

UNIS A2000-E运维管理系统 操作员手册（For Windows）

Copyright © 2021 紫光恒越技术有限公司及其许可者版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。本文档中的信息可能变动，恕不另行通知。

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

关于本文档.....	ii
第 1 章 快速开始.....	1
第 2 章 登录和访问.....	4
通过Web方式访问.....	4
通过Web界面登录A2000-E 运维管理系统.....	4
安装AccessClient.....	7
访问资产.....	7
通过SSH方式访问.....	11
通过SSH客户端登录A2000-E 运维管理系统.....	12
访问资产.....	17
第 3 章 高危操作.....	20
执行高危操作.....	20
执行高危操作（普通方式）.....	21
执行高危操作（操作员自行复核）.....	23
复核会话.....	24
复核命令.....	25
在Web界面复核命令.....	25
在会话窗口复核命令.....	26
第 4 章 文件传输.....	28
网盘传输.....	28
上传文件.....	28
下载文件.....	33
管理文件.....	34
SFTP工具传输.....	36
在Web界面中启动SFTP会话.....	36
通过SFTP工具直连目标资产.....	38
SFTP命令传输.....	39
ZMODEM传输.....	40
第 5 章 工单.....	41
申请资产.....	43
申请密码.....	49
审批工单.....	54
第 6 章 个人帐号设置.....	57
修改个人设置.....	57
设置基本信息.....	57
修改密码.....	58
设置操作员默认展示页面.....	58
修改会话配置.....	59
修改字符会话配置.....	59
修改文件传输配置.....	60
配置密钥.....	61
第 7 章 附录.....	63

使用双因子认证.....	63
共享会话.....	64
发起共享.....	65
加入共享.....	66

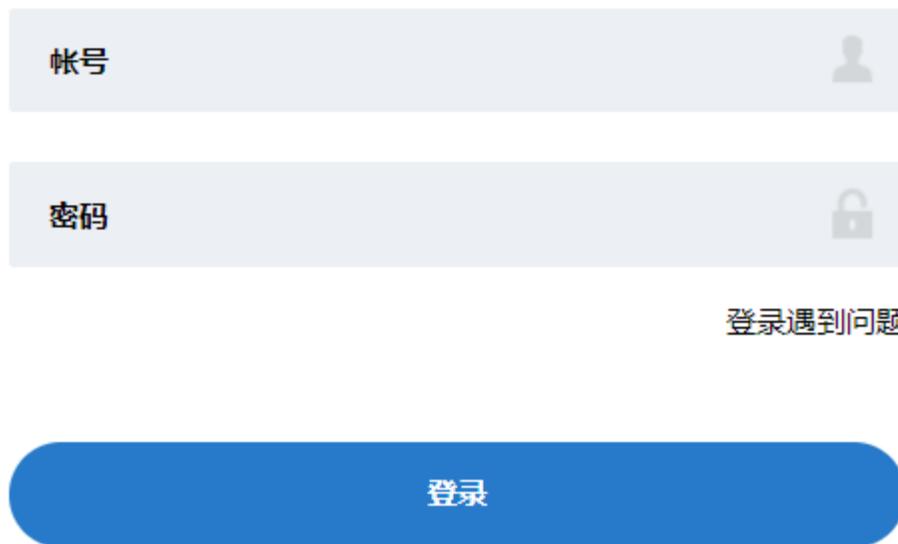
操作员可以通过本节内容快速了解在A2000-E 运维管理系统上的基本操作。如操作过程中遇到问题，或涉及较复杂的登录/认证过程或其他进阶操作，请查阅后续章节中的详细指导。

本节以使用浏览器登录到A2000-E 运维管理系统的Web界面并访问一个Linux资产为例，指导操作员快速完成在A2000-E 运维管理系统上的操作。

1. 在浏览器地址栏中输入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。

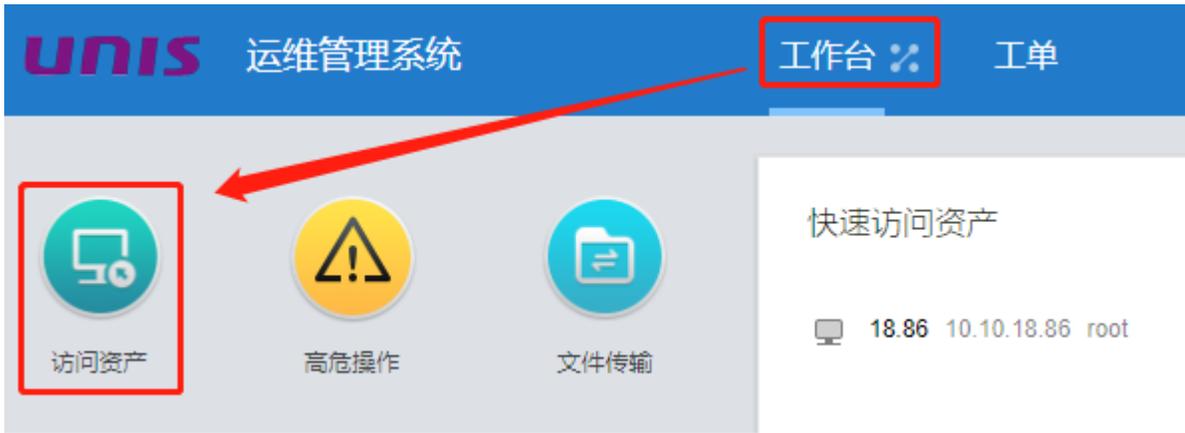
 **说明:** 如出现安全提示，请选择继续前往或添加例外。

2. 输入帐号和密码，单击**登录**。



The screenshot displays a login interface with two input fields: '帐号' (Account) and '密码' (Password). To the right of the password field is a link labeled '登录遇到问题' (Login problem). Below these elements is a large, rounded blue button with the text '登录' (Login).

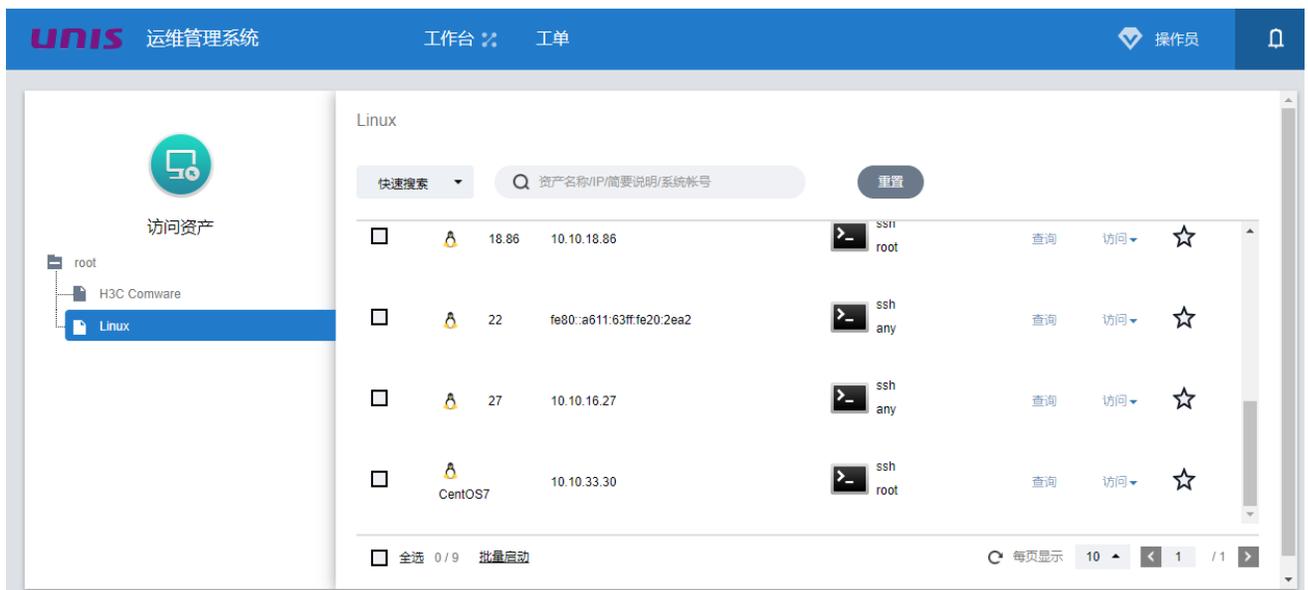
3. 选择**工作台 > 访问资产**，进入资产访问界面。



4. 根据提示单击**下载**并安装AccessClient。如已安装了AccessClient，仍然收到提示，请单击**已安装**进行忽略。



5. 在左侧导航栏中，选择动态视图中的具体节点，例如选择Linux。选择节点后可以在右侧查看该节点下的资产。



6. 单击**访问**，设置使用的**系统帐号**，例如选择已托管密码的root帐号，并单击**启动**。

快速搜索 重置

<input type="checkbox"/>		22	fe80::a611:63ff:fe20:2ea2	ssh any	查询	访问 ▾	☆
<input type="checkbox"/>		27	10.10.16.27	ssh any	查询	访问 ▾	☆
<input type="checkbox"/>		CentOS7	10.10.33.30	ssh root	查询	访问 ▾	☆

ssh xdmcp sftp

系统帐号*

收藏 启动

登录和访问

目录:

- [通过Web方式访问](#)
- [通过SSH方式访问](#)

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。用户可以通过Web方式完成操作员的所有日常操作。本文档主要介绍用户在Web界面上的操作。

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	Windows 7及以上的非服务器版本。
浏览器	<ul style="list-style-type: none">• 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• 密信浏览器。建议更新到最新版本
显示器分辨率	建议最小为1280*1080（系统的缩放设置为100%时）。  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IE11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IE浏览器请单击**详细信息 > 转到此网页（不推荐）**）。

此站点不安全

这可能意味着，有人正在尝试欺骗你或窃取你发送到服务器的任何信息。你应该立即关闭此站点。

 [关闭此标签页](#)

 [详细信息](#)

**你的电脑不信任此网站的安全证书。
该网站的安全证书中的主机名与你正在尝试访问的网站不同。**

错误代码: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

 [转到此网页\(不推荐\)](#)

2. 输入帐号和密码，单击**登录**。

帐号 

密码 

[登录遇到问题](#)

登录

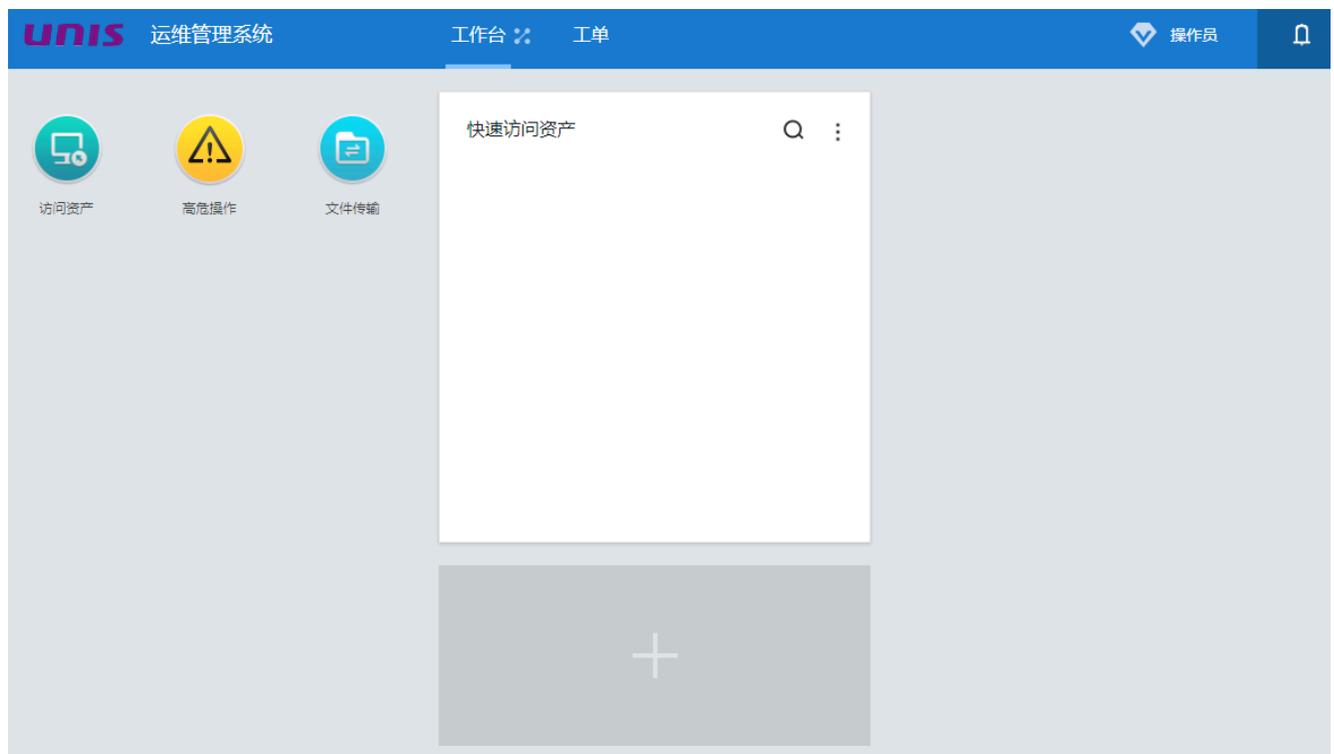


说明:

- 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。



安装AccessClient

在使用A2000-E 运维管理系统访问资产时，除了通过Web方式建立图形会话，其他场景下A2000-E 运维管理系统都会通过AccessClient打开客户端并建立会话。

如本地PC未安装AccessClient，进入**访问资产**菜单后，浏览器上方也会提示安装AccessClient，请根据该提示单击**下载**并安装AccessClient。如已安装了AccessClient，仍然收到提示，请单击**已安装**进行忽略。



访问资产

A2000-E 运维管理系统支持访问的资产包含主机、网络设备。

通过Web界面访问主机/网络设备时，如建立字符会话，需要在本地PC上安装字符客户端，使用的字符客户端类型在**修改字符会话配置**中设置。

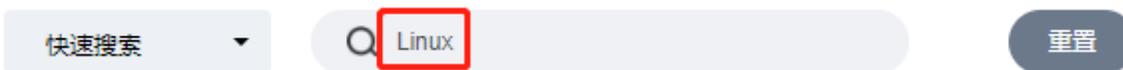
Web界面对字符客户端的要求如下：

表 3: A2000-E 运维管理系统的Web界面支持的字符客户端

访问资产类型	要求
Linux、网络设备	<ul style="list-style-type: none">Putty0.58及以上Xshell4.0及以上 <p> 说明: AccessClient自带Putty。</p>

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**。



最近访问 收藏 会话共享

#	资产名称	资产IP	简要说明	快捷登录	在线会话	登录选项	收藏
<input type="checkbox"/>		18.86	10.10.18.86	ssh root	查询	访问	☆

- 在最近访问中查找：单击访问资产后，选择最近访问页签。



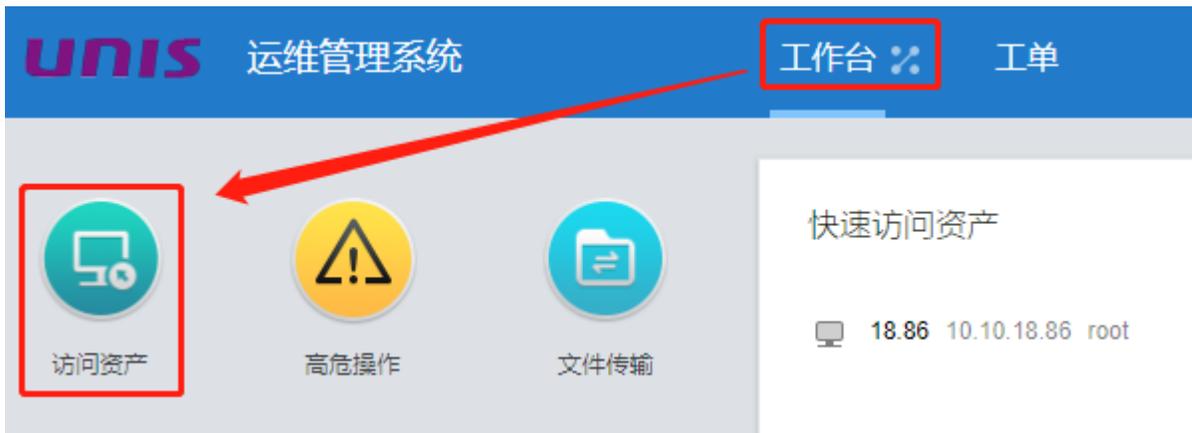
- 收藏并查找：对资产单击☆收藏后，单击访问资产并选择最近访问页签，查看收藏。



查找到资产并启动访问后，A2000-E 运维管理系统将启动对应的客户端并建立字符。会话的全局设置请参考[修改会话配置](#)进行修改。

本节以Linux主机为例，指导完成资产访问。但将对所有资产涉及的参数进行说明。

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



3. 单击访问并设置启动参数。

Linux



表 4: 配置会话参数

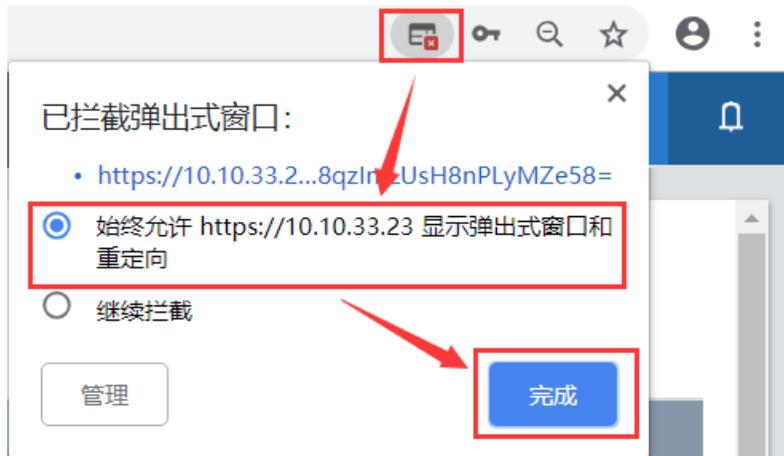
参数	说明
系统帐号	<p>除了VNC登录之外的其他登录方式都需要配置。用于标识登录对应资产时所使用的帐号。有以下几种类型：</p> <ul style="list-style-type: none">• self: 同用户帐号。使用和当前登录A2000-E 运维管理系统的帐号同名的帐号登录资产，请操作员自行确保该帐号在待访问资产上存在。• any: 登录时提供。A2000-E 运维管理系统仅连接到资产的登录界面，不自动输入帐号名称和密码，由访问者手动填写。• A2000-E 运维管理系统上已添加的资产帐号名称，例如root，A2000-E 运维管理系统使用该帐号登录到资产设备。 <p> 说明:</p> <ul style="list-style-type: none">• 帐号名称之前有*，表示该帐号的密码已在A2000-E 运维管理系统上托管，A2000-E 运维管理系统连接该资产时将直接代填密码并登录。• 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。

4. 确认配置无误后，单击**启动**建立远程会话并打开。



说明:

- 当使用Telnet/SSH/SFTP访问资产时，A2000-E 运维管理系统如找不到对应类型的客户端，将弹出窗口，请在该窗口中选择本地PC上安装的Telnet/SSH/SFTP客户端并启动会话。客户端类型请参考[修改字符会话配置](#)进行设置。
- 当使用VNC连接或使用其他Web方式的访问时，将会打开新的网页窗口。请允许该弹出窗口，以下为Chrome浏览器中的操作：



- 使用VNC连接，启动后需要继续输入在待访问资产的VNC server上设置的VNC远程连接的密码。如配置资产时已托管了VNC密码，直接勾选**使用已设置密码**，并单击启动。



- 使用XFWD连接，如初始登录到xterm字符终端，请输入待启动的图形/字符工具的路径，如/usr/bin/xfce4-session或/usr/bin/xfce4-terminal，打开图形或字符会话。

```
sh-4.2# /usr/bin/xfce4-session
```

- 如管理员设置了启动会话时必须或可填备注，请输入备注后并单击**启动**。备注是一个1~100长度的字符串。
- 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](#)。
- 建立会话后，可将会话共享给其他用户，请参考[共享会话](#)。

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：

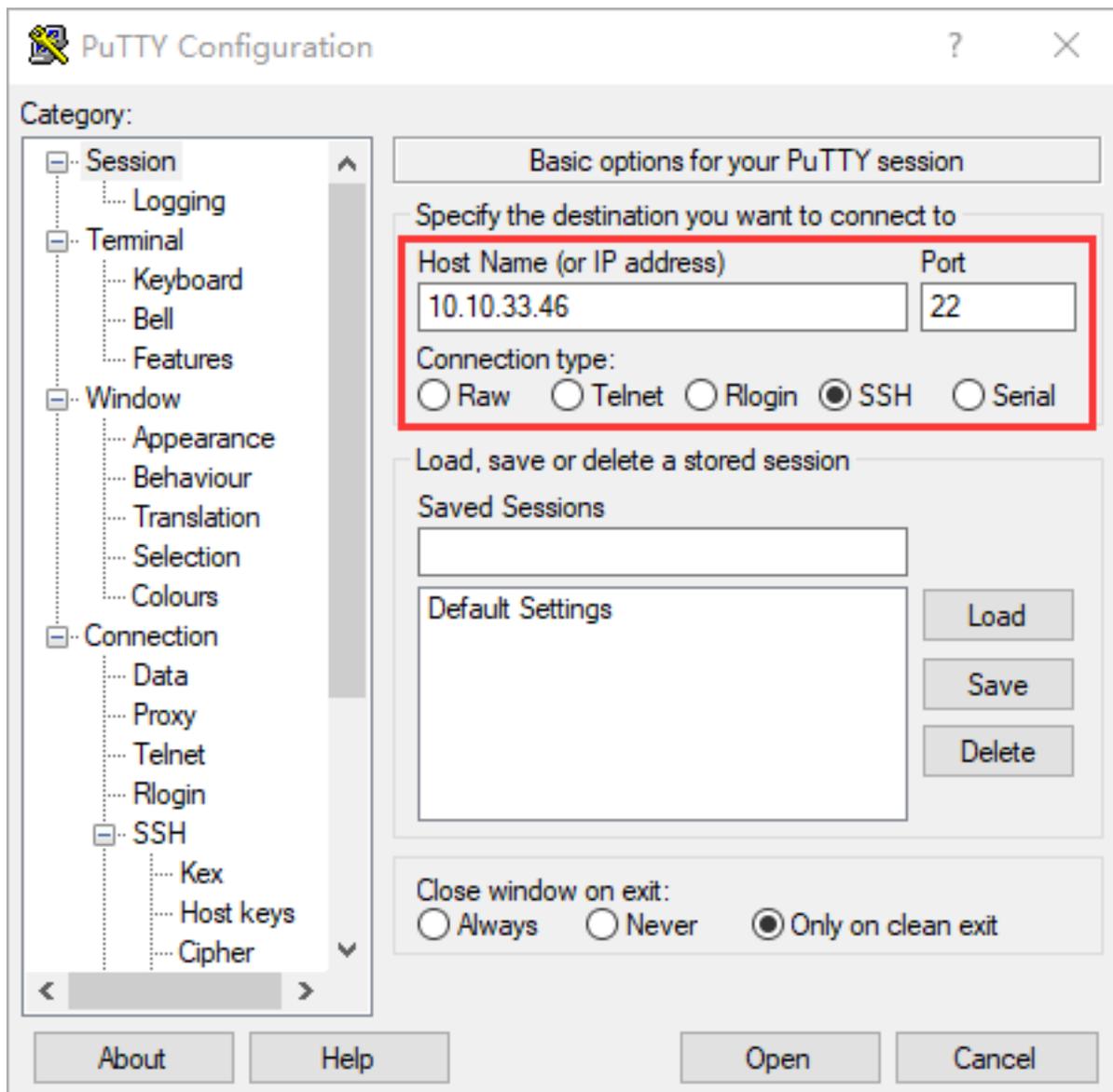
表 5: 通过SSH客户端登录A2000-E 运维管理系统的环境要求

项目	要求
操作系统	Windows 7及以上的非服务器版本。
SSH客户端	已安装了以下客户端软件之一： <ul style="list-style-type: none">• Xshell4.0及以上• Putty0.58及以上

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。

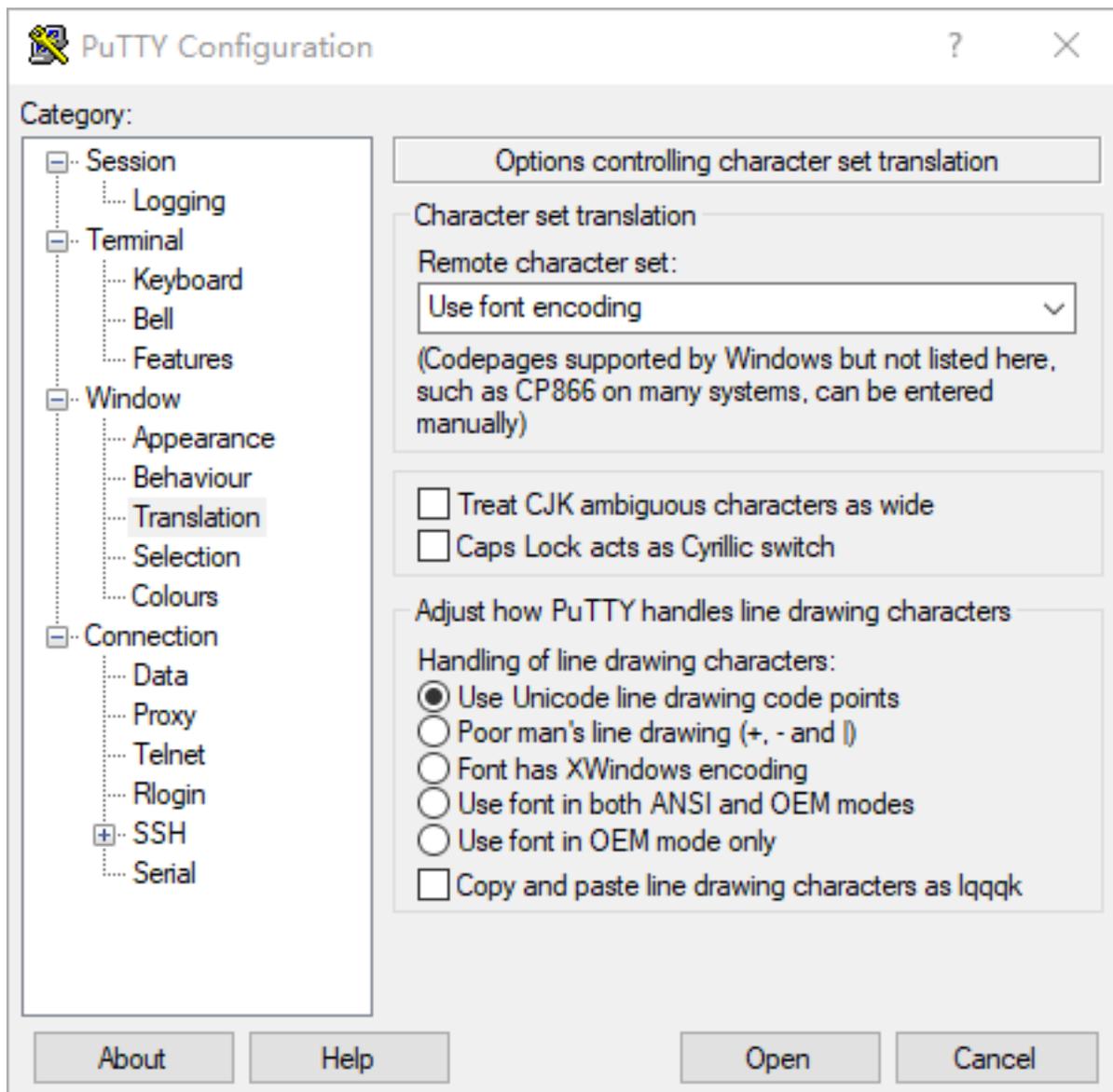
本节以Putty为例，指导完成登录A2000-E 运维管理系统。

1. 打开Putty工具。
2. 在Putty Configuration菜单中，左侧导航选择Session，设置以下参数。
 - **Host Name:** 主机名，A2000-E 运维管理系统的IP或者域名。
 - **Port:** 端口号，22。
 - **Connection Type:** 连接方式，选择SSH。



3. 可选：在左侧导航选择**Window > Translation**，设置终端的编码格式，和A2000-E 运维管理系统保持一致。A2000-E 运维管理系统交互终端编码类型默认为GB18030，如被管理员修改，请咨询管理员。如编码类型不一致，登录后会显示为乱码。

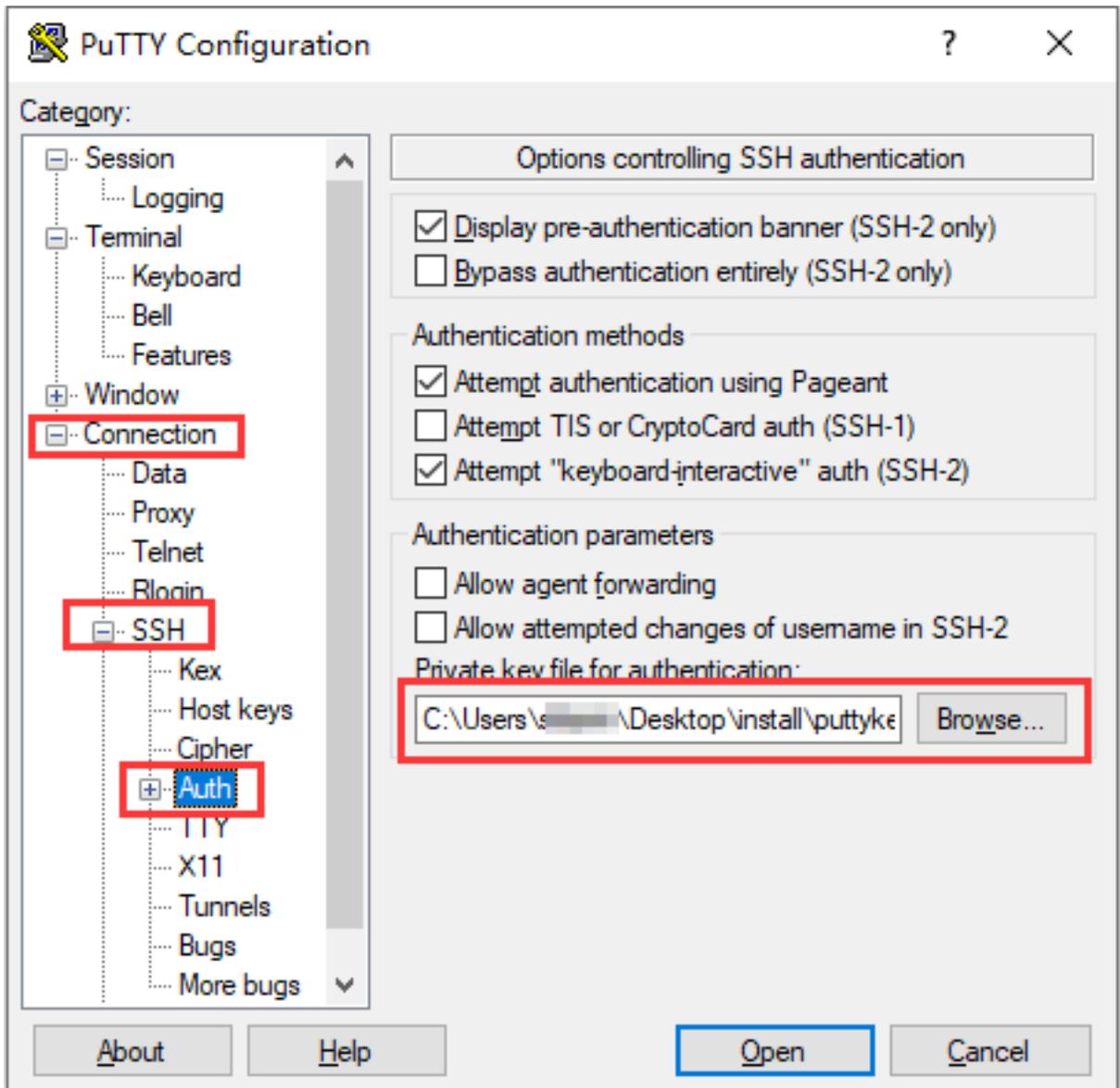
 **说明：** Putty默认的编码类型中没有GB18030，设置为**Use font encoding**即可。



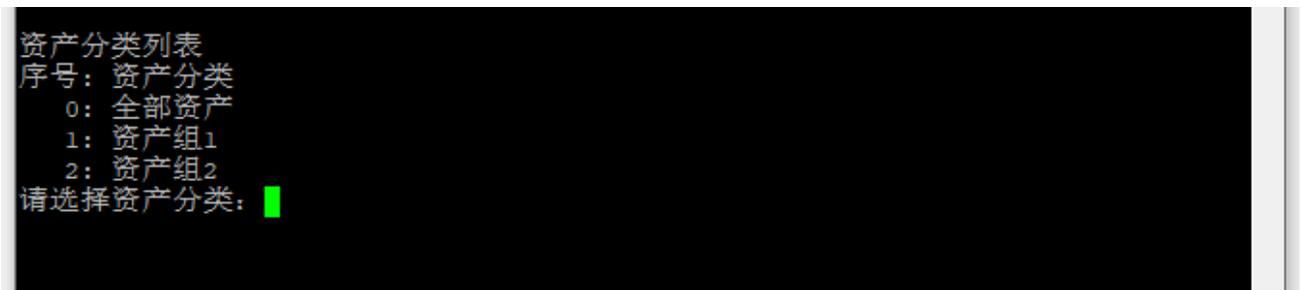
4. 可选：如使用密钥登录，设置用于登录的密钥。

 **说明：**登录前需要先完成配置密钥。对于Putty，只支持ppk格式的密钥，需要使用puttygen工具将用户的私钥转换为ppk格式。

在左侧导航选择**Connection > SSH > Auth**，单击**Browse**，设置用于登录的ppk密钥。



5. 设置完成后，单击下方的**Open**，打开连接。



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 6: SSH交互终端常用操作

使用场景	输入	说明
最外层资产分类列表菜单	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
	/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 资产分类列表菜单
	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

6. 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。

7. 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   CentOS7
  2: 10.10.33.130 CentOS7-2
请选择目标资产: 1
```

8. 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 > CentOS7(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
```

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。用户也可以通过该方法将连接保存到本地，从而快速访问。
- 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须填或可填备注，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

该方式即穿透访问，直接通过A2000-E 运维管理系统连接到目标资产。

如需配置密钥或终端编码，请参考[登录到A2000-E 运维管理系统后查找并访问资产](#)完成配置。

1. 打开SSH客户端工具。

本节以Putty为例指导完成访问资产。

2. 单击Open连接后，输入以下用户名和密码，直接连接到资产。

参数	说明
用户名	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
密码	用户在A2000-E 运维管理系统中的密码。  说明: 如已配置了密钥，将无需输入密码，直接连接到资产。



说明:

- 当使用IPv6地址时，部分客户端支持IPv6地址加中括号，但几乎所有客户端都支持地址不加中括号，因此建议A2000-E 运维管理系统地址和目标资产地址全都不加中括号，例如ssh opt/fc00::1010:32::30/root@fc00::1010:32::1。另外，当目标资产地址为IPv6时，无法在Windows环境下Xshell的命令中使用ssh命令直连访问。
- 如管理员设置了启动会话时必须或可填备注，请输入备注后按回车。

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

目录:

- [执行高危操作](#)
- [复核会话](#)
- [复核命令](#)

管理员如果配置了会话复核或高危命令规则，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。

A2000-E 运维管理系统中的高危操作，包括会话复核和高危命令两部分：

- 会话复核：对会话进行审核授权和监控，执行的动作为允许操作和禁止操作。
- 高危命令：对字符会话执行的命令进行限制和监控，执行的动作为允许、复核、拒绝、切断、通知。

执行高危操作

当管理员配置了高危操作时，特定操作用户如访问特定的资产时，会要求会话复核；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。

操作员在进行资产访问和执行命令时都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。

触发高危操作后的示例如下：

- 触发会话复核：

资产名	CentOS7
帐号	root
备注	请输入... ?
复核人	opt2

启动

- 触发高危命令：

```
[root@localhost ~]# touch test
[root@localhost ~]# rm -rf test
[TERM] This command requires manager's confirmation, are you sure?[Y/n]
[TERM] Waiting for confirmation, press Ctrl-C to cancel.
```

执行高危操作（普通方式）

操作员在执行访问资产及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
通过Web界面建立会话，单击启动后出现 启动资产 窗口，包含 复核人 下拉菜单。	操作员触发了会话复核规则，需要完成会话复核后才能进行操作。	<ol style="list-style-type: none"> 选择复核人并启动会话。 <ul style="list-style-type: none"> Web界面：在复核人下拉菜单中选择一个复核人，并单击启动。 SSH界面：输入复核人对应的编号并按回车启动会话。 启动会话后，操作员无法执行任何操作。请联系选择的复核人完成复核会话，完成复核后操作员可以进行操作。 <p> 说明：会话复核过程中，复核人将观看操作员的所有操作，并可以随时锁定用户的操作。被锁定后请联系复核人进行解锁。</p>
通过SSH客户端建立会话，选择资产和帐号名称后，提示 请选择会话复核用户 。		

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。	<p>1. 确认是否要执行该命令。</p> <ul style="list-style-type: none"> 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。 <p>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。</p> <p> 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。</p> <p>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。</p>
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
在Web界面单击启动会话时，提示 操作失败 。	可能原因：会话复核规则中设置的所有复核人均不可用。	联系管理员检查会话复核规则是否存在问题。
在SSH客户端上启动会话时，提示 Not authorized to login to server 'XX' with account 'YY' 。		
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。

执行高危操作（操作员自行复核）

复核人为使用动态令牌登录，或使用的双因子认证中包含动态令牌的用户时，如复核人暂时无法进行复核，经协商一致，操作员可以向复核人直接获取复核人的PIN2码及动态令牌的动态密码，并由操作员自己进行会话复核。

1. 操作员使用自己的帐号访问资产。
2. 操作员通过Web或SSH访问资产，触发会话复核，选择复核人为使用动态令牌登录的用户。

```
Connecting to root@Linux-01(10.10.33.30) ...
请选择会话复核用户：
 1: admin
 2: opt2
请选择： 2
Last login: Mon Mar 30 14:47:42 2018 from 10.2.234.3
[root@centos ~]# █
```

3. 单击右上角的提醒图标，查看收到的待复核会话的提醒，并单击查看详情，跳转到复核申请列表页面。



4. 单击复核打开对应的会话复核。

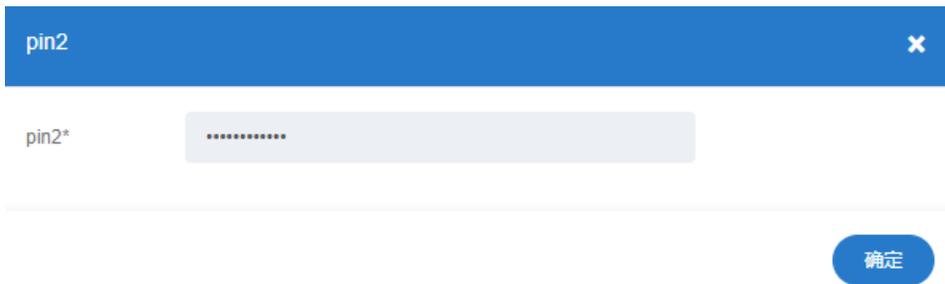
待我复核

申请时间	复核类型	复核内容	操作用户	资产	帐号	操作
2019-03-07 18:56:00	会话复核	字符会话	opt	CentOS7	root	复核

合计：1

5. 在弹出的对话框中，输入密码并单击确定。

密码前半段是从复核人获取的“PIN2码”，后半段是从复核人获取的动态令牌生成的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。



6. 参考[复核会话](#)完成会话复核。

复核会话

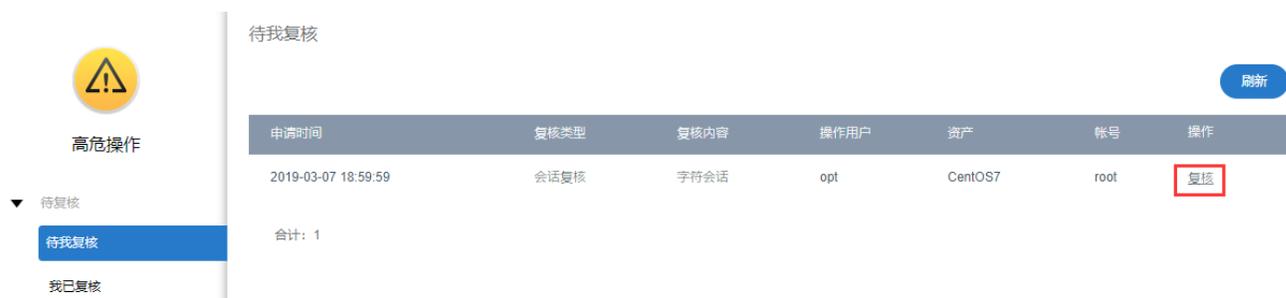
如管理员配置了会话复核规则中，当前用户被设置为复核人之一，则其他用户进行资产访问触发会话复核规则时，可以指定当前用户作为本次会话的复核人。复核人完成会话复核，访问资产的用户才能在建立的会话中进行操作。

需要复核的会话，当操作用户建立会话之后不能执行任何操作，必须等复核人进行确认后才能执行操作。复核人将继续观看用户的所有操作，并在用户将要进行危险操作时及时锁定会话。

1. 使用复核人帐号[访问资产](#)。
2. 单击右上角的  提醒图标，查看收到的待复核会话的提醒，并单击[查看详情](#)，跳转到复核申请列表页面。



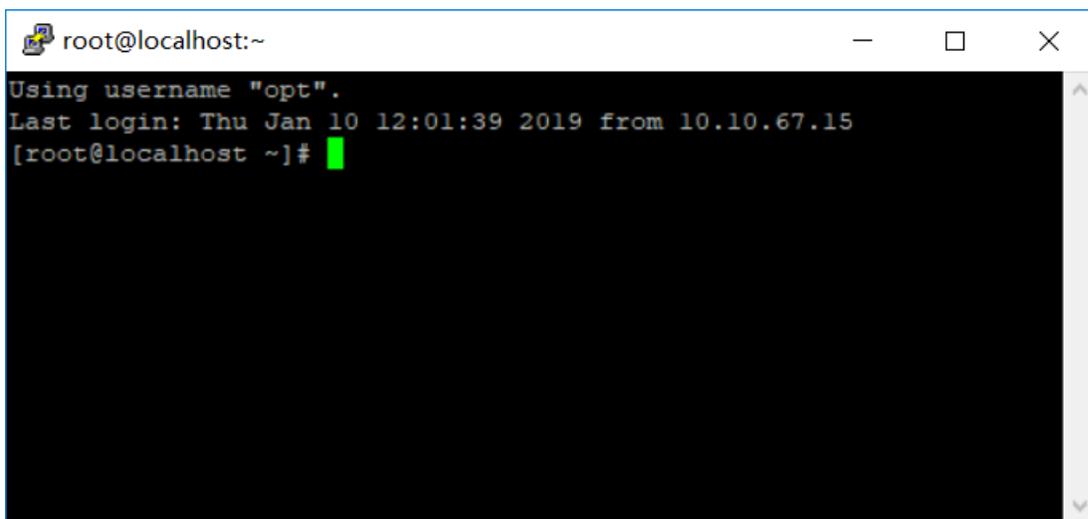
3. 查看收到的复核申请，对于**复核类型为会话复核**的复核申请，单击**复核**，打开对应的会话。



复核使用的客户端与复核人在**帐号设置 > 会话配置**中设置的会话访问方式无关。对于字符会话，默认使用Putty打开会话复核窗口；对于图形会话，默认使用web方法打开会话复核窗口。会话打开后，复核人将看到和操作人一样的操作界面，但不能进行任何输入。

4. 确认该会话合法后，请复核人执行解锁操作允许操作用户进行操作。

- 字符会话：按**空格**或**回车**，解锁或锁定操作用户的操作。
- 图形会话：单击窗口右上角的**continue**按钮，解锁操作；单击**pause**，锁定操作。



5. 当复核人发现操作用户将要进行危险操作时，请执行锁定操作，使操作用户无法继续执行任何操作。

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。

复核人收到提醒并完成复核的情况有以下两种：

- **Web界面复核**：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。
- **会话窗口复核**：当某个会话的会话复核人同时也是该会话的命令复核人之一时，该复核人可以在打开的会话复核窗口中直接收到操作用户发出的复核申请：**Confirmation: Are you allowed to execute this command? [Y/n]**。复核人可以在会话窗口中完成该命令的复核。

在Web界面复核命令

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。



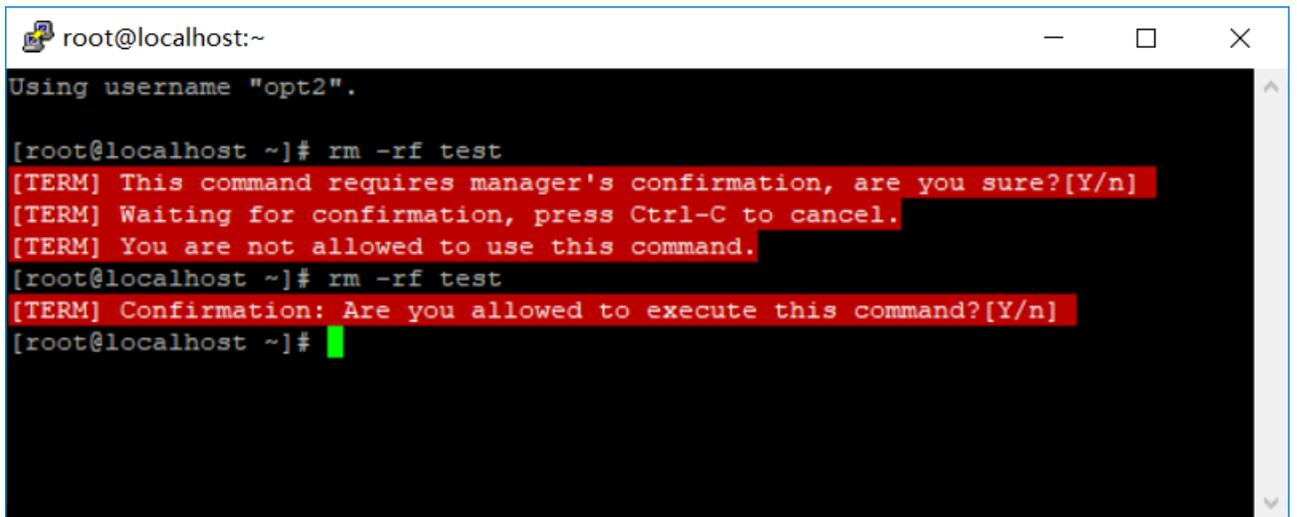
3. 查看收到的复核申请，确认命令是否可以执行。

- 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。



在会话窗口复核命令

1. 用户作为会话复核人，在**复核会话**窗口中复核字符会话。
2. 操作用户发出复核申请后，复核人查看会话窗口中收到的**Confirmation**信息及其具体执行的命令。
3. 确认命令是否可以执行。
 - 是，按**Y**键（忽略大小写），表示允许执行，该命令将直接执行并显示回显。
 - 否，按**N**键（忽略大小写），表示拒绝执行，该命令的执行将被阻断。



```
root@localhost:~  
Using username "opt2".  
[root@localhost ~]# rm -rf test  
[TERM] This command requires manager's confirmation, are you sure?[Y/n]  
[TERM] Waiting for confirmation, press Ctrl-C to cancel.  
[TERM] You are not allowed to use this command.  
[root@localhost ~]# rm -rf test  
[TERM] Confirmation: Are you allowed to execute this command?[Y/n]  
[root@localhost ~]#
```

完成该条命令的复核后，复核人可以在复核窗口中继续对操作人进行会话复核，并在操作人再次触发命令复核时完成复核。

文件传输

目录:

- [网盘传输](#)
- [SFTP工具传输](#)
- [SFTP命令传输](#)
- [ZMODEM传输](#)

介绍如何在本地PC与Linux资产之间传输文件。

下表列出了A2000-E 运维管理系统支持的向Linux资产传输文件的所有方式及相互之间的比较，请用户根据自己的实际情况及喜好，灵活选用文件传输方式：

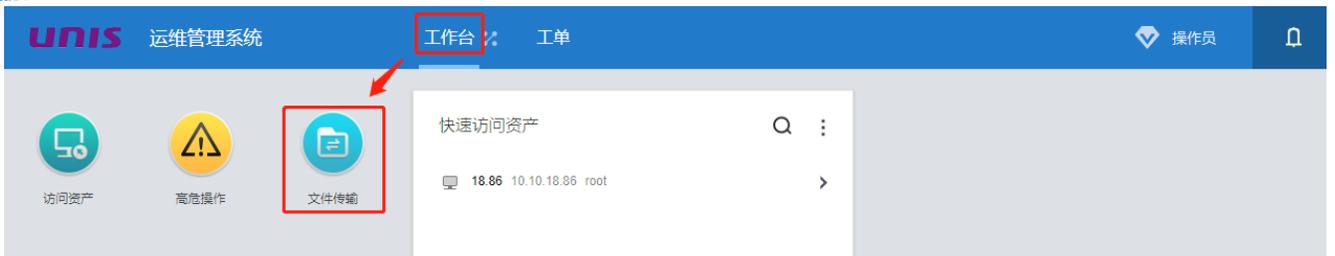
表 7: 不同文件传输方式的比较

传输方式	依赖软件	推荐程度
网盘传输	无	首选
SFTP工具传输	本地PC: SFTP工具 (FileZilla或WinSCP之一)	推荐
SFTP命令传输	需要安装字符终端工具, 如Xshell	本地PC为Linux/Unix时推荐
ZMODEM传输	<ul style="list-style-type: none"> • 目标资产: 已安装lrzsz • 需要安装字符终端工具, 如Xshell, 不支持Putty 	小文件时推荐。不能传输超过2GB的文件

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。

文件传输



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。



拖拽文件上传 或 点击上传

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。

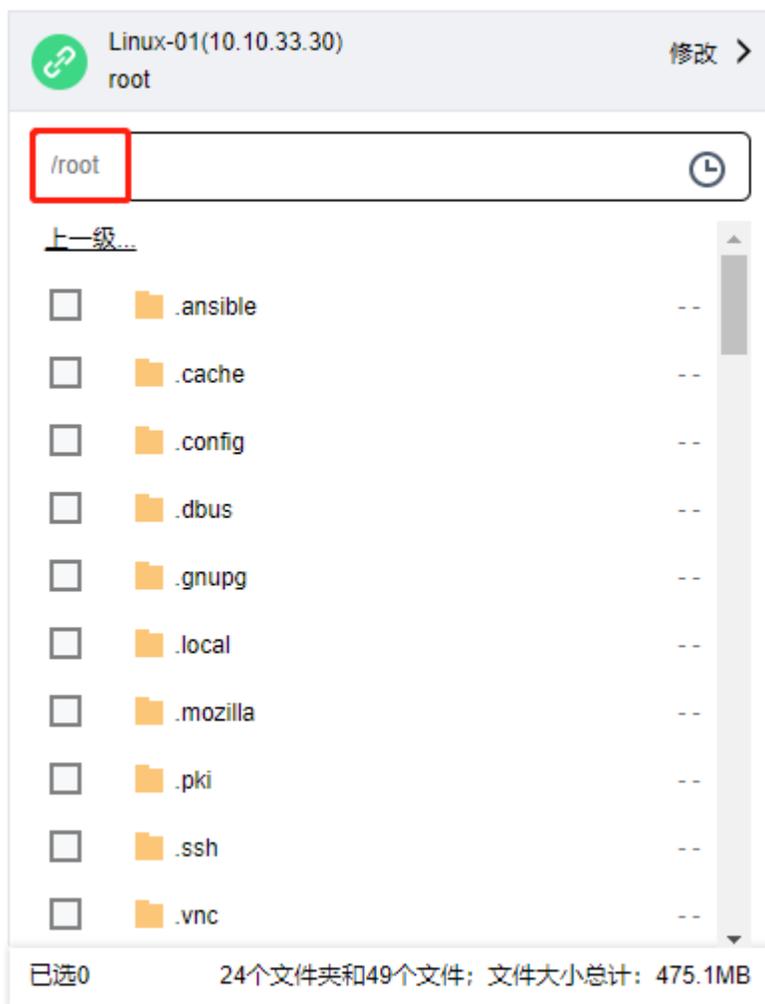
筛选

#	资产名	IP	系统帐号
<input checked="" type="checkbox"/>	CentOS7	10.10.33.30	root
<input checked="" type="checkbox"/>	CentOS7-2	10.10.33.130	root

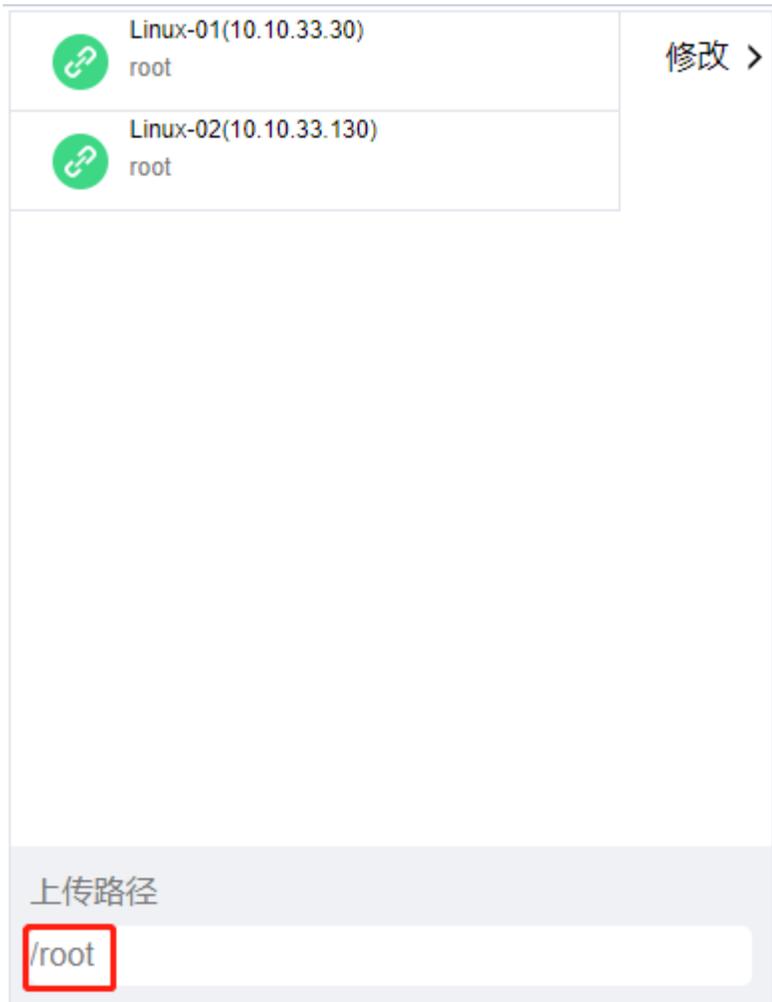
全选 2 / 2 每页 / 1

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。



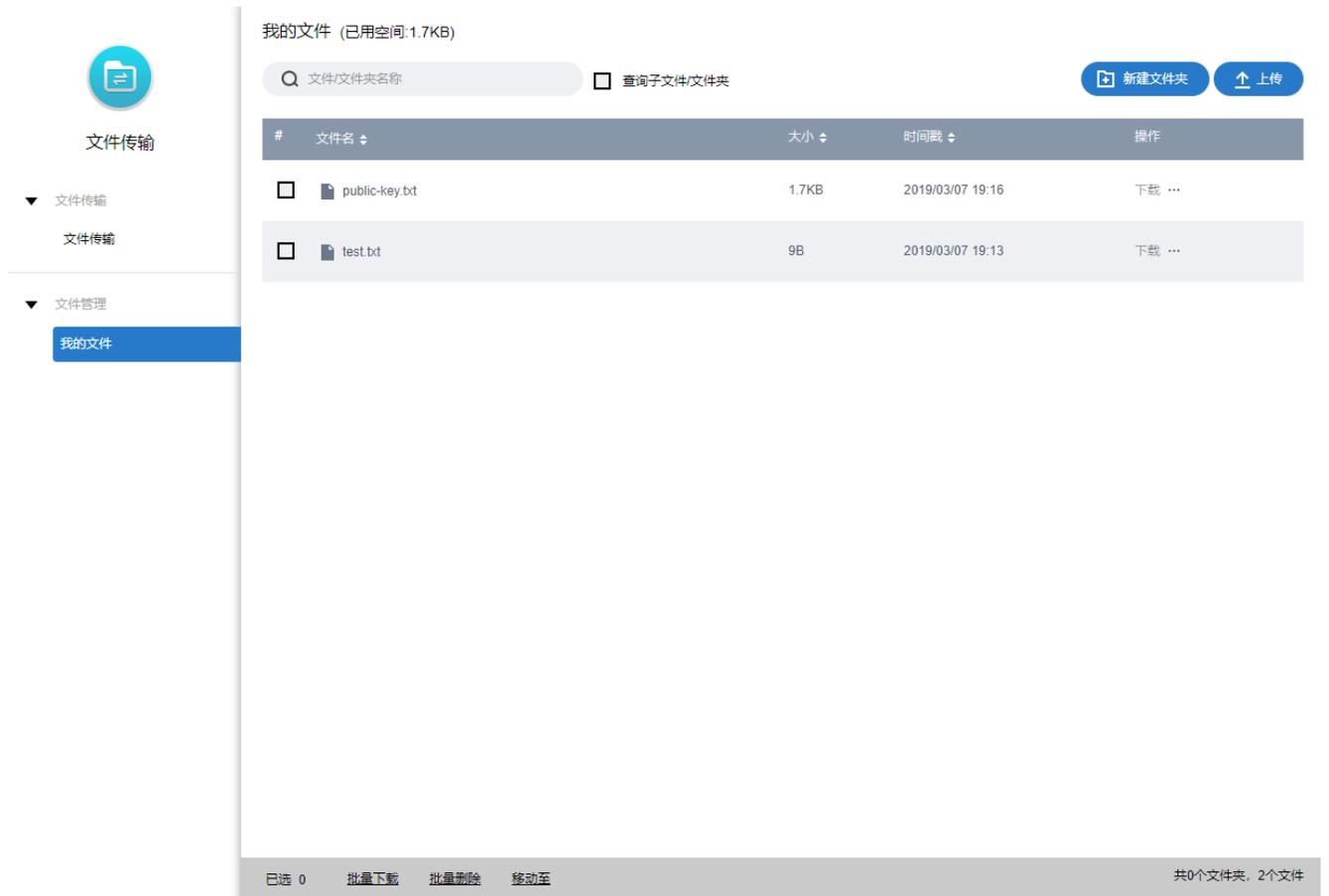
4. 下载到网盘完成后，勾选文件，并单击**批量下载到本地**，将文件从网盘下载到本地。

文件传输



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 Q 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： <ol style="list-style-type: none"> 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。

SFTP工具传输

A2000-E 运维管理系统支持使用SFTP工具，建立本地PC和目标资产之间的SFTP会话，从而完成与目标资产间的文件传输。

使用SFTP工具传输文件，有两种方法：

- 在Web界面中启动SFTP会话：支持Filezilla或WinSCP。
- 通过SFTP工具直连目标资产：支持Filezilla、WinSCP或其他可用的SFTP工具。必须提前获取了目标资产的IP地址和登录帐号名称。

本文以Filezilla为例进行介绍。

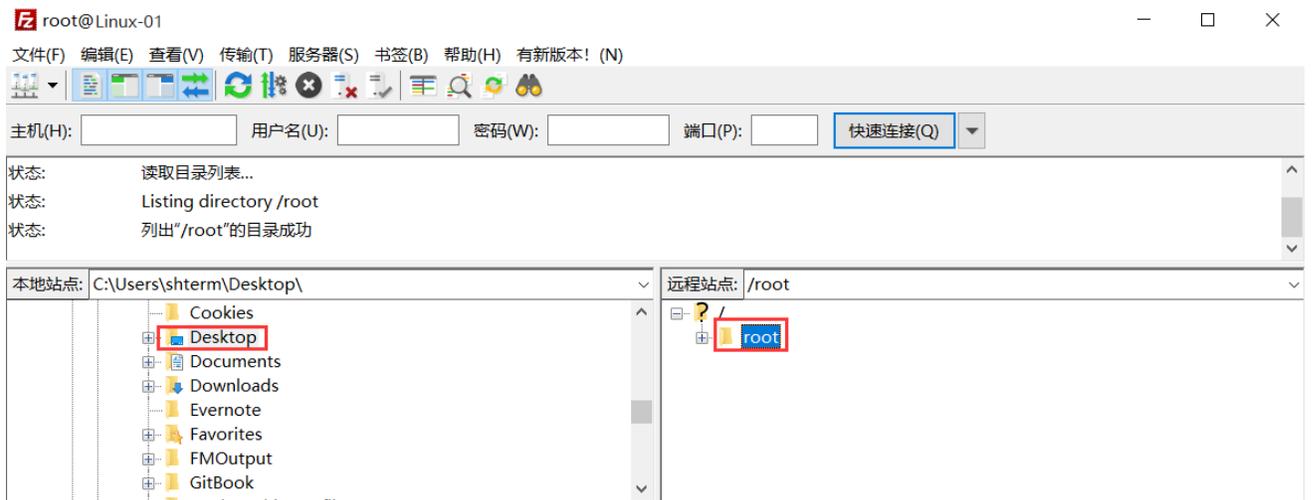
在Web界面中启动SFTP会话

1. 参考[访问资产](#)，建立到目标资产的访问协议为SFTP的会话。



 **说明:** 建立SFTP会话时, 如需要使用未托管密码的帐号, 请选择**any**。

2. 弹出工具窗口后, 在左侧进入下载目标路径或在右侧进入上传目标路径。



3. 上传或下载文件。

以上传文件为例, 在左侧选中待上传的文件后, 单击**上传**。



 **说明:** 单个文件大小如超过文件传输权限中规定的单个文件大小限制，传输会出错，请取消传输或联系安全保密管理员调整权限。

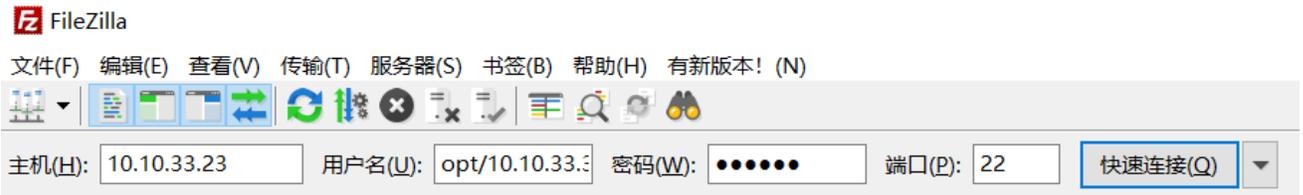
通过SFTP工具直连目标资产

1. 打开SFTP工具，如Filezilla。
2. 在上方输入会话参数，并单击**快速连接**。
 - 主机：A2000-E 运维管理系统的IP地址。
 - 端口号：22
 - 用户名：按照以下格式输入：**A2000-E 运维管理系统上的用户名/目标资产的IP地址/目标资产上的帐号名**。
 - 密码：A2000-E 运维管理系统登录用户名对应的密码

 **说明:** 例如，A2000-E 运维管理系统的IP为10.10.33.23，用户名为opt，目标主机的IP为10.10.33.30，可以访问的帐号为root，已在A2000-E 运维管理系统上托管了密码。则输入的主机名为10.10.33.23，输入的用户名为opt/10.10.33.30/root。

 **说明:** 对于IPv6地址，填写如下：

- 当主机名（A2000-E 运维管理系统地址）使用IPv6地址时，FileZilla中填写主机名必须加中括号，例如[fc00:1010:32::10]，WinSCP可以加中括号也可以不加中括号。
- 当用户名中的目标资产地址使用IPv6地址时，统一不加中括号，例如admin/fc00:1010:32::30/root。



3. 连接成功后，在左侧进入下载目标路径或在右侧进入上传目标路径。
4. 上传或下载文件。

SFTP命令传输

当本地PC为Linux/Unix时，用户可以在命令行中使用sftp命令传输文件。Windows中需要安装能够使用sftp命令的客户端，例如Xshell。

1. 在命令行中，输入sftp命令连接到目标资产。

```
sftp A2000-E  
运维管理系统上的用户名/目标资产的IP地址/目标资产上的帐号@A2000-E  
运维管理系统的IP地址
```

- 说明:** 例如，A2000-E 运维管理系统的IP为10.10.33.23，用户名为opt，目标主机的IP为10.10.33.30，可以访问的帐号为root，已在A2000-E 运维管理系统上托管了密码。则输入sftp opt/10.10.33.30/root@10.10.33.23。
- 说明:** 对于IPv6地址，主机名使用IPv6地址时必须加中括号，目标资产使用IPv6地址时必须不加中括号，例如sftp admin/fc00:1010:32::30/root@[fc00:1010:32::1]。

2. 输入A2000-E 运维管理系统登录用户名对应的密码。

A2000-E 运维管理系统和目标资产的用户名密码均验证通过后，本地PC到目标主机之间的SFTP字符会话建立成功。

```
[root@localhost ~]# sftp opt/10.10.33.30/root@10.10.33.23  
The authenticity of host '10.10.33.23 (10.10.33.23)' can't be established.  
RSA key fingerprint is SHA256:T06laIbrjBa0G0wRaR5IE+VZES5sXb2WvbkhEm0D1ZI.  
RSA key fingerprint is MD5:1d:b7:a1:d1:84:53:3a:d8:78:46:dc:18:83:0c:8a:82.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.10.33.23' (RSA) to the list of known hosts.  
Password authentication  
Password:  
Connected to 10.10.33.23.  
sftp>
```

3. 使用get下载文件或使用put命令上传文件。

```
get 待下载文件的源路径 (远端) 待下载文件的目标路径 (本地)  
put 待上传文件的源路径 (本地) 待上传文件的目标路径 (远端)
```

```
sftp> get /root/test.txt /root
Fetching /root/test.txt to /root/test.txt
/root/test.txt          100% 129    12.1KB/s   00:00
sftp> put /root/abc /root
Uploading /root/abc to /root/abc
/root/abc              100%  0     0.0KB/s   00:00
```

ZMODEM传输

用户可以在建立到资产的字符会话后，使用rz和sz命令上传/下载文件。

ZMODEM是一种使用字符会话传输文件的协议，支持在字符终端上使用rz、sz命令。使用rz、sz命令，需要在服务端上安装lrzsz包，该包是一个第三方软件包，请自行下载。例如，银河麒麟系统可以通过apt install lrzsz命令直接下载并安装。

请使用Xshell等支持ZMODEM的字符终端工具。Putty不支持 ZMODEM传输。

1. [访问资产](#)或[访问资产](#)，建立字符会话。

2. 上传文件到资产。

a) 进入待上传文件的目录，执行rz命令。

```
cd 待上传文件的目录
rz
```

b) 在弹出的对话框中，选中本地待上传的文件，并单击**打开**。

进度条达到100%后，完成文件的上传。

3. 下载文件到本地。

a) 进入待下载文件所在的目录，执行sz命令。

```
cd 待下载文件所在的目录
sz 待下载文件的文件名
```

b) 在弹出的对话框中，选中文件下载的目标路径，并单击**确定**。

进度条达到100%后，完成文件的下载。

目录:

- [申请资产](#)
- [申请密码](#)
- [审批工单](#)

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 8: [工单申请人、使用人和审批人的要求](#)所示。

表 8: 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。

申请时间	工单类型	工单标题	申请人	工单状态	停留时间	操作
2019-03-08 10:21:02	申请资产	1	opt	进行中	1小时前	详情
2019-03-07 19:33:25	申请密码	密码申请	opt	进行中	16小时前	详情 解压缩码 下载密码

合计: 2

每页显示 10 / 1

申请资产

用户可以通过工单来申请资产的访问权限。

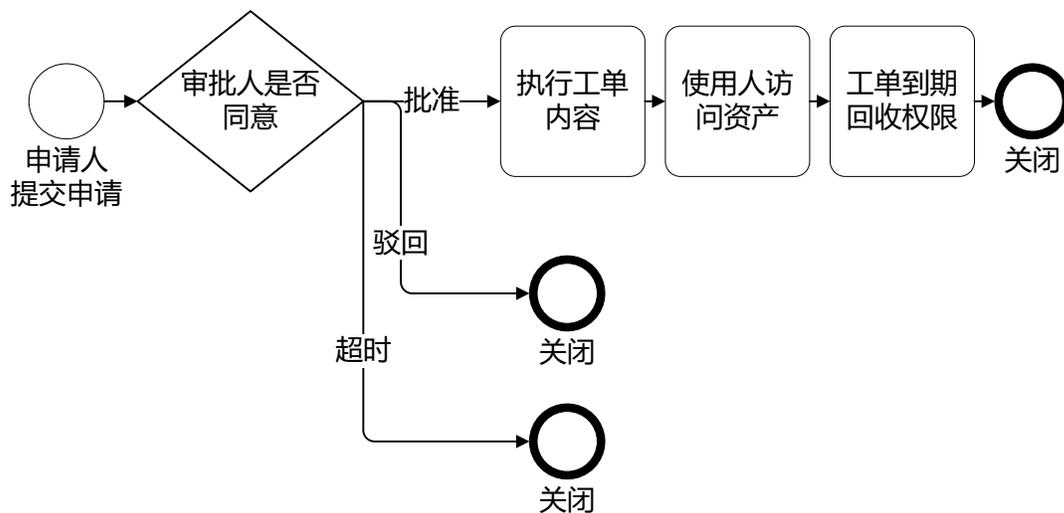
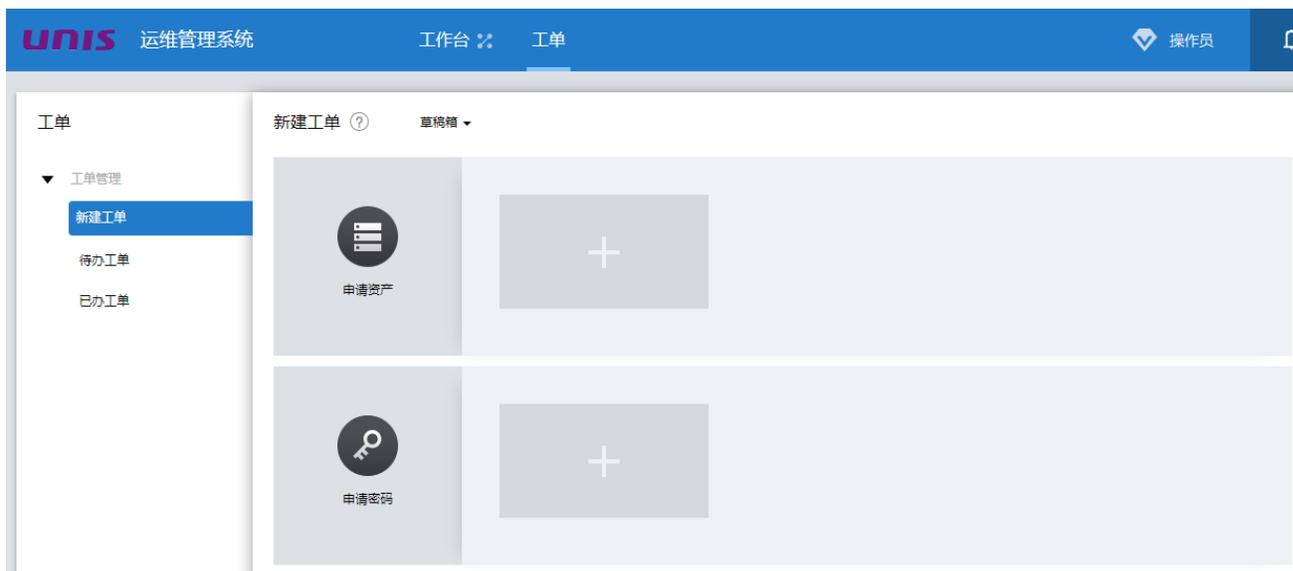


图 1: 资产权限工单处理流程

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	<p>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：</p> <ul style="list-style-type: none"> 开始时间：当前时间点。 结束时间：当前时间点+1天。 <p>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。</p>

申请资产
✕

工单标题 * ?

操作类型 * 日常维护 ▼

申请理由

申请Linux资产，用于日常维护

开始时间 * 2019-04-10 ≡ 10 ▼ : 58 ▼

结束时间 * 2019-04-11 ≡ 10 ▼ : 58 ▼

资产 * +

协议 * 全部协议 指定协议

放行命令

ls
rm -rf .*

使用人 * +

保存为草稿
保存为模板
提交

3. 单击**资产**对应的 \oplus ，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。

添加资产 ✕

≡ 筛选 🔍 资产名/IP/简要说明

#	资产名称	IP	简要说明	系统帐号
<input checked="" type="checkbox"/>	CentOS7	10.10.33.30		root ▾
<input checked="" type="checkbox"/>	CentOS7-2	10.10.33.130		any ▾
<input type="checkbox"/>	H3C VSR 1000	10.10.16.182		super ▾
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

全选 2 / 5 🔄 每页显示 10 ⏪ 1 / 1 ⏩

添加

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 \oplus ，选中要添加权限的用户，单击**添加**。

添加用户 ✕

≡ 筛选

#	帐号	姓名	角色	帐号状态
<input type="checkbox"/>	admin	admin	超级管理员	活动
<input type="checkbox"/>	<input type="text"/>			活动
<input checked="" type="checkbox"/>	opt	操作员	操作员	活动
<input checked="" type="checkbox"/>	opt2	操作员2	操作员	活动

全选 2 / 4 ✕ 每页显示 10 1 / 1

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。

工单类型	申请资产
工单标题	工单
操作类型	日常维护
申请理由	申请Linux资产, 用于日常维护
协议	全部
放行命令	ls rm -rf.*
申请人	opt
申请时间	2019-04-10 11:05:34

操作历史

-  opt 新建工单
2019-04-10 11:05:34
-  cfg 审核工单 批准申请
2019-04-10 11:07:42

资产清单

资产名称	IP	系统帐号	简要说明
CentOS7	10.10.33.30	root	
CentOS7-2	10.10.33.130	root	

合计: 2

使用人	opt opt2
使用时间	2019-04-10 11:04:00 2019-04-11 11:04:00

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。

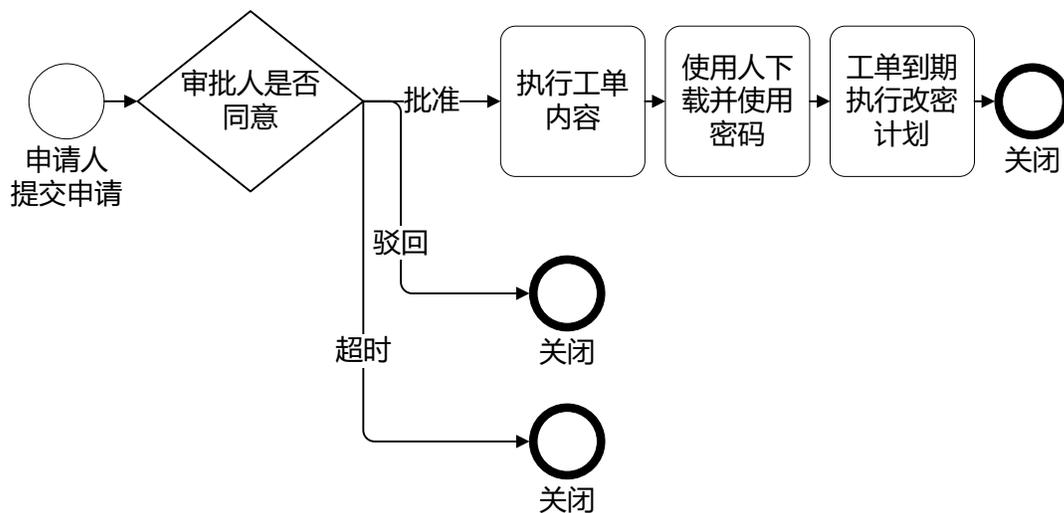
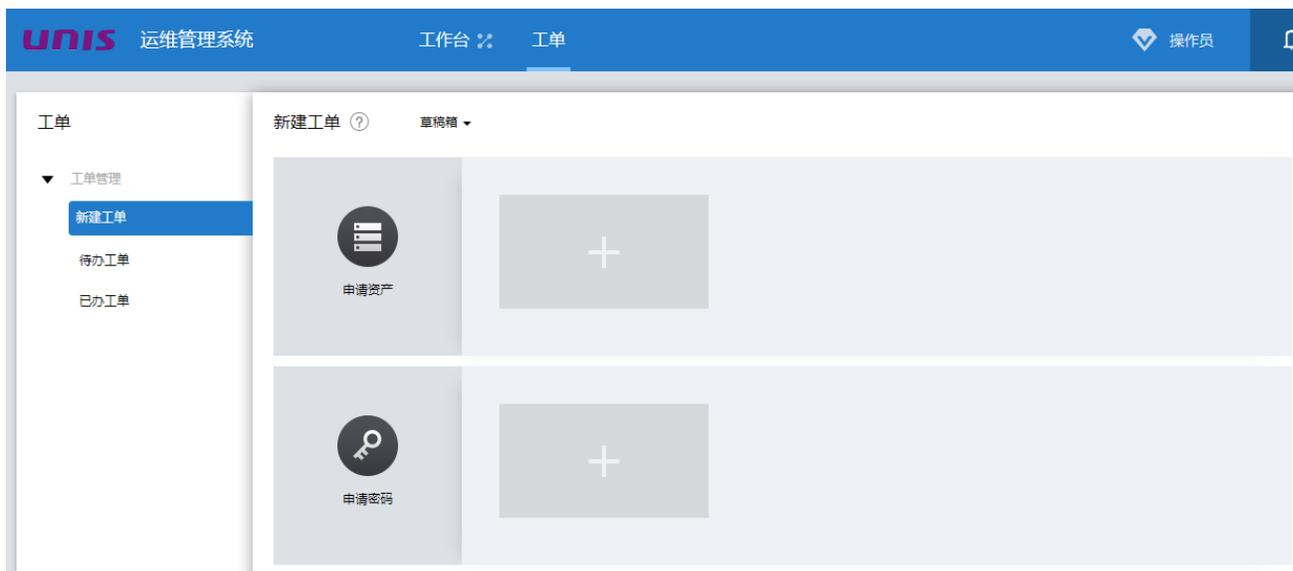


图 2: 密码工单处理流程

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	<p>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：</p> <ul style="list-style-type: none"> 开始时间：当前时间点。 结束时间：当前时间点+1天。 <p>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。</p>

申请密码
✕

工单标题 * ?

开始时间 * ≡ ↓ : ↓

结束时间 * ≡ ↓ : ↓

资产 * +

密码分段 是 否

保存为草稿
保存为模板
提交

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。

☰ 筛选

🔍 资产名/IP/简要说明

#	资产名称	IP	简要说明	系统帐号
<input checked="" type="checkbox"/>	CentOS7	10.10.33.30		root ▾
<input type="checkbox"/>	H3C VSR 100	10.10.16.182		super ▾

 全选 1 / 2

🔄 每页显示 10 ▾ < 1 / 1 >

添加

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。

工单标题* 密码申请 ?

开始时间* 2019-12-19 📅 11 ▼ : 01 ▼

结束时间* 2019-12-20 📅 11 ▼ : 01 ▼

资产*

资产名称	IP	系统帐号	操作
CentOS7	10.10.33.30	root	🗑️

合计: 1

+

密码分段 是 否

前段密码用户* 选择用户 opt(操作员)

后段密码用户* 选择用户 opt2(操作员2)

保存为草稿 保存为模板 提交

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**。

工单

进行中

驳回 批准

操作历史

opt 新建工单
2019-04-10 17:50:07

基本信息

工单类型	申请资产
工单标题	工单
操作类型	日常维护
申请理由	
协议	全部
放行命令	
申请人	opt
申请时间	2019-04-10 17:50:07

资产清单

资产名称	IP	系统帐号	简要说明
CentOS7	10.10.33.30	root	

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



Q 帐号/姓名

#	帐号 ▲	姓名 ▲	工作邮箱 ▲
<input checked="" type="checkbox"/>	opt	操作员	opt@test.com
<input checked="" type="checkbox"/>	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

目录:

- [修改个人设置](#)
- [修改会话配置](#)
- [配置密钥](#)

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	<p>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。</p> <p>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。</p>

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**。

帐号设置

修改信息

个人设置

信息加密

会话配置

密钥管理

字符会话 文件传输

会话访问方式 使用全局设置(putty)

会话访问方式(Mac) 使用全局设置(Terminal)

最大持续时间 使用全局设置 自定义

直连分类方式 资产组

重置 确定

3. 设置需要修改的参数，完成后单击**确定**。

参数	说明
会话访问方式	用于设置本地PC为Windows时的字符会话访问方式。 <ul style="list-style-type: none">• 使用全局设置：默认选项，由超级管理员在系统设置中配置，括号内会显示当前具体的配置。• putty：使用Putty工具建立字符会话。AccessClient安装时会自带Putty。• xshell：使用Xshell工具建立字符会话。需要自己安装Xshell。
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： <ul style="list-style-type: none">• 使用全局设置：默认选项，由超级管理员在系统设置中配置。具体设置值请咨询超级管理员。

参数	说明
	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 无：表示使用管理员配置的全局设置。 资产组 资产类型 责任人

修改文件传输配置

用于设置用户通过Web界面建立SFTP会话时，使用的SFTP工具。需要在本地PC上自行安装对应的工具。

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 > 文件传输**。



3. 设置需要修改的参数，完成后单击**确定**。

参数	说明
会话访问方式	用于设置本地PC为Windows时建立SFTP会话使用的工具，取值范围如下： <ul style="list-style-type: none"> 使用全局设置：默认选项，由超级管理员在系统设置中配置，括号内会显示当前具体的配置。 filezilla：使用FileZilla工具建立SFTP会话。 winscp：使用WinSCP工具建立SFTP会话。



说明： 这些参数修改后，不会对银河麒麟客户端产生作用。

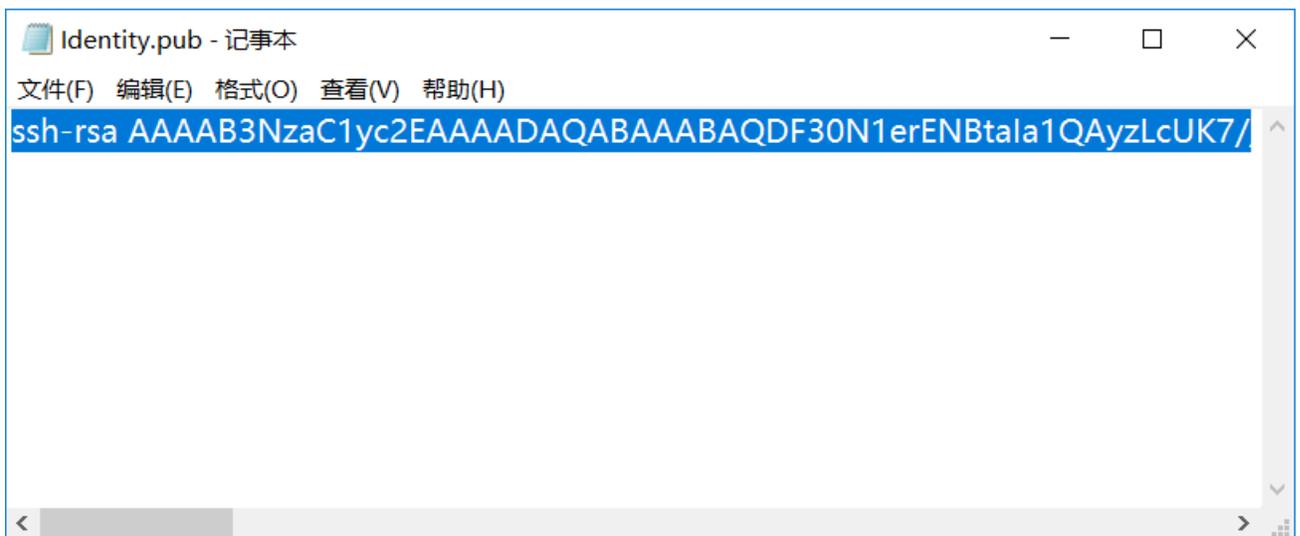
配置密钥

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。

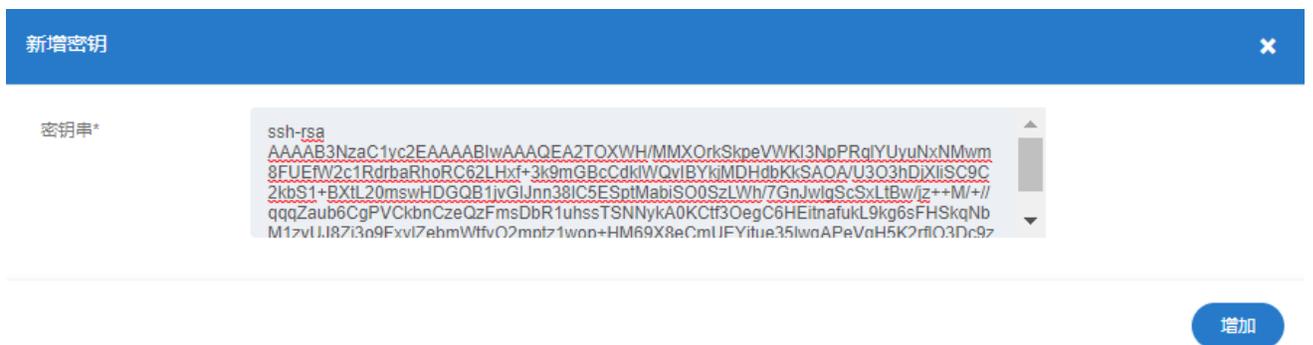
1. 使用工具生成密钥对，例如使用OpenSSH工具。
2. 通过Web界面登录A2000-E 运维管理系统。
3. 单击右上角用户帐号（例如操作员），选择帐号设置。
4. 选择修改信息 > 密钥管理。



5. 单击新建。
6. 以编辑文本文档的方式打开密钥中的公钥。



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。

目录:

- [使用双因子认证](#)
- [共享会话](#)

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）

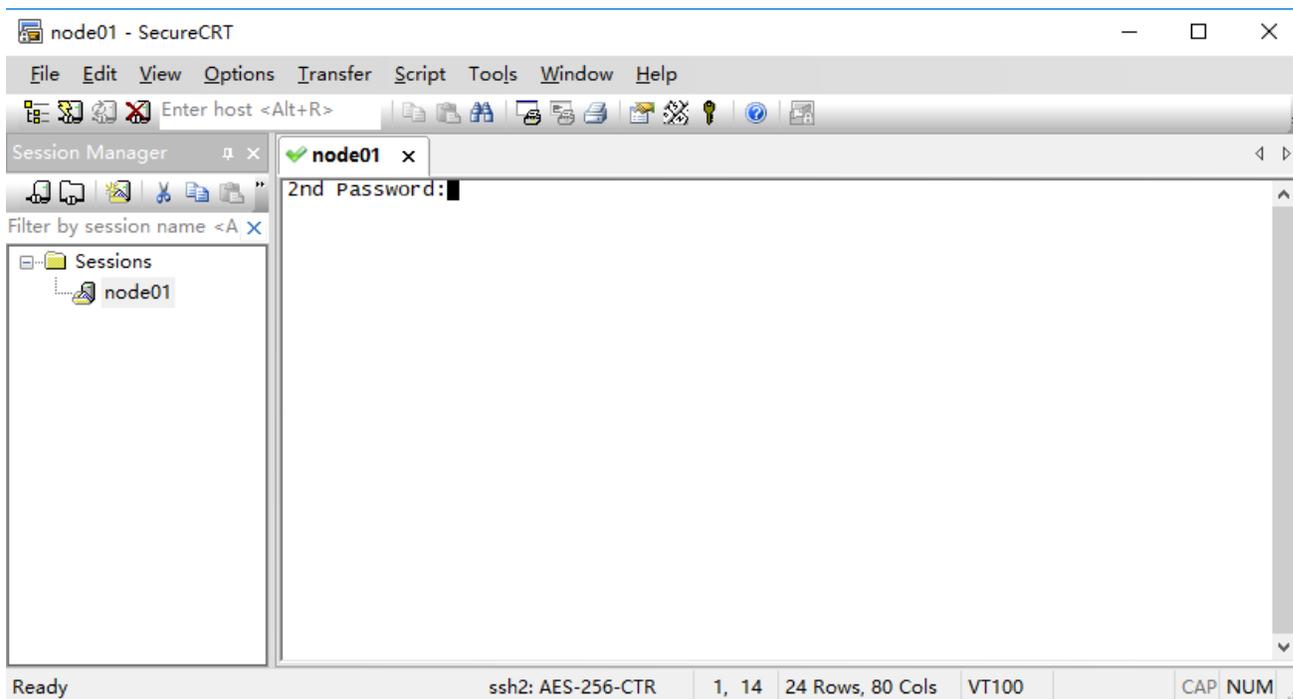
在密码输入框中输入第一重认证的密码，第一重认证通过后，在两步认证窗口中继续输入第二重认证的密码，并提交，进行第二重认证。

- **Web界面**的两步认证界面如下：



The image shows a web interface for two-step authentication. It features a light gray rectangular input field with the text "两步认证密码" (Two-step authentication password) inside. Below the input field, there are two blue rounded rectangular buttons. The left button is labeled "上一步" (Previous step) and the right button is labeled "提交" (Submit).

- **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

共享会话

用户可以通过A2000-E 运维管理系统将已打开的会话，共享给另一个用户，实现两人同时对同一个会话进行操作。

用户加入共享后，开启共享的用户不能取消对该用户的共享。但如果开启共享的用户关掉被共享的会话窗口，所有加入共享的用户的会话窗口都将被自动关闭。

会话共享有以下**使用限制**：

- 待共享的会话必须是通过Web界面或SSH客户端建立的会话。
- 会话共享列表中不显示SFTP会话和被复核的会话。

发起共享

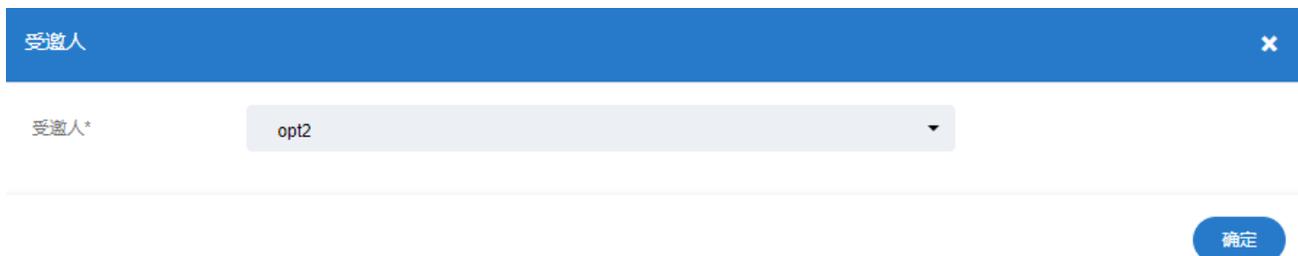
1. 访问资产。
2. 在Web界面中选择**工作台 > 访问资产 > 会话共享**。
3. 单击**共享**，打开可共享的会话列表。



4. 选择要共享的会话，单击**邀请**。



5. 在受邀人**输入框**中填入待邀请的用户名称，在下拉菜单中选中该用户，并单击**确定**，发送邀请给对应的用户。



说明:

- 发送邀请后，会话共享列表中 will 显示该共享会话。受邀人接受邀请之前，发起共享的用户可以单击**撤销**按钮取消邀请。如发起共享的用户在受邀人接受前关闭该会话或退出登录，邀请也将被自动取消。

最近访问 收藏 会话共享

开始时间	会话类型	协议	邀请	资产名	资产IP	系统帐号	操作
2019-03-07 18:41:40	字符会话	ssh	我 -> opt2	CentOS7	10.10.33.30	root	撤销

- 受邀人接受邀请之后，发起共享的用户如刷新列表，将看到该会话的**操作**一栏为**正在加入**，并在加入成功后显示为**已加入**。

最近访问 收藏 会话共享

开始时间	会话类型	协议	邀请	资产名	资产IP	系统帐号	操作
2019-03-07 18:41:40	字符会话	ssh	我 -> opt2	CentOS7	10.10.33.30	root	已加入

加入共享

受邀人收到共享邀请后可以选择加入会话共享。

- 通过Web界面登录A2000-E 运维管理系统。
- 在右上角单击消息提醒图标，可以看到收到的会话共享邀请。单击**查看详情**，将跳转到会话共享界面。也可以直接选择**工作台 > 访问资产 > 会话共享**进入该界面。



- 在会话共享列表中找到该条邀请，单击**加入**，加入到被共享的会话中。

[共享](#)

开始时间	会话类型	协议	邀请	资产名	资产IP	系统帐号	操作
2019-03-07 18:41:40	字符会话	ssh	opt -> 我	CentOS7	10.10.33.30	root	加入

合计: 1

每页显示 10 < 1 / 1 >



说明: 受邀人可以随时关闭被共享的会话窗口（不包括在字符会话中执行exit断开会话），不影响共享发起人和其他受邀人的会话。但再次加入需要共享发起人再次邀请。