

思福迪
运维安全管理系统
使用指南
(运维人员)

杭州思福迪信息技术有限公司

目 录

1. 概述	3
2. 环境确认	4
2.1使用环境.....	4
2.2运维账号.....	6
3. Web运维配置	7
4. 运维操作	8
4 B/S方式运维（推荐使用）	8
4 SSH协议运维	9
4 RDP协议运维	10
4 SFTP协议运维	12
4.2C/S方式运维.....	14
2 MacOS操作系统	14
2 Windows操作系统	23

1. 概述

思福迪堡垒机为云服务器的运维提供完整的审计回放和权限控制服务。思福迪堡垒机基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的AAAA统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

思福迪堡垒机符合各类法令法规的要求，包括等级保护、银监会、证监会、PCI安全标准委员会、企业内控管理等相关政策规定要求。

思福迪堡垒机支持B/S及C/S运维方式，B/S运维方式通常适用于windows操作系统的客户端，运维人员可通过浏览器直接访问运维的服务器；C/S运维方式通常适用于Macos操作系统的客户端，（用户也可以根据使用习惯用于Windows操作系统的客户端），运维人员采用客户端方式运维SSH协议时可以使用Xshell、FlashFXP、Putty等工具，RDP工具可直接使用windows自带的RDP服务。

本指南主要针对运维人员使用云平台内的统一运维管理系统进行指导说明。

2. 环境确认

2.1 使用环境

B/S使用环境：

浏览器要求：建议采用Firefox、Chrome浏览器。

插件及软件安装：Windows办公环境下的运维人员使用思福迪堡垒机之前**必须要安装**（BHostClient插件）

SSH软件：用户可根据使用习惯选择Putty、SecureCRT、Xshell中的任意一个进行安装。

插件下载及安装操作步骤：

1. 打开Firefox或者Chrome浏览器。
2. 在地址栏中，输入https://思福迪堡垒机的访问地址，按回车键（Enter），进入系统登录页面。
3. 在思福迪堡垒机登录页面，输入运维账号的用户名、密码。
4. 单击登录。
5. 点击左侧的“访问工具”菜单，选择“相关下载”，如下图所示：



6. 在相关下载页面，点击BHostClient，下装BhostClient插件并安装，安装完成后会在桌面显示“BhostAlive”快捷方式，如下图所示：



相关下载工具说明：

运维工具	说明
BHostClient	BHostClient是通过 Web方式 调用客户端运维工具时， 必须安装 的登录工具。【运维用户安装这个工具】
BHostReplay	用于在线或离线播放运维审计视频的插件【管理员角色安装这个工具】。
密码查看器	用于查看密码的工具。【密码管理员安装这个工具】

说明：运维客户端必须安装BHostClient插件，否则无法正常运维。

7. 在“相关下载”页面的“全局设定”选项中, 运维人员可以指定运维工具的安装位置，如putty、xshell、PLSql等, 如下图所示：

Netterm(TELNET):	全局 ▾	浏览	SqlAdvantage(SYBASE):	全局 ▾	浏览
isqlw(SYBASE):	全局 ▾	浏览	Putty(SSHCNSOLE):	全局 ▾	浏览
SecureCRT(SSHCNSOLE):	全局 ▾	浏览	XShell(SSHCNSOLE):	全局 ▾	浏览
PLSql(ORACLE):	全局 ▾	浏览	PowerBuilder(ORACLE):	全局 ▾	浏览
SqlPlus(ORACLE):	全局 ▾	浏览	SqlPlusW(ORACLE):	全局 ▾	浏览
Toad(ORACLE):	全局 ▾	浏览	sqldr(ORACLE):	全局 ▾	浏览
MySql(MYSQL):	全局 ▾	浏览	FlashFXP(FTP/SFTP):	全局 ▾	浏览
LeapFtp2.0(FTP):	全局 ▾	浏览	LeapFtp3.0(FTP):	全局 ▾	浏览
WinSCP(FTP/SFTP):	全局 ▾	浏览	filezilla(FTP/SFTP):	全局 ▾	浏览
DB2Cmd(DB2):	全局 ▾	浏览			

保存

C/S使用环境：

软件：命令终端模式、SSH客户端软件。

2.2 运维账号

在使用思福迪堡垒机之前，请确认你已经找思福迪堡垒机的系统管理员申请了**运维账号**和需要**运维的资源**。

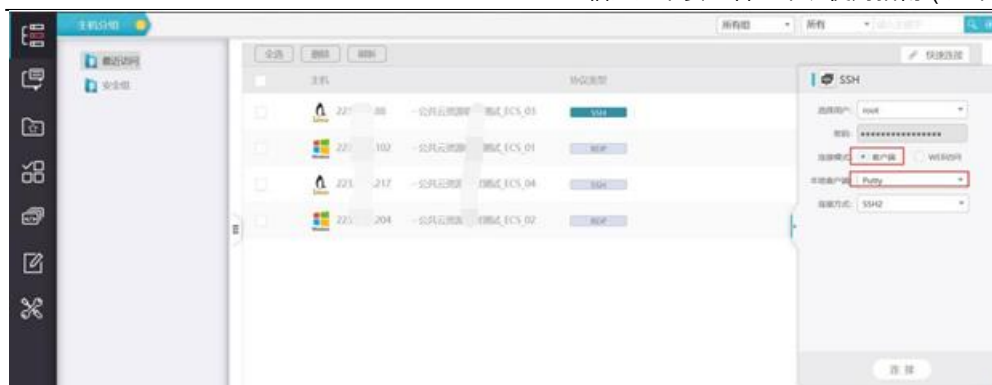
运维人员第一次**登陆统一运维管理系统**时，系统会强制用户修改默认密码。

3. Web运维配置

在确认使用环境已准备好后，需要使用运维账号登陆思福迪堡垒机，对运维工具进行配置。

操作步骤：

1. 打开Chrome浏览器。
2. 在地址栏中，输入https://思福迪堡垒机的访问地址，按回车键（Enter），进入系统登录页面。
3. 输入运维账号、密码、验证码，登录思福迪堡垒机。
4. 点击左侧“分组管理”，协议类型SSH，【RDP协议类型无须配置】在弹出的快捷菜单中选择本地客户端(Putty、SecureCRT、Xshell)等，点击“连接”按钮，在弹出的“客户端路径”对话框中指定默认的SSH连接工具的安装路径，如下图所示：



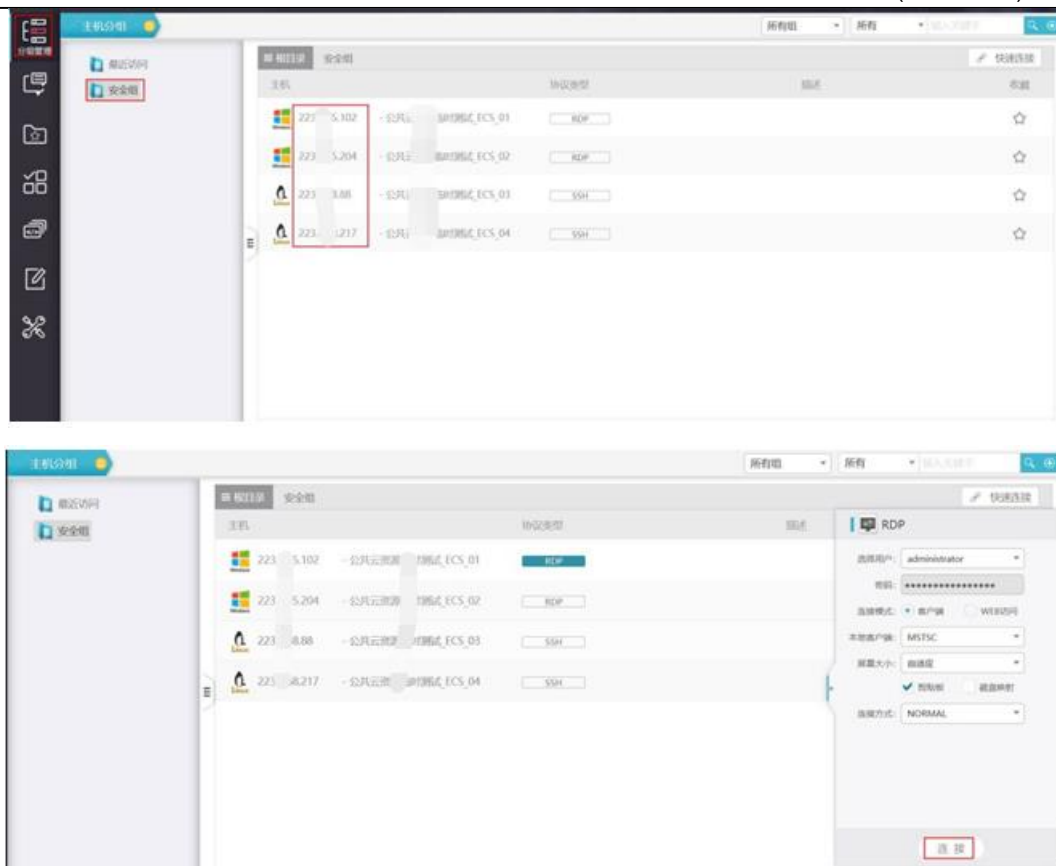
5. 其它运维工具的配置可参照步骤4，最后点击“保存”按钮。

4. 运维操作

4.1 B/S方式运维（推荐使用）

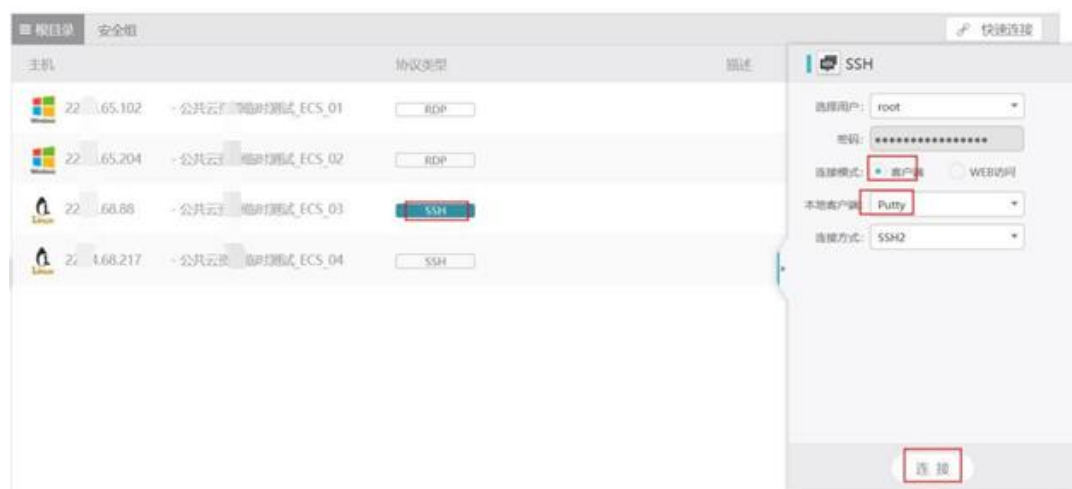
操作步骤：

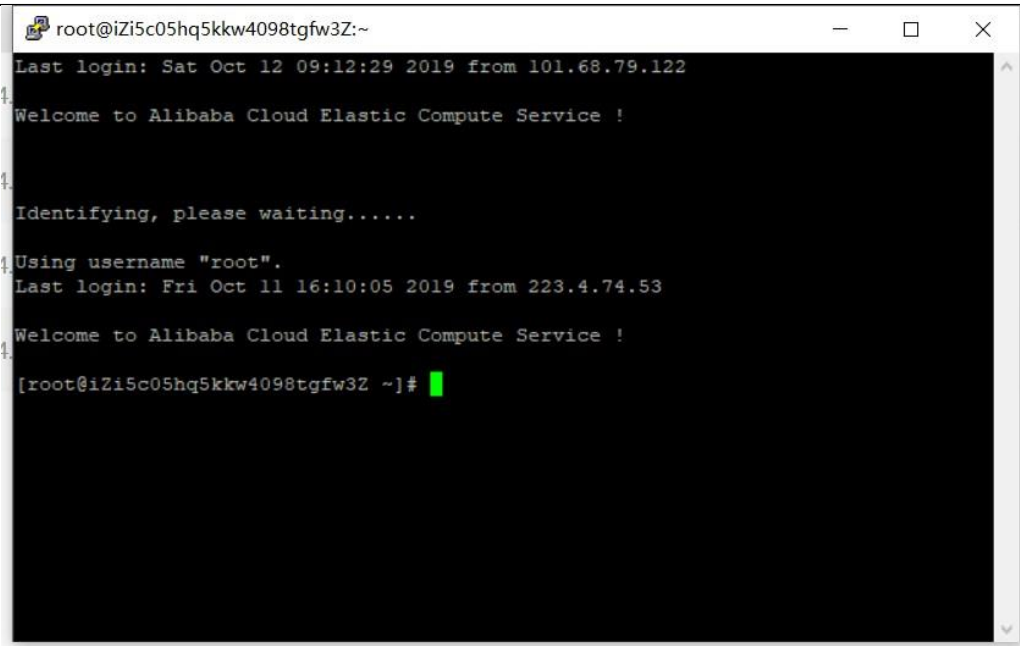
1. 打开Chrome浏览器。
2. 在地址栏中，输入https://思福迪堡垒机的访问地址，按回车键（Enter），进入系统登录页面。输入运维账号、密码【或验证码】，登录思福迪堡垒机。
3. 点击左侧的-分组管理-在主机分组中选择主机的分组，在右侧选择要运维的主机，点击协议类型下面的RDP或SSH，选择右侧的连接模式【客户端：直接调用mstsc的方式运维；WEB访问：直接使用浏览器的新标签进行运维】，（RDP模式可勾选剪贴板和磁盘映射，用户可根据需要自行选择。）点击“连接”按钮，如下图所示：



4.1.1 SSH协议运维

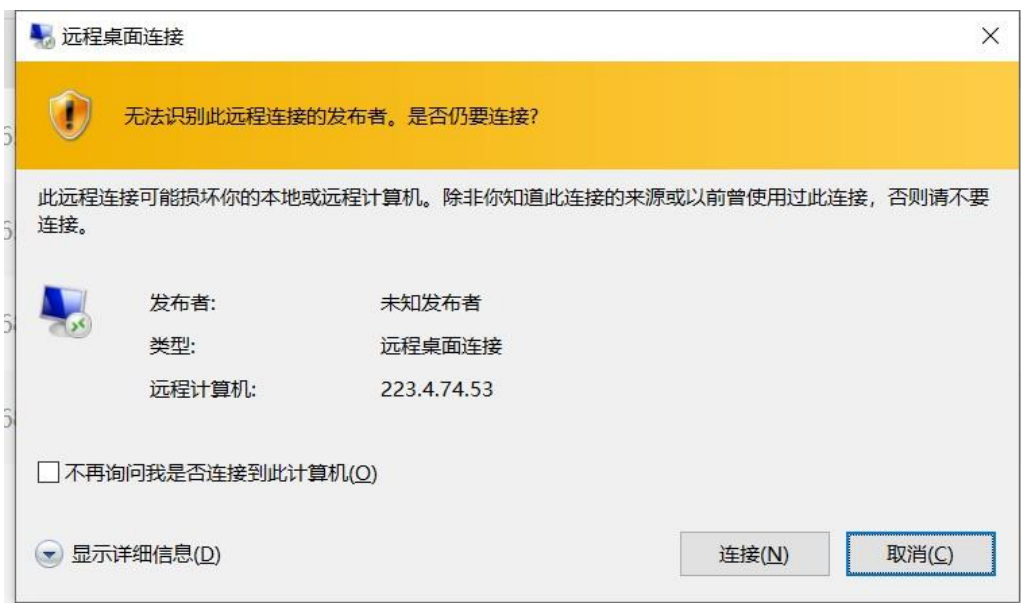
1. 以Centos的SSH为例，当选择主机是SSH类型的协议时，选择客户端方式，putty工具，点击“连接”按钮，系统会使用设置的root账号和密码自动连接到命令管理界面，具体如下图所示：



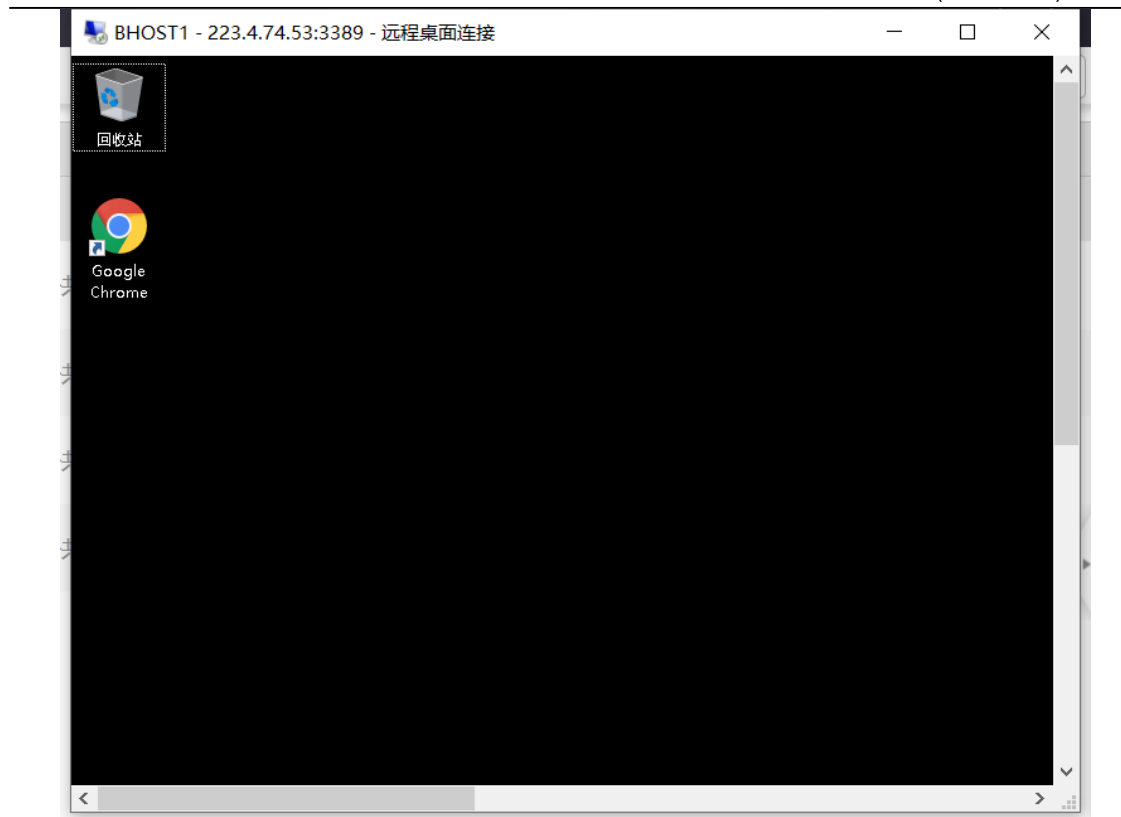


4.1.2 RDP协议运维

1. 以windows的RDP协议为例，在弹出的对话框中选择“连接”，如下图所示：



2. 如果系统管理员在添加主机资产时设置了运维帐号的用户名和密码，将会自动连接到windows的远程桌面，（若没有设置，将会弹出对话框要求用户输入windowsserver的系统管理员的用户名和密码）如下图所示：



4.1.3 SFTP协议运维

1. 可以使用Web方式调用SFTP工具：通过web方式登陆堡垒机、在主机列表中选择，SSH服务，然后在SSH服务配置参数中，选择“Web访问”选项，勾选“连接SFTP”选项，如下图所示：

SSH

选择用户: root

密码:

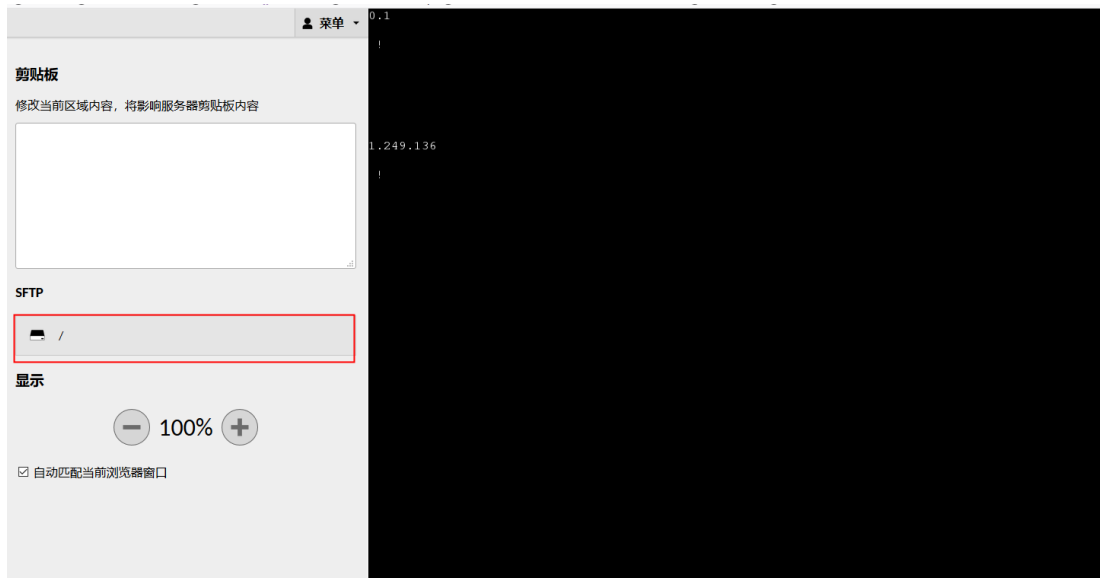
连接模式: ☐ 客户端 ☒ WEB访问

编码方式: UTF-8

☒ 连接SFTP

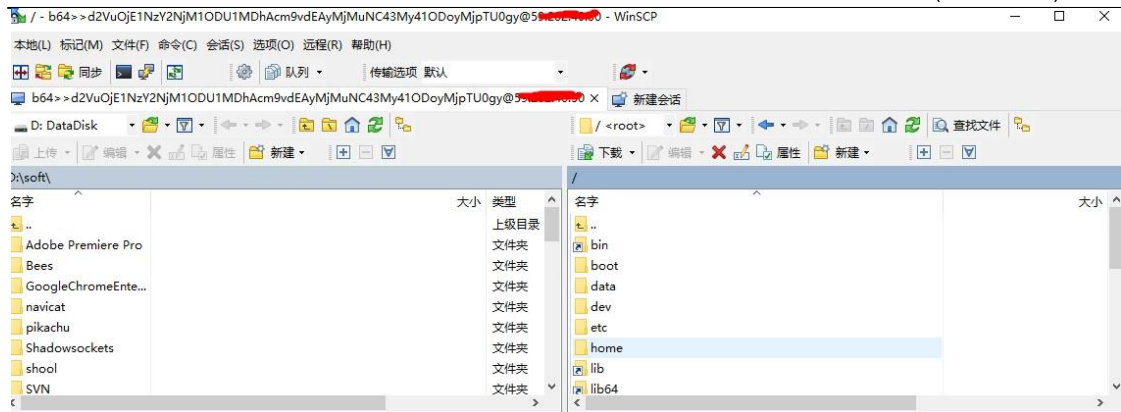
连接方式: SSH2

2. 连接成功后，按快捷键ctrl+shift+alt键可以调出sftp的传输菜单，再次按快捷键ctrl+shift+alt键可以隐藏sftp的传输菜单，如下图所示：



3. 点击上图中的/可进行文件的传输操作。
4. 也可以使用客户端模式，通过调用本地的winscp工具进行sftp协议的传输，选择SFTP协议，本地客户端设置WinSCP工具的路径，连接方式选择SSH2, 点击连接，如下图所示：





注意：

初次使用运维账号登陆，一定要先安装“BHostClient插件”控件，否则无法正常运维！

4.2 C/S方式运维

4.2.1 MacOS操作系统

在使用苹果系统客户端采用C/S模式进行主机运维操作前，请确保已完成下列准备工作：

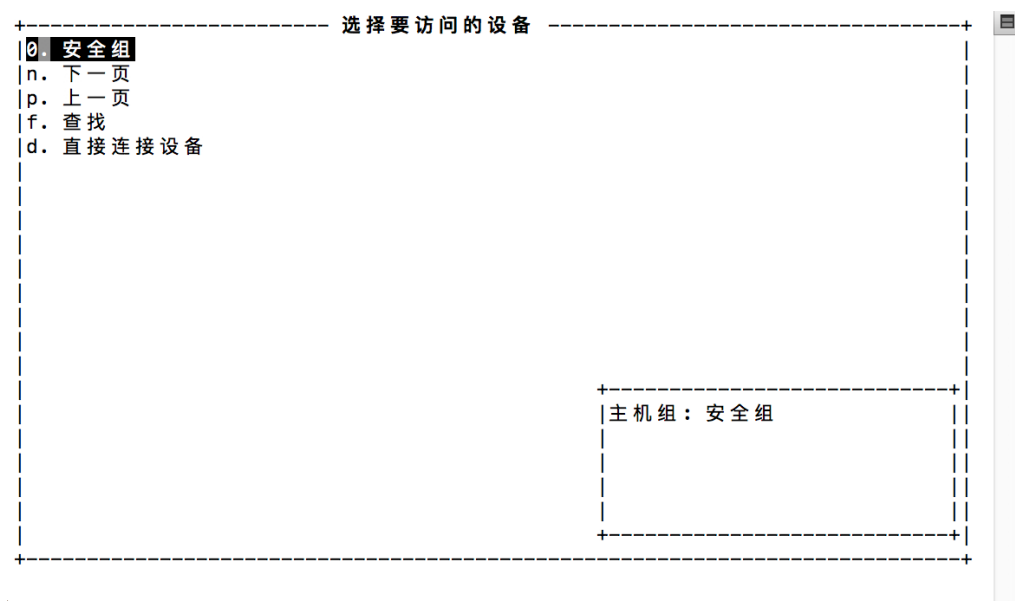
- 本地已安装支持SSH协议的app，例如命令行终端【系统自带不需要安装】、SecureCRT、Xshell等。
- 本地已安装支持RDP协议的app，例如微软的远程桌面连接工具。
- 确保苹果系统客户端与思福迪堡垒机的端口正常连通【思福迪堡垒机的入站要放行TCP的222和3389端口】，主要包括以下两个端口：
 - -222：用于访问SSH协议的主机。
 - -3389：用于访问RDP协议的主机。
- 确保思福迪堡垒机与目标主机的运维端口正常连通，例如SSH协议及端口、RDP协议及端口。

SSH协议运维

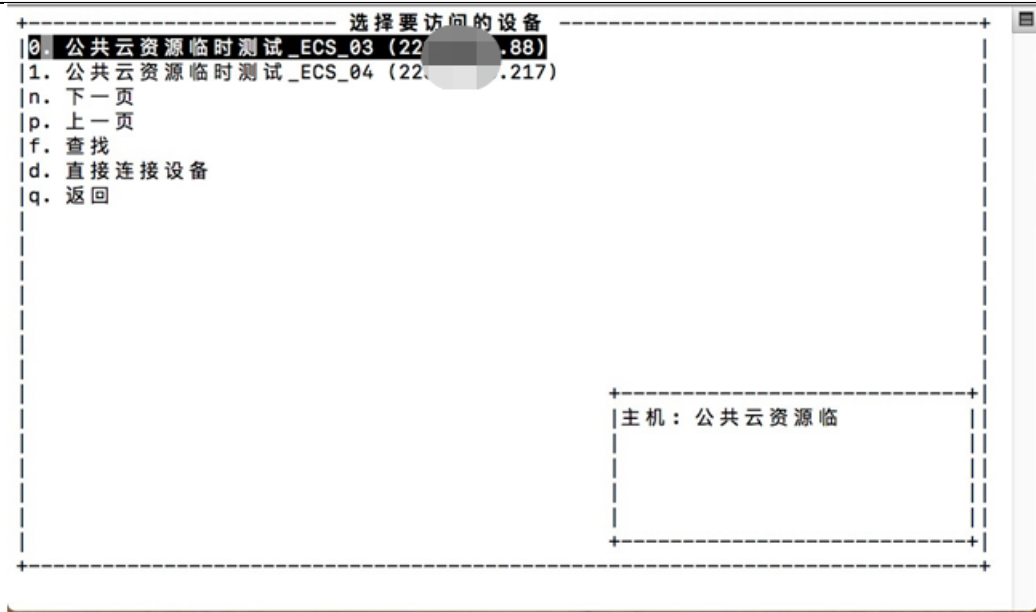
1. 打开命令行终端app, 输入`ssh思福迪堡垒机的用户名@思福迪堡垒机的IP -p222` 命令, 按回车键 (Enter), 输入运维账号的用户名和密码, 如下图所示:



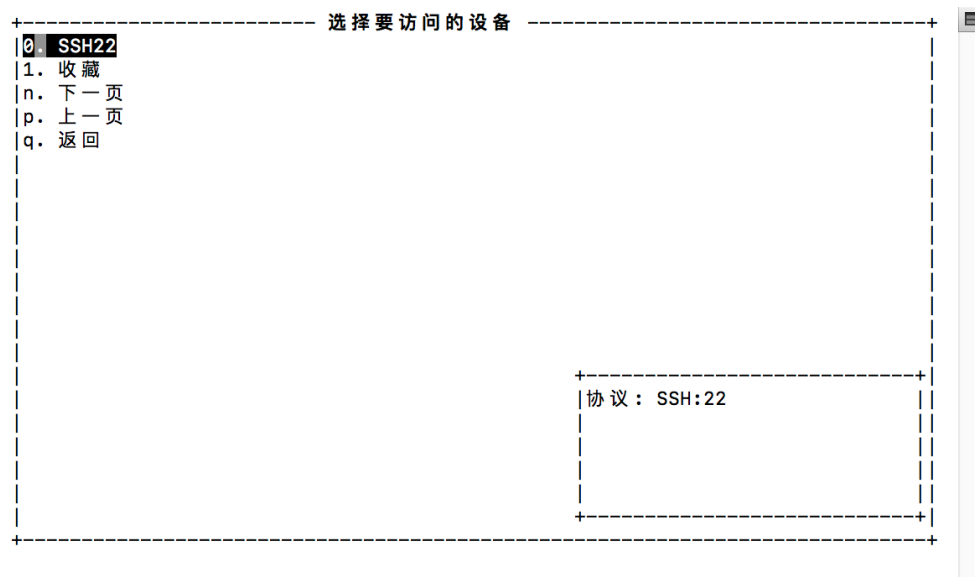
2. 进入运维设备的选择界面, 选择要运维的设备组, 按回车键 (Enter), 如下图所示:



3. 选择要运维的主机设备, 按回车键 (Enter), 如下图所示:



4. 选择协议的类型，按回车键，如下图所示：



5. 选择登陆的用户名，按回车键，选择是否要保存密码，按回车键，即可连接到管理的设备上，具体如下图所示：

选择要访问的设备

0. root
n. 下一页
p. 上一页
q. 返回

用户: root

选择要访问的设备

0. root
n. 下一页
p. 上一页
q. 返回

准备连接

确认使用已保存的密码连接

< 是 > < 否 >

用户: root

Using username "root".
Last login: Sat Oct 12 09:33:06 2019 from 223.4.74.53
Welcome to Alibaba Cloud Elastic Compute Service !
[root@iZi5c05hq5kkw4098tgfw3Z ~]#

RDP协议运维

1. 打开远程桌面连接app，输入思福迪堡垒机IP，如下图所示：



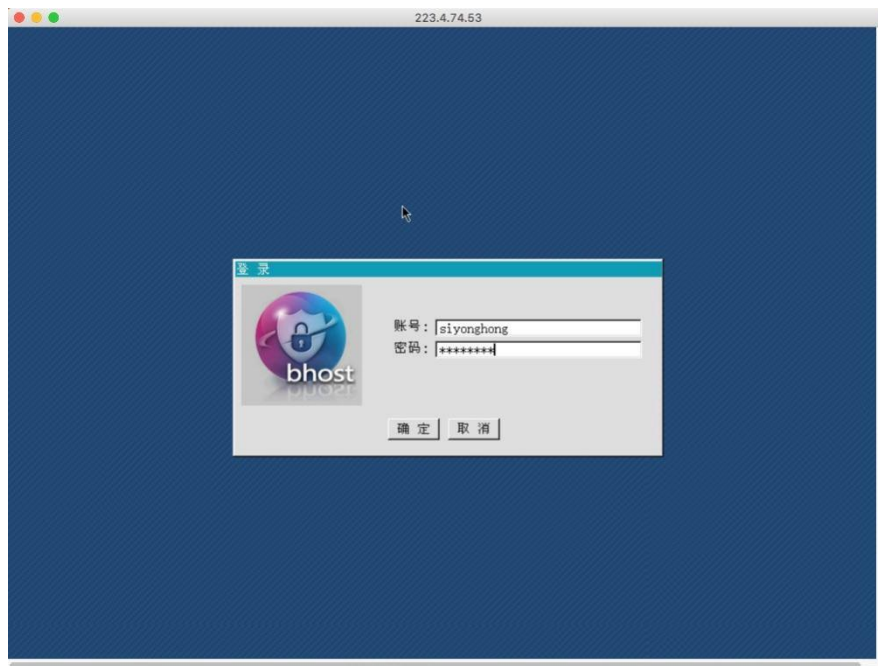
2. 在是否仍要连接此计算机？对话框中，单击**连接**，如下图所示：



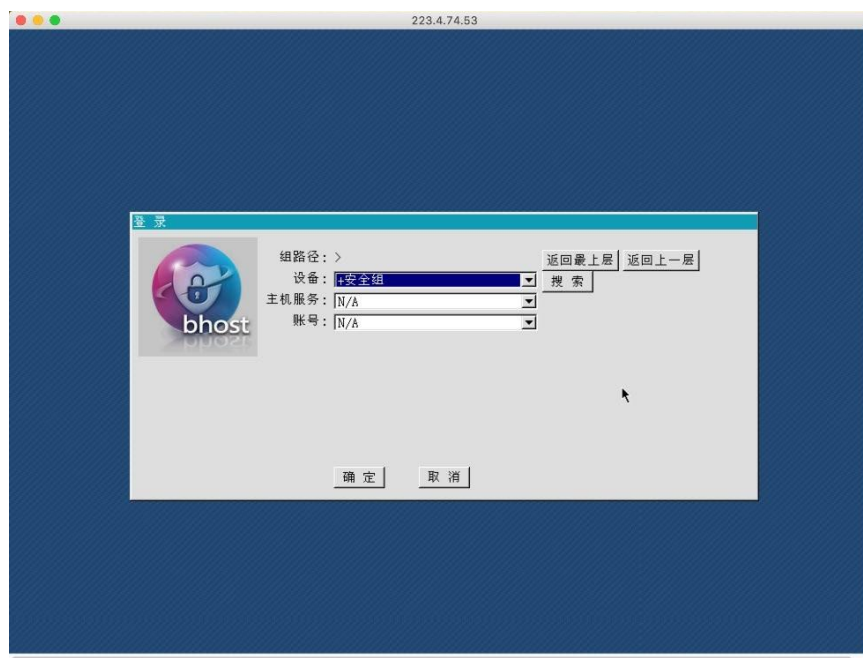
3. 如果一直提示连接，可参照下图的设置（安全性——即使验证失败，也始终连接）：

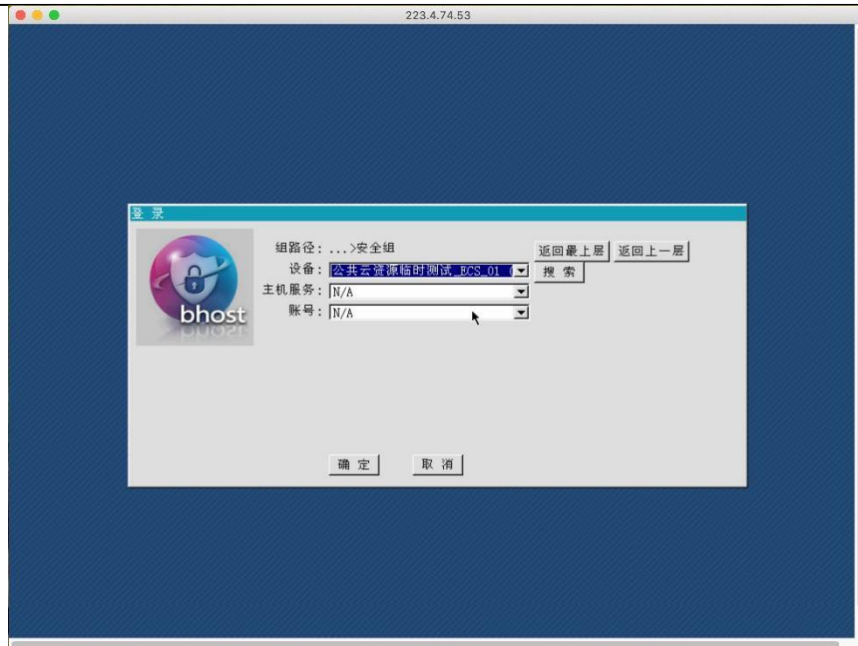


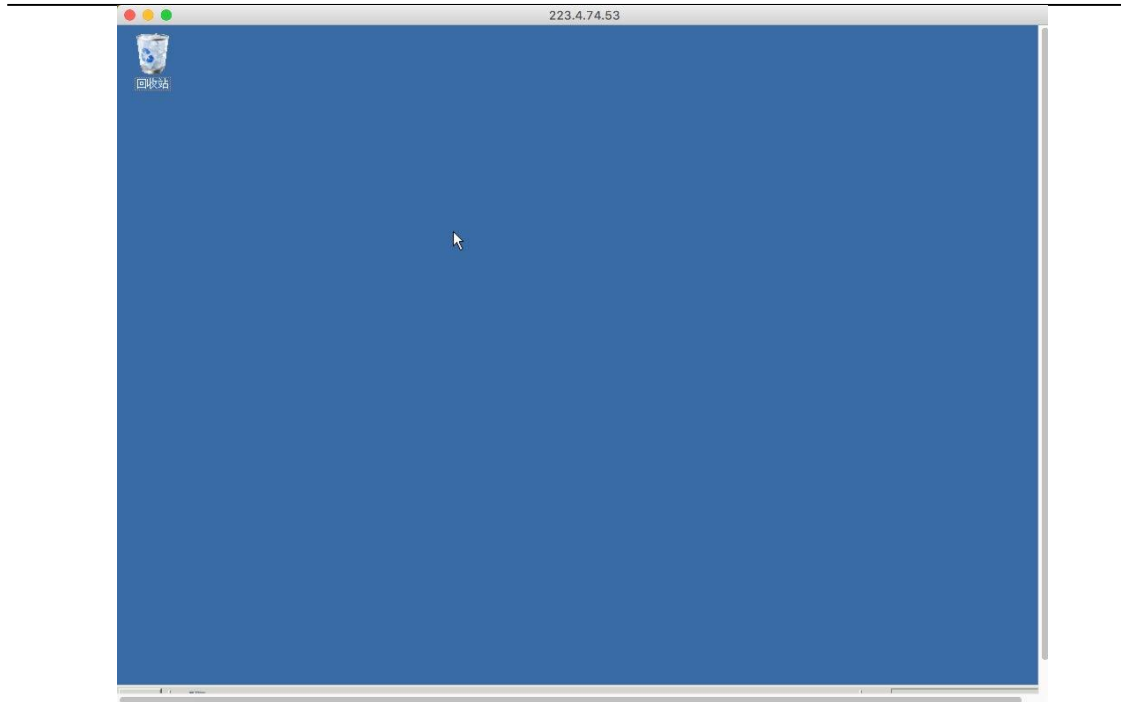
4. 在思福迪堡垒机登录窗口，输入思福迪堡垒机的运维用户名和密码，单击确定，如下图所示：



5. 在设备栏中选择设备组-在显示的设备组列表中选择要运维的设备名称-点击确认按钮，即可远程到要管理的服务端，如下图所示：







SFTP协议运维

1. 通过web方式登陆堡垒机、在主机列表中选择，SSH服务，然后在SSH服务配置参数中，选择“Web访问”选项，勾选“连接SFTP”选项，如下图所示：

SSH

选择用户: root

密码:

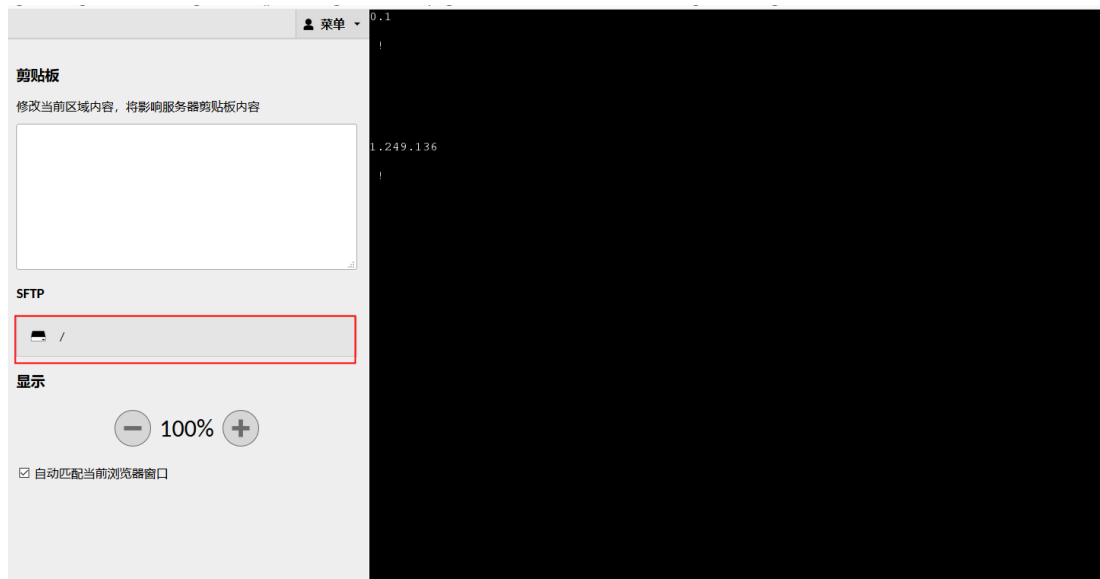
连接模式: ☐ 客户端 ☒ WEB访问

编码方式: UTF-8

☒ 连接SFTP

连接方式: SSH2

2. 连接成功后，按快捷键ctrl+shift+alt键可以调出sftp的传输菜单，再次按快捷键ctrl+shift+alt键可以隐藏sftp的传输菜单，如下图所示：



3. 点击上图红框中的/，然后在弹出的目录中选择要上传文件的目录，点击上面的“上传”按钮，选择本地的文件，点击上传即可完成上传。

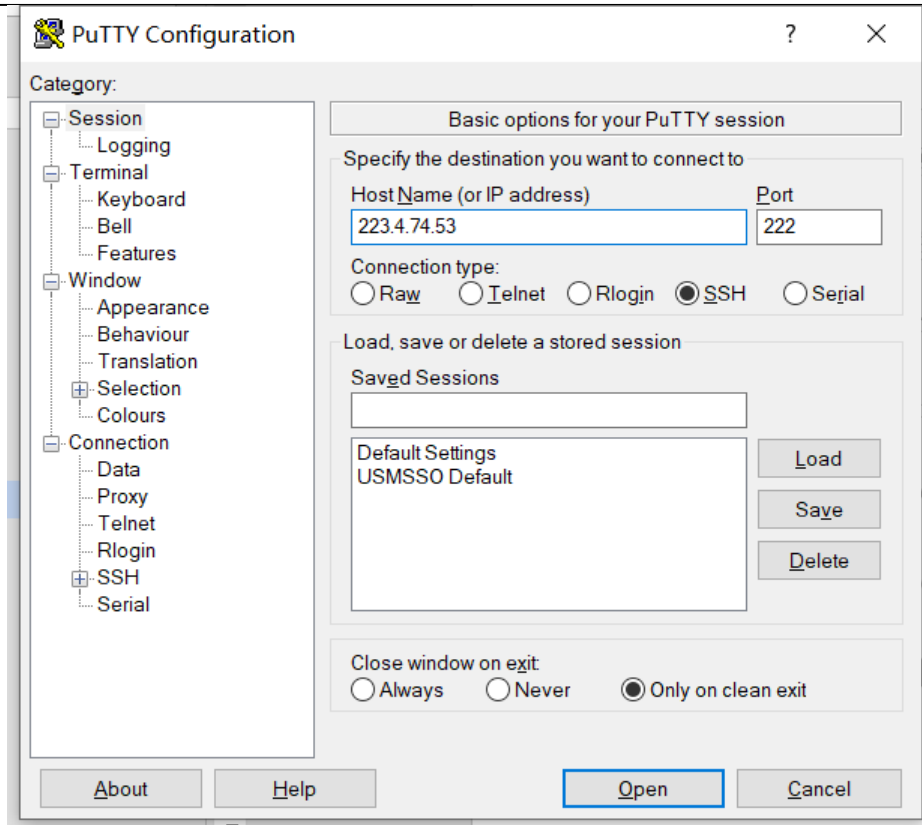
4.2.2 Windows操作系统

在使用Windows系统客户端,进行C/S模式的主机运维操作前,请确保已完成下列准备工作:

- 本地已安装支持SSH协议（包括ssh和sftp）的客户端程序，例如 Putty、SecureCRT、Xshell、FlashFXP等。
- 确保运维客户端到思福迪堡垒机的端口通信正常：
 - 222：用于访问SSH协议的主机。
 - 3389：用于访问RDP协议的主机。

SSH协议运维

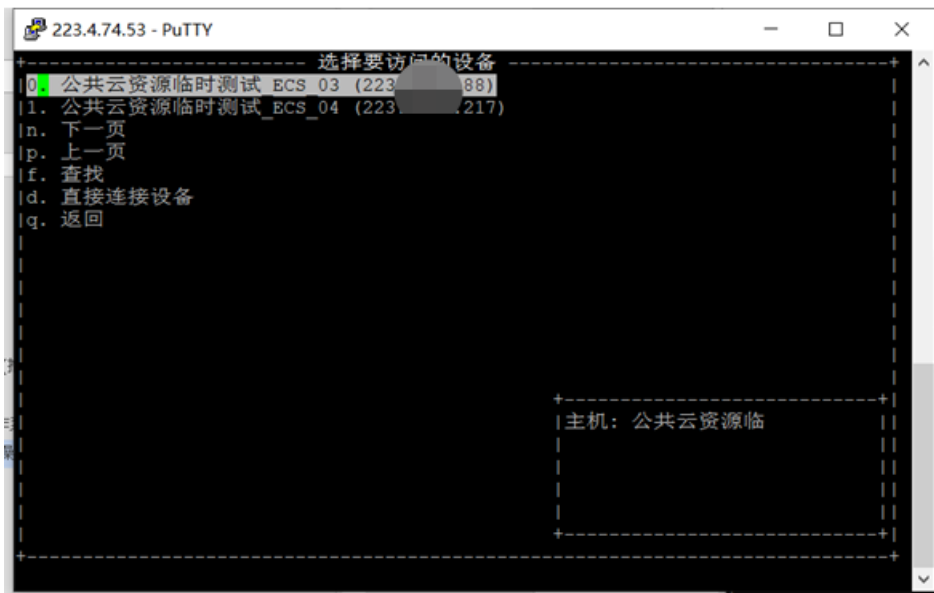
1. 打开Putty客户端，主机或IP处填写思福迪堡垒机的 IP地址，端口填写222，点击open按钮，如下图所示：



2. 在弹出的对话框中输入运维的账号和密码, 如下图所示:



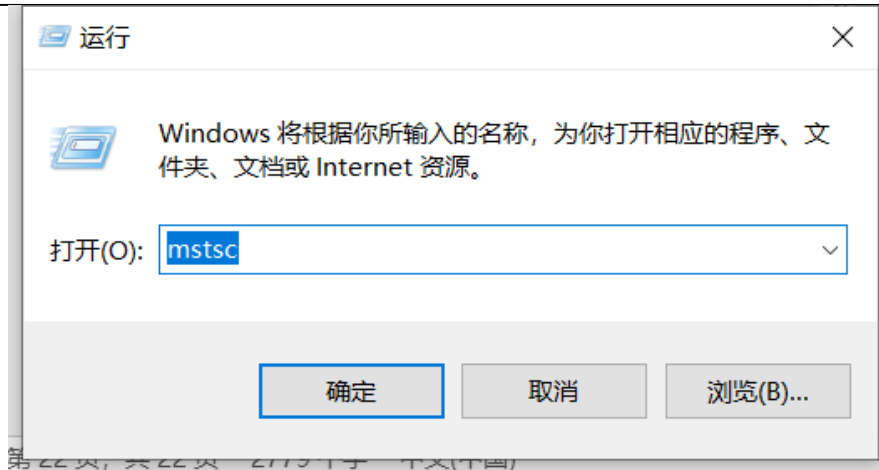
3. 在选择要访问的设备中选择设备组-设备-协议版本-用户-选择是否保存密码选项, 即可进入运维服务器, 如下图所示:



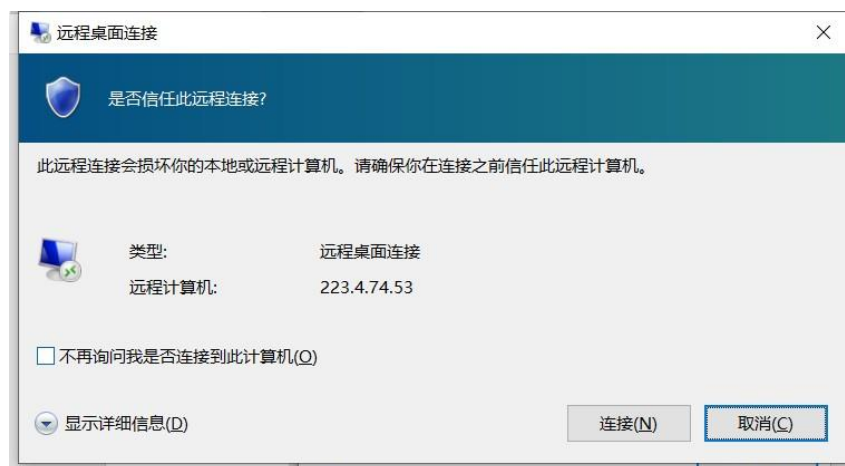
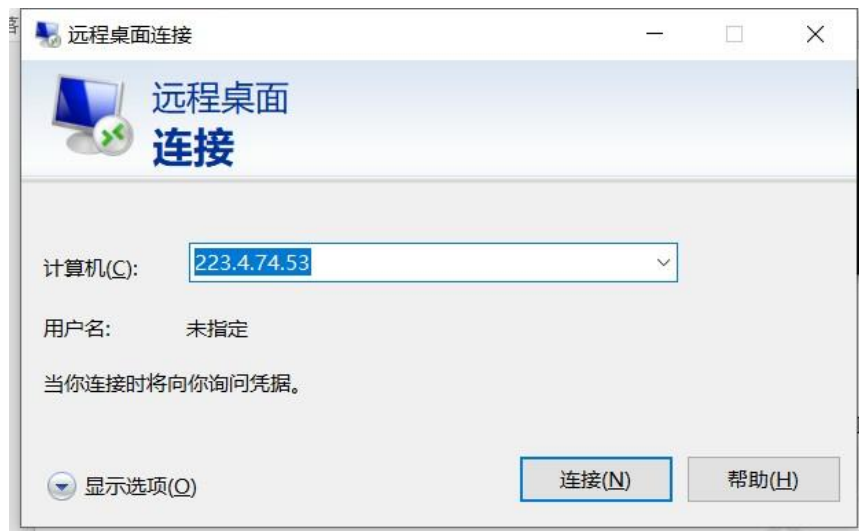


RDP协议运维

1. 点击开始菜单-选择“运行”-输入mstsc命令, 点击确认, 如下图所示:



2. 在弹出的对话框中输入思福迪堡垒机的IP地址, 点击连接按钮, 在弹出的对话框中选择”连接”, 证书信任选择”是”, 如下图所示:

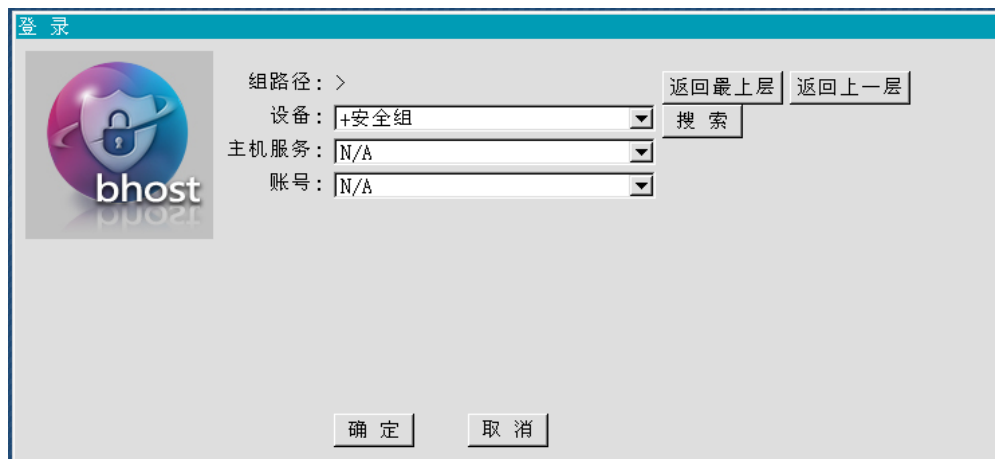




3. 在弹出的窗口中输入运维人员的账号和密码, 按确认按钮, 如下图所示:



4. 选择设备组-设备-选择是否保存用户名密码, 即可远程到要管理的 windows 服务器, 具体如下图所示:



登 录



组路径：...>安全组 返回最上层 返回上一层

设备：公共云资源临时测试_ECS_01 搜索

主机服务：N/A

账号：N/A

确定 取消

登 录



组路径：...>安全组 返回最上层 返回上一层

设备：公共云资源临时测试_ECS_01 搜索

主机服务：RDP3389

账号：提示信息

密：是否保存账号密码？

应用程序： 是 否

访问方：

确定 取消 收藏 取消收藏

登 录



组路径：...>安全组 返回最上层 返回上一层

设备：公共云资源临时测试_ECS_01 搜索

主机服务：RDP3389

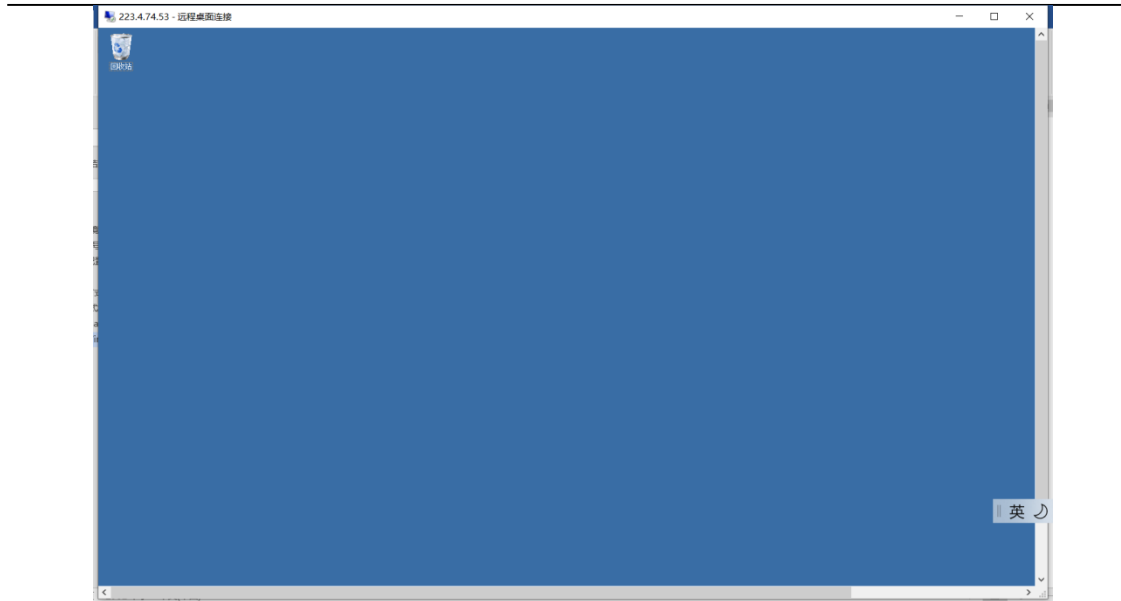
账号：administrator

密码：*****

应用程序：default

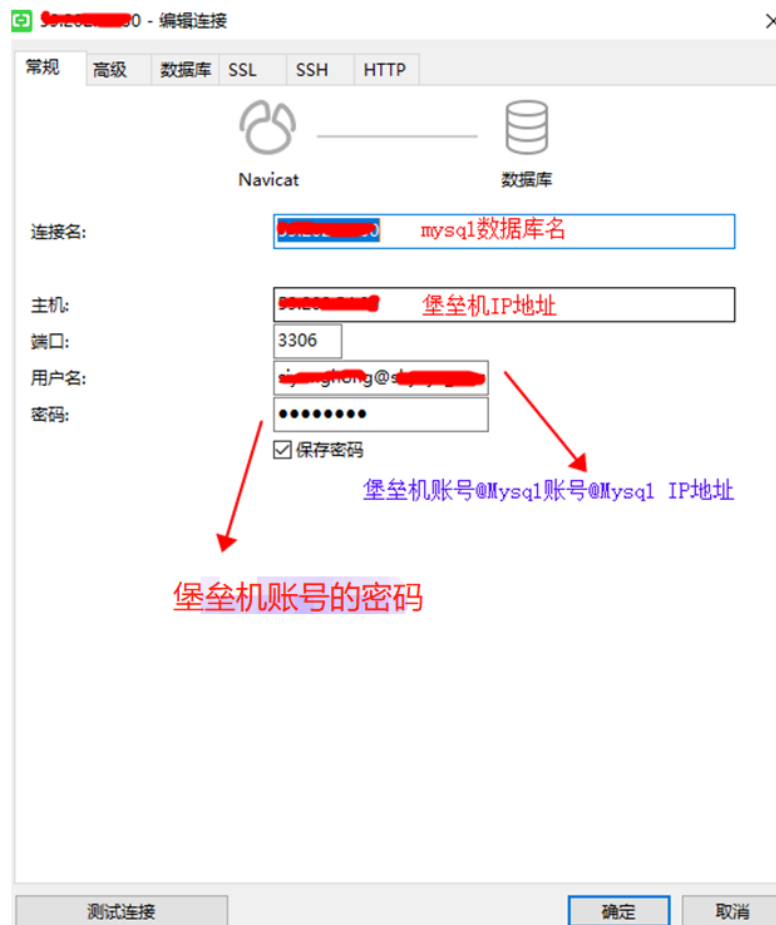
访问方式：NORMAL

确定 取消 收藏 取消收藏



Mysql协议运维

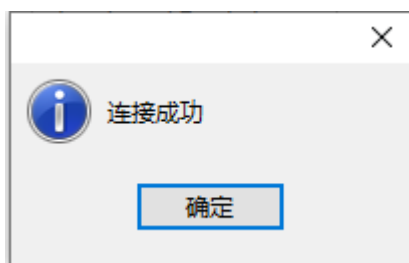
1. 打开NaviCat客户端，具体配置如下的连接属性（连接名、主机、端口、用户名、密码）如下图所示：



配置参数说明：

- **连接名：**可以填写Mysql数据库的名称，用户自定义；
- **主机：**这里填写堡垒机的IP地址；
- **端口：**Mysql数据库的默认端口为3306；
- **用户名：**这里填写格式堡垒机运维账号@Mysql数据库用户名@Mysql数据库IP地址,比如运维账号为zhangsan，数据库用户名为root，数据库Ip地址为192.168.1.100，这里填写的格式为shangsan@root@192.168.1.100
- **密码：**这里填写的密码为运维用户密码。

2. 配置完成后，点击测试连接，会提示连接成功的信息，如下图所示：



3. 配置完成后运维用户就可以直接使用本地的Navicat软件来管理 Mysql数据库了。

SQLServer协议运维

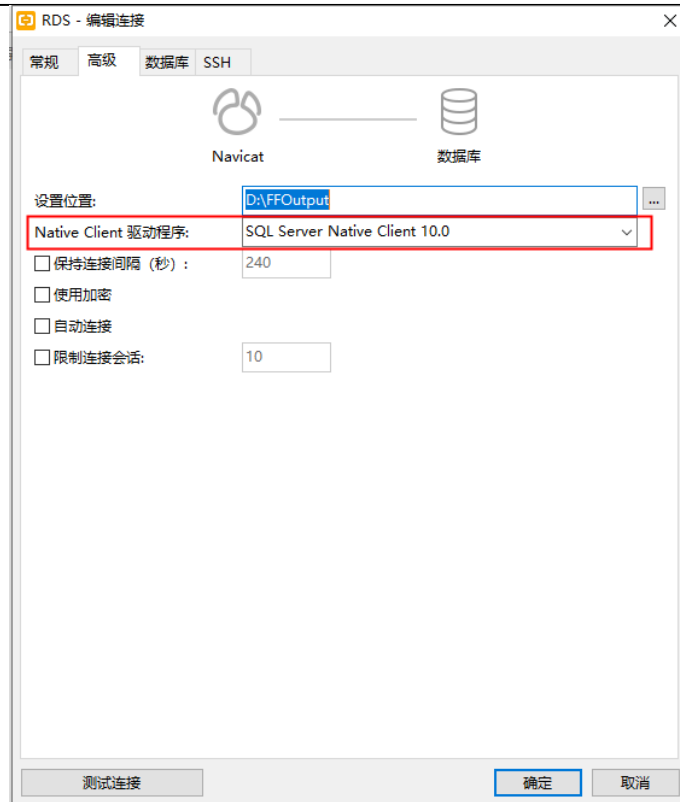
1、 如果您已经安装了Navicat客户端管理工具，需要提前安装

C:\ProgramFiles\PremiumSoft\NavicatPremium12目录下的两个文件：

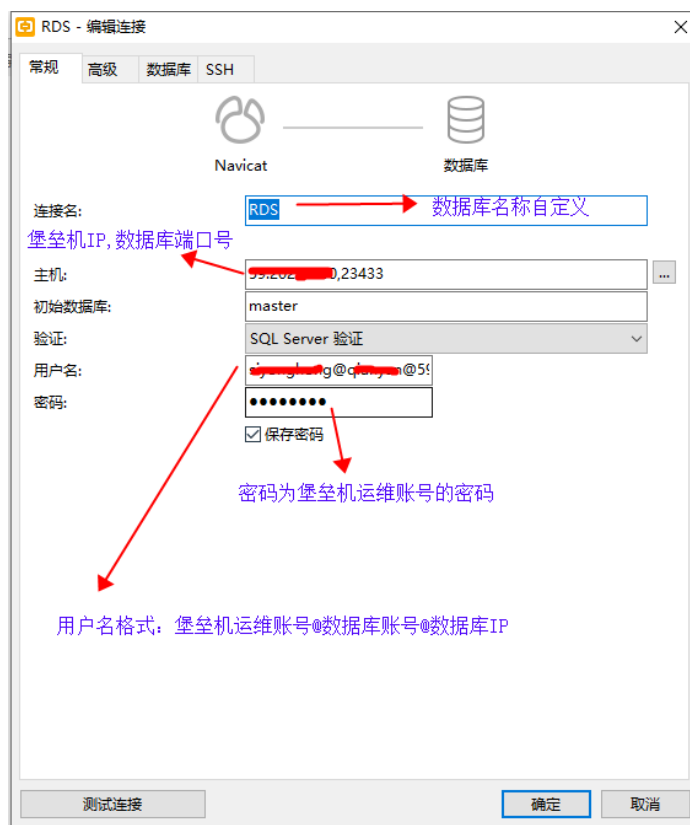
sqlncli.msi、sqlncli_x64.msi，如下图所示：

sqlite.dll	11/20/2018 10:30 AM	应用程序扩展	339 KB
sqlite3.dll	11/20/2018 10:30 AM	应用程序扩展	1,000 KB
sqlncli.msi	11/12/2014 12:24 PM	Windows Install...	4,471 KB
sqlncli_x64.msi	11/12/2014 12:24 PM	Windows Install...	7,885 KB
ssleay32.dll	11/20/2018 10:30 AM	应用程序扩展	349 KB

2、 打开Navicat客户端，点击连接“选择SQLServer”，在新建连接中点击高级，配置“设置位置”、“NativeClient驱动程序”，如下图所示：

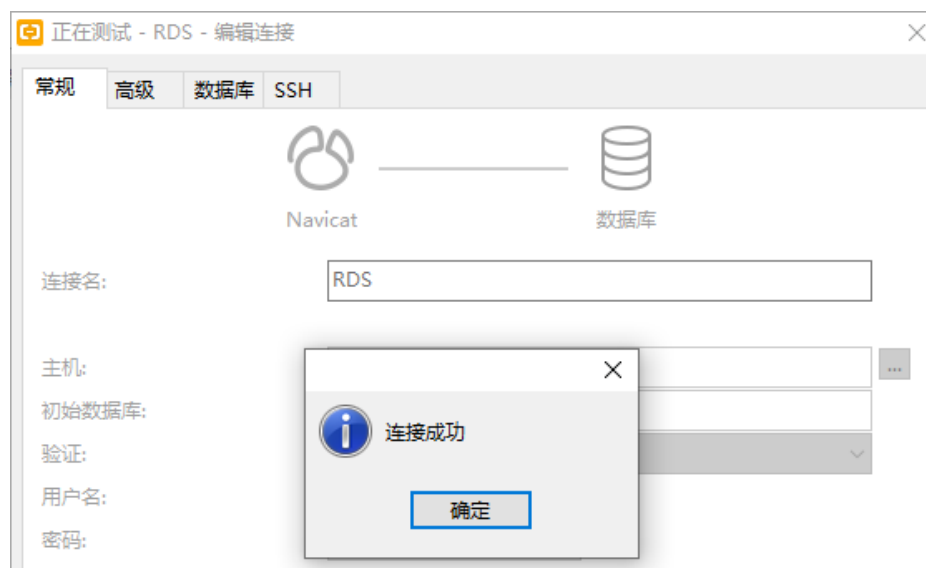


- 3、在“常规”选项卡中，配置如下的连接属性（连接名、主机、端口、用户名、密码）如下图所示：



- 连接名：可以填写SQLServer数据库的名称，用户自定义；
- 主机：这里填写堡垒机的IP地址，数据库端口号；
- 初始数据库：默认master即可；
- 用户名：这里填写格式堡垒机运维账号@SQLServer数据库用户名@SQLServer数据库IP地址,比如运维账号为zhangsan，数据库用户名为sa，数据库Ip地址为192.168.1.100，这里填写的格式为shangsan@sa@192.168.1.100
- 密码：这里填写的密码堡垒机运维账号的密码。

4、配置完成后，点击测试连接，会提示连接成功的信息，如下图所示：



配置完成后运维用户就可以直接使用本地的Navicat软件来管理SQLServer数据库了。