

Alibaba Cloud

堡垒机 快速入门

文档版本: 20220210



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。	
▲ 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) 注意 权重设置为0,该服务器不会再接受新 请求。
⑦ 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。	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.概览	05
2.启用堡垒机	06
3.登录堡垒机系统	08
4.步骤1:同步阿里云ECS资产	10
5.步骤2:导入阿里云RAM用户	14
6.步骤3: 创建运维规则	15
7.步骤4:主机运维	18
8.步骤5:审计运维会话	19

1.概览

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

在使用V3.2版本堡垒机时,您可以按照以下步骤进行操作。

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

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

2. 启用堡垒机

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

背景信息

新购买的堡垒机实例处于未初始化状态,需要启用后才能使用。

操作步骤

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

*	表初始化				
标表	签 出口IP 砌始化	版本	规格	到期时间	启用
		企业版	50 资产 全升配	2020年6月23日 🛞 续费 释放	

3. 在启用面板上,完成以下配置。

启用		×
网络	请选择专有网络 >> 请选择虚拟交换机 >>	
安全组	请选择 ✓ 选择后,允许堡垒机访问安全组内的ECS ()	

配置说明如下表。

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

配置项	说明
	选择ECS对应的安全组。
安全组	 ⑦ 说明 • 堡垒机至少要加入一个普通安全组后才能启用,支持在启用后修改堡垒机所属安全组。堡垒机加入普通安全组后会自动生成访问规则,允许堡垒机访问该安全组内的ECS资产。 • 您也可以为堡垒机手动配置安全组访问规则。配置安全组访问规则后,堡垒机无须再加入安全组。配置安全组访问规则的具体操作,请参见添加安全组规则。 • 堡垒机不支持加入企业安全组,需手动配置企业安全组访问规则实现网络互通。配置安全组访问规则的具体操作,请参见添加安全组规则。

4. 单击**确定**。

单击确定后,堡垒机实例会进入**初始化中**的状态。

⑦ 说明 初始化需要20分钟左右,请您耐心等待。初始化结束后,堡垒机实例会进入运行中的状态,表明该堡垒机实例已成功启用。

初始化中未命名				
标签 出口IP	版本	规格	到期时间	创建中
公网 私网	V3.2.18	基础版 50 资产	2021年6月16日 😌 续费	

执行结果

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

运行中				
标题 山口IP	版本	规格	到期时间	管理
公网 ijvbisf On	V3.2.18 新版本 ⑦升级	高可用版 50 资产 👲 升配	2021年9月7日 间 续费	

3.登录堡垒机系统

本文介绍了如何通过Web方式登录堡垒机系统。

背景信息

⑦ 说明 支持阿里云主账号和RAM账号登录堡垒机Web界面。

操作步骤

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



3. 在堡垒机实例列表中, 单击目标实例右侧的管理, 进入堡垒机系统。

运行中 bastionhost				
华东1(杭州)				會理
标签	版本	规格	到期时间	BAT
☆ (7305		
私 (3)	配置 企业版	50资产 🏦 升配	2019年11月16日 😝 续费	

4. 选择接入方式,连接目标堡垒机Web 管理页面。

云堡垒机	云堡垒机 / 构造					使用向导 >
概章 🕕	统计概况				0	春户端运进入口 《
资产管理 ^	A用户	私 用户组	中主机	品 主机組		公网运维地址
主机	4	0	6	3		psrrcom C 内网运输地址
主机组						psr com 🕽
人员管理 ^	运维统计				0	
用户	2					实时会话
用户组	1.5					※时法援 0 第6会社課
策略 ^	1					NIGVEDK
控制策略	0.5					活动用户 0
审批 ・	0	3 2020年7月21日 2020年7月22	B 2020年7月23日	2020年7月24日 2020年7月25日		MA40205 0
#i+ v	101011121711 10101112101	a, ### a, ###	 文任所能 0、 户数 			210 0 210
系统设置						図1 ¹⁰ 0 文件传輸 0
区域		说明				
1		显示系统的功能	能菜单项。			
2		统计用户、用	户组、主机	、主机组等信息。		
3		运维的内网和:	外网口。			
4		运维统计信息。	D			

最近运维的概况信息。

5

4.步骤1:同步阿里云ECS资产

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

背景信息

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

导入阿里云ECS实例

导入阿里云ECS实例指将您阿里云账号中的ECS实例列表同步到云盾堡垒机系统中。该操作不会影响您阿里云 账号中的ECS实例的现有状态。具体参见以下步骤:

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

	(kille a	(KII) 2	(k)), F
1924 1	<u>१</u> ६२८ २	¥≌⊼C 3	1997년 5
华东1	华东 2	华南1	西南1(成都)
香港	亚太东北 1 (东京)	亚太东南 1 (新加坡)	亚太东南 2 (悉尼)
亚太东南 3 (吉隆坡)	亚太东南 5 (雅加达)		
洲与美洲			
美国东部1(弗吉尼亚)	美国西部1(硅谷)	英国 (伦敦)	欧洲中部1(法兰克福)
东与印度			
亚太南部 1 (孟买)	中东东部1(迪拜)		

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	搜索主机名/主机IP	○ 区域: 全部	∨ 网络类型: 全		
•	名称	内网IP	公网IP	区域	网络类型
~	数据 务器		10.000	华北 2	专有网络
~	数据		10000	华东 2	专有网络
~	launc	10.00		华东 2	专有网络
	launc			华东 2	专有网络
	iZbp:		11232	华东1	专有网络
	数据) 机			华东1	专有网络
	数据/ 例部2			华东1	专有网络
	dbte:			华东1	专有网络
	数据/		10000	华东 1	专有网络

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	X
请确认主机或ECS实例上已经创建了对应的操作系统账户,堡垒机不会将 户同步到主机或ECS实例。	E 机账
* 协议 SSH	
* 登录名 bastiononaliyun.com	
认证类型	
密码 > 密码	
Ø	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	> ■ 主机 >
■ 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 >	172.16.2 。 新增账户
v net	清除主机指纹	删除账户
■删除	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**。

5.步骤2:导入阿里云RAM用户

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

前提条件

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

操作步骤

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

⑦ 说明 如果需要导入单个RAM用户,您可以直接在该用户的操作列中单击导入。

5. 单击导入。

导入完成后,用户即可使用已导入的账号登录堡垒机。

6.步骤3: 创建运维规则

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

授权主机

为用户授权主机,具体操作请参见以下步骤:

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

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 🛛 🗸		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. 在已授权主机页签下,单击授权主机。
- 5. 在授权主机面板上的主机列表中选中要授权的主机,单击确定。

授权主机账户

为用户授权单个主机的登录账户,具体操作请参见以下步骤:

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

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 🛛 🗸		导出授权关系 C
用户名	姓名	认证源	操作	
		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。

			. 解决方案和资源 壽用]	选择账号 -linux]	×
云遥垒机 / 人员管理 / 用户 / 用户详情				_	
← jialin				[SSH] root	
基本信息 已授权主机 已授权主机组 用户公钥					
授权主机 推察主机IP/主机系 Q 操作系统 全部					
主机P	主机名	操作系统	已援权账户		
10 23	linux	Linux	root		
修設 批量 ∨					

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 / 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 🛛 🗸		导出授权关系 C
用户名	姓名	认证源	操作	
		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 / 人员	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	a Q	操作系统: 全部	~		
🔽 主机	,IP 批量授权则	6月		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	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。

7.步骤4: 主机运维

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

CS运维指运维人员通过本地客户端工具登录云盾堡垒机,访问目标服务器主机进行运维。该运维方式支持Windows和Mac操作系统。

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

8.步骤5: 审计运维会话

当堡垒机用户通过SSH、RDP、SFTP协议方式登录云盾堡垒机并对已授权服务器进行运维操作时,管理员可 以在云盾堡垒机审计 > 实时监控页面查看用户会话的详细信息。本文将指导管理员在堡垒机实例中进行审 计查询和阻断高危会话。

搜索会话

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

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

您可以参考以下表格中的搜索项说明设置搜索条件。

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

4. (可选)单击保存,在查询条件名称中输入名称,单击确定,保存查询条件。

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。

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	空				
+h30.	<u>م</u> ش		→ 1 .	津奈文ナ和々た知り	
用户:	<u>キ</u> ア		登录名:	「清朝人生」が行う上がで	
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 シン
✓ 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	1 223 堡	SSH root	z hi 22 46	2019-10-12 17:38:57 4分17秒	播放 详情
~ 12	新会话			总计 1 < 上一!	页 1 下一页 > 20 条/页

4. 单击**阻断会话**。