阿里云 堡垒机

用户指南(V2版本)

文档版本: 20190830

为了无法计算的价值 | [] 阿里云

<u>法律声明</u>

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。
- 3. 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者 提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您 应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

	334 mm	LNK from
俗式	况明	[件17月
•	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。	道 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。
##	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	I
1 术语介绍	1
2 管理员手册	4
2.1 网络配置	4
2.2 服务器管理	8
2.3 凭据管理	13
2.4 授权组管理	14
2.5 双因子认证	17
2.6 操作日志管理	18
2.7 AD/LADP配置	19
2.8 配置备份管理	22
2.9 控制策略管理	25
2.10 服务器组管理	
2.11 透明代理	
2.12 存储管理	
2.13 用户管理	44
3 运维使用手册	49
3.1 SSH协议运维	
3.2 RDP协议运维	52
3.3 SFTP协议运维	56
3.4 Mac系统运维	59
3.5 用户修改密码	77
3.6 BS运维	78

1术语介绍

基本对象

云盾堡垒机有五种对象,分别是用户、服务器、服务器组、凭据、控制策略。

- ・用户:代表技术工程师,也就是自然人,云盾堡垒机目前有本地用户、云子账号用户、AD/ LDAP用户。
- ·服务器:是您在阿里云上的ECS实例。
- ·服务器组:是多个服务器的组合,方便归类管理,统一授权。
- · 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。
- · 控制策略:用于对运维操作行为做策略控制。云盾堡垒机支持RDP协议上传下载控制、来 源IP控制、访问时间段控制、SSH命令控制。

授权组

授权组是将堡垒机中数个独立的对象联系在一起的概念,通过授权组功能可以达到控制某个用户只 能访问他权限内服务器的目的。

以下通过示例帮助您更好地理解授权组的概念:

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)

在这样的情况下,您可以按照如下策略配置授权关系:

云盾账号	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 置被篡改。
opsuser	APP1、APP2、DB1 、DB2、M1、M2	ops	运维人员使用可以 sudo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。

根据这样的授权关系配置进行授权组配置就可以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。

- ・运维人员控制生产服务器。
- · 管理员可以访问所有设备,并通过云盾堡垒机Web管理页面进行审计。

关于详细授权组操作步骤,请参考授权组管理。

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。

默认链接协议规则如下表:

运维协议	端口号	四层协议
SSH	60022	ТСР
Windows远程桌面	63389	ТСР
SFTP	60022	ТСР

您可以使用标准协议客户端(如 Xshell、SecureCRT、PuTTY、及Windows 远程桌面客户端等 工具)直接连接规则表中的端口号,并使用堡垒机用户名、密码进行登录。成功登录堡垒机后,根 据提示即可对授权服务器进行相关运维操作。

关于登录堡垒机进行运维的详细操作步骤,请参考:

・MAC电脑运维

- · SSH协议运维
- ・SFTP协议运维

・RDP协议运维

审计

云盾堡垒机的审计分为两种:实时监控和录像回放。

- ・ 实时审计:专注于事中控制,您可以通过云盾堡垒机Web管理页面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,主要用于对已经结束的会话进行录像回放或命令检索。支持通过时 间段、手机号、服务器 IP、ECS 实例 ID、协议类型等条件进行筛选,还支持通过曾经执行过的 命令进行全局检索,并自动跳转到执行这条命令的会话和时间段进行回放。

关于审计相关的详细操作步骤,请参考:

- ・实时会话
- ・录像回放
- ・指令查询

2 管理员手册

2.1 网络配置

选择网络类型

在购买云盾堡垒机实例时,除了选择地域、套餐、购买时长外,您还需要选择云盾堡垒机实例所使 用的网络类型。



建议您选择与所需接入堡垒机系统进行运维的ECS服务器相同的网络类型:

- ·如果ECS服务器都处于专有网络环境,堡垒机实例的网络应选择专有网络(VPC)。
- ·如果ECS服务器都处于经典网络环境,堡垒机实例的网络应选择经典网络。
- ・如果需要接入ECS服务器既有专有网络环境也有经典网络环境,建议您的堡垒机实例的网络选择专有网络(VPC)。

购买云盾堡垒机实例后,您需要在云盾堡垒机管理控制台中启用该实例,然后才能登录云盾堡垒机 系统。

启用专有网络(VPC)类型的堡垒机实例

参考以下操作步骤, 启用您已购买的专有网络类型的堡垒机实例:

1. 在云盾堡垒机管理控制台中,选择已购买的云盾堡垒机实例,单击启用。

实例应用		×
• 同志:	WYC 网络奥型和交换机在实现应用后将无法参加。	
	请选择专有网络 请选择虚拟交换机	
	- 法理论全组	
	调选择ECS对应的安全组,允许重型机通过该网络访问您的ECS,可多语 等政。	, 町
•公同访 问控制:	 不对公用开放 对公司占名单开放 	
	财公司金部开放	
	and a state of the	
	162 D	57

2. 选择专有网络和交换机。

 说明 建议您选择 专有网络V]: 经与所需运维 PC环境中的	的ECS实例和 DECS实例。	目同的专有网络。	这样,堡	全机系统即	可通过内网访问同一
说明 说明 如果收到以 建一个虚批]: 【下错误提示 【交换机,重	;,则表示该3 〔新启用堡垒4	交换机所在的可用 讥实例。	区已无可	「启用实例。	建议在其它可用区新
* 网络:	VPC	网络类型和交换机	几在实例启用后将无法惨o	ζ.		

3. 单击选择安全组,选择经典网络环境中已有的安全组,单击确定。

wonev/4

📕 说明:

选择安全组后,系统会自动在对应的安全组中创建一条访问控制规则,允许堡垒机系统访问该 安全组中的ECS实例。

📕 说明:

系统并不是将堡垒机实例直接添加至进所选择的安全组中,而是在安全组中添加以下规则允许 堡垒机实例访问安全组中的ECS实例。

内间入方向	内同出方向 公	周入方向 公网	出方向							
经共同地的内容	8入方向规则,推荐代5	电选择安全组接权方	式;如选择即地址方式表	8双,出于安全性的考虑,仅支持单护接权,)	950 : 10.x.y.z/32. #5020					
接权加略	的这类型	MC/SH	授权类型	接权对象	描述	优先级	创建时间			根作
允许	25	-1/-1	安全组访问	sg-bp1ivp9axky7z2dqh915 164979683658	group - 50796549918812	1	2017-09-01 16:35:18	特徵語	s ma	259

圓 说明:

请勿删除该安全组规则。

4. 设置公网访问控制,单击确定,堡垒机实例的状态变为初始化中。

10分钟后,刷新云盾堡垒机管理控制台页面查看堡垒机实例状态,如状态变更为有效,则堡垒机实 例启用成功。

启用经典网络类型的堡垒机实例

参考以下操作步骤, 启用您已购买的经典网络类型的堡垒机实例:

1. 在云盾堡垒机管理控制台中,选择已购买的云盾堡垒机实例,单击启用。

实例应用	×
•网络:	台角 网络美国和女装机在实明但用后将无法惨欢。
	·····································
内网访 问控 制:	innia IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
0.000	请输入中地址,以周文:公开,最多30个。
(司控制)	 不对公转开放 对公局白名单开放
	* 对公司全部开放
	内用边向 第二
	公司访问
注意:安	全组+内房中+公园白名单的总数量,不能超过30条!
	ekst: 566

2. 单击选择安全组,选择经典网络环境中已有的安全组,单击确定。



📕 说明:

选择安全组后,系统会自动在对应的安全组中创建一条访问控制规则,允许堡垒机系统访问该 安全组中的ECS实例。

📕 说明:

系统并不是将堡垒机实例直接添加至进所选择的安全组中,而是在安全组中添加以下规则允许 堡垒机实例访问安全组中的ECS实例。

内间入方向	内局出方向 公	用入方向 公司	出方向					
這角网络的内容	司入方向规则,推荐代5	电选择安全组接权力	1式;如选择即地址方式8	f权,出于安全性的考虑,仅支持单中接权,(NSD : 10.x.y.z/32. #RRQM			
授权放略	物议问题	第〇四日	授权类型	授权对象	描述	代先级	创建时间	损伤
允许	全部	-1/-1	安全细访问	sg-bp1/vp9axky7z2dqh915 164979683658	group - 50796549918812	1	2017-09-01 16:35:18	停放描述 克隆 删除

📋 说明:

请勿删除该安全组规则。

3. 设置堡垒机系统的网络访问控制。

📕 说明:

堡垒机实例启用后,您可以单击网络配置修改访问控制策略。

· 内网访问控制:此处添加的为堡垒机系统的登录白名单,即只有添加在内网访问控制框中的 内网IP可访问堡垒机。例如,您可以在此处添加VPN服务器的内网IP。

📋 说明:

不添加内网IP则表示堡垒机系统对内网访问无限制。

· 公网访问控制:此处可对堡垒机系统的公网访问进行控制。

4. 单击确定后,堡垒机实例的状态变为初始化中。

10分钟后,刷新云盾堡垒机管理控制台页面查看堡垒机实例状态,如状态变更为有效,则堡垒机实 例启用成功。

网络配置FAQ

无法通过公网IP登录堡垒机系统

请检查堡垒机实例网络配置中的公网访问控制选项,确认公网访问方式已启用,或者您用于登录的IP已添加至公网白名单中。



说明:

华东1地域的金融云用户无法通过公网IP登录堡垒机系统。

无法通过内网IP登录堡垒机系统

请检查你的客户端是否可以与堡垒机系统处于同一专有网络VPC环境中的其他ECS服务器。

- ·如果无法连通,请检查VPN服务器状态。
- ·如果可以连通,请尝试通过同一专有网络VPC环境中的其它ECS服务器登录堡垒机系统。如果登录成功,则请检查VPN服务器。

如果堡垒机实例的网络类型为经典网络,请检查网络配置中的内网访问控制是否存在相关限制。

通过堡垒机系统登录ECS服务器的公网IP失败

请尝试不通过堡垒机系统直接访问该ECS服务器的公网IP。

- ·如果无法登录、请检查该ECS服务器的状态。
- ·如果可以登录,请检查该ECS服务器的安全组中是否有堡垒机系统自动添加的规则。如果没有相关安全组规则,您需要在堡垒机实例的网络配置中重新添加一次相关的安全组。

📋 说明:

部分金融云账号默认禁止使用公网IP登录ECS服务器,您必须通过内网IP登录ECS服务器。

通过堡垒机系统登录ECS服务器的内网IP失败

请检查堡垒机实例与目标ECS服务器是否在同一专有网络VPC环境或经典网络环境。

- ·如果目标ECS服务器与堡垒机不在同一网络环境,则无法通过内网连通,您必须通过公网IP登录 该ECS服务器。
- ・如果目标ECS服务器与堡垒机处于同一网络环境,请检查该ECS服务器所在的安全组,确认已对 堡垒机系统开放访问相关运维端口的权限。

2.2 服务器管理

在云盾堡垒机的Web管理页面,您可以执行以下服务器相关的操作:添加、启用/禁用、修改、移 除。

添加服务器

您可以使用三种方式来添加服务器:同步阿里云ECS、手动添加、和批量添加。

同步阿里云ECS

同步ECS云服务器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。参照以下步骤同步阿里云ECS:

- 1. 登录到云盾堡垒机Web管理页面。
- 2. 定位到资产 > 服务器页面,单击页面右上角的同步阿里云ECS。



若需要将ECS按ECS标签分别添加到不同的服务器组,请在系统 > 系统配置中勾选同步ECS标签。

	57里	
云盾●堡垒机	口口	
概览		
 资产 	双因于以证	使用密码运转登录的需要进行二次短证 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
▶ 用户		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	运维连接IP	□ 运维时所有阿里云ECS连接 内网IP ▼
▶ 审计		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	运维端口	□ 运维时所有服务器使用以下端口
系统设置		SSH
存储管理		RDP
配置备份管理		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
操作日志	同步ECS标签	☑ 将阿里云ECS标签同步为服务器组 勾选此选项可以从标签快速创建服务器组,并将相关服务器加入这些服务器组,服务器组可用于授权。
	保存设置	

3. 在同步阿里云ECS对话框中,单击手工刷新以获取最新ECS信息。

三 说明:

如果堡垒机无法正常获取您云账号中的ECS云服务器列表,请确认您已在云盾堡垒机管理控制 台中的实例列表页面授权堡垒机系统读取ECS列表信息。

日10入(0)	未加入(0)		第2人实例名称/10/198	NEO 10
\$MD/88	司用区 (全部) =	PRA	周続実型 (全部) *	秋志 (全部) +

4. 勾选所需添加的云服务器,单击加入云堡垒机。

手动添加服务器

参照以下步骤手动添加服务器:

- 1. 登录到云盾堡垒机Web管理页面。
- 2. 定位到资产 > 服务器页面,单击页面右上角的 添加服务器。



手动添加服务器可以是外部主机,确保该主机与堡垒机网络互通即可。

添加服务器	\times
* 服务器IP 	
* 操作系统 Linux Windows	
确定	取消

3. 在添加服务器对话框中,填写服务器信息后,单击确定完成添加。

批量添加服务器

参照以下步骤手动添加服务器:

- 1. 登录到云盾堡垒机Web管理页面。
- 2. 定位到资产 > 服务器页面,单击页面右上角的 批量添加服务器。
- 3. 在批量添加服务器对话框中,单击下载模板文件将模板文件下载到本地。

批量添加服务器	\times
请下载模板文件,按照文件的格式填写服务器信息后上传,已存在的同名服务器将 被更新 上传文件	
下一步 取消	

- 根据模板文件格式要求填写服务器信息后,单击上传文件,将服务器信息文件上传,单击下一步。
- 5. 确认添加的服务器信息无误后,单击确定完成批量添加。

启用/禁用服务器

参照以下步骤启用/禁用服务器:

- 1. 登录到云盾堡垒机Web管理页面。
- 2. 定位到资产 > 服务器页面,勾选您想要启用或禁用的服务器,单击列表下方的启用或禁用。



您可以单击列表最下方单选框全选本页全部服务器,再选择启用或禁用,则可以启用/禁用本页 全部服务器。

云盾 • 堡垒机	✓ i-bp10egdlk9bxqutfys11	▲ 华东1可用区 F	192.168.51.146 (私有) 专	有网络 SSH: 22	启用
概览 ▼ 资产	✓ i-bp1ednynvqzxcqvd2jli	▲ 华东1可用区E	(公) ● 192.168.2.124 (私有) 专	有网络 SSH: 22	启用
服务器	✓ i-j6c0n0r0zwuw6ujxp88g	▲ 香港可用区 B	(公) • 172.31.140.238 (私有)	有网络 55H: 22	启用
服务器组 氏据	✓ i-bp14ame764574j8hllx6	▲ 华东 1 可用区 F	(公)• 192.168.51.148 (私有)	有网络 SSH: 22	启用
	☑ 禁用 启用 移除	修改端口 配置连接IP			« < 1 > »

操作完成后,查看该服务器右侧对应状态是否为启用/禁用,检验操作是否成功

修改服务器

登录到云盾堡垒机Web管理页面,定位到资产 > 服务器,您可对已添加的服务器进行修改。

・勾选您想要修改的服务器,单击修改端口。您可在弹出的对话框中根据您服务器的实际情况更改 SSH 和 RDP 协议端口的相关配置。

服务和端				×
🕑 SSH	22			
RDP	3389			
		_	确定	取消

・ 勾选您想要修改的服务器,单击配置连接IP。您可在弹出的对话框中根据需要更改连接 IP 的相
 关配置。

▋ 说明:

连接 IP 配置只对拥有公网 IP 和内网 IP 的阿里云ECS云服务器生效。

Ē	配置连接IP			×
	此配置只对有公网	和内网IP的阿里云ECS生效		
	连接IP	内网IP	▼	
			确定	取消

·选择您想要修改的服务器,单击右侧的编辑。您可在弹出的对话框中修改普通服务器的信息。



编辑功能只适用于通过手动方式或批量方式添加的服务器。

修改服务器	\times
* 服务器IP 1.1.1.1 * 名称	
AAAA * 操作系统 Linux Windows	
确定	取消

移除服务器

移除服务器是指从云盾堡垒机列表中将服务器移除,该操作不会影响您帐号中的ECS实例及其他服务器。参照以下步骤移除服务器:

- 1. 登录到云盾堡垒机Web管理页面。
- 2. 定位到资产 > 服务器页面,勾选您想要移除的服务器,单击列表下方的移除。

您可以单击列表最下方单选框全选本页全部服务器,再选择移除,则可以移除本页全部服务器。

(-) 管理控制台		
	i-bp16qiyq4cx7q5hz8yp1 10.28.143.144(私有)	
云盾•堡垒机	✓ Fbp10egdik9bxqutfys11 ▲ 华东1可用区F 192.168.51.146(私有) 专有网络 SSH: 22 度	自用
概览 ▼ 资产	✓ i-bp1ednymvqzxcqvd2jii ▲ 华东1可用区E (公)● 192.168.2.124 (私有) 专有网络 SSH: 22 启	自用
服务器	✓ ij6c0n0r0zwuw6ujxp88g ▲ 香港可用区 B (公) 专有网络 SSH: 22 虐	自用
服务器组	✓ i-bp14ame764574j8hllx6 ▲ 华东 1 可用区 F 192.168.51.148 (私有) 专有网络 SSH: 22 启	自用
用尸管理	✓ 禁用 启用 移除 修改端口 配置连接IP	« < 1 >

3. 确认无误后, 在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.3 凭据管理

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。
- 在云盾堡垒机Web管理页面,您可以执行以下凭据相关的操作:创建、修改、删除。

创建凭据

参照以下步骤创建凭据:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到资产 > 凭据页面,单击新建凭据。
- 3. 在新建凭据对话框中填写以下信息:
 - ・名称:必填,用于标识凭据。
 - ·登录名:必填,登录服务器的用户名。
 - ・凭据类型: 必选, 密码或 SSH 密钥方式。
 - · 密码: 密码类型凭据必填。
 - · SSH密钥: SSH 密钥类型凭据必填。
- 4. 在对话框中, 单击确定, 完成创建凭据操作。

修改凭据

参照以下步骤修改凭据:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到资产 > 凭据页面,选择需要删除的凭据,单击右侧的修改。
- 3. 在修改凭据对话框中,您可根据需要修改名称、登录名、凭据类型和密码等信息。
- 4. 凭据信息修改完成后,单击确定。

删除凭据

参照以下步骤删除凭据:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到资产 > 凭据页面,勾选需要删除的凭据,单击列表下方的删除。
- 3. 在弹出的对话框中,单击确定,完成删除凭据操作。



单击凭据列表下方的单选框勾选本页所有凭据,再单击删除可以删除本页所有凭据。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.4 授权组管理

在云盾堡垒机Web管理页面,您可以执行以下授权组相关操作:新建、修改、克隆、删除。

新建授权组

参照以下步骤新建授权组:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权组,单击新建授权组。
- 3. 在弹出的对话框中填写新授权组的名称,单击确定。

4. 配置已创建的授权组的基本对象。

- ・ 服务器/服务器组
 - a. 选择已创建的授权组,单击服务器/服务器组栏中的数字。

授权组					新建授权组
输入授权组信息模糊查询	到 搜索				
名称	服务器 / 服务器组	用户	凭据	控制策略	操作
cbqrule	1/2	3	2	无	修改名称 克隆
test	0/0	0	0	ALC: NO.	修改名称 克隆
	0/1	1	3	Access 1	修改名称 克隆

- b. 在授权组: 服务器/服务器组对话框中,勾选一个或多个服务器/服务器组,单击加入授权 组。
- ・用户
 - a. 选择已创建的授权组,单击用户栏中的数字。

授权	7组					新建授权组
输入	受权组信息模糊查询	搜索				
	名称	服务器 / 服务器组	用户	凭据	控制策略	操作
	1234	0 / 0	0	0	无	修改名称 克隆
	cbqrule	1/2	3	2	121212	修改名称 克隆
	test	0 / 0	0	0	121212	修改名称 克隆

b. 在授权组:用户对话框中,选择一个或多个用户,单击加入授权组。

・凭据

a. 选择已创建的授权组,单击凭据栏中的数字。

授校	风组					新建授权组
输入	授权组信息模糊查询	搜索				
	名称	服务器 / 服务器组	用户	凭据	控制策略	操作
	1234	0 / 0	0	0	无	修改名称 克隆
	cbqrule	1/2	3	2	121212	修改名称 克隆
	test	0 / 0	0	0	121212	修改名称 克隆

b. 在授权组:凭据对话框中,勾选一个或多个凭据,单击加入授权组。

・控制策略

a. 选择已创建的授权组,单击控制策略栏中的文字。

授权	纽					新建授权组
输入	受权组信息模糊查询	搜索				
	名称	服务器 / 服务器组	用户	凭据	控制策略	操作
	1234	0 / <u>0</u>	0	0	无	修改名称 克隆
	cbqrule	1/2	3	2	121212	修改名称 克隆
	test	0 / 0	0	0	121212	修改名称 克隆

b. 在更改控制策略对话框中,选择一个控制策略,单击加入授权组。

更改控制策略	×
控制策略	
Æ	•
	_

修改授权组

参照以下步骤修改授权组:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权组,选择您需要修改的授权组,单击右侧的修改名称。

授权	授权组							
输入	受权组信息模糊查询	搜索						
	名称	服务器 / 服务器组	用户	凭据	控制策略		操作	
	1234	0 / 0	0	0	无	修改名称	克隆	
	cbqrule	1/2	3	2	121212	修改名称	克隆	
	test	0 / 0	0	0	121212	修改名称	克隆	

3. 在弹出的对黄框中修改授权组名,单击确定。

克隆授权组

参照以下步骤克隆授权组:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权组,选择您需要克隆的授权组,单击右侧的克隆。

授权	纽					新建授权组
输入	受权组信息模糊查询	搜索				
	名称	服务器 / 服务器组	用户	凭据	控制策略	操作
	1234	0 / 0	0	0	无	修改名称 克隆
	cbqrule	1/2	3	2	121212	修改名称 克隆
	test	0 / 0	0	0	121212	修改名称 克隆

3. 在弹出的对话框中填写通过克隆创建的授权组名称,单击确定。

删除授权组

参照以下步骤删除授权组:

1. 登录云盾堡垒机Web管理页面。

2. 定位到授权 > 授权组,勾选您需要删除的授权组,单击列表下方的删除。

(-) 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	操作
▶ 用户	1234	0/0	0	0	无	修改名称 克隆
▼ 授权	cbqrule	1/2	3	2	121212	修改名称 克隆
授权组		iy-krista i dala ada				
控制策略	- 前林 更印	X1至中J 來增				

3. 在弹出的对话框中,单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.5 双因子认证

开启双因子认证之后,运维人员登录云服务器时,需要先输入用户密码,密码验证正确之后,需要输入动态口令(短信/MFA)才能登录成功。

背景信息

双因子认证有如下几种情况:

- 使用密码运维登录
 - 本地用户和AD/LDAP用户要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
 - 本地用户和AD/LDAP用户要使用手机验证码进行二次验证。
 - 云子帐号在勾选此项后需要使用MFA进行二次验证。

参照以下步骤启用/禁用双因子认证:

操作步骤

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。

3. 选择接入方式,连接目标堡垒机Web 管理页面。

4. 定位到 系统 > 系统设置页面,在双因子认证下勾选或取消勾选对应功能选项。



5. 单击保存设置,刷新页面查看操作是否成功。

2.6 操作日志管理

操作日志是指管理员操作、配置云盾堡垒机本身时所产生的日志。您可以在云盾堡垒机Web管理页 面查看所有操作日志,或使用多种过滤条件查询特定的日志记录。

背景信息

参照以下步骤查看和查询操作日志:

操作步骤

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web 管理页面。
- 4. 定位到操作日志页面,查看所有操作日志,您可以选择以下搜索方式进行查询:



支持设置多个搜索条件,单击清空可清空已设置的条件。

・按照操作日期搜索:单击操作日期文本框并设置日期范围,单击搜索。

操作日志											
操作日期:	2018-0	5-01 to 2	2018-05-	25		×		日志美型: 全部	▼ 操作结果	全部	•
日志内容:	<		Ī	百月 201	8		>				
	周日	周一	周二	周三	周四	周五	周六				
	29		1	2	3	4	5				
操作日期	6	7	8	9	10	11	12	2	用户	来源IP	操作结果
2018-05-24 17:17	Ŭ	ŕ	Ŭ	2	10		12	;器: 涉川美东测试服务器	admin	100.000	成功
	13	14	15	16	17	18	19				
2018-05-24 17:17	20	21	22	23	24	25	26	諸書: test_hk_server	admin	100.00	成功
2018-05-17 09:24	27	28	29	30	31	1	2	诸份: 201805170924-v2.1.6	admin	100.00	成功
2018-05-09 23:54		4		6	7	8	9	组: test2	admin		成功

・按日志类型搜索:单击日志类型文本框并选择日志类型(资产、用户、授权组、运维、其
 他),单击搜索。

操作日志								
操作日期:	2018-05-01 to 2018-05-25	×	● 日志类型:	全部	•	操作结果:	全部	Ŧ
日志内容:	输入日志内容关键字模糊查询		全部 资产 用户					
	搜索清空			用户 授权组 运维				
+= //= == ±0	□+±=		Otto	其他			++-XETO	+= //-//+ FR

- ・按操作结果搜索: 单击操作结果文本框并选择成功或失败, 单击搜索。
- ・按日志内容搜索: 在日志内容文本框中输入要在日志内容中搜索的关键字, 单击搜索。

2.7 AD/LADP配置

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。

```
云堡垒机与AD/LDAP服务器对接,可将AD/LDAP服务器用户同步进堡垒机,作为堡垒机用户使用。此功能需具有部署好的AD/LDAP环境,且保证堡垒机至服务器网络可达。
```

AD域设置

- 1. 登录堡垒机Web管理页面,进入用户AD/LDAP设置,将模式调整为AD。
- 在页面内依次填入AD服务器IP、端口、要同步的用户所在的组织、域名、域用户账号、密码,以及姓名、邮箱、手机号码等属性字段名称(带*为必填项)。

道 说明: 需保证填入的用户账号有权限访问Base DN。 说明: 若拉取的用户无手机号码属性,或内容为空,同步下来的用户手机号字段将置空,若打开设 置中的二次认证选项,同步的用户将无法登录堡垒机。

云盾 ● 堡垒机	AD/LDAP设置		
概览	模式	AD •	
 > 资产 ▼ 用户 	*服务器地址	120.55.62.136	
用户管理	备用服务器地址		
AD/LDAP设置	*端口	389 SSL	
▶ 授权	*Base DN	OU=zzx,DC=cbq,DC=com	
 审计 系统 	*城	cbq.com	
操作日志	*帐号	administrator	
	密码		留空则不做修改
	过滤器		例:(&(objectClass=person))
	姓名	displayName	填写AD服务器上表示用户姓名的属性名,如:displayName
	邮箱	mail	填写AD服务器上表示用户邮箱的属性名,如:mail
	手机号码	mobile	填写AD服务器上表示用户手机号码的属性名,如:telephoneNumber
		测试连接	
	保存设置		

3. 配置完成后,单击页面下方测试连接,若结果如图所示,单击保存设置。

测试连接 测试连接成功

若结果如下图所示,则证明堡垒机与AD服务器之间网络或端口不通,需对网络进行排查。

测试连接 主服务器测试连接失败,请检查IP和端口是否填写正确。

4. 配置完成后,进入堡垒机用户 > 用户管理菜单,单击右上方导入AD/LDAP用户,可将Base DN中的用户加入至堡垒机。

导入	AD/LDAP用户						×
	已导入(0)	未見	}入(3)		输入用户名/姓名/手机号	冯模糊查询	搜索
	用户名	姓名	手机号码	邮箱	认证源	状态 (全部) ▼	
	test1	test1	136	xxxxx@xxx.com	AD	正常	
	test2	test2	136	xxxxx@xxx.com	AD	正常	
	test3	test3	136	xxxxx@xx.com	AD	正常	

加入云堡垒机

🔲 加入时覆盖同名用户(若不勾选,则无法加入同名用户)

5. 用户加入堡垒机后,可以运维登录操作。

LDAP设置

1. 登录堡垒机Web管理页面,进入用户 > AD/LDAP设置菜单,将模式调整为LDAP。

2.	在页面依次填入LDAP	服务器信息。
----	-------------	--------

云盾 ● 堡垒机	AD/LDAP设置			
概览	模式	LDAP •		
▶ 资产				
▼ 用户	*服务器地址	118.31		
用户管理	备用服务器地址			
AD/LDAP设置	*端口	389 🔲 SSL		
▶ 授权	*Base DN	dc=my-domain,dc=com		
▶ 审计		an Managar da mu damain da com	/El : en Managor de jou	
▶ 系统	<u>₹</u> ₩*	cn=Manager,ac=my-domain,ac=com	191]: cn=Manager,dc=ex	ampie, dc=com
操作日志	密码		留空则不做修改	
	过滤器			例:(&(objectClass=person))
	登录名属性			默认值为uid
	姓名	displayname	填写LDAP服务器上表示用	用户姓名的属性名 , 如:fullName
	邮箱	mail	填写LDAP服务器上表示F	用户邮箱的属性名,如:mail
	手机号码	mobile	填写LDAP服务器上表示F	用户手机号码的属性名,如:mobile
		测试连接测试连接成功		
	保存设置			

3. 测试连接通过后,保存设置。

4. 参考AD域设置,导入用户,并使用LDAP用户进行认证登录。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.8 配置备份管理

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。堡垒机配置包含所有配置数据, 如 用户、资产、授权、系统等配置数据, 不包含审计日志。

自动配置备份

登录云盾堡垒机Web管理页面,定位到系统 > 配置备份管理,选择启用自动备份,设置备份周 期,单击保存设置。

配置备份管理

选项	□ 允许同阿里	云账户下的其他堡垒	机使用本机备份
自动备份	启用		V
备份周期	1	天	
	自动备份的执行	示周期 , 有效值1-60。 	自动备份会在凌晨2:00 - 5:00进行。
保存设置 手动备份			
本地备份最多保存30条。备份时如]果超出限制,将	将会自动删除最早的	条备份。

手动配置备份

登录云盾堡垒机Web管理页面,定位到系统 > 系统备份管理,单击手动备份,自动生成一条备份记

录。

保存设置 手动备份 本地备份最多保存30条。备份时如果超出限制	」,将会自动删除最早的一条备份。	
本机备份		
名称	备份时间	操作
201712191351-v2.1.4	2017-12-19 13:51:58	还原 删除

共享备份

1. 登录云盾堡垒机Web管理页面,定位到系统 > 配置备份管理,选择勾选下图选项,单击保存设置。

配置备份管理

选项	✓ 允许同阿里云账户下的其他堡垒机使用本机备份
自动备份	启用 ▼
备份周期	1 天 自动备份的执行周期,有效值1-60。自动备份会在凌晨2:00-5:00进行。
保存设置 手动备份 本地备份最多保存30条。备份时处	u果超出限制 , 将会自动删除最早的一条备份。

使用该账号下其他堡垒机登录堡垒机Web管理页面,定位到系统 > 配置备份管理,共享备份将 出现上面堡垒机配置备份数据。

说明: 共享账号只能在同一个账	号下不同堡垒机之间使用。		
共享备份			
名称	实例ID	备份时间	操作
201712191035-v2.1.5	bastionhost-cn-45906fapf005	2017-12-19 10:36:00	还原
201712142220-v2.1.4	bastionhost-cn-vj3065s0g001	2017-12-14 22:20:45	还原
201712142158-v2.1.4	bastionhost-cn-45906fapf005	2017-12-14 21:58:49	还原
201712142158-v2.1.4	bastionhost-cn-45906fapf005	2017-12-14 21:58:44	还原
201712142155-v2.1.4	bastionhost-cn-45906fapf005	2017-12-14 21:55:55	还原

还原备份

登录云盾堡垒机Web管理页面,定位到系统 > 配置备份管理,在本机备份或共享备份列表中,选择 一条记录,单击还原,自动还原该备份数据。

本机备份			
名称	备份时间		操作
201712191351-v2.1.4	2017-12-19 13:51:58		还原 删除
201712190333-v2.1.4	2017-12-19 03:34:01		还原 删除
			« < 1 > »
共享备份			
名称	实例ID	备份时间	操作
201712191035-v2.1.5	bastionhost-cn-45906fapf005	2017-12-19 10:36:00	还原
201712142220-v2.1.4	bastionhost-cn-vj3065s0g001	2017-12-14 22:20:45	还原
201712142158-v2.1.4	bastionhost-cn-45906fapf005	2017-12-14 21:58:49	还原

删除备份

登录云盾堡垒机Web管理页面,,定位到系统 > 配置备份管理,在本机备份列表中,选择一条记录,单击删除,自动删除该备份数据。

本机备份			
名称	备份时间		操作
201712191351-v2.1.4	2017-12-19 13:51:58	还原	删除
201712190333-v2.1.4	2017-12-19 03:34:01	还原	删除
		« < 1 >	»

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.9 控制策略管理

在云盾堡垒机Web管理界面,您可以执行以下与控制策略相关的操作:新建、编辑、克隆、删除。

新建控制策略

参照以下步骤新建控制策略:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权策略, 单击新建控制策略。

 在新建控制策略页面,填入控制策略名称,选择启用并编辑需要的控制策略。您可以选择启用的 控制策略包括:

云盾 • 堡垒机	新建控制策略 < 返回控制策略列表	
概览	通用属性	
▶ 资产	名称	
▶ 用户		
▼ 授权	协议控制	
授权组	状态 禁用 ▼	
控制策略		
▶ 审计	来源IP控制	
▶ 系统	状态	
操作日志		
DATI E.G.	访问时段控制	
	状态 禁用 ▼	
	命令控制	
	状态	
	确定	

·协议控制:选择启用,展开协议控制选项,根据自身需求勾选需要控制的项目。



·来源IP控制:选择启用,展开来源IP控制输入框,填入允许访问的IP或IP段。

来源IP控制	
105	起用 •
允许的来源即	192.168.0.1 192.168.0.1 - 192.168.0.255
	構築部分上連時度式200×地址1200×地址1200-00 構築部分上連時度式200×地址1200×地址1200-00 時代現現一个印度著一段10、回發的起源印料出現印料出現10、101、168.0.1 - 192.168.0.251 若常等項目指称意見: 流行消以1*17升点。

·访问时间段控制:选择启用,展开访问时间控制选项,选择编辑允许访问的时间段。



 ・命令控制:选择启用,展开命令控制输入框(只针对SSH字符命令有效),填入需要禁止的 命令。

命令控制	
状态	2月 •
禁止的命令列表	es "a" axid
	填写命令以行为单位,每一行为一个命令单元(命令+参数),命令和参数力模糊匹配(支持通影符?*[])
	例1:匹配config命令:请填写config部相应的列表中,若要匹配以an开头的命令,请填写an* 份2:匹配os命令及auxef中任意一个参数:请填闭os *a* *u* *x* *a* *f*等相应的列表中,参数匹配沟锁库开

4. 全部策略编辑完成后,单击确定,返回控制策略列表可看到新建的控制策略。

编辑控制策略

参照以下步骤编辑控制策略:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权策略,选择您需要编辑的控制策略,单击右侧的编辑。
- 3. 在进入编辑页面后,进行相应的修改编辑,修改完成后单击确定。

克隆控制策略

参照以下步骤克隆控制策略:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权策略,选择您需要编辑的控制策略,单击右侧的克隆。
- 3. 在弹出的对话框中填写通过克隆创建的控制策略名称,单击确定。

克隆控制策略:测试		\times
• 控制策略名称		
	确定	取消

删除控制策略

参照以下步骤删除控制策略:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到授权 > 授权策略, 勾选您需要删除的控制策略, 单击删除。

控制)策略					新建控制策略
输入	空制策略名称模糊	查询 搜	索			
	名称	协议控制	来源IP控制	访问时段控制	命令控制	操作
✓	测试	×	关	×	 <i></i>	编辑 克隆
	删除					« < 1 > »

3. 确认无误后, 在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.10 服务器组管理

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。

新建服务器组

1. 登录云盾堡垒机Web管理页面,定位到资产 > 服务器组,单击页面右上角的新建服务器组。

C 管理控制台			admin
云盾 • 堡垒机	服务器组		新建成分器组
概览	输入服务器组名称模糊查询 搜索		
▼ 资产	名称	服务器	操作
服务器	aaa-ccc	2	修政名称
服务器组	bbb-bb	1	修改名称
凭据	cbqgroup	2	修改名称
 用户 授权 	册除		

2. 在新建服务器组窗口中,填写服务器组名称后,单击确定。

 C-) 管理控制台 				
云盾。 堡垒机	服务器组	新建服务器组	×	新建艇务继知
概览	输入服务器组名称模糊查询			
▼ 资产	名称			操作
服务器	aaa-ccc		确定取消	修改名称
服务器组	bbb-bb	1		修改名称
凭据	cbqgroup	2		修改名称
 用户 授权 				

修改服务器组名称

1. 登录云盾堡垒机Web管理页面,定位到资产 > 服务器组,单击修改名称。

C-) 管理控制台			admin
云盾 • 堡垒机	服务器组		所建版务器相
概览	输入服务器组名称模糊查询 搜索		
▼ 资产	名称	服务器	操作
服务器	aaa-ccc	2	修改名称
服务器组	bbb-bb	1	修改名称
凭据	cbqgroup	2	修改名称
▶ 用户			
▶ 授权	10964		« (1) »

2. 在修改服务器组窗口中,修改服务器组名称后,单击确定。



修改由ECS标签同步过来的服务器组名称,不会影响ECS标签信息。

C-D 管理控制台				admin
云盾。堡垒机	服务器组	修改服务器组	×	新建服务器组
概览	输入服务器组名称模糊查询	* 服务器组名称 aaa-ccc		
▼ 资产	名称			操作
服务器	aaa-ccc		确定取消	修改名称
服务器组	bbb-bb	1		修改名称
凭据	cbqgroup	2		修改名称
▶ 用户 ▶ 授权				

删除服务器组

1. 登录云盾堡垒机Web管理页面,定位到资产 > 服务器组,勾选您想要移除的服务器,单击列表

下方的删除。

云盾 ● 堡垒机	服务器组		新建服务器组
概览	输入服务器组名称模糊查询 搜索		
▼ 资产	名称	服务器	操作
服务器	aaa-ccc	2	修改名称
服务器组	bbb-bb	1	修改名称
凭据	Cbqgroup	2	修改名称
 用户 授权 			« < 1 > »

2. 确认无误后, 在弹出的对话框中单击确定。

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web管理页面。

2.11 透明代理

本文受众范围: 云盾堡垒机运维人员。

透明代理(socks5代理)模式

堡垒机透明代理(socks5代理)模式,针对linux运维体验进行优化,旨在提高运维人员体验,契 合原有的运维习惯,请结合自身情况判断是否需要使用。

实现原理

- 1. 建立ssh的socks5隧道,隧道建立后产生数据通道A通道为: socks5服务端—ssh客户端进程1 --堡垒机ssh服务
- 2. 设置socks5代理,使对目标主机的访问通过socks5隧道完成。最终的数据通道为:ssh客户端 进程2—socks5客户端—A通道—目标主机

图形客户端配置

以Xshell为例,操作步骤如下:

1. 新建Xshell会话,建立ssh的socks5隧道,即与堡垒机建立隧道连接在会话配置中分别填入堡 垒机IP、端口(60022)。

堡垒机属性				?	\times		
类别(C):							
 ● 连接 ● 用户身份验证 ● 登录提示符 ● 登录脚本 ● SSH ● SSH ● 安全性 	连接 常规 名称(N): 协议(P):	堡垒机 SSH	~				
► 隆道 SFTP TELNET RLOGIN SERIAL 代理 保持活动状态	主机(H): 端口号(o): 说明(D):	120.55. 60022					
□ (健盘 	重新连接 □ 连接异常关 间隔(\/): TCP选项	闭时自动重新连接(A) 0 💽 秒	限制(L): 0	♣ 分	钟		
➡ 文件传输 — X/YMODEM — ZMODEM — ZMODEM — ZMODEM	☐ 使用Nagle算	፤法(ሀ)	确定	取洋	Ĭ		

・填写堡垒机用户名密码/密钥(也可打开会话时手动输入)。



· ssh配置,勾选红框中内容。
堡垒机属性

? X



・进入会话属性的SSH-隧道菜单。

堡垒机属性

×

?

类别 <u>(C</u>):	
 ● 连接 ● 用户身份验证 ● 金录提示符 ● 登录脚本 ● SSH 	连接 > SSH > 隧道 TCP/IP转移 添加/编辑/删除TCP/IP转移规则。此规则连接后自动应用。
安全性 隧道 SFTP TELNET RLOGIN SERIAL 代理 保持活动状态	类型 侦听端 目标 说明
│	添加(<u>A</u>) 编辑(<u>E</u>) 删除(<u>R</u>) X11转移
□ 高级 □	□ 转发X11连接到(<u>X</u>): ③ Xmanager(<u>M</u>) ③ X DISPLAY(<u>D</u>): localhost:0.0
	确定取消

・単击添加,按下图设置。

转移规则		?	\times
类型 <mark>(方向)(</mark> T):	Dynamic (SOCKS4/5)		\sim
源主机(s):			\sim
侦听端口(L):	1080 ~		
	☑ 仅接受本地连接(A)		
目标主机(н):			\sim
目标端口(P):	~		
说明(D):			
	确定	取	消

・ 单击确定,保存并打开会话,保持在如下界面,此时隧道已经建立。

```
● 1 堡垒机 × +

Xshell 5 (Build 0964)

Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.

[c:\~]$

Connecting to 120.55. :60022...

Connection established.

To escape to local shell, press 'Ctrl+Alt+]'.
```

2. 新建会话,填写目标服务器IP、端口。

服务器属性

服务器属性				?	\times
类别(<u>C</u>):					
 □ □ 用户身份验证 □ 登录提示符 □ □ ご □ ○ SSH □ □ ○ SSH □ □ ○ SSH □ □ ○ SSH □ □ ○ ○<td>连接 常规 名称(N): 协议(P): 主机(H): 端口号(O): 说明(D):</td><td>服务器 SSH 101.37 22</td><td>~</td><td></td><td></td>	连接 常规 名称(N): 协议(P): 主机(H): 端口号(O): 说明(D):	服务器 SSH 101.37 22	~		
□ ~ ³ □ · 健盘 □ · VT 模式 □ · 高级 □ · 边距 □ · 高级 □ · 助距 □ · 品级 □ · 小观 □ · 边距 □ · 小 □ · · · · · · · · · · · · · · · · · · ·		:闭时自动重新连接(A) 0 ● 秒 I法(U)	限制(L): 0	• 分	钟
			确定	取消	Í

・填写服务器用户名密码(也可打开会话时输入,若堡垒机授权组内绑定了凭据,则可只填用 户名,不需要填写密码)。



・进入SSH-代理菜单,单击浏览。

服务器属性				?	\times
类别(C):					
→连接	连接> 代理				
 □用尸身份验证 □登录提示符 □登录脚本 □SSH □SSH □SCH □SCH<td>- 代理服务器 用户的网络环境使用 的服务器。若要添加</td><td>代理服务器防火墙 /编辑/删除代理服彡</td><td>时请在如下列 务器的话请点</td><td>]表中选择帖 击"浏览"。</td><td>当</td>	- 代理服务器 用户的网络环境使用 的服务器。若要添加	代理服务器防火墙 /编辑/删除代理服彡	时请在如下列 务器的话请点]表中选择帖 击 " 浏览"。	当
SFTP	代理服务器(R):	<无>	\sim	浏览 <mark>(B)</mark>	
 RLOGIN SERIAL 代理 保持活动状态 终端 建盘 VT 模式 高级 力距 高级 田志记录 文件传输 X/YMODEM ZMODEM 		Γ	協会	υ ΈΓΠ ζ ¹	
			确定	取消	i

・単击会话,添加代理,按照下图配置。

代理服务器设置	×
名称(<u>N</u>):	堡垒机代理
类型(<u>T</u>):	SOCKS5 ~
主机(出):	127.0.0.1
端口(<u>P</u>):	1080
用户名(<u>U</u>):	
密码(<u>A</u>):	
	确定 取消

・保存后,返回代理菜单勾选该服务器。

连接> 代理		
─代理服务器 用户的网络环境使用 的服务器。若要添加	代理服务器防火墙时请 /编辑/删除代理服务器的	在如下列表中选择恰当 的话请点击"浏览"。
代理服务器(<u>R</u>):	堡垒机代理	─ 浏览(B)

· 打开会话,可直接登录至已授权给用户使用的服务器,且流量可在堡垒机内进行审计。

Xshell 5 (Build 0964) Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved. Type `help' to learn how to use Xshell prompt. [c:\~]\$ Looking up proxy server '127.0.0.1'... Host '127.0.0.1' resolved to 127.0.0.1. Connecting to 127.0.0.1:1080... Connection established. To escape to local shell, press 'Ctrl+Alt+]'. Last login: Thu Nov 2 14:21:04 2017 from 120.55 Welcome to Alibaba Cloud Elastic Compute Service ! [root@iZbp1f4z1of2bfb5w17yxsZ ~]# 3. 批量配置代理服务器可在建立多个Xshell会话后,选中多个会话,点击右键属性,批量配置代理服务器。

🍄 会话							×
答:新建 ▼ 🗐 👗 🖻 🖻 🗙 🗟 🗮			•				Q
所有会话						62	¢
名称 ▲	主机	端口	协议	用户名	说明		
🛛 🖾 堡垒机	120.55.3	60022	SSH	13684			
₩₩条器	101.37.1	22	SSH				
₩₩₩5器1	101.11.1	22	SSH				
₩₩₩5器2	101.13.4	22	SSH				
☑ 启动时显示此对话框(s)			<u>ک</u> ٹ	控合	-	と词	
			圧	按(U)		天内	

多个会话的性质		?	×
类别(<u>C</u>):			
□ 连接	连接> 代理		
□ 用 广牙访短证 □ 登录提示符 □ 登录脚本 □ SSH □ SSH	代理服务器 用户的网络环境使用代理服务器防火墙时请在如下 的服务器。若要添加/编辑/删除代理服务器的话请点	列表中选择' 贰击"浏览"。	恰当
·····································	代理服务器(<u>R</u>): * 堡垒机代理 ~	浏览(<u>B</u>)	•
	确定	取氵	肖

4. 配置完成后,只需打开Xshell会话即可登录服务器,不需要先登录堡垒机再选择服务器进入。

openssh配置

说明:

此方法不支持密钥登录堡垒机(密钥登录服务器可将私钥存在堡垒机凭据中)

```
#堡垒机别名
Host __USM__
#堡垒机用户名(本地账号、AD/LDAP账号、RAM子账号)
User 136xxxxxxx
#堡垒机IP
Hostname 120.55.xx.xx
#端口
Port 60022
```

#目标服务器

Host 1* 2* 3* 4* 5* 6* 7* 8* 9* #关闭密钥验证 PubkeyAuthentication no #设置堡垒机为代理 ProxyCommand ssh -F /root/.ssh/ssh_config -A -q __USM__ -W %h:%p Host a* b* c* d* e* f* h* i* j* k* l* m* n* o* p* q* r* s* t* u* v* w* x* y* z* PubkeyAuthentication no ProxyCommand ssh -F /root/.ssh/ssh_config -A -q __USM__ -W %h:%p Host A* B* C* D* E* F* H* I* J* K* L* M* N* O* P* Q* R* S* T* U* V* W* X* Y* Z* PubkeyAuthentication no ProxyCommand ssh -F /root/.ssh/ssh_config -A -q __USM__ -W %h:%p

- 2. 指定配置文件即可通过堡垒机进行登录、文件上传下载等操作。
 - ・通过堡垒机登录xxx.xxx.xxx.xxx服务器。ssh -F .ssh/ssh_config root@xxx.xxx

.xxx.xxx

按要求输入堡垒机用户密码。

・通过堡垒机与xxx.xxx.xxx.xxx互相上传下载文件。scp -F .ssh/ssh_config

filename root@xxx.xxx.xxx.xxx:/

送明:

若连接时出现如下错误: ssh_exchange_identification: Connection closed by remote host, 请删除~/.ssh/known_hosts后再次执行。

Ê	说明:
	00.91.

此功能的目的为减少运维人员登录操作,请依据自身情况判断酌情使用。

2.12 存储管理

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。

自动清除录像

进入系统 > 存储管理页面, 自定义配置录像数据清除时间, 配置后单击保存设置。

(•)	管理控制台	
云盾●	墨垒机	存储管理
概览		存储设置
▶ 资产		洗师 自动清除 180 天前的录像数据 有效值1-365
▶ 用户		等保合规需要保存180天内的审计录像数据,请勿轻易设置为小于180的值。
▶ 授权		磁盘空间满时自动删除最早的数据 等保全机需要保存180千内的审计录像数据 开启此选顶有可能导致180千内的数据被删除
▶ 审计		
▼ 系统		保存设置
系统	设置	
存储	管理	
操作日	志	

审计录像归档

进入系统 > 存储管理界面, 在审计录像归档处自定义配置远程归档相应数据, 配置后单击保存设置。

管理控制台		
云质。保奈圳	审计录像归档	
	状态	启用 ▼
概览		
▶ <u>资</u> 产	时段	U - 23 每天进行录像归档的时段。有效值0-23
▶ 用户	冲座 限 制	
▶ 授权	A THE LEVEL OF THE PARTY OF THE	B B B B B B B B B B B B B B B B B B B
▶ 审计	传输模式	FTP
▼ 系统	ᄪᇶᇔᆂ	
系统设置	NGSERFIC	
存储管理	端口	21
西置备份管理	用户名	
操作日志	密码	留空则不做修改
	Re/72	
	頃仕	绝对路径或相对路径,并确保用户具有此路径的写入权限

2.13 用户管理

在云盾堡垒机Web管理页面,您可以执行以下与用户相关的操作:新建本地用户、新建/导入云子 账号、导入AD/LDAP用户、修改用户、配置公钥、搜索用户、删除用户。

新建本地用户

参照以下步骤新建本地用户:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理, 单击新建本地用户。
- 3. 在新建本地用户对话框中填写以下用户信息:

手机号码	
节为运维登录名	
密码	
3-64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; 4.
⊪字母符号如@,∉,\$。	
⊪字母符号如@,≉,\$, ₿件	
非学母符号如合,#,\$。 邮件 生名	
#字母符号如色, #,s. ### 生名	

- ・手机号码:必填,填写11位真实手机号。
- · 密码: 必填,由8到64个字符组成,必须同时包含大小写字母、数字、和特殊符号(@#\$)。
- ·邮箱:选填,如果填写则必需使用真实且符合规范的邮箱地址。
- ・姓名:选填。

新建云子账号

参照以下步骤新建云子账号:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理, 单击新建云子账号。

3. 在子账号管理页面, 您可以执行以下操作:

- ・导入子账号
 - a. 单击导入子账号, 直接导入RAM子账号信息。
 - b. 在导入阿里云子账号用户对话框, 勾选需要导入的子账号, 单击导入子账号。

寻入阿里云子账	号用户			>
登陆名	7	道		
□ 登录名	显示名	手机号码	邮箱	状态
zzx123	zzx123		123@12.com	正常
日 导入子	长号	共有1条,每页	显示:10条 « ‹	1 > »

新建子账号

a. 单击新建子账号,页面跳转至访问控制 RAM的用户管理页面。

- b. 在RAM用户管理页面新建RAM子账号,具体操作见用户管理。
- ・编辑子账号
 - a. 选择要修改的子账号,单击其操作列下的编辑,页面跳转至访问控制 RAM的用户管理页面。
 - b. 在RAM用户管理页面修改目标子账号信息,具体操作见用户管理。
- 移除子账号:选择要删除的子账号,单击其操作列下的移除,将其从云盾堡垒机子账号列表
 中移除。

📃 说明:

该操作不会影响访问控制 RAM中的子账号信息。

·解锁子账号:选择要解锁的子账号,单击其操作列下的解锁,将其锁定状态解除。

📃 说明:

使用子账号登录时,如果在一小时内密码错误4次,则子账号会被锁定。

・刷新子账号数据:单击列表下方刷新子账号数据,可以从访问控制 RAM 同步RAM子账号信
 息到堡垒机子账号管理。

导入云子账号

参照以下步骤导入云子账号:

1. 登录云盾堡垒机Web管理页面。

- 2. 定位到用户 > 用户管理, 单击导入云子账号。
- 3. 当堡垒机自动获取云子账号信息后,在弹出的对话框中勾选所需添加的云子账号,单击加入云堡 垒机。

搜索

导入AD/LDAP用户

参照以下步骤导入AD/LDAP用户:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理, 单击导入AD/LDAP用户。

📋 说明

```
您必须先在用户 > AD/LDAP设置页面配置好AD/LDAP服务器器信息。
```

3. 当堡垒机自动获取AD/LDAP用户信息后,在弹出的对话框中勾选所需添加的用户,单击加入云 堡垒机。

λΑΙ	D/LDAP用户						×
	已导入(0)	未	导入(1)	输	入用户名/姓名/手机号码	马模糊查询	搜索
	用户名	姓名	手机号码	邮箱	认证源	状态 (全部) 🔻	
~	cccbq		654321@qq.com	654321@qq.com	LDAP	正常	

修改用户

参照以下步骤修改用户:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理,选择您想要修改的本地用户,单击右侧的修改。



3. 在修改用户对话框中,修改用户信息,单击确定。

配置公钥

参照以下步骤配置公钥:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理,选择您想要配置公钥的本地用户,单击右侧的配置公钥。



用户配置公钥后,SSH协议运维操作就可以通过公私密钥对的方式登录堡垒机。

3. 在配置公钥对话框中, 配置用户公钥信息, 单击确定。

3明	
ssh-rsa AAAAB3NzaC1yc2I M1BFHIxKI1cyTO5 CE4TfUcZpVAwfL6 PJuP2xobVyn9uux RHkIoRUxA3b4/F0	AAABIwAAAEA2P59/ZngImJ+kaAdB7RoAGSTYxpEEZ/C0TBI DemcMithLapTPU9TUbLiSeVY4fLvyWC3gWVY2jktfmoVQRWW PFF7q222JXGSV39aqH61nJHzg90/ <u>dTGwRHu7ZU</u> +4sootUv0YY drWmo2872CCuu/WT4okyFPrychac5bedXehrTE1WWCDJpUD
PYGRq+ZhlQPWxC	8CIkUdhe3MHkco1yofw== root@centos83

搜索用户

参照以下步骤搜索用户:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理,在用户列表上方的搜索框中填写姓名、手机号码、或邮箱,单击搜索,即可对填写的字段进行模糊查询。

用户管理 输入线名/手机导码/邮件德服查询 推索

删除用户

参照以下步骤删除用户:

- 1. 登录云盾堡垒机Web管理页面。
- 2. 定位到用户 > 用户管理, 勾选您需要删除的用户, 单击用户列表下方的删除。

您也可以单击用户列表下方的单选框勾选本页所有用户,然后单击删除。

3. 确认无误后, 在弹出的对话框中单击确定。

✓	ramtest		ZZX	
✓	zzx123		zzx123	
	禁用	启用	删除	

启用/禁用用户

参照以下步骤删除用户:

1. 登录云盾堡垒机Web管理页面。

2. 定位到用户 > 用户管理, 勾选您想要禁用或启用的用户, 单击列表下方的启用或禁用。

-		100.00	
		100	1000
総用	席用	制除	

如何登录到云盾堡垒机Web管理页面

参照以下步骤登录云盾堡垒机Web管理页面:

- 1. 登录云盾堡垒机控制台。
- 2. 选择要操作的堡垒机实例,单击其操作列下的管理。
- 3. 选择接入方式,连接目标堡垒机Web 管理页面。

3运维使用手册

3.1 SSH协议运维

本文受众范围:运维工程师、云盾堡垒机管理员、持有阿里云帐号的管理员。

背景信息

运维人员需要通过本地的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。

说明:

请确认在本地主机已安装支持 SSH 协议的运维工具,如 Xshell、SecureCRT、PuTTY 等工具。

下文以Xshell工具为例,介绍运维登录流程:

操作步骤

1. 打开Xshell工具,在连接设置中输入云盾堡垒机的IP和SSH端口号(SSH端口号默认为 60022)。

新建会话属性				?	Х
<u> 类别(C):</u>					
	连接				
□·用户身份验证 □·※录提示符	常规				
登录脚本	名称(≥):	云盾系统			
⊡-SSH	协议 <mark>(</mark> D):	SSH	\sim		
安主任	主机田:				
SFTP	端口号(<u>O</u>):	60022			
RLOGIN	说明(D):				
SERIAL 					
保持活动状态			1		
□ 终端	重新连接				
₩ 進益	□ 连接异常关闭	时自动重新连接(A)			
高级	间隔♥):	0 💠 秒	限制(): 0	👙 分钟	;þ
□		Lummed			
日高级	TCP选项				
一跟踪	☐ 使用Nagle算法	ŧ(U)			
□ 文件传输					
X/YMODEM					
			确定	取消	

新建会话属性				?	×		
类别(C):							
□·连接	连接 > 用户身份验证						
日用户身份验证	请选择身份验证方法和其它参数。						
登來症亦付	会话属性中此部分是为了登录过程更便捷而提供的。如果需要安全性很						
⊡ SSH	的状态的话建议您空出此字段。						
安全性							
™®≝⊅⊒ SFTP	方法()):	Password	\sim	设置(S)			
TELNET	用户名(U):	183		- 9			
SERIAL	密码(P):	•••••		- mil			
	用户密钥(K);	<无>	\sim	浏悟(B)			
·····徐衍活动状态	家码(a);			11/4			
社会	10 H-1 (10) ·						
□- 外观	注释: 公钥和Keyboar	d Interactive仅在SSH/SFTP协议	(中可用	•			
边距							
□ □ 高级							
一般际日志记录							
□文件传输							
···· X/YMODEM							
····· ZMODEM							
		确	定	取消	Í		

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。



如果管理员在云盾堡垒机中配置了用户公钥,则用户可以通过公私密钥对的方式登录,无需输 入密码。在用户身份验证设置中,选择Public Key,输入云盾堡垒机用户名,选择对应的私 钥。

属性				?	×	
类别(C):						
三连接	连接 > 用户身份	验证				
- 登录提示符	请选择身份验证方	请选择身份验证方法和其它参数。				
登录脚本	会话属性中此部分	会话属性中此部分是为了登录过程更便捷而提供的。如果需要安:			态的	
■SSH 一	建议惩空出此子母	(o				
- <u></u>						
SFTP	方注(M)·	Public Key	~	迟罗 (C	1	
RLOGIN	77125(11)	15200				
SERIAL	用户名(U):	15268		09		
一代理	密码(P):				£	
一保持活动状态 目终端	用户密钥(K):	id_rsa_wy	~	浏览(B)	
键盘	◎ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○					
- VT 模式 - 五-99	m + 4(- 4)-					
■外观						
一边距	注释:公钥和Keyb	oard Interactive仅在SSH/SFTP协	议中可用。			
□ 局级 - 跟踪						
日志记录						
■文件传输						
ZMODEM						
			70.03	Her 22	ste	
			佣儿	电关系	a	

3. 单击确定,连接云盾堡垒机。

(可选)如果管理员启用了双因子认证登录,将会弹出双因子口令对话框,请输入您手机上收到的6位数字。

2 云子	】 说明: ·帐号账户使用MFA进行	〕二次验证 。
Two-Step	Vertification required	×
23	Please enter the verification code sent to your mobile phone:	~
	□ 记住密码(R)	

5. 成功登录云盾堡垒机后,进入资产管理界面。通过键盘上的上、下箭头选择您想要进行运维的服 务器主机。

🥩 云盾系统 - USMShell - Xshell 5 (Free for Home/School)	-	
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)		
	3 🗇	-
B ssh://183. 60022		•
□ 要添加当前会话,点击左侧的箭头按钮。		
● <u>1</u> 云盾系统 × +		<
<pre>" Press <j>/<k> or <down>/<up> to move and then <enter> for login. " Press for search and then <n>/<n> to go to next and previous. " Press <u>/ or <pageup>/<pagedown> for page turning. " Press <:{num}> for goto line and then Type 'q' for quit. " Press <r>/<q> for reload and quit. "= NUM NAME IP PROTO USER COMMENT 1: host129 192.168.50.129 SSH admin host129</q></r></pagedown></pageup></u></n></n></enter></up></down></k></j></pre>		^
Type <enter> for login and <q> for quit.</q></enter>		
渠道 转移规则		~
ID 类型 从 到 创建时间 接收到字节 发送的字节		_
ssn://183 @ 60022 @ SSH2 xterm ↓ 110x26 @ 8,54 1 会	a T+	CAP NUM

6. 按 Enter 键即可登录目标服务器主机进行运维操作。

参 云盾系统 - root@129:~ - Xshell 5 (Free for Home/School)	
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)	
	-
☐ ssh://183 :******@ 60022	•
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
● <u>1</u> 云盾系统 × +	<
Last login: Tue Apr 18 15:40:08 2017 from	^
	~
渠道 转移规则	
ID 类型 从 到 创建时间 接收到字节 发送的字节 内容立木岩洋列当台法语点上	. =
ssh://183 の :60022 の SSH2 xterm だ 110x26 in 2.12 1 会話 小山	

3.2 RDP协议运维

本文受众范围:运维工程师、云盾堡垒机管理员、持有阿里云帐号的管理员。

背景信息

运维人员需要通过本地的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。下文 以 Windows 系统自带的 远程桌面连接工具(Mstsc)为例说明运维登录流程:

操作步骤

1. 在本地 Windows 系统主机中打开远程桌面连接工具(Mstsc)。

2. 输入云盾堡垒机的 IP 和 RDP 端口号(RDP 端口号默认为 63389): < IP >:63389, 单



击连接。

堡垒机

🌄 远程桌面连接	妾			_		×
人 。 道	程桌面 接					
计算机(<u>C</u>):	116.1	:63389		\sim		
用户名:	未指定					
当你连接时将向	可你询问凭据。					
全 显示选项(<u>(</u>	<u>2</u>)		连接(<u>N</u>)	帮助(<u>ト</u>	<u>+</u>)

3. 在是否信任此远程连接?对话框中,单击连接。

	桌面连接		×
٢	是否信任此远程连接?		
此远程道	在接会损坏你的本地或远程说	†算机。请确保你在连接之前信任此远程	计算机。
	类型: 远程计算机:	远程桌面连接 116.	
□不再	询问我是否连接到此计算机	(O)	
💽 显示	详细信息(D)		连接(N) 取消(C)

4. 在无法验证次远程计算机的身份。是否仍要连接?对话框中,单击是。

100 远程桌面连接 X
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
■ 请求的过程计算机: ■ 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。
您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 (0)
查看证书 (Y) 是 (Y) 否 (M)

5. 在云盾堡垒机登录窗口中,输入云盾堡垒机的用户名和密码。

登录	
用户名:	
136	
密码:	

登录	
退出	

6. 单击登录,登录云盾堡垒机。



**如果管理员启用了双因子认证登录,将会弹出双因子口令对话框,请输入您手机上收到的6位 数字。

双因子口令:	
Please enter the verification code sent t o your mobile phone:	
确认 取消	



云子帐号使用MFA进行二次验证。

7. 成功登录云盾堡垒机后,进入资产管理界面,双击您需要登录的已授权服务器主机进行登录。

授权主机		
主机名	IP	账户名
zzxtest	120	administrator
zzxtest	120.	administrator

8. 进入目标服务器主机的登录界面,输入主机的账户和密码。

道 说明:



若已在堡垒机中添加凭据,且该凭据添加到该用户的授权组中,则无需输入主机账户密码可直 接登录主机。

9. 按Enter键即可登录服务器主机进行运维操作。

3.3 SFTP协议运维

运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。

背景信息

运维员通过本地的客户端工具登录云盾堡垒机,再访问目标主机。

| ■ 说明:

您必须先在本地安装好支持SFTP协议的运维工具,如:Xftp、WinSCP、FlashFXP等。

下文以Xftp为例介绍运维登录流程:

操作步骤

21-1	1	L1	
1禾	24	厏	
		'V	LL.

1. 打开Xftp工具,在登录窗口中输入云盾系统的IP、端口号60022、用户名、密码。

云盾堡垒机 属性			?	Х
常规 选项				
FTP 站点				
名称(N):	云盾堡垒机			
主机(H):	120.27.14.103			
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):				1
登录 □ 座々啓寻(A)				
□ 使用身份验证代理(G)				
方法(M):	Password	~	设置(S)	
用户名(U):				1
密码(P):				
用户密钥(K):		~	浏览(B)	
密码(E):				
		花中	Ura Nid	
		佣疋	収泊	

说明:

如果管理员在云盾堡垒机中配置了用户公钥,则用户可以通过公私密钥对的方式登录,无需输 入密码。 在用户身份验证设置中,选择Public Key,输入云盾堡垒机用户名,选择对应的私 钥。

TP 站点				
名称(N):	云盾堡垒机			
主机(H):	120.27.14.103			
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):				1
×=				
□ 使用身份验证代理	₽(G)			
方法(M):	Public Key	~	设置(S)	
用户名(U):	152			
密码(P):				
田白宓钮///)・	id_rsa_wy	~	浏览(B)	
用广省玥(N).				
帘码(E):				

2. 单击 确定,连接云盾堡垒机。

E	沿时。
	- 尻明:

如果管理员启用了双因子登录,将会弹出双因子口令对话框,请输入您手机上收到的6位数字。

Two-Step Vertification required					
23	Please enter the verification code sent to your mobile phone:				
		v			
	记住来四(B)				

说明:

云子帐号账户使用MFA进行二次验证。

3. 成功登录云盾堡垒机后,在右侧可以看到已授权的服务器主机列表。

✓ 云蓝堡垒机 - Xftp 5 (Free for Home	a/School)		-	o ×
文件(F) 编辑(E) 查看(V) 命令(C) 工具(「) 窗口(W) 帮助(H)			
🖬 🖬 • 🥜 🥢 🐻 🛛 • 🗃 🗟	e 0 6 6 6 6 6 0 0			
主机名威户地址			• 用/	名 密码
• 文档 ·	<.	一元間保奈机		()
C\Users\wuyan\Documents	~ 80	(m) 1 /		~ BC
Bit accelerate accelerate Freedbacktub Impor NetSang OneNote #U2b Sport OneNote #U2b Vector #U2b Wechar Files Bitty Office Htg Bitty Office Htg Default rdp Bitty Office Htg Default rdp Bitty Office Htg Default rdp	大小 焼田 (秋辺)同 へ 2代-、2代・2017(64,-、 2代・2017(627,- 2代・2017(627,- 2代・2017(627,- 2代・2017(76,-) 2代・2017(76,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 2代・2017(71,-) 10,-) 1	E88 ^ Innow_0510030_next_BLGS	大小	类型 修改时间 文件 2017/11/2 文件 2017/11/2
名称	本地路径 <	£		
sit/a		二进制 1	対象	0 Byte

4. 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。



SFTP运维必须将有效凭据添加到相应授权组,否则无法登入ECS。

ℐ 云唐堡垒机 → Xftp 5 (Free for Hom	e/School)			- C	ı ×
文件(F) 编辑(E) 查看(V) 命令(C) 工具(T) 窗口(W) 帮助(H)				
🖬 🖬 • 💉 🖉 🐻 • 🕞 🗟	e 0 0 • 0 • 0 • 0 •				-
· 主机名成P地址				用户名	密码
• 文档	\leftrightarrow	- 云南堡垒机			\leftarrow \rightarrow
C:\Users\wuyan\Documents	~ 80	Hand I /root			- 60
名称 	大小、規則、使認時間 ~ 文化、2017年4, 2017年4, 2017年4, 2017年62, 2017年62, 2017年62, 2017年62, 2017年61, 20177575757575757575757575757575757575757	名称 ^	52	t小 类型 1 文件 2 文本	修改时间 2017/11/2 2017/11/2
a wuyan.png 金融合法分路 we	4KB PN., 2017/7/11 0 Rotas 立木 2017/10/1 ×	٢			>
10日の 名称 并本 讲座 ナ小	本地路经 < 远程路经 清齋 估计表	余 移			

〕 说明:

主机列表中第一个目录是为了转码使用,如果主机列表编码有问题,可双击第一个目录后刷新 进行转码。

3.4 Mac系统运维

本文受众范围:运维工程师、云盾堡垒机管理员、持有阿里云账号的管理员。适用于使用Mac电脑 通过本地客户端工具登录云盾堡垒机,再访问目标主机的运维工程师。

SSH协议运维

以MAC自带的命令行终端APP为例:

1. 打开命令行终端APP。

2. 输入以下命令: ssh 云盾堡垒机用户名@云盾堡垒机IP -p60022



3. 输入云盾堡垒机密码。





如果管理员启用了双因子登录,将会弹出短信口令对话框,请输入您手机上收到的6位数字。



4. 回车后进入资产管理界面,用上下键选择已授权的资产。

		•	wuya	an — USM	MShell —	ssh 🔳 🔳 💷	3@39.10	8.193.189 -p6002	22 — 80×24
A REPORT OF A REPORT OF A	===== Se: Passo Refi Lango	Quit: Move: arch: Jump: word: resh: uage:	Use Use Use Use Use Use Use Use	":q <ento the curs "/{patto ":{numbo ":passwo "r" to "e" to o</ento 	er>". sor keys. en) <enter er)<enter d<enter> refresh change la</enter></enter </enter 	, or "j" to go r>" and then "r r>" to jump to " to change you lists. anguage encodir	down, "k h"/"N" to line {nu ur passwo	(" to go up.) next/privous s umber).)rd. en UTF-8 and GB2	earching r
	NUM 01: 02:	NAME 堡	垒机 垒机	linux实 linux实	例 _ 勿 刷 例 _ 勿 刷	IP 101.37.15.190 101.37.15.190	PROTO SSH SSH	USER root administrator	COMMENT
Ū	ype <	Enter>	• for	login a	and <q></q>	for quit.			

5. 回车后进入目标主机界面,进行运维操作。



RDP协议运维

以远程桌面连接APP为例:

- 1. 打开命令行终端APP。
- 2. 输入云堡垒机的IP: 63389

	远程桌面连接		
Microsoft [®] 适用于 Mac	的远程桌面连接		
计算机: 39.108.193.1 (示例: MyPC, nan	189:63389 ne.microsoft.com, 192.168.2.8)	连接	

3. 单击连接后,弹出是否仍要连接此计算机?



• • •	39.108.193.189	
	登录	
	密码:	

	登录	
	退出	
企		

4. 单击连接后, 进入云堡垒机登录窗口, 输入: 云堡垒机的用户名和密码



如果管理员启用了双因子登录,将会弹出短信口令对话框,请输入您手机上收到的6位数字。



5. 单击登录后进入资产管理界面:用鼠标选择已授权的资产,或者通过搜索框搜索主机信息。

		00110011001100		
105477-0-40				
授权主机				
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IP	账白乞	备注	
上Windows家		root	8/1	
全型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型型	宾例_勿删L01.37.15.206	administrator		
	•			
	7			
			修改个人密码	注销

6. 双击之后即可进入目标主机进行运维操作。

• • •		39.108.193.189		
回收站				
	▶			
атна 🛃 🗾 🚆			الم	2

文件传输运维

客户端访问堡垒机,再选择ECS方式运维

以SecureFX工具为例:

1. 打开SecureFX工具。

000 SecureFX 3 64 5 -6 0 5 (Enter host <%R> Synchronize Options Tools Use PGP Connect V SecureCRT 🛞 🛃 Local (wuyandeMac.local) ✓ Filter <%F> /Users/wuyan/Desktop ▼ 📙 / Name Size Type . DocumentRevis... <u>.</u> Directory i wuyan.pngi 使用方法.txt .fseventsd .Spotlight-V100 4593 Portable Network Graphics image • • • 🗐 Connect 1053 text "I 🕄 🙆 🕺 🗅 🛍 🗙 😁 🗛 🔛 » .Trashes .vol Filter by session name <%I> 0 Applications bin cores Sessions dev . dev ► 📕 home Show dialog on startup ► Library a net Close Connect Network private sbin tmp Users Shared wuyan .bash_ses... .confia .putty .ssh 2 entries (plus 2 hidden entries) ω Transfer Queue Size of File Bytes Transferred Start Time Finish Time 2017/09/04 23:01 2017/09/04 23:01 Filename Progress Elapsed Time Time Left e Left Speed Status N/A 0.00 KB/s Finished /Applications/.localiz... /.localized 0% 0 bytes 0 00:00:01 /Users/wuyan/Deskt... /使用方法.txt 2017/09/04 23:01 2017/09/04 23:01 2017/09/04 23:01 2017/09/04 23:01 . /使用方法.txt 1.1 KB 1.1 KB 100% 00:00:01 N/A 0.00 KB/s Finished 00:00:00 N/A 0.00 KB/s Finished /Applications/使用方... 100% 1.1 KB 1.1 KB SecureFX Connect Reconnect Disconnect Synchronize Options Tools Use PGP SecureCR Enter host <%F S Local (wuyandeMac.local) ✓ Filter <%F> /Applications Appleations Appleati Anne Anne App Store.app A App Store.app Calculator.app Calculator.app Calculator.app Contacts.app Dashboard.app Dubleyer.app Contacts.app Dubleyer.app Contacts.app Dubleyer.app Contact.app Dubleyer.app Contact.app Dubleyer.app Contact.app Dubleyer.app Contact.app Dubleyer.app Contact.app Dubleyer.app Contact.app Cont Date Modified 2017/09/04 23:01 2015/06/17 12:31 2015/05/08/139 2015/08/22 19:30 2015/08/22 19:30 2015/08/22 11:48 2015/08/22 17:46 2015/08/22 17:46 2015/08/22 17:45 2015/08/22 19:15 2015/08/22 19:15 2015/06/08 11:01 Type Directory Directory Directory Directory Directory • • 🕵 Session Options - 116.62.158.231 Category: Connection Logon Actions SFTP Session Advanced Port Forwarding Remote/X11 Terminal Terminal SSH2 Hostname: 116.62.158.231 Port: 60022 0 irewall: None 2015/05/08 11:01 2015/05/04 17:05 2015/09/19 18:34 2015/08/22 19:23 2015/08/13 01:26 2015/08/22 17:45 Username: Authentication Sentout (X1) Sentout (X1) Sentout (X1) Modes Emacs Mapped Keys Advanced Apperance Advanced Password PublicKey Keyboard Interactive GSSAPI 2015/08/22 17:45 2015/09/03 23:18 2015/09/03 23:18 2012/05/07 14:21 2015/08/22 17:45 2015/09/04 00:11 2015/08/22 21:54 2015/10/08 20:00 2015/09/03 23:21 tmp Users usr var Volumes Ŧ Mission Control.aj Notes.app Photo Booth.app Photos.app Photos.app Preview.app Key exchange Freideauge GuickTime Player.app GuickTime Player.app Reminders.app Reminders.app Safariap Safariap SecureCRT.app SecureCRT.app System Preferences.ap Transmit.app Transmit.app Litilites ✓ ecdh-sha2-nistp521 ✓ ecdh-sha2-nistp384 ✓ ecdh-sha2-nistp256 ✓ diffie-hellman-group1. 2015/09/03 23:21 2015/10/02 22:33 2015/05/08 15:06 2017/09/03 22:26 2015/06/20 13:25 2016/12/02 10:01 2016/12/02 10:01 2015/08/22 18:48 2015/08/22 18:48 2015/08/22 18:48 2015/08/22 18:48 2015/08/22 18:48 2015/08/22 18:48 diffie-hellman-group14 diffie-hellman-group-exchange-sha256 Minimum group exchange prime size: 2048 ٥ Cancel Directory 39 entries (plus 2 hidden entries) Size of File Bytes Transferred % Progress Elapsed Time Time Left Speed Status Einish Time Start Time

2. 新建连接, 输入云堡垒机IP, 端口60022, 账户信息。

3. 单击连接后,按提示输入堡垒机密码。


4. 单击<登录>后进入资产管理界面,请双击选择转码目录(忽略报错信息),再右键选择刷

新,进行转码。



•••				🕵 Se	cureFX					
a 🔍 🚽 🔜 🚽	n 😽 🔁	- 🎕 - 🔒 - 🐻					Enter host	<%R>		
Connect Reconnect Di	sconnect Synchronize Options	Tools Use PGP Secure	eCRT							
S Local (wuyandeMac.loca	0				S 116.62.158	8.231				
/Applications			Filter <3	₩F>	/				Filter <%F>	~
Applications Applications Applications Applications Seventsd Sevent	In Mane	p nnection.app app	Pitter <3		/ In	Trans STATE_EXPECT.NE Inow.gb1800 Inow.gb1800 Inow.gb1800 Inow.gb1800 Inow.gb1800 Ino.gb	· 192.168.51.146-22 SQ.noxLUTF-8 Go To Open Bookmark Add Bookmark Manage Bookmark Manage Bookmark Paste Refresh New Properties Refresh R	¥8 15 16 18 18 18 14 18 19 19 19 19 10 10 11 12 13 14 15 15 16 17 18 18 19 10 10	Filter <%E> Size Type Directory Directory Directory	
39 entries (plus 2 hidden en	tries)				3 entries					6
S	Destination 0'	File Butes Transformed - M Dura	Inned Tires	Tran Time Left	fer Queue	Chart The	Fields Time			
Refresh folder information	Destination Size of	nie sytes iransferred % Prog	ress ::apsed Time	ime Lett Spee	Status	Start Time	⊢inish Time			

5. 转码后资产列表显示正常。

Convect Reconvect Disconvect Synchronize Options Tools Use PGP SecureCit	Sec	Center host < MR>
Local (wuyandemac.local)	Ciltor 2995	
Image: constraint of the second se		Image: Size Type Directory Directory Directory 2 Image:
 net Game Center.app Books.app Books.app Books.app Books.app Game Center.app Books.app Trunes.app Mail.app Secure/RT.app Secure/RT.app 		LSDD : verdor-id reput! REV: [romltple-roots-spoprted reply: 3 SDD : Stat: SDD
39 entries (plus 2 hidden entries)		ResiTest Foile (ResNetWeek): No such file or directory SDD: 15.47 /no.09188/net.UTF SepTest Foile (ResNetWeek): No such file or directory ResTest Foile (ResNetWeek): No such file or directory Generative: 4 406 - 44 - 2017 23:24:00 froetf: 3648(linext8) Gentries Sentries
Elename Destination Size of File Dytes Transferred % Progress	Transf Bapsed Time I Time Left Speed	r Dotud Datus Start Time Pinish Time

 6. 选择目录主机双击进入后,需要先退回到根目录,再右键选择刷新后,进入主机,即可进行运维 操作。



•••		SecureFX	
		Ente	r host <%R>
S Cal (wuyandeMac.local)		S 🚮 116.62.158.231	
/Applications	Filter d	<86F> V	V Filter <%F>
v / g JocumentRevisio b JocumentRevisio b JocumentRevisio b Intravel b Intravel <th>Name App Store.app Automator.app Calculator.app Calculator.app Calculator.app Colentiar.app Dottomsr.app Dottomsr.app Dottomsr.app Dottomsr.app FaceTime.app Font Book.app Game Conter.app Books.app Game Conter.app Mail.app Mail.app Mail.app Mail.app Messages.app Messages.app Messages.app Messages.app QuickTime Player.app Messages.app Messages.app Messages.app Messages.app Messages.app Messages.app Messages.app Stotes.app SecureCatrl.app SecureCatrl.app SecureCatrl.app SecureCatrl.app Stickles.app Stickles.app Stickles.app Stickles.app Stickles.app Messages.</th> <th>v / v / v / v / v / v / v / v / v / v v v selinx solin run v proc proc proc proc file proc<th>Size Type Directory</th></th>	Name App Store.app Automator.app Calculator.app Calculator.app Calculator.app Colentiar.app Dottomsr.app Dottomsr.app Dottomsr.app Dottomsr.app FaceTime.app Font Book.app Game Conter.app Books.app Game Conter.app Mail.app Mail.app Mail.app Mail.app Messages.app Messages.app Messages.app Messages.app QuickTime Player.app Messages.app Messages.app Messages.app Messages.app Messages.app Messages.app Messages.app Stotes.app SecureCatrl.app SecureCatrl.app SecureCatrl.app SecureCatrl.app Stickles.app Stickles.app Stickles.app Stickles.app Stickles.app Messages.	v / v / v / v / v / v / v / v / v / v v v selinx solin run v proc proc proc proc file proc <th>Size Type Directory</th>	Size Type Directory
0	-	Transfer Queue	-
Filename Des	Size of File Bytes Transferred K Progress Tapsed Time	Time Left Speed Status Start Time Finish Tim	e

7. 可正常进行上传下载操作。

•••	戅 Se	ureFX	
		(Enter host <%R>	
Connect Recenter Opened Connect Content C		S 🛃 116.62.158.231	
/Users/wuyan/Desktop	Filter <%F>	/root	▼ Filter <%F> ▼
▼ DocumentRevision freventid Sociality-V100 Vana Sociality-V100 Vana Sociality-V100 Vana Sociality-V100 Vana Sociality-V100 Vana <li< td=""><td></td><td>4996 84-8207 813.129 s.sh (5) </td><td>Size Type D 1053 text 2 Directory</td></li<>		4996 84-8207 813.129 s.sh (5)	Size Type D 1053 text 2 Directory
2 entries (plus 2 hidden entries)		1 entries (plus 10 hidden entries)	6
Destination Disc of File Bytes Transfored % Progress	Trans	er Queue Starts Time Finish Time	
/Users/wuyan/Deskt /root/使用方法.txt 1.1 KB 1.1 KB 100% /root/使用方法.txt /Users/wuyan/Deskt 1.1 KB 1.1 KB 100%	00:00:01 N/A 0.00 KB/s 00:00:03 N/A 0.00 KB/s	Finished 2017/09/04 23:32 2017/09/04 23:32 Finished 2017/09/04 23:32 2017/09/04 23:32	

SSH网关+filezilla直连ECS方式运维

1. 打开命令行终端APP。



2. 输入ssh -T -N -D 127.0.0.1:1080 -oport=60022 用户名@堡垒机IP, 按Enter键。

3. 输入云盾堡垒机密码,按Enter键连接到堡垒机,不要关闭该窗口。

〕 说明:		
如果管理员启用了双因子认证登录,	将会提示输入双因子口令,	请输入您手机上收到的6位数
字。		



说明:

云子账号使用MFA进行二次验证。

4. 打开filezilla客户端,进入设置页面。

关于(A).			FileZilla
设置(S)		1 🔍 象 🛷 🗉 😥 🖻 🙉	
l(⊦ Service	s ▶ 户名(U):	密码(W): 端口(P):	
Hide File Hide Ot Show A	ezilla ೫H hers ℃೫H II		
Quit File	zilla %Q		
站点: /Users	/wuyan/Documents/		✓ 远程站点:
► 🗐 Doc ► 📮 Dor ► 📮 Lib	cuments wnloads rary		
Mo Mu	vies sic		文件名 个
Pic	blic		
Volumes bin			
名 ^	文件大小 文件类型	最近修改	
ileZilla 2.app	日臺	2017/08/14 09	
leZilla 3.app	日录	2017/08/14 09	
leZilla.app	目录	2017/08/14 09	
DC Connec	目录	2017/09/03 22	
S_Store	6,148 文件	2017/10/30 19	
calized	0 文件	2017/08/28 01	
eZilla_3.27	10,349,741 bzip2 compr	2017/08/28 02	
	0 77/7	2017/11/01 04	
tsingleapp	U XIT		

5. 单击通用代理,选择 SOCKS5,设置代理主机: 127.0.0.1,端口: 1080,单击确定。

00	设置
选择页面(P):	通用代理
上注# (10)(P): ● 注接 ● FTP 主动模式 被动模式 FTP 代理服务器 SFTP 通用代理 ● 传输 文件类型 对已存在文件的操作 ▼ 界面 主题 日期/时间格式 文件大小格式 文件網表 语言 ▼ 文件编辑 文件格式关联 更新 日志	代理服务器类型: 无(N) HTTP/1.1 使用 CONNECT 方式 SOCKS 4 SOCKS 5 代理主机(R): 127.0.0.1 代理端口(P): 1080 代理用戶(U): 代理密码(X): 注意:使用代理将强制使用被动模式进行 FTP 连接。

打开站点管理器,输入需要连接运维的服务器IP,设置端口:22;登录类型:正常;输入服务器用户名、密码。



• • •	站点管理器
选择项(S):	常规 高级 传输设置 字符集
▼ ↓ 我的站点 ↓ ECS ↓ 新站点	主机(H): 101.37.15.190 端口(P): 22 协议(T): SFTP - SSH File Transfer Protocol ♀
	登录类型(L): 正常
	密码(W): 注释(M):
新站点(N) 新文件夹(F)	
新建书签(M) 重命名(R)	
	连接(C) 确定(O) 取消

若相关授权组中已添加正确凭据,则无需输入密码。

7. 单击连接, 弹出窗口选择确定。

• •	◎ 未定义的快捷键
\mathbb{Q}	该服务器的主机密匙是未知的。不能保证该服务器就是您所认定的那 台计算机。 ^{详细资料}
	主机: 101.37.15.190:22 指纹: ssh-rsa 2048 1b:b6:9c:34:02:b1:e3:16:0b:ae:45:81:01:f2:ef:47
	信任该主机并继续连接? 总是信任该主机,并将该密钥加入缓存(A)
	取消 确定

•••	ECS - sftp://root@101.37.15.190 - FileZilla			
11 📝 🖻 🗭 🚅 😫 😫 🍇 🖉 🖻 😥 😤 💏				
主机(H): 用户名(U): 密码(W): 端口(P)	: 快速连接(Q) ▼			
状态: 文件传输成功, 传输了 9 字节 (消約1 秒) 状态: 升設下面 (rost)ceshi 状态: 该理Tros*Tis BaPkR, 状态: Listing directory, froat 状态: remote://costeshi => local:/Users/wuyan(Documents/ceshi 状态: 文件传输成功, 传输了 9 字节 (用約1 秒)				0
本地站点: /Users/wuyan/Documents/	✓ 远程站点: /root			×
J Documents Downloads Library	V 22 / V II root			
5 Movies 5 Music	文件名 个	文件大小 文件类型	最近修改 权限	所有者/组
Pictures ▶ Volumes ▶ bin ZYEA 文件大小 文件表型 ■ FileZilla 2.app 日景 ■ FileZilla 3.app 日景 ■ Connec 日景 ■ Josalized 0 文件 1 docalized 0 文件 2017/10/0708/34 01 1 docalized 0 文件 2017/10/1020	.cache .cache .sh .bash_brow .bash_profile .bashrc .cahrc .cahrc .localized .oydistutis.cfg .tcshrc .cshr .sch tcshrc .sth	目录 目录 日录 3,816 文件 176 文件 176 文件 100 文件 64 (07.2午 129 文件 129 文件 12 文件	2017/06/24 drvx 2017/06/24 drvx 2017/09/05 drvx 2009/05/20rw 2009/05/20rw 2009/05/20rw 2004/09/22rw 2015/06/22rw 2017/06/22rw 2017/06/22rw 2017/06/22rw 2017/10/03rw 2017/11/01 2rw	reat root root root
连接了1个文件 大小总址-12 实节	连接了1个文件。大小总共-9 空节			
2014 3 T T ATT 7 VINDO 14 T P	A0+3 11 XIT: 703403.07 P			
sftp://root@101.37.15				
│ /Users/wuyan/Docu>> /root/test 12 正常 2017/ ↓ sftp://root⊛101.37.15	11/02 00时34			
/var/folders/14/jp9yz << /root/ceshi 0 高 2017/	11/02 00时36			
│ /var/folders/14/jp9yz>> /root/ceshi 9 巫 2017/ │ /Users/wuyan/Docu << /root/ceshi 9 正党 2017/	11/02 008336 11/02 008336			
列队的文件 传输失败 成功的传输 (4)			A 100	队列: 空 🔹 🖝

8. 进入远程服务器后,即可进行文件传输运维,堡垒机可正常审计。

3.5 用户修改密码

本文中的修改密码指的是修改堡垒机用户密码,用户指的是通过堡垒机用户页面所创建的用户。本文中的操作步骤无法修改服务器密码与阿里云账号密码。

SSH 协议运维人员修改密码

运维人员请参考SSH协议运维中的操作步骤登录云盾堡垒机后,进行以下操作进行密码修改:

1. 登录云盾堡垒机后,参考菜单界面的说明,输入:passwd命令并按 Enter 键。

Quit: Use "iq-Enters" Move: Use the cursor keys, or " Search: Use '/(patten)-Enters" an Junc: Use ':(nuber)-Enters" to Parsword: Use ':passwd=Enters" to c to the curso of the curson curso. Language: Use 'e" to change language	j" to go down, "k" to g d then "n"/"W" to next/ jump to line {number}. hange your password. e encoding between UTF-	o up. privous searching result. 後朝 8 and 682312.	
NUH NAME IP	PROTO USER	COMMENT	
02: 47.04.00	SSH administrator		
03: 10.007054 116.00.000.000			
84: 10-000000 116.00-000-000	SSH administrator		
05: 01 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	SSH root		
86: 116.	55H administrator		
Type <enter> for login and <q> for qu</q></enter>	it.		
:passwd			

2. 根据提示依次输入当前用户密码、新密码、重复新密码,并按 Enter 键。



3. 云盾堡垒机用户密码修改成功。

RDP 协议运维人员修改密码

运维人员请参考RDP协议运维中的操作步骤登录云盾堡垒机后,进行以下操作进行密码修改:

1. 登录云盾堡垒机后,单击菜单栏下方的修改个人密码。

2. 在弹出的对话框中,依次输入当前用户密码、新密码、重复新密码,单击保存更改。

送明:
 云盾堡垒机密码至少八位,且必须包含以下四项字符:大写字母、写字母、数字、非字母符
 号(如 @, #, \$等)。

3. 云盾堡垒机用户密码修改成功。

3.6 BS运维

BS运维指普通运维用户以RAM子账号身份登录堡垒机控制台并进入Web运维界面,调用本地客户端,单点登录ECS运维。该运维方式仅支持RAM子账号用户使用,可以在Windows环境下使用。

在进行BS运维前,请根据需求设置好RAM子账号权限。您可以使用主账号登录访问控制RAM-用 户管理,给需要运维的RAM子账号授权。建议赋予子账号只读权限,只允许使用运维,避免子账 号进入管理页面,发生越权操作。

	的权限,同一条	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
圣垒机	Q		AliyunYundunBastionHostReadOnl	系統
AliyunYundunBastionHostFullAcc 管理云眉堡垒机(BastionHos	系统	*		
				* 12

RAM子账号登录

参照以下步骤,使用RAM子账号登录运维页面:

1. 通过RAM子账号登录界面,登录云盾堡垒机控制台。

2. 选择要操作的实例,单击运维,进入Web运维界面。

道 说明:		
RAM子账号需要先导入堡垒机,	否则可能无法看到运维按钮,	导入方法参见用户管理。

用户手册 购买堡垒机 ((🌲)) | 堡垒机 云盾 • 堡垒机控制台 实例列表 实例ID 版本授权 区域(全部) 🔻 到期时间 状态(全部) ▼ IP地址 操作 子账号管理 版本:2.1.5 旗舰版 192.168.51.101 (P) 47.96.175.202 (P) 华东 1 2017-12-22 00:00:00 有效 版本:2.1.5 专业版 192, 168,51, 160 (P)) 47,96, 177,90 (P) 2017-12-22 00:00:00 华东 1 host-cs-off-log/log/08 有效

3. 单击下载堡垒机运维助手按钮,下载后进行安装。

📋 说明:	
使用BS运维功能前,	确保堡垒机运维助手启用。

C-) 管理控制台			
云盾 ● 堡垒机	运维		
运维	没有检测到运维助手,请下载堡垒机运维助手并安装。如果您的	已经安装,请确保运维助手已经病	自动。
	输入服务器名称/IP模糊查询 搜索		
	服务器名称	IP地址	登录名
		0 没	有查询到符合条件的记录

- 4. 安装完成后,刷新运维页面,不再提示未检测到堡垒机运维助手。
- 5. 单击运维助手配置,进入运维助手配置界面。
- 6. 分别对所需使用的SSH客户端、RDP客户端、SFTP客户端进行配置。以SFTP为例,步骤如下:

SSH客户端设置 R	DP客户端设置	SFTP客户端设置		
客户端	FileZilla	▼ 1、选择客户端	2、选择客户端安装路径	
应用程序路径	C:\Program Files\FileZilla FTP Client\filezilla.exe 选		选择	
	保存更改	2、保存设置		

BS运维操作

使用RAM子账号登录云盾堡垒机运维页面后,可以看到该账号可以访问的服务器信息。



C-) 管理控制台						wytest
云盾 ● 堡垒机	运维					
运维	输入服务器名称/IP模糊查询	搜索				运维助手配置
	服务器名称		IP地址	登录名	备注	操作
	iZm7sv951ya40kZ	<i>1</i> 4	47.96.173.198	administrator	11	RDP登录
	测试_test_linux	Δ	101.37.15.190	root	22	SSH登录 SFTP登录
						« < 1 > »

・ RDP运维

- 1. 选择需要登录的服务器,单击右侧RDP登录,自动调用mstsc客户端。
- 2. 在弹出界面,单击连接。

🌄 远程桌	瓦连接		×
Û	无法识别此远程连接的	〕发布者。是否仍要连接?	
此远程迫 要连接。	接可能损坏你的本地或	远程计算机。除非你知道此连接	的来源或以前曾使用过此连接,否则请不
	发布者: 类型: 远程计算机:	未知发布者 远程桌面连接	
	旬问我是否连接到此计算	ī机(O)	
€ 显示	é细信息(D)		连接(N) 取消(C)

3. 在弹出界面,单击是,成功登录服务器。

	桌面连接
	无法验证此远程计算机的身份。是否仍要连接?
由于安全 全。	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
名称不	匹酉
1	请求的远程计算机:
	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:
Â	证书上的服务器名错误。
Â	证书来自不信任的证书验证机构。
你想连持	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(V) 是(Y) 否(N)
	明:

MAC环境下RDP客户端不支持自动登入服务器,您在调用RDP客户端后,需要人工选择运 维的服务器,然后双击后连接进入。

・ SSH运维

- 1. 选择需要登录的服务器,单击右侧SSH登录,自动调用所配置的SSH客户端。
- 2. 自动登入服务器,进行运维操作。



・ SFTP运维

- 1. 选择需要登录的服务器,单击右侧SFTP登录,自动调用所配置的SFTP客户端。
- 2. 自动登入服务器,进行运维操作。

🔁【测试_test_linux - 15.190】 - sftp://wytest@:60022 - FileZi — 🛛 🛛 🛛					
文件(F) 编辑(E) 查看(V) 传输(T) 服务器(S) 书签(B) 帮助(H)					
፵੶፪┓┓ҳѸҟѻӷ҂і	Q 🗢 🦚				
主机(H): 用户名(U):	密码(W): 端口(P): 快速连接(Q)				
状态:正在连接 ————————————————————————————————————	^				
状态: Connected to					
状态:读取目录列表	~				
本地站点: ::\Users\wuyan\Pictures\Camera Roll\	/ 远程站点: /root /				
- Camera Roll	· · · · · · · · · · · · · · · · · · ·				
文件名 文件 文件 最近修改	文件名 ^				
<u> </u>	· · ·				
॑॑॑॑॑॑॑॑ deskt 190 配置 2017/6/	.cache				
	.pip				
	ssh				
	openssn-4. Ip I				
	<				
1 个文件。大小总共: 190 字节	19 个文件 和 5 个目录。大小总计: 4,960,652 字节				
服务器/本地 方向 远程文件 大小 优	状态				
列队的文件 传输失败 成功的传输					
	🔒 🕜 队列: 空 👘 🔹				