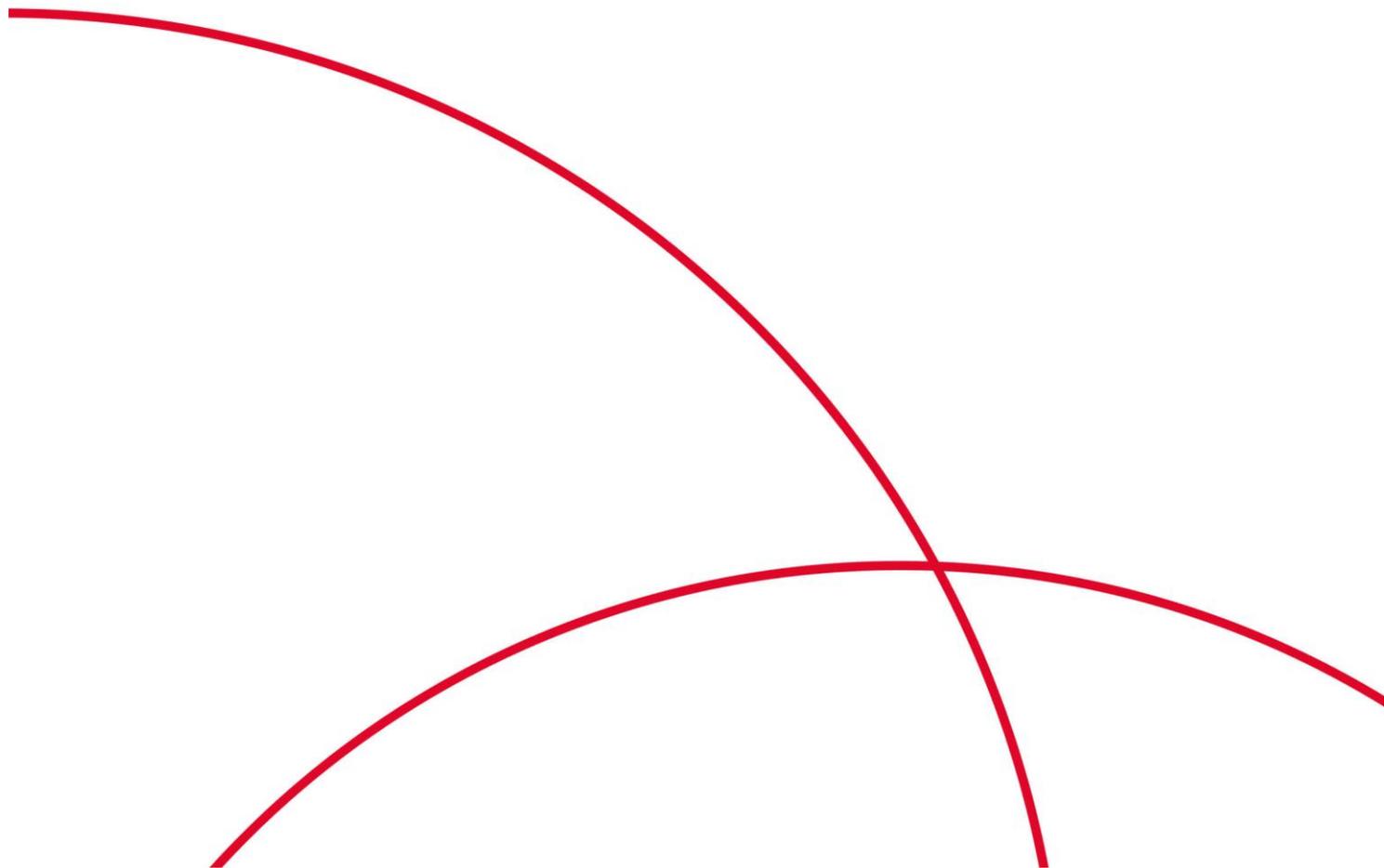


天翼云·云堡垒机

用户使用指南

天翼云科技有限公司



目录

1	概述	1
2	系统登录	1
2.1	系统登录	1
2.2	环境配置	2
3	运维说明	8
3.1	RDP/VNC 访问	8
3.2	Telnet/SSH 访问	9
3.3	FTP 访问	11
3.4	数据库访问	13
3.5	WEB 访问	15
3.6	X11-XDMCP 访问	16
3.7	HTML5 运维	17
3.8	批量登录	18
3.9	运维工单	20
3.9.1	工单申请	20
3.9.2	工单运维	20
3.10	命令自动执行	21
3.11	网络设备配置备份	22
3.12	菜单模式	24
3.12.1	命令行方式	25
3.12.2	图形方式	29

1 概述

本手册详细介绍了云堡垒机进行运维操作过程的使用方法。用户可参考本手册，通过云堡垒机进行各种运维操作。

2 系统登录

2.1 系统登录

用户通过浏览器访问云堡垒机，登录 URL 地址默认为：<https://云堡垒机的 IP 地址>。首先选择正确的认证方式（默认为内置本地认证），然后输入帐号和密码，点击“登录”，认证成功后进入运维界面。

注意：推荐使用以下浏览器：IE10 及以上版本浏览器、谷歌浏览器和火狐浏览器；



图 2.1.1 系统登录界面



图 2.1.2 运维界面

2.2 环境配置

用户在使用云堡垒机对资源进行运维之前，需要安装证书和基础控件。（安装 C/S 客户端无需再安装基础控件和监控回放）。

用户在“相关下载”界面进行下载，“相关下载”可通过系统登录界面和系统首页进入。



图 2.3 登录界面-相关下载



图 2.4 运维界面-相关下载

相关下载

基础控件 (运维、管理基础控件, 堡垒机用户必须安装)

下载

监控回放 (运维监控、审计回放必备组件, 审计用户请安装)

下载

证书下载 (浏览器安全证书, 请安装到“受信任的根证书颁发机构”)

下载

C/S客户端 (堡垒机专用客户端, 通过C/S模式进行运维和管理, 无需再安装基础控件和监控回放)

下载

用户手册 (堡垒机基础管理、运维手册)

下载

图 2.5 证书和基础控件下载

操作步骤

步骤 1 安装证书

1. 在相关下载中下载证书。

相关下载

基础控件 (运维、管理基础控件, 堡垒机用户必须安装)

下载

监控回放 (运维监控、审计回放必备组件, 审计用户请安装)

下载

证书下载 (浏览器安全证书, 请安装到“受信任的根证书颁发机构”)

下载

C/S客户端 (堡垒机专用客户端, 通过C/S模式进行运维和管理, 无需再安装基础控件和监控回放)

下载

用户手册 (堡垒机基础管理、运维手册)

图 2.6 下载证书

2. 解压文件。



图 2.7 解压文件

3. 参考证书使用说明进行安装。



图 2.8 安装证书

步骤 2 安装基础控件

1. 双击基础控件安装包。



图 2.9 基础控件安装包

2. 选择语言（默认选择中文）。



图 2.10 安装基础控件（一）

3. 点击“安装”。

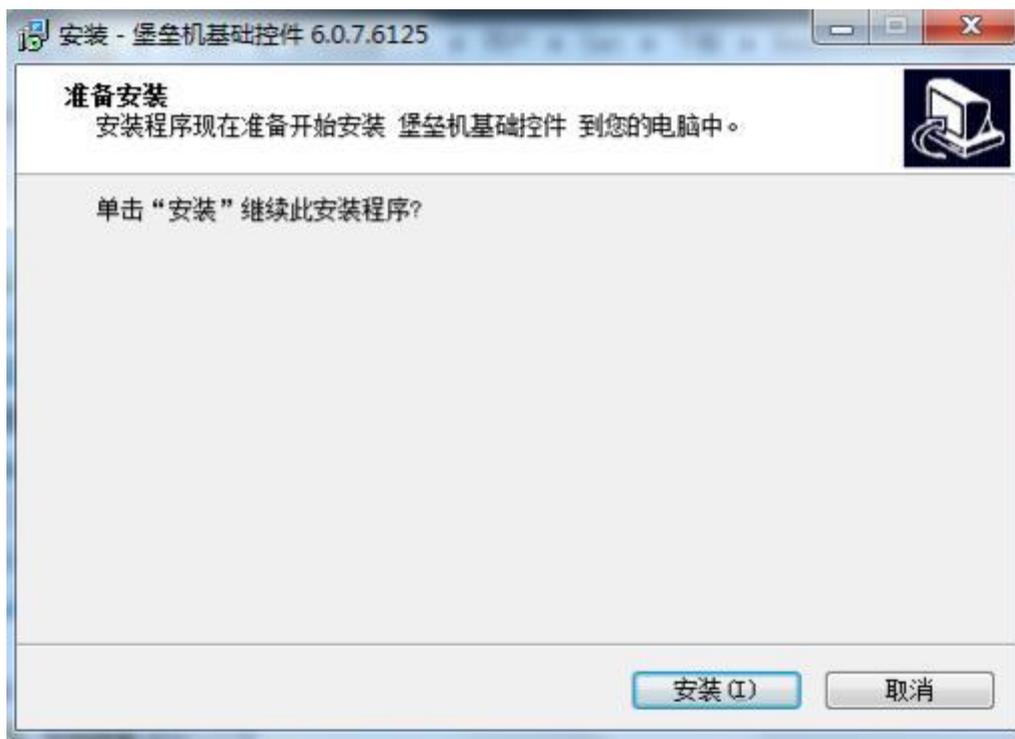


图 2.11 安装基础控件（二）

4. 完成安装。



图 2.12 安装基础控件（三）

步骤 3 配置运维工具路径

1. 在基础控件安装完成时，勾选“运行堡垒机工具路径配置”。



图 2.13 运行工具路径配置（一）

- 在“工具路径配置”界面，单击对应工具名称后的“更改”进行工具路径配置。



图 2.14 运行工具路径配置（二）

- 也在“工具路径配置”界面，单击“自动检测”按钮使工具自动发现已安装在本地终端上的运维工具路径。

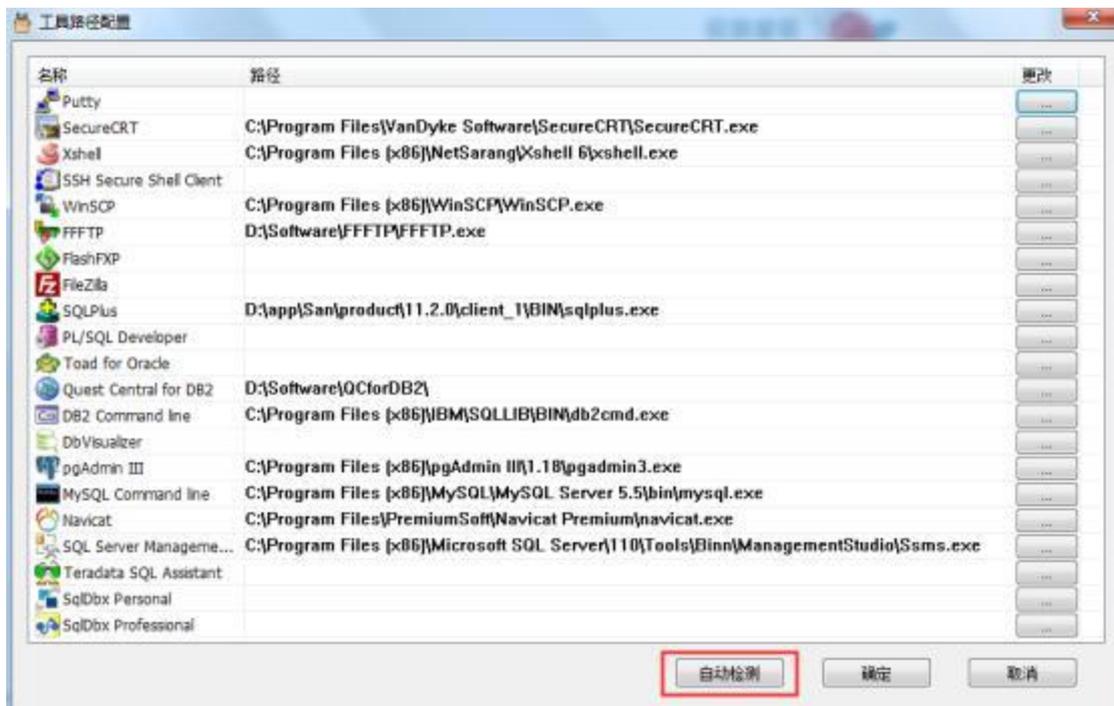


图 2.15 运行工具路径配置（三）

3 运维说明

3.1 RDP/VNC 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录云堡垒机控制台，选择“设备运维”。



图 3.1.1 设备运维

步骤 2 选择登录配置

选择需要运维的 RDP 或 VNC 资源。



图 3.1.2 图形协议运维

根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具、屏幕大小、访问方式等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速

登录)。



图 3.1.3 图形协议运维-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。



图 3.1.4 图形协议运维-立即登录

3.2 Telnet/SSH 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录云堡垒机控制台，选择“设备运维”。



图 3.2.1 设备运维

步骤 2 选择登录配置

选择需要运维的 SSH 或 TELNET 资源。



图 3.2.2 字符协议运维

根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



图 3.2.3 字符协议运维-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。



图 3.2.4 字符协议运维-立即登录

3.3 FTP 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录云堡垒机控制台，选择“设备运维”。



图 3.3.1 设备运维

步骤 2 选择登录配置

选择需要运维的 FTP 资源。



图 3.3.2 文件传输协议运维

根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。

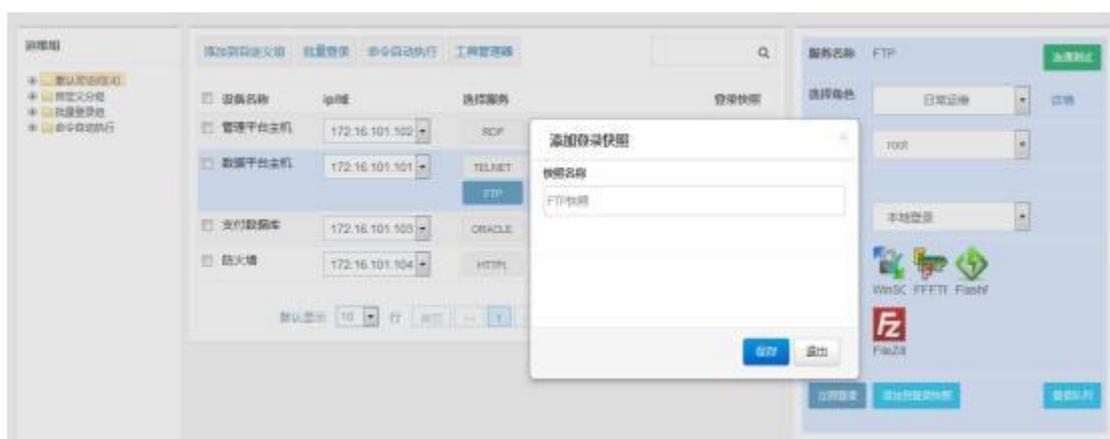


图 3.3.3 文件传输协议运维-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。



图 3.3.4 文件传输协议运维-立即登录

3.4 数据库访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录云堡垒机控制台，选择“设备运维”。



图 3.4.1 设备运维

步骤 2 选择登录配置

选择需要运维的数据库资源。



图 3.4.2 数据库协议运维

根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。

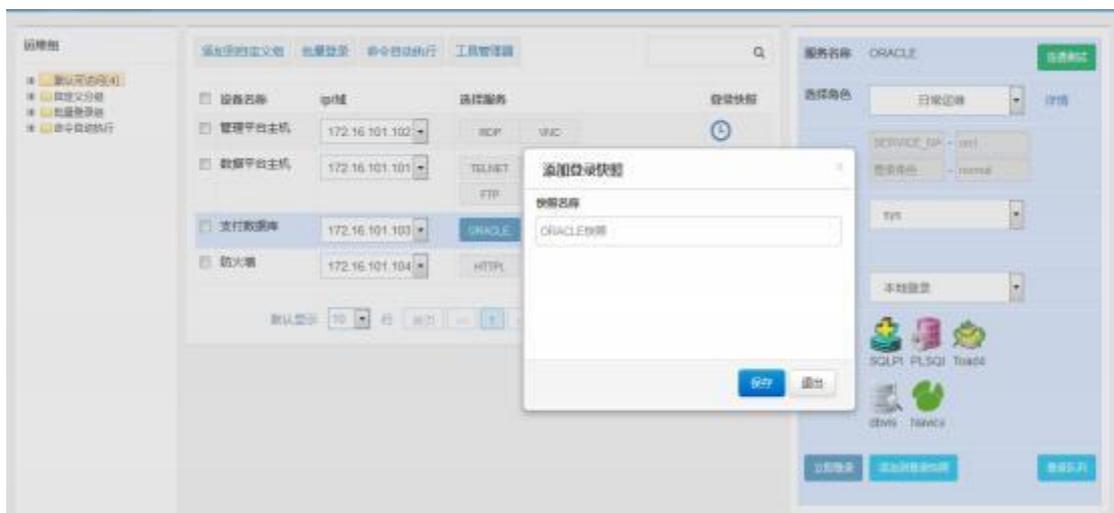


图 3.4.3 数据库协议运维-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。



图 3.4.4 数据库协议运维-立即登录

3.5 WEB 访问

除了字符协议、图形协议、文件协议以及数据库协议以外，较为常见的运维场景还有通过浏览器访问业务系统，本次演示通过应用发布浏览器程序进行 web 业务系统的运维操作。

操作步骤

步骤 1 进入设备运维页面

运维用户登录云堡垒机控制台，选择“设备运维”。



图 3.5.1 设备运维

步骤 2 选择登录配置

选择需要运维的资源。



图 3.5.2 WEB 访问

根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。

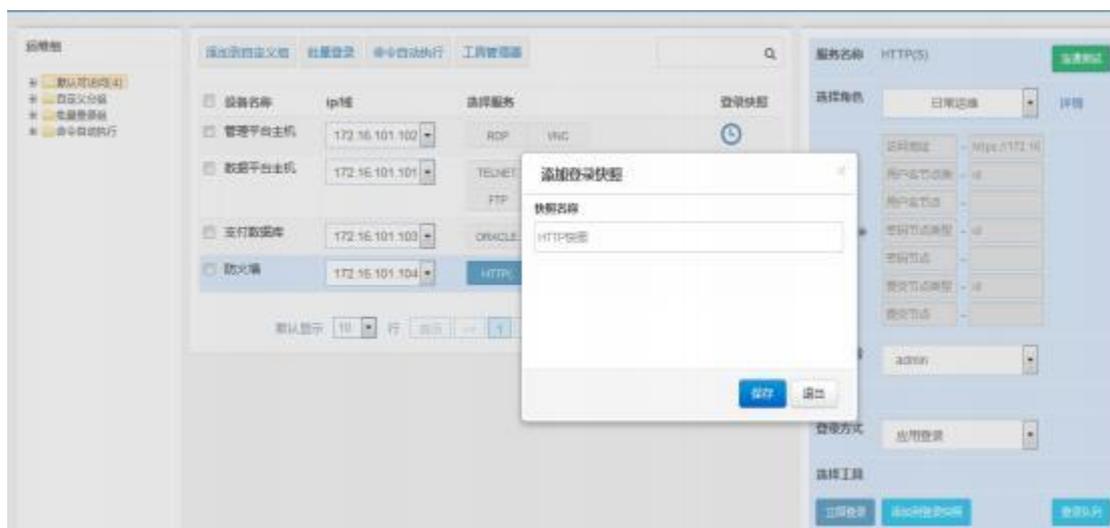


图 3.5.3 WEB 访问-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。

3.6 X11-XDMCP 访问

通过运维用户登录运维操作界面，选择对应资源的 X11-XDMCP 服务进行连接，如图 3.6.1 所示。**注意：X11-XDMCP 服务暂时不支持资源登录帐号和密码的代填功能。**



图 3.6.1 X11-XDMCP 访问

3.7 HTML5 运维

运维操作界面，登录方式选择 HTML5，然后选择立即登陆。如图 3.7.1 所示：

注意事项：

- (1) 使用 HTML5 运维时，推荐使用火狐浏览器和谷歌浏览器版本。
- (2) HTML5 运维支持 RDP/SSH/TELNET/VNC 服务。
- (3) SSH 支持文件上传、下载，TELNET、RDP、VNC 暂不支持文件上传、下载。



图 3.7.1 HTML5 运维登陆

如果第一次连接资源失败，请重新连接一次。如图 3.7.2 所示：



图 3.7.2 HTML5 运维

上传文件操作：选择资源上对应的目录，然后点击鼠标右键，选择上传文件。如图 3.7.3 所示：



图 3.7.3 HTML5 运维文件上传

3.8 批量登录

运维人员可以根据实际需求设置资源批量登录。

操作步骤

步骤 1 添加批量登录组

运维用户根据实际需求添加批量登录组。

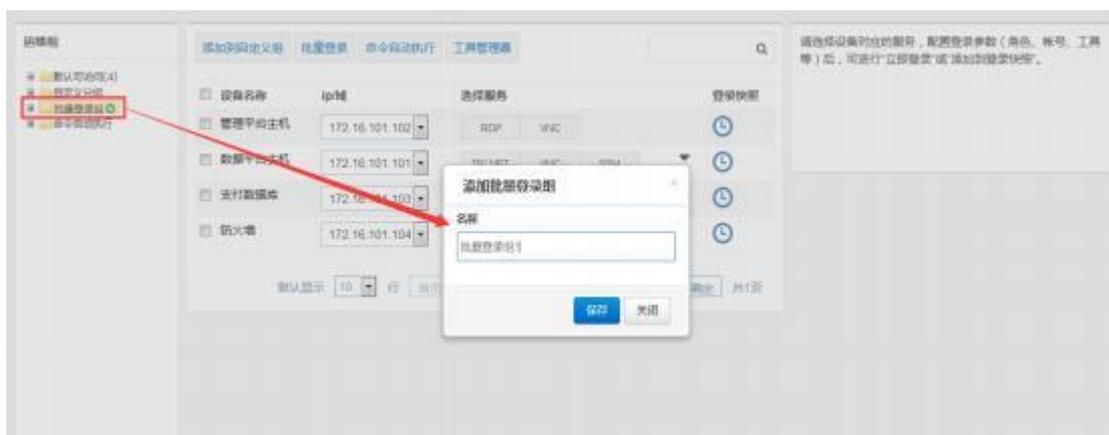


图 3.8.1 批量登录（一）

步骤 2 添加登录快照到批量登录组

运维人员需要设置登录快照，再将登录快照添加到批量登录组。

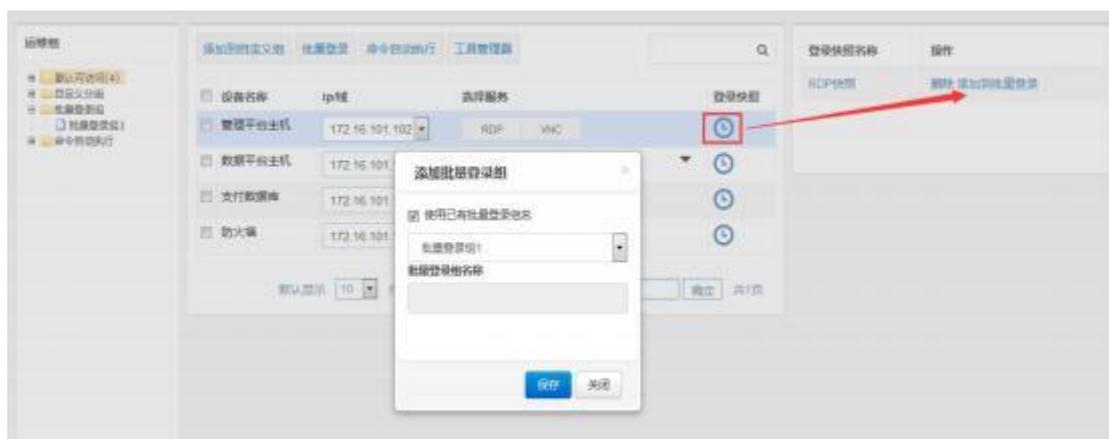


图 3.8.2 批量登录（二）

步骤 3 进行批量登录

单击批量登录组，选择需要批量登录的资源，单击“选中批量登录”或“全部批量登录”。



图 3.8.3 批量登录（三）

3.9 运维工单

3.9.1 工单申请

当用户需要临时访问默认运维权限之外的资源时，可通过“工单”向管理员提交申请，管理员审批通过后即具有相应的运维权限。



图 3.9.1 工单申请

3.9.2 工单运维

当用户申请的工单经管理员审批通过后或者管理员为运维用户下发了工单，用户可进入“工单”界面，选择工单中的资源进行运维。

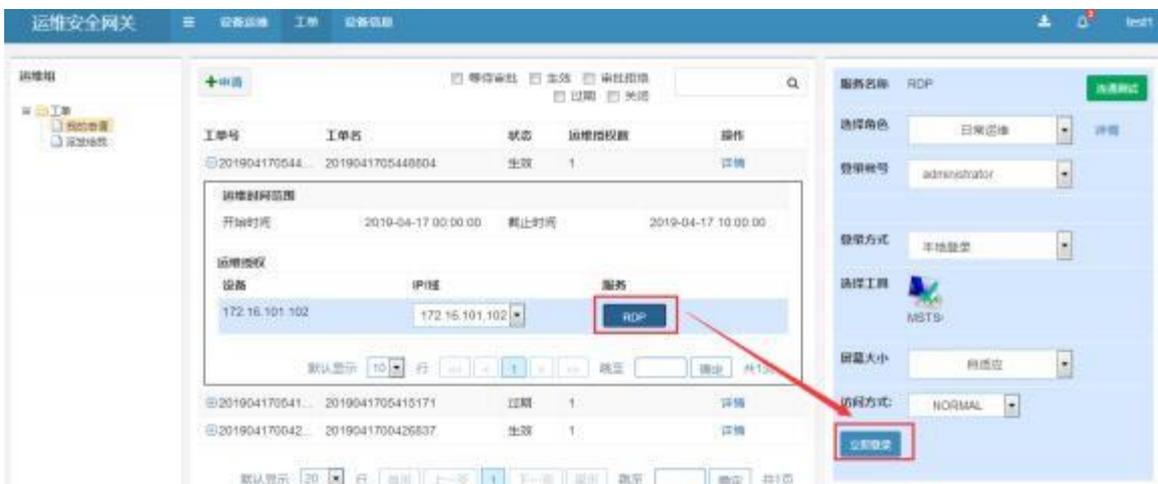


图 3.9.2 工单资源运维

3.10 命令自动执行

运维用户可对单台或多台资源设置命令执行任务，并以文件的形式获取到命令执行结果。

在运维操作界面，先勾选需要自动执行命令的主机，再选择“命令自动执行”，如下图所示。



图 3.10.1 命令自动执行-选择资源

在创建命令自动执行分组界面，设置分组名称、执行频率（立即、周期、定时）、命令详情。选择保存后，堡垒机会根据设置的执行频率登录对应主机上自动执行设置的命令。

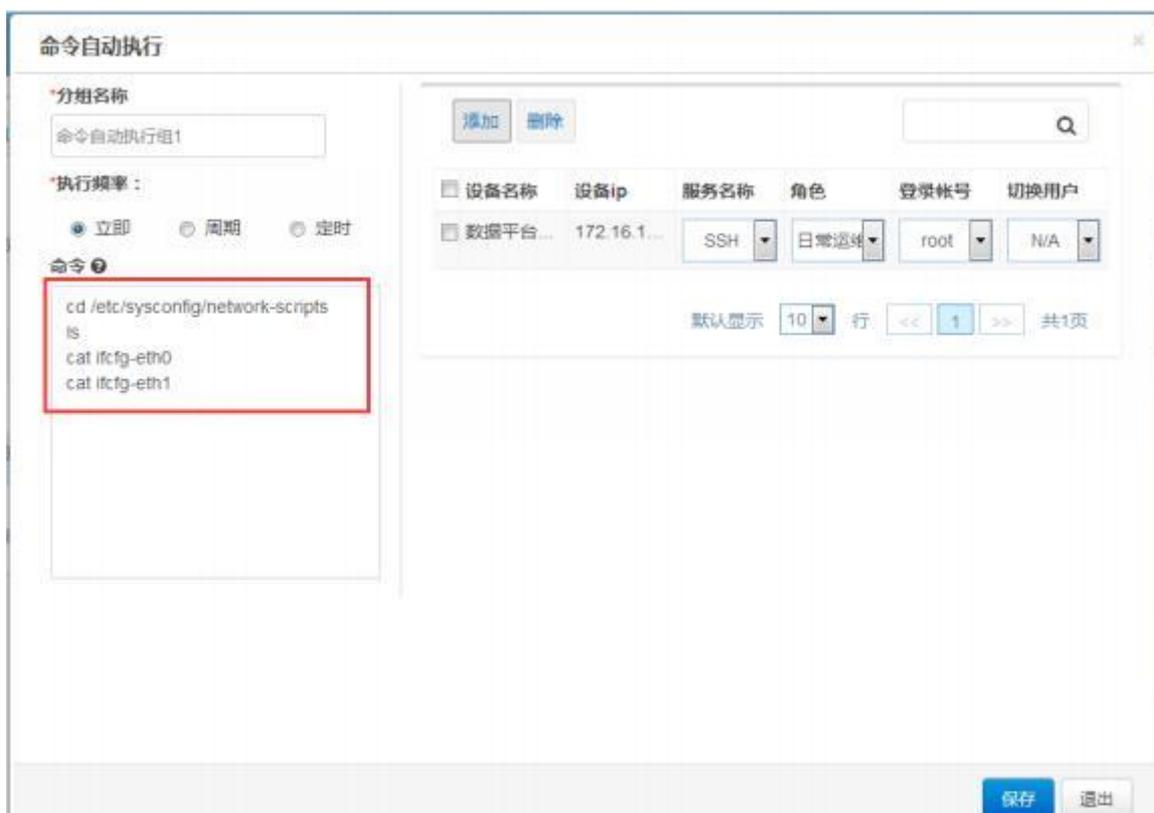


图 3.10.2 命令自动执行-设置详情

待设置的命令自动执行完成后，可选择命令自动执行分组中对应的资源，查看执行结果，并将执行结果文件下载到本地计算机。



图 3.10.3 命令自动执行-执行结果

3.11 网络设备配置备份

运维用户可对网络设备（交换机、路由器）的配置实现定期自动备份，并可下载到本地保存。

默认能支持网络设备类型包括华为、华为 3COM 和思科。

功能模块	厂商	型号	功能版本号	来源
华为_default_SSH_1.0.3	华为	default	1.0.3	内置
华为_default_TELNET_1.0.3	华为	default	1.0.3	内置
华为3COM_default_SSH_1.0.3	华为3COM	default	1.0.3	内置
华为3COM_default_TELNET_1.0.3	华为3COM	default	1.0.3	内置
思科_default_SSH_1.0.3	思科	default	1.0.3	内置
思科_default_TELNET_1.0.3	思科	default	1.0.3	内置

图 3.11.1 网络设备配置备份-功能模块

在运维操作界面，选择“设备信息”。如下图所示：



图 3.11.2 进入网络设备配置备份

在网络设备配置备份界面，先勾选需要备份配置的资源，再选择“添加分组”，设置分组名称、执行频率，打开对应资源的设置选项设置“连接参数”。如下图：



图 3.11.3 进入网络设备配置备份

在资源的连接参数中设置详细的信息。注意登录帐号的权限是否具备查询备份配置，如果权限不足，需要设置切换到特权帐号。厂商类型、设备型号、功能模块（SSH 和 TELNET 需要区分模块）也需要根据资源的实际情况进行选择。如下图所示：



图 3.11.4 设置资源连接参数

待设置的网络设备配置备份完成后，可选择网络设备配置备份分组中对应的资源，查看执行结果，并将执行结果文件下载到本地计算机。



图 3.11.5 网络设备配置备份-执行结果

3.12 菜单模式

当运维终端是 Linux、MAC 等系统，或是运维终端不满足浏览器或运维客户端运维的环境要求。可使用字符协议连接工具或 RDP 客户端工具直连云堡垒机来进行安全运维，能支持运维的协议包括 SSH、TELNET、RDP 和 VNC。

3.12.1 命令行方式

首先通过 SecureCRT 工具（也支持其他字符协议连接工具）连接云堡垒机，主机名为云堡垒机 V6.0 管理 IP 地址，端口号为 20022，如图 3.12.1 所示：

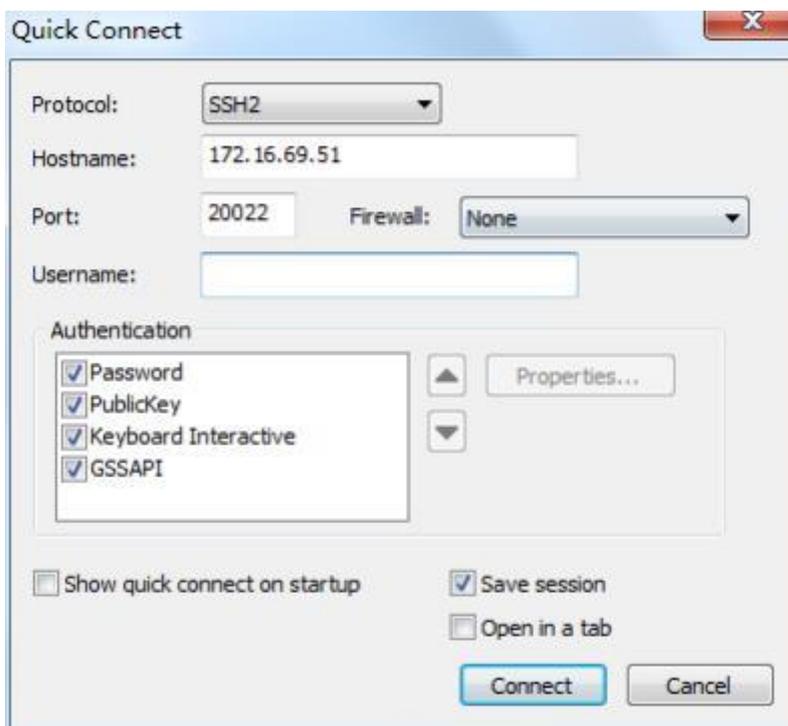


图 3.12.1 连接云堡垒机 V6.0

登录账号密码和该运维用户从 web 界面登录的账号密码一致，如图 3.12.2 所示：

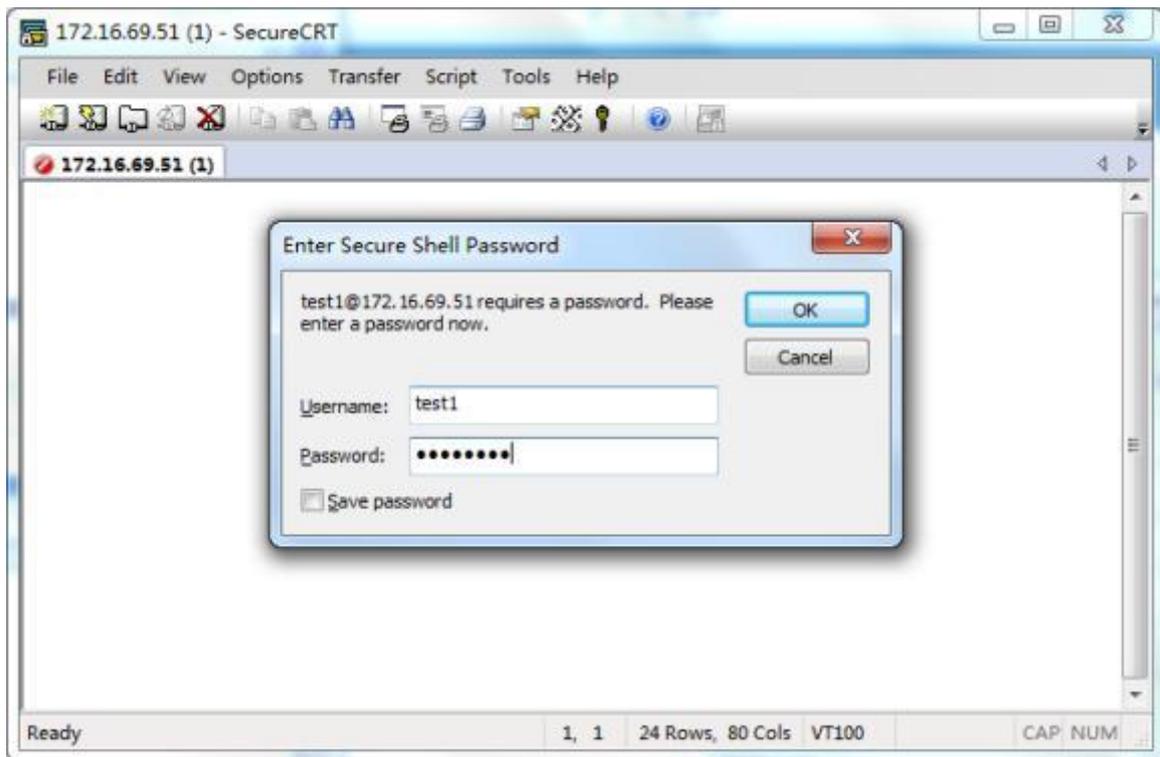


图 3.12.2 登录云堡垒机 V6.0

进入菜单管理界面后,运维用户可以开始选择运维资源。其中“Enter”键为确定,“Esc”键为返回,如图 3.12.3-3.12.7 所示:

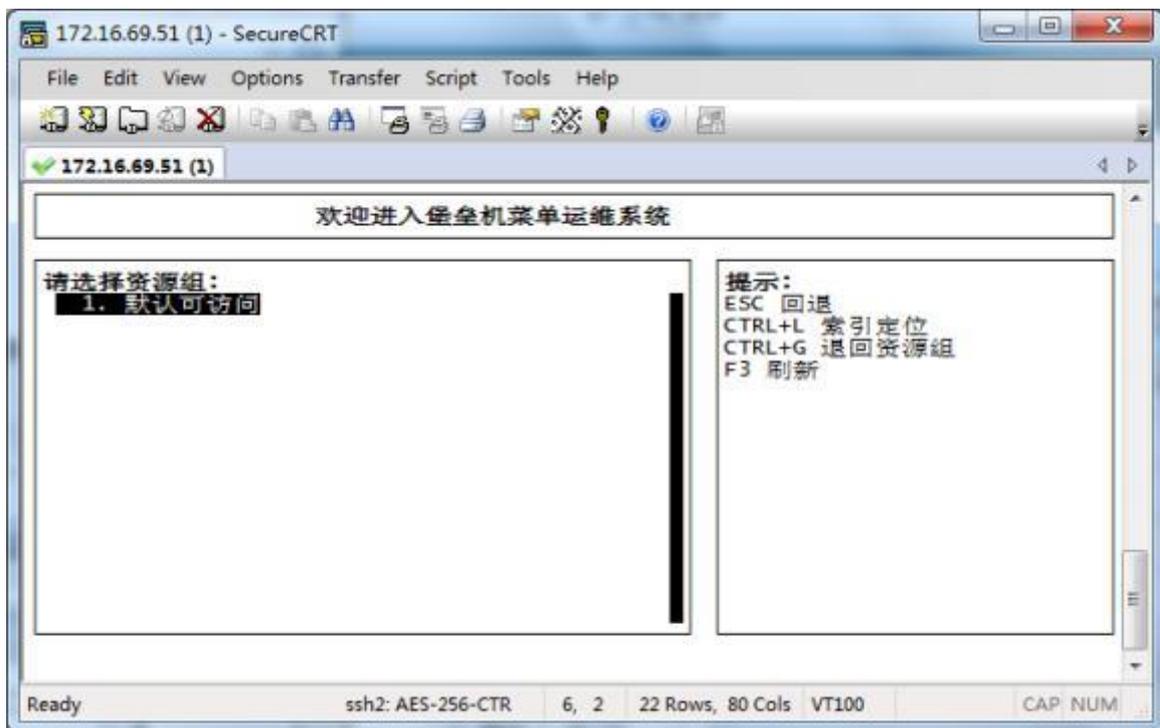


图 3.12.3 选择资源组

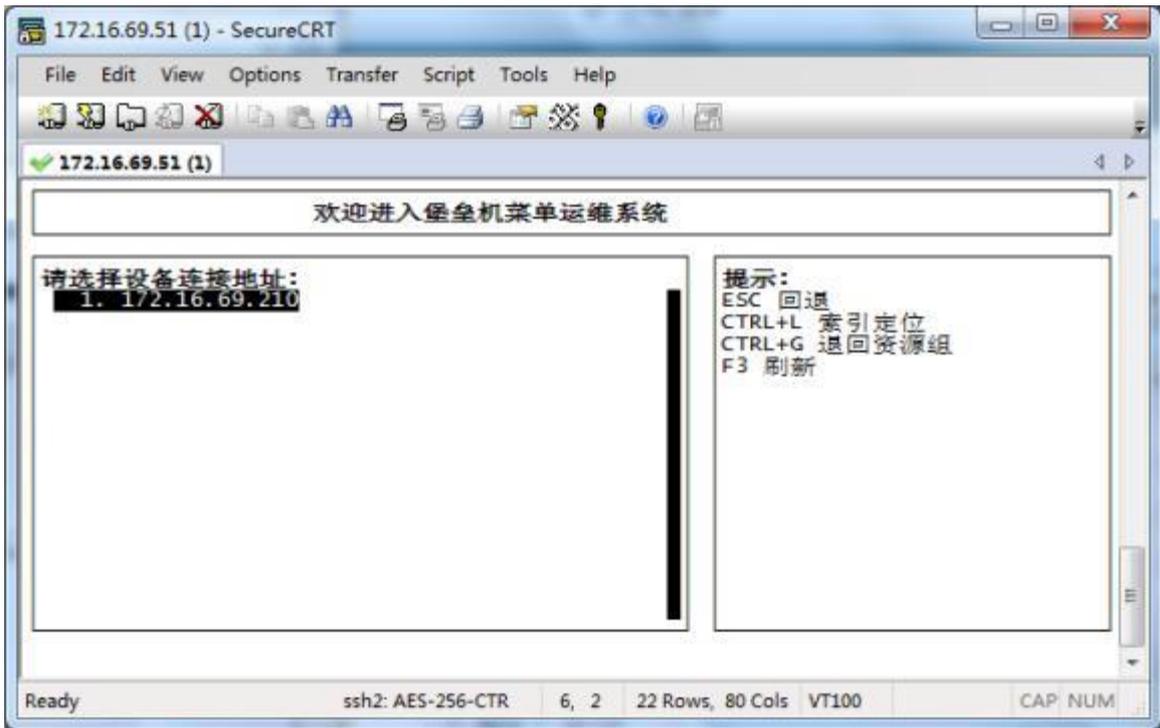


图 3.12.4 选择资源主机

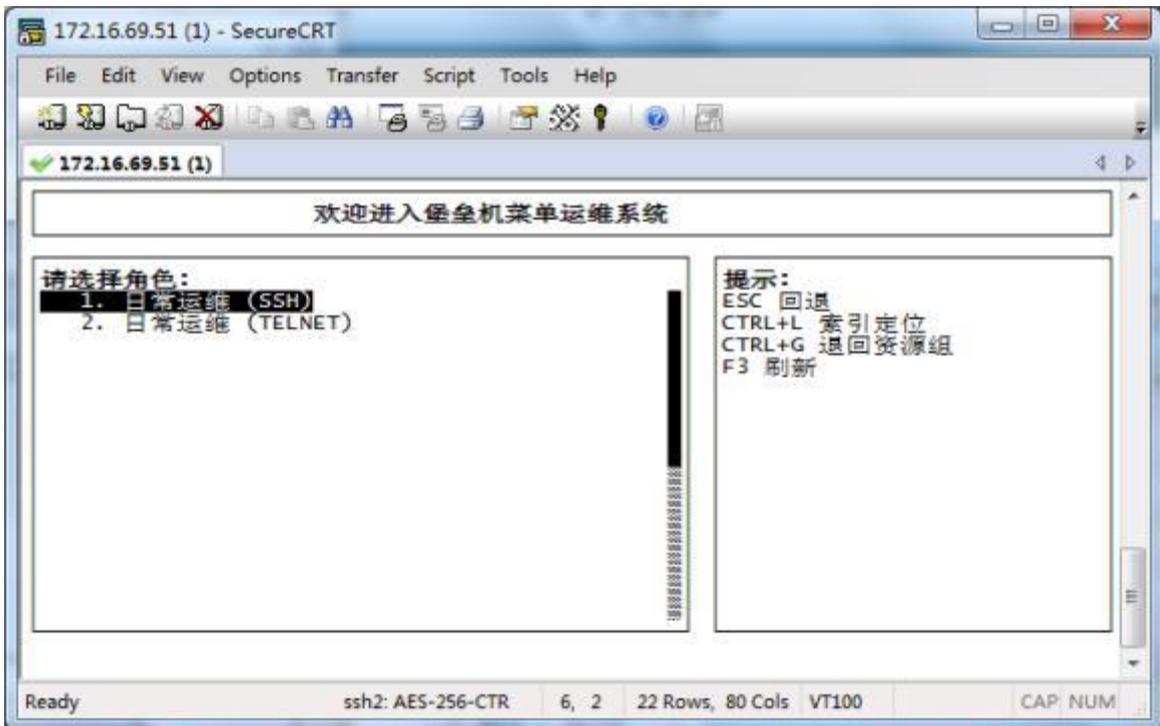


图 3.12.5 选择角色

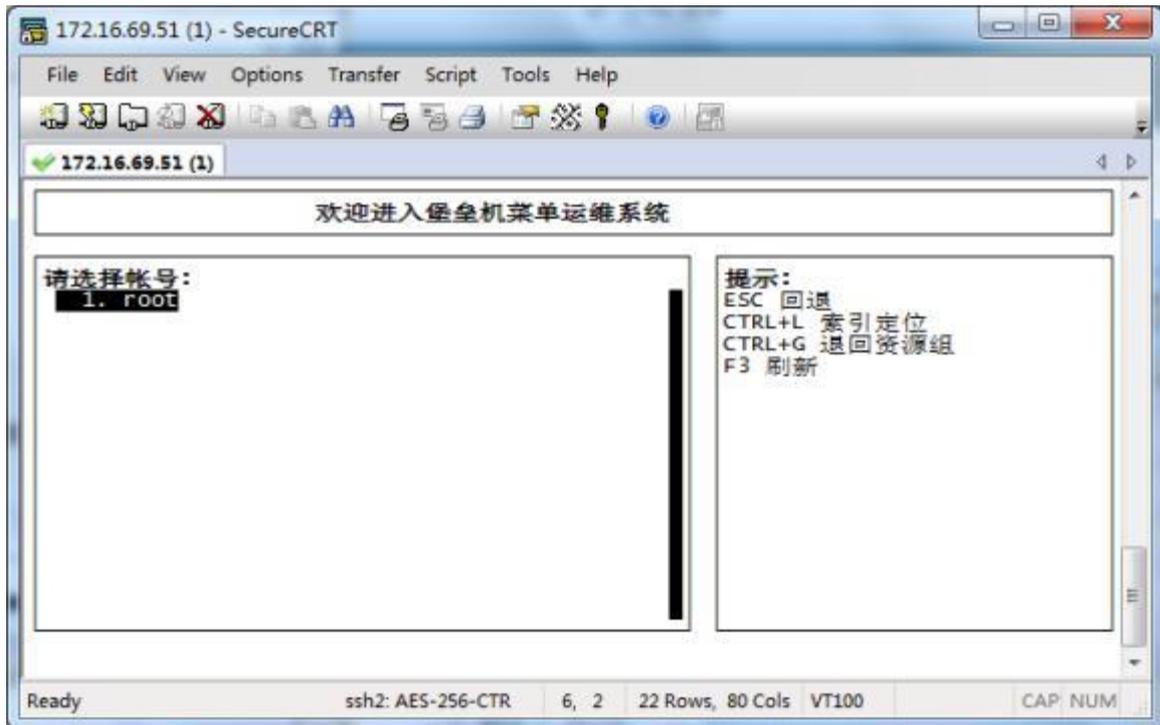


图 3.12.6 选择帐号

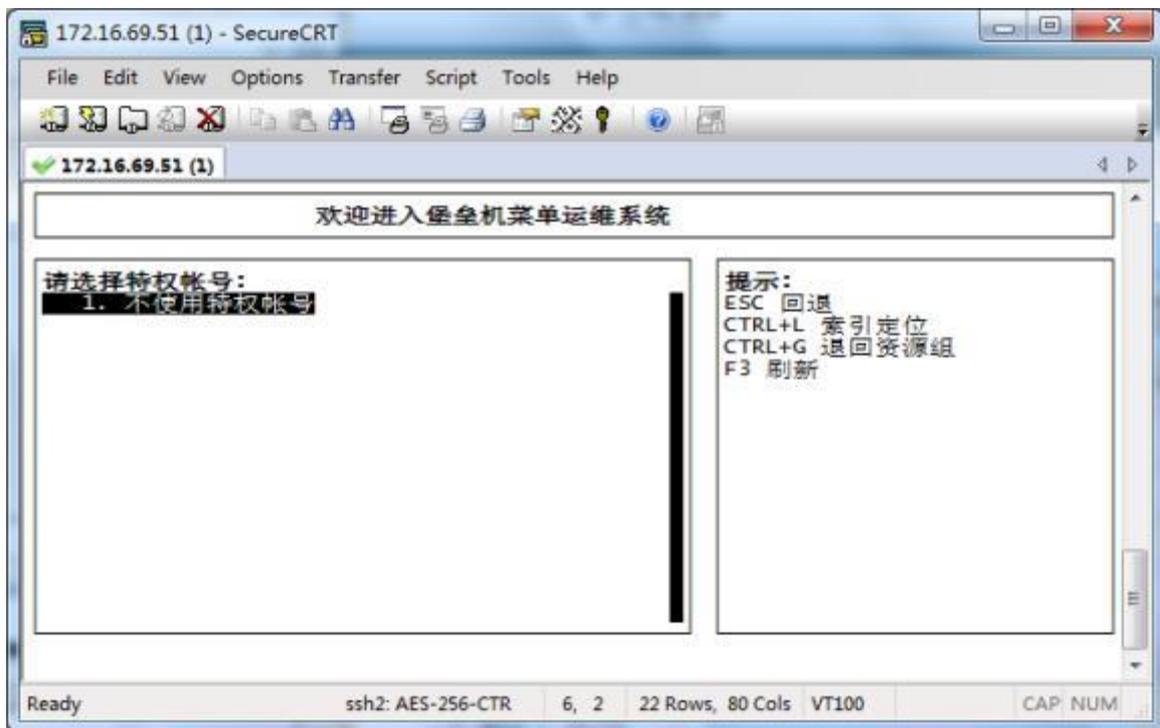


图 3.12.7 确认连接

注意事项：SSH 连接必须保证终端类型为 VT100 或xterm，字符编码：UTF-8（如目标设备字符编码为非 UTF-8，需用户在成功登录目标设备后，再自行调整字符编码），如图 3.12.8-3.12.9 所示：

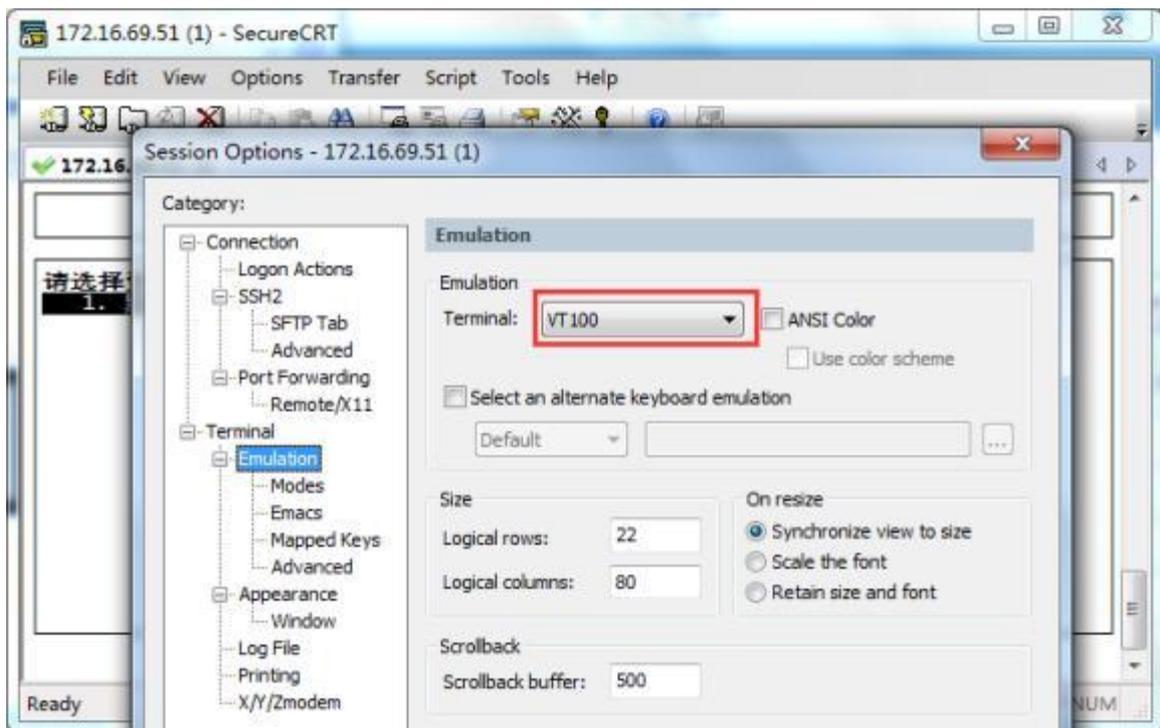


图 3.12.8 终端类型

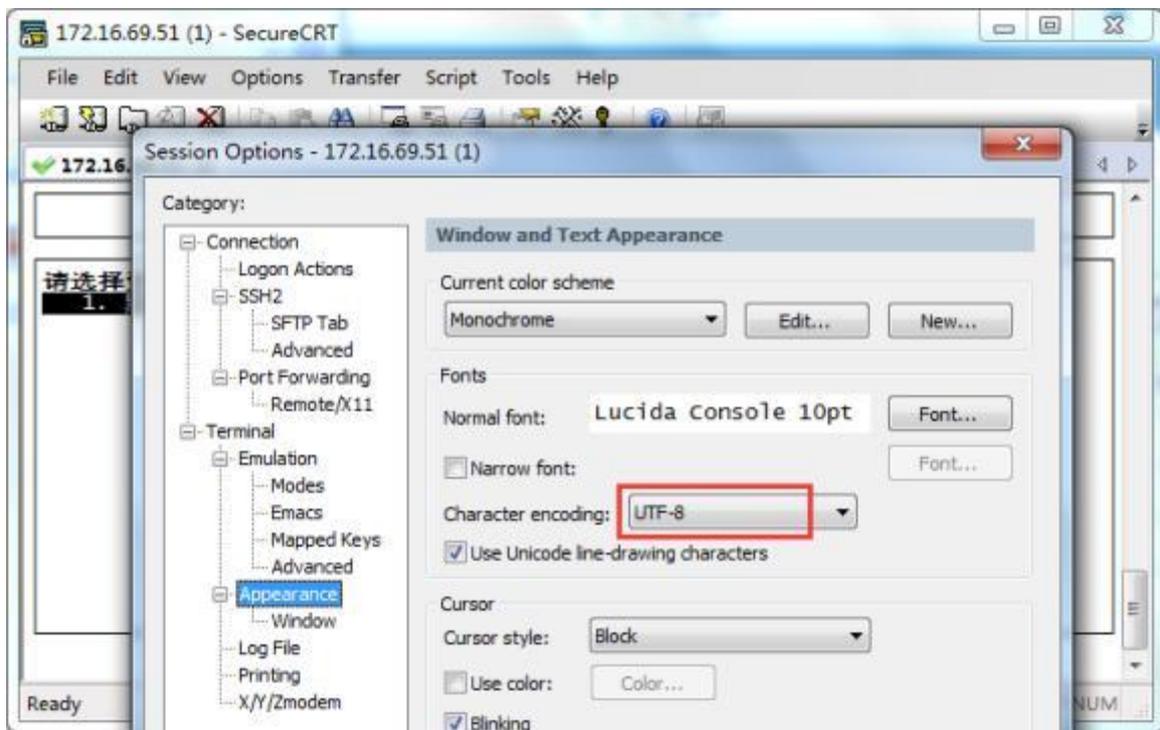


图 3.12.9 终端编码

3.12.2 图形方式

运维用户若希望通过 RDP、VNC 协议远程访问主机资源，可以启用Windows 系统默认的

远程桌面连接工具（RDP: mstsc.exe）进入图形化访问资源菜单。如图 3.12.10 所示，直接输入云堡垒机 V6.0 系统 IP 地址，端口为 23389，然后选择连接，如果需要映射磁盘，请展开选项卡进行设置，如图 3.12.11 所示。



图 3.12.10 图形方式访问菜单登录

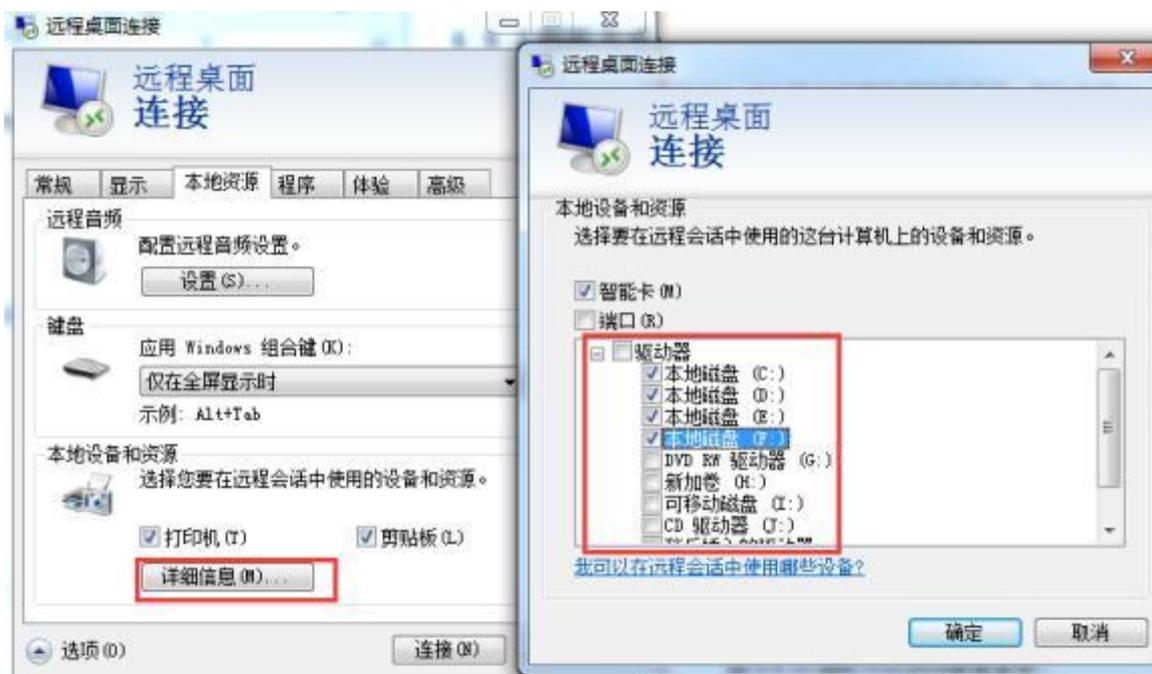


图 3.12.11 开启磁盘映射

输入运维账号、密码，如图 3.12.12 所示。



图 3.12.12 运维用户身份认证

运维账号认证通过后，展现出用户可访问的资源列表，如图 3.10.13 所示，选择对应的资源和账号后，选择“连接”，便会登录到目标服务器上。



图 3.12.13 资源菜单