UNIS A2000-G 系列运维审计系统

Web 配置指导

北京紫光恒越网络科技有限公司
http://www.unishy.com

资料版本：5W100-20180521

前 言

本配置指导介绍了 UNIS A2000-G 系列运维审计系统的原理及其通过 Web 配置的方法，包含原理简介、配置任务描述和配置举例。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格　式	意　义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unishy.com

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 概述

1.1 内容和读者

本文档主要介绍堡垒机中超级管理员、配置管理员、密码管理员、审计管理员、普通用户角色的常见任务及操作方法，供堡垒机的管理员和相关技术人员参考。

1.2 基本环境

客户端环境需要满足下列基本要求。

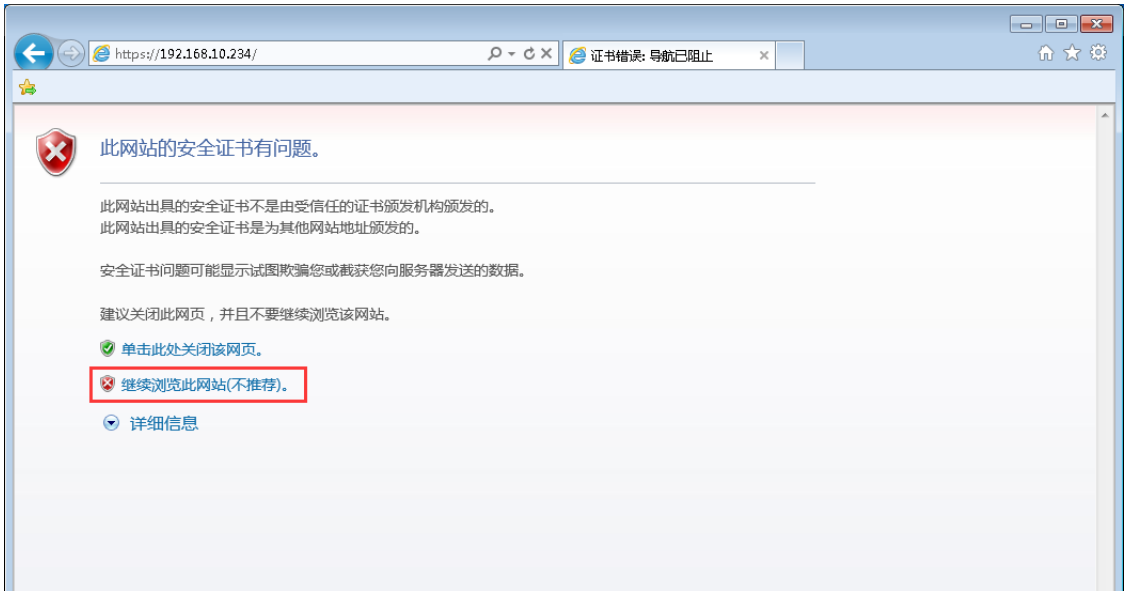
表1-1 客户端环境要求

操作系统	浏览器
Windows XP 或更新版本	IE 10.0 以上版本的浏览器、Google Chrome、Mozilla Firefox

1.3 访问堡垒机

请使用浏览器访问堡垒机的 WEB 页面，通常堡垒机的访问地址为 https://<堡垒机的 IP 地址>。访问后您会看到下图所示的证书错误提示：

图1-1 SSL 证书错误提示



请点击“继续浏览此网站（不推荐）”，将出现堡垒机的登录页面，输入帐号和密码点击登录即可进入堡垒机页面。

图1-2 堡垒机登录页面

说明

堡垒机缺省 IP 为 192.168.0.1、用户名和密码为 admin/admin。

2 超级管理员配置

2.1 操作页面简介

Web 管理界面由菜单栏、状态栏、消息提醒及主内容区组成。每个菜单都有相应的一个或多个子菜单。点击某个菜单项目如基本控制，在相应菜单下方会扩展出其包含的子菜单，点击相应子菜单，即可在主内容区显示相关配置页面。

图2-1 超级管理员操作界面示意图

操作界面介绍如下：

- 菜单栏：提供了超级管理员可进行配置操作的所有菜单。
- 状态栏：右侧的状态栏，显示当前用户角色、用户名和问号菜单，点击用户角色可在多个角色间进行切换，点击用户名可以进行个人账户设置、系统语言变更、退出登录等操作，点击问号菜单，可以查看系统负载和产品关于以及工具下载。
- 消息提醒：用于提示用户与当前账户相关的工单申请、双人授权、命令复核等通知信息，用户可通过点击 0消息 查看具体的消息信息。
- 主内容区：用于显示各级子菜单相应的配置页面。

2.2 用户帐户

2.2.1 用户帐户简述

用户账号是使用者登录堡垒机所使用的账号，用于对使用者进行身份验证和权限管理。堡垒机将用户账户分为下表中的五种角色，除普通用户外，前四种均为管理员角色。

表2-1 用户帐户简述

用户账号角色	操作权限
超级管理员	创建和管理下列角色的用户账号：超级、配置、审计、密码保管员； 设置系统的全局选项，比如身份认证、告警事件、设备类型，授权管理等
配置管理员	创建和管理普通用户、目标设备、系统账号； 管理访问权限、命令权限；管理设备改密计划等
审计管理员	查看系统中的操作日志、事件消息、统计报表等
密码保管员	查看改密计划、下载或备份设备的系统账号密码等
普通用户	通过堡垒机管理目标设备

2.2.2 管理用户账号

1. 用户帐号管理界面简介

菜单位置：基本控制 > 用户帐号

图2-2 用户账号管理页面示意图

2. 新建用户

超级管理员可以新建和管理超级、配置、审计、密码保管员 4 种角色的管理员，下面以创建配置管理员角色为例说明新建用户过程：

菜单位置：基本控制 > 用户帐号 > 新建

图2-3 新建用户示意图

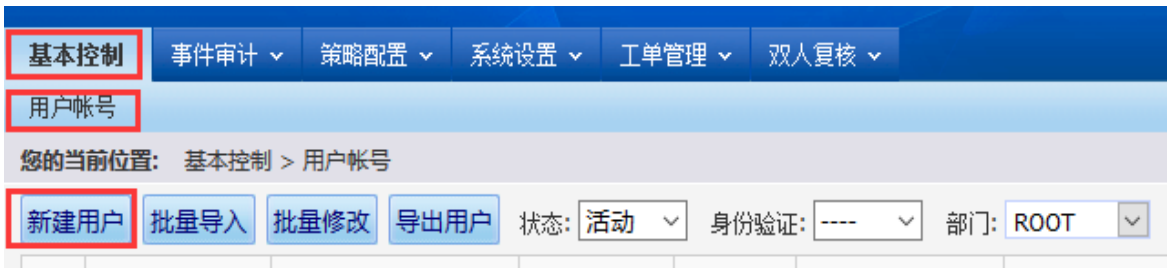


图2-4 新建用户-基本属性

参数解释：

登录名：用户登录堡垒机所使用的用户名（必填），1-20 个字符,可以为数字，英文字母和下列符号 . - _ (不能以._-开头)。

- 真实姓名：用户帐号使用者的真实姓名（必填），1-128 个字符。
- 部门：选择用户帐号的部门，默认为 ROOT。超级管理员可以在“策略配置”>“部门配置”中建立和管理部门。
- 密码：设置用户帐户登录密码，包括手工输入、自动修改两种方式，默认为“手工输入”。其中手工输入、自动修改含义如下：
  - 手工输入：表示管理员为用户帐号设置一个初始的密码，此时堡垒机不对管理员输入的密码做复杂性检查。

- 自动修改：表示堡垒机自动生成用户帐号的密码，用户可以设置新密码的位数。新的密码的默认以密码邮件的方式发送给最终用户。

- 权限：针对所建立的用户分配相应的管理员角色。

当完成了以上必填项后点击保存即可完成用户帐户的添加。

图2-5 新建用户-高级属性示意图

参数解释：

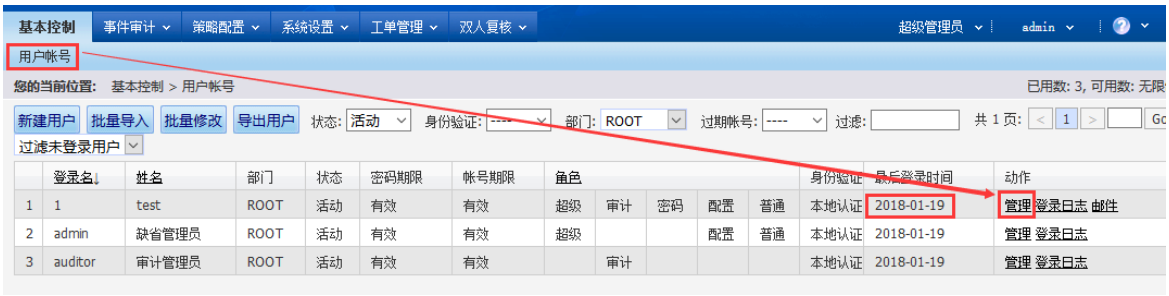
- 密码有效期至：设置用户帐号密码有效期（Native 身份验证方式），默认为 90 天，留空表示密码永不过期。用户可以点击输入框后的“清空”快速清除有效期，或者点击“恢复”还原修改前的值。
- 允许登录 IP：可登录堡垒机的来源 IP 地址，格式如: 192.168.1.1, 192.168.1.1-192.168.1.5, 192.168.1.*。
- 允许登录 MAC：可登录堡垒机的来源 MAC 地址，格式如: 00:00:00:00:00:00, 00:00:00:00:00:00。
- 有效期起止时间：指用户账号的有效期，默认一年，超出设置有效期时间范围则用户账号失效，此处留空表示永不过期。
- 备注：添加用户帐号的备注信息，默认为空。

3. 用户账号管理

菜单位置：基本控制 > 用户帐号 > 管理

当用户账号管理页面显示此账号已登录过堡垒机（查看最后登录时间），由于审计要求此账号只能进行禁用，不能进行删除。

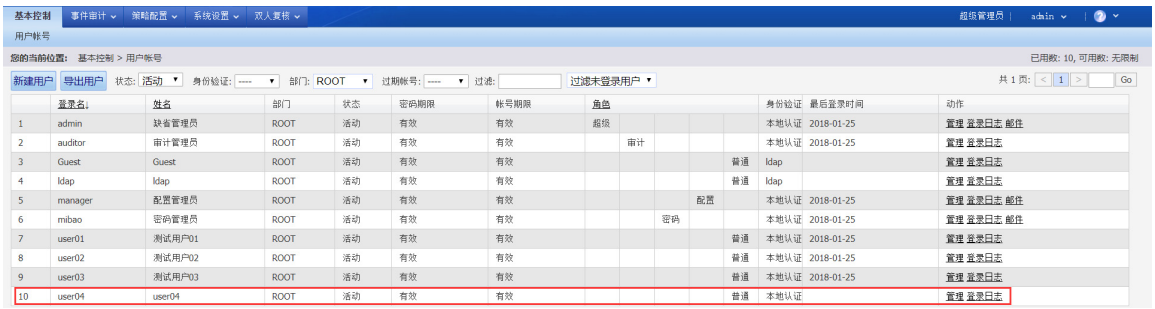
图2-6 用户账号管理示意图



(1) 删除用户账号（只能删除未登录过堡垒机的用户账号）

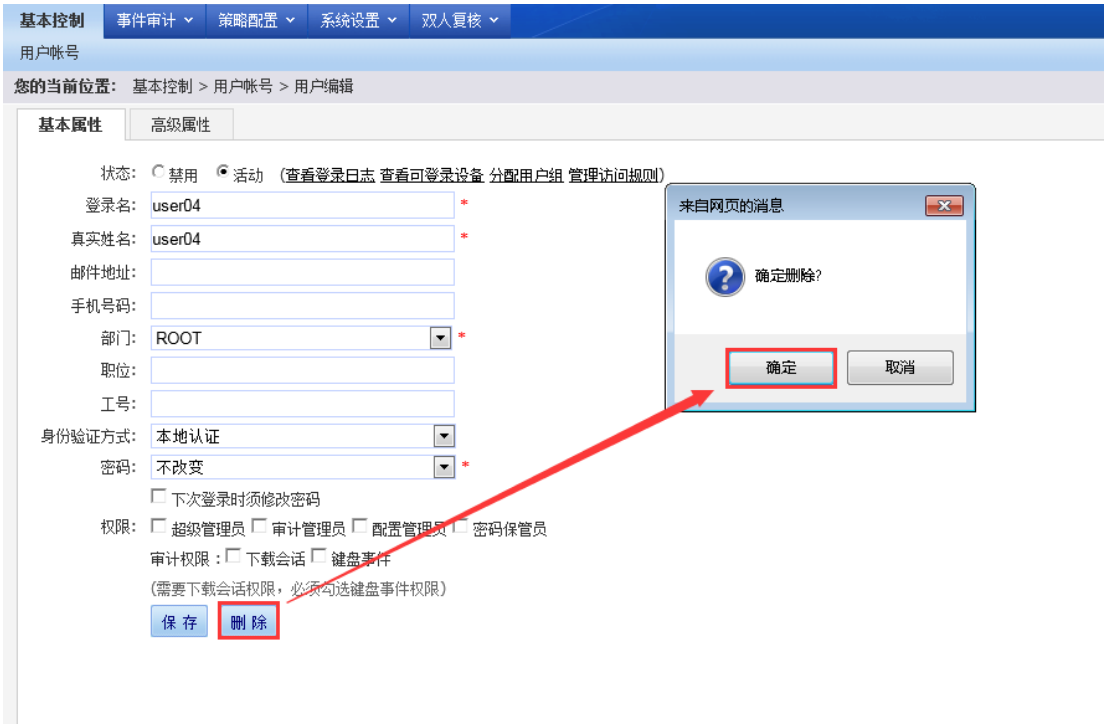
下图中标记的用户账号从未登录过堡垒机，此账号如不再需要登录堡垒机则可以删除。

图2-7 查看用户是否已登录过堡垒机示意图



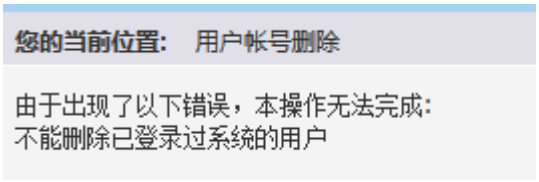
点击删除并确定后完成用户账号删除，如下图。

图2-8 删除用户账号示意图



当如出现下图错误提示，则表示此用户账号已经登录过堡垒机，只能禁用不能删除。

图2-9 删除用户账号示意图



(2) 禁用用户账号（已登录过的账号）

当某个用户账号（已登录过的账号）不再使用则可以变更其状态为“禁用”。

选择状态为“禁用”，点击保存，完成账号禁用操作。

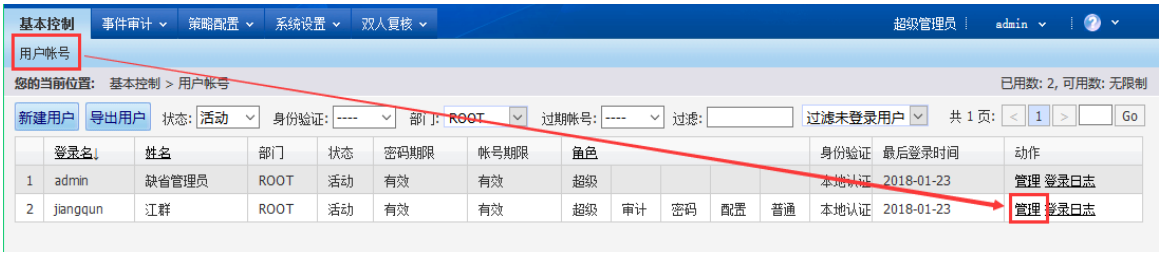
图2-10 禁用用户账号示意图

(3) 用户账号密码重置

当最终用户密码遗失则需要管理员协助完成密码重置工作。

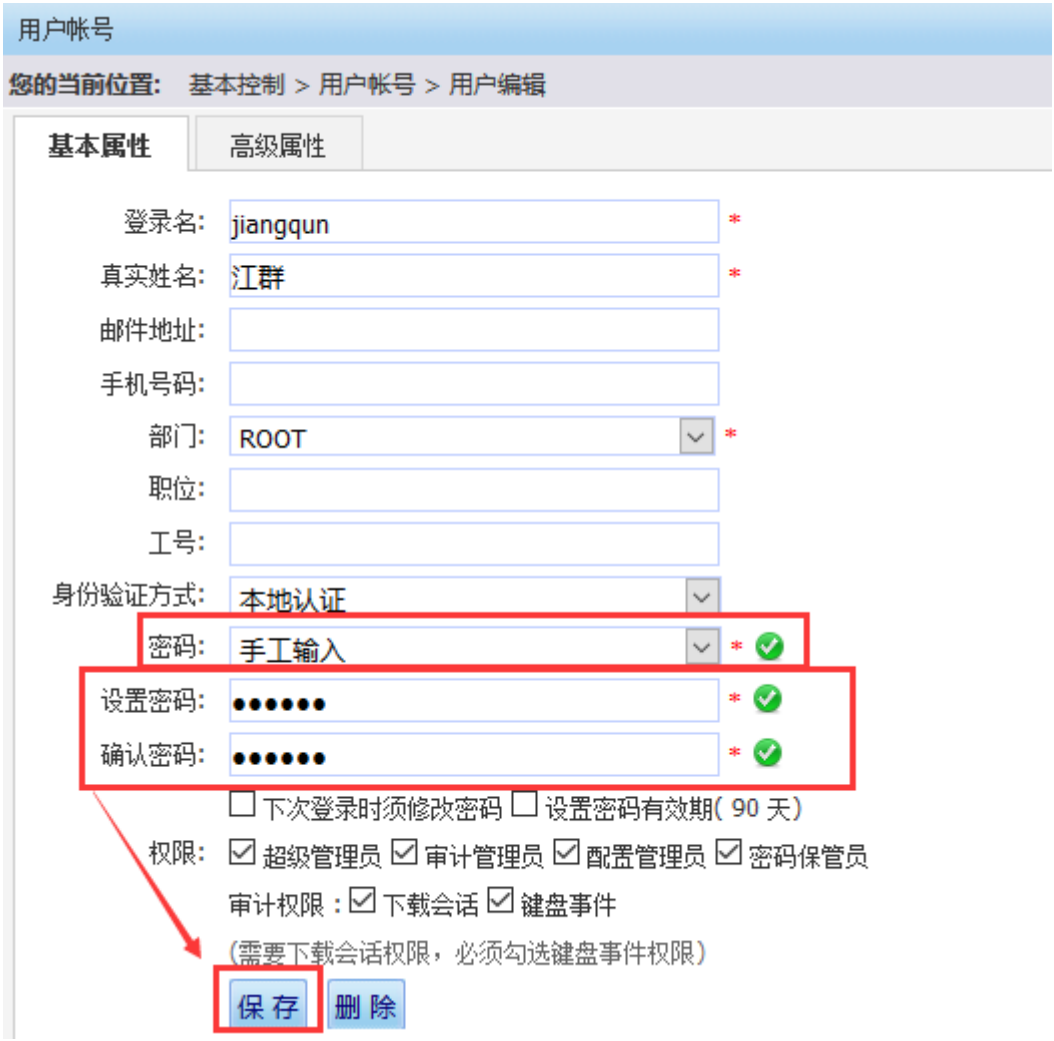
菜单位置：基本控制 > 用户账号 > 管理

图2-11 用户账号密码重置示意图



在密码选项中选择“手工输入”，输入初始密码点击保存完成用户账号密码重置。

图2-12 用户账号密码重置示意图



(4) 用户账号解锁

当最终用户连续 5 次输入错误的密码，用户账号将立即锁定，此时需要管理员协助解锁账号（默认为连续 5 次输入错误密码锁定账号），默认 60 分钟后被锁定的用户账号也会自动解锁。

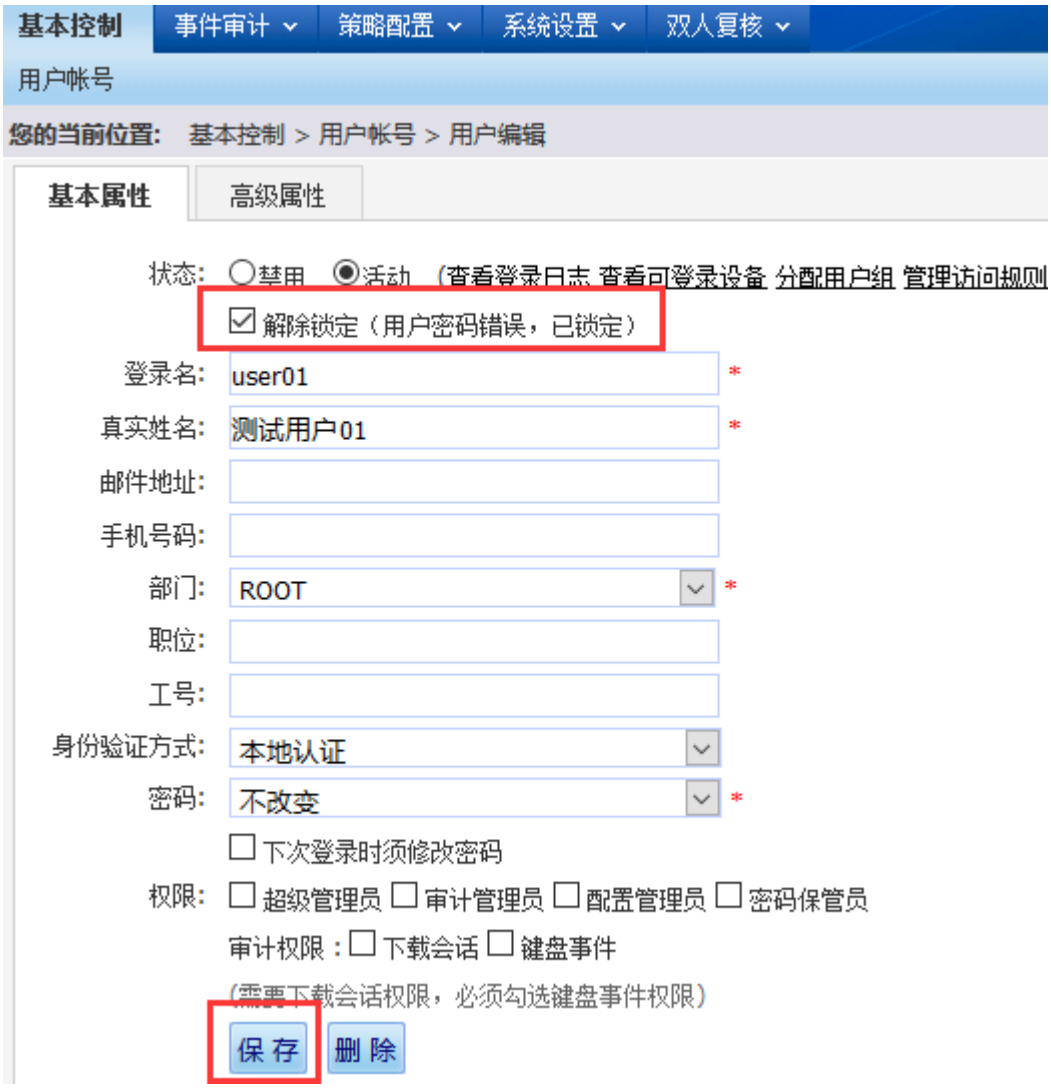
菜单位置：基本控制 > 用户账号 > 管理

如下图所示状态为“密码锁定”的用户账号中点击“管理”。

图2-13 用户账号-密码锁定示意图

勾选“解除锁定”并点击保存，完成用户账号解锁。

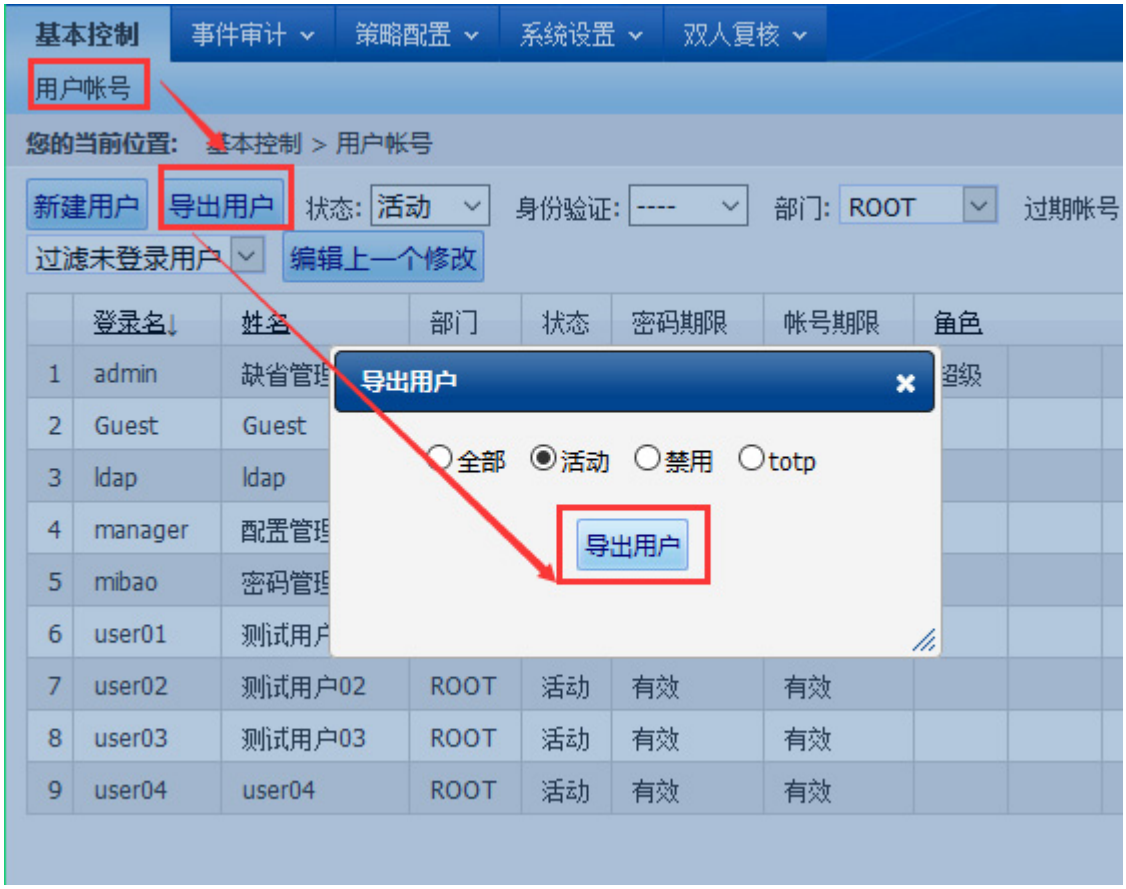
图2-14 用户账号解锁示意图



4. 导出用户

当需要对堡垒机中已有的用户账号进行统计，可以通过导出用户功能完成。

图2-15 导出用户示意图

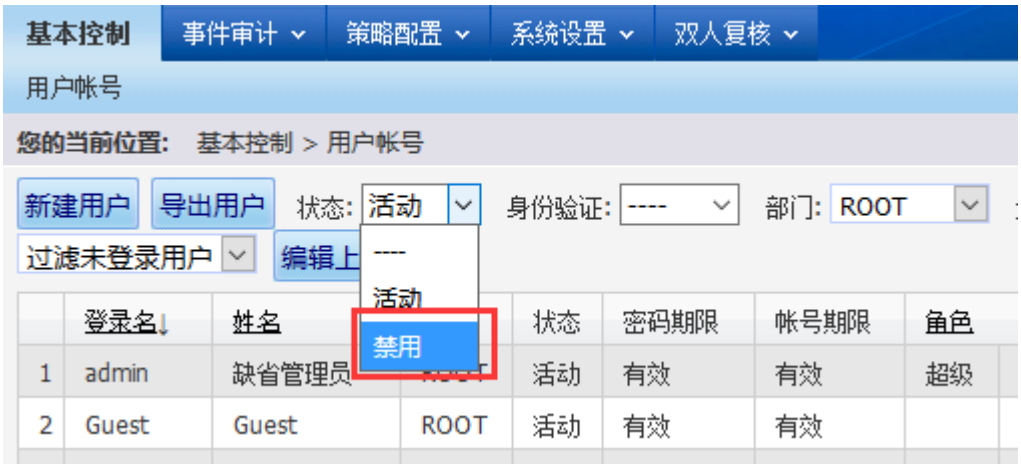


5. 查看已禁用用户

当用户账号状态变更为禁用后，默认不显示在用户账号管理页面，需要查看已禁用的用户账号可以通过选择用户账号状态进行过滤。

菜单位置：基本控制 > 用户账号 >状态，选择禁用

图2-16 过滤用户状态示意图



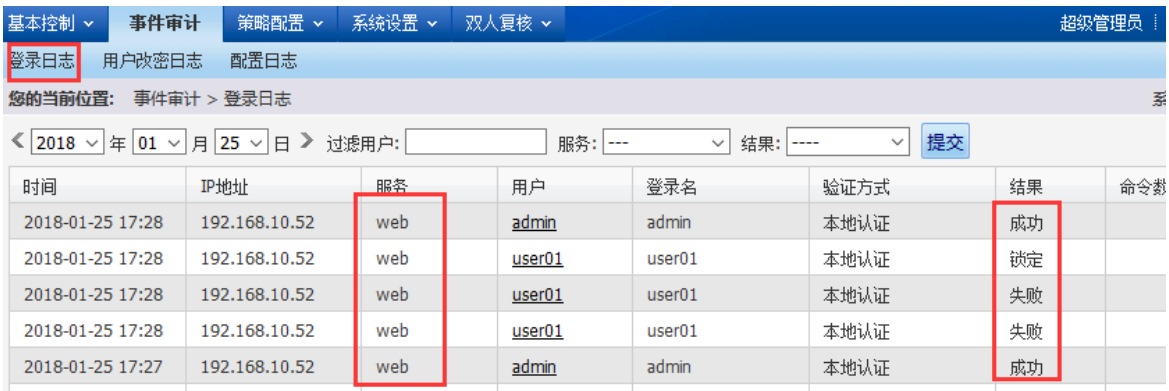
2.3 事件审计

2.3.1 登录日志

超级管理员可以在此页面查看用户登录堡垒机的日志。

菜单位置：事件审计 > 登录日志

图2-17 登录日志示意图



2.3.2 用户改密日志

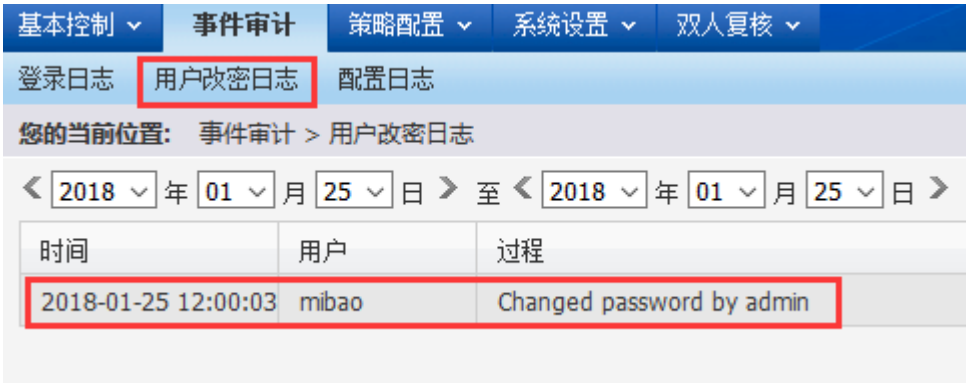
此页面可以查看到用户修改自身登录密码的日志。

说明

由管理员完成的修改用户密码的操作不记录。

菜单位置：事件审计 > 用户改密日志

图2-18 用户改密日志示意图

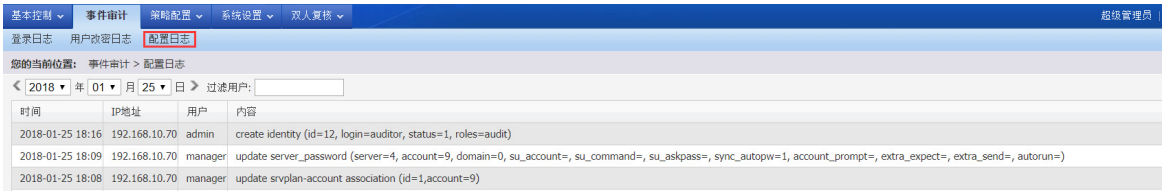


2.3.3 配置日志

菜单位置：事件审计 > 用户改密日志

此页面可以查看管理员的相关配置日志，如下图。

图2-19 配置日志示意图



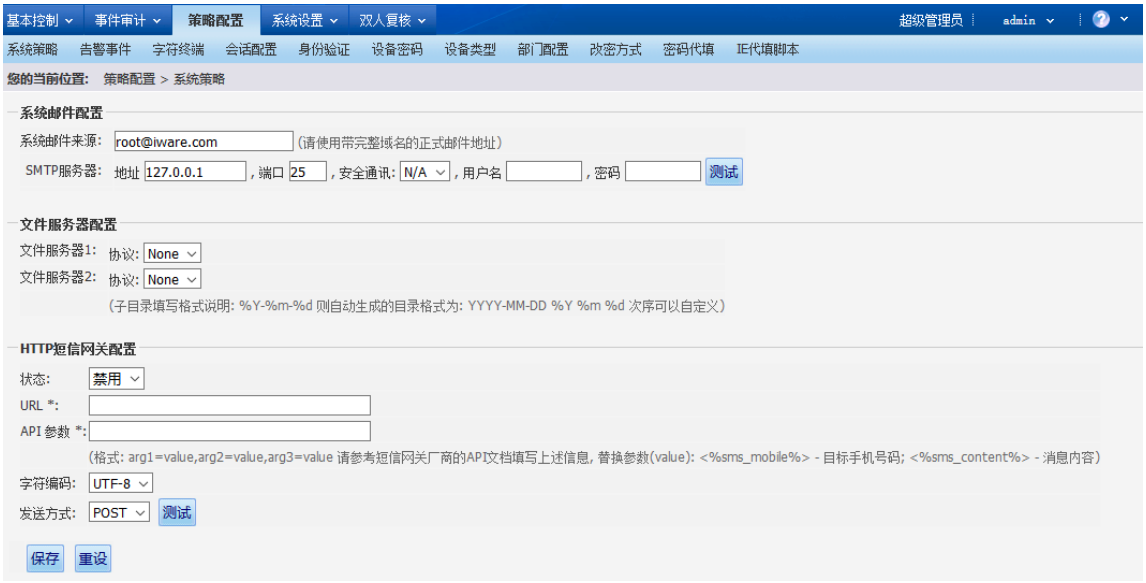
2.4 策略配置

策略配置用于设置堡垒机全局选项，系统策略、告警事件、字符终端、会话配置、身份验证、设备密码、动态属性、部门配置、密码代填、IE 代填脚本，下面分别进行说明。

2.4.1 系统策略

菜单位置：策略配置 > 系统策略

图2-20 系统策略示意图

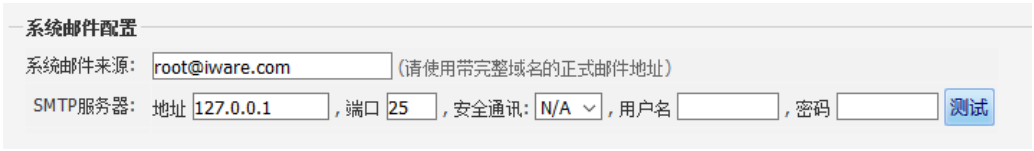


1. 系统邮件配置

配置 SMTP 服务器，可以实现用户账号密码自动设置、用户账号过期密码自动修改、事件消息邮件通知、目标设备改密外发邮件、脚本任务邮件通知、自动报表等功能。

按照图示填写相应选项，然后进行测试。

图2-21 系统邮件设置示意图



配置 SMTP 服务器后进行邮件测试常见的报错信息：

- Connection refused 表示堡垒机无法连接到 SMTP 服务器，请检查网络和通信端口。
- Failed connect server with TLS 表示 SMTP 服务不支持 TLS，安全通信请选择 n/a。
- SMTP AUTH extension not supported by server 表示服务器不支持 SMTP AUTH，请删除用户名和密码。

⚠ 注意

默认系统邮件来源为 root@iware.com，如使用外部邮件系统则此处需要更改为相应的发件人邮箱地址。

---

2. 文件服务器

(1) 文件服务器用途

堡垒机支持在进行改密计划执行结果、手工改密执行结果、密码备份、脚本任务执行结果上传，文件服务器支持 FTP、SFTP 协议。

(2)　如何添加文件服务器

在堡垒机中选择配置的协议后再填写相应的 IP 地址、端口、用户名、密码，如下图所示。

图2-22 文件服务器配置示意图

参数解释：

- 协议：设置文件传输的协议，支持 FTP、SFTP 两种协议。
- 名称：文件服务器的名称。
- 地址：文件服务器的 IP 地址。
- 端口：FTP 协议默认为 21 端口，SFTP 协议默认为 22 端口。
- 用户名/密码：文件服务器的用户名/密码。
- 工作目录：如 图 2-22 所示将会用此用户名登录FTP/SFTP后所在根目录下创建Password的目录。
- 子目录：如 图 2-22 所示在工作目录中创建子目录，默认为%Y-%m-%d，最终将会更具改密日期生成YYYY-MM-DD的子目录。
- 编码：指定密码文件名编码，默认指定 UTF-8。

注意

如果要实现目标设备自动改密功能，则以下 2 种服务至少配置其中一种才可实现通过堡垒机自动修改目标设备系统账号密码。

- SMTP 邮件整合。
- 文件服务器。

2.4.2 告警事件

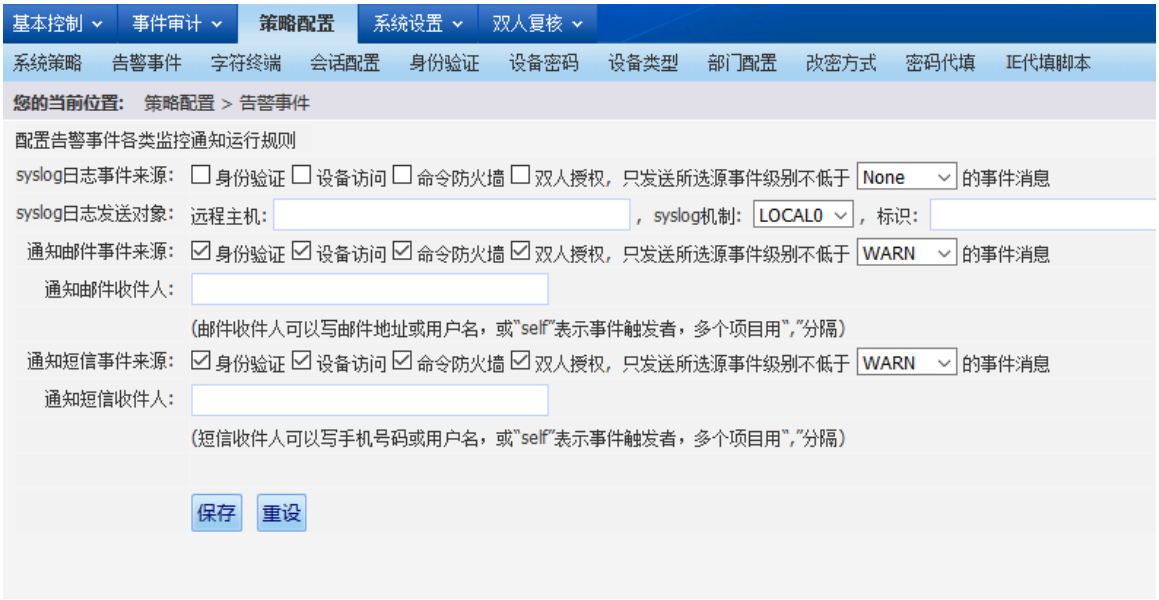
菜单位置：策略配置 > 告警事件

堡垒机支持 syslog 日志外发、邮件事件通知、短信事件通知三种方式发生方式。

- Syslog 日志事件来源：在此项中配置需要外发的事件来源以及接收 syslog 日志远程主机。
- 通知邮件事件来源：在此项中配置需要外发的事件来源以及通知邮件收件人邮件地址。

- 通知短信事件来源：在此项中配置需要外发的事件来源以及通知短信收件人手机号码，短信通知需要配套短信网关使用。

图2-23 告警事件示意图



2.4.3 字符终端

堡垒机对通过 SSH、TELNET 协议访问的会话称为字符会话，字符终端配置可对字符会话全局设定。

菜单位置：策略配置 > 字符终端

图2-24 字符终端示意图

字符终端选项含义如下：

- 字符终端编码：全局设定字符终端编码格式。
- 初始终端标题：使用终端登录堡垒机时 putty、scrt 等 SSH 终端工具的标题栏格式，用于在打开多个会话时区分不同的会话。
- 并发登录限制：“全局”，设定系统全局最大并发终端登录数量，超过后将禁止所有用户新建终端登录连接；“单个用户”，设定单个用户帐户最大并发终端登录数量，超过后堡垒机将拒绝此用户新建终端登录。堡垒机默认全局和单个用户不限制并发数。
- 终端登录菜单：设置用户终端登录堡垒机后每一个选单页的最大行数，可以选择是否在终端登录菜单上先显示访问控制的分组信息，以及设备在终端菜单中的排序方式。
- 终端登录提示：设置终端登录提示语句，用户通过终端软件登录堡垒机后，终端将以 banner 的形式打印提示语。
- 会话访问方式：此为全局选项，设定用户通过堡垒机的 Web 页启动字符会话时使用的的默认工具，堡垒机提供 putty、scrt、xshell 三个工具供选择。其中选择 putty 的话不需要客户端手动安装，选择 scrt 和 xshell 需要在客户端手动安装对应的工具。
- 会话访问方式(Mac)：此为全局选项，设定用户通过 MAC 访问堡垒机的 Web 页启动字符会话时使用的的默认终端。

- 自动登录超时：字符会话自动登录目标设备的超时时间，超过设定时间未能成功登录目标设备时堡垒机将不再尝试自动登录。如果网络环境延迟较大建议设置较长的超时时间。
- 输入超时：终端会话的最大连续无输入时间，超时后该会话将被切断。
- 最大持续时间：一个终端会话持续的最大时间，超时后该会话将被切断，缺省值为 5 天。
- 切断过夜会话：在每天的这个时间切断所有连接超过 5 分钟的会话，不设置表示不切断过夜会话。
- 命令输出限制：可设定字符会话单条命令的最大输出限制，默认不限制。
- 会话输出限制：字符会话的审计日志大小到达该限制后会话会被切断，默认不限制。
- 登录测试调试信息：当配置管理员在进行登录测试发现自动登录测试失败，可启用此项打印调试信息提供更多信息快速定位原因。
- 登录调试信息：启用此项后当普通用户登录目标设备时候打印调试信息到屏幕，堡垒机默认未开启此功能。
- 改密调试信息：当执行目标设备改密时，开启此功能将会记录改密调试信息到改密日志中。

注意

字符会话中参数调整为全局调整，可根据实际使用情况进行调整。

2.4.4 会话配置

堡垒机对通过 RDP、VNC、RDPAPP 协议访问的会话称为图形会话，会话配置可对图形会话的相关参数进行设定。

菜单位置：策略配置 > 会话配置

图2-25 会话配置示意图

会话配置选项含义如下：

- 备注方式：是否要求普通用户在访问目标设备时可填写备注信息。
- Web 超时时间：指用户成功登录堡垒机，在指定时间内无操作则 Web 界面退出至登录界面。
- 会话切断策略：默认为不切断，此为当 web 因超时退出至登录界面时，可以选择切断或不切断由 Web 界面启动的字符、图形会话。
- 双人授权事件：定义双人授权事件的级别，对应告警事件中的级别配置，可完成配置双人授权事件的告警提示规则，事件级别缺省值为 NOTICE。
- 访问/命令权限事件：此处所设级别将作为创建访问权限及命令权限的事件级别默认值，缺省事件级别为 None。
- 隐藏未配置密码的系统账号：如果启用该功能，配置管理员给普通用户分配了相应的系统账号权限，但是如果设备未托管该设备的密码，那么普通用户在访问的时候看不到该系统账号，堡垒机默认未开启功能。
- 初始终端标题：使用终端登录堡垒机时 RDP 终端工具的标题栏格式，用于在打开多个会话时区分不同的会话。
- 活跃 RDP 会话数量：设备访问前，鼠标停留在 rdp 服务图标上会显示活跃 rdp 会话总数/详细。
- RDP 会话默认启动方式：可选 mstsc/java，堡垒机默认为 mstsc。
- GUI 会话文件下载限制: 下载会话审计中相关日志文件大小限制，不设置或设置为 0 表示无限制。
- GUI 键盘记录开关：设置是否记录 GUI 会话的键盘动作，默认为记录。如果您担心键盘记录中包含了敏感信息，可选择不记录。
- GUI 超时时间：设置在设定时间内无操作则图形会话超时退出，默认不受限制。
- 默认分辨率：全局选项，设定用户通过堡垒机的 Web 页启动图形会话时使用的的默认分辨率。
- 文件记录限制：超出限制部分将不做记录，堡垒机默认设置为 0。

 注意

- *会话切断策略只切断或者不切断通过 Web 界面启动的会话，通过 mstsc 等工具和非 Web 界面启动的会话则不受影响。*
- *会话中参数可根据实际使用情况进行调整。*

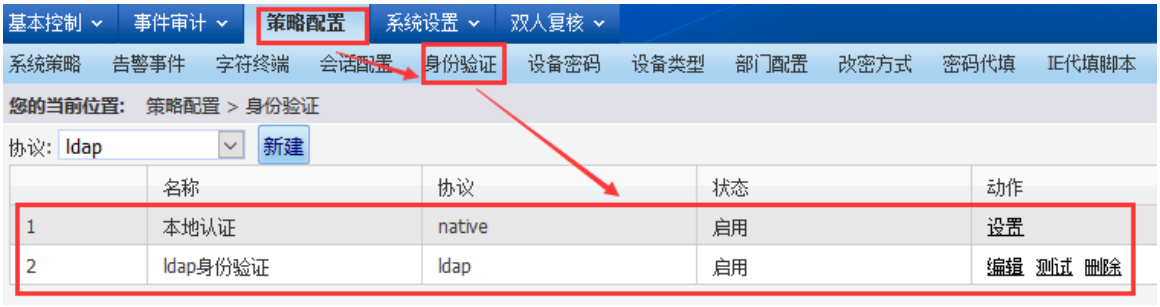
2.4.5 身份验证

1. 概述

堡垒机提供多种身份验证机制，包括 NATIVE、LDAP、TOTP 动态双因素、Radius、MIX 双因素组合。

菜单位置：策略配置 > 身份验证

图2-26 身份验证示意图



2. NATIVE身份验证

堡垒机身份验证方式默认为 native，表示静态密码认证。

菜单位置：策略配置 > 身份验证> native 身份验证-设置

图2-27 Native 身份验证参数设置示意图

图2-28 Native 中参数设置选项含义示意图

参数解释：

- 默认密码：此默认密码为批量导入用户时默认设置的密码。
- 最小密码长度：用户在自行修改密码的时候密码的最小长度要求。
- 自动密码长度：通过堡垒机自动生成的密码长度。
- 手动修改自身密码的强度设定：设置密码的复杂度要求。
- 外部字典检查：加强密码复杂度要求。
- 密码有效期、锁定：设置全局性的账号密码有效期、密码锁定策略。
- 密码手工设置：指定哪个角色管理员可以进行用户账号密码重置操作。

3. LDAP身份验证

堡垒机支持 Simple 和 Digest-md5 两种 LDAP 身份验证方式，区别如下：

- Simple：需用绑定查询用户及口令，配置复杂，但兼容性好，几乎所有的目录服务器都支持该验证方法。
- Digest-md5：Digest-md5 LDAP 的一种身份验证机制，只需要通过 LDAP 的主机名（必须是 FQDN）和 ip 地址来进行身份验证。

(1) DIGEST-MD5 方式

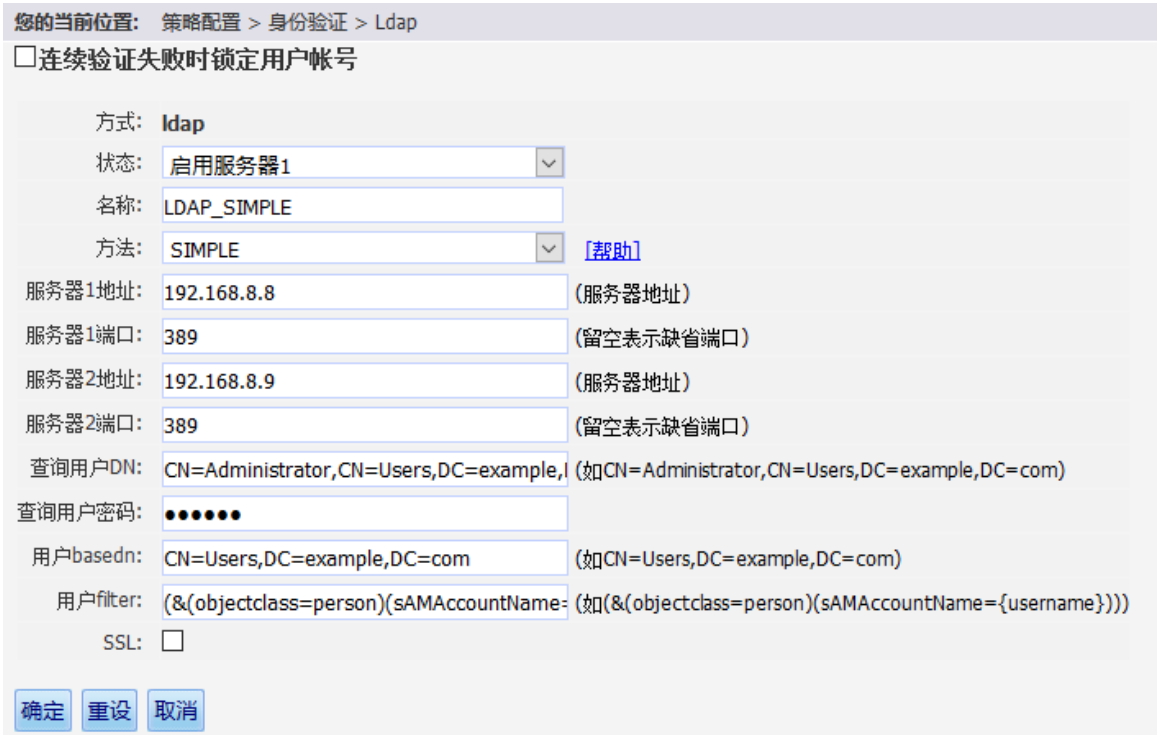
图2-29 DIGEST-MD 方式示意图

参数解释：

- 连续验证失败时锁定用户账号：用户账号锁定策略参见 Native 身份验证设置。
- 服务器全称：AD（LDAP）服务器主机名全称（主机名不正确会导致身份验证失败）。
- 服务器地址：AD（LDAP）服务器 IP 地址。
- 服务器端口：默认使用 TCP 389 端口。

(2) Simple 方式

图2-30 SIMPLE 方式示意图



可点击帮助获取 SIMPLE 配置说明，如下图。

图2-31 SIMPLE 帮助页面示意图

管理 LDAP 身份认证的详细配置请参考《LDAP 配置举例》手册。

4. TOTP身份验证

堡垒机内置动态双因素令牌实现 TOTP（Time-based One Time Password，基于时间的一次性密码）功能，管理 TOTP 身份认证的详细配置请参考《TOTP 配置举例》手册。

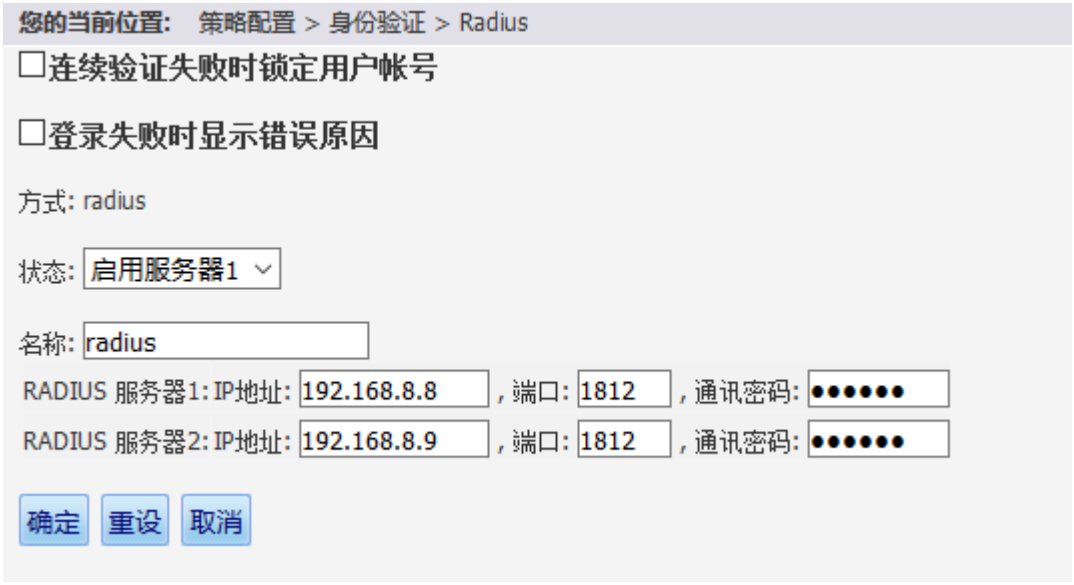
图2-32 TOTP 身份验证示意图

连续验证失败时锁定用户账号：用户账号锁定策略参见 Native 身份验证设置。

5. Radius身份验证

堡垒机可以通过用户的 Radius 服务器（例如 RSA 的认证服务器就是一个 radius 认证服务器）进行身份验证，管理 Radius 身份认证的详细配置请参考《Radius 配置举例》手册。

图2-33 Radius 身份验证示意图



参数解释：

- 连续验证失败时锁定用户账号：用户账号锁定策略参见 Native 身份验证设置。
- 名称：验证方法名称如：RSA，可自定义。
- IP 地址：Radius 服务器 ip 地址。
- 端口：Radius server 的通讯端口，标准的端口为 UDP 1812 或者 UDP 1813。
- 通讯密码：也称为 secret，具体请咨询 Radius server 管理员。

6. 双因素组合(MIX)身份验证

用户可以组合任意 2 种身份验证方式形成 MIX，从而实现自定义双因素组合。管理双因素组合(MIX)身份认证的详细配置请参考《双因素组合(MIX)配置举例》手册。

图2-34 双因素组合 Mix 身份验证示意图

双因素组合选项含义如下：

- 连续验证失败时锁定用户账号：用户账号锁定策略参见 Native 身份验证设置。
- 状态：启用或者禁用，启用后管理员可选择此身份认证方式。
- 名称：用户自定义身份验证名称。
- 第一身份验证方式：选择已有的其中一种身份验证方式。
- 第二身份验证方式：选择第二种身份验证方式，不能与已选第一种身份验证方式一样。
- 逻辑验证方式：与、或关系。

2.4.6 设备密码

堡垒机可提供自动修改目标设备密码功能，其中超级管理员可设定目标设备密码相关的全局选项。

菜单位置：策略配置 > 设备密码

图2-35 设备密码示意图

设备密码选项含义如下：

- 随机密码强度设定：设定随机密码的复杂度及。
- 全局改密通知：当对目标设备进行改密操作时，默认发送改密通知已勾选管理员，该功能要求密码保管员必须设定邮件地址。
- 密码备份规则：默认不允许密码保管员备份密码，超级管理员勾选允许的备份规则后密码保管员方可进行密码备份。

2.4.7 设备类型

1. 设备类型介绍

不同的设备类型在访问协议、登录方式、改密方式上的差异很大，为了便于管理，堡垒机系统内置了如下图所示设备类型，基本满足大多数环境使用。

菜单位置：策略配置 > 设备类型

图2-36 设备类型示意图

名称		分类	字符终端	图形终端	文件传输	特权帐号	普通提示符	特权提示符	改密方式	动作
1	General Linux	linux	telnet ssh	vnc	ftp sftp	root	$	#	general linux	管理
2	General Network	network	telnet ssh	rdpapp		enable	>	#		管理
3	Cisco IOS Device	network	telnet ssh	rdpapp		enable	>	#	cisco ios device	管理
4	Cisco CatOS Device	network	telnet ssh	rdpapp		enable	>	> (enable)		管理
5	Huawei Quidway Device	network	telnet ssh	rdpapp		super	>	>	huawei quidway device	管理
6	H3C Comware Device	network	telnet ssh	rdpapp		super			h3c device	管理
7	HP UX	unix	telnet ssh	vnc	ftp sftp	root	$	#	general unix	管理
8	IBM AIX	unix	telnet ssh	vnc	ftp sftp	root	$	#	general unix	管理
9	General Unix	unix	telnet ssh	vnc	ftp sftp	root	$	#	general unix	管理
10	Microsoft Windows	Windows	telnet	rdp rdpapp	ftp	administrator	>	>	microsoft windows agent	管理

点击“默认设备类型及编码”进行对批量添加设备时默认设备类型及编码进行修改，如下图。

图2-37 设备批量添加及新建时对应选项的默认值设置示意图

堡垒机中默认包含 10 种设备类型，下表中对相关类型进行了简要说明。

表2-2 堡垒机中默认包含 10 种设备类型说明

编号	类型名称	分类	说明
1	General Linux	linux	适用于所有Linux版本
2	General Network	network	适用于Cisco、huawei以外其他类型网络设备
3	Cisco IOS Device	network	适用于运行IOS的Cisco或其他CLI兼容设备
4	Cisco CatOS Device	network	适用于运行CatOS的Cisco或其他CLI兼容设备
5	Huawei Quidway Device	network	适用于Huawei及其他CLI兼容设备
6	H3C Comware Device	network	适用于H3C及其他CLI兼容设备
7	HP UX	unix	适用于HP UX
8	IBM AIX	unix	适用于IBM AIX
9	General Unix	unix	适用于所有Unix-like设备
10	Microsoft Windows	Windows	适用于Windows 2003、2008等Windows设备

不同类型的设备使用的协议一般不同，下表是堡垒机中设备默认服务和允许使用的服务类型清单。

表2-3 堡垒机中设备默认服务和允许使用的服务类型清单

设备类型	默认服务	可选字符服务	可选图形服务
General Linux	ssh vnc	ssh telnet	vnc
General Network	telnet	telnet ssh	rdpapp
Cisco IOS Device	telnet	telnet ssh	rdpapp
Cisco CatOS Device	telnet	telnet ssh	rdpapp
Huawei Quidway Device	telnet	telnet ssh	rdpapp
H3C Comware Device	telnet	telnet ssh	rdpapp
HP UX	telnet vnc	telnet ssh	vnc
IBM AIX	telnet vnc	telnet ssh	vnc
General Unix	telnet vnc	telnet ssh	vnc
Microsoft Windows	rdp	telnet	rdp rdpapp

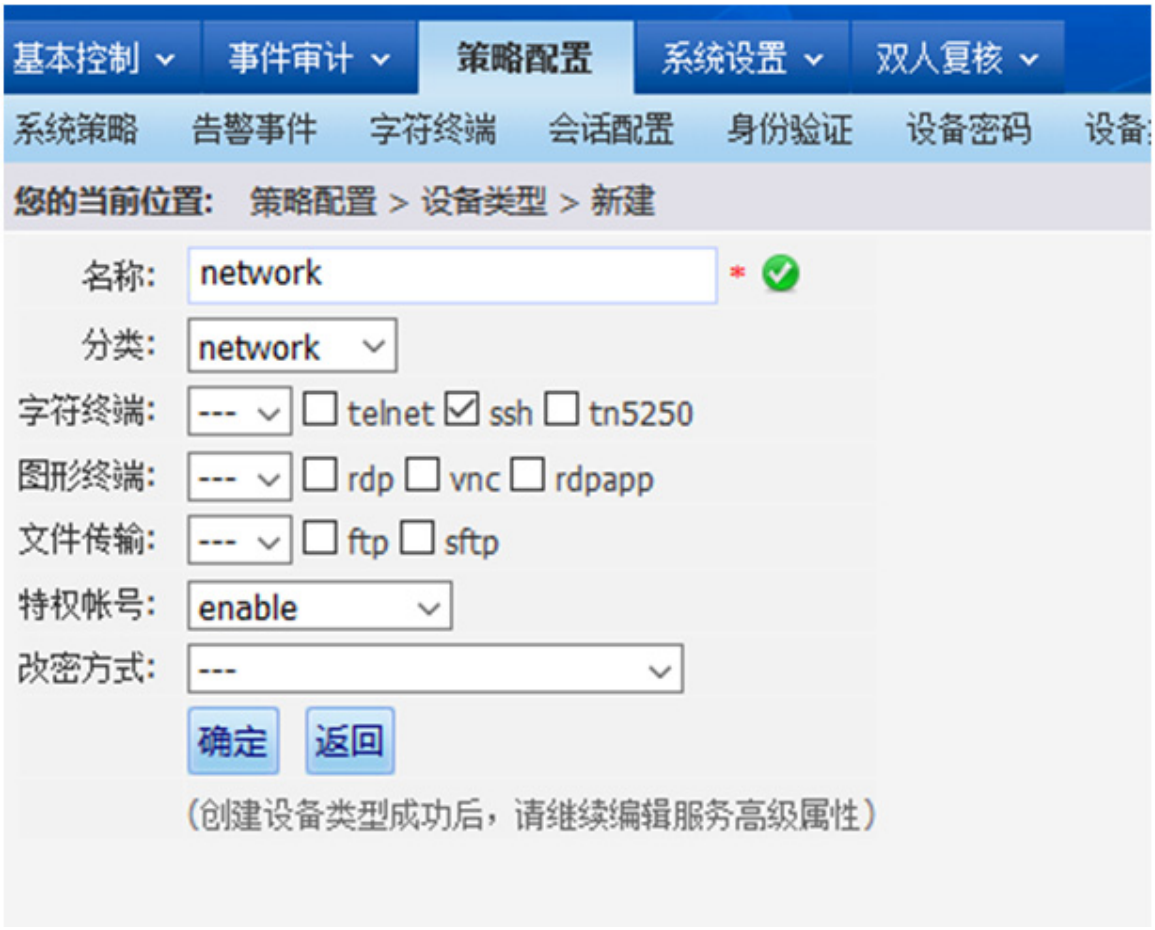
2. 系统支持协议介绍

- RDP（远程桌面）协议：堡垒机支持 Windows 的远程桌面（RDP）服务，默认使用 TCP 3389 端口访问远程桌面。
- SSH 协议：SSH 为 Secure Shell 的缩写，因其通信过程加密安全性较高，因此广泛应用于各种 Linux、UNIX 设备中，默认通信端口为 TCP 22。
- TELNET 协议：Telnet 是字符终端服务之一，主要用于网络设备、较老的 Unix 设备中，默认通信端口为 TCP 23。
- RDPAPP：此服务为堡垒机对访问应用发布的简称，需使用此服务需配置应用发布服务器。
- SFTP\FTP：堡垒机支持 sftp\ftp 协议进行文件传输，SFTP 默认使用 22 端口，FTP 默认为 21 端口（主动模式）。
- VNC：堡垒机支持 VNC (Virtual Network Computer)协议，常用于 Windows、Linux、UNIX 的远程桌面控制，VNC 默认端口为 TCP 5900，也可以在 5900-5999。
- TN5250：TN5250 用于 AS/400 设备，为堡垒机可选模块。

3. 新建设备类型

如果堡垒机默认内置的设备类型无法满足需求，则可以进行新建所需设备类型，如下图所示。

图2-38 新建设备类型示意图



新建设备选项含义如下：

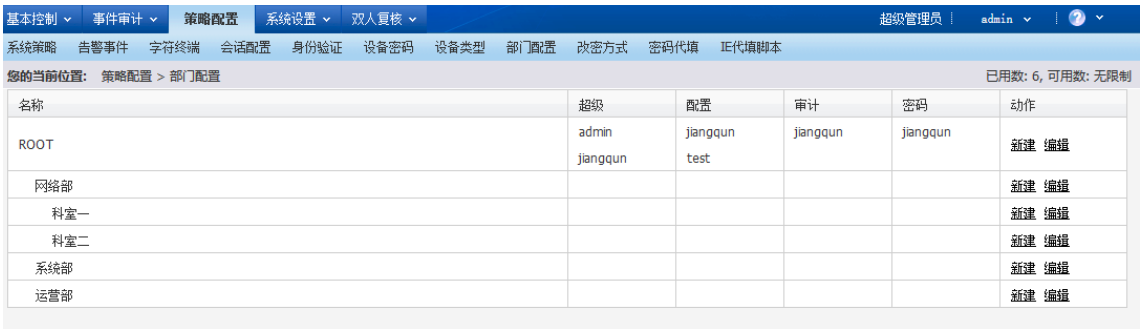
- 名称：填写需要新建的设备类型名称，不可为中文。
- 分类：堡垒机内置常用 network、UNIX、Windows，对新建设备类型进行大致分类。
- 字符终端：默认需要使用的字符终端服务，如 ssh。
- 图形终端：默认需要使用的图形终端服务，如 vnc。
- 文件传输：默认需要使用的文件传输服务，如 sftp。
- 特权账号：设定默认的特权账号，是系统中最高权限的系统账号，如 Linux 系统中的 root 账号，Windows 系统中的 administrator 账号。
- 改密方式：用于选择改密方式，堡垒机内置常用的改密模版如下：
  - Windows 改密：内置支持 agent 改密，改密需要在目标设备安装堡垒机相关 agent。
  - Linux 设备改密：使用内置 General Linux。
  - UNIX 设备改密：支持 hp unix、ibm aix、sco unix 等。
  - Network 设备改密：支持 huawei、cisco。

2.4.8 部门配置

菜单位置：策略配置 > 部门配置

堡垒机可以进行部门划分，堡垒机可以划分二级部门、三级部门以及更多部门实现针对部门的管理员分权（超级管理员除外）。

图2-39 部门配置示意图



注意

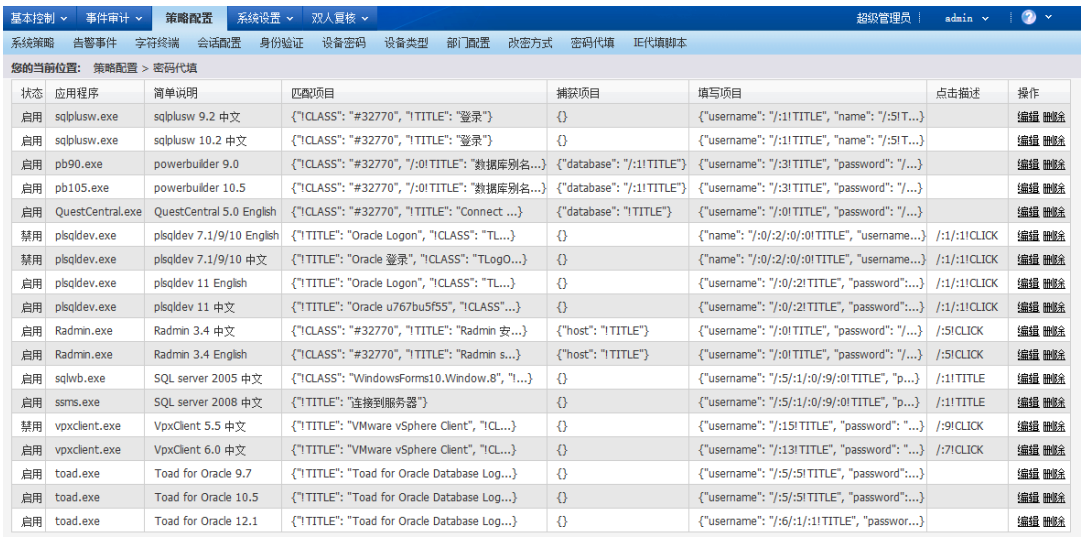
更多相关部门配置参见《部门分权配置举例》手册

2.4.9 密码代填\IE代填脚本

菜单位置：策略配置 > 密码代填\IE 代填脚本

密码代填：针对应用发布 C/S 设备进行密码代填，系统默认可以支持如下 C/S 设备。

图2-40 CS 密码代填示意图



注意

更多关于密码代填、IE 代填脚本配置参见《应用发布配置举例》手册。

2.5 系统设置

2.5.1 授权管理

当堡垒机授权日期到期、授权变更可通过授权管理重新授权。

菜单位置：系统设置 > 授权管理

图2-41 授权管理示意图

注意

初次访问设备需要更新授权才可进行后续配置和使用，申请授权等相关内容请参考《License 激活申请和注册操作指导》手册。

2.5.2 安全证书

HTTPS 安全证书需要在堡垒机上线后进行部署，避免出现部分浏览器无法忽略证书错误阻止访问堡垒机系统。

菜单位置：系统设置 > 安全证书

依次填写下列 C、ST、L、O、OU、CN、SN 字段，点击部署完成 https 证书制作。

图2-42 制作 HTTPS 证书示意图

注意

- CN 字段必须与用户访问堡垒机所使用的 IP 地址或域名一致。
- 堡垒机根证书可选择安装，但会收到浏览器的证书错误提示。
- HTTPS 证书必须在堡垒机系统上线后进行部署，否则可能会有部分浏览器拒绝忽略证书错误提示拒绝访问堡垒机。
- 完成 https 证书部署后会要求重启 https 服务。

2.5.3 节点配置

节点管理主要进行检查当前堡垒机系统的状态情况、补丁安装。

菜单位置：系统设置 > 节点配置

图2-43 节点配置示意图

注意

不可编辑、删除当前节点等操作。

2.5.4 HA安装

用户可通过 Web 界面进行堡垒机的 HA 安装和退出操作。

图2-44 HA 安装示意图

注意

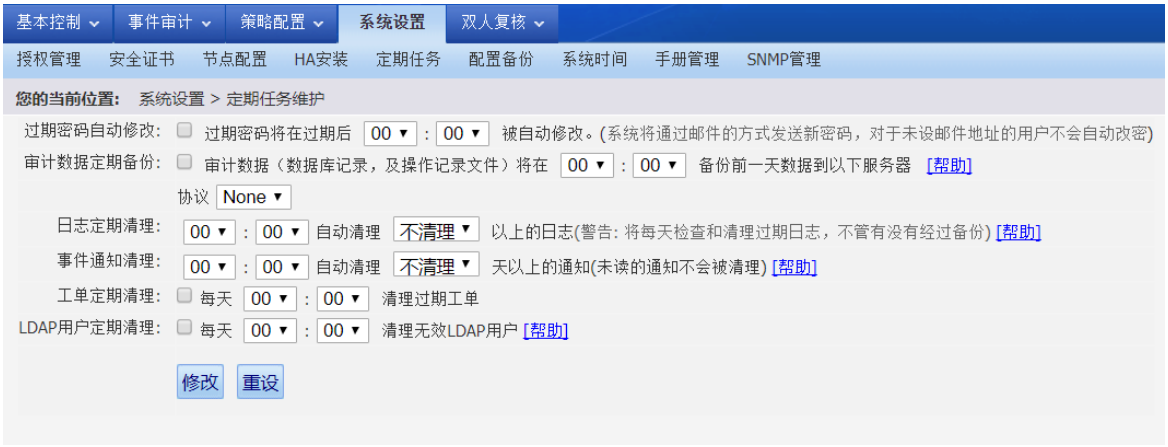
更多关于 HA 配置参见《双机热备（HA）配置举例》手册。

2.5.5 定期任务

通过定期任务可以设定用户账号密码到期自动修改、审计日志自动备份、审计日志自动清理、事件通知日志定期清理。

菜单位置：系统设置 > 定期任务

图2-45 定期任务示意图



定期任务选项含义如下：

- 过期密码自动修改：启用此功能则当用户账号密码到期则系统将通过邮件的方式发送新密码，对于未设邮件地址的用户不会自动改密。
- 审计数据定期备份：对数据库记录，及操作记录文件进行定期备份，备份协议有 ftp/rsync。
- 日志定期清理：清理目录/var/log/unis/下的所有日志文件。警告: 将每天检查和清理过期日志，不管有没有经过备份。
- 事件通知清理：清理过期事件通知（1-3 天），事件类型包括工单、双人授权、命令复核事件通知。
- 工单定期清理：清理过期工单。
- LDAP 用户定期清理：清理 Ldap 服务器上不存在，但堡垒机上存在或者 Ldap 服务器返回用户状态标识为禁用的用户，仅清理 LDAP 身份认证的用户。

注意

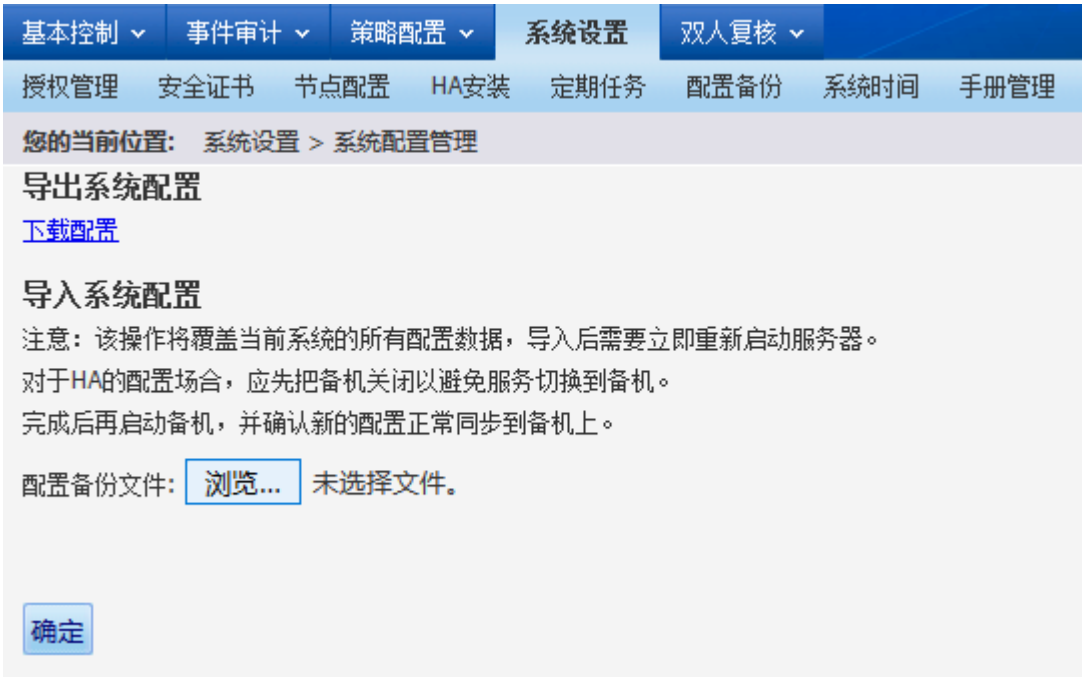
相应的配置详细信息可点击选项后面的“帮助”获取。

2.5.6 配置备份

用户可通过 Web 界面进行堡垒机配置备份、配置还原操作。

菜单位置：系统设置 > 配置备份

图2-46 配置备份示意图



2.5.7 系统时间

用户可自行通过 Web 界面修改堡垒机时间。

菜单位置：系统设置 > 系统时间

图2-47 系统时间示意图

2.5.8 手册管理

用户可通过 Web 界面上传用户手册至运维操作系统，上传并分配给用户后，其他用户可自行下载手册。

图2-48 手册管理示意图

点击“浏览”，选择要上传的手册，点击“上传”，即可上传相应的手册，如下图。

图2-49 上传手册示意图

点击“管理权限”可对手册的权限进行管理。

图2-50 设置手册下载权限示意图

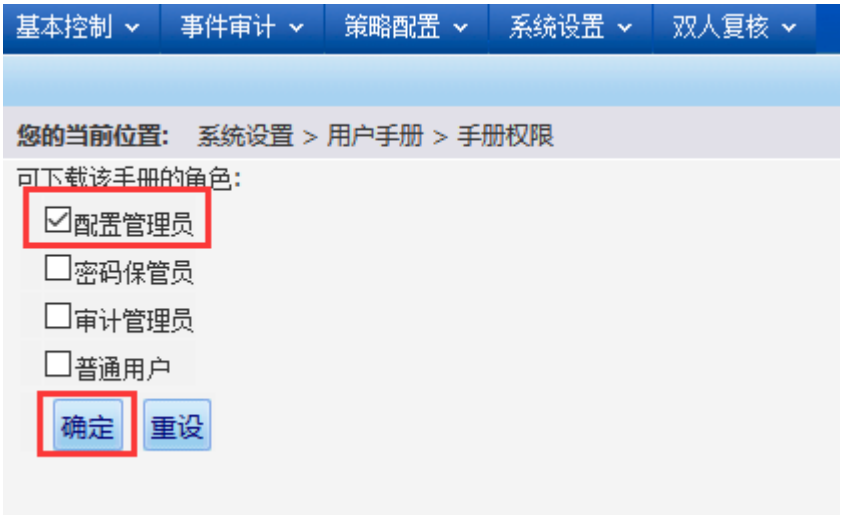


图2-51 具备下载权限的用户界面新增“用户手册”按钮示意图

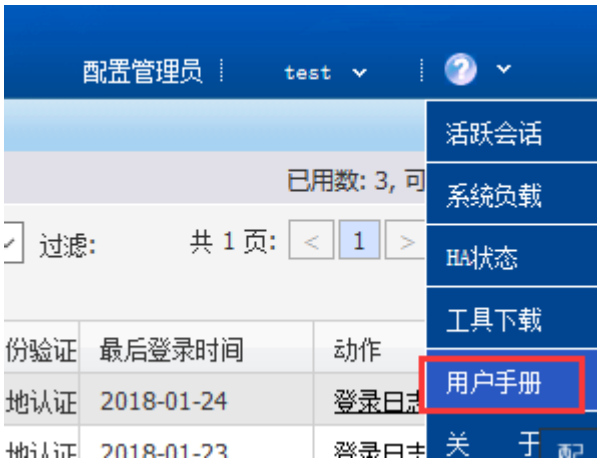
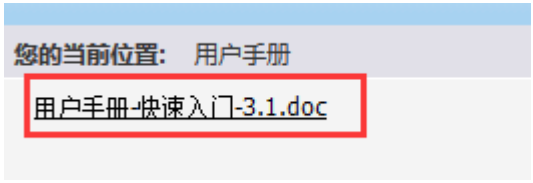


图2-52 下载手册

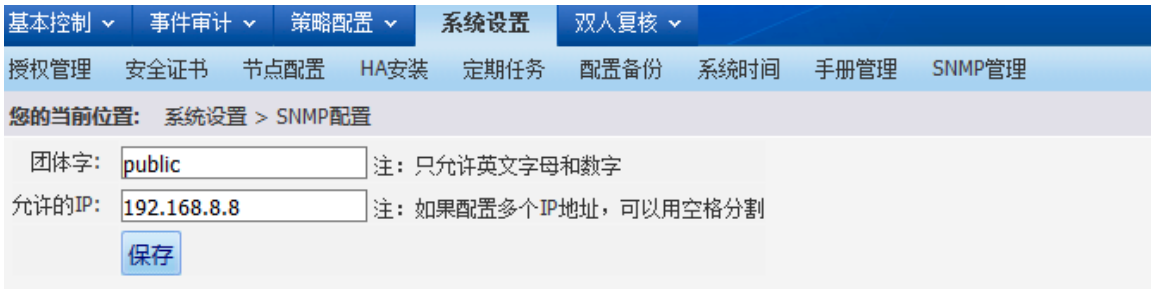


2.5.9 SNMP配置

菜单位置：系统设置>SNMP 管理

用户可自行通过 Web 界面设置 SNMP。

图2-53 SNMP 管理示意图



2.6 命令复核

命令复核又称金库模式，可以实现当 A 用户在执行命令的时候需要 B 用户进行复核，如 B 用户允许执行则命令在目标设备执行，如 B 用户拒绝执行复核的命令则直接拒绝此命令在目标设备执行。

图2-54 命令复核示意图

3 配置管理员配置

3.1 操作页面简介

Web 管理界面由菜单栏、状态栏、消息提醒及主内容区组成。每个菜单都有相应的一个或多个子菜单。当您点击一个菜单项目，如基本控制，在相应菜单下方会扩展出其包含的子菜单：用户账号、临时用户、系统账号、目标设备、自动发现、用户分组、设备分组，点击相应子菜单，即可在主内容区显示相关配置页面。

图3-1 配置管理员操作界面示意图

操作界面说明：

- 菜单栏：提供了配置管理员可进行配置操作的所有菜单。
- 状态栏：右侧的状态栏，显示当前用户角色、用户名和问号菜单，点击用户角色可在多个角色间进行切换，点击用户名可以进行个人账户设置、系统语言变更、退出登录等操作，点击问号菜单，可以查看系统负载和产品关于以及工具下载。
- 消息提醒：用于提示用户与当前账户相关的工单申请、双人授权、命令复核等通知信息，用户可通过点击 

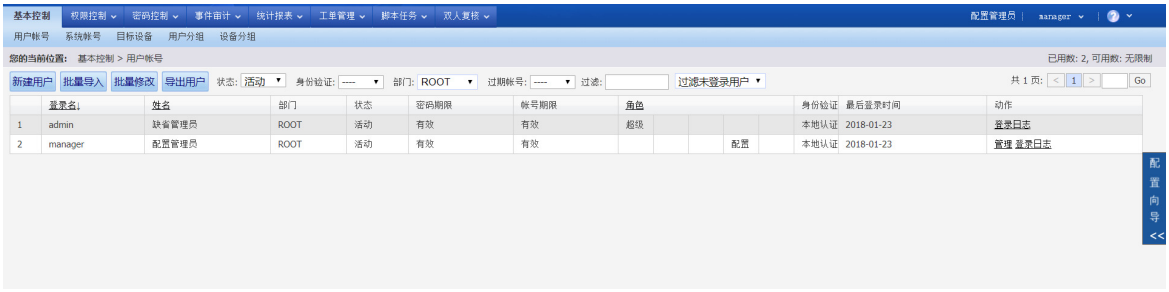
查看具体的消息信息。
- 主内容区：用于显示各级子菜单相应的配置页面。
- 配置向导：配置向导包含配置管理员常见的配置选项，用于帮助管理员快速完成相关策略的设置，点击配置向导即可展开并显示包含的子项目。

3.2 用户账号管理

用户帐号是指堡垒机为所有使用者分配的帐号，如：zhangsan（张三）、lisi（李四）。堡垒机通过用户帐号进行用户的身份验证和审计。配置管理员可以建立和管理配置管理员和普通用户帐号。

通过依次点击“基本控制 > 用户账号”，即可进入用户账号配置界面，通过此菜单可以进行用户账户的创建、修改、导出等操作。

图3-2 用户账号管理界面示意图



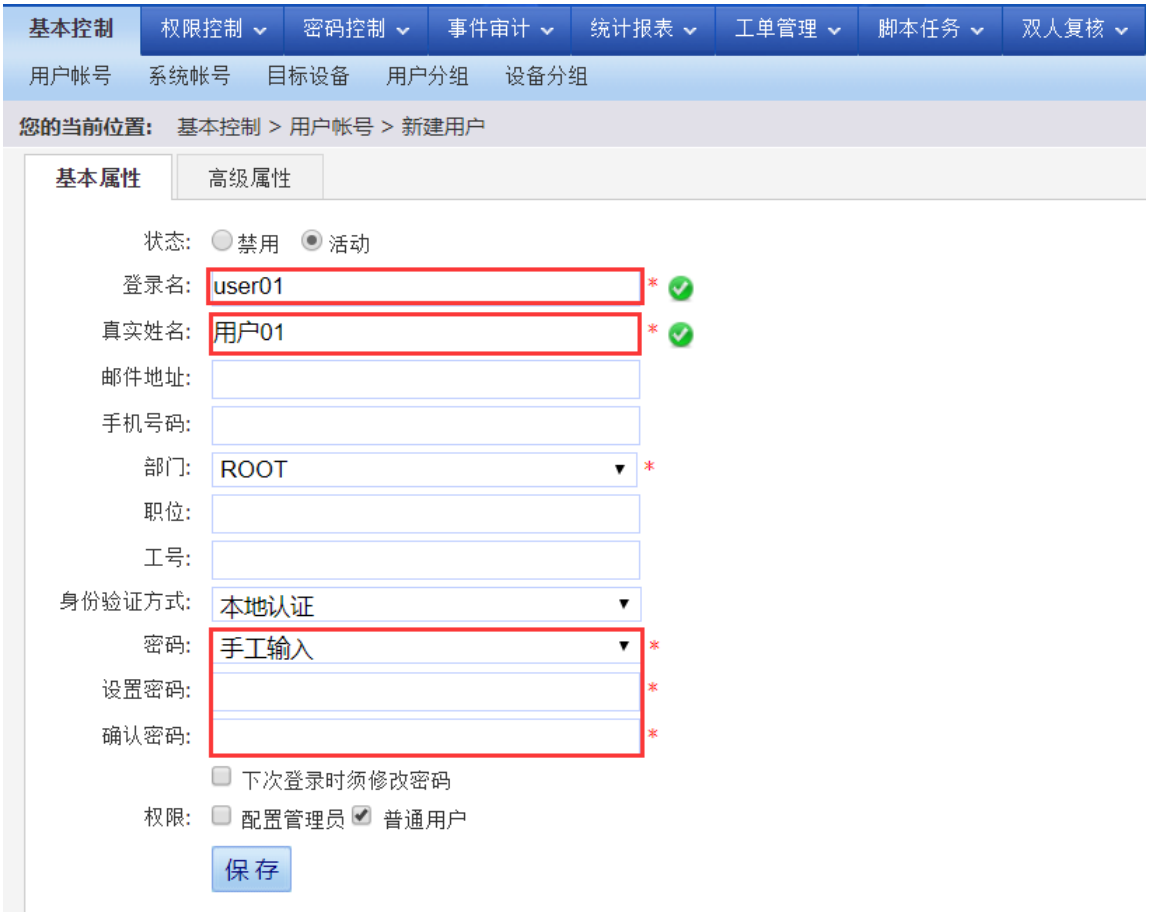
3.2.1 新建用户

菜单位置：基本控制 > 用户账号 > 新建用户

用户账号属性包含：基本属性与高级属性，基本属性中部分信息为创建用户账号时必须填写的项目，高级属性可根据实际情况选择性填写。

1. 基本属性（必填项）

图3-3 基本属性示意图



参数解释：

- 状态：表示当前账户是否可用，默认为“活动”状态。

- 登录名：用户登录堡垒机所使用的用户名，如：zhangsan。
- 真实姓名：用户帐号使用者的真实姓名，如，张三。
- 邮件地址：设置用户帐号的邮件地址，默认为空。若需要使用下列功能，则必须为用户帐号设置邮件地址：
  - 自动设置和修改用户帐号
  - 用户帐号密码过期自动修改
  - 密码保管员和配置管理员接受密码提醒和改密邮件
  - 接受 self 方式的监控邮件通知
- 手机号码：设置用户帐号的手机号码，默认为空。但需要在监控短信通知中使用 self 时，该选项为必填项。
- 部门：选择用户帐号所在的部门，默认为 ROOT。使用超级管理员可以在“策略配置 > 部门配置”中建立和管理部门。
- 职位：设置用户的职位，默认为空。
- 工号：设置用户的工号，默认为空。
- 身份验证方式：设置用户帐号的身份验证方式，默认为本地认证，表示静态密码认证。除本地认证方式外堡垒机还支持下列外部身份验证：LDAP、totp、radius 和双因素认证，关于外部身份验证请参考“超级管理员配置”中的相关介绍。
- 密码：默认为“手工输入”，可通过下拉列表进行选择手工输入或自动设置：
  - 手工输入：表示管理员为用户帐号设置一个初始的密码，此时堡垒机不对管理员输入的密码做复杂性检查。
  - 自动设置：表示堡垒机自动生成用户帐号的密码，您可以设置新密码的位数。新的密码的分发方式默认为发送密码邮件给最终用户。
- 下次登录时必须修改密码：为可选项，默认未选中。如果勾选了该项，用户在首次登录堡垒机的 Web 站点时会被要求修改密码，如果用户没有通过 Web 站点修改过密码直接 ssh 登录堡垒机将收到“Notice: Please change your password on website”的提示。
- 权限：设置用户帐号的权限。配置管理员针对用户账号默认只能设置“配置管理员”和“普通用户”两种角色权限。

用户基本信息创建完成后，如需对账户有效期、登录 IP、登录证书等进行设置，可以通过用户高级属性进行修改。

2. 高级属性（可选项）

图3-4 高级选项示意图

参数解释：

- 密码有效期至：设置用户帐号本地认证密码有效期，默认为 90 天，留空表示密码永不过期。用户可以点击输入框后的“清空”快速清空有效期，或者点击“恢复”还原修改前的值。
- 允许登录 IP：设置允许登录的 IP 或 IP 段，格式如: 192.168.1.1, 192.168.1.1-192.168.1.5, 192.168.1.*。
- 允许登录的 MAC：设置允许登录的一个或多个 MAC，格式如: 00:00:00:00:00:00, 00:00:00:00:00:00。
- 有效期：设置用户帐号的有效期，默认为一年，留空表示永不过期。。
- 备注：添加用户帐号的备注信息，默认为空。

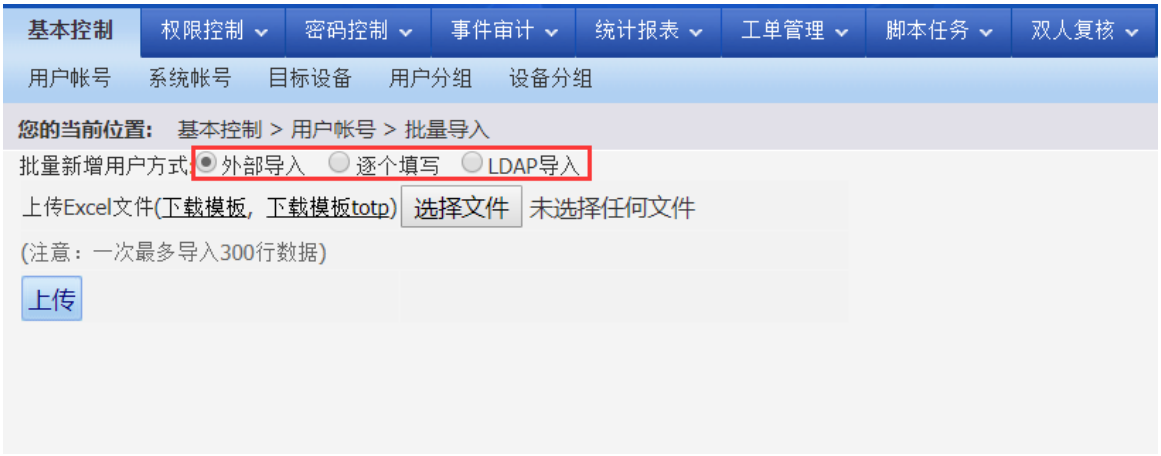
配置管理员可根据实际情况设置相关信息，点击“保存”按钮后完成用户账号的设置。

3.2.2 批量导入用户

菜单位置：基本控制 > 用户账号 > 批量导入

配置管理员通过批量导入的方式可以快速创建多个用户账户。

图3-5 批量导入用户示意图



堡垒机支持以下三种方式导入用户账号：

- 外部导入（默认的批量导入方式）
- 逐个填写
- LDAP 导入

不同方式间可通过点击相应单选按钮进行切换，通过批量导入方式导入的用户均为普通 用户，在后续章节中将逐一介绍三种方式批量导入用户帐号方法。

1. 外部导入

外部导入是指通过 excel 文件将相关用户账号信息导入到堡垒机中，操作前必须确保客户端已安装相应 office 应用程序，用于编辑 excel 模板文件。

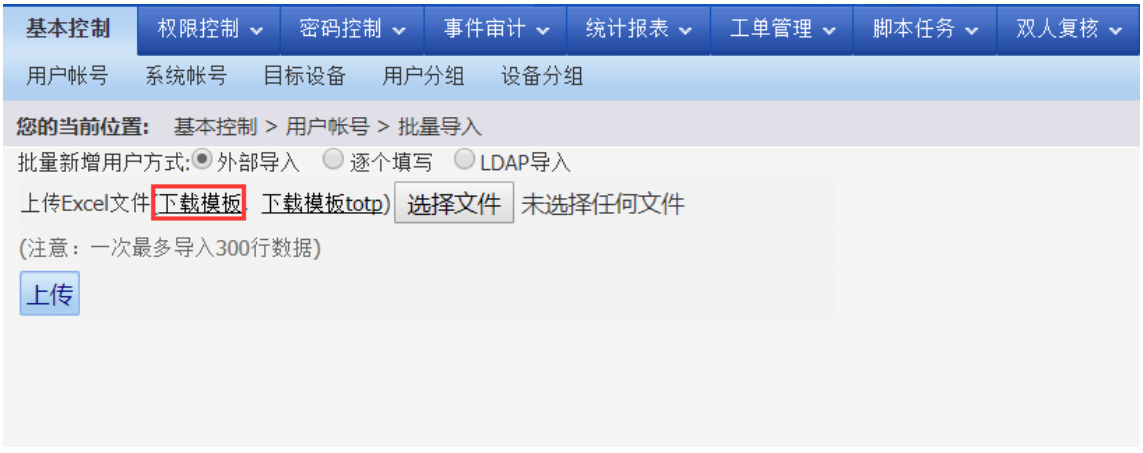
外部导入具体操作方法如下：

(1) 下载模板文件

菜单位置：基本控制 > 用户账号 > 批量导入

确保批量新增用户方式为“外部导入”，点击页面中“下载模板”获取模板文件，如下图所示。

图3-6 获取模板文件示意图



(2) 填写模板文件

打开模板文件 users.xls 填写相关用户信息，如下图所示。

图3-7 填写模板文件示意图

登录名	真实姓名	部门	职位	工号	电子邮件	手机
user01	测试用户01					
user02	测试用户02					
user03	测试用户03					

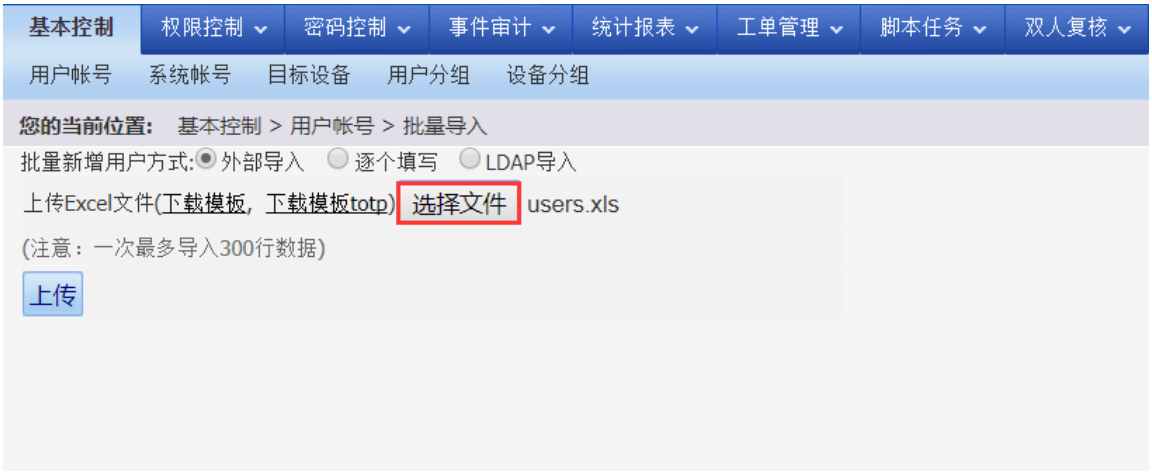
填写时请注意：

- 登录名和真实姓名为必填项，其他选项可留空；
- 单个模板文件中数据量不能超过 300 行；
- 登录名不能与系统中已经存在的用户相同。

(3) 上传模板文件

点击“选择文件”按钮，选择相关模板文件，如下图所示。

图3-8 上传模板文件示意图



点击“上传”按钮，堡垒机 将读取模板文件中相关用户信息，如下图所示。

图3-9 上传模板文件确认示意图

外部导入账户选择身份验证方式及密码，可对默认密码为 123456 进行修改；如需强制用户下次登录时修改密码，请勾选“下次登录时需修改密码选项”。如在界面有红色标记，则此用户可能已经存在，可点击该账号后面的“移除”或列表下方的“移除已存在用户”选项对存在的用户进行移除。在此页面可对相关信息再次编辑，确认信息无误后，点击“确定”按钮完成用户账户的导入，如下图所示。

图3-10 上传模板文件完成示意图

2. 逐个填写

逐个填写是指配置管理员依次填写多个用户帐号信息同时提交的批量导入方法，具体操作如下：

(1) 选择“逐个填写”批量导入方式

菜单位置：基本控制 > 用户账号 > 批量导入

将批量新增用户方式设置为“逐个填写”。

(2) 用户属性设置及填写用户信息

堡垒机会默认填写身份验证方式、默认密码、密码有效期和帐号有效期等信息，用户可根据实际情况进行批量修改。在用户表单处根据实际情况填写相关用户信息，点击“添加”按钮默认添加一行表单，如需添加多行，可在右侧下拉列表处选择相应行数后点击“添加”即可。

图3-11 逐个填写示意图

用户表单中登录名与真实姓名为必填项，如果所填写的登录名称与系统中已存在的用户账户名相同，则在点击确定的时候提示“对于已存在的用户，需要更新吗？”。

选项介绍：

- 更新：新导入的用户信息会覆盖堡垒机中已存在的用户信息。
- 只新增不更新：只添加堡垒机中不存在的用户账号，对已存在的用户账号不作处理。

图3-12 登录名称与系统中已存在的相同

确认无误后点击“确认”按钮完成批量导入，如下图所示。

图3-13 逐个填写完成示意图

3. LDAP导入

LDAP 导入是指从现有的 LADP 服务中获取相关用户账户信息，用来实现堡垒机与 LDAP 服务器账户同步的效果。

具体操作方式如下：

(1) 选择“LDAP 导入”方式

菜单位置：基本控制 > 用户账号 > 批量导入

将批量新增用户方式为设置为“LDAP 导入”

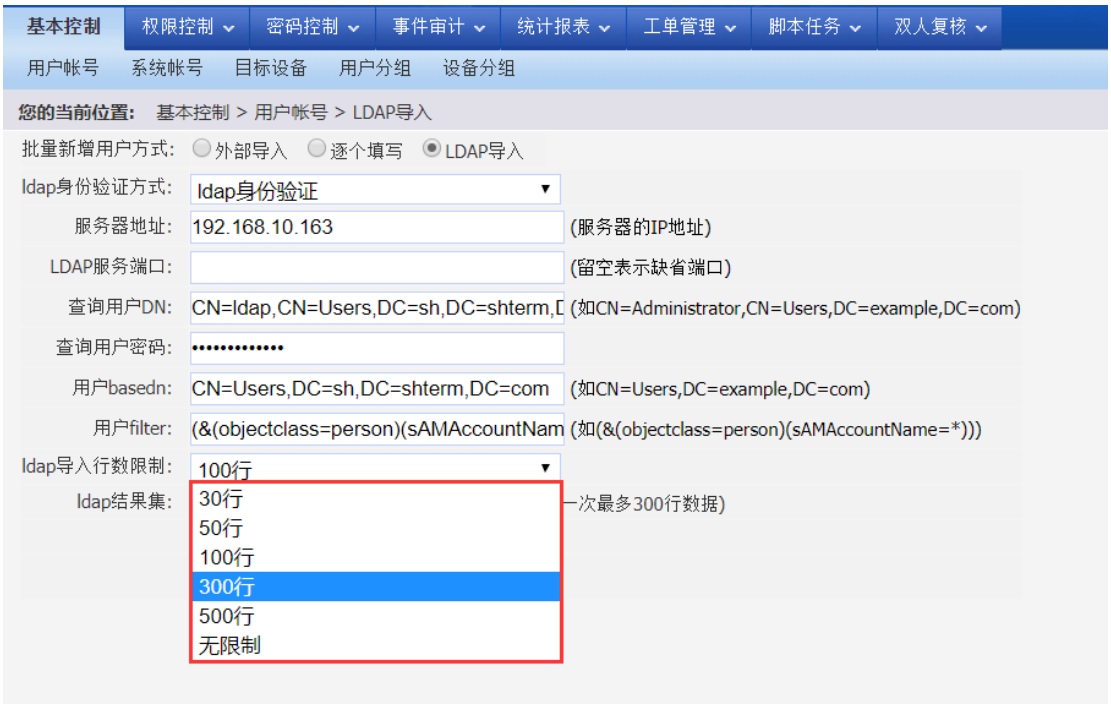
(2) “LDAP 导入”参数配置

如果超级管理员设置了 LDAP 份验证方式，堡垒机将自动填写相关选项（如下图所示）。用户可以在 LDAP 身份验证方式中选择不同的验证方式，在不同的 LDAP 服务器间切换。如果堡垒机中没有任何已配置的 LDAP 验证，用户可以参考超级管理员配置外部认证相关章节先添加 LDAP 认证方式。

图3-14 LDAP 导入示意图

- LDAP 导入行数限制：用户可根据实际情况选择导入用户信息的条数，如下图所示。

图3-15 Ldap 导入行数限制示意图



参数解释：

- LDAP 结果集：选择堡垒机导入账户的显示方式（推荐页面形式）。
- 配置 LDAP 用户属性关系：AD 域中人员的信息 ID，保持默认值即可。

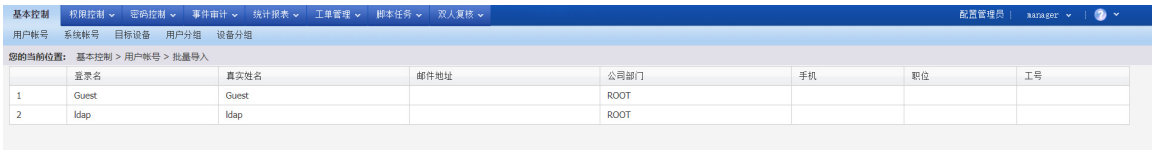
(3) 导入用户信息

确认相关参数后点击“提交”按钮，堡垒机会根据配置的相关信息自动查询 LDAP 服务器中用户账户信息，以相关方式（根据结果集中配置的方式）回显给管理员，如下图所示。

图3-16 导入回显示意图

点击“确定”按钮，在弹出的页面中选择已存在用户的更新方式，如下图所示。

图3-17 导入成功示意图



选项介绍：

- 更新：新导入的用户信息会覆盖堡垒机中已存在的用户信息
- 只新增不更新：只添加堡垒机中不存在的用户账号，对已存在的用户账号不作处理

点击相应按钮后完成用户账户更新，可在“用户账号”页面看到新增的普通用户，当用户认证方式选择为相应 LDAP 认证时，账号密码为原 LDAP 服务器中相同账户所设置的相关密码。

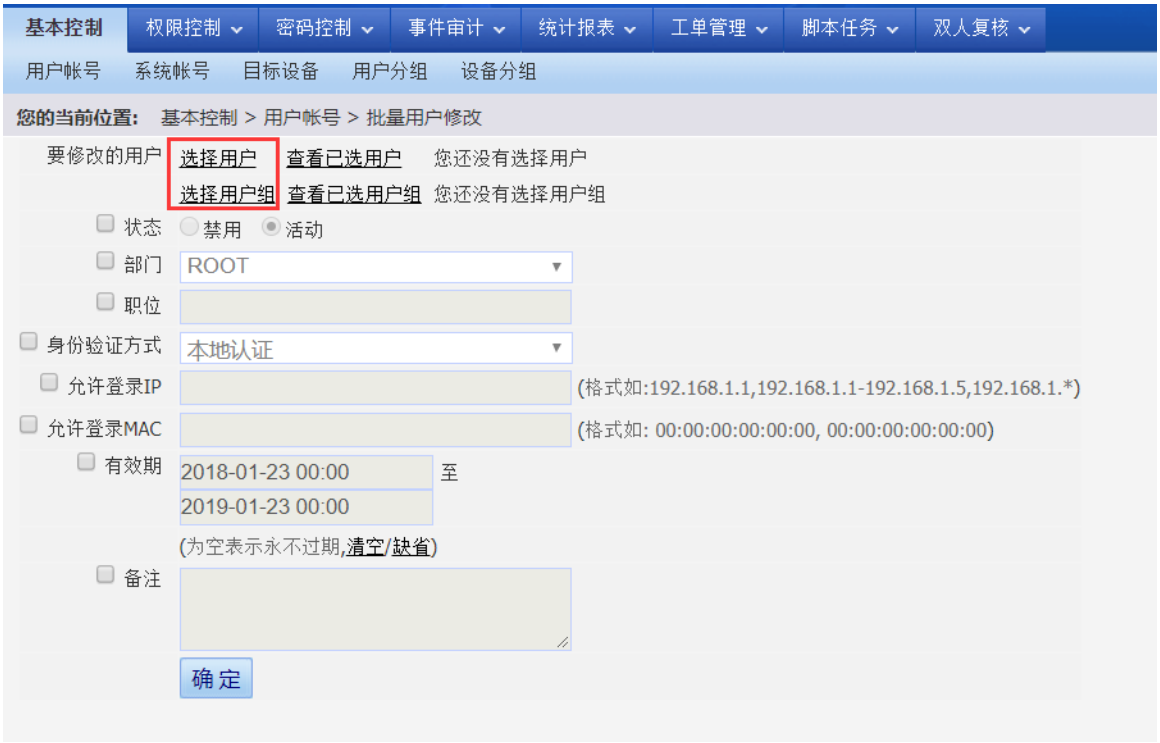
3.2.3 批量修改

通过用户批量修改功能，可帮助管理员快速批量修改用户账号信息。

菜单位置：基本控制 > 用户账号 > 批量修改

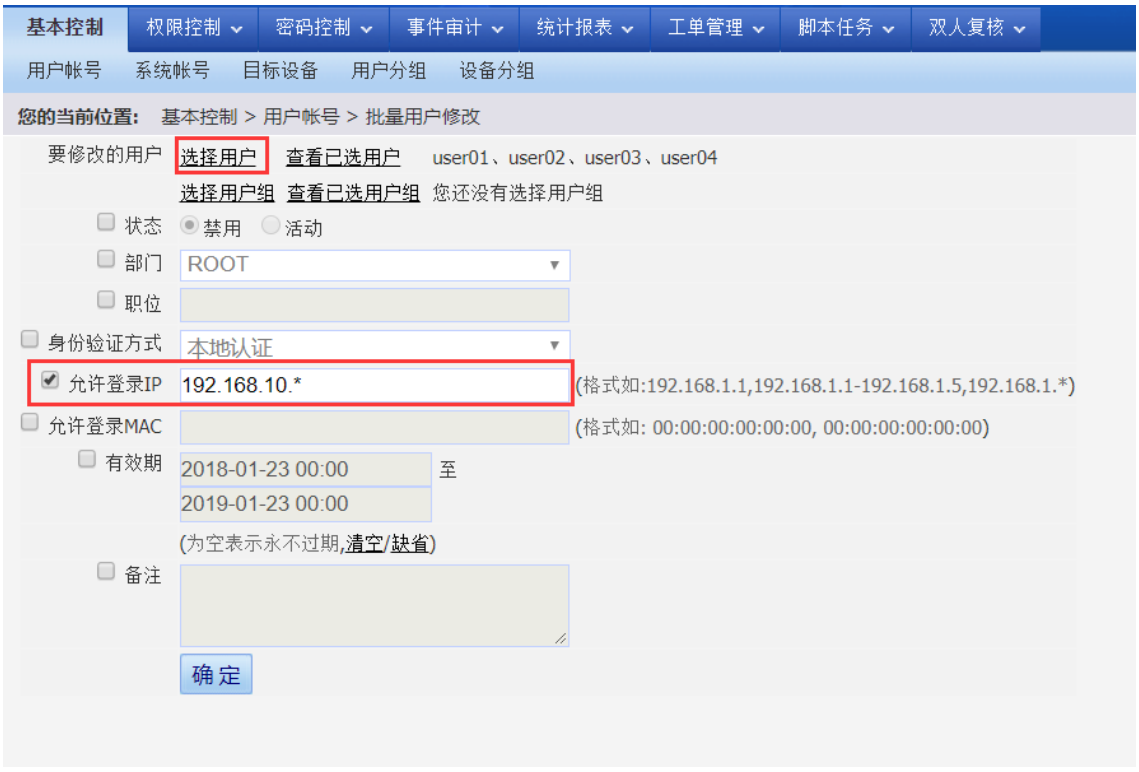
进入用户账号批量修改界面，如下图所示。

图3-18 批量修改示意图



选择需要修改的用户或用户组，在状态、部门、职位、身份验证方式、允许登录 IP、有效期、备注中勾选需要修改的选项，编辑相关信息，如下图所示。

图3-19 批量修改用户示意图



相关信息设置完成后，点击“确定”按钮完成用户修改操作，如下图所示。

图3-20 批量修改成功示意图

3.2.4 导出用户

1. 用户信息过滤

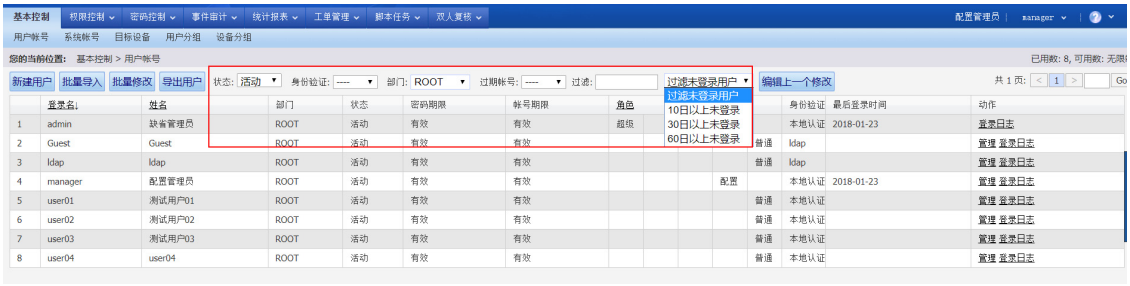
用户信息过滤可以帮助配置管理员快速过滤用户信息，查找相关用户。

堡垒机支持以下方式过滤用户信息：

- 用户状态：活动、禁用
- 用户所属部门
- 关键字
- 登录信息过滤

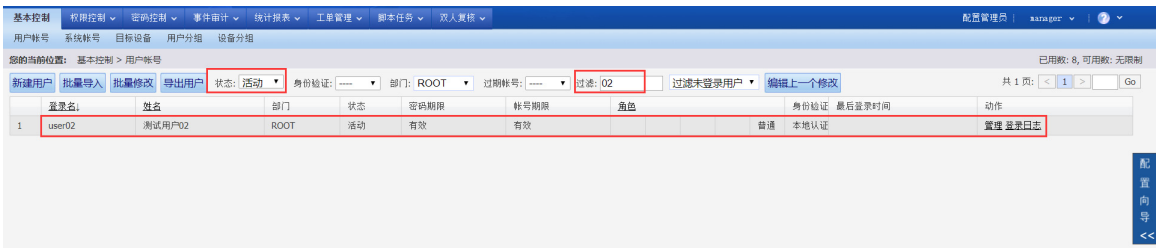
配置管理员可通过“基本控制 > 用户账号”页面，在工具栏处进行用户信息过滤操作，如下图所示。

图3-21 用户信息过滤示意图



堡垒机支持多条件组合过滤。例如：在状态为“活动”的用户列表中查找登录名、姓名、邮箱等信息中包含 02 的用户，如下图所示。

图3-22 多条件组合过滤示意图

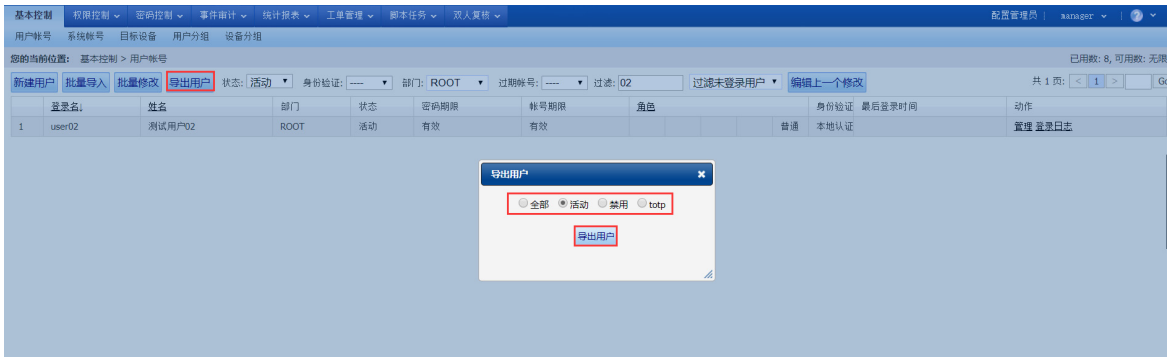


2. 用户信息导出

配置管理员可以通过以下两种方式导出用户帐号：

(1) 在“基本控制 > 用户账号 > 导出用户”页面导出用户账号，用户可根据实际情况选择相应导出方式，如下图所示。

图3-23 用户信息导出示意图



点击“导出用户”按钮后，堡垒机将以 excel 表格方式将用户信息导出到本地。

(2) 在“统计报表 > 配置报表”页面导出用户账号

在“用户信息”处点击“导出”按钮，将用户信息导出到相应 xls 文件中。

图3-24 用户信息导出示意图

3.3 目标设备管理

在堡垒机中被管理的设备统称为目标设备。配置管理员可以在“基本控制>目标设备”中添加和管理目标设备。添加和管理目标设备是配置管理员最重要的任务之一，本章将详细介绍如何添加及管理目标设备。

3.3.1 添加目标设备

为了让配置管理员快速掌握目标设备的创建流程，本章节以添加 windows 设备为例，介绍创建设备的通用流程。如果您是首次使用堡垒机，建议详细阅读此章节。

在创建目标设备前，建议按照以下表格收集待添加设备的信息

设备名	设备类型	IP 地址	简要说明	系统账号/密码	协议/端口
Windowsdemo	Microsoft Windows	192.168.10.164	Windows测试设备	Administrator/123!@#	rdp

信息收集完成后通过以下流程创建目标设备：填写设备信息 > 添加和设置服务 > 设置系统账号及密码（可选），具体操作如下：

(1) 填写设备信息

菜单位置：基本控制 > 目标设备 > 新建

在新建设备页面处填写相关设备信息，如下图所示。

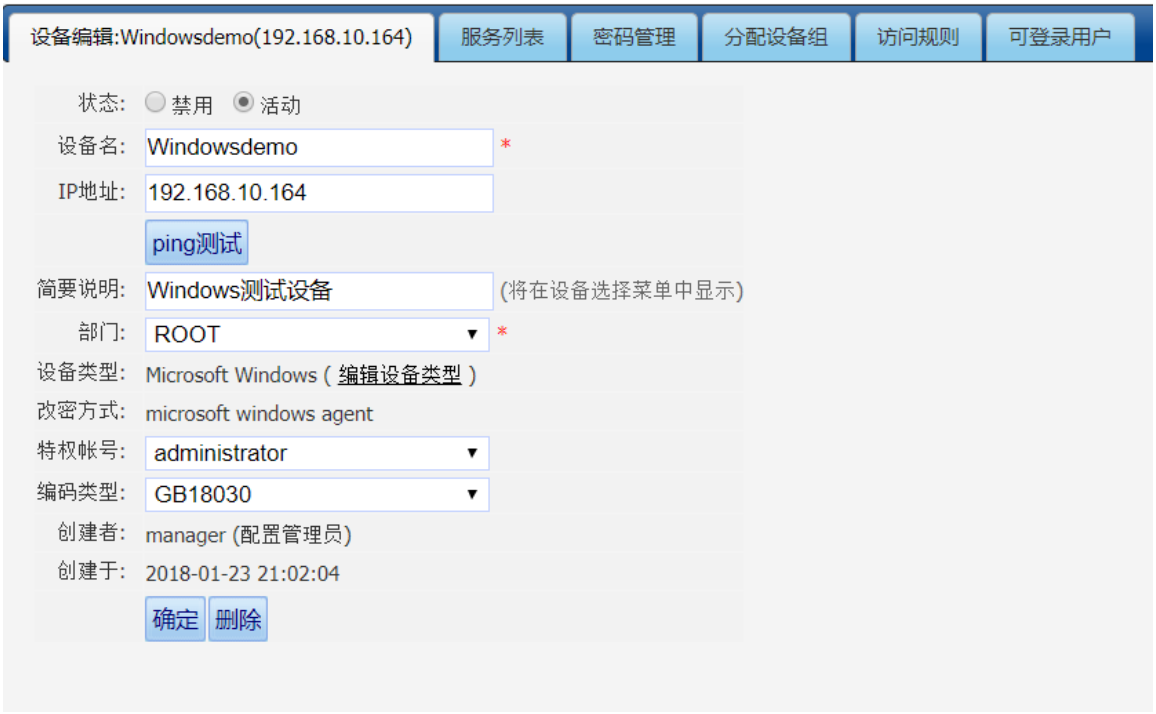
图3-25 新建目标设备示意图

参数解释：

- 状态：设备在堡垒机中的状态，默认为活动，处于禁止状态的设备将无法访问并且不占用设备授权数；
- 设备名：设备命名（必填），1-200 个字符，可以输入英文，数字和.-_。
- IP 地址：填写 IPV4 格式的地址。点击“ping 测试”按钮可以对 IP 是否连通进行检测。
- 简要说明：填写设备用途，可使用中文。
- 设备类型：下拉选择目标设备的设备类型
- 编码类型：设置该设备的字符编码类型，堡垒机使用该编码作为审计管理员查看该设备字符会话日志时的默认字符编码。在您选择设备类型时堡垒机会自动选择该值，因此如果没有特别需要建议保持默认值。

确认相关信息后，点击“确定”按钮完成目标设备基本信息的设置进入设备编辑页面，如下图所示。

图3-26 目标设备编辑页面



参数解释：

- 服务列表：添加和管理设备的服务(协议)
- 密码管理：设置和管理目标设备的系统帐号及密码
- 分配设置组：将该设备加入某个已经存在的设备组
- 访问规则：快速的将设备加入某个已经存在的访问规则
- 可登录用户：查看在堡垒机中可以访问该设备的用户帐号

设备基本信息创建完成后，需要设置用于访问的相关服务，具体操作如下：

(2) 添加和设置服务

在设备编辑页面，点击“服务列表”选项卡，如下图所示。

图3-27 添加服务示意图

堡垒机会根据您选择设备类型的常见访问方式自动添加服务（Microsoft Windows 类型设备默认创建 rdp 服务），如上图所示。

如果您需要的服务不存在，请在右上角选择相应服务点击“新增”按钮，如下图所示。

图3-28 新增服务示意图

添加需要的服务。如果列表中没有找到您需要的服务请参考超级管理员章节中“设备类型”为相应设备类型添加服务。

点击已经存在的服务右侧的“编辑”按钮，进入服务编辑页面，可对当前服务进行编辑，如下图所示。

图3-29 编辑服务示意图

参数解释：

- 状态：表示当前服务是否可用，默认为活动状态。
- 名称：指服务名称，除了 rdpapp 服务外，我们不建议修改服务名称，所以一般保持默认值即可。
- RDP 端口：服务端口，堡垒机会自动填写常见服务的默认端口；点击“连通检测”按钮可以对端口是否连通进行检测。
- 协议选项：设置是否允许使用 RDP 的客户端磁盘映射和 console 模式功能。关于 console 模式请参考“服务管理”章节中的“RDP”部分。

- 应用发布服务器：用于指定 windows 服务器是否为应用发布服务器，默认情况不勾选此选项，具体配置可参照《应用发布配置手册》。
- 剪切板：用于控制 windows 图形会话中剪切板的操作，上行是指由客户端到目标服务器复制粘贴的操作，下行是指由目标服务器到客户端复制粘贴操作。
- 服务图标：点击可以修改服务在普通用户设备访问页面中的显示图标。

正常情况下，对于 RDP、Telnet、ftp 服务采用默认值即可，其他协议的添加说明及注意事项，请参考后续章节中对各种服务的参数的介绍。

完成以上设置后，如果还需使用堡垒机的密码代填功能以便实现自动登录目标设备的效果（单点登录），那么请继续完成“密码托管”的配置。

(3) 设置系统账号及密码（可选）

在设备编辑页面点击“密码管理”选项卡，如下图所示。

图3-30 设置系统账号及密码示意图

在系统账号列表处查看是否有登录该目标设备所需的系统账号，如果没有则点击页面中“新建系统账号”按钮创建相应系统账号，如下图。

图3-31 新建系统账号示意图

在密码管理页面中点击相应账号右侧“新建”按钮，为该账号关联密码，如下图所示。

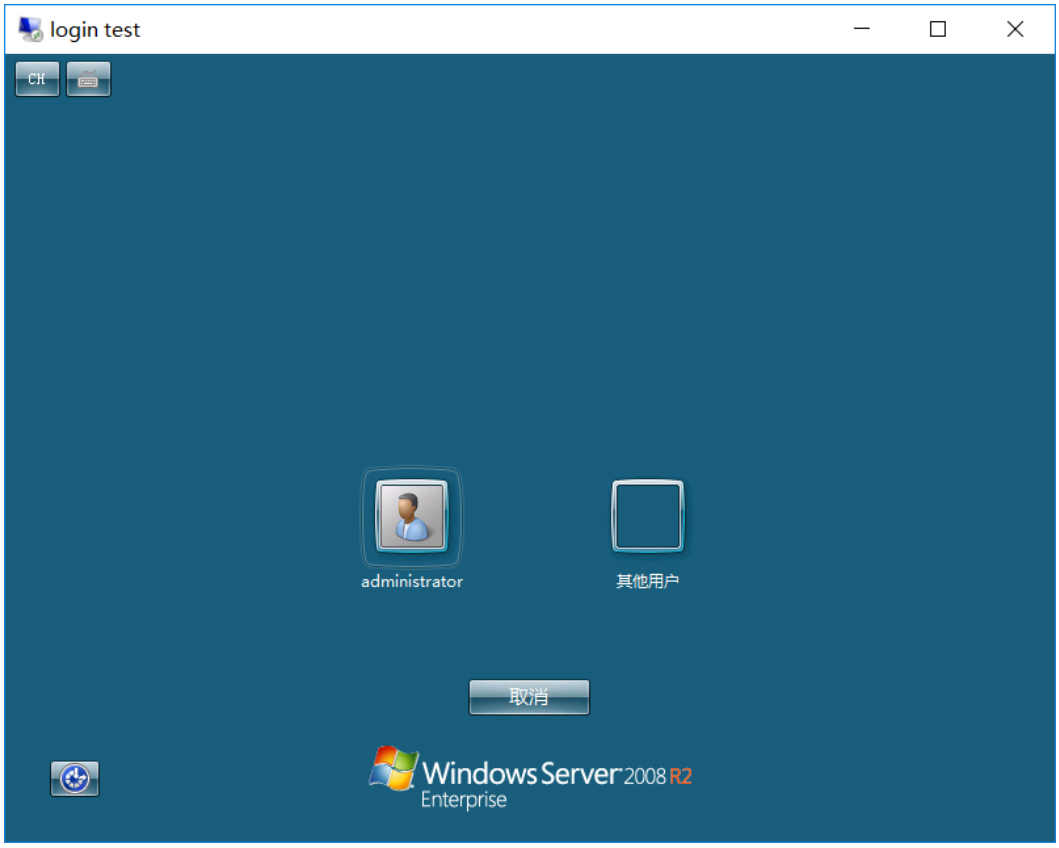
图3-32 关联系统账号密码示意图

在设置密码和确认密码中连续输入该系统帐号的密码，如果登录此 windows 服务器需要使用 AD 域系统账号，请在 domain 中输入 AD 域名称，完成后点击“确定”按钮，如下图所示。

图3-33 添加用户账号密码示意图

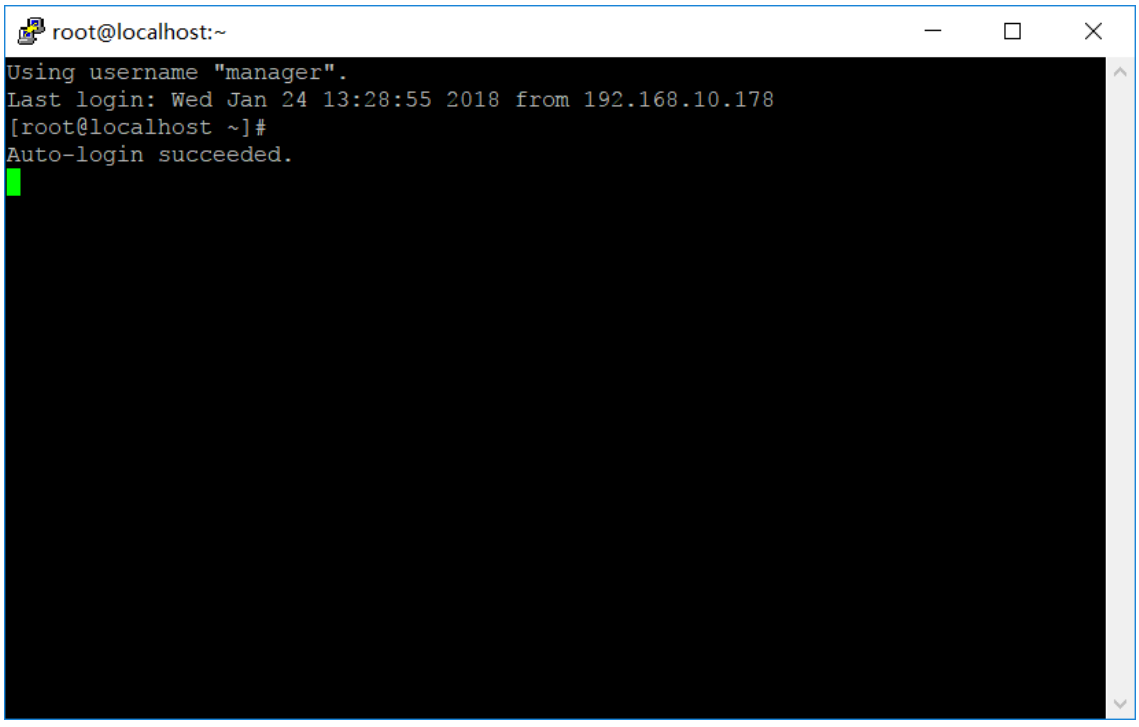
密码设置完成后，请务必在左上角选择相应的服务，然后点击已设置密码的系统帐号右侧的“登录测试”按钮进行一次登录测试。其中 RDP 服务请务必保证堡垒机可以成功登录到该设备，如果账户密码正确，系统会返回相应目标设备桌面，此界面无法操作，仅供管理员参考，如下图所示。

图3-34 RDP 服务登录测试



Telnet 和 SSH 服务请务必保证可以成功返回“Auto-login Succeeded”

图3-35 Telnet 和 SSH 服务登录测试



注意

登录测试需要管理主机安装 JAVA，如未安装可通过点击问号菜单下拉列表中工具下载处获得。

3.3.2 新建设备及服务

本章节介绍针对不同设备类型中各服务的创建及设置方式。

1. 设备类型简介

因为不同类型设备在访问协议、登录方式、改密方式上的差异很大，为了便于管理和快速添加设备，堡垒机根据设备的操作系统对设备进行分类，配置管理员在添加设备时可以通过选择预定义的设备类型快速添加设备。如下图所示。

图3-36 预定义的设备类型

不同的设备类型在默认服务、特权帐号、改密方式等方面均有所差异，因此您在添加设备时请务必选择正确的设备类型。

堡垒机中默认包含 10 种设备类型，下表中对相关类型进行了简要说明

表3-1 堡垒机中默认包含 10 种设备类型说明

编号	类型名称	分类	说明
1	General Linux	linux	适用于所有Linux版本
2	General Network	network	适用于Cisco、huawei以外其他类型网络设备
3	Cisco IOS Device	network	适用于运行IOS的Cisco或其他CLI兼容设备
4	Cisco CatOS Device	network	适用于运行CatOS的Cisco或其他CLI兼容设备
5	Huawei Quidway Device	network	适用于Huawei及其他CLI兼容设备
6	H3C Comware Device	network	适用于H3C及其他CLI兼容设备
7	HP UX	unix	适用于HP UX

编号	类型名称	分类	说明
8	IBM AIX	unix	适用于IBM AIX
9	General Unix	unix	适用于所有Unix-like设备
10	Microsoft Windows	Windows	适用于Windows 2003、2008等Windows设备

除了以上堡垒机中内置的设备类型，超级管理员也可以自定义设备类型，一般我们不建议用户自己修改和添加设备类型，出现下列情况时需要以超级管理员权限修改默认的设备类型：

(1) 为某个设备类型添加服务

(2) 修改某个设备类型的默认服务

(3) 修改某个设备类型的默认服务选项（如修改服务端口、服务参数等）

(4) 修改特权账号

(5) 修改设备改密方式

具体情况请参考超级管理员配置章节。

3.3.3 目标设备服务简介

在堡垒机中我们将访问目标设备的协议称为服务，比如 RDP、telnet、ssh 等

下表包含了所有堡垒机支持的服务及兼容性说明：

表3-2 堡垒机支持的服务及兼容性

类型	服务	协议（标准）	兼容性说明
字符终端	telnet	RFC854	
	ssh	SSH v1 v2	支持keyboard-interactive、password、publickey
图形会话	tn5250	IBM 5250	支持iSeriesAccess工具的直接访问
	RDP	RDP v5 – v7	兼容Windows 2000到Windows 2008 R2全部版本的RDP
	VNC	RFB v3.3 v3.7 v3.8	兼容所有符合标准RFB协议的VNC服务端，如RealVNC Free Editon； 不兼容其他基于标准协议增强后的变种，如RealVNC Enterprise Edition等，如果要通过堡垒机访问这类VNC server必须关闭相关的非标准功能。
	RDPAPP	参考RDP协议，及堡垒机应用发布手册	BS和CS属于rdpapp
文件传输	sftp	参考ssh	支持password、publickey，不支持keyboard-interactive(部分版本的Solaris强制要求使用这种身份验证方式)
	ftp	RFC959 RFC2228 RFC2389	

不同类型的设备使用的协议一般不同，下表是堡垒机中设备默认服务和允许使用的服务类型清单：

表3-3 堡垒机中设备默认服务和允许使用的服务类型清单

设备类型	默认服务	可选字符服务	可选图形服务
General Linux	ssh vnc	ssh telnet	vnc
General Network	telnet	telnet ssh	rdpapp
Cisco IOS Device	telnet	telnet ssh	rdpapp
Cisco CatOS Device	telnet	telnet ssh	rdpapp
Huawei Quidway Device	telnet	telnet ssh	rdpapp
H3C Comware Device	telnet	telnet ssh	rdpapp
HP UX	telnet vnc	telnet ssh	vnc
IBM AIX	telnet vnc	telnet ssh	vnc
General Unix	telnet vnc	telnet ssh	vnc
Microsoft Windows	rdp	telnet	rdp rdpapp

上表中描述的是堡垒机中内置的设备类型与对应的服务，超级管理员也可以自定义设备类型，具体设置请参照超级管理员配置。

1. 创建目标设备

目标设备基本信息包含：设备名、IP 地址、部门、设备类型、编码类型五种基本属性，不同类型设备的“设备类型”属性不同，在创建目标设备时需要根据实际情况进行选择，其他属性为通用选项，创建目标设备操作如下

菜单位置：基本控制 > 目标设备 > 新建

在设备新建页面填写设备基本信息，如下图所示。

图3-37 目标设备基本信息示意图

选择相应设备类型后点击“确定”按钮，完成设备基本信息的设置。

设备基本信息设置完成后，配置管理员可根据需求创建相应服务，后续章节将依次讲解不同类型服务设置方式。

2. RDP服务

(1) 服务简介

堡垒机支持 Windows 的远程桌面（RDP）服务。

RDP 的默认通讯端口为 TCP 3389 请保证堡垒机可以访问目标设备此端口。

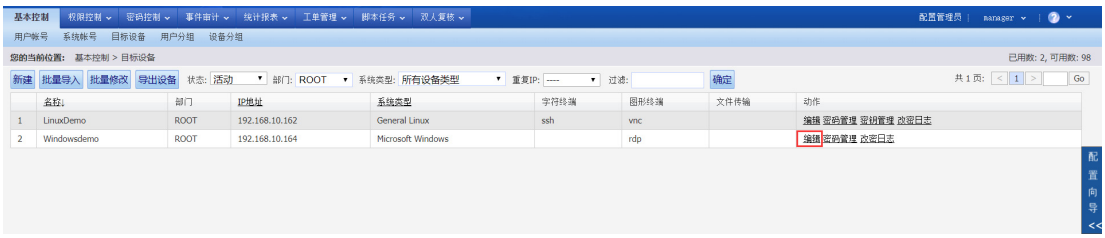
(2) 服务配置

堡垒机中部分类型（如 Microsoft Windows）设备在创建时会自动添加 RDP 服务，只需点击相应服务处“编辑”按钮即可对该服务进行设置。

配置管理员也可以通过以下操作创建此服务：

(3) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-38 目标设备编辑页面示意图



(4) 在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 RDP 服务，点击“新增”按钮，创建此服务，如下图所示。

图3-39 新增 DRP 服务示意图

下图为 RDP 服务在堡垒机中配置界面。

图3-40 RDP 服务配置界面示意图

参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。
- 名称：默认为 rdp，可以自行更改为其他认知名词。
- RDP 端口：RDP 服务的端口，默认为 3389；可以点击“联通检测”按钮进行端口联通测试
- 协议选项：设置普通用户通过堡垒机访问目标设备时是否允许使用下列功能
  - 客户磁盘映射：可以将本地客户端上的磁盘映射到对应的服务器上。
  - Console 模式：相当于 mstsc 的/console 或者/admin 选项，表示是否允许普通用户连接终端服务器的控制台会话（session id=0），用于防止终端服务器授权的会话超过后管理员无法登录目标设备。
- 应用发布服务器：指定相应 windows 服务器为应用发布服务器，具体设置请参照《应用发布配置手册》。
- 剪切板：设置普通用户通过堡垒机访问目标设备时是否允许使用剪切板上行、下行操作。
- 服务图标：可点击进行修改或者上传替换。

配置管理员可以根据实际情况修改 RDP 服务中相关参数（如 RDP 端口），点击“确定”按钮后完成服务的编辑，如果你想实现基于 RDP 服务的自动登录，请在设备编辑页面“密码管理”选项卡中为相应账号设置密码。

3. VNC服务

(1) 服务简介

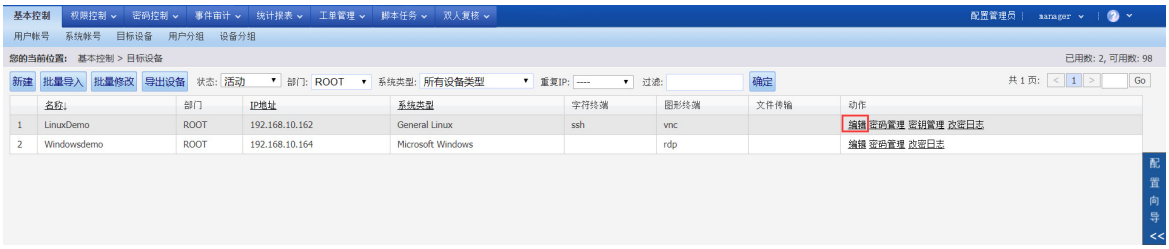
VNC（virtual network computing）,是一种由 AT&T 开发的远程控制的技术，可实现跨平台的远程控制操作。

(2) 服务配置

堡垒机中设备默认图形会话均不包含 VNC 服务，配置管理员可以通过以下操作创建此服务：

(3) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-41 目标设备编辑页面示意图



(4) 在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 VNC 服务，点击“新增”按钮，创建此服务，如下图所示。

图3-42 新增 VNC 服务示意图

如果下拉列表中不存在 VNC 服务，则需要超级管理员为该设备类型添加 VNC 服务。

下图为 VNC 服务在堡垒机中配置界面。

图3-43 VNC 服务配置界面示意图

参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。
- 名称：默认为 vnc，可以自行更改为其他认知名词。
- VNC 端口：一般为 5900，也可以在 5900-5999 之间，例如:5900、5901 等。如果访问目标设备时的 Server 直接填写 IP 地址，目标设备端口一般为 5900，如果服务地址为“IP 地址:1 到 2 位的数字”实际的端口为“5900+数字”，例如，server 为 192.168.5.1:1，那么对应的端口为 5901。
- VNC 密码：设置 VNC 访问密码。
- VNC 商业版：当服务端版本为商业版时勾选此项设置。
- 服务图标：可点击进行修改或者上传替换。

配置管理员可以根据实际情况修改 VNC 服务中相关参数，点击“确定”按钮后完成服务的编辑创建，若目标系统未做过更改推荐使用默认配置。

4. SSH服务

(1) 服务简介

SSH 是 Secure Shell 的简称，是一种字符终端服务，但是因为使用加密通信因此更加安全。SSH 目前已经广泛用于各种 Unix-like 类和网络设备中，其默认的通讯端口为 TCP 22。

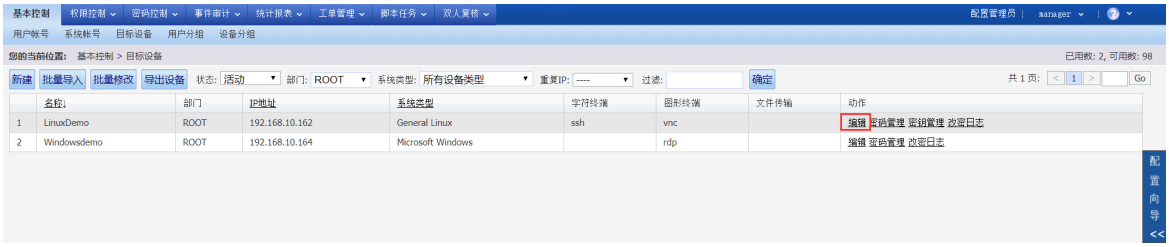
(2) 服务配置

堡垒机中部分设备类型（如 General Linux）在创建时会自动添加 SSH 服务，只需点击相应服务“编辑”按钮即可对该服务进行设置。

配置管理员可以通过以下操作创建此服务：

(3) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-44 目标设备编辑页面示意图



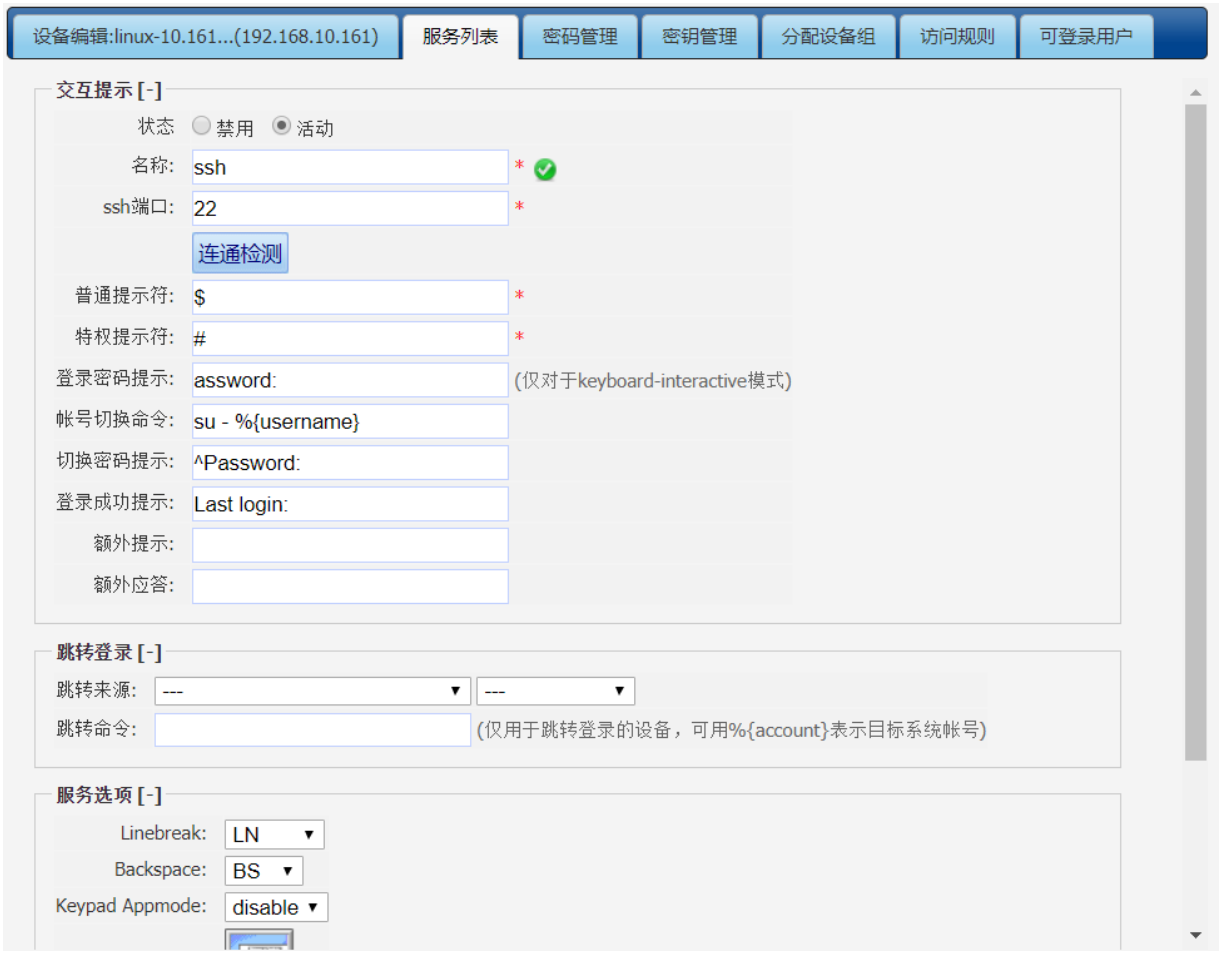
(4) 在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 SSH 服务，点击“新增”按钮，创建此服务，如下图所示。

图3-45 新增 SSH 服务示意图

如果下拉列表中不存在 SSH 服务，则需要超级管理员为该设备类型添加 SSH 服务。

下图为 SSH 服务在堡垒机中配置界面。

图3-46 SSH 服务配置界面示意图



参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。
- 名称：默认为 ssh，可以自行更改为其他认知名词。
- ssh 端口：默认为 22，根据目标设备实际端口情况更改。
- 普通提示符：设置普通用户的命令行提示符，如 Linux 常见的$。
- 特权提示符：设置特权帐号的命令行提示符,如 Linux 常见的#。
- 帐号切换命令：帐号身份切换的命令，如 Linux 中的 su – root。
- 切换密码提示：进行身份切换时的密码输入提示。
- 登录名提示：用于匹配连接目标设备时，目标设备要求输入用户名时的提示，如常见的 Username：、login：……。
- 登录密码提示：用于匹配连接目标设备时，目标设备要求输入密码时的提示，如常见的 Password：。
- 额外提示：用于匹配部分特殊设备在输入密码后返回登录提示符之前，要求用户进一步确认或者回答问题的提示，如 SCO Unix 在输入密码后会返回类似 TERM = (VT100)的提示要求用户确认终端类型。

- 额外应答：匹配到额外提示后的应答方式。仅设置额外提示，额外应答留空，出现额外提示后堡垒机将直接回车。

以上所有提示符均可以使用“^”和“$”限制提示符的开始和结束范围，比如^login:表示必须以 login：开始，前面不能有任何其他字符。允许使用“*”号作为通配符。

- 跳转来源：堡垒机无法直接访问的设备可以通过选择跳转来源 IP 和帐号，堡垒机通过跳转来源访问最终的设备。作为跳转来源的目标设备和帐号在堡垒机中必须可以通过 telnet 或者 ssh 协议成功登录；
- 跳转命令：在跳转来源上执行的用于访问最终设备的命令，如常见的：telnet %{account}@192.168.5.1 ssh %{account}@192.168.5.1；
- Linebreak：设置目标设备的换行符，错误的换行符可能导致无法正确的匹配各种提示符或者发送错误的回车符。可选值包括:LN、CR LN 和 CR；
- Backspace：定义字符终端的删除键映射，如果普通用户通过堡垒机访问目标设备的 telnet 服务时无法删除已输入的字符，可以尝试修改该值。可以选择值包括：BS 和 DEL，分别表示 Backspace 和 DELETE；
- Keypad Appmode：设置通过堡垒机的设备访问页面启动 jterm、putty、SecureCRT 等终端工具时是否开启小键盘的应用程序模式（Keypad Appcation Mode），默认为 disable，表示使用数字键盘模式。选择 enable 表示启用小键盘的应用程序模式，启用后当用户按下键盘上数字键后堡垒机将替代数字键向目标设备上的应用程序发送 3byte 的转义字符串，例如小键盘上 1 将被替代为<Esc>Oq，对转义序列的处理和响应会因为打开的应用程序不同而不同，某些应用的某些功能可能需要使用这种模式。一般情况下建议保持默认的 disable 状态，否则将无法使用小键盘输入数字。（该选项在部分版本中修改后实际取值依然为 disable）。

配置管理员可以根据实际情况修改 SSH 服务中相关参数，点击“确定”按钮后完成服务的编辑创建。

5. TELNET服务

(1) 服务简介

Telnet 是字符终端服务之一，主要用于网络设备、各种带外管理口和较老的 Unix、Linux 设备中，默认的通信端口为 TCP 23。

堡垒机通过匹配预设的各种提示符进行自动应答，从而实现 telnet 的自动登录。

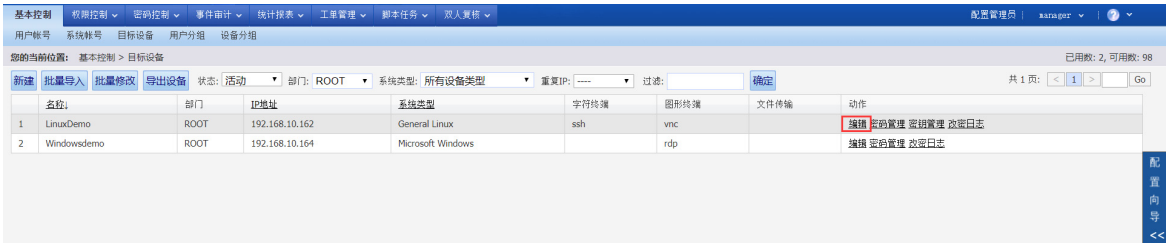
(2) 服务配置

堡垒机中部分设备类型（如 Cisco CatOS Device）在创建时会自动添加 TELNET 服务，只需点击相应服务“编辑”按钮即可对该服务进行设置。

配置管理员可以通过以下操作创建此服务：

(3) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-47 目标设备编辑页面示意图

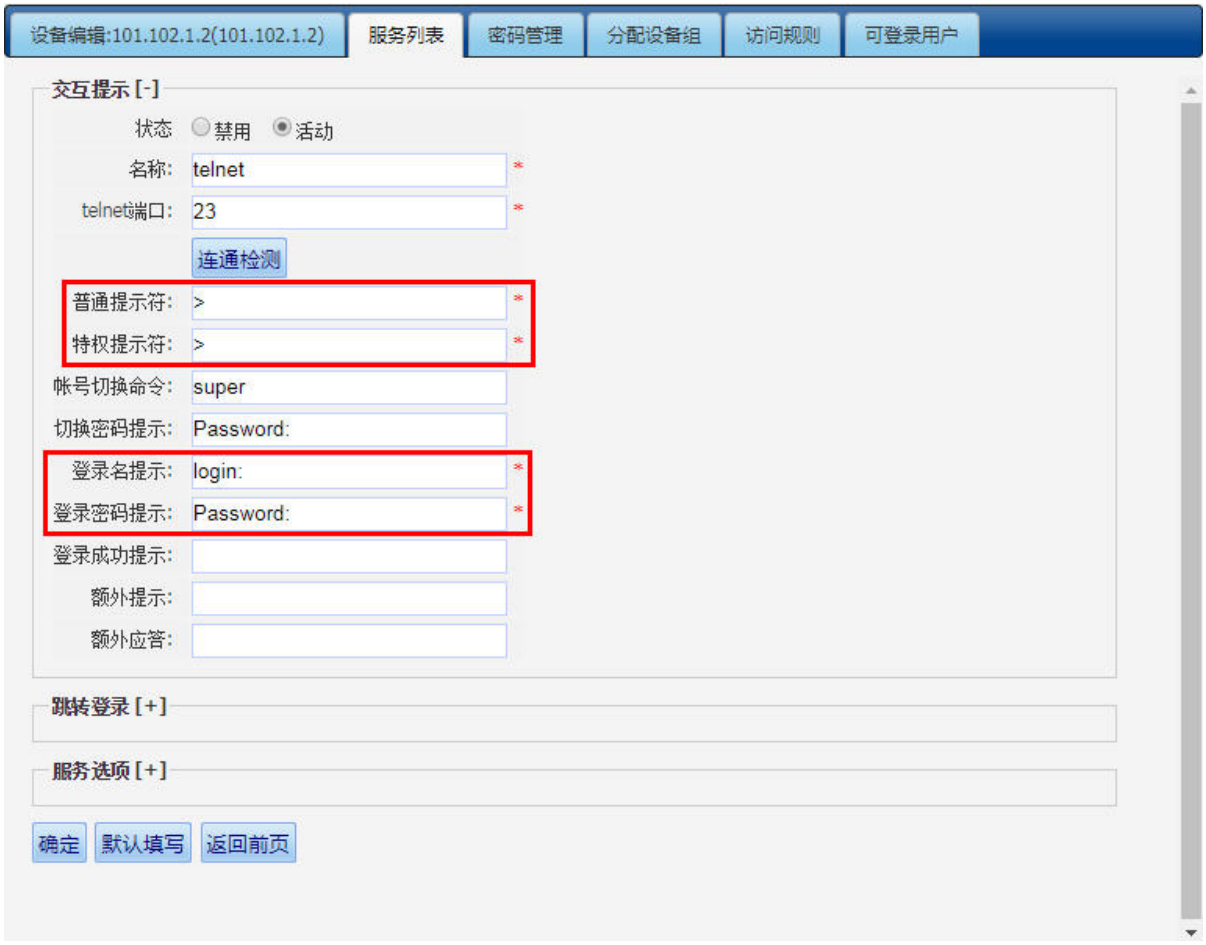


(4) 在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 TELNET 服务，点击“新增”按钮，创建此服务，如下图所示。

图3-48 新增 TELNET 服务示意图

如果在服务列表中不存在 TELNET 服务，则需要需要超级管理员为该设备类型添加 TELNET 服务。下图为 TELNET 服务在堡垒机中配置界面。

图3-49 TELNET 服务配置界面示意图



参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。
- 名称：默认为 telnet，可以自行更改为其他认知名词。
- telnet 端口：默认为 23，根据目标设备实际端口情况更改。
- 普通提示符：设置普通用户的命令行提示符，如常见的>。
- 特权提示符：设置特权帐号的命令行提示符,如常见的>。
- 帐号切换命令：帐号身份切换的命令。
- 切换密码提示：进行身份切换时的密码输入提示。
- 登录名提示：用于匹配连接目标设备时，目标设备要求输入用户名时的提示，如常见的 login:、Username:、……。
- 登录密码提示：用于匹配连接目标设备时，目标设备要求输入密码时的提示，如常见的 Password:。
- 额外提示：用于匹配部分特殊设备在输入密码后返回登录提示符之前，要求用户进一步确认或者回答问题的提示，如 SCO Unix 在输入密码后会返回类似 TERM = (VT100)的提示要求用户确认终端类型。

- 额外应答：匹配到额外提示后的应答方式。仅设置额外提示，额外应答留空，出现额外提示后堡垒机将直接回车。

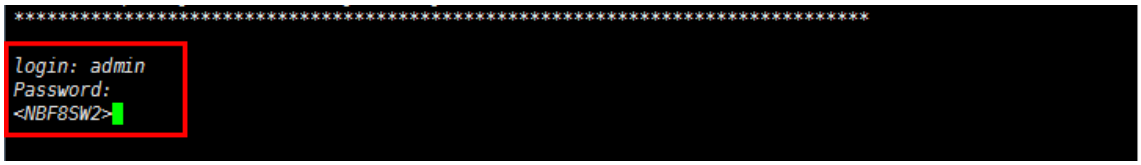
以上所有提示符均可以使用“^”和“$”限制提示符的开始和结束范围，比如“^login:”表示必须以“login:”开始，前面不能有任何其他字符。允许使用“*”号作为通配符。

- 跳转来源：堡垒机无法直接访问的设备可以通过选择跳转来源 IP 和帐号，堡垒机通过跳转来源访问最终的设备。作为跳转来源的目标设备和帐号在堡垒机中必须可以通过 telnet 或者 ssh 协议成功登录；
- 跳转命令：在跳转来源上执行的用于访问最终设备的命令，如常见的：telnet %{account}@192.168.5.1 ssh %{account}@192.168.5.1。

配置管理员可以根据实际情况修改 TELNET 服务中相关参数，点击“确定”按钮后完成服务的编辑创建。

提示

普通提示符、特权提示符、登录名提示和登录密码提示可根据直接连接设备时弹出的提示符填写，如 PC 直接 telnet 到交换机上，可发现登录名提示为 login:，登录密码提示为 Password:，普通提示符为>，若设置 admin 为特权用户，则特权提示符为>。

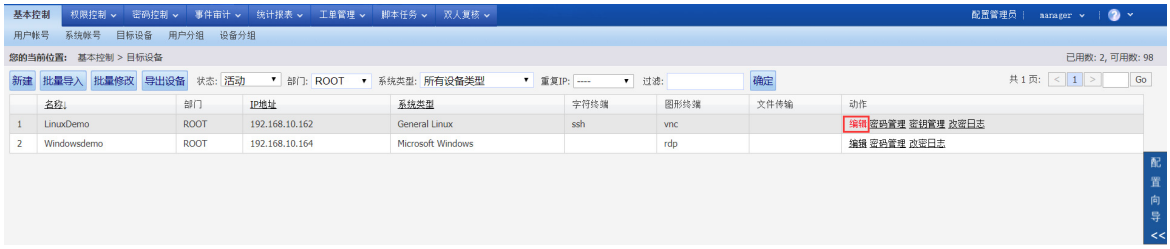


6. FTP服务配置

配置管理员可以通过以下操作创建此服务：

(1) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-50 目标设备编辑页面示意图



(2) 在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 ftp 服务，点击“新增”按钮，创建此服务，如下图所示

图3-51 新增 SSH 服务示意图

下图为 FTP 服务在堡垒机中配置界面。

图3-52 FTP 服务示意图

参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。
- 名称：默认为 ftp，可以自行更改为其他认知名词
- FTP 端口：文件传输连接端口，默认为 21，根据目标设备实际端口情况更改。
- 编码类型：目标设备的编码类型，根据实际情况填写。
- 模式：分为 active(主动模式)，passive(被动模式)。根据实际情况填写。
- 服务图标：可点击进行修改或者上传替换。

配置管理员可以根据实际情况修改 ftp 服务中相关参数（ftp 端口），点击“确定”按钮后完成服务的编辑创建，若目标系统未做过更改推荐使用默认配置。

7. SFTP服务配置

(1) 依次点击“基本控制 > 目标设备”，在相应设备处点击“编辑”按钮进入目标设备编辑页面，如下图所示。

图3-53　目标设备编辑页面示意图

(2)　在设备编辑页面，点击“服务列表”选项卡，在右上角下拉列表中选择 sftp 服务，点击“新增”按钮，创建此服务，如下图所示。

图3-54 新增 SFTP 服务示意图

下图为 SFTP 服务在堡垒机中配置界面。

图3-55 SFTP 服务示意图

参数解释：

- 状态：服务状态，默认为活动，由于审计的要求，访问过的服务不能删除，可以使用禁用。

- 名称：默认为 sftp，可以自行更改为其他认知名词
- 编码类型：目标设备的编码类型，根据实际情况填写。
- SFTP 端口：文件传输连接端口，默认为 22,与 ssh 使用的同一端口，根据目标设备实际端口情况更改。
- 服务图标：可点击进行修改或者上传替换。

配置管理员可以根据实际情况修改 sftp 服务中相关参数，点击“确定”按钮后完成服务的编辑创建，若目标系统未做过更改推荐使用默认配置。

注意

sftp 依赖于 ssh 服务，因此必须确保相应目标设备上创建了 ssh 服务。

3.3.4 设备批量导入

菜单位置：基本控制 > 目标设备 > 批量导入

配置管理员可以通过批量导入的方式快速添加多个目标设备。

进入设备批量导入配置界面，如下图所示。

图3-56 设备批量导入示意图

堡垒机支持以下三种方式批量导入目标设备：

- 外部导入（默认的批量导入方式）
- 自动填写
- 逐个填写

不同方式间可通过点击相应单选按钮进行切换，在后续章节中将逐一介绍三种方式批量导入目标设备方法。

1. 外部导入

外部导入是指通过 excel 文件将相关目标设备信息导入到堡垒机中，因此操作前必须确保管理主机已安装相关 office 应用程序，用于编辑相关 excel 模板文件。

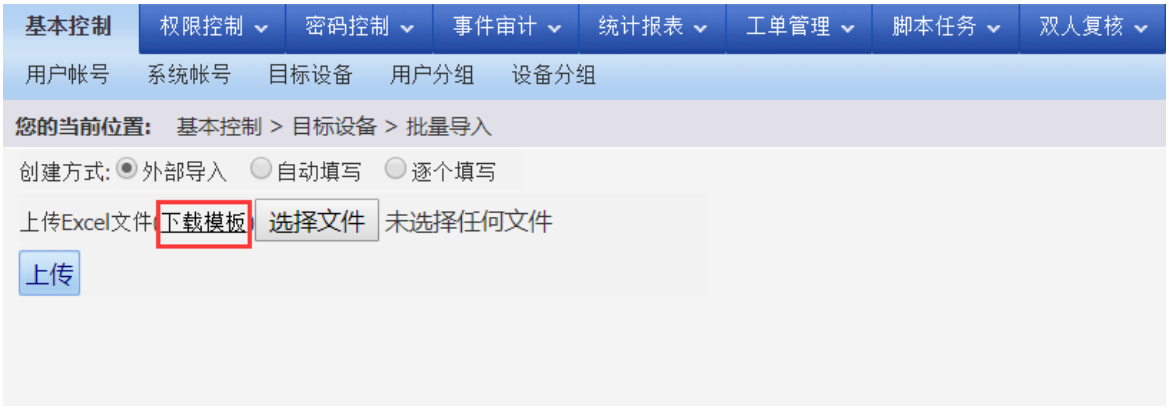
外部导入具体操作方法如下：

(1)　下载模板文件

菜单位置：基本控制 > 目标设备 > 批量导入

确保批量新增用户方式为“外部导入”，点击页面中“下载模板”获取模板文件，如下图所示。

图3-57 下载模板文件示意图



(2)　填写模板文件

打开模板文件 servers.xls 填写相关设备信息，如下图所示。

图3-58 填写模板文件图

	A	B	C	D	E	F	G	H	I
1	设备名	设备类型	IP地址	设备分组	编码类型	简要说明	部门	systype-sample	encoding-sample
2	linux-10.161	General Linux	192.168.10.161	linux组	UTF-8	linux服务器1		General Unix	ISO-8859-1
3	linux-10.162	General Linux	192.168.10.162	linux组	UTF-8	linux服务器2		General Linux	GB18030
4	Windows-10.163	Microsoft Windows	192.168.10.163	Windows组	GB18030	Windows服务器1		General Network	US-ASCII
5	Windows-10.165	Microsoft Windows	192.168.10.165	Windows组	GB18030	Windows服务器2		Cisco IOS Device	UTF-8
6								Cisco CatOS Device	IBM1388
7								Huawei Quidway Device	
8								Microsoft Windows	
9								HP UX	
10								IBM AIX	
11								H3C Comware Device	

参数解释：

- 设备名：设备命名，只允许 1-200 个字母、英文、“.”、“-”、“_”的组合。
- 设备类型：由右边 systype-sample 项中选择对应的设备类型。
- IP 地址：填写 IPV4 格式的地址。
- 编码类型：由右边的 encoding-sample 项中选择相应的编码类型。
- 简要说明：可填写设备用途，可使用中文。
- 部门：默认为 ROOT，根据堡垒机中的部门进行更改。

注意

- 设备名、设备类型、IP 地址、编码类型为必填项，其他选项可留空。
- 设备名称不能为中文且不能重复。
- 表格中的 systype-sample 和 encoding-sample 仅方便表格的填写，填写完成后删除。

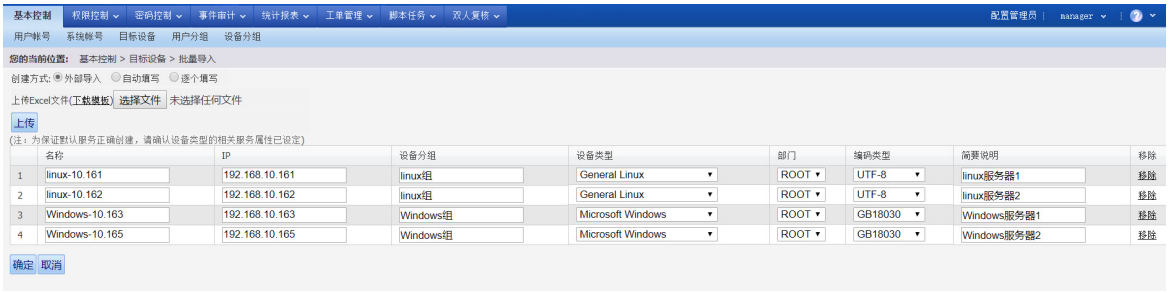
(3) 上传模板文件

点击“选择文件”按钮，选择相关模板文件，如下图所示。

图3-59 上传模板文件示意图

点击“上传”按钮，堡垒机将读取模板文件中相关设备信息，如下图所示。

图3-60 上传设备信息确认示意图



确认信息无误后，点击“确定”按钮完成目标设备的导入，如下图所示。

图3-61 批量添加设备成功示意图

2. 自动填写

自动填写是指堡垒机根据管理员设置的主机名前缀、编号及 IP 地址范围自动产生设备信息并导入堡垒机。具体使用方法如下

(1) 选择“自动填写”批量导入方式

菜单位置：基本控制 > 目标设备 > 批量导入

将批量新增设备方式为设置为“自动填写”。

(2) 填写自动生成的设备信息

在自动填写设置页面，填写相关信息，如下图所示。

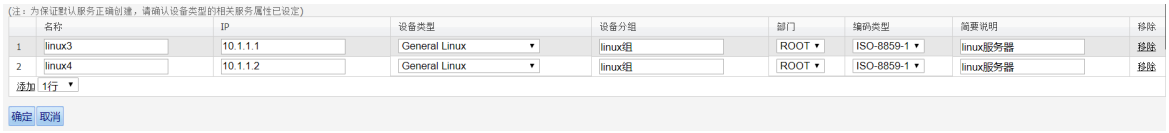
图3-62 自动填写配置示意图

参数解释：

- 名称前缀：指设备名前缀。
- 编号范围：设备名后缀编号。
- IP 范围：设备 IP 地址段。
- 简要说明：设备简要说明。

相关信息填写完成后，点击“自动填写”按钮，堡垒机会根据已填写的信息自动生成设备信息，如下图所示。

图3-63 自动填写确认示意图

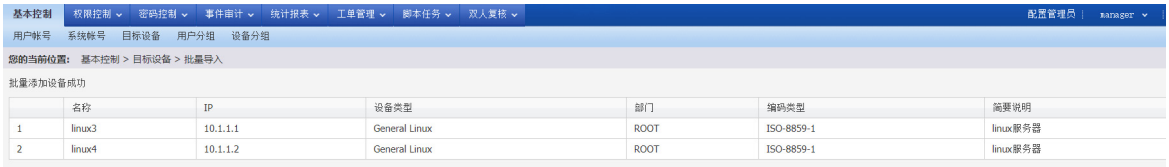


参数解释：

设备类型及编码类型如果不匹配，需要手动去选择。并可对其它相应信息进行修改。

点击“确定”按钮，完成设备信息的导入，如下图所示。

图3-64 自动填写完成示意图



3. 逐个填写

逐个填写是指配置管理员依次填写多个目标设备信息同时提交的批量导入方法，具体操作如下：

(1) 选择“逐个填写”批量导入方式

菜单位置：基本控制 > 目标设备 > 批量导入

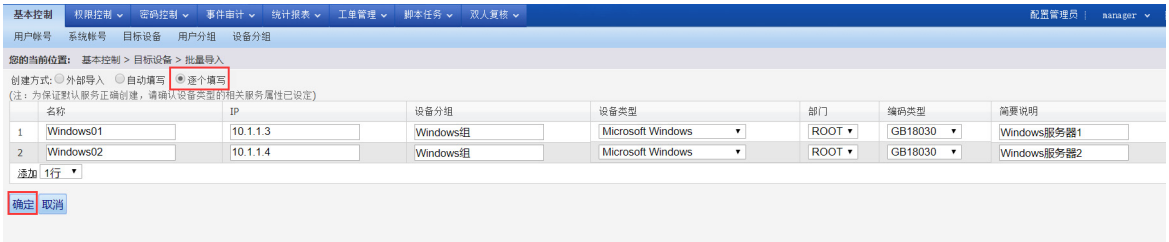
将批量新增设备方式设置为“逐个填写”。

(2) 填写设备信息

在设备表单处根据实际情况填写相关用户信息，“添加”按钮默认添加一行表单，如需添加多行，可在右侧下拉列表处选择相应行数后点击添加即可。

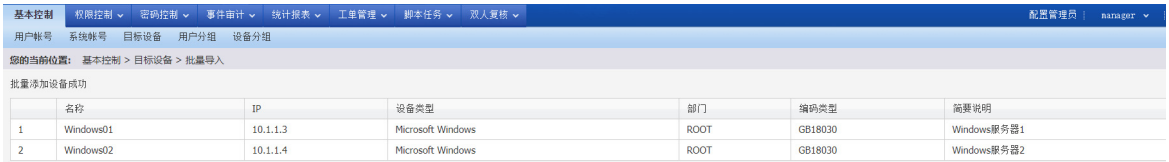
设备表单中名称为必填项，其他选项可根据实际情况选择填写，如下图所示。

图3-65 逐个填写目标设备示意图



确认无误后点击“确认”按钮完成批量导入，如下图所示

图3-66 逐个填写目标设备完成示意图



3.3.5 设备批量修改

通过设备批量修改功能，帮助管理员快速批量修改目标设备信息.

堡垒机支持批量修改目标设备以下三种属性：

- 基本信息
- 设备密码
- 服务

菜单位置：基本控制 > 目标设备 > 批量修改

进入设备批量修改界面，如下图所示。

图3-67 目标设备批量修改示意图

不同方式之间可通过点击相应选项卡进行切换，在后续章节中将逐一介绍三种方式批量修改设备方法。

1. 基本属性批量修改

堡垒机支持两种方式批量修改设备基本属性：

- 方式一：根据所选设备，通过当前页面直接修改设备状态、部门、设备类型、特权账号及编码类型等基本信息。
- 方式二：根据所选设备，生成包含待修改设备列表的 Excel 模板文件，对文件中设备信息进行编辑修改后重新导入到堡垒机中更新设备列表。

用户可根据实际情况选择设备修改方式，两种方式具体操作如下：

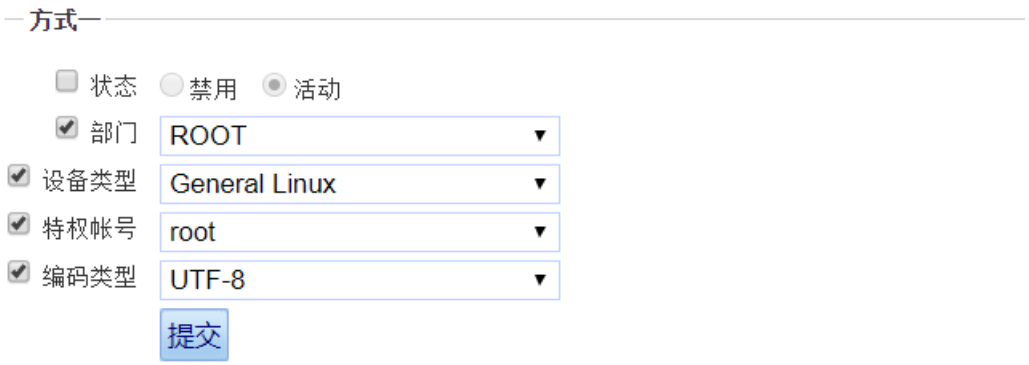
点击“选择设备”或“选择设备组”按钮，在设备列表中勾选需要修改的设备，如下图所示。

图3-68 选择要修改的目标设备示意图

(1) 方式一：

在状态、部门、设备类型、特权账号、编码类型中勾选需要修改的选项，编辑相关信息，如下图所示。

图3-69 方式一示意图



点击“提交”按钮完成设备修改，如下图所示。

图3-70 设备修改成功示意图

(2) 方式二：

点击“下载要修改的设备列表”按钮，将所选设备信息以 Excel 文件方式下载到本地，如下图所示。

图3-71 下载要修改的设备列表

打开下载的模板文件 server_edit.xls，修改相关设备信息，如下图所示。

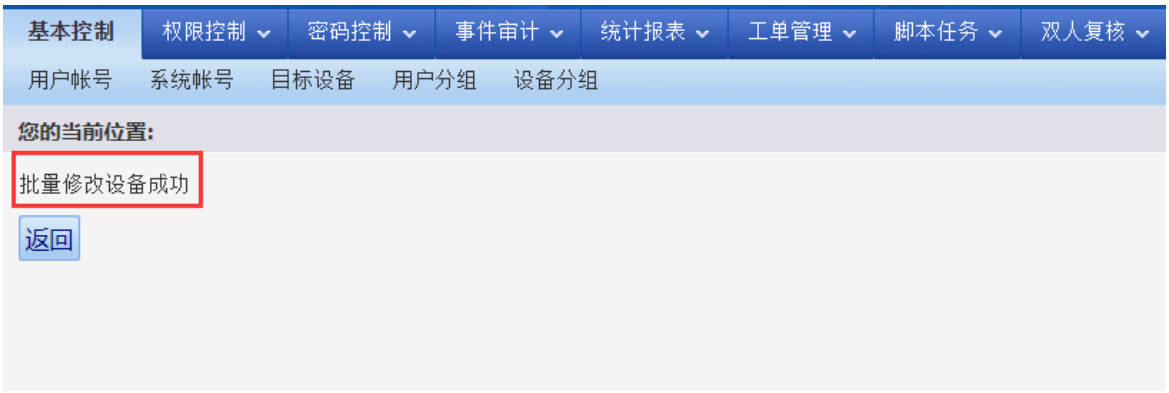
	A	B	C	D	E	F
1	设备名	新设备名	设备类型	IP地址	编码类型	简要说明
2	linux4		General Linux	10.1.1.2	UTF-8	linux服务器
3	linux-10.161		General Linux	192.168.10.161	UTF-8	linux服务器1
4	linux-10.162		General Linux	192.168.10.162	UTF-8	linux服务器2
5	linux3		General Linux	10.1.1.1	UTF-8	linux服务器

- 新设备名：只允许 1-200 个字母、英文、“.”、“-”、“_”的组合。
- 设备类型与编码类型可参照下表中进行修改

设备类型	编码类型
General Unix General Linux General Network Cisco IOS Device Cisco CatOS Device Huawei Quidway Device Microsoft Windows HP UX IBM AIX H3C Comware Device	ISO-8859-1 GB18030 US-ASCII UTF-8 IBM1388

点击“选择文件”按钮，选择编辑完成的模板文件后点击“上传并更新设备列表”，完成批量设备修改，如下图所示

图3-72 批量修改设备成功



2. 批量设置密码

“设置密码”可用于批量设置/清空目标设备系统账号的密码，具体使用方法如下：

(1) 设置批量修改方式为“设置密码”

菜单位置：基本控制 > 目标设备 > 批量修改

点击“设置密码”选项进入相应编辑页面，如下图所示。

图3-73 批量设置密码示意图

(2) 选择相应设备与系统账号

点击“选择设备”或“选择设备组”按钮，在设备列表中勾选相关设备，如下图所示

图3-74 选择设备或设备组示意图

设备关联完成后，点击“选择账号”按钮，在系统账号列表中勾选相应账号，如下图所示。

图3-75 选择账号示意图

(3) 设置批量修改方式

针对已选中的目标设备与相应账号，堡垒机支持以下两种方式对设备密码进行批量操作：

操作一：清空密码

“清空密码”用于擦除目标设备系统账号中已关联的密码。

点击页面中“清空设备密码”按钮，将会清空已选设备相应账号的密码，如下图所示。

图3-76 清空密码示意图

操作二：更新密码

“更新密码”用于批量设置所选目标设备相应系统账号的密码。

点击页面中“下载表格”按钮，下载相应模板文件，如下图所示。

图3-77 下载相应模板文件示意图

打开模板文件 server_password.xls 填写相关信息，如下图所示。

图3-78 模板文件信息示意图

	A	B	C	D	E	F	G
1	Server Name	Server Address	Account	Password	Domain	Su Account	Domain IP
2	linux4	10.1.1.2	root				
3	linux-10.161	192.168.10.161	root				
4	linux-10.162	192.168.10.162	root				
5	linux3	10.1.1.1	root				
6	linux4	10.1.1.2	test				
7	linux-10.161	192.168.10.161	test				
8	linux-10.162	192.168.10.162	test				
9	linux3	10.1.1.1	test				

参数解释：

- Domain：域信息，在域环境中需填写此项信息
- Su Account：设置切换账号，如 user 账户通过敲击 enable 命令切换到 enable 模式，则 enable 账号的 Su Account 账户为 user，user 账号需提前设置好相应密码。

点击“选择文件”按钮，选择编辑完成的模板文件后点击“上传表格”，完成密码的批量设置。

3. 批量创建服务

通过“批量创建服务”功能，可以帮助配置管理员针对同一类型的设备快速创建相同的服务，具体操作如下：

菜单位置：基本控制 > 目标设备 > 批量修改

在批量修改页面点击“创建服务”选项卡，如下图所示。

图3-79 批量创建服务示意图

参数解释：

- 设备类型：选择相应设备类型，指定类型后在选择设备处只显示匹配该类型的目标设备。
- 选择服务：选择需要创建的服务，该服务列表中只显示设备默认的服务，如果未找到需要的服务，请联系超级管理员为该设备类型添加相应服务。

选择相应设备及所要创建的服务如下图所示。

图3-80 选择相应设备及所要创建的服务示意图

勾选相应设备后点击“下一步”按钮进入服务创建页面，相应服务设置请查看目标设备管理中相关章节，在此不做赘述

点击“确定”后完成服务的批量创建

注意

- 名称不能与现有服务名相同；
- 如果选择的设备已有该协议的服务，会将后面的设置覆盖到该设备上第一个该协议的服务。

3.4 系统账号

在堡垒机中我们将登录目标设备所需要的帐号称为系统帐号，如 Unix 中的 root、Windows 中 administrator 等。

堡垒机内置了常见的系统帐号，如下表。

表3-4 堡垒机内置系统账号说明

系统帐号	性质	说明
administrator	常规	Windows设备默认的超级管理员帐号
any	特殊	表示允许普通用户使用任意帐号访问目标设备，一般用于不希望堡垒机代填系统帐号密码的情形
enable	特殊	用于cisco ios，表示执行enable，并自动输入enable的密码
null	特殊	一般用于cisco等网络设备，表示登录时只需要输入密码，不需要输入用户名
root	常规	Unix-like设备中的特权帐号，常用于Unix和Linux设备中

系统帐号	性质	说明
self	特殊	表示使用普通用户在堡垒机中的用户帐号名作为系统帐号，如果用户通过堡垒机的Web页面访问目标设备，通过将用户密码缓存在Web session中，堡垒机将自动采用用户登录堡垒机输入的密码作为系统帐号密码尝试自动登录目标设备

3.4.1 系统账号查看、新建、编辑

配置管理员可以通过依次点击“基本控制 > 系统账号”，在系统账号管理界面查看、新建、编辑系统账号，如下图所示。

图3-81 系统账号示意图

参数解释：

- 新建：建立新的系统帐号
- 编辑：编辑系统账号名称及简要说明
- 新建密钥：当设备采用 SSH 密钥方式登录时需要针对相关账号设置密钥信息。
- 访问规则：用于将相应系统账号与相关访问规则关联

1. 新建系统账号

如果在设备编辑页面给目标设备设置密码时发现没有需要的系统帐号，可以在此页面新建。具体操作如下：

点击“新建”按钮，如下图所示。

图3-82 新建系统账号示意图

在账号新建页面输入账号及相关说明，如下图所示。

图3-83 新建系统账号示意图

点击“确定”后完成系统账号的创建。

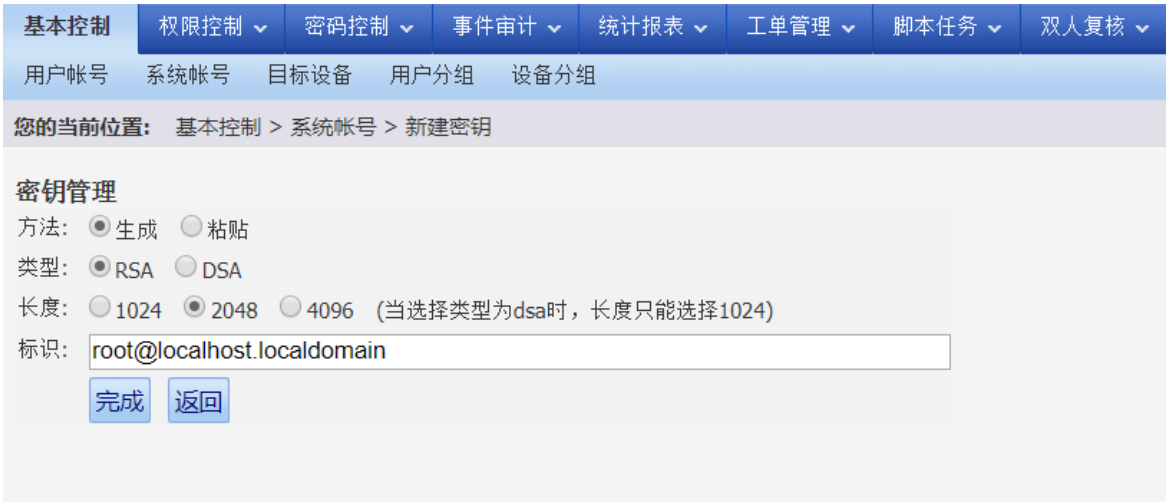
3.4.2 新建密钥

堡垒机中支持使用 SSH 公钥的方式进行登录目标设备的身份验证，具体操作如下：

(1) 为系统帐号创建 SSH 密钥

配置管理员依次点击“基本控制 > 系统帐号”，在系统账号管理界面，找到相应的帐号，点击“新建密钥”，进入密钥编辑页面，如下图所示。

图3-84 新建秘钥示意图



参数解释：

- 方法：选择密钥产生的方法，默认为生成表示堡垒机自动产生新的密钥。如果用户在堡垒机前已经拥有 OpenSSH 格式的密钥文件，也可以选择粘贴，将私钥文件导入堡垒机（导入前必须删除私钥的保护密码 passphrase）。
- 类型：选择新密钥的类型。
- 长度：选择密钥长度，密钥长度越长越安全。；

- 标识：设置密钥的标识，用于区分不同的密钥。

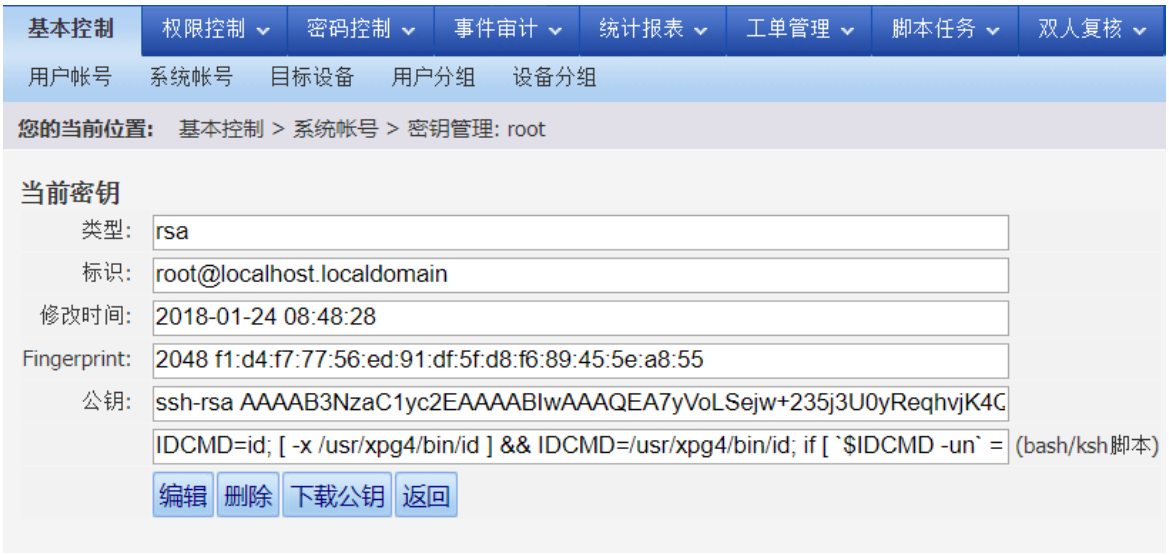
配置管理员可根据实际情况修改相关设置，建议除标识外保持默认即可，点击“完成”按钮完成密钥的创建，如下图所示

图3-85 新建秘钥完成示意图

(2) 密钥管理

在相应系统账号处点击“密钥管理”按钮，编辑当前密钥信息，如下图所示

图3-86 秘钥管理示意图



参数解释：

- Fingprint：为密钥的指纹信息。
- 公钥：第一行为公钥的内容，第二行为 Unix-like 设备中快速登记公钥的 shell 脚本。

注意

为了堡垒机安全不允许包括管理员在内的任何人查看系统帐号的私钥文件。

用户除了可以在“基本控制-系统帐号”中添加密钥外，还可以在目标设备的编辑页面中的密钥管理中为系统帐号添加密钥。前者为堡垒机上同名帐号的全局密钥，后者为单个设备独有密钥。

堡垒机在 ssh 登录时会优先考虑使用局部密钥，如果没有设置，将产生使用全局密钥，如果全局密钥登录失败，将尝试密码登录。

(3) 将公钥写入目标设备

将第一步中产生公钥写入目标设备的信任文件(authorized_keys，不同设备可能不同)。

- Unix-like 设备，可以使用相应帐号身份登录目标设备，将堡垒机系统帐号密钥管理页面公钥中的脚本复制后在目标设备上执行即可
- 非 Unix-like 类设备(如网络设备)，理论上你只要将堡垒机的公钥在设备上安装设备要求的方法进行登记即可。

(4) 密钥登录测试

类似密码登录测试，配置管理员可以在设备编辑页面的“密钥管理”中进行密钥登录测试，如下图所示。

图3-87 秘钥登录测试示意图

3.5 用户分组

为了便于批量管理，堡垒机允许配置管理员通过分组的方式对用户进行管理。在堡垒机下列功能中可以针对已创建的分组进行选择或者关联：

- 用户批量修改
- 访问权限
- 命令权限
- 统计报表
- 设备改密

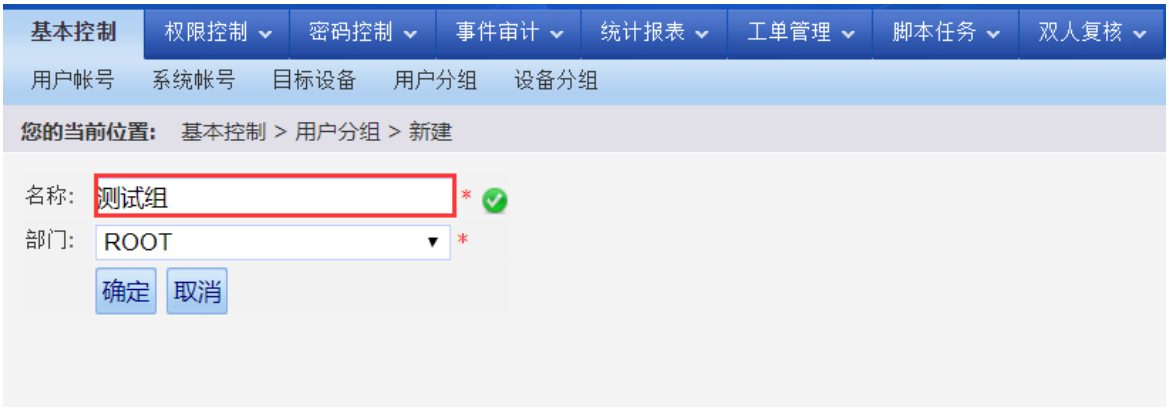
3.5.1 创建用户组

建立用户组的方法如下：

菜单位置：基本控制 > 用户分组 > 新建

根据实际情况填写相关组信息，如下图所示。

图3-88 创建用户组示意图

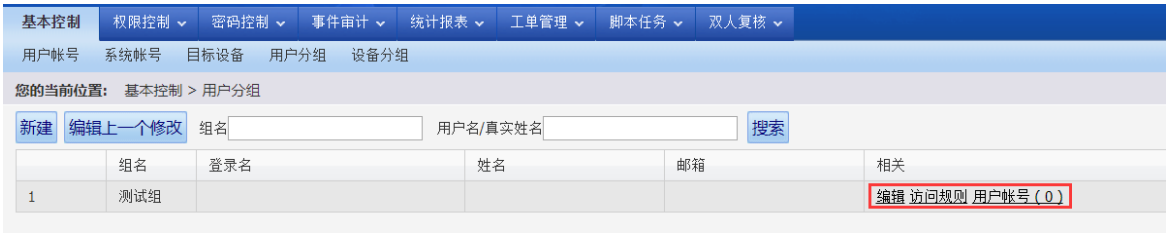


点击“确定”按钮后完成用户组创建。

3.5.2 用户组管理

针对已创建的用户组，管理员可以进行编辑、访问规则关联及组内用户管理等操作，如下图所示。

图3-89 用户组管理示意图

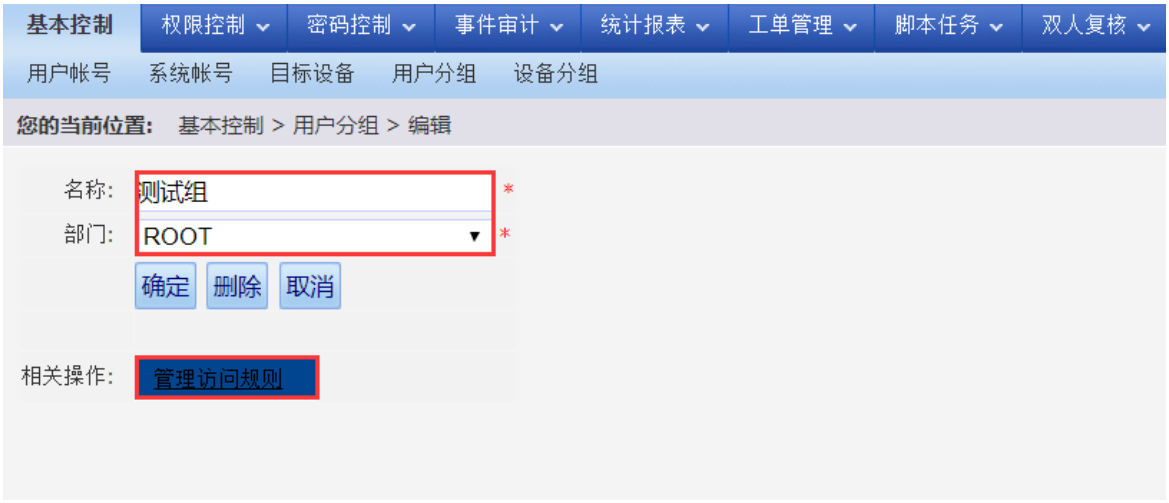


1. 编辑用户组

点击“编辑”按钮，进入用户组信息编辑界面，在此配置管理员可以对用户组名称及所属部门重新进行编辑。

点击“删除”按钮即可删除当前用户组，通过点击“管理访问规则”可以快速将用户组与相关访问规则进行关联。如下图所示。

图3-90 编辑用户组示意图

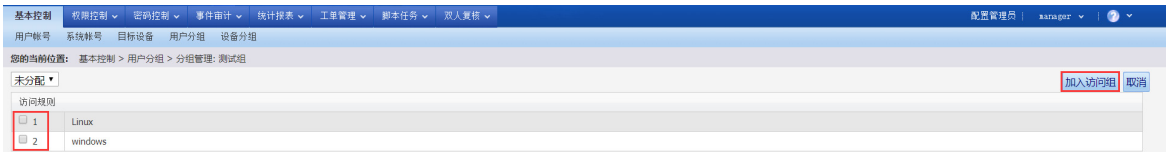


2. 访问规则关联

点击“访问规则”按钮，进入用户组访问规则关联界面，在此配置管理员可以将相应用户组快速加入到相关访问规则中。

勾选相关访问规则，点击“加入访问组”按钮即可完成用户组与相关访问规则的关联，如下图所示。

图3-91 访问规则关联示意图



通过筛选列表可以快速显示已分配/未分配的访问规则，如下图所示。

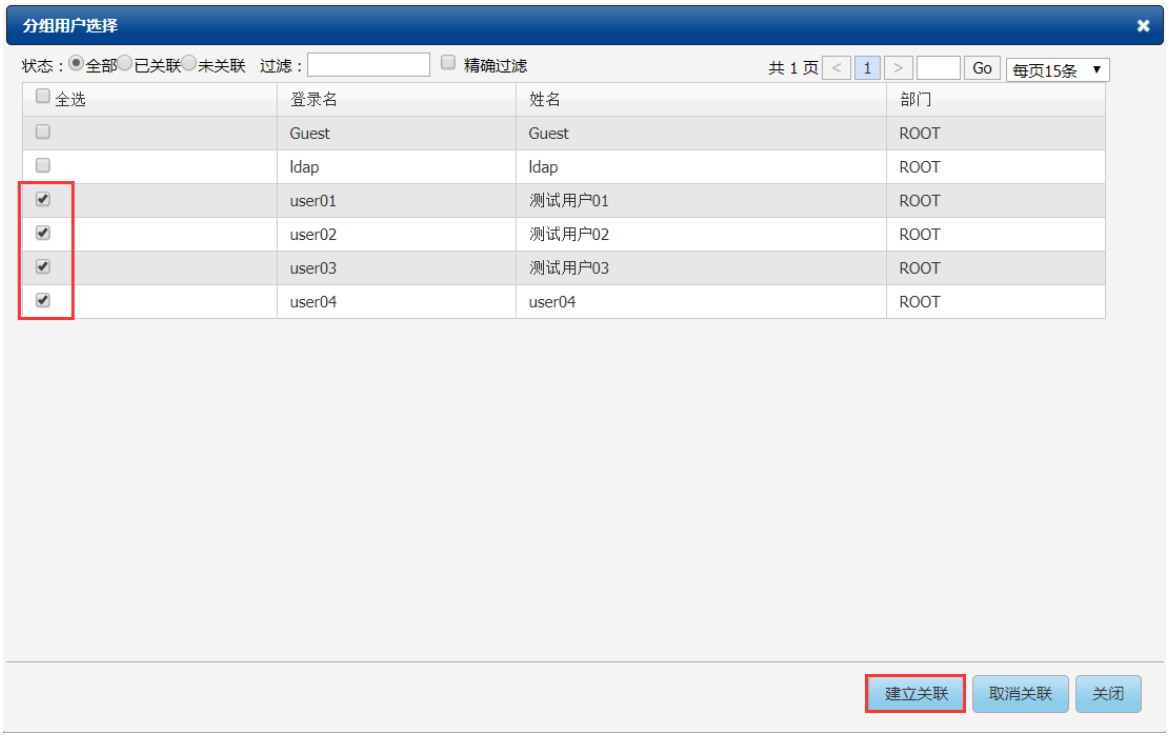
图3-92 访问规则关联筛选示意图

3. 组内用户管理

点击“用户账号(0)”按钮，进入用户分组选择界面，在此配置管理员可以进行组内用户关联操作。

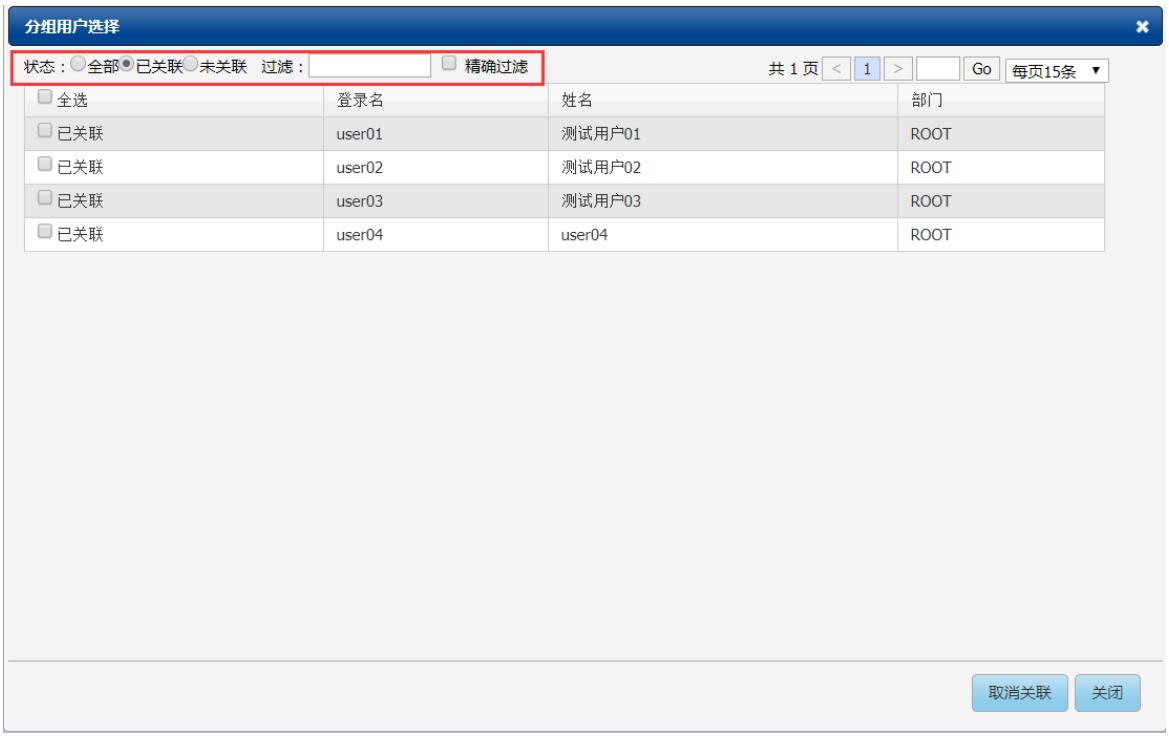
勾选相关用户，点击“建立关联”按钮即可完成用户与用户组的关联操作，如下图所示。

图3-93 组内用户管理示意图



通过状态栏，可快速过滤用户信息，如下图所示。

图3-94 组内用户过滤示意图



3.6 设备分组

为了便于批量管理，堡垒机允许配置管理员通过对设备进行分组管理。在堡垒机下列功能中可以针对已创建的分组进行选择或者关联：

- 设备批量修改
- 访问权限
- 命令权限
- 统计报表
- 脚本任务

3.6.1 创建设备组

建立设备组的方法如下

菜单位置：基本控制 > 设备分组 > 新建

根据实际情况填写相关组信息，如下图所示。

图3-95 创建设备组示意图

点击“确定”按钮后完成设备组创建。

3.6.2 设备组管理

针对已创建的设备组，管理员可以进行编辑、访问规则关联及组内设备管理等操作。

1. 编辑设备组

点击“编辑”按钮，如下图所示。

图3-96 编辑设备组示意图

进入设备组信息编辑界面，在此配置管理员可以对设备组名称及所属部门重新进行编辑，点击“删除”按钮即可删除当前设备组，通过点击“管理访问规则”可以快速将设备组与相关访问规则进行关联。如下图所示。

图3-97 编辑设备组信息示意图

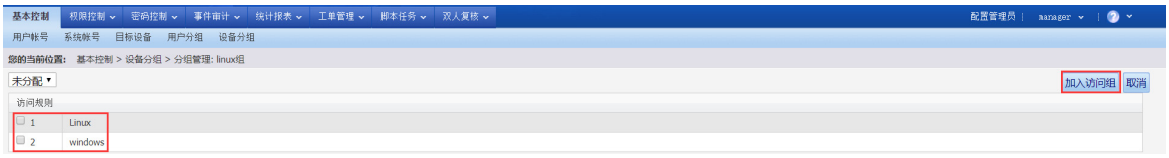
2. 访问规则关联

点击“访问规则”按钮，如下图所示。

图3-98 访问规则关联示意图

进入设备组访问规则关联界面，在此配置管理员可以将相应设备组快速加入到相关访问规则中。勾选相关访问规则，点击“加入访问组”按钮即可完成用户组与相关访问规则的关联，如下图所示。

图3-99 加入访问组示意图



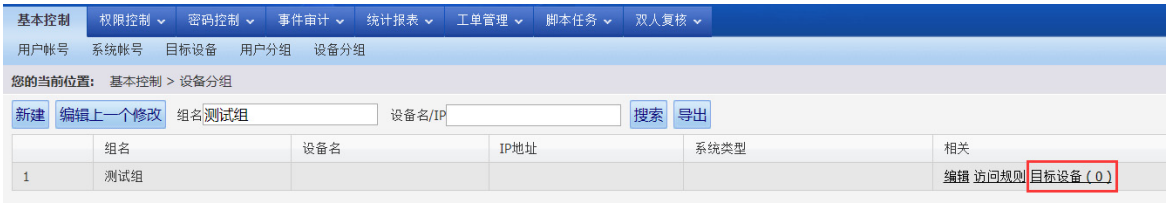
通过左上角筛选列表可以快速显示已分配/未分配的访问规则。

图3-100 筛选访问规则示意图

3. 组内设备管理

点击“目标设备(0)”按钮，如下图所示。

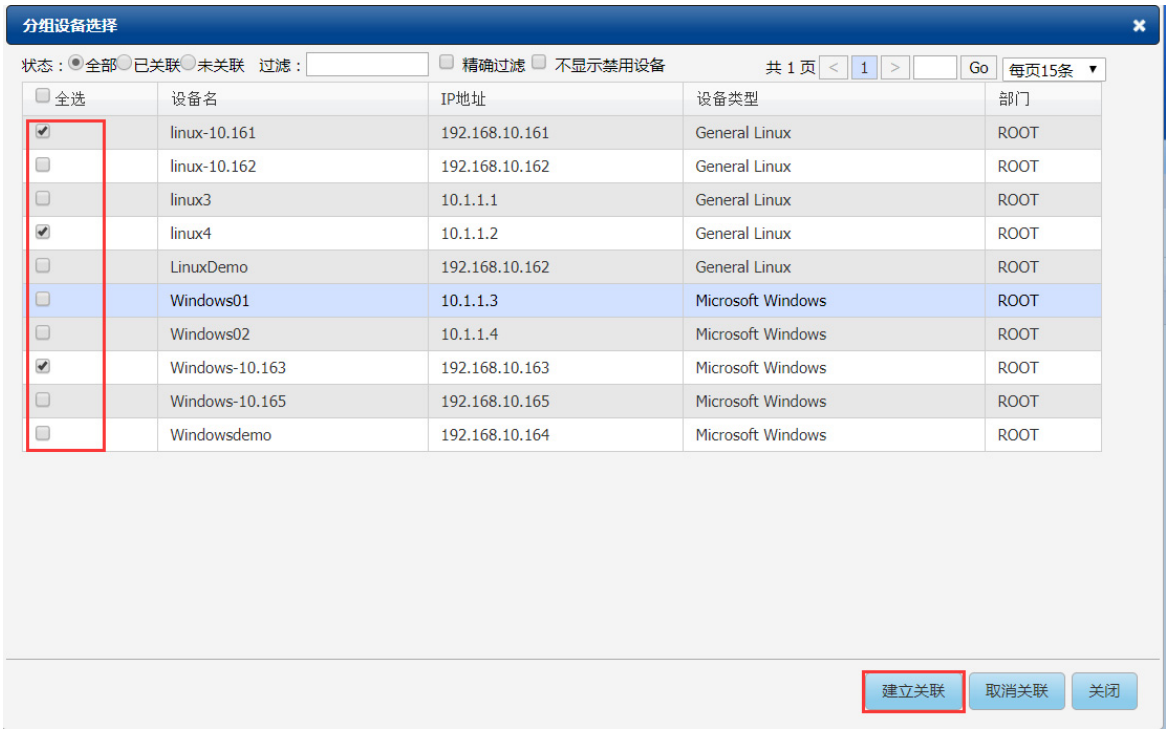
图3-101 组内设备管理示意图



进入设备分组选择界面，在此配置管理员可以进行组内设备关联操作。

勾选相关设备，点击“建立关联”按钮即可完成设备与设备组的关联操作，如下图所示。

图3-102 关联相关设备示意图



通过状态栏，可快速过滤设备信息，如下图所示。

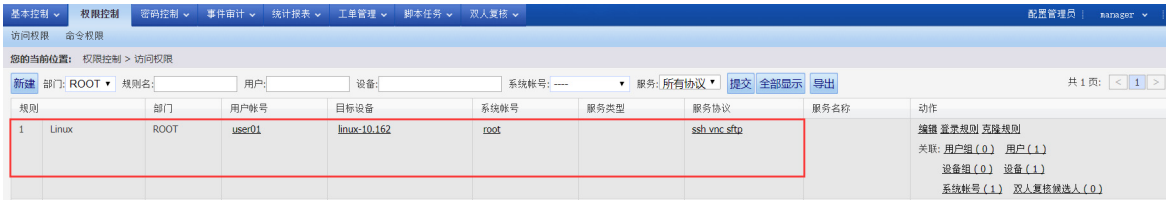
图3-103 过滤设备信息示意图

3.7 访问权限

3.7.1 访问权限介绍

堡垒机通过访问权限建立用户帐号、目标设备、服务、系统帐号之间关系，用户可以根据需要通过访问权限规则建立以上要素之间的关系，从而实现访问权限控制的目的。如下图所示。

图3-104 访问权限示意图



上图展示访问权限与用户帐号的对应关系：图上方为配置管理员设定的访问权限规则，规则名称为“Linux”，规则的含义是用户 user01 可以通过堡垒机访问“linux-10.162”目标设备的 ssh、vnc、sftp 服务，访问时可以使用 root 帐号。

3.7.2 创建访问权限

1. 规划访问权限

在创建访问权限规则前，必须确保堡垒机中已存在相关用户账号、目标设备、系统账号、服务等相关信息，然后根据实际情况规划访问规则，如下表所示。

规则名称	用户账号	目标设备	系统账号	服务
演示	User	Host	administrator	rdp

在规划访问规则时，可以将具有相同权限的用户帐号关联在同一个规则中，这样可以有效的减少堡垒机中规则的数量，提高效率。

2. 新建访问规则

菜单位置：权限控制 > 访问权限 > 新建

在新建规则编辑页面输入相关信息，如下图所示。

图3-105 新建访问规则示意图

参数解释：

- 规则名称（必填项）：为相应规则命名；
- 设备排序：设置规则中的设备在终端菜单中的排序方式，可根据主机名或 ip 地址进行排序；
- 部门（必填项）：规则所属部门，默认为 ROOT；
- 服务类型与服务协议：用于控制该规则允许使用的服务，服务类型是对服务协议的分类，勾选服务类型中相关选项可以快速勾选一类服务协议；
- 事件消息：用于设置普通用户触发该规则时的事件消息级别，高于超级管理员设定的规则的事件将以邮件或者短信的方式通知相应管理员；
- 标题：设定事件消息的标题；
- 磁盘映射：控制该规则下 windows 设备磁盘映射功能是否允许使用。

确定相关信息无误后点击“确定”按钮完成访问规则创建。

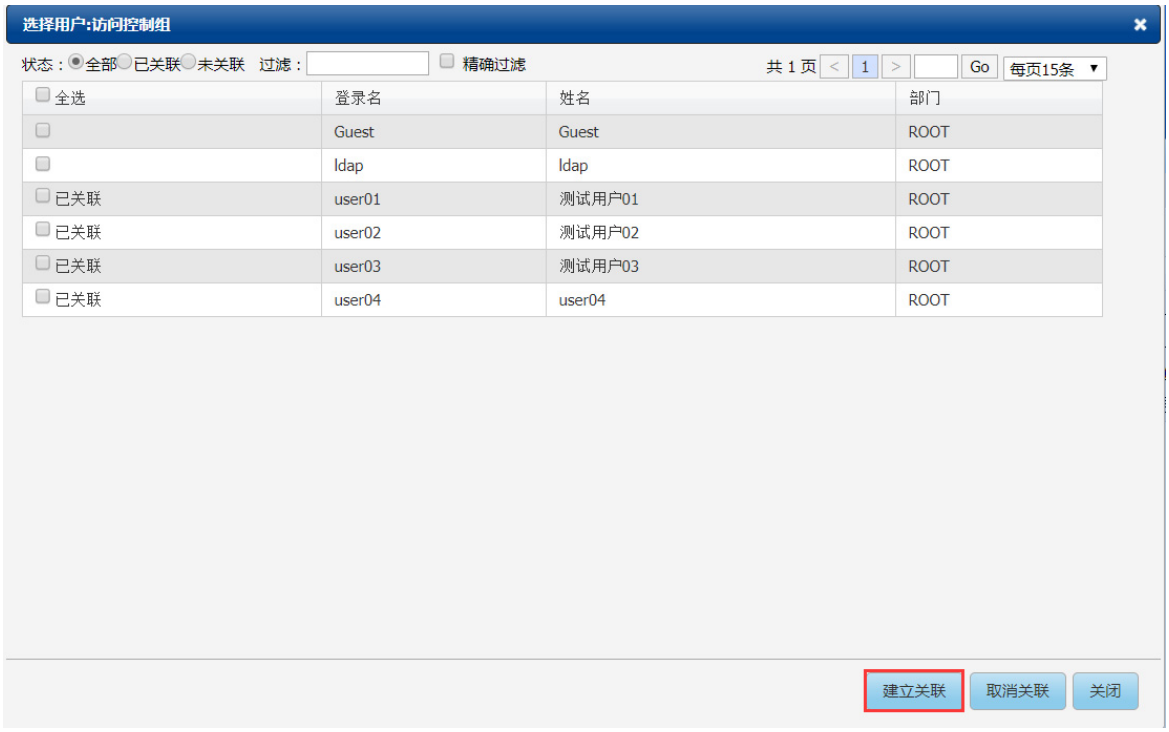
3. 访问规则关联

访问规则创建完成后，需要关联用户、目标设备及系统账号等相关信息后规则才能生效，点击动作栏处用户、设备、系统账号等按钮可进行相关信息的关联，如下图所示。

图3-106 访问规则关联示意图

例如：点击“用户(0)”后在用户关联界面，勾选相应用户（可多选），点击“建立关联”按钮完成用户信息的关联，如下图所示。

图3-107 建立用户关联示意图



参照以上示例完成设备、系统账号等信息的关联，下图为关联后的相应规则。

图3-108 关联后的相应规则示意图

注意

访问规则中必须勾选相应服务协议或服务类型，如果未勾选则相应用户通过堡垒机访问设备时将看不到任何可访问的服务。若在配置访问规则策略时遗忘此选项，可通过动作栏处“编辑”按钮重新勾选相应服务协议或服务类型。

4. 登录规则配置

通过登录规则可以针对某个访问权限生效的时间和访问地址进行控制。

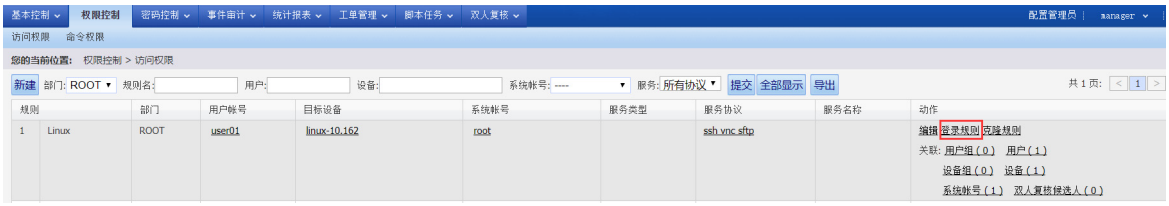
在此以设定测试规则只在每天 9：00 到 17：00 之间从 192.168.5.0/24 网络访问时有效为例说明，具体设置如下：

(1)　设置缺省策略

菜单位置：权限控制 > 访问权限

在相应访问规则处点击“登录规则”按钮，如下图所示。

图3-109 设置缺省策略示意图



在登录规则右上将默认 accept 策略修改为 deny。

图3-110 设置缺省策略示意图

(2)　设置允许的时间和 IP

在登录规则管理页面点击“新建”按钮，如下图所示。

图3-111 设置允许的时间和 IP

设置规则形式为“满足”，时间为 8：00 到 18：00，地址范围为 192.168.10.1-192.168.10.254，如下图所示。

图3-112 设置允许的时间和 IP

点击“确定”后完成登录规则设置，如下图示。

图3-113 设置允许的时间和 IP

用户可以根据需要建立更多规则，当有多条规则并存时堡垒机按照从上到下的顺序依次匹配，当有满足条件的规程被匹配到后就执行动作中设定，如果没有规则被匹配到就执行缺省策略。

5. 克隆规则

配置管理员可以通过克隆规则，快速复制出相应访问规则条目，简化规则配置操作。

“克隆规则”具体操作如下：

点击相应访问规则右侧“克隆规则”按钮，在弹出的克隆规则设置页面，输入新的规则名称后，点击“提交”按钮完成规则克隆。

3.8 命令权限

对于通过 ssh 或者 telnet 协议访问的字符会话，配置管理员可以通过设置命令权限来对操作指令做限制：当普通用户执行指令时，堡垒机会对操作指令进行检查，如果指令违规则堡垒机会操作采取拒绝、切断或者告警动作，从而实现对操作行为进行权限控制，如下图。

图3-114 命令权限示意图

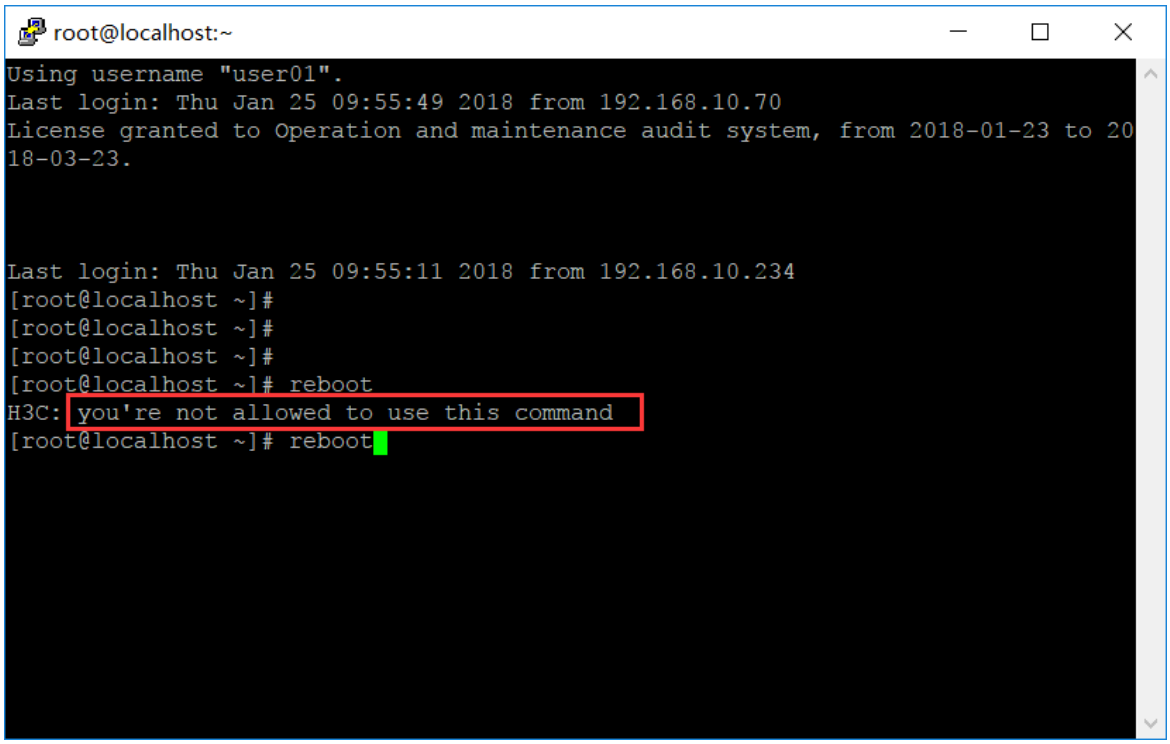
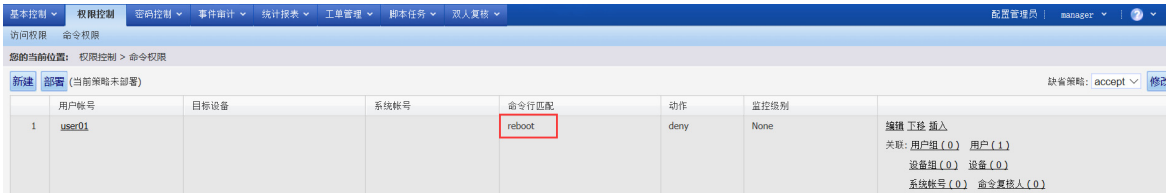


图3-115 命令权限配置示意图



上图中配置管理员设定规则不允许 user01 用户执行 reboot 命令。当 user01 用户执行 reboot 命令后，堡垒机拒绝执行用户的命令。

3.8.1 实现原理

标准的命令分为“命令+命令选项+命令参数”三部分。在堡垒机的命令权限中，把命令分为命令合入附加参数（包括命令选项，命令参数）两个部分。所以在写正则表达式的时候可以将命令分割为两个部分，中间用空格分离。

示例 1：控制用户使用 netstat 的 l 参数，可以利用正则表达式 netstat[空格].*l.*

示例 2：控制用户查看“/”目录，可以利用正则表达式 ls[空格] .*/

3.8.2 匹配原则

基本原则：

- 如果不包含空格，表示只对命令部分进行匹配。

- 如果包含空格，第一个空格以前的部分是对命令的可执行文件部分进行匹配，与上面的规则相同；后面的部分（包括其他空格）对命令的参数部分进行匹配：就是把命令行去掉命令本身之外的所有参数部分作为一个整体，与进行匹配。
- 如果以"^"开头，或者包含"/"字符，表示严格匹配，即命令部分必须完全匹配正则表达式。比如"^passwd$"只匹配"passwd"本身，前面加上任何字符都认为不匹配。比如"/usr/bin/passwd$"只匹配"/usr/bin/passwd"，任何其他路径或不写路径都不接受。否则将把命令的最后一个"/"字符后的部分拿来做匹配。比如"passwd$"匹配"passwd"、"/usr/bin/passwd"、"asdf/passwd"等。
- 最小检查单位：堡垒机对命令的检查是以回车符为界限进行的，只有当用户按下回车提交命令后堡垒机才会执行命令权限检查。

3.8.3 命令解释器（Shell）

命令的执行是通过命令解释器（Shell）翻译成机器语言，从而得到命令执行结果的输出。而命令防火墙是基于 Shell 之上对输入的命令进行一遍过滤，这一点不同于其他网络防火墙，可以对数据包的输入输出或者转发进行控制。所以任何脱离 shell 的操作，都达不到控制的目的。

3.8.4 脚本控制

脚本作为一种特殊的编程形式，可以直接调用 shell 中的命令资源。脚本在执行的时候会将脚本文件直接提交给指定的 shell。因此，堡垒机对于已经被 shell 所接受的命令无法控制。管理员要想控制其操作，唯一能做的就是控制所有脚本的执行，以及所有的执行方式，如相当路径，绝对路径等等。管理员可以将此类脚本任务的执行可以采用命令复核人的方式进行控制，下面将介绍命令复核人。

3.8.5 命令复核人

命令复核人作为堡垒机金库模式的一个标准配置，可以对用户的命令输入进行审核，在确认该命令没有风险的情况下，审核人输入自己的密码审批通过，让命令顺利执行。

图3-116 用户在输入 ifconfig 之后需要得到命令复核人的确认

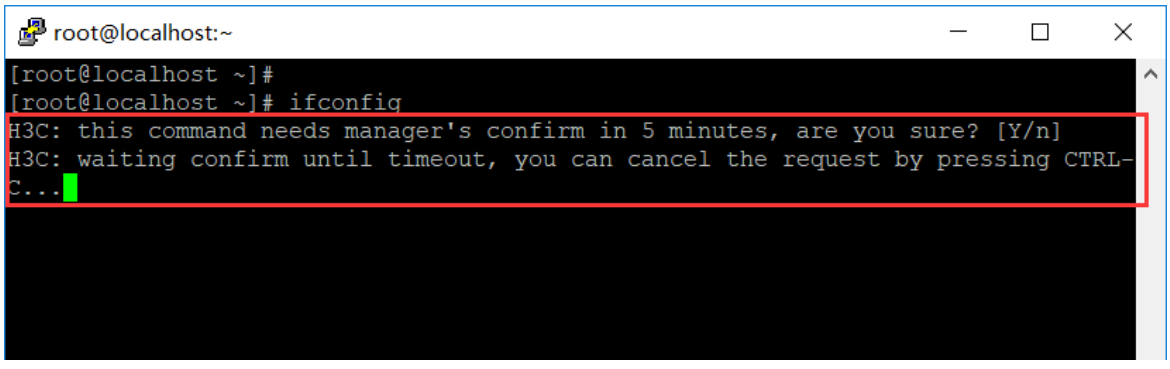
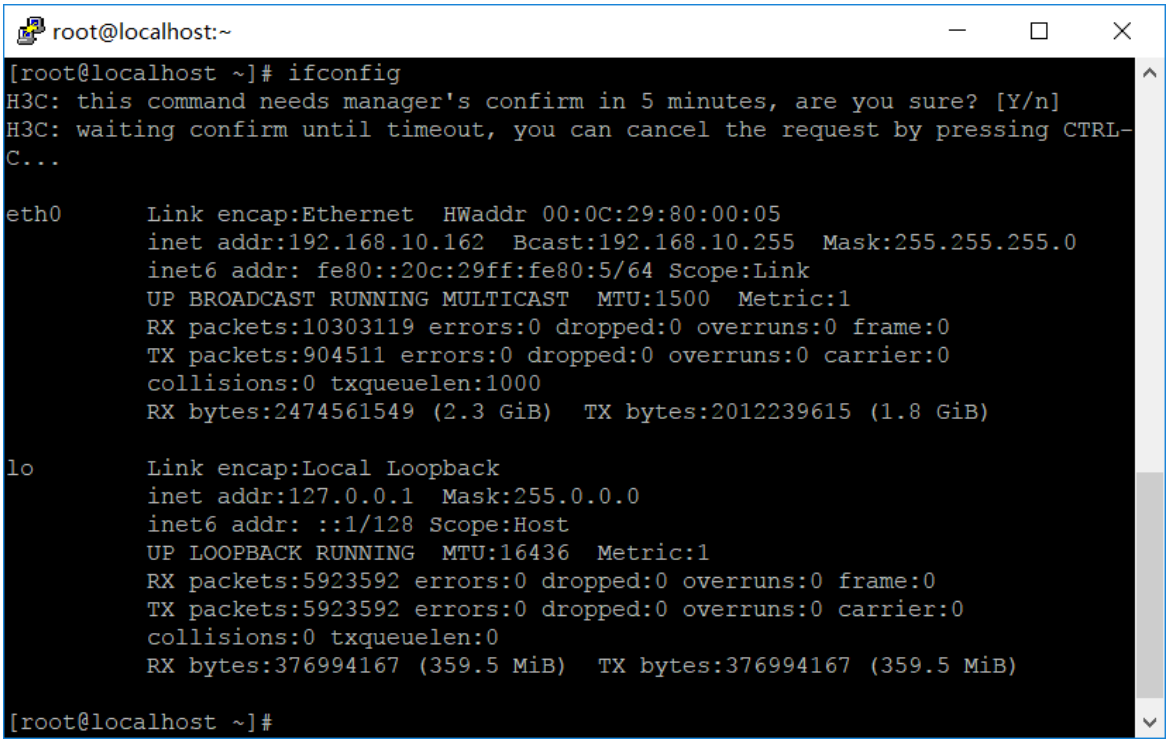


图3-117 复核人在命令复核界面上看到了该条命令的复核申请。

图3-118 复核完成，得到命令输出



3.8.6 优先级

- 堡垒机进行逐条规则匹配，执行第一条符合条件的结果，不再考虑之后的规则。
- 如果所有规则均不满足，按照缺省策略进行。

3.8.7 配置方法

1. 全局设置

在命令权限首页可以看到右上角有叫缺省策略的设置项：如果选择“accept”，则除命令权限列表之外的规则为允许；如果选择“deny”，则除命令权限列表之外的规则为阻止。

2. 新建权限

配置管理员访问“权限控制”-“命令权限”，点击“新建”可以建立新的规则，如下图。

参数解释：

- 操作规则：设置命令规则，遵循正则表达式，允许同时写多条匹配规则，每行为一个规则。
- 动作：设置符合规则的命令的处理方式。Accpet 表示允许执行，deny 表示拒绝执行，kill 表示切断会话，confirm 表示该条策略需要被命令复合人审批之后才能继续执行。
- 时间范围：设置规则的有效时间，具体规则见页面说明。
- 监控级别：设置触发规则后的事件消息级别，高于超级管理员设置的级别后将会发送通知给管理员，通知方式包括邮件、syslog 等，None 将不产生任何事件消息。
- 邮件标题：设置事件消息的邮件标题。

3. 设定规则的适用范围

通过关联用户、设备和系统帐号可以设定规则的适用范围，如下图。

关于规则的适用范围：

- 如果不关联任何用户、设备和系统帐号该规则对所有用户、设备和系统帐号均有效；
- 如果关联了用户、设备和系统帐号规则仅对已关联的用户、设备和系统帐号有效。
- 如果规则是 confirm 的，需要选择至少一个命令复合人。

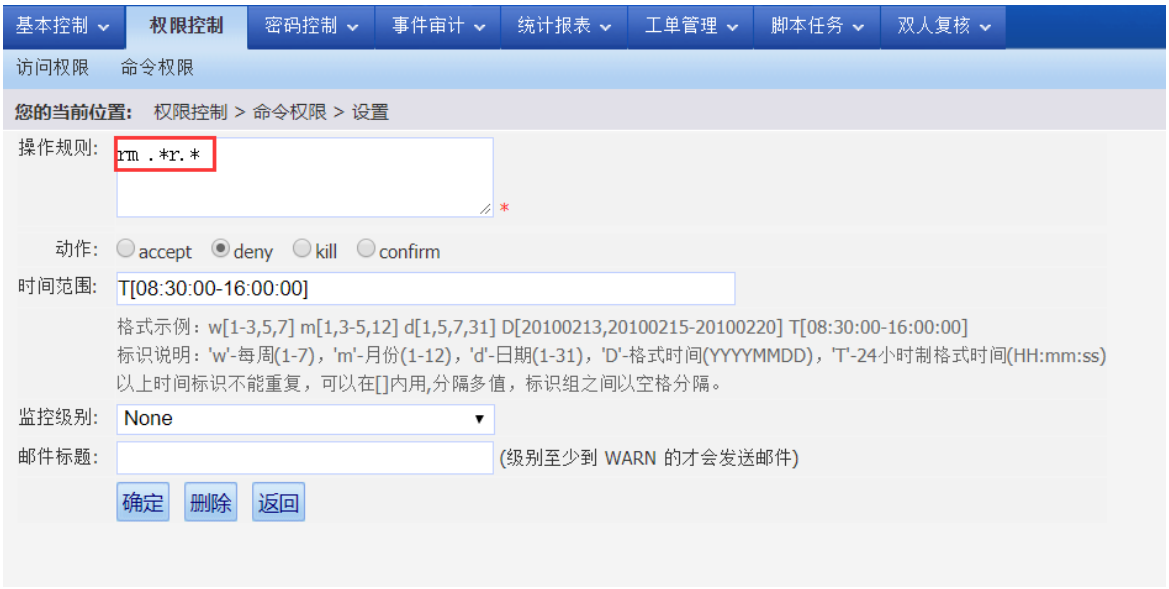
4. 规则生效

新建或者修改规则后规则的变更不会立即生效，如下图。

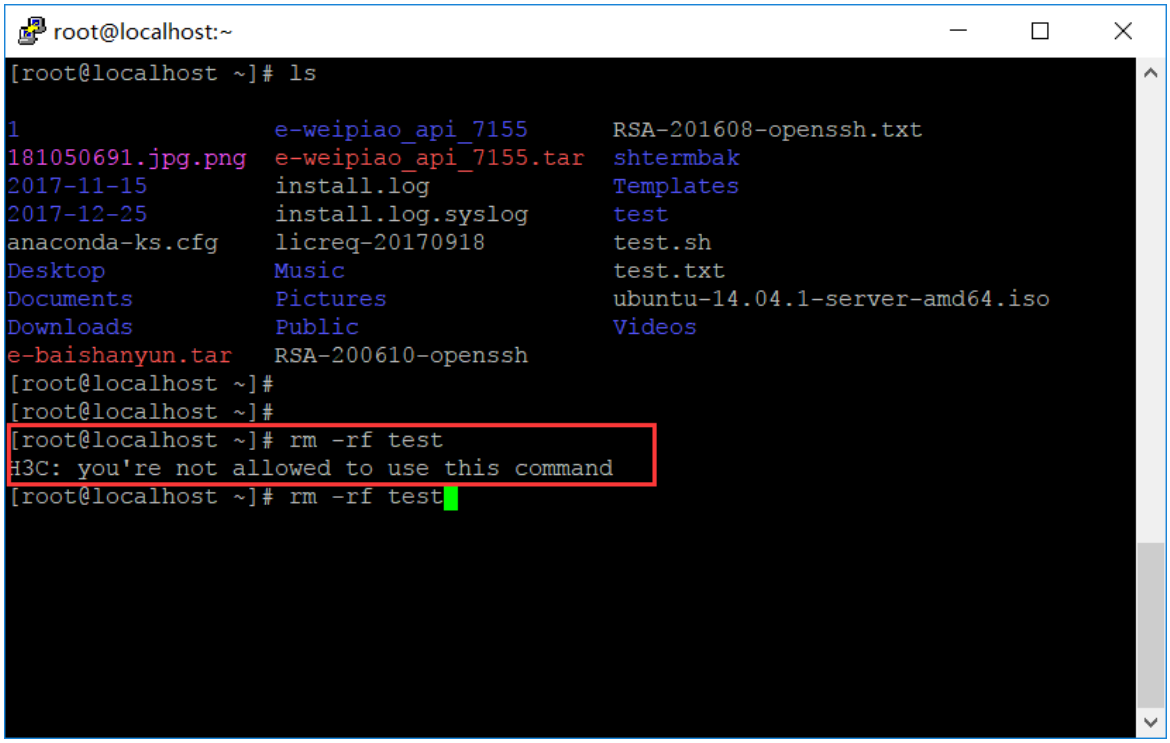
只要有“当前策略未部署”的标记存在就说明变更未生效，要使变更生效必须点击“部署”，部署后规则将在 1 分种后生效，生效后对已经存在的和新建的字符会话均有效。

3.8.8 示例

1. 示例 1：防止用户删除目录（Linux为例）



Linux 下删除目录的命令为 rm –r [目录名]，但是实际操作中有时会添加其他参数，如 rm –rf [目录名]，所以这里匹配规则在参数部分写明的是中间包含 r 字母。但是这样一来如果删除文件的时候，文件名中间有 r 字母也不被允许删除了，这时我们可以利用 linux 本身的通配符来进行删除，如图：



配置好了之后关联相关用户和设备以及系统账号（某项不选择则默认匹配所有），最后一定要点击“部署”按钮使规则生效。

2. 示例 2：防止用户执行bash脚本

脚本的执行方式有很多，这里只列举其中的几种较为常见的。如下：

- ./*　该条策略为防止用户使用相当路径和绝对路径执行脚本。
- bash .*　该条策略防止用户利用 bash 命令执行脚本。
- sh .*　该条策略防止用户用 sh 命令执行脚本。
- .* `.*　该条策略防止用户以命令（如 echo）+`脚本路径`方式执行脚本。

3.9 密码控制

改密计划和设备改密日志请参考《自动改密配置举例手册》。

3.10 事件审计

3.10.1 登录日志

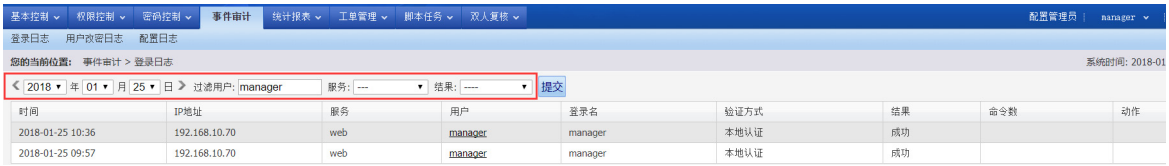
菜单位置：事件审计 > 登录日志

通过登录日志，配置管理员可查看用户登录堡垒机的相关信息（如登录是否成功、账户是否锁定等），如下图所示。

图3-119 登录日志示意图

通过页面中工具栏可帮助管理员快速过滤登录日志信息（如登录失败、账户锁定等），如下图所示。

图3-120 过滤登录日志信息示意图



3.10.2 用户改密日志

菜单位置：事件审计 > 用户改密日志

用户改密日志记录堡垒机用户账号改密信息，如下图所示。

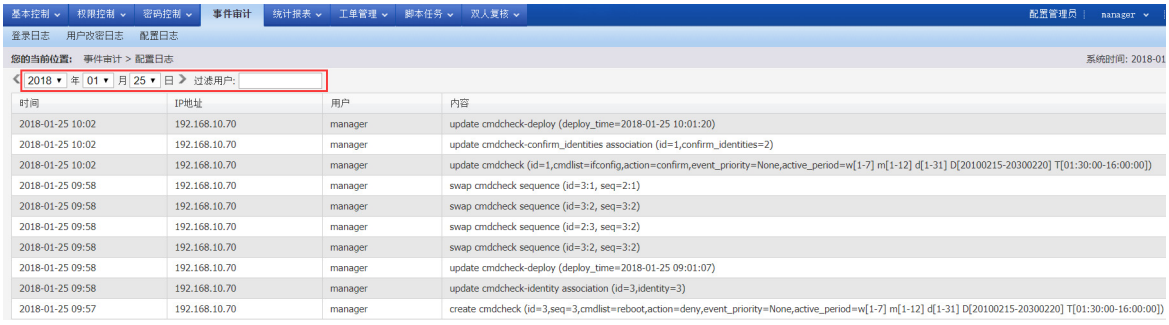
图3-121 用户改密日志示意图

3.10.3 配置日志

菜单位置：事件审计 > 配置日志

配置日志记录堡垒机中所有管理员角色对堡垒机的进行的配置变更记录，如下图所示。

图3-122 配置日志示意图

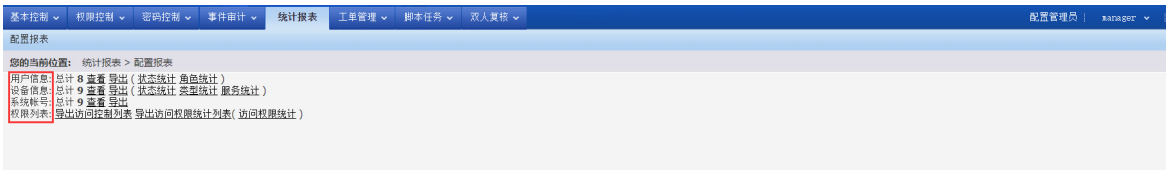


3.11 统计报表

菜单位置：统计报表 > 配置报表

配置管理员可以通过配置报表查看用户信息（用户帐号）、设备信息、系统账号、权限列表等报表信息，如下图所示。

图3-123 统计报表示意图



3.12 工单管理

3.12.1 工单介绍

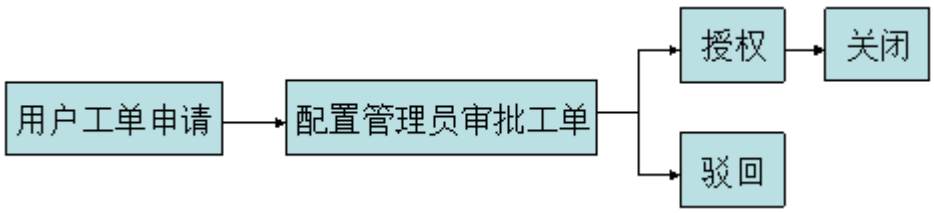
1. 工单简介

工单为用户提供一个临时申请访问权限的途径，这种临时申请的访问权限可以在申请时限到达的时候被自动及时回收，无需管理员干预。

2. 工单流程

配置管理员可以进行工单的审批（驳回、授权、），其他用户可以进行新建工单。工单基本流程如下图所示。

图3-124 工单基本流程示意图



3.12.2 创建工单

1. 新建工单

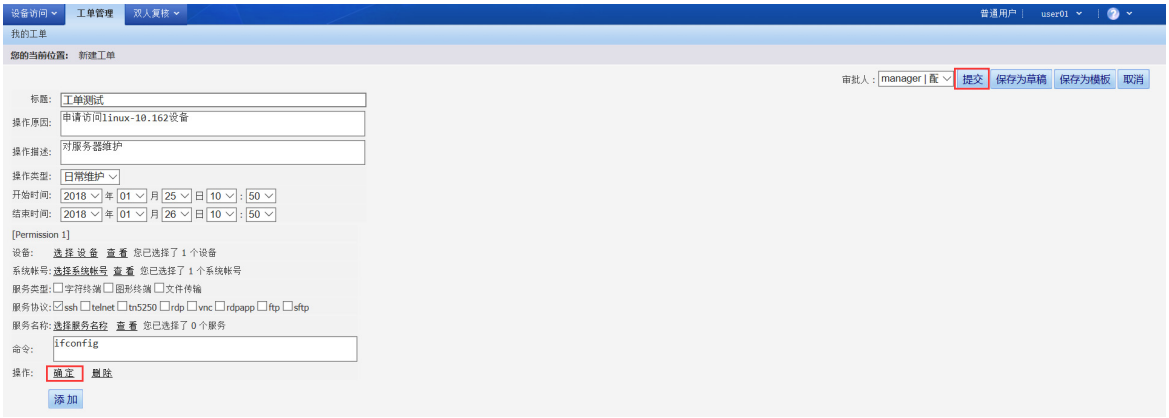
(1) 普通用户登录 Web 界面，“工单管理”>“我的工单”>“新建工单”

图3-125 新建工单示意图

(2)　进入后填写工单具体内容

如下图页面显示。

图3-126 新建工单选项示意图



参数解释：

- 标题：填写所建工单的名称，该项为必填项。
- 操作原因：工单操作的原因。
- 操作描述：操作步骤。
- 操作类型：可选“日常维护”、“抢修”、“实施”、“测试”四种类型，该项为必填项。
- 时间：选择申请工单的时间段，该项为必填项。
- Permission 1：
  - 设备：关联需要使用的设备，该项为必填项。
  - 系统账号：关联需要使用的系统账号，该项为必填项。
  - 服务类型/服务协议/服务名称：关联需要使用的服务，该项为必填项。
  - 命令：描述使用中需要执行的命令，该项为选填项，可根据实际使用情况进行填写。
  - 操作：确认以上填写完成后按“确定”不需要这条 permission 则按“删除”，该项为必操作项。
- 添加：同一条工单中再加一条 permission。

图3-127 Permission 添加完成图

2. 工单提交

新建工单中选项填写完成后，可以选择相应配置管理员审批或者留作模板及草稿

图3-128 工单提交选项图

(1)　提交审批

右上角选择相应“配置管理员”，点击“提交”

返回到“我的工单”页面可见。

图3-129 工单待审图

此处等待配置管理员进行审核。

图3-130 工单驳回图

图3-131 工单驳回图

若管理员驳回，则可询问管理员相关情况，继续修改。

图3-132 工单有效图

若管理员允许，则可针对工单内容进行访问设备，如下图。

图3-133 工单访问示意图

(2)　提交模板

右上角选择相应“配置管理员”，点击“保存为模板”。

则生成工单模板，便于下次使用提交。

图3-134 工单模板图

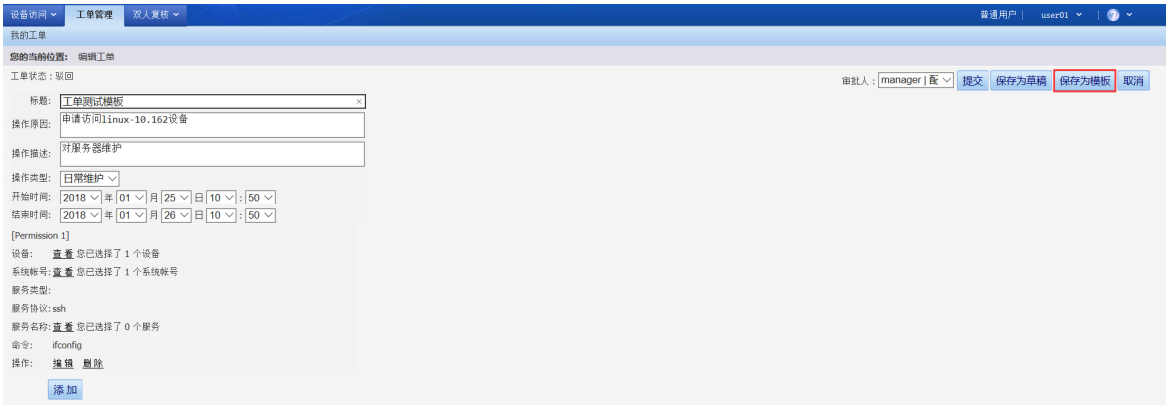


图3-135 工单模板图

(3) 提交草稿

右上角选择相应“配置管理员”，点击“保存为草稿”。

则生成工单草稿，便于下次继续编辑使用。

图3-136 工单草稿图

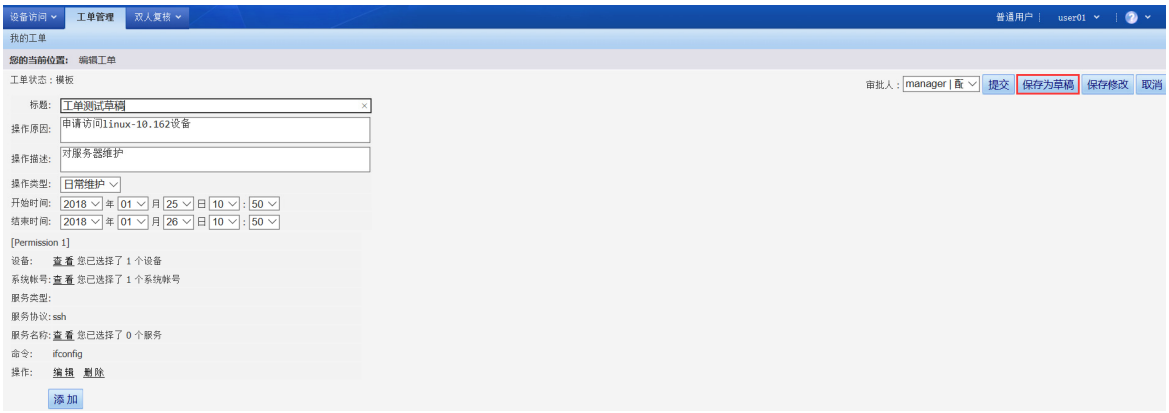


图3-137 工单草稿图

3.12.3 工单审批管理

1. 工单查看

工单查看审核需要使用带“配置管理员”权限的用户

(1) “配置管理员”Web 访问堡垒机

(2) 点击“工单管理”>“全部工单”

图3-138 全部工单示意图

在当前页便可查看当前属于你审批的工单，过滤项说明如下：

图3-139 工单过滤项示意图

- 工单标题：根据工单名称进行搜索，模糊匹配。
- 申请时间：下拉选择时间对工单申请时间进行搜索匹配。
- 工单状态：根据有效、待审、驳回、关闭四种状态进行匹配。
- 申请人：根据申请人进行模糊匹配。
- 翻页：当前页显示工单为 30 个超出可翻页。

2. 工单审批

工单审批分为三个类型，分别是“授权”、“驳回”、“停用”

图3-140 工单审批示意图

当普通用户管理员申请工单后，进入 Web 页面后可在右上角看到黄色“消息”提示，如下图。

图3-141 工单消息提示示意图

点击“消息”可看到未处理的工单，如下图所示。

图3-142 工单消息提示示意图

点击“详细”可查看当前工单主要内容，允许选择“授权”，不允许选择“驳回”。

图3-143 工单详细示意图

点击后页面将会提示“操作成功”返回至“工单管理”>“全部工单”可查看工单当前的状态。若有特殊情况，需要中断该有效工单的使用，可以点击“停用”，如下图。

图3-144 工单停用示意图

点击后将手工终止该工单的使用时限。

3.12.4 工单访问

1. 可访问工单查看

当“配置管理审批后”,“普通用户”可登录 Web 页面，点击“设备访问”>“工单访问”

图3-145 工单访问示意图

可查看当前可以使用工单，停用或过期工单不会显示。

2. 工单详细

点击相应工单“详细”

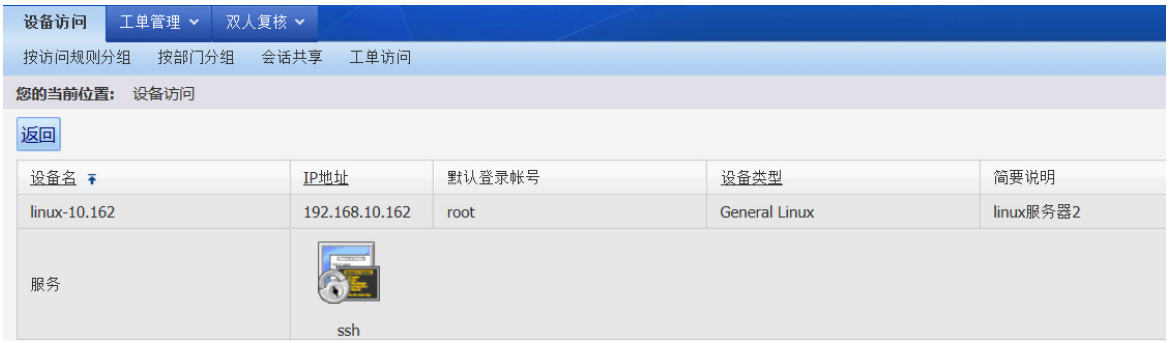
可查看该工单的描述、有效时间、可访问情况，如下图。

3. 工单详细示意图

4. 工单访问

点击相应工单“设备访问”进入到设备访问页面，列出可访问设备，如下图。

图3-146 工单访问示意图



3.13 脚本任务

3.13.1 概述

脚本任务是指堡垒机通过 telnet 或者 ssh 访问登录到目标设备后自动执行脚本协助管理员对目标设备进行批量自动化管理。

堡垒机的脚本任务支持 ssh-batch 和 builtin-interact 两种方式。

1. ssh-batch的特点

- 自定义脚本：用户可以根据需要自己撰写 shell 脚本；也可以上传已经写好的脚本到堡垒机建立脚本任务并执行。
- 工作方式：堡垒机需要先 ssh 登录目标设备建立相应的工作目录，然后以 scp 方式将脚本推送到工作目录内，最终 ssh 到目标设备执行脚本。
- 非交互式：如果需要执行的任务具有交互式的工作，堡垒机将无法使用这种方式执行。
- 不判断执行结果：堡垒机执行脚本后进将执行的输出记录在数据库中，但不对执行结果进行任何的判断。

ssh-batch 方式仅适用于有 ssh 服务的 Unix-like 设备,支持采用非标准 ssh 端口，标准为 22 端口。

2. Builtin-interact的特点

Builtin-interact 方式是指堡垒机内置的交互式脚本，目前堡垒机内置了 get-remote-ip 和 netdev-config-backup 两个交互式脚本，分别用于获取 Unix-like 的 ip 地址（ifconfig）和网络设备的配置备份。

这种方式支持通过 telnet 和 ssh 协议登录执行，交互式脚本由厂商提供。

3.13.2 建立脚本任务

1. 建立ssh-batch脚本任务

配置管理员访问”脚本任务 > 任务浏览”，点击”新建任务”，如下图。

图3-147 建立 ssh-batch 脚本任务

参数解释：

- 任务名称：填写任务的名称。
- 设备和设备组：用于选项需要执行脚本的设备。
- 系统帐号：选择执行脚本所使用的系统帐号，请务必保证该帐号的在选择的设备的 ssh 服务中可以通过登录测试。
- 脚本类型：请选择 ssh-batch。
- 上传文件名：为脚本命名。
- 脚本内容：撰写脚本的内容，请根据需要撰写。
- 上传脚本文件：上传本地脚本文件到堡垒机，上传文件请使用 UTF-8 编码格式,并且文件小于 100K。
- 工作目录：脚本的工作目录，请保证所选择的系统帐号对该目录有写入权限了。
- 结果加密：脚本任务执行结果进行加密上传或者发送，加密方式为 ZIP 密码。
- 结果发送：选择执行结果的接收者，接受者必须配置的电子邮件地址。

- 结果上传：可上传结果至预先设置好的文件服务器。
- 并发数量限制：同时执行脚本的并发个数。
- 下次执行时间：设定下次执行时间。
- 执行周期：设定执行的周期。
- 任务描述：填写任务说明。

2. 内置交互式脚本（网络设备配置备份）

我们以网络设备配置备份为例介绍如何使用内置交互式脚本：

配置管理员访问“脚本任务 > 任务浏览 > 新建任务””。

图3-148 内置交互式脚本示意图

- 脚本类型：请选择 builtin-interact。
- 文件名：请选择 netdev-config-backup，该脚本的可以自动在目标设备上执行 show config 命令。

任务的执行结果输出可在 Web 页面查看或者下载到本地查看。

注意

其他选项与 ssh-batch 脚本任务一样

3.13.3 查看执行情况

可以在“脚本任务 > 执行情况”中查看任务执行情况和输出，如下图所示。

图3-149 执行情况示意图

脚本任务的执行结果输出可在 Web 页面查看，也可以下载到本地查看。

3.14 双人复核

3.14.1 命令复核

命令复核请参考命令权限相关章节。

4 密码管理员配置

4.1 密码保管员职责

密码保管员主要负责：

(1) 定期查看改密计划执行结果。

(2) 对改密计划执行失败的机器以及账号做手工修改。

(3) 执行密码备份任务。

(4) 在应急状况下能出示正确的密码供其他用户使用。

密码保管员可以获取所有托管到堡垒机的设备密码，请慎重分配密码保管员。

4.2 密码保管员信息设置

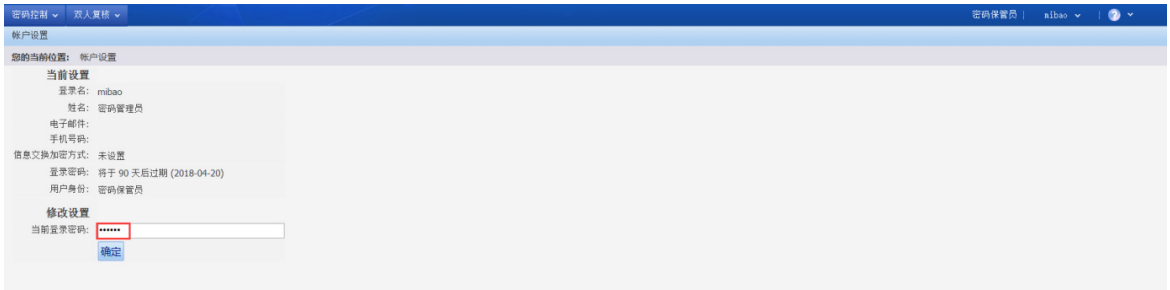
4.2.1 进入账户设置

在当前账号（mibao）下拉列表中选择“账户设置”，如下图。

图4-1 密码保管员账户设置示意图

然后输入登录堡垒机的密码，如下图。

图4-2 密码保管员账户设置输入密码示意图



进入“账号设置”页面，如下图。

图4-3 密码保管员账户设置页面示意图

4.2.2 设置邮箱地址

进入“账户设置”>“个人设置”>“账号信息”，填写有效邮件地址，点击“确定”保存，如下图。

图4-4 密码保管员账户设置设置邮箱地址示意图

配置有效邮箱地址用以接收堡垒机发送的改密邮件或者密码备份邮件。

4.2.3 设置信息交换加密密码

通过堡垒机修改目标设备或者对目标设备进行密码备份时，堡垒机上提供 Zip 密码方式对密码文件进行加密，Zip 密码设置，需配置一个 8 位以上密码，如下图所示。

图4-5 设置信息交换密码示意图

进行密码备份时，SHTEMR 会把密码文件打包成.zip 文件，打包的同时用设置的 zip 密码进行加密。

4.3 密码控制

4.3.1 密码备份

堡垒机支持两种密码备份方式：

- 本地磁盘：密码保管员可以把加密后的密码文件下载到当前使用的电脑上。
- 文件服务器：密码保管员可以加密后的密码文件备份到 ftp 或者 sftp 服务器上。

备份方式使用需要联系超级管理员在“策略配置 > 设备密码”页面开启。

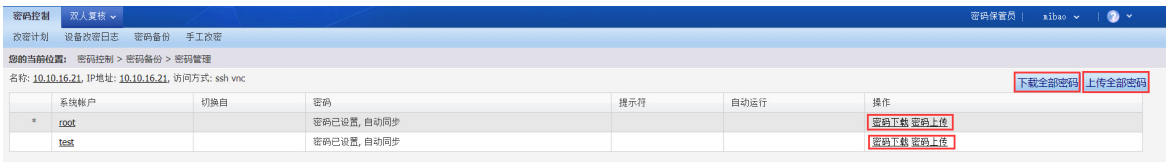
1. 单设备密码备份

进入“密码控制”>“密码备份”，在设备列表中找到要备份的设备，在右边的“动作”栏点击“密码管理”，如下图。

图4-6 单设备密码备份密码管理示意图

打开“密码管理”页面后点击“下载全部密码”（下载到本地）或者“上传全部密码”（上传到 ftp、sftp 服务器）。也可以点击具体系统账号“操作”栏的“密码下载”、“密码上传”，备份单个设备上单系统账号密码。

图4-7 单设备密码备份密码管理示意图



2. 批量密码备份

进入“密码控制” > “密码备份”，直接点击“下载全部密码”或“上传全部密码”或“打印全部密码”，如下图。

图4-8 批量密码备份密码管理示意图

4.3.2 改密计划

改密计划由配置管理员设置，密码可以查看当前所有改密计划的列表。

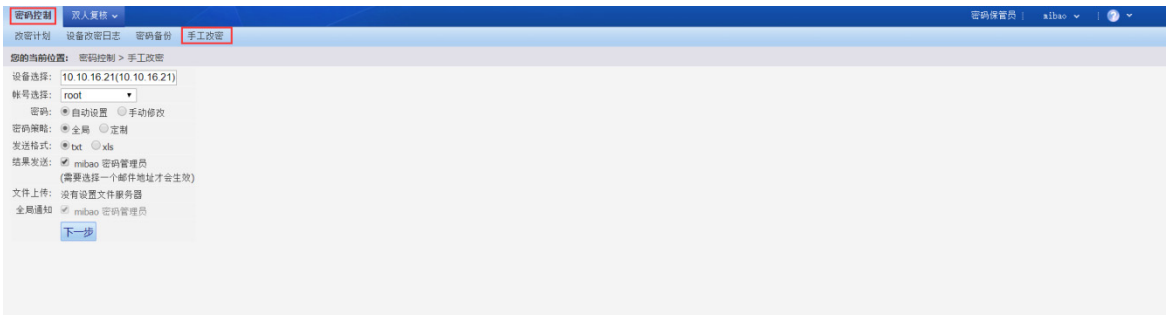
改密计划及设备改密可参考《自动改密配置举例》文档。

4.3.3 手工改密

密码保管员可以手动对单个目标设备的系统账号密码进行修改。

对于改密计划中改密失败的设备和账号，可以通过手动改密进行补救，具体手工改密可参考《自动改密配置举例》文档。

图4-9 手工改密示意图



4.3.4 改密日志

改密日志里面记录了堡垒机对所设备上账号密码的修改记录和日志，如下图。

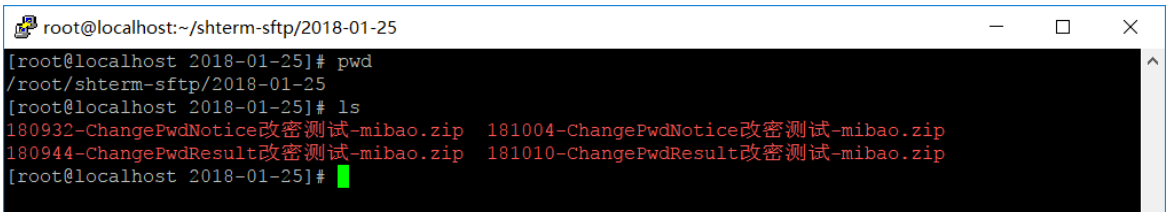
图4-10 改密日志列表示意图

点击“详细”可以查看整个改密过程。

4.3.5 查看密码

备份的密码文件格式为 xx.zip 压缩文件，是用密码保管员设置的 zip 文件密码进行加密的，可使用压缩工具（winzip、winrar、好压等）打开.zip 文件，解压或者直接双击打开密码文件时要求输入密码，输入对应密码保管员的 zip 文件密码即可。

图4-11 查看密码示意图



5 审计管理员配置

审计管理员的日常任务包括对各普通用户的操作行为进行审计和监督，对操作事件进行管理，统计日志报表。

审计管理员第一次登录堡垒机时，需要安装工具下载中提供的 java 和 gui-player。其中，gui-player 为视频回放工具，审计管理员在查看图形会话时必备；java 为该视频回放工具的运行环境。

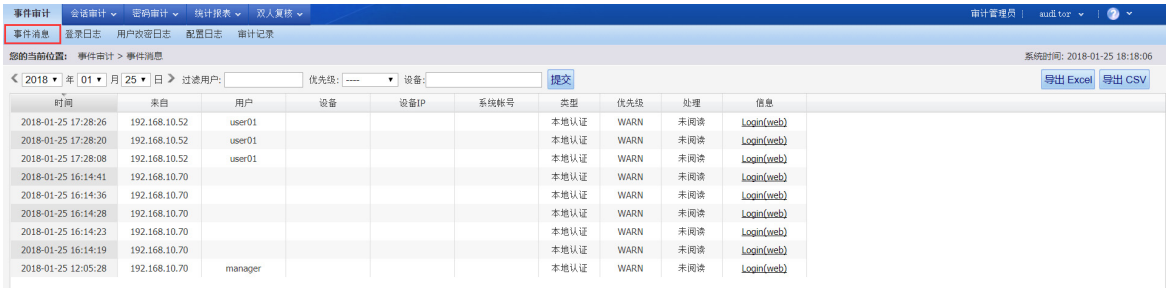
5.1 事件审计

堡垒机中事件的定义是所有在堡垒机上进行的操做，包括对目标设备的操作，包括登录，操作行为；登录堡垒机，对堡垒机进行配置；用户账号密码的更改；临时用户的授权；以及对审计管理员审计行为的审计。

5.1.1 事件信息

配置管理员定制了事件级别之后（大于 NONE），当用户的行为触发了这些规则时系统就会记录这些事件。当这些事件的级别超过了监控通知（日志，邮件，短信）所制定的范围，系统则会发送相应的监控通知。

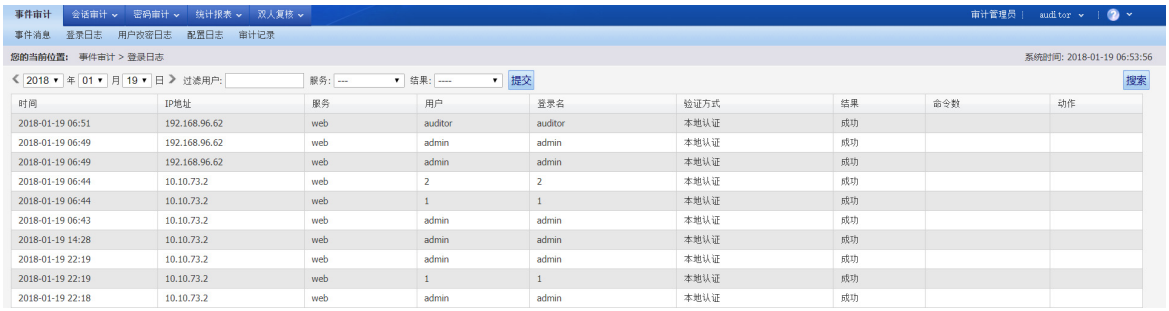
图5-1 事件消息示意图



5.1.2 登录日志

登录日志审计表是对用户登录堡垒机的记录，包括时间点，源 IP 地址，通过哪种渠道（Web 或者字符工具）登录的，用户名，身份验证方式和登录是否成功。

图5-2 登录日志示意图



5.1.3 改密日志

事件审计中的改密日志仅限于堡垒机用户修改了密码的记录，而不是目标设备的账号密码修改。目标设备的改密在接下来的密码密钥审计里面会另做介绍。

图5-3 改密日志示意图

5.1.4 审计记录

审计记录是针对审计管理员的审计行为所设立的。该表主要记录了审计管理员账号，审计的方式（命令，回放，下载或者实时监控）。

点击会话序列号可以看到该条审计记录所针对的会话信息。

图5-4 审计记录示意图

5.1.5 改密计划

改密计划可参考《自动改密配置举例》文档。

5.1.6 改密日志

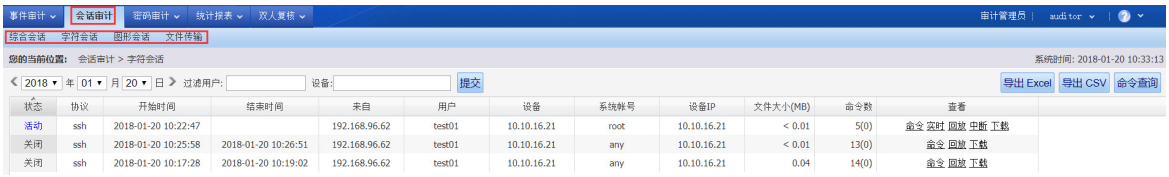
改密日志可参考《自动改密配置举例》文档。

5.2 会话审计

会话审计功能主要针对各普通用户对设备的操作行为做审计，审计管理员在此功能模块中不但可以对历史操作日志进行分类查询，而且可以实时监控正在进行的操作。

会话审计菜单分为四个功能模块：综合会话，字符会话，图形会话和文件传输，如下图。

图5-5 会话审计功能模块示意图



5.2.1 如何使用搜索栏

堡垒机审计管理员界面的搜索栏可以根据时间，设备和用户来进行精确过滤。

1. 过滤时间

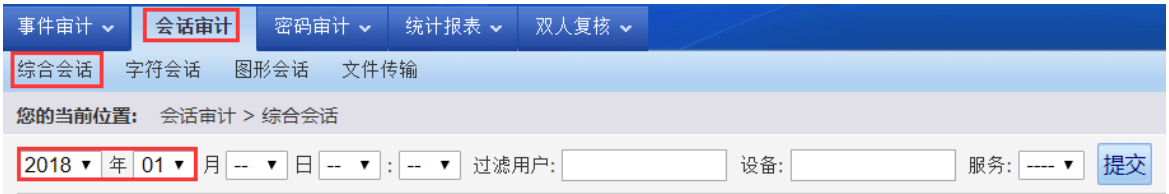
时间段的过滤包括年、月、日、小时、分钟这五个字段，字段为空表示匹配该字段中的所有时间点，例如：

(1) 审计管理员需要过滤出 2018 年 1 月 20 日 10 点开始的日志，直接选择 2018 年 1 月 20 日 10 点，如下图。

图5-6 会话审计时间过滤示意图

(2) 如果审计管理员需要过滤出 2014 年 2 月份每天的日志，直接选择 2014 年 2 月，如下图。

图5-7 会话审计时间过滤示意图



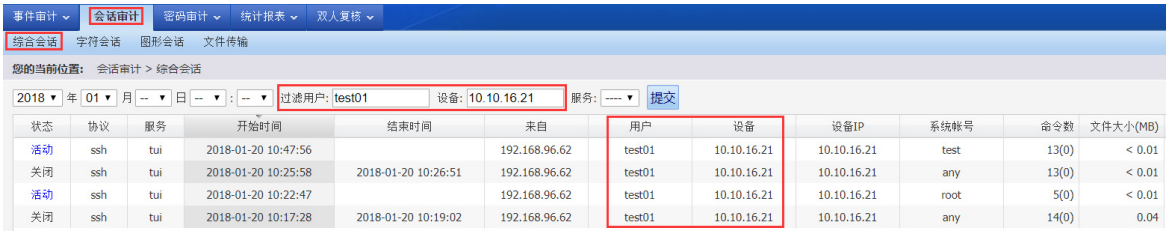
注意

如果有多个留空的字段，堡垒机在过滤时只会匹配时间范围较大的留空字段，例如：如果选择 2018 年 1 月（日留空）10 点（分钟留空），堡垒机只会过滤出 2018 年 1 月份的日志

2. 过滤设备和用户

和时间过滤一样，设备和用户的过滤只需要选择相应的设备或者用户来进行搜索，留空表示匹配该字段所有的日志，如下图。

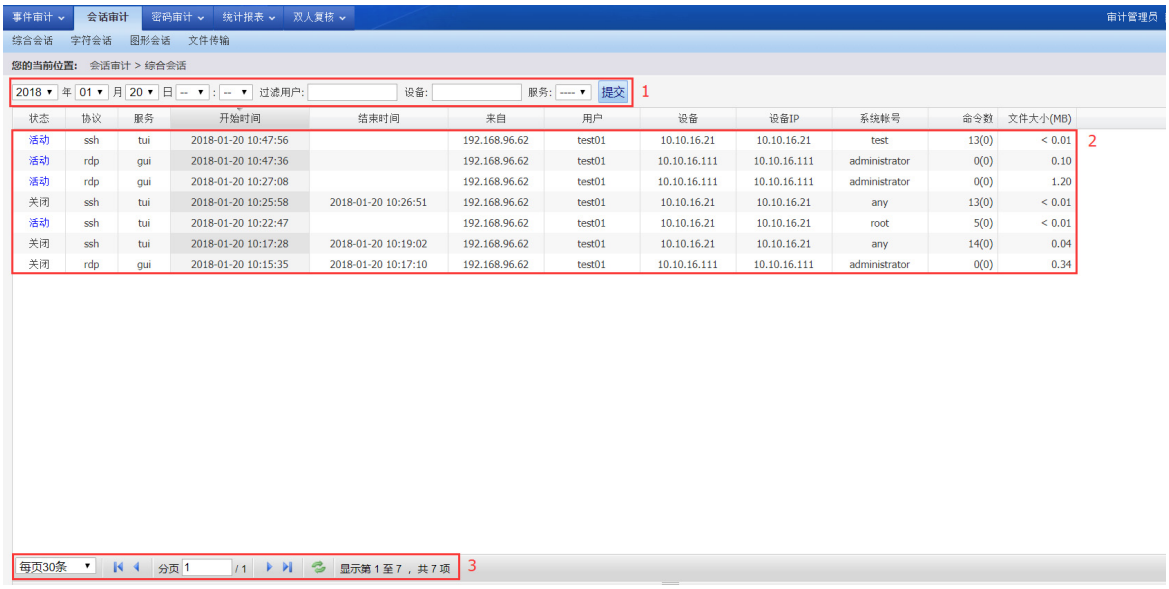
图5-8 会话审计过滤用户设备示意图



5.2.2 综合会话

综合会话是对字符和图形会话的汇总，主要针对每条会话记录了该会话的整体信息，如下图。

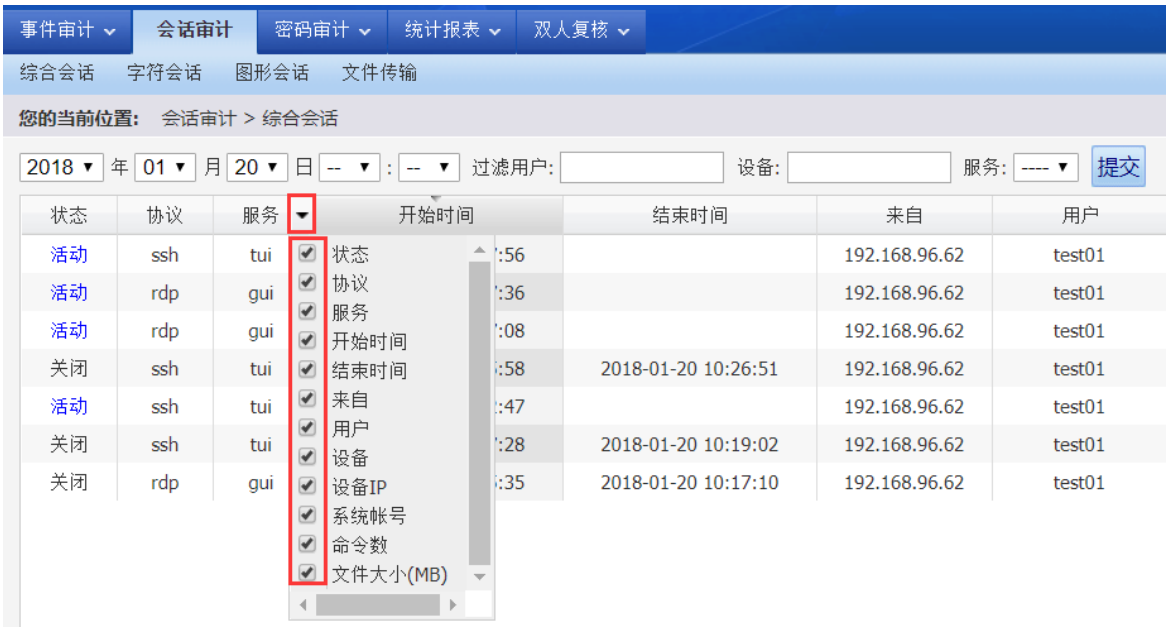
图5-9 会话审计综合会话示意图



- 1 号区域为搜索栏，审计管理员可以根据选择好的条件，点击“提交”按钮后进行搜索过滤。
- 2 号区域中可以根据开始和结束时间进行排序，“服务”一列表示的是图形还是字符会话（图形用 gui 表示，字符用 tui 表示），“文件大小”表示的是堡垒机保存的操作日志的大小。
- 3 号区域中可以选择分页。

鼠标移至表头的列名上可以看到一个下拉符号，点击之后可以勾选所需要的列名来对列进行筛选。如下图。

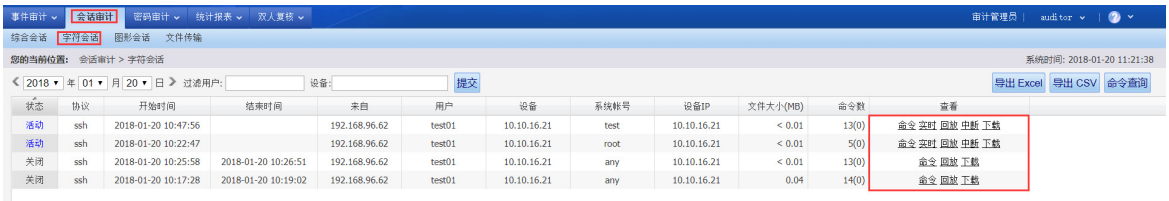
图5-10 综合会话列筛选示意图



5.2.3 字符会话（TUI）

字符会话列表只针对字符会话信息做审计，在查看列中可以选择“命令”或者“回放”链接来进行详细的审计。也可以将此列表按照所选的格式导出，如下图。

图5-11 字符会话示意图

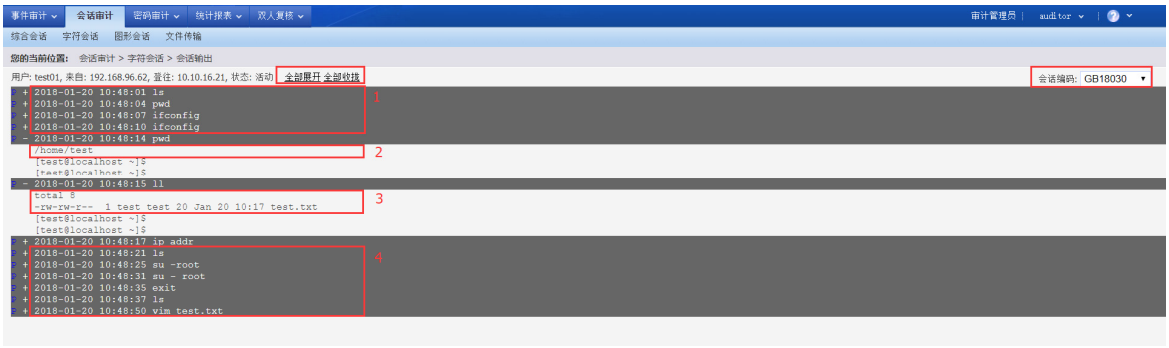


1. 命令审计

点击上图中每条日志的“回放”按钮，会进行该条日志的完整重放。

点击上图中每条日志的“命令”按钮，会进入到日志的命令记录界面，记录了所有输入过的命令以及返回的信息，如下图。

图5-12 命令审计示意图



- 右上角区域可以选择字符编码来查看命令输出，若编码不匹配，则有可能查看到的中文显示为乱码。
- 1号和4号区域为命令输入，这两块区域的底色不同是因为：灰色为堡垒机允许范围内的操作，属于合法操作，有效；紫红色则表示该操作已经触发了堡垒机的命令权限（命令防火墙），属于违规操作，无效。
- 2号和3号区域则是命令输出，默认显示10行的输出。若需要看完整的输出则点击输出栏最下行的提示链接。
- 另外也可以点击正上方的“全部展开”和“全部收拢”链接对所有命令的输入和输出进行完整查看。

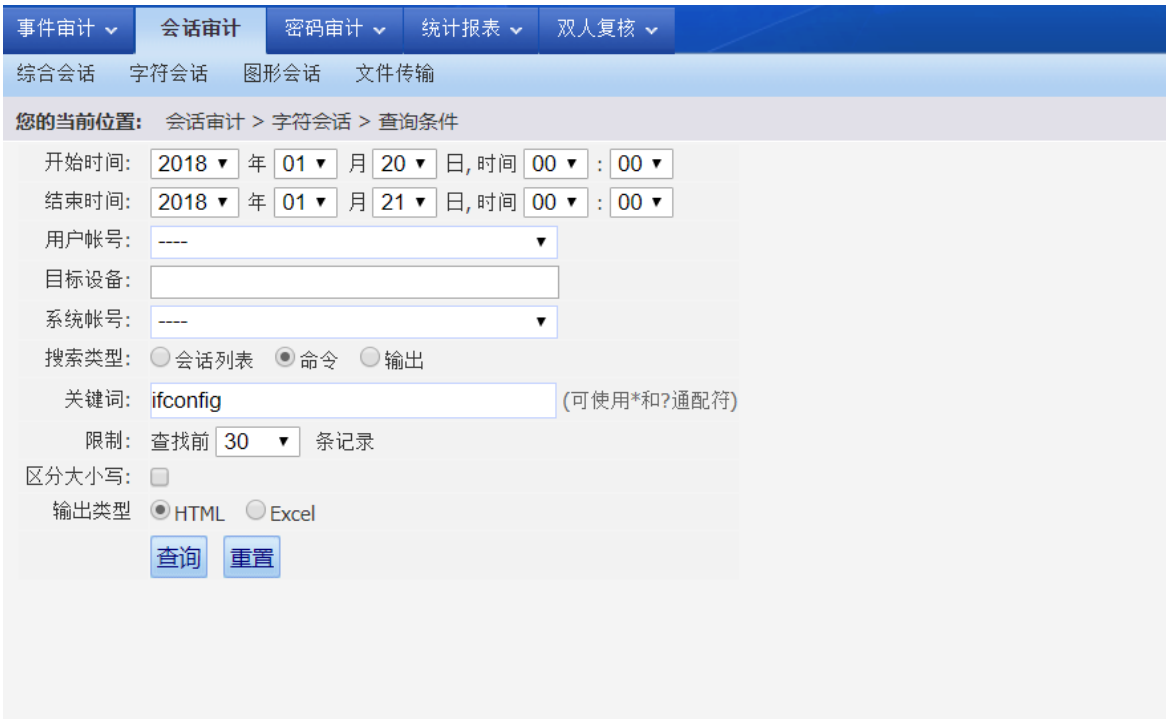
注意

每条命令的左边都有一个大写字母“P”，点击该字母则会弹出java回放窗口进行命令回放，时间点是从这个“P“字母所在的命令输入开始。

2. 命令的查询与导出

在字符会话列表的右上角可以看到有三个按钮，其中“导出Excel”和“导出CSV”都可以将本页面中的会话列表按相应的格式存放到本地。点击“命令查询”按钮会进入到一个命令查询界面，如下图。

图5-13 命令查询示意图



设置查询条件：

- 时间段：审计管理员可以指定时间段（开始时间和结束时间）来进行查询。注意的是这里的时间段不允许空字段。
- 用户账号：审计管理员可以指定特定的普通用户进行查询，若不指定则匹配所有的普通用户。
- 目标设备：审计管理员可以指定特定的目标设备进行查询，若不指定则匹配所有的目标设备。
- 系统账号：审计管理员可以指定特定的系统账号进行查询，若不指定则匹配所有的系统账号。
- 搜索类型：搜索类型分为三种，会话列表，命令和输出：
  - 会话列表：堡垒机会列出所有匹配条件的会话列表。
  - 命令：根据用户在登录字符设备时用键盘输入的指令进行搜索。
  - 输出：用户在输入完指令之后回车执行的屏幕输出。
- 关键词：审计管理员可以这里输入需要搜索的具体字段进行查询，也可以输入“*”号来匹配所有字段，或者输入“？”匹配单个字段。
- 限制：如果查询出来的内容太多了，查找不方便，在可以这里设置查询的输出限制。
- 区分大小写：审计管理员在指定“关键词”之后可以这里选择是否需要对他输入的关键词区分大小写来进行搜索。
- 输出类型：查询的结果可以按照 html 格式或者 excel 格式来进行输出。其中，html 为直接在 Web 界面中显示结果；excel 为保存为 excel 格式下载到本地。

3. 实时监控

在字符会话列表中，状态为活动的会话，在查看栏中会有至少四个选项：命令，实时，回放和中断。命令和回放已经在刚才做了详细的解释，这里介绍实时和中断功能。

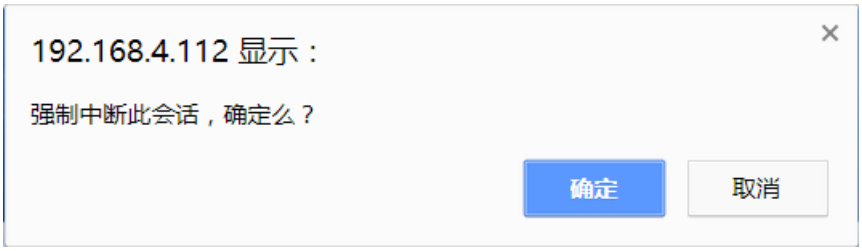
图5-14 实时监控示意图

- 实时：点击该链接，可以进入一个窗口对该会话进行实时监控，包括可以查看到操作者输入的命令和命令反馈，而操作者本身对实时监控无所察觉。如下图。

图5-15 实时监控画面示意图

- 中断：在实时监控过程中如果审计管理员发现有危险操作，可以利用此功能立即切断该会话，如下图。

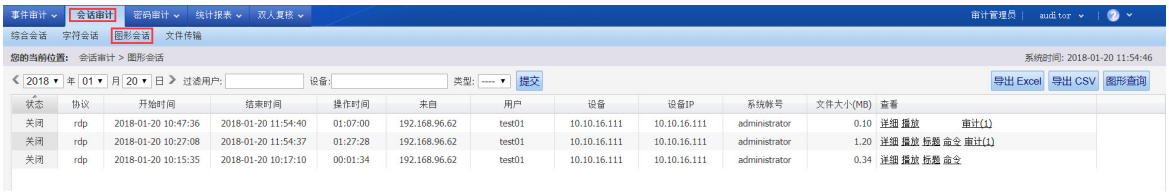
图5-16 强制中断示意图



5.2.4 图形会话（GUI）

图形会话审计的内容包括所有的 windows，应用发布服务（rdpapp），vnc 等以图像方式进行操作的会话。图形会话审计的内容包括所有的键盘输入，屏幕播放和关键字查询。

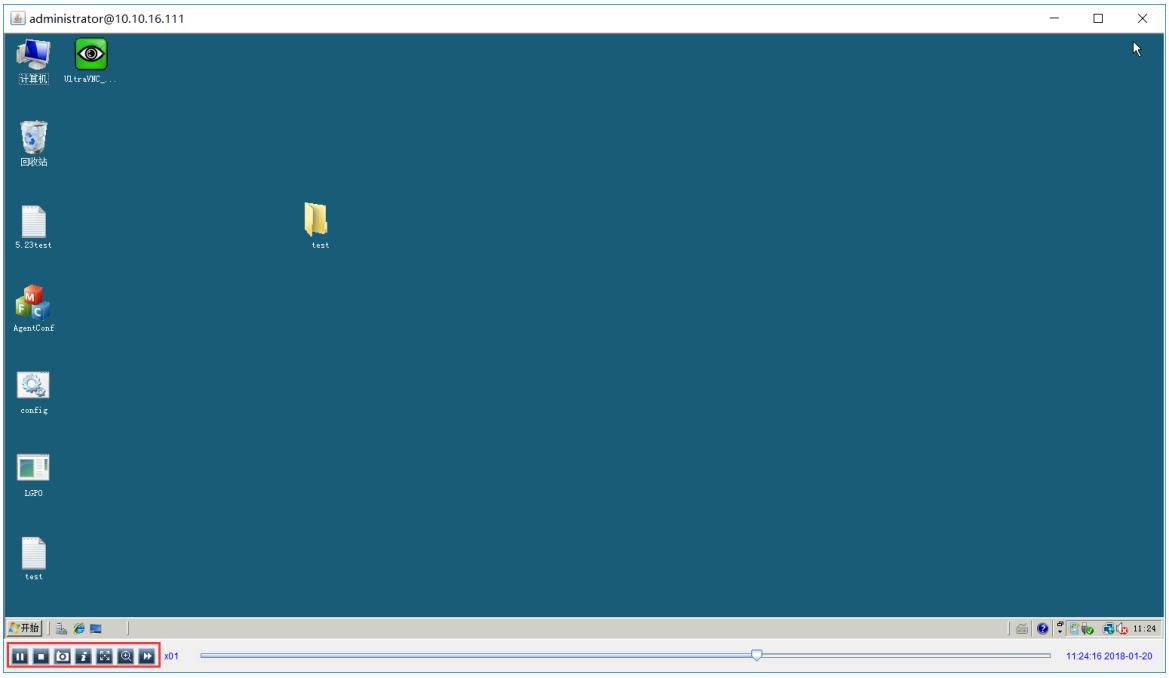
图5-17 图形会话示意图



1. 图形会话的播放

点击图 5-13 中会话列表内的“播放”，堡垒机会启用 gui-player（播放器）来进行图形日志的完整播放，如下图。

图5-18 图形会话播放示意图



播放器功能说明：

-  播放键，和暂停键配合使用。
-  暂停键。
-  停止键，停止正在播放的会话。
-  截图键，对屏幕中的内容进行截图保存。

-  查看键，对会话的信息（用户，系统账号，时间，ip 等）进行查看。
-  全屏键，让正在播放的视频全屏显示。
-  缩放键，调整播放窗口的大小。
-  调速键，可以调整视频播放的速度，最大为 64 倍速度，最小为 0.25 倍。
- 另外进度条也可以由鼠标来进行定位播放。

2. 图形会话的详细信息查看

点击图 5-13 中会话列表内的“详细”进入到图形会话的详细信息界面，可以看到该会话的具体细节,如下图。

图5-19 图形会话详细信息

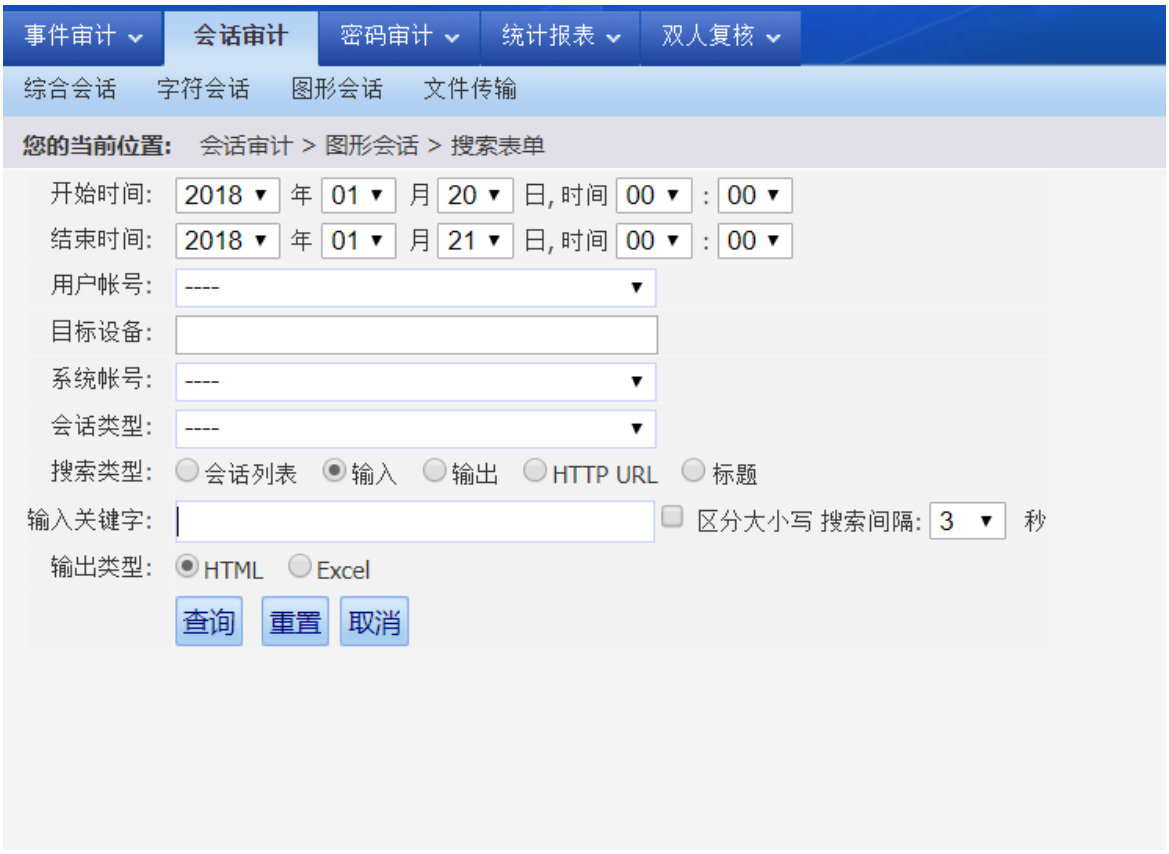
参数解释：

- 其中点击键盘输入栏的“按键列表”可以打开键盘事件表，记录包括所有键盘和鼠标的操作。
- “输入模拟”则是对键盘输入事件进行提取，可以清楚的看到用户都输入了哪些信息。
- 输出显示栏中的“输出列表”是捕获图形界面上的关键字，将这些关键字和其坐标都放在了图形会话输出列表内。
- 这里也可以自定义时间段将会话下载至本地，用 gui-player 播放器进行播放。

3. 图形查询与导出

和字符审计一样，图形审计也可以导出会话列表，这里就不重复说明了。点击图 5-13 中右上角的“图形查询”，可以进入到图形查询界面，主要是针对关键字的查询，这点类似字符会话的命令查询。

图5-20 图形查询示意图



相比于字符审计的命令搜索，这里在搜索类型中多出了“HTTP URL”选项，在输入关键字搜索中也多出了“搜索间隔”，下面来分别说明：

- HTTP URL：针对于 HTTP 类型的应用发布进行 URL 的查询。
- 搜索间隔：用户敲击键盘的时间间隔进行关键字匹配。例如：搜索间隔设置成 10 秒，就必须在 10 秒中之内输入关键字的会话才能被查询。

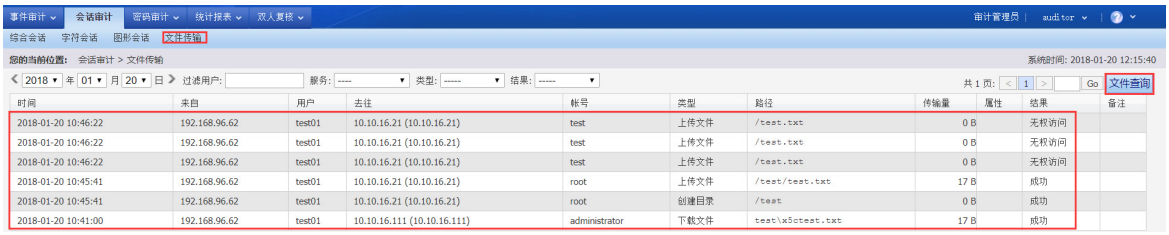
4. 实时监控

对于活动会话可以看多了“实时监控”和“切断”两个功能，这里和字符会话中的“实时”、“切断”类似。

5.2.5 文件传输

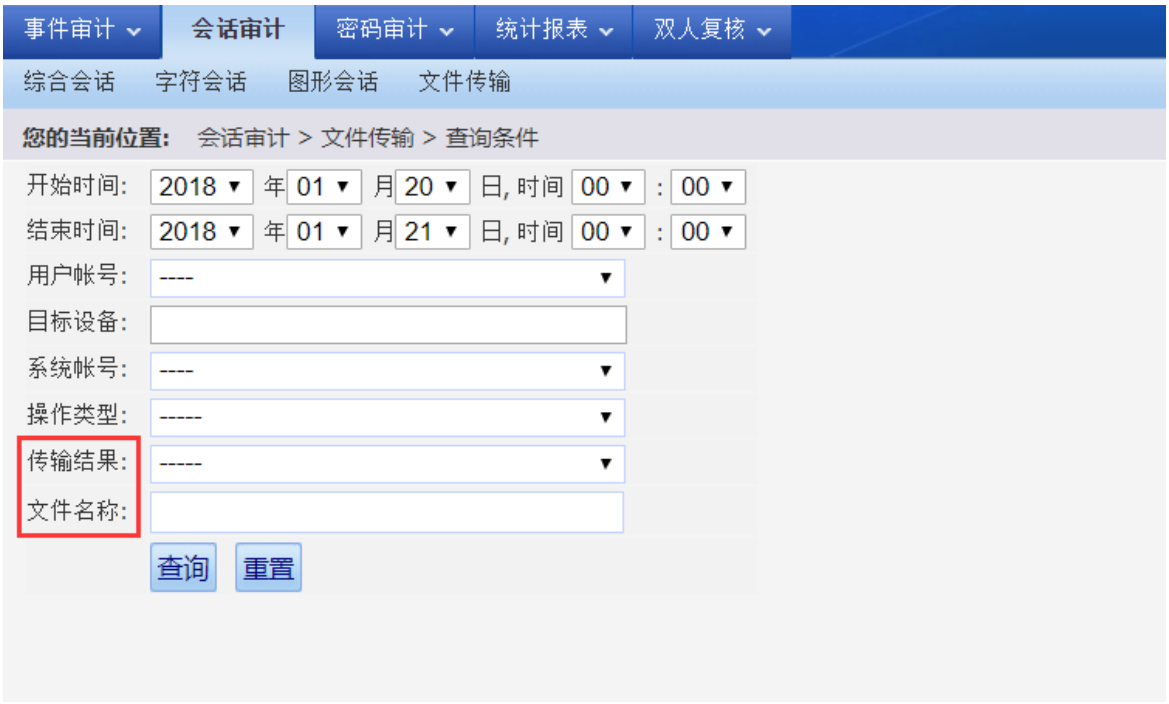
堡垒机的文件传输支持 FTP/SFTP 和 SCP 命令的审计，对上传或者下载的文件信息进行记录。如下图。

图5-21 文件传输示意图



点击图右上角的“文件查询”，可以进入到图形查询界面，主要是针对文件名称的查询，也可针对传输结果进行查询，如下图。

图5-22 文件查询示意图



5.3 统计报表

统计报表这一块内容主要是针对用户登录和操作命令做行为统计，通过报表用户可以很清楚的了解到具体的会话信息统计和命令操作统计。用户还可以按照自身的需求定制报表模板和生成报表任务。

5.3.1 情况总览

在情况总览表中，用户可以根据不同年份，对每个月的操作情况进行统计。

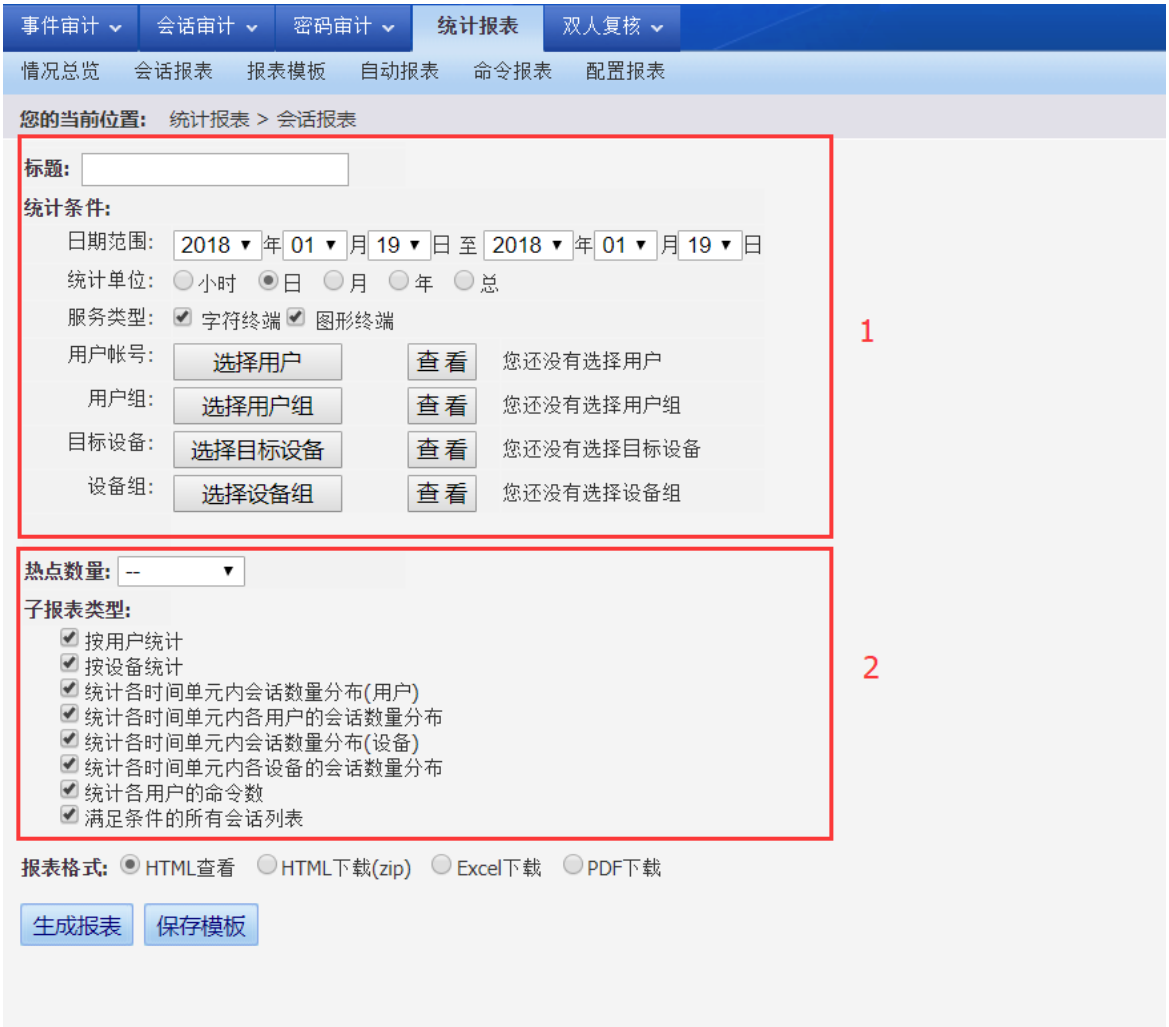
图5-23 情况总览示意图

点击“生成表格”可以把表格下载到本地。审计管理员还可以点击表格中的链接查看详细的记录信息。

5.3.2 会话报表

会话报表功能主要是根据审计需要来定制报表内容，按照不同的条件（时间，用户，设备），不同的审计内容（操作时间，会话长度等信息）来生成用户自己的报表。

图5-24 综合会话报表示意图



1 号区域内用户可以根据时间范围，服务类型，用户和设备来进行条件定制。

2 号区域内用户可以根据定制化的规则来定制报表内容，其中热点表示：客户可设定自己关注的内容，比如说，只想看访问时间长度排在前 10 位的内容，可以按照上图中的设置来选择。

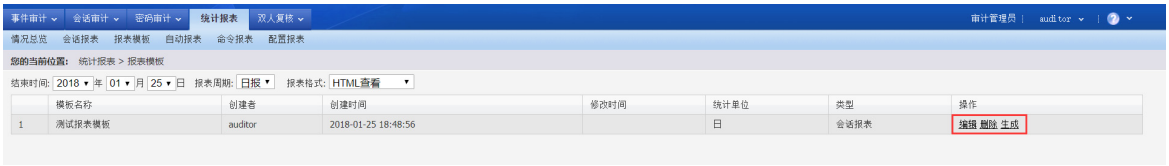
其中，选择 HTML 查看会弹出新的 Web 界面供用户查看，另外三种是根据选择的格式将报表下载到本地。

在选择好报表格式之后，用户就可以点击生成报表来查看了。也可以选择保存模板将本次报表的格式进行保存，保存之后的模板格式会在下一小节中查看到。

5.3.3 报表模板

在会话报表中保存的模板可以在报表模板中查看到，如下图。

图5-25 报表模板示意图



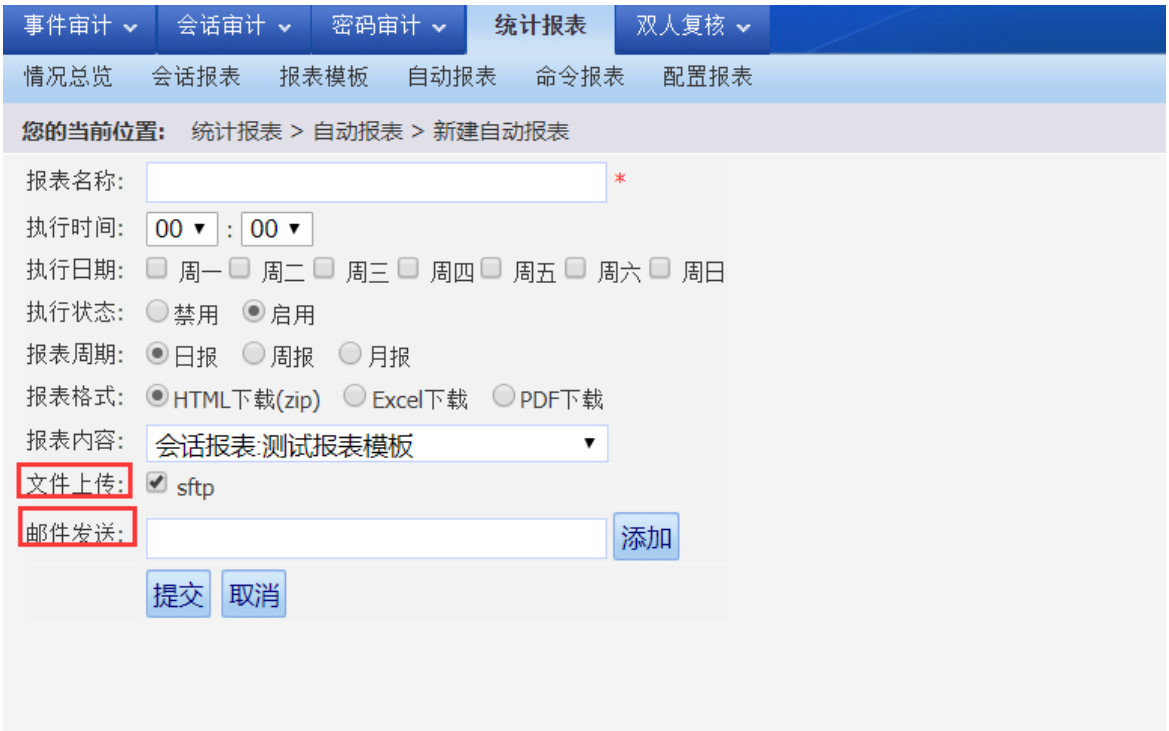
选项说明：

- 报表格式：选择相应的报表格式。
- 操作：
  - 编辑：对该模板进行重新编辑。
  - 删除：删除该模板。
  - 生成：按照模板中的条件和选择的报表格式生成报表。

5.3.4 自动报表

设置报表生成的计划任务，并以文件服务器或者邮件的方式发送。

图5-26 自动报表示意图



5.3.5 命令报表

综合了字符会话和图形会话的命令查询功能，使用上与该两种会话的命令查询相似（具体操作细节可查看）。审计管理员在选择完了用户，设备和系统账号之后，输入查询条件即可得到最终的命令报表：

图5-27 命令报表示意图

6 普通用户访问

6.1 安装所需插件

6.1.1 安装WebClient插件

首次访问堡垒机，系统会有如下提示，请点击下载并安装 WebClient 插件，安装完成后，关闭浏览器再次访问，如果提示还存在，则点击已安装即可。

图6-1 下载 WebClient 客户端

再次访问堡垒机如果有如下提示，点击：已安装即可。

6.1.2 需要安装jre插件情况

当通过堡垒机访问如下远程服务则必须安装 jre 插件，但是对 jre 的版本不再依赖，jre 也不会频繁弹窗。

1. 使用vnc会话

使用 vnc 访问 Linux、Unix 的远程图形会话，则系统需要调用 jre 进行启动远程桌面会话，如下图所示。

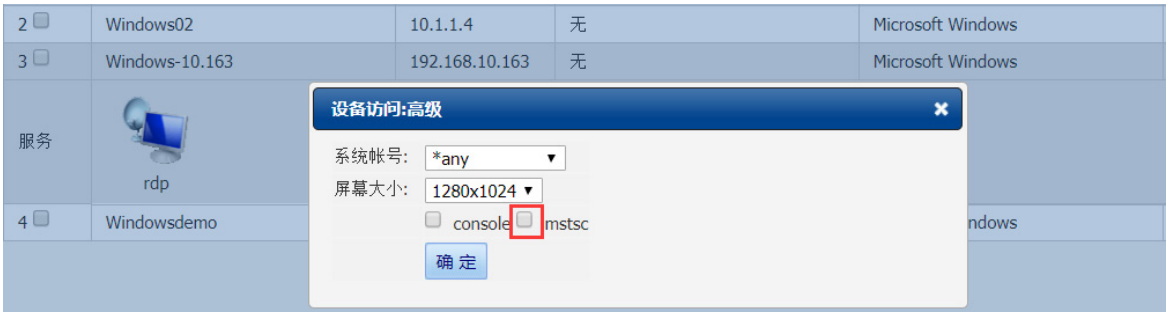
图6-2 使用 vnc 访问 Linux、Unix 的远程图形会话示意图

2. java模式访问Windows设备

堡垒机默认启动 Windows 会话会自动勾选 mstsc，则自动调用本地 mstsc 客户端，不需要 jre 的支持。

当用户访问 Windows 服务器时，鼠标右键弹出高级选项，如果取消 mstsc 复选框，则系统需要调用 jre 进行启动远程桌面会话，如下图所示。

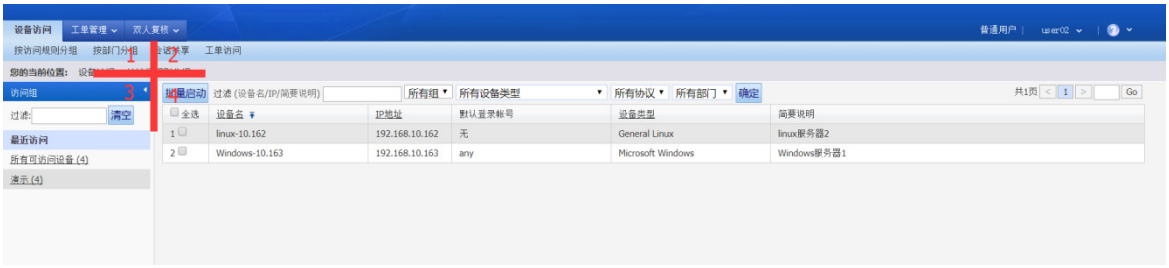
图6-3 java 模式访问 Windows 设备示意图



6.2 如何访问目标设备

6.2.1 页面介绍

图6-4 普通用户页面



为了便于表述我们使用橘黄色标记将页面分为 4 个区域：

左上（1），为菜单栏，包含设备访问、命令复核两个主菜单。

右上（2），用户角色、当前用户和帮助菜单（问号标志），可以切换用户角色、退出登录、设置用户帐号、下载常用工具、查看版本信息。

左下（3），访问规则组列表（多部门时也可为树形部门结构），点击后右下区域可以显示相应的设备。

右下（4），可访问设备清单，默认为最近访问的设备清单，点击左侧规则（部门）可以显示相应的规则（部门）下的设备。

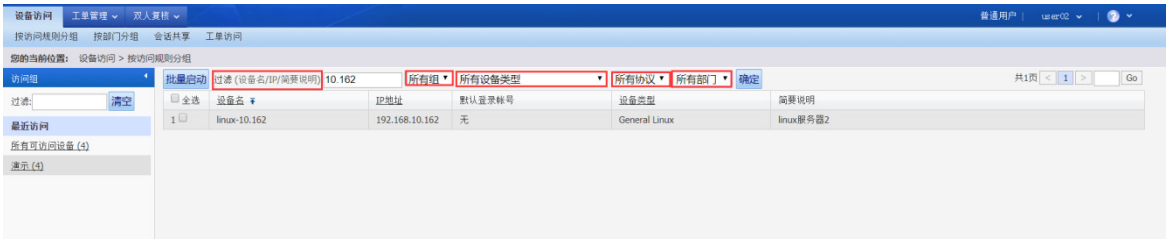
6.2.2 查找设备

用户登录堡垒机后，默认会打开最近访问页面，该页面会列出用户最近已访问过的设备。如果列表中没有，可以通过以下几种方式查找设备：

1. 搜索和过滤设备

设备清单栏上的设备名/IP 搜索框按照设备名或者 IP 进行模糊搜索，或者通过设备类型及协议进行过滤，如下图。

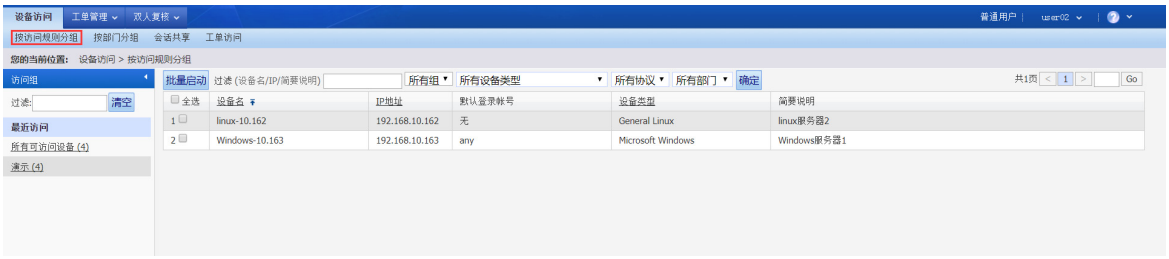
图6-5 搜索设备示意图



2. 按访问规则分组查找设备

在设备访问页面左侧点击相应规则可查看该规则下的设备，如下图。

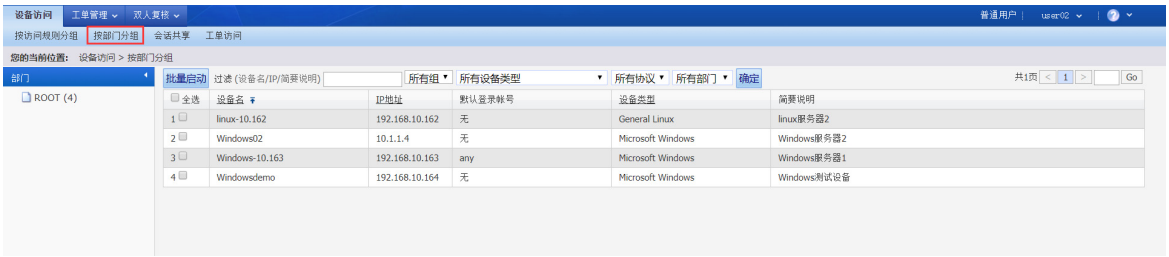
图6-6 按规则查找示意图



3. 按部门分组查找设备

启用了部门分权功能的用户（设备访问页面有“按部门分组”子菜单，默认未开启详情请咨询管理员）也可以选择按照部门查看设备，如下图。

图6-7 按部门查找示意图



6.2.3 访问设备

1. 远程桌面（RDP）会话

对于 Windows 设备，堡垒机支持 Web 方式和远程桌面客户端两种方式访问。

2. Web方式

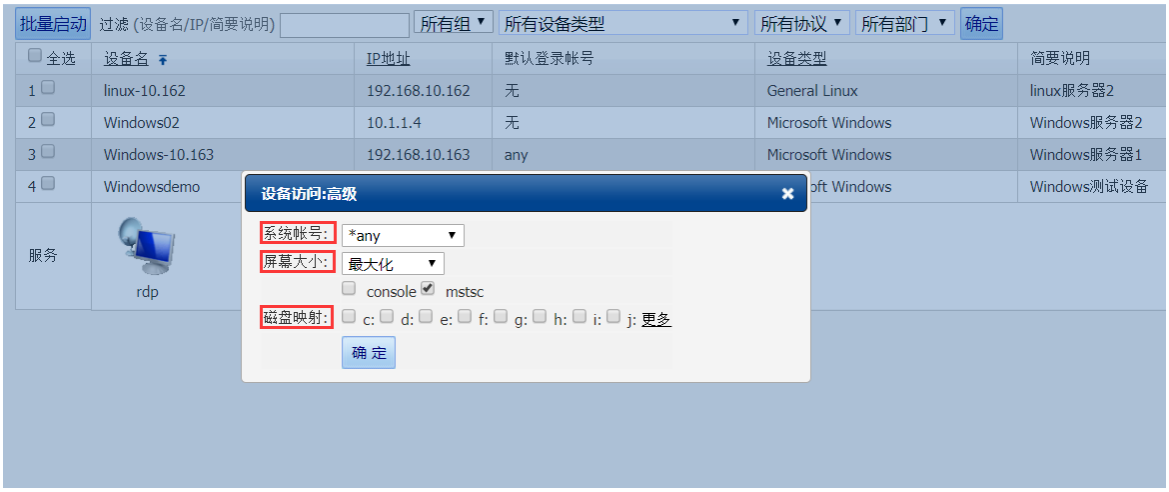
要通过堡垒机使用 RDP 协议，您须先 Web 登录到堡垒机，然后按照以下方法进行：

(1) 查找设备：在设备所在的访问规则组查找设备，或直接过滤搜索要访问的设备。

(2) 选择具体一台设备，点击目设备名后，将立即展开设备在该访问组中所有的服务。

(3) 点击目标设备的 RDP 图标，如果该设备已经访问过，堡垒机将使用上一次访问时登录的系统帐号和启动方式启动会话，如果没有访问过，将弹出高级菜单，如下图。

图6-8 远程桌面（RDP）会话示意图



在弹出的高级选择中可以做相应的调整，如用于登录设备的系统帐号、屏幕大小（分辨率），是否需要映射磁盘等，选择好需要的内容后，点击确定即可登录。

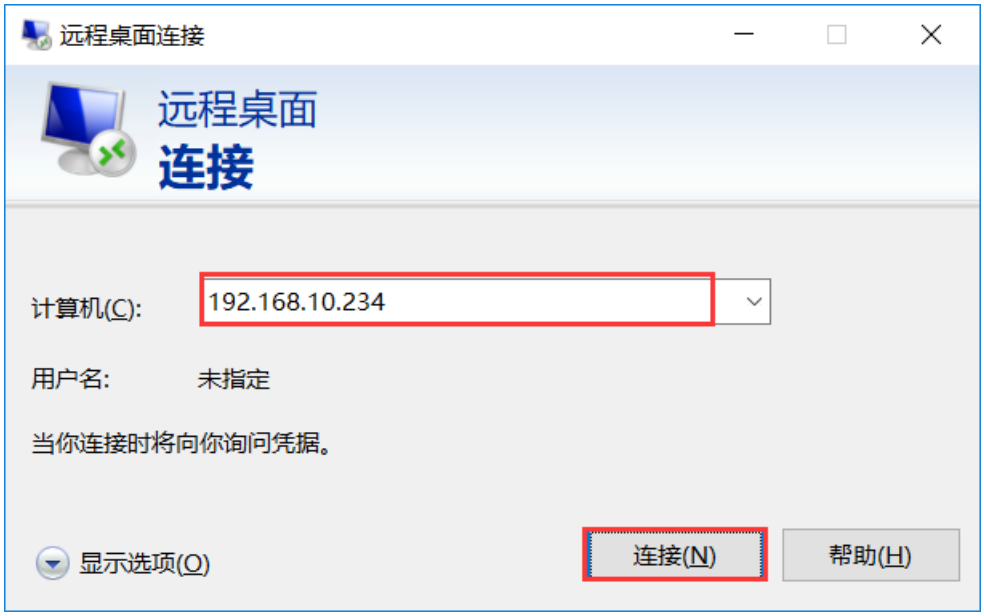
注意

- 1、系统帐号有*号表示为已配置过密码，登录时密码代填，不需要另行输入密码信息。
- 2、如用户已登录过此设备的服务（有默认登录账号），只需鼠标右键击服务图标即可弹出高级选项菜单，选择帐号进行登录。
- 3、如无法看到 console、磁盘映射选项，或连接后无法使用剪切板功能，这表明管理员禁用了相关功能。

3. 远程桌面客户端访问

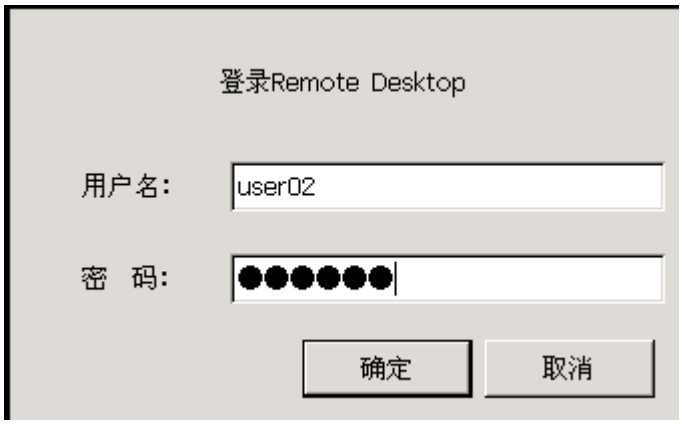
(1) 在运行里输入 mstsc 命令，打开本地远程桌面客户端，如下图。

图6-9 远程桌面客户端访问



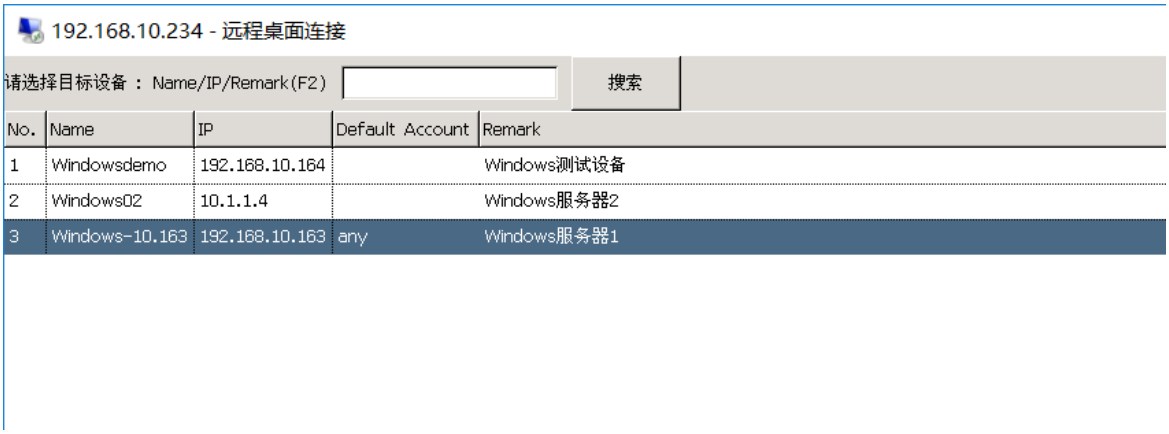
(2) 输入堡垒机的访问地址，点击连接，进入堡垒机登录界面，如下图。

图6-10 远程桌面堡垒机登录界面



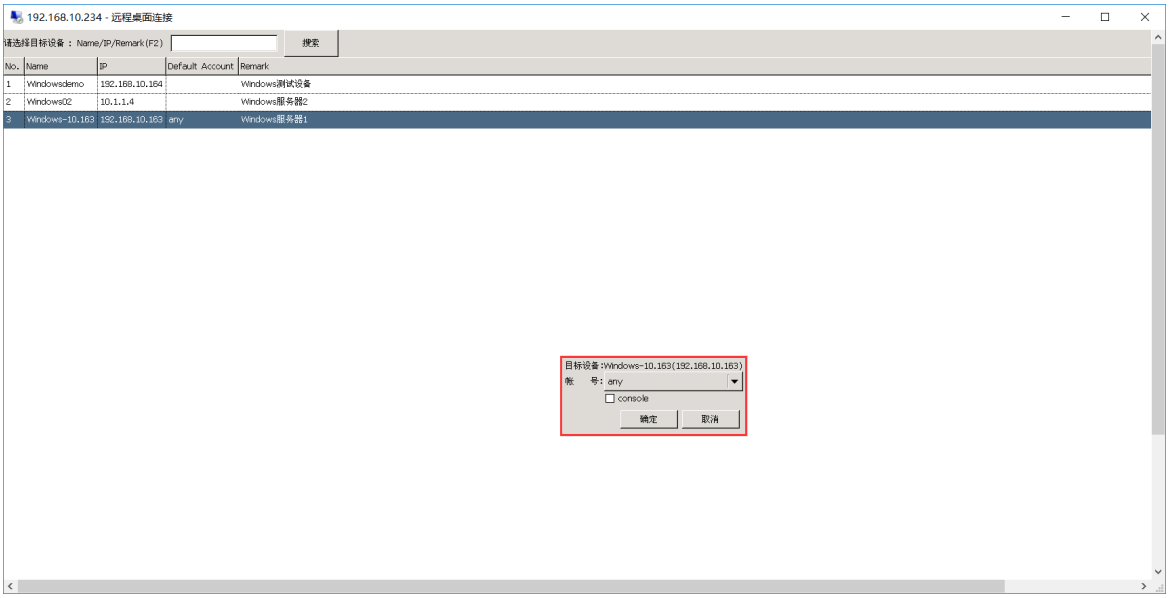
(3) 输入登录堡垒机的用户名和密码，点击确定，进入远程桌面访问界面，如下图。

图6-11 远程桌面客户端访问



(4) 双击要访问的目标服务器，会跳出访问账号选择的界面，如下图。

图6-12 远程桌面客户端访问



选择相应的账号，点击“确定”即可访问目标设备。

4. 应用发布（RDPAPP）会话

Rdpapp 和 RDP 服务一样，如果是第一次登录设备上的服务，会弹出的高级选项，选择好内容后，点击启动即可登录，详情请参考《应用发布配置手册》。

5. 字符设备

对于字符终端设备，堡垒机支持 Web 方式和第三方 SSH 客户端两种方式访问。

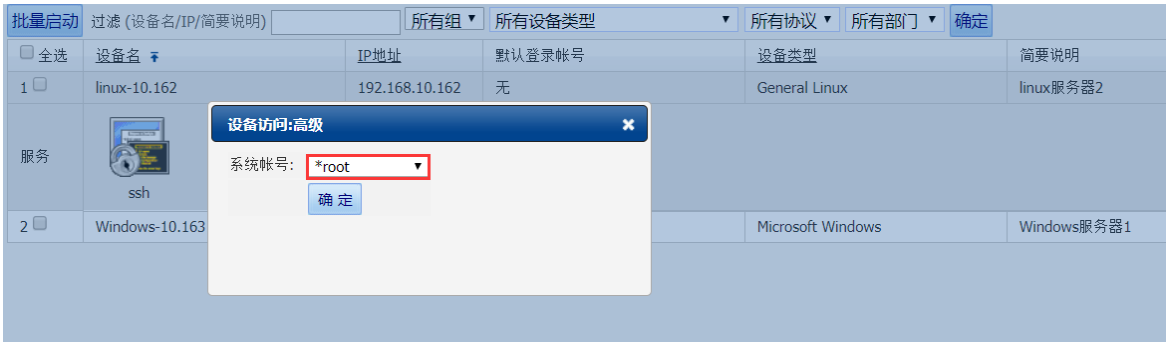
6. Web访问

要使用堡垒机访问 SSH/TELNET 会话，可以先使用 Web 登录到堡垒机，然后按照以下方法进行：

(1) 在设备访问中找到要访问的设备；

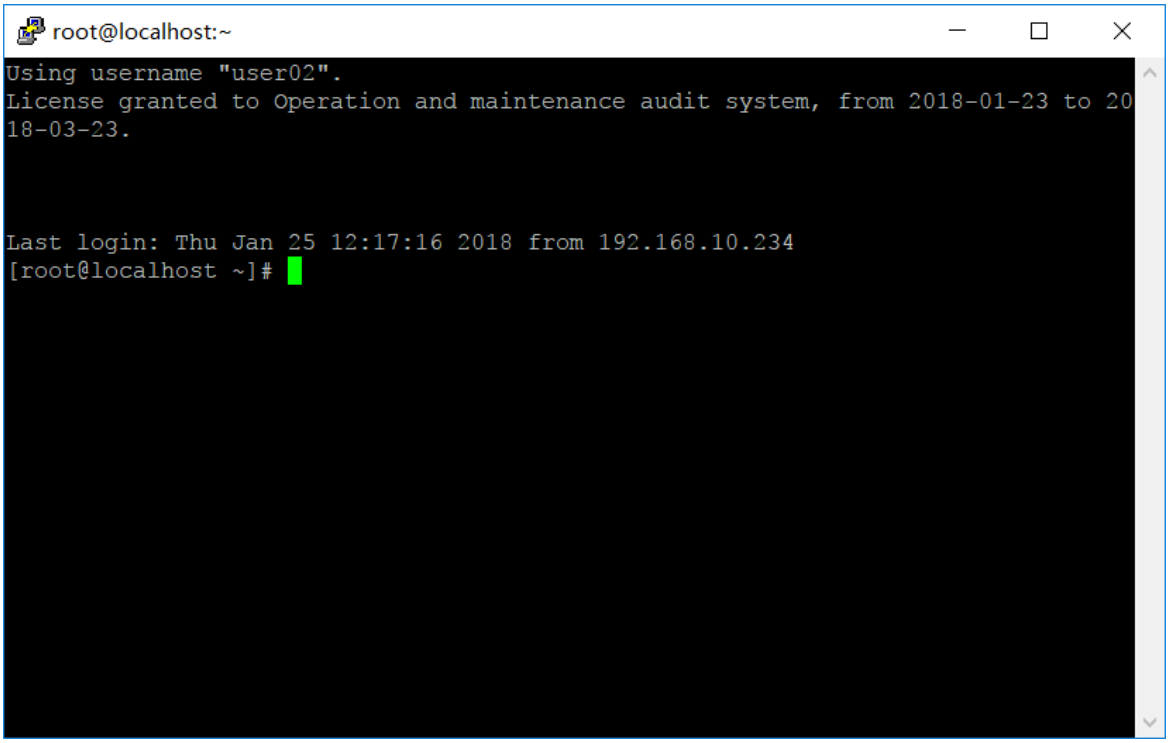
(2) 点击目标设备的服务（协议）图标，如果已经访问过堡垒机将使用上一次访问时登录的系统帐号和启动方式启动会话，如果没有访问过，堡垒机将弹出高级菜单，如下图。

图6-13 字符设备访问示意图



点击确定即可（如下图）。

图6-14 字符设备访问示意图



堡垒机默认调用 Putty 进行字符会话访问，可通过 Web 调用 SecureCRT 和 Xshell 等工具，如果希望通过 Web 启动 SSH 或者 Telnet 会话时直接调用 SecureCRT 或者 Xshell，可以按照以下方法修改个人帐户设定。

- 点击页面右上角帐户名称下的“帐户设置”菜单。
- 输入当前密码，并确定。
- 在“修改个人信息”选项卡中，修改“字符会话客户端”为 SecureCRT 或者 Xshell，完成后点击确定即可。

注意

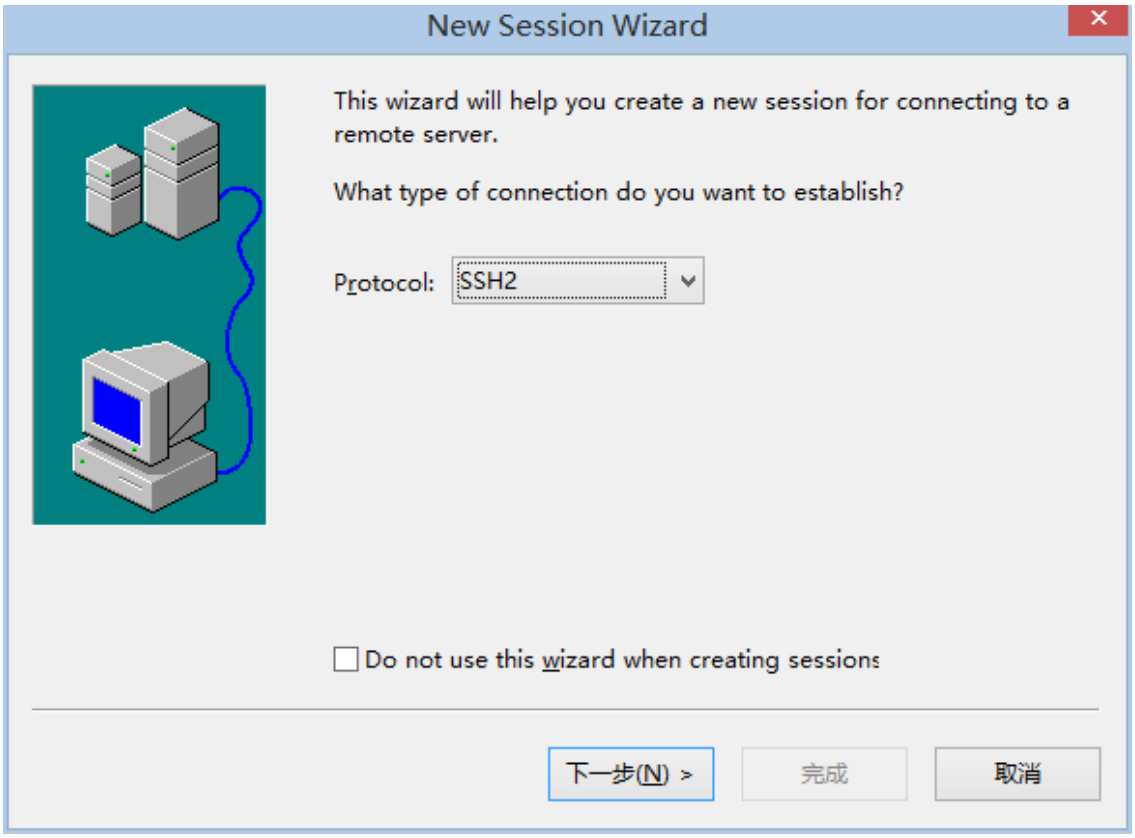
使用 SecureCRT 或 Xshell 作为字符会话客户端，您的计算机上必须已经安装对应的客户端。

7. 使用客户端访问

支持 SSH2 协议的客户端工具均可通过堡垒机访问字符终端设备，如 SecureCRT、PuTTY、XShell 等。我们以 SecureCRT 为例进行介绍。

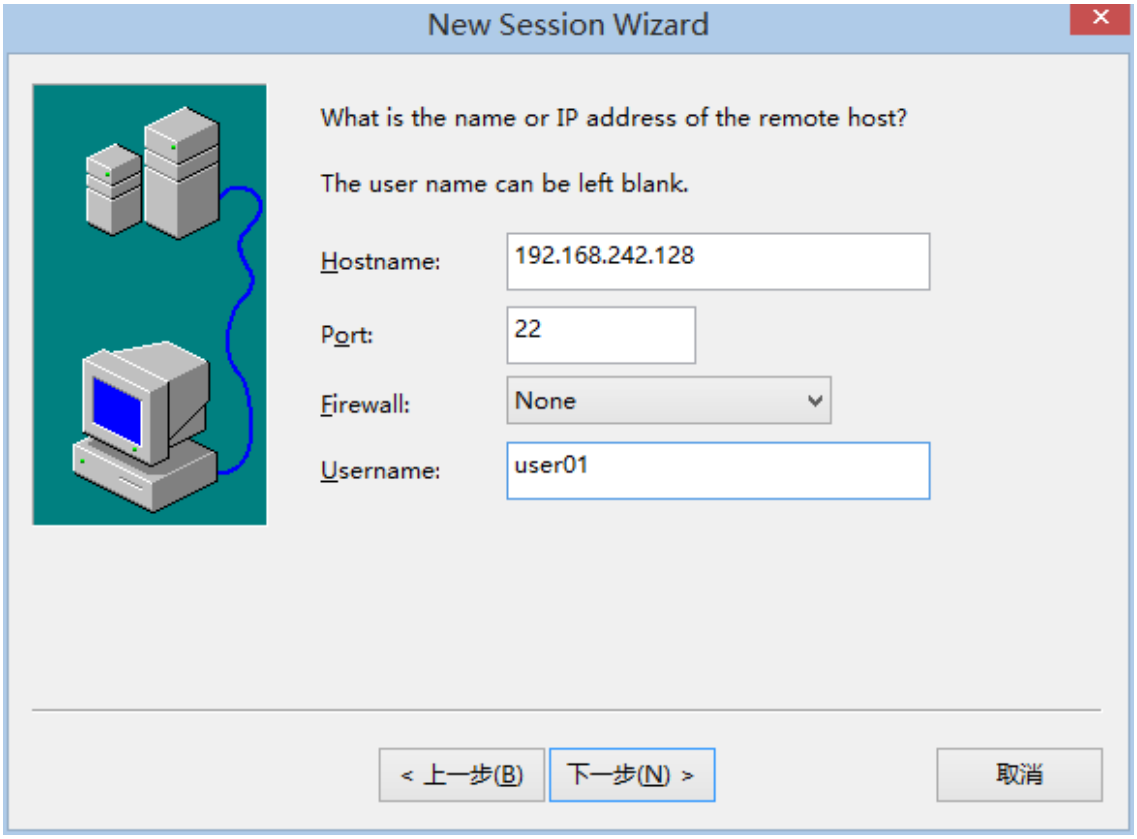
(1) 打开 SecureCRT，新建连接，选择协议为 SSH，如下图。

图6-15 SCRT_SSH 示意图



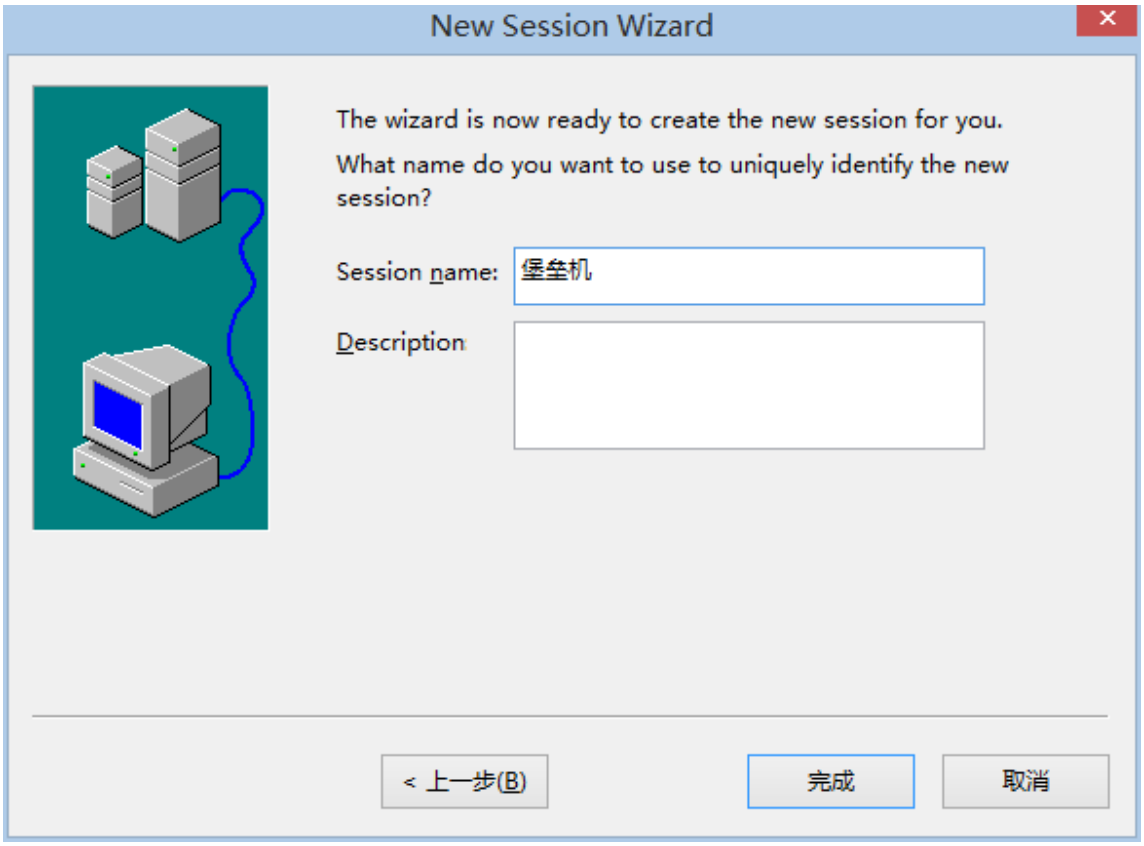
(2) 设置主机名（Hostname）为堡垒机的 IP 或者域名，端口（Port）为 22，用户名（Username）为登录堡垒机的用户帐号。如下图。

图6-16 SCRT_IP 示意图



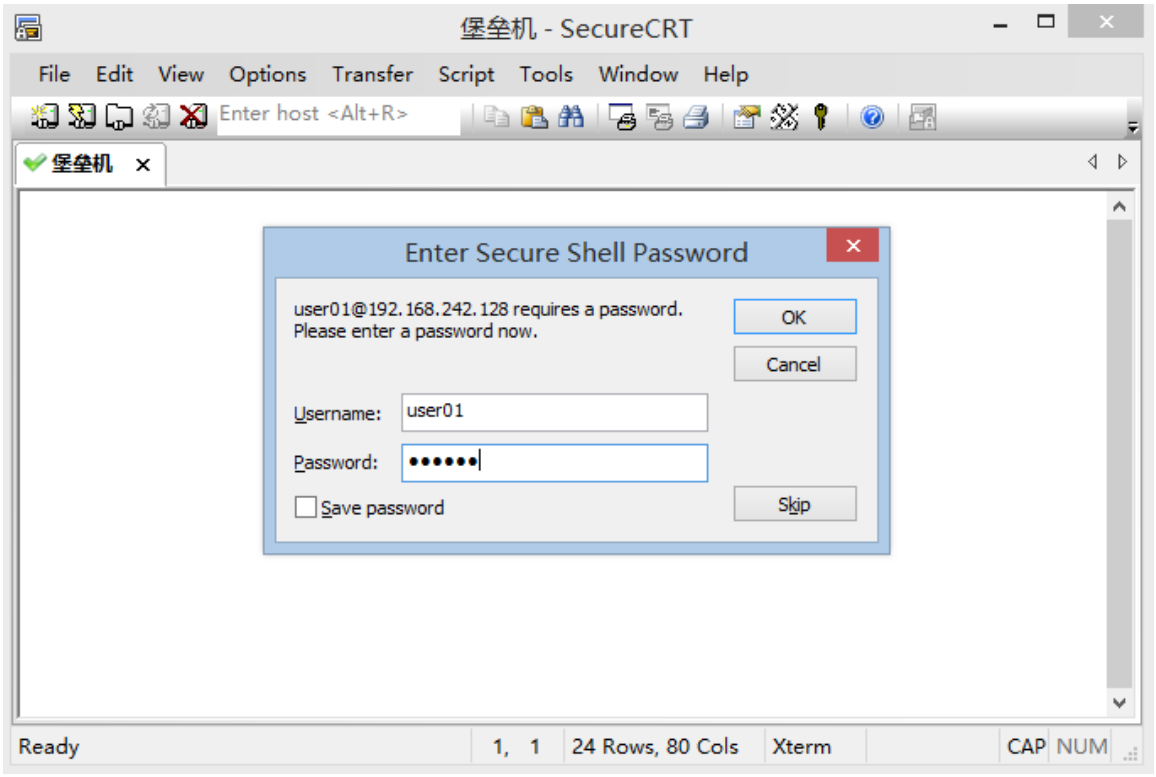
(3) 设置会话名称（Session）为任意希望的名称，如堡垒机：

图6-17 SCRT 示意图



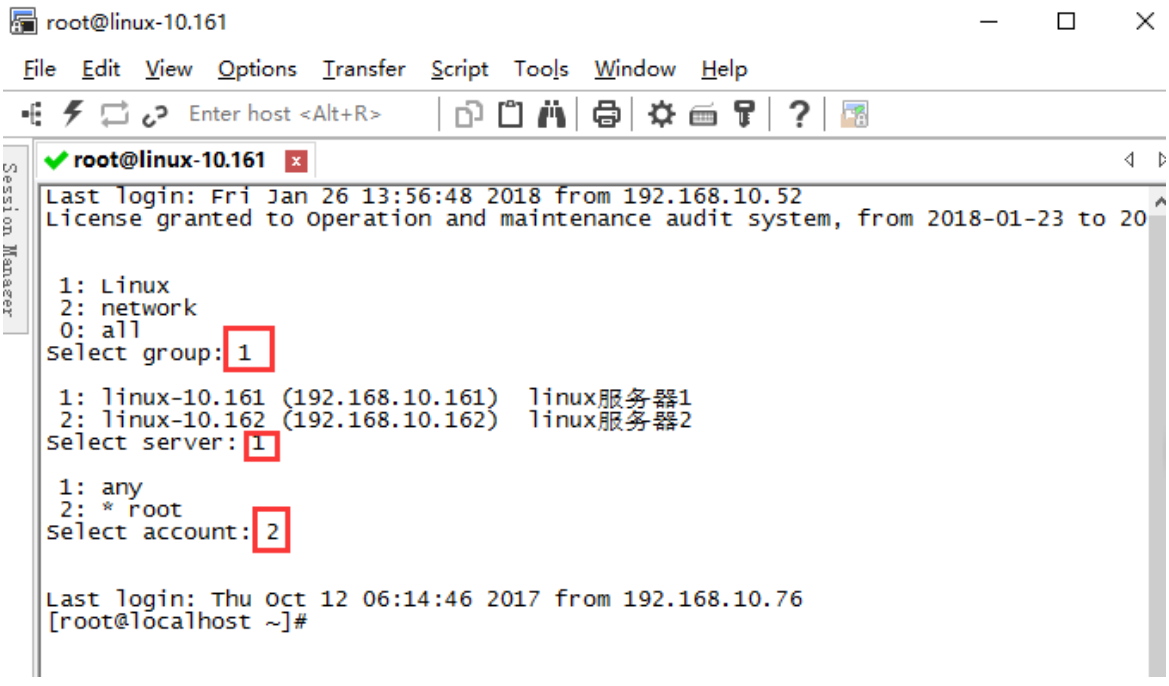
(4) 完成后点击连接（connect），在登录对话框中输入的密码,点击“OK”，即可登录。

图6-18 SCRT_LOGIN 示意图



(5) 登录后依次选择规则、设备和系统帐号后即可访问目标设备。

图6-19 SCRT_LOGIN 示意图



8. 会话共享

会话共享是指两个用户共享同一个图形会话，用于协同任务或者远程协助。

(1) 支持的会话类型

- 支持非 mstsc 方式的 rdp 和 rdpapp 会话， vnc 会话（使用密码代填）。
- 不支持任何字符会话和 mstsc 模式的 rdp 和 rdpapp 会话。

(2) 如何发出邀请？

- 会话要求必须有一个符合支持的会话列表中的活动会话；
- 打开“设备访问”-“会话共享”中的我的会话中找到要共享的会话，点击“邀请”；
- 选择一个用户后点击“发出邀请”；
- 通知本邀请对象。

(3) 如何加入共享的会话

- 在“设备访问”-“会话共享”页面我收到的邀请中找到需要加入的会话，点击“加入”
- 会话启动后即可以多个人同时操作一个会话。

6.3 账户设置

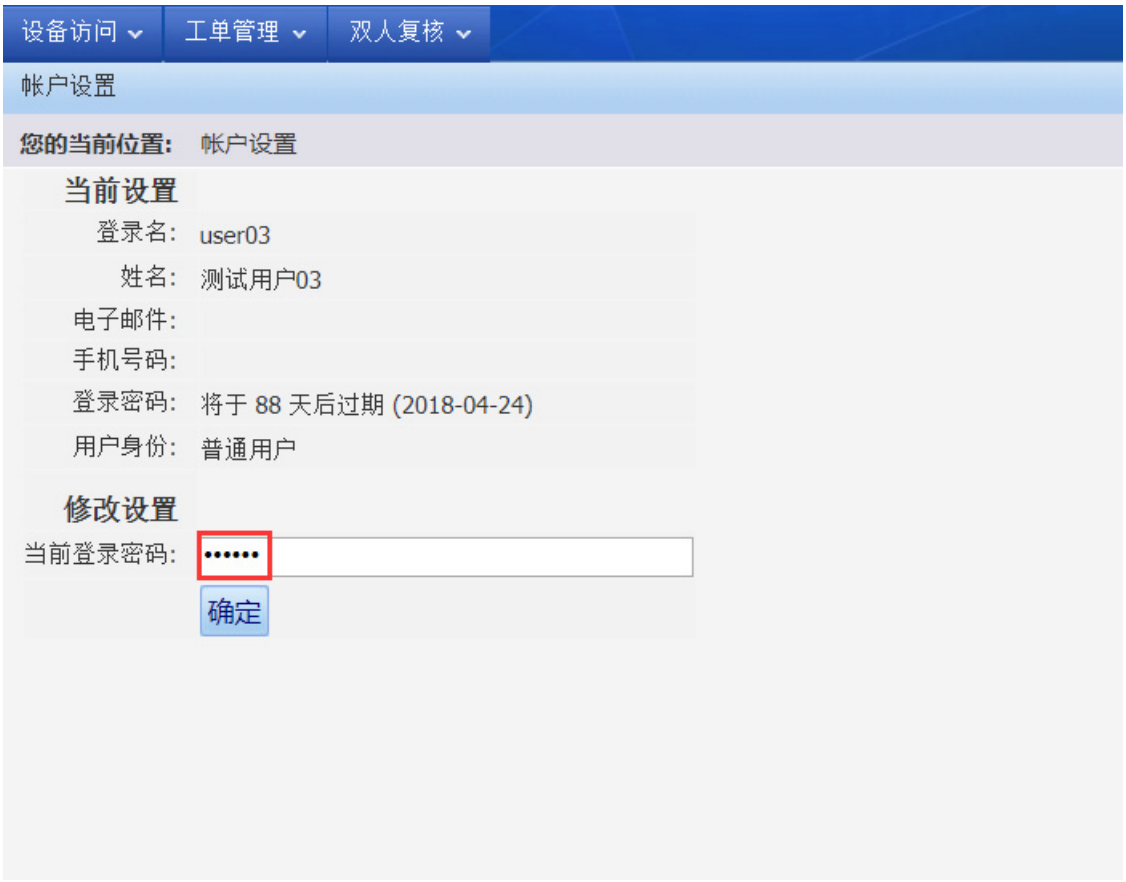
6.3.1 个人信息修改

普通用户可以根据实际情况修改自己的相关信息或做适合自己习惯的个性化定制等，具体的操作过程是右上方用户名下拉菜单账号设置，如下图所示。

图6-20 账户设置示意图

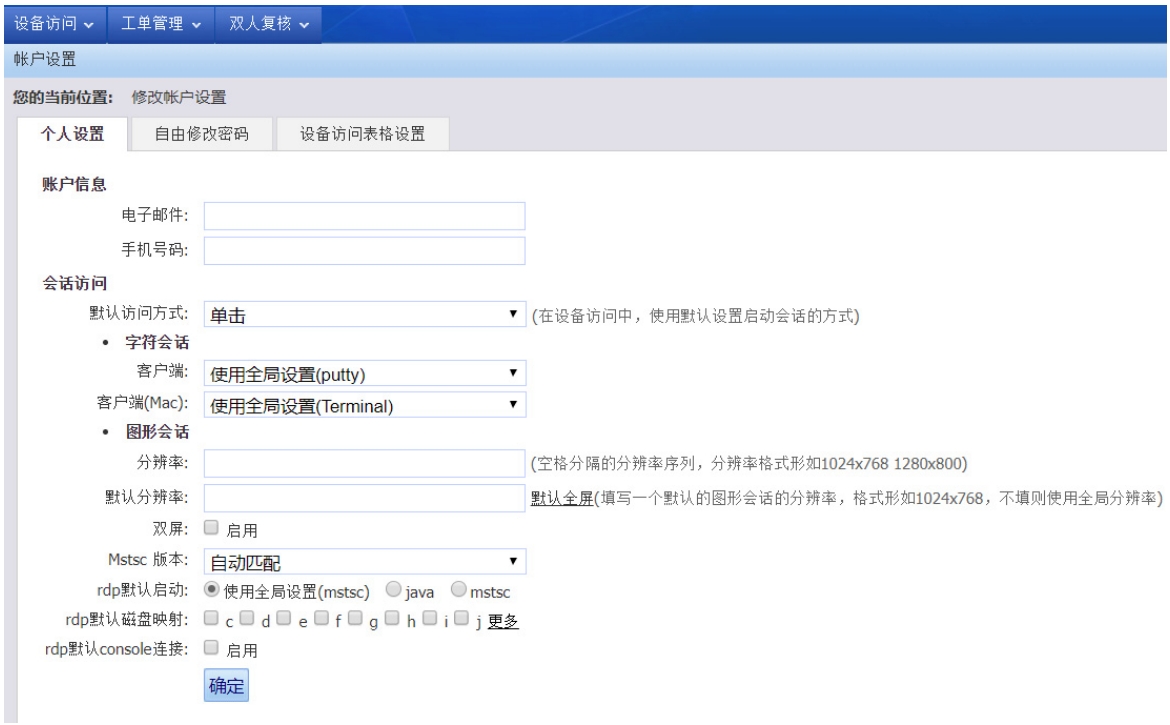
打开账户设置后，会再次验证用户密码，如下图。

图6-21 再次验证用户密码示意图



输入正确的当前登录密码后，就可以进入账号设置页面，在修改个人信息界面中可以修改自己的电子邮件信息、手机号码、默认访问方式、字符会话客户端访问方式、字符终端尺寸、图形会话分辨率等，如下图。

图6-22 个人信息界面示意图



参数解释：

- 字符会话客户端有以下几种：
  - Putty：使用 putty 链接方式，调用自带的 Putty 程序。
  - Scrt：使用 scrt 链接方式，调用本地客户安装的 SecureCRT 程序。
  - Xshell：使用 scrt 链接方式，调用本地客户安装的 Xshell 程序。
- 图形会话默认有两种启动方式：JAVA 和 MSTSC 方式，可根据个人使用习惯选择。
- 设备默认访问方式：分为单机和双击。 这里是指设备访问中直接鼠标左击服务名称，是需要鼠标双击还是单击来启动相应服务。

6.4 密码修改

普通用户还可以修改自己的密码信息，如下图所示。

图6-23 密码修改示意图

手动修改密码需要符合上图红框内所描述，且手动修改密码的规则会根据策略配置设置而改变。

6.5 常见问题

6.5.1 账户密码有效期

默认情况下，帐号有效期为 1 年，密码有效期为 90 天，堡垒机会提前 10 天提醒密码过期时间，请及时修改密码。

6.5.2 如何部署SSL证书

浏览器未检测到有效的安全证书，会在登录页面前弹出提醒页面询问是否知晓存在的问题。

用户可以通过安装部署有效证书解决问题。

(1) 从堡垒机下载并安装。请点击堡垒机页面右上角问号按钮，在“工具下载”中点击“下载根证书”。

图6-24 下载证书示意图

(2) 在保存证书后，双击证书进行安装，选择“将所有的证书放入下列存储”，然后点击“浏览”，选择“受信任的根证书颁发机构”，确认后选择下一步安装。

图6-25 安装证书示意图

(3) 重启浏览器后，就可以正常登录堡垒机。

6.5.3 字符访问乱码

出现字符乱码时，可以尝试修改编码类型，如下图所示。

图6-26 修改编码示意图