【文档密级：公开】

明御®运维审计与风险控制系统

（云堡垒机）

用户手册

适用于阿里云 v2.0.20066f 版本

杭州安恒信息技术有限公司

二〇一五年十月

目 录

1 基本配置

1.1 Web方式登录

(1) 启动浏览器，登录运维审计系统的管理 IP（例如：https://192.168.0.1），输入用户名、密码（出厂用户和密码为：admin/123456）及验证码。

图 1-1 系统登录框示意图

(2)　单击<登录>按钮后进入 Web 管理页面。

2 用户组配置

2.1 功能简介

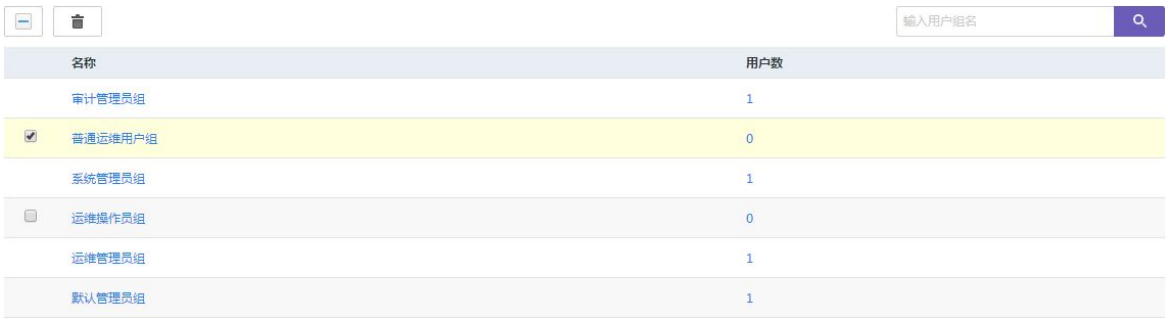
默认出厂提供这五种用户组（即用户角色）：

- 审计管理员组：查看审计日志：会话审计、会话报表、运维报表。
- 系统管理员组：配置明御运维审计与风险控制系统（堡垒机）的系统信息：系统用户配置、网络配置、许可证管理等。
- 运维操作员组：仅提供主机运维和应用中心运维。
- 运维管理员组：配置资产信息、会话管理、会话审批等。
- 默认管理员组：提供最高权限的用户。

2.2 配置描述

(1) 进入[用户/用户组管理]界面中，可以看到出厂设置好的用户组，如下图：

图 2-1 用户组管理页面示意图



(2) 单击<+新建用户组>，进入配置界面，定义用户组名、勾选功能模块权限，如下图：

图 2-2 新建用户组示意图

说明

用户可以根据自身的权限需求进行定制用户角色和用户组。

(3) 配置完成后，单击<创建用户组>即可创建成功。

2.3 配置举例

以新增一个“普通运维用户组”为例，其只拥有对目标主机进行运维的权限：

(1) 进入[用户/用户组管理]界面，单击<+新建用户组>，进入配置页面，编辑用户组名称：

图 2-3 新建用户组页面示意图

(2) 在配置页面中，勾选“运维权限”下的“主机运维”和“应用中心”：

图 2-4 新建用户组页面示意图

(3)　单击<创建用户组>即可创建成功，并返回“用户组列表”中查看到新增的用户组信息：

图 2-5 用户组管理页面示意图

3 用户配置

用户即运维人员、管理员，用于登录明御运维审计与风险控制系统（堡垒机）的用户配置；用户管理可以实现单个手工添加或批量表格导入。

3.1 单个用户配置

3.1.1 功能简介

单个用户配置是针对少量的用户添加或者编辑。

3.1.2 配置描述

(1) 进入[用户/用户管理]界面中，可以到默认出厂内置了一个 admin 用户：

图 3-1 用户管理页面示意图

说明

admin 用户拥有明御运维审计与风险控制系统（堡垒机）管理的最高权限。

(2) 单击<+新建用户>，进入配置界面，定义用户名、密码、用户组、姓名等信息。如下图：

图 3-2 新建用户页面示意图

提示

- 标“*”部分为必填项，其他部分为可选项。
- 用户名请不要使用中文，长度限制在 16 个字符内。
- 密码长度限制在 6 至 64 个可见字符。
- 如需设置“临时用户”根据登录 IP 和登录时间进行限制。

(3) 配置完成后，单击<+创建用户>即可创建成功。

3.1.3 配置举例

以新增一个“test”普通运维用户为例，并将该用户加入到“普通运维用户组”中：

(1) 进入[用户/用户管理]界面，单击<+新建用户>，进入配置页面，编辑用户名、密码、用户组、姓名等：

图 3-3 新建用户页面示意图

(2) 完成配置后，单击<创建用户>即可创建成功，并返回“用户列表”中查看到新增的用户信息：

3.2 批量导入用户

3.2.1 功能简介

批量导入用户通过表格的方式统计将用户信息导入到明御运维审计与风险控制系统（堡垒机）中，方便快捷。

3.2.2 配置描述

(1) 进入[用户/用户管理]界面，单击<更多操作>：

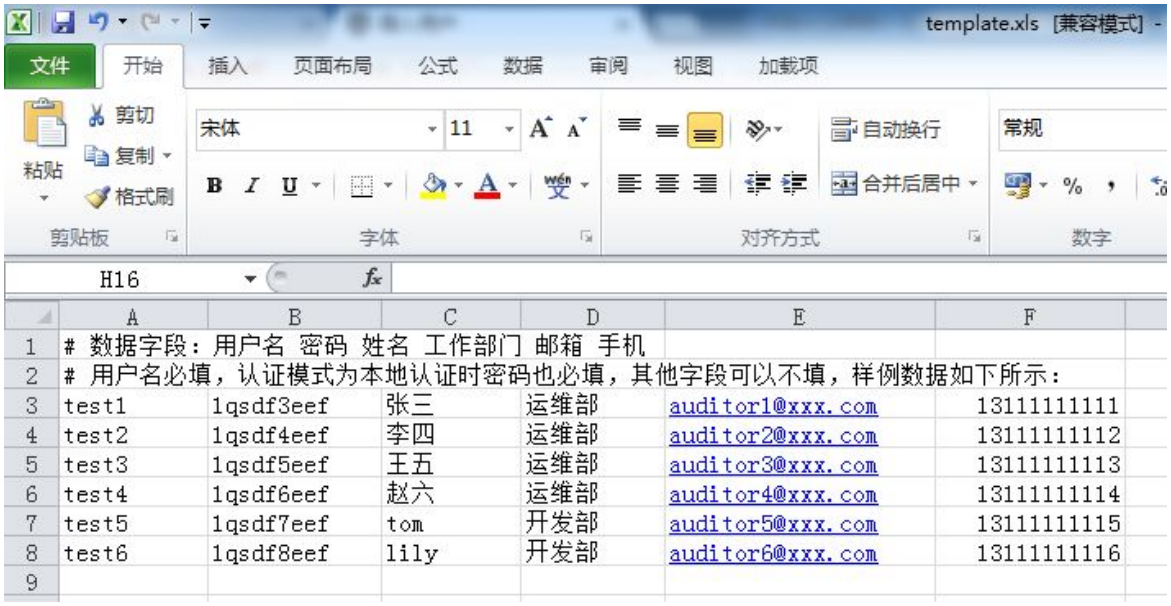
图 3-4 用户管理页面示意图

(2) 单击<导入用户>，进入“导入用户”页面：

图 3-5 导入用户页面示意图

(3) 单击<下载模板文件>将模板下载至本地，解压后打开一个用户统计表格进行编辑，参考下图：

图 3-6 导入用户表格模板示意图



说明

第一列为用户名（必填项）、第二列为密码（必填项）、第三列为姓名（可选项）、第四列为工作部门（可选项）、第五列为邮箱（可选项）、第六列为电话号码（可选项）。

(4) 保存表格后，单击<上传文件>，可以选择是否勾选“覆盖已有用户”：

图 3-7 导入用户页面示意图

说明

勾选“覆盖已有用户”：如果存在相同的用户名，将会被覆盖成新的用户信息。

(5) 单击<导入全部>后即可导入成功。

4 主机及帐户配置

主机及帐户及目标服务器的信息管理，如 IP、主机名、网络协议、端口号、帐户、密码等信息。
主机及帐户配置既能单个手工添加，又能批量表格导入。

4.1 单个主机及账户配置

4.1.1 功能简介

主机即目标服务器，用于管理目标主机资产的 IP、主机名、协议等；
帐户即目标服务器的帐户，用于管理目标主机资产的帐户、密码、协议、登录方式；
帐户组用于对目标服务器的帐户进行分类管理。

4.1.2 配置描述

(1) 进入[资产/主机管理]界面：

图 4-1 主机管理页面示意图

(2) 单击<+添加主机>，进入配置页面，可以编辑主机的 IP、主机名称、协议等信息：

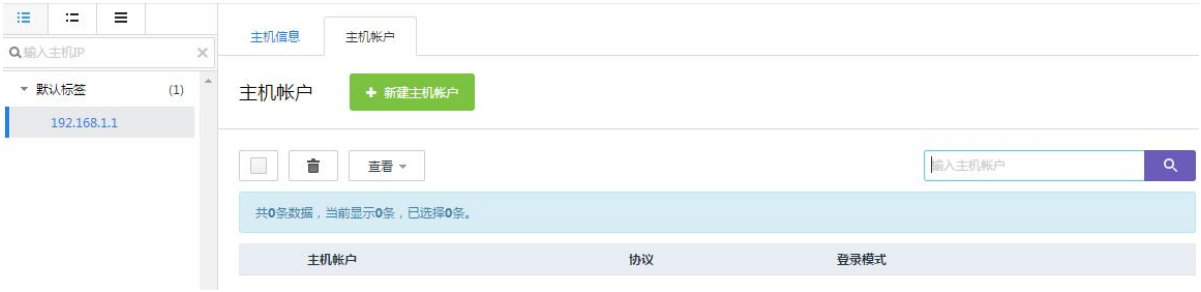
图 4-2 新建用户页面示意图

(3) 编辑完成后，单击<添加主机>，弹出“成功添加主机 X.X.X.X”提示框：

图 4-3 添加主机成功提示示意图

(4) 单击<给这台主机增加主机帐户>，进入帐户配置页面：

图 4-4 主机帐户管理页面示意图



(5) 单击<+新建主机帐户>，弹出“新建主机帐户”框，编辑目标主机的协议、登录模式、帐户、密码：

图 4-5 新建主机帐户页面示意图

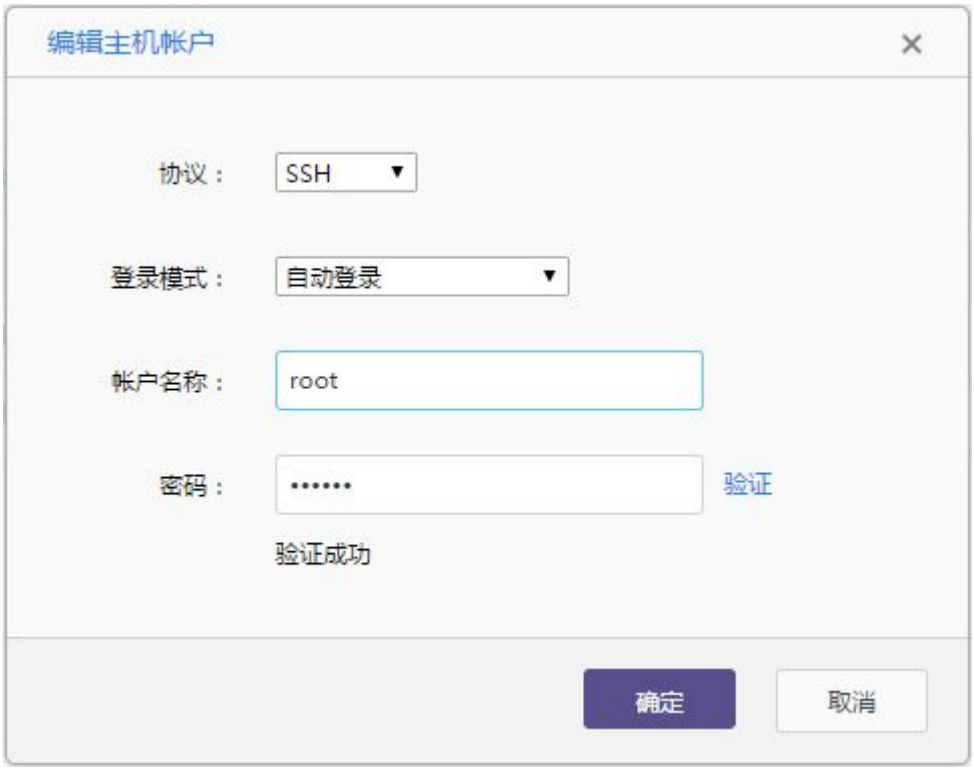


表 4-1 新建主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录(二次登录)和手工登录。
自动登录	将正确的主机账号和密码录入明御运维审计与风险控制系统（堡垒机），运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录(二次登录)	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的账户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

(6) 单击<确定>后即可编辑成功，并且在页面的上方提示“帐户已创建”：

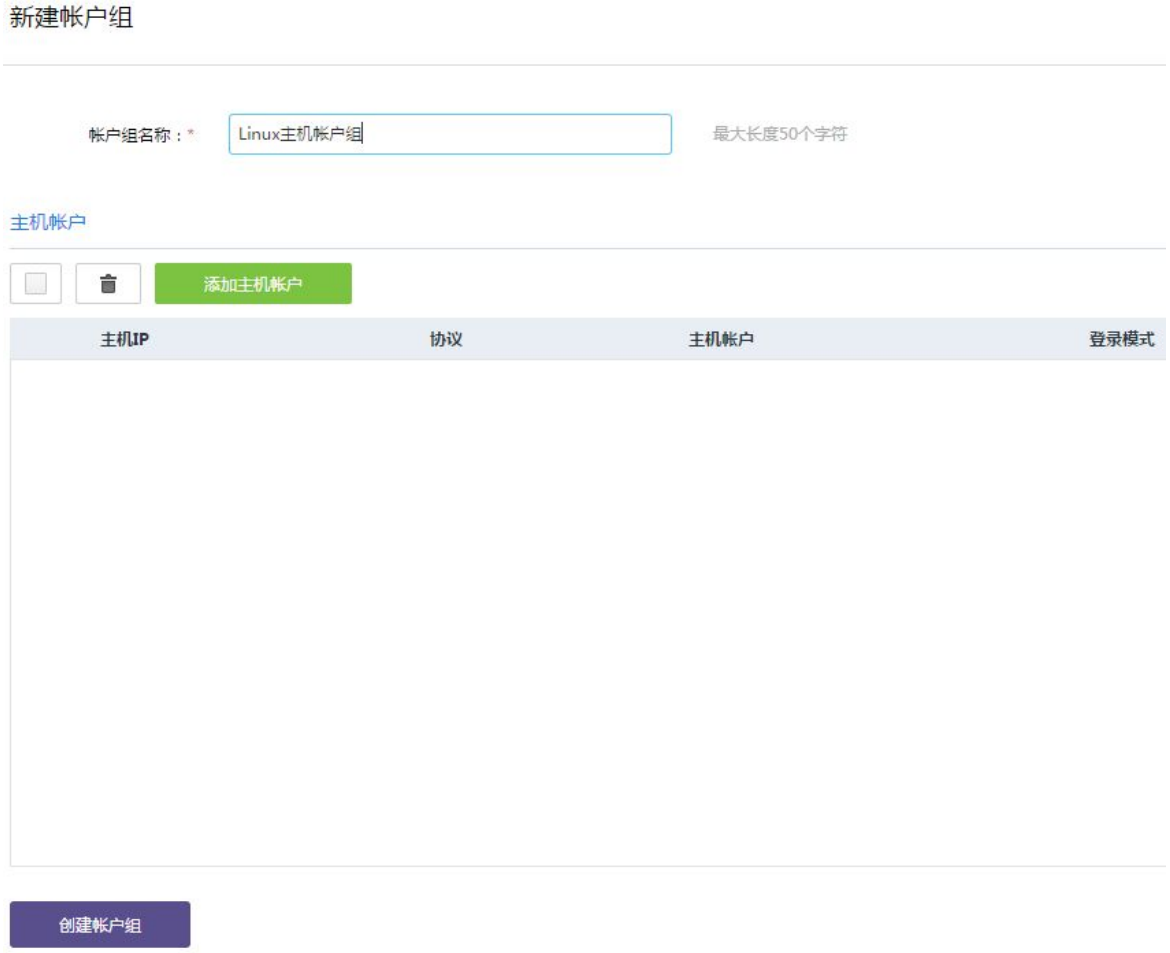
图 4-6 主机帐户管理页面示意图

(7) 然后进入[资产/帐户管理]界面：

图 4-7 帐户组管理页面示意图

(8) 单击<+新建帐户组>，进入配置页面，编辑帐户组名称：

图 4-8 新建帐户组页面示意图



说明

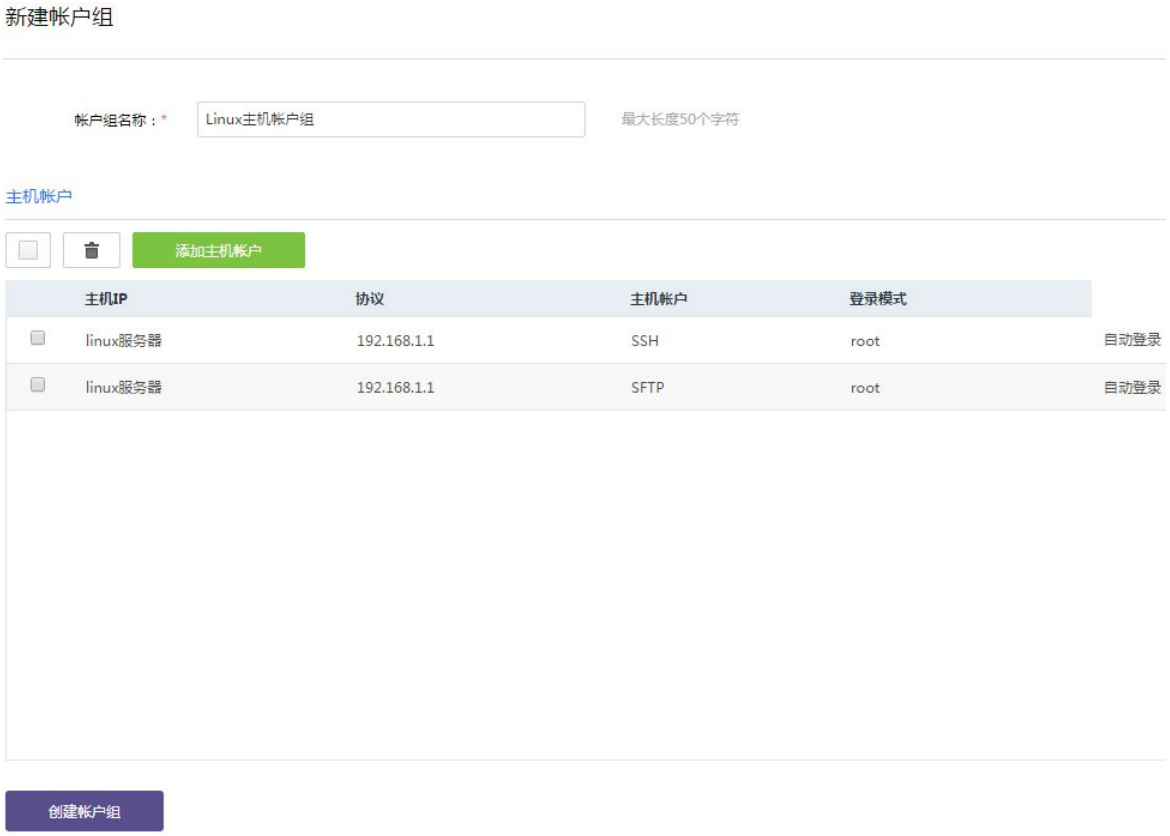
帐户组用于对主机的帐户进行分组管理，目的是为了进行区分类别和便于授权。

(9) 单击<添加主机帐户>，弹出“主机帐户列表”，可以勾选所属该帐户组的主机帐户信息：

图 4-9 主机帐户列表页面示意图

(10) 单击<添加>后即可添加成功：

图 4-10 新建帐户组页面示意图



(11) 单击<创建帐户组>即可创建成功，返回“帐户组列表”中查看帐户组：

图 4-11 帐户组管理页面示意图

4.1.3 配置举例

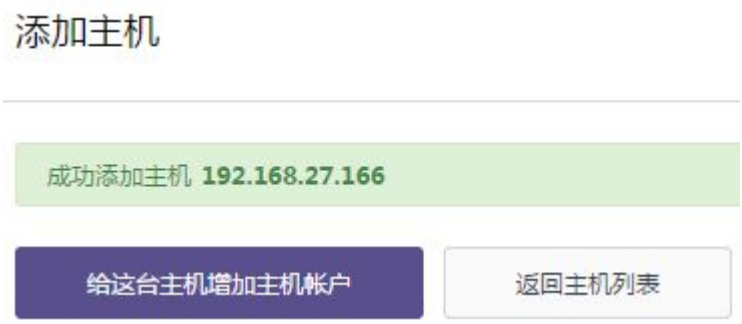
以新增一个“交换机”为例，将交换机的帐户和密码添加进去，并将该主机放到“网络设备帐户组”中：

(1) 进入[资产/主机管理]界面中，单击<+添加主机>，进入配置页面，将交换机的 IP、名称、协议、端口号等填写正确：

图 4-12 新建主机页面示意图

(2) 单击<添加主机>后，提示“成功添加主机 X.X.X.X”：

图 4-13 添加主机成功提示示意图



(3) 单击<给这台主机增加主机帐户>，进入主机帐户管理页面：

图 4-14 主机帐户页面示意图

(4) 单击<+新建主机账户>，弹出“新建主机账户”窗口，编辑运维协议、登录模式、远程帐户、密码、enable 特权命令、登录密码。如需确认帐户和密码是否正确，请单击“验证”即可验证是否成功。

图 4-15 新建主机帐户页面示意图

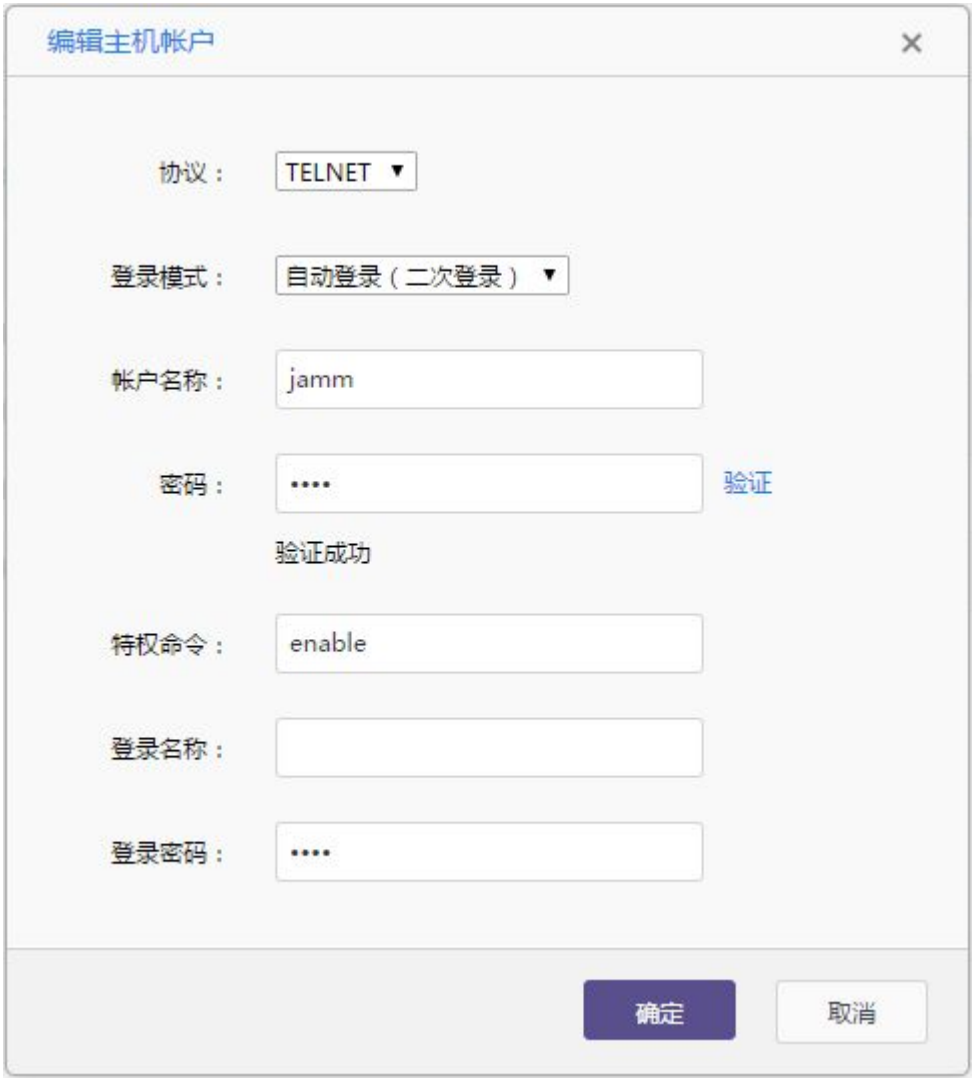


表 4-2 新建主机帐户选项说明

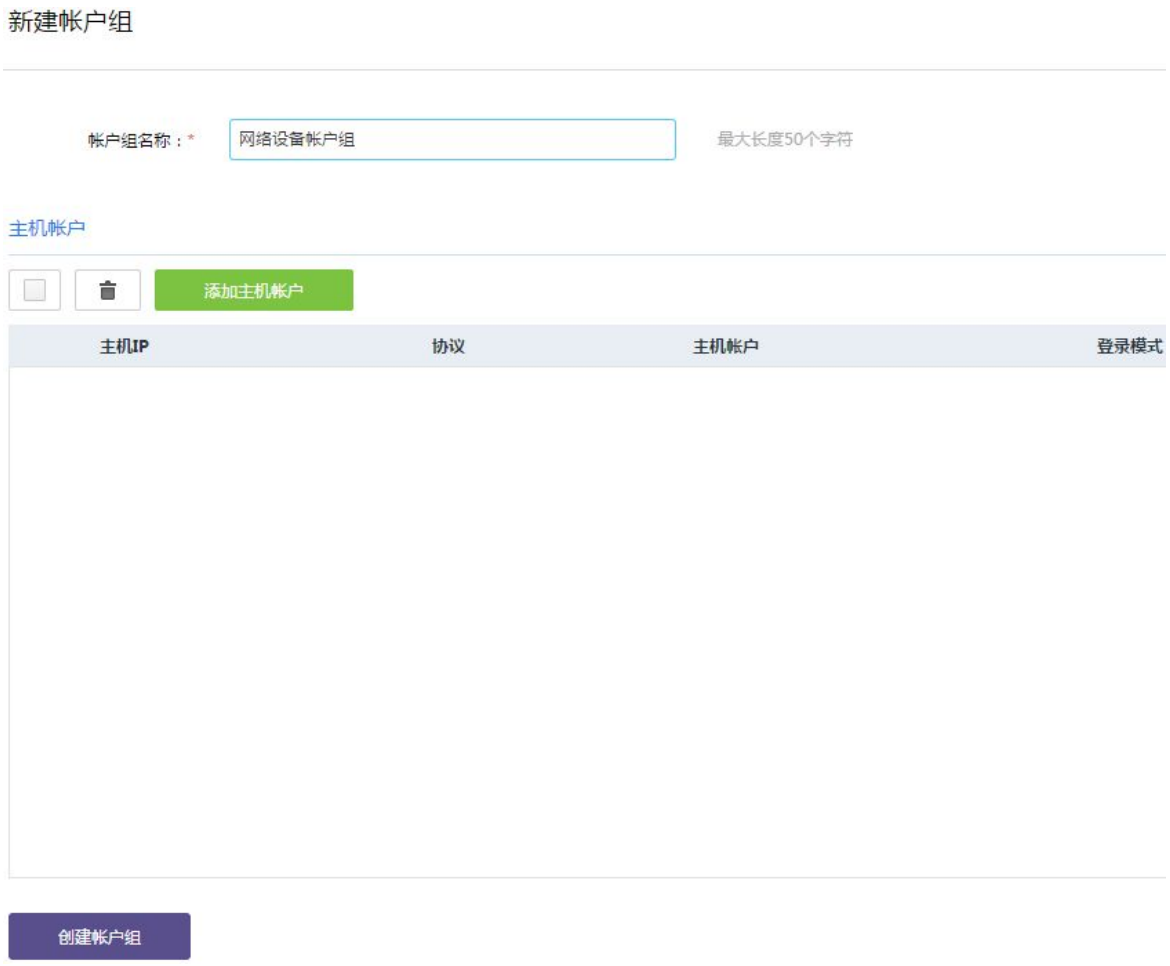
选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录(二次登录)和手工登录。
自动登录	将正确的主机账号和密码录入明御运维审计与风险控制系统（堡垒机），运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录(二次登录)	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的账户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

(5) 单击<确定>后即可新建成功，并在界面上方提示“帐户已更新”：

图 4-16 主机帐户管理页面示意图

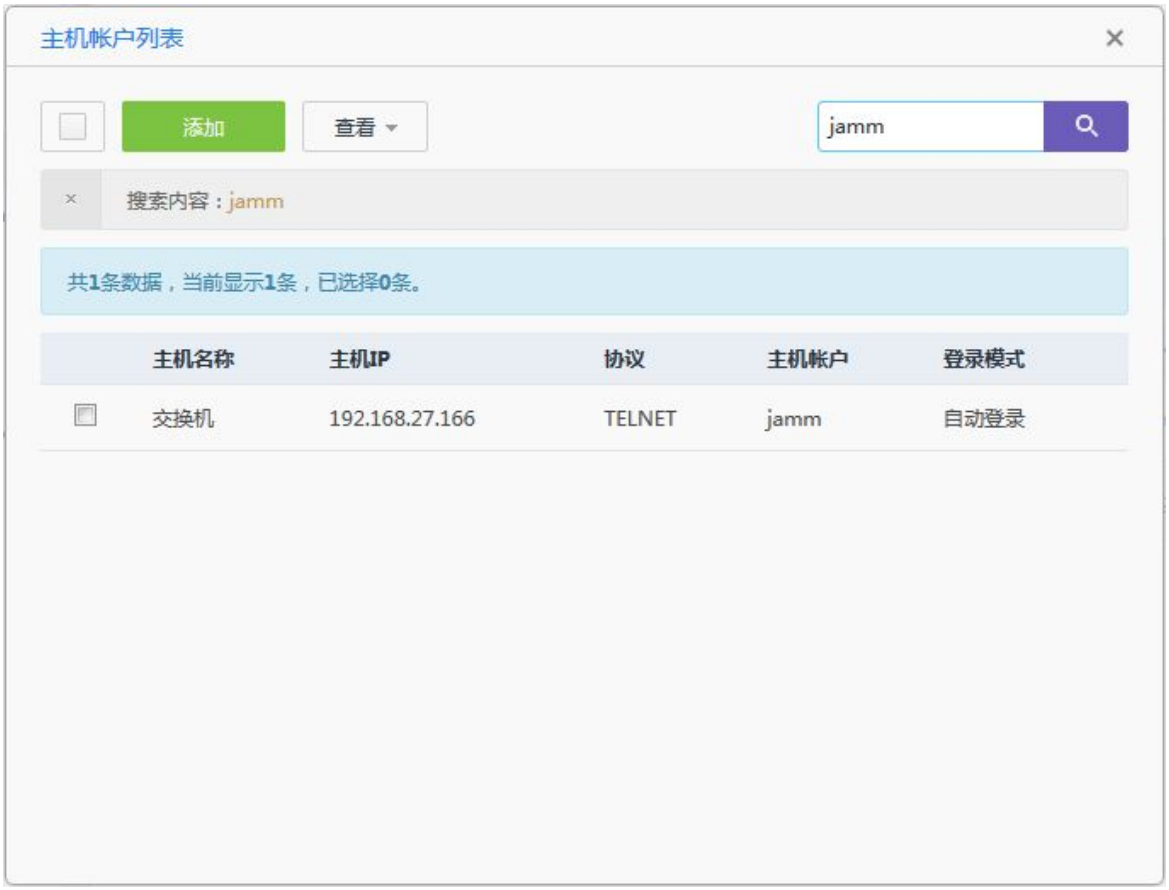
(6) 进入[资产/帐户管理]界面中，单击<+新建帐户组>，进入配置页面，编辑帐户组名称“网络设备帐户组”：

图 4-17 新建帐户组页面示意图



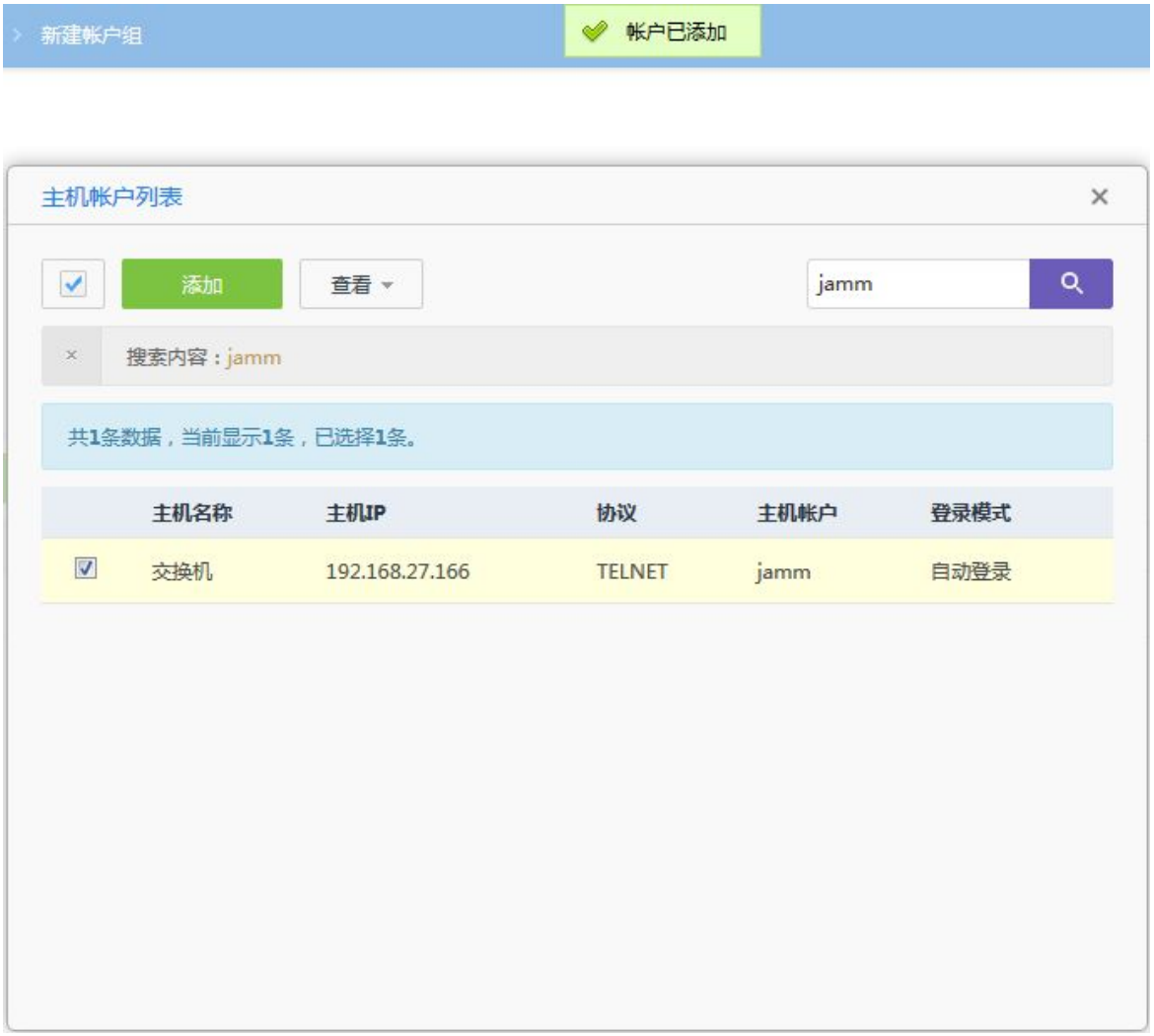
(7) 单击<添加主机帐户>，弹出“主机帐户列表”复选框，勾选“cisco 交换机”的帐户信息：

图 4-18 主机帐户列表示意图



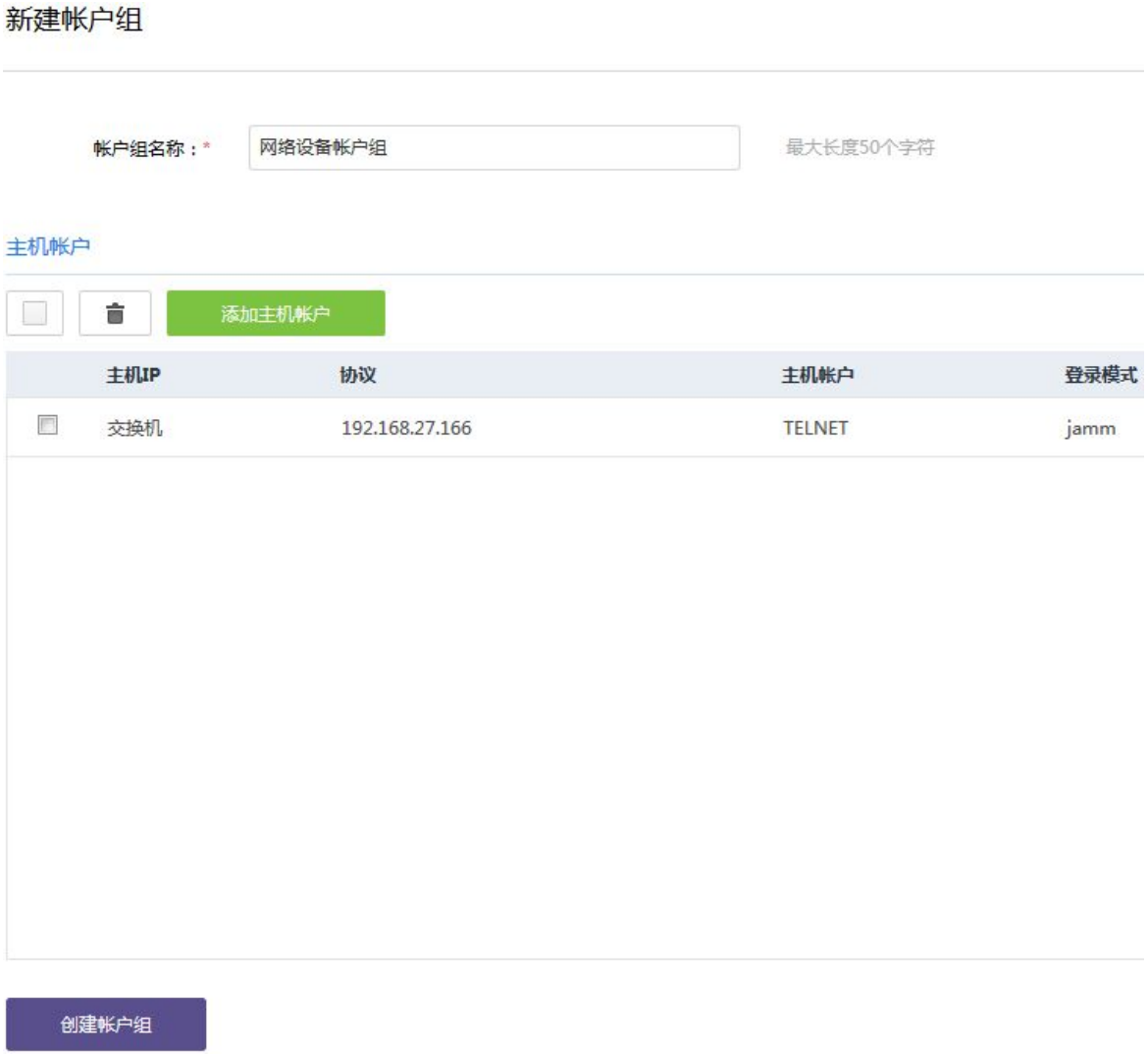
(8) 单击<添加>后，提示“帐户已添加”：

图 4-19 主机帐户列表示意图



(9) 关闭“主机帐户列表”后，可以在“主机帐户”复选框中查看到已选中的主机账户信息：

图 4-20 新建帐户组页面示意图



(10) 单击<创建帐户组>即可创建成功，并返回账户组列表：

图 4-21 帐户组管理页面示意图

4.2 批量导入主机和帐户

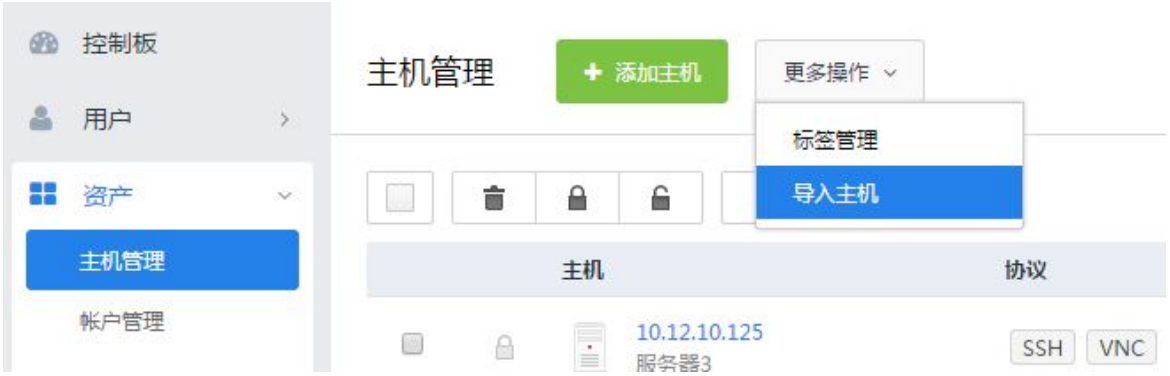
4.2.1 功能简介

批量导入主机和帐户通过表格的方式将主机信息、帐户信息、帐户组进行统一导入，方便快捷。

4.2.2 配置描述

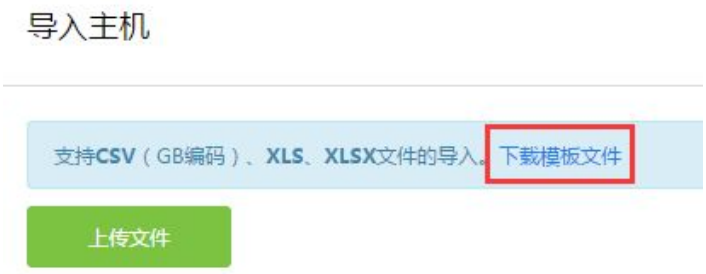
(1) 进入[资产/主机管理]界面中，单击<更多操作>：

图 4-22 主机管理页面示意图



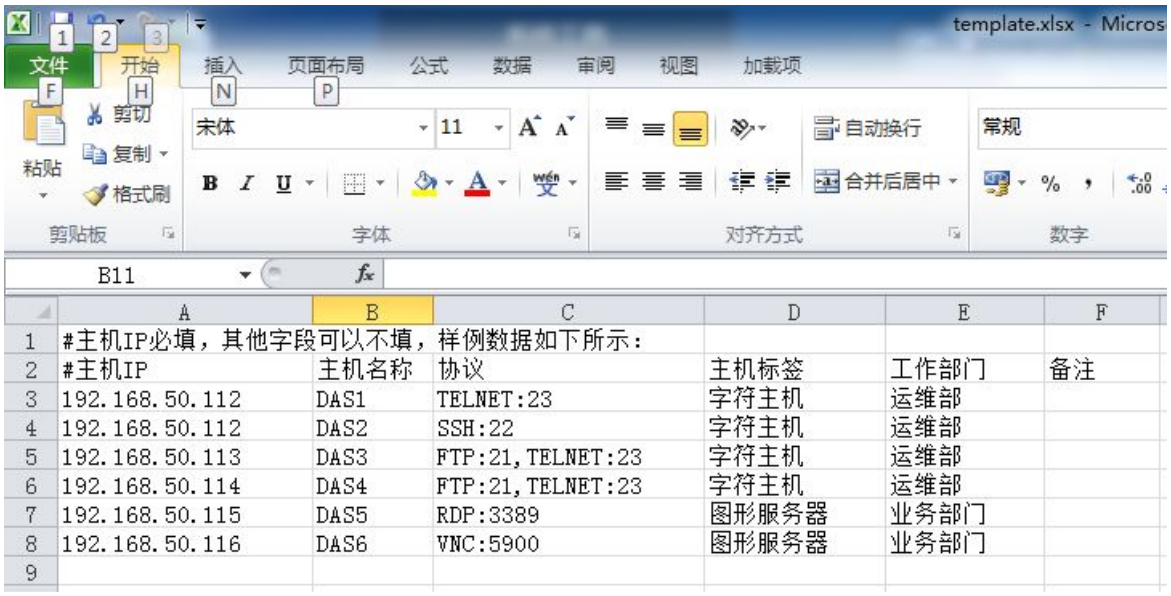
(2) 再单击<导入主机>，进入“导入主机”页面：

图 4-23 导入主机页面示意图



(3) 单击<下载模板文件>将模板下载至本地，解压后打开一个主机统计表格进行编辑，如下图：

图 4-24 导入主机表格模板示意图



template.xlsx - Micros

文件 开始 插入 页面布局 公式 数据 审阅 视图 加载项

剪切 复制 格式刷 粘贴 剪贴板 宋体 11 字体 自动换行 合并后居中 对齐方式 常规 数字

B11

	A	B	C	D	E	F
1	#主机IP必填，其他字段可以不填，样例数据如下所示：					
2	#主机IP	主机名称	协议	主机标签	工作部门	备注
3	192.168.50.112	DAS1	TELNET:23	字符主机	运维部	
4	192.168.50.112	DAS2	SSH:22	字符主机	运维部	
5	192.168.50.113	DAS3	FTP:21,TELNET:23	字符主机	运维部	
6	192.168.50.114	DAS4	FTP:21,TELNET:23	字符主机	运维部	
7	192.168.50.115	DAS5	RDP:3389	图形服务器	业务部门	
8	192.168.50.116	DAS6	VNC:5900	图形服务器	业务部门	
9						

说明

第一列为主机 IP（必填项）、第二列为主机名称（必填项）、第三列为网络协议及端口号（必填项）、第四列为主机标签（可选项）、第五列为工作部门（可选项）、第六列为备注说明（可选项）。

网络协议的格式为“协议:端口号”（中间用英文的冒号隔开），如“SSH:22”；如果存在多个协议及端口号，就如“TELNET:23,FTP:21”（中间用英文的逗号隔开）。

主机标签用于对主机进行区分分类的。

(4) 保存表格后，单击<上传文件>，可以选择是否勾选“覆盖已有主机”：

图 4-25 导入主机页面示意图

导入选择 导入全部 覆盖已有主机

共6条数据，当前显示6条，已选择6条。

	主机IP	主机名称	协议	标签	工作部门	备注
☑	192.168.50.112	主机名称	TELNET:23	标签名称	部门	备注
☑	192.168.50.112	主机名称2	SSH:22	标签名称2	部门2	备注2
☑	192.168.50.113	主机名称	FTP:21,SFTP:22	标签名称	部门	备注
☑	192.168.50.114	主机名称	FTP:21,SFTP:22	标签名称	部门	备注
☑	192.168.50.115	主机名称	RDP:3389	标签名称	部门	备注
☑	192.168.50.116	主机名称	VNC:5900	标签名称	部门	备注

说明

勾选“覆盖已有主机”：如果存在相同的主机 IP，将会被覆盖成新的主机信息。

(5) 单击<导入全部>后即可导入成功。

5 授权分配

授权分配有四种方式可选：基于用户授权、基于用户组授权、基于主机授权和基于账户授权。目的是为了让运维人员有权限访问目标主机及帐户。

5.1 基于用户授权

5.1.1 功能简介

用户授权可以基于用户的方式对主机帐户、账户组进行授权管理。

5.1.2 配置描述

(1) 进入[用户/用户管理]界面：

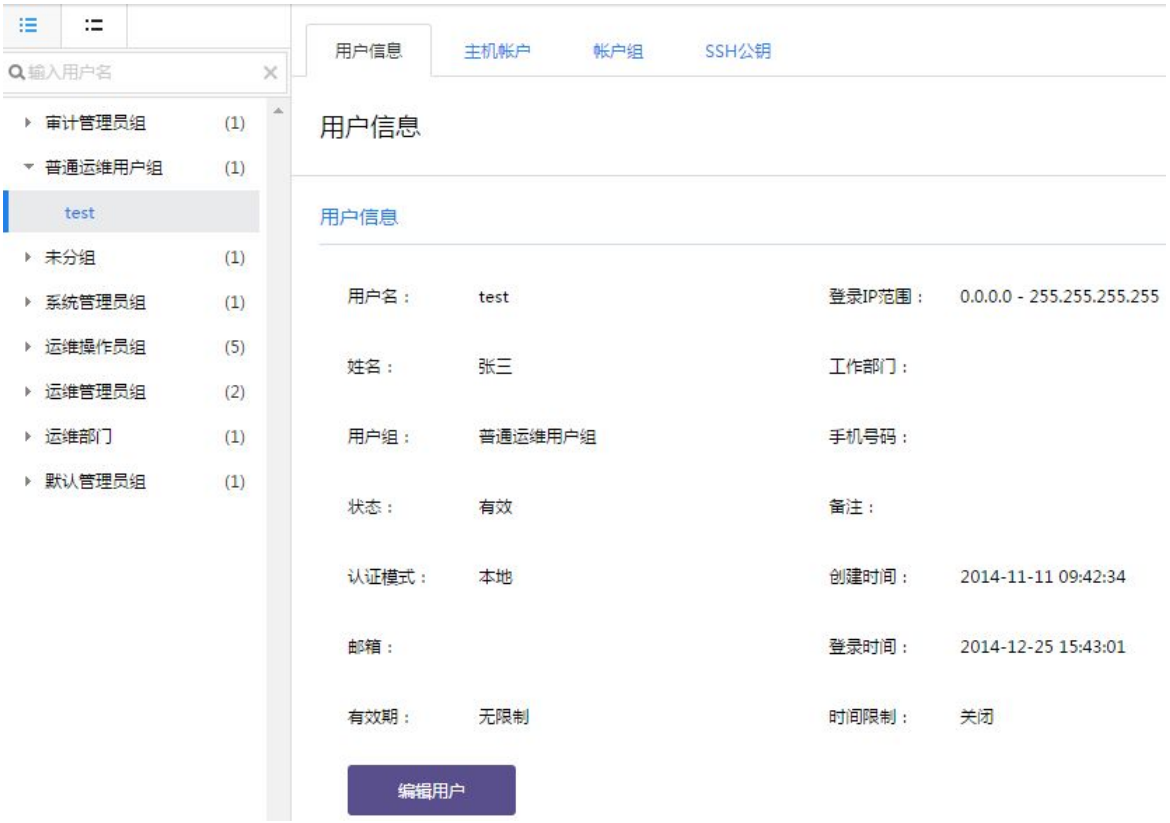
图 5-1 用户管理页面示意图

说明

如果用户信息太多，可以通过右上角的搜索框进行过滤搜索，方便快捷。

(2) 单击某个用户名，进入配置页面：

图 5-2 用户编辑页面示意图



(3) 单击“主机帐户”或“帐户组”，分别可对帐户或帐户组授权：

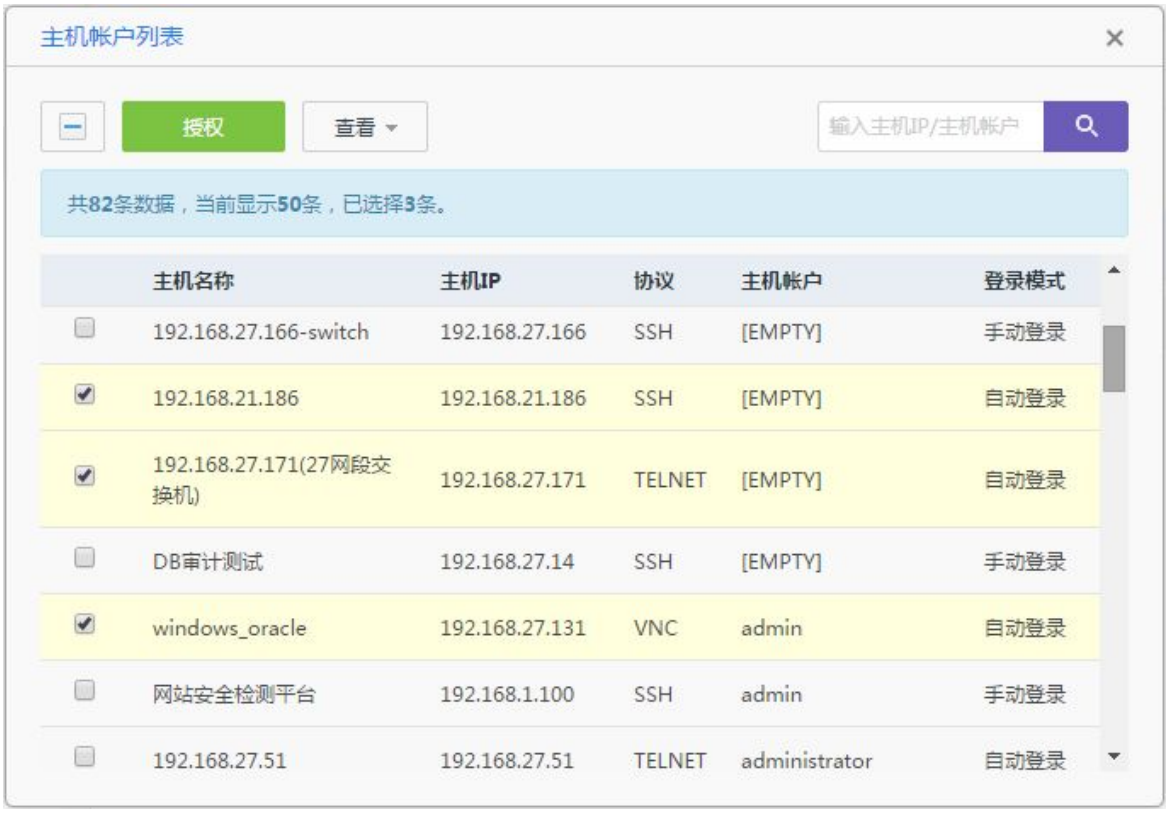
图 5-3 用户授权页面示意图

说明

对主机帐户授权，是对若干个主机帐户进行授权;
对帐户组授权，是对若干个帐户组进行授权。

(4) 单击<+授权>，弹出“主机帐户列表”，勾选需要授权的帐户：

图 5-4 主机帐户列表示意图

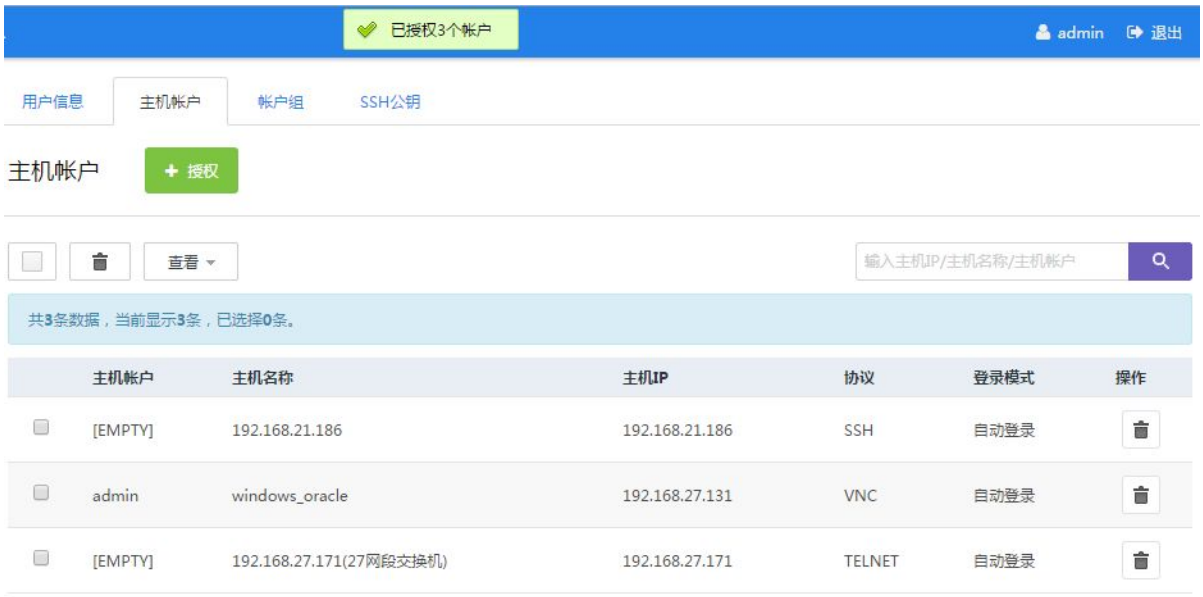


说明

如果帐户太多，可以通过右上角的搜索框进行过滤搜索“主机 IP 或帐户”，方便快捷。

(5) 单击<授权>后即可授权成功，在页面上方会提示“已授权 N 个帐户”：

图 5-5 用户授权页面示意图



5.1.3 配置举例

以给“test”用户分配一个“网络设备帐户组”为例：

(1) 进入[用户/用户管理]界面中，过滤搜索 test 用户：

图 5-6 用户管理页面示意图

(2) 单击“test”用户名，进入用户配置页面：

图 5-7 用户管理页面示意图

(3) 单击“帐户组”下的<+授权>，弹出“帐户组列表”页面，在页面中勾选“网络设备帐户组”：

图 5-8 帐户组列表示意图

(4) 单击<授权>后即可授权成功，并在页面上方提示“已授权 N 个帐户组”：

图 5-9 用户授权页面示意图

5.2 基于用户组授权

5.2.1 功能简介

用户组授权可以基于用户组别的方式对主机帐户、账户组进行授权管理。

5.2.2 配置描述

(1) 进入[用户/用户组管理]界面，搜索或者挑选“某个用户组”：

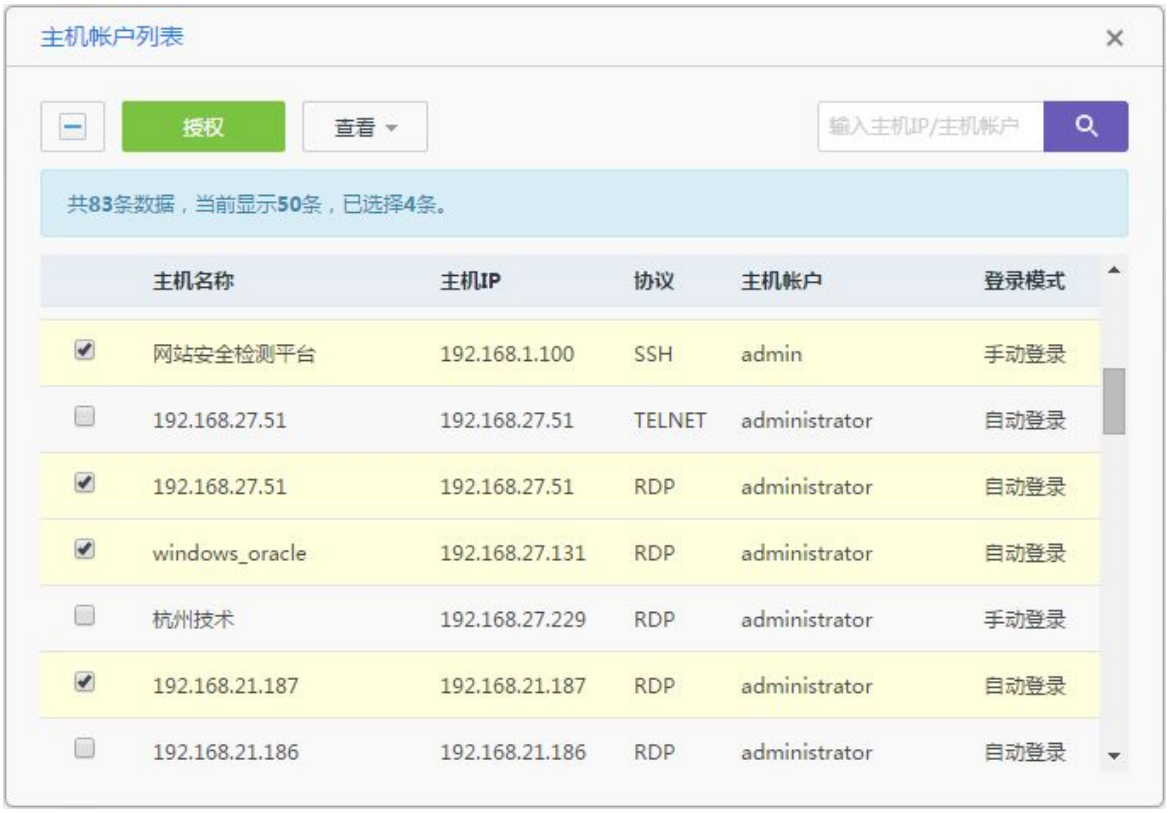
图 5-10 用户组管理页面示意图

(2) 单击“某个用户组”后，进入配置页面：

图 5-11 用户组授权页面示意图

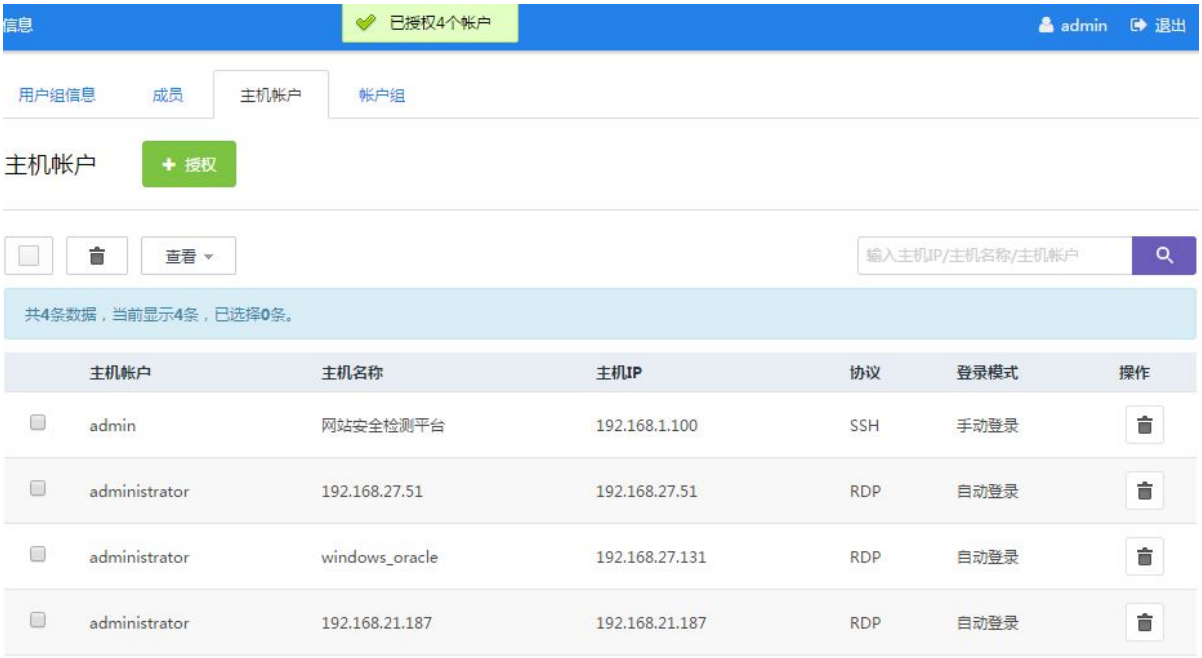
(3) 单击[主机帐户]下的<+授权>，弹出“主机帐户列表”，在列表中勾选需要授权的主机帐户：

图 5-12 主机帐户列表示意图



(4) 单击<授权>后即可授权成功，并在页面上方提示“已授权 N 个帐户”：

图 5-13 用户组授权页面示意图

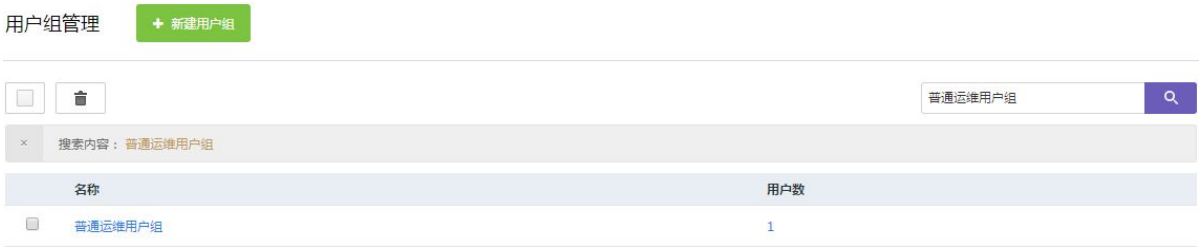


5.2.3 配置案例

以将“网络设备帐户组”授权给用户组“普通运维用户组”为例。

(1) 进入[用户/用户组管理]界面中，搜索“普通运维用户组”：

图 5-14 用户管理页面示意图



(2) 单击“普通运维用户组”，进入配置页面：

图 5-15 用户组授权页面示意图

(3) 进入[帐户组]页面，单击<+授权>，弹出“帐户组列表”，勾选“网络设备帐户组”：

图 5-16 帐户组列表示意图

(4) 单击<授权>后即可授权成功，并在页面的上方提示“已授权 N 个帐户组”：

图 5-17 用户组授权页面示意图

5.3 基于主机及帐户授权

5.3.1 功能简介

主机及帐户授权可以基于主机及帐户的方式对用户、用户组进行授权管理。

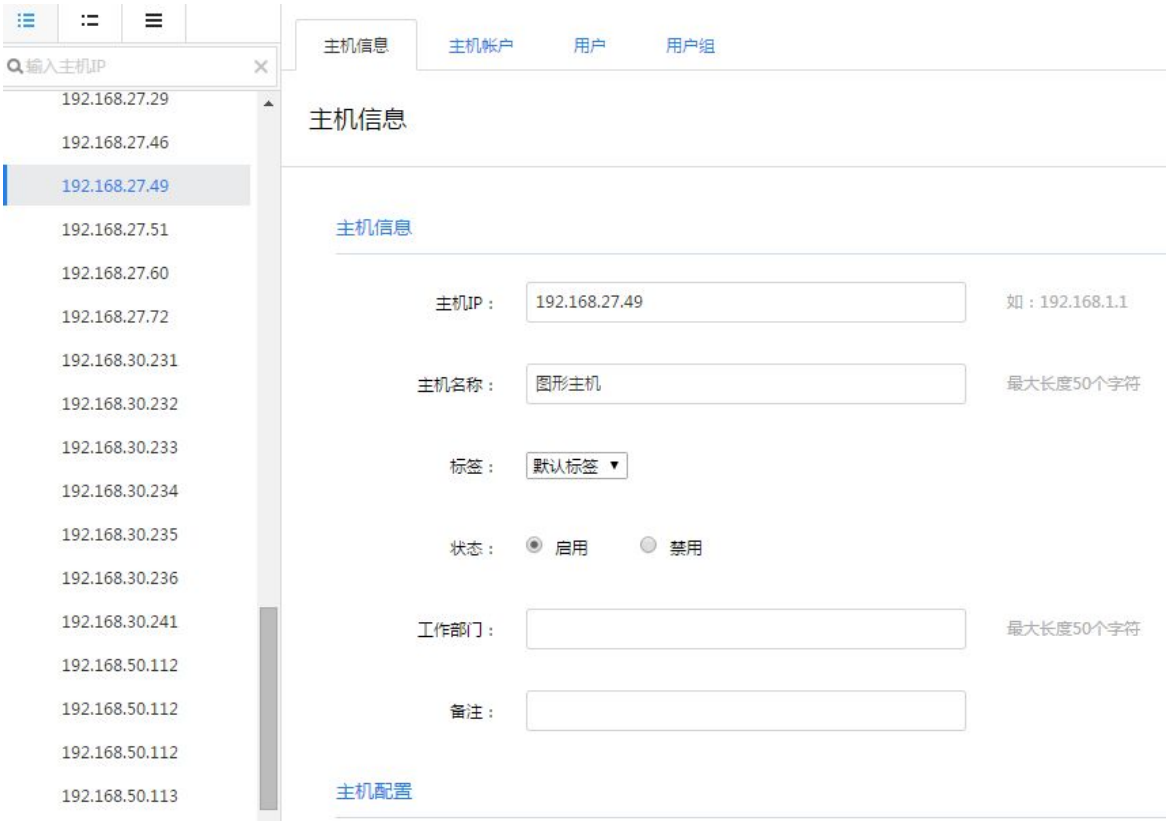
5.3.2 配置描述

(1) 进入[资产/主机管理]界面，如果主机很多，可以搜索主机 IP 或主机名称，过滤需要授权的主机：

图 5-18 主机管理页面示意图

(2) 单击“主机 IP”，进入配置页面：

图 5-19 主机编辑页面示意图

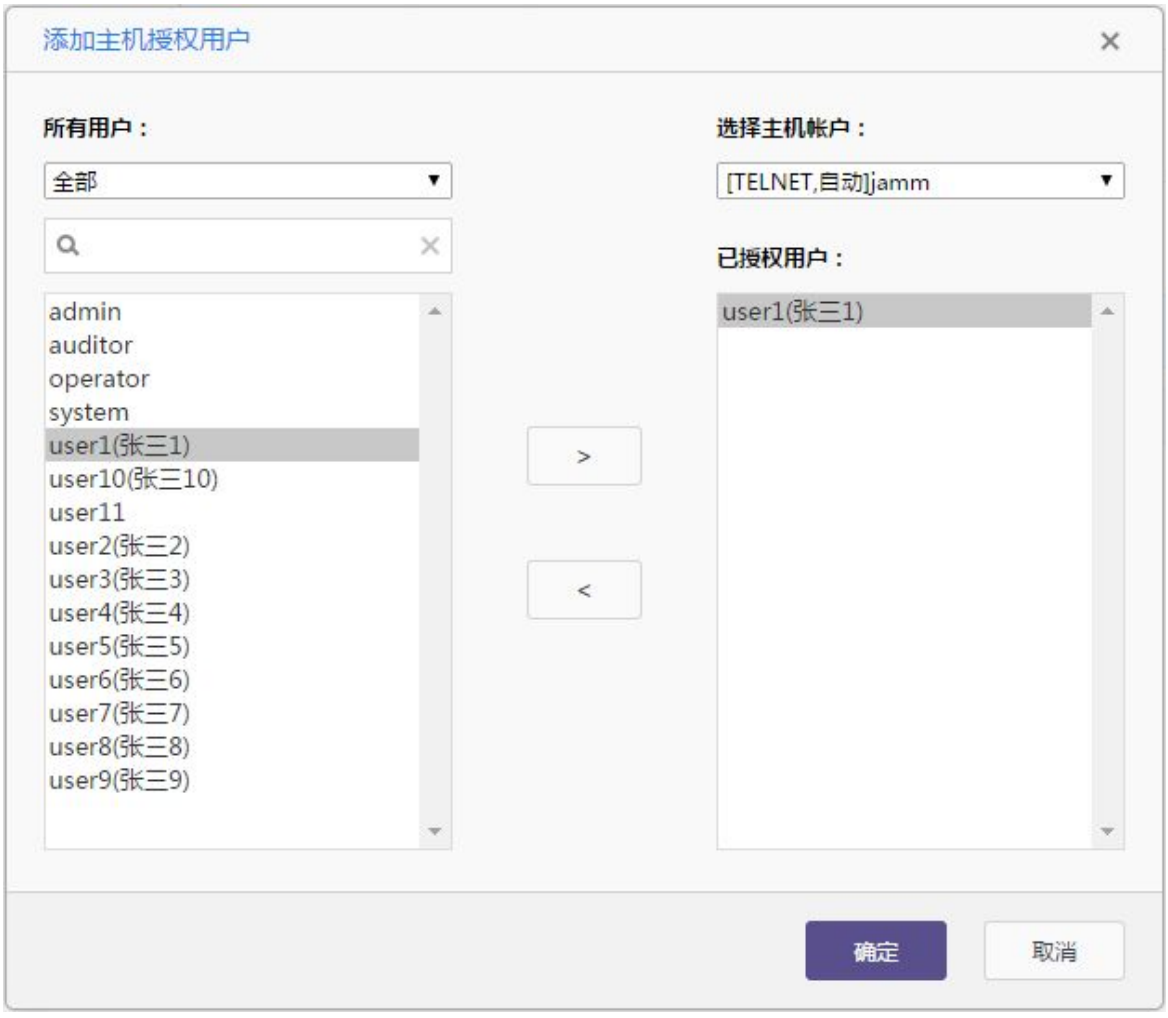


(3) 单击[用户]或者[用户组]，进入授权配置页面：

图 5-20 主机授权页面示意图

(4) 单击<+授权>，弹出“添加主机授权用户”窗口，先“选择主机帐户”，再将左边的用户移至右侧：

图 5-21 主机授权用户页面示意图



提示

先选择主机帐户，再选择用户。

(5) 单击<确定>后即可授权成功，并在页面上方提示“授权用户已保存”：

图 5-22 主机授权页面示意图

5.3.3 配置举例

以交换机授权给普通运维用户组为例：

(1) 进入[资产/主机管理]界面，找到“交换机”：

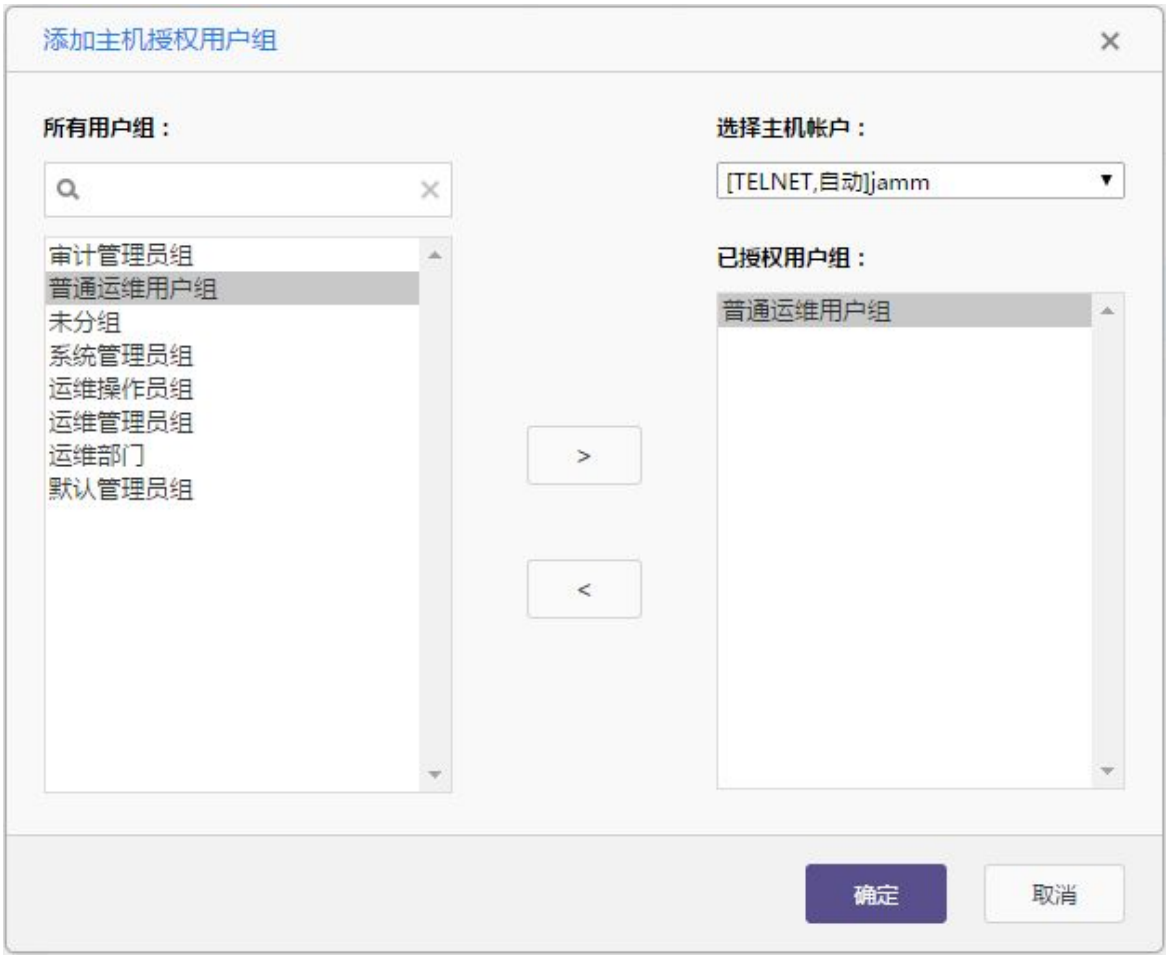
图 5-23 主机授权用户页面示意图

(2) 单击“设备的 IP”，进入配置页面，然后单击[用户组]，进入授权页面：

图 5-24 主机授权用户组管理页面示意图

(3) 单击<+授权>后，弹出“添加主机授权用户组”窗口，先选择交换机的帐户，再选择普通运维用户组：

图 5-25 主机授权用户组页面示意图



(4) 单击<确定>后即可授权成功，并在页面的上方提示“授权用户组已保存”：

图 5-26 主机授权用户组管理页面示意图

5.4 基于帐户组授权

5.4.1 功能简介

帐户组授权可以基于帐户组别的方式对用户、用户组组进行授权管理。

5.4.2 配置描述

(1) 进入[资产/帐户管理]界面，找到需要授权的帐户组：

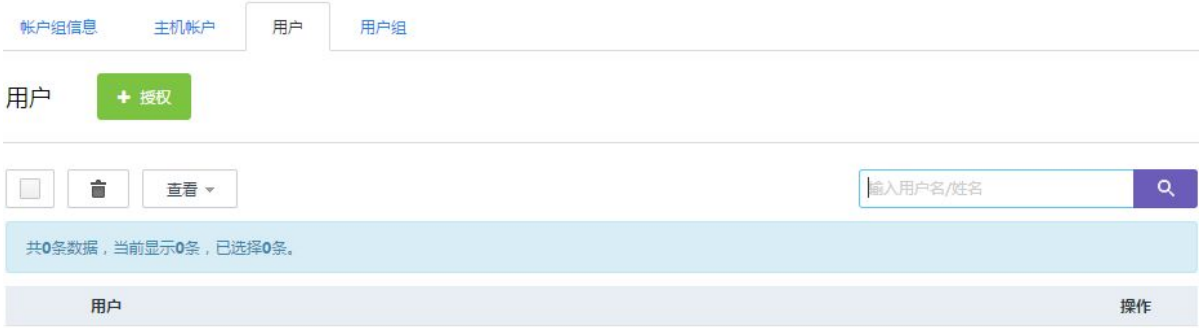
图 5-27 帐户组管理页面示意图

(2) 单击某个账户组，进入配置页面：

图 5-28 帐户组编辑页面示意图

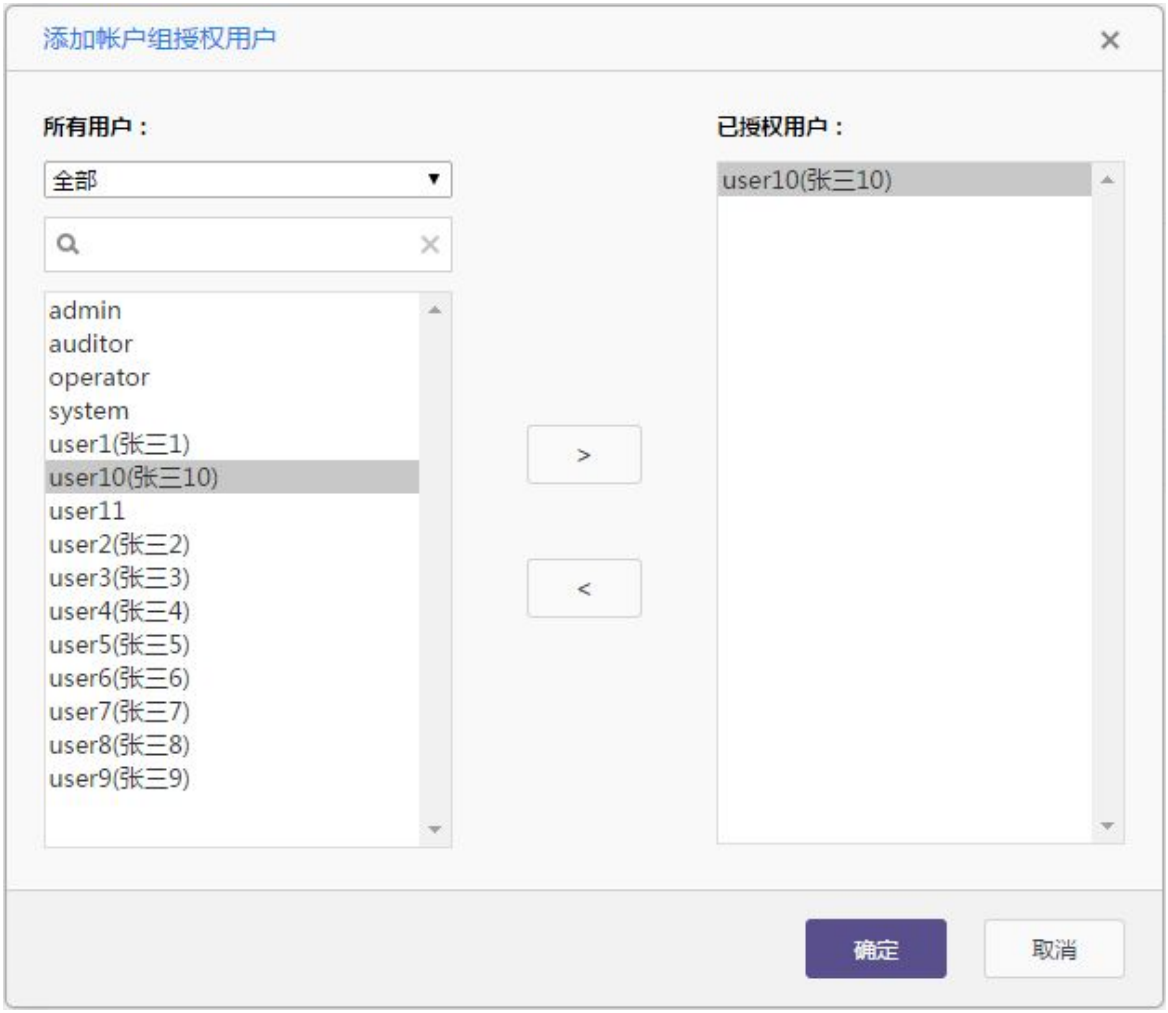
(3) 单击[用户]或[用户组]，进入授权页面：

图 5-29 帐户组授权用户管理页面示意图



(4) 单击<+授权>，弹出“添加帐户组授权用户”窗口，将左侧的用户移至右侧：

图 5-30 帐户组授权用户页面示意图



(5) 单击<确定>后即可授权成功。

5.4.3 配置举例

以给网络设备帐户组授权普通运维用户组为例。

(1) 进入[资产/帐户管理]界面，找到网络设备帐户组：

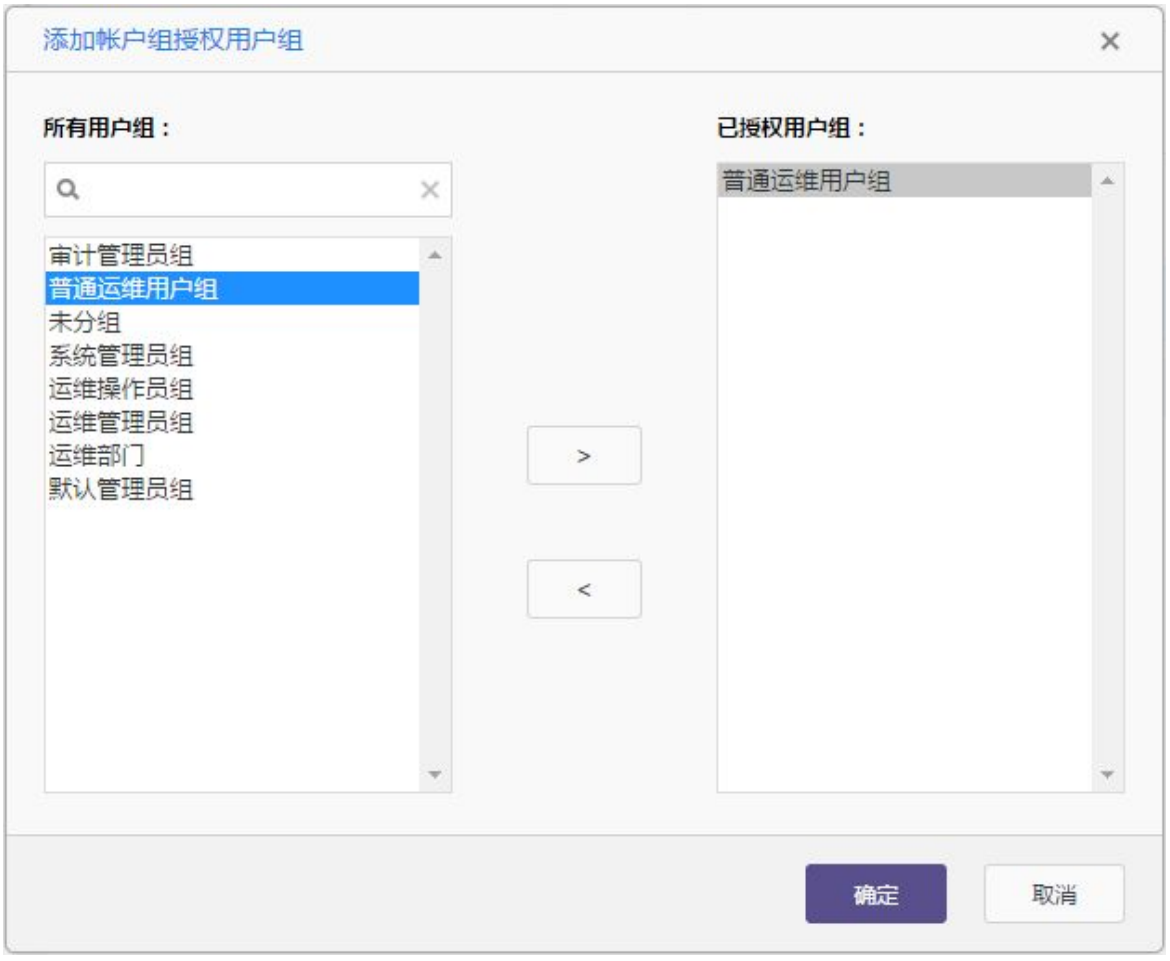
图 5-31 帐户组管理页面示意图

(2) 单击“网络设备帐户组”，进入配置页面，单击[用户组]，进入授权页面：

图 5-32 帐户组授权用户组页面示意图

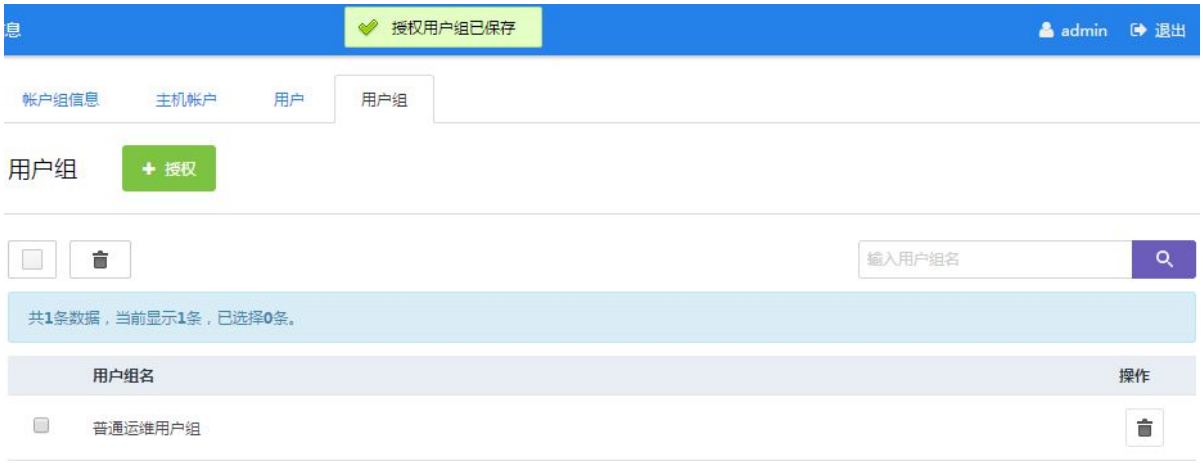
(3) 单击<+授权>，弹出“添加帐户组授权用户组”窗口，将左侧的普通运维用户组移至右侧：

图 5-33 帐户组授权用户组页面示意图



(4) 单击<确定>后即可授权成功，并在页面上方提示“授权用户组已保存”：

图 5-34 帐户组授权用户组页面示意图



6 工具下载

工具下载用于运维人员在登录主机前的下载需要用到的运维工具。

6.1 单点登录器

(1) 进入[运维/工具下载]页面中。

(2) 下载“单点登录器”并安装在本地。

提示

单点登录器是用于 Web 方式调用运维客户端工具时，须安装的登录工具。

6.2 IE代填工具

(1) 进入[运维/工具下载]页面中。

(2) 下载“IE 代填工具”。

(3) 上传至应用服务器中，并安装好。

提示

IE 代填工具用于发布 IE 代填应用时的辅助工具。

6.3 USBKEY控件(IE)

(1) 进入[运维/工具下载]页面中。

(2) 下载“USBKEY 控件”并安装在本地。

提示

USBKEY 控件用于明御运维审计与风险控制系统（堡垒机）启用 USBKEY 认证方式时的登录工具。

6.4 离线播放器与Adobe AIR

(1) 进入[运维/工具下载]页面中。

(2) 下载“离线播放器”与“Adobe ATR”，并安装在本地。

提示

离线播放器与 Adobe ATR 是用于会话审计里的日志导出后进行离线查看的工具。

6.5 Flash Player

(1) 进入[运维/工具下载]页面中。

(2) 下载“Flash Player”，并安装在本地。

提示

Flash Player 用于通过 Web 方式查看会话审计的日志。

6.6 字符客户端

(1) 进入[运维/工具下载]页面中。

(2) 下载支持 SSH 和 telnet 协议的客户端工具，并安装在本地。

提示

客户端工具用于连接 SSH、telnet 协议的主机

6.7 图形客户端

(1) 进入[运维/工具下载]页面中。

(2) 下载支持 RDP 和 VNC 协议的客户端工具，并安装在本地。

提示

图形客户端工具用于连接 windows 服务器、VNC 服务器

6.8 文件传输客户端

(1) 进入[运维/工具下载]页面中。

(2) 下载支持 SFTP 和 FTP 协议的客户端工具，并安装在本地。

提示

文件传输客户端工具用于连接 SFTP/FTP 服务器。

7 主机运维

主机运维用于运维人员登录主机的 Web 页面。

7.1 全局配置

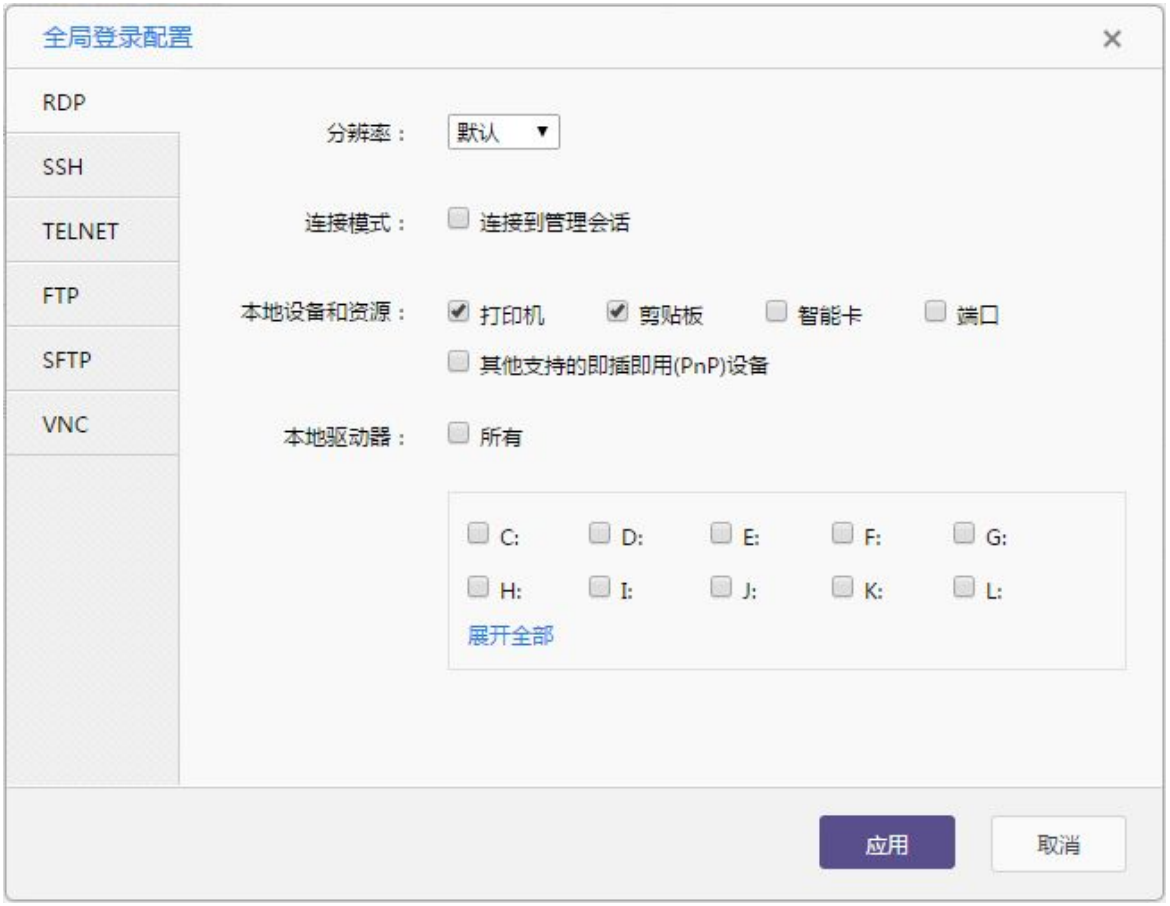
7.1.1 配置 RDP 参数

(1) 进入[运维/主机运维]页面。

图 7-1 主机运维页面示意图

(2) 单击右上角是<⚙>，默认进入 RDP 配置页面。设置分辨率、连接模式、本地设备和资源、本地驱动。

图 7-2 全局登录配置页面示意图

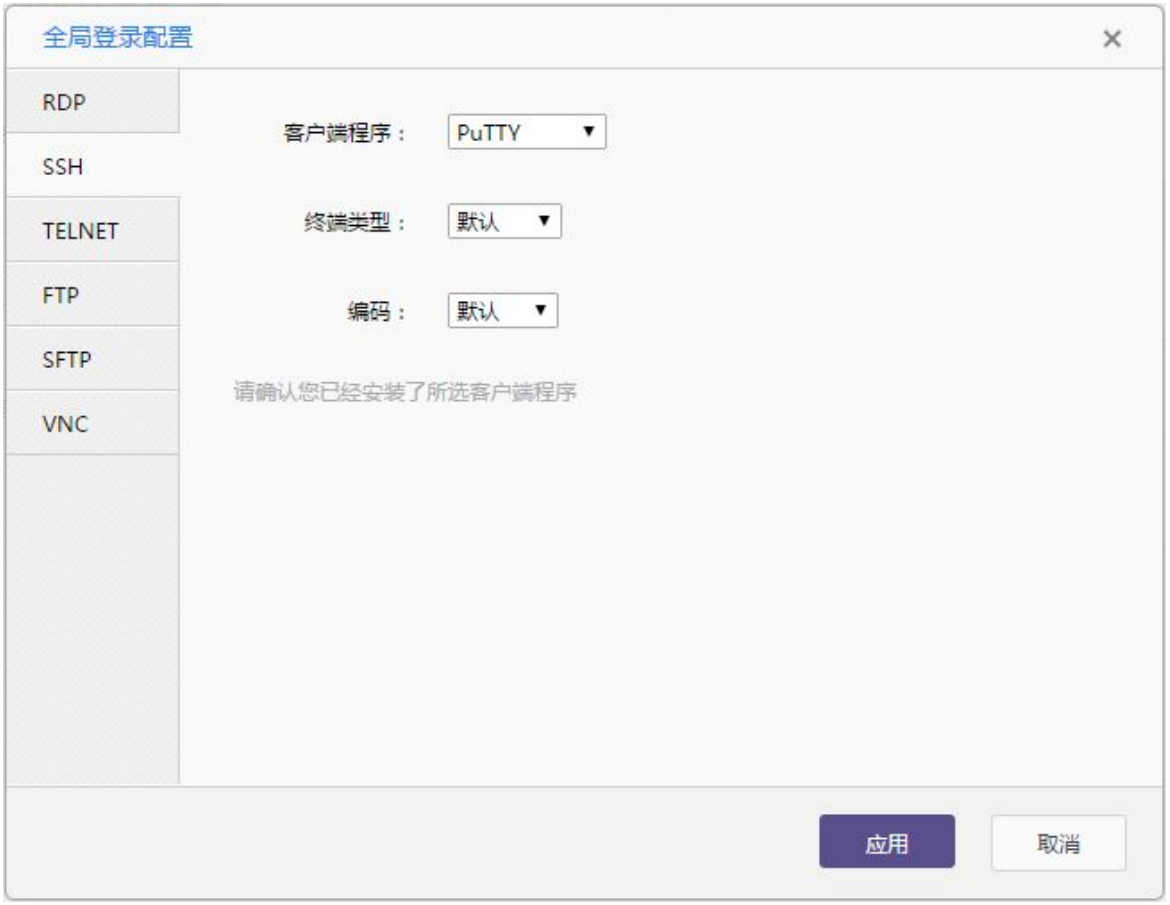


(3) 单击<应用>即可生效。

7.1.2 配置 SSH 参数

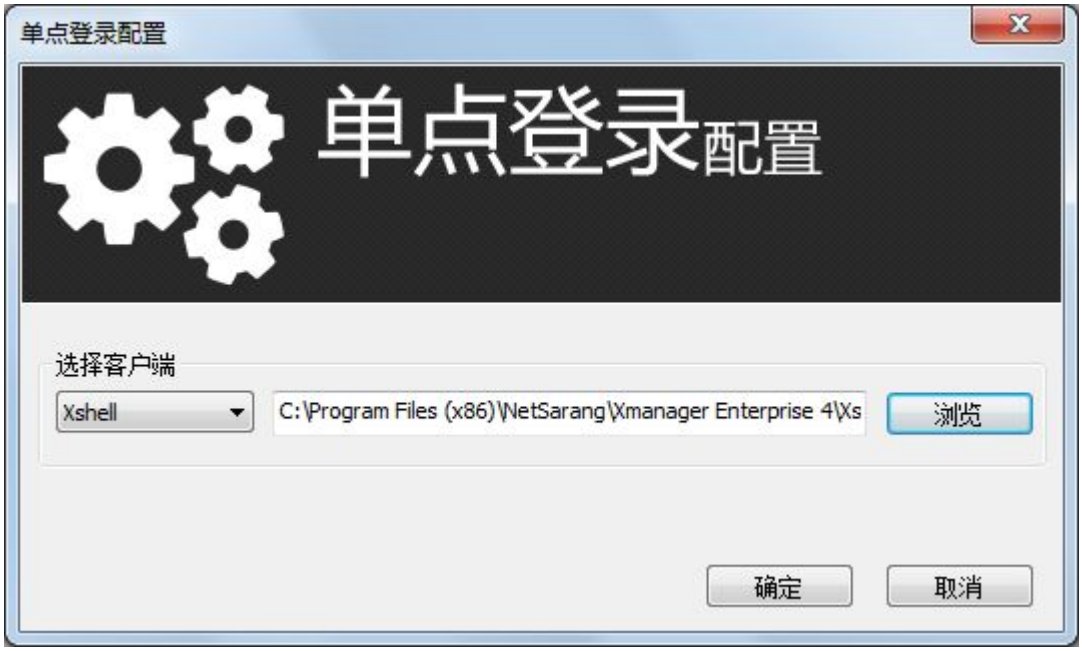
(1) 单击<SSH>，进入配置页面。选择客户端程序、终端类型、编码格式。

图 7-3 全局登录配置页面示意图



(2) 单击<应用>后，弹出窗口。指定本地的应用程序。

图 7-4 单点登录配置页面示意图



(3) 单击<确定>后，提示配置成功。

图 7-5 配置成功提示示意图

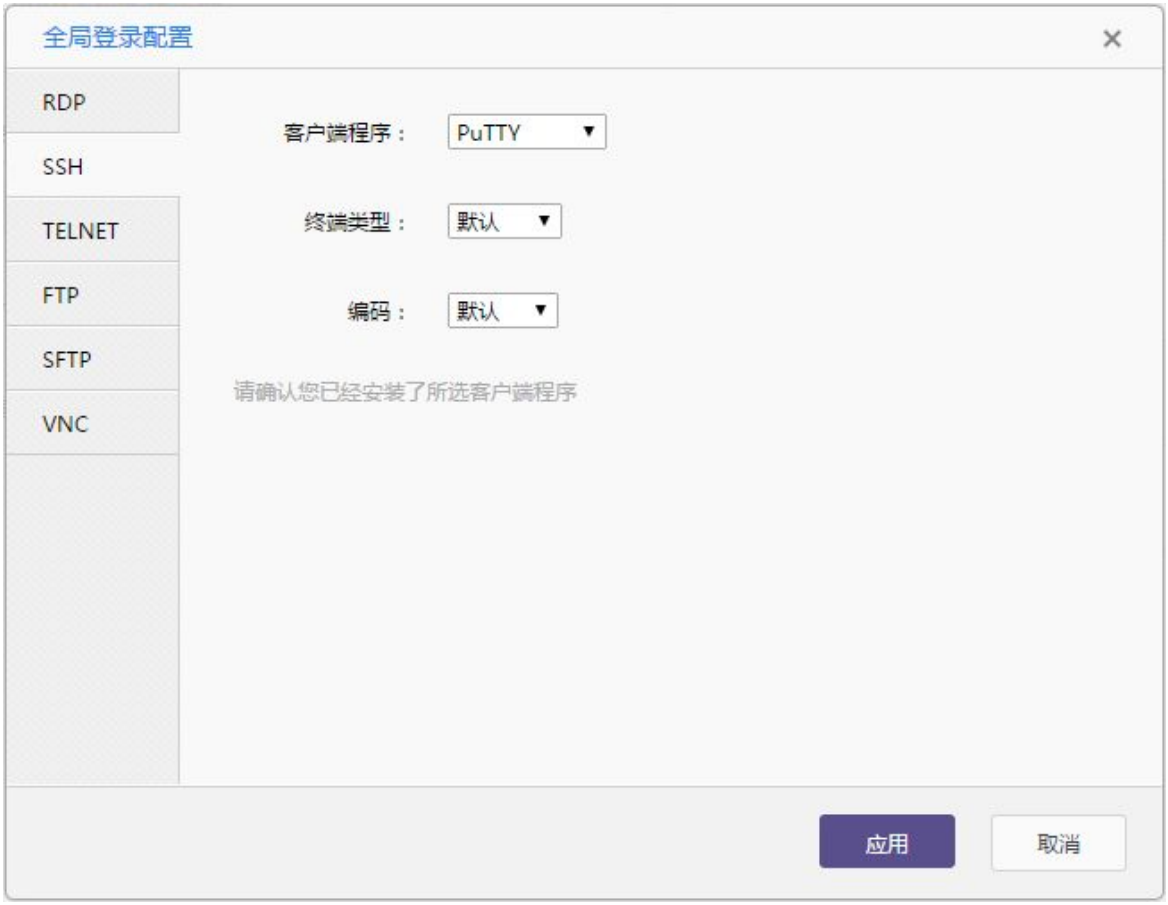
(4) 单击<确定>后生效。

(5) 配置完成之后，关闭页面即可。

7.1.3 配置 telnet 参数

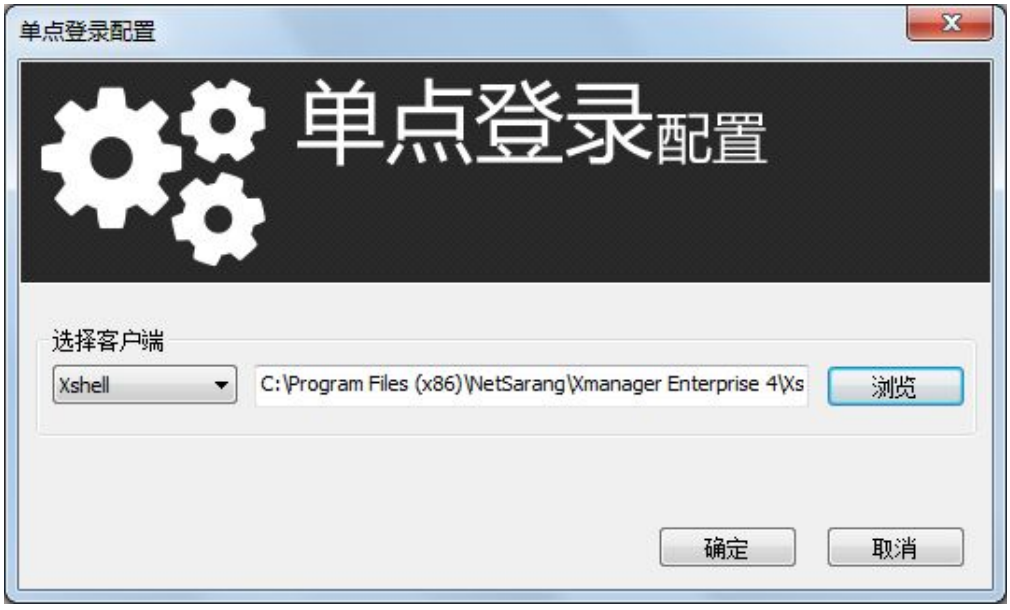
(1) 单击<TELNET>，进入配置页面。

图 7-6 全局登录配置页面示意图



(2)　单击<应用>后，弹出窗口。指定本地的应用程序。

图 7-7 单点登录配置页面示意图



(3) 单击<确定>后，提示配置成功。

图 7-8 配置成功提示示意图

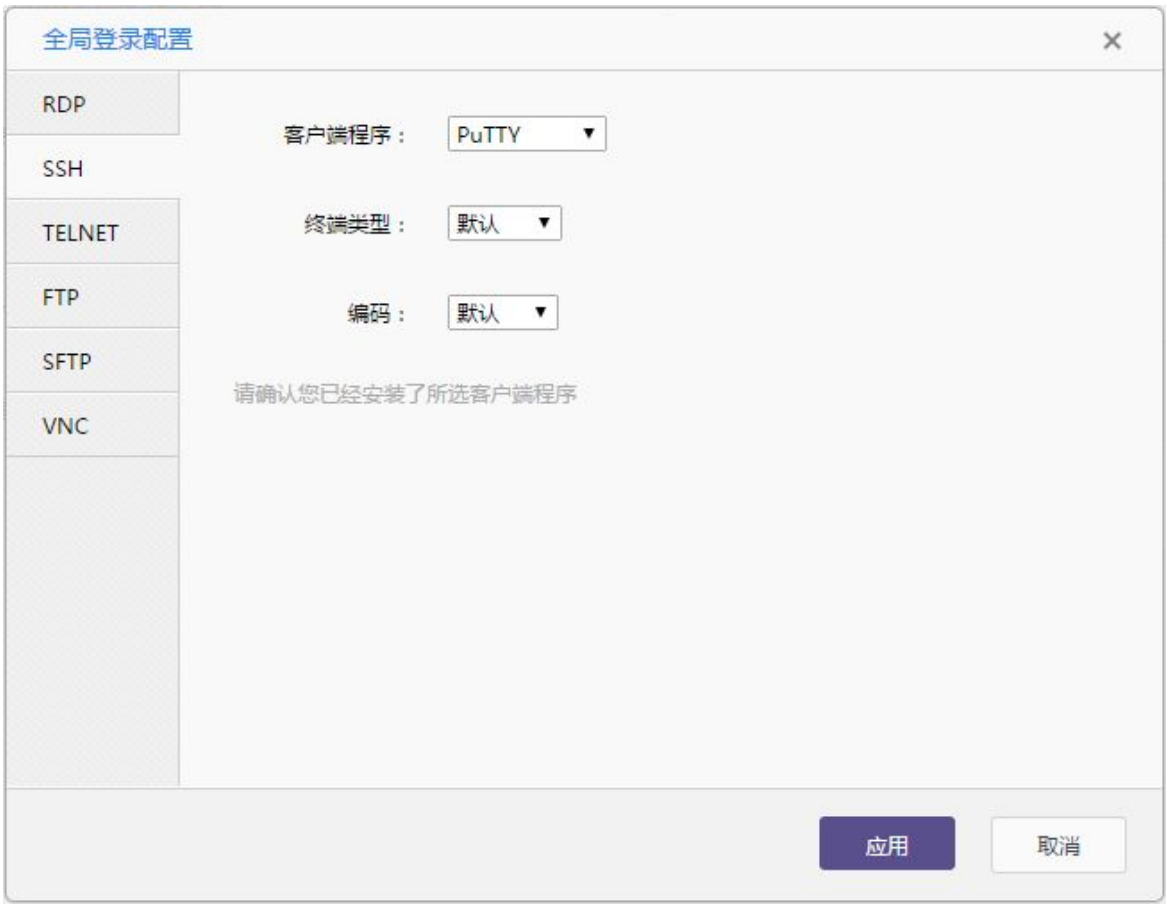
(4) 单击<确定>后生效。

(5) 配置完成之后，关闭页面即可。

7.1.4 配置 FTP 参数

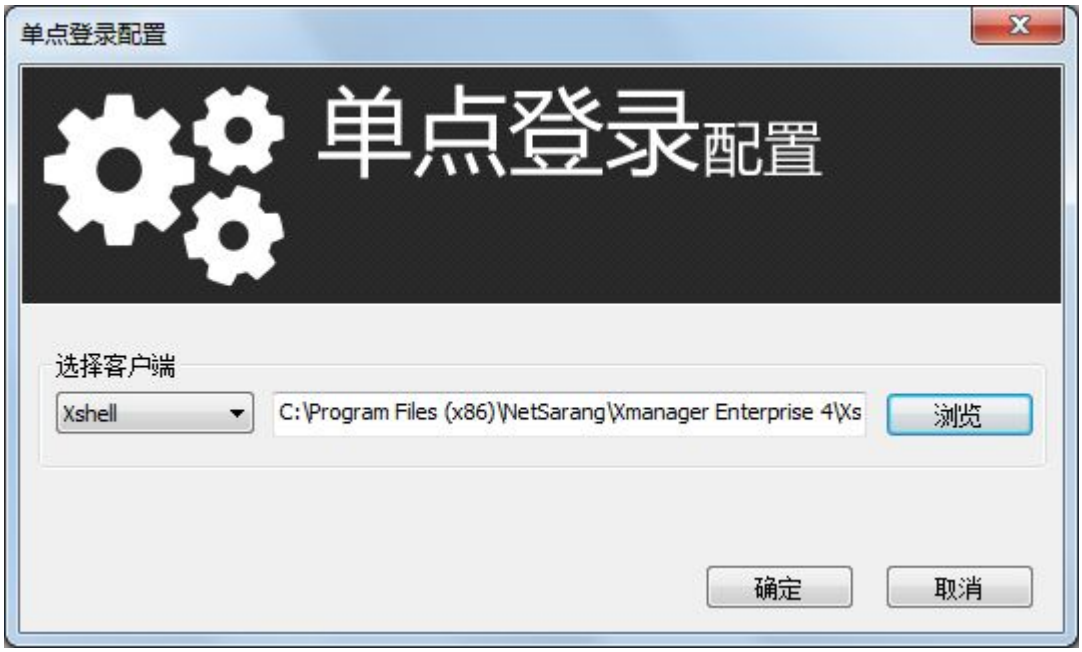
(1) 单击<SFTP>，进入配置页面。

图 7-9 全局登录配置页面示意图



(2) 单击<应用>后，弹出窗口。指定本地的应用程序。

图 7-10 单点登录配置页面示意图



(3) 单击<确定>后，提示配置成功。

图 7-11 配置成功提示示意图

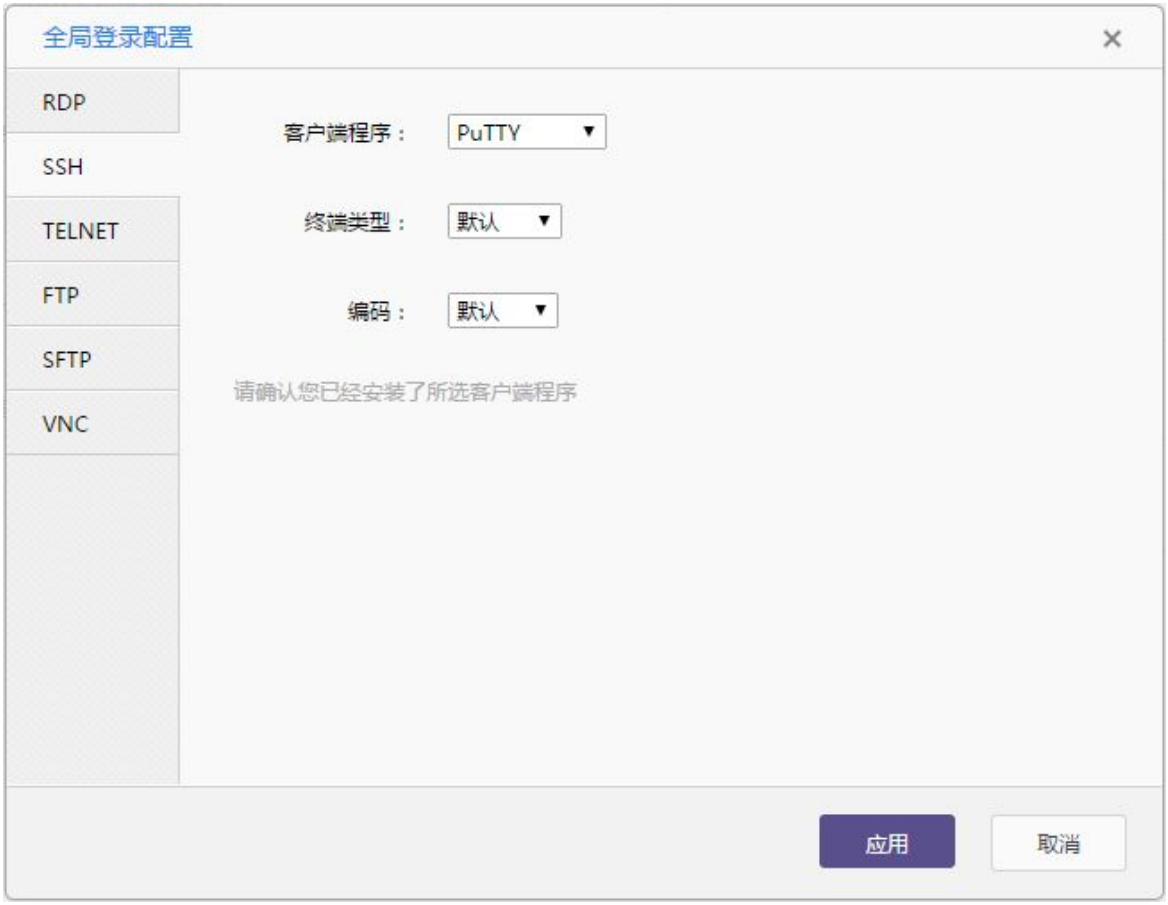
(4) 单击<确定>后生效。

(5) 配置完成之后，关闭页面即可。

7.1.5 配置 SFTP 参数

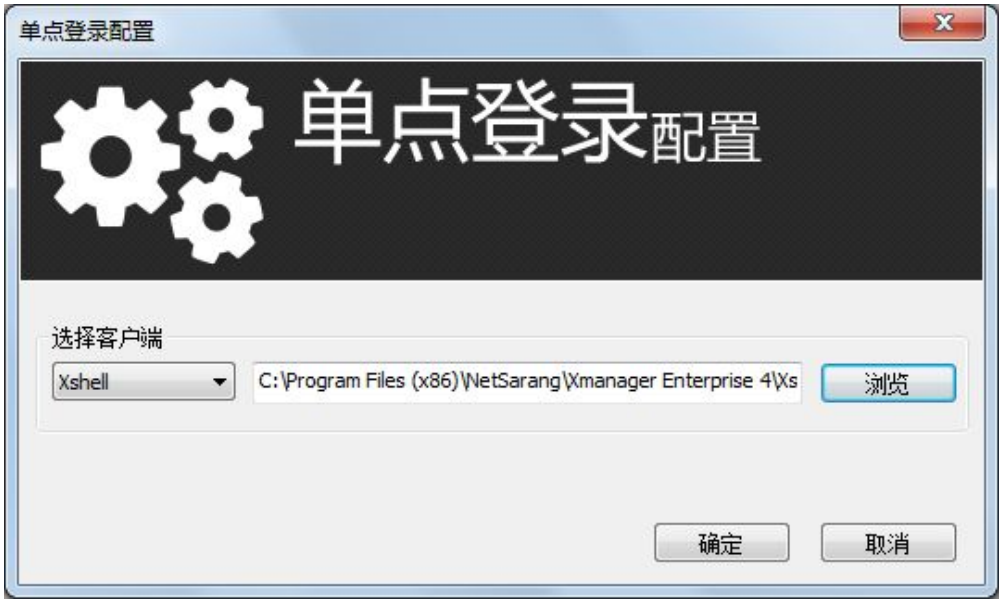
(1) 单击<SFTP>，进入配置页面。

图 7-12 全局登录配置页面示意图



(2)　单击<应用>后，弹出窗口。指定本地的应用程序。

图 7-13 单点登录配置页面示意图



(3) 单击<确定>后，提示配置成功。

图 7-14 配置成功提示示意图

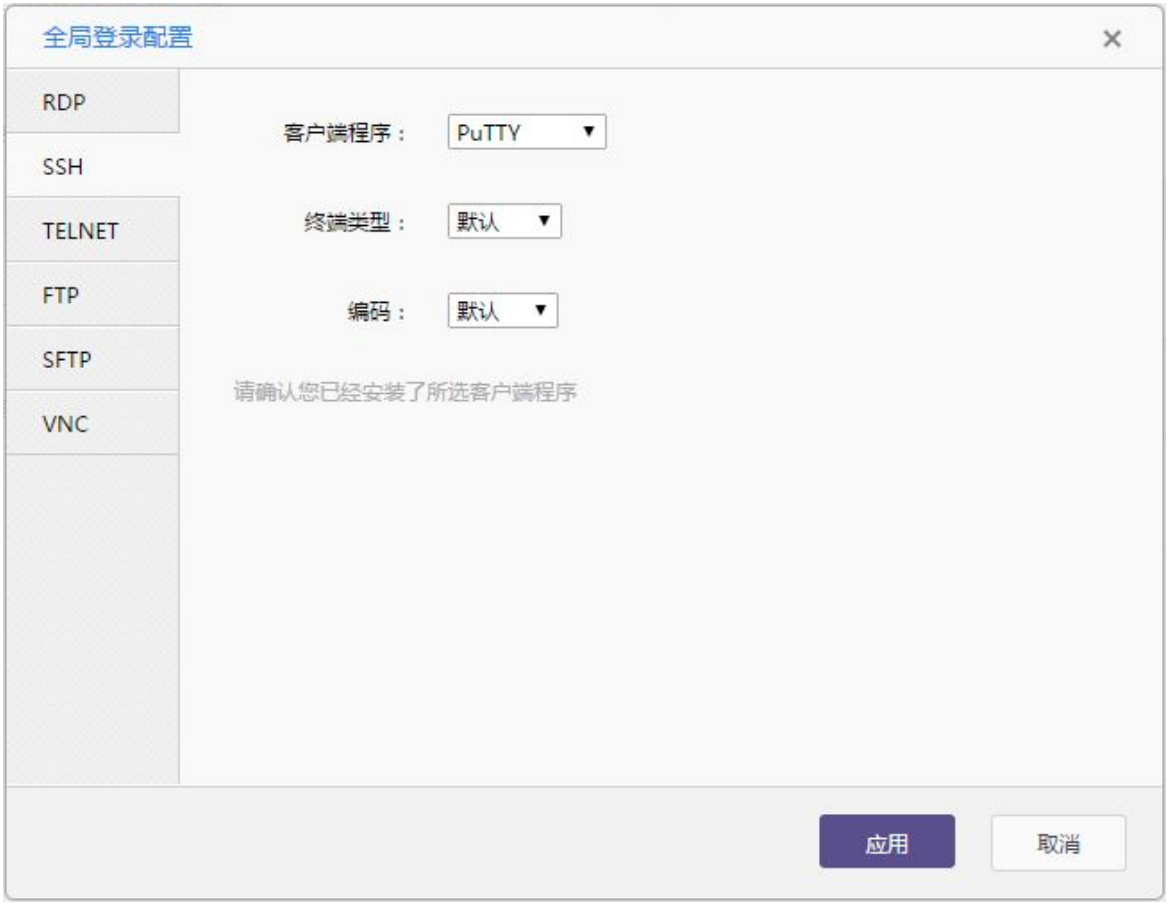
(4) 单击<确定>后生效。

(5) 配置完成之后，关闭页面即可。

7.1.6 配置 VNC 参数

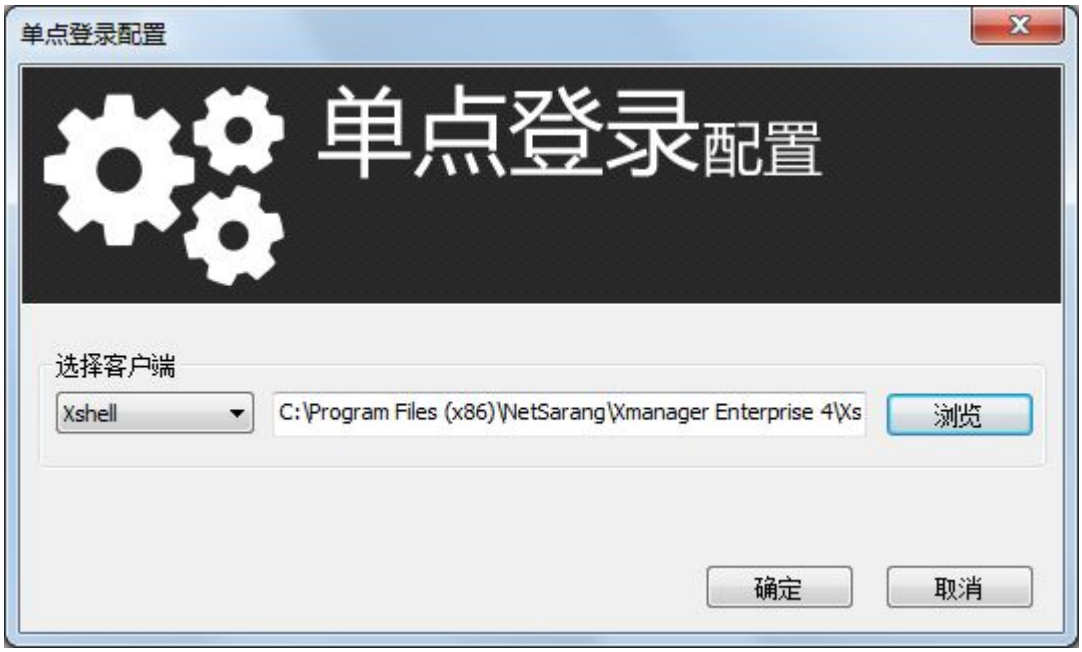
(1) 单击<VNC>，进入配置页面。

图 7-15 全局登录配置页面示意图



(2) 单击<应用>后，弹出窗口。指定本地的应用程序。

图 7-16 单点登录配置页面示意图



(3) 单击<确定>后，提示配置成功。

图 7-17 配置成功提示示意图

(4) 单击<确定>后生效。

(5) 配置完成之后，关闭页面即可。

7.2 主机登录

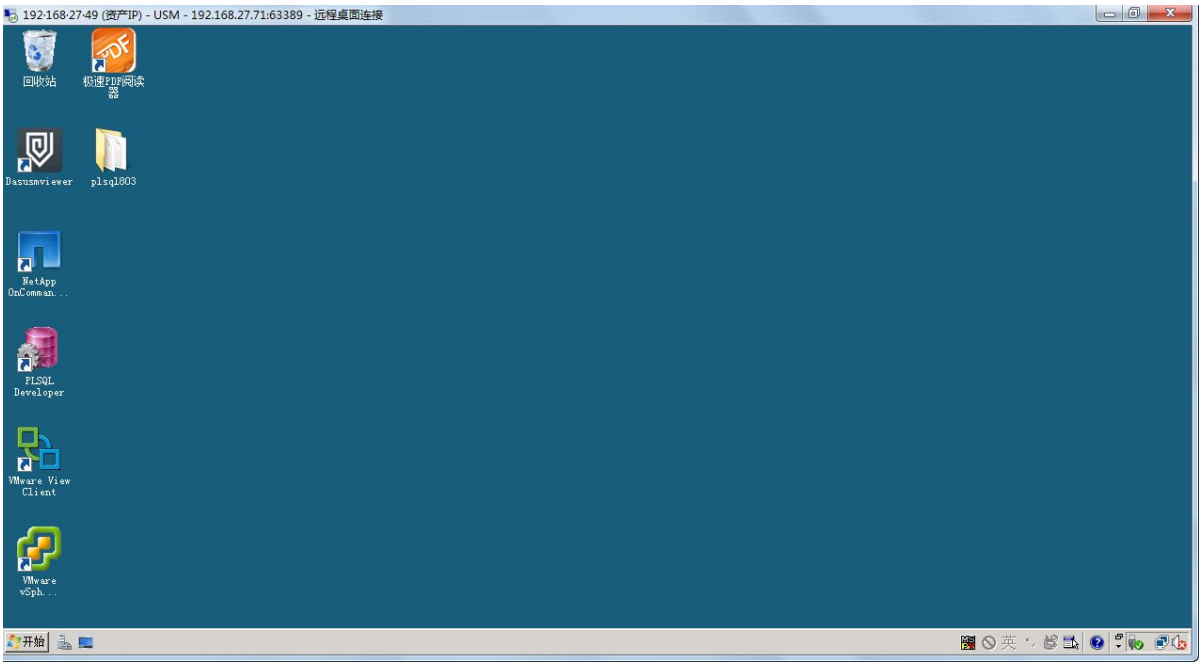
7.2.1 RDP 主机登录

(1) 进入[运维/主机运维]页面。以 windows2008 为例。

图 7-18 主机运维页面示意图

(2) 单击<>后即可登录成功。

图 7-19 主机登录成功示意图



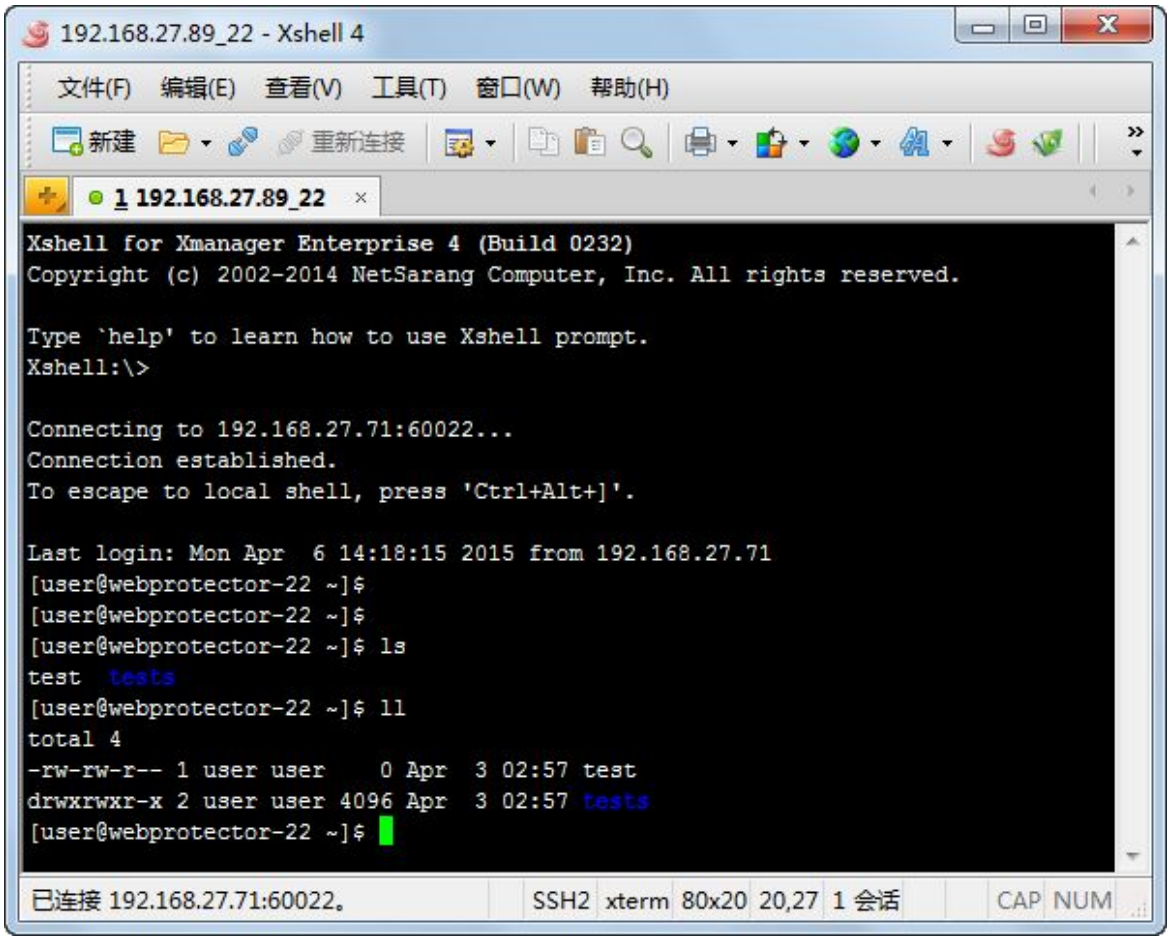
7.2.2 SSH/telnet 主机登录

(1) 进入[运维/主机运维]页面。以 centOS 为例。

图 7-20 主机运维页面示意图

(2) 单击<>后即可登录成功。

图 7-21 主机登录成功示意图



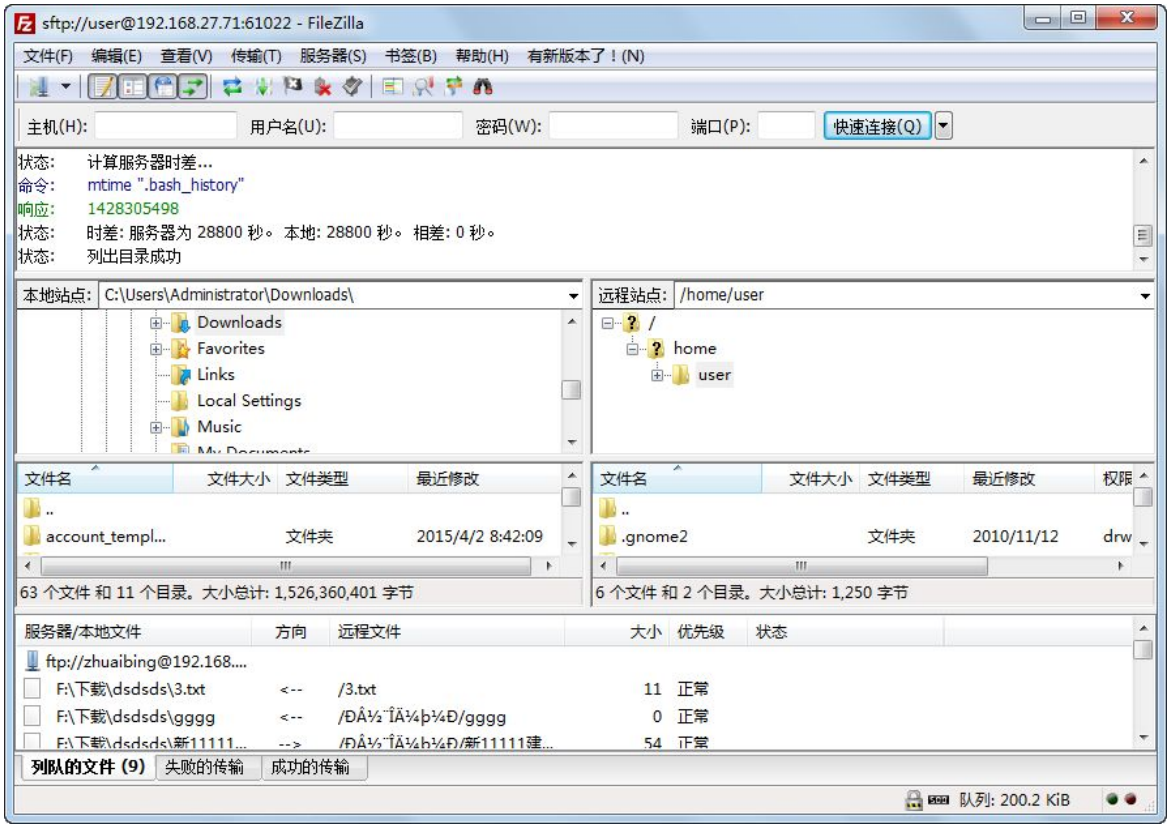
7.2.3 FTP/SFTP 主机登录

(1) 进入[运维/主机运维]页面。以 SFTP 服务器为例。

图 7-22 主机运维页面示意图

(2) 单击<>后即可登录成功。

图 7-23 主机登录成功示意图



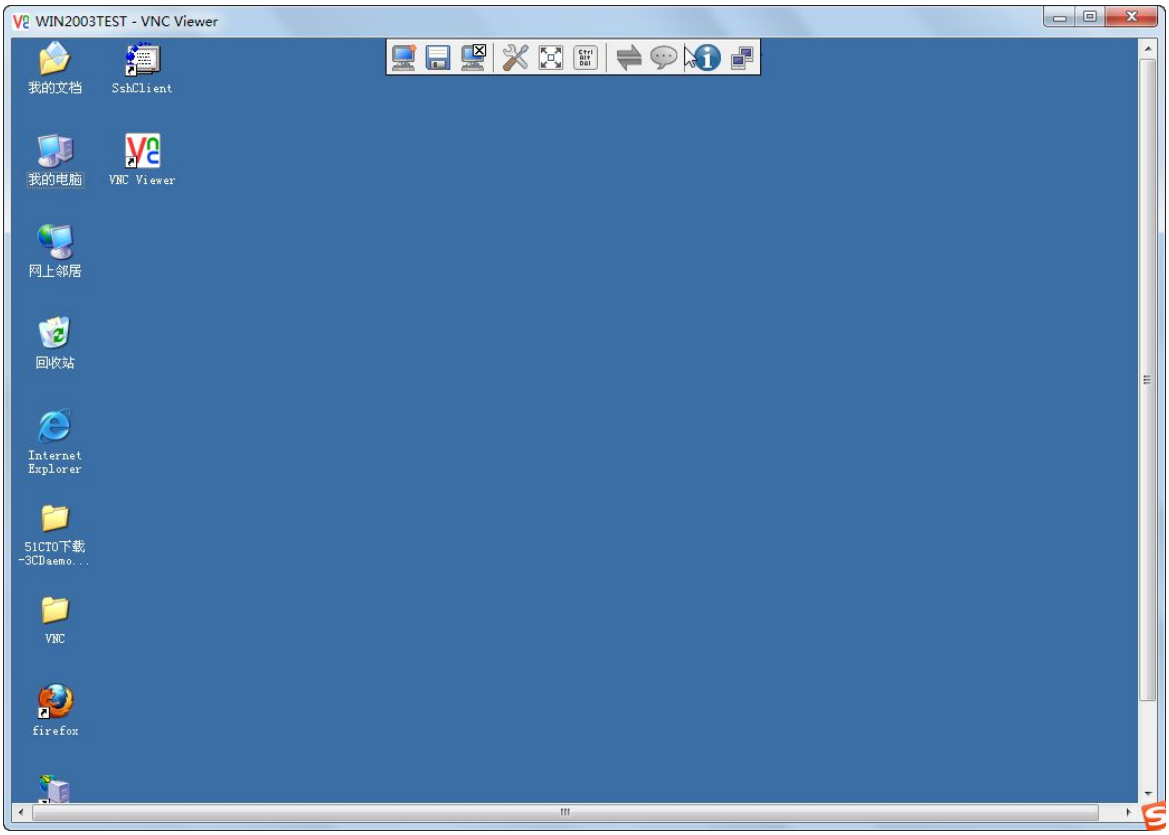
7.2.4 VNC 主机登录

(1) 进入[运维/主机运维]页面。以 VNC 服务器为例。

图 7-24 主机运维页面示意图

(2) 单击<>后即可登录成功。

图 7-25 主机登录成功示意图



7.3 快速搜索

(1) 进入[运维/主机运维]页面。

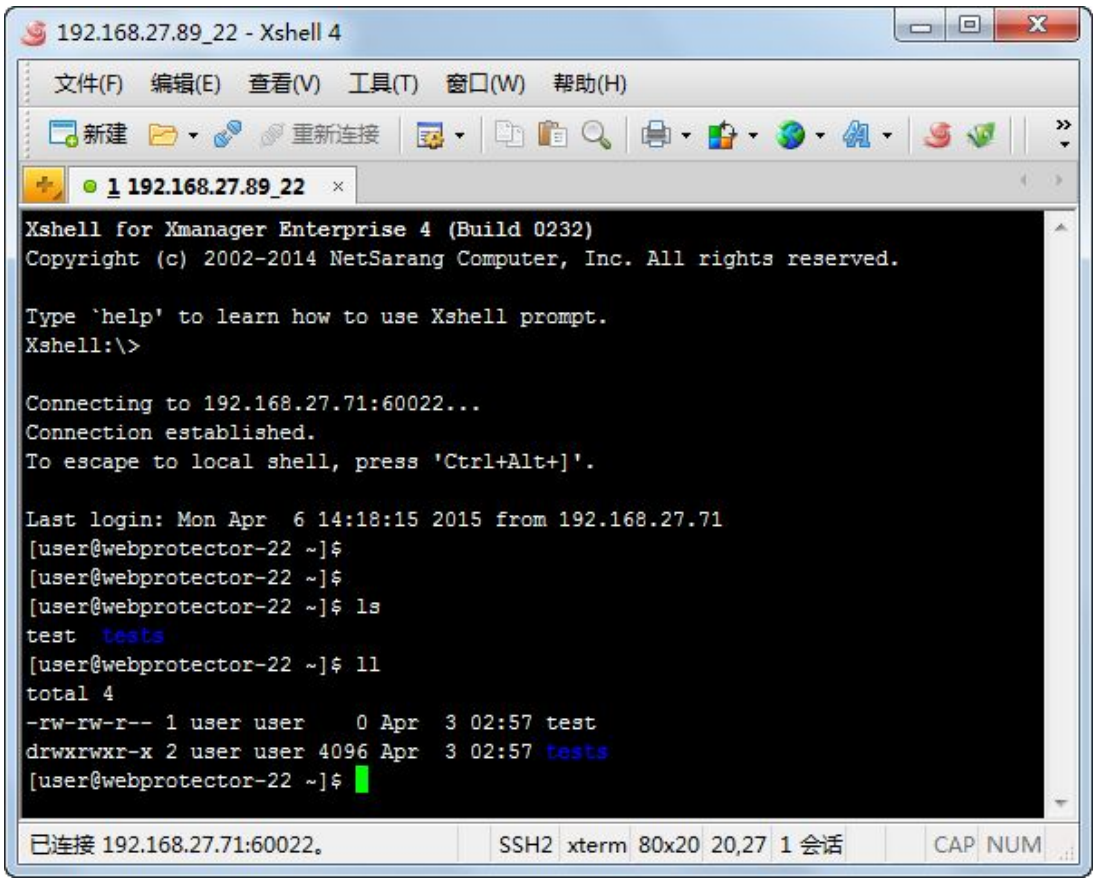
图 7-26 主机运维搜索框示意图

(2) 在搜索框中输入主机 IP/主机名/账户名、或关键信息，系统会自动过滤出与目标主机有关的信息。

图 7-27 主机搜索成功示意图

(3) 单击需要登录的目标主机及帐户后，即可成功登录。

图 7-28 主机登录成功示意图

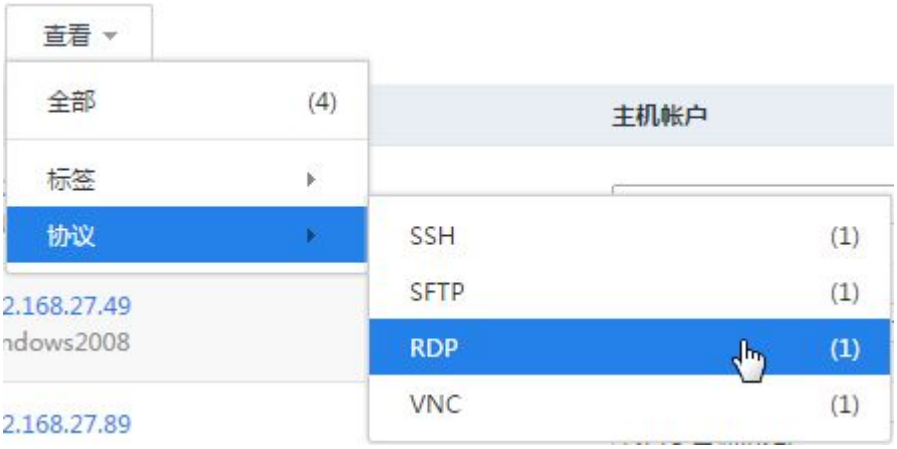


7.4 查看主机

(1) 进入[运维/主机运维]页面中。

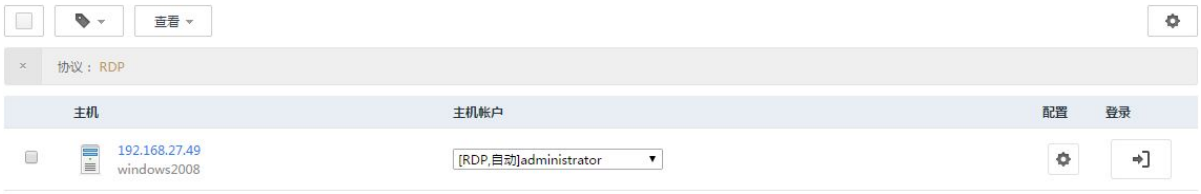
(2) 单击<查看>列出需要查看的条件。

图 7-29 查看主机示意图



(3) 单击某个条件后即可过滤成功。

图 7-30 主机运维页面示意图



8 命令行运维

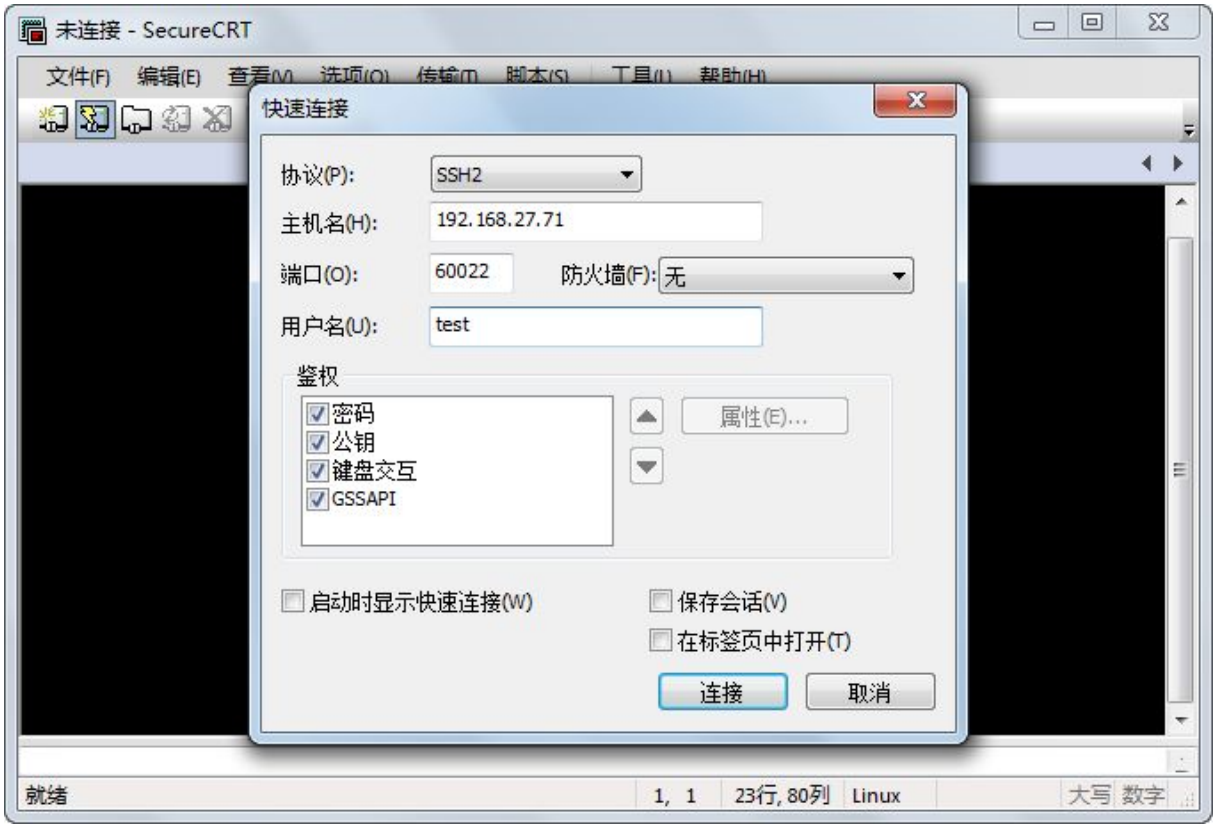
8.1 登录系统

说明

1. 本地PC终端须预先安装好运维工具，如SecureCRT、putty、Xshell等。
2. 工具必须支持SSH2协议。
3. 如果PC端与运维审计系统之间经过防火墙或交换机，那必须在防火墙或交换机上开放60022。

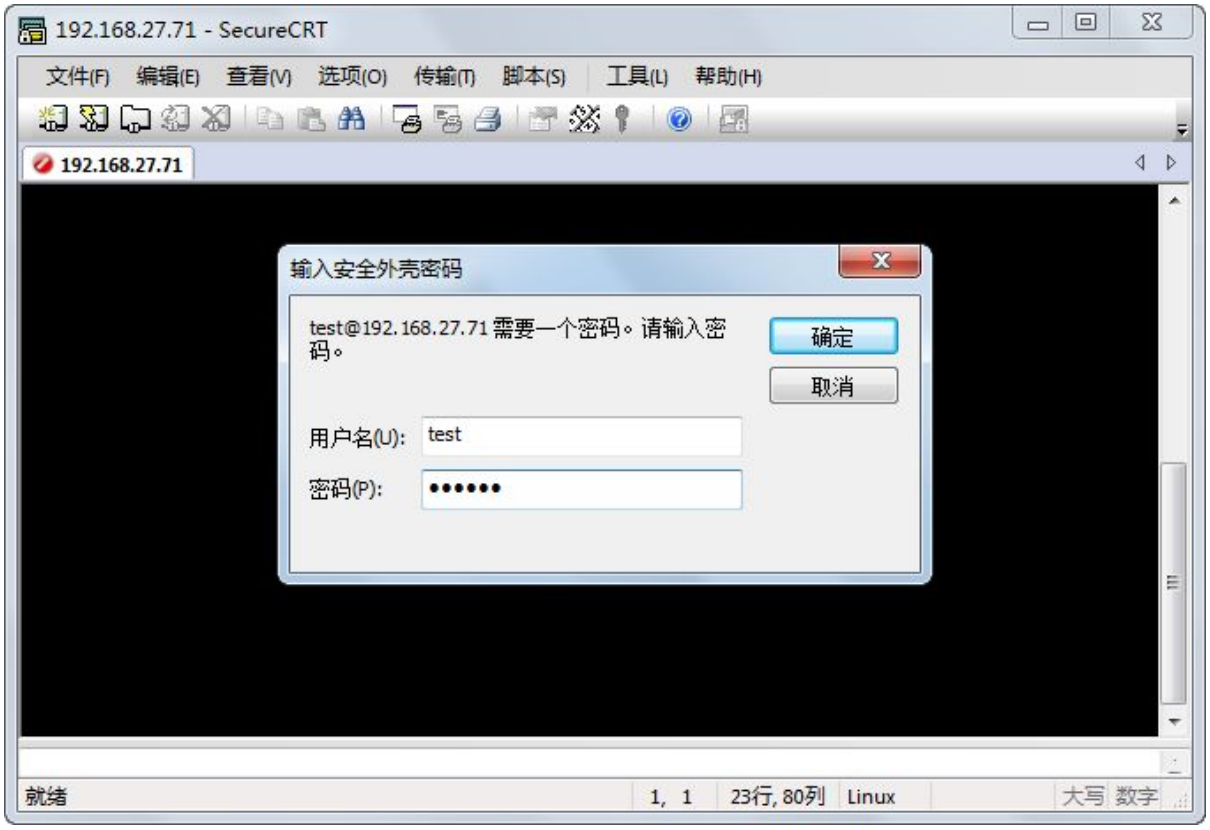
本手册以 SecureCRT 为例。

步骤 1 打开本地终端的 SecureCRT 程序，进入“快速连接”窗口：

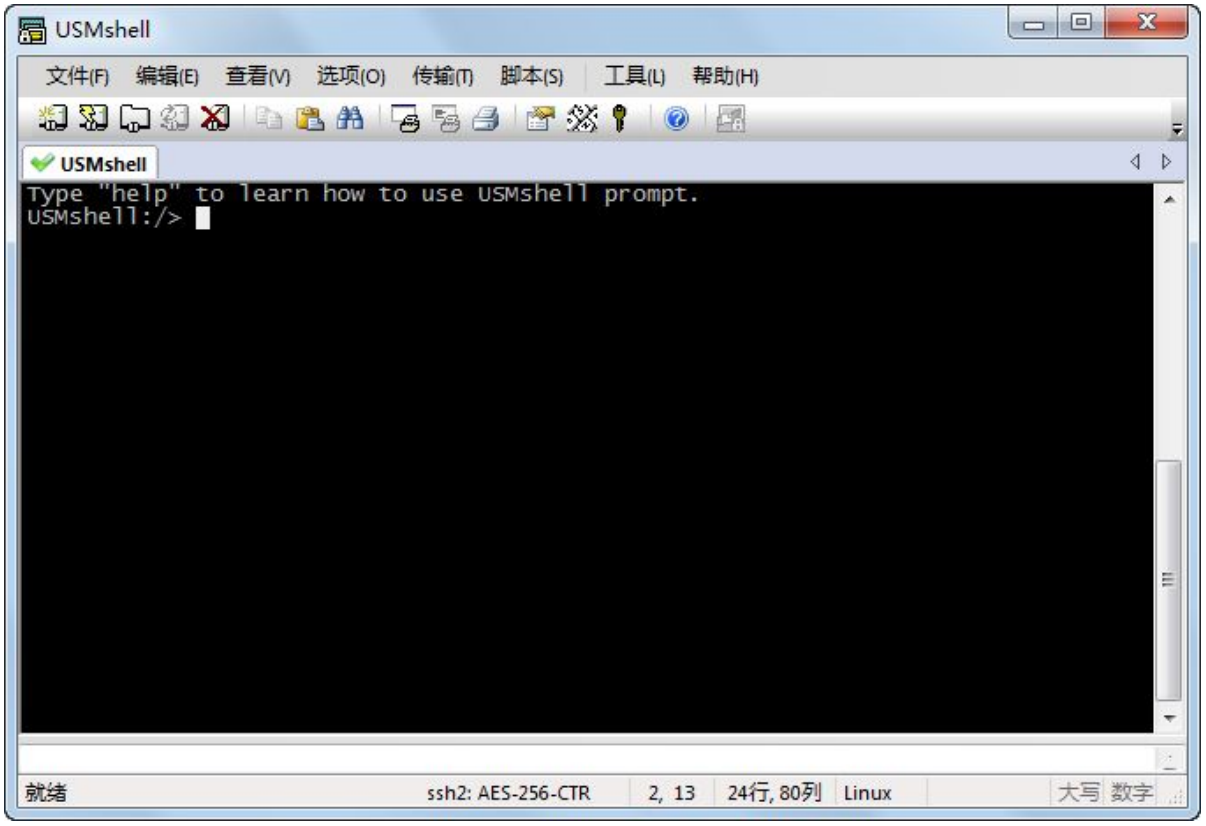


步骤 2 输入运维审计系统的 IP、端口（60022）、用户名。

步骤 3 单击<连接>后，进入“输入安全外壳密码”窗口：输入运维审计系统的用户名和密码。



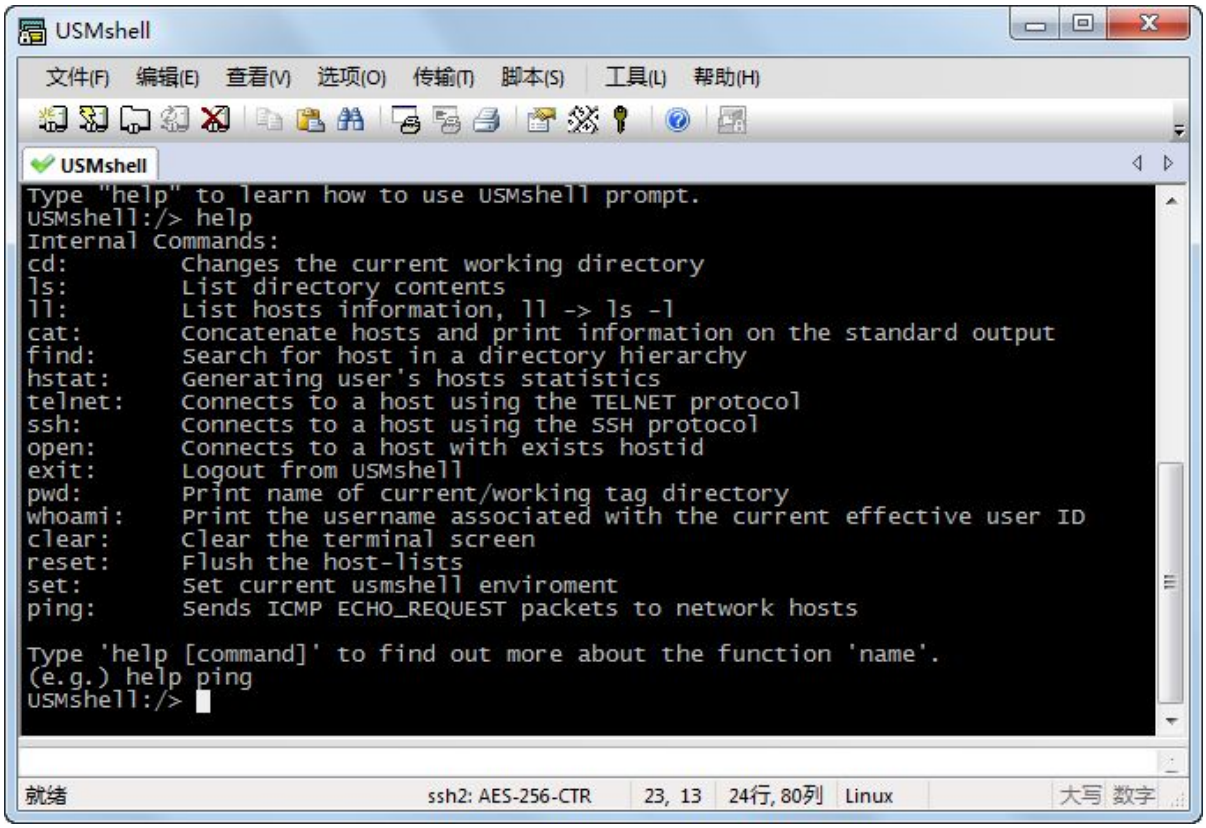
步骤 4 单击<确定>后，进入系统视图界面：


USMshell
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
USMshell
Type "help" to learn how to use USMshell prompt.
USMshell:/>
就绪
ssh2: AES-256-CTR
2, 13
24行, 80列
Linux
大写 数字

8.2 命令介绍

8.2.1 help

在系统视图中，输入 help 命令回车后，可以查看可使用的命令：



8.2.2 cd

1. 命令行关键字

cd { text | text-number | **~** | **/** | **..** | }

2. 命令行参数

cd *text* ：指定进入目录。

cd *text-number* ：指定进入目录编号；text-number 表示目录的编号。

cd ~ ：指定进入宿主目录。

cd / ：指定进入根目录。

cd .. ：指定进入上一级目录。

3. 命令行描述

cd（change directory）命令在 dos 中是常用命令之一，它的主要作用是用来切换路径或目录。

4. 命令行样式如下

进入“默认标签”目录的编号：

USMshell:/>cd 4

```
USMshell:/> ll
Id      Name                    Host                    Protocol  Username
1       1.1.xlx/
2       dsdasda/
3       jamm/
4       默认标签/
USMshell:/> cd 4
USMshell:/默认标签> pwd
/默认标签/
USMshell:/默认标签> ll
Id      Name                    Host                    Protocol  Username
15      192.168.30.231          192.168.30.231:22       SSH       root
16      192.168.30.235          192.168.30.235:22       SSH       root
14      linux服务器             192.168.27.89:22        SSH       root
17      字符主机                192.168.30.241:22       SSH       root
18      字符主机                192.168.30.241:22       SSH       test
USMshell:/默认标签>
```

8.2.3 ls

1. 命令行关键字

ls [-l | *text*] *

2. 命令行参数

ls ：显示当前目录下的文件名或目录名称。

ls -l ：显示当前目录下的文件名列表或目录名列表。

ls *text* ：指定显示这个文件或目录下的信息；text 可以表示一个文件名或者一个目录名。

ls -l *text* ：指定显示这个文件或目录下的列表信息。

3. 命令行描述

ls 命令的含义是 list 显示当前目录中的文件名字。

注意：不加参数它显示除隐藏文件外的所有文件及目录的名字。

4. 命令行样式如下

查看“jamm”目录下的列表信息：

USMshell:/>ls –l /jamm

```
USMshell:/jamm> ls -l /jamm
Id      Name                    Host                    Protocol  Username
2       192.168.21.186          192.168.21.186:22       SSH
5       192.168.27.13           192.168.27.13:22        SSH       root
10      192.168.27.191(web服务器)  192.168.27.191:22       SSH       root
12      192.168.27.51           192.168.27.51:23        TELNET    administrator
9       Cisco交换机             192.168.27.166:22       SSH       jamm
6       DB审计测试              192.168.27.14:22        SSH
7       DB审计测试              192.168.27.14:22        SSH       root
8       DB审计测试              192.168.27.14:22        SSH       jamm
USMshell:/jamm>
```

8.2.4 ll

1. 命令行关键字

ll [*text*]

2. 命令行参数

ll ：显示当前目录下的文件名列表和目录名列表。

ll *text* ：指定显示这个文件或者目录下的列表信息。

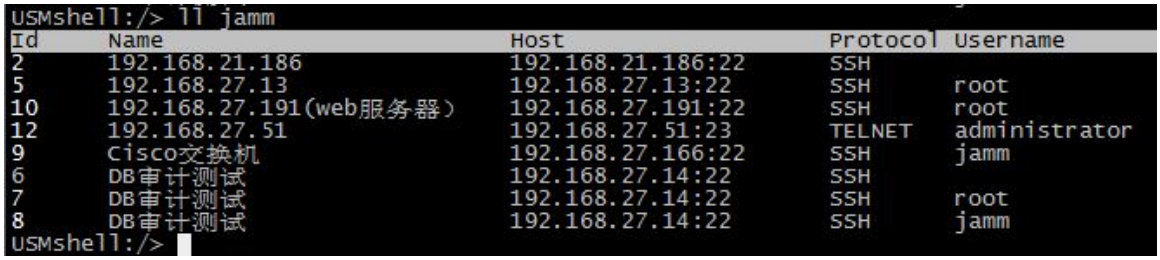
3. 命令行描述

ll 以列表方式显示文件或者目录的属性等信息。

4. 命令行样式如下

查看“jamm”目录下的文件属性：

USMshell:/>ll jamm



8.2.5 cat

1. 命令行关键字

cat *text*

2. 命令行参数

cat *text*：一次显示整个文件。

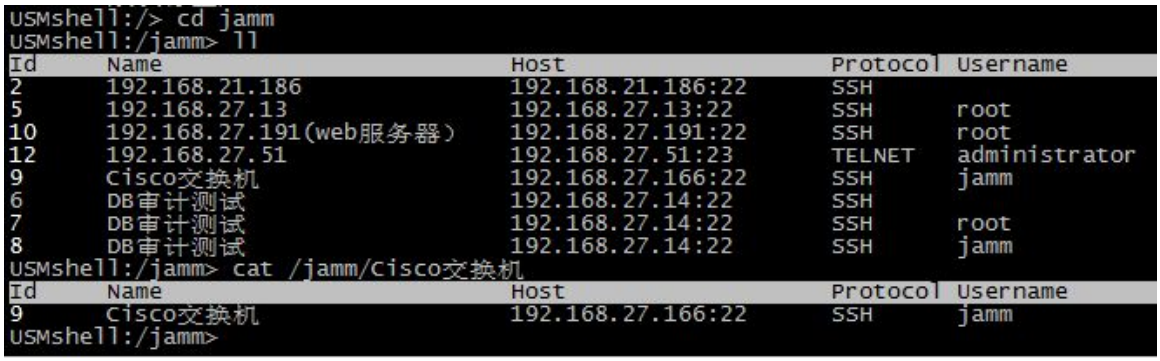
3. 命令行描述

cat 是一个文本文件查看和连接工具。查看一个文件的内容，用 cat 比较简单，就是 cat 后面直接接文件。

4. 命令行样式如下

查看 Cisco 交换机的信息：

USMshell:/>cat /jamm/cisco 交换机



8.2.6 find

1. 命令行关键字

find –name *text*

2. 命令行参数

find –name *text*：查找目标文件名或关键文件名。

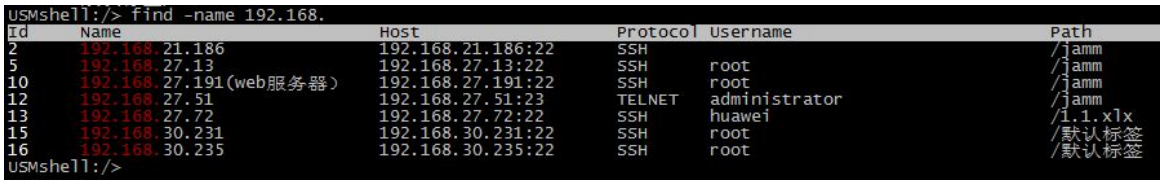
3. 命令行描述

find 用于查找文件信息或者关键文件信息。

4. 命令行样式如下

查找有关“192.168.”的资产信息：

USMshell:/>find –name 192.168.



8.2.7 hstat

1. 命令行关键字

hstat

2. 命令行参数

hstat：统计当前用户可访问的主机数量。

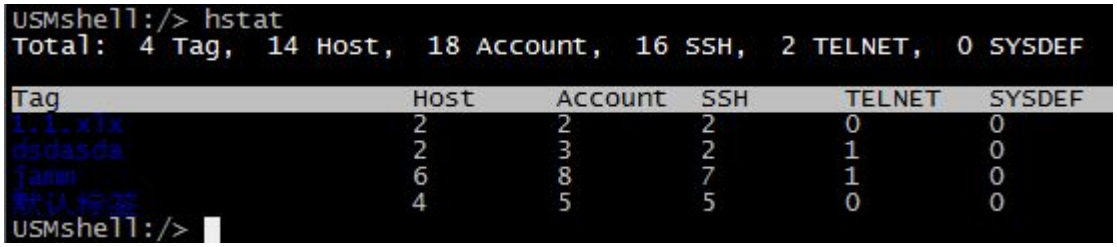
3. 命令行描述

hstat：统计当前用户可访问的主机数量。

4. 命令行样式如下

查看当前用户下所能访问的主机数量：

USMshell:/>hstat



8.2.8 telnet

1. 命令行关键字

telnet [*username*@][*/path/*]<*host*>[*port*]

2. 命令行参数

telnet [*username*@][*/path/*]<*host*>[*port*]：远程登录目标主机/用户/目录/端口。

3. 命令行描述

telnet 可以远程登录 telnet 协议的主机，或者用于验证目标主机的端口是否能通。

4. 命令行样式如下

验证目标主机 192.168.27.166 和 192.168.27.49 的 3389 端口是否通：

- 192.168.27.166 的 3389 端口不通，说明可能是网络限制或服务器未开放 3389 端口。
- 192.168.27.49 的 3389 端口通的，说明服务器的协议可达。

USMshell:/> telnet 192.168.27.166 3389
Username: administrator
Password:
[Errno 110] Connection timed out
USMshell:/> telnet 192.168.27.49 3389
Username: administrator
Password:

8.2.9 ssh

1. 命令行关键字

ssh [*username*@][*/path/*]<*host*>[*port*]

2. 命令行参数

ssh [*username*@][*/path/*]<*host*>[*port*]：远程登录目标主机/用户/目录/端口。

3. 命令行描述

ssh 可以远程登录 ssh 协议的主机。

4. 命令行样式如下

远程登录目标主机：

USMshell:/> ssh 192.168.27.166
Switch>enable
Password:
Switch#

8.2.10 open

1. 命令行关键字

open <*id*>

2. 命令行参数

open <*id*>：连接主机的 ID。

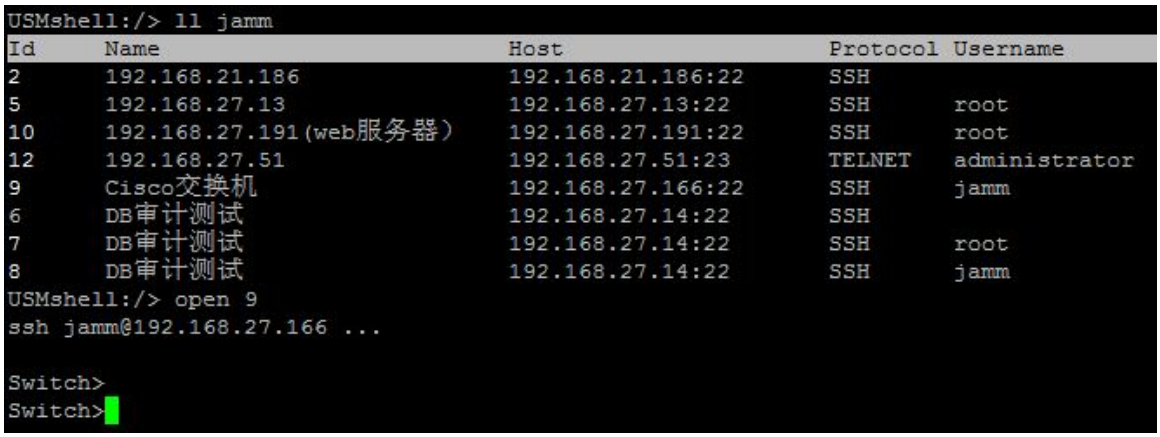
3. 命令行描述

open 可以连接到目标主机。

4. 命令行样式如下

登录一台 cisco 交换机为例：

USMshell:/>open 9



8.2.11 exit

1. 命令行关键字

exit

2. 命令行参数

exit：退出当前的 shell。

3. 命令行描述

执行 exit 可以退出当前的 shell。

4. 命令行样式如下

退出系统视窗界面：

USMshell:/>exit

8.2.12 pwd

1. 命令行关键字

pwd

2. 命令行参数

pwd：显示当前目录的全路径名称。

3. 命令行描述

pwd 命令可以显示当前目录的完整路径名。

4. 命令行样式如下

查看当前目录的路径名：

USMshell:/>cd /jamm

USMshell:/jamm> pwd

/jamm/

USMshell:/jamm>

8.2.13 whoami

1. 命令行关键字

whoami

2. 命令行参数

whoami：显示当前的用户名。

3. 命令行描述

whoami 命令可以显示当前的用户名。

4. 命令行样式如下

显示当前用户名称：

USMshell:/jamm>whoami

admin

USMshell:/jamm>

8.2.14 clear

1. 命令行关键字

clear

2. 命令行参数

clear：清除当前屏幕。

3. 命令行描述

clear 命令可以清除当前的屏幕。

4. 命令行样式如下

清理当前屏幕的信息：

USMshell:/jamm>clear

8.2.15 reset

1. 命令行关键字

reset

2. 命令行参数

reset：刷新主机列表信息。

3. 命令行描述

当主机信息变更后，可执行 reset 命令进行刷新，再查看主机信息。

4. 命令行样式如下

在系统配置界面中把 192.168.27.191 的名称进行变更，然后再刷新查看：

USMshell:/jamm>reset

```
USMshell:/jamm> ll
Id      Name                    Host                    Protocol Username
2       192.168.21.186          192.168.21.186:22       SSH
5       192.168.27.13           192.168.27.13:22        SSH      root
10      192.168.27.191          192.168.27.191:22       SSH      root
12      192.168.27.51           192.168.27.51:23        TELNET   administrator
9       Cisco交换机             192.168.27.166:22       SSH      jamm
6       DB审计测试              192.168.27.14:22        SSH
7       DB审计测试              192.168.27.14:22        SSH      root
8       DB审计测试              192.168.27.14:22        SSH      jamm
USMshell:/jamm> reset
USMshell:/jamm> ll
Id      Name                    Host                    Protocol Username
2       192.168.21.186          192.168.21.186:22       SSH
5       192.168.27.13           192.168.27.13:22        SSH      root
10      192.168.27.191(web服务器)  192.168.27.191:22       SSH      root
12      192.168.27.51           192.168.27.51:23        TELNET   administrator
9       Cisco交换机             192.168.27.166:22       SSH      jamm
6       DB审计测试              192.168.27.14:22        SSH
7       DB审计测试              192.168.27.14:22        SSH      root
8       DB审计测试              192.168.27.14:22        SSH      jamm
USMshell:/jamm>
```

8.2.16 set

1. 命令行关键字

set [-p] [*name=value*]

2. 命令行参数

set [-p] [*name=value*]：设置 shell 环境。

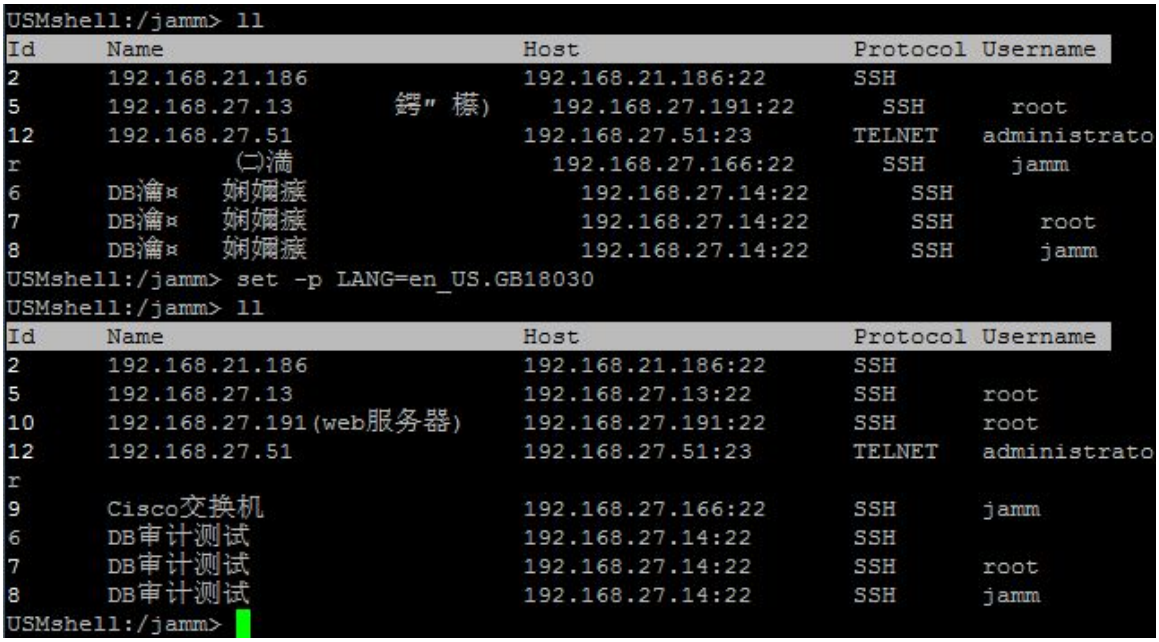
3. 命令行描述

set 可以设置 shell 环境的语言、编码、颜色。

4. 命令行样式如下

发现 shell 环境的编码不对，可以利用 set 命令修改编码格式：

USMshell:/jamm>set –p LANG=en_US.GB18030



8.2.17 ping

1. 命令行关键字

ping [*id* | *host*]

2. 命令行参数

ping [*id* | *host*]：发送 icmp 给目标主机。

3. 命令行描述

ping 可以验证目标主机是否连通。

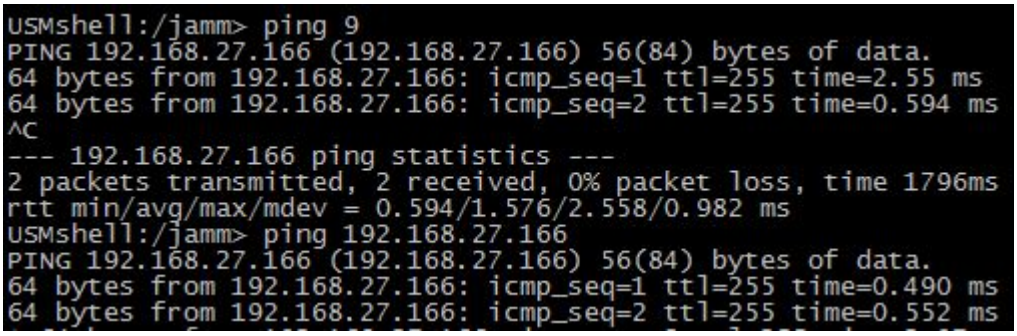
4. 命令行样式如下

验证 192.168.27.166 是否连通：

USMshell:/>ping 9

或

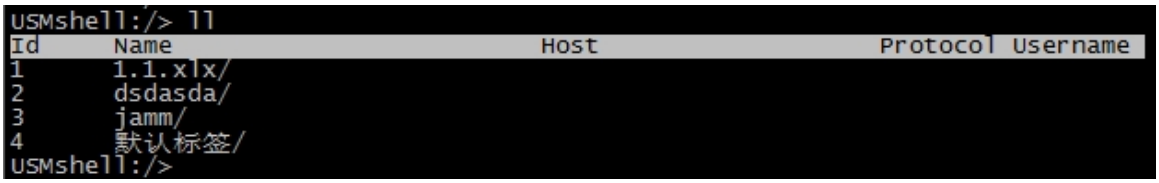
USMshell:/>ping 192.168.27.166



8.3 进入标签目录

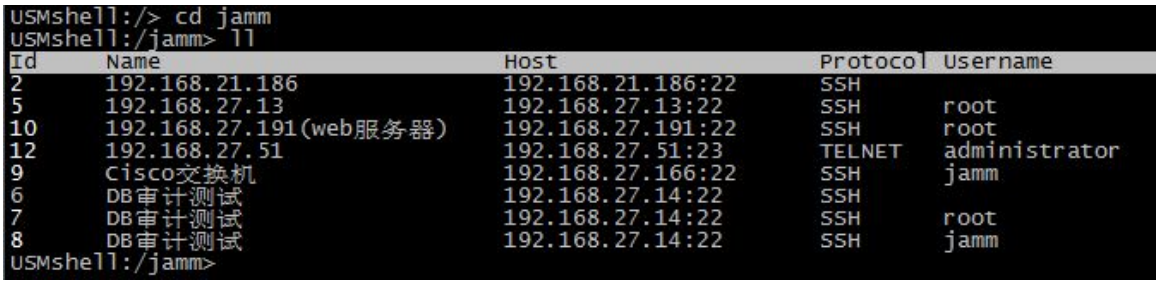
8.3.1 ll 命令查看目录

查看标签目录和目录的 ID：



8.3.2 cd 切入标签目录

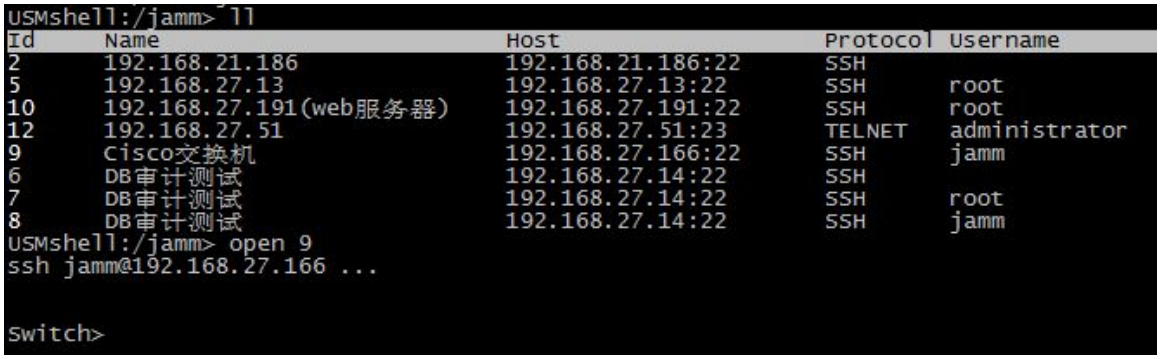
进入需要管理的标签目录：



8.4 登录主机运维

8.4.1 open 连接目标主机

选择需要登录的目标主机，执行 open+ID 即可登录成功。



8.4.2 对目标主机进行运维操作