件:	清除保存					默认条件 🗸 🗸
✓ 类型	主机	协议/登录名	用户	/来源IP	开始时间/时长	会话操作
SHEL	223 堡	SSH root	z 22	hi 46	2019-10-12 17:38:57 4分17秒	播放 详情
	所会活				总计 1 〈 上一引	页 1 下一页 > 20条/页 ∨

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。

⑦ 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		42 164	成功
2020-04-29 17:02:20	AddUsersToGroup		42 64	成功
2020-04-29 16:12:49	RemoveHostsFromGroup		42. 64	成功
2020-04-29 16:10:52	AddHostsToGroup	ALC: NO. 10.10	42. 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00:00-3前时间。
昨日	时间范围:昨天的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。

总路 会话大小 运進次数 运维时长			
总体		运维次数	
运维主机款	7	息运维欠数	32
运维来源IP数	3	SSH	28
运维用户数	4	RDP	4
		SFTP	0
		平均每日运维次数	1.3
运维时长		会话大小	
总运建时长	1 时 52 分 44 秒	总会适大小	16.26MB
SSH	1时46分24秒	SSH	71.53KB
RDP	6分20秒	RDP	16.19MB
SFTP	0秒	SFTP	08
平均每日运维时长	4分41秒	平均每日会适大小	693.57KB
最大运進时长	37 分 49 秒	最大会活大小	10.18MB
最小运维时长	0秒	最小会活大小	ов

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。

1025/P	
15U/MB	
1096	
3500	
4708	
0	时间
● 554 ● 40 P ● 517 ● 518	
7475	
H%289	
118 14 20 277 <u>Bit</u>	
2022/#15/9/12-02/195/9/12 06 08 08	
2021#3/F1E-2021#3/F1E 9.47/63 09 9.47/6	
2011부터 여 여 여 여	
2011년8月7日-1021년8月31日 62.84년 16.194년 68 16.234년	
2014년(AUE-1014년)(AUE-1014)	

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。

运维报表				
日期:	本日 昨日 本周 本月 2021-05-27 00:000 ~ 2021-05-27 15:40:44 🗇 💿	导出报表 ∨		
总览	会活大小 运嫌次数 运播时长			
趋势资				
接小时 缺天 他間 做月				

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。

⑦ 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。

⑦ 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。

主机运维						
搜索主机名/主机P Q	撮作系统: 全部 ∨	主机来源:全部 🛛 🗸				
主机名	主机P	备注	操作系统	主机来源	主机账户	登录
	172.16		Linux	ECS	[SSH] root \lor	۲
banner测试-ubuntu20	192.1		Linux	ECS	[SSH] root \lor	۲
banner测试-centos7.5	192.1		Linux	ECS	[SSH] root \lor	۲
win测试2019	116.6		Windows	ECS	无已授权主机账户	
linux词定	121.43		Linux	ECS	[SSH] root \lor	-
1.1.1.1_ApiTest		APItest	Windows	Local	无已授权主机账户	49

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。

⑦ 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		
	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。
用户锁定配 置	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。
	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。
用户状态配 置	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。

云堡垒机 / 人员管理 / 认证设置			
认证设置			
安全配置 双因子认证 AD	以证 LDAP认证		
* 服务器地址:	11 = 109		
备用服务器地址:		0	
* 端口:	=		
SSL:			
* Base DN :	dc=ad-server,dc=com		
* 域:	a m		
* 账号:	a or		
* 密码:	ø		
过滤器:		0	

- 9. 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。

云堡垒机 / 人员管理 / 认证	段置		
认证设置			
安全配置 双因子认	证 AD认证 LDAP认证		
* 服务器地址:	1000000-0-		
备用服务器地址:		0	
* 端口:			
SSL:			
* Base DN :	d m		
* 账号:	an Anna an Anna Anna Anna Anna Anna		
* 密码 :	····· Ø		
过滤器:		0	
登录名属性:		0	

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。

系统设	豊									
安全配置	双因子认证	AD认证	LDAP认证	运维配置	网络诊断					
连通性测试 * 目标地址:			ww.example	2						
* 端口:			80							
			测试连接							

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。		
		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。		
	允许开启个性化桌面	⑦ 说明 个性化桌面会消耗大量带宽,请谨慎开 启。		

用户指南(V3.2版本)·管理员手册

配置类型	配置项	说明
告告的这时下吗?	-11	
运 维 全 闲 的 太 限 精	in the second	

堡垒机

配置类型	配置项	说明
运维总时长限制		

用户指南(V3.2版本)·<mark>管理员手册</mark>

配置类型	配置项	说明
		1

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。

存储状态		
存储状态:		1%
	16.25MB / 1TB	

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。

自动删除				
自动删除:	✓ 会话数据最大保存时长	180	天 ③	
	保存			

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。

⑦ 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。

堡垒机

2021年5月6日 09:04:54							
<< <		20	21年 4	月		> >>	
_	Ξ	Ξ	四	五	六	Β	
29	30	31	1	2	3	4	7
5	6	7	8	9	10	11	
12	13	14	15	16	17	18	
19	20	21	22	23	24	25	
26	27	28	29	30	1	2	
3	4	5	б	7	8	9	
此刻				选择	时间	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。

⑦ 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。		
	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。		
存储告警通知	⑦ 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。		
	⑦ 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。		
	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。		
共享密钥到期提醒,到期提示时间	⑦ 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。		
	当网络域代理服务异常时,堡垒机将通过站内信发送通知。		
网络域代理告警通知	⑦ 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。
- 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。

⑦ 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
- SFT P协议运维

Mac客户端运维

- SSH协议运维
- RDP协议运维
- SFT P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。

云堡垒机 / 概范					
统计概范				运维入口	
A.用户	魚 用户组	UP 主机	品 主机组	公网运维地址	
8	1	19	3	piumiaopkr 内网运输地址 piumiabpk	
运维统计					
14				实时会话	宣君
12				实时连接	0
10				剩余连接	50
6					0
2				活动主机	0
2020-04-23	2020-04-24 2020-04-25	2020-04-26 2020-04-27	2020-04-28 2020-04-29		
				字符	0
				图形	0
				文件传输	0

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。

新建会话属性			? ×
类别(C):			
□ 连接	连接		
	常规		
	名称(N):	云盾系统	_
⊡- SSH	协议(P):	SSH ~	
安全性 	主机(H):	cfu-public alivuncs.com	
SFTP	10000	cia public scorri	
TELNET	端口号(O):	60022	
- RLOGIN SERIAI	说明(D):	^	
代理			
保持活动状态		×	
□ □· 終端 ####	重新连接		
		时自动重新连接(A)	
高级			
□□ • 外观	间隔(V):	0 ▲ 秒 限制(L): 0	- 分钟
~ 突出			
□. 高级	TCP选项		
	□ 使用Nagle算	法(U)	
日志记录			
→文件传输			
ZMODEM			
			TTP:///
		连接 确定	取消

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。

新建会话属性			? ×
类别(C):			
□·连接	连接 > 用户身份验证		
□ 用户身份验证	请选择身份验证方法和非	其它参数。	
登录脚本	使用此部分以节省登录	时间。但是,为了最大限度地提高安全性,	如果担心安全问题,
⊡- SSH	建议您将此部分留空。		
安全性			
·····································	±;±(►4).	Descovord	27.要70)
TELNET	万/云(IVI);	*	反亘(5)…
RLOGIN	用户名(U):	zha na e shi	
SERIAL	密码(P):	•••••	
保持活动状态	用户密钥(K):	<无> ~	刘贤(B)
□· 终端	577 (A)		1/33/0/1/11
键盘	出(H);		
高级			
□ 外观	注释: 公钥和Kevboard	Interactive仅在SSH/SFTP协议中可用。	
窗口	, <u></u> ,,		
□ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○			
日本の			
钟			
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□			
X/YMODEM			
ZMODEM			
	1	连接 确定	取消

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**。

Ture Char	Mentionation follows interest and and	~
Two-step	vertication failure, please try again	\sim
23	Please enter the MFA verification code:	^
		\vee

	□记住密码(R)	
	确定取消	

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。

ext/privous searching result.
er}.
host}:{port} [-p port] <enter>" for login.</enter>
] <enter>" for check host status.</enter>
UTF-8 and GB2312.

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(Mst sc)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。

云堡垒机 / 桐览					
統计概范 《用 ^{pp} 8	奏 用户组 1	中主机 19	点 主印紙 3	送後入口 公院活体地注 planiaby注 planiaby注 planiaby注 planiaby注 planiaby注 C	
运维统计 14 12 10 8				实时会话 实时法师 前会连接	宣吾 0 50
		2020.04.07	2020 04 25	活动用户 活动主机	0
2020-04-23	2020-04-24 2020-04-25	2020-04-28 2020-04-27 字符 💊 四形 💊 文件传輸 ∿ 总数	2020-04-28 2020-04-29	字符 图形 文件得输	0 0 0

操作步骤

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

퉣 远程桌面连	接	_		\times
تَن 😽 🐱	起程桌面 连接			
计算机(<u>C</u>):	escfu-public.basses	.com:63389 ∨		
用户名:	未指定			
当你连接时将向	向你询问凭据。			
💽 显示选项(<u>O</u>)	连接(<u>N</u>)	帮助(上	<u>1</u>)

3. 在远程桌面连接提示框中,单击是。

1号 远程桌面连接 ン	<
无法验证此远程计算机的身份。是否仍要连接?	
由于安全证书存在问题,因此远程计算机无法通过身份验证。继续操作可能不安 全。	
名称不匹配	
19 请求的远程计算机:	
ylbnç s.com	
📮 来自远程计算机的证书中的名称:	
BAOLEIJI	
证书错误 验证远程计算机的证书时遇到下列错误:	
⚠ 证书上的服务器名错误。	
▲ 证书来自不信任的证书验证机构。	
你想连接到远程桌面而忽略这些证书错误吗?	
□不再询问我是否连接到此计算机(D)	
查看证书() 是() 否()	

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**。

双因子口令:	
9	
Please enter the MFA de:	verification co
确认	取消

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。

主机名	IP	账户名		端口	
差垒机-windows	101 .54	adı tor	3389		
				_	
				修改个人密码	注销

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。

堡垒机 / 概范					
统计概范 A.用户 8	朱.用户组 1	中主机 19	あ 主印組 3	道後入口 公照道地址 pluniabokr O 内照道地址 pluniabok O	
运编统计 14 12 10 8				实时会话 实时绘话 刻余处语	2 1
6 4 2 0				活动用户 活动主机	
2020-04-23	2020-04-24 2020-04-25	2020-04-26 2020-04-27 字符 💊 図形 💊 文件核編 ∿ 总数	2020-04-28 2020-04-29	字符 图形	1

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。

新建会话属性		? ×
常规 选项		
FTP 站点		
名称(N):	云盾系统	
主机(H):	bli com	
协议(R):	SFTP ~	设置(S)
端口号(O):	60022	
代理服务器(X):	<无> ~	浏览(W)
说明(D):		
登录		
■ 匿名登录(A)		
□使用身份验证代理(G)		
方法(M):	Password 🗸	
用户名(U):	zha	
密码(P):	•••••	
用户密钥(K):	~	浏览(B)
密码(E):		
	确题	Ē 取消

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。

A state of the set			* * `	<i>y</i> 7-							-t+ 777	
◎ 王机名或IP地址							_			• 用户名	密码	
桌面 ×					\rightarrow	● 云盾系统	×					
🔲 💻 桌面				~ 13	с 🗉 -						~ 🖬 (0 🗖
三 桌面	名称	大小	类型	修改时间	^	••• <mark>•</mark> /	名称	大小	美型	修改时间	属性	所有者
🗉 🤱 Administrator			系统文件夹	1970/1/1 星期四, 8:00			Inow_gb18030,next		文件夹	2019/10/14 星期一, 11	drwxr-xr-x	2
● — — 此电脑	控制面板		系统文件夹	1970/1/1 星期四, 8:00			ssh_root@堡垒机-lin		文件夹	2019/10/14 星期—, 11	drwxr-xr-x	2
	库		系统文件夹	1970/1/1 星期四, 8:00							4	
	🚅 网络		系统文件夹	1970/1/1 星期四, 8:00								
	Administrator		系统文件夹	2019/9/17 星期二, 14:								
	Sector Control to	1KB	快捷方式	2019/5/29 星期三, 10:								
	Berne Contractor	1KB	快捷方式	2019/5/29 星期三, 10:								
	A Real Property lies	644 Bytes	快捷方式	2019/5/29 星期三, 9:25								
	Sec. 11	714 Bytes	快捷方式	2019/8/19 星期—, 17:								
	State Street	738 Bytes	快捷方式	2019/5/29 星期三, 10:								
		2KB	快捷方式	2019/6/20 星期四, 15:								
		828 Bytes	快捷方式	2019/5/28 星期二, 17:								
		1KB	快捷方式	2019/6/1 星期六, 11:29								
		1KB	快捷方式	2019/5/31 星期五, 18:								
		2KB	快捷方式	2019/5/29 星期三, 9:18								
		2KB	快捷方式	2019/9/12 星期四, 12:								
	and the second sec	849 Bytes	快捷方式	2019/5/31 星期五, 13:								
		4KB	快捷方式	2019/10/10 星期四, 16								
-		742 Bytes	快捷方式	2019/9/17 星期二, 14:	~		<					,
输日志												
称	状态 逆	疲 大/	k.	本地路径	<	-> 远程路径	速度	估计剩余				

- 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。
 - ⑦ 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)。

• • •	👚 admin — ssh zhai	shi@yll	.com -p60022 -	- 101×24
admindeMac-mi	ini:~ admin\$ ssh zha	shi@yll	particular and the second second	.com -p60022
zha	shi@yll	\$.C	com's password: 🦹	

- 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)。

 Image: Shi@ylb
 .aliyuncs.com -p60022 — 101×24

 IadmindeMac-mini:~ admin\$ ssh zhang
 shi@ylb
 .aliyuncs.com -p60022

 Izhang
 shi@ylb
 .aliyuncs.com's password:

 Two-Step Vertification required
 Please enter the MFA verification code:

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。

۲			admin — USMShell — ssh zhang shi@ylb .aliyuncs.com -p60022 — 101×24	
["				
	Quit:	Use	":q <enter>".</enter>	
	Move:	Use	the cursor keys, or "j" to go down, "k" to go up, "u" to PageUp, "p" to PageDown.	
	Search:	Use	"/{patten} <enter>" and then "n"/"N" to next/privous searching result.</enter>	
	Jump:	Use	":{number} <enter>" to jump to line {number}.</enter>	
	Command:	Use	":[ssh telnet rlogin] [-l user] {user}@{host}:{port} [-p port] <enter>" for login.</enter>	
		Use	":[ping traceroute connect] {host} [port] <enter>" for check host status.</enter>	
	Refresh:	Use	"r" to refresh lists.	
	Language:	Use	"e" to change language encoding between UTF-8 and GB2312.	
	Lusmshell	J +n n.		
	001: 季至,	NC - T:	INUX 101.57 0.223:22 SSN FOOT	

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。

9 用户 8	魚 用户组	(7) shaft		通道へ口	
3	风田戸垣		P ++0.40	A TRANSPORT	
	1	19	as ±0.68 3	22/Habenese plumlabpk/	
国编统计				实时会话	3
12				实时连接	
8				剩余连接	
6				活动用户	
2	<u></u>			活动主机	
2020-04-23	2020-04-24 2020-04-25	2020-04-26 2020-04-27	2020-04-28 2020-04-29		
	n :	字符 💊 図形 💊 文件传输 ∿ 总数		210	

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。

	远程桌面连接
Ma 通	斷 開于 Mac 的远程桌面连接
计算机	: ylbnaliyuncs.com:6 连接 (示例: MyPC, name.microsoft.com, 192 2.8)

3. 输入云盾堡垒机的用户名和密码,单击登录。

登录	
用户名:	
密码:	
	登录
	退出

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**。

双因子口	令 :				
9					
Please de:	enter th	ne MFA	verif	ication	со
	确认			取消	

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。

1.17.6	10	n k+ 4		
王机名 举机-windows	101 .54	u 账户名 adu cor	3389	端口
ETA NTHONS	101	201 201	0000	J

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。

云堡垒机 / 桐览					
統计概范 A用户 8	み用 ^{の祖} 1	中主机 19	点 主11/8 3	接後入口 小和回答的法 plustingpy 内別回答的法 plustingpy の	
运输统计 14 12 10 8				实时会话 实过进程 剩余进程	查看 0 50
6 4 2 2020-04-23	2020-04-24 2020-04-25	2020-04-26 2020-04-27	2020-04-28 2020-04-29	活动用户 活动主机	0
	∿ 9	帯 • 野形 • 文件検描 • 息数		李符 图形 文/持续编	0 0 0

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。

			💯 SecureFX					
Connect Syn Lze	Download Refresh Stop Folder Tree							
💿 🔄 Local (adminde	Mac-mini.local)							
/							▼ Filter <%F>	*
Y ↓ / Cocumer Jewents Je	Revis d sandb V100 rs d bin c Spolight-V100 rol c Spo	sions-V100 oxManager oxManager-Sy	Size Type Directory Directory Directory Directory Directory Directory Directory Directory Connect Sessions Close Urectory Directory	íň 🔹 »	Date Modified 10/14/19 14:40 10/14/19 14:40 10/14/19 14:40 10/14/19 14:24 10/14/19 14:24 10/14/19 14:24 10/14/19 14:38 10/14/19 14:38 10/14/19 14:40 10/04/19 14:40 10/04/19 15:04 09/20/19 12:34 10/14/19 15:04 09/20/19 12:34 10/14/19 15:04 10/14/19 14:38 10/14/19 14:38			
0			Transfer Queue					
Filename	Destination Si	ze of File 3ytes Transferred Pro	gress Bapsed Time Time Left Speed Statu	5	Start Time	Finish Time		

3. 输入堡垒机的运维地址、端口号(60022)和用户名, 单击OK。

	💯 Session Options - New				
Category:	SSH2				
 Connection SSH2 Advanced File Transfer FTP/SFTP Advanced 	Hostname: ylbn				
	Key exchange ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14 diffie-hellman-group-exchange-sha256 Minimum group exchange prime size: 2048				
	Cancel 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。

	💯 Enter Secure Shell Password	
ylbr requires a p	aliyuncs.com. assword. Please enter a password now.	ОК
Username:	zhanç shi	Cancel
Fassword:	•••••	
Save password		Skip

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。

💿 💿 💿 🌠 Two-Step Vertification required Auth	nentication
Two-Step Vertification required prompt for zhang shi@ylbraliyuncs.com.	OK
Please enter the MFA verification code:	
03	Skip

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。

⑦ 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。

		🗐 Se	cureFX			Orenert Bar	
Connect Synchronize Download	cal)		0 🖾 111			Connect Bar	
1	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Filter <%F>	1			✓ Filter <%F>	~
✓ ✓ /	Name f.seventsd P.KinstallSandboxManager P.KinstallSandboxManager-Sy Spotlight-V100 Applications bin cores dev etc home Library net Network private abin System trp Users usr var	Size	 ▼ ► / ► Inow.gb18030,nex ► ssh_root@±#ÀY#ú (5000 : Real/Rath, base (Real/Wed Real/Rath) (draw-xr-x 4995 Mon 14-0ct. <	Name Inow ssh.ro 2019 17:52:17 Inoxgb18035	Size Type Directory Directory ,next_UTF-8 (5) Yeo-1 Inux_181 2	Date Modified 10/14/19 17:52 10/14/19 17:52	
vm						(-/	
28 entries (plus 2 hidden entrie	es)		2 entries				
0		Tran	ifer Queue				
Filename Dr	estination Size of File 3ytes Transferred	Progress ::lapsed Time Time Le	ft Speed Status	Start Time	Finish Time		