堡垒机

故障处理

腾讯云

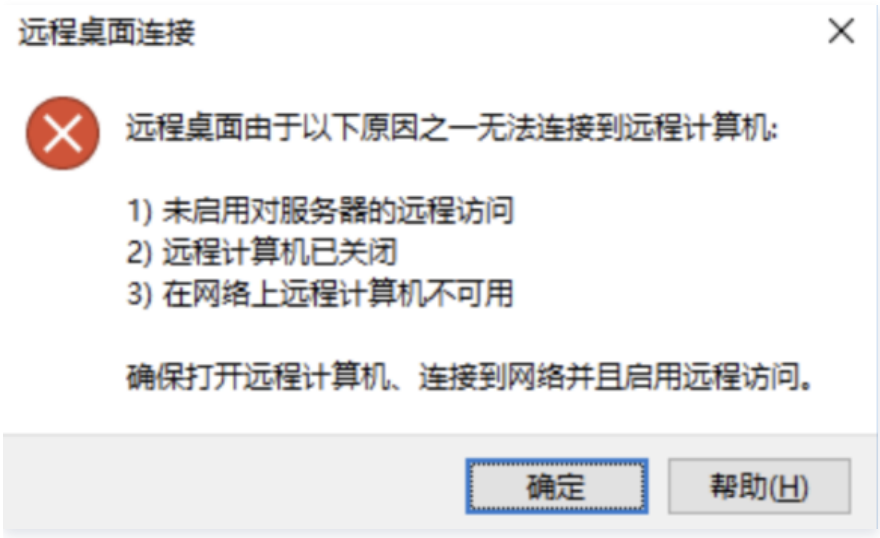
文档目录

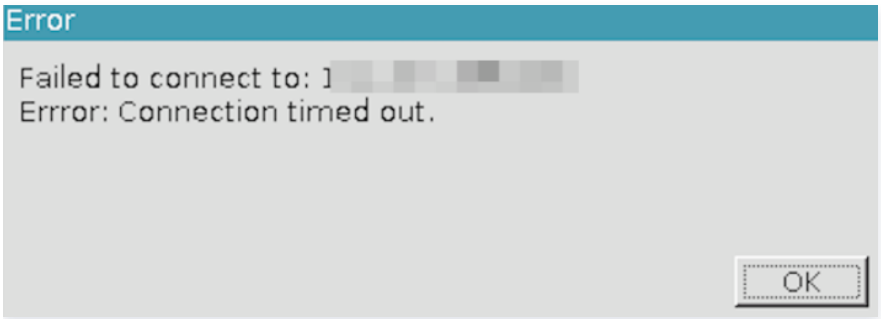
故障处理
SaaS 型堡垒机
Windows 资源登录提示 Connection timed out

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。

> **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。

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。

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。

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**。

- 修改：单击**编辑**，修改来源 IP 和协议端口，单击**保存**。

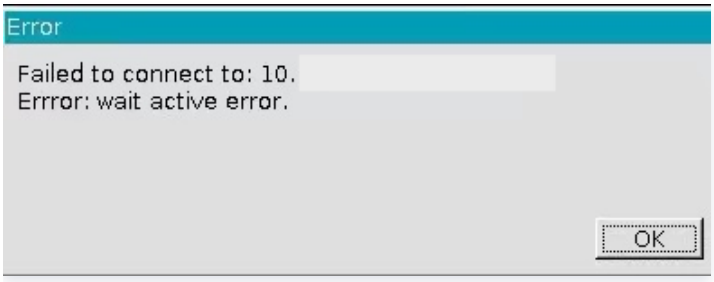
7. 在堡垒机的 主机页面，单击**主机信息**，检查资源端口号配置，确认为在使用远程桌面端口，如果不正确请根据实际情况进行修改。

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

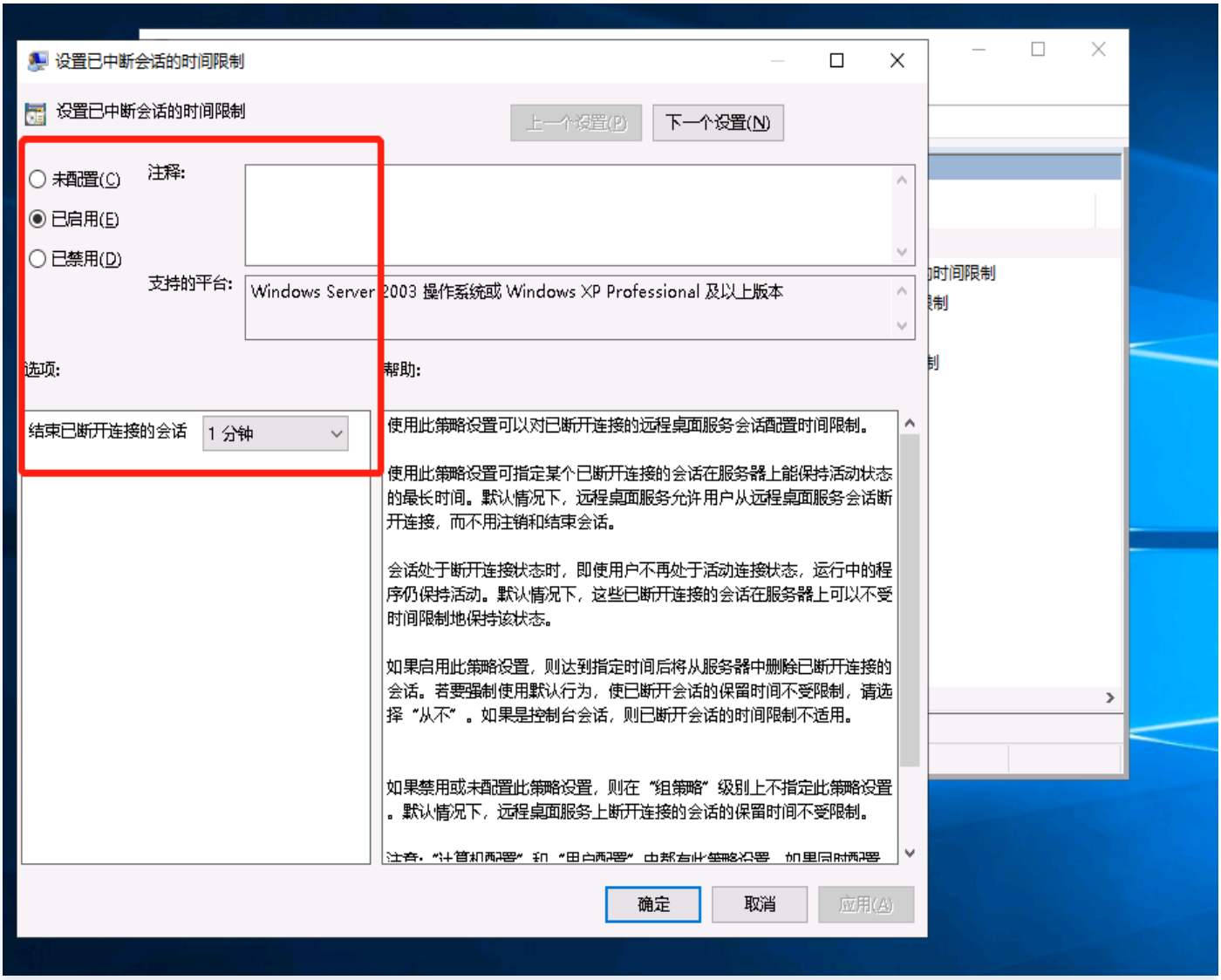
远程桌面授权未激活，用户未加入 Remote Desktop Users 组。

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 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

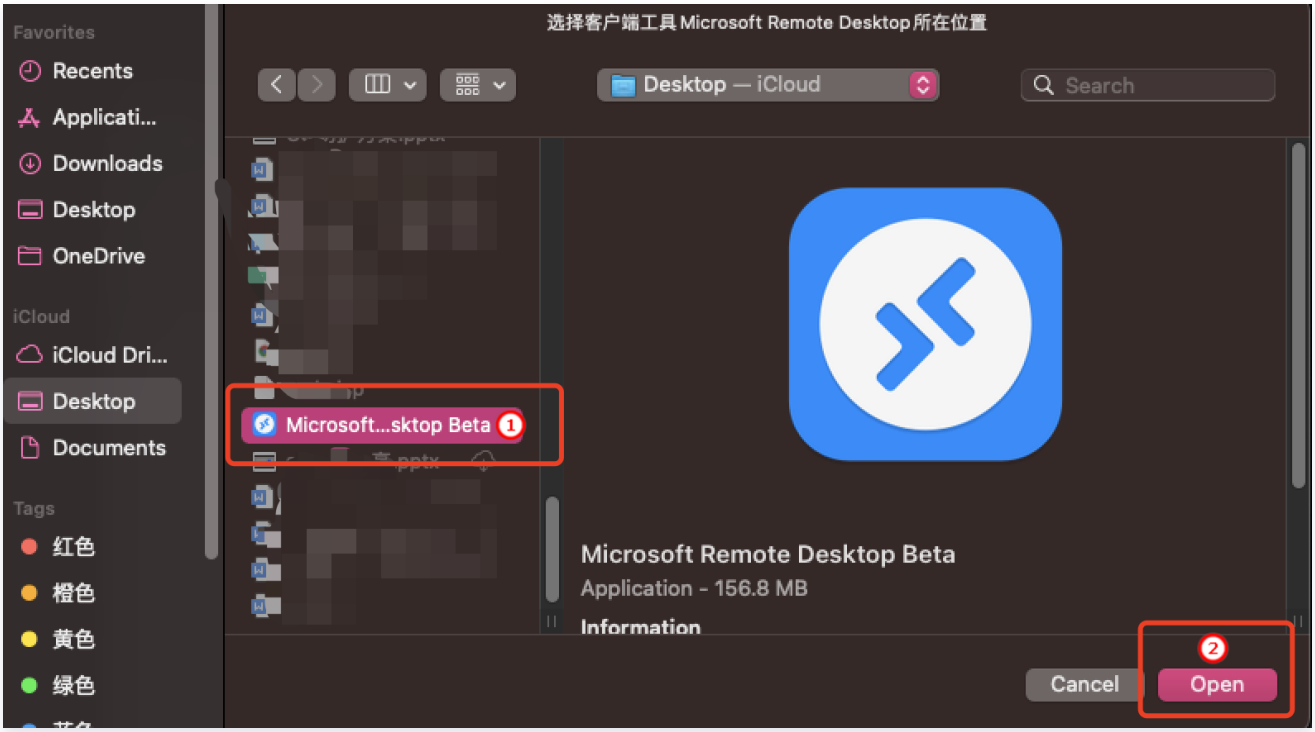
Mac 系统未内置 RDP 的远程工具，需要用户自己安装工具并进行设置。

解决思路

在 Mac 系统中安装 RDP 的远程工具。

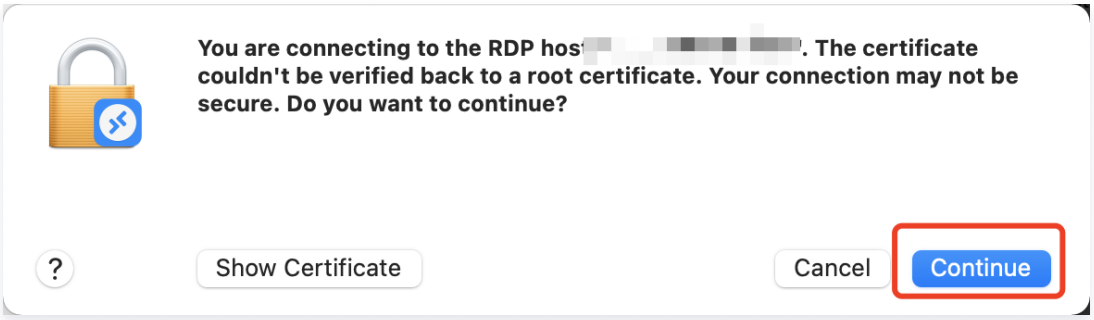
处理步骤

1. 下载并安装：Microsoft Remote Desktop，推荐版本 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 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。

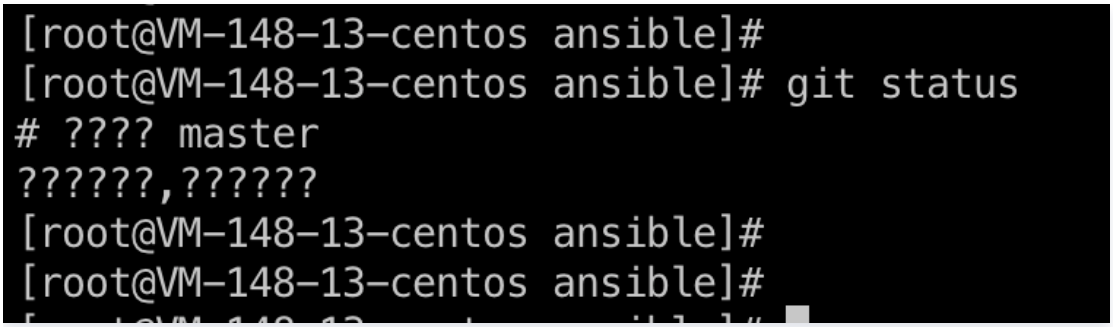


Mac 系统使用 iTerm 客户端运维时出现乱码

最近更新时间：2024-04-18 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：



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_*
```

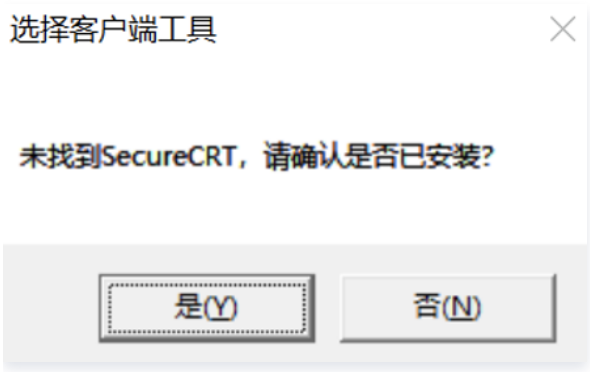
3. 关闭 iTerm 客户端，重新使用堡垒机访问目标设备，确认乱码问题是否解决。

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 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

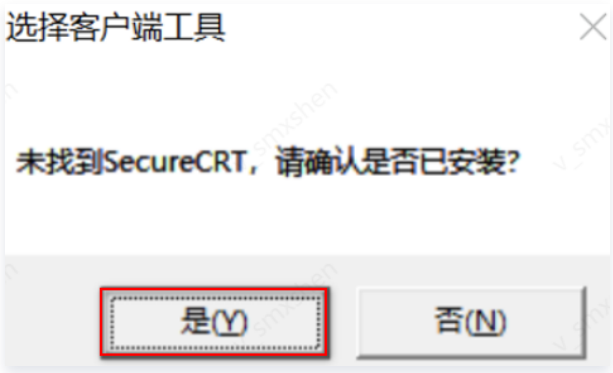
工具未安装在程序的默认目录C:\Program Files 或者 C:\Program Files (x86)，导致 BHLoader 无法直接拉起工具。

解决思路

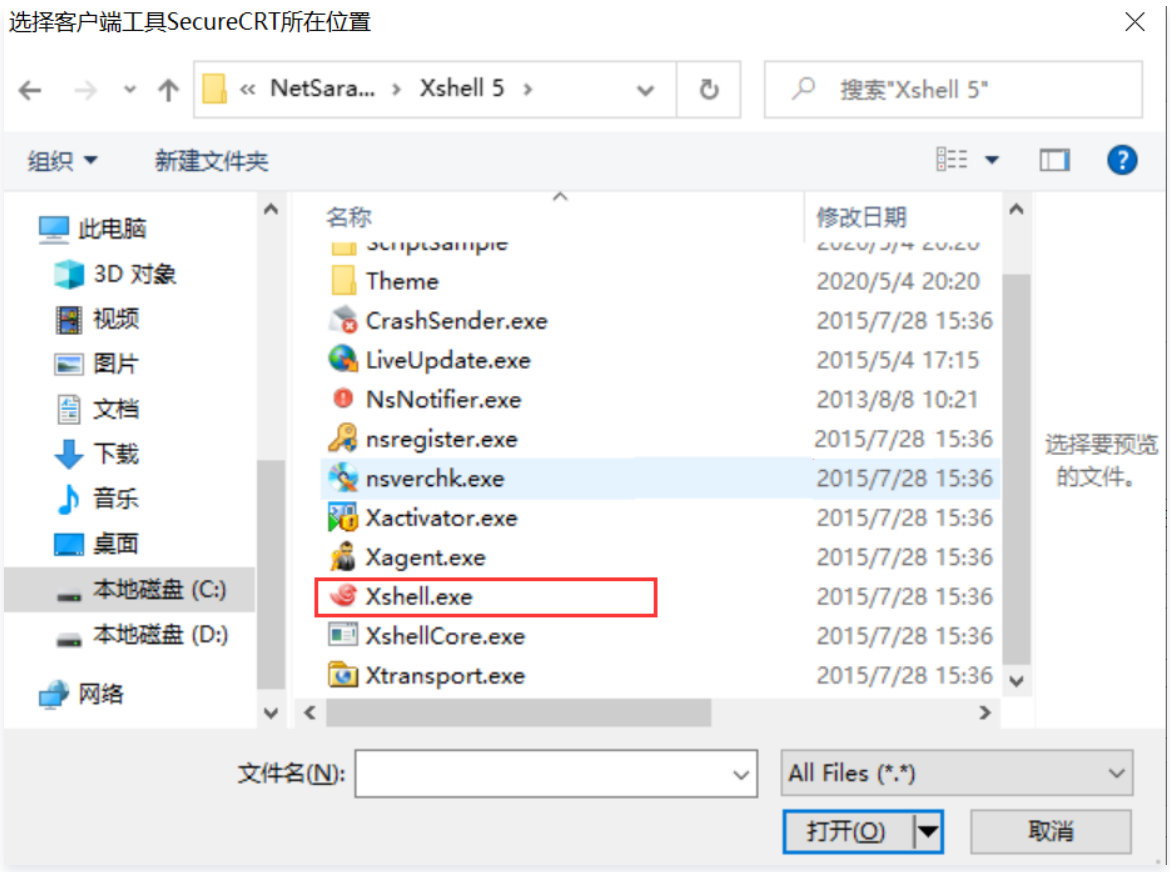
重新安装 Xshell 或 SecureCRT，使用默认路径安装，或手动选择工具路径。

处理步骤

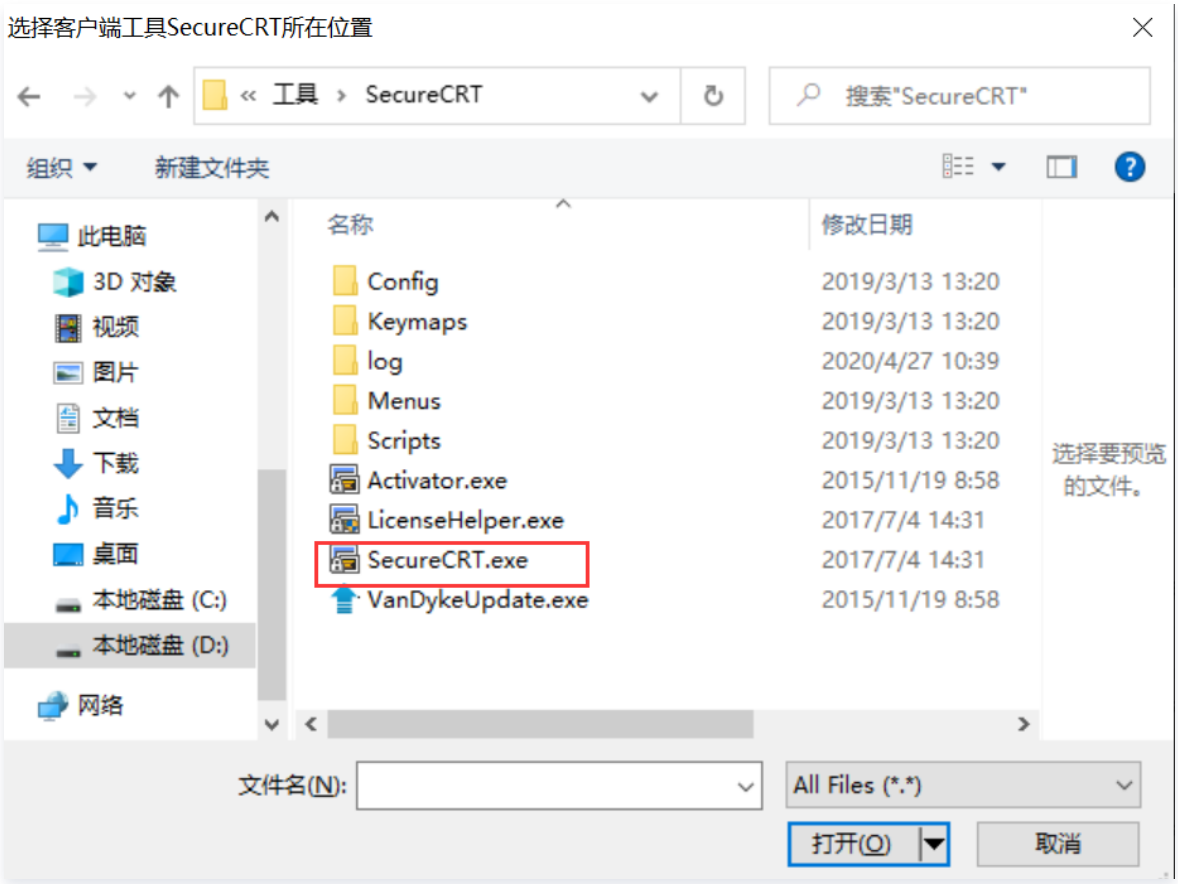
1. 重新安装 Xshell 或 SecureCRT，安装路径选择默认目录：C:\Program Files 或者 C:\Program Files (x86)。
2. 当运维用户第一次使用工具访问资源时，BHLoader 会弹窗提示，提示是否已安装工具，选择“是”。



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



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。

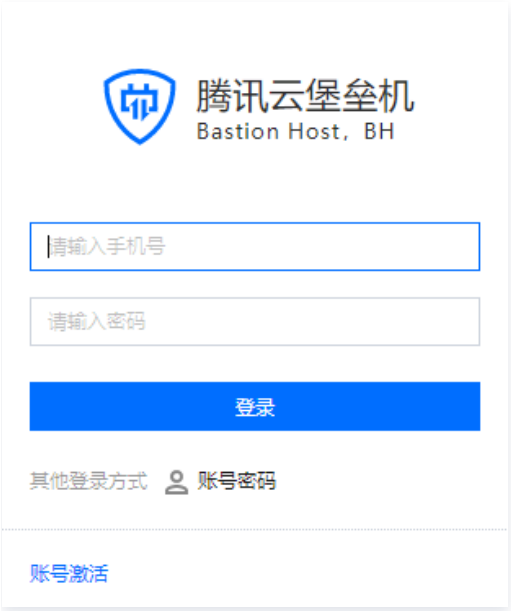
可能原因

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

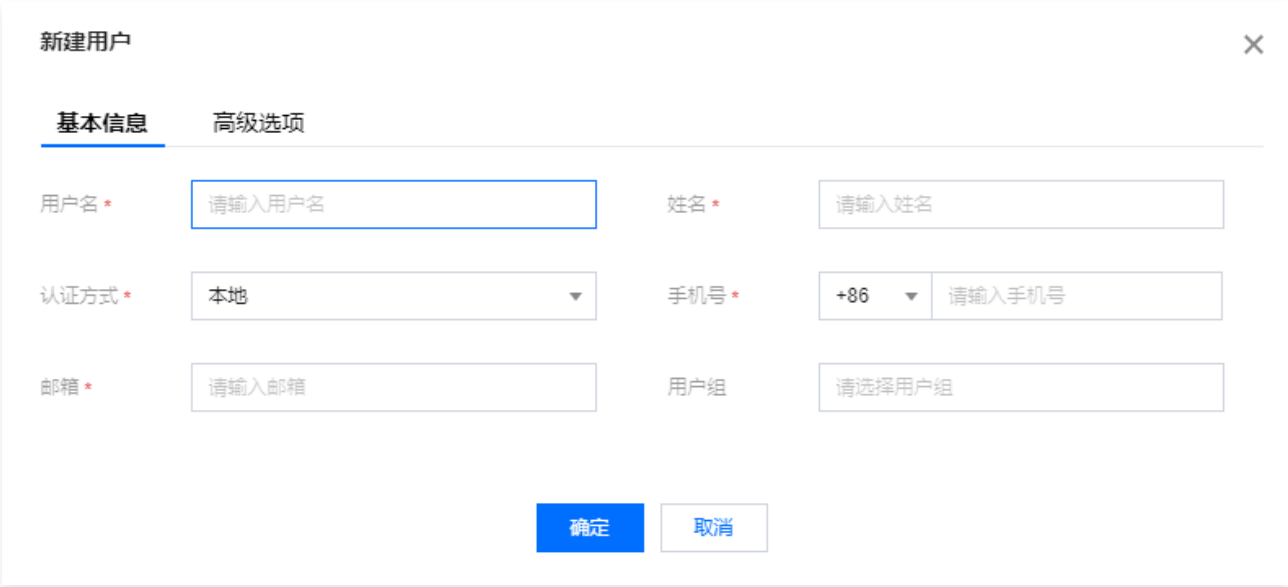
检查在登录或激活时输入的手机号是否正确，如不正确，重新输入正确手机号尝试登录。



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。

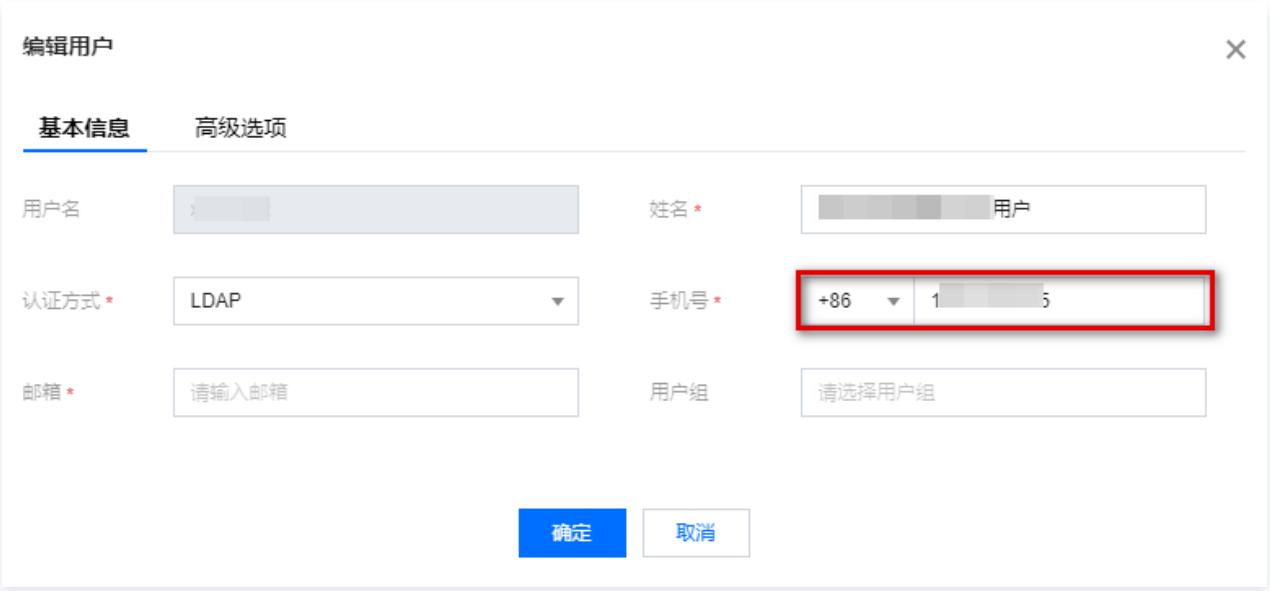
3. 在新建用户弹窗中，配置相关信息，单击**确定**保存设置。



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。

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。



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。

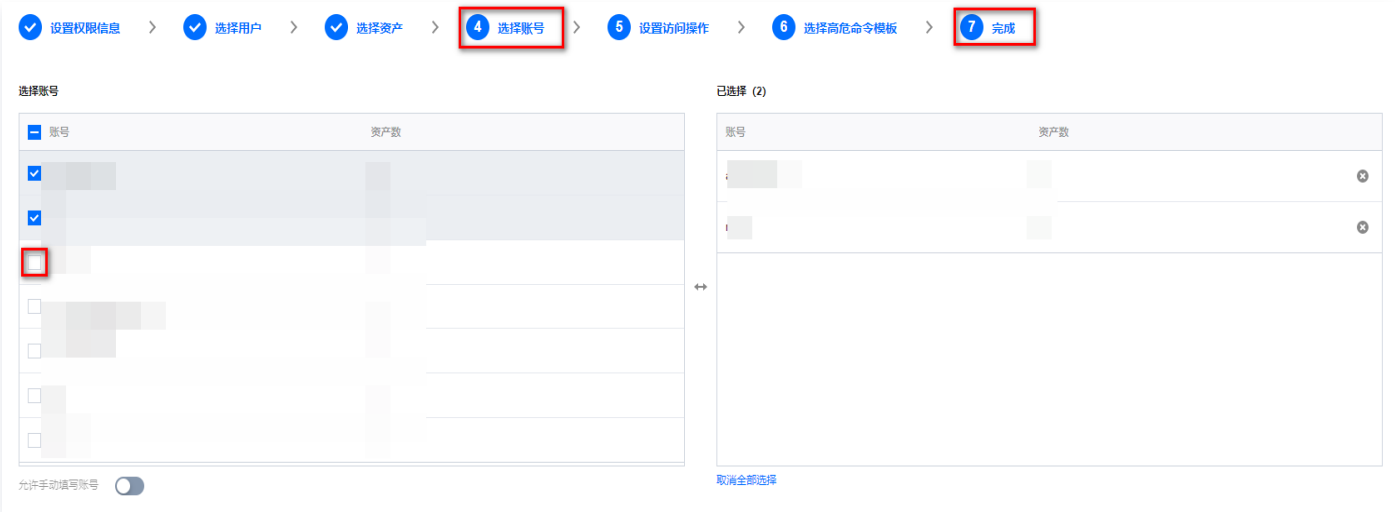
4. 在账号管理弹窗，单击**设置**，设置托管密码和托管私钥，单击**确定**保存。

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**。

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**。

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。

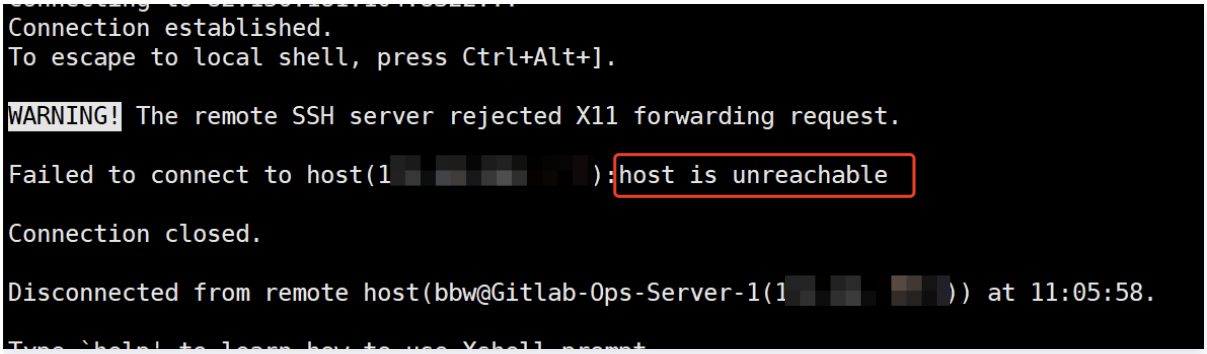


Linux 资源登录提示主机不可达

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：



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 。

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。

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。

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。

5. 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 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**。

- 修改：单击**编辑**，修改来源 IP 和协议端口，单击**保存**。

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。

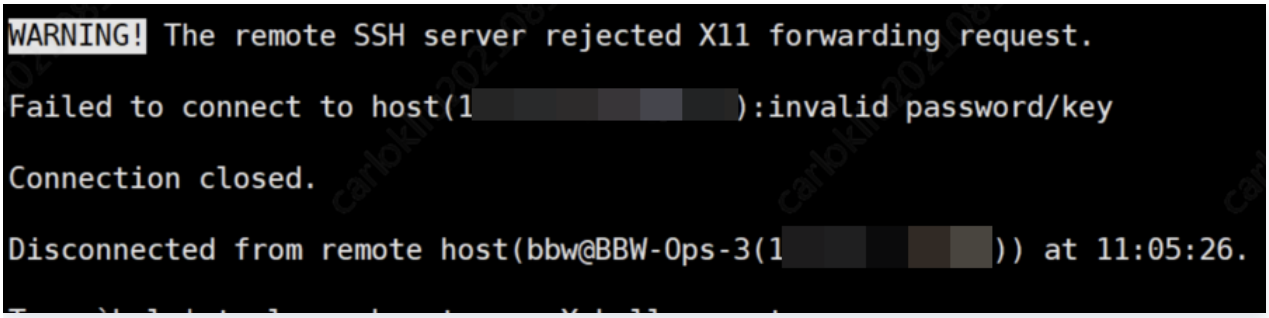
> **说明：**
> 检查网络中是否还有其他安全产品策略进行了访问限制，如有限制，则需进行放通。

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：



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。

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。