

运维人员使用手册

天玥运维安全网关产品

启明星辰信息技术集团股份有限公司

2022 年 8 月



版权申明

北京启明星辰信息技术有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于北京启明星辰信息技术有限公司。未经北京启明星辰信息技术有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责声明

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦 邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

修订记录

修订版本号	日期	备注
V1.0	2022-08-30	无

目 录

1 关于本手册	6
1.1 约定	6
1.1.1 注意事项	6
1.1.2 文本	6
1.1.3 插图	6
2 windows 使用说明	7
2.1 系统登录	7
2.2 国密配置	8
2.3 环境配置	9
2.4 运维说明	16
2.4.1 RDP/VNC 访问	16
2.4.2 Telnet/SSH 访问	17
2.4.3 FTP 访问	19
2.4.4 数据库访问	21
2.4.5 WEB 访问	23
2.4.6 X11-XDMCP 访问	25
2.4.7 HTML5 运维	25
2.4.8 批量登录	27
2.4.9 运维工单	28
2.4.10 命令自动执行	29
2.4.11 网络设备配置备份	31
2.5 菜单模式	33
2.5.1 命令行方式	33
2.5.2 图形方式	37

3 MACOS 使用说明	39
3.1 系统登录	39
3.2 环境配置	41
3.3 运维说明	45
3.3.1 RDP/VNC 访问	45
3.3.2 Telnet/SSH 访问	47
3.3.3 FTP 访问	49
3.3.4 数据库访问	51
3.3.5 X11-XDMCP 访问	54
3.3.6 HTML5 运维	54
3.3.7 批量登录	56
3.3.8 运维工单	57
3.3.9 命令自动执行	58
3.3.10 网络设备配置备份	60
3.4 菜单模式	62
3.4.1 命令行方式	62
3.4.2 图形方式	67
4 国产操作系统使用说明	71
4.1 终端说明	71
4.1.1 系统登录	72
4.1.2 国密配置	75
4.1.3 终端升级	76
4.2 运维说明	78
4.2.1 RDP/VNC 访问	78
4.2.2 Telnet/SSH 访问	79
4.2.3 FTP 访问	80

4.2.4 数据库访问	81
4.2.5 X11-ssh 访问	82
4.2.6 运维工单	84
4.3 异常情况说明	85
4.3.1 用户登录失败	85
4.3.2 退出登录	86
5 参考文档	87
6 技术支持	87

1 关于本手册

天玥运维安全网关，是启明星辰综合内控系列产品之一。

天玥运维安全网关是针对业务环境下的用户运维操作进行控制和审计的合规性管控系统。管理员可以使用天玥运维安全网关控制运维人员能运维哪些设备，执行哪些操作命令，避免运维人员非法或无意执行高危操作，并对运维人员的操作进行实时监控和事后审计。

本手册详细介绍了天玥运维安全网关包括用户管理、资源与授权、规则管理、帐号与密码管理、自动运维、工单管理、审计管理、系统管理各功能模块的使用方法，用户可参考本手册，对天玥运维安全网关进行各种管理配置。



说明：若产品在发行时附有版本说明。且版本说明中的信息与本手册中的信息有所差异时，请遵循版本说明中的指示。

1.1 约定

本文中所有图例均为实际拍摄或屏幕截取

菜单名称和按钮名称的表示方法：“菜单名称”，“按钮名称”

1.1.1 注意事项

图标	类型	说明
	提示信息	系统管理、配置的重要说明、提示信息
	配置信息	相关功能配置的举例说明信息

1.1.2 文本

约定	说明
菜单名称表示方法	文档中菜单名称表示为“菜单名称”
按钮名称表示方法	文档中按钮名称表示为“按钮名称”

1.1.3 插图

本文中所有图例均为实际拍摄或屏幕截取

2 WINDOWS 使用说明

2.1 系统登录

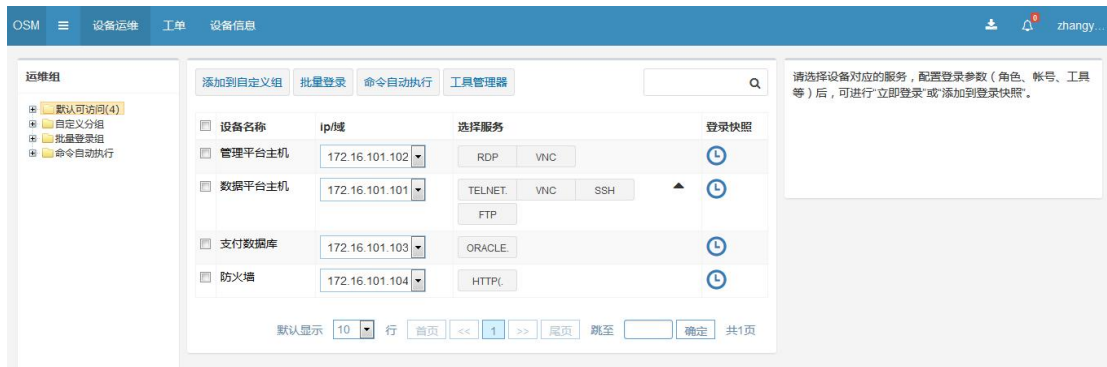
用户通过浏览器访问天玥运维安全网关系统，登录 URL 地址默认为：<https://天玥运维安全网关的 IP 地址>。首先选择正确的认证方式（默认为内置本地认证），然后输入帐号和密码，点击“登录”，认证成功后进入运维界面。

推荐操作系统：Winodws7、Winodws10、windows11、Windows Server 2008 R2、Windows Server 2012、Windows Server 2016

推荐浏览器：IE 浏览器（IE9-IE11）、谷歌浏览器（52 及以上版本）、火狐浏览器（56 及以上版本）



系统登录界面



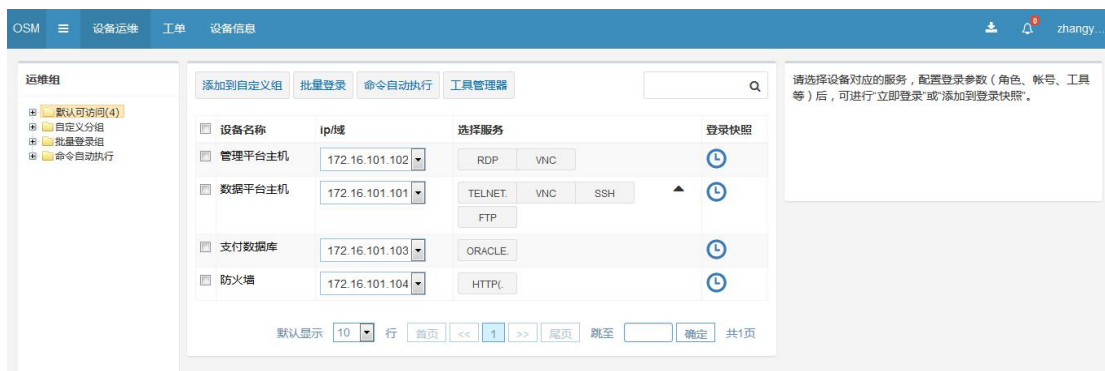
运维界面

如果配置了 CAS 单点登录，输入 <https://天玥运维安全网关的 IP 地址> 后会跳转到 cas 服务器

登录页，输入用户名和密码认证成功后进入天玥运维安全网关运维界面



跳转到 cas 服务器登录页



认证成功进入运维页

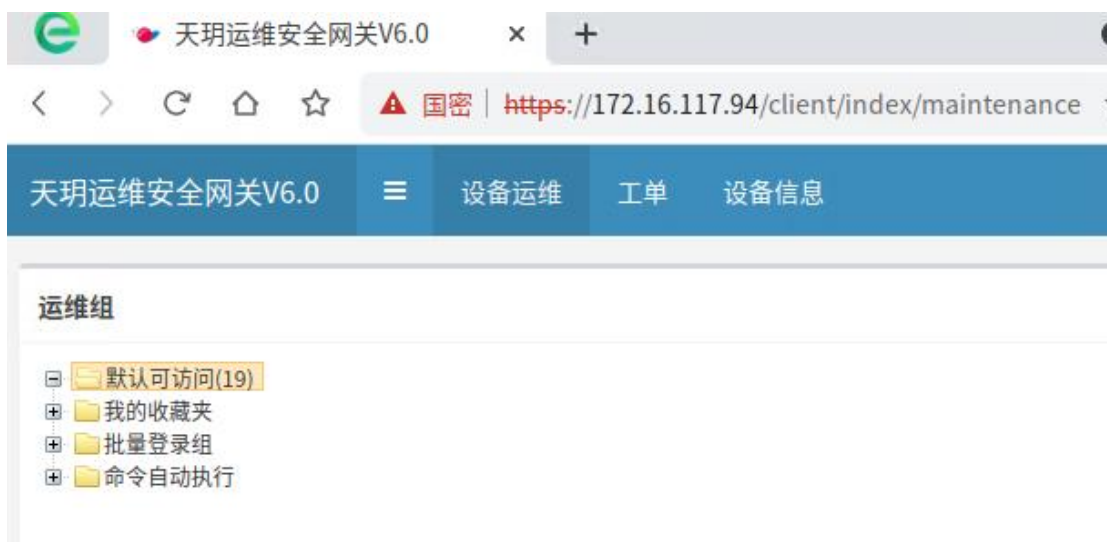
2.2 国密配置

如果“HTTPS 协议”配置的“国密 HTTPS”，用户在使用时需要在浏览器配置国密登录，
举例浏览器：360 企业安全浏览器

配置方法：浏览器“设置”->“安全设置”，“国密通讯协议”勾选启用国密 SSL 协议支持
 （重启浏览器后生效）



启用国密 SSL 协议支持



国密 HTTPS 运维

2.3 环境配置

用户在使用天玑运维安全网关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）。

用户同时需要根据本地运维需求安装运维工具。运维工具推荐版本信息如下：

运维工具	工具名称	推荐版本
	mstsc	系统自带
	Putty	0.7.0

	SecureCRT	8.1.3
	SecureFX	8.1.3/9.0/9.2
	Xshell	6.0086/7.0.0.1
	SSH Secure Shell Client	3.2.9
	WinSCP	5.13.2
	FFFTP	3.3
	FlashFXP	5.4.0
	FileZilla	3.33.0
	XFTP	7.0.0097
	SQLPlus	11.2.0.1.0
	PL/SQL Developer	8.0.4.1514
	Toad for Oracle	11.6
	Sql developer	20.4.1.407/22.2.0.173
	Quest Central for DB2	5.0.2.4
	DB2 Command line	9.7.0
	DBVisualizer	10.0.12
	pgAdmin III	1.18.1
	MySQL Command line	5.7.21
	Navicat	12.0.29/15.0.28/16.0.14
	SQL Server Management Studio	14.7/17.0/18.12.1
	Teradata SQL Assistant	14.10.0.2
	SqlDlx Personal	4.3
	SqlDlx Professional	3.29

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。



登录界面-相关下载



运维界面-相关下载

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

环境检查助手 (用于检查堡垒机用户本地环境是否正常)

Windows版下载

基础控件 (运维、管理基础控件, 堡垒机用户必须安装)

MacOS版(X86)下载

MacOS版(ARM)下载

Windows版下载

监控回放 (安装基础控件后, 才可以正常使用该组件, 运维监控、审计回放必备组件, 审计用户请安装)

Windows版下载

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)

Windows版下载

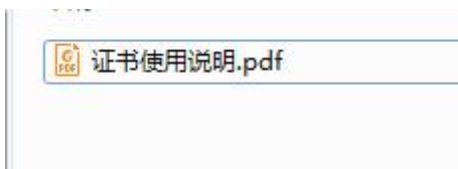
下载证书

- 解压文件。



解压文件

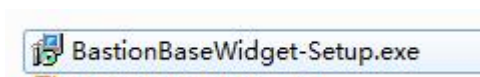
- 参考证书使用说明进行安装。



安装证书

步骤 2 安装基础控件

- 双击基础控件安装包。



基础控件安装包

- 选择语言（默认选择中文）。



安装基础控件（一）

3. 确认安装。



安装基础控件（二）

4. 完成安装。



安装基础控件（三）

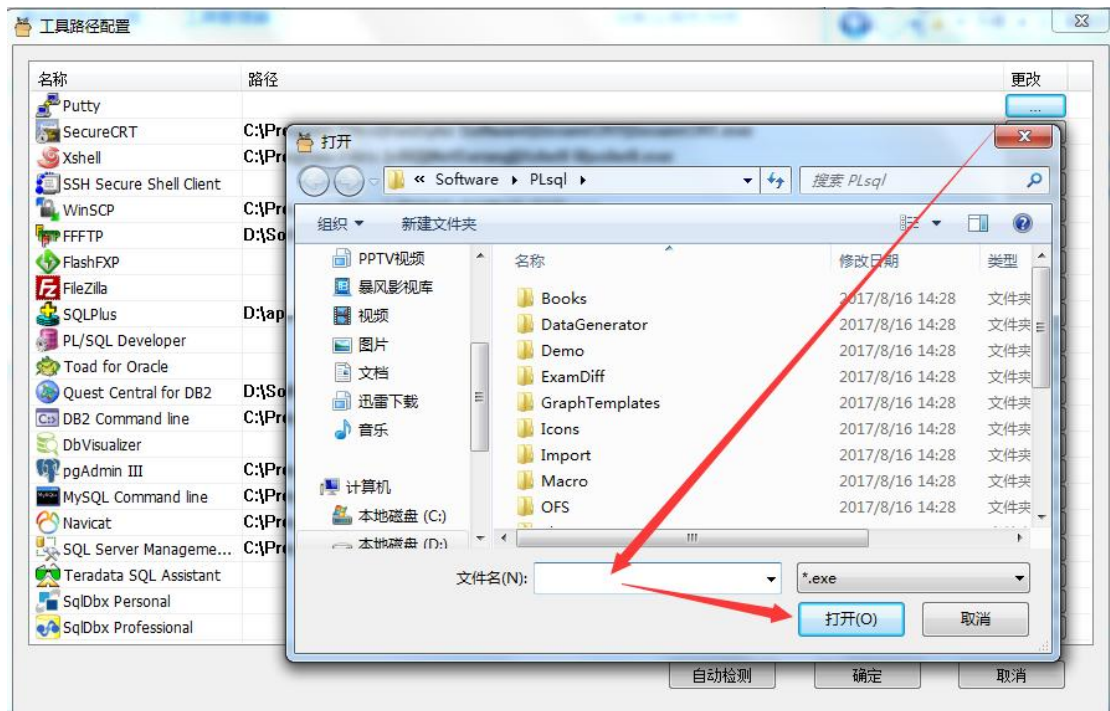
步骤 3 配置运维工具路径

1. 在基础控件安装完成时，勾选“运行堡垒机工具路径配置”。



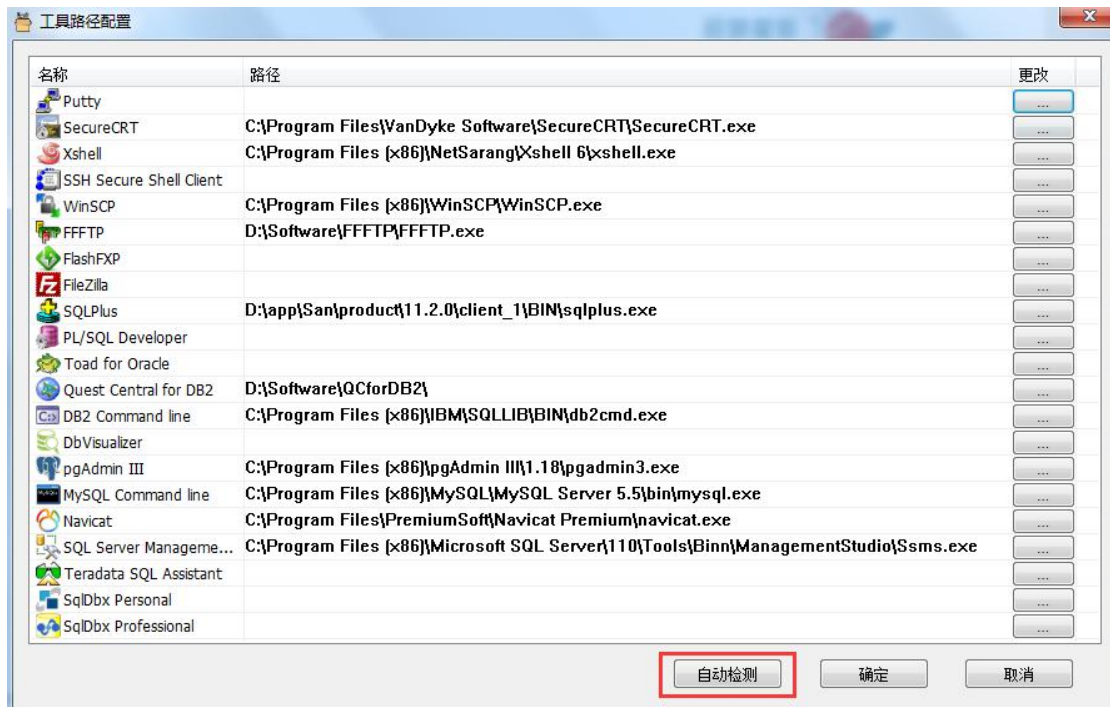
运行工具路径配置（一）

2. 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。



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。



运行工具路径配置（三）

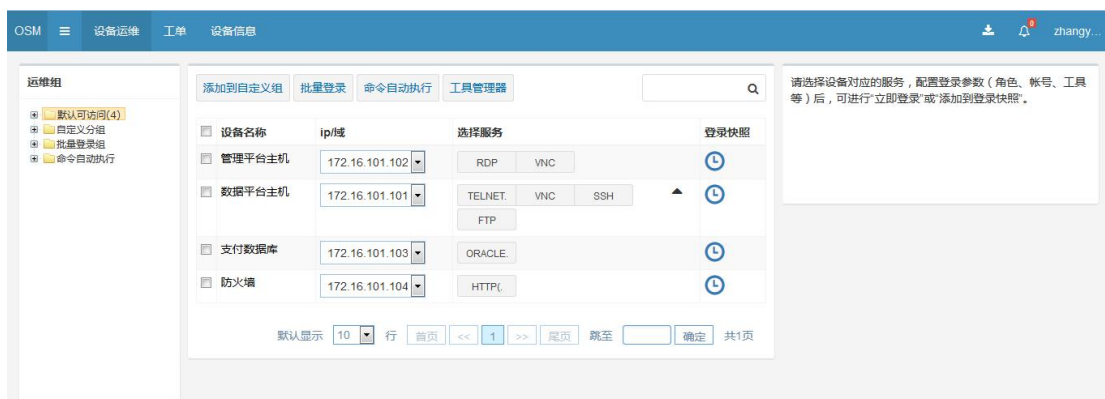
2.4 运维说明

2.4.1 RDP/VNC 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

步骤 2 选择登录配置

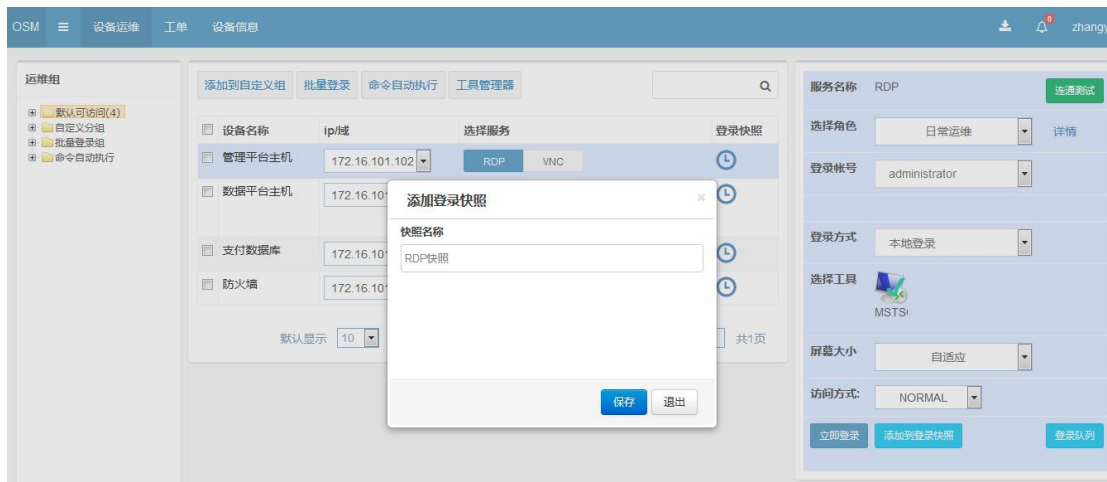
选择需要运维的 RDP 或 VNC 资源。



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”。



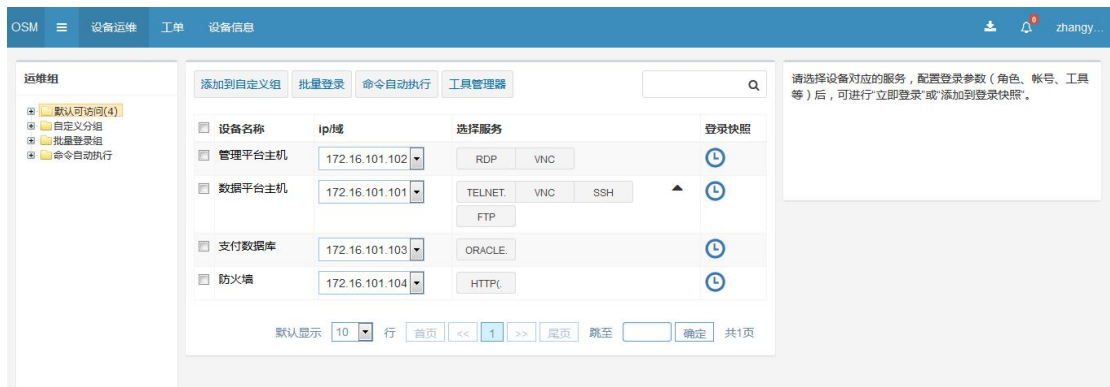
图形协议运维-立即登录

2.4.2 TELNET/SSH 访问

操作步骤

步骤 1 进入设备运维页面

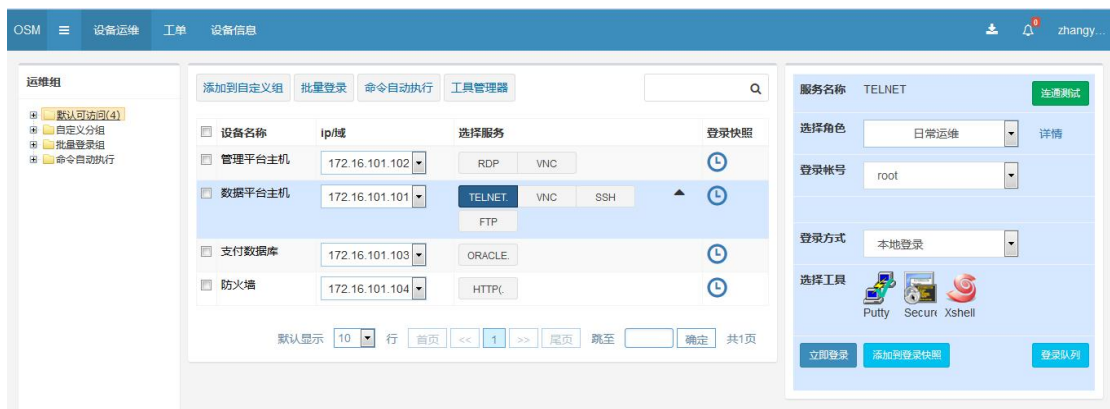
运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

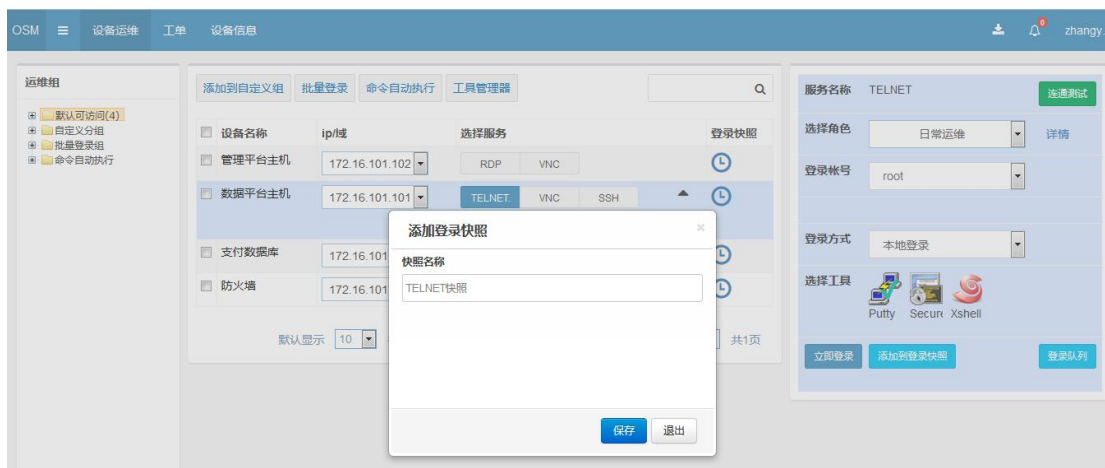
步骤 2 选择登录配置

选择需要运维的 SSH 或 TELNET 资源。



字符协议运维

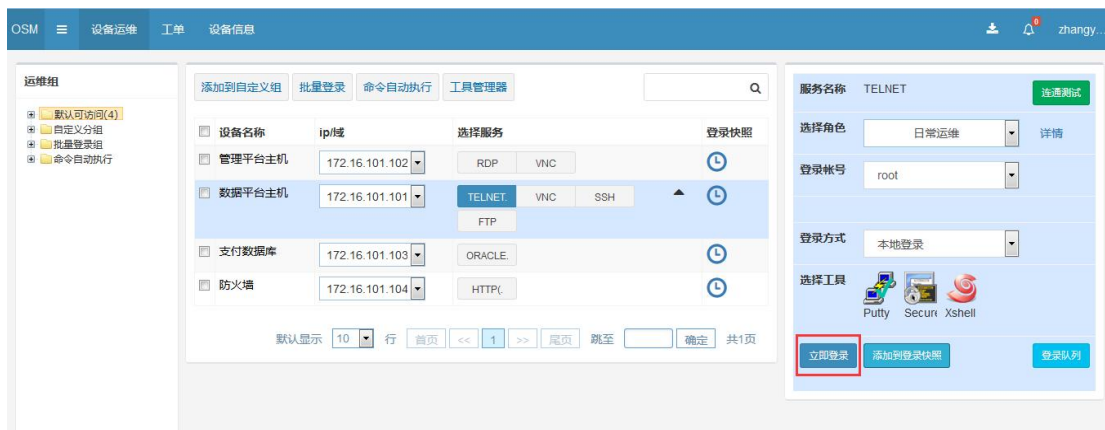
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



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”。



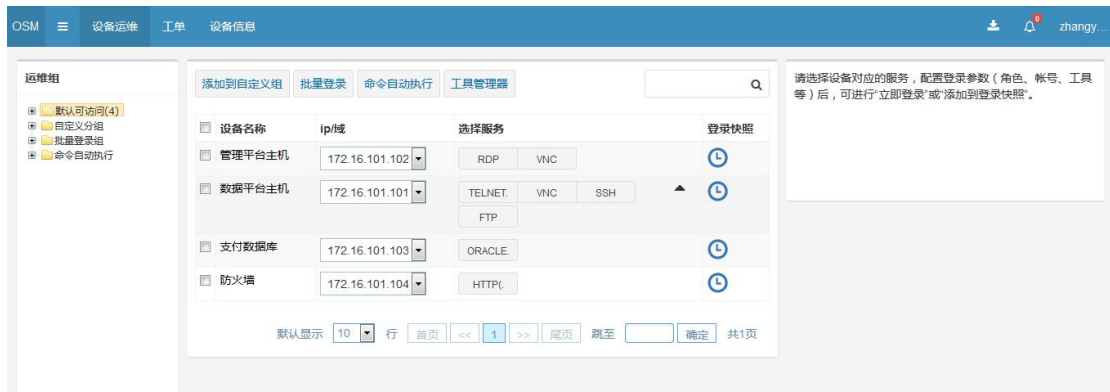
字符协议运维-立即登录

2.4.3 FTP 访问

操作步骤

步骤 1 进入设备运维页面

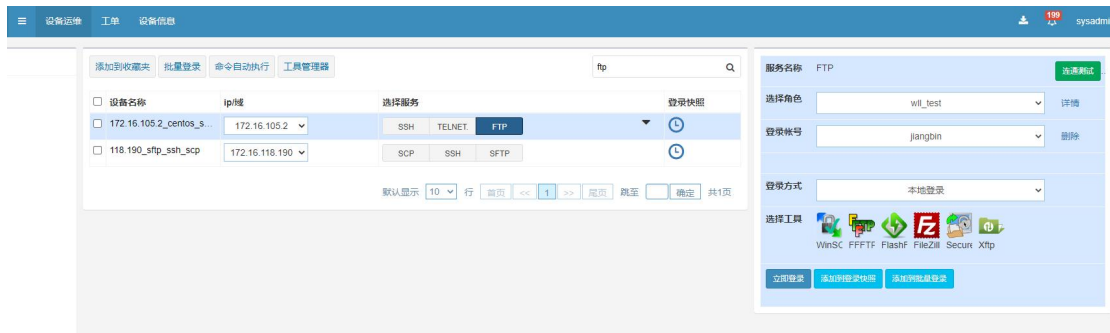
运维用户登录天玑运维安全网关控制台，选择“设备运维”。



设备运维

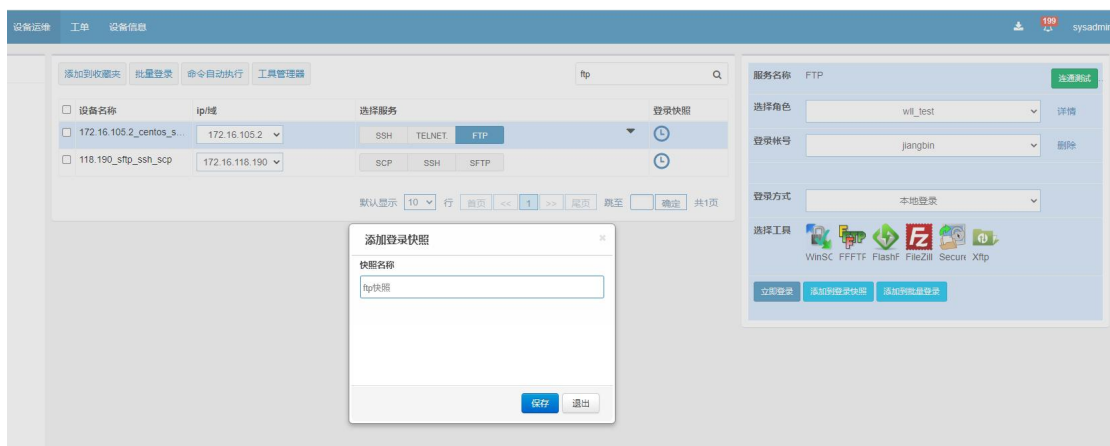
步骤 2 选择登录配置

选择需要运维的 FTP 资源。



文件传输协议运维

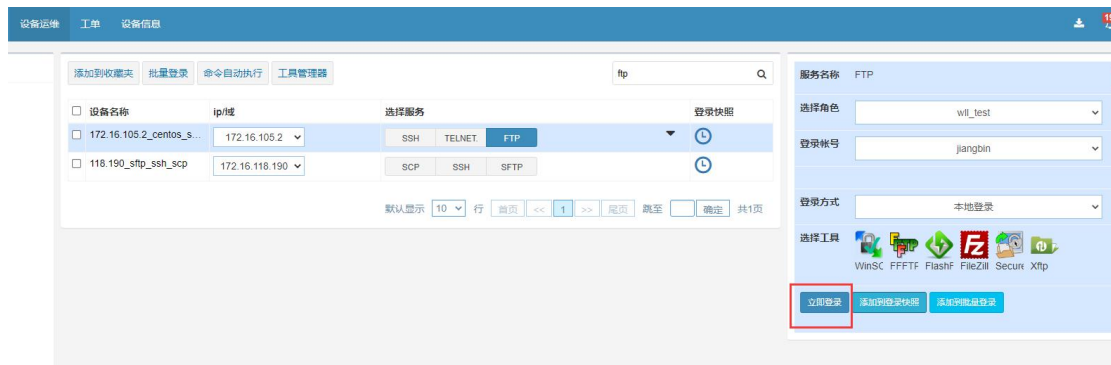
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



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”。



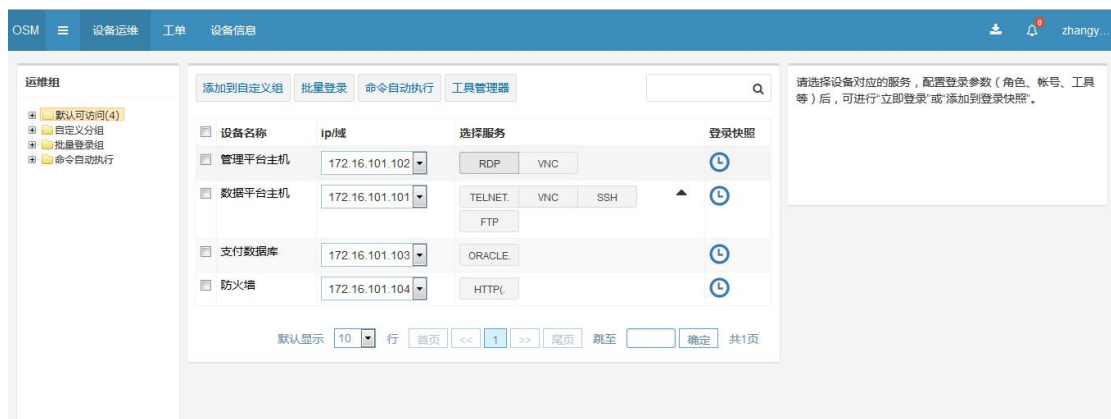
文件传输协议运维-立即登录

2.4.4 数据库访问

操作步骤

步骤 1 进入设备运维页面

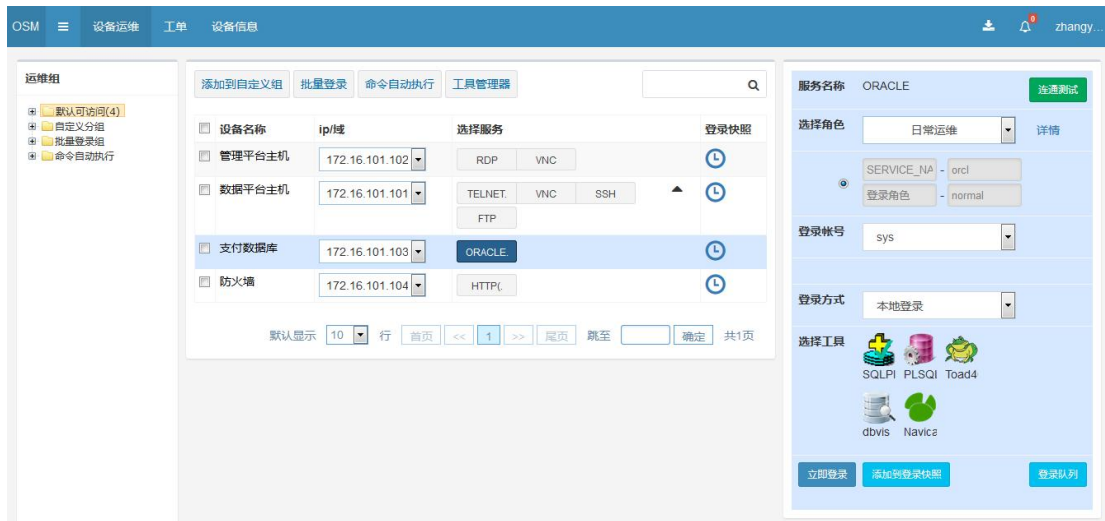
运维用户登录天玑运维安全网关控制台，选择“设备运维”。



设备运维

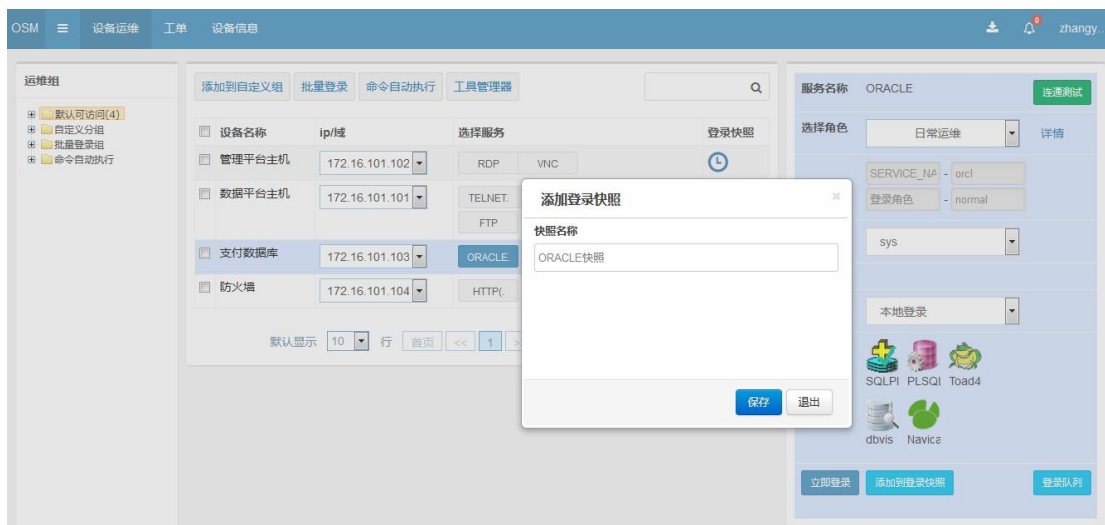
步骤 2 选择登录配置

选择需要运维的数据库资源。



数据库协议运维

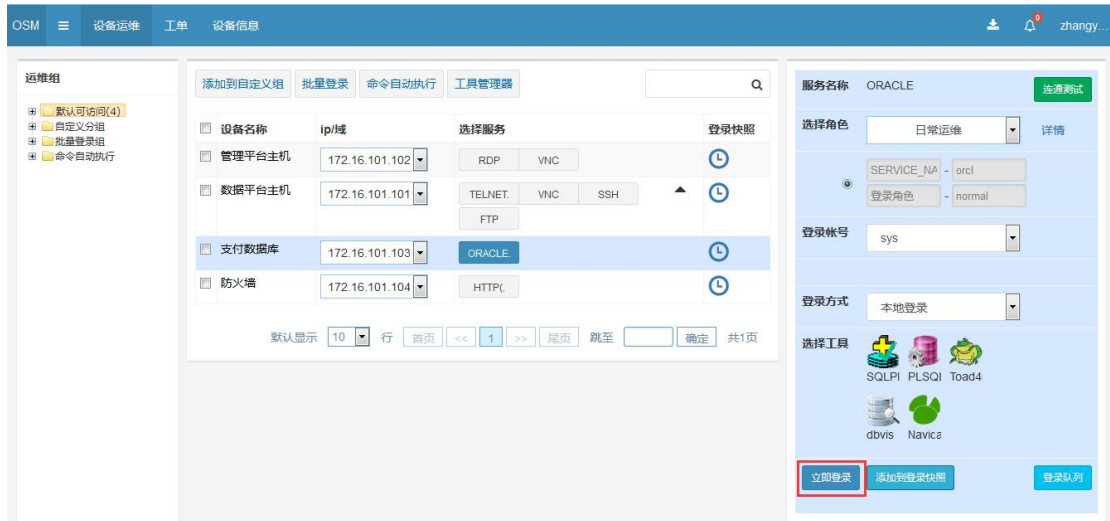
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



数据库协议运维-添加登录快照

步骤 3 进行运维登录

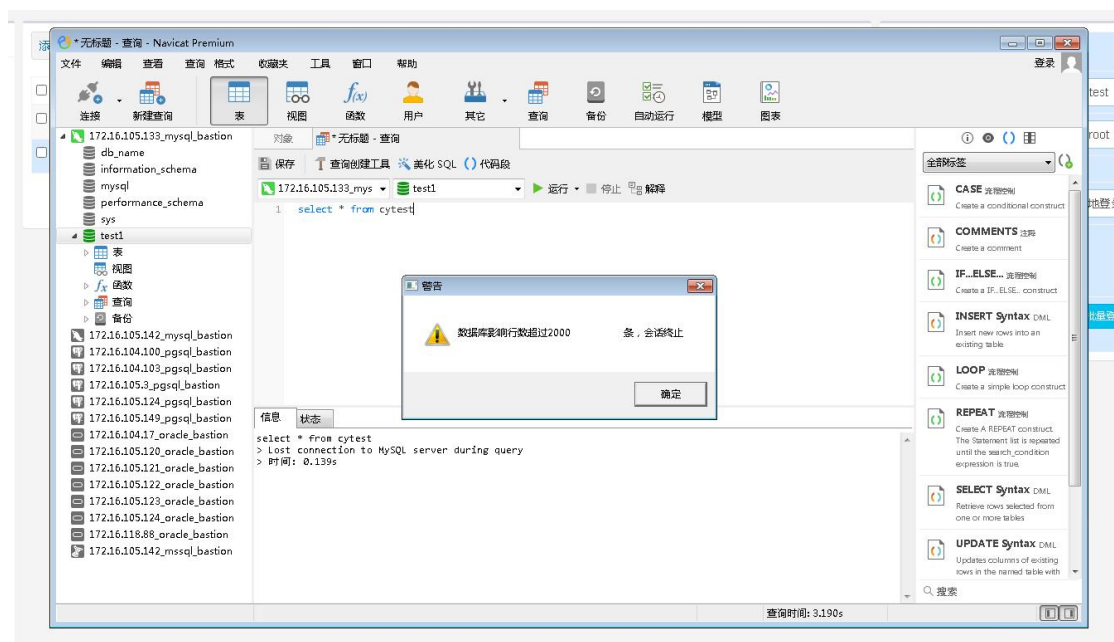
确认登录配置后，单击“立即登录”。



数据库协议运维-立即登录

步骤 4 数据策略触发

当执行数据库命令影响行数超过设置的条数时, 执行日志告警或者会话阻断。



会话阻断

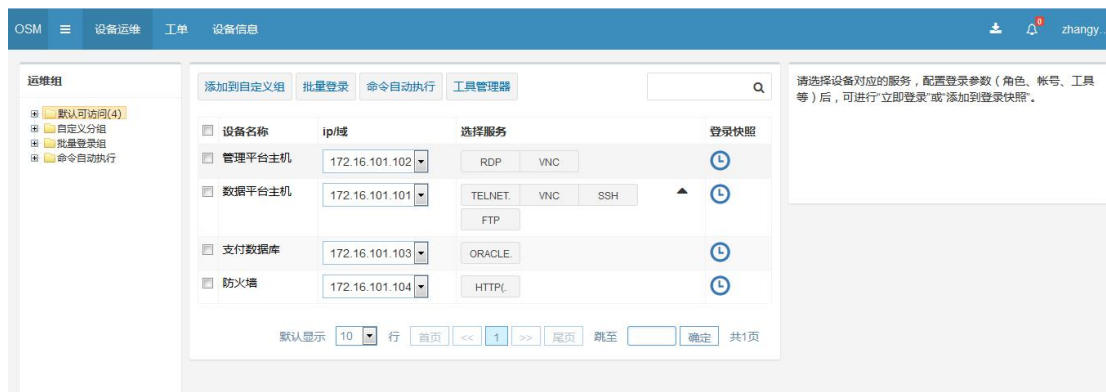
2.4.5 WEB 访问

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

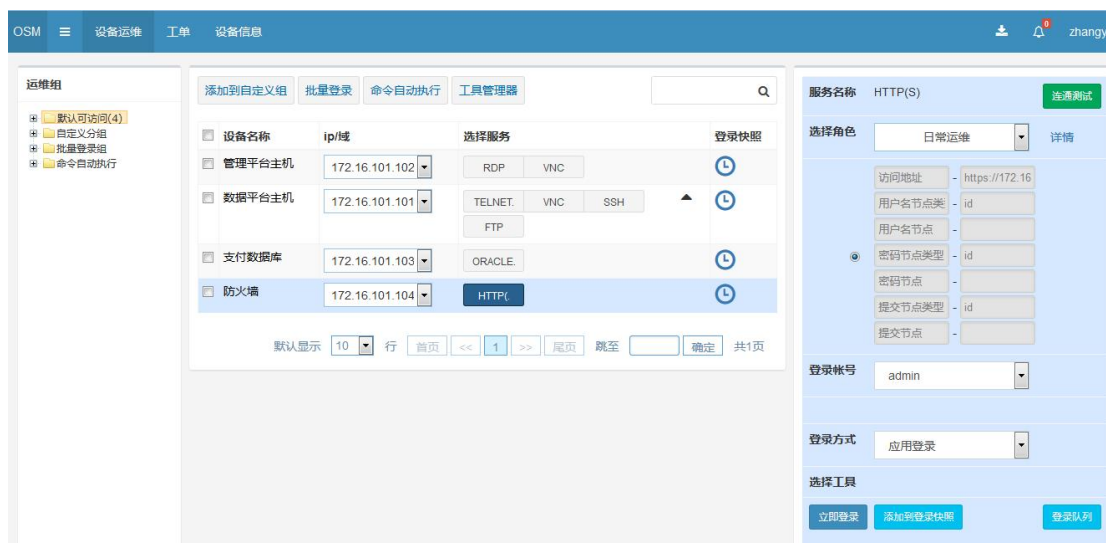
运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

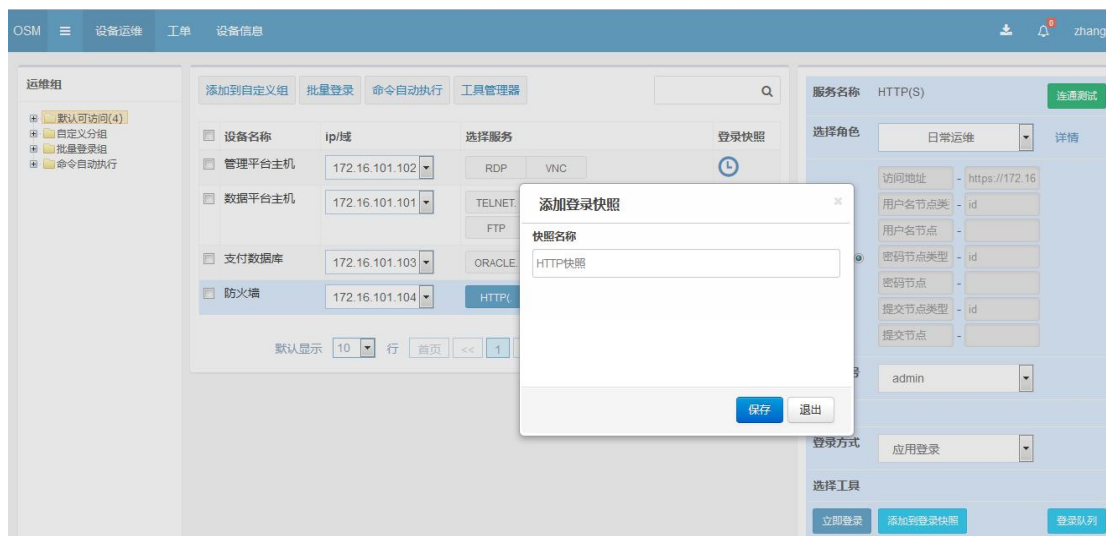
步骤 2 选择登录配置

选择需要运维的资源。



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）。



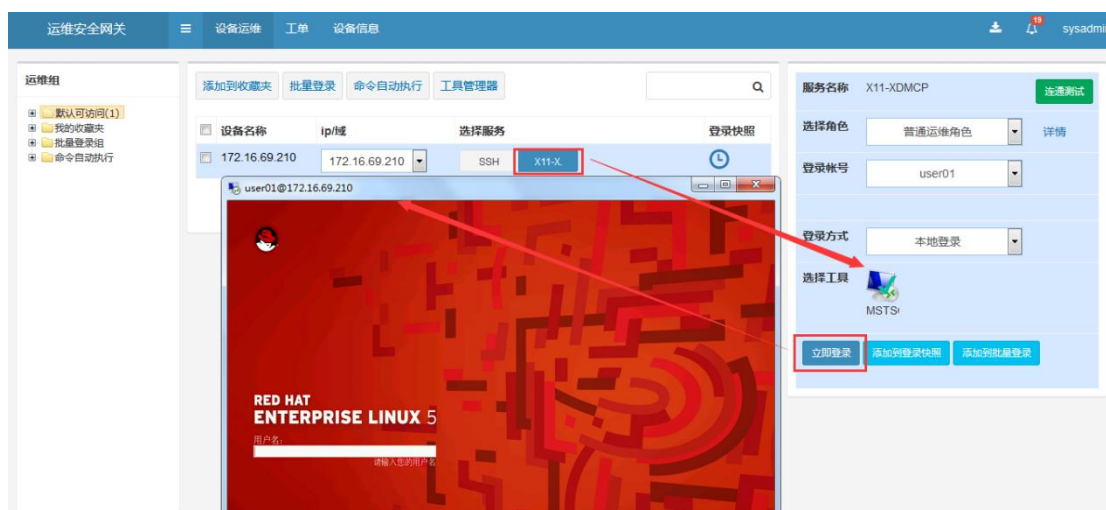
WEB 访问-添加登录快照

步骤 3 进行运维登录

确认登录配置后，单击“立即登录”。

2.4.6 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。**



X11-XDMCP 访问

2.4.7 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。



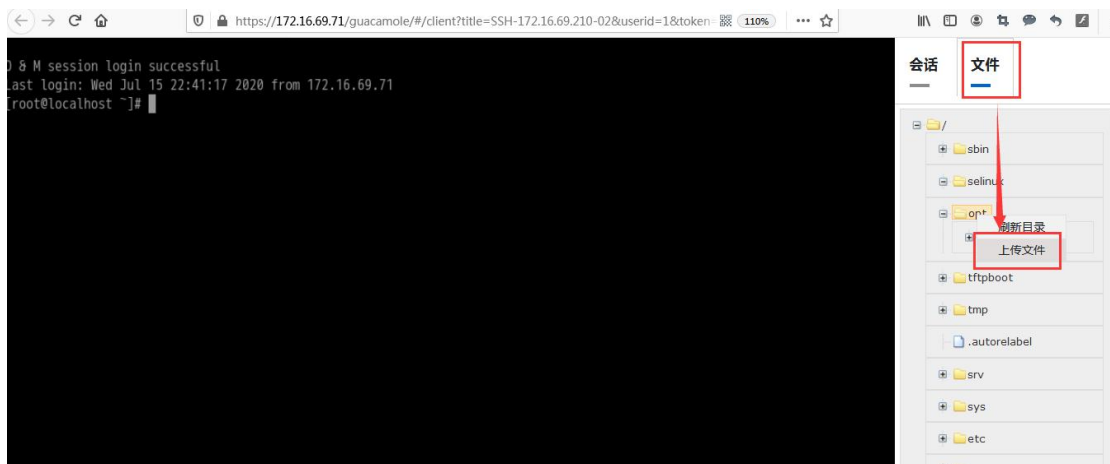
HTML5 运维登陆

如果第一次连接资源失败，请重新连接一次。如图所示：



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。如图所示：



HTML5 运维文件上传

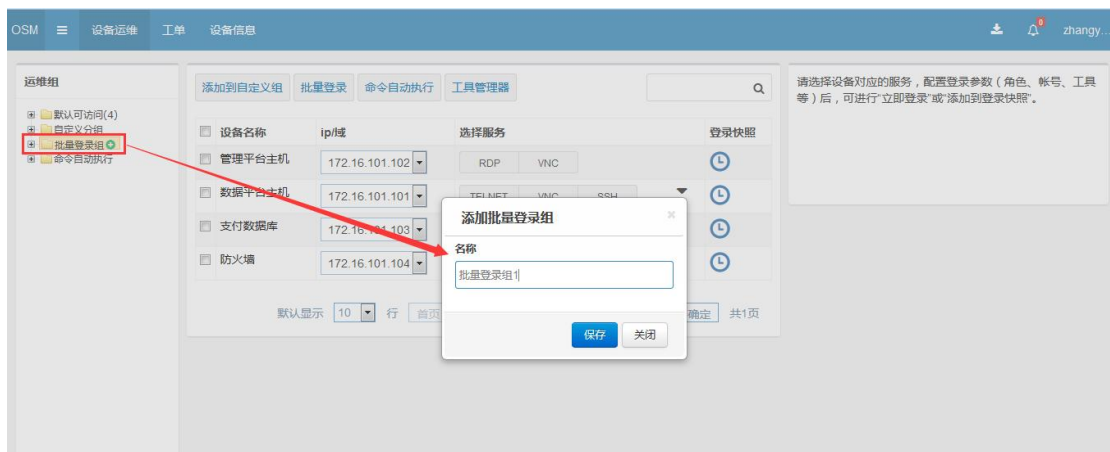
2.4.8 批量登录

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

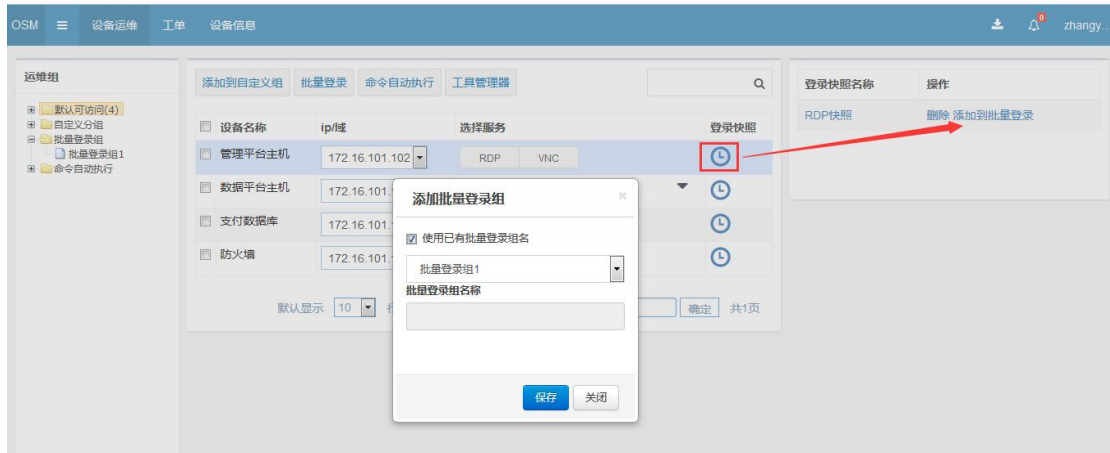
运维用户根据实际需求添加批量登录组。



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。



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”。



批量登录（三）

2.4.9 运维工单

2.4.9.1 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。

工单申请

2.4.9.2 工单运维

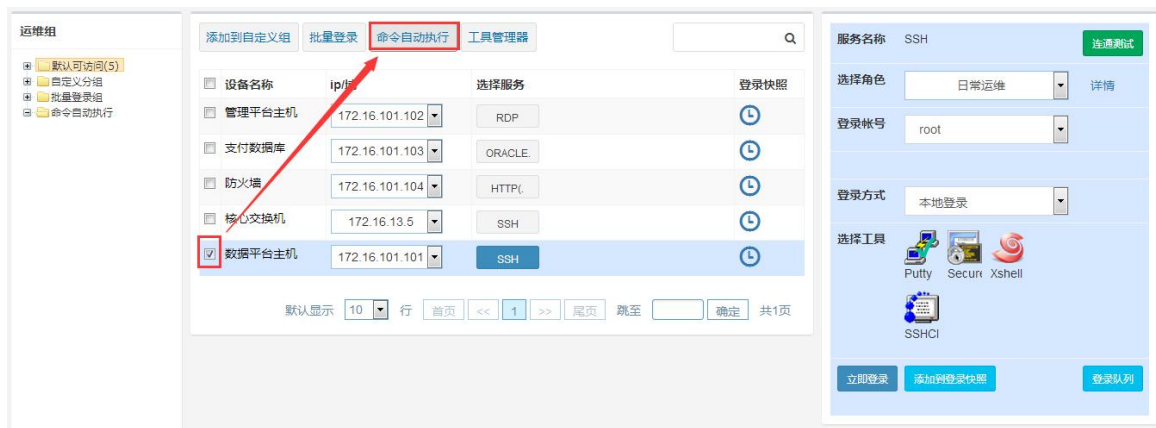
当用户申请的工单经管理员审批通过后或者管理员为运维用户下发了工单，用户可进入“工单”界面，选择工单中的资源进行运维。

工单资源运维

2.4.10 命令自动执行

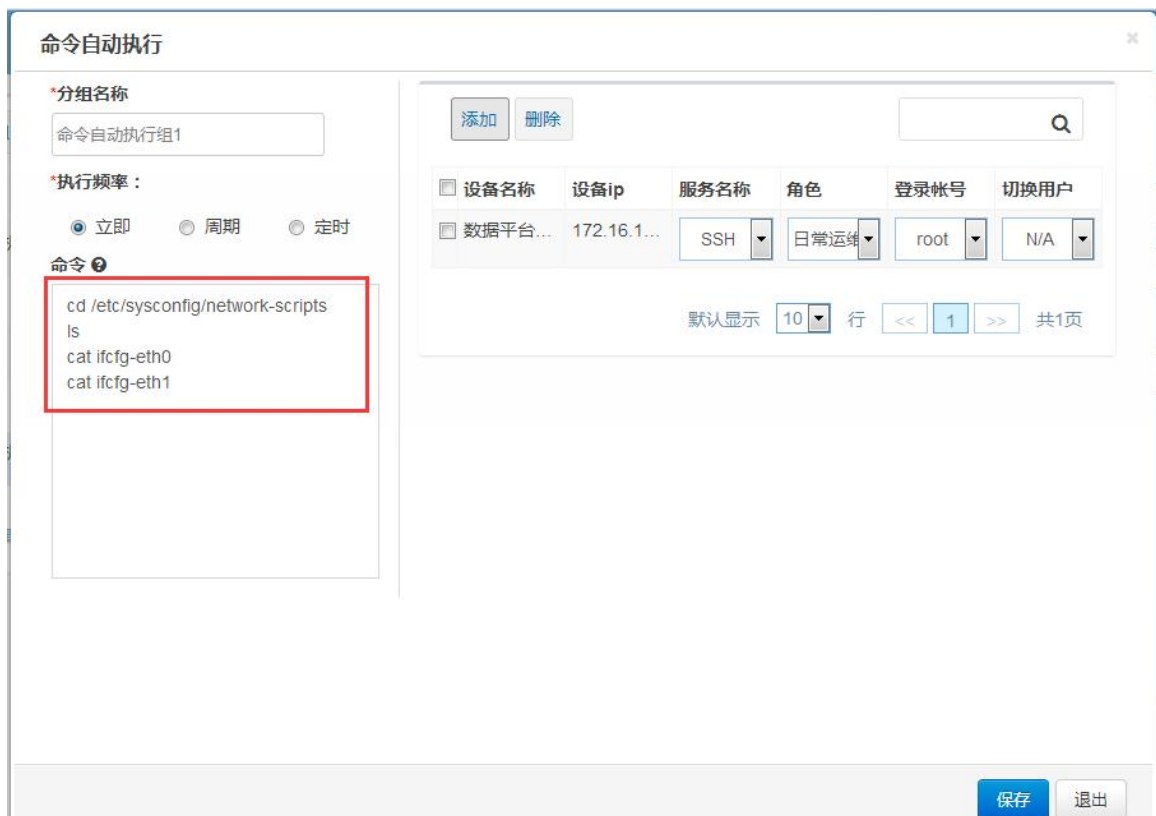
运维用户可对单台或多台资源设置命令执行任务，并可以文件的形式获取到命令执行结果。

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”，如图所示。



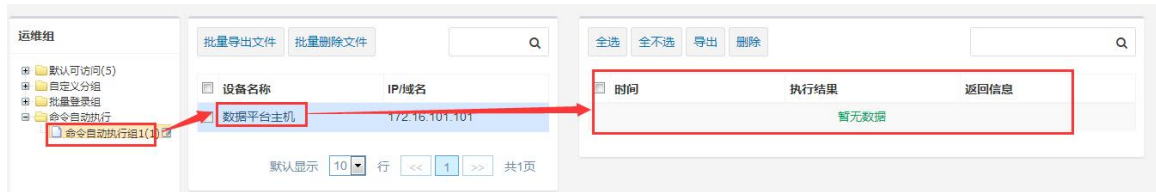
命令自动执行-选择资源

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。



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，并可将执行结果文件下载到本地计算机。



命令自动执行-执行结果

2.4.11 网络设备配置备份

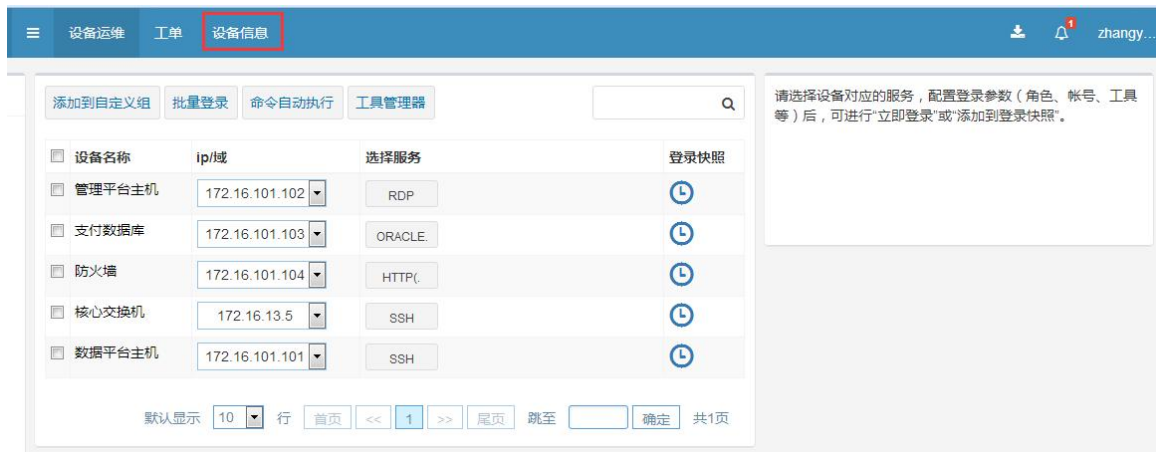
运维用户可对网络设备（交换机、路由器）的配置实现定期自动备份，并可下载到本地保存。

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
<input type="checkbox"/> 华为_default_SSH_1.0.3	华为	default	1.0.3	内置
<input type="checkbox"/> 华为_default_TELNET_1.0.3	华为	default	1.0.3	内置
<input type="checkbox"/> 华为3COM_default_SSH_1.0.3	华为3COM	default	1.0.3	内置
<input type="checkbox"/> 华为3COM_default_TELNET_1.0.3	华为3COM	default	1.0.3	内置
<input type="checkbox"/> 思科_default_SSH_1.0.3	思科	default	1.0.3	内置
<input type="checkbox"/> 思科_default_TELNET_1.0.3	思科	default	1.0.3	内置

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”。如图所示：



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”。如图所示：



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。如图所示：



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，并可将执行结果文件下载到本地计算机。



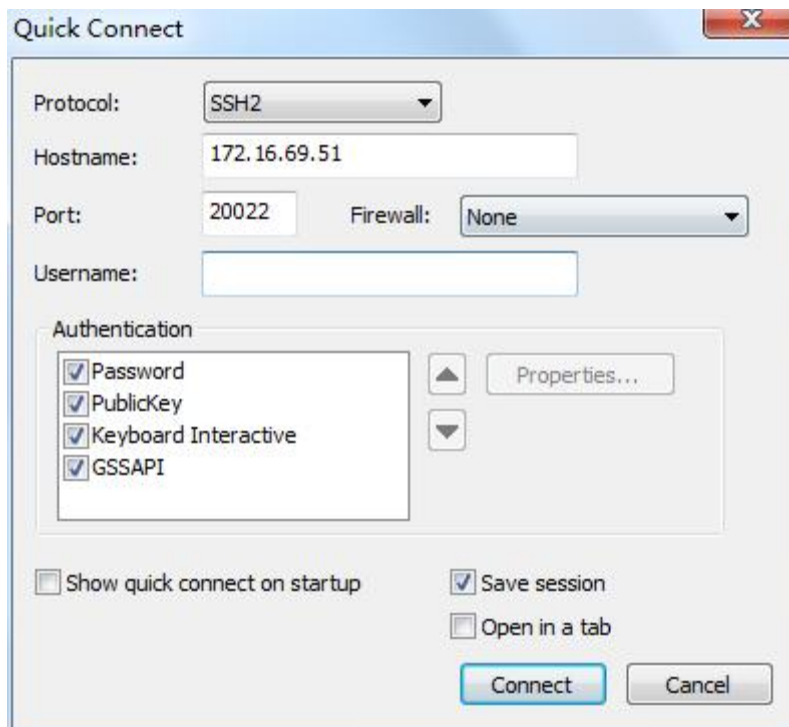
网络设备配置备份-执行结果

2.5 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 客户端工具直连天玑运维安全网关来进行安全运维，能支持运维的协议包括 SSH、TELNET、RDP 和 VNC。

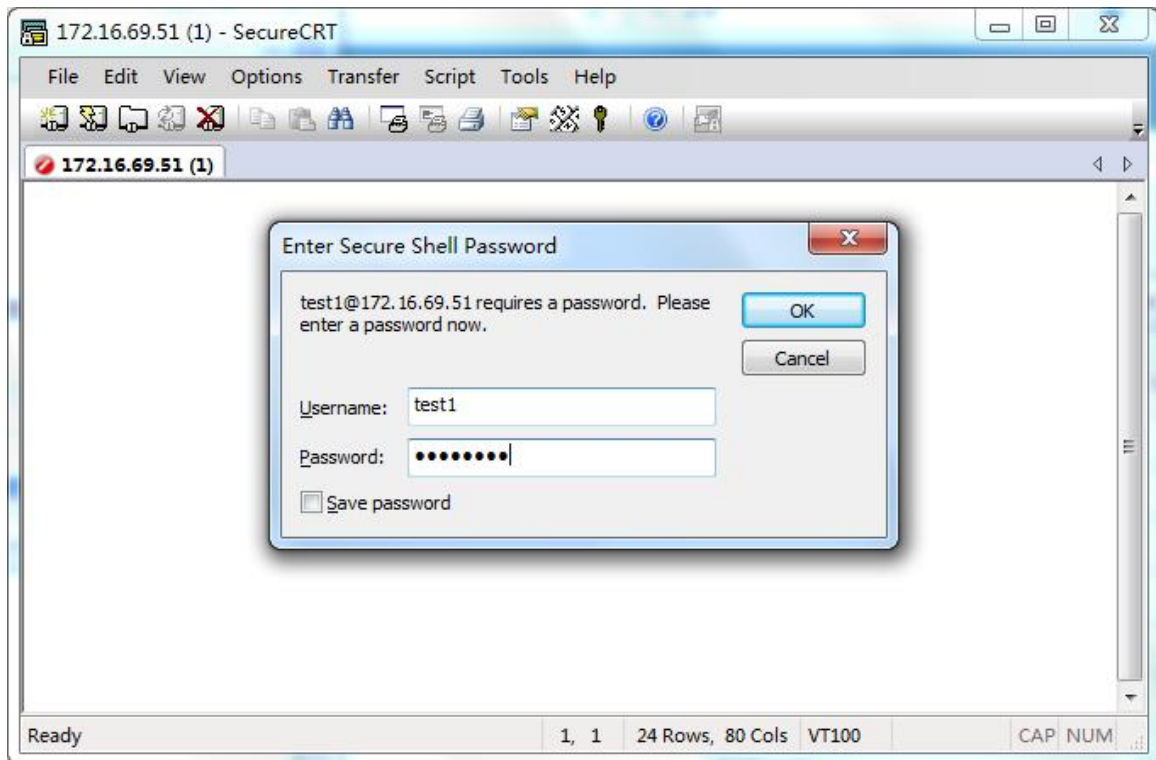
2.5.1 命令行方式

首先通过 SecureCRT 工具（也支持其他字符协议连接工具）连接天玑运维安全网关，主机名为天玑运维安全网关 V6.0 管理 IP 地址，端口号为 20022，如图所示：



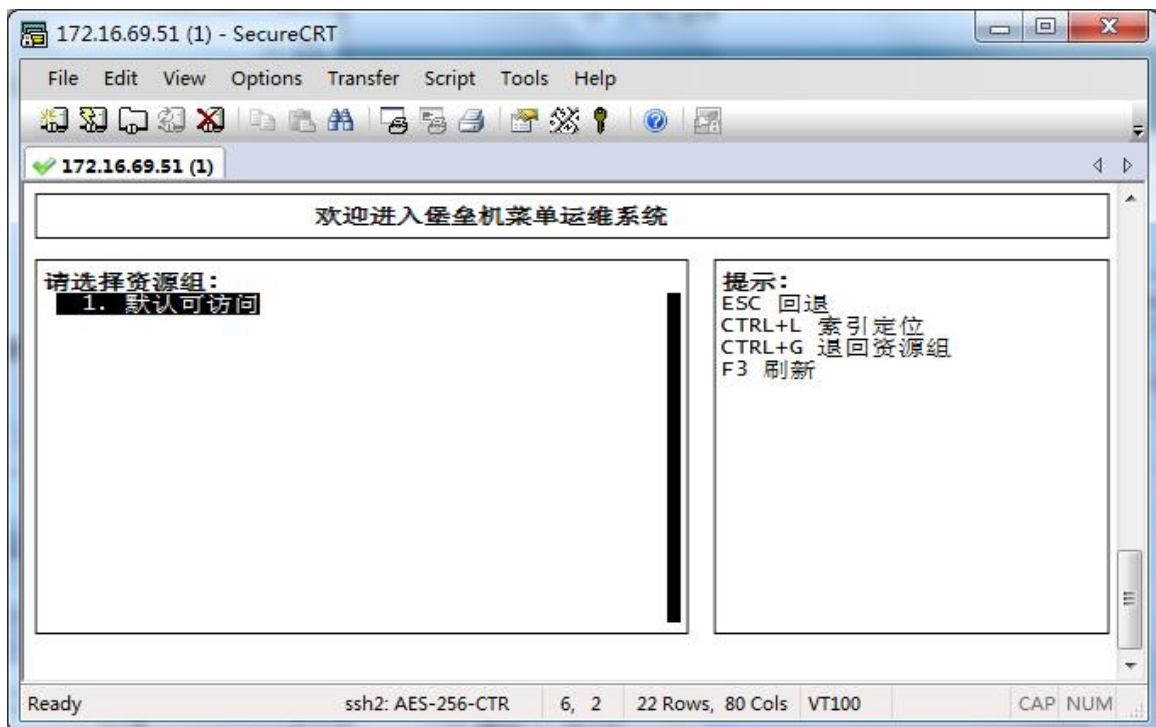
连接天玑运维安全网关 V6.0

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，如图所示：

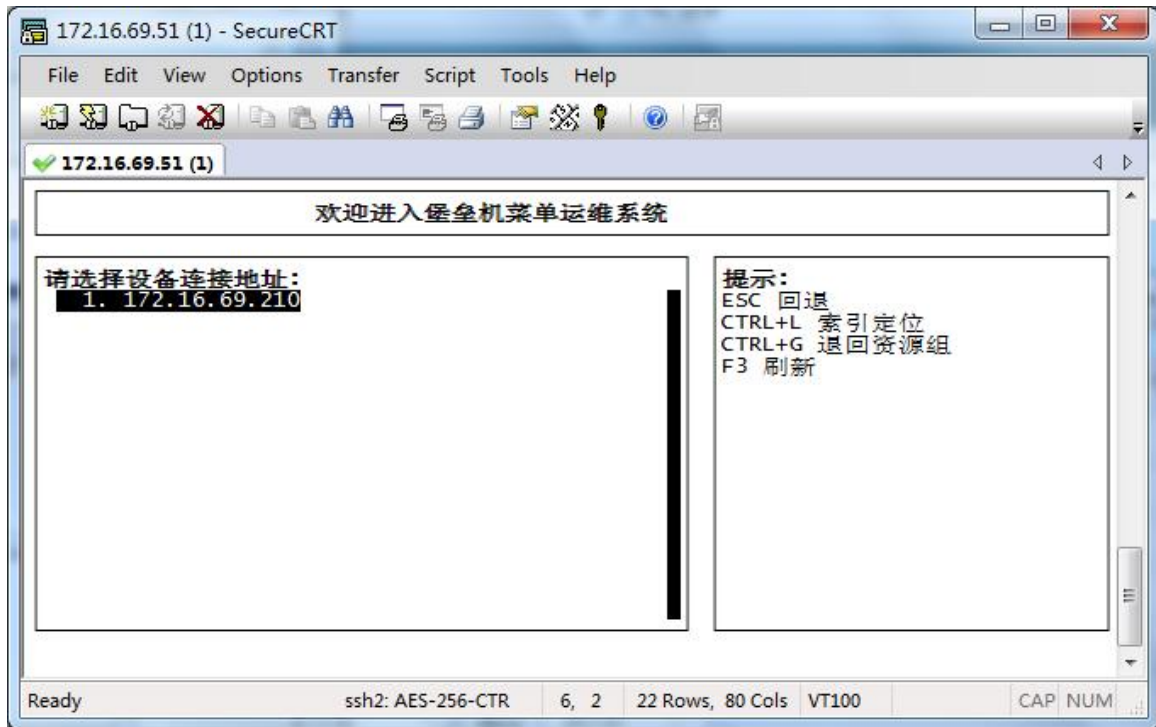


登录天玑运维安全网关 V6.0

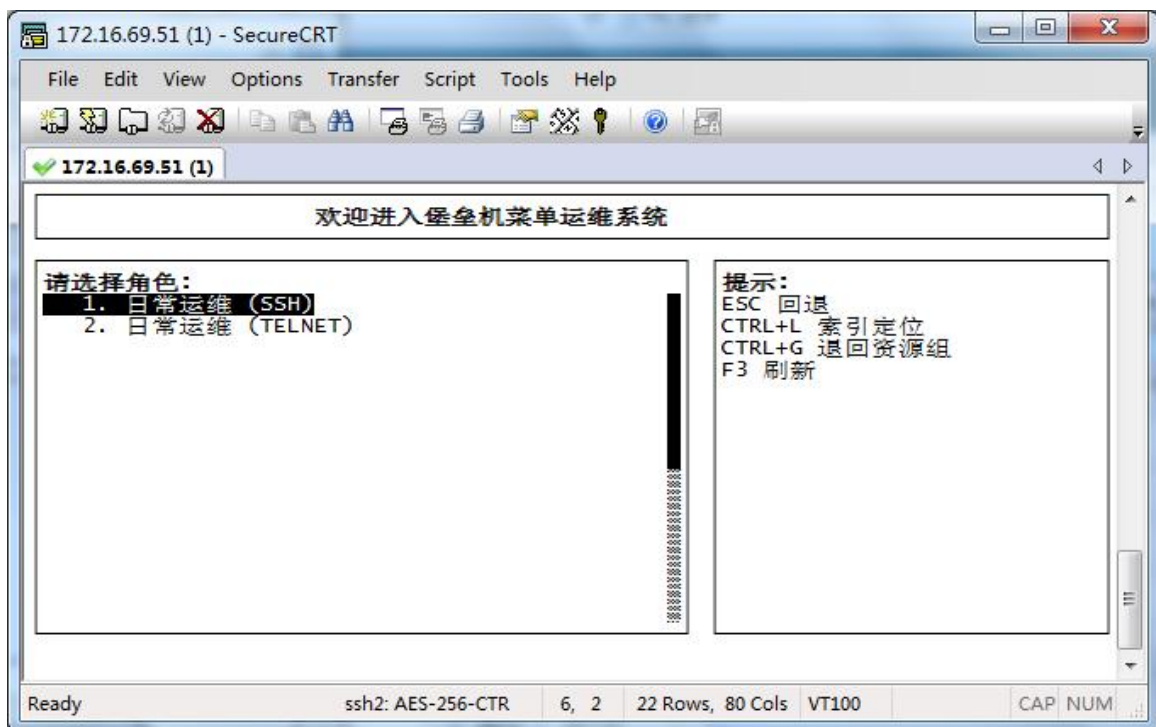
进入菜单管理界面后，运维用户可以开始选择运维资源。其中“Enter”键为确定，“Esc”键为返回，如图所示：



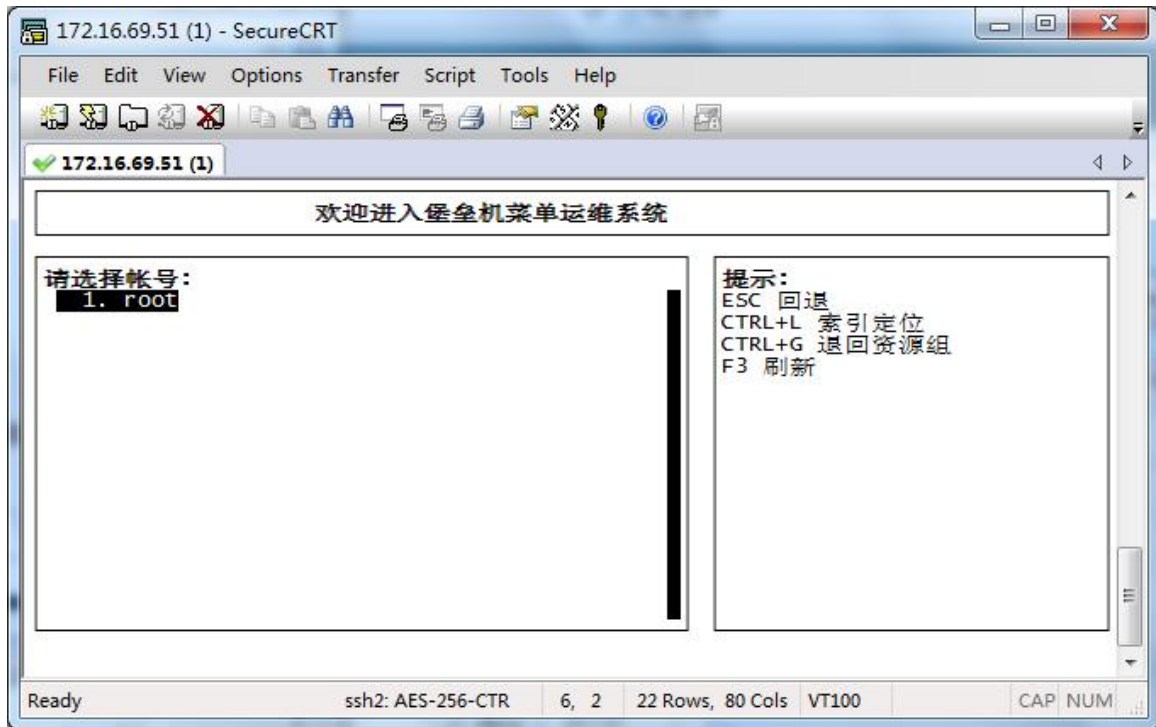
选择资源组



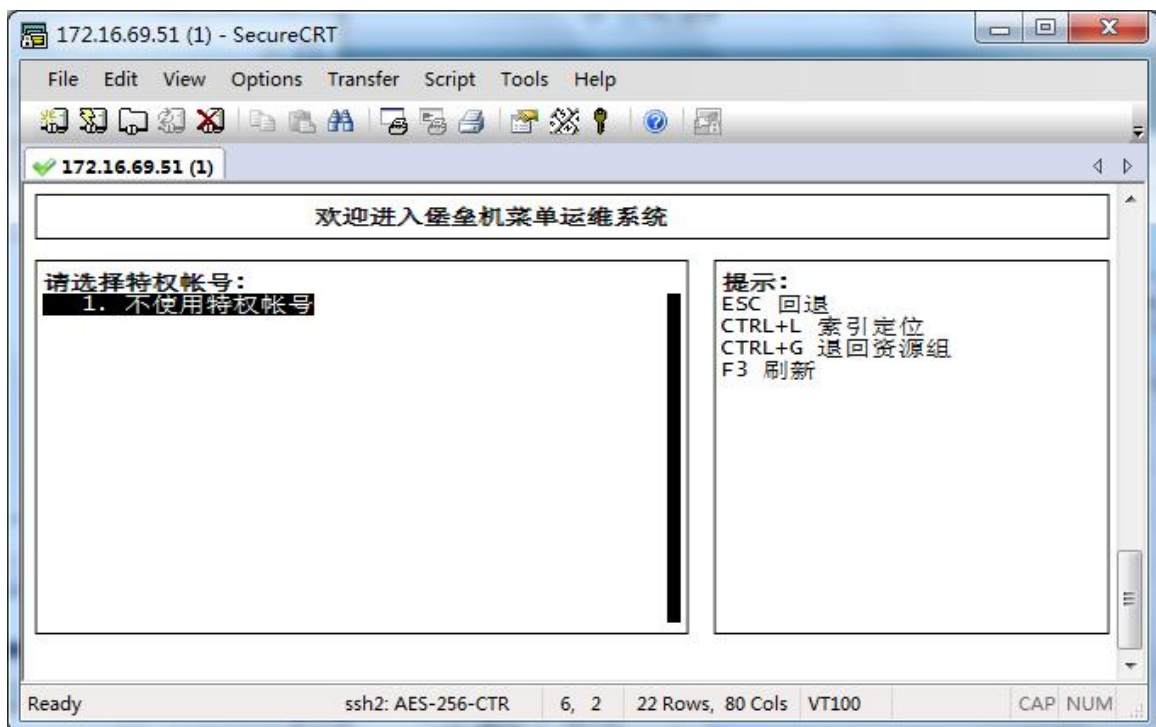
选择资源主机



选择角色

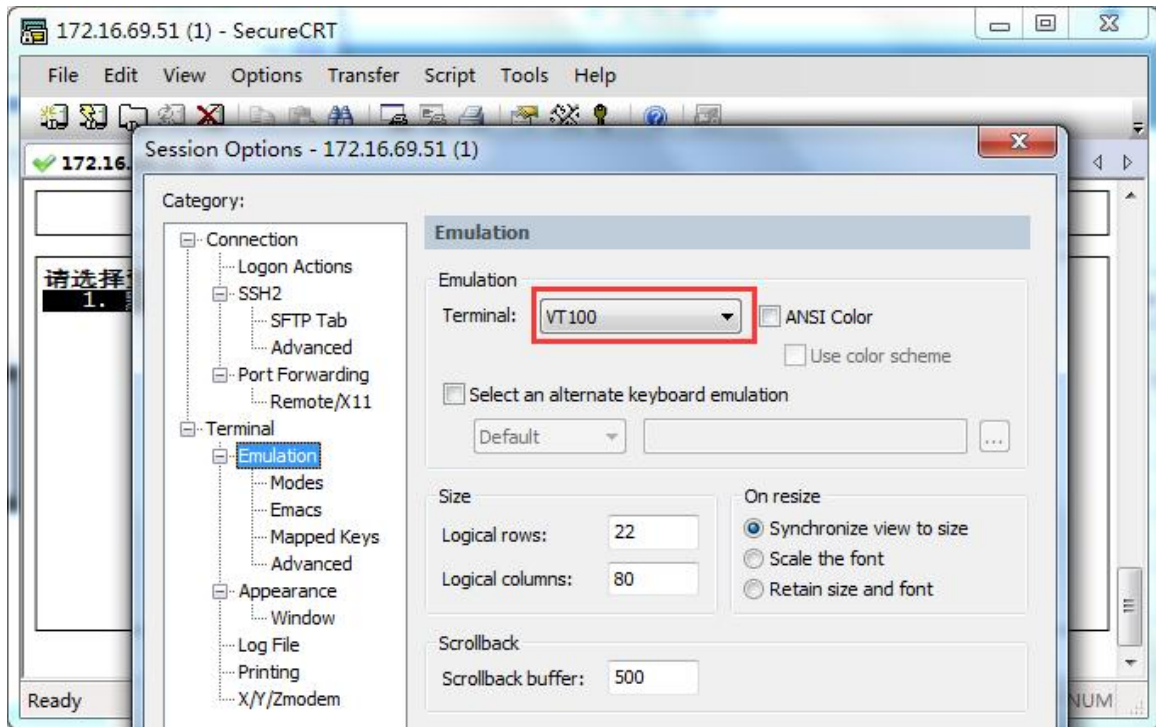


选择帐号



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），如图所示：



终端类型



终端编码

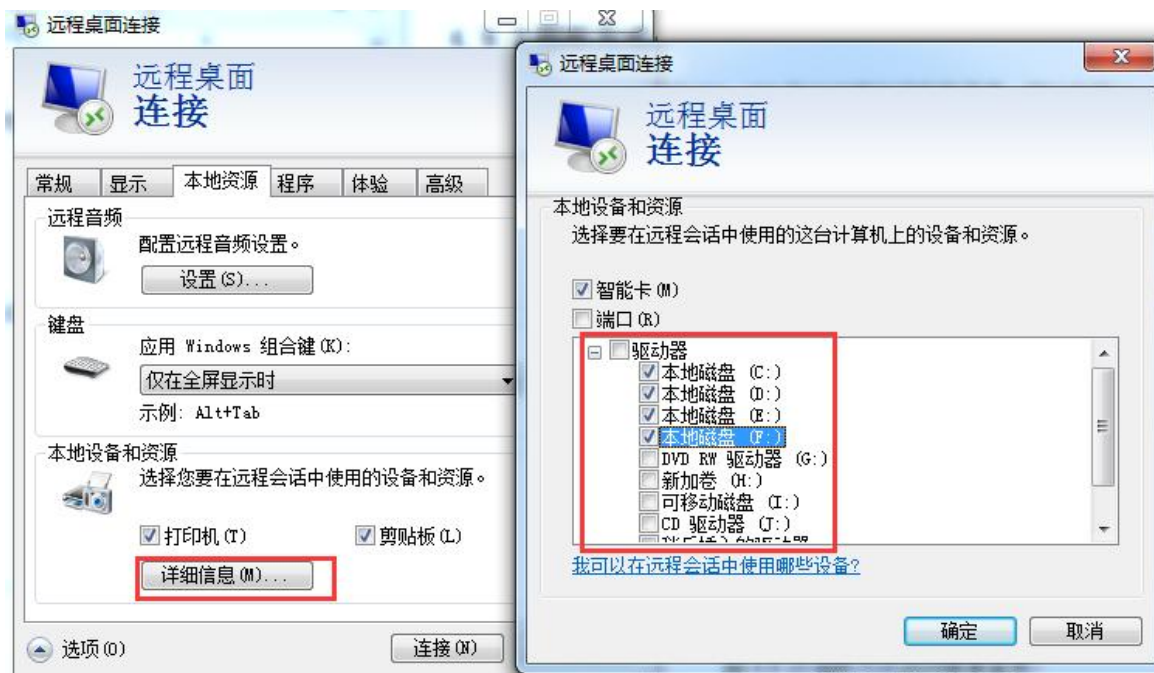
2.5.2 图形方式

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。如图所示，直接输入天玥运维安全网关 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，如图所示。



图形方式访问菜单登录



开启磁盘映射

输入运维账号、密码，如图所示。



堡垒机登录

认证源

用户名

密 码

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。



资源列表 - test1

设备组

设 备

地 址

服 务

角 色

帐 号

资源菜单

3 MACOS 使用说明

3.1 系统登录

用户通过浏览器访问天玑运维安全网关系统，登录 URL 地址默认为：<https://天玑运维安全网关的 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。

推荐操作系统： 10.14、10.15、10.13.6、11.6.1、12.0.1

推荐浏览器：Safari 浏览器(操作系统自带)。

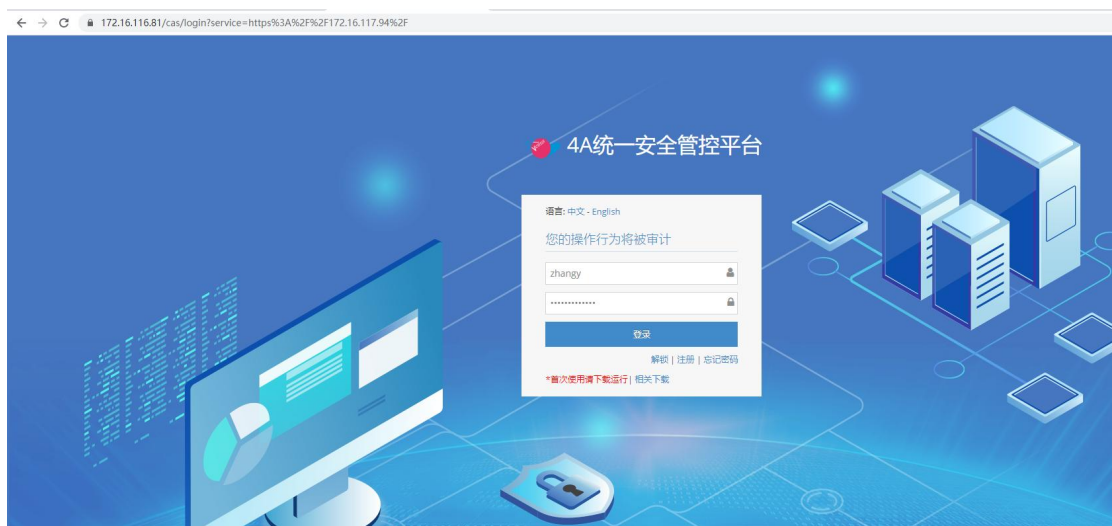


系统登录界面



运维界面

如果配置了 CAS 单点登录，输入 <https://天玥运维安全网关的 IP 地址> 后会跳转到 cas 服务器登录页，输入用户名和密码认证成功后进入天玥运维安全网关运维界面



跳转到 cas 服务器登录页



认证成功进入运维页

3.2 环境配置

用户在使用天玥运维安全网关对资源进行运维之前，需安装基础控件、根据运维需求在本地安装所需运维工具，推荐工具版本如下：

本地运维工具	工具名称	推荐版本
	Openssh	系统自带
	SecureCRT	8.3.3
	FileZilla	3.46.0
	MSTSC	10.2.0
	SecureFX	8.3.3
	MYSQL	11.6
	dbvisualizer	9.2.6
	Navicat	12.1.27

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。



登录界面-相关下载

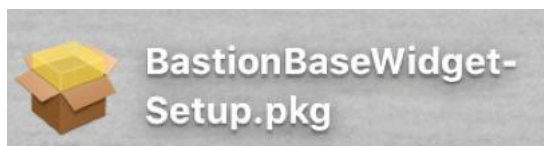
操作步骤

步骤 1 下载基础控件



下载基础控件

步骤 2 双击基础控件安装



基础控件安装包

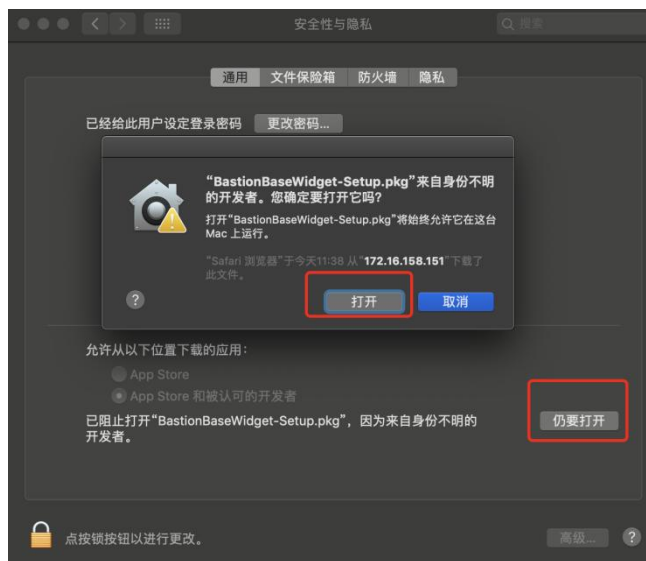
步骤 3 出现安全性提示，需要在系统偏好设置-安全性与隐私-通用，仍要打开



安全性提示

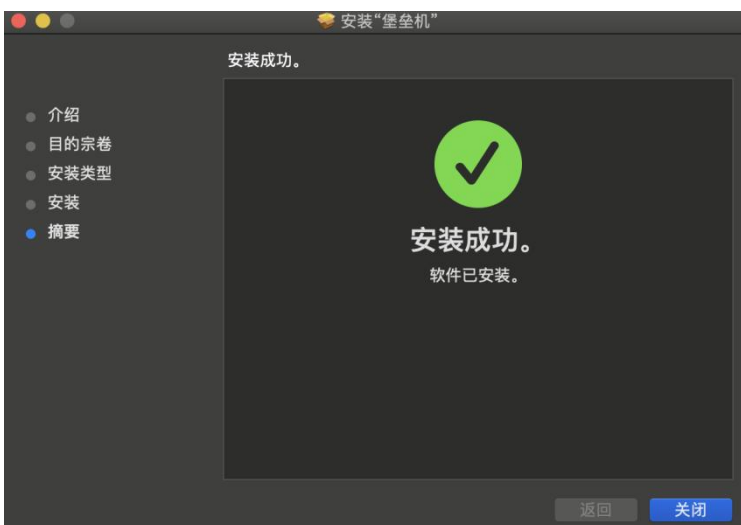
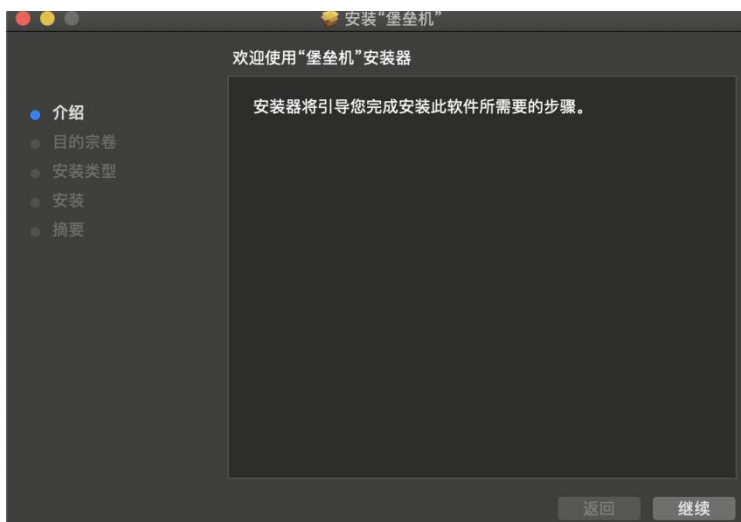


系统偏好设置



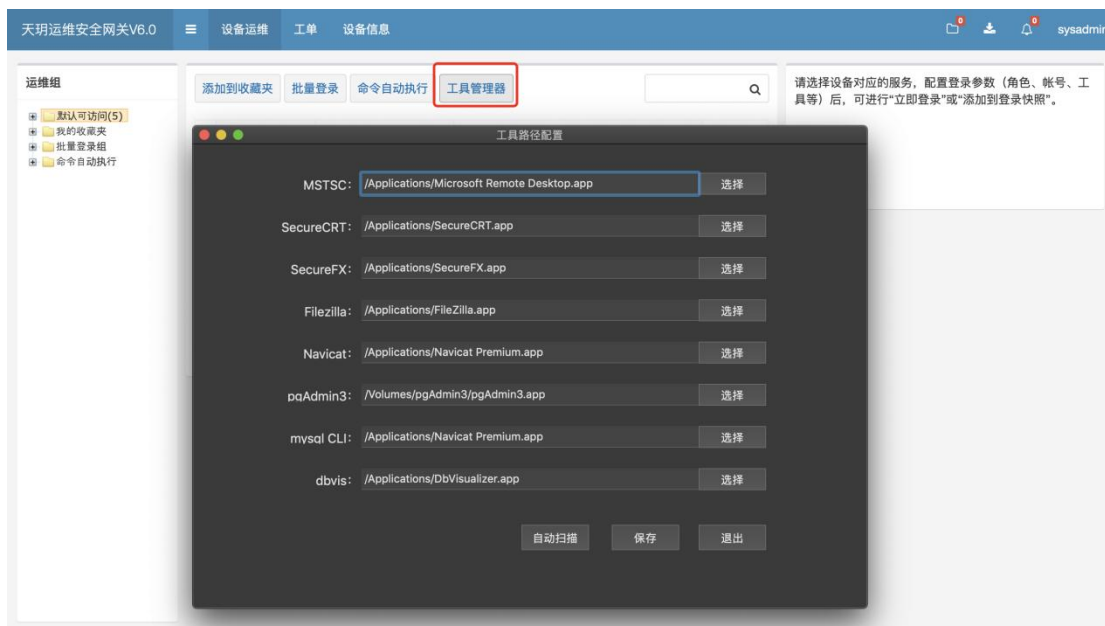
安全性隐私

步骤 4 开始安装，全程默认安装即可安装完成



步骤 5 配置运维工具路径

运维界面单击“工具管理器”进行工具路径配置，支持自动扫描和手动配置。



运行工具路径配置

3.3 运维说明

3.3.1 RDP/VNC 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

步骤2 选择登录配置

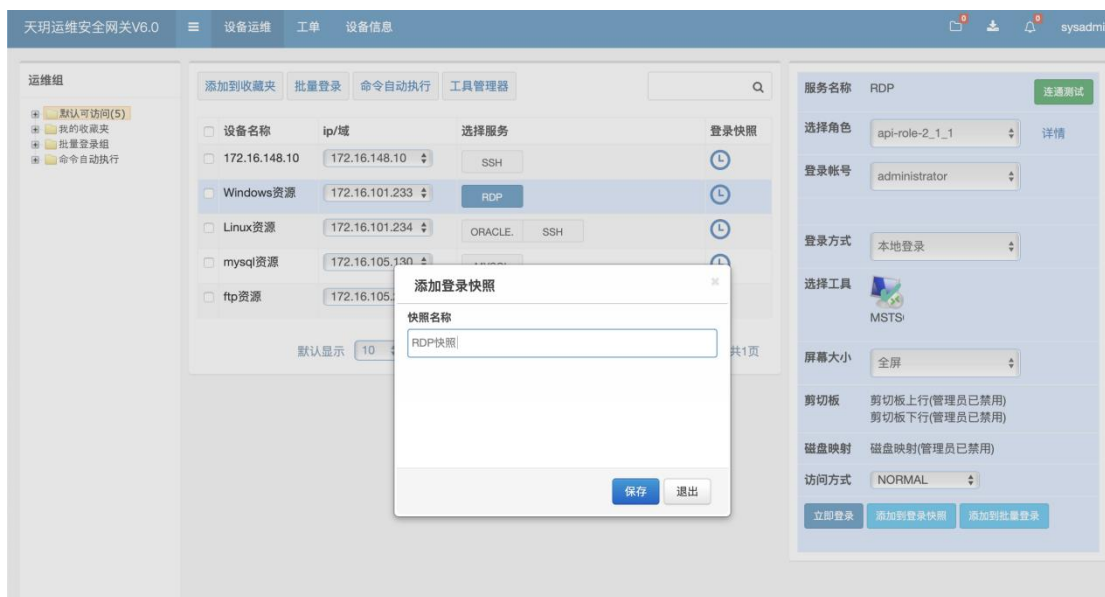
选择需要运维的 RDP 或 VNC 资源。



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。

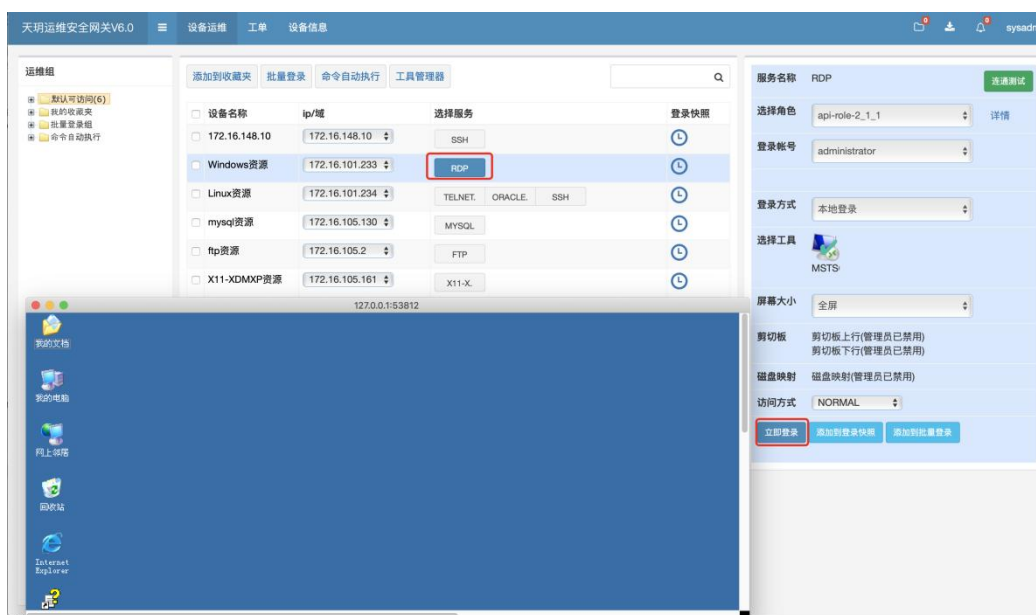
选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



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”，即可连接资源。



图形协议运维-立即登录连接资源

3.3.2 TELNET/SSH 访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

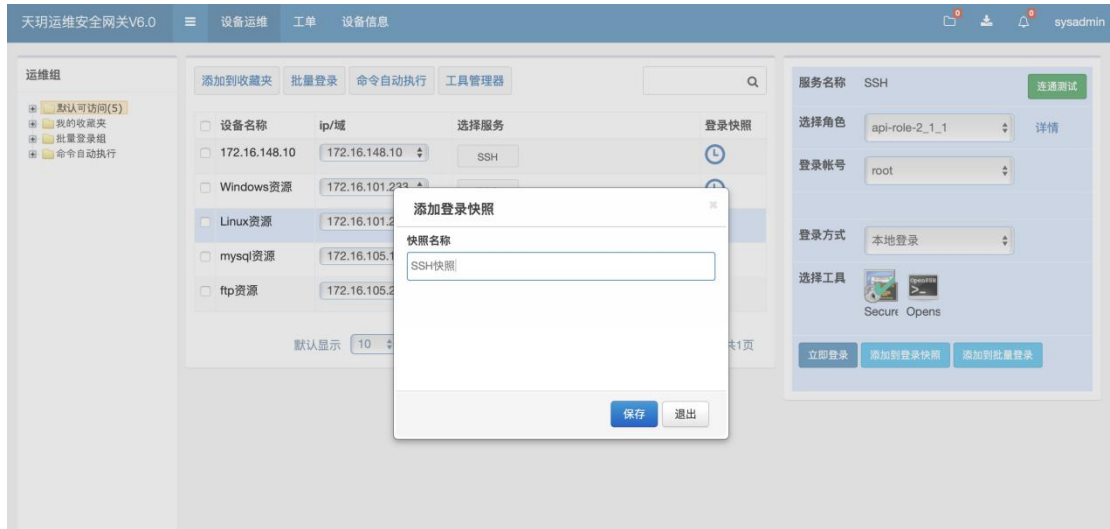
步骤 2 选择登录配置

选择需要运维的 SSH 或 TELNET 资源。



字符协议运维

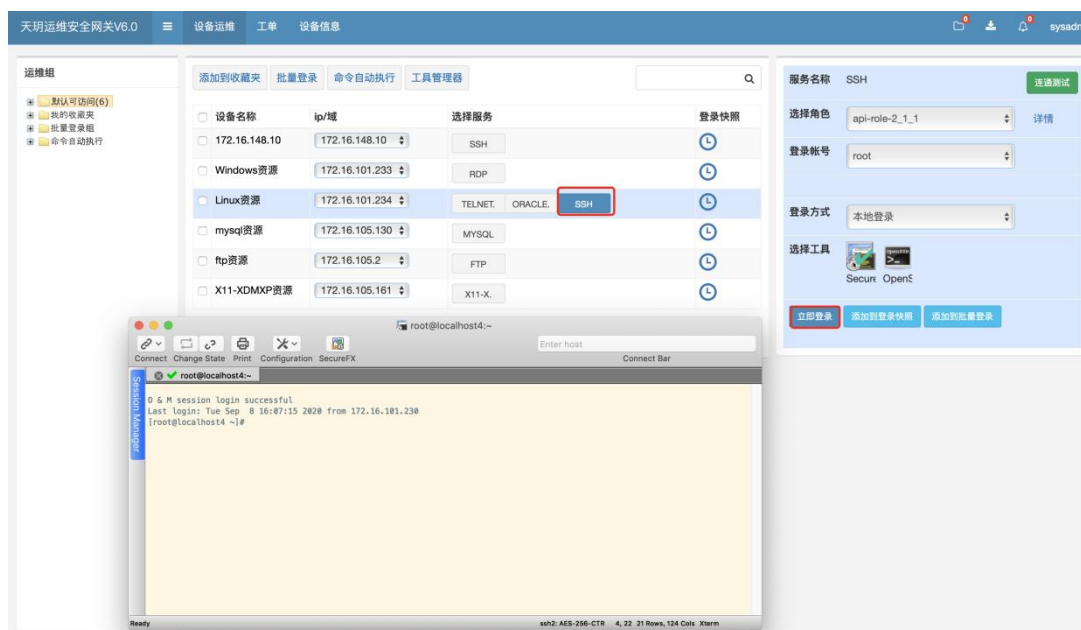
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



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”，即可连接资源。



字符协议运维-立即登录连接资源

3.3.3 FTP 访问

操作步骤

步骤1 进入设备运维页面

运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

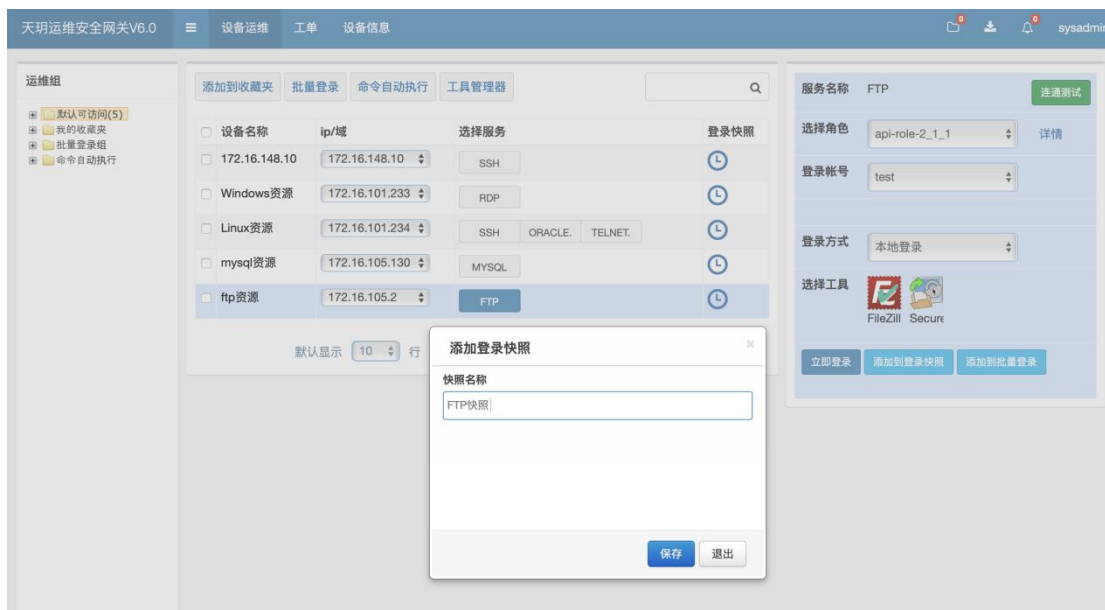
步骤2 选择登录配置

选择需要运维的 FTP 资源。



文件传输协议运维

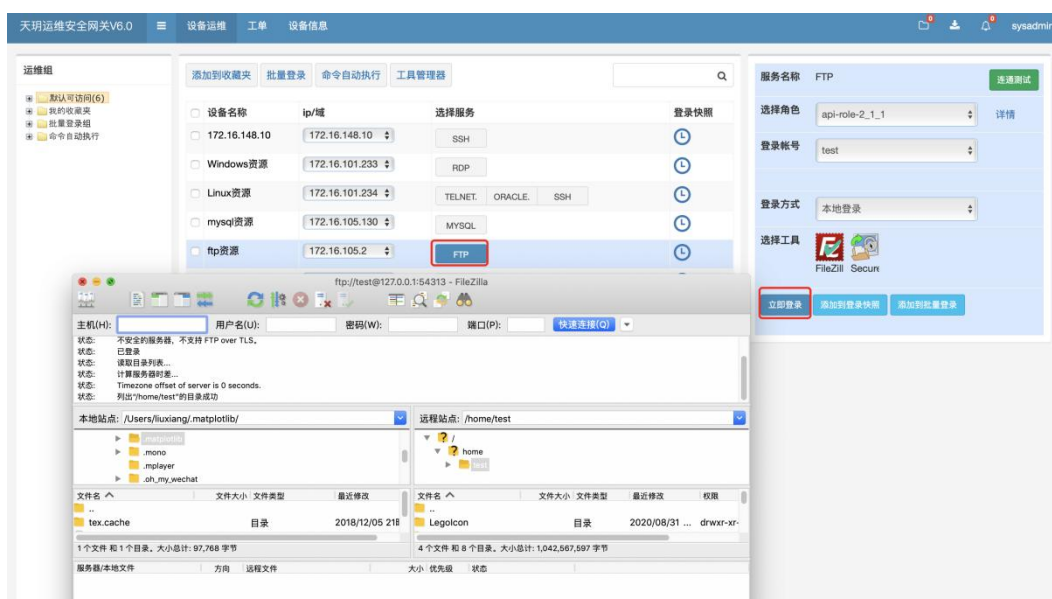
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



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”，即可连接资源。



文件传输协议运维-立即登录连接资源

3.3.4 数据库访问

操作步骤

步骤 1 进入设备运维页面

运维用户登录天玥运维安全网关控制台，选择“设备运维”。



设备运维

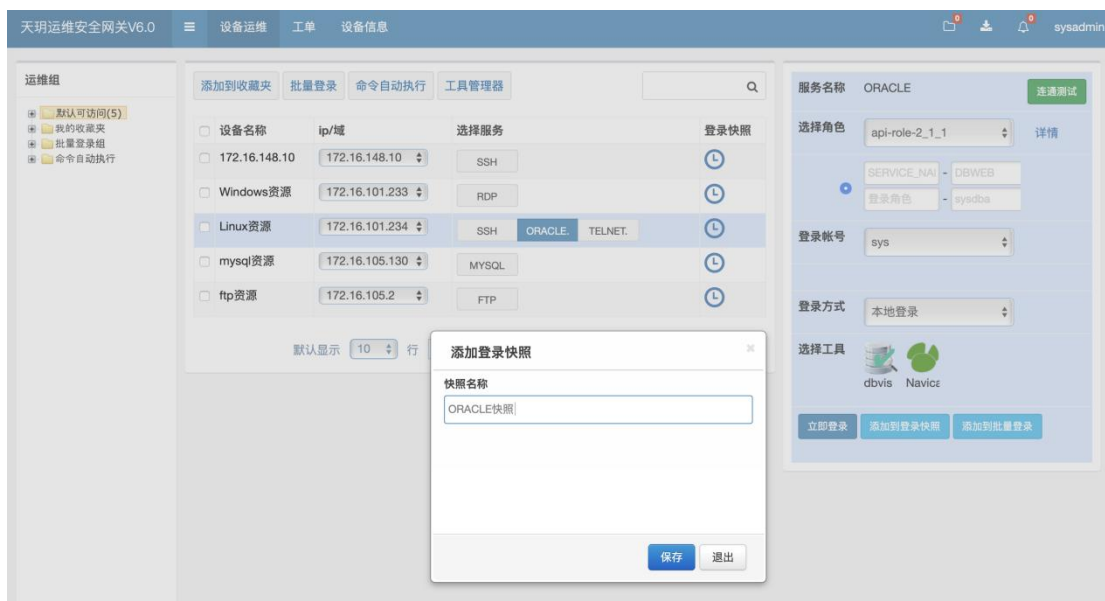
步骤 2 选择登录配置

选择需要运维的数据库资源。



数据库协议运维

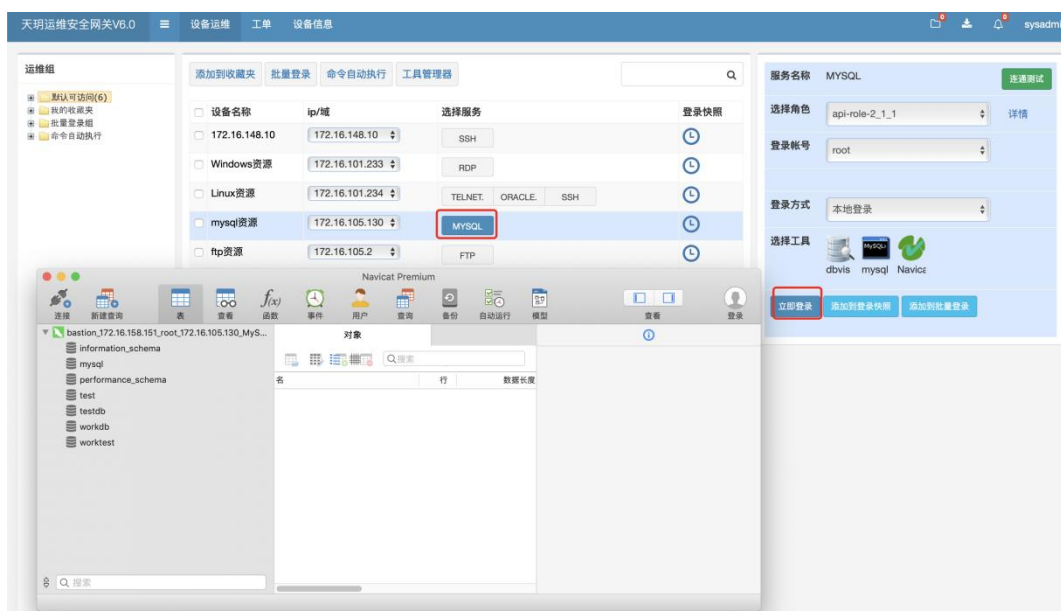
根据实际情况选择运维设备、服务、角色、登录帐号、登录方式、工具等。选择完毕后可选择“立即登录”和“添加到登录快照”：“立即登录”-配置完成后直接登录；“添加到登录快照”-保存本次配置（下次登录时可以直接选择登录快照进行快速登录）。



数据库协议运维-添加登录快照

步骤 3 进行运维登录

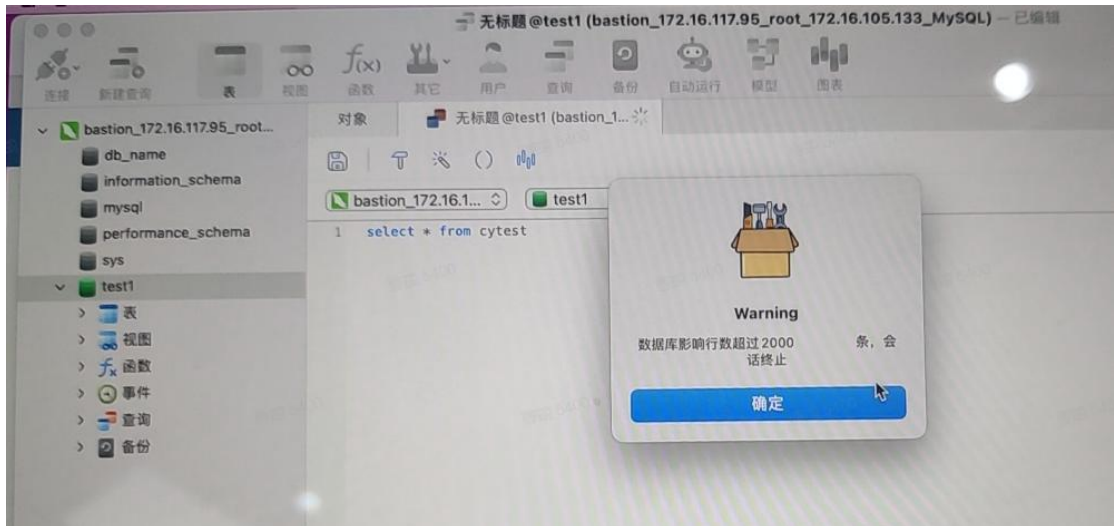
确认登录配置后，单击“立即登录”，即可连接资源。



数据库协议运维-立即登录连接资源

步骤 4 数据策略触发

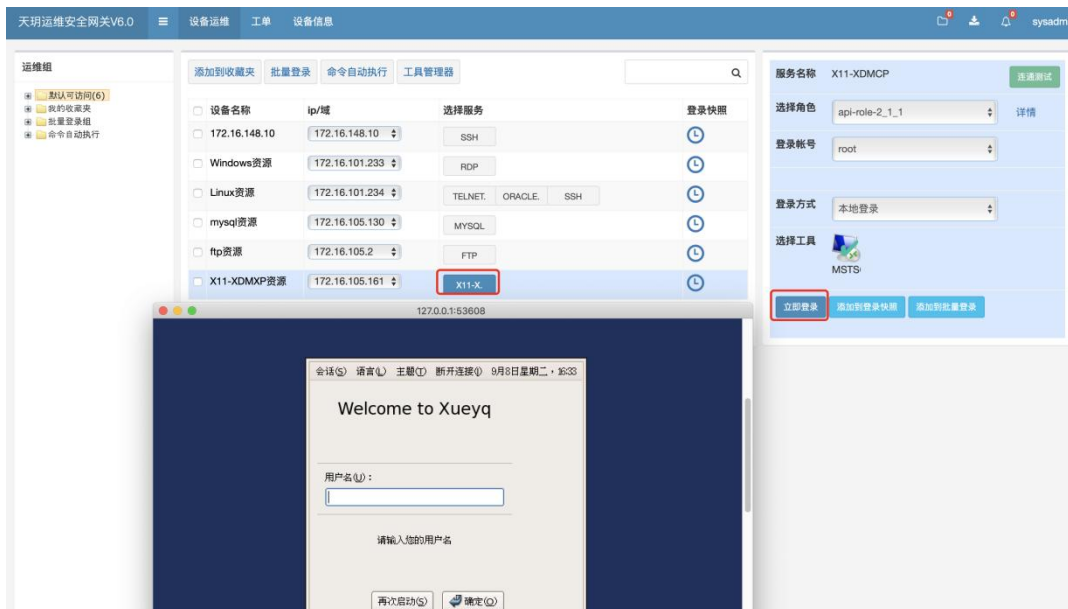
当执行数据库命令影响行数超过设置的条数时，执行日志告警或者会话阻断。



会话阻断

3.3.5 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。**



X11-XDMCP 访问

3.3.6 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：

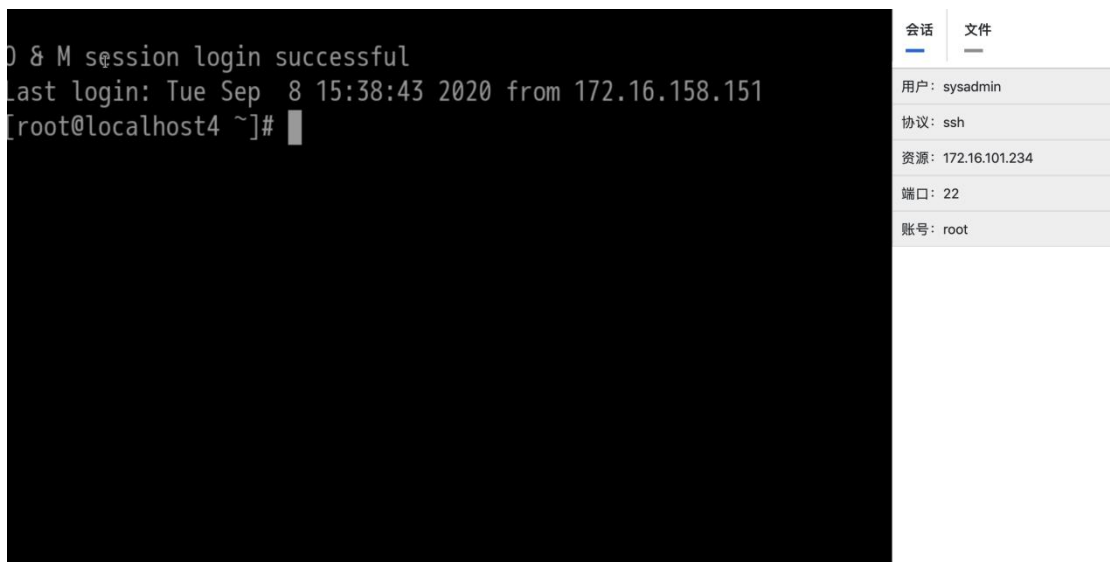
注意事项：

- (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。



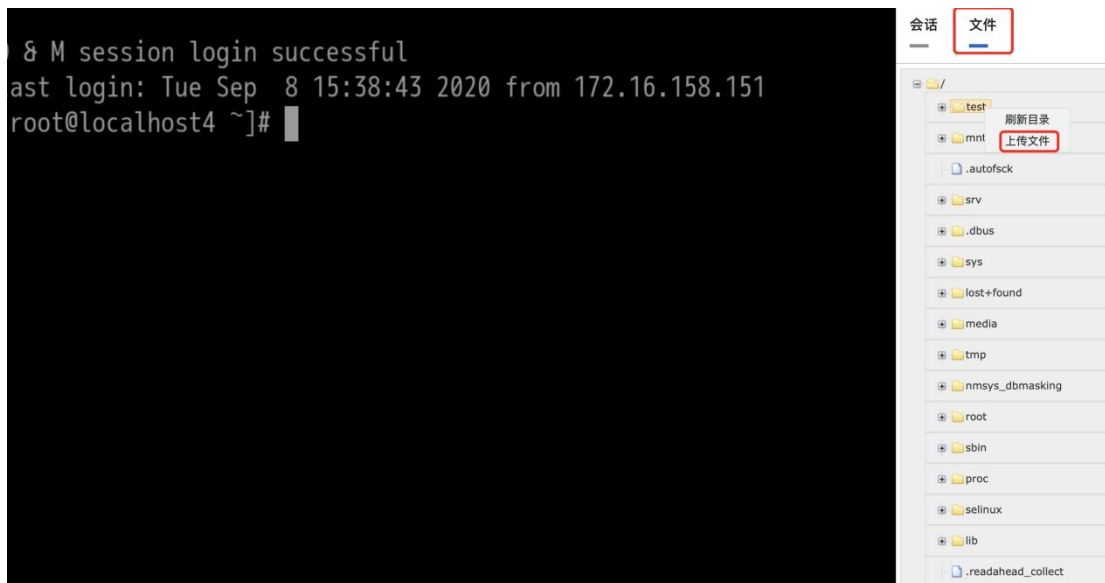
HTML5 运维登陆

如果第一次连接资源失败，请重新连接一次。如图所示：



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。如图所示：



HTML5 运维文件上传

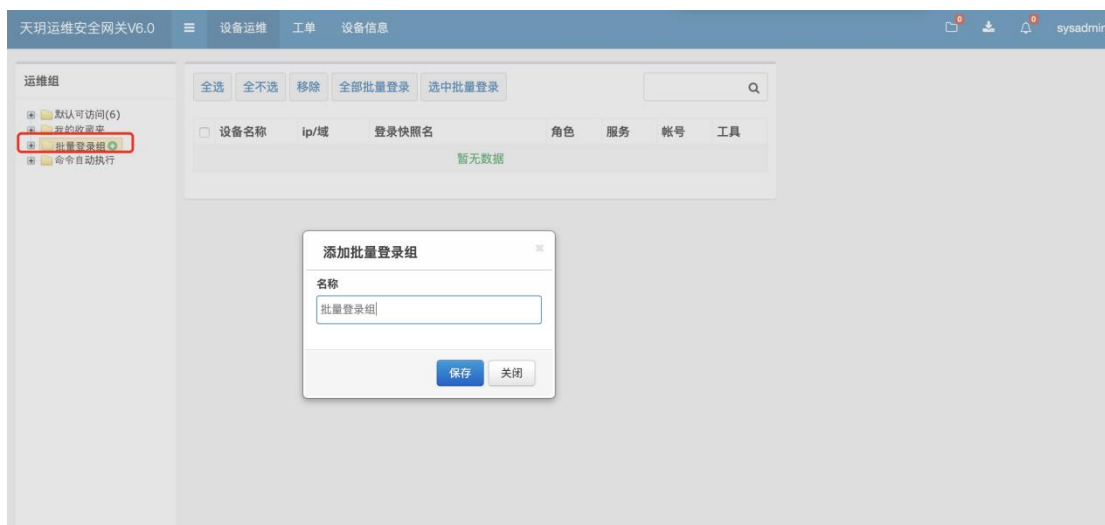
3.3.7 批量登录

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

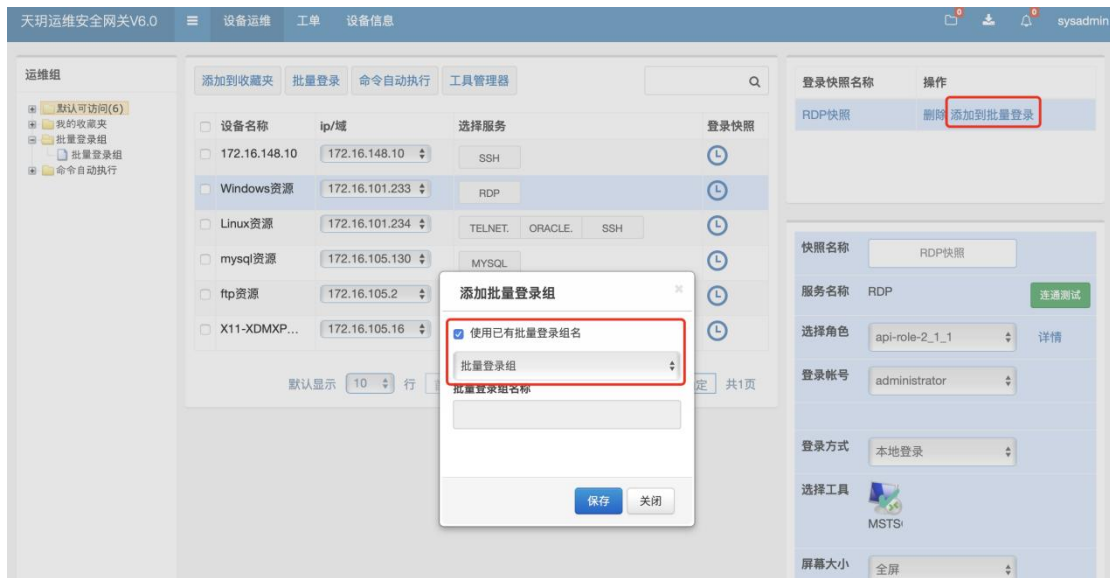
运维用户根据实际需求添加批量登录组。



批量登录（一）

步骤 2 添加登录快照到批量登录组

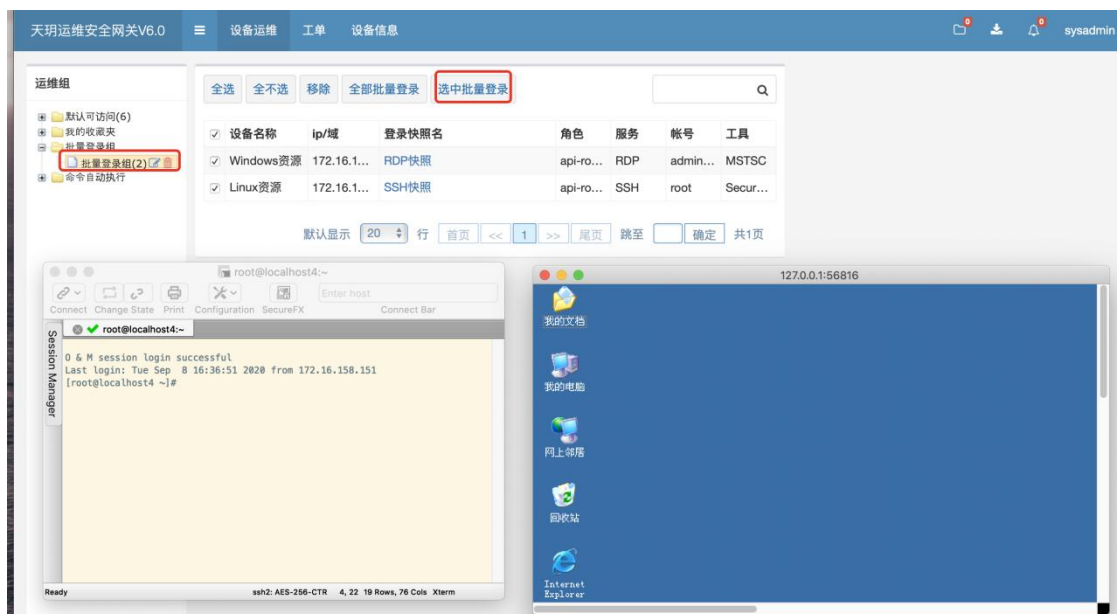
运维人员需要设置登录快照，再将登录快照添加到批量登录组。



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”。



批量登录（三）

3.3.8 运维工单

3.3.8.1 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。

工单申请

3.3.8.2 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。

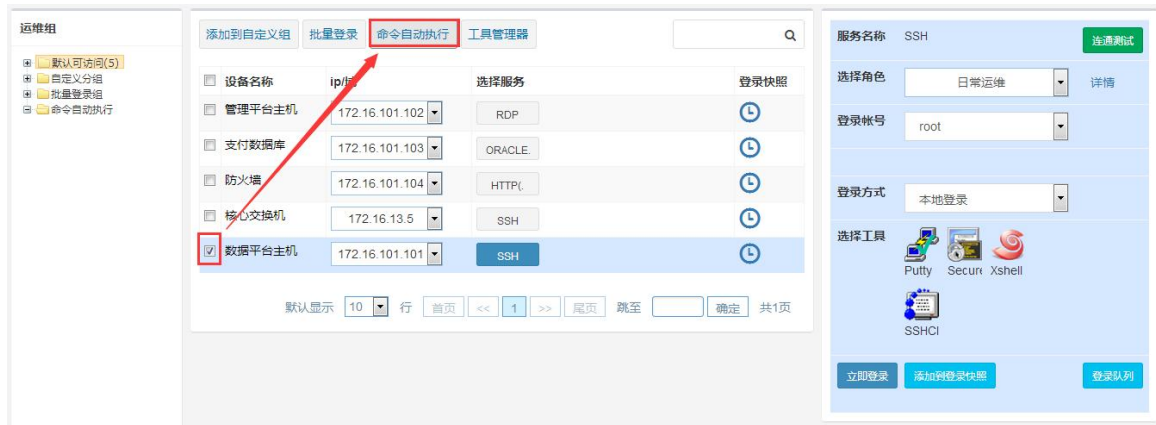
工单资源运维

3.3.9 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

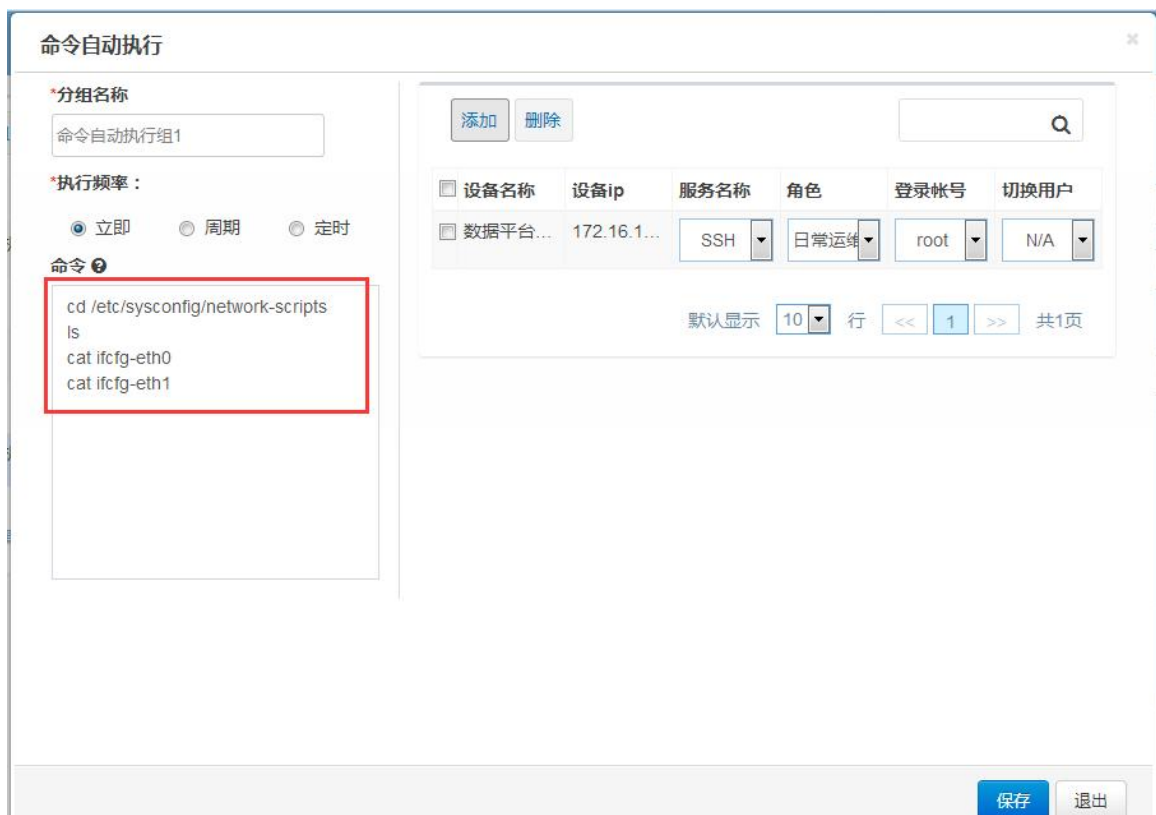
果。

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”，如图所示。



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。



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,并可将执行结果文件下载到本地计算机。



命令自动执行-执行结果

3.3.10 网络设备配置备份

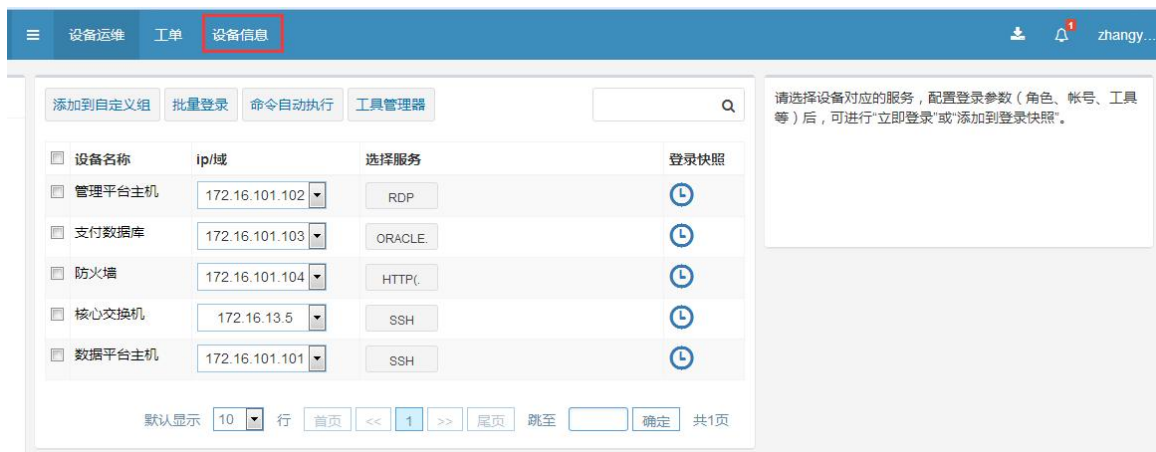
运维用户可对网络设备（交换机、路由器）的配置实现定期自动备份,并可下载到本地保存。

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
<input type="checkbox"/> 华为_default_SSH_1.0.3	华为	default	1.0.3	内置
<input type="checkbox"/> 华为_default_TELNET_1.0.3	华为	default	1.0.3	内置
<input type="checkbox"/> 华为3COM_default_SSH_1.0.3	华为3COM	default	1.0.3	内置
<input type="checkbox"/> 华为3COM_default_TELNET_1.0.3	华为3COM	default	1.0.3	内置
<input type="checkbox"/> 思科_default_SSH_1.0.3	思科	default	1.0.3	内置
<input type="checkbox"/> 思科_default_TELNET_1.0.3	思科	default	1.0.3	内置

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”。如图所示:



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”。如图所示:



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。如图所示：



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，并可将执行结果文件下载到本地计算机。



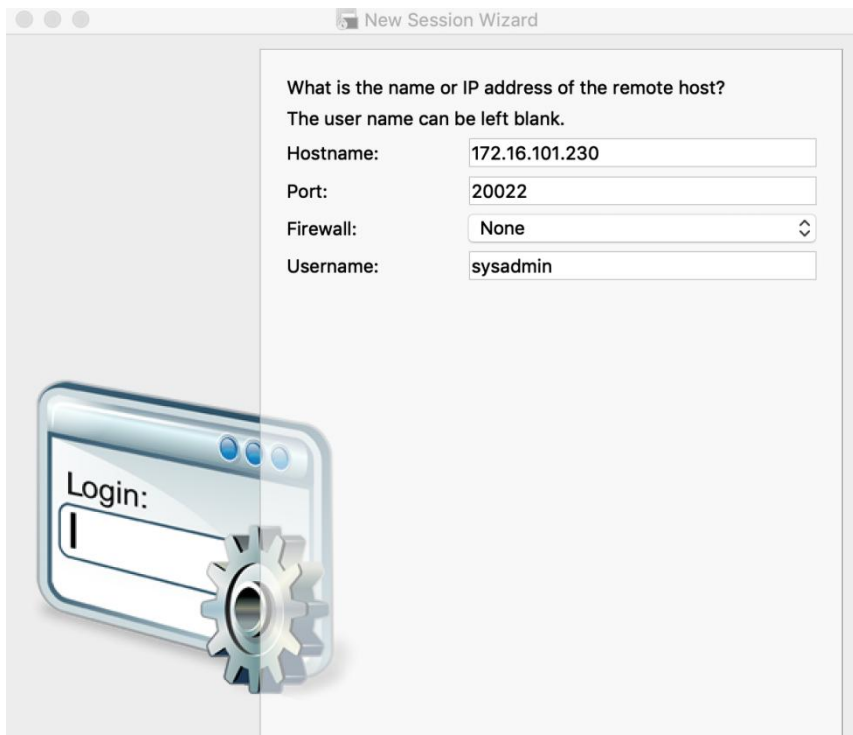
网络设备配置备份-执行结果

3.4 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 客户端工具直连天玑运维安全网关来进行安全运维，能支持运维的协议包括 SSH、TELNET、RDP 和 VNC。

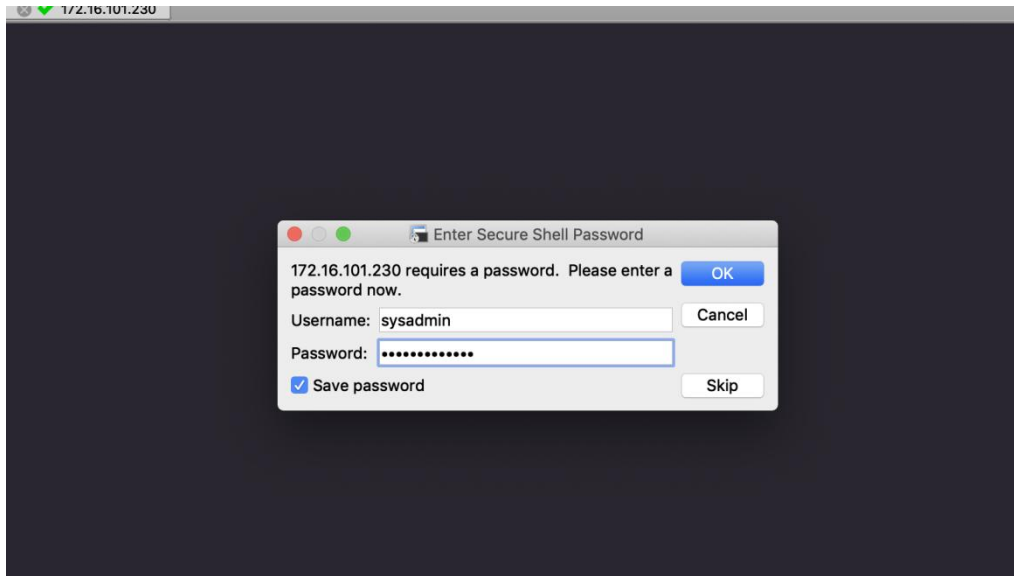
3.4.1 命令行方式

首先通过 SecureCRT 工具（也支持其他字符协议连接工具）连接天玑运维安全网关，主机名为天玑运维安全网关 V6.0 管理 IP 地址，端口号为 20022，如图所示：



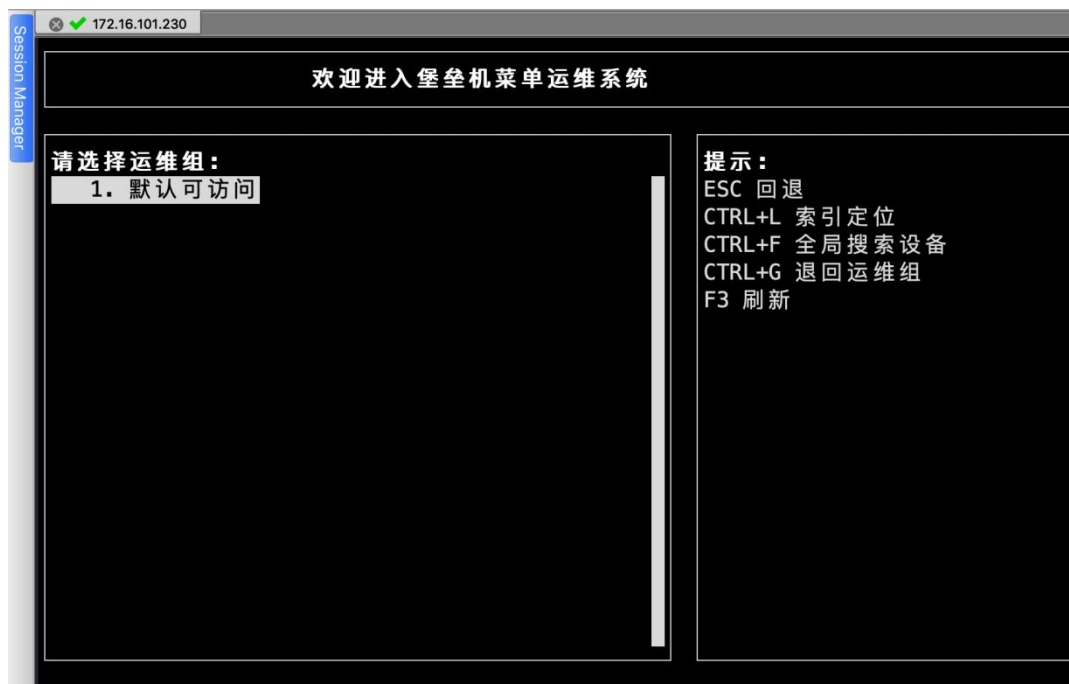
连接天玑运维安全网关 V6.0

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，如图所示：



登录天玥运维安全网关 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，如图所示：



选择资源组



选择设备



选择设备连接地址



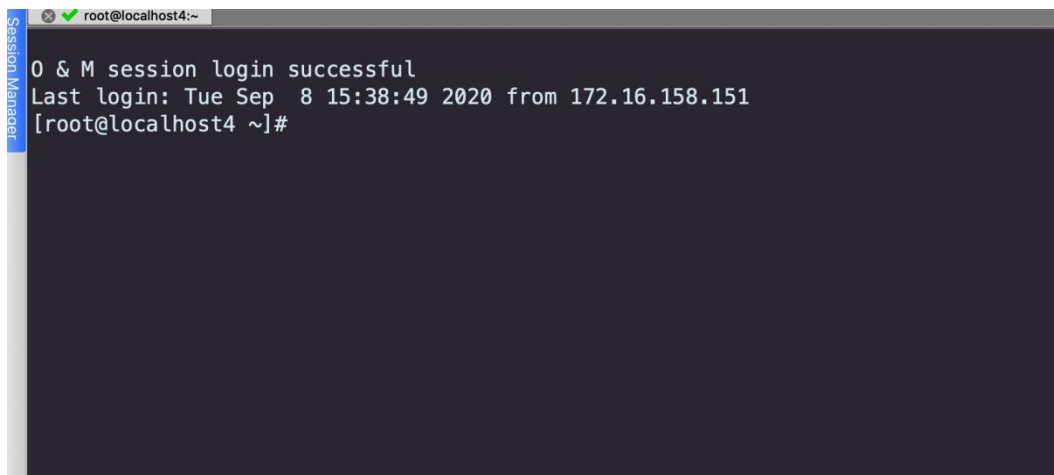
选择角色



选择帐号

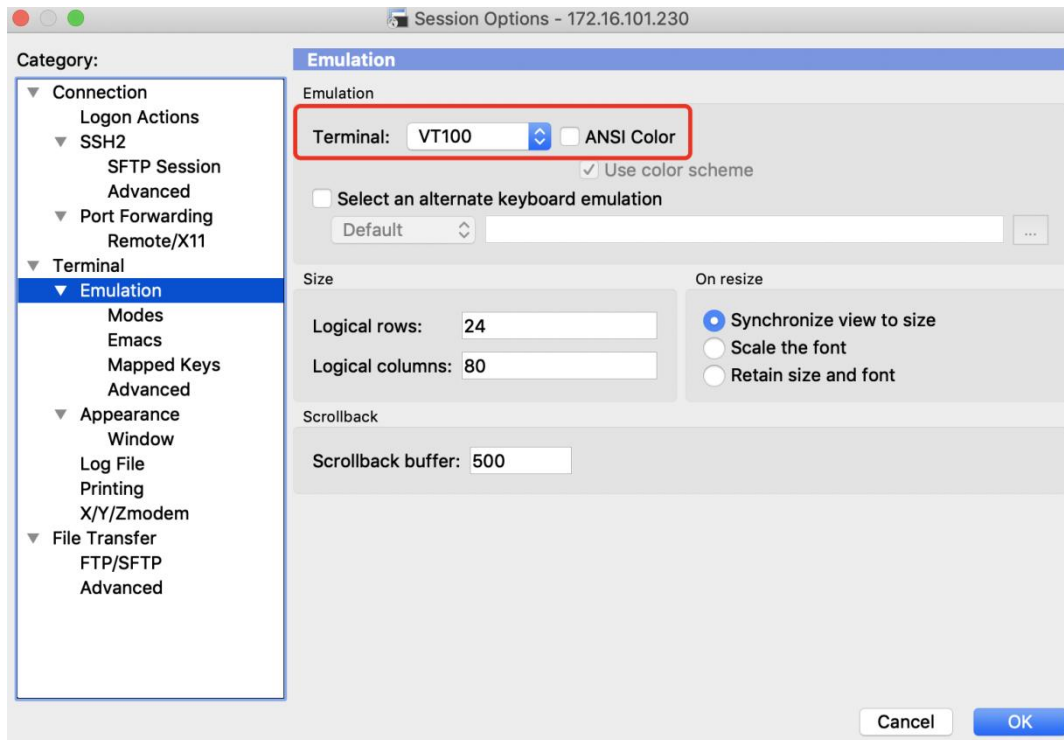


确认连接

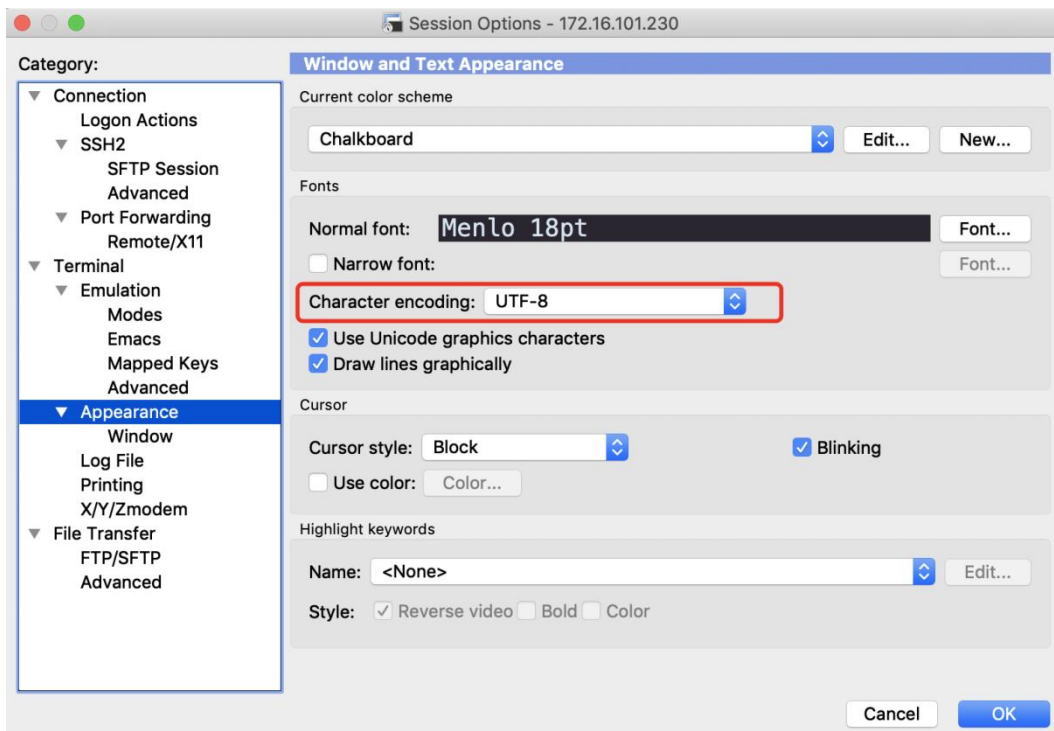


直连资源成功

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），如图所示：



终端类型

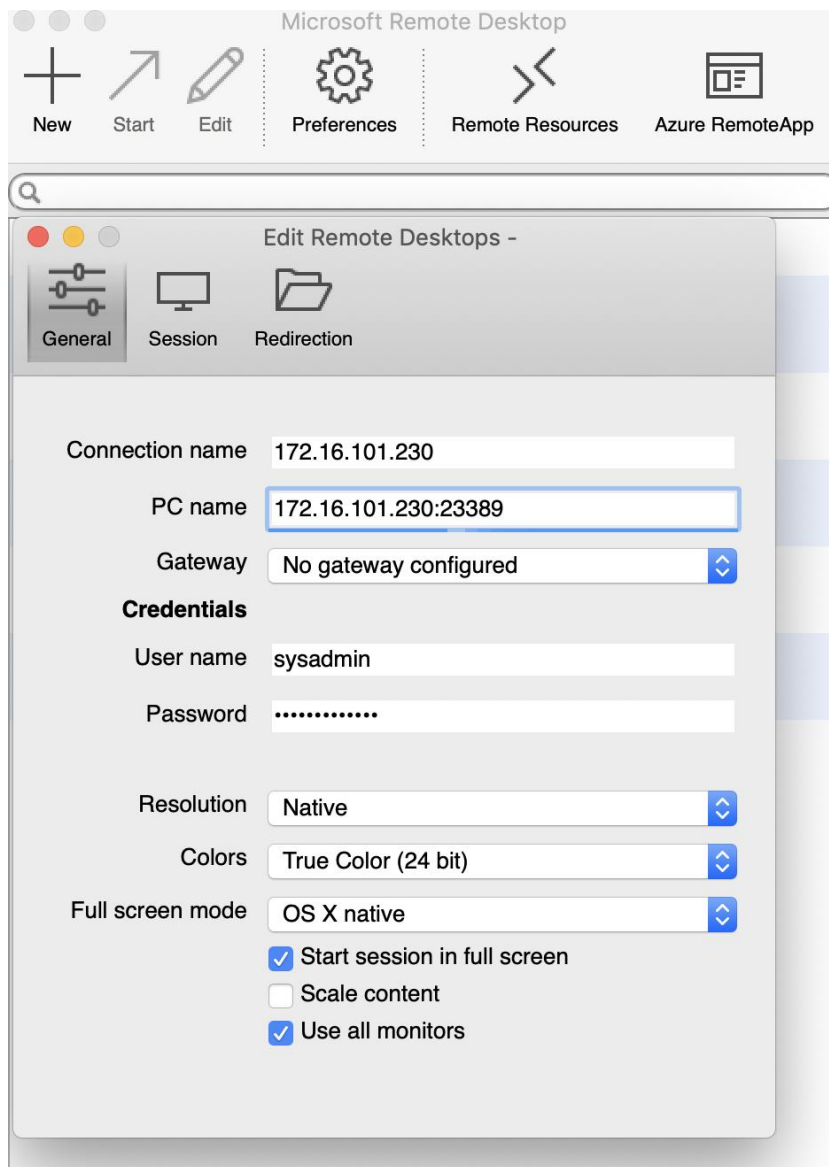


终端编码

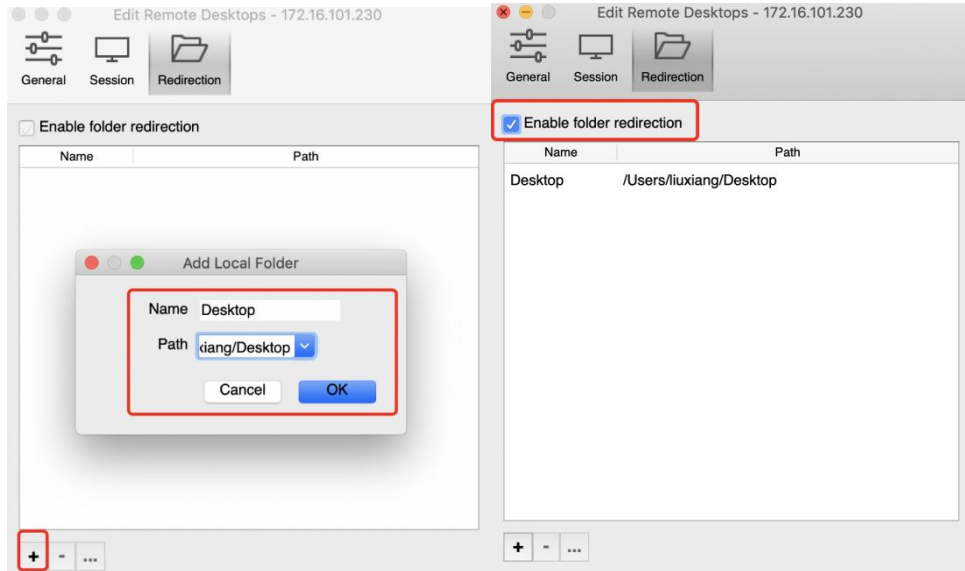
3.4.2 图形方式

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 MACOS 的远程桌面

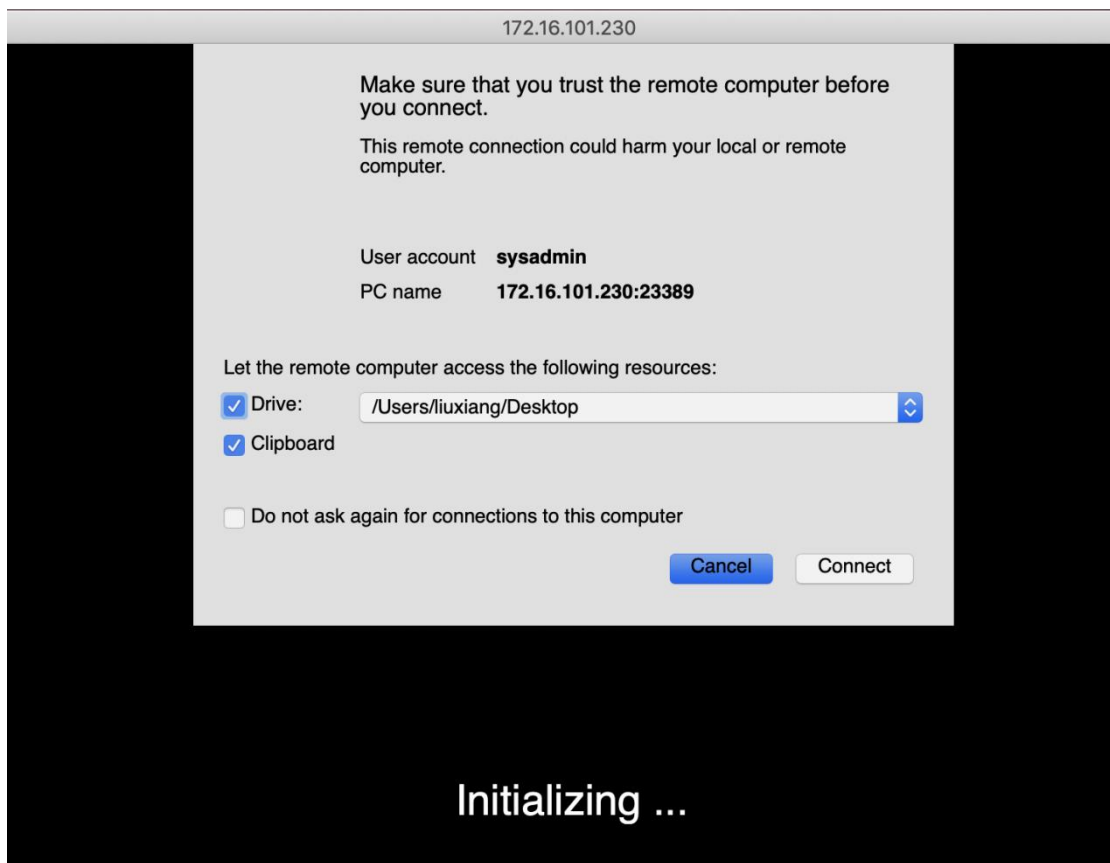
连接工具（Microsoft Remote Desktop）进入图形化访问资源菜单。如图所示，直接输入天玥运维安全网关 V6.0 系统 IP 地址，端口为 23389，然后选择连接，如果需要映射磁盘，请展开选项卡进行设置，如图所示。



图形方式访问菜单登录

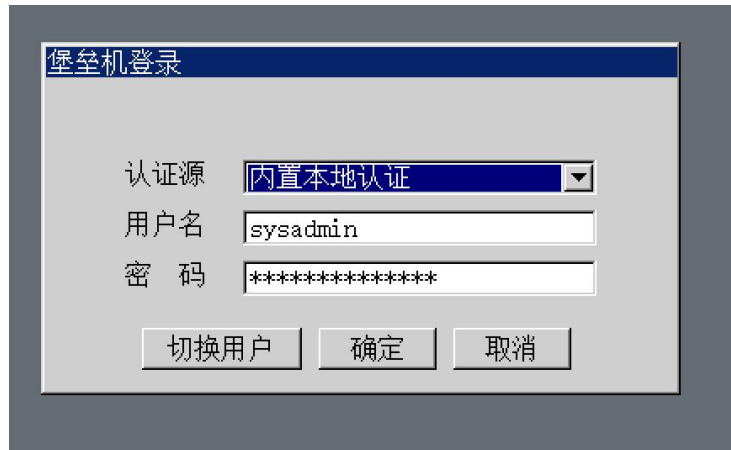


开启磁盘映射



连接堡垒机

输入运维账号、密码，如图所示。



堡垒机登录

认证源: 内置本地认证

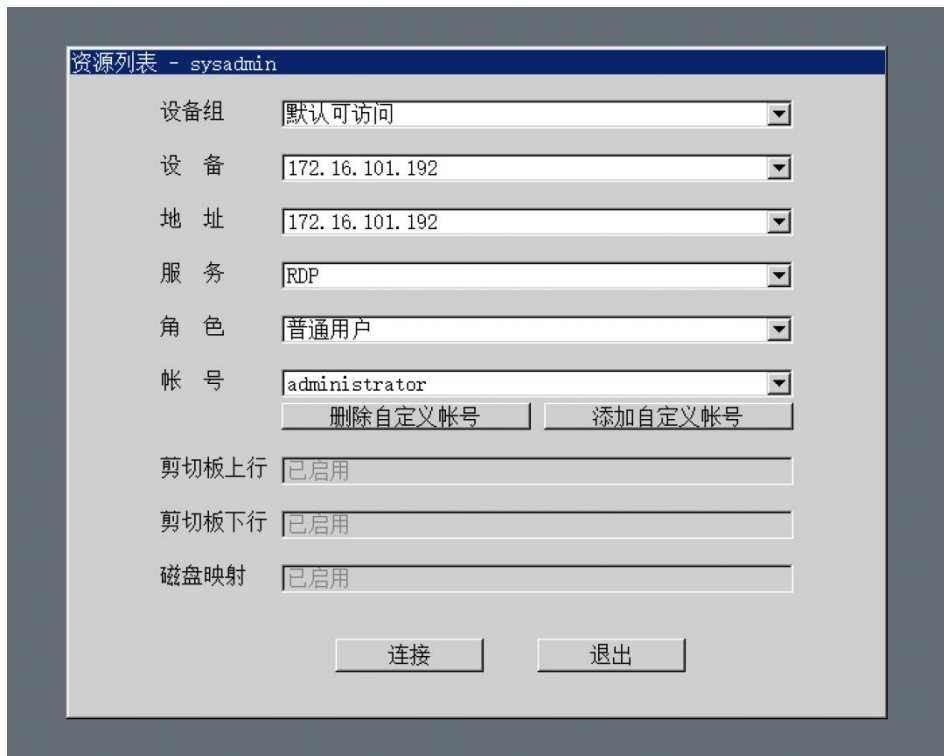
用户名: sysadmin

密码: *****

切换用户 确定 取消

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。



资源列表 - sysadmin

设备组: 默认可访问

设备: 172.16.101.192

地址: 172.16.101.192

服务: RDP

角色: 普通用户

帐号: administrator

删除自定义帐号 添加自定义帐号

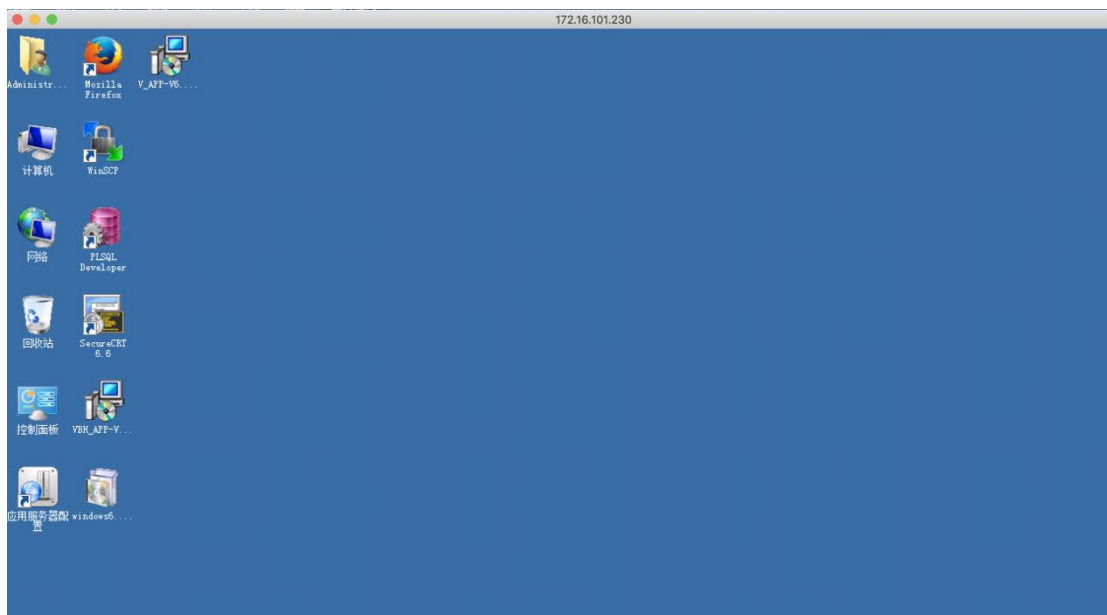
剪贴板上行: 已启用

剪贴板下行: 已启用

磁盘映射: 已启用

连接 退出

资源菜单



直连资源成功

4 国产操作系统使用说明

4.1 终端说明

用户通过终端中的客户端程序，输入正确的用户名及密码后，连接到 `linuxportal` 中进行运维操作

支持操作系统：凝思 42、统信 V20 桌面版、银河麒麟 V10 桌面版、湖南麒麟 3.0、湖南麒麟 3.2

客户端下载地址：“相关下载”页面进行下载

相关下载

环境检查助手 (用于检查堡垒机用户本地环境是否正常)

Windows版下载

基础控件 (运维、管理基础控件，堡垒机用户必须安装)

MacOS版(X86)下载

MacOS版(ARM)下载

Windows版下载

监控回放 (安装基础控件后,才可以正常使用该组件,运维监控、审计回放必备组件,审计用户请安装)

Windows版下载

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)

Windows版下载

Linux应用发布服务器运维客户端 (Linux应用发布服务器专用客户端)

银河麒麟V10桌面版下载

统信UOS桌面版V20下载

凝思42下载

湖南麒麟3.0下载

湖南麒麟3.2下载

用户手册 (堡垒机基础管理、运维手册)

下载

客户端下载

4.1.1 系统登录

用户登录国产化系统桌面，启动客户端程序后输入已注册的 **linuxportal** 的 **ip** 和端口，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”，认证成功后登陆到 **linuxportal** 桌面，运行运维终端进入运维界面进行运维操作



登录系统桌面后启动客户端程序



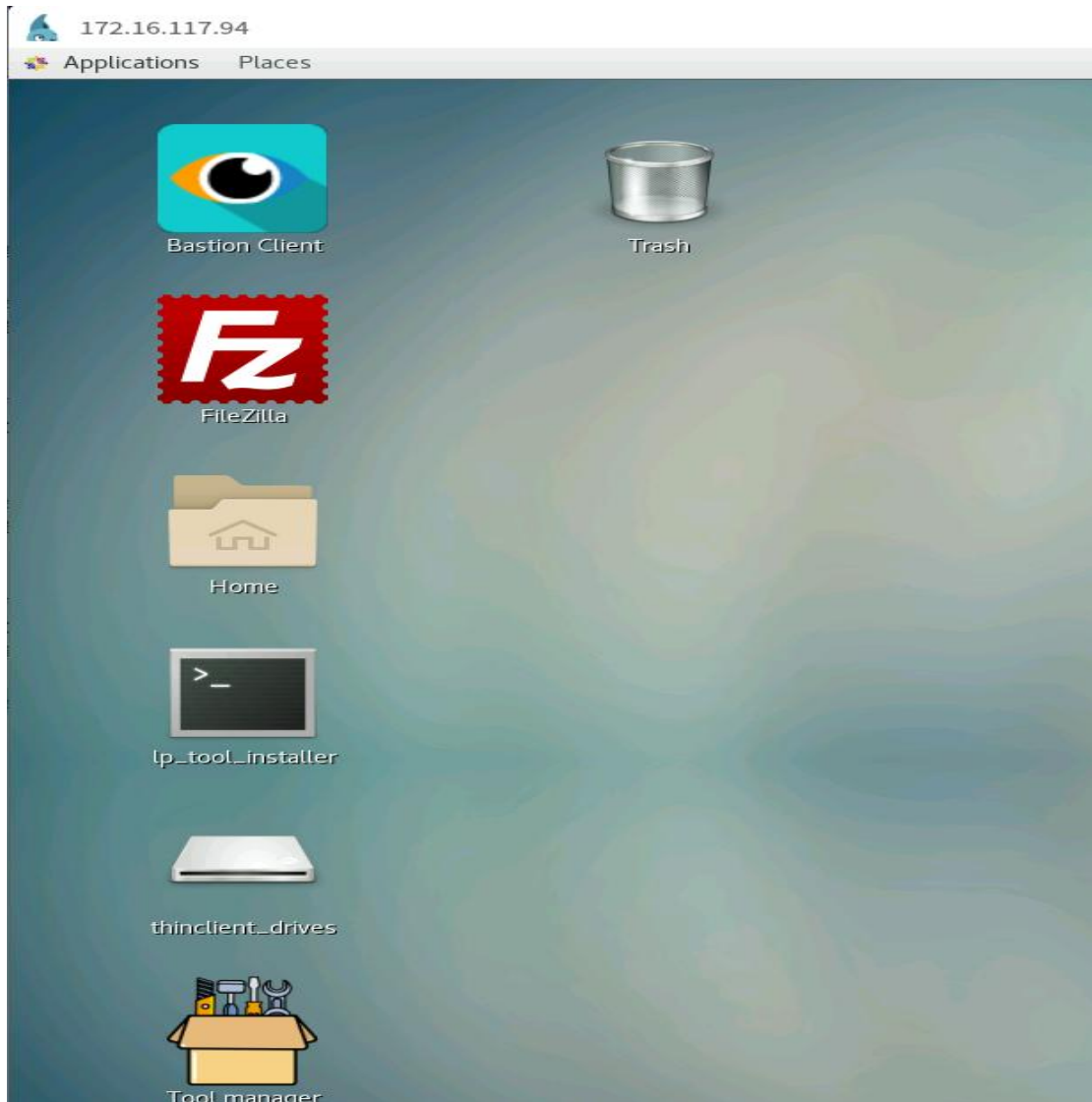
输入正确参数

用户配置了增强认证，需第一次认证通过后，进行增强认证，每级认证超时时间 10 分钟

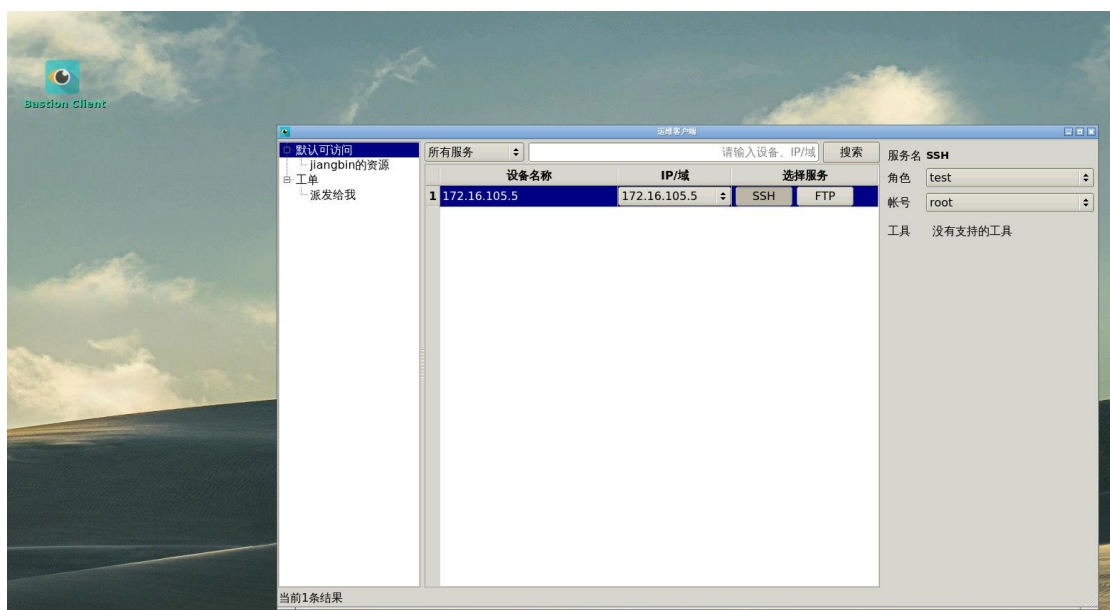


增强认证

管理员登录成功进入管理员界面，运维用户登录成功后进入运维人员界面。



管理员登录成功



运维人员登陆成功

用户退出时，需右键点击 Log Out 进行退出操作



退出登陆

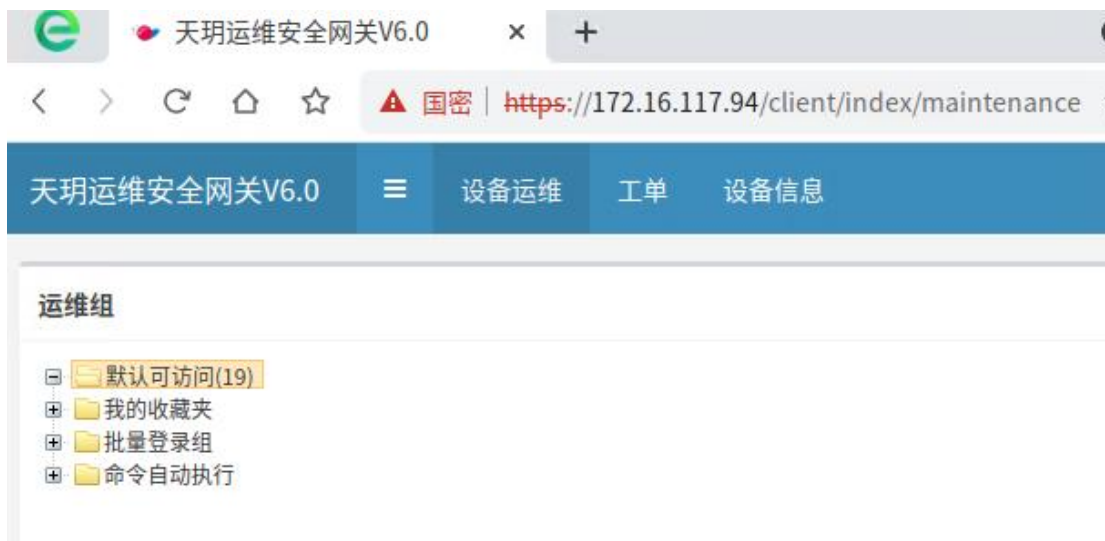
4.1.2 国密配置

如果“HTTPS 协议”配置的“国密 HTTPS”，用户在使用时需要在浏览器配置国密登录，
 举例浏览器：360 安全浏览器

配置方法：浏览器“设置”->“高级设置”，点击国密 SSL 通讯协议，启用国密 SSL 通讯协议。



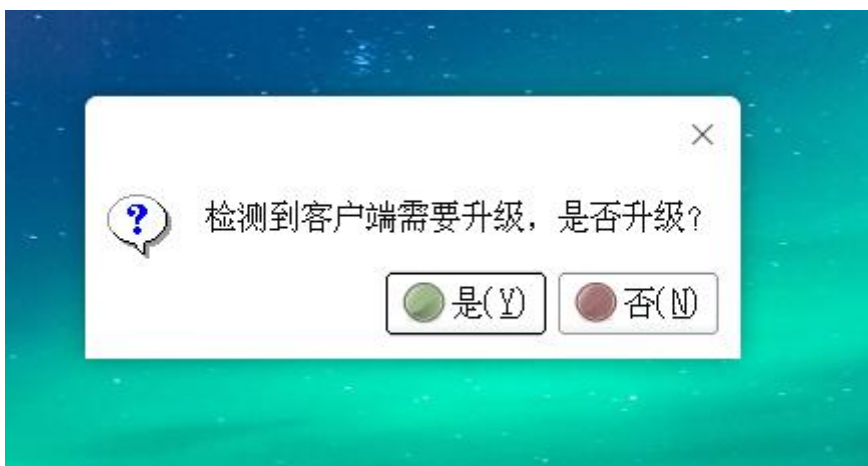
启用国密 SSL 通讯



协议国密 HTTPS 运维

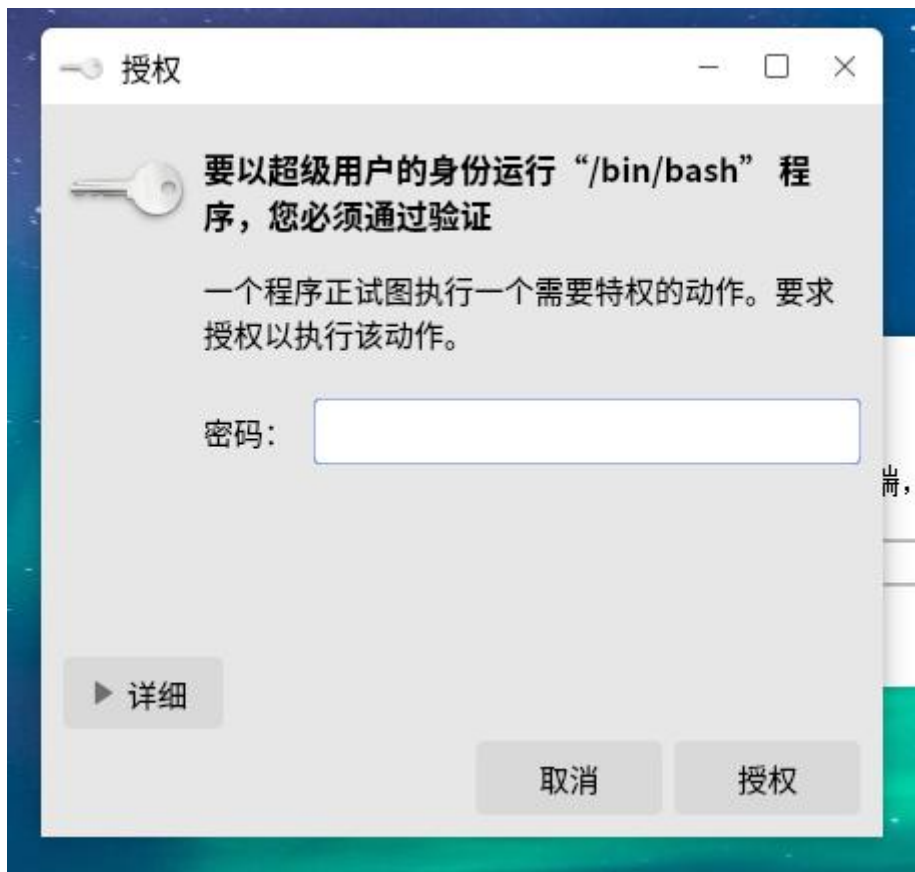
4.1.3 终端升级

当用户启动客户端程序并正确输入 linuxportal 的 ip 和端口后，如果当前客户端程序和 linuxportal 中的客户端程序版本不一致，将会提示“检测到客户端需要升级，是否升级？”



提示升级

升级需要管理员权限



需要管理员权限

如果不进行升级，客户端界面将会有提示信息“当前版本不匹配，请重启程序完成更新!”



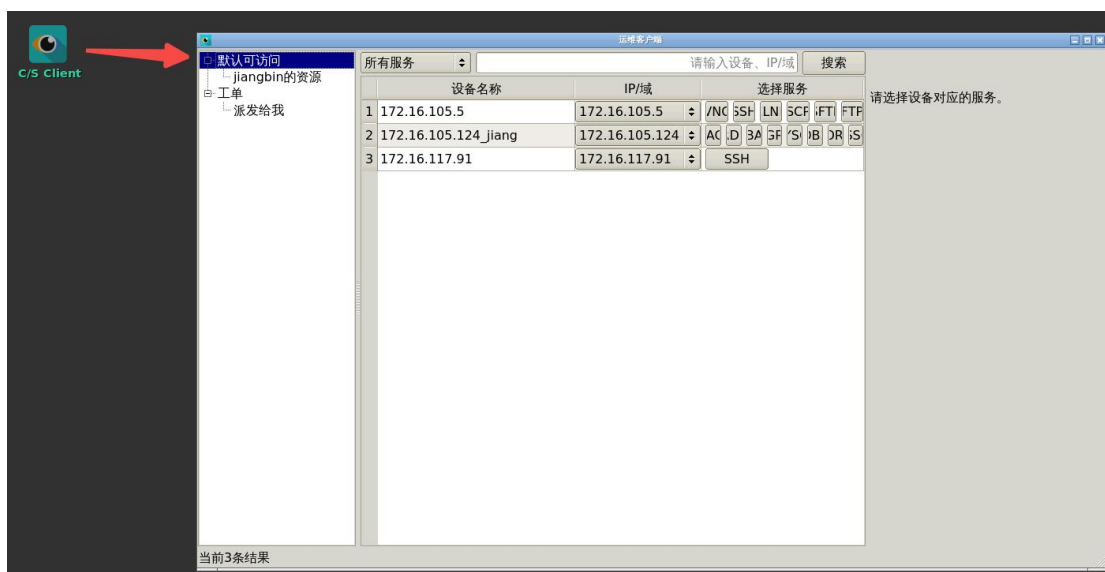
提示“版本不匹配”

4.2 运维说明

4.2.1 RDP/VNC 访问

操作步骤

步骤 1 登录到 linuxportal，进入到运维终端界面



运维界面

步骤 2 选择登录配置

选择需要运维的 RDP 或 VNC 资源。



选择资源和服务

步骤 3 进行运维登录

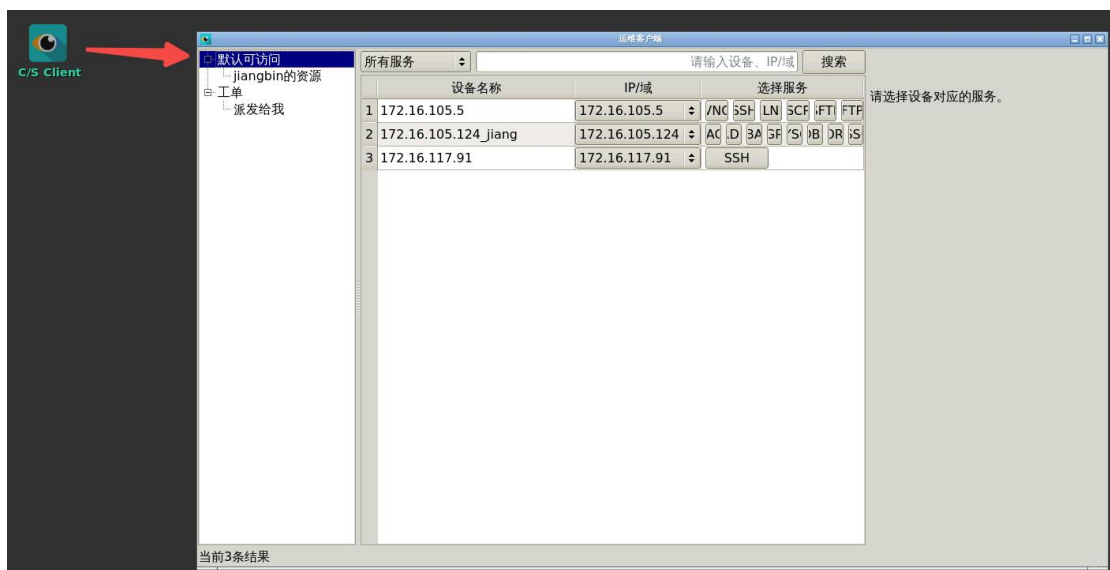
确认登录配置后，单击“登录”，即可连接资源。



登录资源

4.2.2 TELNET/SSH 访问

步骤 1 登录到 linuxportal，进入到运维终端界面



运维界面

步骤 2 选择登录配置

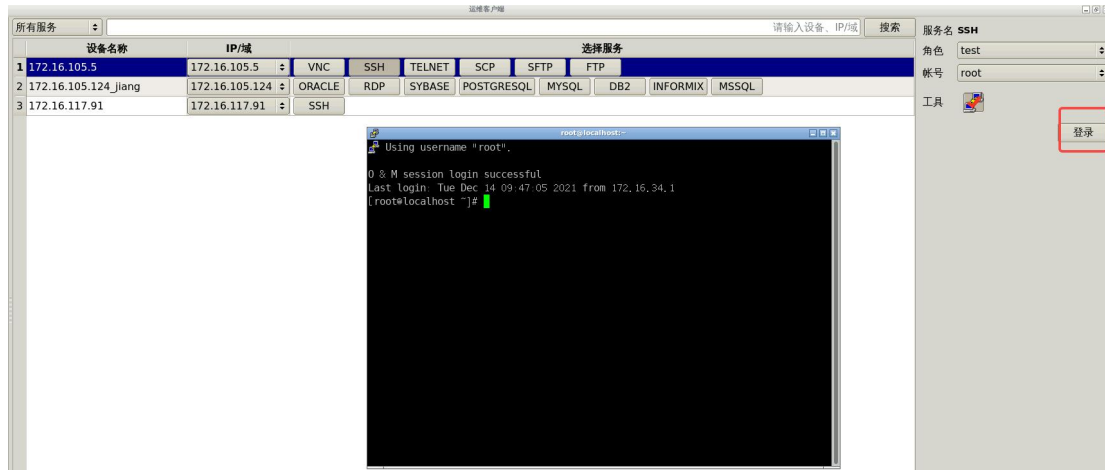
选择需要运维的 Telnet 或 SSH 资源。



选择资源和服务

步骤 3 进行运维登录

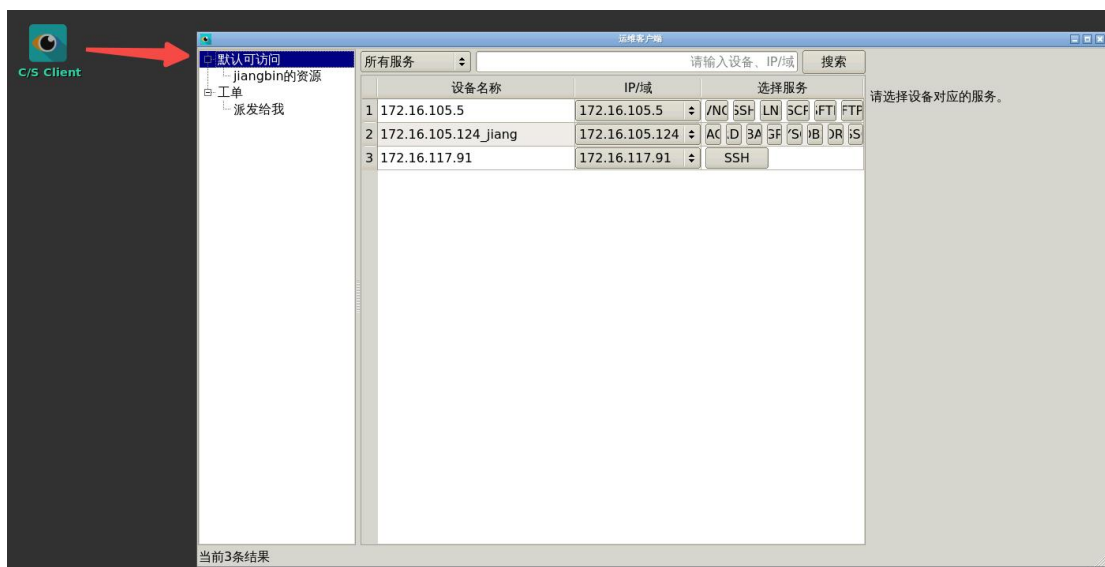
确认登录配置后，单击“登录”，即可连接资源。



登录资源

4.2.3 FTP 访问

步骤 1 登录到 linuxportal，进入到运维终端界面



运维界面

步骤 2 选择登录配置

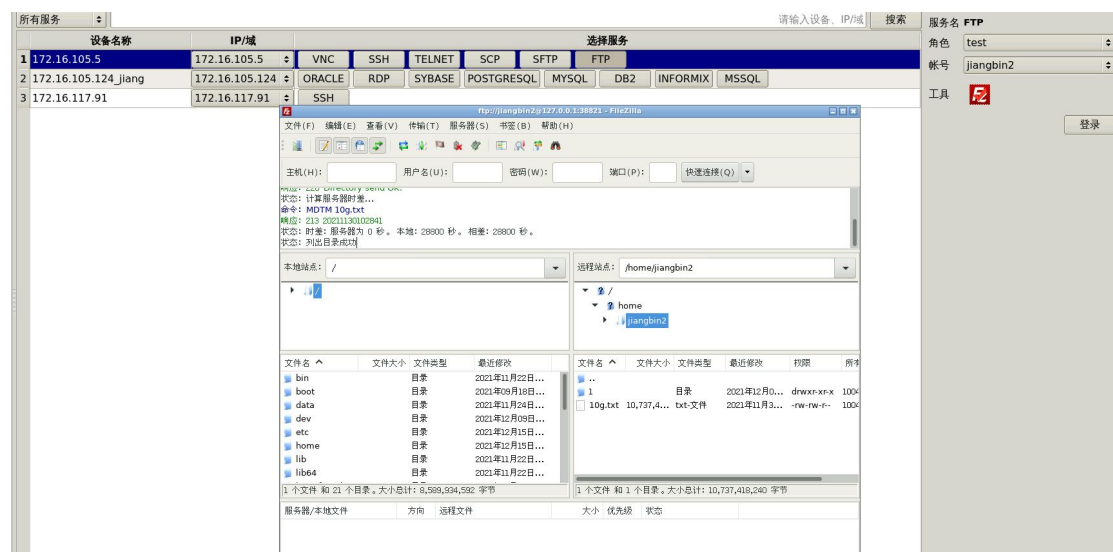
选择需要运维的 FTP 资源。



选择资源和服务

步骤 3 进行运维登录

确认登录配置后，单击“登录”，即可连接资源。



登录资源

4.2.4 数据库访问

步骤 1 登录到 linuxportal，进入到运维终端界面



运维界面

步骤 2 选择登录配置

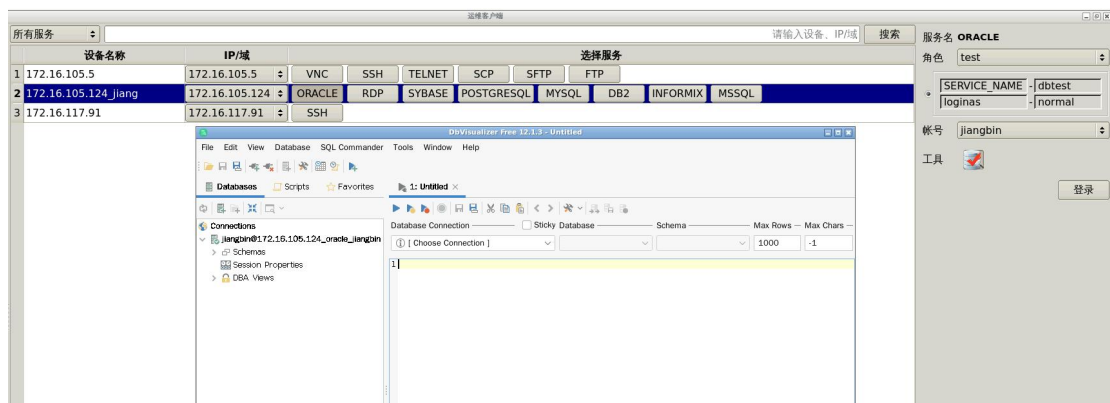
选择需要运维的数据库资源。



选择资源和服务

步骤 3 进行运维登录

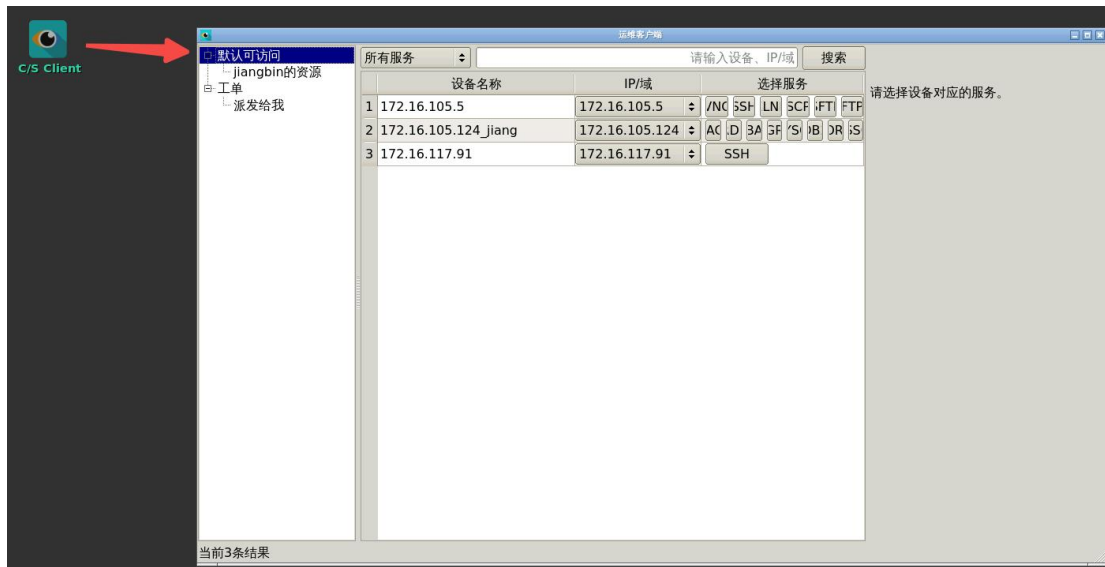
确认登录配置后，单击“登录”，即可连接资源。



登录资源

4.2.5 X11-SSH 访问

步骤 1 登录到 linuxportal，进入到运维终端界面



运维界面

步骤 2 选择登录配置

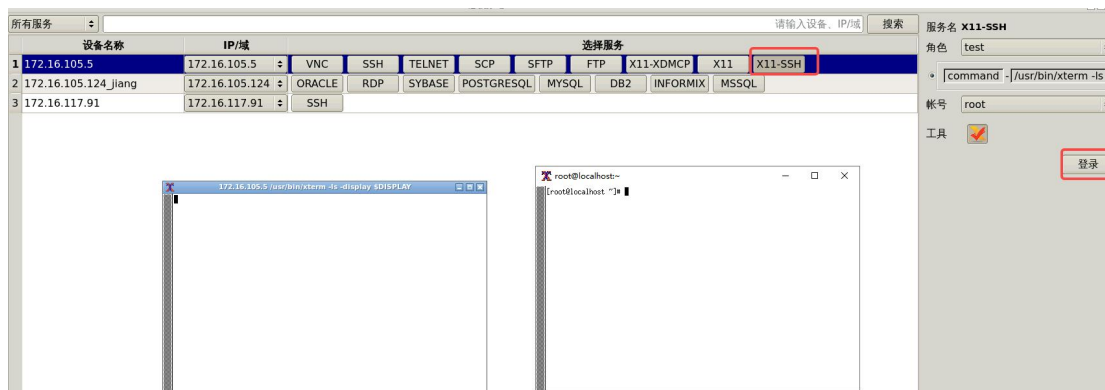
选择需要运维的 X11-SSH 资源。



选择资源和服务

步骤 3 进行运维登录

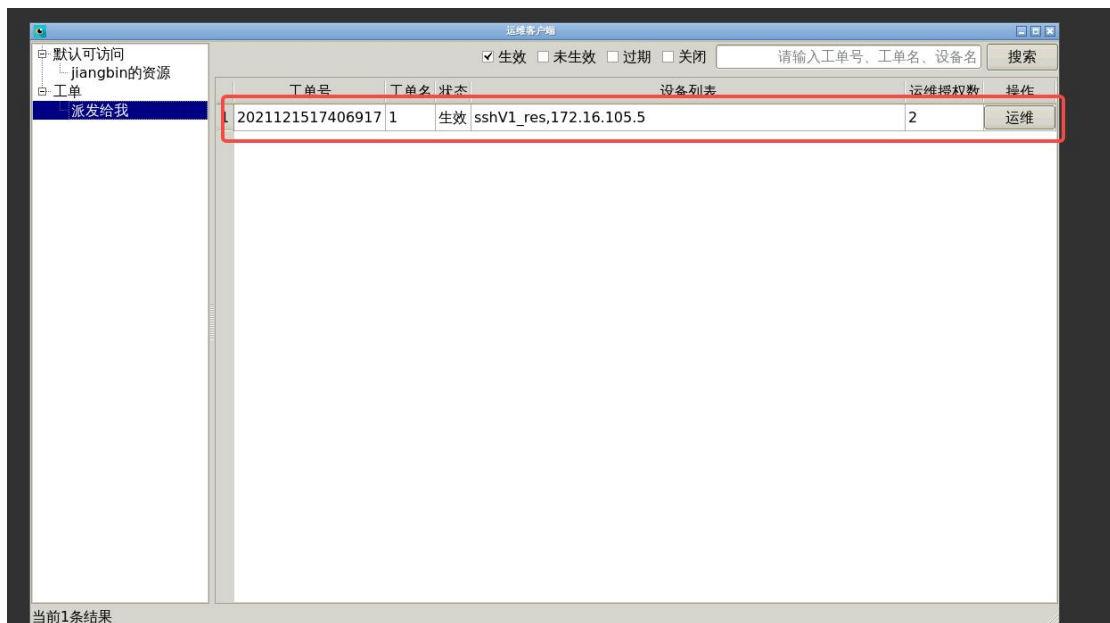
确认登录配置后，单击“登录”，即可连接资源。



登录资源

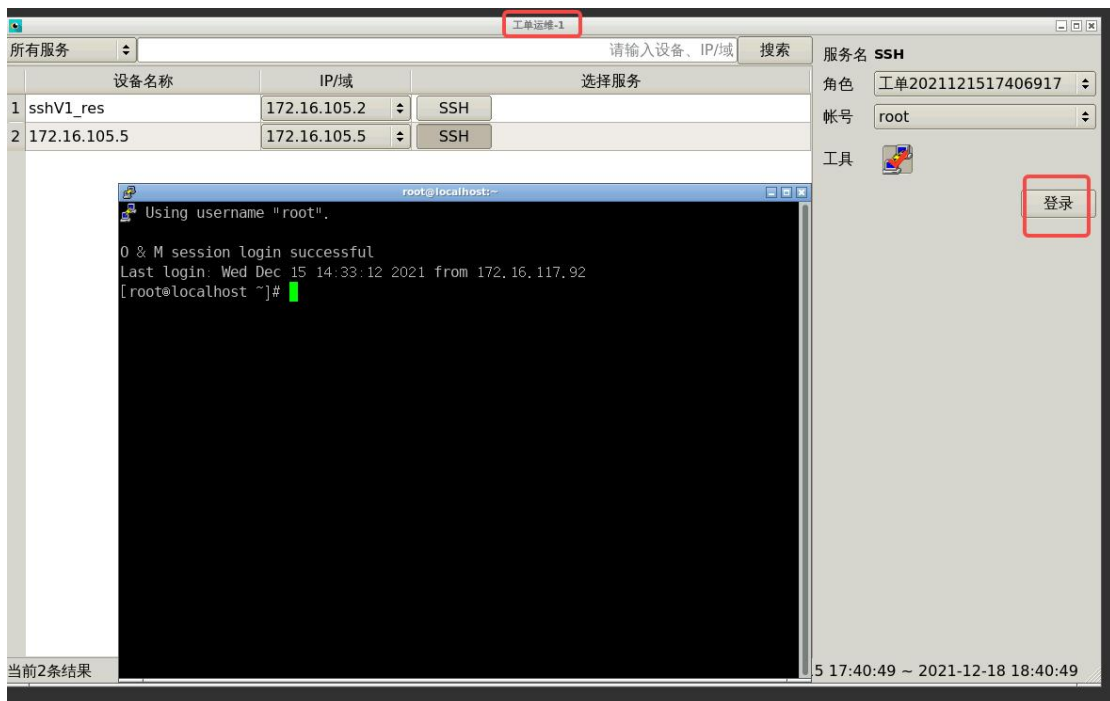
4.2.6 运维工单

管理员派发工单后，运维用户在运维界面“派发给我”界面中可以看到派发的工单



工单运维

点击运维按钮，进入到工单详情页面，选择需要运维的资源进行运维操作



工单详情

4.3 异常情况说明

4.3.1 用户登录失败

用户名或密码错误



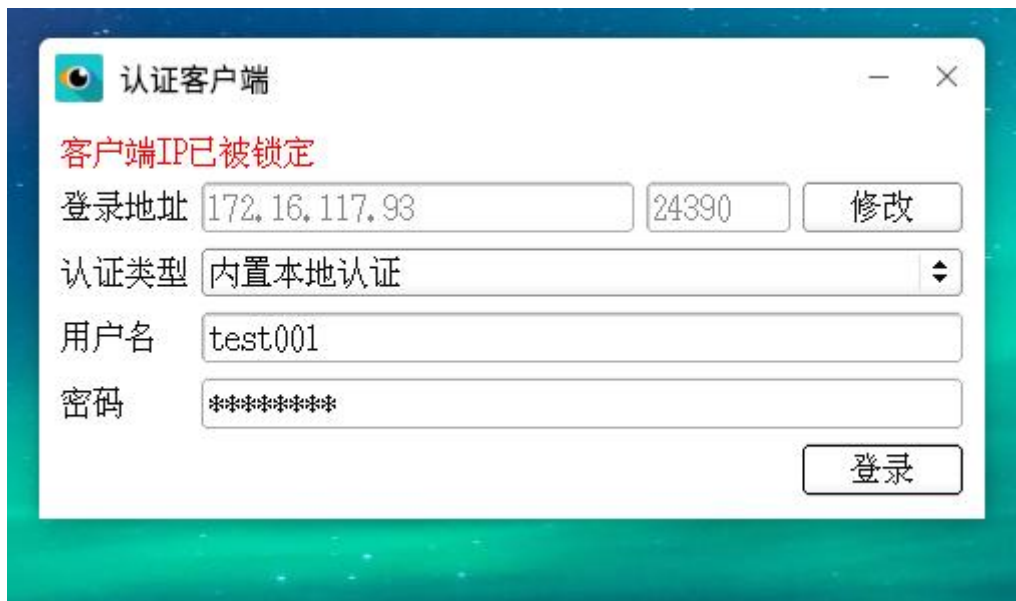
用户名或密码错误

当客户端与 linuxportal 无法通讯时，提示“错误：登录地址网络不可达”



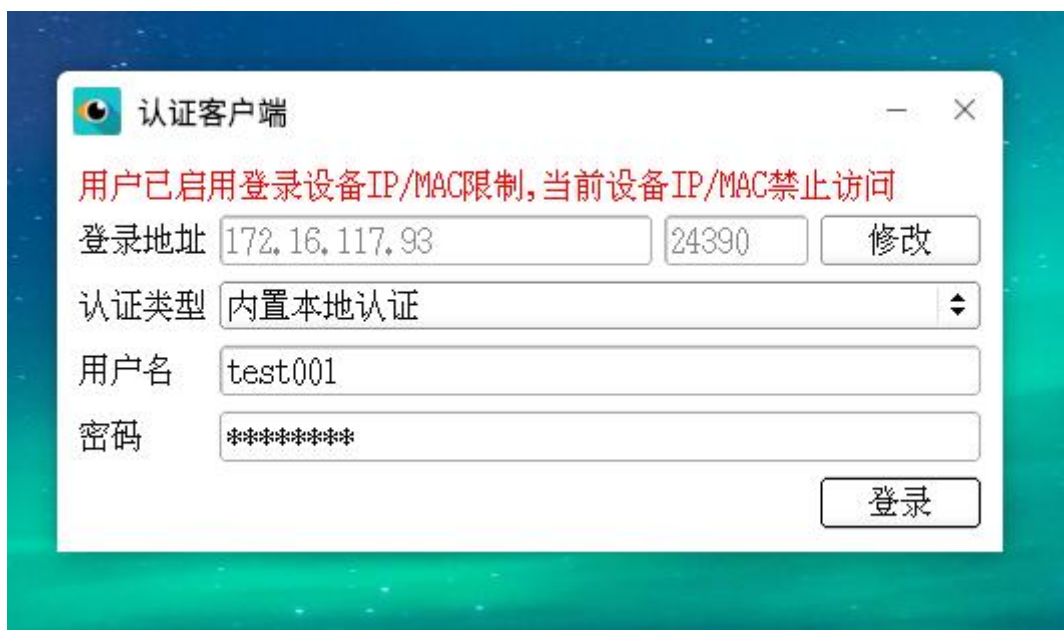
网络不通

密码多次输入错误，ip 被锁定时



ip 被锁定

配置了 ip/mac 限制

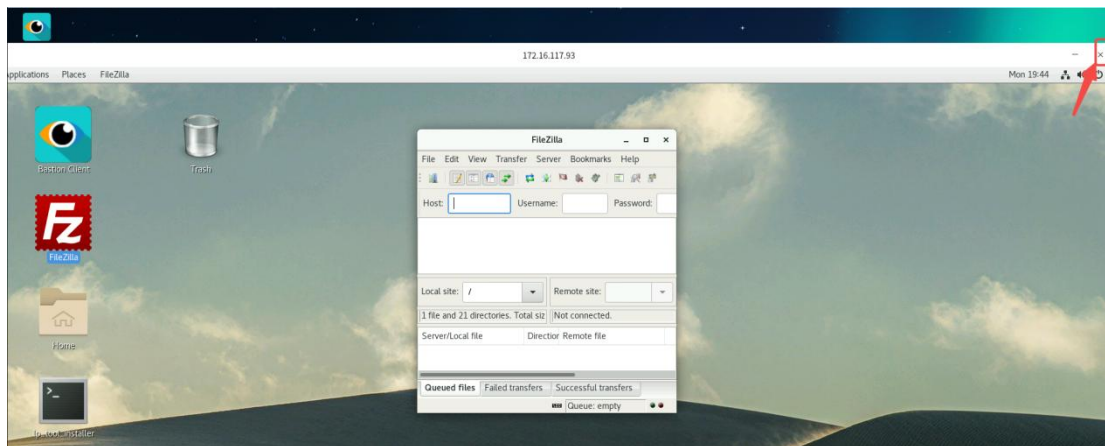


配置了 ip/mac 限制

注意：Server 端配置同一时刻登录限制对 linuxportal 无效，linuxportal 总是后登陆优先

4.3.2 退出登录

用户退出登录时，直接点击关闭按钮，下次登陆时会显示上次退出的页面



直接点击退出

5 参考文档

无

6 技术支持

使用过程中,如果在遇到难以确定或难以解决的问题,通过文档的指导仍然不能解决时,请通过以下方式获取帮助:

- (1) 联系启明星辰信息技术集团股份有限公司客户服务中心。
客户服务电话: 400-624-3900
- (2) 联系启明星辰信息技术集团股份有限公司驻当地办事处的技术支持人员