

**齐治科技**

**特权账号安全管理系统**

**Privilege Account Management**

**V 3.0**

**2020年10月16日**

**版本：1.0**

版权说明

包含于此篇文档中的信息属于商业或财务机密（或授权）信息。浙江齐治科技股份有限公司所专有，除非被浙江齐治科技股份有限公司授权，否则此文档的全部或者部分信息不得用于再版或者引用。

内容

[1. 安装部署说明 3](#_Toc53808705)

[1.1 概述 3](#_Toc53808706)

[1.2 网络要求 3](#_Toc53808707)

[1.3 客户端要求 4](#_Toc53808708)

[1.4 登录系统 4](#_Toc53808709)

[2. 使用说明 7](#_Toc53808710)

[2.1 用户管理 7](#_Toc53808711)

[2.2 资产管理 8](#_Toc53808712)

[2.3 帐号管理 10](#_Toc53808713)

[2.4 配置改密计划 25](#_Toc53808714)

[2.5 配置密码备份 29](#_Toc53808715)

[2.6 生命周期管理 31](#_Toc53808716)

[2.7 密码工单管理 33](#_Toc53808717)

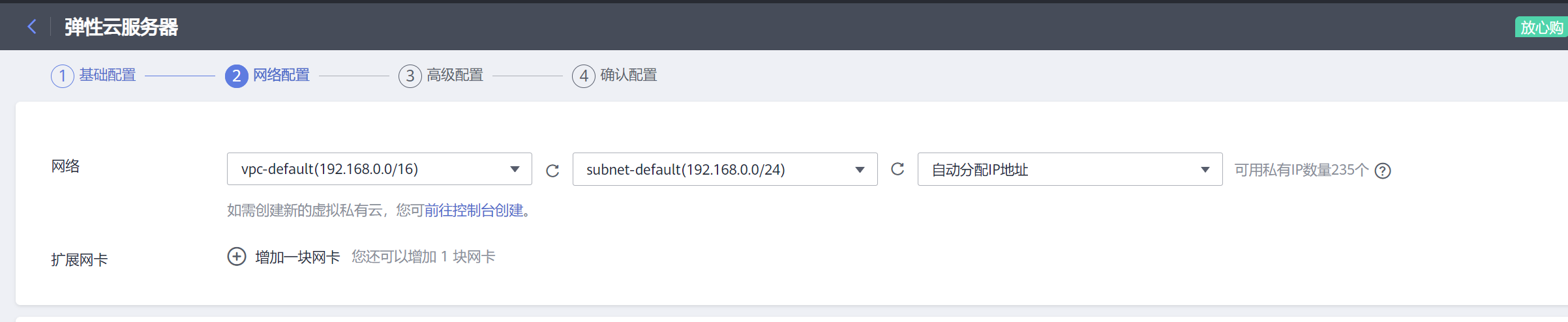
# 安装部署说明

## 概述

集中化账号管理是运维安全管控的前提，也是运维安全管理的必然发展趋势。齐治特权账号安全管理系统（Privileged Account Management，简称PAM）在部署后，实现密码的自动改密、账号发现、提供账号工单功能。

## 网络要求

登录华为云的控制台页面，在创建ECS服务器时，设置所需要的VPC中，选择自动分配IP地址。



创建后找到通过镜像生成的主机的IP地址。便于设定后续网络条件以及内网IP地址。

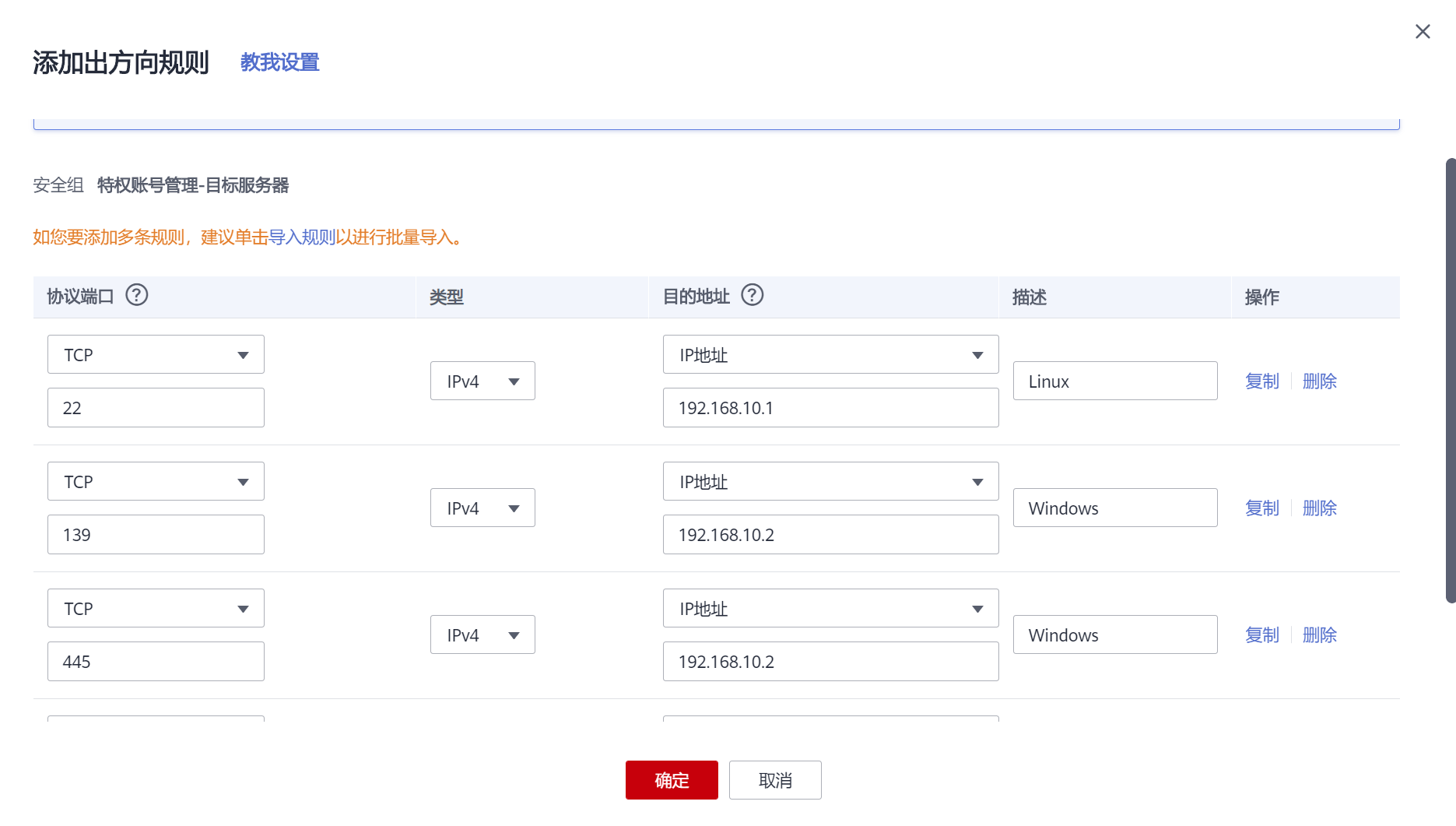


通过云控制台的安全组，开放如下网络策略：

|  |  |  |  |
| --- | --- | --- | --- |
| 源地址 | 目标地址 | 端口 | 备注 |
| 用户PC | 本系统或本系统的弹性IP | 443 | 浏览器访问PAM系统管理页面 |
| 本系统 | 被管理的Windows | 139/445 |  |
| 本系统 | 被管理的Linux | 22 |  |
| 本系统 | 被管理的Oracle | 1521 | 根据实际IP地址变化 |
| 本系统 | 被管理的MSSQL | 1433 | 根据实际IP地址变化 |

可以在华为云的VPC设置安全组





访问https://<ip>/ 查看是否能够打开主页。

## 客户端要求

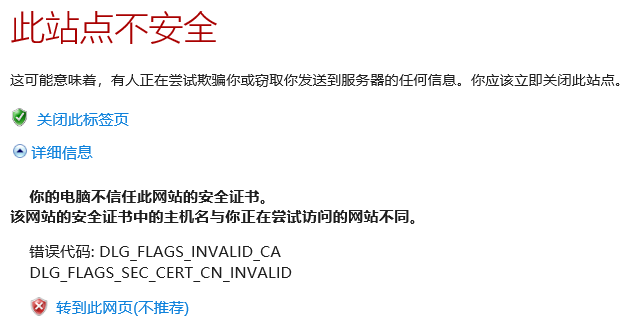
通过Web界面登录本系统的PC端环境要求请参考下表：

| 项目 | 要求 |
| --- | --- |
| 操作系统 | Windows XP SP3及以上版本 |
| 浏览器 | * Microsoft Internet Explorer 11.0及以上版本 * Mozilla Firefox 50及以上版本 * Google Chrome 49及以上版本 |
| 显示器分辨率 | 建议最小为1280\*1080（系统的缩放设置为100%时）。  **注:** 如使用更小的分辨率，或系统缩放大于100%，可以降低浏览器的缩放比率，使Web界面所有内容能够全部正常显示。 |

## 登录系统

1. 用户登录时，在浏览器地址栏中输入PAM的公网地址（https://<PAM-弹性IP>），进入PAM的Web登录页面。

**说明：**如出现安全提示，请选择继续前往或添加例外。



看到下述页面后，输入默认用户名和密码 admin / admin



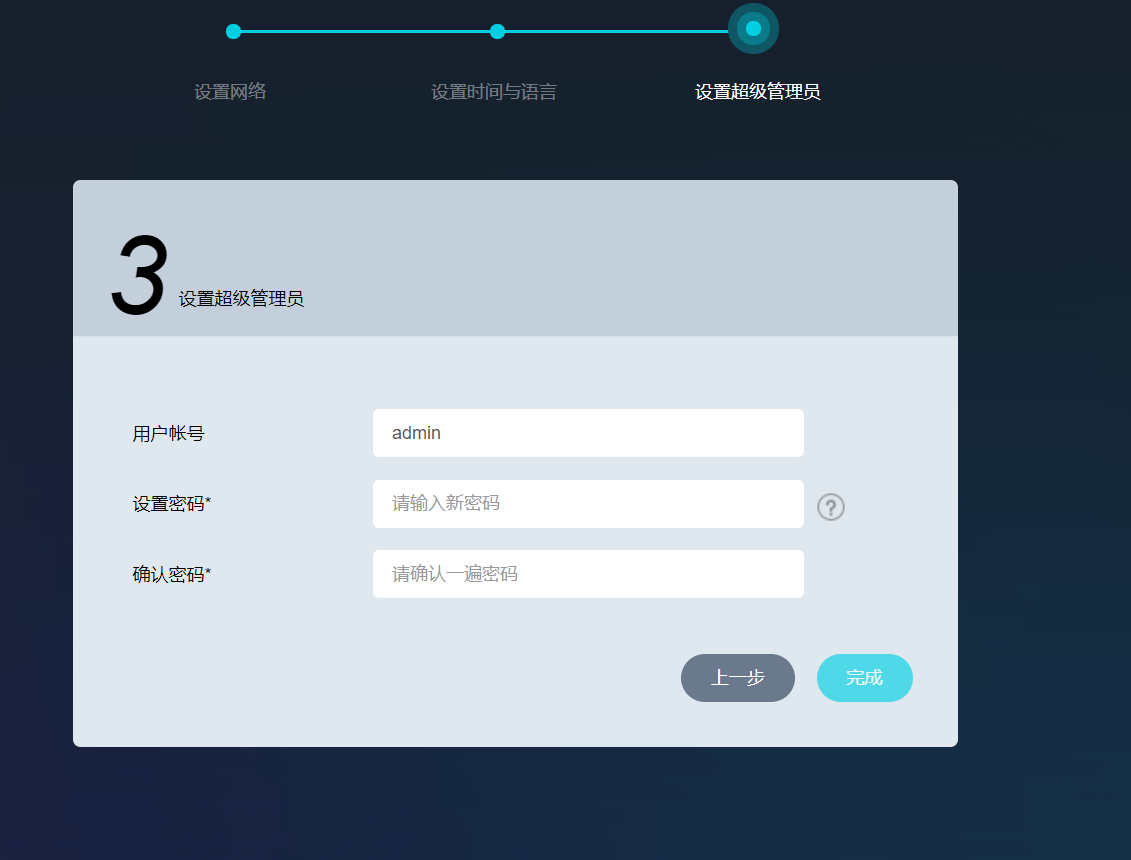
初始化网卡，不用变更。



云上机器不用设置NTP，直接点击下一步



重新设置管理员密码，以完成登录。



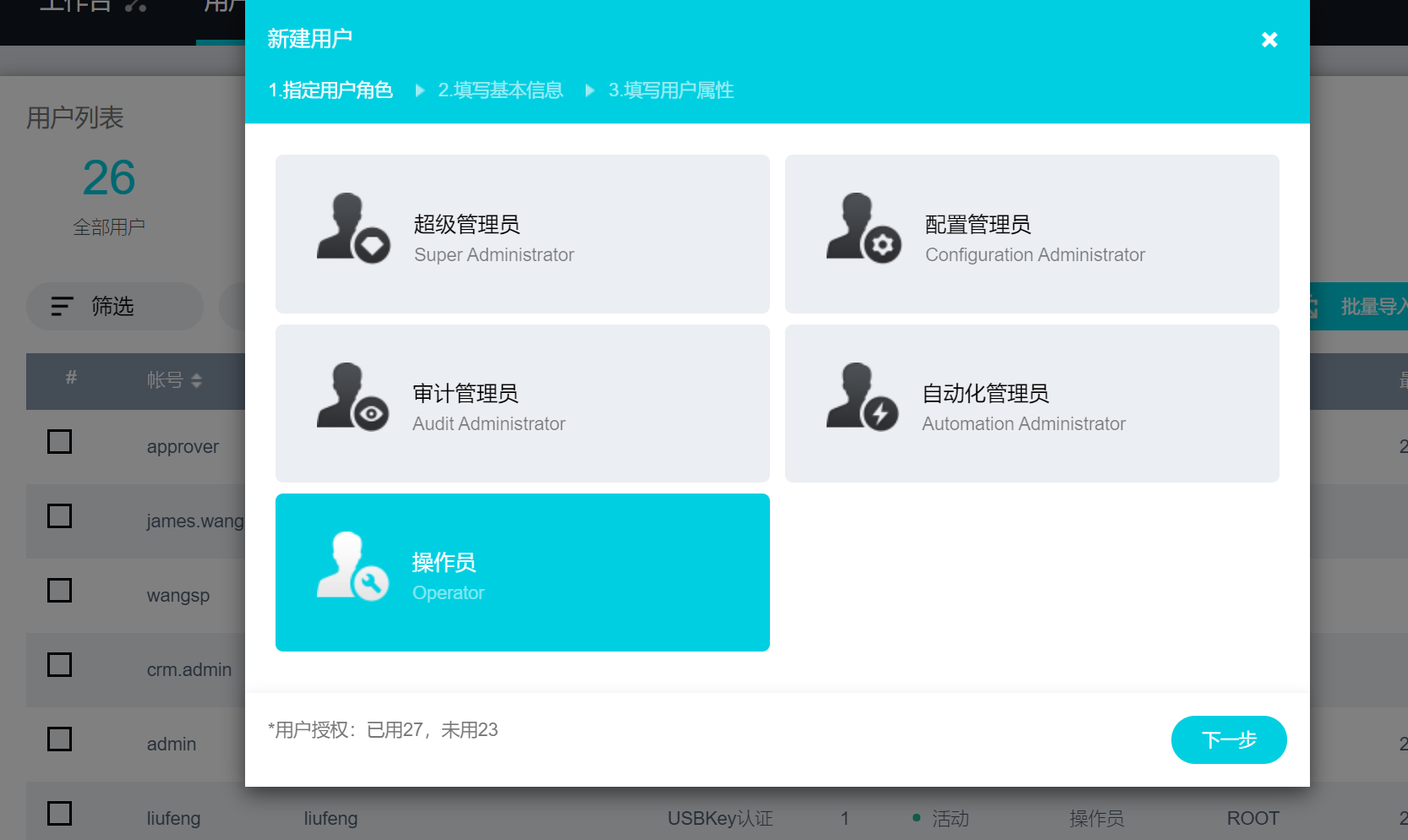
# 使用说明

## 用户管理

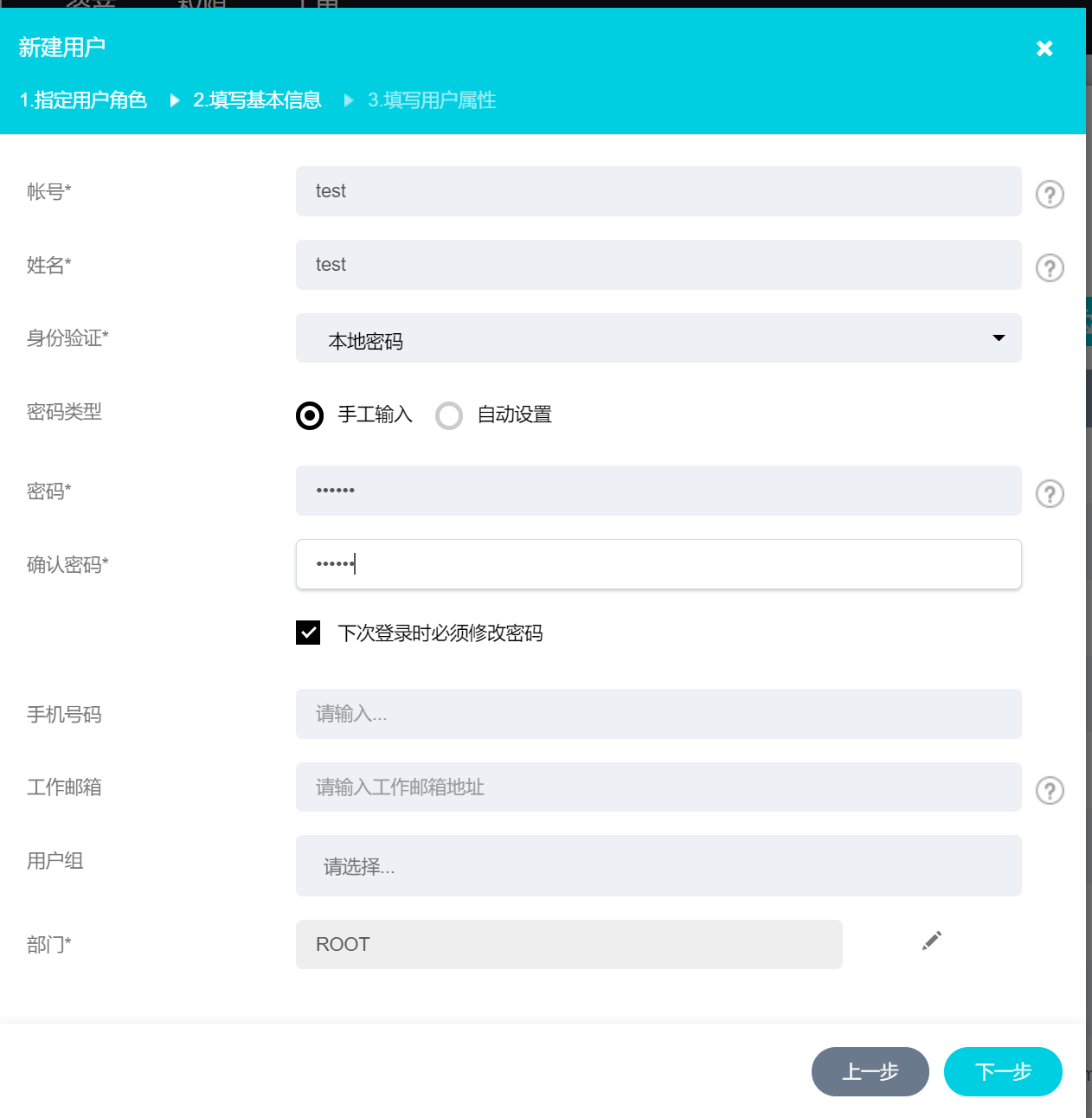
点击【用户】Tab页



点击【新建用户】



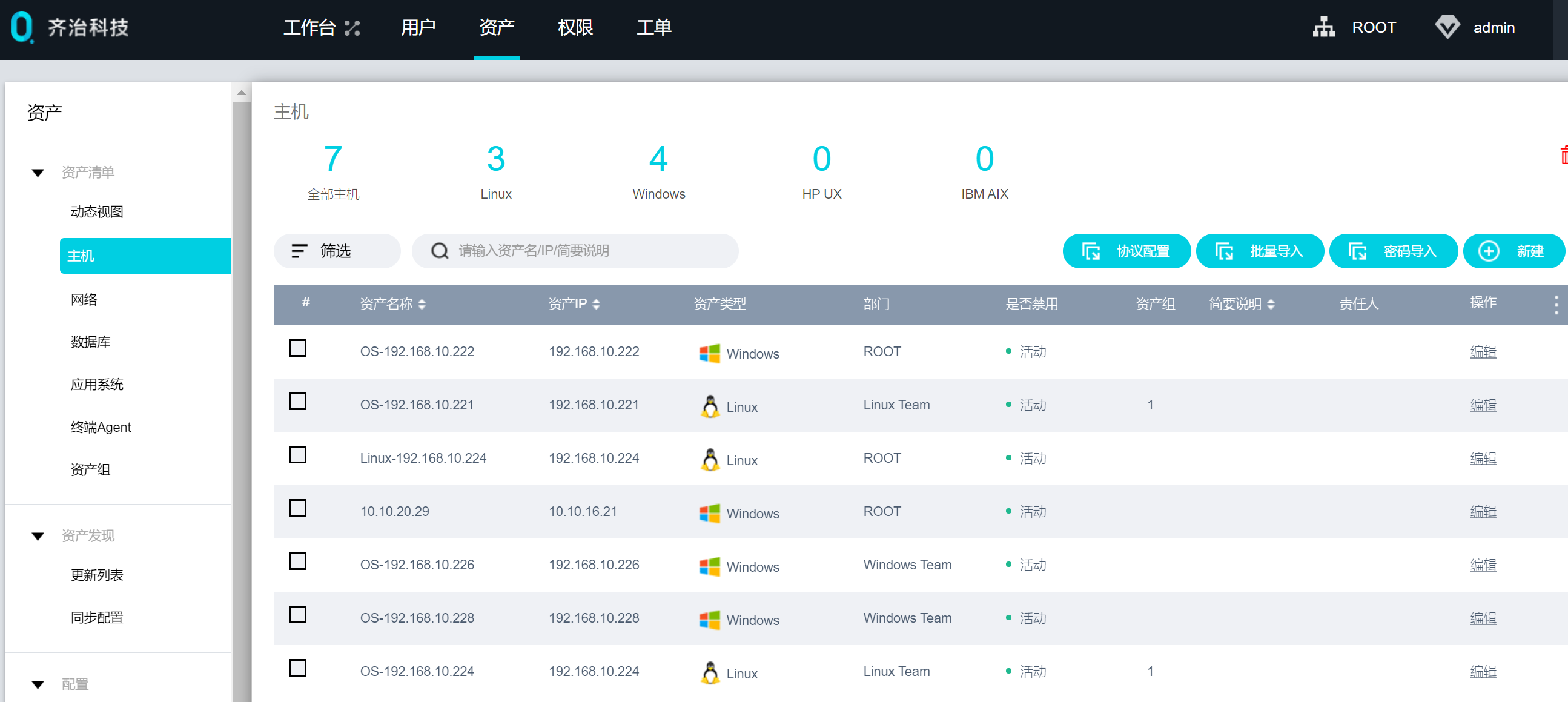
输入相关信息后，点击下一步直到保存。

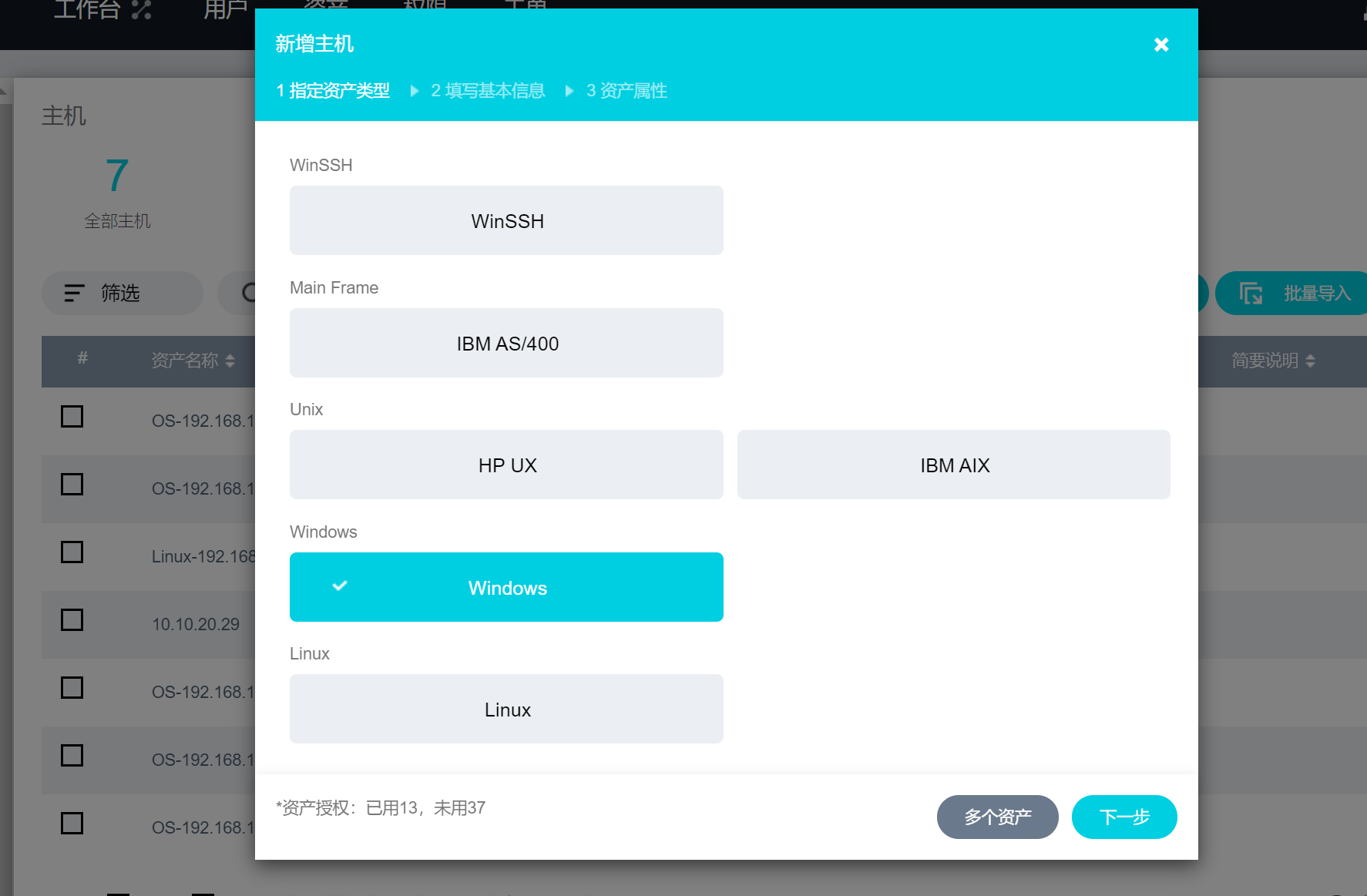




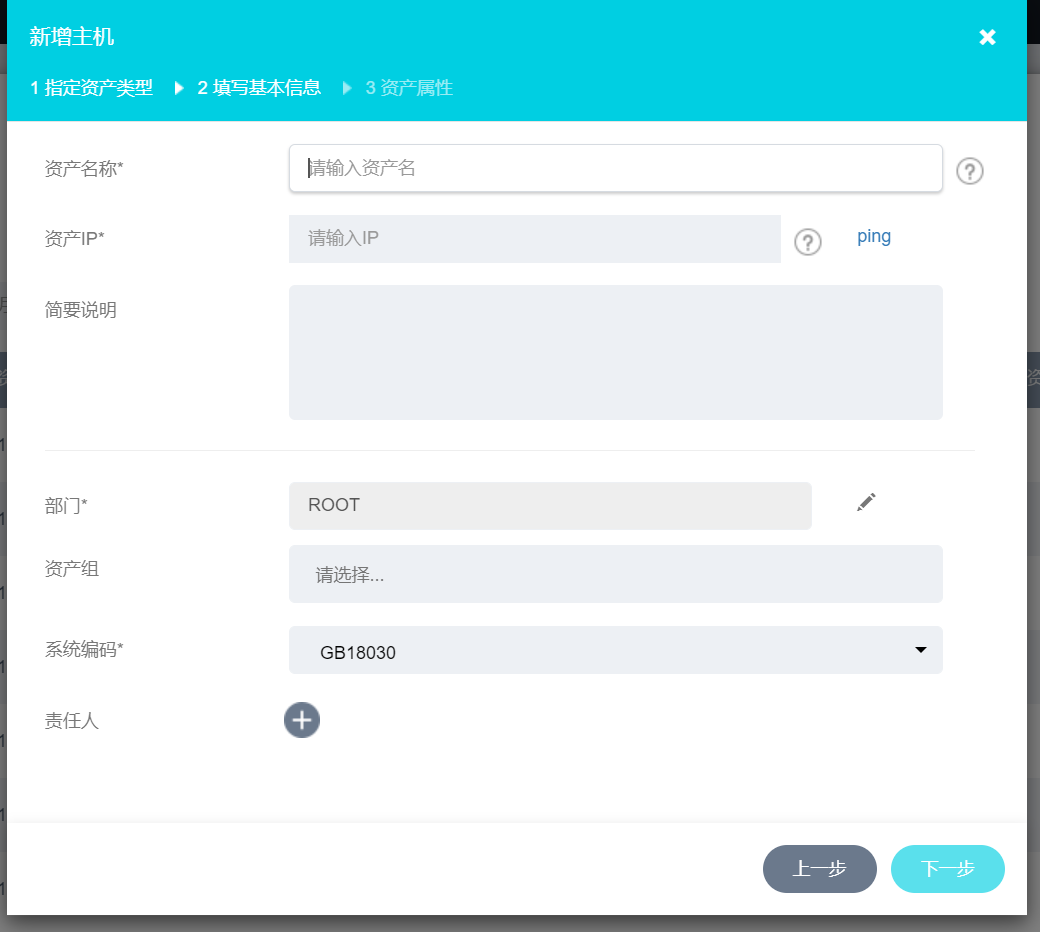
## 资产管理

点击【资产】Tab页面





输入IP等信息



输入账号密码



## 帐号管理

帐号管理可实现对主机、网络等设备的系统帐号的基本信息管理、密码修改、帐号巡检、帐号发现和密码备份。

* [**管理帐号资产**](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0001.html)  
  在帐号资产中可以以帐号为中心，对帐号的基本信息进行集中查询和更新。
* [**帐号维护**](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0002.html)
* [**日志报表**](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0007.html)  
  日志报表中可以查看PAM对帐号资产的全部日志记录和历史密码。
* [**系统设置**](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0010.html)  
  帐号管理相关的系统设置。
* [**帐号管理兼容性列表**](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_compatibility_0005.html)  
  PAM的登录测试、帐号巡检、帐号发现和改密计划等帐号管理功能，不同类型的资产支持情况有所不同。

在帐号资产中可以以帐号为中心，对帐号的基本信息进行集中查询和更新。

只有以下角色的用户可以管理帐号资产：

* 超级管理员
* 配置管理员
* 同时具有资产和帐号管理授权的自定义用户角色

PAM根据帐号所属的资产类型将帐号分为：

| **类型** | **说明** |
| --- | --- |
| 主机帐号 | 指资产类型为主机的帐号，比如Linux、Windows、AIX。 |
| 网络帐号 | 指资产类型为网络的帐号，比如Cisco IOS、Huawei Quidway、H3C Comware。 |
| 数据库帐号 | 指资产类型为数据库的帐号，比如Oracle、MYSQL、MSSQL、DB2。 |
| 应用帐号 | 指资产类型为应用系统的帐号，比如BS应用、CS应用、Weblogic应用。 |
| 域帐号 | 指Windows域帐号，请参考[管理域帐号](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0001.html" \l "task_zrl_ytc_flb)。 |

Note: 因产品软件版本和设备型号不同，可管理的帐号类型会有所不同。

在帐号资产中您可以对帐号进行下列操作：

* 查看帐号基本信息。
* 配置帐号基本属性，包括设置帐号类型、是否可改密、设置私钥等基本信息。
* 维护帐号密码，包括重新录入密码、自动修改密码。
* 查看帐号历史日志。
* 批量更新帐号基本属性。
* 批量导出帐号。

### 查看帐号属性

帐号的属性是指帐号的UID、所属组、创建时间、过期时间、上次改密时间等信息，PAM通过读取资产上的相关文件或者查询相关数据的方式获取。

* 完成帐号发现或者帐号巡检。

帐号属性是通过帐号发现或者帐号巡检功能获取的，对于自动发现的帐号PAM会自动获取属性，对于手工添加的帐号PAM会在帐号巡检时获取属性，请确保已经配置并执行了帐号巡检任务。否则帐号属性中将全都显示为无数据。

* 了解支持的帐号类型。

PAM仅支持部分类型的主机、数据库和域帐号的属性查看。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要查看的帐号类型。
3. 选择要查看的资产及帐号，单击编辑，选择帐号属性。

| Table 1. Windows帐号属性 | |
| --- | --- |
| **属性** | **说明** |
| 上次改密时间 | 帐号在目标资产上的上次修改密码的时间。仅支持通过帐号巡检方式获取。 |
| 所属组 | 帐号在目标资产上所属的用户组，比如administrators。 |
| 最后登录时间 | 帐号在目标资产上的最后登录时间。仅支持Agent方式获取，通过RPC方式进行帐号发现和巡检，无此属性。 |
| 过期时间 | 帐号在目标资产上的过期时间。仅支持Agent方式获取，通过RPC方式进行帐号发现和巡检，无此属性。 |
| Table 2. Linux和IBM AIX帐号属性 | |
| **属性** | **说明** |
| UID | 帐号在目标资产上的用户ID。 |
| 上次改密时间 | 帐号在目标资产上的上次改密时间。仅支持通过帐号巡检方式获取。 |
| 所属组 | 帐号在目标资产上所属的组的组名。 |
| 最后登录时间 | 帐号在目标资产上的最后登录时间。 |
| 过期时间 | 帐号在目标资产上的过期时间。IBM AIX不支持。 |
| home | 帐号在目标资产上的home目录。 |
| shell | 帐号在目标资产上的shell。 |

1. Note: 帐号在目标资产的/etc/passwd文件中必须有密码字段或者配置了SSH公钥，PAM才会获取其属性，否则将作为不可登录帐号不显示。

| Table 3. Oracle帐号属性 | |
| --- | --- |
| **属性** | **说明** |
| UID | 帐号在目标资产上的用户ID。 |
| 帐号状态 | 对应目标资产user$表中的astatus。 |
| 创建时间 | 帐号在目标资产上的创建时间。 |
| 缺省表空间 | 对应目标资产user$表中的defalut\_tablespace。 |
| 过期时间 | 对应目标资产dba\_users表中expiry\_datavv。 |
| 帐号系统权限 | 帐号在目标资产上的系统权限。 |
| 最后登录时间 | 帐号在目标资产上的最后登录时间。仅支持Oracle DataBase 12c。 |
| 帐号角色 | 帐号在目标资产上的帐号角色。 |
| Table 4. MSSQL帐号属性 | |
| **属性** | **说明** |
| 创建时间 | 帐号在目标资产上的创建时间。 |
| 上次修改时间 | 帐号在目标资产上的上次被修改的时间。 |
| 帐号角色 | 帐号在目标资产的帐号角色。 |



| Table 5. Window域帐号属性 | |
| --- | --- |
| **属性** | **说明** |
| 创建时间 | 帐号在域中的创建时间。必须通过帐号巡检方式获取。 |
| 过期时间 | 帐号在域中的过期时间。必须通过帐号巡检方式获取。 |
| 上一次改密时间 | 帐号在域中的上次改密时间。必须通过帐号巡检方式获取。 |
| 域名 | 帐号所属的域的域名。在新增域帐号时获取。 |
| 用户DN | 帐号在域中的DN信息，例如：CN=admin,CN=Users,DC=example,DC=com。在新增域帐号时获取。 |
| 域内组信息 | 该帐号在Windows域中的组信息。必须执行两次帐号巡检后才能获取到。 |

### 设置帐号属性

帐号资产中允许对帐号进行设置，相关的操作也可以在资产 > 资产清单 > 主机（或其他）中单击编辑进行。

Note: 帐号的责任人属性继承自其所属的资产，不支持单独设置，您可以在资产中选择要修改的资产，单击编辑修改责任人属性。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要配置的帐号类型。
3. 选择要配置的资产和帐号，单击编辑，选择帐号编辑。
4. 设置各参数，完成后单击确定。

| **参数** | **说明** |
| --- | --- |
| 帐号类型 | 帐号在目标资产上的权限类型，PAM对目标资产进行改密操作时将优先使用特权帐号登录。对于需要通过ssh和telnet访问的设备，特权帐号和普通帐号的登录提示符也不同，该设置会影响PAM自动登录目标设备。   * + 特权帐号：目标资产上权限最高的帐号，比如Linux中的root、Windows中的Administrator、Cisco IOS中的enable、Oracle中的SYSDBA帐号。   + 普通帐号：目标资产上特权帐号以外的帐号。 |
| 是否可改密 | 是否允许PAM自动修改该帐号的密码：   * + 可改密：允许PAM对该帐号进行自动改密。   + 不可改密：不允许PAM进行自动改密。 |
| 登录密码 | 仅修改PAM上的密码，一般用于当PAM上的该帐号密码设置错误时进行重设。 |
| 确认密码 | 必须和登录密码完全一致。 |
| 用户访问 | 是否允许用户使用该帐号访问资产。   * + 启用：允许用户使用该帐号访问资产。   + 禁用：禁止任何用户使用该帐号访问资产，仅允许使用帐号改密、发现和巡检等功能。   禁用后，在工作台 > 访问资产中访问该资产，或使用SSH/RDP客户端访问该资产时，可用帐号列表中都将不显示该帐号。 |
| 切换自 | Linux、Unix和网络设备中的特权帐号可能不允许直接telnet或者ssh远程登录，此时可以选择一个低权限的帐号作为切换来源，PAM在登录目标资产时会先使用切换自帐号登录，然后再通过su等切换命令切换到特权帐号的身份。 |
| 私钥(含SSH服务的资产) | 访问目标资产的SSH密钥。可以在资产 > 配置 > 密钥管理中查看或者添加新的密钥。 |
| 互备帐号 | 仅用于应用改密中的中间件改密或调用密码SDK。  互备帐号是具有同样权限的两个帐号，应用通过其中任意一个帐号登录资产（例如数据库），都能正常执行操作（例如查询数据库）。  设置时需要该资产上有未被设置为互备帐号的其他帐号，并从中下拉选择一个。需要同时设置互备状态。  Note: 互备帐号的具体使用，请参考《应用改密典型配置指导》。 |
| 互备状态 | 仅当配置了互备帐号时，才会显示该参数。  互备帐号中的两个帐号状态必须分别为活动和非活动。应用访问资产只会使用活动帐号登录；执行改密计划时，只会修改非活动帐号的密码，修改密码后会将非活动帐号的状态修改为活动，并将活动帐号的状态修改为非活动。  对一个帐号设置互备帐号和互备状态后，PAM会自动将其互备帐号的状态设置为相反的状态。 |

### 管理域帐号

域帐号中可以有多个特权帐号，但其中只有一个**连接帐号**，即在资产 > 配置 > Windows域中配置的域帐号。连接帐号只能在Windows域界面添加，不能在域帐号界面添加。

新增其他域帐号时，会通过连接帐号登录域并获取新增的域帐号的信息。因此如连接帐号不存在或配置有问题，将无法完成新增域帐号。

1. 在工作台 > 帐号管理 > 帐号资产 > 域帐号中，单击新增域帐号。
2. 在弹出的对话框中设置相关参数信息。

| **参数** | **说明** |
| --- | --- |
| 帐号名 | 域帐号的帐号名称，字符串格式，长度范围是1~200个字符，不能包含"**/**"和中文字符。 |
| 所属域 | 通过下拉菜单选择待添加帐号的所属域。 |
| 帐号类型 | * + 特权帐号：待添加的帐号为特权帐号。   + 普通帐号：待添加的帐号为普通帐号。 |
| 是否可改密 | * + 可改密：允许PAM对该帐号进行自动改密。   + 不可改密：不允许PAM进行自动改密。 |
| 帐号密码/确认密码 | 待添加帐号对应的登录密码。 |

1. 完成后单击确定。

Note: 当新增帐号在选择的所属域上不存在时，单击确定后，页面将提示未查询到该帐号,请确认域上是否存在。

当Windows域界面配置的**连接帐号**无效时，例如配置的帐号密码不正确、配置帐号缺少DN等，单击确定后，页面将提示连接帐号异常,请前往资源-Window域配置。

### 管理选定帐号密码

通过帐号资产的密码管理，您可以对选定的帐号进行单次密码自动修改、登录测试、查看最近的密码修改和备份情况、查看历史密码。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要配置的帐号类型。
3. 选择要配置的资产和帐号，单击编辑，选择密码管理。
4. 根据需要，可对选定的帐号进行下列管理操作：

查看最近的密码修改和备份情况。

| **属性** | **说明** |
| --- | --- |
| 当前密码 | 该帐号当前密码的状态，空密码、正常或异常。   * + 如当前帐号已托管了密码，可以单击登录测试，PAM使用当前帐号及密码登录资产查看登录是否成功。如果登录成功，当前密码显示为正常，否则显示为异常。   + 自动改密，在弹出的对话框中设置改密规则，单击确定，PAM将根据选定的规则登录目标资产修改选定帐号的密码。 |
| 下次改密时间 | PAM下一次对该帐号进行自动改密的时间，如果没有设置改密计划该值为空。改密计划在帐号管理 > 帐号维护 > 改密计划中设置。 |
| 改密计划 | 该帐号涉及的改密计划将被列出。可以单击查看改密计划，跳转到改密计划页面进行查看。 |
| 历史密码 | 该帐号使用的历史密码的数量。可以单击查看历史密码，在弹出的页面的表格中查看以下信息：   * + **时间**：该次修改密码的时间。   + **事件**。哪个用户（或系统）对该帐号的密码执行了什么动作。   + **结果**：事件的执行结果，成功或失败。   + **操作**：在当前保存的密码不可用的情况下，用户可以单击对应历史密码的登录测试，尝试是否可以使用某个历史密码登录。可以单击下载密码将历史密码下载到本地。   Note: 为了安全不能查看最近一次改密的成功的历史密码，如果需要查看请通过密码备份的方式进行。 |
| 上次备份时间 | PAM最近一次备份该帐号密码的时间，如果没有备份过记录为空。 |

Note:

* + 部分资产类型不支持登录测试，不支持的资产类型将不会出现登录测试按钮。具体不支持的资产类型可以参考[Table 2](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0003.html#ug_ma_0003__table_hq1_q4r_q2b)中的帐号异常支持情况。
  + 此处的登录测试功能，与[资产管理](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mr_0000.html)中的登录测试功能，实际测试方式不同。资产管理中的登录测试相当于用户实际执行了一次访问；帐号管理中的登录测试，Windows资产会使用RPC登录，Linux资产会使用后台登录，并对登录提示符进行检查。因此如果两边的登录测试结果不一致，是正常现象。
  + 执行自动改密前，必须先在帐号管理 > 系统设置 > 密码规则中添加对应的改密规则。改密结果将根据设置的备份方式发送给对应的通知人。改密规则的备份方式如设置为同密码备份，需要在帐号管理 > 帐号维护 > 密码备份中设置密码备份方式。

### 查看选定帐号日志

在帐号资产中可以查看指定帐号在PAM中的全部操作日志。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要配置的帐号类型。
3. 选择要配置的资产和帐号，单击编辑，选择帐号日志。
4. 选择要查看的日志记录，单击查看日志详情可查看日志详细信息。

Note: 如果查看的是修改密码失败的日志，管理员可以查看改密交互过程，便于管理员在改密失败时排查问题。

### 批量更新帐号

在帐号资产中可以通过Excel批量导入的方式更新帐号的帐号类型、密码和是否可改密属性。

Note:

* 不支持对域帐号的批量更新。
* 如果需要更新域名、密钥、切换自、是否特权和密钥列表这些帐号属性时，请在资产页面，右上角单击密码导入可以进行批量更新。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要配置的帐号类型。
3. 单击页面右上角的批量更新。
4. **Optional:** 单击下载模板，选择要更新的帐号，完成后单击下一步，确认无误后单击下载模板。
5. 在Excel模板文件录入各字段，留空的字段现有的参数将不被更新。

| **参数** | **说明** |
| --- | --- |
| 帐号类型 | 帐号在目标资产上的权限类型，PAM对目标资产进行改密操作时优先使用特权帐号登录，对需要通过ssh和telnet访问的设备，特权帐号和普通帐号的登录提示符也不同，该设置会影响PAM自动登录目标设备。   * + 特权帐号：目标资产上权限最高的帐号，比如Linux中的root、Windows中的Administrator、Cisco IOS中的enable、Oracle中的sysdba帐号。   + 普通帐号：目标资产上特权帐号以外的帐号。 |
| 密码 | 帐号在目标资产上的密码。 |
| 是否可改密 | 是否允许PAM自动修改该帐号的密码：   * + 可改密：允许PAM对该帐号进行自动改密。   + 不可改密：不允许PAM进行自动改密。PAM自动同步的域帐号默认值均为该值。 |
| 用户访问 | 是否允许用户使用该帐号访问资产。   * + 启用：允许用户使用该帐号访问资产。   + 禁用：禁止任何用户使用该帐号访问资产，仅允许使用帐号改密、发现和巡检等功能。   禁用后，在工作台 > 访问资产中访问该资产，或使用SSH/RDP客户端访问该资产时，可用帐号列表中都将不显示该帐号。 |

1. 在批量更新页面，批量上传填写完毕的Excel文件。您可以通过两种方式上传： 
   * 将文件直接拖到页面的矩形区域内。
   * 单击文件上传，选择文件并上传。
2. 上传后，PAM将显示从文件中读取的信息，请核对要更新的信息是否正确，完成后单击开始更新。如果有红色标记，说明录入的信息不正确，您可以： 
   * 直接页面上修改或者单击移除异常的数据。
   * 重新编辑Excel文件，后单击文件上传，重新上传。

更新完成后，状态栏将显示更新结果，您可以单击下载更新结果。

### 批量导出帐号

通过批量导出可以导出选择的帐号的基本属性到Excel文件中。

如果要导出密码，需要用户完成[配置ZIP文件密码](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0002.html)或[配置PGP公钥](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0014.html)。

Note: 不支持域帐号的导出。

1. 选择工作台 > 帐号管理 > 帐号资产。
2. 选择要配置的帐号类型。
3. 单击页面右上角的密码导出或批量导出。

Note: 密码导出导出的信息将比批量导出多了帐号密码一列。

1. 选择要导出的帐号，单击下一步。
2. **Optional:** 勾选左下角的特权帐号和普通帐号，可选择性导出特定类型的帐号。
3. 单击导出。

导出的Excel文件中将包含选定帐号的资产名、资产IP、责任人、帐号、帐号类型和是否可改密属性。如果执行的是密码导出，还会显示密码。如该帐号未托管密码，则该单元格为空。 执行密码导出后，需要使用用户在[配置ZIP文件密码](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0002.html)或[配置PGP公钥](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0014.html)时配置的密码/密钥进行解密后才能解压缩。

### 配置帐号巡检

帐号巡检可以批量、定期对PAM中的帐号进行安全检查，包括弱密码检查、密码是否正确检查、密码最后修改时间检查、帐号权限变更检查。根据检查结果，您可以及时地发现并修正帐号相关的安全问题。

在进行帐号巡检前请确保要巡检的帐号和密码已经录入PAM，PAM仅对已经录入并设置了密码的帐号进行巡检。

Note: 帐号巡检的执行还将受到交互超时时间和任务执行超时时间的影响，默认为20秒和180秒。若在执行过程中登录资产或执行脚本超过了设定的时间，将导致巡检失败。用户可以在[配置资产适配](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0024.html" \o "对于有些比较特殊的登录提示符，通过内置代填提示符无法匹配成功时，需要针对这些资产进行适配。)中，对特定的资产手动设置交互超时时间和任务执行超时时间。

如果需要使用弱密码帐号检查，请先[配置弱密码规则](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0011.html" \l "task_bbc_25b_p2b)。

PAM可以发现的帐号异常如[Table 1](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0003.html" \l "ug_ma_0003__table_zck_bnn_q2b)所示。

| Table 1. 帐号巡检异常清单 | |
| --- | --- |
| **检查项** | **说明** |
| 弱密码帐号 | 检查PAM中存储的系统帐号密码是否符合设定的弱密码规则。  Note: 不会使用弱密码库的密码对目标资产进行试探性登录。 |
| 网络异常 | 对帐号进行巡检时PAM访问目标资产发生错误，包括IP地址不可达、协议不可达。 |
| 帐号异常 | 使用PAM中存储的密码登录目标资产时，登录失败，通常是密码错误导致。 |
| 三个月未改密 | 检查目标资产上帐号密码的最后修改时间是否超过三个月。 |
| 权限变更 | 检查系统帐号在目标资产上所属的用户组是否和上次巡检时相同。 |

不同资产类型的帐号可支持巡检项有所不同，具体如[Table 2](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0003.html#ug_ma_0003__table_hq1_q4r_q2b)所示。

| Table 2. 帐号巡检兼容列表 | | | | | |
| --- | --- | --- | --- | --- | --- |
| **资产类型** | **弱密码帐号** | **网络异常** | **帐号异常** | **三个月未改密** | **权限变更** |
| Windows | 支持 | 支持 | 支持 | 支持 | 支持 |
| Linux | 支持 | 支持 | 支持 | 支持 | 支持 |
| AIX | 支持 | 支持 | 支持 | 支持 | 支持 |
| HP-UX | 支持 | 支持 | 支持 | 不支持 | 不支持 |
| 网络设备 | 支持 | 支持 | 支持 | 不支持 | 不支持 |
| 数据库 | 支持 | 支持 | 支持 | 不支持 | 不支持 |
| B/S应用 | 不支持 | 不支持 | 不支持 | 不支持 | 不支持 |
| C/S应用 | 不支持 | 不支持 | 不支持 | 不支持 | 不支持 |
| Weblogic | 支持 | 支持 | 支持 | 不支持 | 不支持 |

### 配置手工触发巡检

如果需要对特定的帐号资产进行巡检，可以通过手工触发的方式进行，手工触发支持精确巡检、指定IP范围巡检或者只对已知有异常的帐号进行巡检。

1. 选择工作台 > 帐号管理 > 帐号维护 > 帐号巡检。
2. 单击开始巡检，根据具体需要选择巡检方式。 
   * 精确巡检，选择要巡检的资产，单击确定，PAM将对选定的资产进行帐号巡检。
   * 范围巡检，填写要巡检资产的起始IP和结束结束IP，单击确定，PAM将对已添加的符合指定IP范围的资产进行帐号巡检。
   * 异常帐号巡检，单击后将立即开始对已经发现有异常的帐号进行重新巡检。
3. **Optional:** 巡检过程中，单击页面底部进度条后的终止巡检，可以立即停止巡检任务。
4. **Optional:** 巡检完成，点击页面底部进度条后的返回，可重新开始巡检。

### 配置定期自动巡检

定期自动巡检可按天或者按月定期自动对PAM中的全部帐号资产进行巡检。

1. 选择工作台 > 帐号管理 > 帐号维护 > 帐号巡检。
2. 单击页面右上角的，单击设置定期巡检，填写各参数后，单击确认。

| **参数** | **说明** |
| --- | --- |
| 执行时间 | 任务的首次执行日期和每次的执行时间。 |
| 执行间隔 | 任务的执行周期，支持：   * + 月：执行间隔是月。整数形式，取值范围是1～12。   + 天：执行间隔是天。整数形式，取值范围是1~365。 |
| 任务通知 | 任务执行完毕发送E-mail通知选定的用户。  Note: 只有设置了工作邮箱的用户帐号才会出现在待选列表里。管理员可以在用户 > 用户管理 > 用户列表中为用户帐号设置工作邮箱。 |

设定完成后，PAM将按照设定的时间和周期进行巡检，您可以在工作台 > 帐号管理 > 帐号维护 > 帐号巡检中查看最新的巡检结果。或者单击页面右上角的查看上一次巡检时间、下一次巡检时间、下载巡检的详细日志。

### 配置帐号发现

帐号发现包括帐号扫描和帐号录入。帐号扫描是指PAM扫描目标设备的帐号并与PAM上的帐号对比，找出仅在目标设备上存在的帐号和仅在PAM上存在的帐号，这两类帐号统称为“幽灵帐号”。帐号录入是指将仅在目标设备存在的帐号添加到PAM上（添加前可以编辑帐号属性），以及将仅在PAM上存在的帐号删除，使PAM上的帐号与目标设备上的帐号保持一致。

* 对于PAM扫描发现的帐号，需要资产的责任人确认和处理，请确保配置资产时添加了责任人。对未设置责任人的资产，PAM不会发送帐号确认信息。
* 待巡检的Windows资产采用Agent模式，需要在目标Windows上[安装Agent](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0004.html" \l "task_ffp_2hd_mmb)；采用RPC模式，需要在目标Windows上[配置Windows共享区域](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0004.html" \l "task_z5r_dhd_mmb)，同时打开TCP的135、139和445端口，且防火墙允许PAM访问这些端口。

帐号发现的结果中将不显示以下帐号：

* Windows资产中锁定或禁用的帐号。
* 类Unix系统中的nologin帐号。
* 密码为空的帐号。

Note: 帐号发现的执行还将受到交互超时时间和任务执行超时时间的影响，默认为20秒和180秒。若在执行过程中登录资产或执行脚本超过了设定的时间，将导致帐号发现失败。用户可以在[配置资产适配](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0024.html" \o "对于有些比较特殊的登录提示符，通过内置代填提示符无法匹配成功时，需要针对这些资产进行适配。)中，对特定的资产手动设置交互超时时间和任务执行超时时间。

### 帐号扫描和确认

PAM支持帐号扫描的资产类型和要求如[Table 1](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0004.html" \l "task_m14_4tb_p2b__table_ztn_g4q_w2b)所示。

| Table 1. 支持帐号扫描的资产类型和要求 | |
| --- | --- |
| **资产类型** | **要求** |
| Windows | 对于Windows系统，PAM能够扫描系统中属于**Administrators**和**Remot Desktop Users**组中的用户，支持RPC和Agent两种方式。  如果使用RPC方式，目标设备和PAM需要满足如下要求。  如果目标设备上已安装Agent，且Agent上已配置PAM的IP地址和端口（缺省端口是TCP 3301），则不需要要目标设备在PAM上托管密码。   * **Windows设备**   + 目标设备上已打开TCP的135、139和445端口，且防火墙允许PAM访问这些端口。   + 如果目标设备的版本是Windows Server 2003，请共享admin$的权限。 * **PAM**   已在PAM上托管目标设备上属于Administrators组的帐号密码。 |
| Linux和IBM AIX | * **Linux和IBM AIX设备**   帐号已配置密码或者密钥。   * **PAM**   + PAM上资产的访问协议（SSH或者Telnet）配置正确。   + 已在PAM上托管目标设备上的特权帐号密码。 |
| HP UX | * PAM上资产的访问协议（SSH或者Telnet）配置正确。 * 已在PAM上托管目标设备上的特权帐号密码。 |
| Oracle | 已在PAM上托管目标系统上属于SYSDBA角色的帐号密码。  Note: PAM会在扫描结果中过滤掉SYS、DBSNMP等内置帐号。 |
| MSSQL | 已在PAM上托管目标系统上的特权帐号（可以不属于sysadmin角色）密码。 |
| Weblogic | 已在PAM上托管目标系统上属于administrator角色的帐号密码。 |

PAM支持以下几种帐号扫描方式。

* **手动精准扫描**：对指定的具体资产进行帐号扫描。
* **手动范围扫描**：对指定IP地址段内的资产进行帐号扫描。
* **自动定期发现**：定期对所有资产进行帐号扫描。

PAM扫描目标设备的帐号时，会与前一次的扫描结果对比，仅展示有变化的资产和帐号。例如：资产A本次扫描到的帐号与前一次相比无变化，则资产A不会展示在扫描结果中。如果扫描失败，PAM会给出失败原因。

PAM支持以下几种查看扫描结果的方式。

* 扫描任务执行过程中，直接在帐号扫描中查看。
* 扫描任务执行结束后，在帐号确认中查看。
* 扫描任务执行结束后，在帐号管理 > 仪表盘 > 幽灵帐号中查看。

帐号扫描能发现的帐号属性如[Table 2](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0004.html" \l "task_m14_4tb_p2b__table_zgc_3wx_w2b)所示。注意PAM不会获取帐号对应的密码。

| Table 2. 帐号扫描发现的帐号属性 | |
| --- | --- |
| **属性** | **说明** |
| 帐号名 | 帐号的名称。 |
| 类型 | * 普通帐号 * 特权帐号 |
| 状态 | * 新增：目标设备上存在但PAM上不存在的帐号。 * 删除：目标设备上不存在但PAM上存在的帐号。 |

1. 选择工作台 > 帐号管理 > 帐号维护 > 帐号发现。
2. 配置帐号发现。 
   * **手动精准扫描**

单击手动扫描帐号，选择精准扫描，选中要扫描的资产，单击确定。

如果资产数量大，可通过以下方式查找满足条件的资产。

* + - 在搜索文本框中输入资产名称、IP或者简要说明的关键字。
    - 单击筛选，使用资产的属性设置过滤条件，单击筛选。

扫描过程中，界面下方会显示扫描进度，如果不想继续扫描，请单击终止扫描。扫描结束后请单击返回。

* + **手动范围扫描**

单击手动扫描帐号，选择范围扫描，输入起始IP和结束IP，单击确定。

扫描过程中，界面下方会显示扫描进度，如果不想继续扫描，请单击终止扫描。扫描结束后请单击返回。

* + **自动定期扫描**

单击界面右上角的，然后再单击设置定期发现，设置各参数，完成后单击确定。

| **参数** | **说明** |
| --- | --- |
| 执行时间 | 定期发现的执行日期和时间，同时这也是第一次执行定期发现的日期和时间，后续按照配置的间隔执行。 |
| 执行间隔 | 定期扫描的执行间隔，可以配置为按天或者按月。   * + - 天：取值范围是1~365。     - 月：取值范围是1~12。 |
| 任务通知 | 单击添加通知用户，选择接收任务通知的用户，完成后单击确定。  如果用户数量大，在搜索文本框中输入帐号或者姓名的关键字来查找满足条件的用户。 |

如果想查看定期发现的日志，请单击界面右上角的，然后再单击下载日志，将json格式的日志保存在本地PC上查看。

定期发现的执行结果统计，请在帐号管理 > 仪表盘 > 最近任务 > 帐号发现中查看。

1. 单击扫描历史记录，在弹出的对话框中单击详情，查看历史扫描结果的详细情况，单击下载，下载历史扫描结果。

下载的历史扫描结果文件中包括资产名称，资产IP，资产类型，资产责任人，帐号名，帐号类型和帐号状态信息。

帐号扫描结束后，PAM发送通知消息和通知邮件给资产的责任人。如果存在幽灵帐号，PAM会给资产责任人下发**帐号发现**工单。

Note: 如果帐号扫描前资产没有配置责任人，请先给资产配置责任人，然后在帐号确认中单击重发提醒，资产责任人会收到通知。

### 帐号编辑和录入

PAM下发**帐号发现**工单给资产责任人后，资产责任人单击打开工单或者直接进入待办工单中对帐号进行编辑、录入。

责任人能够编辑的帐号属性包括：

* 帐号类型：取值包括普通帐号和特权帐号。
* 是否可改密：取值包括可改密和不可改密。
* 密码：手工输入帐号的密码、切换自或者私钥。

Note: 责任人也可以通过[配置改密计划](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0005.html" \o "改密计划支持按照设定的周期、时间和规则对RIS中帐号资产按照资产类型和帐号类型进行定期自动改密。)实现密码自动托管，而不是手工输入。

对于状态为新增的幽灵帐号，录入表示在PAM上增加该帐号；对于状态为删除的幽灵帐号，录入表示在PAM上删除该帐号

PAM支持以下几种资产编辑和录入方式。

* 逐个编辑和录入：编辑帐号属性后直接录入。
* 逐个编辑批量录入：逐个编辑帐号属性后，多个帐号一次性录入。
* 批量编辑和录入：将帐号以Excel格式下载到本地PC后编辑，然后再上传到PAM，实现批量编辑和录入。

Note: 如果资产责任人仅录入帐号，不对帐号进行编辑，可以直接选择工作台 > 帐号管理 > 仪表盘，单击幽灵帐号，然后再单击帐号对应的确认，将帐号录入PAM。

1. 资产责任人单击界面右上角的，单击帐号发现的查看详情，跳转到待办工单界面。
2. 单击处理。
3. 编辑和录入帐号。 
   * **逐个编辑和录入**

单击帐号编辑对应的各个属性进行修改，完成后单击录入。

* + **逐个编辑批量录入**

逐个单击帐号编辑对应的各个属性进行修改，完成后选中多个帐号，单击批量录入。

* + **批量编辑和录入**
    1. 选择资产或者帐号，单击批量编辑，单击下载模板，将模板文件保存到本地PC。
    2. 打开本地模板文件，设置各参数（参数说明请参见[配置资产的帐号和密码](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mr_0010.html" \o "创建资产后，用户可以在RIS上添加访问资产的帐号和密码，即将密码托管在RIS上，这样用户访问目标设备时由RIS代替用户输入帐号和密码。用户也可以只添加帐号或者帐号和密码都不添加，在访问目标设备时由用户手工输入。)），完成后保存文件。
    3. 单击批量编辑，然后单击上传文件，选择编辑好的模板文件，单击开始导入，完成后单击关闭。

Note:

* + - * 不需要导入的帐号和密码，请直接单击帐号和密码对应的，从列表中删除该帐号和密码。如需使该帐号下次扫描时不再被发现，请执行[帐号排除](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0004.html#task_mbb_1fq_wjb)。
      * 单击下载导入结果，查看导入的帐号。

### 帐号排除

所有有帐号管理权限的角色都能执行帐号排除。

PAM支持对帐号发现找到的幽灵帐号进行排除，即添加例外。将幽灵帐号排除以后，这些帐号将不再被标记为幽灵帐号，并且后续帐号发现的结果中也将不包含这些帐号。

排除和取消排除操作记录操作日志，可以在工作台 > 审计 > 事件审计 > 配置日志中查看。

**排除幽灵帐号**

1. 选择工作台 > 帐号管理 > 仪表盘。
2. 在需要关注的帐号中，单击幽灵帐号对应的数字。

Note: 必须执行过帐号发现，存在未处理的幽灵帐号。

1. 对需要排除的帐号单击排除，将这些帐号添加到帐号排除列表中。

幽灵帐号被排除后，将从幽灵帐号列表、帐号扫描结果和责任人的帐号确认工单中删除。

**查看已排除帐号**

1. 在工作台 > 帐号管理 > 帐号维护 > 帐号发现，单击右上角的已排除帐号，查看所有已被排除的幽灵帐号。

**取消排除帐号**

1. 对需要取消排除的帐号单击取消排除，或勾选多个帐号后，勾选批量取消排除。

取消排除后，该帐号不会再添加到幽灵帐号列表、帐号扫描结果和帐号确认工单中，但下次执行帐号发现时将重新发现该帐号。

## 配置改密计划

改密计划支持按照设定的周期、时间和规则对PAM中帐号资产按照资产类型和帐号类型进行定期自动改密。

在使用改密计划前，请先完成以下配置工作：

* [配置改密规则](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0011.html#task_a4h_d5b_p2b)。
* [配置资产、帐号和密码](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mr_0003.html#ug_mr_0003)。

PAM执行改密计划的流程如[Figure 1](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0005.html" \l "ug_ma_0005__fig_ggb_nll_ggb)所示。

Figure 1. 改密流程图

Note: 当改密计划关联的密码规则中，备份方式勾选的是邮件备份时，如果使用本地postfix转发的方式发送密码备份邮件，PAM统一认为密码备份成功；如果不使用本地postfix转发的方式发送，PAM将根据邮件服务器的响应来判断密码是否备份成功。

PAM支持帐号改密的资产类型和要求如[Table 1](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0005.html" \l "ug_ma_0005__table_ztn_g4q_w2b)所示。

| Table 1. 支持帐号改密的资产类型和要求 | |
| --- | --- |
| **资产类型** | **要求** |
| Windows | Windows系统支持RPC和Agent两种方式，推荐使用Agent方式。  Note: 请参照以下方式安装Agent：   1. 单击右上角的用户姓名，并选择帮助 > 其他应用 > 下载 > Windows相关应用，单击下载Agent。 2. 将agent.exe上传到资产上并安装。 3. 设置地址为PAM的地址，如PAM为HA部署，则填写虚IP地址；集群部署则填写外部虚IP地址。   如之前已安装了Agent，PAM会检查并自动升级所连接的Agent到最新版本。  如果目标设备上已安装Agent，且Agent上已配置PAM的IP地址和端口（缺省端口是TCP 3301），则不需要要目标设备在PAM上托管密码。  如果使用RPC方式，目标设备和PAM需要满足如下要求。   * **Windows设备**   目标设备上已打开TCP的135、139和445端口，且防火墙允许PAM访问这些端口。   * **PAM**   已在PAM上托管目标设备上属于Administrators组的帐号密码。 |
| Linux / HP UX / IBM AIX和网络设备 | * **Linux / HP UX / IBM AIX和网络设备**   帐号已配置密码或者密钥。   * **PAM**   + PAM上资产的访问协议（SSH或者Telnet）配置正确。   + 已在PAM上托管目标设备上的特权帐号密码。   Note: 特权帐号如配置了切换自，PAM在改密时支持根据配置自动完成切换。但对于自定义类型的资产，需要在[资产适配](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0024.html" \o "对于有些比较特殊的登录提示符，通过内置代填提示符无法匹配成功时，需要针对这些资产进行适配。)中配置帐号切换命令，否则帐号切换可能失败。 |
| Oracle | 已在PAM上托管目标系统上属于SYSDBA角色的帐号密码。  Note: PAM会在扫描结果中过滤掉SYS、DBSNMP等内置帐号。 |
| MSSQL | 已在PAM上托管目标系统上的特权帐号（可以不属于sysadmin角色）密码。 |
| Weblogic | 已在PAM上托管目标系统上属于administrator角色的帐号密码。 |

1. 选择工作台 > 帐号管理 > 帐号维护 > 改密计划。
2. 单击新建改密计划。
3. 在弹出的窗口中配置改密计划的各项参数，并单击下一步。

改密计划的具体参数说明如下：

| **参数** | **说明** |
| --- | --- |
| 计划名称 | 改密计划的名称。 |
| 执行方式 | * + 手工执行：PAM会在指定时间通知用户改密，用户可以单击立即执行来改密。   + 自动执行：PAM会在指定时间自动改密并通知用户。 |
| 下次执行时间 | 对于手工执行，是下一次通知用户改密的时间；对于自动执行，是下一次自动执行该改密计划的时间。 |
| 执行间隔 | 对于手工执行，是发送改密通知周期的间隔天数；对于自动执行，是改密计划的执行周期间隔天数。 |
| 登录测试 | 可以根据需要勾选。如勾选，改密计划完成后，PAM将执行登录测试，并返回改密后的登录测试结果，供用户参考。 |
| 通知方式 | 可以根据需要勾选一个或多个通知方式。对于手工执行，将会提醒用户执行手工改密；对于自动执行，会在改密开始时和改密完成后各发送一个通知，通知中只会给出改密计划的名称，不会显示具体密码。   * + 邮件通知：将改密提醒通过邮件发送给通知人。   + 站内通知：将改密提醒通过右上角的站内提醒发送消息给通知人。 |
| 通知人 | 可以根据需要勾选一个或多个通知人。通知人必须超级管理员、配置管理员或其他拥有帐号管理和资产权限的自定义角色。对于邮件通知，必须是配置了邮箱的用户；对于站内通知，用户可以不配置邮箱。 |
| 简要说明 | 改密计划的简要说明。 |

1. 选择改密所使用的密码规则，完成后单击下一步。

密码规则可以选择模板选择和新建模板：

* + 模板选择：从已有的密码规则模板中选择一个，在下拉菜单中选取。
  + 新建模板：新建一个密码规则模板，相关参数的配置请参见[配置密码规则](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0011.html)。

1. 为改密计划关联待改密的帐号。

不同方式关联的帐号，在生效时将取并集。有以下三种方式：

* + 指定帐号：单击之后，在所有可改密的帐号中勾选若干个待改密的帐号，并单击确定。也可以单击右上角的批量关联，在弹出的批量更新对话框中下载批量关联模板并填写所有待关联帐号后上传。
  + 动态关联：单击之后可以配置动态规则。不同规则在生效时会取交集：
    - 在资产或帐号后单击，设置规则的属性、匹配和内容。资产可以设置的内置属性包括资产名、IP、简要说明、责任人、资产组和资产类型；帐号可以设置的内置属性包括**指定帐号**和**帐号类型**。
    - 可以单击或，对规则进行修改或删除。
    - 可以单击左下角的查看帐号，查看当前设置的规则可以关联上哪些帐号。

全部确认无误后单击确定保存动态关联的修改。

* + 域帐号：单击之后，在所有可以改密的域帐号中勾选若干个待改密的域帐号，并单击确定。域帐号在资产 > 配置 > Windows域中设置。

Note: 改密计划的执行还将受到交互超时时间和任务执行超时时间的影响，默认为20秒和180秒。若在执行过程中登录资产或执行脚本超过了设定的时间，将导致改密失败。用户可以在[配置资产适配](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0024.html" \o "对于有些比较特殊的登录提示符，通过内置代填提示符无法匹配成功时，需要针对这些资产进行适配。)中，对特定的资产手动设置交互超时时间和任务执行超时时间。

1. 确认三个页签信息是否设置正确。可以单击上一步检查前几步设置的信息，确认全部正确后单击保存，完成改密计划的创建。

执行改密计划后，密码规则中配置的备份方式对应的备份人，将在改密开始和改密完成后分别收到通知，两个通知中分别包含旧密码和新密码。密码的ZIP包需要使用该用户在帐号设置 > 信息加密中设置的ZIP文件密码或PGP密钥进行解压。

可以单击密码备份下载，将当前改密计划对应的帐号的密码下载到本地。下载后的ZIP包同样需要进行解密。

已添加的改密计划，将在该页面的表格中显示以下相关信息。

| **项目** | **说明** |
| --- | --- |
| 改密计划 | 改密计划的名称。 |
| 状态 | 改密计划的状态，取值范围是无、正在执行和正在终止。 |
| 执行方式 | 自动或手动。 |
| 关联帐号 | 改密计划将要修改密码的帐号的数量。 |
| 上次改密结果 | 仅当该改密计划被执行后才会出现。显示最近一次改密帐号数量以及改密成功和改密失败的帐号数量。可以分别单击成功或失败查看具体成功或失败的信息。  Note: 改密成功时，改密的日志信息内容默认为空。如需显示详细的改密过程信息，需要超级管理员[修改配置文件](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0065.html)，在shterm.conf中设置shterm.changepwd.success.detail=true。修改后无需重启，下次执行改密计划成功时将看到详细的日志信息。 |
| 下次执行时间 | 改密计划下一次执行的时间。当改密计划在执行时，显示为正在执行。 |
| 简要说明 | 改密计划的简要说明。 |
| 操作 | * 编辑：单击编辑修改改密计划的参数，参数解释请参见新建改密计划的步骤。 * 立即执行：单击立即执行，手动执行一次该改密计划。 * 终止执行：改密计划正在执行时，单击该按钮，取消继续执行改密计划。取消后，未执行改密的帐号数量会记录在上次改密结果列表中。   Note: 只有在密码备份结束后，才能终止改密计划。终止执行将仅终止未进行的改密，当前正在执行改密的帐号还是会继续改密。   * 历史记录：仅当该改密计划被执行后才会出现。单击历史记录查看该改密计划每次被执行的记录信息。   单击历史记录对话框中已执行的改密计划对应的改密记录，可以查看具体的改密信息，并可以在弹出的对话框中导出改密计划的执行结果的Excel文件。  其中，改密失败的原因有连接设备超时、密码错误、网络异常、帐号过期、帐号被锁定、帐号权限不足和未知这七类。 |

Note: 当改密帐号在[配置应用改密](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ma_0014.html)中配置了对应的应用时，改密后会将新密码更新到应用所在的Agent。因此PAM会检查该Agent是否在线，如不在线，改密计划的执行将失败。如确认不需要进行密码同步，请删除应用配置中的该Agent所在的服务器，并重新执行改密计划。

通过编辑改密计划，可以设置改密计划是否禁用为活动或禁用。改密计划被禁用后，将不会自动执行，也将默认不显示在改密计划列表中。只有单击筛选并设置是否禁用为禁用时，才能看到所有被禁用的改密计划。

## 配置密码备份

目标设备的帐号和密码在PAM托管后，为了保证密码的安全性，请定期备份密码。

* 已完成[配置信息加密](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0013.html)，PAM使用该密码或密钥加密密码文件，用户收到密码文件后也需要使用该密码或密钥解密。
* 如果密码备份到文件服务器，请先完成[配置文件服务](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0028.html)。
* 如果密码发送到用户邮箱，请先完成[配置邮件服务](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0027.html" \o "RIS支持通过邮件发送通知和告警，要正常使用这些功能，需要配置邮件服务。)。

PAM支持的密码备份方式包括：

* 文件服务：密码文件定期备份到文件服务器。
* 邮件服务：密码文件定期发送到用户邮箱。

Note: 为了确保密码的安全性，PAM备份时会对密码文件加密。

1. 选择工作台 > 帐号管理 > 帐号维护 > 密码备份。
2. 选择启用，开启密码备份。
3. 设置各参数，完成后单击确定。

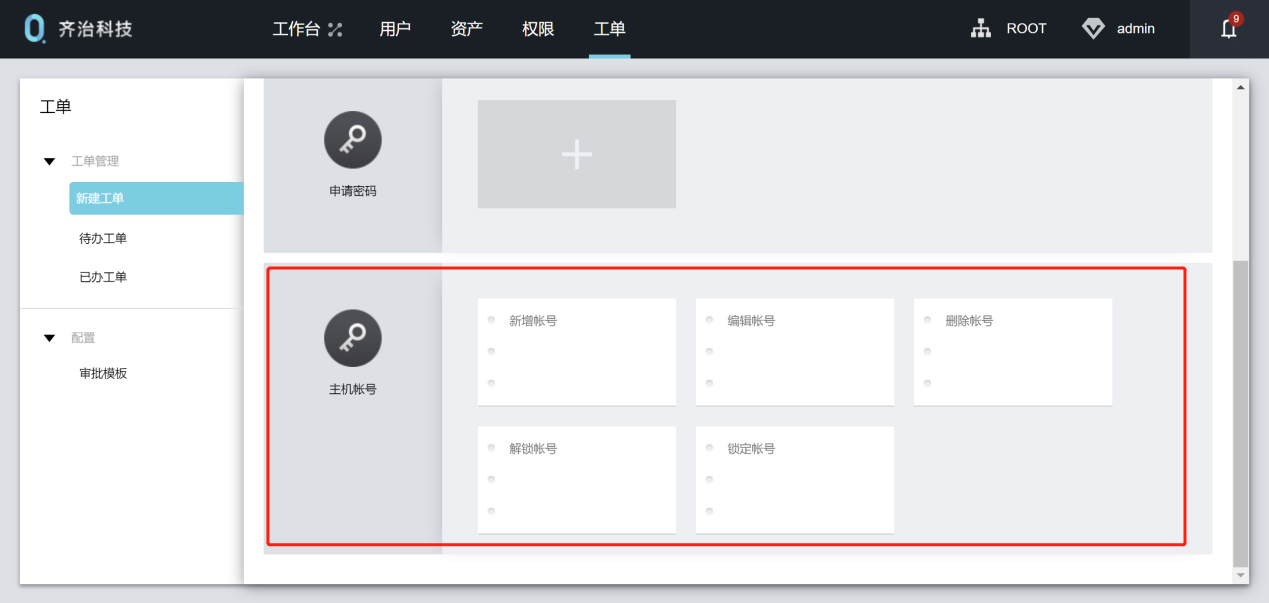
| **参数** | **说明** |
| --- | --- |
| 执行时间 | 密码备份的执行日期和时间。 |
| 执行间隔 | 密码备份的执行间隔。   * + 月：执行间隔是月。整数形式，取值范围是1～12。   + 天：执行间隔是天。整数形式，取值范围是1~365。 |
| 密码分段 | 密码备份时是否分段。   * + 如果选择是，密码将被分成两段，前、后半段需要分别选择不同的备份方式和通知用户。   + 如果选择否，密码被作为一个整体备份。 |
| 备份方式 | 密码备份采取的方式。选择好备份方式后，请单击添加通知用户来设置接收密码备份通知的用户。   * + 邮件备份：加密后的密码以邮件的方式发送给通知用户，请确保该用户的邮箱已配置。邮件备份的具体配置请参见[基本设置：配置邮件服务](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0027.html" \o "RIS支持通过邮件发送通知和告警，要正常使用这些功能，需要配置邮件服务。)。   + 文件备份：加密后的密码上传到文件服务器，发送给通知用户。文件备份的具体配置请参见[基本设置：配置文件服务](mk:@MSITStore:C:\Temp\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_ms_0028.html)。   用户收到加密的密码文件后，请使用[配置信息加密](mk:@MSITStore:C:\\Temp\\RIS数据中心风险洞察系统3.3.9%20用户手册(高级版).chm::/um/ug_mi_0013.html" \o "仅当用户类型为超级管理员和配置管理员时会显示该页签并可以配置。当RIS需要将密码信息提供给用户时（例如密码备份），会按照用户设置的密码对信息进行加密，从而确保文件的安全性。)中配置的密码或密钥解密。 |
| 执行记录 | 单击查看，查看密码备份的执行记录。 |
| 下载 | * + **全量下载**：超级管理员单击全量下载，直接下载包含密码的备份文件。   + **配置下载（无敏感信息）**：超级管理员或配置管理员单击配置下载（无敏感信息），直接下载不包含密码的备份文件。   Note: **全量下载**和**配置下载（无敏感信息）**需要超级管理员用户在系统设置 > 其他 > 高级设置中手动开启。 |

配置完成后，可以单击立即执行，手动执行一次密码备份。 如需暂时停用密码备份功能，请选择禁用并单击确定。禁用后不会保存执行时间和间隔的设置，下次启用后需要重新设置。但备份方式设置不受禁用影响，用户在配置密码规则或改密计划时，可以使用此处配置的备份方式。

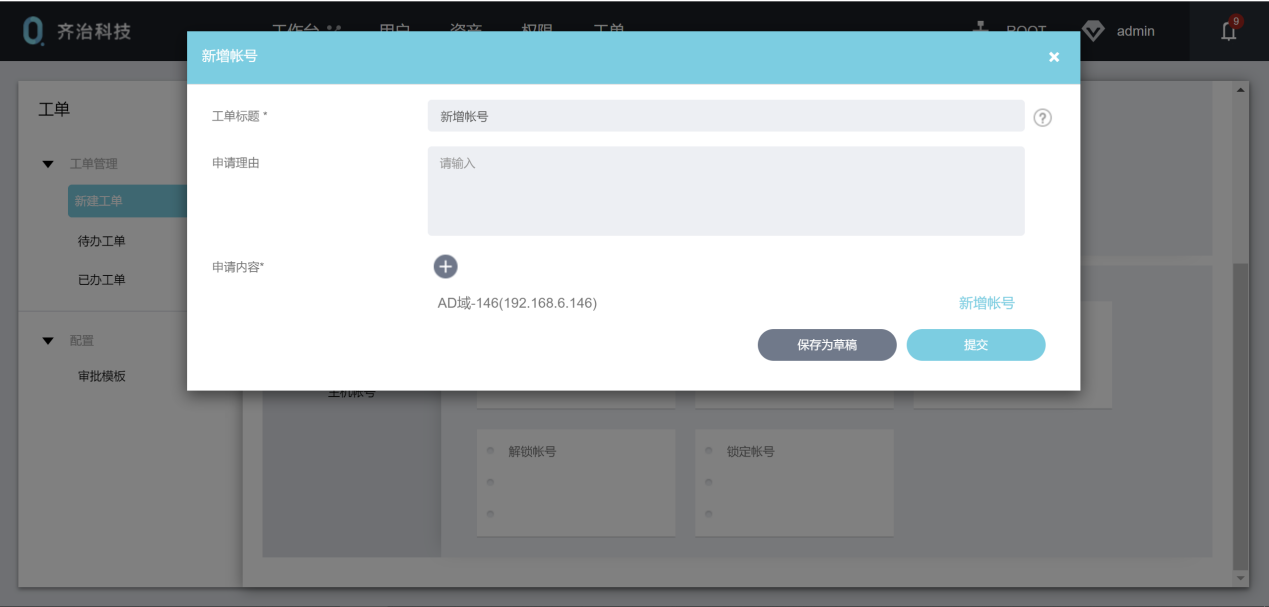


## 生命周期管理

PAM支持账号集中化管理功能，可详细记录相应账号从创建至删除的一系列变更操作。同时系统引入自动化管理手段，采用工单流的模式实现对特权账号创建、变更、修改、锁定、删除进行统一维护，统一管控。



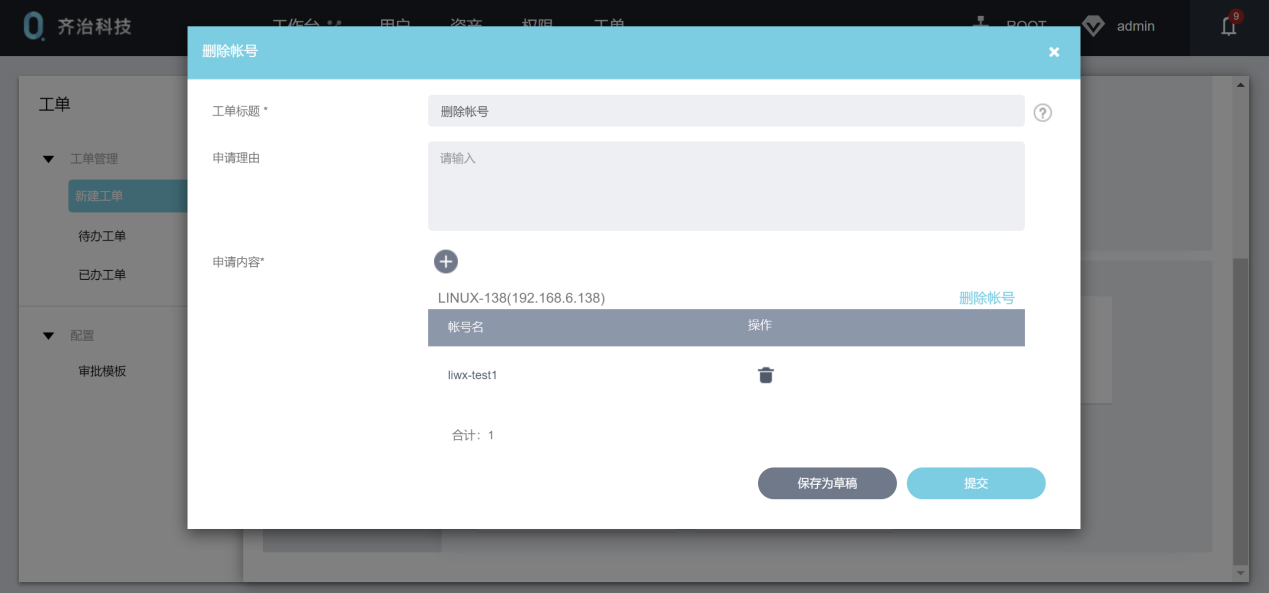
新增账号



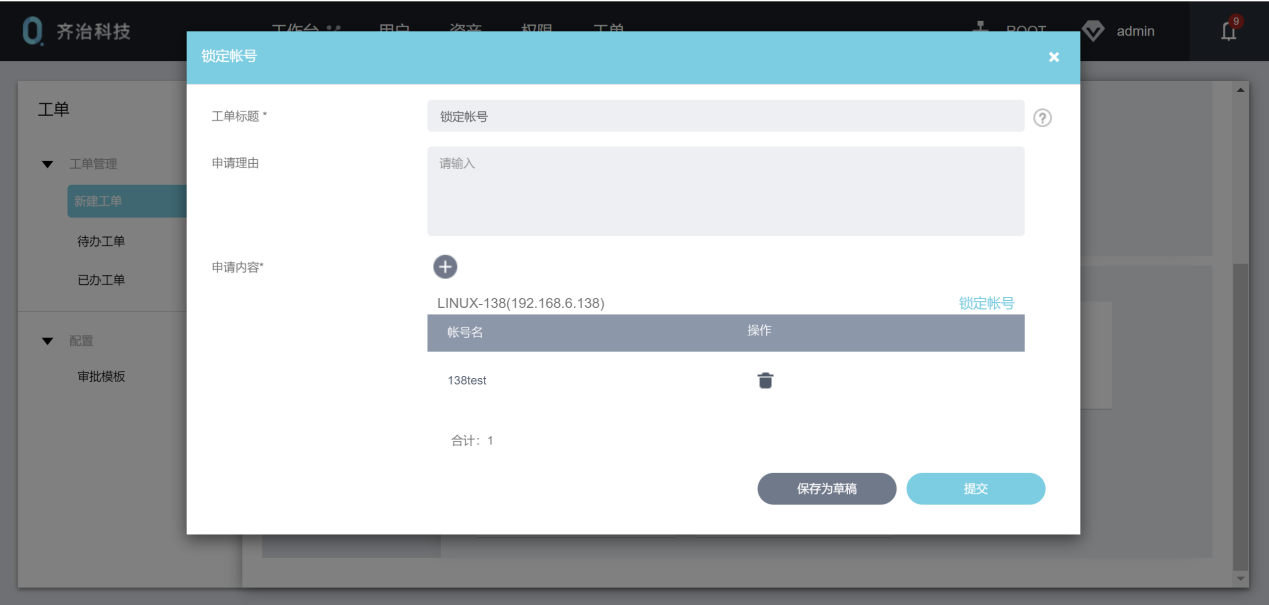
编辑账号



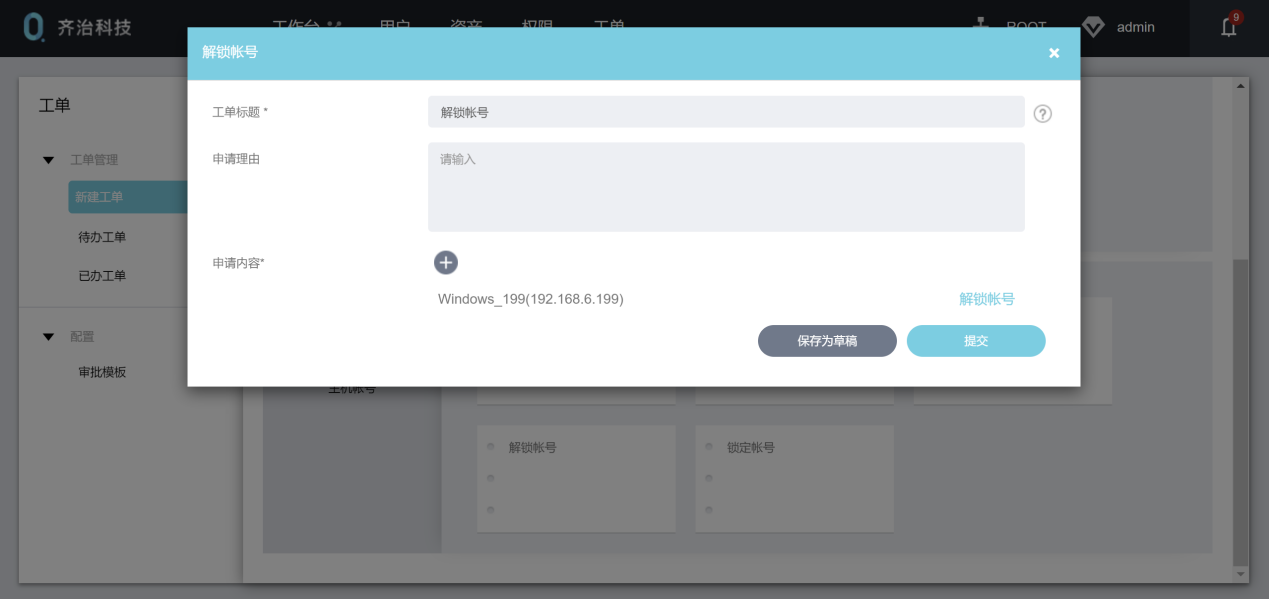
删除账号



锁定账号

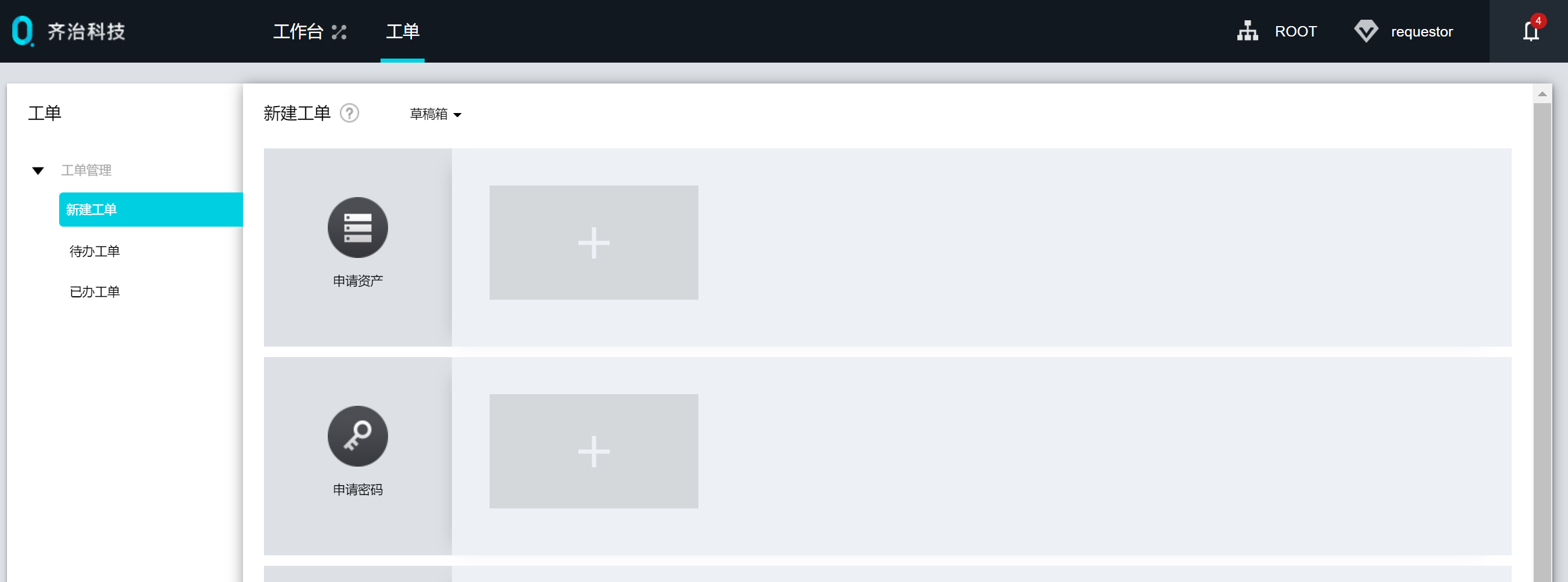


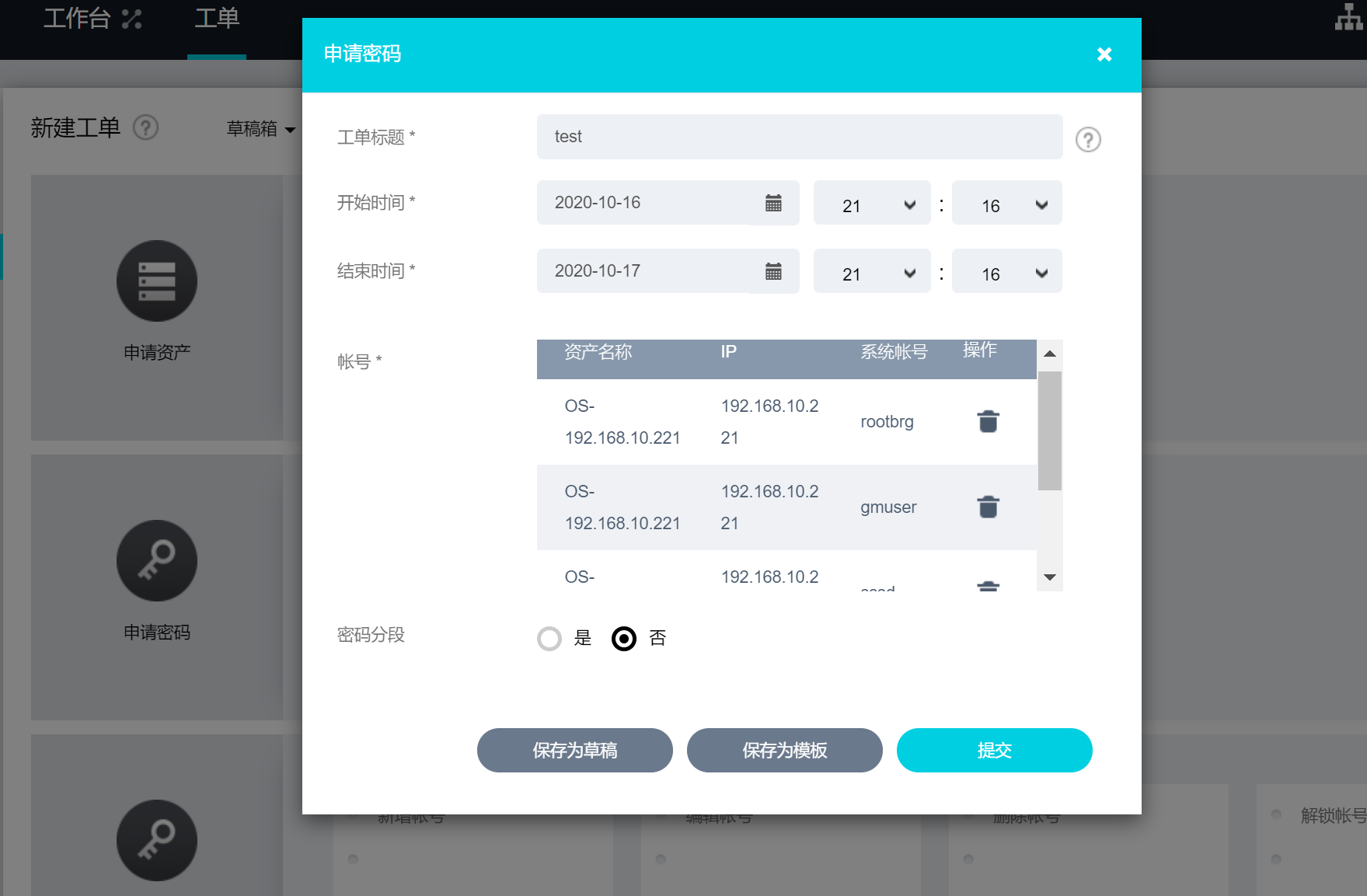
解锁账号



## 密码工单管理

申请密码





审批人登录系统审批



申请人再登陆系统进行查看



