文档 4

思福迪

LogBase SOM 运维安全管理系统

运维用户使用手册

杭州思福迪信息技术有限公司

目录

欢迎使用

欢迎您使用 LogBase 运维安全管理系统！

版权声明

获取帮助

产品相关资料可以访问我公司网站：http://www.logbase.cn

您也可以通过 Email 来获取资料或反馈信息：support@logbase.cn

获取更详尽有关思福迪网络安全专业服务信息、商务信息，您可通过如下方式联系我们：

- 全国 24 小时服务热线：400-678-1500
- 商务咨询热线：0571-88923189
- 技术支持热线：0571-88923665
- 技术支持 QQ：4006781500

格式约定

本文中所有图例均为实际拍摄或屏幕截取；

特殊名称的表示方法：**《章节》**，**『菜单名称』**，**[标题/按钮名称]**，**「标题栏」**，**"选项名称"**；

产品中采用了大量的浮层设计，将鼠标放置在列表数据上会出现浮层，图标说明：  ：回放，  ：监控，  ：阻断，  ：关联数据，  ：编辑，  ：删除，  ：导出，  ：下载，  ：启用，  ：停用，  ：查看详情，  ：查看报告，  ：再次执行

系统页面常用图标说明：  ：返回，  ：收拢条件，  ：查询，  ：添加条件

 ：为重要提示说明；

名词释义

- 堡垒机：本文档中特指 LogBase 运维安全管理系统；
- 运维用户：本文档中特指通过 LogBase 运维安全管理系统访问的用户；
- 运维主机：本文档中特指托管在 LogBase 运维安全管理系统中的主机；

手册概述

LogBase 运维安全管理系统是我公司自主研发的，具有完全知识产权的安全审计类产品。该系统能够实现对运维人员日常服务器、网络设备、数据库维护过程的行为记录、监视、控制等功能，具备异常操作行为的告警及阻断能力，拥有完善的安全审计报表系统，是一款具备事前控制、事后审计能力的产品；同时还具备服务器密码管理，访问权限控制等功能，通过该产品的部署，各组织单位能够获得对内部以及第三方运维人员操作行为的全面审计与控制能力，弥补传统系统审计能力不足的缺点，完善企事业单位安全审计体系建设。

本手册详细介绍了 LogBase 运维安全管理系统包括超级管理员、配置管理员、审计管理员、密码管理员、系统管理员以及系统审计员各功能模块的使用方法，用户可参考本手册，通过 LogBase 运维安全管理系统进行各种运维管理和审计管理。

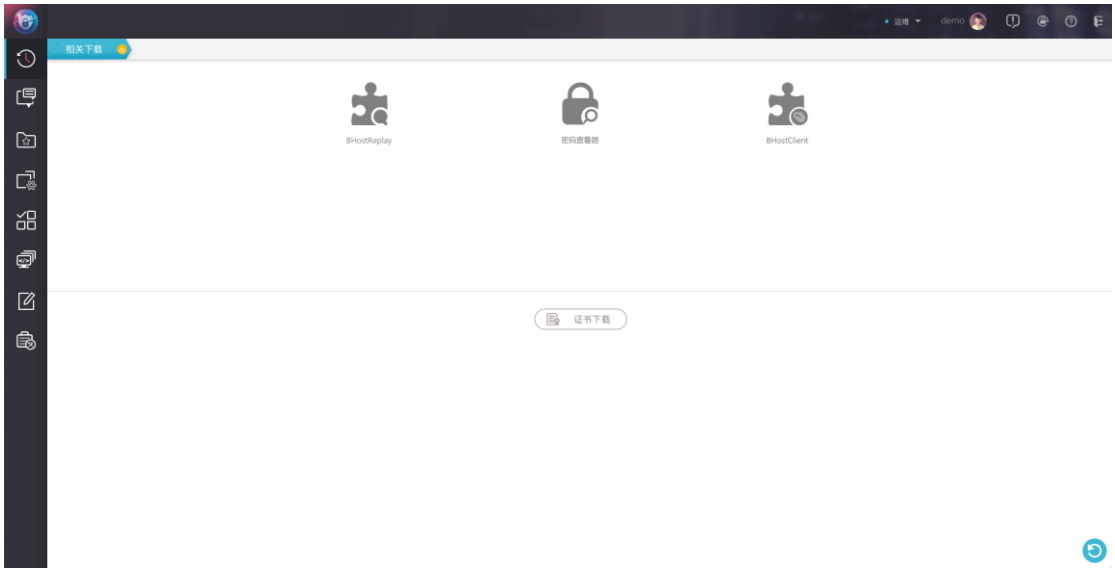
1. 系统登录

LogBase 运维安全管理系统采用 B/S 架构管理，使用浏览器访问 https://[IP]即可登录系统界面，登录界面如图所示：

2. 快速使用

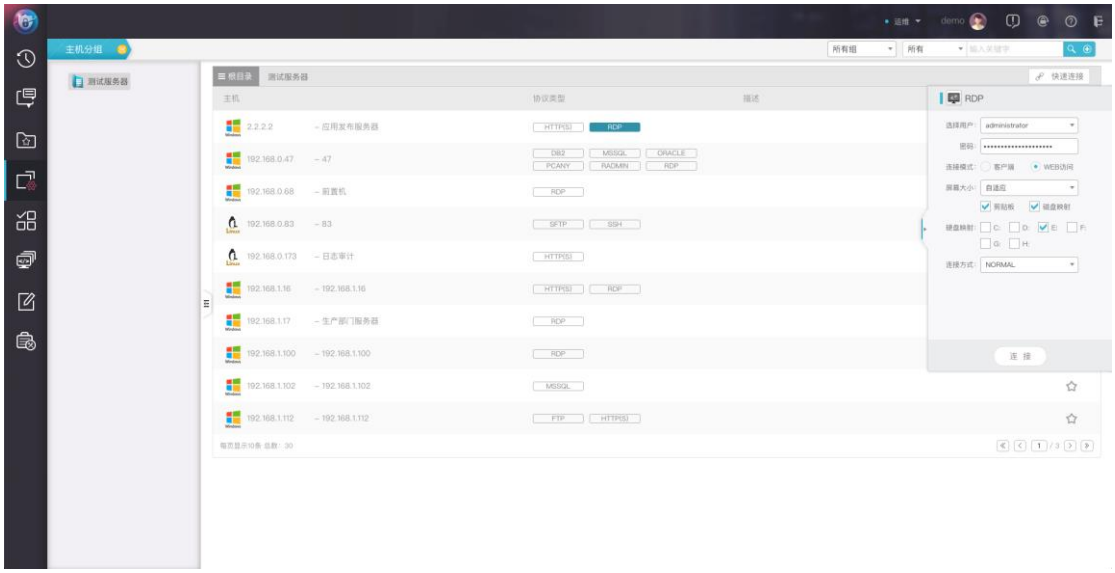
2.1. 运维客户端安装

登录系统后点击右上角**[相关下载]**，下载[BhostClient]，下载完成后根据安装提示默认安装即可，如图所示：



2.2. WEB 访问

在『**主机列表**』中选择要访问的主机及协议，如图所示：



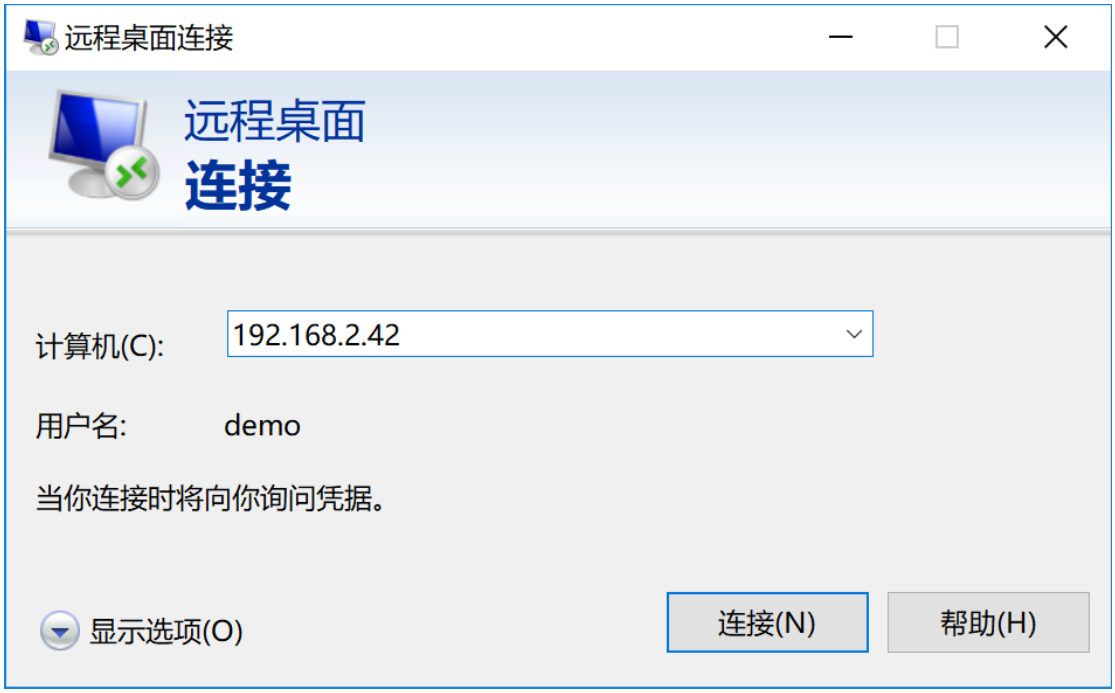
在右侧连接窗口中选择配置用户、连接模式、分辨率及其他辅助功能，点击连接即可。

运维访问支持[客户端]和[WEB]两种方式，选择[客户端]方式点击连接可配置该客户端的本地路径。

2.3. C₩S 菜单访问

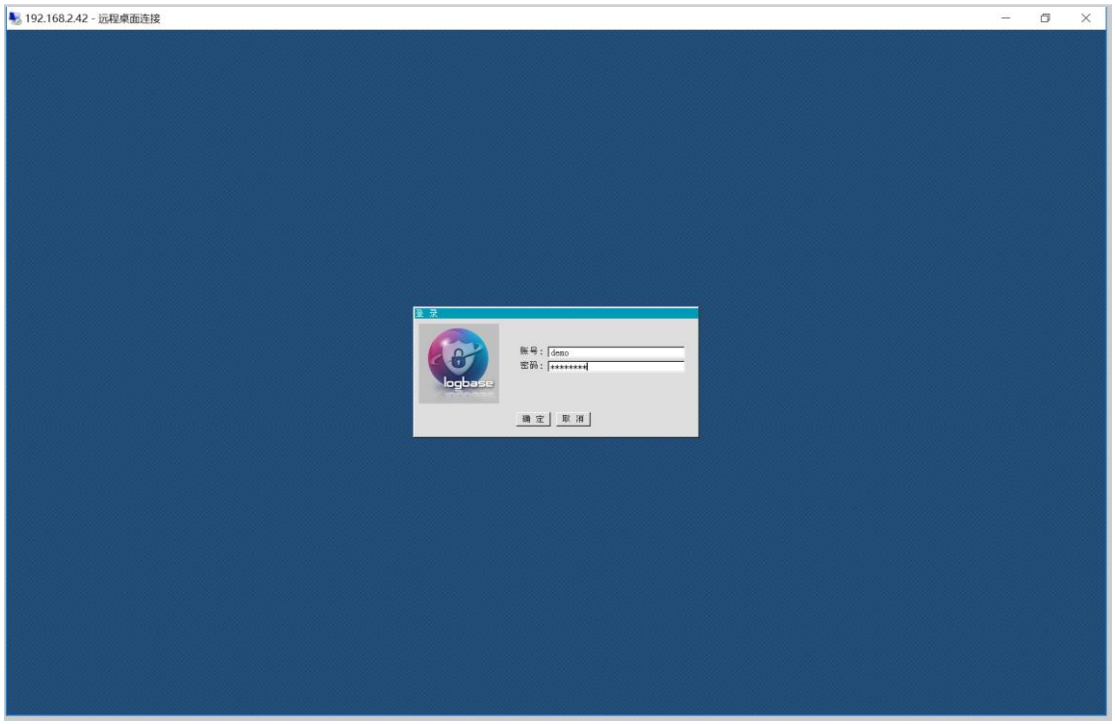
2.3.1. 图形化 C₩S 菜单

使用远程桌面连接工具（如：Mstsc、RDC、Desktop 等）连接堡垒机 C₩S 菜单模式可访问所有图形协议（如：RDP、VNC、X11、应用发布等），连接方式如下：



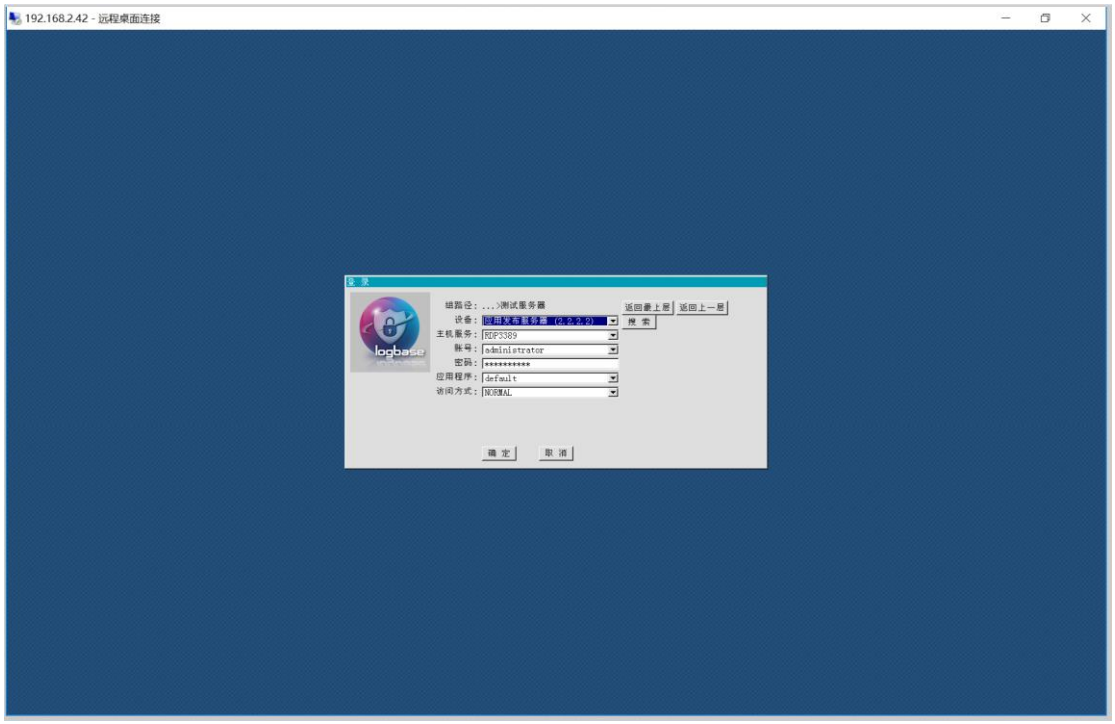
- 计算机：堡垒机 IP；
- 用户名：堡垒机运维账号，也可未指定连接后再填写；
- 显示选项：可开启 RDP 剪贴板及磁盘映射等辅助功能；

点击[连接]进入图形化 C₩S 菜单登录界面，如图所示：



- 账号：运维账号；
- 密码：运维账号密码；

点击[确定]进入图形化 CWS 菜单选择界面，如图所示：



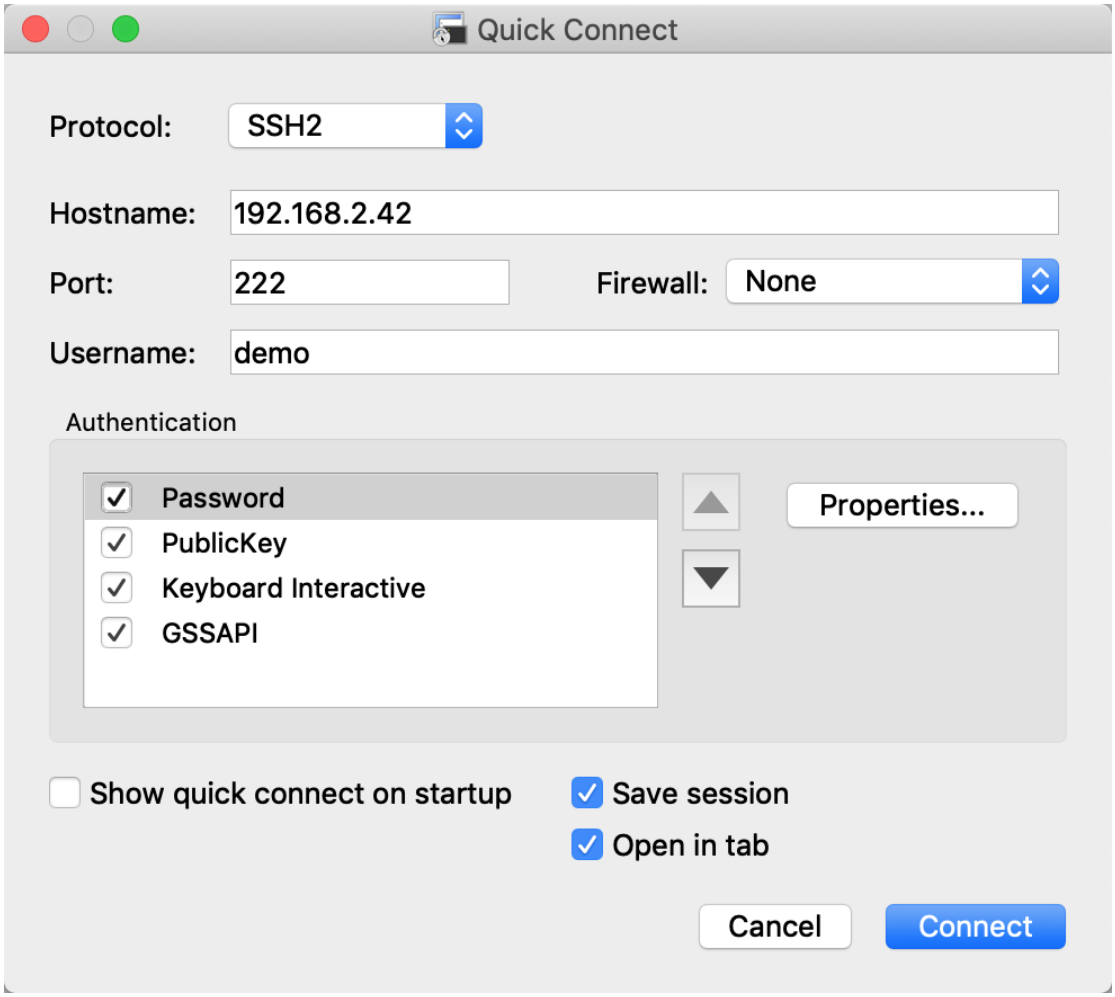
- 组路径：显示当前主机组路径；

- 设备：选择要访问的主机；
- 搜索：根据 IP 或主机名进行搜索；
- 主机服务：选择要访问的服务；
- 账号：选择或填写主机账号
- 密码：填写主机账号密码；
- 应用程序：选择应用发布时所需的工具；
- 访问方式：选择协议特有的访问方式。

点击**[确定]**即可连接当前主机访问。

2.3.2. 字符型 C₩S 菜单

使用字符型终端连接工具（如：SecureCRT、Xshell、Putty、Terminal for Mac、Terminal for Linux 等）连接堡垒机 C₩S 菜单模式可访问所有字符型协议（如：SSH、Telnet、Rlogin 等），连接方式如下：

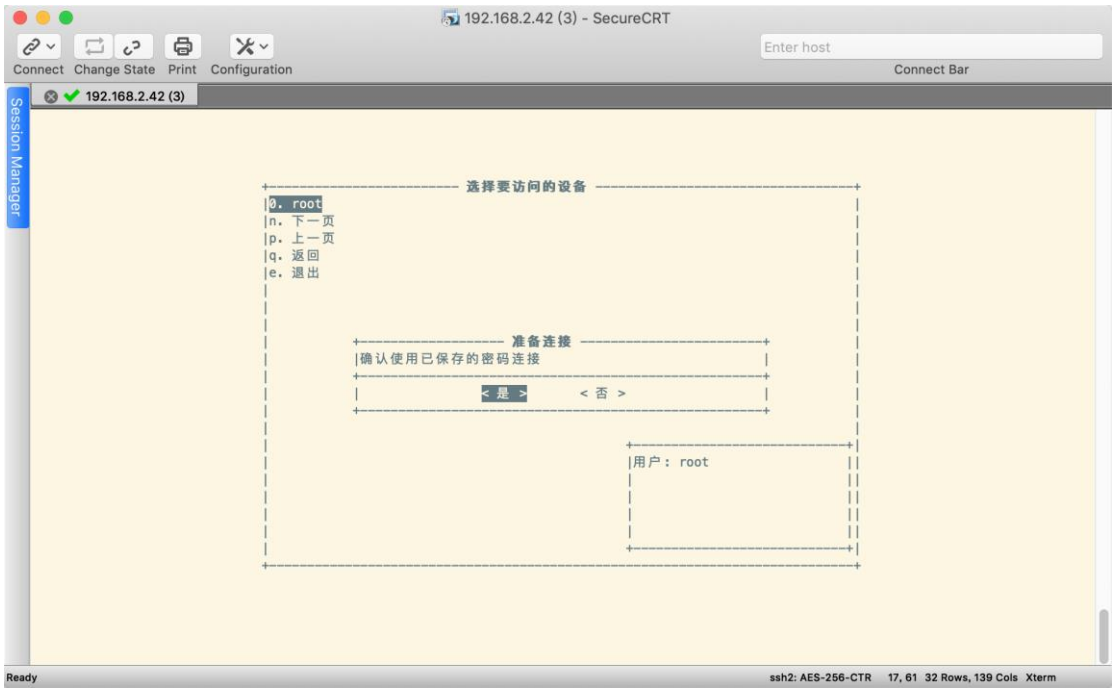


- 主机名：堡垒机 IP；
- 端口：222；
- 用户名：堡垒机运维账号。

点击[连接]输入运维用户密码后进入字符型 CWS 菜单选择界面，如图所示：

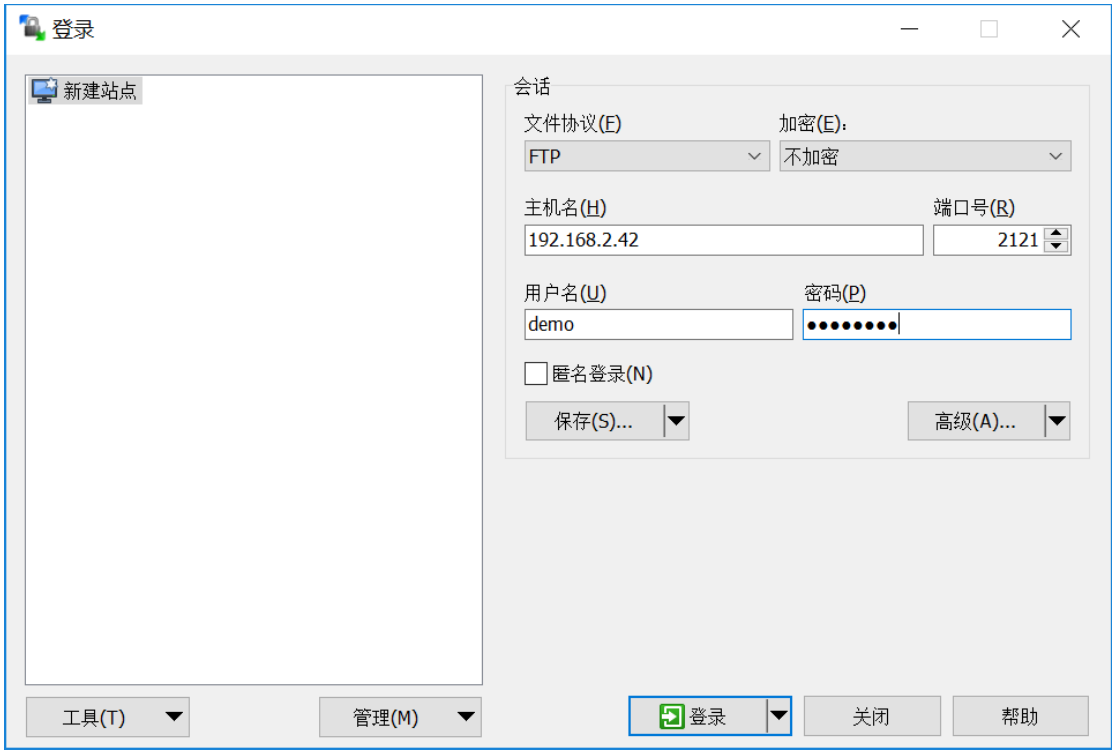
- 选择键：方向键上下进行选择，或者按前面序号对应的数字及字母，回车会确定；
- 0-5：选择主机组或主机；
- N：进入下一页；
- P：返回上一页；
- F：可根据 IP 主机进行查找；
- D：自主填写信息进行连接；
- E：退出菜单模式。

选择完主机、协议、账号后按[回车]即可进行连接，如图所示：



2.3.3. 文件传输 C₩S 菜单

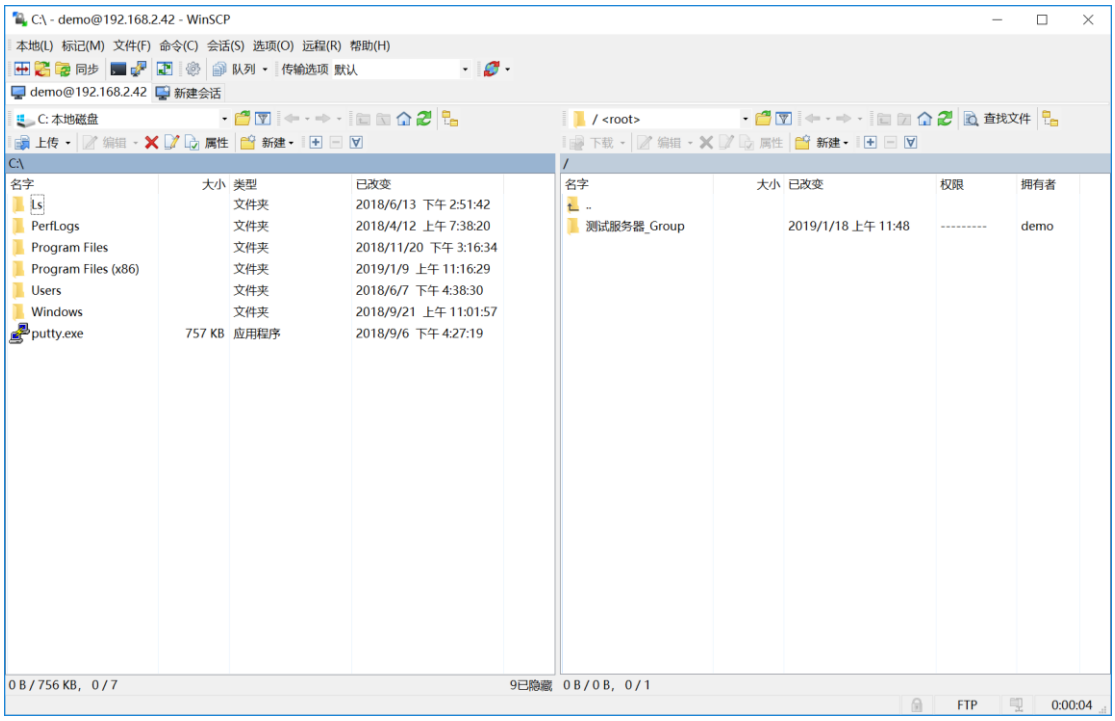
使用文件传输连接工具（如：FlashFXP、WinSCP、FileZilla、Yummy 等）连接堡垒机 C₩S 菜单模式可访问所有文件传输协议（如：FTP、SFTP），连接方式如下：



- 主机名：堡垒机 IP；

- 端口：2121；
- 用户名：堡垒机运维账号;
- 密码：运维账号密码。

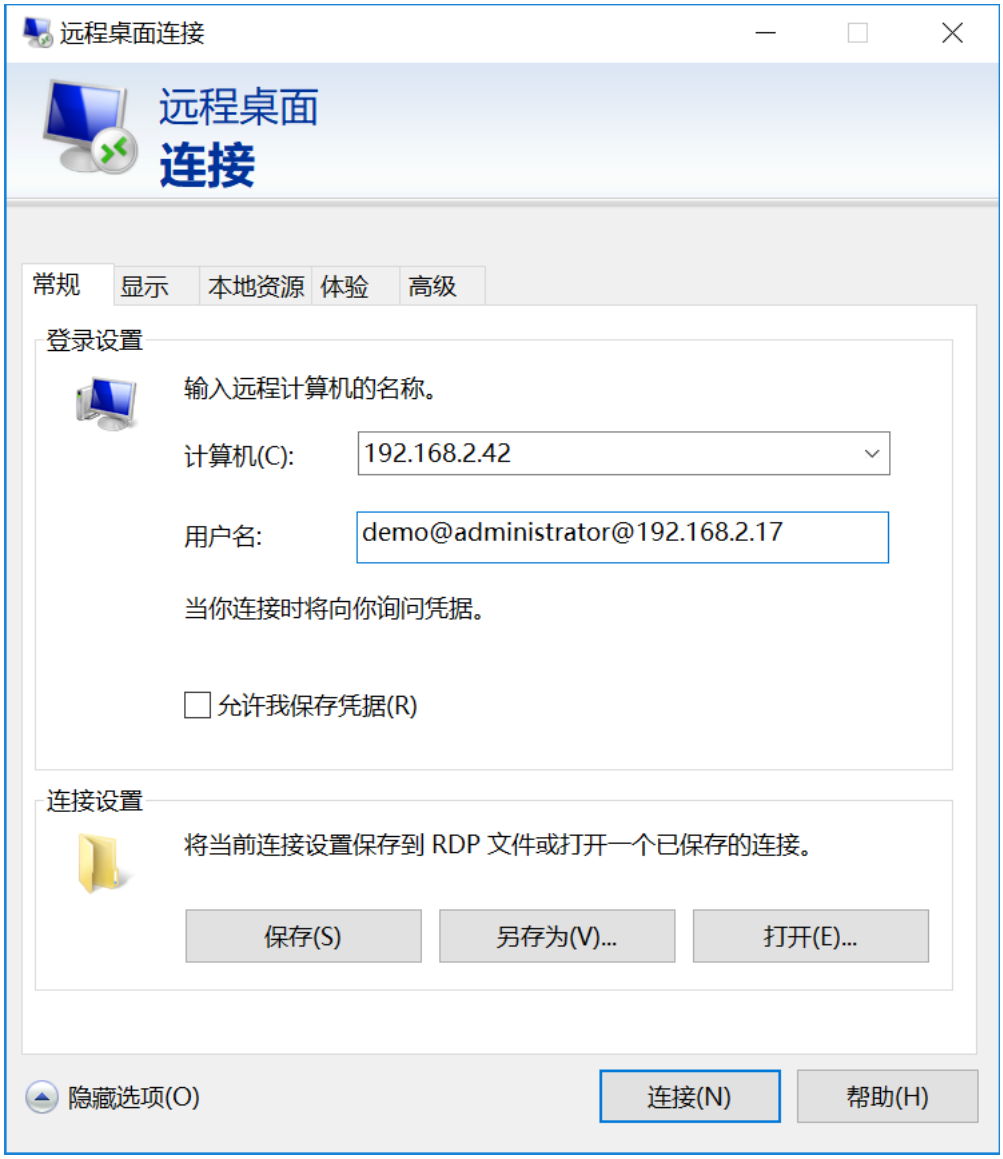
点击[连接]进入文件传输 C₩S 菜单选择界面，选择主机后即可进行连接，如图所示：



2.4. C₩S 直连访问

2.4.1.图形化 C₩S 直连

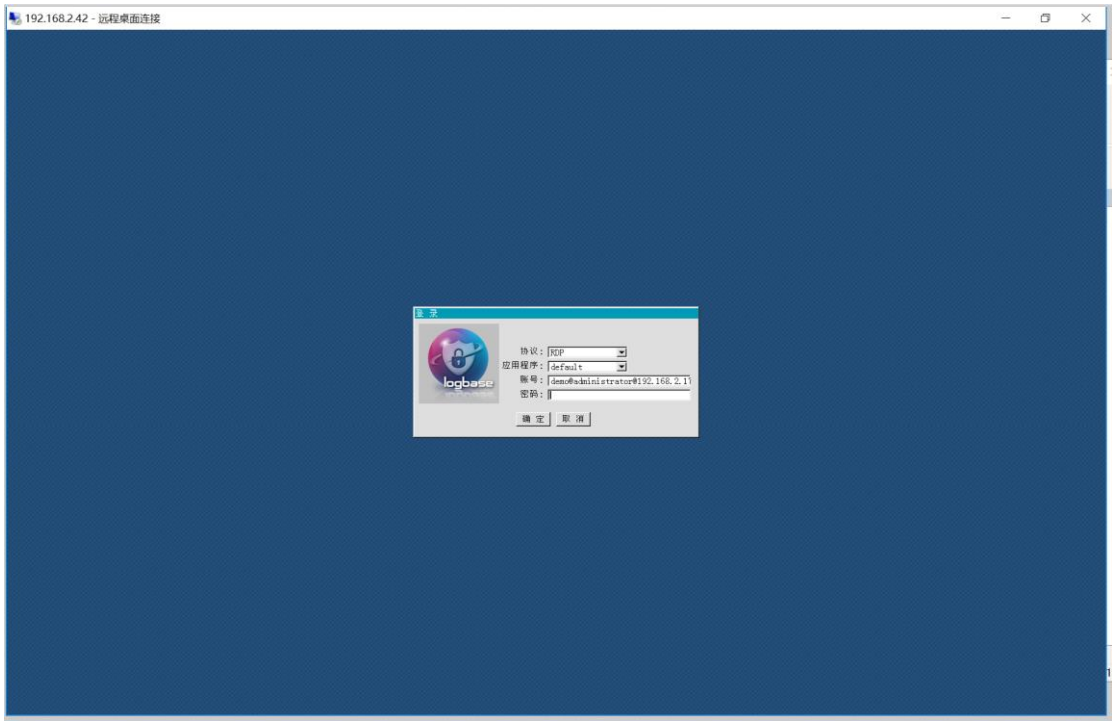
使用远程桌面连接工具（如：Mstsc、RDC、Deskto 等）通过 C₩S 直连模式可访问所有图形协议（如：RDP、VNC、X11、应用发布等），连接方式如下：



- 计算机：堡垒机 IP；
- 用户名：格式为**"堡垒机账号@主机账号@主机 IP"**或**"堡垒机账号@别名"**。

：别名配置详见本手册《9.2 别名管理》。

点击**[连接]**进入图形化 CWS 直连登录界面，如图所示：

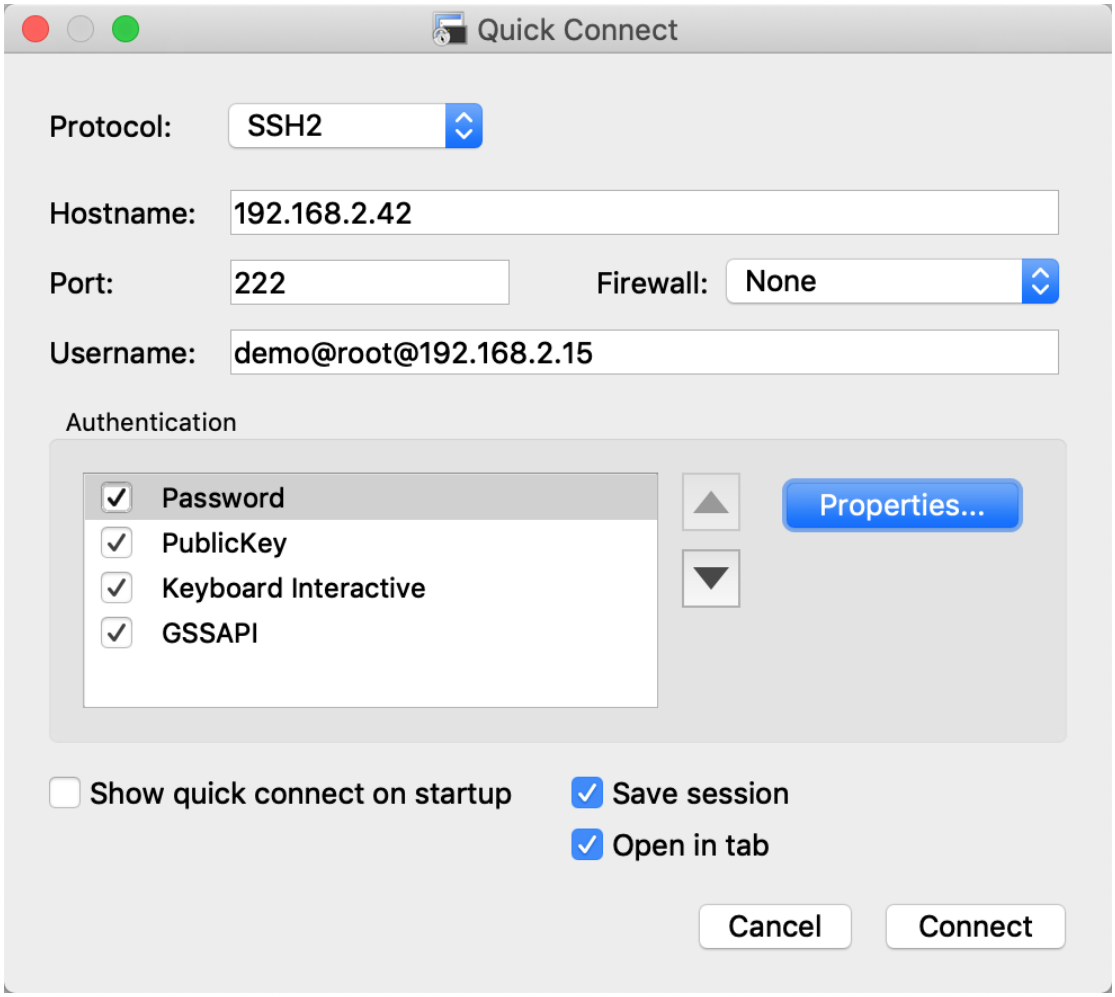


- 协议：选择要访问的协议；
- 应用程序：选择应用发布时所需的工具；
- 账号：格式为**"堡垒机账号@主机账号@主机 IP"**或**"堡垒机账号@别名"**；
- 密码：主机账号密码已托管时输入运维账号密码即可，主机账号密码为托管时**"运维账号密码+主机账号密码"**；

：假设运维账号密码为"12345678"，主机账号密码为"Abcd1234"，密码输入为"12345678Abcd1234"。

2.4.2. 字符型 C₩S 直连

使用字符型终端连接工具（如：SecureCRT、Xshell、Putty、Terminal for Mac、Terminal for Linux等）通过堡垒机 C₩S 直连模式可访问所有字符型协议（如：SSH、Telnet、Rlogin 等），连接方式如下：

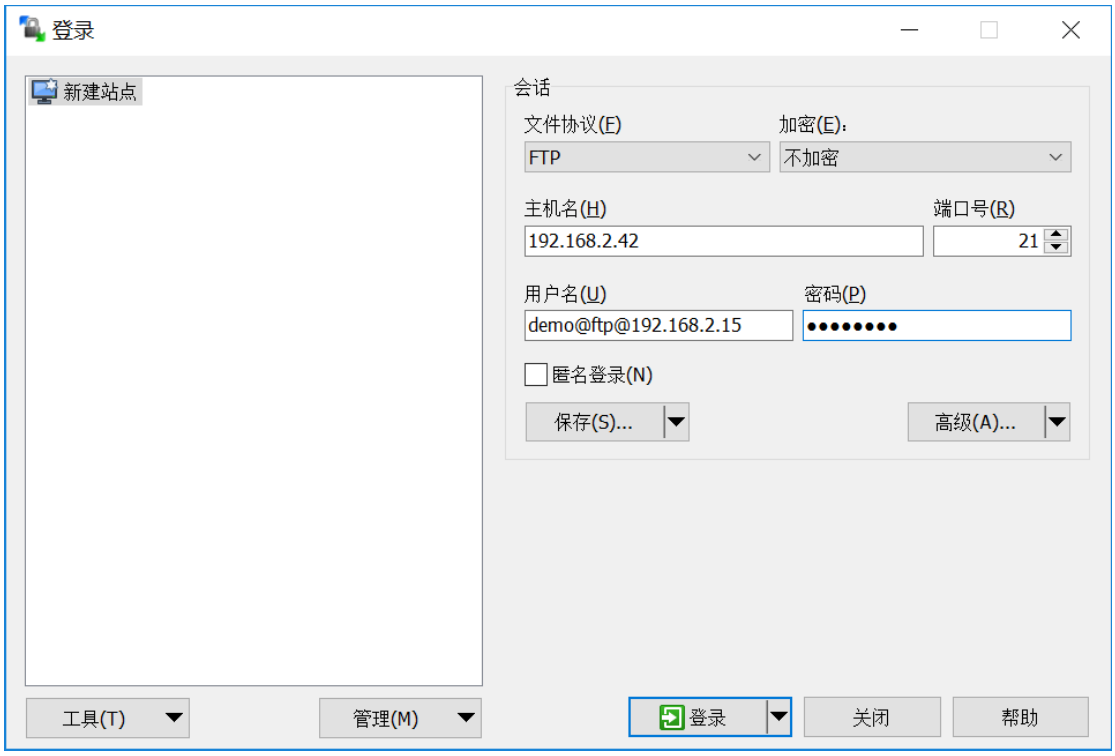


- 协议：选择访问协议；
- 主机名：堡垒机 IP；
- 端口：222；
- 用户名：格式为**"堡垒机账号@主机账号@主机 IP"**或**"堡垒机账号@别名"**;
- 密码：主机账号密码已托管时输入运维账号密码即可，主机账号密码为托管时**"运维账号密码+主机账号密码"** ；

：假设运维账号密码为"12345678"，主机账号密码为"Abcd1234"，密码输入为"12345678Abcd1234"。

2.4.3. 文件传输 C₩S 直连

使用文件传输连接工具（如：FlashFXP、WinSCP、FileZilla、Yummy 等）通过堡垒机 C₩S 直连模式可访问所有文件传输协议（如：FTP、SFTP），连接方式如下：

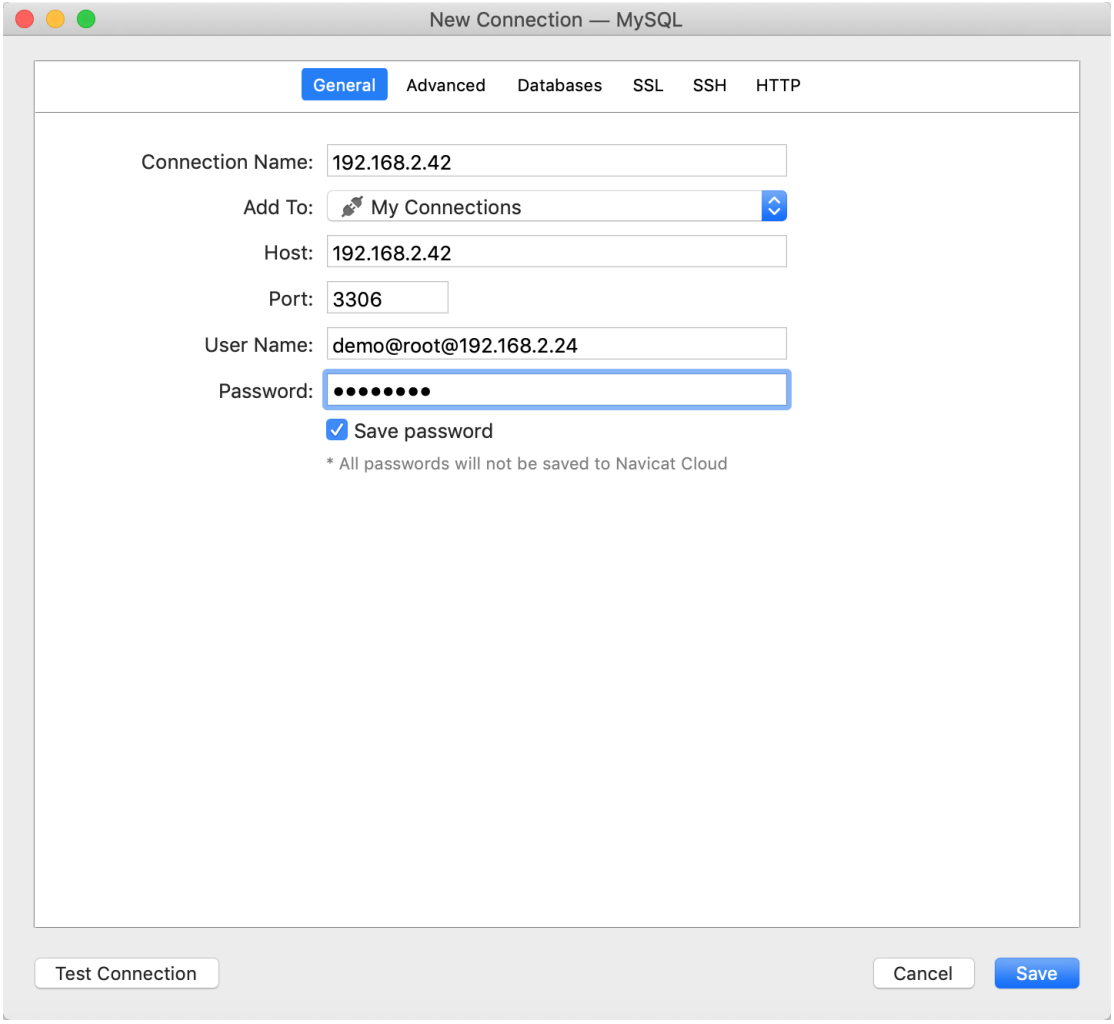


- 协议：选择访问协议；
- 主机名：堡垒机 IP；
- 端口：21；
- 用户名：格式为**"堡垒机账号@主机账号@主机 IP"**或**"堡垒机账号@别名"**；
- 密码：主机账号密码已托管时输入运维账号密码即可，主机账号密码为托管时**"运维账号密码+主机账号密码"**；

⚠：假设运维账号密码为"12345678"，主机账号密码为"Abcd1234"，密码输入为"12345678Abcd1234"。

2.4.4. 数据库 C₩S 直连

使用数据库终端连接工具（如：SQL Manager、Navicat、ISQLW、DBVisualizer等）通过堡垒机 C₩S 直连模式可访问 MSSql、MySql、DB2、Sybase，连接方式如下：



- 主机名：堡垒机 IP；
- 端口：与数据库端口相同：
  - MSSql 2000：1433
  - MSSql 2005：1533
  - MSSql 2008：1633
  - MySql：3306

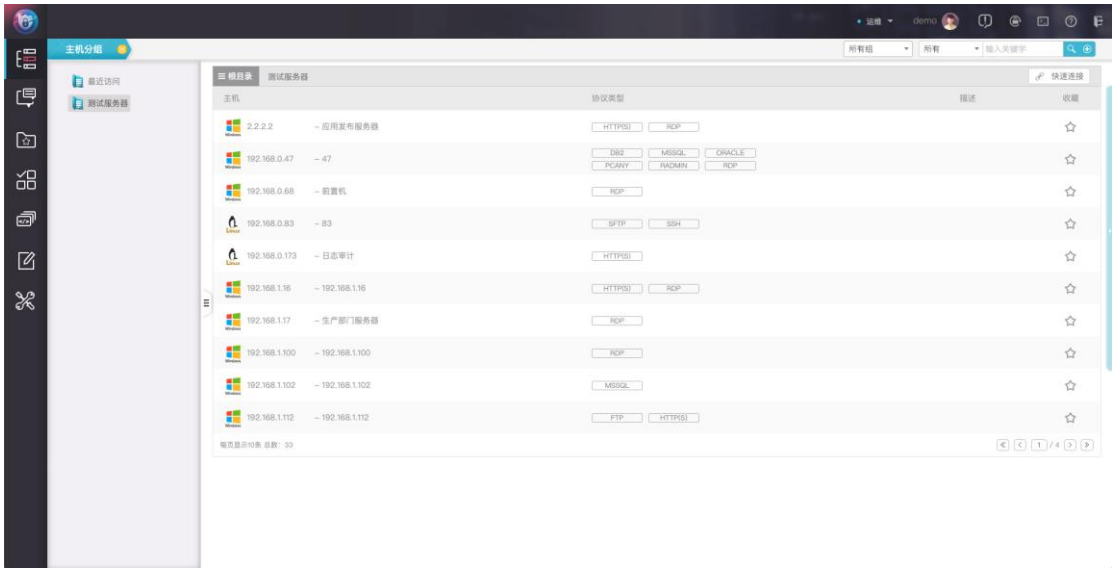
- DB2：50000
- MySql：3306

- 用户名：格式为**"堡垒机账号@主机账号@主机 IP"**或**"堡垒机账号@别名"**；
- 密码：主机账号密码已托管时输入运维账号密码即可，主机账号密码为托管时**"运维账号密码+主机账号密码"** ；

：假设运维账号密码为"12345678"，主机账号密码为"Abcd1234"，密码输入为"12345678Abcd1234"，Mysql**必须代填主机账号密码**。

3. 主机列表

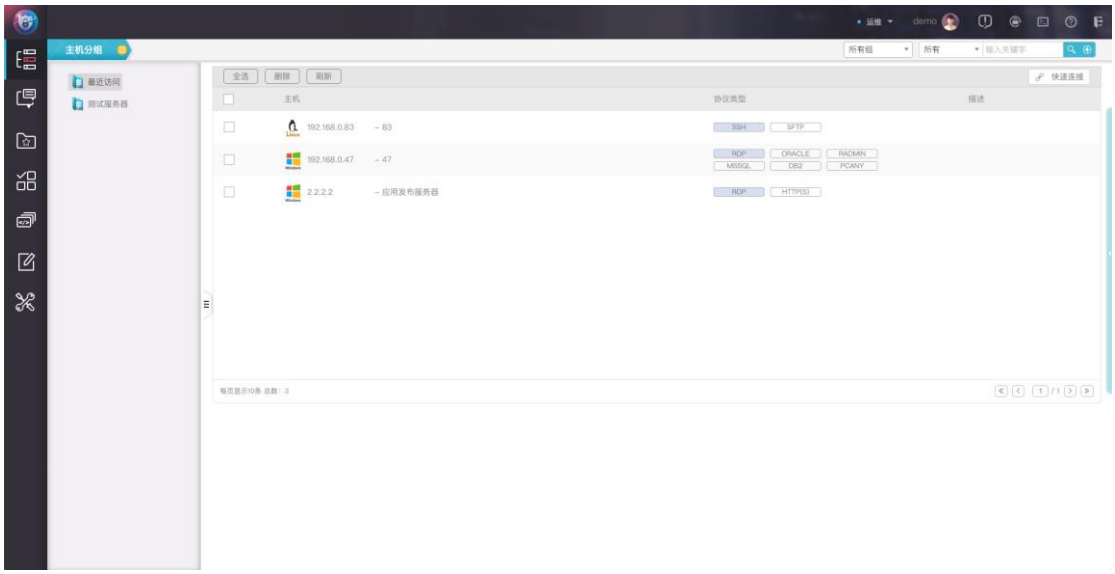
「主机列表」中显示所有当前可访问的主机，如图所示：



- 最近访问：显示最近访问过的主机列表；
- 快速连接：可直接填写配置主机 IP、协议、账号进行连接；
- 展开/收拢主机组：点击 可展开/收拢主机组列表；
- 添加收藏夹：点击☆可自定义添加收藏夹名称。

3.1. 最近访问

[最近访问]中显示最近访问过的主机列表，如图所示：



不同颜色标注的协议即为最近连接的协议；可点击浮层中的删除按钮将主机从[最近访问]中删除。

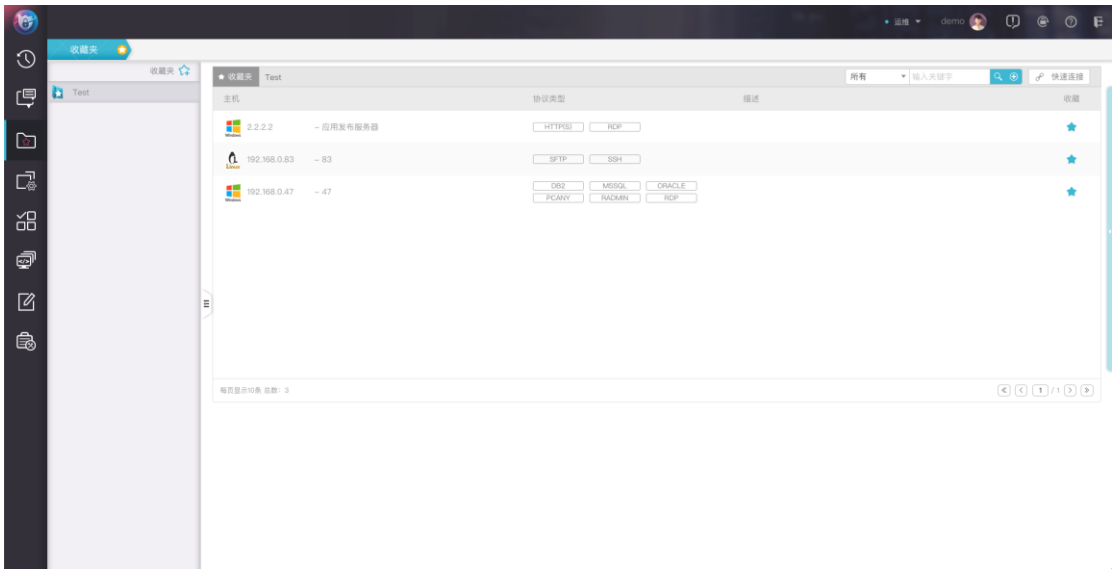
3.2. 快速连接

[快速连接]中可自行填写配置主机 IP、协议、账号进行连接，如图所示：

- 搜索：可自动搜索读取已配置账号的密码。

4. 收藏夹

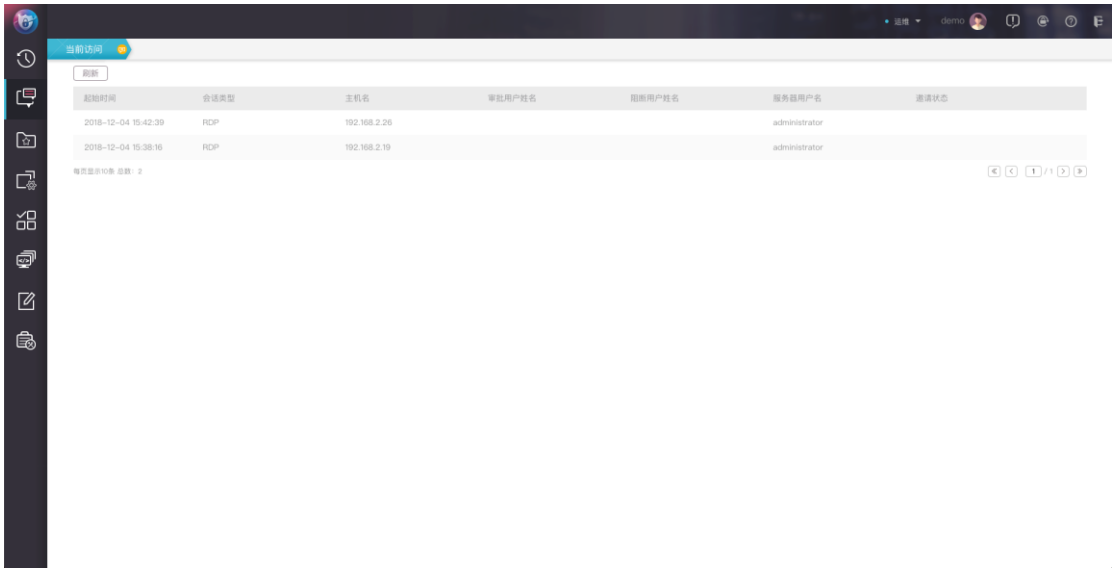
『**收藏夹**』中可添加自定义组，将常用主机添加至收藏夹组中，如图所示：



- 添加收藏夹：点击 可自定义添加收藏夹名称；
- 取消收藏：点击主机列表中的 可取消收藏。

5. 当前访问

『**最近访问**』中显示当前连接的主机，可邀请其他运维人员协同操作，如图所示：

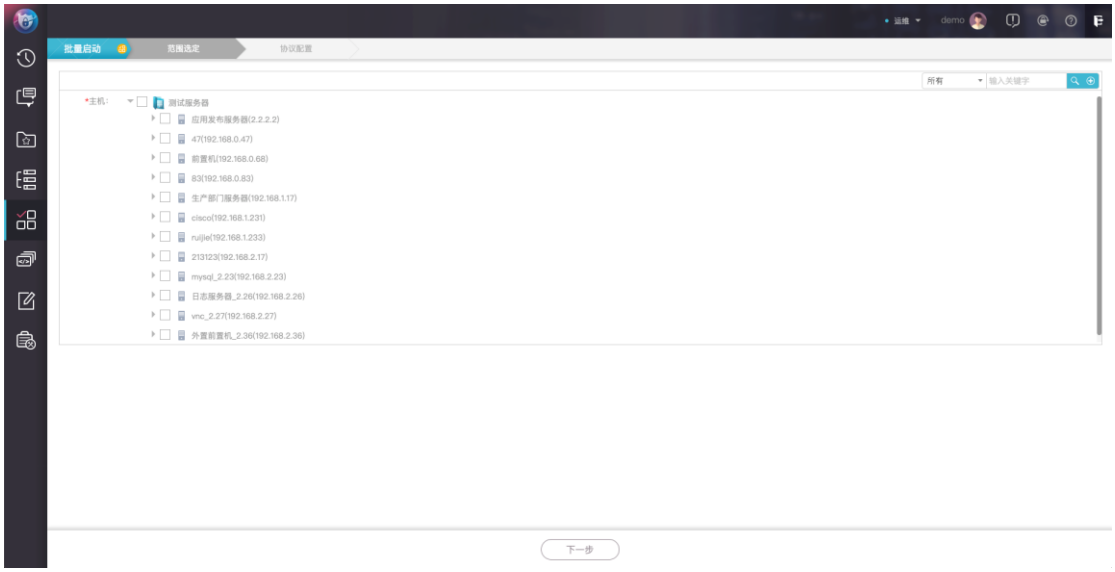


- 邀请：选择运维用户邀请其进行协同操作。

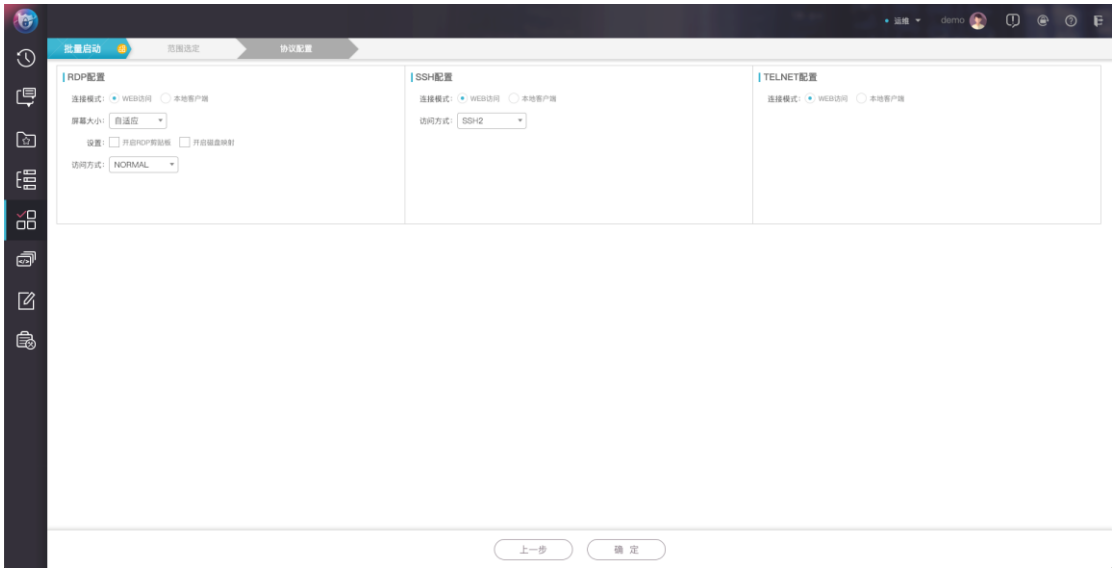
：协同邀请的消息在[消息中心]查看。

6. 批量启动

『批量启动』中可选择配置多台服务器批量启动，如图所示：



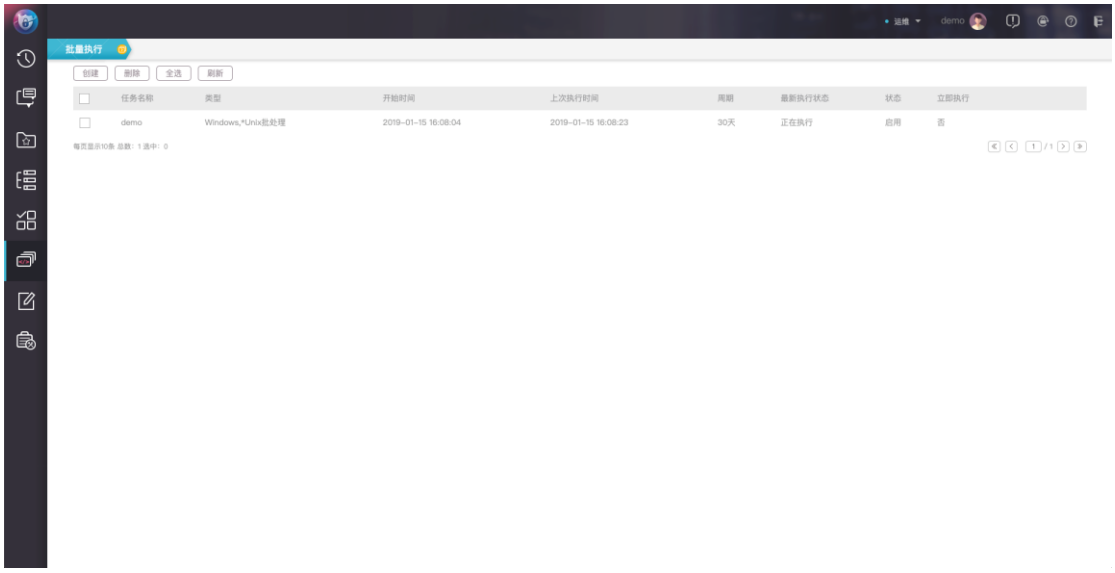
[范围选定]中选择需要批量启动的服务器，然后点击[下一步] ，如图所示：



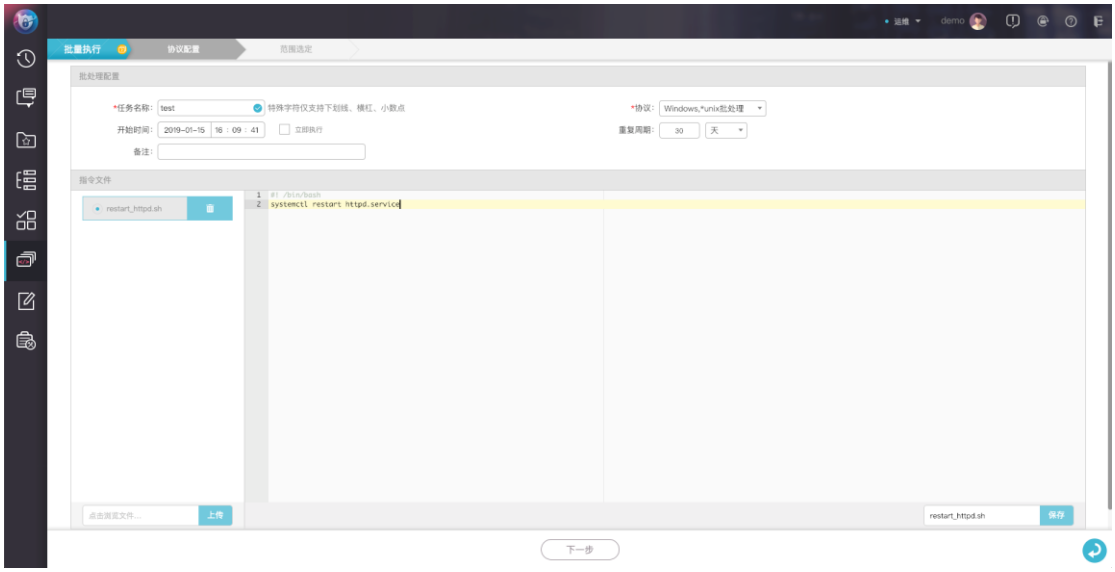
[协议配置]中可配置 RDP、SSH、TELNET 的连接模式和其他辅助功能，点击[确定]后堡垒机即会执行批量启动。

7. 批量执行

『批量执行』中可配置脚本周期性自动执行，如图所示：



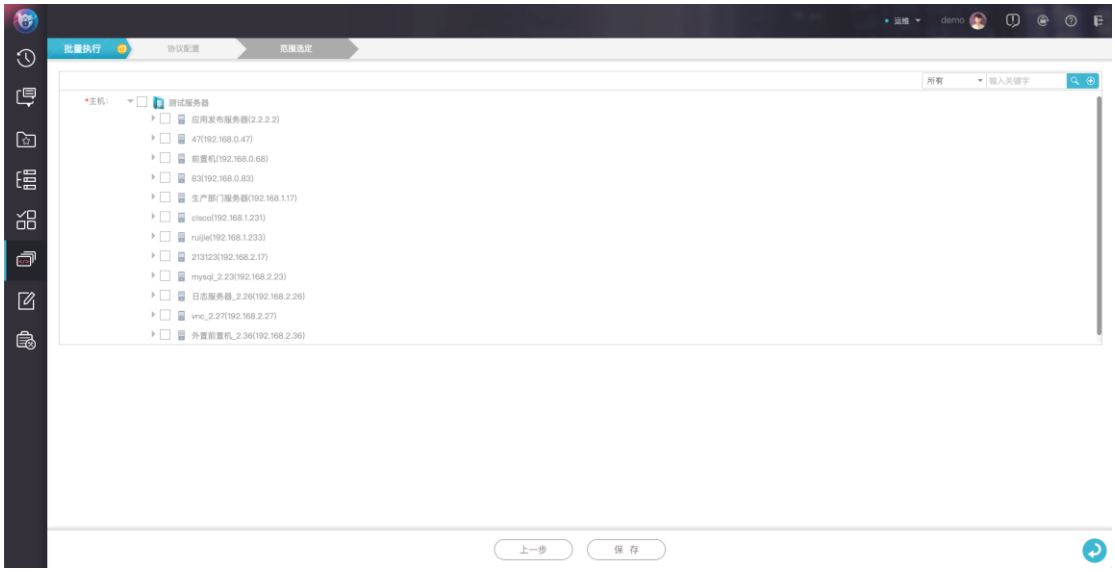
点击[创建]添加执行计划，如图所示：



- 任务名称：配置执行任务名称；
- 协议：支持 Windows、*UNIX、Mysql、Oracle 批处理；
- 开始时间：配置脚本第一次执行时间；
- 立即执行：立即执行该任务；
- 重复周期：根据分钟/天周期性执行；
- 备注：填写任务备注；
- 指令文件：选择执行的脚本文件，脚本文件可选择上传和在线编辑保存；

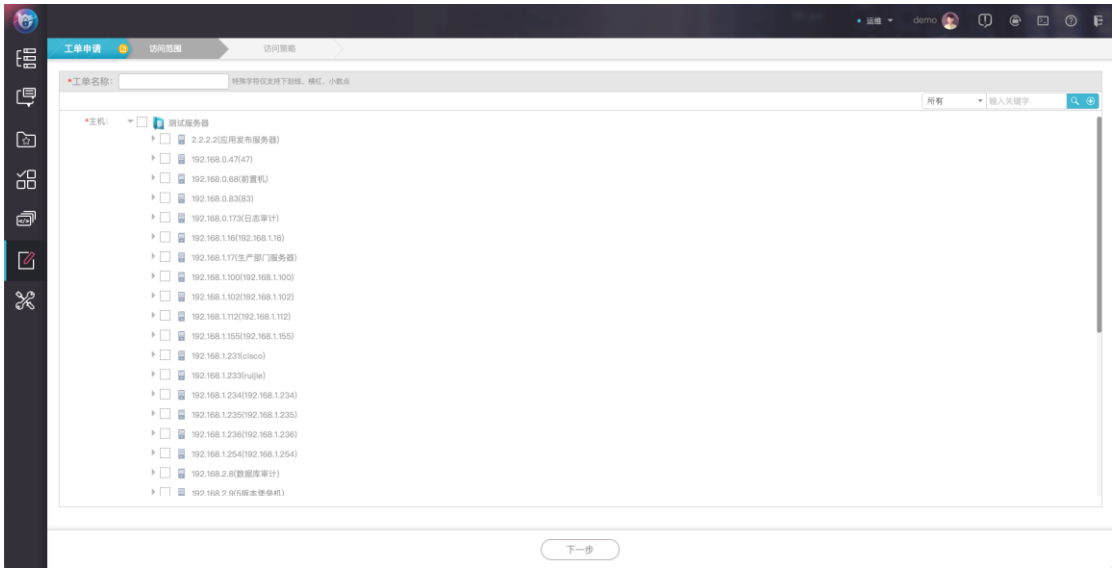
：指令文件必须为系统可直接执行的脚本文件！

配置完指令文件后点击[下一步]选择需要执行的主机，如图所示：

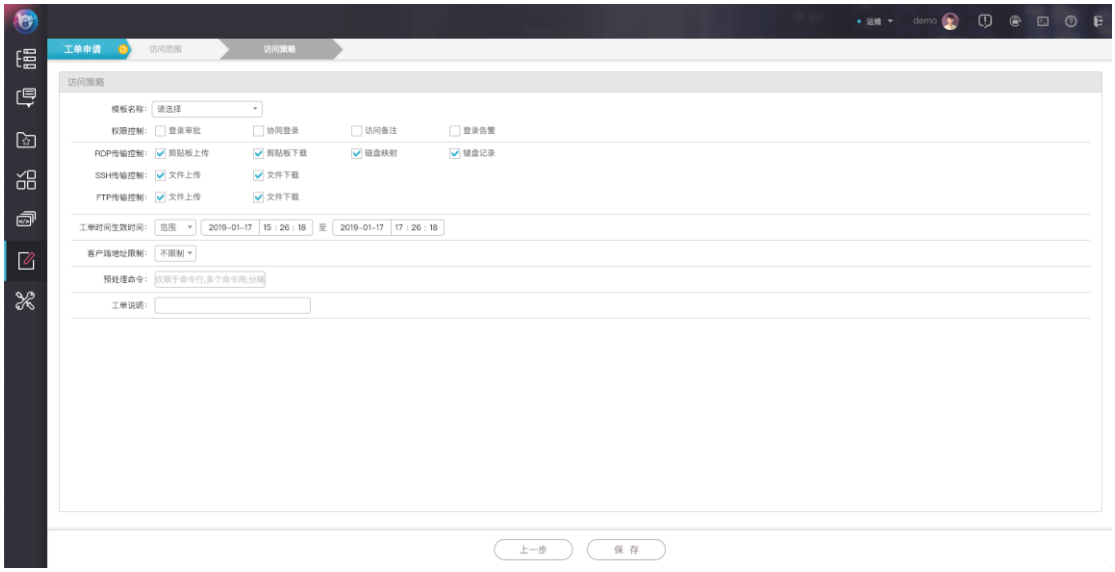


8. 工单申请

『**工单申请**』中可根据工单授权中的主机进行工单申请，如图所示：

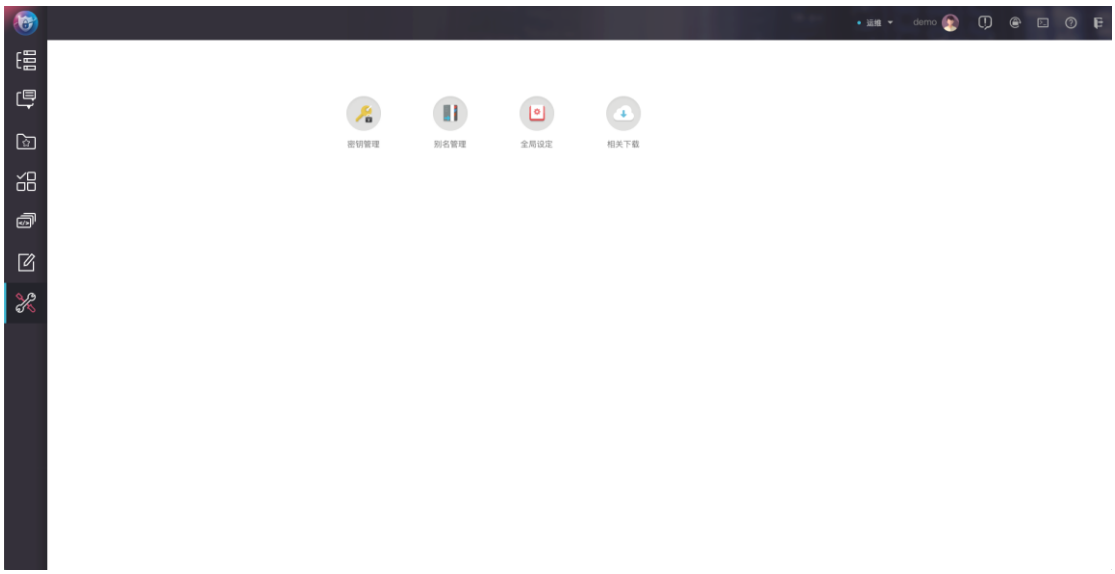


填写申请工单名称及选择访问的主机，然后点击下一步，选择工单访问时间及工单说明，如图所示：



9. 访问工具

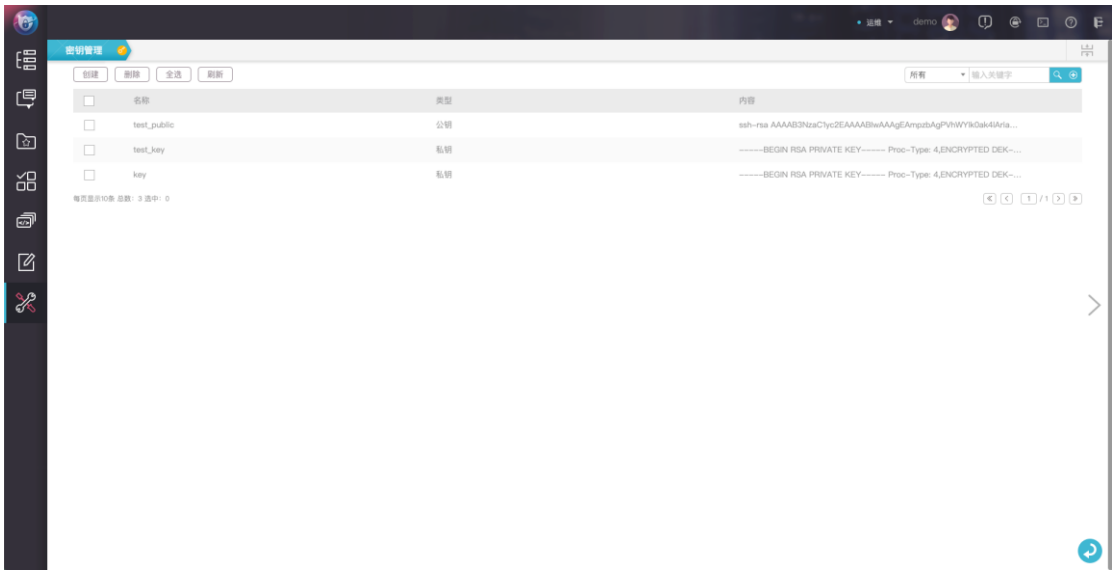
「访问工具」中可配置一些访问常用的配置信息，如图所示：



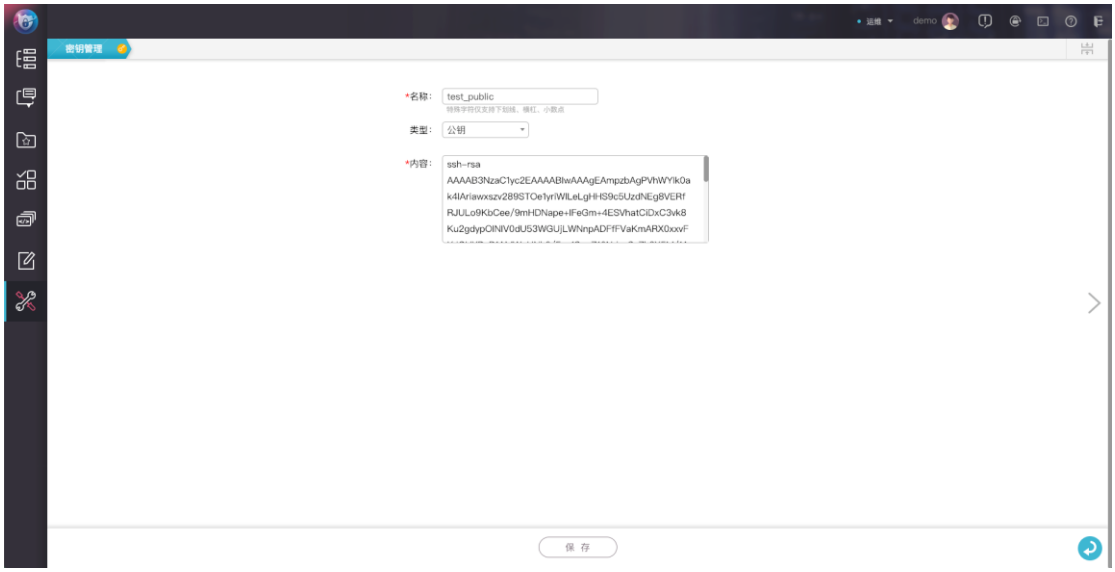
- 密钥管理：配置 SSH 密钥；
- 别名管理：配置主机与账号的别名；
- 全局设定：配置本地客户端的路径。

9.1. 密钥管理

[密钥管理]中可配置 SSH 密钥，如图所示：

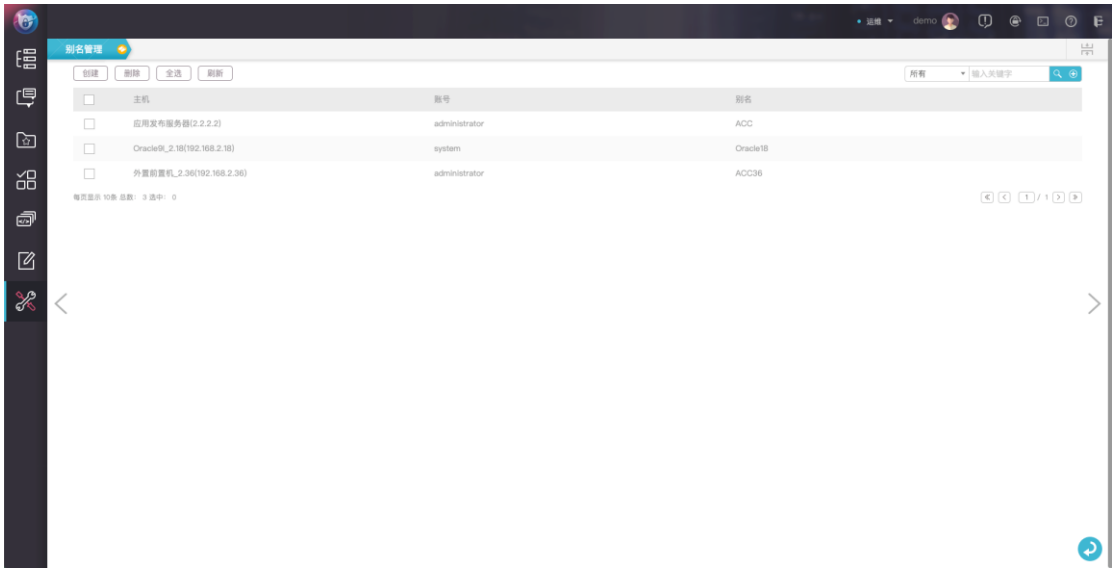


点击[创建]可添加 SSH 公钥或私钥，如图所示：

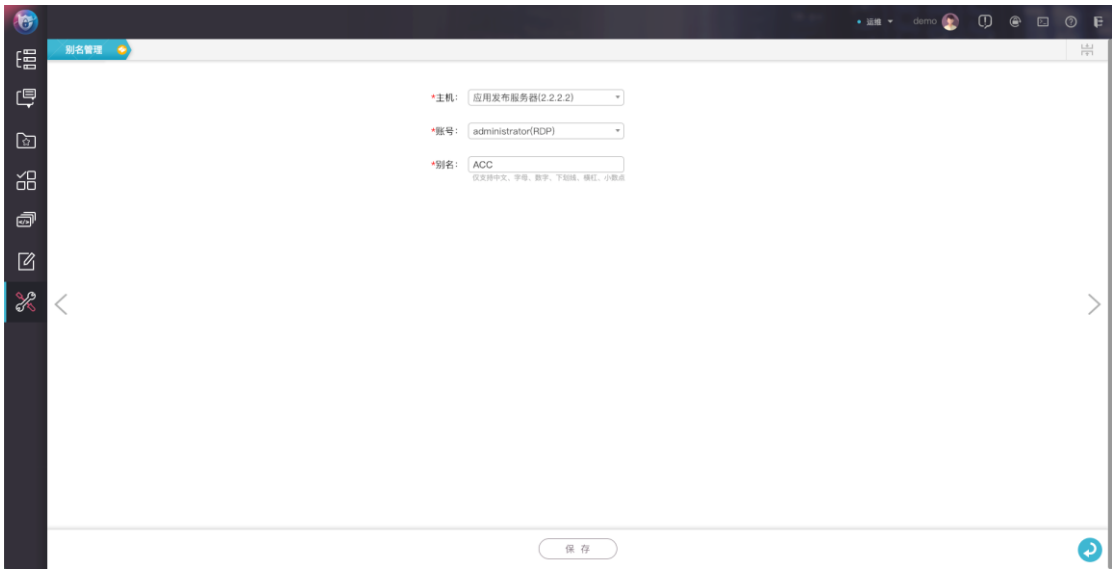


9.2. 别名管理

[别名管理]中可为主机与账号配置别名，如图所示：



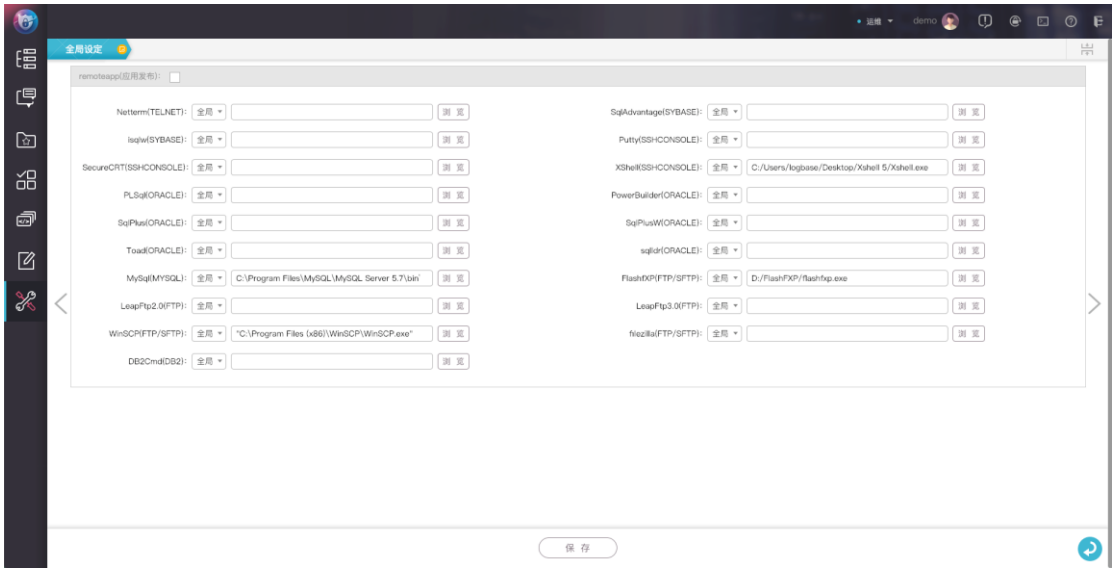
点击[创建]可为主机与账号配置别名，如图所示：



：别名的访问方式详见本手册《2.4 C₩S 直连访问》。

9.3. 全局设定

[全局设定]中可配置本地客户端路径与启用 RemoteAPP 方式，如图所示：


全局设定
remoteapp(应用发布):
Netterm(TELNET):
Isqlw(SYBASE):
SecureCRT(SSHCONSOLE):
PLSql(ORACLE):
SqlPlus(ORACLE):
Toad(ORACLE):
MySql(MYSQL):
C:\Program Files\MySQL\MySQL Server 5.7\bin
LeapFtp2.0(FTP):
WinSCP(FTP/SFTP):
"C:\Program Files (x86)\WinSCP\WinSCP.exe"
DB2Cmd(DB2):
SqlAdvantage(SYBASE):
Putty(SSHCONSOLE):
XShell(SSHCONSOLE):
C:/Users/logbase/Desktop/Xshell 5/Xshell.exe
PowerBuilder(ORACLE):
SqlPlusW(ORACLE):
sqlldr(ORACLE):
FlashFXP(FTP/SFTP):
D:/FlashFXP/flashfxp.exe
LeapFtp3.0(FTP):
filezilla(FTP/SFTP):
全局
浏 览
保 存