堡垒机

用户使用指南

天翼云科技有限公司

前言

概述

感谢您选择天翼云的安全产品。本手册详细描述了堡垒机的配置方法，包括快速入门、Web 配置页面简介、控制板、部门、用户、资产、授权、策略、运维、审计、工单、任务、系统等。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用堡垒机的人员，包括系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP 等基础网络通讯协议
- 数据库、服务器、路由器、交换机等常见设备（系统）的基本工作原理和配置、操作
- 堡垒机及网络安全运维工具的基本工作原理和操作

格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如：“在菜单栏选择‘**系统状态**’进入**系统状态**页面，选择**接口状态**页签”。
< >	Web 界面上的按钮。例如：“微信认证失败，点击<**我要上网**>不弹出微信认证界面”。
➢	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等）。例如：“在菜单栏选择‘**策略配置➢认证管理➢认证策略**’查看是否开启了认证策略”。
斜体字	可变参数，必须使用实际值进行替代。例如：“在浏览器地址栏输入‘http://*管理 IP*’，回车后进入系统 Web 管理平台登录页面”。

本手册图标格式约定如下。

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

修订记录

日期	修订版本	修改记录
2025-01-20	01	优化文档结构和部分描述。
2023-06-30	01	初次发布。

目录

1 快速入门 1
1.1 产品简介 1
1.2 登录系统 2
1.3 主要业务流程 2
2 部门 3
2.1 新建部门 3
2.2 安全码管理 3
2.3 修改部门 5
2.4 删除部门 5
3 用户 7
3.1 角色管理 7
3.1.1 新建角色 7
3.1.2 修改角色 8
3.1.3 删除角色 10
3.2 用户管理 10
3.2.1 新建用户 10
3.2.2 导入用户 12
3.2.3 批量修改用户信息 13
3.2.4 用户配置 13
3.2.5 SSH 公钥管理 17
3.2.6 查看已授权主机 18
3.2.7 查看已授权应用 18
3.3 用户组管理 19
3.4 动态令牌管理 20
4 资产 21
4.1 主机管理 21
4.1.1 新建主机 21
4.1.2 导入主机 23

4.1.3 导出主机 25
4.1.4 修改主机 25
4.1.5 查看已授权用户信息 31
4.1.6 选择要展示的主机列表信息 32
4.1.7 查看指定时间段内未被运维的主机 32
4.2 帐户管理 33
4.2.1 主机帐户 33
4.2.2 共享帐户 33
4.3 主机组管理 35
4.4 帐户组管理 36
4.5 应用管理 37
4.5.1 新建应用 37
4.5.2 导出应用 48
4.5.3 导入应用 48
4.5.4 应用授权与运维 49
4.6 应用帐户组管理 50
5 授权 52
5.1 运维规则 52
5.1.1 新建运维规则 52
5.1.2 修改运维规则 53
5.2 审批规则 56
5.3 未授权登录审核 58
6 策略 59
6.1 主机命令策略 59
6.1.1 新建主机命令策略 59
6.1.2 修规主机命令策略 60
6.1.3 复制主机命令策略 61
6.1.4 删除主机命令策略 62
6.1.5 关联运维规则 62

6.2 数据库控制策略 63
6.2.1 新建数据库控制策略 63
6.2.2 其他操作 64
7 审计 66
7.1 会话审计 66
7.2 事件审计 68
7.3 审计规则 69
8 工单 71
8.1 创建工单 71
8.1.1 创建运维工单 71
8.1.2 创建密码工单 72
8.1.3 其他操作 74
8.2 工单审批 75
9 运维 76
9.1 主机运维 76
9.1.1 运维配置 76
9.1.2 主机运维配置 78
9.1.3 应用运维 83
9.1.4 工单运维 84
9.1.5 未授权登录 85
9.2 实时监控 86
9.3 命令审批 86
9.4 运维审批 87
9.5 运维报表 87
9.5.1 查看运维报表 88
9.5.2 导出报表 88
9.5.3 报表自动发送 88
10 任务 90
10.1 改密计划 90
10.1.1 创建改密计划 90

10.1.2 修改改密计划 92
10.1.3 管理关联主机账户 93
10.1.4 管理关联应用帐户 94
10.1.5 一键检测帐户删除状态 94
10.1.6 查看托管账户信息 94
10.2 自动运维 96
10.3 资产巡检 98
10.3.1 创建资产巡检任务 98
10.3.2 执行资产巡检任务 100
11 系统 101
11.1 网络配置 101
11.1.1 基础信息设置 101
11.1.2 Web 配置 106
11.1.3 静态路由 109
11.1.4 SNMP 配置 109
11.1.5 集群配置 110
11.1.6 IP 源防护 112
11.2 认证管理 113
11.2.1 安全配置 113
11.2.2 远程认证 116
11.2.3 双因子认证 118
11.2.4 第三方 HTTP 平台认证 122
11.2.5 单点登录 124
11.3 系统配置 126
11.3.1 运维配置 127
11.3.2 告警配置 129
11.3.3 语言和界面 132
11.3.4 功能设置 133
11.3.5 改密脚本 138

11.3.6 API 访问控制 139
11.4 存储管理 140
11.4.1 数据归档 140
11.4.2 网盘管理 142
11.4.3 日志备份 145
11.4.4 NAS 146
11.4.5 审计数据升级 147
11.4.6 录像导出 148
11.5 操作日志 149
11.6 系统报表 151

1 快速入门

1.1 产品简介

天翼云堡垒机是一款统一安全运维管理与审计产品。产品集身份认证（Authentication）、帐户管理（Account）、控制权限（Authorization）、日志审计（Audit）功能于一体。支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，具备全方位运维风险控制能力，可满足各类法律法规（如等级保护、赛班斯法案 SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001 等）对运维审计的要求。

堡垒机的主要功能请参见下表。

功能	描述
认证&授权	
双因子认证	◆ 内置手机 APP 认证（谷歌动态口令验证）、OTP 动态令牌、USBkey 双因素认证引擎。 ◆ 提供短信认证、AD、LDAP、RADIUS 认证接口。 ◆ 支持多种认证方式组合。
权限管理	系统预置多种用户角色：超级管理员、部门管理员、运维管理员、审计管理员、运维员、审计员、系统管理员和密码管理员。每种用户角色的权限均不同，且可自定义用户角色。
集中授权	梳理用户与主机之间关系，提供一对一、一对多、多对一、多对多的灵活授权模式。
单点登录	托管主机的帐户和密码，运维人员直接点击<**登录**>即可成功自动登录到目标主机中进行运维操作，无需输入主机的帐户和密码。
自动学习	运维人员通过堡垒机成功登录目标主机后即可自动录入主机信息，减轻管理员配置主机信息、用户与主机关系的工作量。
运维&审计	
运维协议支持	◆ 支持管理 Linux/Unix 服务器、Windows 服务器、网络设备（如思科/H3C/华为等）、文件服务器、Web 系统、数据库服务器、虚拟服务器、远程管理服务器等。 ◆ 兼容 Xshell、XFTP、SecureCRT、MSTSC、VNC Viewer、PuTTY、WinSCP、FlashFXP、SecureFX 等多种客户端工具。
统一审计	◆ 对所有操作进行详细记录，提供综合查询；审计日志可在线或离线播放，自动备份归档。 ◆ 审计内容包括图形、字符、文件、应用、SQL 语句等会话及应用会话。
浏览器客户端运维	◆ 基于 H5 技术实现浏览器客户端运维，无需安装本地工具，直接通过浏览器打开运维界面。 ◆ 支持通过 SSH、Telnet、Rlogin、RDP、VNC 协议的 Web 客户端运维。
文件传输审计	◆ 记录所有操作会话，包括在线监控、实时阻断、日志回放、起止时间、来

功能	描述
	源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容。 ◆ 完整备份传输文件，为上传恶意文件、拖库、窃取数据等危险行为提供查询依据。
自动运维	实现自动化的运维任务并将执行结果通知相关人员。
资产管理	支持主机、主机组、帐号、帐号组、应用等多种资产类型。
命令控制	集中命令控制基于不同主机、不同用户设置不同的命令控制策略，包括命令阻断、命令黑名单、命令白名单、命令审核四种动作。
工单流程	运维人员向管理员申请需要访问的设备，选择条件包括设备 IP、设备帐户、运维有效期、备注事由等，运维工单以邮件方式通知管理员。
其他	
系统自审	对系统自身变化信息进行审计，形成系统分析报表。
冗余架构	结合端口聚合技术、RAID 技术和 HA 技术，实现三重冗余备份的高可用架构。
API 接口	◆ 提供用户、资产、授权的增删改查等 API 接口。 ◆ 允许第三方平台调用 API 接口，实现用户、资产、权限自动同步。

1.2 登录系统

产品仅支持从天翼云平台页面单点登录堡垒机系统的管理平台。

1.3 主要业务流程

系统的主要业务流程包括：

步骤 1. 创建部门：超级管理员或部门管理员创建部门。详情请参见新建部门。

步骤 2. 创建用户：创建系统用户，例如运维员等。详情请参见新建用户。

步骤 3. 创建主机：将主机添加至系统后，系统才能对主机的运维进行审计。详情请参见主机管理。

步骤 4. 创建运维规则：授权运维员可以登录主机进行运维。详情请参见运维规则。

步骤 5. 运维员对主机进行维护：运维员通过系统登录主机并对主机进行维护。详情请参见主机运维。

步骤 6. 创建审计规则：审计管理员创建审计规则，赋予审计员审计主机的权限。详情请参见审计规则。

步骤 7. 审计员对主机的运维操作进行审计：审计员进行会话审计。详情请参见会话审计。

步骤 8. 操作录像数据归档配置：对会话录像进行归档。详情请参见数据归档。

2 部门

超级管理员或系统管理员在“**系统➤系统配置➤功能设置**”页面中开启**部门管理**功能后，才能配置**部门**功能。

在堡垒机中，部门是一种虚拟组织结构，用于将用户、主机等资源划分到不同的逻辑分区。每个部门都可以包含资产、用户、用户组和子部门，由部门管理员统一管理。不同部门之间的数据和权限相互隔离，部门管理员无法查看或管理本部门之外的数据。

2.1 新建部门

步骤 1. 在系统菜单栏选择“**部门**”，进入**部门**页面，点击<**新建部门**>。

步骤 2. 选择部门所属的上级部门并输入部门名称，点击<**创建部门**>完成创建。

部门创建成功后将加入到部门管理列表，点击部门名称前 ▸ 图标展开查看选中部门下的子部门及各级子部门中的用户和资产信息；点击**用户数**和**资产数**列下的数字跳转到**用户管理**和**主机管理**页面查看用户和资产，更多信息请参见用户管理和主机管理。

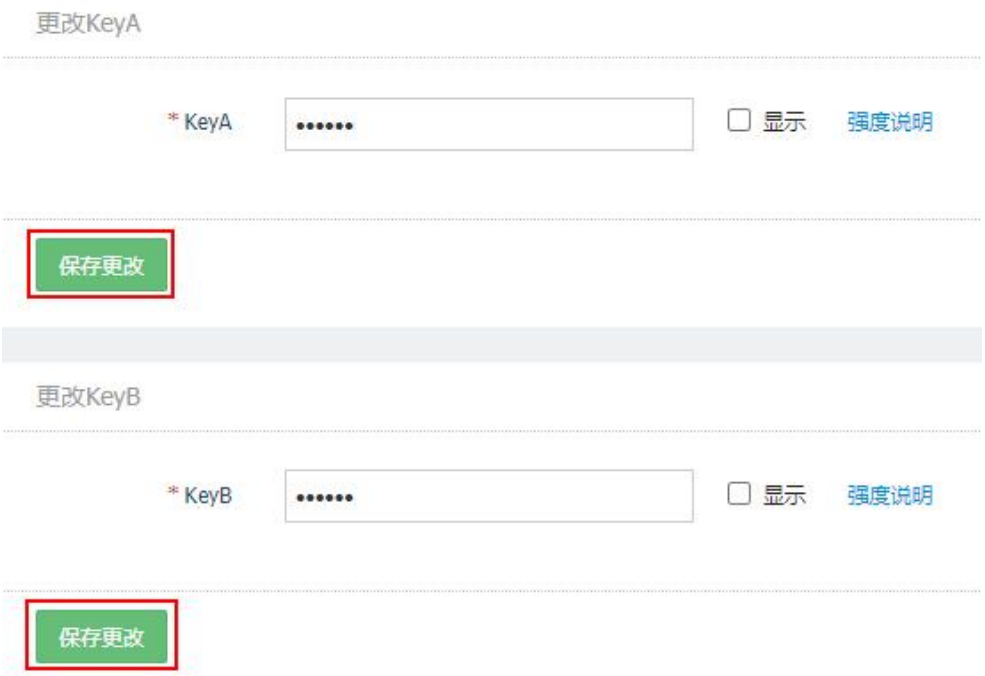
2.2 安全码管理

安全码是部门导出主机密码文件 zip 包的加密密码，分为两部分。运维管理员可以设置安全码前半段（KeyA）；密码管理员可以设置安全码后半段（KeyB）；超级管理员和部门管理员可以对安全码的前

后两部分进行设置。安全码机制可以防止管理员权限过于集中，通过分权机制保障密码文件的安全性。关于密码文件导出的详细信息，请参见改密计划。

步骤 1. 在系统菜单栏选择“**部门**”，进入**部门**页面，在部门列表的**安全码**列下点击<**管理**>。

步骤 2. 在安全码页面设置 KeyA，点击<**保存更改**>，设置 KeyB，点击<**保存更改**>。点击<**强度说明**>可查看安全码的强度说明。



安全码设置完成后，可选择将 KeyA 和 KeyB 发送至指定邮箱，有关邮箱配置的更多信息，请参见邮件配置。

2.3 修改部门

步骤 1. 在部门树目录中点击部门（如“部门 1”）。

步骤 2. 进入**部门信息**页面，修改部门名称，点击<**保存更改**>即可修改部门。

2.4 删除部门

超级管理员可删除除用户根之外的所有部门；部门管理员可删除本部门下的子部门。

删除部门会同时删除其中的用户、用户组、主机、主机组、帐户组、应用、改密计划、自动运维任务、运维授权、审计规则等数据，请谨慎操作。

步骤 1. 选择要删除的部门，点击<**删除部门**>。

步骤 2. 在弹出的对话框中点击<**确定**>即可删除部门。

3 用户

在堡垒机中，用户必须隶属于某一部门，超级管理员或者部门管理员给用户指定角色后，用户便具备相应的权限，可在系统中对指定资源进行管理。

3.1 角色管理

有权限的用户（超级管理员或部门管理员等）可自定义角色并给其赋予相应权限。支持创建、编辑和删除自定义角色。系统内置的 9 种角色不支持编辑和删除操作。

3.1.1 新建角色

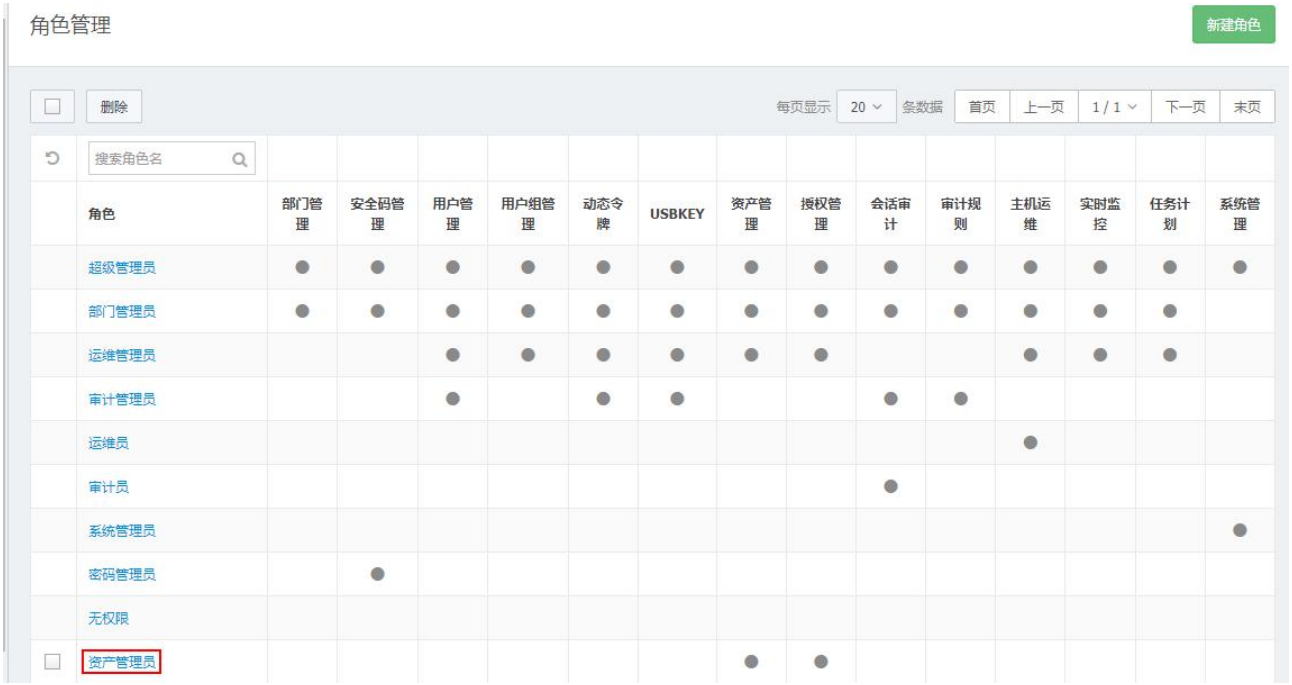
步骤 1. 在系统菜单栏选择“**用户➤角色管理**”，进入**角色管理**页面。点击<**新建角色**>，进入**新建角色**页面。

步骤 2. 在**新建角色**页面输入自定义的角色名称，勾选需要赋予的权限，点击<**创建角色**>。

创建自定义角色后，可新增自定义角色用户，具体请参见新建用户。

3.1.2 修改角色

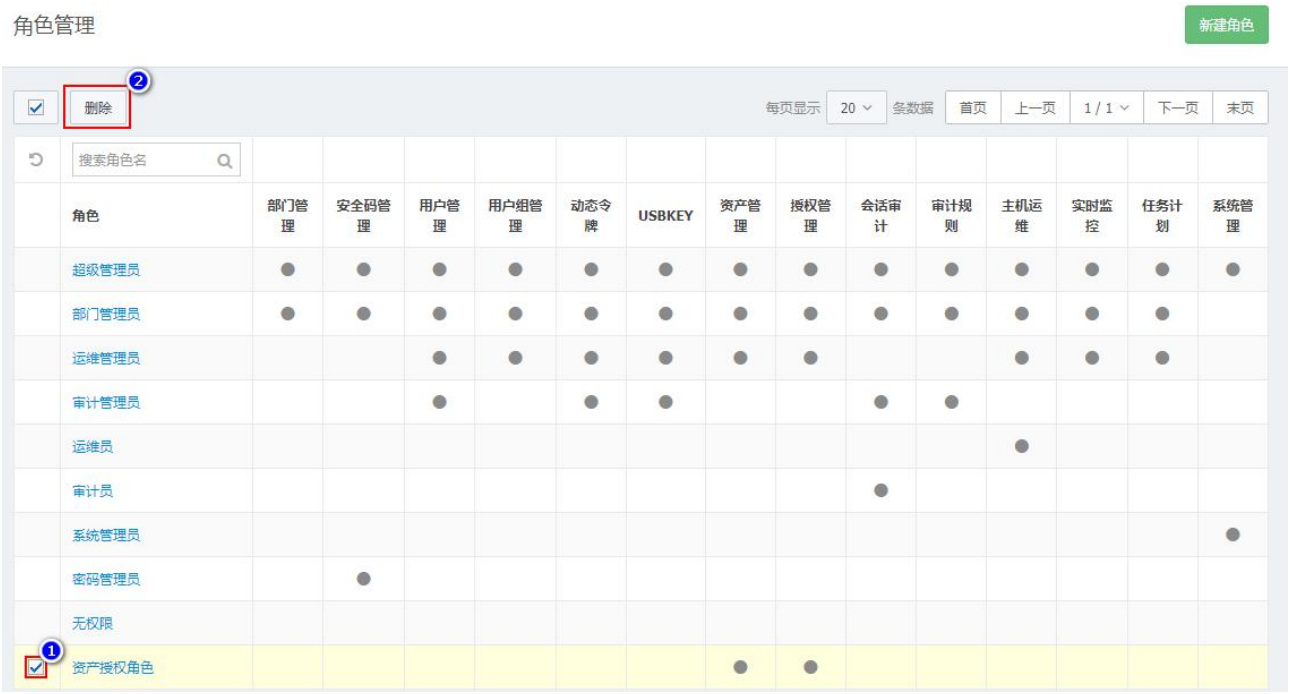
步骤 1. 在**角色管理**页面点击自定义角色。



步骤 2. 在**角色信息**页面可修改角色名称和权限，点击<**保存更改**>。

3.1.3 删除角色

在**角色管理**页面勾选需要删除的自定义角色（可勾选多个），点击<**删除**>即可删除自定义角色。



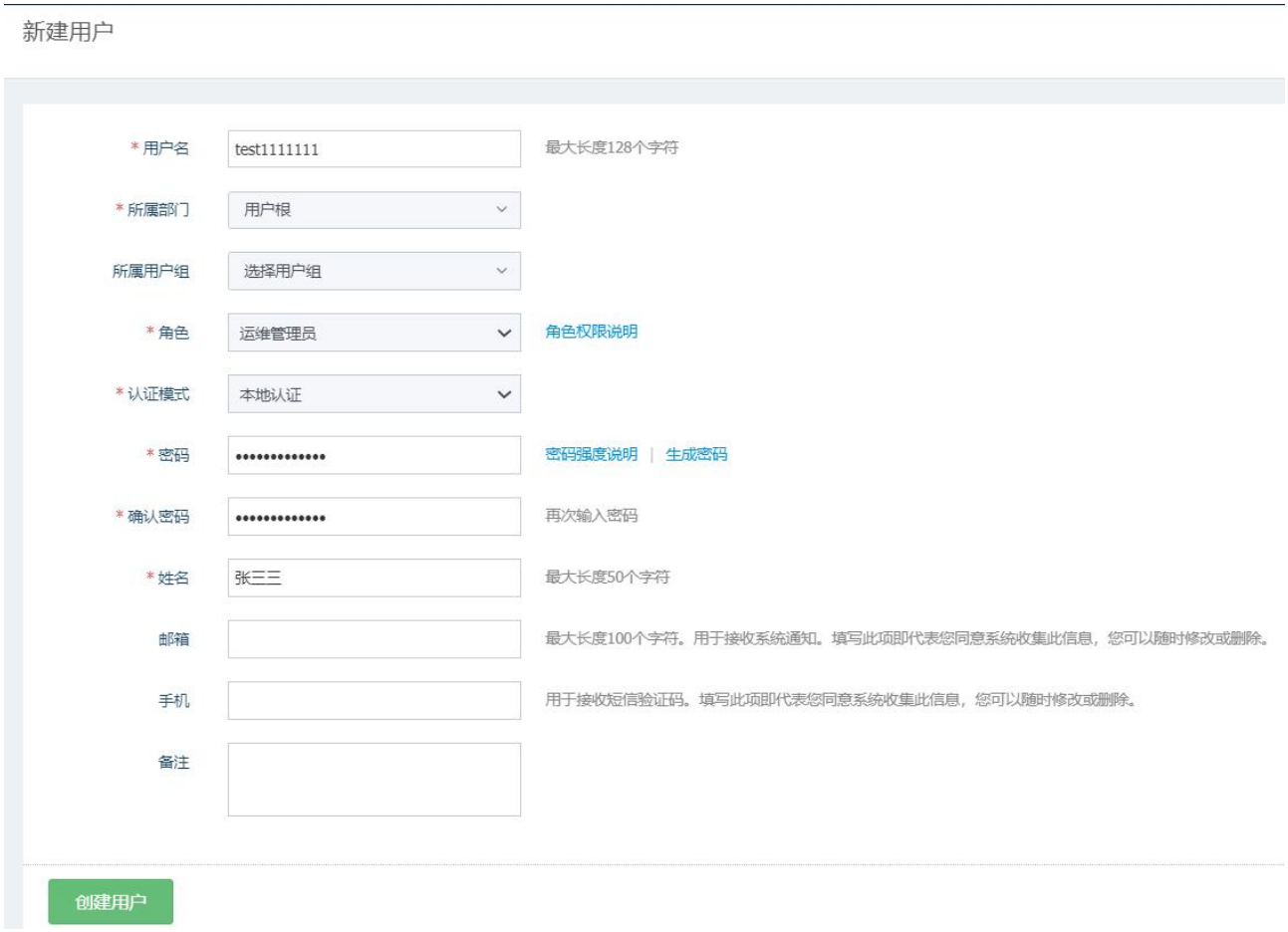
删除自定义角色后，属于该自定义角色的用户的角色会变为“无权限”。

3.2 用户管理

3.2.1 新建用户

步骤 1. 在菜单栏选择“**用户➤用户管理**”，进入**用户管理**页面，点击<**新建用户**>。

步骤 2. 进入**新建用户**页面，编辑相关信息，点击<**创建用户**>。



详细配置请参见下表。

配置项	说明
用户名	最大长度为 128 字符。
所属部门	设置用户所属部门，关于部门的更多信息请参见部门。
所属用户组	设置用户所属的用户组，关于用户组的更多信息请参见用户组管理。
角色	系统内置 9 种角色，角色权限说明可点击<**角色权限说明**>进行查看。用户仅可创建自身所属权限集合范围内的角色用户。
认证模式	选择认证模式： ◆ AD：通过远程 AD 服务器对用户进行认证。 ◆ 本地认证：通过密码对用户进行认证。 ◆ Radius：通过远程 Radius 服务器对用户进行认证。有关 Radius 服务器配置的更多信息，请参见远程认证。 ◆ LDAP：通过远程 LDAP 服务器对用户进行认证。
密码	密码需符合**密码强度说明**中的要求。点击<**生成密码**>可以自动生成随机密码。
姓名	用户姓名，最大长度为 50 字符。

创建成功后新建用户将加入到用户管理列表，点击用户名进入用户基本信息页面，在基本信息页面可以修改用户部门、角色、密码等信息。

3.2.2 导入用户

新建用户的效率较低，可使用导入用户的方法批量创建用户，导入文件最大限制为 5MB。操作方法如下：

步骤 1. 在**用户管理**页面点击<**导入用户**>。

步骤 2. 在**导入用户**页面点击<**下载模板文件**>，将模板文件下载至本地。

步骤 3. 在本地编辑模板文件并保存。点击<**上传文件**>上传编辑好的模板文件，选择认证模式，并选择是否覆盖已有同名用户，点击<**导入用户**>。

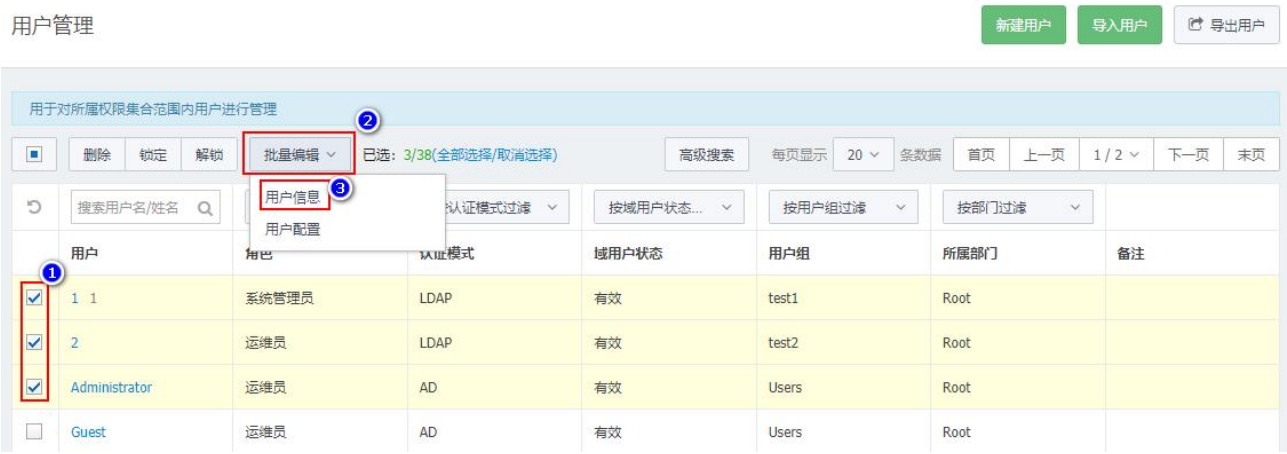
详细配置请参见下表。

配置项	说明
认证模式	设置用户登录时的认证方式，包括： ◆ 本地认证：用户登录时在本地进行认证的认证方式，即用户的帐户和密码信息存储在堡垒机系统中，用户登录时与用户输入的帐户和密码进行比对。 ◆ AD：通过远程 AD 服务器对用户进行认证。通过 AD 认证的用户会自动同步至系统，无需管理员手动创建用户。 ◆ LDAP：通过远程 LADP 服务器对用户进行认证。通过 LADP 认证的用户会自动同步至系统，无需管理员手动创建用户。 ◆ Radius：通过远程 Radius 服务器对用户进行认证。有关 AD、LDAP、Radius 认证的更多信息，请参考远程认证。
覆盖已有同名用户	若勾选该选项，当系统中存在与导入文件同名的用户，则系统中已经存在的同名用户信息将被导入文件中的同名用户信息替换。

3.2.3 批量修改用户信息

系统提供批量修改用户信息的功能，减少人工配置量，操作方法如下：

步骤 1. 在**用户管理**页面勾选需要修改用户信息的用户，点击“**批量编辑➤用户信息**”。



步骤 2. 在弹出的对话框中修改角色与认证模式，点击<**保存更改**>。

3.2.4 用户配置

可修改用户配置信息，操作方法如下。

步骤 1. 在系统菜单栏选择“**用户➤用户管理**”，进入**用户管理**页面，点击用户名进入**用户信息**页面。

步骤 1. 选择**用户配置**页签进入用户配置页面。设置用户锁定状态、认证方式、VPN 接入配置、登录 IP 黑白名单和登录时间限制，点击<**保存更改**>。

详细配置请参见下表。

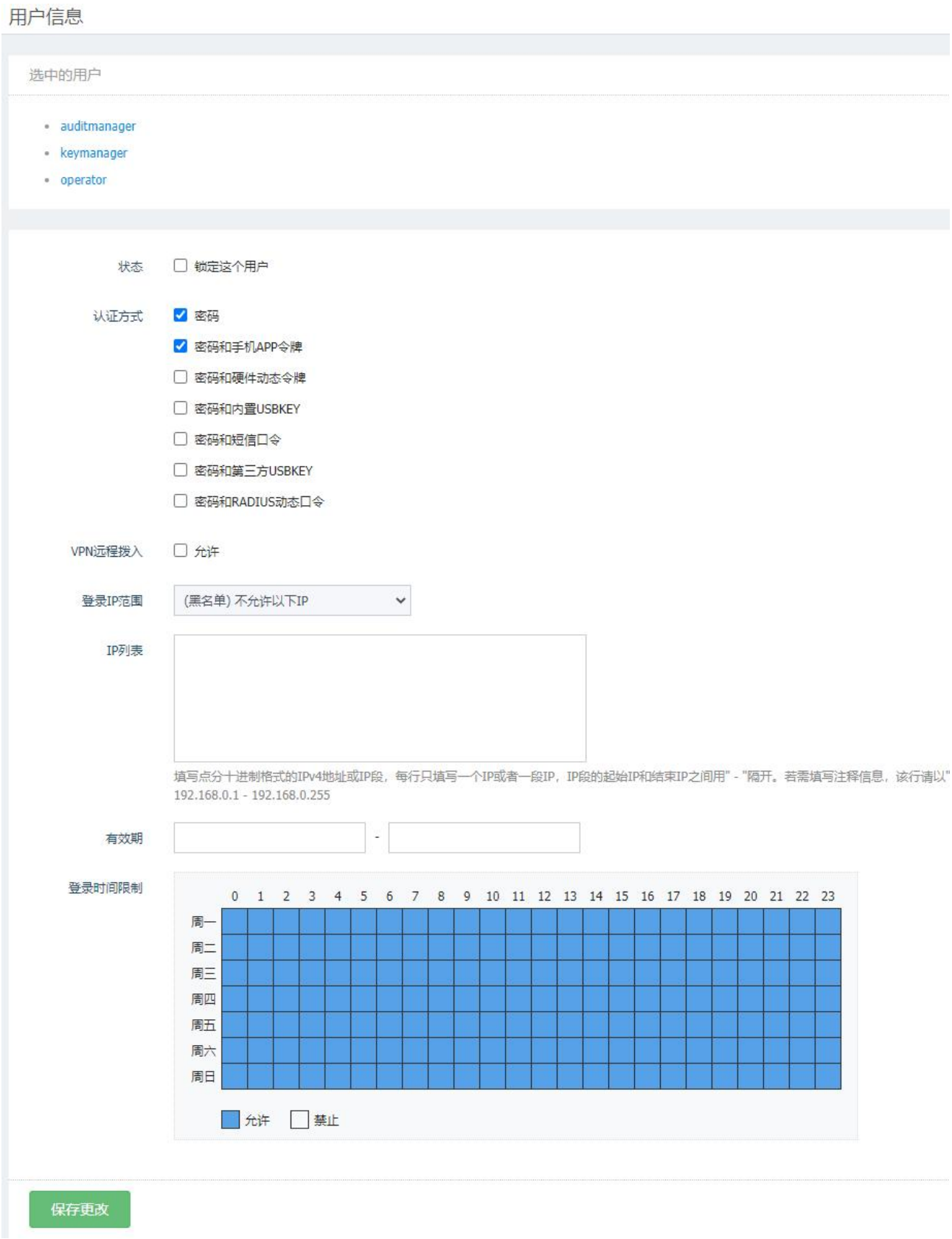
配置项	说明
锁定这个用户	用户被锁定后将无法登录系统，解除锁定后即可登录系统。

认证方式	用户登录时的认证方式。
手机 APP 验证器	显示手机 APP 验证器的状态。更多信息请参见个人信息的手机身份验证器设置。
VPN 远程拨入	设置是否允许用户通过 VPN 远程登录到系统。有关 VPN 配置的更多信息，请参见 VPN 管理。
登录 IP 范围	设置用户可以登录的 IP 地址范围，当选择黑名单时，指定的 IP 地址范围不能登录系统；当选择白名单时，仅允许指定的 IP 地址可以登录系统。
有效期	用户的有效期。只有在有效期内用户才能登录系统。
登录时间限制	指定允许登录的时间段。

可以批量修改用户配置，操作方法如下：

步骤 1. 在**用户管理**页面勾选要修改配置的用户，点击“**批量编辑➤用户配置**”。

步骤 2. 在弹出的对话框中编辑相关信息，点击<**保存更改**>即可。

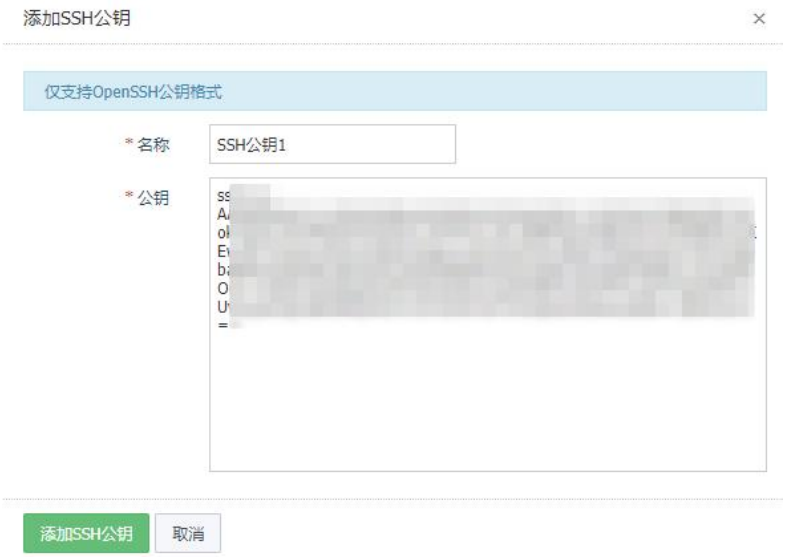


3.2.5 SSH 公钥管理

当用户使用 SSH 协议登录系统时，需要配置 SSH 公钥。

步骤 1. 在**用户信息**页面选择 **SSH 公钥**页签，点击<**添加 SSH 公钥**>。

步骤 2. 弹出**添加 SSH 公钥**对话框，设置公钥名称和公钥内容（仅支持 OpenSSH 公钥格式）。点击<**添加 SSH 公钥**>。



3.2.6 查看已授权主机

在**用户信息**页面选择**已授权主机**页签，查看对此用户已授权的主机。

3.2.7 查看已授权应用

在**用户信息**页面选择**已授权应用**页签，查看对此用户已授权的应用。

3.3 用户组管理

为便于对用户进行管理，可以将用户划分到不同的用户组，实现批量授权功能。

新建用户组并添加用户的操作方法如下：

步骤 1. 在系统菜单栏选择“**用户➤用户组管理**”，进入**用户组管理**页面，点击<**新建用户组**>。

步骤 2. 弹出**新建用户组**对话框，选择部门，设置名称，点击<**创建用户组**>。

步骤 3. 在创建完成提示页面或用户组列表页面点击用户组名称跳转到**用户组信息**页面，点击<**添加成员**>。

步骤 4. 在**选择用户**对话框中勾选用户并点击<**添加**>，将用户添加到用户组。

已添加的用户将会显示在用户组成员列表中，勾选用户，点击<**移除**>将选中的用户从当前用户组中移除。

关于用户的更多信息，请参见用户管理。

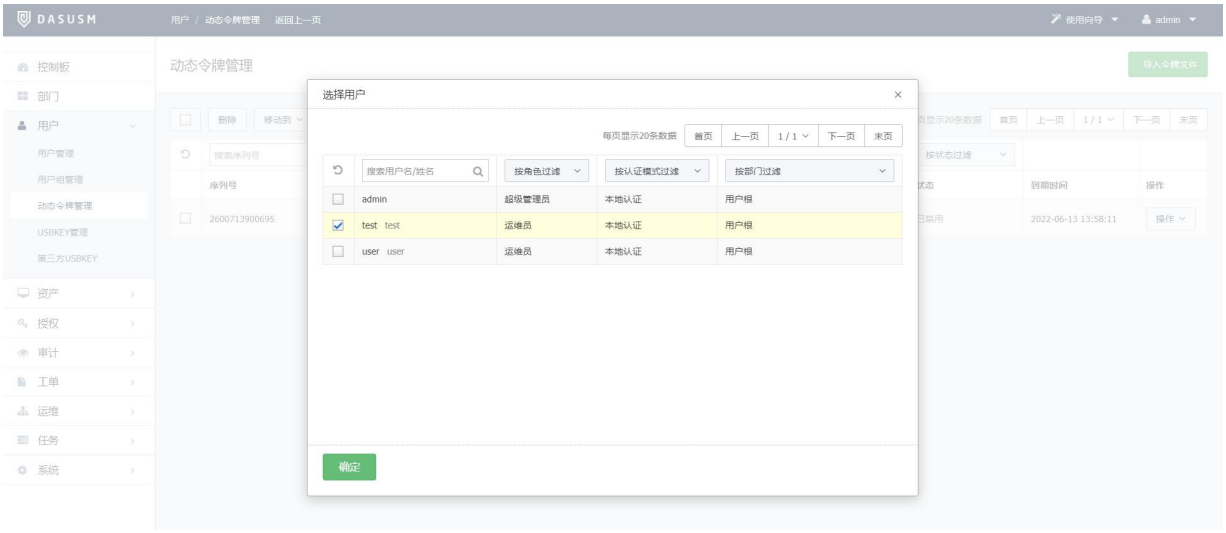
3.4 动态令牌管理

动态令牌管理是指对用户通过动态令牌登录系统进行管理。包括令牌绑定用户、禁用令牌、挂失令牌等。

新增令牌并绑定用户的操作如下：

步骤 1. 在系统菜单栏选择“**用户➤动态令牌管理**”，进入**动态令牌管理**页面。点击页面右上角的<**导入令牌文件**>，选择令牌文件并上传，完成令牌文件导入。

步骤 2. 令牌文件导入完成后，点击令牌文件右侧的“**操作➤绑定用户**”，选择用户绑定动态令牌。绑定完成后，该用户即可使用对应的动态令牌登录系统。



- 当动态令牌被禁用或挂失时，用户不能再使用该动态令牌登录系统。直到管理员重新启用令牌后，用户才可使用该令牌登录系统。
- 当动态令牌与用户之间解除绑定后，用户不能再使用该动态令牌登录系统，直到管理员重新将动态令牌与用户绑定后，用户才可使用该令牌登录系统。

4 资产

本文中所述的资产包括接入堡垒机的主机及主机中的帐户、应用等。超级管理员、部门管理员和运维管理员可对权限内的资产进行管理。

4.1 主机管理

主机管理包括新建主机、修改主机、禁用主机、删除主机等。

4.1.1 新建主机

管理员在 UMS 新建主机后，运维员才能通过堡垒机对主机进行运维操作。

步骤 1. 在系统菜单栏选择“**资产➤主机管理**”，进入**主机管理**页面。点击页面右上角的<**新建主机**>。

步骤 2. 进入**新建主机**页面，编辑相关信息，点击<**创建主机**>完成新建主机。

详细配置请参见下表。

配置项	说明
所属部门	选择主机所属部门，关于部门的更多信息请参见部门。
主机网络	配置主机所属的网络。点击<**新建**>可创建局域网。
操作系统	选择主机的操作系统，点击<**新建**>可以创建操作系统，以匹配主机的实际情况。
主机 IP	支持 IPv4、IPv6 和域名格式。
主机名称	最大长度为 50 个字符。
主机编码	设置主机编码的格式，与被管理主机上的编码设置保持一致： ◆ UTF-8：是针对 Unicode 的一种可变长度字符编码。 ◆ GB18030：全称《信息技术 中文编码字符集》，是中华人民共和国国家标准所规定的变长多字节字符集。

步骤 3. 主机创建成功后，在提示信息中点击<**创建主机帐户**>，进入主机帐户页面。

步骤 4. 点击<**添加主机帐户**>。

步骤 5. 在**新建主机帐户**对话框中选择协议、登录模式、帐户类型，填写登录名和密码，点击<**创建主机帐户**>完成主机帐户添加。

详细配置请参见下表。

配置项	说明
协议	设置用户登录时使用的协议，包括：SYSDEF、Telnet、SSH、FTP、SFTP、RDP、VNC、SQL Server、MySQL、Oracle、DB2、PostgreSQL、KingbaseES、DM、X11 和 Rlogin。
登录模式	设置主机的登录模式：自动登录、手动登录和自动登录（二次登录）。 ◆ 自动登录：将正确的主机帐号密码托管到堡垒机，运维时堡垒机自动代填密码。 ◆ 手动登录：在运维时需要用户输入正确的主机帐号密码才可登录成功。 ◆ 自动登录（二次登录）：只支持 SSH 和 Telnet 协议，用于管理两个帐户自动跳转登录。如交换机既有远程帐户又有 enable 命令特权帐户，若需要自动登录到 enable 命令特权帐户，则必须采取自动登录（二次登录）模式。
帐户类型	包括普通帐户和交换机特权命令帐户两种类型。
登录名	主机帐户登录名。
密码	主机帐户密码。

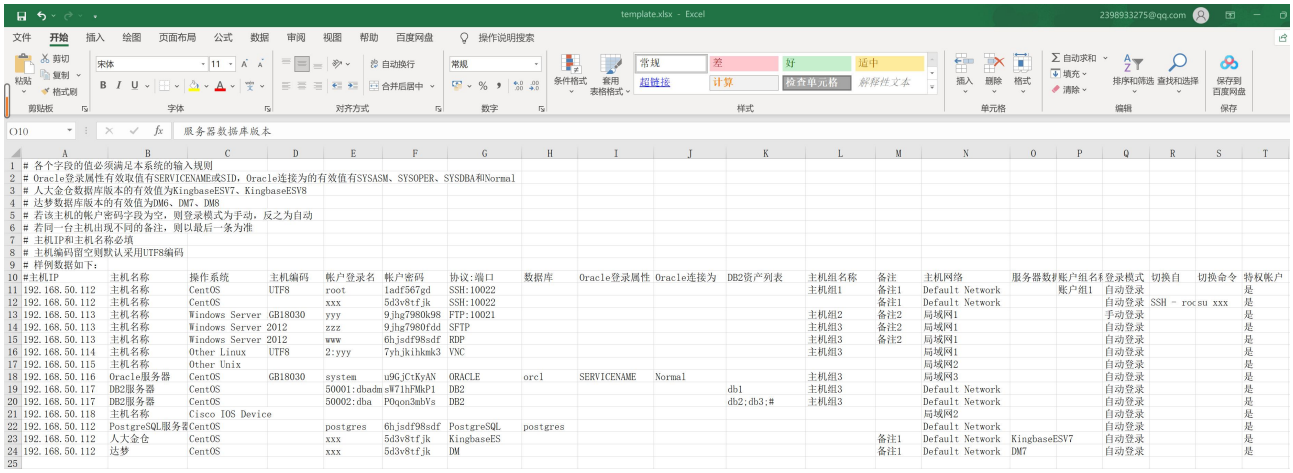
4.1.2 导入主机

手动逐个新建主机的效率较低，可使用导入主机的方法批量创建主机。操作方法如下：

步骤 1. 在**主机管理**页面点击右上角的<**导入主机**>，进入**导入主机**页面。

步骤 2. 点击<**下载模板文件**>，将模板文件保存至本地。

步骤 3. 根据模板格式添加主机及主机帐户，修改模板文件后保存文件。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	# 各个字段的值必须满足本系统的输入规则																			
2	# Oracle登录属性有效取值有SERVICENAME或SID，Oracle连接为的有效值有SYSASM、SYSOPER、SYSDBA和Normal																			
3	# 人大金仓数据库版本的有效值为KingbaseESV7、KingbaseESV8																			
4	# 达梦数据库版本的有效值为DM6、DM7、DM8																			
5	# 若该主机的帐户密码字段为空，则登录模式为手动，反之为自动																			
6	# 若同一台主机出现不同的备注，则以最后一条为准																			
7	# 主机IP和主机名称必填																			
8	# 主机编码留空则默认采用UTF8编码																			
9	# 样例数据如下：																			
10	#主机IP	主机名称	操作系统	主机编码	帐户登录名	帐户密码	协议:端口	数据库	Oracle登录属性	Oracle连接为	DB2资产列表	主机组名称	备注	主机网络	服务器数目	账户组名称	登录模式	切换自	切换命令	特权帐户
11	192.168.50.112	主机名称	CentOS	UTF8	root	1adf567gd	SSH:10022					主机组1	备注1	Default Network		账户组1	自动登录			是
12	192.168.50.112	主机名称	CentOS		xxx	5d3v8tfjk	SSH:10022						备注1	Default Network			自动登录	SSH - rocsu xxx		是
13	192.168.50.113	主机名称	Windows Server	GB18030	yyy	9jhg7980k98	FTP:10021					主机组2	备注2	局域网1			手动登录			是
14	192.168.50.113	主机名称	Windows Server 2012		zzz	9jhg7980fdd	SFTP					主机组3	备注2	局域网1			自动登录			是
15	192.168.50.113	主机名称	Windows Server 2012		www	6hjsdf98sdf	RDP					主机组3	备注2	局域网1			自动登录			是
16	192.168.50.114	主机名称	Other Linux	UTF8	2:yyy	7yhjkihkmk3	VNC					主机组3		局域网1			自动登录			是
17	192.168.50.115	主机名称	Other Unix											局域网2			自动登录			是
18	192.168.50.116	Oracle服务器	CentOS	GB18030	system	u9GjCtKyAN	ORACLE	orcl	SERVICENAME	Normal		主机组3		局域网3			自动登录			是
19	192.168.50.117	DB2服务器	CentOS		50001:dbadm	sW71hFMkP1	DB2				db1	主机组3		Default Network			自动登录			是
20	192.168.50.117	DB2服务器	CentOS		50002:dba	POqon3mbVs	DB2				db2;db3;#	主机组3		Default Network			自动登录			是
21	192.168.50.118	主机名称	Cisco IOS Device											局域网2			自动登录			是
22	192.168.50.112	PostgreSQL服务器	CentOS		postgres	6hjsdf98sdf	PostgreSQL	postgres						Default Network			自动登录			是
23	192.168.50.112	人大金仓	CentOS		xxx	5d3v8tfjk	KingbaseES						备注1	Default Network	KingbaseESV7		自动登录			是
24	192.168.50.112	达梦	CentOS		xxx	5d3v8tfjk	DM						备注1	Default Network	DM7		自动登录			是
25																				

步骤 4. 在**导入主机**页面点击<**上传文件**>，选择编辑好的模板文件并上传，上传完成后选择导入模式（标准、修改或新建），点击<**导入主机**>。完成批量添加主机及主机帐户。

4.1.3 导出主机

步骤 1. 进入**主机管理**页面，在页面右上角点击<**导出主机**>。

步骤 2. 在弹出的**导出主机**对话框中设置文件加密密码（点击<**密码强度说明**>查看密码强度要求），点击<**导出主机**>可将主机信息导出至本地（为 zip 文件，若设置了文件加密密码，解压缩时需要输入密码解密）。

4.1.4 修改主机

创建主机后可对主机信息进行修改，操作方法如下：

步骤 1. 修改主机基本信息。

1) 在系统菜单栏选择“**资产➤主机管理**”，进入**主机管理**页面。
2) 点击主机 IP 进入主机基本信息页面。

3) 在**主机信息**区域可修改主机网络、操作系统、主机 IP、主机名称以及主机编码等信息，修改完成后点击<**保存更改**>。

4) 在**协议端口配置**区域修改主机协议端口信息，点击<**保存更改**>。

步骤 2. 修改主机配置信息。

选择**主机配置**页签，进入主机配置页面，可配置主机协议控制等选项。


主机信息
基本信息
主机配置
主机帐户
共享帐户
已授权用户
主机配置
状态
禁用这台主机
会话选项
开启会话二次审批
开启会话备注
开启历史会话审计
开启实时会话监控
RDP选项
启用键盘记录
允许打印机/驱动器映射
允许使用剪贴板下载文字
允许使用剪贴板上传文字
允许使用剪贴板下载文件
允许使用剪贴板上传文件
允许磁盘映射方式文件上传
允许磁盘映射方式文件下载
SSH选项
允许X11转发
允许打开SFTP通道
允许请求exec
首选密钥交换算法配置
仅当某些交换机设备握手失败时可尝试更改此配置
默认模式
diffie-hellman-group1-sha1 兼容模式
diffie-hellman-group14-sha1 兼容模式
diffie-hellman-group-exchange-sha1 兼容模式
SFTP/SCP/ZMODEM传输控制
禁止文件上传
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
FTP选项
禁止文件上传
FTP属于不安全协议，请谨慎使用
禁止文件下载
禁止文件删除
禁止重命名
禁止目录创建
禁止目录删除
文件审计
生成文件SHA1
保存文件
保存下载文件
保存上传文件
启用文件压缩
不保存超过
30
KB
的文件
单个会话保存的文件超过
100
MB
时停止保存
保存更改

详细配置请参见下表。

选项	功能	解释
会话选项	开启会话二次审批	需要对该主机进行审核后才可登录。
	开启会话备注	需要写明登录主机的原因或目的才可登录。
	开启历史会话审计	对运维会话进行审计。
	开启实时会话监控	管理员可以对主机进行实时监控。
RDP 选项	启用键盘记录	记录 RDP 主机的键盘符操作记录。
	允许打印机/驱动器映射	运维 RDP 主机时，可以映射本地打印和本地磁盘。
	允许使用剪切板下载文字/文件	运维 RDP 主机时，可以使用复制-粘贴功能从主机下载文字或文件。
	允许使用剪贴板上传文字/文件	运维 RDP 主机时，可以使用复制-粘贴功能上传至主机文字或文件。
	允许磁盘映射方式文件上传	运维 RDP 主机时，可以使用磁盘映射方式上传文件至 RDP 主机。
	允许磁盘映射方式文件下载	运维 RDP 主机时，可以使用磁盘映射方式从 RDP 主机下载文件至本地主机。
SSH 选项	允许 X11 转发	运维时可以通过 SSH 方式转发 X11 协议。
	允许打开 SFTP 通道	运维时可以使用 SSH 的客户工具直接打开 SFTP 协议。
	允许请求 exec	可以直接使用 exec 指令。
	首选密钥交换算法配置	选择优先使用的密钥交换算法： ◆ 默认模式：libssh 推荐的算法优先级，密钥交换算法、证书算法、加密算法，安全性越高的算法优先级越高。 ◆ diffie-hellman-group1-sha1 兼容模式：密钥交换算法优先使用 diffie-hellman-group1-sha1，证书算法优先使用 RSA，加密算法优先使用 AES128。 ◆ diffie-hellman-group14-sha1 兼容模式：密钥交换算法优先使用 diffie-hellman-group14-sha1，证书算法优先使用 RSA，加密算法优先使用 AES128。 ◆ diffie-hellman-group-exchange-sha1 兼容模式：密钥交换算法优先使用 diffie-hellman-group-exchange-sha1，证书算法优先使用 RSA、加密算法优先使用 AES128。 仅当交换机设备握手失败时，可尝试更改此配置。
SFTP/SCP/ZMODEM 传输控制	禁止文件上传	运维时禁止通过 SFTP/SCP/ZMODEM 方式上传文件。
	禁止文件下载	运维时禁止通过 SFTP/SCP/ZMODEM 方下载文件。
	禁止文件删除	运维 SFTP 主机时禁止删除文件。
	禁止重命名	运维 SFTP 主机时禁止重命名。
	禁止目录创建	运维 SFTP 主机时禁止创建目录。

选项	功能	解释
	禁止目录删除	运维 SFTP 主机时禁止删除目录。
FTP 选项	禁止文件上传	运维 FTP 主机时禁止上传文件。
	禁止文件下载	运维 FTP 主机时禁止下载文件。
	禁止文件删除	运维 FTP 主机时禁止删除文件。
	禁止重命名	运维 FTP 主机时禁止重命名。
	禁止目录创建	运维 FTP 主机时禁止创建目录。
	禁止目录删除	运维 FTP 主机时禁止删除目录。
文件审计	生成文件 SHA1	可以对 SFTP/FTP 传输的文件进行 SHA1 签名，确保文件的唯一性与不重复。
	保存文件	可以将 SFTP/FTP 传输的文件进行保存在堡垒机系统中。
	保存下载文件	可以保存下载的文件。
	保存上传文件	可以保存上传的文件。
	启用文件压缩	可以对传输的文件进行压缩。
	不保存超过*KB 的文件	可以根据单个文件的大小进行保存。取值范围：1~1,000,000。
	单个会话保存的文件总大小超过*MB 时停止保存	可以控制单个会话保存的文件大小。取值范围：1~1,000,000。

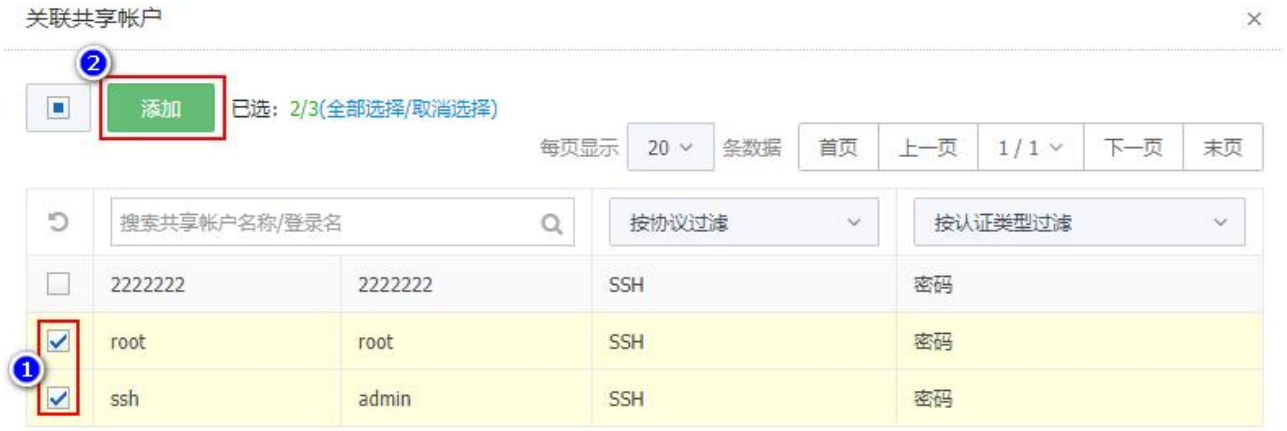
步骤 3. 修改主机账户信息。

选择**主机帐户**页签，点击登录名，编辑主机帐户信息；点击<**添加主机帐户**>，添加主机帐户。

步骤 4. 修改共享账户信息。

1) 选择**共享帐户**页签进入共享帐户页面，点击<**关联共享帐户**>。关于共享帐户的详细信息，请参见共享帐户。

2) 在弹出的对**关联共享帐户**话框中勾选需要关联的共享帐户，点击<**添加**>。



此外，系统支持批量修改主机信息，操作方法如下：

- 在**主机管理**页面勾选要修改信息的主机，点击“**批量编辑➤主机信息**”可批量修改主机的操作系统、主机编码信息。
- 点击“**批量编辑➤端口配置**”可批量修改主机的协议端口配置信息。

4.1.5 查看已授权用户信息

在**主机信息**页面选择**已授权用户**页签，可查看已授权此主机的用户。

4.1.6 选择要展示的主机列表信息

主机列表支持自定义展示列，操作方法如下：

步骤 1. 在系统菜单栏选择“**资产➤主机管理**”，进入**主机管理**页面，点击<**修改展示列**>。

步骤 2. 在弹出的**修改展示列**对话框中勾选需要展示的列，点击<**保存**>。

4.1.7 查看指定时间段内未被运维的主机

步骤 1. 在**主机管理**页面点击<**高级搜索**>。

步骤 2. 在弹出的**高级搜索**对话框中设置未运维开始时间和未运维结束时间，点击<**搜索**>即可搜索指定时间段内未被运维的主机。

4.2 帐户管理

4.2.1 主机帐户

在系统菜单栏选择“**资产➤帐户管理**”，可查看主机帐户信息。在账户管理页中可以查看帐户有效性等信息。对于无效帐户，点击**<无效>**即可查看帐户无效原因。

无效原因说明如下。

日志详情	说明
日志中包含 No route to host	网络无法连通
日志中包含 Authentication failure 或 Access denied	认证失败
日志中包含 Connection time out	验证超时
日志中包含 Login fail	登录失败
其他错误	根据具体日志具体分析

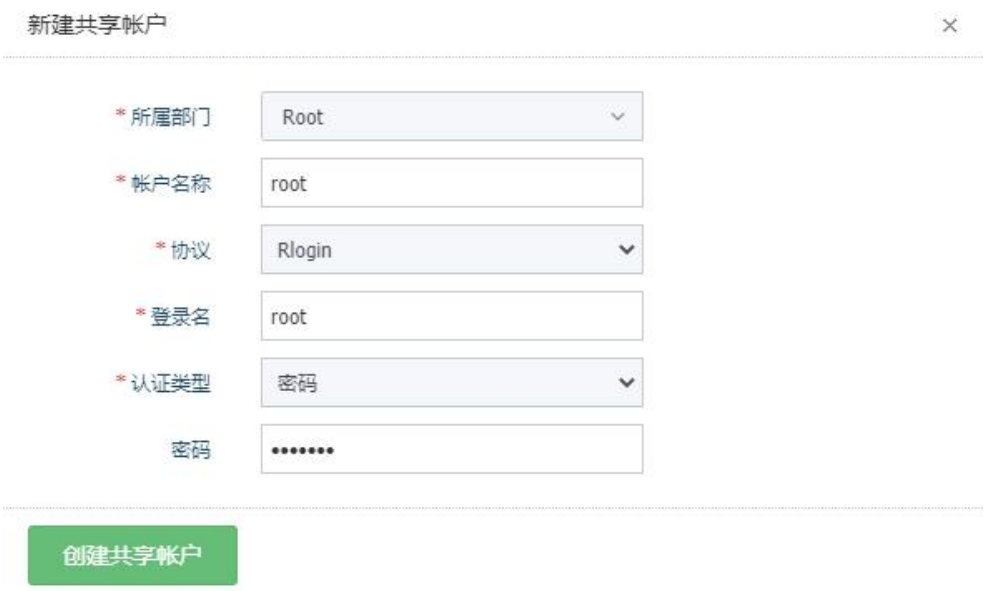
关于主机帐户的更多信息请参见新建主机。

4.2.2 共享帐户

具有权限的用户可使用共享帐户登录共享帐户关联的多个主机，可减少为主机创建帐户的工作量。创建共享帐户并关联主机的操作方法如下：

步骤 1. 在系统菜单栏选择“**资产➤帐户管理**”，选择**共享帐户**页签。点击右上方的<**新建共享帐户**>。

步骤 2. 在弹出的**新建共享账户**对话框中选择共享帐户所属部门、协议，填写帐户名称、登录名，选择认证类型，填写密码/密钥，点击<**创建共享帐户**>完成共享帐户添加。



部分参数的详细配置请参见下表。

配置项	说明
协议	帐户登录系统使用的协议，包括 Telnet、SSH、FTP、SFTP、RDP、VNC 和 Rlogin。
认证类型	当使用 SSH 协议时，可选择密码和密钥；使用其他协议时仅可选择密码。

步骤 3. 点击共享帐户右侧的<**关联主机**>。

步骤 4. 进入**共享帐户信息**页面，点击<**关联主机**>。

步骤 5. 在弹出的**关联主机**对话框中勾选主机，点击<**添加**>即可添加关联主机。

4.3 主机组管理

对主机进行分组，便于对主机进行集中授权，减少配置工作量。创建主机组并添加主机的方法如下：

步骤 1. 在系统菜单栏选择“**资产➤主机组管理**”，进入**主机组管理**页面，点击<**新建主机组**>。

步骤 2. 在弹出的**新建主机组**对话框中选择主机组所在部门，填写主机组名称，点击<**创建主机组**>，完成主机组创建。

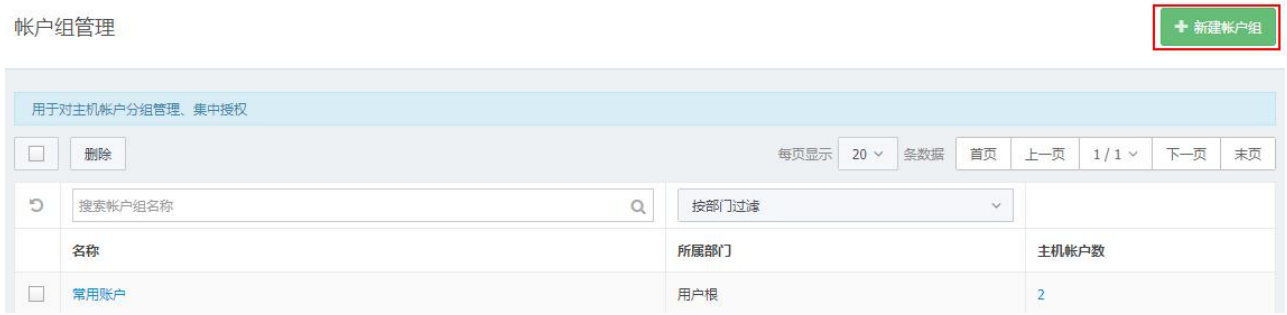
步骤 3. 点击主机组名称，进入**主机组信息**页面（默认展示**主机组成员**页签），点击<**添加主机**>。

步骤 4. 在弹出的**选择主机**对话框中勾选主机，点击<**添加**>即可将主机添加到主机组中。

4.4 帐户组管理

为帐户分组，便于对帐户进行批量设置。创建帐户组并添加帐户的操作方法如下：

步骤 1. 在系统菜单栏选择“**资产➤帐户组管理**”，进入**帐户组管理**页面，点击<**新建帐户组**>。



步骤 2. 在弹出的对话框中选择帐户组所在部门，填写帐户组名称，点击<**创建帐户组**>，完成帐户组创建。

步骤 3. 在创建帐户组成功提示信息中点击帐户组名称链接，进入**帐户组信息**页面管理帐户组成员。点击<**添加主机帐户**>。

步骤 4. 在弹出的对话框中勾选主机帐户，点击<**添加**>即可为帐户组添加帐户。

4.5 应用管理

当用户进行运维操作时使用的客户端工具以及协议（如 HTTPS 协议）不在堡垒机的支持范围内，但仍需要堡垒机对用户的运维操作进行审计时，需要借助应用发布服务器来实现对用户的运维操作进行审计。

4.5.1 新建应用

新建应用的操作方法如下（本文以域控实例举例说明）：

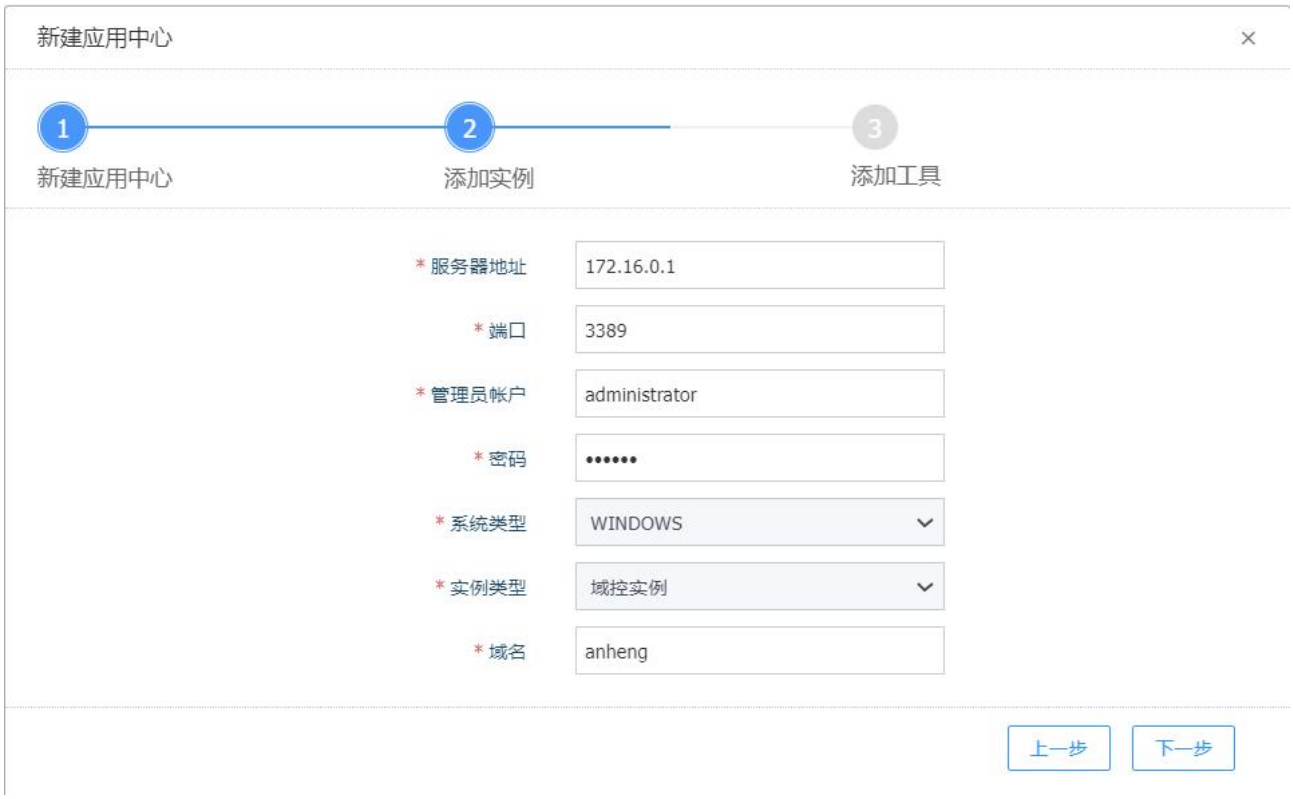
步骤 1. 新建应用中心。

1) 联系天翼云额外订阅云主机配置为“应用发布服务器”（即应用中心）。根据实际使用的操作系统版本在云主机上进行应用发布相关配置。

2) 在系统菜单栏选择“**资产➤应用管理**”，选择**应用中心**页签，进入**应用中心管理**页面，点击<**新建应用中心**>。

3) 在弹出的对话框中选择部门，输入应用中心名称，点击<**下一步**>。

4) 编辑相关信息，点击<**下一步**>。



详细配置请参见下表。

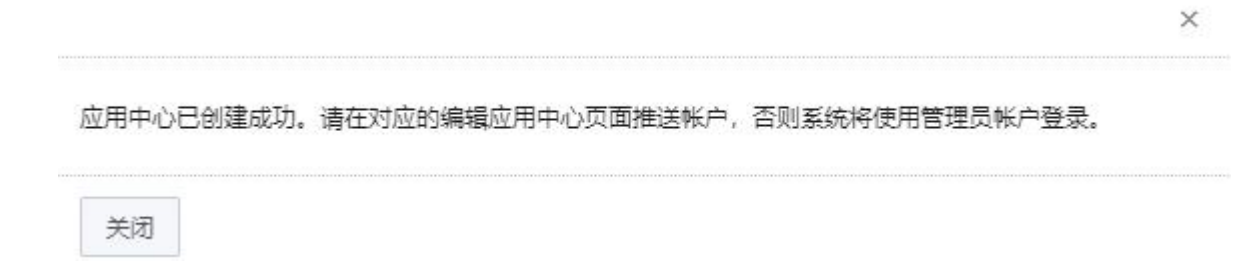
配置项	说明
服务器地址	应用中心服务器的 IP。
端口	应用中心服务器的端口，用于进行远程桌面连接，通常为 3389。
管理员帐户	应用中心服务器的管理员帐户。

配置项	说明
密码	应用中心服务器管理员账户对应的密码。
系统类型	包括 Windows 和 Linux。
实例类型	包括域控实例和单机实例。 ◆ 域控实例：适用于应用中心需要以集群方式部署的场景，需通过 AD 域方式实现集群。选择“域控实例”时需要配置域名称。 ◆ 单机实例：适用于应用中心以单台服务器部署的场景。Linux 系统主机仅支持单机实例。
域名	当**实例类型**选择“域控实例”时需要配置域名称。

5) 根据实际需要增加或删除应用中心工具，设置完成后点击<**完成**>，完成应用中心的创建。

点击工具右侧的<**删除**>删除工具，点击<**新建工具**>为应用中心添加工具，双击启动路径可修改工具路径（根据实际应用的安装路径进行修改）。

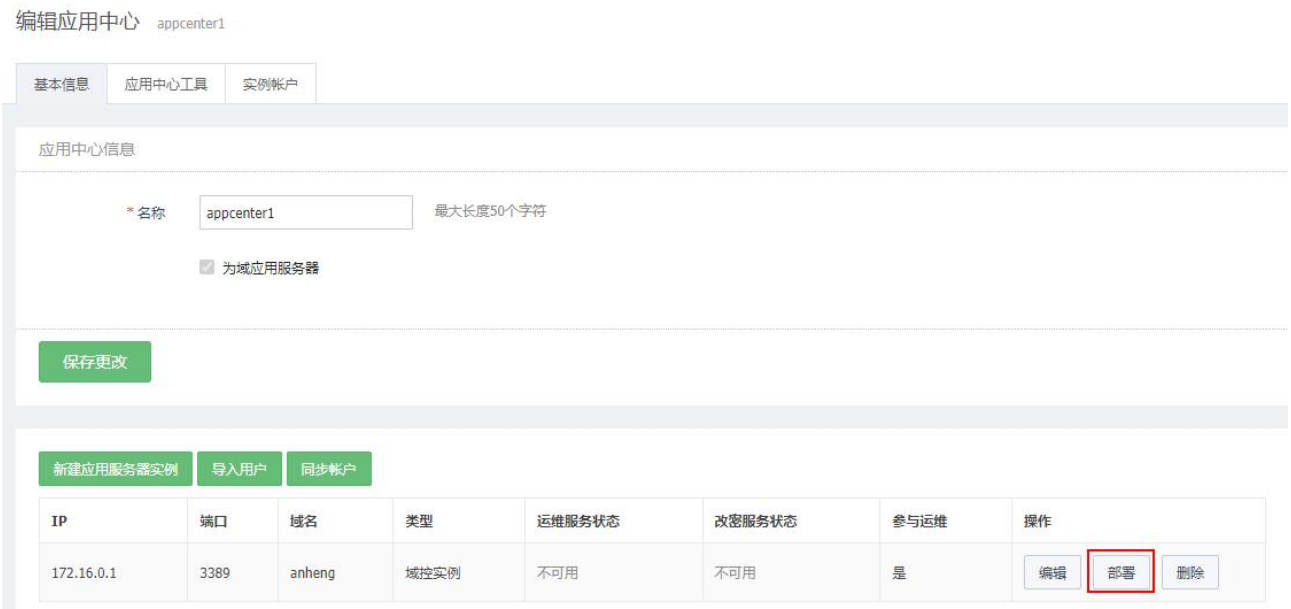
6) 点击<**关闭**>。



步骤 2. 部署应用中心。

1) 点击应用中心名称或应用中心右侧的<**编辑**>，进入**编辑应用中心**页面。

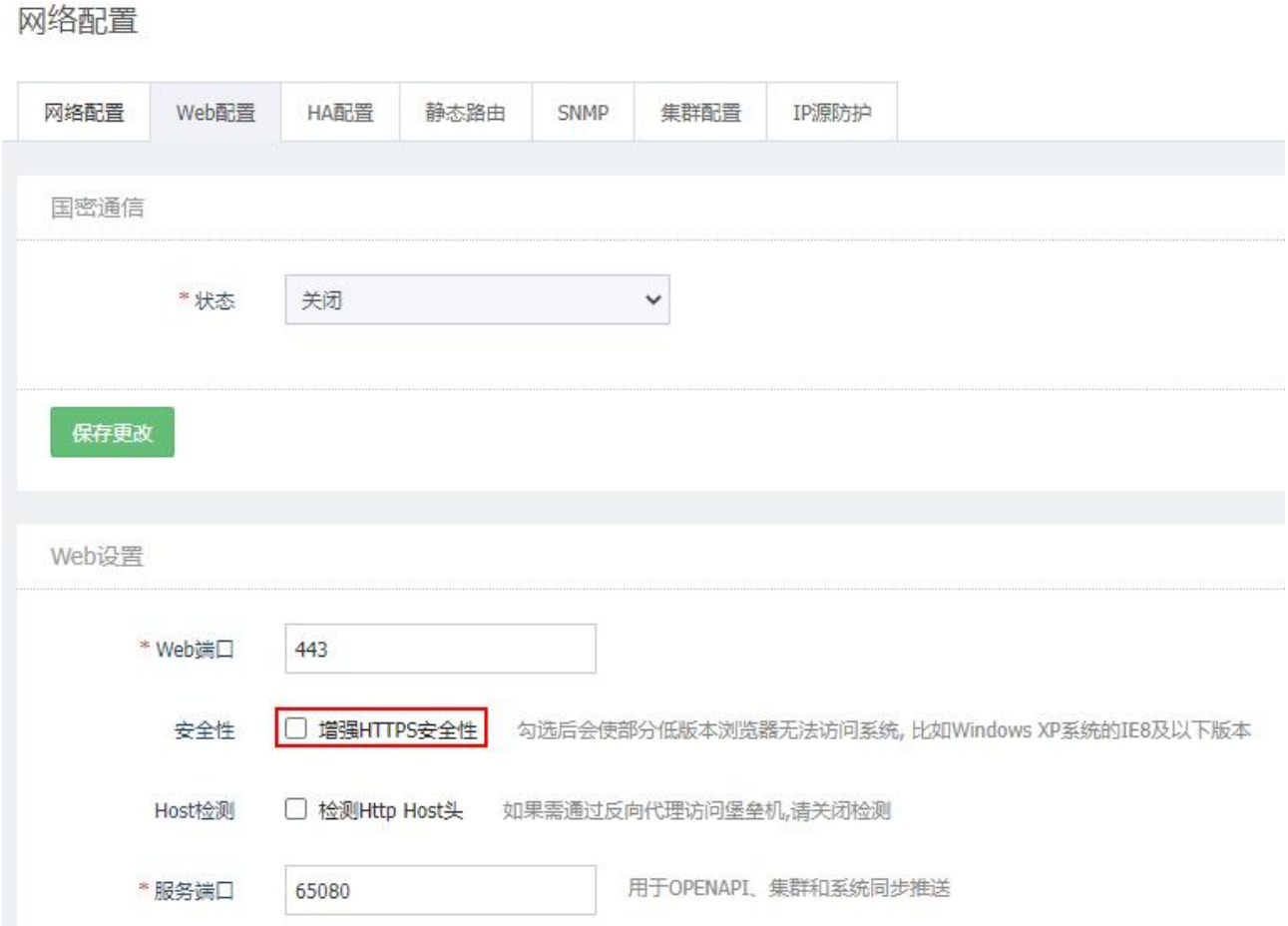
2) 在应用中心的**基本信息**页面点击<**部署**>。



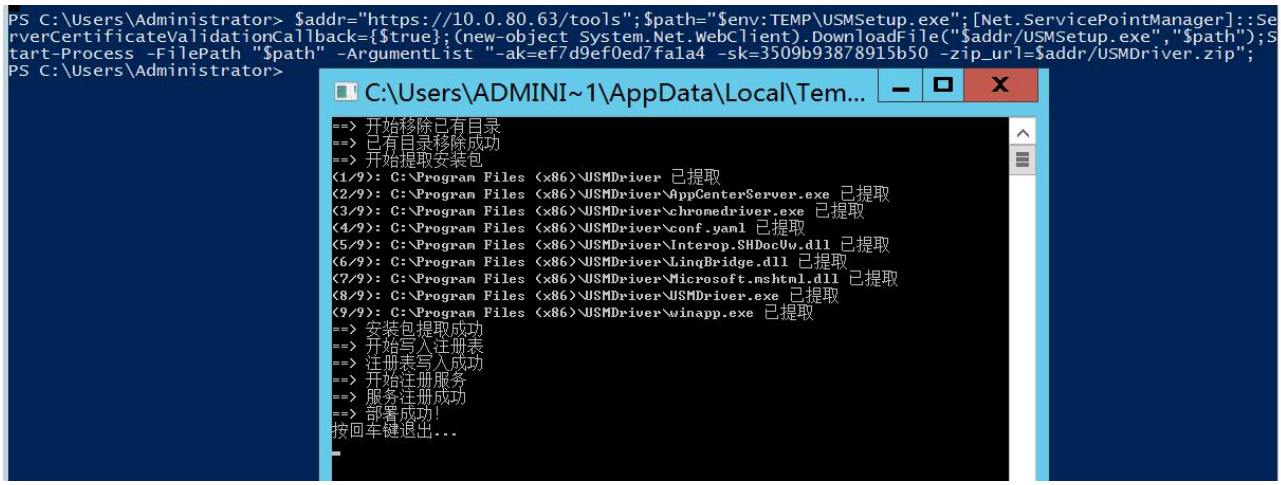
3) 在弹出的对话框中点击<**生成命令**>。使用管理员帐户登录应用服务器，以管理员身份打开 PowerShell，将生成的命令复制粘贴到应用服务器中的 PowerShell 中执行，部署应用中心预控服务器实例。

4) 若在部署时出现“未能创建 SSL/TLS 安全通道”的报错，需要将堡垒机的“增强 HTTPS 安全性”选项关闭，再进行部署。

关闭“增强 HTTPS 安全性”选项的操作方法如下：登录系统 Web 管理平台，在系统菜单栏选择“**系统➤网络配置**”，选择 **Web 配置**页签，在 **Web 设置**区域中取消勾选**增强 HTTPS 安全性**，点击<**保存更改**>。配置完成后再登录应用服务器部署应用中心域控服务器实例。



5) 等待应用中心预控服务器实例部署完成后，按回车键退出。

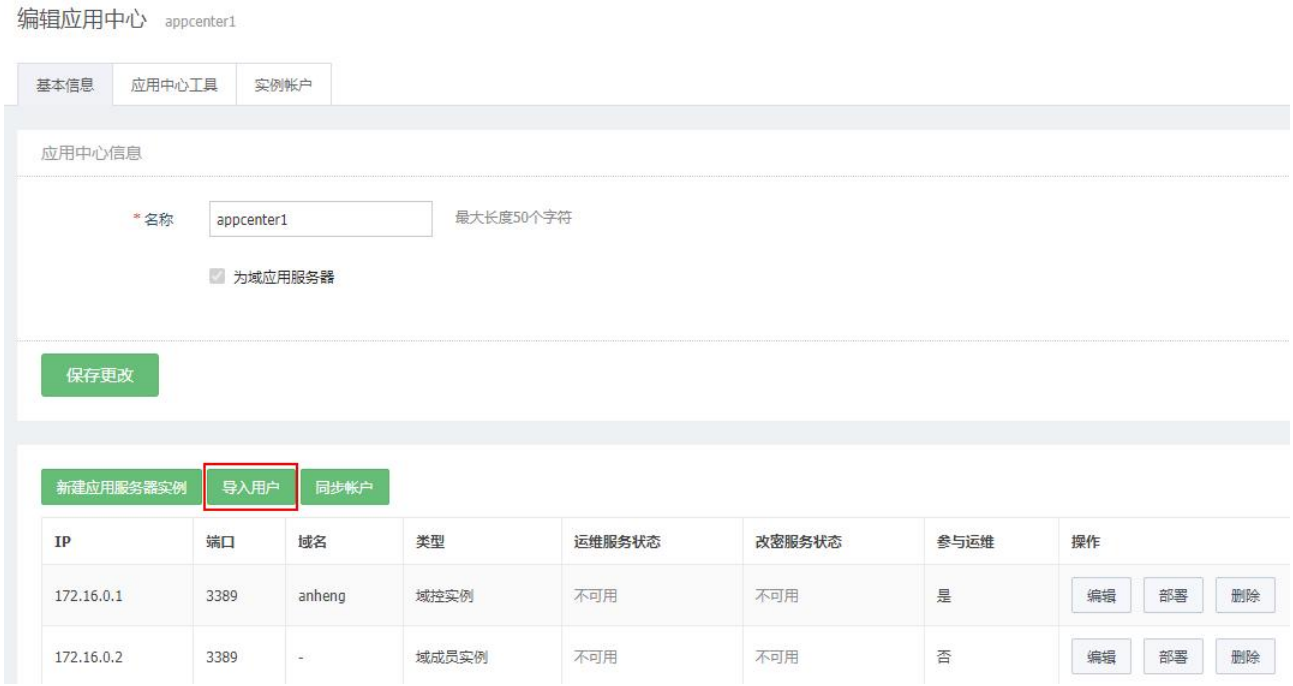


6) 部署域成员服务器实例。

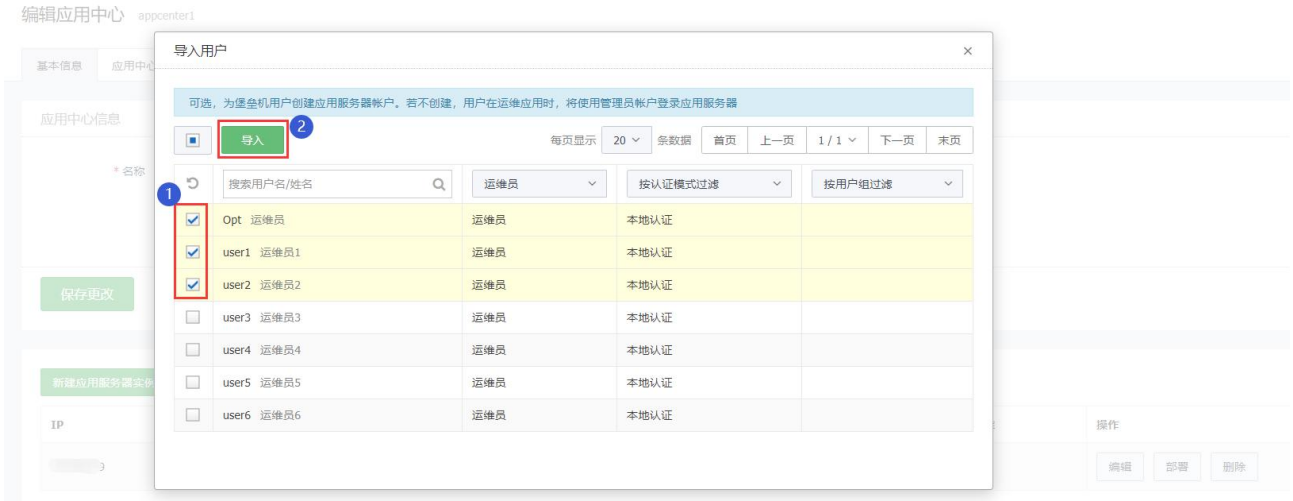
登录系统 Web 管理平台，在系统菜单栏选择“**资产➤应用管理**”，选择**应用中心**页签，点击应用中心右侧的<**编辑**>进入**编辑应用中心**页面。在**编辑应用中心**页面点击<**新建应用服务器实例**>可以添加域成员服务器实例。添加完成后，参考 2)~5)部署域成员服务器实例。

7) 在**编辑应用中心**页面的**基本信息**中点击<**导入用户**>。

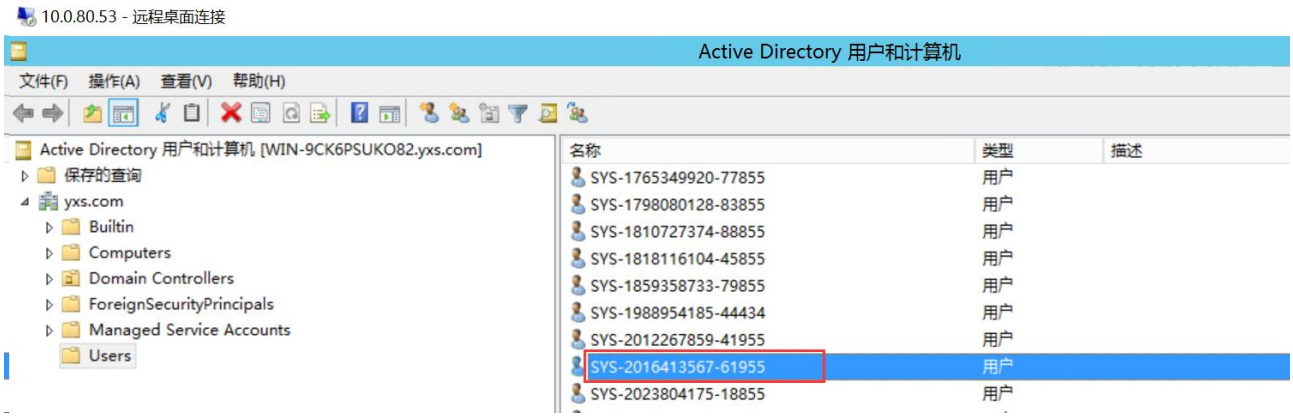
为堡垒机用户创建应用服务器帐户。若不创建，用户在运维应用时，将使用管理员帐户登录应用服务器。



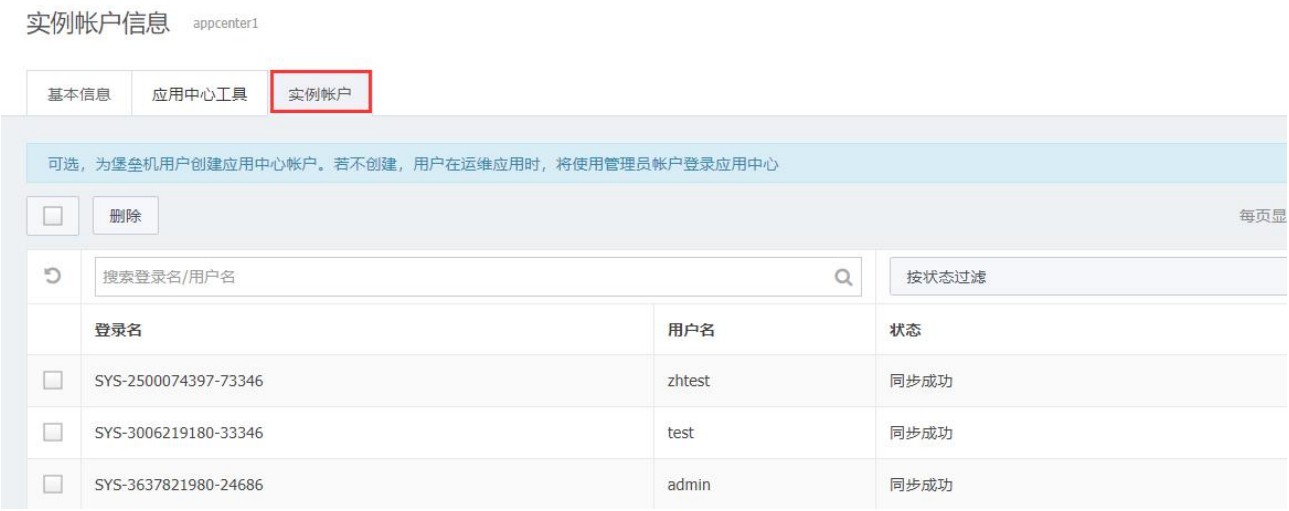
8) 在弹出的对话框中勾选需要导入的用户，点击<**导入**>，为堡垒机用户创建应用服务器帐户。



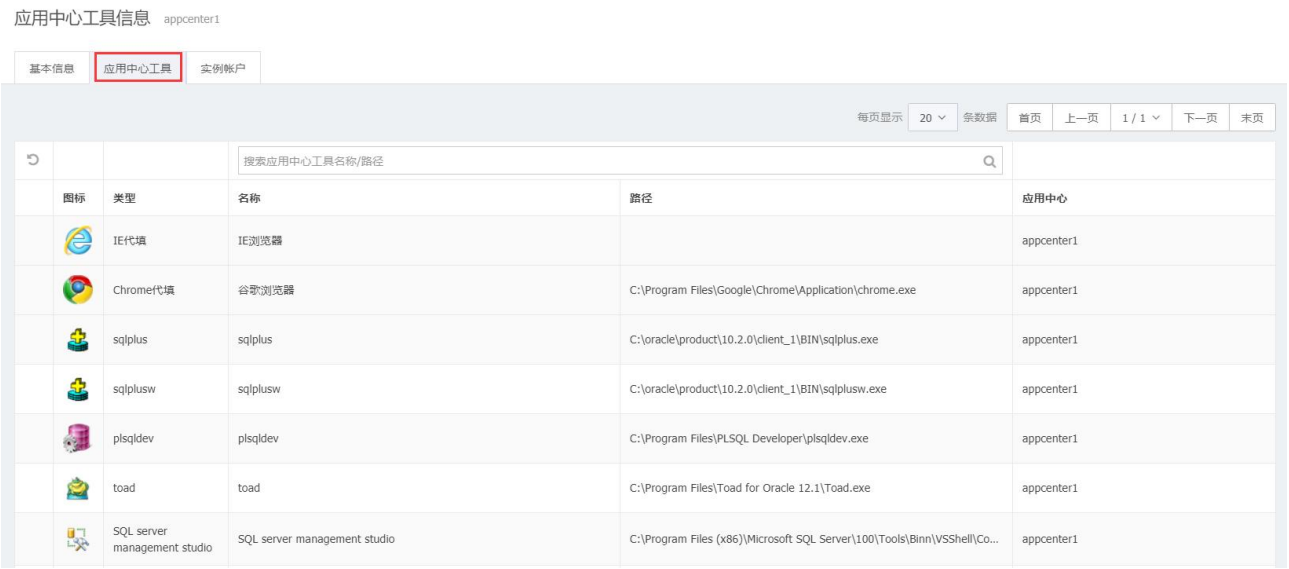
导入用户后，登录应用服务器，在应用服务器的用户帐户中可以查看到导入的帐户，登录名格式为：账户名-时间戳-ID 进行哈希后的字符串。



9) 选择**实例帐户**页签，可查看实例账户状态等信息。勾选实例帐户，点击<**删除**>，可将实例帐户从远程应用服务器上删除。

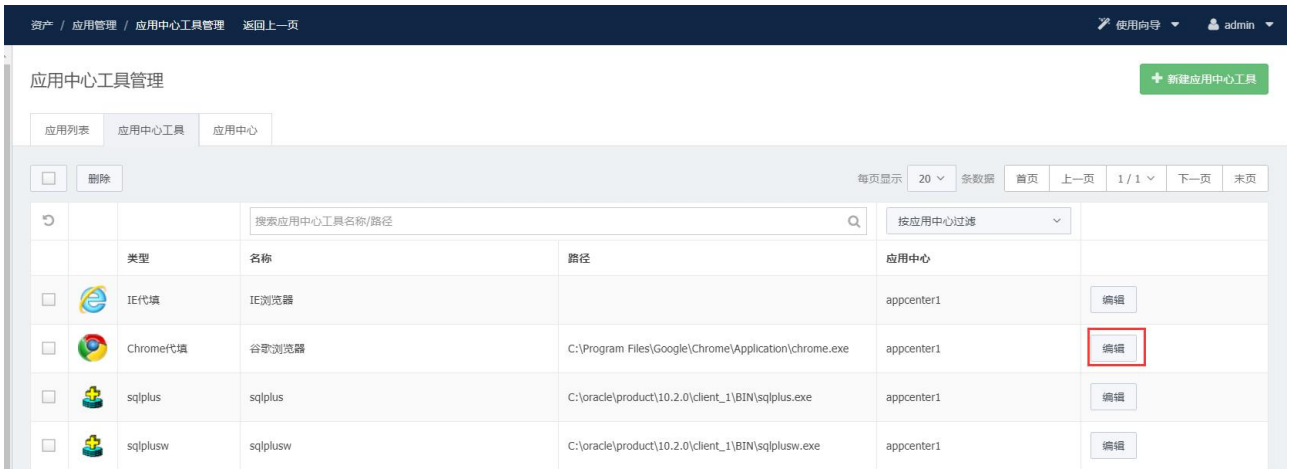


10) 选择**应用中心工具**页签，可查看当前应用中心下的工具信息。

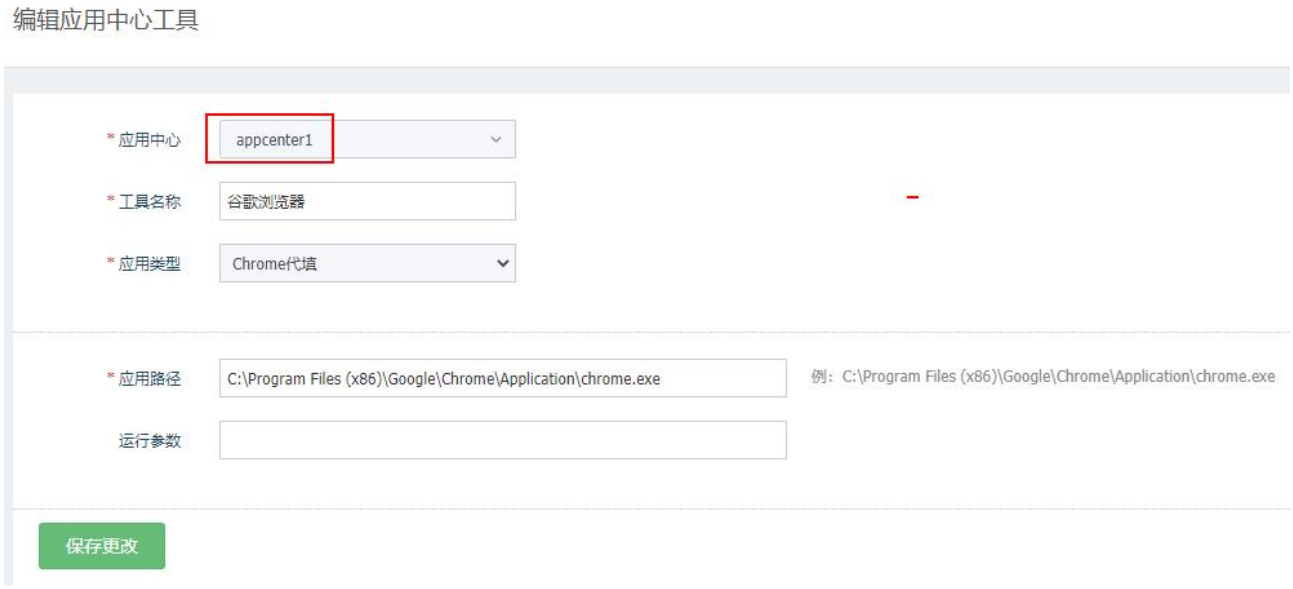


步骤 3. 修改应用中心的工具（编辑工具或新建工具）。

1) 在系统菜单栏选择“**资产➤应用管理**”，进入**应用管理**页面，选择**应用中心工具**页签，进入**应用中心工具管理**页面。选择上文新建应用中心的工具，点击工具右侧的<**编辑**>。

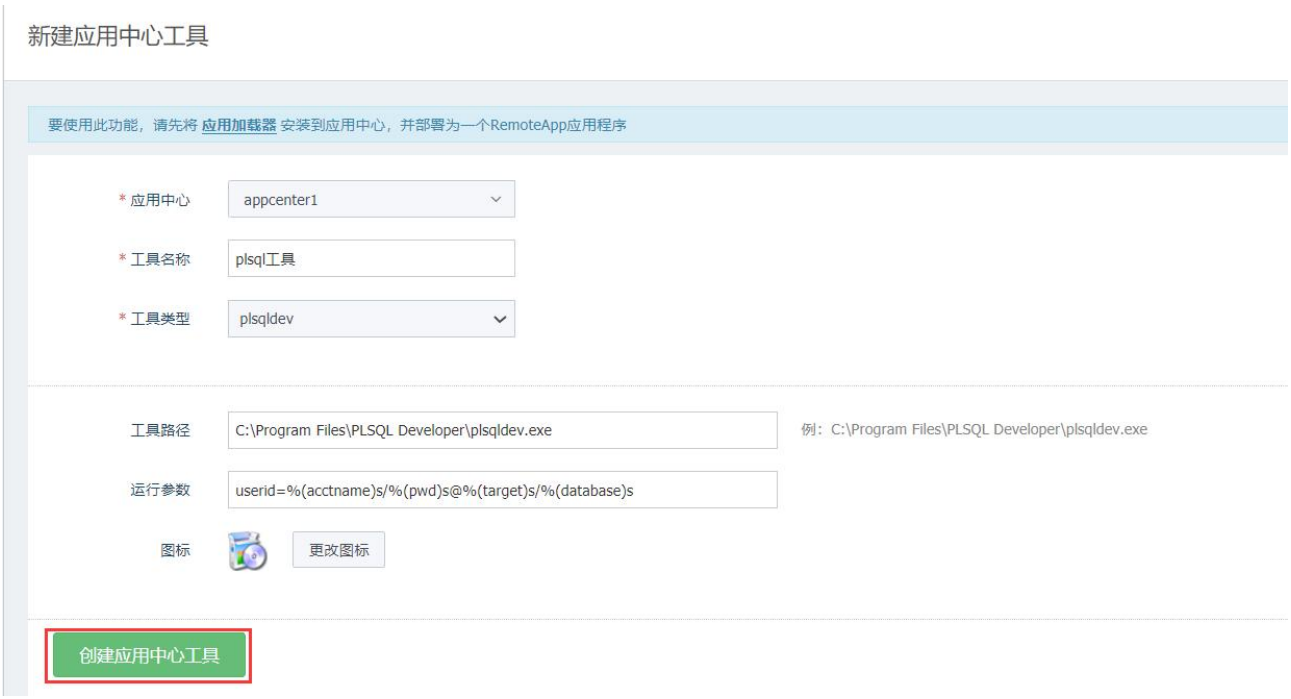


2) 修改相关信息，点击<**保存更改**>。



3) 在**应用中心工具管理**页面点击右上角的<**新建应用中心工具**>。

4) 选择应用中心（选择上文新建的应用中心）和工具类型，填写工具名称、工具路径和运行参数信息，点击<**创建应用中心工具**>完成工具创建。



步骤 4. 在应用中心上新建应用。

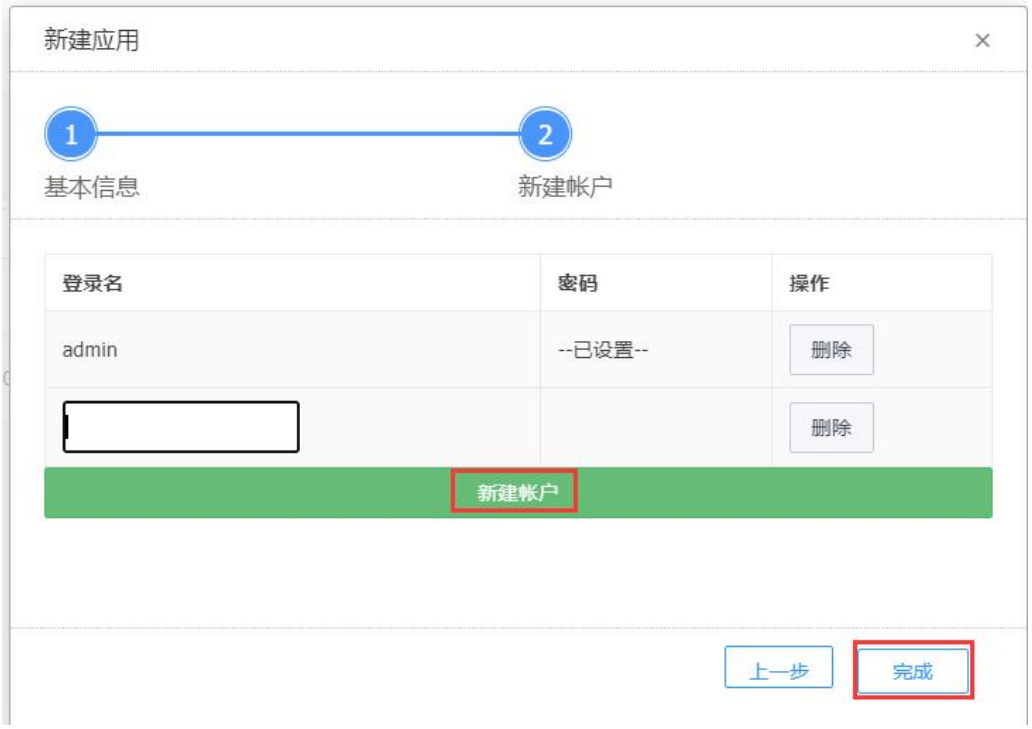
1) 在系统菜单栏选择“**资产➤应用管理**”，选择**应用列表**页签，点击页面右上角的<**新建应用**>。

2) 在弹出的**新建应用**对话框中编辑相关信息，点击<**下一步**>。

详细配置请参见下表。

配置项	说明
所属应用中心	选择应用所属的应用中心。
应用类型	支持 Web 应用、Oracle 数据库、SQL Server 数据库、MySQL 数据和自定义类型。
应用名称	最大长度为 50 字符。
目标地址	当应用类型为 Web 应用和自定义时，需要输入应用的 URL。例如：https://192.168.0.1/index.php
数据库 IP	当应用类型为数据库时，需要输入数据库服务器的 IP。
数据库名	当应用类型为数据库时，需要输入数据库库名。

3) 点击<**新建帐户**>，在登录名、密码单元格中双击，输入登录名和密码信息，为应用添加应用帐户，点击<**完成**>完成应用创建。



其他操作

- 在应用列表中点击应用右侧的<**编辑**>，可修改应用的信息。
- 勾选需要删除的应用，点击<**删除**>，在弹出的对话框中点击<**确定**>即可删除应用。

4.5.2 导出应用

可将新建应用导出至本地进行查看。操作方法如下：

步骤 1. 点击应用列表右上角的<**导出应用**>。

步骤 2. 在弹出的对话框中设置密码（可点击<**密码强度说明**>查看密码强度要求，设置密码后在解压导出的文件时需要输入密码），点击<**导出应用**>，将应用导出至本地。

4.5.3 导入应用

通过批量导入应用的方式可以提高新建应用的效率。操作方法如下：

步骤 1. 在应用列表页面点击右上角的<**导入应用**>。

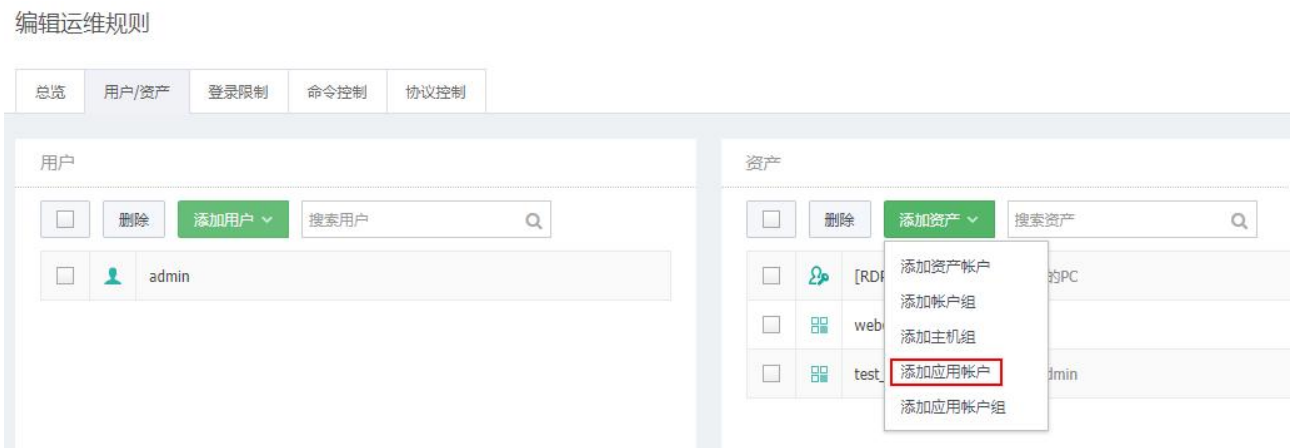
步骤 2. 在弹出的**导入应用**对话框中点击<**下载模板文件**>，下载模板文件至本地。参照模板文件示例修改文件。

步骤 3. 点击<**上传文件**>，选择已修改的模板文件（文件大小要在 10MB 内），设置是否覆盖已有应用，点击<**导入**>即可导入应用。

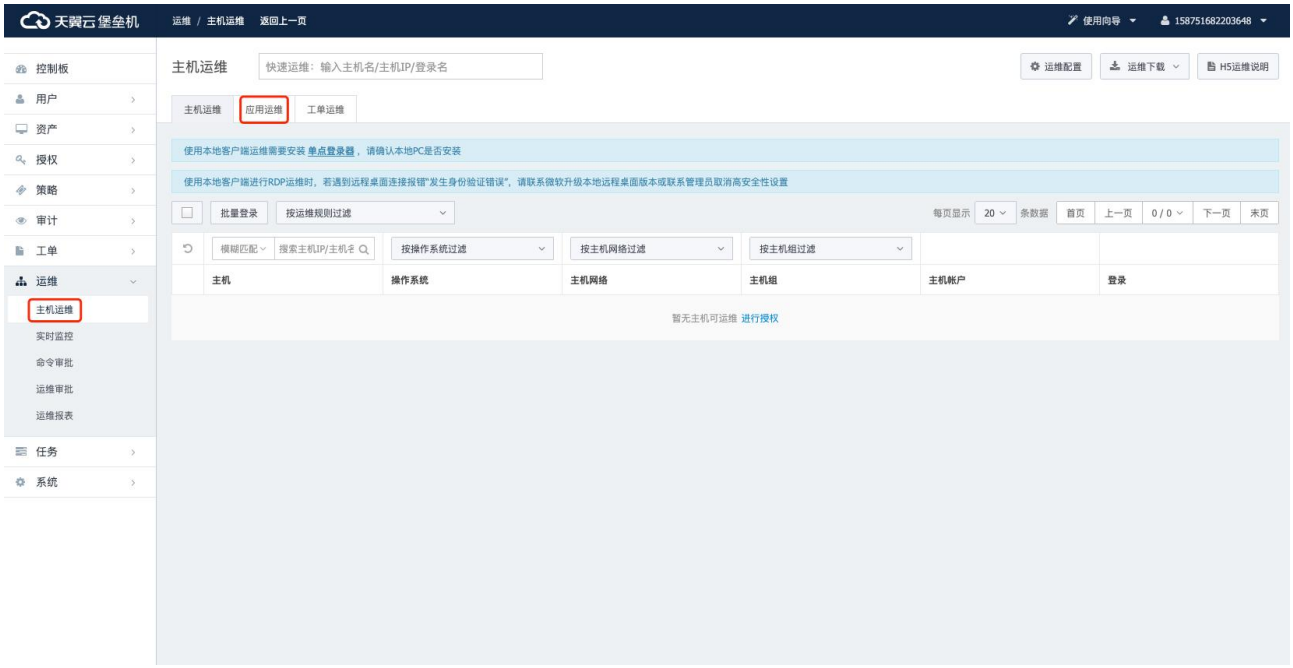
4.5.4 应用授权与运维

步骤 1. 应用帐户授权。

在菜单栏选择“**授权➤运维规则**”，进入**运维规则**页面，点击目标运维规则，在运维规则中添加应用帐户，将应用帐户授权给堡垒机用户进行运维。



步骤 2. 完成授权后，被授权用户登录系统 Web 管理平台，在菜单栏选择“**运维➤主机运维**”，选择**应用运维**页签，选择被授权的应用进行运维操作。

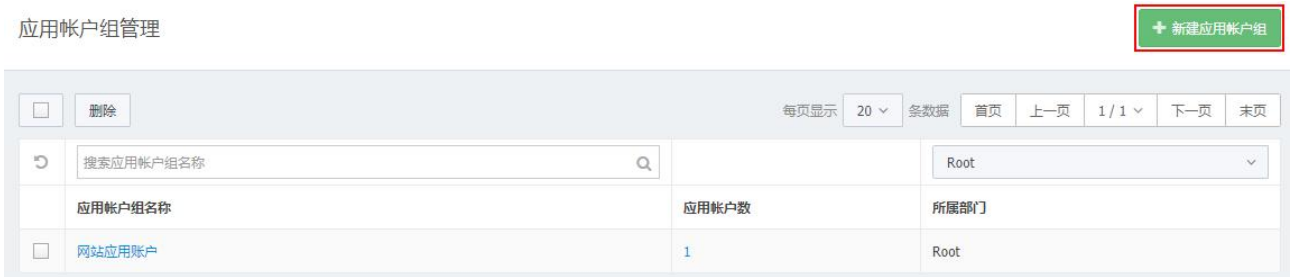


步骤 3. 运维应用时，若堡垒机用户已导入到了应用服务器中，则会使用对应的帐户登录应用服务器进行运维；若未导入到应用服务器中，则会使用管理员帐户登录应用服务器进行运维。

4.6 应用帐户组管理

将应用帐户分组，便于对应用帐户进行批量设置，减少配置工作量。创建应用帐户组并添加应用帐户的操作方法如下：

步骤 1. 在系统菜单栏选择“**资产➤应用帐户组管理**”，进入**应用账户组管理**页面，点击<**新建应用帐户组**>。



步骤 2. 选择应用组所在部门，填写应用组名称，点击<**创建应用帐户组**>，完成应用帐户组创建。

步骤 3. 在创建应用帐户组成功提示信息中点击应用帐户组名称链接进入**应用帐户组信息**页面，点击<**添加应用帐户**>。

步骤 4. 在弹出的**添加应用帐户**对话框中勾选应用账户，点击<**添加**>。

5 授权

在堡垒机中，授权管理包括运维授权和主机访问策略管理两部分内容：

- 运维授权是指将指定资产的运维权限赋予指定用户。
- 主机访问策略管理包括命令审批、运维二次审批和未授权登录审核。

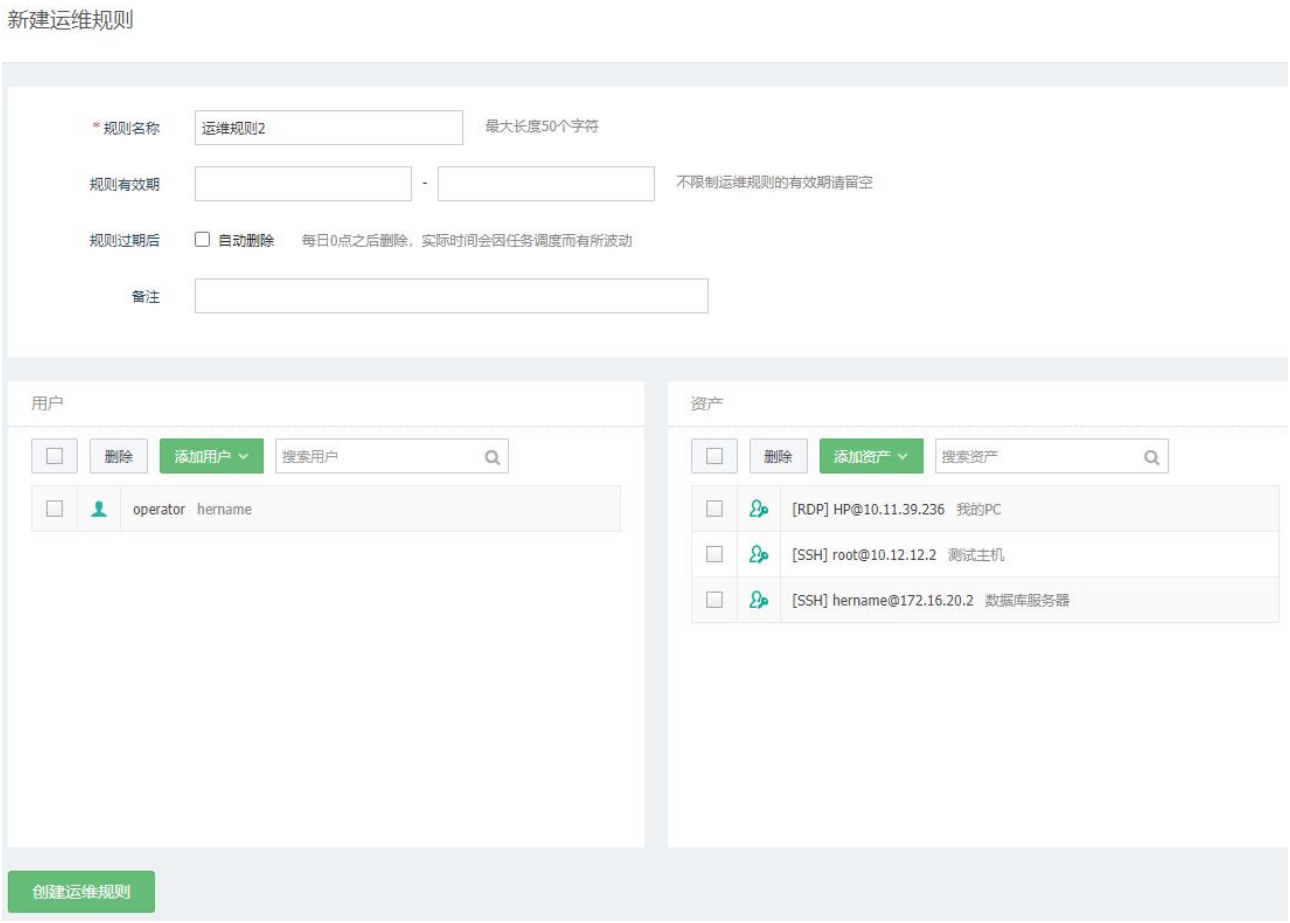
5.1 运维规则

运维规则是指将资产（包括主机、主机帐户、应用帐户）授权给用户进行运维。

5.1.1 新建运维规则

步骤 1. 在系统菜单栏选择“**授权➤运维规则**”，进入**运维规则**页面。点击右上角的<**新建运维规则**>。

步骤 2. 进入**新建运维规则**页面，填写运维规则名称、有效期等信息，设置用户与资产的对应关系（将资产的运维权限赋予给用户），点击<**创建运维规则**>，完成运维规则的创建。



部分配置项的说明请参见下表。

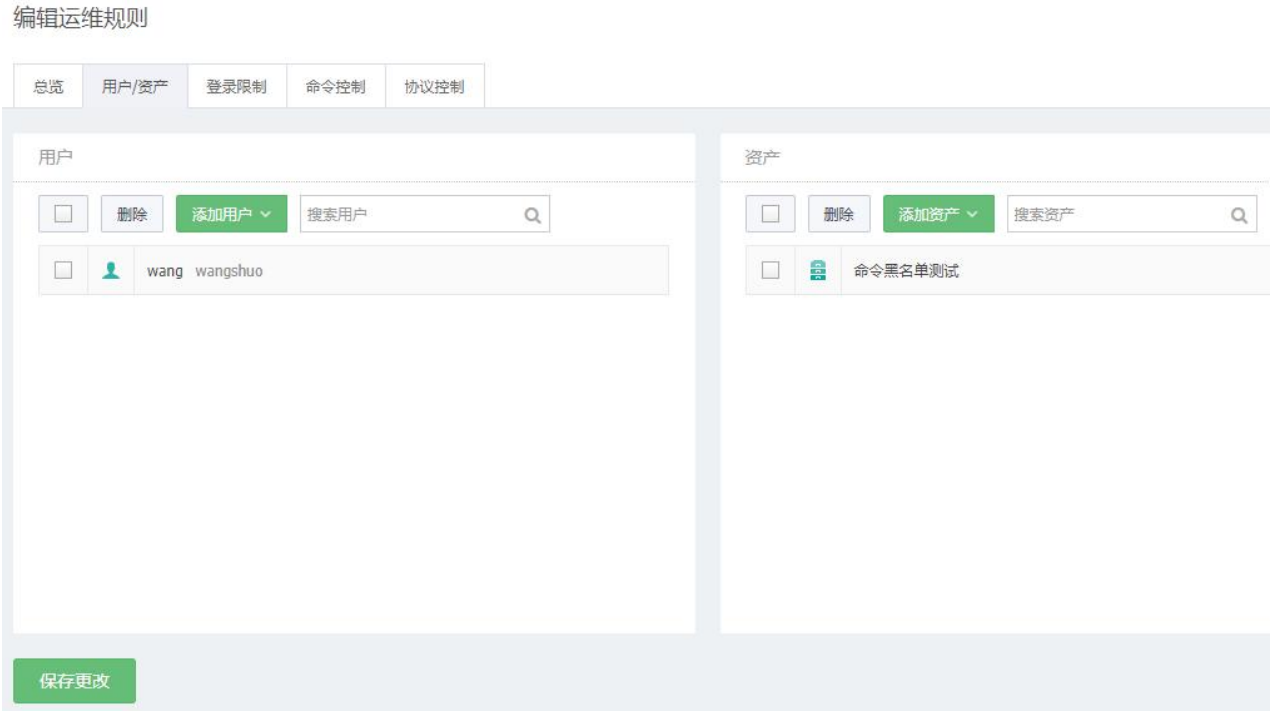
配置项	说明
用户	设置资产由哪些用户进行运维操作，包括用户和用户组。例如：点击“**添加用户➤添加用户组**”，在弹出的对话框中勾选用户组，点击<**添加**>。
资产	设置用户可以运维的资产，包括资产帐户、帐户组、主机组、应用帐户和应用帐户组。例如：点击“**添加资产➤添加帐户组**”，在弹出的对话框中勾选帐户组，点击<**添加**>。

5.1.2 修改运维规则

创建运维规则后，可修改运维规则。操作方法如下：

步骤 1. 在系统菜单栏选择“**授权➤运维规则**”，进入**运维规则**页面。点击运维规则名称或者点击运维规则右侧的“**操作➤编辑规则**”，进入**编辑运维规则**页面。修改运维规则名称、规则有效期等信息，点击<**保存更改**>。

步骤 2. 选择**用户/资产**页签，修改运维规则中的用户、资产间的授权关系，点击<**保存更改**>。

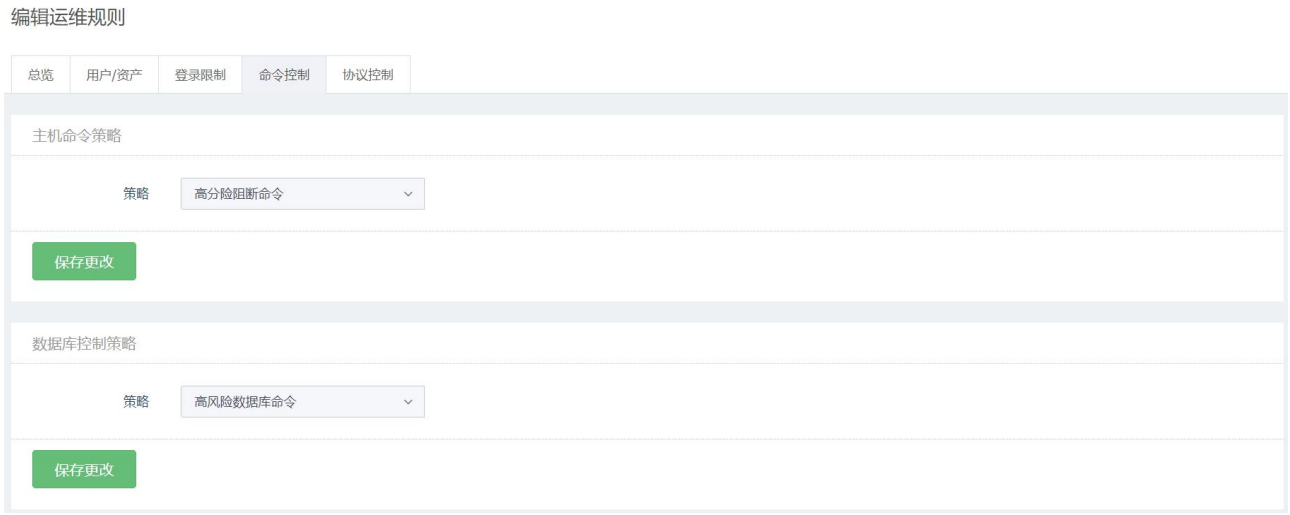


详细配置请参见下表。

配置项	说明
添加用户/用户组	◆ 点击“**添加用户➢添加用户**”，在弹出的对话框中勾选用户，点击<**添加**>。 ◆ 点击“**添加用户➢添加用户组**”，在弹出的对话框中勾选用户组，点击<**添加**>。
删除用户/用户组	勾选用户/用户组，点击<**删除**>。
添加资产	点击<**添加资产**>，在下拉菜单中选择**添加资产帐户/添加帐户组/添加主机组/添加应用帐户/添加应用帐户组**，可添加资产帐户/帐户组/主机组/应用帐户/应用帐户组等资产。
删除资产	勾选资产，点击<**删除**>。

步骤 3. 选择**登录限制**页签，勾选**启用登录限制**，设置源 IP 的黑/白名单列表及登录时段限制，点击<**保存更改**>。

步骤 4. 选择**命令控制**页签，分为主机命令和数据库控制两个策略，选择对应的控制策略，点击<**保存更改**>。关于策略的详细信息，请参见策略。



步骤 5. 选择**协议控制**页签，勾选**启用协议控制**，配置相关选项，点击<**保存更改**>。协议控制中的选项控制效果与主机配置中的选项控制效果相同。未启用运维规则协议控制时，系统默认使用主机配置中的协议控制，请参考修改主机的步骤 2。

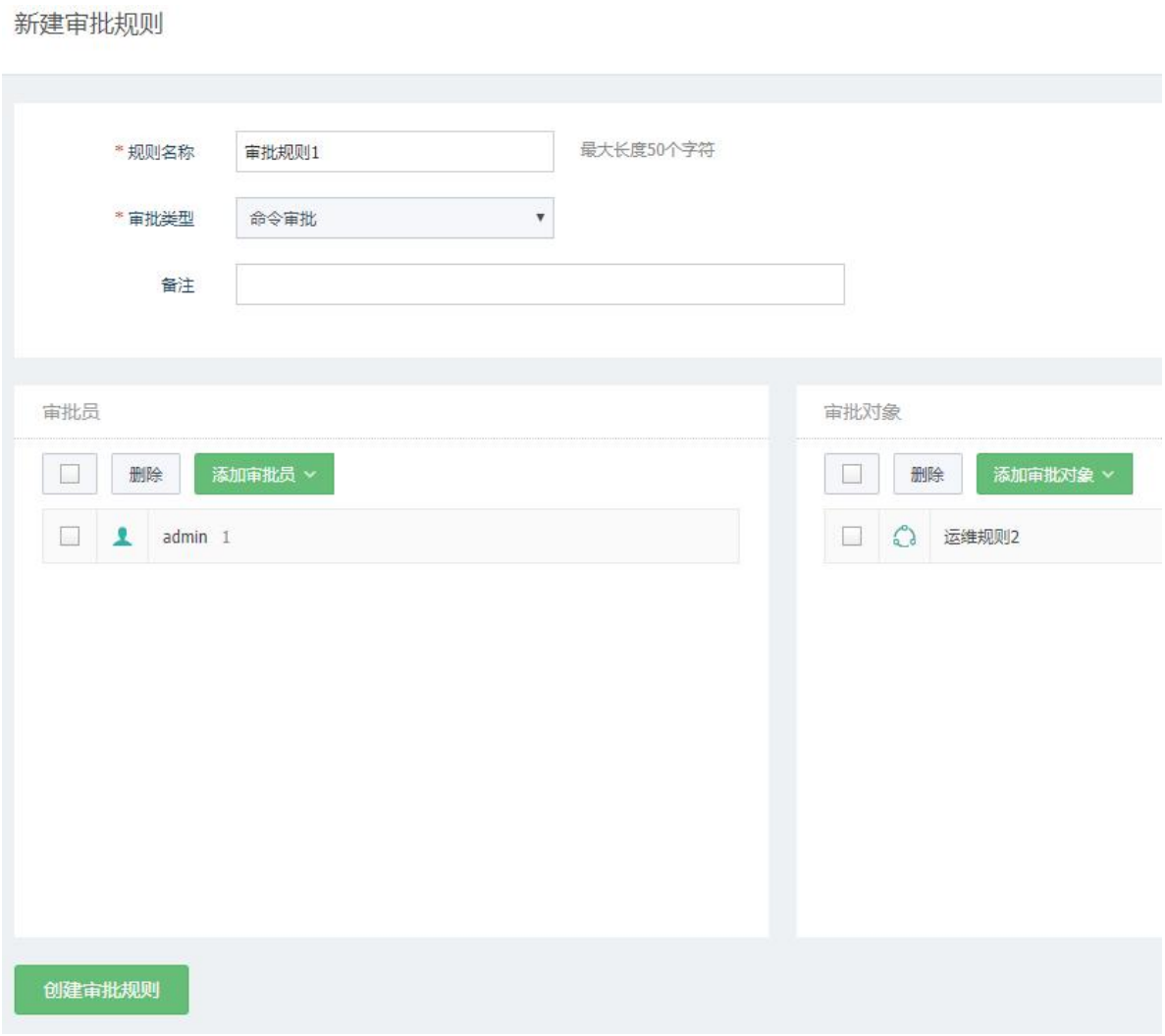
5.2 审批规则

审批规则可提供命令审批和运维二次审批规则单独管理功能，即为运维规则或主机的命令审批或运维二次审批单独指定审批人。

创建审批规则的操作方法如下：

步骤 1. 在系统菜单栏选择“**授权➤审批规则**”，进入**审批规则**页面，点击<**新建审批规则**>。

步骤 2. 填写审批规则名称，选择审批类型，添加审批员、审批对象后点击<**创建审批规则**>。



详细配置请参见下表。

配置项	说明
审批类型	◆ 命令审批：运维规则中开启命令控制时，可设置命令审批类型的审批规则，指定命令审批人。若该运维规则未指定审批人，则默认命令审批人为运维的资产所在部门及其上级部门的运维管理员和部门管理员。 ◆ 运维二次审批：协议控制中开启会话二次审批时，需要审批人审批通过后运维员方可登录主机进行运维。运维二次审批可为运维规则或主机指定会话二次审批的审批人。若未在审批规则中指定会话二次审批的审批员，则默认审批员为运维的资产所在部门及其上级部门的运维管理员和部门管理员。
审批员	设置审批员。点击“**添加审批员➤添加用户**”，在弹出的对话框中选择用户。
审批对象	审批员要审批的运维规则或者主机或者应用账户。 ◆ 点击“**添加审批对象➤添加运维规则**”，在弹出的对话框中选择运维规则。 ◆ 点击“**添加审批对象➤添加主机**”，在弹出的对话框中选择主机。 ◆ 点击“**添加审批对象➤应用账户**”，在弹出的对话框中选择应用账户。

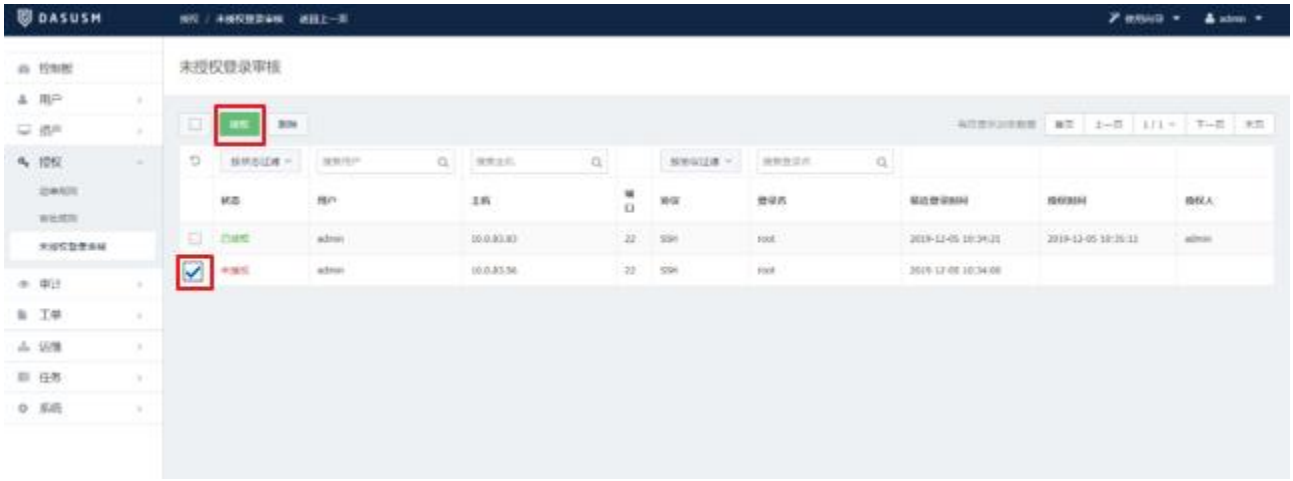
进入**审批规则**页面，点击审批规则名称/审批员/审批对象，进入**编辑审批规则**页面，可修改审批规则名称、审批类型、审批员、审批对象等信息。勾选审批规则，点击<**删除**>，在弹出的对话框中点击<

确定>即可删除审批规则。

5.3 未授权登录审核

未授权登录审核是指管理员对用户登录未授权主机的操作进行审核。审核通过后，该主机将在对应用户的主机运维列表中显示，之后该用户再次运维该主机时无需再输入主机信息。未授权登录审核的操作方法如下：

在系统菜单栏选择“**授权➤未授权登录审核**”，进入**未授权登录审核**页面，勾选未授权条目，点击<**授权**>，即可自动创建相应的授权关系。



6 策略

策略是指当运维员在执行特定命令（主机命令或者数据库命令）时，堡垒机会执行对应的控制操作（如“阻断会话”等）。

6.1 主机命令策略

6.1.1 新建主机命令策略

步骤 1. 在系统菜单栏选择“**策略➤主机命令策略**”，进入**主机命令策略**页面，点击<**新建策略**>。

步骤 2. 进入**新建主机命令策略**页面，编辑策略名称，点击<**新建命令集**>。

步骤 3. 在弹出的**新增命令集**对话框中编辑相关信息，点击<**保存**>。

详细配置请参见下表。

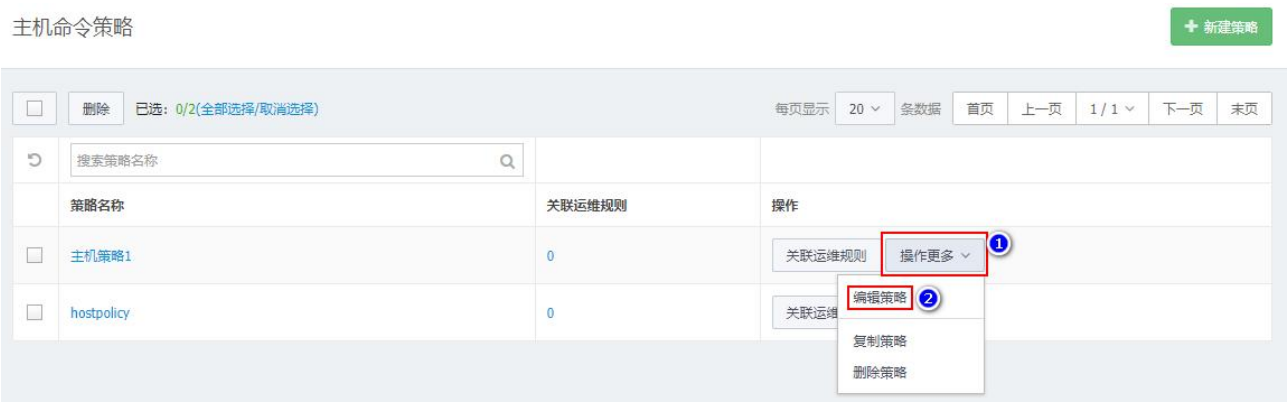
配置项	说明
命令集名称	用来标识命令集，最大长度为 50 字符。
动作	对符合/不符合的规则执行相应动作（如“阻断会话”等）。
日志级别	当堡垒机匹配到该策略时会产生日志信息，指定日志信息的级别，包括非法、高危、中危、低危和提示。
匹配方式	支持通配符和正则表达式。
命令集	设置命令，需遵循通配符或者正则表达式使用规范。

可新增多条命令集。

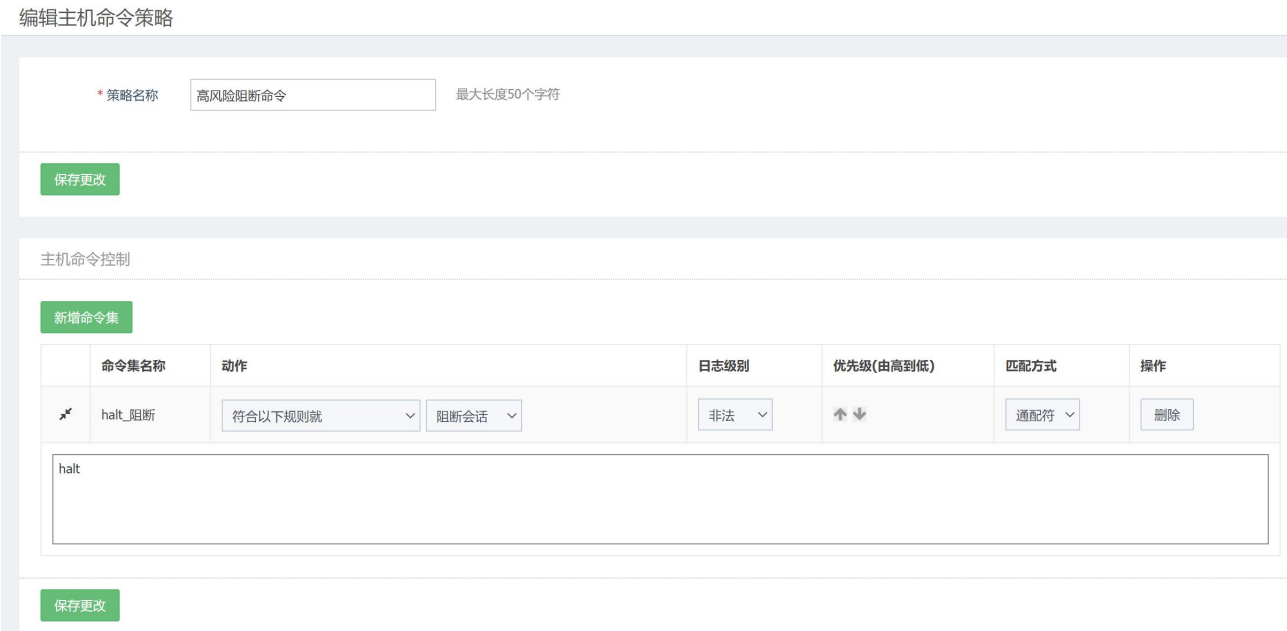
步骤 4. 点击<**创建策略**>，即可创建主机命令策略。

6.1.2 修规主机命令策略

步骤 1. 在目标策略的**操作**列中点击“**操作更多➤编辑策略**”。



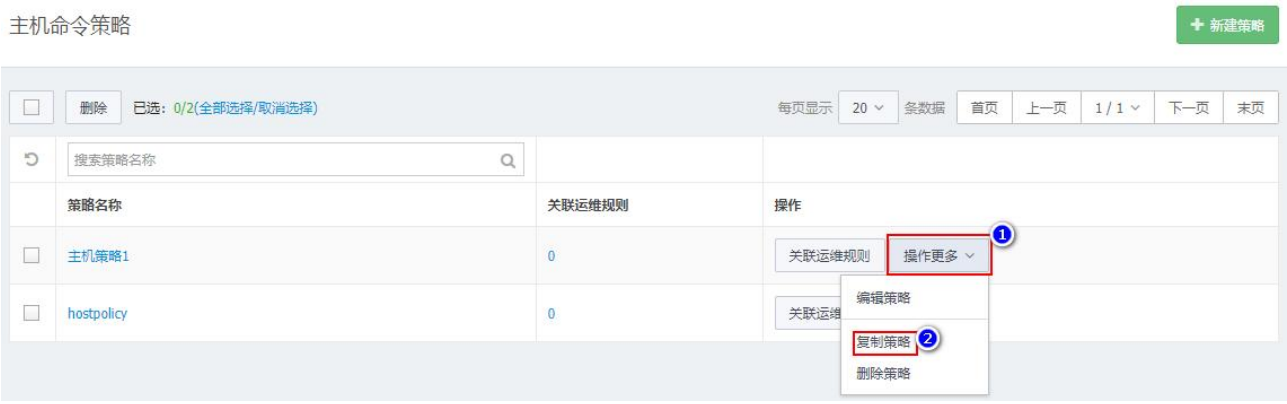
步骤 2. 进入**编辑主机命令策略**页面，修改相关信息，点击<**保存更改**>。



6.1.3 复制主机命令策略

复制主机命令策略，方便用户在已有策略的基础上进行修改。操作方法如下：

步骤 1. 在目标策略的**操作**列中点击“**操作更多➤复制策略**”。



步骤 2. 在弹出的**复制策略**对话框中编辑策略名称，点击<**复制策略**>。

6.1.4 删除主机命令策略

勾选需要删除的策略，点击<**删除**>，在弹出的对话框中点击<**确定**>即可删除主机命令策略。

6.1.5 关联运维规则

创建主机命令策略后，需要关联运维规则。当运维员运维关联运维规则中的资产时，则会执行该主机命令策略。关联运维规则的操作方法如下：

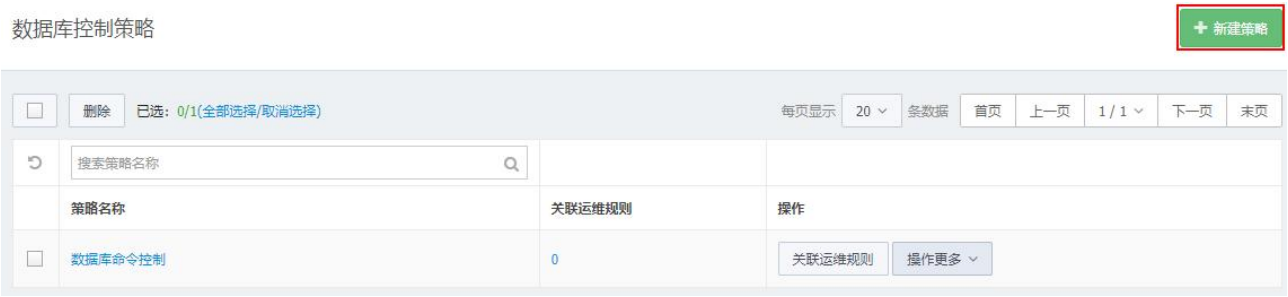
步骤 1. 在目标策略的**操作**列中点击<**关联运维规则**>。

步骤 2. 在弹出的**添加运维规则**对话框中勾选运维规则（可勾选多项），点击<**添加**>。

6.2 数据库控制策略

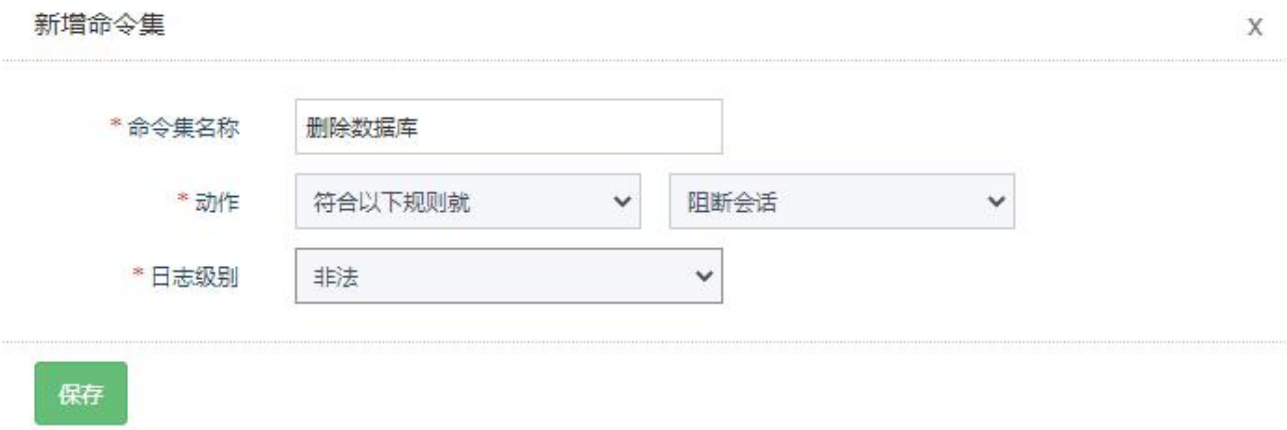
6.2.1 新建数据库控制策略

步骤 1. 在系统菜单栏选择“**策略➤数据库控制策略**”，进入**数据库控制策略**页面，点击<**新建策略**>。



步骤 2. 进入**新建数据库控制策略**页面，编辑策略名称，点击<**新建命令集**>。

步骤 3. 在弹出的**新增命令集**对话框中编辑相关信息，点击<**保存**>。



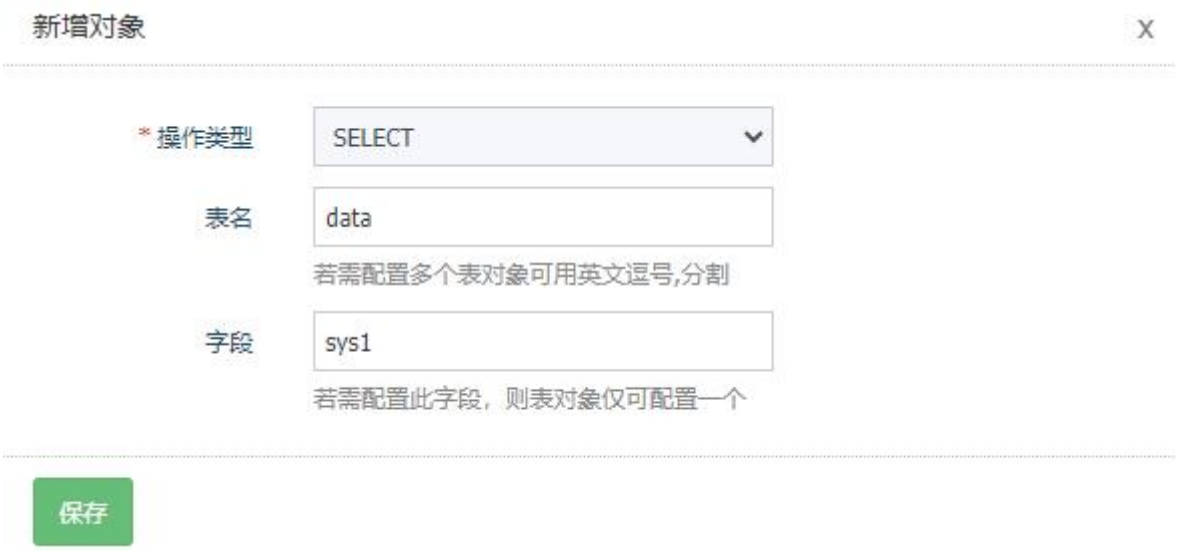
详细配置请参见下表。

配置项	说明
命令集名称	用来标识命令集，最大长度为 50 字符。
动作	对符合/不符合的规则执行相应动作（如“阻断会话”等）。

日志级别	当堡垒机匹配到该策略时会产生日志信息，指定日志信息的级别，包括非法、高危、中危、低危和提示。

步骤 4. 在命令集列表中点击**操作**列的<**新增对象**>。

步骤 5. 在弹出的**新增对象**对话框中编辑相关信息，点击<**保存**>。



步骤 6. 点击<**创建策略**>，即可创建数据库控制策略。

6.2.2 其他操作

在**数据库控制策略**页面可进行以下操操作：

- 修改数据库控制策略：在目标策略的**操作**列中点击“**操作更多➤编辑策略**”。
- 复制数据库控制策略：在目标策略的**操作**列中点击“**操作更多➤复制策略**”。
- 删除数据控制策略：在目标策略的**操作**列中点击“**操作更多➤删除策略**”，在弹出的对话框中点击<**确定**>。
- 关联运维规则：在目标策略的**操作**列中点击<**关联运维规则**>。

详细操作不再赘述，与主机命令策略的操作方法类似，可参考主机命令策略。


数据库控制策略
新建策略
删除
已选：0/2(全部选择/取消选择)
每页显示 20 条数据
首页
上一页
1 / 1
下一页
末页
搜索策略名称
策略名称
关联运维规则
操作
数据库命令控制
0
关联运维规则
操作更多
禁止删除数据库
0
编辑策略
复制策略
删除策略

7 审计

审计是指审计员对运维员的运维操作记录进行审计，可查看运维员的操作行为记录，作为事件追溯和事故分析的依据。

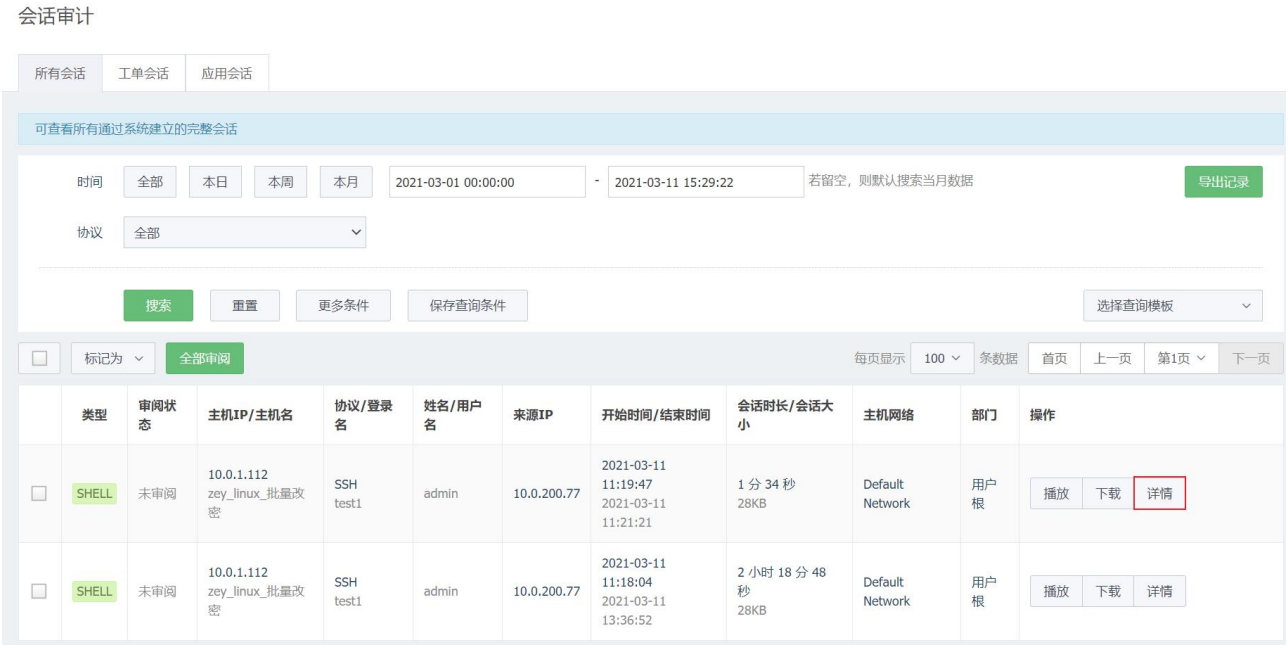
7.1 会话审计

会话审计用于记录运维员对主机操作过程的会话日志。审计员可通过会话审计定位故障及追溯故障根源。会话审计支持在线播放以及下载后离线播放两种查看方式。

会话审计支持通过时间段、主机网络、来源 IP、协议类型等条件进行筛选；支持通过执行过的命令进行全局检索，并定点跳转到命令所在的会话时间回放会话。会话审计专注于事后审计，主要用于对已经结束的会话进行录像回放或命令检索。

会话审计的操作方法如下：

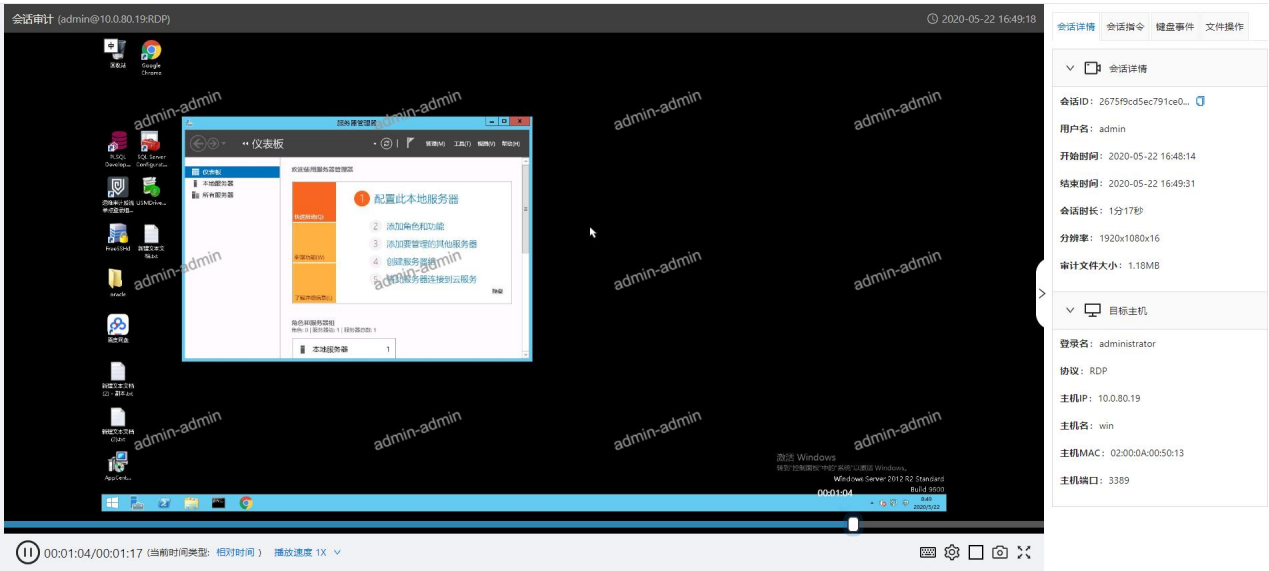
步骤 1. 在系统菜单栏选择“**审计➤会话审计**”，进入**会话审计**页面。在所有会话页面可以查看字符、图形、文件传输、应用类型的会话日志。



步骤 2. 点击**操作**列中的<**详情**>，查看详细的会话信息。

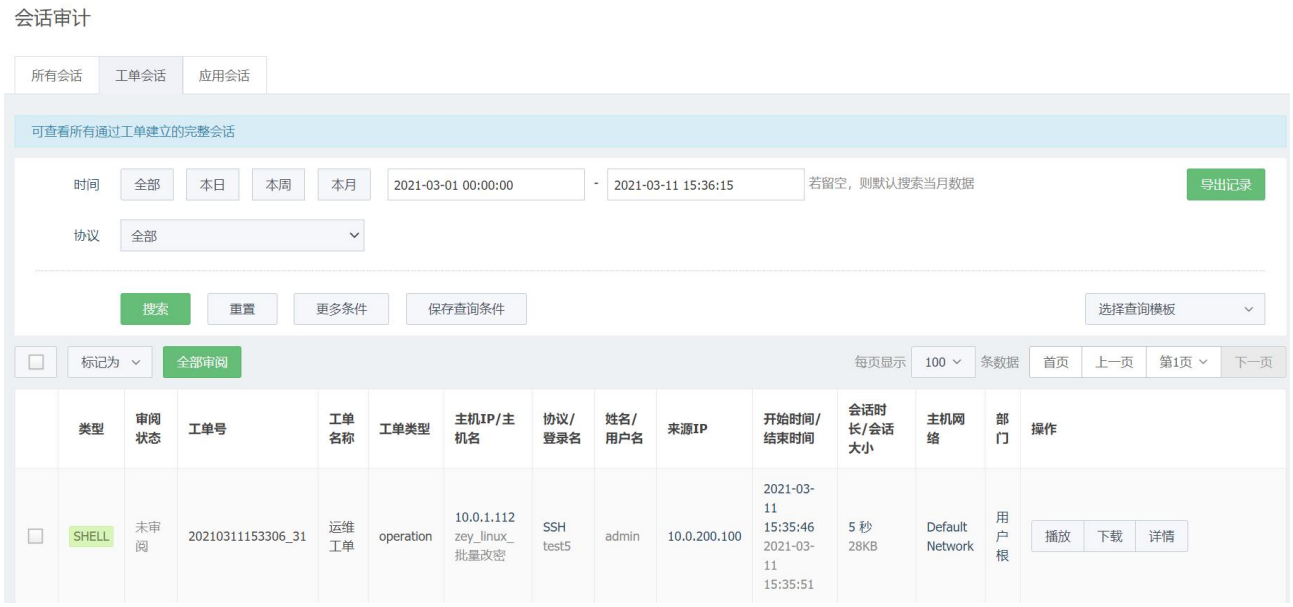
步骤 3. 在**工具下载**页面中下载离线播放器并安装到本地 PC 中。在**会话审计**页面点击**操作**列中的<**下载**>或者在会话详情对话框中点击<**下载**>，即可下载会话文件到本地，通过离线播放器播放。

步骤 4. 在**会话审计**页面点击**操作**列中的<**播放**>或者在会话详情对话框中点击<**播放**>，即可通过 Web 方式在线播放审计会话。使用 Web 方式在线播放 SFTP/FTP/Oracle/MySQL/SQL Server/DB2 协议的审计会话。



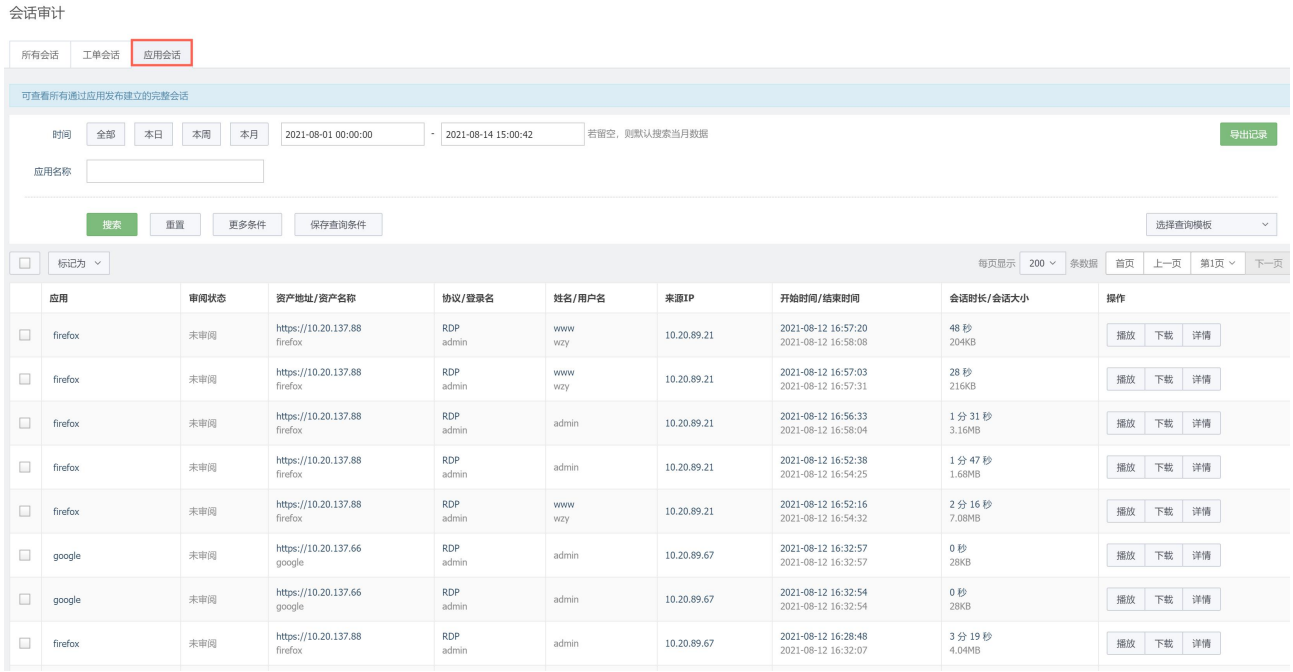
查看工单会话的操作方法如下：

在**会话审计**页面选择**工单会话**页签，可以查看工单的会话日志信息。



查看应用会话的操作方法如下：

在**会话审计**页面选择**应用会话**页签，可以查看应用的会话日志。



查看工单会话/应用会话详情、在线/离线播放工单会话/应用会话的操作方法与其他类型会话相同。

7.2 事件审计

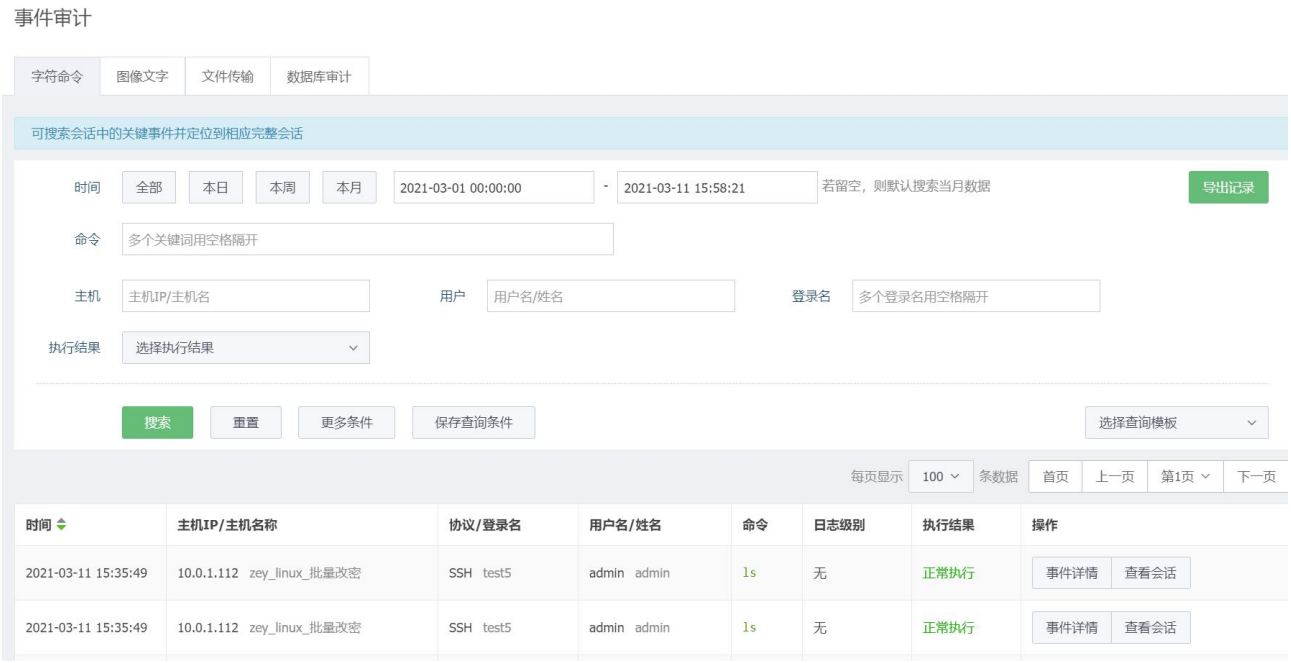
事件审计用于记录运维员操作主机的事件日志。审计员可通过事件审计定位故障原因及追溯故障根源。

事件审计包括字符命令、图像文字、文件传输和数据库审计四种类型，四种类型的事件审计的操作方法类似，本文仅以字符命令举例说明。

字符命令事件审计的操作方法如下：

步骤 1. 在系统菜单栏选择“**审计➤事件审计**”，进入**事件审计**页面，选择**字符命令**页签，可查看所有的字符命令事件审计信息。

步骤 2. 在目标事件**操作**列中点击<**事件详情**>，即可查看事件详情；点击<**查看会话**>，即可通过 Web 方式播放事件的记录。



步骤 3. 点击<**导出记录**>，在弹出的对话框中勾选需要导出字段，点击<**确定**>，即可将事件信息导出至本地进行查看。

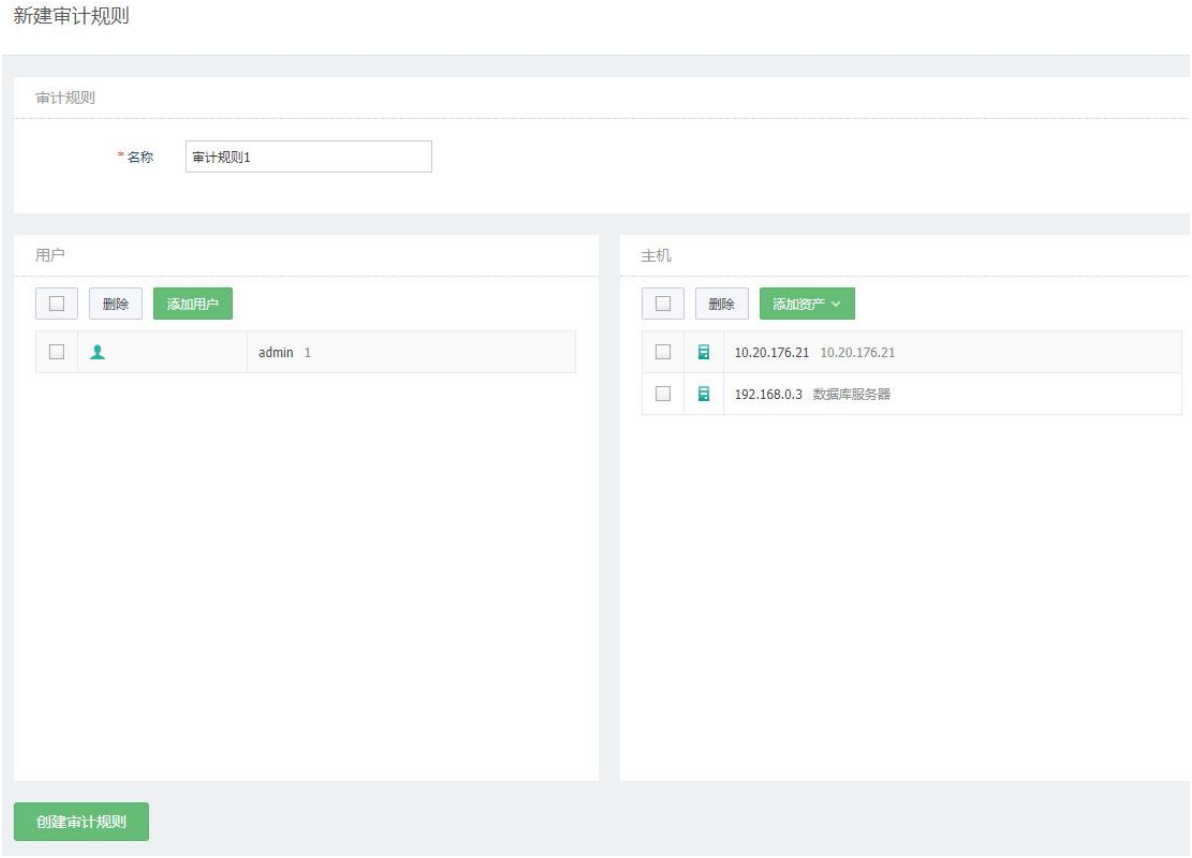
7.3 审计规则

审计规则是授权审计员审计对应的资产。

创建审计规则的操作方法如下：

步骤 1. 在系统菜单栏选择“**审计➤审计规则**”，进入**审计规则**页面，点击<**新建审计规则**>。

步骤 2. 进入**新建审计规则**页面，填写审计规则名称，添加审计员和审计资产，点击<**创建审计规则**>。



8 工单

当运维员需要运维未被授权的资产，且管理员没有开启未授权登录时，运维员可以通过工单向管理员申请运维这些资产。管理员批准工单后系统将自动创建工单中的运维授权关系。

8.1 创建工单

工单分为运维工单和密码工单两种。运维工单用于申请运维资产；密码工单用于申请获取资产的密码。

8.1.1 创建运维工单

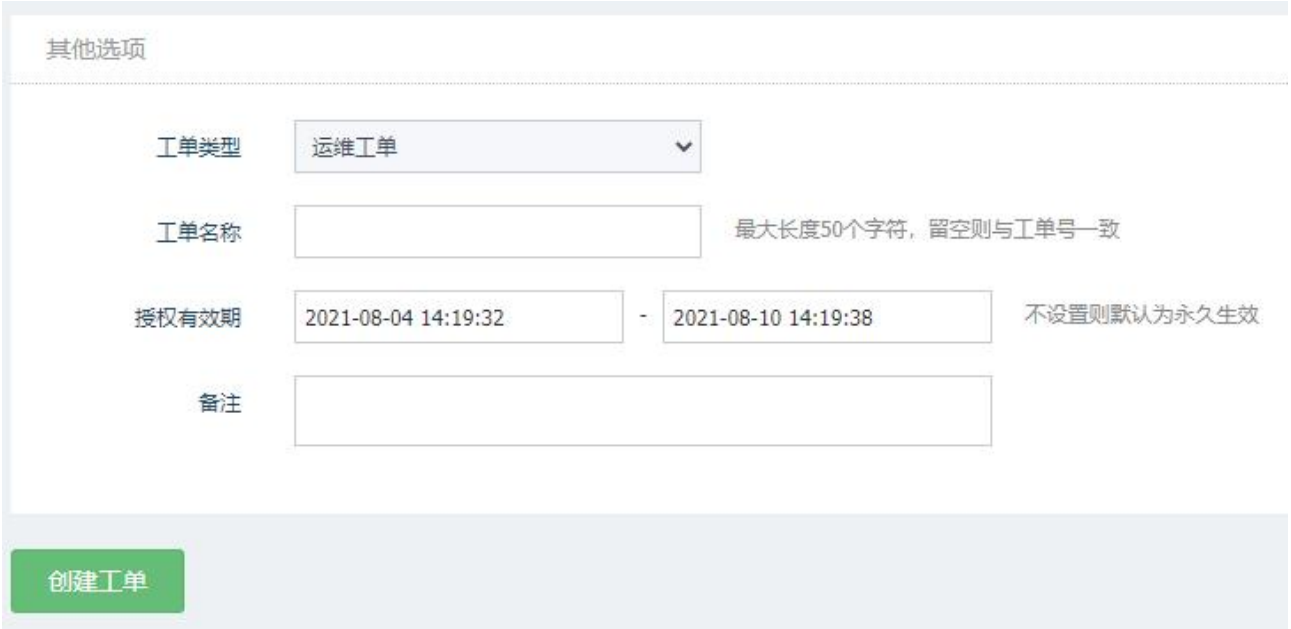
创建运维工单并进行运维的操作方法如下：

步骤 1. 在系统菜单栏选择“**工单➤我的工单**”，进入**我的工单**页面，点击<**新建工单**>。

步骤 2. 进入**新建工单**页面，点击“**添加资产➤添加主机账户**”或“**添加资产➤添加应用账户**”。

步骤 3. 在弹出的对话框中勾选要申请的资产，点击<**添加**>。

步骤 4. 工单类型设置为“运维工单”，设置授权有效期（可选），点击<**创建工单**>，完成工单申请。



步骤 5. 等待管理员审批工单通过后，运维员可在工单运维页面登录主机进行运维，详情请参见工单运维。

8.1.2 创建密码工单

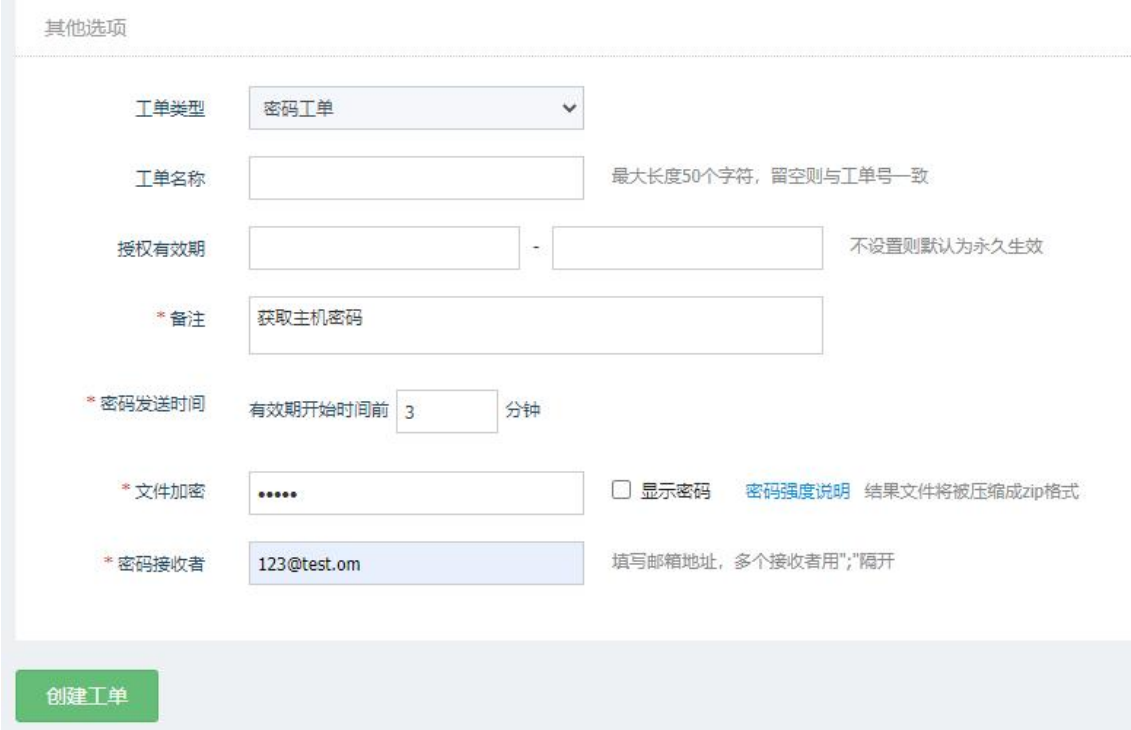
创建密码工单的操作方法如下：

步骤 1. 在系统菜单栏选择“**工单➤我的工单**”，进入**我的工单**页面，点击<**新建工单**>。

步骤 2. 进入**新建工单**页面，点击“**添加资产➤添加主机账户**”或“**添加资产➤添加应用账户**”。

步骤 3. 在弹出的对话框中勾选要申请的资产，点击<**添加**>。

步骤 4. 工单类型设置为“密码工单”，编辑相关信息，点击<**创建工单**>，完成密码工单的申请。



详细配置请参见下表。

配置项	说明
工单名称	最大长度为 50 字符，不设置则与工单号一致。
授权有效期	授权的有效时间。不设置则默认为永久生效。
备注	填写对于申请密码工单的备注。
密码发送时间	填写在该密码工单生效前几分钟发送密码邮件至密码接收者。
文件加密	用于密码文件的加密，可点击<**密码强度说明**>查看密码强度要求。
密码接收者	填写密码接收者的邮件地址，可以填写多项，用“;”分隔。需在**系统配置**页面中完善邮件配置，具体请参见邮件配置。

8.1.3 其他操作

进入**我的工单**页面，对于处于“待审批”状态的工单，可以点击工单右方的<**详情**>，进入工单信息页面修改工单信息，修改完成后点击<**保存更改**>完成工单信息修改。

勾选处于待审批状态的工单，点击<**取消**>即可取消工单申请。

对于处于“已批准”或“已拒绝”状态的工单，点击工单号或工单右方的<**详情**>，进入工单信息页面可查看工单详细信息。

运维员创建完工单后，本部门及上级部门的部门管理员和运维管理员会收到邮件提醒。

管理员能收到邮件提醒的前提条件为：

- 管理员在个人信息中填写了邮箱。
- 在系统菜单栏选择“**系统➤系统配置**”，选择**告警配置**页签，已经配置了**邮件配置**并可以正常发送测试邮件。

8.2 工单审批

运维员申请工单后，管理员对工单进行审批，审批通过后运维员才能运维工单中申请的资产。

审批工单的操作方法有以下两种：

- 在系统菜单栏选择“**工单➤工单审批**”，进入**工单审批**页面。点击工单右方<**详情**>可进入工单信息页面查看工单详细信息，对于状态为“待审批”的工单，管理员可以修改工单的信息后再审批。

工单审批

- 进入**工单审批**页面，勾选需要审批的工单，点击<**批准**>同意此工单；点击<**拒绝**>拒绝此工单。对于已批准的工单，点击<**撤销**>撤销此工单。

工单审批

9 运维

运维是指运维员登录主机或应用进行维护操作。

9.1 主机运维

9.1.1 运维配置

在进行主机运维前需要进行运维配置，操作方法如下：

步骤 1. 在系统菜单栏选择“**运维➤主机运维**”，进入**主机运维**页面，点击<**运维配置**>。

步骤 2. 弹出**运维配置**对话框，默认进入 RDP 配置页面。设置分辨率（分辨率选择“全屏”，客户端运维自动全屏，H5 运维提示全屏，批量运维只支持默认分辨率）、会话标题、连接模式、本地设备和资源、本地驱动器。

步骤 3. 点击<**SSH&TELNET&Rlogin**>，选择客户端程序、终端类型、编码格式、会话标题。

步骤 4. 点击<**FTP**>，选择对应的客户端程序、设置会话标题。

步骤 5. SFTP、VNC&X11、SQL Server、MySQL、DB2、PostgreSQL、KingbaseES、DM 配置与 FTP 配置类似，参考 FTP 配置即可。

步骤 6. 点击<**Oracle**>，选择对应的客户端程序，填写配置文件路径、会话标题。

步骤 7. 点击<**保存**>。

9.1.2 主机运维配置

主机运维支持 B/S 运维、C/S 运维和 H5 运维三种运维方式。

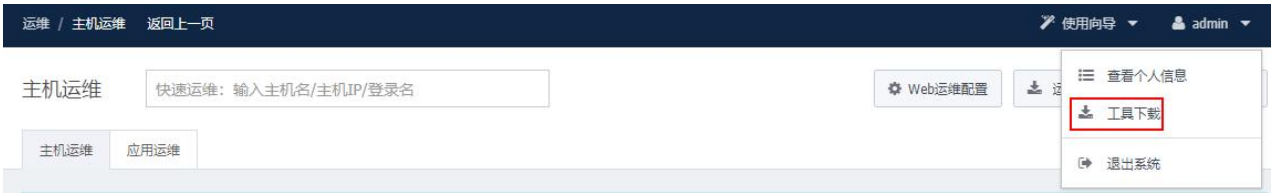
- B/S 运维支持 SSH、Telnet、Rlogin、FTP、SFTP、VNC、X11、RDP、Oracle、SQL Server、MySQL、DB2、PostgreSQL、KingbaseES、DM 协议。
- C/S 运维支持 SSH、Telnet、Rlogin、FTP、SFTP、RDP、Oracle 协议。
- H5 运维支持 SSH、Telnet、Rlogin、VNC、X11、RDP、SFTP、FTP 协议。

进行主机运维前，需要做好以下准备工作：

- 管理员创建相应用户和资产的运维规则。
- 下载运维工具。

下载运维工具的操作方法如下：

步骤 1. 在页面右上角点击当前登录用户名，从下拉菜单选择“**工具下载**”，进入**工具下载**页面。



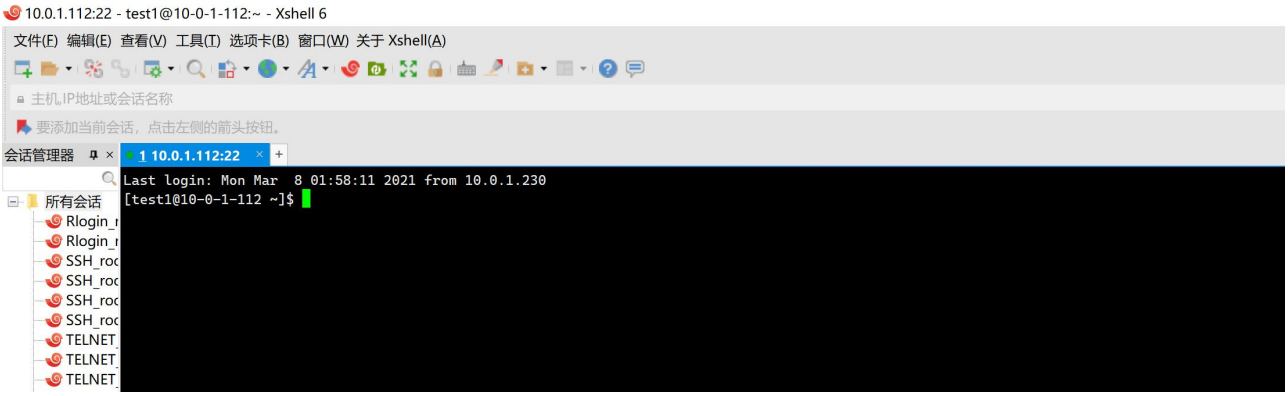
步骤 2. 点击工具右侧的<**本地下载**>，下载相应工具的安装包到本地。或点击<**官方网站**>，到相应工具的官方网站获取安装包。各工具的用途请参见下表。

名称	说明
单点登录器	单点登录器是当使用 Web 方式调用运维客户端工具时需要用到的登录工具。
USBKEY 控件（IE）	USBKEY 控件用于系统启用 USBKEY 认证方式时的登录插件。
USBKEY 控件（国密）	USBKEY 控件用于系统启用国密 USBKEY 认证方式时的登录插件。
离线播放器	旧版离线播放器，与 Adobe ATR 一起安装使用。
Web 代填/改密代填脚本 Chrome 浏览器插件	Web 应用代填/改密脚本录制插件
运维客户端	使用运维客户端进行主机运维和应用运维。
新审计离线播放器	用于会话审计里的录像文件导出/归档后进行离线查看。
Adobe AIR	旧版离线播放器运行环境。
Flash Player 12	Flash 播放器，页面上传/下载按钮、播放审计会话的依赖插件。
Chrome	谷歌浏览器。
FileZilla	用于连接 SFTP/FTP 服务器。
WinSCP	用于连接 SFTP/FTP 服务器。
PuTTY	用于连接 SSH、telnet、Rlogin 协议服务器。
Mstsc	用于连接 RDP 协议服务器。
RealVNC	用于连接 VNC 协议服务器。
SecureFX	用于连接 SFTP/FTP 服务器。
SecureCRT	用于连接 SSH、telnet、Rlogin 协议服务器。
Xshell	用于连接 SSH、telnet、Rlogin 协议服务器。

◆ B/S 运维：

步骤 1. 在系统菜单栏选择“**运维➢主机运维**”，进入**主机运维**页面，点击资产列表**登录**列中的图标，选择登录方式。

步骤 2. 点击<**本地客户端登录**>，自动调用运维配置中配置的 SSH 客户端登录服务器。

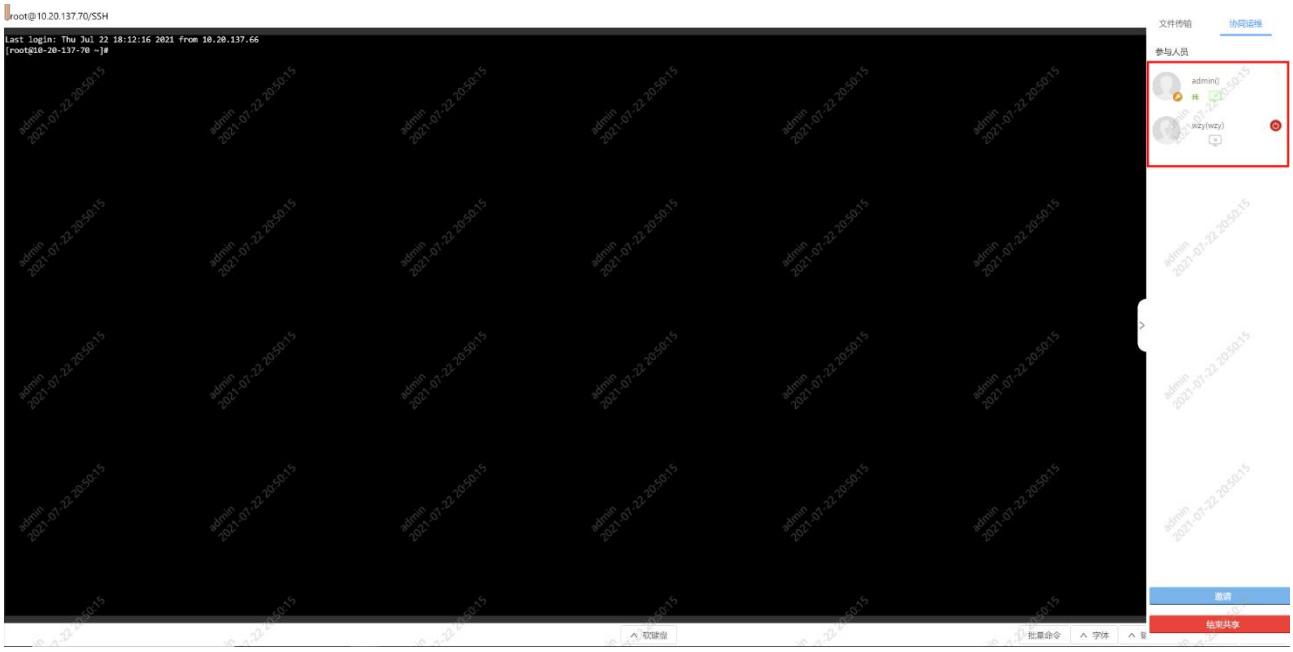


◆ H5 运维：

步骤 1. 在系统菜单栏选择“**运维➤主机运维**”，进入**主机运维**页面，点击资产列表**登录**列中的图标，选择登录方式。

步骤 2. 点击<**H5 客户端登录**>，通过 H5 客户端登录服务器。

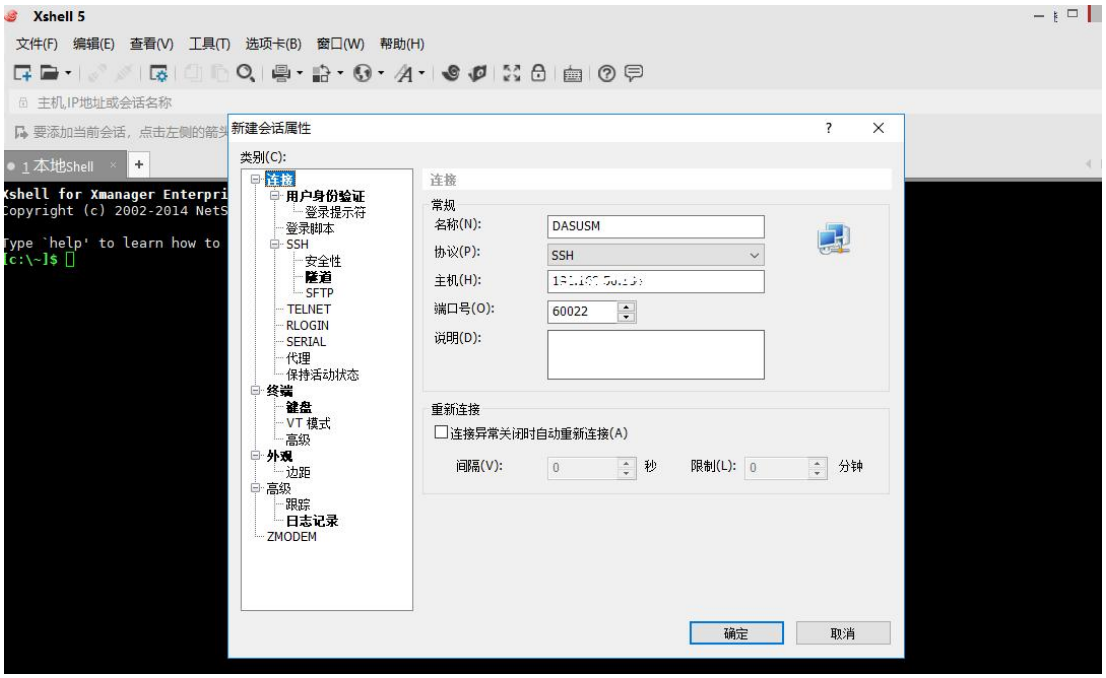
步骤 3. H5 运维方式支持协同运维。点击<**开始分享**>，生成一个链接，将链接发送给其他堡垒机用户，其他堡垒机用户登录后，即可实现协同运维。



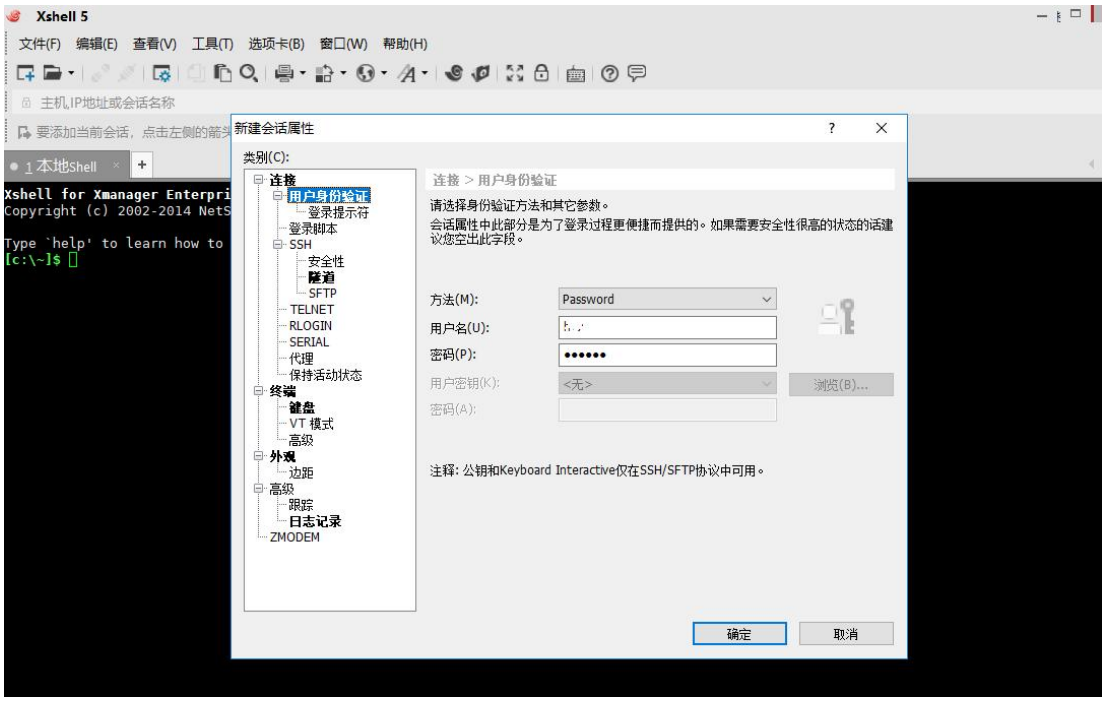
SSH、Telnet、Rlogin 协议的 H5 运维仅支持 Edge、Firefox 34 及以上版本、Chrome 31 及以上版本浏览器。

◆ C/S 运维（以 Xshell 工具为例）：

步骤 1. 打开 Xshell 工具，在连接设置中输入堡垒机的 IP 和 SSH 协议端口号（SSH 端口号可在“**系统➤网络配置**”页面查看，默认为 60022）。

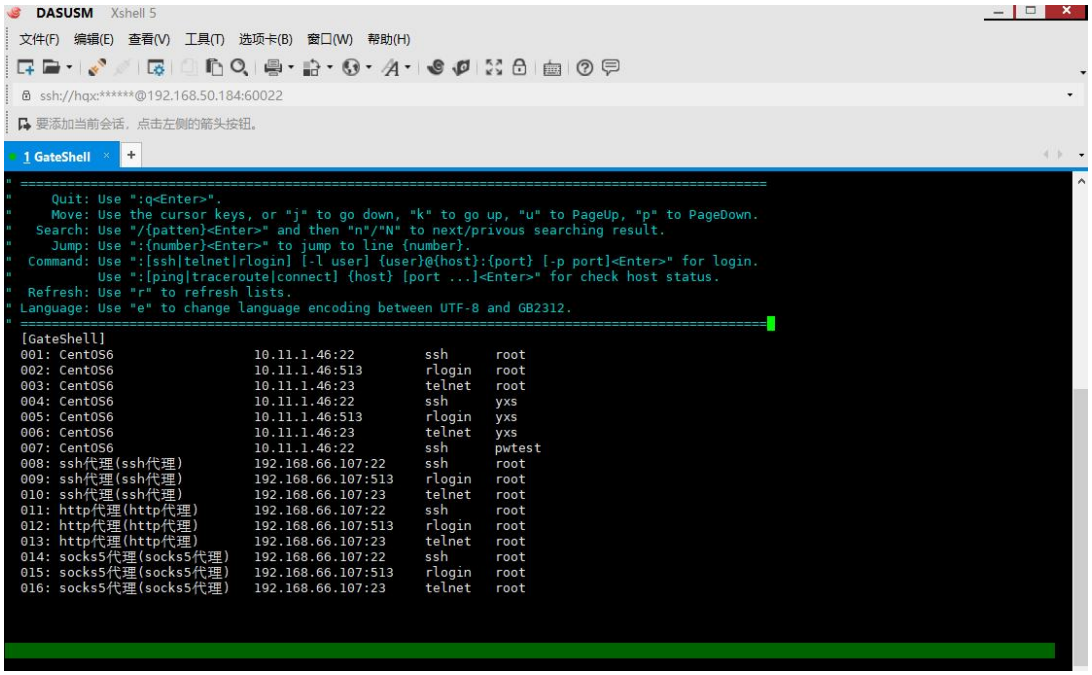


步骤 2. 在用户身份验证设置中选择 Password 方式登录，输入堡垒机的用户名和密码。或选择 Public Key 方式登录，选择对应的私钥，使用 Public Key 方式登录需要在堡垒机的个人信息中配置用户 SSH 公钥。



步骤 3. 点击<**确定**>，连接堡垒机。成功登录系统后，进入资产选择界面，通过键盘的上、下方向键选择想要运维的服务器主机，按回车键即可登录目标服务器主机进行运维。

需要在菜单栏选择“**系统➤系统配置**”，在 **SSH 登录**配置项中取消勾选 **Shell 使用命令行方式**，才能在 SSH 登录界面查看到如下的资产信息。



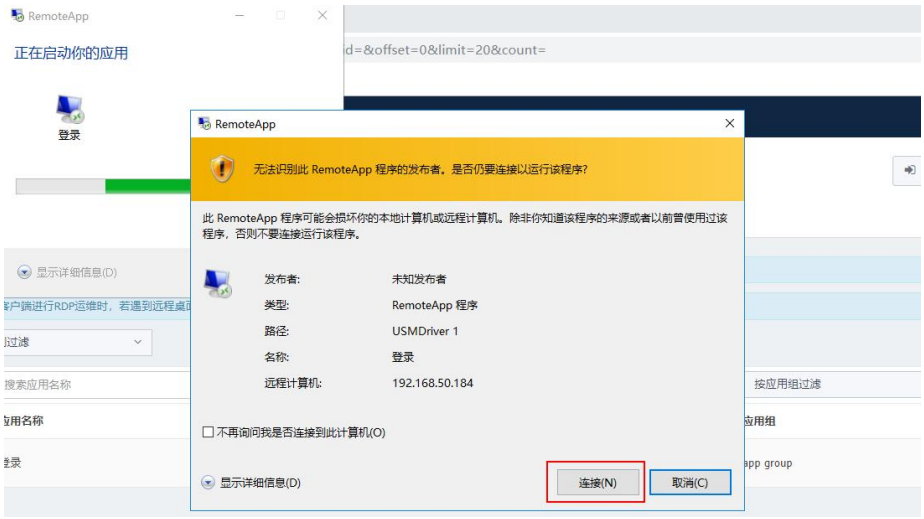
9.1.3 应用运维

应用运维支持 B/S 和 H5 两种方式运维。

◆ B/S 运维

步骤 1. 在系统菜单栏选择“**运维➤主机运维**”，进入**主机运维**页面，选择**应用运维**页签。

步骤 2. 在应用列表中点击**登录**列中的图标，自动调用 RemoteApp 程序发起连接，点击<**连接**>，连接远程应用服务器进行运维。



◆ H5 运维

在应用运维页面，在应用列表中点击**登录**列中的图标，通过 H5 客户端登录应用服务器进行应用运维。

9.1.4 工单运维

当主机运维工单被管理员审批通过后，运维员可在**工单运维**页面登录主机进行运维，操作方法如下：

步骤 1. 在菜单栏选择“**运维➤主机运维**”，选择**工单运维**页签，点击<**详情**>。

步骤 2. 在弹出的**详情**对话框中点击<**登录**>。

步骤 3. 在弹出的**运维登录**对话框中设置端口，选择登录方式，点击<**确定**>，即可登录主机进行运维操作。

9.1.5 未授权登录

未授权登录是指运维员登录未被管理员授权的主机。此功能需管理员在**系统配置**中开启**允许 Web 未授权登录**。未授权登录的操作方法如下：

步骤 1. 在**主机运维**页面点击<**未授权登录**>。

步骤 2. 在弹出的**运维登录**对话框中编辑相关信息，点击<**确定**>。之后按照页面提示进行操作。

详细配置请参见下表。

配置项	说明
主机 IP	支持 IPv4 和 IPv6。

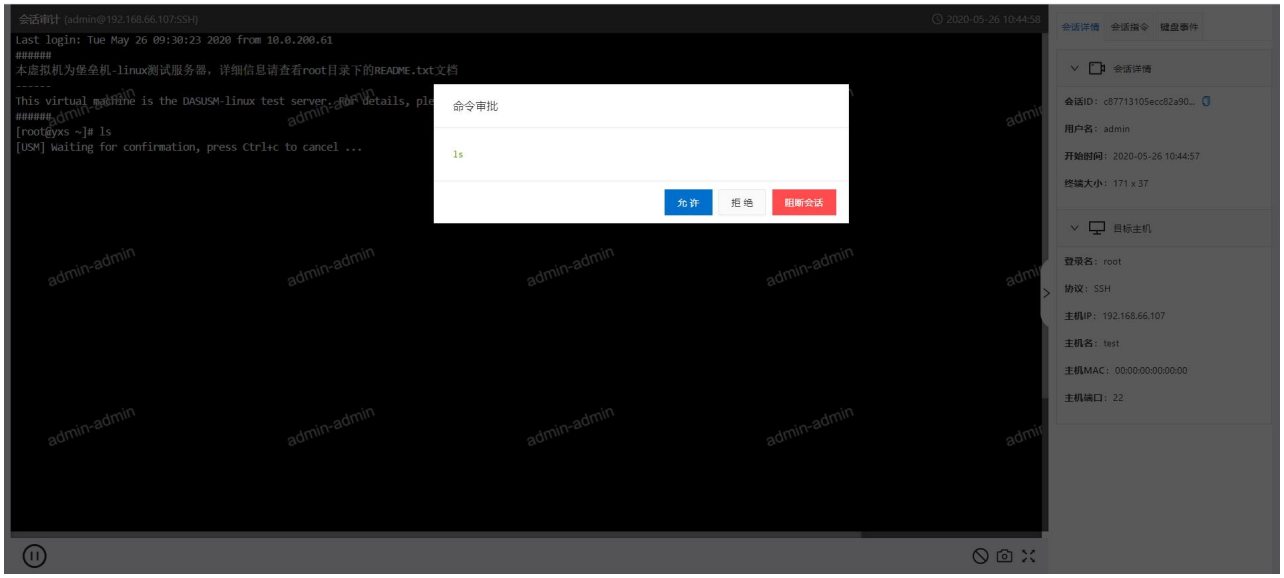
协议	选择登录目标主机所使用的协议。包括 Telnet、SSH、SFTP、RDP、VNC、SQL Server、MySQL、Oracle、DB2、PostgrSQL、KingbaseES、X11、DM 和 Rlogin。
端口	目标主机的端口。建议使用默认端口。
登录名	目标主机的用户名。
密码	目标主机用户名对应的密码。
登录方式	包括本地客户端和 H5 客户端登录。

9.2 实时监控

实时监控用于管理正在运维的主机的会话，进行命令审批或会话阻断等操作。操作方法如下：

在系统菜单栏选择“**运维➤实时监控**”，进入**实时监控**页面。选择**所有会话**页签，可查看当前正在运维的会话。选择**需要命令审批**页签，可查看当前正在运维且需要命令审批的会话。勾选会话后点击<**阻断会话**>可将正在运维的会话阻断。

在会话列表中点击**操作**列中的<**播放**>可查看会话内容。对于需要命令审批的会话，可在播放页面对命令操作进行审批。



9.3 命令审批

当运维员申请执行在主机命令策略中设置的命令时，管理员/命令审批员可在**命令审批**页面进行命令审批操作。命令审批的操作方法如下：

在系统菜单栏选择“**运维➤命令审批**”，进入**命令审批**页面。勾选状态为“**待审批**”的条目，点击<

允许>批准执行该命令；点击<**拒绝**>不允许执行该命令。

9.4 运维审批

运维审批即会话二次审批。对于设置了会话二次审批的主机，即使经过授权，运维员也不能直接登录主机。系统会自动生成运维申请，由管理员审批通过之后，运维员才能运维该主机。

运维审批的操作方法如下：

在系统菜单栏选择“**运维➤运维审批**”，进入**运维审批**页面，勾选状态为“待审批”的条目。点击<**批准**>，在弹出的对话框中设置审批有效期，点击<**批准**>，允许此次运维；或点击<**拒绝**>，不允许此次运维；点击<**删除**>可将运维申请从列表中删除。

在系统菜单栏选择“**运维➤运维审批**”，进入**运维审批**页面，选择**我的申请**页签。在本页面申请人可查看运维申请的审批情况。审批通过后，申请人可在此页面选择运维登录方式（点击<**本地客户端登录**>或<**H5 客户端登录**>）登录资产进行运维。

9.5 运维报表

运维报表用于统计用户的运维信息。

9.5.1 查看运维报表

在系统菜单栏选择“**运维➤运维报表**”，进入**运维报表**页面。选择用户及日期（今天、昨天、本周、本月）即可查看到该用户相应时间段内的运维数据报表。

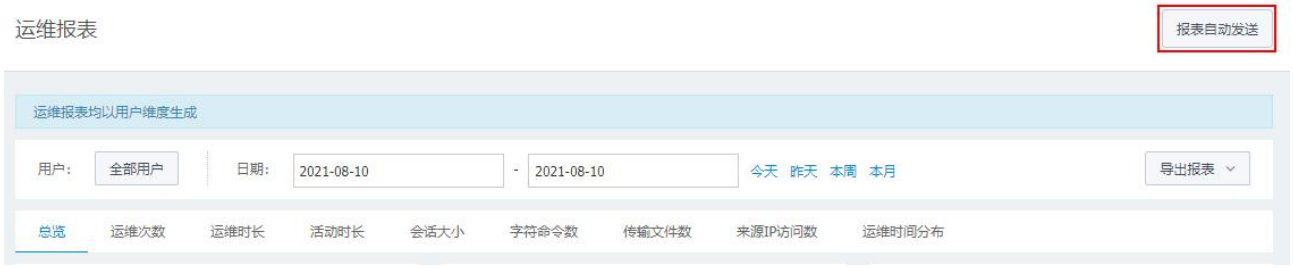
9.5.2 导出报表

点击<**导出报表**>，选择导出文件格式（DOC、PDF、HTML 和 CSV），可将报表数据导出至本地文件进行查看。

9.5.3 报表自动发送

可设置将运维报表自动以邮件形式发送给本部门的部门管理员和审计管理员。（需要先在**告警配置**页面配置收件人邮箱信息，具体请参见邮件配置）。操作方法如下：

步骤 1. 点击<**报表自动发送**>。



步骤 2. 在弹出的对话框中将状态设置为**开启**，选择发送周期和文件格式，点击<**确定**>。

10 任务

系统提供自动化的任务功能，减轻用户的手工配置工作量。任务包括改密计划、自动运维和资产巡检三个功能。

10.1 改密计划

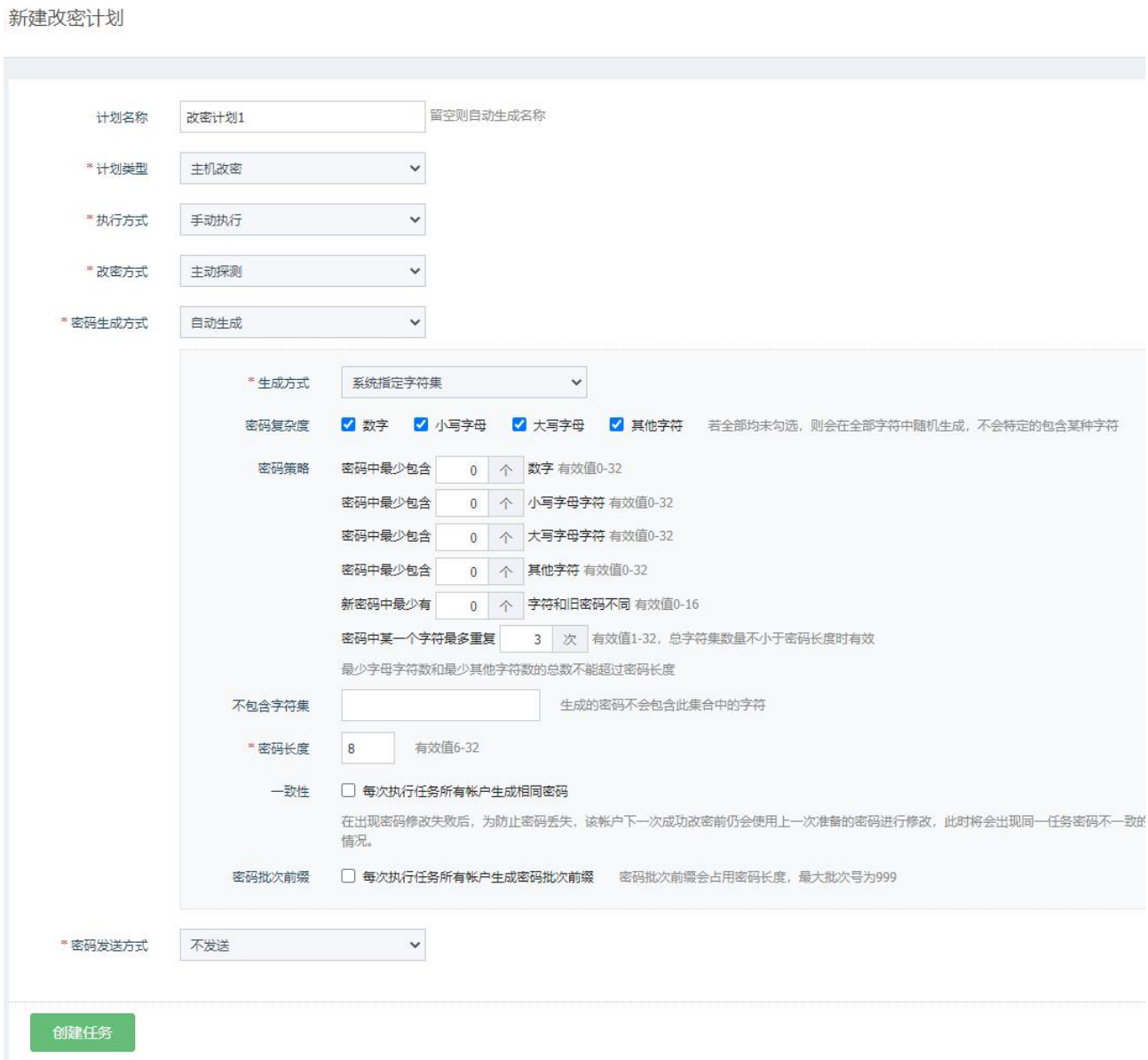
通过堡垒机的改密计划功能，可以实现主机帐户、数据库账户、Web 应用账户的密码托管。使用密码托管，可以对主机帐户、数据库账户、Web 应用账户完成一次性自动改密及定时周期改密任务。

10.1.1 创建改密计划

改密计划类型分为主机改密、数据库改密、Web 应用改密和主机工单改密。四种类型的改密计划的创建方式类似，本文仅以创建主机改密计划举例说明。

步骤 1. 在系统菜单栏选择“**任务➤改密计划**”，进入计划列表页面，点击<**新建改密计划**>。

步骤 2. 进入**新建改密计划**页面，填写计划名称，选择执行方式、改密方式、密码生成方式、密码发送方式，点击<**创建任务**>。



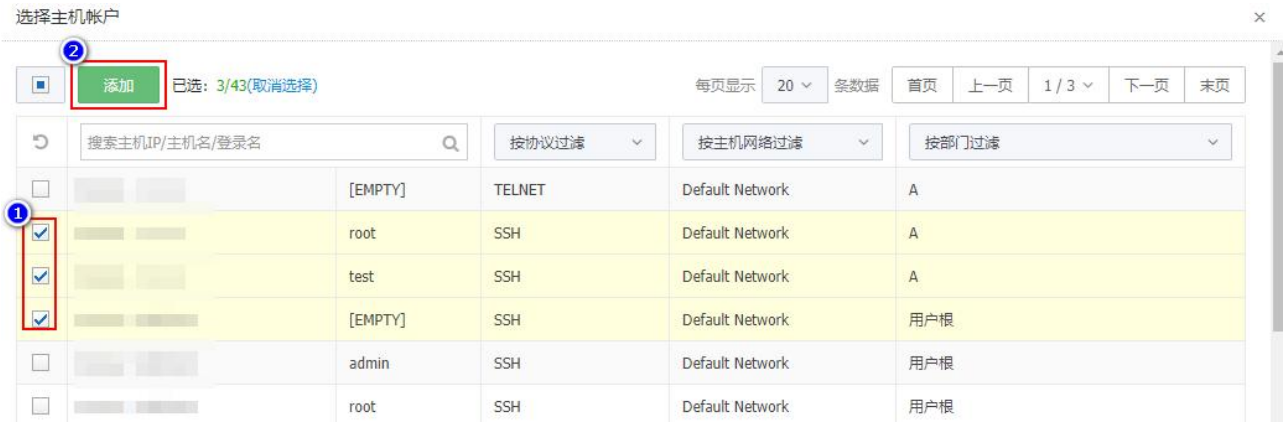
详细配置请参见下表。

配置项	说明
计划类型	支持主机改密、数据库改密、Web 应用改密和主机工单改密。
执行方式	支持手动执行、定时执行和周期执行。
改密方式	支持以下三种方式： ◆ 主动探测：在改密主机类型未知的情况下，通过探测确定主机类型进行改密。 ◆ 自定义：在已知主机类型的情况下，定义脚本命令来进行改密。了解脚本语法请点击<**帮助**>。 ◆ 改密脚本：改密脚本适用于多个计划中的托管帐户全部为同类系统中的帐户时，需要通过脚本改密的情况。改密脚本可在“**系统➤系统配置➤改密脚本**”页面进行设置。

配置项	说明
密码生成方式	支持以下三种方式： ◆ 自动生成：系统自动生成密码，可指定密码复杂度、密码长度等。 ◆ 上传密码：通过上传密码文件（支持.txt 和.csv 格式）指定密码。 ◆ 手工指定：手工指定密码，密码长度 6~32 位。
密码发送方式	支持以下四种方式： ◆ 不发送。 ◆ 邮件：以邮件形式发送至用户的邮箱，多个用户用“；”隔开。 ◆ FTP：发送至 FTP 服务器，可指定发送的文件路径，默认为用户帐户根目录（例如 Windows 系统为 C:\Users****，“****”为具体的用户名）。 ◆ SFTP：发送至 SFTP 服务器，可指定发送的文件路径，默认为用户帐户根目录（例如 Windows 系统为 C:\Users****，“****”为具体的用户名）。

步骤 3. 任务创建成功后将自动跳转到计划信息托管帐户页面，点击<**添加主机帐户**>。

步骤 4. 在弹出的对话框中勾选主机帐户，点击<**添加**>。



10.1.2 修改改密计划

步骤 1. 进入计划列表页面，点击计划名称进入编辑计划基本信息页面，可以修改计划名称、执行方式、密码生成方式和密码发送方式。

步骤 2. 选择**托管帐户**页签，可以进行添加托管主机账户、删除托管主机帐户、手工改密、密码恢复等操作。

10.1.3 管理关联主机账户

堡垒机中托管了同一资产不同协议的同一帐户时，若其中一个协议帐户执行了改密，为使该帐户下的其他协议可以正常运维，需要将改密后的密码同步到该帐户下的所有协议中。操作方法如下：

步骤 1. 在托管帐户页面点击托管帐户后的“**操作➤管理关联主机帐户**”。

步骤 2. 进入**关联主机帐户管理**页面，点击<**添加主机帐户**>。

步骤 3. 在弹出的对话框中勾选主机帐户，点击<**添加**>即可。

10.1.4 管理关联应用帐户

堡垒机中托管了同一资产不同协议的等价帐户（即通过不同的协议访问资产，账户的用户名和密码都相同）时，若资产中一个协议帐户执行了改密，为使该资产下的等价账户可以正常运维，需要将改密后的密码同步到该资产下的等价账户中。

管理关联应用帐户的操作与管理关联主机帐户的操作类似，不再赘述。

10.1.5 一键检测帐户删除状态

对于系统升级前创建的改密计划，在升级后由于实际使用需求变更了资产，如在资产中删除了改密计划中添加过的帐户时，可以通过一键检测帐户删除状态功能检测出改密计划中已经被删除的帐户。操作方法如下：

步骤 1. 在系统菜单栏选择“**任务➤改密计划**”，进入**改密计划**页面，选择**全部托管主机帐户**页签或**全部托管数据库帐户**页签。

步骤 2. 点击<**一键检查帐户删除状态**>，在弹出的对话框中点击<**确定**>。

步骤 3. 检测完成后，资产中已经被删除账户的状态将会变为“已删除”。

10.1.6 查看托管账户信息

在系统菜单栏选择“**任务➤改密计划**”，选择**全部托管主机帐户**页签、**全部托管数据库帐户**页签或**全部托管 Web 应用帐户**页签，查看对应的帐号信息。

相关操作

◆ 停止改密：勾选帐户，点击<**停止改密**>，在弹出的对话框中点击<**确定**>，可停止账号改密。

◆ 手工改密：

步骤 1. 勾选帐户，点击<**手工改密**>。

步骤 2. 在弹出的**手工改密**对话框中设置密码，点击<**确定**>，即可手工修改帐户密码。

10.2 自动运维

堡垒机支持自动运维操作，即由系统代替运维员进行运维操作。自动运维支持普通命令、交互式命令以及特殊键。

创建自动运维的操作方法如下：

步骤 1. 在系统菜单栏选择“**任务➤自动运维**”进入任务列表页面，点击<**新建自动运维任务**>。

步骤 2. 进入**新建自动运维任务**页面，填写任务名称，选择执行方式、运维结果发送方式，添加运维命令，点击<**创建任务**>。

详细配置请参见下表。

配置项	说明
执行方式	包括手动执行、定时执行和周期执行三种。
运维结果发送方式	包括以下四种方式： ◆ 不发送。 ◆ 邮件：以邮件形式发送至用户的邮箱。 ◆ FTP：发送至 FTP 服务器，可指定发送的文件路径，默认为用户帐户根目录（例如 Windows 系统为 C:\Users****，“****”为具体的用户名）。 ◆ SFTP：发送至 SFTP 服务器，可指定发送文件路径，默认为用户帐户根目录（例如 Windows 系统为 C:\Users****，“****”为具体的用户名）。
命令列表	支持命令、交互式命令和特殊键三种方式。关于命令列表的格式说明，请点击

配置项	说明
	<**帮助**>进行查看。

步骤 3. 任务创建成功后将自动跳转到任务帐户页面，点击<**添加主机帐户**>。

步骤 4. 在弹出的对话框中勾选主机帐户，点击<**添加**>。

10.3 资产巡检

资产巡检是指对主机、主机账户、主机状态、主机账户状态进行手动、定期和周期性的扫描检测。支持扫描指定网段中存在的资产，资产中存在的主机帐户等。

10.3.1 创建资产巡检任务

创建资产巡检任务的的操作方法如下：

步骤 1. 在系统菜单栏选择“**任务➤资产巡检**”，进入**资产巡检**页面，点击<**新建巡检任务**>。

步骤 2. 进入**新建资产巡检任务**页面，编辑相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	说明
任务名称	用来标识任务，最大长度为 50 字符。
任务类型	包括主机发现、主机帐户发现、主机状态检查、主机帐户状态检查四种类型。
执行方式	包括手动执行、定时执行和周期执行三种。
目标网段	输入待巡检资产的网段，例如：172.16.1.0/24，仅支持 20 位及以上掩码。

步骤 3. 任务创建成功后将自动跳转到**任务对象**页面（主机发现任务不支持），根据所选任务类型的不同，点击<**添加目标主机**>或<**添加目标主机帐户**>添加任务对象。

步骤 4. 在弹出的对话框中勾选主机或主机账户，点击<**添加**>。

10.3.2 执行资产巡检任务

对于手动执行的资产巡检任务，请参照以下方法执行任务：

步骤 1. 勾选需要执行的资产巡检任务，点击<**开始**>，则开始执行资产巡检任务。

步骤 2. 任务执行完成后，点击**操作**列中的**<导出执行结果>**。

步骤 3. 在弹出的对话框中设置密码，点击<**结果导出**>，将执行结果导出至本地。

设置密码后，解压缩导出的文件时需要输入密码。

11 系统

系统管理用于对系统运行参数进行设置以及对系统进行维护，以适配实际应用场景。包括网络配置、VPN 管理、认证管理、系统配置、存储管理、操作日志、系统报表和本机维护。

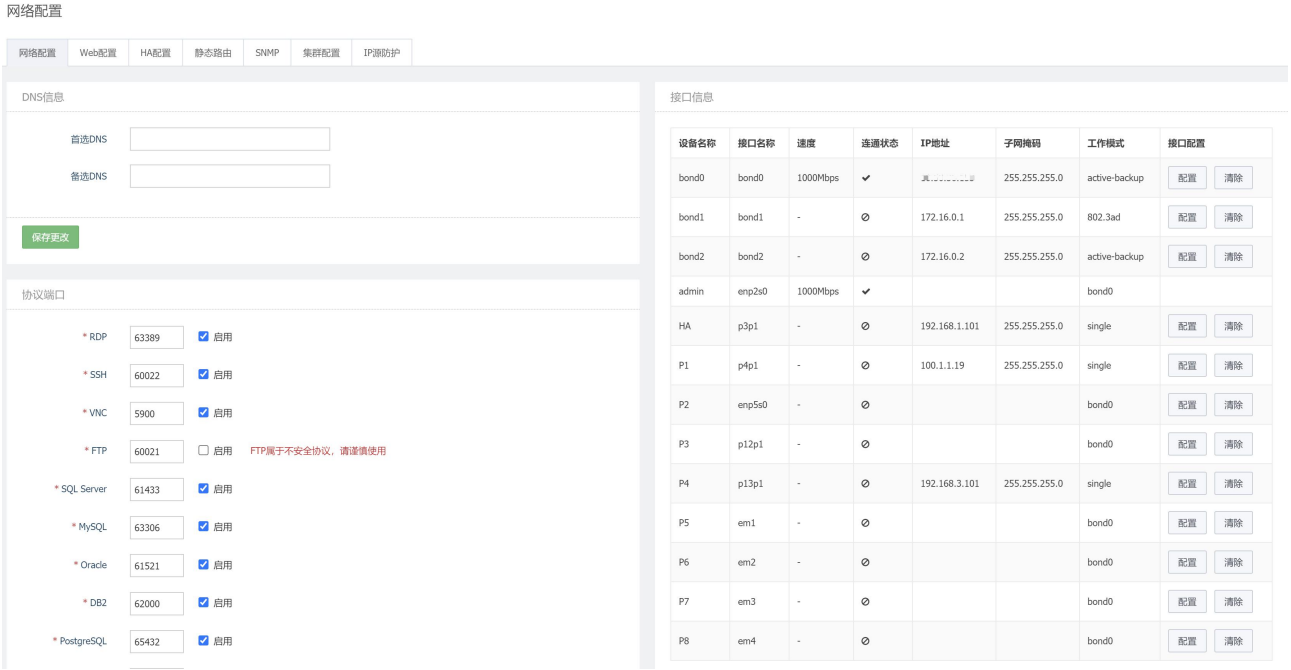
11.1 网络配置

11.1.1 基础信息设置

在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，在网络配置页面可以配置 IPv4/IPv6 接口信息、DNS 信息、协议端口信息、RDP 网关、TLS 安全性。

配置相关信息后，点击<保存更改>即可保存配置成功。

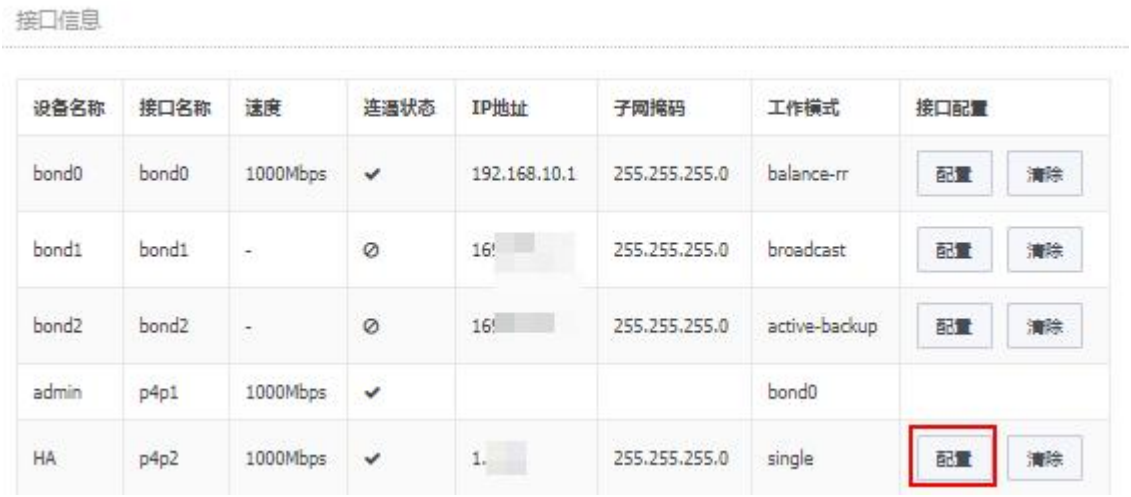
本文以硬件版设备举例说明。



◆ 配置 DNS 信息：设置首选 DNS 和备选 DNS，点击<**保存更改**>。

◆ 配置物理端口的模式

步骤 1. 选择目标物理端口（以 HA 口为例），点击<**配置**>。



步骤 2. 选择模式（single 表示独立模式；nat 表示地址转换模式；bond0/bond1/bond2 表示加入对应聚合端口；VLAN 表示使用当前设置的 VLAN 号进行通信），点击<**保存更改**>。

◆ 配置独立接口的 IP 地址（single 模式或 nat 模式接口）：

步骤 1. 选择目标接口，点击<**配置**>。

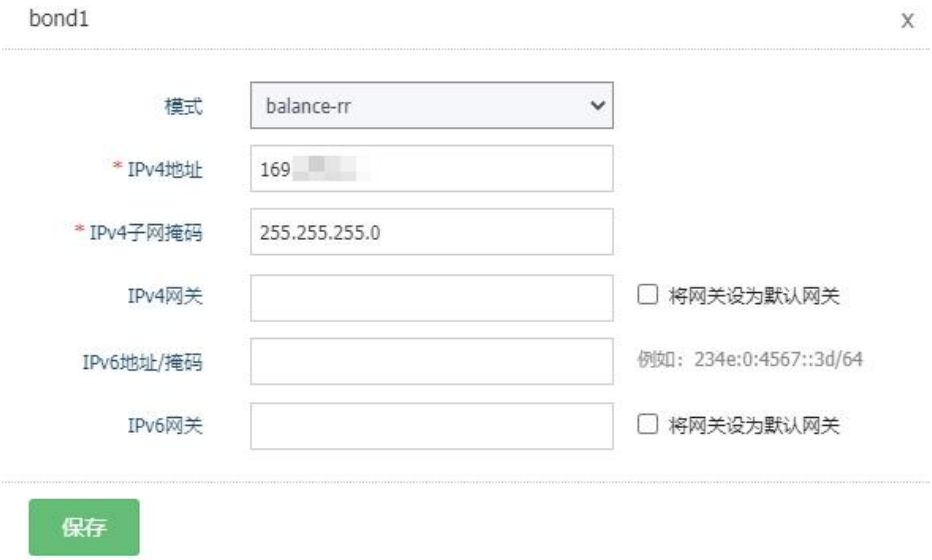
步骤 2. 设置 IPv4 地址及 IPv6 地址信息，点击<**保存**>。

修改接口 IP 地址后需要使用新的地址登录系统。

◆ 配置聚合接口的 IP 地址（以 bond1 为例）

步骤 1. 选择目标接口，点击<**配置**>。

步骤 2. 在弹出的对话框中，设置该聚合端口的 IP 地址、子网掩码及工作模式，点击<**保存更改**>。



详细配置请参见下表。

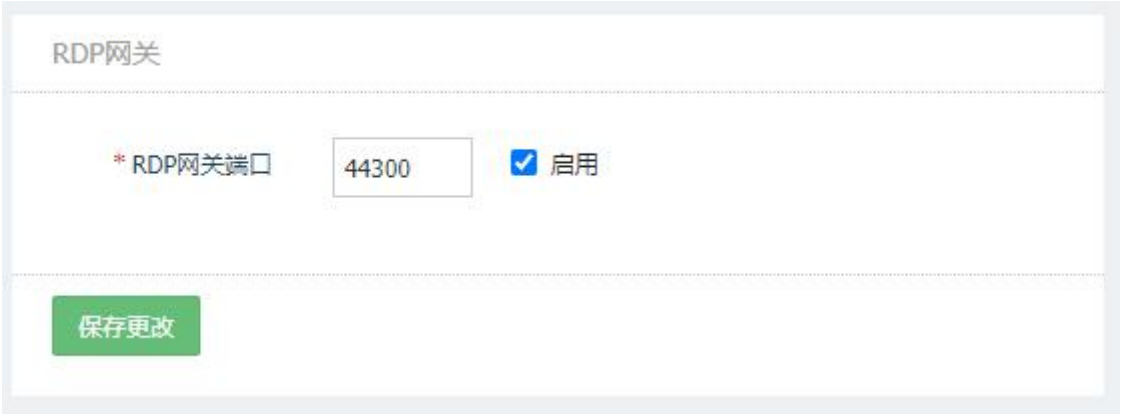
配置项	说明
IPv4 地址	端口的 IPv4 地址。加入聚合端口的所有物理端口均使用该 IPv4 地址。
IPv4 子网掩码	端口 IP 地址对应的子网掩码，例如：255.255.255.0。
IPv4 网关	端口的 IPv4 网关，即端口的下一跳地址。
IPv6 地址/掩码	端口的 IPv6 地址和掩码，例如:234e:0:4567::3d/64。加入聚合端口的所有物理端口均使用该 IPv6 地址。
IPv6 网关	端口的 IPv6 网关，即端口的下一跳地址。
MTU	最大传输单元，合法值 64-65536
模式	设置端口的工作模式： ◆ balance-rr：平衡循环模式。例如：聚合端口包含 2 个物理端口 GE1 和 GE2，则第一个数据包从 GE1 端口转发，第二个数据包从 GE2 端口转发，第三个数据包从 GE1 端口转发，第四个数据包从 GE2 端口转发……以此循环，直至数据包转发完成。 ◆ active-backup：主-备份策略。聚合端口由主端口发送数据，当主端口发生故障时由其他备端口发送数据。

	◆ balance-xor：基于指定 HASH 策略传输数据包。此模式提供负载均衡和容错能力。 ◆ broadcast：广播策略，在聚合端口组中的所有备端口中发送所有数据包。 ◆ 802.3ad：动态链路聚合模式。需要对端交换机支持 IEEE 802.3ad 协议。 ◆ balance-tlb：适配器传输负载均衡模式。在聚合端口组中所有备端口转发数据，根据当前负载（根据端口速率计算）分配转发流量。 ◆ balance-alb：适配器适应性负载均衡模式。

◆ 设置端口信息：勾选**启用**，并设置端口号，点击<**保存更改**>。则启用对应协议，并设置该协议使用的端口号。

RDP、VNC、SSH、FTP 协议在关闭协议端口后，RDP、VNC、SSH、RLOGIN、TELNET、FTP、SFTP、X11 协议无法进行 BS/CS 运维，不影响 RDP、VNC、SSH、RLOGIN、TELNET、FTP、SFTP、X11 协议的 H5 运维。

- 启用 RDP 网关端口（当 RDP 协议为 8.0 及上版本时，需要使用 RDP 网关），并设置端口（默认端口为 44300），点击<**保存更改**>。



◆ TLS 安全性配置：勾选**启用**，点击<**保存更改**>。可提高 FTPS、RDG 和 RDP 协议的安全性。

11.1.2 Web 配置

Web 配置是指对用户登录系统 Web 管理平台进行设置，包括登录时使用的端口、Web 证书配置等，以提高用户访问系统 Web 管理平台的安全性。

在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，选择 **Web 配置**页签。在 Web 配置页面可以配置国密通信、Web 设置、Web 证书配置、自定义 Web 证书，每一项配置完成后需要点击<**保存更改**>方可生效。

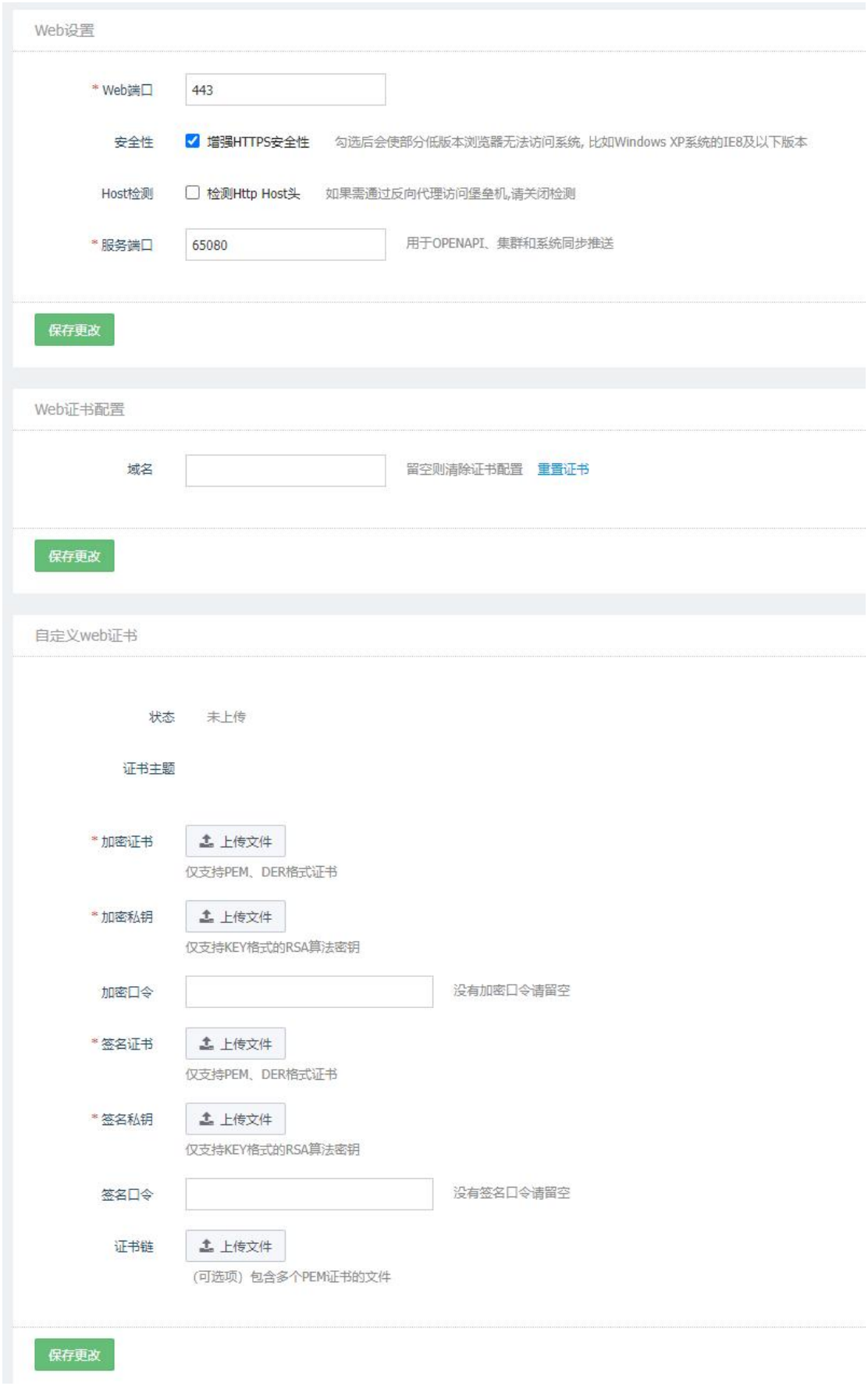
国密通信

开启国密通信后，需使用国密浏览器登录堡垒机进行运维操作。

详细配置请参见下表。

配置项	说明
状态	关闭：为普通的 RSA 通信。 开启：为单向国密通信。
国密双向通信	双向通信需在开启单向国密通信后，并且配置国密管理员 USBKEY 后才能开启，国密 USB 配置方法请参见 USBKEY 管理。

其他配置


Web设置
* Web端口
443
安全性
增强HTTPS安全性
勾选后会使部分低版本浏览器无法访问系统，比如Windows XP系统的IE8及以下版本
Host检测
检测Http Host头
如果需通过反向代理访问堡垒机,请关闭检测
* 服务端口
65080
用于OPENAPI、集群和系统同步推送
保存更改
Web证书配置
域名
留空则清除证书配置
重置证书
保存更改
自定义web证书
状态
未上传
证书主题
* 加密证书
上传文件
仅支持PEM、DER格式证书
* 加密私钥
上传文件
仅支持KEY格式的RSA算法密钥
加密口令
没有加密口令请留空
* 签名证书
上传文件
仅支持PEM、DER格式证书
* 签名私钥
上传文件
仅支持KEY格式的RSA算法密钥
签名口令
没有签名口令请留空
证书链
上传文件
(可选项) 包含多个PEM证书的文件
保存更改

详细配置请参见下表。

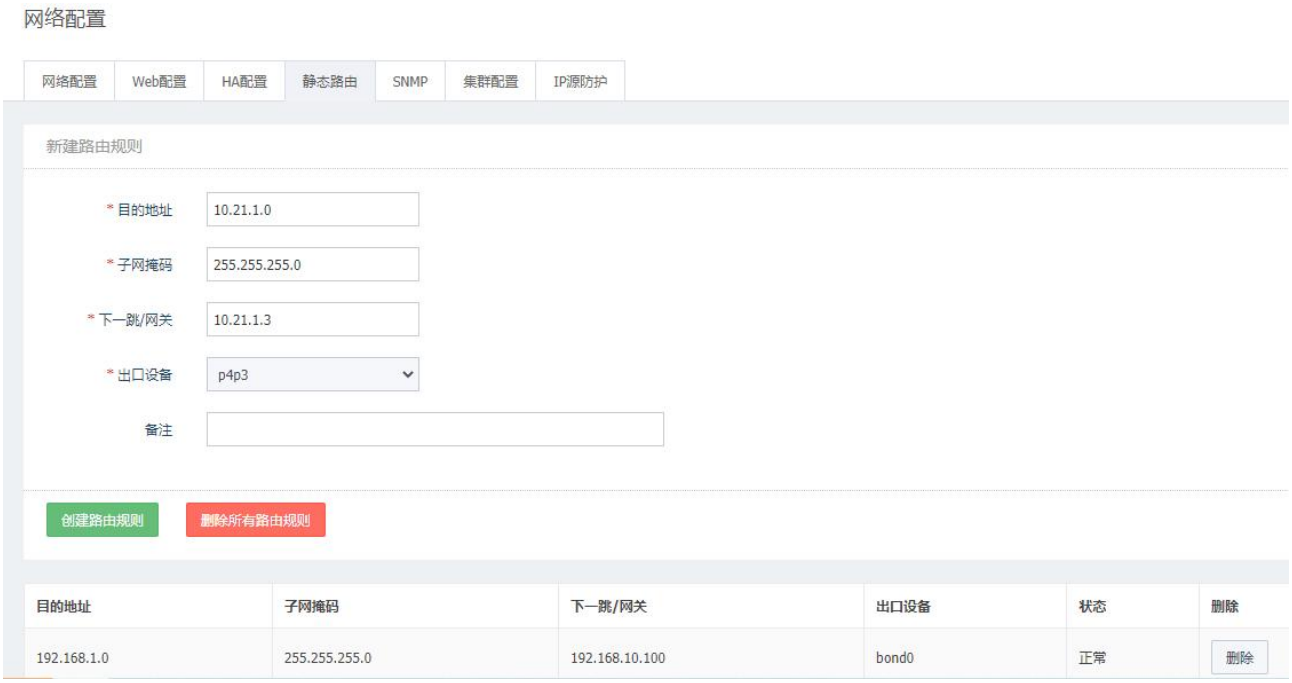
配置项	说明
Web 端口	访问堡垒机系统 Web 管理平台所使用的端口号。
安全性	如勾选<**增强 HTTPS 安全性**>，部分低版本浏览器将无法访问系统，如 Windows XP 系统的 IE8 及以下版本。
Host 检测	如需通过反向代理访问堡垒机，请关闭 Host 检测。
服务端口	用于 OpenAPI、集群和系统同步推送的端口号。
系统 IP	证书服务器的 IP，留空则清除证书配置。当 CA 证书的地址与实际地址不一致时，点击<**重置证书**>，可重置证书。
证书	仅支持 PEM、DER 格式证书。
私钥	仅支持 RSA 算法密钥。

11.1.3 静态路由

当堡垒机存在多个路由出口时，需配置静态路由，以方便运维员通过堡垒机登录不同路由出口的目标主机。

当堡垒机仅有一个路由出口时，不能创建静态路由规则。

在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，选择**静态路由**页签。选择出口设备，输入目的地址、子网掩码、下一跳网关，点击<**创建路由规则**>完成路由规则创建。点击规则后的<**删除**>即可删除相应的路由规则。



11.1.4 SNMP 配置

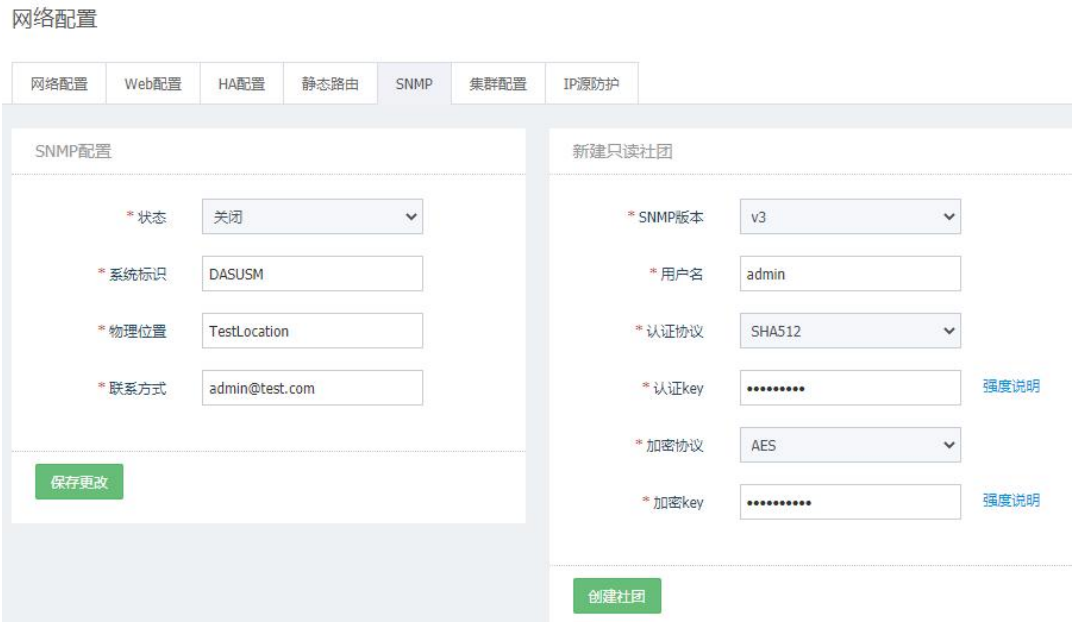
支持通过 SNMP 协议对堡垒机进行远程监控。SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支持目前主流的网络管理系统，用于监测网络上的设备

是否有存在异常情况。

步骤 1. 在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，选择 **SNMP** 页签。

步骤 2. 选择状态为**开启**，设置系统标识、物理位置和联系方式，点击<**保存更改**>进行 SNMP 全局设置。

步骤 3. 编辑相关信息，点击<**创建社团**>创建只读社团。此处设置应与 SNMP 网管平台设置保持一致。



详细配置请参见下表。

配置项	说明
SNMP 版本	设置 SNMP 版本，支持 v1、v2c、v3。建议使用 v3 版本，安全性更高。
用户名	SNMP 社团用户名，最大长度为 32 个字符，可以包含大写字母、小写字母和数字，不允许包含空格。
认证协议	支持 MD5、SHA、SHA256 和 SHA521。
认证 key	认证密码，必须包含大写字母、小写字母、数字和特殊字符，长度为 10~20 字符。
加密协议	支持 AES、AES192、AES256 和 DES。
加密 key	必须包含大写字母、小写字母、数字和特殊字符，长度为 10~20 字符。

11.1.5 集群配置

堡垒机支持集群模式部署，多台设备组成集群提供更高业务处理性能及可靠性。

在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，选择**集群配置**页签。集群功能需要配合 HA 功能使用，集群主节点为 HA 主机，其他的堡垒机设置为集群从节点。

设置主、从节点的操作方法如下：

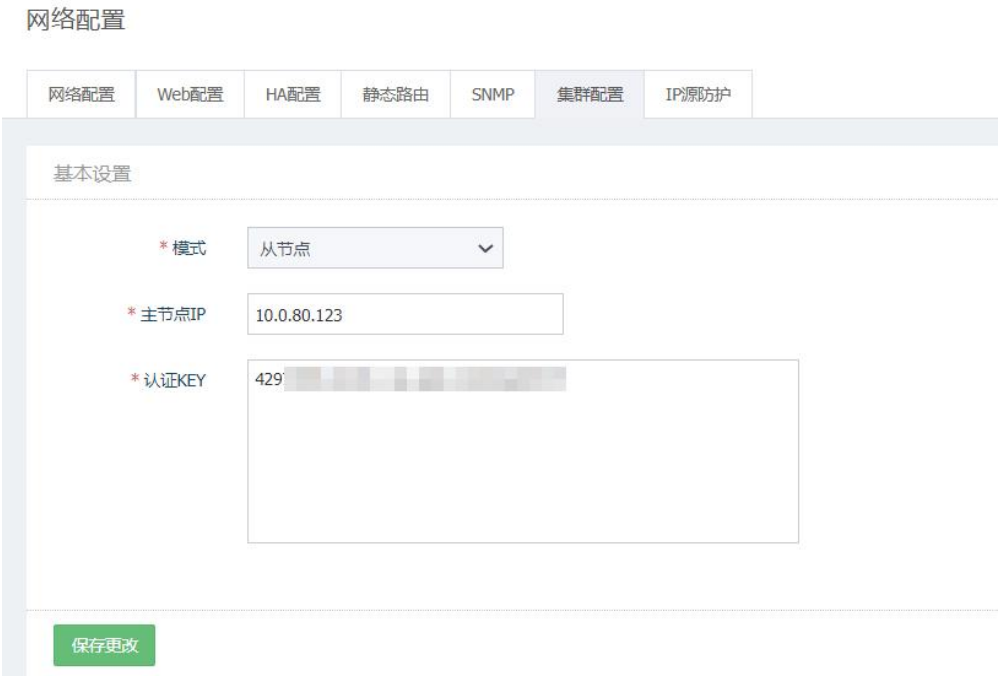
步骤 1. 在 **HA 配置**中设置当前运行模式为“**热备模式-HA 主机**”，点击<**保存更改**>。HA 配置成功，服务重启完成后，进入集群配置页面，查看设备当前模式为主节点。

步骤 2. 点击<**新建集群节点**>。

步骤 3. 在弹出的对话框中填写从节点名称和 IP，点击<**新建集群节点**>。

步骤 4. 将生成的认证 KEY 复制备份，方便后续在从节点中进行设置。

步骤 5. 在从节点的集群配置页面，选择模式为“**从节点**”，填写主节点 IP（此处需填写 HA 的服务/虚拟 IP，可在 HA 配置页面查看）和新建集群节点时生成的认证 KEY，点击<**保存更改**>。



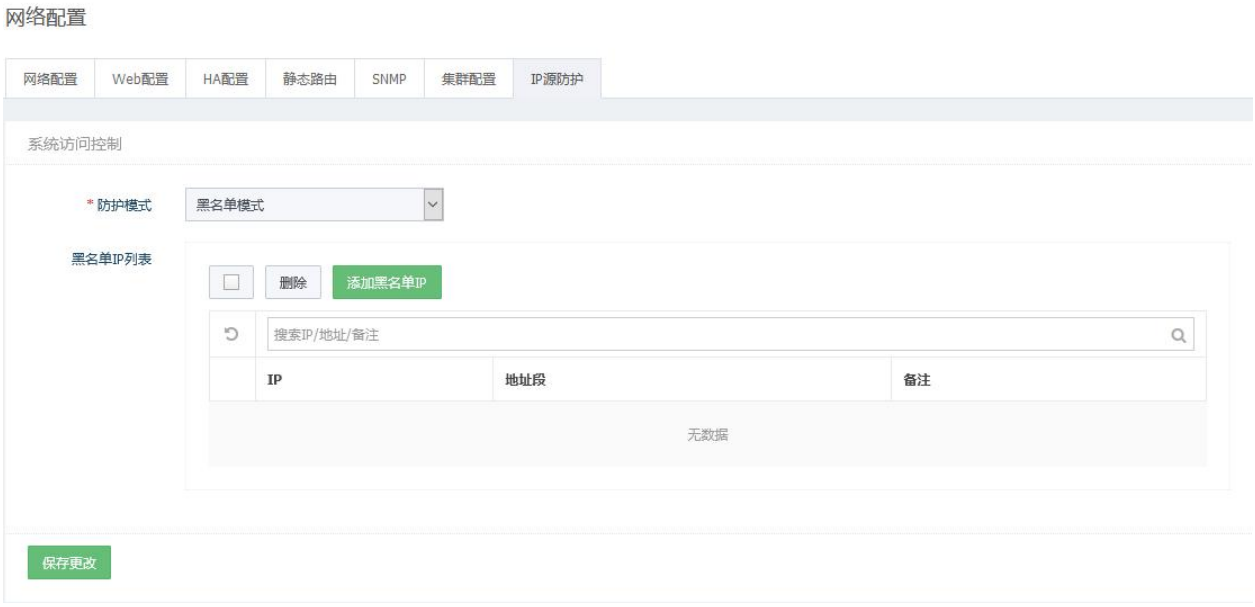
11.1.6 IP 源防护

可设置黑名单模式或白名单模式对源 IP 进行防护，当设置为黑名单模式时，黑名单 IP 列表中的 IP 无法访问系统；当设置为白名单模式时，仅允许白名单列表中的 IP 访问系统。操作方法如下：

步骤 1. 在系统菜单栏选择“**系统➤网络配置**”，进入**网络配置**页面，选择 **IP 源防护**页签。

步骤 2. 选择防护模式为黑名单模式/白名单模式，点击<**添加黑名单 IP**>或<**添加白名单 IP**>。

步骤 3. 填写黑名单 IP/白名单 IP 后，点击<**添加到 IP 列表**>，然后点击<**保存更改**>。

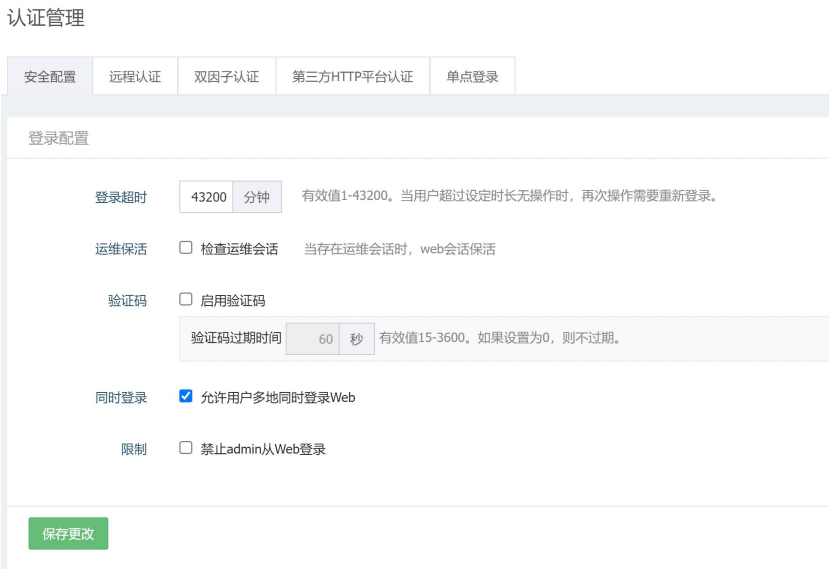


11.2 认证管理

11.2.1 安全配置

在堡垒机的安全配置页面可以配置系统的登录安全性、用户名策略、用户密码策略等。操作方法如下：

步骤 1. 在系统菜单栏选择“**系统➤认证管理**”，进入**认证管理**页面，选择**安全配置**页签。在**登录配置**项中编辑登录超时时间，选择是否运维保活，是否启用验证码，是否允许用户多地同时登录，是否禁止 admin 从 Web 登录，点击<**保存更改**>。



步骤 2. 在**用户锁定**项中，设置密码尝试次数、锁定时长和重置计数器，点击<**保存更改**>。

配置项说明请参见下表。

配置项	说明
密码尝试次数	允许用户尝试密码的次数，如果输入密码错误的次数达到设置值后，用户帐号将被锁定，在锁定时长内不能登录系统。取值范围 0~999，设置为 0 表示不限制用户尝试密码的次数。
锁定时长	用户帐号被锁定的时长，达到锁定时长后，用户可重新登录系统。取值范围 0~10,080，设置为 0 表示帐户被锁定后需要管理员手动进行解锁。
重置计数器	重置尝试密码次数的时间间隔。取值范围 1~10,080。设置为 5 分钟，表示：当输入密码错误的次数小于密码尝试次数时，间隔 5 分钟后再尝试输入密码，此时用户尝试密码的次数重新从 1 开始。

步骤 3. 在**长期未登录用户锁定配置**项，设置状态为“开启”时，设置执行周期和锁定条件，点击<**保存更改**>。当用户未登录时间超过设置的锁定条件时，系统会将该用户自动锁定。锁定后的用户将无法登录系统，直到管理员将其解锁。

步骤 4. 在**用户名策略配置**项，编辑用户名字符黑名单（创建的用户名不能包含用户名字符黑名单，例如当设置用户名黑名单为 dd 时，则用户名不能设置为*dd*，“*”表示任意字符串），点击<**保存更改**>。

步骤 5. 设置用户密码配置策略，点击<**保存更改**>。

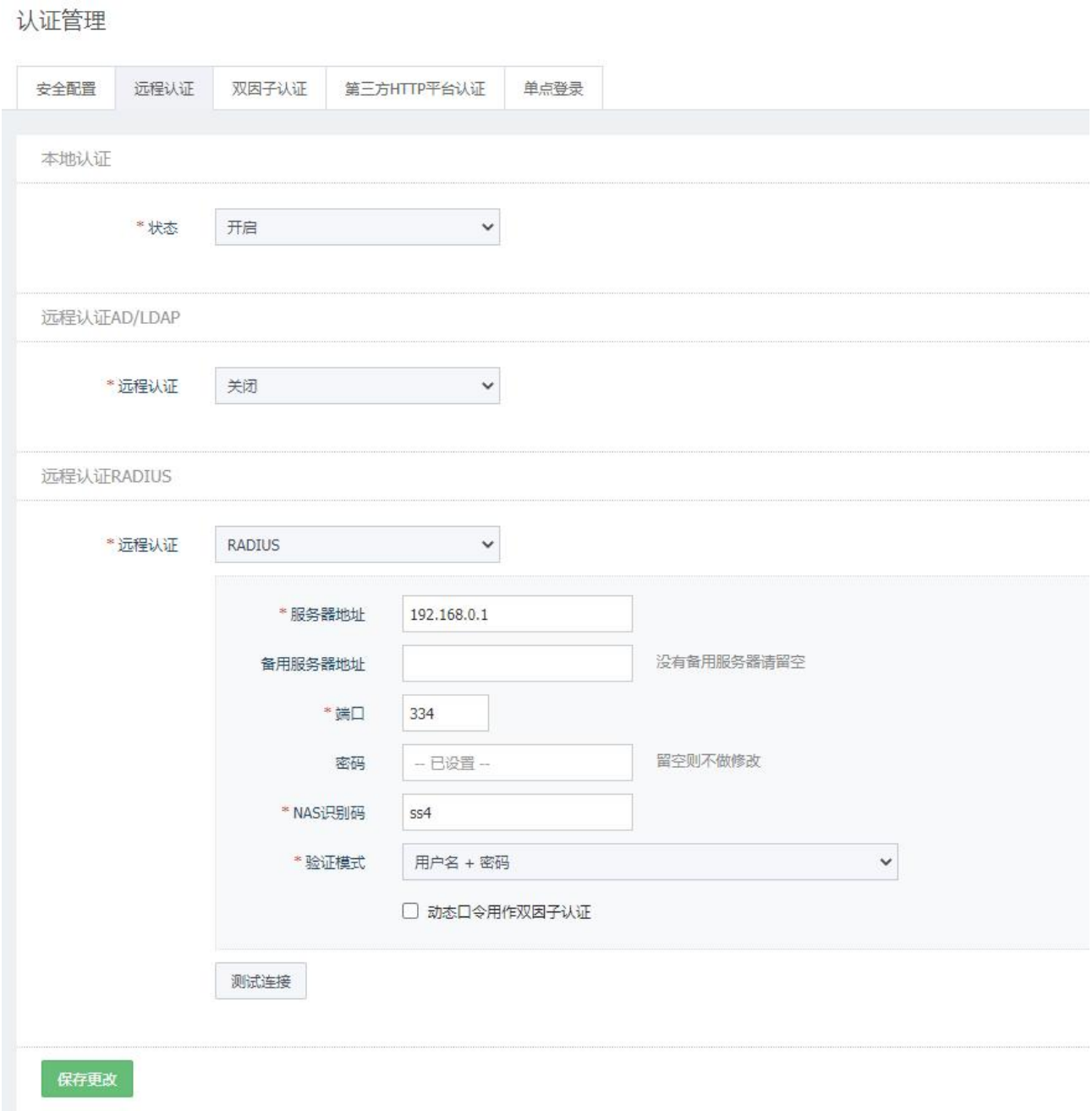
部分配置项说明请参见下表。

配置项	说明
长度	密码长度，取值范围 10~64 字符。
历史密码	改密时检查的历史密码个数，取值范围 0~5；为 0 时，则不检查历史密码。
密码使用期限	取值范围 0~999 天，设置为 0 表示密码不过期。
密码过期前警告时间	设置密码过期前多少天，系统提醒用户修改密码。设置为 0，表示不提醒。

11.2.2 远程认证

远程认证是指当用户登录系统时，调用远程服务器对用户帐户信息进行认证，认证通过后方可登录系统。远程认证的配置方法如下：

在系统菜单栏选择“**系统➤认证管理**”，进入**认证管理**页面，选择**远程认证**页签。在本地认证项中设置是否开启本地认证。在远程认证项中设置远程认证模式，填写远程认证服务器信息，填写完成后点击<**保存更改**>。



详细配置请参见下表。

配置项	说明
远程认证	设置远程认证的类型，包括 LDAP、AD 和 RADIUS 三种。关闭表示不启用远程认证。

配置项	说明
	◆ LDAP 是轻量目录访问协议（Lightweight Directory Access Protocol）的缩写，是互联网上目录服务的通用访问协议。LDAP 服务可以有效解决众多网络服务的用户帐户问题，LDAP 服务器是用于查询和更新 LDAP 目录的服务器，包括用户帐号目录。 ◆ AD 是活动目录（Active Directory）的缩写，用于在 Windows 服务器集中管理所有 Windows 帐户、登录密码及权限。AD 服务器可实现集中的安全管理和统一的安全策略。 ◆ RADIUS 是远程认证拨号用户服务（Remote Authentication Dial In User Service）的缩写，广泛应用于小区宽带上网、IP 电话、移动电话预付费、无线网络接入等业务。RADIUS 服务器负责接收用户的连接请求、认证用户，然后向请求方返回所有必要的配置信息。
RADIUS	
服务器地址	远程认证服务器的 IP。
端口	远程认证服务器的端口。
密码	远程认证服务器的密码。
NAS 识别码	网络访问服务器识别码，认证服务器配置文件中 nastype 字段内容。如果认证服务器配置文件无 nastype 字段内容，则填写堡垒机的管理 IP。
验证模式	进行远程认证时的模式，包括：用户名+密码、用户名+动态口令、用户名+动态口令+令牌 PIN 三种。
AD	
服务器地址	AD 域控服务器的地址，可为 IP 地址或域名。
端口	AD 域控服务器的端口。
Base DN	AD 域控服务器的根节点，即 AD 服务器收到认证请求时目录查询的起始点。
域	AD 域控服务器的域名称。
帐号	AD 域控服务器的帐户。
密码	AD 域控服务器帐户对应的密码。
过滤器	过滤条件，符合过滤条件的用户将被同步至堡垒机。
LDAP	
服务器地址	LDAP 域控服务器的地址，可为 IP 地址或者域名。
端口	LDAP 域控服务器的端口。
Base DN	LDAP 域控服务器的根节点，即 LDAP 服务器收到认证请求时目录查询的起始点。
帐号	LDAP 域控服务器的帐号。
密码	LDAP 域控服务器帐号对应的密码。
过滤器	过滤条件，符合过滤条件的用户将会被同步至堡垒机。
登录名属性	LDAP 用户登录名的属性，例如 uid、sn 等。

当认证模式选择 LDAP 或者 AD 时，保存更改后，点击<**立即同步用户**>会将配置信息立即同步至用户。如果选择了<**自动同步用户**>，则系统将在 5 小时内将配置信息同步至用户。

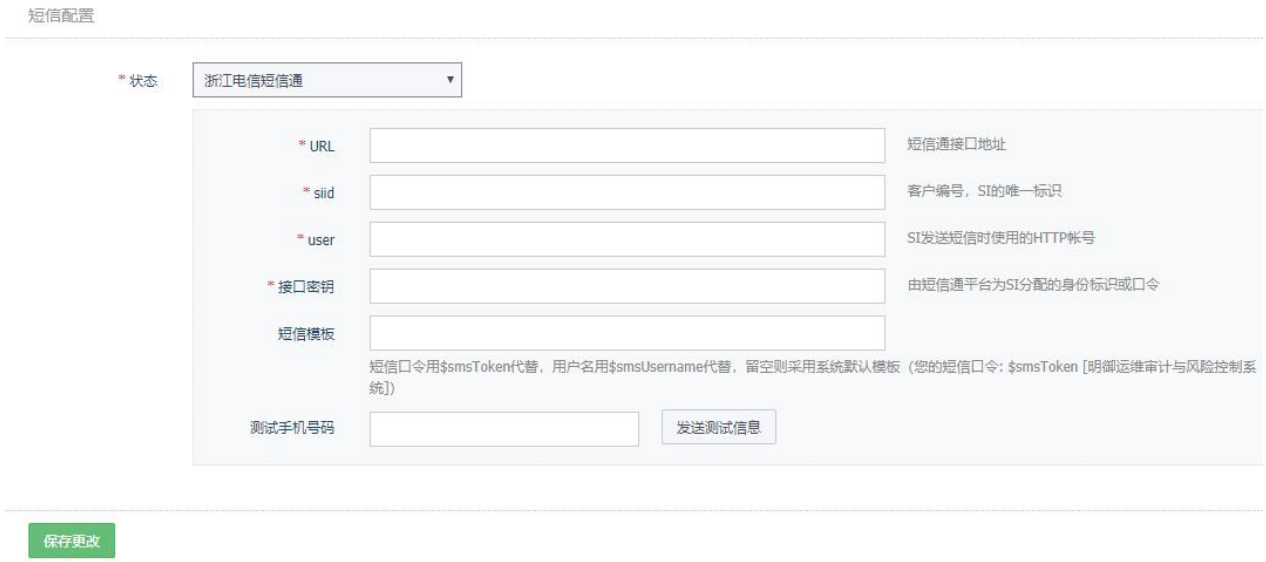
11.2.3 双因子认证

双因子认证是指用户登录堡垒机时，除了需要密码认证成功之外还需要其他一种认证方式（如短信口令）认证成功后才可成功登录堡垒机。

步骤 1. 在系统菜单栏选择“**系统➤认证管理**”，进入**认证管理**页面，选择**双因子认证**页签。勾选需要启用的认证方式，点击<**保存更改**>。

- 勾选**密码和短信口令**后，需进行短信配置。
- 勾选**密码和第三方 USBKEY** 后，需进行第三方 USBKEY 通用配置。

步骤 2. 设置短信配置，选择状态，编辑相关信息（具体配置参数请咨询选中的短信服务提供商），点击<**保存更改**>。



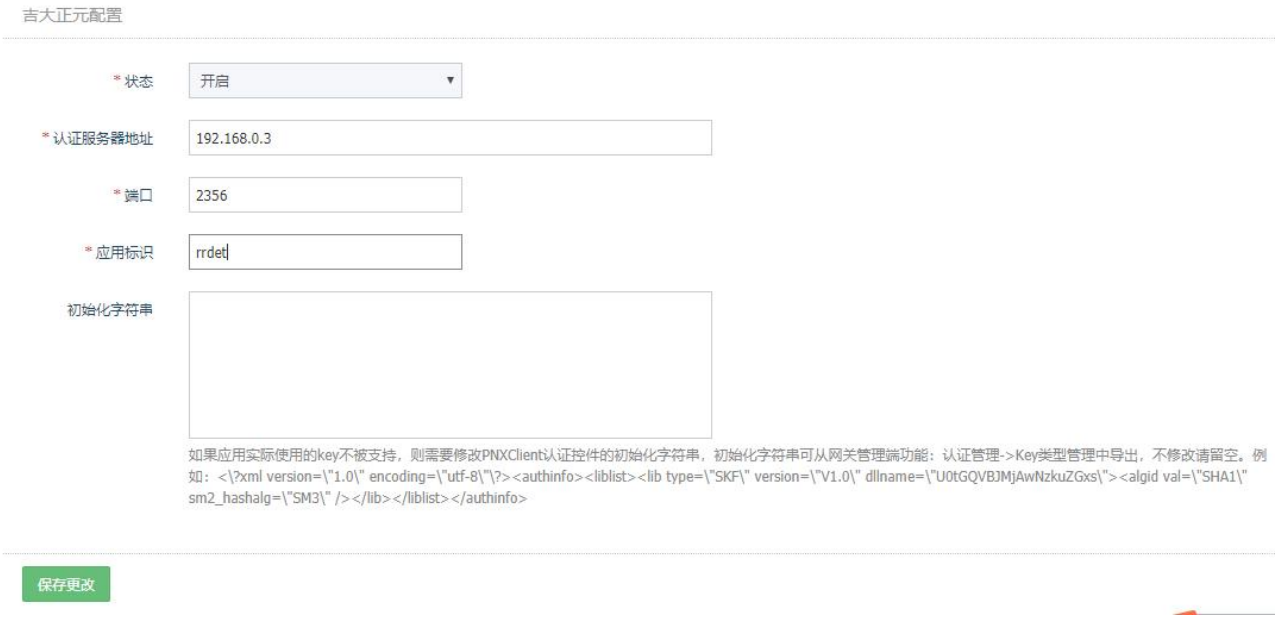
步骤 3. 配置第三方 USBKEY 通用配置。

以下六种认证方式只能开启其中的一种认证方式：

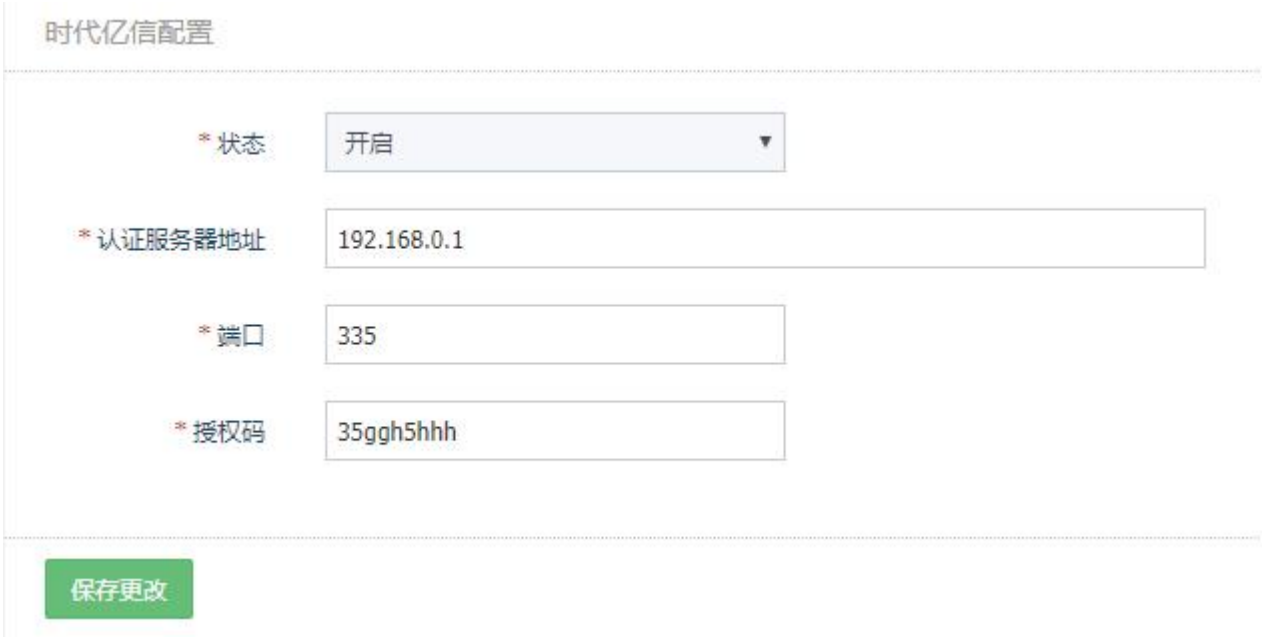
- 北京数字认证股份有限公司的认证
- 吉大正元认证
- 时代亿信认证
- 深圳 CA
- 网联清算
- 中石化认证

- 配置北京数字认证股份有限公司的认证，具体参数请咨询厂家。配置完成后，需要点击<**保存更改**>。

◆ 设置吉大正元配置，具体参数请咨询厂家，配置完成后需要点击<保存更改>。

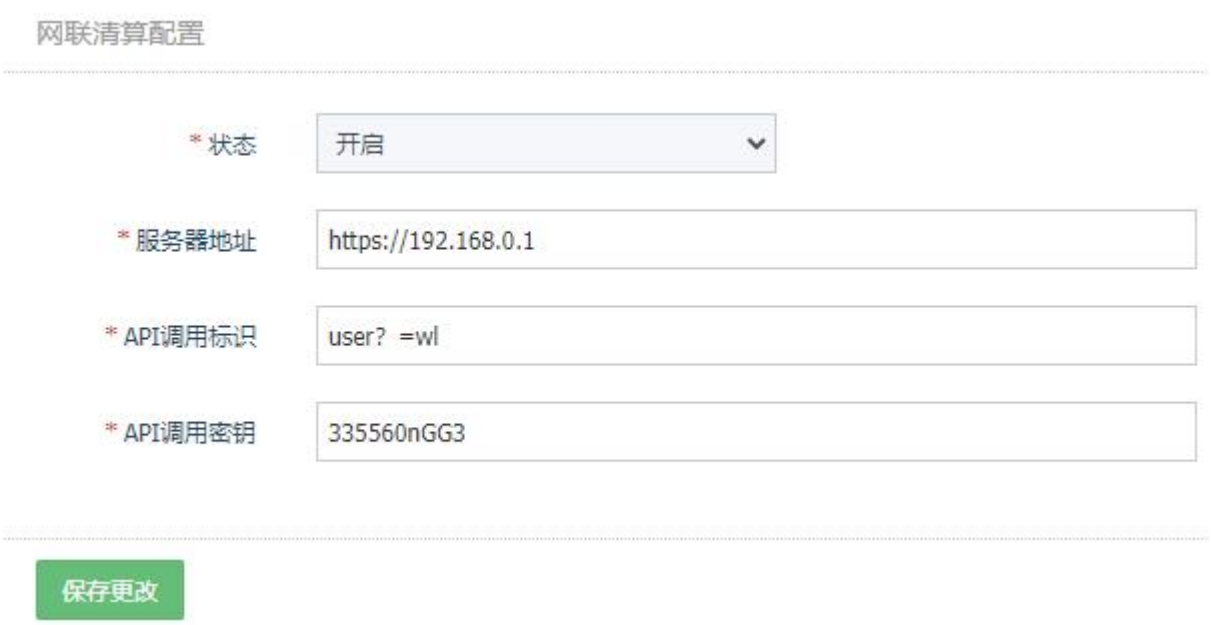


◆ 设置时代亿信配置，具体参数请咨询厂家，设置参数后，点击<保存更改>。



◆ 设置深圳 CA 配置，具体参数请咨询厂家，设置参数后，点击<保存更改>。

◆ 设置网联清算配置，具体参数请咨询厂家，设置参数后，点击<**保存更改**>。



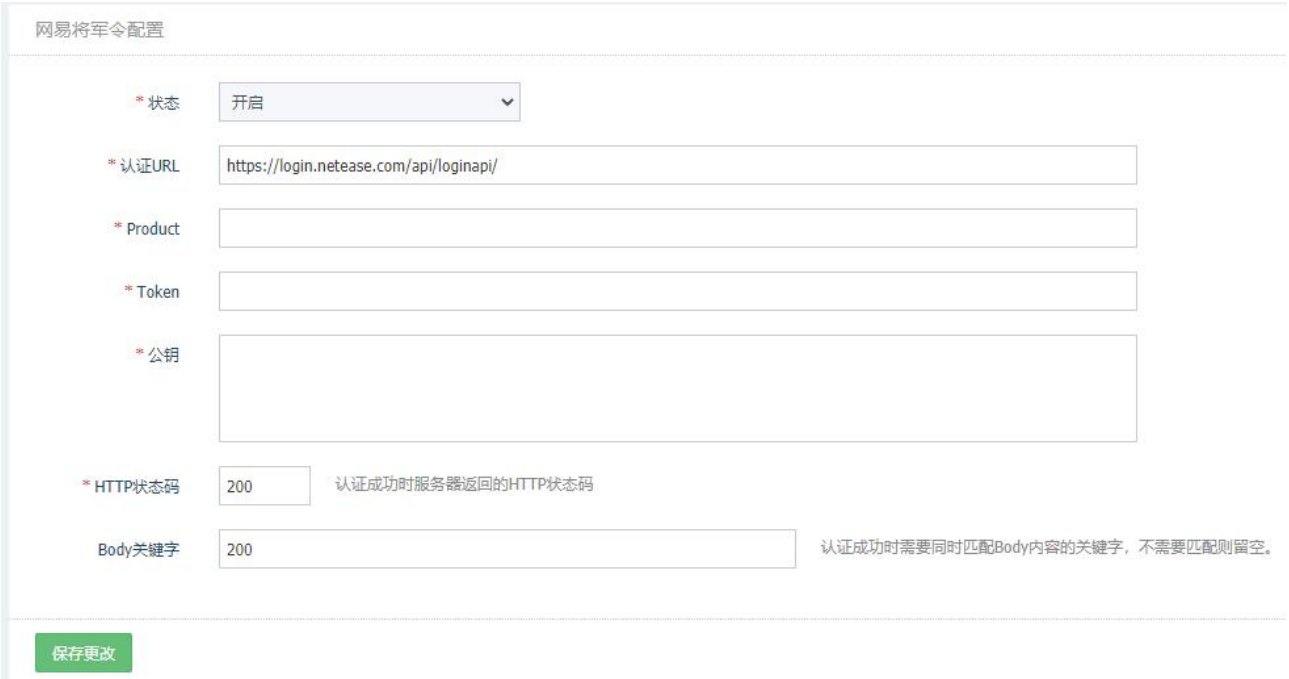
◆ 设置中石化配置，具体参数请咨询厂家，设置参数后，点击<**保存更改**>。

11.2.4 第三方 HTTP 平台认证

第三方 HTTP 平台认证是指通过网易将军令或其他第三方平台认证登录堡垒机。

在系统菜单栏选择“系统➤认证管理”，进入认证管理页面，选择第三方 HTTP 平台认证页签。可配置以下第三方平台认证：

◆ 网易将军令配置。在网易将军令配置中设置状态为开启，配置相关信息，点击<**保存更改**>。



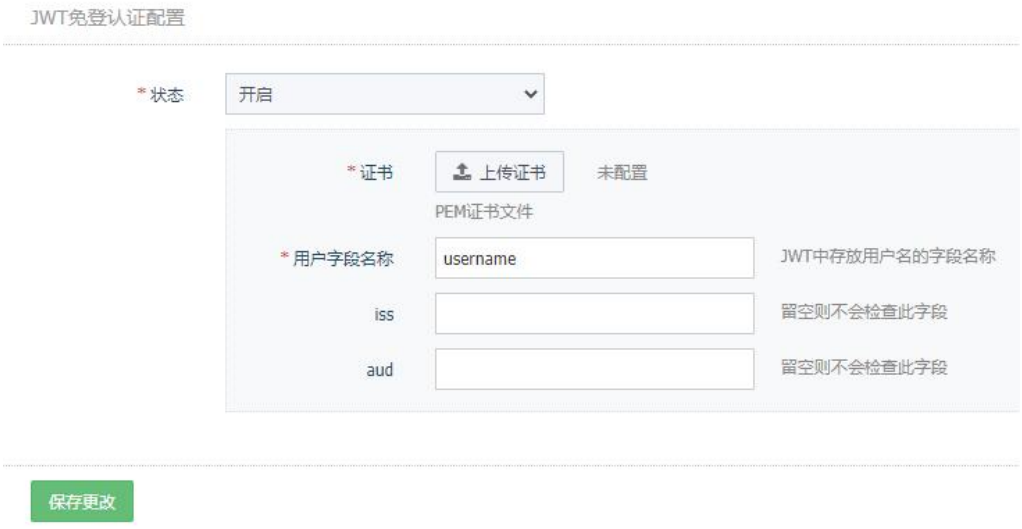
详细配置请参见下表。

配置项	说明
认证 URL	认证 URL 中包含了认证所需的用户名、密码等关键字。需要以实际情况为准。
Product	网易将军令用于验证的 header 信息中的 product 关键字。

Token	网易将军令用于验证的 header 信息中的 token 关键字。
公钥	网易将军令用于验证的 header 信息中的密钥。
HTTP 状态码	认证成功时，服务器所返回的状态码。
Body 关键字	如果认证成功时需要同时匹配 Body 内容的关键字，则填写此项，否则留空。

- 第三方平台单点登录认证配置。在第三方平台单点登录认证中设置状态为“开启”，填写认证URL，点击<**保存更改**>。

- JWT 免登认证配置。在 JWT 免登认证配置中设置状态为“开启”，点击<**上传证书**>上传 PEM 证书文件，填写用户字段名称等信息，点击<**保存更改**>。



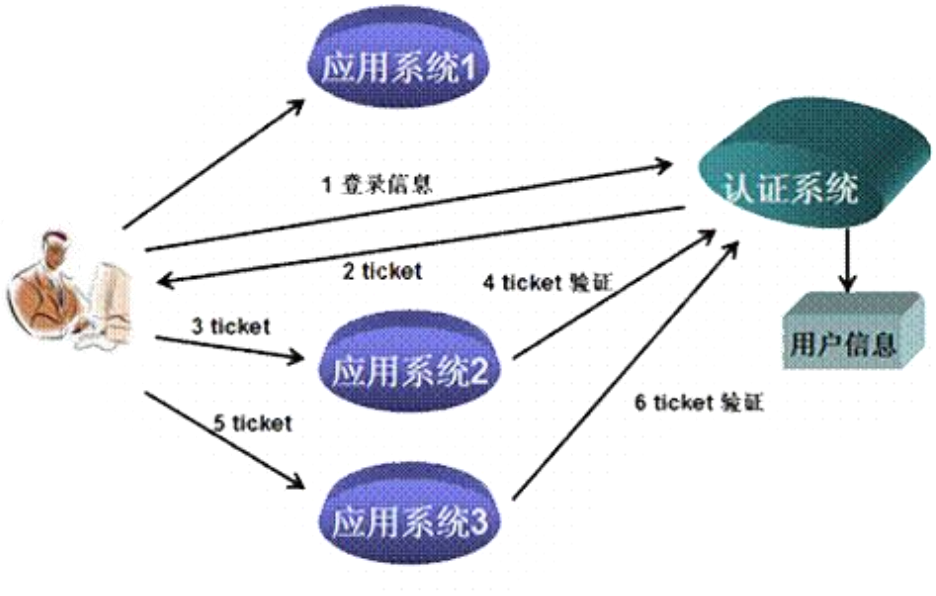
- 江苏意源配置。在**江苏意源配置**中设置状态为“开启”，填写认证服务器地址、服务器认证端口、客户端认证端口、应用标识，点击<**保存更改**>。

- 吉大正元统一身份认证配置。在**吉大正元统一身份认证**中设置状态为“开启”，填写加密密钥、应用标识和认证服务地址，点击<**保存更改**>。

以上第三方 HTTP 平台认证参数，请咨询对应的服务提供商。

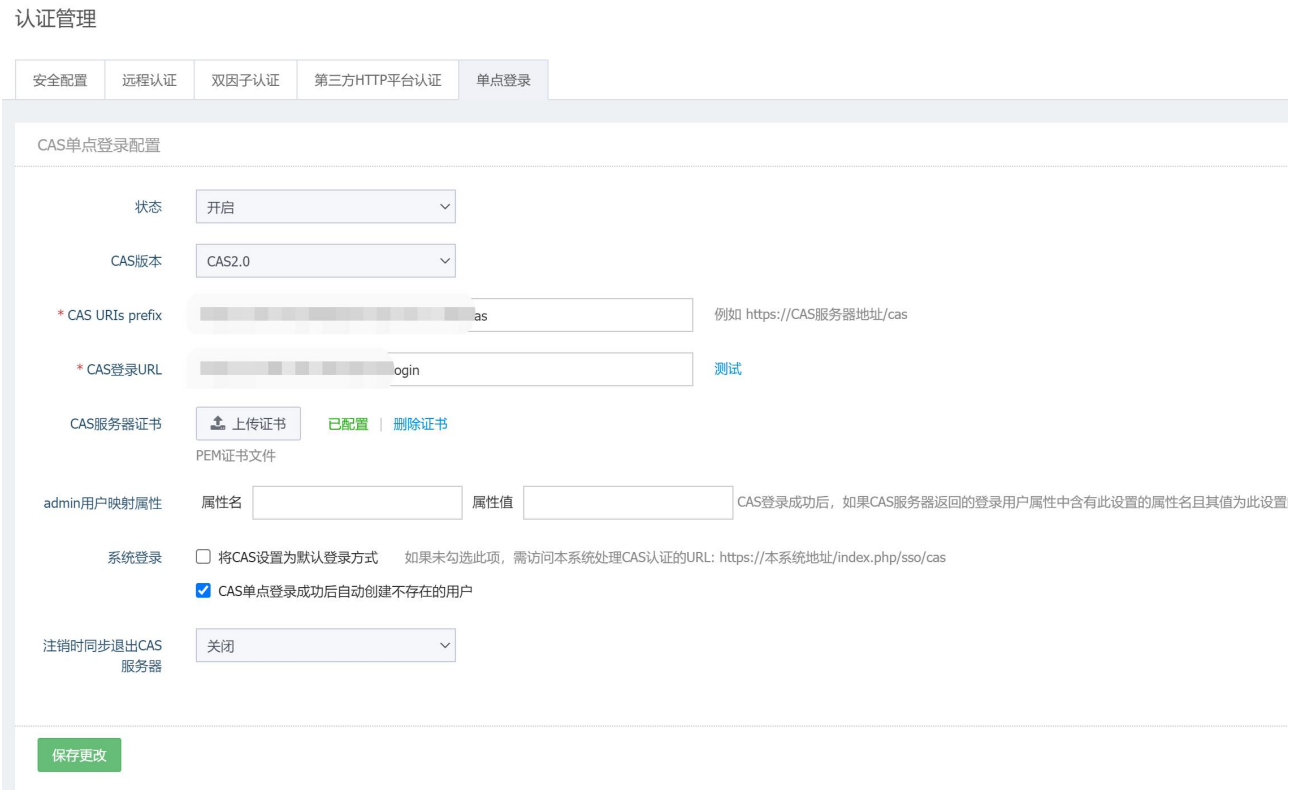
11.2.5 单点登录

单点登录是指用户只需经过一次认证（使用帐号及密码登录某一个应用），就可以免登录直接访问其他相互信任的应用。单点登录功能能够有效地提高用户的工作效率，用户无需记忆多个应用的帐户、密码信息，而只需要记住单个应用的帐号、密码即可。堡垒机支持 CAS 和 SAML2 两种单点登录协议。



在系统菜单栏中选择“**系统➤认证管理**”，进入**认证管理**页面，选择**单点登录**页签。根据单点登录所采用的协议情况进行配置：

- CAS 单点登录配置。在 CAS 单点登录配置中设置状态为“开启”，设置 CAS 版本，填写 CAS URIs prefix、CAS 登录 URL，上传 CAS 服务器证书，点击<**保存更改**>。



- SAML2 单点登录配置。在 CAS 单点登录配置中设置状态为“开启”，设置 IDP Login URL 等参数，点击<**保存更改**>。

详细配置请参见下表。

配置项	说明
IDP Login URL	SAML 认证服务器的 URL 地址。
SP ACS URL	服务提供者的目标地址，默认已内置好，无需修改。
SAML2 服务器证书	SAML2.0 认证的服务器证书，仅支持 PEM 证书文件。
IDP Enty ID	SAML 服务器的实例 ID
SP Enty ID	堡垒机的实例 ID，默认为 USM，无需修改。
用户名属性映射	用户登录名的属性。例如：name。
admin 用户映射属性	用户通过 SAML2 登录成功后，如果 SAML2 服务器返回的登录用户属性中含有此设置的属性名且其值为此设置的属性值，则会将该用户映射成堡垒机的 admin 用户。
将 SAML2 设置为默认登录方式	将 SAML2 设置为默认登录方式后，访堡垒机的 Web 管理平台会自动跳转到 SAML2 登录页面进行认证。
SAML2 单点登录成功后自动创建不存在的用户	通过 SAML2 登录页面认证成功的用户，若堡垒机本身不存在这个用户，则会在堡垒机上自动创建此用户。

11.3 系统配置

11.3.1 运维配置

11.3.1.1 未授权登录配置

运维授权配置主要是对未授权登录进行相关配置，支持 Web 未授权登录及 API 未授权登录。

在系统菜单栏选择“**系统➤系统配置**”，进入**系统配置**页面（默认展示**运维配置**页签），在**未授权登录**项中配置未授权登录选项。

详细配置请参见下表。

配置项	说明
允许 Web 未授权登录	允许未授权的用户通过 Web 方式登录主机。
允许 API 未授权登录	允许未授权的用户通过 API 方式登录主机。
收集未授权登录	用户进行未授权登录后，系统会自动收集用户和主机的授权对应关系。
收集主机帐户和密码	用户进行未授权登录后，系统会自动收集用户所登录主机的帐户和密码。
自动创建运维规则	系统检测到未授权登录的事件发生后，会自动创建相应授权关系，不需要管理员进行手动授权。

11.3.1.2 运维登录配置

在**运维登录**项中配置运维登录选项。

详细配置请参见下表。

配置项	说明
允许使用用户密码登录主机	允许用户使用堡垒机帐户登录主机，主要适用于用户和帐户同

配置项	说明
	属于 AD/LDAP 的场景。
允许使用 SSH 私钥登录主机	勾选此项后，系统将允许用户无需输入密码，直接使用 SSH 私钥登录主机进行运维。
允许使用 SSH-agent-forwarding 方式登录 SSH 服务器	勾选此项后，系统将支持 SSH-agent-forwarding 特性，适用于 SSH 服务器要求采用 publickey 方式登录的场景。需要在 SSH 登录项中设置 SSH banner。
开启应用会话共享	勾选此项后，不同应用共享的同一会话，审计权限由第一个应用决定。
检查授权时对主机端口进行强匹配	勾选此项后，在运维时会对授权关系中的主机端口进行强匹配。主要用于当系统中有多个相同 IP 不同端口的资产进行隧道方式运维时的场景。C/S 运维时需要主机端口与资产信息中的端口一致才能运维成功。

11.3.1.3 SSH 登录配置

在 **SSH 登录**项中配置 SSH 登录选项。

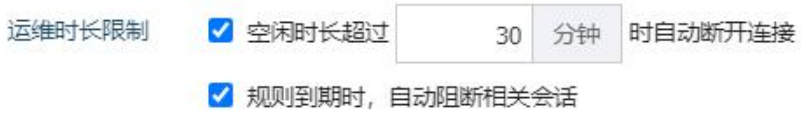
详细配置请参见下表。

配置项	说明
允许使用公钥登录	勾选此项后，用户可以使用 SSH 公钥登录堡垒机和目标服务器。
允许使用密码登录	勾选此项后，用户将通过密码登录堡垒机和目标服务器。
允许发送环境变量	勾选此项后，用户可以选择允许发送运维用户信息和运维来源 IP。
Shell 使用命令行方式	勾选此项后，将通过命令行方式登录目标服务器。
SSH banner	配置此项后方可使用 SSH-agent-forwarding 方式登录 SSH 服务器。

11.3.1.4 运维时长限制

勾选复选框后，开启对应功能。

设置空闲时长（取值范围：1~99,999）。

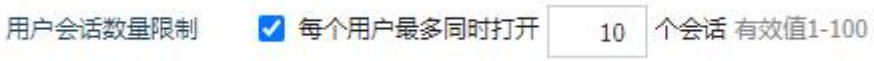


各协议空闲时长定义如下：

- RDP、VNC：客户端无数据发送时。
- FTP：命令通道和数据通道均无数据发送时。
- SSH、Telnet、SFTP、MySQL、SQL server、Oracle：客户端和服务端均无数据发送时。

11.3.1.5 用户会话数量限制

用户打开超过规定会话值时将受到限制，将无法再打开新的运维会话。



配置完成后，需点击**<保存更改>**。

11.3.2 告警配置

在系统菜单栏选择“**系统➤系统配置**”，进入**系统配置**页面，选择**告警配置**页签。

11.3.2.1 邮件配置

在**邮件配置**项中配置邮件的地址、端口、帐号、密码、收件人邮箱，点击**<保存更改>**保存邮件配置。点击**<发送测试邮件>**可测试邮件是否配置成功。

11.3.2.2 Syslog 配置

在 **Syslog 配置**项中填写发送者标识、Syslog 服务器 IP、端口，选择数据格式，点击**<保存更改>**保存 Syslog

配置。点击<**发送测试数据**>可测试 Syslog 是否配置成功。

详细配置请参见下表。

配置项	说明
发送者标识	能够标识发送者身份的信息。
服务器 IP	支持 IPv4 和 IPv6。
端口	服务器 Syslog 服务使用的端口。
数据格式	竖线分割：使用“|”分隔字符串。 JSON：JavaScript Object Notation，JS 对象简谱。采用完全独立于编程语言的文本格式来存储和表示数据。 请根据 Syslog 服务器的实际情况进行选择。

11.3.2.3 告警外送配置

告警外送是指将操作日志告警信息发送给邮件服务器或者 Syslog 服务器以及将主机命令外送至 Syslog 服务器。

在**告警外送配置**中将**操作日志**状态设置为**开启**，勾选需要外送的告警等级（包括邮件告警和 Syslog 告警），点击<**保存更改**>。

11.3.2.4 系统资源告警配置

在**系统资源告警配置**项中设置告警阈值，启用邮件告警，点击**<保存更改>**。当达到告警阈值时系统将会发送告警邮件。

11.3.2.5 Zabbix 配置

需要在 Zabbix 平台配置堡垒机的相关信息后，堡垒机才能向 Zabbix 平台发送数据。关于 Zabbix 平台的配置方法，请参考《堡垒机 V2.0.8.4 配置案例手册》。

通过 Zabbix 平台（需用户自备）监控堡垒机自身进程、端口、文件系统等核心模块，并支持阈值告警。

设置状态为“开启”，编辑服务器地址、主机名和同步配置频率，点击**<保存更改>**。

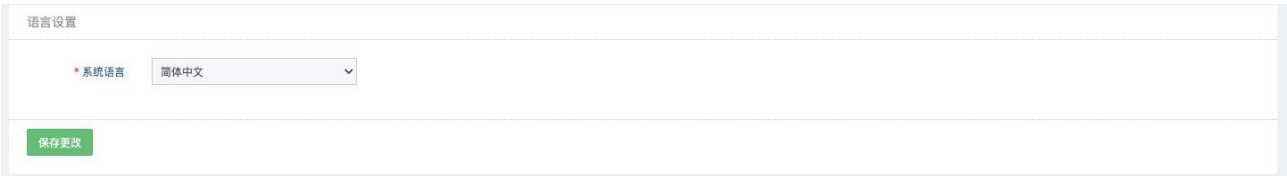
详细配置请参见下表。

配置项	说明
服务器地址	Zabbix 服务器的地址，支持 IPv4 和 IPv6。
主机名	堡垒机的名称，与 Zabbix 服务器上的配置保持一致。
同步配置频率	堡垒机与 Zabbix 服务器同步数据的的频率，单位为秒，取值范围 60~3600。

11.3.3 语言和界面

在系统菜单栏选择“**系统➤系统配置**”，进入**系统配置**页面。选择**语言和界面**页签，在语言设置项中可以设置系统语言。在网站备案号设置中配置备案号及其链接地址。

系统支持三种界面显示语言：简体中文、繁体中文和英文。启用了**允许用户切换界面语言**功能时，用户在登录时可以自由选择界面语言。当用户选择的界面语言设置与系统语言设置不一致时，系统外送的各类通知、日志等文本将仍然使用系统语言设置的语言。设置完成后需点击<**保存更改**>。



当堡垒机的地址以域名形式发布在公网时，需要对此域名进行备案。

设置网站备案号的信息，具体配置信息请以实际为准。配置完成后点击<**保存更改**>。

11.3.4 功能设置

在系统菜单栏选择“**系统➤系统配置**”，进入**系统配置**页面，选择**功能设置**页签。

11.3.4.1 部门管理

开启部门管理后，可以实现用户、资产的层级管理。

设置状态为“**开启**”，点击<**保存更改**>。

11.3.4.2 主机导出配置

当设置不导出密码时，导出文件的密码字段会置空。

文件在导入时，密码字段为空的帐户会视为手动登录模式，反之为自动登录模式。

相同的帐户名，不同的登录模式，视为不同帐户，故在导入时会出现新建帐户，而非修改帐户的情况。

选择是否导出密码，点击<**保存更改**>。

11.3.4.3 资产扫描配置

主机及主机帐户周期性扫描配置默认为关闭状态，若需要执行周期扫描，则在**配置项**中勾选对应项目，点击**<保存更改>**即可。开启主机连通性周期性检查、主机帐户有效性周期性检查后，每天 0 点自动触发资产的周期性扫描任务。

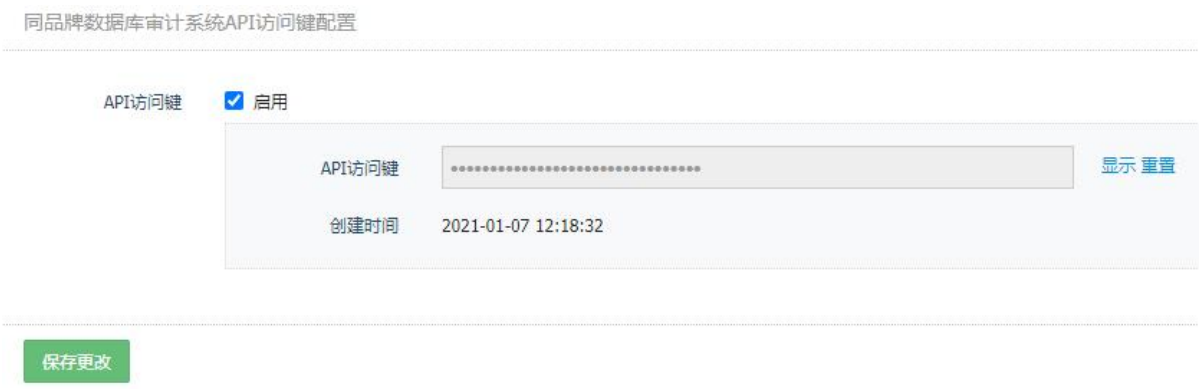
11.3.4.4 工单配置

关闭工单功能后，运维员无法通过新建工单浏览系统中所有的主机 IP 地址和主机帐户列表。设置**状态**为“开启”，点击**<保存更改>**即可开启工单功能。

11.3.4.5 同品牌数据库审计系统 API 访问键配置

API 访问键用于为第三方开发人员提供应用程序接口。同品牌数据库审计系统 API 访问键是提供给数据库审计与风险控制系统的应用程序接口。设置 API 访问键的操作方法如下：

勾选**启用**，点击**<重置>**，重置 API 访问键（可选操作），点击**<保存更改>**。



11.3.4.6 报表自动统计

开启报表自动统计后，可以提升报表页面数据加载效率。开启报表自动统计后，系统会在每日 0 点后自动统计前一周期的报表数据，会消耗一定系统 CPU 资源并持续一定时间，请按需设置。

设置状态为“**开启**”或“**关闭**”，点击<**保存更改**>。

11.3.4.7 同主机 SFTP/SSH 同名帐号关联

将状态设置为“开启”，点击<**保存更改**>。开启同名帐号户关联后，编辑帐户和设置改密计划时，同主机下同名的 SFTP 和 SSH 帐户将会被同步修改。

11.3.4.8 审计分页配置

当查询过滤数据不超过设置的范围时，在**会话审计**页面可显示末页页数。

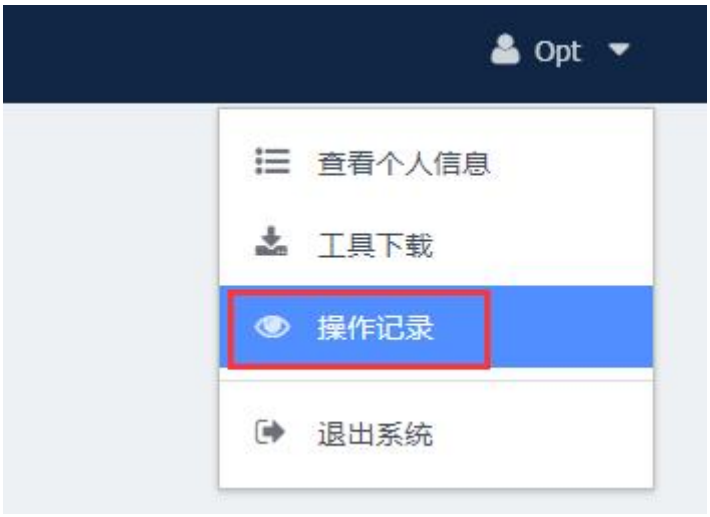
11.3.4.9 数据库审计控制

设置 SQL 语句最大长度，点击<**保存更改**>。当运维员通过堡垒机运维数据库时，执行的 SQL 语句长度不能超过设置值。

11.3.4.10 允许审计自查

在**允许审计自查**区域设置**状态**为“开启”，点击<**保存更改**>。用户可查看自己的历史运维记录。

在页面右上角的用户信息区点击当前用户名，从下拉菜单选择“**操作记录**”。



进入**会话自审计**页面查看当前登录用户的运维会话记录。

11.3.4.11 改密计划验密限制

为防止在特定条件下，网络中的其他安全设备将堡垒机的改密计划验密操作误判为暴力破解行为，可对堡垒机的改密计划验密操作进行限制。操作方法如下：

设置最大尝试次数和超时设置，点击**<保存更改>**。当满足任一条件时，系统会停止验密操作。

11.3.4.12 改密计划登录间隔

设置间隔时长，点击**<保存更改>**。当执行改密计划时，主机如果设置了登录频率限制，自动改密会触发登录频率限制，导致改密失败。针对此情况，可设置改密时主机帐户的登录频率。

11.3.5 改密脚本

改密脚本用于改密计划中通过改密脚本方式改密。适用于多个计划中的托管帐户全部为同类系统中的帐户的情况。新增改密脚本完成后，将改密脚本关联至改密计划任务的操作步骤请参见改密计划。

新建改密脚本的操作方法如下：

步骤 1. 在系统菜单栏点击“**系统➤系统配置**”，进入**系统配置**页面，选择**改密脚本**页签。点击<**新建改密脚本**>。

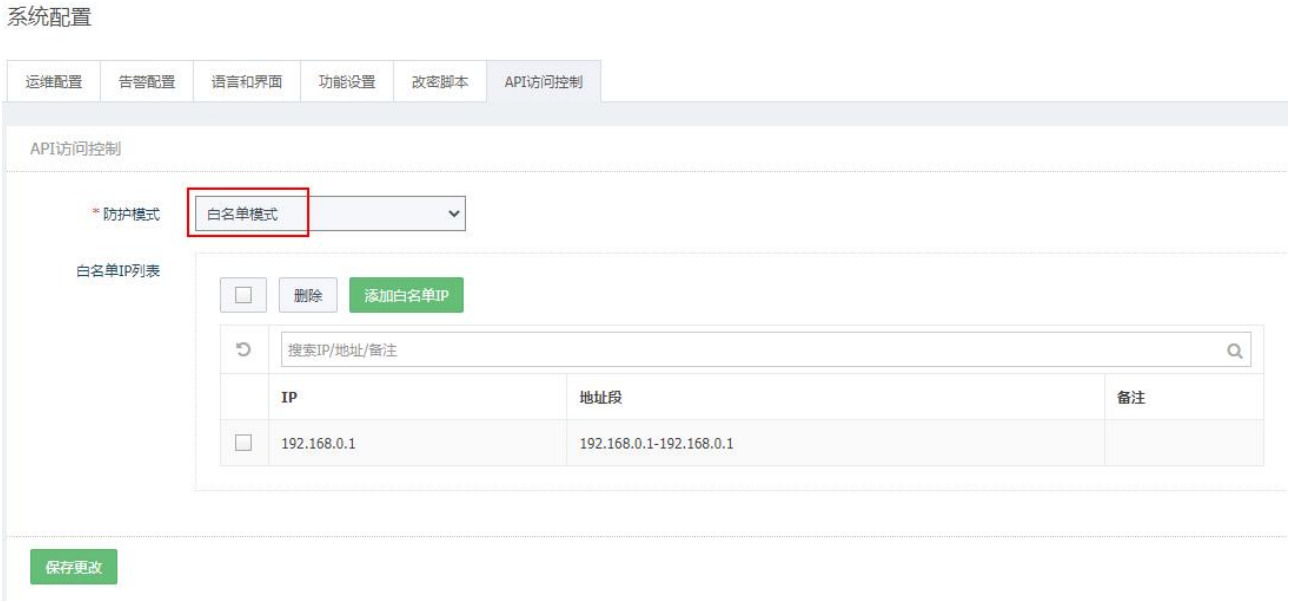
步骤 2. 在弹出的**创建改密脚本**对话框中填写脚本名称和脚本命令（关于脚本命令的说明可点击<**帮助**>进行查看看），点击<**创建**>完成改密脚本创建。

11.3.6 API 访问控制

API 访问控制可对开启了 API 访问键的用户进行访问权限上的控制。

API 访问控制开启后，只有 IP 在**白名单 IP 列表**中的用户才能进行 API 访问。

步骤 1. 在系统菜单栏点击“**系统➤系统配置**”，进入**系统配置**页面。选择 **API 访问控制**页签，设置**防护模式**默为“白名单模式”。



步骤 2. 点击<**添加白名单 IP**>，在弹出的的对话框中设置 IP，点击<**添加到白名单列表**>。

步骤 3. 返回 API 访问控制页面后点击<**保存更改**>。

11.4 存储管理

11.4.1 数据归档

数据归档是指对会话的录像进行归档，并对归档文件设置自动删除规则。操作方法如下：

步骤 1. 在系统菜单栏选择“**系统➤存储管理**”，进入**存储管理**页面（默认展示**数据归档**页签）。在**数据盘使用状态**项中可以查看详细的数据盘分区使用状态。

步骤 2. 在**录像归档**项中可以开启录像归档功能，将会话文件保存到远程归档服务器中。编辑相关信息，点击<**保存更改**>，保存录像归档配置。

详细配置请参见下表。

配置项	说明
状态	设置为“开启”时，将审计数据存储到服务器；设置为“关闭”时，将审计数据存储到本设备上。
时段	每天进行审计数据归档的时间，取值范围：0~23。
速度限制	限定审计数据归档的传输速度，取值范围：0~100，设置为 0 表示表示不限制传输速度。
时间范围	仅归档设定时间范围内的录像数据。
传输模式	包括 FTP 和 SFTP。
服务器地址	存储审计数据的服务器 IP 地址。
端口	存储审计数据的服务器接收数据时使用的端口。
用户名	存储审计数据的服务器的用户名。
密码	存储审计数据的服务器的密码。
路径	相对路径，例如:/test，对应的绝对路径为：文件服务器配置路径/test。请确保用户具有此路径的写入权限。

步骤 3. 在**自动删除**项中设置自动删除条件，点击<**保存更改**>，可以自动清理系统数据盘空间。

步骤 4. 在**历史审计文件同步**项中开启或关闭历史审计文件同步，可以控制集群中主从节点审计文件的同步行为。开启此功能时，会将从节点上的会话审计文件同步到主节点中进行保存，占用主节点存储空间，请根据需要进行设置。

11.4.2 网盘管理

网盘管理是指当用户采用 H5 的运维方式运维 RDP 协议的服务器时，需要在本地和远程服务器之间进行文件传输，需要借助网盘的功能来支持文件传输。

在系统菜单栏选择“**系统➤存储管理**”，进入**存储管理**页面。选择**网盘管理**页签，网盘配置默认为关闭状态。

系统支持本地存储、SFTP 存储和 NFS 存储三种存储方式。

◆ 本地存储方式

将**状态设置**为“开启”，**存储服务器**设置为“本地存储”，设置总容量，点击<**保存更改**>。

点击<**查询已使用容量**>，可查看网盘的已使用容量。

◆ SFTP 存储方式

将**状态设置**为“开启”，**存储服务器**设置为“SFTP 存储”，编辑相关信息，点击<**保存更改**>。

详细配置请参见下表。

配置项	说明
服务器 IP	SFTP 服务器的 IP。
端口	SFTP 服务器连接使用的端口。
用户名	SFTP 服务器的用户名。
密码	SFTP 服务器的密码。
总容量	SFTP 服务器的存储容量，请根据服务器的实际情况进行配置。
存储路径	SFTP 服务器的存储路径，例如：/opt。

◆ NFS 存储方式

将**状态设置**为“开启”，**存储服务器**设置为“NFS 存储”，编辑相关信息，点击<**保存更改**>。

详细配置请参见下表。

配置项	说明
服务器 IP	NFS 服务器的 IP。
存储路径	NFS 服务器的存储路径。
总容量	NFS 服务器的存储容量，请根据服务器的实际情况进行配置。

此外，需要在 NFS 服务器上进行相应配置，可点击**<NFS 服务器配置指导>**，根据配置指导进行配置。

11.4.3 日志备份

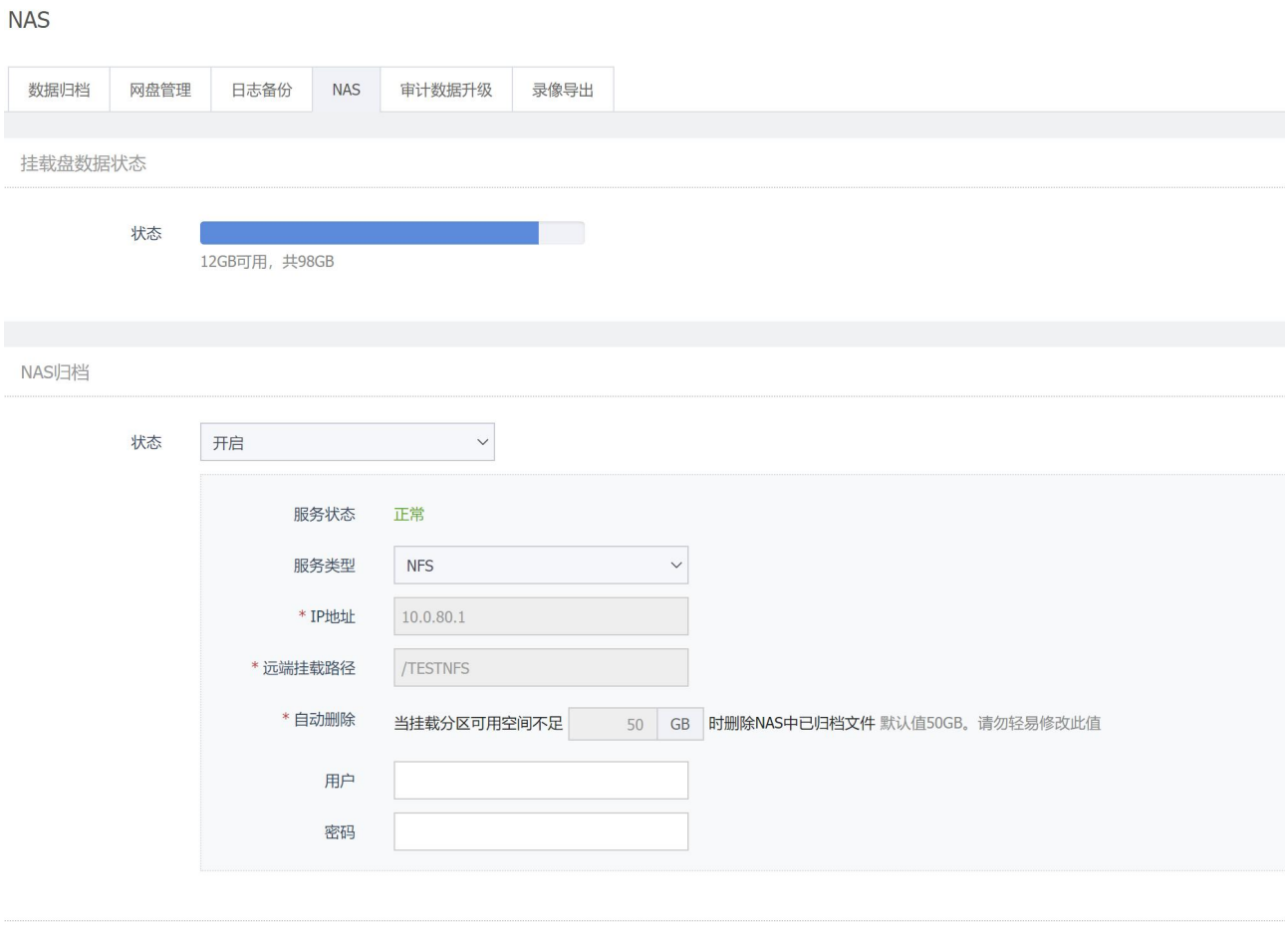
在系统菜单栏选择“**系统➤存储管理**”，进入**存储管理**页面。选择**日志备份**页签，选择需要备份的时间范围和备份内容，点击<**创建日志备份**>进行日志备份。

在备份列表中可查看创建的日志备份，点击**操作**列中的<**下载**>可将备份下载到本地文件中查看。点击**操作**列中的<**删除**>可以删除日志备份。

11.4.4 NAS

当开启 NAS 归档时，会话数据将自动归档到 NAS 服务器挂载路径中。开启 NAS 归档功能的操作方法如下：

在系统菜单栏选择“**系统➤存储管理**”，进入**存储管理**页面。选择 **NAS** 页签，将**状态**设置为“开启”，编辑相关信息，点击<**保存更改**>。



详细配置请参见下表。

配置项	说明
服务类型	可选择 NAS 的类型：NFS 或者 CIFS
IP 地址	NAS 服务器的 IP。
远端挂载路径	NAS 服务器的存储路径。
自动删除	当挂载分区空间小于设置值时，会删除 NAS 中已归档的文件，默认为 50GB，请勿轻易修改此值。
用户	登录 NAS 服务器的用户名
密码	登录 NAS 服务器的用户密码

开启 NAS 归档后，可在会话审计详情页面查看审计录像文档是否已归档 NAS 服务器。

11.4.5 审计数据升级

系统软件版本升级后，因数据库的改动，需要对审计数据进行迁移。

在菜单栏选择**系统➤存储管理**”，进入**存储管理**页面。选择**审计数据升级**页签，可以查看旧版审计数

据迁移升级的状态。点击<**下载日志**>，可将审计数据升级日志下载到本地查看。

11.4.6 录像导出

可将系统的审计录像导出至服务器。操作方法如下：

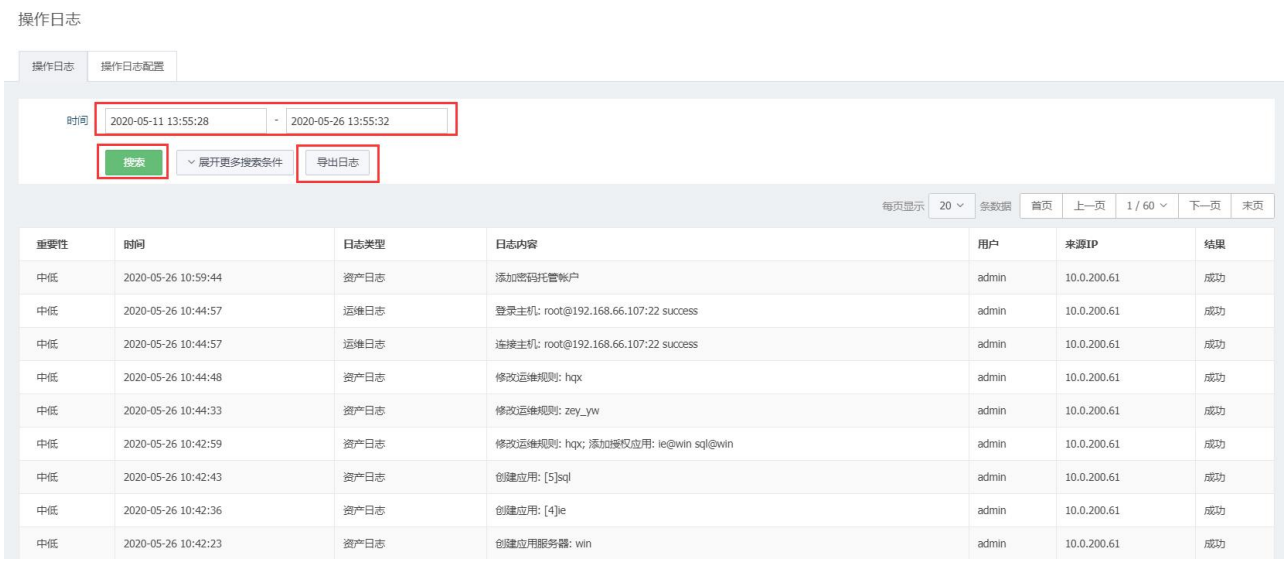
在系统菜单栏选择“**系统➤存储管理**”，进入**存储管理**页面。选择**录像导出**页签，编辑相关信息，点击<**导出**>。

详细配置请参见下表。

配置项	说明
时间范围	设置审计录像的时间范围。
传输模式	数据传输使用的协议，包括 SFTP 和 FTP。
服务器地址	接收审计录像数据的服务器的 IP，支持 IPv4 和 IPv6。
端口	服务器接收审计录像数据使用的端口。
用户名	服务器的用户名。
密码	服务器的密码。
路径	服务器存储审计录像数据的路径，请确保用户有此路径的写入权限。

11.5 操作日志

在系统菜单栏选择“**系统➤操作日志**”，进入**操作日志**页面，设置时间，点击<**展开更多搜索条件**>可设置其他搜索条件，点击<**搜索**>可查询符合条件的操作日志。点击<**导出日志**>可将日志文件导出至本地。



选择**操作日志配置**页签，进入操作日志配置页面，选择日志类型，设置重要性，点击**<保存更改>**。点击**<恢复默认设置>**可恢复默认配置。

11.6 系统报表

系统报表是用于统计系统的状态及操作记录（包括系统状态信息、操作重要性、用户控制、主机控制、会话控制、用户与资产操作、用户源 IP、异常用户、异常 IP 和报表导出）。

在系统菜单栏选择“**系统➤系统报表**”，进入**系统报表**页面。选择按小时/按天/按周/按月查看系统报表各项数据。

选择**报表导出**页签，进入报表导出页面，选择报表类型、周期、报表分析时间范围和导出文件格式，点击<**导出系统报表**>，将系统数据报表导出至本地进行查看。