阿里云 堡垒机

快速入门

文档版本:20181128



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
•	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。	禁止: 重置操作将丢失用户配置数据。
A	该类警示信息可能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,恢复业务所需 时间约10分钟。
	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	送 说明: 您也可以通过按 Ctrl + A 选中全部文件。
>	多级菜单递进。	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。	单击 确定。
courier 字体	命令。	执行 cd /d C:/windows 命令,进 入Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid 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。	<pre>swich {stand slave}</pre>

目录

法律声明	I
通用约定	
1 限制说明	1
2 使用说明	2
3 快速入门	5
4 3.0.X 版快速入门	12

1 限制说明

云盾堡垒机系统支持通过 SSH、SFTP、及 Windows 远程桌面等协议的方式代理接入授权的服务器,并实现全程录像。同时,支持使用标准客户端(如 Xshell、SecureCRT、PuTTY 等工具)对 授权的服务器直接进行运维连接。

使用云盾堡垒机服务前需要注意以下内容:

- 所有接入堡垒机实例的 ECS 云服务器,需要正常开机并保持运行中状态。
- 堡垒机实例与要与接入的 ECS 云服务器属于一个相同的网络环境,且可以网络连通。例如,同属于一个安全组,或同属于一个 VPC 专有网络。

2 使用说明

本文受众范围:云盾堡垒机管理员、持有阿里云账号的管理员、审计人员、运维人员。

对象

云盾堡垒机有三种对象,分别是用户、主机、和凭据。

- 用户代表技术工程师,也就是自然人,登录堡垒机时用户名即为手机号码。
- 主机是您在阿里云上的ECS实例。
- 凭据是用于登录ECS实例的用户名、密码或用户密钥。其中凭据名称用于辨识不同的凭据;登录名为要登录的ECS上的用户名(例如administrator、root);密码或密钥为该用户的密码或密钥。

授权组

授权组是将堡垒机中数个独立的对象个体联系在一起的概念,通过授权组功能可以达到控制某个用 户只能访问他权限内主机的目的。假设您单位的运维模型如下:

您在阿里云上共10个ECS实例,其中:

- 应用服务器2个(APP1、APP2)
- 数据库服务器2个(DB1、DB2)
- 中间件服务器2个(M1、M2)
- 开发测试服务器4个(TEST1-4)

您单位共有三类工作人员:

- 开发人员(devuser):负责开发产品原型,以及测试。
- 运维人员(opsuser):负责维护线上服务器和应用系统。
- 管理员(adminuser):全面协调公司内部技术人员工作,并定期进行审计。

您在ECS实例中使用三种主机账号:

- dev (不能sudo)
- ops (可以sudo)
- shadow_r00t (可以sudo)

在此模型下,就可以按照如下策略配置授权关系:

个人账号	ECS主机	主机账号	说明
devuser	TEST1-4	dev	开发人员只能使用开发 机,且使用不能sudo的 账号防止基础系统配置 被改。
opsuser	APP1、APP2、DB1、 DB2、M1、M2	ops	运维人员使用可以sudo 权限的账号维护主机基 础系统配置。
adminuser	所有	shadow_r00t	管理员使用可以sudo的 账号登录系统。

这样就可以通过授权组实现职责明晰的技术管理策略:开发人员对开发测试服务器有完全的控制权限;运维人员控制生产机;管理员则可以访问所有设备并通过云盾堡垒机Web管理页面进行审计。

运维

云盾堡垒机的运维操作可以通过连接协议代理端口实现,现有规则表如下:

运维协议	端口号	四层协议
SSH	60022	ТСР
Windows远程桌面	63389	ТСР
SFTP	60022	ТСР
FTP	60021	ТСР
VNC	5900	ТСР
Windows远程桌面网关	44300	ТСР

您可以使用标准协议客户端如Xshell、SecureCRT、PuTTY、Windows远程桌面客户端直接连接上述端口号,并通过堡垒机用户名、密码登录,连接后根据提示进行下一步操作。详细的运维操作步骤,请参阅用户手册-运维手册。

审计

云盾堡垒机的审计分为两种,分别是实时监控和录像回放。实时审计专注于事中控制,可以通过云 盾堡垒机管理平台随时切入某个运维会话查看现场操作;录像回放专注于事后审计,主要用于已经 结束的会话进行录像回放或命令检索,检索可以使用时间段、手机号、主机IP地址、ECS实例ID、 协议类型等条件筛选结果,还可以通过曾经执行过的命令进行全局检索,并自动跳转到这条命令的 会话和时间段播放。

3 快速入门

本文介绍了如何配置、使用云盾堡垒机,帮助您快速熟悉产品。

在购买云盾堡垒机实例后,您需要进行如下配置操作:

- 登录云盾云堡垒机控制台,选择您已购买的堡垒机实例,单击启用,启用堡垒机,具体操作请参考网络配置。
- 2. 启用堡垒机实例后,单击管理。

云盾 • 堡垒机控制台	堡垒机	((▲)) 4				用户手册 购买垦垒机
实例列表	实例ID/名称	版本授权	地区(全部) ▾	到期时间	状态(全部) ▼	IP地址	操作
子账号管理	test111	版本:2.1.6 专业版	华东 1	2019-01-18 00:00:00	有效		管理 频格升级购买 软件升级 网络 配置 续器

- 3. 选择内网接入或公网接入,即通过内网还是公网连接云盾堡垒机 Web 管理页面。
- 在云盾堡垒机Web管理页面中,定位到资产>服务器页面,单击页面右上角的同步阿里云ECS。

Θ	管理控制台					
云盾。	• 堡垒机	服务器				同步阿里云ECS
概览	ī	输入实例名称/ID/IP模糊查询	搜索			全局运维端口
▼ 资产	:	服务器名称/实例ID	可用区(全部) 🗸	IP地址	网络类型 (全部) 🔻	运维端口
服	务器	test_hk_server	Δ	10.00		SSH: 22
服	务器组		▲ 美国东部1 可用区A	1 (B) (B) (B' () (B' ()))	专有网络	SSH: 22

同步阿	可里云ECS 许可限制]:最多能加入20台朋	资 器						\times
	已加入(2)	未加入(106)				输入实例名称/ID/IF	模糊查询	搜索	
	实例ID/名称				可用区 (全部) ▼	IP地址	网络类型 (全 部) ▼	状态 (全部) ▼	^
	1001			<i>8</i>	亚太东南1 可用 区A		经典网络	正常	
>	-84114			۵	亚太东南1 可用 区A		经典网络	正常	
	加入云堡垒机	已选:1				女]]果ECS数据不是最新	f,请点击手工刷	新



1 说明:

如果您的服务器使用的端口不是默认的端口(如 SSH 不是默认 22 端口,或 RDP 不是默认 3389 端口),或者您需要指定堡垒机实例连接的云服务器资产是通过公网 IP 还是内网 IP,您可通过以下两种方式进行配置:

定位到资产>服务器页面,勾选需要修改的服务器,单击服务器列表下方的修改端口及配置
 连接IP进行修改。

云盾 • 堡垒机	服务器	
概览	输入实例名称/ID/IP模糊查询 搜索	
▼ 资产	服务器名称/实例ID 可用区(全部)▼	IP地址
服务器	✓ <u>∧</u>	AT 10.11.10
服务器组	□ ▲ 美国东部1 可用区A	100000
▶ 用户	□	
 ▶ 授权 ▶ 审计 	禁用 启用 移除 修改端口 配置连接IP	

定位到系统 > 系统设置页面,进行运维端口及运维连接 IP 的全局设置,单击保存修改后生效。

📕 说明:

如果您通过此方式进行全局设置,所有服务器都将使用该配置方式,且服务器单独的配置修改不生效。

云盾●堡垒机	设置
概览▶ 资产▶ 用户	 双因子认证 使用密码运维登录时需要进行二次验证 本地用户和AD/LDAP用户使用手机验证码进行二次验证;云子帐号无论是否勾选此项都需要使用MFA进行二次 使用公钥运维登录时需要进行二次验证 本地用户和AD/LDAP用户使用手机验证码进行二次验证;云子帐号使用MFA进行二次验证。
 授权 审计	运维连接IP ☑ 运维时所有阿里云ECS连接 公网IP 勾选此项之后,运维时所有的阿里云ECS都将应用此配置,不再使用阿里云ECS自身的运维连接IP配置
▼ 系统 系统设置	 运维端口 ✓ 运维时所有服务器使用以下端口 SSH 22
存储管理操作日志	RDP 3389 勾选此项之后,运维时所有的服务器都将应用此配置,不再使用服务器自身的运维端口配置

6. 定位到资产 > 凭据页面,单击新建凭据。

C-D 管理控制台				admin
云盾 ● 堡垒机	凭据管理			新建凭据
概览	输入凭据名称/登录名模	期查询 搜索		
▼ 资产	名称	登录名	凭据类型 (全部) ▼	操作
服务器				
服务器组			♥ 沒有笪闻到付合余件的记录	
凭据				
▶ 用户				
▶ 授权				

7. 在新建凭据对话框中,输入名称、登录名、凭据类型、密码,单击确定。

道 说明 :	
关于凭据的作用,请参考术语介绍	名。

新建凭据	×
* 名称	
test	
* 22-26	
root	
* 先編英型	
2010249) 50110249)	
* 密码	
•••••	
aduste Root	5

8. 定位到用户 > 用户管理页面,单击新建本地用户。



更多新建用户的操作,请参考用户管理。

C) 管理控制台								admin
云盾。堡垒机	用户管理				新建	本地用户新建云子帐号	导入云子账号	导入AD/LDAP用户
概览	输入用户名/姓名/手机号码模	期查询 搜索						
▶ 资产	用户名	姓名	手机号码	邮件	认证源 (全部) 🔻	状态 (全部) 🔻		操作
▼ 用户	13558638100	13558638100	13558638100		本地认证	启用	ŧ	扁楫 配置公钥
用户管理 AD/LDAP设置	京 禁用 启用	删除						1 > »
▶ 授权								

9. 在新建用户对话框中,输入手机号码、密码、邮件、姓名,单击确定。

道 说明:	
您输入的手机号码就是运维登录的用户名。	

* 手机号码	
1000 0000000	
作为运维登录名	
* 密码	
•••••	
8-64个可见字符 , 必须包含以下4项:1.大写字母A-Z; 2.小写字母a-z; 3.数字0-9 非字母符号如@,#,\$。	; 4.
* 曲闪牛	
C Milling Milling	
姓名	

10.定位到授权 > 授权组页面,单击右上角的新建授权组。在弹出的对话框中,输入授权组名称,单 击确定。

€ ● 管理控制台						admin
云盾 • 堡垒机	授权组					新建授权组
概览	输入授权组信息模糊查询	搜索				
▶ 资产	名称	服务器 / 服务器组	用户	凭据	控制策略	撮作
▶ 用户	test	0/0	0	0	无	修改名称 克隆
▼ 授权	test2	0/0	0	0	无	修改名称 克隆
授权组	test_hk	0/0	0	0	无	修改名称 克隆
控制策略) 审计	創除更改控制	则策略				« < 1 > »

11.单击已创建的授权组中服务器/服务器组、用户、凭据、控制策略下方的文字,可将堡垒机的用户、服务器、凭据绑定在一起,并配置相应的控制策略。

	说明:	
其□	及务器和凭据要对应,否则可能导致无法登录。	
6)	管理控制台	

		i i			
云盾 ● 堡垒机	授权组				
概览	输入授权组信息模糊查询 搜索				
▶ 资产	名称 服务器 / 服务器组	用户	凭据	控制策略	
▶ 用户	test 0 / 0	0	0	无	
▼ 授权	删除 更改控制策略				
授权组					
控制策略					

12.如果您希望堡垒机用户在通过 SSH 或 RDP 协议方式登录堡垒机时需要使用密码 + 短信验证码 的双因子认证方式,可在系统 > 系统设置页面中勾选双因子认证选项,并单击保存修改。

(-) 管理控制台	
云盾 • 堡垒机	设置
 概览 ▶ 资产 ▶ 用户 	 双因子认证 使用密码运维登录时需要进行二次验证 本地用户和AD/LDAP用户使用手机验证码进行二次验证;云子帐号无论是否勾选此项都需要使用MFA进行二次验证。 ☑ 使用公钥运维登录时需要进行二次验证
▶ 授权▶ 审计	本地用户和AD/LDAP用户使用手机验证码进行二次验证;云子帐号使用MFA进行二次验证。 运维连接IP 运维时所有阿里云ECS连接 公网IP 勾选此项之后,运维时所有的阿里云ECS都将应用此配置,不再使用阿里云ECS自身的运维连接IP配置
▼ 系统 系统设置	运维端口 运维时所有服务器使用以下端口 SSH
存储管理 操作日志	RDP 勾选此项之后,运维时所有的服务器都将应用此配置,不再使用服务器自身的运维端口配置

审计查询操作

当用户以堡垒机用户的身份,通过 SSH、RDP、或 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,您可在云盾堡垒机 Web 管理页面中查看该用户会话的详细信息。



用户登录云盾堡垒机时,使用的用户名即为之前设定的用户手机号码。

关于如何登录堡垒机进行系统运维,请参考:

- Mac_{电脑运维}
- SSH协议运维
- SFTP协议运维
- RDP协议运维

当用户登录堡垒机后对已授权服务器进行运维操作时,您可在审计>实时会话页面查看该用户的实时会话情况。单击查看可以对该会话进行监控,也可以单击切断连结直接中断该实时会话。

c	管理控制台								admin
云盾●	堡垒机	实时	会话						
概览		输入会	会话相关信息模糊	相査询	搜索				全部: 1 RDP: 0 SSH: 1
▶ 资产			服务器	IP地址	可用区 / 网络类型	用户	连接方式	开始时间 / 时长	操作
▶ 用户				用户已登录云堡垒桥	1,尚未连接到任何主机	ramuser2 user2	SSH	2017-10-28 15:32:38 1 分 17 秒	切断连接 查看
▶ 授权									
▼ 审计			切断连接						< 1 >
实明	付会话								
录信	象回放								
指令	令查询								

当用户的会话连接断开后,您可在审计 > 录像回放页面查看该用户的会话情况,单击播放查看该会 话执行的操作。

C) 管理控制台								admin
云盾•堡垒机	录像回放							
概览	时间:	选择日期范围	连接方式:	全部	•			
 资产 	实例ID:	输入实例ID精确查询	服务器名称:	输入服务器名称模糊查询		服务器IP:	输入IP地址精确查询	
▶ 用户	手机号码:	输入手机号码精确查询	姓名:	输入姓名模糊查询		来源IP:	输入IP地址精确查询	
▶ 授权		搜索 清空						
▼ 审计	连接方式	服务器	服务器IP	可用区/网络类型	用户	来源IP	开始时间/时长	操作
实时会话	RDP		101.37.15.206	华东 1 可用区 E	······	112.10.94.66	2017-10-28 15:43:26	播放
录像回放		i-bp16qiyq4cx7q5hz8yp1		经典网络	3		28 秒	
指令查询								\leftarrow 1 \rightarrow

您也可以在审计 > 指令查询页面, 查看用户会话中输入并执行了哪些指令。



说明:

此功能仅针对已授权服务器上执行的命令行操作。

C-D 管理控制台											admin
云盾 ● 堡垒机	指令查询										
概览	时间:	选择日期范围	×	Ċ	指令类型:	全部	¥	指令	: 输入指令关键:	字模糊查询	
▶ 资产	实例ID:	输入实例ID精确查询			服务器名称:	输入服务器名称模糊查询		服务器IP	: 输入IP地址精制	角查询	
▶ 用户	手机号码:	输入手机号码精确查询			姓名:	输入姓名模糊查询		来源IP	: 输入IP地址精确	自查询	
▶ 授权		搜索 清空									
▼ 审计	时间	指令类型	指令内容			服务器	服务器	P	用户	来源IP	操作
实时会话	2017-10-28 15:43	3-54 上街保存	ocr.txt				101.37	15.206	1.000	112 10 94 66	編放
录像回放		11000				i-bp16qiyq4cx7q5hz8yp1					
指令查询	2017-10-28 15:43	3:51 图形文字	新建文本文	(档.txt	- 记事本	i-bp16qiyq4cx7q5hz8yp1	101.37	15.206		112.10.94.66	播放
▶ 系统											
操作日志											

43.0.X版快速入门

登录云盾堡垒机系统

第一次登录时需要启用堡垒机实例。

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击启用。



只有当实例状态为未初始化时,才会有启用操作。已初始化实例可以直接登录堡垒机系统。

云盾 • 堡垒机控制台	堡垒机					用户手册	购买堡垒机
实例列表	实例ID/名称	版本授权	地区(全部) ▼	到期时间	状态(未初始化) ▼	IP地址	操作
子账号管理	Service Renter Table 2001	版本: 堡垒机_20资产授权	华东1(杭州)	2018-09-29 00:00:00	未初始化	(内) (外)	启用

- 3. 在启用对话框中,完成以下配置。
 - a. 选择网络类型、已创建网络、交换机。

说明:

- 网络类型和交换机在实例启用后无法修改。
- 若选择交换机后不可启用,是因为交换机下资源已用完。请更换一台交换机,或新建交换 机供堡垒机部署选择。
- 若堡垒机是VPC类型,只要所选的VPC和ECS处于同一个VPC网络,交换机可任意选择(不会影响堡垒机和ECS内网相通)。
- b. 单击安全组ID,并选择ECS对应的安全组。

🧾 说明 :

此操作允许堡垒机访问安全组内的ECS,可多选,支持启用后修改。

C. 勾选公网访问控制类型。可选值:

- 不对公网开放
- 对公网白名单开放:勾选后,需进一步设置白名单IP。最多可填写30个IP或IP段。
- 对公网全部开放

d. 单击确定。等待启用生效。



启用堡垒机后,参照以下步骤登录堡垒机系统:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击管理。

云盾 • 堡垒机控制台	堡垒机						用户手册 购买堡垒机
实例列表	实例ID/名称	版本授权	地区(全部) ▼	到期时间	状态(有效) 🔻	IP地址	操作
子账号管理	Salarian A Lange and	版本: 堡垒机_50资产授权	华东1(杭州)	2019-03-18 00:00:00	有效	(内)	管理 规格升级购买 网络配置 续费

3. 在管理对话框中,选择并单击接入方式:内网接入、公网接入。

管理		×
请选择以私网还是	公网连接方式访问堡垒机控制台	
内网接入	公网接入	
		取消

进入云盾堡垒机系统。

步骤1:同步阿里云ECS资产

如果需要管理阿里云ECS以外的机器,请参考<u>主机管理</u>,手动创建主机或导入主机。

前提条件

- 授权堡垒机读取ECS列表信息。首次登录堡垒机控制台时会收到提示,需要您授权堡垒机读 取ECS列表信息,以实现ECS快速接入。
 - 1. 登录云盾堡垒机控制台。
 - 2. 在页面上方提示中单击授权,完成授权。

ഘ		
ا	说明	:

已完成授权时,不会出现该提示。

	堡垒机	((t \$))		
实例列表	让ECS快捷接入堡垒机	1管理,需要您 <mark>授权</mark> 卖取ECS列表信息	L	
子账号管理	实例ID	版本授权	地区(全部) ▼	到期时间

• 购买堡垒机的阿里云账号上有ECS实例。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 前往资产 > 主机管理 页面,单击ECS同步页签。
- 3. 单击页面右上角的同步阿里云ECS。

C-> 云盾堡垒机系统	控制版 / 主机管理 / ECS同步	法制版 / 主机营理 / ECS同步								
叠 控制板	主机管理	管理								
▲ 用户 >	主机列表 ECS同步 主机连接	主机列表 ECS同步 主机连接配置								
□ 资产 ~ → 机管理								2 ~ 下一页 末页		
共享帐户	つ 搜索主机名/主机IP	つ 投票主机名/主机IP Q			按主机网络过滤 ~	按可用区过滤 ~	按网络类型过滤 ~	请选择 ~		
主机组管理	主机	内网IP	公网IP	操作系统	主机网络	可用区	网络类型	状态		
帐户组管理		1.000	3.274.81	Windows Server 2012	经典网络@华北 2		经典网络	正常		
ዺ 授权 →		3.007430	0.000.00	Ubuntu	经典网络@华北 2	华北 2 可用区 C	经典网络	正常		

4. 在导入云主机对话框中,勾选要导入的主机,并单击导入。



如果ECS数据不是最新的,单击手动刷新重新检测。

导入云主机								
□ 导入 如果ECS数据不是最新,请点击 <mark>手工刷新</mark>								
Ċ	搜索主机名/主机IP		Q	按网络类型过滤 ≻	按可用区过滤 >			
	MONTH!	1000	12103	专有网络	美国东部1 可用区A			
	MORE NO.	0.000	10040	专有网络	美国东部1 可用区A			
	MARKED .	1000	10000	专有网络	美国东部1 可用区A			
	ROUTE THE REPORT	100.000	0.00.000	经典网络	华东 1 可用区 B			
	0.946.000	1000.000	0.000	经典网络	华东 1 可用区 D			
	ROUTE THE REAL	10000	0.000	经典网络	华东 1 可用区 B			
	07040	0.0000.00	0.00	经典网络	华北 2 可用区 A			
	mapping programming	0.000	0.000	经典网络				
	1000AT, 201.000	10.000		专有网络	华北 2 可用区 A			

成功导入ECS主机。

5. 在资产 > 主机管理页面主机列表中,单击要操作的主机IP,进入主机信息页面。

【→】 云盾堡垒机系统	论初版 / 主机管理						
m 控制板	主机管理				新建主机 更多操作 ≻		
▲ 用户 >	主机列表 ECS同步 主机连接配置						
□ 资产 ~ 主机管理	● 割除 第用 直页 1/2 ∨ 下一页 末页						
共享帐户	つ 捜索主机IP/主机名/登录名		Q	按操作系统过滤 ~	按主机网络过滤 ~		
主机组管理	主机	主机帐户数	共享帐户数	操作系统	所属主机网络		
帐户组管理	CONTRACTOR AND A DATA STOR	0	0	CentOS	经典网络@华北 2		

6. 单击主机帐户页签, 然后单击添加主机帐户。

云盾堡垒机系统	拉制版 / 主机管理 / 主机编包	🎢 使用向导 👻 💄 admin 👻
ab 控制板	主机帐户	
▲ 用户 >	基本信息 主切配置 主切帐户 共享帐户	
♀ 资产 ~ 主机管理	□ 前除 法10±11(M/²)	
共享帐户	⑦ 22 定要要素	
主机组管理	登录名 协议 密码 SSH低胡	登录模式
帐户组管理	无败据	
ペ、授权 >		

 在新建主机帐户对话框中,选择协议类型,并填写有效的主机帐户登录名和密码(服务器上已 经创建并存在的帐户和对应密码),单击创建主机帐户。

关于主机帐户选项的说明,请参考主机帐户选项说明。

新建主机帐户			×
协议	SSH	T	
登录模式	自动登录	Ŧ	
帐户类型	普通帐户	▼	
登录名			
密码	特权帐户	验证	
创建主机帐户]		

成功创建主机帐户。

步骤2:导入阿里云子账号

如果需要新建本地用户,请参考用户管理。

前提条件

- 要导入的子账号需要关联虚拟MFA设备。
 - 1. 登录阿里云访问控制RAM控制台。
 - 2. 在用户管理页面,选择要操作的子账号,单击管理。

访问控制 RAM	用户管理			新建用户 〇 刷新
概览	田古夕 - 法给》田古夕进行接到本海	地去		
用户管理		18.54		
群组管理	用户名/显示名	备注	创建时间	操作
策略管理	inge anver		2018-11-12 12:14:15	管理 授权 删除 加入组
角色管理	finans angu		2018-08-29 15:52:07	管理 授权 删除 加入组

3. 在用户详情页面,单击启用虚拟MFA设备。

<	Losi					
用户详情	其木信自			٥	e4217+/20	•
用户授权策略	用户名		UID Internet in the second	创建时间 2018-11-12 12:14:15	用相至441日定.	^
用户加入的组	显示名 aegis		手机	邮箱		
	备注 -					
	Web控制台登录管理	0		关闭控制台登录	重置密码	^
	必须开启多因素认证❷		上次登录时间: 2018-11-12 12:16:14	下次登录必须重置密码:		
	多因素认证设备					^
	类型	简介	启	用状态	ŧ	操作
	虚拟MFA设备	遵循TOTP标准算法来产生6位数字验证	码的应用程序 未	:)自用	启用虚拟MFA设备	R

4. 在启用虚拟MFA设备页面,使用阿里云App(或其他MFA应用程序)扫码添加账

号。	► 阿里云 多因素认证-启用虚拟MFA设备
	启用虚拟MFA设备
	您必须先在智能设备上安装一个MFA应用程序,才可继续进行操作。您可以直接使用官方的阿里云 App 进
	如果您的账号已被多人共享使用,那么当您成功绑定MFA之后,其他未绑定MFA的人将无法登录。解决方法最佳实践来看,我们建议您取消多人共享账号。
	完成 MFA 配置后,当您再次登录账户时,需要提供密码和 MFA 应用生成的验证码。请勿随意卸载 MFA) 置。
	扫码获取 手输信息获取
	推荐使用 阿里云 App 进行扫码

成功添加账号后,在阿里云App的虚拟MFA页面会显示已关联账号和每60s自动刷新生成的安全码。

- 5. 在启用虚拟MFA设备页面的第一组安全码和第二组安全码中输入阿里云App中连续获取的两 组安全码。
- 6. 单击确定启用。
- 完成子账号授权。

堡垒机用户权限分为超级管理员 (admin)和运维员两种。

- 阿里云主账号登录为admin权限,可以查看和管理所有数据。
- 子账号权限由主账号分配,可分配admin权限或者运维员权限。从限权角度,一般建议分配运 维员权限。本地用户是运维员权限。

参照以下步骤为子账号授权:

- 1. 登录阿里云访问控制RAM控制台。
- 2. 在用户管理页面,选择要操作的子账号,单击授权。

访问控制 RAM	用户管理			新建用户	€周新
概览		10.5			
用户管理	用戶名 • 前输入用戶名並行模糊直询	援系			
群组管理	用户名/显示名	留注	创建时间		攝作
策略管理	22		2018-11-12 12:14:15	管理 授权	删除 加入组
角色管理	treps;		2018-08-29 15:52:07	管理 授权	删除 加入组

- 在编辑个人授权策略对话框,可选授权策略名称下,输入"云盾堡垒机"搜索可用的系统策略。
 共有四个可用的系统策略:
 - AliyunYundunBastionHostFullAccess (管理员权限)
 - AliyunYundunBastionHostReadOnlyAccess(运维员权限)
 - AliyunYundunBastionHostOperateOnlyAccess(运维员权限)
 - AliyunYundunBastionHostOperateOnlyAccess(运维员权限)

其中,FullAccess是管理员权限,其余三个是运维员权限,且无差别。

罐个人授权策略					
添加授权策略后,该账户即具有该条策略的	的权限,同一翁	發授权策略不能被	重复添加。		
可选授权策略名称	类型		已选授权策略名称		类型
堡垒机	Q				
AliyunYundunBastionHostFullAcc 管理云盾堡垒机(BastionHos	系统				
AliyunYundunBastionHostReadOnl 只读访问云盾堡垒机(BastionH	系统	<			
AliyunYundunBastionHostOperate 管理云盾堡垒机(BastionHos	系统				
AliyunYundunBastionHostAuditOn 管理云盾堡垒机(BastionHos	系统				
				确定	关闭

4. 选择要授予当前子账号的权限后,单击确定,完成授权。

操作步骤

1. 登录云盾堡垒机控制台。

2. 在子账号管理页面,单击子账号列表下方的刷新子账号数据,从RAM获取最新的子账号数据。

3. 单击页面右上角的导入子账号。

4. 在导入阿里云子账号用户对话框中,勾选需要导入的子账号,并单击导入子账号。

步骤3:创建运维规则

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 在授权 > 运维规则页面,单击新建运维规则。

【→】 云盾堡垒机系统	控制版 / 运维 4 周 向 号 マ ▲ admin			🌾 使用向导 🔻 🚨 admin 👻
▲ 控制板	运维规则			+ 新建运维规则
▲ 用户 > ↓ 资产 >	□ 副除 禁用 启用 			
9、 授权 ~	り 捜索运维规则名称 Q	搜索用户 Q、	搜索资产Q	按状态过滤 ~
运维规则	名称	甩户	资产	状态
未授权登录审核	无数据			

3. 在新建运维规则页面,填写规则名称,选择授权用户和资产,并单击创建。

送明:

您可以选择设置规则有效期。在规则过期后,用户和主机的运维授权关系即解除。

【-】 云盾堡垒机系统	拉制版 / 运维规则 / 新建运作规则	ፇ 使用向导 ▼	📥 admin 🔻
命 控制板	新建运维规则		
▲ 用户 >			
□ 资产 >	* 规则名称 显大长度50个字符		
♀、授权 ~	规则有效期 - 不限制运性规则的有效期谐雷空		
运维规则 未授权登录审核	规则过期后 目动删除 每日0点之后删除,实际时间会因任务调度而有所波动		
● 审计 >	爾注		
■工単 >			
▲ 运维 →	用户		
奈 系统 >			
	请添加用户 · · · · · · · · · · · · · · · · · · ·		
	创建运带规则		

4. 成功创建规则后,您可以进一步编辑该规则,启用更多限制功能。例如,

- 启用登录限制,限制允许/拒绝的访问来源IP,限制访问时间段等。
- 启用命令控制,限制允许访问者使用的命令。
- 启用协议控制,配置各个协议会话中的相关控制选项。

具体请参考运维授权。

步骤4:主机运维

Windows客户端

分为BS运维和CS运维。CS运维请参考SSH协议运维。BS运维需满足以下前提条件:

- 下载安装单点登录器。
 - 1. 登录云盾堡垒机系统。
 - 2. 在右上角用户菜单下单击工具下载。

[-] 云盾堡垒机	系统				γ	使用向导 ▼ 💄 admin ▼
企 控制板						注 查看个人信息 ▲ 工具下载
▲ 用户	>	用户	主机		运维规则	▶ 退出系统
□ 资产	>			7777	FT \ 40) - (0)	
♀、 授权	>	一周冱难次数统计		一周用户运维 TOP 5	一周王机运维	TOP 5

3. 下载并安装单点登录器。

送 说明:

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

工具下载	
运维及审计工具	
名称	下载
单点登录器 运维登录必备工具	本地下载
高线播放器 播放下载到本地的会话数据	本地下载

- 设置相应协议的运维配置。
 - 1. 登录云盾堡垒机系统。
 - 2. 在运维 > 主机运维页面,单击右上角的Web运维配置。

【一】 云盾堡垒机系统	- 拉制板 / 主机运输			
企 控制板	主机运维 快速运维:输入主机名/主机印/登录名	✿ Web运维配置 ▲ 运维下载	~	
	 新EI的联邦运行 	首页 上一页 0/0 ~ 下一页 末辺	Ω	
역、授权 >	ウ 技操作系统过端 ぐ 技主机网络过端 ぐ 技主机网络过端	过端 ~		
● 审计 >	主机 操作系统 主机网络 主机组	主机帐户 登录		
■ 工単 >	· 智元主机可运用 进行接权			
▲ 运维 ~				
主机运维				
实时监控				

3. 在Web运维配置对话框中完成相应配置。具体请参考BS运维操作。

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

4. 单击保存,完成配置。

Mac客户端

因Mac环境和单点登录器不兼容,仅支持CS运维。具体请参考SSH协议运维。