UNIS A2000-E运维管理系统
操作员手册（银河麒麟）

关于本文档

本文档是面向A2000-E 运维管理系统的操作员的操作指导手册。

操作员是A2000-E 运维管理系统的普通用户，拥有登录A2000-E 运维管理系统并进行资产访问等基本功能的权限。

本文将指导操作员完成在A2000-E 运维管理系统上可以进行的这些基本操作。

格式约定

格式	说明
粗体	各类界面控件名称采用**加粗**字体表示，如单击**确定**。
>	多级菜单用 **>** 隔开。如选择**用户管理** > **用户列表**，表示选择**用户管理**菜单下的**用户列表**子菜单。

目录

登录和访问

1

目录:

A2000-E 运维管理系统支持使用Web界面和SSH客户端登录方式登录并访问资产。

A2000-E 运维管理系统用户的登录支持以下几种认证方式，每个用户都由管理员设置了其中一种认证方式。如用户不清楚自己的登录方式和密码，请和管理员确认自己的登录认证方式，并获取对应的密码。

表 1: 身份认证方式

认证方式	获取密码	说明
静态密码	向管理员获取密码	使用本地密码或LDAP服务器对应的用户密码。
RADIUS认证	向管理员了解密码获取方式	通过用户公司/机构的内部RADIUS认证系统获取RADIUS口令。
动态令牌	向管理员获取动态令牌和PIN1码。	使用分配的动态令牌生成的动态密码。请在令牌左侧倒计时走完之前完成输入。 输入的密码前半段是“PIN1码”，后半段是绑定的动态令牌生成的6位数字密码。在同一个密码输入框内输入该拼接后的字符串。
双因子认证	-	使用以上其中两种认证方式的组合。需要分别使用两种认证的密码完成认证。 请参考使用双因子认证。

通过Web方式访问

Web界面是A2000-E 运维管理系统最主要的访问入口。

通过Web界面登录A2000-E 运维管理系统

请参考表 1: 身份认证方式准备登录所需的密码。

通过Web界面登录A2000-E 运维管理系统的环境要求请参考下表：

表 2: 通过Web界面登录A2000-E 运维管理系统的环境要求

项目	要求
操作系统	麒麟桌面操作系统（龙芯版） V7.0 **说明:** 麒麟操作系统不支持安装AccessClient或SFTP等软件，也不支持以调用工具的方式开启会话。
浏览器	使用麒麟自带的Mozilla Firefox
显示器分辨率	建议最小为1280*1080（系统的缩放设置为100%时）。 **说明:** 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。

本节以Firefox浏览器为例，指导完成登录到A2000-E 运维管理系统的Web界面。

1. 在浏览器中输入A2000-E 运维管理系统的IP地址(**https://A2000-E 运维管理系统的IP地址**)，进入A2000-E 运维管理系统的Web登录页面。

   说明: 登录时如出现以下界面，请选择继续前往（例如Firefox浏览器请单击**我已充分了解可能的风险** > **添加例外**，并在弹出的对话框中单击**确认安全例外**）。

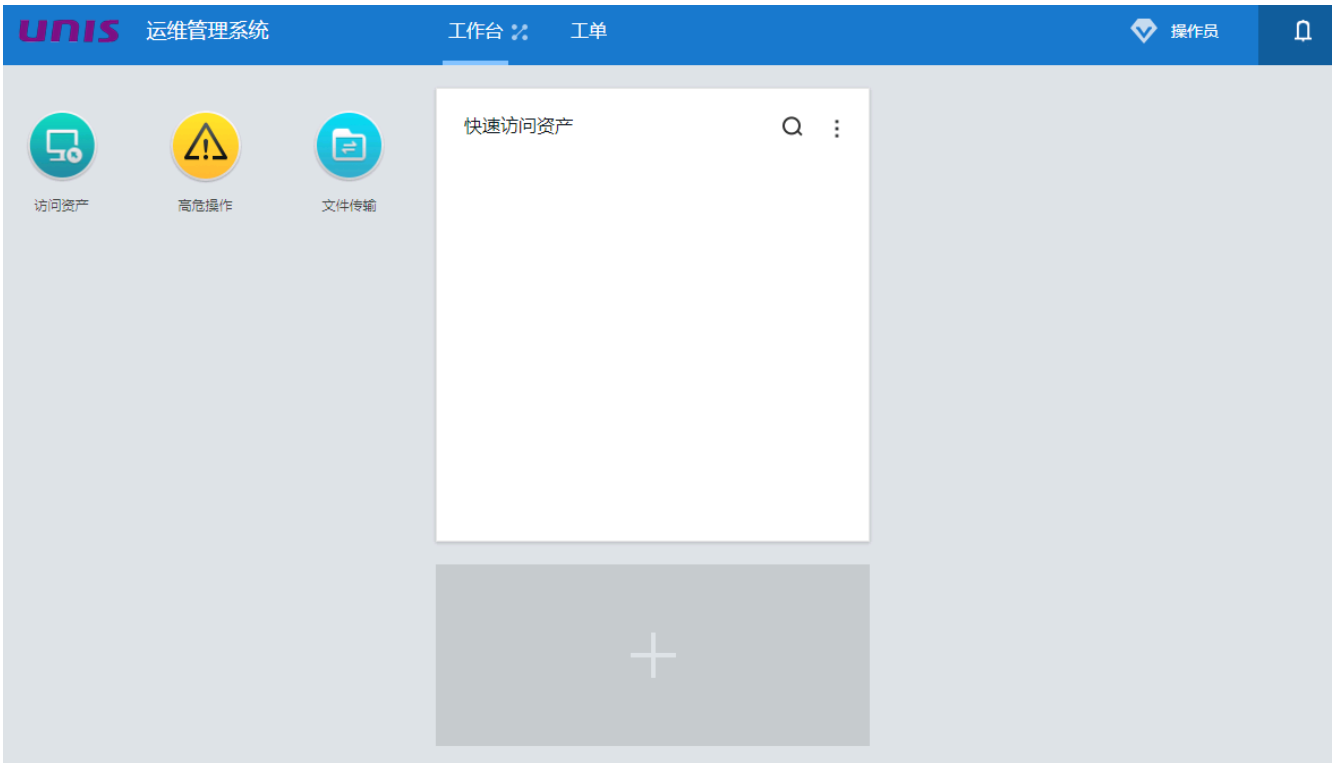
2. 输入帐号和密码，单击**登录**。

说明:

- 密码的输入方式请参考表 1: 身份认证方式。
- 如使用双因子登录，密码输入方式请参考使用双因子认证。

登录成功后，进入A2000-E 运维管理系统的Web界面主页面。

- 在任一界面单击左上角的UNIS，可以回到首页。
- 在任一界面单击上方的**工作台**，可以切换到不同的服务项。
- 单击右上角的用户帐号名称（例如操作员），可以打开**帐号设置**、**访问记录**和**帮助**菜单，或退出登录。



访问资产

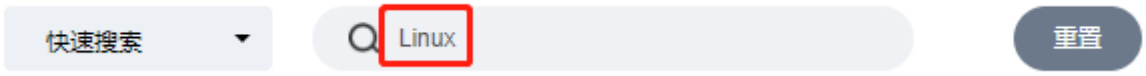
A2000-E 运维管理系统支持在Web界面，通过xdmcp、xfwd以及vnc协议访问Linux主机资产。

通过Web界面访问Linux时，需要完成以下操作。

- 在A2000-E 运维管理系统上为待访问资产配置了xdmcp、xfwd或vnc访问协议。
- 在待访问的资产上开启了相关服务和监听端口。

用户在Web界面的**访问资产**界面中查找资产，有以下几种方式：

- **直接查找**：在左侧导航栏中，选择动态视图中的具体节点并查看节点下的资产。
- **快速搜索**：在动态视图选择节点后，如资产仍较多，在搜索框中输入资产名称/IP/简要说明/系统帐号的全部或一部分进行模糊查找。



- **高级筛选**：在动态视图选择节点后，如资产仍较多，单击下拉框选择**高级筛选**，设置筛选条件后单击**筛选**。

- **在最近访问中查找**：单击**访问资产**后，选择**最近访问**页签。

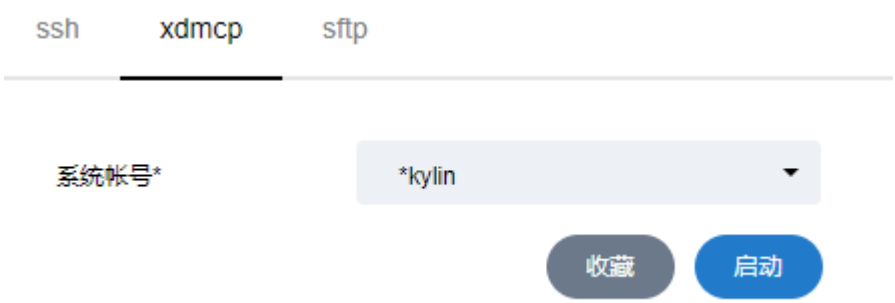
- **收藏并查找**：对资产单击☆收藏后，单击**访问资产**并选择**最近访问**页签，查看收藏。

查找到资产并启动访问后，A2000-E 运维管理系统将通过浏览器建立访问会话。

本节以xdmcp协议为例，指导完成资产访问。通过xfwd和vnc协议访问资产的过程类似。

1. 通过Web界面登录A2000-E 运维管理系统。
2. 单击**工作台** > **访问资产**，并找到待访问的资产。

3. 单击**访问**，选择**xdmcp**，并设置**系统帐号**。



除了通过vnc协议登录之外，通过其他协议登录时都需要配置**系统帐号**。用于标识登录对应资产时所使用的帐号。有以下几种类型：

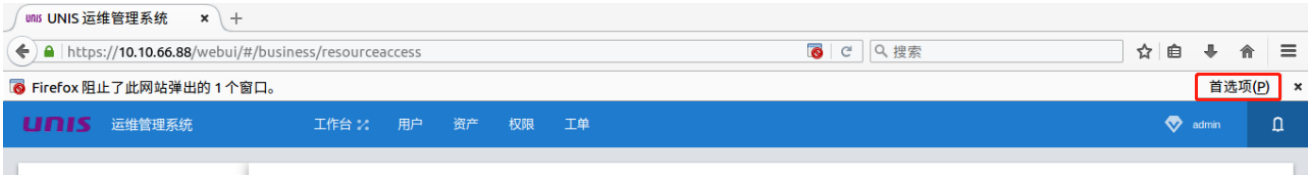
- self：同用户帐号。使用和当前登录A2000-E 运维管理系统的帐号同名的帐号登录资产，请操作员自行确保该帐号在待访问资产上存在。
- any：登录时提供。A2000-E 运维管理系统仅连接到资产的登录界面，不自动输入帐号名称和密码，由访问者手动填写。

- A2000-E 运维管理系统上已添加的资产帐号名称，例如**kylin**，A2000-E 运维管理系统使用该帐号登录到资产设备。

4. 确认配置无误后，单击**启动**，浏览器将打开远程会话。

说明:

当出现图中所示的情况是，可以单击**首选项**，选择**允许 10.10.66.88 弹出窗口**。



远程会话启动成功后，页面将显示待访问资产，用户可以在该窗口中对资产进行操作和管理。

通过SSH方式访问

用户如果需要快速访问允许通过SSH或者Telnet访问的资产，可以使用SSH登录A2000-E 运维管理系统的交互终端。

通过SSH客户端登录A2000-E 运维管理系统

通过SSH客户端登录A2000-E 运维管理系统后仅能查看并访问当前用户可通过SSH/Telnet访问的资产。

请参考表 1: 身份认证方式准备登录所需的密码。

通过SSH客户端登录A2000-E 运维管理系统的环境要求请参考下表：

表 3: 通过SSH客户端登录A2000-E 运维管理系统的环境要求

项目	要求
操作系统	银河麒麟桌面操作系统（龙芯版） V7.0
SSH客户端	银河麒麟操作系统自带的终端。

如登录帐号被管理员在A2000-E 运维管理系统上设置了下次登录时必须修改密码，请先通过Web界面登录并重设密码。

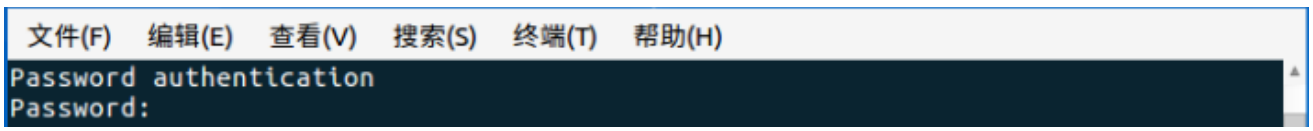
1. 鼠标右击，选择**在终端中打开**。

2. 在终端窗口输入ssh opt@10.10.66.88，并按回车。

3. 选择通过密码或密钥登录。

   - 通过密码登录：

     根据提示输入opt的登录密码，并按回车。



   - 通过密钥登录：

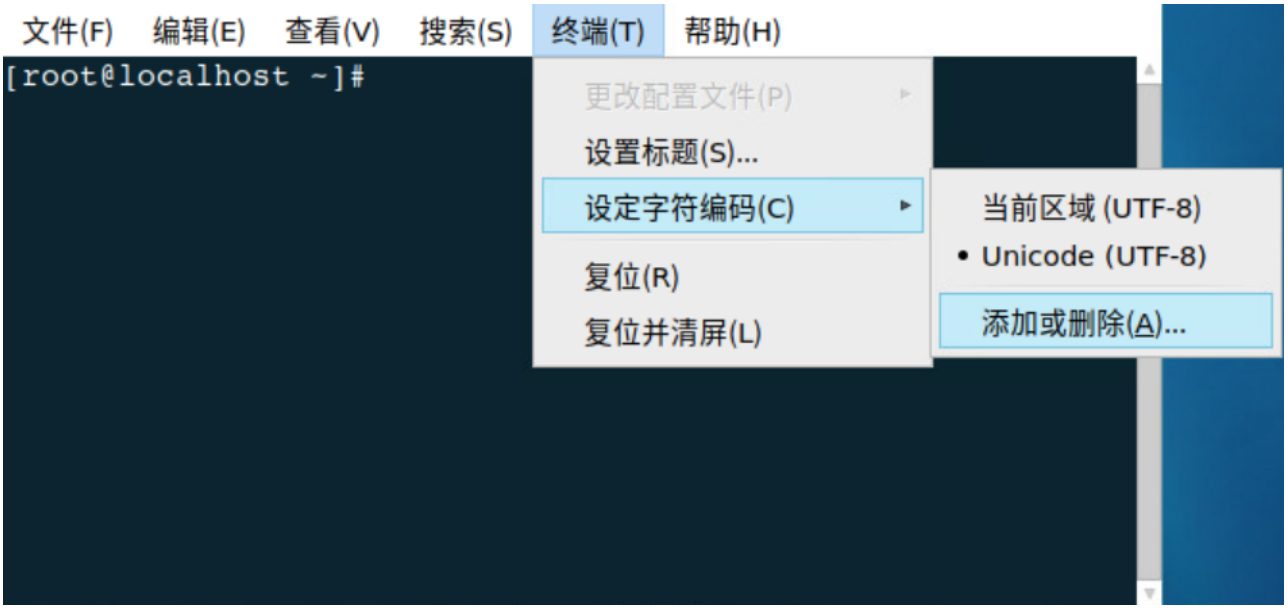
需要先完成配置密钥。此时用户无需输入密码，SSH客户端会直接从密钥的默认存储地址中获取私钥，并与A2000-E 运维管理系统中配置的公钥进行验证。验证通过后，登录成功。

```
The authenticity of host '10.10.66.88 (10.10.66.88)' can't be established.
RSA key fingerprint is SHA256:KlKWMYNTDm9zaWHFF0M/DkpMG+X/+hGSn5qKu5DkQpw.
RSA key fingerprint is MD5:90:0c:34:b6:f7:be:72:a4:65:18:83:fb:47:90:93:a5.
Are you sure you want to continue connecting (yes/no)?yes
```

连接成功后显示下列菜单，可以选择要访问的资产，并通过SSH/Telnet连接到该资产。

4. 可选： 如果登录后的页面显示乱码，可以在当前终端窗口中通过以下方法修改字符编码后，按回车键即可显示正常。

   a) 选择**终端** > **设定字符编码** > **添加或删除**。



   b) 在弹出的对话框左侧选中**GB18030 简体中文**，通过→添加到右侧，完成后单击**关闭**。

c) 选择**终端** > **设定字符编码**，勾选**简体中文（GB18030）**。

通过SSH客户端登录A2000-E 运维管理系统后，可以执行以下常用操作：

表 4: SSH交互终端常用操作

使用场景	输入	说明
最外层**资产分组列表**菜单	q	退出登录A2000-E 运维管理系统
	l	切换语言（从中文到英文，或从英文到中文）
	r	重新加载数据
	/设备IP、名称或说明	过滤设备
目标资产列表菜单	i	按IP排序
	a	按设备名称排序

使用场景	输入	说明
	/设备IP、名称或说明	过滤设备
任意子菜单	直接按回车键	返回上一级菜单
断开到设备的会话后	直接按回车键	回到**资产分组列表**菜单
	r	重新连接到已断开的会话
	q	退出登录A2000-E 运维管理系统

访问资产

在A2000-E 运维管理系统的SSH交互终端中只支持访问允许Telnet/SSH访问的资产。

通过A2000-E 运维管理系统的SSH交互终端访问资产有三种方式：

- 先通过SSH客户端登录A2000-E 运维管理系统，在A2000-E 运维管理系统找到待访问的资产后再建立字符会话进行访问。
- 直接建立到待访问资产的字符会话。必须提前知道待访问资产的IP地址和登录帐号。
- 通过SSH远程执行命令。一般用于脚本中，仅执行单条命令，执行完后断开连接。

登录到A2000-E 运维管理系统后查找并访问资产

1. 通过SSH客户端登录A2000-E 运维管理系统。
2. 根据提示输入待访问资产所在的资产分类编号，并按回车键确定。

```
资产分类列表
序号: 资产分类
  0: 全部资产
  1: 资产组1
  2: 资产组2
请选择资产分类：1
```

> **说明:** 资产分类会根据字符会话配置中的**直连分类方式**进行展示。上图中是按资产组进行分类。如果不存在可用分类，连接后将直接进入未分类资产列表中；如只存在一个可用分类，连接后将直接进入该分类。

3. 根据提示输入待访问的资产的序号、IP地址或名称，并按回车键确定。

```
已选择：资产组1
目标资产列表
序号: IP 地址       名称(说明) *
  1: 10.10.33.30     Linux-01
  2: 10.10.33.130    Linux-02
请选择目标资产：1
```

4. 根据列出的登录帐号列表，输入访问资产要使用的帐号的序号或完整帐号名称（含协议名称），并按回车键确定。建立字符会话。

```
已选择：资产组1 > Linux-01(10.10.33.30)
登录帐号列表
序号:  帐号名
  1:  any
  2: * root
```

```
 3: self
请选择登录帐号：2
```

说明:

- 帐号列表说明如下：
  - self：同用户帐号。使用和当前登录A2000-E 运维管理系统的帐号同名的帐号登录资产。请操作员自行确保该帐号在待访问资产上存在。
  - any：登录时提供。A2000-E 运维管理系统仅连接到资产的登录界面，不自动输入帐号名称和密码，由访问者手动填写。
  - A2000-E 运维管理系统上已添加的资产帐号名称，例如**administrator**，A2000-E 运维管理系统使用该帐号登录到资产设备。
- *表示该帐号的密码已在A2000-E 运维管理系统上托管，将无需输入密码直接登录。
- 当选择的帐号为self时，如用户使用LDAP/RADIUS其中之一认证或双因子认证中包含LDAP/RADIUS之一，则使用对应的LDAP/RADIUS用户名同名的帐号登录资产；如用户使用LDAP+RADIUS双因子认证，则使用第一重认证所使用的LDAP/RADIUS用户名同名帐号。
- 如管理员设置了启动会话时必填或可填备注，请输入备注后按回车。备注是一个1~100长度的字符串。

  ```
  Connecting to root@Linux-01(10.10.33.30) ...
  请输入备注：备注内容
  ```
- 该会话如匹配对应的高危操作规则，将受到高危操作规则的影响，需要进行复核，请参考执行高危操作。

直接访问资产

1. 选择**应用程序** > **收藏**，双击**终端**。
2. 执行以下命令：

   ```
   ssh A2000-E
           运维管理系统的用户名/目标资产的地址/访问目标资产的帐号@A2000-E
           运维管理系统的地址
   ```

   例如：

   ```
   ssh user01/10.10.33.30/root@10.66.38.139
   ```
3. 在收到密码提示后，输入A2000-E 运维管理系统的密码。

   目标资产登录成功后显示如下信息。

通过SSH执行命令

需要满足以下前提条件：

- 必须使用OpenSSH客户端。
- 目标资产已在A2000-E 运维管理系统上托管了帐号和密码。

OpenSSH客户端的SSH命令，支持在待访问的地址之后添加command参数，填写待在目标资产上执行的命令，执行完命令后断开连接。一般用于在脚本中连接资产并远程执行命令。

通过该方式执行的命令，不会受到会话复核的限制，无需被复核即可执行。但如配置了命令复核，只要规则中执行的动作不为允许，该命令的执行的都将被拒绝，请参见执行高危操作。

本节以在OpenSSH客户端的Shell中执行命令为例，实际使用中可以将该命令写到脚本中。

1. 打开OpenSSH客户端的Shell菜单。
2. 执行以下命令：

   ```
   ssh A2000-E
           运维管理系统的用户名/目标资产的地址/访问目标资产的帐号@A2000-E
           运维管理系统的地址 命令内容
   ```

   例如：

   ```
   ssh opt/10.10.33.30/root@10.10.33.23 pwd
   ```

3. 在收到密码提示后，输入A2000-E 运维管理系统的密码。

   命令执行成功后，将显示命令的回显。

   ```
   [root@unis-node01 ~]# ssh opt/10.10.33.30/root@10.10.33.23 pwd
   Password authentication
   Password:
   /root
   ```

   说明:

- 资产的密码将由A2000-E 运维管理系统自动代填，如未托管密码，命令执行将失败。
- 如需执行多条命令，可以使用;、&、|等符号进行分割。
- 命令如需要在脚本中执行，建议配置密钥，使执行过程中不需要进行密码交互。

高危操作

2

目录:

管理员如果配置了高危命令规则，指定用户在访问资产和执行命令时将受到限制。根据配置的规则，操作员可以作为被复核人受到这些规则的限制，也可以作为复核人来复核其他用户的操作。

执行高危操作

当管理员配置了高危操作时，如在特定资产的字符会话上执行某些特定的命令时，会触发高危命令，执行的命令被发送通知、被要求复核、被直接拒绝，或被直接断开会话。

操作员在执行命令时有可能触发已配置的高危操作规则，已配置的具体规则请向管理员咨询。

触发高危命令后的示例如下：

操作员在字符会话中执行命令，正常触发高危操作后的现象及处理方法如下：

现象	说明	处理方法
执行命令，提示**This command requires manager's confirmation, are you sure?[Y/n]**。	操作员触发了命令复核规则，需要完成命令复核后命令才能被执行。	**1.** 确认是否要执行该命令。 • 是，输入**Y**（忽略大小写），转到下一步。 • 否，输入**N**（忽略大小写），命令被撤回，操作结束。 **2.** 联系命令复核对应的复核人中的任意一个完成复核命令。如不清楚有哪些命令复核人请咨询管理员。 **说明:** 在复核人进行复核之前，操作员可以按**Ctrl**+**C**，取消命令复核，所有复核人收到的命令复核申请都将被撤回，命令的执行也被取消。 复核人完成复核并允许命令执行之后，命令将开始执行并显示执行结果；复核人如拒绝命令执行，该命令的执行将被取消。
执行命令，提示**You are not allowed to use this command**。	操作员触发了拒绝用户执行的高危命令	请使用其他允许被执行的命令。
执行命令，提示**Session will be killed because of this command**。	操作员因执行高危命令，触发了断开会话的操作	请重新打开会话，并使用其他允许被执行的命令。

高危操作规则如配置有误，访问资产或执行命令将无法进行，具体现象和处理方法如下：

现象	说明	处理方法
执行命令，提示**No valid user for confirmation. Please contact the administrator**。	命令复核规则没有设置复核人或设置的所有复核人均不可用。	联系管理员为命令复核规则设置可用的复核人。

复核命令

如管理员配置了命令复核规则，则当有其他用户触发命令复核规则时，当前用户如为复核人之一，可以对操作人要执行的命令进行复核。

操作人触发命令复核时，所有复核人都将收到命令复核提示，当有一个复核人完成复核之后，其他复核人收到的复核请求将失效并被撤回。操作人如自行撤回复核申请，复核人将无法再复核。

复核人收到提醒后，可以通过Web界面复核，即复核人在Web界面右上角收到命令复核提醒：**有待复核的命令**。复核人直接在Web界面处理高危命令复核申请。

1. 使用复核人帐号通过Web界面登录A2000-E 运维管理系统。
2. 单击右上角的  提醒图标，查看收到的待复核命令的提醒，并单击**查看详情**，跳转到复核申请列表页面。

3. 查看收到的复核申请，确认命令是否可以执行。
   - 是，单击**允许**，该命令将直接执行并显示回显。
   - 否，单击**拒绝**，该命令的执行将被阻断。

文件传输

3

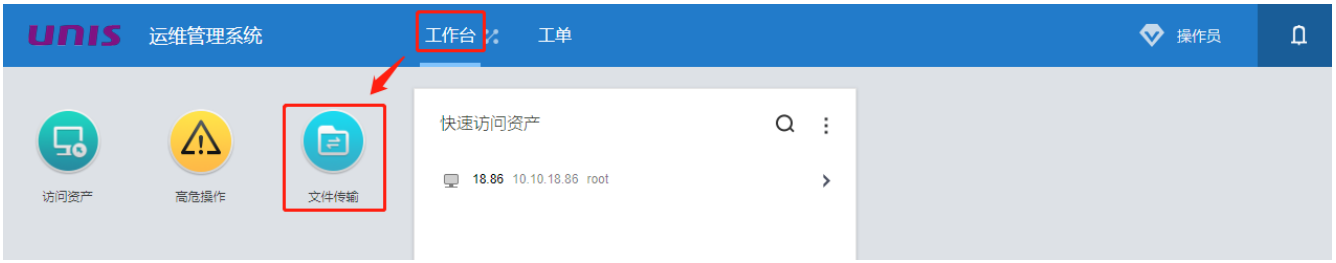
目录:

介绍如何在本地PC与Linux资产之间传输文件。

网盘传输

通过A2000-E 运维管理系统客户端的自带的**文件传输**功能，用户可以将文件在本地PC、A2000-E 运维管理系统、目标资产设备之间上传/下载。

使用A2000-E 运维管理系统网盘的相关功能，请通过Web界面登录A2000-E 运维管理系统后选择**工作台** > **文件传输**。

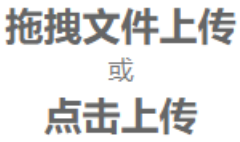


上传文件

1. 选择**文件传输** > **文件传输**。

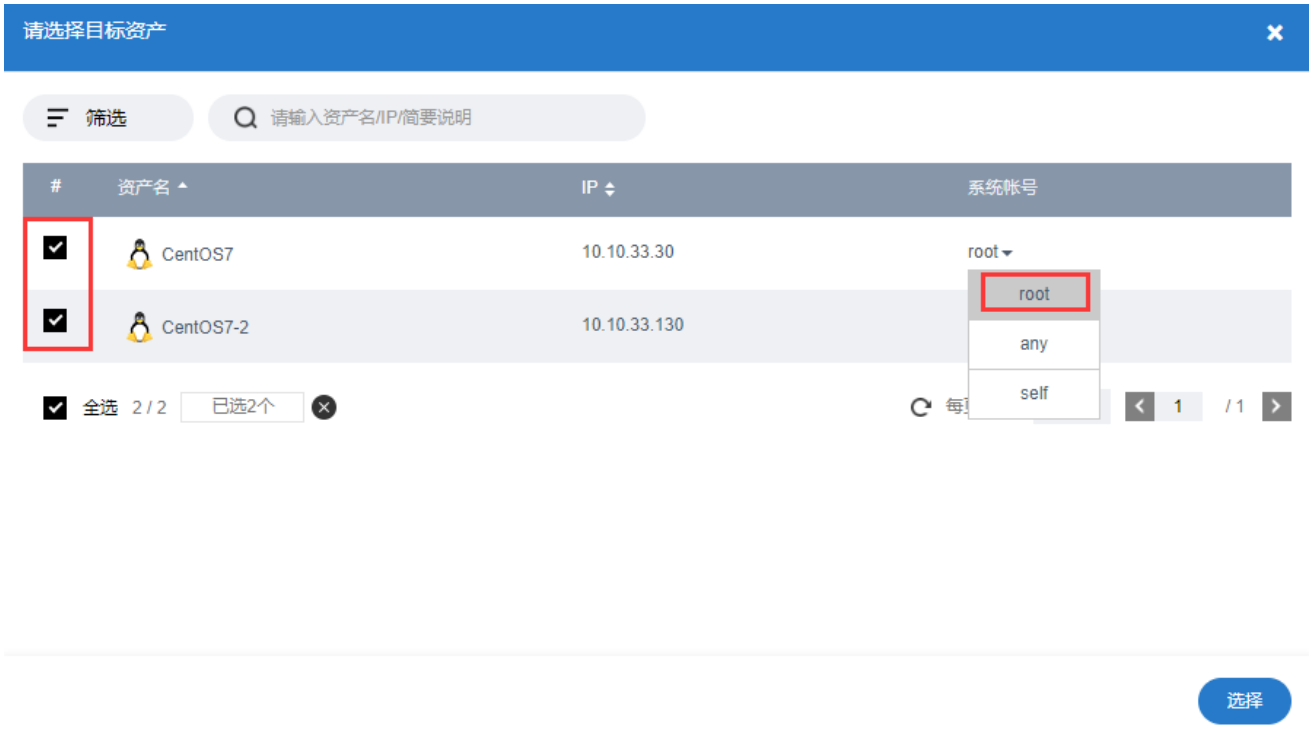
2. 单击**从本地上传**，上传文件到A2000-E 运维管理系统。

3. 拖拽文件或直接单击并在弹出的窗口中选择待上传的文件。



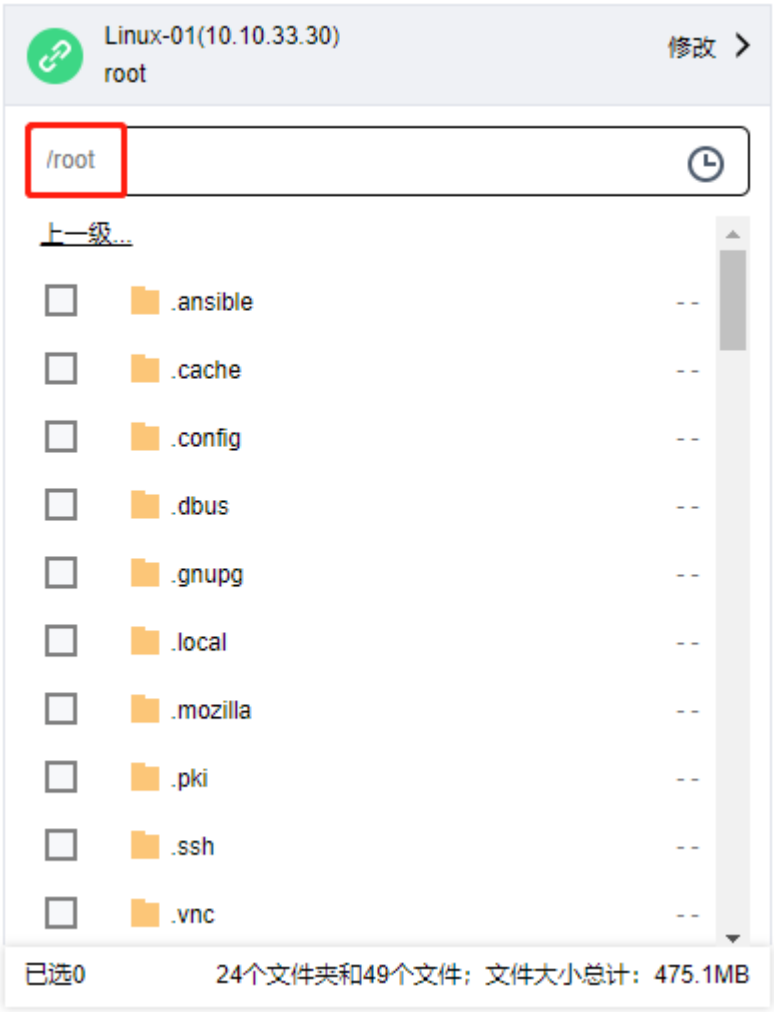
4. 单击右侧的**选择目标资产**，勾选一个或多个待连接的Linux/Unix资产，并下拉选择帐号上传使用的帐号。

> **说明:** 使用的帐号必须为已托管了密码的帐号。如需使用未托管密码的帐号，选择**any**帐号；指定多个目标资产时，不可使用any帐号。



5. 选择上传的路径。

   - 选择单个资产时，填写上传路径或在窗口中选择目录层级。



- 选择多个资产时，填写统一的上传路径。

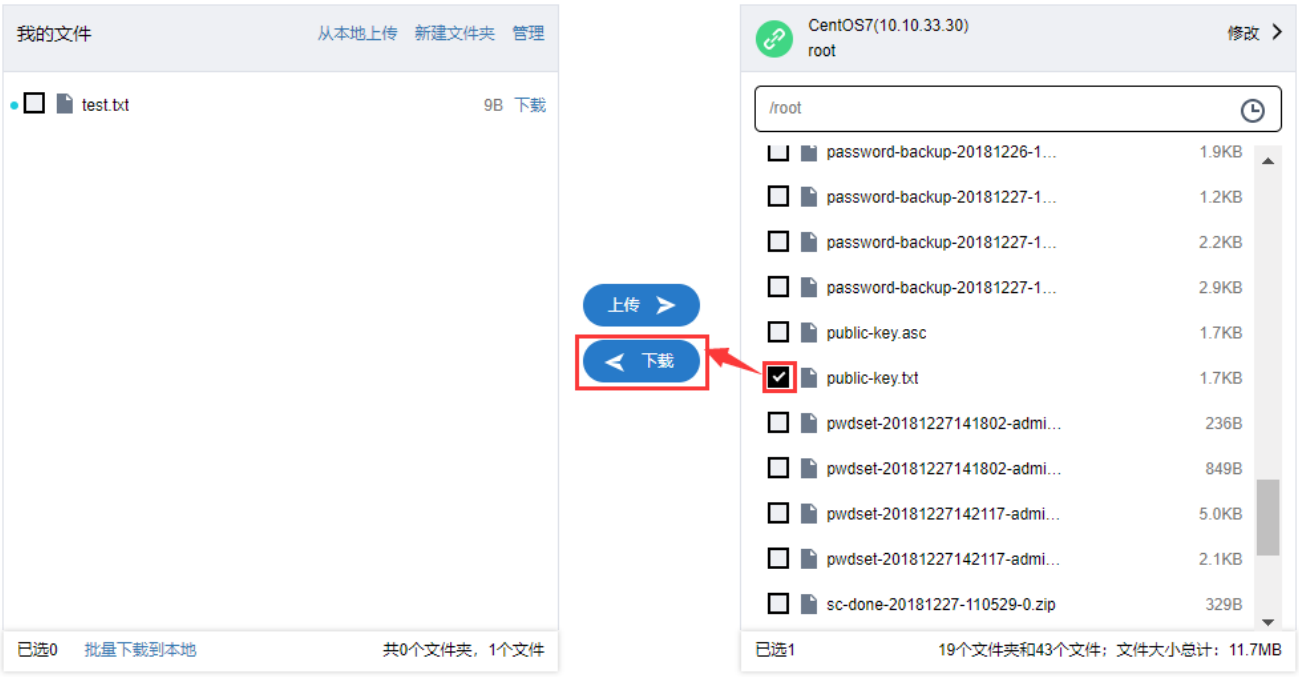
6. 在左侧勾选待上传的文件，并单击**上传**，将文件从A2000-E 运维管理系统的网盘上传到目标资产中。

下载文件

1. 选择**文件传输** > **文件传输**。
2. 单击右侧的**选择目标资产**，勾选一个待连接的Linux/Unix资产，并下拉选择帐号上传使用的帐号。

   说明: 只能勾选一个资产，勾选多个资产时将仅能上传不能下载。

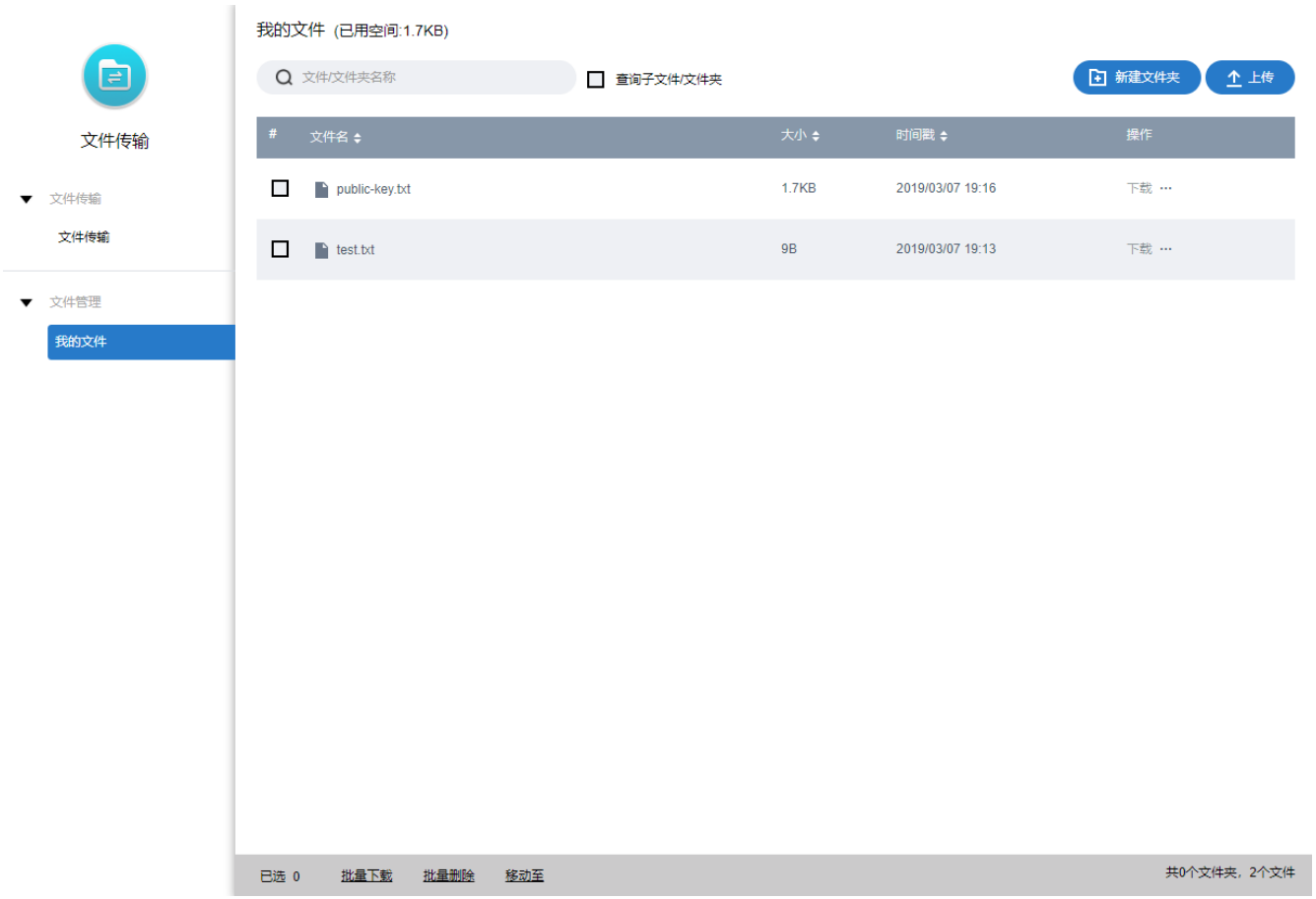
3. 在右侧找到待下载的文件并勾选，单击**下载**，将文件下载到网盘中。



4. 下载到网盘完成后，勾选文件，并单击**批量下载到本地**，将文件从网盘下载到本地。

管理文件

在**我的文件**界面，可以对已上传或下载到A2000-E 运维管理系统的文件进行管理。



该页面主要有以下管理操作：

操作	**说明**
查询	在对话框中，输入文件或文件夹的名称并按回车键进行查询。如未勾选**查询子文件/文件夹**，只会搜索当前文件夹内的内容。但勾选了**查询子文件/文件夹**后，不能执行批量操作。
新建文件夹	在文件列表中进入指定的目录，然后单击**新建文件夹**，填入文件夹的名称，在当前路径新建文件夹。
上传	在文件列表中进入指定的目录，然后单击**上传**，并在弹出的对话框中选中本地PC上待上传的文件，将文件上传到当前进入的目录。 **说明：**该操作要求当前用户拥有足够的配额空间。界面上方会标出**已用空间：已用大小/配额大小**，如未设置配额上限，则不会显示配额大小。如配额不够用，请先删除多余的文件，以使配额满足要求。
下载	在文件列表中找到待下载的文件或文件夹，单击**下载**将文件下载到本地PC。如需批量下载，请勾选所有待下载的文件，并单击下方的**批量下载**，下载文件夹或批量下载文件，A2000-E 运维管理系统将使用zip压缩包打包。

操作	说明
删除	在文件列表中找到待删除的文件或文件夹，单击**...**，在下拉菜单中选择**删除**，并单击**确认**。如需批量删除，请勾选所有待删除文件，并单击下方的**批量删除**。
重命名	在文件列表中找到待重命名的文件或文件夹，单击**...**并在下拉菜单中选择**重命名**，在对话框中输入新的文件名并单击**确定**。新的文件名必须是一个长度为1~100的字符串，不能以“.”开头且不能包含“\”或“/”。
移动至	在文件列表中找到待移动的文件，单击**...**并在下拉菜单中选择**移动至**，在弹出的对话框中选择目的路径。如需批量移动，请勾选所有待移动的文件，并单击下方的**移动至**。文件夹不能进行移动。
分享文件	在文件列表中找到待分享的文件，单击**...**并在下拉菜单中选择**分享文件**，在弹出的对话框中输入有效时长（天），取值范围为1~30天。单击**确定**后，会弹出分享链接及密码。已分享的文件可以单击**...**并在下拉菜单中选择**查看分享链接**或**取消分享**。
获取分享的文件	获取分享文件的用户必须具有文件传输权限。用户接收到分享链接和密码之后，请按以下操作获取文件： **1.** 使用自己的帐号通过Web界面登录A2000-E 运维管理系统。 **2.** 在同一浏览器中新建页签，输入分享链接，并跳转到该链接。 **3.** 页面跳转后将弹出密码输入框，请输入分享文件的密码。 **4.** 单击**保存至**将该文件保存至A2000-E 运维管理系统上自己的文件空间中，或单击**下载**，将文件下载到本地。

工单

4

目录:

在A2000-E 运维管理系统上可以通过工单申请资产权限、资产密码。

操作员可以提交以下类型的工单，不同类型的工单对使用人和审批人的要求如表 5: 工单申请人、使用人和审批人的要求所示。

表 5: 工单申请人、使用人和审批人的要求

工单类型	使用人	审批人
资产权限	用户具有**访问资产**权限。	由超级管理员指定的审批人名单中的用户。如未指定，则为所有安全保密管理员。
资产密码	用户具有工单权限。	同上

申请人提交工单后，审批人会收到通知；审批人审批工单后，申请人、使用人也会收到通知。A2000-E 运维管理系统支持以下通知方式。

- **消息**：用户登录Web界面后，单击右上角的  查看通知消息。

- **邮件**：如果已配置用户的工作邮箱，用户会收到通知邮件。

申请人可以在**待办工单**或**已办工单**中查看工单详情：

- 申请人已提交申请的但未完成审批的工单，将显示在**工单** > **工单管理** > **待办工单**中。
- 申请人已提交申请且已完成审批的工单，将显示在**工单** > **工单管理** > **已办工单**中。

申请资产

用户可以通过工单来申请资产的访问权限。

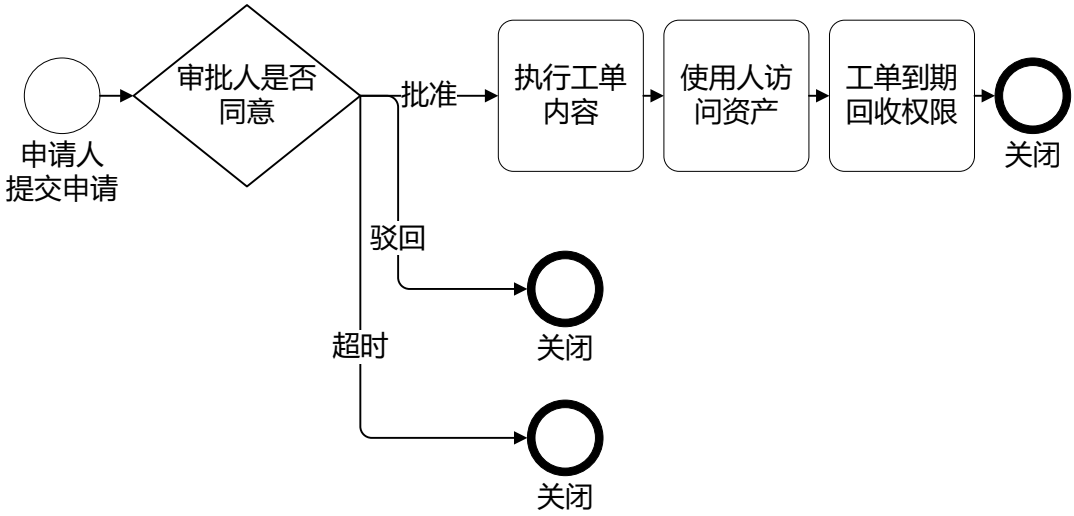


图 1: 资产权限工单处理流程

1. 选择**工单** > **工单管理** > **新建工单**。

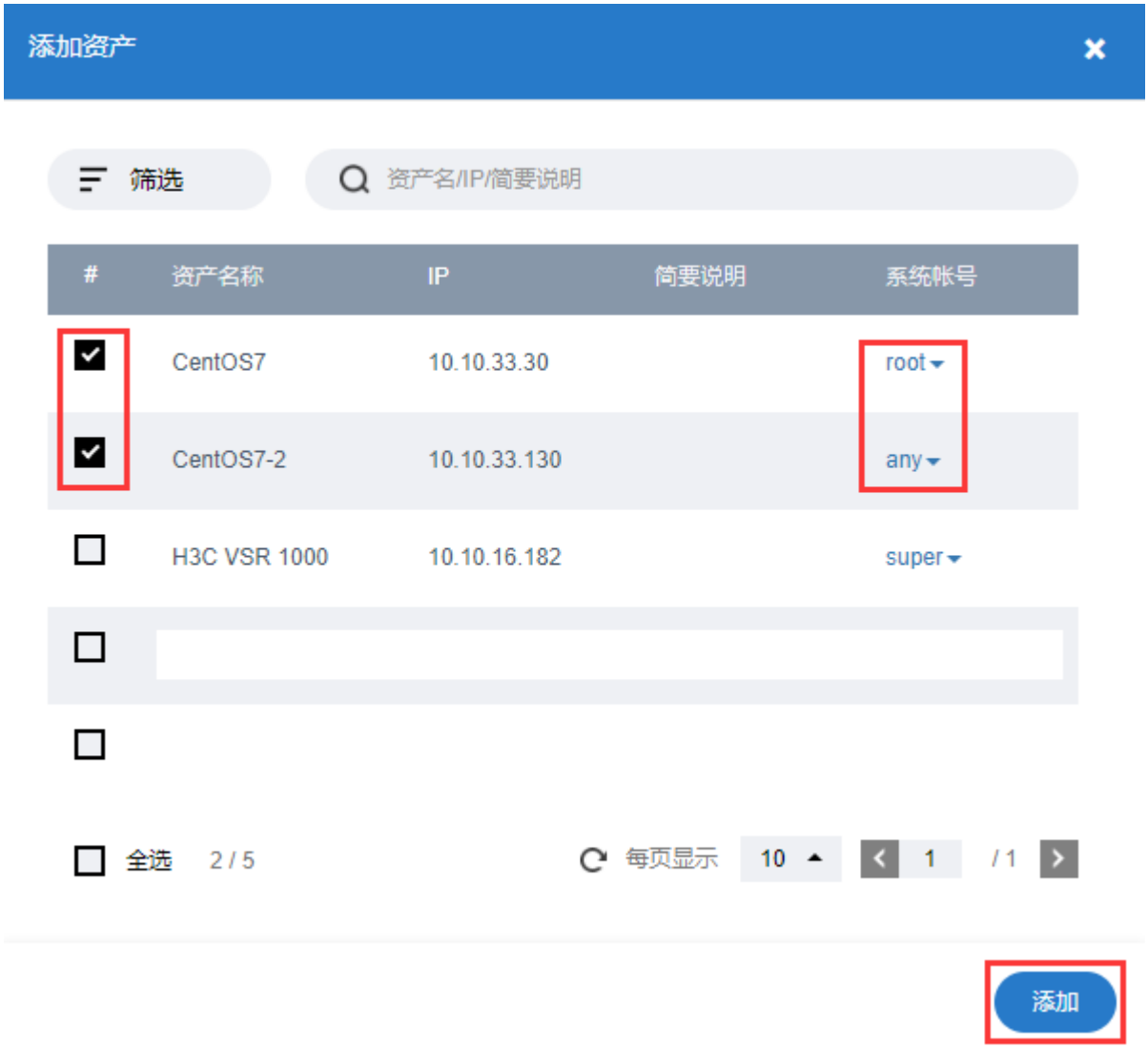
2. 单击**申请资产**对应的，设置各参数。

参数	说明
工单标题	工单的标题。字符串格式，长度范围是1~30个字符。

参数	说明
	工单标题会出现在通知消息标题和通知邮件主题中，建议使用精简的语言把任务描述清楚。
操作类型	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	工单的申请理由。字符串格式，长度范围是0~512个字符。
开始时间/结束时间	权限生效的开始时间和结束时间。开始时间和结束时间的缺省值为： • 开始时间：当前时间点。 • 结束时间：当前时间点+1天。 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。

3. 单击**资产**对应的，选中要添加权限的资产，然后在**系统帐号**中选择帐号，单击**添加**。

   - 一次最多能够选择100个资产，如果要添加权限的资产数大于100，请分批添加。
   - 一个资产一次只能选择一个帐号，如果要申请一个资产的多个帐号的权限，请重复执行本步骤。



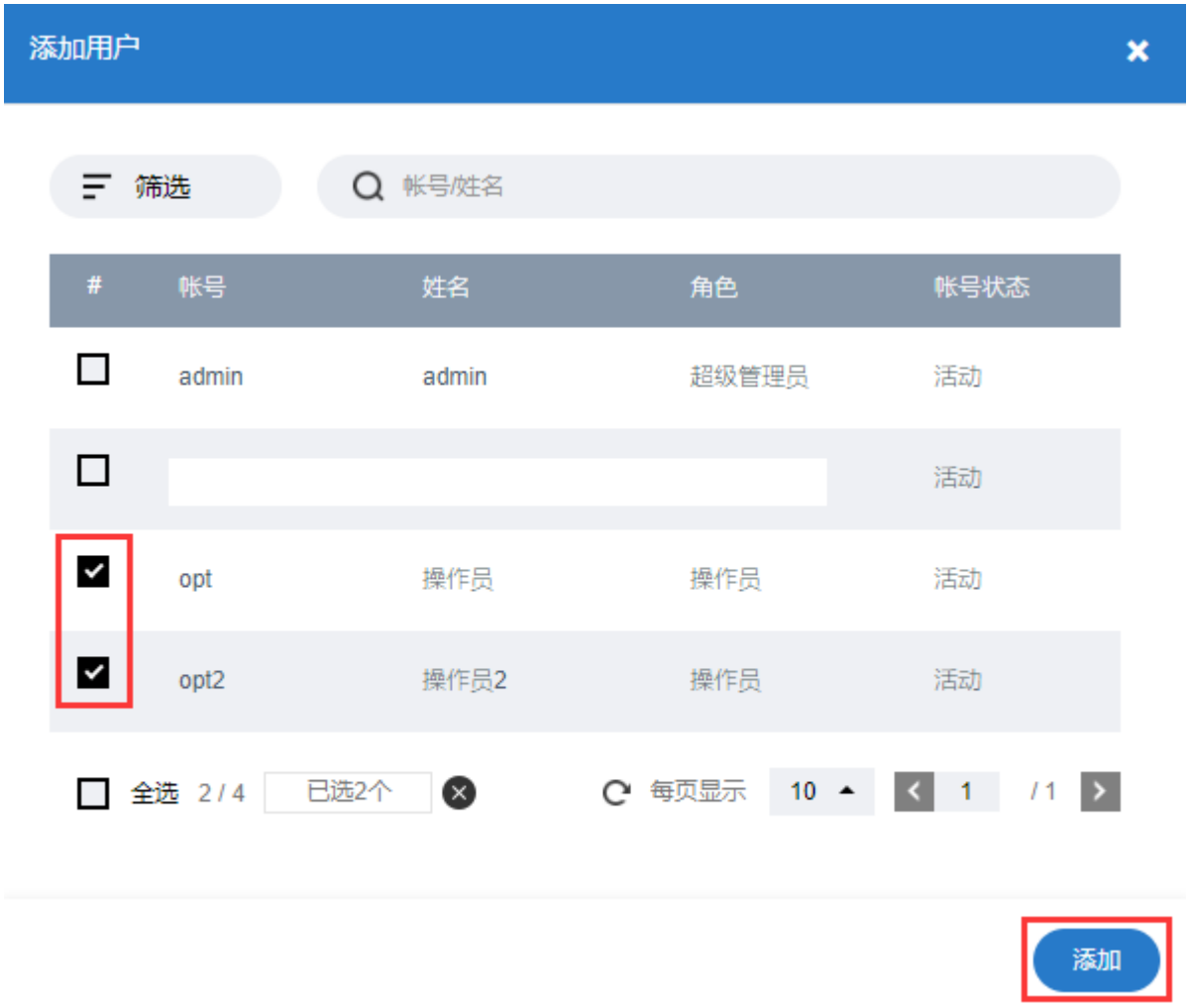
4. 配置访问协议。

   缺省情况下，A2000-E 运维管理系统选中的是**全部协议**。如果需要更精细化的管理，请选中**指定协议**，并配置允许的访问协议，协议包括**SSH**、**Telnet**、**XDMCP**、**VNC**和**XFWD**。

5. 可选： 如果需要在高危命令的配置中，允许工单申请资产的使用人执行某些命令，请填写**放行命令**，多条命令之间用回车分隔。

   说明: 放行命令可以直接填写完整的命令，例如crontab -l，也可以填写命令的正则表达式，例如rm -rf.*。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**，并将有着比高危命令配置更高的优先级。

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**。

说明:

- 如果暂时不提交，请单击**保存为草稿**，下次在**草稿箱**中打开工单继续填写、提交。
- 用户还可以单击**保存为模板**，将当前工单作为模板，后续直接使用模板创建工单，减少相同内容的填写工作量。

8. 可选： 超级管理员如手动指定了审批人，申请人提交后需要在弹出窗口中手动勾选一个或多个审批人。这些审批人将会收到提醒，并由其中任意一个完成审批。

申请人提交工单后，审批人会收到通知消息和通知邮件。审批人单击**批准**后，A2000-E 运维管理系统将用户和所选资产、帐号关联。

执行结束后，A2000-E 运维管理系统发送通知消息和通知邮件给申请人。在工单中配置的开始时间和结束时间范围内，使用人能够使用指定的帐号和协议访问指定的资产。结束时间到了后，访问中的会话会被断开，使用人在能访问的资产列表中也找不到该资产。

完成审批后，最后一层审批人可以对该工单执行撤销操作。撤销后，工单状态显示为已完成，使用人将无法访问该资产。

申请密码

用户可以通过工单来申请资产帐号的密码。

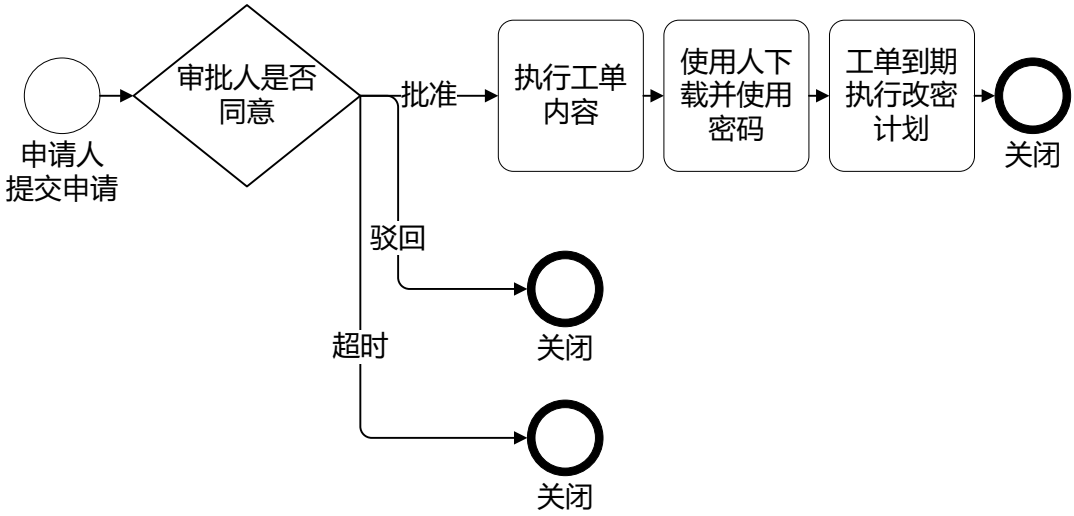


图 2: 密码工单处理流程

1. 选择**工单** > **工单管理** > **新建工单**。

2. 单击**申请密码**对应的，设置各参数。

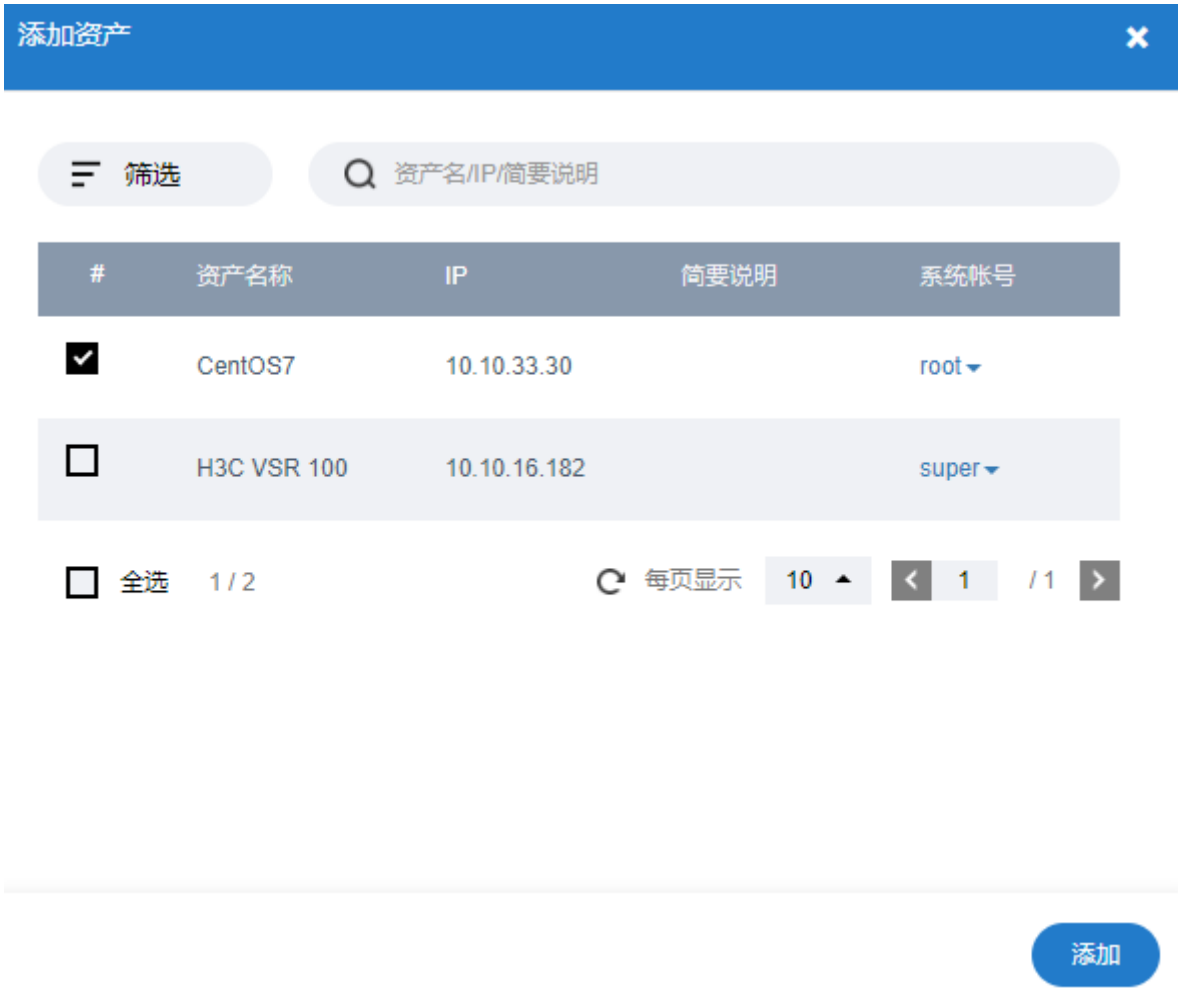
参数	说明
工单标题	工单的标题。字符串格式，长度范围是1~30个字符。

参数	说明
	工单标题会出现在通知消息标题和通知邮件主题中，建议使用精简的语言把任务描述清楚。
开始时间/结束时间	使用密码的开始时间和结束时间。开始时间和结束时间的缺省值为： • 开始时间：当前时间点。 • 结束时间：当前时间点+1天。 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。

3. 单击**资产**对应的，选中要申请密码的资产，然后在**系统帐号**中选择帐号，单击**添加**。

说明:

- 一次最多能够选择100个资产，如果要申请密码的资产数大于100，请分批添加。
- 系统帐号中显示资产上的所有帐号，但正在使用中的帐号不能添加。正在使用中的帐号是指其他密码申请工单中已申请的帐号且还在使用时间范围内。
- 一个资产一次只能选择一个帐号，如果要申请一个资产的多个帐号的密码，请重复执行本步骤。



4. 选择密码是否分段。

   - 如果申请人就是密码使用人，请选择**否**。工单审批完成后申请人会收到通知邮件。
   - 如果申请人不是密码使用人，请选择**是**，并设置**前段密码用户**和**后段密码用户**。工单审批完成后，两段密码的用户都会收到通知消息和通知邮件。

5. 单击**提交**。

说明:

- 如果暂时不提交，请单击**保存为草稿**，下次在**草稿箱**中打开工单继续填写、提交。
- 用户还可以单击**保存为模板**，将当前工单作为模板，后续直接使用模板创建工单，减少相同内容的填写工作量。

6. 可选： 超级管理员如手动指定了审批人，申请人提交后需要在弹出窗口中手动勾选一个或多个审批人。这些审批人将会收到提醒，并由其中任意一个完成审批。

- **密码不分段**：

  申请人提交工单后，审批人会收到通知消息和通知邮件。审批人单击**批准**后，A2000-E 运维管理系统发送通知消息和通知邮件给申请人。

  工单中填写的开始时间到期后，申请人在**已办工单**中执行以下操作获取密码。

1. 单击工单对应的**解压密码**，输入登录帐号对应的密码，单击**确定**。用户会获取到解压密码，请牢记该密码。
2. 单击**下载密码**，将压缩的密码文件保存到本地PC，然后解压缩密码文件（需要输入解压密码），用户即可获取指定资产指定帐号的密码（Excel文件）。

- **密码分段**：

  申请人提交工单后，审批人会收到通知消息和通知邮件。审批人单击**批准**后，A2000-E 运维管理系统发送通知消息和通知邮件给前段、后段密码用户。

  两段密码的用户分别在**已办工单**中执行以下操作获取分段密码，最后将两段密码拼接成完整的密码。

1. 单击工单对应的**解压密码**，输入登录帐号对应的密码，单击**确定**。用户会获取到解压密码，请牢记该密码。
2. 单击**下载密码**，将压缩的密码文件保存到本地PC，然后解压缩密码文件（需要输入解压密码），用户即可获取指定资产指定帐号的密码（Excel文件）。

工单结束时间到期后，工单状态变为**已完成**，解压密码入口消失。如果帐号配置了改密计划，A2000-E 运维管理系统对该帐号改密。

审批完成后，最后一层审批人可以对该工单执行撤销操作。撤销后，解压密码入口消失，工单状态显示为已完成，使用人将无法访问该资产。

审批工单

工单的默认审批人是安全保密管理员。仅当超级管理员手动指定了某种类型的工单的审批人名单，且名单中包含操作员时，操作员才能审批工单。

1. 登录A2000-E 运维管理系统的Web客户端后，请单击左上角收到的工单审批的提醒中的**查看详情**。

说明: 也可以直接选择**工单** > **工单管理** > **待办工单**，并单击**详情**查看待审批的工单。

2. 查看工单的具体内容后，如果同意，请单击**批准**，然后单击**确定**；如果不同意，请单击**驳回**，然后填写**拒绝理由**，完成后单击**确定**。

3. 可选： 批准工单后，如果超级管理员设置了多级审批，存在下一级审批人，且下一级审批人为超级管理员指定的审批人时，需要从下一级审批人名单中勾选一个或多个审批人。这些审批人将会收到提示并由其中之一继续完成审批。


添加审批用户
帐号/姓名
#
帐号
姓名
工作邮箱
opt
操作员
opt@test.com
opt2
操作员2
全选 2 / 2
已选2个
每页显示
10
1
/ 1
确定

个人帐号设置

5

目录:

修改个人设置

设置基本信息

基本信息包含个人帐号名称、姓名、手机号码、工作邮箱等。但帐号名称只能查看不能修改。

1. 单击右上角用户帐号（例如**操作员**），选择**帐号设置**。

2. 选择**修改信息** > **个人设置** > **基本信息**。

3. 设置需要修改的参数，完成后单击**确定**。

参数	说明
姓名	用于标识该帐号所属的具体人员的姓名，会显示在右上角。取值范围为1~100长度的字符串，不能为空。

参数	说明
手机号码	标准格式的手机号码。
工作邮箱	在需要发送邮件给用户时，A2000-E 运维管理系统会将相关信息发送到用户设置的该邮箱中。 标准格式的邮箱地址。如不设置，则在需要发送相关信息的目标用户时，无法选中当前用户。

修改密码

仅当用户使用本地密码登录，或使用双因子登录中的第一身份验证方式为本地密码时会显示该页签，并可以在此处修改本地密码。

1. 单击右上角用户帐号（例如**操作员**），选择**帐号设置**。
2. 选择**修改信息** > **个人设置** > **修改密码**。

3. 输入原始密码及新密码，新密码需要连续输入两次。

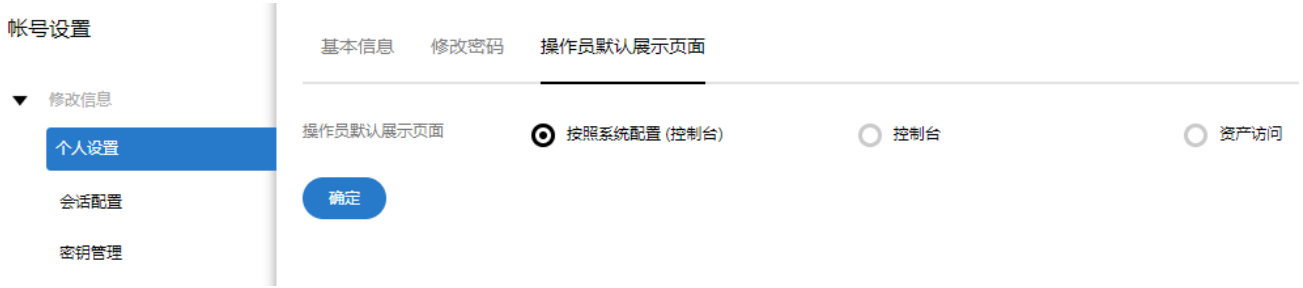
说明: 新密码需要满足系统的密码复杂度策略，密码复杂度策略请将鼠标移动到图标上进行查看。

4. 确认输入无误后，单击**确定**完成密码修改。

设置操作员默认展示页面

用于设置操作员登录到A2000-E 运维管理系统的Web界面之后默认展示的页面。

1. 单击右上角用户帐号（例如**操作员**），选择**帐号设置**。
2. 选择**修改信息** > **个人设置** > **操作员默认展示页面**。



3. 根据需要勾选要展示的页面，并单击**确定**保存。

   - **按照系统配置**：默认选项，展示控制台。
   - **控制台**：默认登录的主界面，会包含工作台中的各个按钮、快速访问资产模块、以及用户自定义添加的其他模块。
   - **资产访问**：登录后直接进入**资产访问**菜单中，从而快速进行操作。

修改会话配置

用于设置用户在访问资产并进行字符和文件传输时的相关参数。

修改字符会话配置

用于设置用户访问资产时建立的字符会话的访问方式及持续时间。

1. 单击右上角用户帐号（例如**操作员**），选择**帐号设置**。
2. 选择**修改信息** > **会话配置** > **字符会话**。

3. 设置需要修改的参数，完成后单击**确定**。

参数	说明
最大持续时间	用于设置字符会话的最大持续时间，取值包括： • 使用全局设置：默认选项，由超级管理员在系统设置中配置。具体设置值请询问超级管理员。 • 自定义：按照“天/时/分”设置会话最大持续时间。达到最大持续时间后会话将被切断。单击上下箭头按钮设置时间时最小单位为15分钟，手动输入时最小单位为1分钟，不能设置为0天0小时0分钟。
直连分类方式	用户使用SSH直连方式访问时资产的分类方式，取值包括： • 无：表示使用管理员配置的全局设置。 • 资产组 • 资产类型

参数	说明
	• 责任人

修改文件传输配置

对于麒麟操作系统，仅支持通过网盘传输文件，不支持通过SFTP客户端传输文件。因此，在**修改信息** > **会话配置** > **文件传输**页面的设置均不生效。

配置密钥

用于当用户通过SSH客户端登录A2000-E 运维管理系统时，使用此处配置的密钥对应的私钥进行验证，从而不输入密码登录到A2000-E 运维管理系统的字符交互终端。

1. 在终端使用命令行生成密钥对。密钥类型为RSA，密钥长度为512、1024或2048。

   a) 鼠标右击，选择**在终端中打开**。

   b) 输入ssh-keygen，并按回车。

   ```
   ssh-keygen
   Generating public/private rsa key pair.
   ```

   c) 根据提示输入密钥对的存储位置，不输入表示存储在默认的文件夹中。

   ```
   ssh-keygen
   Generating public/private rsa key pair.
   Enter file in which to save the key (/home/kylin/.ssh/id_rsa):
   ```

   d) 根据提示输入认证密码。

   ```
   ssh-keygen
   Generating public/private rsa key pair.
   Enter file in which to save the key (/home/kylin/.ssh/id_rsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   ```

   当屏幕回显以下信息时，表示秘钥对已经生成。

   ```
   ssh-keygen
   Generating public/private rsa key pair.
   Enter file in which to save the key (/home/kylin/.ssh/id_rsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /root/.ssh/id_rsa.
   Your public key has been saved in /root/.ssh/id_rsa.pub.
   The key fingerprint is:
   e0:52:44:f6:7f:0b:d5:28:f3:ff:15:2c:70:ec:8d:6e root@localhost.localdomain
   The key's randomart image is:
   +--[ RSA 2048]----+
   |    .+           |
   |    o .   .o     |
   |     o . o.oo.   |
   |    o . . =+ +   |
   |   . . S o o+ + |
   |    .    o.o. .|
   |         .E. .|
   |          .  ..|
   ```

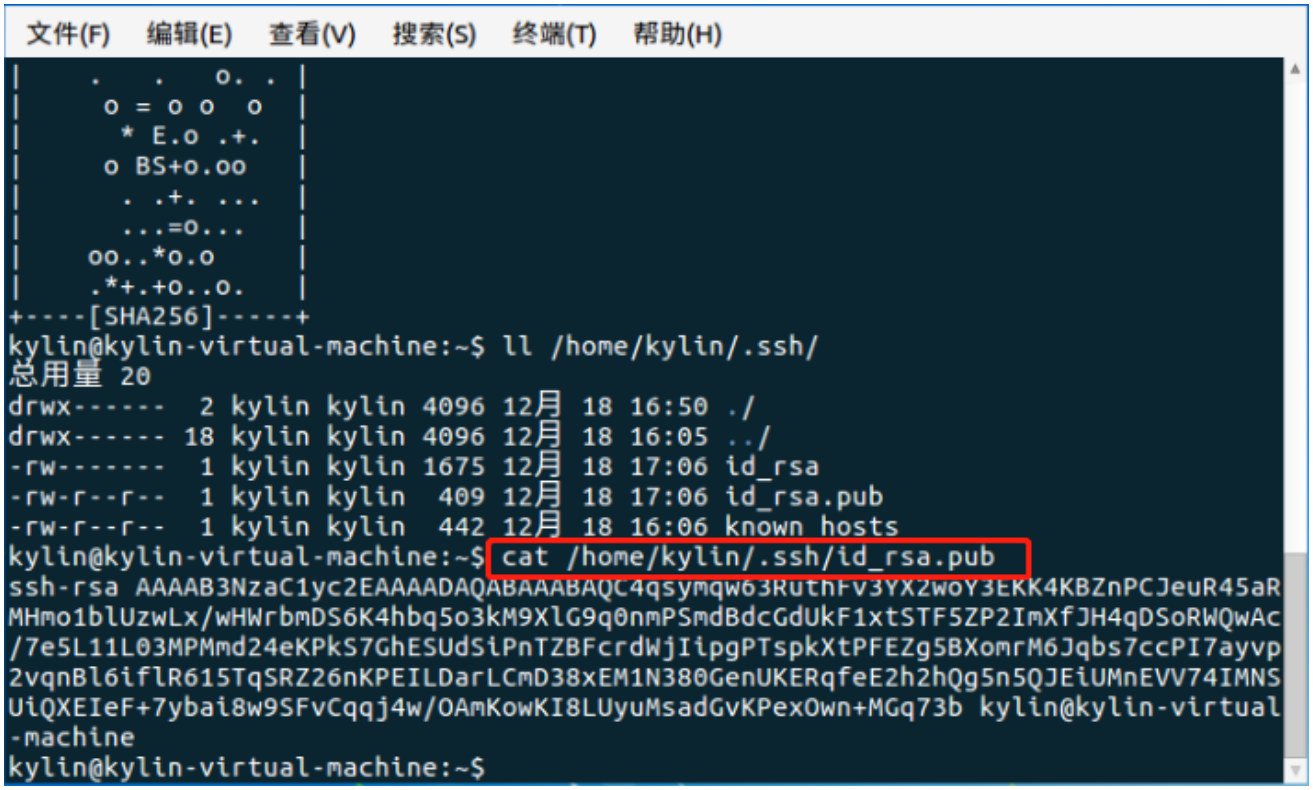
```
|         .|
+-----------------+
```

e) 输入ll /home/kylin/.ssh/，查看已生成的密钥对。

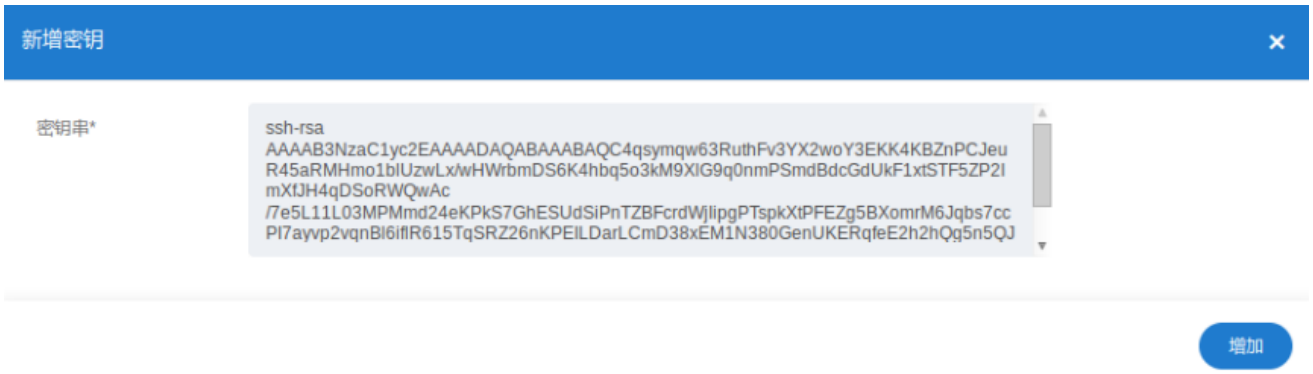
```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
Your identification has been saved in /home/kylin/.ssh/id_rsa.
Your public key has been saved in /home/kylin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:xz74vxRZRnFVgOnnopiZm4taLi931JEoTmeGjfBnQzs kylin@kylin-virtual-machine
The key's randomart image is:
+---[RSA 2048]----+
|             o+o*|
|    .   .   o. . |
|     o = o o  o  |
|      * E.o .+.  |
|     o BS+o.oo   |
|      . .+. ...  |
|      ...=o...   |
|    oo..*o.o     |
|    .*+.+o..o.   |
+----[SHA256]-----+
kylin@kylin-virtual-machine:~$ ll /home/kylin/.ssh/
总用量 20
drwx------  2 kylin kylin 4096 12月 18 16:50 ./
drwx------ 18 kylin kylin 4096 12月 18 16:05 ../
-rw-------  1 kylin kylin 1675 12月 18 17:06 id_rsa
-rw-r--r--  1 kylin kylin  409 12月 18 17:06 id_rsa.pub
-rw-r--r--  1 kylin kylin  442 12月 18 16:06 known_hosts
kylin@kylin-virtual-machine:~$
```

2. 通过Web界面登录A2000-E 运维管理系统。
3. 单击右上角用户帐号（例如**操作员**），选择**帐号设置**。
4. 选择**修改信息** > **密钥管理**。

5. 单击**新建**。
6. 输入**cat /home/kylin/.ssh/id_rsa.pub**，查看生成的密钥对的公钥信息。



7. 将公钥文件中的密钥串，粘贴至Web界面的**密钥串**框体中，并单击**增加**。



已完成新增密钥。

完成新增密钥后，当前用户通过字符终端工具登录A2000-E 运维管理系统的SSH交互终端时，可以通过已生成的私钥进行验证，参见通过SSH客户端登录A2000-E 运维管理系统。用户可以添加多个密钥。请用户妥善保管自己的私钥，并且对于不用的密钥，及时在**密钥管理**中禁用或删除。

附录 6

目录:

使用双因子认证

用户如使用双因子认证，在输入密码时，请参考本节指导完成输入。

Web界面、SSH交互终端均支持使用双因子认证。

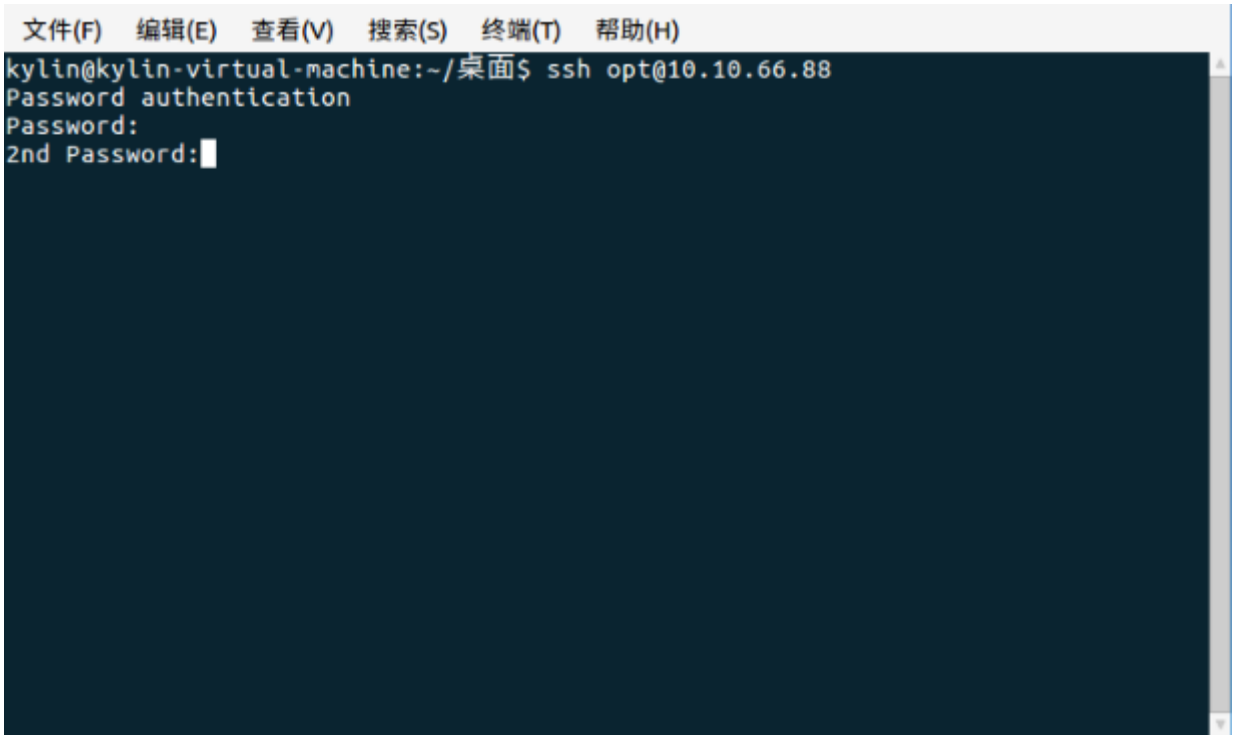
双因子认证有以下两种输入方式，请用户根据自己的实际情况进行选择。

分两次输入密码（推荐）

在密码输入框中输入第一重认证的密码，第一重认证通过后，在两步认证窗口中继续输入第二重认证的密码，并提交，进行第二重认证。

- **Web界面**的两步认证界面如下：

- **SSH交互终端**的两步认证界面如下，请在**2nd Password：**提示符后继续输入第二重认证的密码，并按回车。



使用组合密码

组合密码允许用户在同一密码输入框内直接输入第一重密码和第二重密码的组合，从而直接完成登录认证。

当使用SSH客户端时，如双因子认证的两种认证方式全都为静态密码时，可以保存会话，并将密码保存为组合密码，从而简化登录。其他情况下，不建议使用该密码输入方式。

组合密码的输入方式有以下两种。以第一重密码为abcdef，第二重密码为123456为例：

输入格式	说明	举例
第一重密码+空格+第二重密码	推荐使用该方式。	abcdef 123456
第一重密码+第二重密码	仅当第二重认证的密码为6位数字时，可使用该方式。	abcdef123456