天翼云•安全专区•云堡垒机

用户使用指南

中国电信股份有限公司云计算

目录

1. 云堡垒机概述

1.1. 概述

随着信息安全的快速发展，需求的增长和信息技术的进步，先进的设计理念和技术手段的提升，来自内部的安全威胁日益增多，综合防护、内部威胁防护等思想越来越受到重视，而各个层面的政策合规，如“萨班斯法案”,“信息系统等级保护”等等也纷纷对运维人员的操作行为审计提出明确要求。构建规范灵活的互联网信息化架构，强化安全等级保护，加强基础设施支撑，进一步完善和创新应用，推动互联网业务系统优化整合、互联互通、信息共享和业务协同，实现应用上更加规范合理、技术上更加先进、安全上更加可靠的目的。云堡垒机作为运维安全审计产品将成为信息系统安全的最后一道防线，其作用将越来越重要，应用范围势必会快速扩展到各个行业的信息系统。

云堡垒机实现对信息系统运维人员的操作方法、操作过程、操作结果、系统提示等进行全方位记录的功能，并可以进行“行为重现”，以便对操作行为的真实性、正确性、合规性、效益性进行审查和监督。

为了加强各业务系统运维人员高效使用本系统，特定制了本手册，用于指导互联网业务系统运维人员、运维审计员和系统管理员的日常维护工作。

8.1.2 名词解释

- **用户组**

用户组是所有用户依照组织架构构建的集合，用于划分用户组织范围。

- **资源组**

资源组是内网所有设备依照组织架构构建的集合，用于划分设备的归属范围。

- **用户**

用户是指用内网中所有运维人员及管理员的集合。该用户是内网自然人身份的唯一标识。用于实现基于真实身份的身份认证和审计。

- **资源**

资源是指添加到本平台的目标设备的集合，包括各类主机、网络设备、数据库、B/S 应用系统等。

- **授权**

授权是指通过本平台对运维用户授予目标资源或账号的访问权限的行为。

- **运维审计**

运维审计是指本平台对普通运维人员访问目标资源的运维行为进行的审计记录。

- **配置审计**

配置审计是指平台管理人员对平台的配置、授权、数据修改等行为的审计记录。

- **密码包接收人**

密码包接收人是指接收改密过程中密码包的人员。

- **解密密钥接收人**

解密密钥接收人接收改密过程中解密密钥的人员。

- **可管理角色**

配置可管理角色的角色赋予用户后，该用户拥有把可管理的角色分配给其他用户的权限。

云堡垒机初始化操作

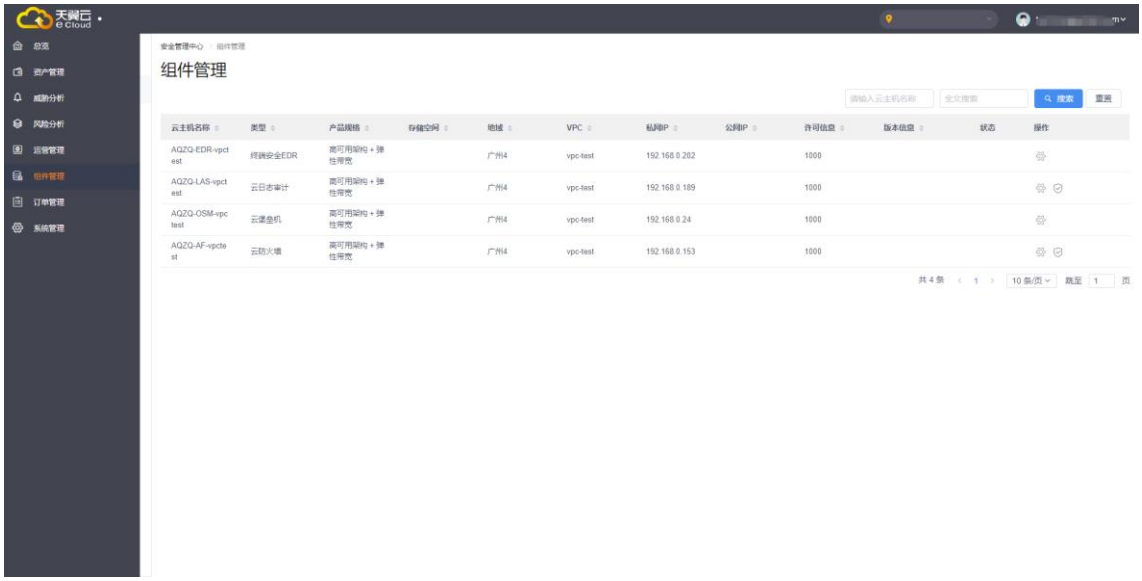
云堡垒机登录方式请参考天翼云安全专区安全管理中心手册，建立符合内部实际使用的管理员账号。

使用 WEB 方式登录方式

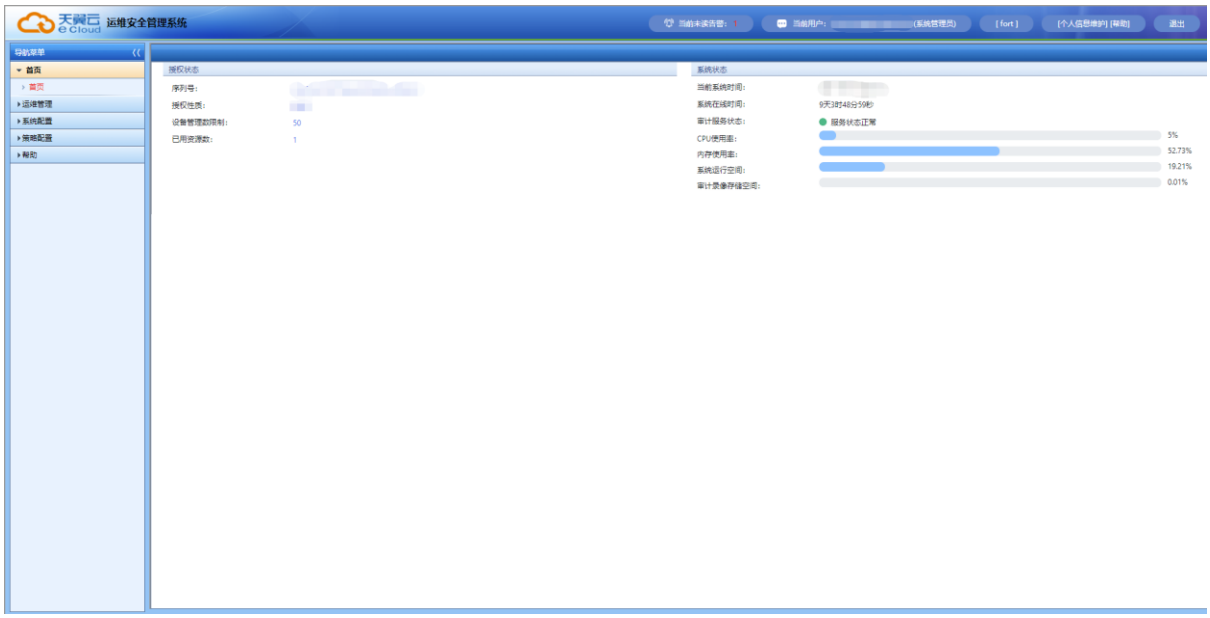
操作步骤:

单点登录日志审计

1、 通过天翼云安全账号登录天翼云控制中心，进入天翼云等保安全专区安全管理平台，在平台中找到安全专区，点击【云堡垒机】->【操作】登录。



2、从安全管理平台进行单点登录，无需密码，点击进入，即跳转进入。



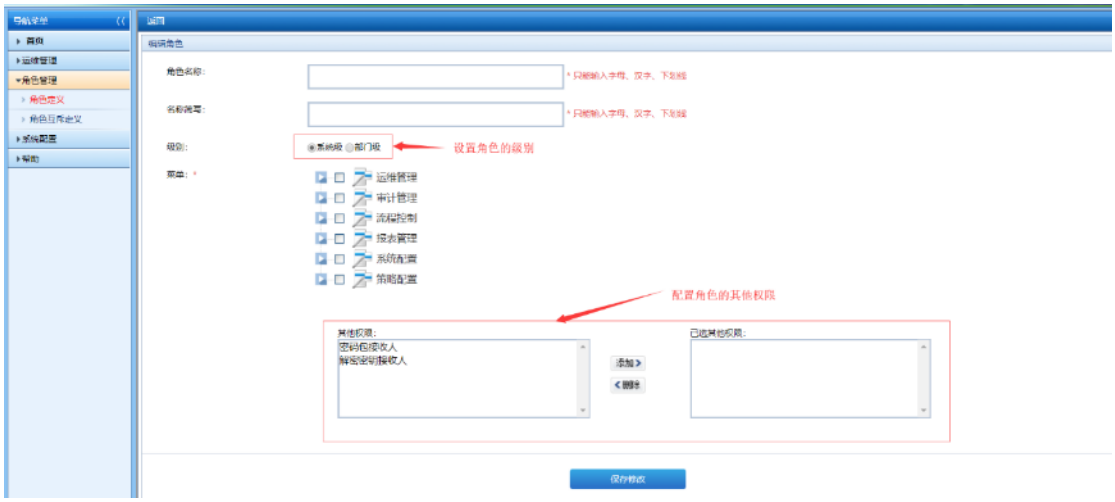
角色管理

角色管理用于给用户定义使用权限。角色管理可以自定义角色，也可使用预置角色（初始化用户、运维操作员、系统管理员、安全管理员、审计管理员）。

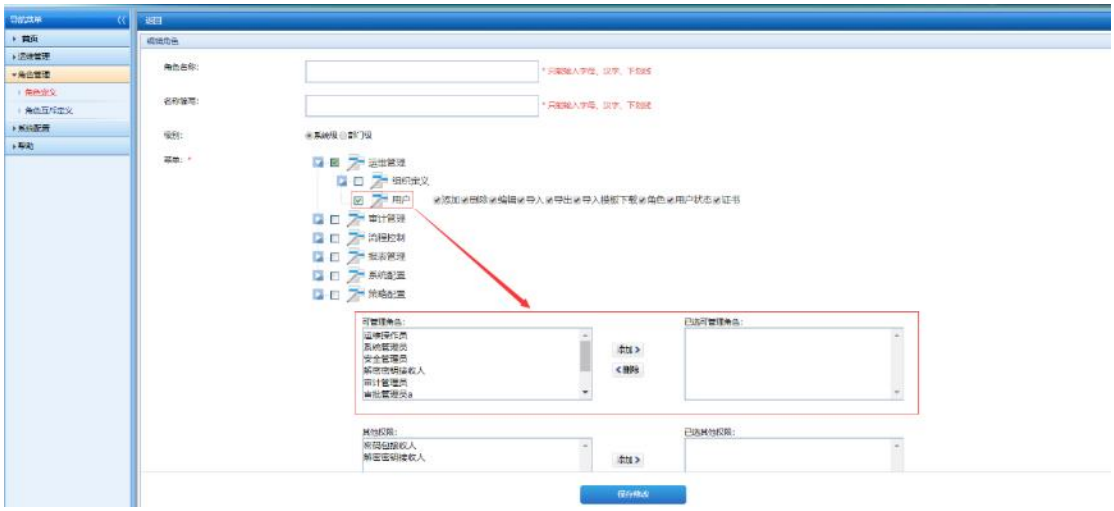
用**系统管理员**登录系统，点击系统菜单上**角色管理**进入角色管理界面。

角色设置：

- 级别：系统级 or 部门级；
- 密码包接收人：配置密码包接收人权限的角色赋予用户后，该用户可以接收改密过程中的密码包。
- 解密密钥接收人：配置解密密钥接收人权限的角色赋予用户后，该用户可以接收改密过程中的解密密钥。



配置可管理角色的角色赋予用户后，该用户拥有把可管理的角色分配给其他用户的权限（拥有【运维管理】->【用户】模块的角色才能配置可管理角色）。

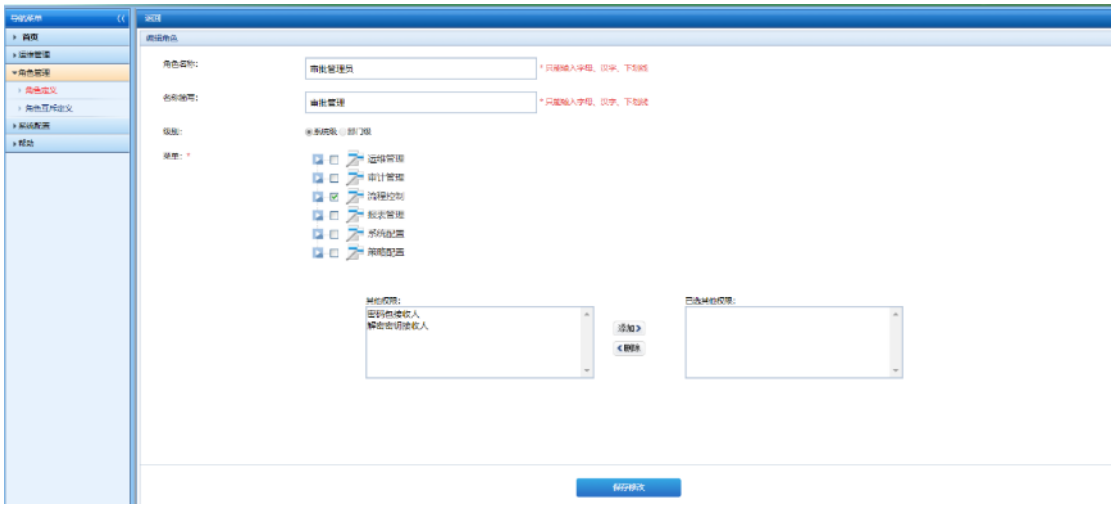


1.2. 角色定义

1.2.1. 角色添加

用系统管理员 admin 登录系统，点击**添加**按钮。

进入编辑角色界面，角色名称填写为审批管理员，级别选择系统级。

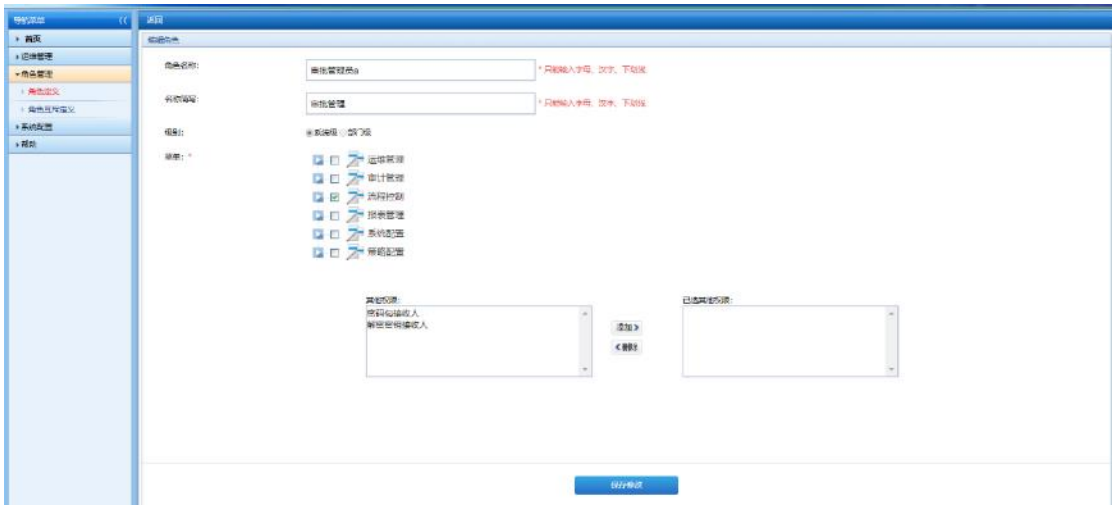


点击保存按钮后角色定义成功,点击返回按钮，角色定义页面显示审批管理员条目。

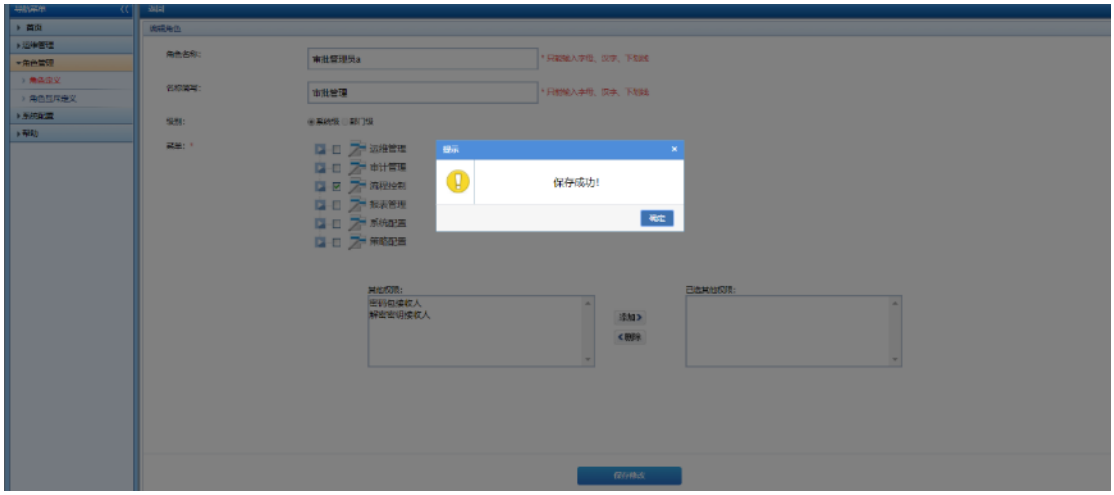
1.2.2. 角色编辑

点击审批管理员角色的编辑按钮。

进入编辑角色界面，将审批管理员更改为审批管理员 a。



点击保存按钮，提示：保存成功!



点击返回按钮，角色定义页面审批管理员更改为审批管理员 a。

1.2.3. 角色删除

找到需要删除的角色，点击删除按钮。

弹出提示窗口，点击确定按钮。

角色定义页面超级审计员条目已删除。

1.3. 角色互斥定义

角色互斥定义的功能是约束用户的权限。互斥的两个角色不能同时赋予同一个用户。系统内置了系统管理员、安全管理员、审计管理员角色，三个角色互为互斥。

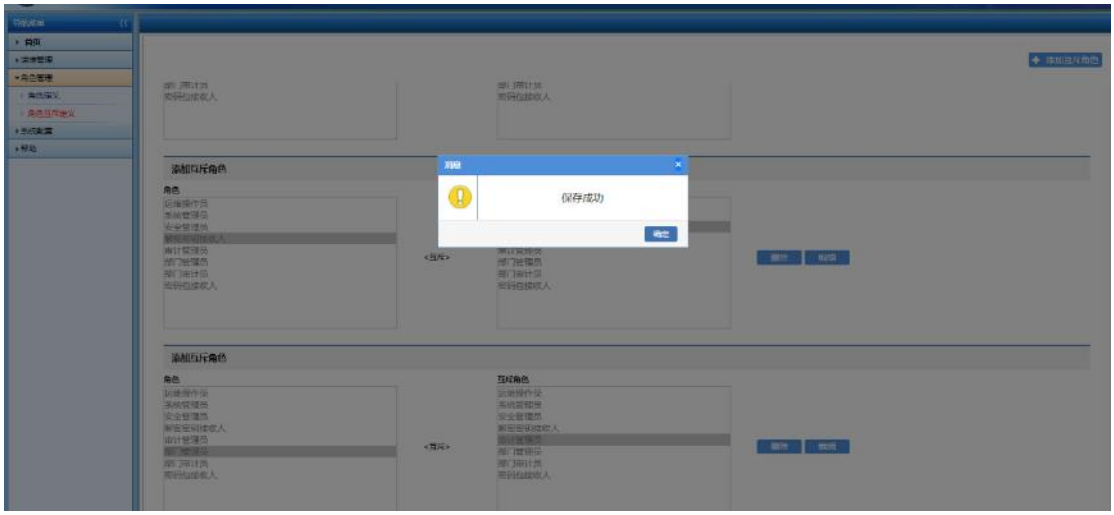
用系统管理员 admin 登录系统，点击系统菜单上角色管理->角色互斥定义进入角色互斥定义界面。

1.3.1. 角色互斥添加

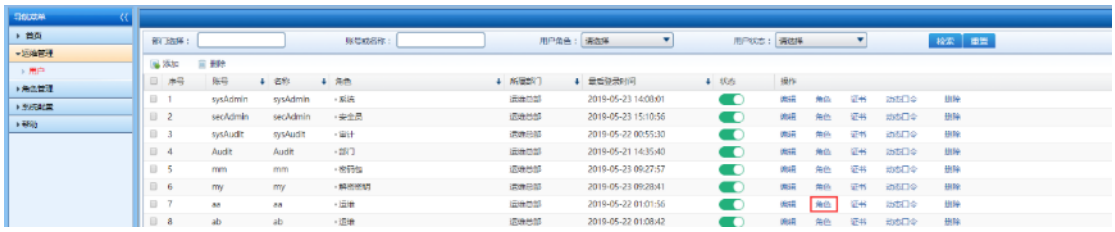
用系统管理员 sysAdmin 登录系统，点击添加互斥角色按钮。

角色列选择部门管理员，互斥角色列选择部门审计员。

点击保存按钮，弹出提示窗口。



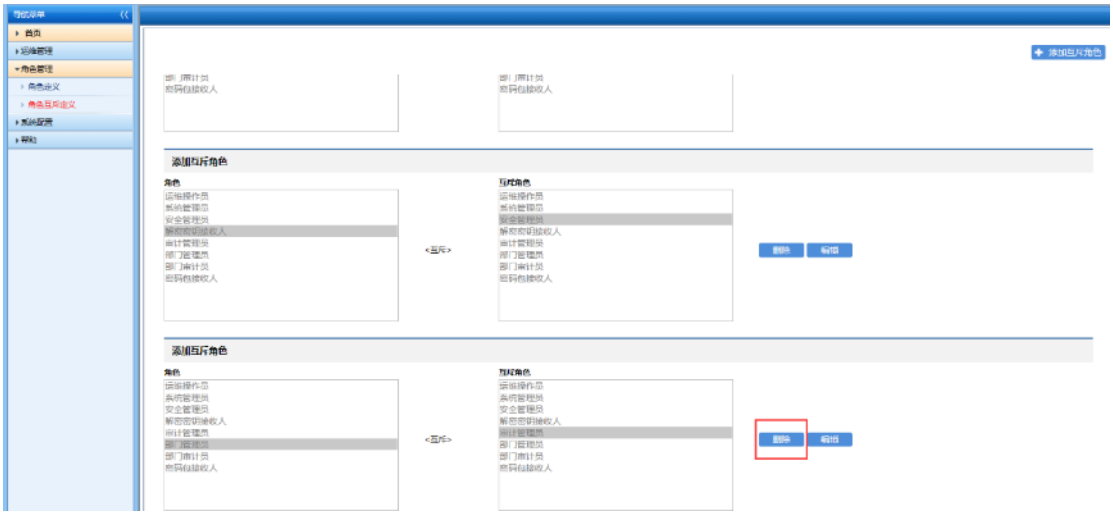
用安全管理员 admin 登录系统，点击用户 aa 的角色按钮。



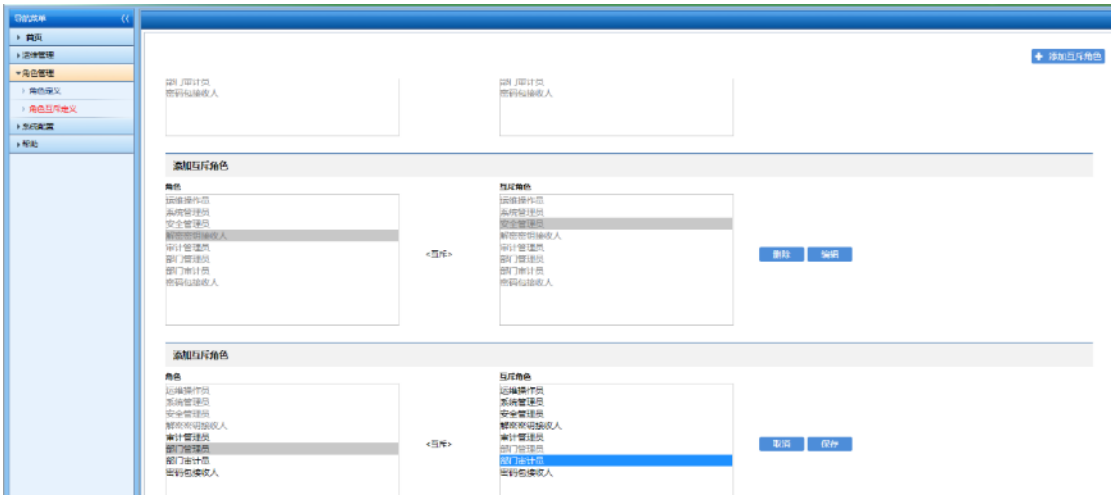
跳转到角色编辑页面，给用户 aa 添加部门管理员、部门审计员角色。选中部门管理员、部门审计员，点击添加按钮，弹出提示窗口。

1.3.2. 角色互斥编辑

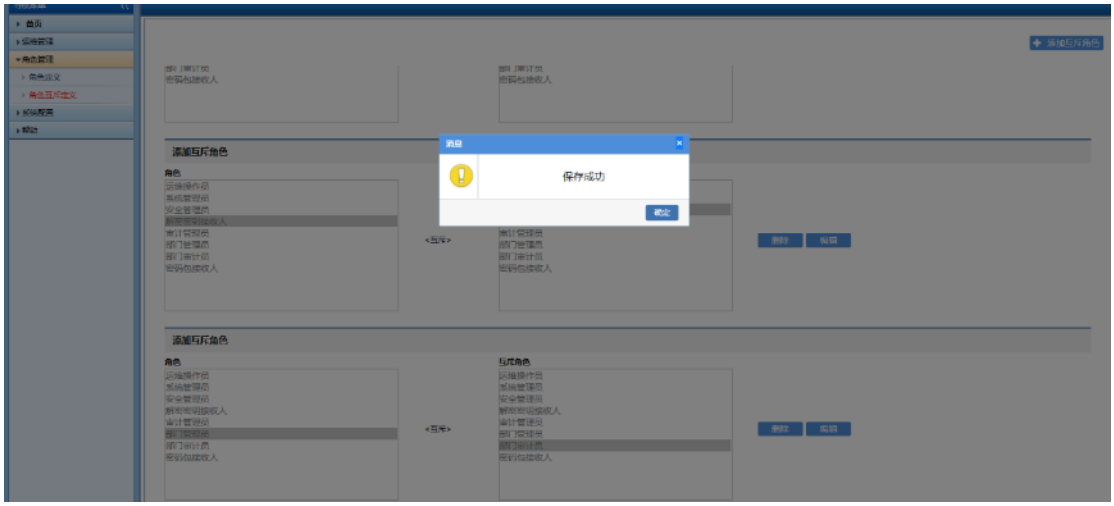
用系统管理员 admin 登录系统，点击部门管理员和部门审计员互斥角色的编辑按钮。



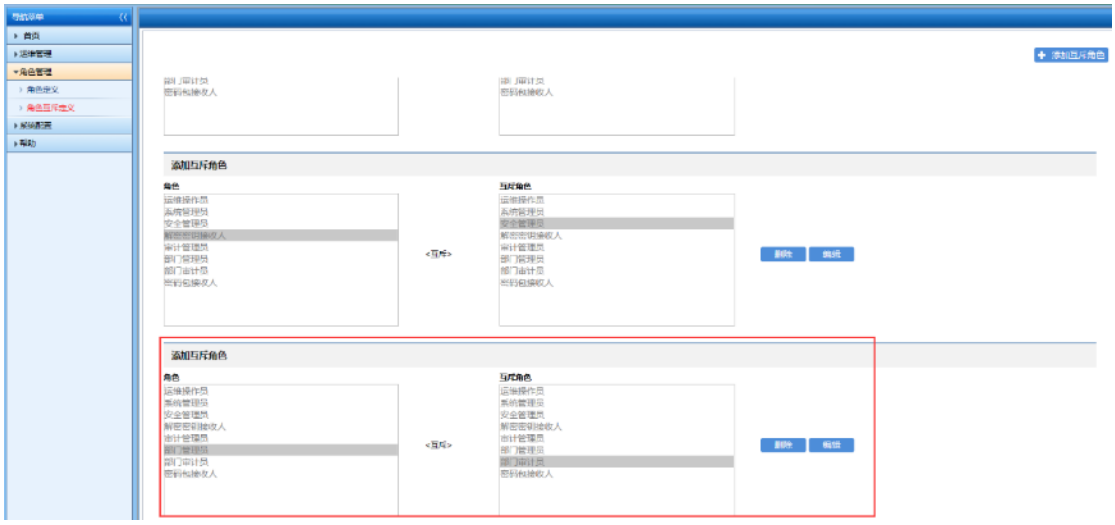
将部门管理员和部门审计员互斥角色，更改为部门安全员和部门审计员角色互斥。



点击保存按钮，弹出提示窗口。



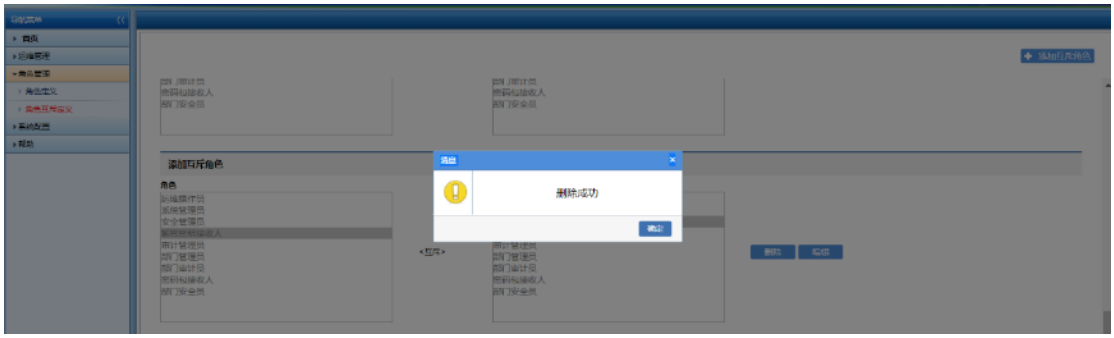
部门管理员和部门审计员互斥角色，已经改为部门安全员和部门审计员角色互斥。



1.3.3. 角色互斥删除

点击部门安全员和部门审计员互斥角色的删除按钮。

弹出提示窗口。

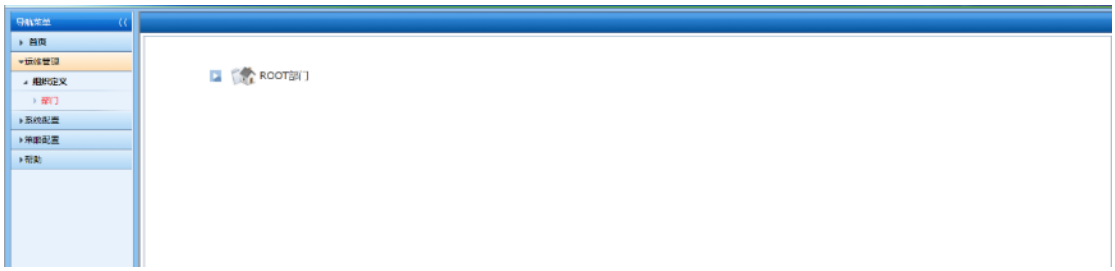


1.4. 组织定义

组织定义由部门、用户组和资源组三部分组成。部门用于组建企业组织架构，可设置多级部门，用户组用于对内部人员按用户组进行分组管理，资源组用于把内部运维设备按设备类型或者按照部门进行分组管理。

1.4.1. 部门

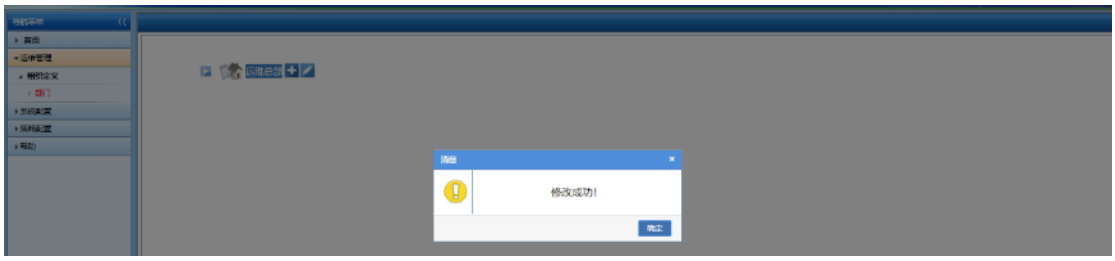
用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击运维管理->组织定义链接进入组织定义界面。



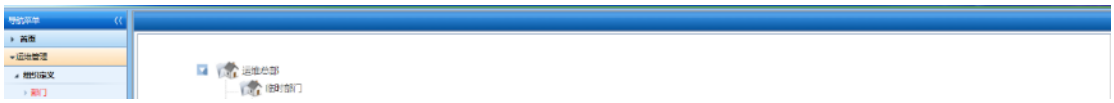
1.4.1.1 部门重命名

点击 ROOT 部门，再点击重命名图标，在弹出的输入框中输入你要编辑的部门名，点击确定按钮。

弹出提示信息修改成功！



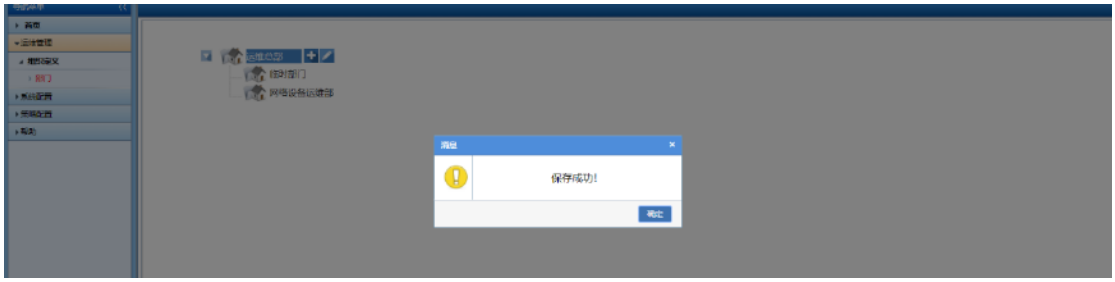
点击确定按钮，返回部门界面，ROOT 部门名称变为运维总部，至此部门重命名完成。



1.4.1.2 部门添加

点击运维总部，再点击添加图标  ，在弹出的输入框中输入你要添加的部门名，点击确定按钮。

弹出提示信息保存成功！



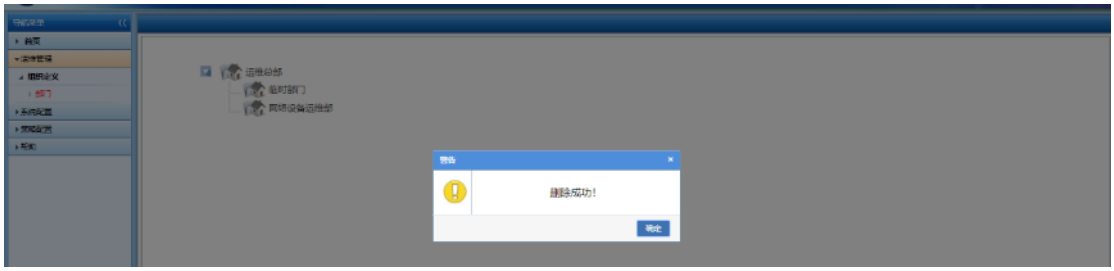
点击确定按钮，返回部门界面，运维总部下增加了名称为网络设备运维部的新部门，至此部门添加完成。

1.4.1.3 部门删除

点击数据库运维部，再点击删除图标  。

弹出提示信息确认删除部门数据库运维部？

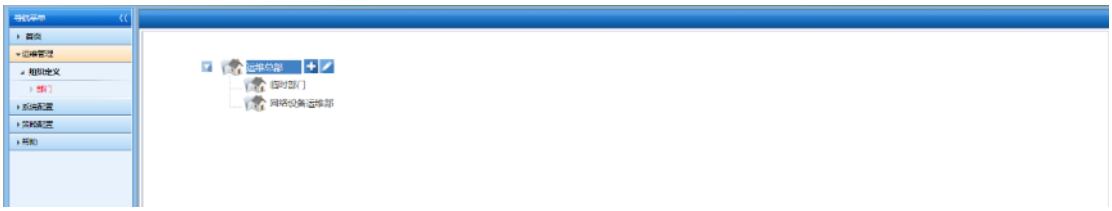
点击确定按钮，弹出提示信息删除成功！



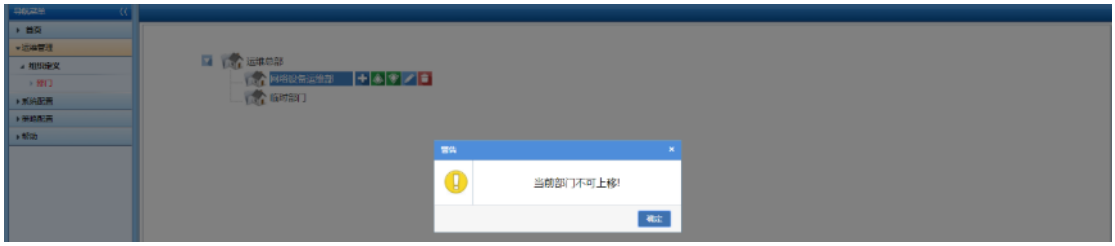
点击确定按钮，返回部门界面，运维总部下不显示名称为数据库运维部的部门，至此部门删除完成。

1.4.1.4 部门上移下移

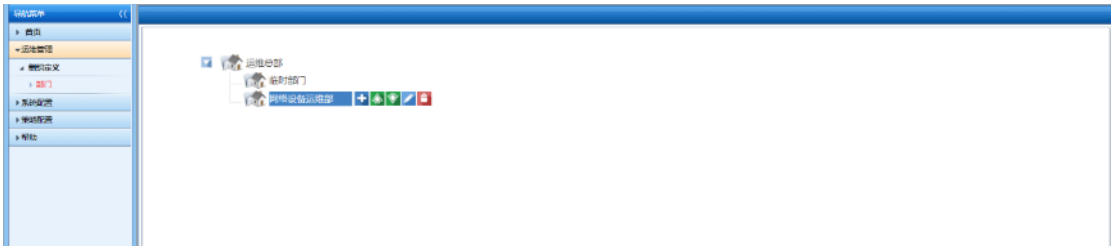
同级部门之间可通过上移/下移按钮进行排序，以网络设备运维部为例。



点击网络设备运维部，再点击上移图标  ，弹出告警信息当前部门不可上移！当部门已处于同级部门的最上方时，不可再进行上移，下移同理。

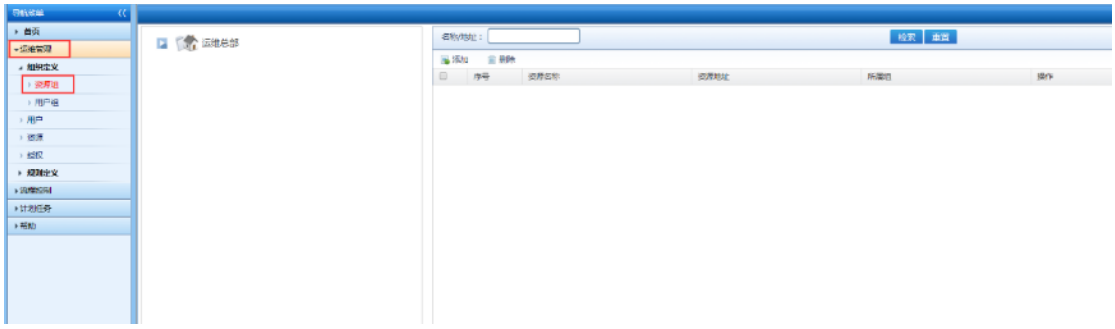


点击网络设备运维部，再点击下移图标  ，网络设备运维部则向下移动一位。至此部门上移/下移完成。



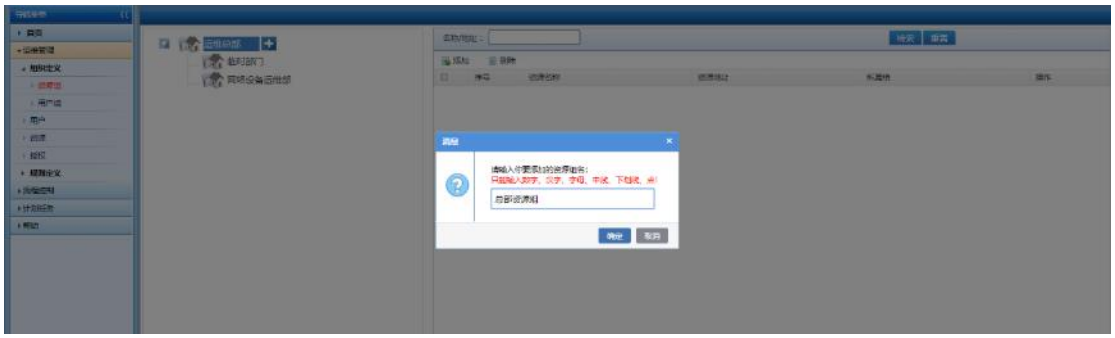
1.4.2. 资源组

用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理 ->组织定义->资源组链接进入资源组界面。

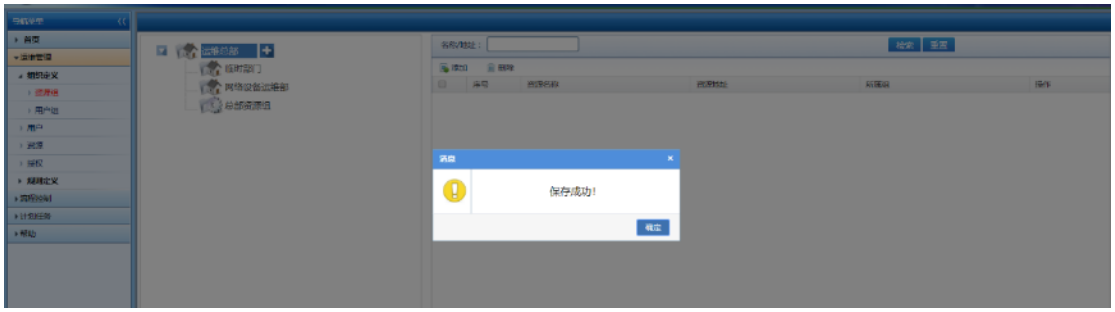


1.4.2.1 资源组添加

点击运维总部，再点击添加图标  ，在弹出的输入框中输入你要添加的资源组名，点击确定按钮。



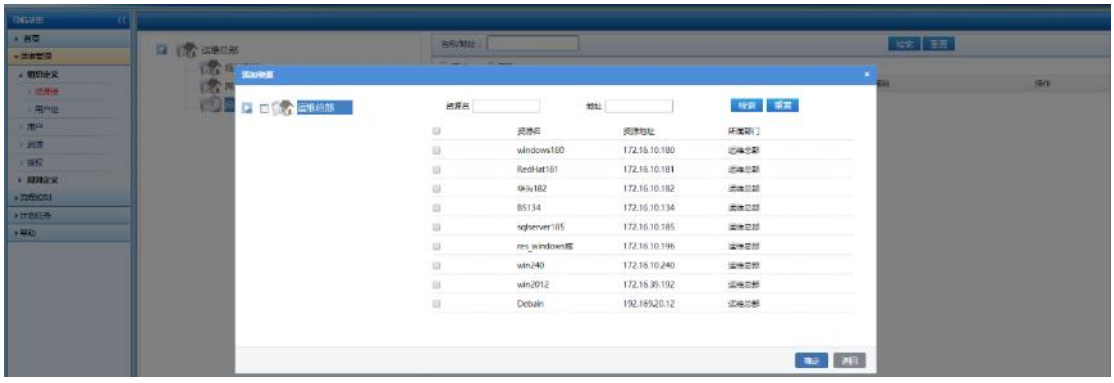
弹出提示信息保存成功！



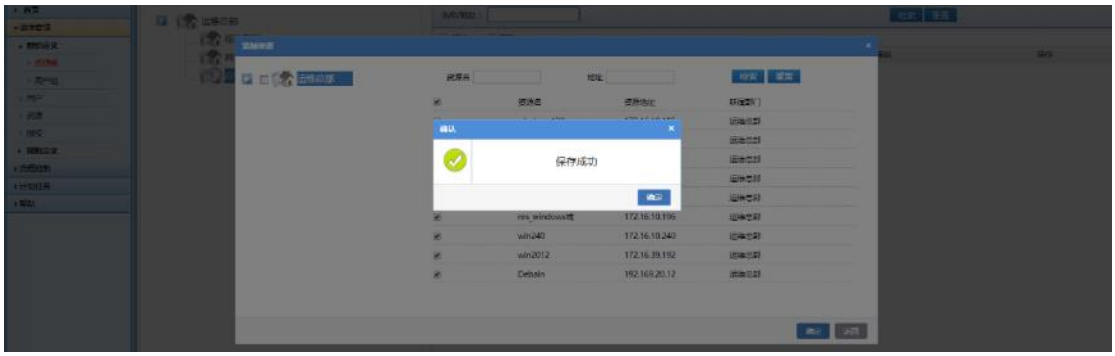
点击确定按钮，返回资源组界面，运维总部下增加了总部资源组。

可在资源组中添加资源，将运维设备按设备类型或者按照部门进行分组管理。选择总部资源组，点击右侧列表的添加按钮。

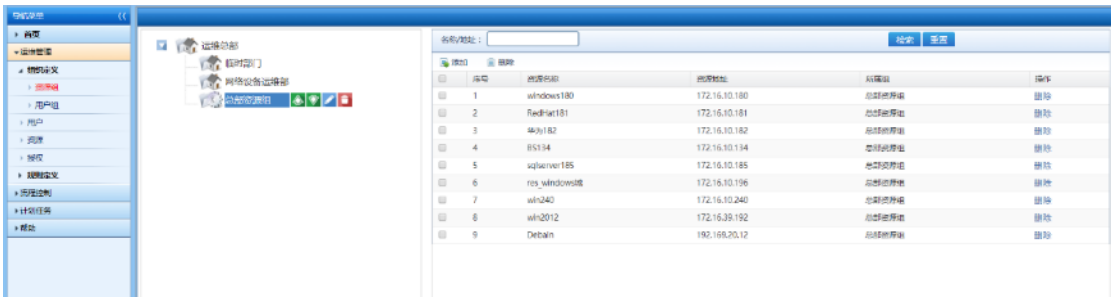
弹出添加资源选择框，点击检索按钮，在资源列表中勾选待选资源，加入总部资源组，点击确定按钮。



弹出提示信息保存成功！



点击确定按钮，返回资源组界面，总部资源组中增加了资源。



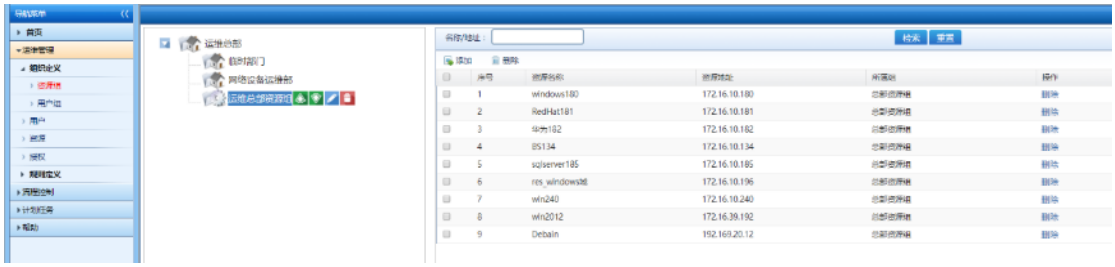
至此资源组添加完成。

1.4.2.2 资源组重命名

点击总部资源组，再点击重命名图标  ，在弹出的输入框中输入你要编辑的资源组名，点击确定按钮。

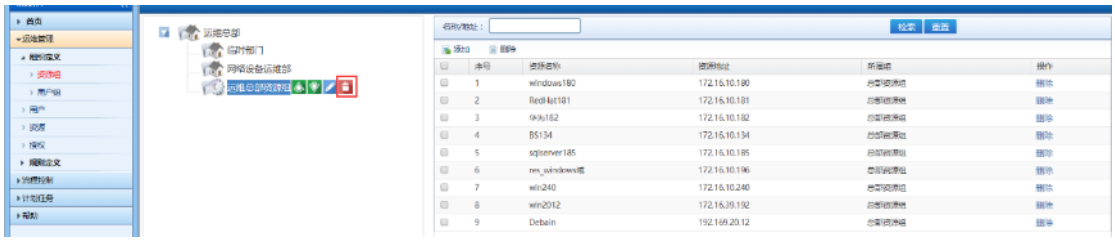
弹出提示信息修改成功！

点击确定按钮，返回资源组界面，总部资源组名称变为运维总部资源组，至此资源组重命名完成。

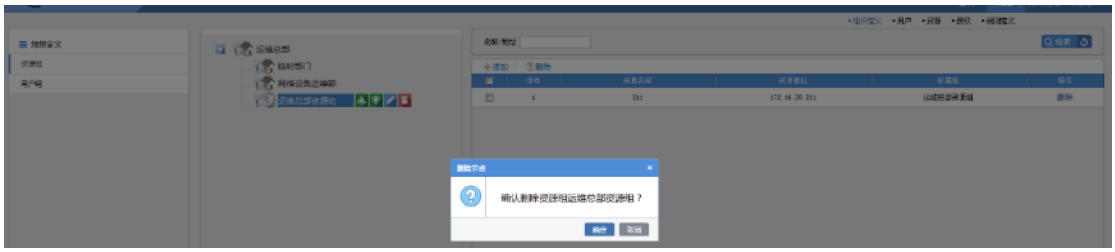


1.4.2.3 资源组删除

点击运维总部资源组，再点击删除图标  。

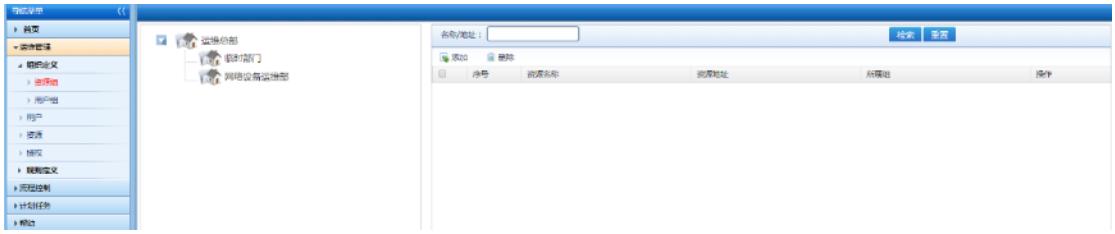


弹出提示信息确认删除资源组运维总部资源组？



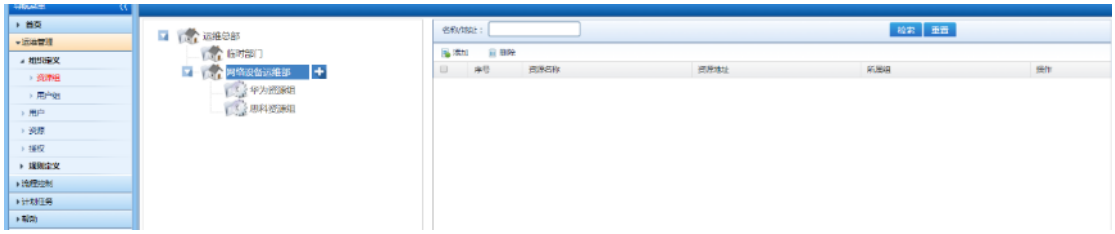
点击确定按钮，弹出提示信息删除成功！

点击确定按钮，返回资源组界面，运维总部下不显示名称为运维总部资源组的资源组，至此资源组删除完成。

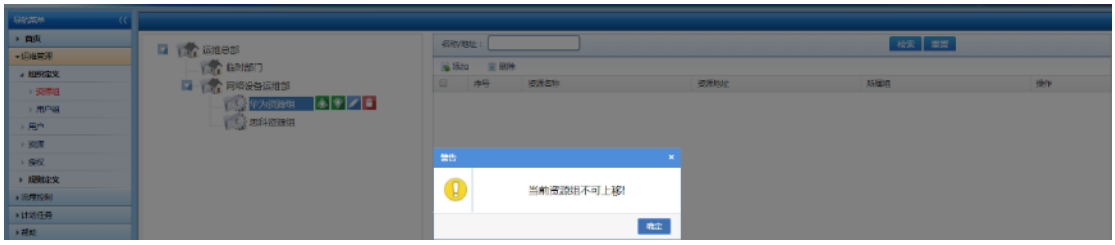


1.4.2.4 资源组上移下移

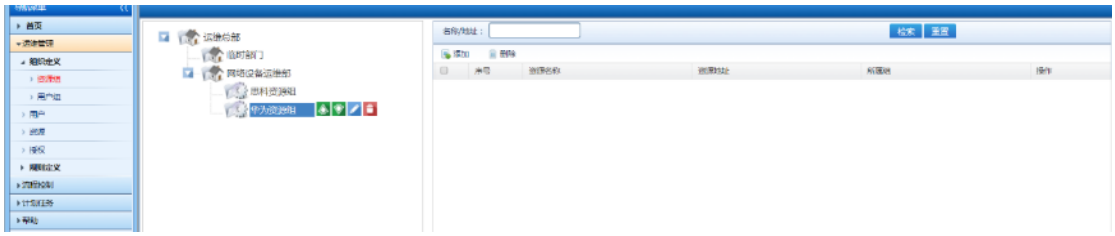
同部门内可通过上移/下移按钮将资源组进行排序，以网络设备运维部下的资源组为例。



点击华为资源组，再点击上移图标  ，弹出告警信息当前资源组不可上移！当资源组已处于其部门的最上方时，不可再进行上移，下移同理。



点击华为资源组，再点击下移图标  ，华为资源组则向下移动一位。至此资源组上移/下移完成。

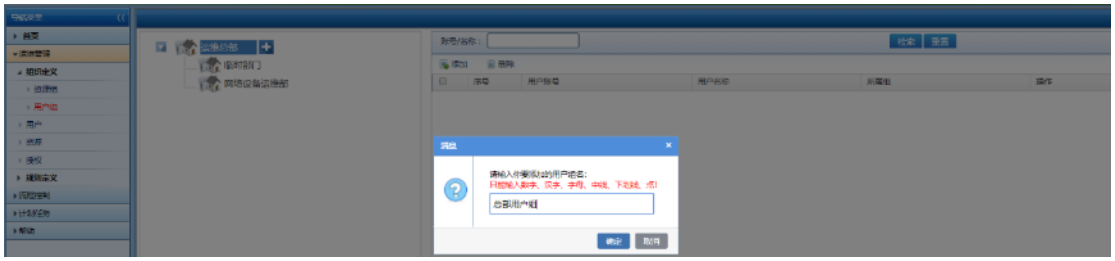


1.4.3. 用户组

用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理 ->组织定义->用户组链接进入用户组界面。

1.4.3.1 用户组添加

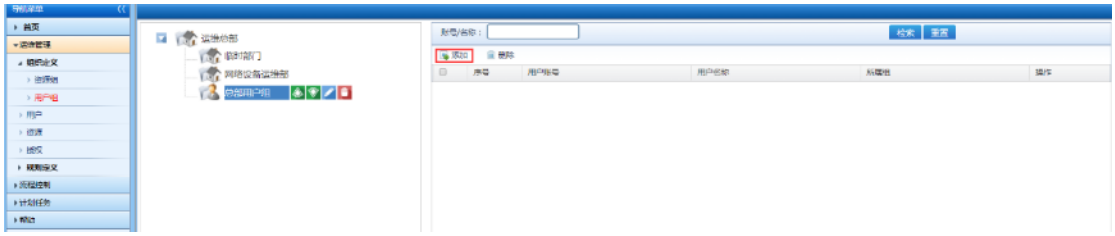
点击运维总部，再点击添加图标  ，在弹出的输入框中输入你要添加的用户组名，点击确定按钮。



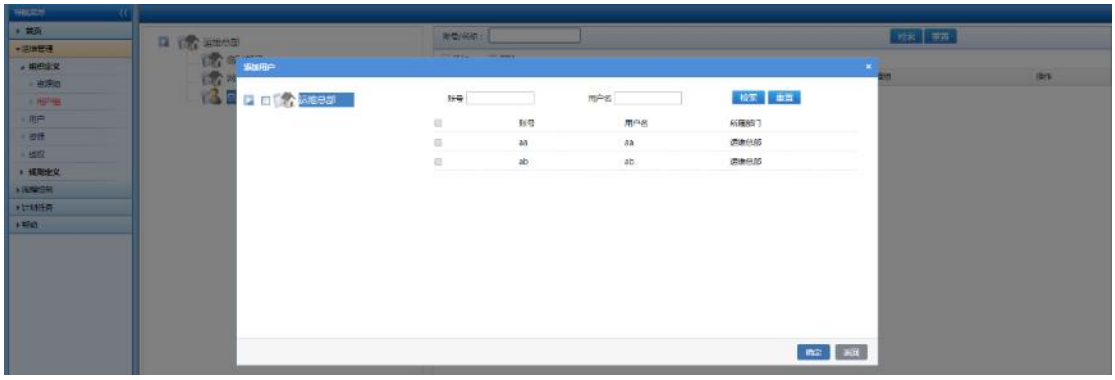
弹出提示信息保存成功！

点击确定按钮，返回用户组界面，运维总部下增加了总部用户组。

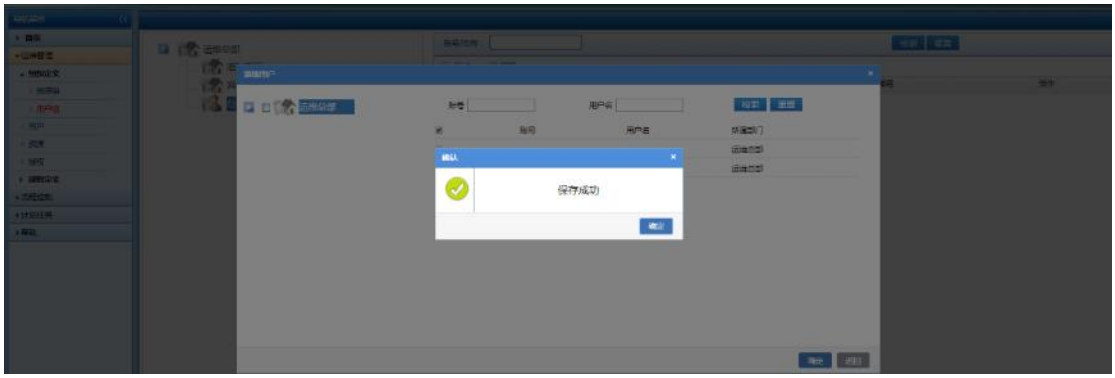
可在用户组中添加用户，将用户按用户组进行分组管理。选择总部用户组，点击右侧列表的添加按钮。



弹出添加用户选择框，点击检索按钮，在用户列表中勾选待选用户，加入总部用户组，点击确定按钮。



弹出提示信息保存成功！



点击确定按钮，返回用户组界面，总部用户组中增加了用户 aa。

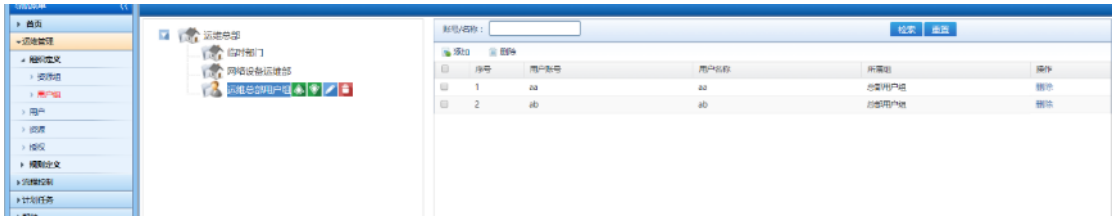
至此用户组添加完成。

1.4.3.2 用户组重命名

点击总部用户组，再点击重命名图标，在弹出的输入框中输入你要编辑的用户组名，点击确定按钮。

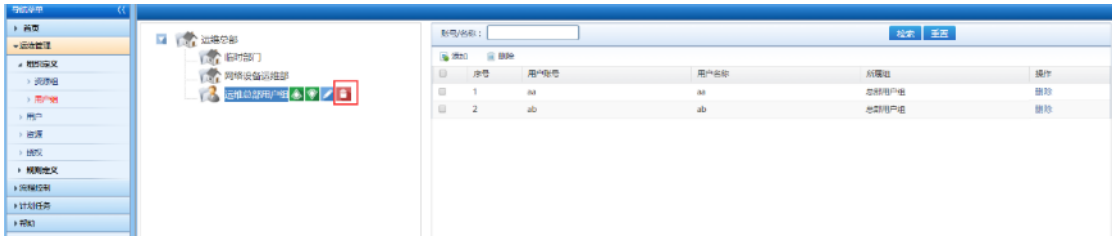
弹出提示信息修改成功！

点击确定按钮，返回用户组界面，总部用户组名称变为运维总部用户组，至此用户组重命名完成。

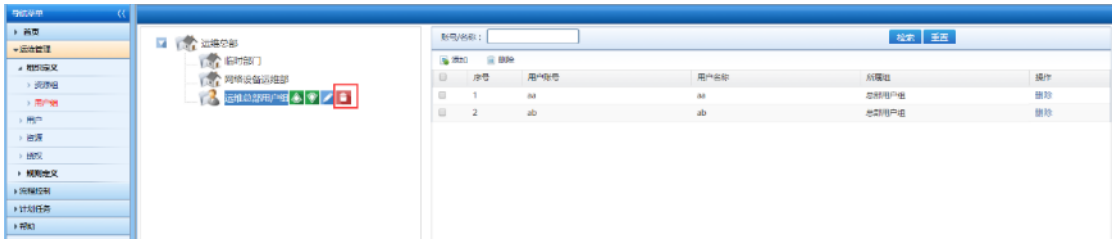


1.4.3.3 用户组删除

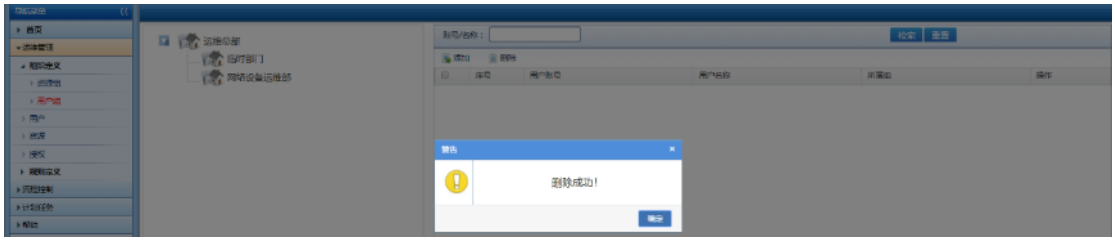
点击运维总部用户组，再点击删除图标  。



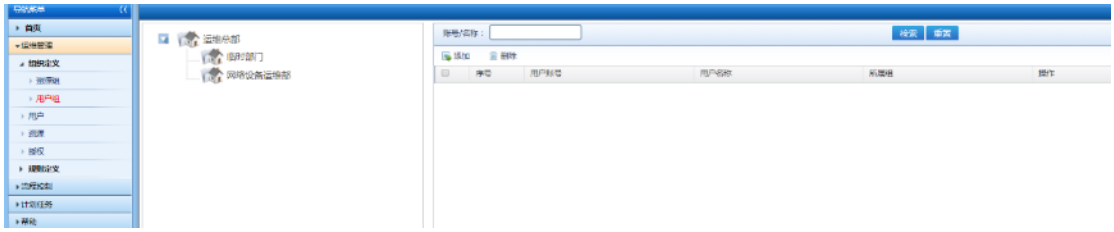
弹出提示信息确认删除用户组运维总部用户组？



点击确定按钮，弹出提示信息删除成功！



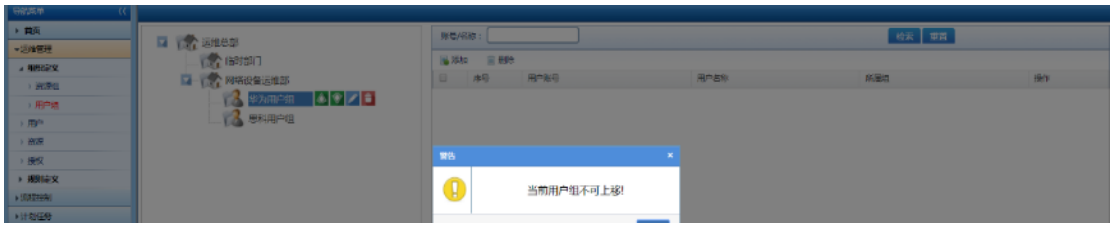
点击确定按钮，返回用户组界面，运维总部下不显示名称为运维总部用户组的用户组，至此用户组删除完成。



1.4.3.4 用户组上移下移

同部门内可通过上移/下移按钮将用户组进行排序，以网络设备运维部下的用户组为例。

点击华为用户组，再点击上移图标  ，弹出告警信息当前用户组不可上移！当用户组已处于其部门的最上方时，不可再进行上移，下移同理。

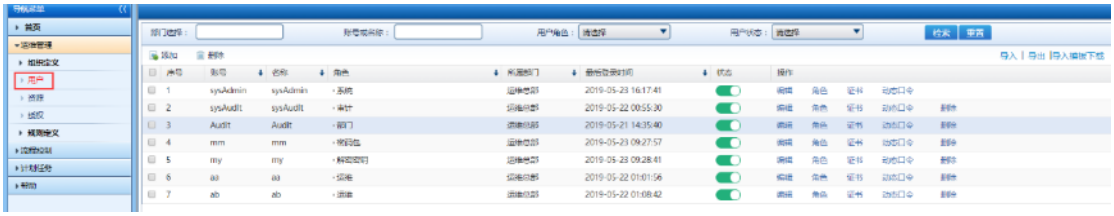


点击华为用户组，再点击下移图标  ，华为用户组则向下移动一位。至此用户组上移/下移完成。

2. 用户

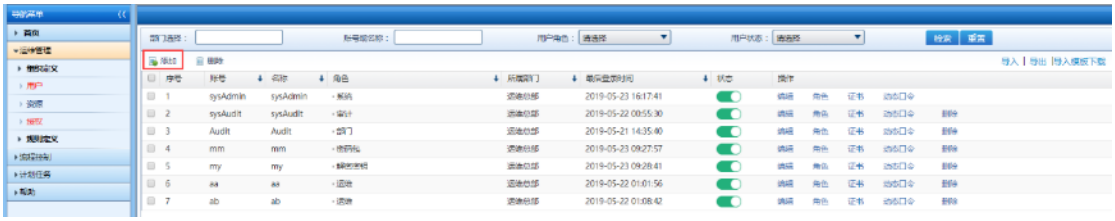
用户模块用于添加、编辑、删除系统的登录账户，设置用户口令、所属部门、电子邮箱、有效期等基本信息，并设置用户的角色信息。

用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击**运维管理->用户**链接进入用户界面。



2.1. 用户添加

用户界面，点击**添加**按钮。



跳转到用户编辑页面，填写用户基本信息：

1) **用户帐号：**Audit
2) **用户名称：**Audit
3) **所属部门：**运维总部
4) **口令：admin@1234，确认口令：admin@1234**

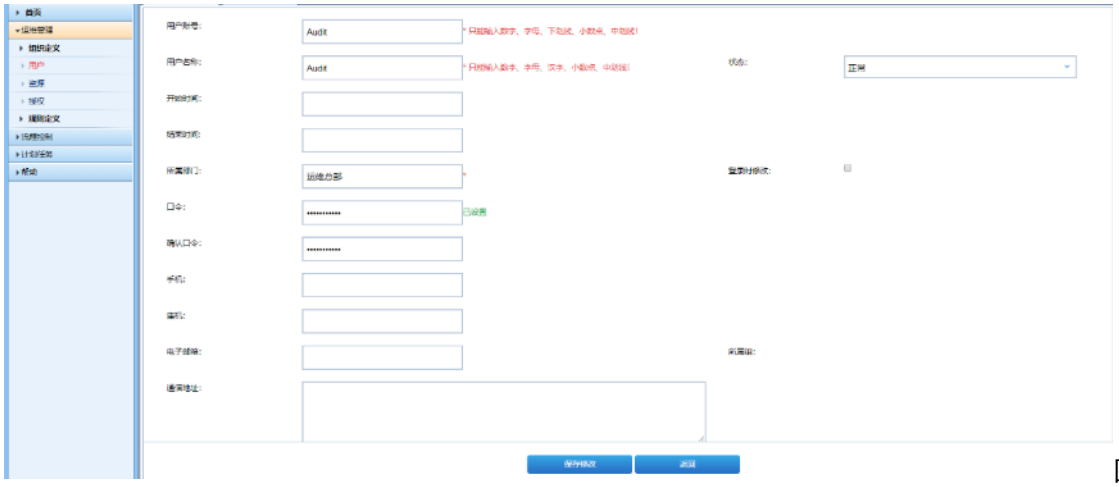
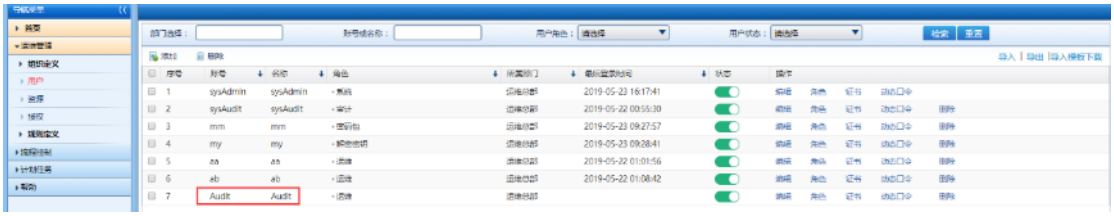


图 1.4.3-1

点击保存提示**保存成功！**

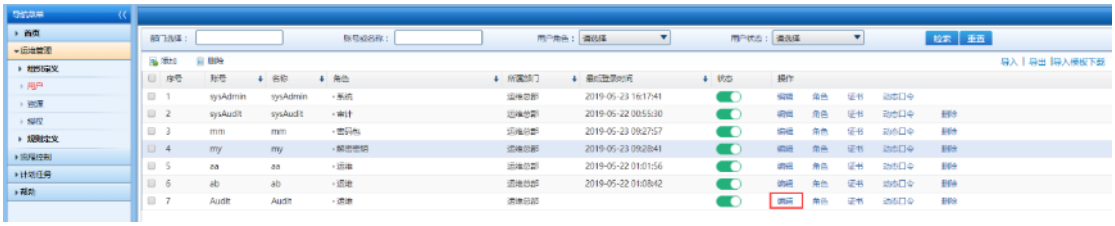
点击弹出框上的**确定**按钮，点击**返回，**页面切换到用户列表页面，列表显示帐号为 **Audit**，名称为 **Audit** 的用户。



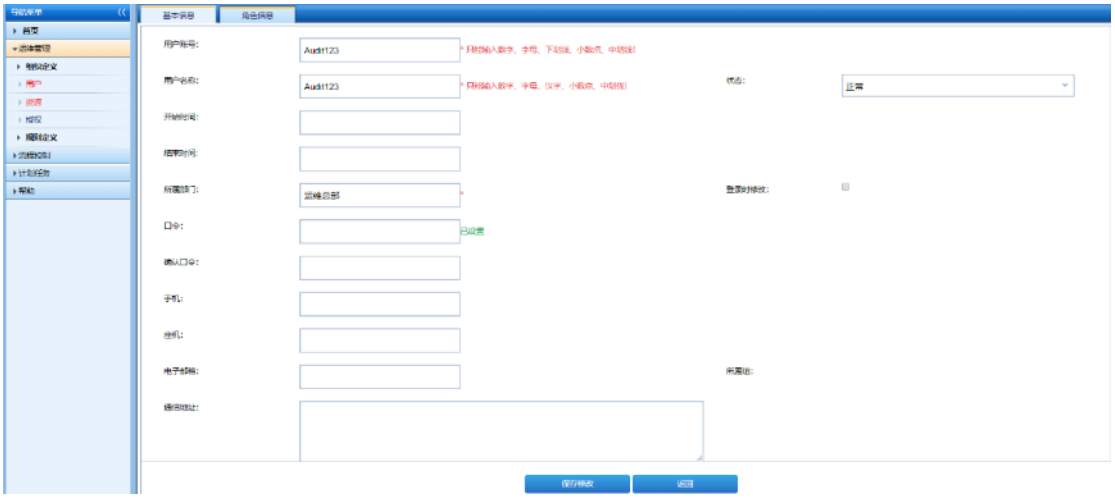
至此添加用户成功。

2.2. 用户修改

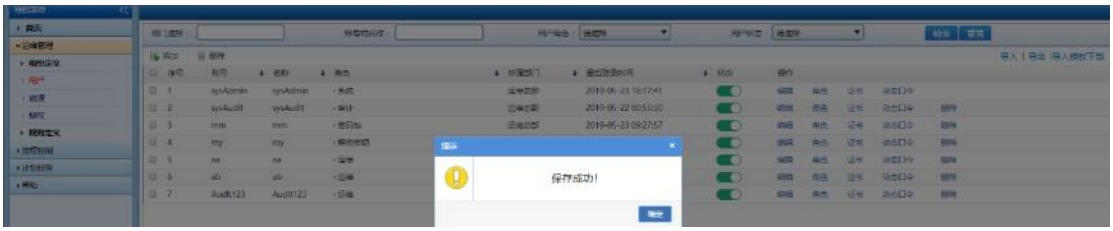
可修改用户的基本属性、口令、用户策略及角色权限，在用户列表页面，点击帐号为 **Audit** 的用户对应的**编辑**。



跳转到用户编辑页面，用户帐号修改为 **Audit123**。



点击**保存**提示**保存成功！**

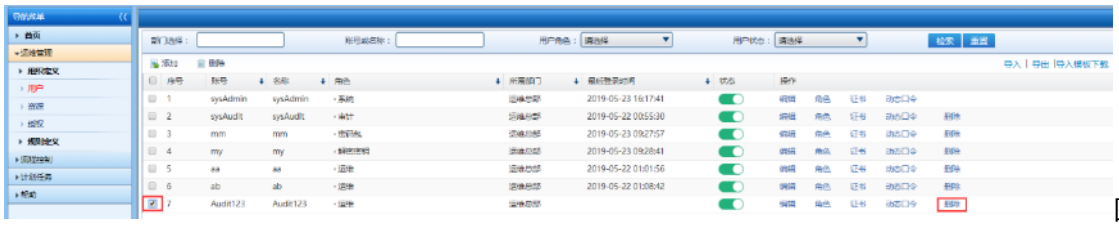


点击弹出框上的**确定**按钮，点击**返回，**页面切换到用户列表页面，列表显示帐号为 **Audit123**，名称为 **Audit123** 的用户。

至此修改用户成功。

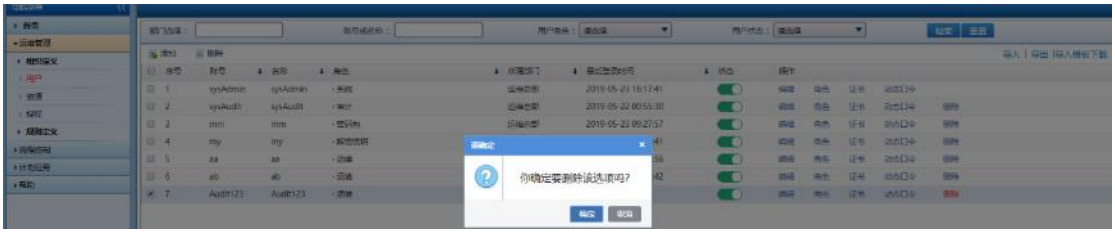
2.3. 用户删除

可对单个账号进行删除，也可一次勾选多个帐号进行删除。以删除单个帐号为例，在用户列表页面，点击帐号为 **Audit123** 的用户对应的**删除**，或者勾选用户 **Audit123**，点击左上方**删除**。

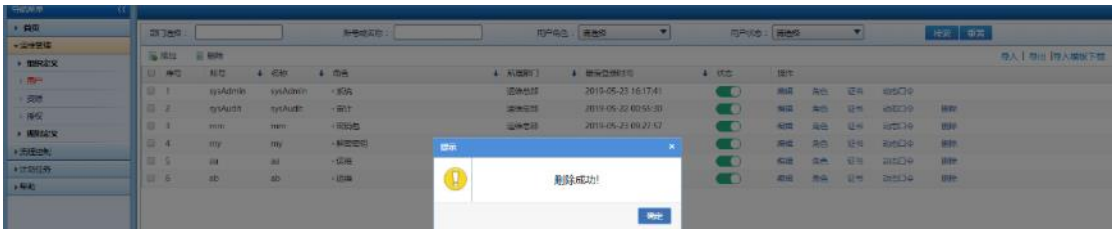


图

弹出提示信息**确定删除该选项吗？**



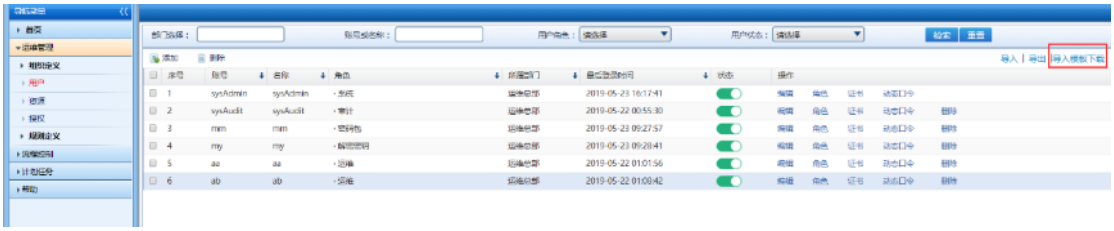
点击**确定**按钮，弹出提示信息**删除成功！**



点击**确定**按钮，返回用户界面，用户列表不显示名称为 **Audit123** 的用户，至此用户删除完成。

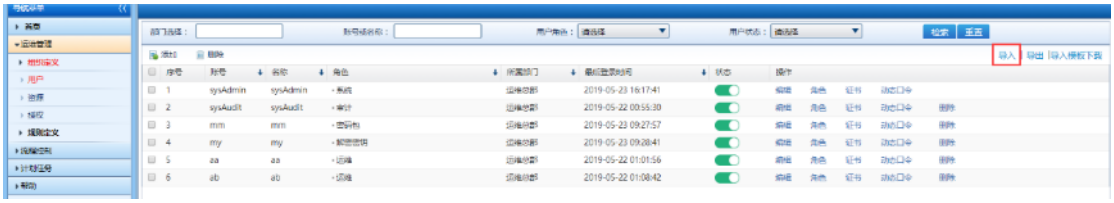
2.4. 用户导入

可进行单个用户的导入，也可进行批量导入。以单个用户的导入为例，点击**运维管理->用户->导入模板下载**，下载用户账号导入模板。

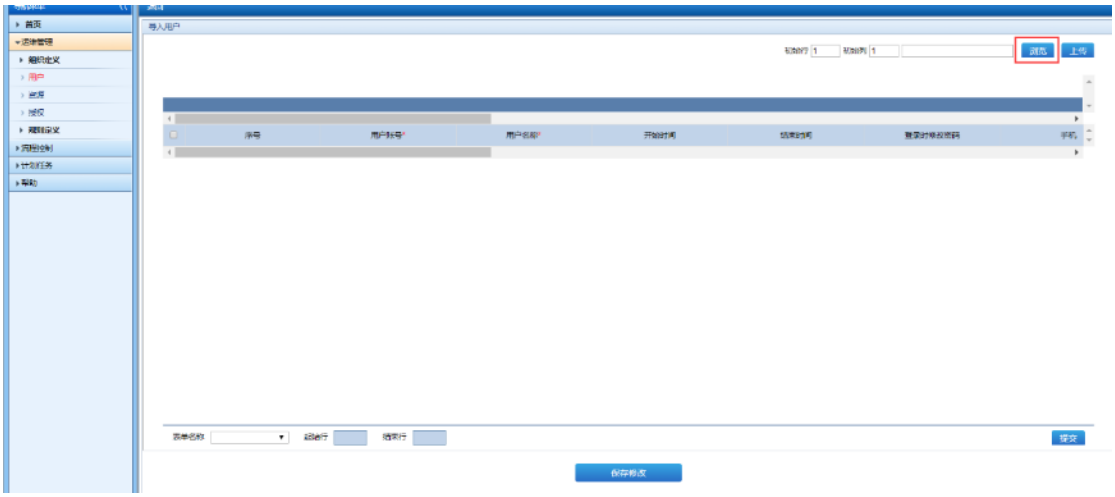


编辑该 XLS 文档，按模板格式填写用户帐号、用户名称、所属部门、角色等信息，并保存。

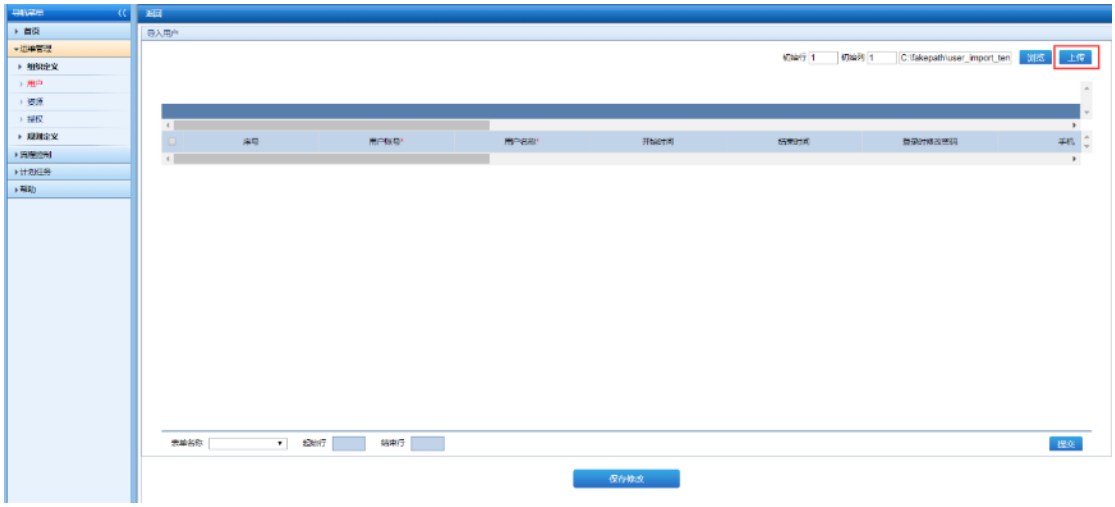
点击**运维管理->用户->导入**。



点击**浏览**，选择按模板编辑的用户表格。



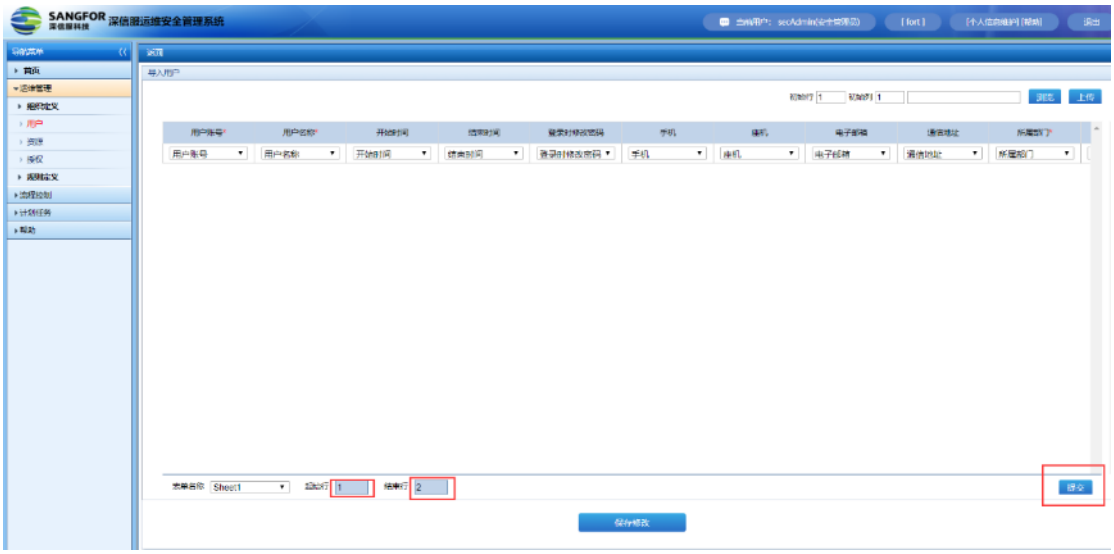
点击**上传**按钮。



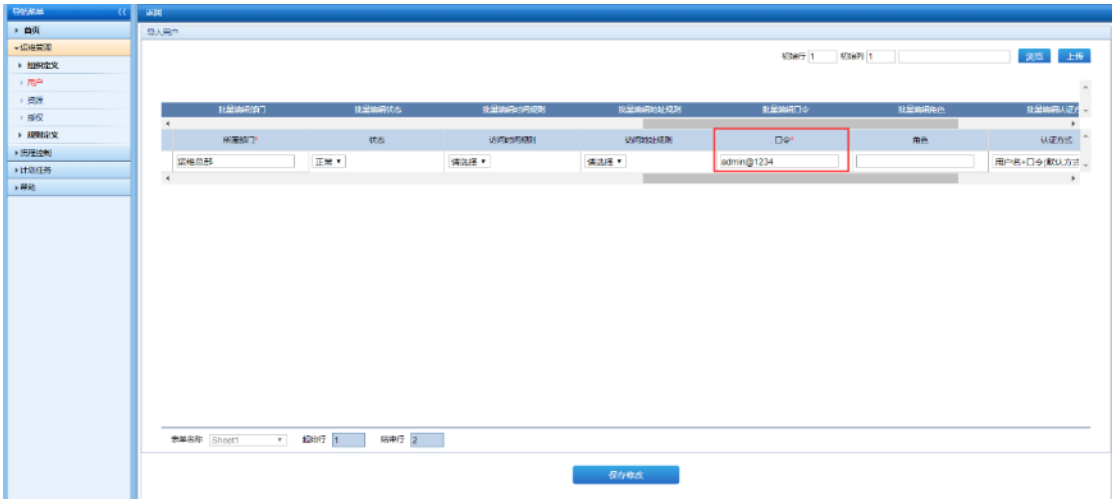
图

1.4.3-5

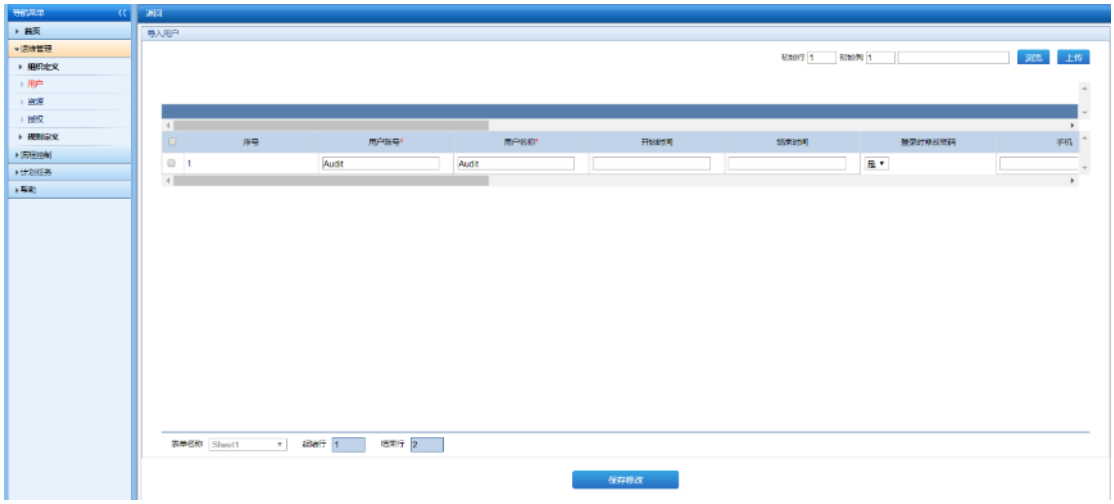
编辑**起始行**和**结束行**，点击**提交**按钮。



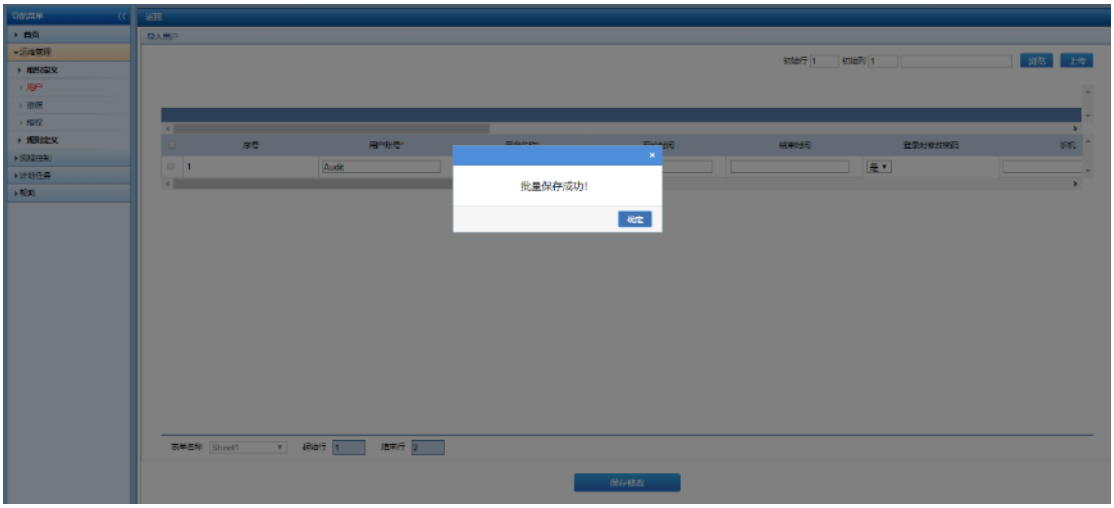
向后拖动滚动条，编辑用户口令。



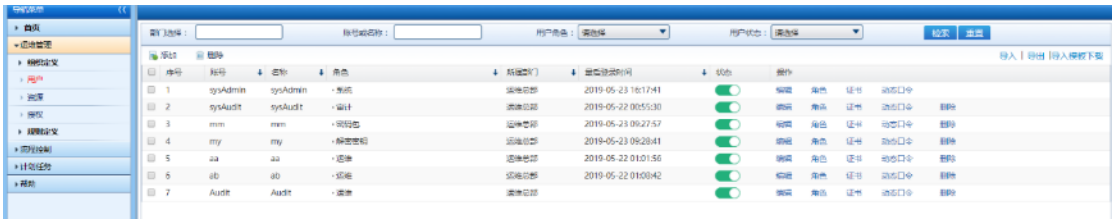
勾选需要保存的用户，点击**保存**按钮。



弹出提示信息**批量保存成功！**



点击弹出框上的**确定**按钮，页面切换到用户列表页面，列表显示帐号为 **Audit**，名称为 **Audit** 的用户。



至此用户导入成功。

2.5. 用户导出

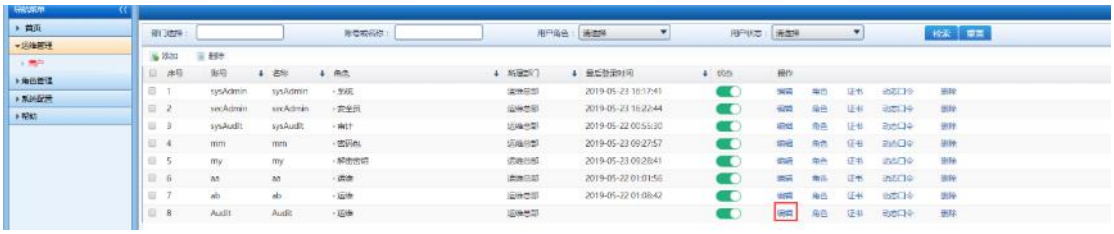
可进行单个用户的导出，也可进行批量导出。以单个用户的导出为例，勾选需要导出的用户，点击**导出**按钮，选择文件路径，即可导出用户基本信息。

在导出文件存储路径，打开导出的表格，即可看到导出的用户信息。

至此用户导出成功。

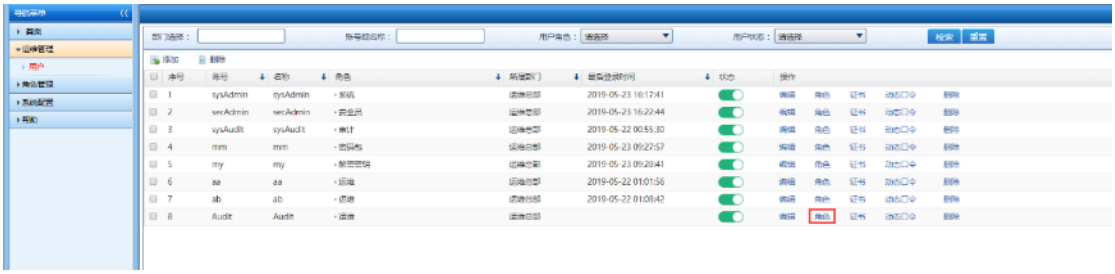
2.6. 用户角色信息

使用 admin 登陆，在运维管理-用户列表页面，点击帐号为 **Audit** 的用户对应的**编辑**。



跳转到用户编辑页面，点击**角色信息**。

或者在用户列表页面，点击帐号为 **Audit** 的用户对应的**角色**。



均可跳转到用户的**角色编辑**页面。

选择左侧列表的**部门管理员**角色，点击**添加**按钮，即可将**部门管理员**角色赋予用户 **Audit**。

点击**保存**提示**保存成功！**

点击弹出框上的**确定**按钮，然后点击**返回，**页面切换到用户列表页面，帐号为 **Audit**，名称为 **Audit** 的用户增加了**部管**（**部门管理员**的简称）角色。

用户 **Audit** 登录系统，切换至**部门管理员**角色，拥有部门管理员的权限。

至此添加用户角色成功。

3. 资源

本章主要介绍云堡垒机资源的配置信息。

3.1. 支持资源类型

支持添加的资源类型如下所示：

- Windows 类型资源（支持 RDP、VNC 等图形协议，FTP 等文件传输协议）
- linux 类型资源（SSH1、SSH2 等字符型协议，SFTP 文件传输协议）
- 网络设备类型资源（telnet 等字符型协议）
- 数据库类型资源
- 应用系统类型资源

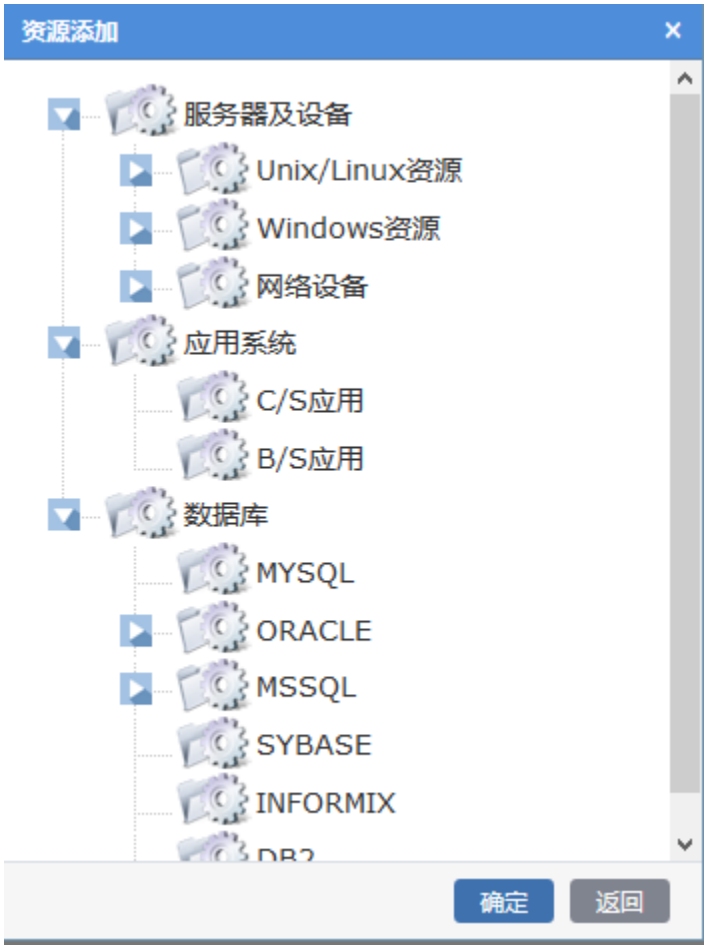
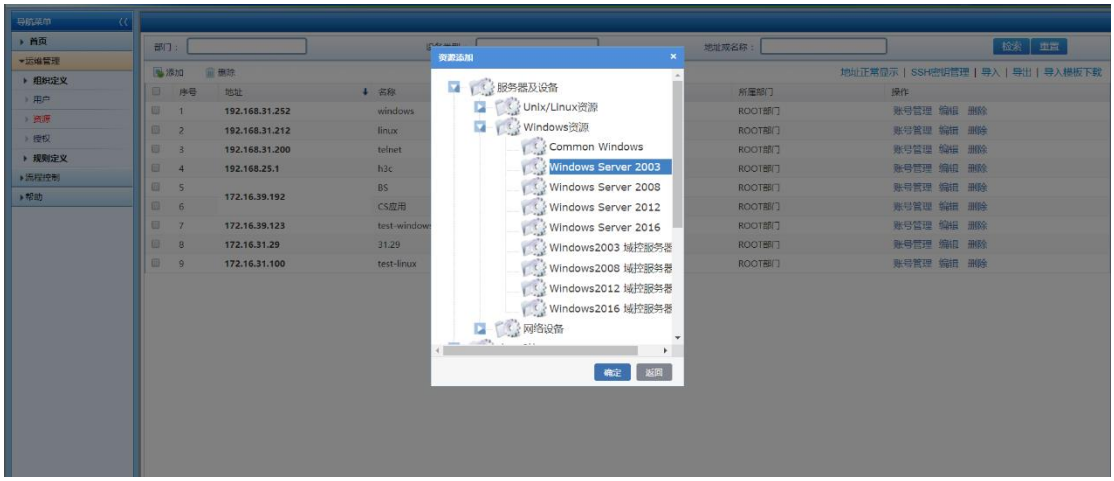


图 3.4.1-1

3.2. 资源添加

3.2.1. Windows 资源

用安全管理员 secAdmin 登录系统，点击运维管理->资源->添加，选择 windows server 2003 类型，点击确定。



填写服务器信息：

1) 名称：windows180
2) IP 地址：172.16.10.180
3) 选择归属部门：运维总部
4) 运维协议：RDP
5) RDP 安全模式：

Windows 资源添加界面的 RDP 安全模式选择，设计目的是根据用户服务器上远程桌面不同的类型设置堡垒机协议代理连接时的选项：

rdp

标准的 RDP 加密。Windows 远程桌面默认值，如果没有做过安全加固默认为此值。

nla

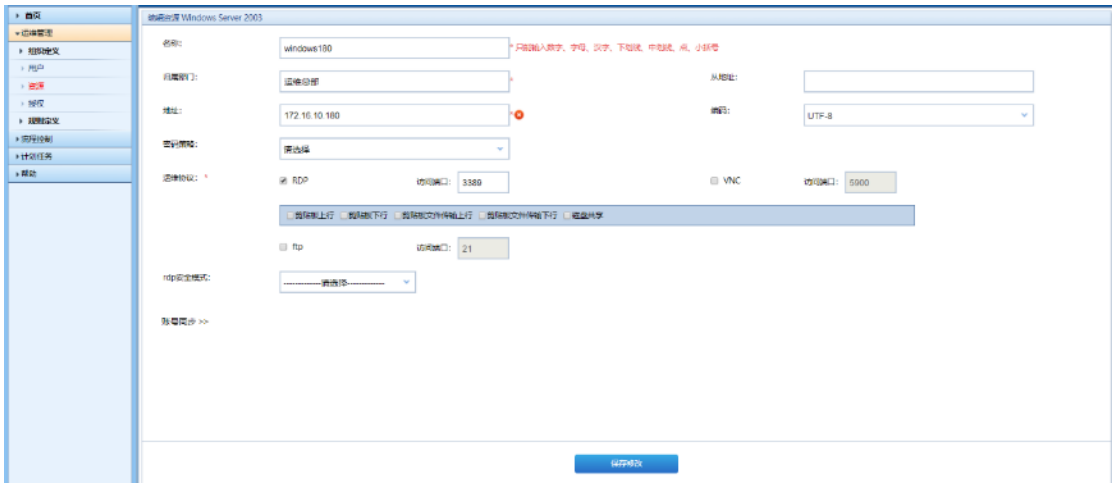
网络级认证。服务开了只需要网络级别身份认证时推荐使用此级别。

tls

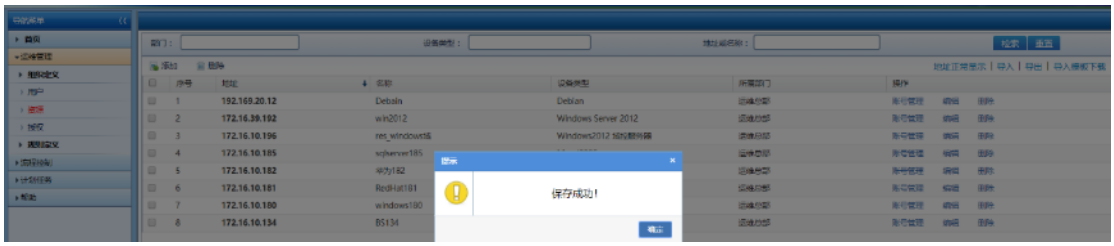
TLS 加密。TLS（传输层安全性）是 SSL 的继承者。服务器设置为此模式时使用。

any

允许服务器选择安全类型。服务器配置为自适应模式时选择此项。



点击保存提示保存成功！

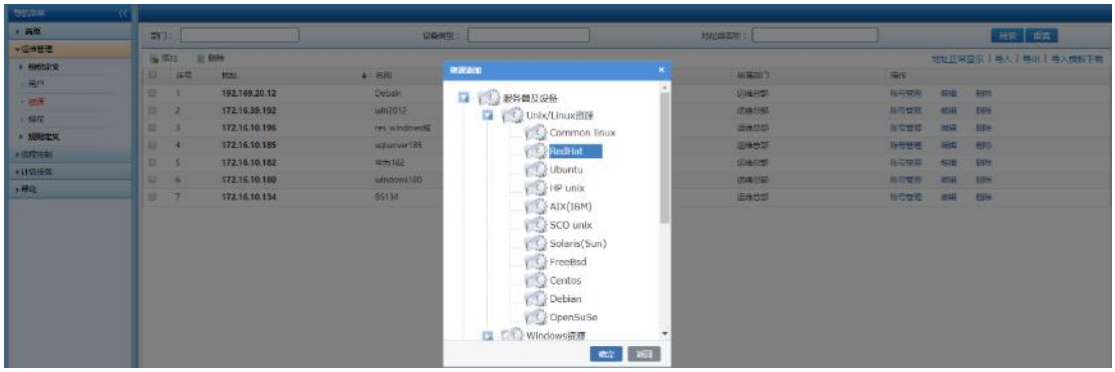


点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，列表显示 IP 为 172.16.10.180、名称为 windows180 的 windows 资源。

至此 windows 类型资源添加成功。

3.2.2. Uinx/Linux 资源

用安全管理员 secAdmin 登录系统，点击运维管理->资源->添加，选择 Unix/Linux 资源下的 RedHat 类型，点击确定。



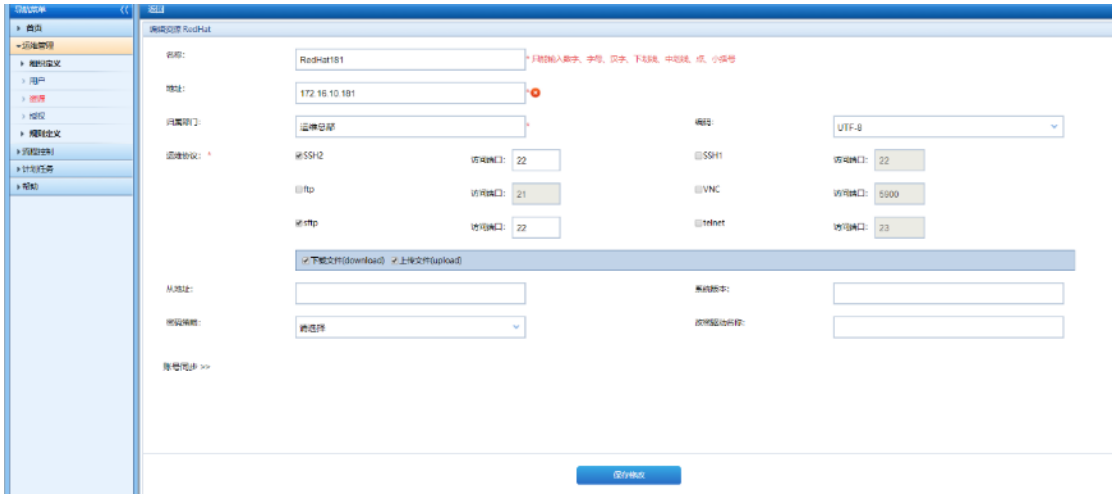
填写服务器信息：

1) 名称：RedHat181

2) IP 地址：172.16.10.181

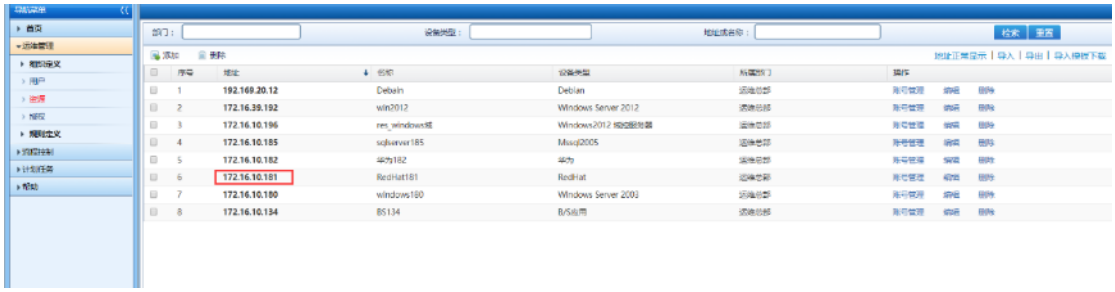
3) 选择归属部门：运维总部

4) 运维协议：SSH2、sftp



点击保存提示保存成功！

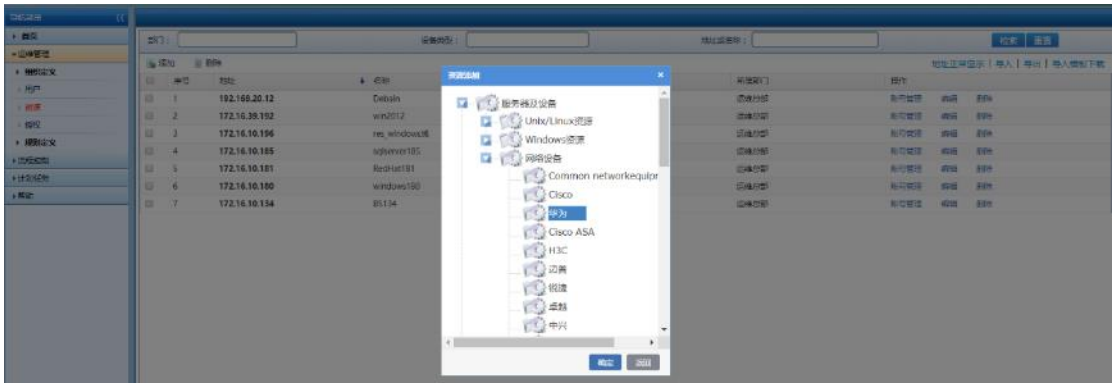
点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，列表显示 IP 为 172.16.10.181、名称为 RedHat181 的 RedHat 资源。



至此 RedHat 类型资源添加成功。

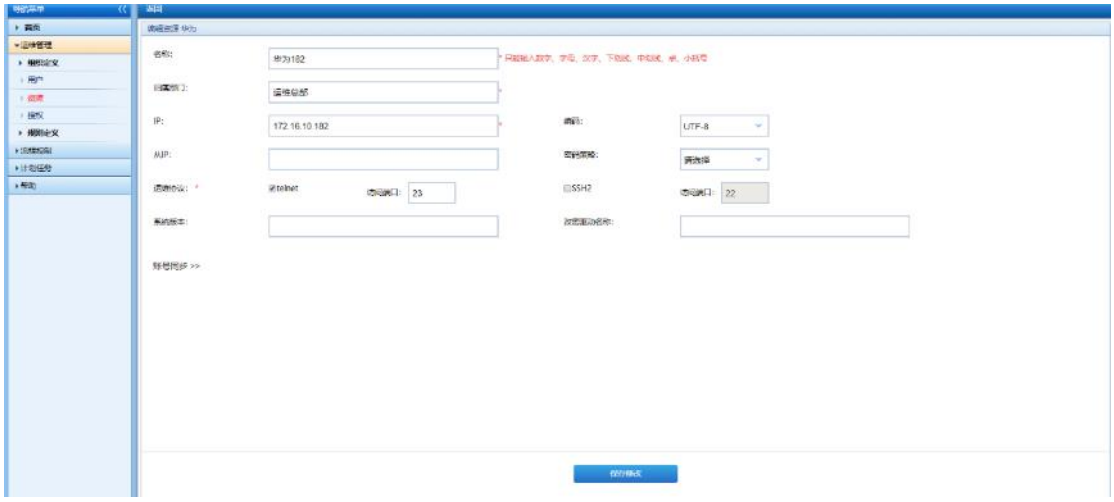
3.2.3. 网络设备

用安全管理员 secAdmin 登录系统，点击运维管理->资源->添加，选择网络设备下的华为类型，点击确定。

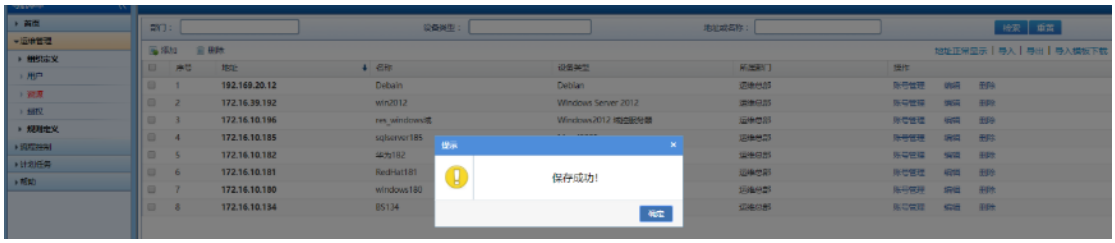


填写服务器信息：

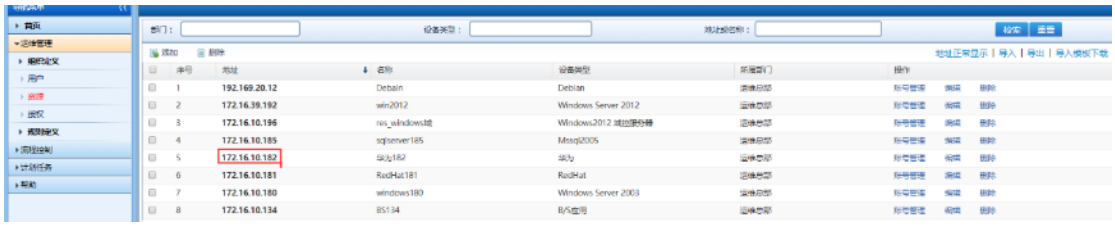
1) 名称：华为 182
2) IP 地址：172.16.10.182
3) 选择归属部门：运维总部
4) 运维协议：telnet/SSH2
5) 系统版本、改密驱动版本为用到交换机自定义脚本改密时填写参数。



点击保存提示保存成功！



点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，列表显示 IP 为 172.16.10.182、名称为华为 182 的华为资源。

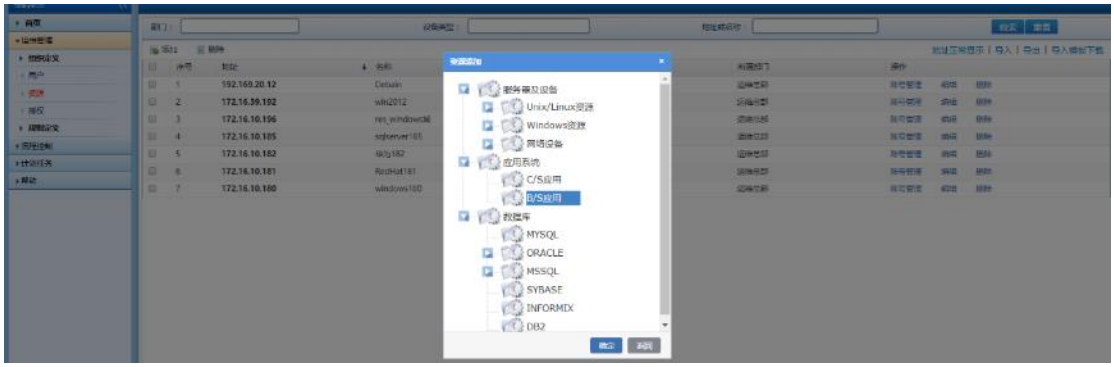


至此网络设备类型资源添加成功。

3.2.4. BS 应用

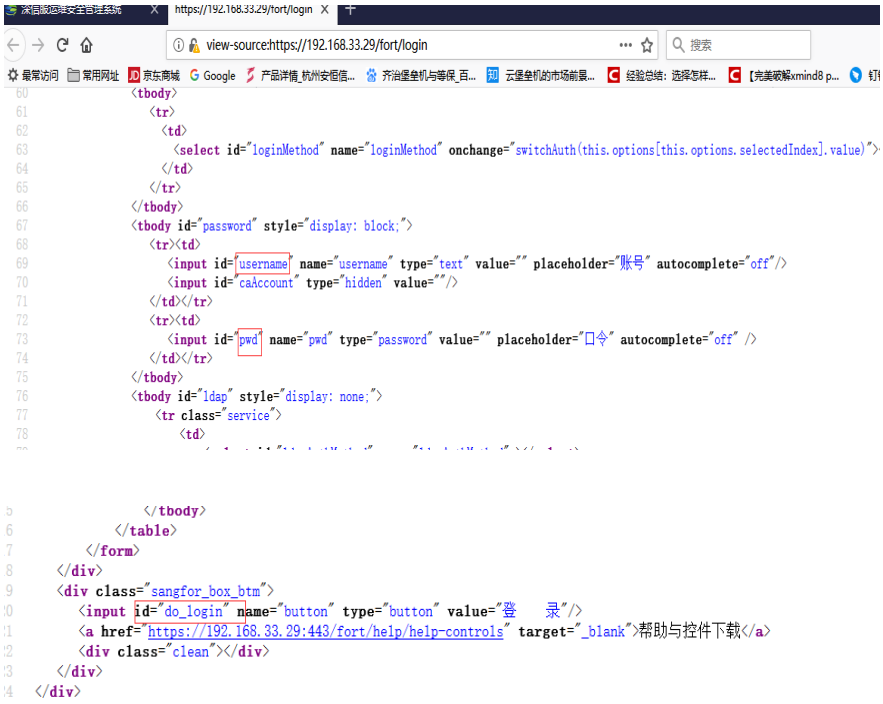
需要使用云堡垒机管理 BS 业务系统时配制。

用安全管理员 secAdmin 登录系统，点击运维管理->资源->添加，选择 BS 类型，点击确定。

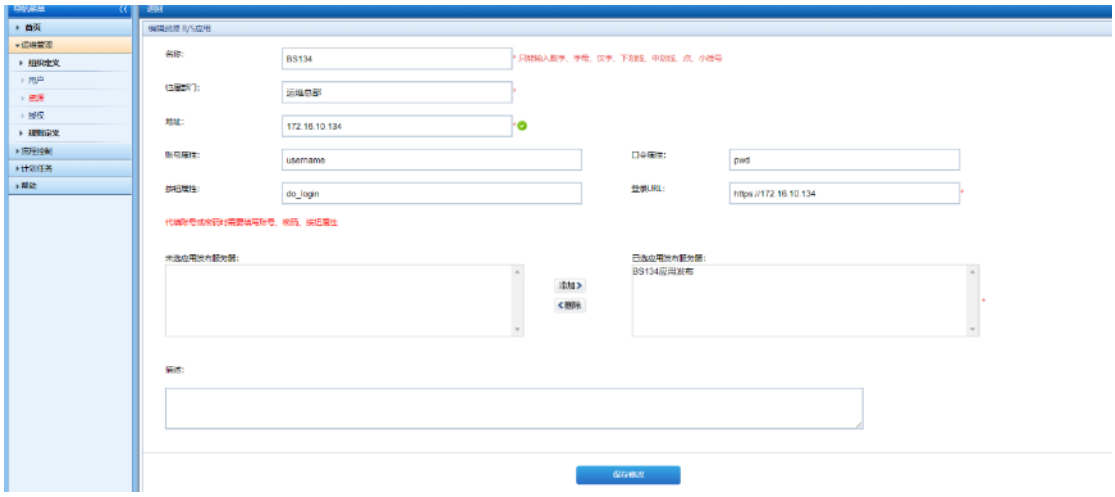


填写服务器信息：

1) 名称：BS134
2) IP 地址：172.16.10.134
3) 选择归属部门：运维总部
4) 登陆 URL：https://172.16.10.134
5) 选择对应的应用发布服务器
6) 账号属性、口令属性以及按钮属性仅在需要代填 BS 应用系统的账号密码时填写，可在打开 URL 登陆页面后右键查看源文件或者使用 F12 查看器获取对应的属性名称，例如云堡垒机的对应属性为：



获取属性后填写如下：



点击保存提示保存成功！

点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，列表显示 IP 为 172.16.10.134、名称为 BS134 的 BS 资源。

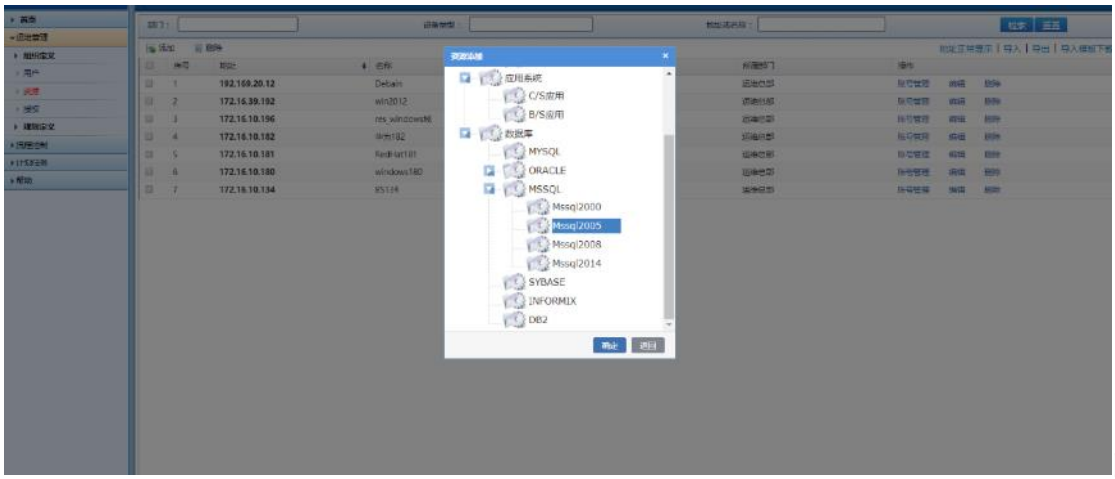
至此 BS 类型资源添加成功。

3.2.5. 数据库和 CS 应用

需要使用云堡垒机管理数据库或 CS 业务系统时配制，需要将数据库或 CS 业务系统的客户端安

装到应用发布服务器上并设定相关客户端配置配合调用/ 代填等操作，系统内置了常用数据库应用的默认客户端配置。

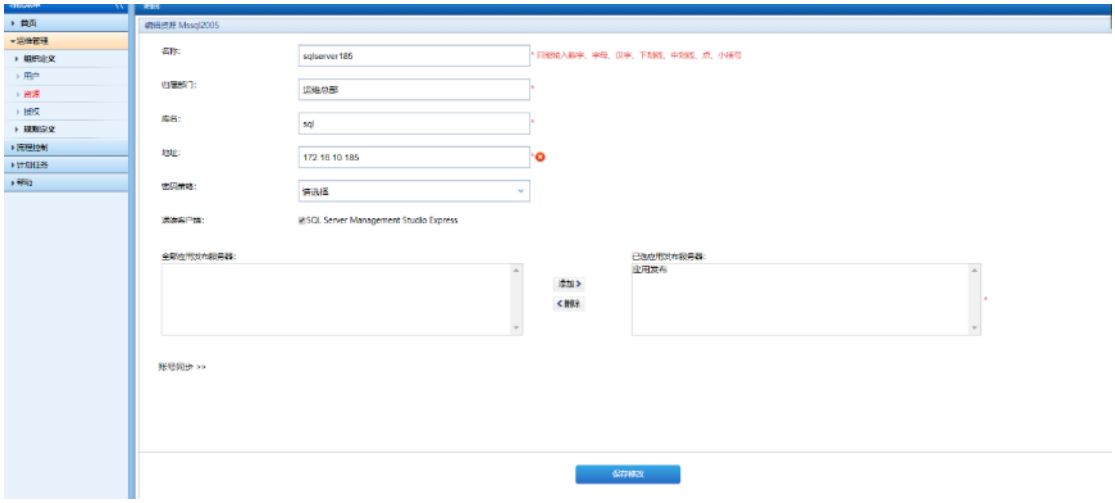
用安全管理员 secAdmin 登录系统，点击运维管理->资源->添加，选择数据库类型下的 Mssql2005 类型，点击确定。



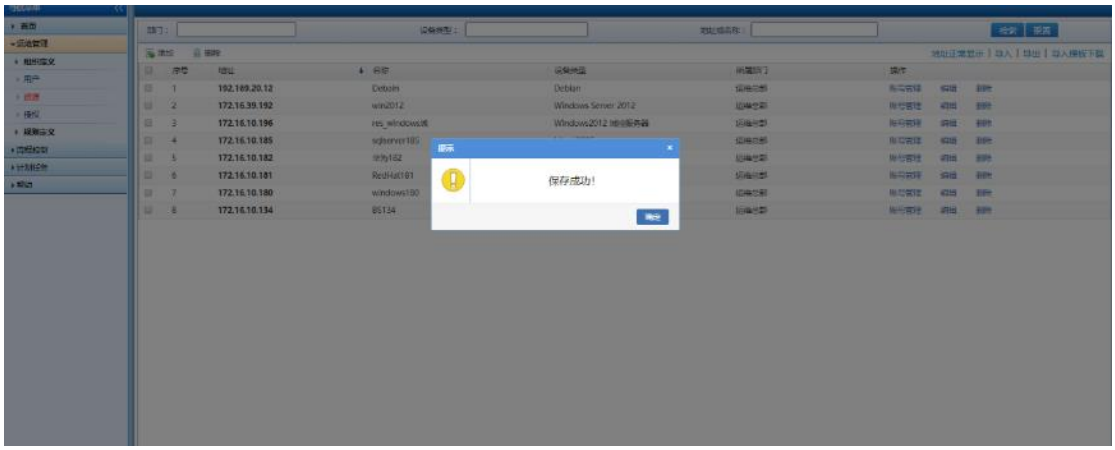
图

填写服务器信息：

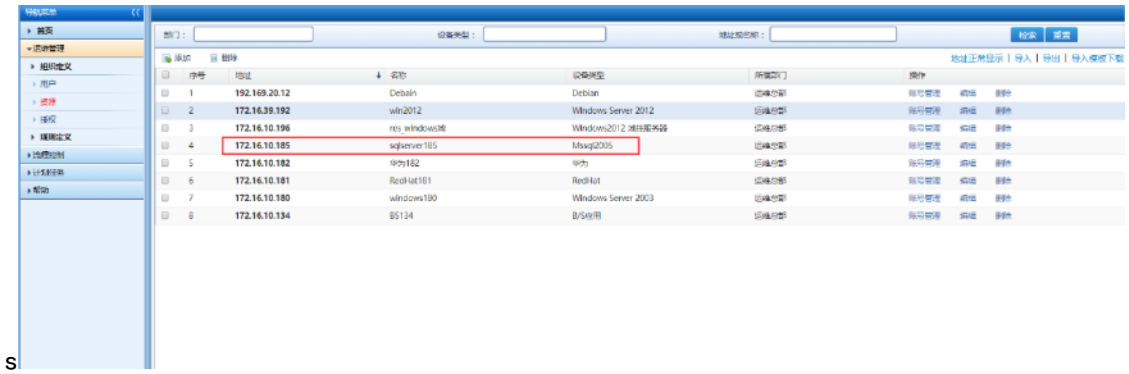
1) 名称：sqlserver185
2) IP 地址：172.16.10.185
3) 选择归属部门：运维总部
4) 库名：sql（需要访问的数据库名）
5) 运维客户端：选择默认的 SQL Server Management Studio Express
6) 选择应用发布



点击保存提示保存成功！



点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，列表显示 IP 为 172.16.10.185、名称为 sqlserver185 的 Mssql2005 资源。

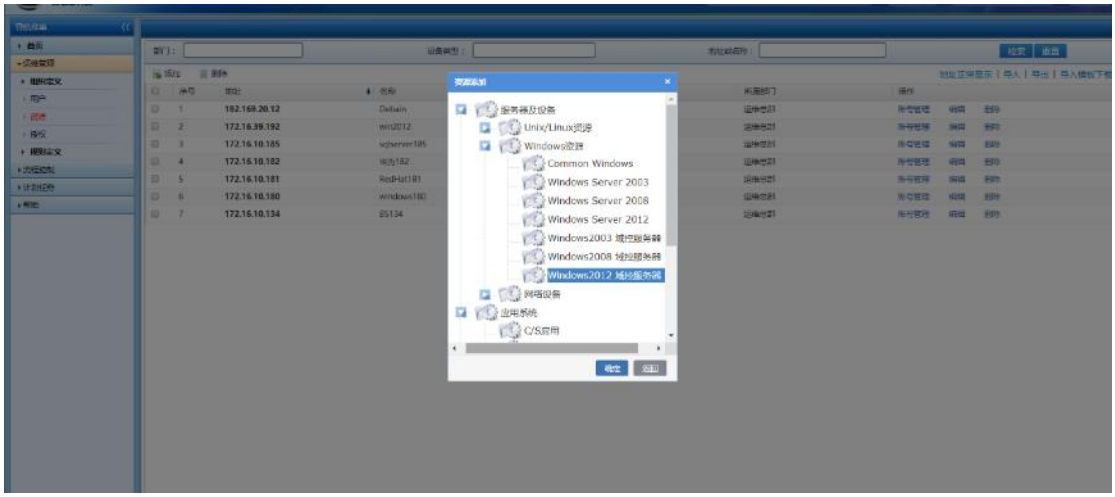


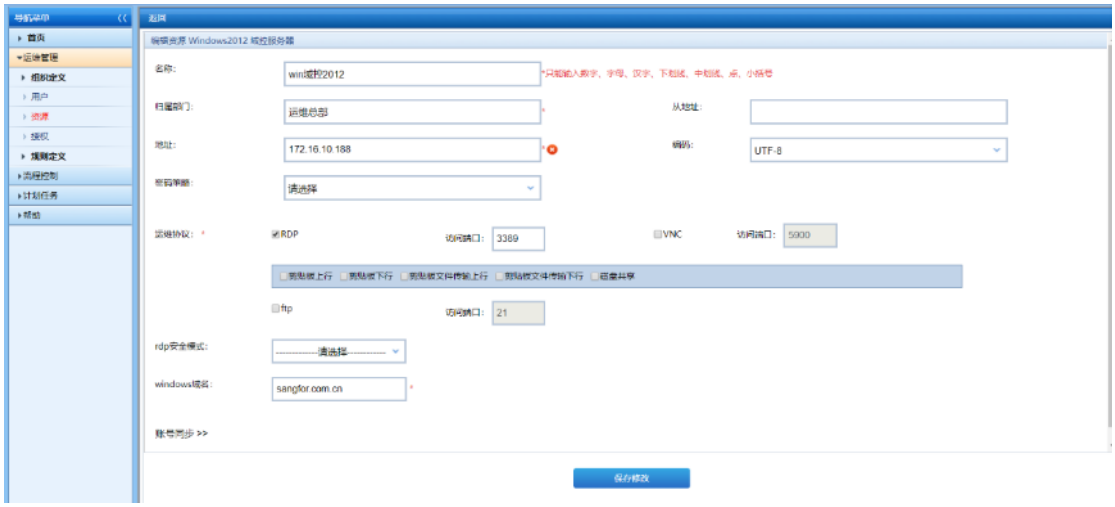
S

至此数据库类型资源添加成功。

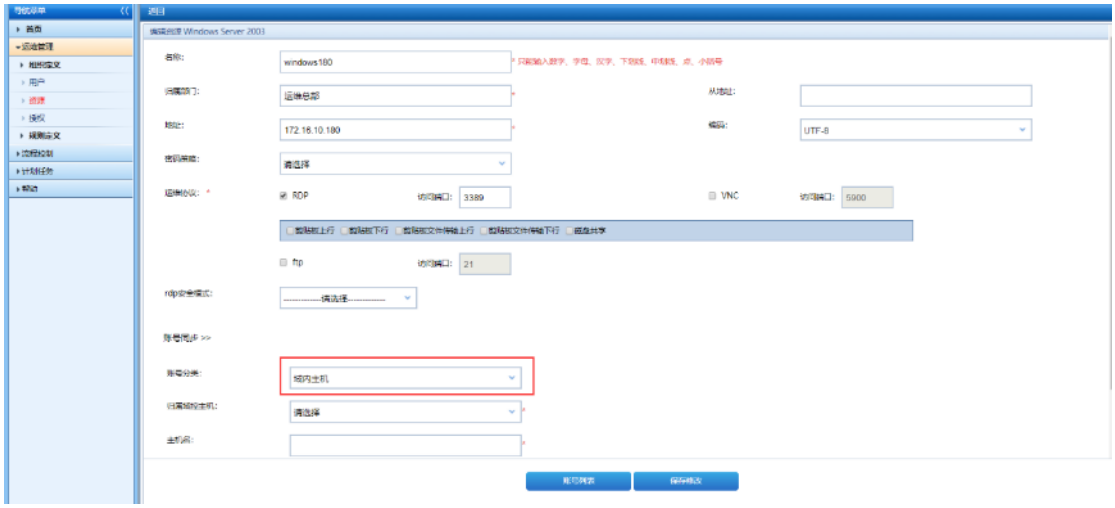
3.2.6. Windows 域内资源

在用户需要使用域环境的管理目标 windows 服务器时使用，添加域内主机之前需要先添加对应的域控服务，切换为域内主机后需要选择所属的域控服务器。

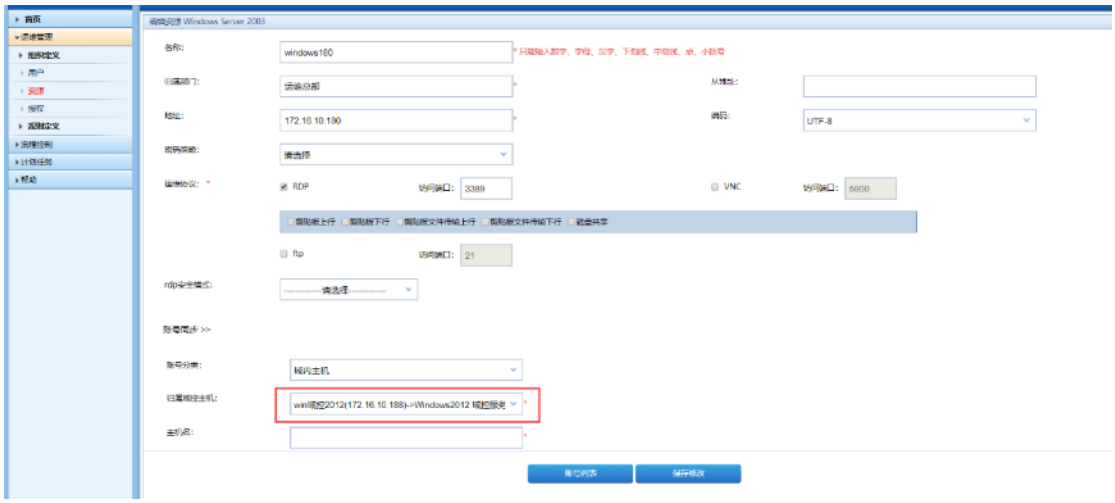




添加域内的 windows 资源时资源类型需要选择普通 windows 类型（Windows Server 2003、Windows Server 2008、Windows Server 2012），添加后切换为域内主机。



切换后选择对应域控：



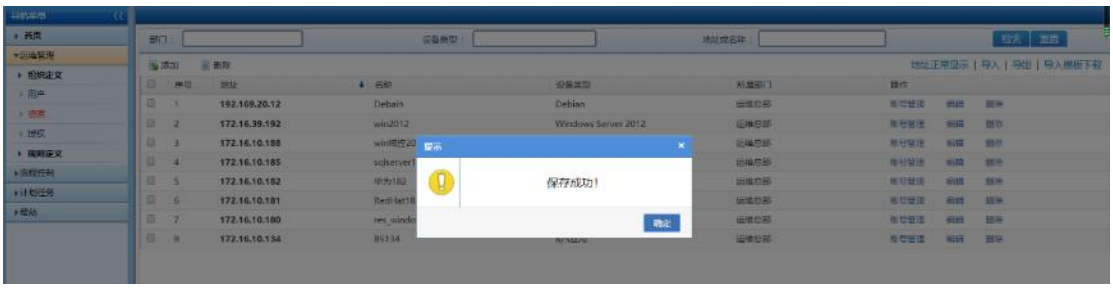
至此 Windows 域内类型资源添加成功。

3.3. 资源修改

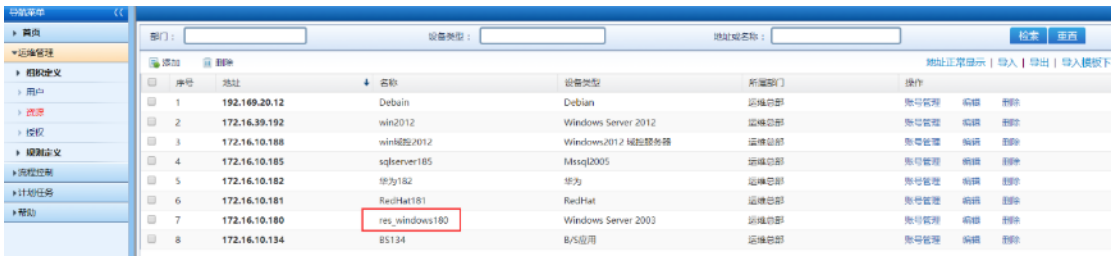
点击运维管理->资源，进入资源列表页面。点击资源 windows180 后面对应的编辑。

修改资源名称为 res_windows180。

点击保存，提示保存成功！



点击弹出框上的确定按钮，点击资源，页面切换到资源列表页面，IP 为 172.16.10.180 的 windows180 的资源名称显示为 res_windows180。



至此 windows 类型资源修改成功。

3.4. 资源删除

资源删除用于删除废弃的资源。可对单个资源进行删除，也可一次勾选多个资源进行删除。

点击运维管理->资源，进入资源列表页面。勾选资源名称为 res_windows180 的资源。

点击删除，弹出如下图所示提示。

图 3.4.4-2

点击弹窗框的确定，提示删除成功。

图

点击弹出框上的确定按钮，页面切换到资源列表页面，列表中不显示 ip 为 172.16.10.180 的 res_windows180 资源。

至此 windows 类型资源删除成功。

3.5. 资源导入

资源导入提供了 2 种方式：

- 明文文件导入（xls 格式，系统下载的导入模板，或从系统中导出的 xls 文件详见详见章节 3.4.6.1.只导出资源）
- 密文文件导入（raot 格式，从系统中导出的文件，不能编辑修改，导出方式详见章节 3.4.6.3.导出资源+资源账号+资源账号密码）

3.5.1. 明文文件导入

点击运维管理->资源->导入模板下载，下载资源导入模板（或从系统中导出的 xls 文件）。

编辑该 XLS 文档，按模板格式添加 windows 资源。

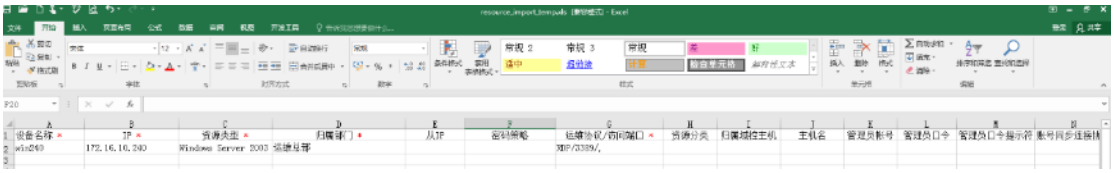
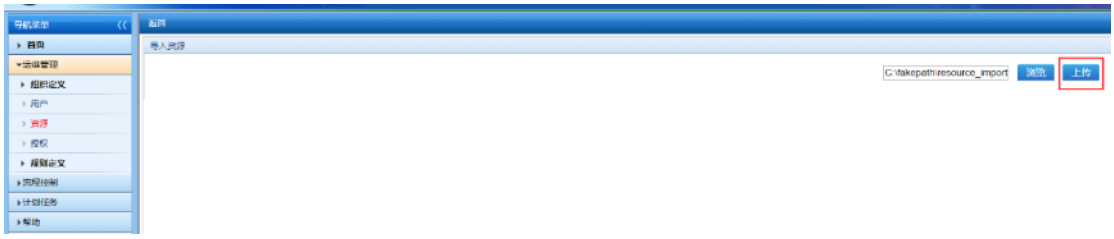


图 3.4.5.1-2

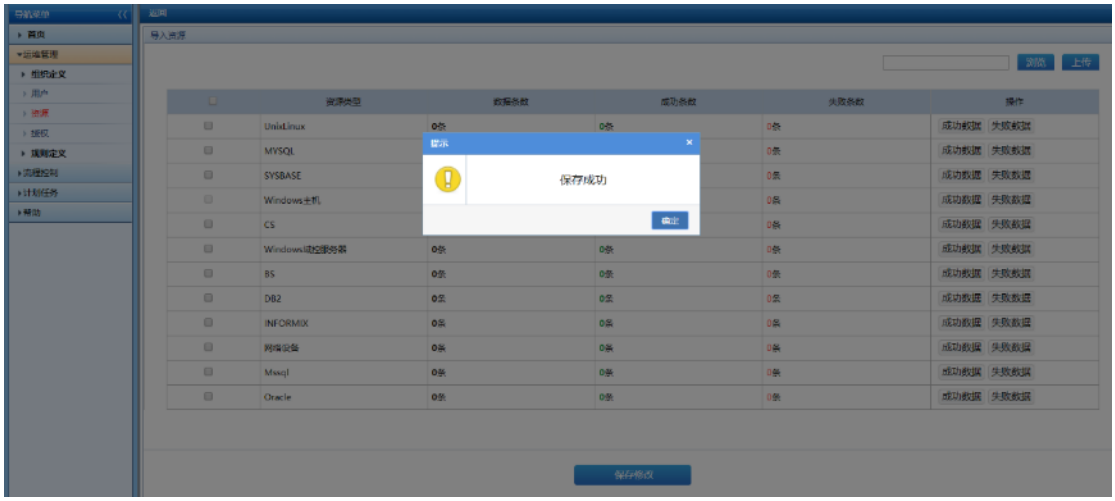
准备好导入文件后，点击运维管理->资源->导入。

点击浏览，选择文件，点击上传按钮。



勾选 windows 主机资源类型，点击保存。

点击保存之后，提示保存成功。

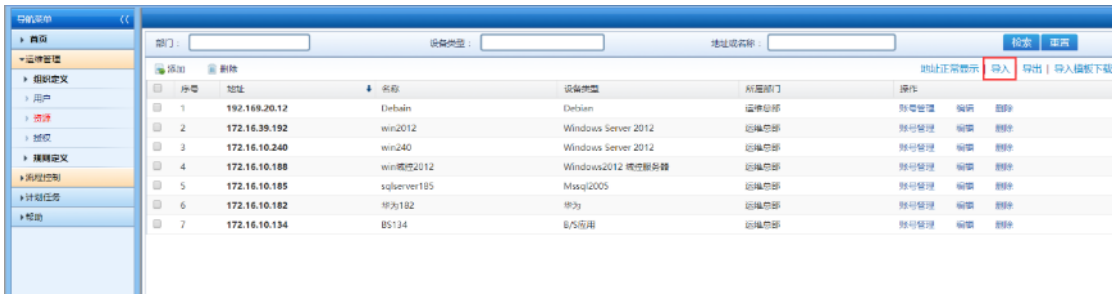


点击弹出框上的确定，然后点击页面左边的资源按钮，跳转到资源列表页面，列表中显示导入的 windows 资源。

3.5.2. 密文文件导入

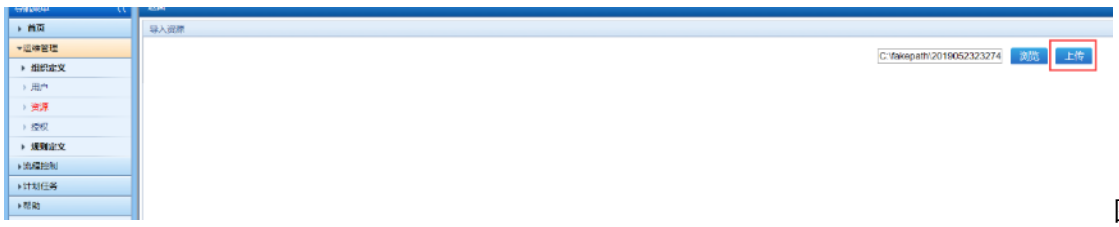
系统中导出的 raot 格式文件，不能编辑修改，可直接导入。

点击运维管理->资源->导入。



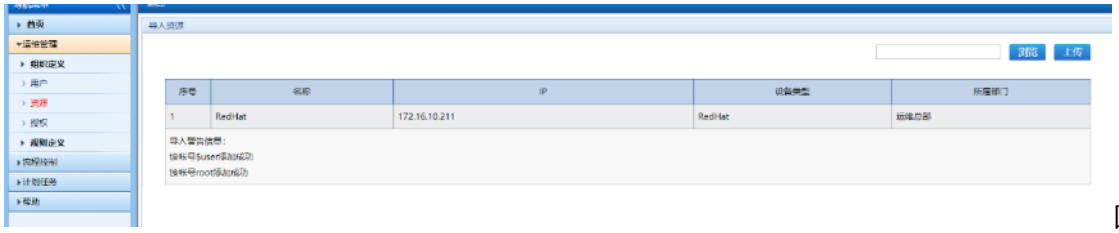
图

点击浏览，选择文件，点击上传按钮。



图

资源导入成功，可查看导入警告信息。



图

然后点击页面右下角的返回按钮，跳转到资源列表页面，列表中显示导入的资源。


图

至此资源的导入完成，资源导入提高了添加效率，实现了资源的批量添加。

3.6. 资源导出

资源导出提供了 3 种方式：

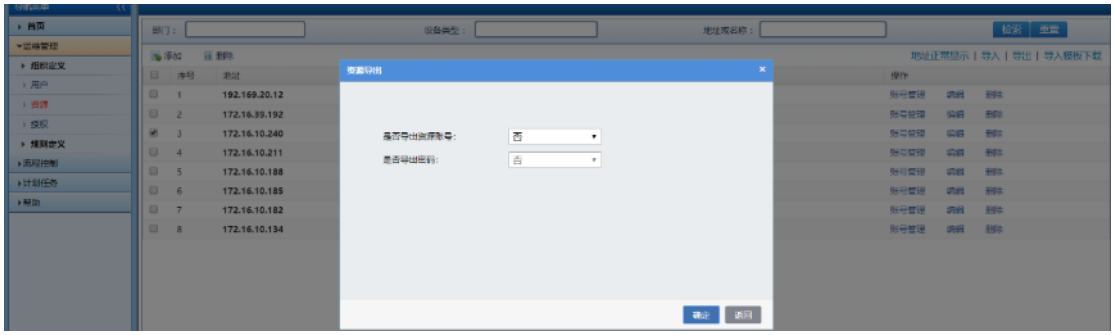
- 只导出资源（xls 格式）
- 导出资源+资源账号（xls 格式）
- 导出资源+资源账号+资源账号密码（raot 格式，不能编辑修改）

3.6.1. 只导出资源

将选中的设备资源以 xls 格式备份，导出的文件方便用户对资源信息的阅读、保存，极大的方便了资源数据的恢复。

点击运维管理->资源，勾选 win240 资源，点击导出。

点击导出之后，弹出以下页面，是否导出资源账号选择否，点击确定按钮，选择存储路径即可导出资源基本信息。

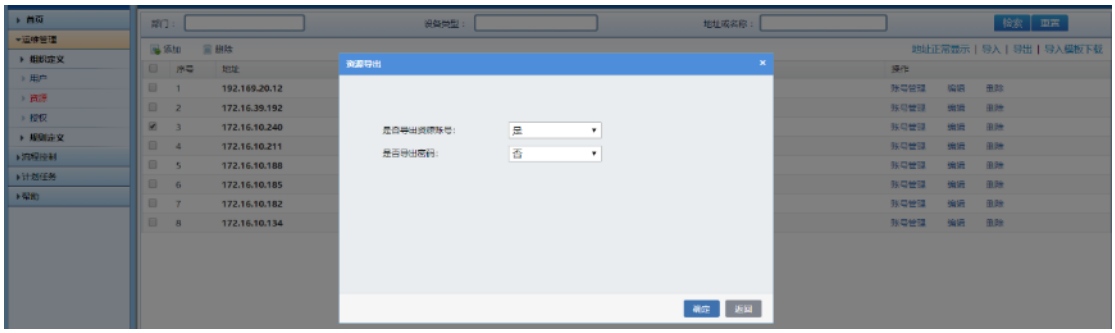


在存储路径下找到导出的xls文件resource_temp.xls，打开该文件即可查看导出的资源信息，至此资源导出成功。

3.6.2. 导出资源+资源账号

点击运维管理->资源，勾选 win240 资源，点击导出。

点击导出之后，弹出以下页面，是否导出资源账号选择是，是否导出密码选择否，点击确定按钮，选择存储路径即可导出资源+资源账号信息。



在存储路径下找到导出的xls文件resource_temp.xls，打开该文件即可查看导出的资源信息，

包含资源账号信息，至此资源+资源账号导出成功。

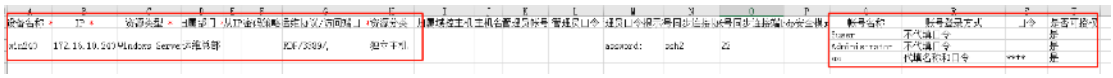
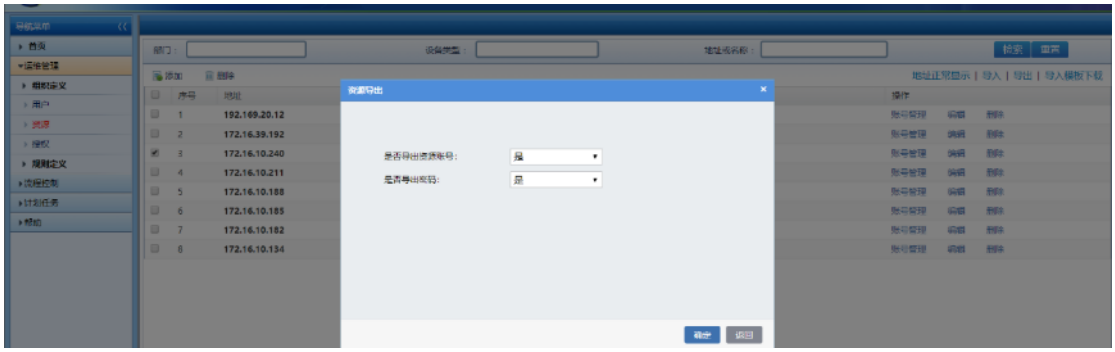


图 3.4.6.2-3

3.6.3. 导出资源+资源账号+资源账号密码

点击运维管理->资源，勾选 win240 资源，点击导出。

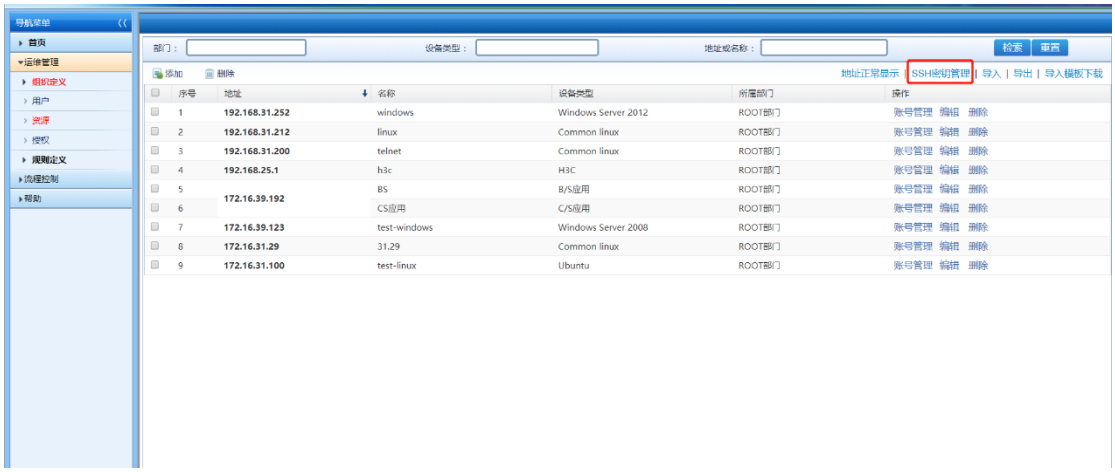
点击导出之后，弹出以下页面，是否导出资源账号选择是，是否导出密码选择是，点击确定按钮，选择存储路径即可导出资源+资源账号+资源密码。



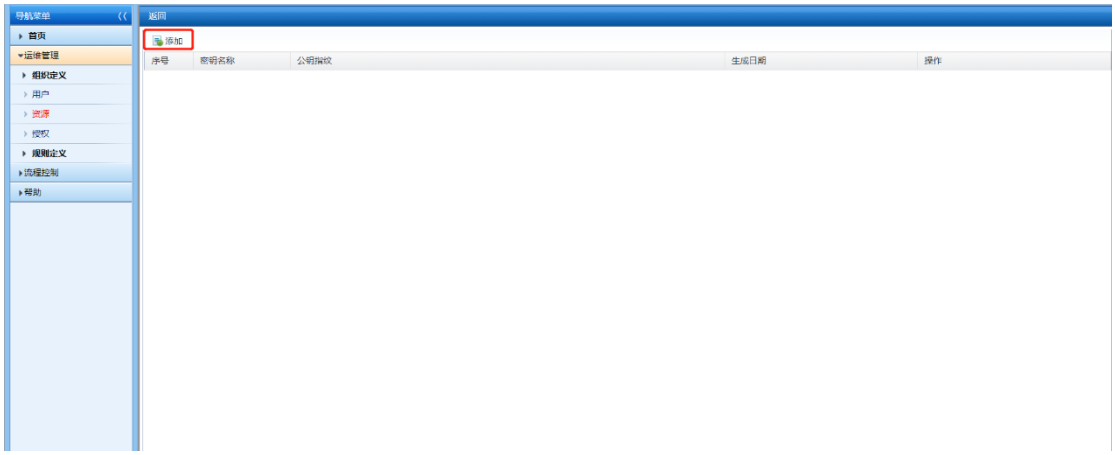
在存储路径下找到导出的 roat 文件 20190523232743039_RESOUCEACCOUNT_1000.raot ，包含资源账号及资源账号密码信息，不能编辑修改，只能导出导入，方便备份资源数据，至此资源+资源账号+资源账号密码导出成功。

3.7. SSH 密钥管理

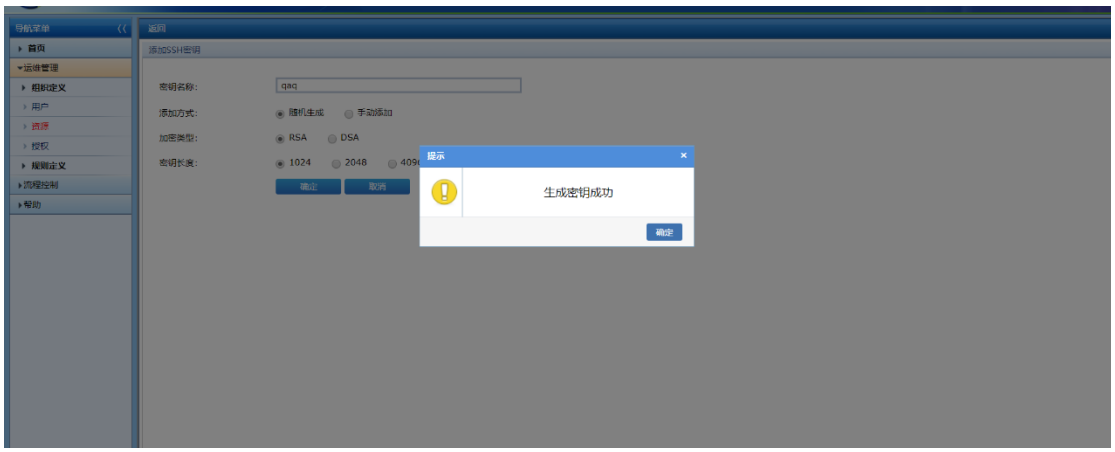
点击运维管理->资源，点击 SSH 密钥管理



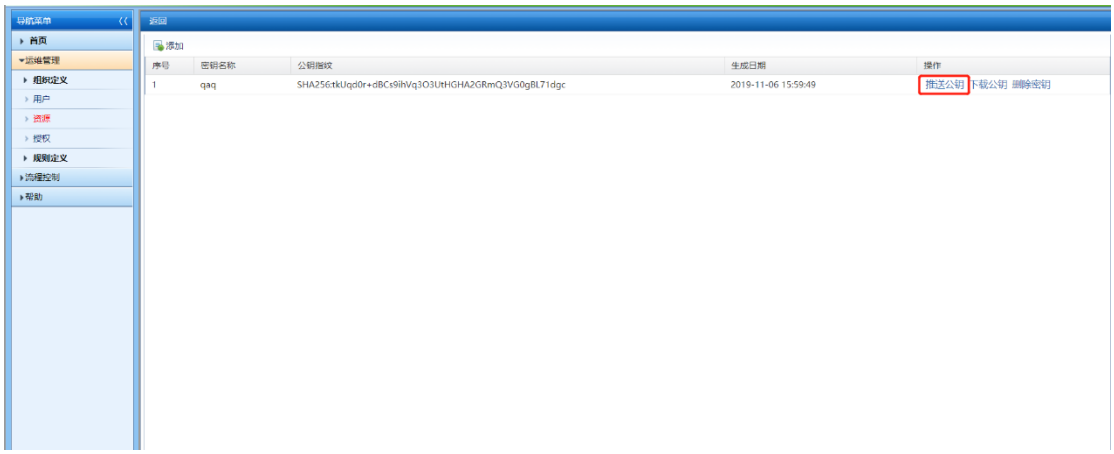
点击添加按钮，进入到添加 SSH 密钥界面



填写密钥名称，添加方式：随机生成，加密类型：RSA，密钥长度：1024，点击确定生成密钥，提示生成密钥成功

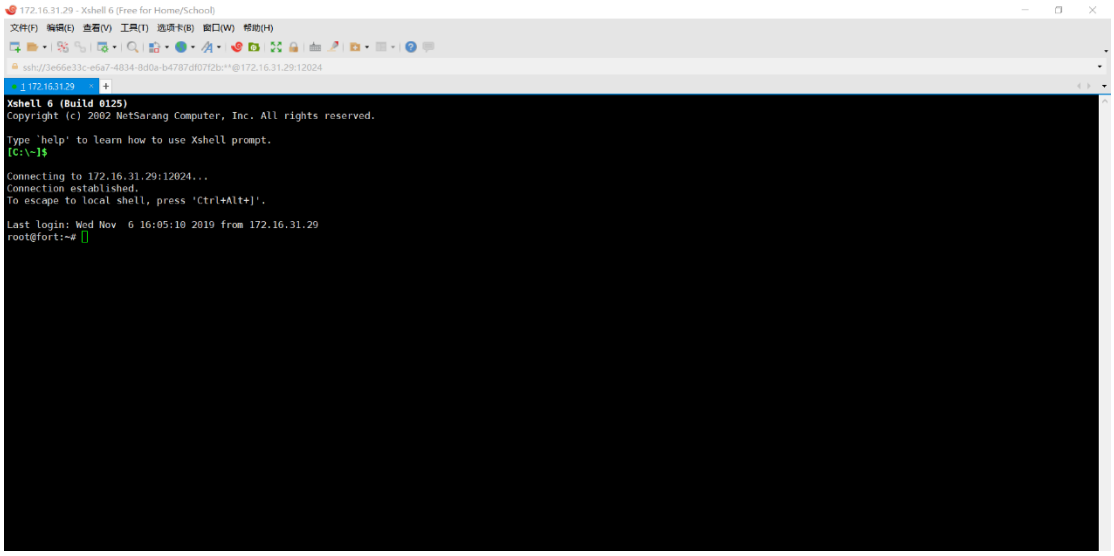


查看已生成的公钥，点击推送公钥进入推送界面



选择需要推送的服务器，点击推送公钥，提示推送成功

使用运维管理员登陆资源，资源登陆成功



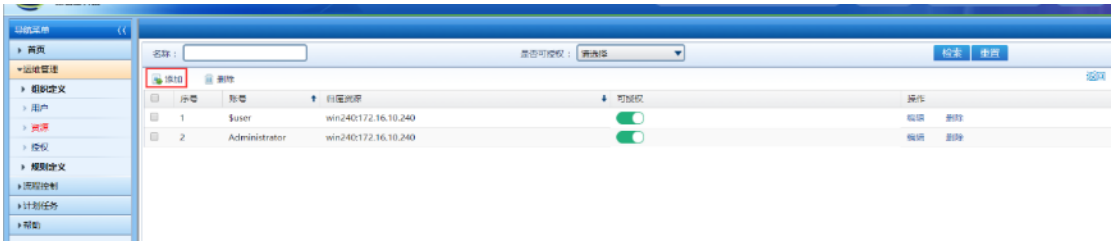
4. 资源账号

资源账号就是目标服务器的登录账号，本章针对账号的基本操作进行详细的介绍。

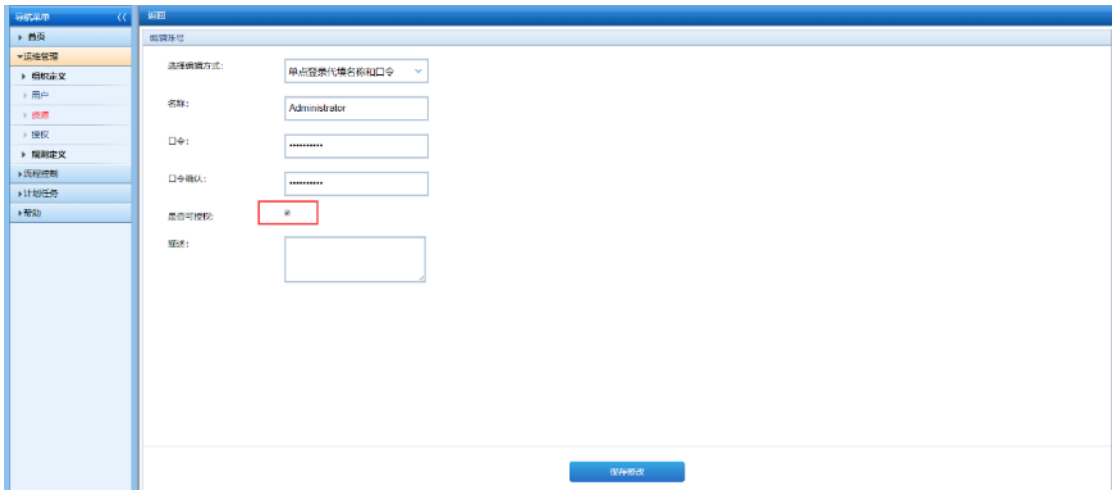
4.1. 资源账号添加

用安全管理员 secAdmin 登录系统，点击**运维管理**->**资源**，点击资源名称为 win240 对应的**账号管理**。

进入账号编辑页面，点击**添加**按钮。

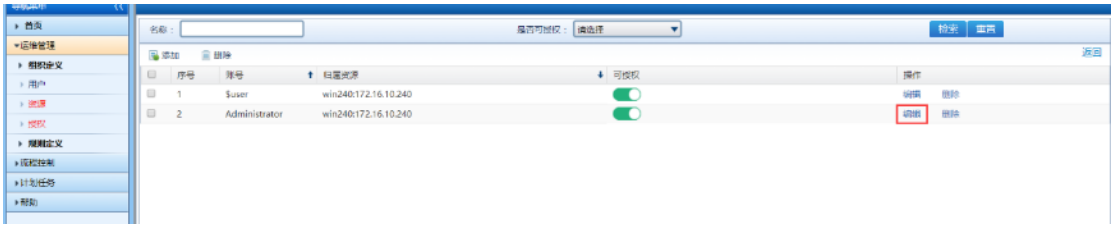


依次输入账号名称、口令，勾选“是否可授权”复选框，点击**保存**即可完成账号添加。



4.2. 资源账号修改

点击**运维管理**->**资源**，点击资源名称为 win240 对应的**账号管理**按钮，点击 Administrator 对应的**编辑**按钮，即可对该账号进行编辑。



4.3. 资源账号删除

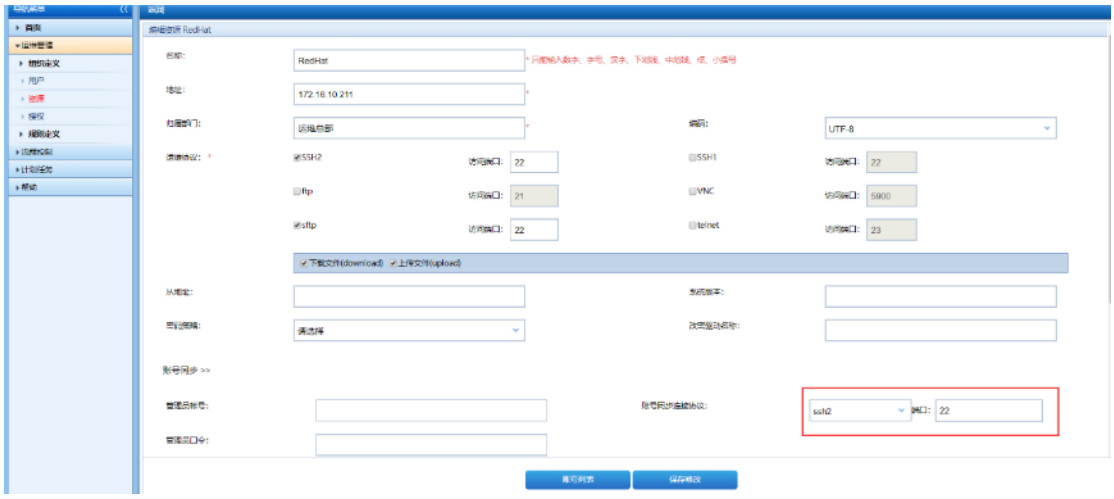
资源账号删除用于删除废弃的资源账号。可对单个资源账号进行删除，也可一次勾选多个资源账号进行删除。

点击**运维管理**->**资源**，点击资源名称为 win240 对应的**账号管理**按钮。点击 Administrator 账号对应的**删除**按钮，即可完成对资源账号的删除。

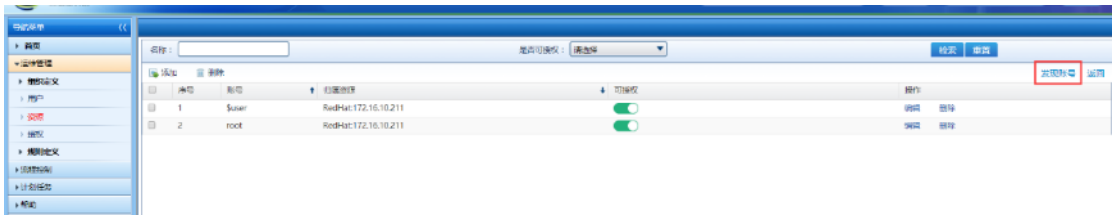
4.4. 资源账号自动发现

资源账号自动发现用于收集资源设备上的资源账号。

点击**运维管理->资源**，点击资源名称为 redhat 对应的**编辑**按钮，进入资源编辑页面。点击**账号同步**，填写管理员账号和口令，选择账号同步协议，点击**保存**。



点击**运维管理->资源**，点击资源名称为 redhat 对应的**账号管理**按钮，进入账号管理界面。点击**发现账号**按钮，完成该资源所有账号的发现。资源账号自动发现实现了账号的批量添加。



4.5. 资源账号导入

明文文件导入，编辑 xls 文档，为 win240 资源添加账号 aa。

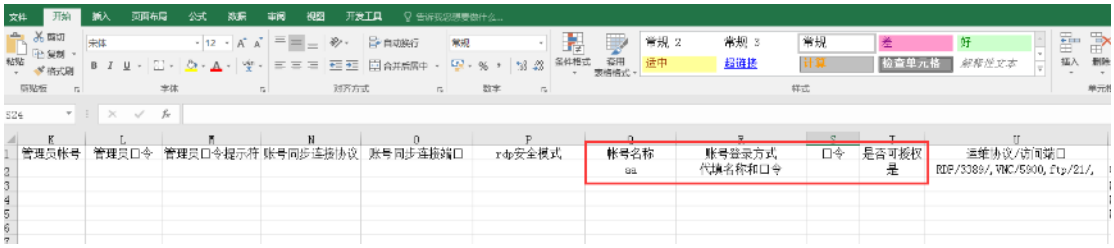
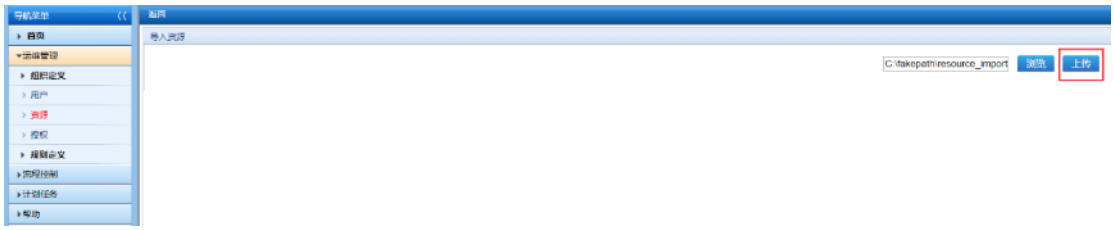


图 3.5.5-1

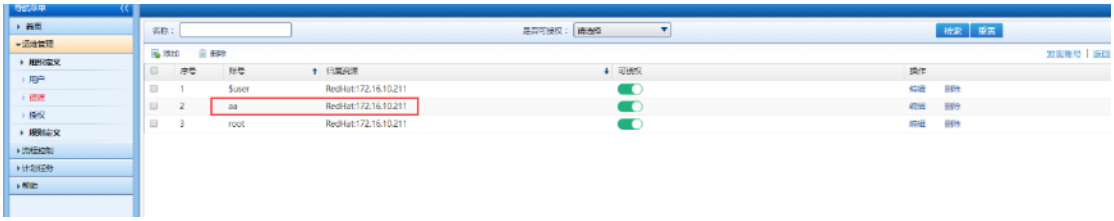
点击**运维管理->资源->导入**。

选择 xls 文件，点击**上传**按钮。



勾选 windows 资源，点击**保存**。

点击**运维管理->资源**，点击 win240 后面的账号管理按钮，账号列表显示 aa。



密文文件导入详见章节。

4.6. 资源账号导出

资源账号以 xls 明文方式导出）。

将选中的资源账号以 raot 加密方式导出，为资源账号密码的安全提供了保障，极大的方便了账号数据的恢复（详见章节导出资源+资源账号+资源账号密码）。

5. 授权

云堡垒机提供基于用户、目标设备、协议类型、IP、行为等要素实现细粒度的操作授权，最大限度保护用户资源的安全。

授权可将用户与资源进行一对一、一对多、多对多的关系绑定。用户和用户组可只选择一种，也可以同时选择两种，同理资源、资源账号、资源组也可选择任意一种或多种进行绑定，方便用户灵活授权。

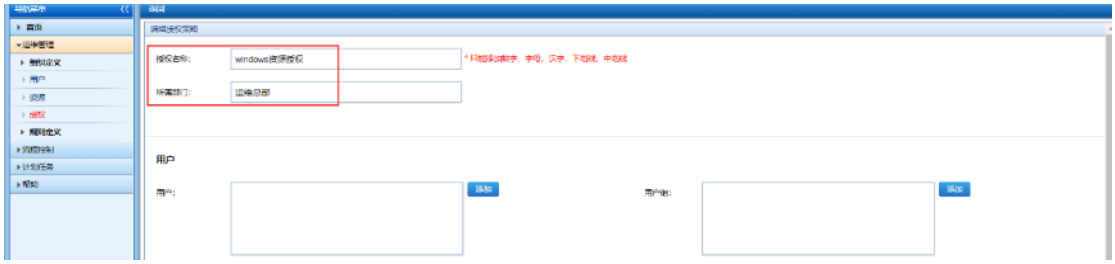
下面举例说明几种授权关系的绑定。

5.1. 用户和资源授权

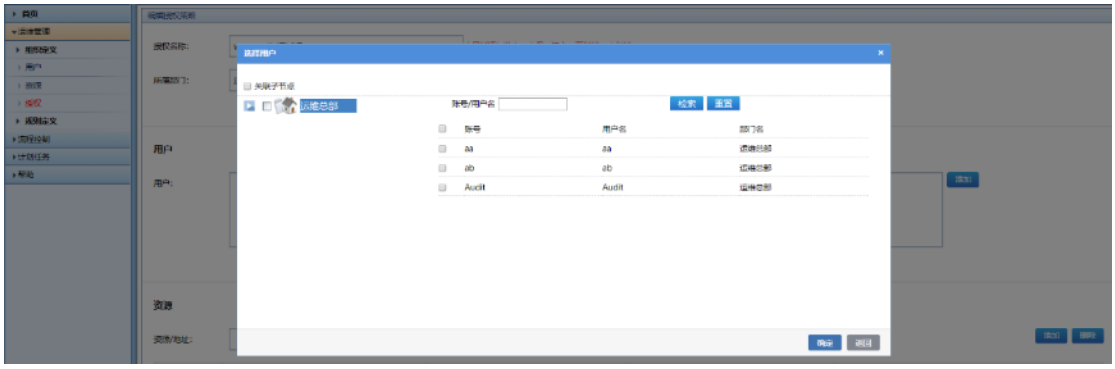
用户和资源授权是为单个用户和资源建立授权关系。

用安全管理员 secAdmin 登录系统，点击**运维管理**->**授权**->添加，页面跳转到授权信息编辑页面。

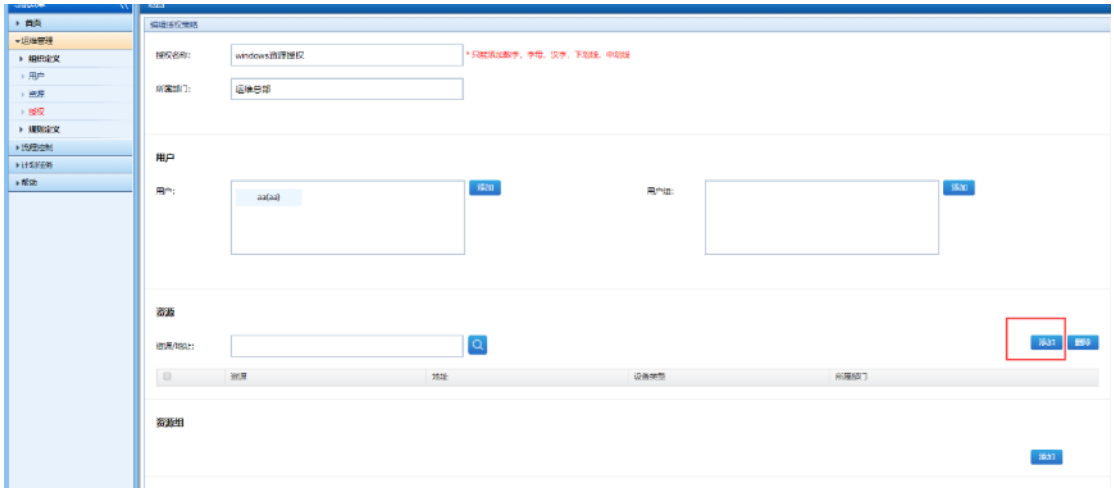
填写授权名称，选择授权所属部门，点击**添加用户**。



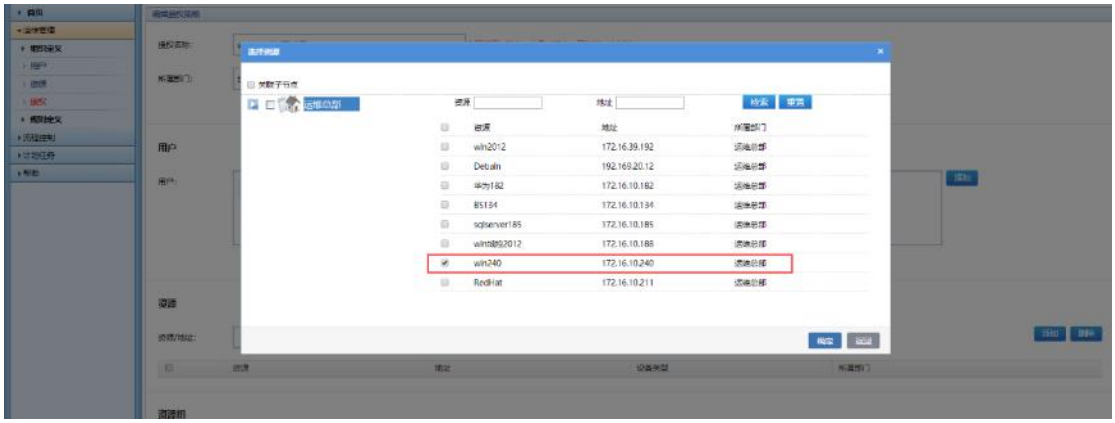
勾选用户部门，点击检索，选择运维用户 aa，点击确定。



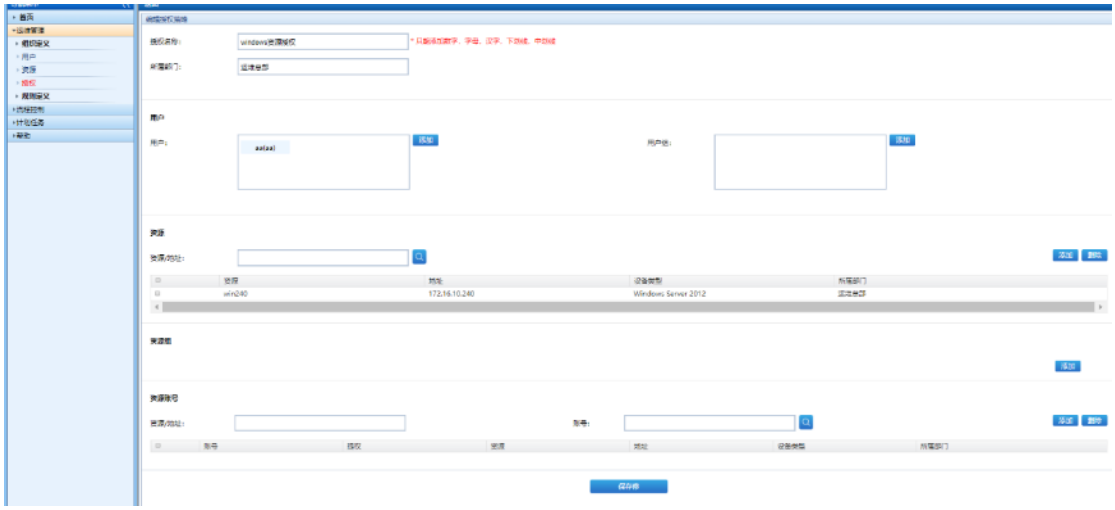
返回到授权编辑页面，用户一栏下面可以看到添加的运维用户。下面开始授权资源的添加。点击**添加资源**按钮，切换到资源选择页面。



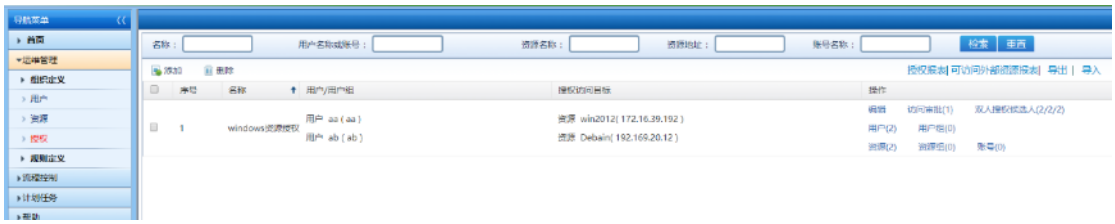
勾选资源部门，点击检索，选择资源，点击确定。



返回到授权编辑页面，资源一栏下面可以看到添加的运维资源。点击保存。



点击运维管理->授权，切换到授权列表页面，列表中显示授权名称为 windows 资源授权的条目。

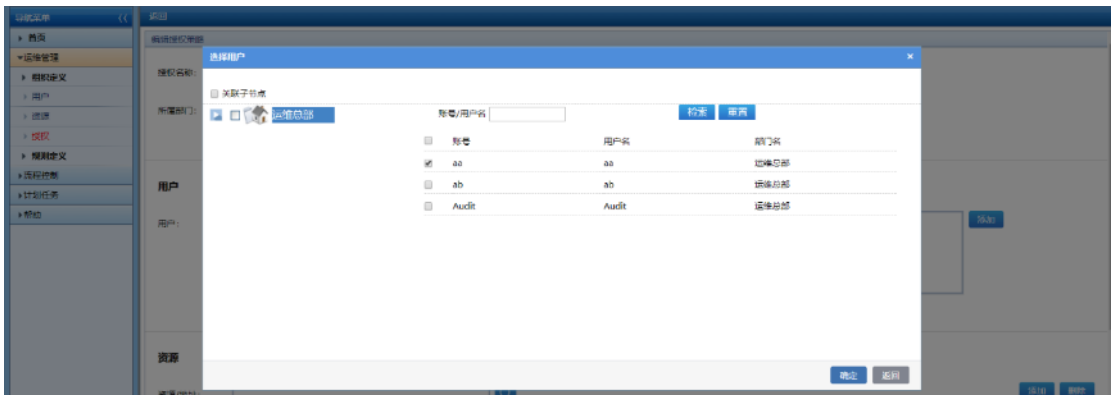


5.2. 用户和资源组授权

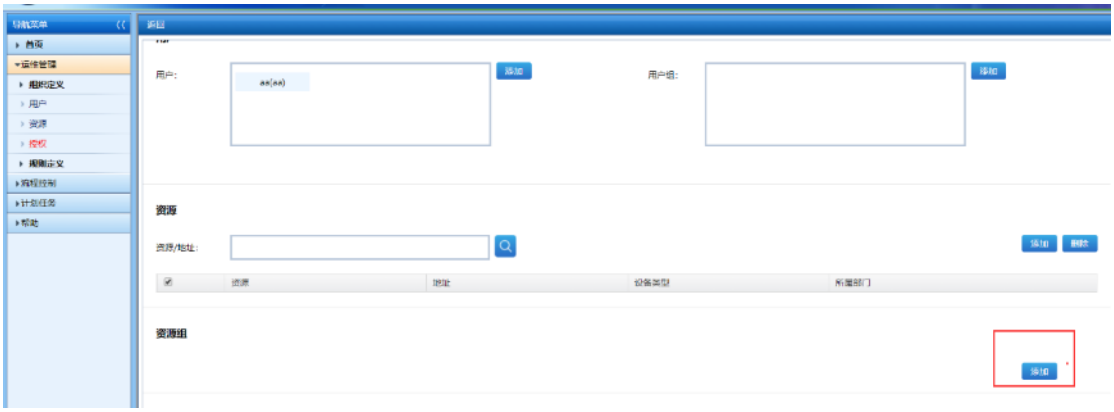
用户和资源组授权是为单个用户和资源组建立授权关系。

点击运维管理->授权->添加，切换到授权编辑页面，填写授权名称，选择所属部门，点击添加用户。

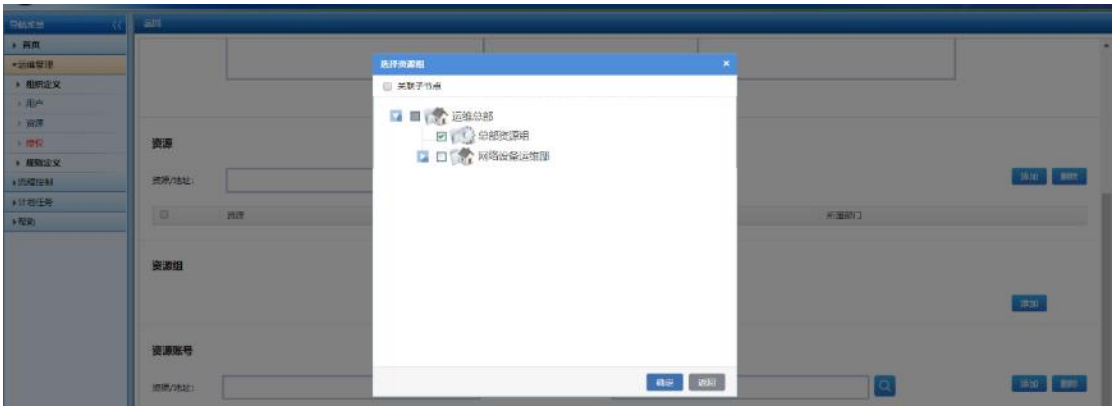
切换到用户选择页面，勾选用户部门，点击检索，选择运维用户 aa，点击确定。



返回到授权编辑页面，用户一栏下面可以看到添加的运维用户。下面开始授权资源组的添加。点击添加资源组按钮。



切换到资源组选择页面，选择资源组，点击确定。



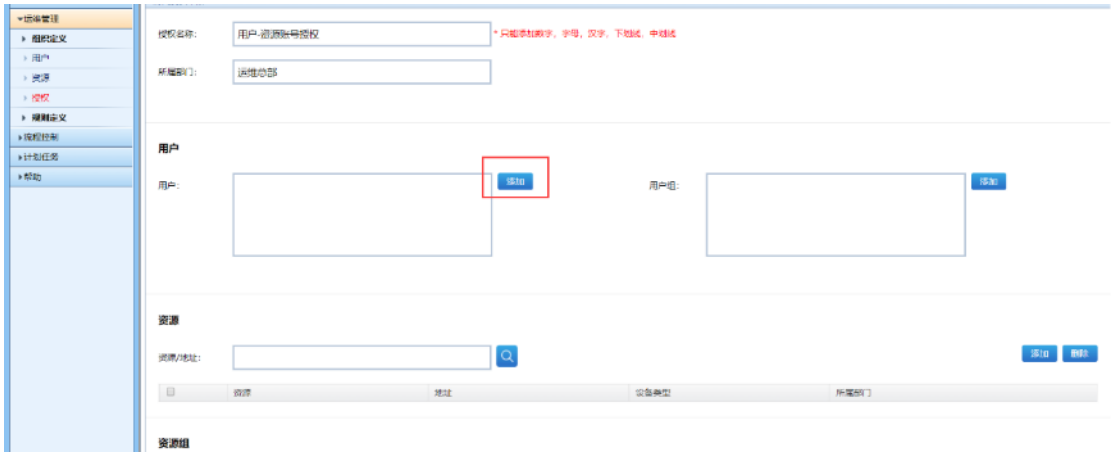
返回到授权编辑页面，资源组一栏下面可以看到添加的资源组，点击保存。

点击运维管理->授权，切换到授权列表页面，列表中显示授权名称为用户-资源组的条目。

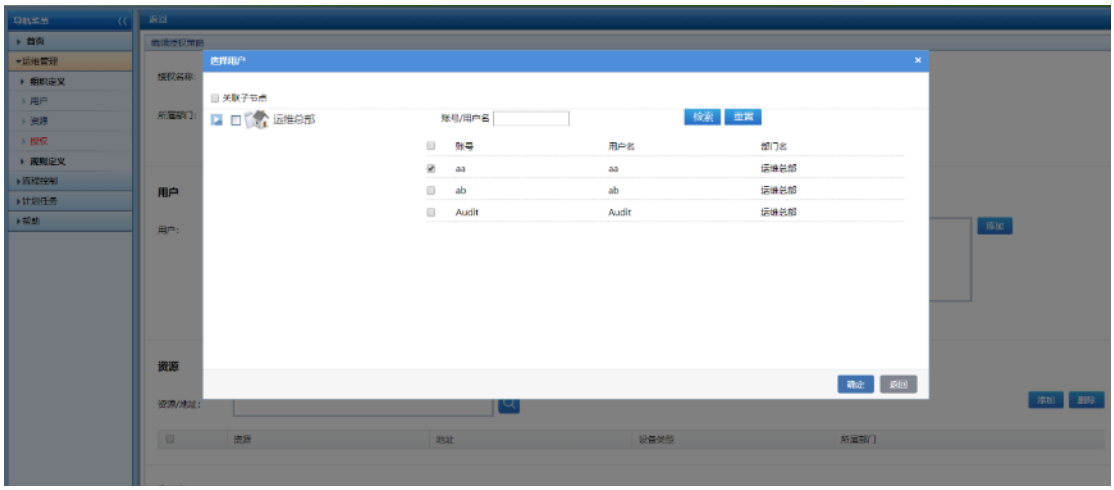
5.3. 用户和资源帐号授权

用户和资源账号授权是为单个用户和资源账号之间建立授权关系。

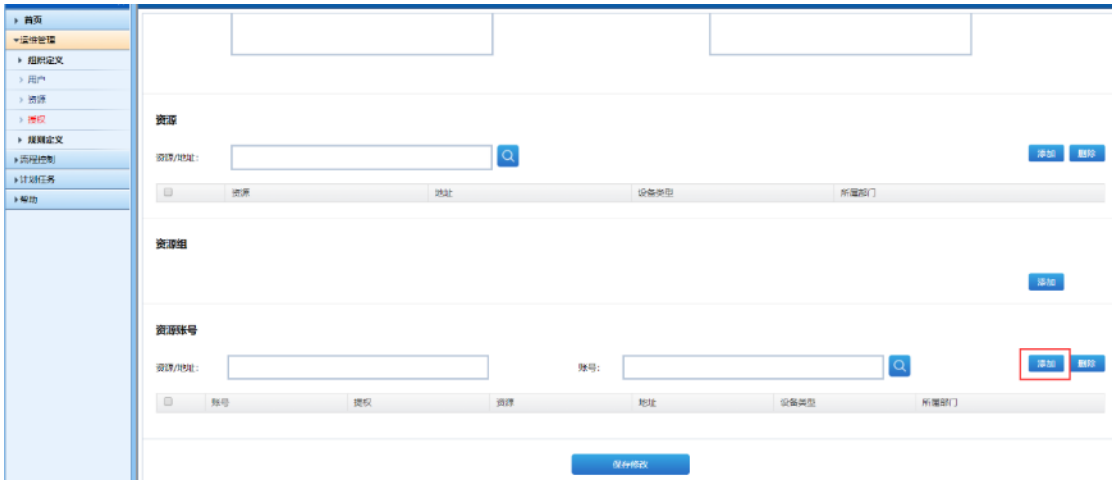
点击运维管理->授权->添加，切换到授权编辑页面，填写授权名称，选择所属部门，点击添加用户。



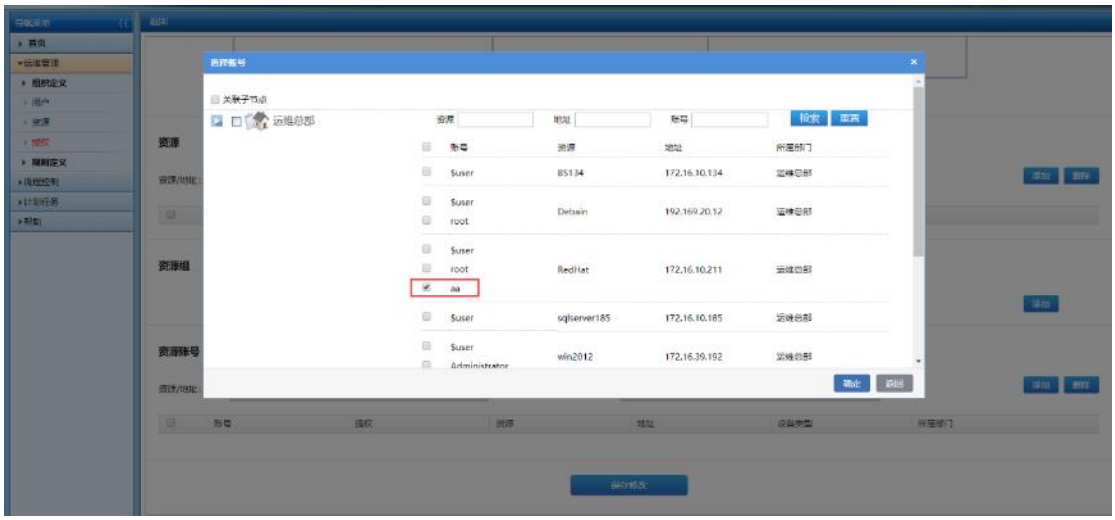
展开部门，点击检索，勾选运维用户 aa，点击确定。



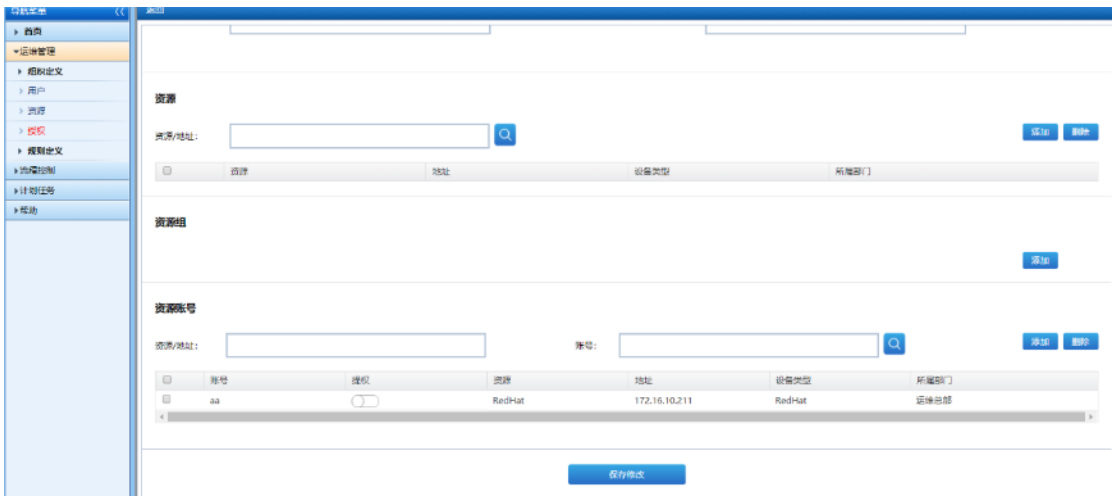
切换到资源账号选择页面，用户一栏下面可以看到添加的运维用户。下面开始授权资源账号的添加，点击添加资源账号。



勾选资源部门，点击检索，勾选资源账号，点击确定。



返回到授权编辑页面，资源账号一栏下面可以看到添加的资源账号，点击保存。

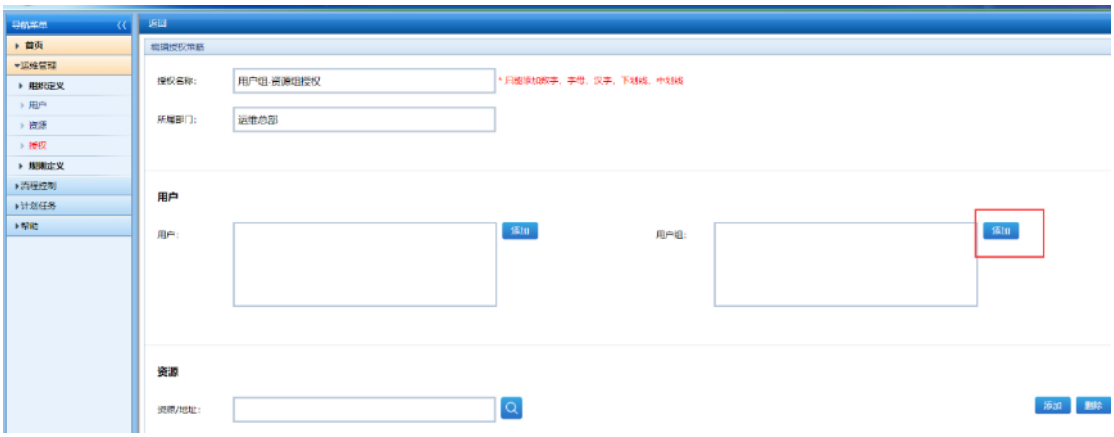


点击运维管理->授权，切换到授权列表页面，列表中显示授权名称为用户-资源账号的条目。

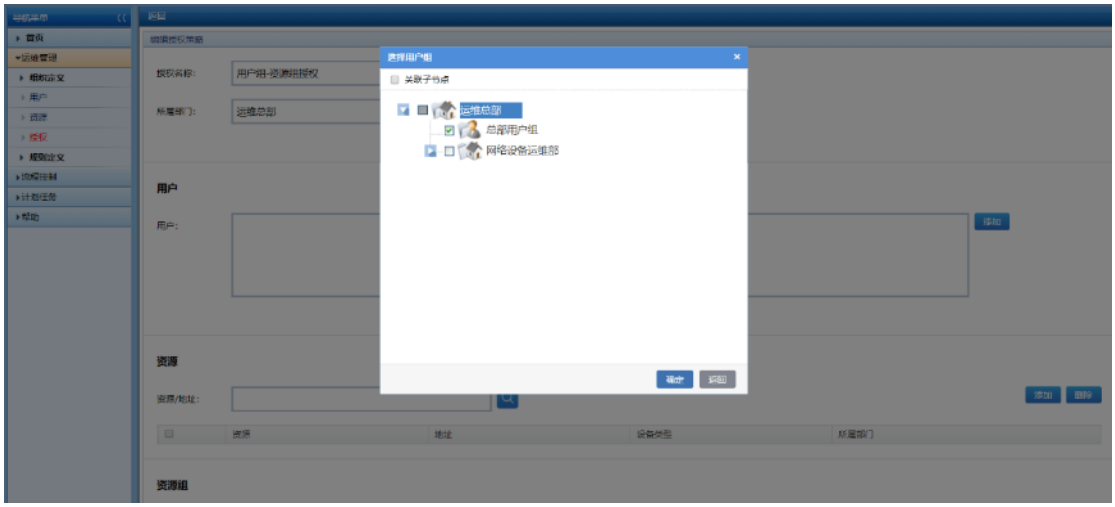
5.4. 用户组和资源组授权

用户组和资源组授权是为用户组和资源组之间建立授权关系。

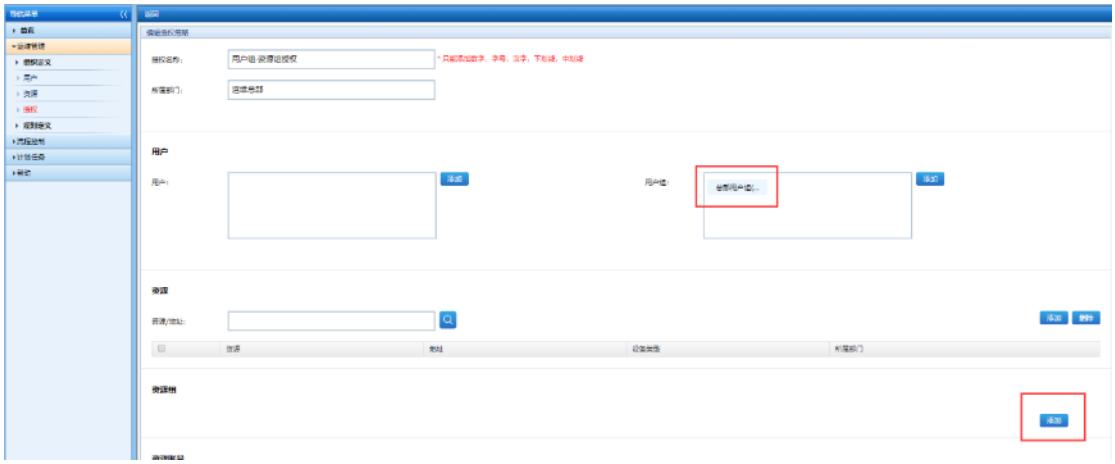
点击**运维管理**->**授权**->添加，切换到授权编辑页面，填写授权名称，选择所属部门，点击**添加用户组**。



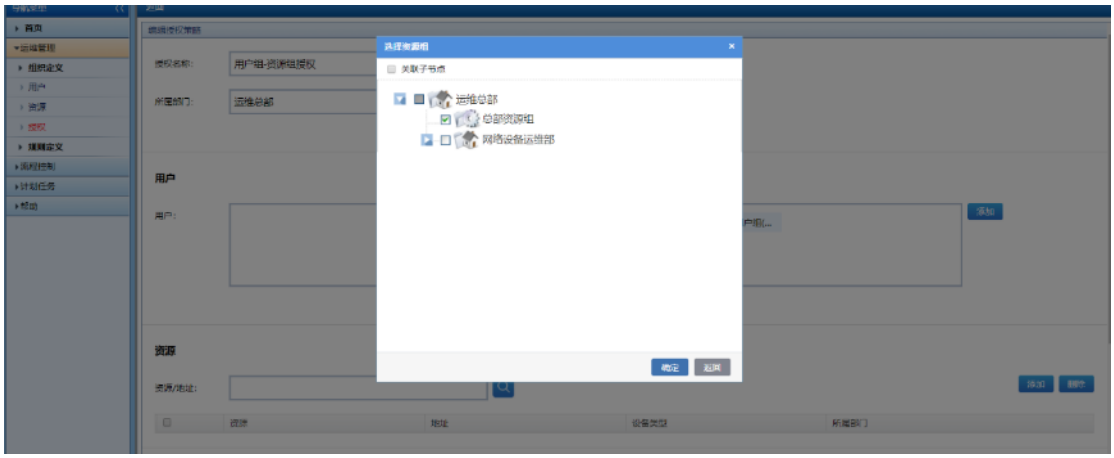
展开用户部门，勾选名称为**总部用户组**的用户组，点击**确定**。



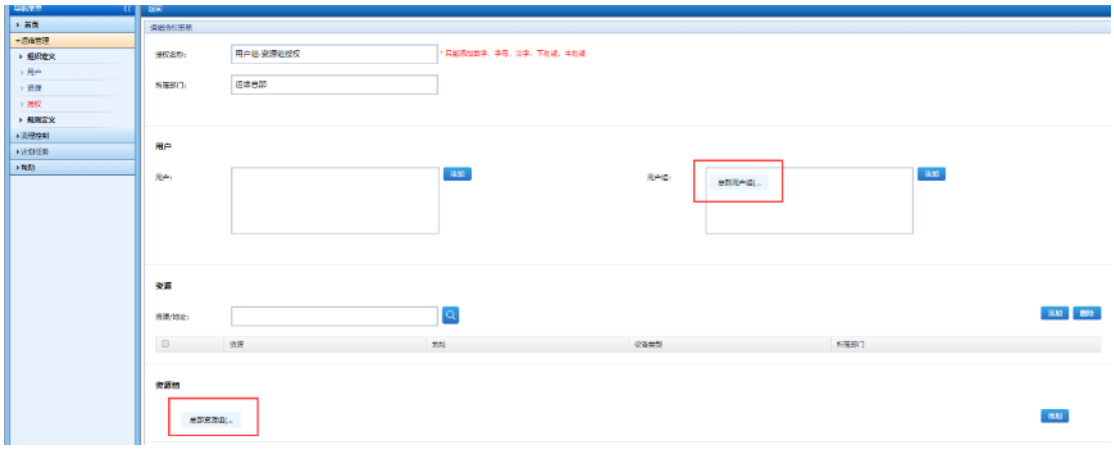
返回到授权编辑页面，用户组栏下面显示添加的用户组，点击**添加资源组**。



展开资源部门，勾选名称为**总部资源组**的资源组，点击**确定**。



返回到授权编辑页面，资源组一栏下面可以看到添加的资源组，点击保存。

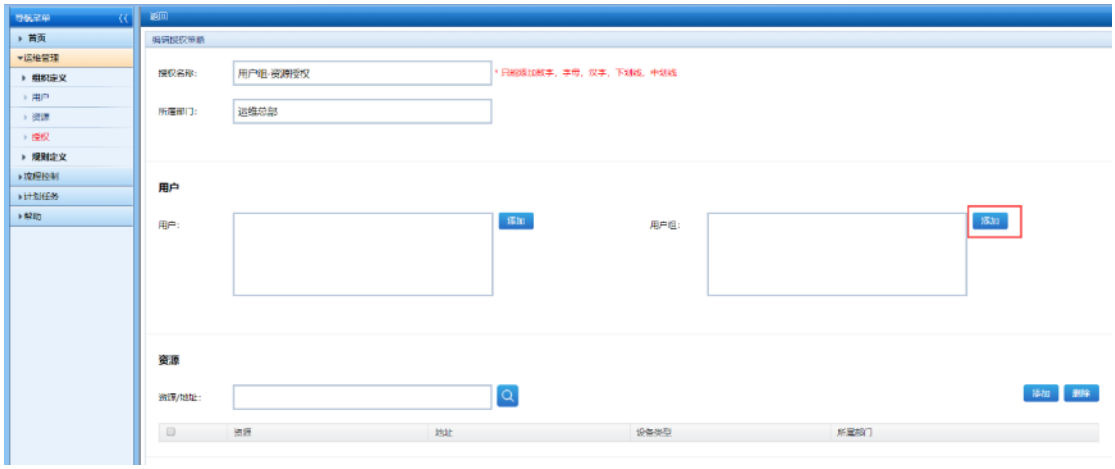


点击运维管理->授权，切换到授权列表页面，列表中显示授权名称为用户组-资源组的条目。

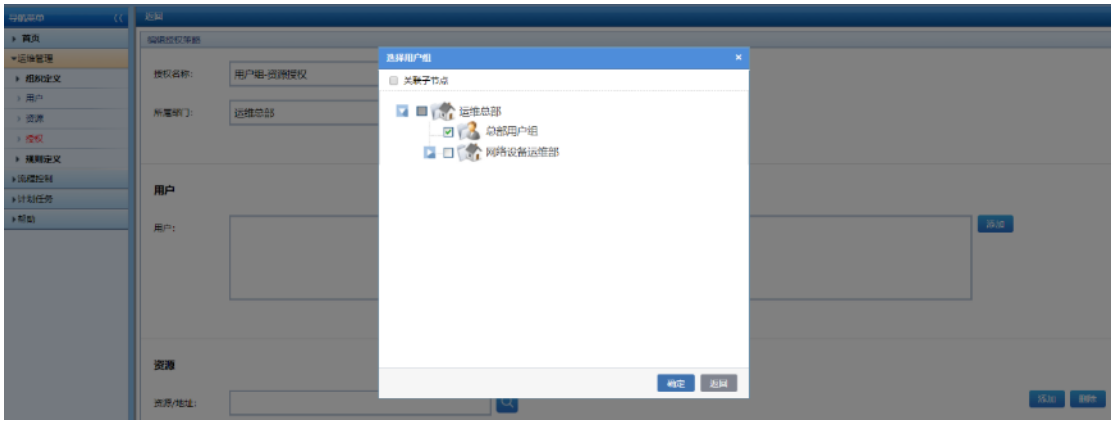
5.5. 用户组和资源授权

用户组和资源授权是为用户组和资源之间建立授权关系。

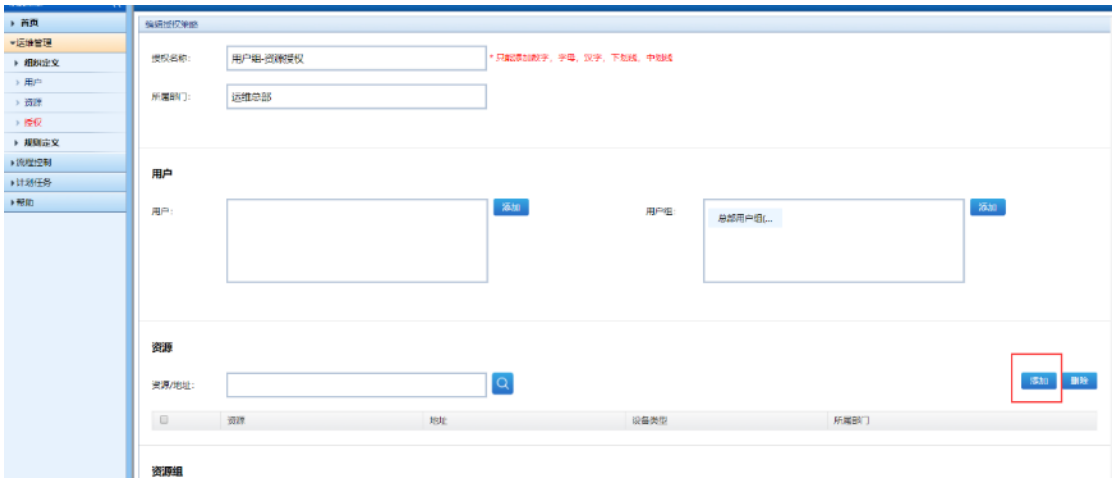
点击**运维管理**->**授权**->添加，切换到授权编辑页面，填写授权名称，选择所属部门，点击**添加用户组**。



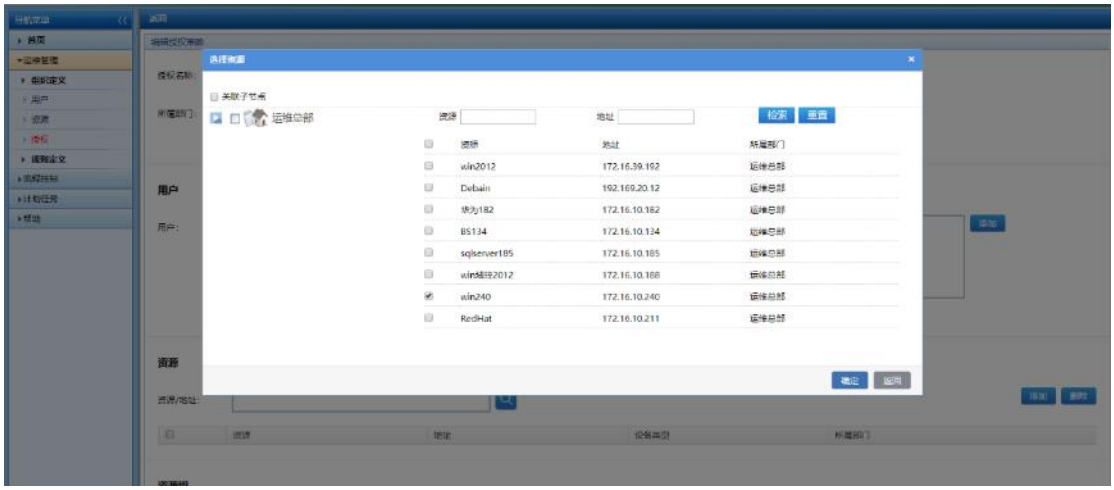
页面切换到用户组选择页面，勾选名称为**总部用户组**的用户组，点击**确定**。



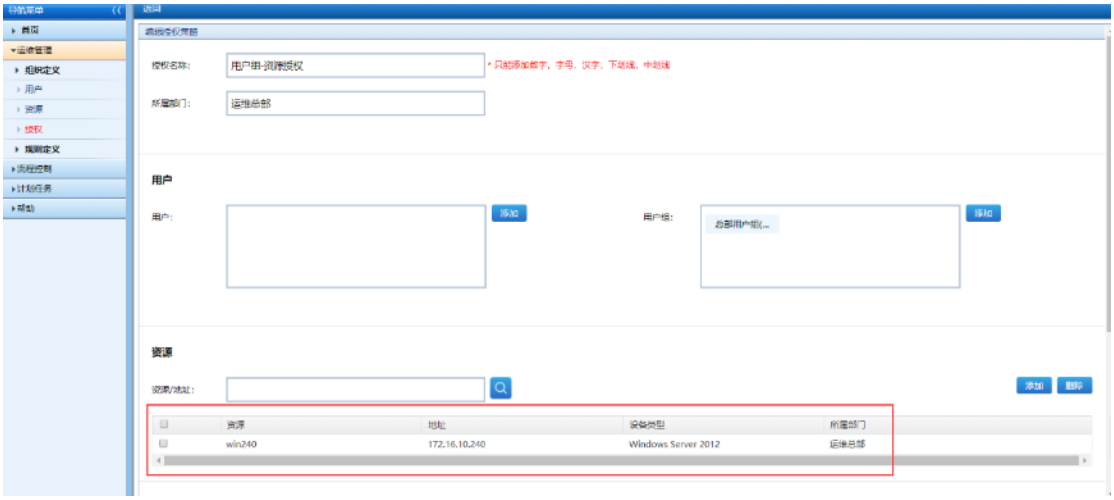
返回到授权编辑页面，用户组栏下面显示添加的用户组，点击**添加资源**。



选择资源部门，点击**检索**，勾选想要添加的资源，点击**确定**。



返回到授权编辑页面，资源一栏下面可以看到添加的资源，点击保存。

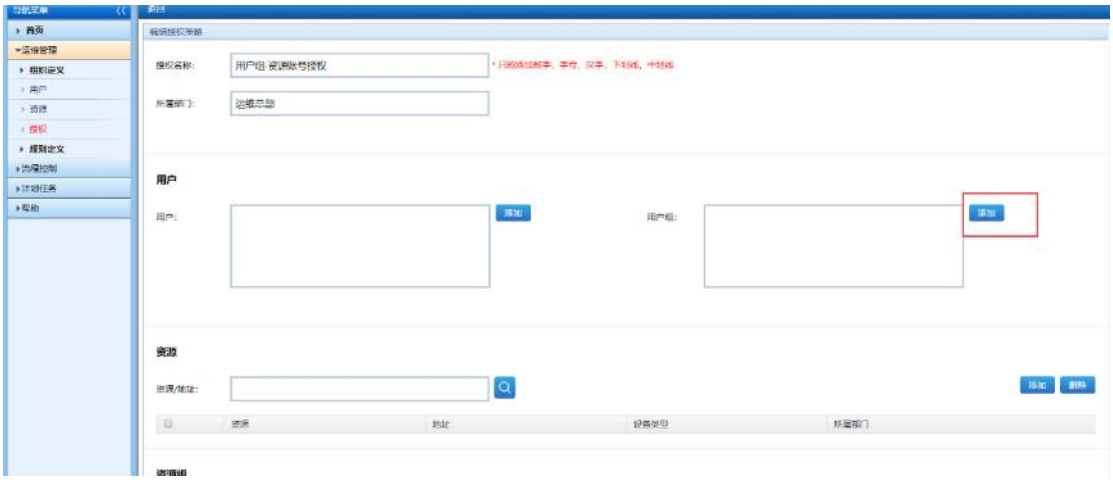


点击运维管理->授权，切换到授权列表页面，列表中显示授权名称为用户组-资源授权的条目。

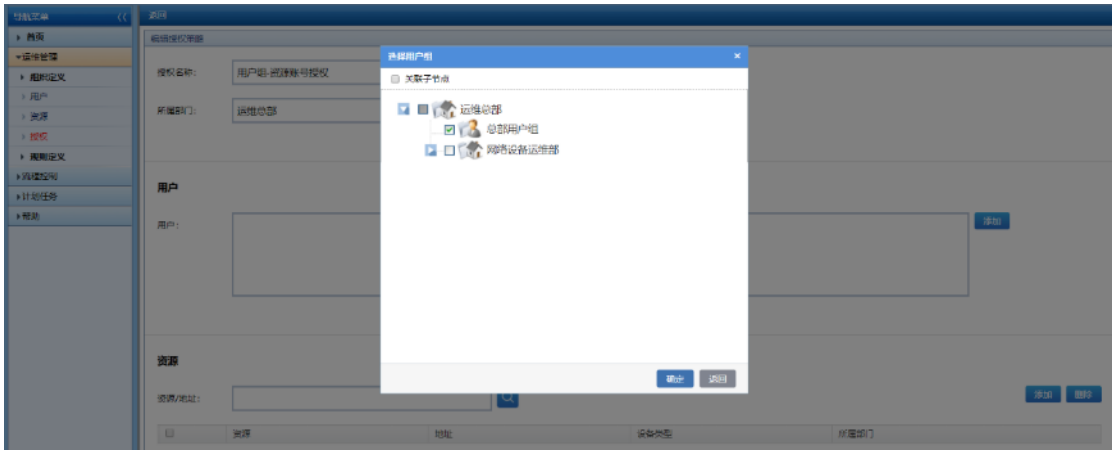
5.6. 用户组和资源账号授权

用户组和资源组授权是为用户组和资源账号之间建立授权关系。

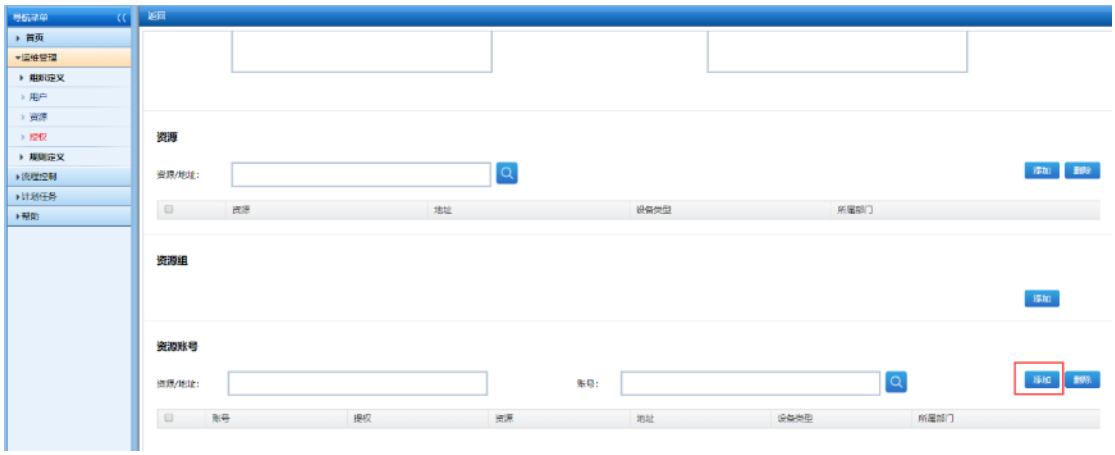
点击**运维管理**->**授权**->添加，切换到授权编辑页面，填写授权名称，选择所属部门，点击**添加用户组**。



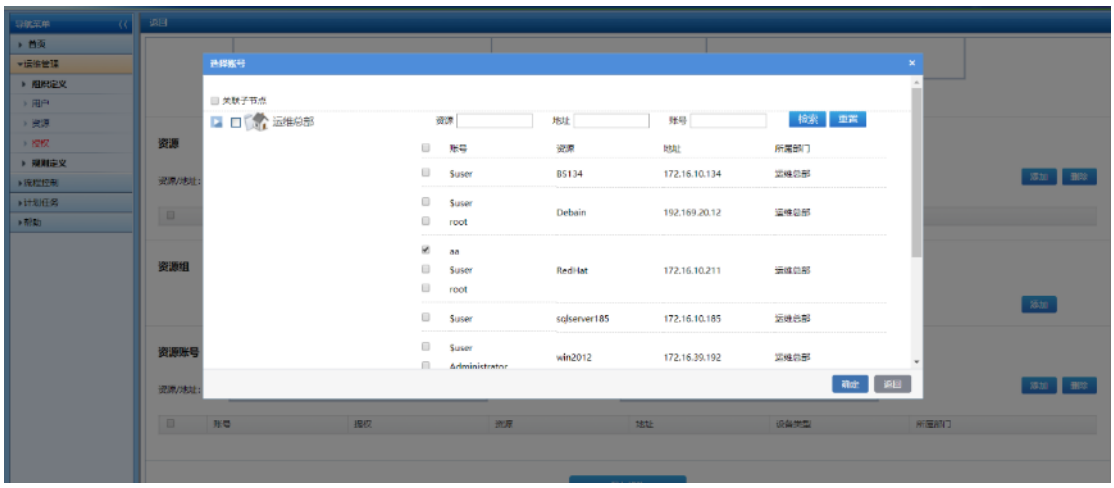
切换到用户组选择页面，勾选名称为**总部用户组**的用户组，点击**确定**。



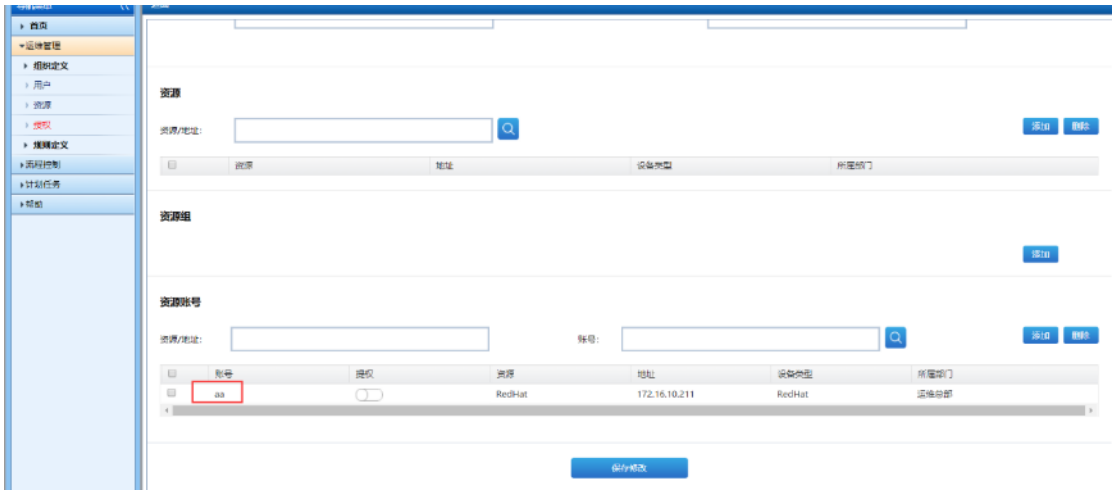
返回到授权编辑页面，用户组栏下面显示添加的用户组，点击**添加资源账号**。



勾选资源部门，点击**检索**，勾选想要添加的资源账号，点击**确定**。



返回到授权编辑页面，资源帐号一栏下面可以看到添加的资源账号，点击保存。



点击**运维管理**->**授权**，切换到授权列表页面，列表中显示授权名称为用户组和资源账号的条目。

5.7. 授权检索

授权可以按照名称、用户名或账号、资源名称、资源 IP、账号名称等关键字进行检索。

5.7.1. 按名称检索

名称检索是将授权名称作为检索条件。

点击**运维管理**->**授权**，在名称检索栏中输入“windows”，点击**检索**按钮。

授权列表显示授权名称中包含关键字“windows”的条目，并且名称一栏显示为红色字体。

5.7.2. 按用户名或账号检索

用户名或账号检索是将用户名或账号作为检索条件。

点击**运维管理->授权**，在用户名或账号检索栏中输入“aa”，点击**检索**按钮。

授权列表显示用户名或账号中包含关键字“Audit”的条目，并且包含“aa”的用户名或账号字体显示为红色。

5.7.3. 按资源名称检索

资源名称检索是将资源名称作为检索条件。

点击**运维管理**->**授权**，在资源名称检索栏中输入“redhat”，点击**检索**按钮。

授权列表显示资源名称中包含关键字“redhat”的条目，并且包含“redhat”的资源字体显示为红色。

5.7.4. 按资源地址检索

资源地址检索是将资源地址作为检索条件。

点击**运维管理**->**授权**，在资源地址检索栏中“172.16.20.211”，点击**检索**按钮。

授权列表显示资源 IP 中包含关键字“172.16.20.211”的条目，并且包含“172.16.20.211”的资源字体显示为红色。

5.7.5. 按账号名称检索

账号名称检索是将账号名称作为检索条件。

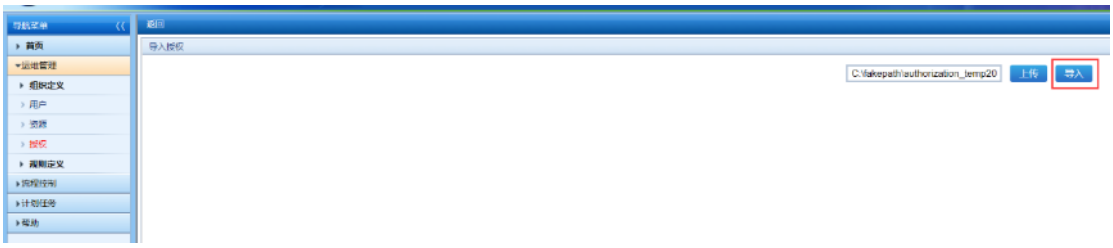
点击**运维管理->授权**，在账号名称检索栏中“Administrator”，点击**检索**按钮。

授权列表显示出账号名称中包含关键字的条目，并且包含“Administrator”资源字体显示为红色。

5.8. 授权导入

点击**运维管理->授权->导入**。

点击**上传**，选择授权文件，点击**导入**。



导入授权页面出现导入提示信息，点击**返回**。

切换到授权列表页面，列表中显示导入的授权条目。导入功能实现了授权的批量添加，方便了授权数据的恢复。

5.9. 授权导出

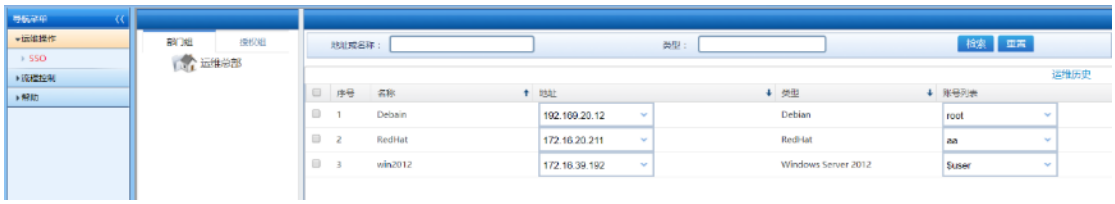
授权导出不用勾选条目，点击导出之后，该部门的授权全部被导出。导出的文件为 pwdbak 格式，方便用户保存，也为授权数据的恢复提供了保障。

点击**运维管理->授权->导出**。

导出成功，导出文件如图所示： authorization_temp2019-05-24.pwdbak

6. 单点登录

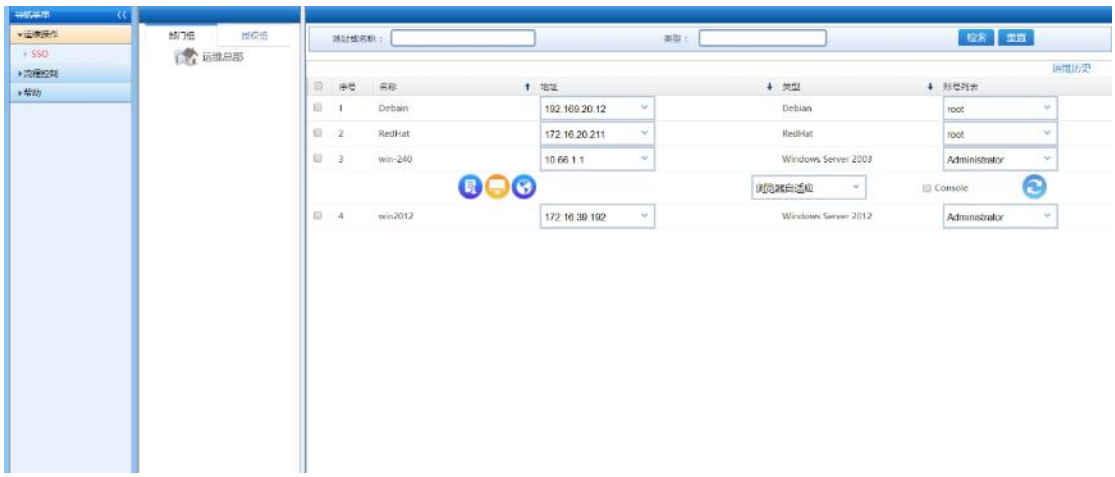
使用运维操作员角色的用户 aa 登录系统，登录成功后看到用户 aa 已被授权的资源列表。



6.1. windows 类型资源

6.1.1. 自动代填帐号和口令

登录系统后点击运维操作-> sso ->部门组->运维总部。



点击  图标，打开 FTP 文件传输页面（需要目标服务器开启 ftp 服务）。

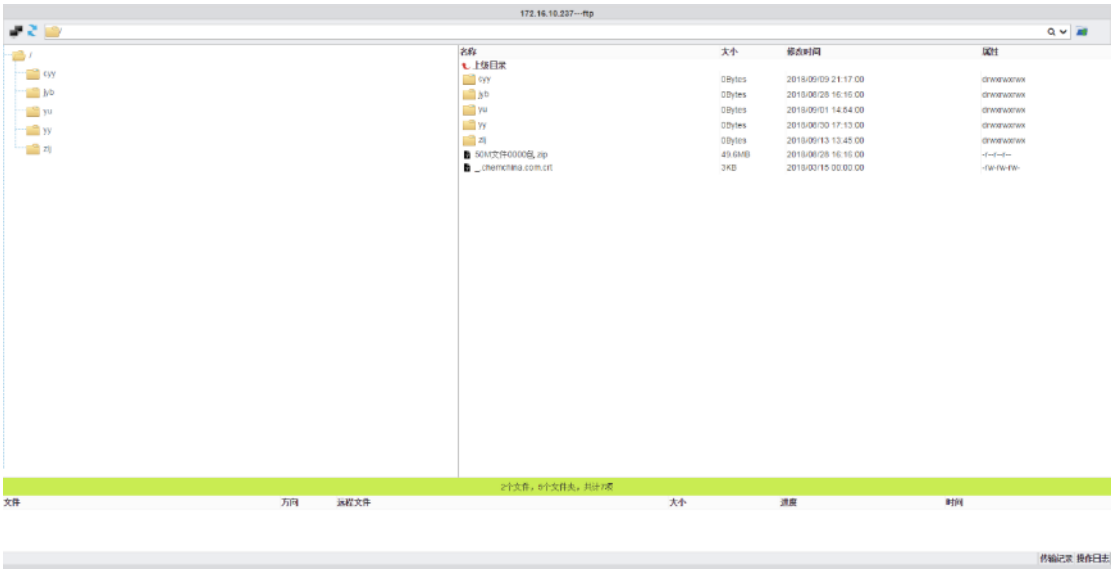
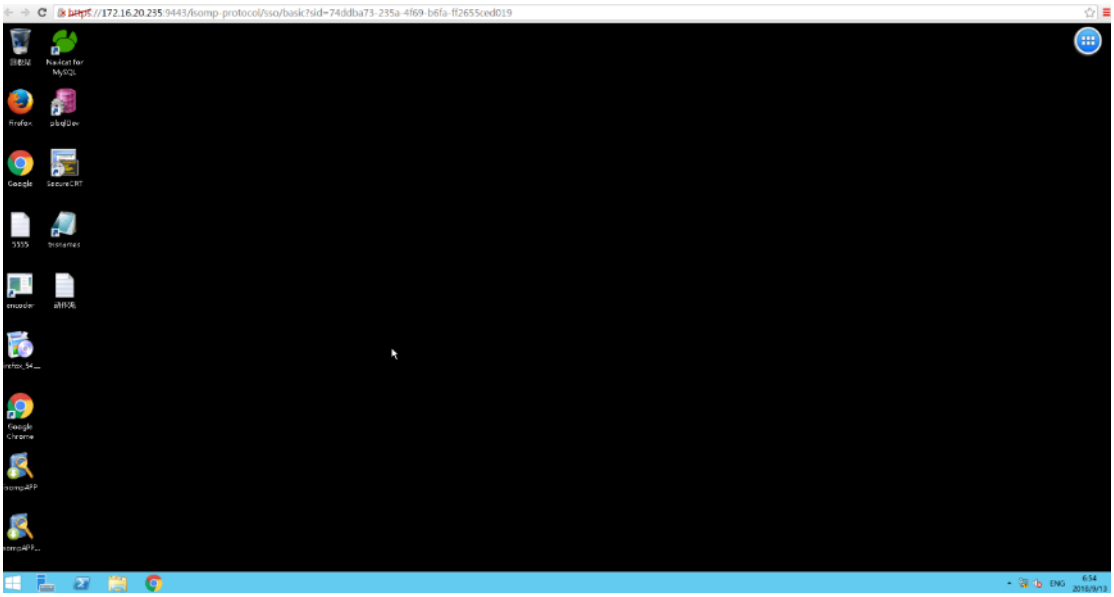
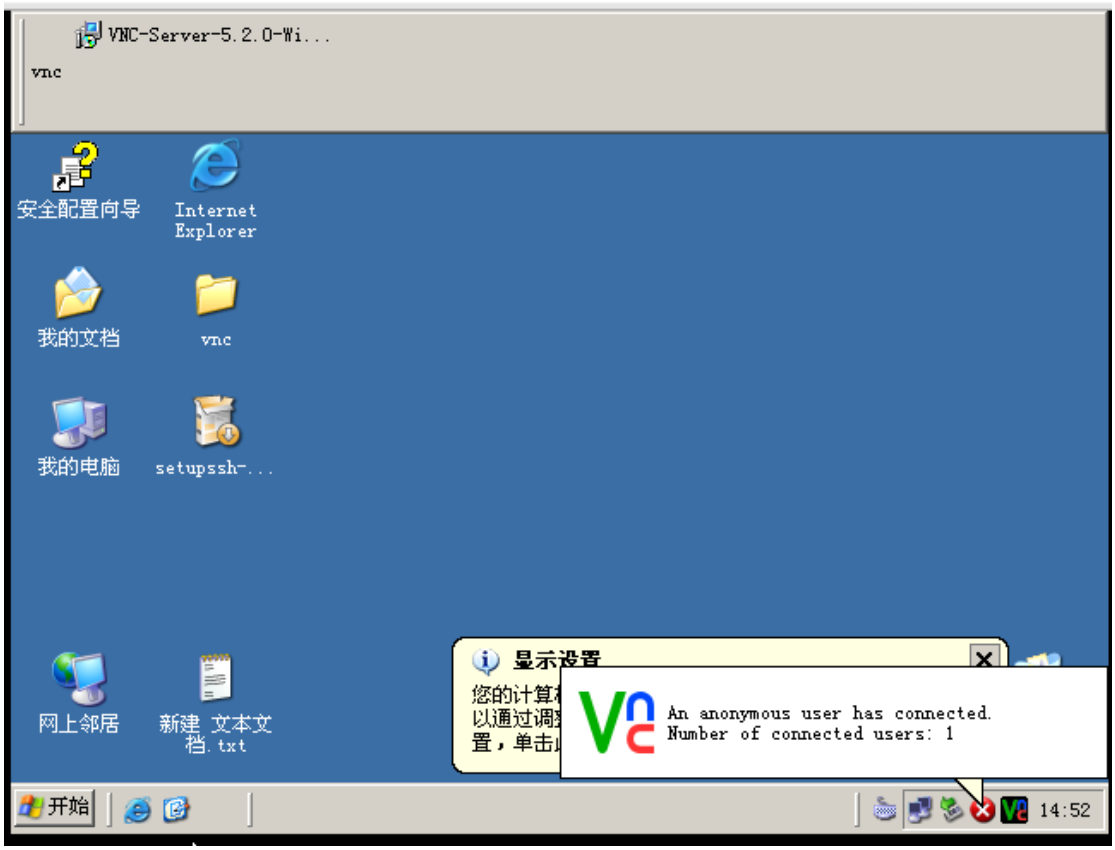


图 3. 7. 1. 1-2

点击  图标，进入 windows 服务器。



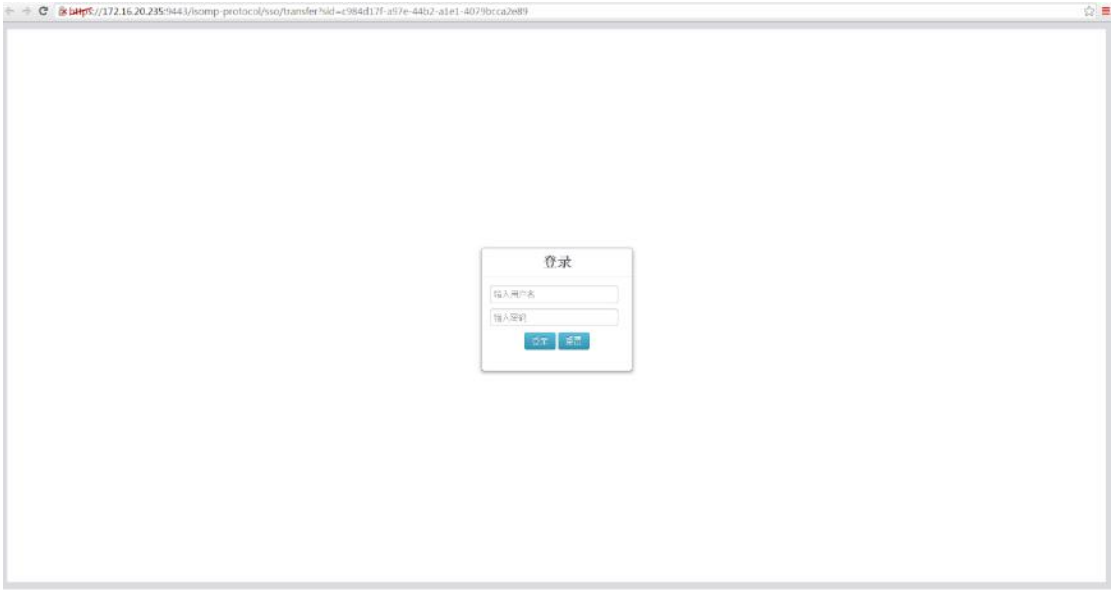
点击  图标,使用 vnc 协议进行单点登录。



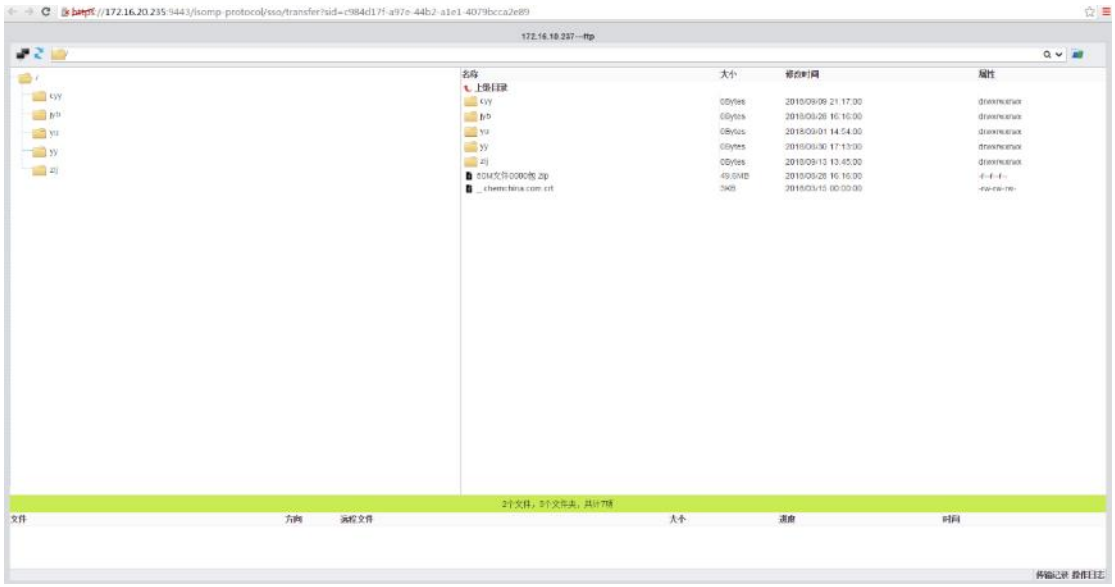
6.1.2. 手动输入账号和口令

点击 

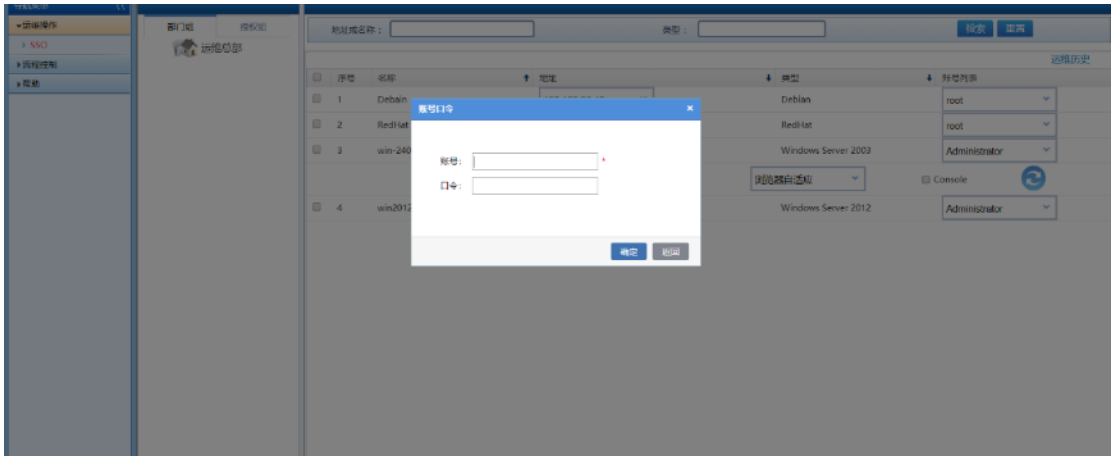
图标，打开 FTP 文件传输页面。



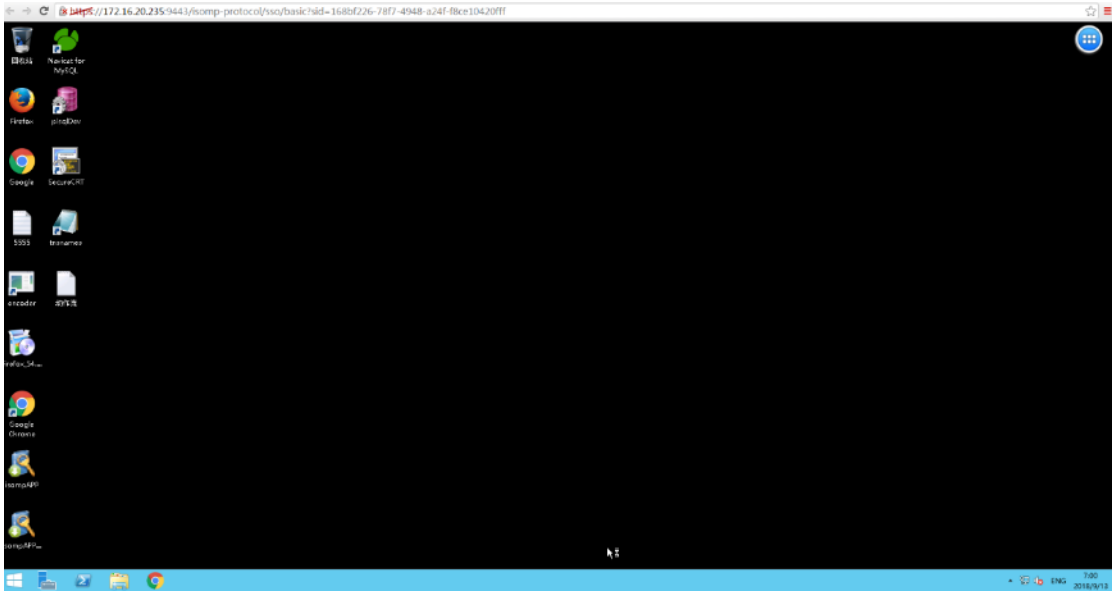
输入用户名和口令，点击登陆按钮，进入 FTP 文件传输页面（需要目标服务器开启 ftp 服务）。



点击  图标，弹出选择 RDP 访问控制窗口。

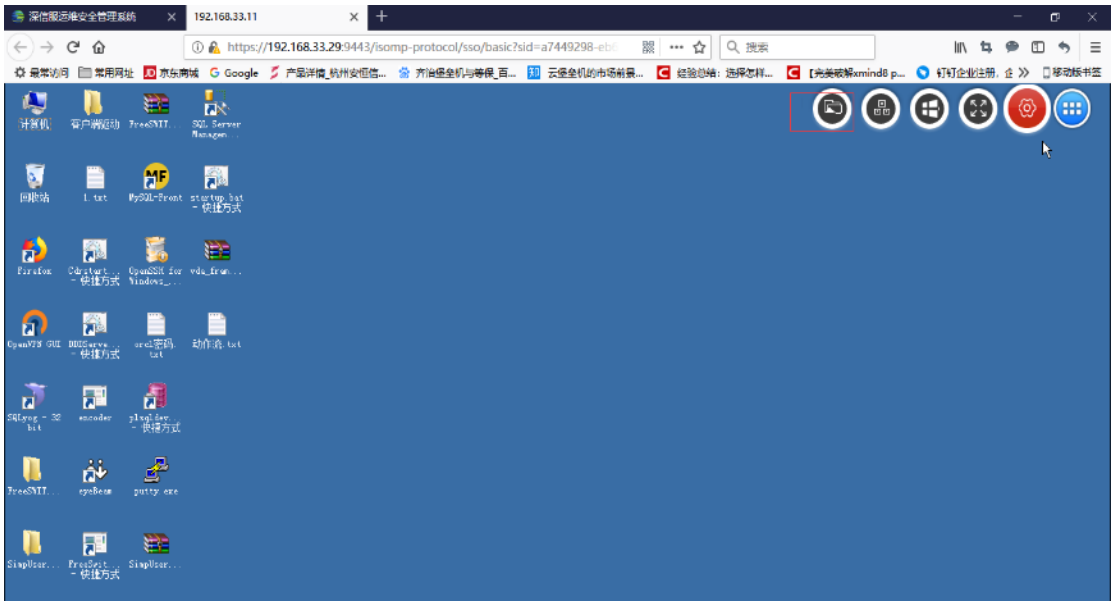


输入账号和口令，点击确定按钮，进入 windows 系统。

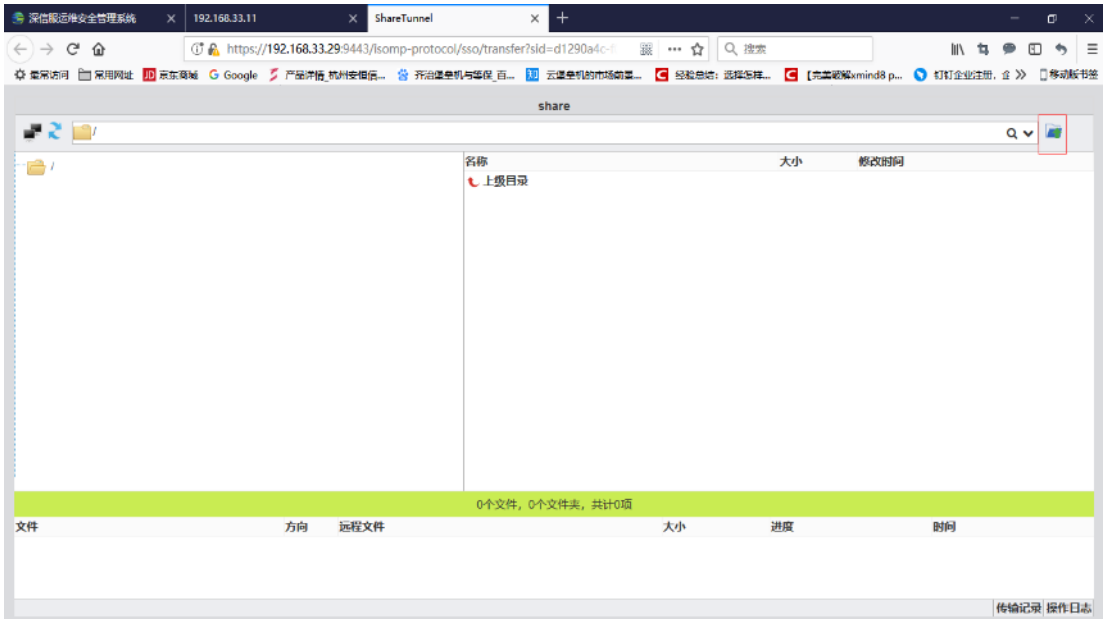


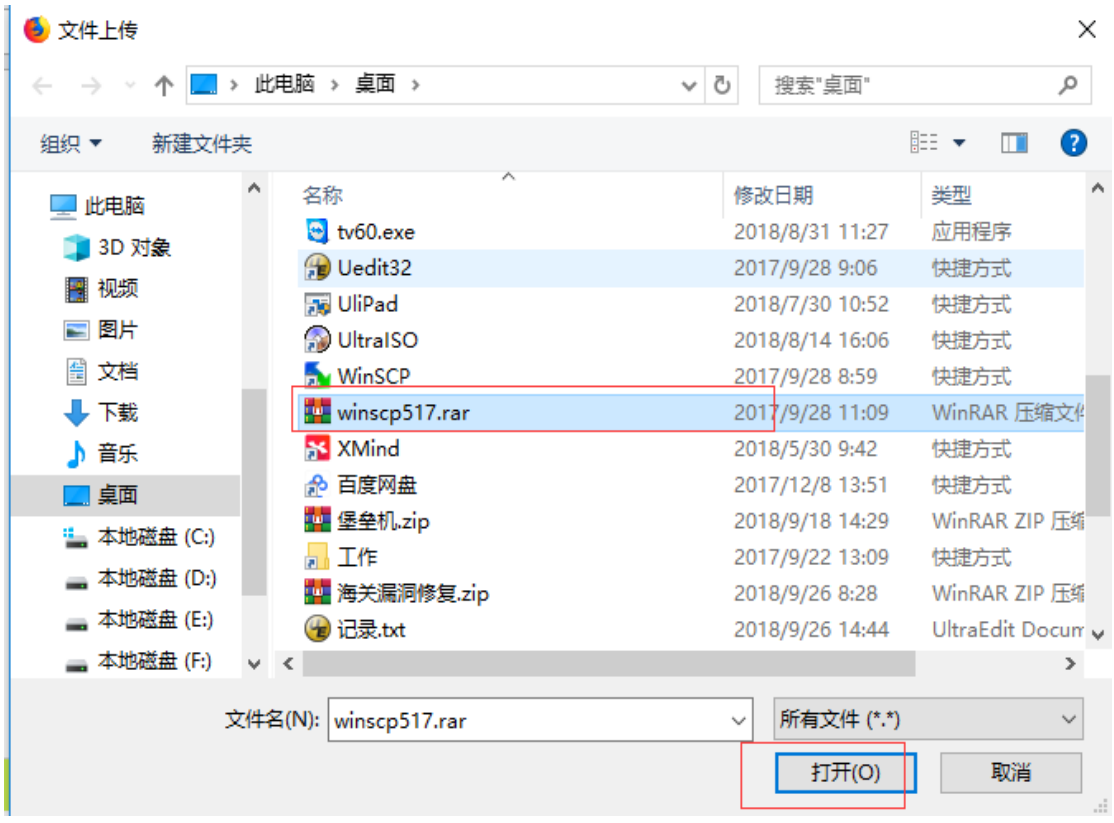
6.1.3. 文件传输

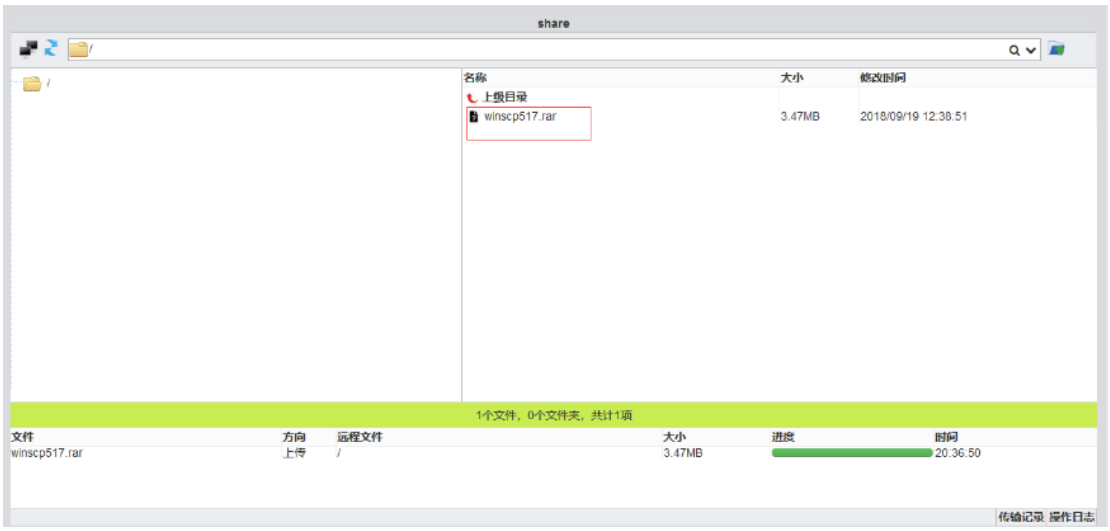
除上文介绍的 ftp 文件传输之外，单点登陆后可以使用磁盘映射方式传输文件，点击单点登陆后的右上角操作按钮：



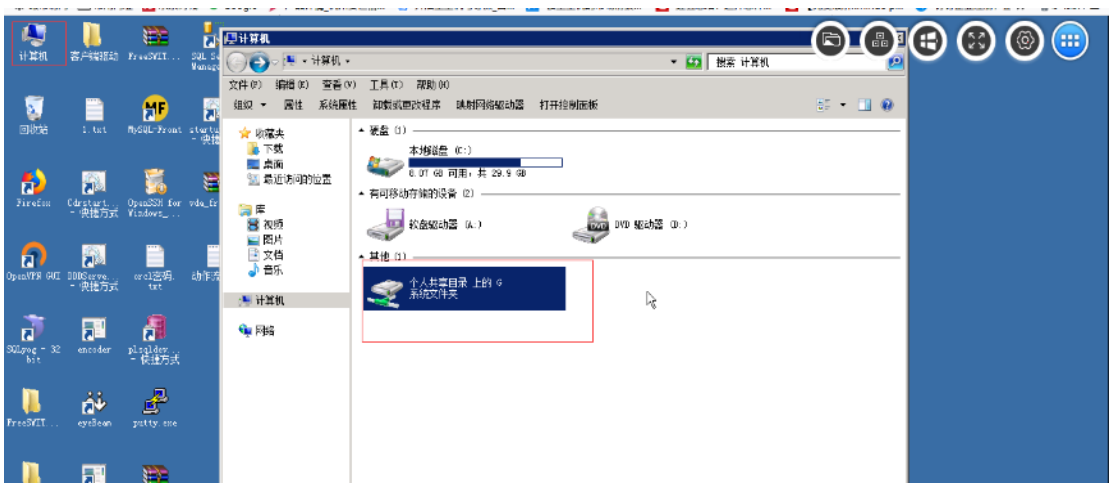
弹出传输文件对话框，可点击浏览按钮选择文件上传：

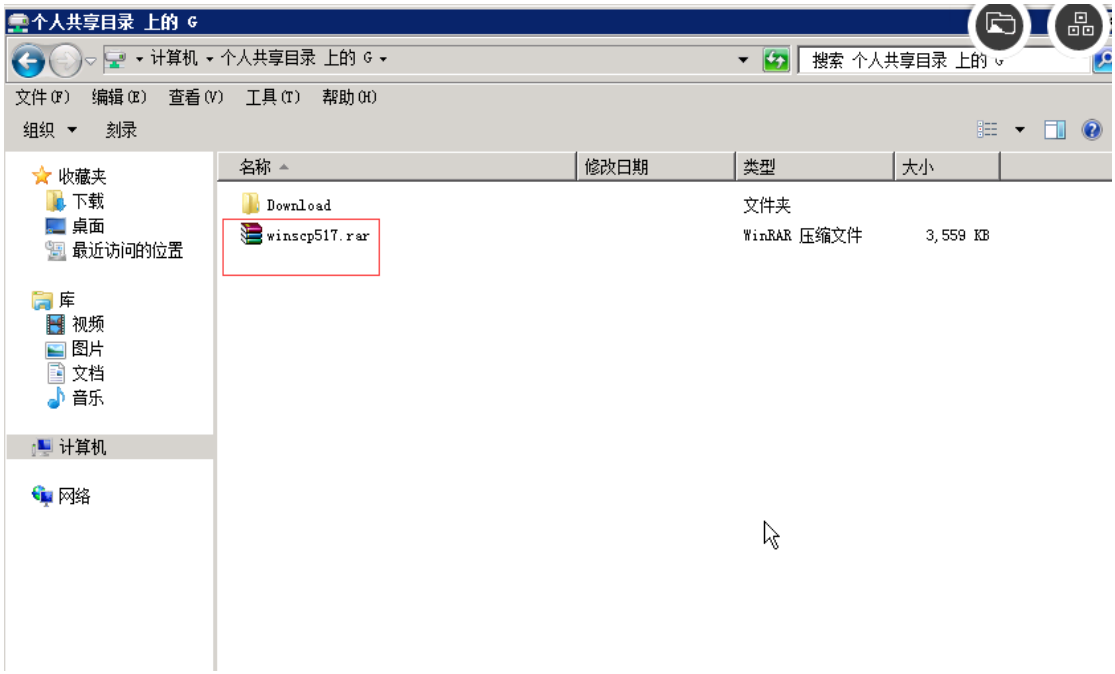

ShareTunnel
share
名称
大小
修改时间
上级目录
0个文件，0个文件夹，共计0项
文件
方向
远程文件
大小
进度
时间


文件上传
此电脑 › 桌面 ›
搜索"桌面"
组织
新建文件夹
此电脑
3D 对象
视频
图片
文档
下载
音乐
桌面
本地磁盘 (C:)
本地磁盘 (D:)
本地磁盘 (E:)
本地磁盘 (F:)
名称
修改日期
类型
tv60.exe 2018/8/31 11:27 应用程序
Uedit32 2017/9/28 9:06 快捷方式
UliPad 2018/7/30 10:52 快捷方式
UltraISO 2018/8/14 16:06 快捷方式
WinSCP 2017/9/28 8:59 快捷方式
winscp517.rar 2017/9/28 11:09 WinRAR 压缩文件
XMind 2018/5/30 9:42 快捷方式
百度网盘 2017/12/8 13:51 快捷方式
堡垒机.zip 2018/9/18 14:29 WinRAR ZIP 压缩
工作 2017/9/22 13:09 快捷方式
海关漏洞修复.zip 2018/9/26 8:28 WinRAR ZIP 压缩
记录.txt 2018/9/26 14:44 UltraEdit Docum
文件名(N): winscp517.rar
所有文件 (*.*)
打开(O)
取消

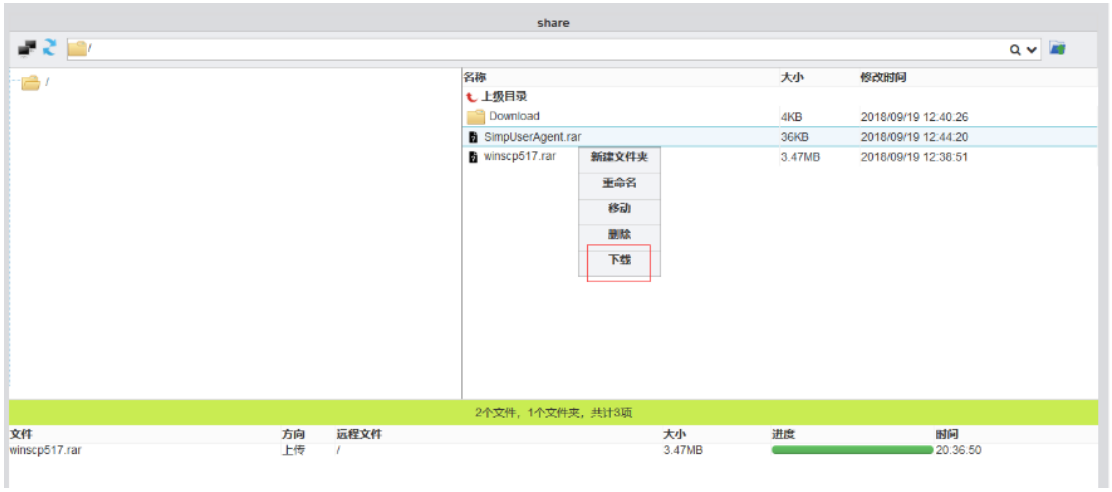


传输完成后在单点登陆界面打开我的电脑“个人共享目录”获取上传的文件：





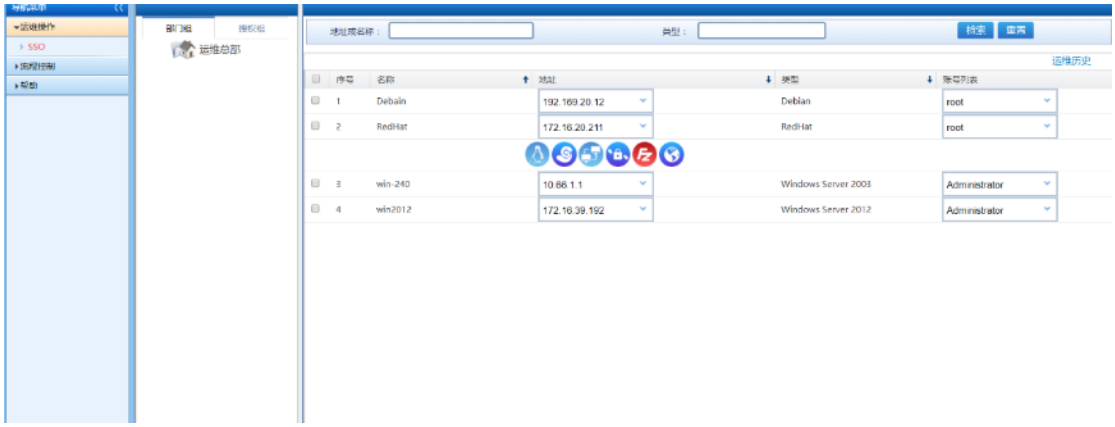
在该目录将文件拷贝到需要目录下使用，如果需要从服务传输文件到客户端电脑，则反向操作，先将文件从服务器目录拷贝到个人共享目录下，然后到文件传输界面点击下载操作即可：



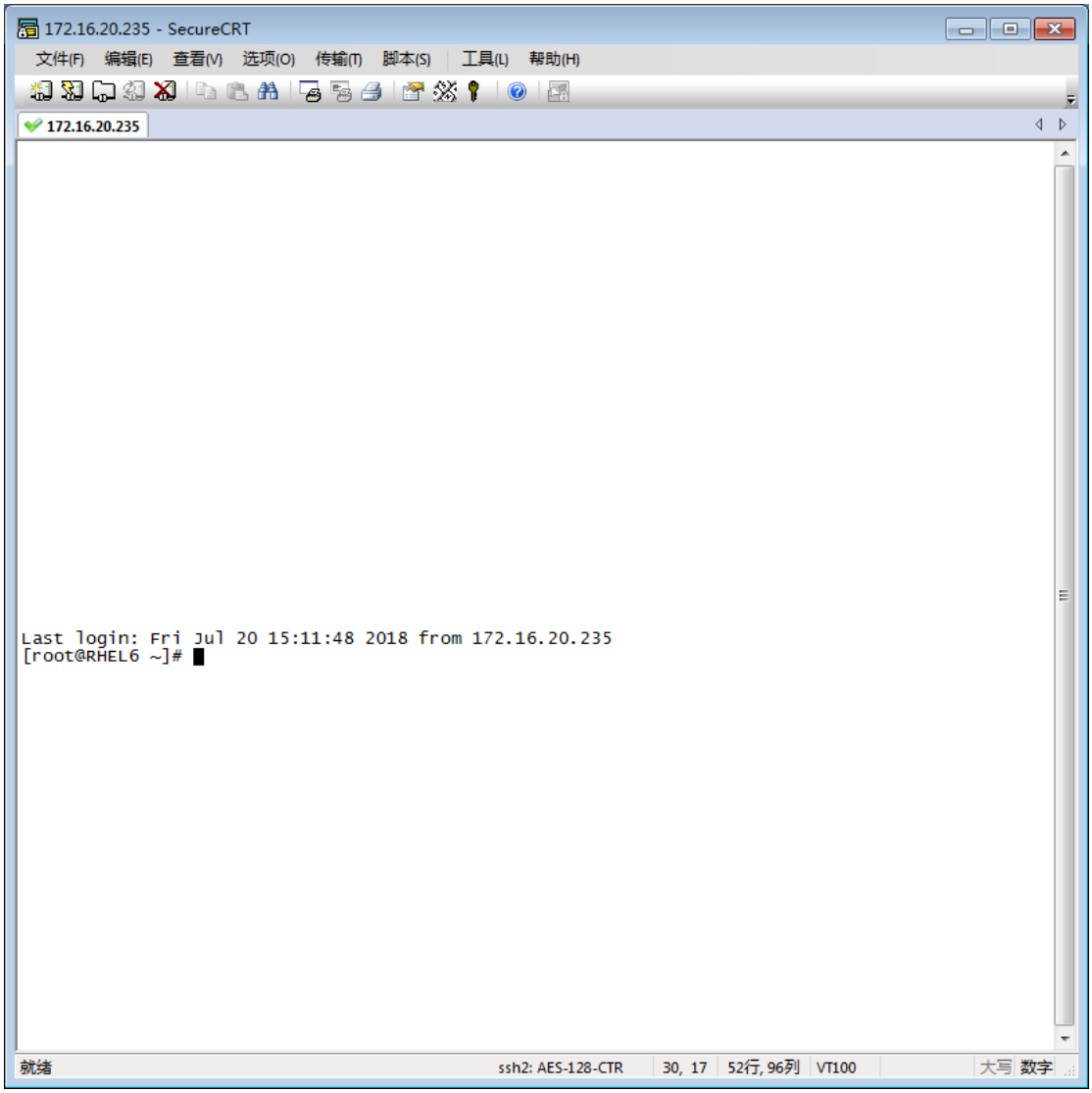
6.2. linux 类型资源

6.2.1. 自动代填账号和口令

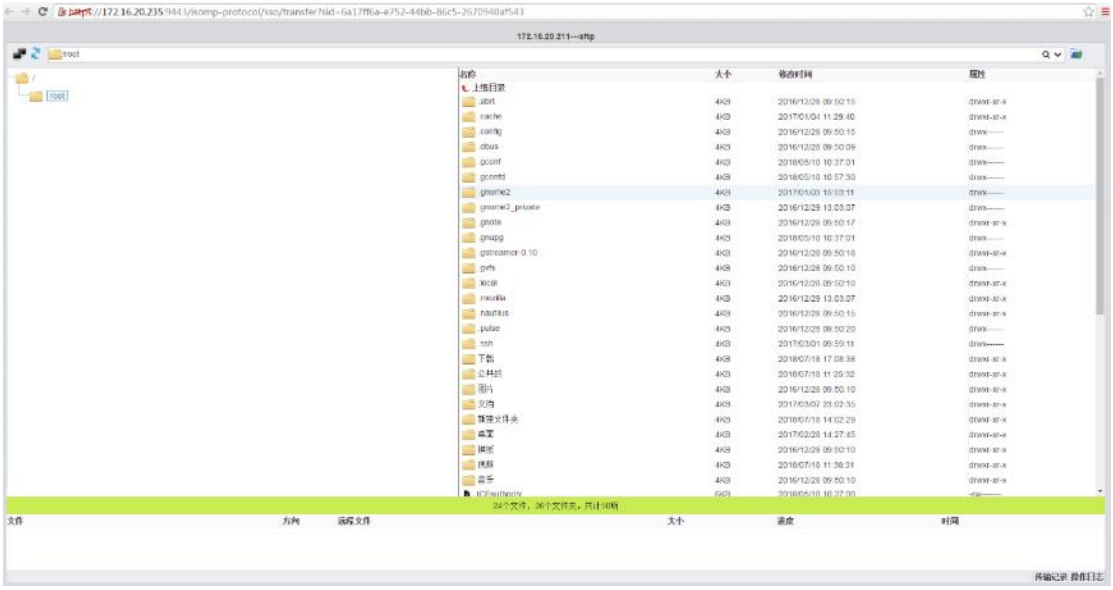
登录系统后点击运维操作-> SSO ->部门组->运维总部。



点击  图标，连接到 linux 资源。

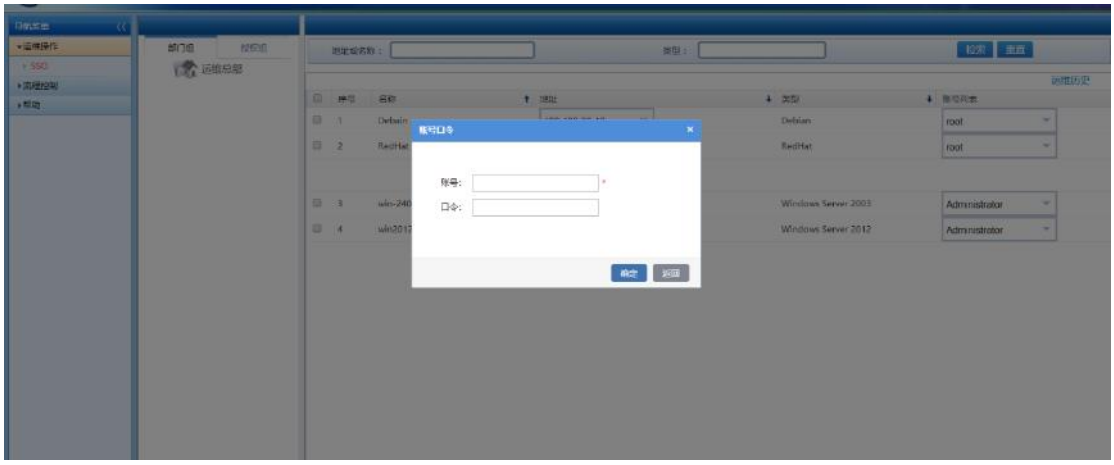


点击  图标，打开 SFTP 文件传输页面。

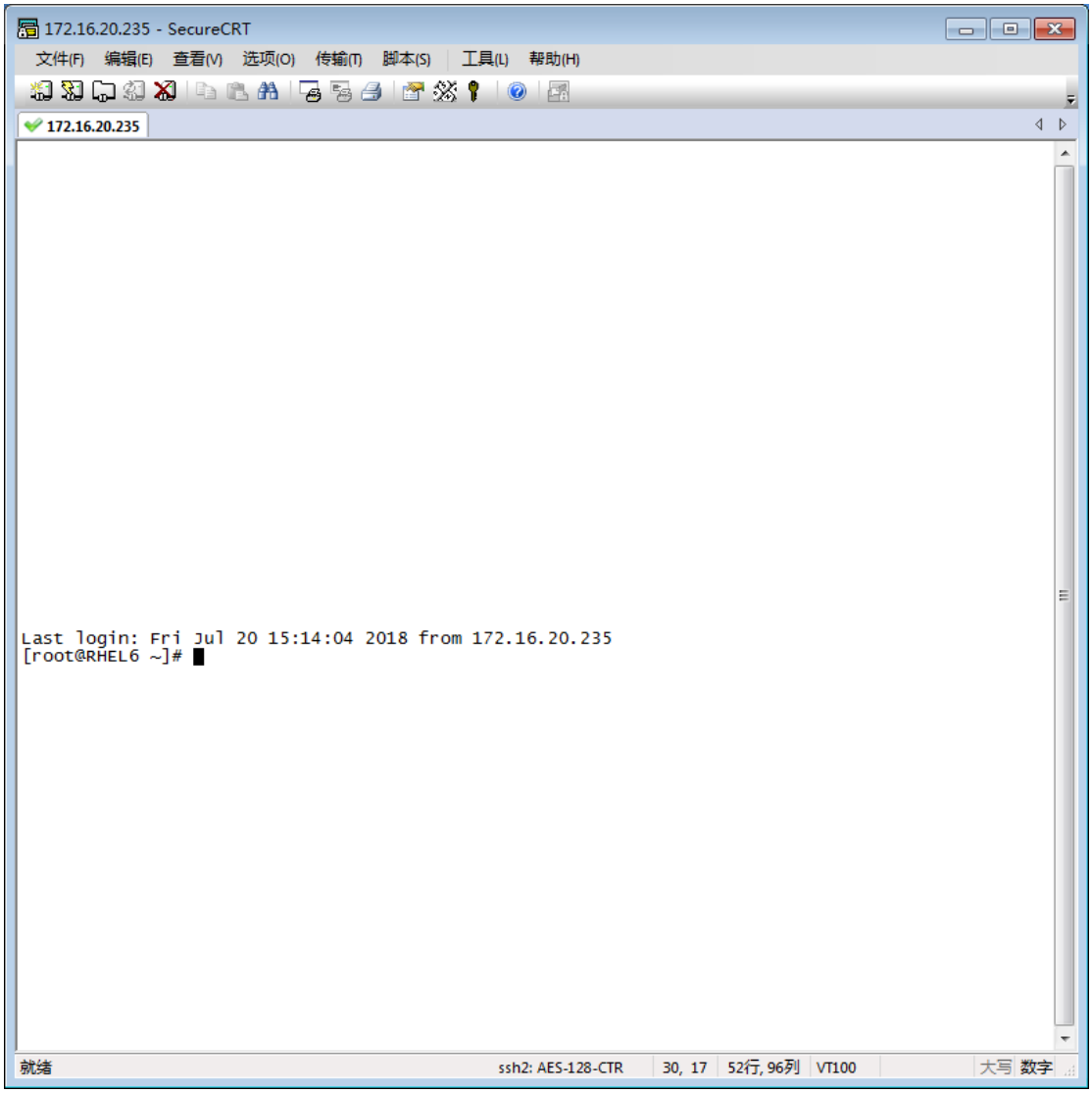


6.2.2. 手动输入账号和口令

点击  图标，手动输入账号和口令。

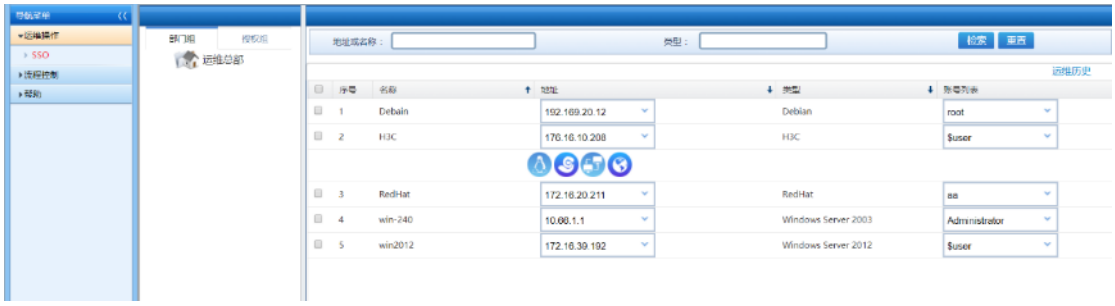


点击确定按钮，进入 linux 单点登陆界面。

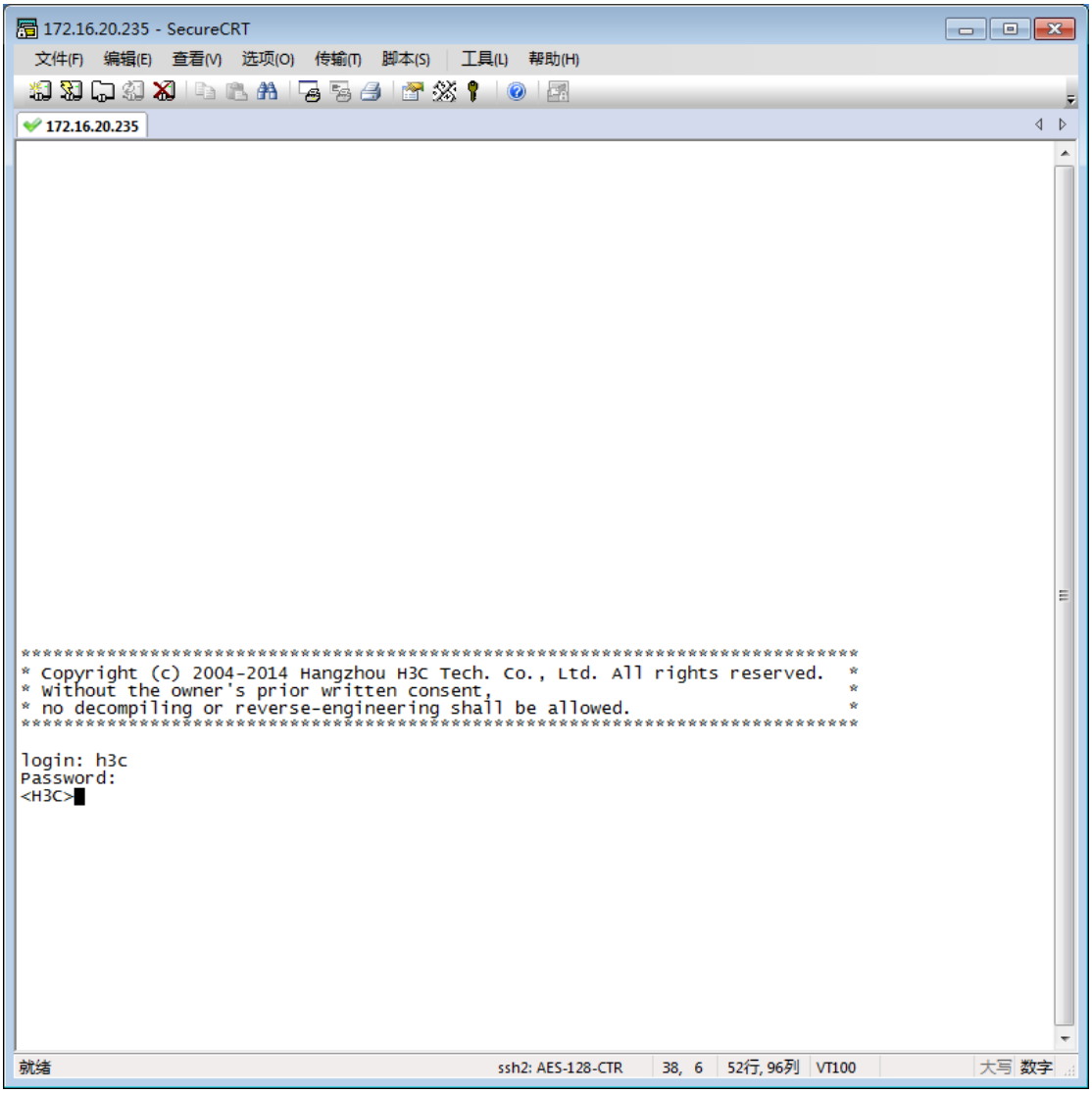


6.3. 网络设备类型资源

登录系统后点击运维操作-> SSO ->部门组->运维总部。



点击  图标，使用 telnet 协议登陆到网络设备。

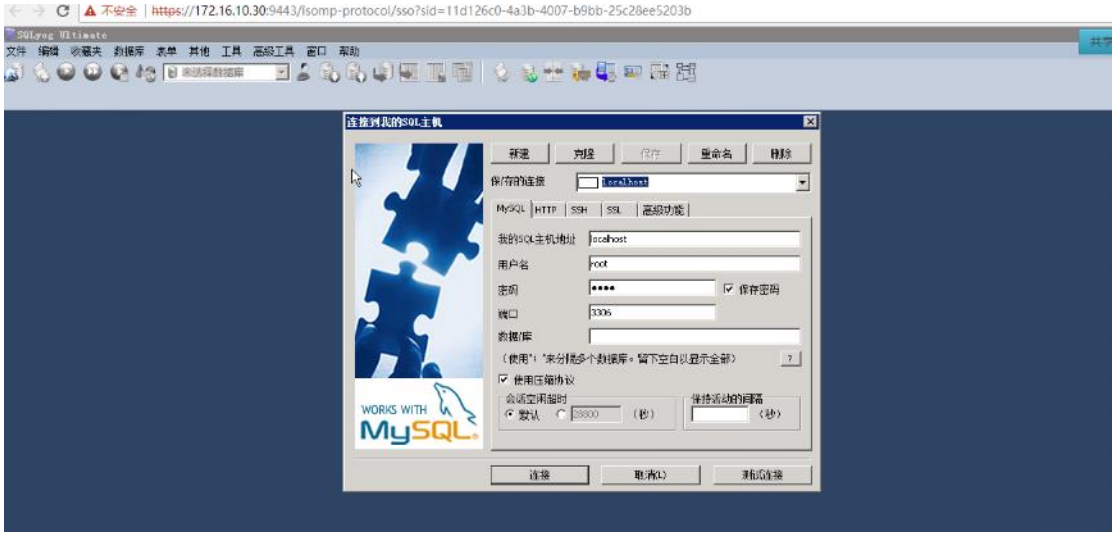


图

6.4. 数据库类型资源

登录系统后点击运维操作-> sso ->部门组->运维总部。

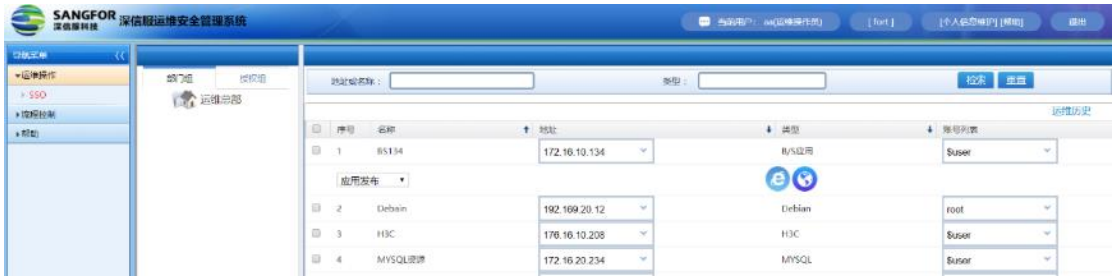
点击  图标，远程登录服务器，自动代填 mysql 资源的账号和口令登录完成。



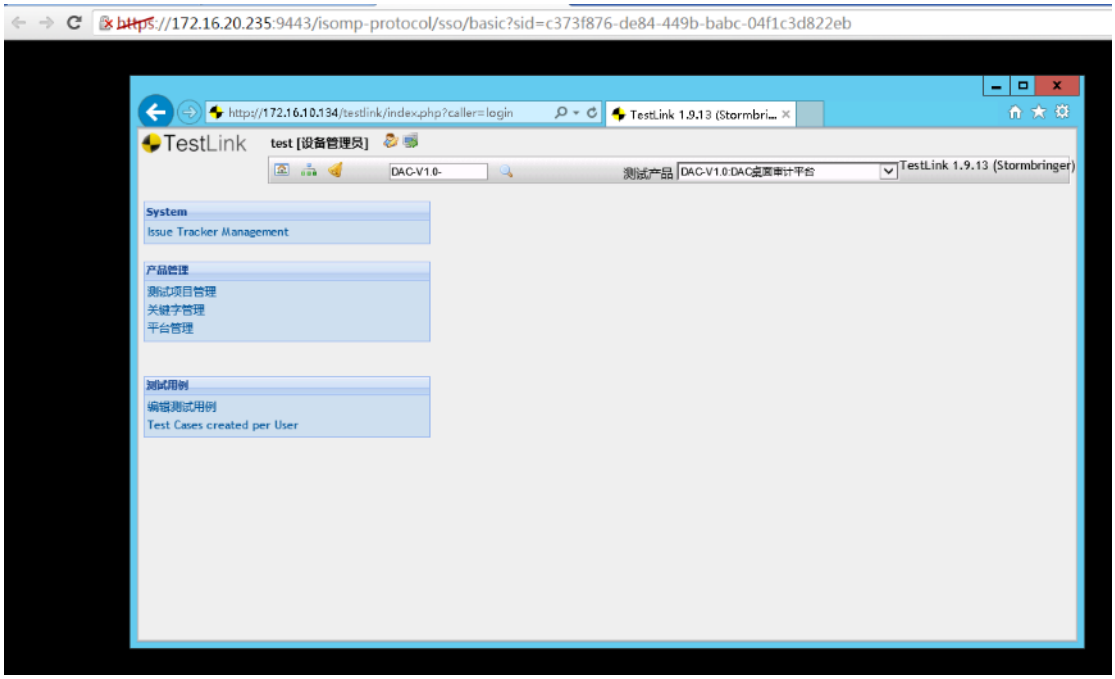
6.5. 应用系统类型资源

6.5.1. BS 资源类型

登录系统后点击运维操作-> sso ->部门组->运维总部。

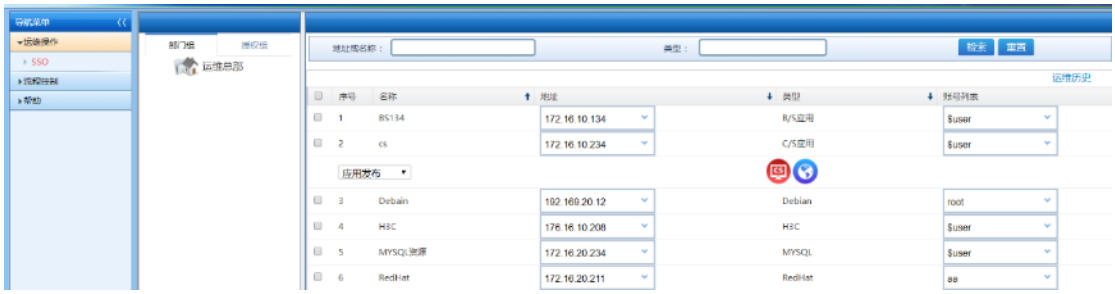


点击  图标，远程登录服务器，自动代填 BS 资源的账号和口令登录完成。

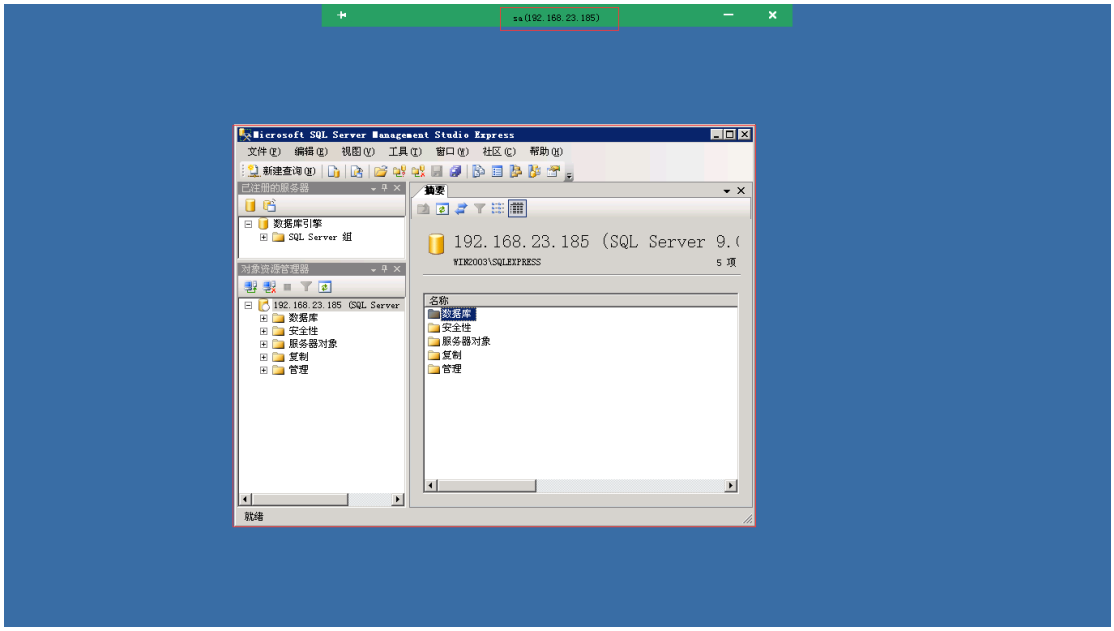


6.5.2. 资源类型

登录系统后点击运维操作-> sso ->部门组->运维总部。



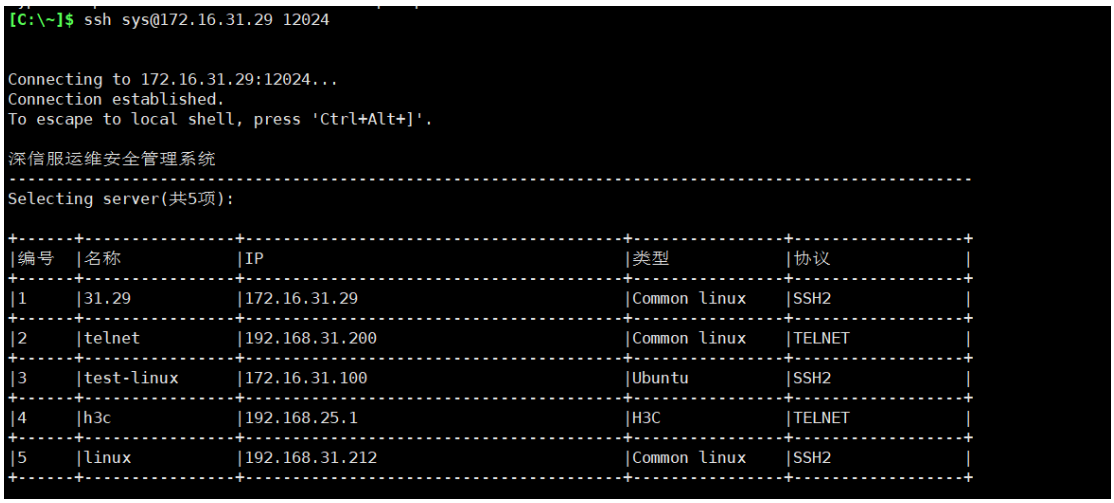
点击  图标，远程登录服务器，自动代填 CS 资源的账号和口令登录完成。



6.6. 命令直连菜单

命令直连菜单，包含 ssh、telnet 协议的支持。

打开 xshell 工具，命令行输入 ssh sys@172.16.31.29 12024（172.16.31.29 为堡垒地址），回车输入正确的运维管理员账号 sys 的登陆密码。登录成功，展示已授权的资源列表页



输入 172.16.31.29 资源的编号 1，进入下一步选择资源账号

```
可选命令:  t根据类型过滤资源;  n 下一页; m 上一页; g 关键字模糊查找; exit 退出菜单
Selecting server:1
+------+--------------------------------------+
|0     |返回上一层                            |
+------+--------------------------------------+
|1     |$user                                 |
+------+--------------------------------------+
|2     |root                                  |
+------+--------------------------------------+
```

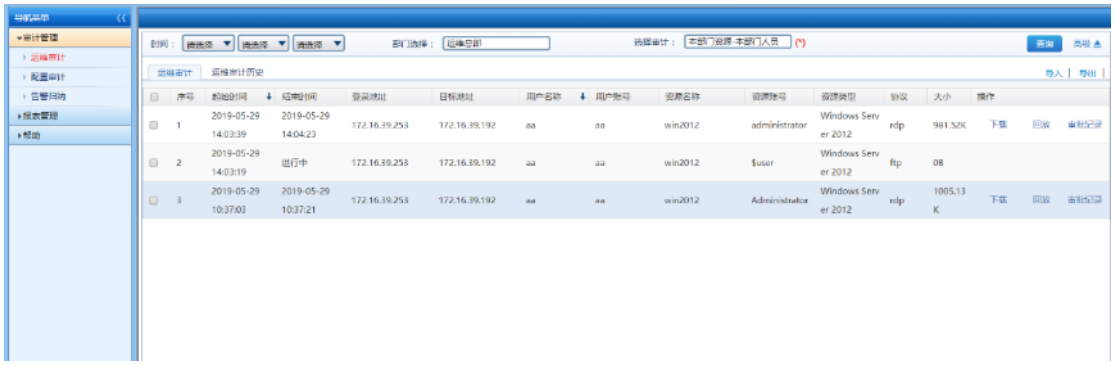
选择资源账号 root，输入正确的资源编号 2 及密码，root 账号登陆成功

```
可选命令:  t根据类型过滤资源;  n 下一页; m 上一页; g 关键字模糊查找; exit 退出菜单
Selecting server:1
+------+--------------------------------------+
|0     |返回上一层                            |
+------+--------------------------------------+
|1     |$user                                 |
+------+--------------------------------------+
|2     |root                                  |
+------+--------------------------------------+
Select: 31.29(172.16.31.29) -> Selecting Account:2
Last login: Wed Nov  6 16:07:09 2019 from 172.16.31.29
root@fort:~#
```

7. 运维审计

运维审计主要由检索、回放、监控、阻断、下载、剪切板、键盘记录、文件传输、命令详情等功能组成。

用审计管理员 sysAudit 登录系统，点击审计管理->运维审计链接进入运维审计界面。



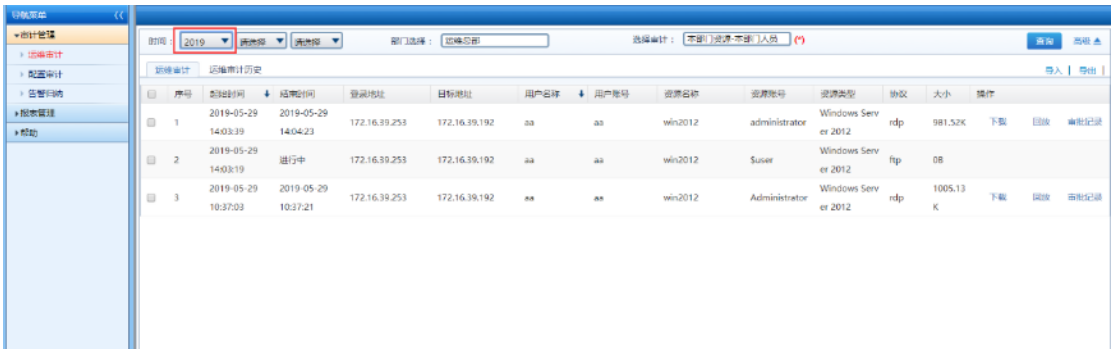
7.1. 运维审计-检索

运维审计检索可以根据时间、部门进行普通检索，还可以根据运维协议、资源类型、资源帐号、用户名称、目标 IP/名称、起始时间、结束时间、登录 IP、用户帐号进行高级检索。

7.1.1. 普通检索

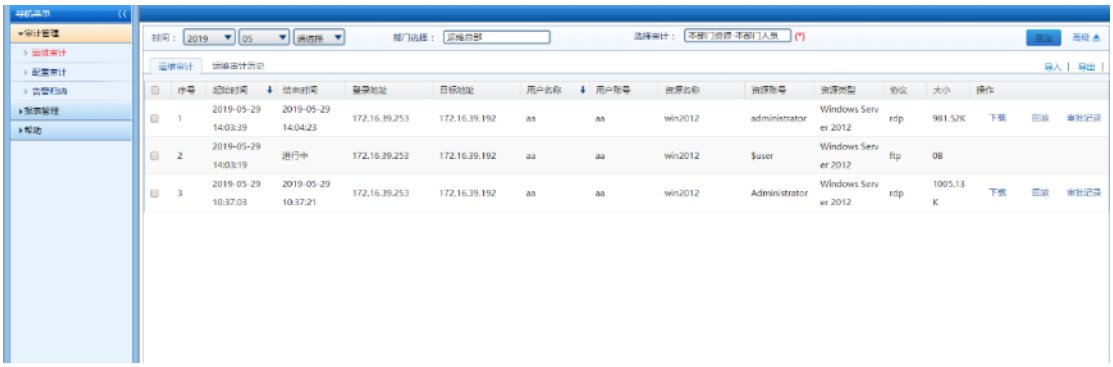
1.按年检索

选择 2019 年，点击检索按钮，即可查询到 2019 年的运维审计记录。



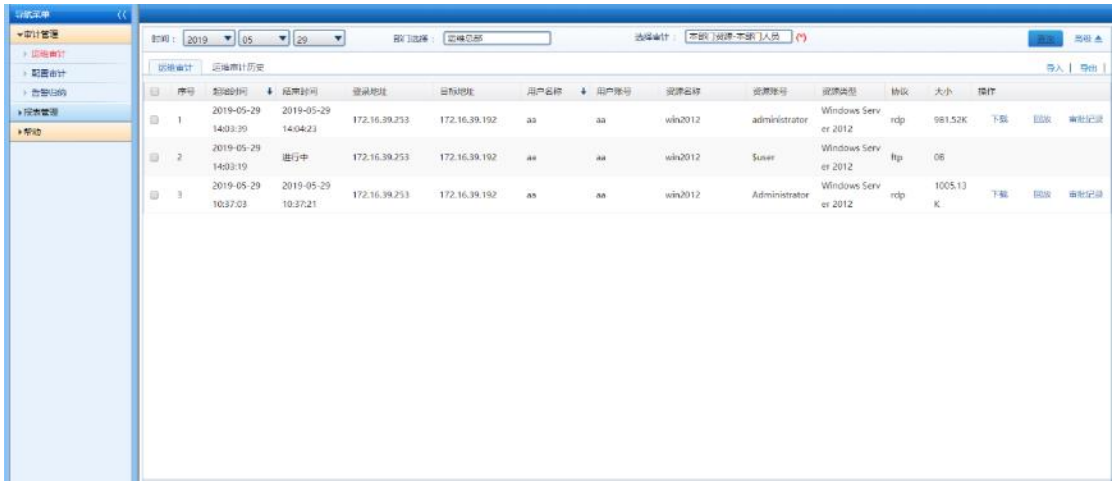
2.按月检索

选择 2019 年 05 月，点击检索按钮，即可查询到 2019 年 05 月的运维审计记录。



3.按日检索

选择查询时间 2019 年 05 月 29 日，点击检索按钮，即可查询到 2019 年 05 月 29 日的运维审计记录。



4.按部门检索

选择部门运维总部，点击检索按钮，即可查询到运维总部人员的运维审计记录。

7.1.2. 高级检索

1.按运维协议检索

点击高级按钮，选择运维协议 RDP，点击检索按钮，即可查询到运维协议为 RDP 的运维审计记录。

2.按资源类型检索

点击高级按钮，选择资源类型 Windows Server 2012，点击检索按钮，即可查询到资源类型为 Windows Server 2012 的运维审计记录。

3.按资源帐号检索

点击高级按钮，输入资源帐号$user，点击检索按钮，即可查询到资源帐号为$user 的运维审计记录。

4.按用户名称检索

点击高级按钮，输入用户名称 aa，点击检索按钮，即可查询到用户名称为 aa 的运维审计记录。

5.按目标地址/名称检索

点击高级按钮，输入目标地址/名称 172.16.39.192，点击检索按钮，即可查询到目标地址/名称为 172.16.39.192 的运维审计记录。

6.按起始时间检索

点击高级按钮，输入起始时间 2019-05-28 14:15:14，点击检索按钮，即可查询到起始时间在 2019-05-28 14:15:14 之后的运维审计记录。

7.按结束时间检索

点击高级按钮，输入结束时间 2019-05-29 14:16:11，点击检索按钮，即可查询到结束时间在 2019-05-29 14:16:11 之前的运维审计记录。

9.按登录地址检索

点击高级按钮，输入登录地址 172.16.39.253，点击检索按钮，即可查询到登录地址为 172.16.39.253 的运维审计记录。

10.按用户帐号检索

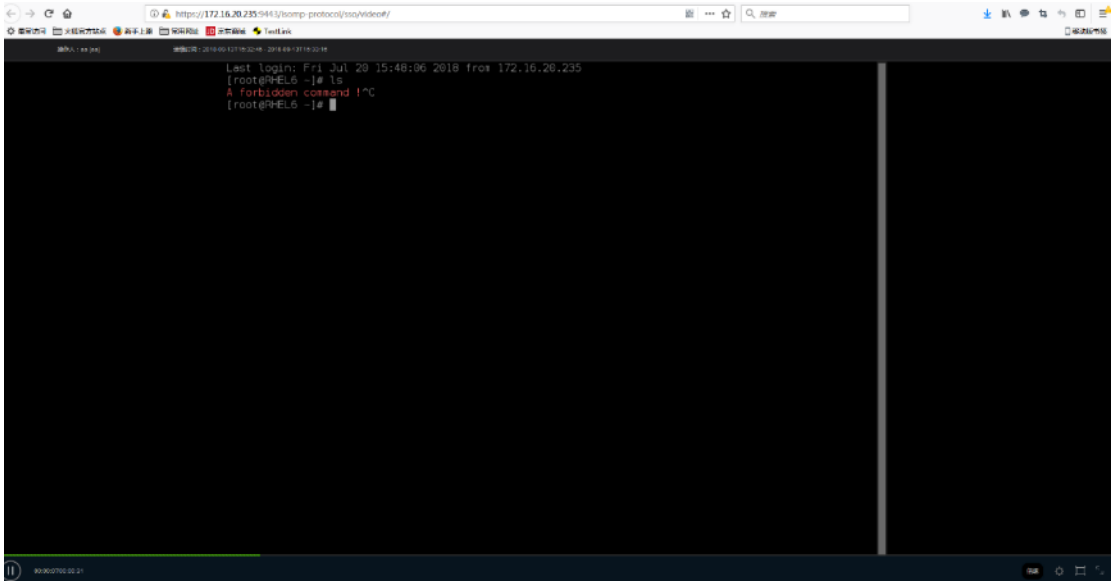
点击高级按钮，输入用户帐号 aa，点击检索按钮，即可查询到用户帐号为 aa 的运维审计记录。

至此运维审计检索功能完成。

7.2. 运维审计-回放

审计回放功能记录着用户进行运维操作的过程。点击运维记录的回放按钮。

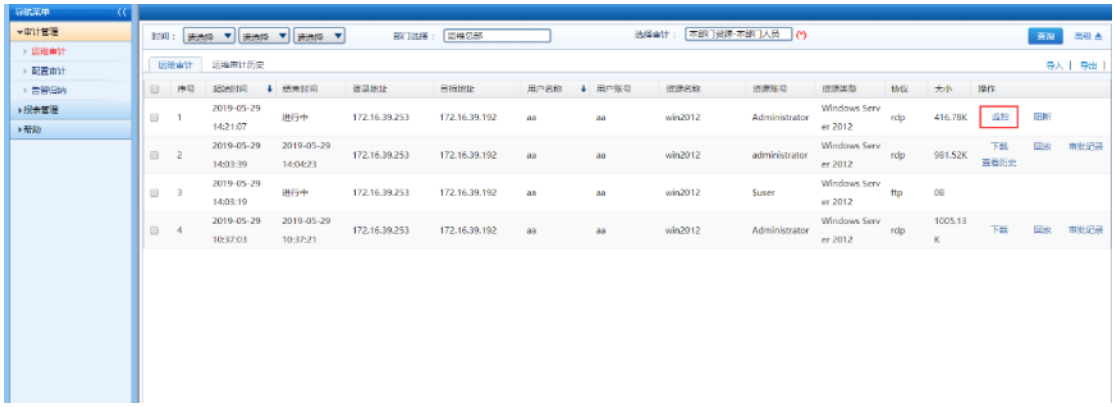
弹出运维操作的录像内容。



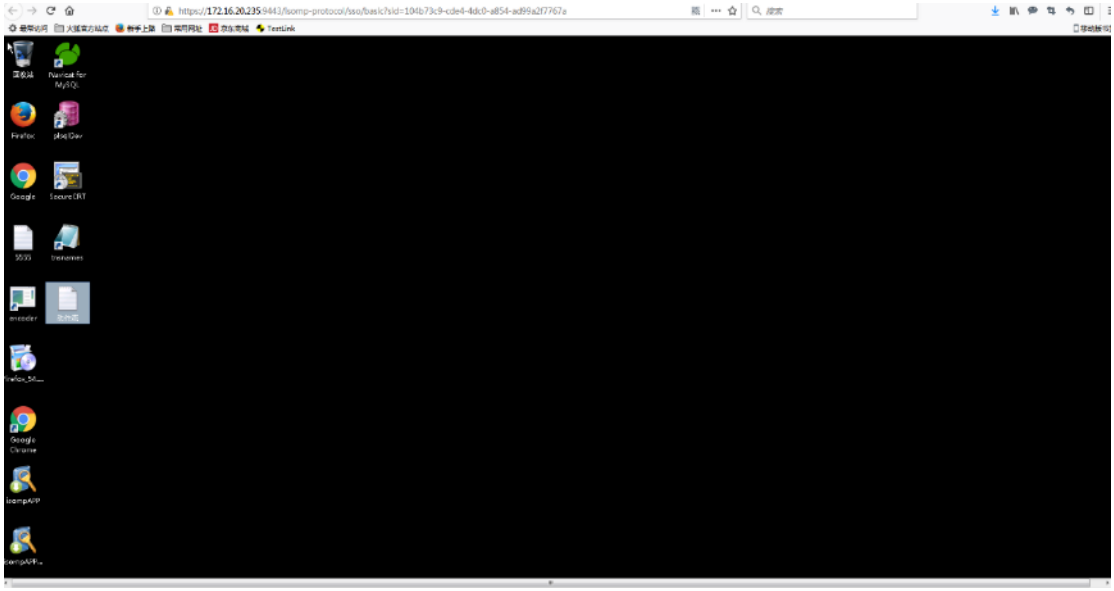
至此运维审计回放功能完成。

7.3. 运维审计-监控

运维审计监控功能可以对正在进行的运维操作过程进行监控。点击运维记录的监控按钮。



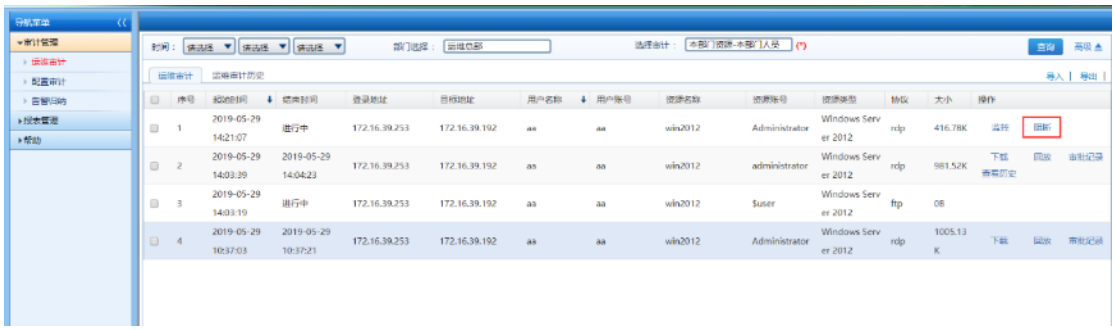
弹出正在进行的运维操作内容。



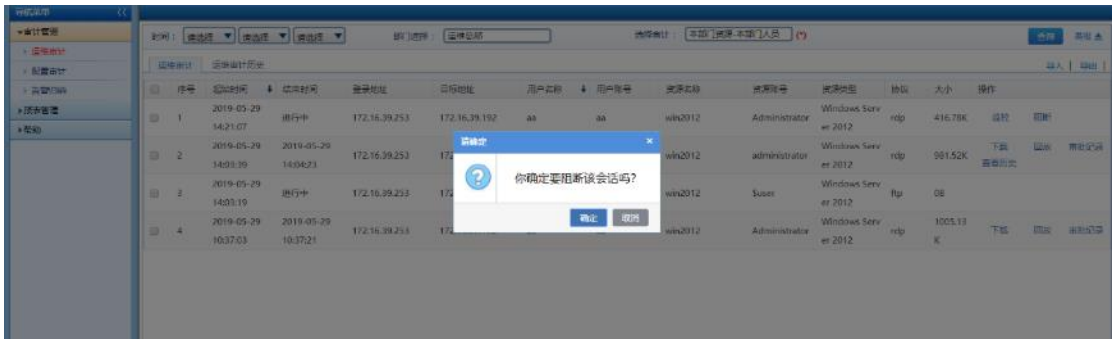
至此运维审计监控功能完成。

7.4. 运维审计-阻断

运维审计阻断功能可以对正在进行的运维操作进行阻断。点击运维记录的阻断按钮。



弹出提示信息你确定要阻断该会话吗？



点击确定按钮，弹出提示信息阻断成功！

运维会话窗口被强制关闭，至此运维审计阻断功能完成。

7.5. 运维审计-下载

运维审计下载功能可以对运维操作的录像文件进行下载。点击运维记录的下载按钮。

弹出提示信息弹出下载框之前请不要做其他操作，否则会中断下载，点击保存按钮，选择文件存储路径下载运维操作录像文件。

下载完成后找到录像文件下载路径，可查看到下载文件。

至此运维审计下载功能完成。

7.6. 运维审计-命令详情

运维审计命令详情功能可以记录运维操作过程中的操作命令，只有 SSH、TELNET 运维协议会产生命令详情。点击运维记录的命令详情按钮。

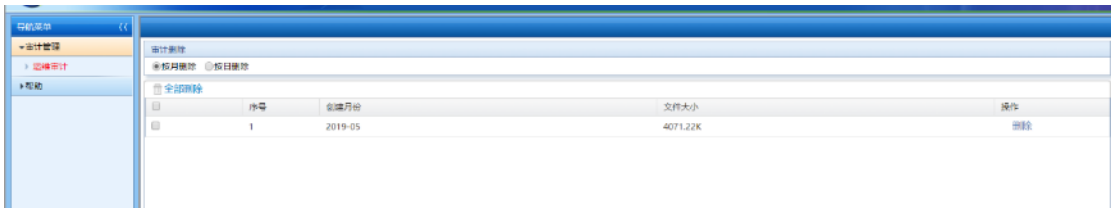
跳转到命令详情页面，查看运维操作过程中的命令详情。

至此运维审计命令详情功能完成。

7.7. 审计删除

用审计删除员 delAudit（拥有系统级审计管理-运维审计权限）登录系统，审计删除功能可以删除运维操作过程中产生的录像文件。点击运审计管理->运维审计->审计删除按钮。

跳转到审计删除页面，可选择按月删除/按日删除。



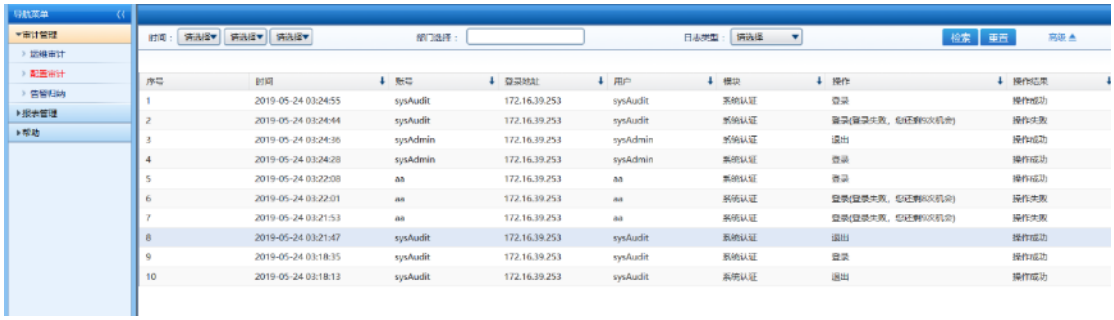
8. 配置审计

8.1. 配置审计概述

配置审计主要记录了用户的登录认证、内部操作、配置变更、计划任务等配置信息。

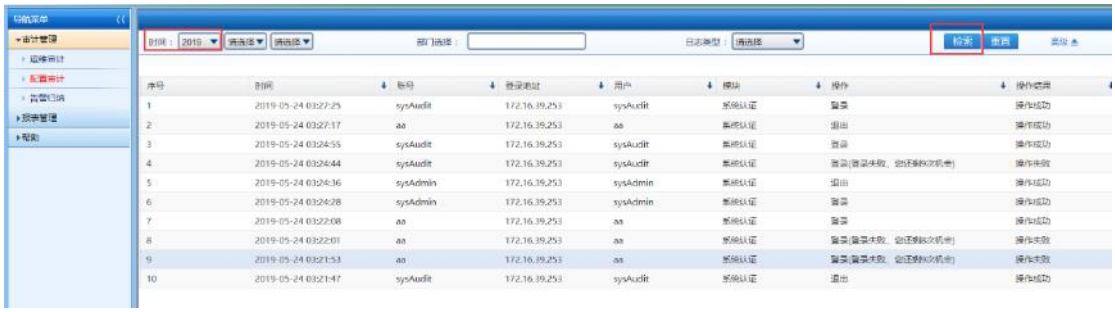
8.2. 配置审计-检索

用审计管理员 sysAudit 登入系统后，点击审计管理->配置审计菜单进入配置审计界面开始查询。



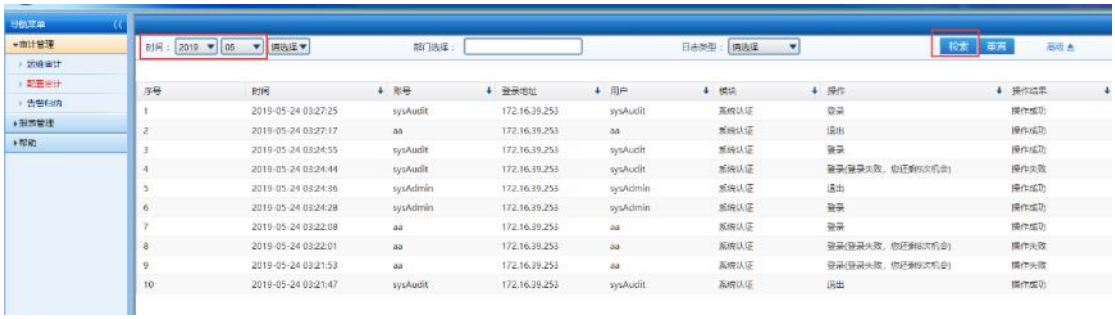
8.2.1. 按年检索

选择 2019 年，点击检索按钮，即可查询到 2019 年的配置审计记录。



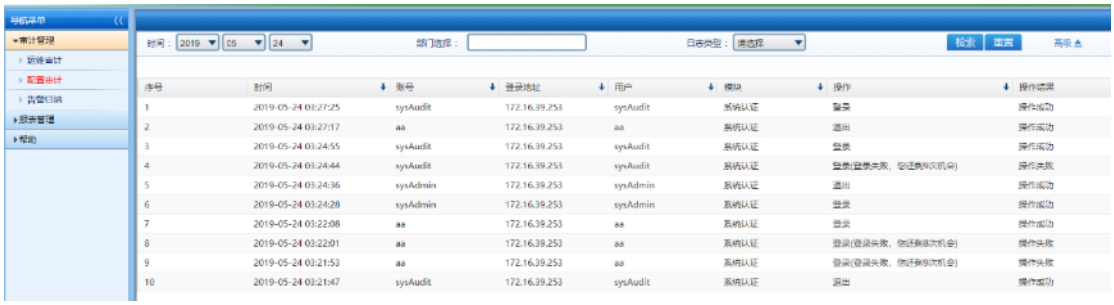
8.2.2. 按月检索

选择 2019 年 5 月，点击检索按钮，即可查询到 2019 年 5 月的配置审计记录。



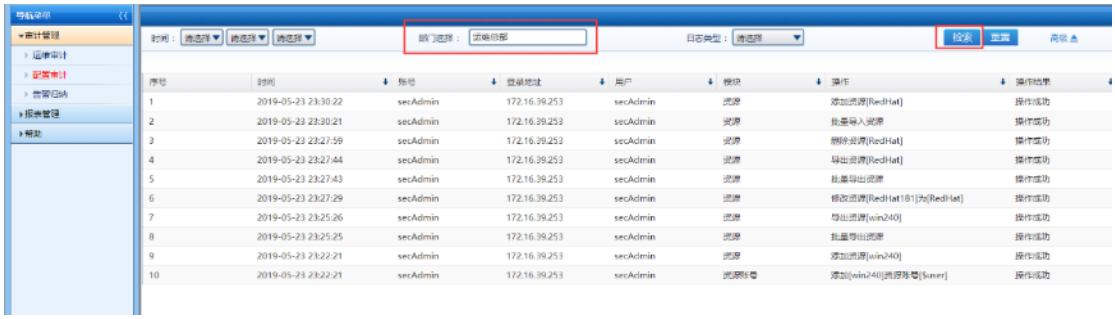
8.2.3. 按日检索

选择查询时间 2019 年 05 月 24 日，点击检索按钮，即可查询到 2019 年 05 月 24 日的配置审计记录。



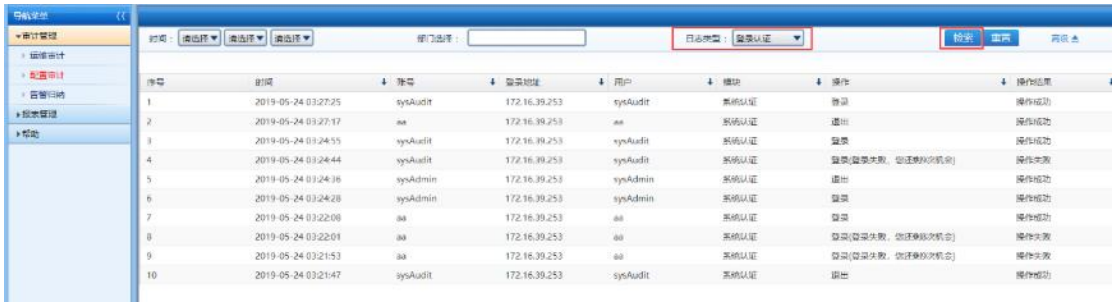
8.2.4. 按部门检索

选择部门运维总部，点击检索按钮，即可查询到运维总部人员的配置审计记录。



8.2.5. 按日志类型检索

选择日志类型登录认证，点击检索按钮，即可查询到登录认证用户的配置审计记录。



9. 流程

流程功能是为了保障运维操作的安全和规范，使运维操作的整体过程可控。运维操作时，需进行事前申请，审批通过后，方可进行运维操作。

9.3. 审批类型

审批类型包含双人授权、命令审批、访问审批、审计下载审批四种类型。

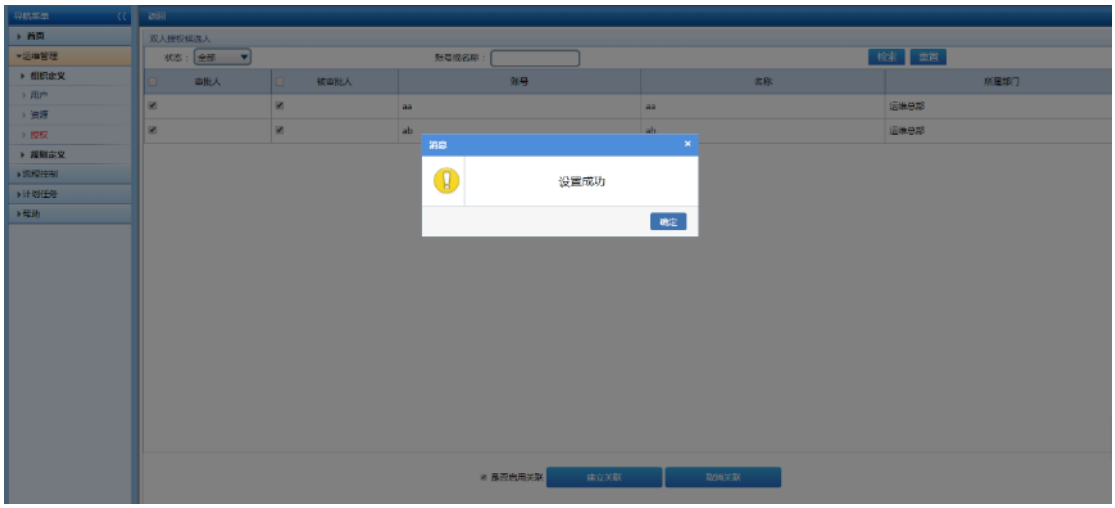
9.3.1. 双人授权

双人授权功能是运维操作员进行运维操作时，经授权人通过审批，才可以进行运维操作。（同一个用户可以被设置为审批人和被审批人，如果只有本身一个审批人则无需进行双人审批，如果有其他审批人，则只能选择其他审批人进行审批。）

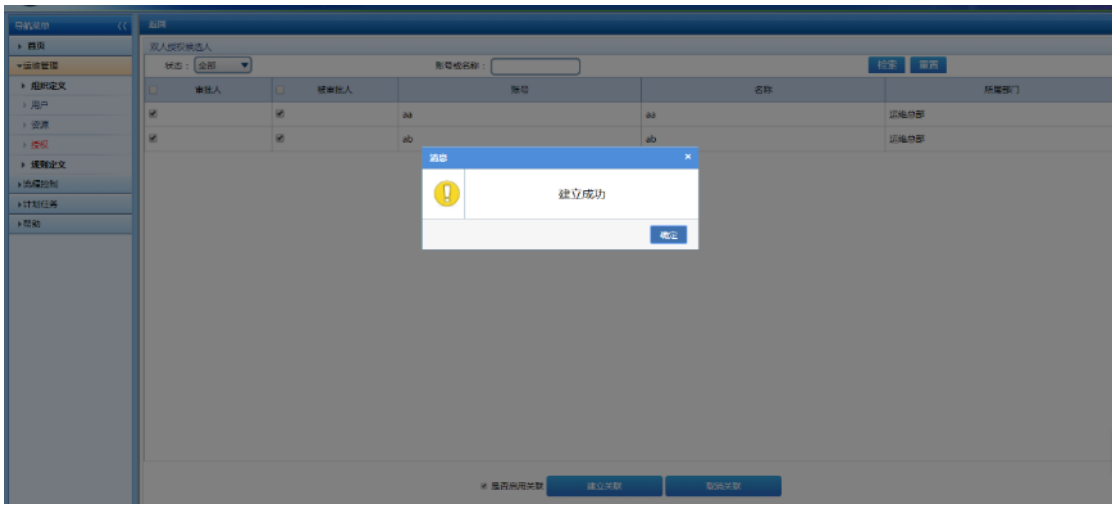
用安全管理员 secAdmin 登录系统，点击运维管理->授权建立流程测试授权 。

在授权列表页面，点击双人授权候选人按钮，弹出双人授权候选人选择窗口。

勾选审批人和被审批人选框，再次勾选是否启用关联单选框，弹出提示窗口。

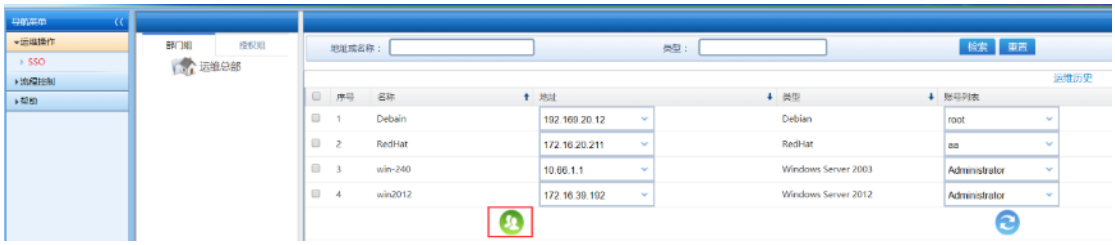


点击确定按钮，点击建立关联按钮，弹出提示窗口。



点击确定按钮，回到双人授权候选人选择页面，点击返回按钮，回到授权列表页面。页面显示双人授权候选人(2/2/2)，所代表含义是双人授权候选人 2,双人授权审批人 2,授权总用户数 2。

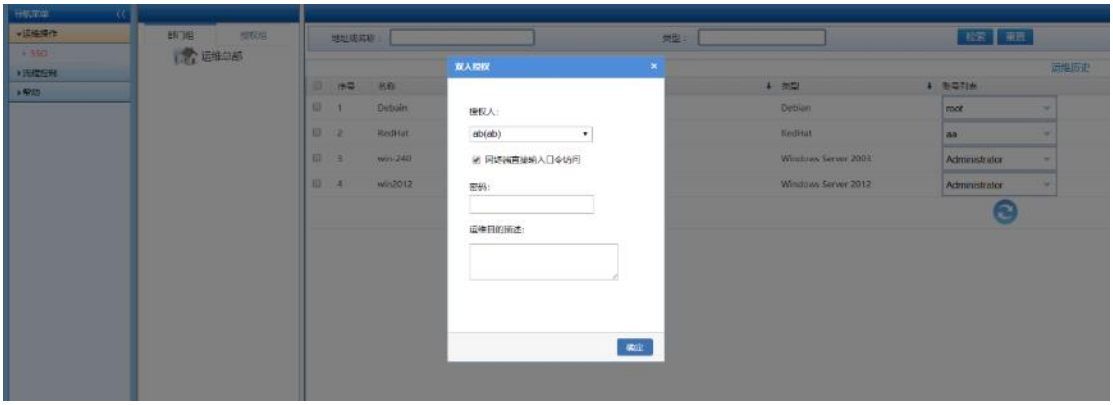
用申请人 aa 运维人员登录系统，登录成功后看到申请人 aa 已被授权的资源单点登录图标变为双人图标。



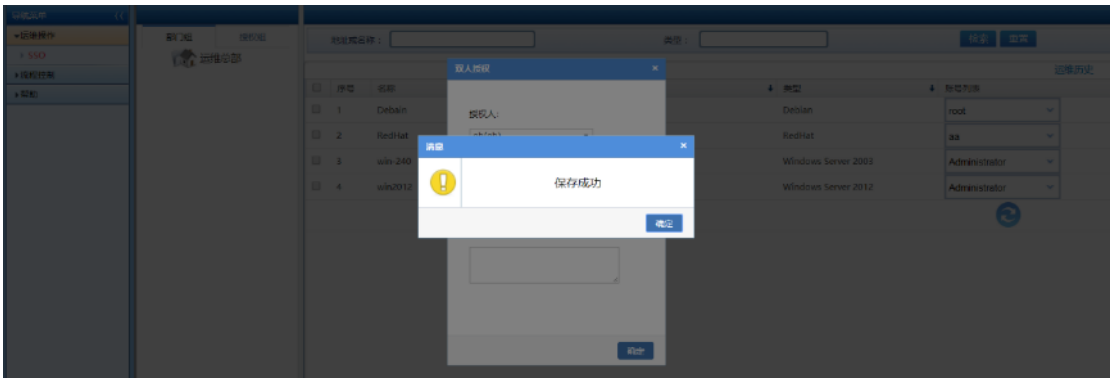
1.同终端审批

同终端审批功能是申请人和审批人在同一台机器上所做的申请和批复操作。

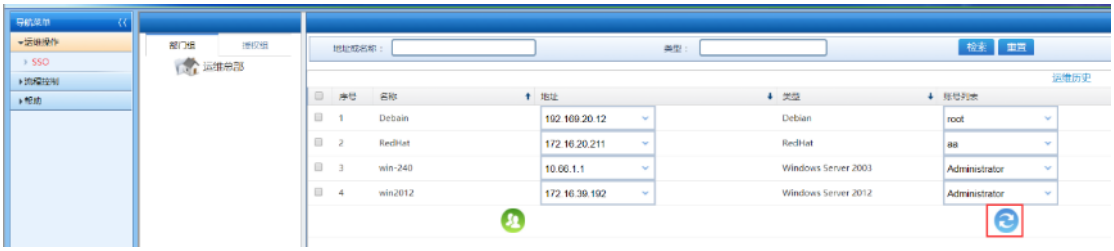
点击  图标，弹出双人授权窗口。



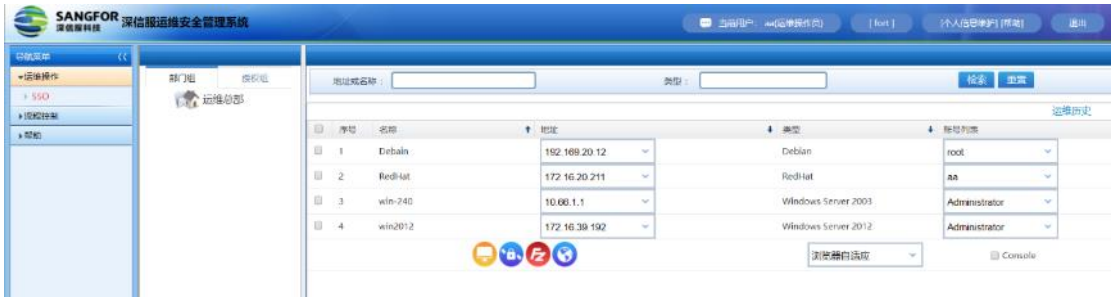
选择审批人 Audit，勾选同终端审批，输入密码，填写运维目的描述，点击确定按钮，弹出提示窗口。



点击确定按钮。跳转到运维操作->SSO 页面。



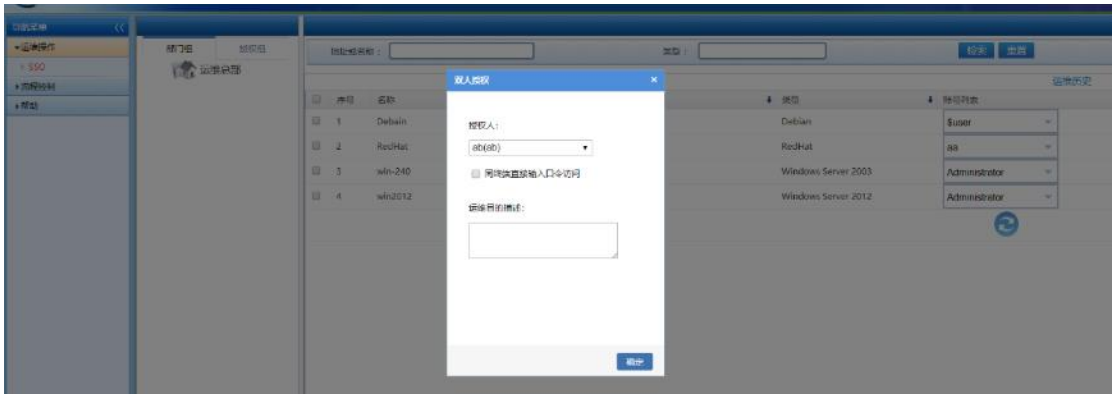
点击  按钮，双人授权图标变为单点登录图标。



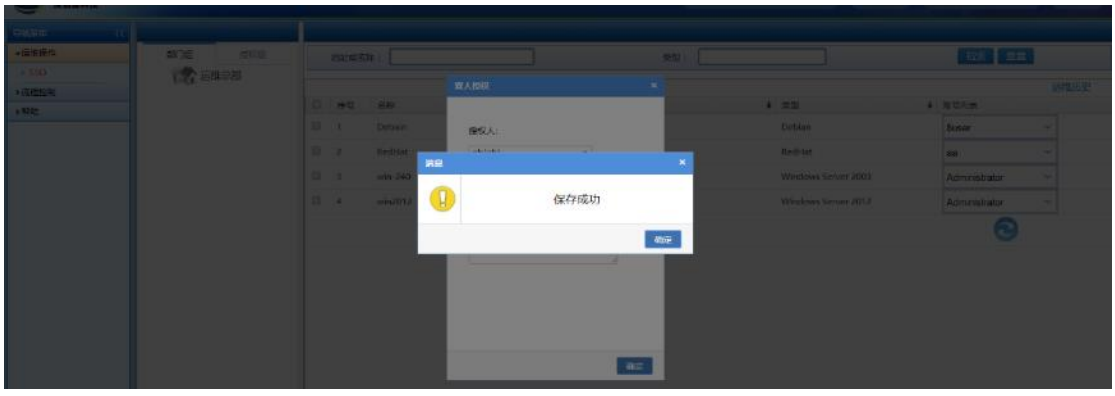
2.异终端审批

终端审批功能是申请人和审批人在不同机器上所做的申请和批复操作。

点击  图标，弹出双人授权窗口。

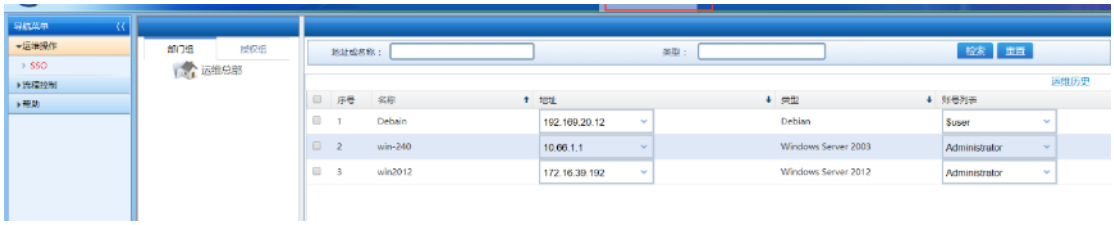


选择审批人 operator，不勾选同终端审批，填写运维目的描述，点击确定按钮，弹出提示窗口。



点击确定按钮，跳转到运维操作->SSO 页面。

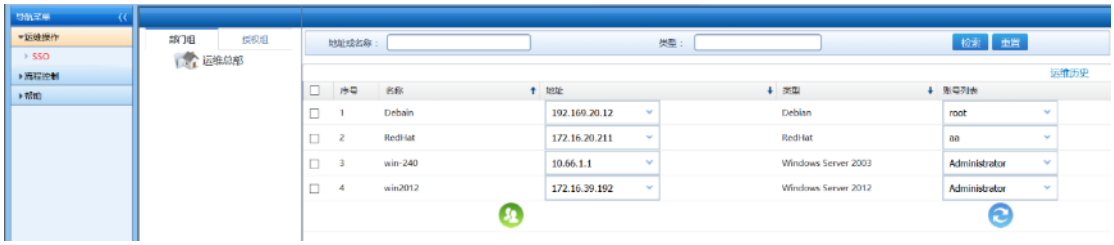
使用审批人 operator 登录系统，页面弹出一条消息提示。



➢ 拒绝申请

点击消息的详情按钮，弹出审批申请单窗口，选择拒绝，点击确定。

申请人 aa 登录系统页面会弹出一条消息提示。



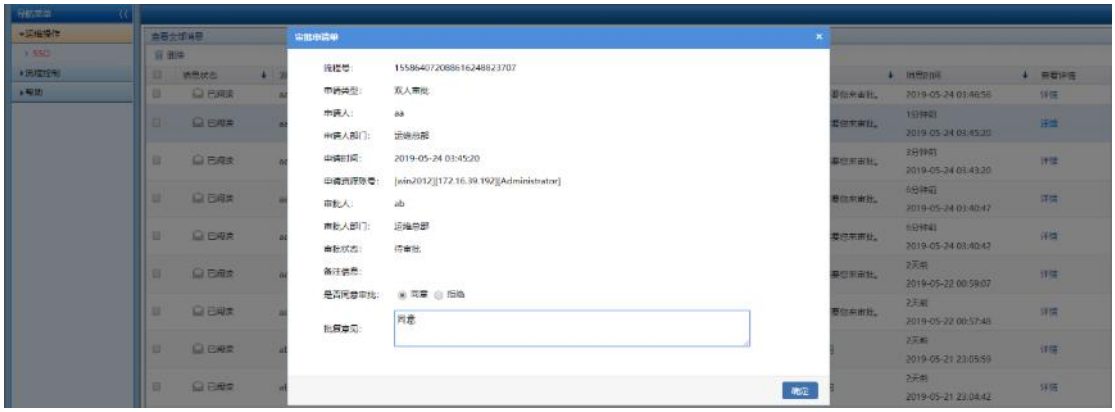
点击消息的详情按钮，申请未通过。

➢ 已过期申请

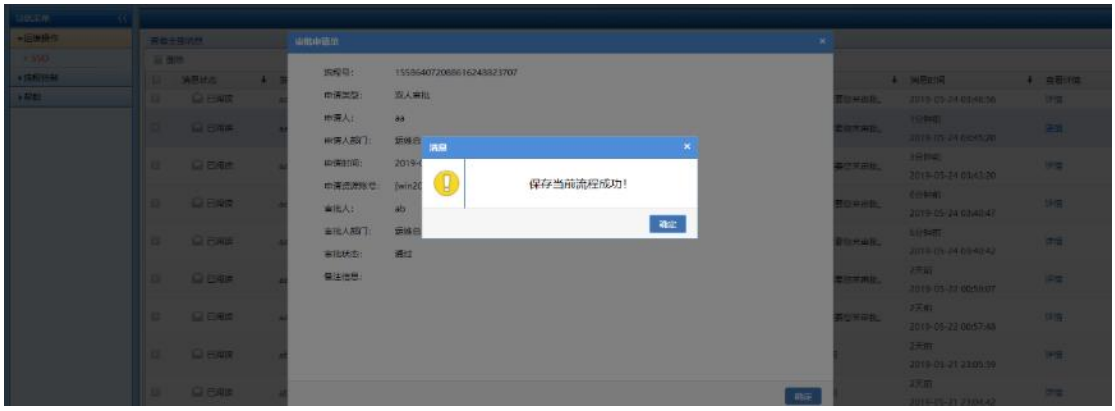
申请人 aa 退出系统后，审批人 operator 登录系统点击消息的详情按钮，弹出审批申请单窗口。

➢ 同意申请

点击消息的详情按钮，弹出审批申请单窗口。

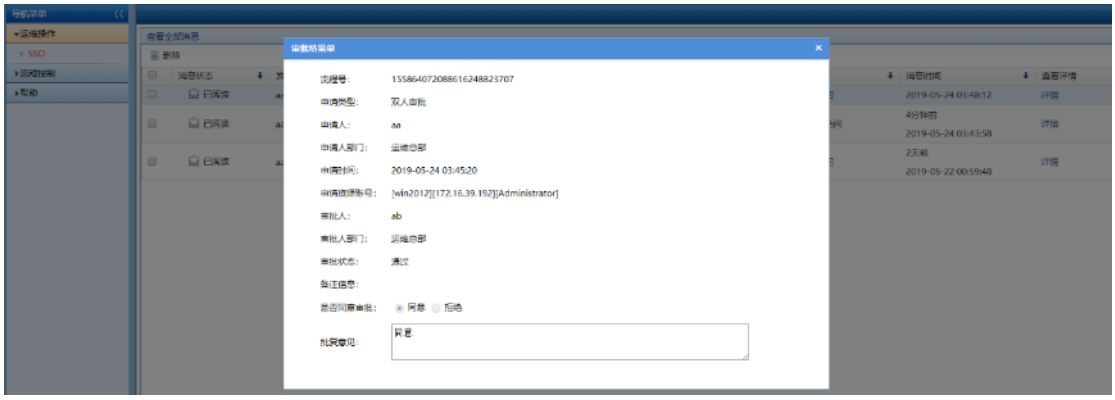


选择同意单选按钮，点击确定按钮，弹出提示窗口。

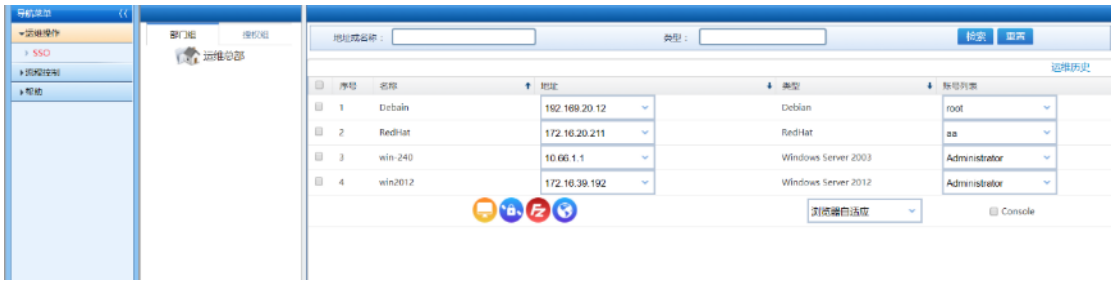


申请人 aa 登录系统页面会弹出一条消息提示。

点击详情按钮，弹出审批结果单窗口。



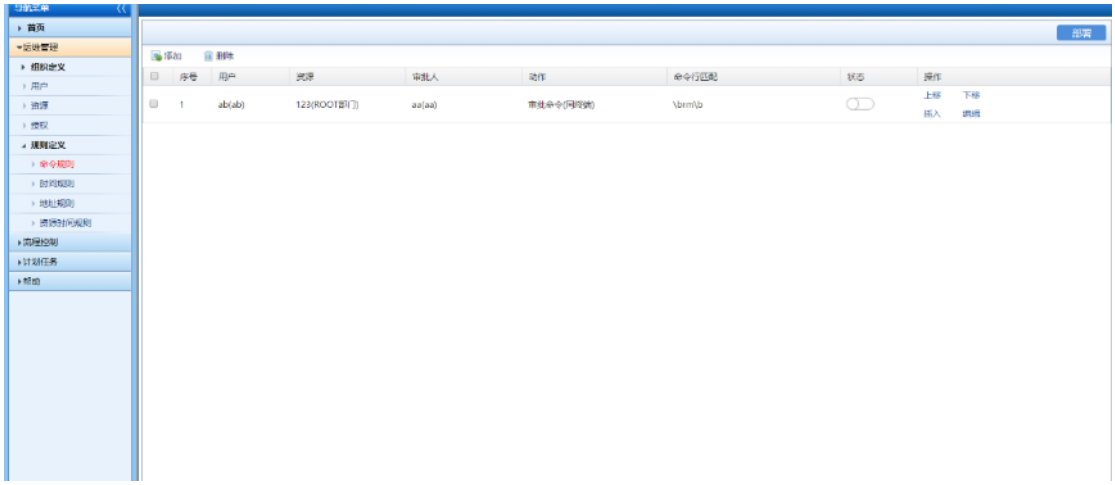
点击  按钮，双人授权图标变为单点登录图标。



9.3.2. 命令审批

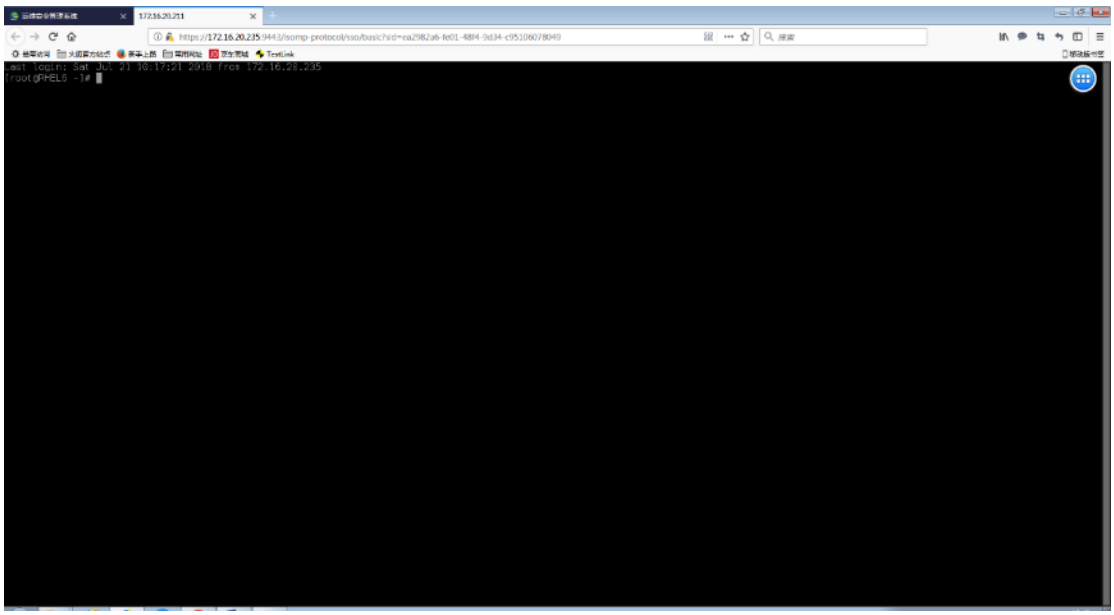
命令审批功能是运维操作员进行运维操作时，对输入的字符型命令进行审批。命令审批属于同终端审批，只给申请人发送消息通知。

用安全管理员 secAdmin 登录系统，点击运维管理->规则定义->命令规则建立命令审批。



使用申请人 aa 登录系统页面。

点击  图标，自动代填账号和口令登录完成。



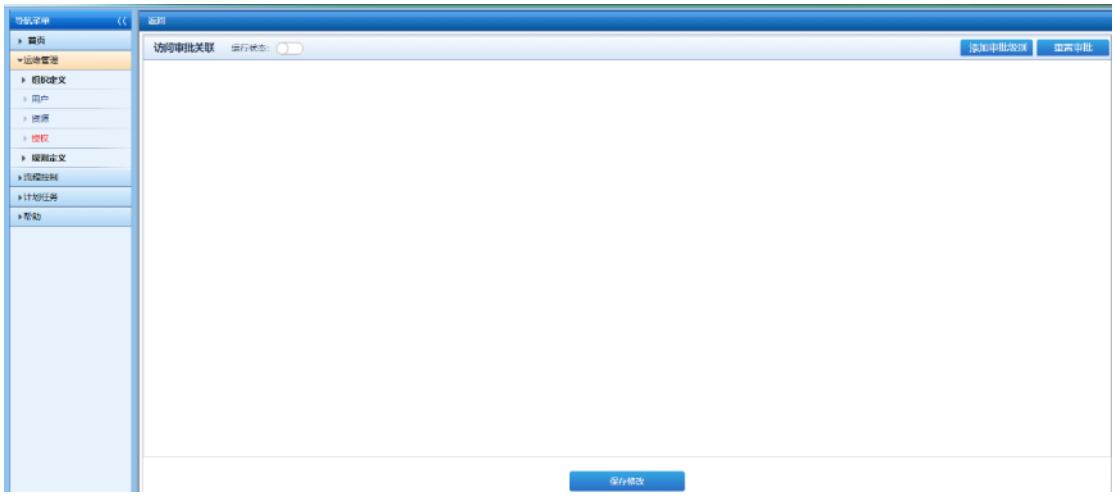
输入需要审批命令 date，点击回车键，系统页面弹出一条消息，提示需要命令审批，按照审批流程执行结束（同意）后方可执行成功，拒绝则执行失败。

9.3.3. 访问审批

访问审批包含上级审批和紧急运维两种。

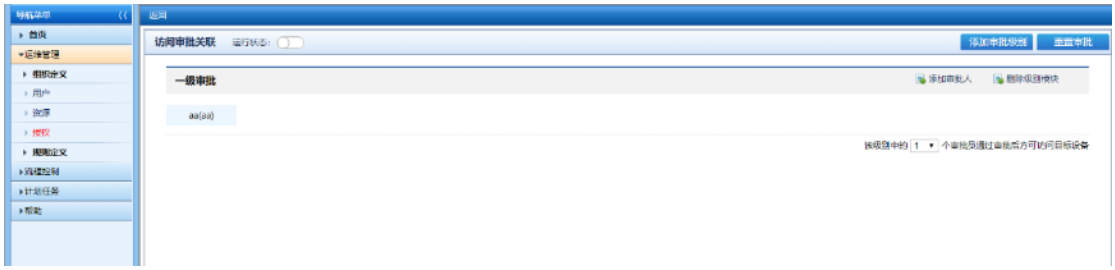
用安全管理员 secAdmin 登录系统，点击运维管理->授权建立访问审批。

点击访问审批按钮，跳转到访问审批关联页面。

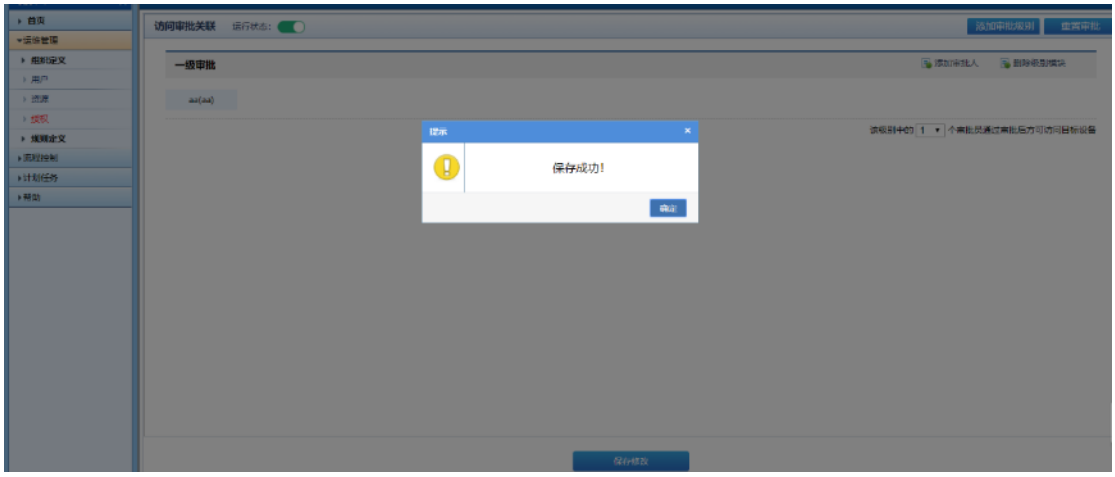


点击添加审批级别按钮，弹出选择审批人窗口。

点击确定按钮，跳转到访问审批关联页面。



打开访问审批关联开关，点击保存按钮。



点击确定按钮后，点击返回按钮，跳转到授权列表页面，页面显示访问审批(1)，所表示含义是访问审批 1 级审批人有 1 人，至少需要 1 人通过。

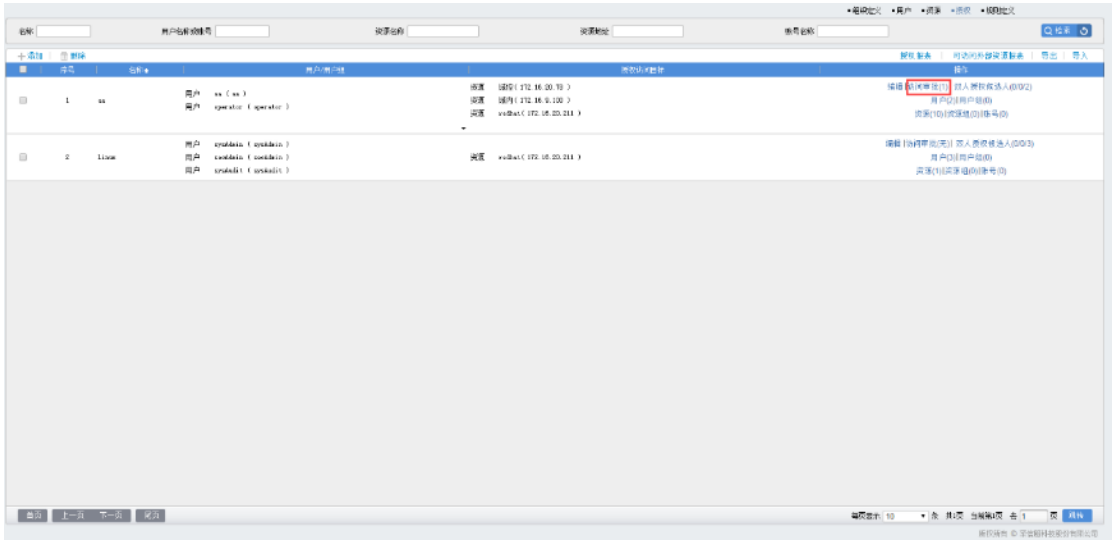
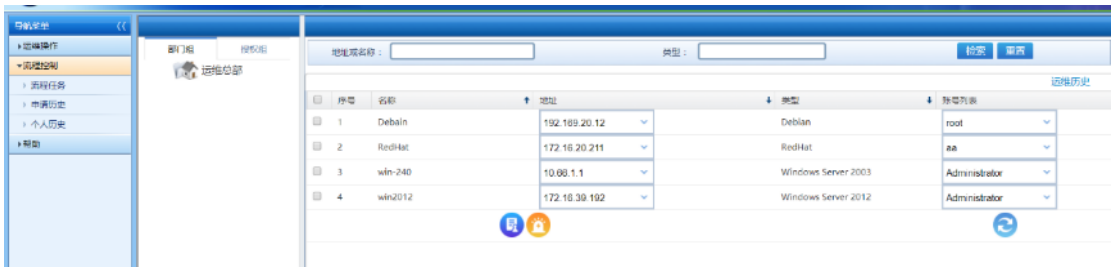


图 3.10.1.3-6

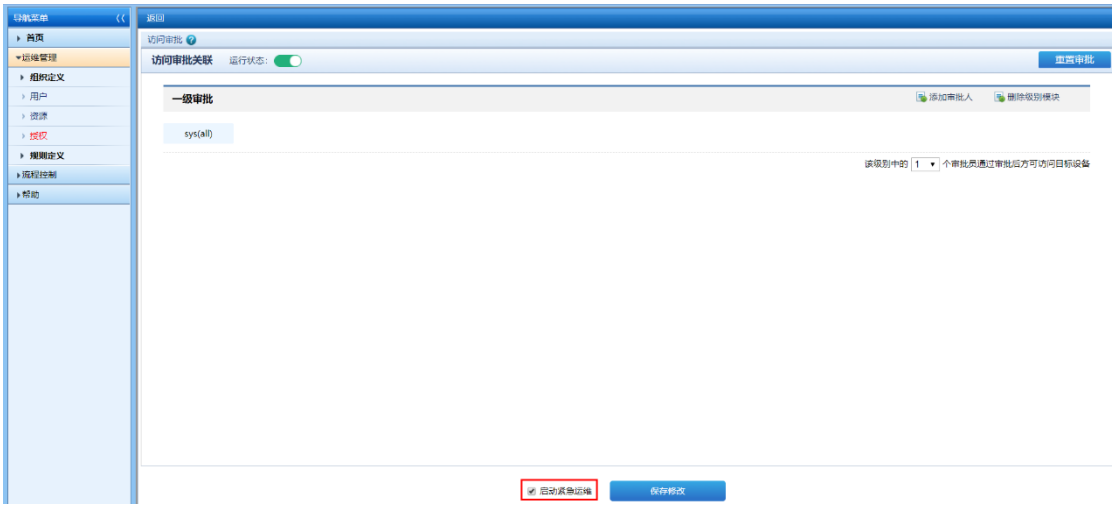
使用申请人 aa 登录系统页面，登录成功后看到申请人 aa 已被授权的资源单点登录图标变为访问审批和紧急运维图标。



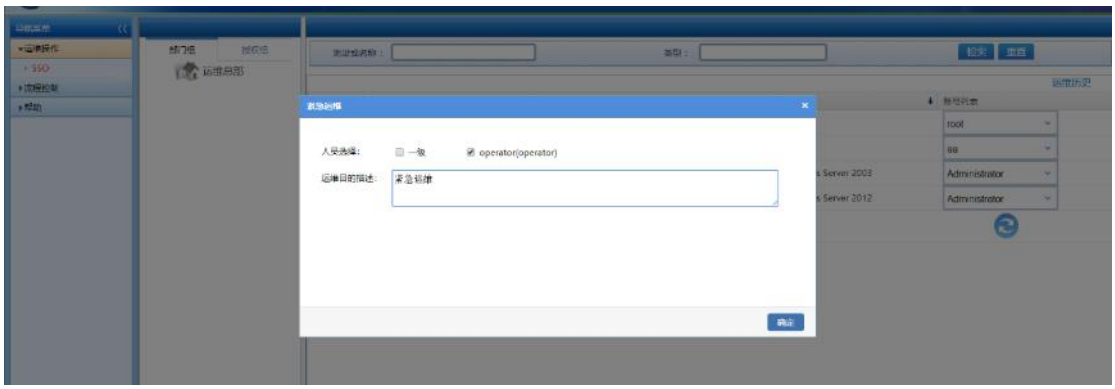
1.紧急运维

紧急运维功能是运维操作员进行运维操作时，因审批人不在，需要马上做运维操作，所采取的紧急运维措施；紧急运维属于事后审批。（只有在运维操作员不退出的情况下，紧急运维申请后，不用再次申请；用户退出，再登录系统需再次申请）

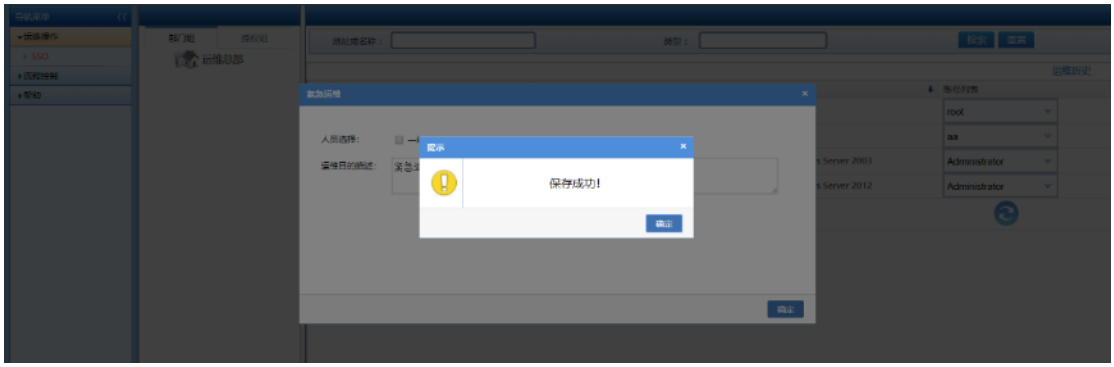
切换至运维管理->授权，授权页面，点击 cyy 授权上的访问审批按钮，跳转到访问审批页面，勾选启动紧急运维按钮，启动紧急运维，点击保存修改



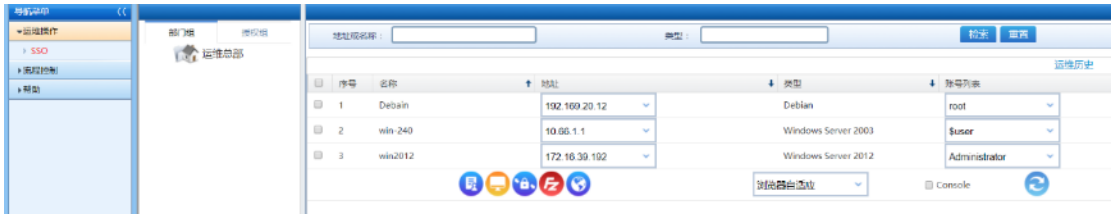
点击  图标，弹出紧急运维窗口。



点击确定按钮，弹出提示窗口。



点击确定按钮，点击  按钮。紧急运维图标变为单点登录图标。



审批人 operator 登录系统，页面显示一条消息。

➢ 同意申请

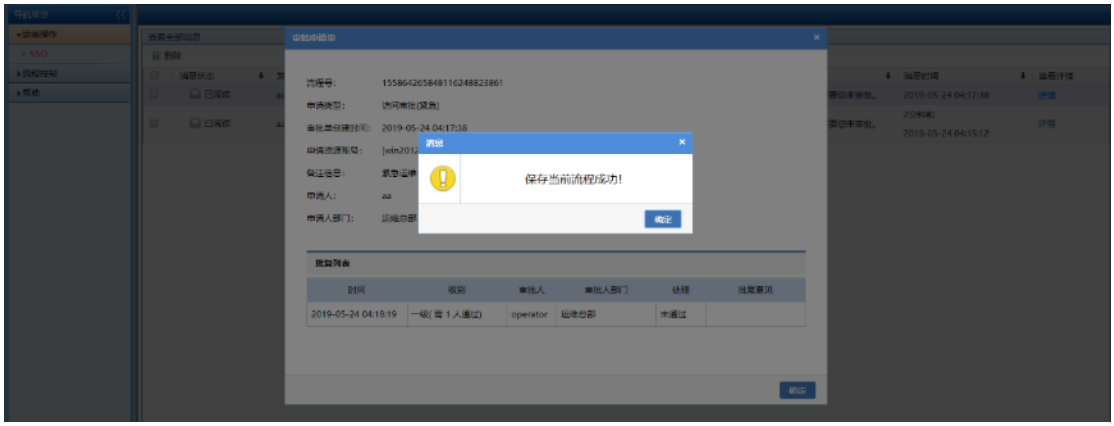
点击详情，弹出审批申请单。

点击确定按钮，弹出提示窗口。审批人通过，不会触发告警。

➢ 拒绝申请

点击详情，弹出审批申请单。

点击确定按钮，弹出提示窗口。审批人拒绝，会触发告警。



使用系统管理员 sysAdmin 登录系统，点击策略配置->告警策略->告警归纳。

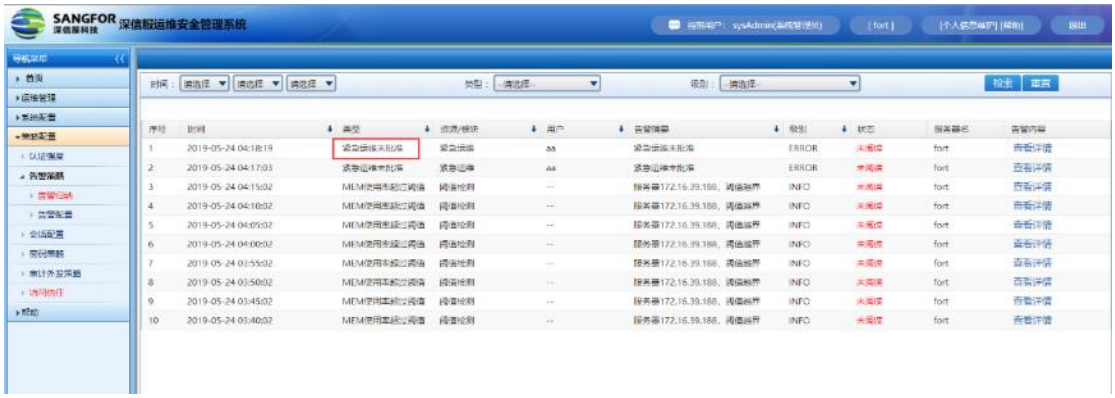
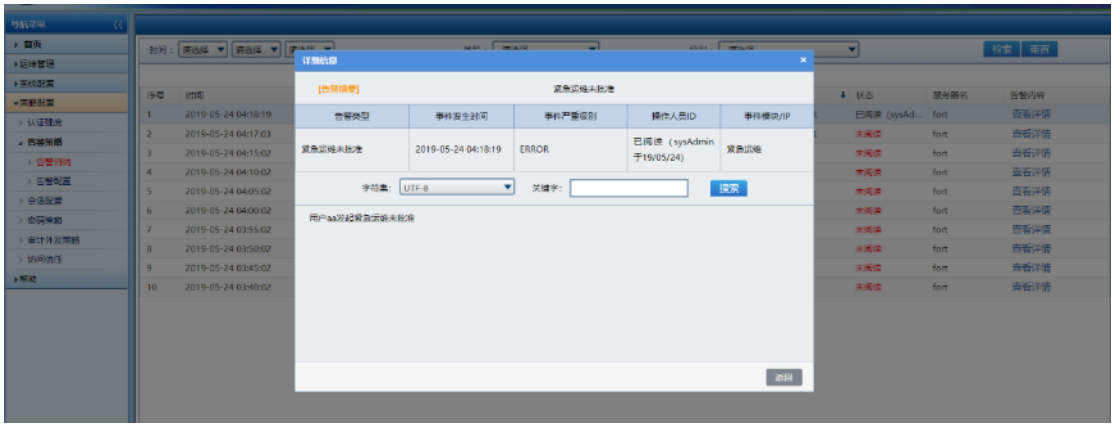


图 3.10.1.3.1-9

点击查看详情按钮，弹出详细信息窗口。

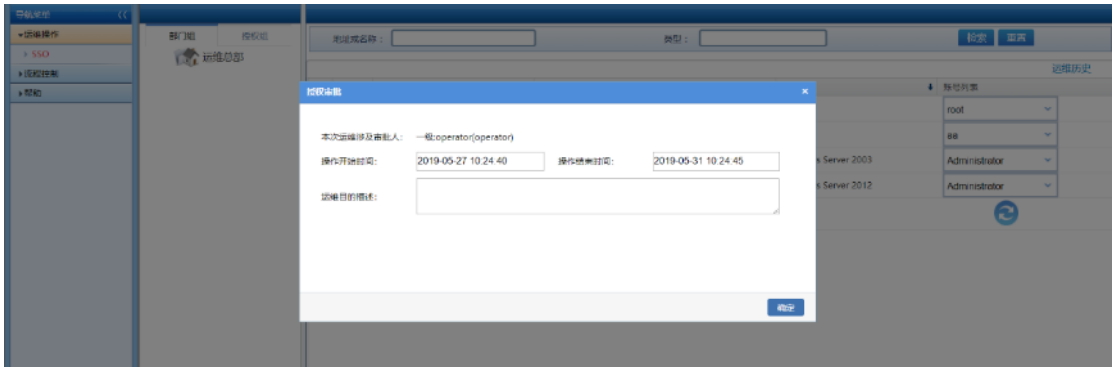


2.上级审批

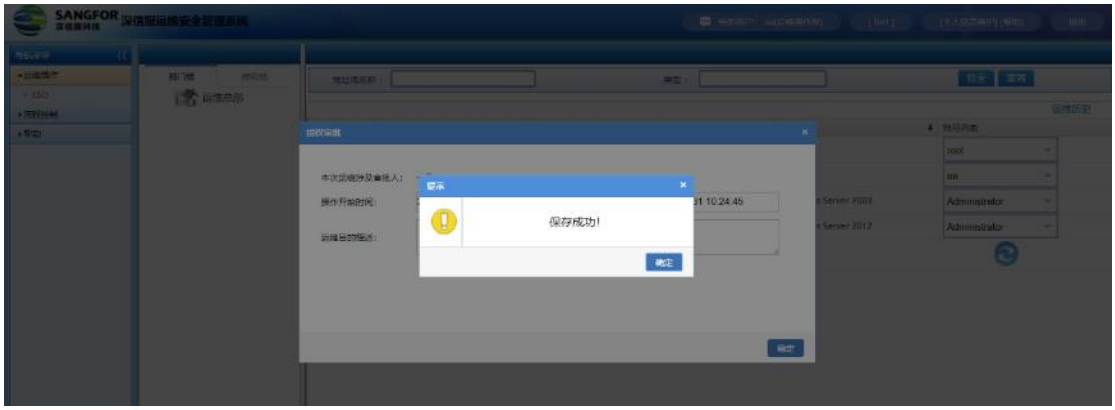
上级审批功能是指运维操作员在进行运维操作时，需进行上级审批，由审批人批复后，才可进

行运维操作。

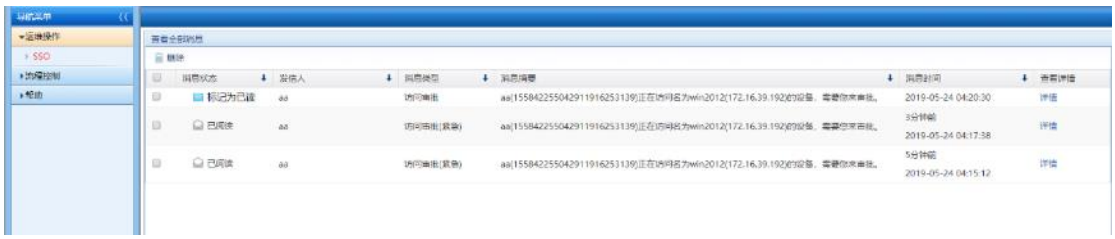
点击  图标，弹出授权审批窗口。



点击确定按钮，弹出提示窗口。

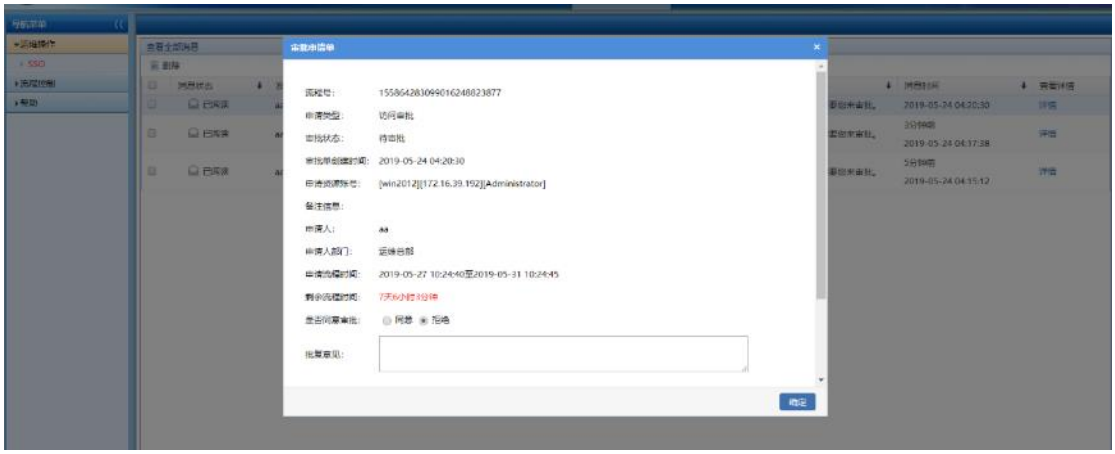


使用审批人 operator 登录系统，页面弹出一条消息。

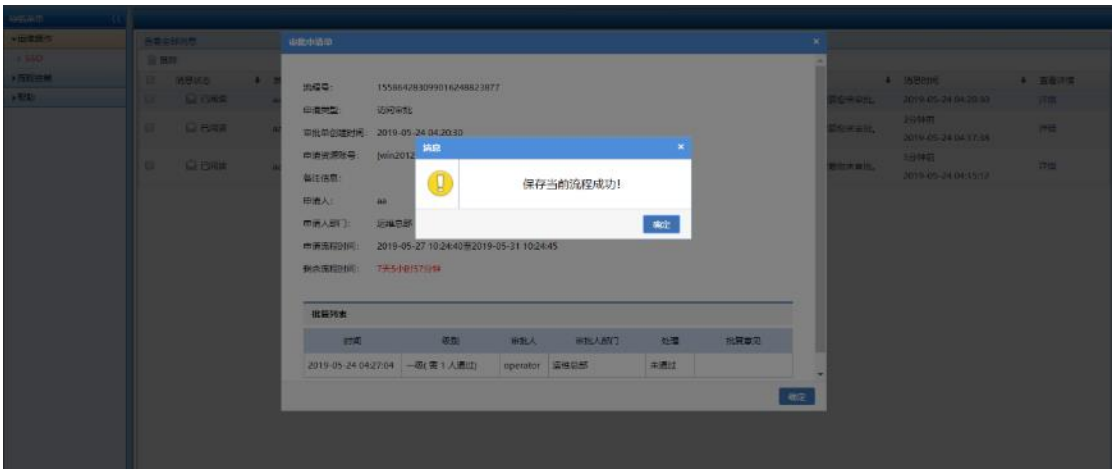


➢ 拒绝审请

点击详情，弹出审批申请单。



选择拒绝，点击确定按钮，弹出提示窗口。（审批人拒绝申请，申请人可再次发送申请）



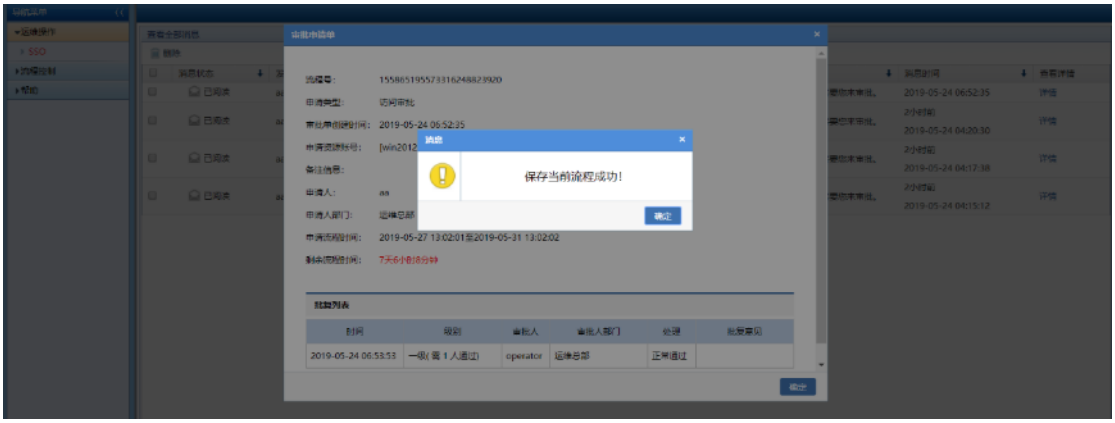
使用申请人 aa 登录系统，页面弹出一条消息提示。

点击详情按钮，弹出审批结果单窗口。

➢ 同意审请

点击详情按钮，弹出审批申请单窗口。

选择同意，点击确定按钮，弹出提示窗口。



使用申请人 aa 登录系统，页面弹出一条消息提示。

点击详情按钮，弹出审批结果单窗口。

审批人同意申请，申请人 aa 在该段时间内可以直接进行运维操作，不需要进行申请操作。

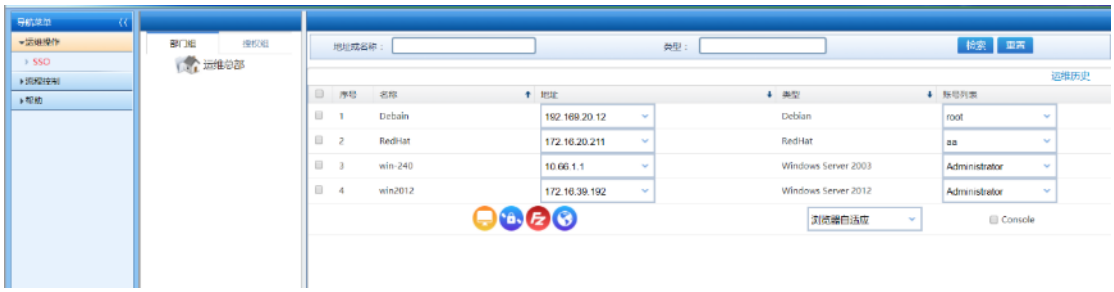


图 3.10.1.3.2-12

9.4. 流程控制

流程控制包含流程任务、申请历史、个人历史、部门历史、全部历史五种类型。

9.4.1. 流程任务

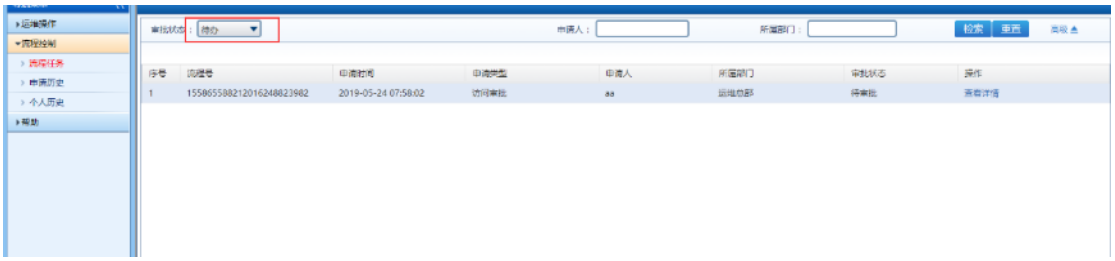
流程任务显示需要当前登录系统的用户批复的所有流程列表。

使用审批人 operator 登录系统，点击流程控制->流程任务。

1.普通检索

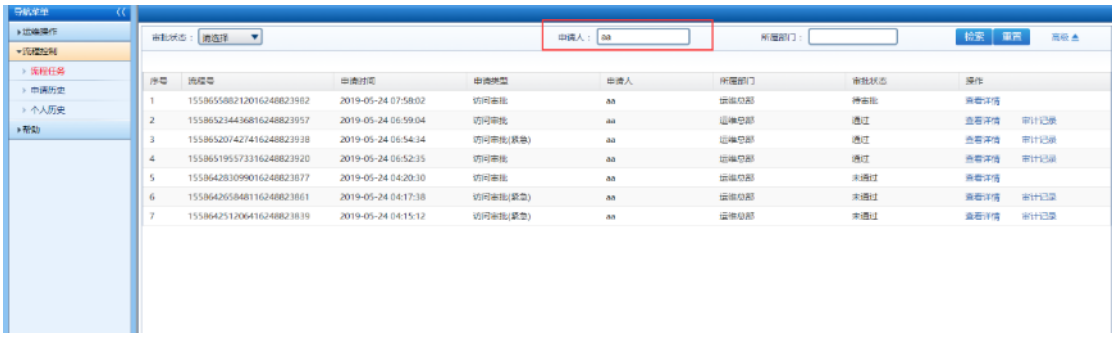
➢ 按审批状态检索

选择审批状态待办，点击检索按钮，即可查询到审批状态待办的流程任务记录。



➢ 按申请人检索

填写申请人 aa，点击检索按钮，即可查询到申请人 aa 的流程任务记录。



➢ 按所属部门检索

选择所属部门运维总部，点击检索按钮，即可查询到运维总部的流程任务记录。

2.高级检索

➢ 按流程号检索

填写流程号 23938，点击检索按钮，即可查询到流程号 23938 的流程任务记录。

➢ 按申请类型检索

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的流程任务记录。

➢ 按目标IP检索

填写目标 IP172.16.20.78，点击检索按钮，即可查询到目标 IP172.16.20.78 的流程任务记录。

➢ 按年检索

选择 2018 年，点击检索按钮，即可查询到 2018 年的流程任务记录。

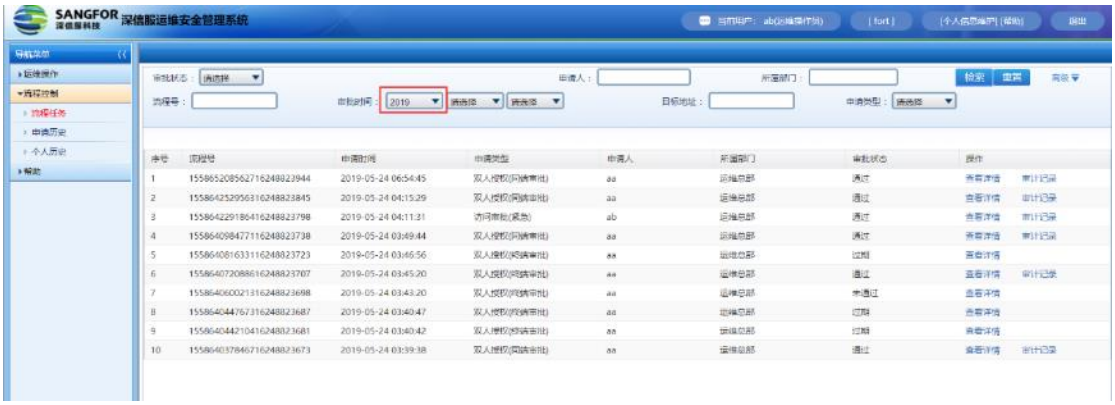
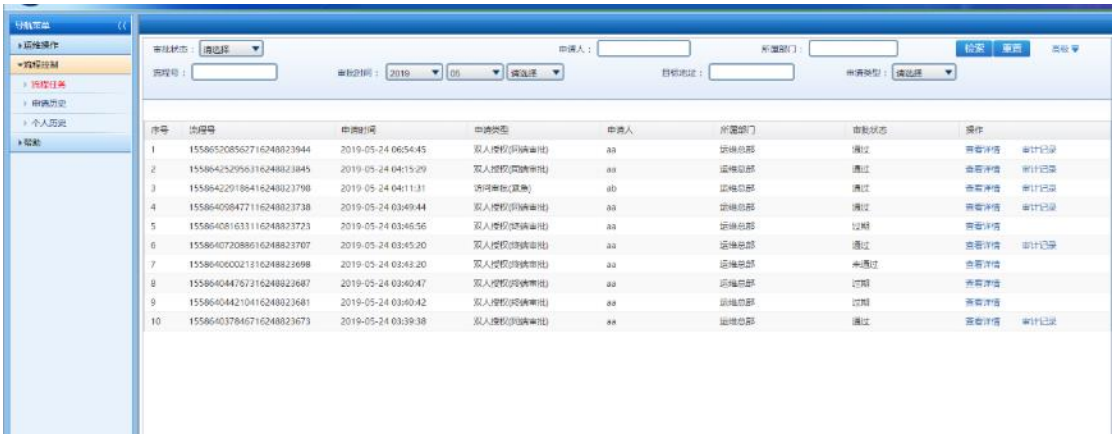


图 3. 10. 2. 1. 2-4

➢ 按月检索

选择 2019 年 5 月，点击检索按钮，即可查询到 2019 年 5 月的流程任务记录。



➢ 按日检索

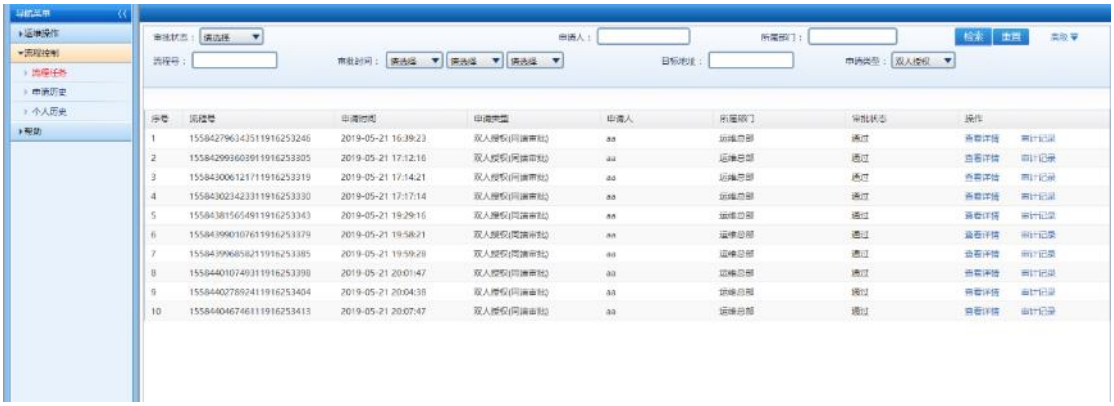
选择 2019 年 5 月 22 日，点击检索按钮，即可查询到 2019 年 5 月 22 日的流程任务记录。

3.查看详情

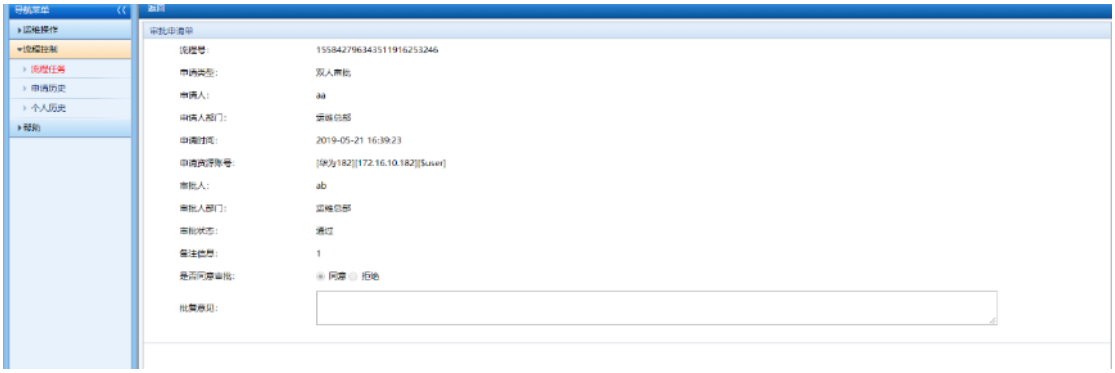
使用审批人 operator 登录系统，点击流程控制->流程任务。

➢ 双人授权查看详情

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的流程任务记录。



点击双人授权的查看详情按钮，页面跳转到审批申请单页面。



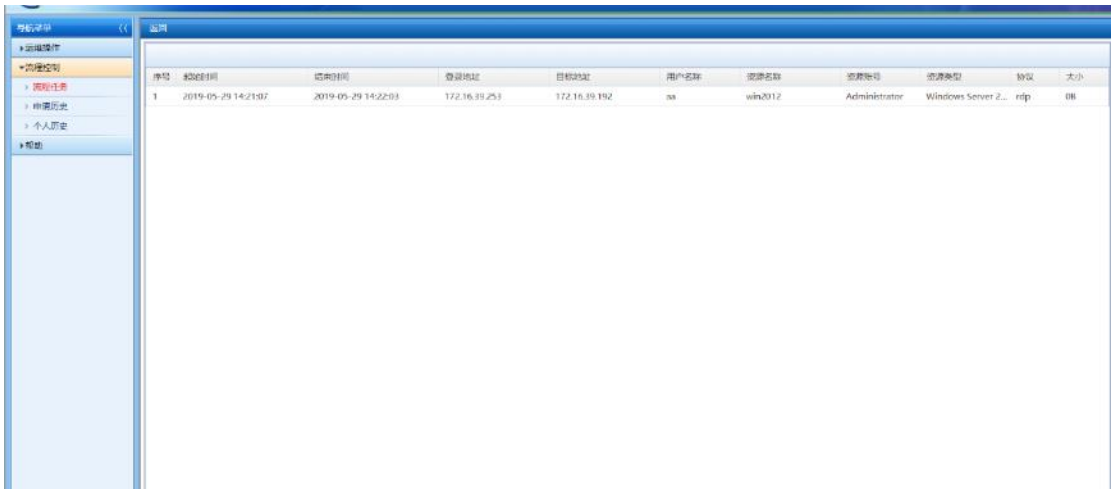
➢ 访问审批查看详情

选择申请类型访问审批，点击检索按钮，即可查询到申请类型访问审批的流程任务记录。

点击访问审批的查看详情按钮，页面跳转到审批申请单页面。

4.审计记录

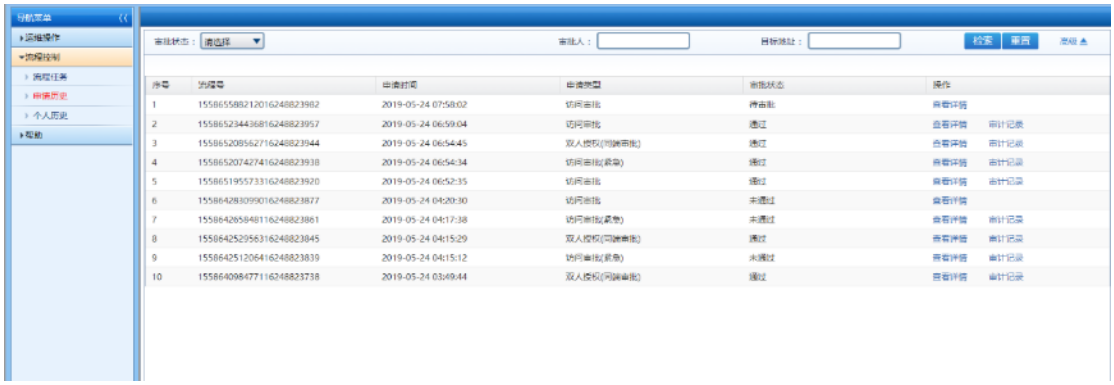
点击审计记录按钮，页面跳转到审计记录详情页面。



9.4.2. 申请历史

申请历史显示当前登录系统的用户申请的所有流程列表。

使用申请人 aa 登录系统，点击流程控制->申请历史。



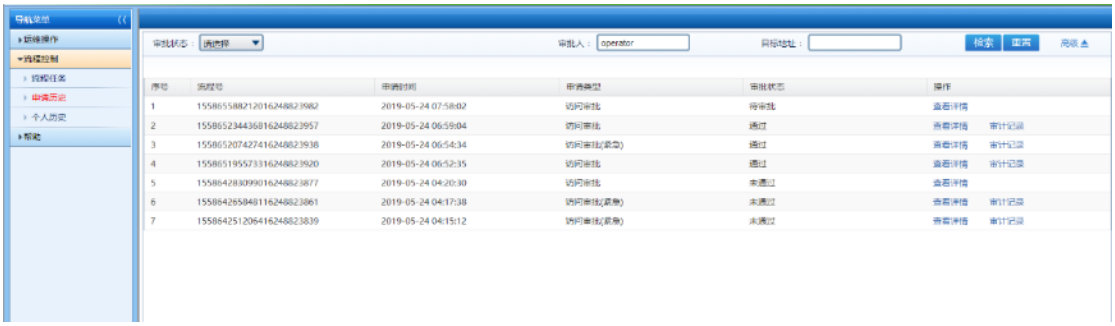
1.普通检索

➢ 按审批状态检索

选择审批状态通过，点击检索按钮，即可查询到审批状态通过的申请历史记录。

➢ 按审批人检索

填写审批人 operator，点击检索按钮，即可查询到审批人为 operator 的申请历史记录。



➢ 按目标IP检索

填写目标 IP172.16.20.78，点击检索按钮，即可查询到目标 IP172.16.39.192 的申请历史记录。

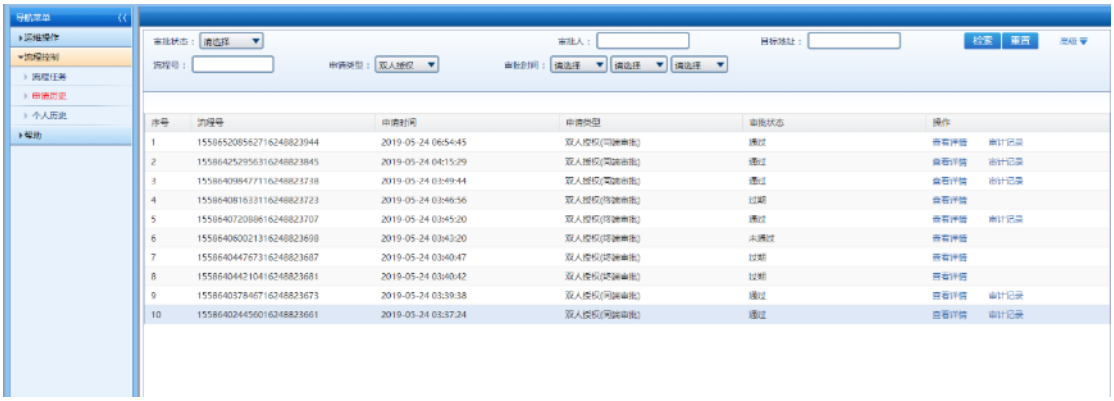
2.高级检索

➢ 按流程号检索

填写流程号 58326，点击检索按钮，即可查询到流程号 23982 的申请历史记录。

➢ 按申请类型检索

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的申请历史记录。



➢ 按年检索

选择 2019 年，点击检索按钮，即可查询到 2019 年的申请历史记录。

➢ 按月检索

选择 2019 年 5 月，点击检索按钮，即可查询到 2019 年 5 月的申请历史记录。

➢ 按日检索

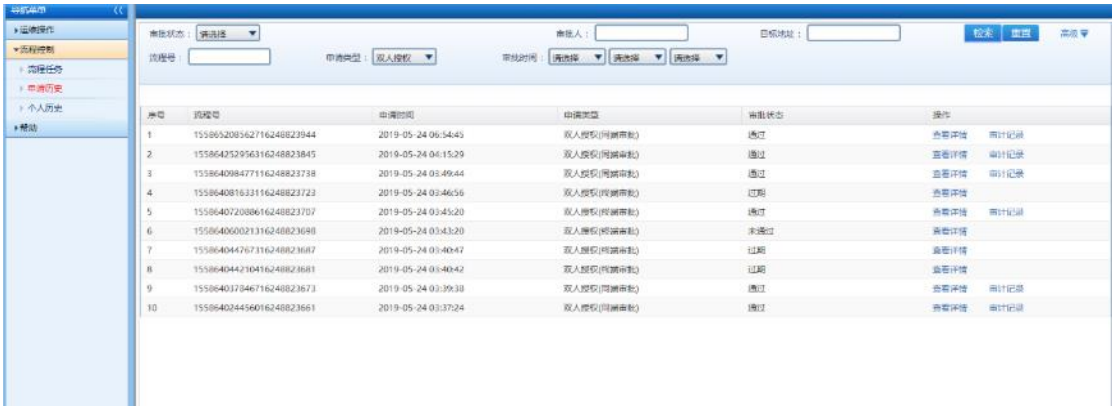
选择 2018 年 5 月 24 日，点击检索按钮，即可查询到 2019 年 5 月 24 日的申请历史记录。

3.查看详情

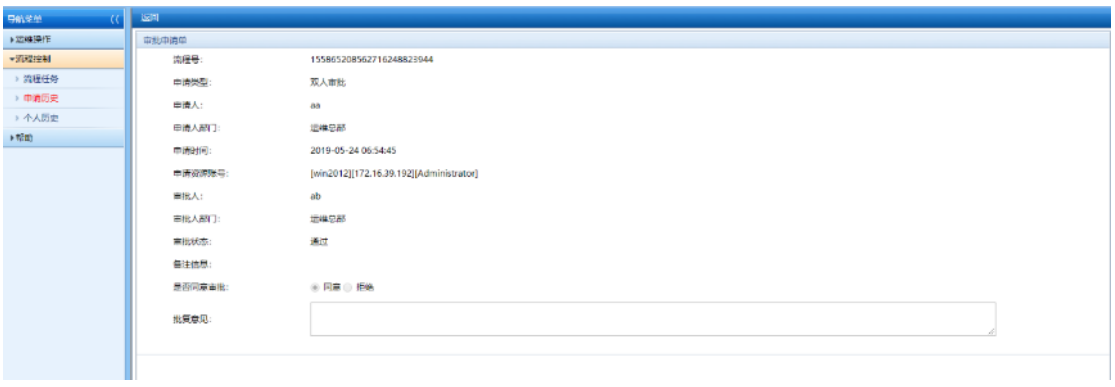
使用申请人 aa 登录系统，点击流程控制->申请历史。

➢ 双人授权查看详情

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的申请历史记录。

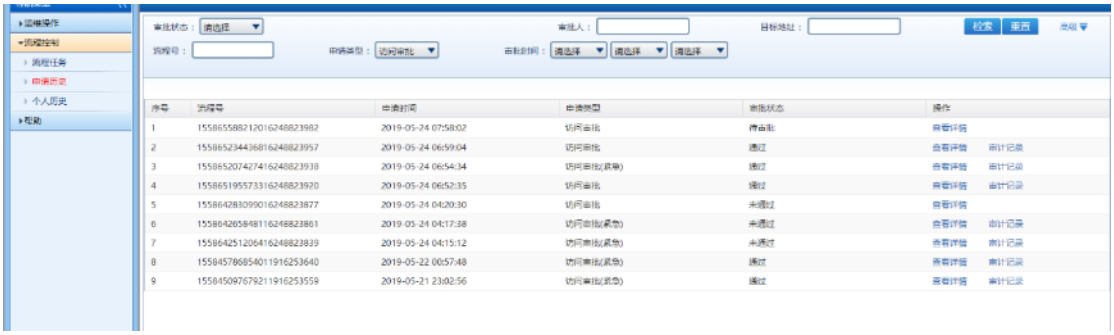


点击双人授权的查看详情按钮，页面跳转到审批申请单页面。



➢ 访问审批查看详情

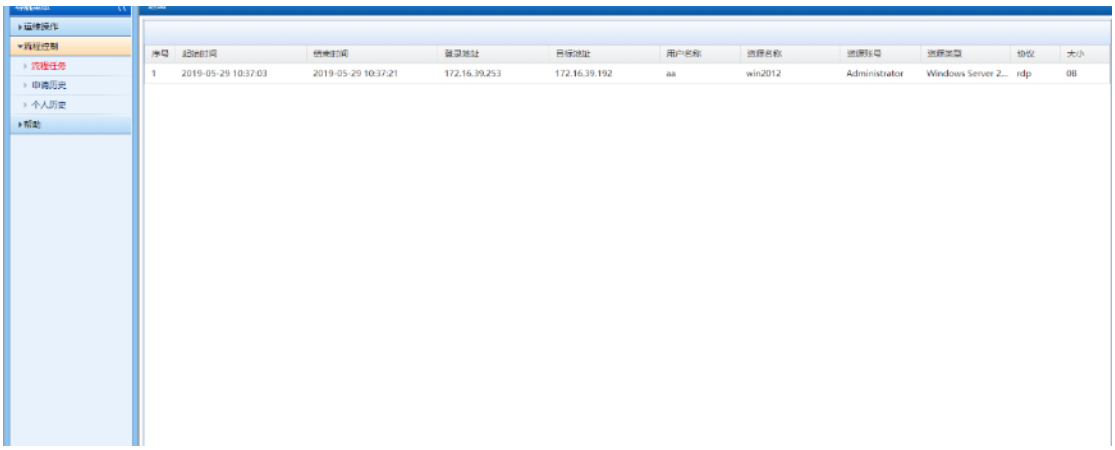
选择申请类型访问审批，点击检索按钮，即可查询到申请类型访问审批的申请历史记录。



点击访问审批的查看详情按钮，页面跳转到审批申请单页面。

4.审计记录

点击审计记录按钮，页面跳转到审计记录详情页面。



9.4.3. 个人历史

个人历史显示需要当前登录系统的用户批复的整体流程状态列表。

使用审批人 operator 登录系统，点击流程控制->个人历史。

1.普通检索

➢ 按审批状态检索

选择审批状态通过，点击检索按钮，即可查询到审批状态通过的个人历史记录。

➢ 按申请人检索

填写申请人 aa，点击检索按钮，即可查询到申请人 aa 的个人历史记录。

➢ 按审批人检索

填写审批人 operator，点击检索按钮，即可查询到审批人 operator 的个人历史记录。

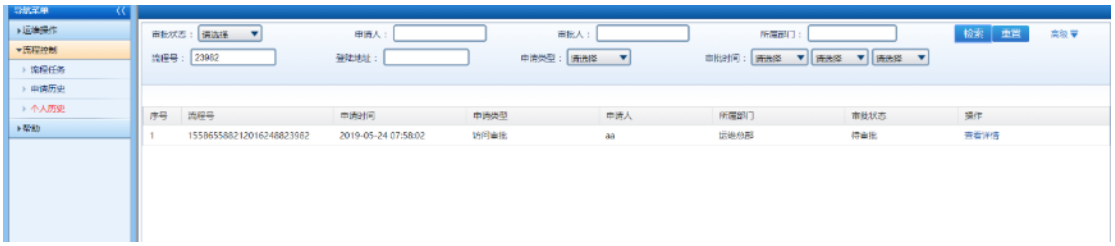
➢ 按所属部门检索

选择部门运维总部，点击检索按钮，即可查询到运维总部人员的个人历史记录。

2.高级检索

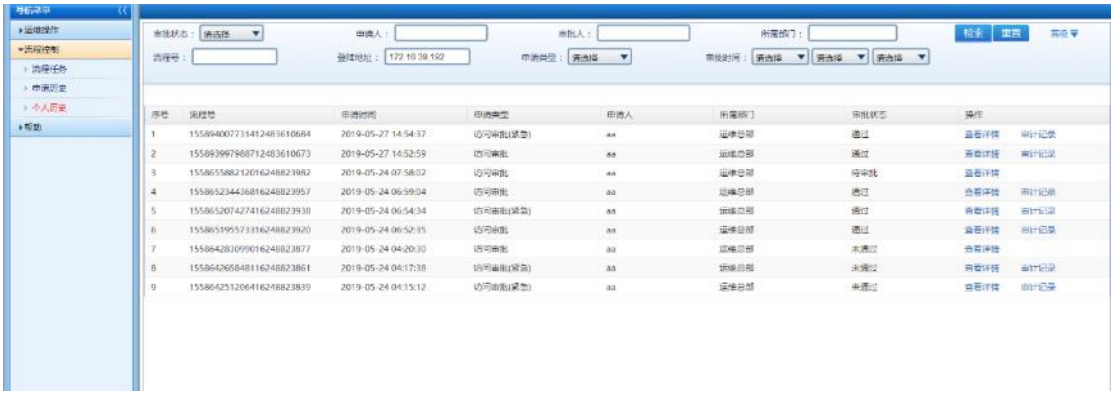
➢ 按流程号检索

填写流程号 23982，点击检索按钮，即可查询到流程号 23982 的个人历史记录。



➢ 按登陆地址检索

填写登陆地址 172.16.39.192，点击检索按钮，即可查询到登陆地址 172.16.20.78 的个人历史记录。



➢ 按申请类型检索

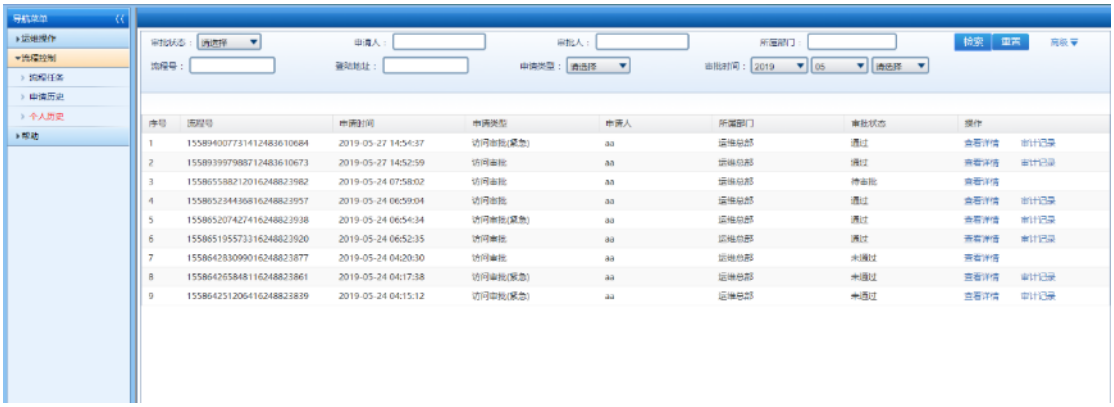
选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的个人历史记录。

➢ 按年检索

选择 2019 年，点击检索按钮，即可查询到 2019 年的个人历史记录。

➢ 按月检索

选择 2018 年 9 月，点击检索按钮，即可查询到 2018 年 9 月的个人历史记录。



➢ 按日检索

选择 2019 年 5 月 24 日，点击检索按钮，即可查询到 2019 年 5 月 24 日的个人历史记录。

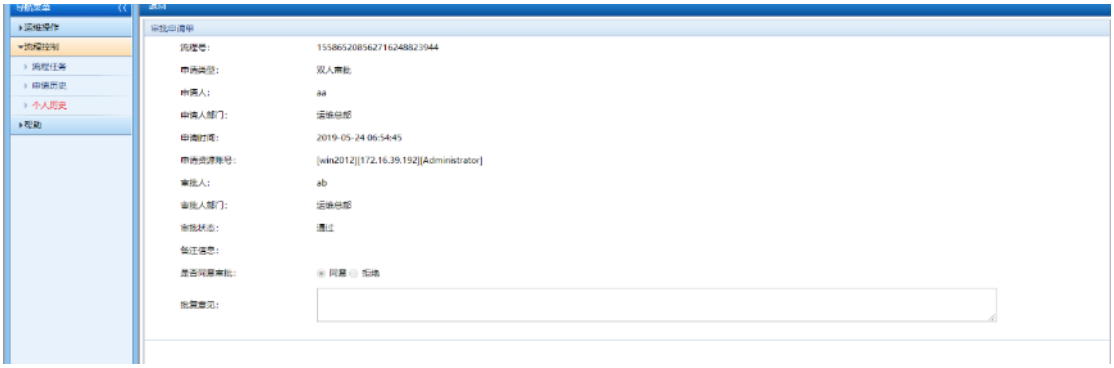
3.查看详情

使用审批人 operator 登录系统，点击流程控制->个人历史。

➢ 双人授权查看详情

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的个人历史记录。

点击双人授权的查看详情按钮，页面跳转到审批申请单页面。



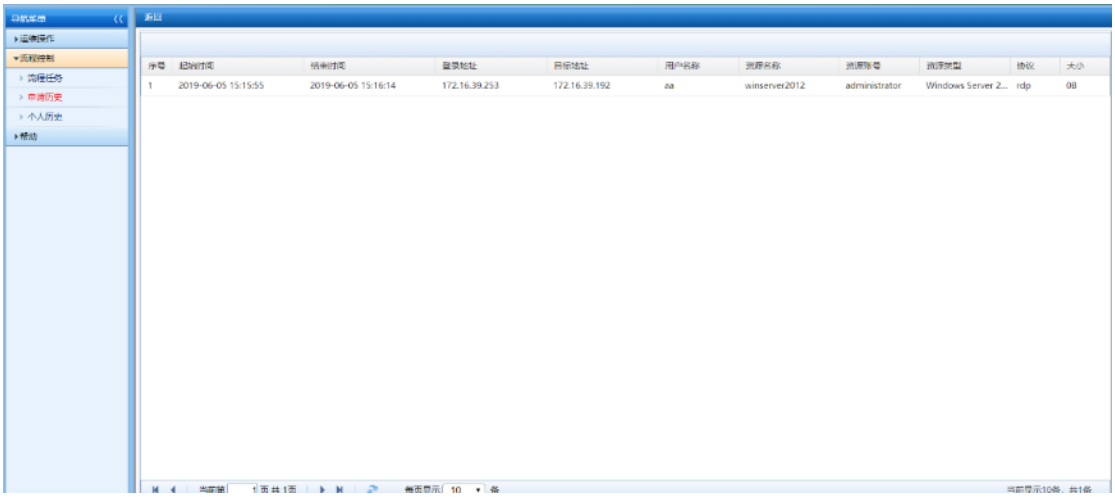
➢ 访问审批查看详情

选择申请类型访问审批，点击检索按钮，即可查询到申请类型访问审批的个人历史记录。

点击访问审批的查看详情按钮，页面跳转到审批申请单页面。

4.审计记录

点击审计记录按钮，页面跳转到审计记录详情页面。



9.4.4. 部门历史

部门历史显示安全管理员所属部门下的所有流程列表。

使用安全管理员 secAdmin 登录系统，点击流程控制->部门历史。

1.普通检索

- **按审批状态检索**

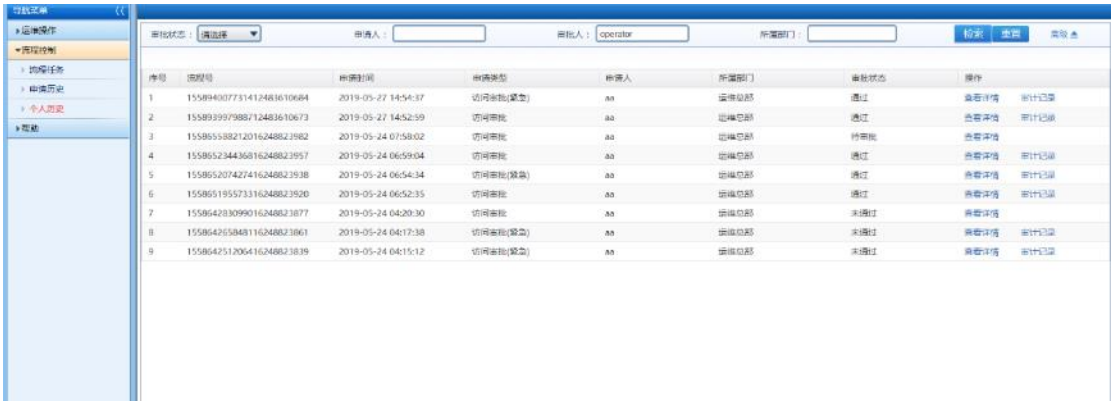
选择审批状态通过，点击检索按钮，即可查询到审批状态通过的部门历史记录。

➢ 按申请人检索

填写申请人 aa，点击检索按钮，即可查询到申请人 aa 的部门历史记录。

➢ 按审批人检索

填写审批人 operator，点击检索按钮，即可查询到审批人 operator 的部门历史记录。



➢ 按所属部门检索

选择部门运维总部，点击检索按钮，即可查询到运维总部人员的部门历史记录。

2.高级检索

➢ 按流程号检索

填写流程号 23982，点击检索按钮，即可查询到流程号 23982 的部门历史记录。

➢ 按登陆地址检索

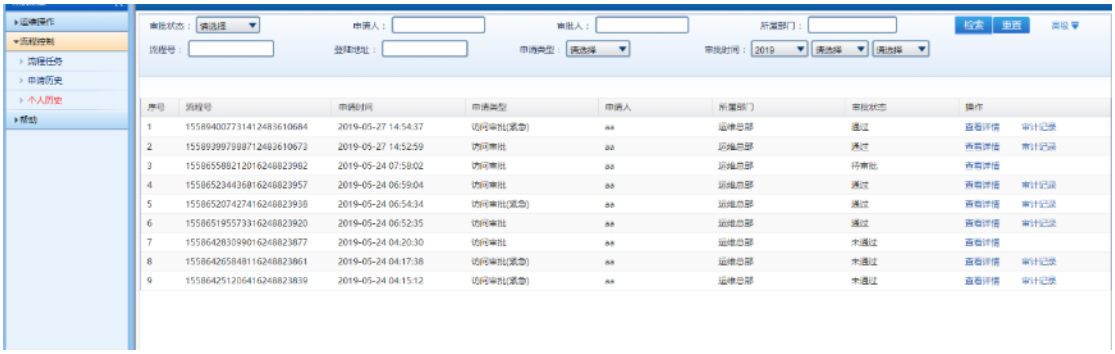
填写登陆地址 172.16.39.192，点击检索按钮，即可查询到登陆地址 172.16.39.192 的部门历史记录。

➢ 按申请类型检索

选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的部门历史记录。

➢ 按年检索

选择 2019 年，点击检索按钮，即可查询到 2019 年的部门历史记录。



➢ 按月检索

选择 2019 年 5 月，点击检索按钮，即可查询到 2019 年 5 月的部门历史记录。

➢ 按日检索

选择 2019 年 5 月 24 日，点击检索按钮，即可查询到 2019 年 5 月 24 日的部门历史记录。

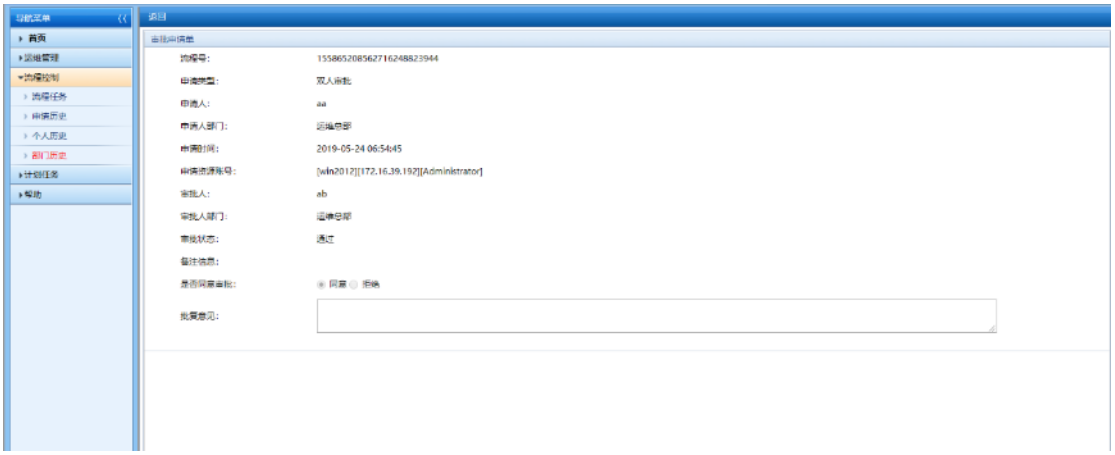
3.查看详情

使用安全管理员 secAdmin 登录系统，点击流程控制->部门历史。

➢ 双人授权查看详情

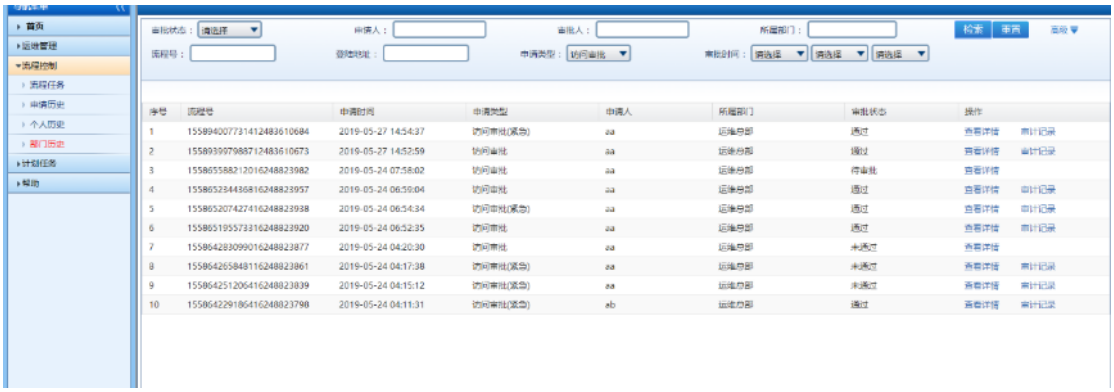
选择申请类型双人授权，点击检索按钮，即可查询到申请类型双人授权的部门历史记录。

点击双人授权的查看详情按钮，页面跳转到审批申请单页面。



➢ 访问审批查看详情

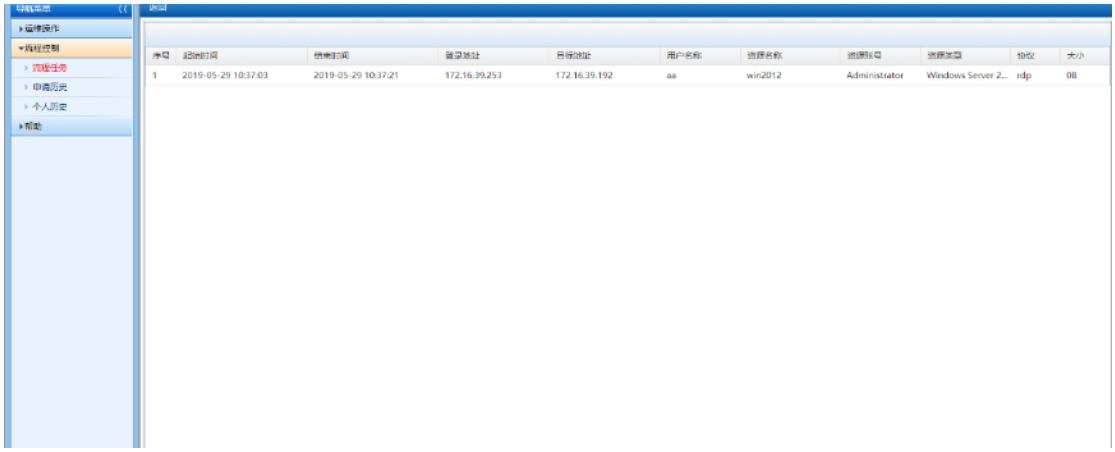
选择申请类型访问审批，点击检索按钮，即可查询到申请类型访问审批的部门历史记录。



点击访问审批的查看详情按钮，页面跳转到审批申请单页面。

4.审计记录

点击审计记录按钮，页面跳转到审计记录详情页面。



9.4.5. 全部历史

全部历史显示系统内所有的流程列表。

使用系统审批员 appr（拥有系统级流程控制模块权限）登录系统，点击流程控制->全部历史。

其余检索和查询条件同部门历史。

10. 规则定义

规则定义由命令规则、时间规则，地址规则和资源时间规则四部分组成。

10.1. 命令规则

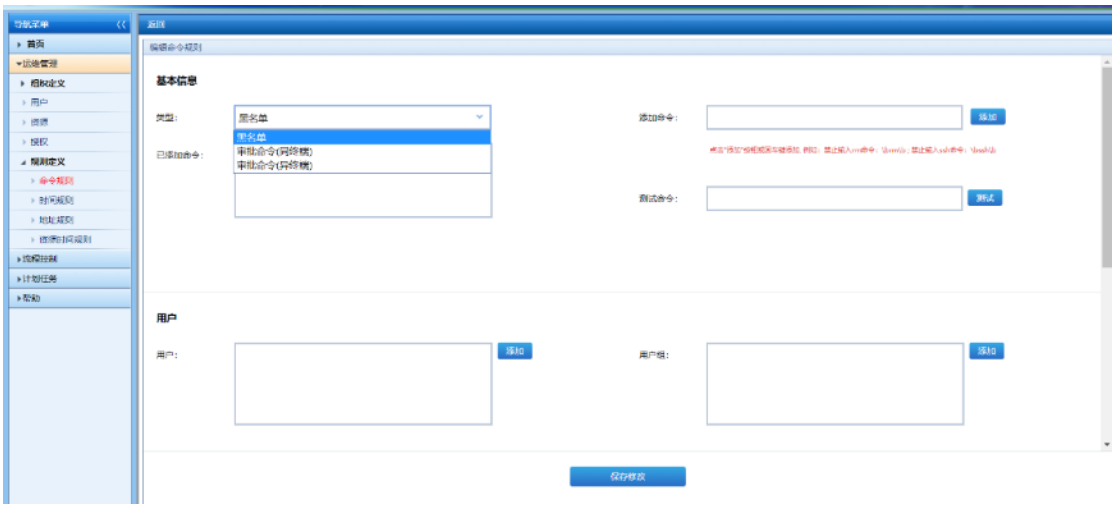
命令规则分为黑名单策略和审批命令策略，限制运维操作员在运维操作时的行为。

使用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->规则定义->命令规则链接进入命令规则界面。

10.1.1. 命令规则添加

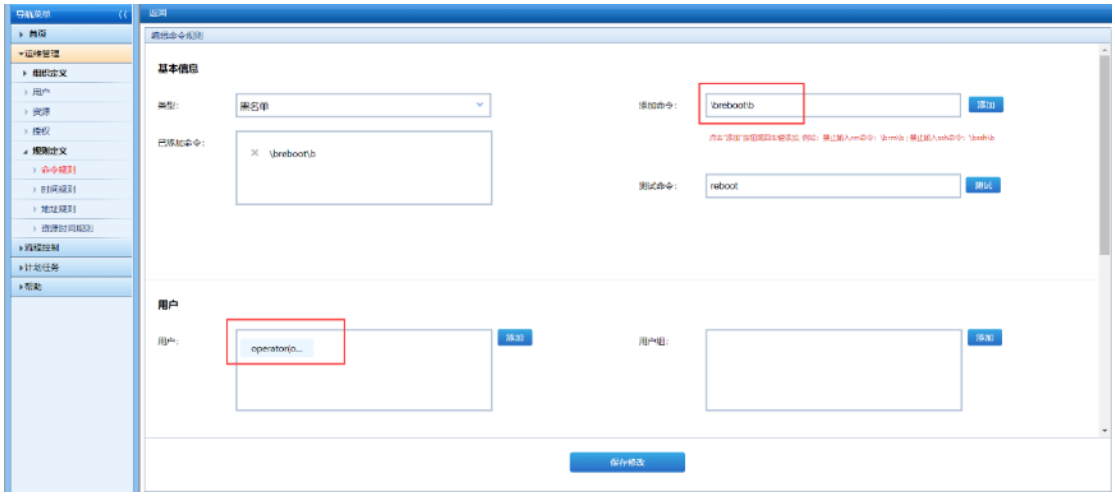
在命令规则界面点击添加。

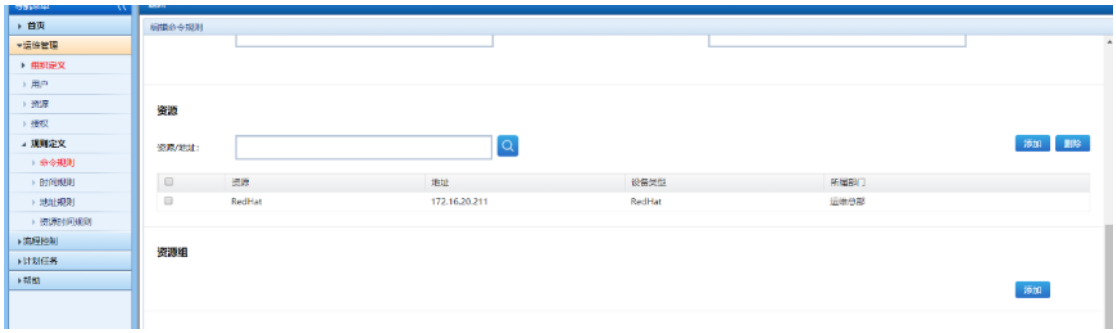
跳转到命令规则编辑页面，命令规则分为黑名单类型和审批命令类型。



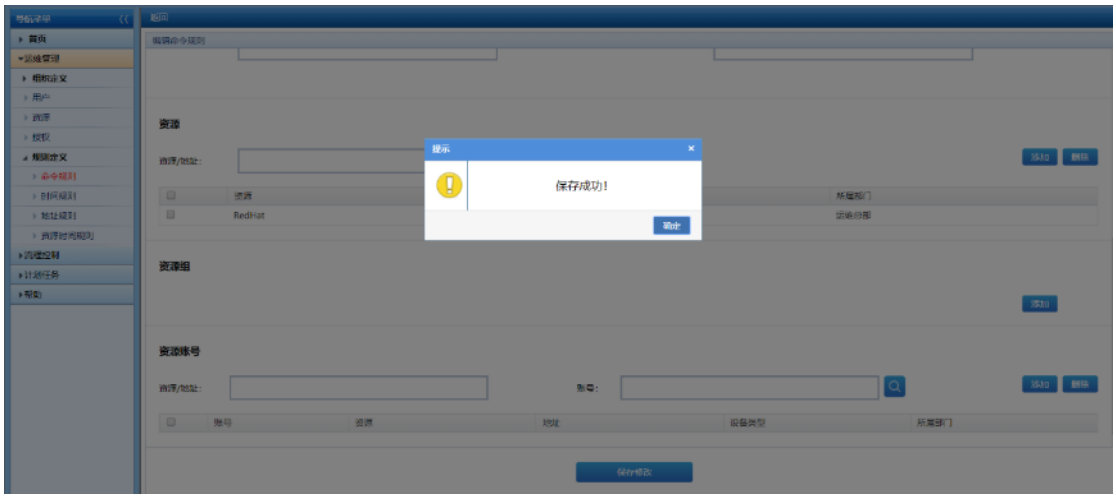
1.添加黑名单类型

添加命令为 reboot，添加用户为 operator，添加资源为 redhat。





点击保存，提示保存成功！



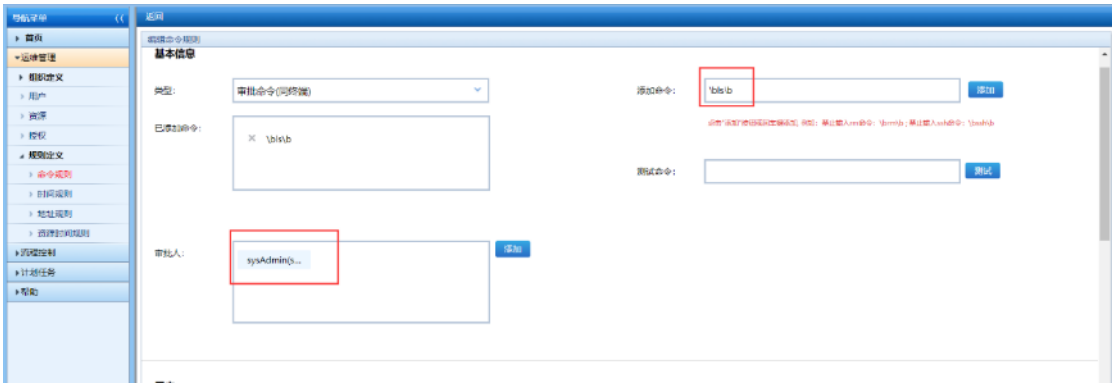
点击弹出框上的确定按钮，点击返回，页面切换到命令规则列表页面，列表显示用户为 operator 的命令规则，至此黑名单类型命令规则添加完成。

将状态改为 ON，或点击部署，此规则生效。

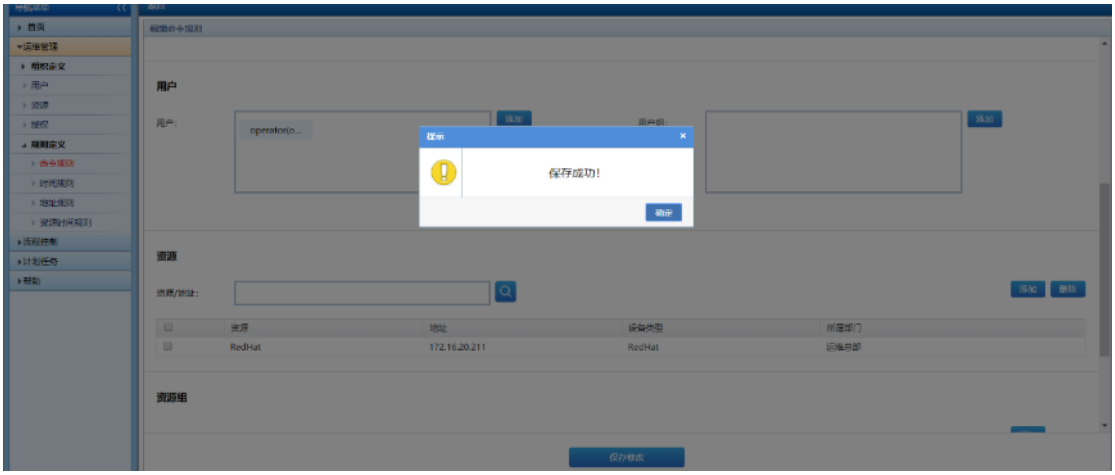
使用 operator 用户对 redhat 资源进行运维操作，输入命令 reboot，提示命令被阻断。

2.添加审批命令类型

添加命令为 ls，添加审批人为 sysAdmin，添加用户为 operator，添加资源为 redhat。



点击保存，提示保存成功！



点击弹出框上的确定按钮，点击返回，页面切换到命令规则列表页面，列表显示用户为 operator 的命令规则，至此审批命令类型命令规则添加完成。

图

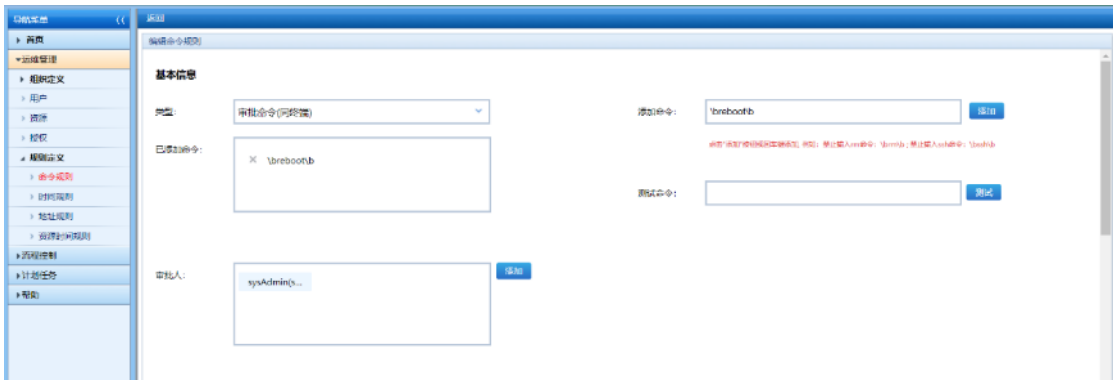
将状态改为 ON，或点击部署，此规则生效。

使用 operator 用户对 redhat 资源进行运维操作，输入命令 reboot，提示需要审批。

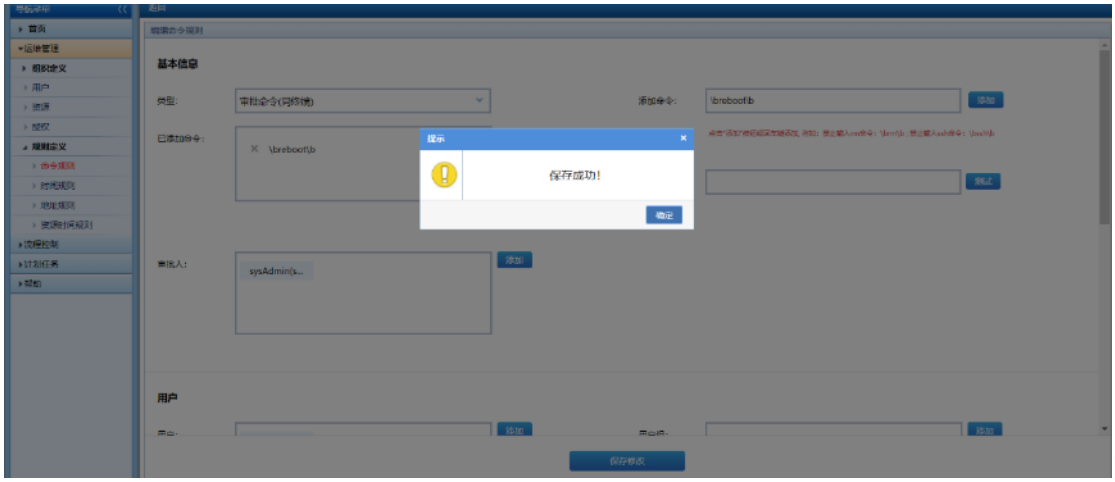
10.1.2. 命令规则修改

点击编辑可修改命令规则信息。

跳转到编辑页面，将添加命令 ls 修改为命令 reboot。



点击保存，提示保存成功！



图

点击弹出框上的确定按钮，点击返回，页面切换到命令规则列表页面，

列表命令修改为 reboot

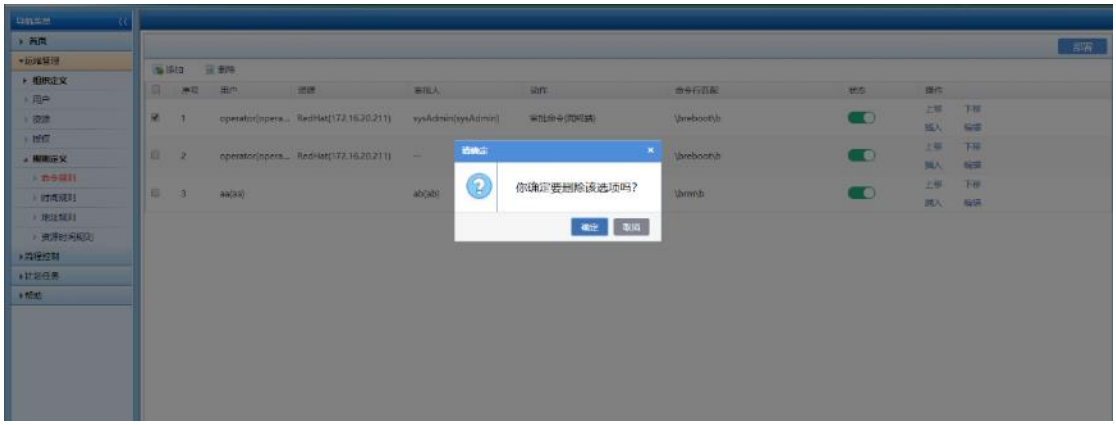
把该命令规则状态改为 ON，并重新部署后生效

至此命令规则修改完成。

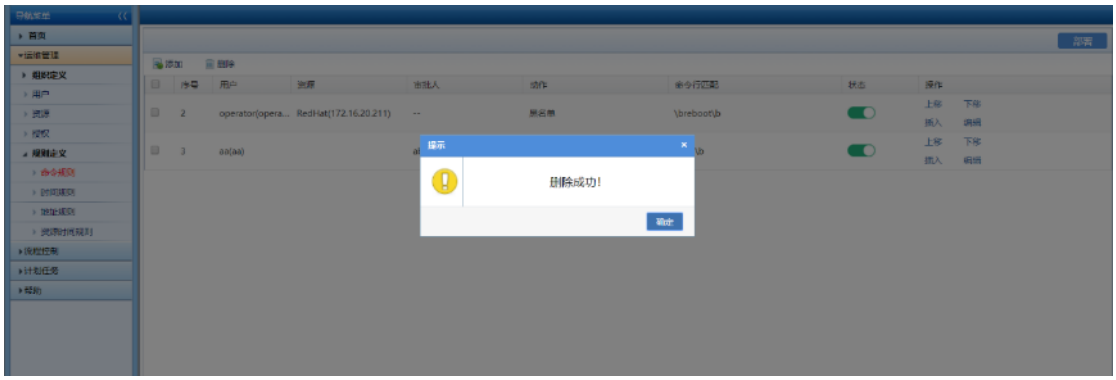
10.1.3. 命令规则删除

在命令规则列表页面，勾选**命令规则**，点击左上方**删除**。

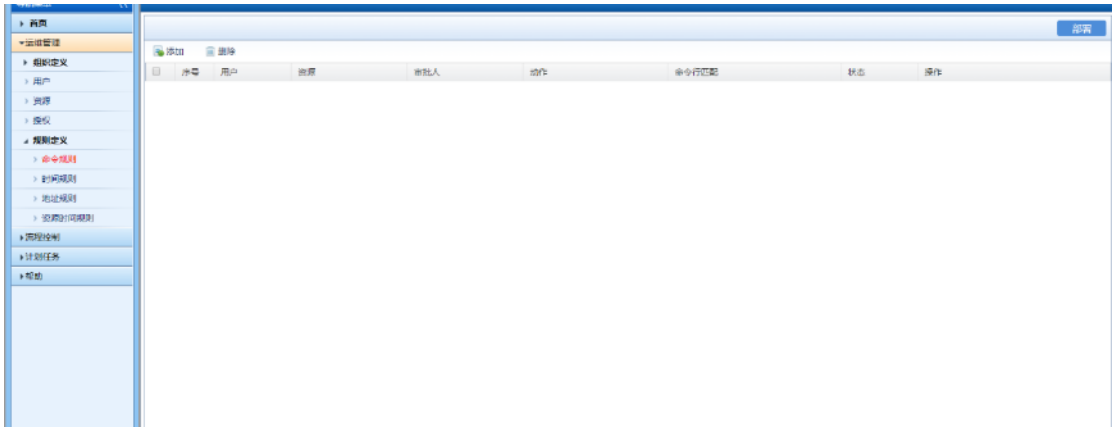
提示你确定要删除该选项吗？



点击确定，提示删除成功！



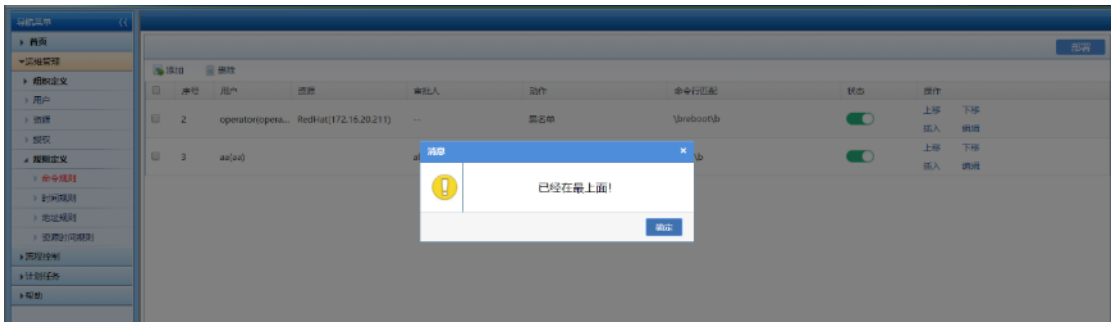
点击确定，返回命令规则页面，列表已删除的规则，至此命令规则删除完成。



10.1.4. 命令规则排序

命令规则条目之间可通过上移/下移/插入按钮进行排序。

当规则已处于最上方时，不可再进行上移，点击上移，弹出告警信息已经在最上面！下移同理。



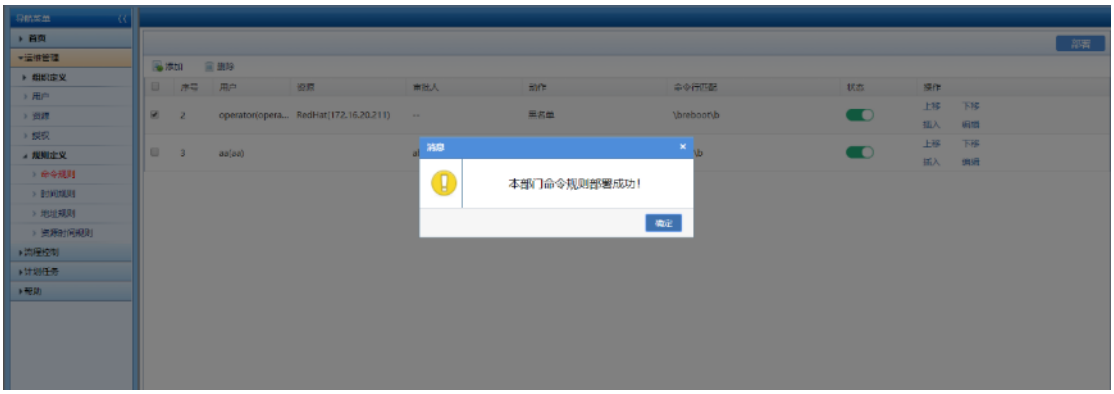
点击上移，用户为 operator 的规则向上移动一位，下移同理。

10.1.5. 命令规则状态

命令规则分为 ON，OFF 两种状态。ON 代表规则生效，OFF 代表规则无效。

将用户为 operator 规则的状态由 OFF 改为 ON，该条规则生效。

点击命令规则页面的部署，弹出提示消息本部门命令规则部署成功！



点击确定，状态为 ON 的规则生效。

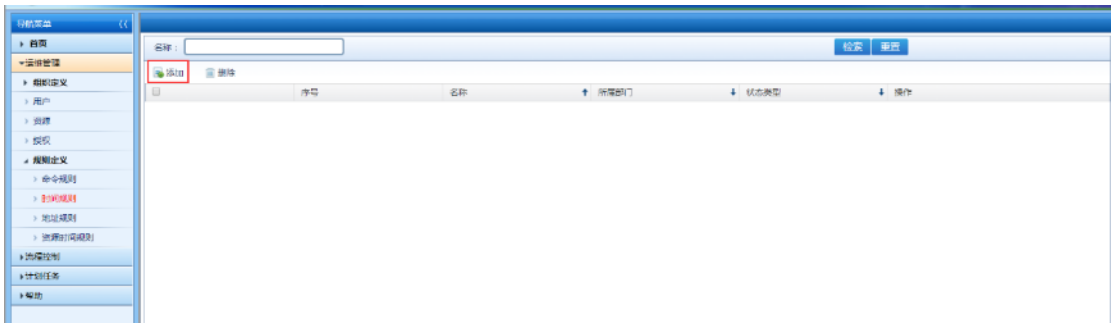
10.2. 时间规则

时间规则是对用户登录系统的时间进行限制。时间规则分为允许使用，禁止使用两种状态。允许使用是允许用户在该时间内登录系统；禁止使用是禁止用户在该时间内登录系统。

使用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->规则定义->时间规则链接进入时间规则界面。

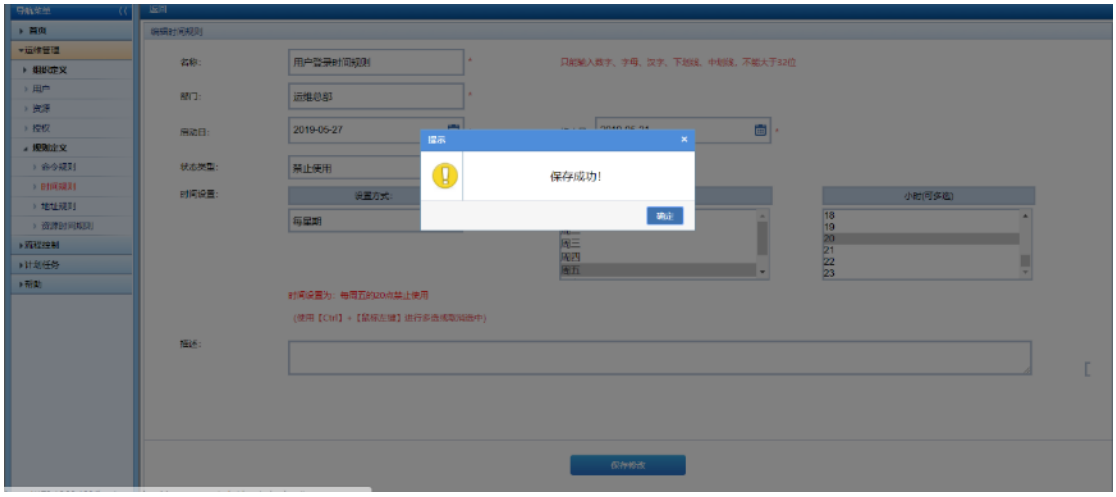
10.2.1. 时间规则添加

在时间规则界面点击添加。



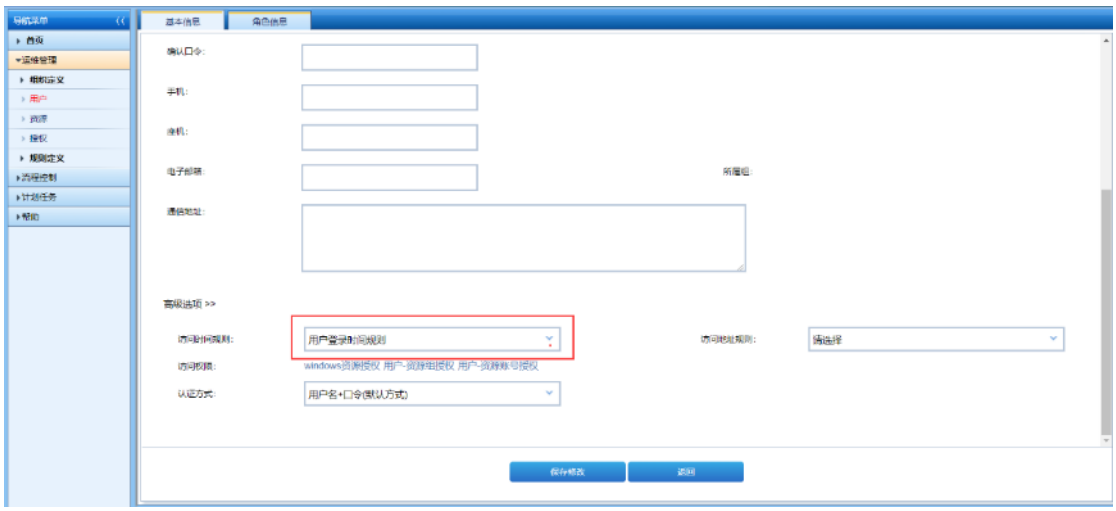
跳转到时间规则编辑页面，填写信息。

点击保存，提示保存成功！



点击弹出框上的确定按钮，点击返回，页面切换到时间规则列表页面，列表显示一条名称为用户登录时间规则的数据，至此时间规则添加完成。

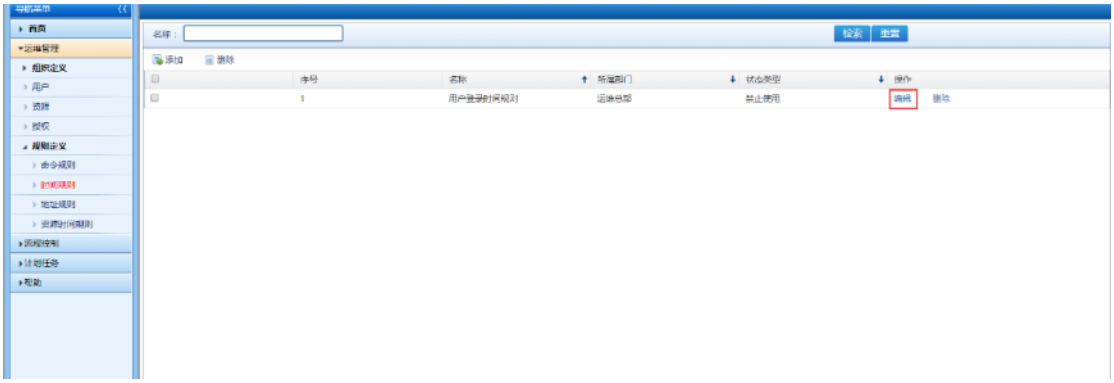
点击运维管理->用户->选择用户 aa 点击编辑->高级选项->选择访问时间规则->保存，将时间规则与用户关联。



使用用户 aa 在规定禁止登陆时间范围内的时间登录，提示您没有当前时间的登录权限！

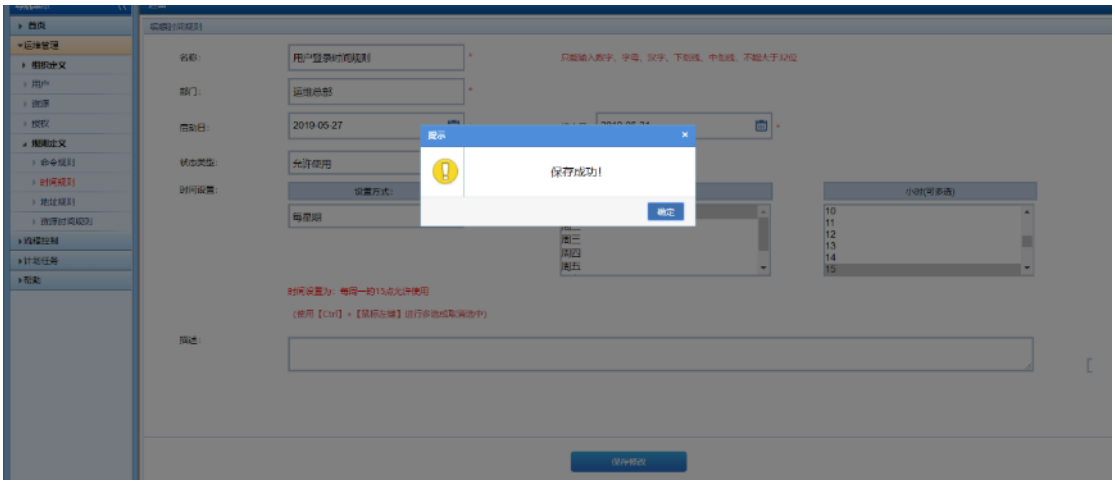
10.2.2. 时间规则修改

点击名称为**时间规则**右侧的**编辑**。



跳转到编辑页面，将名称为**时间规则**的状态类型修改为**允许使用**。

点击保存，提示保存成功！



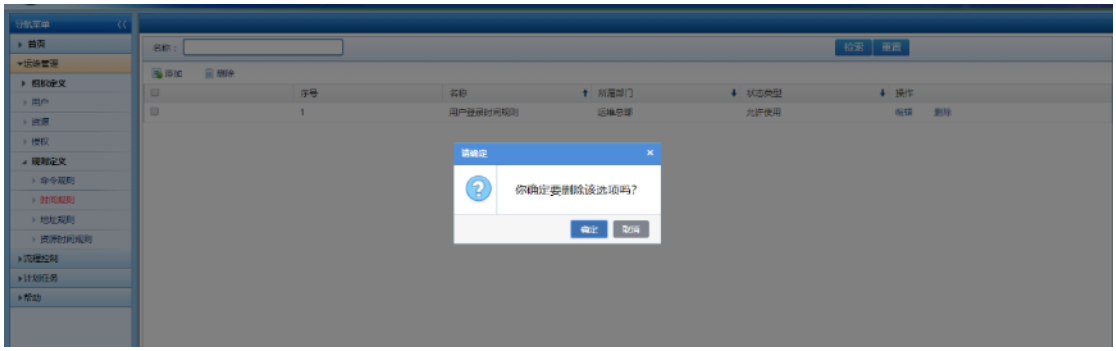
点击弹出框上的确定按钮，点击返回，页面切换到时间规则列表页面，列表名称为时间规则的状态类型是允许访问，至此时间规则修改完成。

10.2.3. 时间规则删除

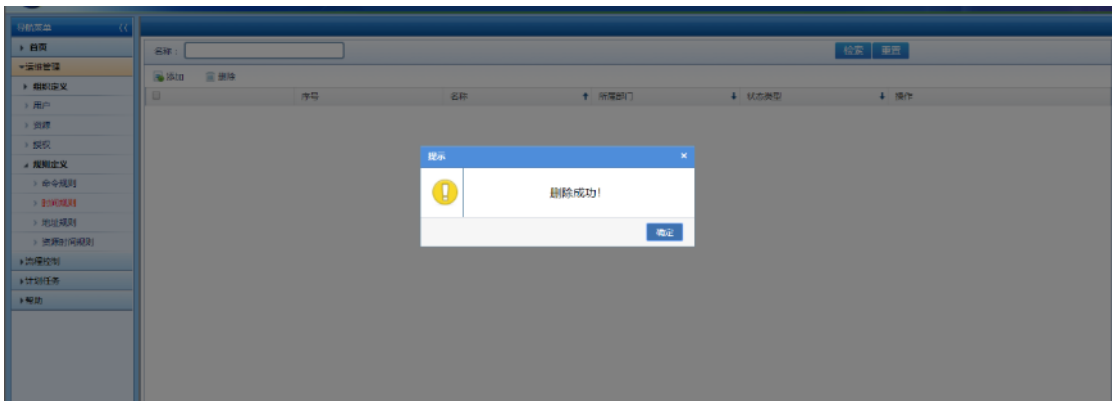
1.逐条删除时间规则

点击名称为**时间规则**右侧的**删除**。

提示你确定要删除该选项吗？



点击确定，提示删除成功！

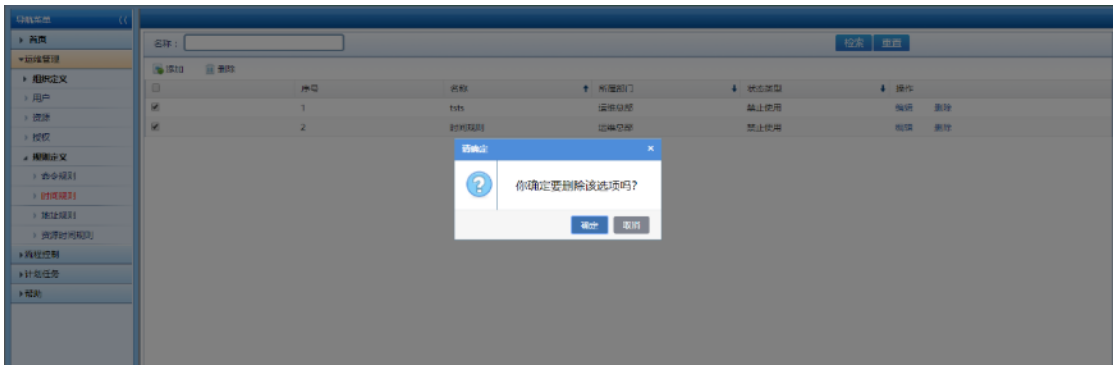


点击确定，返回时间规则页面，列表不显示名称为用户登录时间规则的数据，至此时间规则删除完成。

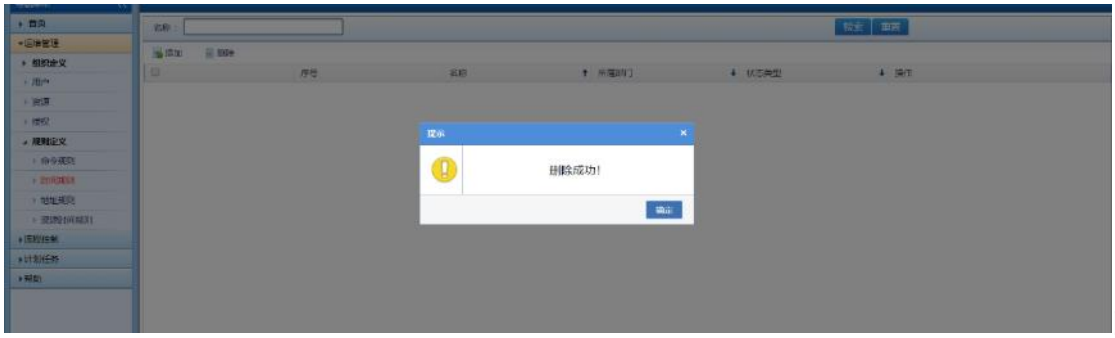
2.批量删除时间规则

勾选名称为时间规则和 test 的规则，点击删除。

提示你确定要删除该选项吗？



点击确定，提示删除成功！



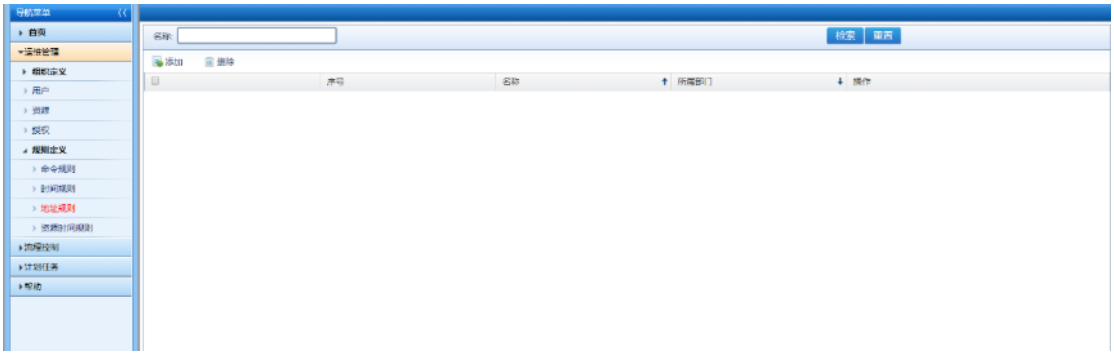
图

点击确定，返回时间规则页面，列表不显示名称为时间规则和 test 的规则，至此时间规则删除完成。

10.3. 地址规则

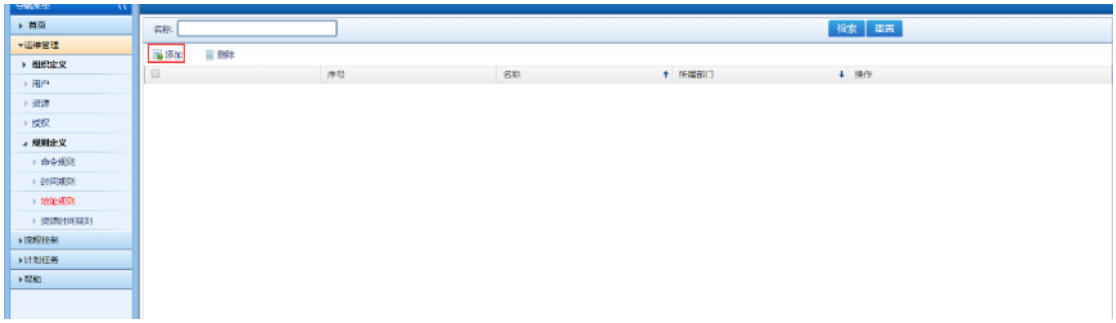
地址规则是对用户登录系统的 IP 地址进行限制。地址规则分为允许访问，禁止访问两种状态。允许访问是允许用户使用该 IP 地址登录系统；禁止访问是禁止用户使用该 IP 地址登录系统。

使用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->规则定义->地址规则链接进入地址规则界面。

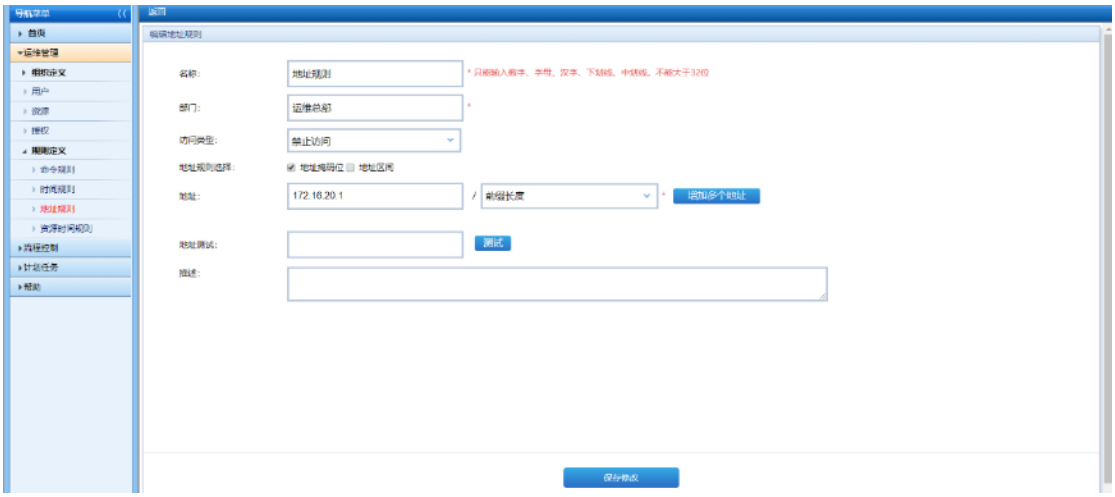


10.3.1. 地址规则添加

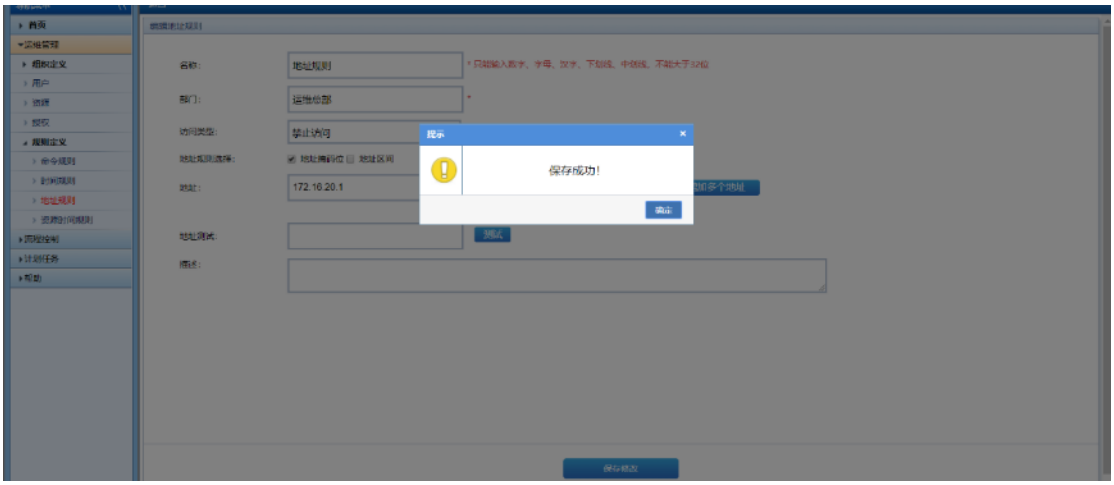
在地址规则界面点击添加。



跳转到地址规则编辑页面，填写信息。

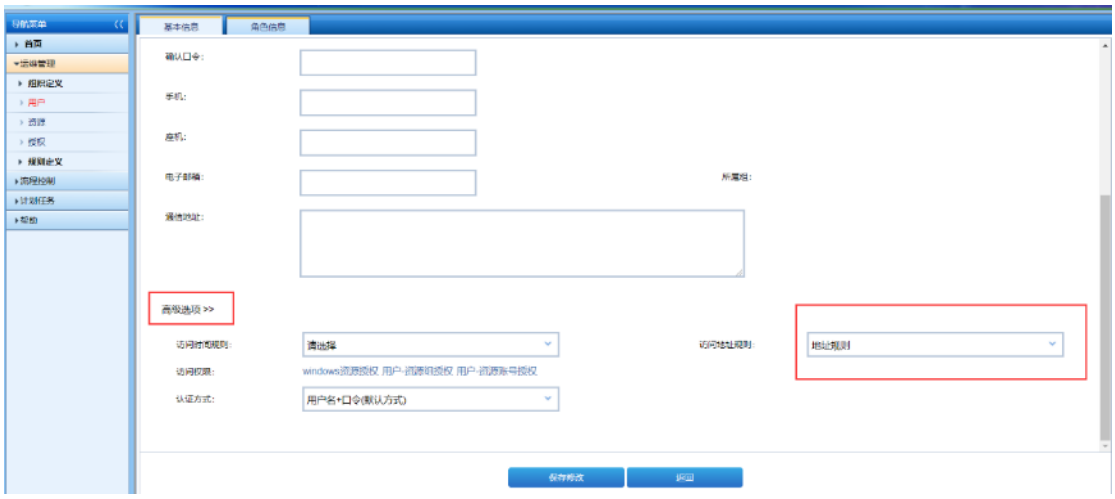


点击保存，提示保存成功！



点击弹出框上的确定按钮，点击返回，页面切换到地址规则列表页面，列表显示一条名称为地址规则的数据，至此地址规则添加完成。

点击运维管理->用户->选择用户 aa 点击编辑->高级选项->选择访问地址规则->保存，将地址规则与用户关联。



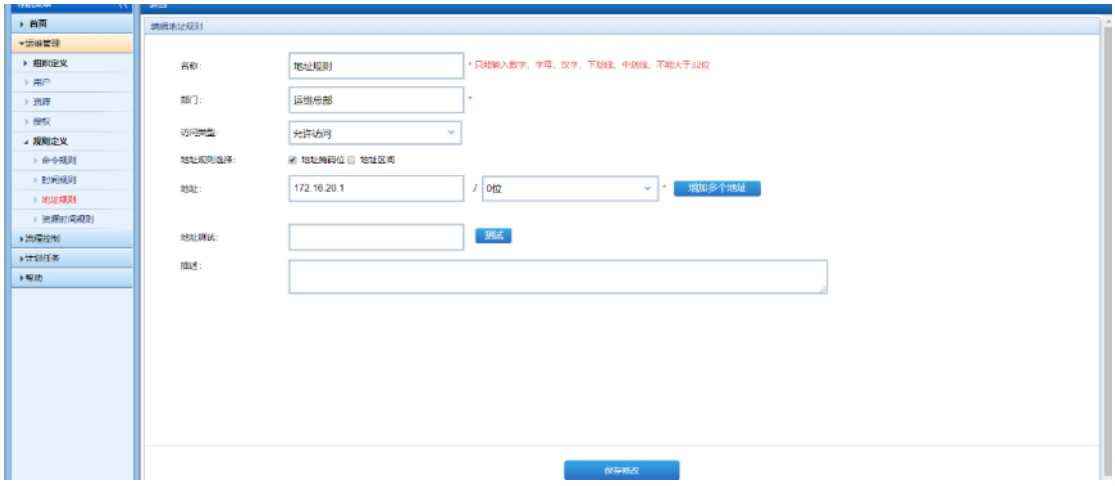
使用用户 aa 登录，提示您没有在 ip：172.16.10.14 下登录的权限。

10.3.2. 地址规则修改

点击名称为**地址规则**右侧的**编辑**。

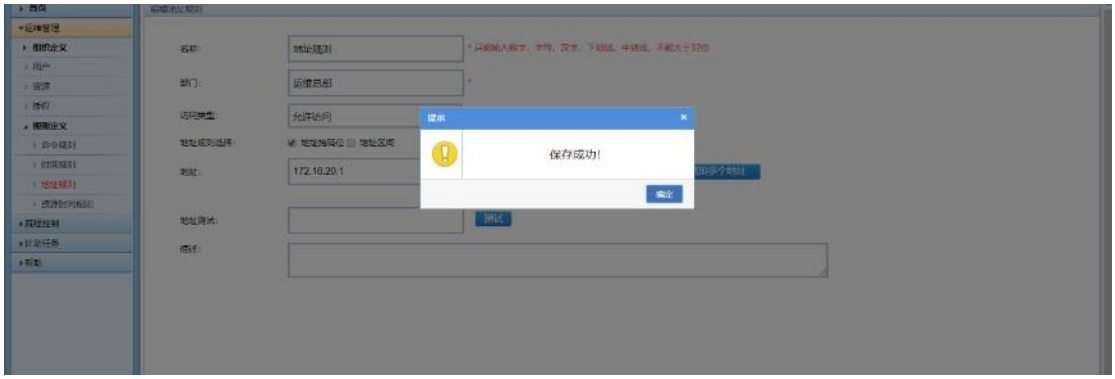
图

跳转到编辑页面，将名称为**地址规则**的访问类型修改为**允许访问**。

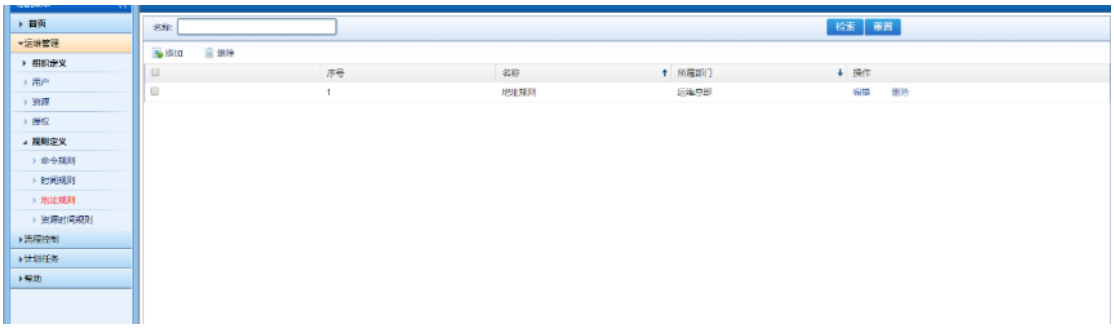


图

点击保存，提示保存成功！



点击弹出框上的确定按钮，点击返回，页面切换到地址规则列表页面。

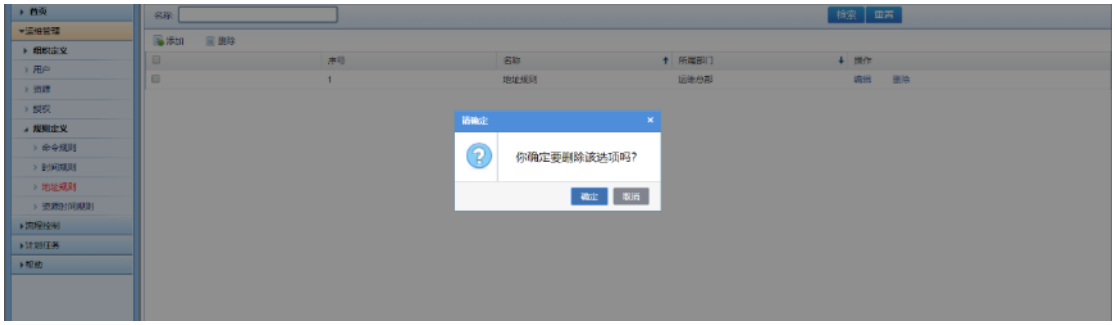


10.3.3. 地址规则删除

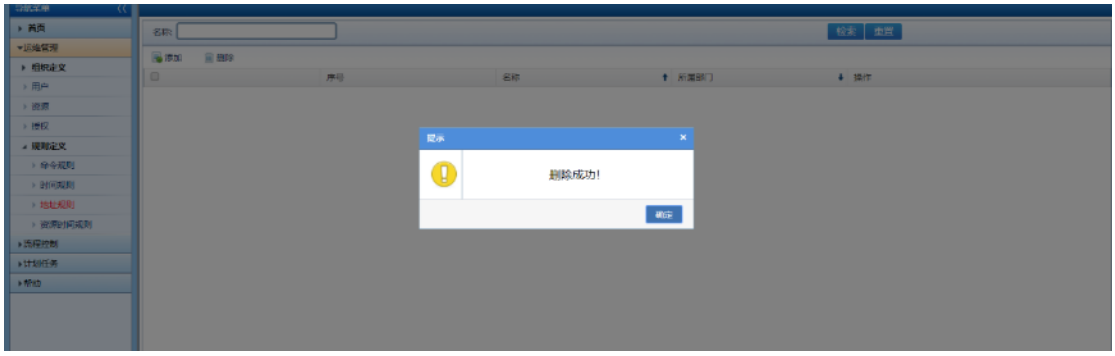
1.逐条删除地址规则

点击名称为**地址规则**右侧的**删除**。

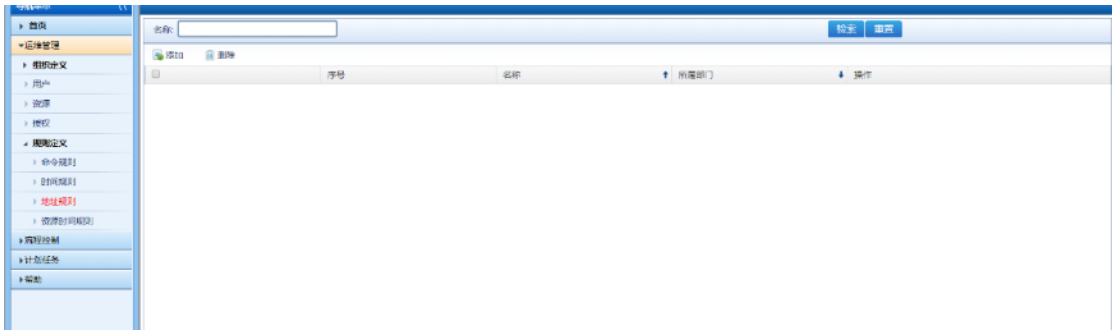
提示你确定要删除该选项吗？



点击确定，提示删除成功！



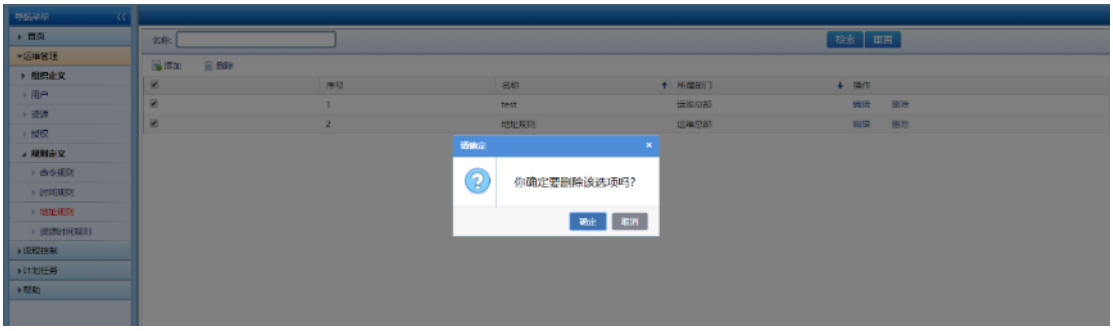
点击确定，返回地址规则页面，列表不显示名称为地址规则的数据，至此地址规则删除完成。



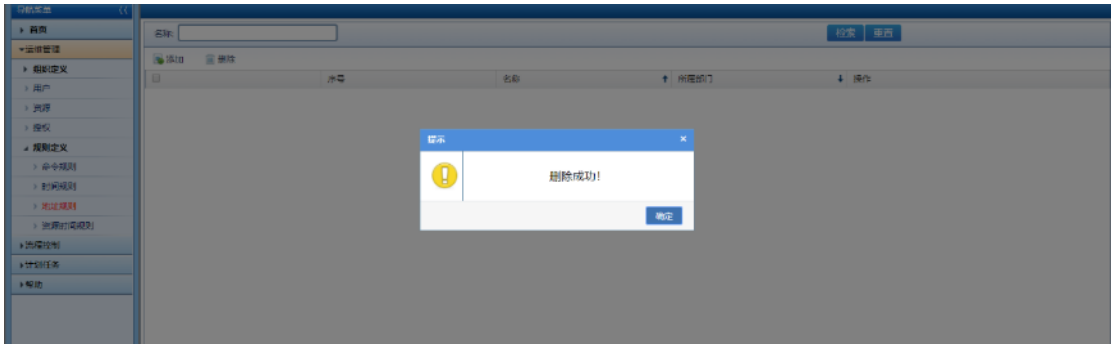
2.批量删除地址规则

勾选名称为地址规则和 test 的规则，点击删除。

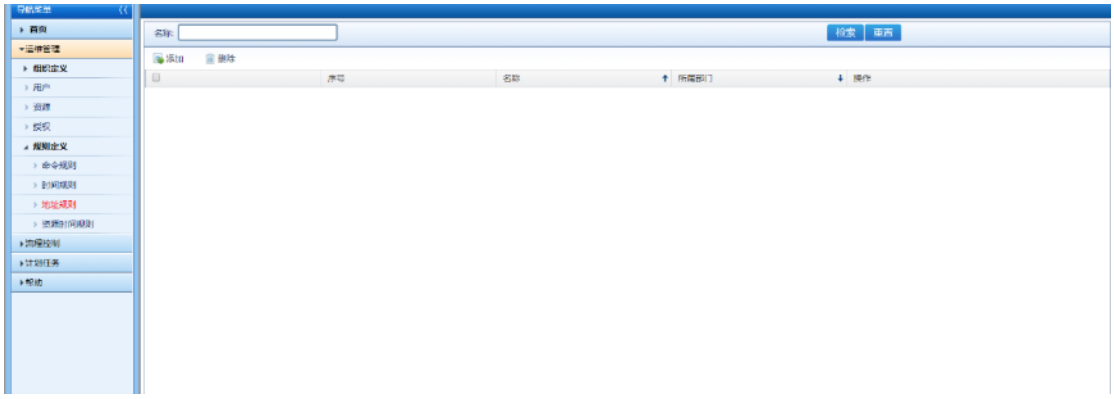
提示你确定要删除该选项吗？



点击确定，提示删除成功！



点击确定，返回地址规则页面，列表不显示名称为地址规则和 test 的规则，至此地址规则删除完成。

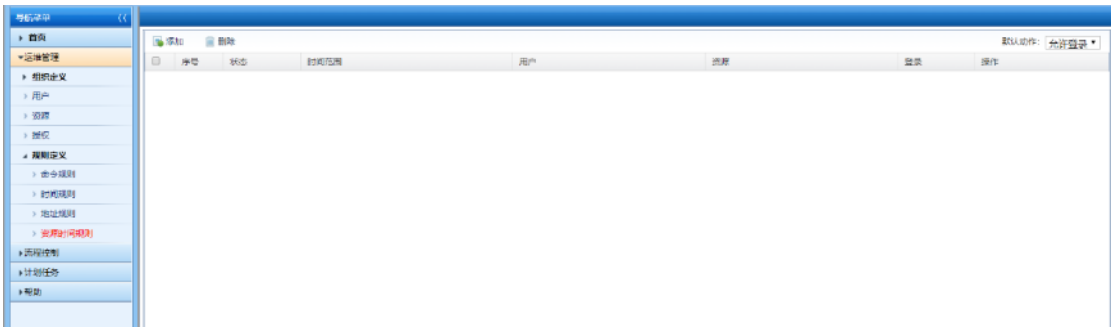


10.4. 资源时间规则

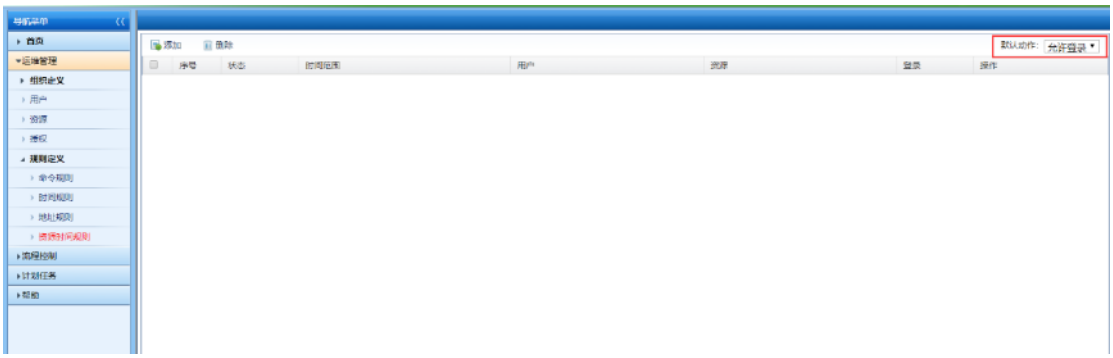
资源时间规则是对被授权的资源进行运维操作时间的限制。

使用安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->规则定义->资

源时间规则链接进入资源时间规则界面。

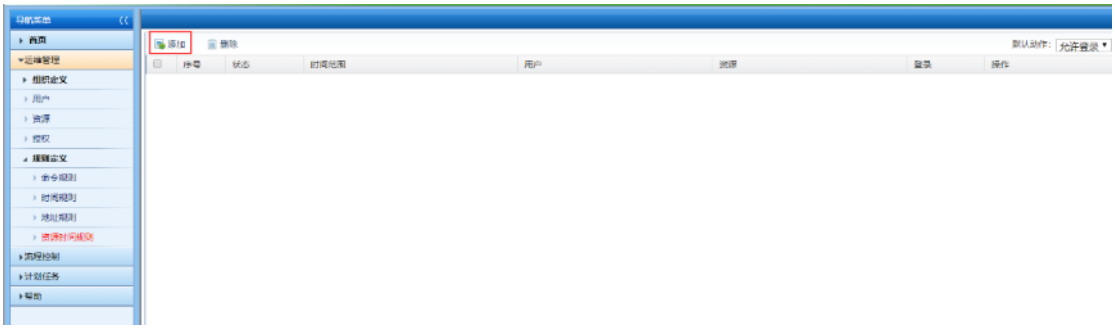


资源时间规则的默认动作为允许登录，被授权的资源是否可进行运维操作只与编辑资源时间规则时的动作有关。默认动作修改为禁止登录后，被授权的资源均不可进行运维操作。

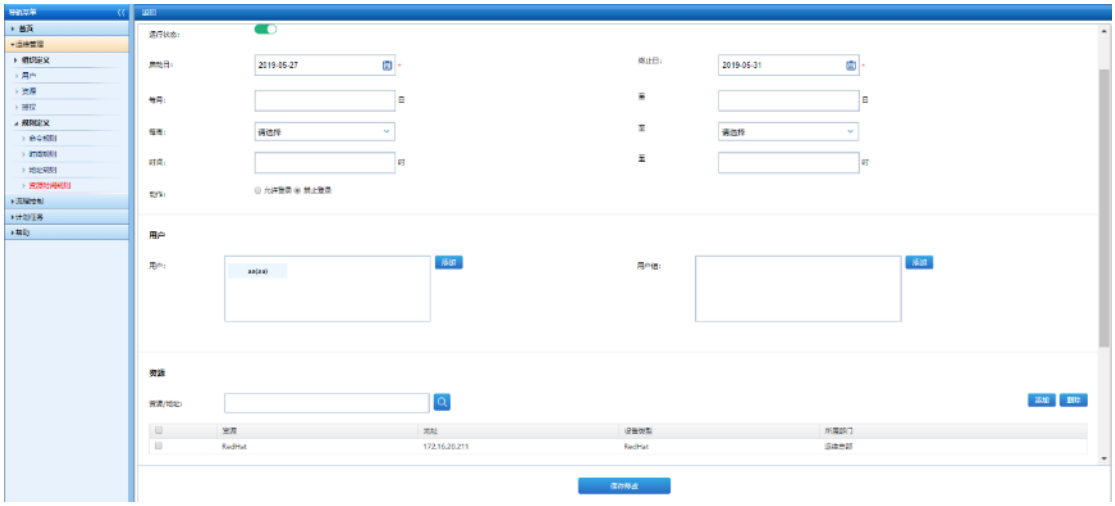


10.4.1. 资源时间规则添加

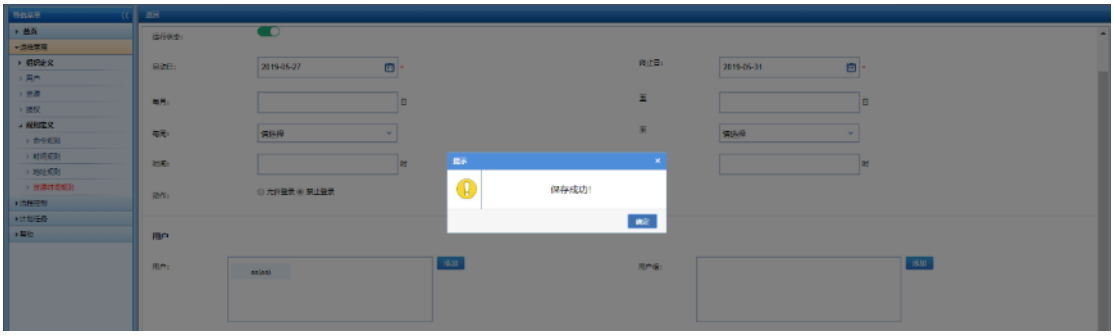
在资源时间规则界面点击添加。



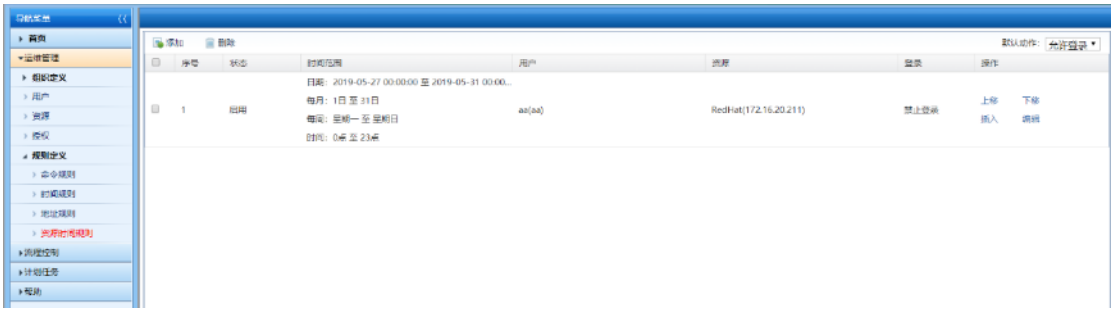
跳转到资源时间规则编辑页面，添加基本信息，动作选择禁止登录，添加用户为 aa，添加资源为 redhat。



点击保存，提示保存成功！



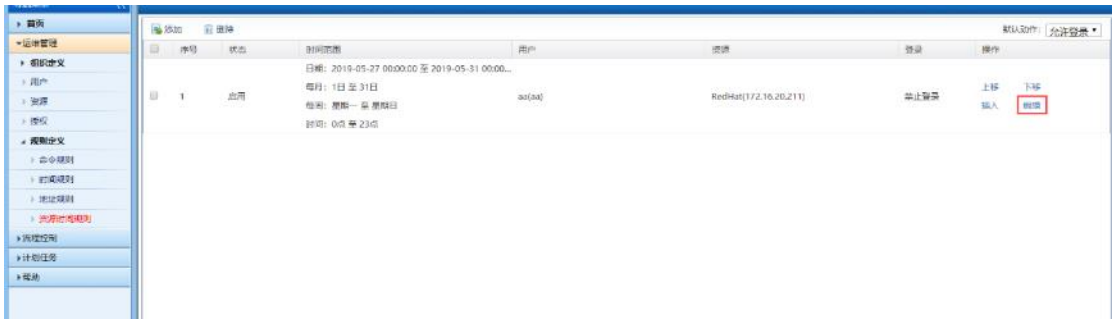
点击弹出框上的确定按钮，点击返回，页面切换到资源时间规则列表页面，列表显示一条资源时间规则，至此资源时间规则添加完成。



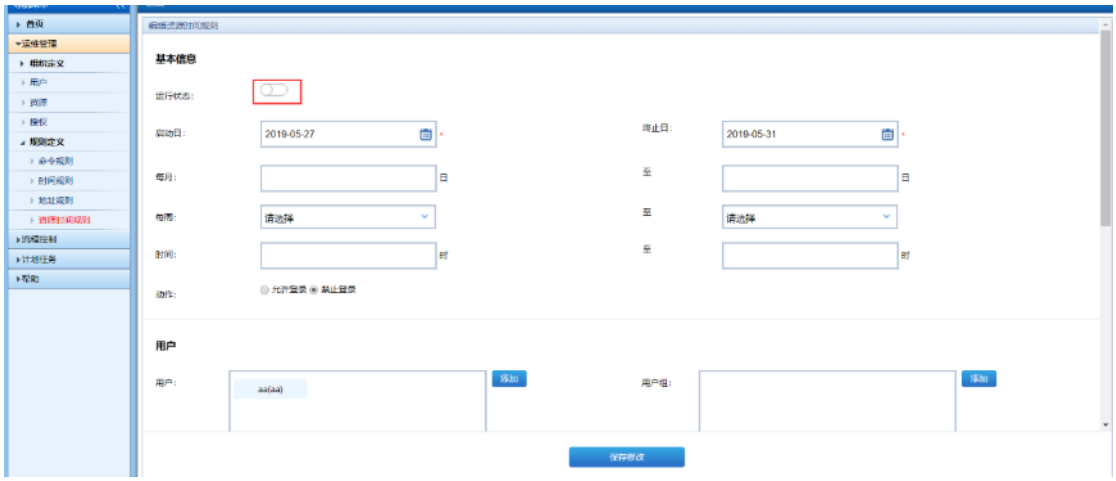
使用 aa 用户对 redhat 资源进行运维操作，提示此资源受时间规则影响，当前时间不允许连接。

10.4.2. 资源时间规则修改

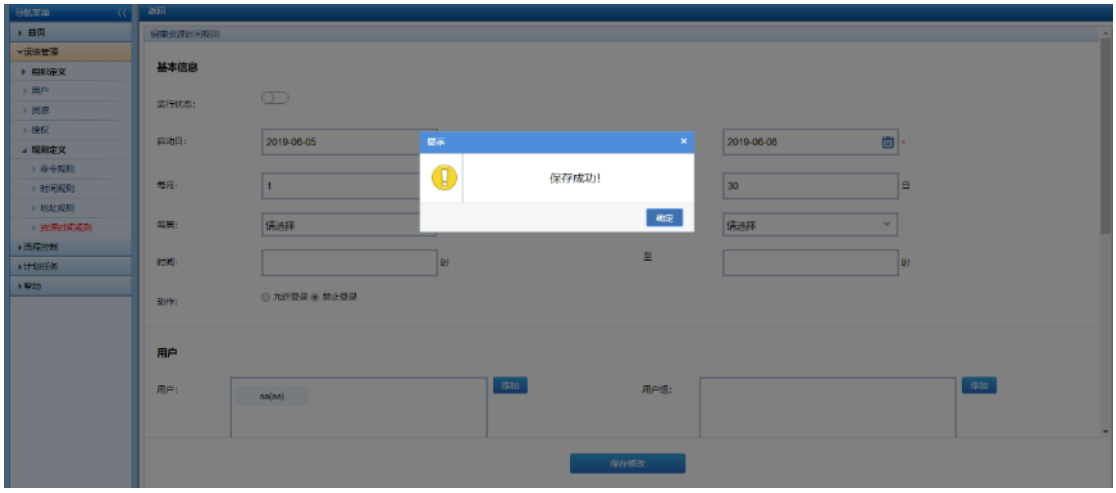
点击编辑可修改资源时间规则信息。



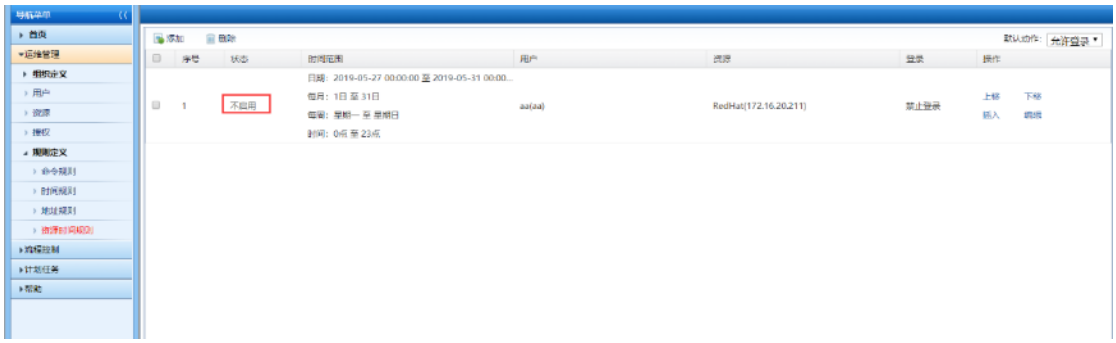
跳转到编辑页面，将运行状态修改为关闭状态。



点击保存，提示保存成功！

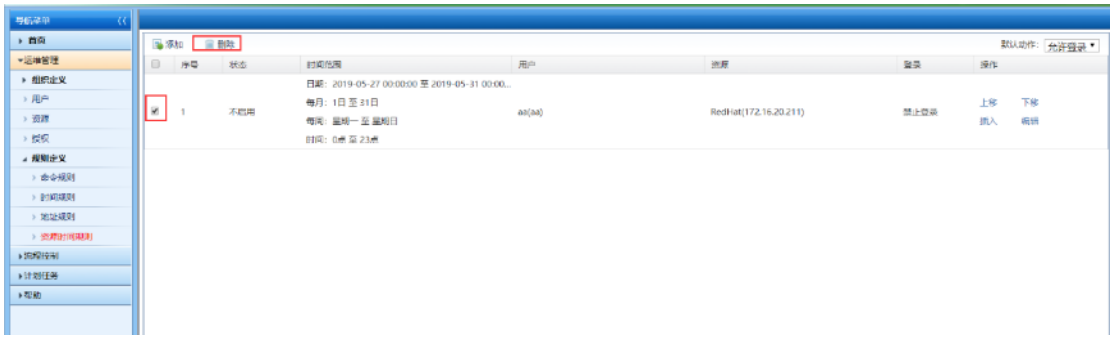


点击弹出框上的确定按钮，点击返回，页面切换到资源时间规则列表页面，列表中资源时间规则的状态修改为不启用。

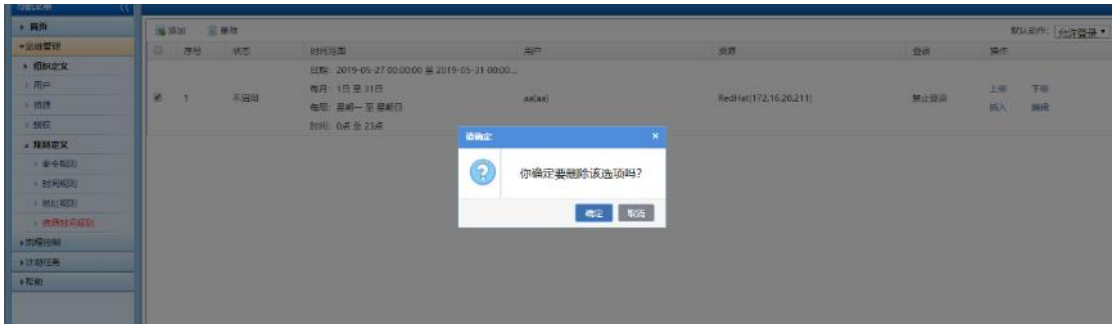


10.4.3. 资源时间规则删除

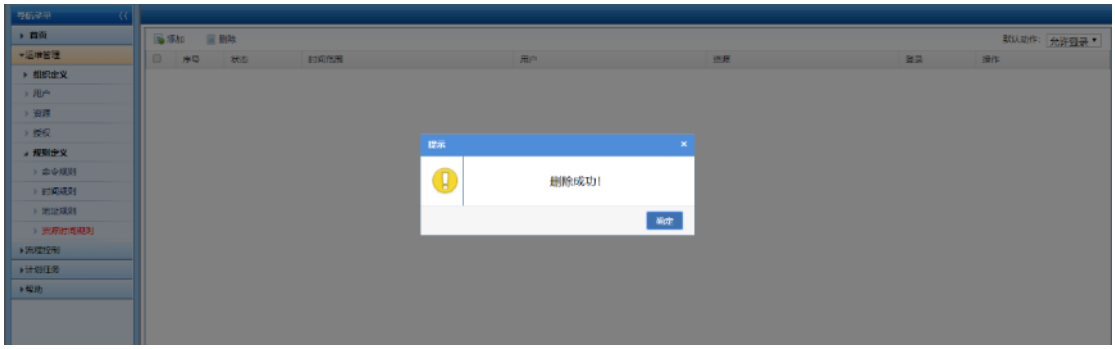
在资源时间规则列表页面，勾选**规则**，点击左上方**删除**。



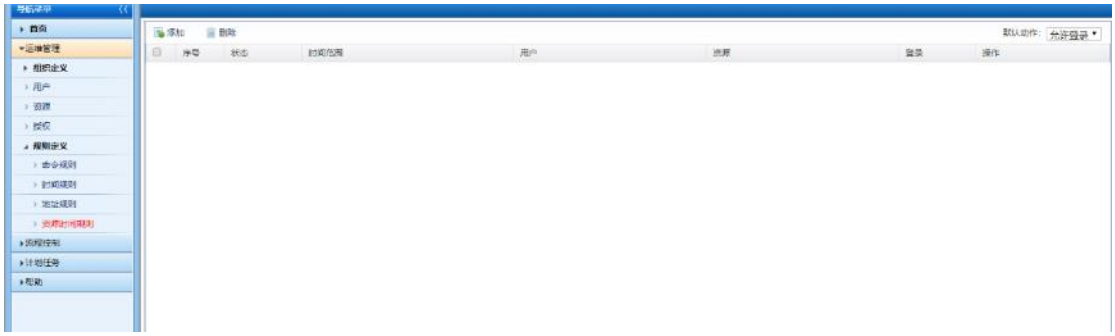
提示你确定要删除要删除该选项吗？



点击确定，提示删除成功！

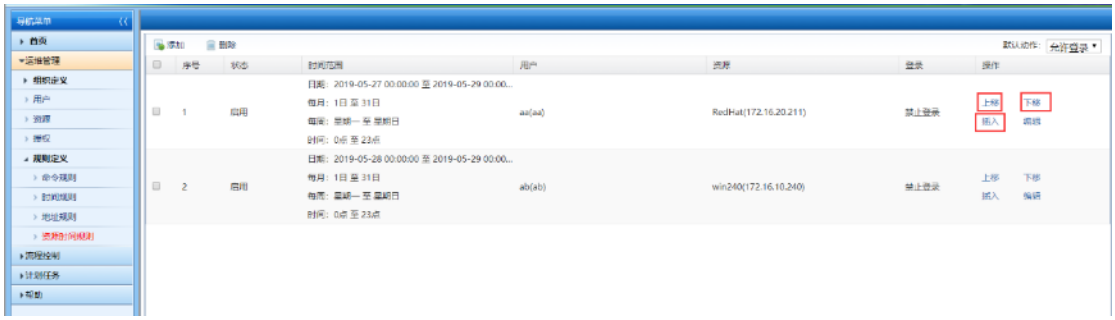


点击确定，返回资源时间规则页面，列表不显示用户为 aa 的规则，至此资源时间规则删除完成。



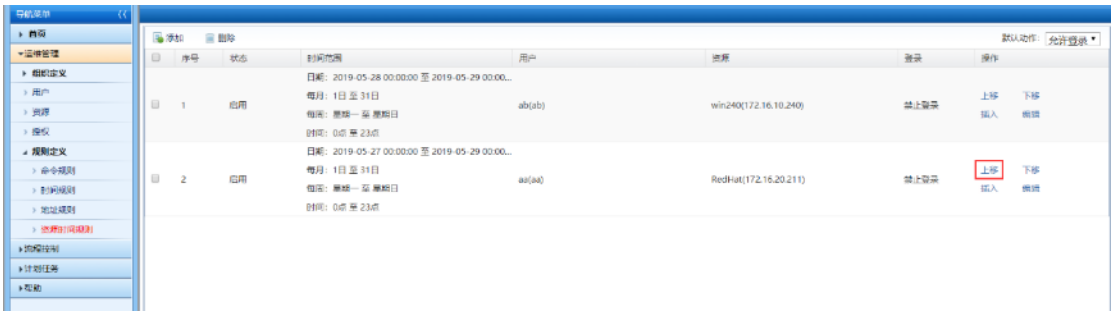
10.4.4. 资源时间规则排序

资源时间规则条目之间可通过上移/下移/插入按钮进行排序。

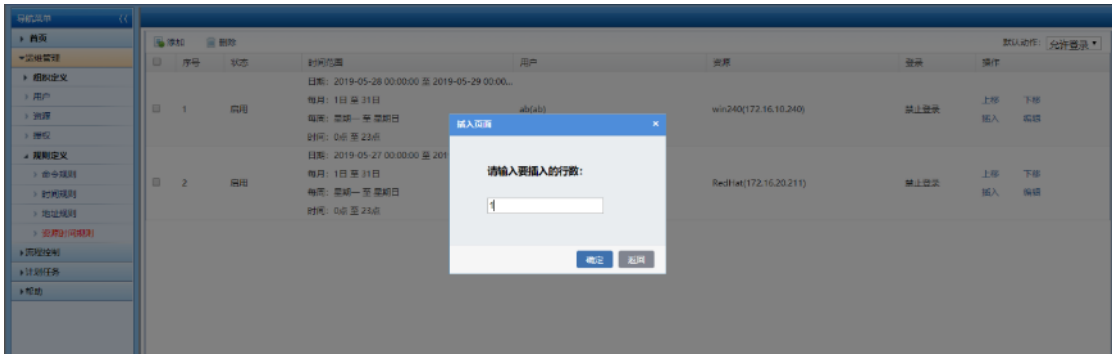


当规则已处于最上方时，不可再进行上移，点击上移，弹出告警信息已经在最上面！下移同理。

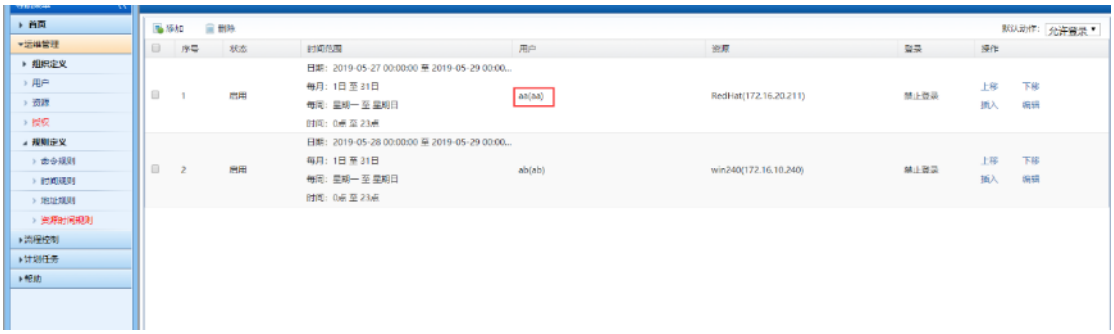
点击上移，用户为 aa 的规则向上移动一位，下移同理。



选择用户为 aa 的规则点击插入，弹出插入页面，在要插入的行数中写入 1。



点击确定，用户为 aa 的规则变为第一行。

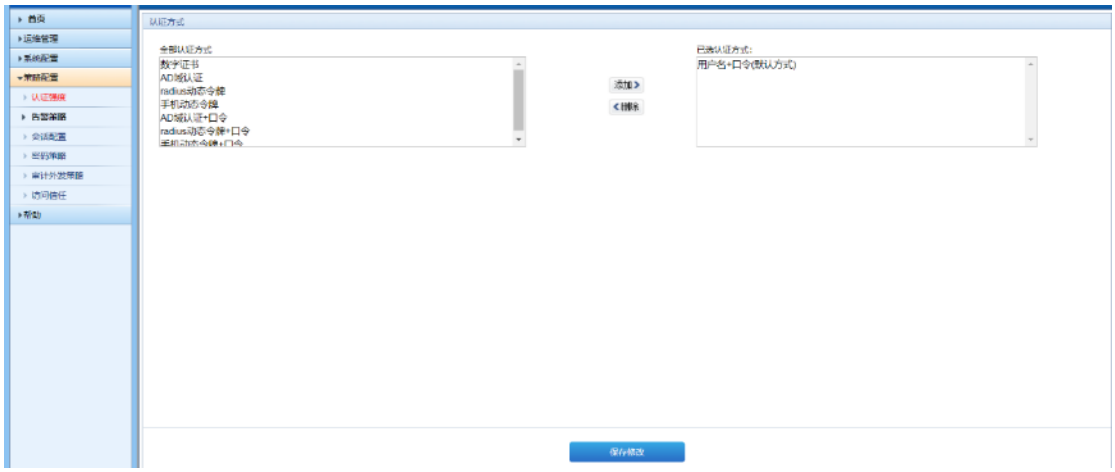


11. 策略配置

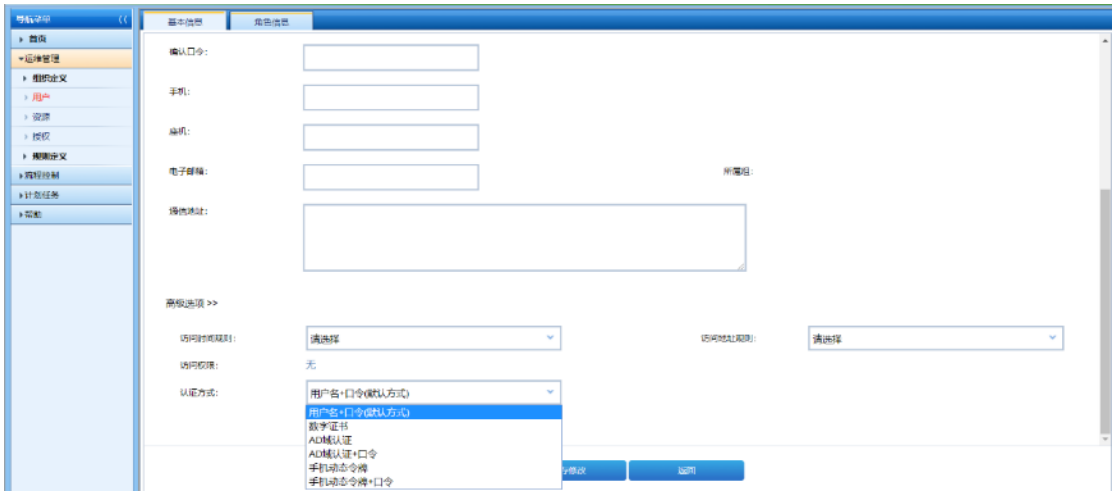
11.1. 认证强度

认证强度是指用户登录系统的认证方式。支持的认证方式包括用户名+口令（默认方式）、AD 域认证、AD 域认证+口令、radius 动态令牌、radius 动态令牌+口令、数字证书。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->认证强度链接进入认证强度界面。

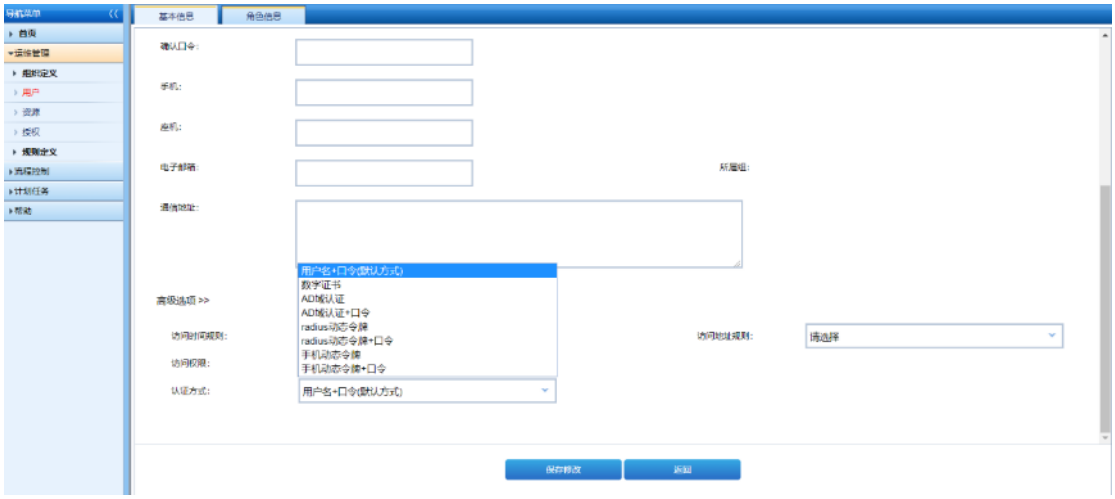


配置完成认证方式后，安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户->编辑->高级选项链接选择用户登录认证方式。

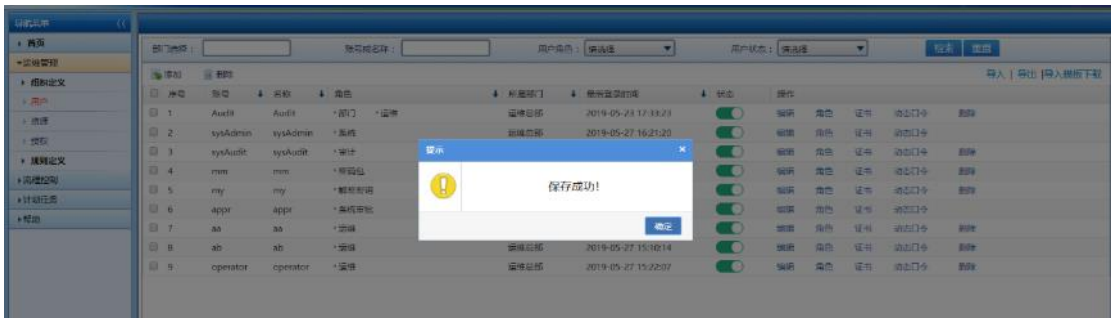


11.1.1. 用户名+口令

在认证强度页面，选择用户名+口令（默认方式），点击添加按钮，将用户名+口令（默认方式）添加到已选认证方式列表。



点击保存，提示保存成功！



点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示用户名+口令（默认方式）。因用户名+口令为默认登录方式，所以无需在用户高级选项中进行配置。

在用户登录界面，选择用户名+口令（默认方式）登录方式，输入正确的账号和口令。

点击登录按钮，即可登录系统。

11.1.2. AD 域认证

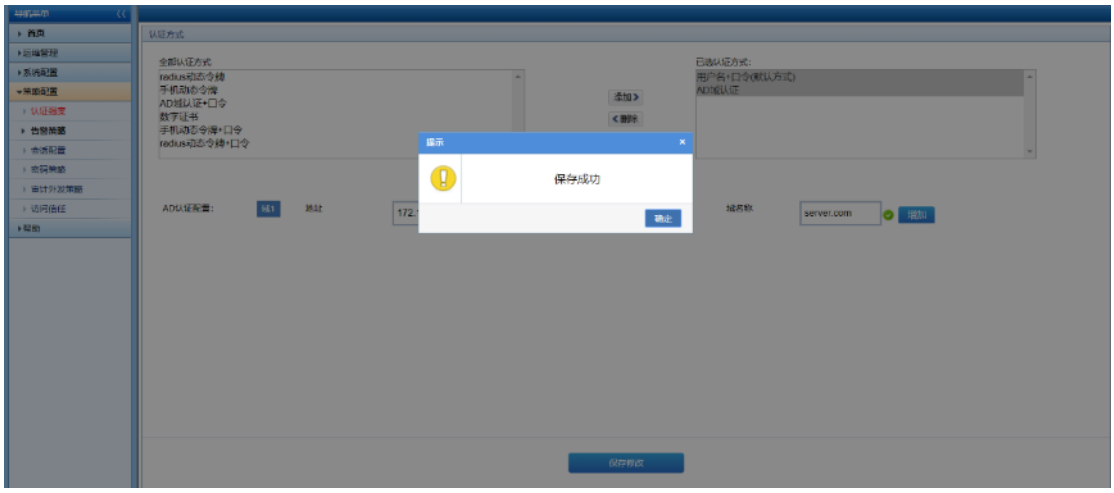
在认证强度页面，选择 AD 域认证，点击添加按钮，将 AD 域认证添加到已选认证方式列表。并进行 AD 认证配置：

1) 域 IP：172.16.10.26

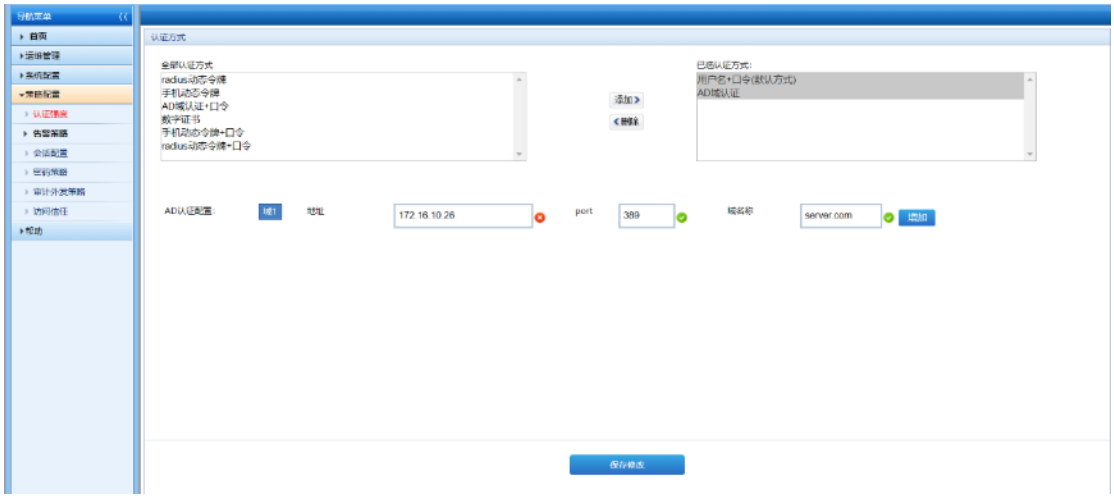
2) port：389

3) 域名称：server.com

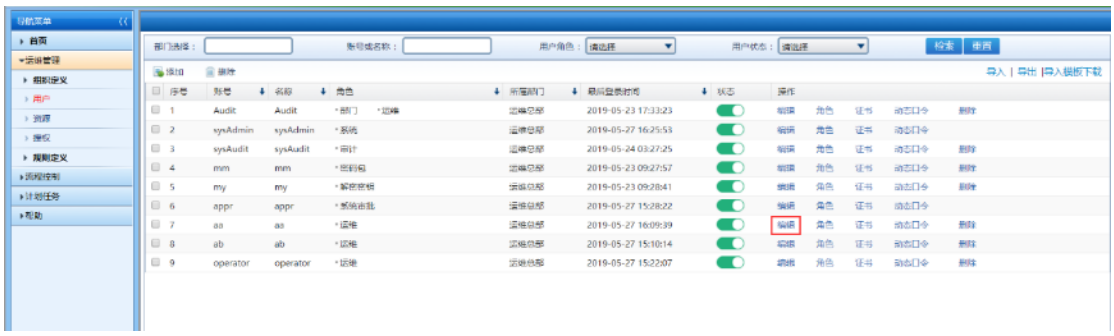
点击保存，提示保存成功！



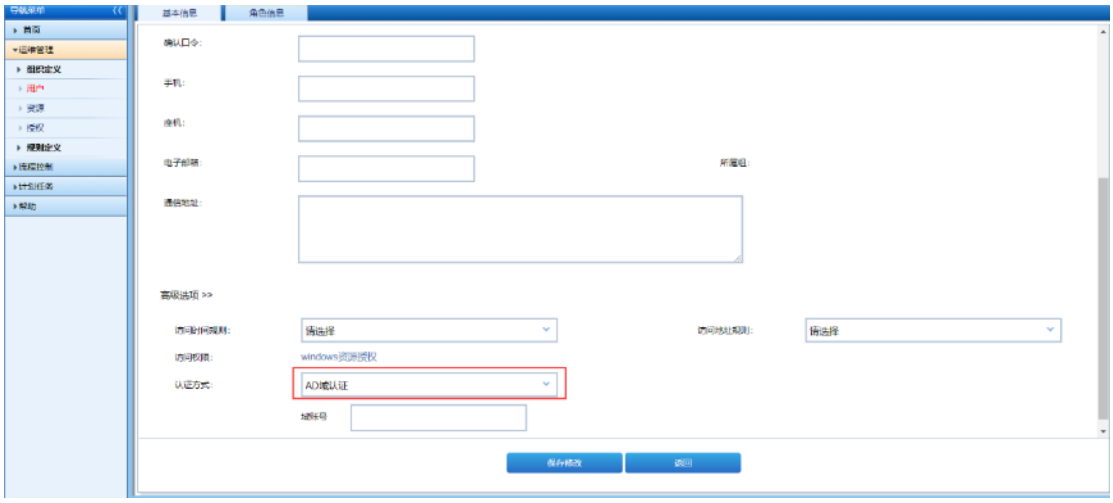
点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示 AD 域认证。



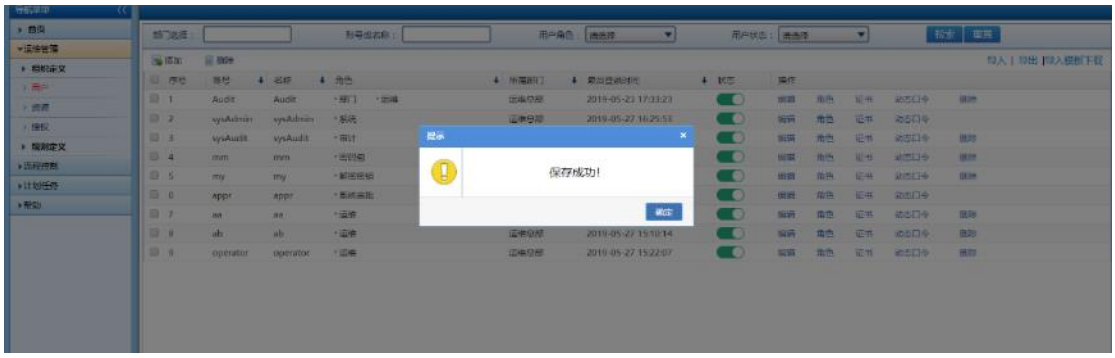
安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的编辑按钮。



进入用户基本信息编辑页面，点击高级选项，选择用户认证方式 AD 域认证，输入域帐号 aa。



点击保存，提示保存成功！



点击弹出框上的确定按钮，即为用户 aa 绑定了 AD 域认证的登录方式，在用户登录界面，选择 AD 域认证登录方式，输入正确的用户名和域口令。

点击登录按钮，即可登录系统。

11.1.3. AD 域认证+口令

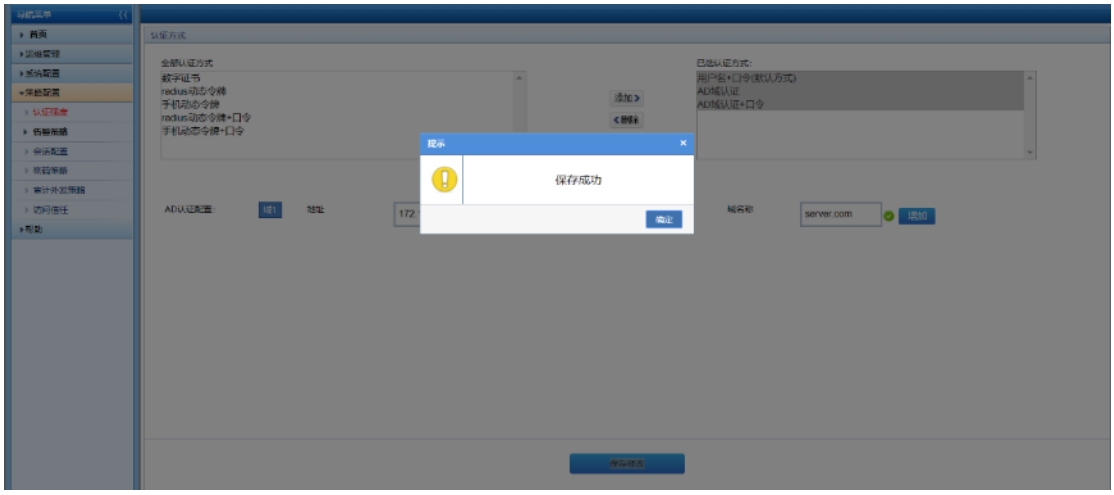
在认证强度页面，选择 AD 域认证+口令，点击添加按钮，将 AD 域认证+口令添加到已选认证方式列表。并进行 AD 认证配置：

1) 域 IP：172.16.10.26

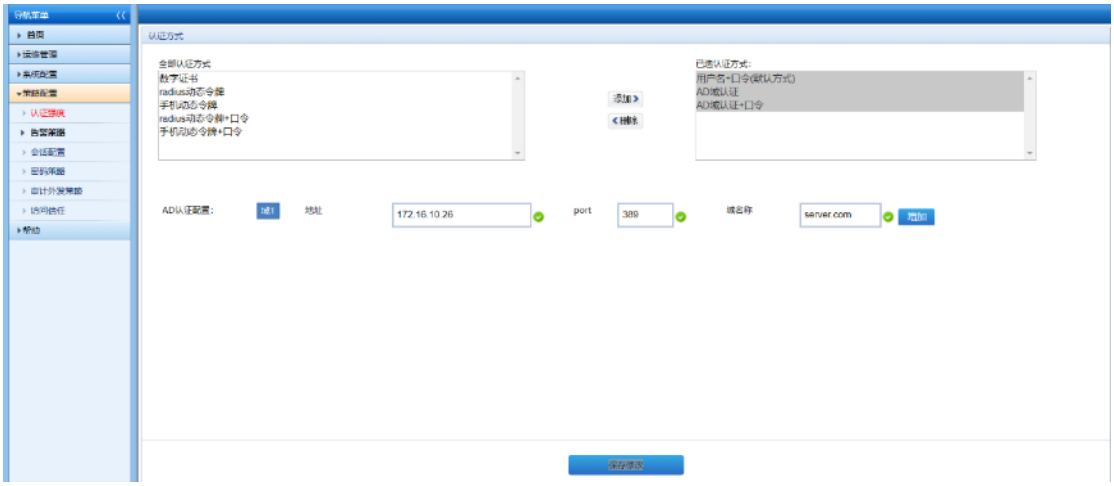
2) port：389

3) 域名称：server.com

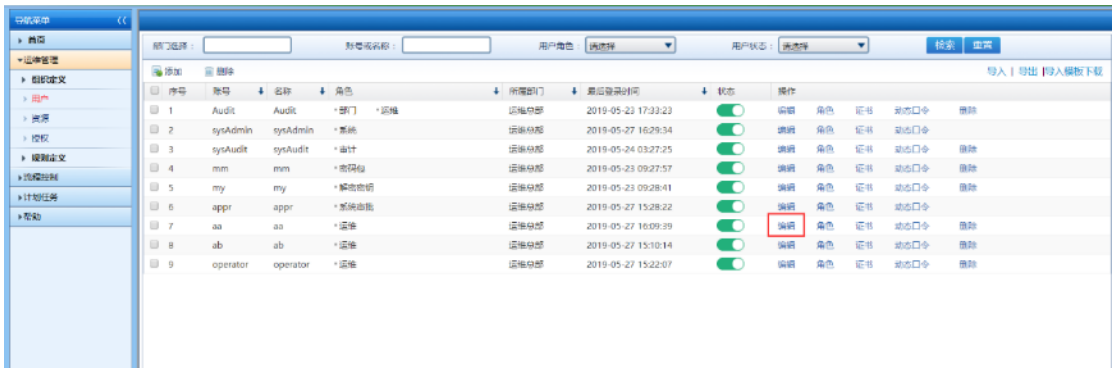
点击保存，提示保存成功！



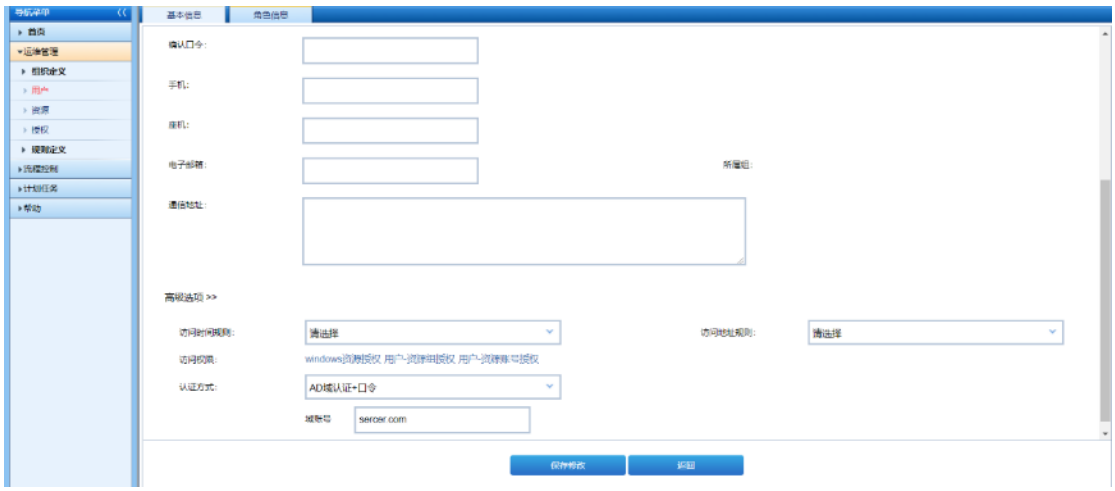
点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示 AD 域认证+口令。



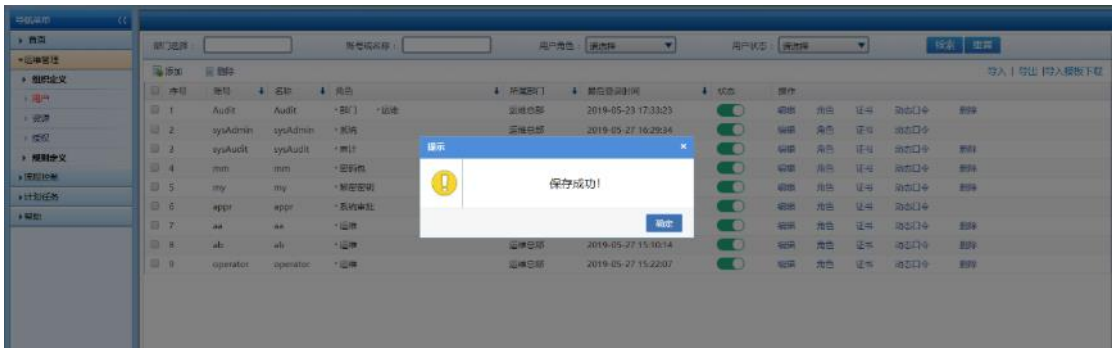
安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的编辑按钮。



进入用户基本信息编辑页面，点击高级选项，选择用户认证方式 AD 域认证+口令，输入域帐号 lc。



点击保存，提示保存成功！



点击弹出框上的确定按钮，即为用户 aa 绑定了 AD 域认证+口令的登录方式，在用户登录界面，选择 AD 域认证+口令登录方式，输入正确的用户名、口令和域口令。

点击登录按钮，即可登录系统。

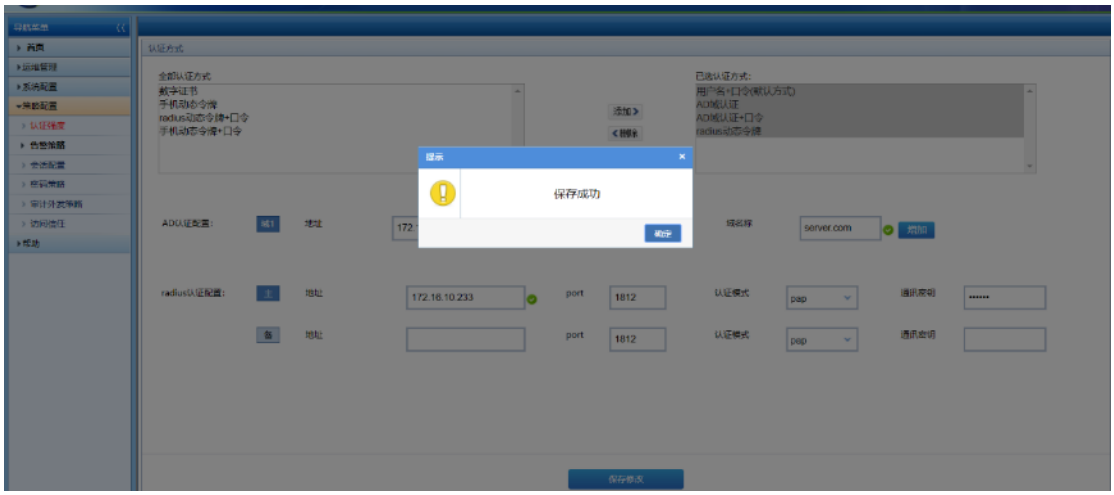
11.1.4. radius 动态令牌

在认证强度页面，选择 radius 动态令牌，点击添加按钮，将 radius 动态令牌添加到已选认证方式列表。并进行 radius 认证配置：

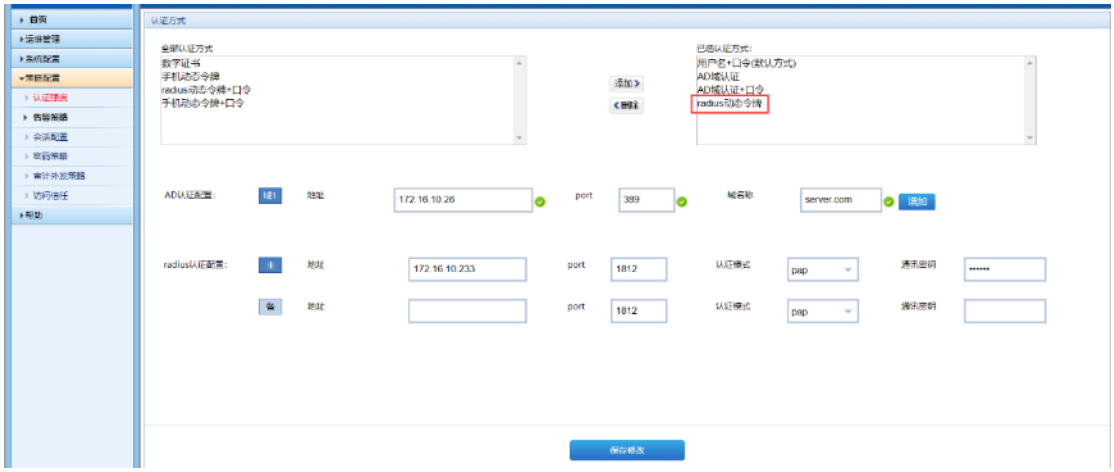
1) 主 IP：172.16.10.223
2) port：1812
3) 认证模式：pap

4) 通讯密钥：12345678

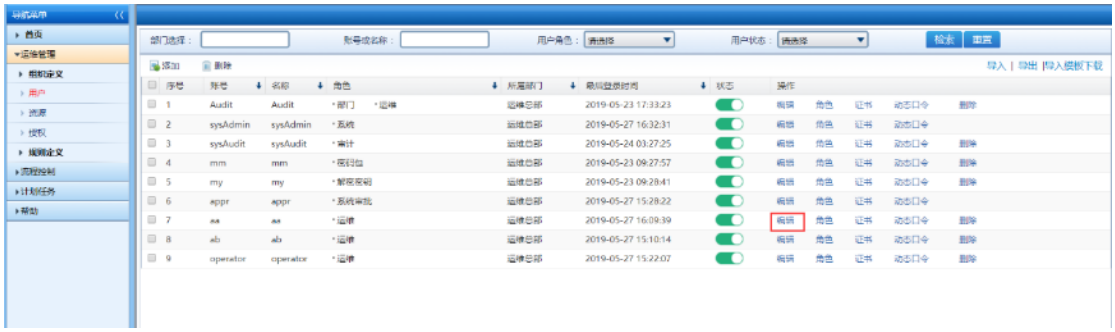
点击保存，提示保存成功！



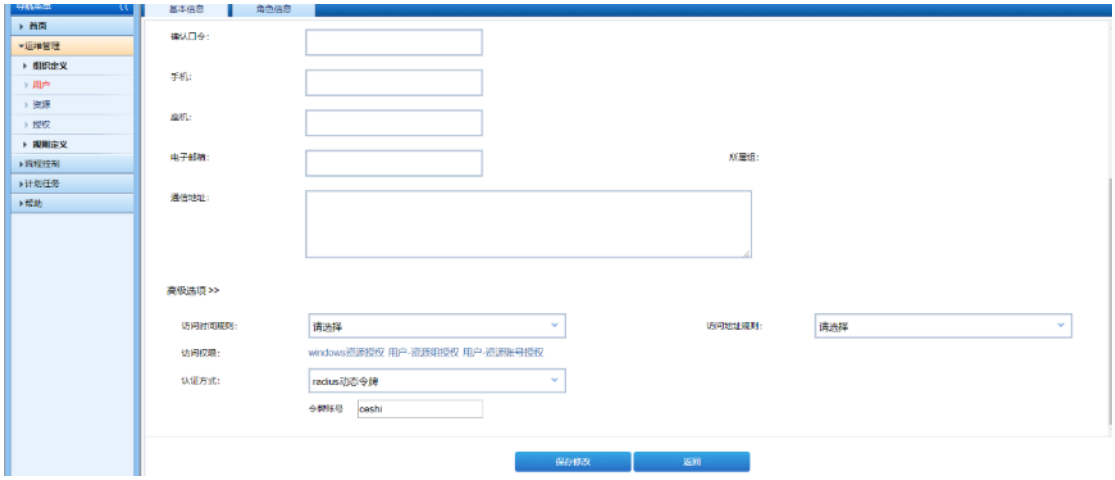
点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示 radius 动态令牌。



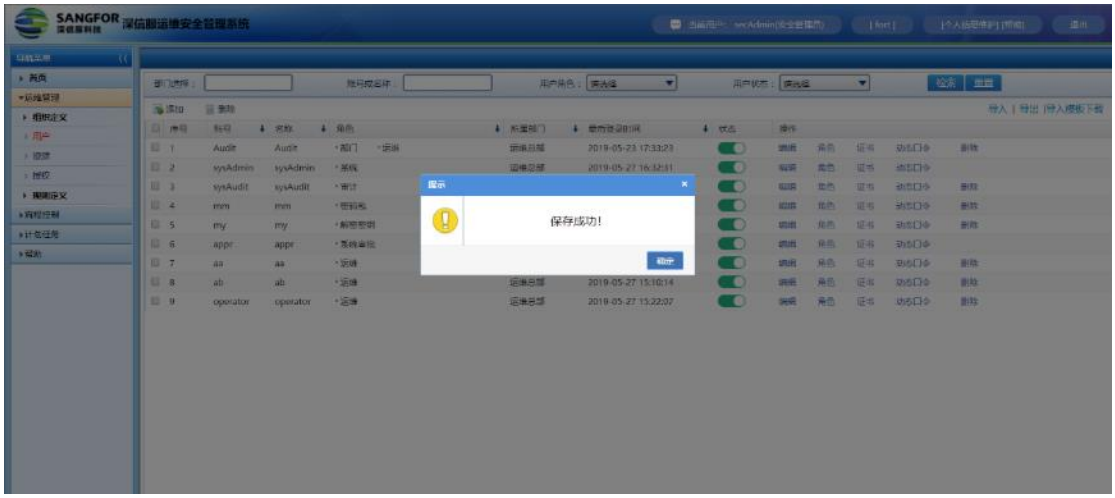
安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的编辑按钮。



进入用户基本信息编辑页面，点击高级选项，选择用户认证方式 radius 动态令牌，输入令牌帐号 ceshi。



点击保存，提示保存成功！

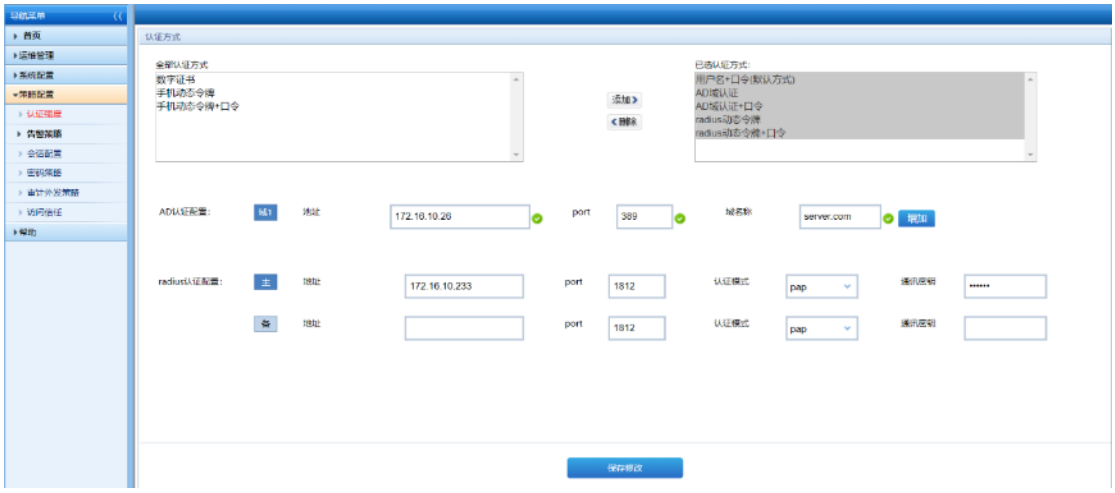


点击弹出框上的确定按钮，即为用户 aa 绑定了 radius 动态令牌的登录方式，在用户登录界面，选择 radius 动态令牌登录方式，输入正确的用户名和动态口令。

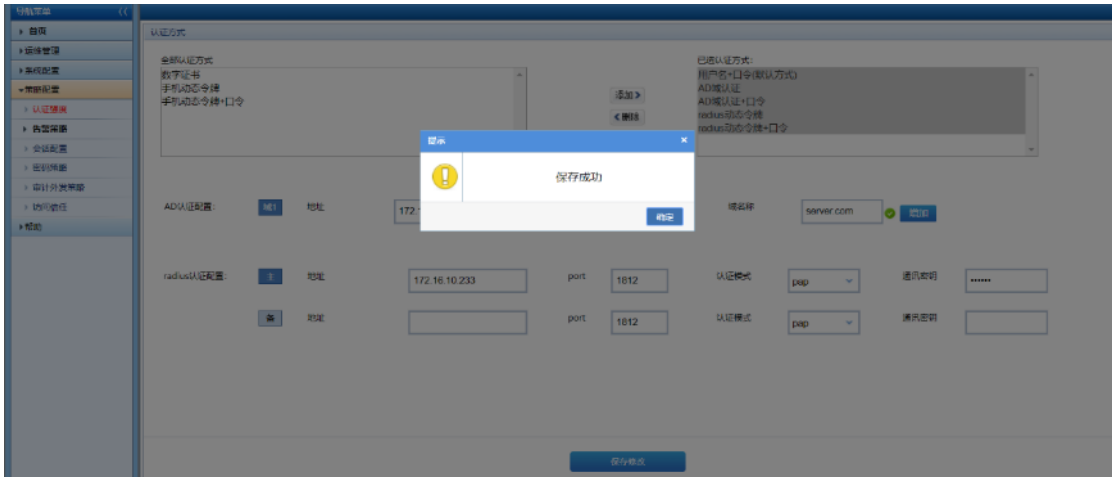
11.1.5. radius 动态令牌+口令

在认证强度页面，选择 radius 动态令牌+口令，点击添加按钮，将 radius 动态令牌+口令添加到已选认证方式列表。并进行 radius 认证配置：

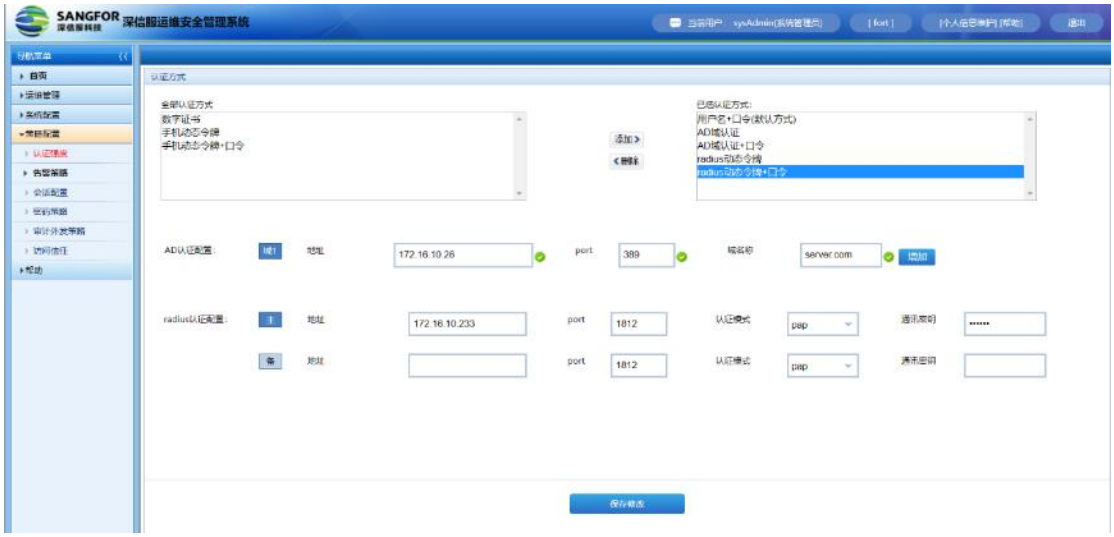
1) 主 IP：172.16.10.223
2) port：1812
3) 认证模式：pap
4) 通讯密钥：12345678



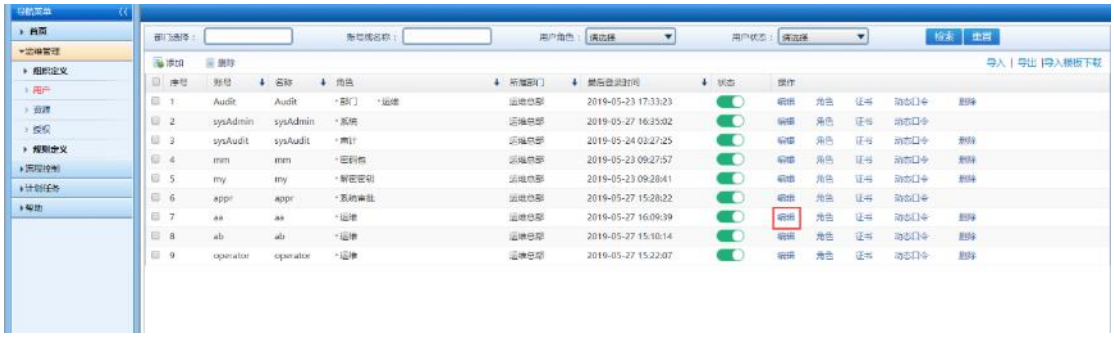
点击保存，提示保存成功！



点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示 radius 动态令牌+口令。

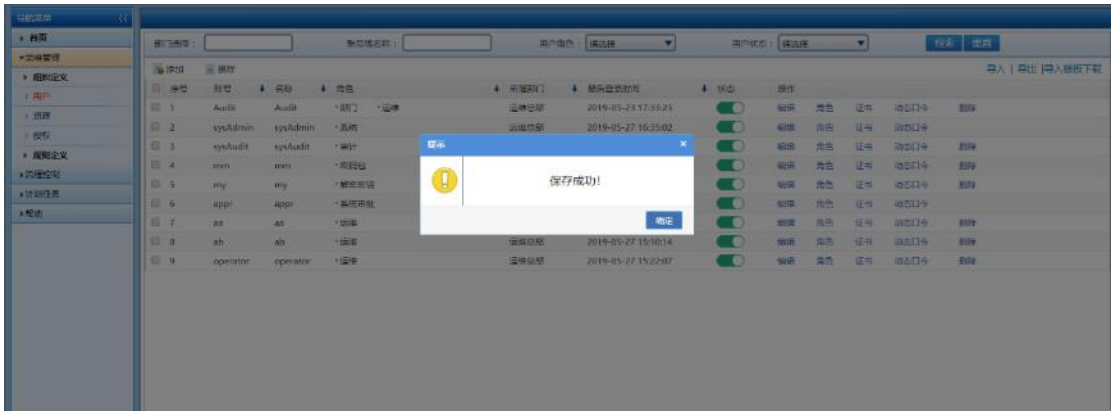


安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的编辑按钮。



进入用户基本信息编辑页面，点击高级选项，选择用户认证方式 radius 动态令牌+口令，输入令牌帐号 ceshi。

点击保存，提示保存成功！



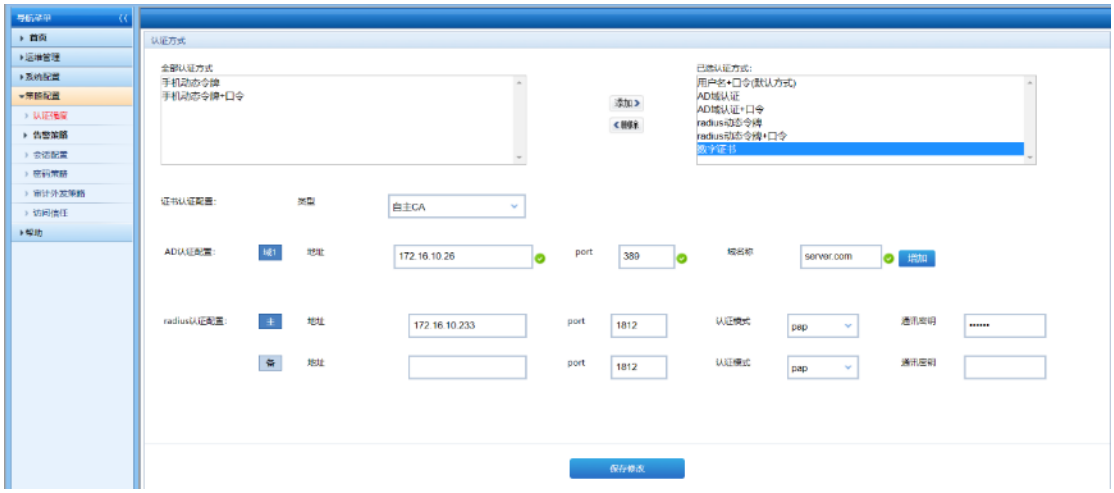
点击弹出框上的确定按钮，即为用户 aa 绑定了 radius 动态令牌+口令的登录方式，在用户登录界面，选择 radius 动态令牌+口令登录方式，输入正确的账号、口令和动态口令。

点击登录按钮，即可登录系统。

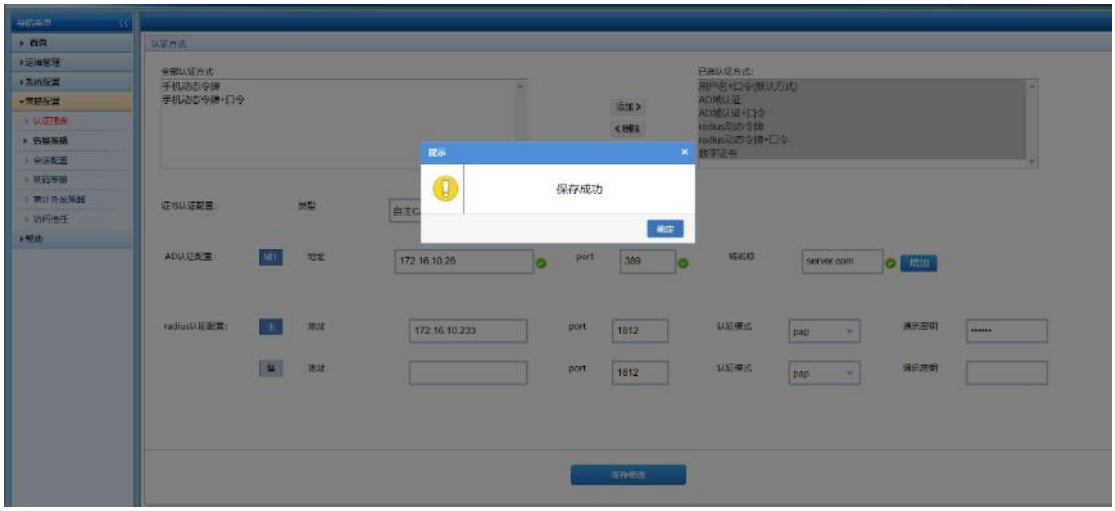
11.1.6. 数字证书

在认证强度页面，选择数字证书，点击添加按钮，将数字证书添加到已选认证方式列表。并进行证书认证配置：

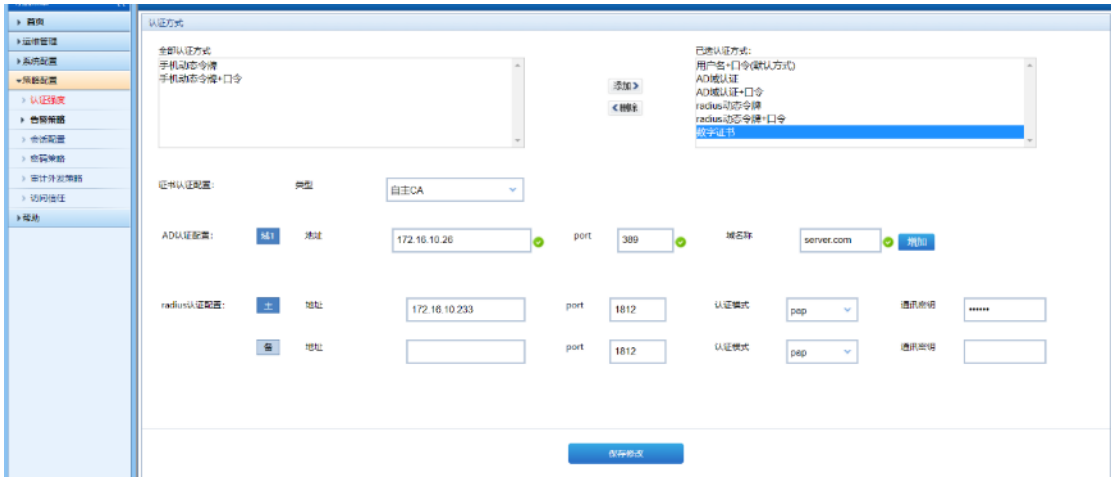
类型：自主 CA



点击保存，提示保存成功！

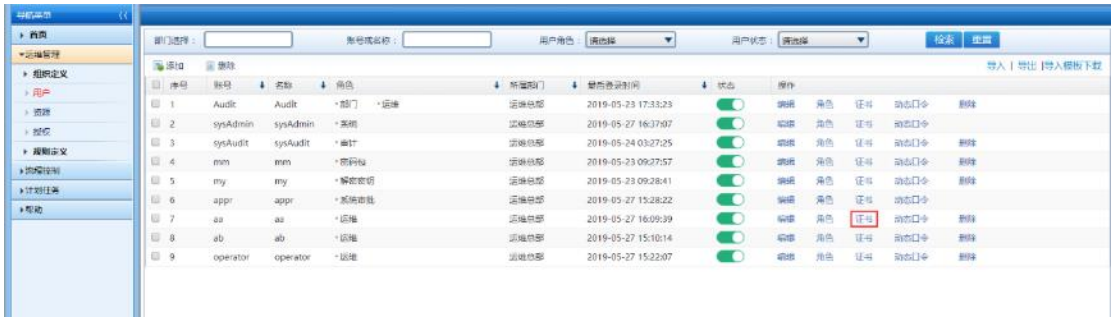


点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示数字证书。

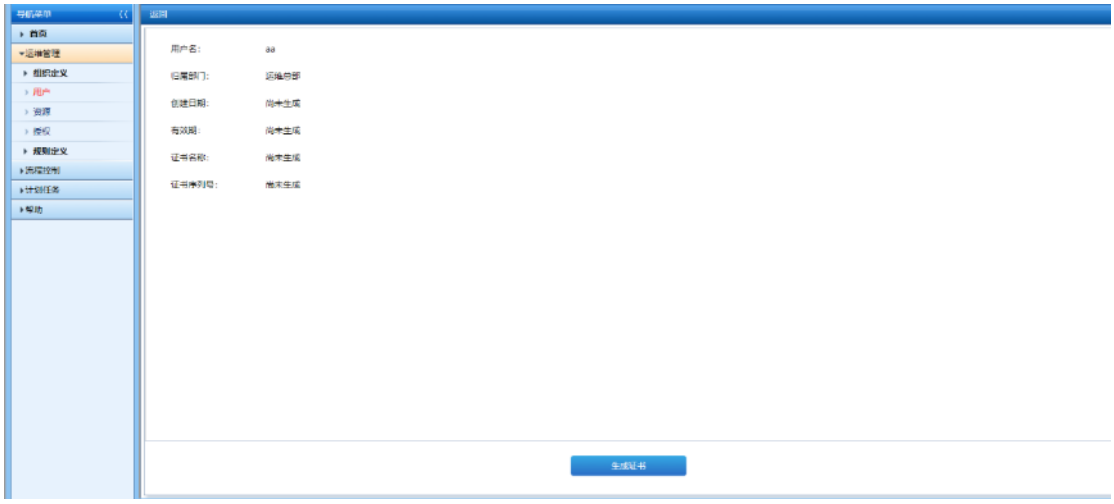


1.生成证书

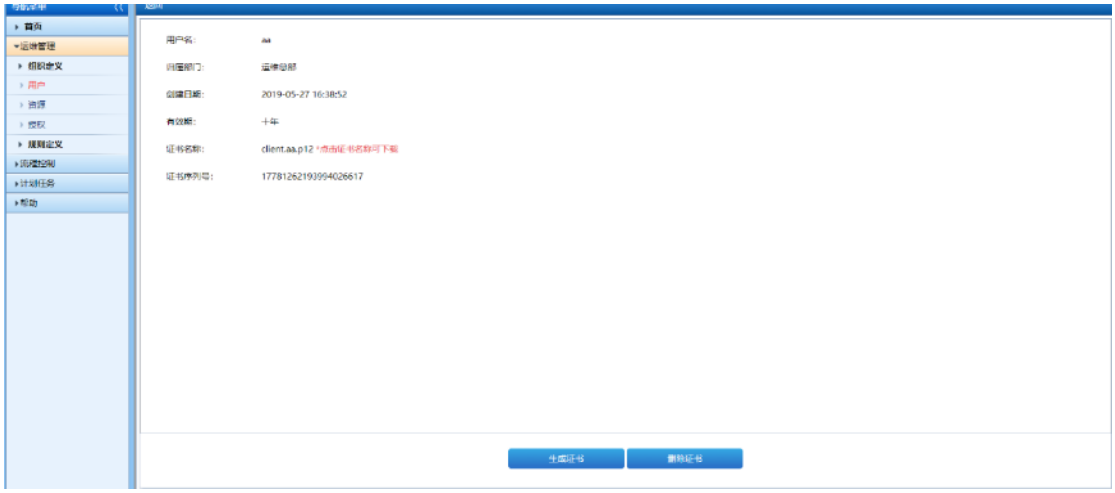
安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的证书按钮。



跳转到用户证书管理页面，点击生成证书按钮。

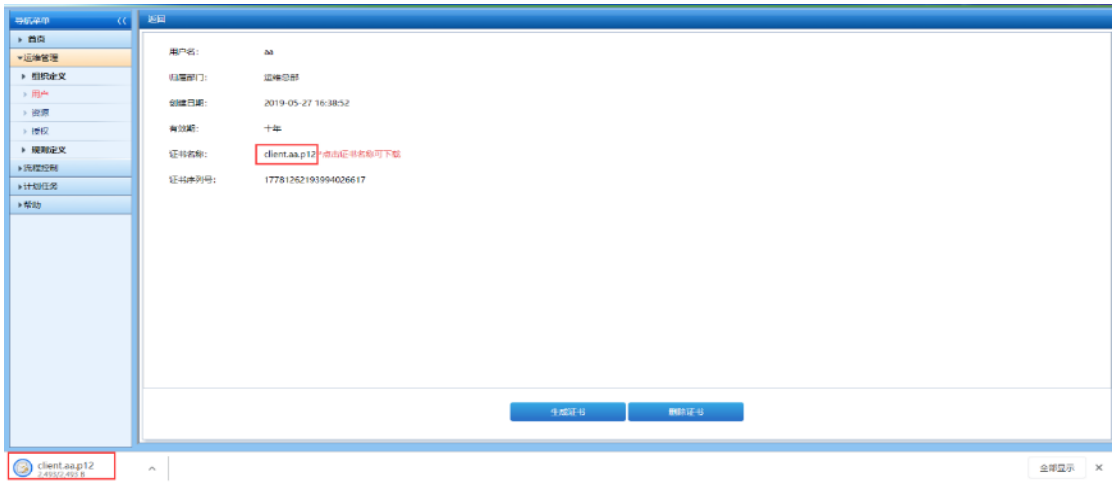


页面即显示证书创建日期、有效期、证书名称、证书序列号。



2.下载证书

用户证书管理页面，点击证书名称，选择存储路径下载证书。



在证书下载路径找到下载的用户证书 client.aa.p12 。

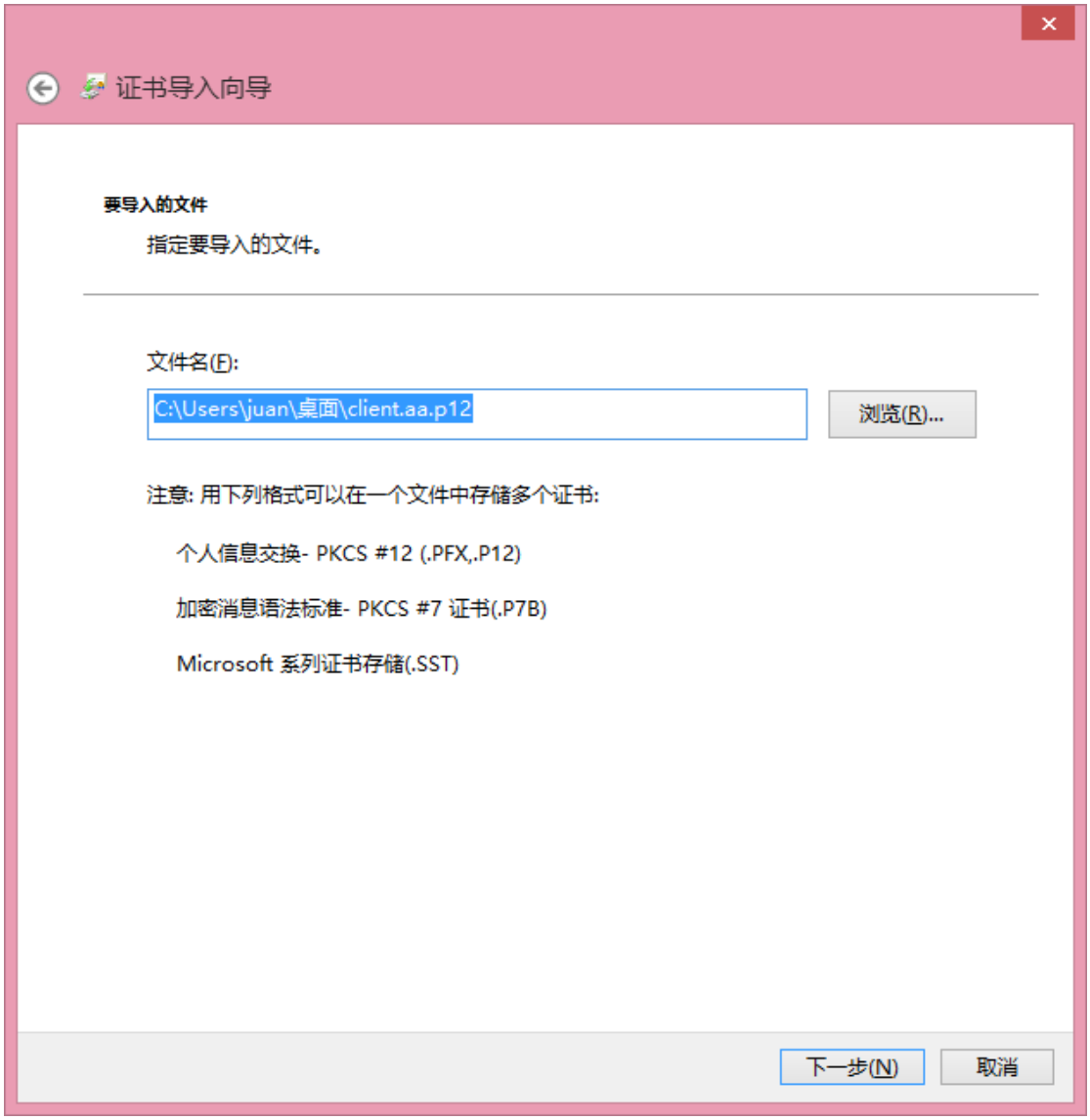
3.安装证书

谷歌浏览器直接安装证书即可，火狐浏览器需要导入。

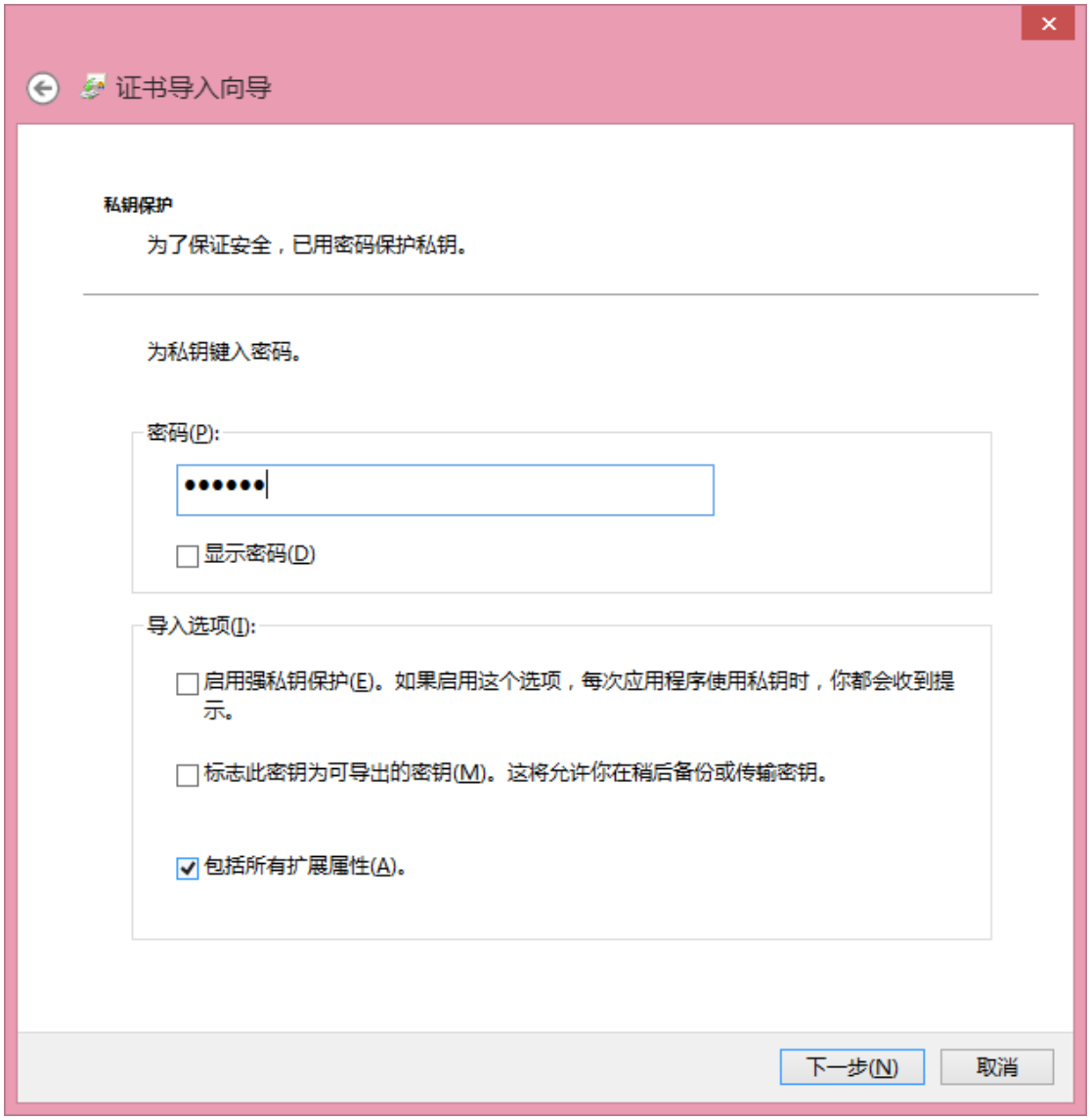
- 谷歌浏览器安装证书：

双击证书 client.aa.p12 ，弹出证书导入向导。

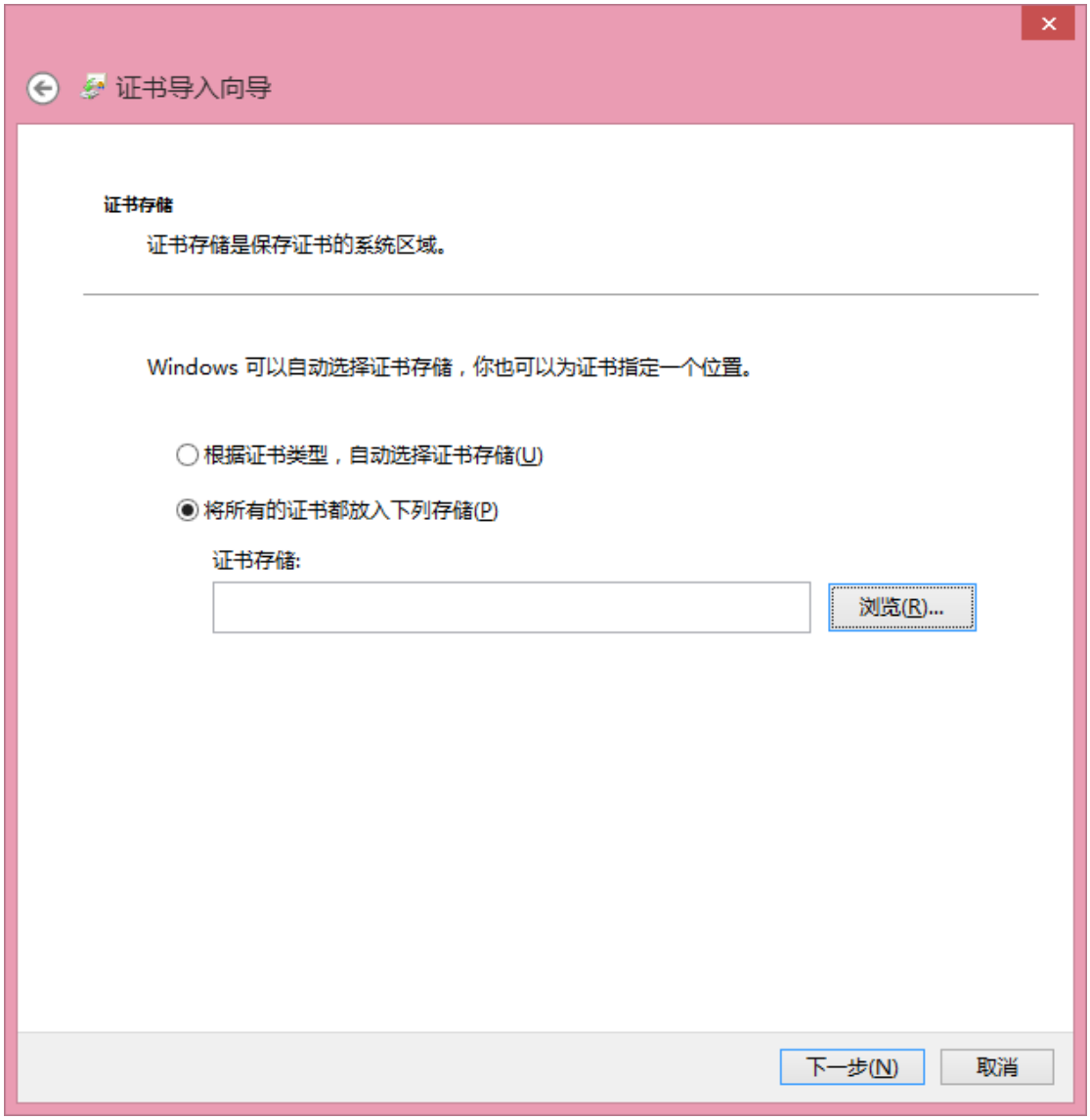
自动显示文件路径，点击下一步。



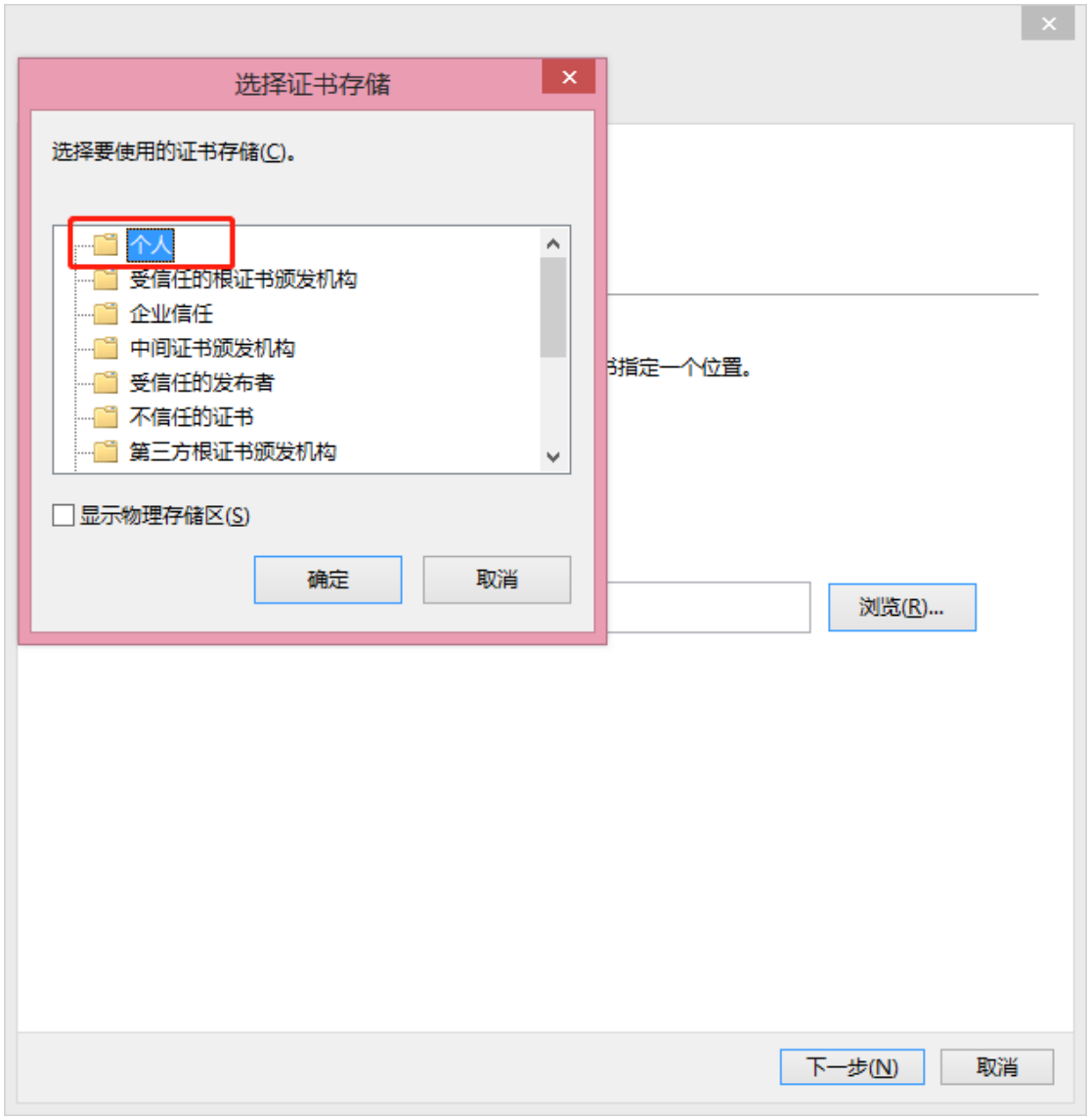
输入密码 **123456**，点击下一步。



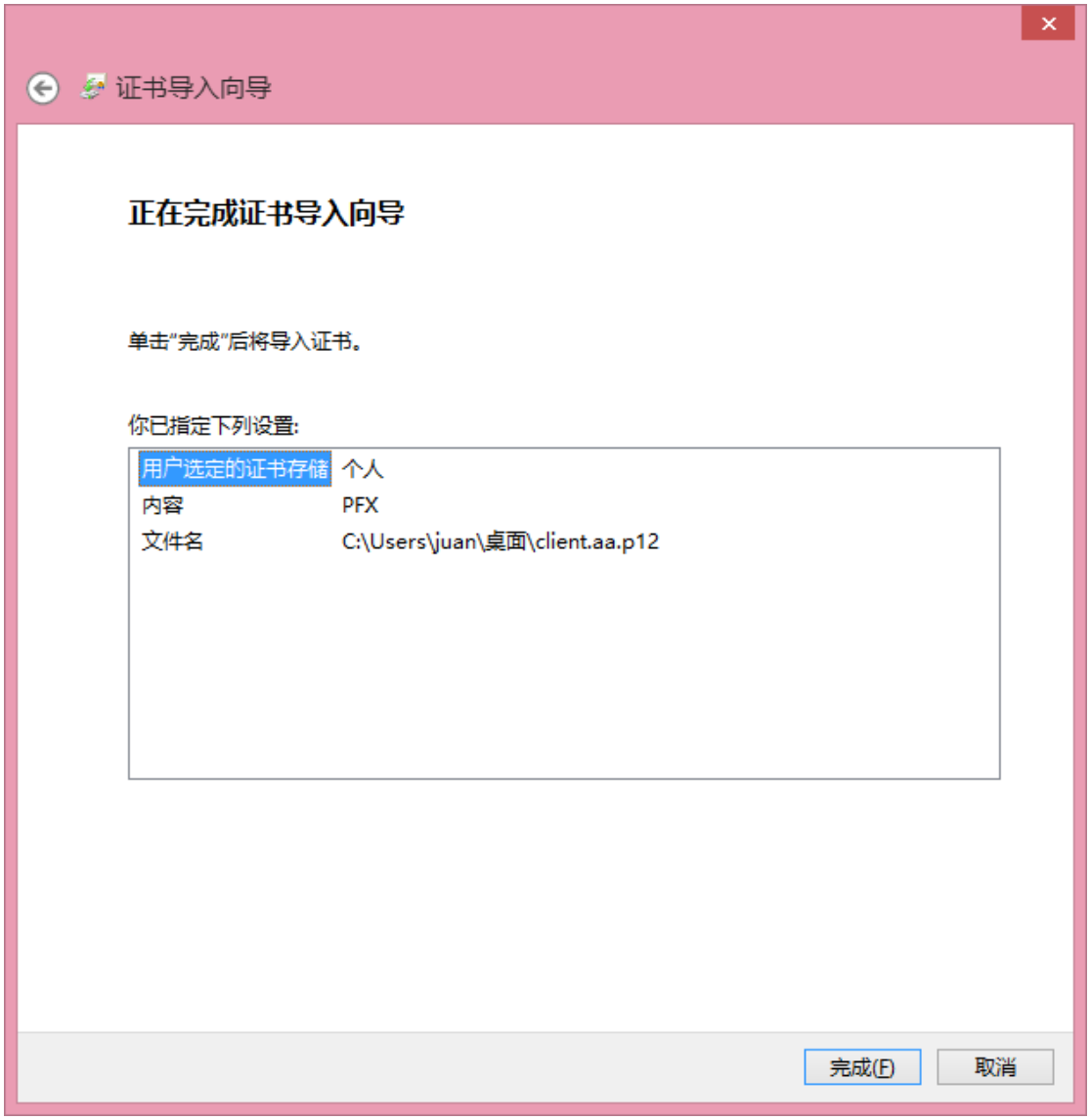
选择将所有的证书放入下列存储（P）。



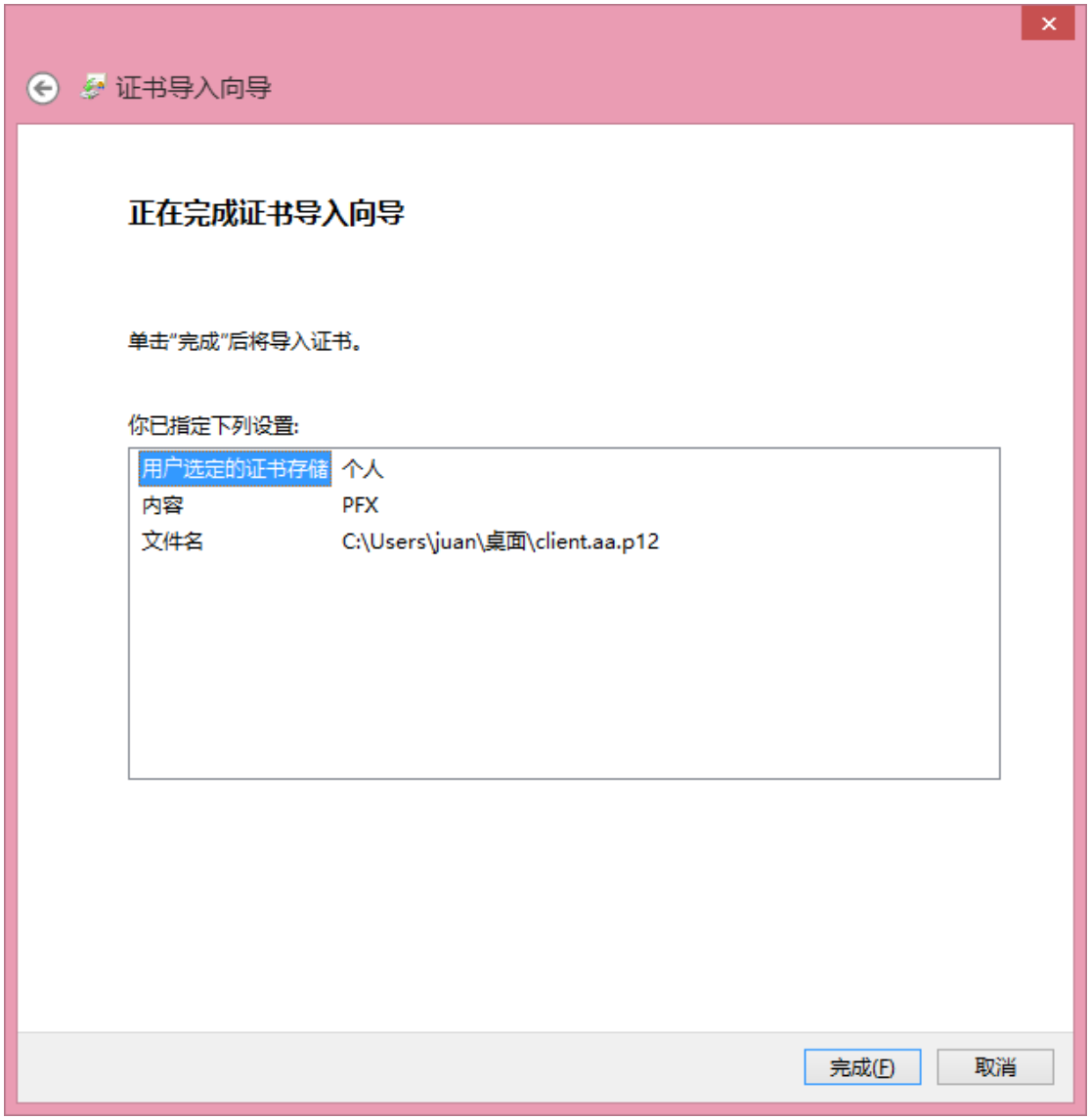
点击浏览，弹出选择证书存储框，选择个人，点击确定按钮。


选择证书存储
选择要使用的证书存储(C)。
个人
受信任的根证书颁发机构
企业信任
中间证书颁发机构
受信任的发布者
不信任的证书
第三方根证书颁发机构
显示物理存储区(S)
确定
取消
指定一个位置。
浏览(R)...
下一步(N)
取消

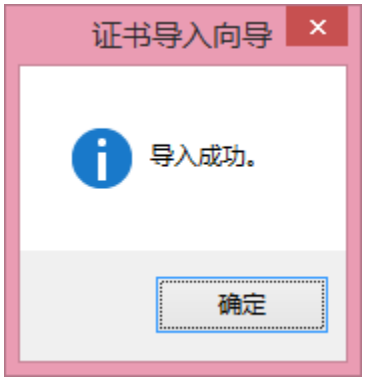
点击下一步。



点击完成，完成证书导入向导。



弹出提示信息导入成功。



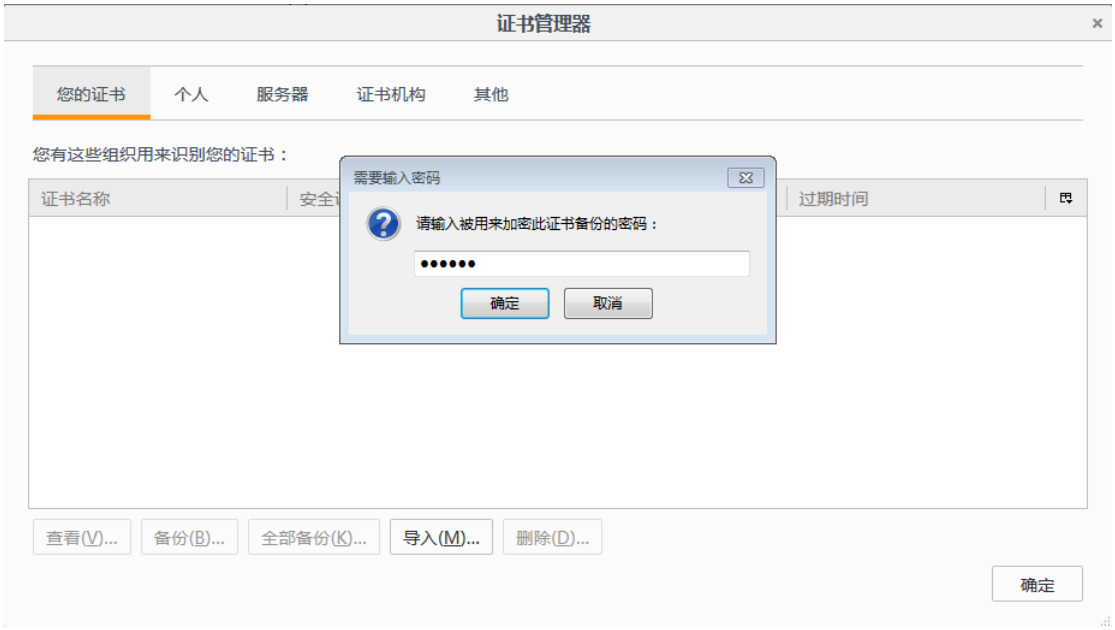
至此用户 aa 证书导入完成。

- 火狐浏览器导入证书

火狐浏览器点击选项->隐私与安全->查看证书。

在弹出的证书管理器窗口**您的证书**，点击**导入**，选择证书存储路径。

输入密码 **123456**，点击**确定**。



证书管理器列表中出现用户 aa 的证书。

至此用户 aa 证书导入完成。

4.数字证书登录

安全管理员 secAdmin 登录系统，切换至安全管理员角色，在用户列表页面点击编辑，将 aa 用户登陆方式改为数字证书。

登录界面，选择数字证书登录方式，弹出确认证书列表，选择证书 aa，点击确定。

2

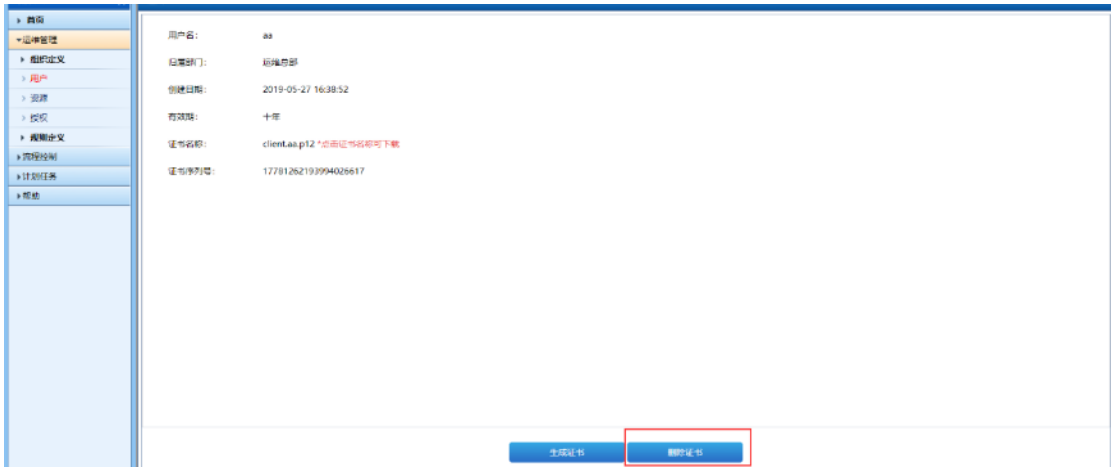
页面跳转到 444 端口，点击高级->继续前往。

跳转到用户数字证书登录界面，输入用户口令。

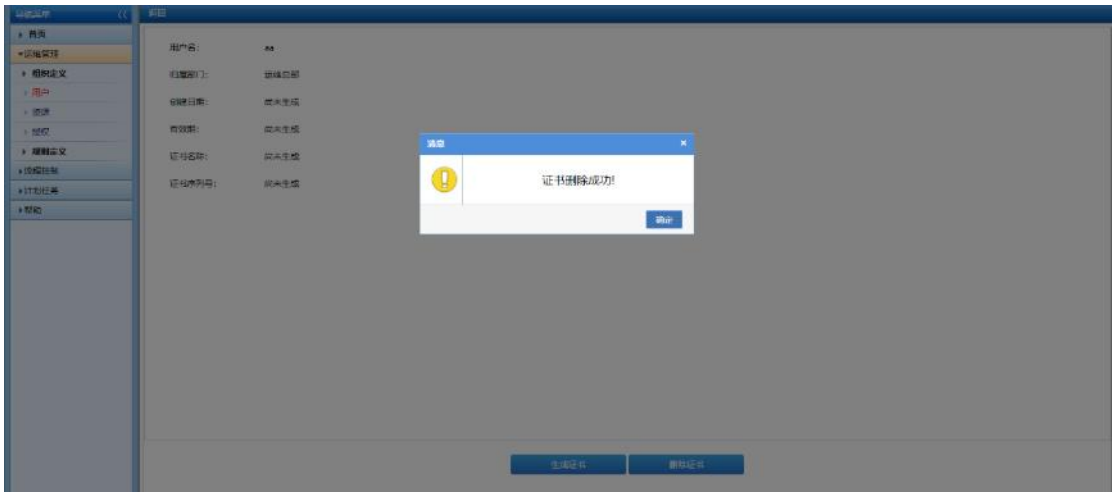
点击登录按钮，即可登录系统。

5.删除证书

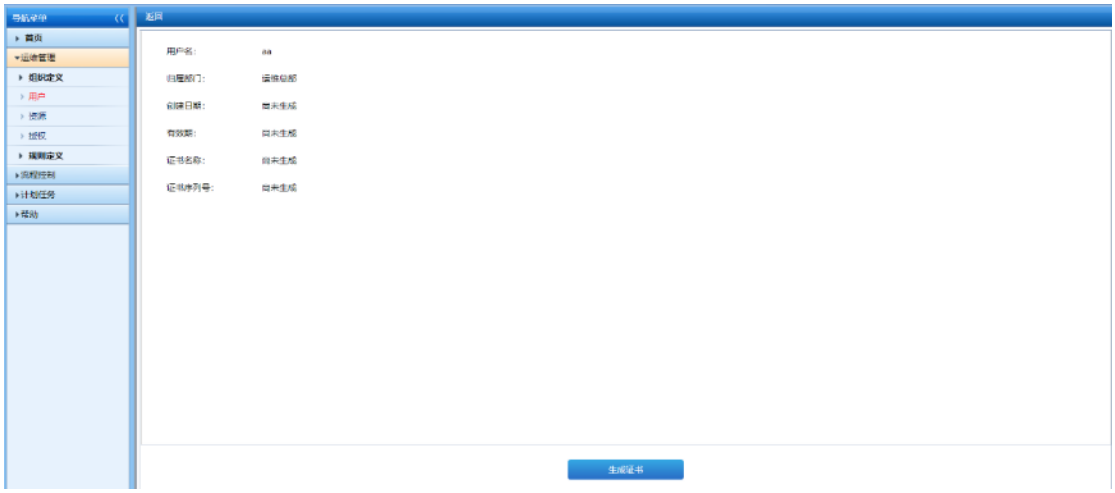
在用户 aa 证书管理页面，点击删除证书按钮。



弹出提示信息证书删除成功！



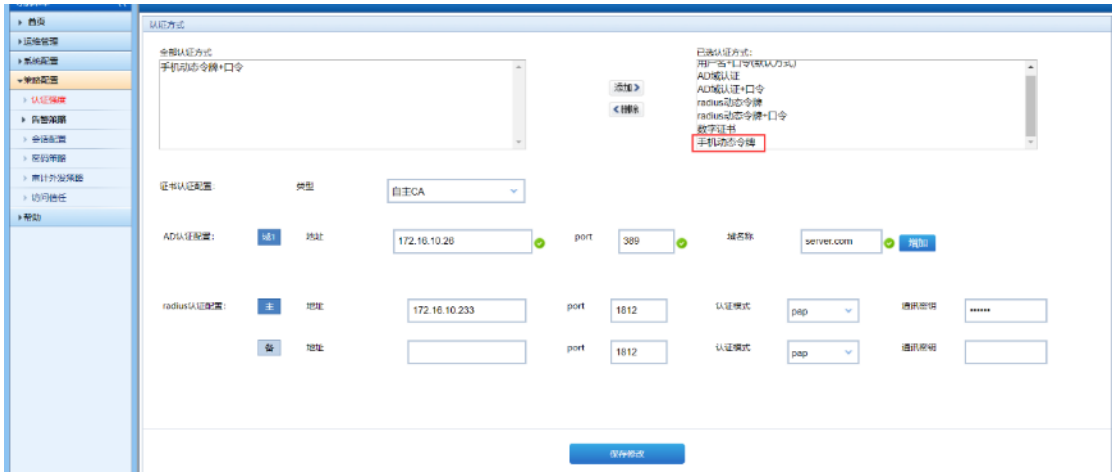
点击弹出框上的确定按钮，返回到证书管理页面，不显示用户证书信息。



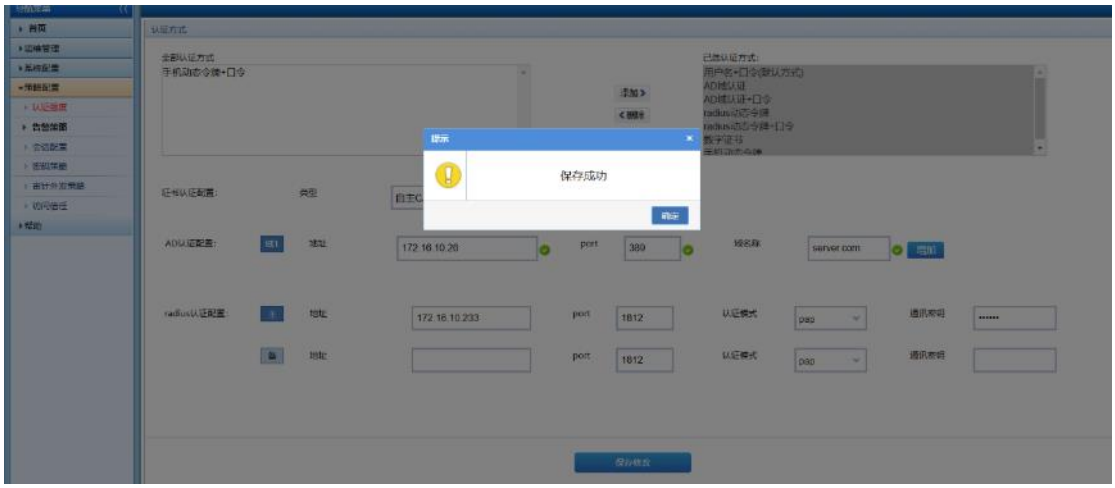
至此删除数字证书完成。

11.1.7. 手机动态令牌

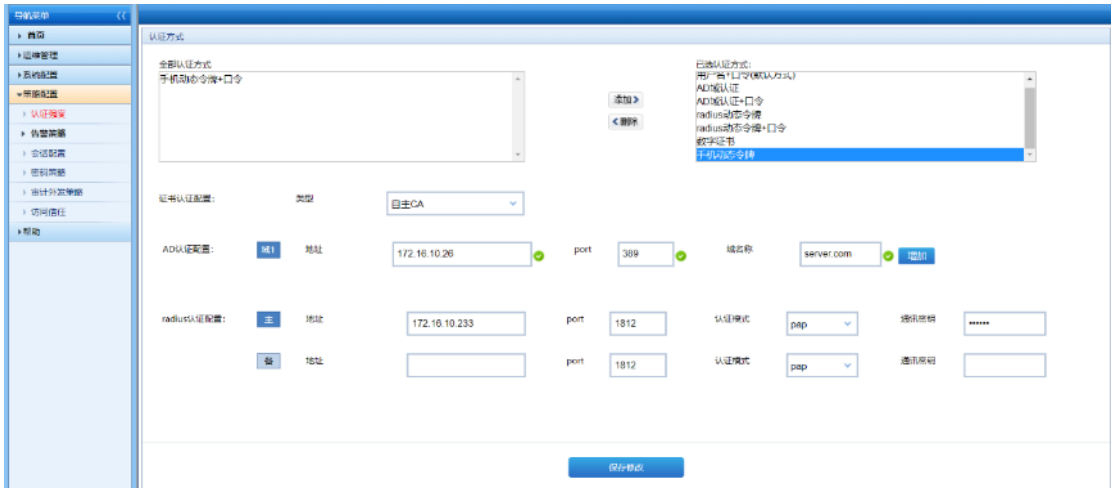
在认证强度页面，选择手机动态令牌，点击添加按钮，将手机动态令牌添加到已选认证方式列表。



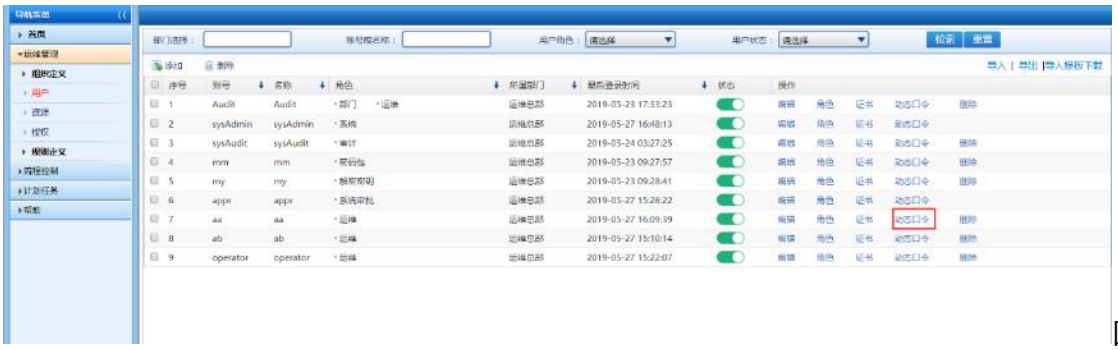
点击保存，提示保存成功！



点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示手机动态令牌。



安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的动态口令按钮。

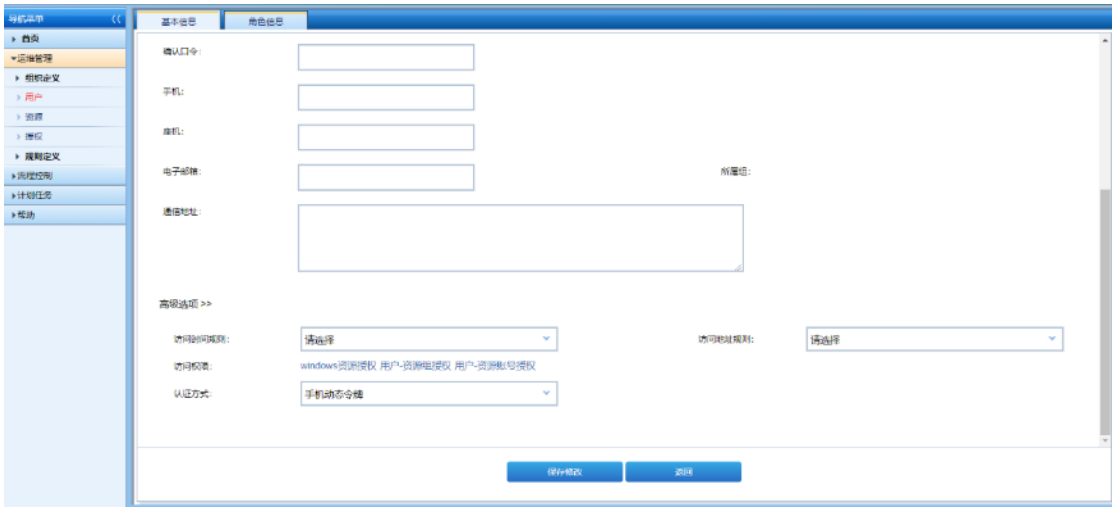


图

弹出生成动态口令框。

点击立即生成，生成动态口令码，将动态口令码输入谷歌身份验证器上，获取动态码。

在用户列表页面点击编辑，将 aa 用户登陆方式改为手机动态令牌。

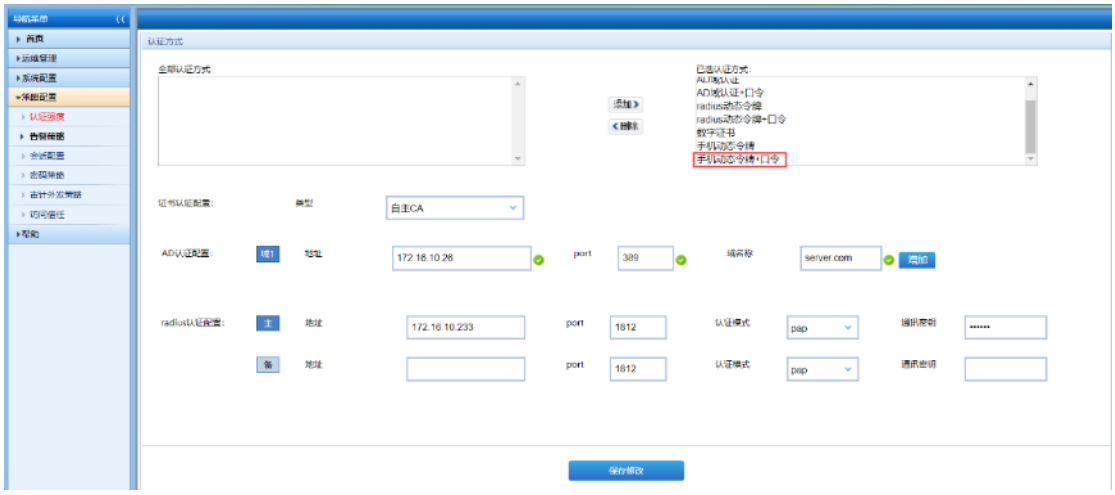


在用户登录界面，选择手机动态令牌登录方式，输入正确的账号和手机 APP 动态口令。

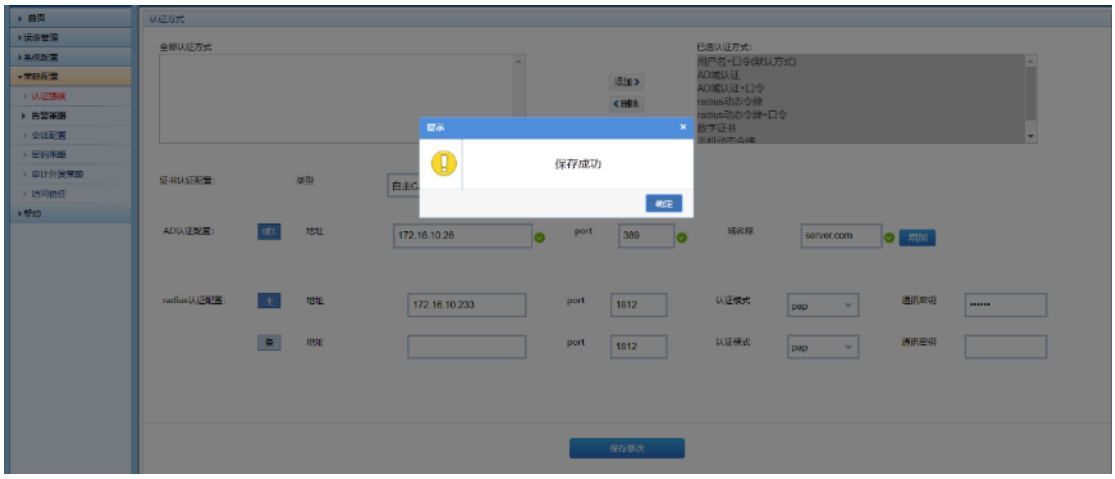
点击登录按钮，即可登录系统。

11.1.8. 手机动态令牌+口令

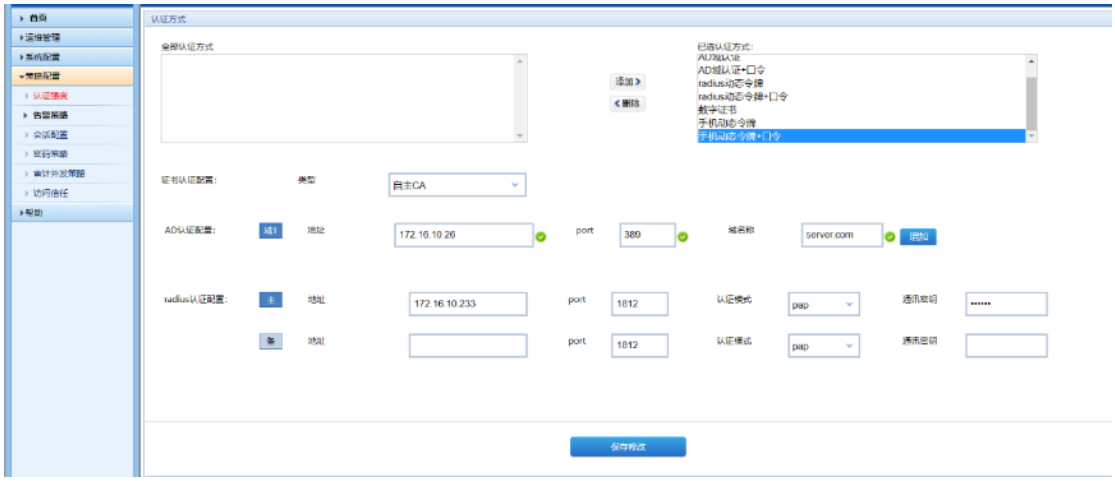
在认证强度页面，选择手机动态令牌+口令，点击添加按钮，将手机动态令牌+口令添加到已选认证方式列表。



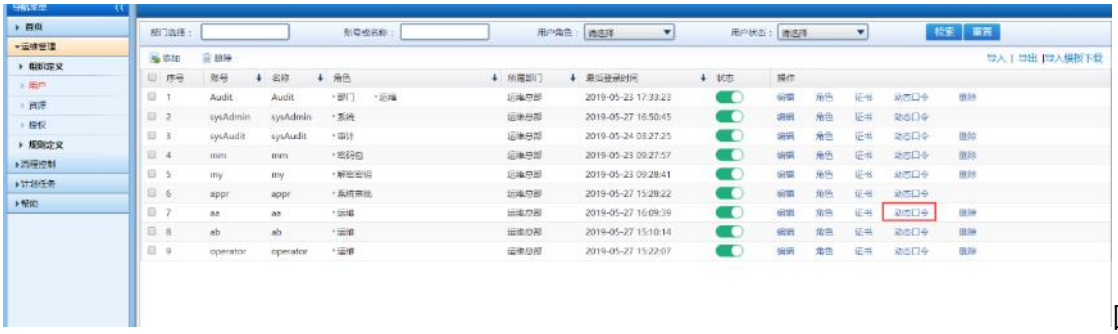
点击保存，提示保存成功！



点击弹出框上的确定按钮，返回到认证强度页面，已选认证方式列表显示手机动态令牌+口令。



安全管理员 secAdmin 登录系统，切换至安全管理员角色，点击运维管理->用户链接选择进入用户界面，点击 aa 用户的动态口令按钮。

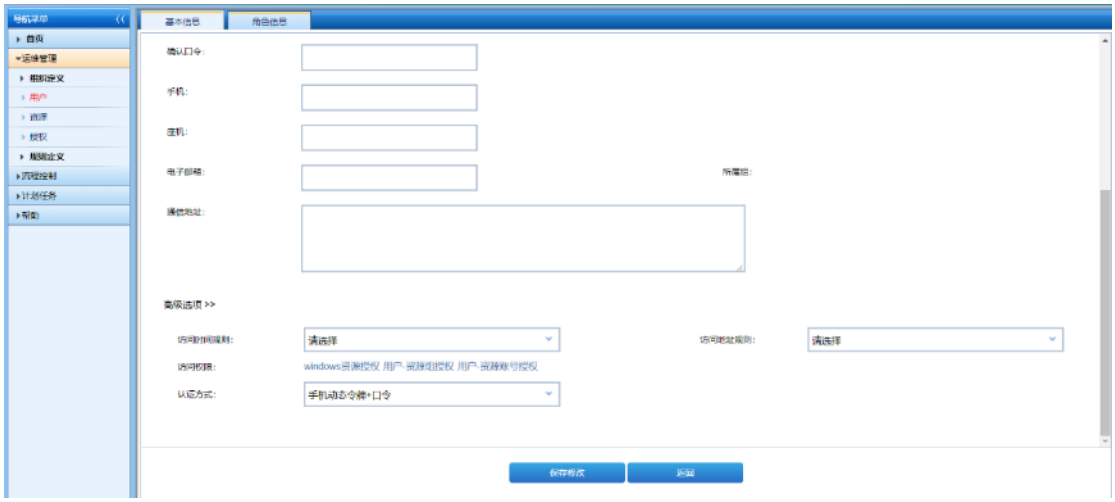


图

弹出生成动态口令框。

点击立即生成，生成动态口令码，将动态口令码输入谷歌身份验证器上，获取动态码。

在用户列表页面点击编辑，将 aa 用户登陆方式改为手机动态令牌+口令。



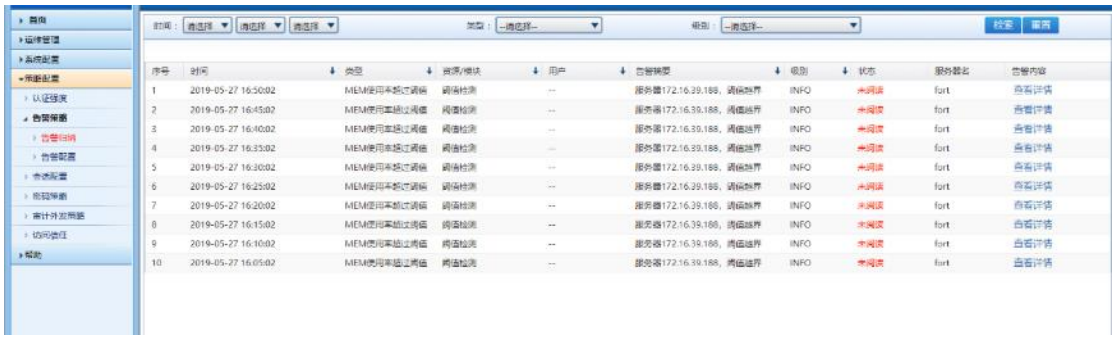
在用户登录界面，选择手机动态令牌登录方式，输入正确的账号、口令和手机 APP 动态口令。

点击登录按钮，即可登录系统。

11.2. 告警策略

告警策略包含高危运维、运行状态告警、认证异常三种类别，当用户触发某一种拟定的策略时产生告警。同时在告警归纳页面产生告警条目，告警发送方式支持 syslog 和邮件发送方式。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->告警策略进入到告警策略界面。

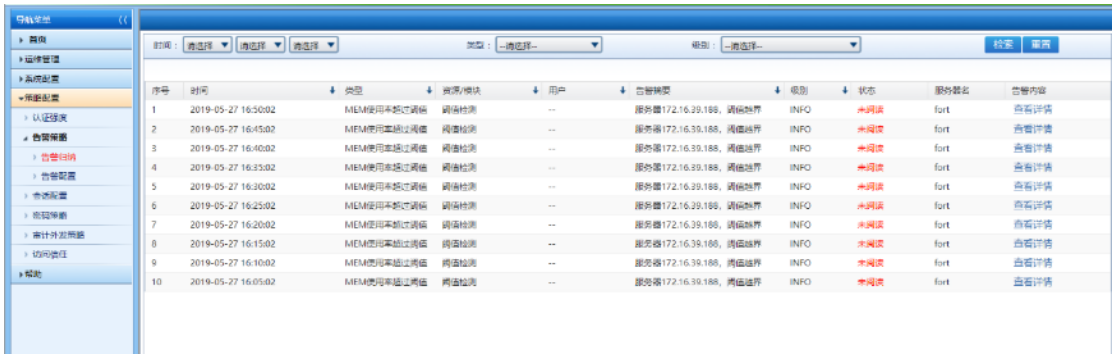


11.2.1. 告警归纳

告警归纳总结了用户触发告警时产生的条目，形成的列表包含：序号、时间、类型、资源/模块、用户、告警摘要、级别、状态、服务器名、告警内容等信息。

1.告警归纳时间检索

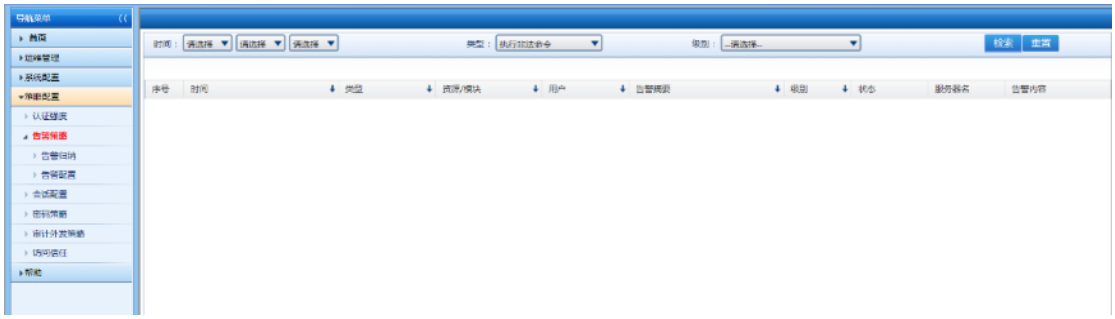
在告警归纳页面在时间下拉框选择时间：2019-05-24，点击检索。



页面检索出所有时间为 2019-05-24 日的条目。

2.告警归纳类型检索

选择类型：执行非法命令，点击检索。



页面检索出所有告警条目类型为执行非法命令的条目。

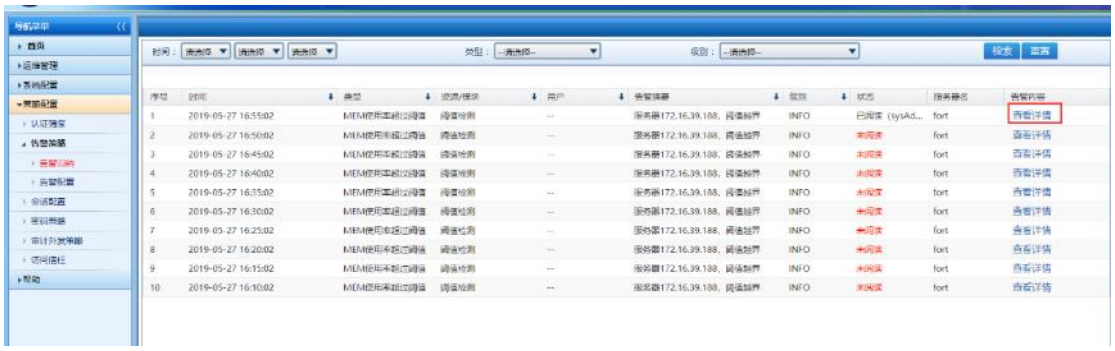
3.告警归纳级别检索

选择告警级别：0 调试信息，点击检索。

页面检索出所有告警级别为 0 级的条目。

4.告警归纳查看详情

在告警归纳页面，点击类型为执行非法命令，告警内容列的查看详情。



页面跳转到类型为执行非法命令的详细信息页面。页面显示告警类型、事件发生时间、事件严重级别、事件严重级别、操作人员 ID、事件模块/IP 等信息。

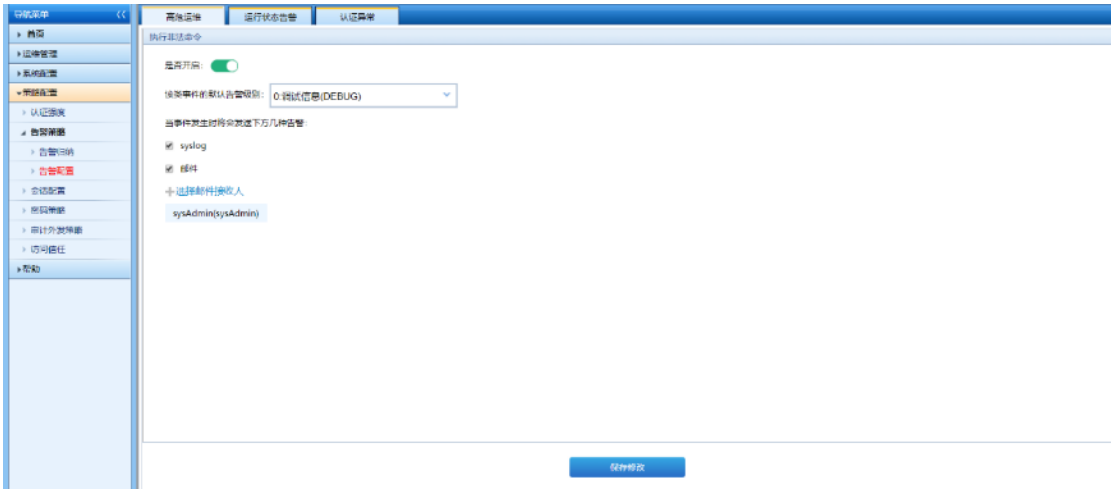
11.2.2. 告警配置

告警配置分为：高危运维、运行状态告警、认证异常三种告警类别，用户可设定告警条件，触发告警。

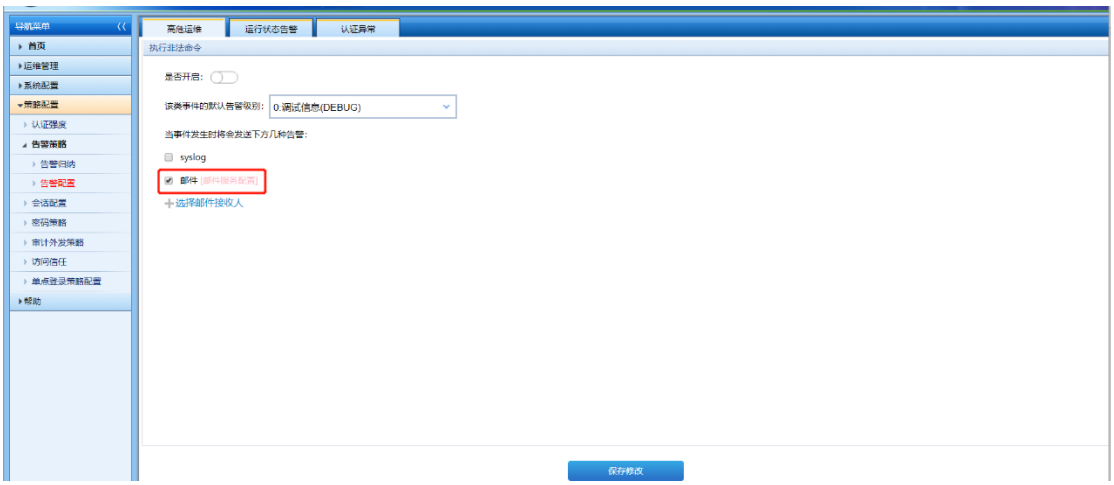
1.高危运维

高危运维指在运维操作中输入非法命令触发的告警。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->告警策略->告警配置进入到告警配置界面，在高危运维页面，勾选 syslog（需配置 syslog 日志服务器），勾选邮件，选择邮件接收人，点击保存。

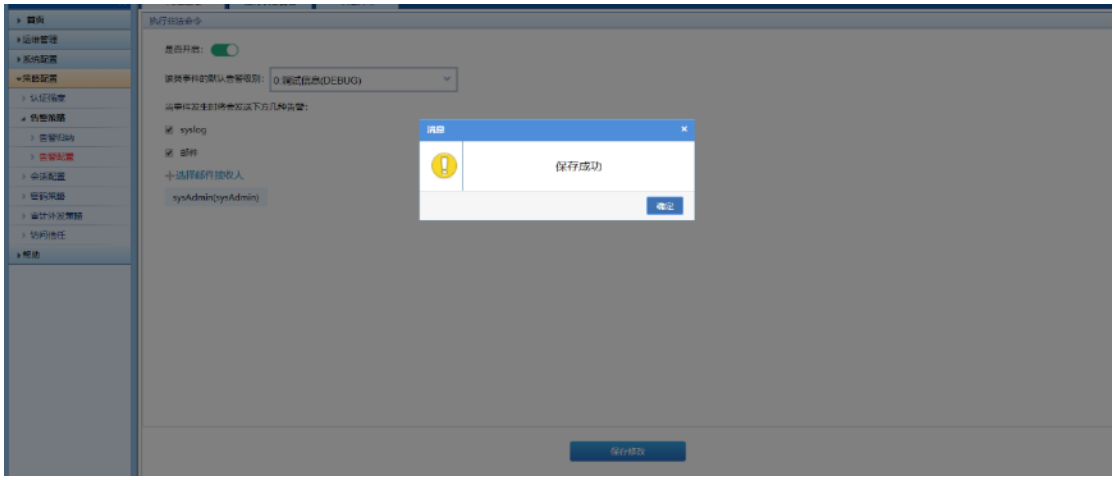


勾选邮件，显示邮件服务配置红色字样，点击邮件服务配置，跳转到邮件服务配置页面



配置邮件服务后，点击返回，跳转到高位运维页面

页面弹出提示框：保存成功。

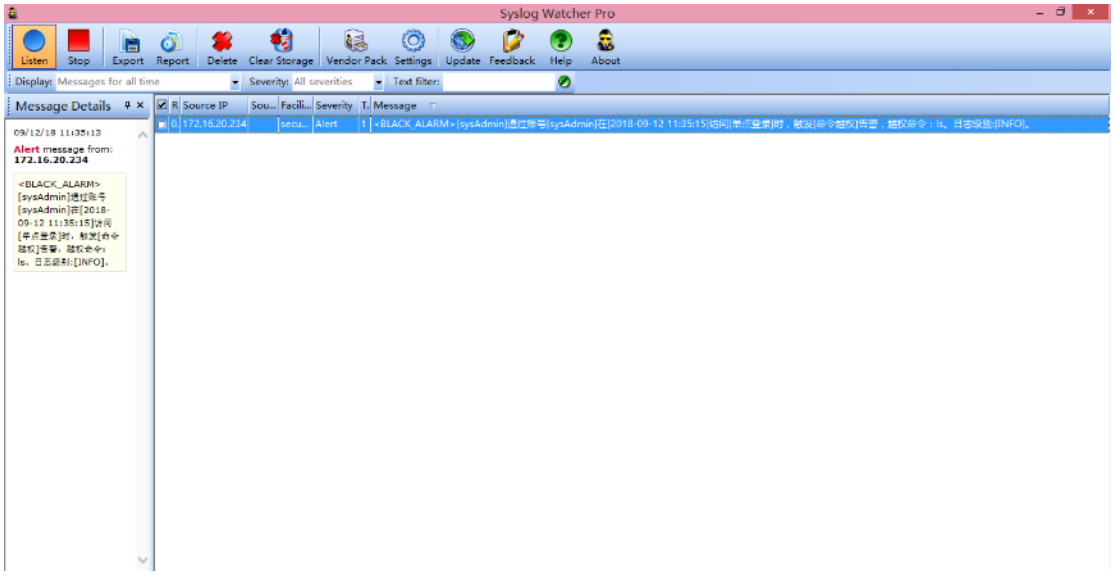


安全管理员 secAdmin 登录系统，切换至安全管理员角色，添加 linux 资源 IP172.16.20.211 并绑定授权，授权名称 linux。

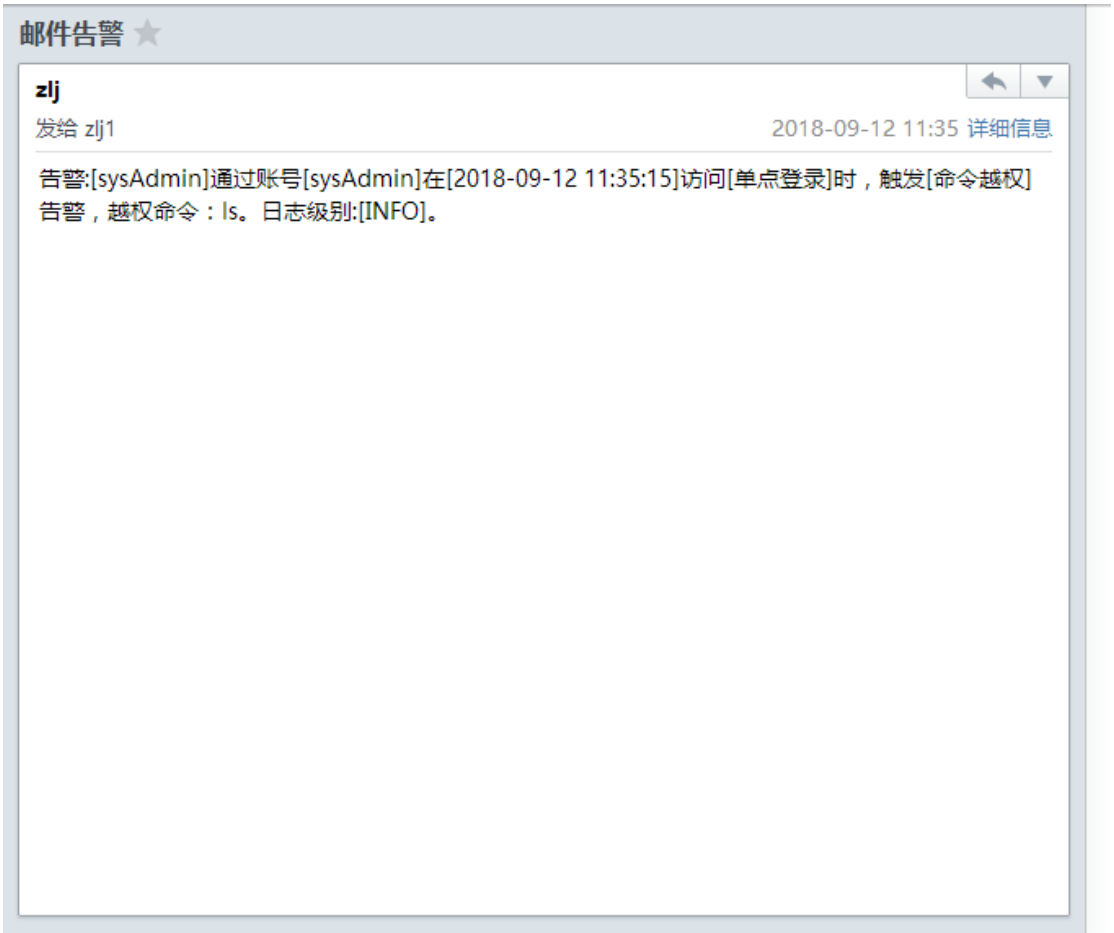
在运维管理->规则定义->命令规则为资源 ip172.16.20.211 添加黑名单。

用户 sysAdmin 切换至运维操作员角色，对 linux 资源 IP172.16.20.211 进行单点登录输入越权命令 ls。

syslog 日志服务器收到告警信息格式： <BLACK_ALARM>[sysAdmin]通过账号[sysAdmin]在[2018-09-12 11:35:15]访问[单点登录]时，触发[命令越权]告警，越权命令：ls。日志级别:[INFO]。



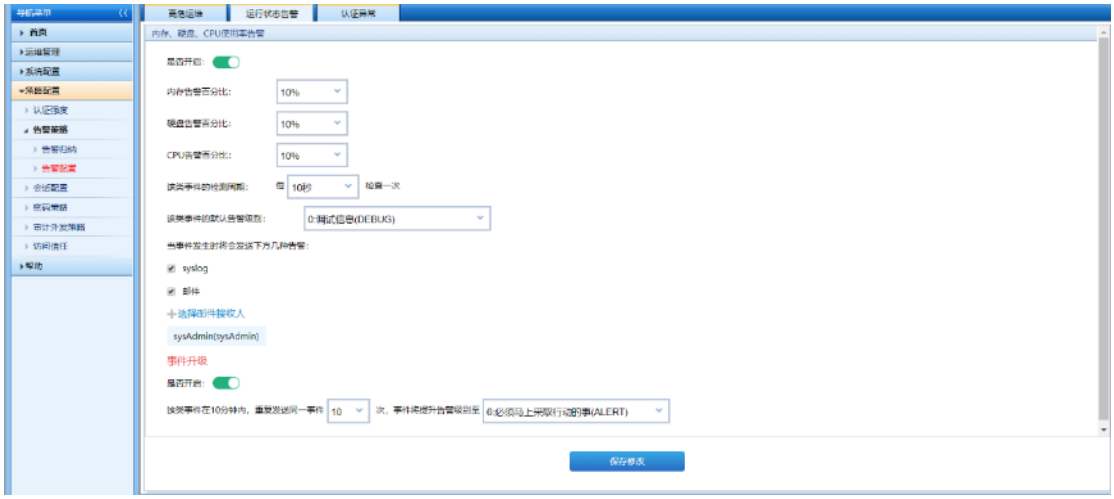
邮件收到告警信息格式：告警:[sysAdmin]通过账号[sysAdmin]在[2018-09-12 11:35:15]访问[单点登录]时，触发[命令越权]告警，越权命令：ls。日志级别:[INFO]。



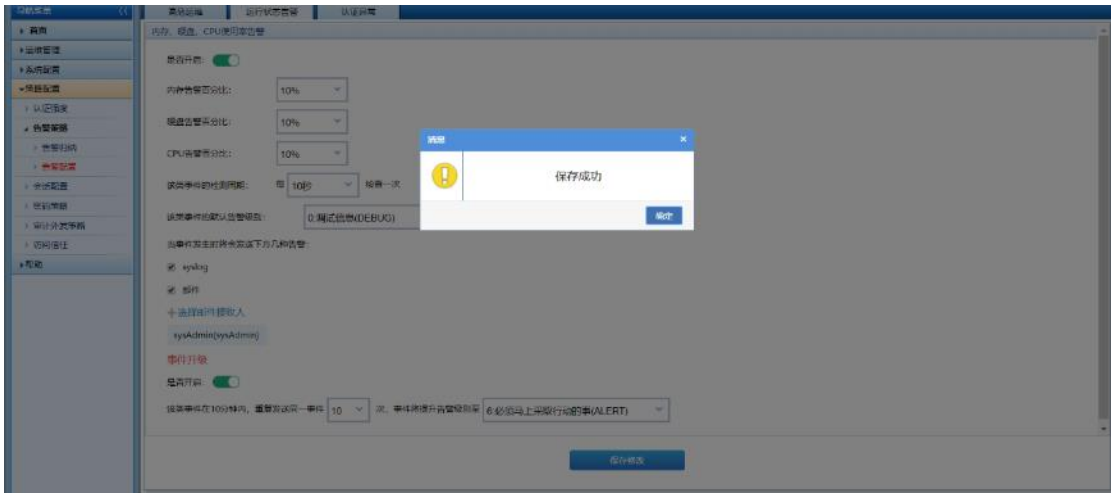
2.运行状态告警

运行状态告警是指设备达到内存、CPU、硬盘使用率阈值时，触发告警。

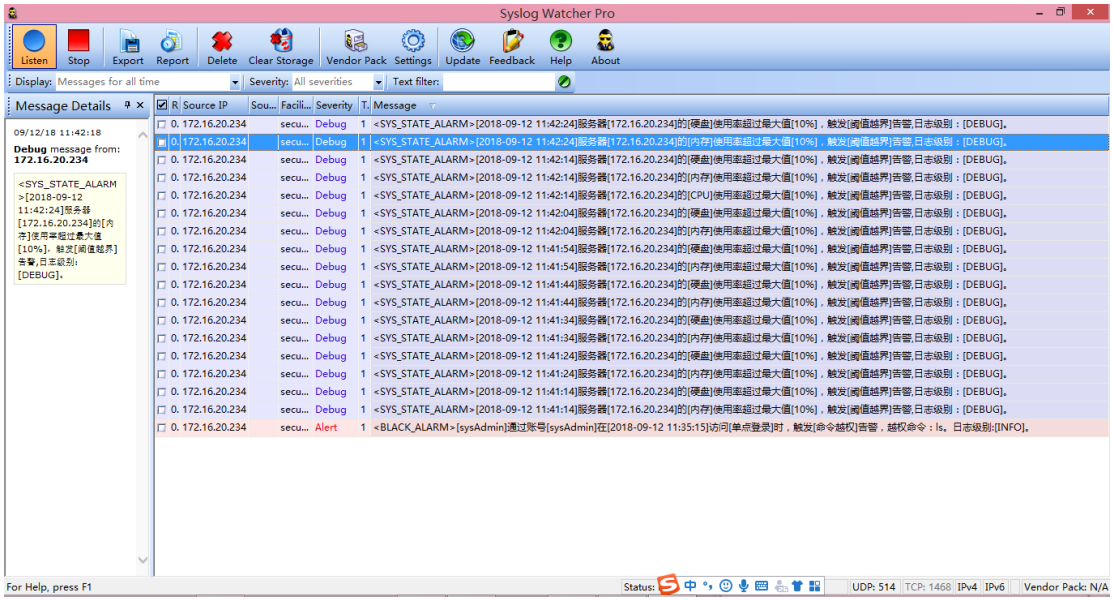
用系统管理员 sysAdmin 登录系统，切换至超级管理员角色，点击运行状态告警进入到运行状态告警界面。把内存、CPU、硬盘使用率分别设置为 10%，勾选 syslog（需配置 syslog 日志服务器），勾选邮件选择邮件接收人，点击保存。



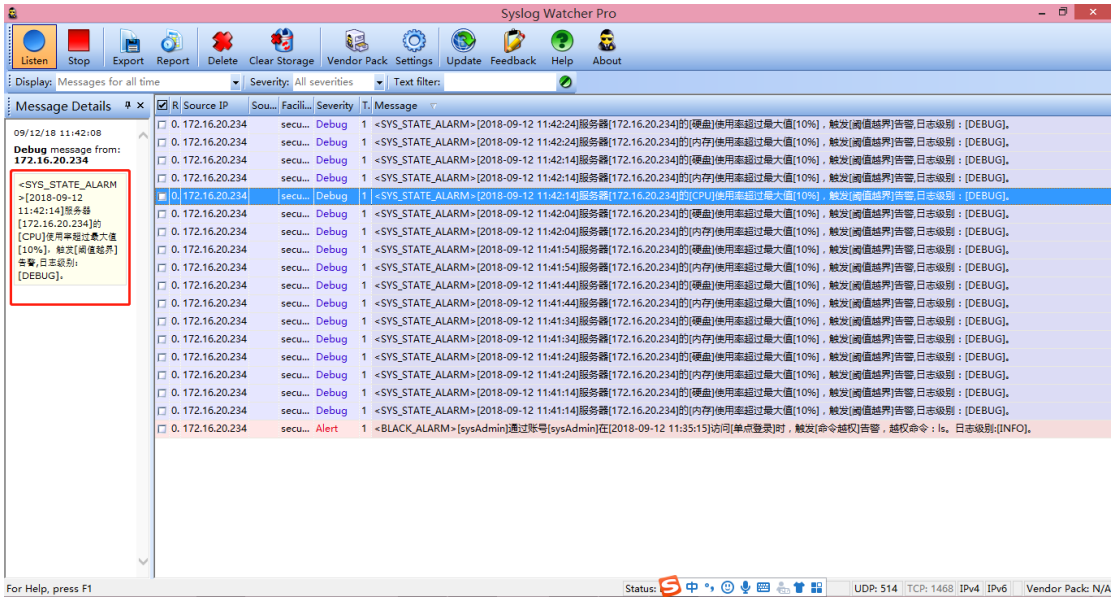
页面弹出提示框：保存成功。



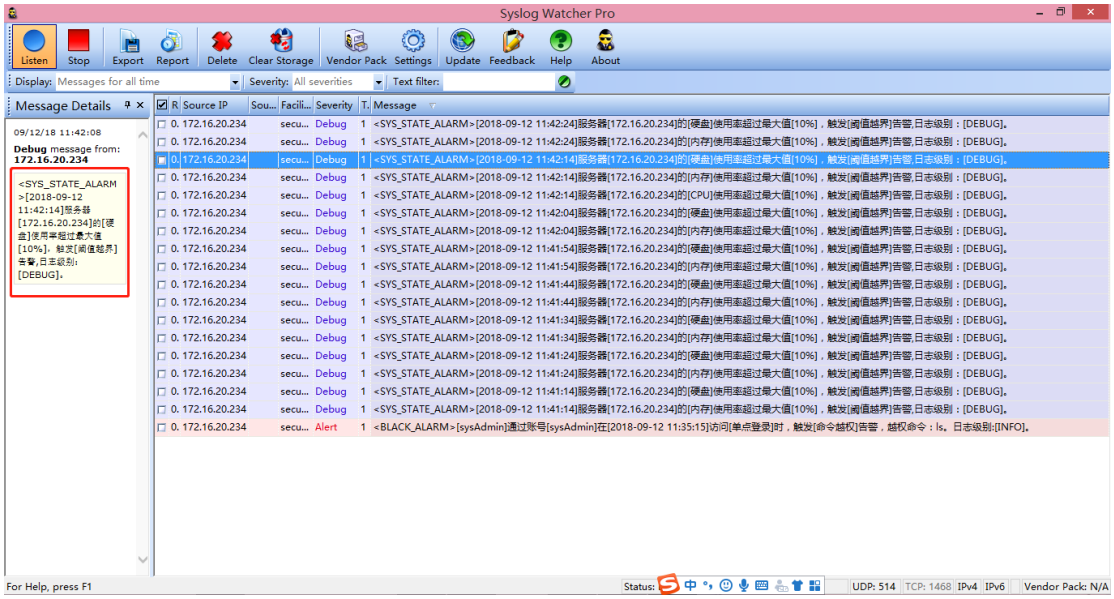
当内存使用率达到 10%时，触发告警，syslog 日志服务器收到告警条目格式：<SYS_STATE_ALARM>[2018-09-12 11:42:24]服务器[172.16.20.234]的[内存]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。



当 CPU 使用率达到 10%时，触发告警，syslog 日志服务器收到告警条目格式:SYS_STATE_ALARM>[2018-09-12 11:42:14]服务器[172.16.20.234]的[CPU]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。



当硬盘使用率达到 10%时，触发告警，syslog 日志服务器收到告警条目格式：<SYS_STATE_ALARM>[2018-09-12 11:42:14]服务器[172.16.20.234]的[硬盘]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。

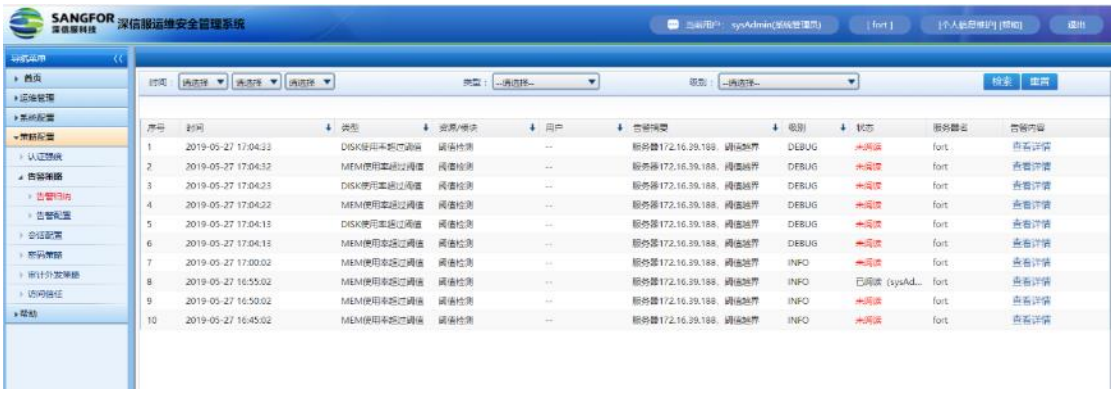


当内存使用率达到 10%时，触发告警，邮件服务器收到告警条目格式：告警:[2018-09-12 11:41:14]服务器[172.16.20.234]的[内存]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。

当 CPU 使用率达到 10%时，触发告警，邮件服务器收到告警条目格式：告警:[2018-09-12 11:42:14]服务器[172.16.20.234]的[CPU]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。

当硬盘使用率达到 10%时，触发告警，邮件服务器收到告警条目格式：告警:[2018-09-12 11:42:24]服务器[172.16.20.234]的[硬盘]使用率超过最大值[10%]，触发[阈值越界]告警,日志级别：[DEBUG]。

在告警归纳页面产生告警条目。

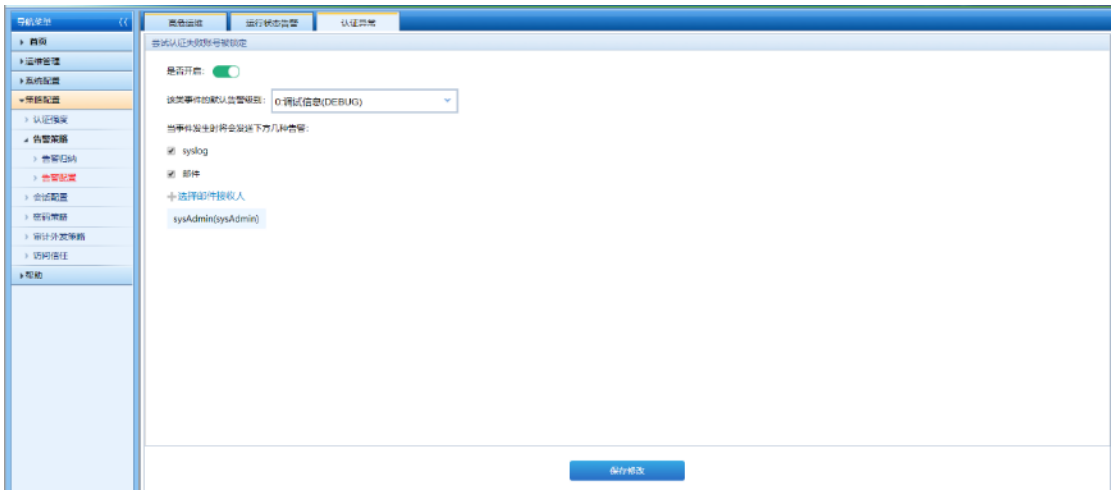


3.认证异常

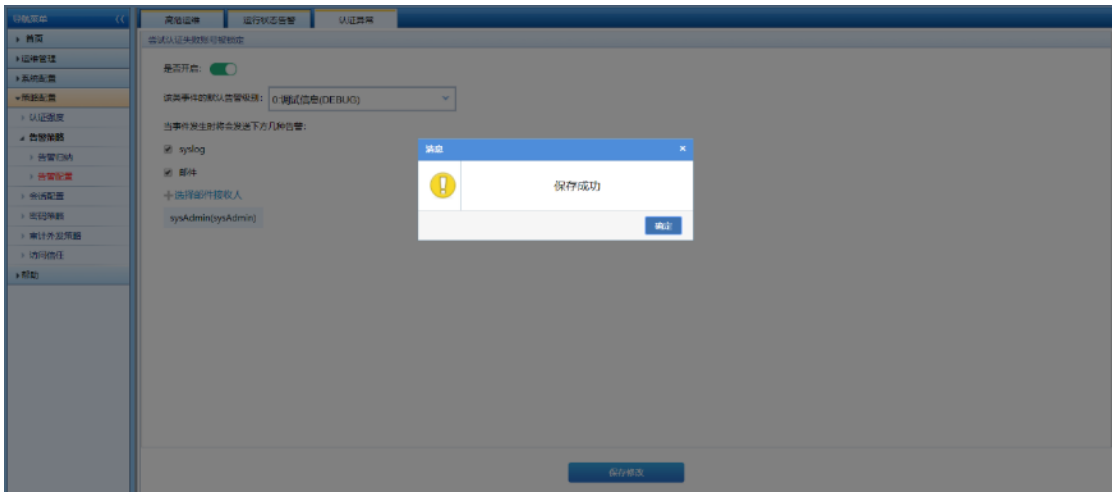
认证异常是指用户登录认证失败被锁定，触发告警。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击认证异常进入到认证异常界

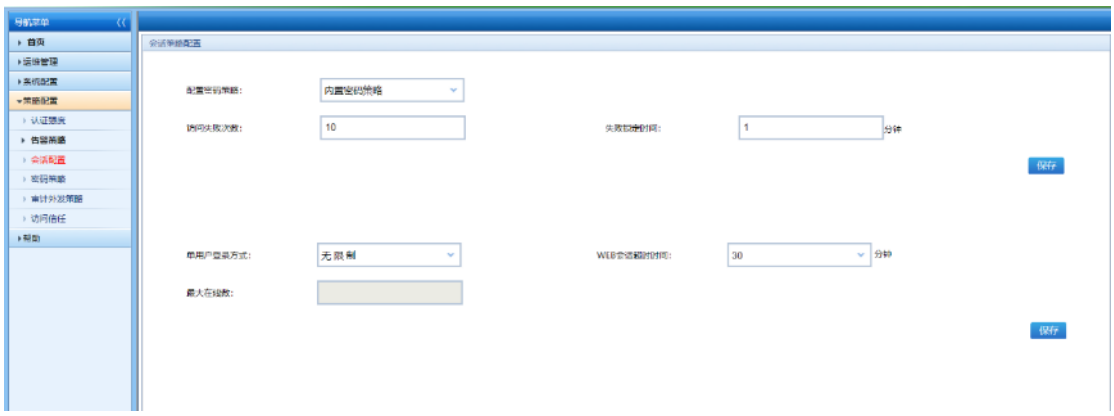
面。勾选 syslog（需配置 syslog 日志服务器），勾选邮件选择邮件接收人，点击保存。



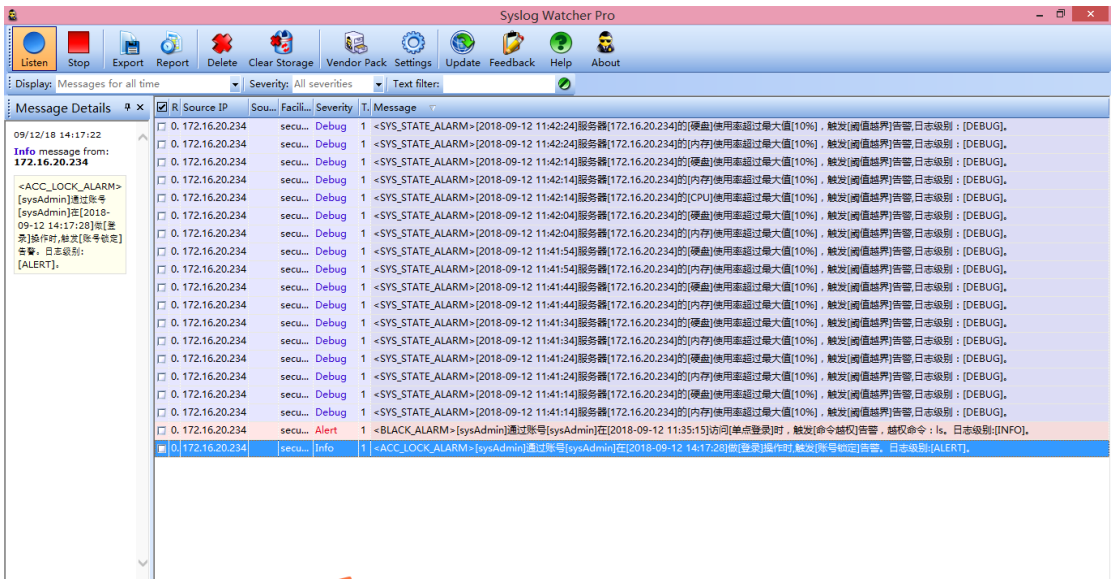
页面弹出提示框：保存成功。



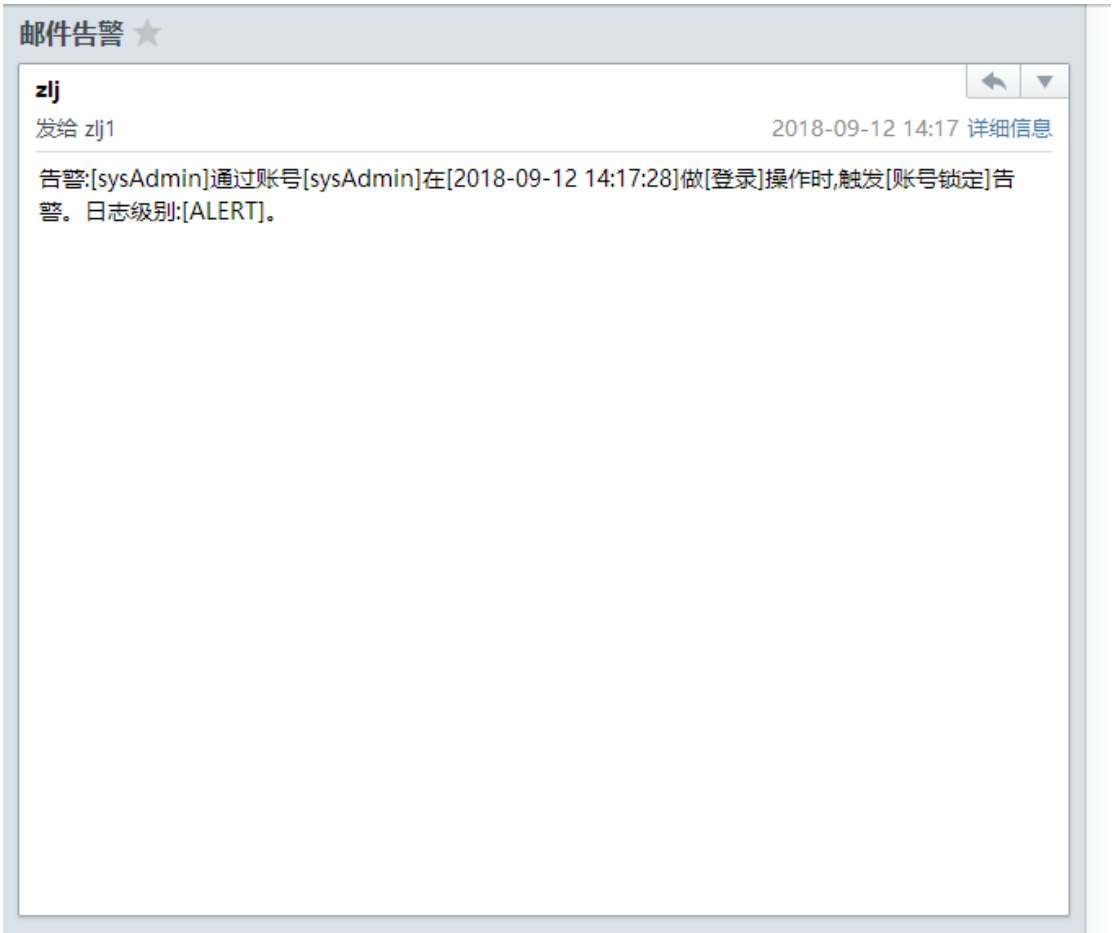
在策略配置->会话配置页面配置访问失败次数为 1，锁定时间为 1 分钟。



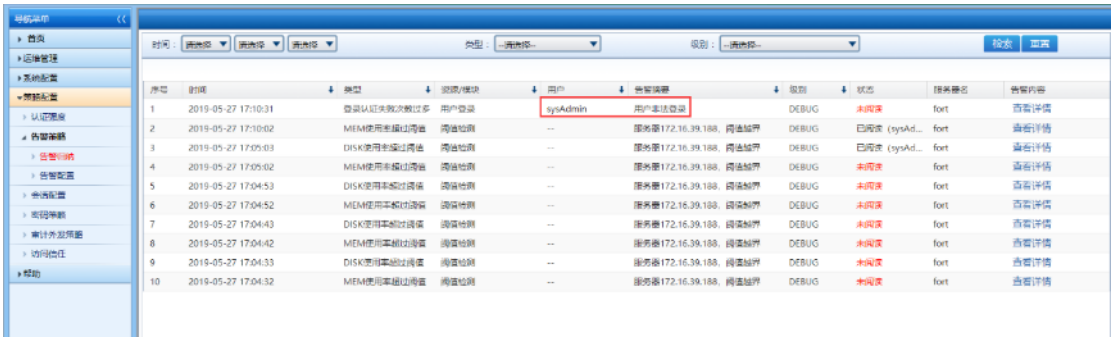
用户 sysAdmin 退出系统，页面跳转到登录界面，使用用户 sysAdmin，输入 1 次错误密码，点击用户登录触发账号锁定告警，syslog 日志服务器收到告警信息格式：<ACC_LOCK_ALARM>[sysAdmin]通过账号[sysAdmin]在[2018-09-12 14:17:28]做[登录]操作时,触发[账号锁定]告警。日志级别:[ALERT]。



邮件服务器收到告警信息格式：告警:[sysAdmin]通过账号[sysAdmin]在[2018-09-12 14:17:28]做[登录]操作时,触发[账号锁定]告警。日志级别:[ALERT]。



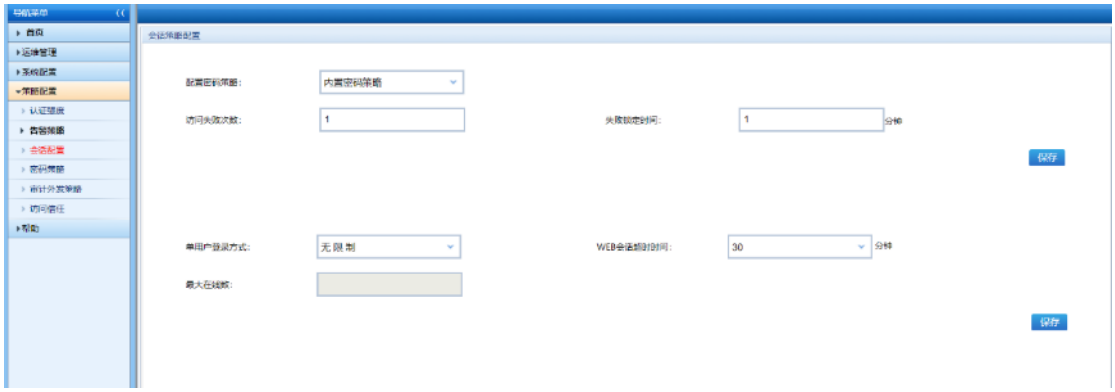
在告警归纳页面显示告警条目。



11.3. 会话配置

会话配置分为用户密码策略、用户锁定策略、单用户登录方式、WEB 会话超时四部分。

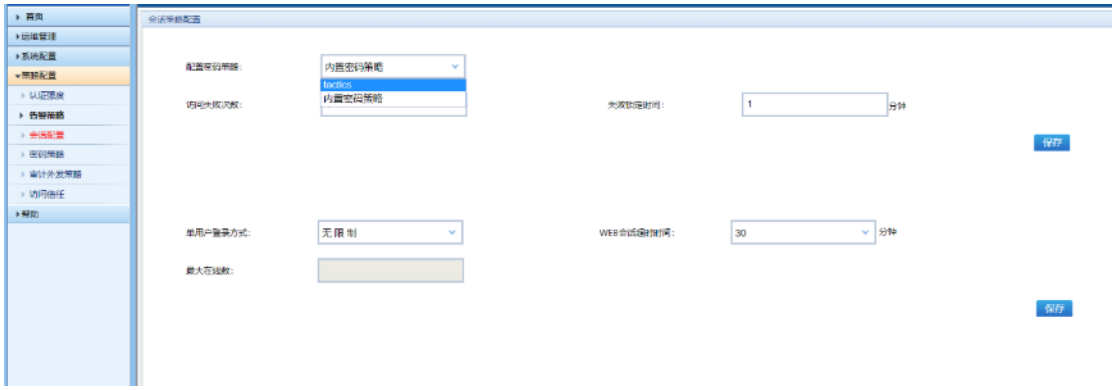
用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->会话配置进入到会话配置界面。



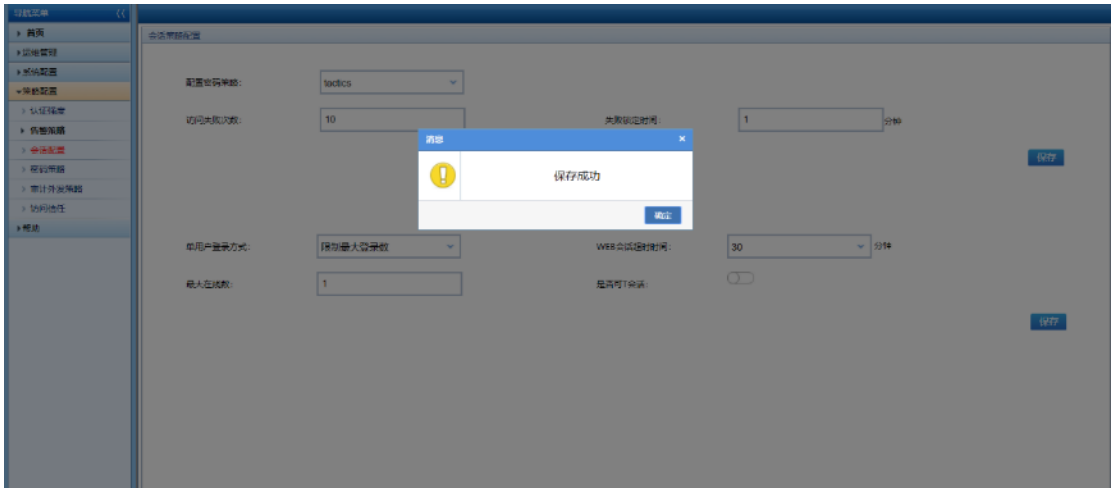
11.3.1. 用户密码策略

配置密码策略为系统全局用户设定的策略，用户修改口令要符合密码策略的范畴。

在配置密码策略下选择已添加成功的密码策略 tactics，点击保存。



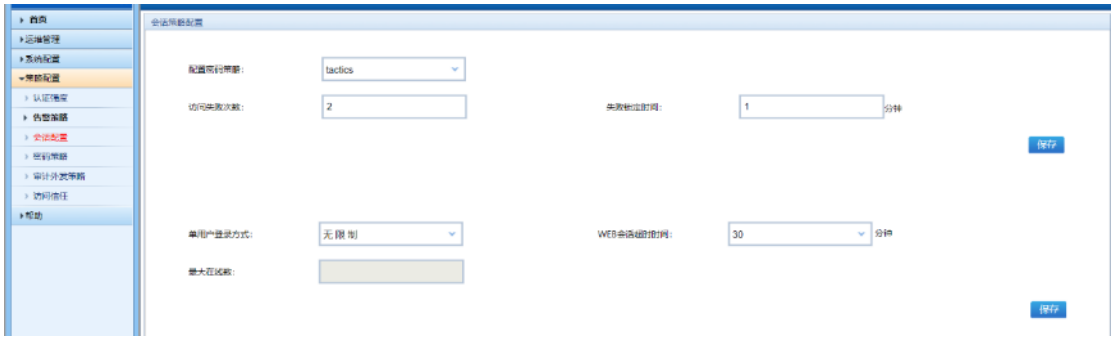
页面弹出提示弹框：保存成功。



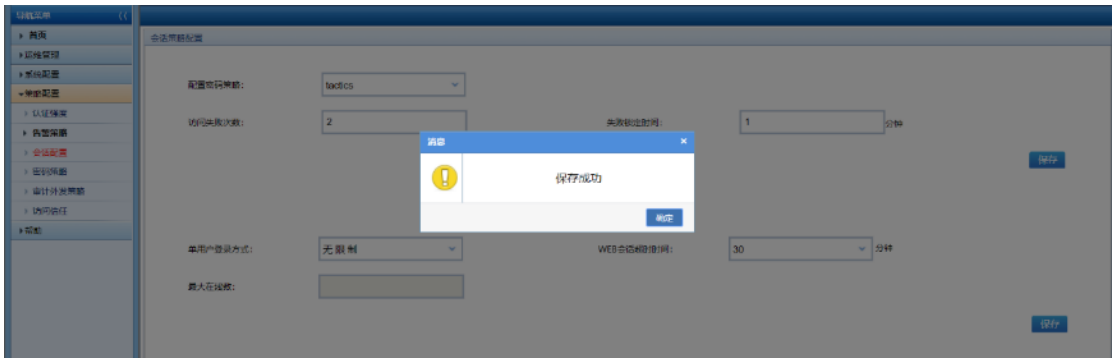
11.3.2. 用户锁定

用户锁定策略为用户登录系统过程中，超过设定访问失败次数时，用户自动锁定。

在会话配置页面，输入访问失败次数为：2，失败锁定时间为：1，点击确定。



页面弹出提示弹框：保存成功！



用户 sysAdmin 退出系统，页面跳转到系统登录界面，输入用户 aa，输入错误的口令，点击用户登录。

页面弹出提示框：账号或口令错误，您还有 1 次机会。

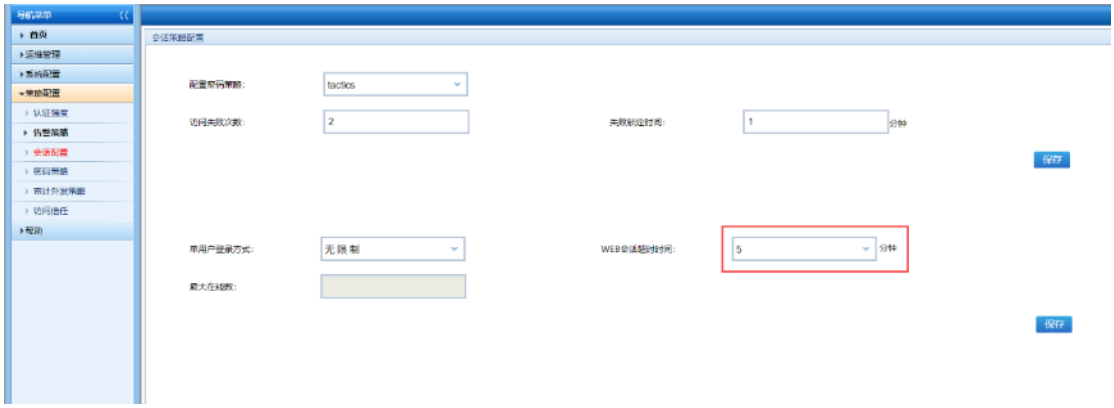
输入错误口令，再次点击用户登录。

页面弹出提示框：账号已被锁定，请 59 秒后重试。

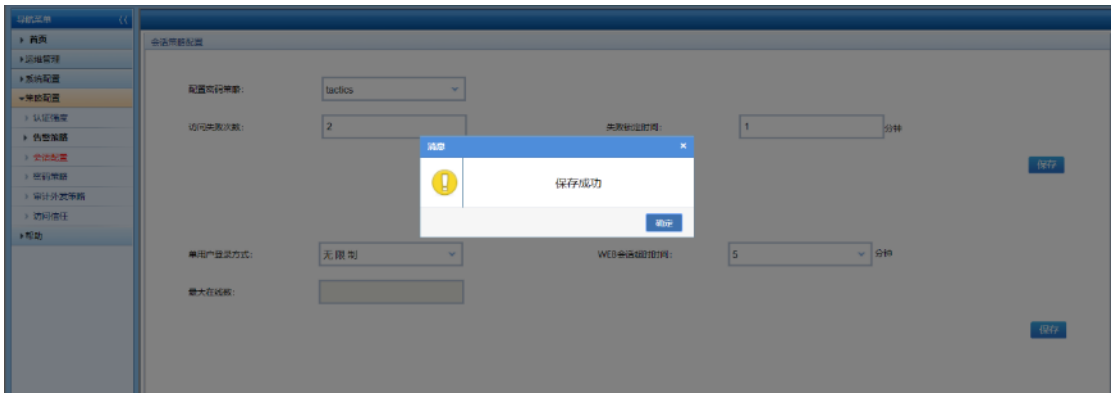
11.3.3. Web 会话超时

WEB 会话超时是指用户在设定时间内没有对系统做任何操作，刷新页面，用户已超过 web 超时时间，需重新登录系统。

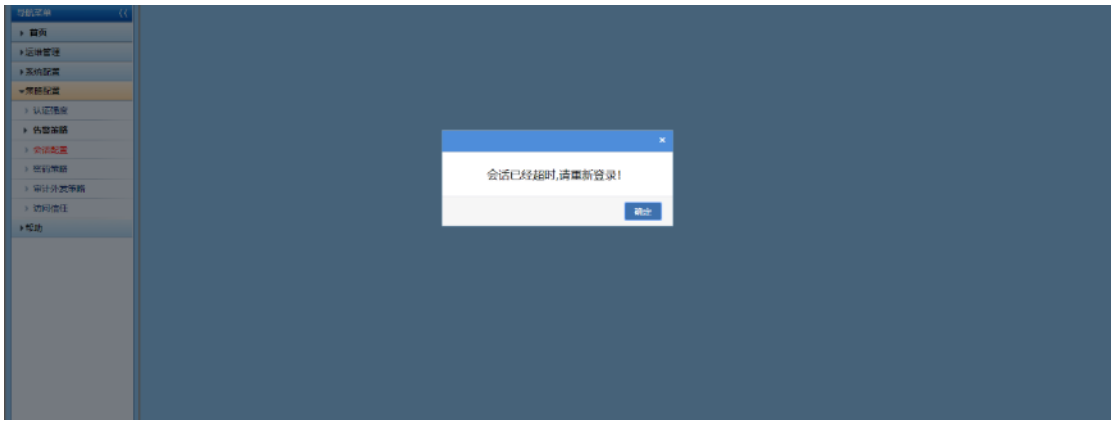
在会话配置页面，设置 web 会话超时时间为 5 分钟，点击确定。



页面弹出提示框：保存成功！



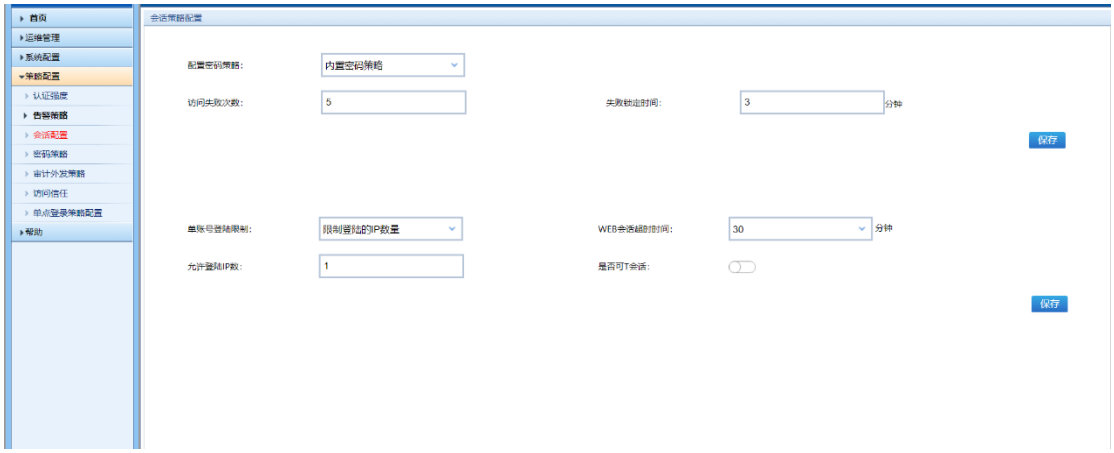
当用户 sysAdmin 五分钟没有对系统做任何操作，五分钟后点击页面，系统提示会话已经超时，请重新登录！



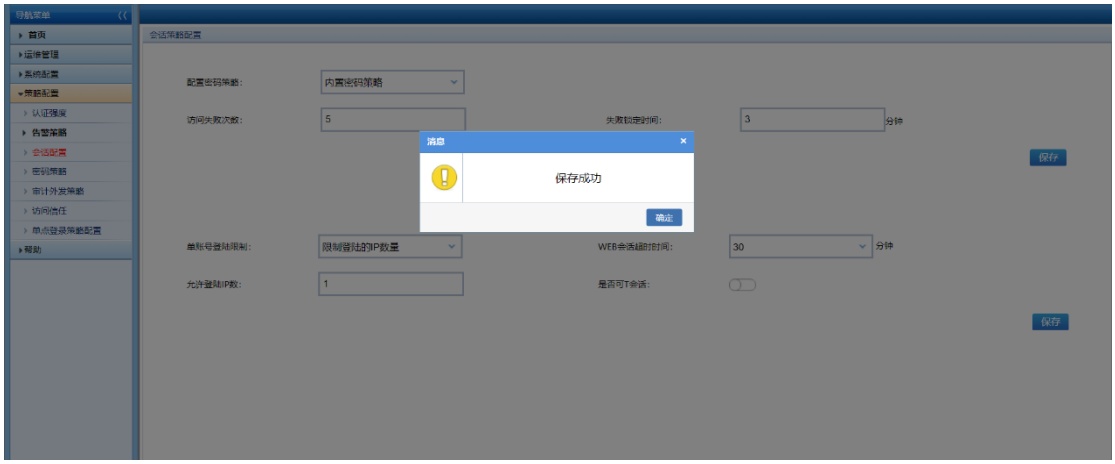
11.3.4. 单用户登录方式

单用户登录方式分为无限制 ip 登录和限制 ip 登录的数量。无限制 ip 登录指同一个系统账号可以同时在不同 ip 的设备上登录系统；限制 ip 登录的数量指同一系统用户账号在多 ip 地址登陆的数量限制。

在会话配置页面，选择单用户登录方式：限制登录的 ip 数量，允许登陆 IP 数：1，点击确定。



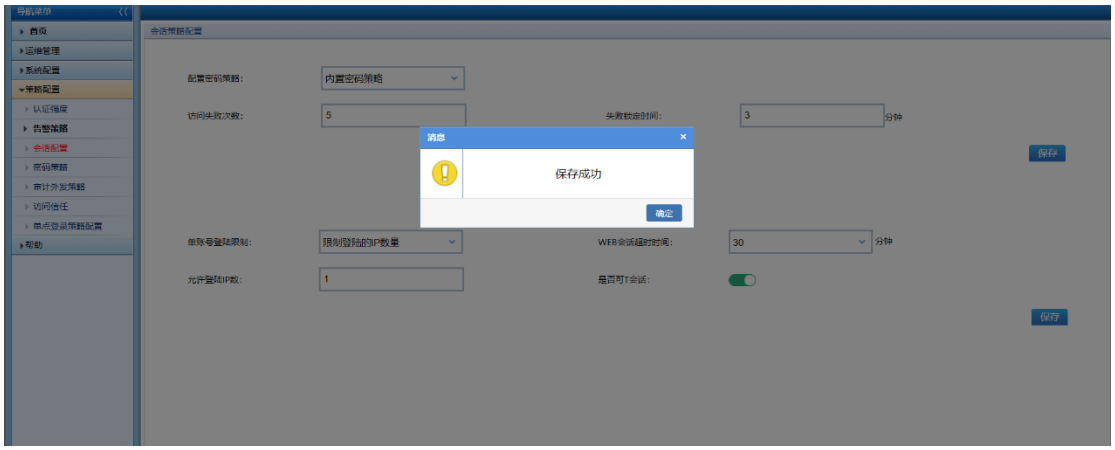
页面弹出提示框：保存成功！



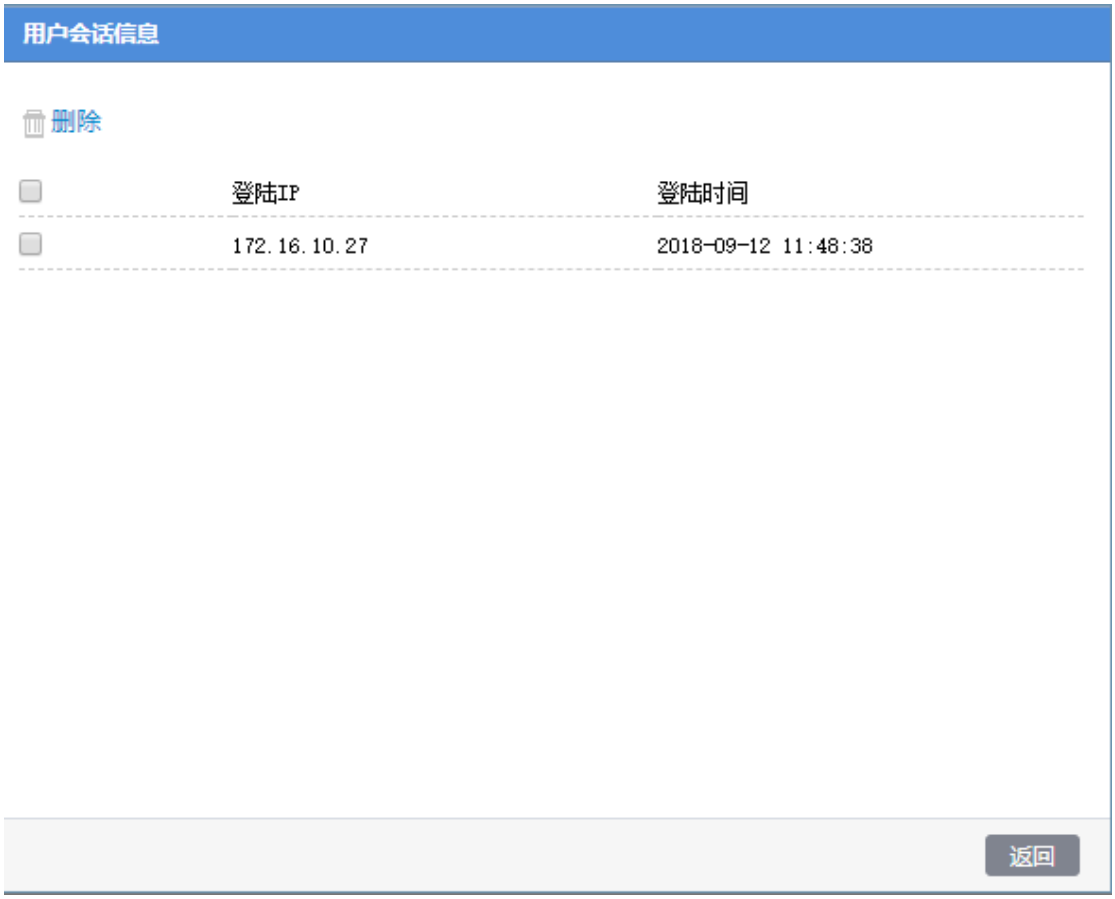
通过其他主机访问系统，使用用户 sysAdmin 登录，登录界面提示：当前登录数已达到最大。

在会话配置页面，选择单用户登录方式：限制最大登录数，最大在线数：1，打开可 T 会话按钮开关，点击确定。

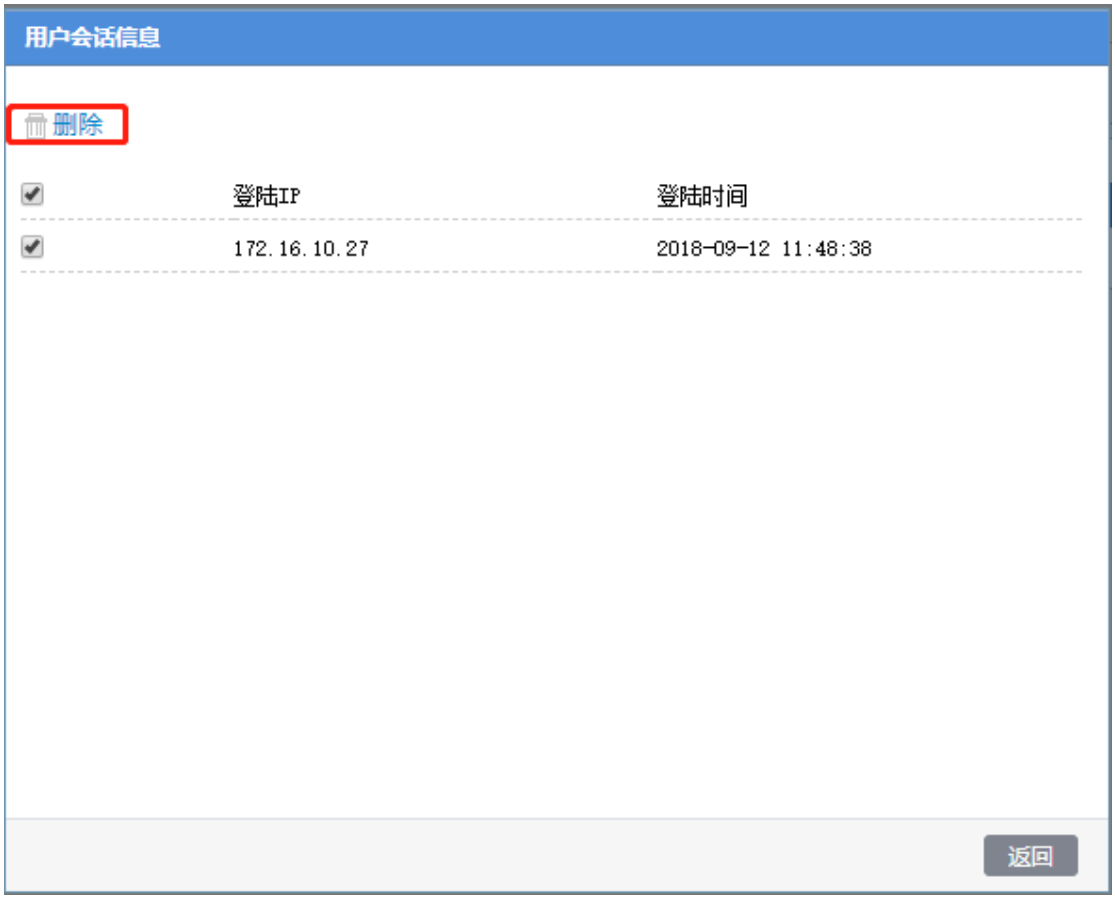
页面弹出提示框：保存成功！



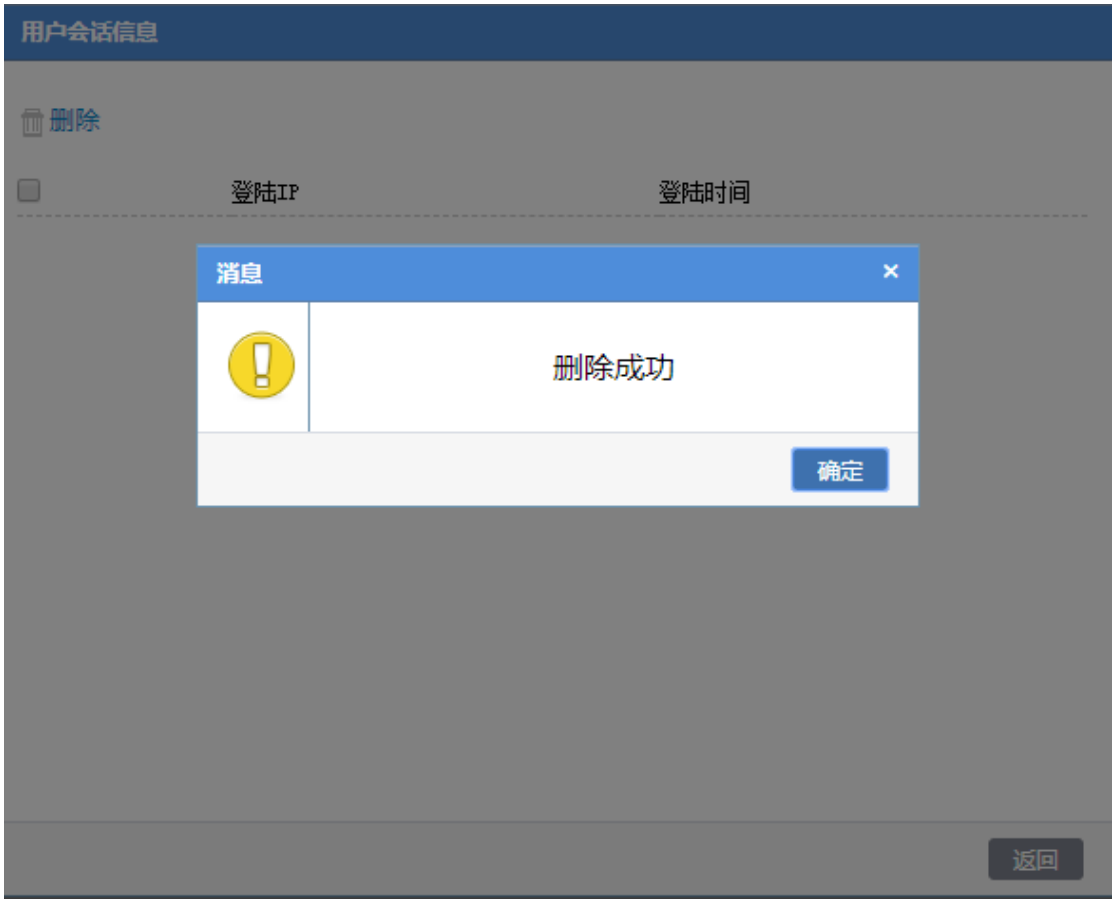
通过其他主机访问系统，使用用户 sysAdmin 成功登录，界面弹出用户会话信息弹框。



勾选需要 T 掉的登录 IP172.16.10.27，点击删除。



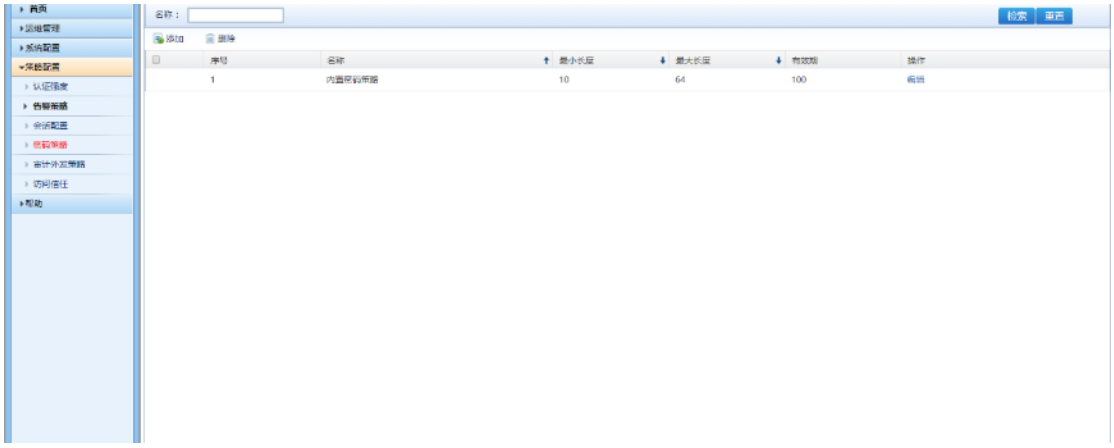
页面弹出提示弹框：确定要 T 掉所选会话吗？点击确定，页面提示删除成功。



11.4. 密码策略

密码策略是按照口令策略的规则设定进行修改口令以保证密码符合密码复杂度要求。

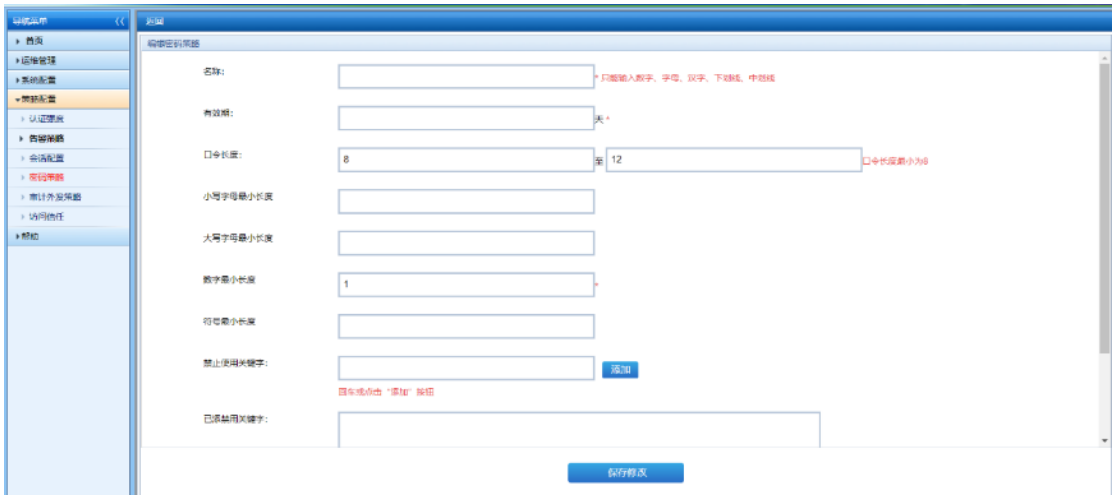
用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->密码策略进入到密码策略界面。



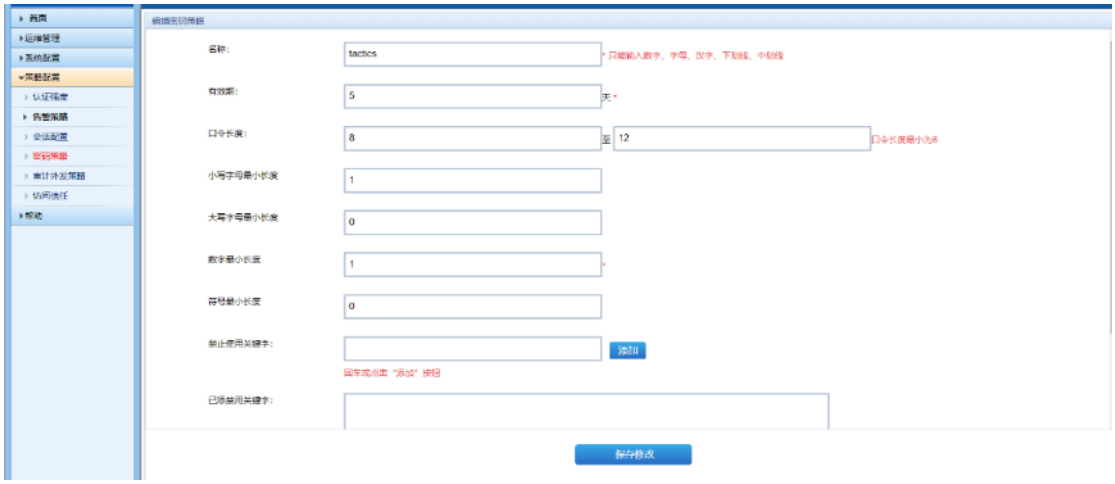
11.4.1. 添加密码策略

在密码策略页面，点击添加。

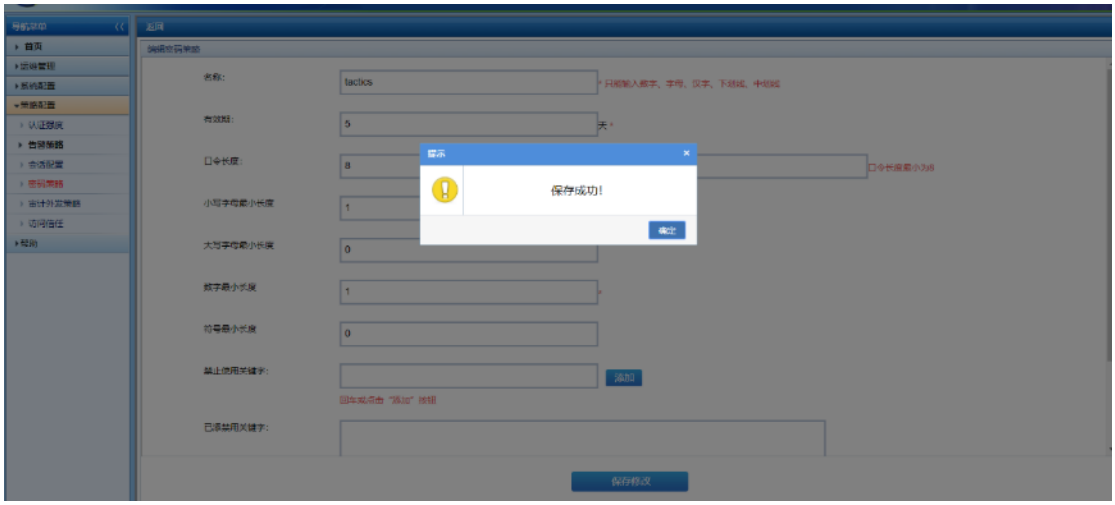
页面跳转到编辑密码策略界面。



输入密码策略名称：tactics，有效期：5 天，口令长度：8 到 12 位，小写字母长度：1，点击保存。



页面弹出提示框：保存成功！

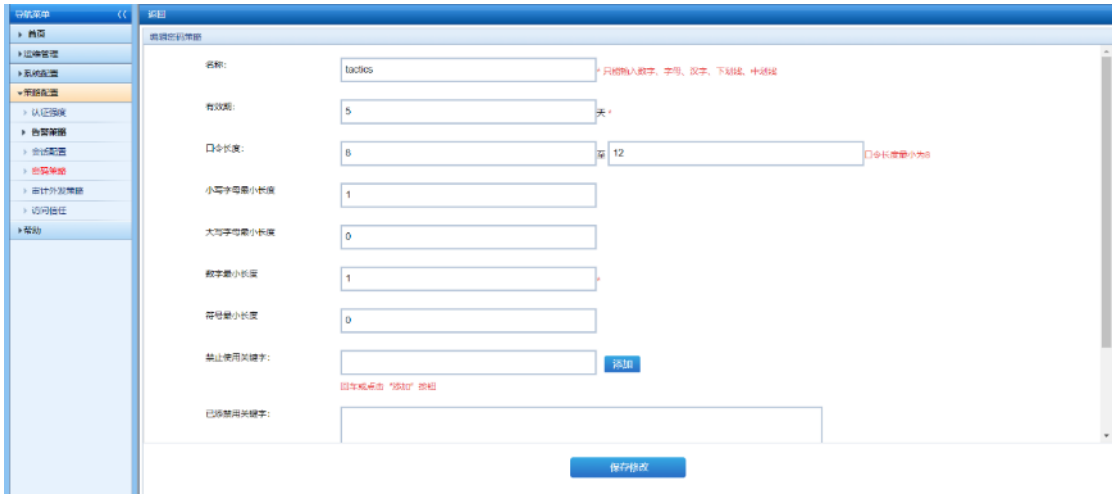


在密码策略页面显示已添加的 tactics 密码策略。

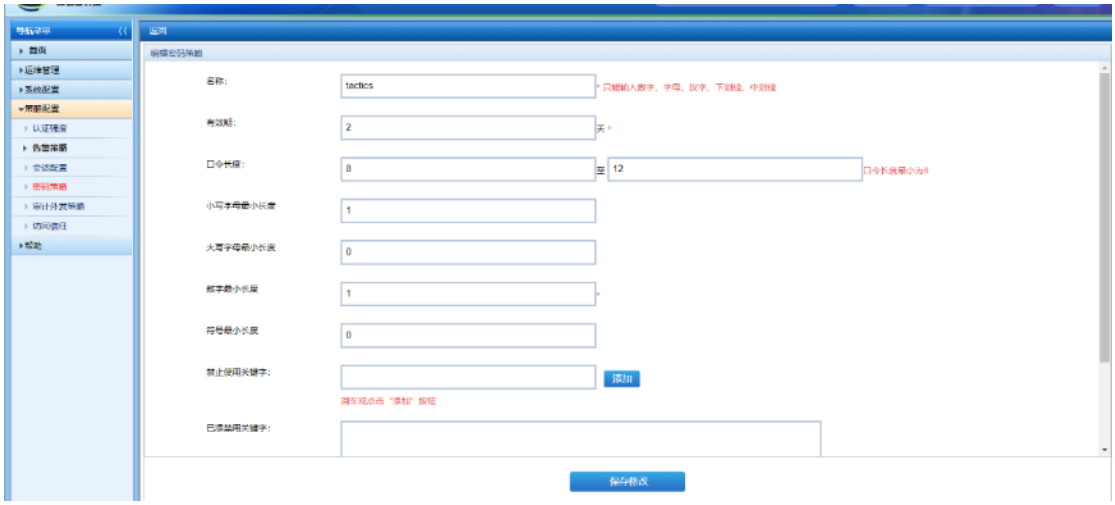
11.4.2. 编辑密码策略

在密码策略界面，点击 tactics 操作列编辑按钮。

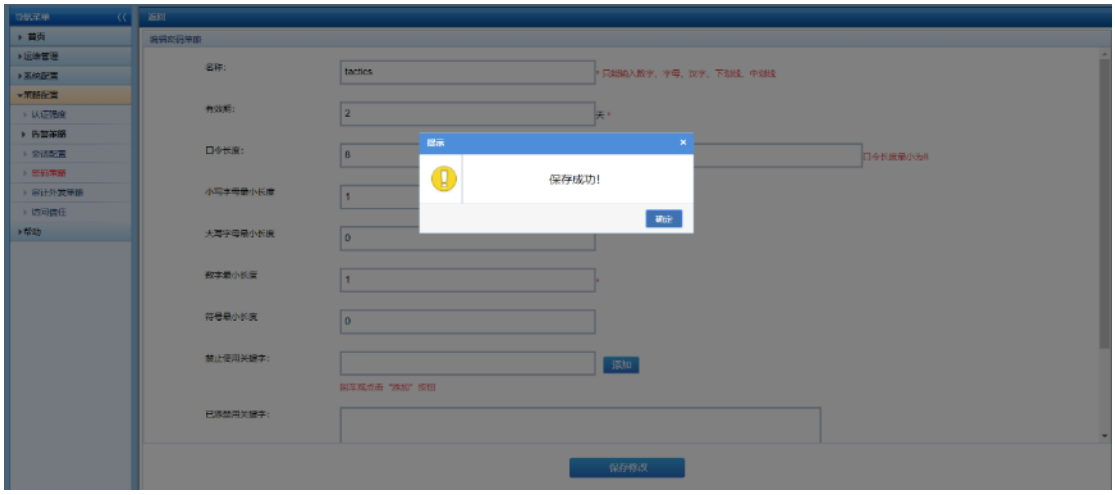
页面跳转到编辑密码策略界面。



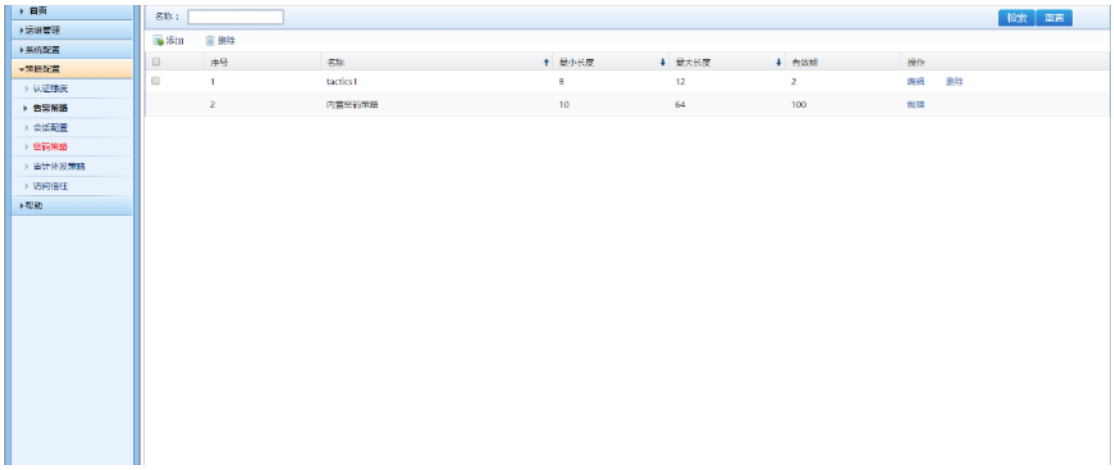
编辑需要修改的名称：tactics1，有效期：2 天，点击保存。



页面弹出提示框：保存成功。



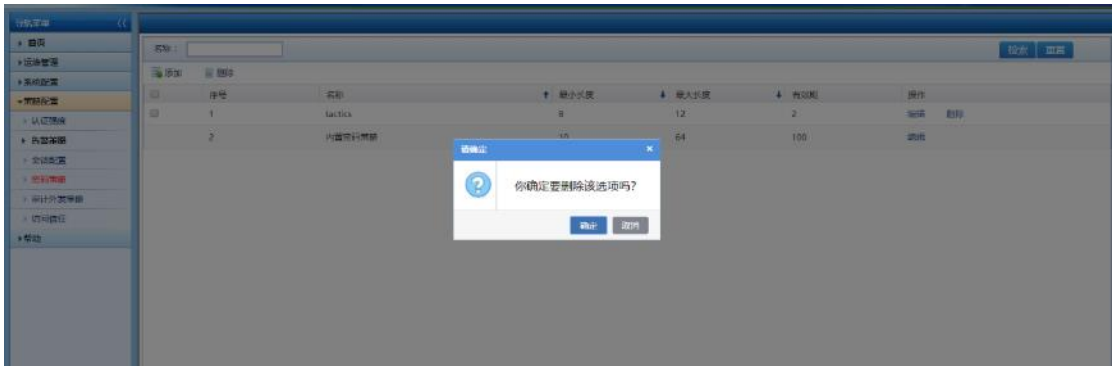
返回到密码策略页面，显示已修改的名称：tactics1，有效期：2 天。



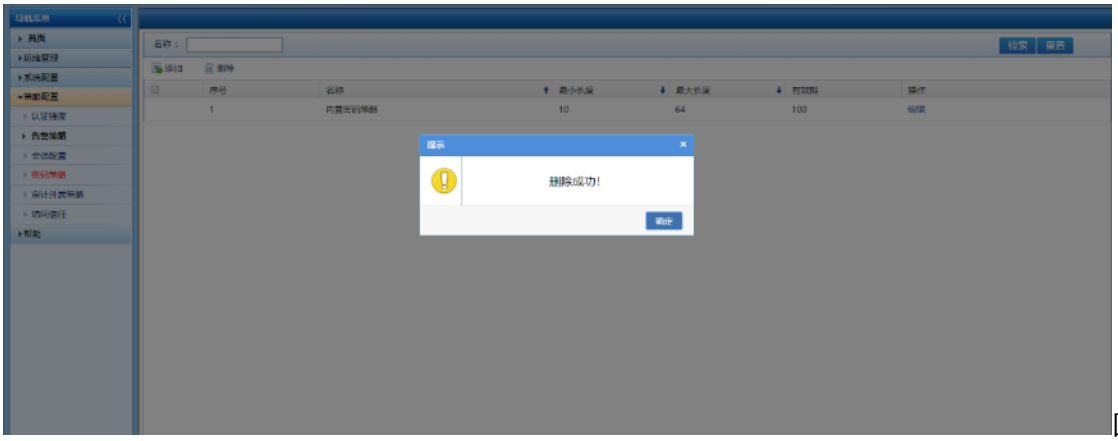
11.4.3. 删除密码策略

在密码策略页面，tactics 口令策略操作列下，点击删除。

页面弹出提示弹框：确定要删除该选项吗？点击确定。



页面弹出提示框：删除成功。

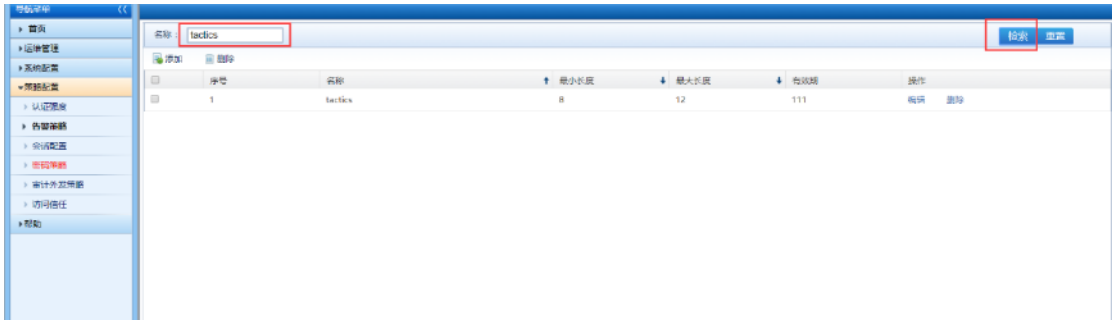


图

11.4.4. 密码策略名称检索

在密码策略页面，名称检索框内输入：tactics，点击检索按钮。

页面检索出名称含有 tactics 的口令策略。

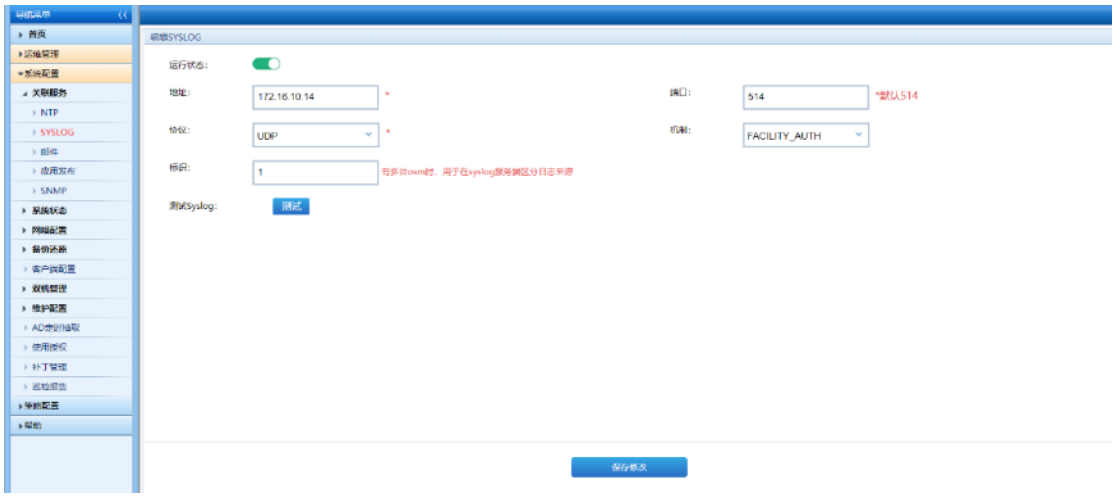


11.5. 审计外发策略

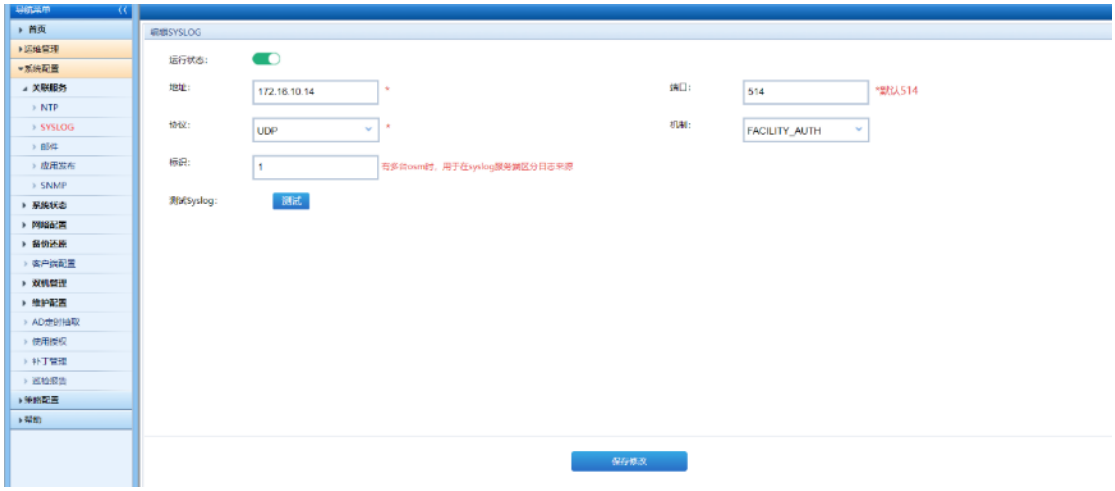
审计外发策略包含运维审计外发，配置审计外发。发送方式以 syslog 方式发送到日志服务器。

11.5.1. 配置 syslog 日志服务器

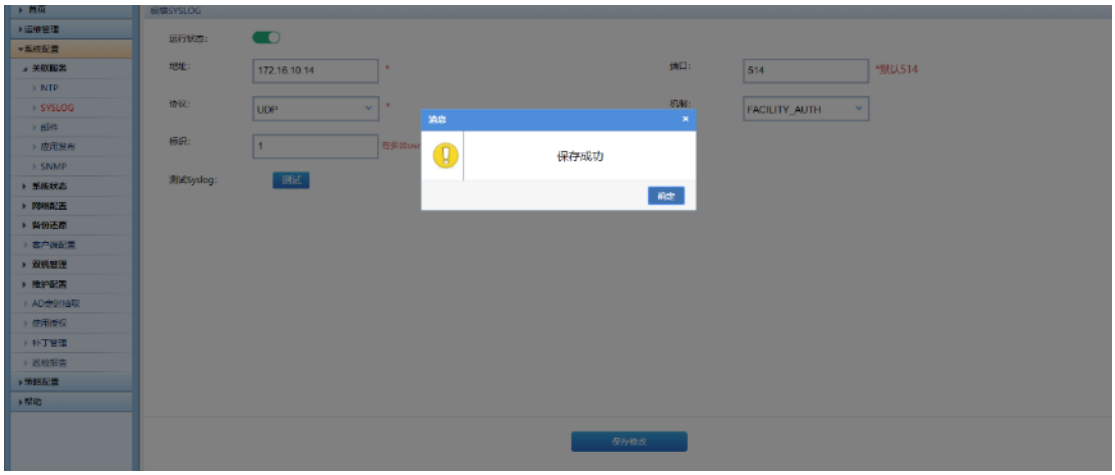
用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->关联服务->SYSLOG 进入到 syslog 界面。



syslog IP 设定为日志服务器接收的 IP:172.16.10.14，点击保存。



页面弹出提示框：保存成功。

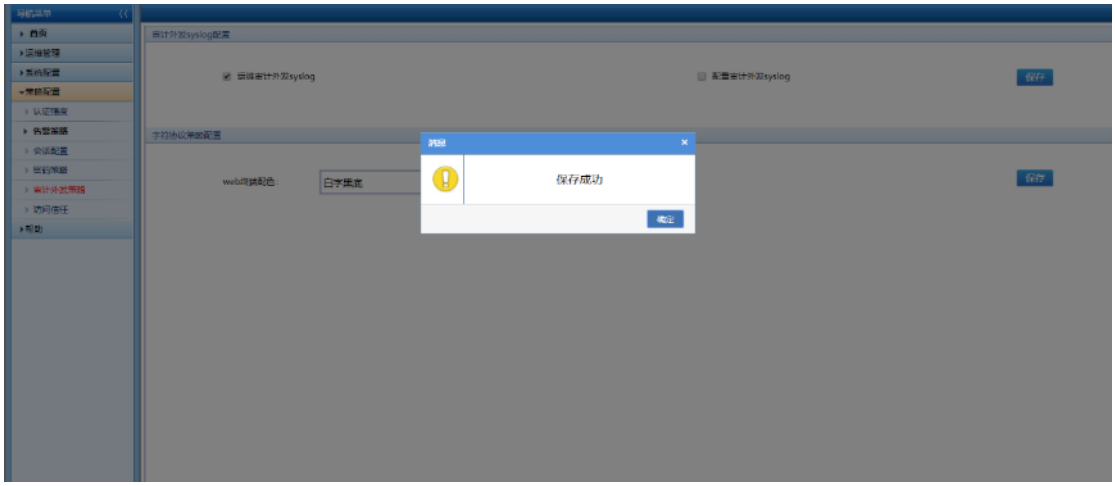


11.5.2. 运维审计外发 syslog

用户在系统中进行单点登录操作结束时，运维审计会向 syslog 日志服务器发送信息。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->审计外发策略进入到审计外发策略界面，勾选运维审计外发 syslog，点击保存。

页面弹出提示框：保存成功，用户 sysAdmin 退出系统。



安全管理员 secAdmin 登录系统，切换至安全管理员角色，添加 linux 资源 IP172.16.20.211 并绑定授权，授权名称 linux。

用户 sysAdmin 切换至运维操作员角色，对 linux 资源 IP172.16.20.211 进行单点登录。

syslog 日志服务器收到日志信息格式<AUDIT_LOG>[sysAdmin](通过账号[sysAdmin]登录在[2018-09-12 15:15:53]到[2018-09-12 15:16:22]通过[172.16.10.14]访问[172.16.20.211],用[root]账号

通过[ssh2]协议访问[211](资源类型[RedHat])。日志级别:[INFO]

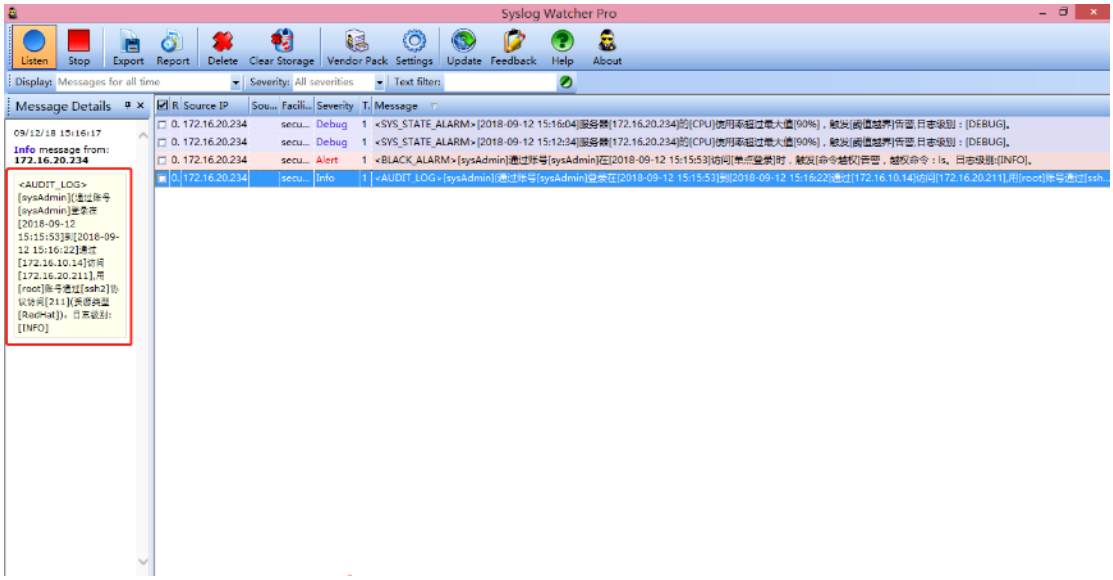
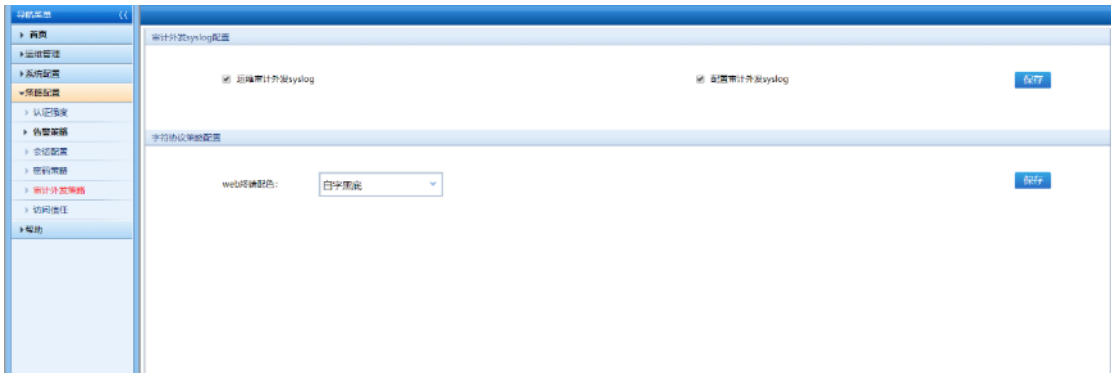


图 3.12.5.2-4

11.5.3. 配置审计外发 syslog

用户对系统进行配置操作时，配置审计会向 syslog 服务器发送信息。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->审计外发策略进入到审计外发策略界面，勾选配置审计外发，点击保存。



页面弹出提示框：保存成功。

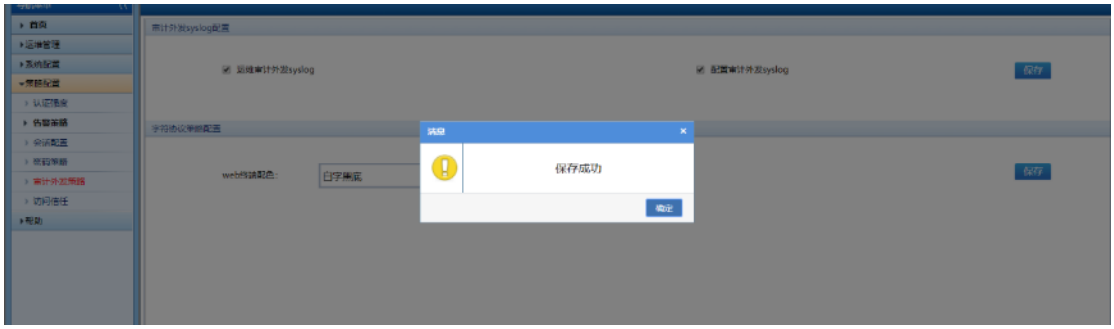


图 3.12.5.3-2

Syslog 日志服务器收到日志信息格式：sysAdmin(通过账号 sysAdmin 登录)，在 2018-09-12 15:19:30 通过 172.16.10.14 做登录操作，操作成功。日志级别：[INFO]。

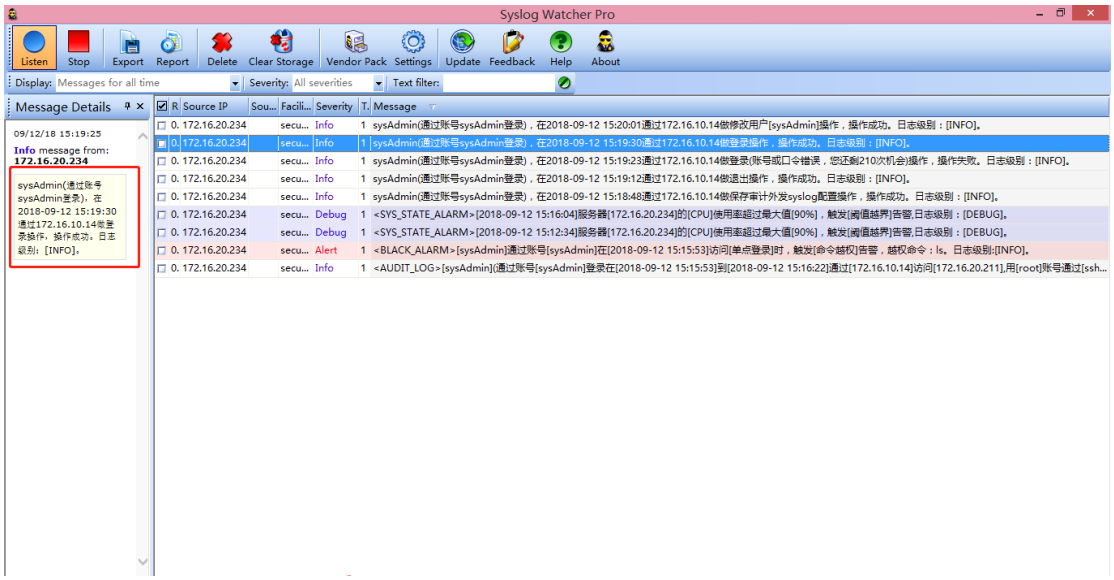


图 3.12.5.3-3

11.6. 访问信任

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->访问信任进入到访问信任界面。

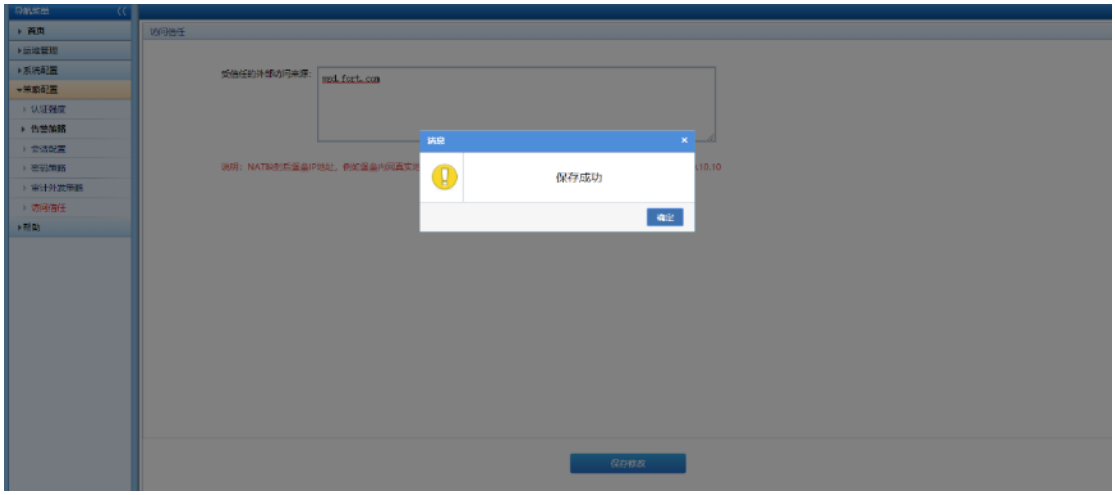


图 3.12.6-1

受信任的外部访问来源输入 wsd.fort.com，点击保存按钮，保存成功。在地址栏输入 https://wsd.fort.com，可以访问系统。

11.7. 单点登录策略配置

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击策略配置->单点登录策略配置，进入到单点登录策略配置界面。

图 3.12.7-1

12. 口令计划

口令计划由口令修改计划，口令备份计划，口令备份 FTP 三部分组成。

口令修改计划可创建改密计划，对系统中的资源账号进行一次或多次改密。

口令修改计划支持的口令设置方式：

- 手动指定固定口令
- 通过密码表生成
- 依照各资源本身制定的密码策略生成各自相应的密码
- 选取一种密码策略生成同一个密码

口令备份计划可备份系统内的资源账号及口令。

口令备份计划支持的备份方式：

- 本地备份
- FTP 备份

口令备份 FTP 是配置 FTP 服务器的地址和远程备份路径。当口令备份计划备份方式为 FTP 发送时，此配置生效。

12.1. 口令修改计划

用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令修改计划链接进入口令修改计划界面。

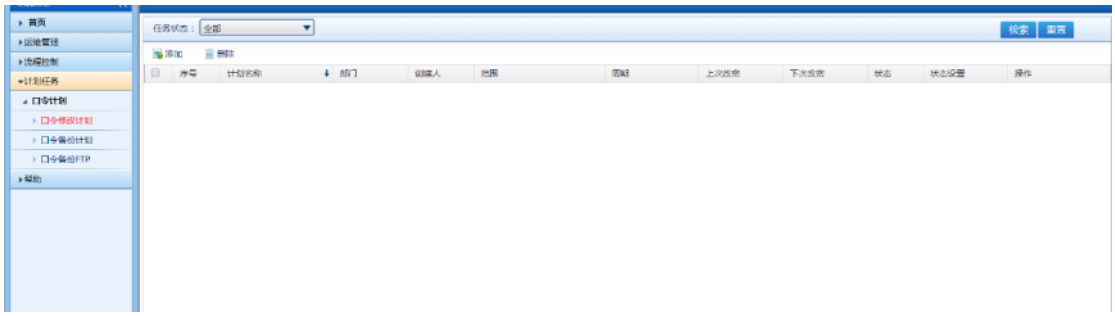


图 3.13.1-1

12.1.1. 添加密码包接收人

密码包接收人是指口令修改计划完成后接收密码包的用户。

密码包接收人必须具备的条件：

- 拥有密码包接收人角色权限
- 配有邮件地址

具体操作如下:

初始化用户 admin 登陆系统，点击角色管理->角色定义链接进入角色定义界面。

图 3.13.1.1-1

点击添加按钮，跳转到角色定义编辑页面。

图 3.13.1.1-2

填写角色基本信息：

1) 角色名称：密码包接收人
2) 名称简写：密码包
3) 级别：部门级
4) 菜单：计划任务
5) 其他权限：密码包接收人

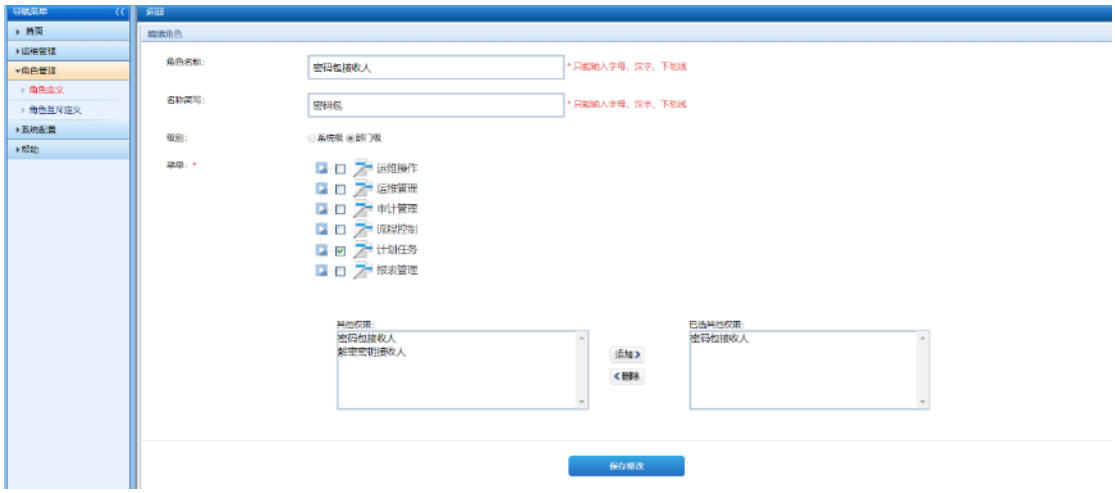


图 3.13.1.1-3

点击保存，提示保存成功！

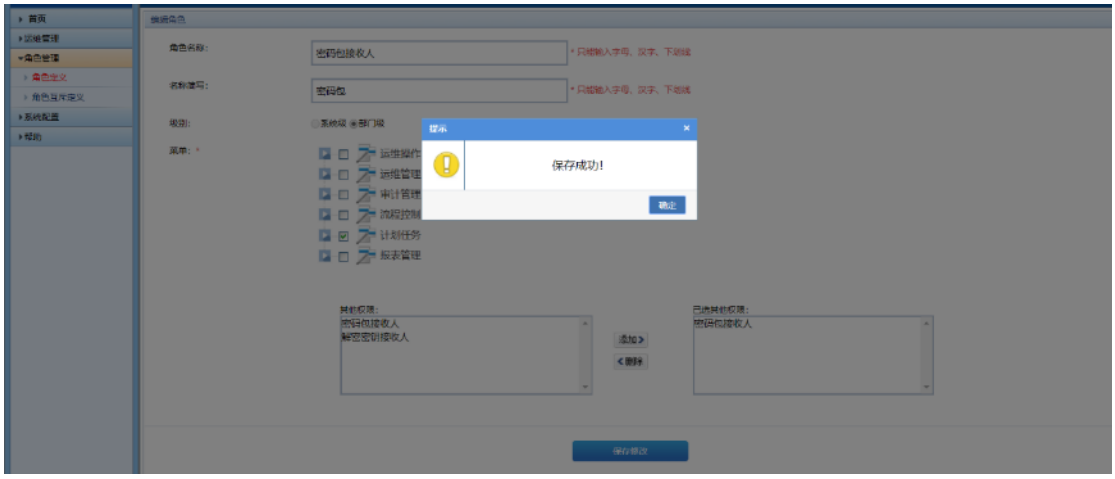


图 3.13.1.1-4

点击确定，返回列表页，列表页显示密码包接收人角色。

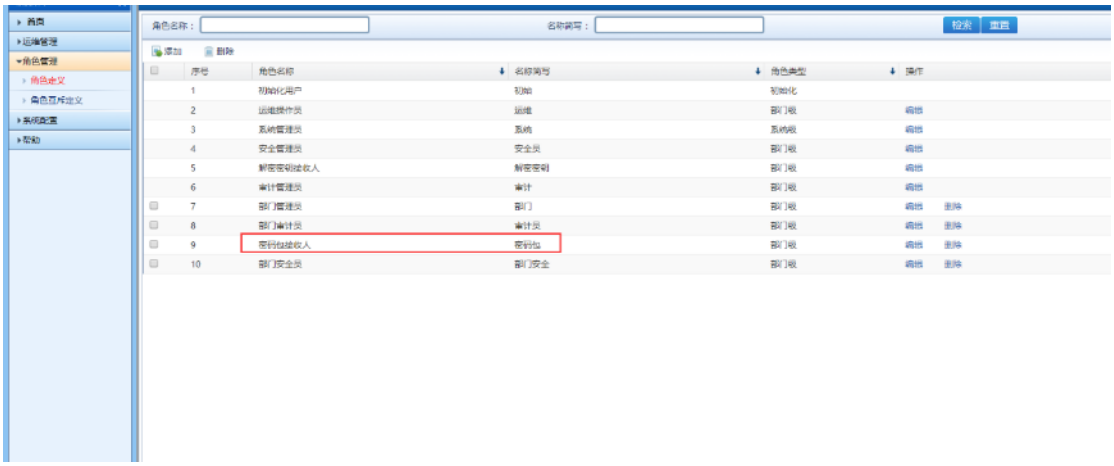


图 3.13.1.1-5

点击运维管理->用户链接，进入用户界面。

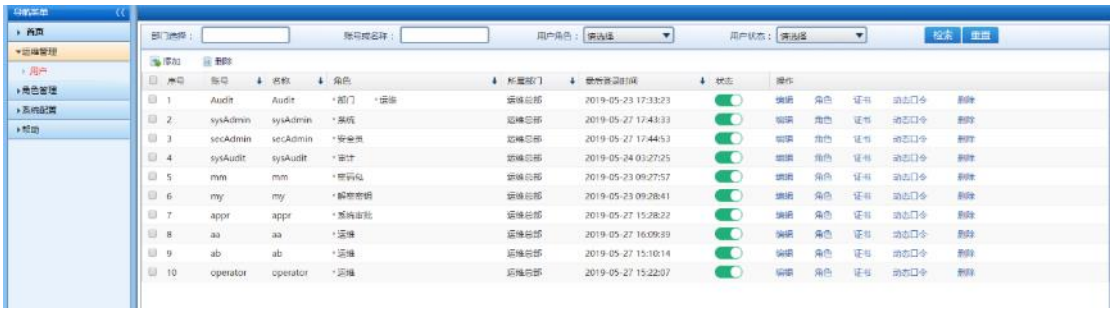


图 3.13.1.1-6

点击添加，进入用户编辑页面。

图 3.13.1.1-7

用户的基本信息如下：

1) 用户账号：mm
2) 用户名称：密码包接收人
3) 口令：admin@1234，确认口令：admin@1234
4) 电子邮箱：zlj1@fort.cn（接收密码包的指定邮箱）

图 3.13.1.1-8

角色选择密码包接收人。

图 3.13.1.1-9

点击保存，提示保存成功！

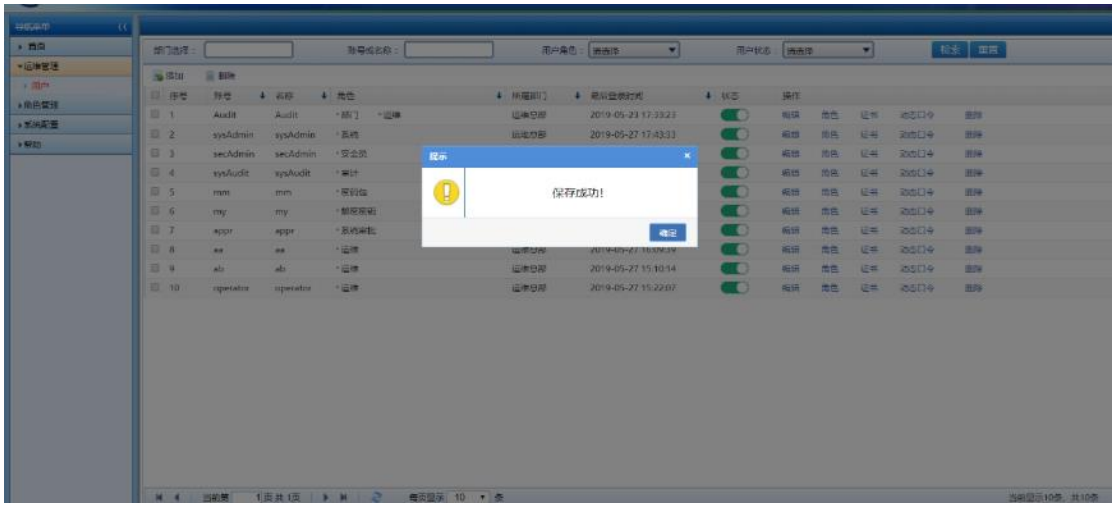


图 3.13.1.1-10

点击确定，返回用户列表页，列表页显示名称为密码包接收人的用户。

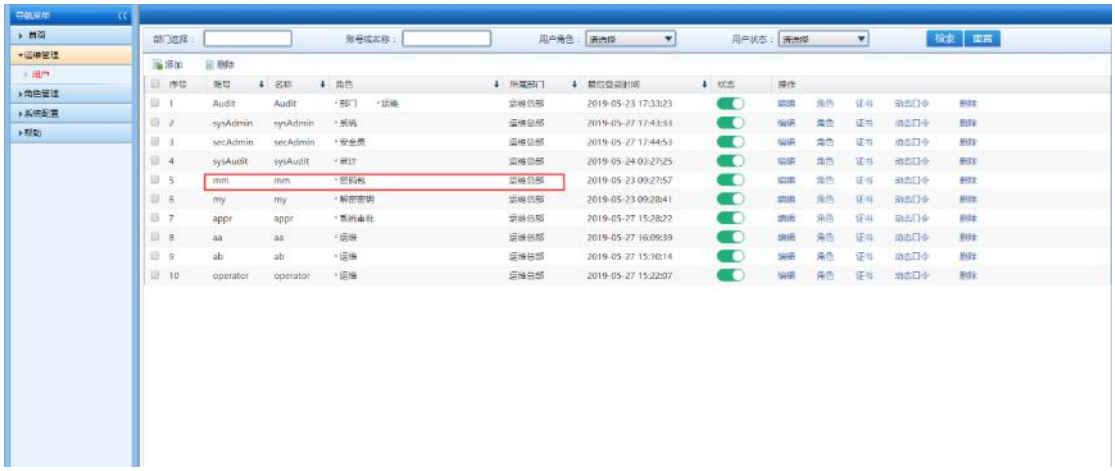


图 3.13.1.1-11

12.1.2. 添加解密密钥接收人

解密密钥接收人是指口令修改计划完成后接收解密密钥的用户。

系统中默认的解密密钥接收人为系统管理员角色用户。

解密密钥接收人必须具备的条件：

- 拥有解密密钥接收人角色权限
- 配有邮箱

具体操作如下:

初始化用户 admin 登陆系统，点击角色管理->角色定义链接进入角色定义界面。

图 3.13.1.2-1

点击添加按钮，跳转到角色定义编辑页面。

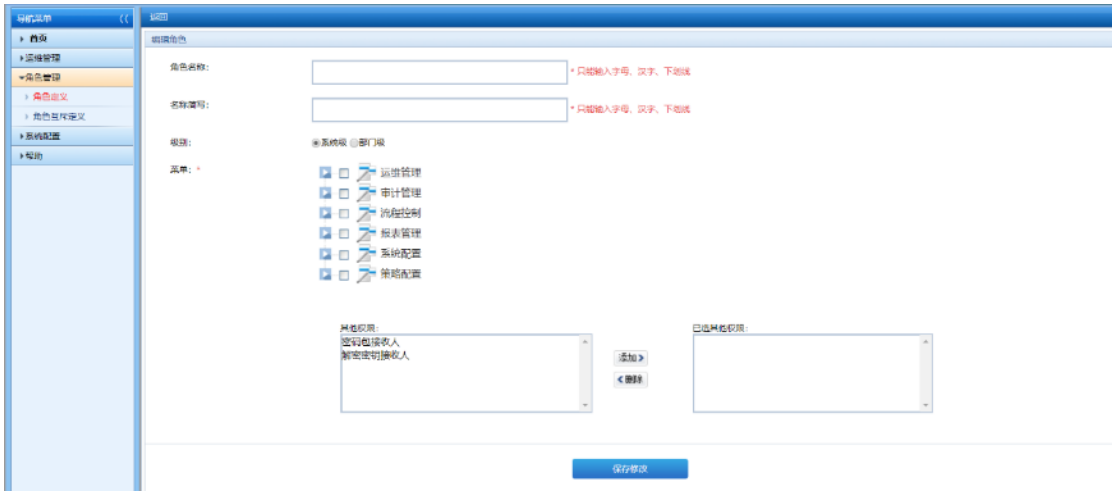


图 3.13.1.2-2

填写角色基本信息：

1) 角色名称：解密密钥接收人
2) 名称简写：密钥
3) 级别：部门级
4) 菜单：计划任务
5) 其他权限：解密密钥接收人

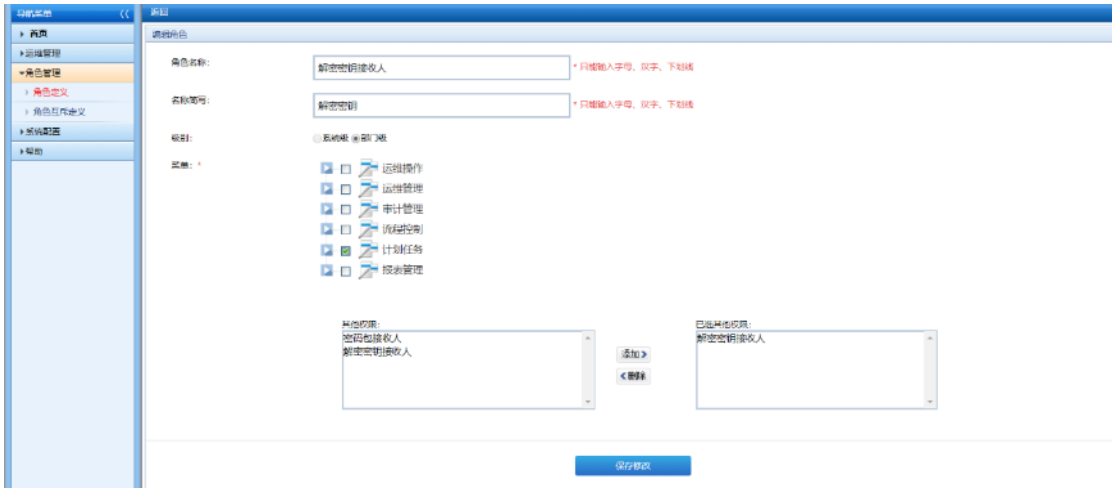


图 3.13.1.2-3

点击保存，提示保存成功！

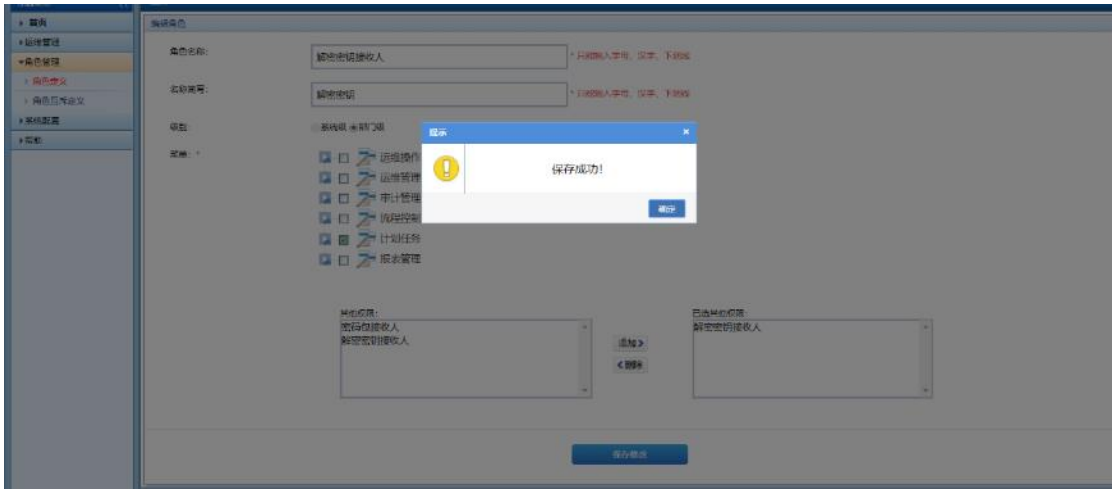


图 3.13.1.2-4

点击确定，返回列表页，列表页显示解密密钥接收人角色。

图 3.13.1.2-5

点击运维管理->用户链接进入用户界面。

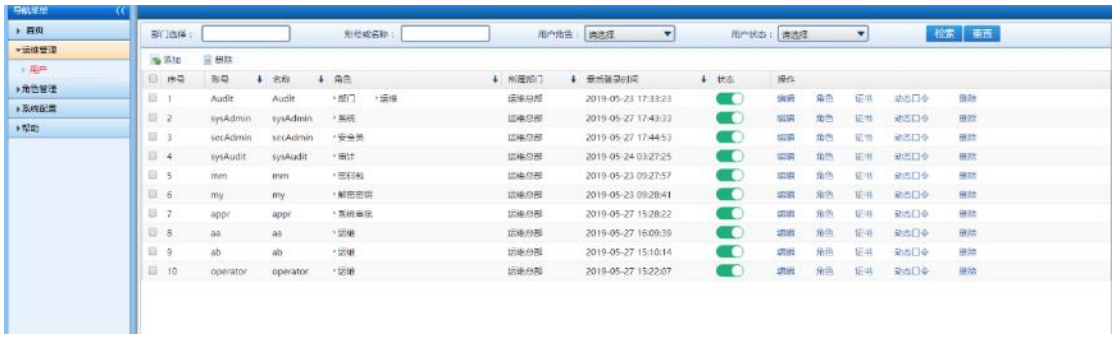


图 3.13.1.2-6

点击添加，进入用户编辑页面。

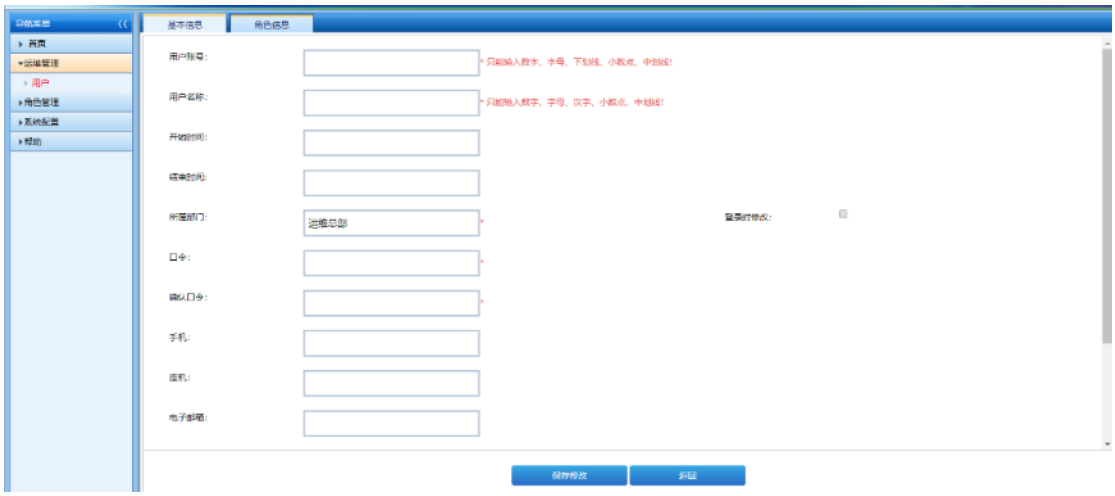


图 3.13.1.2-7

用户基本信息如下：

1) 用户账号：my
2) 用户名称：解密密钥接收人
3) 口令：admin@1234，确认口令：admin@1234
4) 电子邮箱：zlj1@fort.cn（接收解密密钥的指定邮箱）

图 3.13.1.2-8

角色选择解密密钥接收人。

图 3.13.1.2-9

点击保存，提示保存成功！

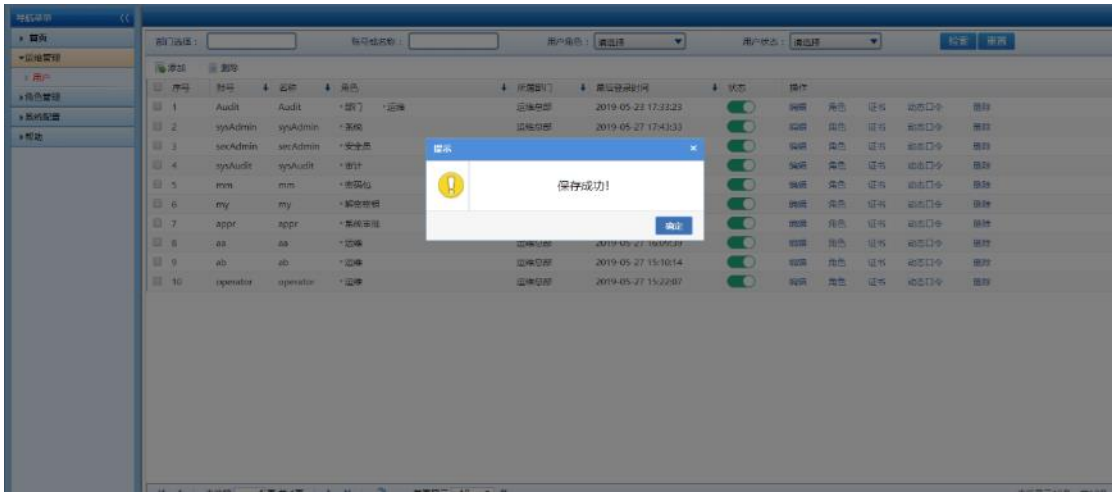


图 3.13.1.2-10

点击确定，返回用户列表页，列表页显示名称为解密密钥接收人的用户。

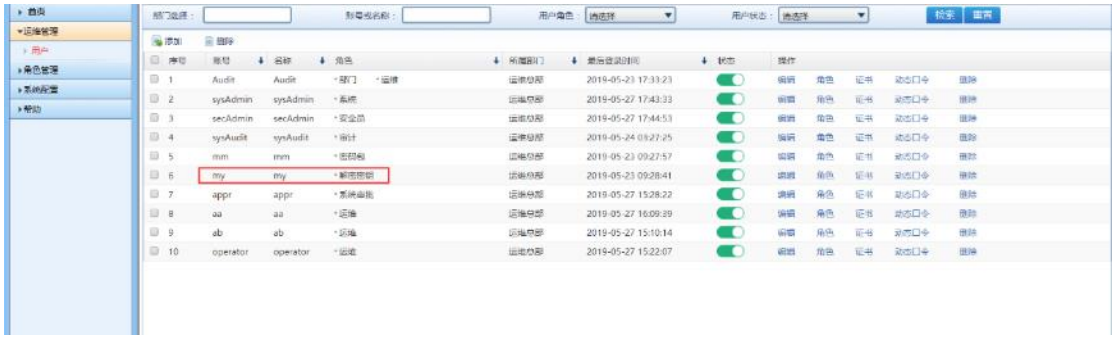


图 3.13.1.2-11

12.1.3. 添加并执行口令修改计划

1.定时执行-一次性执行

一次性执行是指口令修改计划到达设定时间后开始执行改密计划且只执行一次。

具体操作如下：

用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令修改计划链接进入口令修改计划界面。

图 3.13.1.3.1-1

点击添加，跳转到口令修改计划编辑页面。

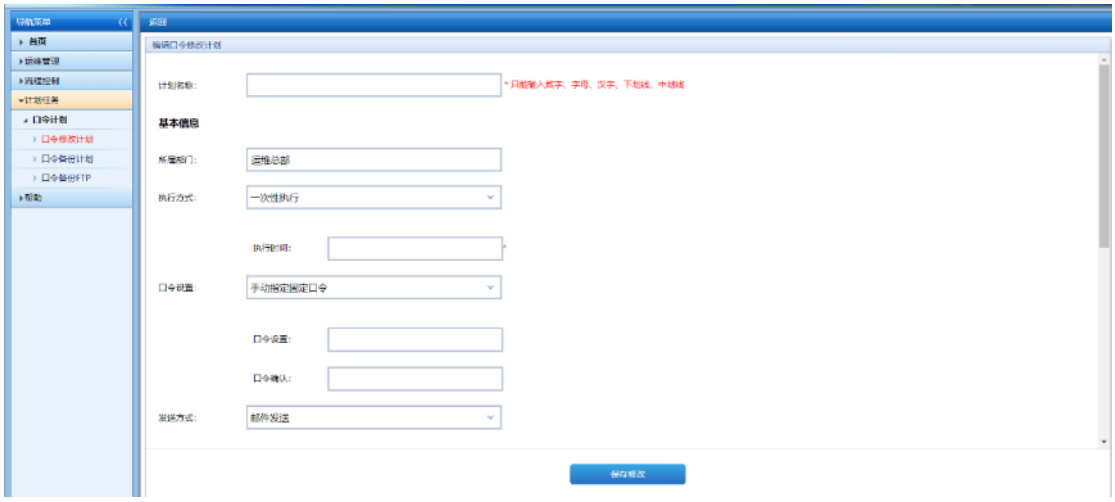


图 3. 13. 1. 3. 1-2

口令修改计划基本信息如下：

1) 计划名称：test1
2) 执行方式：一次性执行
3) 执行时间：今天
4) 口令设置：手动指定固定口令
5) 口令设置 admin@1234,口令确认 admin@1234
6) 发送方式：邮件发送
7) 添加需要改密的资源账号、资源或资源组

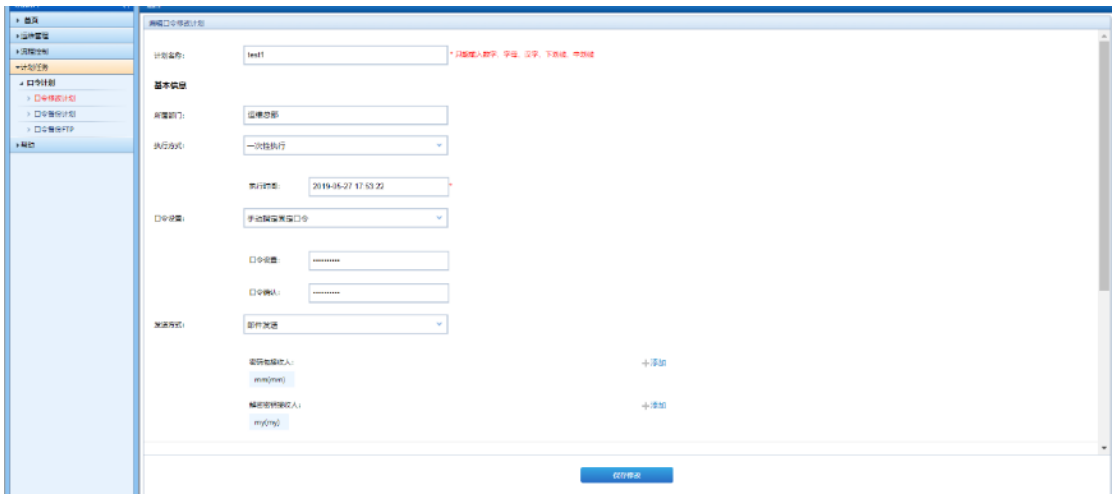


图 3.13.1.3.1-3

点击保存，提示保存成功！

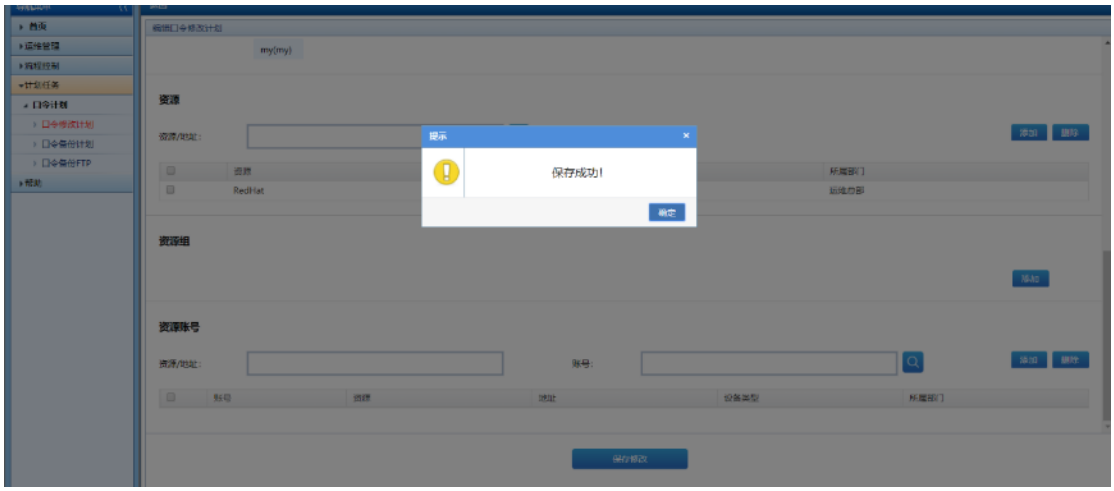


图 3.13.1.3.1-4

点击确定，返回列表页，列表中显示名称为 test1 的口令修改计划。

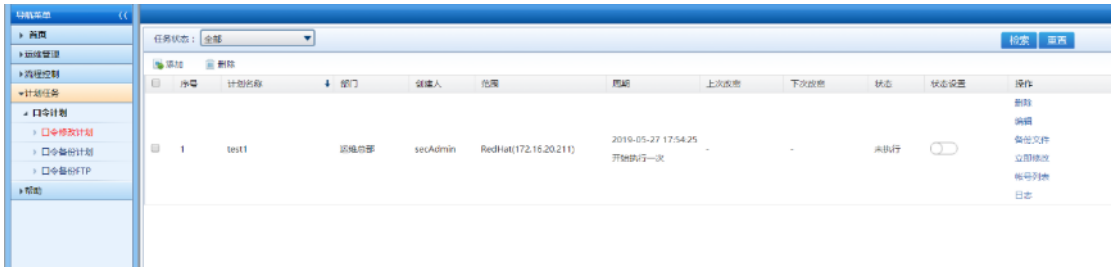


图 3.13.1.3.1-5

状态设置为开，定时开启，到达设定时间开始改密。

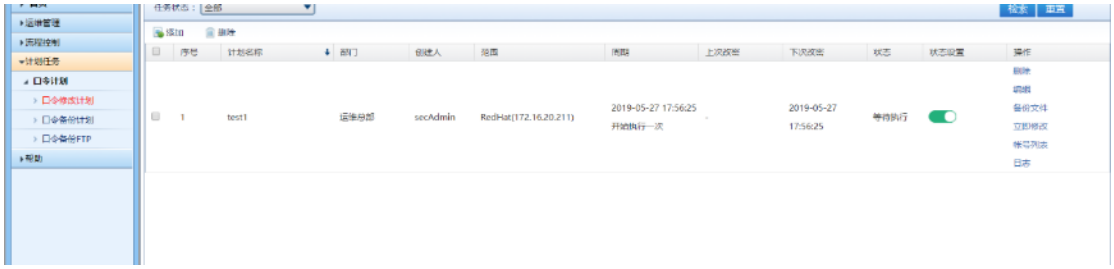


图 3.13.1.3.1-6

点击日志，可查看具体的改密过程中的情况。

图 3.13.1.3.1-7

改密完成后，将邮箱里接收的密码包和解密密钥用解密器进行解密。

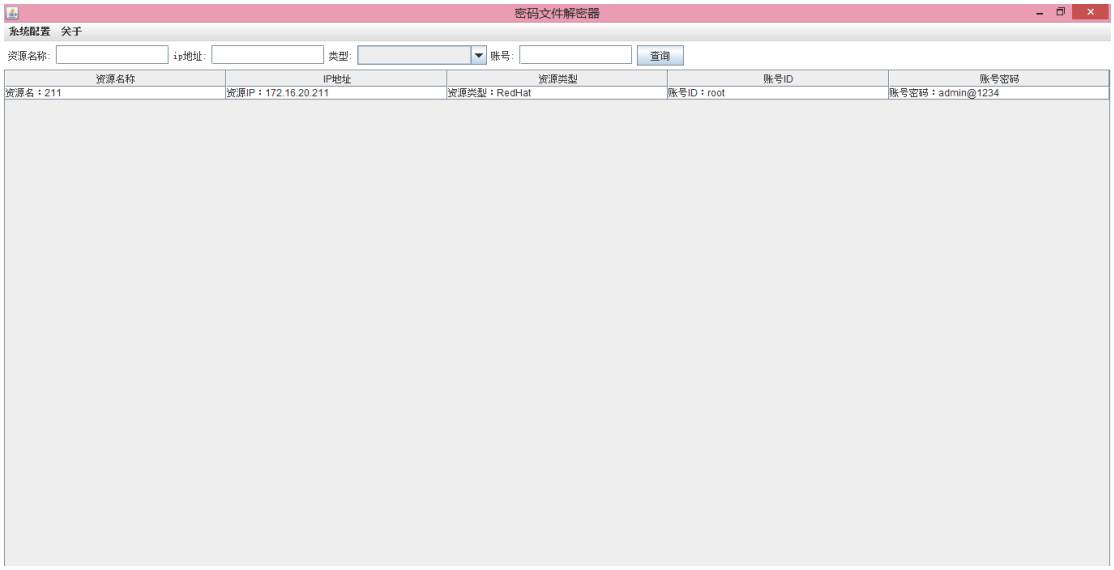


图 3.13.1.3.1-8

2.定时执行-周期性执行

周期性执行是指口令修改计划在一定时间范围内定期执行改密操作。

具体操作如下：

点击添加，跳转到口令修改计划编辑页面。

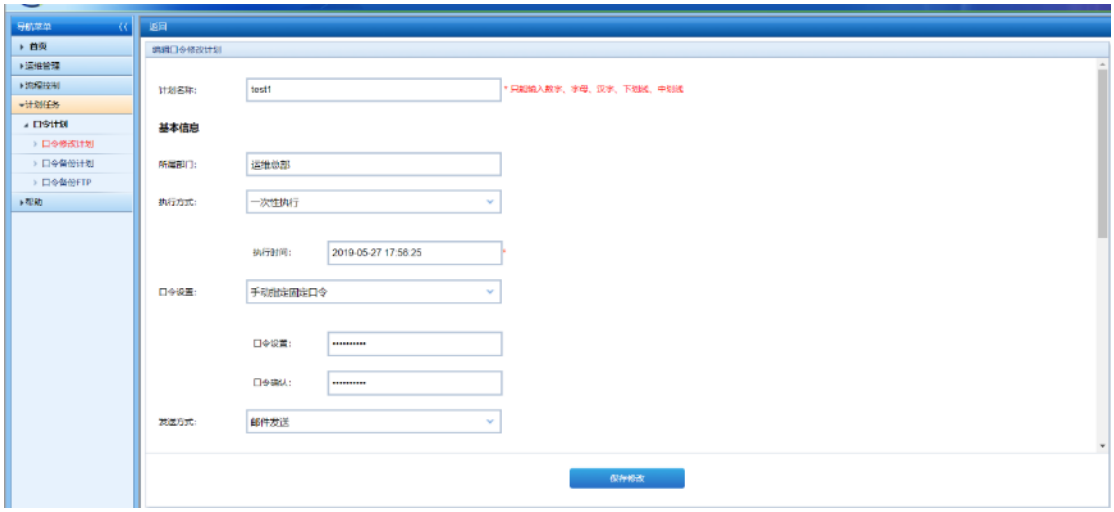


图 3. 13. 1. 3. 2-1

口令修改计划基本信息如下：

1) 计划名称：test2
2) 执行方式：周期性执行
3) 执行时间：16 时 27 分
4) 执行方式：按天执行
5) 口令设置：手动指定固定口令
6) 口令设置 admin@1234,口令确认 admin@1234
7) 发送方式：邮件发送
8) 添加需要改密的资源账号、资源或资源组

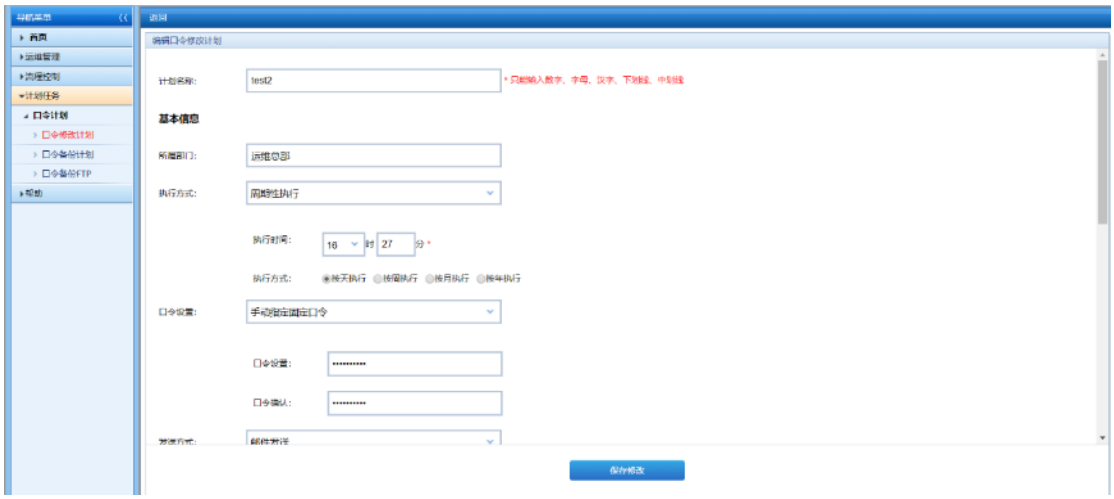


图 3.13.1.3.2-2

点击保存，提示保存成功！

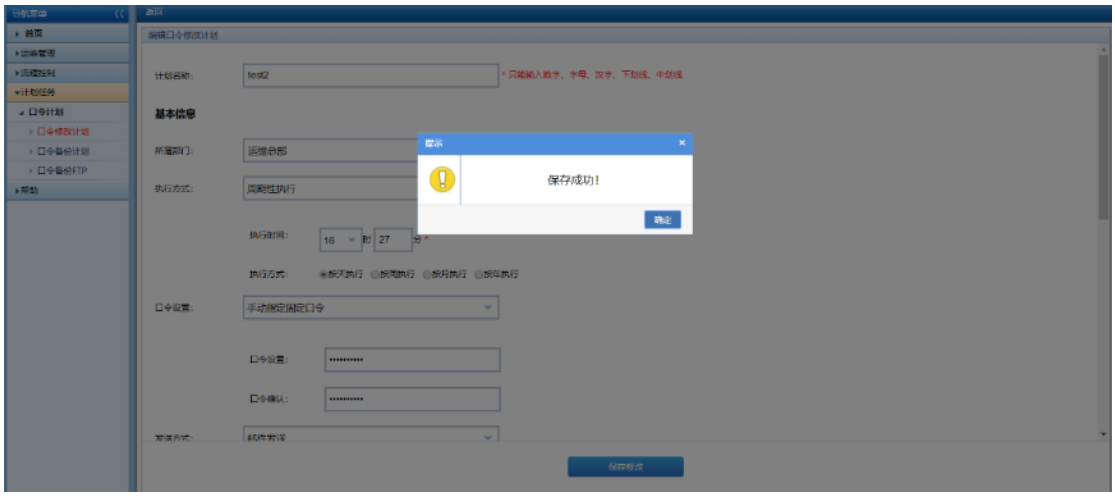


图 3.13.1.3.2-3

点击确定，返回列表页，列表中显示名称为 test2 的口令修改计划。

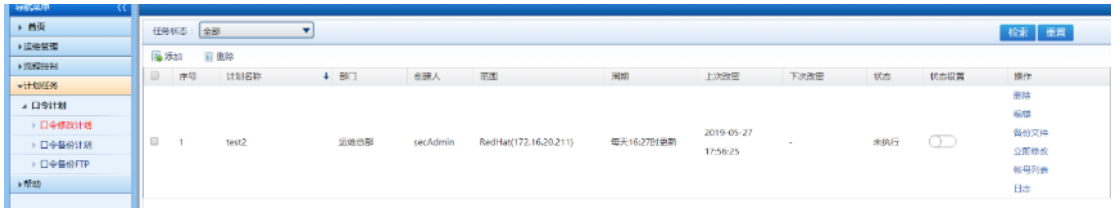


图 3.13.1.3.2-4

状态设置为开，定时开启，到达设定时间开始改密。

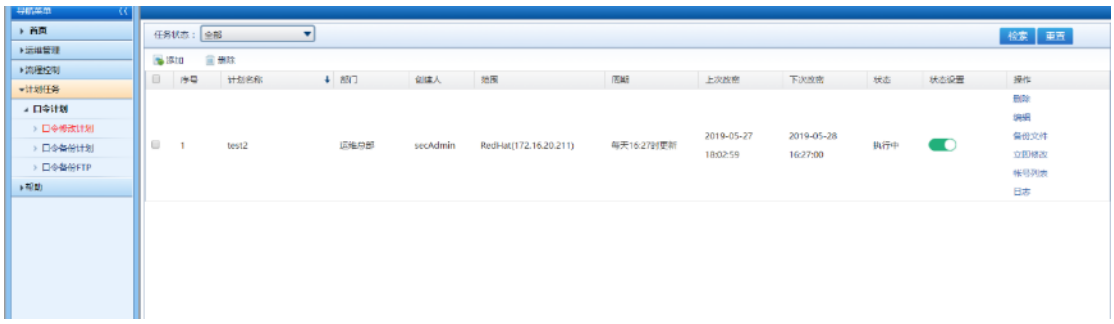


图 3.13.1.3.2-5

点击日志，可查看具体的改密过程中的情况。

图 3.13.1.3.2-6

改密完成后，将邮箱里接收的密码包和解密密钥用解密器进行解密。

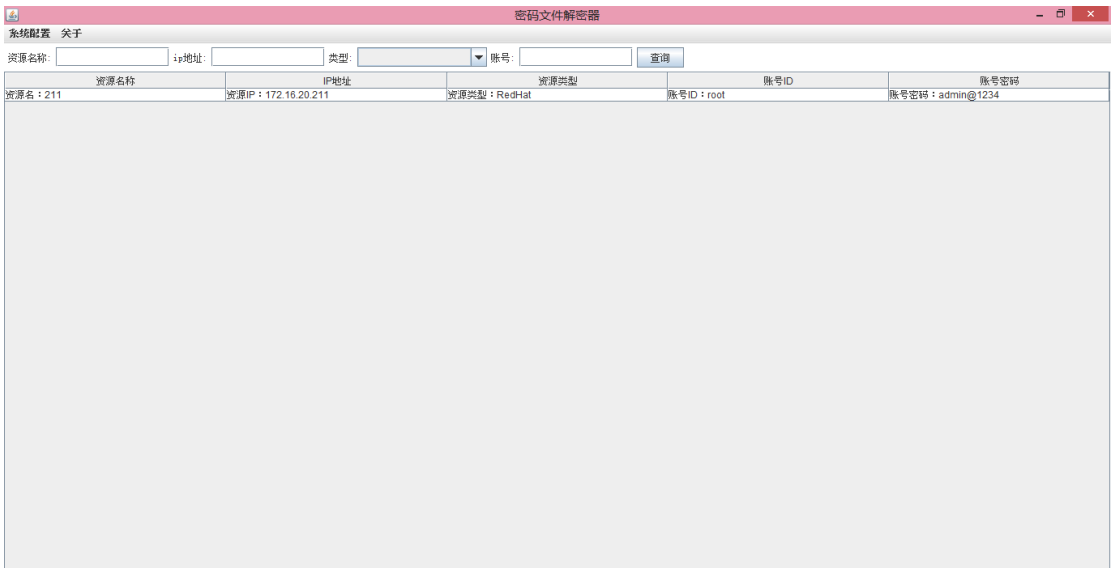


图 3.13.1.3.2-7

3.口令设置-通过密码表生成

口令修改计划允许添加多个密码进入密码表，改密时根据密码表的先后顺序选定密码进行改密操作。

具体操作如下：

点击添加，跳转到口令修改计划编辑页面。

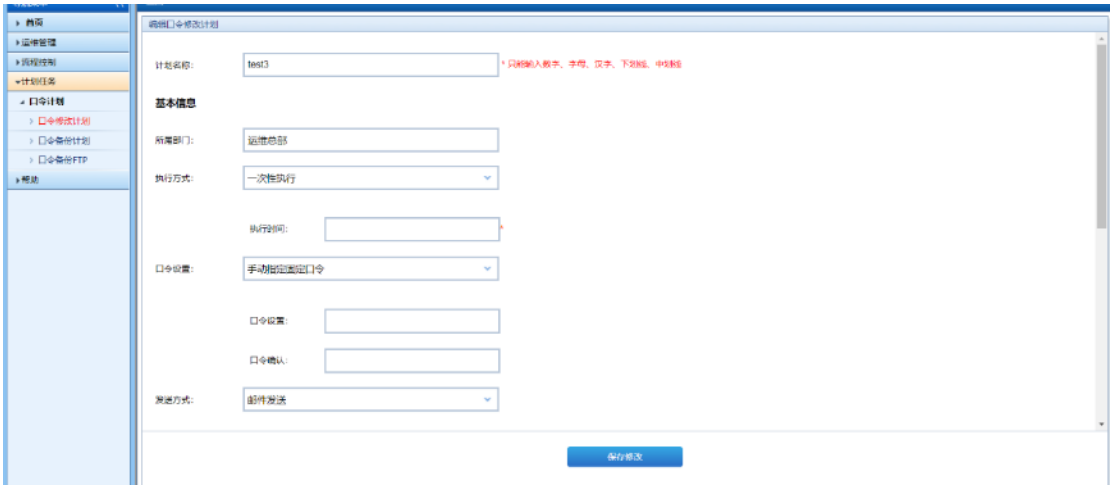


图 3. 13. 1. 3. 3-1

口令修改计划基本信息如下：

1) 计划名称：test3
2) 执行方式：一次性执行
3) 开始时间：今天
4) 口令设置：通过密码表生成
5) 口令表中添加的口令有 admin@1234 和 admin@12345
6) 发送方式：邮件发送
7) 添加需要改密的资源账号、资源或资源组

图 3. 13. 1. 3. 3-2

点击保存，提示保存成功！

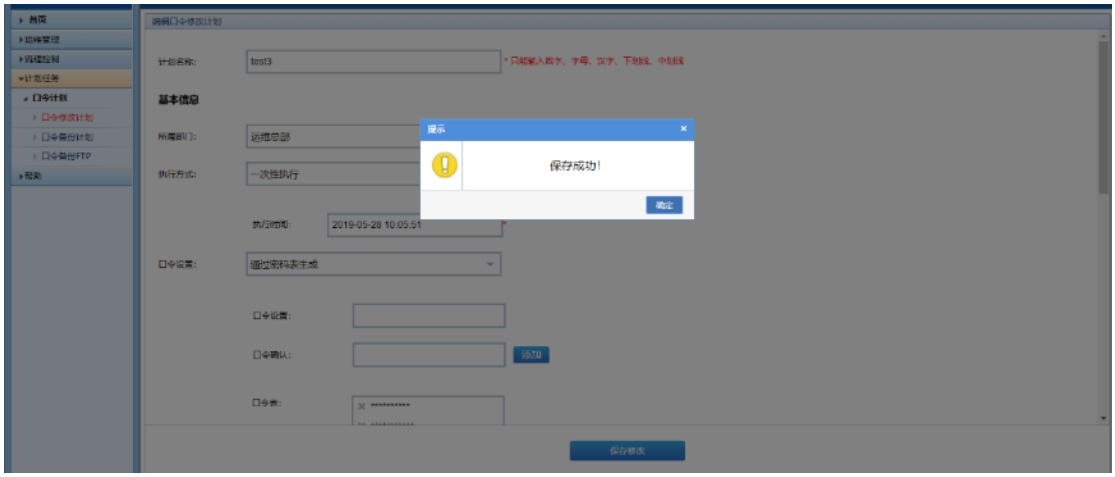


图 3.13.1.3.3-3

点击确定，返回列表页，列表中多出名称为 test3 的口令修改计划。

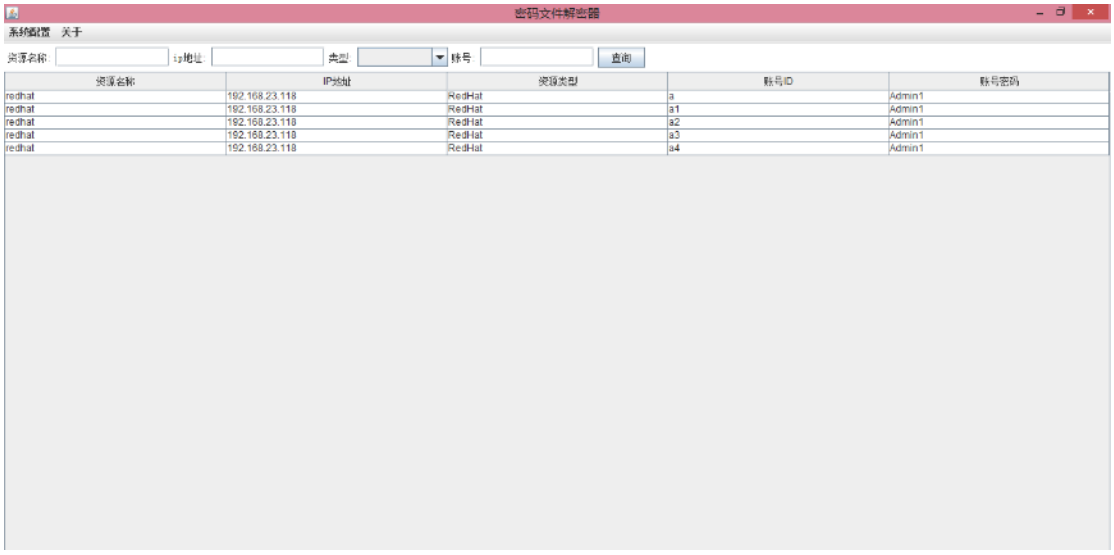
图 3.13.1.3.3-4

点击立即修改，开始改密。

图 3.13.1.3.3-5

点击日志，可查看具体的改密过程中的情况。

改密完成后，将邮箱里接收的密码包和解密密钥用解密器进行解密。

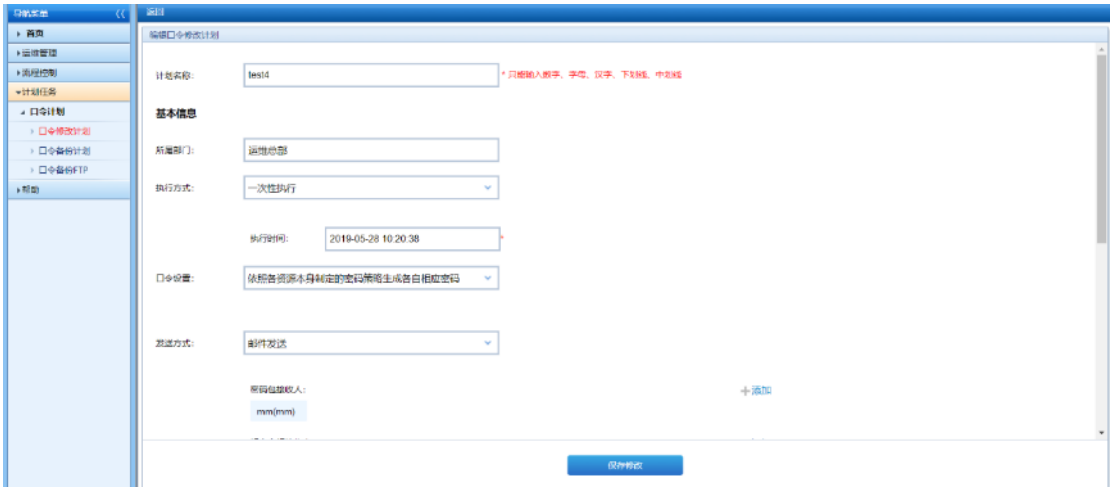


4.口令设置-依照各资源本身制定的密码策略生成各自相应密码

依照各资源本身制定的密码策略生成各自相应的密码是指根据资源本身绑定的密码策略进行改密操作。（没有绑定密码策略则使用系统默认的密码策略进行改密，默认策略为字符 32 位，包含字母，数字，特殊符号）。

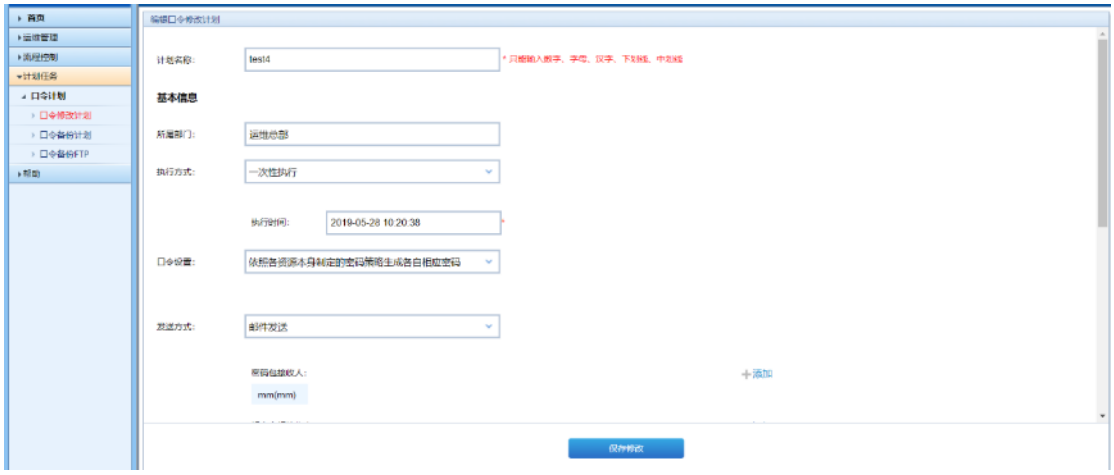
具体操作如下：

点击添加，跳转到口令修改计划编辑页面。

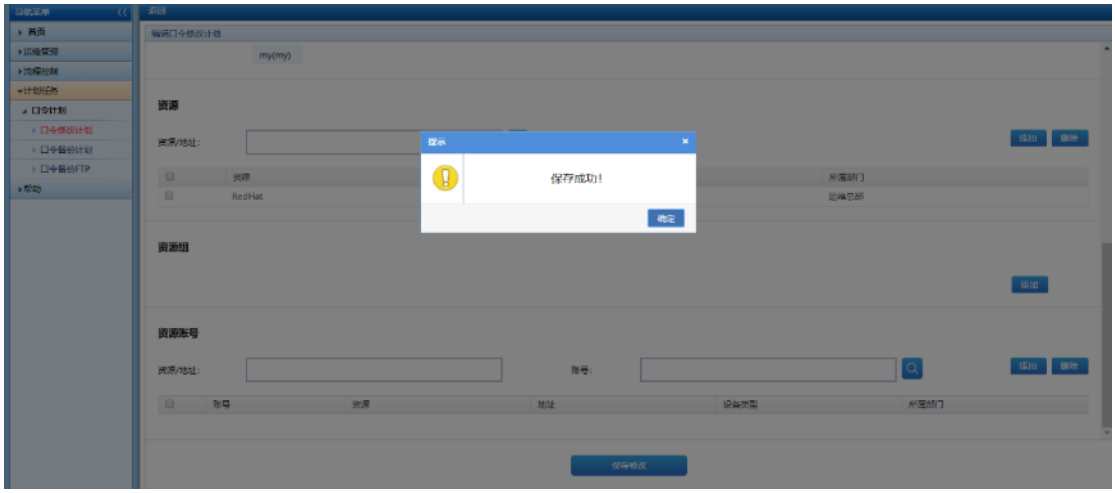


口令修改计划基本信息如下：

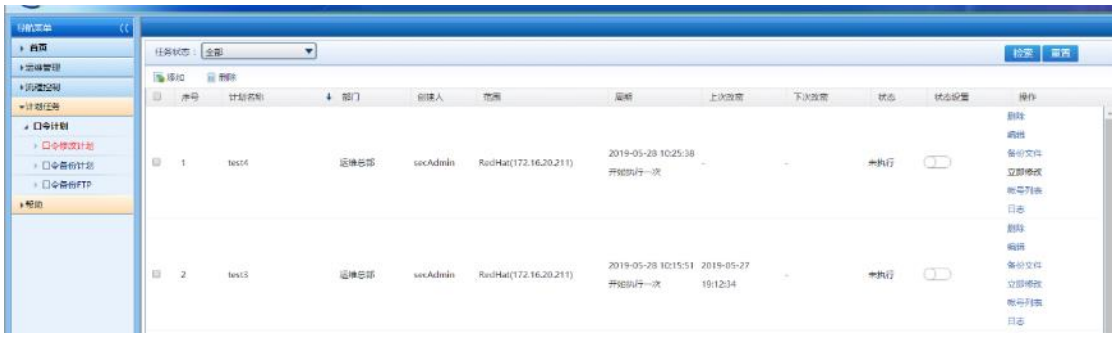
1) 计划名称：test4
2) 执行方式：一次性执行
3) 开始时间：今天
4) 口令设置：依照各资源本身制定的密码策略生成各自相应的密码
5) 发送方式：邮件发送
6) 添加需要改密的资源账号、资源或资源组



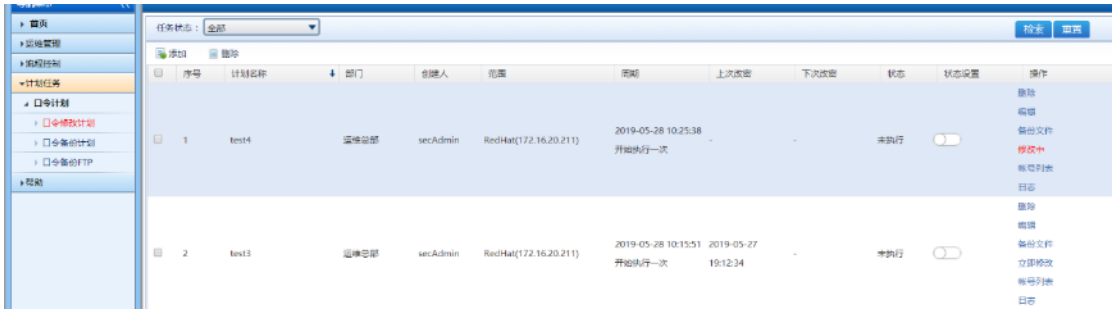
点击保存，提示保存成功！



点击确定，返回列表页，列表中显示名称为 test4 的口令修改计划。

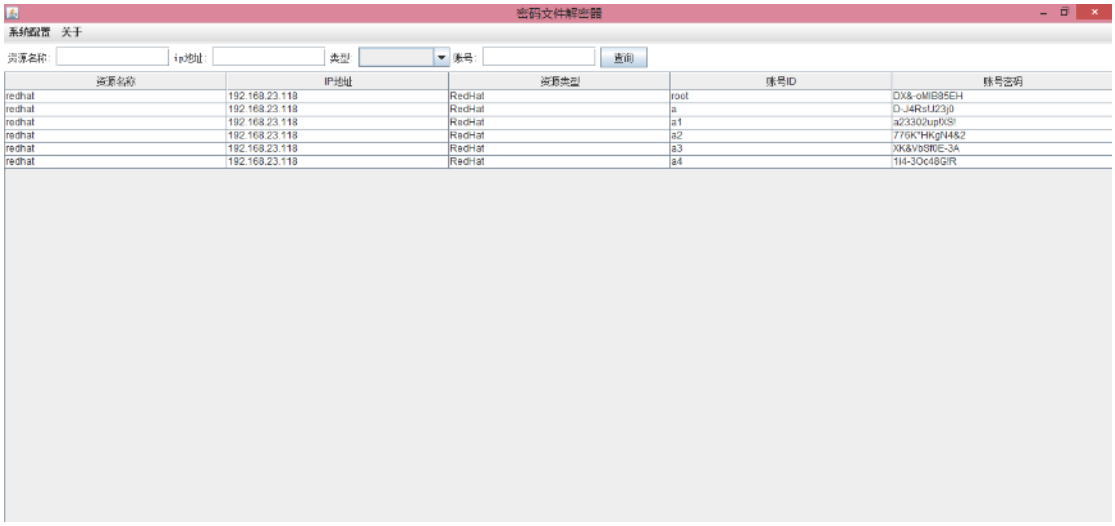


点击立即修改，开始改密。



点击日志，可查看具体的改密过程中的情况。

改密完成后，将邮箱里接收的密码包和解密密钥用解密器进行解密。

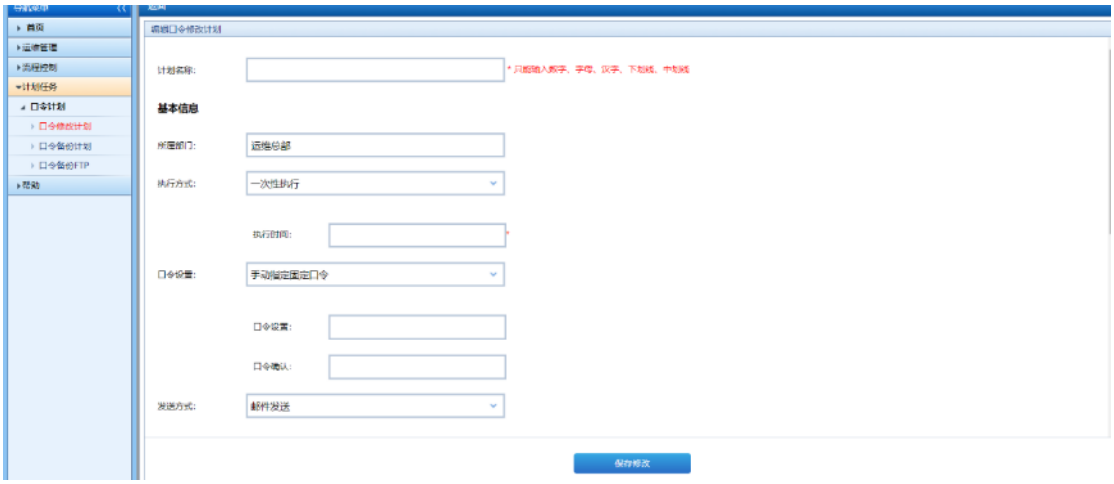


5.口令设置-选取一种密码策略生成同一个密码

选取一种密码策略生成同一个密码是指选取一种密码策略，通过该密码策略生成一个密码，改密计划按照生成的密码进行改密。

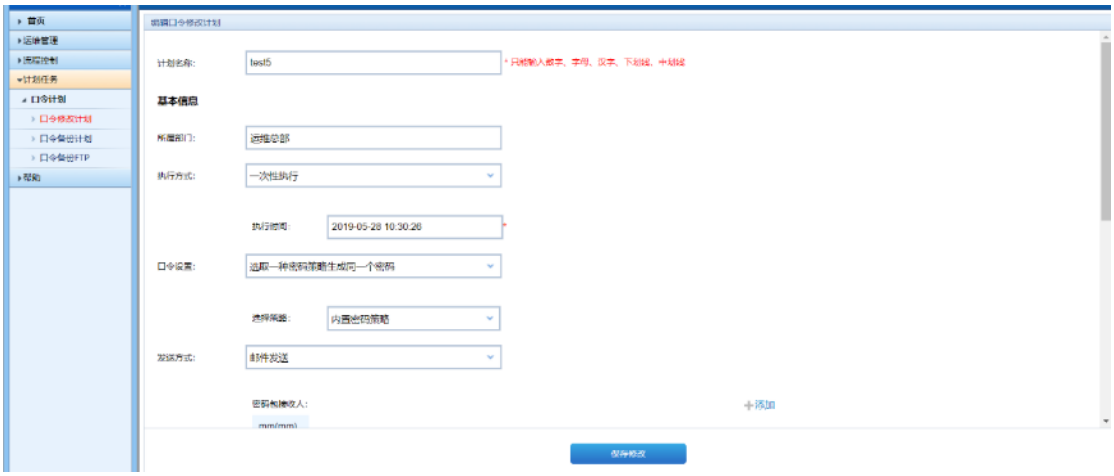
具体操作如下：

点击添加，跳转到口令修改计划编辑页面。

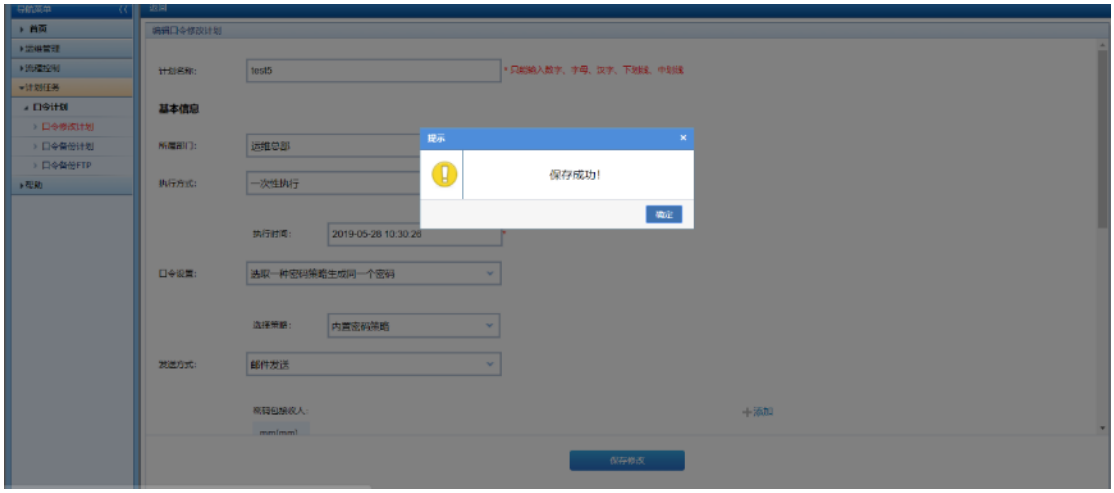


口令修改计划基本信息如下：

1) 计划名称：test5
2) 执行方式：一次性执行
3) 开始时间：今天
4) 口令设置：选取一种密码策略生成同一个密码
5) 选择密码策略
6) 发送方式：邮件发送
7) 添加需要改密的资源账号、资源或资源组

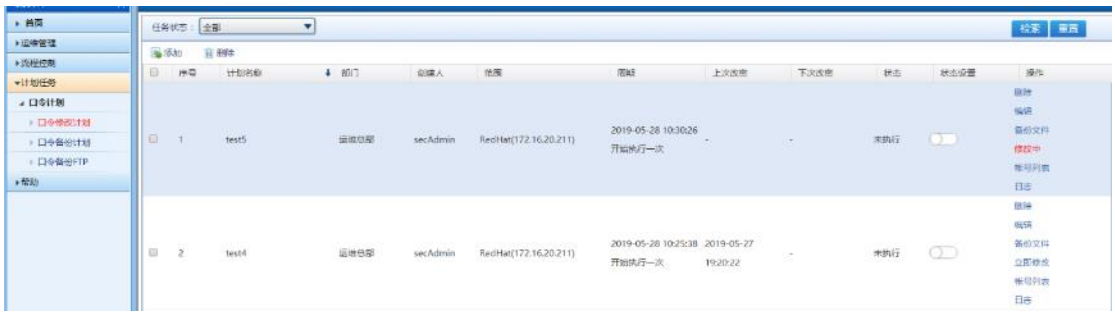


点击保存，提示保存成功！



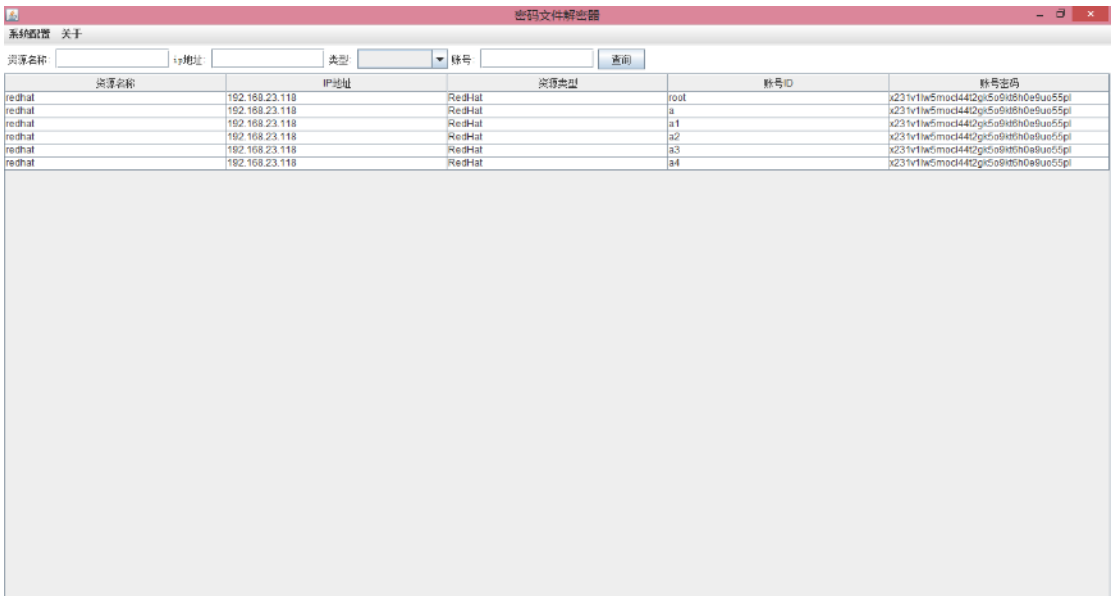
点击确定，返回列表页，列表中显示名称为 test5 的口令修改计划。

点击立即修改，开始改密。



点击日志，可查看具体的改密过程中的情况。

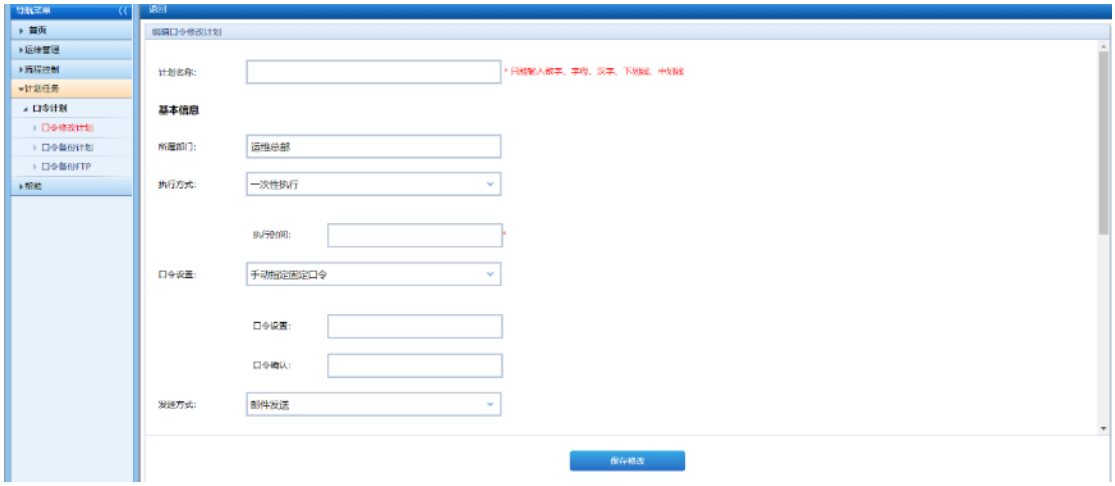
改密完成后，将邮箱里接收的密码包和解密密钥用解密器进行解密。



6.发送方式-不发送

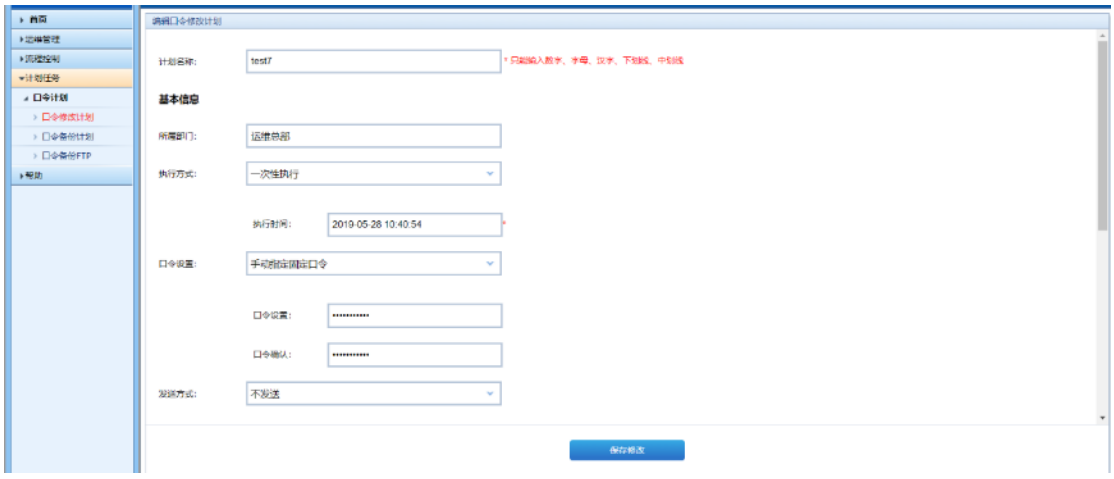
当发送方式设定为不发送，默认将解密密钥发送给拥有解密密钥接收人角色权限的用户（该用户需配有邮件地址）。

点击添加，跳转到口令修改计划编辑页面。

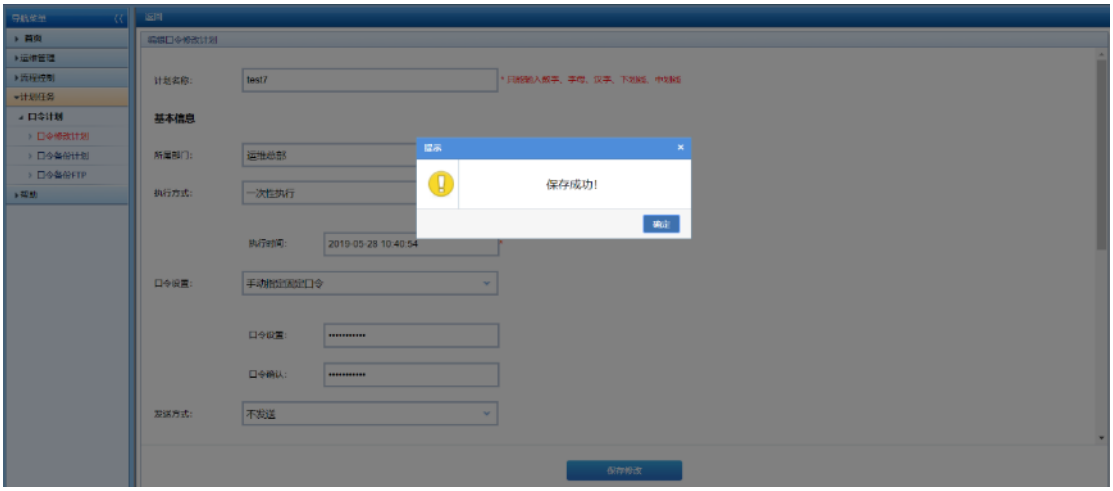


口令修改计划的基本信息如下：

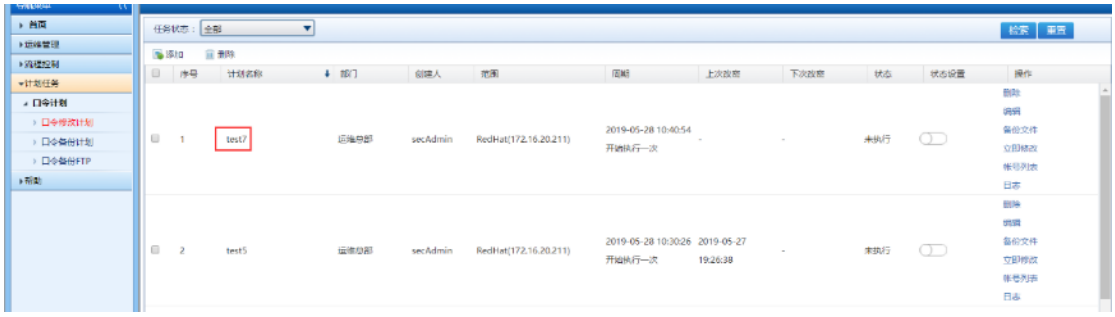
1) 计划名称：test7
2) 执行方式：一次性执行
3) 开始时间：今天
4) 口令设置 admin@1234,口令确认 admin@1234
5) 发送方式：不发送
6) 添加需要改密的资源账号、资源或资源组



点击保存，提示保存成功！

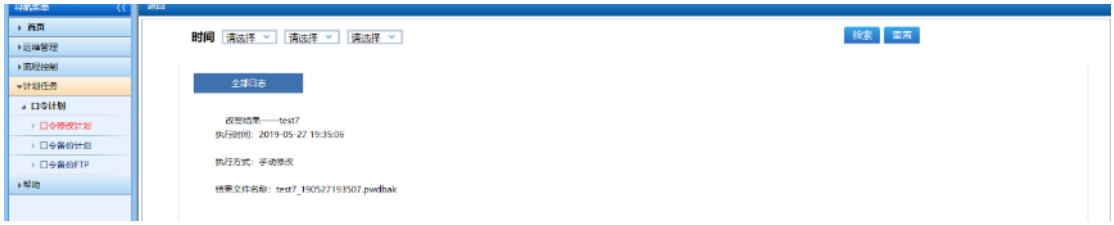


点击确定，返回列表页，列表中显示名称为 test7 的口令修改计划。



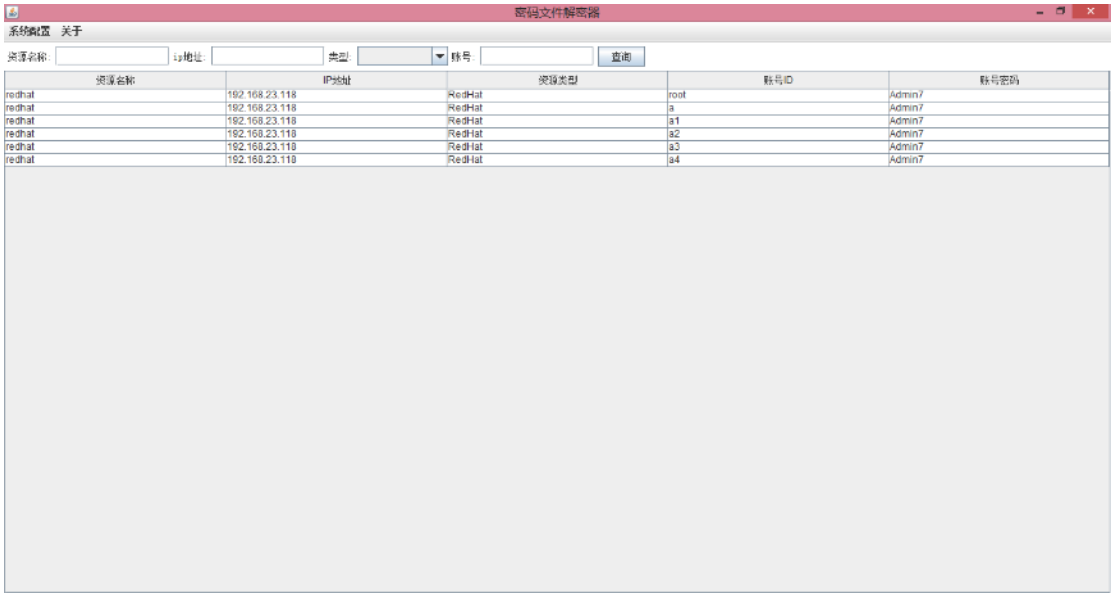
点击立即修改，开始改密。

点击日志，可查看具体的改密过程中的情况。



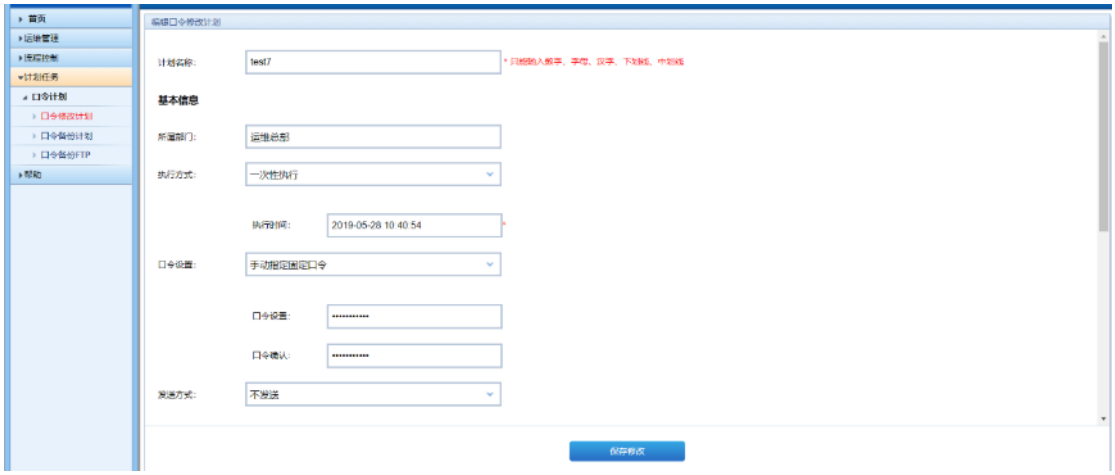
改密完成后，密码包接收人mm登录系统，密码包可在口令修改计划操作栏下备份文件中下载，拥有解密密钥接收人角色权限的用户可在邮箱查看解密密钥。

使用解密器解密。

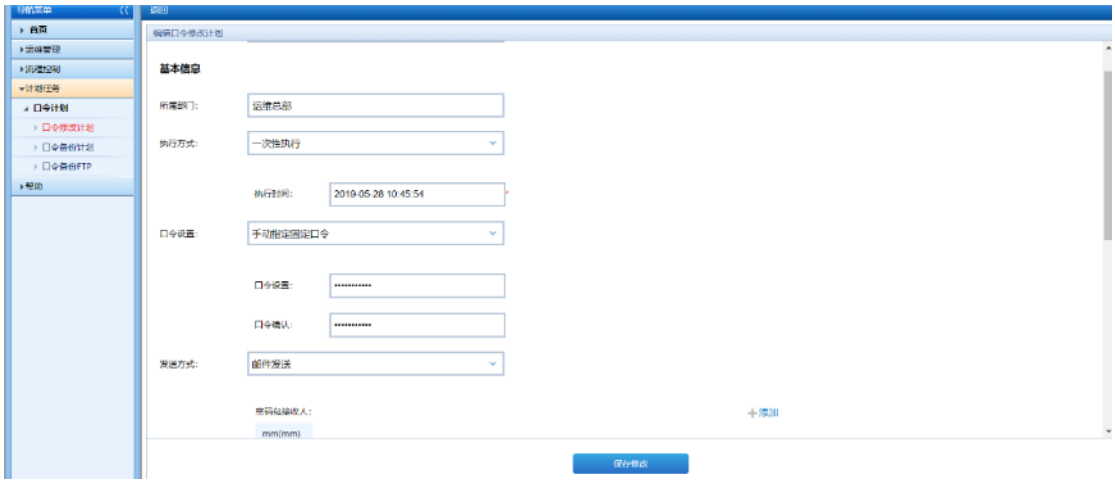


12.1.4. 编辑口令修改计划

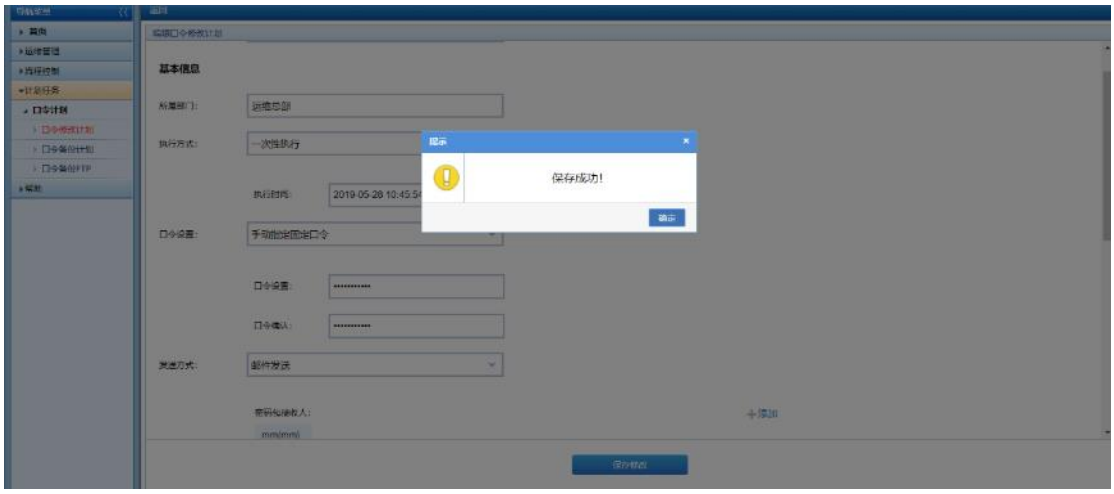
在 test7 后点击编辑，跳转到口令修改计划编辑页面。



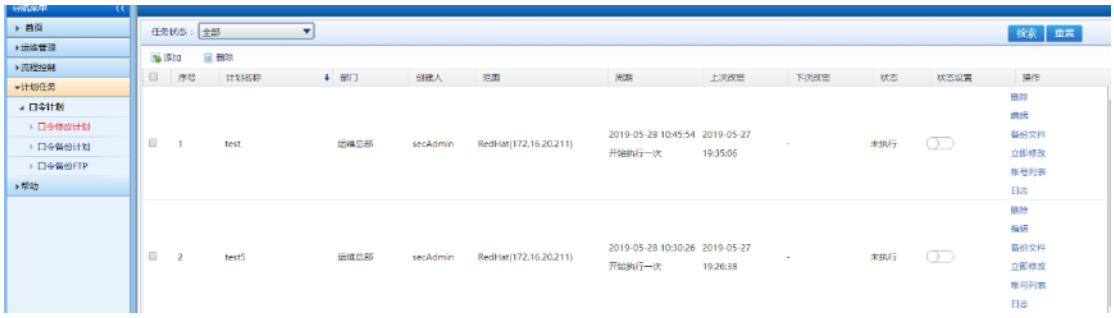
名称修改为 test，执行时间选择今天，发送方式修改为邮件发送。



点击保存，提示保存成功！

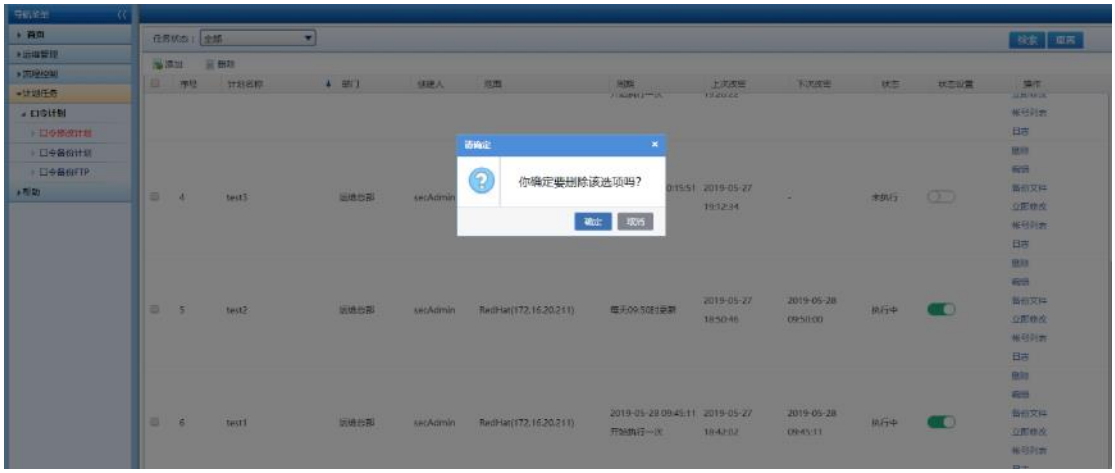


点击确定，返回列表页，列表中名称为 test7 的口令修改计划改为名称为 test。

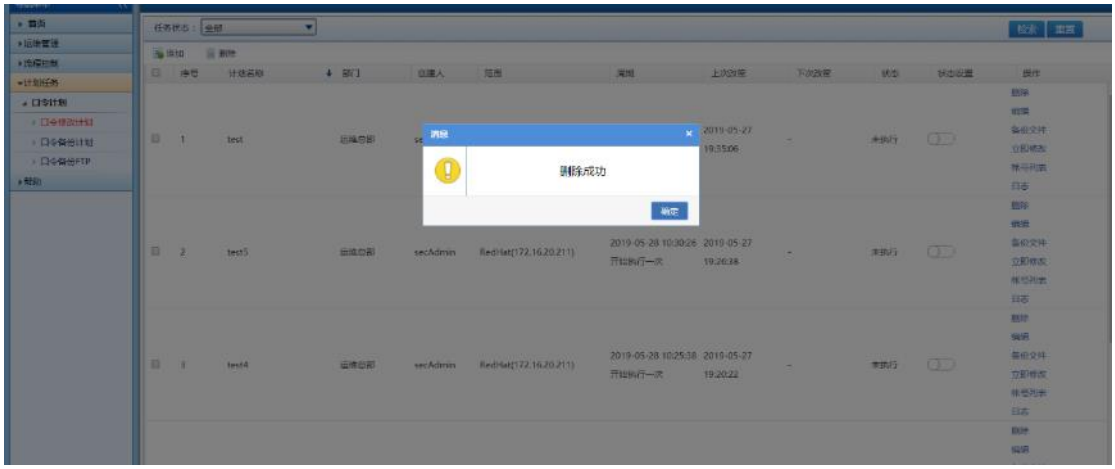


12.1.5. 删除口令修改计划

在 test1 后点击删除，提示你确定要删除该选项吗？



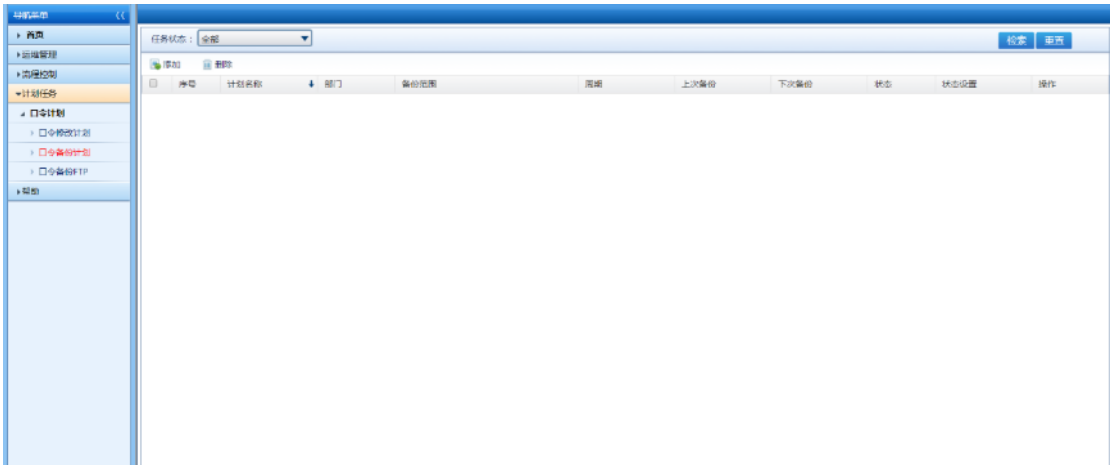
点击确定，提示删除成功。



口令修改计划列表页不存在计划名称为 test1 的口令修改计划。

12.2. 口令备份计划

用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令备份计划链接进入口令备份计划界面。



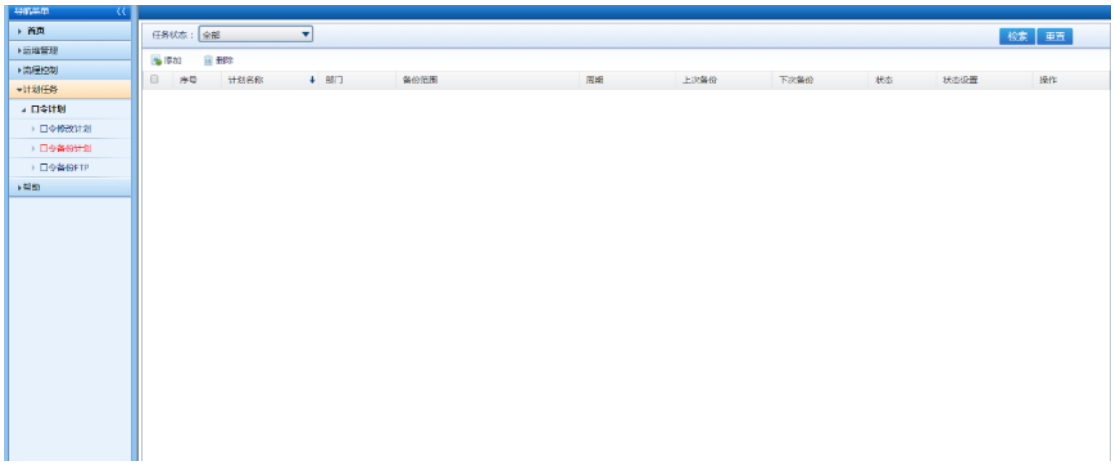
12.2.1. 添加并执行口令备份计划

1.定时执行-一次性备份

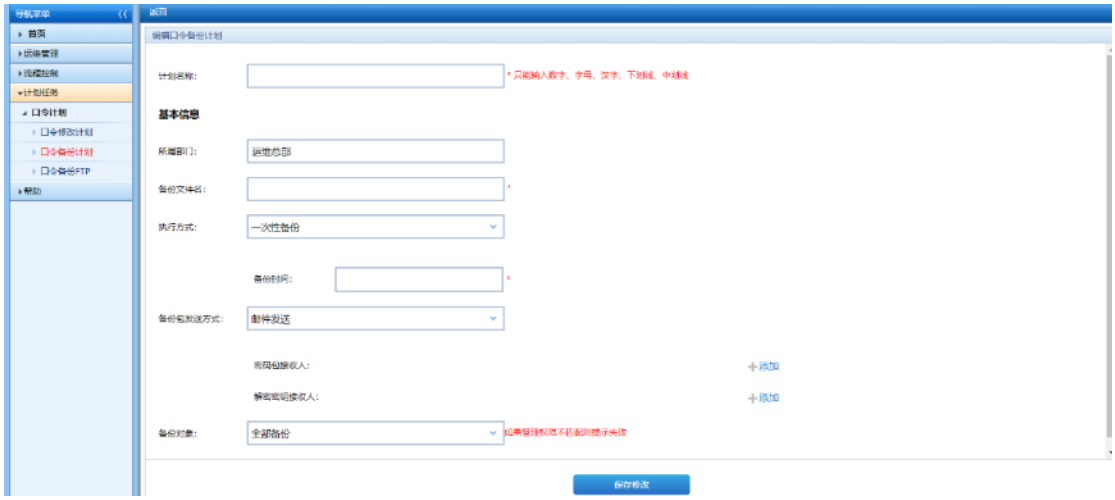
一次性执行是指口令备份计划到达设定时间后开始执行备份计划且只执行一次。

具体操作如下：

用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令备份计划链接进入口令备份计划界面。

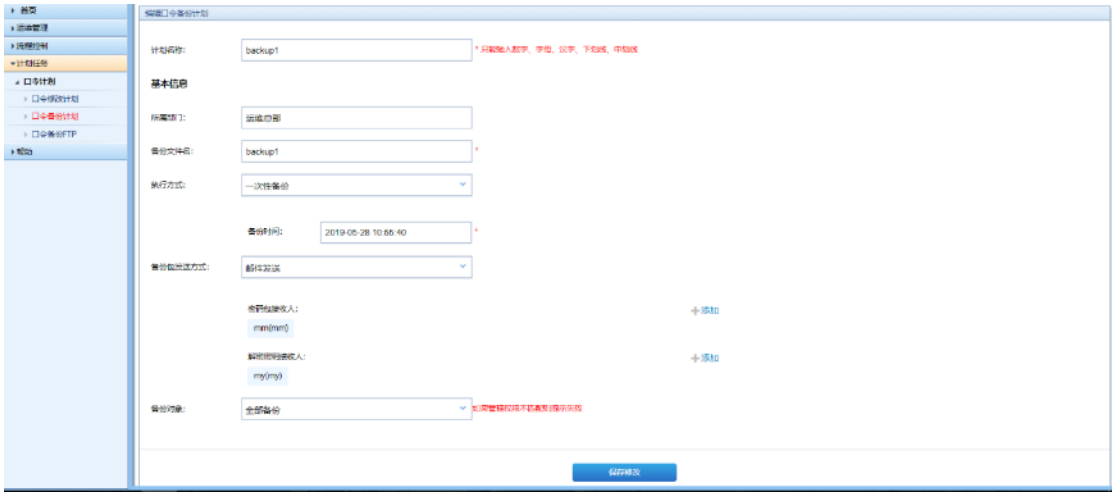


点击添加，跳转到口令备份计划编辑页面。

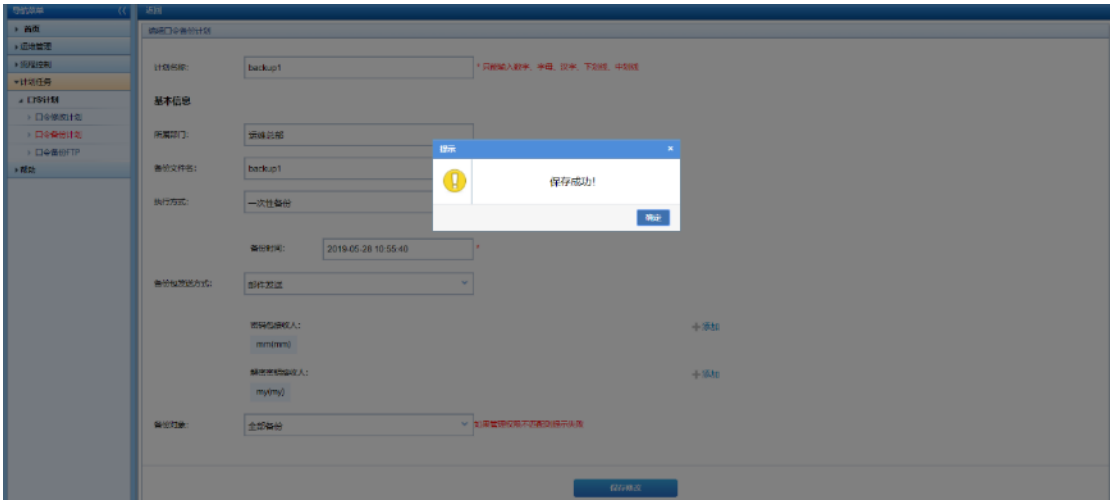


口令备份计划基本信息如下：

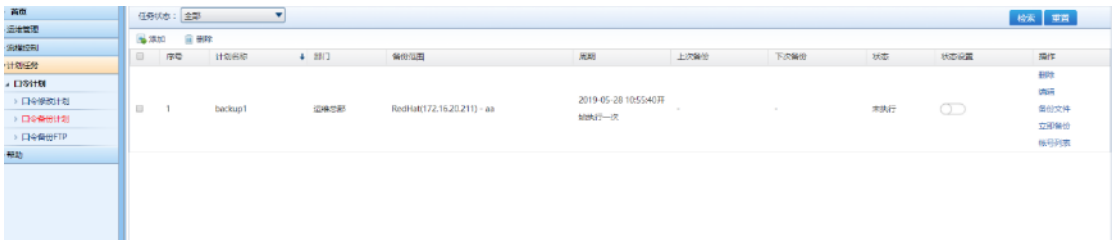
1) 计划名称：backup1
2) 备份文件名称：backup1
3) 执行方式：一次性备份
4) 备份时间：今天
5) 备份包发送方式：邮件发送
6) 备份对象：全部备份



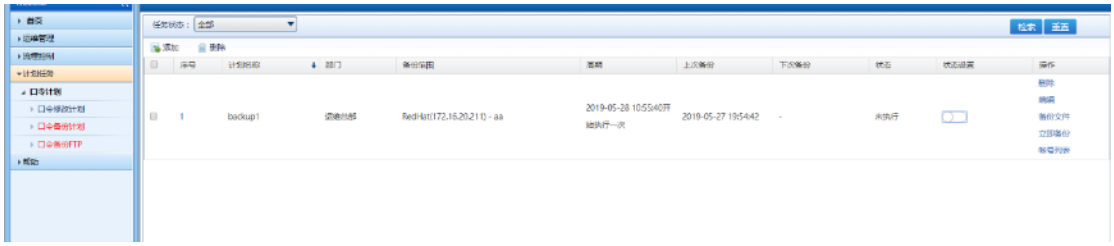
点击保存，提示保存成功！



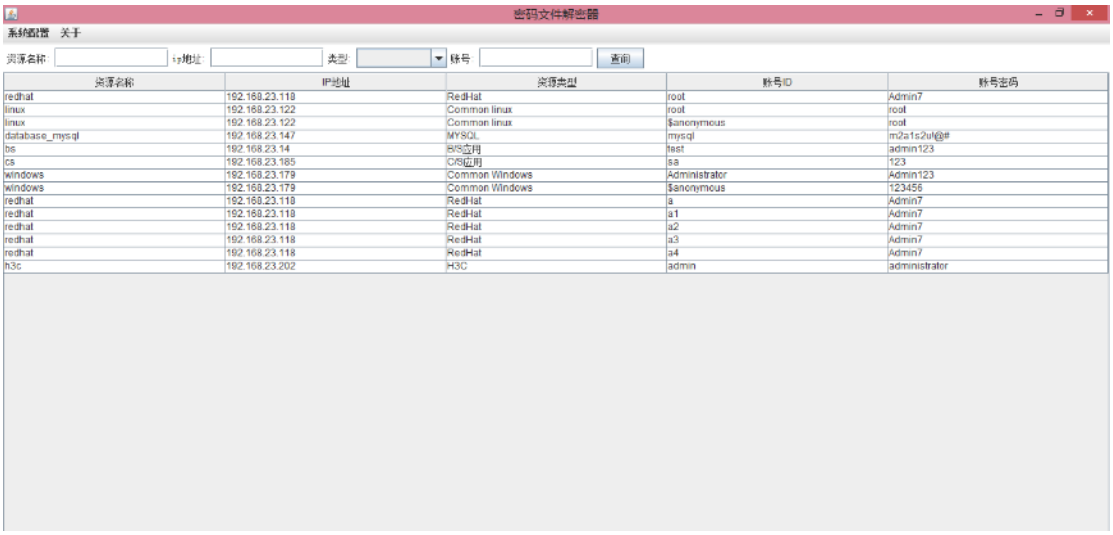
点击确定，返回列表页，列表中显示名称为 backup1 的口令备份计划。



状态设置为开，定时开启，到达设定时间开始备份。



备份完成后，将密码包接收人邮箱里接收的密码包和解密密钥接收人邮箱里接收的解密密钥用解密器进行解密，解密后可查看资源账号及密码。

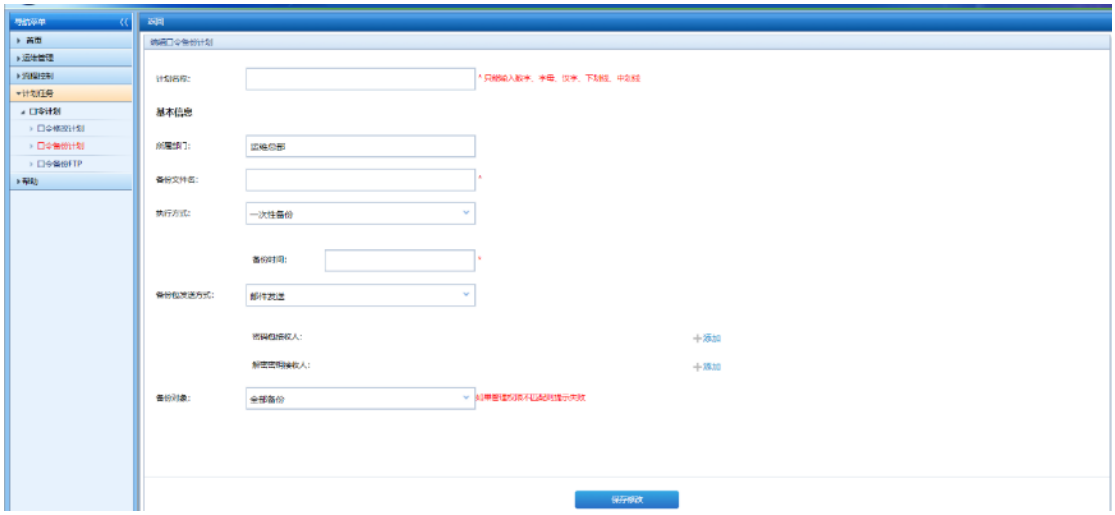


2.定时执行-周期备份

周期性备份是指口令备份计划在一定时间范围内定期执行备份操作。

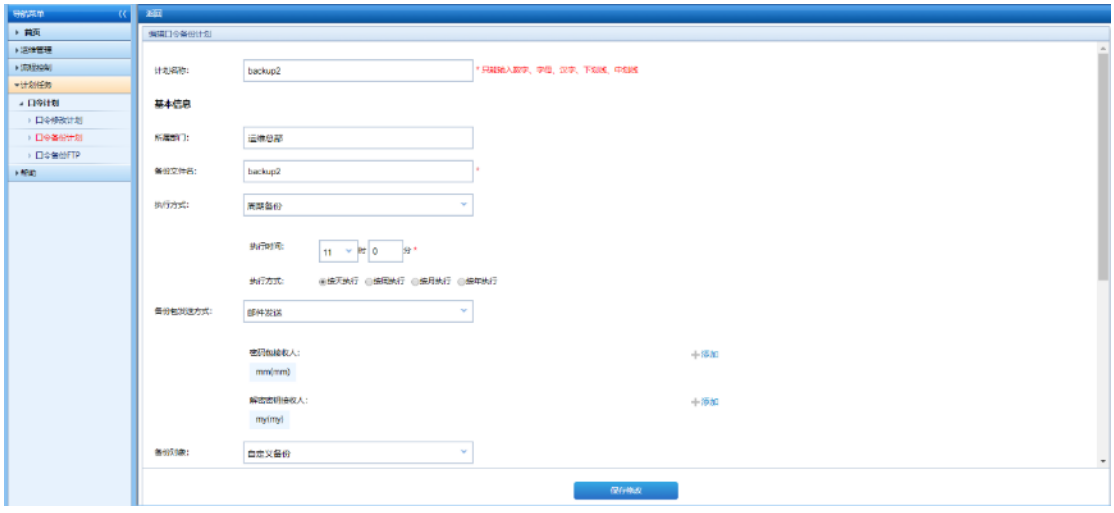
具体操作如下：

点击添加，跳转到口令备份计划编辑页面。

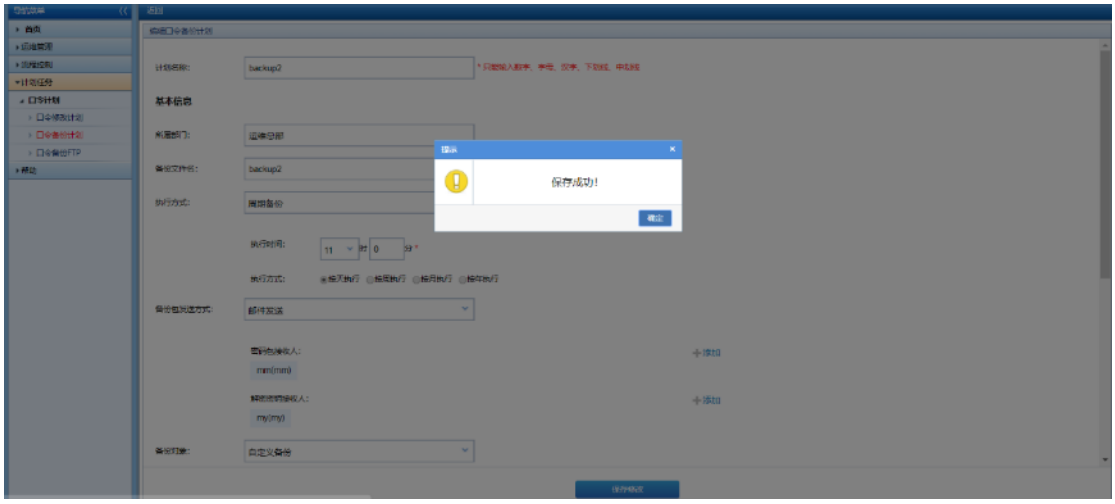


口令备份计划基本信息如下：

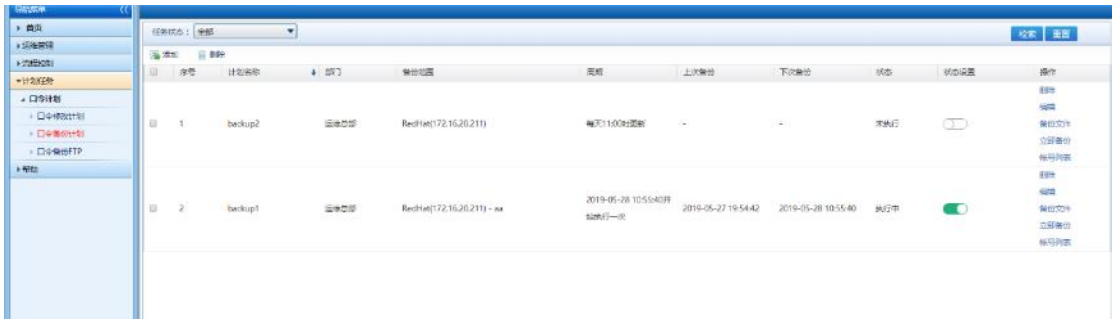
1) 计划名称：backup2
2) 备份文件名称：backup2
3) 执行方式：周期备份
4) 执行时间：17 时 19 分
5) 执行方式：按天执行
6) 发送方式：邮件发送
7) 备份对象：自定义备份，选择需要备份的资源账号



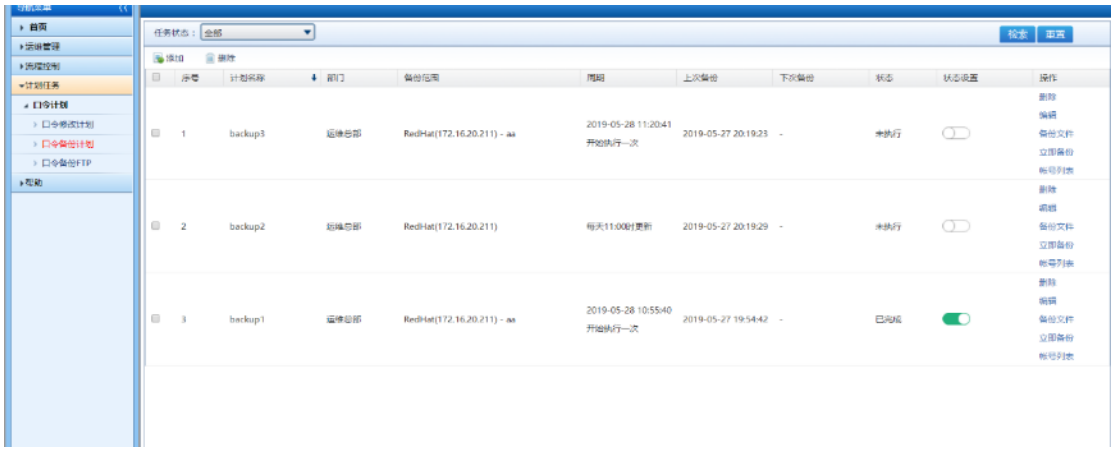
点击保存，提示保存成功！



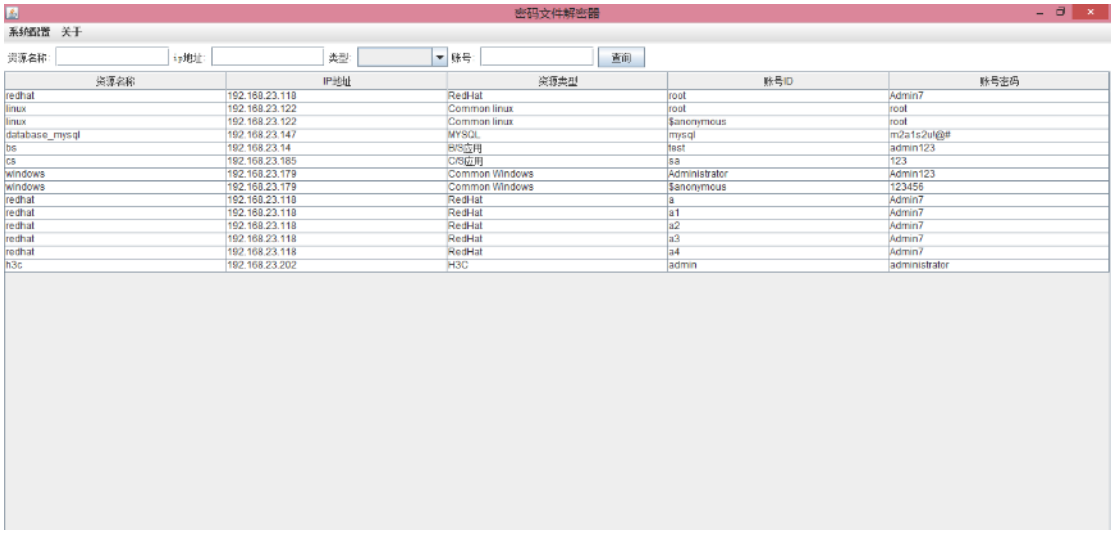
点击确定，返回列表页，列表中显示名称为 backup2 的口令备份计划。



状态设置为开，定时开启，到达设定时间开始备份。



备份完成后，将密码包接收人邮箱里接收的密码包和解密密钥接收人邮箱里接收解密密钥用解密器进行解密，解密后可查看资源账号及密码。



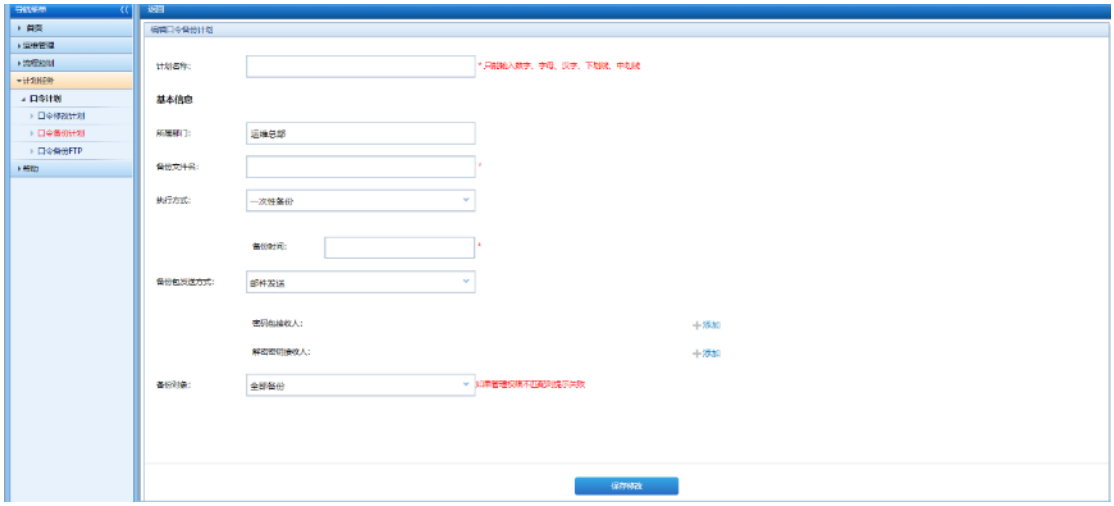
3.备份包发送方式-FTP 发送

FTP 发送是将密码包发送到 FTP 服务器上保存。

具体操作如下：

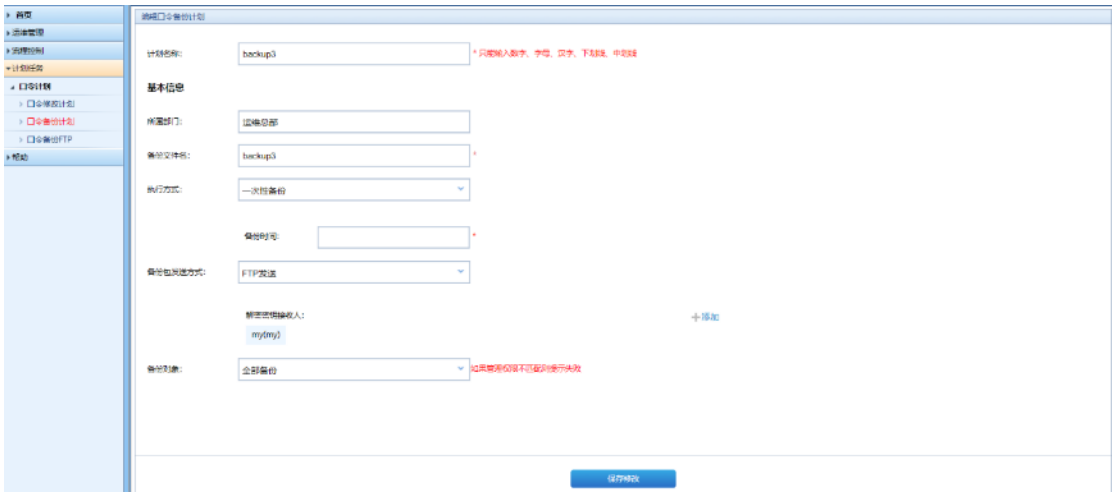
用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令备份计划链接进入口令备份计划界面。

点击添加，跳转到口令备份计划编辑页面。

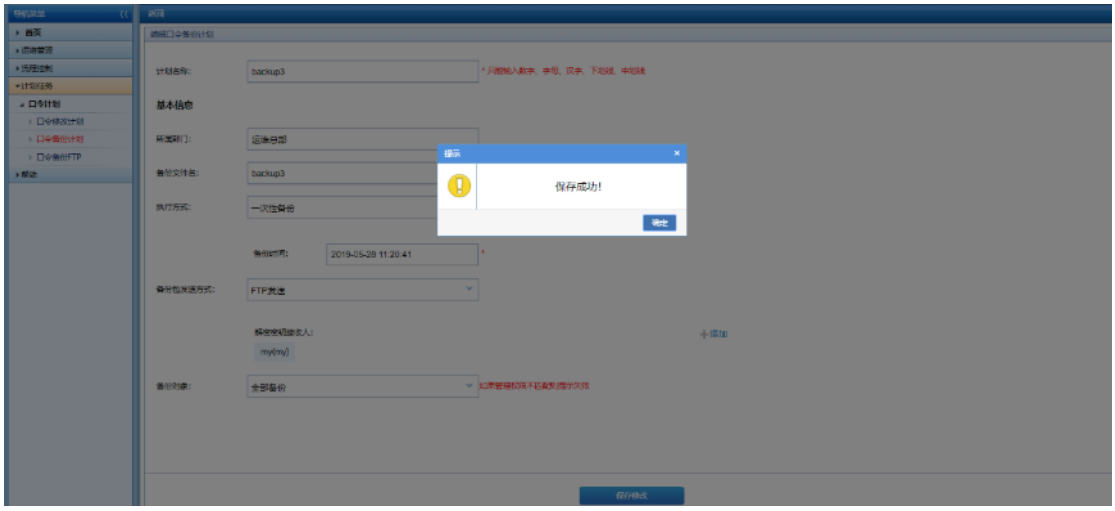


口令备份计划基本信息如下：

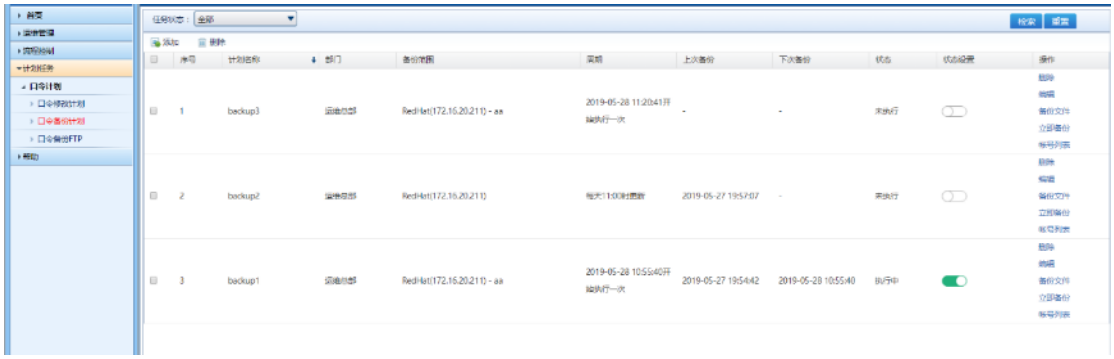
1) 计划名称：backup3
2) 备份文件名称：backup3
3) 执行方式：一次性备份
4) 备份时间：今天
5) 备份包发送方式：FTP 发送
6) 备份对象：全部备份



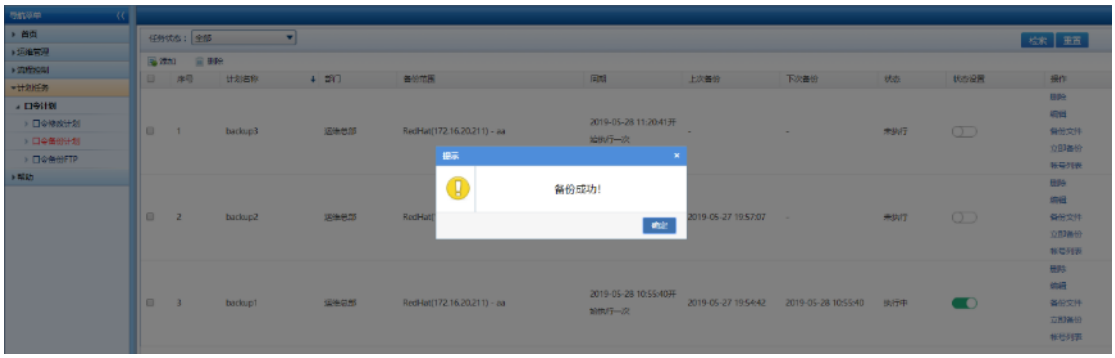
点击保存，提示保存成功！



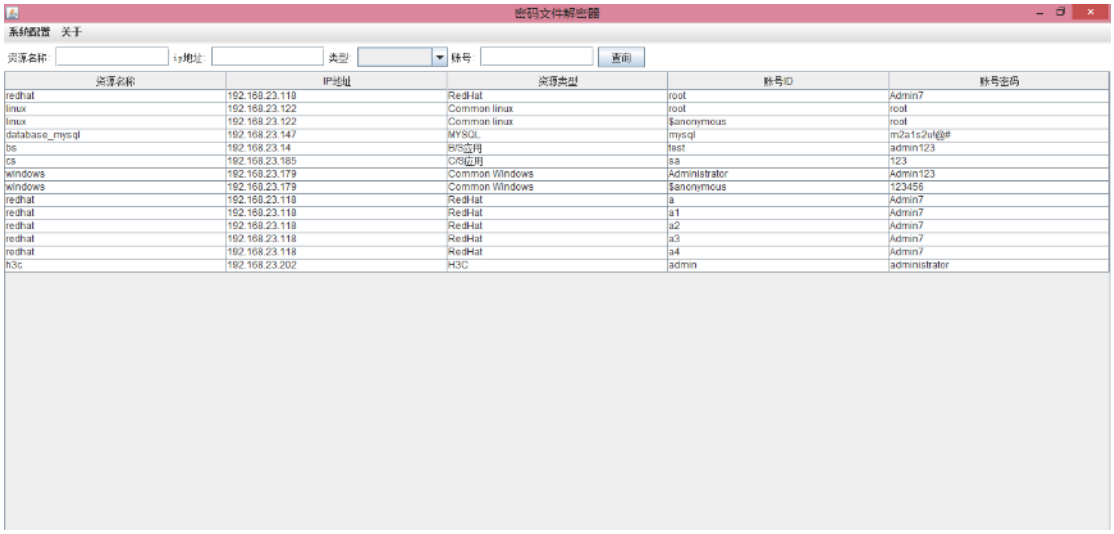
点击确定，返回列表页，列表中显示名称为 backup3 的口令备份计划。



点击立即备份，提示备份成功！



备份完成后，将远程 FTP 服务器上的密码包和解密密钥接收人邮箱里接收的解密密钥用解密器进行解密，解密后可查看资源账号及密码。



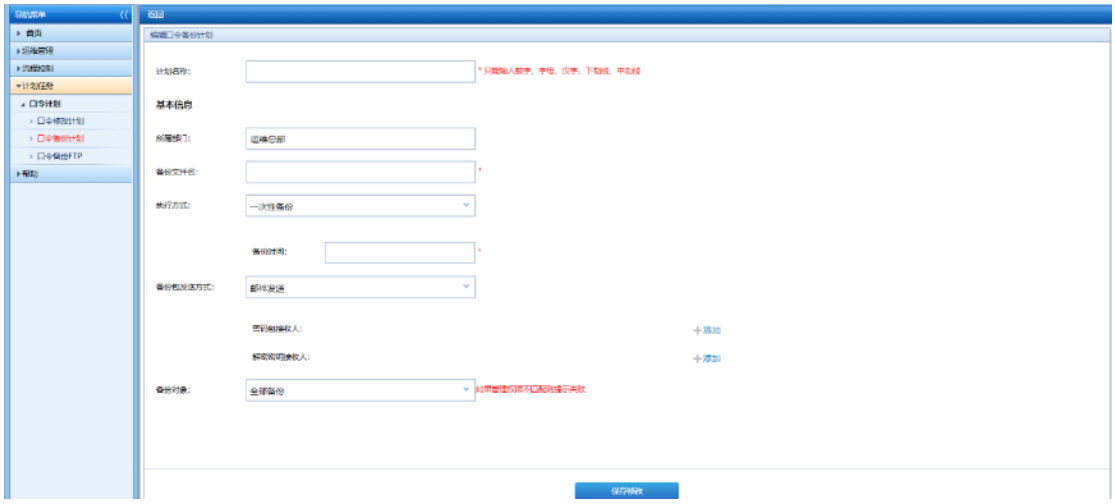
4.备份包发送方式-不发送

当备份包发送方式设定为不发送，默认将解密密钥发送给拥有解密密钥接收人角色权限的用户（该用户需配有邮件地址）。

具体操作如下：

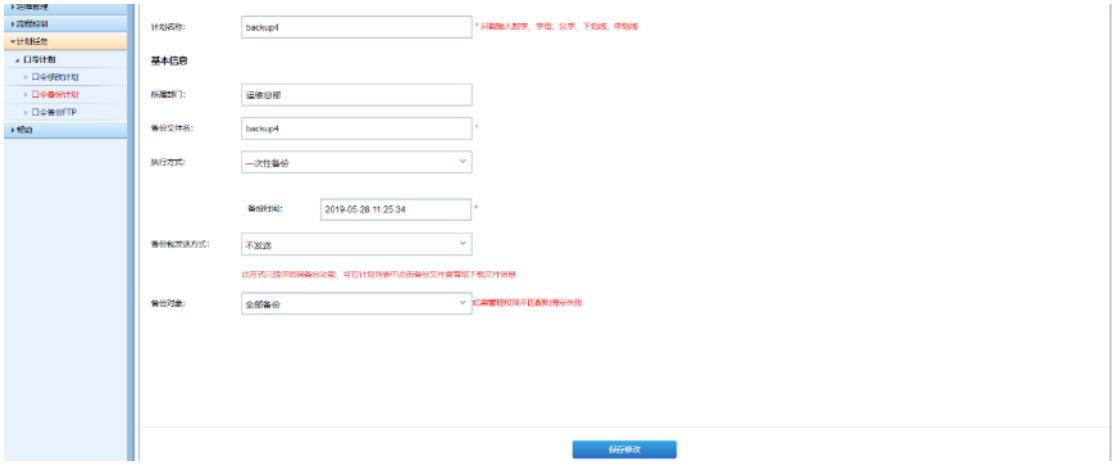
用安全管理员 secAdmin 登陆系统，切换至安全管理员角色，点击计划任务->口令计划->口令备份计划链接进入口令备份计划界面。

点击添加，跳转到口令备份计划编辑页面。

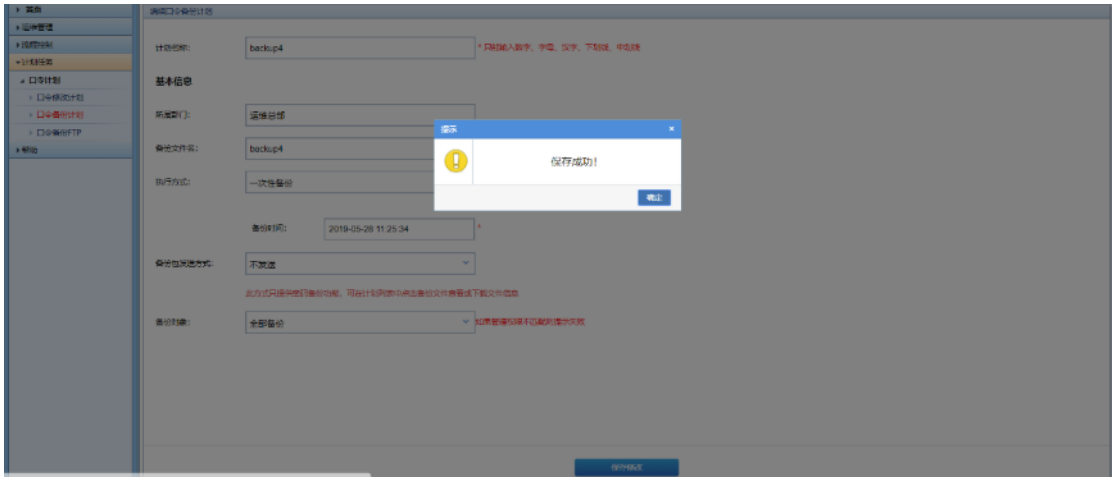


口令备份计划基本信息如下：

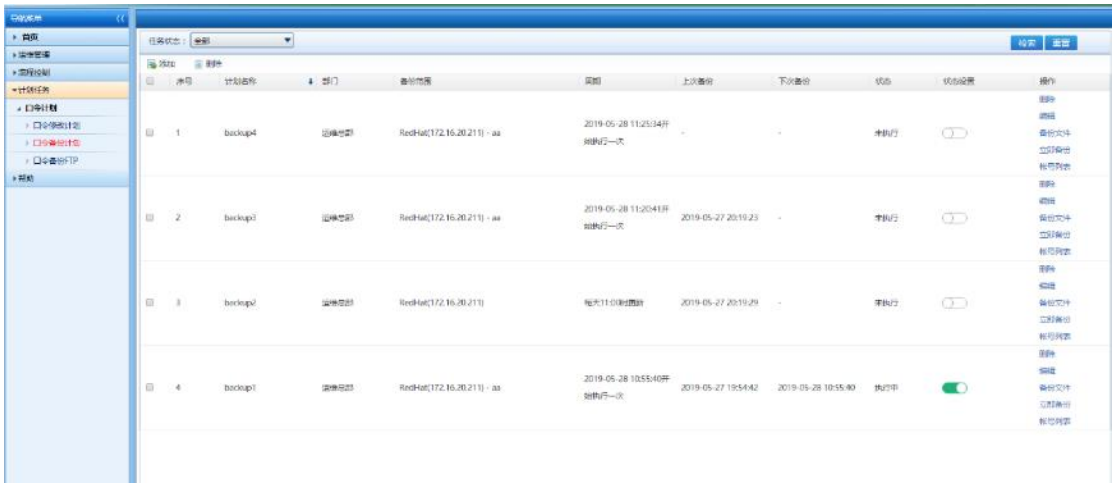
1) 计划名称：backup4
2) 备份文件名称：backup4
3) 执行方式：一次性备份
4) 备份时间：今天
5) 备份包发送方式：不发送
6) 备份对象：全部备份



点击保存，提示保存成功！



点击确定，返回列表页，列表中显示名称为 backup4 的口令备份计划。



点击立即备份，提示备份成功！

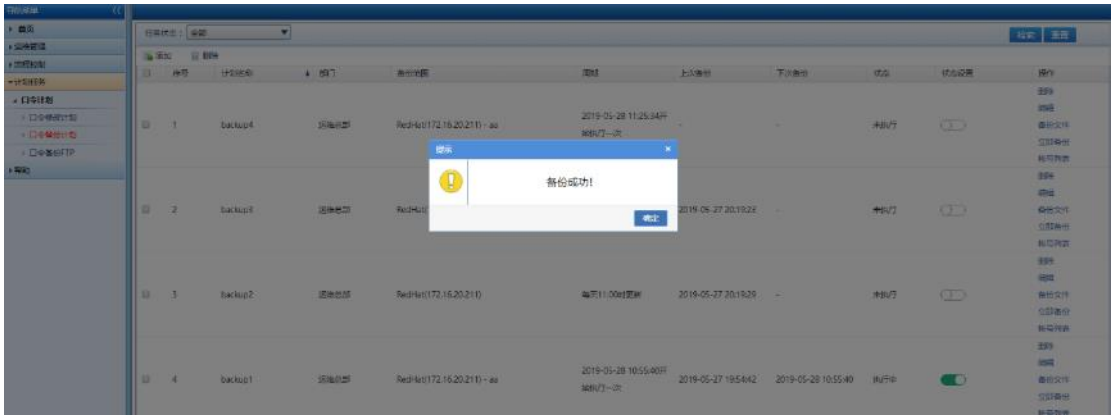
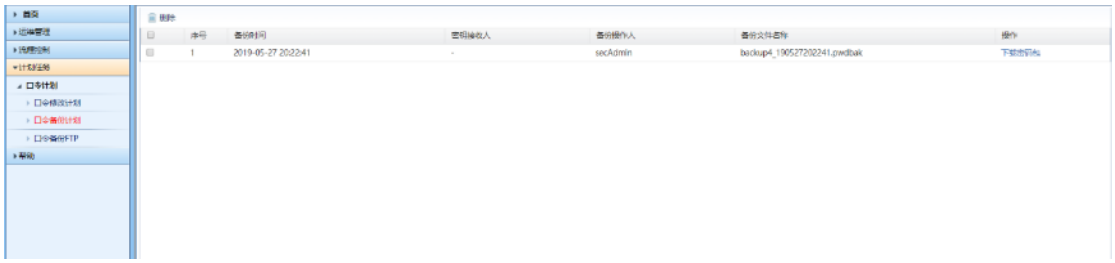
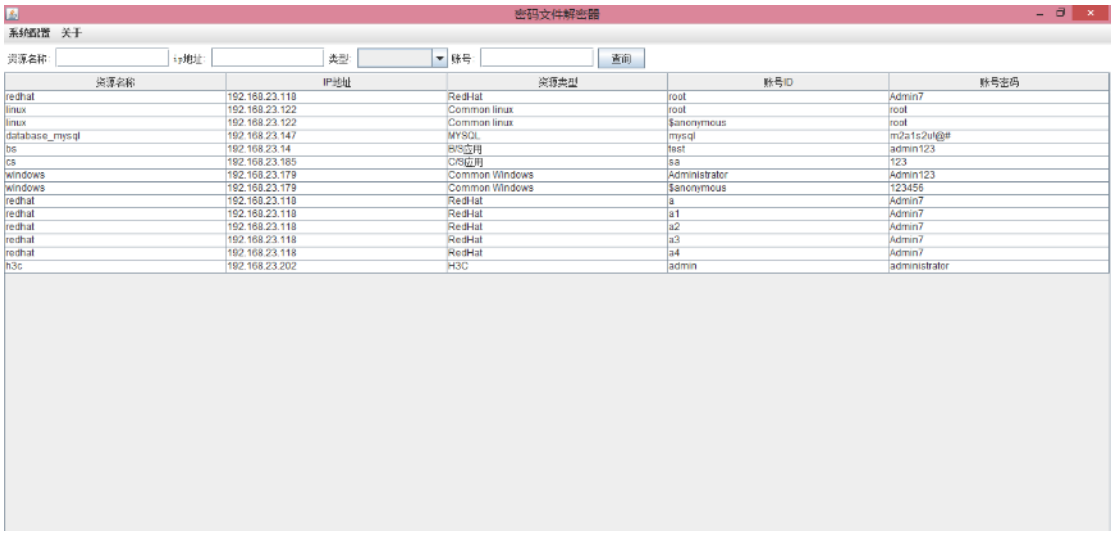


图 3.13.2.1.4-6

在备份文件里可查看生成的密码包。

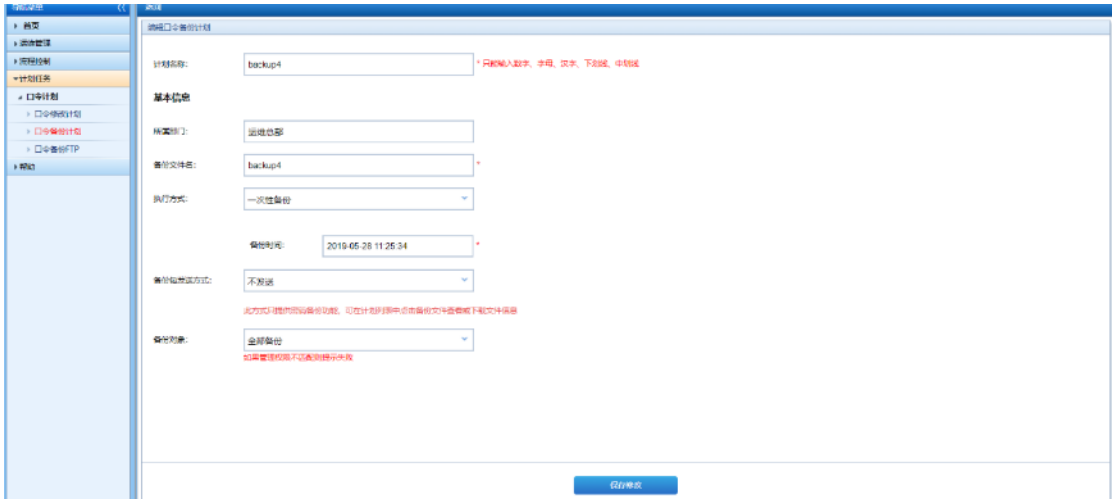


备份完成后，密码包接收人 mm 登录系统，密码包可在口令修改计划操作栏下备份文件中下载的密码包和解密密钥接收人邮箱里接收的解密密钥用解密器进行解密，解密后可查看资源账号及密码。

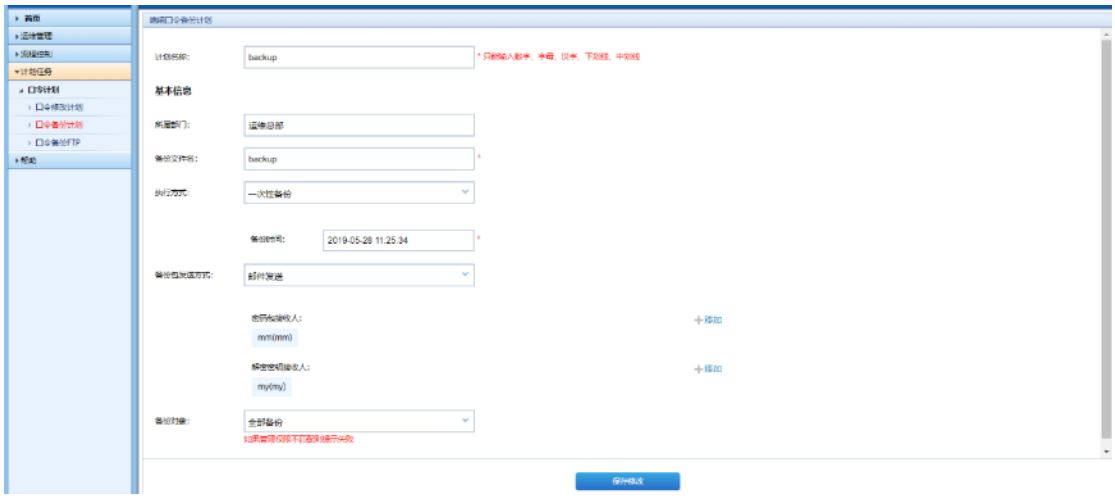


12.2.2. 编辑口令备份计划

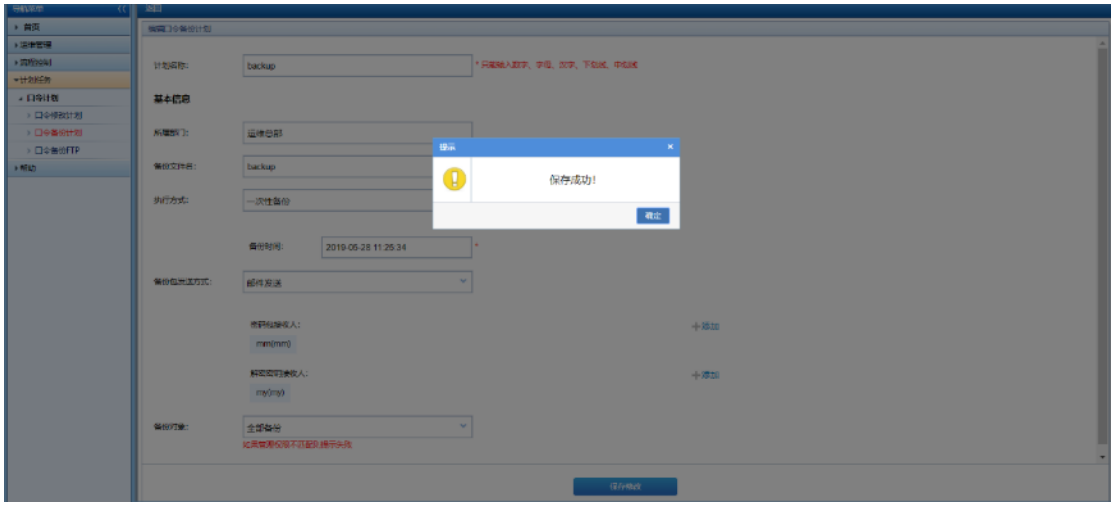
在 backup4 后点击编辑，跳转到口令备份计划编辑页面。



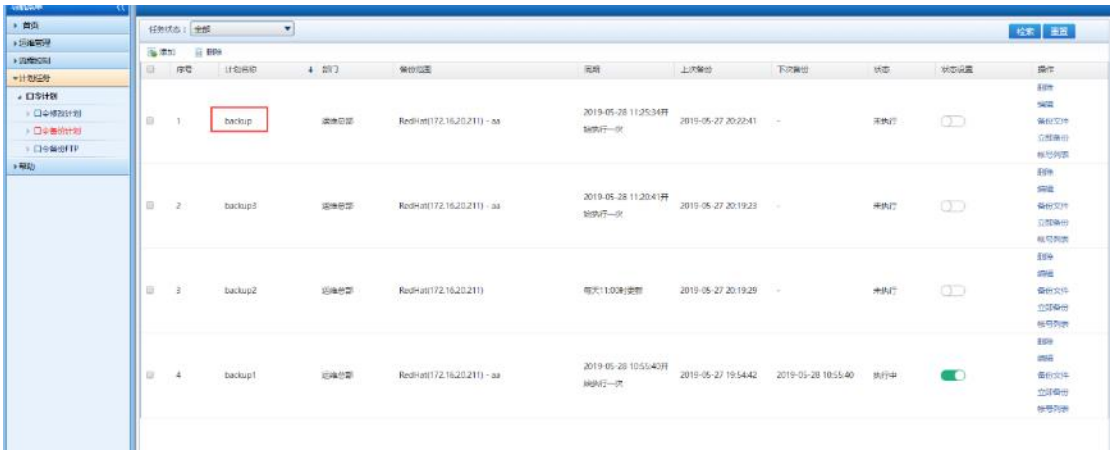
名称修改为 backup，备份时间选择今天，发送方式修改为邮件发送。



点击保存，提示保存成功！

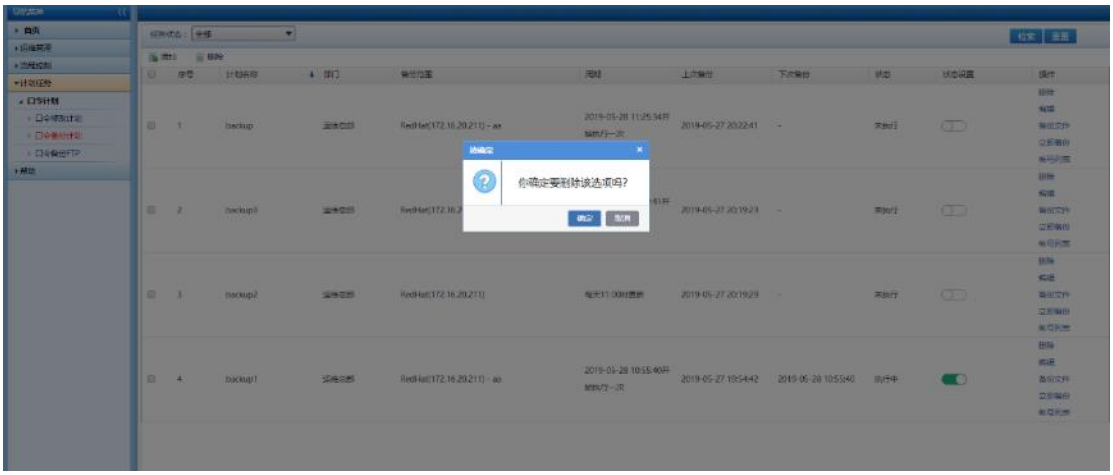


点击确定，返回列表页，列表中名称为 backup4 的口令备份计划名称改为 backup。

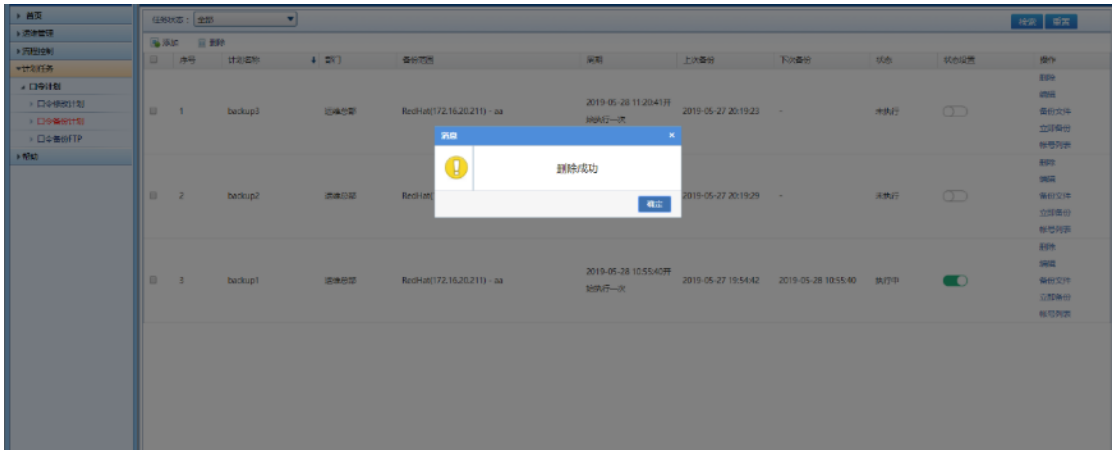


12.2.3. 删除口令备份计划

在 backup 后点击删除，提示你确定要删除该选项吗？



点击确定，提示删除成功。



口令备份计划列表页不存在计划名称为 backup 的口令备份计划。

12.3. 口令备份 FTP

点击计划任务 ->口令备份 FTP 链接进入口令备份 FTP 界面，配置 FTP 服务器的基本信息。

13. 审计报表

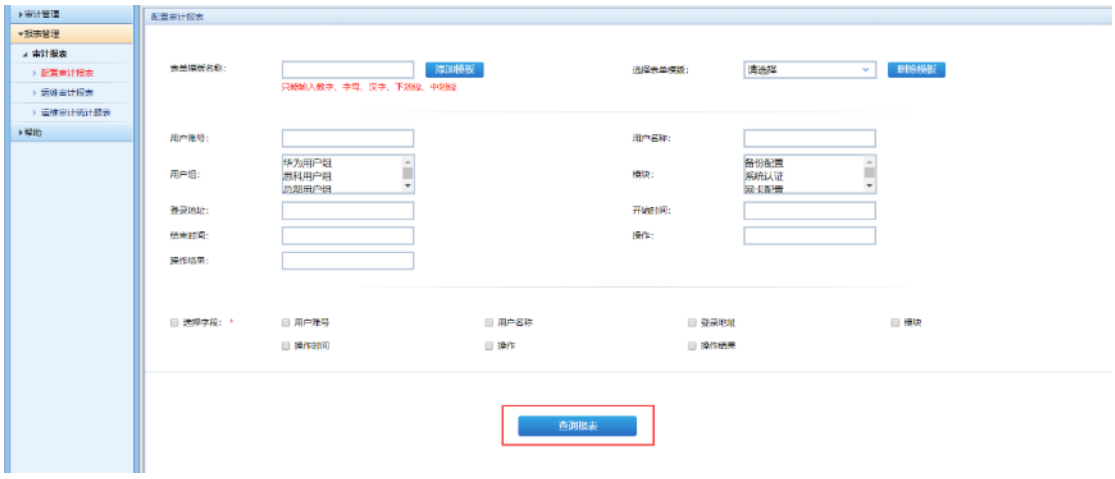
审计报表将运维操作过程生成的记录以报表形式展现。

13.1. 配置审计报表

13.1.1. 直接生成审计报表

审计管理员 sysAudit 登录，切换至审计管理员角色，点击报表管理 ->审计报表->配置审计报表链接，进入配置报表审计界面。

选择所需查询的字段，点击查询报表。



查询结果：用户访问次数以折线图形式展现，用户操作的详细信息以报表格式展现。

图

序号	用户账号	用户名称	登录地址	模块	操作时间	操作动作	操作结果
1	admin	初始化用户	10.251.251.55	备份配置	2019-01-21 1…	恢复出厂设置	操作成功
2	admin	初始化用户	10.251.251.55	系统认证	2019-01-21 1…	退出	操作成功
3	admin	初始化用户	10.251.251.120	系统认证	2019-05-21 0…	登录	操作成功
4	admin	初始化用户	10.251.251.112	系统认证	2019-05-21 0…	登录(登录失…	操作失败
5	admin	初始化用户	10.251.251.112	系统认证	2019-05-21 0…	登录	操作成功
6	admin	初始化用户	10.251.251.112	系统认证	2019-05-21 0…	登录	操作成功
7	admin	初始化用户	10.251.251.120	系统认证	2019-05-21 0…	登录	操作成功
8	admin	初始化用户	10.251.251.120	网卡配置	2019-05-21 1…	改变网卡	操作成功
9	admin	初始化用户	10.251.251.120	系统认证	2019-05-21 1…	登录	操作成功
10	admin	初始化用户	10.251.251.120	系统认证	2019-05-21 1…	登录	操作成功

当前第 1 页 共 110页　当前显示10条，共1097条　每页显示 10 条

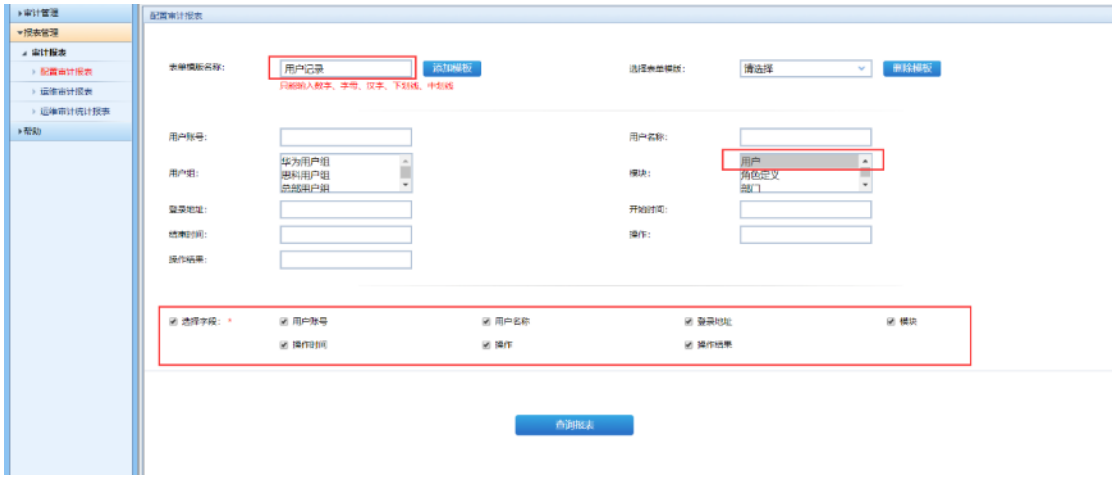
13.1.2. 按模板生成配置审计报表

配置审计模板是将经常使用的查询条件添加成模板，添加的模板可重复使用，方便查询。

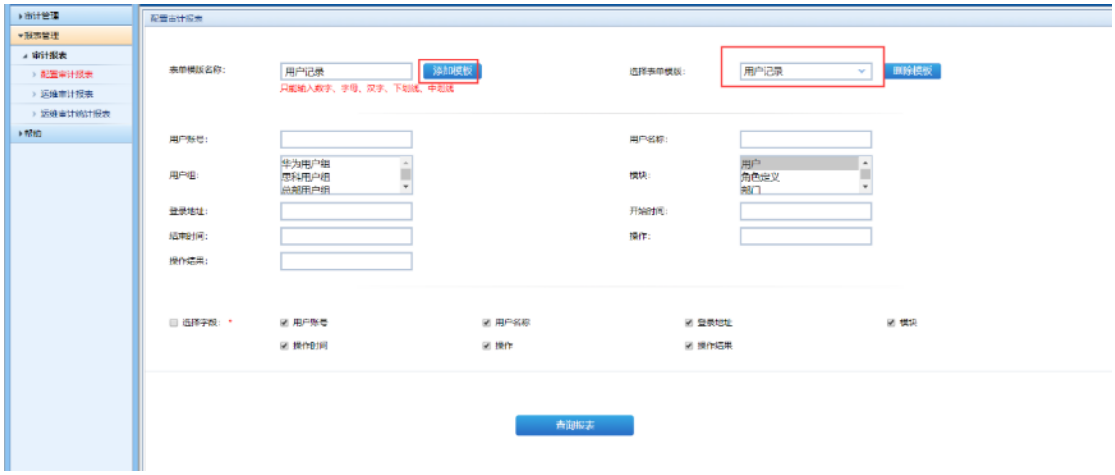
点击报表管理 ->审计报表->配置审计报表链接，进入配置审计报表界面。

将操作用户模块的记录作为查询条件添加到报表模板中，添加步骤如下：

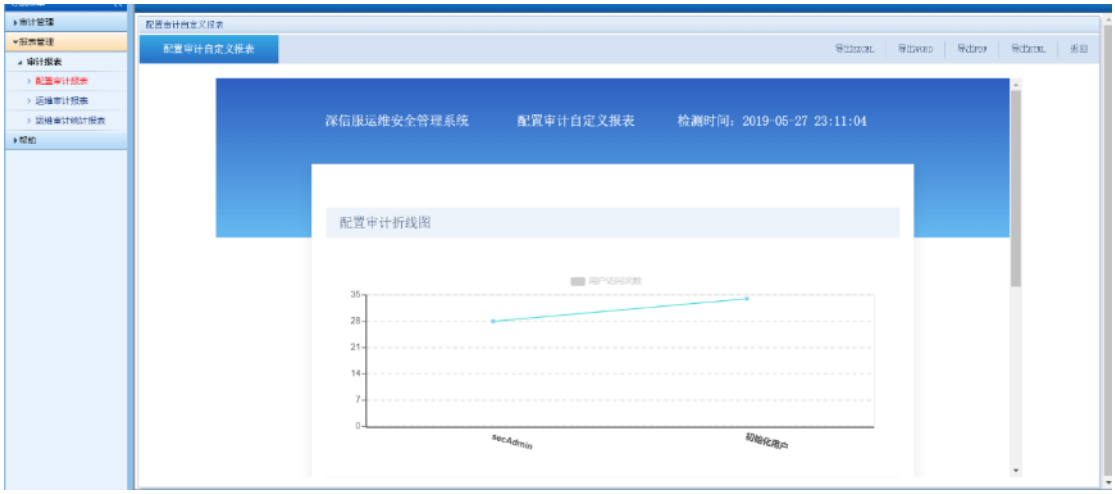
1) 输入表单模板名称
2) 添加查询条件
3) 勾选显示字段
4) 点击添加模板



点击选择表单名称，选择用户记录模板，点击查询报表。



查询页面显示操作用户模块的记录。

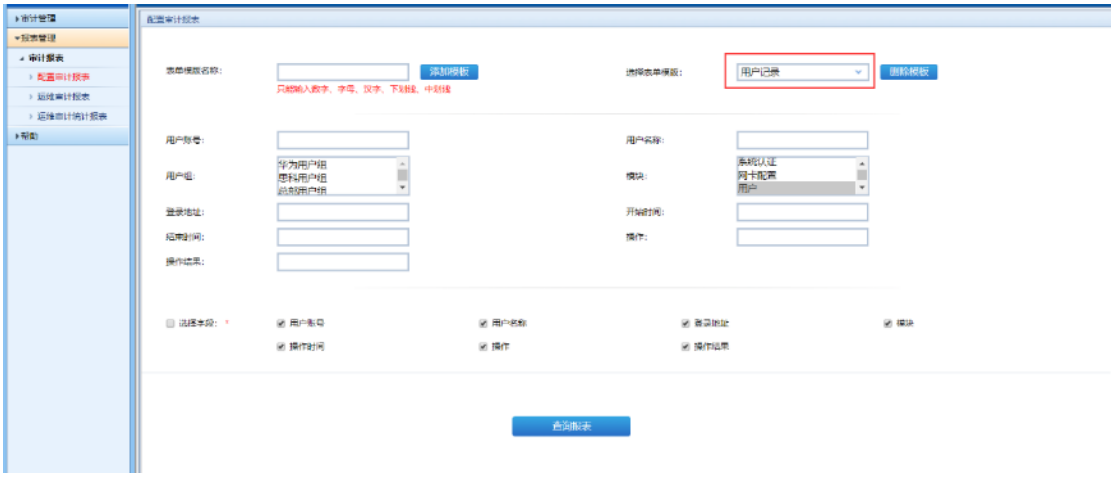


13.1.3. 配置审计报表导出

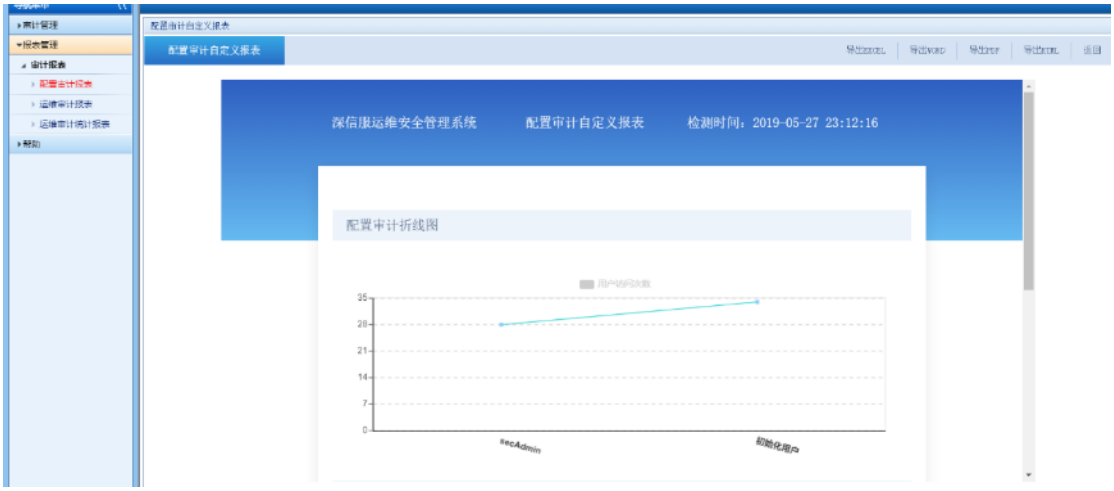
配置审计报表导出：将报表导出到本地，方便用户的使用和阅读。报表支持的导出格式：

- excel 格式
- word 格式
- pdf 格式
- html 格式

点击报表管理->审计报表->配置审计报表链接，进入配置报表审计界面。选择报表模板用户记录，点击查询报表。

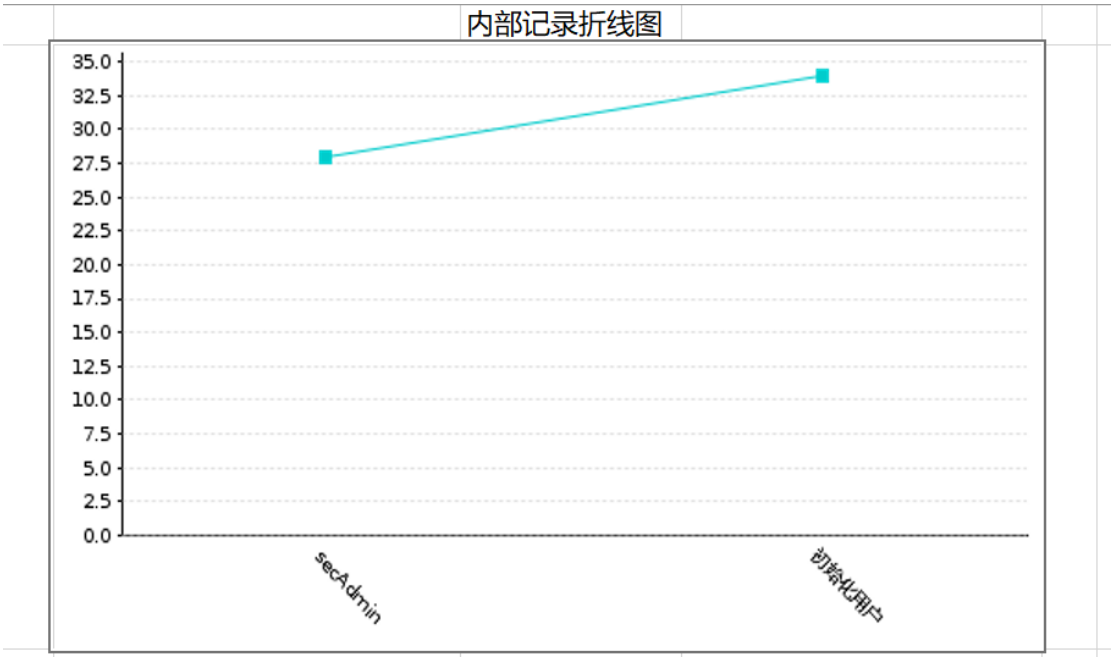


查询页面显示导出方式。



- excel 格式导出

点击导出 EXCEL，以 excel 格式导出，导出的 excel 文件含有两个工作表，FortSystemLog 存放登录账号操作用户模块次数的折线图。FortSystemLog2 存放用户操作详细信息，如



序号	用户账号	用户名	登录地址	模	操作时间	操作	操作结果
1	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:28:54	添加用户[sysadmin]	操作成功
2	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:29:50	修改用户[sysadmin]为[sysAdmin]	操作成功
3	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:17	添加用户[secAdmin]	操作成功
4	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:56	添加用户[sysAduit]	操作成功
5	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:17	修改用户[sysAduit]为[sysAudit]	操作成功
6	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:37	修改用户[sysAudit]	操作成功
7	admin	初始化用户	172.16.23.253	用户	2019-05-21 11:32:24	修改用户[secAdmin]	操作成功
8	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:17	添加用户[Audit]	操作成功
9	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:35	修改用户[Audit]为[Audit123]	操作成功
10	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:16:07	修改用户[Audit123]为[Audit]	操作成功
11	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:19:18	修改用户[Audit]	操作成功
12	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:19:24	修改用户[Audit]	操作成功
13	admin	初始化用户	172.16.23.253	用户	2019-05-21 14:20:31	修改用户[Audit]	操作成功
14	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:21:09	修改用户[Audit]	操作成功
15	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 15:09:10	添加用户[aa]	操作成功
16	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 16:34:15	添加用户[ab]	操作成功
17	admin	初始化用户	172.16.39.253	用户	2019-05-22 02:04:56	添加用户[mm]	操作成功

- word 格式导出

点击导出 WORD，以 WORD 格式导出。打开导出的 word 文件，图 3.14.1.3-5 的折线图表示登录账号操作用户模块的次数。图 3.14.1.3-6 显示操作用户模块的详细信息。

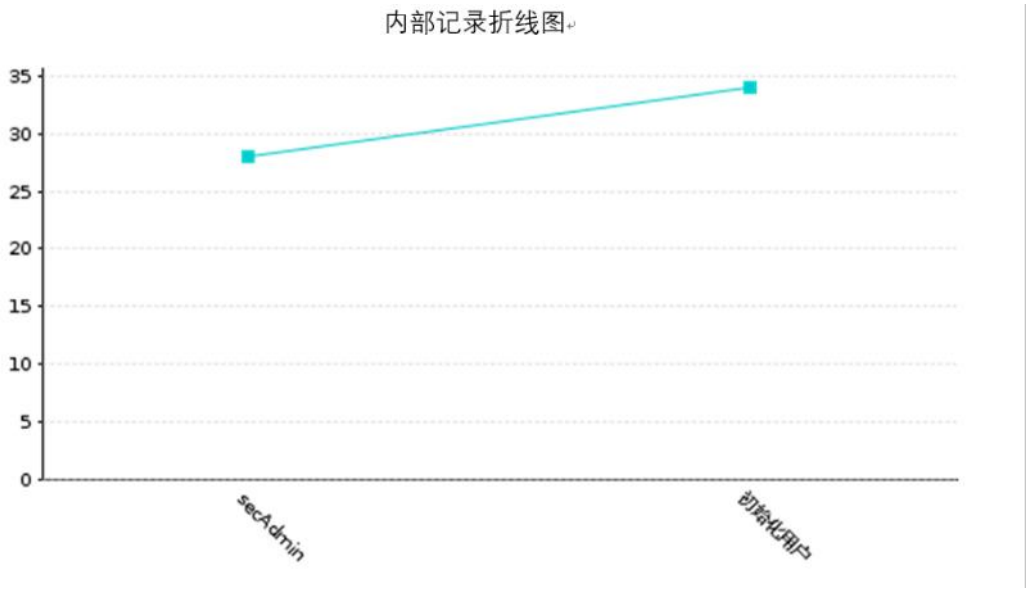


图 3. 14. 1. 3-5

序号	用户账号	用户名称	登录地址	模	操作时间	操作	操作结果
1	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:28:54	添加用户[sysadmin]	操作成功
2	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:29:50	修改用户[sysadmin]为[sysAdmin]	操作成功
3	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:17	添加用户[secAdmin]	操作成功
4	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:56	添加用户[sysAduit]	操作成功
5	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:17	修改用户[sysAduit]为[sysAudit]	操作成功
6	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:37	修改用户[sysAudit]	操作成功
7	admin	初始化用户	172.16.23.253	用户	2019-05-21 11:32:24	修改用户[secAdmin]	操作成功
8	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:17	添加用户[Audit]	操作成功
9	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:35	修改用户[Audit]为[Audit123]	操作成功
10	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:16:07	修改用户[Audit123]为[Audit]	操作成功
11	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:19:18	修改用户[Audit]	操作成功

- pdf 格式导出

点击导出 PDF，以 PDF 格式导出。打开导出的 pdf 文件，图 3.14.1.3-7 的折线图表示登录账号操作用户模块的次数。图 3.14.1.3-8 显示操作用户模块的详细信息。

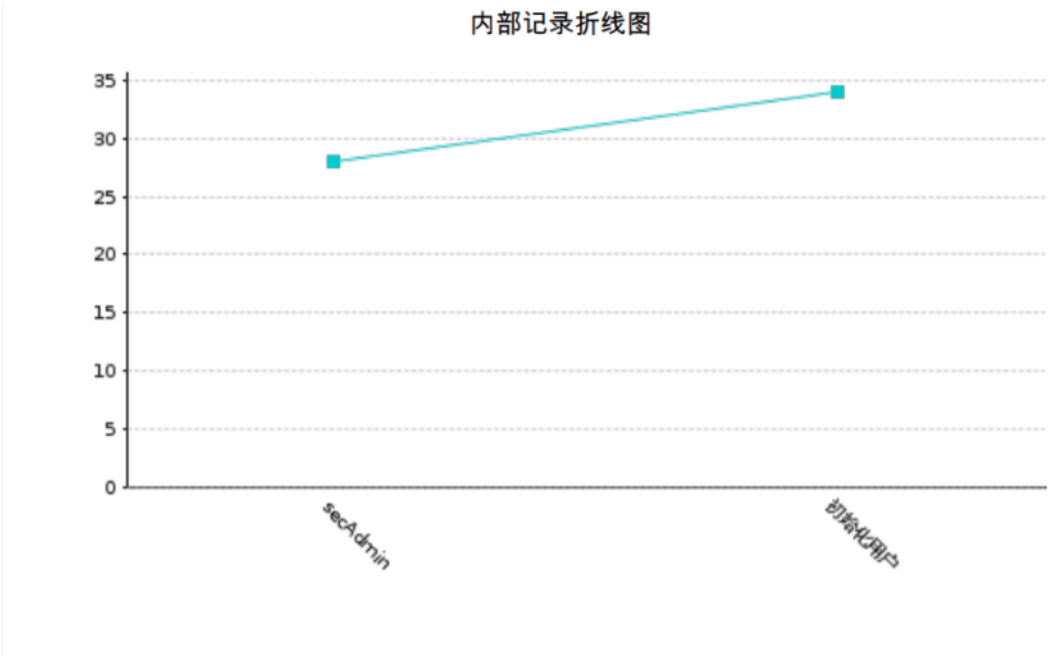
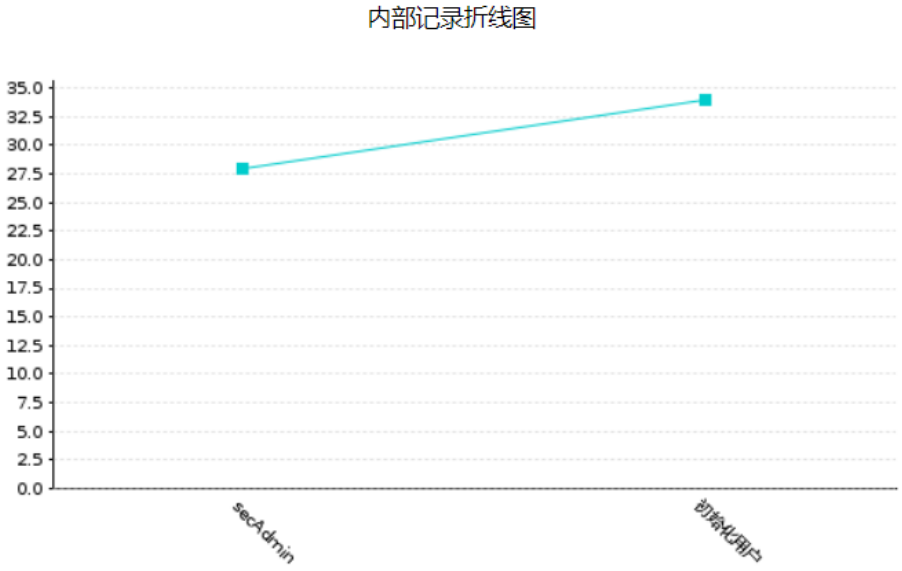


图 3. 14. 1. 3-7

序号	用户账号	用户名称	登录地址	模	操作时间	操作	操作结果
1	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:28:54	添加用户[sysadmin]	操作成功
2	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:29:50	修改用户[sysadmin]为[sysAdmin]	操作成功
3	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:17	添加用户[secAdmin]	操作成功
4	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:30:56	添加用户[sysAduit]	操作成功
5	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:17	修改用户[sysAduit]为[sysAudit]	操作成功
6	admin	初始化用户	172.16.23.253	用户	2019-05-21 10:31:37	修改用户[sysAudit]	操作成功
7	admin	初始化用户	172.16.23.253	用户	2019-05-21 11:32:24	修改用户[secAdmin]	操作成功
8	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:17	添加用户[Audit]	操作成功
9	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:10:35	修改用户[Audit]为[Audit123]	操作成功
10	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:16:07	修改用户[Audit123]为[Audit]	操作成功
11	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:19:18	修改用户[Audit]	操作成功
12	secAdmin	secAdmin	172.16.23.253	用户	2019-05-21 14:19:24	修改用户[Audit]	操作成功

- html 格式导出

点击导出 HTML，以 html 格式导出。打开导出的 html 文件，图 3.14.1.3-9 的折线图表示登录账号操作用户模块的次数。显示操作用户模块的详细信息。



序号	用户账号	用户名称	登录地址	模块 操作时间	操作	操作结果
1	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:28:54	添加用户[sysadmin]	操作成功
2	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:29:50	修改用户[sysadmin]为[sysAdmin]	操作成功
3	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:30:17	添加用户[secAdmin]	操作成功
4	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:30:56	添加用户[sysAduit]	操作成功
5	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:31:17	修改用户[sysAduit]为[sysAudit]	操作成功
6	admin	初始化用户	172.16.23.253	用户 2019-05-21 10:31:37	修改用户[sysAudit]	操作成功
7	admin	初始化用户	172.16.23.253	用户 2019-05-21 11:32:24	修改用户[secAdmin]	操作成功
8	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:10:17	添加用户[Audit]	操作成功
9	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:10:35	修改用户[Audit]为[Audit123]	操作成功
10	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:16:07	修改用户[Audit123]为[Audit]	操作成功
11	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:19:18	修改用户[Audit]	操作成功
12	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:19:24	修改用户[Audit]	操作成功
13	admin	初始化用户	172.16.23.253	用户 2019-05-21 14:20:31	修改用户[Audit]	操作成功
14	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 14:21:09	修改用户[Audit]	操作成功
15	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 15:09:10	添加用户[aa]	操作成功
16	secAdmin	secAdmin	172.16.23.253	用户 2019-05-21 16:34:15	添加用户[ab]	操作成功

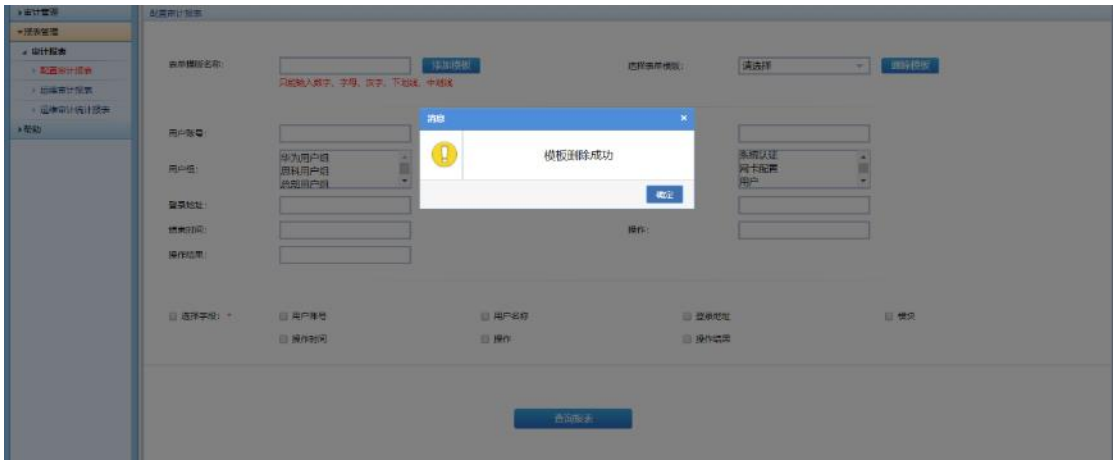
13.1.4. 配置报表模板删除

配置报表模板删除用于删除废弃的报表模板。

点击报表管理 ->审计报表->配置审计报表链接，进入配置报表审计界面。选择报表模板用户

记录，点击删除模板。

提示：模板删除成功！



13.2. 运维审计报表

13.2.1. 直接生成运维报表

点击报表管理 ->审计报表->运维审计报表链接，进入运维审计报表界面。

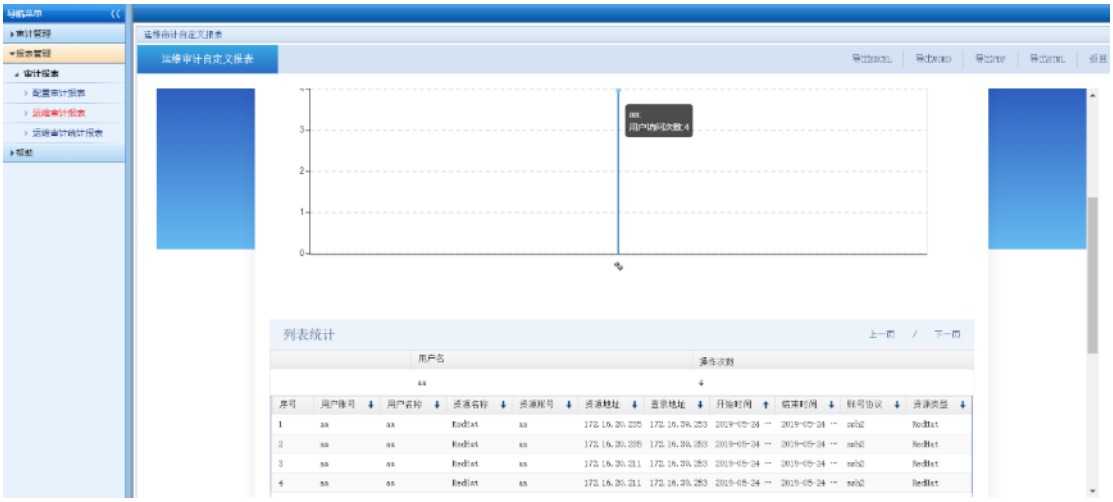
选择所需查询的字段，点击查询报表。

查询结果如下图所示：用户单点登录次数以折线图形式展现，访问资源的详细信息以报表表格形式展现。

13.2.2. 按模板生成运维报表

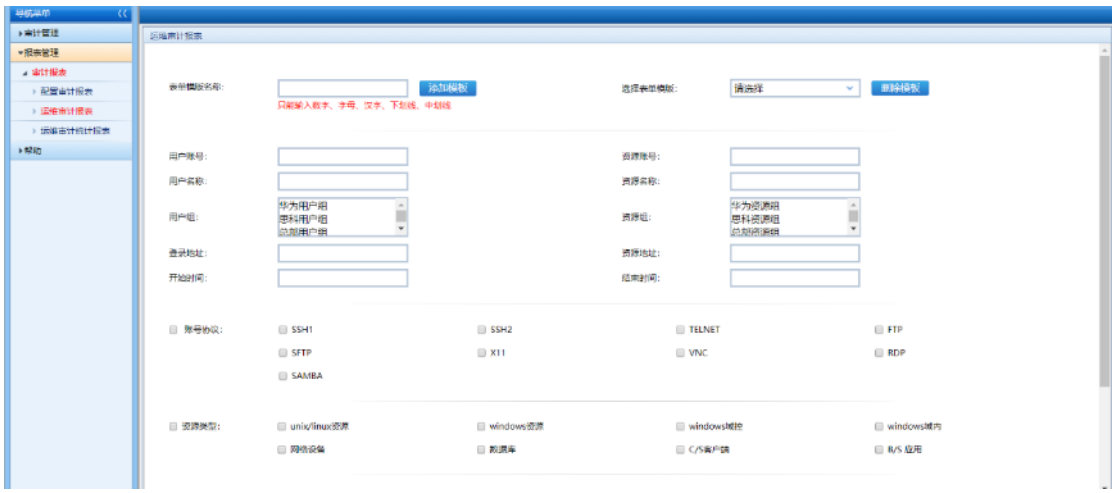
运维模板是将经常使用的查询条件添加成模板。添加的模板可重复使用，方便了查询。

点击报表管理 ->审计报表->运维审计报表链接，进入运维审计界面。



查询用户通过 RDP 协议运维 windows 资源的记录，添加查询条件到报表模板中。报表模板的添加步骤如下：

1) 输入表单模板名称
2) 添加查询条件
3) 勾选查询资源和协议类型
4) 勾选显示字段
5) 点击添加模板



点击选择表单名称，选择 SSH2，点击查询报表。

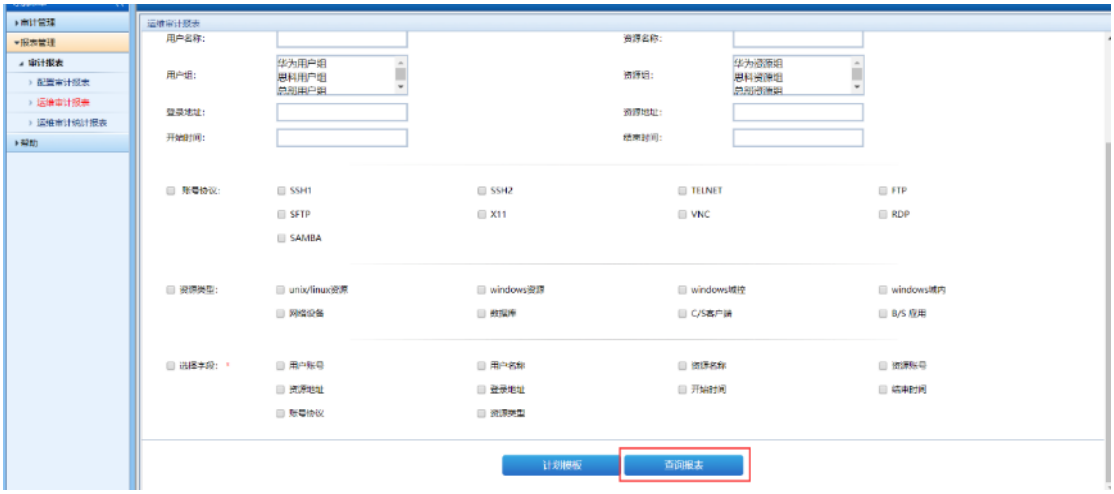
查询页面显示用户通过 ssh2 运维 unix/linux 资源的记录。

13.2.3. 运维报表导出

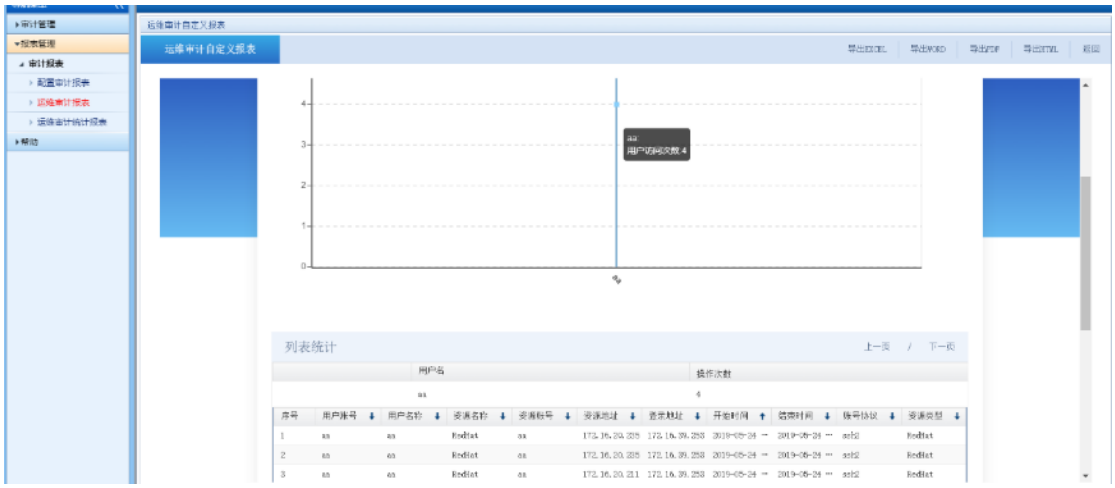
运维报表导出可将报表导出到本地，方便用户的使用和阅读，审计报表支持的导出格式：

- excel 格式
- word 格式
- pdf 格式
- html 格式

点击审计管理 ->审计报表->运维审计报表链接，进入运维审计报表界面。选择报表模板 SSH2，点击查询报表。

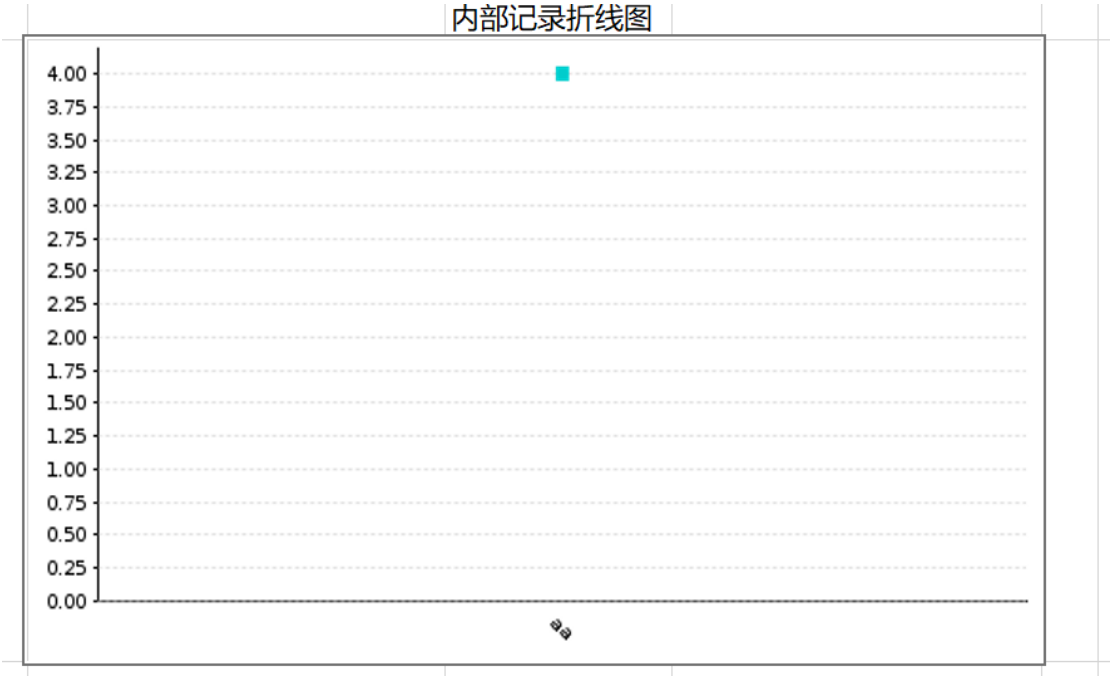


查询页面显示导出方式。



- **excel 格式导出**

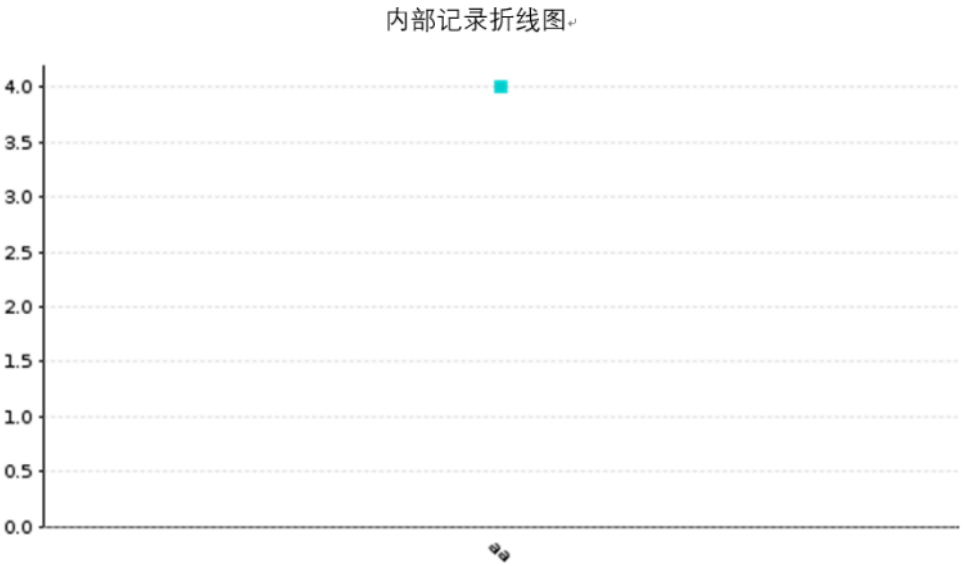
导出的 excel 文件含有两个工作表，FortSystemLog 存放用户单点登录次数的折线图；FortSystemLog2 存放用户单点登录的详细信息。



序号	用户账号	用户名称	资源名称	资源账号	开始时间	结束时间	账号协议	资源类型
1	aa	aa	RedHat	aa	2019-05-24 03:56:08	2019-05-24 03:56:11	ssh2	RedHat
2	aa	aa	RedHat	aa	2019-05-24 03:56:18	2019-05-24 03:56:21	ssh2	RedHat
3	aa	aa	RedHat	aa	2019-05-24 03:58:43	2019-05-24 03:58:46	ssh2	RedHat
4	aa	aa	RedHat	aa	2019-05-24 03:59:12	2019-05-24 03:59:16	ssh2	RedHat

- word 格式导出

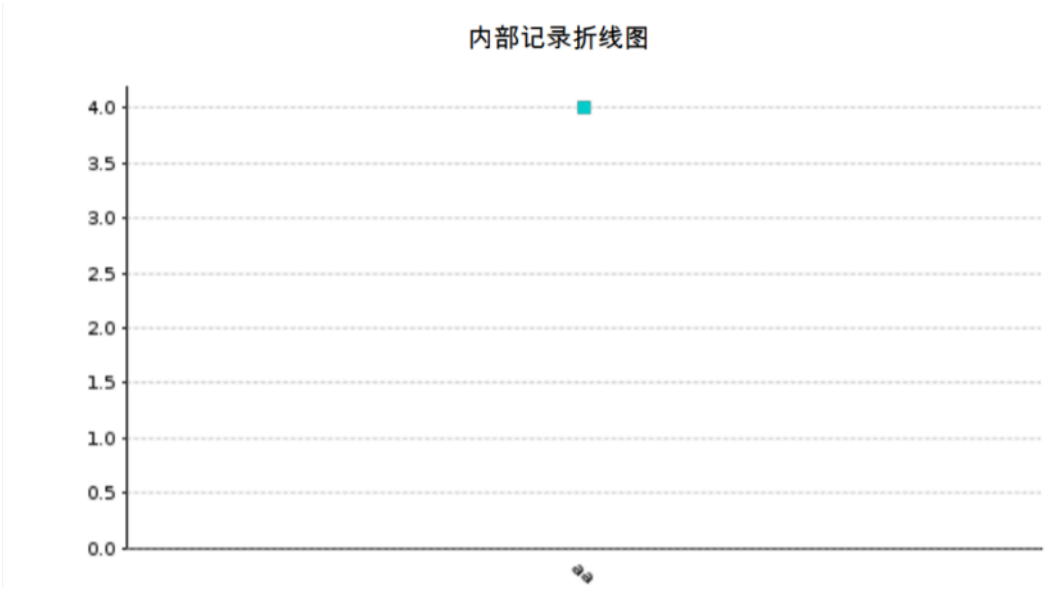
点击导出 WORD，以 WORD 格式导出。打开导出的 word 文件，的折线图表示用户通过 SSH2 协议运维 unix/linux 资源的次数。显示用户运维的详细信息。



序号	用户账号	用户名称	资源名称	资源账号	登录地址	开始时间	结束时间	账号协议	资源类型
1	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:56:08	2019-05-24 03:56:11	ssh2	RedHat
2	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:56:18	2019-05-24 03:56:21	ssh2	RedHat
3	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:58:43	2019-05-24 03:58:46	ssh2	RedHat
4	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:59:12	2019-05-24 03:59:16	ssh2	RedHat

- pdf 格式导出

点击导出 PDF，以 PDF 格式导出。打开导出的 pdf 文件，图 3.14.2.3-7 的折线图表示用



户通过 SSH2 协议运维 unix/linux 资源的次数。显示用户运维的详细信息。

序号	用户账号	用户名称	资源名称	资源账号	登录地址	开始时间	结束时间	账号协议	资源类型
1	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:56:08	2019-05-24 03:56:11	ssh2	RedHat
2	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:56:18	2019-05-24 03:56:21	ssh2	RedHat
3	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:58:43	2019-05-24 03:58:46	ssh2	RedHat
4	aa	aa	RedHat	aa	172.16.39.253	2019-05-24 03:59:12	2019-05-24 03:59:16	ssh2	RedHat

- html 格式导出

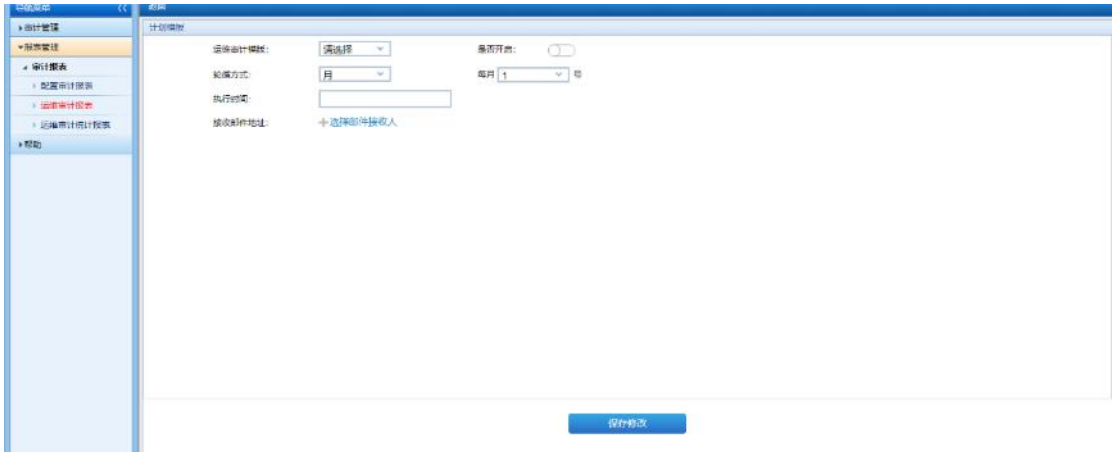
点击导出 HTML，以 html 格式导出。打开导出的 html 文件，图 3.14.2.3-9 的折线图表示用户通过 SSH2 协议运维 unix/linux 资源的次数，图 3.14.2.3-10 的表格显示用户运维的详细信息。

图 3.14.2.3-9

13.2.4. 计划模板

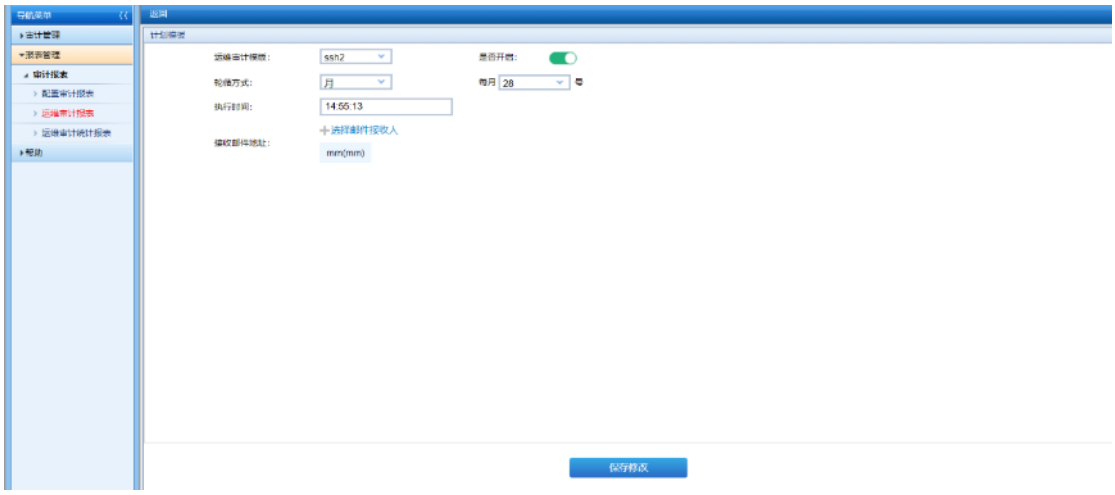
计划模板是将创建好的运维审计报表模板，按照制定的时间计划以邮件的形式向外发送运维审计报表

点击报表管理 ->审计报表->运维审计报表->计划模板链接，进入计划模板页面。

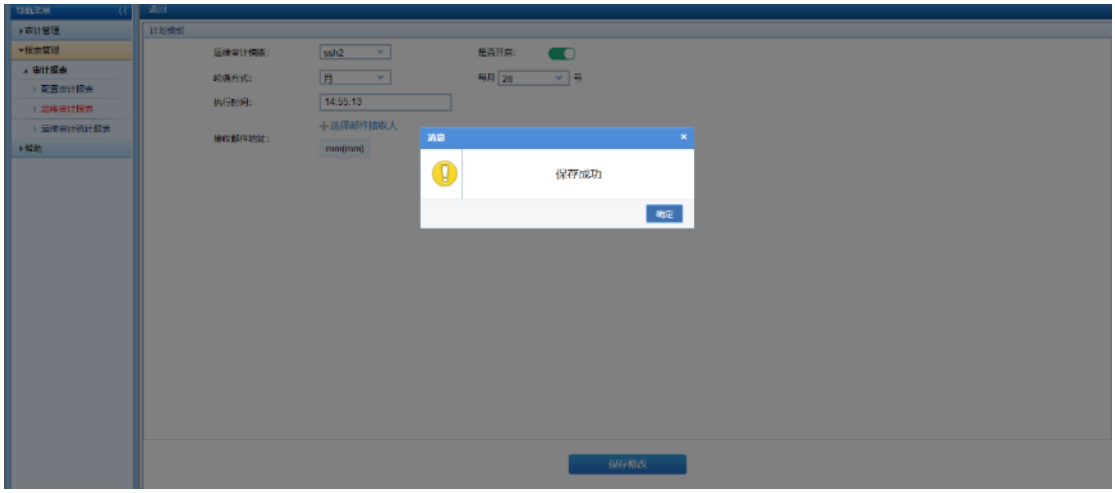


具体操作如下：

- 运维审计模板：SSH2
- 是否开启：开启
- 轮循方式：月
- 每月：13 号
- 执行时间 ：10:21:45
- 选择邮件接收人



点击保存，提示：保存成功



每月的 13 号 10:21:45 可以邮箱中接收运维审计报表。

13.2.5. 运维报表模板删除

运维报表模板删除用于删除废弃的运维报表模板。

点击报表管理 ->审计报表->运维审计报表链接，进入运维审计界面。选择报表模板 ssh2，点击删除模板。

13.3. 运维审计统计报表

13.3.1. 活跃资源统计

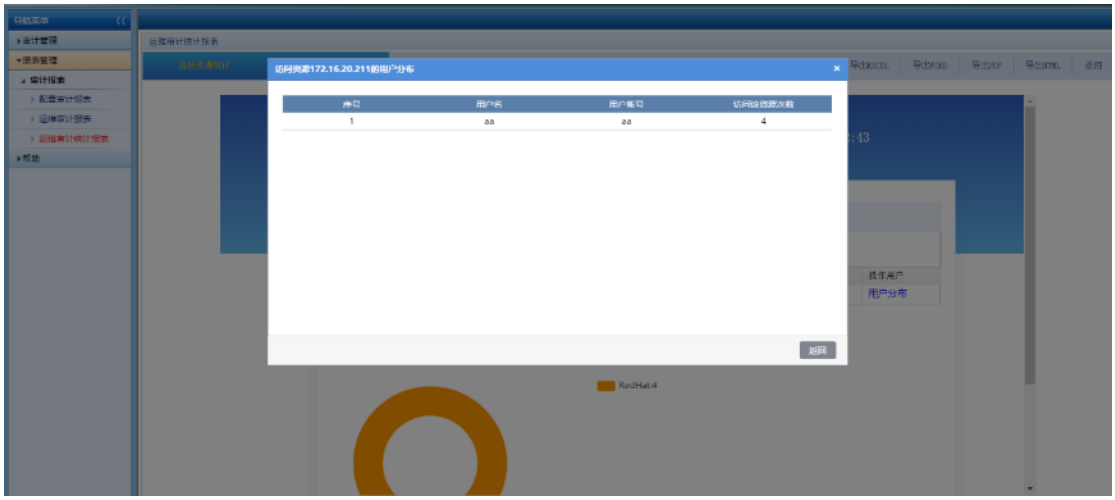
审计管理员 sysAudit 登录，切换至审计管理员角色，点击报表管理->审计报表->运维审计统计

报表->活跃资源统计链接，进入活跃资源统计界面。

➢ 查看用户分布

点击用户分布。

显示该资源的用户分布情况。



➢ 活跃资源统计报表导出

活跃资源统计报表导出可将报表导出到本地，方便用户的使用和阅读，资源统计报表支持的导出格式：

- excel 格式
- word 格式
- pdf 格式
- html 格式

● excel 格式导出

点击导出 EXCEL，以 excel 格式导出，导出的报表如图：

- word 格式导出

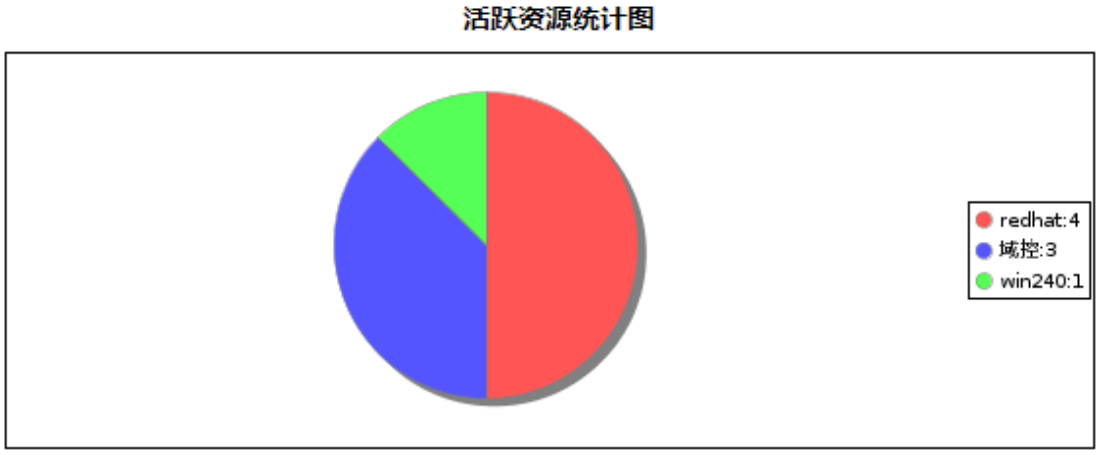
点击导出 WORD，以 word 格式导出，导出的报表如图：

- PDF 格式导出

点击导出 PDF，以 pdf 格式导出，导出的报表如图：

- HTML 格式导出

点击导出 HTML，以 html 格式导出，导出的报表如图：



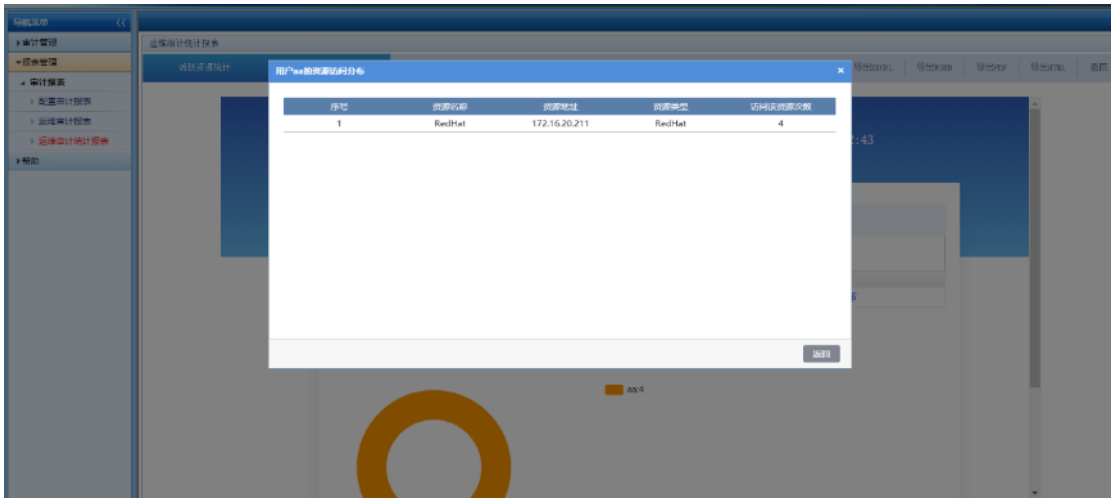
13.3.2. 活跃用户统计

审计管理员 sysAudit 登录，切换至审计管理员角色，点击报表管理->审计报表->运维审计统计报表->活跃用户统计链接，进入活跃用户统计界面。

➢ 查看资源分布

点击资源分布。

显示该用户的资源分布情况。



➢ 活跃用户统计报表导出

活跃用户统计报表导出可将报表导出到本地，方便用户的使用和阅读，用户统计报表支持的导出格式：

- excel 格式
- word 格式
- pdf 格式
- html 格式

- **excel 格式导出**

点击导出 EXCEL，以 excel 格式导出，

- word 格式导出

点击导出 WORD，以 word 格式导出，导出的报表如图：图 3.14.3.2-6

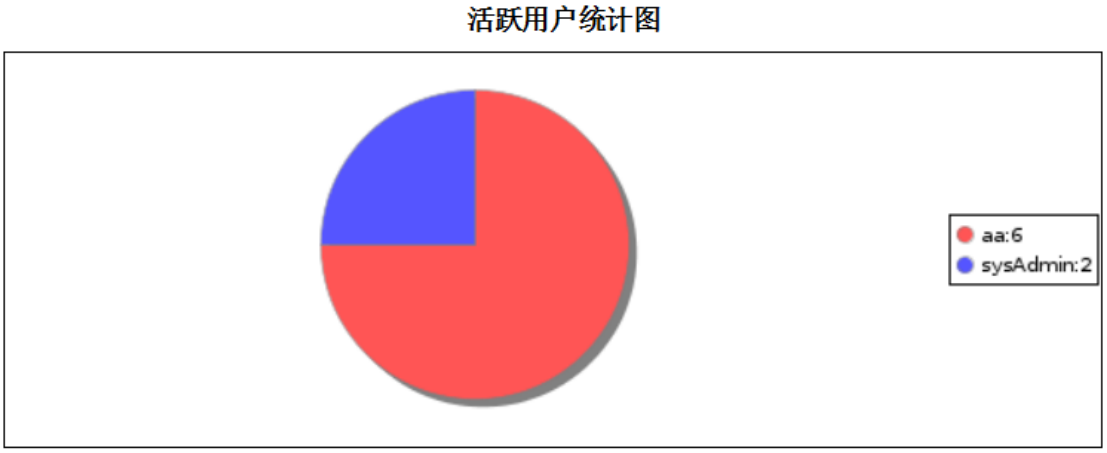


图 3.14.3.2-6

- PDF 格式导出

点击导出 PDF，以 pdf 格式导出，导出的报表如图：图 3.14.3.2-7

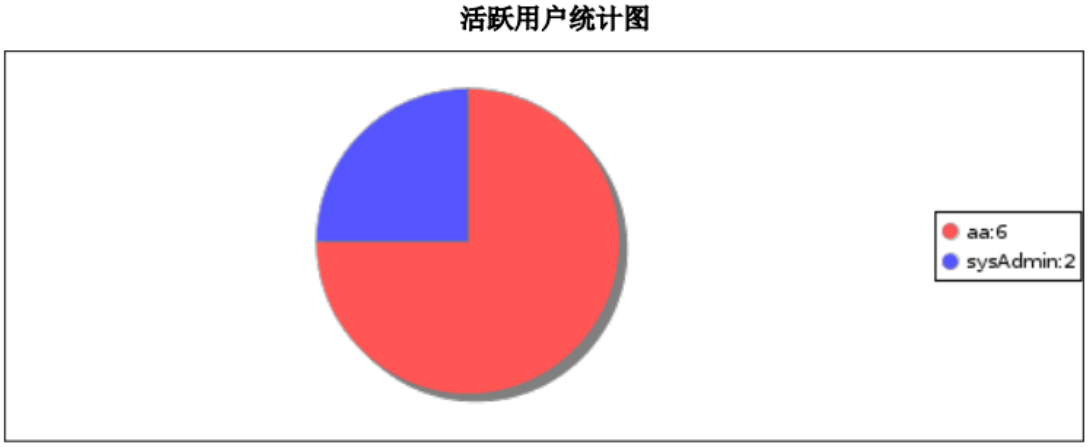
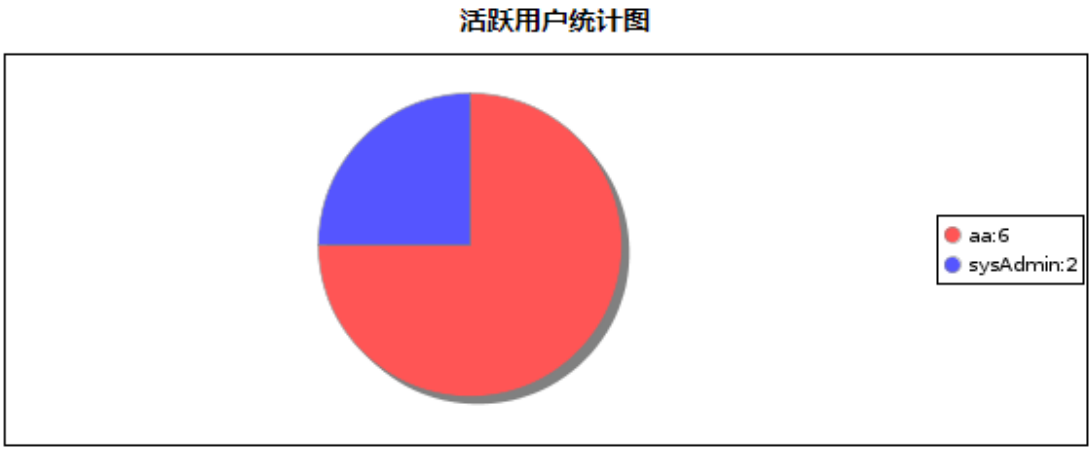


图 3.14.3.2-7

- HTML 格式导出

点击导出 HTML，以 html 格式导出，导出的报表如图：图 3.14.3.2-8



14. 系统配置

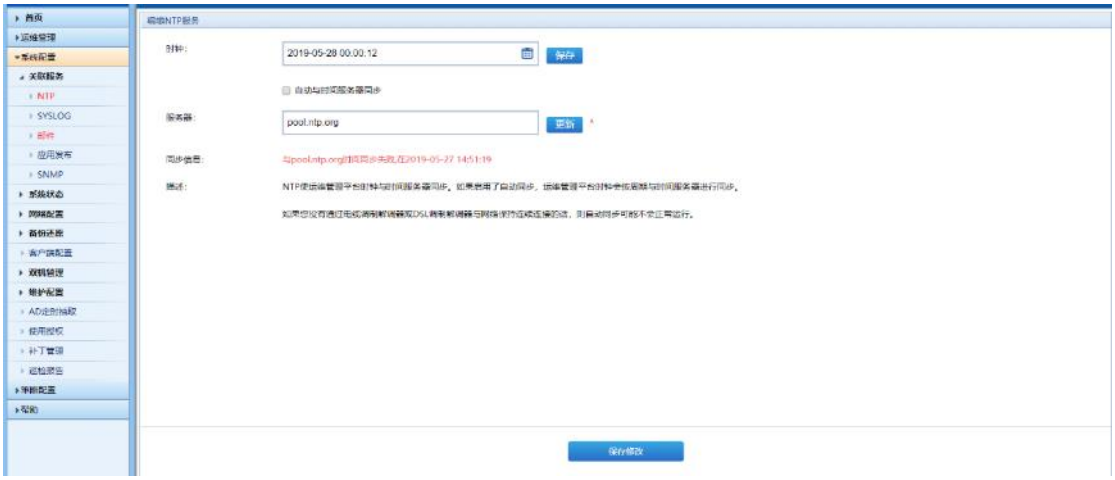
14.1. 服务配置

14.1.3. 关联服务

14.1.4. NTP

NTP 可配置使用系统服务器与时间服务器同步。

使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->关联服务->NTP 链接进入 NTP 界面。



1.前台修改系统时间

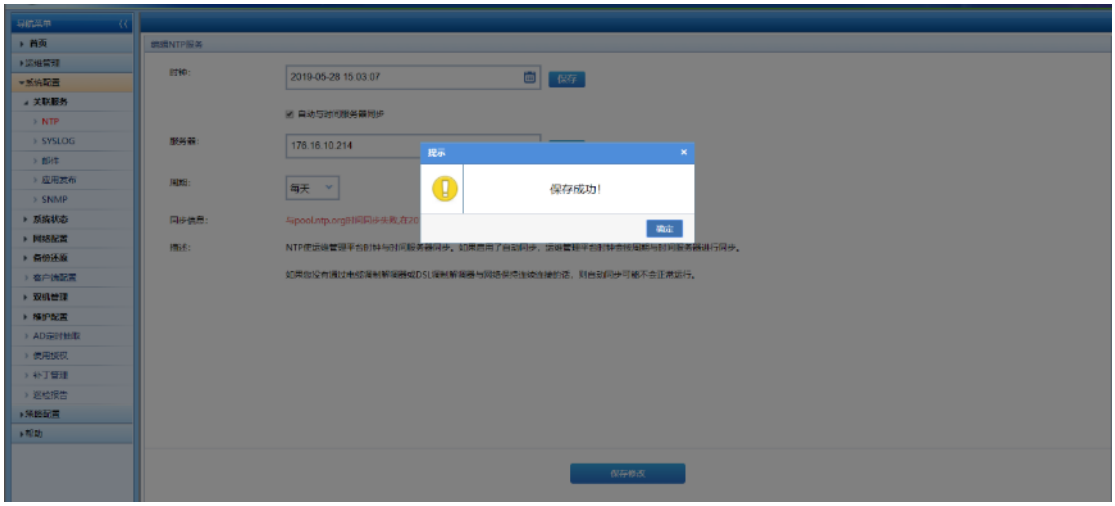
在时钟后选择时间，点击保存按钮，系统时间修改成功。

2.时间同步服务器同步

输入服务器 IP172.16.10.214 后点击更新，同步信息显示同步失败或成功，且时钟输入框显示同步后的时间。

勾选自动与时间服务器同步，输入服务器 IP172.16.10.214，选择周期每天。

点击保存，提示保存成功！系统可按周期时间自动更新。



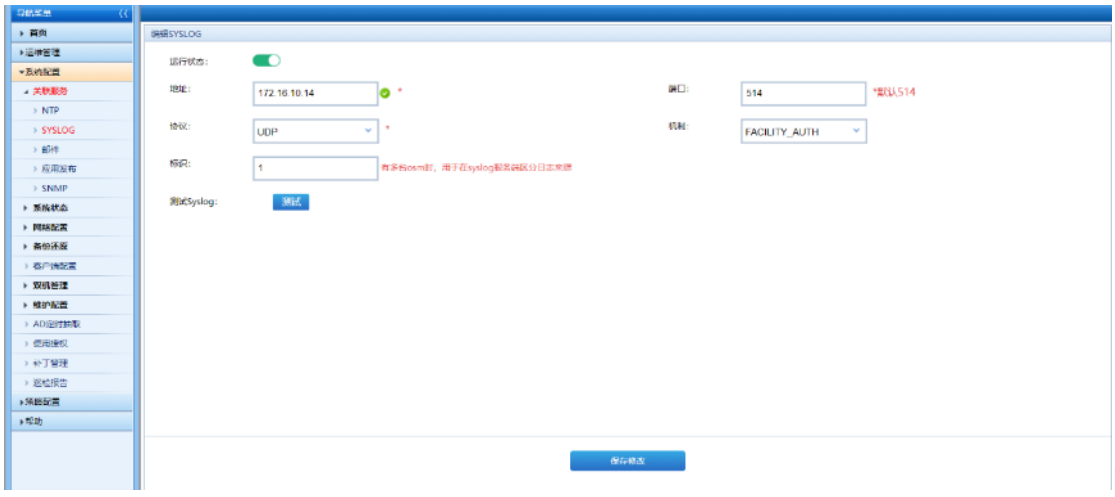
点击确定，系统可按周期时间自动更新。

14.1.5. SYSLOG

syslog 日志服务器基本配置。

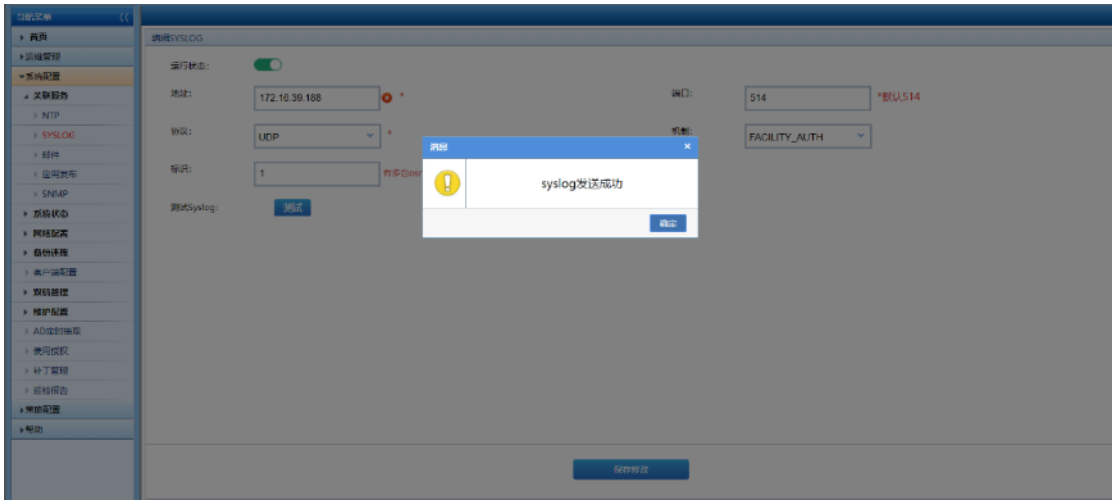
使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->关联服务->SYSLOG 链接进入 SYSLOG 界面。

填写完整信息，点击保存。运行状态为 ON 可以推送日志，为 OFF 则不能推送。



图

IP 地址可用，点击测试，提示 syslog 发送成功，测试的结果与运行状态无关。



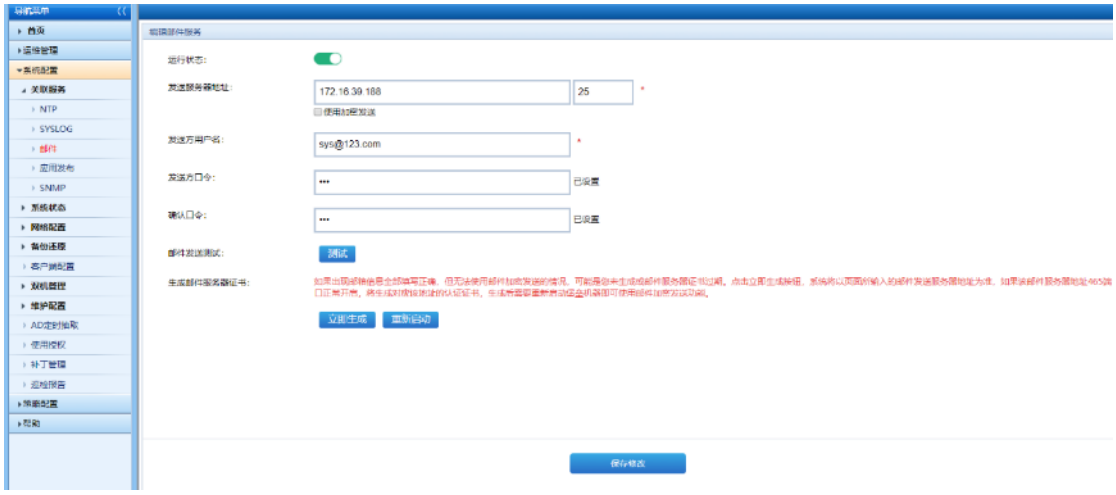
图

14.1.6. 邮件

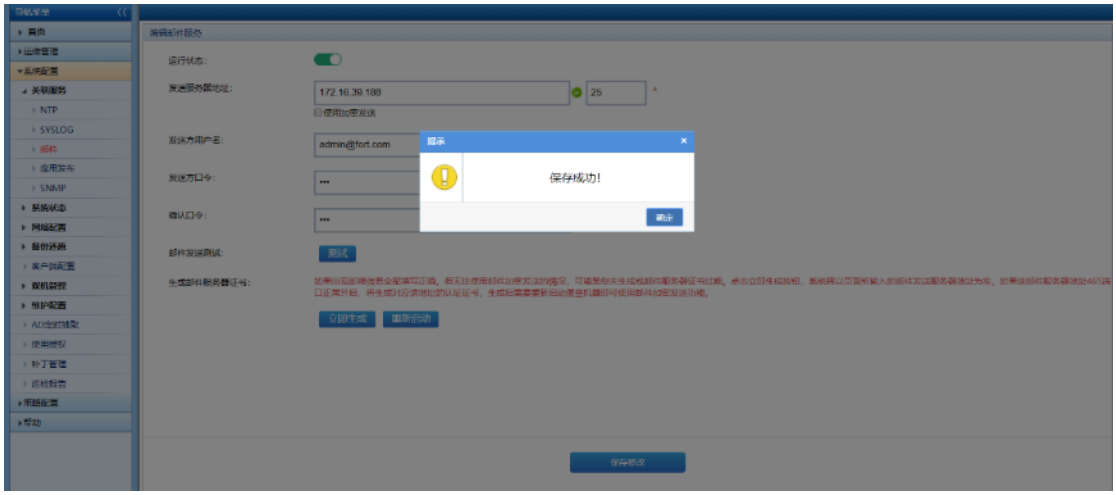
邮件服务器基本配置。

使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->关联服务->邮件链接进入邮件界面。

填写完整信息，点击保存。运行状态为 ON 可以发送邮件，为 OFF 则不能发送。



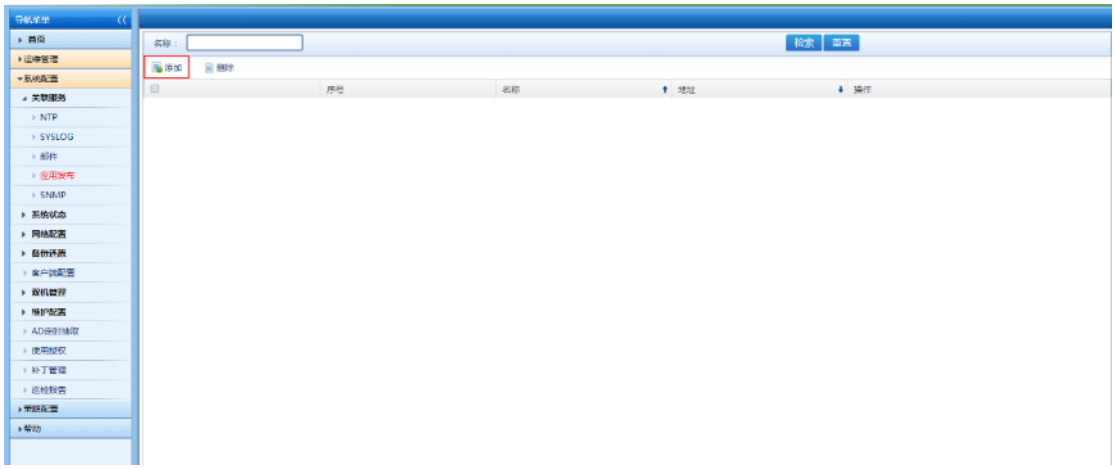
发送服务器地址可用，点击测试，提示邮件发送成功，测试的结果与运行状态无关。



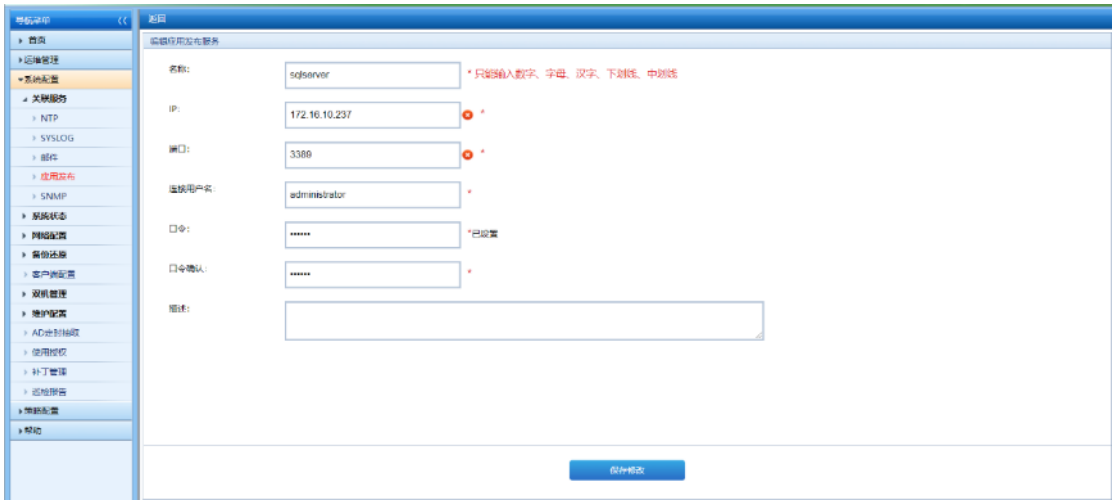
14.1.7. 应用发布

1.应用发布添加

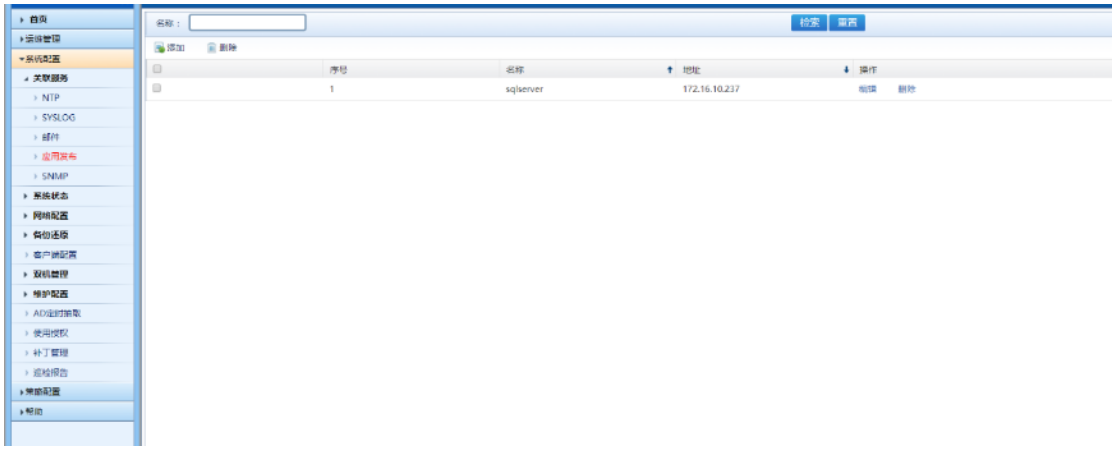
使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->关联服务->应用发布链接，点击添加。



切换到应用发布编辑页面，填写应用发布基本信息，点击保存。



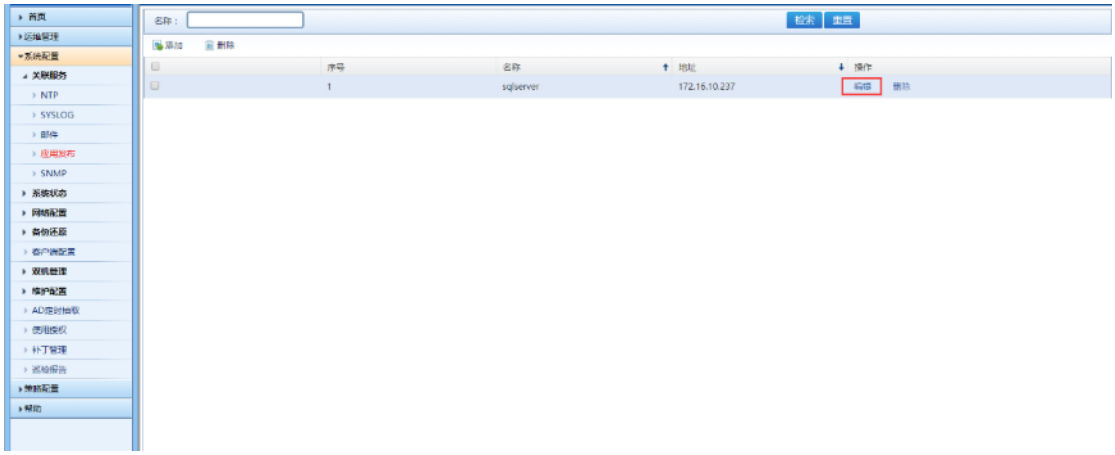
切换到应用发布列表页面，列表中显示名称为 sqlserver 的条目。



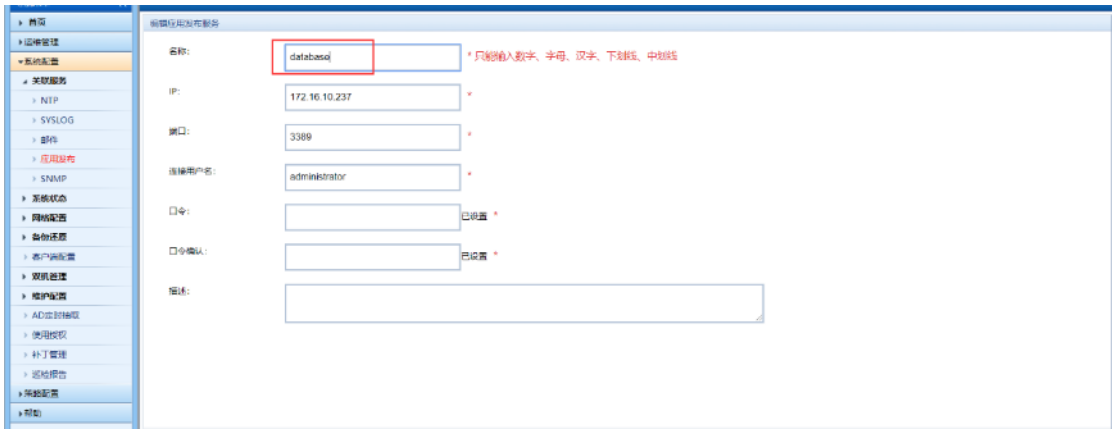
2.应用发布编辑

修改应用发布的名称、IP、连接用户名、连接口令等。

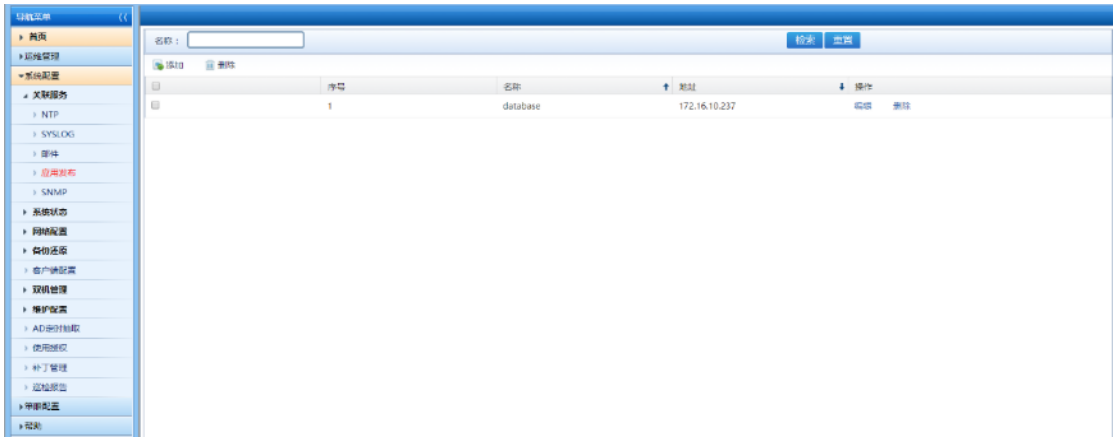
点击系统配置->关联服务->应用发布链接，点击名称为 sqlserver 的应用发布对应的编辑按钮。



修改应用发布名称为 database，点击保存。



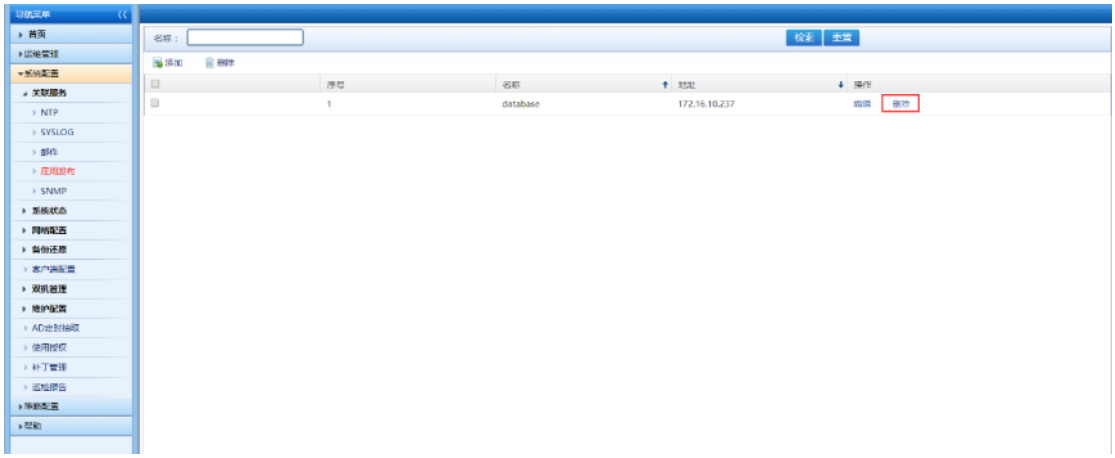
点击系统配置->关联服务->应用发布链接，切换到应用发布列表页面，列表中显示名称为 database 的条目。



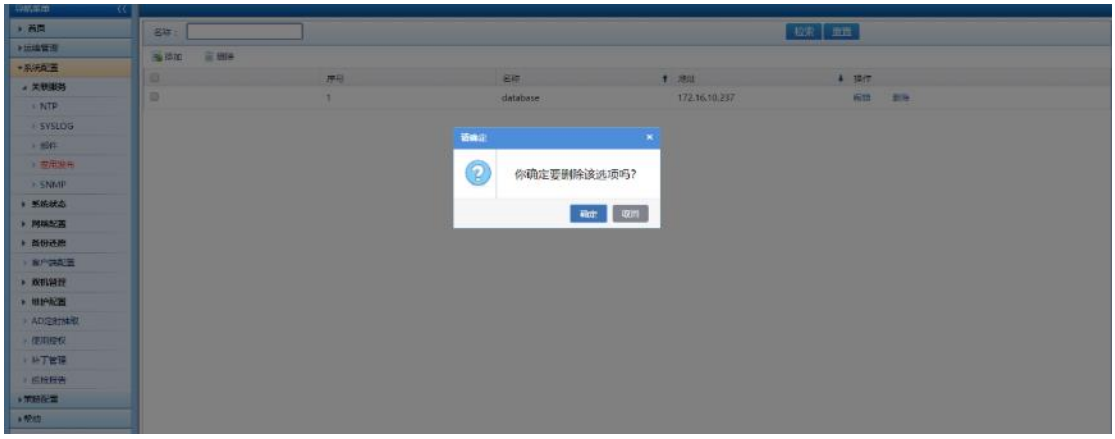
3.应用发布删除

删除不再使用的应用发布。可对单个应用发布进行删除，也可一次勾选多个应用发布进行删除。

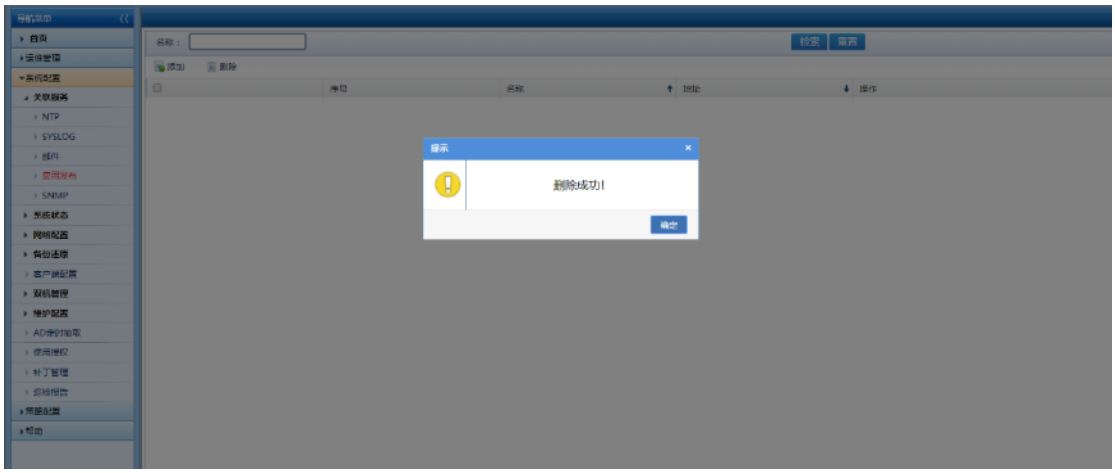
点击系统配置->关联服务->应用发布链接，点击名称为database的应用发布对应的删除按钮。



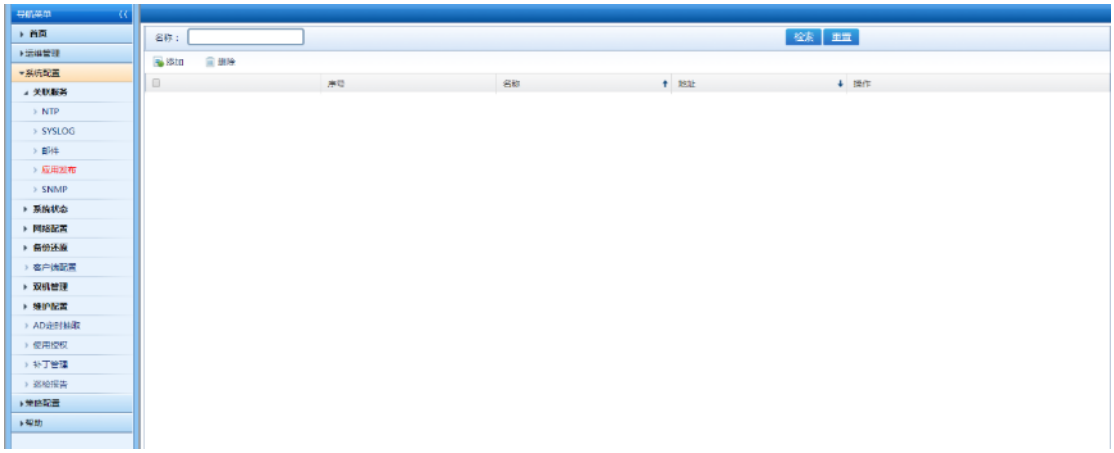
弹出提示你确定删除该选项吗？



点击弹出框上的确定。提示删除成功！

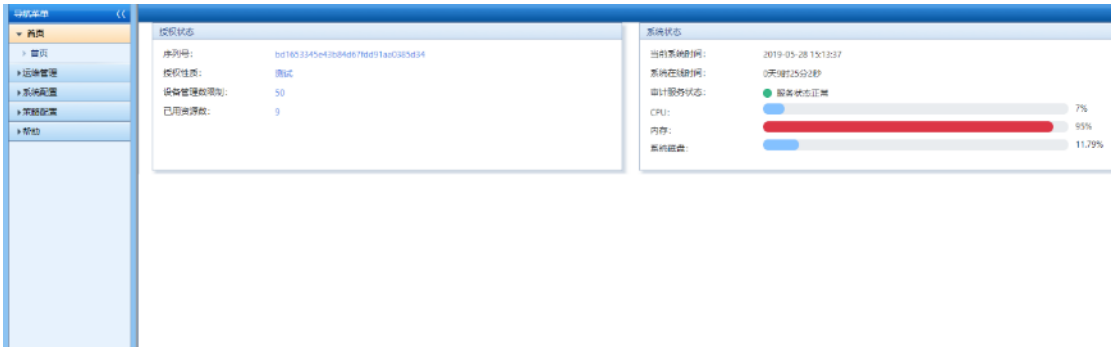


点击系统配置->关联服务->应用发布链接，切换到应用发布列表页面，列表中不显示名称为 database 的条目。



14.1.8. 系统状态

使用系统管理员身份登陆系统后，系统首页会默认显示系统状态总览页：

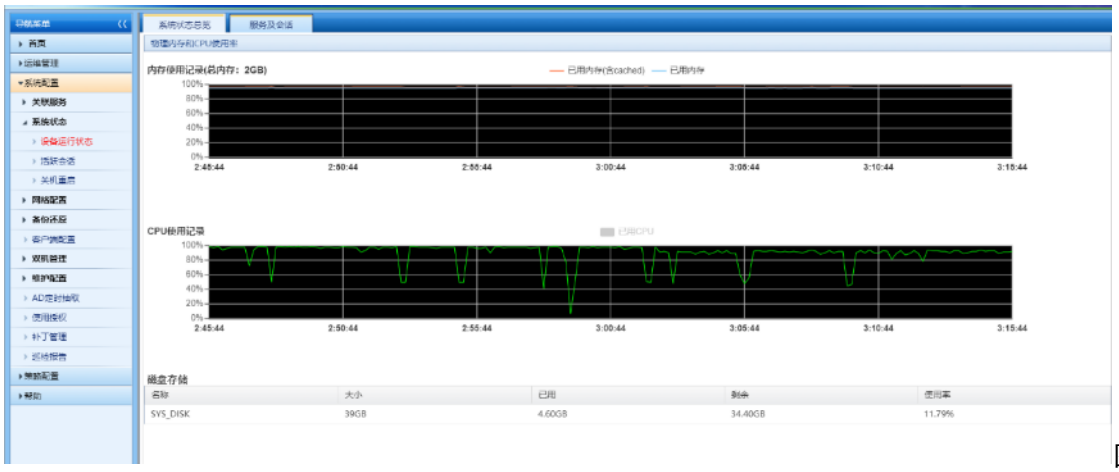


1.设备运行状态

设备运行状态分为系统状态总览和服务及会话。

使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->系统状态->设备运行状态链接进入设备运行状态界面。

系统状态总览包含了物理内存使用情况折线图，CPU 使用率折线图，磁盘存储的大小、已用、剩余和使用率。



图

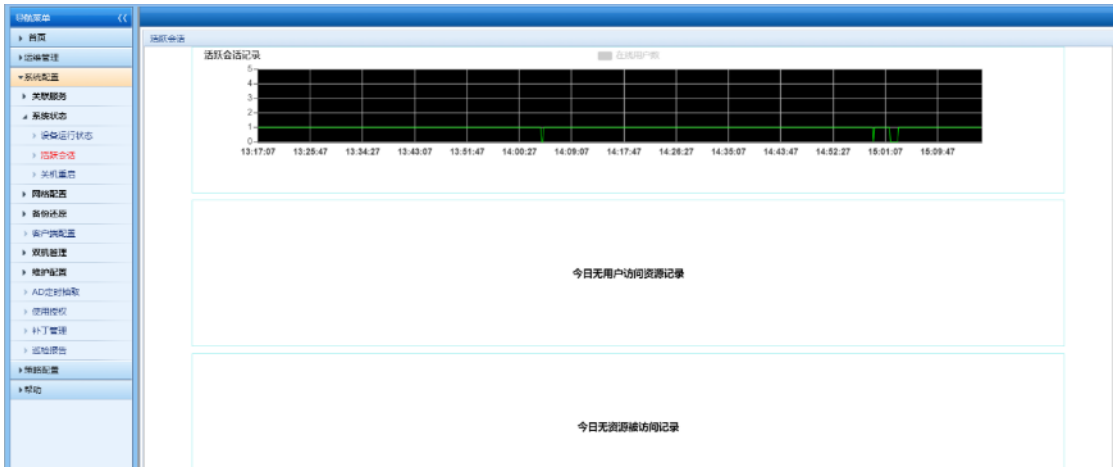
服务及会话中可以查看系统时间，系统连续运行时间，文件传输个数，字符个数，图形个数，审计服务状态。

图

2.活跃会话

活跃会话包含了活跃会话记录即在线用户数，当天用户的登录情况，用户访问资源状况，当天资源访问状况，资源被访问状况。

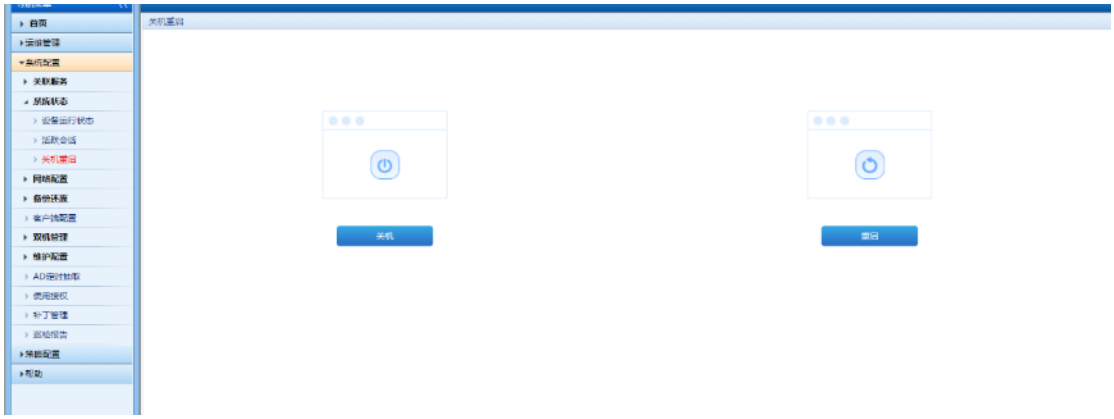
使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->系统状态->活跃会话链接进入活跃会话界面。



3.关机重启

关机重启的作用是关闭系统，重启系统。

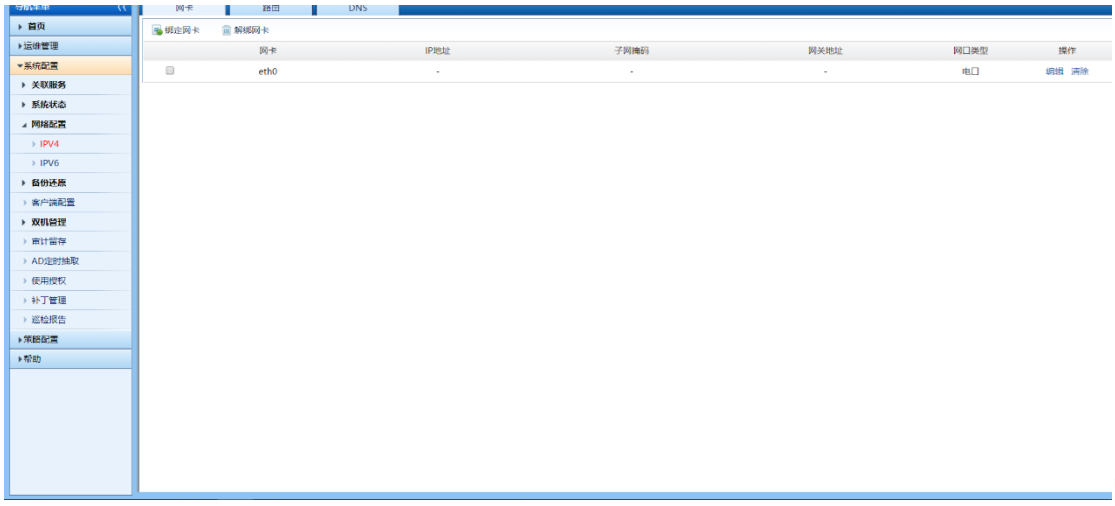
使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->系统状态->关机重启链接进入关机重启界面。



14.1.9. 网络配置

网络配置分为 IPV4 网卡配置和路由配置。

使用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->系统状态->网络配置链接进入网络配置界面。

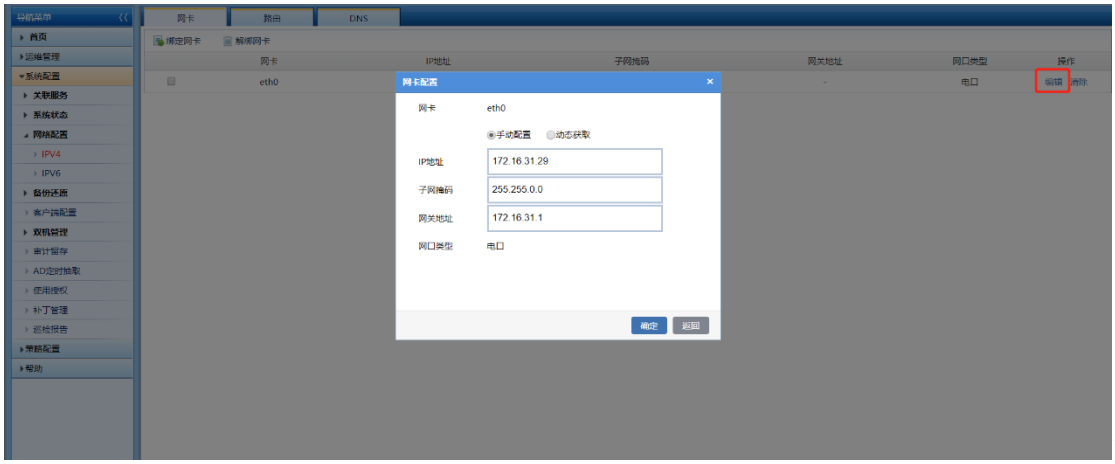


图

1.网卡配置

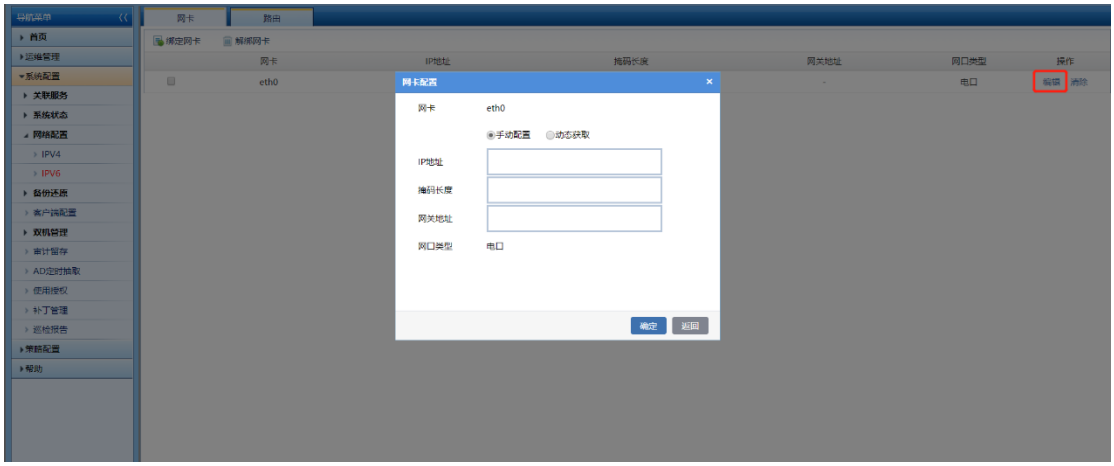
网卡配置是设置网卡的 IP 地址。

点击网卡配置链接进入网卡配置界面，点击编辑进行添加 IP 和网关。

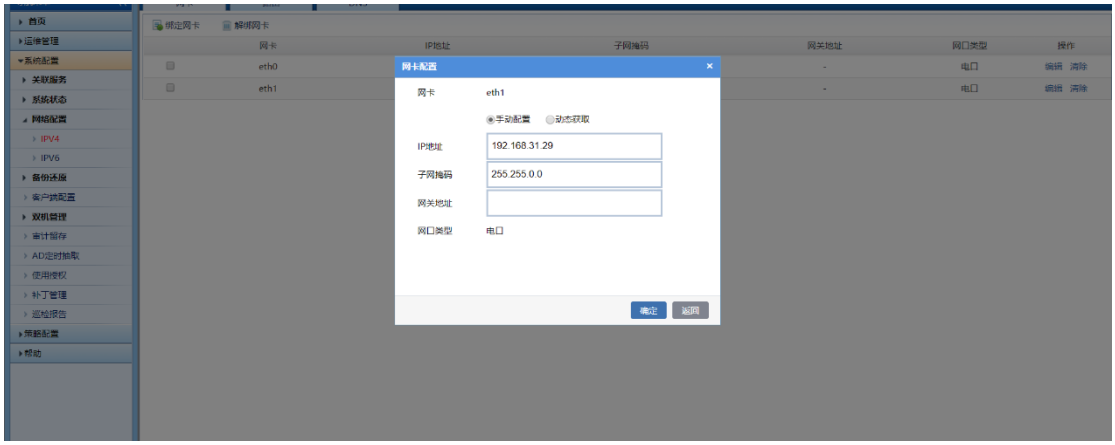


图

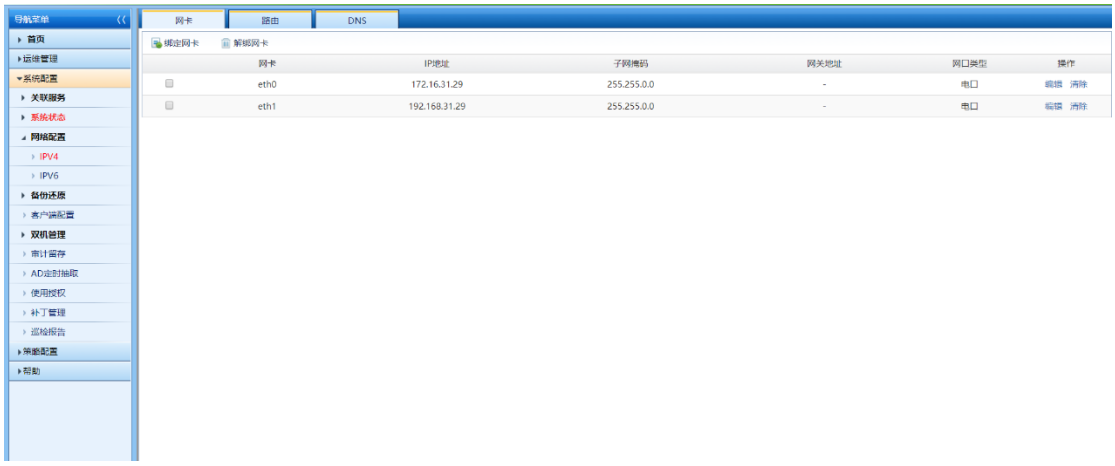
点击 IPv6 网卡配置，进入网卡配置界面，添加 IP 和网关即可设置网卡



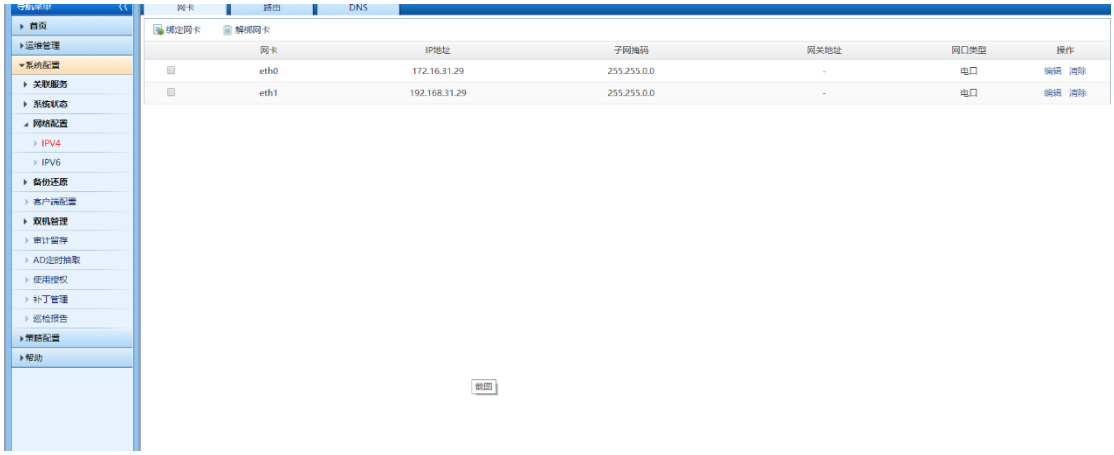
双网卡设置，点击新增网卡，在 eth1 中添加 IP



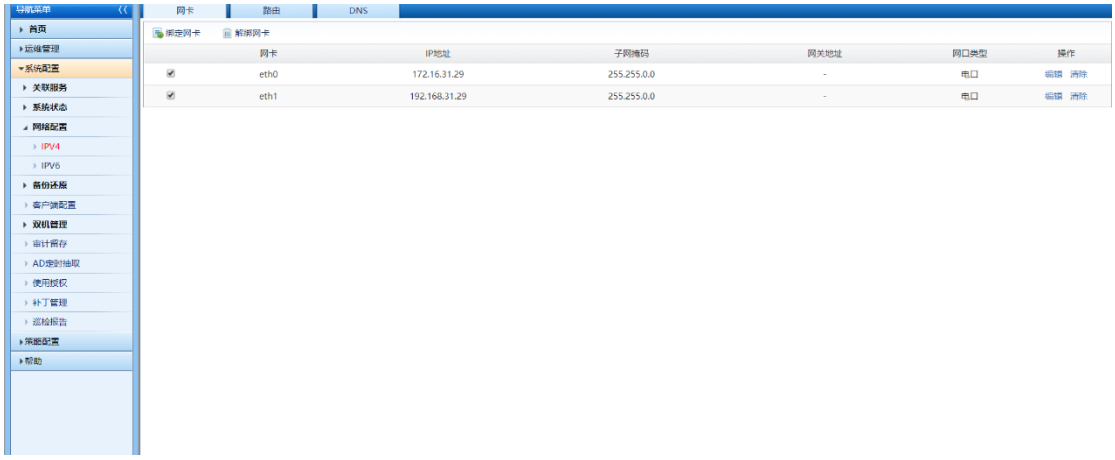
添加完成后点击设置网卡，第二个网卡添加完成



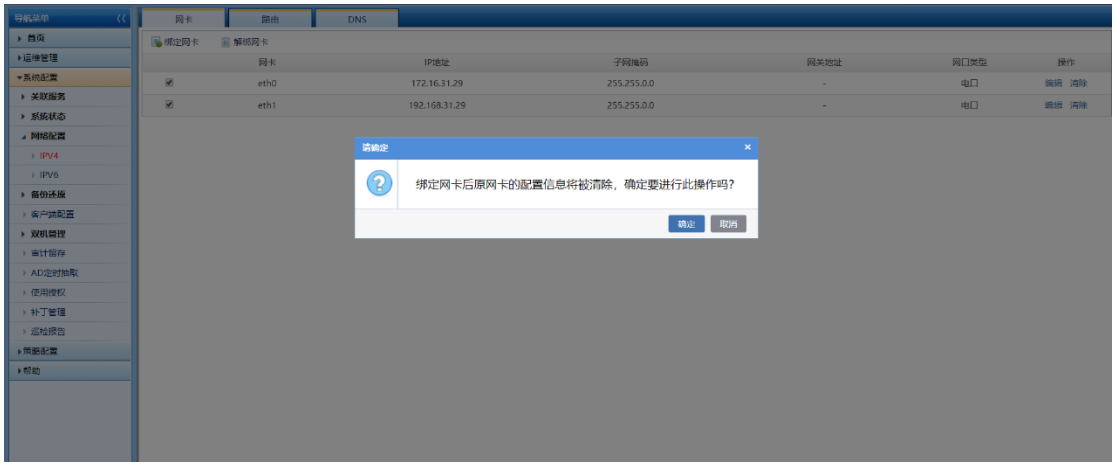
点击网卡绑定，在界面中绑定双网卡

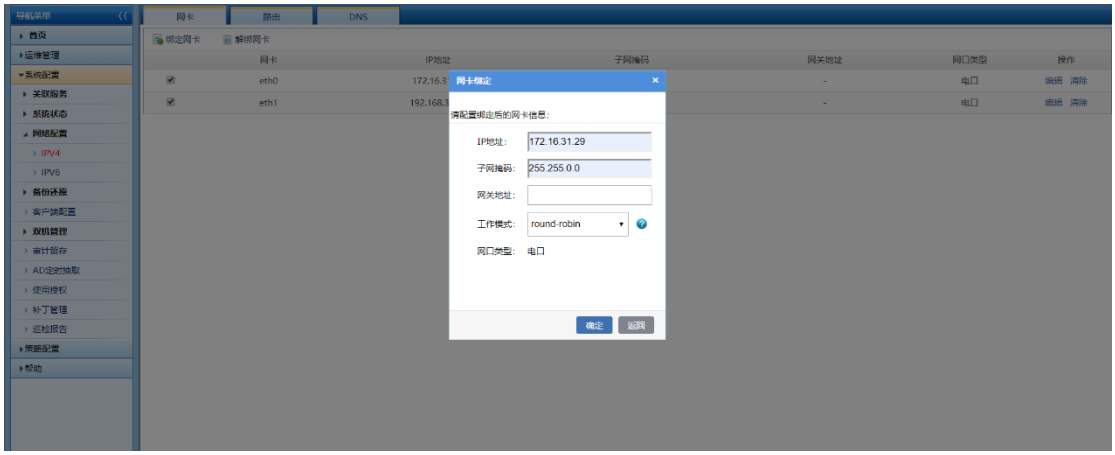


勾选 eth0 和 eth1 两个网卡，点击绑定进行双网卡绑定

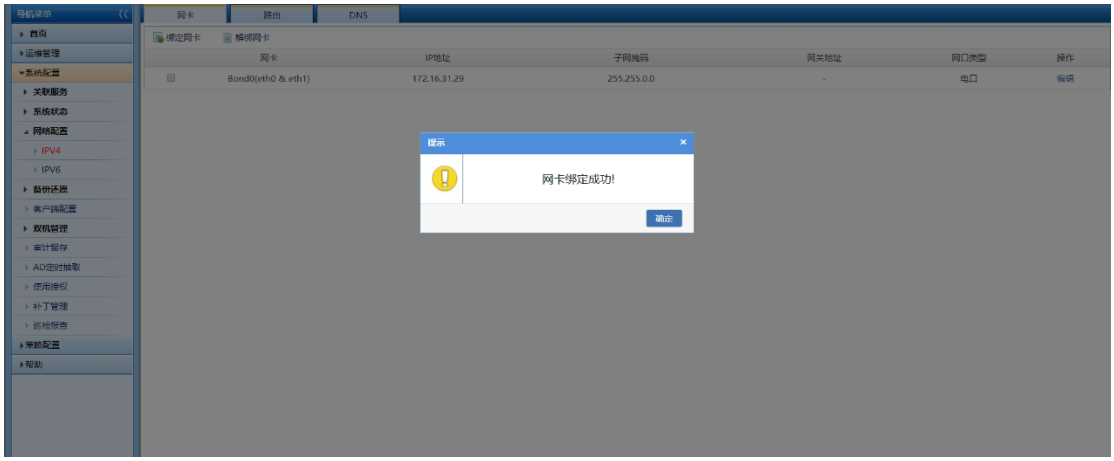


点击绑定会提示 绑定网卡后原网卡的配置信息将被清除，确定要进行此操作吗？点击确定弹出网卡绑定信息界面





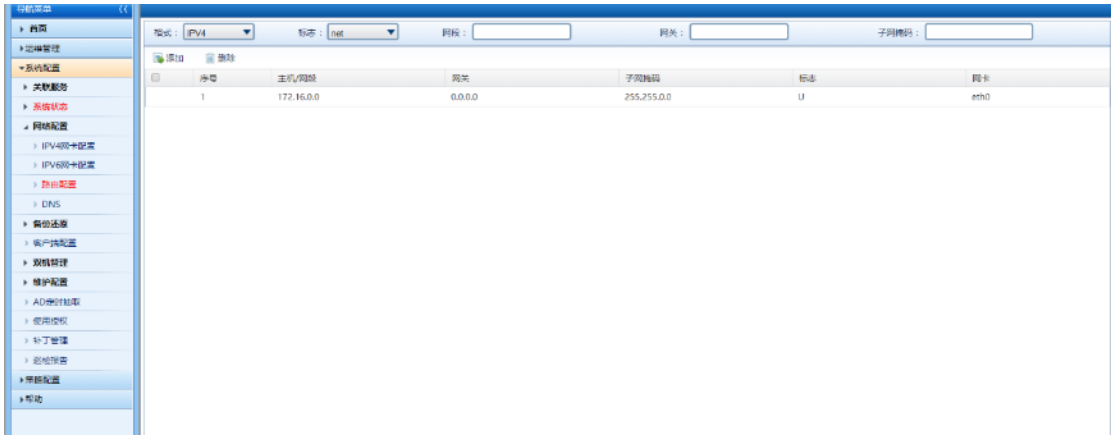
保存后界面弹出开始绑定网卡，绑定完成后将自动重启系统，至此双网卡绑定完成。



2.路由配置

路由配置是提供给用户自定义添加静态路由。

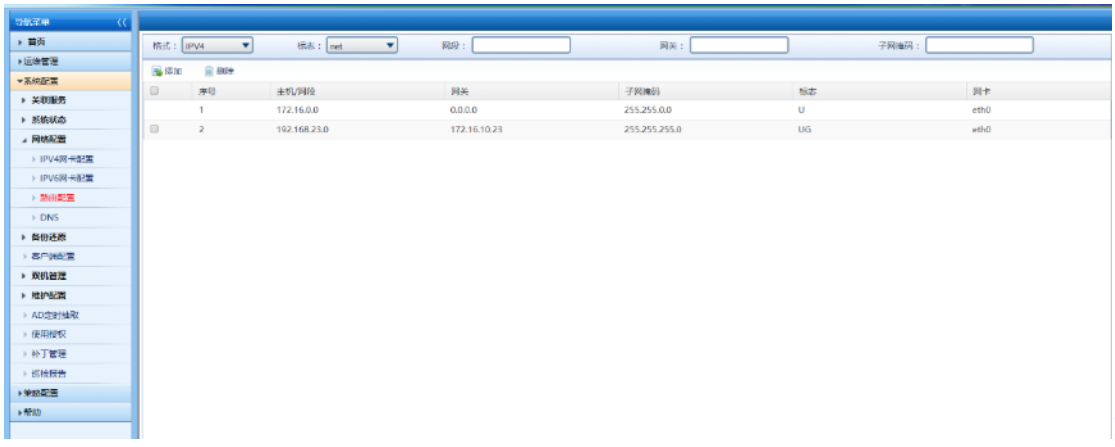
点击路由配置链接进入路由配置界面。



路由添加

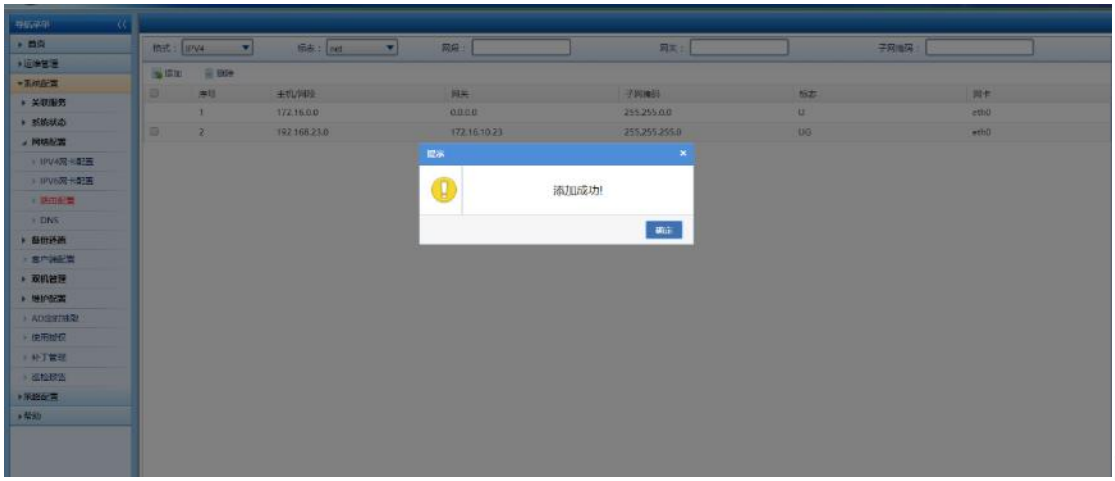
- net 类型

填写网段为 192.168.23.0，网关为 172.16.10.23，子网掩码为 255.255.255.0，点击添加。



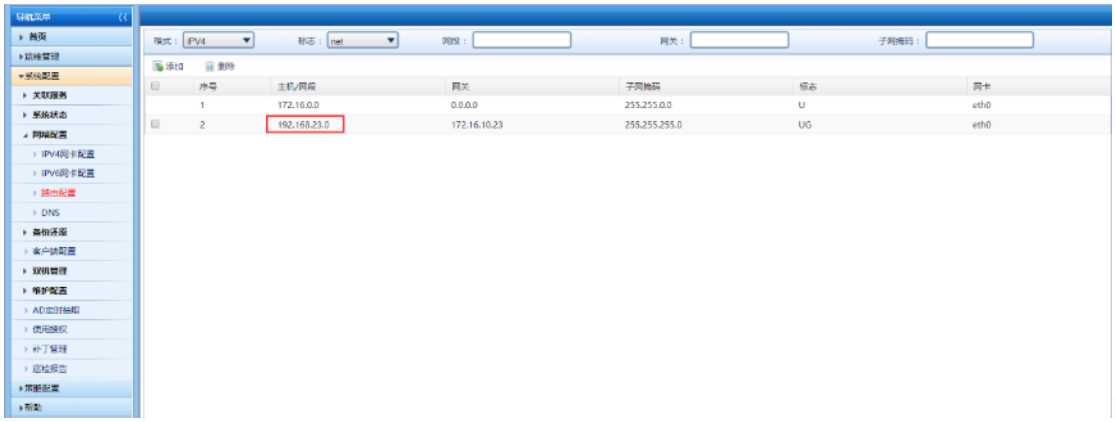
图

提示添加成功！



图

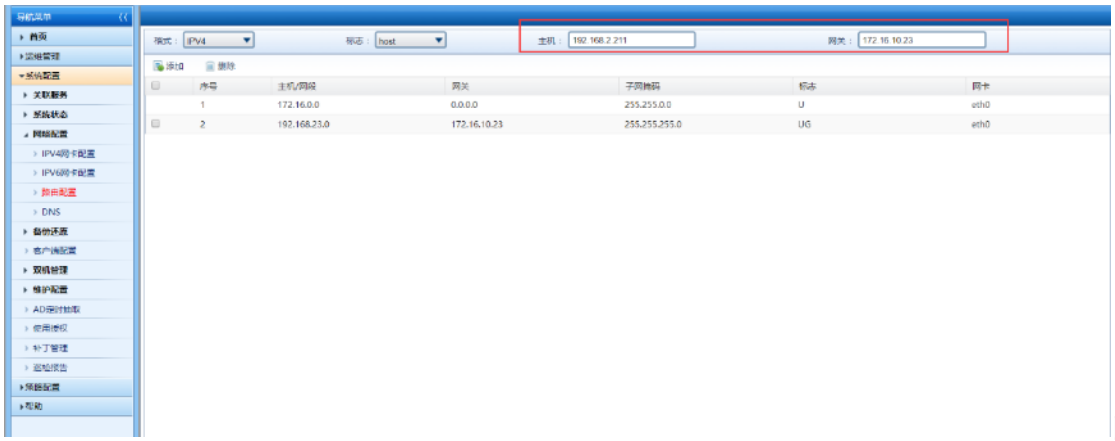
点击确定，路由列表中显示网段为 192.168.23.0 的路由。



图

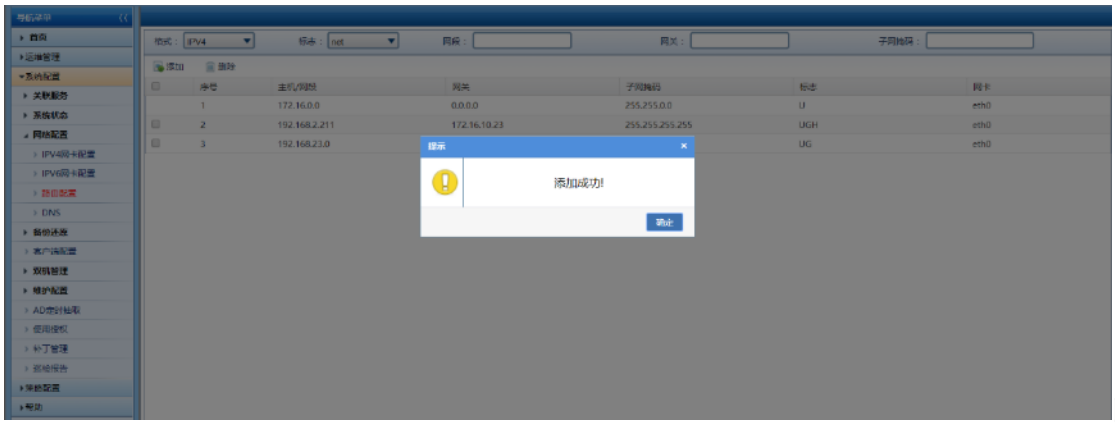
- host 类型

填写主机为 192.168.2.211，网关为 172.16.10.23，点击添加。



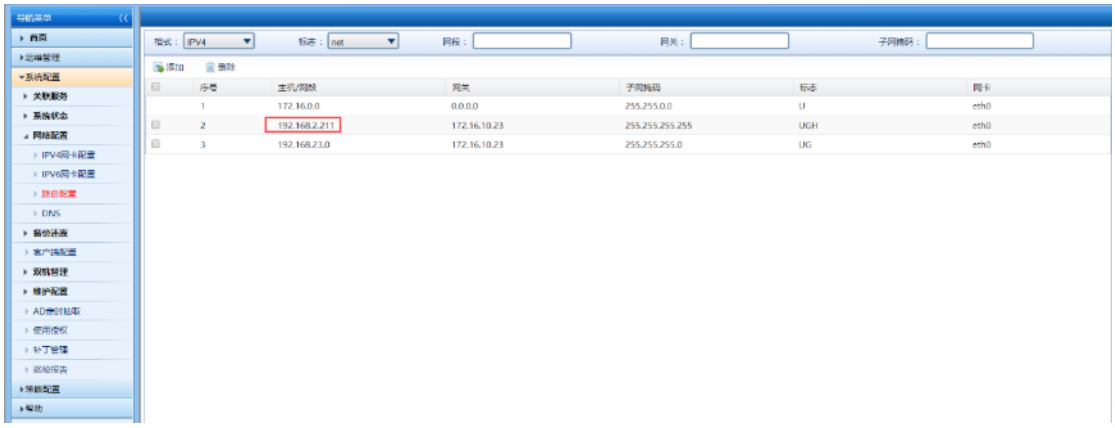
图

提示添加成功！



图

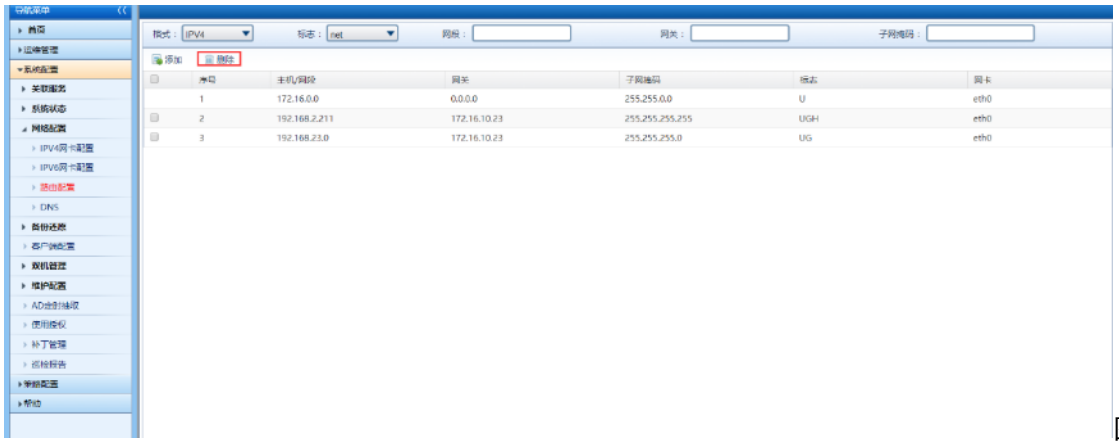
点击确定，路由列表中显示主机为 192.168.2.211 的路由。



图

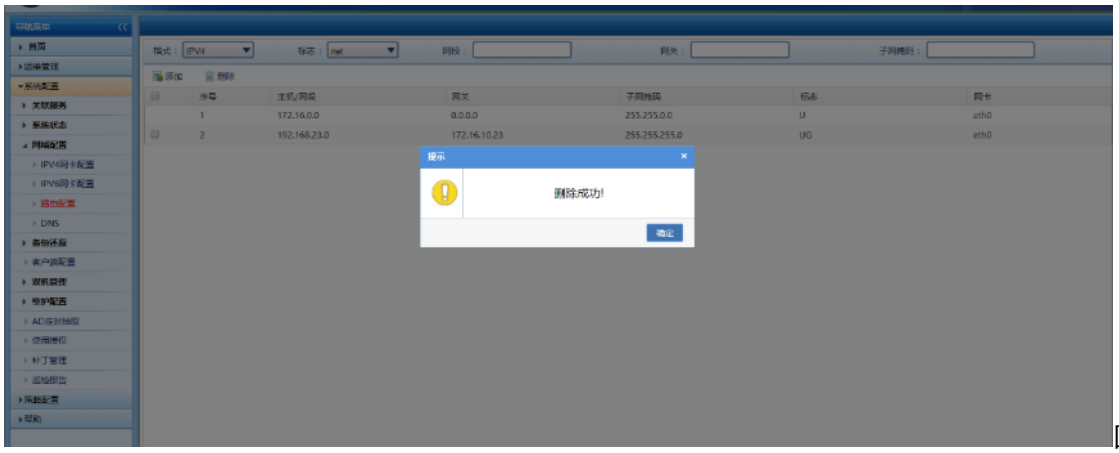
路由删除

在路由配置列表页面，勾选主机为 192.168.2.211 的**路由**，点击左上方**删除。**



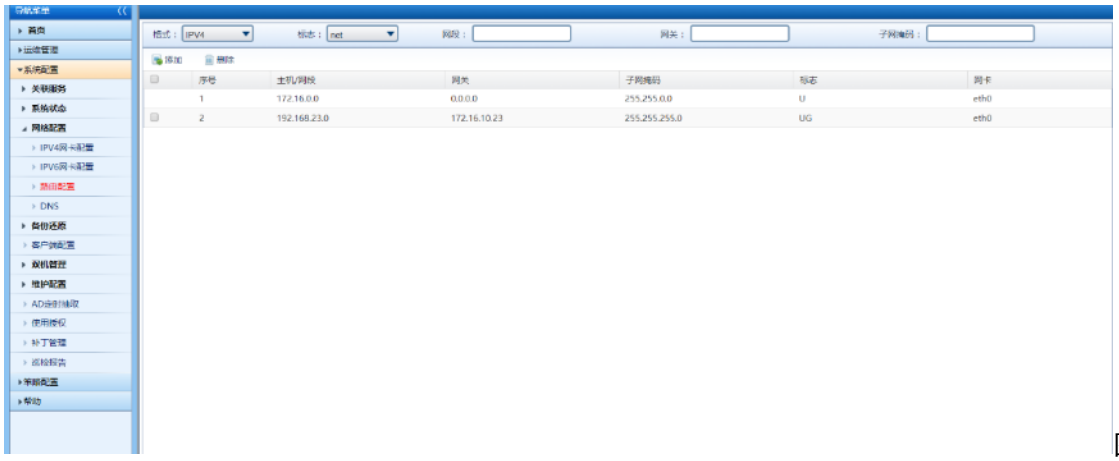
图

提示删除成功！



图

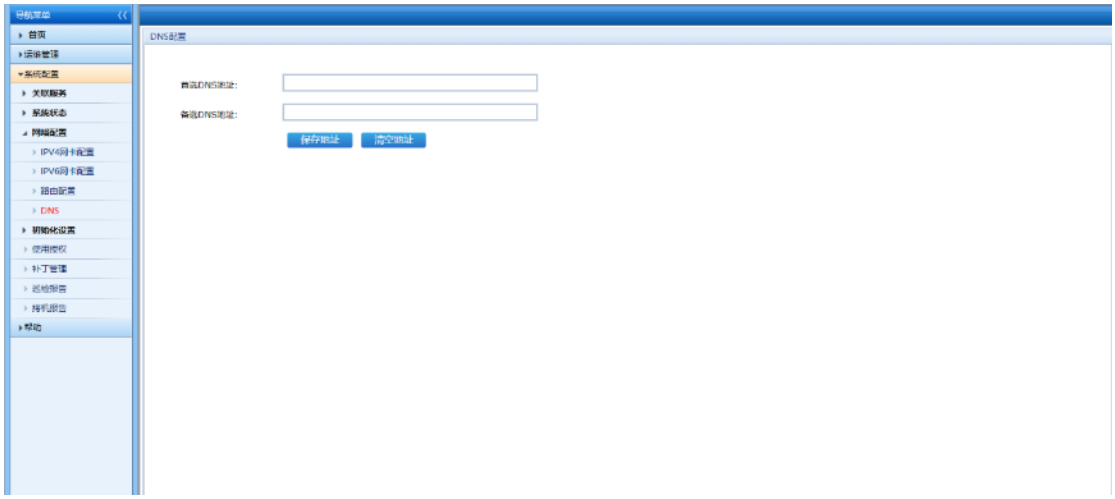
点击确定，路由列表中不显示主机为 192.168.2.211 的路由。



图

14.1.10. DNS 配置

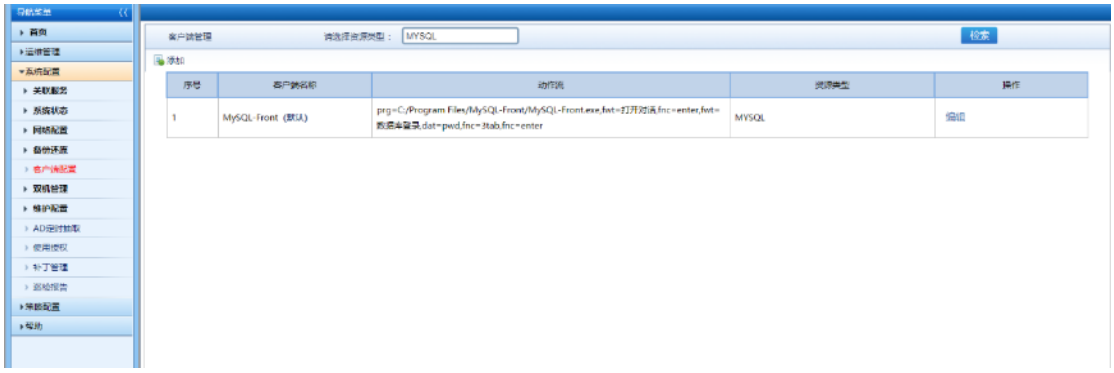
首选 DNS 地址配置：114.114.114.114，备选 DNS 地址配置：8.8.8.8



14.1.11. 客户端配置

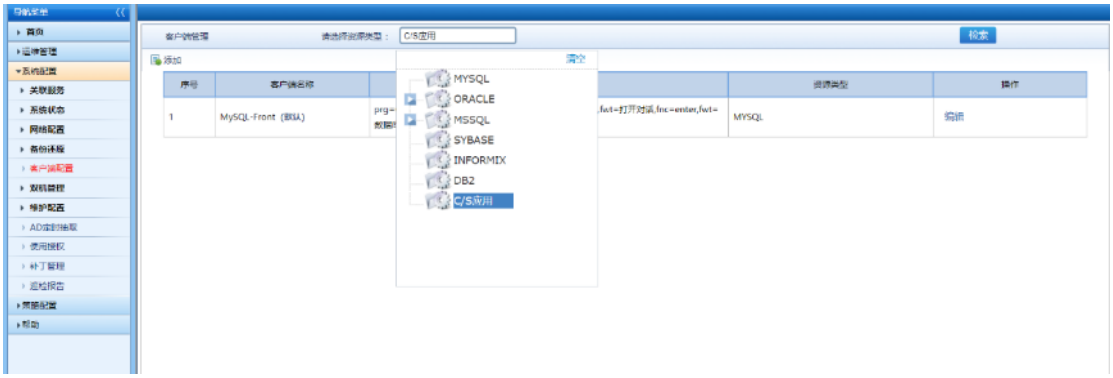
用户通过客户端配置可以自定义数据库、C/S、B/S 客户端的属性配置，形成有序的动作流，从而对资源进行运维操作。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->客户端配置链接进入客户端管理界面。

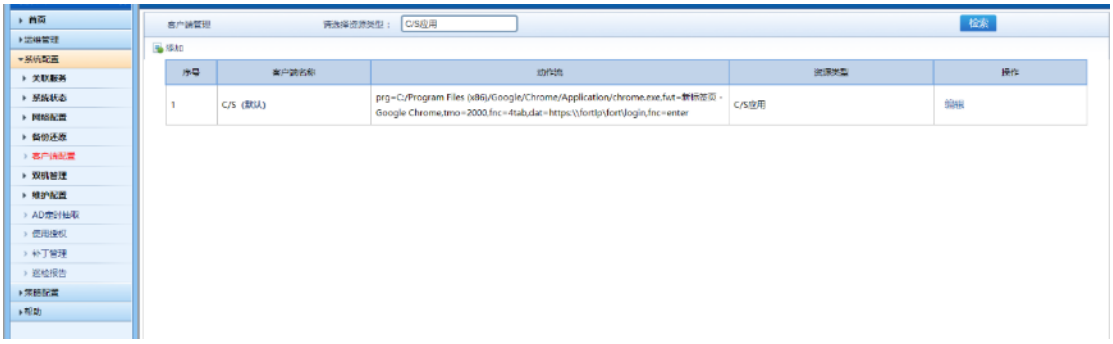


1.客户端配置-检索

可根据资源类型进行检索，选择 C/S 应用，点击检索按钮。



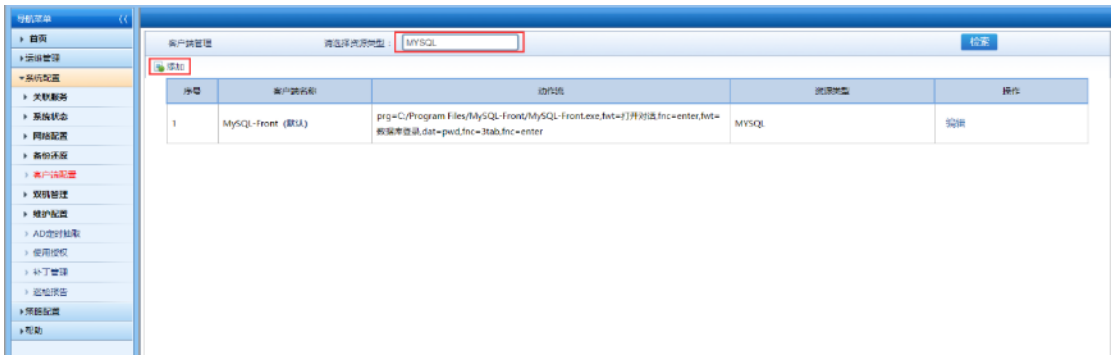
即可检索到 C/S 应用类型资源的客户端列表。



至此客户端配置检索功能完成。

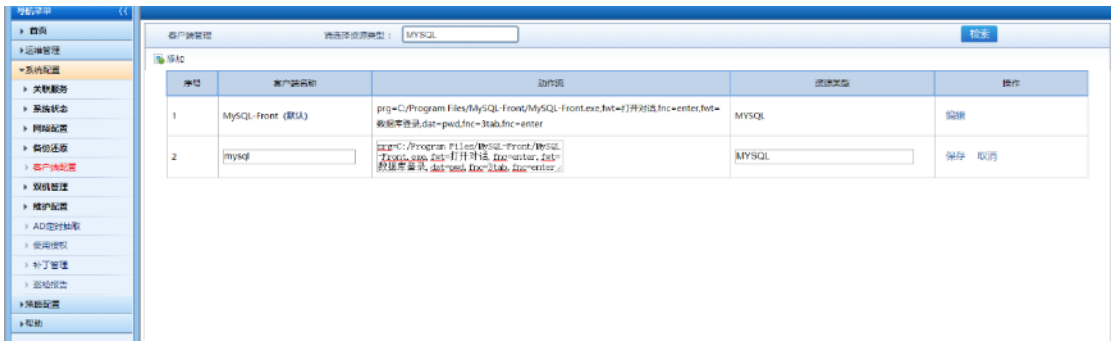
2.客户端配置-添加

在客户端管理界面，选择 MYSQL 资源类型，点击添加按钮。

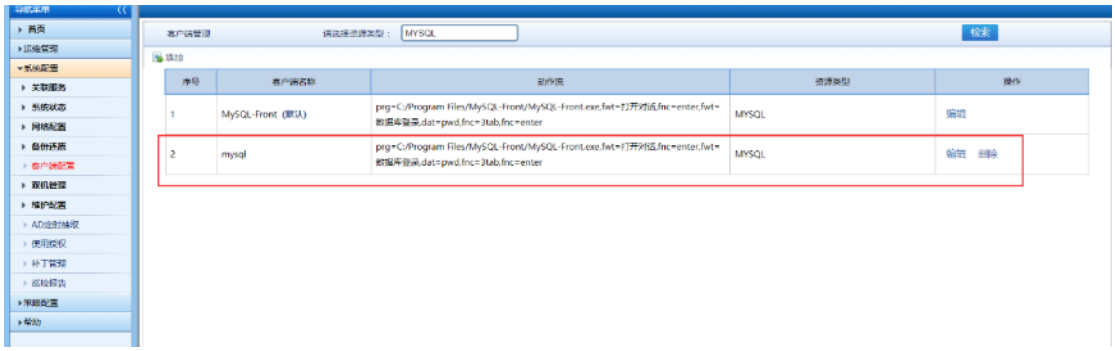


输入客户端信息：

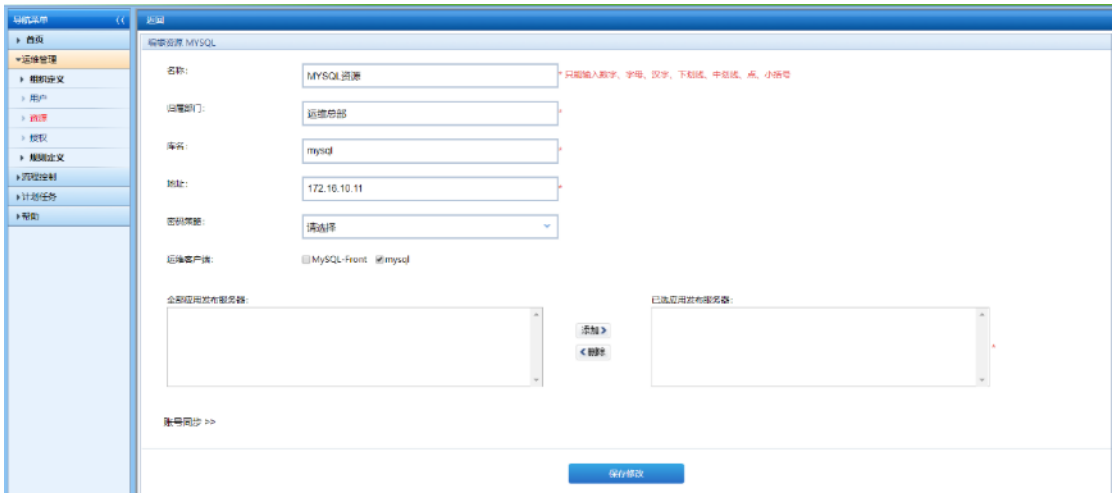
- 客户端名称：mysql
- 动作流：prg=C:/Program Files/MySQL-Front/MySQL-Front.exe,fwt=打开对话,fnc=enter,fwt=数据库登录,dat=pwd,fnc=3tab,fnc=enter
- 资源类型：MYSQL



点击保存按钮，MYSQL 客户端列表显示已添加的客户端 mysql。



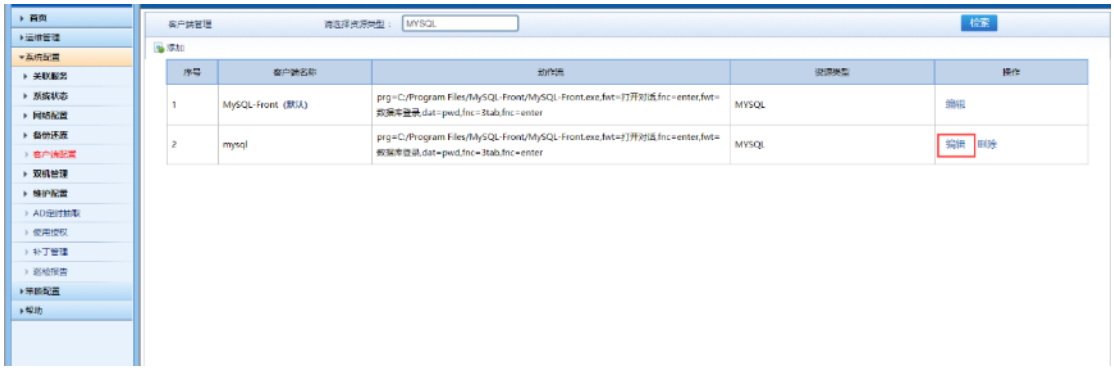
在添加 MYSQL 资源时即可勾选 mysql 客户端，用户对 MYSQL 类型资源进行运维操作。



至此客户端配置添加功能完成。

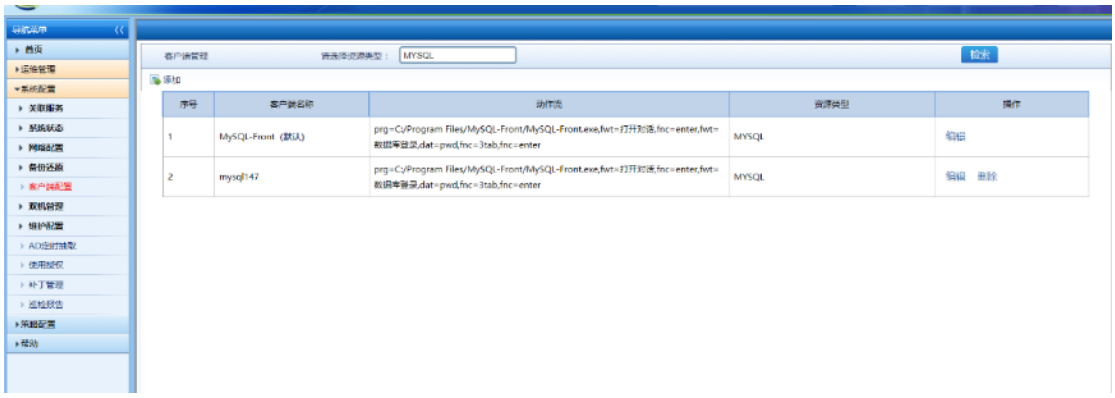
3.客户端配置-编辑

在客户端管理界面，选择 MYSQL 资源类型，点击 mysql 客户端的编辑按钮（当客户端在资源中已被勾选时，不能进行编辑）。



mysql 客户端即变为可编辑状态，可对客户端名称和动作流进行编辑，修改客户端名称为 mysql147。

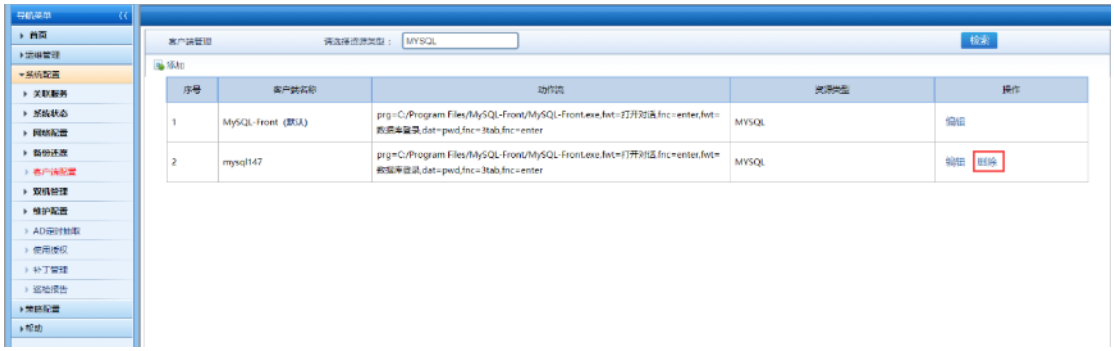
点击保存按钮，返回客户端管理页面，mysql 客户端名称由 mysql 变为 mysql147。



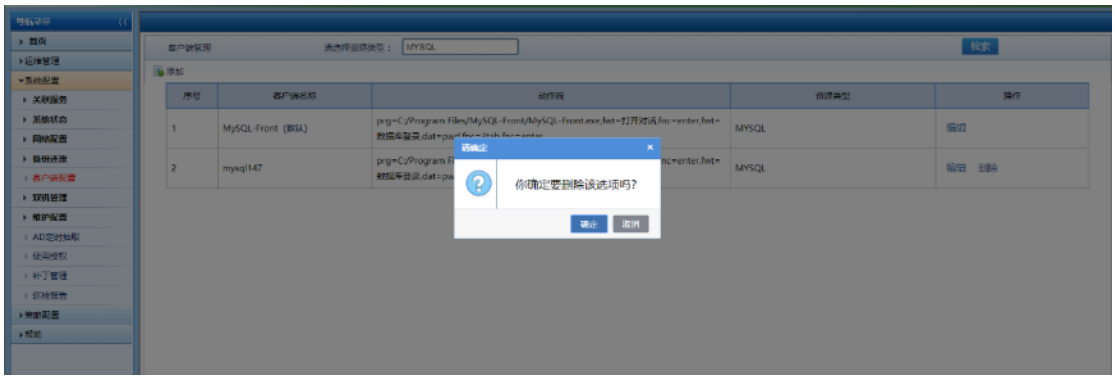
至此客户端配置编辑功能完成。

4.客户端配置-删除

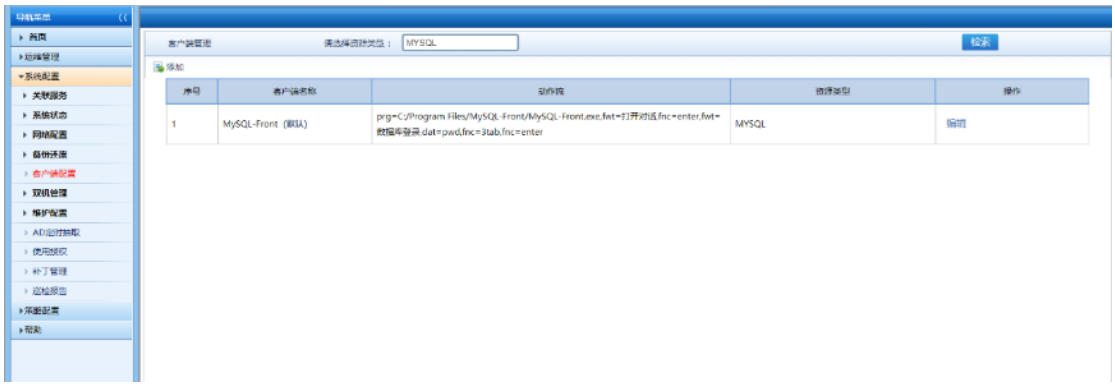
在客户端管理界面，选择 MYSQL 资源类型，点击 mysql147 客户端的删除按钮（当客户端在资源中已被勾选时，不能进行删除）。



弹出提示信息确定删除该选项吗？



点击确定按钮，返回客户端管理页面，不显示客户端 mysql147。



至此客户端配置删除功能完成。

14.1.12. 备份还原

备份还原功能是指将系统的系统配置、实体配置进行备份，在必要的时刻将已备份的文件进行还原。可通过立即备份、一次性备份、周期备份的方式将备份文件存储到本地或异地 FTP。

用系统管理员 sysAdmin 登录系统，切换至系统管理员角色，点击系统配置->备份还原链接进入备份还原界面。

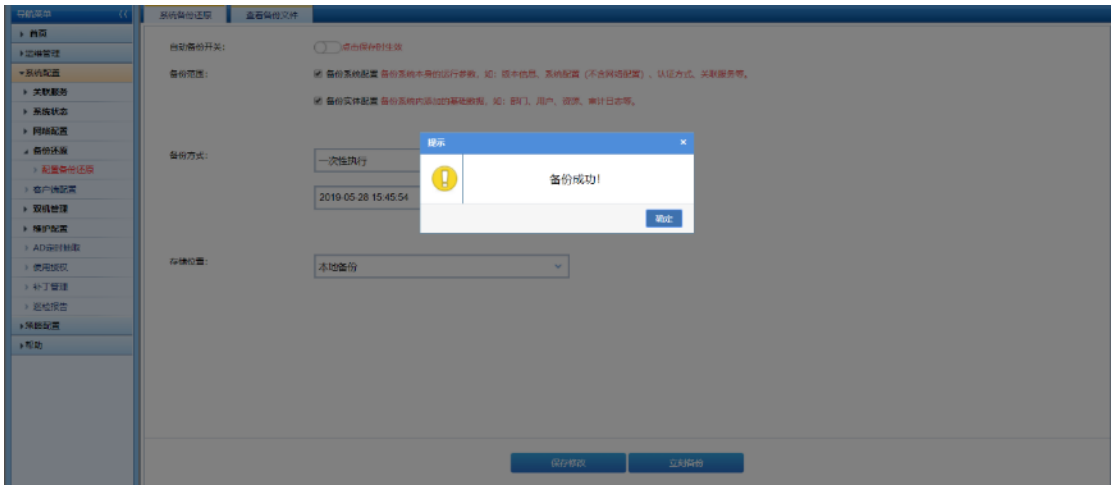
1.配置备份还原

配置备份还原主要包括：

1) 自动备份开关：ON/OFF
2) 备份范围：□备份系统配置、□备份实体配置
3) 备份方式：一次性执行、周期执行
4) 存储位置：本地备份、FTP 异地备份

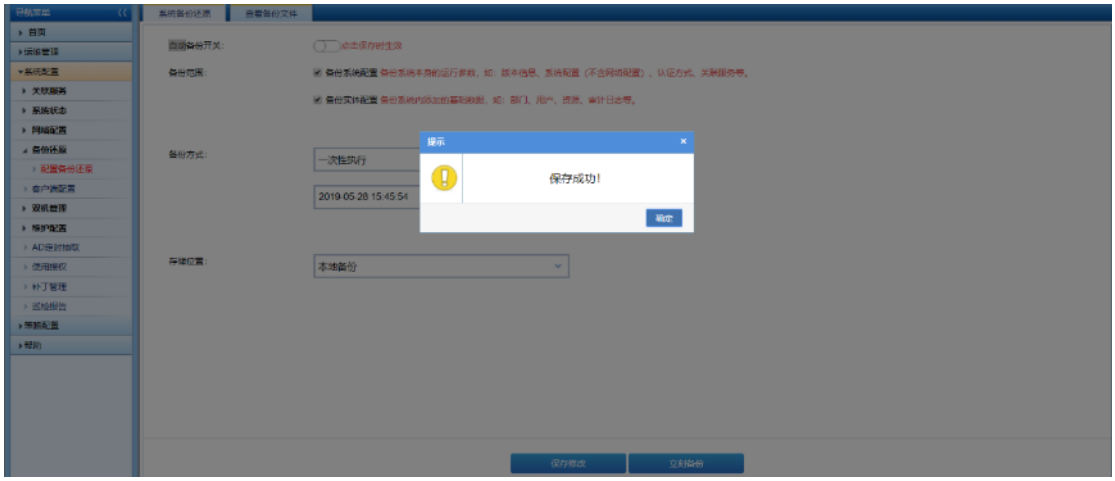
配置完成后若点击立即备份按钮，则按照当前配置直接备份。

弹出提示信息备份成功！



点击弹出框上的确定按钮，返回配置备份还原界面，点击查看备份文件，在备份文件列表显示备份文件内容。

配置完成后若点击保存按钮，弹出提示信息保存成功！则当前配置保存成功，后续会按照保存的配置内容执行一次性或周期性定时备份。



至此配置备份还原功能完成。

2.本地备份

存储位置选择本地备份，即将备份文件存储至系统硬盘内。

完成备份还原的其他配置，到达备份时间后，点击查看备份文件按钮，查看备份文件内容。

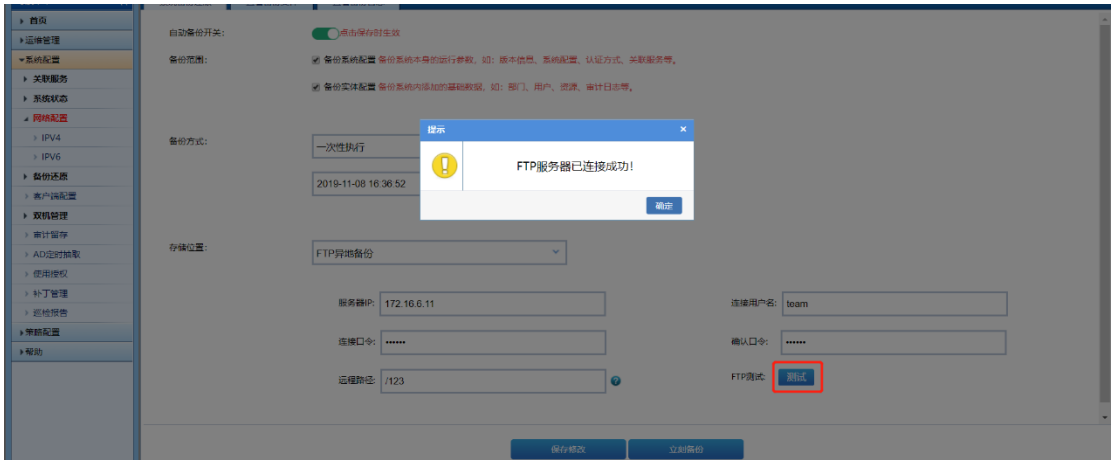
至此本地备份功能完成。

3.FTP 备份

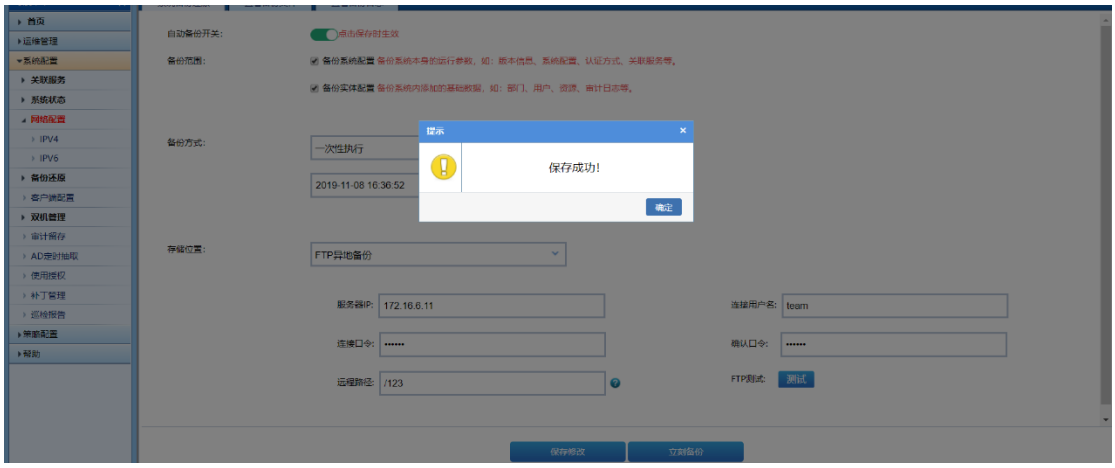
存储位置选择 FTP 异地备份，即将备份文件存储至远端 FTP 服务器上。配置远端 FTP 服务器：

1) 远程路径：/123
2) 服务器 IP：172.16.6.11
3) 连接用户名：team
4) 连接口令：123456

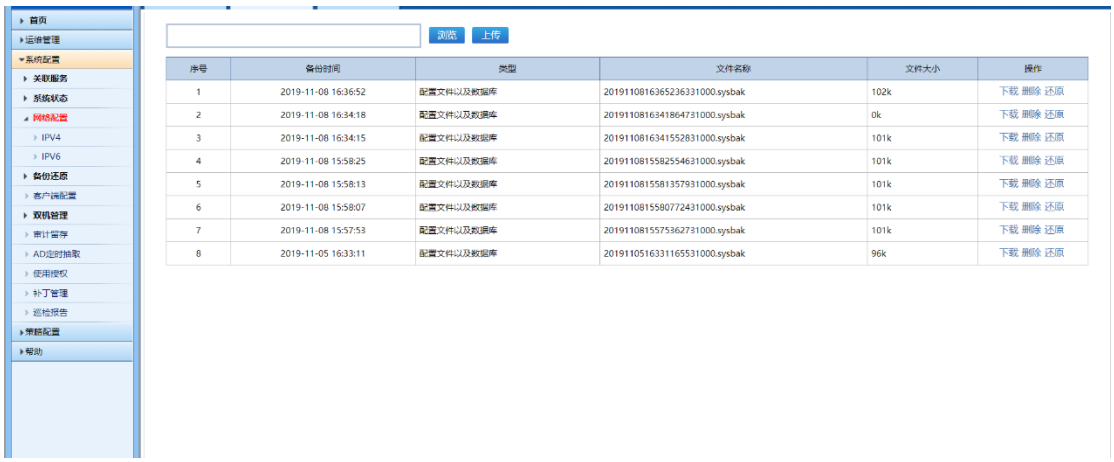
点击测试按钮，测试 FTP 服务器连接是否成功



配置完成后，点击保存按钮，弹出提示信息保存成功！



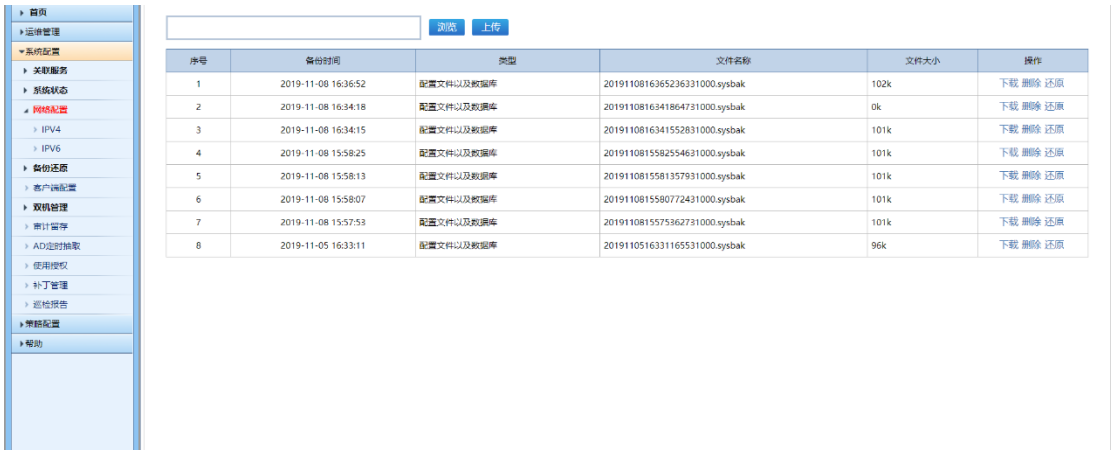
点击弹出框上的确定按钮，返回配置备份还原界面。到达备份时间后，点击查看备份文件按钮，查看备份文件列表内容。



在远端 FTP 服务器也可查看到备份文件，至此 FTP 备份功能完成。

4.备份恢复

在配置备份还原界面，点击查看备份文件按钮，跳转到备份文件列表页面。

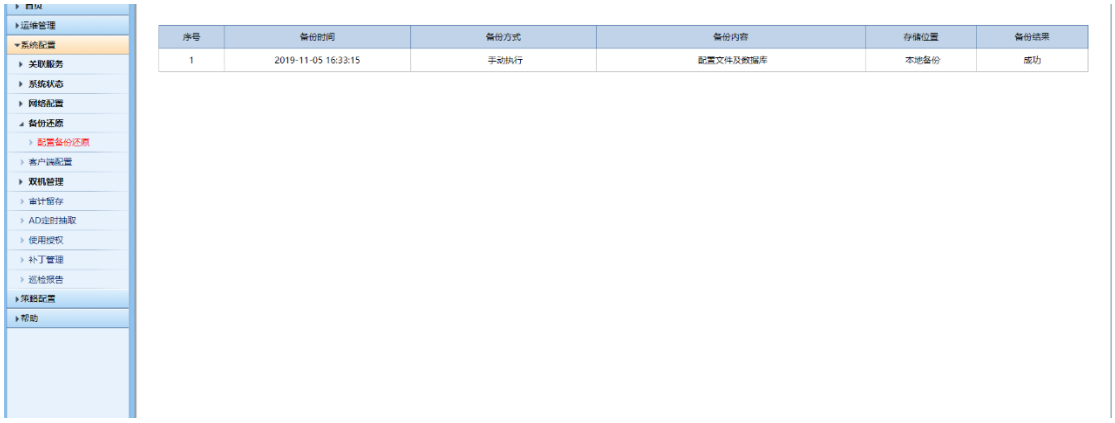


点击还原按钮，即可将当前系统的系统配置/实体配置还原到备份文件时的状态。

至此备份恢复功能完成。

5.查看备份日志

在查看备份日志界面，备份日志页面显示一条数据“备份时间、备份方式、备份内容、存储位置、备份结果”的数据。



14.1.13. 维护配置

维护配置整合为审计留存一个模块

审计留存是指系统硬盘使用率到达一定百分比时对运维审计文件进行删除的操作。

删除的类型有：

- 不再生成新纪录的运维审计文件
- 删除最早一个月的运维审计文件
- 删除最早一天的运维审计文件
- 删除最早一个会话的运维审计文件

审计存储扩展是将系统的录像存储在存储服务器上。

存储类型有：

- Windows
- Linux
- ISCSI

归档配置是将运维审计进行自动归档操作。

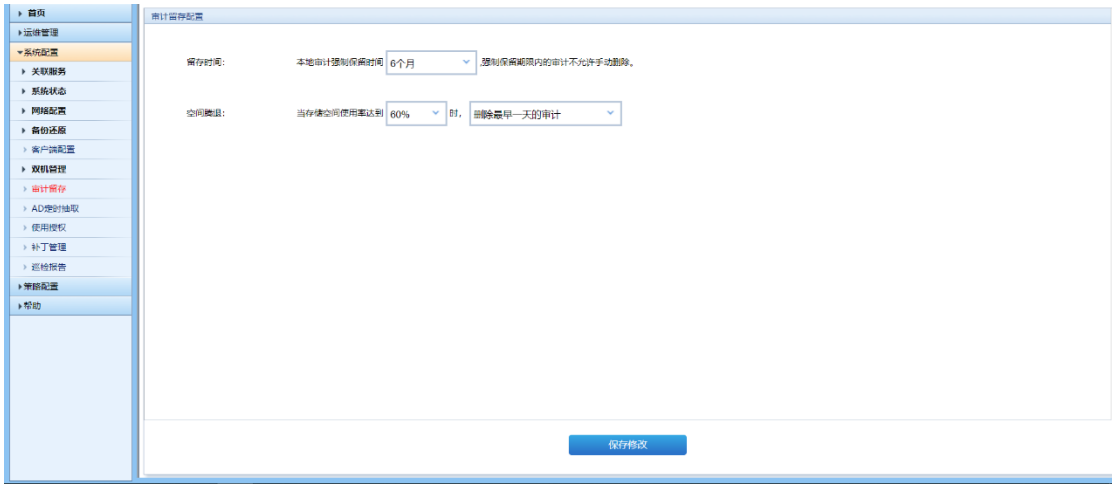
执行方式有：

- 每天执行
- 阈值触发

- 一次性归档

1.审计留存

用系统管理员 sysAdmin 登陆系统，切换至系统管理员角色，点击系统配置->维护配置->审计留存链接进入审计留存界面。

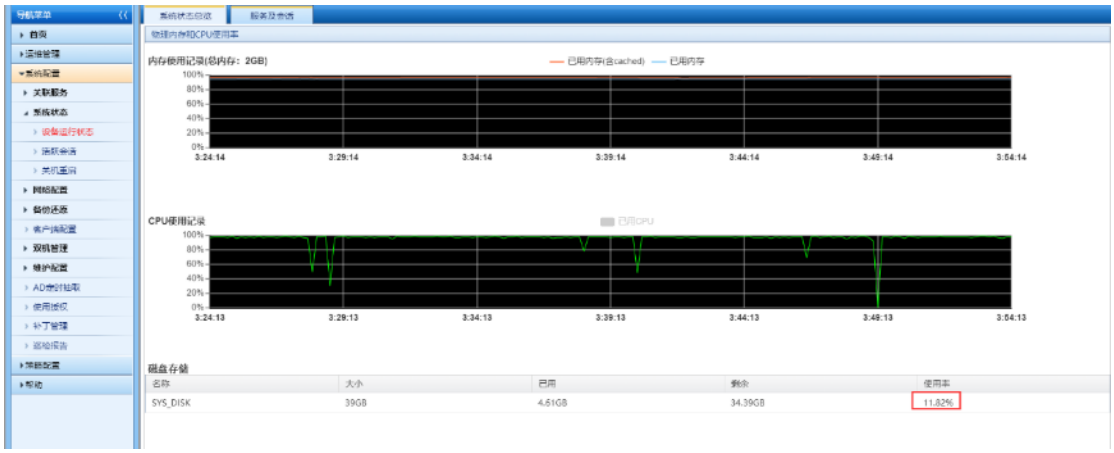


（1）不再生成新纪录的运维审计文件

不再生成新纪录的运维审计文件是指当硬盘使用率达到设置的百分比时不再生成新的运维审计文件（设置的百分比必须比告警配置中硬盘告警百分比大）。

具体操作如下：

点击系统配置->系统状态->设备运行状态可查看硬盘的使用率。



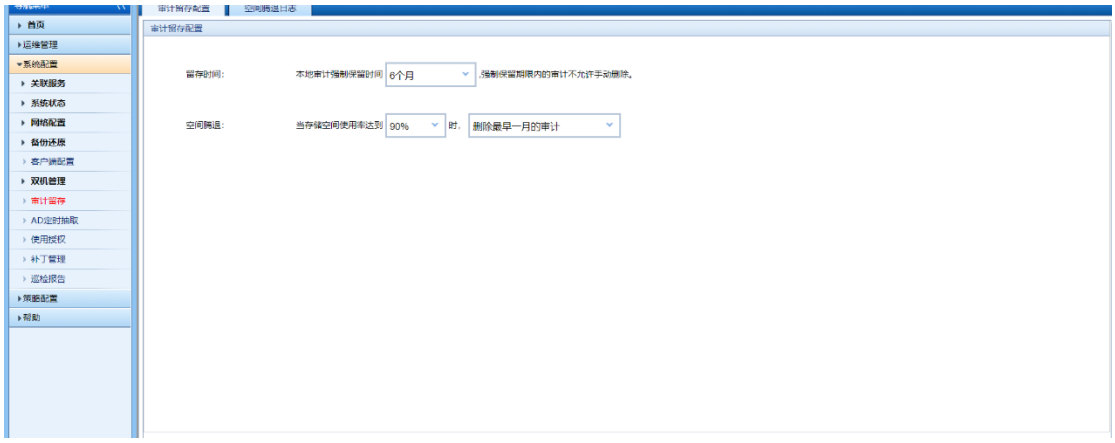
（2）删除最早一个月的运维审计文件

删除最早一个月的运维审计文件是指当硬盘使用率达到设置的百分比时从最早一个月开始按月删除运维审计文件（设置的百分比必须比告警配置中硬盘告警百分比大）。

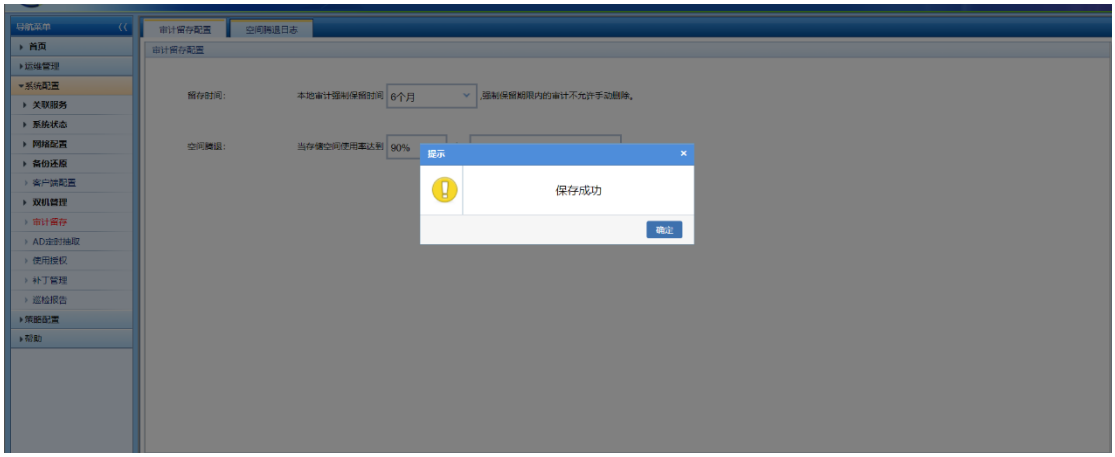
具体操作如下：

点击系统配置->系统状态->设备运行状态可查看硬盘的使用率。

当硬盘使用量达到硬盘总量 90%时，删除最早一个月的运维审计文件。



点击保存，提示保存成功。

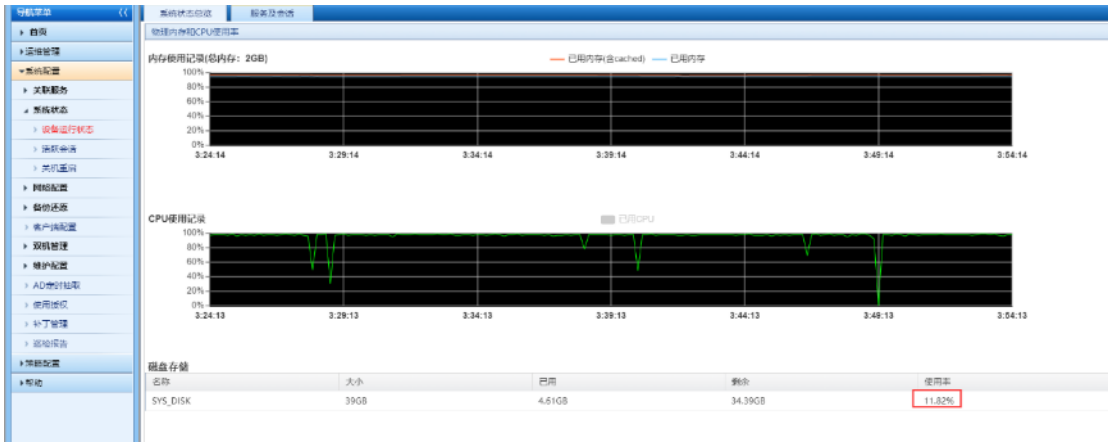


（3）删除最早一天的运维审计文件

删除最早一天的运维审计文件是指当硬盘使用率达到设置的百分比时从最早一天开始按天删除运维审计文件（设置的百分比必须比告警配置中硬盘告警百分比大）。

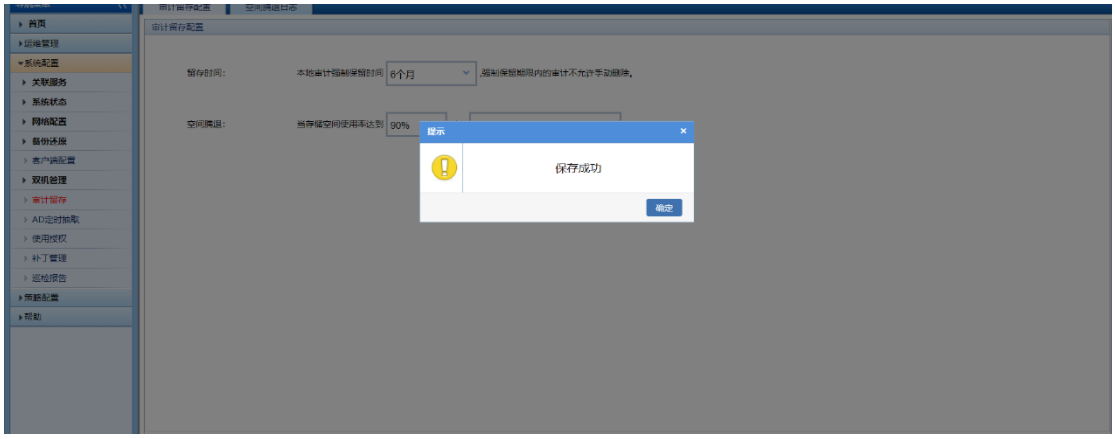
具体操作如下：

点击系统配置->系统状态->设备运行状态可查看硬盘的使用率。



当硬盘使用量达到硬盘总量 90%时，删除最早一天的运维审计文件。

点击保存，提示保存成功。



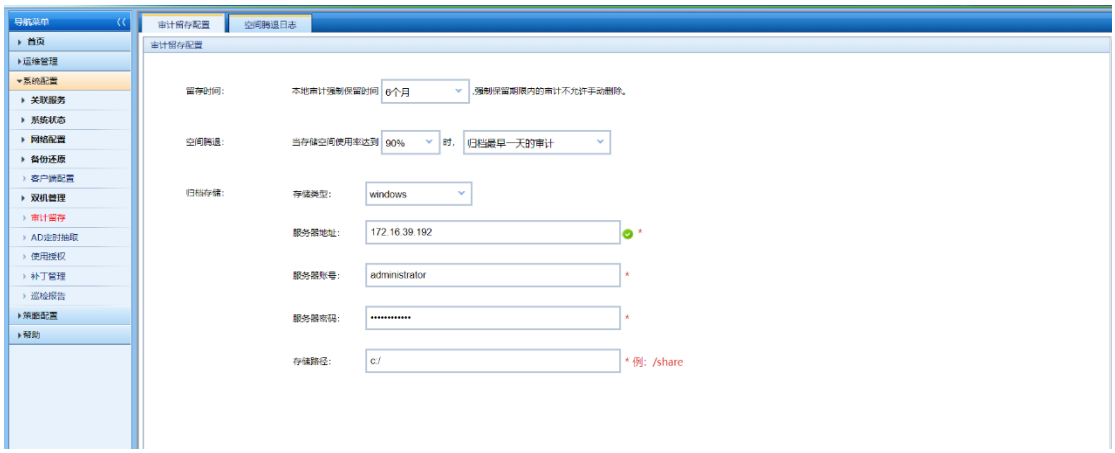
（4）归档最早一个会话的运维审计文件

归档最早一个会话的运维审计文件是指当硬盘使用率达到设置的百分比时从最早一个会话开始归档运维审计文件（设置的百分比必须比告警配置中硬盘告警百分比大）。

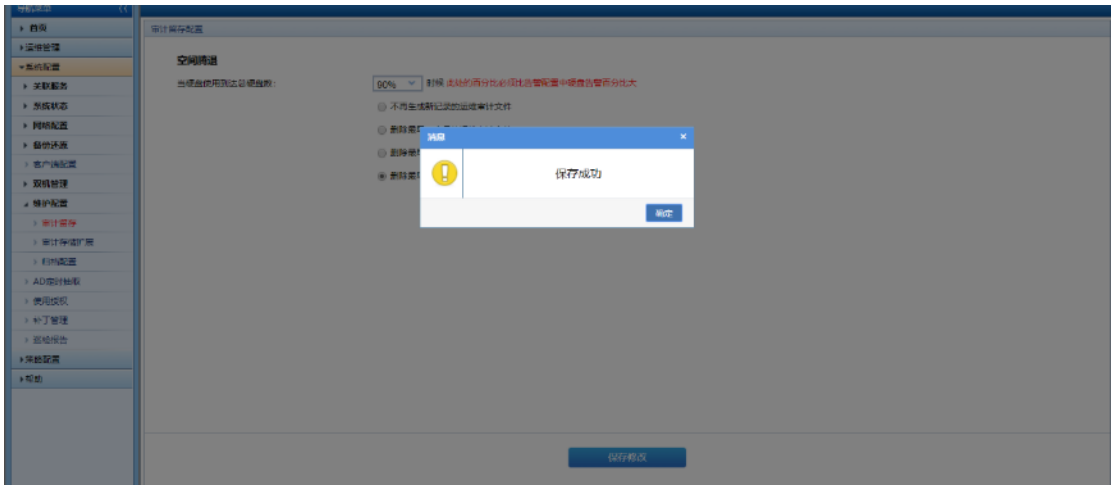
具体操作如下：

点击系统配置->系统状态->设备运行状态可查看硬盘的使用率。

当硬盘使用量达到硬盘总量 90%时，归档最早一个会话的运维审计文件。



点击保存，提示保存成功。

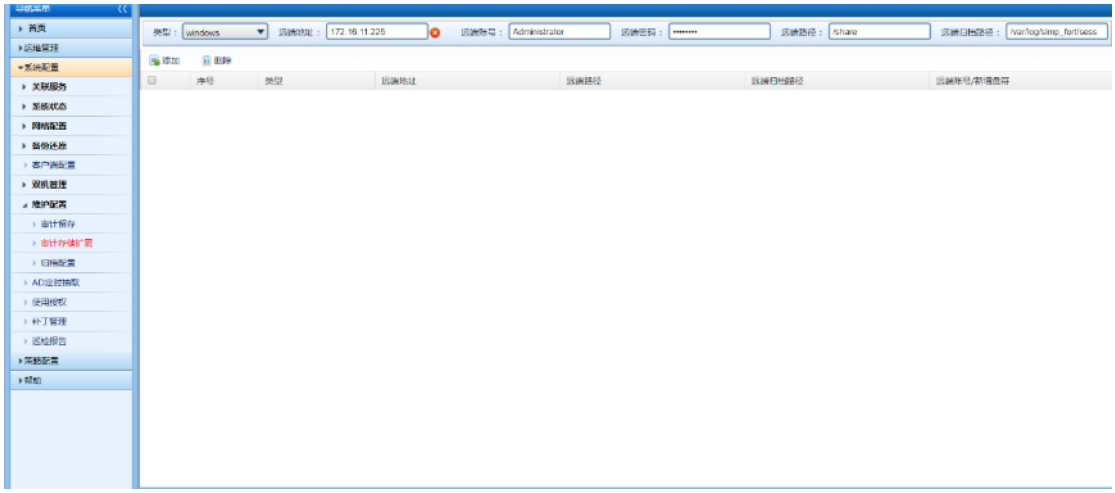


（5）存储类型-windows

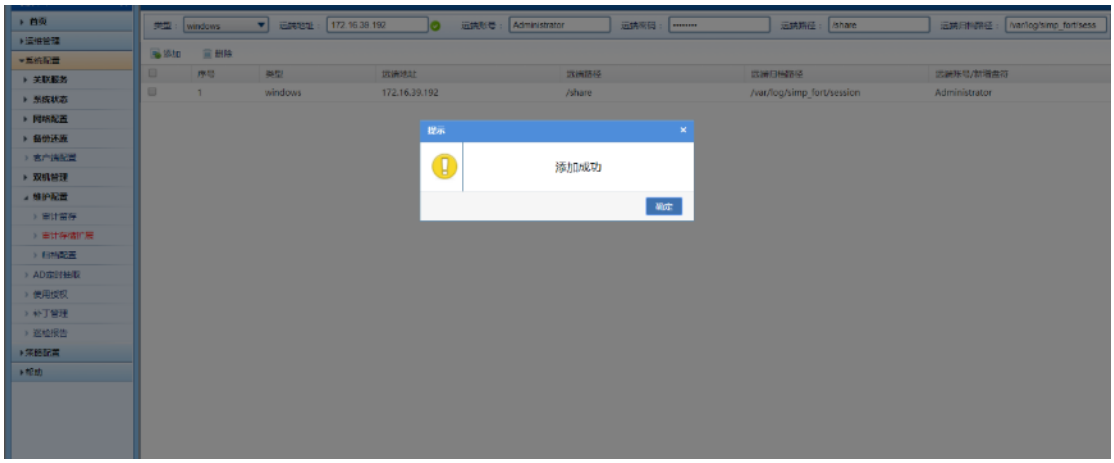
➢ 添加 windows 存储类型

Windows 存储类型基本信息如下：

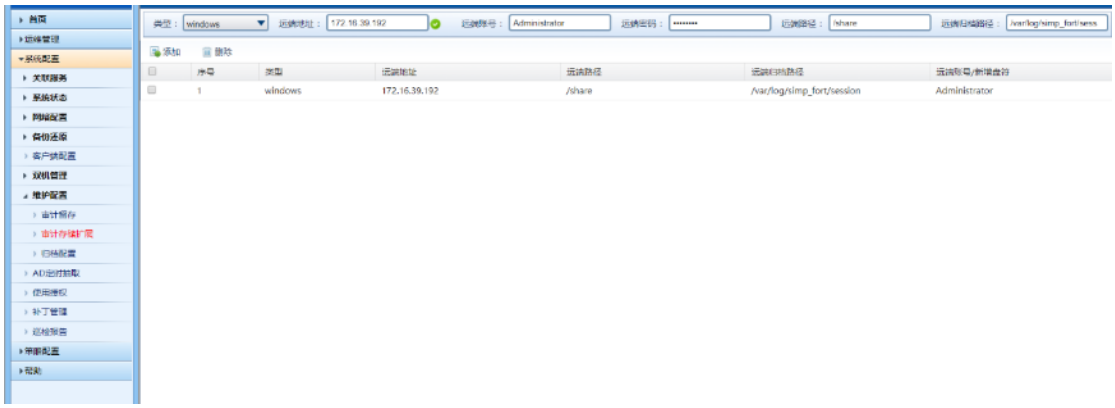
- 类型：windows
- 远端 IP：172.16.11.225（此 IP 为 windows 类型存储服务器 IP）
- 远端账号：Administrator
- 远端密码：admin123
- 远端路径：/share（此路径为存储服务器上存录像文件路径）
- 远端归档路径：/share/guidang（此路径为存储服务器上存归档录像文件路径）



点击添加，提示添加成功。

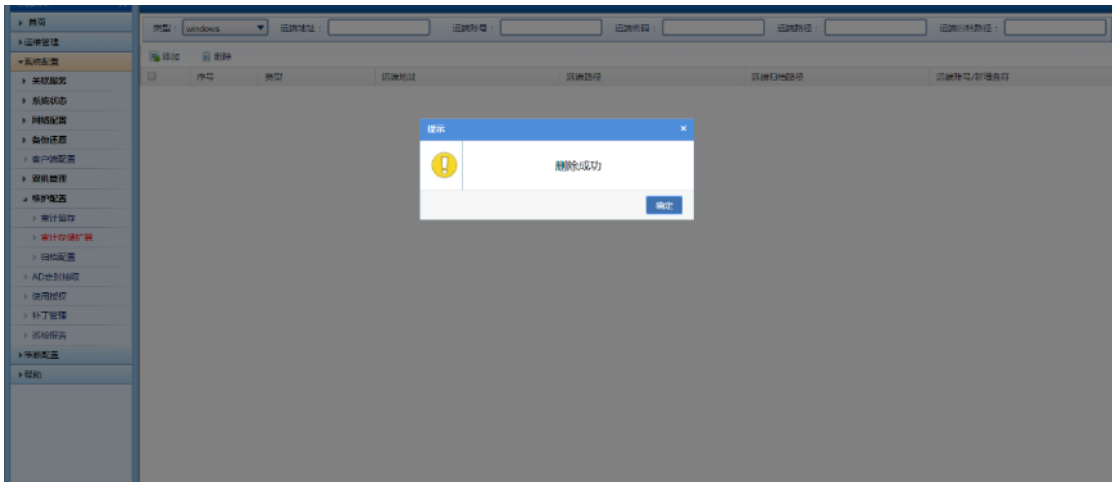


点击确定，列表页显示添加的 windows 类型的外接存储。

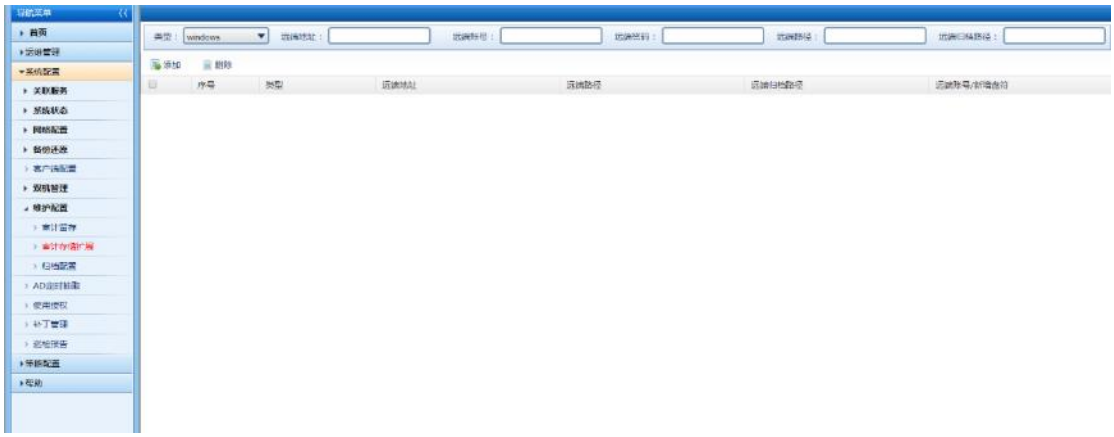


➢ 删除 windows 存储类型

选中 windows 类型的存储，点击删除，提示删除成功。



点击确定，列表页不显示 windows 类型外接存储的条目。

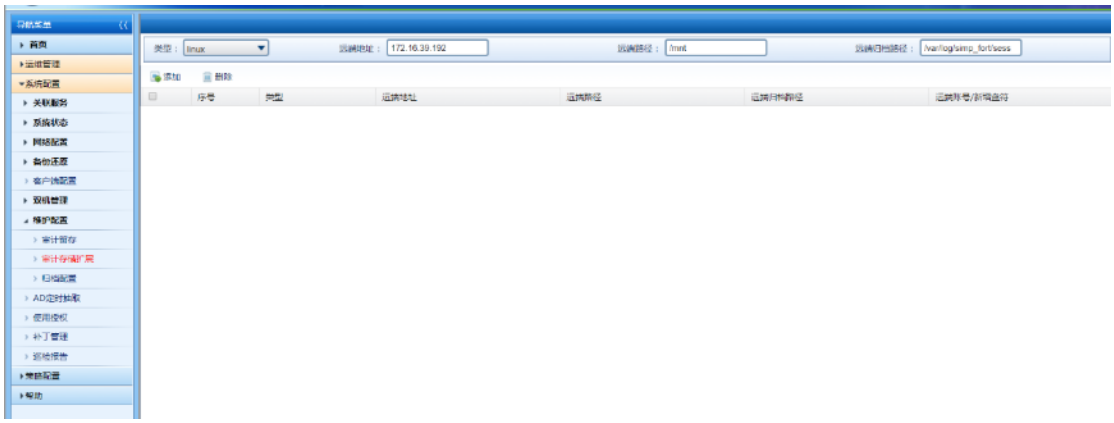


（6）存储类型-linux

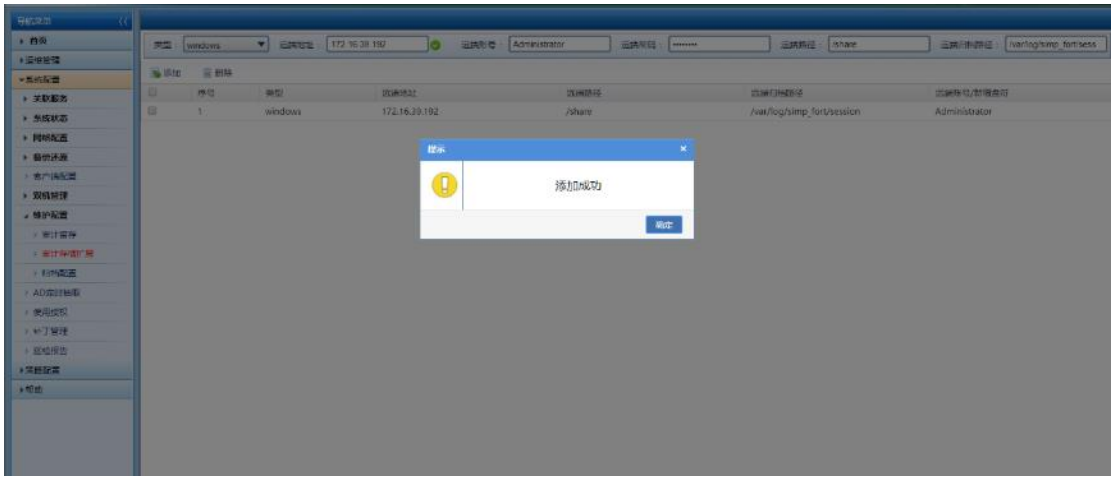
➢ 添加 linux 存储类型

linux 存储类型基本信息如下：

- 类型：linux
- 远端 IP：172.16.20.211（此 IP 为 linux 类型存储服务器 IP）
- 远端路径：/mnt（此路径为存储服务器上存储录像文件路径）
- 本地路径：/var/log/simp_fort/session（此路径为本地存储录像文件路径）

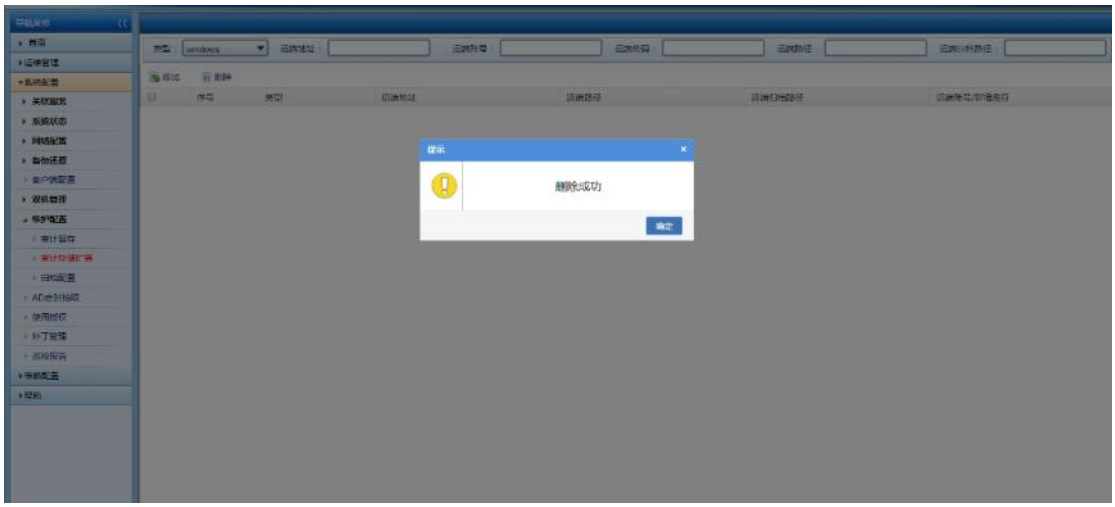


点击添加，提示添加成功。

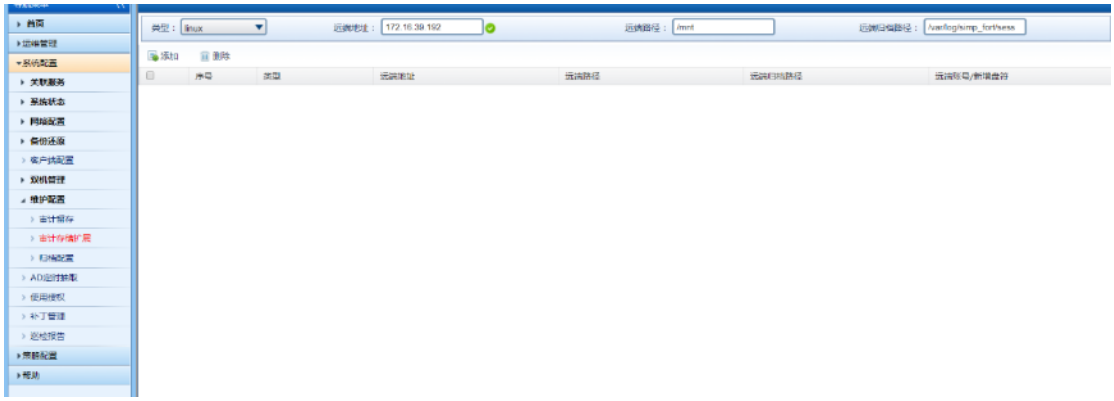


➢ 删除 linux 存储类型

选中 linux 类型的存储，点击删除，提示删除成功。



点击确定，列表页不显示 linux 类型外接存储的条目。



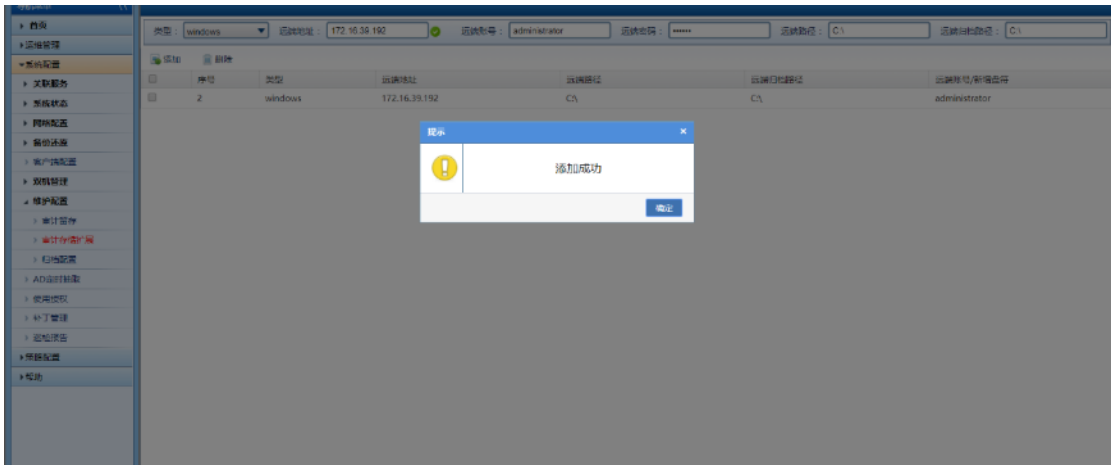
（7）类型-ISCSI

➢ 添加 ISCSI 存储类型

ISCSI 存储类型基本信息如下：

- 类型：ISCSI
- 远端 IP：172.16.20.240（此 IP 为 ISCSI 类型存储服务器 IP）
- ISCSI 名称：lun-0
- 本地路径：/var/log/simp_fort/session（此路径为本地存储录像文件路径）
- 新增盘符：/dev/sdb

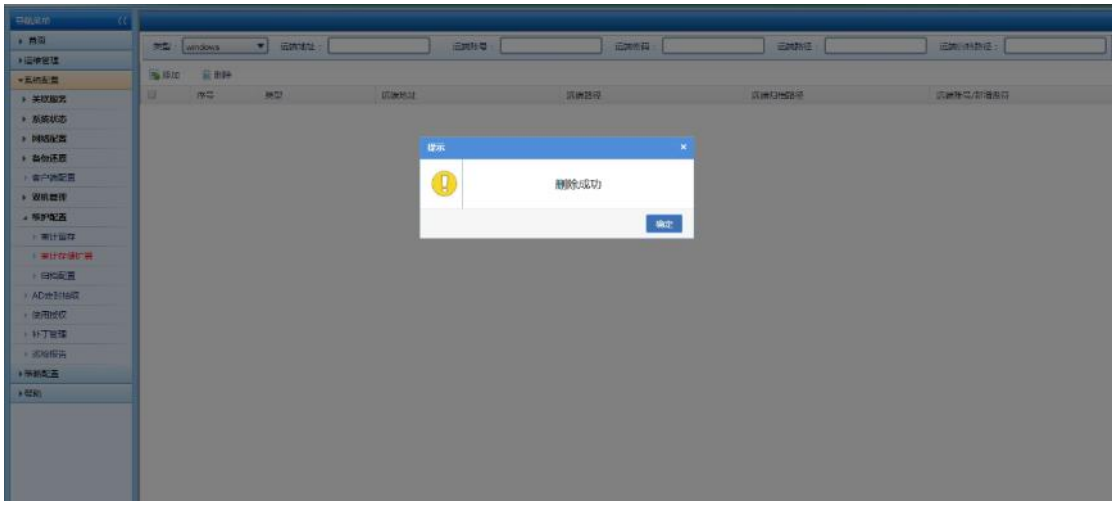
点击添加，提示添加成功。



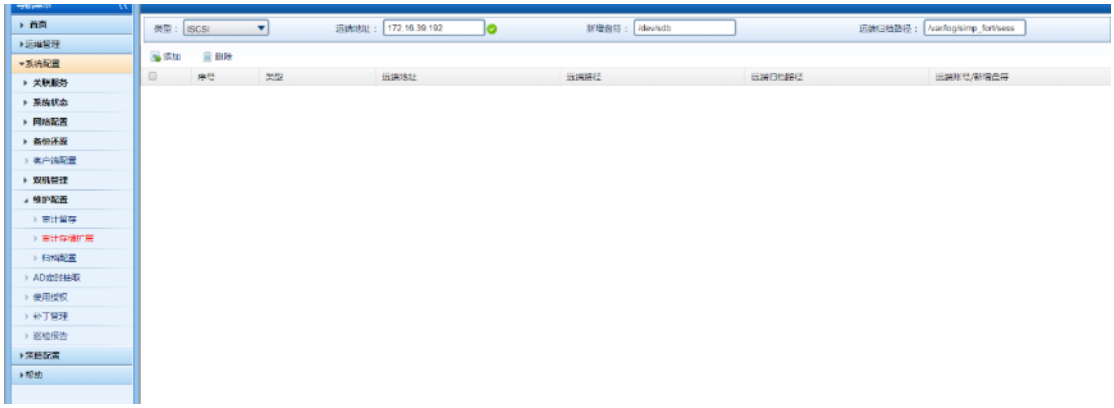
点击确定，列表页显示添加的 ISCSI 类型的外接存储。

➢ 删除 ISCSI 存储类型

选中 ISCSI 类型的存储，点击删除，提示删除成功。



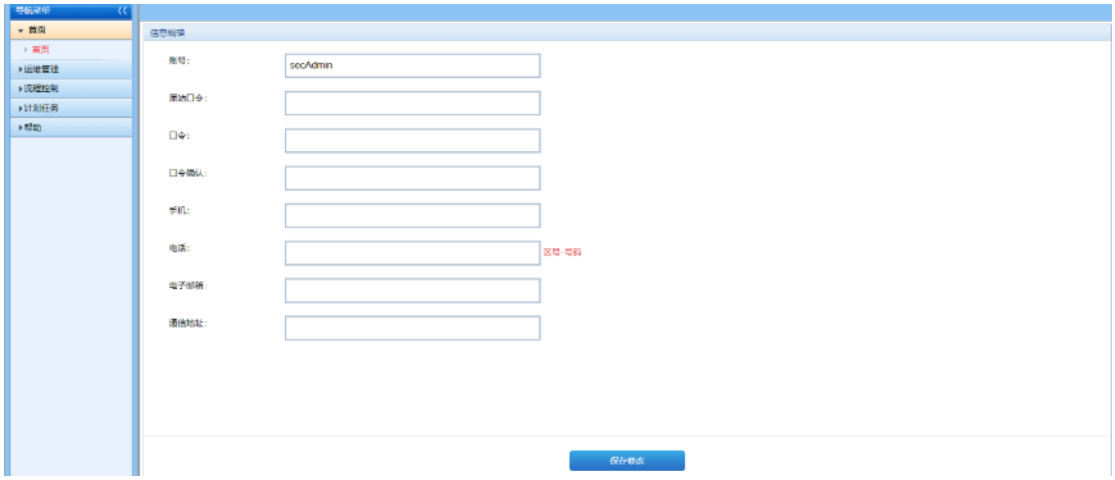
点击确定，列表页不显示 ISCSI 类型外接存储的条目。



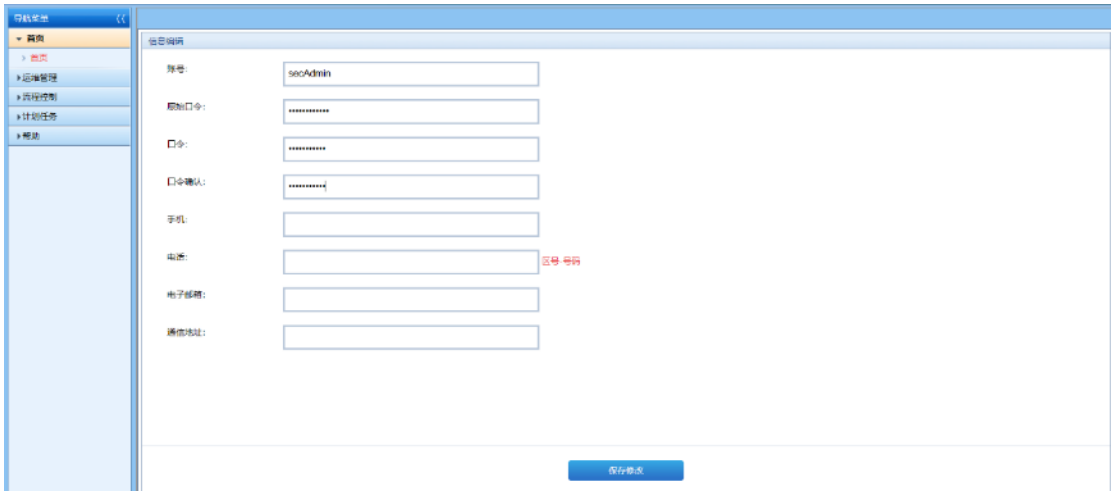
14.2. 个人信息维护

个人信息维护用于修改当前登录用户的密码、邮箱、电话等信息。

用户登录云堡垒机系统，点击个人信息维护，跳转到个人信息编辑页面。

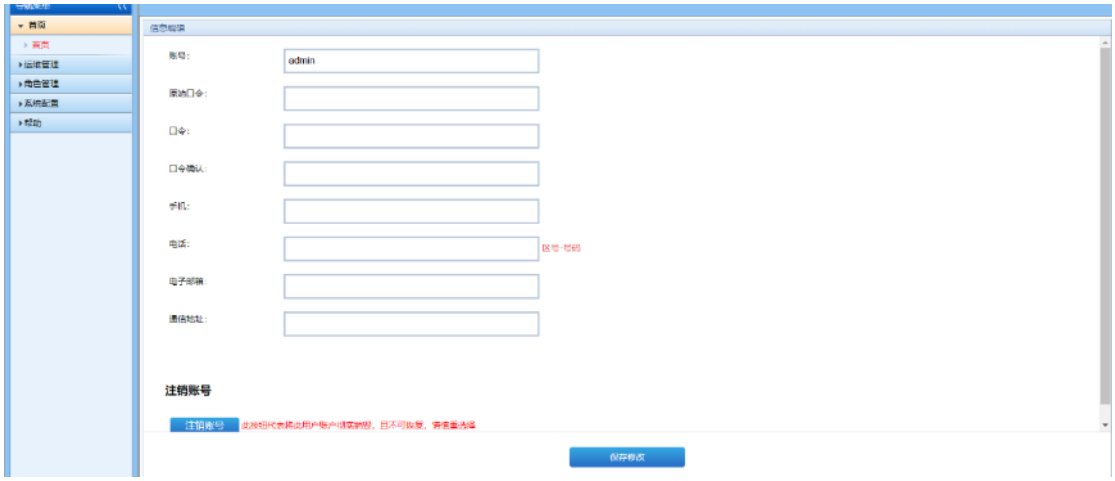


修改用户的密码，需要输入原始口令，再输入新口令，点击保存。用户再次登录的时候需输入新口令才可以登录云堡垒机。

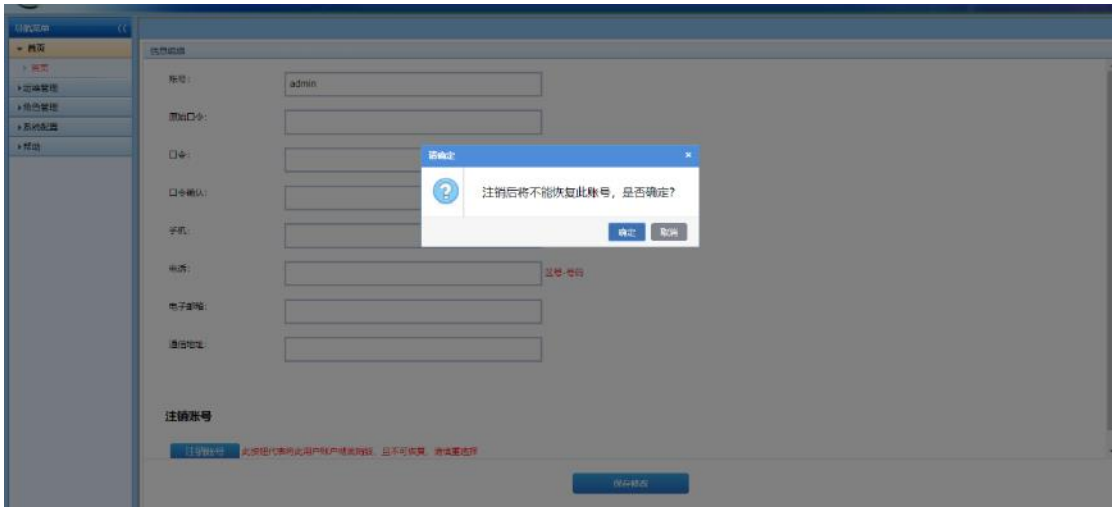


14.3. admin 自我注销

初始化用户 admin 登录系统，点击个人信息维护，跳转到个人信息编辑页面。



点击注销账户按钮，提示注销后将不能恢复此账号，是否确定？



点击确定按钮，初始化用户 admin 被注销，返回登录页面。

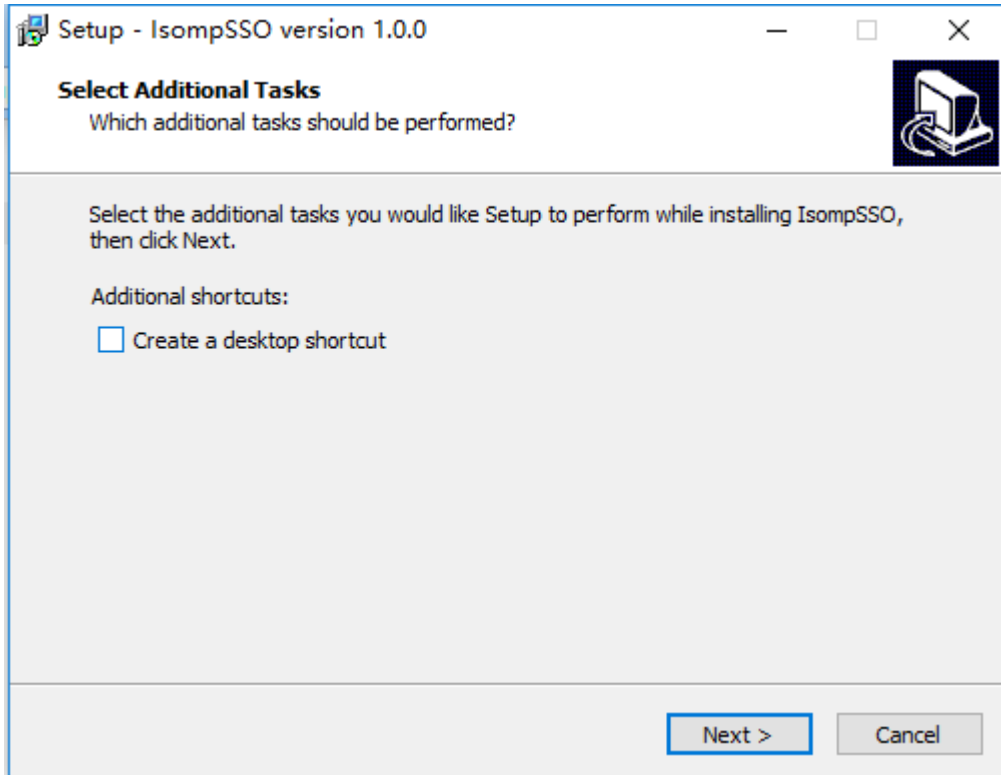
15. 帮助与控件下载

系统登录页面的“帮助与控件下载”以及登录页面右上角的“帮助”菜单提供单点登陆控件以及搭建应用发布服务器所需的 AppAgent 控件下。

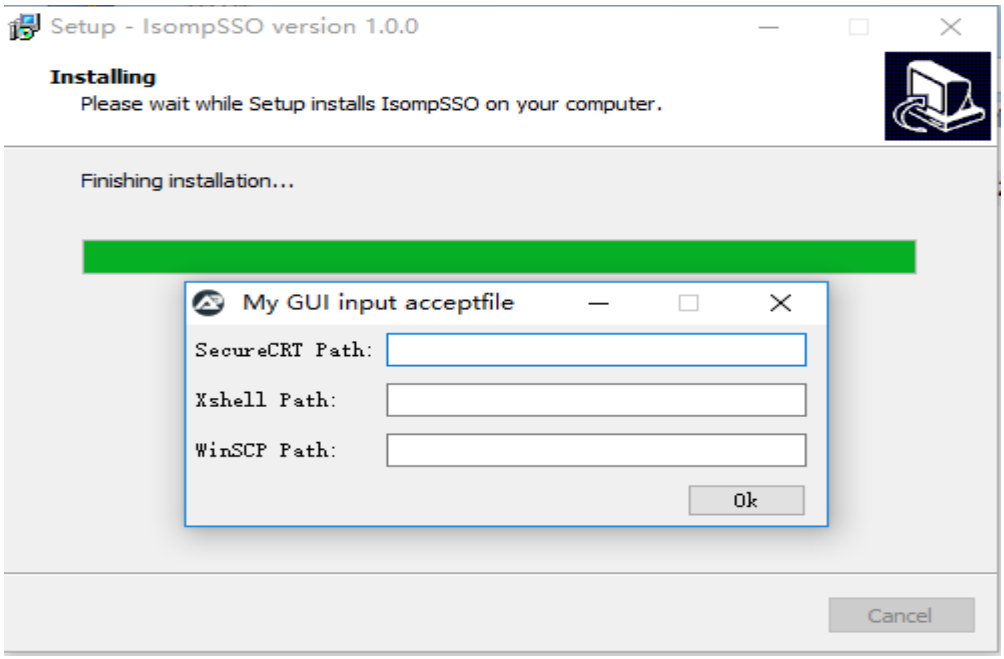
15.1. 单点登陆控件

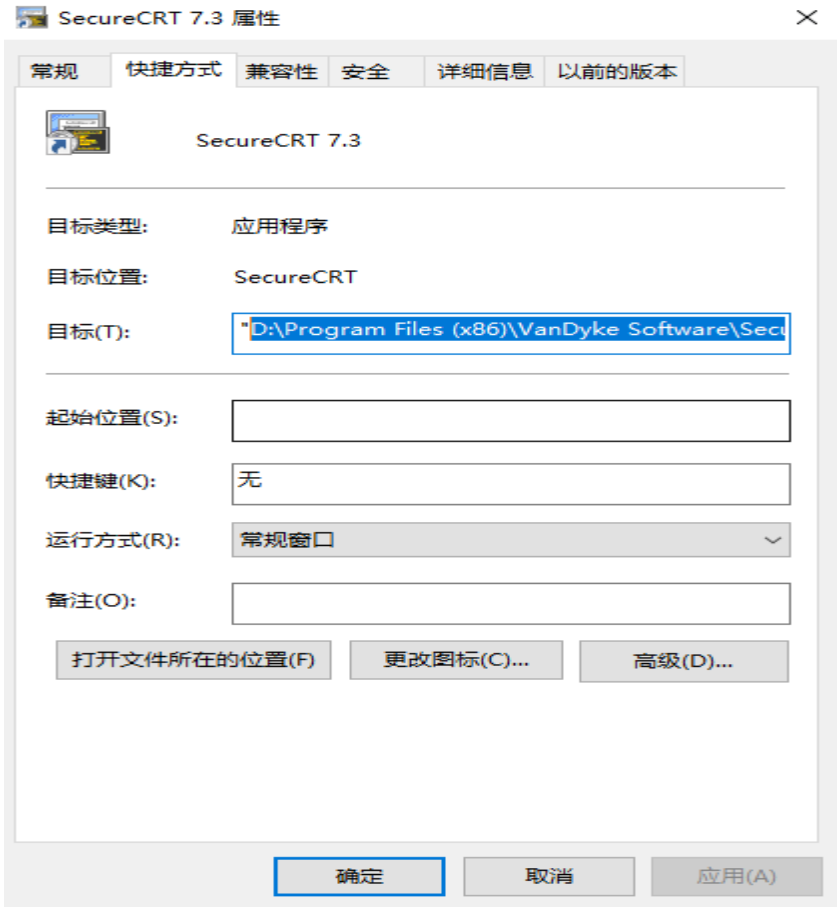
15.1.1. 下载

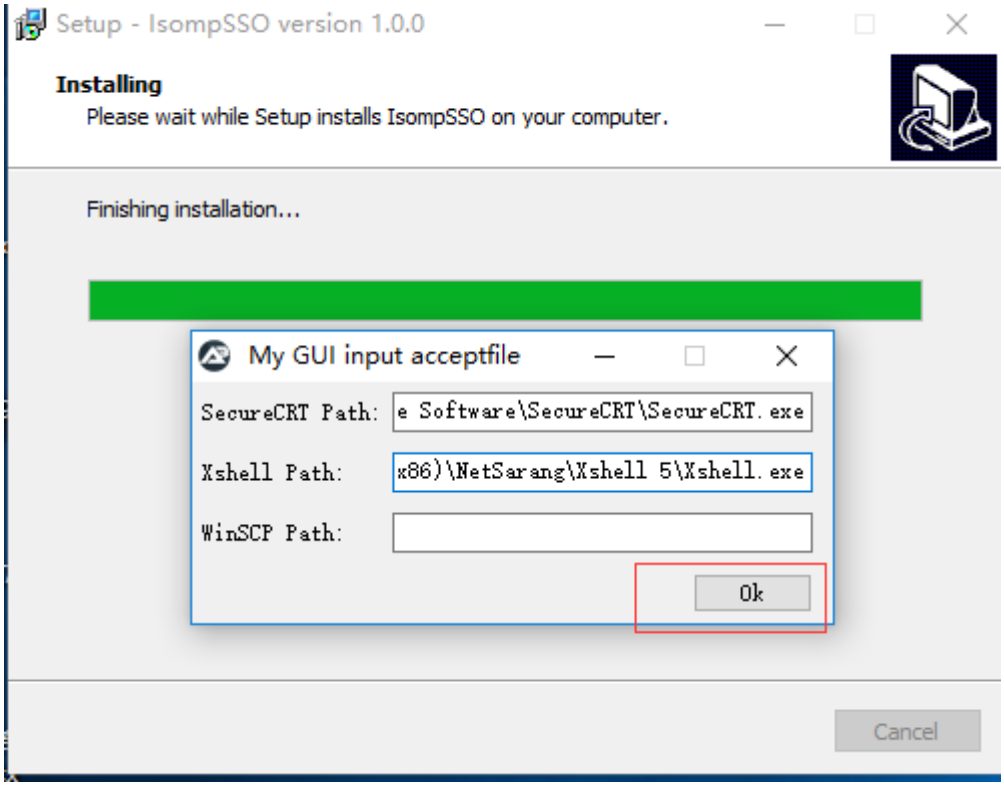
15.1.2. 安装



安装结束时配置调用本地字符客户端工具路径：







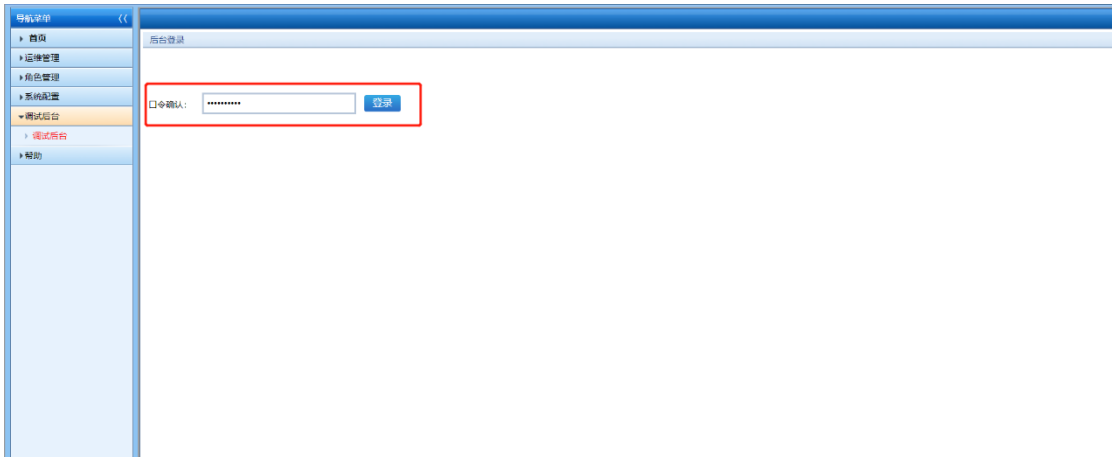
15.2. 应用发布 AppAgent 控件

安装步骤详见应用发布搭建手册。

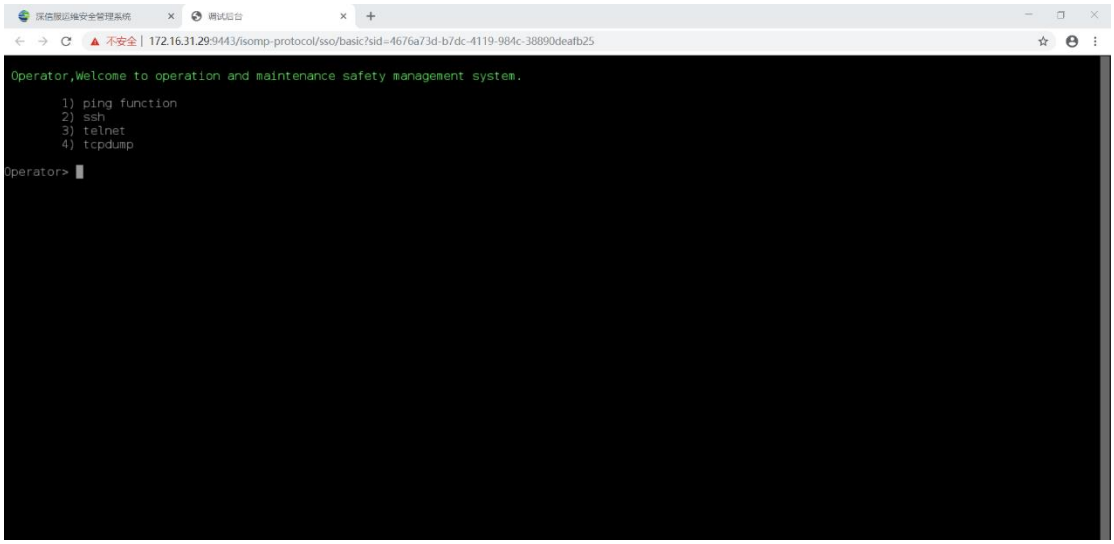
16. 调试后台

使用初始化用户密码登录，后台命令菜单前台化。

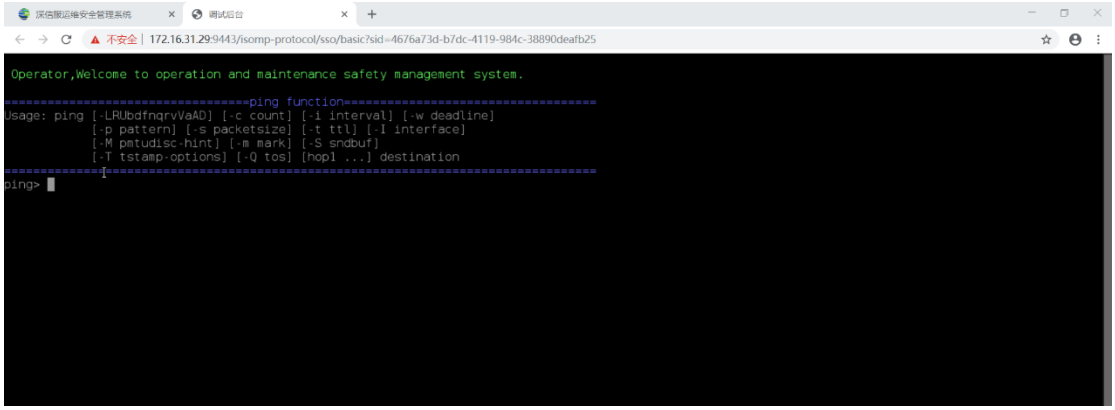
依次点击调试后台-调试后台，输入正确的初始化账户密码，点击登陆按钮



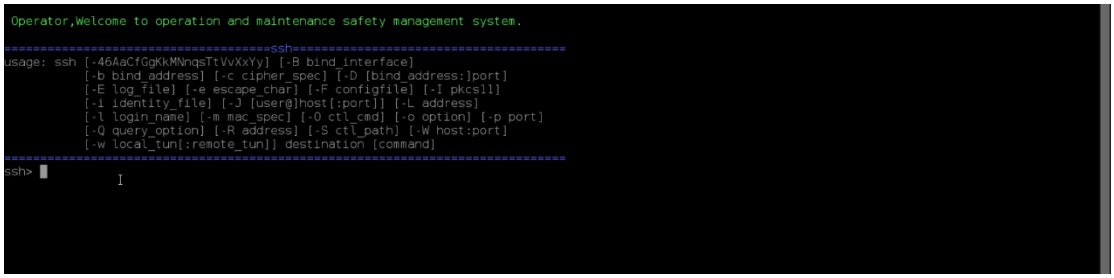
在浏览器新的标签栏中，进入调试后台页面，数字 1 为 ping，数字 2 为 ssh，数字 3 为 telnet，数字 4 为 tcpdump。输入不同的数字进入相应的界面，进行后台调试



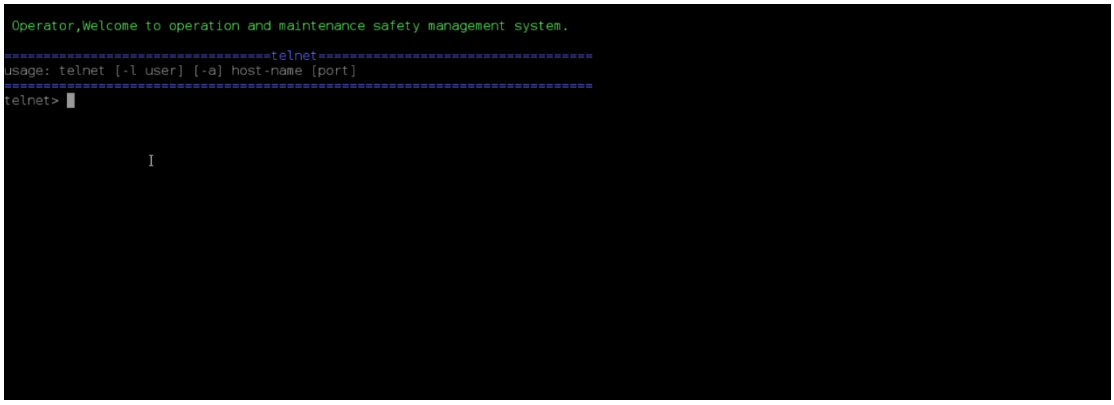
输入数字 1 进入 ping 的界面



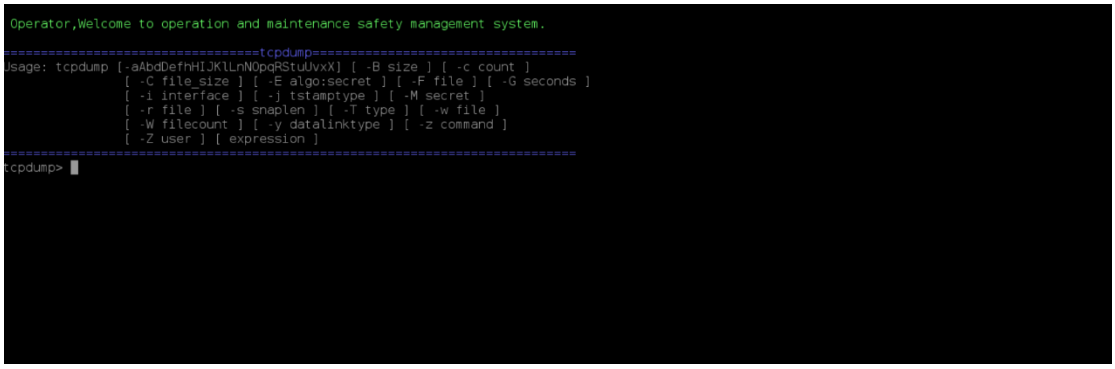
输入数字 2 进入 ssh 界面



输入数字 3 进入 telnet 界面



输入数字 4 进入 tcpdump 抓包界面



调试完成后，切换到初始化管理员界面，可选择结束调试或本地下载