

堡垒机 故障处理



腾讯云

【 版权声明 】

©2013–2024 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內容。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 】

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

SaaS 型堡垒机

Windows 资源登录提示 Connection timed out

Windows 资源登录提示 wait active

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

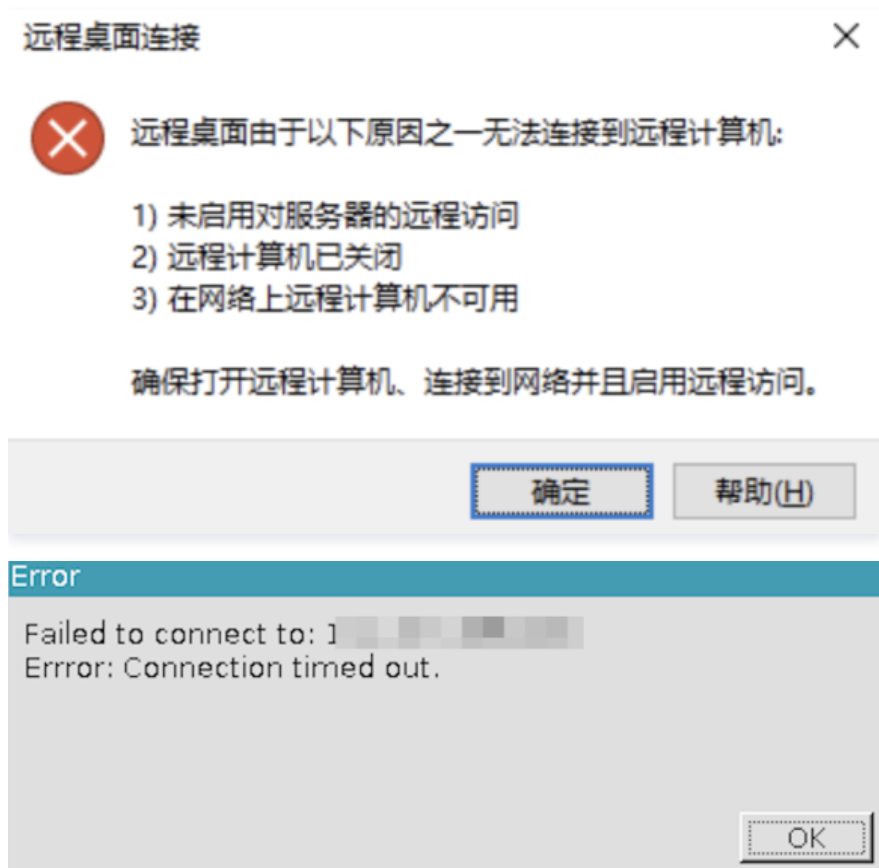
SaaS 型堡垒机

Windows 资源登录提示 Connection timed out

最近更新时间：2024-04-18 09:43:41

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：



可能原因

SaaS 型堡垒机到资源 CVM 网络或者端口不通，导致堡垒机无法代理访问资源。

解决思路

1. 如果 SaaS 型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。
2. 若资源存在安全组限制，则堡垒机无法访问目标资源。需要放通资源安全组限制，允许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 [SaaS 型堡垒机控制台](#)，在左侧导航选择**开通服务**，进入开通服务页面。
2. 在开通服务页面，单击**购买**，购买多个服务。

④ 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](#)。



安全组限制

1. 登录 [SaaS 型堡垒机控制台](#), 在左侧导航选择**开通服务**, 进入开通服务页面。
2. 在开通服务页面, 查看无法访问目标资源的堡垒机的内外网 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) ... (内)	50	2021-09-17	成都	...	续费 升级

3. 登录 [云服务器控制台](#), 单击实例与镜像菜单下的**实例**, 进入实例页面。
4. 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	实例计费模式	网络计费模式	所属项目	操作
ip-0...	...	运行中	广州六区	标准型S5	2核 4系统盘 网络:	... (内)	包年包月	按流量计费	默认项目	登录 续费 更多

5. 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。

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, 详情请参考 [限制说明](#)

已绑定安全组	规则预览																	
<table border="1"> <thead> <tr> <th>优先级</th> <th>安全组ID/名称</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>s-...</td> <td>编辑</td> </tr> <tr> <td>2</td> <td>c-...</td> <td>编辑</td> </tr> </tbody> </table>	优先级	安全组ID/名称	操作	1	s-...	编辑	2	c-...	编辑	<table border="1"> <thead> <tr> <th>入站规则</th> <th>出站规则</th> </tr> </thead> <tbody> <tr> <td> <table border="1"> <tr> <td>...</td> <td>编辑规则</td> </tr> </table> </td> <td> <table border="1"> <tr> <td>s-...</td> <td>编辑规则</td> </tr> </table> </td> </tr> </tbody> </table>	入站规则	出站规则	<table border="1"> <tr> <td>...</td> <td>编辑规则</td> </tr> </table>	...	编辑规则	<table border="1"> <tr> <td>s-...</td> <td>编辑规则</td> </tr> </table>	s-...	编辑规则
优先级	安全组ID/名称	操作																
1	s-...	编辑																
2	c-...	编辑																
入站规则	出站规则																	
<table border="1"> <tr> <td>...</td> <td>编辑规则</td> </tr> </table>	...	编辑规则	<table border="1"> <tr> <td>s-...</td> <td>编辑规则</td> </tr> </table>	s-...	编辑规则													
...	编辑规则																	
s-...	编辑规则																	

6. 在入站规则页面, 可增加或修改入站规则, 允许堡垒机内网 IP 访问资源远程桌面端口。

说明:

- 来源: 根据实际情况, 精确放通 IP。
- 端口协议: 输入远程桌端口。

○ 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 ^①	协议端口 ^①	策略	备注
自定义 ▼	如10.0.0.1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 ^②
↓

<input type="checkbox"/> 来源 ^①	协议端口 ^①	策略	备注	修改时间	操作
<input type="checkbox"/> [redacted]	[redacted]	允许 ▼	放通内网 (云私有网络)	[redacted]	保存 取消

7. 在堡垒机的 **主机页面**，单击**主机信息**，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。

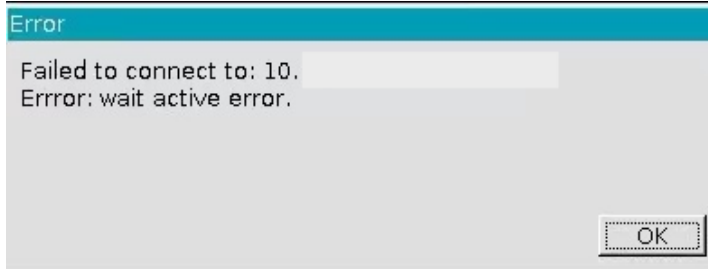
ID/主机名	主机IP	地域	所属堡垒机服务	操作系统	主机账号数	操作
<input type="checkbox"/> ext-Lint	[redacted]	其他	① [redacted]	Linux	1	主机信息 主机账号 访问权限 删除
<input type="checkbox"/> ins-dcl	[redacted] (内)	广州	① bt [redacted]	Windows Server 2016 DataCenter ...	1	主机信息 主机账号 访问权限 删除

Windows 资源登录提示 wait active

最近更新时间：2024-04-18 09:43:41

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

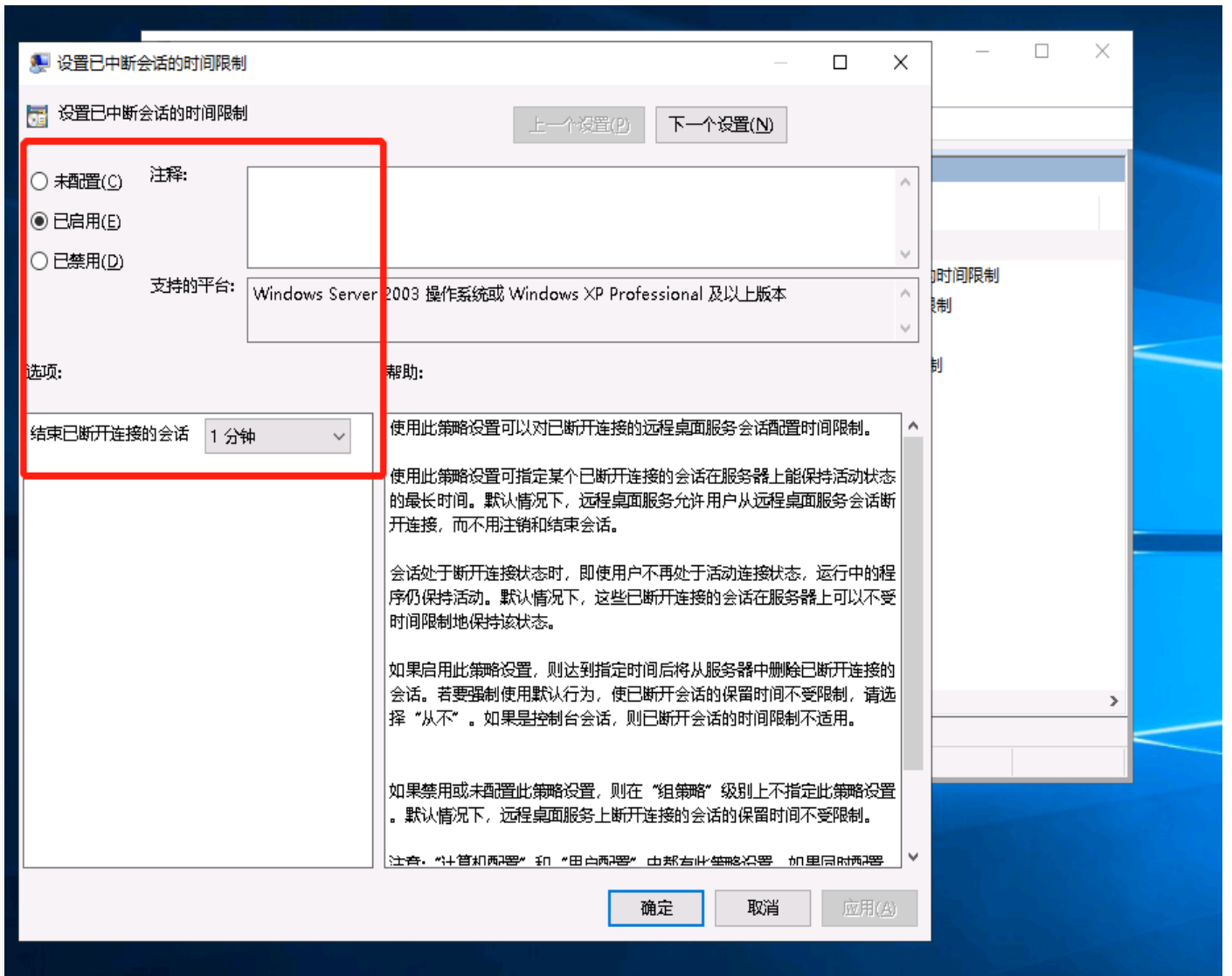
远程桌面授权未激活，用户未加入 Remote Desktop Users 组。

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 ，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。



4. 将用户添加到 Remote Desktop Users 组。

Mac 系统用户无法访问 Windows 资源

最近更新时间：2024-04-18 09:43:41

现象描述

Mac 系统用户安装完 BHLoder 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

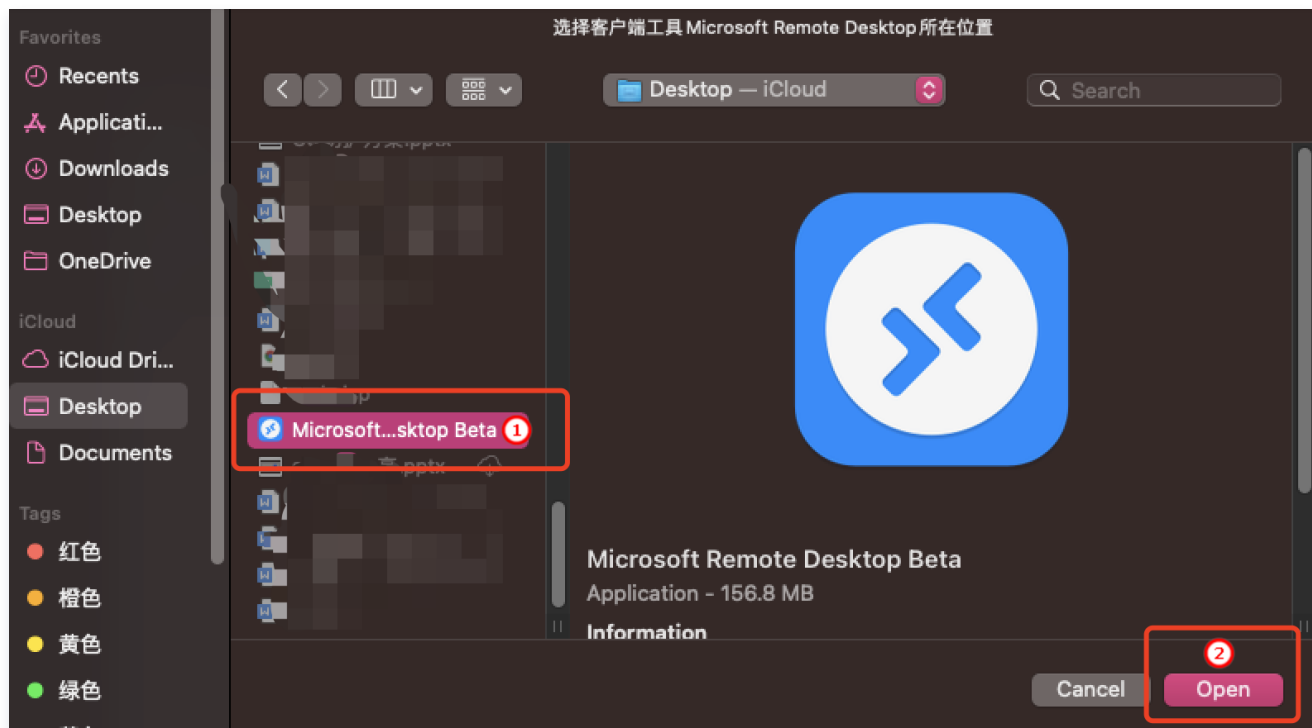
Mac 系统未内置 RDP 的远程工具，需要用户自己安装工具并进行设置。

解决思路

在 Mac 系统中安装 RDP 的远程工具。

处理步骤

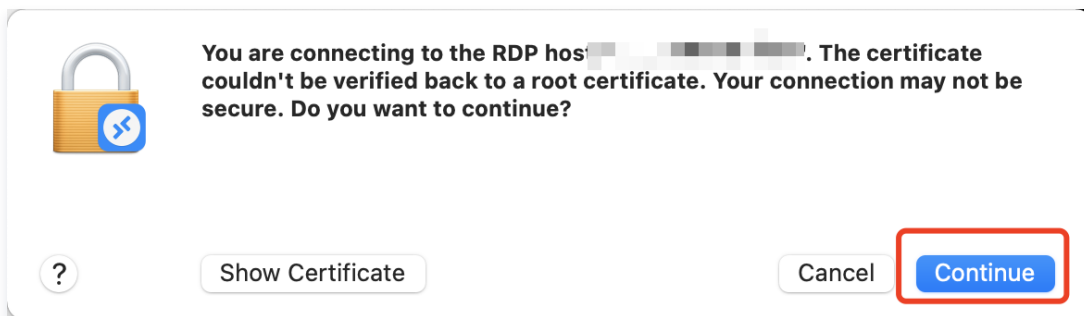
1. 下载并安装：[Microsoft Remote Desktop](#)，推荐版本 10.5.1(1852)，使用默认安装即可。
2. 访问 Windows 资源，根据提示设置工具调取路径。



3. 设置完成后，单击访问，触发拉起 BLoader 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：2024-04-18 09:43:41

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：

```
[root@VM-148-13-centos ansible]#  
[root@VM-148-13-centos ansible]# git status  
# ???? master  
??????,??????  
[root@VM-148-13-centos ansible]#  
[root@VM-148-13-centos ansible]#  
[root@VM-148-13-centos ansible]#
```

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_*`。

```
# Tunnel no  
# TunnelDevice any:any  
# PermitLocalCommand no  
# VisualHostKey no  
# ProxyCommand ssh -q -W %h:%p gateway.example.com  
# RekeyLimit 1G 1h  
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k  
Host *  
SendEnv LANG LC_*
```

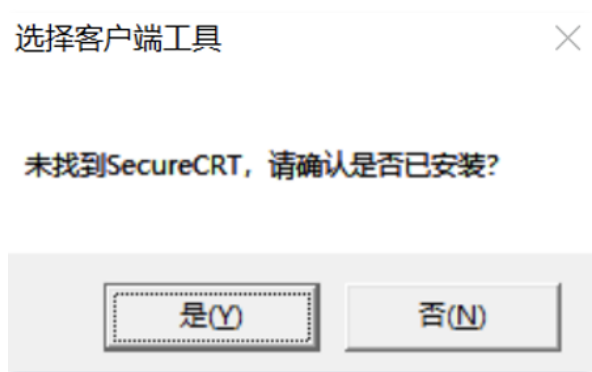
3. 关闭 iTerm 客户端，重新使用堡垒机访问目标设备，确认乱码问题是否解决。

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 BHLoder 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

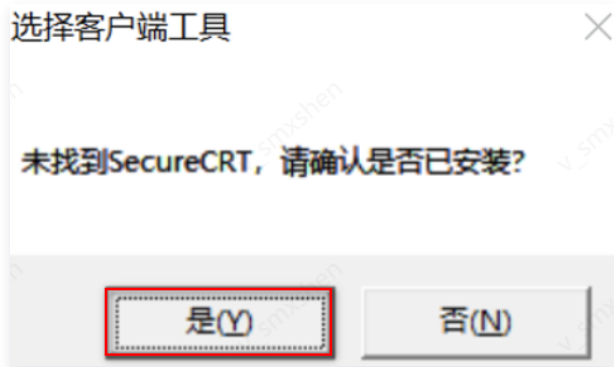
工具未安装在程序的默认目录 C:\Program Files 或者 C:\Program Files (x86)，导致 BHLoder 无法直接拉起工具。

解决思路

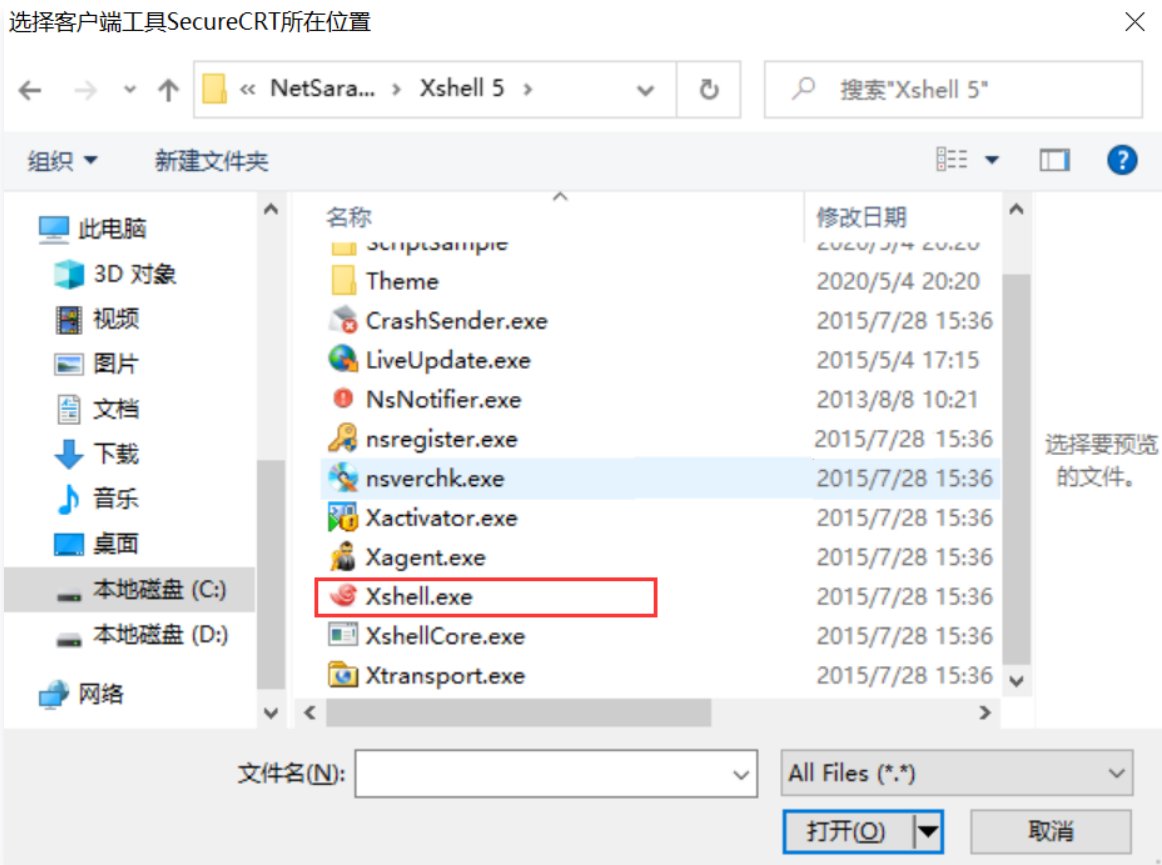
重新安装 Xshell 或 SecureCRT，使用默认路径安装，或手动选择工具路径。

处理步骤

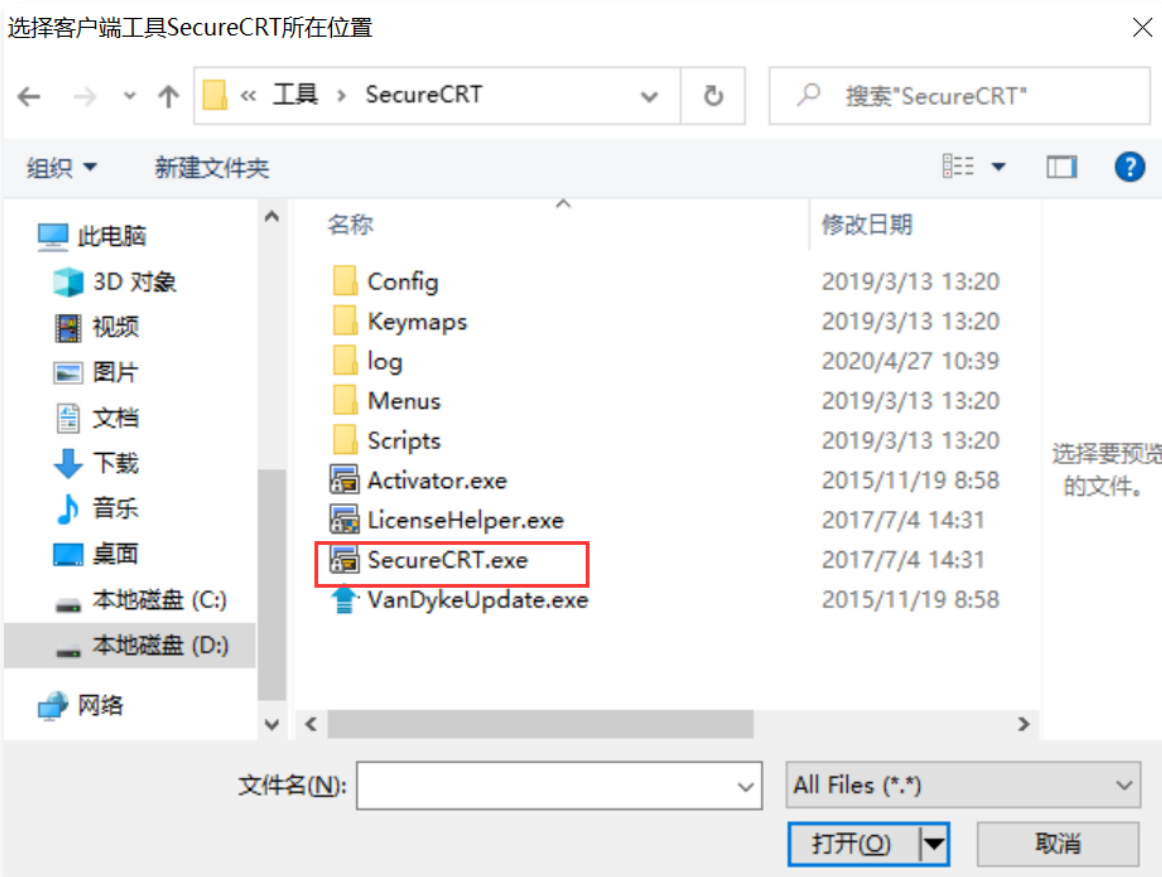
1. 重新安装 Xshell 或 SecureCRT，安装路径选择默认目录：C:\Program Files 或者 C:\Program Files (x86)。
2. 当运维用户第一次使用工具访问资源时，BHLoder 会弹窗提示，提示是否已安装工具，选择“是”。



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，BHLoder 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



运维用户无法收到验证码短信

最近更新时间：2023-10-20 14:46:56

现象描述

SaaS 型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。



运维用户不在用户列表中

1. 登录 [SaaS 型堡垒机控制台](#)，在左侧导航选择[用户管理](#) > [用户](#)，进入用户页面。
2. 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](#)，弹出新建用户弹窗。



<input type="checkbox"/>	用户名	姓名	状态	手机号	认证方式	邮箱	用户组	操作
<input type="checkbox"/>			正常	+86 1...	LDAP			编辑 重置 权限 删除
<input type="checkbox"/>			正常	+86 1...	LDAP	2...		编辑 重置 权限 删除

3. 在新建用户弹窗中，配置相关信息，单击**确定**保存设置。

新建用户
✕

基本信息

高级选项

用户名 *

认证方式 * 本地

邮箱 *

姓名 *

手机号 * +86

用户组 请选择用户组

确定
取消

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**，弹出编辑用户弹窗。

新建用户
导入用户
导出用户
编辑访问时间限制
删除

<input type="checkbox"/>	用户名	姓名	状态 ▼	手机号	认证方式 ▼	邮箱	用户组	操作
<input type="checkbox"/>	█	█	正常	+86 1 █	LDAP			编辑 重置 权限 删除
<input type="checkbox"/>	█		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

认证方式 * LDAP

邮箱 *

姓名 *

手机号 * +86

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。

运维人员登录资源无法获取到账号

最近更新时间：2024-04-18 09:43:41

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 [SaaS 型堡垒机控制台](#)，在左侧导航选择资产管理 > 主机资产。
2. 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，弹出账号管理弹窗。



3. 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。



4. 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**。

ID/资产名	资产IP	地域	所属堡垒机服务	操作系统	账号数	操作
[blurred]	[blurred]	广州	[blurred]	TencentOS Server 2.4	2	编辑 账号 权限 删除
[blurred]	[blurred]	广州	[blurred]	Debian 10.2 64位	1	编辑 账号 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 [blurred] 的访问权限

用户名	姓名	手机	操作
[blurred]	[blurred]	[blurred]	收起

权限名称	状态	账号	访问操作	高危命令模板	操作
[blurred]	已生效	[blurred]	[blurred]	[blurred]	编辑

共 1 条 10 条 / 页 1 / 1 页

[blurred] 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**完成** > **确认提交**，保存设置。

设置权限信息 > 选择用户 > 选择资产 > **4 选择账号** > 5 设置访问操作 > 6 选择高危命令模板 > **7 完成**

选择账号

账号	资产数
<input checked="" type="checkbox"/>	[blurred]
<input checked="" type="checkbox"/>	[blurred]
<input type="checkbox"/>	[blurred]
<input type="checkbox"/>	[blurred]
<input type="checkbox"/>	[blurred]

已选择 (2)

账号	资产数
[blurred]	[blurred]
[blurred]	[blurred]

取消全部选择

Linux 资源登录提示主机不可达

最近更新时间：2024-04-18 09:43:41

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：

```
Connecting to 10.10.10.10:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

WARNING! The remote SSH server rejected X11 forwarding request.

Failed to connect to host(10.10.10.10): host is unreachable

Connection closed.

Disconnected from remote host(bbw@Gitlab-Ops-Server-1(10.10.10.10)) at 11:05:58.

Type `help` to learn how to use Yeshell prompt.
```

可能原因

SaaS 型堡垒机到资源 CVM 网络或者端口不通，导致 SaaS 型堡垒机无法代理访问资源。

解决思路

1. 如果 SaaS 型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。
2. 若资源存在安全组限制，则堡垒机无法访问目标资源。需要放通资源安全组限制，允许堡垒机访问资源的 SSH 端口（默认22）。

处理步骤

不在同一个 VPC

1. 登录 [SaaS 型堡垒机控制台](#)，在左侧导航选择**开通服务**，进开通服务页面。
2. 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	10.10.10.10 (外) 10.10.10.10 (内)	7/50	16Mbps	2023-11-17	广州		续费 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	[Red Box]	7/50	16Mbps	2023-11-17	广州	[Redacted]	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**，进入实例页面。
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。

ID/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
[Red Box]		运行中	广州六区	标准型S5	2核 4G 系统盘 网络:	[Redacted]	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进站规则页面。

基本信息 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, 详情请参考 [限制说明](#)

优先级	安全组ID/名称	操作
1	[Redacted]	解绑
2	[Redacted]	解绑

规则预览

进站规则 出站规则

[Red Box] 编辑规则

[Redacted] 编辑规则

5. 在进站规则页面，可增加或修改进站规则，允许堡垒机内网 IP 访问资源 SSH 远程端口。

说明:

- 来源: 根据实际情况，精确放通 IP。
- 端口协议: 输入远程桌端口。

- 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	IP 地址或 CIDR 段 如 192.168.1.0 或 192.168.1.1	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
出站规则

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

来源
协议端口
策略
备注
修改时间
操作

IP 地址或 CIDR 段

ALL

允许

2023-09-12 14:56:40

保存
取消

6. 在堡垒机的 [主机页面](#)，单击[主机信息](#)，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。

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。

ID/主机名	主机IP	地域	所属堡垒机服务	操作系统	主机账号数	操作
ext-Lin		其他		Linux	1	主机信息 主机账号 访问权限 删除
ins-dcl	(内)	广州		Windows Server 2016 DataCenter ...	1	主机信息 主机账号 访问权限 删除

Linux 资源登录失败提示密码错误

最近更新时间：2023-10-20 14:46:56

现象描述

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：

```
WARNING! The remote SSH server rejected X11 forwarding request.
Failed to connect to host(1[REDACTED]):invalid password/key
Connection closed.
Disconnected from remote host(bbw@BBW-0ps-3(1[REDACTED])) at 11:05:26.
```

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。
2. 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 [SaaS 型堡垒机控制台](#)，在左侧导航选择**资产管理 > 主机资产**，进入主机资产页面。
2. 在主机资产页面，找到相关资产，单击**账号**，弹出账号管理弹窗。

<input type="checkbox"/>	资产ID/名称	资产IP	地域	所属堡垒机服务	操作系统	操作
<input type="checkbox"/>	[REDACTED] 位	[REDACTED] (外)	广州	未绑定	CentOS 8.5 6...	编辑 账号 (0) 权限 删除
<input type="checkbox"/>	[REDACTED] 4位	[REDACTED] 2 (外)	广州	未绑定	CentOS 8.0 6...	编辑 账号 (0) 权限 删除

3. 在账号管理弹窗，单击密码的**设置**，重新设置密码。



4. 在账号管理弹窗，单击私钥的设置，设置托管私钥。



5. 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` 配置文件中，找到 `PermitRootLogin` 所在行，并修改对应的值为 `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。