UNIS A2000-E运维管理系统
典型配置举例

目录

用户

1

目录:

举例：LDAP认证

通过配置LDAP认证可以实现用户帐号登录A2000-E 运维管理系统时使用LDAP进行集中身份验证。

在配置LDAP前，请确保您已经理解了LDAP相关的概念和术语。

A2000-E 运维管理系统缺省提供一个名称为**LDAP**的认证方式（名称支持修改），状态为禁用。用户可以使用缺省的认证方式，也可以创建新的LDAP认证服务器。本节以新建LDAP认证服务器为例进行介绍。

请使用超级管理员进行以下操作。

1. 准备LDAP基本信息。

包括：

- 服务地址和端口：LDAP通讯端口默认为389，如果要使用SSL默认的端口为636。
- 查询用户DN和密码：查询用户DN可以在LDAP服务器通过ldapsearch命令获取。如果LDAP允许匿名查询，也可以不提供。
- BaseDN：需要登录A2000-E 运维管理系统的用户DN的范围，比如"dc=mydomain,dc=org"。
- 用户名属性：LDAP中的登录名的属性名称，如uid、cn等。
- SSL相关文件：如果要使用SSL，还需要提供LDAP服务的CA证书，如果LDAP服务器要求使用证书验证A2000-E 运维管理系统的身份，您还需要准备A2000-E 运维管理系统的客户端证书（CERT）和对应的KEY文件。当然如果不要求客户端身份验证，您也可以不提供上述文件。

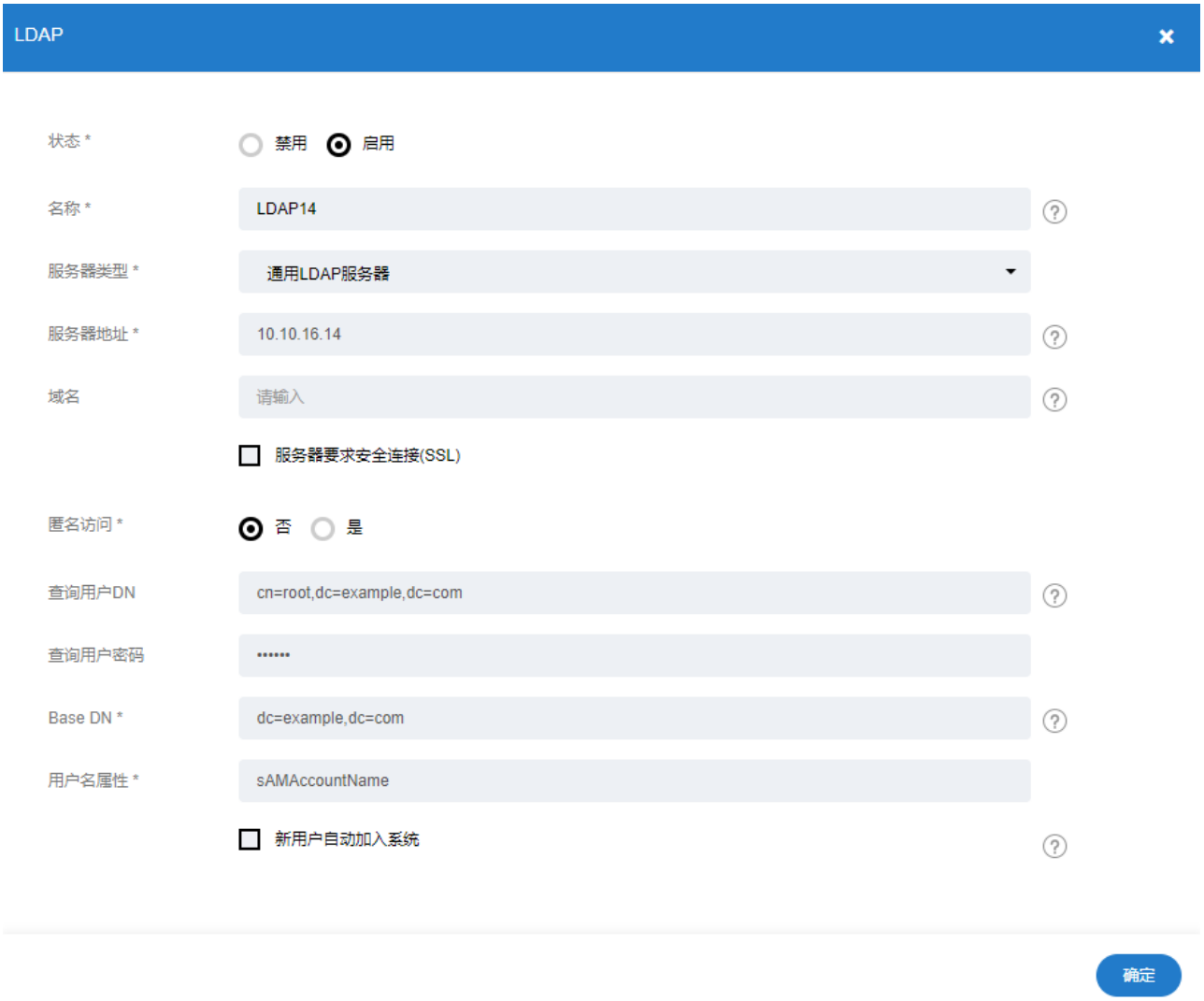
2. 在A2000-E 运维管理系统中设置LDAP服务器。

a) 单击右上角的用户帐号（比如admin），选择**系统设置**。

b) 选择**用户** > **登录认证** > **LDAP**，单击**添加**。

c) 选择**服务器类型**为**通用LDAP服务器**。

d) 设置各参数，完成后单击**确定**。



说明:

- 如果您希望LDAP中的用户自助登录A2000-E 运维管理系统，您可以选中**新用户自动加入系统**，然后设置新用户的角色。设置完成后LDAP中的用户可以直接用LDAP中的用户名和密码登录A2000-E 运维管理系统，用户首次登录时会自动建立同名的用户帐号。
- 如果勾选了**服务器要求安全连接(SSL)**，但是不希望提供证书，您可以勾选**允许忽略无效证书**。

3. 设置用户帐号的身份验证方式。

a) 选择**用户** > **用户管理** > **用户列表**，单击**新建用户**。

b) 选择用户角色后，单击**下一步**。

c) 设置各参数，单击**创建**。

- 帐号：一般填写LDAP的登录名。
- 姓名：按实际填写。
- 身份验证：选择LDAP服务器的名称。

说明: 如果A2000-E 运维管理系统中的帐号和LDAP中的不一致，可以在**LDAP用户名**中单独设置LDAP中对应的帐号名。

如果配置正确，身份验证为LDAP的用户可以使用LDAP中的密码登录A2000-E 运维管理系统。

举例：RADIUS认证

1. 收集RADIUS服务器的信息。
   - 服务器的IP地址。
   - 服务器RADIUS服务的端口号。
   - 服务器RADIUS服务的共享密钥。
   - 服务器RADIUS服务支持的认证方式（例如：PAP或者CHAP）。
2. 确保A2000-E 运维管理系统能访问RADIUS服务器的认证端口。
3. 拥有超级管理员帐号。

RADIUS 是一种用于在需要认证其链接的网络访问服务器（NAS）和共享认证服务器之间进行认证、授权和记帐信息的文档协议。RADIUS在A2000-E 运维管理系统中，主要体现的是认证功能。

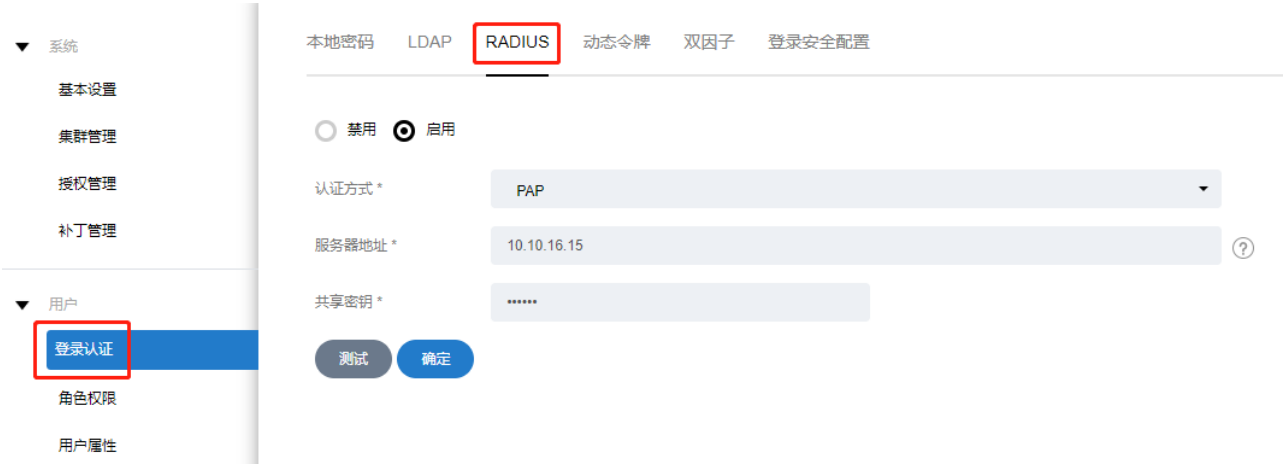
请使用超级管理员进行以下操作。

1. 配置RADIUS认证方式。

a) 单击当前帐号，选择**系统设置**。

b) 选择**登录认证** > **RADIUS**，输入RADIUS信息，单击**确定**。

- 选择**启用**。
- 认证方式：选择RADIUS服务器的认证方式（PAP或者CHAP）。
- 服务器地址：输入RADIUS服务器的IP地址。
- 共享密钥：输入RADIUS服务的共享密钥。



说明:

- 如果RADIUS使用的端口是非默认的1812端口，服务器地址输入格式为“IP地址:端口”。
- 如果使用主备RADIUS服务器，服务器之间可以使用“,”分隔。

2. 用户绑定RADIUS认证方式。

a) 选择**用户** > **用户列表** > **新建用户**。

b) 选择角色，单击**下一步**。

c) 设置用户信息，完成后单击**创建**。

- 帐号：输入登录帐号。
- 姓名：输入帐号登录者的真实姓名。
- 身份验证：选择RADIUS协议。
- RADIUS用户名：RADIUS用户名可以不填写，如果不填写，默认使用的名称就是帐号。

3. 用户登录测试。

   输入RADIUS的帐号密码，单击**登录**。

举例：动态令牌认证

A2000-E 运维管理系统支持基于时间的动态令牌认证。动态令牌可以独立作为一种认证方式，也可以和其他认证方式结合使用形成双因子认证方式。

- 已获取管理员分配的动态令牌。
- 已配置A2000-E 运维管理系统系统时间。请在**系统设置** > **系统** > **基本设置** > **系统时间**中配置。

> **说明：** A2000-E 运维管理系统支持手工修改和NTP同步两种方式修改系统时间和日期，推荐配置NTP方式。

TOTP （基于时间的一次性口令）使用加密散列函数将密钥与当前时间戳结合，来生成一次性口令。TOTP定期产生一个新口令，要求客户端和服务器能够十分精确的保持正确的时钟，客户端和服务端基于时间计算的动态口令才能一致。使用TOTP令牌不需要令牌和A2000-E 运维管理系统之间保持网络通信，也不需要其他额外的认证服务器。

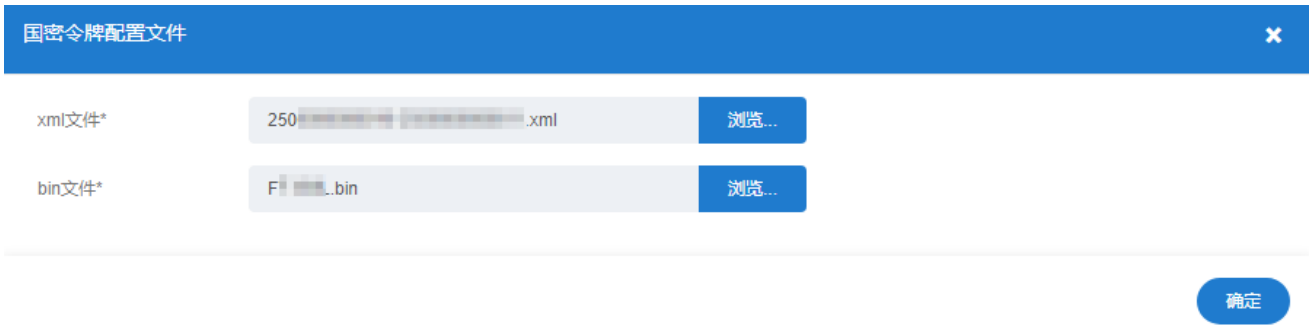
请使用超级管理员或系统管理员的帐号登录执行以下操作。

1. 单击右上角用户帐号（例如**admin**），选择**系统设置**。
2. 选择**用户** > **登录认证** > **动态令牌**。

3. 可选： 单击**配置PIN码安全性配置**，设置PIN码的参数信息，完成后单击**确定**。

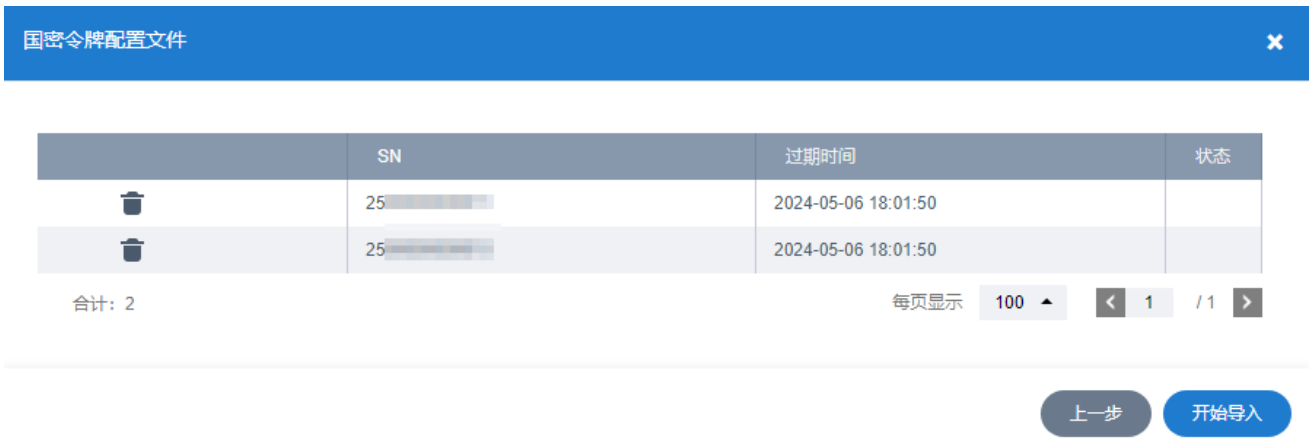
   PIN码使用本地密码的安全性设置，具体配置请参考《A2000-E 运维管理系统Web配置指导》中系统设置章节下的登录认证：配置本地密码参数。

4. 单击**国密令牌配置**，上传国密令牌的xml文件和bin文件，完成后单击**确定**。



说明: xml文件和bin文件由生产令牌厂家提供。

5. 成功读取到国密令牌信息后，单击**开始导入**，导入所有动态令牌。



说明:

- 如果读取令牌信息失败，请检查xml和bin文件是否匹配，内容是否正确。
- 如果不需要导入所有令牌，请单击删除不想导入的令牌后再执行导入。

配置完成后如下图所示。

说明:

- 如果动态令牌数量大，在搜索框中输入令牌的SN或者绑定用户名的关键字，可以筛选出特定的令牌。单击**重置**清空关键字，查看所有令牌。
- 如果使用双因子认证，请先在**用户** > **登录认证** > **双因子**中配置双因子认证，并将**认证方式2**选择为动态令牌，新建用户身份时身份验证选择刚才配置的双因子认证方式。

6. 设置用户帐号的身份验证方式。

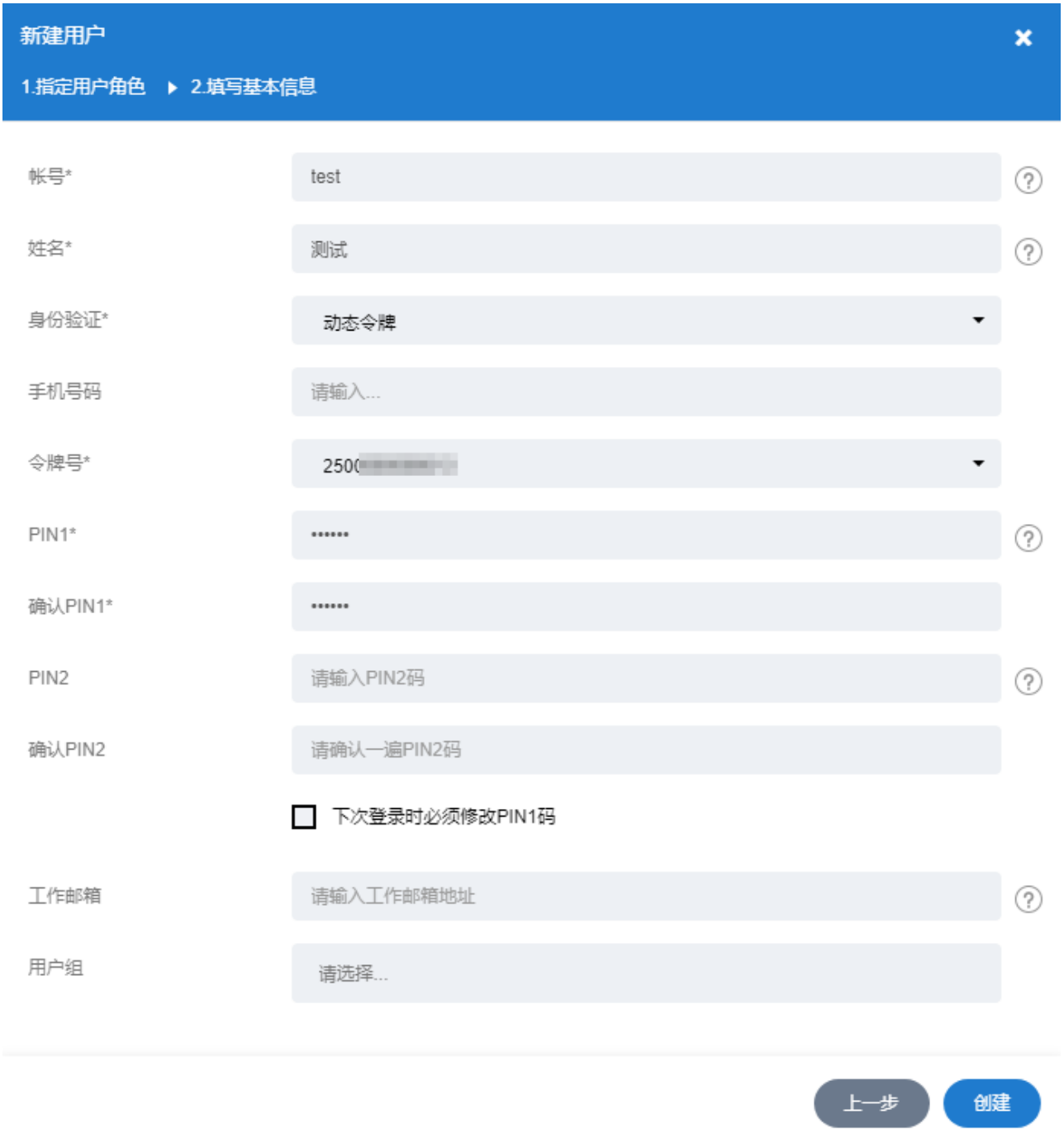
a) 选择**用户** > **用户管理** > **用户列表**，单击**新建用户**。

b) 选择用户角色后，单击**下一步**。

c) 设置各参数，单击**创建**。

参数	说明
帐号	登录帐号
姓名	帐号登录者的真实姓名

参数	说明
身份验证	动态令牌
令牌号	请选择A2000-E 运维管理系统已添加的动态令牌。 **说明:** 一个令牌只能和一个用户关联。令牌被用户关联后不能被删除。
PIN1/确认PIN1	用户自己登录A2000-E 运维管理系统使用**PIN1码+动态密码**。
PIN2/确认PIN2	用于会话复核。具体请参考《A2000-E 运维管理系统Web配置指导》用户管理章节中的配置用户（手工创建）小节。
下次登录时必须修改PIN1码	如果选中，用户首次登录时需要修改PIN1码。



7. 用户登录测试。

   输入登录的帐号密码，单击**登录**。

   说明:

   - 使用动态令牌登录认证时，输入PIN1码+动态密码。
   - 使用双因子认证时密码输入方式有以下两种。
     - 输入第一重密码后按回车或者单击**登录**按钮后再输入PIN1码+动态密码。
     - 输入组合密码：直接在第一个密码框中输入第一重密码+空格+PIN1码+动态密码。

举例：LDAP导入

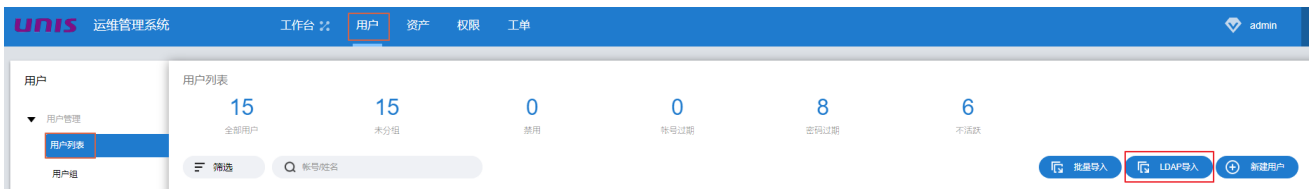
A2000-E 运维管理系统支持导入LDAP用户（LDAP服务器的用户）。导入A2000-E 运维管理系统的用户的缺省角色是操作员、状态是活动。

如果LDAP导入的用户使用LDAP认证，请先配置LDAP认证，如果使用其他认证方式，不需要配置LDAP认证。

本节将详细介绍批量导入LDAP用户的操作方式。已知数据信息如下表所示。

参数	取值	说明
LDAP地址	10.10.16.14	LDAP服务器的IP地址和端口，缺省端口号是389，如果使用SSL是636。 **说明：** 如果服务器的端口号是缺省的389或者636，仅输入IP地址即可；如果不是，输入格式为**IP地址:端口号**。
认证方式	密码认证	
baseDN	cn=root,dc=example,dc=com	查询用户DN。
密码	123456	查询用户的密码。
baseDN	ou=People,dc=example,dc=com	登录A2000-E 运维管理系统的用户DN的范围。
objectClass	objectClass=person	选择设置用户所属的分组。

1. 选择**用户** > **用户管理** > **用户列表**。
2. 单击**LDAP导入**。



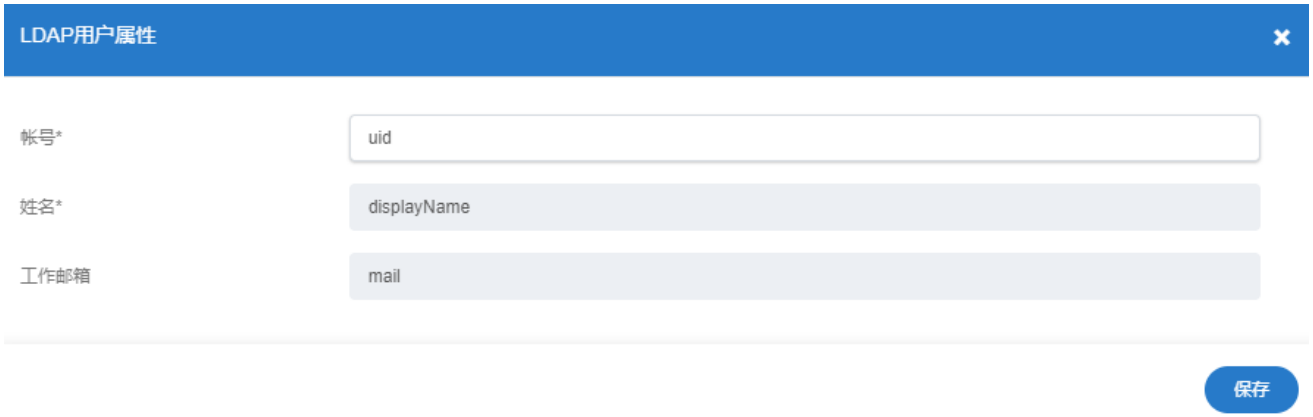
3. 设置各参数。

4. 可选： 如果是LDAP over SSL (LDAPS)服务器，请选中**服务器要求安全连接(SSL)**，设置各参数。

参数	**说明**
CA	LDAP服务器的CA证书，单击**浏览**选择文件上传。
CERT	A2000-E 运维管理系统的客户端证书CERT，单击**浏览**选择文件上传。
KEY	A2000-E 运维管理系统的客户端证书对应的KEY，单击**浏览**选择文件上传。
允许忽略无效证书	如果选中，A2000-E 运维管理系统不对LDAP服务器的证书进行合法性检查；如果不选，A2000-E 运维管理系统将对LDAP服务器的证书进行合法性检查，对于使用非知名CA签发证书的LDAP服务器，请务必上传CA证书。

5. 单击**设置ldap用户属性关系**，设置各参数，完成后单击**保存**。

参数	**取值**	**说明**
帐号	uid	配置将LDAP服务器上的用户的什么属性作为A2000-E 运维管理系统的帐号。缺省值为**uid**。
姓名	displayName	设置将LDAP服务器上的什么属性作为A2000-E 运维管理系统的姓名，缺省值为**displayName**。



6. 单击**查询**。

7. 可选： 单击**设置帐号选项**，设置各参数，完成后单击**保存**。

8. 单击**开始导入**。

说明: 不需要导入的帐号，请直接单击帐号对应的，从列表中删除该帐号。

导入时，如果A2000-E 运维管理系统上已存在相同的帐号，该帐号导入失败。

9. 可选： 单击**下载导入结果**，查看导入的帐号。

LDAP导入的用户的自定义用户属性为空，如果需要设置自定义属性或者需要修改用户的状态、帐号有效期、密码有效期等高级属性，请参考《A2000-E 运维管理系统Web配置指导》用户管理章节中的修改用户属性小节。

资产 2

目录:

举例：Linux资产管理和访问

本节以新增一个Linux资产，并使用SSH客户端访问该资产为例，详细介绍Linux主机资产管理和访问的具体方法。

已知数据信息如下表所示：

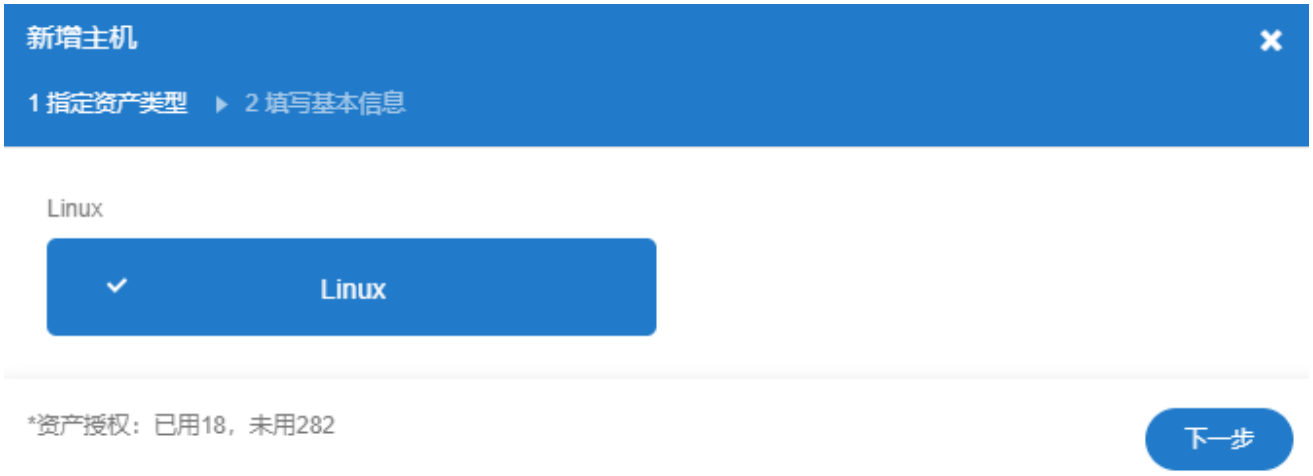
表 1: Linux资产数据信息

参数	取值	说明
资产名称	Linux-01	资产的名称。字符串格式，长度范围是1~100个字符。
资产IP	10.10.16.21	目标资产的IP。
系统帐号/密码	root/password	目标资产的登录帐号和登录密码。

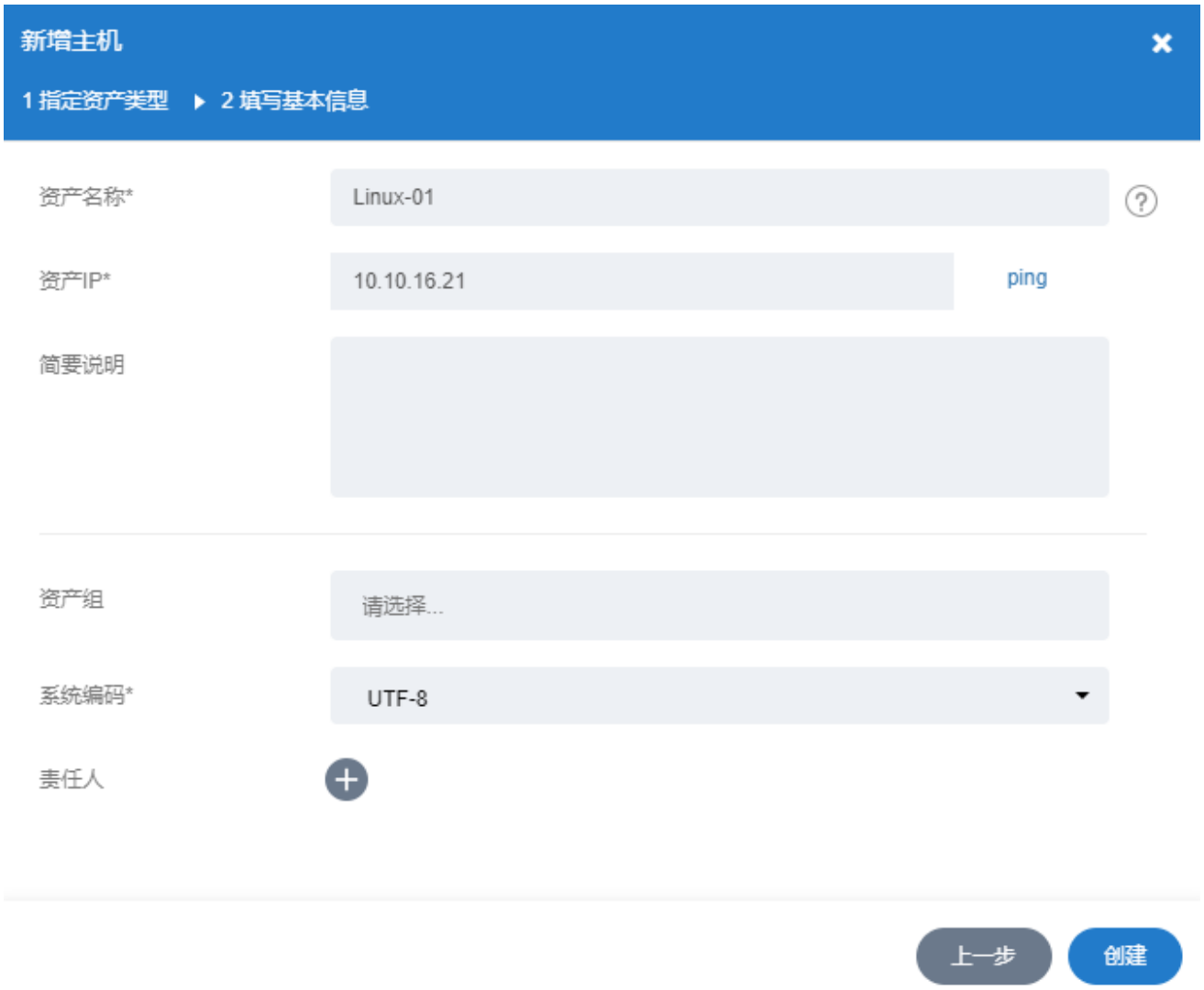
新建Linux主机资产

1. 选择**资产** > **资产清单** > **主机**，单击**新建**。

2. 选择**Linux**资产类型，单击**下一步**。



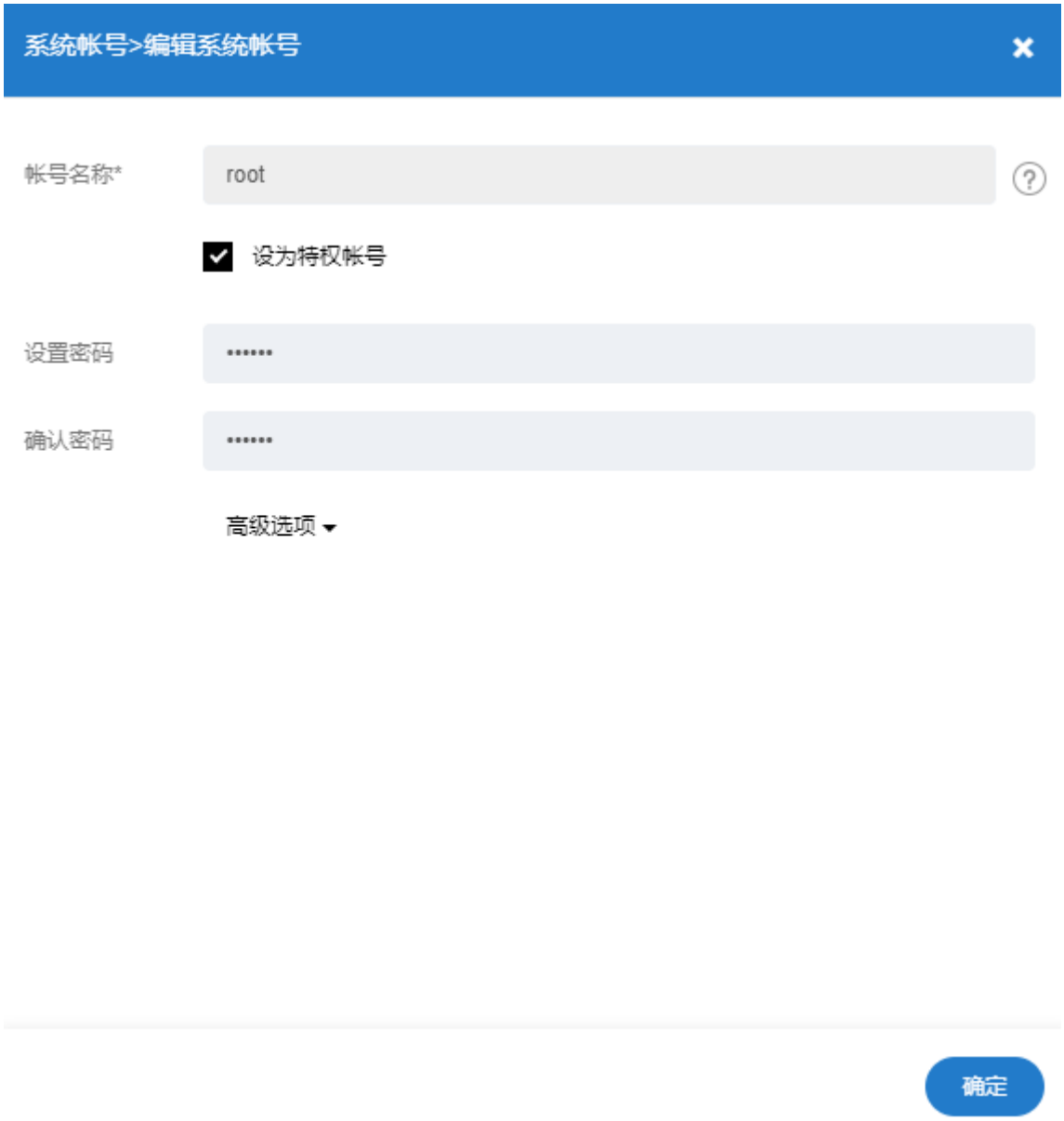
3. 设置各参数信息，完成后单击**创建**。



4. 单击Linux-01资产对应的**编辑**。

5. 选择**系统帐号**，并单击**root**帐号对应的**编辑**。

6. 在弹出的对话框中输入**root**对应的登录密码，完成后单击**确定**，并单击**保存**。



增加访问权限

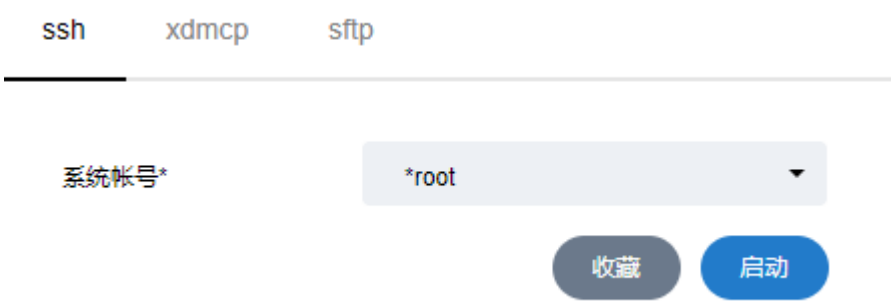
7. 选择**权限 > 权限配置 > 动态权限**，单击**新增动态权限**。

8. 设置动态权限的参数信息，完成后单击**保存**。

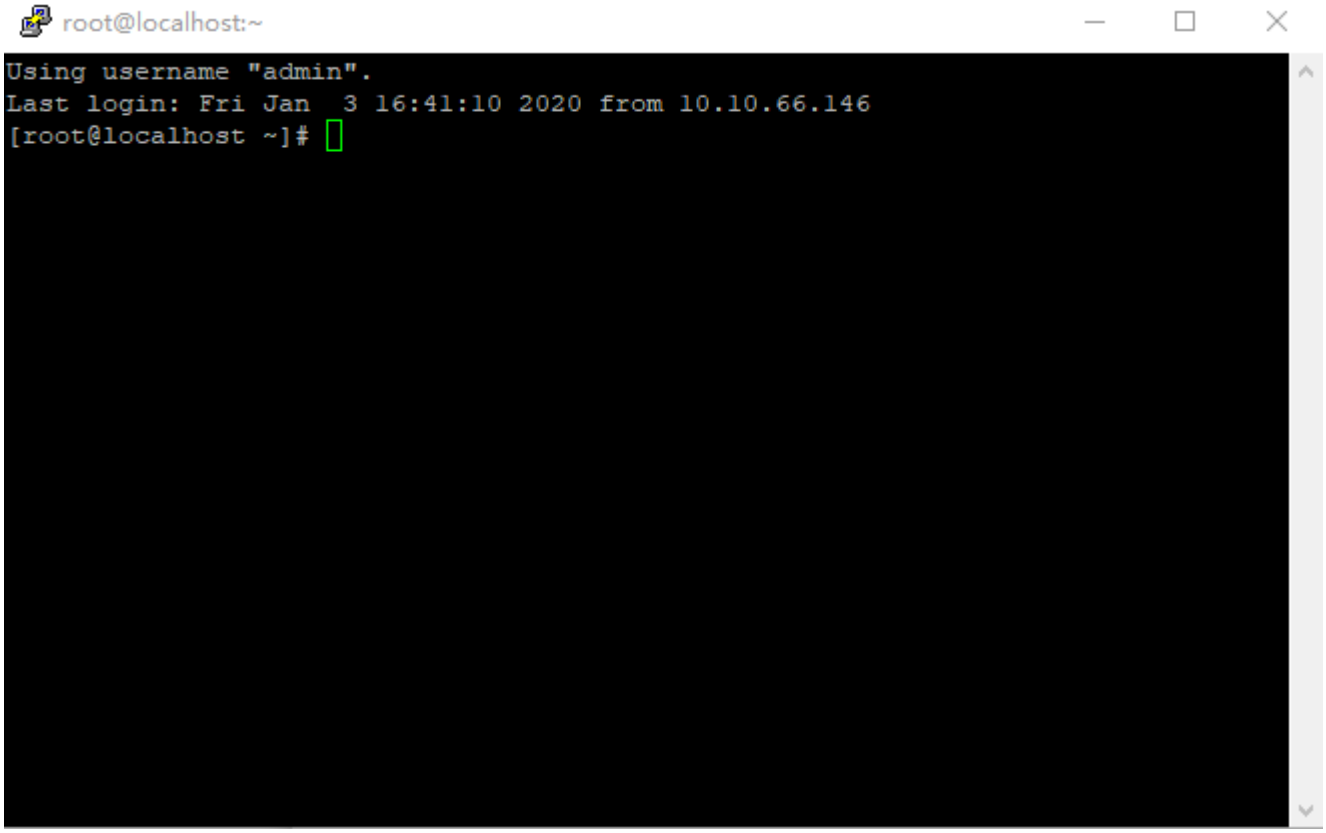
通过SSH客户端访问新建的Linux资产

9. 选择**工作台** > **访问资产**，在左侧的动态视图中找到已添加的Linux资产，单击**访问**按钮。

10.单击**启动**，通过默认参数信息访问目标数据库。



如果配置正确，将通过SSH客户端打开对应的界面，并使用托管的帐号密码完成登录。



举例：H3C Comware资产管理和访问

本节以新增一个H3C Comware资产，并使用Telnet客户端访问该资产为例，详细介绍网络设备资产管理和访问的具体方法。

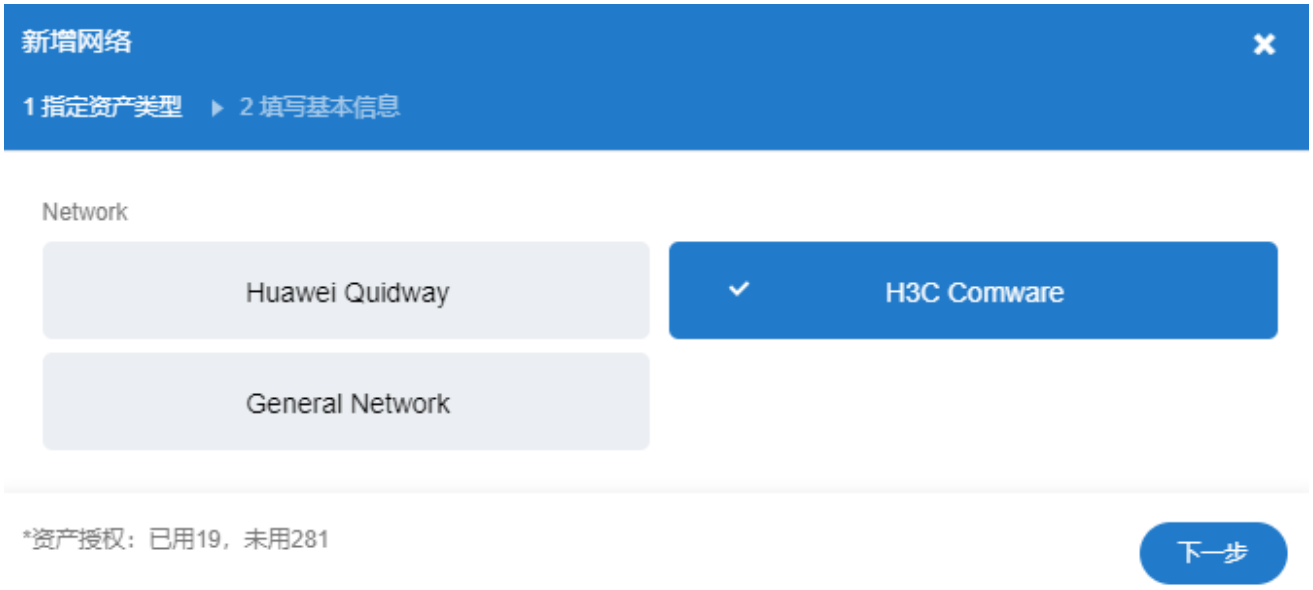
已知数据信息如下表所示：

表 2: H3C Comware资产数据信息

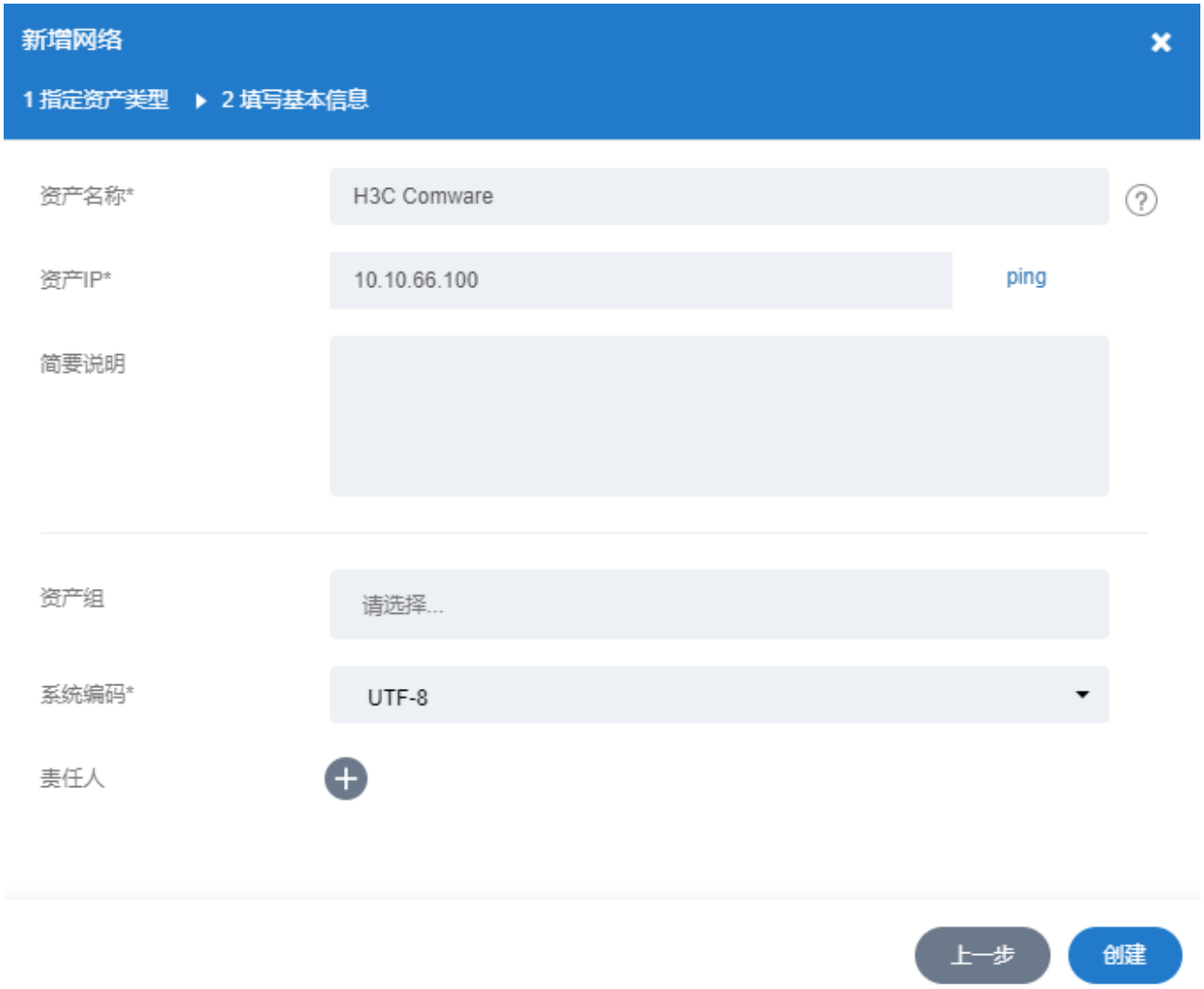
参数	取值	说明
资产名称	H3C Comware	资产的名称。字符串格式，长度范围是1~100个字符。
资产IP	10.10.66.100	目标资产的IP。
系统帐号/密码	admin/password	访问目标资产使用的帐号。

1. 选择**资产** > **资产清单** > **网络**，单击**新建**。

2. 选择**H3C Comware**资产类型，单击**下一步**。



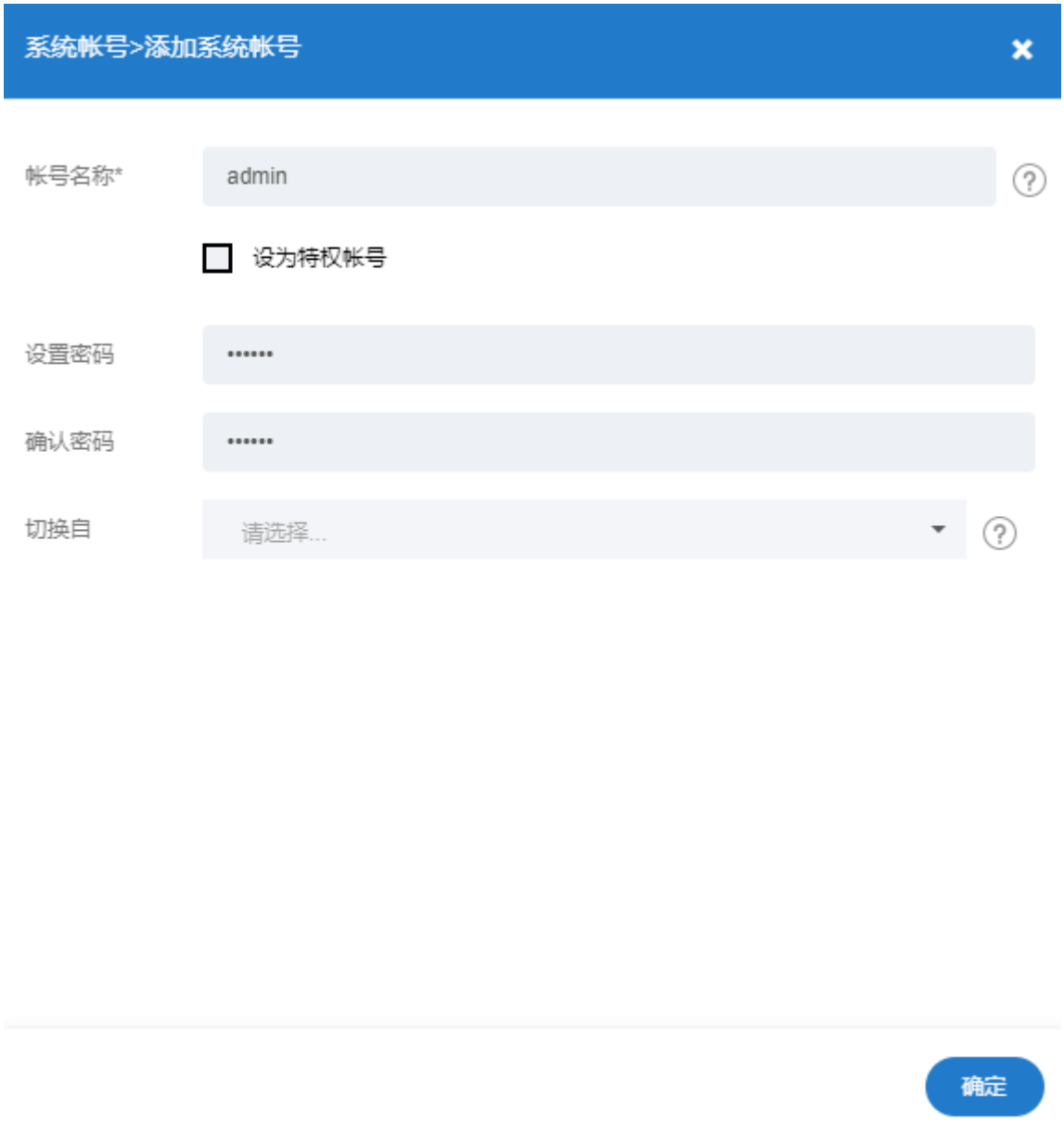
3. 设置各参数信息，完成后单击**创建**。



4. 单击**H3C Comware**对应的**编辑**。

5. 选择**系统帐号**页签，单击**添加帐号**。

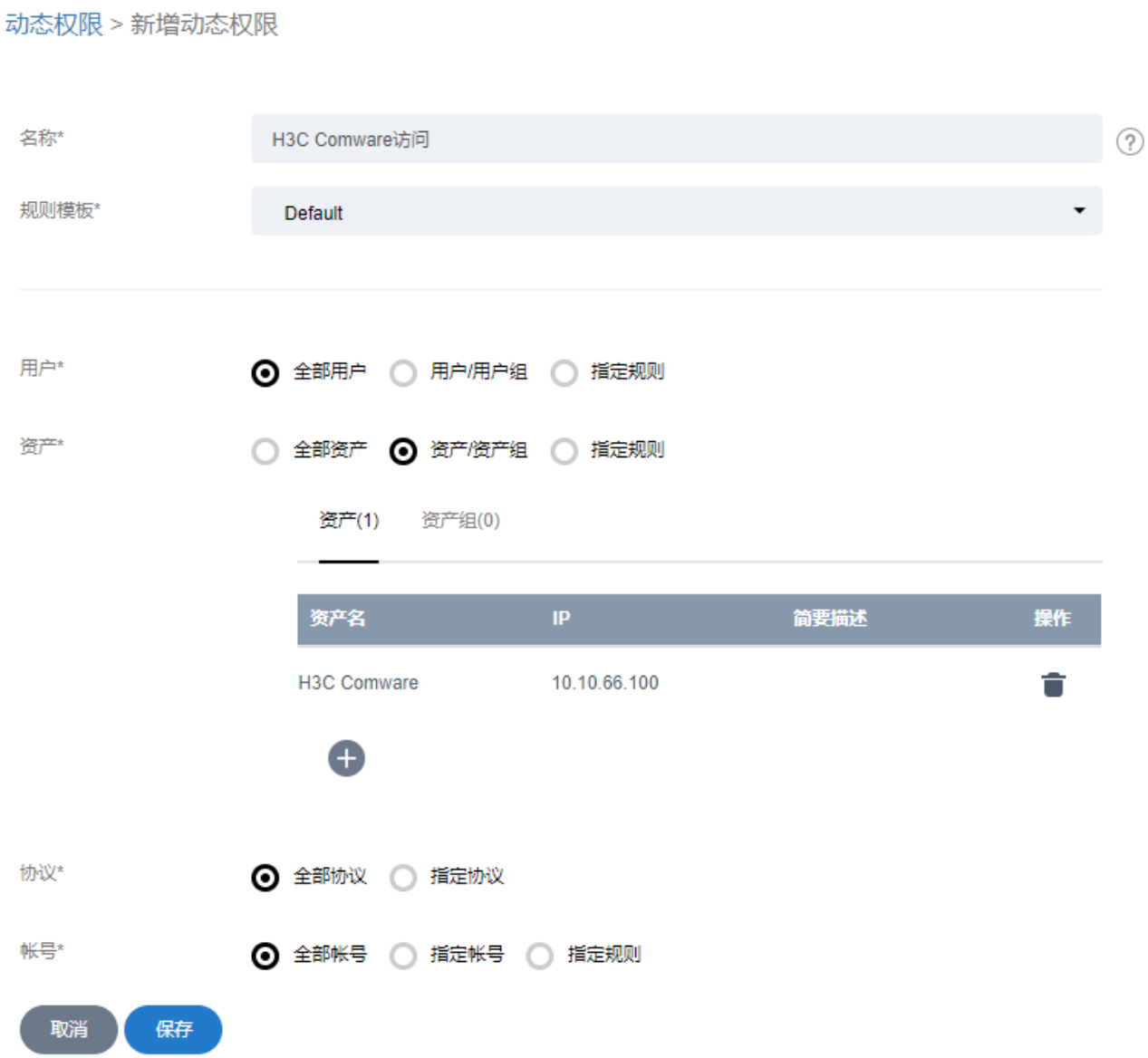
6. 在弹出的对话框中输入帐号对应的密码，完成后单击**确定**，并单击**保存**。



增加访问权限

7. 选择权限**权限 > 权限配置 > 动态权限**，单击**新增动态权限**。

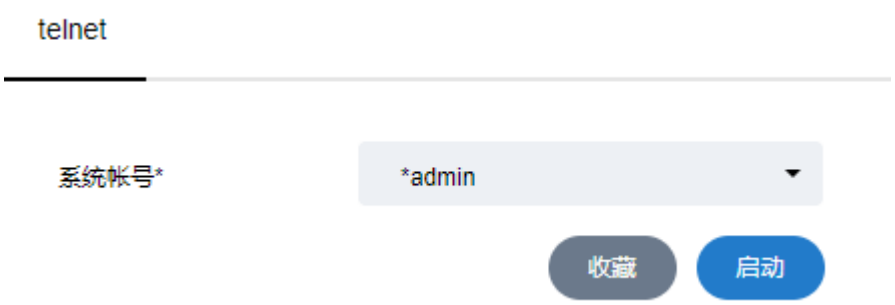
8. 设置动态权限的参数信息，完成后单击**保存**。



通过Telnet客户端访问建立的H3C Comware资产

9. 选择**工作台** > **访问资产**，在左侧的动态视图中找到已添加的H3C Comware资产，单击**访问**按钮。

10.选择已添加的系统帐号，并单击**启动**。



如果配置正确，将通过Telnet客户端打开对应的界面，并使用托管的帐号密码完成登录。

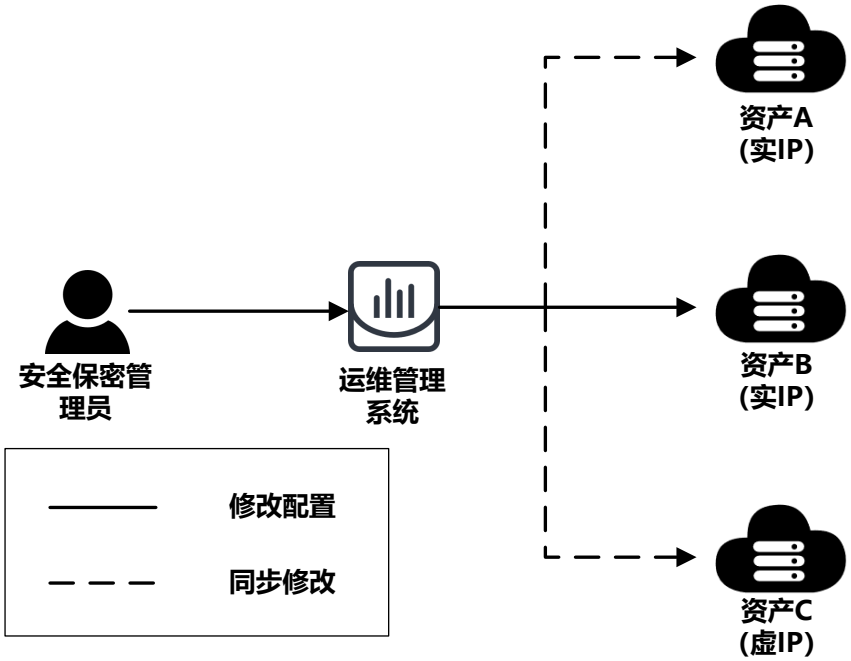
举例：等价资产

对等价资产中任意一个资产进行A2000-E 运维管理系统上的配置修改，部分配置会自动同步到等价资产中的其他成员。

等价资产一般用于以下两种情况。

- 资产为HA部署时，将HA中的各节点设置为等价资产。
- 资产有多个IP，例如有实IP和虚IP，IPv4和IPv6时，将该资产的不同IP分别配置为一个资产，并设置为等价资产。

例如，资产A和资产B组成HA，在A2000-E 运维管理系统上添加资产A和资产B的同时，也将HA的虚IP设置为资产C。这种情况下可以将这3个资产设置为等价资产。当安全保密管理员修改资产B的配置时，也会将修改的配置同步到资产A和资产C。



A2000-E 运维管理系统仅会对资产的部分配置进行同步，不同资产类型被同步的配置不相同，具体请参见《A2000-E 运维管理系统Web配置指导》的配置等价资产章节。对于主机/网络资产，仅同步**访问协议**、**系统帐号**和**责任人**。

本节以将两个部署成HA的Linux主机资产及其虚IP添加为3个不同的资产，并设置为等价资产为例，介绍等价资产的设置，并在修改其中一个资产的配置后进行验证。已知资产数据如下表所示，本例中暂不添加帐号。

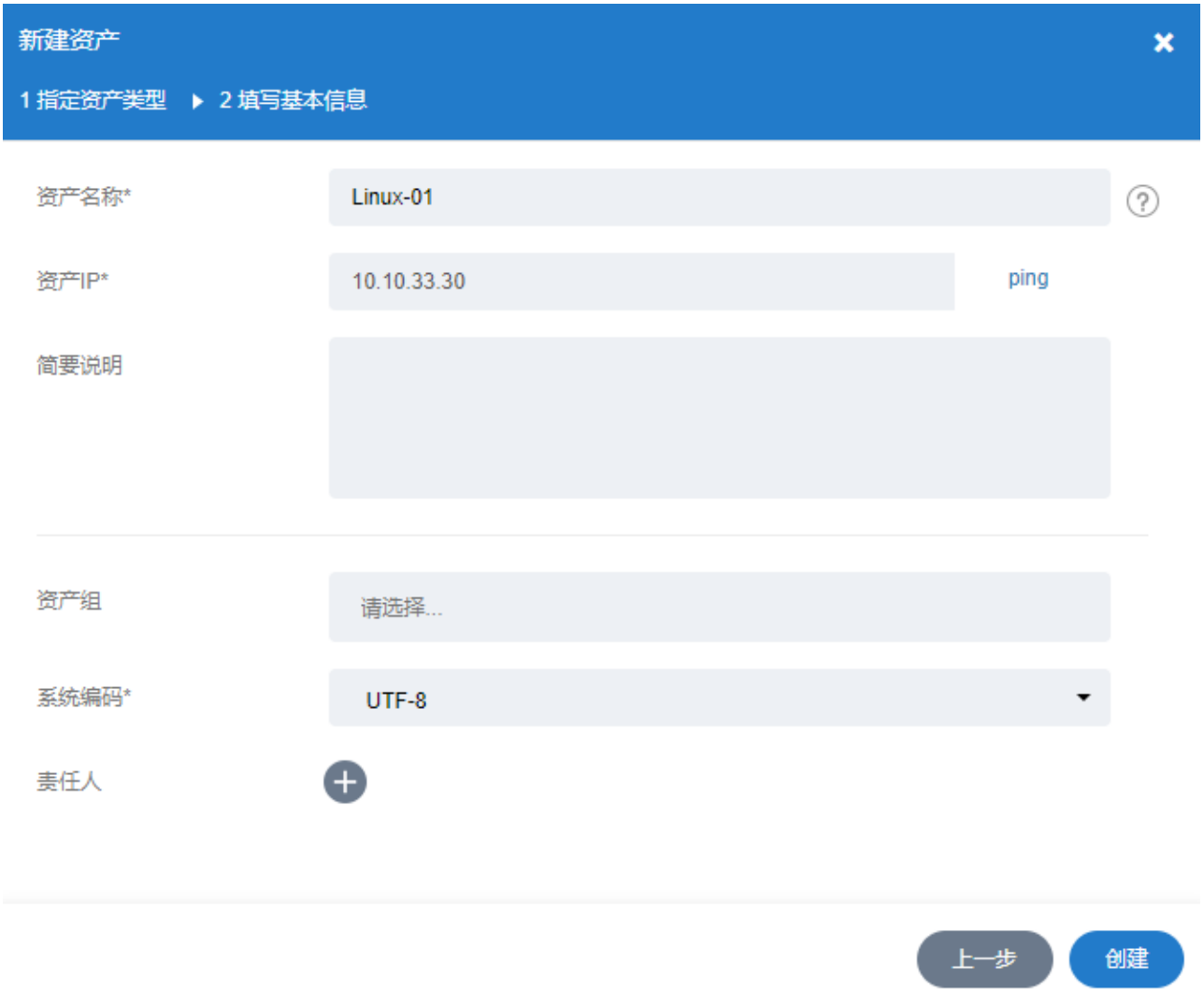
名称	**IP**	**说明**
Linux-01	10.10.33.30	IP配置为第一台主机的实IP。
Linux-02	10.10.33.130	IP配置为第二台主机的实IP。
VIP	10.10.33.100	IP配置为HA的虚IP。

1. 新建资产。

a) 选择**资产** > **资产清单** > **主机**。

b) 单击**新建**，选择**Linux**，单击**下一步**。

c) 设置资产Linux-01的各参数，完成后单击**创建**。

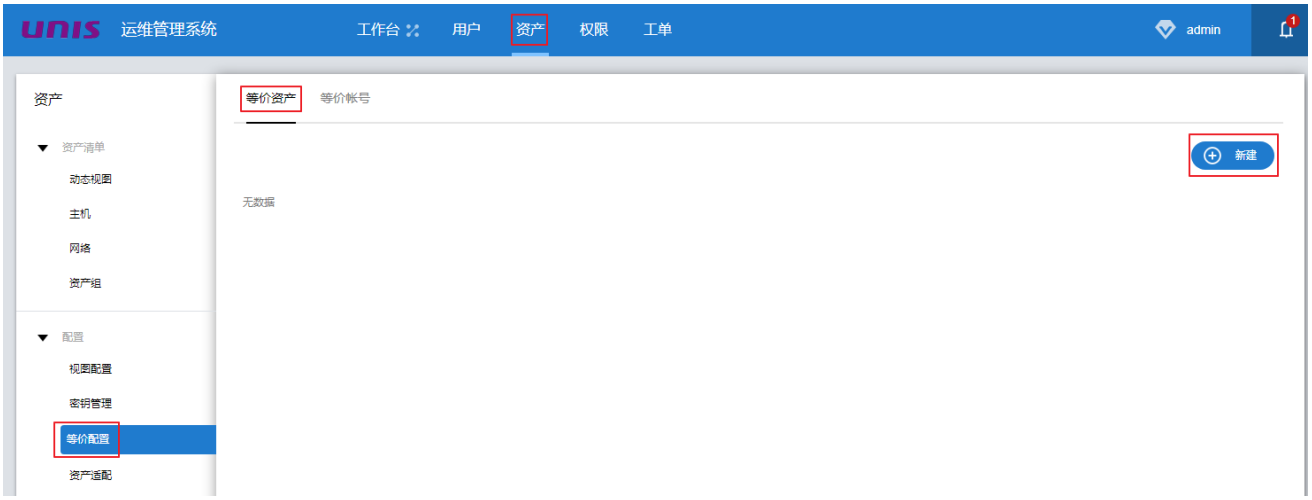


d) 参照以上步骤同样完成Linux-02和VIP资产的创建。

2. 检查等价资产的属性是否满足等价资产的组成条件。

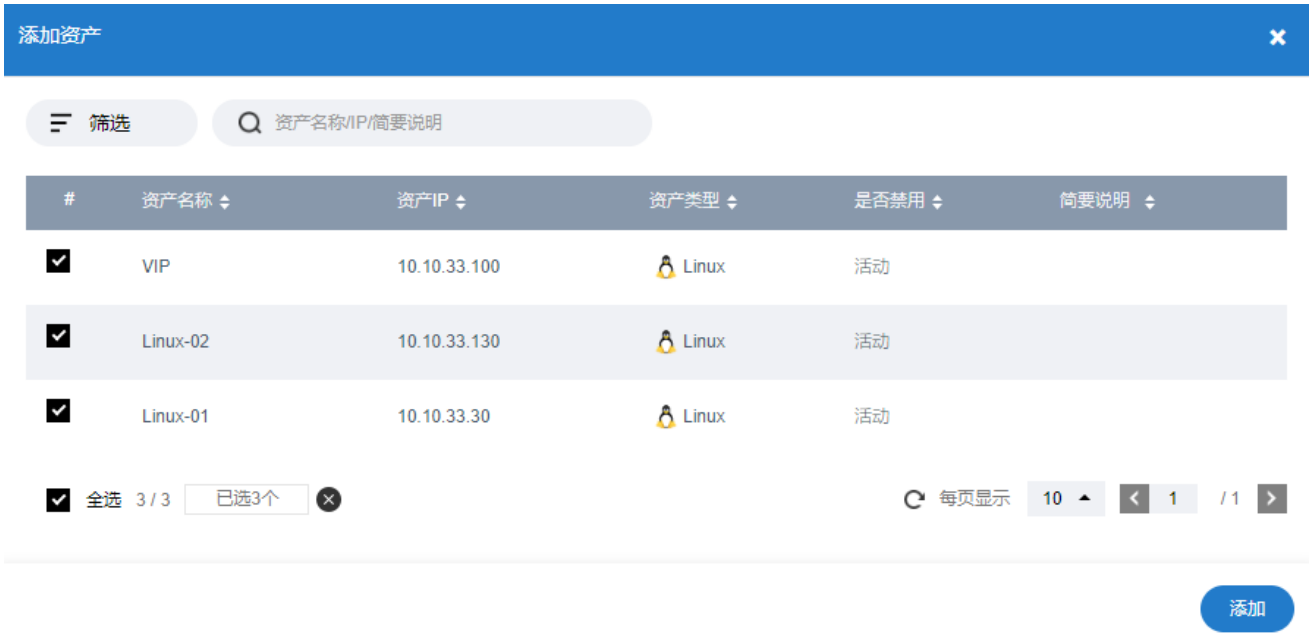
> **说明:** 设置为等价资产的各个资产，其资产属性必须一致，A2000-E 运维管理系统会对其组成条件进行检查，具体请参见《A2000-E 运维管理系统Web配置指导》的配置等价资产章节。对于主机/网络资产，仅检查**资产类型**是否一致，相同访问协议的**端口和状态**是否一致、相同帐号的**密码和特权属性**是否一致。

3. 选择**资产** > **配置** > **等价配置** > **等价资产**，并单击**新建**。

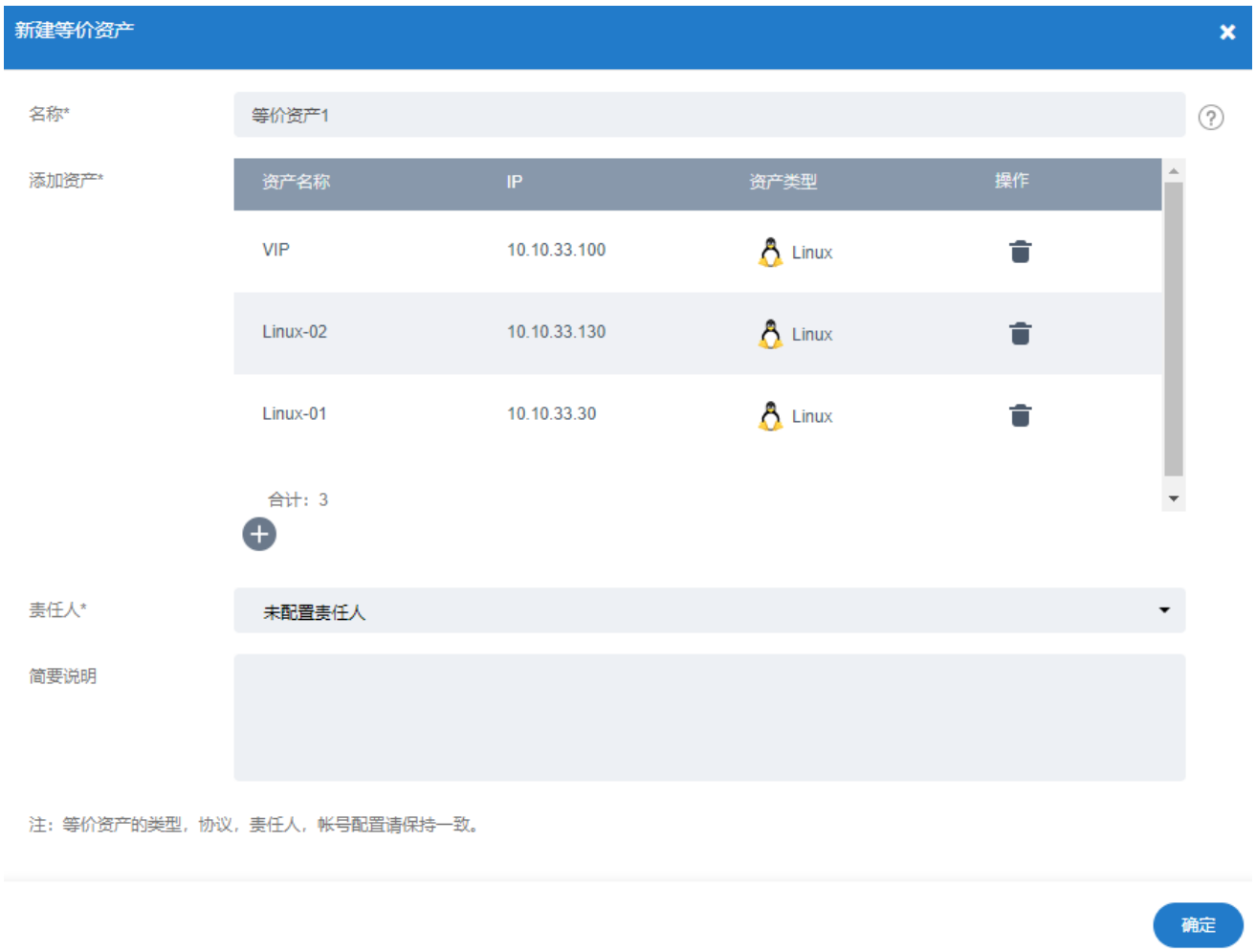


4. 输入等价资产的**名称**，并单击**添加资产**后的，添加等价资产。

5. 勾选待设置为等价资产的资产，并单击**添加**。



6. 选择**责任人**，并单击**确定**。

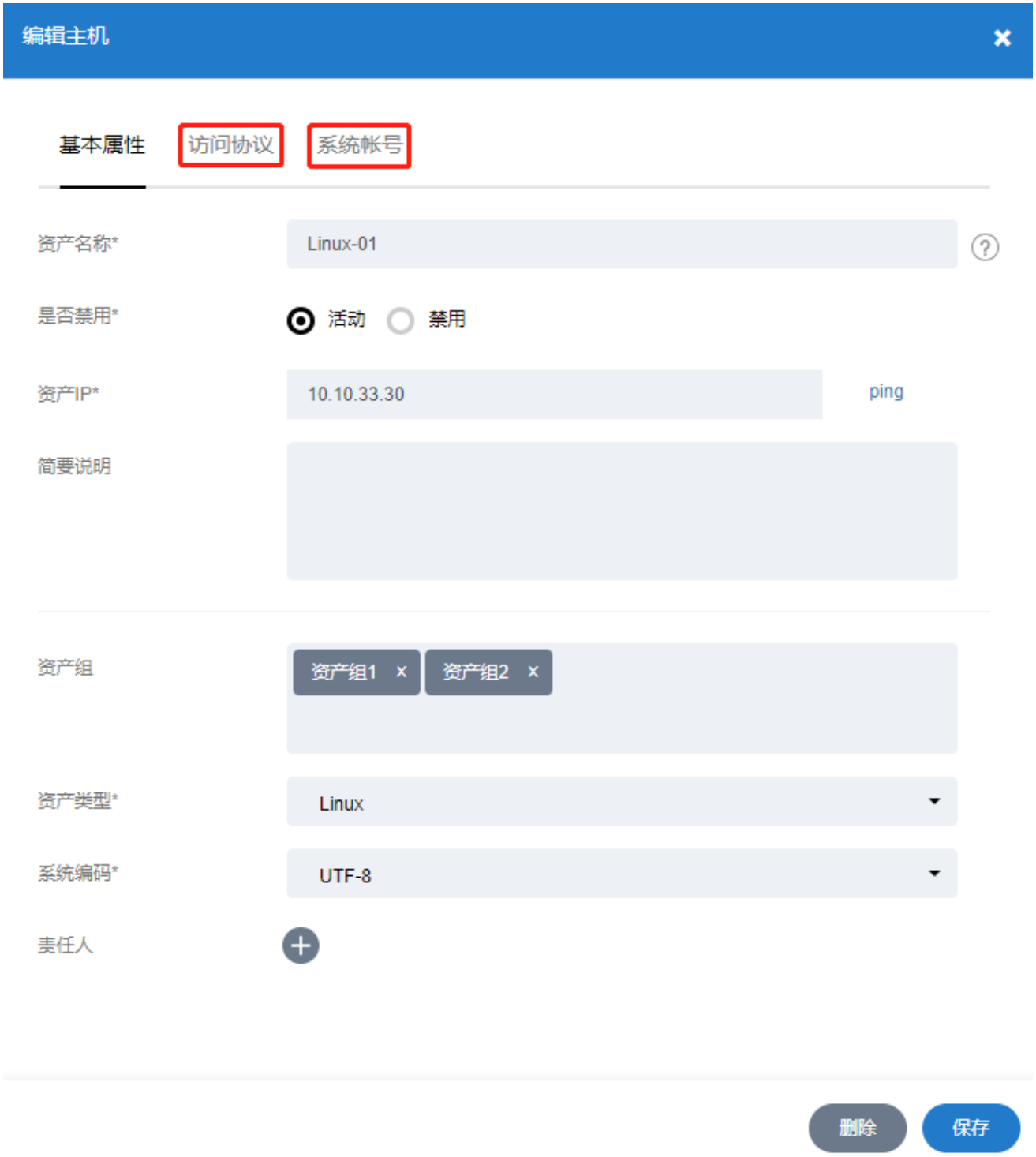


说明: 等价资产的责任人必须一致，**责任人**列表中会列出各个资产之前配置的责任人，从中选择一个作为等价资产的责任人，也可以都设置为**未配置责任人**。

说明: 单击**确定**后将检查是否满足组成条件，如不满足则添加等价资产失败，请重新检查2。

完成等价资产的配置之后，对其中一个资产修改特定的配置，将自动同步到其他资产。用户可以进行以下验证：

1. 选择**资产** > **主机**菜单。
2. 编辑其中一个资产，如Linux-01，修改**责任人**，并修改**访问协议**和**系统帐号**，新增或删除一个协议或帐号。



3. 编辑等价资产中的其他资产，查看相应的属性是否发生变化。本例中修改责任人后，其他资产的责任人也被改变，说明等价资产的配置已生效：

#	资产名称	资产IP	资产类型	是否禁用	资产组	简要说明	责任人	操作
☐	Linux-01	10.10.33.30	Linux	活动	2		admin(admin)	编辑
☐	VIP	10.10.33.100	Linux	活动			admin(admin)	编辑
☐	Linux-02	10.10.33.130	Linux	活动			admin(admin)	编辑

权限

3

目录:

举例：动态权限

管理员通过指定动态权限的基础四要素（用户、资产、协议、帐号），可以快速地完成权限配置。

说明: 如果存在多条动态权限，各条权限之间是并集关系。即满足任一条权限，用户即可访问。

现新增一条test动态权限，要求操作员通过普通帐号访问A2000-E 运维管理系统中指定的Linux主机资产时，只允许从目标资产下载文件。已知参数信息如下表所示。

表 3: 动态权限参数信息

参数	取值	说明
名称	test	动态权限的名称。字符串格式，长度范围是1~30个字符。
规则模板	test规则模板	动态权限引用的规则模板。
用户	指定规则：角色=操作员	设置能够访问资产的用户。
资产	Linux-01	设置待访问的目标资产。
协议	全部协议	访问目标资产使用的协议。
帐号	指定规则：帐号类型=特权帐号	访问目标资产使用的帐号。

表 4: 规则模板参数信息

参数	取值	说明
模板名称	test规则模板	定义该规则模板名称。
控制策略	允许访问	选择该条策略禁止或允许访问。
文件传输权限	下载	仅能通过Web页面云盘模式和SFTP模式从目标资产上下载文件。
下载单文件限制	10240	通过Web页面云盘模式进行传输，当文件超出该限制，无法上传、下载。 通过SFTP模式，当文件超出该限制，无法下载，但可以上传，只上传单文件限制部分的大小。

新增规则模板

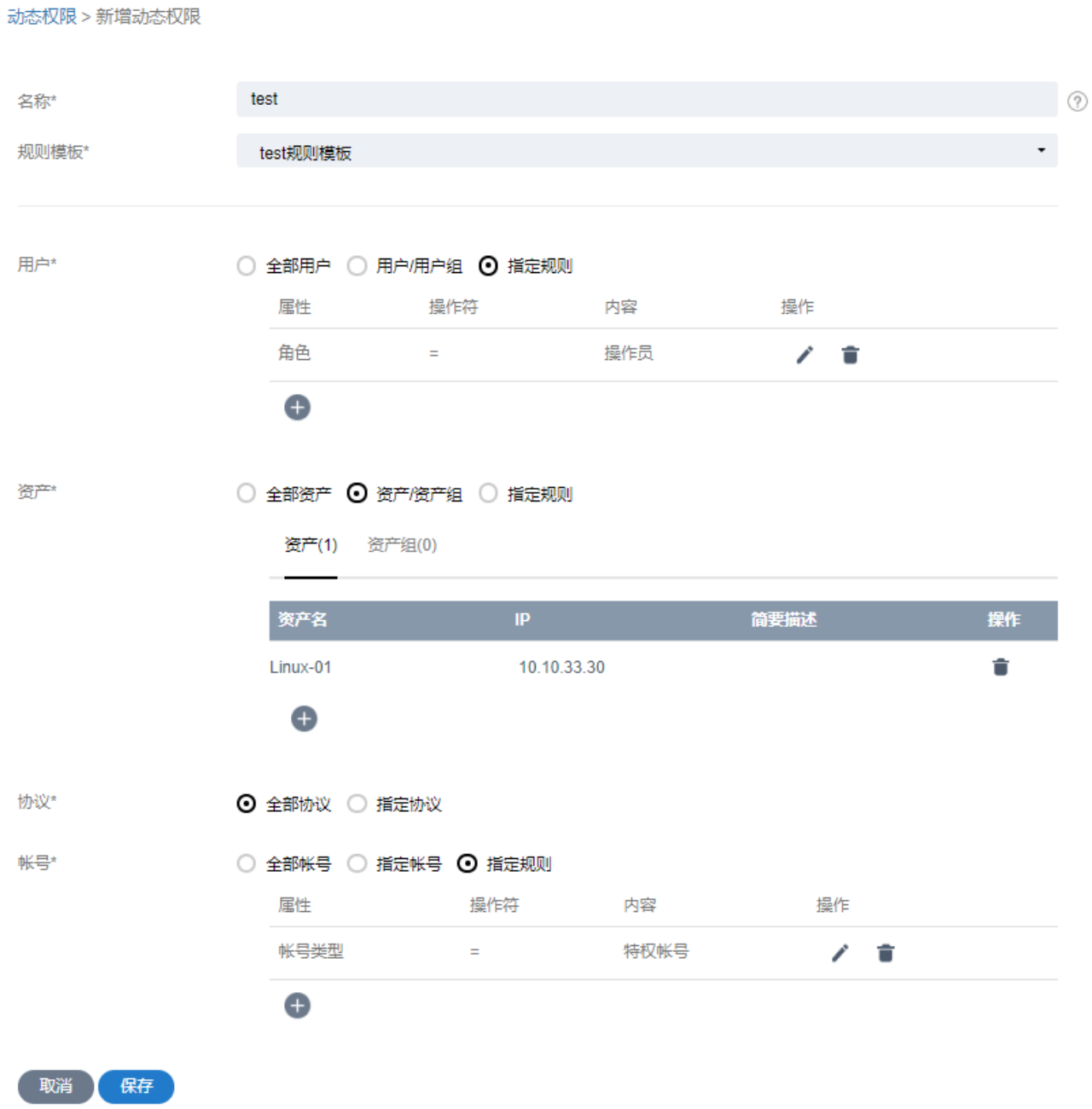
1. 选择**权限 > 权限配置 > 规则模板**，单击**新增规则模板**。

2. 在弹出的对话框中设置各参数信息，完成单击**保存**。

新增动态权限

3. 选择**权限 > 权限配置 > 动态权限**。

4. 单击**新增动态权限**，设置各参数。



说明: 指定规则可以让管理员针对各种属性做出灵活地匹配。针对用户、资产或帐号，管理员可以指定多条规则，必须满足指定的所有规则，才能够匹配该条权限。

5. 单击**保存**，完成动态权限的创建。

举例：变更单

变更单是一个Excel表格，在上面可以填写名称、申请人、到期时间、使用人、使用资产、访问帐号、协议等信息。将填写好的变更单上传到A2000-E 运维管理系统形成访问权限。

现要求admin替opt01申请一个在规定时间内使用Linux-01主机资产的变更单，已知数据如下表所示。

参数	取值	说明
申请单名称	变更单申请	变更申请单的名称。字符串格式，长度范围是1~128个字符。
申请人帐号	admin	申请人的帐号，该帐号必须在A2000-E 运维管理系统上存在且处于活动状态。
到期时间	2020/06/14	申请单中权限到期日期和时间。
申请原因	日常巡检	变更单申请原因。
权限	使用人：opt01 资产：10.10.16.21 帐号：root 协议： ssh、xdmcp	变更单申请的权限清单。一个变更单中可以有多条权限，一条权限对应一行。每条权限包含以下字段： • 使用人：使用人的帐号，该帐号必须在A2000-E 运维管理系统上存在且状态为活动。 • 资产：要访问的资产名称或IP。如果输入的IP地址被多个资产共用，那么权限会关联共用IP的全部资产。 • 帐号：使用资产的哪个帐号访问。 • 协议：取值包括ssh、telnet、vnc、xfwd、xdmcp，不填写是表示全部协议。

1. 选择**权限** > **权限配置** > **变更单**，单击**下载模板**，将模板文件下载到本地PC。

2. 编辑模板内容。

	A	B	C	D
1	申请单名称*	变更单申请		
2	申请人帐号*	admin		
3	到期时间(yyyy/MM/dd)*	2020/1/5		
4	申请原因（用途）			
5	日常巡检			
6	权限(多行记录使用换行分隔，可选协议：ssh，telnet，vnc，xfwd，xdmcp，不填默认全部)*			
7	使用人	资产	帐号	协议
8	opt01	10.10.16.21	root	ssh xdmcp

3. 单击**上传变更单**，上传配置好的变更单。

说明：成功导入变更单后，变更单中的权限会立即生效，直到到期。

单击变更单对应的**详情**，可以查看变更单的详细信息。

举例：申请权限工单

通过工单来申请资产的访问权限。

新建一条申请资产工单，要求操作员opt01通过工单为自己申请Linux-01主机资产的root帐号访问权限。已知参数信息如下表所示。

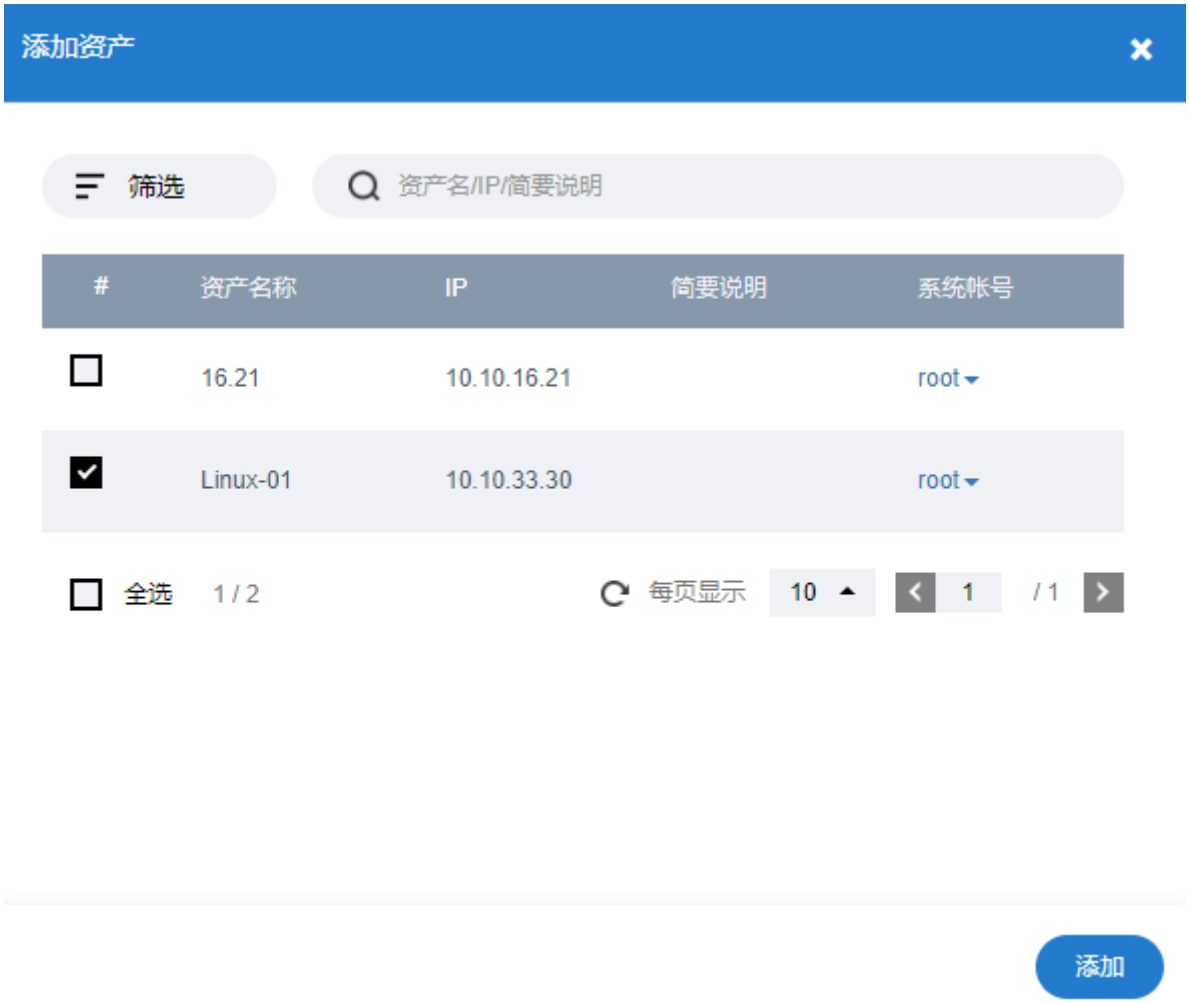
参数	取值	说明
申请人	opt01	申请权限工单的用户。
工单标题	opt01申请Linux-01主机资产	工单的标题。字符串格式，长度范围是1~30个字符。
操作类型	日常维护	用户要申请的操作类型，取值包括**日常维护**和**定期巡检**。
申请理由	Linux设备日常维护	工单的申请理由。字符串格式，长度范围是1~512个字符。
开始时间/结束时间	• 开始时间：2020/01/06 14:00 • 结束时间：2020/01/07 14:00	权限生效的开始时间和结束时间。 开始时间和结束时间使用的是A2000-E 运维管理系统的系统时间，而非本地PC的时间。
资产	10.10.33.30	待添加权限的资产。
协议	SSH、Telnet和XDMCP	使用人允许访问资产使用的协议。
放行命令	• mkdir.* • rm -rf.*	放行命令可以直接填写完整的命令，也可以填写命令的正则表达式，最多512个字符。
使用人	opt01	工单申请资产的实际使用用户。

申请工单

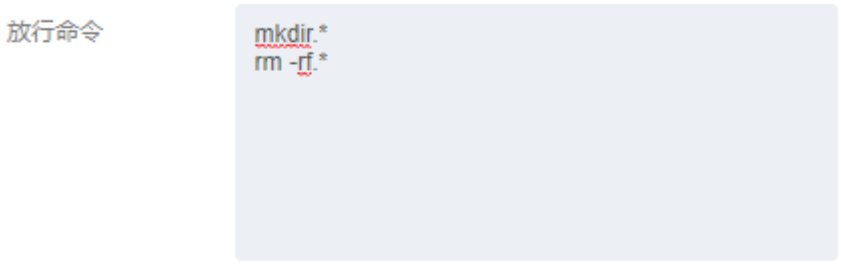
1. 操作员opt01登录A2000-E 运维管理系统Web界面后，选择**工单** > **工单管理** > **新建工单**，单击**申请资产**对应的 。

2. 设置各参数信息。

3. 添加**资产**。单击**资产**对应的，在弹出的对话框中勾选要添加权限的资产，并在**系统帐号**中选择访问帐号，单击**添加**。

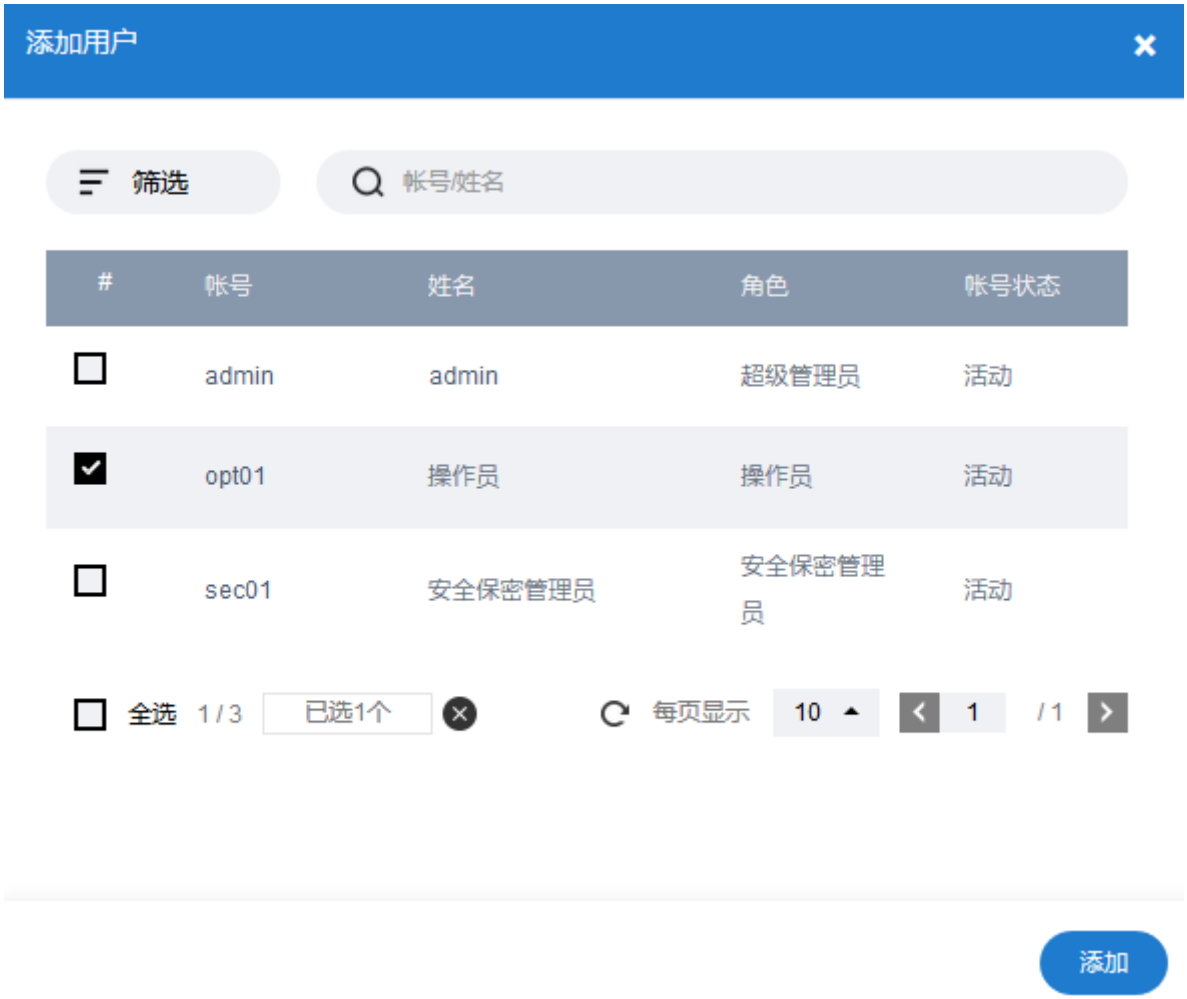


4. 配置访问协议。选择**指定协议**，并勾选**ssh**、**telnet**和**xdmcp**协议。
5. 如果管理员配置了高危命令，工单申请人可以通过设置放行命令，允许工单申请资产的使用人执行某些命令。填写**放行命令**，多条命令之间用回车分隔。



说明: 此处放行的命令相当于在命令模板中配置对应的命令为**允许**，且将拥有比高危命令配置更高的优先级。只要用户执行的命令能够匹配上此处的放行命令，则在高危命令配置中的拒绝、需复核、终止会话将不再生效，命令将可以直接执行。

6. 单击使用人对应的，选中要添加权限的用户，单击**添加**。



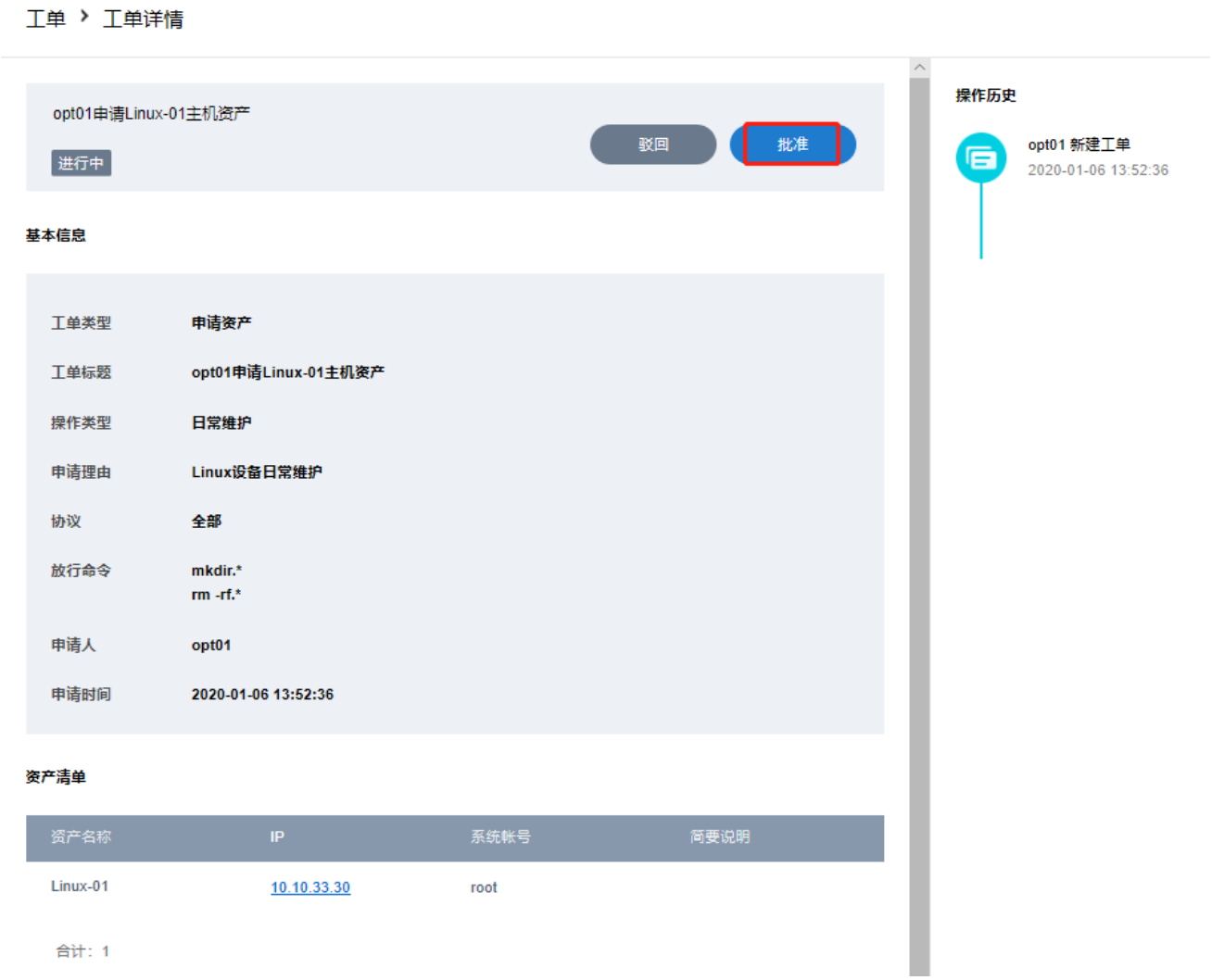
7. 单击**提交**。

   申请人提交工单后，审批人会收到通知消息。待审批人批准后，A2000-E 运维管理系统将用户和所选资产、帐号进行关联。

审批工单

8. 安全保密管理员登录A2000-E 运维管理系统Web界面后，单击右上角的，查看待审批的工单，单击**查看详情**。

9. 在弹出的页面中查看工单详情，确认无误后单击**批准**。



安全保密管理员批准工单后，opt01会收到通知消息。

单击**查看详情**，可以查看审批后的工单的详细信息。

opt01申请Linux-01主机资产

进行中

基本信息

工单类型	**申请资产**
工单标题	**opt01申请Linux-01主机资产**
操作类型	**日常维护**
申请理由	**Linux设备日常维护**
协议	**全部**
放行命令	**mkdir.*** **rm -rf.***
申请人	**opt01**
申请时间	**2020-01-06 13:52:36**

资产清单

资产名称	IP	系统帐号	简要说明
Linux-01	10.10.33.30	root	

合计：1

使用人	opt01
使用时间	2020-01-06 14:00:00 2020-01-07 14:00:00

操作历史

opt01 新建工单
2020-01-06 13:52:36

sec01 审核工单 批准申请
2020-01-06 13:54:41

改密

4

目录:

举例：密码备份（邮件）

目标设备的帐号和密码在A2000-E 运维管理系统上托管后，为了保证密码的安全性，请定期备份密码。

本节以通过ZIP加密方式对密码备份信息进行加密为例，详细介绍通过邮件实现密码备份的配置方式。已知数据如下表所示。

表 5: 邮件服务器参数信息

参数	取值	说明
邮件服务器	10.1.2.20	邮件服务器地址，可填写IP地址或者域名，必填，默认值127.0.0.1，请修改为您的邮件服务器地址。 **说明:** 如果使用非缺省端口（25或SSL465），请在地址后面加上 “:端口”。
发件人地址	test@example.com	发件人地址，必填，格式需要符合RFC5322中定义的E-mail地址格式。
发件人名称	消息提醒	发件人的显示名称。选填，任意字符，不超过64的字符。
服务器要求身份验证	勾选	SMTP服务器是否要求进行身份验证，默认未勾选。
用户名/密码	test@example.com/ password	• **用户名**，SMTP服务器上的用户名。 • **密码**，SMTP服务器上的密码。 **说明:** 如服务器需要使用授权码，请将**密码**配置为获取的授权码。

表 6: 密码备份参数信息

参数	取值	说明
执行时间	2019-06-14 18:05	密码备份的执行日期和时间。
执行间隔	每3月	密码备份的执行间隔。

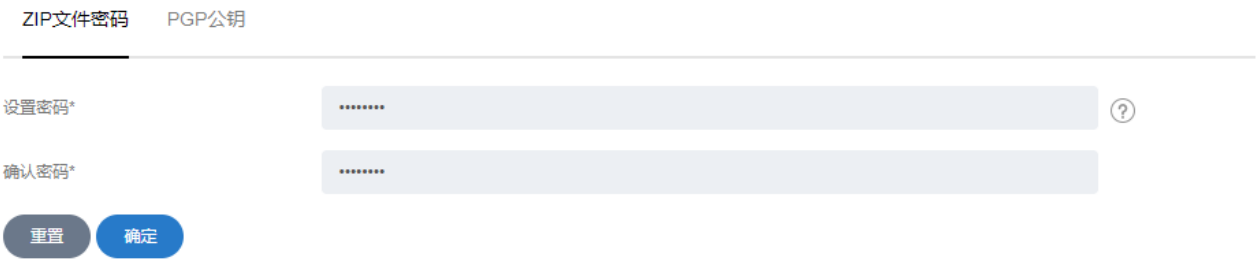
参数	取值	说明
密码分段	否	密码备份时是否分段。 • 如果选择**是**，密码将被分为两段，前、后半段需要分别选择不同的备份方式和通知用户。 • 如果选择**否**，密码被作为一个整体备份。
备份方式	邮件备份	密码备份采取的方式。
通知用户	admin	密码备份时，接收邮件通知的用户。

配置密码备份相关参数

1. 配置信息加密。

   a) 单击右上角的**admin**，选择**帐号设置**，单击**信息加密**，选择**ZIP文件密码**页签。

   b) 设置密码信息，完成后单击**确定**。



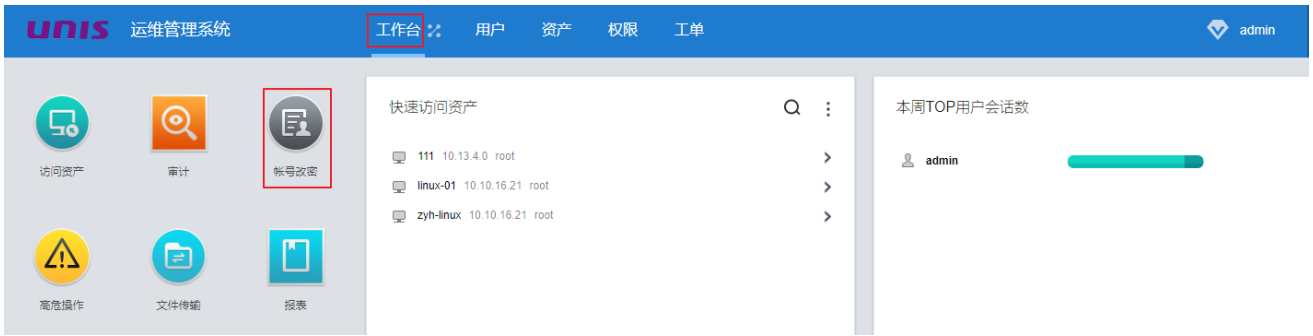
2. 配置邮件服务。

   a) 单击右上角的**admin**，选择**系统设置** > **系统** > **基本设置** > **邮件服务**。

b) 设置邮件服务参数信息，完成后单击**确定**。

配置密码备份

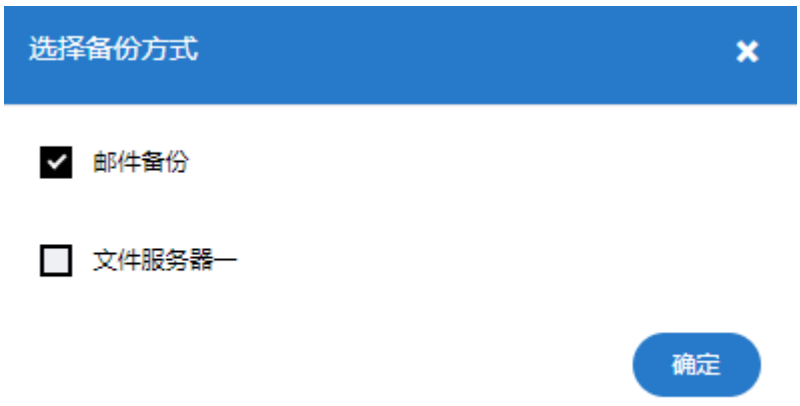
3. 选择**工作台** > **帐号改密**。



4. 选择**帐号维护** > **密码备份**。

5. 设置各参数信息。

6. 单击**选择备份方式**，在弹出的对话框中勾选**邮件备份**，完成后单击**确定**。



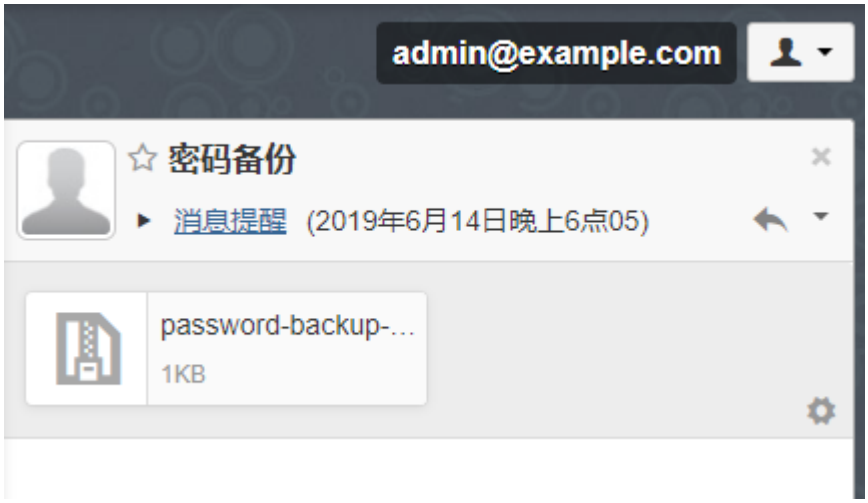
7. 单击**添加通知用户**，在弹出的对话框中勾选需要通知的用户，完成后单击**确定**。

8. 确认设置的信息无误后，单击**确定**。

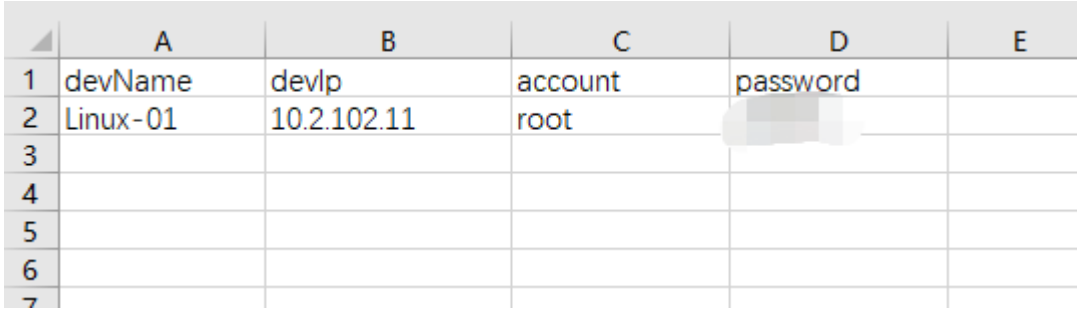
说明: 密码备份执行完成后可以直接单击执行记录对应的**查看**按钮，查看执行结果。

查看密码备份结果：

1. 通知用户收到密码备份邮件。



2. 下载附件文件，利用解压软件打开压缩包。
3. 输入设置的ZIP文件密码，打开压缩包中的Excel文件，即可查看已备份的密码信息。



	A	B	C	D	E
1	devName	devIp	account	password	
2	Linux-01	10.2.102.11	root		
3					
4					
5					
6					

举例：密码备份（文件服务器）

本节以通过ZIP加密方式对密码备份信息进行加密为例，详细介绍通过文件服务器密码备份的配置方式。已知数据如下表所示。

表 7: 文件服务器一参数信息

参数	取值	说明
地址	10.1.2.12	文件服务器的IP地址。
端口	22	文件服务器的端口。 SFTP默认为22 。
用户名/密码	root/password	文件服务器的用户名和密码 。

表 8: 密码备份参数信息

参数	取值	说明
执行时间	2019-06-14 18:30	密码备份的执行日期和时间。
执行间隔	每3月	密码备份的执行间隔。

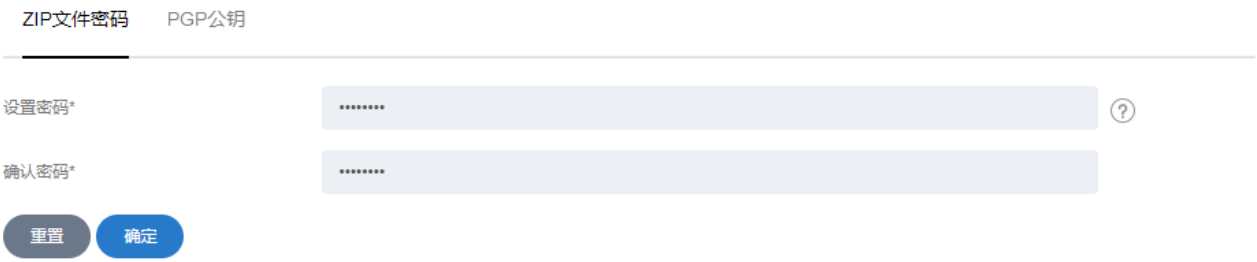
参数	取值	说明
密码分段	否	密码备份时是否分段。 • 如果选择**是**，密码将被分为两段，前、后半段需要分别选择不同的备份方式和通知用户。 • 如果选择**否**，密码被作为一个整体备份。
备份方式	文件服务器一	密码备份采取的方式。
通知用户	admin	密码备份时，接收信息通知的用户。

配置密码备份相关参数

1. 配置信息加密。

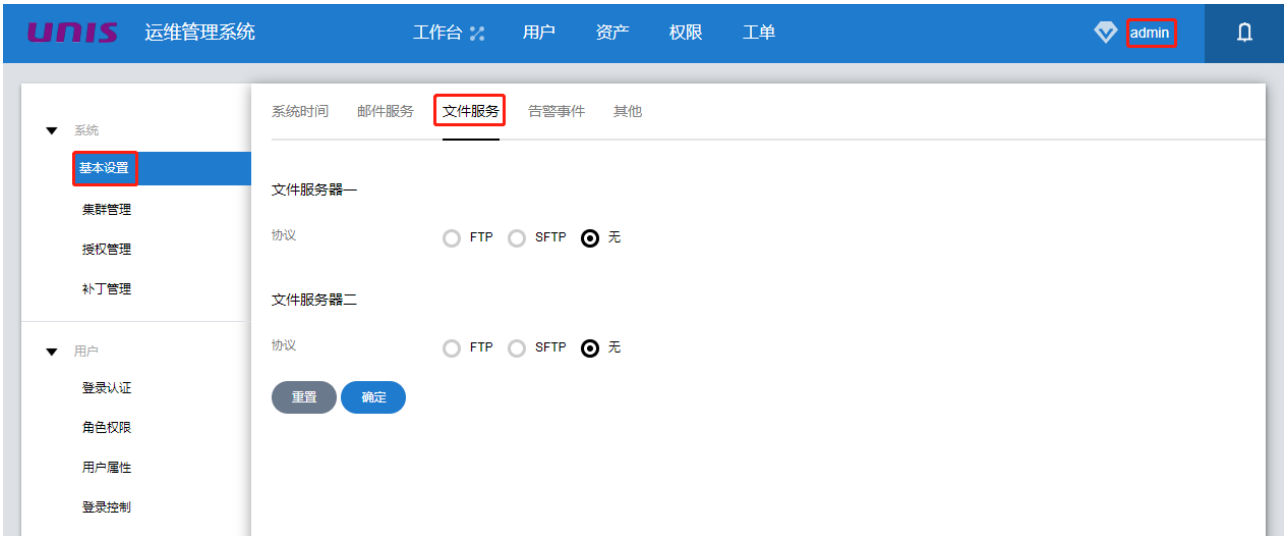
   a) 单击右上角的**admin**，选择**帐号设置**，单击**信息加密**，选择**ZIP文件密码**页签。

   b) 设置密码信息，完成后单击**确定**。

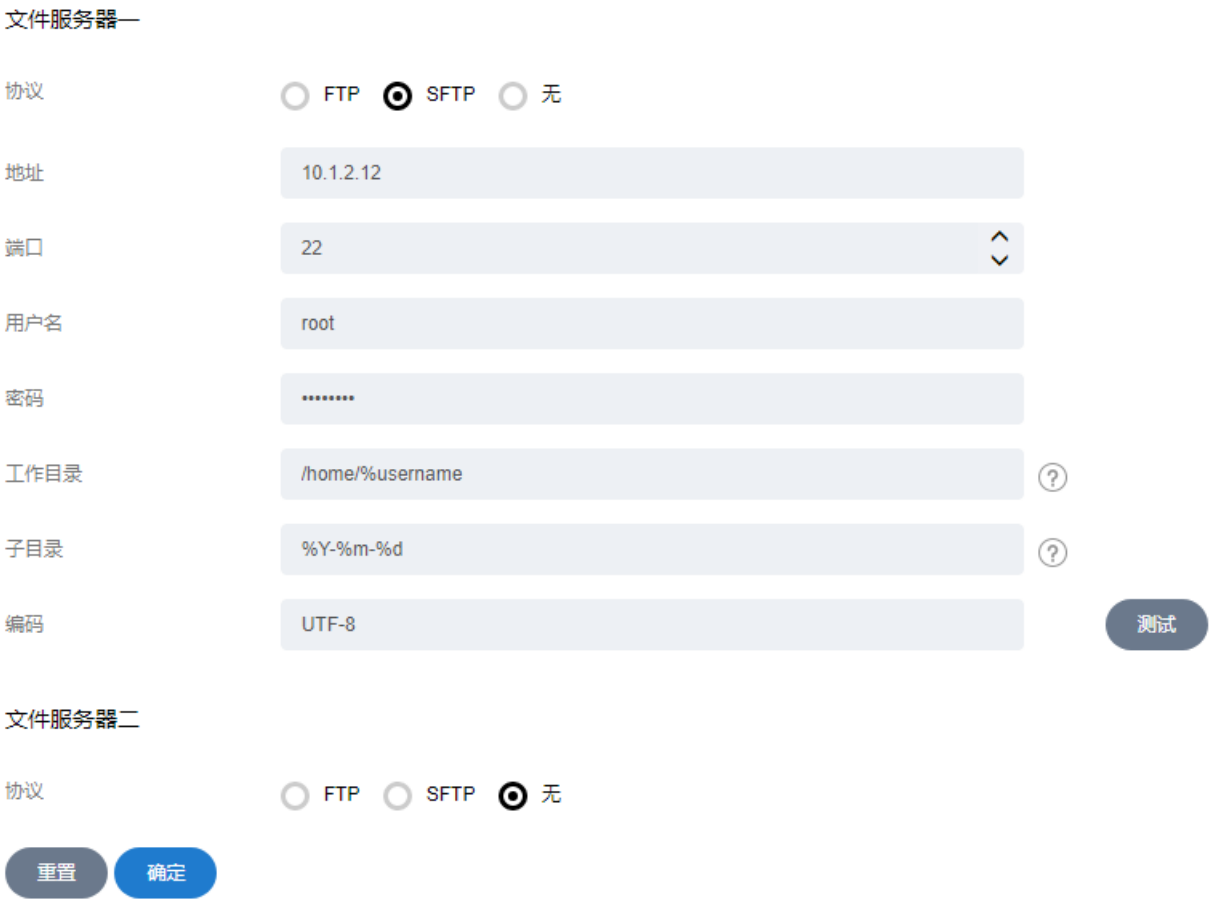


2. 配置文件服务。

   a) 单击右上角的**admin**，选择**系统设置** > **系统** > **基本设置** > **文件服务**。

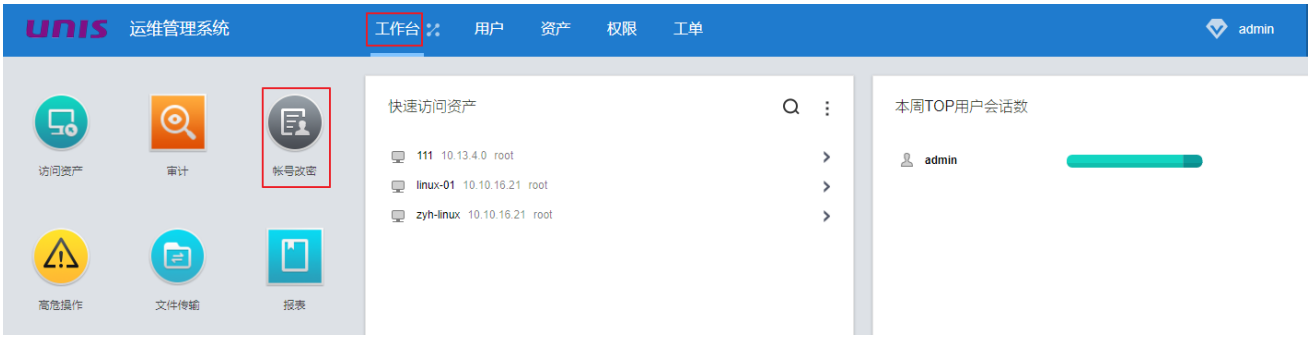


b) 设置文件服务参数信息，完成后单击**确定**。



配置密码备份

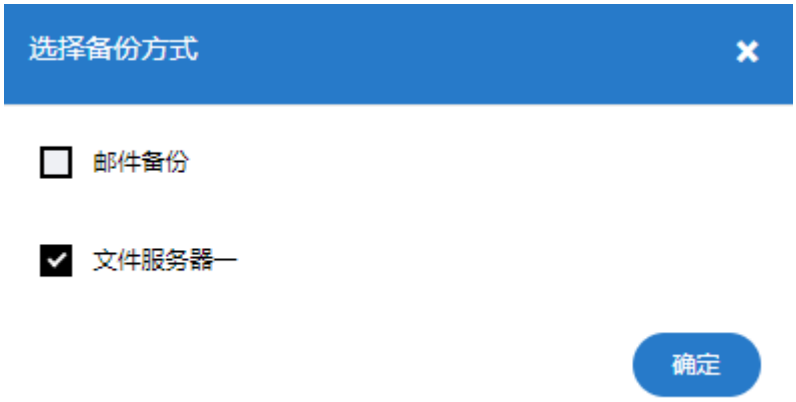
3. 选择**工作台** > **帐号改密**。



4. 选择**帐号维护 > 密码备份**。

5. 设置各参数信息。

6. 单击**选择备份方式**，在弹出的对话框中勾选**文件服务器一**，完成后单击**确定**。



7. 单击**添加通知用户**，在弹出的对话框中勾选需要通知的用户，完成后单击**确定**。

8. 确认设置的信息无误后，单击**确定**。

说明: 密码备份执行完成后可以单击执行记录对应的**查看**按钮，查看执行结果。

查看密码备份：

1. 通过SSH远程登录到文件服务器一，查看密码备份文件。

```
[root@localhost ~]# cd /home/root/2019-6-14
[root@localhost 2019-6-14]# ls
password-backup-20190614-183000-admin.zip
[root@localhost 2019-6-14]#
```

2. 将密码备份文件下载到本地，利用解压软件打开压缩包。
3. 输入设置的ZIP文件密码，打开压缩包中的Excel文件，即可查看已备份的密码信息。

	A	B	C	D	E
1	devName	devIp	account	password	
2	Linux-01	10.2.102.11	root		
3					
4					
5					
6					

举例：Linux系统改密

Linux系统改密需要满足以下条件：

- 帐号已配置密码或密钥。
- A2000-E 运维管理系统上资产的访问协议（SSH或Telnet）配置正确。

现要求通过A2000-E 运维管理系统为Linux系统上的本地用户改密，已知数据如下表所示。

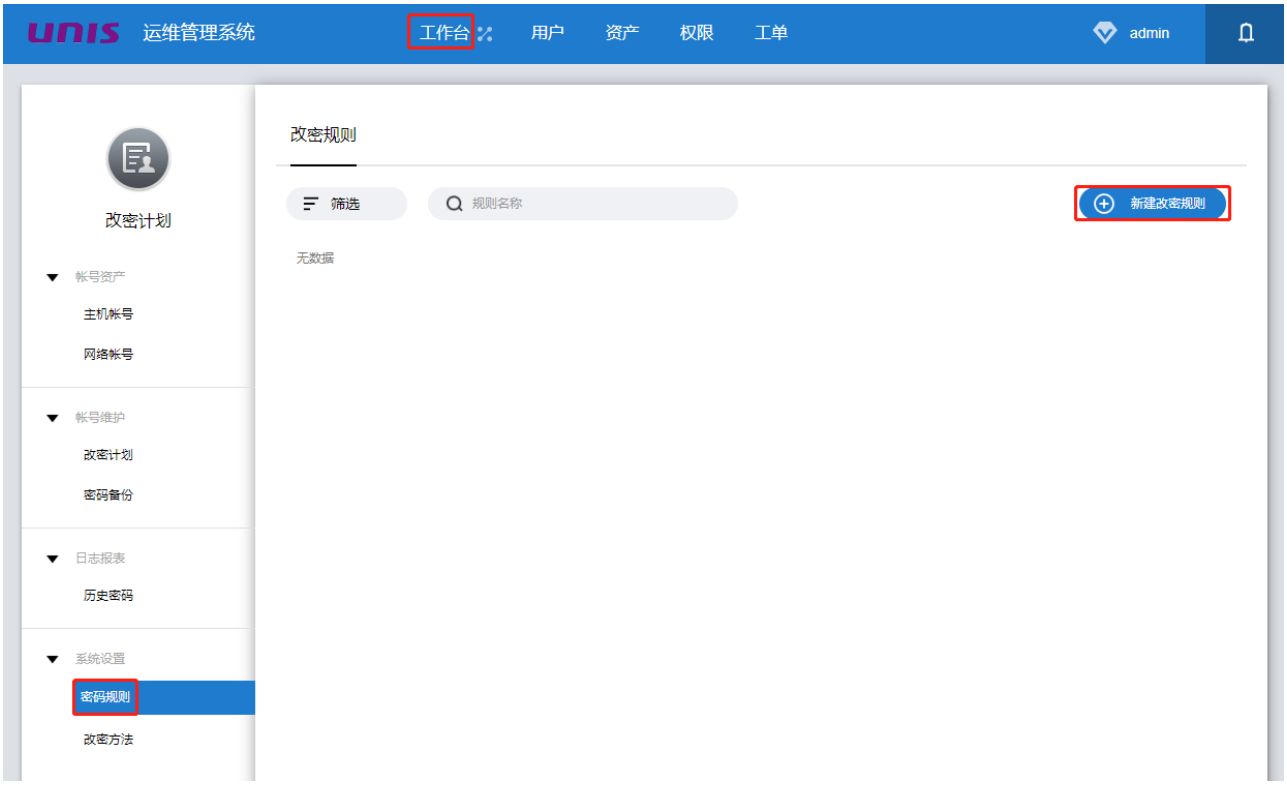
系统	数据	说明
A2000-E 运维管理系统	• 用户帐号：admin • 用户工作邮箱： admin@example.com • 用户ZIP文件密码：12345678	A2000-E 运维管理系统上接收改密通知和密码备份文件的用户，本例中为admin。实际使用中请根据需要配置成其他用户。

Linux	• IP地址：10.2.102.11
	• 特权帐号：
	  • 名称：root
	  • 密码：123456
		无

SFTP服务器	• IP地址：10.2.102.11 • 端口：22 • 用户名：root • 密码：123456	存放密码备份文件的文件服务器。A2000-E 运维管理系统支持将密码备份文件发送到用户的邮箱或者上传到文件服务器，本例中为上传到文件服务器。

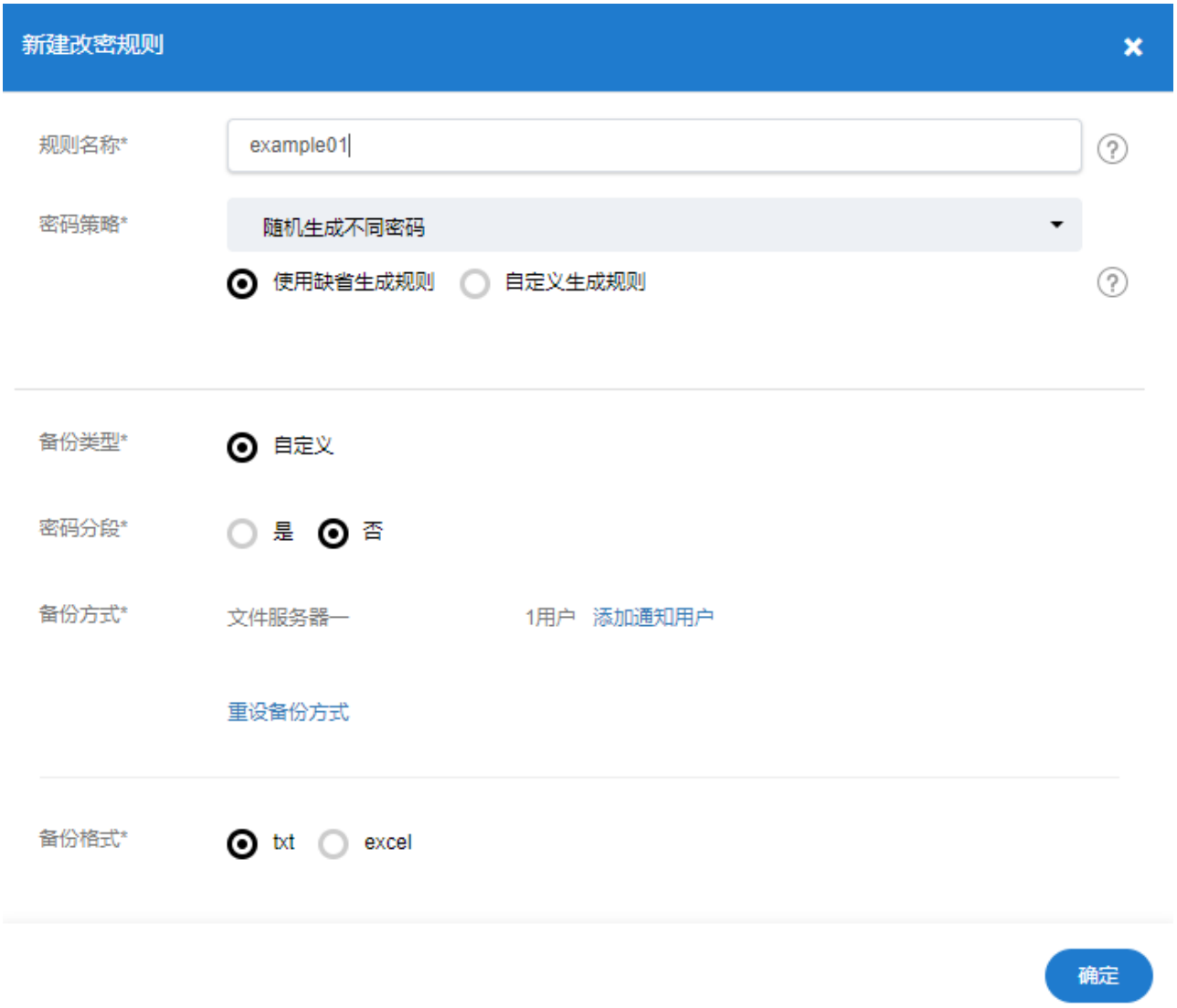
配置密码备份相关参数

1. 配置信息加密与文件服务。
2. 配置改密规则。
   a) 选择**工作台** > **帐号改密** > **系统设置** > **密码规则**。



b) 在**改密规则**中单击**新建改密规则**，设置各参数，完成后单击**确定**。

- 密码策略：生成密码的规则，本例中采取**随机生成不同密码规则**并**使用缺省生成规则**，您可以根据需要选择其他的密码策略。
- 备份方式：在弹出的对话框中勾选**文件服务器一**。
- 添加通知用户：在弹出的对话框中勾选**admin**。

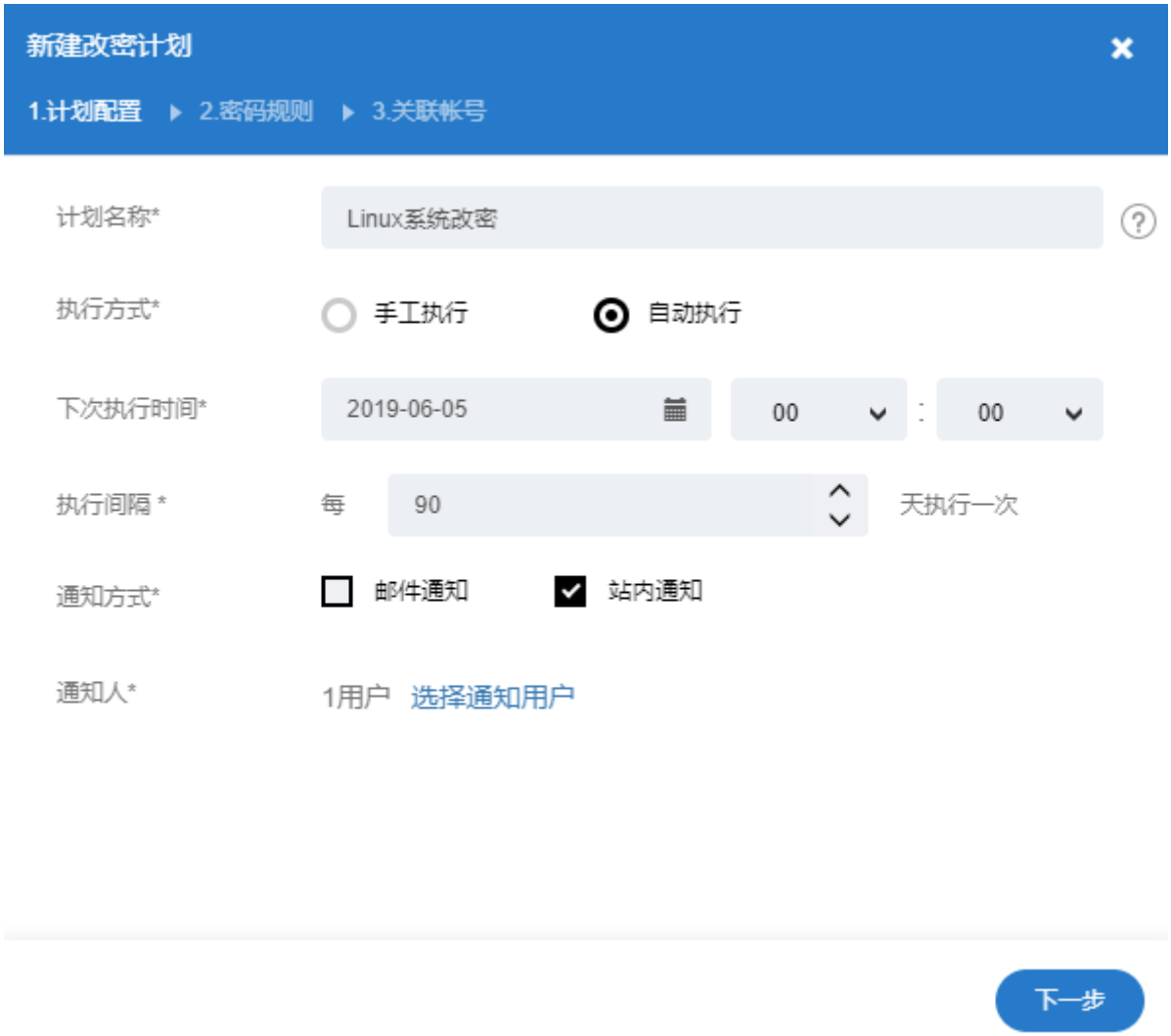


配置改密计划

3. 选择**工作台** > **帐号改密** > **帐号维护** > **改密计划**，单击**新建改密计划**。

4. 设置各参数信息，完成后单击**下一步**。

- 通知方式：选择**站内通知**。
- 通知人：在弹出的对话框中勾选**admin**。



5. 设置密码规则，完成后单击**下一步**。
   - 密码规则：选择**模板选择**。
   - 模板选择：选择**example01**。

6. 设置关联帐号。单击**指定帐号**对应的**已关联**，在弹出的对话框中勾选目标Linux资产，单击**确定**，完成后单击**保存**。

配置完成后，A2000-E 运维管理系统会按照计划中的时间执行改密。也可以单击**Linux系统改密**对应的**立即执行**，当提示**立即执行改密计划时**时单击**确定**，实现手工立即执行改密计划。

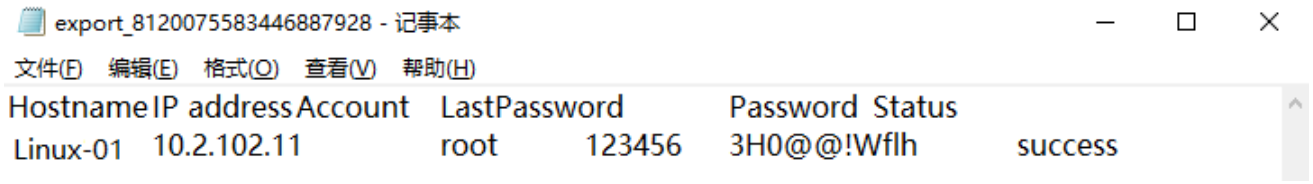
改密操作执行结束后，可以通过以下两种方式查看改密结果。

- 在改密计划对应的**上次改密结果**中查看执行结果。

说明：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。下载后需要根据在**帐号设置 > 信息加密**中配置的加密方法进行解密。

- 登录SFTP服务器，可以看到改密前后的密码备份文件。

- 下载备份文件并使用ZIP密码解压缩，可以看到修改前后的密码。



验证修改后密码的正确性。

1. 选择**工作台 > 帐号改密 > 帐号资产 > 主机帐号**。
2. 单击**Linux-01**，然后单击**root**对应的**编辑**。
3. 选择**密码管理**，单击**登录测试**。

   如果提示**登录成功**，表示**root**的新密码已在A2000-E 运维管理系统上更新，**当前密码**的状态为**正常**。

其他 5

目录:

举例：导出即时报表

本节将新建一个即时报表，并使用预置的报表模板导出报表为例，详细介绍导出报表的具体方法。

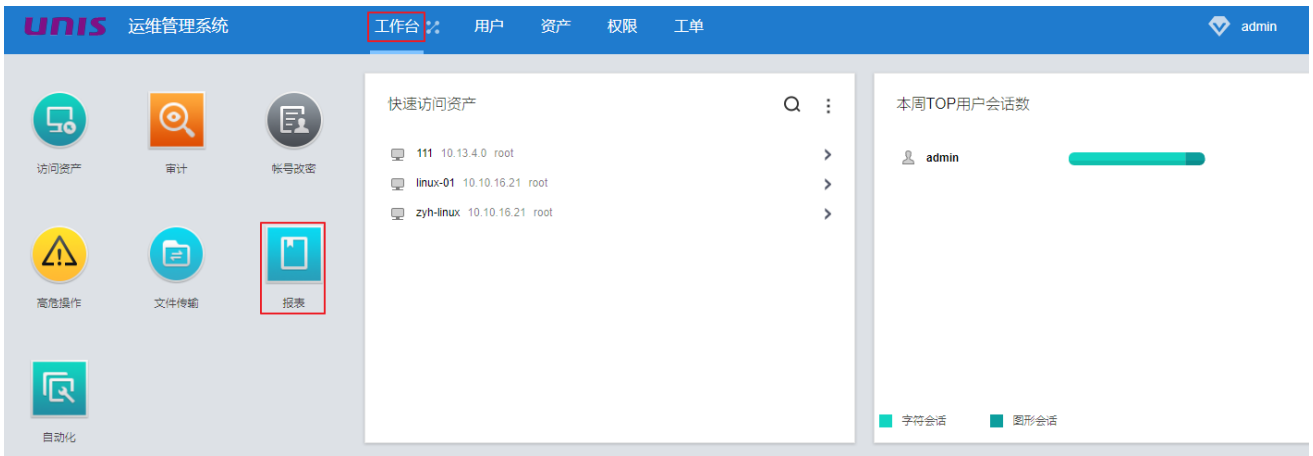
已知数据信息如下表所示：

表 9: 新建报表数据信息

参数	取值	说明
报表名称	用户统计	报表名称。用于标识一个报表，全局唯一。长度为1~30字符串。
报表类型	即时报表	通过手动单击**生成报表**，立即生成一个报表。
自动生成	否	表示只能手动生成该报表。
报表模板	用户基本报表	用于定义报表的具体内容。
统计起始时间点	2019-08-09 00:00/2019-08-10 00:00	导出报表的时间范围。

新建报表

1. 使用超级管理员登录Web界面，选择**工作台**，单击**报表**。



2. 选择**报表查看** > **报表**，单击**新建报表**。

3. 设置各参数信息，完成后单击**保存**。

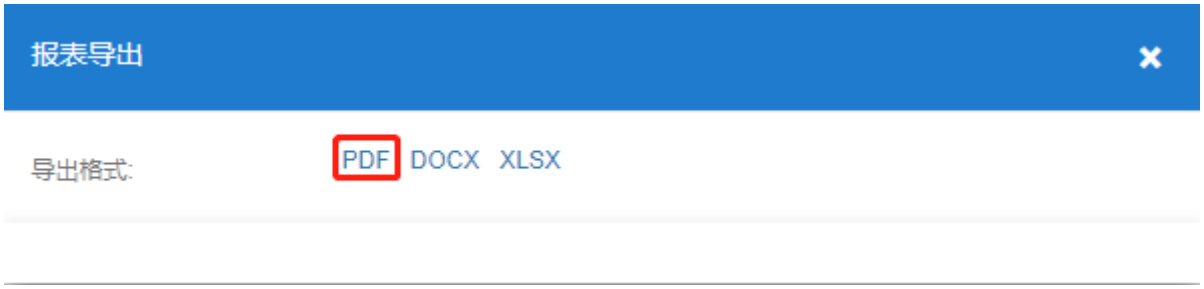
生成报表

4. 单击**生成报表**。

导出报表

5. 生成报表如下，单击右上角的 。

6. 在弹出的对话框中，选择**PDF**，下载该报表的PDF格式。



举例：导出周期报表

本节将新建一个周期报表，并使用预置的报表模板导出报表为例，详细介绍导出报表的具体方法。

已知数据信息如下表所示：

表 10: 新建报表数据信息

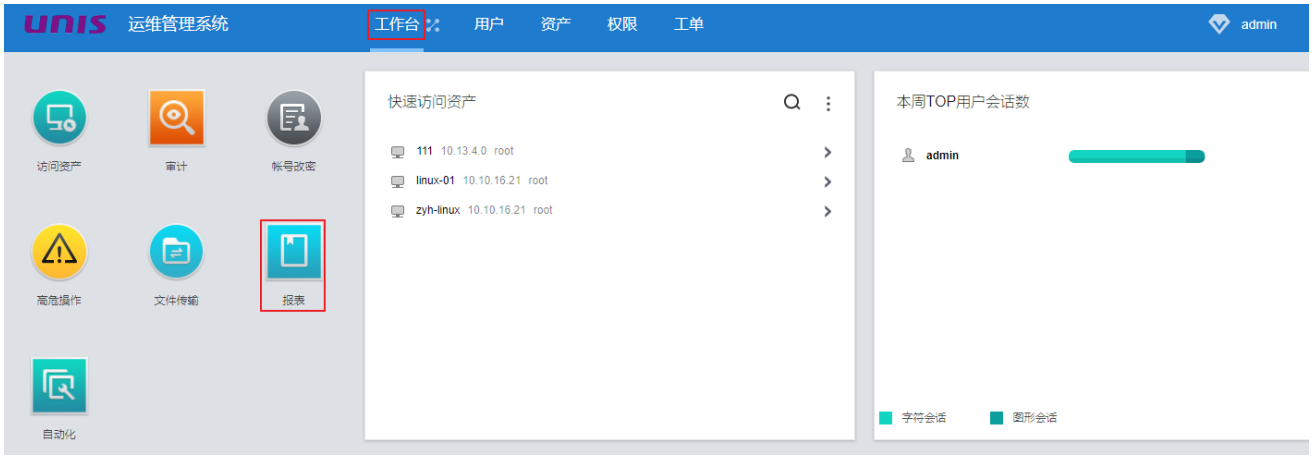
参数	取值	说明
报表名称	用户统计	报表名称。用于标识一个报表，全局唯一。长度为1~30字符串。
报表类型	周期报表	表示按固定的统计周期进行统计，每一个统计周期内统计从开始到结束的信息，并在每一个生成周期时间点上生成上一个统计周期的报表。
自动生成	是	表示按固定的生成周期生成。
周期类别	按日	表示统计周期，也表示生成周期。即按什么频率统计报表信息并生成报表。
报表模板	用户基本报表	用于定义报表的具体内容。报表的简要说明请在**报表配置 > 报表模板**中查看。

表 11: 编辑报表数据信息

参数	取值	说明
统计日期	周五	当周期类别为按日时，勾选需要对每周的哪几天进行统计并生成；其他情况下配置每个统计周期开始的时间点。
邮件发送	否	选择生成报表后是否通过邮件通知指定收件人。需要保证系统服务中的邮件服务设置正确。

新建报表

1. 使用超级管理员、安全保密管理员或其他具有报表权限的用户登录Web界面，选择**工作台**，单击**报表**。



2. 选择**报表查看 > 报表**，单击**新建报表**。

3. 设置各参数信息，完成后单击**保存**。

4. 单击用户报表对应的**编辑**。

5. 选择**高级属性**，选择统计日期，单击**保存**。

生成报表

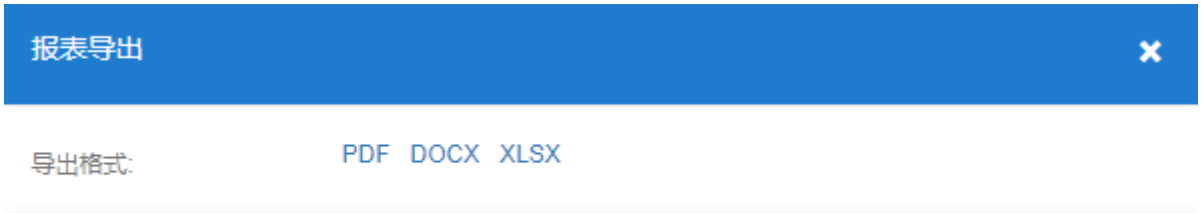
6. 在报表自动生成之后，单击**历史报表**，可查看周期报表的生成时间和状态。

导出报表

7. 单击**历史报表**并**查看**，并单击右上角的下载按钮 。

   生成报表如下：

8. 在弹出的对话框中，选择**PDF**，下载该报表的PDF格式。



举例：脚本任务（Linux系统）

本节将以在一个Linux资产中执行bash脚本为例，介绍在Linux系统中执行脚本任务的具体方法。

已知数据信息如下：

表 12: 自定义脚本文件信息

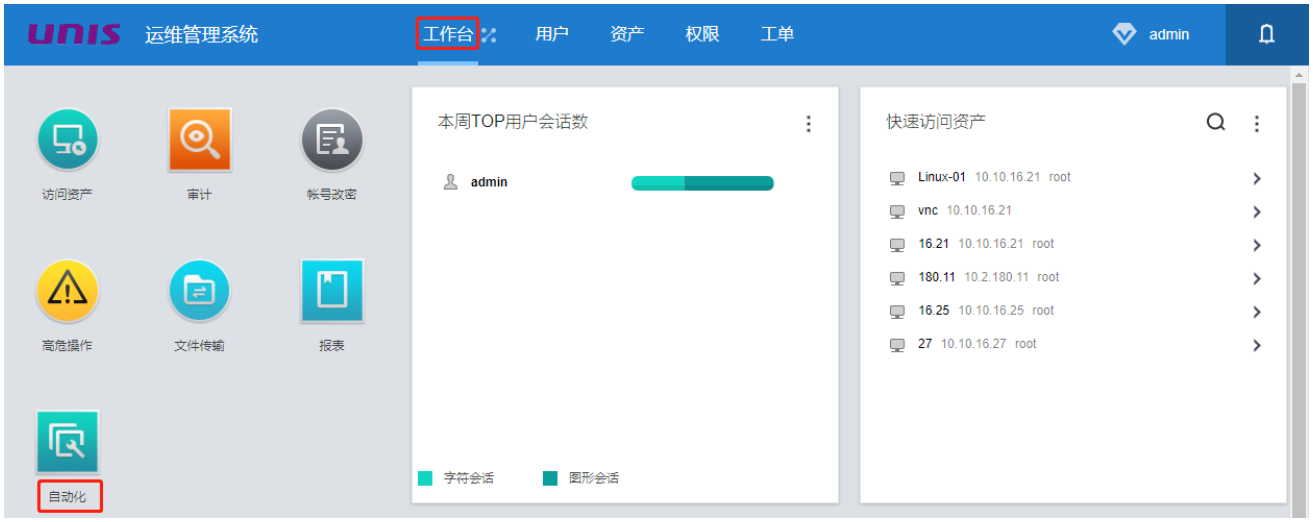
脚本名称	内容
bash.sh	自定义。例：#!/bin/sh echo hello world

表 13: 脚本任务信息

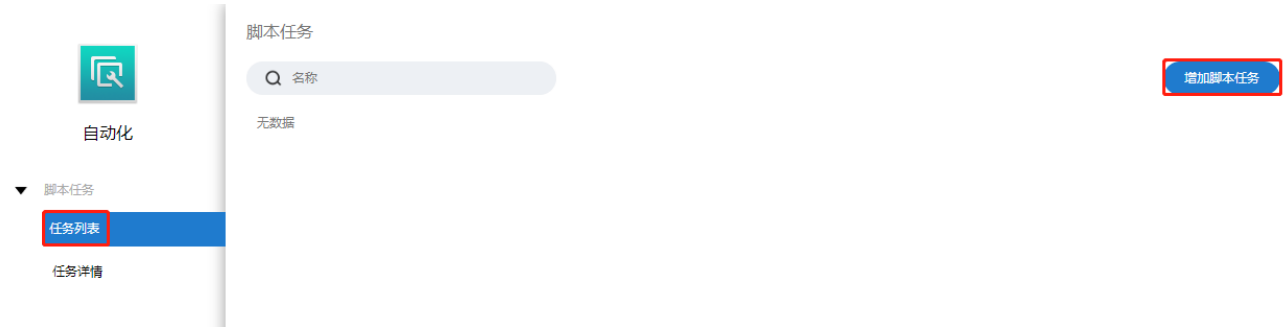
参数	取值	说明
任务名称	bash	脚本任务的名称。字符串格式，长度范围是1~30个字符。
目标资产	Linux-01	目标资产访问必须添加SSH协议，以及使用特权帐号登录。
执行时间	2020-01-07 15:25	脚本任务第一次执行的时间，包括**年/月/日/时/分**。
执行间隔	执行一次	脚本任务的执行间隔，可选项包括：执行一次、按日、按月。
通知方式	站内通知	将脚本任务执行完成提醒通过右上角的站内提醒发送消息给通知人。

增加脚本任务

1. 使用超级管理员或安全保密管理员登录Web界面。
2. 选择**工作台**，单击**自动化**。



3. 选择**脚本任务** > **任务列表**，单击**增加脚本任务**。



4. 上传准备好的自定义脚本，并设置各参数信息，完成后单击**保存**。

5. 单击**立即执行**。

6. 单击**确定**。

查看执行结果

7. 在**任务详情**中单击刷新结果，直到任务显示**结束时间**，即执行完毕。

说明: 当脚本任务执行完成时，右上角也会显示脚本任务通知。

8. 单击**详情**，查看任务执行的结果。

如果脚本任务配置正确，可以看到脚本任务执行的详细结果。

举例：脚本任务（网络设备）

本节将以在一个网络设备资产中执行自定义脚本为例，介绍在类网络设备中执行脚本任务的具体方法。

已知数据信息如下：

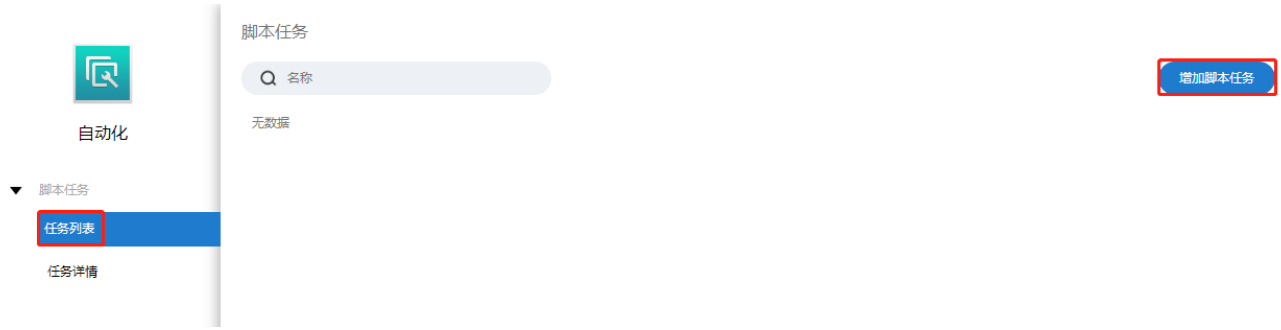
表 14: 脚本任务信息

参数	取值	说明
任务名称	net	脚本任务的名称。字符串格式，长度范围是1~30个字符。
目标资产	H3C Comware1	目标资产访问必须添加Telnet协议，以及使用特权帐号登录。
文件来源	网络资产配置命令 在下拉列表框中选择**自定义**	以自定义脚本为例。
配置命令	ping 10.10.16.182	可直接在配置命令窗口中编辑脚本文件。 例：ping 10.1.2 14 display ip routing-table
执行时间	2020-01-06 15:28	脚本任务第一次执行的时间，包括**年**/**月**/**日**/**时**/**分**。
执行间隔	执行一次	脚本任务的执行间隔，可选项包括：执行一次、按日、按月。

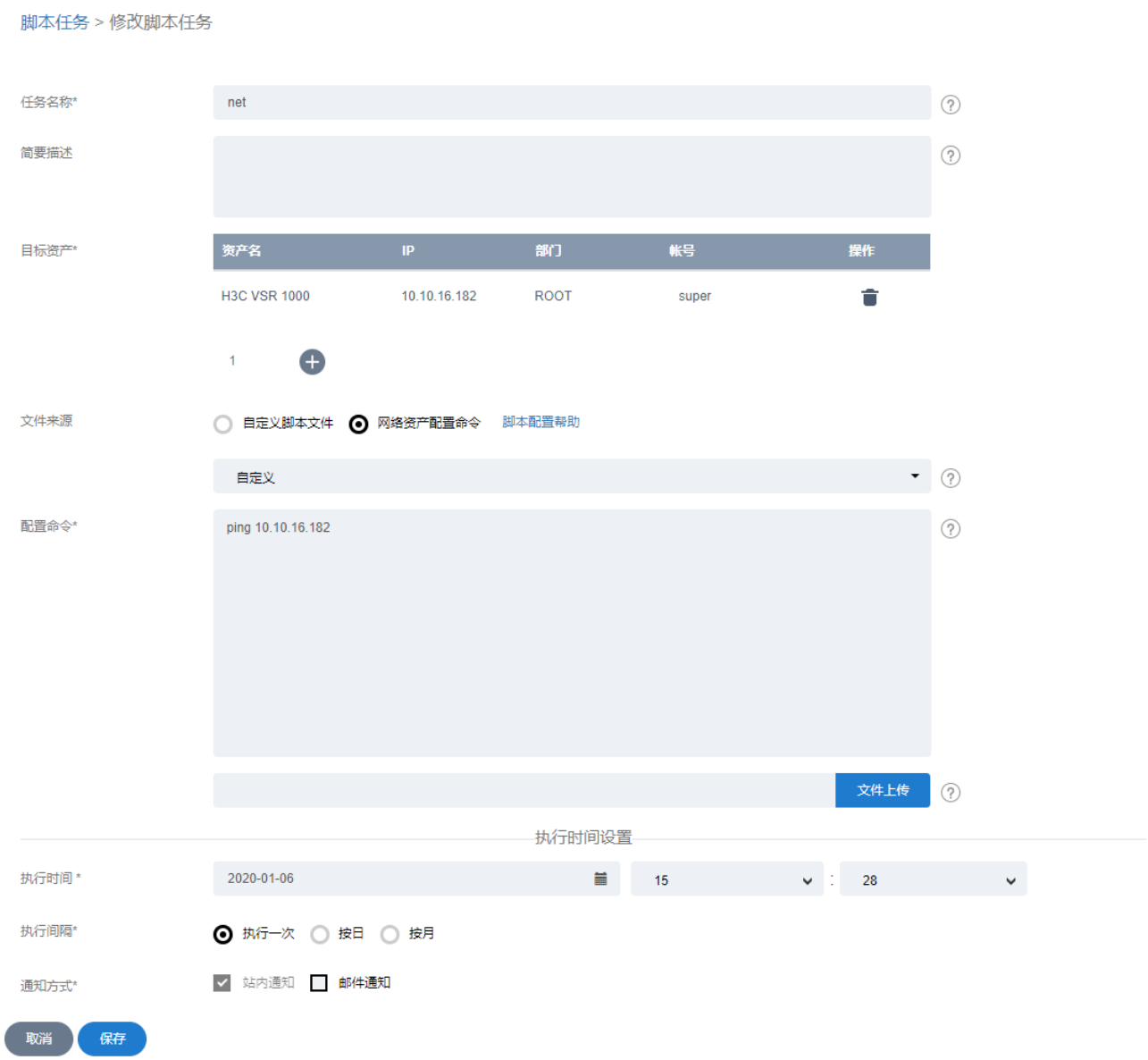
增加脚本任务

1. 使用超级管理员或者安全保密管理员登录Web界面。
2. 选择**工作台**，单击**自动化**。

3. 选择**脚本任务** > **任务列表**，单击**增加脚本任务**。



4. 设置各参数信息，完成后单击**保存**。



5. 单击**立即执行**。

6. 单击**确定**。

查看执行结果

7. 在**任务详情**中单击刷新结果，直到任务显示**结束时间**，即执行完毕。

说明: 当脚本任务执行完成时，右上角也会显示脚本任务通知。

8. 单击**详情**，查看任务执行的结果。

如果脚本任务配置正确，可以看到脚本任务执行的详细结果。


详情
资产名/IP
1 全部
0 失败
1 成功
0 超时
资产名
资产IP
执行结果
简要描述
详情
H3C VSR 1000
10.10.16.182
成功
下发脚本成功
<H3C>ping 10.10.16.182
Ping 10.10.16.182 (10.10.16.182): 56 data bytes, press CTRL_C to break
56 bytes from 10.10.16.182: icmp_seq=0 ttl=255 time=0.069 ms
56 bytes from 10.10.16.182: icmp_seq=1 ttl=255 time=0.085 ms
56 bytes from 10.10.16.182: icmp_seq=2 ttl=255 time=0.066 ms
56 bytes from 10.10.16.182: icmp_seq=3 ttl=255 time=0.093 ms
56 bytes from 10.10.16.182: icmp_seq=4 ttl=255 time=0.074 ms
--- Ping statistics for 10.10.16.182 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.066/0.077/0.093/0.010 ms
<H3C>
<H3C>
<H3C>
<H3C>
<H3C>
合计：1
每页显示
10
1
/ 1