

运维安全中心(堡垒机) 故障处理





【版权声明】

©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云 事先明确书面许可,任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成 对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的 商标,依法由权利人所有。未经腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复 制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依法采取措施追究法律责 任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则, 腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或 95716。



文档目录

故障处理

Windows 资源登录提示 Connection timed out

Windows 资源登录提示 wait active

Mac 电脑登录 Linux 提示 no matching host key type found

Mac 系统用户无法访问 Windows 资源

Mac 系统使用 iTerm 客户端运维时出现乱码

无法调用本地 Xshell 或 SecureCRT

运维用户无法收到验证码短信

运维人员登录资源无法获取到账号

Linux 资源登录提示主机不可达

Linux 资源登录失败提示密码错误



故障处理 Windows 资源登录提示 Connection timed out

最近更新时间: 2025-03-17 10:15:23

现象描述

Windows 资源访问异常,提示无法连接到远程计算机,如下图所示:

远程桌顶	面连接	×
\times	远程桌面由于以下原因之一无法连接到远程计算机:	
	1) 未启用对服务器的远程访问 2) 远程计算机已关闭 3) 在网络上远程计算机不可用	
	确保打开远程计算机、连接到网络并且启用远程访问。	
	确定 帮助(<u>H</u>)	
Error		
Failed Errror	to connect to: 1 Connection timed out.	
		OK

可能原因

运维安全中心(堡垒机)到资源 CVM 网络或者端口不通,导致运维安全中心(堡垒机)无法代理访问资源。

解决思路

- 1. 如果 运维安全中心(堡垒机)和资源不在同一个 VPC 则无法访问,需要购买多个服务或者打通 VPC 网络。
- 若资源存在安全组限制,则运维安全中心(堡垒机)无法访问目标资源。需要放通资源安全组限制,允许运维安 全中心(堡垒机)访问资源的远程协议端口。

处理步骤

不在同一个 VPC

- 1. 登录 运维安全中心(堡垒机)控制台。
- 2. 在左侧导航栏中,选择开通服务。
- 3. 在开通服务页面,单击购买,购买多个服务。

开通服务 ⑤ 普通区 服务列表 网络域	•								
购买 资源ID/名称	状态↓	(j) qi	剩余授权数	剩余网络域数	带宽	到期时间 🕈	地域	网络信息 访	操作
	已开通			0/0					续费 升级 !
4									۲
 说明: 也可使用和 	私有网络打证	鱼 VPC 网络	络,详情请参	多见 连接其	它 VPC。				

安全组限制

- 1. 登录 运维安全中心(堡垒机)控制台。
- 2. 在左侧导航栏中,选择开通服务。
- 3. 在开通服务页面,查看无法访问目标资源的运维安全中心(堡垒机)的内外网 IP,并记录内网 IP,用于加入到 步骤6 的入站规则中。

资源ID	状态 \$	IP	授权主机数	到期时间 \$	地域	VPC ID/名称	操作
bh-	已开通	4 1 (外) 1 (内)	100	2021-10-07	广州		续费 升级
bh-	已开通	(外)	50	2021-09-17	成都		续费 升级

- 4. 登录 云服务器控制台,单击实例与镜像菜单下的实例。
- 5. 在实例页面,单击需要绑定安全组的 CVM 实例 ID/实例名 > 安全组,进入该实例详情的安全组页面。

ID/名称	监控	状态 ▼	可用区 〒	实例类型 ▼	实例配置	主IPv4地址 (j)	实例计费模式 ▼	网络计赛模式 ▼	所属项目 ▼	操作
					搜索 "实例类型	找到 15 条结果 返回原列表				
in 9	di	🐼 运行中	广州六区	标准型85 🛟	2核 4 系统曲 网络:	》 [] 》[1]	包年包月	按流量计费	默认项目	登录 续费 更多 ▼

6. 在安全组页面,单击编辑规则,进入私有网络的安全组规则的入站规则页面。



を信息 弾性网卡	公网IP 监控 安全组 操作图	日志 执行命令			
 通知: 2019年12月17日 	3后,将增加实例最多绑定安全组数、安全组绑定最多	3 实例数、规则引用数畴限制,详情请)) (1) (1) (1) (1) (1) (1) (1) (1) (1) (
已绑定安全组			排序 绑定	规则预范	
优先级 ①	安全组ID/名称	操作		入站规则 出站规则	
1	S <u>i</u> 须	解绑			编辑规
2	e ž	解绑			
				> 5	编辑规则

7. 在入站规则页面,可增加或修改入站规则,允许运维安全中心(堡垒机)内网 IP 访问资源远程桌面端口。



○ 增加: 单击添加规则, 配置相关参数, 单击完成。

添加入站规则					×
类型	来源 🛈	协议端口 🛈	策略	备注	
自定义	♥ 2010.0.0.1或10.0.0.0/16	如UDP:53,TCP:80,443或TC	允许 ▼		
		+新增一行			
		完成取消			

○ 修改: 单击编辑, 修改来源 IP 和协议端口, 单击保存。

入站规则	出站规则					
添加规则	导入规则	排序 删除 一键放通	教我设置 🖸			<u>+</u>
来源()	т	协议端口 🕄	策略	备注	修改时间	操作
1			允许	▼ 放通内网 (云私有网络)		保存取消

8. 在运维安全中心(堡垒机)的 主机页面,单击编辑,检查资源端口号配置,确认为在使用远程桌面端口,如果不 正确请根据实际情况进行修改。



资产管理 ⑤ 普通区 ▼ 主机资产 数据库资产 W	Veb应用资产 资产组					上次同步时间: 2025-03-13 14:58:10 ④
同步资产	H 常敬产 副除 更多操作 - 土 三					() 通道評單性进行过滤
资产ID/名称	资产IP	网络城 下	托管状态	托管堡垒机 ▼	操作系统 T	操作
ins-Highbor 2.860/06210	NE NE.014 (0) N.235.358-15 (0)	nd my ¹ ddy 16-san dyraff Arlad school denah		10-100-044-087	CentOS 7.9 64f2	编辑 账号 (3) 权限 删除
101 102007101-0140-1 100-100	01.04.5.08	-		未绑定	Windows	编辑》 班·号(1) 和JR 副目的
101-100/78x1-010-1 07/880-rea	10.00.014	net-gkalleti 18-saan-oogillee delaad sehech dorsais		the same angle of	Linux	编辑 账号 (2) 权限 删除



Windows 资源登录提示 wait active

最近更新时间: 2024-11-26 15:34:54

现象描述

Windows 资源访问异常,提示 wait active error,如下图所示:



可能原因

远程桌面授权未激活,用户未加入 Remote Desktop Users 组。

解决思路

激活远程桌面服务,将用户加入 Remote Desktop Users 组。

处理步骤

1. 参考文档 设置允许多用户远程登录 Windows 云服务器 进行配置。

- 2. 在操作系统界面,单击 ², 输入 gpedit.msc ,按 Enter,打开 "本地组策略编辑器"。
- 3. 依次打开运行 > gpedit.msc > 计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制,找到"设置已中断会话的时间限制",启用并将"结束已断开连接的会话"设置为1分钟。

👰 设置已中断会话的时间限制	— D X	<] –	×	
设置已中断会话的时间限制	上一个设置(?) 下一个设置(N)				
○ 未配置(C) 注释: ● 已启用(E)	,	^			
○ 已禁用(D) 支持的平台: Windows Serve	2003 操作系统或 Windows XP Professional 及以上版本	× ^ ×	」时间限制 制		
·	帮助:		钊		
结束已断开连接的会话 1 分钟 🗸	使用此策略设置可以对已断开连接的远程桌面服务会话配置时间限制。 使用此策略设置可指定某个已断开连接的会话在服务器上能保持活动状态 的最长时间。默认情况下,远程桌面服务允许用户从远程桌面服务会话断 开连接,而不用注销和结束会话。	^			
	会话处于断开连接状态时,即使用户不再处于活动连接状态,运行中的程序仍保持活动。默认情况下,这些已断开连接的会话在服务器上可以不受时间限制地保持该状态。 如果它用此等略得等。则达到指完时间后路从服务器中删除已断开连接的				
	如果后用此最相交量,如此当时是他们可用在环心版告诉在不顾尽管,可是我的 会话。若要强制使用默认行为,使已断开会话的保留时间不受限制,请选择"从不"。如果是控制台会话,则已断开会话的时间限制不适用。			>	
	如果禁用或未配置此策略没置,则在"组策略"级别上不指定此策略没置。 "默认情况下,远程桌面服务上断开连接的会话的保留时间不受限制。 注音·"计算机两署"和"田户两署"由新声叶等略沿署 的里同时两署	~			
	确定 取消 应用(<u>A</u>)				

4. 将用户添加到 Remote Desktop Users 组。

🔗 腾讯云



Mac 电脑登录 Linux 提示 no matching host key type found

最近更新时间: 2024-05-30 17:54:31

现象描述

在 MAC 系统上登录 Linux 服务器时,提示"no matching host key type found"的错误。

```
Last login: Tue Oct 10 14:56:44 on ttys007
guanlewang@111deMacBook-Pro ~ % /tmp/connection.sh ; exit;
Unable to negotiate with 111.231.123.235 port 8322: no matching host key type fo
und. Their offer: ssh-rsa
Saving session...
...copying shared history...
...saving history...truncating history files...
...completed.
[进程已完成]]
```

可能原因

从 OpenSSH 8.8起,默认不支持 ssh-rsa。

解决思路

修改 sshd 文件,增加算法。

处理步骤

1. 在本地电脑上执行:

sudo vim /etc/ssh/ssh_config

2. 在 sshd 文件的最后追加一行(注意缩进):

HostKeyAlgorithms +ssh-rsa,ssh-dss



PubkeyAcceptedKeyTypes +ssh-rsa



SendEnv LANG LC_* HostKeyAlgorithms +ssh-rsa,ssh-dss PubkeyAcceptedKeyTypes +ssh-rsa

3. 重新登录 Linux 服务器。



Mac 系统用户无法访问 Windows 资源

最近更新时间: 2024-11-26 15:34:54

现象描述

Mac 系统用户安装完 BHLoader 插件后访问 Windows 资源,提示未找到 Microsoft Remote Desktop,无 法访问资源。如下图所示:



可能原因

Mac 系统未内置 RDP 的远程工具,需要用户自己安装工具并进行设置。

解决思路

在 Mac 系统中安装 RDP 的远程工具。

处理步骤

- 1. 下载并安装: Microsoft Remote Desktop,推荐版本 Version 10.9.8、Version 10.9.9、Version 10.9.10,使用默认安装即可。
- 2. 访问 Windows 资源,根据提示设置工具调取路径。



Favorites	选择客户端工具 Microsoft Remote Desktop 所在位置
Applicati	Contraction of the second s
Downloads	
Desktop	
🗎 OneDrive	
iCloud	
CiCloud Dri	
Desktop	
Documents	Microsoftsktop Beta
Tags	
● 红色	Microsoft Remote Desktop Beta
● 橙色	Application - 156.8 MB
● 黄色	Information 2
● 绿色	Cancel Open
• #A	

- 3. 设置完成后,单击访问,触发拉起 BHLoader 插件。
- 4. 单击确认,调用 MRD 客户端。



5. 单击 continue,完成访问资源调用工具验证,开始资源访问。







Mac 系统使用 iTerm 客户端运维时出现乱

码

最近更新时间: 2024-05-29 17:00:45

现象描述

Mac 系统使用 iTerm 客户端访问 Linux 服务器时,中文出现乱码。如下图所示:

可能原因

Mac 系统内 SSH 配置文件问题。

解决思路

修改 Mac 系统中的 ssh_config 文件。

处理步骤

- 1. 打开 Mac 系统的终端,输入命令: vi /etc/ssh/ssh_config 。
- 2. 将 SendEnv LANG 处的配置修改为 SendEnv LANG LC_* 。



3. 关闭 iTerm 客户端,重新使用运维安全中心(堡垒机)访问目标设备,确认乱码问题是否解决。





无法调用本地 Xshell 或 SecureCRT

最近更新时间: 2024-04-18 09:43:41

现象描述

已经安装了 Xshell/SecureCRT,但是单击访问 Linux 资源时 BHLoader 插件没有拉起对应工具,而是弹出了 如下文件选择框。



可能原因

工具未安装在程序的默认目录C:\Program Files 或者 C:\Program Files (x86),导致 BHLoader 无法直接拉 起工具。

解决思路

重新安装 Xshell 或 SecureCRT,使用默认路径安装,或手动选择工具路径。

处理步骤

- 1. 重新安装 Xshell 或 SecureCRT,安装路径选择默认目录: C:\Program Files 或者 C:\Program Files (x86)。
- 2. 当运维用户第一次使用工具访问资源时,BHLoader 会弹窗提示,提示是否已安装工具,选择"是"。





- 3. 在选择客户端工具弹窗中,选择 Xshell/SecureCRT 的安装目录与应用程序,BHLoader 会把本次选择的结果保存在配置中,后续不用再选择。
 - Xshell 选择程序



○ SecureCRT 选择程序

选择客户端工具SecureC	CRT所在位置	×
← → * ↑	< 工具 → SecureCRT v ひ 2 搜索"SecureCRT"	
组织 ▼ 新建文件	夹 胆 🗸	□ ?
💻 此电脑	へ 修改日期	
🧊 3D 对象	Config 2019/3/13 13:20	
📲 视频	Keymaps 2019/3/13 13:20	
 ■ 图片	log 2020/4/27 10:39	
	Menus 2019/3/13 13:20	
	Scripts 2019/3/13 13:20	选择要预览
	Activator.exe 2015/11/19 8:58	的文件。
」 首乐	LicenseHelper.exe 2017/7/4 14:31	
三 桌面	SecureCRT.exe 2017/7/4 14:31	
🚃 本地磁盘 (C:)	The second secon	
🔜 本地磁盘 (D:)		
L Mat	v < >	
2	之件名(<u>N</u>):	~
	打开(<u>O</u>) ▼	取消



运维用户无法收到验证码短信

最近更新时间: 2024-11-29 17:50:53

现象描述

运维安全中心(堡垒机)运维用户在激活账号、登录运维账号时无法收到短信验证码。

可能原因

- 1. 登录或激活时输入的手机号错误。
- 2. 运维用户不在用户列表中。
- 3. 运维用户在用户列表中,但是运维用户的手机号不正确。
- 4. 手机短信被拦截。

处理步骤

输入号码不正确

检查在登录或激活时输入的手机号是否正确,如不正确,重新输入正确手机号尝试登录。

运维安全中心 堡 垒 机	
请输入手机号	
请输入密码	
登录	
其他登录方式 2 账号密码	
账号激活	

运维用户不在用户列表中

- 1. 登录 运维安全中心(堡垒机)控制台。
- 2. 在左侧导航栏中,选择**用户管理 > 用户**。
- 3. 在用户页面,检查无法收到验证码的运维用户是否在用户列表中,当不在用户列表中,单击新建用户。



同步CAM用户	新建用户	导入用户	导出用户	编辑访问时间限制	編編部门	搜索用	户名,姓名			Q	Ŧ
更多 ▼											Ξ
用户名	姓名	状态 ▼	手机号	认证方式 🔻	邮箱	用户组	部门 ▼	操作			
								编辑 重置	权限 删除		
								编辑 重置	权限 删除		

4. 在新建用户弹窗中,配置相关信息,单击确定保存设置。

基 4 信息	向		
∄户名★	请输入用户名	姓名 *	请输入姓名
人证方式 *	本地	▼ 手机号 *	+86 ▼ 请输入手机号
87年1月 *	请输入邮箱	用户组	请选择用户组

运维用户在用户列表中

1. 在 用户页面,找到无法接收验证码的用户,检查运维用户的手机号是否正确。如不正确,单击该用户的编辑。

新建用	户 导入用户	导出用户	编辑访问时间限	制删除		搜索用户名/姓名			Q	φ
□ 用户	名 姓名	状态 ▼	手机号	认证方式 ▼	邮箱	用户组	操作			
		音 正常	+86 1)	LDAP			编辑 重置	权限 删除		
		正常	+86 1	LDAP	2		编辑 重置	权限 删除		

2. 在编辑用户弹窗中,重新编辑用户正确手机号,单击确定,即可保存新的用户信息。



编辑用户					>
基本信息	高级选项				
用户名			姓名 *	用户	
认证方式 *	LDAP	v	手机号 *	+86 💌 1 5]
由3箱 ★	请输入邮箱		用户组	请选择用户组	
	_				
		确定	取消		

手机短信被拦截

查看手机短信垃圾箱,是否被手机当作垃圾软件误拦截。如果被拦截,请将该号码移出黑名单。

其他情况

以上排查如果无法解决问题,请 提交工单 进行进一步排查。

腾讯云

×

运维人员登录资源无法获取到账号

最近更新时间: 2024-11-29 17:50:53

现象描述

运维人员登录资源时,单击**访问主机**,提示"未被授权该主机的任何账号",无法正常访问资源,如下图:





可能原因

主机资源未录入账号信息或者是创建策略时未给用户绑定账号权限。

解决思路

录入相关账号或配置绑定账号权限。

处理步骤

未录入账号

- 1. 登录 运维安全中心 (堡垒机) 控制台。
- 2. 在左侧导航栏中,选择资产管理 > 主机资产。
- 3. 在主机资产页面,找到对应资产,查看是否录入账号,如果未录入需要录入相关系统的登录账号,单击**账号**。

同步资产 添加资产	托管资产	删除	更多操作 ▼ 📕	=	请选择属性进行过泸	100	Q
资产ID/名称	资产IP	网络域 ▼	托管状态	托管堡垒机 🍸	操作系统 ▼ 部门 ▼	操作	
						编辑 账号 (0) 权限 删除	
						编辑 账号 (0) 权限 删除	



4. 在账号管理弹窗,单击添加资产账号,输入资产账号,单击确定保存。

添加资产则	K号	×
资产账号 *		
	确定取消	

5. 在账号管理弹窗,单击**设置**,设置托管密码和托管私钥,单击确定保存。

已录入账号

1. 在 主机页面,找到对应资产,查看是否录入账号。如果已录入相关系统的登录账号,单击操作列的权限。

同步资产 添加资产	托管资产	删除	多操作 ▼ 👤	Ξ	请选择属性进行过滤		Q, (
资产ID/名称	资产IP	网络域 ▼	托管状态	托管堡垒机 ▼	操作系统 🔻 部门 🍸	操作	
						编辑 账号 (0) 权限 删除	
						编辑 账号 (0) 权限 删除	

2. 在访问权限页面,选择所需用户名,单击**展开**,选择所需权限,单击编辑。

以下用户具备对资产			的访问权限			×
					输入用户名,姓名	Q Ø
用户名	姓名		手机		操作	
•					收起	
权限名称	状态	账号	访问操作	高危命令模	版 操作	
	已生效				编辑	
共 1 条			1	0▼条/页 ᢂ	▲ 1 /1页	► H
•					展开	



3. 在访问权限配置页面,单击**选择账号**,并单击 _____勾选所需账号,单击**下一步:完成 > 确认提交**,保存设置。

🕑 设置权限信息 👌 🕑 选	译用户 〉 💙 选择资产 〉 🚺 选择账号	- > 5 设置访问操作 > 6 选择高	危命令模版 〉	
选择账号		已选择 (2)		
<mark>-</mark> 账号	资产数	影号	资产数	
				0
				0
允许手动填写账号		取消全部选择		





Linux 资源登录提示主机不可达

最近更新时间: 2024-12-11 16:45:44

现象描述

Linux 资源访问异常,提示主机不可达(host is unreachable),连接关闭,如下图所示:

Connection established. To escape to local shell, press Ctrl+Alt+].
WARNING! The remote SSH server rejected X11 forwarding request.
Failed to connect to host(1):host is unreachable
Connection closed.
Disconnected from remote host(bbw@Gitlab-Ops-Server-1(1)) at 11:05:58.
Ture 'help' te leern heu te uee Vehell prempt

可能原因

运维安全中心(堡垒机)到资源 CVM 网络或者端口不通,导致 运维安全中心(堡垒机)无法代理访问资源。

解决思路

- 1. 如果 运维安全中心(堡垒机)和资源不在同一个 VPC 则无法访问,需要购买多个服务或者打通 VPC 网络。
- 若资源存在安全组限制,则运维安全中心(堡垒机)无法访问目标资源。需要放通资源安全组限制,允许运维安 全中心(堡垒机)访问资源的 SSH 端口(默认22)。

处理步骤

不在同一个 VPC

- 1. 登录 运维安全中心(堡垒机)控制台。
- 2. 在左侧导航栏中,选择开通服务。
- 3. 在开通服务页面,单击购买,购买多个服务。

() 说明: 也可使用私有网络打通 VPC 网络,详情请参见 连接其它 VPC。



购买								
资源ID/名称	状态 🕈	IP	剩余授权数	带宽	到期时间 \$	地域	VPC ID/名称	操作
T-Sec-堡垒机(SaaS型)/专业版	已开通	(外) 内) 内)	7/50	16Mbps	2023-11-17	广州		续要│升级│更多 ▼

安全组限制

1. 在 开通服务 页面,查看无法访问目标资源的运维安全中心(堡垒机)的内外网 IP,并记录内网 IP,用于加入 到 步骤5 的入站规则中。

购买								
资源ID/名称	状态 \$	IP	剩余授权数	带宽	到期时间 🕈	地域	VPC ID/名称	操作
T-Sec-堡垒机(SaaS型)/专业版	已开通	外) 内) 内)	7/50	16Mbps	2023-11-17	广州		续费 │ 升级 │ 更多 ▼

- 2. 登录 云服务器控制台,单击实例与镜像菜单下的实例。
- 3. 在实例页面,单击需要绑定安全组的 CVM 实例 ID/实例名 > 安全组 , 进入该实例详情的安全组页面。

D/名称	监控	状态 ▼	可用区 ▼	实例类型 ▼	实例配置	主IPv4地址 🛈	实例计费模式 ▼	网络计费模式 ▼	所属项目 ▼	操作
					搜索 实例类型	找到 15 条结果 返回原列表				
in 9	di	🛞 运行中	广州大区	标准型S5∰	2核 4 系统重 网络:	公) 「」 ?(内)	包年包月	按流量计费	默认项目	登录 续费 更多 ▼

4. 在安全组页面,单击编辑规则,进入私有网络的安全组规则的入站规则页面。

本信息 弹性网卡	公网IP 监控 安全组	操作日志 执行命令			
 通知: 2019年12月 	17日后,将增加实例最多绑定安全组数、安全	组绑定最多实例数、规则引用数等限制,详情诸	毒参考 <u>限制说明</u> 🗹		
已绑定安全组			排序 绑定	规则预览	
优先级 🛈	安全组ID/名称	操作		入站规则 出站规则	
1	St 澳	解绑			編輯规
2	s ž	解绑			(a+8+6)
				× 5	988-882 XVU

5. 在入站规则页面,可增加或修改入站规则,允许运维安全中心(堡垒机)内网 IP 访问资源 SSH 远程端口。





○ 增加: 单击添加规则, 配置相关参数, 单击完成。

添加入站规则								:
类型		来源 🛈		协议端口 🚯	策略	备	注	
自定义	v	IP 地址或 CIDR 段 如 192.168.1.0 或 192.168.	▼ 1.(如UDP:53,TCP:80,443或T	允许	•		
				+新增一行				
				确定取消				

○ 修改: 单击编辑,修改来源 IP 和协议端口,单击保存。

入站规则 出並	占规则					
添加规则	导入规则 (优先级排序 全部编辑	删除一键放通	教我设置 🗹	5个关键字用竖线 "1" 分隔,多个过滤标签用	回车键分隔 Q 上
来源 () ▼	ŧ	协议端口 🕄	策略	备注	修改时间	操作
IP 地址或 CIDI	R段 ▼	ALL	允许 ▼		2023-09-12 14:56:40	保存取消

 在运维安全中心(堡垒机)的 主机资产页面,单击编辑,检查资源端口号配置,确认为在使用远程桌面端口,如 果不正确请根据实际情况进行修改。

主机资产 数据库资产 务 同步资产 添加资产	27产組 托倍数产 創除 更多操作 マ 上	Ξ				请遗拜属性进行过发		Q¢
资产ID/名称	资产IP	网络城 T	托管状态	托管堡垒机 ▼	操作系统 🔻	部门 T	操作	
C State Strengt	11111	-		未期定	Windows Server 2022 發掘中心廠 64位 中文版		编辑 影号 (0) 权限 删除	
In Table	11111 A.			未期定	CentOS 7.9(arm64)		编辑 账号 (0) 权限 删除	
1.1000	111.5	-		未绑定	OpenCloudOS Server 9		编辑 账号 (0) 权限 删除	
 说明: 检查网络中是否还有其他安全产品策略进行了访问限制,如有限制,则需进行放通。 								

Linux 资源登录失败提示密码错误

最近更新时间: 2024-11-29 17:50:53

现象描述

腾讯云

访问 Linux 资源,使用选择远程工具进行登录,提示"invalid password/key",如下图所示:



可能原因

资源账户信息录入错误,或者资源进行了 SSH 登录限制策略。

解决思路

- 1. 检查资源录入的账号密码是否正确,如果有误进行重新录入。
- 确认资源是否设置了只允许通过密钥的方式进行登录,不允许通过密码进行登录,可以在运维安全中心(堡垒 机)设置托管密钥的方式登录,或者在资源系统内取消登录限制。

处理步骤

- 1. 登录 运维安全中心(堡垒机)控制台。
- 2. 在左侧导航栏中,选择资产管理 > 主机资产。
- 3. 在主机资产页面,找到相关资产,单击**账号**。

资产ID/名称	资产IP	地域 ▼	所属堡垒机服务 ▼	操作系统 ▼	操作
	(17)	广州	未绑定	CentOS 8.5 6	编辑 账号 (0) 权限 删除
□ ¥位	2 (95)	广州	未绑定	CentOS 8.0 6	编辑 账号 (0) 权限 删除

4. 在账号管理弹窗,单击密码的设置,重新设置密码。



账号管理		×
添加资产账号 删除	搜索资产账号	Q Ø
资产账号	密码	私钥
	未托管密码 设置	未托管私钥 设置
	已托管密码 设置 清除	已托管私钥 设置 清除

5. 在账号管理弹窗,单击私钥的设置,设置托管私钥。

账号管理		×
添加 资产账号 删除	搜索资产账号	Q Ø
资产账号	密码	私钥
	未托管密码 设置	未托管私钥 设置
	已托管密码 设置 清除	已托管私钥 设置 清除

6. 如若以上设置托管账号密码密钥无误,请检查资源 SSH 配置文件,设置资源允许密码登录:修改

/etc/ssh/sshd_config 配置文件,将 PasswordAuthentication 所在行选项改为 yes。具体情况如下 所示:

- 情况1
 - 故障原因:如果资源设置了不允许 root 账号通过 SSH 登录,将会导致使用 root 用户登录资源失败。
 - 解决方法:在修改 /etc/ssh/sshd_config
 修改对应的值为 yes。
- 情况2
 - 故障原因:如果资源设置了 SSH 白名单,将会导致只允许部分用户登录,此时,需要把对应的账号加 入到白名单中。
 - 解决方法: 在 /etc/ssh/sshd_config 配置文件中,设置 AllowUsers 选项,添加对应的账 号。