RIS 数据中心风险洞察系统

用户手册

浙江齐治科技股份有限公司

齐治科技 QIZHI TECHNOLOGY

声明

商标声明

- 齐治科技 QIZHI TECHNOLOGY 是浙江齐治科技股份有限公司的商标或注册商标。
- 本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受浙江齐治科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，浙江齐治科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

关于本文档

本文档详细介绍RIS的各种功能特性，内容包括RIS的特性介绍和操作指导。

本文档适用于RIS的管理员和操作员等多种用户角色，请根据自己的操作角色，参考权限列表，阅读相应的指导，或者在实际操作中有疑问时查阅本文档。

产品版本

与本文档相对应的产品和版本如下表所示。

产品名称	产品版本
齐治科技RIS数据中心风险洞察系统	3.3.7

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

插图清单

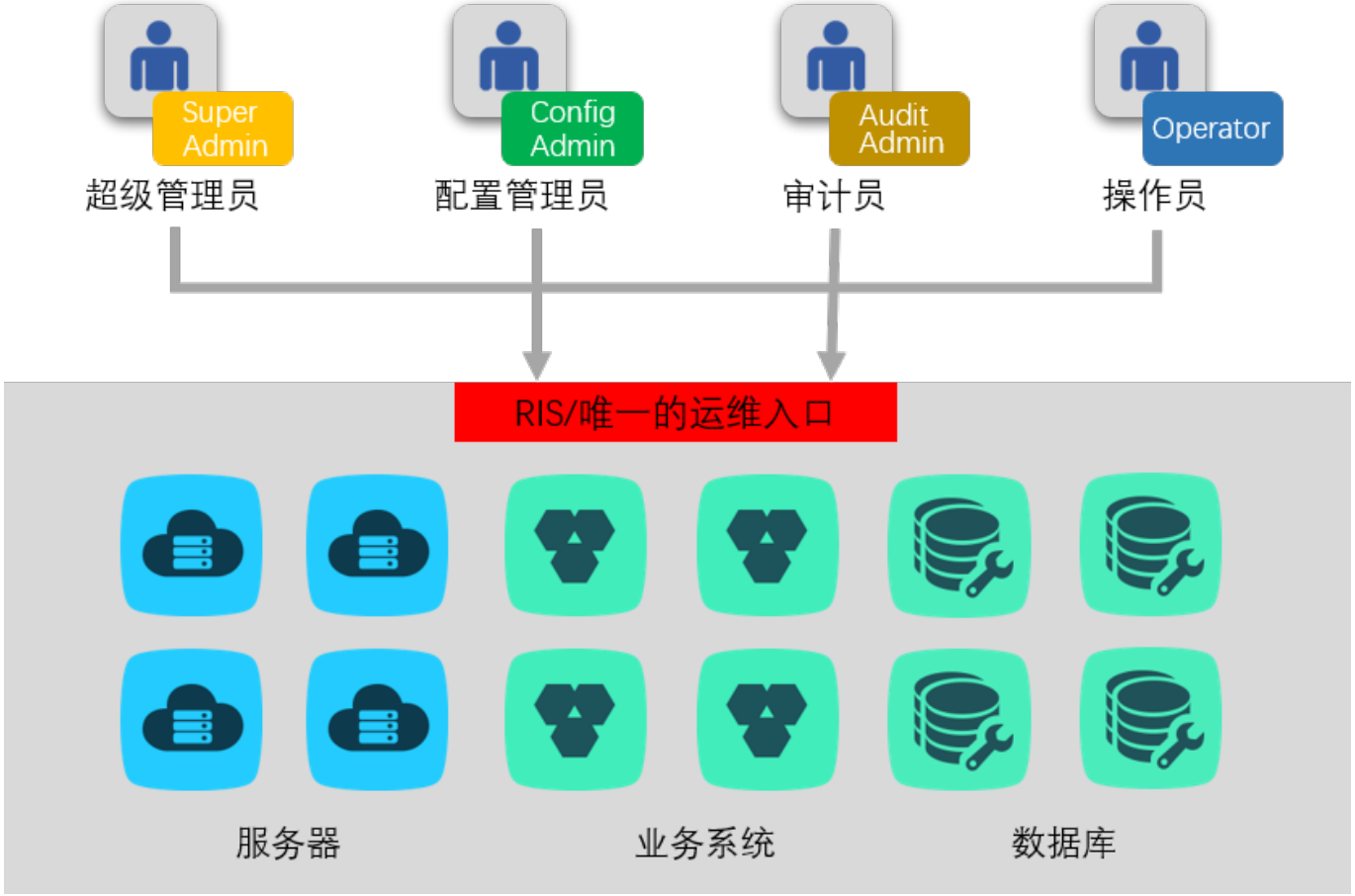
表格清单

概述

1

目录:

操作角色



RIS为了解决用户身份识别问题，为每一个用户创建一个身份认证帐号，用于平台身份鉴别，并借助访问权限将平台身份帐号与相应资产中系统帐号一一关联，实现用户操作与其身份相关联。

RIS中每一个创建的帐号，都需要设置为以下几种角色之一。不同的角色拥有不同的管理和访问权限。

帐号角色	角色描述
超级管理员	RIS最高权限角色，除了具备配置管理员、审计管理员等其他角色的权限，还可做基础设置和全局属性配置。
配置管理员	RIS的配置管理角色，可以配置用户、资产、访问权限。
审计管理员	RIS中的审计角色，拥有所管理的审计系统中所有的会话和事件的权限。
操作员	RIS中对各种资产和设备进行实际操作的角色，即普通用户。

说明:

- 此处列出的是系统默认的用户类型。用户也可以根据自己的需要，添加自定义的角色类型，并设置其拥有的权限。

权限列表

由于不同的角色类型对应不同的操作权限，因此本文档所列出的各种操作，只能由拥有权限的部分角色执行。

请不同用户根据自己的角色类型，查阅下面的权限列表，查找到当前用户角色所允许的操作有哪些，并查看这些操作所对应的操作指导：

操作		超级管理员	配置管理员	审计管理员	自动化管理员	操作员
管理	用户管理	√	√	×	×	×
	资产管理	√	√	×	√	×
	权限管理	√	√	×	×	×
访问	资产访问	√	√	×	√	√
	文件传输	√	√	×	√	√
	高危操作	√	√	×	×	√
审计		√	×	√	×	×
报表		√	√	√	×	×
自动化		√	√	×	√	×
工单		√	√	√	√	√
帐号		√	√	×	×	×
个人设置		√	√	√	√	√
系统配置		√	×	×	×	×

说明:

“√”表示拥有该项操作的权限；“×”表示没有该项操作的权限。

登录方式

RIS支持Web界面、Console控制台、RDP登录、SSH登录四种登录方式。管理员和普通用户可以通过Web方式完成大部分的日常操作；如果少数管理操作无法在Web界面完成，超级管理员还可以登录管理后台进行操作；普通用户如果需要快速运维Windows资产可以使用RDP登录；普通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。

登录RIS Web界面

Web界面是RIS最主要的访问入口，管理员、操作员、审计员都需要登录Web界面，并完成在RIS的各项操作。

服务端要求

- 已完成RIS的安装与配置。
- 已为RIS分配了IP，并且和本地客户端的网络相连通。
- RIS已上电，且各项服务的状态正常。
- 使用非本地密码方式登录时，已根据用到的登录方式完成了AD/LDAP服务器、RADIUS服务器、动态令牌、短信网关或手机令牌的相关配置。

客户端环境要求

本地PC客户端环境必须具备下列基本要求，才能够按照本文档的指引完成各项操作任务。本文以Windows 10和Google Chrome浏览器为例进行介绍。

项目	要求
操作系统	• Windows XP SP3及以上版本 • MAC OS。建议更新到最新版本
浏览器	• Microsoft Internet Explorer 11.0及以上版本 • Mozilla Firefox 50及以上版本 • Google Chrome 49及以上版本
显示器分辨率	建议最小为1280*1080（系统的缩放设置为100%时）。 **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。

说明:

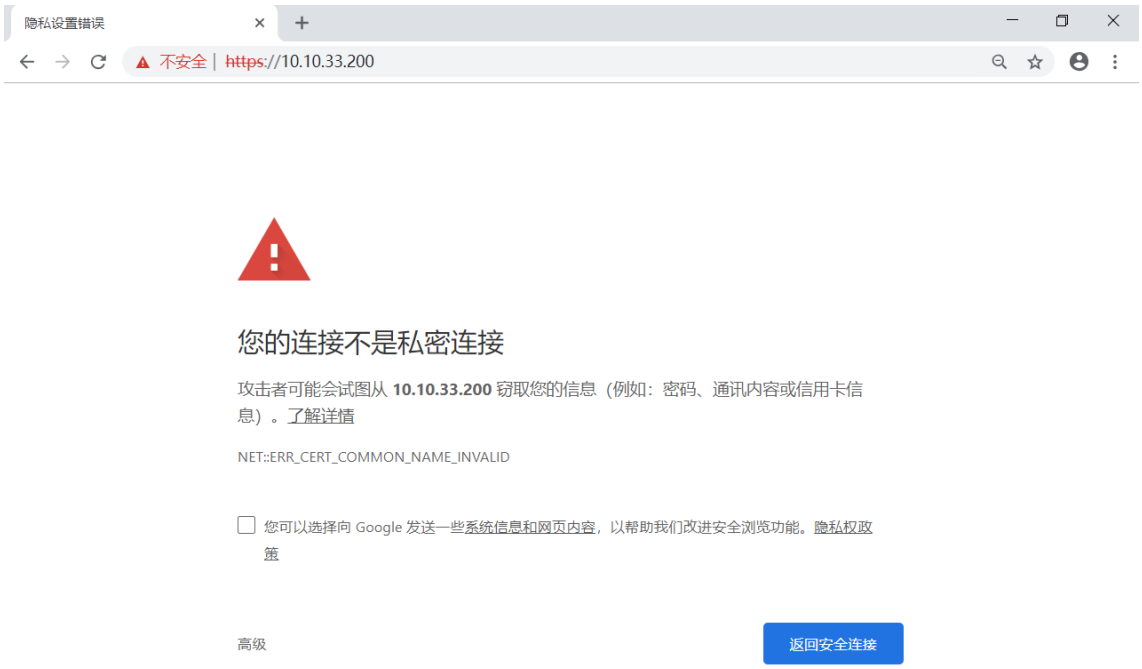
- 如果需要在IE早期版本（6/7/8/9）中使用，可以单击右上角的用户帐号，选择**帮助** > **浏览器支持** > **IE 6/7/8/9**，下载并安装IE浏览器插件，但该版本的IE的兼容性无法完全保障。

- 如果使用Windows XP/Windows 7，可以单击右上角的用户帐号，选择**帮助** > **浏览器支持** > **Chrome离线下载**，下载并安装相应版本的Chrome。

使用本地密码登录RIS

1. 请在浏览器中输入RIS的地址(https://RIS的IP地址)，进入RIS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Chrome浏览器请单击**高级** > **继续前往******），或者为Web界面安装安全证书并重新登录。



2. 输入帐号和密码，单击**登录**。

   说明: 首次登录请使用超级管理员的缺省用户名**admin**，密码为**admin**，后续登录请使用管理员分配好的用户名和密码。

3. 进入RIS的Web配置页面。

说明:

- 在任一界面单击左上角的齐治科技，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admin），可以打开系统设置菜单。

使用其他方式登录RIS

使用其他方式登录的方法和使用本地密码登录的步骤基本相同，只是在输入密码时会有一些区别。

此处仅就使用其他方式登录时的密码输入方式进行说明：

- 使用**AD/LDAP**方式登录：输入的用户名是Web界面上定义的的用户名，但密码是AD/LDAP服务器上关联用户对应的密码。如在AD/LDAP服务器上设置了下次登录时修改密码，则直接通过Web界面登录会失败，请先在AD/LDAP服务器上完成密码的重设。
- 使用**RADIUS**方式登录：输入的用户名是Web界面上定义的的用户名，但密码是RADIUS服务器上关联用户对应的密码。
- 使用**动态令牌**方式登录：输入的密码是一个拼接起来的字符串，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。

如果动态令牌与其他认证方式结合使用，在用户登录时，输入密码的方式有以下两种：

- 输入第一重密码后按回车或者单击**登录**等按钮后再输入“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”。

- 使用**手机令牌**方式登录：手机令牌只能作为双因子认证中的第二重认证方式。

1. 根据启用的双因子认证的第一重认证方式，输入第一重认证的密码，并单击**登录**。
2. 第一次登录时，界面上会弹出提示，要求使用客户端扫码绑定。在手机上安装Google Authenticator或Free OTP，并使用**扫码绑定**或**手动输入**的方式进行绑定。绑定完成之后单击**完成绑定**。

3. 打开手机上安装的Google Authenticator或Free OTP，使用绑定的生成器生成一个动态密码，在密码时效内输入到**两步认证密码**对话框中，并单击**提交**。

说明: 第一次登录时如在客户端上已完成绑定，但在界面上未绑定成功，第二次登录仍会提示要求绑定。请先在手机上删除已绑定的生成器，并重新绑定。如未删除旧的绑定就重新进行绑定，则手机上的绑定将不会更新，后续生成的密码将始终无效且无法再重新绑定，此时请联系配置管理员重置密码。

- 使用**短信认证**方式登录：短信认证只能作为双因子认证中的第二重认证方式。
  1. 根据启用的双因子认证的第一重认证方式，输入第一重认证的密码，并单击**登录**。
  2. 输入绑定的手机上收到的短信验证码，并单击**提交**。如未收到短信，120秒后单击**重新发送验证码**按钮重新发送。

说明: 如在完成第一重认证之后就提示**短信发送失败**，说明短信网关配置有误。

- 使用**USBKey认证**方式登录：需要先安装USB Key设备内的et199auto.exe控件，并安装**帮助**菜单中下载的ET199Plugin.exe插件。完成安装后，在IE11浏览器中访问，输入第一重验证的密码（无第一重验证则密码为空），并在弹出的菜单中输入USB Key的密码，完成验证。

- 使用**双因子认证**方式登录：双因子认证是将以上的的各种登录方式的其中两种组合在一起完成验证。

  在登录界面的**密码**输入框中输入第一重认证的密码，单击**登录**认证成功后，会弹出**两步认证密码**输入框，继续输入第二重认证的密码并单击**提交**完成认证。

登录RIS的Console

Console控制台支持通过多种方式使用root帐号登录。登录到控制台之后，管理员可以进行重置admin帐号、使用系统工具、修改主机名等功能。

RIS的Console支持以下登录方式：

- SSH远程登录
- 串口登录
- 显示器直连

其中，显示器直连，请准备一台支持VGA接口的显示器、VGA连接线、键盘，将显示器和键盘直接连接到设备上登录进行操作，并使用帐号“root”，默认密码4OO88O2393（O为大写字母），登录到Console控制台。

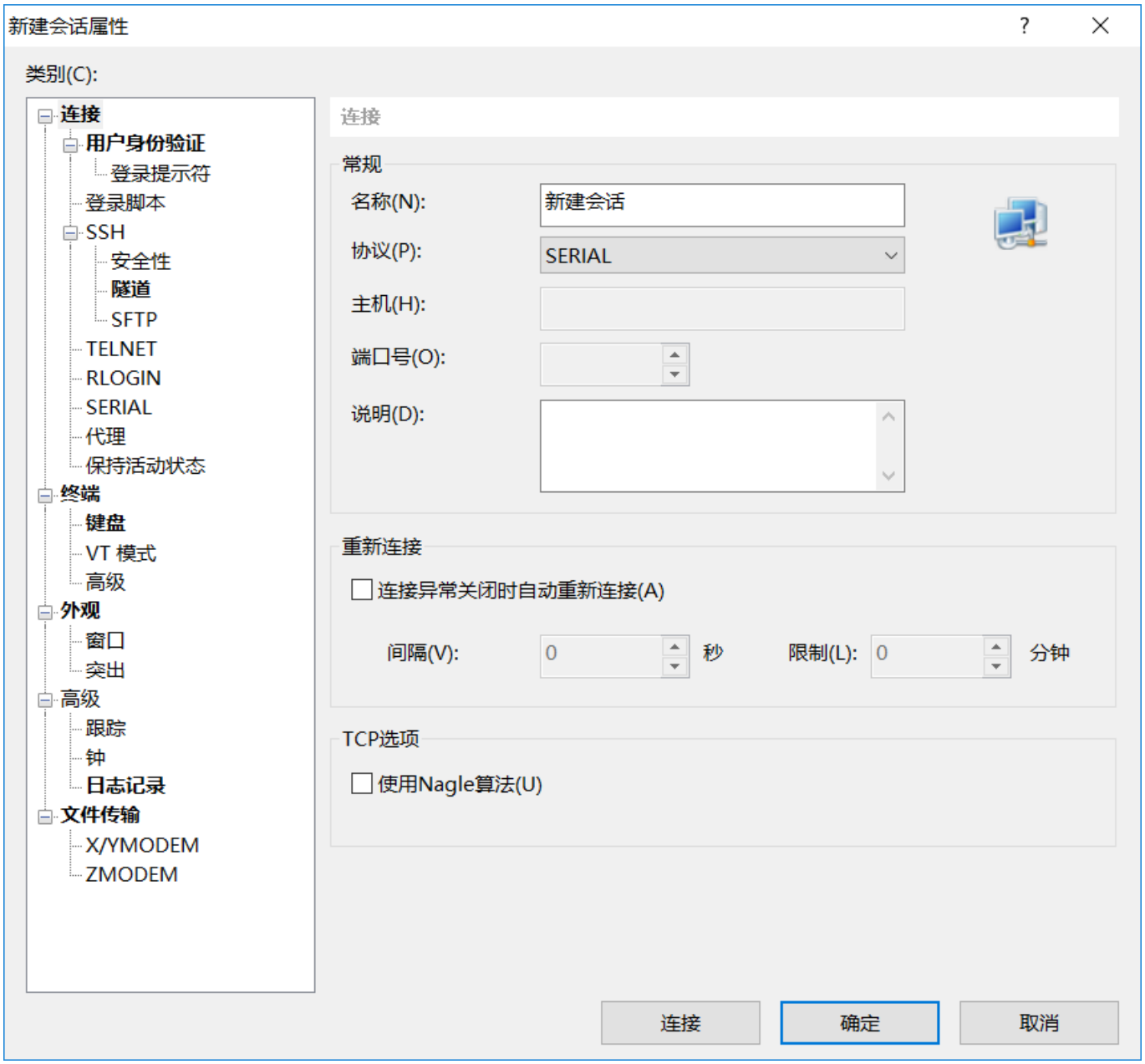
本文主要介绍如何通过串口登录和SSH远程登录的方式访问Console。

通过串口登录Console

如使用串口登录Console，需要提前准备Xshell、SecureCRT等支持串口登录的工具。

本文以Xshell为例介绍串口登录步骤，SecureCRT和Putty的配置与Xshell基本相同。

1. 将本地PC和RIS通过串口线相连。
2. 在Xshell主界面，选择**文件** > **新建**，新建一个连接。
3. 将**协议**设置为**SERIAL**。

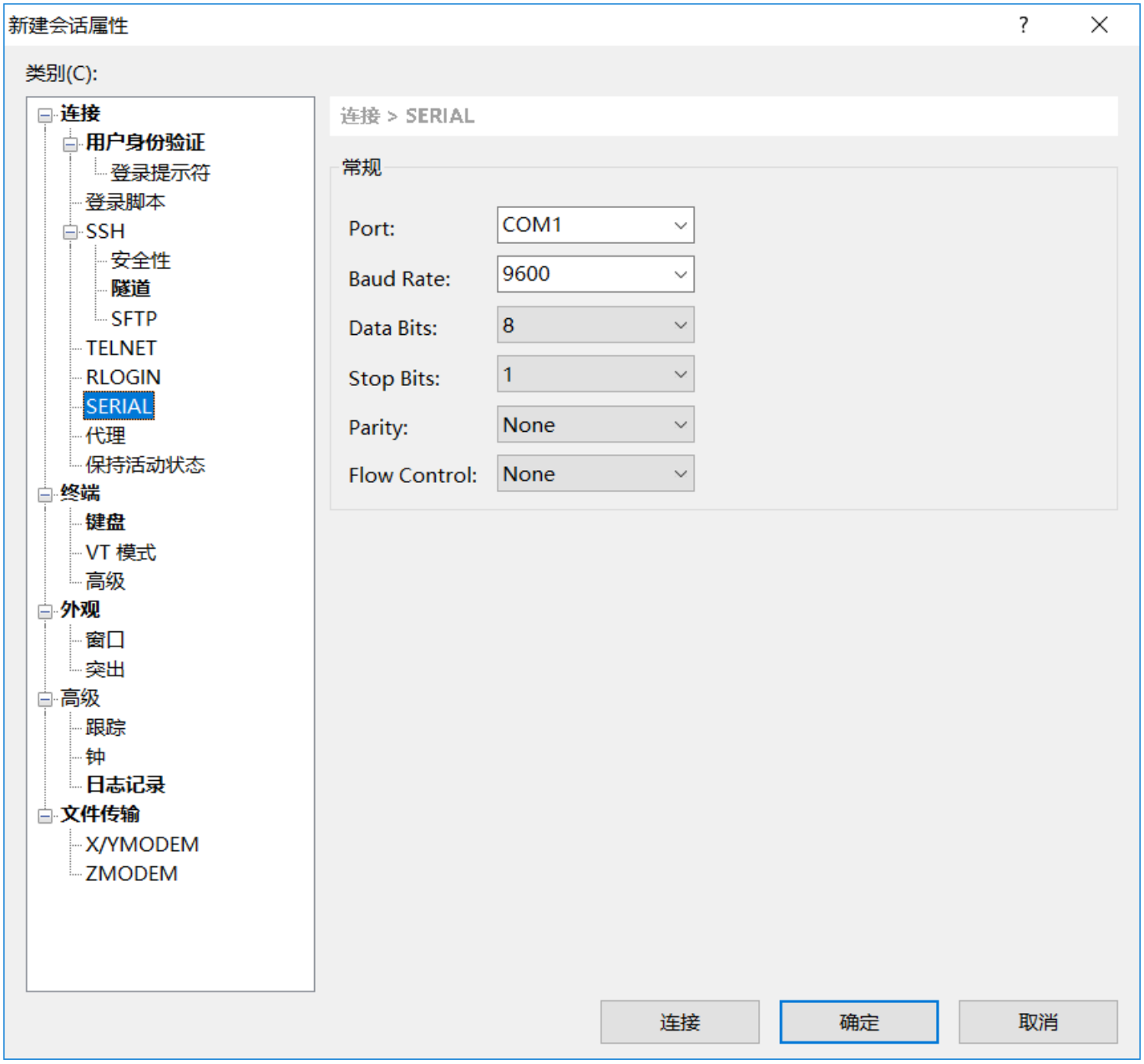


4. 在左侧选择**SERIAL**，设置串口属性。

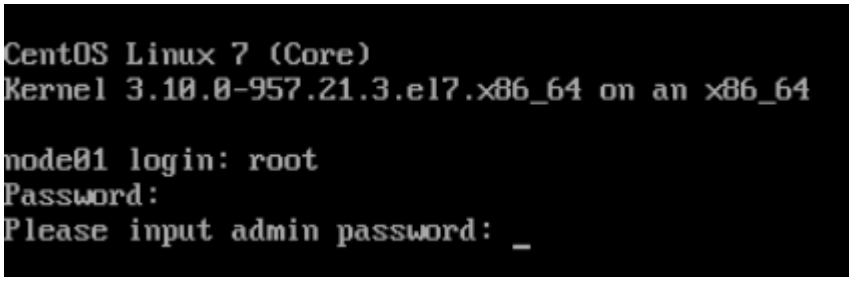
   使用Xshell时，全部使用以下默认值即可。

   - Port：COM
   - Baud rate：9600

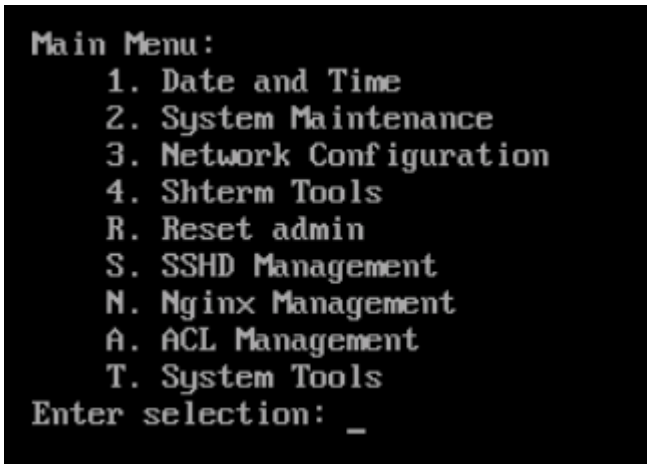
- Data bits：8
- Stop bits：1
- Parity：None
- Flow Control：None



5. 单击**连接**，连接成功后，输入用户名**root**，密码4OO88O2393（O为大写字母）。



6. 输入admin帐号的登录密码，完成后按回车，进入Console主菜单。



说明:

- 当收到**Wrong password**提示时，请检查是否正确输入了admin用户的密码。
- 当收到**Request verify password timeout**提示时，请等待系统进程完全启动。

密码输入超时或错误3次后，可以选择通过challenge进入。请联系齐治科技技术支持人员并提供显示的**User Code**，获取challenge码。

此处的admin登录验证不会受到全局用户登录控制中的限制。

通过SSH远程登录Console

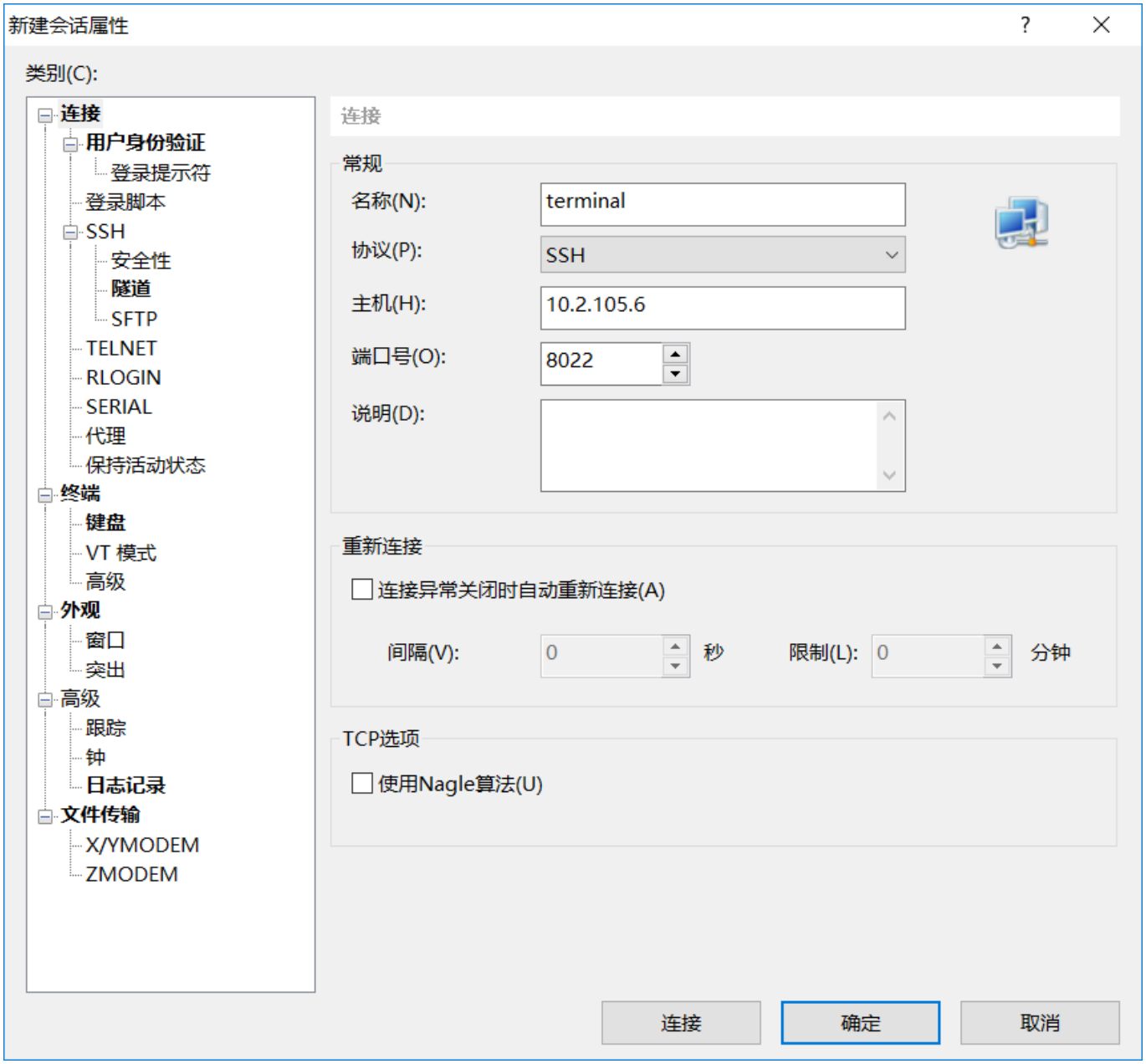
使用SSH远程登录Console，需要提前准备Xshell、SecureCRT等支持SSH协议的工具。

另外还需要满足以下前提条件：

- 已为RIS分配了IP，并且和本地客户端的网络相连通。
- RIS的TCP/8022端口可用，未受到防火墙限制。
- RIS默认禁用通过SSH登录Console控制台，登录前已在Web界面的**系统设置** > **系统** > **系统状态**中设置**sshd外部访问**参数为**开启**。
- 已获取用于登录RIS的私钥。私钥文件名为“RSA-****-openssh”，其中“****”为时间戳。如未获取请联系齐治科技技术支持获取。

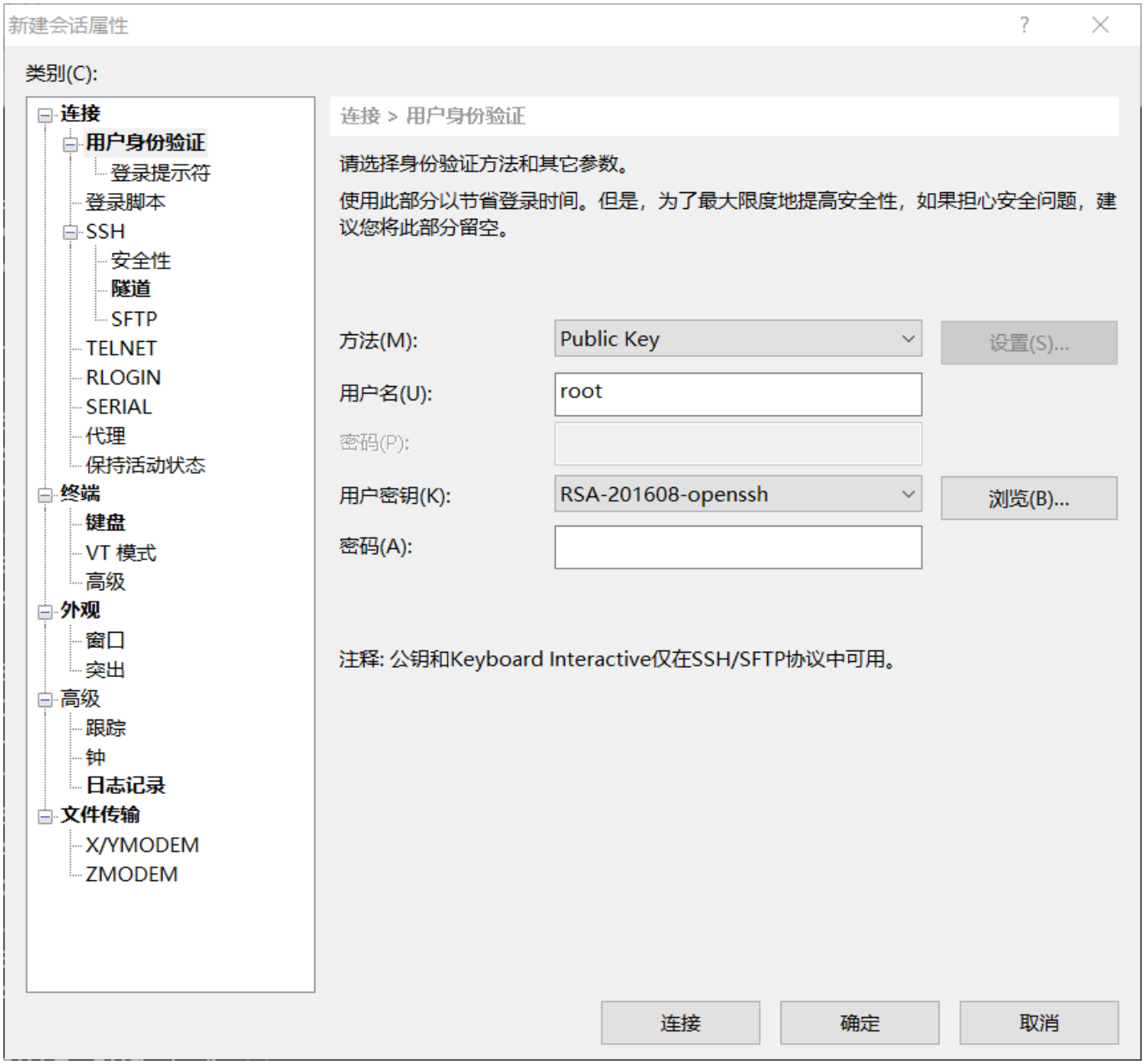
本文以Xshell为例介绍登录步骤，SecureCRT的配置与Xshell基本相同。

1. 在Xshell主界面，选择**文件** > **新建**，新建一个SSH连接。
2. 在**连接**菜单设置会话以下属性：
   - **名称**：用户自定义的连接名称
   - **协议**：SSH
   - **主机**：RIS的IP地址
   - **端口号**：8022



3. 在**连接** > **用户身份验证**菜单，配置以下属性：
   - **方法**：Public Key
   - **用户名**：root

- **用户密钥**：选择已获取的用于登录的私钥
- **密码**：默认为空



4. 单击**连接**，连接成功后要求用户输入admin帐号的登录密码。

```
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Last login: Wed May 29 10:13:07 2019 from 10.10.66.17
Please input admin password:
```

说明:

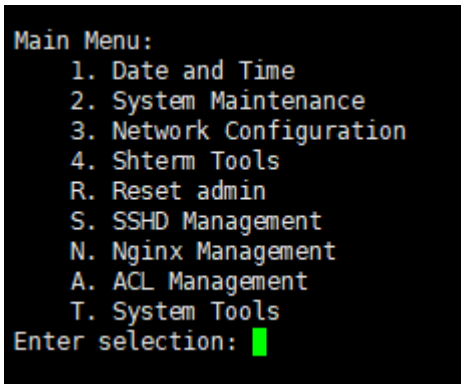
- 当收到**Wrong password**提示时，请检查是否正确输入了admin用户的密码。

- 当收到**Request verify password timeout**提示时，请等待系统进程完全启动。

  密码输入超时或错误3次后，可以选择通过challenge进入。请联系齐治科技技术支持人员并提供显示的**User Code**，获取challenge码。

  此处的admin登录验证不会受到全局用户登录控制中的限制。

5. 输入后按回车，进入下列菜单，可以执行菜单相关选项进行控制台管理。



登录到Console之后，可以执行菜单选项进行控制台管理，或者输入q并按回车退出登录。

通过RDP登录RIS

操作员可以通过RDP的方式登录到RIS，从而直接打开图形会话对设备进行操作。

前提条件如下：

- 已完成RIS的安装与配置。
- 已为RIS分配了IP，并且和本地客户端的网络相连通。
- 本地PC支持RDP服务。
- 已在Web界面上完成了相应用户、资产、权限的配置。

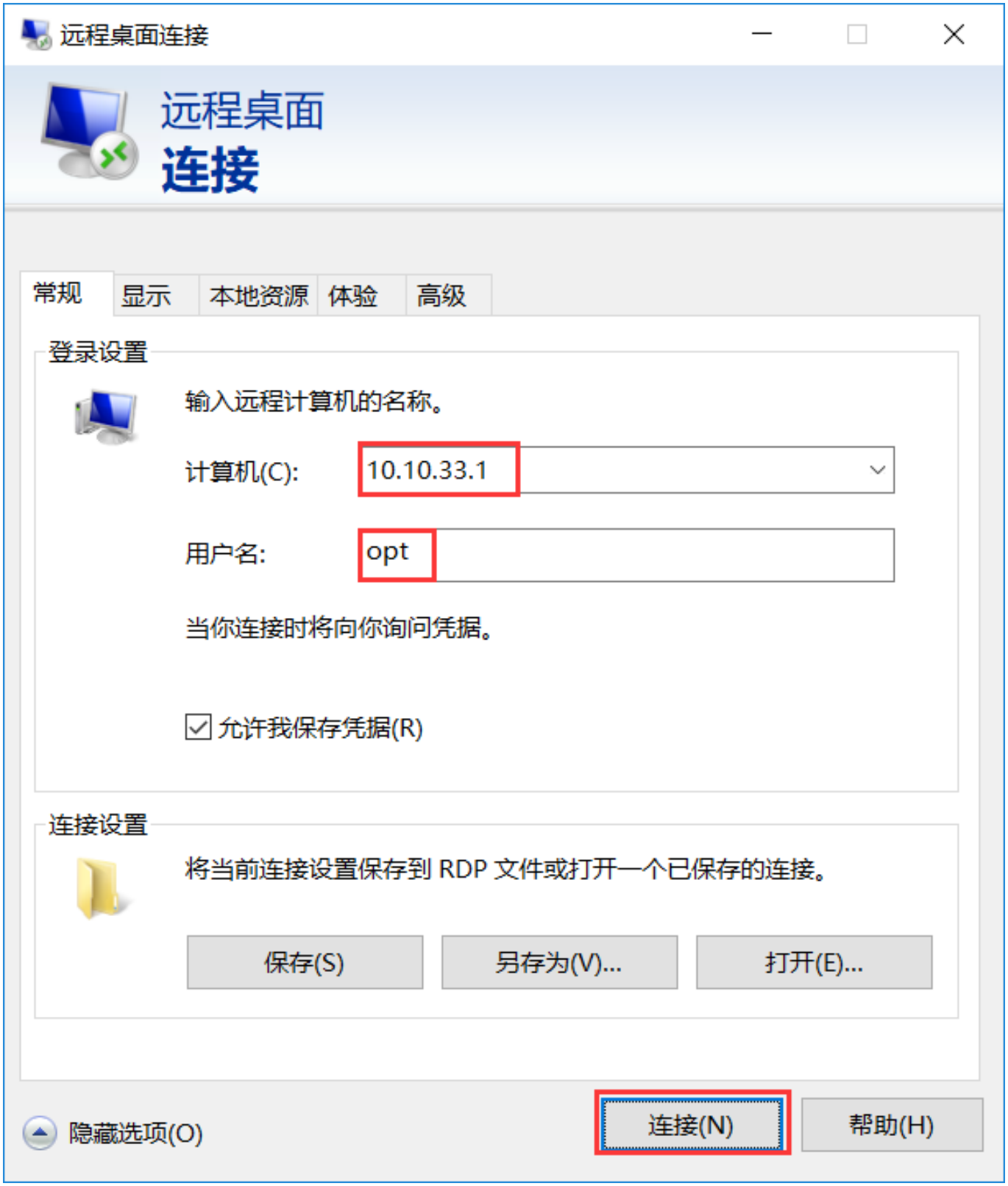
RDP登录到RIS之后只能执行资产/设备访问操作，不能对RIS进行管理，并且只能看到当前帐号拥有访问权限且支持RDP访问的资产/设备。

使用USB Key认证的用户不能通过该方式登录RIS。

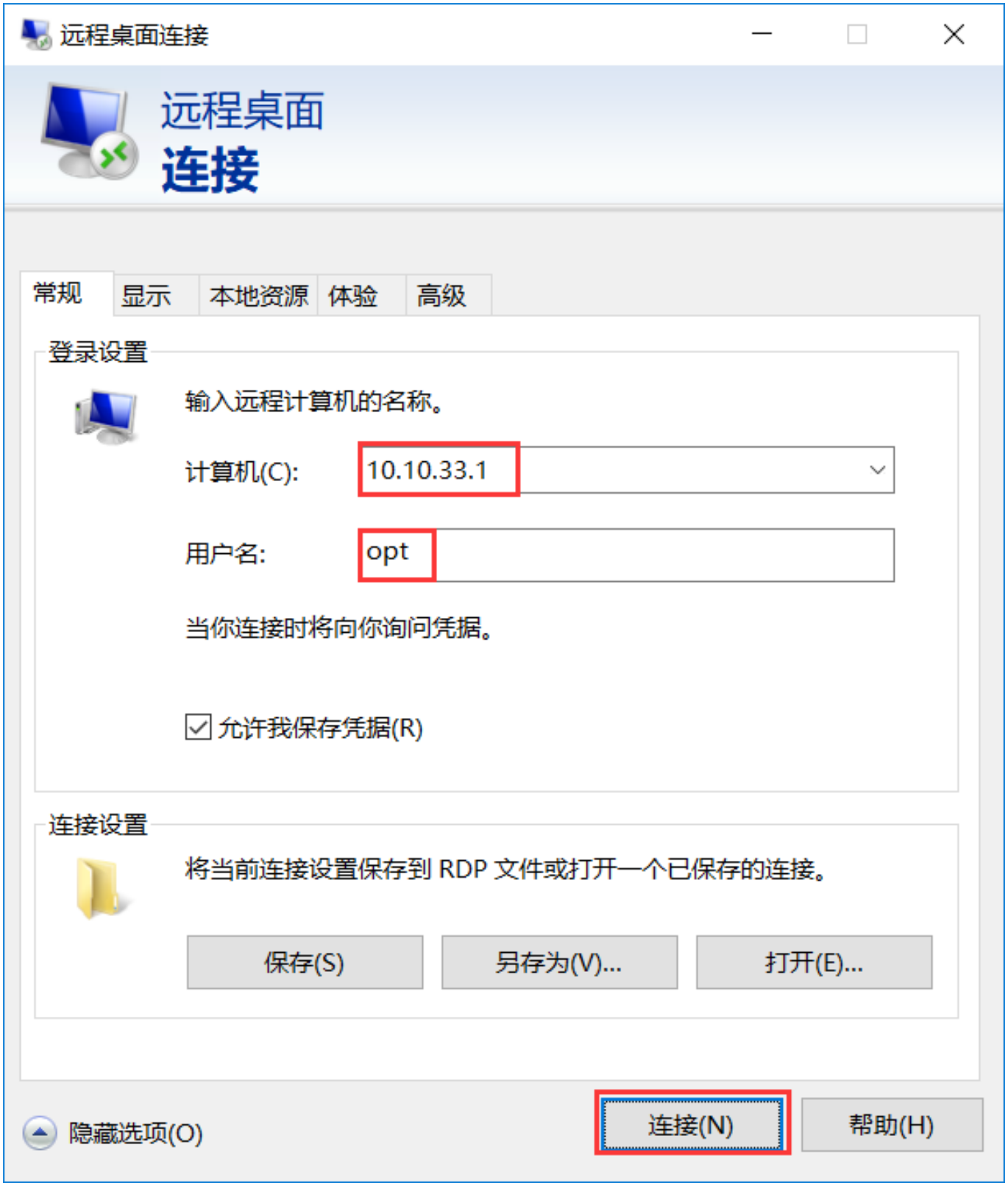
本文以装有Windows系统的本地PC为例进行介绍。

1. 在Windows系统的**运行**或搜索框中输入**mstsc**，打开**远程桌面连接**。

2. **计算机**输入RIS的IP地址，**用户名**输入操作员在RIS上帐号名称，并单击**连接**。



3. 在弹出的**Windows安全性**对话框中，输入当前操作员在RIS上的密码，并单击**确定**。

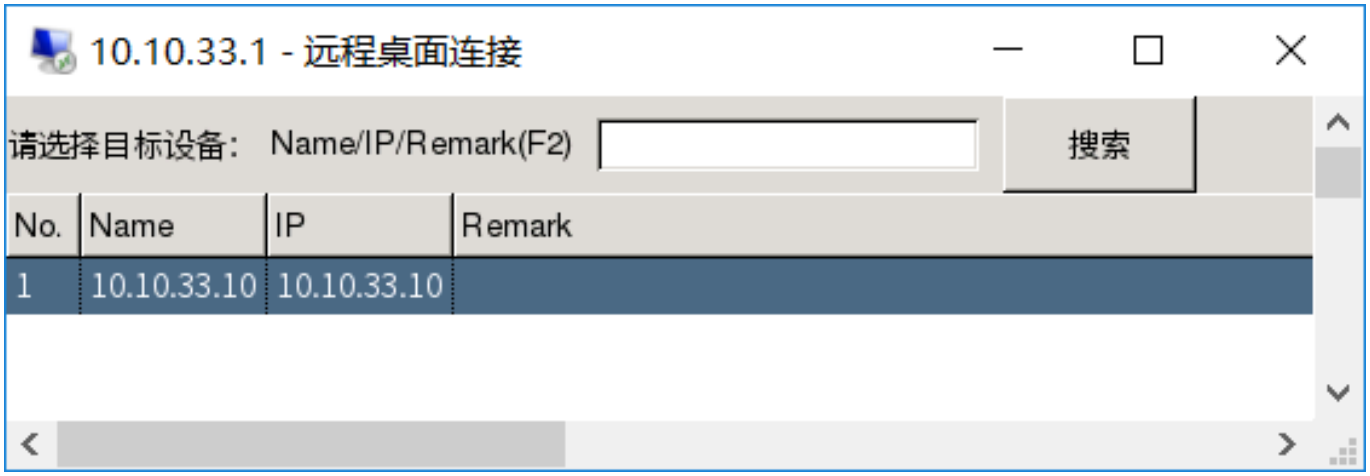


说明:

- 如未弹出该对话框或认证失败，将跳转到RIS的RDP登录界面，请将窗口最大化，并在窗口中央的登录窗口中重新填入用户名和密码，并单击**确定**。

- 使用其他认证方式时，密码的输入和Web界面类似，请参考使用其他方式登录RIS输入密码并完成登录。其中手机令牌登录，由于首次登录需要扫码绑定，请先在Web页面登录并完成绑定之后再通过RDP登录。

4. 成功连接到RIS之后，会显示所有可以通过RDP连接的设备，选中一台待连接的设备后，双击连接到该设备。



说明: 如配置了HA，则连接时可以通过虚IP或主机的IP连接，无法通过备机的IP连接。

通过SSH登录RIS

操作员可以通过SSH的方式登录到RIS交互终端，从而直接建立Telnet/SSH字符会话对设备进行操作。

- 已完成RIS的安装与配置。
- 已为RIS分配了IP，并且和本地客户端的网络相连通。
- RIS的TCP/22（SSH）端口可用，未受到防火墙限制。
- 本地PC已安装了Xshell、SecureCRT或Putty等支持SSH协议的远程连接工具。
- 配置管理员已在Web界面上完成了相应用户、资产、权限的配置。

通过SSH登录到RIS之后只能执行资产/设备访问操作，不能对RIS进行管理，并且只能看到当前帐号拥有访问权限且支持SSH访问的资产/设备。

使用USB Key认证的用户不能通过该方式登录RIS。

本文以Xshell为例介绍登录步骤，SecureCRT、Putty的配置与Xshell基本相同。

1. 在Xshell主界面，选择**文件** > **新建**，新建一个SSH连接。
2. 在**连接**菜单设置会话以下属性：
   - **名称**：用户自定义的连接名称
   - **协议**：SSH
   - **主机**：RIS的IP地址
   - **端口号**：22
3. 在**连接** > **用户身份验证**菜单，配置以下属性：
   - 方法：
     - 当不使用双因子认证和密钥认证时，选择**Password**。
     - 当使用双因子认证时，选择**Keyboard Interactive**。
     - 当使用密钥认证时，选择**Public Key**。
   - **用户名**：待登入的操作员的用户名，需要先在Web界面中进行配置，如admin。
   - **密码**：在Web界面配置的该用户的登录密码。如使用双因子认证，则输入双因子认证中的第一重认证的密码。如使用密钥认证，则输入用户密钥对应的密码，用户密钥没有密码则不填写。
   - **用户密钥**：仅当使用密钥认证时配置，从而不输入密码登录到RIS交互终端。在下拉菜单中选择，或单击**浏览**选择已添加到RIS Web界面中的公钥对应的私钥。该密钥对必须已预先通过配置密钥完成添加。
4. 单击**连接**，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。

说明:

- 如登录帐号使用双因子认证，当第一重认证成功后，会显示**2nd Password:** ，请参考使用其他方式登录RIS输入密码并完成登录。

- 如登录帐号设置了使用手机令牌登录后，然后直接通过SSH登录会失败，请先通过Web界面登录并绑定手机令牌。
- 如登录帐号在Web界面上设置了**下次登录时必须修改密码**后，然后直接通过SSH登录，登录完成后会提示在Web界面修改密码并退出，请先通过Web界面登录并重设密码。
- 如登录帐号在AD/LDAP服务器上设置了下次登录时修改密码，然后直接通过SSH登录会失败，请先在AD/LDAP服务器上完成密码的重设。
- 如登录成功后，界面显示为乱码，请在Xshell的会话属性中，选择**终端**，修改编码类型，和Web界面的**系统设置** > **访问设置** > **字符终端** > **终端字符编码**中的编码类型保持一致。该设置只有超级管理员能够查看并修改，其他用户请联系超级管理员获取。
- 退出登录，在**资产分类列表**界面，输入**q**并按回车。如在子菜单中请按先回车键返回**资产分类列表**界面。

通过SSH登录RIS后，请参考通过Telnet/SSH客户端建立字符会话，访问相关资产。

安装安全证书

访问RIS的Web界面时，如果提示证书错误，请安装RIS的安全证书。
管理员已制作RIS的安全证书，具体请参见配置安全证书。

1. 单击地址栏中的**证书错误**，然后单击**查看证书**。

2. 单击**导出到文件**，将证书保存在本地PC。
3. 双击证书文件名，单击**打开**。
4. 单击**安装证书**。
5. 选择存储位置，单击**下一步**。
6. 选中**将所有的证书都放入下列存储**，单击**浏览**，选择**受信任的根证书颁发机构**，单击**确定**。
7. 单击**下一步**，然后单击**完成**。

8. 查看安全警告信息，单击**是**，提示导入成功，单击**确定**。

9. 重启浏览器，访问RIS的Web界面，不再提示证书错误。

安装AccessClient

在使用RIS访问资产时，除了通过Web方式建立图形会话，其他场景下RIS都会通过AccessClient打开会话。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，也可根据该提示下载并安装AccessClient。如已安装了AccessClient，仍然收到提示，请单击**已安装**进行忽略。

1. 登录RIS Web界面。

2. 单击右上角单击帐号名称，在下拉菜单中选择**帮助**。

3. 在**AccessClient** > **下载**页面，单击**下载**，将AccessClient.exe下载到本地。

4. 双击运行AccessClient.exe，并单击**Install**进行安装。

获取帮助

RIS的Web界面提供了帮助页面，包括查看软件版本、管理软件包和用户手册等。

获取软件版本信息

在RIS的Web界面可以获取软件版本号和各组件的版本信息。

1. 单击右上角用户帐号（例如admin），选择**帮助**。

2. 选择**关于** > **软件信息**。

3. 在**组件版本信息**中查看各组件的版本，其中**webapp**后的X.X.X就代表RIS软件版本号。

   例如**webapp-3.3.7-186.x86_64**表示RIS的版本号是**3.3.7**。

管理软件包和用户手册

超级管理员和自定义角色中包含系统设置权限的用户可以上传用户手册和软件包，也可以删除过时或者错误的内容；所有用户可以下载用户手册和软件包。

管理用户手册

1. 单击右上角用户帐号（例如admin），选择**帮助**。

2. 选择**关于** > **软件信息**。

3. 在**用户手册**中管理用户手册。

   - 超级管理员和自定义角色中包含系统设置权限的用户：

     - 单击**上传**，从本地PC选择用户手册上传到RIS。

表 1: 用户手册上传要求说明表

项目	描述
大小	每个文件不超过100MB。
格式	• pdf • word：包括doc、docx、docm、dot、dotm、dotx
文件名	字符串格式，最大长度为85个字符，建议使用中英文字符和数字。上传后文件名不能再被修改。

说明: 如果还有其他文件需要上传，请重复执行本步骤。

- 单击某个用户手册对应的**删除**，删除该手册。

- 所有用户：

  单击某个用户手册对应的**下载**，下载该手册。

管理软件包

1. 单击右上角用户帐号（例如admin），选择**帮助**。
2. 选择**其他应用** > **下载**。
3. 在**下载用户软件包**中管理软件包。

- 超级管理员和自定义角色中包含系统设置权限的用户：
  - 单击**上传**，从本地PC选择软件包上传到RIS。

表 2: 软件包上传要求说明表

项目	描述
大小	每个文件不超过500MB。
文件名	字符串格式，最大长度为85个字符，建议使用中英文字符和数字。上传后文件名不能再被修改。

说明: 如果还有其他文件需要上传，请重复执行本步骤。

- 单击某个软件包对应的**删除**，删除该软件包。

- 所有用户：

  单击某个软件包对应的**下载**，下载该软件包。

用户管理

2

目录:

用户是指RIS的使用者，包含帐号、角色、身份验证方式等多种属性。RIS支持多种用户配置方式。

按照权限范围的大小，RIS将用户划分为多种不同的角色。RIS缺省提供的用户角色如下，RIS支持自定义新的用户角色。

- **超级管理员**：系统中的最高权限角色，拥有其他所有角色的权限之和。另外，系统的基础功能、全局参数等也只有超级管理员角色有配置权限。
- **配置管理员**：系统中的配置管理权限，该角色能够配置用户、资产和资产访问权限。
- **审计管理员**：系统中的审计权限，该角色能够查看操作审计和事件审计结果。
- **操作员**：系统中的操作权限，该角色能够访问主机、网络设备等资产。

RIS缺省提供了一个超级管理员角色的用户**admin**（缺省密码也是**admin**），请再根据实际情况创建不同角色的用户。

创建用户时，RIS缺省提供的预定义用户属性如表 3: 预定义用户属性所示。如果RIS预定义用户属性不满足需求，可以自定义用户属性。

表 3: 预定义用户属性

属性	说明
帐号	用户的帐号，用来唯一标识用户。
姓名	用户的姓名，用户登录Web界面后，姓名会显示在Web界面的右上角。
身份验证	用户的身份验证方式。RIS缺省支持的是本地密码，即用户身份验证功能由RIS完成。如果已部署了AD、LDAP、RADIUS等认证服务器，RIS支持与这些第三方认证服务器对接完成身份验证。除此之外，RIS还支持手机令牌、双因子认证和X.509证书认证。
手机号码	用户的手机号码。
工作邮箱	用户的工作邮箱，用来接收密码、改密通知等各种信息。
用户组	用户所属的用户组。用户组是用户的一种组织形式，相同权限的用户可以划分到同一个分组。配置用户的权限时就能够以用户组为单位而不是用户，可有效减轻配置负担。
部门	用户所属的部门。
状态	用户的状态，包括**活动**和**禁用**，缺省为**活动**。
帐号有效期	用户帐号的有效期。帐号过期后，用户登录RIS会提示帐号状态异常。

属性	说明
密码有效期	用户密码的有效期。密码过期后，用户必须修改密码才能重新登录。
用户登录控制	允许或者禁止用户登录的时间和IP地址范围。
备注	用户的备注信息。

RIS支持多种用户创建方式：

1. 手工创建

   使用手工方式逐一创建用户。

2. 批量导入

   对于本地用户和RADIUS用户，建议使用批量导入的方式快速在RIS上创建大量用户。

3. LDAP导入

   对于AD用户和LDAP用户，请使用LDAP导入功能将用户导入到RIS。另外，RIS还支持LDAP用户定期同步和新用户自动加入。

对于用户组，支持手工创建和批量导入两种创建方式。在批量导入用户中设置好用户组，创建用户的同时也创建了用户组。

配置用户（手工创建）

在RIS的Web界面上手工设置用户属性，逐个创建用户。

- 如果需要自定义用户角色，请先配置用户角色权限。
- 如果需要自定义用户属性，请先配置用户属性。
- 如果需要使用其他身份验证方式，请先配置，具体请参见：
  - 登录认证：配置AD认证
  - 登录认证：配置LDAP认证
  - 登录认证：配置RADIUS认证
  - 登录认证：配置动态令牌认证（TOTP）
  - 登录认证：配置手机令牌认证
  - 登录认证：配置短信认证
  - 登录认证：配置X.509证书认证
  - 登录认证：配置USB Key认证

1. 选择**用户** > **用户管理** > **用户列表**。
2. 单击**新建用户**，选择用户角色，单击**下一步**。

   超级管理员可以创建所有角色的用户，配置管理员可以创建操作员角色的用户。

3. 配置**帐号**、**姓名**和**身份验证**和**Web登录是否验证X.509证书**。

参数	**说明**
帐号	用户的帐号。字符串格式，长度范围是1~100个字符，不能包含"+"、":"、"/"、空格和中文字符。
姓名	用户的姓名。字符串格式，长度范围是1~100个字符。
身份验证	用户的身份验证方式，缺省值为**本地密码**。 如果要修改本地密码的最小长度、复杂程度等参数时，请参见登录认证：配置本地密码参数。
Web登录是否验证X.509证书	配置X.509证书认证后，新建/修改用户时就可以选择是否验证X.509证书。

4. 根据不同的身份验证方式，选择设置相应的参数。

- 本地密码或者包含本地密码的双因子身份验证方式：

参数	**说明**
密码类型	设置本地密码的方式，包括： • 手工输入：由管理员手工输入密码。 • 自动设置：由RIS自动生成密码。 自动生成的密码会以邮件的方式发送给用户，请正确配置用户的工作邮箱（见下一步）和配置邮件服务。 本地密码的最小长度、复杂度、有效期限等配置请参见登录认证：配置本地密码参数。
下次登录时必须修改密码	如果选中，用户首次登录时需要修改密码。缺省为选中。

- RADIUS和AD/LDAP等第三方服务器身份验证方式：

  以RADIUS为例，如果上一步配置的帐号与RADIUS服务器上的用户名相同，可以不配置**RADIUS用户名**，RIS缺省以上一步配置的帐号登录RADIUS服务器；如果帐号和RADIUS用户名不同，请在**RADIUS用户名**输入RADIUS服务器上的用户名，这样就建立起RIS帐号和RADIUS服务器用户名之间的关联关系。用户使用RIS帐号登录后自动使用关联的RADIUS用户名登录RADIUS服务器。

  AD/LADP服务器的**LDAP用户名**情况与RADIUS相同。

- 动态令牌或者包含动态令牌的双因子身份验证方式：

参数	说明
令牌号	请选择RIS已添加的动态令牌。如何配置动态令牌请参见配置动态令牌。 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RIS使用**PIN1码+动态密码**。 PIN码的最小长度、复杂度、有效期限与本地密码相同，具体等配置请参见登录认证：配置本地密码参数。
PIN2/确认PIN2	在会话复核中，包含动态令牌身份验证的用户作为复核人，当操作用户发起会话时，复核人和操作用户都会收到通知消息。如果复核人不方便执行复核操作，可以将**PIN2码+动态密码**告诉操作用户。操作用户打开通知消息，输入**PIN2码+动态密码**即可完成复核。具体请参见执行高危操作。
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。

说明： 使用动态令牌认证时，输入的密码是一个拼接起来的字符串，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。

5. 设置其他参数。

参数	说明
手机号码	用户的手机号码。
工作邮箱	用户的邮箱地址，长度范围是1~64个字符。
用户组	用户所属的分组。用户组的具体配置请参见配置用户组。
部门	用户所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。

6. 如果配置了自定义用户属性，请先单击**下一步**设置各参数，然后单击**创建**；如果没有配置自定义用户属性，直接单击**创建**。

用户配置完成后，您可以继续执行以下操作：

- 如果需要修改用户的状态、帐号有效期、密码有效期等高级属性，请参见修改用户属性。
- 如果要删除用户，请单击用户对应的**编辑**，然后单击**删除**。如果需要批量删除用户，请勾选所有待删除的用户后，单击**批量删除**。
- 如果要导出用户，请单击**导出全部**来导出全部用户，或者选中用户的复选框后单击**导出选中**。

配置用户（批量导入）

RIS支持从Excel文件中批量导入用户。导入RIS的用户缺省角色是操作员，状态是活动。

- 如果需要自定义用户属性，请先配置用户属性。
- 如果需要使用其他身份验证方式，请先配置，具体请参见：
  - 登录认证：配置AD认证
  - 登录认证：配置LDAP认证
  - 登录认证：配置RADIUS认证
  - 登录认证：配置动态令牌认证（TOTP）
  - 登录认证：配置手机令牌认证
  - 登录认证：配置短信认证
  - 登录认证：配置双因子认证
  - 登录认证：配置X.509证书认证
  - 登录认证：配置USB Key认证

1. 选择**用户** > **用户管理** > **用户列表**。
2. 单击**批量导入**，请先选择**身份验证**方式，然后设置各参数，完成后单击**下一步**。
   - 本地密码或者包含本地密码的双因子身份验证方式：

参数	说明
Web登录是否验证X.509证书	配置X.509证书认证后，导入用户时就可以选择是否验证X.509证书。
设置密码	• 不选中**设置密码**，则RIS自动生成的缺省密码是**123456**，用户第一次登录时需要修改密码。 • 选中**设置密码**，选择以下方法之一来设置密码，用户第一次登录时需要修改密码。 • 手工输入：由管理员手工输入密码。 • 自动设置：由RIS自动生成密码。 自动生成的密码会以邮件的方式发送给用户，请正确配置用户的工作邮箱和基本设置：配置邮件服务。
密码有效期	密码的有效期。取值包括：不限、30天、90天、180天、360天、同系统配置。缺省值为**同系统配置**

参数	说明
	密码有效期的系统配置和过期处理方式请参见登录认证：配置本地密码参数。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切换，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。

- RADIUS和AD/LDAP等第三方服务器身份验证方式：

参数	说明
Web登录是否验证X.509证书	配置X.509证书认证后，导入用户时就可以选择是否验证X.509证书。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切换，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。

- 动态令牌或者包含动态令牌的双因子身份验证方式：

参数	说明
Web登录是否验证X.509证书	配置X.509证书认证后，导入用户时就可以选择是否验证X.509证书。
PIN1/确认PIN1	用户自己登录RIS使用**PIN1码+动态密码**。 PIN码的最小长度、复杂度、有效期限与本地密码相同，具体等配置请参见登录认证：配置本地密码参数。

参数	说明
	说明: 批量导入时不支持导入**pin2码**。
下次登录时必须修改PIN1码	如果选中，用户下次登录时需要修改PIN1码。缺省为选中。
密码有效期	密码的有效期。取值包括：不限、30天、90天、180天、360天、同系统配置。缺省值为**同系统配置**。 密码有效期的系统配置和过期处理方式请参见登录认证：配置本地密码参数。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切换，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。

3. 单击**下载模板**，将模板文件保存到本地PC。
4. 打开本地模板文件，设置各参数，完成后保存文件。

参数	说明
帐号	用户的帐号，字符串格式，长度范围是1~100个字符，不能包含"+"、":"、"/"、空格和中文字符。帐号全局唯一，如果和已有帐号相同则会导入失败。该项必填。 RIS一次性导入的用户数最多是5000个，用户数大于5000时请分批导入。
姓名	用户的姓名，字符串格式，长度范围是1~100个字符。该项必填。
工作邮箱	用户的邮箱地址，长度范围是1~64个字符。如果用户需要接收通知邮件时，该项必填。
用户组	用户所属的分组，该项选填。 如果导入的分组不存在，RIS将会创建该分组。同一用户可加入多个用户组，多个用户组之间请使用","分隔。
手机号码	用户的手机号码。如果身份验证方式中包含短信认证时，该项必填。

参数	说明
令牌号	如果身份验证方式是动态令牌，RIS上已添加的动态令牌会显示在模板文件中，一个令牌只能和一个用户关联。
自定义用户属性	如果已配置自定义用户属性，这些属性会显示在模板文件中。

5. 单击**上传文件**，选择编辑好的模板文件，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。

6. 可选： 单击**下载导入结果**，查看导入的帐号。

用户配置完成后，您可以继续执行以下操作：

- 如果需要修改用户的状态、帐号有效期、密码有效期等高级属性，请参见修改用户属性。
- 如果要删除用户，请单击用户对应的**编辑**，然后单击**删除**。如果需要批量删除用户，请勾选所有待删除的用户后，单击**批量删除**。
- 如果要导出用户，请单击**导出全部**来导出全部用户，或者选中用户的复选框后单击**导出选中**。

配置用户（LDAP导入）

RIS支持导入LDAP用户。导入RIS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认证或者配置AD认证，如果使用其他认证方式，不需要配置LDAP认证和AD认证。

如果希望能定期将LDAP服务器上增、删、改的用户同步到RIS上，请配置LDAP用户定期同步。如果希望LDAP用户能够直接登录RIS，请在配置LDAP认证时选中**新用户自动加入系统**。

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。

参数	说明
LDAP地址	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**。 • 只支持配置一台LDAP服务器。
认证方式	• 如果LDAP服务器允许匿名访问，请选中**匿名认证**。

参数	说明
	• 如果LDAP服务器不允许匿名访问，请选中**密码认证**，并设置**bindDN**和**密码**。 **说明:** LDAP服务器上可使用ldapsearch获取bindDN,AD服务器上可使用dsquery获取bindDN。
baseDN	登录RIS的用户DN的范围，例如"dc=mydomain,dc=org"。
objectClass	选择设置LDAP对象类。
memberOf	选择设置用户所属的分组。
过滤条件	设置过滤条件来筛选用户，过滤条件的语法请参考RFC4515。

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	RIS的客户端证书CERT，单击**浏览**选择文件上传。 如果服务器端不要求对客户端认证，可以不提供。
KEY	RIS的客户端证书对应的KEY，单击**浏览**选择文件上传。 如果服务器端不要求对客户端认证，可以不提供。
允许忽略无效证书	如果选中，RIS不对LDAP服务器的证书进行合法性检查；如果不选，RIS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	说明
帐号	设置将LDAP服务器上的用户的什么属性作为RIS的帐号，缺省值为AD中的用户名字段**sAMAccountName**。 **说明:** Open LDAP中用户名对应的字段为**uid**，如果是Open LDAP服务器且仍使用用户名字段作为帐号，此处就要修改为**uid**。
姓名	设置将LDAP服务器上的什么属性作为RIS的姓名，缺省值为**displayName**。
工作邮箱	设置将LDAP服务器上的什么属性作为RIS的工作邮箱，缺省值为**mail**。

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**。

参数	说明
身份验证	用户的身份验证方式。如果RIS已配置LDAP认证或者已配置AD认证，缺省值为**AD/LDAP**，否则缺省值为**本地密码**。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切换，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。

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RIS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，请参见修改用户属性。

修改用户属性

创建用户后，管理员可以修改用户的基本属性、自定义用户属性和高级属性。

修改单个用户的属性

1. 选择**用户** > **用户管理** > **用户列表**，单击帐号对应的**编辑**。
2. 可选： 选择**基本属性**，修改角色、手机号码、工作邮箱、用户组等基本用户属性。
3. 可选： 选择**用户属性**，修改自定义用户属性。
4. 选择**高级属性**，设置各参数，完成后单击**保存**。

参数	说明
状态	用户的状态，包括**活动**和**禁用**，缺省为**活动**。

参数	说明
	说明：用户的状态设置为**禁用**时，在线会话会在1分钟内被切断。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切断，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。
密码有效期	如果身份验证选择的是本地密码或者包含本地密码的双因子认证，需要设置密码有效期。取值包括：不限、30天、90天、180天、360天、同系统配置。缺省值为**同系统配置**。 密码有效期的系统配置和过期处理方式请参见登录认证：配置本地密码参数。
用户登录控制	允许或禁止用户登录RIS的时间、IP地址和MAC地址范围，各参数含义与全局配置相同，全局配置请参见配置全局用户登录控制。 单个用户登录控制的优先级高于全局配置。对于单个用户来说： • 如果选择**启用**，则用户使用此处配置的参数。 • 如果选择**禁用**，则用户使用全局配置。
备注	用户的备注信息。

批量修改多个用户的属性

1. 选择**用户** > **用户管理** > **用户列表**。
2. 选中需要修改属性的用户。
3. 单击**批量编辑**，设置各参数，完成后单击**保存**。

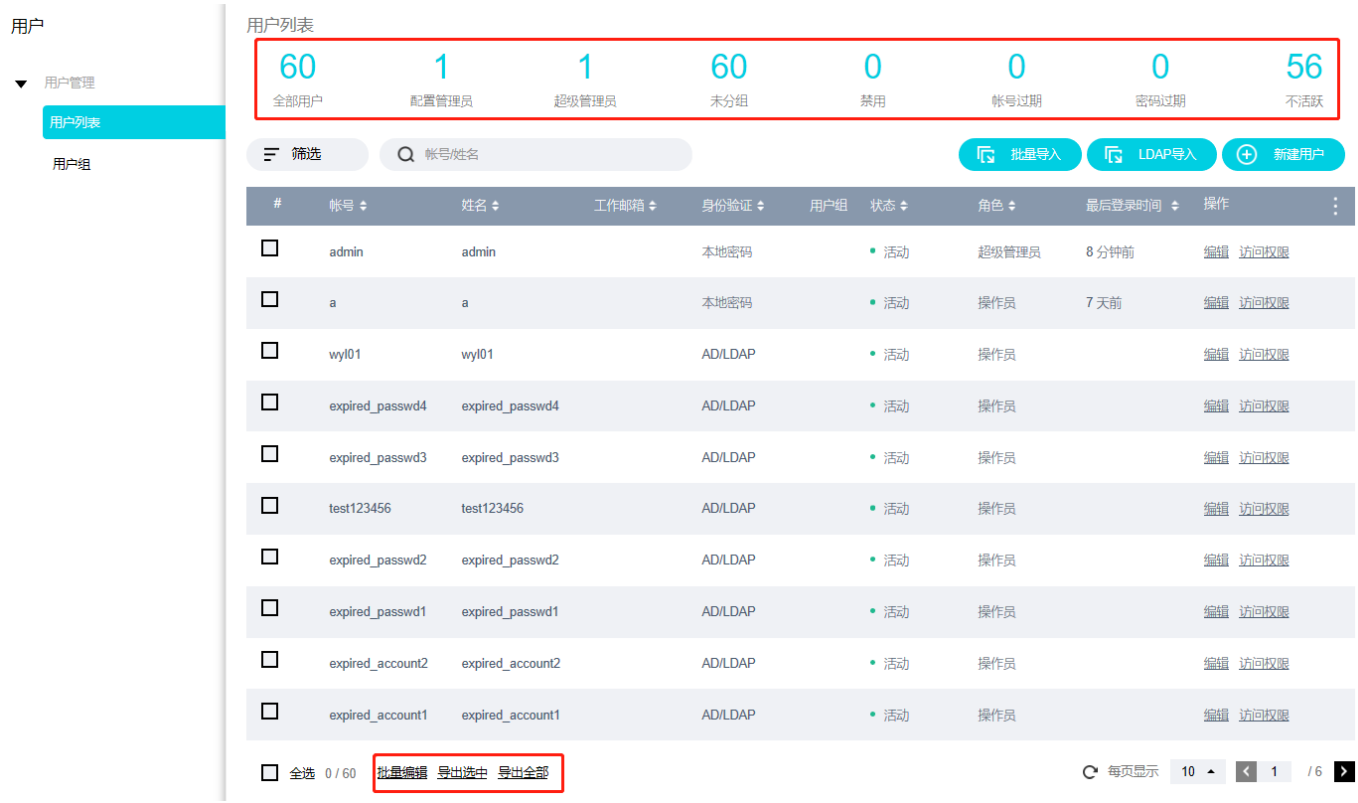
参数	说明
角色	用户的角色。
用户组	用户所属的组。
状态	用户的状态，取值包括**活动**和**禁用**。

参数	说明
	说明: 用户的状态设置为**禁用**时，在线会话会被切断。
身份验证	用户的身份验证方式。如果选择**本地密码**，需要同时设置密码。
Web登录是否验证X.509证书	是否验证用户的X.509证书。
帐号有效期	帐号在RIS上的有效期限。取值包括： • 长期有效 • 指定日期有效（精确到时/分） 如果选择**指定日期有效**，请选择生效开始和结束日期、时和分。 用户的帐号到期时，状态显示为**帐号过期**，在线会话会被切换，用户登录时提示**帐号状态异常**，无法登录。 对于已经过期的帐号，管理员可以修改帐号的有效期，修改后立即生效。

查看用户

本节介绍如何查看用户的信息和状态。

1. 选择**用户** > **用户管理** > **用户列表**，查看用户的信息。



2. 界面上方列出用户的统计信息，单击对应的快捷标签可以查看满足该条件的用户。例如上图中配置管理员有1个，单击**配置管理员**后用户列表仅显示这一个配置管理员。

   RIS最多支持8个快捷标签，缺省如下。

   - 全部用户
   - 配置管理员
   - 超级管理员
   - 未分组
   - 禁用
   - 帐号过期
   - 密码过期
   - 不活跃：包括近3个月未登录RIS和从未登录RIS的用户。

3. 单击左上角的**筛选**，使用用户属性设置筛选条件，完成后单击**筛选**，可以查看满足条件的用户。

   设置完筛选条件后，还可以单击**保存至快捷**将该筛选条件保存为快捷标签，方法如下：

   1. 单击**保存至快捷**。如快捷标签已达到8个，需要在弹出的菜单中单击**移除**，并勾选待移除的快捷标签，并重新单击**保存至快捷**。
   2. 输入**快捷名称**，并单击**保存**，生成新的快捷标签。

4. 在搜索框中输入帐号或者姓名的关键字，可以查看满足条件的用户。

设置完搜索条件后，还可以单击**保存至快捷**将该搜索条件保存为快捷标签。

5. 单击**导出全部**，将全部用户信息导出为Excel文件保存在本地PC；或者选择帐号对应的复选框单击**导出选中**。
6. 单击帐号对应的**访问权限**，查看用户关联的资产访问权限。

配置用户组

用户组是指将具有相同权限的用户划为一组，配置权限时基于组来配置，从而减轻管理员的配置负担。一个用户可以加入多个组。

用户组的创建方式包括：

- 手工创建用户组，本节将进行详细描述。
- 批量导入用户时自动创建用户组，具体请参见配置用户（批量导入）。

将用户加入用户组的方式有两种。

- 先创建用户组，然后在创建用户的时候选择预先创建好的用户组。
- 先创建用户，然后在创建用户组的时候关联预先创建好的用户。

配置完用户组后，就可以在配置权限、会话复核、命令复核等时直接引用用户组。

1. 选择**用户** > **用户管理** > **用户组**。
2. 单击+，设置各参数，完成后单击**创建**。

参数	**说明**
分组名	用户组的名称。字符串格式，长度范围是1~30个字符。
部门	用户组所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。

3. 单击用户组名称，然后单击**关联用户**。
4. 可选： 单击**筛选**，设置各参数，完成后单击**筛选**。

说明:

1. 配置筛选条件时，用户的属性都可以作为参数，且支持关键字匹配。例如在帐号中输入**ad**，则包含**ad**的帐号都会被筛选出来。
2. 各筛选条件之间是与的关系，即用户要同时满足设置的所有条件才能被筛选出来。

参数	**说明**
帐号	用户帐号包含的关键字。
姓名	用户姓名包含的关键字。

参数	说明
工作邮箱	用户工作邮箱包含的关键字。
用户组	用户所属的用户组，可以选择多个。
状态	用户的状态，包括：活动、密码过期、帐号过期和禁用。
角色	用户的角色。
最后登录时间	用户的最后登录时间范围。
部门	用户所属的部门。

5. 选中要关联的用户，单击**关联**。

- 您可以单击用户对应的**移除关联**，或者选中多条用户后单击**批量移除关联**，将用户从当前所属的用户组中删除。
- 您可以将鼠标指向用户组名称，单击修改名称，或者单击删除用户组。

资产管理

3

目录:

资产是被管理设备在RIS上的称谓，包含资产名称、IP、系统帐号等多种属性。RIS支持多种资产配置方式。

资产类型

为了便于管理，RIS将资产进行了分类，具体如表 5: 网络资产所示。如果RIS内置的资产类型不满足需求时，请自定义资产类型。

表 4: 主机资产

资产类型	访问方式
Linux	字符终端访问协议：SSH / Telnet 图形终端访问协议：VNC / XDMCP / XFWD
HP UX	
IBM AIX	
Windows	图形终端访问协议：RDP

表 5: 网络资产

资产类型	访问方式
Cisco IOS	字符终端访问协议：SSH / Telnet
Huawei Quidway	
Juniper NetScreen	
H3C Comware	
General Network	

表 6: 数据库资产

资产类型	访问方式
Oracle	客户端软件：Toad / plsqldev / SqlDbx / sqlplusw / sqldeveloperW / oem
MYSQL	客户端软件：navicat / SQLyog

资产类型	访问方式
MSSQL	客户端软件：Ssms
DB2	客户端软件：SqlDbxForDB2 / QuestCentral / ToadForDB2

表 7: 应用系统资产

资产类型	访问方式
B/S	客户端软件：Chrome / Firefox
C/S	客户端软件：Radmin / SQLAdvantage / SybaseCentral4.3 / VpxClient / asdm / vncviewer
Weblogic	客户端软件：Chrome / Firefox
B/S IE	客户端软件：Internet Explore

资产属性

不同类型的资产，包含的属性也不相同，RIS支持的常见属性如表 8: 常见资产属性所示。如果RIS预定义的资产属性不满足需求时，请自定义资产的属性。

表 8: 常见资产属性

参数	说明
资产名称	资产的名称，要求在RIS中唯一。
资产IP和端口	资产的IP地址和端口。
部门	资产所属的部门。
资产组	资产所属的资产组。资产组是资产的一种组织形式，相同权限的资产可以划分到同一个分组。配置权限时就能够以资产组为单位而不是资产，可有效减轻配置负担。
脚本类型	访问资产使用的脚本类型，一般用于应用系统。
访问协议	访问资产使用的协议，一般用于主机和网络设备。
客户端	访问资产使用的客户端，一般用户数据库和应用系统。例如：Firefox、Chrome、Internet Explorer。
帐号和密码	访问资产使用的帐号和密码。
系统编码	资产使用的系统编码。

资产创建方式

RIS支持以下几种资产创建方式：

- **批量导入**：先按照RIS提供的模板填写资产的参数，然后导入。
- **手工添加**：在RIS的Web界面上填写资产的参数，手工创建资产。

资产创建后，需要继续配置资产的访问协议、系统帐号和密码。支持的配置方法包括批量配置（批量导入）和逐条配置。配置完成后，可以进行登录测试或者代填测试。

- **登录测试**：RIS使用帐号和密码直接访问资产，一般用于主机和网络设备。
- **代填测试**：RIS模拟用户实际的访问过程，包括打开访问协议或者客户端，自动填入用户名和密码访问资产，一般用于数据库和应用系统，在配置资产的基本信息时需要指定代填脚本类型。

说明:

- 登录测试和代填测试弹出的界面仅用于查看测试结果，不能进行交互操作。
- 执行登录测试或者代填测试时，如果在填写帐号和密码前弹出其他提示，由于不能进行交互操作，因此无法完成测试。

配置资产

在RIS上配置资产的基本属性、访问协议、帐号和密码。

配置资产（手工创建）

在RIS的Web界面上手工设置资产属性，逐个创建资产。

- 如果需要自定义资产类型，请先配置资产类型。
- 如果需要自定义资产属性，请先配置资产属性。

配置主机和网络资产

RIS缺省支持的主机资产类型包括**HP UX**、**IBM AIX**、**Windows**和**Linux**。

RIS缺省支持的网络资产类型包括**Cisco IOS**、**Huawei Quidway**、**Juniper NetScreen**、**H3C Comware**和**General Network**。

1. 选择**资产** > **资产清单** > **网络**。

   如果配置主机资产，请选择**资产** > **资产清单** > **主机**。

2. 单击**新建**。
3. 选择资产类型，单击**下一步**。
4. 设置各参数。

参数	说明
资产名称	资产的名称，字符串格式，长度范围是1~100个字符。
资产IP	资产的IP地址，IPv4和IPv6都支持。单击**ping**可以进行连通性测试。
简要说明	资产的简要说明。
部门	资产所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。

参数	说明
资产组	资产所属的分组。资产组的具体配置请参见配置资产组。
系统编码	资产使用的系统编码类型，取值包括ISO-8859-1、GB18030、UTF-8等。如果系统编码选择不正确，可能会出现以下异常问题： • 资产访问异常 • 改密不成功 • 文件传输时文件名出现乱码 • 查看审计日志时出现乱码 • 高危命令中对命令识别错误
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。

5. 如果配置了自定义资产属性，请先单击**下一步**设置各参数，然后单击**创建**；如果没有配置自定义资产属性，直接单击**创建**。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

  说明： 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的访问协议，请参见配置资产的访问协议
- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

配置数据库资产

RIS缺省支持的数据库类型包括**Oracle**、**MYSQL**、**MSSQL**和**DB2**。

1. 选择**资产** > **资产清单** > **数据库**。
2. 单击**新建**。
3. 选择资产类型，单击**下一步**。
4. 设置各参数。

参数	说明
资产名称	资产在RIS上的名称。字符串格式，长度范围是1~100个字符。

参数	说明
数据库名（**MySQL**和**DB2**）	数据库的名称。字符串格式，长度范围是1~30个字符。

连接方式（**Oracle**）	数据库的连接方式，包括：
	• **服务名**：使用数据库的ServiceName连接。执行以下命令可以获得服务名。
	`select value from v$parameter where name = 'service_names';`
	• **SID**：使用数据库的SID连接。执行以下命令可以获得SID。
	`select instance_name from v$instance;`
	• **TNS**：使用数据库的TNSName连接。请确保TNS配置串的格式正确，示例如下。
	(DESCRIPTION =(ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCP)(HOST = 10.10.16.81)(PORT = 1521)))(CONNECT_DATA =(SERVICE_NAME = devdb)))

资产IP	资产的IP地址和服务端口，IPv4和IPv6都支持。
OEM URL	Oracle Enterprise Manager的URL地址。如果**客户端**中选择了**oem**，则同时必须填写**OEM URL**。
实例名（**MSSQL**）	数据库的实例名，包括默认实例和自定义实例。字符串格式，长度范围是1~30个字符。
简要说明	资产的简要说明。
部门	资产所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。
资产组	资产所属的分组。资产组的具体配置请参见配置资产组。
客户端	访问资产使用的客户端软件。
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。

5. 如果配置了自定义资产属性，请先单击**下一步**设置各参数，然后单击**创建**；如果没有配置自定义资产属性，直接单击**创建**。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

说明： 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

配置应用系统资产

RIS缺省支持的应用系统类型包括**B/S**、**C/S**、**Weblogic**和**B/S IE**。

1. 选择**资产** > **资产清单** > **数据库**。
2. 单击**新建**。
3. 选择资产类型，单击**下一步**。
4. 设置各参数。

参数	**说明**
资产名称	资产在RIS上的名称。字符串格式，长度范围是1~100个字符。
资产IP	资产的IP地址，IPv4和IPv6都支持。
URL（**B/S**、**B/S IE**和**Weblogic**）	资产的Web访问地址，支持HTTP和HTTPS两种格式。
脚本类型（**B/S**、**B/S IE**和**Weblogic**）	用户访问资产时是否由RIS代填登录信息（例如用户名和密码）。 • 不代填：用户自己填写用户名、密码等登录信息，不用RIS代填。 • 通用：用户名、密码等登录信息由RIS代填，且使用RIS预定义的通用代填脚本。 • 高级：用户名、密码等登录信息由RIS代填，且用户需要自定义代填脚本。需要自定义的参数包括： • 用户名输入框 • 密码输入框 • 登录按钮 • Iframe输入框 • 自定义：用户名、密码等登录信息由RIS代填，且用户需要上传自定义代填脚本（JSON格式）。
是否限制其他URL（**B/S**、**B/S IE**和**Weblogic**）	用户通过RIS访问目标资产的URL时能否在同一客户端访问其他地址。 • 限制：除了白名单内的URL，用户不能访问其他地址。 • 不限制：用户可以访问其他任意地址。

参数	说明
白名单（**B/S**、**B/S IE**和**Weblogic**）	**是否限制其他URL**选择了**限制**时，可以配置白名单。白名单表示除了URL以外允许用户访问的地址列表。配置白名单时请使用正则表达式，一个地址一行，可配置多行。
简要说明	资产的简要说明。
部门	资产所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。
资产组	资产所属的分组。资产组的具体配置请参见配置资产组。
客户端	访问资产使用的客户端软件。选择客户端软件后，需要设置对应的代填参数，确保RIS能代填成功。
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。
port（**C/S**）	资产的服务端口。当**客户端**选择的是代填脚本支持自定义端口号的软件时（例如**vncviewer**、**SybaseCentral4.3**和**Radmin**），请在此配置资产的端口，确保RIS能代填成功。
codepage（**C/S**）	资产使用的字符集。当**客户端**选择的是代填脚本支持自定义字符集的软件时（例如**SybaseCentral4.3**），请在此配置资产使用的字符集，确保RIS能代填成功。

5. 如果配置了自定义资产属性，请先单击**下一步**设置各参数，然后单击**创建**；如果没有配置自定义资产属性，直接单击**创建**。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

  说明： 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

配置资产（批量导入）

RIS支持从Excel文件中批量导入资产，导入RIS的资产缺省状态是**活动**。

- 如果需要自定义资产类型，请先配置资产类型。
- 如果需要自定义资产属性，请先配置资产属性。

导入主机和网络资产

RIS缺省支持的主机资产类型包括**HP UX**、**IBM AIX**、**Windows**和**Linux**。

RIS缺省支持的网络资产类型包括**Cisco IOS**、**Huawei Quidway**、**Juniper NetScreen**、**H3C Comware**和**General Network**。

1. 选择**资产** > **资产清单** > **网络**。

   如果配置主机资产，请选择**资产** > **资产清单** > **主机**。

2. 单击**批量导入**，选择**新增模式**或者**编辑模式**。

   说明:

   - **新增模式**：表示批量导入新资产。
   - **编辑模式**：表示批量修改已有资产的属性。

3. 单击**下载模板**，将模板文件保存到本地PC。

4. 打开本地模板文件，设置各参数，完成后保存文件。

   说明: 如果是在编辑模式中修改已有资产的属性请注意：

   - **资产名称**和**资产IP**必须输入正确，否则导入时RIS会提示资产不存在。
   - 需要修改的资产属性，单元格中输入修改后的值；不需要修改的资产属性，单元格保持为空即可；需要清空的资产属性，单元格中输入**NULL**。

参数	说明
资产名称	资产的名称，字符串格式，长度范围是1~100个字符。
资产IP	资产的IP地址，IPv4和IPv6都支持。
资产类型	资产的类型。
部门	资产所属的部门。
编码类型	资产的编码类型。对于主机来说，缺省取值包括： • GB18030 • ISO-8859-1 • US-ASCII • UTF-8 • IBM1388
简要说明	资产的简要说明。

参数	说明
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。
资产组	资产所属的资产组。如果导入的分组不存在，RIS将会创建该分组。同一资产可加入多个资产组，多个资产组之间请使用","分隔。
帐号名	访问该资产的帐号名，最多填写一个。可以不填，表示仅导入资产不导入帐号。 **说明:** 如果需要导入同一个资产的多个帐号，请参考批量导入帐号和密码。
密码	仅当填写了**帐号名**参数时填写，用于设置该帐号名对应的密码。可以不填，表示不托管密码。
是否特权	• **是**：将导入的帐号设为特权帐号。 • **否**：将导入的帐号设置为普通帐号。
自定资产属性	如果已配置自定义资产属性，这些属性会显示在模板文件中。

5. 单击**上传文件**，选择编辑好的模板文件，完成后单击**关闭**。

   说明: 对于文件中数据正确的资产，RIS会直接导入；对于数据不正确的资产，RIS在列表中显示。如果需要继续导入，请单击错误数据并直接编辑，然后单击**开始导入**。如果不需要导入，请直接单击资产对应的，从列表中删除该资产。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

  说明: 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的访问协议，请参见配置资产的访问协议
- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

导入数据库资产

RIS缺省支持的数据库类型包括**Oracle**、**MYSQL**、**MSSQL**和**DB2**。

1. 选择**资产** > **资产清单** > **数据库**。
2. 单击**批量导入**，选择**新增模式**或者**编辑模式**。

说明:

- **新增模式**：表示批量导入新资产。
- **编辑模式**：表示批量修改已有资产的属性。

3. 选择资产类型，单击**下一步**。
4. 单击**下载模板**，将模板文件保存到本地PC。
5. 打开本地模板文件，设置各参数，完成后保存文件。

说明: 如果是批量修改已有资产的属性请注意：

- **资产名称**和**资产IP**必须输入正确，否则导入时RIS会提示资产不存在。
- 需要修改的资产属性，单元格中输入修改后的值；不需要修改的资产属性，单元格保持为空即可；需要清空的资产属性，单元格中输入**NULL**。

参数	说明
资产名称	资产的名称，字符串格式，长度范围是1~100个字符。

连接方式（**Oracle**）	数据库的连接方式，包括：
	• **服务名**：使用数据库的ServiceName连接，必须填写**资产IP**和**服务名**。执行以下命令可以获得服务名。
	`select value from v$parameter where name = 'service_names';`
	• **SID**：使用数据库的SID连接，必须填写**资产IP**和**SID**。执行以下命令可以获得SID。
	`select instance_name from v$instance;`
	• **TNS**：使用数据库的TNSName连接，必须填写**资产IP**和**配置串**。请确保TNS配置串的格式正确，示例如下。
	(DESCRIPTION =(ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCP)(HOST = 10.10.16.81)(PORT = 1521)))(CONNECT_DATA =(SERVICE_NAME = devdb)))

部门	资产所属的部门。
资产IP	资产的IP地址，IPv4和IPv6都支持。
端口	数据库服务的端口。各种数据库类型的缺省端口如下： • Oracle：1521 • MYSQL：3306 • MSSQL：1433

参数	说明
	• DB2：50000
实例名（**MSSQL**）	数据库的实例名，包括默认实例和自定义实例。字符串格式，长度范围是1~30个字符。
数据库名（**MySQL**和**DB2**）	数据库的名称。字符串格式，长度范围是1~30个字符。
客户端	访问资产使用的客户端软件，多个软件使用“,”分隔。
简要说明	资产的简要说明。
OEM URL（**Oracle**）	Oracle Enterprise Manager的URL地址。如果**客户端**中填写了**oem**，则同时必须填写**OEM URL**。
资产组	资产所属的资产组。如果导入的分组不存在，RIS将会创建该分组。同一资产可加入多个资产组，多个资产组之间请使用","分隔。
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。
帐号名	访问该资产的帐号名，最多填写一个。可以不填，表示仅导入资产不导入帐号。 **说明:** 如果需要导入同一个资产的多个帐号，请参考批量导入帐号和密码。
密码	仅当填写了**帐号名**参数时填写，用于设置该帐号名对应的密码。可以不填，表示不托管密码。
角色（**Oracle**）	用户的角色。取值包括：**SYSDBA**、**SYSOPER**和**Normal**。缺省值为**SYSDBA**。
是否特权	• **是**：将导入的帐号设为特权帐号。 • **否**：将导入的帐号设置为普通帐号。
自定资产属性	如果已配置自定义资产属性，这些属性会显示在模板文件中。

6. 单击**上传文件**，选择编辑好的模板文件，完成后单击**关闭**。

说明: 对于文件中数据正确的资产，RIS会直接导入；对于数据不正确的资产，RIS在列表中显示。如果需要继续导入，请单击错误数据并直接编辑，然后单击**开始导入**。如果不需要导入，请直接单击资产对应的，从列表中删除该资产。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

  说明: 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

导入应用系统资产

RIS缺省支持的应用系统类型包括**B/S**、**C/S**、**Weblogic**和**B/S IE**。

1. 选择**资产** > **资产清单** > **应用系统**。
2. 单击**批量导入**，选择**新增模式**或者**编辑模式**。

   说明:

   - **新增模式**：表示批量导入新资产。
   - **编辑模式**：表示批量修改已有资产的属性。

3. 选择资产类型，单击**下一步**。
4. 单击**下载模板**，将模板文件保存到本地PC。
5. 打开本地模板文件，设置各参数，完成后保存文件。

   说明: 如果是批量修改已有资产的属性请注意：

   - **资产名称**和**资产IP**必须输入正确，否则导入时RIS会提示资产不存在。
   - 需要修改的资产属性，单元格中输入修改后的值；不需要修改的资产属性，单元格保持为空即可；需要清空的资产属性，单元格中输入**NULL**。

参数	说明
资产名称	资产在RIS上的名称。字符串格式，长度范围是1~100个字符。
资产IP	资产的IP地址，IPv4和IPv6都支持。
URL（**B/S**、**B/S IE**和**Weblogic**）	资产的Web访问地址，支持HTTP和HTTPS两种格式。
脚本类型（**B/S**、**B/S IE**和**Weblogic**）	用户访问资产时是否由RIS代填登录信息（例如用户名和密码）。 • 不代填：用户自己填写用户名、密码等登录信息，不用RIS代填。 • 通用：用户名、密码等登录信息由RIS代填，且使用RIS预定义的通用代填脚本。

参数	说明
	说明：不支持导入**高级**和**自定义**脚本类型的应用。
白名单（**B/S**、**B/S IE**和**Weblogic**）	白名单表示除了URL以外允许用户访问的地址列表。配置白名单时请使用正则表达式，一个地址一行，多个地址使用**ALT + Enter**换行，示例如下： http://www.myhost.com.* http://10.10.10.*
客户端	访问资产使用的客户端软件。
简要说明	资产的简要说明。
部门	资产所属的部门。
资产组	资产所属的资产组。如果导入的分组不存在，RIS将会创建该分组。同一资产可加入多个资产组，多个资产组之间请使用"**,**"分隔。
责任人	资产所属的责任人，责任人必须是在RIS上已存在的用户。
帐号名	访问该资产的帐号名，最多填写一个。可以不填，表示仅导入资产不导入帐号。 **说明：**如果需要导入同一个资产的多个帐号，请参考批量导入帐号和密码。
密码	仅当填写了**帐号名**参数时填写，用于设置该帐号名对应的密码。可以不填，表示不托管密码。
是否特权	• **是**：将导入的帐号设为特权帐号。 • **否**：将导入的帐号设置为普通帐号。
自定义资产属性	如果已配置自定义资产属性，这些属性会显示在模板文件中。

6. 单击**上传文件**，选择编辑好的模板文件，完成后单击**关闭**。

   说明：对于文件中数据正确的资产，RIS会直接导入；对于数据不正确的资产，RIS在列表中显示。如果需要继续导入，请单击错误数据并直接编辑，然后单击**开始导入**。如果不需要导入，请直接单击资产对应的，从列表中删除该资产。

   - 对于**B/S**、**B/S IE**和**Weblogic**，批量导入后**是否限制其他URL**的缺省值为**限制**，且**白名单**为空。
   - 对于**C/S**，批量导入后代填参数为空。

资产配置完成后，您可以继续执行以下操作：

- 如果要修改单个资产的状态（状态包括**活动**和**禁用**）和其他基本属性，请单击资产对应的**编辑**进行修改；如果要修改多个资产的属性，请选中资产对应的复选框，单击**批量编辑**。

  说明： 资产被禁用后，仍会占用资产的授权数量。如需使该资产不占用授权，请删除该资产。

- 如果要配置资产的帐号和密码，请参见配置资产的帐号和密码。
- 如果要删除单个资产，请单击资产对应的**编辑**，然后单击**删除**；如果要删除多个资产，请选中资产对应的复选框，单击**批量删除**。
- 如果要导出资产，请单击**导出全部**来导出全部资产，或者选中资产的复选框后单击**导出选中**。

配置资产的访问协议

创建主机和网络资产后，RIS会根据资产类型创建缺省的访问协议，您也可以修改访问协议的参数或者添加新的访问协议。配置方式支持批量和逐条配置两种。

RIS针对不同的资产类型提供了不同的访问协议，例如Windows主机支持的访问协议有RDP和VNC（缺省为RDP），Linux/Unix主机支持的访问协议有SSH、Telnet、VNC、XDMCP、XFWD（缺省为SSH和XDMCP）。超级管理员可以修改指定资产类型的访问协议和缺省值，具体请参见配置资产类型。

主机和网络设备支持配置协议，且配置的的方法类似，本文以主机设备为例介绍操作过程，并对差异进行说明。

批量配置访问协议

对于相同类型的资产，如果访问协议相同，可以采取批量配置一次性完成。批量配置资产的访问协议时，一次只能配置一个协议。如果配置的协议已存在，则会覆盖之前的配置。

1. 选择**资产** > **资产清单** > **主机**。

   如果配置网络资产，请选择**资产** > **资产清单** > **网络**。

2. 单击**协议配置**。
3. 单击**资产**对应的  ，选中资产（要求资产类型相同），单击**添加**。

   如果资产数量大，可通过以下方式查找满足条件的资产。

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

4. 选择要配置的协议，单击**下一步**。
5. 设置各参数，完成后单击**创建**。

表 9: 访问协议参数说明

参数	说明
名称	访问协议的名称，字符串格式，长度范围是1~30个字符，仅支持英文字符、数字、"-"和"_"。

参数	说明
说明	访问协议的说明。
状态	访问协议的状态。取值包括： • 活动 • 禁用
端口	访问协议的端口。单击**连通检测**，可以测试端口的连通状态。 **说明:** • 对于XDMCP协议，单击**端口侦听**，RIS会临时打开6999端口（时长为1分钟）供您在目标资产上连接,以测试目标设置到RIS的反向连接端口是否通畅。 • XFWD协议是基于SSH协议的，没有独立的端口，不需要配置此项。
Telnet/SSH	
跳转来源	跳转来源是指访问当前资产时从哪个设备使用哪个帐号跳转过来。例如当前设备是A，配置跳转来源为B，则用户先访问B，再从B自动跳转到A。 支持配置跳转来源的协议有SSH和Telnet，且支持自定义协议端口。RIS不支持多级跳转，即被配置为跳转来源的设备不能再配置跳转来源。 作为跳转来源的设备需满足如下条件： • 资产类型是主机，且资产状态是活动的。 • 已配置SSH或者Telnet，且状态是活动的。 • 帐号有密码或者密钥且没有配置切换自。
RDP	
Console	相当于Windows中mstsc的/console或者/admin选项，表示是否允许普通用户连接服务器的控制台会话（session id=0）。
VNC	
enterprise商业版	RIS支持Real VNC，且缺省情况下支持的是VNC Open版本，如果目标设备采用的是VNC Enterprise Edition，请选中此项。
VNC密码	VNC服务器端的密码。
XFWD	

参数	说明
xfwd_cmdline命令	如果用户使用SSH X forwarding协议访问目标设备，部署RIS后，需要在RIS上增加访问协议XFWD，并且需要满足以下条件： • 目标设备的**sshd_config**配置文件中**X11Forwarding**的取值是**yes**。 • 已为资产配置了访问协议SSH，且没有配置**来源设备**和**跳转自**。 **xfwd_cmdline命令**中可以设置服务端执行的命令来进入相应的界面，示例如下。 **说明:** 要求目标设备上已经安装**gnome**、**xfce4**或者**xterm**软件。 • 进入图形界面： • /usr/bin/gnome-session • /usr/bin/xfce4-session • 进入字符界面： • /usr/bin/xfce4-terminal • /usr/bin/gnome-terminal • xterm

逐条配置访问协议

1. 选择**资产** > **资产清单** > **主机**。
2. 单击资产对应的**编辑**。
3. 选择**访问协议**。
4. 单击已有访问协议对应的，设置各参数，完成后单击**确定**。

   参数说明如表 9: 访问协议参数说明所示。
5. 单击下拉列表框选择其他协议，单击**添加**，设置各参数，完成后单击**确定**。

   参数说明如表 9: 访问协议参数说明所示。
6. 单击**保存**。

配置资产的帐号和密码

创建资产后，用户可以在RIS上添加访问资产的帐号和密码，即将密码托管在RIS上，这样用户访问目标设备时由RIS代替用户输入帐号和密码。用户也可以只添加帐号或者帐号和密码都不添加，在访问目标设备时由用户手工输入。

RIS针对不同的资产类型提供了不同的缺省系统帐号，例如Windows主机的**administrator**，Linux主机的**root**。

超级管理员可以修改指定资产类型的缺省系统帐号，具体请参见配置资产类型。

创建资产时，RIS会根据资产的类型配置好帐号，用户可以增加新的帐号，也可以修改已有帐号的参数，配置方式支持批量导入和手工配置两种。

所有资产配置帐号的方法类似，本文以主机设备为例介绍操作过程，并对差异进行说明。

批量导入帐号和密码

批量导入帐号和密码用于一次性将相同类型资产的密码托管在RIS上的场景，RIS支持导入帐号的**密码**、**切换自**、**密钥**和**域名**信息。编辑模板文件时，确保至少有一项不能为空。

1. 选择**资产** > **资产清单** > **主机**。
2. 单击**密码导入**。
3. 单击**资产**对应的  ，选中资产，单击**添加**。

   如果资产数量大，可通过以下方式查找满足条件的资产。

   - 在搜索文本框中输入资产名称、IP或者简要说明的关键字。
   - 单击**筛选**，使用资产的属性设置过滤条件，单击**筛选**。
4. 选择或者输入帐号（不输或输入多个都可以），单击**下一步**。
5. 单击**下载模板**，将模板文件保存到本地PC。
6. 打开本地模板文件，设置各参数，完成后保存文件。

表 10: 资产的帐号和密码参数（手工批量导入）

参数	说明
资产名称	资产的名称。资产必须在RIS上已存在。
帐号	资产的帐号，字符串格式，长度范围是1~100，不能包含"**/**"和中文字符。如果同一个资产存在多个帐号，每个帐号占用表格的一行。如果与已有帐号相同，表示修改已有帐号的属性。 **说明:** Windows帐号不区分大小写。对于网络设备，如需添加null帐号，请将帐号名称填写为大写的NULL。
是否特权	该帐号是否为资产上的最高权限帐号，如果是请填写**是**，如果否请填写**否**。如果什么都不填写，表示保持原来的设置。
密码	帐号对应的密码。

参数	说明
支持Telnet/SSH访问协议的主机和网络设备 **说明：**对于SSH，如果要配置**切换自**，需要使用密码方式登录，不能使用密钥方式。	
切换自	切换自是指访问资产时从哪个帐号切换过来。例如当前帐号是A，切换自为B，则A用户访问资产时RIS会先使用B帐号登录，再切换到A帐号。用于A不能直接登录目标资产的场景。 支持配置切换自的协议包括SSH和Telnet，且支持自定义协议端口。 作为切换自的帐号和所在的资产需满足如下条件： • 资产类型为Linux、HP、IBM AIX等主机和网络设备。 • 已配置SSH或者Telnet。 • 有密码或者密钥。 **说明：**当配置的切换自帐号是普通帐号时，当前帐号必须有密码；当配置的切换自帐号是特权帐号时，当前帐号可以没有密码。 • 没有配置切换自。即不支持多级切换自，被配置为切换自的帐号不能再配置切换自。 RIS支持跳转来源和切换自结合使用，例如资产A跳转来源为资产B，对应资产A系统帐号root切换自资产B帐号admin。
密钥	对于支持SSH访问协议的Linux、HP、IBM AIX主机类资产和网络资产，使用密钥方式登录时，请填写密钥标识，密钥的配置请参见配置密钥。
Windows和MSSQL **说明：**如果同时配置了密码和域名，优先使用域名。	
域名	对于Windows域用户，请填写域名称，域的配置请参见配置Windows域。
Oracle	
角色	用户的角色。取值包括：**SYSDBA**、**SYSOPER**和**Normal**。缺省值为**SYSDBA**。

7. 单击**上传文件**，选择编辑好的模板文件，单击**开始导入**，完成后单击**关闭**。

说明：

- 不需要导入的帐号和密码，请直接单击帐号和密码对应的，从列表中删除该帐号和密码。

- 单击**下载导入结果**，查看导入的帐号和密码。

手工配置帐号和密码

1. 选择**资产** > **资产清单** > **主机**。
2. 单击资产对应的**编辑**。
3. 选择**系统帐号**。
4. 单击已有帐号对应的**编辑**，设置各参数，完成后单击**确定**。

表 11: 资产的帐号和密码参数（手工配置）

参数	说明
帐号名称	帐号的名称，字符串格式，长度范围是1~100，不能包含"**/**"和中文字符。 **说明:** 对于网络设备，如需添加null帐号，请将帐号名称填写为大写的NULL。
设为特权帐号	如果该帐号是目标资产上的特权帐号，请选中。
设置密码/确认密码	帐号对应的密码。
支持Telnet/SSH访问协议的主机和网络设备 **说明:** 对于SSH，如果要配置**切换自**，需要使用密码方式登录，不能使用密钥方式。	

参数	说明
切换自	切换自是指访问资产时从哪个帐号切换过来。例如当前帐号是A，切换自为B，则A用户访问资产时RIS会先使用B帐号登录，再切换到A帐号。用于A不能直接登录目标资产的场景。 支持配置切换自的协议包括SSH和Telnet，且支持自定义协议端口。 作为切换自的帐号和所在的资产需满足如下条件： • 资产类型为Linux、HP、IBM AIX主机和网络设备。 • 已配置SSH或者Telnet。 • 有密码或者密钥。 **说明：** 当配置的切换自帐号是普通帐号时，当前帐号必须有密码；当配置的切换自帐号是特权帐号时，当前帐号可以没有密码。 • 没有配置切换自。即不支持多级切换自，被配置为切换自的帐号不能再配置切换自。 RIS支持跳转来源和切换自结合使用，例如资产A跳转来源为资产B，对应资产A系统帐号root切换自资产B帐号admin。
私钥（仅SSH协议）	对于支持SSH访问协议的Linux、HP、IBM AIX主机类资产和网络资产，使用密钥方式登录时，请选择对应的密钥标识，密钥的配置请参见配置密钥。
Windows和MSSQL **说明：** 如果同时配置了密码和Domain，优先使用Domain。	
Domain	对于Windows域用户，请填写域名称，域的配置请参见配置Windows域。
Oracle	
角色	用的角色。取值包括：**SYSDBA**、**SYSOPER**和**Normal**。缺省值为**SYSDBA**。

5. 单击**添加帐号**，设置各参数，完成后单击**确定**。

   参数说明如表 11: 资产的帐号和密码参数（手工配置）所示。

6. 可选： 单击**登录测试**，选择访问协议（只有一种协议时不需要选择），单击**登录测试**。

   说明:

   - XDMCP协议不支持登录测试。
   - 主机、网络类设备执行的是登录测试，数据库和应用系统执行的是代填测试。

7. 单击**保存**。

配置资产组

RIS支持将多个资产划为一组，这样在配置动态权限、高危操作等时基于组来配置，从而减轻管理员的配置负担。一个资产可以加入多个资产组。

将资产加入资产组的方式有两种。

- 先创建资产组，然后在创建资产的时候选择预先创建好的资产组。
- 先创建资产，然后在创建资产组的时候关联预先创建好的资产。

配置资产组后，您可以在动态权限、高危命令、会话复核、改密计划等配置过程中直接引用资产组。

1. 选择**资产** > **资产清单** > **资产组**。
2. 单击＋，设置各参数，完成后单击**创建资产组**。

参数	**说明**
名称	资产组的名称。字符串格式，长度范围是1~30个字符。
简要描述	资产组的简要描述。字符串格式，长度范围是0~60个字符。
部门	资产组所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。

3. 选中资产组，然后单击**添加资产**。
4. 选中要添加的资产，单击**添加**。

   如果资产数量大，可通过以下方式查找满足条件的资产。

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

- 您可以单击资产对应的**移除关联**，或者选中多条资产后单击**批量移除关联**，将资产从当前所属的资产组中删除。
- 您可以将鼠标指向资产组名称，单击修改名称，或者单击删除资产组。

查看资产

本节介绍如何查看资产的信息和状态。

说明： 如果要查看全部资产的信息和状态，请在动态视图中查看，如果要查看特定类型的资产的信息和状态，请在该资产类型下查看，本机以查看主机类型的资产为例进行介绍，网络、数据库和应用系统的查看方法与主机相同。

1. 选择**资产** > **资产清单** > **主机**，查看资产的信息。

2. 界面上方列出资产的统计信息，单击对应的快捷标签可以查看满足该条件的资产。例如上图中Windows资产有2个，单击**Windows**后资产列表仅显示这2个Windows资产。

   RIS最多支持8个快捷标签，缺省的快捷标签为资产类型。

3. 单击左上角的**筛选**，使用资产属性设置筛选条件，完成后单击**筛选**，可以查看满足条件的资产。

   设置完筛选条件后，还可以单击**保存至快捷**将该筛选条件保存为快捷标签。例如筛选条件中将**是否禁用**设置为**禁用**，完成后单击**保存至快捷**，界面上方就会出现禁用的快捷标签，单击该标签可以快速查看所有被禁用的资产。

4. 在搜索框中输入资产名称、IP或者简要说明的关键字，可以查看满足条件的资产。

   设置完搜索条件后，还可以单击**保存至快捷**将该搜索条件保存为快捷标签。

5. 单击**导出全部**，将全部资产信息导出为Excel文件保存在本地PC；或者选择资产对应的复选框单击**导出选中**。

查看动态视图

RIS支持动态地展示资产层级结构以及各节点下的资产，并对资产进行查看、新建、编辑、删除、导出等操作。

RIS根据配置视图的层级中的层级结构展示所有资产，视图会根据层级关系的变化动态调整。动态视图的各个层级可以是不同的资产属性，也可以是部门的层级（必须完成了部门层级的配置）。本节以配置为不同的资产属性为例进行介绍。

对于作为动态视图层级节点的属性，如果资产的属性值为空时，RIS自动创建空节点与之对应。例如图 1: 菜单布局的动态视图中视图的层级中定义第1层节点为“责任人”，图中上面两个资产已配置责任人为admin，则这两个资产在**admin**节点下面，下面两个资产没有配置责任人，则在**空**节点下面。

动态视图有两种布局方式，一种是菜单，一种是树形。其中树形布局还能以横向或者纵向方式展示。在菜单布局下，单击 切换到树形布局；树形布局下单击 切换到菜单布局。

图 1: 菜单布局的动态视图

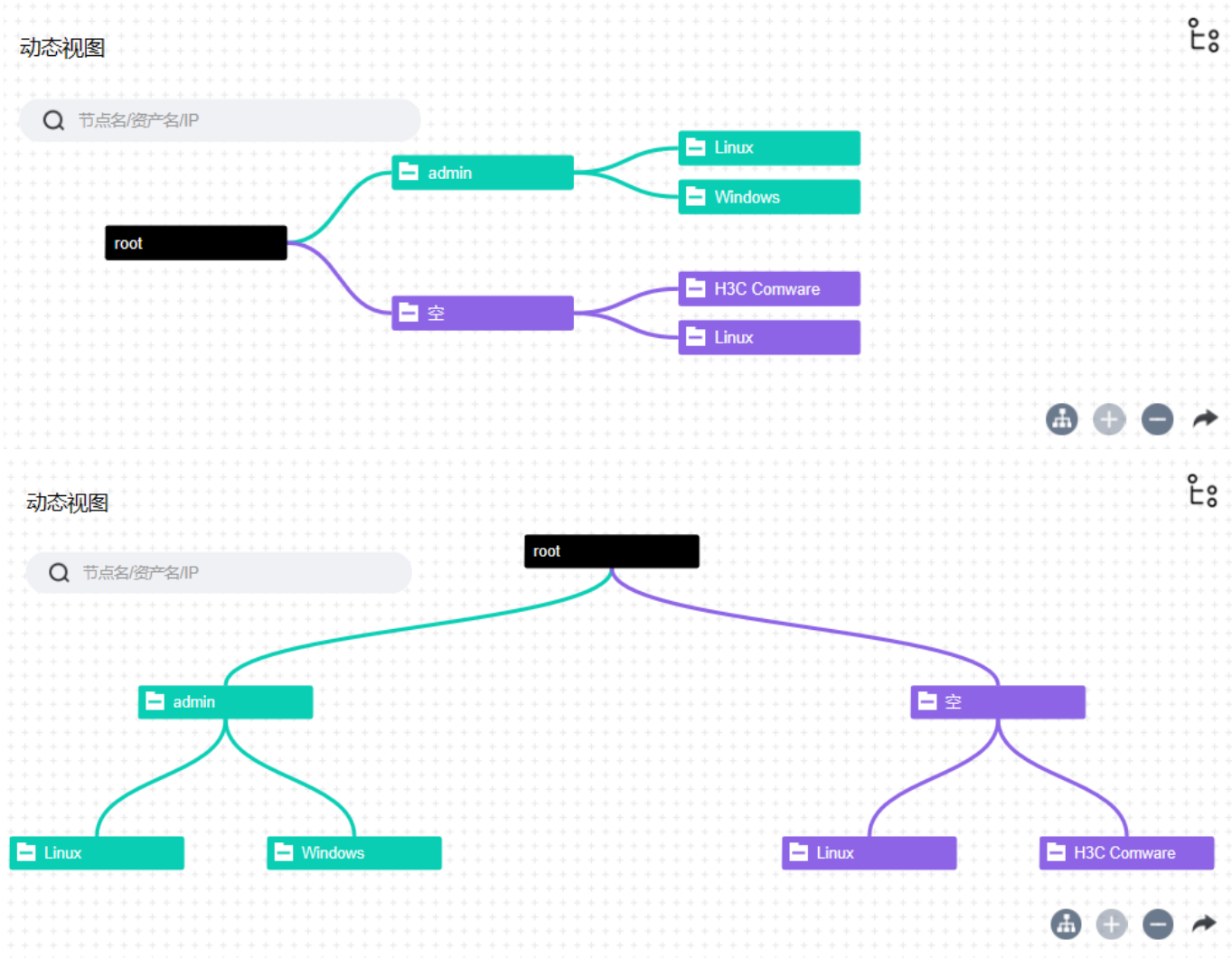


图 2: 树形布局的动态视图

表 12: 树形布局动态视图按钮说明

按钮	说明
	收起、展开节点。
	放大字体。

按钮	说明
	缩小字体。
	切换树形布局的横向、纵向展示方式。

1. 选择**资产** > **资产清单** > **动态视图**。
2. 可选： 在**动态视图**的搜索框中输入节点名、资产名或者资产IP地址的关键字来筛选出特定资产。
3. 可选： 选中节点，查看该节点下所有资产的信息。

   a) 如果资产数量大，可通过以下方式查找满足条件的资产。

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

   b) 单击资产属性对应的  或者  ，对资产进行排序。

   c) 单击资产列表最右边的  ，选择列表中显示的资产属性。
4. 可选： 单击资产对应的**编辑**，或者选中多个资产后单击**批量编辑**，修改资产的属性。
5. 可选： 选中资产后单击**批量删除**，删除指定资产。
6. 可选： 选中资产后单击**导出选中**或者直接单击**导出全部**，将资产信息以Excel格式导出到本地PC。
7. 可选： 单击**新建资产**来创建各类型资产，具体请参见配置资产（手工创建）。

   新创建的资产会按照配置的视图层级展示在动态视图中。

相关任务

配置视图的层级

配置视图的层级

RIS使用资产的属性作为视图的层级节点，并根据视图层级结构动态地生成视图来展示资产。

RIS支持资产的以下属性作为视图层级节点：

- 预定义属性：**系统类型**、**责任人**、**资产组**和**部门**。
- 自定义属性：全部。请确保已配置资产的自定义属性。

缺省情况下，RIS已提供了根节点和第1层节点。

- 根节点：缺省值为**root**，支持重命名，不能删除。
- 第1层节点：缺省值为**系统类型**，支持修改，不能删除。

说明： **部门**只能作为第1层节点，在第1层节点设置为**部门**后无法新增下层节点。即动态视图的组织方式有两种，一种按部门，一种是按资产除部门外的其他属性的组合。

本节以将视图的层级配置为其他资产属性为例进行指导。如果将视图配置为按部门划分，则不需要进行以下操作。

1. 选择**资产** > **配置** > **视图配置**。

2. 修改视图的根节点名称和第1层节点使用的资产属性。

参数	说明
根节点名称	根节点的名称，字符串格式，长度范围是1~30个字符。缺省值为**root**。
第1层节点	视图的第1层节点，取值为资产的属性，缺省值为**系统类型**。

3. 单击**新增下级节点**，选择剩余的资产属性作为层级节点。

   重复执行本步骤，完成视图各层级节点的配置。

   说明: 除根节点外，视图的层级最多不超过10层，即用户能够配置第1到第10层节点。

4. 单击**保存**，完成视图各层级节点的配置。
5. 可选： 单击**视图预览**，查看按照当前视图层级结构生成的动态视图。

   说明: 对于没有资产的节点，动态视图汇中不显示该节点。

   表 13: 预览视图按钮说明

按钮	说明
	收起、展开视图的节点。
	放大视图，从而更清楚地查看局部细节。
	缩小视图，从而查看视图的总体情况。

- 第1层到第10层的节点使用的资产属性都支持修改。
- 第2层到第10层的节点都支持删除，且各层级的节点相互独立，不存在依赖关系，可删除任意层级的节点。

修改或者删除视图的层级节点后，资产的动态视图及时跟随调整。

配置Windows域

如果用户希望通过RIS以Windows域的方式登录RDP资产，需要在这里配置Windows域。

- 拥有Windows域控主机。
- 拥有该域控主机上具有查询权限的帐号，并且知道该帐号的DN和密码。

1. 选择**资产** > **配置** > **Windows域**。
2. 单击**新建域**，设置各参数，完成后单击**确定**。

参数	说明
域名	域的名称。字符串格式，长度范围是1~30个字符。
域IP	域控主机的IP地址。
简要说明	域的简要说明。
部门	域所属的部门。

3. 单击**特权帐号**下的 ，设置特权帐号的相关信息，完成后单击**确定**。

   说明：在单击**确定**前，可以单击**测试**进行帐号连通性测试。

参数	说明
帐号名称	输入域控主机上具有查询权限帐号的用户名。
bindDN	输入该帐号的DN，例如**CN=Administrator,CN=Users,DC=example,DC=com**。 通过域控主机执行CMD命令获得： dsquery user -name *username*
帐号密码/确认密码	输入该帐号的密码。

4. 可选： 单击**帐号过滤条件**对应的取值，编辑过滤条件，完成后单击**确定**。

   过滤条件的格式为**(参数=属性)**，例如：**(objectClass=person)**。缺省的Windows域帐号过滤条件为**(objectClass=person)**，一般不需要修改。

Windows域配置完成后，管理员再执行以下操作即可实现使用Windows域用户访问Windows域中的资产。

1. 在**工作台** > **帐号改密** > **帐号资产** > **域帐号**中选择要管理的域，单击从域中同步帐号。
2. 帐号同步完成后，单击某个帐号对应的**编辑**，选择**帐号编辑**，设置该帐号的密码。具体请参见管理帐号资产。
3. 设置了帐号的密码后，在**资产** > **资产清单**，单击Windows域中的资产对应的**编辑**，选择**系统帐号**，单击**添加帐号**，在**高级选项**中选择Windows域，然后在**帐号名称**中选择具体的Windows域帐号。

配置密钥

管理员可以通过密钥管理功能新建密钥，以支持SSH会话使用密钥方式登录。

RIS支持两种新建密钥的方式：

- 生成：由RIS生成密钥。
- 粘贴：将其他系统生成的密钥粘贴到RIS中使用。

生成新密钥

1. 选择**资产** > **配置** > **密钥管理**。
2. 单击**新建**，选择**生成**，设置各参数，完成后单击**确定**。

参数	说明
类型	密钥的类型，取值包括**RSA**和**DSA**。
长度	密钥的位数，取值包括1024/2048和4096，位数越大安全性越高。
标识	密钥的标识。在资产的系统帐号中，通过该标识引用密钥。
部门	密钥所属的部门。仅当该部门的配置管理员可以使用该密钥。

3. 单击密钥对应的**编辑**，单击**下载公钥**，将公钥下载在本地计算机。

粘贴已有密钥

1. 选择**资产** > **配置** > **密钥管理**。
2. 单击**新建**，选择**粘贴**，设置各参数，完成后单击**确定**。

参数	说明
标识	密钥的标识。在资产的系统帐号中，通过该标识引用密钥。
部门	密钥所属的部门。
密码	如果粘贴的密钥设置了密码，在此处输入该密码。
粘贴	将已有的私钥内容粘贴进去。

配置等价资产

对等价资产中任意一个资产进行RIS上的配置修改，配置会自动同步到等价资产中的其他成员。等价资产多用于HA环境。

同一个设备，出于被访问的需求，在RIS中可能被配置成为多个资产。例如一个既有真实IP，又有虚拟IP的主机，在RIS中基于IP地址被配置成为两个资产，这两个资产就是等价资产。

在添加等价资产之前，管理员需要确认待添加的等价资产属性是一致的，否则将无法组成等价资产；修改等价资产在RIS上配置，只有关键的配置会被同步。

表 14: 等价资产的组成条件和同步的配置

资产类型	组成条件	同步的配置
主机/网络	• 资产类型需要一致。 • **访问协议**中如果拥有相同的协议，协议的属性需要一致。例如：端口一致、状态一致等。 • **系统帐号**中如果拥有相同帐号，该帐号的属性需要一致，例如：特权帐号一致、密码一致等。	• 访问协议 • 系统帐号 • 责任人
数据库	• 资产类型需要一致。 • **连接方式、服务名、客户端**属性需要一致。 • **系统帐号**中如果拥有相同帐号，该帐号的属性需要一致，例如：特权帐号一致、密码一致等	• 连接方式、服务名、客户端 • 系统帐号 • 责任人
应用系统（B/S）	• **URL、脚本类型、是否限制URL、白名单**属性需要一致。 • **系统帐号**中如果拥有相同帐号，该帐号的属性需要一致，例如：特权帐号一致、密码一致等	• URL、脚本类型、是否限制URL、白名单 • 系统帐号 • 责任人
应用系统（C/S）	• **port**属性需要一致。 • **系统帐号**中如果拥有相同帐号，该帐号的属性需要一致，例如：特权帐号一致、密码一致等	• port • 系统帐号 • 责任人

1. 选择**资产** > **配置** > **等价配置** > **等价资产**。
2. 单击**新建**，设置各参数，完成后单击**确定**。

参数	说明
名称	等价资产的名称。字符串格式，取值范围是1~30个字符。
添加资产	单击  选择资产。

参数	说明
责任人	等价资产的责任人。
简要说明	等价资产的简要说明。

配置等价帐号

对等价帐号中的任何一个帐号进行RIS上的密码修改，密码都会同步到等价帐号中的其他成员。

同一个资产，因为使用目的的不同会被配置成为两种资产类型。例如防火墙设备，既有SSH访问接口，又有Web访问接口，管理员会创建**主机**类型的资产以满足SSH访问，创建**应用系统**类型的资产以满足Web访问。由于访问这两种资产类型的帐号都是一致的，这类型帐号被称为等价帐号。

等价帐号组成条件：等价帐号可以跨资产类型，但是必须是相同帐号名，且以密码类型登录（密钥登录、切换自登录不行）。

等价帐号同步的配置：等价帐号只能同步密码。

1. 选择**资产** > **配置** > **等价配置** > **等价帐号**。
2. 单击**新建**，设置各参数，完成后单击**确定**。

参数	说明
名称	等价帐号的名称。字符串格式，取值范围是1~30个字符。
资产	单击  选择资产。
帐号名	等价帐号的帐号名。
简要说明	等价帐号的简要说明。

配置资产适配

对于有些比较特殊的登录提示符，通过内置代填提示符无法匹配成功时，需要针对这些资产进行适配。

在以下场景，RIS会代填用户名和密码。

- 登录测试
- 资产访问
- 帐号改密

RIS已内置了通用的登录提示符，涵盖了大多数字符设备，这些设备RIS都能代填成功。

当通用的登录提示符满足不了需求时，RIS支持用户自定义登录提示符。配置登录提示符时，可以针对单个资产配置，也可以针对资产类型配置。匹配时单个资产登录提示符的优先级最高，资产类型的次之，通过的最低。

管理员在配置资产适配提示符中，可以只配置通用提示符处理不了的过程，不需要全都过程都填写。例如，一台设备的普通用户提示符是“-”，通用提示符对于其他登录过程都支持，则管理员只需要修改普通提示符为“-”，其他登录过程会按照通用提示符进行匹配。

1. 选择**资产** > **配置** > **资产适配**。
2. 单击**新建**，设置各参数，完成后单击**确定**。

参数	**说明**
资产分类	取值包括**资产类型**和**资产**。如果选择**资产类型**，请继续选择具体的资产类型；如果选择**资产**，请单击  添加具体的资产。
部门	资产所属的部门。
服务选项	• 协议名：取值包括**ssh**和**telnet**。 • 服务名：指资产的访问协议名称。字符串格式，长度范围是1~30个字符。
帐号	资产的帐号。如果留空，代表匹配所有帐号。
普通提示符	普通帐号的提示符，字符串格式，长度范围是1~100个字符，支持正则表达式。默认提示符为**>**。仅影响改密和帐号发现和帐号巡检中的登录测试。 **说明：** 使用SSH协议的主机登录时不是通过登录提示符来验证的，不会受到影响。
特权提示符	特权帐号的提示符，字符串格式，长度范围是1~100个字符，支持正则表达式。默认提示符为**#**。仅影响改密和帐号发现和帐号巡检中的登录测试。 **说明：** 使用SSH协议的主机登录时不是通过登录提示符来验证的，不会受到影响。
登录超时时间	RIS登录资产的超时时间。单位为秒，范围为0~9999秒。缺省值为20秒。 仅影响字符会话、自动化脚本、帐号改密。 **说明：** 登录超时时间必须小于任务超时时间。
任务执行超时时间	RIS执行脚本任务超时时间。单位为秒，范围为0~9999秒。缺省值为180秒。 仅影响自动化脚本、帐号改密。
帐号切换命令	帐号的切换命令，字符串格式，长度范围是1~100个字符，支持正则表达式。默认切换命令为**su**。

参数	说明
	当配置了使用切换自的资产，且切换命令非默认切换命令时，需要配置该值。仅影响访问、登录测试和帐号改密。
切换自失败匹配符	登录切换执行失败时返回的错误提示，字符串格式，长度范围是1~100个字符，支持正则表达式。默认为([Ii]ncorrect)|((?i)su.*(fail|incorrect))|([Dd]eny)|([Dd]enied)。 当配置了使用切换自的资产，且切换失败时显示该值，仅用于帐号改密。
切换密码提示	切换时的密码提示符，字符串格式，长度范围是1~100个字符，支持正则表达式。通用切换密码提示为**Password:**。 当配置了使用切换自的资产，且切换密码提示非默认切换命令时，需要配置该值。仅影响访问、登录测试和帐号改密。
登录名提示	系统的登录名提示符，字符串格式，长度范围是1~100个字符，支持正则表达式。默认登录名提示为**login:**。 当资产的登录名提示非默认登录名提示时，需要配置该值。仅影响Telnet协议的访问和登录测试。
登录密码提示	系统的登录密码提示符，字符串格式，长度范围是1~100个字符，支持正则表达式。通用登录密码提示为**Password:**。 当资产的登录密码提示符非默认登录密码提示符时，需要配置该值。仅影响访问和登录测试。

说明: 配置正则表达式时，* ( ) + ? \ [ ]{}为特殊字符，需要转义，转义符为\。例如，*转义为*。

客户端代填兼容性列表

用户通过RIS访问B/S、C/S应用系统，RIS在代填帐号、密码等登录信息时，不同的客户端支持情况有所不同。

说明:

- 对于B/S应用来说，RIS能否代填成功不仅与使用的浏览器类型和版本有关系，还与具体应用系统有关系。
- 对于C/S应用来说，RIS是否支持代填主要取决于客户端软件的版本和中英文环境，服务器端的版本和中英文环境基本无影响（Oracle数据库除外）。
- 本兼容性列表仅代表实验室验证结果。

表 15: 客户端代填兼容性列表

客户端名称和版本	资产类型和版本	登录代填	备注
Firefox 55 ~ 59 Chrome 65	• B/S • Weblogic	支持	Chrome代填需要安装JAVA，建议安装JRE 1.8。
Internet Explorer 11	B/S IE	支持	• 不支持Edge • 不支持js Iframe跨域
sqlplusw 10（图形界面） SqlDbx英文版 Toad 12英文版 PL/SQL Developer 11.0英文版	Oracle： • Oracle 9i • Oracle Database 10g • Oracle Database 11g • Oracle Database 11g Release 2 RAC • Oracle Database 12c	支持	无
OEM	• Oracle Database 11g • Oracle Database 11g Release 2 RAC • Oracle Database 12c	B/S模式下支持	Oracle 9i和Oracle Database 10g不支持。
SQL Developer 1.5.5	Oracle	不支持	无
SSMS 2014中文版	SQL Server	支持	连接方式为TCP，且身份认证方式为SQL Server（Windows身份认证方式不支持）
Navicat中文版	MySQL	支持	不支持Premium版本。
SQLyog中文版	MySQL	支持	无
Quest Central	DB2	不支持	无
SqlDbx for DB2英文版	DB2	支持	无
Toad for DB2	DB2	支持	用户第一次登录时由于会出现引导页面而导致无法代填，请手工填写。
SQL Advantage	C/S	支持	无
vncviewer 5.2.3中文版	C/S	支持	无
Radmin 3.4	C/S	支持	无
ASDM	C/S	支持	无
VpxClient 6.0	C/S	支持	无

客户端名称和版本	资产类型和版本	登录代填	备注
Sybase Central v4.3	C/S	支持	无

权限管理

4

目录:

通过权限配置，用户可以实现对RIS资产的访问。

权限配置目的

用户通过RIS可以访问在其上的资产，需要针对不同权限的用户指定其相应的访问规则。

例如：指定系统管理员只能访问主机类型资产，不能访问网络类型资产。

权限配置四要素

配置一个基础权限需要四要素，配置好四者的对应关系，就能形成访问权限。

- 谁来访问：RIS上的帐号。
- 访问什么资产：RIS的待访问资产。
- 使用什么协议：RIS资产上的访问协议。
- 使用什么访问帐号登录资产：RIS的资产帐号。

例如：felix帐号使用administrator帐号和RDP协议访问Windows2012资产。

扩展的访问权限

RIS还支持从资产访问的各种角度对权限进行精细化管理。

- 允许/禁止访问的时间范围。
- 允许/禁止访问的IP范围。
- 允许/禁止图形会话磁盘映射。
- 允许/禁止图形会话剪切板上下行。
- 允许/禁止文件传输上传下载权限。
- 上传下载单文件大小限制。

配置权限方法

在RIS有两种配置权限的方法：

1. 变更单：可以通过提交电子变更单的方式，将变更单上的权限应用于RIS上。此方式支持指定权限的到期时间。

2. 动态权限：在RIS上直接选择用户、资产、访问帐号，形成访问权限。此方法配置快速便捷。

配置权限

通过变更单、动态权限配置基础权限，通过规则模板配置扩展权限。

管理员为某用户访问指定资产配置了权限后，该用户才能在**访问资产**界面看到这些资产，并对这些资产进行访问。

当为某用户设置了访问指定资产组的权限时，如果该资产组中的资产同时属于别的资产组，则这些资产组也将会在**访问资产**界面显示。但是在这些资产组节点下将只会看到实际拥有访问权限的资产。

配置动态权限

动态权限可以让管理员快速、灵活地配置权限。

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。

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。

配置四要素时，既可以指定具体的取值，也可以指定筛选规则。

说明: 协议只能指定具体的值。

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的规则，才能够匹配该条权限。

当管理员在RIS上添加用户、资产、访问帐号的时候，已经设置了相关的属性，例如针对用户的用户名、工作邮箱、角色、认证方式等；针对资产的资产名、IP、责任人等。可以通过条件匹配的方式，匹配出具有相同属性的内容。

RIS中的数据有两种格式，一种是字符串格式，一种是日期格式。

- 字符串格式：RIS中大多数据属于这种格式，可以使用的匹配方法为：**=、!=、>、<、>=、<=、包含、不包含、正则匹配、正则不匹配、前缀为、非前缀为、后缀为、非后缀为。**
- 日期格式：RIS中指定了扩展信息并且使用了日期类型的数据属于这种格式，可以使用的匹配方法为：**在日期范围内**、**不在日期范围内。**日期格式只能和日期格式进行匹配，如果使用字符串格式和日期格式进行匹配，内容即使一致，匹配也会失败。

表 16: 动态权限匹配方式说明

匹配方式	说明
=	被匹配的数据要和内容完全匹配。
!=	被匹配的数据要和内容完全不匹配。
>	被匹配的数据的ASCII码要大于内容的ASCII码。
<	被匹配的数据的ASCII码要小于内容的ASCII码。
>=	被匹配的数据的ASCII码要大于或等于内容的ASCII码。
<=	被匹配的数据的ASCII码要小于或等于内容的ASCII码。

匹配方式	说明
包含	被匹配的数据要包含内容。
不包含	被匹配的数据要不包含内容。
正则匹配	被匹配的数据要和内容的正则表达式完全匹配。
正则不匹配	被匹配的数据要和内容的正则表达式完全不匹配。
在日期范围内	被匹配的数据的日期要在时间范围内。
不在日期范围内	被匹配的数据的日期不要在时间范围内。
前缀为	被匹配的数据的前缀要内容完全匹配。
非前缀为	被匹配的数据的前缀要内容完全不匹配。
后缀为	被匹配的数据的后缀要内容完全匹配。
非后缀为	被匹配的数据的后缀要内容完全不匹配。

1. 选择**权限** > **权限配置** > **动态权限**。
2. 单击**新增动态权限**，设置各参数，完成后单击**保存**。

参数	说明
名称	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	动态权限引用的规则模板，具体请参见配置规则模板。
部门	动态权限所属的部门，缺省为**ROOT**。部门的具体配置请参见配置部门。
用户	设置能够访问目标资产的用户。 • 全部用户 • 用户/用户组：单击选择用户或者用户组。 • 指定规则：单击添加用户筛选规则。支持匹配的用户属性包括：用户帐号、用户名、工作邮箱、备注、角色、认证方式、用户组和所有自定义用户属性。
资产	设置待访问的目标资产。 • 全部资产 • 资产/资产组：单击选择资产或者资产组。 • 指定规则：单击添加资产筛选规则。支持匹配的资产属性包括：资产名、IP、简要说明、责任人、资产组、资产类型和所有自定义资产属性。
协议	访问目标资产使用的协议。 • 全部协议

参数	说明
	• 指定协议：包括ssh、telnet、rdp、xdmcp、vnc和xfwd
帐号	访问目标资产使用的帐号。 • 全部帐号 • 指定帐号：输入访问目标资产使用帐号，多个帐号之间用英文逗号","分隔。 **说明:** 指定帐号时，必须保证权限规则涉及的资产上已创建了对应的系统帐号，否则权限将无法生效，查看权限时也看不到对应的数据。 • 指定规则：单击设置帐号筛选规则。 • 指定帐号：配置匹配帐号的筛选规则。 • 帐号类型：配置匹配帐号类型的筛选规则。帐号类型包括**特权帐号**和**普通帐号**。

- 单击一条动态权限对应的**编辑**，修改动态权限的各参数。
- 单击一条动态权限对应的**删除**，删除这条动态权限。
- 单击一条动态权限对应的**克隆**，在弹出的页面中输入新规则名称，完成后单击**确定**，克隆出一条新的动态权限。克隆后除名称不同外其他都相同，管理员可以在此基础上编辑权限，简化权限配置过程。

配置变更单

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。最后将变更单上传到RIS形成访问权限。

用户按照RIS提供的变更单模板填写变更单内容，提交访问资产的申请，将权限加载到RIS中，此配置方法还可以设置权限到期时间。

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。

参数	说明
申请单名称	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	申请人的帐号，该帐号必须在RIS上存在且状态为活动。
部门	变更单所属的部门。
到期时间	申请单中权限到期日期和时间。
申请原因	变更单申请原因。
权限	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：

参数	说明
	• 使用人：使用人的帐号，该帐号必须在RIS上存在且状态为活动。 • 资产：要访问的资产名称或者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、rdp、xfwd、xdmcp，不填写时表示全部协议。

3. 单击**上传变更单**，上传配置好的变更单。

   成功导入变更单后，变更单中的权限会加载到RIS中。

变更单导入RIS后，管理员可以进行以下操作：

- 单击**延期**按钮，然后输入延期日期和时间并单击**保存**，修改对应变更单的结束日期。不输入表示无限期。
- 单击**禁用**按钮，禁用该变更单，使权限无效。

  禁用的变更单默认不显示在页面上，如果需要重新启用，单击**筛选**，选中**状态**为**禁用**，筛选出禁用的变更单。如果要重新启用该变更单，请单击**启用**。
- 单击**详情**查看变更单的详细信息，包括基本信息和权限清单。详情页面，除了可以执行延期和禁用变更单操作外，还可以删除变更单，修改、克隆和删除权限。
  - 单击**基本信息**对应的**删除**按钮，删除变更单。
  - 单击权限各字段的取值（包括**用户**、**资产**、**帐号**、**协议**和**规则**），修改对应字段的取值。例如单击用户对应的取值，可以增加或者删除用户；单击帐号对应的取值，可以增加或者删除帐号。
  - 单击权限对应的**克隆**按钮，克隆一条权限。
  - 单击权限对应的**删除**按钮，删除该条权限。

配置规则模板

扩展的访问权限可以在这里配置。

权限配置除了配置用户、资产、访问帐号的基础权限，还可以配置磁盘映射、文件传输等扩展权限。RIS中的扩展权限是通过规则模板配置的。

规则模板

规则模板中可以定义磁盘映射、剪贴板上下行、文件传输上下行、文件传输单文件大小限制等权限，管理员可以配置基础权限的规则模板来增加对基础权限的限制。规则模板中可以定义多个规则列表。

规则列表

规则列表属于规则模板中的详细条目，规则列表可以对访问时间、访问IP做限制。一个规则模板中可以有多个规则列表。当用户访问时，会按照规则列表中从上至下，逐一匹配的方式，当所有规则列表都不匹配，最终会匹配规则模板中的控制策略。

RIS中有一条名为Default的默认规则模板，该规则模板开放了所有的访问。

1. 新增规则模板。

   a) 选择**权限** > **权限配置** > **规则模板**，单击**新增规则模板**。

   b) 配置需要控制的权限。

图 3: 编辑权限规则模板

参数	**说明**
模板名称	定义该规则模板名称。
控制策略	选择该条策略禁止或允许访问。
设为全局缺省模板	RIS中有且只能有一个缺省模板。如果存在缺省模板，配置新的缺省模板，会发生抢占。如果删除缺省模板，系统会提示“系统必须存在一个全局缺省登录模板”。

参数	说明
工单缺省模板	RIS中有且只能有一个工单缺省模板。如果存在缺省模板，配置新的缺省模板，会发生抢占。如果删除缺省模板，系统会提示“系统必须存在一个全局缺省工单规则模板”。
允许客户端磁盘映射	针对通过Windows RDP方式的访问，是否允许磁盘映射。
剪贴板	针对图形会话的访问，能否使用剪贴板上下行。
文件传输权限	是否允许Web页面云盘模式和SFTP模式的文件上传、下载。
上传/下载单文件限制	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。例如限制2MB，只上传文件的前2MB部分。 取值范围为1~10240MB。
事件级别	当使用告警事件功能时，访问资产可以产生告警事件并发送到日志服务器或邮箱。在这里定义告警事件的级别。 当定义的告警事件级别不低于系统定义的最低级别，访问资产将发送日志到日志服务器或邮箱。 告警事件，配置方法参考基本设置：配置告警事件。
标题	告警事件使用什么标题来标记这次的访问事件。标题将出现在当前访问日志的记录中，以方便管理员查看，并且该标题下记录了访问的详细参数。

2. 新增规则列表。

a) 单击相应规则模板的**规则管理**按钮。单击**新增规则**。

b) 输入规则列表的内容。

IP范围说明

- 单IP：IP地址，例如192.168.1.1。
- IP地址段（掩码）：网络号/掩码位数，例如192.168.1.0/24。
- IP地址段（非掩码）：起始IP-结束IP，这种方式要求IP地址连续，例如192.168.1.1-192.168.1.200，

可以多种IP方式组合，中间通过英文逗号隔开，例如192.168.1.0/24,192.168.2.211。

时间范围说明

- 基于星期指定：w[1]（每周一）、w[2-4]（每周二到每周四）、w[1,4,7]（每周一、四、七）。
- 基于月份指定：m[2]（每年2月）、m[3-11]（每年3到11月）、m[4,7,9]（每年4、7、9月）。
- 基于小时、分钟指定：T[10:30]（每天10:30）、T[08:30-18:30]（每天08:30到18:30时间段）。
- 基于每月中的日期指定：d[4]（每月4日）、d[10-20]（每月10到20日）、d[1,15,30]（每月1、15、30日）。
- 基于时间段指定：D[20160809]（2016年8月9日）、D[20160809-20160910]（2016年8月9日到2016年9月10日时间段）、D[20160809,20160811,20160813]（2016年8月9日、2016年8月11日、2016年8月13日）。

每种格式只能出现一次，如果一个格式中有多个内容，请在同一格式中用英文逗号分隔，例如：D[20160806,20160809-20160910]。

可以多种格式组合，中间通过空格隔开，例如：m[1,3-5,12] d[1,5,7,31] w[1-3,5,7] T[08:30-16:00]。

查看权限

按用户查看权限

按用户查看访问权限，会分别列出变更单、动态、工单方式产生的访问权限。

1. 选择**权限** > **权限查看** > **按用户**，单击相应用户，或者使用过滤方式来搜索用户。
2. 出现的访问权限将以变更单、动态权限、工单方式都显示出来。单击相应权限的来源可以进入相关权限中配置。

说明:

- 单击相应用户，在出现该用户的权限列表中，可以通过资产名、帐号再次过滤。
- 筛选多个用户，然后单击筛选页的**导出**，可以一次导出多个用户的权限；单击相应用户，单击该用户权限页的**导出**，可以导出该用户的权限。

按资产查看权限

按资产查看访问权限，会分别列出变更单、动态、工单方式产生的访问权限。

1. 选择**权限** > **权限查看** > **按资产**，单击相应资产，或者使用过滤方式来搜索资产。
2. 出现的访问权限将以变更单、动态权限、工单方式都显示出来。单击相应权限的来源可以进入相关权限中配置。

说明:

- 单击相应资产，在出现该资产的权限列表中，可以通过用户名、帐号再次过滤权限。
- 筛选多个资产，然后单击筛选页**导出**，可以一次导出多个资产的权限。单击相应资产，单击该资产权限页的**导出**，可以导出该资产的权限。

配置高危操作

管理员通过配置会话复核或高危命令规则，可以对操作员访问资产和执行命令进行控制，以减小操作员访问资产及执行操作可能存在的风险。

能够使用配置高危操作的角色包括：超级管理员、配置管理员、操作员及其他自定义的拥有高危操作授权的用户。但操作员仅具有进行命令复核和查看复核日志的权限，不能对高危操作规则进行设置。管理员可以通过配置高危操作规则，对特定的操作员访问特定的资产要求在进行复核后才能访问，或对操作员执行特定的命令，要求在进行复核后才能执行或直接拒绝执行，从而达到访问控制和命令控制的目的。

RIS中的配置高危操作，包括配置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，执行的动作包括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，执行的动作包括允许、复核、拒绝、切断、通知。

复核高危操作

当管理员正确地完成了配置会话复核或配置高危命令后，操作用户的访问操作如果匹配会话复核或高危命令中的规则，复核人将收到复核提醒。收到复核提醒后，请复核人登录Web界面并进行复核。

复核高危操作又分为**复核会话**和**复核高危命令**，其中复核高危命令又分为**离线复核**和**在线复核**。本节将分别对这几种复核操作进行介绍。

会话的复核人，只能为操作用户所选取的固定的一个复核人；命令的复核人，可以是所有可用复核人中的任意一个，每个可用复核人都会收到复核申请消息，当有一个复核人完成复核之后，其他复核人将不能再进行复核。

复核会话

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。

复核会话要求复核人能够成功打开字符或图形会话，即当前**帐号设置** > **会话配置**中的配置正确，且本地PC安装了对应的会话客户端。

当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，复核人可以将自己的PIN2码及动态令牌的动态密码发给操作员，并由操作员自己进行会话复核，具体方法参见：操作员自行复核。

1. 使用复核人帐号登录RIS Web界面。
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。也可以直接选择**工作台** > **高危操作** > **待复核** > **待我复核**。
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，解锁操作用户的操作。

   说明： 复核人必须保持复核窗口打开，从而在线观看用户的所有操作，一旦复核人关闭复核窗口，操作用户的会话也将被自动锁定。
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。
   - 字符会话：再次按下**空格**或**回车**，锁定操作用户的操作。
   - 图形会话：单击窗口右上角的**pause**按钮，锁定操作用户的操作。
6. 当复核人需要暂时离开时，可以直接关闭会话窗口，从而锁定会话。

复核人断开会话后，操作用户将仍然保持连接，但会话会被锁定，不能执行操作。同时复核人会收到会话复核提醒，可以在操作用户的会话关闭前，重新对会话进行复核。

复核命令（离线）

离线复核即在不打开复核会话窗口的情况下，处理高危命令复核申请。

仅当命令模板中的规则对应的执行动作为**需复核**时，复核人才会收到命令复核申请，其他执行动作不会触发命令复核申请。

1. 使用复核人帐号登录RIS Web界面。
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。也可以直接选择**工作台** > **高危操作** > **待我复核**。
3. 查看收到的复核申请，对于**复核类型**为**命令复核**的复核申请，查看其**复核内容**、**操作用户**、**资产**、**帐号**等信息。
4. 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。

   说明: 当一个复核人执行复核操作后，其他复核人收到的复核请求将失效并撤回。操作员也可以自行撤回复核申请。

复核命令（在线）

在线复核是指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，并在会话窗口中完成命令复核。

前提：该复核人已参照复核会话打开了会话复核窗口，并观看操作用户的所有操作。

1. 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。
2. 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。

   说明: 当其他复核人或该复核人自己先采用离线复核的方式完成了复核，观看窗口中的复核申请将失效，命令将直接被执行或被阻断。操作员也可以自行撤回复核申请。

相关信息

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。

查看已复核操作

复核人可以在Web界面中查看自己所完成的所有会话复核和命令复核的日志。

1. 使用复核人帐号登录RIS Web界面。

2. 选择**工作台** > **高危操作** > **待复核** > **我已复核。**
3. 选择**会话复核日志**页签，查看所有的会话复核日志。

   该日志是一个可翻页的表格，表格中每一行表示一条会话复核记录，每一列信息如下：

项目	**说明**
会话类型	**字符会话**或**图形会话。**
操作用户	操作用户的用户名和姓名。
操作资产	建立会话的资产在RIS上的名称。
帐号	操作用户登录资产所使用的资产帐号。
完成时间	会话结束后到现在已经过去的时间。如会话仍在进行，则该项显示为空。
会话时长	会话持续时间。如会话仍在进行，单击刷新。
状态	会话状态： • **活跃**：会话仍在进行中。 • **结束**：操作用户已结束了图形会话。 • **断开**：操作用户已结束了字符会话。 • **强制断开**：操作用户因执行命令触发了高危命令中的**终止会话**规则，会话已被强制切断。
操作	单击**详情**可查看该会话的更多详情，包括： • **来自**：发起会话的客户端IP。 • **登往**：被访问资产的IP。 • **帐号**：操作用户登录资产所使用的资产帐号。 • **协议**：建立会话所使用的协议。 • **状态**：会话状态，含义同上。 • **执行时间**和**状态**表格：**状态**显示为**允许执行**和**禁止执行**，表示会话过程中复核人进行锁定和解锁的记录，并显示具体的时间点。

   说明: 复核人可以在搜索框中输入操作用户或操作资产名称，快速检索对应的会话复核记录。

4. 选择**命令复核日志**页签，查看所有的命令复核日志。

项目	说明
复核类型	固定取值为**命令复核**。
复核内容	操作用户执行的具体命令。
操作用户	操作用户的用户名。
操作资产	建立会话的资产在RIS上的名称。
帐号	操作用户登录资产所使用的资产帐号。
发起时间	发起命令复核到现在已经过去的时间。
状态	会话状态： • **活跃**：会话仍在进行中。 • **结束**：操作用户已结束了图形会话。 • **断开**：操作用户已结束了字符会话。 • **强制断开**：操作用户因执行命令触发了高危命令中的**终止会话**规则，会话已被强制切断。
复核结果	**允许执行**或**拒绝执行**，表示命令被复核人允许或阻断。

说明： 复核人可以在搜索框中输入复核内容、操作用户或操作资产名称，快速检索对应的会话复核记录。

配置会话复核

管理员可以通过在Web界面的**会话复核**菜单中定义各种规则，来控制具体的会话复核行为，即要求特定的操作用户在访问特定的资产时，必须由特定的复核人进行复核之后，才能在该资产上执行各种操作。

说明： SFTP协议不支持会话复核。

本节以新增一条会话复核规则为例，对配置会话复核进行指导。在已添加了会话复核规则之后，也可以通过单击对应的**编辑**和**删除**按钮，对已有的会话复核规则进行管理。

如配置了多条操作用户和资产有重复的会话复核规则，则受多条规则影响的操作用户在启动会话时，复核人列表将是所有匹配的会话复核规则中定义的可用复核人的并集。

1. 使用管理员帐号登录RIS Web界面。
2. 选择**工作台** > **高危操作** > **设置** > **会话复核**。
3. 单击右上角的**新增会话复核**。
4. 填写会话复核规则的名称。

   该名称为一个长度1~30的字符串，全局唯一。

5. 添加会话**复核人**。单击，在弹出的对话框中选择**用户**或**用户组**页签，勾选待添加的用户或用户组。

   在配置了会话复核之后，操作用户访问资产且匹配会话复核规则时，在会话启动前会要求选择会话复核人，该会话复核人将在此处添加的会话复核人中选取。

   说明:

   - 会话复核人必须是具有高危操作中的复核权限（例如审计管理员不具有复核权限），且可以正常登录的用户（不存在帐号过期、密码过期、被禁用），否则都无法作为会话复核人：
     - 无法作为会话复核人的用户，将不被显示在可勾选列表中。
     - 用户组中如包含无法作为会话复核人的用户，该用户将被忽略。
     - 如只勾选了用户组，但用户组为空，或所有用户组中都只包含无法作为会话复核人的用户，则该会话复核规则将无法生效，会话将不被复核。
   - 复核人可以和操作人相同，当某用户被同时配置为了复核人和操作用户时，如还有其他复核人，则该用户访问资产时只能选择其他的复核人进行复核；如没有其他复核人，则该用户的访问不需要复核。
   - 如添加了多个用户和用户组，且互相之间有重复用户，则复核人将取所有勾选的用户和用户组之间的并集。

6. 添加需要进行会话复核的**操作用户**。单击，在弹出的对话框中选择**用户**或**用户组**页签，勾选待添加的用户或用户组。

   说明:

   - 操作用户必须是具有访问资产权限（例如审计管理员不具有访问资产权限），且可以正常登录的用户（不存在帐号过期、密码过期、被禁用），否则都无法作为操作用户：
     - 无法作为操作用户的用户，将不被显示在可勾选列表中。
     - 用户组中如包含无法作为操作用户的用户，该用户将被忽略。
     - 如只勾选了用户组，但用户组为空，或所有用户组中都只包含无法作为操作用户的用户，则该会话复核规则将无法生效。
   - 如添加了多个用户和用户组，且互相之间有重复用户，则操作用户将取所有勾选的用户和用户组之间的并集。

7. 添加建立会话时需要进行复核的**资产**。单击，在弹出的对话框中选择**资产**或**资产组**页签，勾选待添加的资产或资产组。

   如添加了多个资产和资产组，且互相之间有重复资产，则将取所有勾选的资产和资产组之间的并集。

8. 添加资产**帐号**，仅当使用该资产帐号访问资产时需要进行会话复核。

默认勾选**全部帐号**，即操作用户使用任何帐号访问特定资产时都需要会话复核。如需单独设置帐号，请去勾选**全部帐号**，请在下方的对话框中，输入要添加的帐号，并按回车确定。单击该对话框也将列出RIS上记录的这些资产所拥有的所有帐号，选中某个帐号或者按回车之后，该帐号将在下方表格中列出，表示添加成功。

9. 设置**开始待审核会话时生成事件**。

a) 设置**事件级别**。在下拉菜单中选中一个事件级别。

事件级别由低到高依次为：NONE （不发送告警事件）—>DEBUG（调试级）—>INFORMATIONAL（通知级）—>NOTICE（注意级）—>WARNING（告警级）—>ERROR（错误级）—>CRITICAL（临界级）—>ALERT（警戒级）—>EMERGENCY（致命级）。

b) 设置**标题**，格式为一个长度1~30的字符串。

说明：开始待审核会话时生成事件会影响告警事件和短信通知。

- 当触发会话复核时：
  - 如**系统设置** > **系统** > **基本设置** > **告警事件**中的**syslog日志事件来源**的**会话复核**选项被勾选，RIS会将该事件发送给syslog服务器。
  - 如**通知邮件事件来源**的**会话复核**选项被勾选时，RIS会将该事件发送邮件给设定的邮件收件人。如勾选了**事件触发者**，会同时发送给发起会话的用户。
  - 如**短信配置** > **发送短信功能**中的**会话复核**被勾选，并且指定的会话复核人配置了手机号码时，则RIS会将该事件发送短信给该复核人。
- 仅当**事件级别**不低于**syslog日志事件来源**或**通知邮件事件来源**中配置的发送事件的最低级别时，才会发送相应的日志或邮件通知。
- 此处配置的**事件级别**和**标题**，都将显示在触发高会话复核后RIS发送的日志、邮件、短信的内容中。

10.确定配置无误后，单击**保存**，使规则生效。

完成配置后，如果在进行配置会话复核时配置有误，或者管理员后续对于用户或资产的操作对会话复核配置有影响，都会导致会话复核规则的状态异常。例如复核人用户组中成员都没有会话复核权限，帐号过期或被禁用，用户组/资产组被清空等。此时RIS会通过以下手段进行通知：

- 状态异常的**会话复核名称**会显示为红色。
- 所有超级管理员和配置管理员，在每次登录时右上角会收到提醒，提示哪些会话复核存在问题。
- 当某个操作使某条会话复核规则的状态由正常变为异常时，所有在线的超级管理员都会收到提示。
- 当操作用户访问资产时触发会话复核规则，而没有可用的会话复核人时，操作用户访问资产的行为将被阻止，并且收到无权访问资产的提示。

请管理员在收到系统提醒或收到操作用户的反馈时，及时处理状态异常的会话复核规则，保证每条规则中可用的复核人、操作用户、资产都不为空。可以单击会话复核列表中的，在弹出的窗口中，查看指定规则对应的可用的复核人、操作用户、资产有哪些。

配置高危命令

管理员可以通过在Web界面的**高危命令**菜单中定义各种规则，针对特定的用户、资产、帐号启用特定的高危命令模板，从而对用户在字符会话中的操作行为进行控制。

该配置需要预先定义**命令模板**，并在此处引用。

说明:

高危命令只对Telnet/SSH字符会话有效，如通过XDMCP或XFWD等图形会话方式打开字符终端并执行命令，将不受高危命令的约束。

高危命令的上下顺序代表优先级高低，单击↑或↓可以调整优先级。当配置了多个命令模板，命令模板中有多条可匹配的规则时，建立会话时的命令权限检查流程流程图如图 4: 命令权限检查流程图所示。

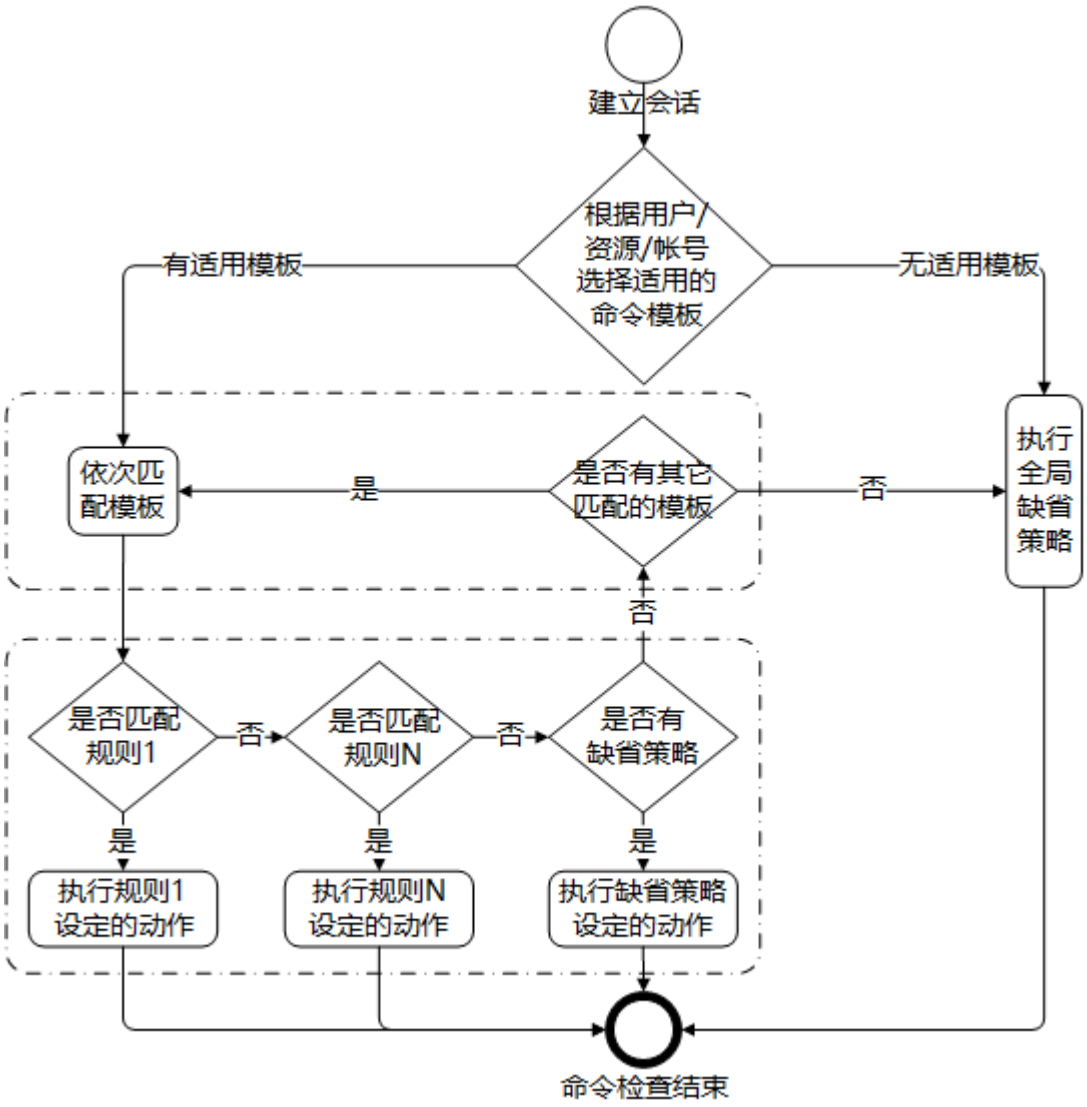


图 4: 命令权限检查流程图

本节以新增一条高危命令规则为例，对配置高危命令进行指导。在已添加了高危命令规则之后，也可以通过单击对应的**编辑**和**删除**按钮，对已有的高危命令规则进行管理。

1. 使用管理员帐号登录RIS Web界面。

2. 选择**工作台** > **高危操作** > **设置** > **高危命令**。
3. 单击右上角的**全局缺省策略**，将全局缺省策略配置为**允许执行**或**禁止执行**，完成后单击**保存**。

   如果所有的高危命令的都无法匹配，则使用此全局缺省策略。全局缺省策略的缺省值为**允许执行**。
4. 单击右上角的**新增高危命令**。
5. 填写高危命令规则的名称。

   该名称为一个长度1~30的字符串，全局唯一。
6. 在下拉菜单中选择待引用的**命令模板**的名称。该模板必须先在**设置** > **命令模板**中定义，然后在此引用。
7. 可选： 当模板中存在**需复核**的规则时，添加高危命令**复核人**。单击  ，在弹出的对话框中选择**用户**或**用户组**页签，勾选待添加的用户或用户组。

   在配置了高危命令的复核人之后，当操作用户触发高危命令，且在**命令模板**中设置的高危命令的**执行动作**是**需复核**时，RIS会将命令复核提醒发送给每一个可用的复核人，由其中任意一人完成命令复核。

   说明:

   - 高危命令复核人必须是具有高危操作中的复核权限（例如审计管理员不具有复核权限），且可以正常登录的用户（不存在帐号过期、密码过期、被禁用），否则都无法作为复核人：
     - 无法作为复核人的用户，将不被显示在可勾选列表中。
     - 用户组中如包含无法作为复核人的用户，该用户将被忽略。
     - 如只勾选了用户组，但用户组为空，或所有用户组中都只包含无法作为会话复核人的用户，则该高危命令规则将无法生效。
   - 复核人可以和操作人相同，当某用户被同时配置为了复核人和操作用户时，如还有其他复核人，则该用户执行高危命令时只能由其他的复核人进行复核；如没有其他复核人，则该用户的访问不需要复核。
   - 如添加了多个用户和用户组，且互相之间有重复用户，则复核人将取所有勾选的用户和用户组之间的并集。
8. 添加**操作用户**，被添加的操作用户执行操作时会触发高危命令。

   操作用户默认勾选**全部用户**。如需单独设置操作用户，请去勾选**全部用户**，并单击  ，在弹出的对话框中选择**用户**或**用户组**页签，勾选待添加的用户或用户组。可以勾选**临时操作用户**，将所有临时用户也都添加到待复核的操作用户名单中。

   管理员也可以选中**排除以下用户**，然后选择要排除的用户。

   说明:

- 操作用户必须是具有访问资产权限（例如审计管理员不具有访问资产权限），且可以正常登录的用户（不存在帐号过期、密码过期、被禁用），否则都无法作为操作用户：
  - 无法作为操作用户的用户，将不被显示在可勾选列表中。
  - 用户组中如包含无法作为操作用户的用户，该用户将被忽略。
  - 如只勾选了用户组，但用户组为空，或所有用户组中都只包含无法作为操作用户的用户，则该高危命令规则将无法生效。
- 如添加了多个用户和用户组，且互相之间有重复用户，则操作用户将取所有勾选的用户和用户组之间的并集。

9. 添加**资产**，在被添加的资产上执行操作时会触发高危命令。

资产默认勾选**全部资产**。如需单独设置资产，请去勾选**全部资产**，并单击  ，在弹出的对话框中选择**资产**或**资产组**页签，勾选待添加的资产或资产组。如添加了多个资产和资产组，且互相之间有重复资产，则将取所有勾选的资产和资产组之间的并集。

管理员也可以选中**排除以下资产**，然后选择要排除的资产。

10.添加资产**帐号**，仅当使用该资产帐号访问资产并执行操作时会触发高危命令。

默认勾选**全部帐号**，即操作用户使用任何帐号访问特定资产时都会触发高危命令。如需单独设置帐号，请去勾选**全部帐号**，请在下方的对话框中，输入要添加的帐号，并按回车确定。单击该对话框也将列出RIS上记录的这些资产所拥有的所有帐号，选中某个帐号或者按回车之后，该帐号将在下方列出，表示添加成功。

管理员也可以选中**排除以下帐号**，然后输入要排除的帐号，多个帐号之间用英文逗号","分隔。

11.设置**生效时间**。

配置生效时间的格式如下：

- 周：w[1-3,5,7]
- 月：m[1,3-5,12]
- 天：d[1,5,7,31]
- 日期：D[20180101,20180101-20180301]
- 时间：T[03:30-18:00]

利用该功能，可以实现以下效果：

- 特定的命令只在特定的时间段做限制
- 不同的时间段对不同的命令做限制

12.设置**触发高危命令时生成事件**。

a）设置**事件级别**。在下拉菜单中选中一个事件级别。

事件级别由低到高依次为：NONE （不发送告警事件）—>DEBUG（调试级）—>INFORMATIONAL（通知级）—>NOTICE（注意级）—>WARNING（告警级）—>ERROR（错误级）—>CRITICAL（临界级）—>ALERT（警戒级）—>EMERGENCY（致命级）。

b) 设置**标题**，格式为一个长度1~30的字符串。

说明：触发高危命令时生成事件会影响告警事件和短信通知。

- 当触发高危命令时：
  - 如**系统设置** > **系统** > **基本设置** > **告警事件**中的**syslog日志事件来源**的**命令防火墙**选项被勾选，RIS会将该事件发送给syslog服务器。
  - 如**通知邮件事件来源**的**命令防火墙**选项被勾选时，RIS会将该事件发送邮件给设定的邮件收件人，如勾选了**事件触发者**，会同时发送给触发高危命令的用户。
  - 如**短信配置** > **发送短信功能**中的**命令复核**被勾选时，RIS会将该事件发送短信给所有设置了手机号的复核人。
- 仅当**事件级别**不低于**syslog日志事件来源**或**通知邮件事件来源**中配置的发送事件的最低级别时，才会发送相应的日志或邮件通知。
- 此处配置的**事件级别**和**标题**，都将显示在触发高危命令后RIS发送的日志、邮件、短信的内容中。

13.确定配置无误后，单击**保存**，使规则生效。

完成配置后，如果在进行配置高危命令时配置有误，或者管理员后续对于用户或资产的操作对高危命令配置有影响，都会导致高危命令规则的状态异常。例如因复核人用户组中成员都没有操作复核权限，帐号过期或被禁用，用户组/资产组被清空等。此时RIS会通过以下手段进行通知：

- 状态异常的**高危命令名称**会显示为红色。
- 所有超级管理员和配置管理员，在每次登录时右上角会收到提醒，提示哪些高危命令规则存在问题。
- 当某个操作使某条高危命令规则的状态由正常变为异常时，所有在线的超级管理员都会收到提示。
- 当操作用户访问资产并执行一条需要复核的高危命令，而没有可用的复核人时，操作执行的命令将直接失败，并且收到没有可用复核人的提示。

请管理员在收到系统提醒或收到操作用户的反馈时，及时处理状态异常的高危命令规则，保证每条规则中可用的复核人、操作用户、资产都不为空。可以单击高危命令列表中的，在弹出的窗口中，查看指定规则对应的可用的复核人、操作用户、资产有哪些。

配置命令模板

命令模板定义了高危命令触发的基本规则，即哪些命令会触发高危命令事件，以及触发之后具体执行的动作，包括：允许、拒绝、需复核、通知和终止会话。

命令模板采用正则表达式进行精确匹配。RIS使用通用的正则表达式规则，请查阅正则表达式的通用规范书写正则表达式。表达式可以写成**命令+空格+参数**的形式，也可以写成**仅命令**的形式：

- **命令+空格+参数**：包含空格的表达式。RIS会严格按照该正则表达式进行匹配。例如，表达式rm -rf只能匹配到完整的rm -rf命令，无法匹配到rm -rf files，需要将表达式写成rm -rf.*从而匹配到命令rm -rf files。

- **仅命令**：不包含空格的表达式。RIS会将表达式视作一条不带参数的命令，匹配该表达式本身，以及携带任何参数的情况，即正则表达式expr可匹配命令(expr)|(expr +.*)。例如，表达式shutdown可以匹配到shutdown本身，也可以匹配到shutdown 参数的情况，如shutdown -r。

当用户执行的命令中存在**|**、**&**或**;**时，RIS会将这些符号视作分隔符，并将分隔符前后当做不同命令来处理。因此，不能使用通配符匹配命令中的这些分隔符。当被分隔符分隔的命令受不同规则控制时，**通知**会被执行，其他动作会按照以下优先级：**断开会话**>**拒绝**>**需复核**>**允许**，只执行优先级最高的动作。

同一模板中的多条规则按从上到下的顺序对应从高到低的**优先级**。假如同一条命令匹配上了不同的规则，则只会按照这些规则中最上面的一条规则，执行对应的动作。可以在进行**规则管理**时单击  或  ，对规则优先级进行调整。

本节以新增一个命令模板为例，对配置命令模板进行指导。在已添加了命令模板之后，也可以通过单击对应的**规则管理**按钮编辑规则，或单击**编辑**按钮编辑模板名称和缺省策略，单击**删除**按钮删除模板，从而对已有的命令模板进行管理。

1. 使用管理员帐号登录RIS Web界面。
2. 选择**工作台** > **高危操作** > **设置** > **命令模板**。
3. 单击右上角的**新增命令模板**。
4. 在弹出的对话框中填入**命令模板名称**、设置**缺省策略**，并单击**保存**。

参数	**说明**
命令模板名称	用于标识一个命令模板，全局唯一，长度为1~30的字符串。
缺省策略	如果资产、用户和帐号都匹配上，但规则中配置的命令没有匹配上时RIS采取的缺省策略，取值包括： • 允许：允许用户执行该命令。 • 禁止：禁止用户执行该命令。 • 无：继续匹配下一条高危命令。

   单击**保存**后，命令模板列表中会显示该新增的模板。需要继续为该模板配置具体的规则。

5. 在**命令模板列表**中找到新增的规则，单击对应的**规则管理**。
6. 编辑命令模板规则的具体内容。

   a) 单击**新增规则**，为命令模板新增一条规则。

   b) 在新增的规则中设置**执行动作**，在下拉菜单中选择一个动作，匹配上对应的命令之后将执行对应的动作。

执行动作	说明
允许	匹配上的命令将被允许执行。
拒绝	匹配上的命令将被拒绝执行。
终止会话	用户执行一条匹配的命令时，将在收到提示后直接断开该会话。
需复核	用户执行一条匹配的命令时，将收到需要复核的提醒。操作员确认后，复核人将收到复核提醒。完成复核后，该命令才能执行。
通知	不影响用户执行命令，但如配置了syslog日志通知、邮件通知、短信提醒等功能，该命令将触发事件并作为日志、邮件、短信的内容通知日志服务器或通知对象。

说明：在**缺省策略**为**允许/禁止**时，单独配置规则的执行动作为**允许/拒绝**没有必要。但**允许**和**禁止**的动作可以按照优先级互相覆盖。管理员可以结合运用缺省策略、执行动作和优先级，实现更精确的范围控制。例如，将**缺省策略**配置为**禁止**，**允许**rm，**拒绝**rm -rf.*，且设置允许的优先级较高，就可以实现只允许rm，并可以搭配其他参数，但拒绝rm -rf.*。

c) 在新增的规则中设置**命令控制**，在输入框中输入命令的正则表达式。输入一条表达式之后按回车键可以继续输入第二条表达式。

d) 重复6.a~6.c，直到所有规则添加完毕。

e) 单击↑或↓调整各规则之间的优先级。

f) 确认无误后，单击**保存**。

命令模板配置之后，必须在**高危命令**中被引用才能生效。

资产访问

5

目录:

能够访问资产的用户角色包括：**操作员**、**超级管理员**、**配置管理员**及其他自定义的拥有资产访问授权的用户角色。本章节指导用户完成RIS所有基本的资产访问操作。资产访问可以通过Web界面访问，也可以直接通过RDP或SSH/Telnet工具先登录到RIS后，再跳转访问各种资产。

在访问资产前，请先确保已完成以下设置：

- 已完成安装AccessClient。
- 已完成资产的创建和帐号设置。
- 已完成了对待访问资产的权限配置，允许当前用户访问。
- 如不使用密码托管，已获取了待登录设备的帐号和密码。

RIS所支持的所有可访问的资产类型如下：

资产类型	说明
主机	包含Windows、Linux、HP UX、IBM AIX。
网络设备	包含Cisco IOS、Huawei Quidway、Juniper NetScreen、H3C Comware、General Network。
数据库	包含Oracle、MSSQL、MYSQL、DB2。
应用系统	包含B/S、C/S、Weblogic、BS IE。

RIS所支持的所有资产访问协议如下：

访问协议	说明
SSH	Secure Shell。一种字符终端服务，但是因为使用加密通信因此更加安全。SSH目前已经广泛用于各种Unix-like类和网络设备中，其默认通信端口为TCP 22。

访问协议	说明
Telnet	字符终端服务之一，主要用于网络设备、各种带外管理口和较老的Unix、Linux设备中，默认的通信端口为TCP 23，是一种明文传输方式。
RDP	Remote Desktop Protocol，远程桌面协议。是由微软开发的一种专有图形会话协议，默认通信端口为TCP 3389。
XDMCP	X Display Manager Control Protocol，Unix中默认的图形访问协议。使用该服务要求目标设备开启UDP 177端口。
VNC	Virtual Network Computing。一种使用RFB协议的显示屏画面分享及远程操作软件。此软件借由网络，可发送键盘与鼠标的动作及即时的显示屏画面。VNC与操作系统无关，因此可跨平台使用。默认通信端口为5900，也可以设置在5900-5999之间。
XFWD	X11 Forwarding。一种采用SSH进行端口转发，实现Unix-like设备图形访问的方法。使用该服务要求必须为目标设备配置SSH服务，并开放目标设备上sshd服务的X Forward功能。
SFTP	SSH File Transfer Protocol，也称Secret File Transfer Protocol，SSH文件传输协议，是一种数据流连接，提供文件访问、传输和管理功能的网络传输协议。

查找资产

访问RIS中的资产，需要先根据资产管理和权限管理，配置添加好对应的资产及权限，然后查找到对应的资产并进行访问。

在Web界面中查找资产主要有以下方式：

直接查找

1. 使用操作员帐号登录RIS Web界面。
2. 选择**工作台** > **访问资产**。
3. 在左侧导航栏中，选择动态视图中的具体节点，查看对应节点下资产。
4. （可选）在右侧下拉菜单中选择**快速搜索**，并在搜索框中输入资产名称/IP/简要说明/系统帐号，并按回车键进行搜索；或在下拉菜单中选择**高级筛选**，设置待查找资产对应的筛选条件并单击**筛选**，进行资产筛选。
5. 在右侧列表中找到对应的资产，列表从左到右会依次显示资产名称、IP、简要说明、快捷登录、登录选项及收藏按钮。

在最近访问中查找

1. 选择**工作台** > **访问资产**。如已在访问资产界面，单击左上角的**访问资产**图标，返回访问资产主界面。

2. 在右侧选择**最近访问**页签。下方会根据访问时间由近到远，依次列出最近访问过的资产。选择一条资产进行访问。

添加收藏并访问收藏

1. 在**访问资产**界面的资产列表最右侧，单击☆，将该条资产加入登录用户的收藏中。
2. 选择**工作台** > **访问资产**。如已在访问资产界面，单击左上角的**访问资产**图标，返回访问资产主界面。
3. 选择**收藏**页签，下方会列出登录用户所有收藏的资产。选择一条资产进行访问。

建立会话

通过RIS建立会话有以下3种方式。

会话（Session）是指用户通过本地终端与目标资产设备之间建立连接，并进行通信的过程。通过RIS建立的会话分为字符会话、图形会话、数据库会话和文件传输会话。

为了保证安全性，RIS要求用户不能直接从本地终端访问目标资产，而是先登录RIS，再通过RIS访问目标资产，从而使用户可以访问目标资产，即建立起本地终端和目标资产之间的会话。

通过Web界面建立会话

通过RIS的Web界面建立会话，支持RIS中所允许的所有形式的访问。基于Web界面的各种资产访问方式的步骤基本一致，只在前提条件和配置步骤上有一些差异，本文仅给出通用的步骤，并对不同访问方式的差异进行说明。

当前登录帐号使用的全局会话设置，请在**帐号设置**菜单中修改。请参考修改会话配置完成帐号会话配置的修改。

针对不同的资产类型和通信协议，访问相应的资产需要满足的前提条件如下。如资产无法访问，请联系管理员检查以下前提条件是否满足，并参考资产管理和权限管理完善配置。

主机和网络设备

表 17: 主机/网络设备支持的不同协议类型的前提条件

主机类型	协议类型	前提条件
Linux、HP UX、IBM AIX主机和各种网络设备	SSH	• SSH访问规则中没有对RIS的IP进行限制。 • 待访问主机的防火墙已开放了SSH服务所用的端口，如TCP 22。
	Telnet	• 待访问主机上已安装了telnet-server，并启用了telnet.socket服务。 • 待访问主机上Telnet的配置如不支持缺省root帐号登录，待访问主机上已配置了root帐号以外的其他可访问帐号。 • 待访问主机的防火墙开放了Telnet服务所用的端口，如TCP 23。

主机类型	协议类型	前提条件
	VNC	• 待访问主机上已安装了VNC Server，如tigervnc-server，并启动了相关服务。 • 待访问主机上已安装了图形界面工具，如gdm或lightdm，并启动了相关服务。 • 已为VNC Server配置了用于远程访问的密码。 • 待访问主机的防火墙已开放了VNC服务所用的端口，如TCP 5901。 • 待访问主机在RIS上配置的访问权限支持通过any帐号访问。
	XDMCP	• 待访问主机上已安装了图形界面工具，如lightdm和xfce桌面，并启动了相关服务。 • 待访问主机的防火墙已开放了XDMCP服务所用的端口，如UDP 177。
	XFWD	• 待访问主机上已安装了图形界面工具，如lightdm和xfce桌面，并启动了相关服务。 • 待访问主机上已安装了终端模拟器工具，如xterm。 • 待访问主机的/etc/ssh/sshd_config的X11_Forwarding已设置为**yes**。 • 待访问主机的防火墙已开放了SSH服务所用的端口，如TCP 22。
	SFTP	• 本地PC上已安装了FileZilla或WinSCP工具，和**帐号设置** > **会话配置** > **文件传输**中设置的会话访问方式相匹配。 • 待访问主机的防火墙已开放了SSH服务所用的端口，如TCP 22。
Windows主机	RDP	• 待访问的主机支持远程桌面连接，并且被设置为允许连接。 • 待访问主机的防火墙已开放了RDP服务所用的端口，如TCP 3389。
	VNC	• 待访问的主机安装了VNC server。 • 已为VNC Server配置了用于远程访问的密码。 • 待访问主机的防火墙已开放了VNC服务所用的端口，如TCP 5900。 • 待访问主机在RIS上配置的访问权限支持通过any帐号访问。

数据库

- 待访问的数据库所安装的主机，满足表 17: 主机/网络设备支持的不同协议类型的前提条件。

- 应用发布服务器已安装了对应的数据库软件并完成相关配置，如：SqlDbx , Toad , oem , plsqldev , sqldeveloperW , sqlplusw，Ssms，SQLyog , navicat，QuestCentral , SqlDbxForDB2 , ToadForDB2。如需要密码代填，已完成代填脚本的导入。

应用系统

- 应用发布服务器状态正常。
- RIS上已完成了应用发布远程客户端的相关配置。如需要密码代填，已完成代填脚本的导入。

通过Web界面建立会话的配置步骤如下：

1. 使用操作员帐号登录RIS Web界面并查找资产。
2. 单击**访问**，在下拉菜单中配置会话相关参数。

表 18: 配置会话参数

参数	说明
系统帐号	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： • self：同用户帐号。使用和当前登录RIS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。RIS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。 • RIS上已添加的资产帐号名称，例如**root**，RIS使用该帐号登录到资产设备。 **说明:** • 帐号名称之前有*，表示该帐号的密码已在RIS上托管，RIS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AD/LDAP/RADIUS其中之一认证或双因子认证中包含AD/LDAP/RADIUS之一，则使用对应的AD/LDAP/RADIUS用户名同名的帐号登录资产；如用户使用AD/LDAP+RADIUS双因子认证，则使用第一重认证所使用的AD/LDAP/RADIUS用户名同名帐号。
客户端	仅当访问的资产是数据库、应用系统时需要配置。 用于选择使用哪种客户端打开对应的资产。选项范围为由超级管理员全局添加并由配置管理员在配置资产时勾选的所有客户端。

参数	说明
屏幕大小	仅当帐号设置中RDP会话使用mstsc方式启动，且待访问的资产为Windows主机或应用系统时为需要配置。应用系统需要该应用的远程客户端设置中，**RemoteAPP**参数设置为**不使用**，否则将不显示该参数。 用于选择打开的远程会话的屏幕的分辨率。
磁盘映射	仅当帐号设置中RDP会话使用mstsc方式启动，并且访问的资产是Windows主机（使用RDP方式登录）、应用系统时需要配置。用于标识是否启用磁盘映射并选择磁盘映射的盘符。 启用磁盘映射，并勾选或手动设置待映射的盘符，将本地PC对应盘符的硬盘，映射到待访问的资产上，使访问者可以直接在该资产上对本地PC上的相应硬盘进行读写操作。
启用Console连接	仅当使用RDP方式登录Windows主机，且该资产的RDP访问协议设置中勾选了**console**时显示该参数。 仅当待访问的主机系统是Windows Server时需要启用Console连接。启用Console连接表示使用**/console**参数登录Windows Server 2003，从而打开一个session id为0的控制台会话，或使用/admin参数登录Windows Server 2008/2012/2016，打开一个session id为0的管理员模式的会话。

说明:

- 所有资产在被访问过之后，都会生成一个快捷登录图标，如  ，也可以直接单击该图标，采用和上次访问同样的配置再次访问该资产，或单击**更多**，选择其他访问过的配置。主机和网络设备即使没有被访问过，也会默认显示一个图标，其他资产之前未被访问过，则不会显示此图标。
- 如需要一次打开多个资产，请在每一条待启动的资产条目前进行勾选，并单击下方的**批量启动**按钮。
- 用户可以单击**在线会话**列对应的**查询**按钮，查看当前有哪些**在线会话**和**相关会话**。**相关会话**只针对主机资产，当不同的主机资产的IP地址相同时，这些资产的会话都会显示在这里。
- 用户可以通过单击右上角的  ，勾选访问界面要显示的列信息，包括资产名称、资产IP、部门和简要说明。

3. 确认配置无误后，单击**启动**建立远程会话并打开。

说明:

- 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。
- 使用SFTP连接，在当前本地PC首次启动后需要选择FileZilla或WinSCP的安装路径。完成选择之后，后续启动时将不需要再次进行选择。
- 如超级管理员在**系统设置** > **资产** > **访问设置** > **所有会话**中设置了默认备注方式为**可填**或**必填**，则单击**启动**后会弹出输入的备注的对话框，请输入备注后并单击**启动**。备注是一个1~100长度的字符串。
- 使用VNC、XDMCP、XFWD或Web方式启动的RDP协议打开图形会话时，可以单击上方的**展开/收起**按钮，展开标题栏，并单击右上方的按钮，实现**发送Ctrl+Alt+Del**、**剪贴板**、**全屏**、**断开连接**等操作。
- 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。

通过Mstsc客户端建立图形会话

通过Mstsc（Microsoft terminal services client）客户端建立到Windows服务器的图形会话有两种方式：RDP直连和RDP透传。

- RDP直连：操作员使用Mstsc先登录到RIS，在RIS找到待访问的资产后再建立图形会话进行访问。
- RDP透传：操作员如果提前知道待访问资产的IP地址和登录帐号，并且该帐号在RIS上已托管了帐号密码，可以直接使用Mstsc建立到待访问资产的图形会话。

说明： 不管是RDP直连还是RDP透传，屏幕大小、剪贴板和磁盘映射参数都需要在Mstsc客户端中进行配置。RIS连接到资产时将沿用用户在Mstsc上的配置。

RDP直连

1. 通过RDP登录RIS。界面中会列出当前登录用户所有可以访问的Windows主机资产和上一次连接使用的帐号。
2. 在**Name/IP/Remark(F2)**输入待访问资产的名称、IP或说明内容，并按**搜索**进行搜索。
3. 选中一条待访问的资产，双击该资产，设置会话参数，并单击**确定**，建立图形会话。

表 19: 配置Mstsc客户端图形会话参数

参数	说明
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RIS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。RIS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。 • RIS上已添加的资产帐号名称，例如**administrator**，RIS使用该帐号登录到资产设备。 **说明:** • 帐号名称之前有*，表示改帐号的密码已在RIS上托管，RIS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，仅支持使用本地密码或AD/LDAP/RADUIS这些认证方式，并使用对应同名帐号的密码完成在登录资产时的代填；如使用双因子认证，将仅使用第一维认证的密码。。
console	仅当该资产的RDP访问协议设置中勾选了**console**时显示该参数。 仅当待访问的主机系统是Windows Server时需要启用Console连接。启用Console连接表示使用**/console**参数登录Windows Server 2003，从而打开一个session id为0的控制台会话，或使用/admin参数登录Windows Server 2008/2012/2016，打开一个session id为0的管理员模式的会话。

RDP透传

1. 在Windows系统的**运行**或搜索框中输入**mstsc**，打开**远程桌面连接**。
2. 参数设置如下，完成后单击**连接**。

参数	说明
计算机名	**RIS的IP地址**
用户名	**RIS的用户名/目标资产的IP地址/访问目标资产的帐号**

说明:

- 通过RDP透传访问时，目标资产仅支持IP地址，不支持域名。
- 如果目标资产的IP地址或者帐号输入有误，则进入RDP直连RIS的界面。
- 如目标资产使用IPv6地址，不能加中括号；如RIS使用IPv6地址，可以加中括号也可以不加。

通过Telnet/SSH客户端建立字符会话

操作员可以使用Telnet/SSH客户端，如Xshell、Putty、SecureCRT，通过SSH登录到RIS，然后选择待访问的资产，并通过Telnet/SSH进行访问。

操作员如果提前知道待访问资产的IP地址和登录帐号，并且该帐号在RIS上已托管了帐号密码，可以直接在字符终端中输入用户名为**RIS的用户名/目标资产的IP地址/访问目标资产的帐号**，IP地址为**RIS的IP地址**，密码/密钥为**该用户名在RIS上的密码/密钥**进行访问，例如：

```
ssh opt/10.10.33.30/root@10.10.33.1
```

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RIS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的命令行中使用ssh命令直连访问。

通过该方式连接后，操作员可以直接经过RIS登录到待访问资产。RIS会根据该资产配置的访问协议（Telnet/SSH）自动进行连接，如该资产同时配置了Telnet/SSH，则默认使用SSH进行连接。

本节主要介绍通过SSH登录到RIS交互终端，并通过交互终端的菜单选择待资产从而进行访问的过程。通过SSH登录RIS之后，各种基本操作如下：

表 20: 字符会话常用操作

使用场景	输入	说明
最外层**资产分组列表**菜单	q	退出登录RIS
	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

使用场景	输入	说明
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RIS

1. 通过SSH登录RIS。
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。界面上会显示出该资产分组下，当前用户所有可访问的资产列表。

   说明: 资产分类会根据修改字符会话配置中的**直连分类方式**进行展示。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。
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。

   说明:

   - self：同用户帐号。使用和当前登录RIS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。RIS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。
   - RIS上已添加的资产帐号名称，例如**root**，RIS使用该帐号登录到资产设备。

   帐号名称之前有*，表示该帐号的密码已在RIS上托管，RIS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，仅支持使用本地密码或AD/LDAP/RADUIS这些认证方式，并使用对应同名帐号的密码完成在登录资产时的代填；如使用双因子认证，将仅使用第一维认证的密码。

   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。

共享会话

用户可以通过RIS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。

会话共享支持同一个用户同时共享多个字符或图形会话，并且每个会话都可以共享给多个不同的用户。会话共享后，所有加入共享的用户都将看到同一个会话界面，并且同步所有键鼠操作。

会话共享不要求加入共享的用户拥有该资产的访问权限，只需要开启共享的用户拥有访问权限。

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。

RIS没有对同一个会话共享加入的人数设置限制，只有字符会话会受到系统设置中字符终端的并发登录数量的限制。但不建议一个会话同时共享给太多人，因为不同人的操作会互相影响。

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Telnet/SSH客户端建立的会话。在本地PC通过Mstsc客户端建立的会话，无法进行会话共享。
- 会话共享不支持共享SFTP会话和配置了会话复核的会话。SFTP会话和配置了会话复核的会话将不会在可共享的列表中显示。
- RDP会话共享仅支持Web方式。如果**帐号设置** > **会话配置** > **图形会话**中的图形会话访问方式被设置为mstsc，则所有RDP会话将不会在可共享的列表中显示。
- 应用系统会话共享，仅支持Web方式且不能使用RemoteAPP。如果系统设置使用RemoteAPP打开应用系统会话，则所有应用系统会话将不会在可共享的列表中显示。如需共享这些会话，请联系超级管理员，在**系统设置** > **远程客户端** > **远程客户端**中，设置启动应用系统的浏览器的**RemoteAPP**参数为**不使用**。
- 只有会话共享的发起者可以将会话共享给其他用户，会话共享的受邀人不能再将该会话共享给其他用户。

发起共享

1. 通过Web界面建立会话或通过Telnet/SSH客户端建立字符会话。
2. 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，在下拉菜单过滤中选中该用户，并单击**确定**，发送邀请给对应的用户。

   说明:

   - 发送邀请后，会话共享列表中将显示该共享会话。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。
   - 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**。

加入共享

受邀人收到共享邀请后可以选择加入会话共享。

1. 登录RIS Web界面。

2. 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。
3. 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。

> **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。

传输文件

传输文件是指用户将本地PC通过RIS访问目标设备，并且将本地PC作为客户端，将资产设备作为服务端，从资产设备上上传/下载文件的操作。

基于RIS的文件传输方式有很多种。下表列出了RIS支持的所有文件传输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。

> **说明:** 对于配置了**跳转来源**的资产或者**切换自**的帐号，不支持通过SFTP传输文件。

表 21: 不同文件传输方式的比较

传输方式	目标资产系统类型	依赖软件	推荐程度
通过Web界面建立SFTP会话传输文件	Linux、HP Unix、IBM AIX	本地PC： • AccessClient • SFTP工具（FileZilla或WinSCP之一）	目标资产非Windows时推荐
通过SFTP工具直连目标资产传输文件	Linux、HP Unix、IBM AIX	本地PC：SFTP工具（FileZilla、WinSCP、Xftp等）	不推荐
在字符终端中通过SFTP传输文件	Linux、HP Unix、IBM AIX	本地PC为Windows时需要安装字符终端工具，如Xshell	本地PC为Linux/Unix时推荐
在字符会话中通过ZMODEM传输文件	Linux、HP Unix、IBM AIX	• 目标资产：lrzsz • 本地PC为Windows时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
在RDP图形会话中通过剪贴板传输文件	Windows	本地PC：Mstsc客户端	目标资产为Windows时推荐

传输方式	目标资产系统类型	依赖软件	推荐程度
在RDP图形会话中通过磁盘映射传输文件	Windows	本地PC：Mstsc客户端	目标资产为Windows时推荐

通过Web界面建立SFTP会话传输文件

用户可以登录RIS客户端，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。

前提条件如下：

- 目标资产的类型必须为Linux、HP Unix、IBM AIX其中之一。
- 本地PC的类型必须为Windows或MacOS。
- （请和配置管理员确认）用户具有目标资产的访问权限，且传输的单文件大小没有超过单文件大小上限。
- 使用的资产帐号具有文件待下载路径的读权限和待上传路径的写权限。
- 本地PC已安装了Filezilla或WinSCP工具。

通过RIS Web界面建立SFTP会话，只能使用Filezilla或WinSCP工具，在**帐号设置** > **会话配置** > **文件传输**中设置。本文以WinSCP为例进行介绍。

1. 参考通过Web界面建立会话，建立到目标资产的SFTP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**。

   会话建立成功后，会弹出WinSCP的界面，左侧和右侧分别是本地PC和目标资产的文件列表。

2. 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。
   - 上传：在左侧选中待上传的文件或文件夹，单击**上传**或**后台上传**。
   - 下载：在右侧选中待下载的文件或文件夹，单击**下载**或**后台下载**。

   说明： 可以使用**Shift**或**Ctrl**选中多个文件并上传/下载。

4. 在弹出的对话框中，直接采用默认传输设置并单击**确定**。

   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，请取消传输或联系配置管理员调整权限。

通过SFTP工具直连目标资产传输文件

用户可以直接通过SFTP工具，建立从本地PC到RIS再到目标资产之间的SFTP会话，从而完成与目标资产间的文件传输。

前提条件如下：

- 目标资产类型必须为Linux、HP Unix、IBM AIX其中之一。
- 本地PC类型必须为Windows或MacOS。
- （请和配置管理员确认）用户具有目标资产的访问权限，且传输的单文件大小没有超过单文件大小上限。
- 使用的资产帐号具有文件待下载路径的读权限和待上传路径的写权限。

- 本地PC已安装了Filezilla、WinSCP或Xftp工具。
- 用户已提前获取了目标资产的IP地址。
- 使用的资产帐号已在RIS中托管了密码。

可以使用各种支持SFTP协议的工具，如Filezilla、WinSCP、Xftp等，建立到目标资产的会话。本文以WinSCP为例进行介绍。

通过SFTP工具无法在连接到RIS之后再查看可以连接的资产并连接资产。因此必须提前准备好目标资产的IP地址，并确保连接目标资产的帐号已在RIS上托管密码。

1. 打开SFTP工具，如WinSCP。
2. 单击**新建会话**，会话参数如下：
   - 文件协议：SFTP
   - 主机名：RIS的IP地址。
   - 端口号：22
   - 用户名：按照以下格式输入：**RIS的用户名/目标资产的IP地址/访问目标资产的帐号**
   - 密码：RIS登录用户名对应的密码

   说明：例如，RIS的IP为10.10.33.1，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RIS上托管了密码。则输入的主机名为10.10.33.1，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（RIS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、Xftp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. 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。
   - 上传：在左侧选中待上传的文件或文件夹，单击**上传**或**后台上传**。
   - 下载：在右侧选中待下载的文件或文件夹，单击**下载**或**后台下载**。

   说明：可以使用**Shift**或**Ctrl**选中多个文件并上传/下载。
5. 在弹出的对话框中，直接采用默认传输设置并单击**确定**。

   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，请取消传输或联系配置管理员调整权限。

在字符终端中通过SFTP传输文件

用户可以在字符终端中，直接通过SFTP命令，建立从本地PC到RIS 再到目标资产之间的SFTP会话，从而完成与目标资产间的文件传输。用户也可以在字符终端中直接打开文件传输工具，例如在Xshell中单击文件传输图标，启动Xftp进行文件传输，操作方法请参见通过SFTP工具直连目标资产传输文件。

前提条件如下：

- 目标资产的类型必须为Linux、HP Unix、IBM AIX其中之一。
- （请和配置管理员确认）用户具有目标资产的访问权限，且传输的单文件大小没有超过单文件大小上限。
- 使用的资产帐号具有文件待下载路径的读权限和待上传路径的写权限。
- 用户已获取目标资产的IP地址。
- 使用的资产帐号已在RIS中托管了密码。

1. 打开本地字符终端。如本地PC为Windows，请使用Xshell等工具。
2. 输入sftp命令连接到目标资产：

   ```
   sftp RIS的用户名/目标资产的IP地址/访问目标资产的帐号@RIS的IP地址
   ```

   说明： 例如，RIS的IP为10.10.33.1，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RIS上托管了密码。则输入sftp opt/10.10.33.30/root@10.10.33.1。

   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]。
3. 输入RIS登录用户名对应的密码。

   RIS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。
4. 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）
   ```

在字符会话中通过ZMODEM传输文件

用户可以在字符终端中连接到RIS，并通过RIS再连接到目标资产，然后使用rz和sz命令上传/下载文件。

前提条件如下：

- 目标资产类型必须为Linux、HP Unix、IBM AIX其中之一。
- 本地PC类型必须为Windows或MacOS。
- 如本地PC类型为Windows，已安装了字符终端工具，如Xshell、SecureCRT，不支持Putty。
- （请和配置管理员确认）用户具有目标资产的访问权限。
- 使用的资产帐号具有文件待下载路径的读权限和待上传路径的写权限。
- 目标资产上已安装了lrzsz包。

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，并将文件以字符的形式进行传输，完成文件的上传和下载。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，CentOS系统可以通过yum install lrzsz命令直接下载并安装。

建立本地PC和目标资产直接的字符会话，可以通过Web界面来建立，也可以直接通过字符终端连接到RIS再跳转到目标资产。

1. 通过Web界面建立字符会话或通过Telnet/SSH客户端建立字符会话。
2. 决定上传或下载文件：
   - 上传文件 => 3。
   - 下载文件 => 4。
3. 上传文件。
   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。
4. 下载文件。
   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。

在RDP图形会话中通过剪贴板传输文件

本地PC与Windows主机之间的文件传输，建议首选此方式。通过RDP登录到目标主机后使用剪贴板完成文件传输。

通过剪贴板传输文件的前提条件如下：

- 目标资产和本地PC类型都必须为Windows（不支持Windows Server 2003），目标资产支持远程登录，本地PC支持远程访问其他主机。
- （请和配置管理员确认）用户拥有目标主机的访问权限。
- （请和配置管理员确认）用户使用的权限规则模板中，**上行文件**和**下行文件**选项被勾选。
- 通过RIS Web界面建立RDP图形会话时，必须将**帐号设置** > **会话配置** > **图形会话**中的图形会话访问方式设置为**mstsc**。

通过RIS Web界面建立RDP图形会话，和直接通过mstsc远程登录到RIS并跳转到目标主机，都可以使用剪贴板实现文件传输。

1. 通过Web界面建立会话或通过Mstsc客户端建立图形会话。

说明： 通过Mstsc客户端建立会话，需要启用远程桌面的剪贴板设置，该设置默认启用。如未启用，需要在连接到RIS前修改远程桌面设置。以本地PC为Windows10为例，请在**本地资产** > **本地设备和资产**中勾选**剪贴板**。

2. 使用复制粘贴的方式在图形会话窗口和本地PC之间传输文件。

说明： 如无法复制粘贴，请参照前提条件，检查是否拥有该主机的访问剪贴板的权限。如权限正常，请检查目标主机和本地PC上是否存在rdpclip.exe进程，并尝试启动或重启该进程。

在RDP图形会话中通过磁盘映射传输文件

本地PC与Windows主机之间的文件传输，可以使用此方式。通过RDP登录到目标主机后，将本地PC的硬盘映射到目标主机，完成文件传输。

通过磁盘映射传输文件的前提条件如下：

- 目标资产和本地PC类型都必须为Windows，目标资产支持远程登录，本地PC支持远程访问其他主机。
- （请和配置管理员确认）用户拥有目标主机的访问权限。
- （请和配置管理员确认）用户使用的权限规则模板中，**允许客户端磁盘映射**选项被勾选。
- 通过RIS Web界面建立RDP图形会话时，必须将**帐号设置** > **会话配置** > **图形会话**中的图形会话访问方式设置为**mstsc**。

通过RIS Web界面建立RDP图形会话，和直接通过mstsc远程登录到RIS并跳转到目标主机，都可以使用磁盘映射实现文件传输。

1. 通过Web界面建立会话或通过Mstsc客户端建立图形会话。

说明： 启动会话前，需要配置磁盘映射，配置方法如下：

- 通过Web界面建立会话，设置启动参数时，需要勾选待映射的**磁盘映射**的盘符，或在**其他盘符**中手动填入映射盘符。
- 通过Mstsc客户端建立会话，需要在连接到RIS前就进行磁盘映射的设置。以本地PC为Windows10为例，在远程桌面连接中，选择**本地资产** > **本地设备和资产** > **详细信息**，在**驱动器**节点下，勾选待映射的磁盘盘符。

2. 打开**Windows资产管理器**，找到映射的磁盘，名称显示为**本地PC名称上的盘符**，如“DESKTOP-PC1 上的C”。
3. 进入该磁盘，将该磁盘和目标主机本地磁盘之间的文件进行复制粘贴操作，以实现文件传输。

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。

根据管理员在配置高危操作中的配置，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。

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。 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。**	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。	1. 选择复核人并启动会话。 • 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。 2. 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会话复核，完成复核后操作员可以进行操作。 **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。
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命令复核。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。

现象	说明	处理方法
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。

说明：当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。具体方法如下：

1. 操作员使用自己的帐号登录RIS Web界面。
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。也可以直接选择**工作台** > **高危操作** > **待复核** > **待我复核。**
3. 单击**复核**打开对应的会话复核。
4. 在弹出的对话框中，输入密码并单击**确定。**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。
5. 参考复核高危操作完成会话复核。

复核人不是使用动态令牌的用户时，操作员将收不到该复核提醒，无法自己进行复核。该方法仅适用于会话复核，不支持命令复核。

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。

客户端兼容性列表

RIS支持的客户端如表 22: 客户端兼容性列表所示。其中Web界面、Console控制台访问客户端用于访问RIS，其他客户端用于通过RIS访问资产。

表 22: 客户端兼容性列表

客户端类型	客户端名称	支持版本
Web界面&图形会话（Web）	IE	IE11及以上
	Chrome	Chrome49及以上
	Firefox	Firefox50及以上
字符会话&控制台访问	Putty	Putty0.58及以上
	Xshell	Xshell4.0及以上
	SecureCRT	SecureCRT6.5及以上 **说明：** 如RIS或资产的地址为IPv6，建议使用SecureCRT8.0版本。
	Terminal	Terminal2.7及以上
	pcomm（仅字符会话）	只支持固定的版本，请参考表 23: 字符会话建议使用的客户端列表。
图形会话（mstsc）	mstsc	5.1及以上
文件传输	FileZilla	3.2及以上
	WinSCP	5.11及以上

部分字符客户端在特定环境下使用时可能存在兼容性问题。但字符会话客户端由于版本众多，和操作系统版本也存在一定的对应关系，无法一一列举。表 23: 字符会话建议使用的客户端列表中给出了特定操作系统下建议使用的客户端，这些客户端经过了充分的测试，请在遇到问题时直接安装该表格中建议的客户端。

表 23: 字符会话建议使用的客户端列表

操作系统	建议客户端
windows xp x86 SP3	• Putty0.67 • SecureCRT6.5 • Xshell4

操作系统	建议客户端
windows 7 x86 sp2	• Putty0.58 • SecureCRT7.3 • Xshell5 • pcomm5.0(CN)、pcomm5.7(EN)和pcomm5.8(CN) **说明：** pcomm5.7(EN)不支持通过Web界面打开，但支持外部直连和审计功能。
windows 7 x64 sp1	• Putty0.58 • SecureCRT7.0 • Xshell4 • pcomm5.9 **说明：** pcomm5.9仅支持审计功能，不支持Web访问和外部直连。
Windows 8.1 x86	• Putty0.67 • SecureCRT8.1 • Xshell5
Windows 8.1 x64	• Putty0.67 • SecureCRT8.0 • Xshell5
Windows 10 x86	• Putty0.67 • SecureCRT7.0 • Xshell6
Windows 10 x64	• Putty0.67 • SecureCRT8.0 • Xshell5 • pcomm 6.0（EN） **说明：** pcomm 6.0（EN）不支持通过Web界面打开，但支持外部直连和审计功能。

操作系统	建议客户端
MAC OS 10	• SecureCRT7.3、SecureCRT8.3 • Terminal2.7

说明: 在Windows7_x64、Windows8.1_x64、Windows10_x32、Windows10_x64系统下，如使用SecureCRT7.3及以上版本访问字符会话，将看到以下提示：

```
The client has disconnected from the server.  Reason:
Message Authentication Code did not verify (packet #4). Data integrity has been compromised.
```

此时请在该会话的**Properties**设置中，选择**Connection** > **SSH2** > **Advanced** > **MAC**，去勾选**SHA2-512**选项，并单击**OK**保存。

同样，通过字符客户端访问RIS的Console控制台时，部分客户端版本也可能存在兼容性问题。建议使用的客户端版本请参考：

表 24: 登录Console控制台建议使用的客户端列表

操作系统	客户端
Windows 7 x64 SP1	• SecureCRT6.5/7.0/8.0/8.1 • Xshell4/5 • Putty0.67
Windows10 x86	• SecureCRT6.6/7.0/7.3/8.0/8.1 • Xshell4/5 • Putty0.67

mstsc建议的版本及操作系统如下：

表 25: mstsc建议版本

操作系统	建议版本
Windows XP SP2	5.1.2600/6.0.6000/6.0.6001
Windows XP SP3	6.0.6001/6.1.7600
Windows 7 SP1	6.1.7601/6.2.9200
windows 8	6.2.9600
windows 10	10.0.10240

操作系统	建议版本
Windows Server 2003 SP2	5.2.3790/6.0.6000
Windows Server 2008 SP1	6.0.6002
Windows Server 2012	6.3.9600

审计

6

目录:

能够使用审计功能的用户类型包括：**审计管理员**、**超级管理员**及其他自定义的拥有审计授权的用户类型。本章节指导用户完成RIS所有基本的审计操作。审计操作均需要在RIS的Web界面上执行。

审计是指在Web界面上，对RIS用户和系统的所有操作行为进行查看，以解决操作事故责任认定的问题，确保事故发生后，能快速定位操作者和事故原因，还原事故现场和举证。

拥有审计权限的用户实现审计操作的前提条件如下：

- 已完成安装AccessClient。
- 已在本地PC安装了JAVA JRE（建议版本为1.6及以上）从而对图形会话进行回放。

超级管理员和审计管理员默认拥有所有审计权限。自定义的用户角色如添加了审计权限，可以具体配置是否勾选**查看键盘记录**和**下载会话**权限，参见配置用户角色权限。这两项权限具体对应的操作如下：

权限	**支持的操作**
查看键盘记录	在**工作台** > **审计** > **问题检索** > **按会话操作检索**界面支持以下操作 • 会话类型可以选择**字符会话**。 • 检索图形会话时可以输入**模拟操作**进行检索。
	在**工作台** > **审计** > **操作审计** > **字符会话**界面支持查看**详情**。
	在**工作台** > **审计** > **操作审计** > **图形会话**界面支持以下操作： • 单击**按键**查看具体的按键记录。 • 单击**详情**后可以查看**模拟操作**和**剪贴板记录**。 • 执行**回放**操作时，可以通过**e**或**k**快捷键显示按键操作。
下载会话	在**工作台** > **审计** > **操作审计** > **字符会话**界面，支持单击**下载**，下载会话记录文件。

权限	支持的操作
	在**工作台** > **审计** > **操作审计** > **图形会话**界面，支持单击**下载**或在查看**详情**页面时单击**下载**，下载会话记录文件。

本章节后续内容将默认用户拥有**查看键盘记录**和**下载会话**权限来进行介绍，如找不到对应的功能，请对照上表检查是否具备相应权限。

审计操作分为两种，**操作审计**和**事件审计**。RIS也提供了**审计数据概览**、**会话情况统计**及**问题检索**等功能，方便审计管理员快速了解RIS的安全状况并对具体审计记录进行快速检索。

所有审计操作都必须在RIS Web界面上进行，因此请先登录RIS Web界面。本章节所有内容均默认用户已使用拥有审计权限的帐户登录了Web界面。本章节面向的读者对象主要是审计管理员，因此下文中提到的用户均称为审计管理员。

查看审计概览与统计

在RIS审计操作主界面，可以通过切换页签，查看**审计数据概览**与**会话情况统计**等相关信息，从而对系统的整体运行情况进行直观的了解。

查看审计数据概览

审计管理员可以查看审计数据概览，对当前的在线会话、用户、资产等信息进行查看，并通过单击相应内容，进行更细致的查看。

1. 进入审计界面主菜单。

   单击**工作台** > **审计**。如已在审计菜单中，单击左上角的**审计**图标，返回主菜单。

2. 选择**审计数据概览**页签。

3. 查看审计数据概览中的在线会话、用户、资产信息。可以单击各条统计信息的数字，跳转到详细的数据查看页面。

项目	说明	单击跳转后的内容
在线会话	显示当前所有在线的字符、图形、数据库会话的总数。	跳转到**在线会话**菜单，请参考审计在线会话进行相关操作。
在线字符会话	显示当前所有在线的字符会话的总数。	跳转到**字符会话**菜单，并在筛选条件中设置了状态为**活跃**。请参考审计字符会话进行相关操作。
在线图形会话	显示当前所有在线的图形会话的总数。	跳转到**图形会话**菜单，并在筛选条件中设置了状态为**活跃**。请参考审计图形会话进行相关操作。
在线数据库会话	显示当前所有在线的数据库会话的总数。	跳转到**数据库会话**菜单，并在筛选条件中设置了状态为**活跃**。请参考审计数据库会话进行相关操作。

项目	说明	单击跳转后的内容
在线用户	显示当前Web界面的所有在线用户的总数。	跳转到单独的Web在线用户查看页面。可以查看当前Web在线用户的帐号、姓名、来源IP、角色、活动会话数，并对指定用户执行强制下线。 **说明:** • 同一用户通过不同IP登录，或同一用户和IP通过不同浏览器登录，都会显示为不同的在线用户条目。 • 强制下线会使该用户的Web界面登录强制登出，是否会同时切断会话，取决于**系统设置** > **访问设置** > **所有会话**中的**会话切断策略**的设置。
在线资产	显示当前所有通过RIS建立了在线会话的资产的总数。	跳转到单独的在线资产查看页面。可以查看当前已建立会话的资产的资产名称、资产IP、资产类型、简要说明和活动会话数。 可以在搜索框中输入资产名称、资产IP、简要说明进行模糊查询，筛选要查看的在线的资产范围。

4. 查看**实时会话**信息。

   页面中央以折线图的形式显示了一天之内的实时会话变化数量，横坐标是时间，范围由当天0:00到第二天0:00，纵坐标是在该时间点在线会话的总数。RIS会将会话数量发生变化的每个时间点连接起来，以显示会话数量变化的折线图。

   审计管理员可以单击**全部会话**、**字符会话**、**图形会话**、**数据库会话**这些标签，决定折线图显示的不同内容。将鼠标移动到折线图上会显示具体的数量和时间点。

   说明: 该实时会话的折线图，也会默认直接显示在审计管理员登录之后的首页中。各审计管理员也可以登录RIS之后直接在首页进行查看，如果不需要也可以单击首页图形的右上角，选择**删除**，使该折线图不在首页显示。

查看会话情况统计

审计管理员可以查看RIS的会话情况统计，包括**本周TOP用户会话数**、**本周TOP资产会话数**、**在线会话**和**会话文件大小**。

请进入审计界面主菜单（单击**工作台** > **审计**；如已在审计菜单中，单击左上角的**审计**图标，返回主菜单），并选择**会话统计情况**进行查看。

会话情况统计的各块内容介绍如下：

本周TOP用户会话数

显示一周之内（从当前时间点往前的7*24小时内）访问会话数最多的5个用户。每个用户的会话总数以柱状图的形式呈现，柱状图中的每一块内容分别代表字符、图形、数据库会话的数量，具体含义参见图表下方的图例所示。

本周TOP资产会话数

显示一周之内（从当前时间点往前的7*24小时内）被访问次数最多的5个资产。每个资产建立的会话总数以柱状图的形式呈现，柱状图中的每一块内容分别代表字符、图形、数据库会话的数量，具体含义参见图表下方的图例所示。

在线会话

显示在线会话的总数以及字符、图形、数据库会话各自的总数。和**审计数据概览**中显示的相同，但此处仅作为显示，不能单击数字跳转到对应的页面。

会话文件大小

显示当前RIS后台存储的会话记录文件占用的磁盘空间大小。分为字符会话和图形会话两部分。单位为GB和MB，例如会话文件大小显示为5GB 20MB，表示实际大小为5GB+20MB。

说明：审计管理员登录之后的首页中，会默认显示**本周TOP用户会话数**，也可以在首页单击**+**，将本节中其他内容添加显示到首页。

检索问题

审计管理员可以按不同的检索方式对会话审计记录进行检索，从而快速找到期望的审计记录并进行问题定位。

在审计记录中检索问题，有以下4种方式：直接检索、按资产检索、按用户检索、按会话操作检索。

1. 选择**工作台** > **审计** > **问题检索**。
2. 在上方选择检索的时间范围，设置起始时间点和结束时间点，起始时间点必须早于结束时间点，结束时间点必须晚于RIS启动审计的时间，最小单位为分钟。不选择则默认时间范围为7天内。
3. 选择要使用的问题检索方式。
   - 直接检索：不设置其他检索筛选条件，直接检索当前设置的时间范围内的所有会话的审计记录。
   - 按资产检索：仅检索具体的一条或多条资产相关的会话审计记录。请勾选待检索的具体资产。

     可以先单击**筛选**设置筛选查找条件，或在搜索框中输入资产名称/IP/简要说明，查找到对应的资产并进行勾选，然后单击**确定**。如不勾选则默认检索当前审计管理员在RIS上可审计的所有资产。

     也可以单击下方的**Top活跃资产**列表中的某个资产，直接检索该资产相关的审计记录。
   - 按用户检索：仅检索指定用户相关的会话审计记录。请勾选待检索的用户。

可以先单击**筛选**设置筛选查找条件，或在搜索框中输入帐号/姓名，查找到对应的用户并进行勾选，然后单击**确定**。如不勾选则默认检索RIS上的所有用户。

也可以单击下方的**Top活跃用户**列表中的某个用户，直接检索该用户相关的审计记录。

- 按会话操作检索：仅检索包含某个具体操作的会话审计记录。单击**按会话操作检索**之后，会继续弹出对话框并进行选择。在下拉菜单中选择对应的选项，并在对话框中填入待筛选的值，单击**确定**。

选项	说明
字符会话	输入字符终端上执行的命令，例如ls、cd。
图形会话	输入以下内容其中的一条或多条： • 窗口标题：在会话的图形界面上打开的窗口的标题，例如库、任务管理器、Firefox。 • URL：B/S应用系统会话中，在浏览器窗口中访问的URL地址。例如www.example.com、192.168.1.1。 • 模拟操作：用户进行的鼠标或键盘的按键操作，包含在各种对话框、终端、编辑器中键入的文字内容。例如：<CtrlAlt-Delete>、cd D:\boot。
数据库会话	输入SQL语句，例如select。
文件传输	输入文件路径，例如/root。

说明:

- 在输入一条命令或其他内容后，需要按回车键，将该条命令生成一个筛选标签，此时可以单击**x**删除对应的标签。可以插入多个筛选标签。
- 所有内容都输入完之后，可以单击保存一个检索模板，这样会在窗口的最上方直接显示各个模板。可以直接单击某个模板名称选择套用该模板，单击删除该模板，或者单击清空输入内容。
- 检索条件设置好之后，可以单击下方的**指定资产检索**，设置同时启用资产检索作为第二重筛选条件；也可以直接单击**直接检索**，只按会话操作来检索。

4. 查看检索结果。

检索结果中，每行表示一条检索出来的会话。采用不同的检索方式时，检索结果的各列内容会有少许差异，具体如下：

显示项	说明
会话时间	会话开始的时间，例如**2018-08-06 19:24:19**。

显示项	说明
发起用户	通过RIS建立该会话的RIS用户的用户名及连接到资产的主机的IP地址，例如**admin(10.10.10.10)**。
连接资产	会话连接的资产名称及IP地址，例如**CentOS7(192.168.1.10)**。
操作信息	使用**按会话操作检索**时不会显示。另外，根据不同的会话类型，显示的内容会不一样： • 窗口标题数：仅图形会话时显示。用户打开的不同窗口的数量。仅有通过mstsc方式启动的，且使用Windows经典主题的图形会话，支持记录应用窗口的标题；只有IE浏览器支持记录标题，其他浏览器不支持。当不支持记录标题时，窗口标题数量始终显示为0。 • 执行命令数：仅字符会话时显示。 用户执行的命令的数量，括号前的数字表示命令总数，括号内的数字表示敏感命令的数量。敏感命令是在高危操作中定义的高危命令，当部署的RIS未启用高危操作功能时该数字始终为0。 • 文件传输结果：文件传输会话时会显示。显示为文件传输操作的结果，例如**下载文件成功**、**上传文件失败**、**下载文件无权访问**、**新建文件失败**等。
匹配结果	仅当**按会话操作检索**时会显示，显示匹配上的操作的数量，例如**已匹配5条**。并且在该条记录的下方会显示详细的匹配情况，匹配上的内容会用颜色标出。
更多	用户可以执行的更多操作，包含**详情**、**回放**、**下载**，在线会话还会显示**实时**和**切断**。具体含义请参考查看审计结果（操作类）中的介绍。

5. 可选： 切换会话类型。

可以选择页面上方的页签，按会话类型查看会话。**按会话操作的结果**不支持此功能。

页签	说明
会话	按用户设置的筛选条件检索出来的所有结果。
敏感会话	检索结果中包含敏感命令的会话。敏感命令是在高危操作中定义的高危命令，当部署的RIS未启用高危操作功能时请忽略此页签。
大日志会话	检索结果中会话审计记录文件超过100MB的会话。
特权会话	检索结果中使用特权帐号登录资产的帐号。

页签	说明
所有会话	仅当使用**直接检索**或**按用户检索**时会显示该页签。除了**会话**页签显示的会话之外，还会将符合筛选条件的用户的所有的登录、登出和修改设置的操作都作为会话列出来。但仅能对该页签中的各访问资产的会话条目执行**更多**操作。

6. 可选： 设置更多检索条件。
   - 在右上角单击，设置**会话类型**、**状态**、**协议**、**系统帐号**等筛选条件，从而组合更多的筛选条件。
   - 在页面底部选择**日期**、**资产**、**用户**，并在上拉菜单中勾选检索结果中的部分对象，从而缩小检索范围。
   - 单击最上方的时间范围，重新设置时间范围。
   - 在**按会话操作检索**的结果中，单击左上角的操作筛选条件之一，例如 ls (4) ll cd (0) ，变为白色的操作将不再被当做筛选条件进行检索。
7. 可选： 单击，或在**按会话操作检索**的结果中勾选待导出的会话后单击**导出**，将检索结果以.xls表格的形式下载到本地。

查看审计结果（操作类）

审计管理员可以查看所有在线或已完成的用户会话，查看会话的回放、按键、标题等信息，并对在线会话执行实时查看和切断等操作。

审计在线会话

审计管理员可以查看当前所有的正在进行的会话，对会话内容进行实时监视，并随时切断会话。

在线会话只会显示正在进行的字符和图形会话，不会显示文件传输会话。

1. 选择**工作台** > **审计** > **操作审计** > **在线会话**。
2. 查看在线会话信息。

   每一行都是一个在线会话。每一列显示的信息分别如下：

项目	说明
开始时间	会话开始的时间，例如**2018-08-06 19:24:19**。
来自	直接连接到资产的主机的IP地址。
用户帐号	用户登录RIS的帐号。
资产名	会话连接的资产在RIS上记录的名称。
系统帐号	会话连接使用的该资产上的帐号名称。
会话类型	图形会话或字符会话。
协议	会话使用的协议名称，例如ssh、rdp。应用系统会话该信息为空。

项目	说明
会话时长	会话从开始到当前时间的总计时长。单击↻后才会刷新该时长。
用户姓名	登录RIS的用户的姓名，在**帐号设置**中设置。
资产IP	会话连接的资产的IP地址。
操作	• **详情**：单击进入会话详情页面查看。具体解释请参见字符会话和图形会话对应的章节。 • **实时**：单击之后，针对图形会话，会给审计管理员打开一个vnc会话的web监视窗口；针对字符会话，会给审计管理员打开一个putty监视窗口。在该窗口中会显示操作员在图形或字符会话中的所有操作，但审计管理员不能进行任何操作。当操作员断开会话后，审计管理员的实时会话监视窗口也会被关闭；审计管理员也可以自行关闭实时监视窗口。 • **回放**：单击之后，会弹出一个对应的回放窗口，回放该会话的整个过程，具体解释请参见字符会话和图形会话对应的章节。 • **切断**：单击并确认之后，可以切断该正在进行的会话，正在进行会话的操作员将被强制断开会话连接。 • **更多** > **按键**：仅当会话为图形会话时会显示该选项。单击之后，会进入**按键**信息页面，可以查看到操作员在该会话界面执行的所有键盘和鼠标的操作以及具体的操作命令，并可以单击**回放**，从该操作的时间点开始回放所有操作。 • **更多** > **下载**：单击后将该会话的记录文件下载到本地，字符会话下载后的格式为.txt，图形会话下载后的格式为.rfx。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/姓名/资产/资产IP进行模糊查找，筛选出符合条件的会话。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条会话后单击**导出选中**，或直接单击**导出全部**，将会话列表导出为.xls格式的表格并下载到本地。

审计字符会话

审计管理员可以查看所有在线或已关闭的字符会话，并执行查看会话详情和回放等功能。字符会话包括所有主机、网络设备中使用ssh、telnet协议建立的会话。

1. 选择**工作台** > **审计** > **操作审计** > **字符会话**。
2. 查看所有字符会话信息。

   每一行都是一个字符会话。每一列显示的信息分别如下：

项目	说明
开始时间	会话开始的时间，例如**2018-08-06 19:24:19**。

项目	说明
结束时间	会话结束的时间，例如**2018-08-06 19:33:15**。
来自	直接连接到资产的主机的IP地址。
用户帐号	用户登录RIS的帐号。
用户姓名	用户登录RIS的帐号对应的姓名，在**帐号设置**中设置。
资产名	会话连接的资产在RIS上记录的名称。
系统帐号	会话连接使用的该资产上的帐号名称。
协议	会话使用的协议名称：ssh、telnet。
命令数	用户执行的命令的数量，括号前的数字表示命令总数，括号内的数字表示敏感命令的数量。敏感命令是在高危操作中定义的高危命令，当部署的RIS未启用高危操作功能时该数字始终为0。
会话时长	会话从开始到当前时间的总计时长。单击↻后才会刷新该时长。
状态	会话的连接状态：活跃、断开，或强制断开。强制断开表示审计管理员使用**切断**功能强制切断了该会话。
资产IP	会话连接的资产的IP地址。
文件(MB)	会话记录文件的大小，当大小小于0.01MB时只显示为“**<0.01 MB**”。
操作	• **详情**：单击进入会话详情页面查看。在会话详情页会按执行时间从早到晚的顺序依次列出该会话中执行过的各条命令，可以单击，从该条命令开始回放直到会话结束；单击**+**展开某条命令查看命令的回显，单击**-**收起命令回显。 • **回放**：单击之后，会弹出一个putty窗口（AccessClient自带），回放该字符会话从开始到结束的全过程，即每条用户输入的命令及命令回显。审计管理员可以按**空格**键暂停/取消暂停回放。 • **更多** > **下载**：单击后将该会话的记录文件以.txt的格式下载到本地。如果审计文件不存在，单击后，RIS将提示**文件尚未生成或已被迁移**。 • **更多** > **实时**：单击后会弹出一个putty窗口（AccessClient自带），实时显示操作员正在执行的所有命令及命令回显。当操作员断开会话后，审计管理员的实时会话监视窗口也会被关闭；审计管理员也可以自行关闭实时监视窗口。 • **更多** > **切断**：仅当该会话状态为**活跃**时会显示该选项。单击并确认之后，可以切断该正在进行的会话，正在进行会话的操作员将被强制断开会话连接。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/姓名/资产/资产IP进行模糊查找，筛选出符合条件的会话。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条会话后单击**导出选中**，或直接单击**导出全部**，将会话列表导出为.xls格式的表格并下载到本地。

审计图形会话

审计管理员可以查看所有在线或已关闭的图形会话，并执行查看会话详情和回放等功能。图形会话包括所有主机、网络设备中使用rdp、xdmcp、xfwd、vnc协议建立的会话、数据库会话及应用系统会话。

1. 选择**工作台** > **审计** > **操作审计** > **图形会话**。
2. 查看所有图形会话信息。

   每一行都是一个图形会话。每一列显示的信息分别如下：

项目	说明
开始时间	会话开始的时间，例如**2018-08-06 19:24:19**。
结束时间	会话结束的时间，例如**2018-08-06 19:33:15**。
来自	直接连接到资产的主机的IP地址。
用户帐号	用户登录RIS的帐号。
用户姓名	用户登录RIS的帐号对应的姓名，在**帐号设置**中设置。
资产名	会话连接的资产在RIS上记录的名称。
系统帐号	会话连接使用的该资产上的帐号名称。
协议	会话使用的协议名称：rdp、xdmcp、xfwd、vnc。应用系统会话该信息为空。
文件(MB)	会话生成的记录文件的大小。
会话时长	会话从开始到当前时间的总计时长。单击↻后才会刷新该时长。
状态	会话的连接状态：活跃、断开，或强制断开。强制断开表示审计管理员使用**切断**功能强制切断了该会话。
操作	• **详情**：单击进入会话详情页面查看。具体请参见4。 • **回放**：单击之后，会弹出一个JAVA窗口，回放该图形会话从开始到结束的全过程。具体请参见3。 • **标题**：单击之后，会显示用户操作的所有窗口的标题，仅支持Windows Server 2003使用XP主题或Windows Server 2003/2008使用经典主题，其他环境下将无法获取标题。

项目	说明
	• **更多** > **下载**：单击后将该会话的记录文件以.rfx的格式下载到本地。审计管理员可以单击右上角的用户名，选择**帮助** > **图形终端** > **离线回放**，下载GuiPlayer，安装后打开.rfx文件查看回放。如果审计文件不存在，单击后，RIS将提示**文件尚未生成或已被迁移**。 • **更多** > **实时**：单击后会弹出一个vnc窗口，实时显示操作员正在执行的所有操作及屏显。当操作员断开会话后，审计管理员的实时会话监视窗口也会被关闭；审计管理员也可以自行关闭实时监视窗口。 • **更多** > **切断**：仅当该会话状态为**活跃**时会显示该选项。单击并确认之后，可以切断该正在进行的会话，正在进行会话的操作员将被强制断开会话连接。
资产IP	会话连接的资产的IP地址。数据库、应用系统会话该项信息为空。
客户端类型	建立会话所使用的客户端类型，包括mstsc和novnc。
屏幕高	会话实际占用的屏幕高度。最大化时不包含任务栏的高度。
屏幕宽	会话实际占用的屏幕宽度。
应用地址	数据库、应用系统的IP地址。其他会话该项信息为空。
应用类型	数据库、应用系统的类型，包括DATABASE、B/S、C/S、B/S IE和Weblogic。其他会话该项信息为空。
应用客户端	连接数据库、应用系统所使用的应用客户端，例如Toad、chrome等。其他会话该项信息为空。

3. 可选： 在一条会话记录后，单击**回放**，打开回放窗口，观看该图形会话的整个过程。

   说明: 观看并控制回放窗口，请参考播放会话录屏。

4. 可选： 在一条会话记录后，单击**详情**，进入**会话详情**页面查看会话详情。

   审计管理员可以单击**会话详情**页面的各个页签，查看不同的信息：

   - **按大小切片**：为了防止单个会话记录文件过大，RIS会按文件大小或窗口标题进行切片，该页面会显示所有切片后的文件，如未满足要求没自动进行切片则不显示。需要超级管理员在**系统设置**中设置。默认切片大小为1MB，不使用**按标题切片**。

     说明: 目前标题审计仅支持以下环境，使用其他操作系统或主题，将无法正常产生按标题的切片：

     - Windows Server 2003使用XP主题
     - Windows Server 2003/2008使用经典主题

- **模拟操作**：显示用户进行的所有鼠标或键盘的按键操作。包括在各种对话框、终端、编辑器中键入的文字内容。例如：<CtrlAlt-Delete>、cd D:\boot。可以在某一条记录后单击**回放**，从该操作处开始回放直到结束。
- **剪贴板记录**：显示用户所有通过剪贴板复制或粘贴的文字。可以单击**筛选**设置筛选条件，单击**下载**将剪贴板记录以.txt文件的形式下载到本地。

参数	**说明**
时间	完成复制或粘贴操作的时间。
记录	复制到剪贴板中的文本，如文本过长，将对部分文本进行省略，最后显示为省略号。
方向	• **上行**表示通过剪贴板粘贴到远端资产中的文本。 • **下行**表示在远端资产上复制到剪贴板中的文本。和最终是否粘贴及在哪里粘贴无关。
操作	• **回放**：从该操作开始回放会话，直到会话结束。 • **剪贴板详细**：在弹出的新窗口中显示完整的剪贴板文本。

- **会话复核**：显示在**高危操作**中设置并在本次会话中触发和进行复核的的操作。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/姓名/资产/资产IP进行模糊查找，筛选出符合条件的会话。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条会话后单击**导出选中**，或直接单击**导出全部**，将会话列表导出为.xls格式的表格并下载到本地。

审计数据库会话

审计管理员可以查看所有在线或已关闭的数据库会话，结合同时记录的图形会话，完成对用户的数据库操作的审计。

数据库会话中会记录用户通过客户端登录数据库及在数据库上执行的所有语句。用户在数据库客户端上执行的所有键鼠操作，同时也都会记录在图形会话中，因此建议审计管理员将数据库会话和图形会话结合起来，完成对数据库访问过程的审计。

用户必须通过RIS代填主机名及服务名并连接到数据库，才会在RIS中留下审计记录。如果自己填写主机名和服务名并进行连接，相当于不通过RIS建立数据库会话，审计管理员将无法看到对应的数据库会话审计记录，但可以看到图形会话审计记录。

1. 选择**工作台** > **审计** > **操作审计** > **数据库会话**。
2. 查看所有数据库会话信息。

项目	说明
开始时间	会话开始的时间，例如**2018-08-06 19:24:19**。
结束时间	会话结束的时间，例如**2018-08-06 19:33:15**。
来自	直接连接到数据库的IP地址。
用户帐号	用户登录RIS的帐号。
用户姓名	用户登录RIS的帐号对应的姓名，在**帐号设置**中设置。
资产名	会话连接的数据库在RIS上记录的名称。
系统帐号	会话连接使用的该数据库上的帐号名称。
会话时长	会话从开始到当前时间的总计时长。单击↻后才会刷新该时长。
资产IP	会话连接的资产的IP地址。
状态	会话的连接状态：活跃、断开。
数据库类型	会话访问的数据库类型，例如Oracle、MSSQL。
数据库名	会话访问的数据库名称，例如devdb、sql2000。
数据库客户端	连接数据库所使用的数据库客户端，例如Toad、Ssms。
操作	• **详情**：单击进入会话详情页面查看。 • **图形会话**：单击跳转到该数据库会话对应的**图形会话**记录中。 • **回放**：单击播放该数据库会话的图形会话记录。当多条数据库会话对应同一图形会话时，会播放同一图形会话的完整记录。

3. 可选： 在一条会话记录后，单击**详情**，进入**会话详情**页面查看会话详情。

   在**会话详细**页面，会通过表格形式显示该数据库会话的每一条语句执行的记录。表格每一列显示的信息如下：

项目	说明
执行时间	执行该SQL语句的具体时间。
语句	被执行的SQL语句的具体内容。客户端自身执行的SQL语句也会被记录。
操作	• **细节**：单击后在弹出的对话框中显示被执行的语句的完整内容。 • **回放**：单击后从该操作开始回放会话，直到会话结束。

项目	说明
	• **忽略**：单击后将该行语句添加到忽略，不在该会话记录中显示。可以在**操作审计** > **数据库会话**中单击右上角的**忽略项**，查看有哪些内容被忽略，并单击对应的**取消**按钮，取消对于相应内容的忽略。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/姓名/资产/资产IP进行模糊查找，筛选出符合条件的会话。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条会话后单击**导出选中**，或直接单击**导出全部**，将会话列表导出为.xls格式的表格并下载到本地。

审计文件传输

审计管理员可以查看所有已完成的文件传输会话，并执行查看详情的功能。RIS可以审计到的文件传输会话包含传输文件中所用到的所有文件传输方式。

1. 选择**工作台** > **审计** > **操作审计** > **文件传输**。
2. 查看所有文件传输会话信息。

   每一行都是一个文件传输会话。每一列显示的信息分别如下：

项目	说明
开始时间	文件传输操作开始的时间，例如**2018-08-06 19:24:19**，不是会话建立的时间。
结束时间	文件传输结束的时间，例如**2018-08-06 19:24:21**。
来自	和资产设备之间传输文件的主机的IP地址。
用户帐号	用户登录RIS的帐号。
用户姓名	用户登录RIS的帐号对应的姓名，在**帐号设置**中设置。
资产名	会话连接的资产在RIS上记录的名称。
系统帐号	会话连接使用的该资产上的帐号名称。
操作类型	用户在文件传输会话中执行的具体操作，例如**上传文件**、**下载文件**、**删除文件**、**新建文件夹**等。
文件路径	无论上传或下载，只显示该文件在资产设备上的路径。远端资产设备为Windows设备时仅显示文件名。
文件大小	传输的文件的总大小和单位。
状态	文件传输的结果，例如：**成功**、**失败**、**无权访问**、**失去连接**。
会话时长	完成该次文件传输所花费的时间，最小单位为1秒。

项目	说明
文件权限	仅当远端资产设备为Linux/Unix主机时会显示，三位数字的Linux/Unix格式的权限，表示该文件在该远端资产上的权限。
操作	• **详情**：单击后将进入**基本信息**页面，会显示文件的**文件名**、**传输路径**、**文件大小**、**文件权限**、**传输状态**等内容。其中**传输路径**和**文件权限**仅当远端资产设备为Linux/Unix主机时会显示。 • **下载**：单击**下载**将传输的文件下载到本地。必须满足以下条件才能正常下载： • **系统设置** > **资产** > **访问设置** > **文件传输**中的**是否留痕**设置为**是**。 • 当次传输的文件大小未超过**文件留痕阈值**。 **说明：**当审计文件不存在时，单击**下载**按钮后，RIS将提示**下载文件失败**。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/姓名/资产/资产IP进行模糊查找，筛选出符合条件的会话。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条会话后单击**导出选中**，或直接单击**导出全部**，将会话列表导出为.xls格式的表格并下载到本地。

查看审计结果（事件类）

审计管理员除了对会话进行审计，也可以审计Web界面中的各种事件，包括登录日志、配置日志和审计记录。

审计登录日志

审计管理员可以查看所有用户的登录日志，以确保RIS没有异常登录的情况。

1. 选择**工作台** > **审计** > **事件审计** > **登录日志**。
2. 查看所有登录日志信息。

   每一行都是一条登录事件信息。每一列显示的信息分别如下：

项目	说明
时间	该帐号登入或登出的时间。
来自	该帐号登录请求的来源IP。如登录操作经过了跳转，显示的IP为直接连接RIS的IP。
用户帐号	该登录帐号的名称。
用户姓名	该登录帐号的姓名，在**帐号设置**中设置。登录失败时不显示。
验证方式	该帐号登录时采用的身份验证方法，取值为系统允许的各种登录认证方式。使用双因子认证时将显示为使用的双因子认证方式模板的名称。使用密钥登录SSH交互终端时，会显示为pubkey。

项目	说明
登录方式	该帐号登录RIS的方式，取值范围如下： • WEB：使用Web界面登录RIS。 • GUI：使用Mstsc客户端登录RIS。 • TUI：使用SSH客户端登录到RIS交互终端。 • 空值：登出时显示为空。
登录描述	该帐号登录情况，取值为“登录成功”、“登录失败”、“登出成功”之一。
登录结果	该帐号登录或登出的结果，取值为“成功”或“失败”之一。

说明：用户如果选择使用any帐号登录，自行输入帐号密码，当登录失败时，审计记录中将看不到该用户的该次登录操作。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/来自IP进行模糊查找，筛选出符合条件的事件。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条事件后单击**导出选中**，或直接单击**导出全部**，将事件列表导出为.xls格式的表格并下载到本地。

审计配置日志

审计管理员可以查看所有用户的配置日志。配置日志中记录了系统或用户在RIS上执行的所有配置操作。

1. 选择**工作台** > **审计** > **事件审计** > **配置日志**。
2. 查看所有配置日志信息。

   每一行都是一条配置事件信息。每一列显示的信息分别如下：

项目	说明
时间	用户执行该配置操作的时间。
来自	用户登录请求的来源IP。如登录操作经过了跳转，显示的IP为直接连接RIS的IP。如果是RIS系统本身，显示为localhost地址。
用户帐号	登录RIS的帐号的名称，如果是RIS系统本身，显示为**系统**。
用户姓名	登录帐号的姓名，如果是RIS系统本身，显示为**系统**。
操作类型	用户执行的配置操作的类型，例如**重启**、**删除用户**等。
影响内容	用户执行的配置操作具体影响的范围。 • 修改系统属性时，该值显示具体的系统属性的名称。 • 修改用户、资产相关的设置时，该值显示为对应的用户或资产的名称。

项目	说明
	• 修改个人设置时，该值显示为对应的用户名。
结果	配置操作的结果。**成功**或**失败**。
操作	单击**详情**，在弹出的窗口中查看事件详情。**基本属性**为本表格中列举的以上属性，**高级属性**会显示用户修改配置的操作所保存的所有属性。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/来自IP进行模糊查找，筛选出符合条件的事件。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条事件后单击**导出选中**，或直接单击**导出全部**，将事件列表导出为.xls格式的表格并下载到本地。

查看审计记录

审计管理员也可以对自身以及其他审计管理员在Web界面上所进行的所有审计操作进行审计，了解所有审计管理员都审计了哪些内容。

1. 选择**工作台** > **审计** > **事件审计** > **审计记录**。
2. 查看所有审计记录信息。

   每一行都是一条审计记录信息。每一列显示的信息分别如下：

项目	说明
时间	用户执行该审计操作的时间。
来自	用户登录请求的来源IP。如登录操作经过了跳转，显示的IP为直接连接RIS的IP。如果是RIS系统本身，显示为localhost地址。
用户帐号	登录RIS的审计管理员帐号的名称。
用户姓名	登录帐号的姓名。
操作路径	审计管理员执行的审计操作的名称，如实现该操作需要连续操作，显示为一系列连续操作对应的窗体及控件名称，中间用/隔开，例如**文件传输/详情/基本信息**。
操作类型	审计管理员执行的审计操作的类型，如**详情**、**切断**等。
会话类型	审计管理员审计的会话的对应的会话类型，例如**字符会话**、**图形会话**、**文件传输**。
资产IP	用于标识审计管理员审计的会话连接到哪个资产，显示该资产的IP地址，例如**10.10.10.10**。
目标资产	用于标识审计管理员审计的会话连接到哪个资产，显示该资产在RIS上记录的名称，如**CentOS7**。

项目	说明
会话序列号	审计管理员审计的会话的对应的会话ID。可以单击该序列号跳转到对应的会话审计记录中，查看该会话记录的具体信息。

- 单击**更多**设置筛选条件，或在搜索框中输入用户/来自IP进行模糊查找，筛选出符合条件的事件。
- 单击右上角的⋮，勾选要显示的表格列信息。
- 勾选一条或多条事件后单击**导出选中**，或直接单击**导出全部**，将事件列表导出为.xls格式的表格并下载到本地。

播放会话录屏

在审计界面中单击**回放**或**实时**，可以播放会话录屏。请参考本节内容，在会话录屏的播放过程中对播放进行控制。

会话录屏的播放方式有两种，包括以下两种方式：

- web：在浏览器中播放会话录屏
- java：在JAVA窗口中播放会话录屏

如需修改播放方式，请在**帐号设置** > **会话配置** > **图形会话**中，修改**回放方式**为**web**或**java**。

使用JAVA窗口播放，要求本地PC必须预先安装JAVA JRE，建议版本为1.6及以上。

在JAVA窗口中播放会话录屏
会话录屏窗口是一个JAVA视频播放窗口，记录了图像会话从开始到结束的整个过程，可以拖动下方的进度条，选择具体的时间点。其他操作如下表所示：

图标	快捷键	说明
	**Space**或**P**	单击该按钮或按空格键播放/暂停回放，按**P**键播放回放。
	**S**	停止回放。
	**C**	在当前回放时间点截图。请在弹出的窗口中指定截图保存路径和截图名称。生成的截图下方，将附带截图时间点、访问资产的用户名称和地址、资产帐号、协议、被访问的资产名称和地址等会话信息。
	**I**	显示当前回放的会话信息，包括资产帐号、访问资产的用户名称和地址、被访问资产的名称和地址、会话开始时间和协议等会话信息。
	**F**	开启/取消全屏播放。
	无	选择回放画面的缩放比例，单击后有以下选项： • 固定设置：100%、85%、80%、75%、50%、25% • 自动适应：AutoFit • 手动输入：单击**More**后手动输入缩放的百分比，并单击**OK**。输入的值必须在10到200之间。

图标	快捷键	说明
	**上/下**或**+/-**	选择播放回放的速度倍率。单击后有以下选项： x0.25、x0.5、x01、x02、x04、x08、x16、x32、x64。按键盘的方向键**上/下**或**+/-**，可以使播放速度加快一倍/减慢一倍。
时间点，例如**15:42:40 2018-10-08**	**T**	选择播放时间点。单击右下角的播放时间点，在打开的窗口中，输入待跳转到的时间点，单击**OK**后从该时间点开始播放。 输入的时间点必须符合“年-月-日 时:分:秒”的格式，且必须在该回放的起始到结束时间范围内。
无	**左/右**	按键盘的方向键**左/右**，跳转到当前播放时间点的5秒前或5秒后继续播放。
无	**K**	打开/关闭按键回显（按字幕方式），显示在播放画面和下方的按钮面板之间。用户按下的其他键盘按键，将按时间顺序显示在该栏位右侧，从右向左进行滚动。 另外，该栏位的左侧，会从左到右依次显示6个按键指示符，当回放中用户按下指定的按键时，相应的指示符会短暂显示为红色。指示符从左到右依次为： • L：鼠标左键 • M：鼠标中键 • R：鼠标右键 • Ctrl：键盘Ctrl键 • Shift：键盘Shift键 • Alt：键盘Alt键
无	**E**	打开/关闭按键回显（按字幕方式）。该窗口在打开后，会从上到下依次记录回放过程中被审计用户的所有按键动作。每一条记录从左到右依次显示按键时间点、输入设备（key或mouse）、按键动作（up或down）以及具体的按键名称。

说明: 以上所有快捷键不区分大小写。

在浏览器中播放会话录屏

会话录屏窗口在浏览器中以网页形式打开，该页面可以执行以下操作：

操作	说明
控制播放	• 单击  ，暂停播放。 • 单击  ，继续播放。 • 单击  ，跳转到上一个关键帧。 • 单击  ，跳转到下一个关键帧。 • 单击进度条上某个时间点，跳转到该时间点进行播放。进度条上的白色圆点表示关键帧。

操作	说明
查看操作列表	仅Windows会话支持该功能。播放窗口左侧显示了用户在终端上执行的所有操作的列表。列表中每一个操作，从上到下依次显示操作时间、操作动作和文本记录（窗体名称或键入、复制的文本）。 可以单击操作列表中的某个操作，跳转到该操作对应的时间点进行播放。
文本信息模糊查找	在左上角输入框中输入文本信息进行筛选查找。输入的内容必须是操作列表中某个操作的文本记录的一部分或全部。
查看字幕	仅Windows会话支持该功能。当有键盘输入时，播放窗口下方会以字幕的方式，从右向左滚动显示所有按键信息。
调整播放速度	单击或，加快或减慢播放速度。播放速度默认为1倍速，调整时可以在0.25倍速~64倍速之间选择。
全屏/取消全屏	单击右下角的进入全屏播放或取消全屏播放。全屏播放时将无法使用操作列表功能。
保存截图	在播放过程中，右键单击播放画面可以选择将当前帧以png格式保存到本地。

数据库审计兼容性列表

用户通过RIS使用不同的客户端访问数据库时，支持情况有所不同。

表 26: 数据库审计兼容性列表

客户端	数据库版本	数据库审计
• sqlplusw10 • SqlDbx • Toad 12 • PL/SQL Developer 11.0 • SQL Developer 1.5.5	• Oracle9i • Oracle 10g • Oracle 11g • Oracle 11gR2-RAC • Oracle 12c	支持
OEM	• Oracle9i • Oracle 10g • Oracle 11g • Oracle 11gR2-RAC • Oracle 12c	不支持

客户端	数据库版本	数据库审计
SSMS 2014	• SQLServer2000 • SQLServer2005 • SQLServer2008 • SQLServer2012 • SQLServer2014 • SQLServer2016	支持
Navicat	• mysql 5.6.32 • mysql 5.7.18	支持
SQLyog		
Quest Central	DB2 v9.7	不支持
SqlDbx for DB2		
Toad for DB2		

报表

7

目录:

报表是利用表格、图表等形式动态地统计并展示RIS中各项信息，如系统中的资产和用户总量的变化情况，从而满足用户对RIS数据进行审查和汇报的需要。能够使用报表的角色包括各种管理员：超级管理员、配置管理员、审计管理员及其他自定义的拥有报表授权的用户。

RIS支持的报表类型包括：用户统计报表、资产统计报表、会话统计报表和帐号类报表。RIS预定义了一些对应以上各种类型的报表模板，其他报表模板需要用户自定义导入，并对应以上四种类型。

配置报表

用户可以通过配置报表，引用报表模板，即时或周期性地生成报表。配置报表仅定义报表的生成方式，报表具体的内容在**报表模板**中定义。必须先配置了**报表模板**，然后在此引用。

报表有固定的**统计周期**，自动生成的报表也有固定的**生成周期**。**周期报表**是指按固定的生成周期自动生成有固定统计周期的报表，**即时报表**可以手动设定统计周期并立即生成，也可以在固定的生成周期时间点上自动生成从指定起始时间点开始的统计周期内的报表。

1. 登录RIS Web界面。
2. 选择**工作台** > **报表** > **报表查看** > **报表**。
3. 单击右上角的**新增报表**，设置以下参数后，单击**保存**。

参数	说明
报表名称	用于标识一个报表，全局唯一。长度为1~30的字符串。
报表类型	该参数需要与**自动生成**搭配使用。 • **周期报表**： • 当**自动生成**设置为**是**时，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。

参数	说明
	• 当**自动生成**设置为**否**时，表示禁用该报表的周期统计和生成，这种情况下和即时报表完全相同。 • **即时报表**： • 当**自动生成**设置为**是**时，也会周期性生成报表，但会在每一个生成周期时间点上，统计从指定时间开始到该时间点这一段时间内的信息，并同时生成报表。 • 当**自动生成**设置为**否**时，通过单击**生成报表**，立即生成一个报表。
自动生成	• **是**：表示按固定的生成周期生成该报表。 • **否**：表示只能手动生成该报表。
统计起始时间点	仅当**报表类型**为**即时报表**，且**自动生成**为**是**的情况下需要配置。用于指定即时报表统计的起始日期（时间点为0:00），RIS在该起始时间点之后的每个生成周期时间点上生成报表时，都统计从该起始时间点到报表生成时间点之间的信息。 对于只统计一个时间点而不统计一个时间段的自定义模板，该设置无效。
周期类别/生成周期	对于**周期报表**，既表示统计周期，也表示生成周期；对于**即时报表**，仅表示生成周期，而统计周期则由**统计起始时间点**和该**生成周期**的时间点决定。 所有统计周期都统计从第一天的0:00:00到最后一天的23:59:59之间的数据。 所有生成周期时间点都是当天的2:00。
报表模板	用于定义报表的具体内容，在**报表** > **报表配置** > **报表模板**中定义，然后在此引用。不同的**报表类型**对应不同的**报表模板**，同一**报表模板**可以有不同的**报表类型**。
其他	根据引用的报表模板的不同，会有一些其他信息需要配置。例如**用户分类统计报表**需要设置**包含角色**，**资产信息统计报表**需要设置**是否禁用**和**资产类型**。请在预设的下拉菜单中选择一个或多个。

4. 设置新建报表的**高级属性**。

   仅当**自动生成**为**是**时需要设置高级属性。对新建的报表单击**编辑**。**基本属性**页签是新建报表时设置的参数，请选择**高级属性**页签设置以下参数：

参数	说明
统计周期	仅当**报表类型**为**周期报表**时需要配置。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。

参数	说明
生成周期	**周期类别/生成周期**为**按日**时不需要配置，固定为每天的2:00；其他情况下配置每个生成报表的日期，时间点为该日的2:00。
邮件发送	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。
报表格式	仅当**邮件发送**选择**是**时需要配置。勾选一种或多种通过邮件发送的报表格式。
收件人邮箱	仅当**邮件发送**选择**是**时需要配置。单击**选择收件人**选择一个或多个登记了邮箱的用户，或者单击**添加邮箱**直接添加一个邮箱地址，报表在生成后将自动发送到这些邮箱地址。

说明: 以上参数中部分在界面上没有具体的参数名称，请根据参数提示自行对应。

5. 可选： 手动生成报表。单击**生成报表**，设置统计周期的起始时间和结束时间后，立即生成该报表，并可在弹出的窗口中查看该生成的报表。

   说明: 引用的模板如果只统计当前时间点，则将不选择时间直接生成报表。

6. 可选： 查看历史报表。单击**历史报表**，跳转并查看历史报表。

   说明: 只有自动生成的报表能够被记录并在历史报表中查看。

查看历史报表

自动生成的报表可以在**历史报表**中查看并保存。

1. 登录RIS Web界面。
2. 选择**工作台** > **报表** > **报表查看** > **历史报表**。
3. 查看所有历史报表信息。

   每一行都是一条已生成或待生成的历史报表。每一列显示的信息分别如下：

项目	参数
报表名称	**报表** > **报表查看** > **报表**中定义的报表名称。
模板名称	该报表引用的模板名称。
生成时间	已生成的报表的生成时间，及待生成的报表下一次生成的时间。
生成状态	成功、失败、待生成其中之一。
操作	单击**查看**，在弹出的窗口中查看生成的报表，并单击 将报表导出为不同的格式。

配置报表模板

RIS已预置了一些报表模板。用户也可以自行上传自定义的报表，请联系齐治科技技术支持，定制自定义的报表模板。

RIS已预置的报表模板如下：

- 用户基本报表
- 用户变更报表
- 用户分类统计报表
- 会话数据报表
- 资产基本报表
- 资产信息统计报表
- 资产变更报表
- 帐号基本报表

1. 联系齐治科技技术支持，获取定制的*.rpt格式的报表模板。
2. 登录RIS Web界面。
3. 选择**工作台** > **报表** > **报表配置** > **报表模板**。
4. 单击右上角的**上传报表模板**，在弹出的对话框中，单击**浏览**，选中已获取的报表模板。
5. 单击**下一步**，设置以下参数后单击**保存**。

参数	**说明**
模板名称	用于标识一个模板，全局唯一。长度为1~30的字符串。
简要说明	可选参数，用于对该报表模板的进行解释说明。最大长度为512的字符串。
分类	在下拉菜单中选择一个报表分类。该分类仅用于添加一个分类信息，模板的具体内容由模板本身决定。

配置报表参数

报表参数中，只能对报表logo进行修改。该logo展示在预设模板的页眉处，自定义模板需引用该字段才会进行显示。

1. 登录RIS Web界面。
2. 选择**工作台** > **报表** > **报表配置** > **报表参数**。
3. 单击**浏览**，从本地PC选择一张报表logo图片，并单击**打开**。

   该图片格式只能为gif、png、jpg、jpeg之一。图片大小建议在150*50之内，如大于该尺寸RIS将自动进行缩放。

4. 导入成功后，单击**确定**保存logo。

说明：可以单击**恢复出厂设置**，将logo还原为默认的齐治科技的logo。

自动化

8

目录:

超级管理员、配置管理员和具有自动化授权的自定义角色可以在RIS上创建自动化运维任务，例如脚本任务。

配置脚本任务

RIS支持通过Telnet或者SSH协议登录到目标资产上自动执行脚本，并支持配置执行时间和执行间隔。

目标资产包括类Unix系统和网络设备，用户可以上传自定义的脚本文件，也可以选择系统预置的命令文件。

表 27: 目标资产和脚本支持情况

目标资产和协议		自定义脚本	系统预置命令
类Unix系统	SSH	✓	
网络设备	Telnet/SSH	✓	✓

说明: 网络设备如果同时配置了Telnet和SSH协议，RIS将优先使用Telnet协议，如果失败不会再尝试使用SSH。

- **类Unix系统的自定义脚本**

  类Unix系统的自定义脚本文件类型可以是该资产上允许执行的任何脚本类型，但资产上必须安装了相应的解释器，并且在脚本开头声明了该脚本使用的解释器，例如#!/bin/bash、#!/usr/bin/python2、#!/usr/bin/perl等等。

  脚本内容符合该资产的操作系统及脚本语言对于脚本的规范要求即可，RIS并未对脚本内容做其他限制。

  RIS执行自定义脚本的过程如下：

  1. 通过sftp方式将脚本文件上传到目标资产的指定系统帐号家目录下。
  2. 给脚本加上执行权限，chmod +x /脚本路径/脚本名称。
  3. 使用配置的系统帐号登录目标资产执行命令，/脚本路径/脚本名称。

- **网络设备的自定义脚本**

  网络设备的脚本文件是一个网络设备配置命令的集合，请参考编辑窗口中的提示举例进行编辑。执行时将在网络设备资产上按从上到下的顺序依次执行脚本中的各条命令。

- **系统预置命令**

表 28: 系统预置命令表

名称	操作
h3c_reboot	在目标资产上执行命令**reboot**，适用于H3C网络设备。
h3c_save	在目标资产上执行命令**save**（不指定文件名，使用资产缺省文件名），适用于H3C网络设备。

说明:

- 脚本任务的默认并发数是6，默认的执行超时时间是180s。可以在配置资产适配中修改默认值。
- 在HA环境，任务仅会在主节点上执行。

1. 选择**工作台** > **自动化** > **脚本任务** > **任务列表**。
2. 单击**增加脚本任务**。
3. 设置任务名称和简要描述。

参数	说明
任务名称	脚本任务的名称。字符串格式，长度范围是1~30个字符。
简要描述	脚本任务的简要描述。字符串格式，长度范围是0~128个字符。

4. 单击**目标资产**对应的，选中要配置脚本任务的资产，然后在**系统帐号**中选择RIS登录目标资产使用的帐号，单击**确定**。

   说明: 选择目标资产时需要注意一个脚本任务中所有资产执行的脚本是相同的。

   如果资产数量大，可通过以下方式查找满足条件的资产。

   - 在搜索文本框中输入资产名称、IP或者简要说明的关键字。
   - 先单击左上角的**筛选**，然后在下拉列表框中设置过滤条件，最后单击**筛选**按钮。

   说明: 如果选择的资产配置了资产适配，脚本任务的执行还将受到资产适配中配置的登录超时时间和任务执行超时时间的影响。若在执行过程中超过了设定的时间，将导致脚本任务执行失败。

5. 选择脚本文件来源。

   - 如果目标资产是类Unix系统，请选中**自定义脚本文件**，并单击**文件上传**从本地PC选择脚本文件。
   - 如果目标资产是网络设备，请选中**网络资产配置命令**，在下拉列表框中选择预置的脚本文件，或在下拉列表框中选择**自定义**，上传或编辑自定义脚本文件。

     说明:

对于网络设备的自定义脚本文件，用户可以单击**文件上传**选择上传自定义脚本文件，或直接在**配置命令**窗口中编辑脚本文件。

6. 设置脚本任务执行时间和间隔。

参数	说明
执行时间	脚本任务第一次执行的时间，包括**年/月/日/时/分**。
执行间隔	脚本任务的执行间隔，可选项包括： • 执行一次 • 按日 • 按月

7. 可选： 设置邮件通知。

说明: 站内通知默认勾选，无法取消。站内通知的收件人为超级管理员、配置管理员、自动化管理员和其它自定义的具有自动化权限的用户，无法修改。

a) 勾选**邮件通知**。

b) 单击**通知人**对应的，在弹出的对话框中勾选邮件通知的用户。

说明: 通知人仅对邮件通知生效。请用户自行保证已提前配置好了邮件服务器，并保证用户是具有自动化权限的角色，状态为**活动**，且配置了邮箱。RIS将不会对这些设置做检查，如这些设置有误，通知人配置可以正常保存，但将收不到邮件设置。

8. 单击**保存**。

脚本任务配置完成后，管理员可以执行以下操作：

- 在搜索文本框中输入任务名称的关键字来查找脚本任务。
- 单击**立即执行**，立即执行一次脚本任务。
- 单击**编辑**，修改脚本任务的配置。
- 单击**禁用**或者**启用**，禁用、启用对应的脚本任务。
- 单击**删除**，删除对应的脚本任务。
- 单击**查看详情**，查看脚本任务执行历史和结果。

查看脚本任务执行历史和结果

管理员能够查看、下载脚本任务的执行结果。

1. 选择**工作台** > **自动化** > **脚本任务** > **任务详情**，查看脚本任务执行结果列表。

说明: 在搜索文本框中输入任务名称的关键字来查找脚本任务。

RIS会记录每次脚本任务的执行结果，内容包括：

- 结束时间
- 任务名称
- 创建人
- 任务类型：包括自定义脚本文件和系统预置命令文件。
- 脚本文件
- 对应资产总量：脚本任务中目标资产的数量。
- 执行结果：脚本任务中目标资产的数量和执行成功的资产数量。
- 开始时间
- 查看详情
- 下载执行结果

2. 可选： 单击**详情**，查看对应脚本任务的执行结果。

说明: 管理员可以在搜索文本框中输入资产名称或者资产IP的关键字来过滤；也可以单击右边的**全部**、**失败**、**成功**或者**超时**来根据执行结果过滤。

执行结果展示的内容包括：

- 资产名
- 资产IP
- 执行结果：包括**成功**和**失败**。
- 简要描述：执行结果的简要描述。
- 详情：如果执行结果是**成功**，显示执行过程；如果执行结果是**失败**，显示错误信息。常见错误信息和可能原因请参见表 29: 常见错误信息和可能原因。

表 29: 常见错误信息和可能原因

错误信息	可能原因
资产帐号 “*admin*” 未配置密码或密钥	RIS登录目标资产使用的帐号未托管密码或者密钥。
没有可用协议: telnet	RIS上该资产的访问协议未添加Telnet。

错误信息	可能原因
没有可用协议: ssh	RIS上该资产的访问协议未添加SSH。
Password or key error (account: *admin*)	SSH用户的密码或者密钥错误。
password is incorrect	Telnet用户的密码错误。
Resource connect timeout (account: *root*)	IP不通或者其他连接异常。
failed to connect to *1.1.1.1*	端口不通或者其他连接异常。
timeout when matching:.*Y/N.*|.*y/n.*|.*yes/no.*|.*YES/NO.*.	系统预置命令与目标资产不匹配。例如目标资产是Juniper的交换机，选择了**h3c_reboot**预置命令后，由于预置命令无法在目标资产上执行，就会出现该错误提示。

3. 可选： 单击**下载**，将对应脚本任务的执行结果下载到本地PC，后缀为**xls**。

   执行结果展示的内容包括：

   - 资产：资产的名称
   - 类型：资产的类型
   - IP地址：资产的IP地址
   - 帐号
   - 脚本文件
   - 执行结果：包括**成功**和**失败**。
   - 详情：如果执行结果是**成功**，显示执行过程；如果执行结果是**失败**，显示错误信息。常见错误信息和可能原因请参见表 29: 常见错误信息和可能原因。

工单

9

目录:

在RIS上可以通过工单申请资产权限、资产密码。

RIS支持的工单包括：

- **申请资产**：申请资产的访问权限。
- **申请密码**：申请资产帐号的密码。

不同类型的工单对申请人、使用人和审批人的要求如表 30: 工单申请人、使用人和审批人的要求所示。

表 30: 工单申请人、使用人和审批人的要求

工单类型	申请人	使用人	审批人
资产权限（内部人员）	用户具有工单权限。	用户具有**访问资产**权限。	可以由超级管理员在配置审批模板中指定。 缺省为自动分配，即所有配置管理员，开启了部门分权时为所有本部门及上级部门的配置管理员。 **说明:** 只能是系统内置的配置管理员角色，不包含用户自定义的角色。
资产密码	用户具有工单权限。	用户具有工单权限。	

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。RIS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。

审批人收到工单通知后，可以在待办工单中查看工单信息并审批（批准或者驳回）。

- **批准**：审批人判断申请合理时批准工单，RIS执行工单内容，不管执行成功还是失败，申请人都会收到通知消息和通知邮件。如果执行成功，对于一次性操作的工单（例如申请密码），工单状态为**已完成**；对于持续性的工单（例如申请资产权限），在结束时间前工单状态为**进行中**，在结束时间后为**已完成**。如果执行失败或者工单填写错误未执行，工单状态均为**已完成**。
- **驳回**：审批人判断申请不合理时驳回工单，申请人收到通知消息和通知邮件。工单状态为**已完成**。
- **撤销**：资产和密码工单审批通过后，在工单有效期内，最后一级审批人可以随时撤销工单，撤销后工单将立即失效。

说明:

- 如果审批人一直没有审批工单，对于配置了结束时间的工单，在结束时间后工单超时并关闭，工单状态为**已完成**；对于没有配置结束时间的工单，工单状态一直为**进行中**。
- 如果存在多个审批人，当其中一个审批人审批工单后，其他审批人不能再处理。
- 如果在配置审批模板时配置了多级审批，其中一级的审批人完成审批后需要下一级审批人继续完成审批，直到所有审批人完成审批后，工单才能生效。

为了便于用户新建工单，RIS的工单支持草稿和模板。

- **草稿**：如果工单暂时不提交，可以将工单保存为草稿，下次在草稿箱中打开工单继续填写、提交。
- **模板**：如果工单内容比较通用，可以将工单保存为模板，下次直接使用模板新建工单。

新建资产权限申请工单

通过工单来申请资产的访问权限。

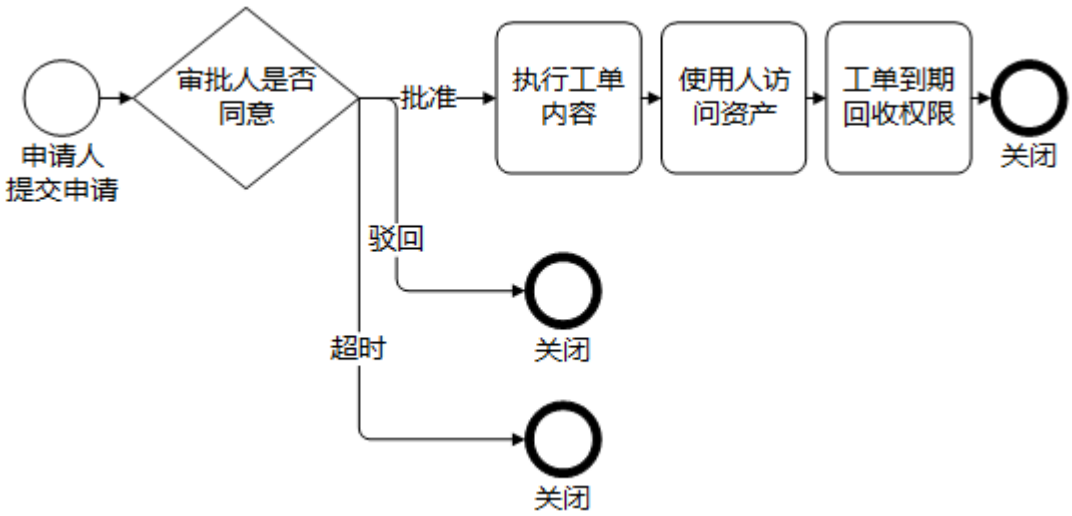


图 5: 资产权限工单处理流程

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。 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。不同的工单标题可以配置为相同，为了区分不同的工单，建议配置不同的标题。
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RIS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**。

   说明:

   - 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。
   - 系统帐号中显示资产上的所有帐号加上**any**和**self**。
     - **any**：任意帐号，登录时由用户输入。
     - **self**：同用户帐号，即使用和当前登录RIS的帐号同名的帐号登录资产，请确保该帐号在待访问资产上存在。
   - 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。

   如果资产数量大，可通过以下方式查找满足条件的资产。

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

4. 配置访问协议。

   缺省情况下，RIS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**、**RDP**、**XDMCP**、**VNC**和**XFWD**。

5. 可选： 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。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，也可以填写命令的正则表达式。正则表达式的具体写法请参考配置命令模板。

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。即只要用户执行的命令能匹配上此处的放行命令，则在高危命令中配置的拒绝、需复核、终止会话将不生效，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**。

   - 使用人列表中只显示具有访问资产权限的用户，包括：超级管理员、配置管理员、操作员、自定义具有访问资产权限角色的用户。对于已与所选资产和帐号关联过的用户，不再显示。
   - 一次最多能够选择100个用户，如果要添加权限的用户数大于100，请分批添加。

   如果用户数量大，可通过以下方式查找满足条件的用户。

   - 在搜索文本框中输入帐号或者姓名的关键字。
   - 单击**筛选**，使用用户的属性设置过滤条件，单击**筛选**。

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： 超级管理员如配置审批模板时手动指定了审批人，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，RIS将用户和所选资产、帐号关联。

执行结束后，RIS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。

新建密码申请工单

通过工单来申请资产帐号的密码。

对于配置了改密计划的帐号，支持一次一密，即申请的密码到期后，RIS会对该帐号进行改密，用户不能再使用老的密码登录设备。对于未配置改密计划的帐号，不支持一次一密，为了确保安全，请先配置改密计划。

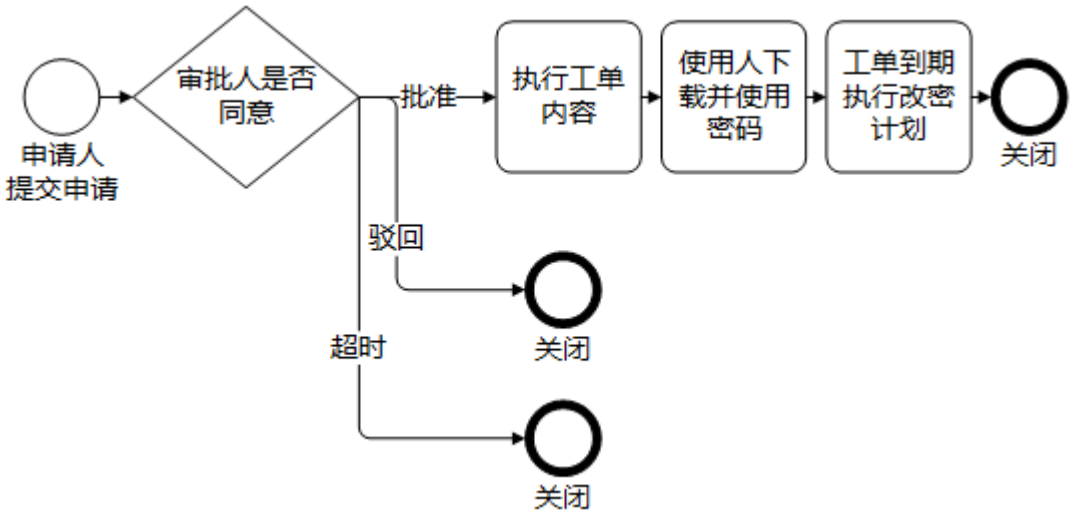


图 6: 密码工单处理流程

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。 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。不同的工单标题可以配置为相同，为了区分不同的工单，建议配置不同的标题。
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RIS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。
- RIS不支持为类型是**C/S**的资产申请密码。
- 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。

如果资产数量大，可通过以下方式查找满足条件的资产。

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

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： 超级管理员如配置审批模板时手动指定了审批人，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，RIS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，RIS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，RIS对该帐号改密。如该帐号对应多个改密计划，RIS会使用其中ID最小的一个改密计划进行改密，该ID无法由用户自行查看。

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。

审批待办工单

待用户审批的所有工单都会显示在待办工单中，用户可以在查看工单信息后进行审批。

1. 选择**工单** > **工单管理** > **待办工单**。
2. 可选： 设置筛选条件，包括工单类型、工单标题或者申请人的关键字，单击**筛选**，筛选出特定的工单。

   说明: 单击**重置**，可以清除所有已设置的筛选条件。

3. 单击工单对应的**详情**查看工单内容，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**（0~300个字符），完成后单击**确定**。
   - 单击**批准**后，RIS会执行工单中定义的任务，完成后申请人会收到通知消息和通知邮件。查看工单详情，工单状态为**已完成**，结果可能为**成功**、**失败**或者**异常**。如果结果为失败或异常，请查看原因并解决。
   - 单击**驳回**后，申请人会收到通知消息和通知邮件。查看工单详情，工单状态为**已完成**，但结果是**未执行**。
4. 可选： 当超级管理员在配置审批模板中设置了多级审批时，如果存在下一级审批人，且下一级审批人为超级管理员指定的审批人时，当前审批人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通知并由其中之一继续完成审批。

   说明: 当下一级审批人为自动分配时，当前审批人无需选择下一级审批人。批准后，所有配置管理员将会收到通知并继续完成下一级审批。如开启了部门分权，则只有当前部门及上级部门的配置管理员会收到审批通知。

查看（撤销）已办工单

用户申请和审批过的所有工单都会显示在已办工单中，用户可以查看工单的申请时间、工单类型、工单状态、操作结果等信息。

1. 选择**工单** > **工单管理** > **已办工单**。
2. 可选： 设置筛选条件，包括工单类型、工单状态、工单标题或者申请人的关键字，单击**筛选**，筛选出特定的工单。

   说明: 单击**重置**，可以清除所有已设置的筛选条件。

3. 查看工单的信息，如果要查看某个工单更详细的信息，请单击对应的**详情**。

   工单详情中会显示工单的状态、工单内容和结果。如果结果是失败，可以单击**失败**了解原因。

4. 审批通过后，针对申请资产权限和申请密码这两种类型的工单，可由最后一层的审批人撤销已经生效的工单，即在**工单详情**页面中单击**撤销**按钮，完成撤销工单操作。

说明： 如果最后一层审批人有多个，则每个审批人都能够执行撤销操作。只有最后一层审批人**已办工单**中对应工单的**详情**页面存在**撤销**按钮。

当RIS系统从3.3.6及之前的版本升级到最新的版本后，升级前就已申请的工单，将只能由最后一个审批人本人完成撤销操作，审批人列表中的其他最后一层审批人将不能撤销工单。

撤销工单后，该工单将立即失效，相关用户需要重新创建申请工单。

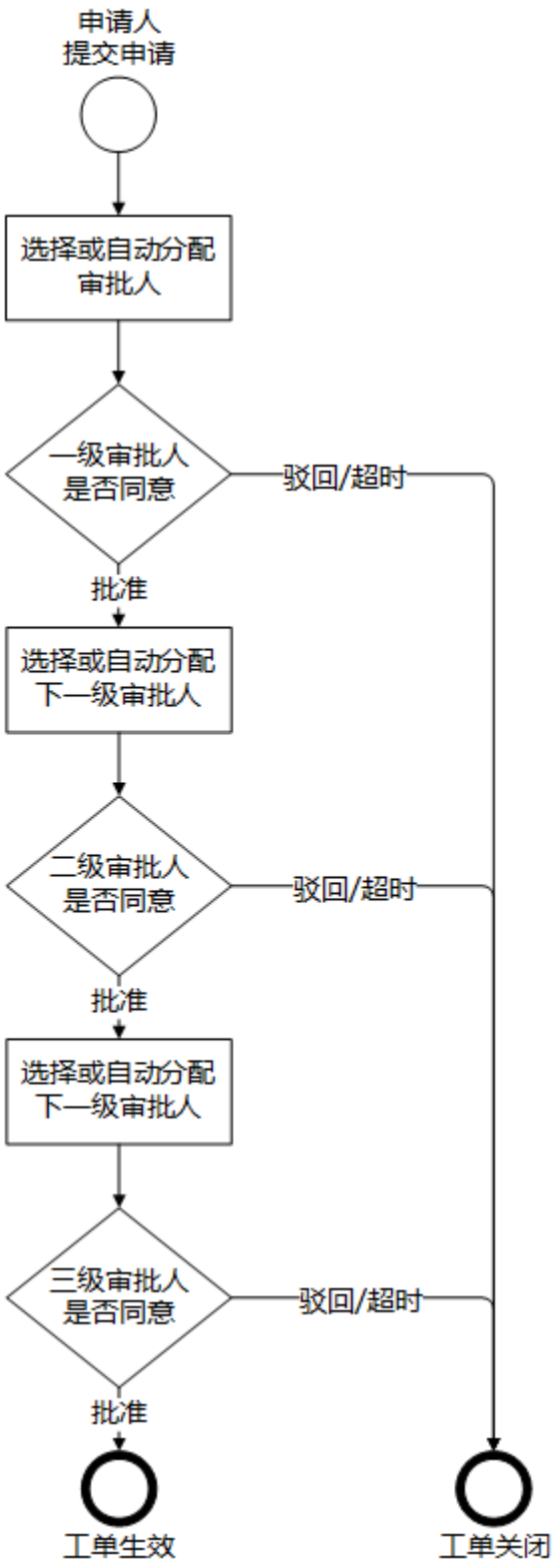
配置审批模板

超级管理员可以为不同的工单类型配置审批模板，包括配置审批的层级数，及每一层的审批人员。
如不对审批模板进行修改，所有审批模板默认为只进行一级审批，规则为自动分配，即审批人为所有配置管理员。

说明： 如开启了工单审批人选项，即在修改配置文件时设置了worksheet.enableApproverSetting=true时，在此处配置的审批模板将失效。

配置了多级审批后，一级审批人完成审批后，将由二级审批人、三级审批人依次完成审批。每一级中只要有一个审批人批准了工单，工单就会进入到下一级审批中，各级审批都完成后，工单生效；只要有一个审批人驳回了工单，或所有审批人在工单结束时间之前都没有完成审批，该工单就将关闭。

某类型的工单设置了三级审批之后，该类型工单审批流程如下：



修改审批模板，将不会对已创建的工单生效。

1. 选择**工单** > **配置** > **审批模板**。
2. 设置审批模板相关参数，并单击**保存**。

参数	说明
模板名称	用于标识一个审批模板的名称。缺省为申请密码和申请资产。
工单	该审批模板对应的工单类型。仅作显示，不能修改。
审批级别	取值范围为一级、二级、三级其中之一。默认为一级。
审批规则	设置每一级审批的审批人： • 自动分配：审批人为所有配置管理员。当开启了部门分权时，为申请用户所在部门及上级部门的所有配置管理员。  **说明:** 如各级别都设置为自动分配，则同一个配置管理员可以独立完成各级别的审批。 • 手动指定：从所有用户中，手动选择若干审批人。当上一级审批人批准工单后，需要从这些审批人中选择一个或多个，作为下一级审批人。

帐号改密

10

目录:

帐号改密可实现对主机、网络等设备的系统帐号的密码修改。

管理帐号资产

在帐号资产中可以以帐号为中心，对帐号的基本信息进行集中查询和更新。

RIS根据帐号所属的资产类型将帐号分为:

类型	说明
主机帐号	指资产类型为主机的帐号，比如Linux、Windows、AIX。
网络帐号	指资产类型为网络的帐号，比如Cisco IOS、Huawei Quidway、H3C Comware。
域帐号	指Windows域帐号，可以先在**资产** > **配置** > **Windows域**中添加或管理Windows域；然后在**工作台** > **帐号改密** > **帐号资产** > **域帐号**中选择要管理的域，单击从域中同步帐号。

说明: 因产品软件版本和设备型号不同，可管理的帐号类型会有所不同。

在帐号资产中您可以对帐号进行下列操作:

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

设置帐号属性

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

说明：帐号的**责任人**属性继承自其所属的资产，不支持单独设置，您可以在**资产**中选择要修改的资产，单击**编辑**修改**责任人**属性。

1. 选择**工作台** > **帐号改密** > **帐号资产**。
2. 选择要配置的帐号类型。
3. 选择要配置的资产和帐号，单击**编辑**，选择**帐号编辑**。
4. 设置各参数，完成后单击**确定**。

参数	说明
帐号类型	帐号在目标资产上的权限类型，RIS对目标资产进行改密操作时将优先使用特权帐号登录。对于需要通过ssh和telnet访问的设备，特权帐号和普通帐号的登录提示符也不同，该设置会影响RIS自动登录目标设备。 • 特权帐号：目标资产上权限最高的帐号，比如Linux中的root、Windows中的Administrator、Cisco IOS中的enable。 • 普通帐号：目标资产上特权帐号以外的帐号。
是否可改密	是否允许RIS自动修改该帐号的密码： • 可改密：允许RIS对该帐号进行自动改密。 • 不可改密：不允许RIS进行自动改密。RIS自动同步的域帐号默认值均为该值。
登录密码	仅修改RIS上的密码，一般用于当RIS上的该帐号密码设置错误时进行重设。
确认密码	必须和**登录密码**完全一致。
切换自	Linux、Unix和网络设备中的特权帐号可能不允许直接telnet或者ssh远程登录，此时可以选择一个低权限的帐号作为切换来源，RIS在登录目标资产时会先使用切换自帐号登录，然后再通过su等切换命令切换到特权帐号的身份。
私钥(含SSH服务的资产)	访问目标资产的SSH密钥。可以在**资产** > **配置** > **密钥管理**中查看或者添加新的密钥。

管理选定帐号密码

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

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

查看最近的密码修改和备份情况。

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

说明:

- 部分资产类型不支持**登录测试**，不支持的资产类型将不会出现**登录测试**按钮。
- 此处的**登录测试**功能，与资产管理中的登录测试功能，实际测试方式不同。资产管理中的登录测试相当于用户实际执行了一次访问；帐号管理中的登录测试，Windows资产会使用RPC登录，Linux资产会使用后台登录，并对登录提示符进行检查。因此如果两边的登录测试结果不一致，是正常现象。
- 执行自动改密前，必须先在**帐号改密** > **系统设置** > **密码规则**中添加对应的改密规则。改密结果将根据设置的备份方式发送给对应的通知人。改密规则的备份方式如设置为**同密码备份**，需要在**帐号改密** > **帐号维护** > **密码备份**中设置密码备份方式。

查看选定帐号日志

在帐号资产中可以查看指定帐号在RIS中的全部操作日志。

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

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

批量更新帐号

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

> **说明:**
>
> - 不支持对域帐号的批量更新。
> - 在**资产**页面，右上角单击**密码导入**可以批量更新更多的帐号属性。

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

参数	说明
帐号类型	帐号在目标资产上的权限类型，RIS对目标资产进行改密操作时优先使用特权帐号登录，对需要通过ssh和telnet访问的设备，特权帐号和普通帐号的登录提示符也不同，该设置会影响RIS自动登录目标设备。 • 特权帐号：目标资产上权限最高的帐号，比如Linux中的root、Windows中的Administrator、Cisco IOS中的enable。 • 普通帐号：目标资产上特权帐号以外的帐号。
密码	帐号在目标资产上的密码。
是否可改密	是否允许RIS自动修改该帐号的密码： • 可改密：允许RIS对该帐号进行自动改密。 • 不可改密：不允许RIS进行自动改密。RIS自动同步的域帐号默认值均为该值。

6. 在批量更新页面，批量上传填写完毕的Excel文件。您可以通过两种方式上传：

- 将文件直接拖到页面的矩形区域内。
- 单击**文件上传**，选择文件并上传。

7. 上传后，RIS将显示从文件中读取的信息，请核对要更新的信息是否正确，完成后单击**开始更新**。如果有红色标记，说明录入的信息不正确，您可以：
   - 直接页面上修改或者单击移除异常的数据。
   - 重新编辑Excel文件，后单击**文件上传**，重新上传。

批量导出帐号

通过批量导出可以导出选择的帐号的基本属性到Excel文件中。

如果要导出密码，需要用户完成配置ZIP文件密码或配置PGP公钥。

说明: 不支持域帐号的导出。

1. 选择**工作台** > **帐号改密** > **帐号资产**。
2. 选择要配置的帐号类型。
3. 单击页面右上角的**密码导出**或**批量导出**。

   说明: **密码导出**导出的信息将比**批量导出**多了帐号密码一列。
4. 选择要导出的帐号，单击**下一步**。
5. 可选： 勾选左下角的**特权帐号**和**普通帐号**，可选择性导出特定类型的帐号。
6. 单击**导出**。

导出的Excel文件中将包含选定帐号的资产名、资产IP、责任人、帐号、帐号类型和是否可改密属性。如果执行的是**密码导出**，还会显示密码。如该帐号未托管密码，则该单元格为空。

执行**密码导出**后，需要使用用户在配置ZIP文件密码或配置PGP公钥时配置的密码/密钥进行解密后才能解压缩。

帐号维护

通过帐号维护可以对帐号设置改密计划、设置密码备份计划。

配置改密计划

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

在使用改密计划前，请先完成以下配置工作：

- 配置改密规则。
- 配置资产、帐号和密码。

RIS执行改密计划的流程如图 7: 改密流程图所示。

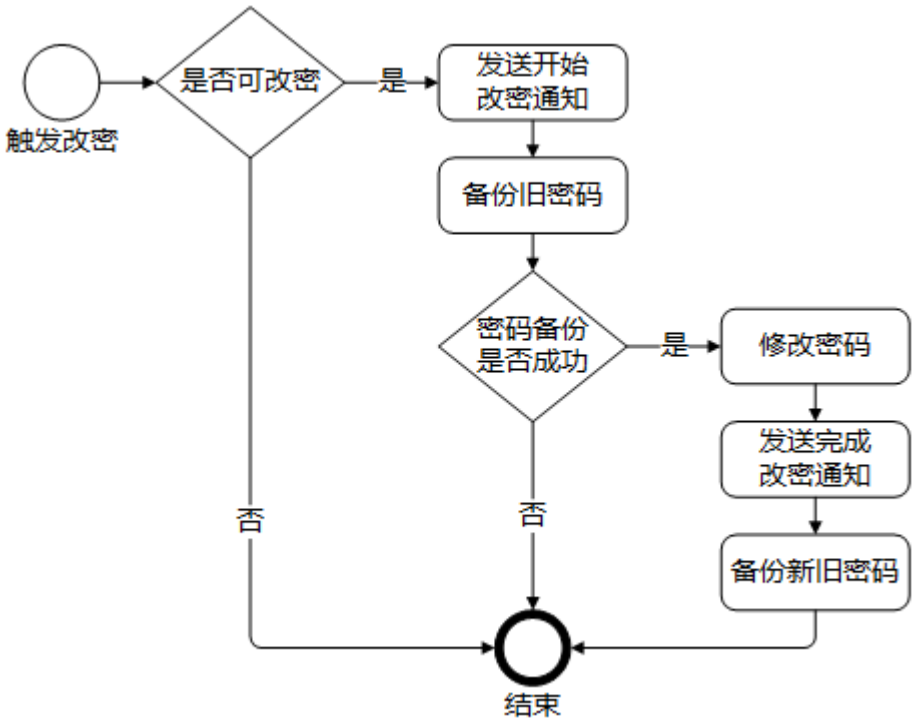


图 7: 改密流程图

RIS支持帐号改密的资产类型和要求如表 31: 支持帐号扫描的资产类型和要求所示。

表 31: 支持帐号扫描的资产类型和要求

资产类型	要求
Windows	Windows系统支持RPC和Agent两种方式，推荐使用Agent方式。 **说明:** 请参照以下方式安装Agent： 1. 单击右上角的用户姓名，并选择**帮助** > **其他应用** > **下载** > **Windows相关应用**，单击下载Agent。 2. 将agent.exe上传到资产上并安装。 3. 设置**地址**为RIS的地址，如RIS为HA部署，则填写虚IP地址。 如之前已安装了Agent，RIS会检查并自动升级所连接的Agent到最新版本。 如果目标设备上已安装Agent，且Agent上已配置RIS的IP地址和端口（缺省端口是TCP 3301），则不需要要目标设备在RIS上托管密码。 如果使用RPC方式，目标设备和RIS需要满足如下要求。 • **Windows设备** 目标设备上已打开TCP的135、139和445端口，且防火墙允许RIS访问这些端口。 • **RIS** 已在RIS上托管目标设备上属于Administrators组的帐号密码。
Linux / HP UX / IBM AIX和网络设备	• **Linux / HP UX / IBM AIX和网络设备** 帐号已配置密码或者密钥。 • **RIS** • RIS上资产的访问协议（SSH或者Telnet）配置正确。 • 已在RIS上托管目标设备上的特权帐号密码。 **说明:** 特权帐号如配置了切换自，RIS在改密时支持根据配置自动完成切换。但对于自定义类型的资产，需要在资产适配中配置**帐号切换命令**，否则帐号切换可能失败。

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

   改密计划的具体参数说明如下：

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

4. 选择改密所使用的密码规则，完成后单击**下一步**。

   密码规则可以选择**模板选择**和**新建模板**：

   - **模板选择**：从已有的密码规则模板中选择一个，在下拉菜单中选取。
   - **新建模板**：新建一个密码规则模板，相关参数的配置请参见配置密码规则。

5. 为改密计划关联待改密的帐号。

   不同方式关联的帐号，在生效时将取并集。有以下三种方式：

   - **指定帐号**：单击之后，在所有可改密的帐号中勾选若干个待改密的帐号，并单击**确定**。
   - **动态关联**：单击之后可以可以配置动态规则。不同规则在生效时会取交集：
     - 在**资产**或**帐号**后单击  ，设置规则的**属性**、**匹配**和**内容**。**资产**可以设置的内置属性包括资产名、IP、简要说明、责任人、资产组和资产类型；**帐号**可以设置的内置属性包括**指定帐号**和**帐号类型**。

- 可以单击  或  ，对规则进行修改或删除。
- 可以单击左下角的**查看帐号**，查看当前设置的规则可以关联上哪些帐号。

全部确认无误后单击**确定**保存动态关联的修改。

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

说明： 改密计划的执行还将受到登录超时时间和任务执行超时时间的影响，默认为20秒和180秒。若在执行过程中登录资产或执行脚本超过了设定的时间，将导致改密失败。用户可以在配置资产适配中，对特定的资产手动设置登录超时时间和任务执行超时时间。

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

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

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

已添加的改密计划，将在该页面的表格中显示以下相关信息。

项目	说明
改密计划	改密计划的名称。
执行方式	自动或手动。
下次执行时间	改密计划下一次执行的时间。当改密计划在执行时，显示为**正在执行**。
关联帐号	改密计划将要修改密码的帐号的数量。
上次改密结果	仅当该改密计划被执行后才会出现。显示最近一次改密的改密成功和改密失败的帐号数量。可以分别单击**成功**或**失败**查看具体成功或失败的信息。  **说明：** 改密成功时，改密的**日志信息**内容默认为空。如需显示详细的改密过程信息，需要超级管理员修改配置文件，在shterm.conf中设置shterm.changepwd.success.detail=true。修改后无需重启，下次执行改密计划成功时将看到详细的日志信息。
操作	• **编辑**：单击**编辑**修改改密计划的参数，参数解释请参见新建改密计划的步骤。 • **立即执行**：单击**立即执行**，手动执行一次该改密计划。 • **历史记录**：仅当该改密计划被执行后才会出现。单击**历史记录**查看该改密计划每次被执行的记录信息。

通过编辑改密计划，可以设置改密计划**是否禁用**为**活动**或**禁用**。改密计划被禁用后，将不会自动执行，也将默认不显示在改密计划列表中。只有单击**筛选**并设置**是否禁用**为**禁用**时，才能看到所有被禁用的改密计划。

配置密码备份

目标设备的帐号和密码在RIS托管后，为了保证密码的安全性，请定期备份密码。

- 已完成配置信息加密，RIS使用该密码或密钥加密密码文件，用户收到密码文件后也需要使用该密码或密钥解密。
- 如果密码备份到文件服务器，请先完成配置文件服务。
- 如果密码发送到用户邮箱，请先完成配置邮件服务。

RIS支持的密码备份方式包括：

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

说明: 为了确保密码的安全性，RIS备份时会对密码文件加密。

1. 选择**工作台** > **帐号改密**。
2. 选择**帐号维护** > **密码备份**。
3. 设置各参数，完成后单击**确定**。

参数	说明
执行时间	密码备份的执行日期和时间。
执行间隔	密码备份的执行间隔。 • 月：执行间隔是月。整数形式，取值范围是1～12。 • 天：执行间隔是天。整数形式，取值范围是1~365。
密码分段	密码备份时是否分段。 • 如果选择**是**，密码将被分成两段，前、后半段需要分别选择不同的备份方式和通知用户。 • 如果选择**否**，密码被作为一个整体备份。
备份方式	密码备份采取的方式。选择好备份方式后，请单击**添加通知用户**来设置接收密码备份通知的用户。 • 邮件备份：加密后的密码以邮件的方式发送给通知用户，请确保该用户的邮箱已配置。邮件备份的具体配置请参见基本设置：配置邮件服务。 • 文件备份：加密后的密码上传到文件服务器，发送给通知用户。文件备份的具体配置请参见基本设置：配置文件服务。 用户收到加密的密码文件后，请使用配置信息加密中配置的密码或密钥解密。

参数	说明
任务通知	接受改密通知的用户。执行改密任务时如果改密规则选择了**同密码备份**时,RIS会在改密前和改密后发送通知给设定的用户。
执行记录	单击**查看**，查看密码备份的执行记录。

日志报表

日志报表中可以查看历史密码。

查看历史密码

历史密码中记录了RIS中所有密码修改操作，一条记录对应一次修改操作，用户可以下载该条记录中的密码。

用户下载密码时，RIS会使用当前登录用户的ZIP文件密码对密码进行压缩，请确保已配置信息加密。用户下载密码后需要使用该密码或密钥解密密码文件。

RIS的密码修改分为两种情况，第一种情况是仅修改RIS上资产帐号的密码，第二种情况是同时修改资产自身的密码和RIS上资产帐号的密码。这些操作都会被记录在历史密码中。

选择**工作台** > **帐号改密** > **日志报表** > **历史密码**，查看资产的历史密码记录。

如果帐号数量大，可通过以下方式查找满足条件的帐号。

- 在搜索文本框中输入帐号、所属资产的名称或者IP的关键字。
- 单击**筛选**，使用历史密码的属性设置过滤条件，单击**筛选**。

参数	说明
帐号名	帐号的名称。
所属资产	帐号所在的资产。
资产IP	资产的IP地址。
密码日期	修改密码的时间。
事件	修改密码的事件类型。
事件结果	上述事件的结果，取值包括**成功**和**失败**。
操作	单击**下载**，将密码文件保存到本地PC。用户也可以选中多个帐号单击**批量下载**或者直接单击**下载全部**，一次性下载更多密码文件。 **说明:** 如果**事件结果**是**成功**，则下载的密码文件是改密前的旧密码；如果**事件结果失败**，则下载的密码文件是改密后的新密码。

系统设置

帐号管理相关的系统设置。

配置密码规则

进行帐号改密，需要先配置改密规则。

改密规则用于设置RIS修改目标资产帐号密码时的新密码策略、密码备份方式和改密计划的最大执行间隔。根据密码策略不同分为:

- 随机生成不同密码
- 随机生成相同密码
- 手工指定密码
- 密码集

配置改密规则（随机生成不同密码）

如果需要在改密时给不同资产和帐号随机生成不同的密码,可以参考以下方式配置改密规则。

1. 选择**工作台** > **帐号改密**。
2. 选择**系统设置** > **密码规则** > **改密规则**。
3. 单击页面右上角的**新建改密规则**,设置各参数,完成后点击确定。

参数	说明
规则名称	密码规则在RIS的唯一名称。允许任意字符,不超过30个字符。
密码策略	请选择**随机生成不同密码**。
使用缺省生成规则	指按照缺省规则生成新密码,密码为长度10位,字符随机。
自定义生成规则	自定义新密码生成规则,参数包括: • **密码长度**,密码总长度,其它字符个数之和不可以超过密码长度。默认值8,允许的值为8-30位之间的数字。 • **最少数字字符个数**,密码中最少包含的数字的个数,默认值2。 • **最少大写字母个数**,密码中最小包含的大写字母的个数,默认值2。 • **最小小写字母个数**,密码中最少包含的小写字母个数,默认值2。 • **最少特殊字符个数**,密码中最少包含的特殊字符个数,默认值2。 • **特殊字符集合**,密码中允许出现的特殊字符,只允许输入半角字符,多个连续输入即可,比如!@#$。
备份类型	设置修改密码时如何备份密码:

参数	说明
	• **自定义**,具体设置参考配置密码备份。 • **同密码备份**,直接使用配置密码备份的设置,如果密码备份中的设置有修改将同步修改。

配置改密规则（随机生成相同密码）

如果需要在改密时给同一批资产及其帐号设置相同的密码,可以参考以下方式配置改密规则。

1. 选择**工作台** > **帐号改密**。
2. 选择**系统设置** > **密码规则** > **改密规则**。
3. 单击页面右上角的**新建改密规则**,设置各参数,完成后单击**确定**。

参数	说明
规则名称	密码规则在RIS的唯一名称。允许任意字符,不超过30个字符。
密码策略	请选择**随机生成相同密码**。
使用缺省生成规则	指按照缺省规则生成新密码,密码为长度10位,字符随机。
自定义生成规则	自定义新密码生成规则,参数包括: • **密码长度**,密码总长度,其它字符个数之和不可以超过密码长度。默认值8,允许的值为8-30位之间的数字。 • **最少数字字符个数**,密码中最少包含的数字的个数,默认值2。 • **最少大写字母个数**,密码中最小包含的大写字母的个数,默认值2。 • **最小小写字母个数**,密码中最少包含的小写字母个数,默认值2。 • **最少特殊字符个数**,密码中最少包含的特殊字符个数,默认值2。 • **特殊字符集合**,密码中允许出现的特殊字符,只允许输入半角字符,多个连续输入即可,比如!@#$。
备份类型	设置修改密码时如何备份密码: • **自定义**,具体设置参考配置密码备份。 • **同密码备份**,直接使用配置密码备份的设置,如果密码备份中的设置有修改将同步修改。

配置改密规则（手工指定密码）

如果需要在改密时给同一批资产及其帐号设置指定的密码,可以参考以下方式配置改密规则。

1. 选择**工作台** > **帐号改密**。
2. 选择**系统设置** > **密码规则** > **改密规则**。
3. 单击页面右上角的**新建改密规则**,设置各参数,完成后点击确定。

参数	**说明**
规则名称	密码规则在RIS的唯一名称。允许任意字符,不超过30个字符。
密码策略	请选择**手动指定密码**。
密码输入	输入新密码。
重复确认	再次输入新密码,如果和第一次输入的不一致将提示"两次密码输入不一致"。
备份类型	设置修改密码时如何备份密码: • **自定义**,具体设置参考配置密码备份。 • **同密码备份**,直接使用配置密码备份的设置,如果密码备份中的设置有修改将同步修改。

配置改密规则（密码集）

如果需要给同一批帐号设置新密码时,仅从特定的随机密码集合中选取密码,可以参考以下方式配置改密规则。

1. 选择**工作台** > **帐号改密**。
2. 选择**系统设置** > **密码规则** > **改密规则**。
3. 单击**新建改密规则**,设置各参数,完成后点击确定。

参数	**说明**
规则名称	密码规则在RIS的唯一名称。允许任意字符,不超过30个字符。
密码策略	请选择**密码集**。
使用缺省生成规则	指按照缺省规则生成新密码,密码为长度10位,字符随机。
自定义生成规则	自定义新密码生成规则,参数包括: • **密码长度**,密码总长度,其它字符个数之和不可以超过密码长度。默认值8,允许的值为8-30位之间的数字。 • **最少数字字符个数**,密码中最少包含的数字的个数,默认值2。 • **最少大写字母个数**,密码中最小包含的大写字母的个数,默认值2。 • **最小小写字母个数**,密码中最少包含的小写字母个数,默认值2。 • **最少特殊字符个数**,密码中最少包含的特殊字符个数,默认值2。

参数	说明
	• **特殊字符集合**,密码中允许出现的特殊字符,只允许输入半角字符,多个连续输入即可,比如!@#$。
密码有效期(月)	密码集的有效期,到期后将自动产生新的密码集。默认值为3个月,可选6个月或者12个月。
密码数量	密码集中包含的密码的数量。默认20个,可选50个、100个、200个。
备份类型	设置修改密码时如何备份密码: • **自定义**,具体设置参考配置密码备份。 • **同密码备份**,直接使用配置密码备份的设置,如果密码备份中的设置有修改将同步修改。

配置完成后您可以在当前页面单击**下载密码集**,密码文件将使用您在**帐号设置** > **修改信息** > **信息加密**中设置的**ZIP文件加密**加密。您也可以在当前页面点击**重新生成**,生成新的密码集。

配置改密方法

如果RIS内置的改密方法无法满足需求时可以配置自定义改密方法。

推荐使用RIS内置的改密方法修改资产密码，您可以在**系统设置-资产-资产类型**中修改资产类型的**改密方式**，调整内置的改密方法。如果一定要自定义改密方法，请确保:

- 目标资产支持通过Telnet或者SSH方式修改密码。
- 了解目标资产的改密命令和输出。

警告: 错误的改密方法可能导致密码丢失或者其它严重的问题，请谨慎配置。

1. 选择**工作台** > **帐号改密** > **系统设置** > **改密方法**。
2. 单击**新增改密方法**，依次完成后续操作后单击**保存**。
3. 填写**方法名**，改密方法的唯一名称，允许任意字符，不超过30字符。
4. 配置**改密工具**。
   a) 单击**改密工具**后的。
   b) 选择**工具类型**。

工具类型	工具说明
交互式指令(Telnet)	RIS通过Telnet方式登录目标资产，执行指令，并根据目标资产的命令提示自动完成改密相关的交互。
交互式指令(SSH)	RIS通过SSH方式登录目标资产，执行指令，并根据目标资产的命令提示自动完成改密相关的交互。

工具类型	工具说明
Groovy脚本	RIS以Groovy脚本的方式调用Apache HttpComponents访问B/S应用，实现对B/S应用的密码修改。关于Groovy可参考The Apache Groovy programming language。 **说明:** • 仅作为技术预览，如果需要适配新的B/S资产需要付费定制，具体请联系技术支持人员。 • 自定义Groovy脚本必须执行命令**shtermtools zip xxx.groovy**生成**xxx.groovy.zip**后才能上传。
Python脚本	RIS支持用户在改密方法中上传Python类型的脚本，访问B/S应用，实现对B/S应用的密码修改。 **说明:** • Python脚本可以在线编辑和格式化，但需要在shterm.conf文件中配置accountManage.supportEditPython=true。 • Python脚本需要付费定制，具体请联系技术支持人员。 • 自定义Python脚本必须执行命令**shtermtools zip xxx.py**生成**xxx.py.zip**后才能上传。

c) 单击**下载模板**，修改脚本后，单击**文件上传**，选择编写好的脚本上传，然后单击**保存**。

说明: 上传脚本文件后，管理员可以单击将脚本文件下载到本地PC，也可以单击删除不需要的脚本文件。

交互式指令(包括Telnet和SSH)模板是一个JSON文件，以模板为例：

```
{
 "changesecret":{
  "expectparams": [
   {
    "id": "1",
    "cmd": "export LANG=C LC_ALL=en_US.UTF-8"
   },{
    "id": "2",
    "cmd": "[ -x /usr/bin/pwdadm ] && /usr/bin/pwdadm -f NOCHECK <%account%>",
    "pid": "1"
   },{
    "id" : "3",
    "cmd": "passwd <%account%>",
    "pid": "2"
   },{
    "id" : "4",
    "cmd": "passwd",
    "ptn": "[oO]nly",
    "pid": "3"
   },{
    "id": "5",
    "cmd": "<%oldpassword%>",
    "ptn": "([cC]urrent)|([oO]ld)",
    "alt": "<oldpwd>",
    "pid": "4"
   },{
    "id": "6",
```

```
    "cmd": "<%password%>",
    "ptn": "[nN]ew.*assword:",
    "alt": "<pwd>",
    "pid": ["3", "5"]
   },{
    "id": "7",
    "cmd": "<%password%>",
    "ptn": "[rR]e.*assword:",
    "alt": "<pwd>",
    "pid": "6"
   },{
    "id": "8",
    "cmd": "[ -x /usr/bin/pwdadm ] && /usr/bin/pwdadm -c <%account%>",
    "pid": "7"
   }
  ]
 },
 "changesecretandverify":{
  "expectparams": [
   {
    "id": "1",
    "cmd": "export LANG=C LC_ALL=en_US.UTF-8"
   },{
    "id": "2",
    "cmd": "[ -x /usr/bin/pwdadm ] && /usr/bin/pwdadm -f NOCHECK <%account%>",
    "pid": "1"
   },{
    "id" : "3",
    "cmd": "passwd <%account%>",
    "pid": "2"
   },{
    "id" : "4",
    "cmd": "passwd",
    "ptn": "[oO]nly",
    "pid": "3"
   },{
    "id": "5",
    "cmd": "<%oldpassword%>",
    "ptn": "([cC]urrent)|([oO]ld)",
    "alt": "<oldpwd>",
    "pid": "4"
   },{
    "id": "6",
    "cmd": "<%password%>",
    "ptn": "[nN]ew.*assword:",
    "alt": "<pwd>",
    "pid": ["3", "5"]
   },{
    "id": "7",
    "cmd": "<%password%>",
    "ptn": "[rR]e.*assword:",
    "alt": "<pwd>",
    "pid": "6"
   },{
    "id": "8",
    "cmd": "[ -x /usr/bin/pwdadm ] && /usr/bin/pwdadm -c <%account%>",
    "pid": "7"
   },{
    "id": "9",
    "cmd": "LANG=C LC_ALL=en_US.UTF-8 su - <%account%>",
    "pid": "8"
   },{
    "id": "10",
    "cmd": "LANG=C LC_ALL=en_US.UTF-8 su - <%account%>",
    "pid": "9"
   },{
    "id": "11",
    "cmd": "<%password%>",
    "ptn": "assword",
    "alt": "<pwd>",
    "pid": ["9", "10"]
   },{
    "id": "12",
    "cmd": "",
    "pid": "11"
   },{
    "id": "13",
    "cmd": "",
    "ptn": "([Ii]ncorrect)|(Ff)ail",
    "pid": "11"
   },{
    "id": "14",
    "cmd": "echo FAILE",
    "ptn": "SHTERM VERIFY PASSWORD FAILED",
    "pid": "13"
   },{
    "id": "15",
    "cmd": "",
    "pid": "10"
   }
  ]
 },
 "verify":{
  "expectparams": [
   {
```

```
    "id": "1",
    "cmd": "echo flag"
   },{
    "id": "2",
    "cmd": "echo verify success",
    "ptn": "flag.*flag",
    "pid": "1"
   }
  ]
 }
}
```

- 改密过程模板包含**changesecret**、**changesecretandverify**和**verify**三个改密过程对象，分别表示改密、改密并验证和验证三个改密过程。配置时，只能同时配置**改密**和**验证**，或者只配置**改密并验证**。
- 每一个改密过程都有一个**expectparams**对象，每一个**expectparams**包含多个键/值对组成Step记录。
- Step记录允许的键包括：
  - id：表示Step ID，必填，大于等于1的正整数，RIS会按照id的顺序依次执行。
  - pid：父Step ID，除id为1的无父id，其它Step都必须填写，父id的数字不能大于id的数字。允许有多个值，表示分支，RIS将根据匹配到的ptn自动选择分支，比如 ["3", "5"]。
  - ptn：表示要匹配命令提示，支持正则表达式，如果留空将使用目标资产的默认提示符如#或者$。比如，如果出现"new passwd:"后输入新密码，ptn可以设置为"new passwd:"。
  - cmd：要执行的命令，比如passwd指令。
  - alt：改密日志中替换cmd输出的文本，比如改密的命令是net user <%account%> <%password%>，为了防止改密日志中直接看到密码，可以将alt设置为net user xxx xxx，最终改密日志中将显示成net user xxx xxx。
- ptn、cmd和alt支持使用变量，支持的变量包括：

变量	**说明**
<%account%>	需要改密的帐号名
<%password%>	新密码
<%oldpassword%>	旧密码

5. 对于Telnet和SSH脚本，可以单击，在弹出的对话框中编辑已经上传的交互式脚本。

- 将鼠标悬停在对话框左上角**编辑改密工具**旁边的上，查看对正则表达式字符的转义说明。
- RIS支持在线校验json格式的脚本是否有格式错误。通过单击**格式化**按钮，检查已编辑的脚本。如存在问题，RIS将指出错误位置，并给出错误信息。

a) 单击左下角的**添加测试帐号**，在弹出的对话框中勾选测试帐号。

b) 单击左下角的**添加改密规则**，弹出**请选择改密计划**对话框，在**改密规则**下拉菜单中选择对应的改密规则，完成后单击**确定**。

在添加了测试帐号之后，**编辑改密工具**页面出现**登录测试**、**重置密码**和**改密测试**三个按钮。

- 单击**登录测试**，可以对在编辑脚本页面直接设置的帐号密码执行登录测试，并返回测试结果。
- 单击**重置密码**，可以手动修改该帐号在RIS中托管的密码。仅当RIS中托管的密码错误时使用该功能。
- 单击**改密测试**，RIS将立即对校验通过的脚本做改密测试，并返回结果和命令执行详情，改密成功则直接更新对应帐号的密码。

说明: 同一个改密方法中允许同时添加多种改密工具，改密时将按顺序尝试不同的工具，直到改密成功为止，如果全部失败将使用**系统设置** > **资产** > **资产类型**中配置改密方法。您可以使用↑和↓调整不同改密方法的顺序。

6. 配置改密方法的适用范围。

参数	说明
适用资产	按资产选择改密方法适用的资产。默认为空，选填。单击⊕可在弹出页中添加和删除。
适用资产组	按资产组选择改密方法适用的资产。默认为可，选填。单击⊕可在弹出页中添加和删除。
适用帐号	适用的帐号。不选择表示适用于选定资产或者资产组的全部帐号。单击**修改**，可以输入适用帐号的帐号名，比如root，输入后回车后可以保存。

7. 可选： 已经添加的改密方法，单击**编辑**，可以修改或者**删除**。

相关任务

配置资产类型

管理员修改资产类型的属性，新增资产类型。

个人帐号相关设置

11

目录:

所有用户都能够进行个人帐号相关设置。个人相关设置包括Web界面的**帐号设置**和**访问记录**中的所有查看及修改设置的操作。

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admin），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，并在管理员进行用户/资产/权限管理时作为提示信息。取值范围为1~100长度的字符串，不能为空。
手机号码	在以下场景会使用该手机号码： • 用户启用了短信认证，登录RIS时，RIS会将短信密码发送到该手机号。 • 系统启用了会话复核发送短信的功能，被复核人在建立会话后，复核人的手机号码会收到提醒复核的手机短信。 • 系统启用了命令复核发送短信的功能，被复核人执行满足条件的命令后，复核人的手机号码会收到提醒复核的手机短信。 标准格式的手机号码。如设置为空则不会发送短信给用户。
工作邮箱	在需要发送邮件给用户时，如发送备份的密码给相关用户时，RIS会将相关信息发送到用户设置的该邮箱中。

参数	说明
	标准格式的邮箱地址。如不设置，则在需要设置发送密码备份等信息的目标用户时，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。使用AD/LDAP、RADIUS认证的用户请在对应的AD/LDAP、RADIUS服务器上修改密码；使用手机令牌、短信认证、动态令牌的用户，请联系配置管理员在用户管理菜单中修改密码。

1. 单击右上角用户帐号（例如admin），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。

修改语言设置

用于设置用户登录到RIS Web界面之后的语言，支持中文和英文。

1. 单击右上角用户帐号（例如admin），选择**帐号设置**。
2. 选择**修改信息** > **个人设置** > **语言设置**。
3. 根据需要勾选待设置的语言，并单击**确定**保存。

   - **同系统配置**：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。
   - **中文**
   - **英文**

修改成功后，不用重新登录，Web界面的语言修改将立即生效。

设置操作员默认展示页面

仅当用户类型为操作员时会显示该页签。用于设置操作员登录到RIS Web界面之后默认展示的页面。

1. 单击右上角用户帐号（例如operator），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，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。
   - **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。

配置信息加密

仅当用户类型为超级管理员和配置管理员时会显示该页签并可以配置。当RIS需要将密码信息提供给用户时（例如密码备份），会按照用户设置的密码对信息进行加密，从而确保文件的安全性。

配置信息加密有两种方式：

- 将信息打包成ZIP包并通过ZIP密码加密。
- 将信息文件通过PGP加密。

当用户同时配置了以上两种加密方式时，单个文件将仅使用PGP加密；如存在多个文件需要打包加密，RIS会将其先打包成ZIP包，使用ZIP加密， 再使用PGP公钥加密。

完成配置信息加密的设置之后，用户在**帐号改密**中进行以下操作时，获得的密码文件将被加密：

- 在**帐号维护** > **密码备份**中备份密码时获得备份的密码。
- 在**帐号维护** > **改密计划**中执行改密计划时获得改密前和改密后的密码。
- 在**帐号资产**中**编辑**帐号，并选择**密码管理** > **查看历史密码**。
- 在**日志报表** > **历史密码**中，查看历史密码。
- 在**系统设置** > **密码规则**中，下载密码集。

请通过设置的ZIP密码，或PGP私钥对获得的加密文件进行解密，从而查看其中的信息。

配置ZIP文件密码

1. 单击右上角用户帐号（例如admin），选择**帐号设置**。
2. 选择**修改信息** > **信息加密** > **ZIP文件密码**。
3. 输入修改后的ZIP文件密码，该密码需要重复输入两次。
   - 密码必须为8~32长度的字符串，不能包含空格。
   - 为了确保安全性，ZIP文件密码一旦设置了就不能取消，只能对密码进行修改。
4. 确认设置的密码无误后，单击**确定**保存ZIP文件密码设置。

   完成ZIP密码设置，当前用户后续收到或下载的ZIP文件将被加密，请使用该密码解密。

配置PGP公钥

用户可以在此处配置PGP公钥。RIS会将用户的密码信息通过该公钥加密，用户可以通过对应的私钥来解密。

PGP（Pretty Good Privacy）是一套用于消息加密、验证的应用程序。用户可以使用GPG4WIN等加密解密软件来生成密钥对，并进行加密和解密。

1. 单击右上角用户帐号（例如admin），选择**帐号设置**。
2. 选择**修改信息** > **信息加密** > **PGP公钥加密**。
3. 在**输入公钥**输入框内粘贴入PGP加密软件生成的公钥。

说明：也可以单击**浏览**上传公钥文件。RIS仅支持上传asc格式的公钥文件。上传成功后，公钥文件中的公钥将被读取并显示在**输入公钥**的框体中。

4. 确认无误后单击**确定**，保存公钥设置。

完成PGP公钥设置后，当前用户后续收到或下载的敏感信息文件将被加密为.gpg后缀的文件。请通过公钥对应的私钥进行解密。

如用户收到或下载的是多个文件，将被先打包成ZIP包再进行PGP加密，用户将收到.zip.pgp后缀的文件。请先通过PGP私钥解密成ZIP包，再通过配置ZIP文件密码中的密码解压ZIP包。

如需清除PGP公钥配置，请单击**重置**并单击**确定**。

修改会话配置

仅当用户角色为操作员、超级管理员、配置管理员时会显示该页签并可以配置。用于设置用户在访问资产并进行字符、图形会话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admin），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
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，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，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。 • scrt：使用SecureCRT工具建立字符会话。需要自己安装SecureCRT。 • xshell：使用Xshell工具建立字符会话。需要自己安装Xshell。
会话访问方式(Mac)	用于设置本地PC为Mac时的字符会话访问方式，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，括号内会显示当前具体的配置。 • Terminal：使用MacOS自带的字符会话终端建立字符会话。 • scrt：使用SecureCRT工具建立字符会话。需要自己安装SecureCRT。
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：

参数	说明
	• 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。最小单位为15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：表示使用全局设置，具体请参见配置字符终端参数。 • 资产组 • 资产类型 • 责任人

修改图形会话配置

用于设置用户访问资产时建立的图形会话的分辨率、访问方式、最大持续时间等参数。

1. 单击右上角用户帐号（例如admin），选择**帐号设置**。
2. 选择**修改信息** > **会话配置** > **图形会话**。
3. 设置需要修改的参数，完成后单击**确定**。

参数	说明
图形会话分辨率	仅当图形会话访问方式设置为**mstsc**时该参数的设置有效。 用于在启动RDP图形会话及应用系统图形会话的分辨率选项列表中，添加用户自定义的分辨率。RIS分辨率选项列表中默认提供的分辨率包括：800x600、1024x768、1280x1024、全屏、最大化，该参数设置的图形会话分辨率将添加到该列表中，供访问时选择。 分辨率的取值范围为640x480~9999x9999。多个分辨率之间用空格隔开，例如“1280x800 1920x1080”。
默认分辨率	仅当图形会话访问方式设置为**mstsc**时该参数的设置有效。 用于在启动RDP图形会话及应用系统的图形会话的分辨率选项中，设置分辨率的默认值。取值范围为640x480~9999x9999，或fullscreen、maximize。 该参数为空表示使用系统设置的全局默认分辨率。如设置的默认分辨率不在图形会话分辨率列表中，RIS会自动将该分辨率也添加到分辨率列表中。
图形会话访问方式	用于设置RDP图形会话及应用系统的图形会话的访问方式，取值范围如下：

参数	说明
	• 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。 • web：当在Web界面中建立图形会话时，使用Web方式建立图形会话。 • mstsc：当在Web界面中建立图形会话时，使用mstsc方式建立图形会话。 **说明：** web和mstsc的访问方式，请根据实际情况选择。这两种访问方式对不同功能的支持也有一定限制，如web方式不支持通过剪贴板和磁盘映射传输文件，mstsc方式不支持会话共享。
启用Console连接	勾选该参数仅表示在配置所有RDP图形会话的启动参数时，都默认勾选**启用Console连接**，跟用户最终建立会话时是否勾选**启用Console连接**无关。 仅当待访问的资产的RDP访问协议中勾选了**console**时，该资产建立RDP会话时才会显示**启用Console连接**，此时**帐号设置**中该参数的设置才有效。 **说明：** 仅当待访问的主机系统是Windows Server时需要启用Console连接。启用Console连接表示使用**/console**参数登录Windows Server 2003，从而打开一个session id为0的控制台会话，或使用/admin参数登录Windows Server 2008/2012/2016，打开一个session id为0的管理员模式的会话。
最大持续时间	用于设置字符会话的最大持续时间，取值范围如下： • 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。最小单位为15分钟，不能设置为0天0小时0分钟。
磁盘映射	仅当图形会话访问方式设置为**mstsc**时该参数的设置有效。 设置该参数仅表示在配置所有RDP图形会话及应用系统的图形会话的启动参数时，磁盘映射都默认勾选该参数设置的磁盘盘符。用户最终建立会话时是否会勾选对应磁盘的映射由用户自己决定。 该参数输入格式为单个字母表示的盘符，多个盘符之间用英文逗号隔开，例如“c,d,f”。 **说明：** 启用磁盘映射，并勾选或手动设置待映射的盘符，将本地PC对应盘符的硬盘，映射到待访问的资产上，使访问者可以直接在该资产上对本地PC上的相应硬盘进行读写操作。

参数	说明
回放方式	仅当登录用户为具有审计权限的角色（如超级管理员、审计管理员）时，显示该选项。 用于控制进行图形审计回放时的回放方式，取值范围如下： • 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。 • web：在浏览器中播放会话录屏。 • java：在JAVA窗口中播放会话录屏。 **说明：** web和java方式的详细区别，请参考播放会话录屏。

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admin），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： • 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。
会话访问方式(Mac)	用于设置本地PC为Mac时建立SFTP会话使用的工具，取值范围如下： • 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。

配置密钥

仅当用户可以登录交互终端并访问资产时该页签配置有效，比如用户类型为操作员、超级管理员、配置管理员。用于当用户通过SSH登录RIS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RIS的字符交互终端。

1. 使用工具生成密钥对。密钥类型为RSA，密钥长度为512、1024或2048。

   本文以Xshell为例介绍密钥对的生成。也可以使用其他能够生成RSA密钥对的工具。

a) 选择**工具** > **新建用户密钥生成向导**。

b) 设置密钥类型为**RSA**，密钥长度为**512**、**1024**或**2048**位，并单击**下一步**。

c) 显示**公钥对已成功生成**之后，单击**下一步**。

d) 设置密钥名称和密码，并单击**下一步**。对安全性没有较高要求的情况下不用设置密码。

e) 设置公钥格式为**SSH-OpenSSH**，单击**保存为文件...**，将公钥保存到本地。

f) 在弹出的**用户密钥**界面中（或选择**工具** > **用户密钥管理者**），选中刚才生成的密钥，单击**导出**，将私钥保存到本地，用于当使用SSH连接到RIS时进行验证。

2. 登录RIS Web界面。
3. 单击右上角用户帐号（例如admin），选择**帐号设置**。
4. 选择**修改信息** > **密钥管理**。
5. 单击**新建**。
6. 在输入框中输入通过密钥生成工具生成的公钥，并单击**增加**。用记事本打开1.e中生成的公钥并复制，或在1.e的窗口中直接复制生成的公钥。

   已完成新增密钥。

当前用户通过字符终端工具登录RIS交互终端时，可以通过1.f中保存的密钥进行验证，参见通过SSH登录RIS。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。

查看访问记录

用户可以通过查看**访问记录**中的信息，查看当前帐号的登录、登出情况，以确保帐号的安全。访问记录中会包含该用户的所有访问记录，除非管理员对登录日志做了清理。

1. 单击右上角用户帐号（例如admin），选择**访问记录**。
2. 查看访问记录的内容。可以单击右下角的箭头翻页，或者单击进行刷新。

   访问记录每一列显示的信息解释如下：

项目	说明
时间	当前帐号登入或登出的时间。
来自	当前帐号登录请求的来源IP。如登录操作经过了跳转，显示的IP为直接连接RIS的IP。
姓名	登录帐号的姓名，在**帐号设置**中设置。登录失败时不显示。
帐号	当前登录帐号的名称。
身份验证	当前帐号登录时采用的身份验证方法，取值为系统允许的各种登录认证方式。使用双因子认证时将显示为使用的双因子认证方式模板的名称。使用密钥登录SSH交互终端时，会显示为pubkey。

项目	说明
登录方式	当前帐号登录RIS的方式，取值范围如下： • WEB：使用Web界面登录RIS。 • GUI：使用Mstsc客户端登录RIS。 • TUI：使用SSH客户端登录到RIS交互终端。 • 空值：登出时显示为空。
登录描述	当前帐号登录情况，取值为“登录成功”、“登录失败”、“登出成功”之一。
操作结果	当前帐号登录或登出的结果，取值为“成功”或“失败”之一。

系统设置 12

目录:

系统

基本设置：配置网络参数

超级管理员可以在该界面查看RIS网口的硬件信息及IP配置，并对IP相关配置和静态路由配置进行修改。HA、部署环境下不支持直接修改IP地址。

配置系统IP地址

在配置IP地址前请确保已经正确的连线。

注意： HA部署的RIS，请先将需要修改的节点从HA中移除才可以修改IP，，否则将不支持修改IP地址。

修改IP地址将造成Web界面暂时无法访问，请等待系统后台重启完成后重新访问Web界面，一般需要等待1分钟左右。

系统IP地址、网关、DNS通常在安装和部署时完成，可以在此处查看。单机部署环境下也可以在Web界面重新修改或者配置其它网口的IP地址。

1. 选择**系统设置** > **系统** > **基本设置** > **系统IP**。
2. 查看网口信息。

参数	说明
网口	网口名称。当有多个网口时可以下拉选择，下方的其他信息将对应显示该网卡的信息。
网口类型	光口或电口。
网口速率	网口传输速率。
已连接	网口状态。
IP	该网口上配置的IP地址，包括IPv4和IPv6地址。当有多个IP时可以下拉选择，**掩码/前缀**将显示为对应的IP的掩码/前缀。
掩码/前缀	IPv4地址将显示为掩码，IPv6地址将显示为前缀。

参数	说明
网关	该网口的默认网关地址。
主DNS	主DNS服务器。
备DNS	备DNS服务器。

3. 单击**配置**，填写待修改的参数，完成后单击**确定**。

注意：修改该菜单的参数，可能导致Web界面断开连接，如配置错误将无法连接到RIS，请确认无误后再保存配置。

参数	说明
网口	选择要配置的网口。比如eth0、eth1，RIS型号不同可选的网口会有所不同。
方式	IP地址的配置方式： • **静态**：默认值，表示手工配置静态IP。 • **DHCP**：表示通过DHCP Server获取自动获取，正式部署的RIS不建议采用这种方式。 **注意：** • 启用DHCP时会检查DHCP服务器是否可用，如不可用将无法启用DHCP。但如DHCP服务器一开始可用，并成功启用了DHCP，后来将**方式**修改为**静态**后，DHCP服务器故障，此时能够再启用DHCP，但将会无法分配IP。此时请在Console菜单中重启系统解决该问题。 • 使用DHCP必须给对应的网口插好网线，否则RIS启动时将会报错。 • **None**：表示清空该网口的所有配置。 **说明：**该网口如配置了默认网关，将不允许执行清空操作。必须将默认网关配置到其他网口上后，再执行清空操作。
IPv4	IPv4地址，**方式**为静态IP是必填，DHCP时无此选项。
子网掩码	掩码填写方式。**掩码**或**前缀**。
掩码/前缀	子网掩码，必填，DHCP时无此选项。**子网掩码**选择**掩码**时填写完整的掩码，选择**前缀**时仅填写掩码前缀。
网关	IPv4地址的默认网关，选填，DHCP时无此选项。

参数	说明
	说明： 存在多个网口时，请勿给多个网口同时配置IPv4网关，否则可能导致网络不可达。如果需要配置静态路由，请登录RIS的Console控制台进行配置。
主DNS	主DNS服务器，选填，DHCP时无此选项。
备DNS	备DNS服务器，选填，DHCP时无此选项。
IPv6	IPv6地址，选填，DHCP时无此选项。支持用户使用该IPv6地址访问RIS。
IPv6前缀	IPv6格式对应的前缀格式的掩码，1~128。仅当配置了IPv6地址时需要填写。
IPv6缺省网关	IPv6地址的默认网关，仅当配置了IPv6地址时需要填写。 **说明：** 存在多个网口时，请勿给多个网口同时配置IPv6网关，否则可能导致网络不可达。

配置静态路由

用户可以在此执行对RIS的静态路由配置的查看、添加和删除操作。

1. 选择**系统设置** > **系统** > **基本设置** > **系统IP**。
2. 查看当前系统路由信息。

   在**当前系统路由**框体中显示了RIS的所有路由配置，包括IPv4和IPv6路由，例如：

   ```
   default via 10.10.32.1 dev eth0 proto static metric 100
   1.1.1.0/24 dev virbr0 proto kernel scope link src 1.1.1.1
   10.10.32.0/20 dev eth0 proto kernel scope link src 10.10.33.32 metric 100
   fc00:1010:32::/64 dev eth0 proto kernel metric 256 expires 2591576sec pref medium
   fe80::/64 dev eth0 proto kernel metric 256 pref medium
   default via fe80::3a22:d6ff:fe71:db1 dev eth0 proto ra metric 1024 expires 1376sec hoplimit 64 pref medium
   ```

   可以单击按钮，刷新当前系统路由信息显示。

   说明： 此处显示的路由配置，即为Linux命令ip route show和ip -6 route show两条命令的结果。请参照这两条命令的解释理解路由信息的具体含义。

3. 如需新增路由，单击，填写新增路由的**目标地址**和**网关地址**。

参数	说明
目标地址	通过路由访问的目标地址，可以是具体的IP，例如10.10.17.12；也可以是**网段/掩码前缀**的形式，例如10.10.17.0/24。
网关地址	路由转发地址，填写网关的具体IP，例如10.10.17.1。

说明： 如需添加多条路由，多次单击并填写每一条路由的信息。如需删除路由，则单击该条路由对应的。

4. 完成路由的新增或删除操作后，单击**更新路由配置**。

单击**更新路由配置**后，RIS将会把Web界面上配置的路由同步到路由表中。同步时会检测路由配置是否正确，如路由不可达，将弹出错误提示。

如需删除所有非系统初始配置的路由，请单击**删除静态路由配置**，执行该操作将清空Web页面上的所有新增的路由配置并同步到路由表中。

基本设置：配置系统时间

RIS支持手工修改和NTP同步两种方式修改系统时间和日期，您也可以通过Web页面查看系统时间。

查询系统当前时间

要查看当前系统时间：

1. 选择**系统设置** > **系统** > **基本设置** > **系统时间**。
2. 页面将显示当前系统时间。

说明： 页面中显示的时间是RIS的系统时间，但时区将会按照本地PC的时区进行显示。

手工配置系统时间

要手工修改系统时间：

1. 选择**系统设置** > **系统** > **基本设置** > **系统时间**。
2. 选择**手工校准服务器时间**。
3. 设置新的日期和时间，完成后单击**确定**。

   手工配置时间不支持对秒进行配置。

完成后系统时间将更新，如果之前配置了NTP，将停用NTP。HA部署的所有节点的时间将同步更新。

配置NTP服务

要让系统时间和NTP服务器保持一致，可以配置NTP服务。

1. 选择**系统设置** > **系统** > **基本设置** > **系统时间**。
2. 选择**配置NTP服务**。
3. 填写**服务主机名或IP地址**，完成后点击**确定**。

   服务主机名或IP地址，可以填NTP服务器的域名或者IPv4地址。

说明： 请确保RIS可以和NTP服务器的UDP 123端口通讯。

完成后，RIS将立即与NTP进行一次同步，并启动同步服务，持续和NTP服务器进行时间校准。HA部署的所有节点的时间将同步更新。

基本设置：配置邮件服务

RIS支持通过邮件发送通知和告警，要正常使用这些功能，需要配置邮件服务。

要使用邮件服务器，需要先进行下列准备工作:

- 准备一台邮件服务器。
- 给RIS分配邮件帐号。
- 确保RIS可以访问邮件服务器的SMTP端口。

1. 选择**系统设置** > **系统** > **基本设置** > **邮件服务**。
2. 配置各参数，完成后点击**确定**。

参数	说明
邮件服务器	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	发件人地址，必填，格式需要符合RFC5322中定义的E-mail地址格式。默认值root@shterm.com，请修改为您的邮件服务器中分配的地址。
发件人名称	发件人的显示名称。选填，任意字符，不超过64的字符。比如您可以设置成RIS。
服务器要求安全连接(SSL/TLS)	RIS和邮件服务器之间的通讯是否需要加密，默认值未勾选，请根据实际情况选择。
本地postfix转发	仅当**邮件服务器**地址不为默认值127.0.0.1时显示此选项。勾选后，表示使用RIS作为邮件转发服务器，邮件先发到RIS再转发到邮件服务器。默认未勾选，请根据实际情况选择。
服务器要求身份验证	SMTP服务器是否要求进行身份验证，默认未勾选，请根据实际情况选择。如果选择了需要填写: • **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。

如果配置正确，单击**测试**，填写**收件人地址**，单击**确定**，收件人可以收到标题为**This is a test mail**的测试邮件。

基本设置：配置文件服务

如果需要使用RIS的审计数据定期备份或者希望将帐号密码备份到文件服务器，需要准备FTP或者SFTP服务器并在RIS中配置文件服务器。

在配置文件服务器前，请先:

- 准备FTP或者SFTP服务器。
- 创建FTP或者SFTP帐号和密码。

1. 选择**系统设置** > **系统** > **基本设置** > **文件服务**。
2. 设置各参数，完成后单击**确定**。

说明:

- RIS支持同时配置两个文件服务器。实际使用哪一个，取决于帐号管理和审计数据备份中的具体设置。
- 参数设置完成，您可以单击**测试**进行连通性测试。

参数	说明
协议	文件服务器使用的传输协议。 • **FTP** • **SFTP**：通常安装有OpenSSH Server的Linux或者Unix都支持。 • **无**：缺省值，表示不启用。
地址	文件服务器的IP地址。该项必填。
端口	文件服务器的端口。FTP默认为21，SFTP默认为22。该项必填。
用户名	文件服务器的用户名。该项必填。
密码	文件服务器的密码。该项必填。
工作目录	文件存放目录，要求必须使用Unix格式的目录风格。支持通配符，例如Linux的家目录可以配置为**/home/%username**（%username表示用户名）。该项必填。 建议采用绝对路径，例如**/a/b/c**。如果采用的是相对路径，例如**a/b/c**，对于Linux服务器会将**/**作为起点，对于Windows服务器会将FTP/SFTP的根目录作为起点。 **说明:** • 请确保用户对该目录有读、写、执行权限。 • 如果填写的目录不存在，RIS将在审计数据备份或者密码备份时自动创建。
子目录	文件存放的子目录。该项选填。子目录建立在工作目录下，支持日期变量: • %Y：将被替换为执行任务时的年，比如2018。 • %m：将被替换为执行任务时的月，比如07。 • %d：将被替换为执行任务时的日，比如10。

参数	说明
	说明： 仅在帐号管理功能中使用。
编码	文件服务器的文件名编码，缺省值UTF-8，常见的中文编码还包括GBK、GB2312、GB18030。该项必填。 **说明：** RIS会检测文件服务器是否支持UTF-8编码，如支持则优先使用UTF-8编码，此处的配置将不生效；如文件服务器不支持UTF-8编码，此处的配置才会生效。

相关任务

定期任务：配置审计数据备份

RIS支持对审计数据进行手动和定期备份，手动或定期自动将RIS中的审计数据备份到文件服务器上。

基本设置：配置告警事件

通过配置告警事件可以实现身份认证成功/失败、访问特定资产、执行高危操作以及会话复核时发送Syslog或者邮件告警。

RIS支持Syslog和邮件两个方式发送告警事件。

配置Syslog告警

配置Syslog告警可以在触发告警条件时，将Syslog日志发送到Syslog服务器。

1. 选择**系统设置** > **系统** > **基本设置** > **告警事件**。
2. 设置各参数，完成后单击**确定**。

参数	说明
syslog日志事件来源	配置需要通过Syslog发送的日志类型和最低发送级别(Severity)。 事件类型： • **身份验证**：表示用户登录RIS的事件，包括登录成功（级别为INFORMATIONAL）和登录失败（级别为WARNING）。 • **资产访问**，表示发送资产访问的事件。请参考配置规则模板配置资产访问的事件级别。 • **命令防火墙**：表示用户执行了高危命令中动作除了**允许**之外的命令，包括拒绝、终止会话、需复核、通知和全局禁止。对于需复核的命令，复核人执行复核操作后才会发送日志。 • **会话复核**：表示用户执行了需要复核的会话。会话复核的级别和标题在**工作台** > **高危操作** > **设置** > **会话复核**中配置。配置了复核的会话一启动，RIS就会发送日志。

参数	说明
	• **字符审计日志**：表示用户通过访问字符会话执行操作的事件，事件级别为INFORMATIONAL。 • **系统负载告警**：当RIS的系统资源占用率连续超过了系统内置的阈值时，发送告警日志。 事件级别：在**只发送级别不低于X的事件消息**中选择需要发送的事件级别，只有和所选级别相同或者更高的事件才会发送。如果选择NONE表示不发送。 事件级别由低到高依次为：NONE （不发送告警事件）—>DEBUG（调试级）—>INFORMATIONAL（通知级）—>NOTICE（注意级）—>WARNING（告警级）—>ERROR（错误级）—>CRITICAL（临界级）—>ALERT（警戒级）—>EMERGENCY（致命级）。
syslog日志发送对象	配置Syslog服务器： • **远程主机**，Syslog服务器IP地址，默认端口为514，自定义端口可在ip地址后加“:端口号”，例如“10.10.16.201:8022”。 • **syslog机制**，设置Syslog消息的Facility值，用于指定Syslog服务的日志保存路径并对日志进行分类，与Syslog服务器上的实际设置保持一致。 • **标识**，用于配置Syslog的identifier，可以是任意字符，长度不超过30。建议配置为RIS或者您对RIS的其它称谓。

说明： 各种告警事件日志的样例如下：

- 身份验证：

```
Dec 27 18:20:13 node01 node1: login(WEB)(INFORMATIONAL)(service=native,identity=admin,from=10.10.67.15,login authorize
 success)
```

- 资产访问：

```
Dec 27 18:24:24 node01 node1: access(INFORMATIONAL)(id=S0IAIA8C8X3QZV,service=tui
 login,server=CentOS(10.10.33.30),account=root,identity=admin(admin),from=10.10.67.15)
```

- 命令防火墙：

```
Dec 27 18:36:39 node01 node1: cmd(NOTICE)
(id=S0R9ADXQE020K7,service=cmdcheck,action=confirm(pass),server=CentOS(10.10.33.30),account=root,identity=test(test),from=10.10.67.15,
 -a)
```

- 会话复核：

```
Dec 27 15:58:04 node01 node01: session(WARNING)
(id=S2TGD1JJY69K4P,service=sessionReview,server=CentOS(10.10.33.30),account=root,identity=test(test),from=10.10.67.15,authorizer=admin,w
 for reviewing)
```

- 字符审计日志：

```
Jun 27 14:33:42 node01 node01: TUILOG(INFORMATIONAL)
(id=S0E56FWNPTLV66,service=tuilog,server=10.10.33.30(CentOS7),account=root,identity=admin(admin),from=10.10.66.190,action=allow,comm
```

配置邮件告警

1. 选择**系统设置** > **系统** > **基本设置** > **告警事件**。
2. 设置各参数，完成后单击**确定**。

参数	说明
通知邮件事件来源	配置需要通过邮件发送的事件类型和最低发送级别。 事件来源： • **身份验证**：表示用户登录RIS的事件，包括登录成功（级别为Informational）和登录失败（级别为Warning）。 • **资产访问**，表示发送资产访问的事件。请参考配置规则模板配置资产访问的事件级别。 • **命令防火墙**：表示用户执行了高危命令中动作除了**允许**之外的命令，包括拒绝、终止会话、需复核、通知和全局禁止。对于需复核的命令，复核人执行复核操作后才会发送邮件。 • **会话复核**：表示用户执行了需要复核的会话。会话复核的级别和标题在**工作台** > **高危操作** > **设置** > **会话复核**中配置。配置了复核的会话一启动，RIS就会发送邮件。 事件级别：在**只发送级别不低于X的事件消息**中选择需要发送的事件级别，只有和所选级别相同或者更高的事件才会发送。如果选择NONE表示不发送。 事件级别由低到高依次为：NONE （不发送告警事件）—>DEBUG（调试级）—>INFORMATIONAL（通知级）—>NOTICE（注意级）—>WARNING（告警级）—>ERROR（错误级）—>CRITICAL（临界级）—>ALERT（警戒级）—>EMERGENCY（致命级）。
通知邮件收件人	配置收件人，支持同时三种类型的收件人： • **选择收件人**，单击后可以选择RIS中配置了工作邮箱的用户帐号，邮件将发生给对应帐号的邮件地址。 • **添加邮箱**，单击后可以直接输入邮箱地址，仅允许设置一个邮箱地址。 • **事件触发者**，向事件触发者用户帐号在RIS中配置的工作邮箱发送告警邮件（如果没有配置工作邮箱则不发送）。

参数	说明
	说明：您可以参考配置配置用户（手工创建）用户帐号的邮箱。

基本设置：配置短信网关和发送通知短信的功能

RIS支持与用户的HTTP短信网关对接，同时也支持和阿里云短信网关、腾讯云短信网关对接，只能同时启用一个短信网关。配置短信网关后，可以使用RIS的短信通知和短信认证功能。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **短信配置**。
3. 根据实际情况选择对接的短信网关类型，单击**状态**对应的**启用**。
4. 设置各参数，完成后单击**确定**。

- HTTP短信网关填写以下参数：

参数	说明
URL	HTTP短信网关的URL，必须为标准的HTTP或者HTTPS地址。例如**http://1.1.1.1:8082**。
API参数	RIS发送短信内容使用的API参数，格式为**arg=value**，多个API参数使用“**,**”进行分隔。例如**mobile=<%mobile%>,content=<%content%>**。 **说明：**RIS的**value**支持**mobile**和**content**，分别表示手机号码和消息内容。 请参考HTTP短信网关厂家的API文档设置API参数。
字符编码	RIS发送短信内容使用的字符编码，取值包括：**GBK**、**UTF-8**和**ASCII**，缺省值为**UTF-8**。请与HTTP短信网关的设置保持一致。
发送方式	RIS发送短信内容使用的方式，取值包括**POST**和**GET**，缺省值为**GET**。

- 阿里云短信网关填写以下参数：

参数	说明
签名	阿里云文本短信的**签名管理**界面添加的签名对应的签名名称。例如****公司。****替换为实际显示的内容，下同。
密钥ID	阿里云**AccessKey**界面创建的AccessKey对应的AccessKey ID。例如LTAIraSv********。
密钥	阿里云**AccessKey**界面创建的AccessKey对应的Access Key Secret。例如eAA44h****……。

参数	说明
模板ID	阿里云文本短信的**模板管理**界面添加的模板对应的模板CODE。例如SMS_146******。
模板参数	格式为格式为**arg=value**，多个API参数使用“**,**”进行分隔。例如**mobile=<%mobile%>,content=<%content%>**。请参考阿里云短信服务文档的**模板变量规范**填写变量。

- 腾讯云短信网关填写以下参数：

参数	说明
签名	腾讯云短信内容配置的**短信签名**界面创建的签名对应签名内容。例如**公司。
AppID	腾讯云短信的**应用配置**界面显示的SDK AppID。例如：140016****。
AppKey	腾讯云短信的**应用配置**界面显示的App Key。例如：8794afd****……。
模板ID	腾讯云短信内容配置的**短信正文**界面创建的正文模板对应的模板ID。例如231***。
模板参数	格式为格式为**arg=value**，多个API参数使用“**,**”进行分隔。例如**mobile=<%mobile%>,content=<%content%>**。请参考腾讯云文档平台的短信文档填写变量。

5. 单击**测试**，设置**手机号码**和**测试内容**，然后单击**确定**。如果能接收到短信，说明配置正确；如果不能，请排查解决。
6. 选择需要发送短信通知的功能特性。

参数	说明
会话复核	配置会话复核后，当操作用户访问资产时，复核人会收到短信通知。短信的主要内容为：哪个操作员使用哪个帐号启动哪个资产的会话，需要您进行复核。
命令复核	配置高危命令后，当操作在资产上执行定义的高危命令时，复核人会收到短信通知。短信的主要内容为：哪个操作员使用哪个帐号在哪个资上执行哪个命令，需要您进行复核。
系统告警	选中**系统告警**，单击**选择通知人**，选择接收通知短信的用户（如果用户数量大，请输入帐号、姓名等属性进行筛选），完成后单击**确定**。

参数	说明
	系统异常或者服务状态异常时（例如磁盘占用率超过80%或者某个服务已停止），RIS会在Web界面最上方显示告警信息（红底）。启用发送通知短信功能后，通知人就能收到系统告警通知短信。

7. 单击**确定**。

相关任务

登录认证：配置短信认证

基本设置：备份系统配置

配置备份可以对RIS的配置进行导出和导入。导出系统配置支持手动备份和定期备份。

配置备份仅备份数据库和必要的配置文件配置信息，不包含：

- 审计数据
- 网络配置，比如RIS的IP地址。

手动备份

1. 选择**系统设置** > **系统** > **基本设置** > **配置备份**。
2. 单击**下载配置**。

配置文件将下载到本地。

可以单击**管理备份文件**，当次下载的配置将显示为**备份类型**为**手动备份**的一条记录。可以对该次配置执行**还原**、**删除**或**下载**。

定期备份

配置定期备份，需要先配置文件服务器。

1. 选择**系统设置** > **系统** > **基本设置** > **配置备份**。
2. 设置定期备份的时间，精确到分钟。RIS将在每天的指定时间进行备份，备份前一天的数据。
3. 勾选备份文件上传的文件服务器，至少勾选一个。
4. 单击**保存**，使定期备份生效。

定期备份被执行后，备份文件将上传到文件服务器的/configurationBackup路径下。

可以单击**管理备份文件**，当次执行的定期备份将显示为**备份类型**为**自动备份**的一条记录。可以对该次配置执行**还原**、**删除**或**下载**。

导入配置

说明: HA部署时不能导入配置。

1. 选择**系统设置** > **系统** > **基本设置** > **配置备份**。
2. 单击**配置备份**后的**浏览**按钮，选中待导入的配置文件。
3. 单击**确定**导入配置文件。

将覆盖当前系统的所有配置数据，导入后会自动重启服务器，Web服务将暂时不可用。

基本设置：配置logo

设置RIS的Web登录界面的logo和Web页面左上角的logo。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **设置logo**。
3. 分别单击**登录页logo**和**导航页logo**对应的**浏览**，从本地选择logo图片上传，完成后单击**确定**。

参数	说明
登录页logo	RIS的Web登录页面显示的logo。建议图片大小不超过**74 * 125**。
导航页logo	RIS的Web页面左上角显示的logo。建议图片大小不超过**115 * 32**。

如果需要重新设置logo，重复执行本步骤即可。

说明: 建议使用透明背景的logo。

设置完成后，RIS的Web界面左上角的导航logo会变成新上传的图片；退出Web界面，可以看到Web界面的登录logo变成新上传的图片。

4. 可选： 如果需要将logo恢复成出厂设置，单击**恢复出厂设置**。

基本设置：修改服务端口

修改RIS对外开放的服务的端口号。

说明:

- 修改服务端口时RIS会自动重启对应的服务，重启期间服务不可用，已经连接的会话会中断。
- 如果运维人员PC和RIS之间部署了防火墙，修改RIS的服务端口后请对应修改防火墙策略。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **端口配置**。
3. 修改服务端口并单击对应的**确定**。

参数	说明
字符服务	RIS的字符服务（SSH服务）端口号，缺省值为22。修改后通过SSH登录RIS时请使用自定义的端口。
图形服务（RDP）	RIS的图形服务（RDP服务，通过Mstsc客户端连接）端口号，缺省值为3389。修改后通过RDP登录RIS时请使用自定义的端口。
图形服务（Web方式）	RIS的图形服务（Web服务，通过Java客户端连接）端口号，缺省值为5899。修改后使用Web方式建立图形会话或者查看图形会话回放时将使用自定义的端口。

参数	说明
应用发布服务	RIS访问的应用发布服务器的端口号，缺省值为3389。如果应用发布服务器对外开放的端口不是3389，请修改此处，确保RIS访问的应用发布服务器的端口号是正确的。
Web服务	RIS的Web服务（HTTPS服务）端口号，缺省值为443。修改后登录RIS Web界面时请使用自定义的端口。

基本设置：修改配置文件

修改RIS的配置文件，包括**shterm.conf**和**xrdp.ini**。

警告： 配置文件修改不当会导致系统异常，请务必在技术支持人员的指导下修改配置文件。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **配置文件**。
3. 选择**shterm.conf**或者**xrdp.ini**，修改配置文件的内容，完成后单击**保存**。

   修改**shterm.conf**后，需要管理员手工重启RIS才生效，RIS采用HA部署时，需要手工重启所有节点；修改**xrdp.ini**后，RIS会自动重启对应的服务，重启期间服务不可用。

   说明： 单击**加载**，可以将配置文件恢复到最近一次保存的内容。

基本设置：配置其他系统基本参数

其他系统参数包含管理员联系方式、操作员默认首页等全局配置参数。

配置系统Web界面语言

配置RIS的Web界面缺省使用的语言，支持中文和英文。

说明： 此处用于配置系统的缺省语言，是如果要配置用户个人的缺省语言，请参见修改语言设置。

1. 选择**系统设置** > **系统** > **基本设置** > **其他**。
2. 在**系统缺省语言**选择**中文**或者**英文**，完成后单击**确定**。

配置完成后，当前用户再次登录RIS的Web界面时配置生效。

配置管理员联系方式

配置管理员联系方式，可以让RIS操作员在遇到问题时快速的找到管理员。

1. 选择**系统设置** > **系统** > **基本设置** > **其他**。
2. 设置各参数，完成后单击**确定**。

参数	说明
系统管理员	系统管理员姓名或者称呼，允许任意字符，不超过30位。

参数	说明
联系方式	系统管理员的联系方式，可以是电话、邮箱、IM等，允许任意字符，不超过64位。

配置完成后在RIS的Web登录页面单击**登录遇到问题**可以查看系统管理员联系方式。

配置操作员默认首页

根据操作员需求配置正确的默认首页可以有效的提高操作员的效率。

1. 选择**系统设置** > **系统** > **基本设置** > **其他**。
2. 选择操作员默认展示页面。
   - **控制台**，操作员登录后默认进入RIS的控制台。
   - **资产访问**，操作员登录后直接进入资产访问页面。

配置SNMP

RIS支持通过SNMPv1和SNMPv2c被网管管理，常用的MIB节点如表 32: 常用MIB节点所示。

表 32: 常用MIB节点

指标	OID	请求方式
系统描述	1.3.6.1.2.1.1.1.0	get
设备OID	1.3.6.1.2.1.1.2.0	get
SNMP守护程序的正常运行时长	1.3.6.1.2.1.1.3.0	get
网络接口个数	1.3.6.1.2.1.2.1.0	get
网络接口信息	1.3.6.1.2.1.2.2.1.2	walk
接口接收的总字节数	1.3.6.1.2.1.2.2.1.10	walk
接口接收的单播报文个数	1.3.6.1.2.1.2.2.1.11	walk
接口入方向丢弃的报文个数	1.3.6.1.2.1.2.2.1.13	walk
接口发送的总字节数	1.3.6.1.2.1.2.2.1.16	walk
接口发送的单播报文个数	1.3.6.1.2.1.2.2.1.17	walk
接口出方向丢弃的报文个数	1.3.6.1.2.1.2.2.1.19	walk
系统正常运行时长	1.3.6.1.2.1.25.1.1.0	get
内存总大小	1.3.6.1.4.1.2021.4.5.0	get
内存利用率（已使用的内存大小除以内存总大小）	1.3.6.1.4.1.2021.4.6.0	get
CPU利用率（空闲率）	1.3.6.1.4.1.2021.11.11.0	get

1. 选择**系统设置** > **系统** > **基本设置** > **其他**。
2. 选中**SNMP配置**中**SNMP**对应的**开启**。

   开启SNMP后，RIS会打开UDP 161端口，如果网管和RIS之间部署了防火墙，请添加防火墙策略允许网管访问RIS的UDP 161端口。

3. 设置各参数，完成后单击**确定**。

参数	说明
SNMP读团体字	RIS与网管之间使用团体字认证，缺省值为**public**。网管侧的读团体字必须与RIS的读团体字保持一致，如果不一致网管侧访问RIS将会失败。
白名单IP	允许管理RIS的网管IPv4地址，可以配置多个（一次输入一个，输入多次）。该项必须配置，如果不配置，则任何网管都不能管理RIS。

配置HTTP Host 头攻击防护

为了保证RIS不存在HTTP Host头攻击风险，管理员可以启用HTTP Host 头攻击防护，并设置HTTP Host 头白名单。配置后，当用户访问RIS的Web界面时，将会检查用户访问请求中的Host头是否匹配白名单中的域名或IP，只有匹配成功时才能够访问Web界面。

RIS一般需要将业务网口的IP添加到白名单中；如果是HA部署，且需要使用虚IP和各节点的实IP访问Web界面，则将这些IP都添加到白名单中；如果是集群部署，且需要使用外部虚IP和各节点的实IP访问Web界面，则将这些IP都添加到白名单中。如果做了域名的映射，需要将所有域名都添加到白名单中。

1. 选择**系统设置** > **系统** > **基本设置** > **其他**。
2. 选择**启用**。
3. 设置**HTTP Host头**的白名单取值。

   说明:

   - 如需配置IPv6地址，具体的地址需要加上中括号，例如[fc00:1010:32::1]。
   - 域名可以使用模糊匹配或使用正则表达式，例如*.example.org、~^www\d+\.example\.net$。
   - 如需配置为网段，必须使用模糊匹配或正则表达式，例如10.10.10.0/24网段，写成10.10.10.*。对于IPv6网段，只能使用正则表达式，正则表达式不加中括号，并将:用.代替，例如fc00:1010:32::/64网段，写成~.*.fc00.1010.32.0.*。
   - 多个IP或域名之间用空格进行分隔。
4. 单击**确定**保存白名单配置。
5. 单击**重启Nginx服务**，重启Nginx，使配置生效。

   注意: 重启Nginx服务前，请仔细检查配置是否正确，白名单中已包含了RIS的IP和域名，否则重启后将无法访问Web界面并修改配置。

重启Nginx服务后，白名单配置将生效，如访问RIS时的HTTP Host头不匹配，浏览器将返回403错误。
如因配置错误导致Web界面无法访问，请在Console控制台中重新配置Host头防护。

配置部门

RIS支持用户设置不同的部门属性，并根据设置的部门实现部门分权。

部门分权的详细指导请参考《RIS部门分权典型配置指南》，本节仅介绍**部门管理**界面的配置。

1. 单击右上角的用户姓名（例如admin），选择**系统设置** > **系统** > **部门管理**。
2. 单击根部门对应的**新建**，填写部门**名称**并单击**保存**，增加一个子部门。
3. 重复2，直到完成所有部门的添加。
4. 可选： 如需修改已配置的部门名称，单击**编辑**，输入新的名称并单击**保存**。例如可以对根部门ROOT的名称进行修改。
5. 可选： 如某个部门配置多余，可以单击**删除**，并单击**确定**，删除该部门。

   说明: 删除某个部门，必须保证该部门名下没有关联的用户、资产、子部门或其他配置。请先删除相关配置或将相关配置所属部门修改为其他部门，再进行部门删除。

   完成所有部门的添加后，超级管理员需要为每个部门设置对应的管理员，包括配置管理员、审计管理员。请在各部门中新建相应角色的用户或修改已存在用户的部门属性，并完成资产和权限的部门属性的配置。

   部门管理页面将显示每个部门对应的各种管理员的数量，单击数字之后，可以看到对应管理员的详情。

配置HA

RIS支持主备模式的HA。

- 已配置两台RIS的主机名，且主机名不相同。如何配置主机名请参见配置主机名。
- 已按规划配置两台RIS的IP地址（接口eth0和eth1）。如何配置IP地址请参见基本设置：配置网络参数。

为了提高可靠性，可以部署两台RIS组成双机热备。两个节点之间可以连接心跳线，检测与对端连通性，从而减少脑裂的发生。HA中的所有IP，包括虚IP、ping检测地址、主备节点的业务IP、心跳IP，都必须配置为同一格式，即同为IPv4或同为IPv6。

如IP配置为IPv4格式，心跳地址为可选配置，如IP配置为IPv6格式，心跳地址为必选配置。

连接心跳线的HA组网如图 8: HA组网所示。

图 8: HA组网

一般情况下，业务流量只经过节点1（称为主节点），节点1将数据及时备份至节点2（称为备节点）。当节点1发生故障时，进行主从切换，由节点2来处理业务流量，从而确保业务的连续性。

配置HA前，请确保两个节点的软、硬件环境保持一致。HA配置成功后，数据会从主节点同步至备节点。同步的数据包括：

- 数据库
- 配置文件
- ElasticSearch
- 审计数据

主节点会定时进行故障检测，如果主节点发生故障，就会进行主从切换，确保业务的连续性。故障检测包括：

- 网络故障检测：通过ping对端节点和网关IP地址检测网络的连通性。
- 服务检测：检测主节点的**elasticsearch**、**rabbitmq-server**等服务是否正常，如果不正常会尝试重启，连续3次启动不成功就认为主节点发生故障。

请根据实际情况规划HA的数据，本文以下表为例配置HA。

项目	**节点1**	**节点2**	**说明**
主机名	node01	node02	两个节点的主机名不能一样。
IP地址（业务口）	eth0: 10.10.33.6/20	eth0: 10.10.33.7/20	业务口的IP地址，必须在同一个网段。建议两个节点的业务口连接同一个交换机。

以下操作请在**node01**上执行。

1. 选择**系统** > **集群管理**，单击**创建集群**。
2. 选中**高可用模式**，单击**下一步**。
3. 设置集群参数，完成后单击**下一步**。

参数	**说明**
虚IP	虚IP，与业务口的IP地址在同一个网段。HA配置完成后，用户必须通过虚IP访问RIS。
虚IP绑定网卡	虚IP绑定的网卡，即主节点业务口所在的网卡。
ping检测地址	检测网络连通性使用的目的IP地址，建议配置为主节点业务口IP地址的网关。

4. 设置主节点参数，完成后单击**下一步**。

参数	**说明**
网口	主节点的业务口，不可配置。
IP地址	主节点业务口的IP地址，不可配置。

参数	说明
子网掩码	主节点业务口IP地址的掩码，不可配置。
心跳地址	主节点心跳口的IP地址。主节点和备节点的心跳地址必须在同一个网段，且与业务口IP地址不再同一个网段。建议两个节点的心跳口直接相连。 业务网口如使用IPv6地址则必配，如使用IPv4则选配。格式必须与业务网口地址格式一致。

5. 设置备节点参数，完成后单击**下一步**。

参数	说明
IP地址	备节点的业务口IP地址。
用户名	配置过程中主节点访问备节点Web界面时使用的用户名，必须为超级管理员。该数据仅在配置过程中需要，HA配置成功后不再需要。
密码	用户名对应的密码。
心跳地址	备节点心跳口的IP地址。

6. 确认HA相关信息，无误后单击**部署**。

   部署完成后，RIS会提示重启主、备节点的服务。

7. 使用虚IP登录Web界面，进入集群管理页面，查看集群状态，可以看到**node01**是主。

   说明: 配置完集群后，请使用虚IP登录Web界面，而不是主备节点的实IP。当使用备节点的实IP访问Web界面时，会提示不能登录。

8. 单击**node01**对应的**主从切换**，进行主从切换测试。

   说明: 配置完HA后，请执行主从切换测试，确保HA配置的正确性。

   切换完成后，使用虚IP登录Web界面，进入集群管理页面，查看集群状态，可以看到**node02**是主。

- 如果需要升级软件或者安装补丁，请先在**系统状态**界面启用维护模式，然后分别升级主、备节点，完成后关闭维护模式。
- 如果需要拆除HA配置，请在**集群管理**界面单击**拆除HA**按钮拆除HA，也可以登录Console控制台并拆除HA。

配置共享登录

RIS支持SimpleSSO，即用户在一套RIS上登录后就可以自由切换到其他相互信任的RIS上。

如果部署了多套RIS（不管是单机部署，还是HA，都是一套），可以将多套RIS组成一个SSO群。用户登录到一套RIS环境后，可以快速切换到其他RIS环境，即RIS支持SimpleSSO。

用户能成功切换的唯一依据是帐号相同。例如**node01**上的用户**user01**要切换到**node02**上，只要**node02**上存在同名帐号**user01**（状态是活动的），用户就能成功切换，与用户的认证方式无关（注意如果用户设置了验证X.509证书，切换时需要选择正确的证书）。切换成功后，用户直接进入目标节点的Web界面。

共享登录有**站点之间网络互通**和**站点之间网络隔离**这两种方案。这两种方案完全互斥，请用户根据自己的实际使用场景决定使用哪种方案，并参看对应的配置指导。如站点之间网络，部分互通部分隔离，则无法使用共享登录。

共享登录功能具有以下限制：

- 只有超级管理员和拥有系统设置权限的自定义角色用户能够配置该功能。
- 不支持使用IPv6地址跳转。
- 如果跳转登录前后客户端使用的IP地址不同，请在shterm.conf中添加sso.client.ignore=true，忽略对客户端的校验。
- 跳转后访问资产时不支持self代填。

配置共享登录（站点之间网络互通）

使用该方案必须满足以下条件：

- 所有站点之间的网络全部可达。
- 本地PC和所有站点之间的网络可达。

在需要设置共享登录的每一个站点，都执行以下操作。其中，HA在任意节点执行以下操作，将会自动同步配置。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **配置文件**。
3. 选择**shterm.conf**，在shterm.conf中添加以下参数，后，单击**保存**。

参数	**说明**
shared.login	是否开启共享登录功能。true是开启，false是关闭，缺省值为false。示例：shared.login=true。
share.key	共享密钥。需要相互跳转的站点之间必须配置相同的共享密钥，可以为最长50位的字符串。示例：share.key=b1e0e2db-c3f2-4a3a-a180-a0110a1885c9。
sso.shareKey.timeout	使用共享密钥生成的TOTP密码的有效时间。可选参数。单位为秒，缺省值为60。 **说明：**各站点的时间一致（相差60秒内）才能跳转成功。如果相差大，请修改系统时间，或者修改该参数。

示例如下：

```
shared.login=true
share.key=b1e0e2db-c3f2-4a3a-a180-a0110a1885c9
sso.shareKey.timeout=60
```

说明：修改**shterm.conf**后，需要管理员手工重启RIS才生效，RIS采用HA部署时，需要手工重启所有节点。

4. 选择**系统设置** > **系统** > **共享登录**。
5. 选择**启用**，启用共享登录。
6. 单击**添加**，将所有其他站点都添加进来。设置跳转站点的各参数后，单击**保存**。

参数	说明
节点名称	跳转站点的名称，在跳转时用于识别跳转到哪个节点。支持中英文。
访问IP	跳转站点的IP地址，HA部署时请填写VIP。如果使用非缺省的443端口访问，格式为IP:端口号。
管理IP	可选参数。如果当前站点和跳转站点之间存在NAT设备，请在此配置跳转站点NAT后的地址。
用户名	跳转的用户名，该用户角色必须为超级管理员，状态为活动。

7. 单击**确定**。

配置完成后，将可以在以下两个地方使用共享登录：

- 登录RIS时，Web登录界面会出现站点切换下拉框（下拉框中包含当前站点和其他站点），用户可以选择登录到哪个节点（帐号、密码要与登录的节点对应）。
- 登录RIS后，Web界面右上角都会出现站点切换下拉框（下拉框中不包含当前站点），单击目标站点后用户即可完成自动跳转。

如需停止使用共享登录，请在**系统设置** > **系统** > **共享登录**界面选择**禁用**并单击确定。禁用之后所有的跳转站点配置将被清空。

配置共享登录（站点之间网络隔离）

使用该方案必须满足以下条件：

- 所有站点之间的网络都完全隔离。
- 本地PC和所有站点之间的网络可达。

当站点之间的网络完全隔离时，不能直接通过共享密钥进行互相跳转，因此需要使用本方案，用户在跳转时从当前站点获取共享密钥并在跳转站点上进行登录验证。

该方案的所有配置都是在shterm.conf中进行设置。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统** > **基本设置** > **配置文件**。
3. 选择**shterm.conf**，在shterm.conf中添加以下参数，后，单击**保存**。

参数	说明
closed.sso.enable	是否开启共享登录功能。true是开启，false是关闭，缺省值为false。示例：closed.sso.enable=true。
closed.sso.site.addr	跳转站点的IP地址，HA部署时请填写虚IP。多个站点间请以英文逗号分隔。
closed.sso.site.name	跳转站点的名称，在跳转时用于识别跳转到哪个节点。支持中英文。多个站点间请以英文逗号分隔，需要和**closed.sso.site.addr**顺序一致。
closed.sso.site.port	跳转站点的端口。多个站点间请以英文逗号分隔，需要和**closed.sso.site.addr**顺序一致。
share.key	共享密钥。需要相互跳转的站点之间必须配置相同的共享密钥，可以为最长50位的字符串。示例：share.key=b1e0e2db-c3f2-4a3a-a180-a0110a1885c9。
sso.shareKey.timeout	使用共享密钥生成的TOTP密码的有效时间。可选参数。单位为秒，缺省值为60。 **说明:** 各站点的时间一致（相差60秒内）才能跳转成功。如果相差大，请修改系统时间，或者修改该参数。

其中一个站点（10.10.33.1）上的配置示例如下：

```
closed.sso.enable=true
closed.sso.site.addr=10.10.33.2,10.10.33.3
closed.sso.site.name=站点2,站点3
closed.sso.site.port=443,443share.key=b1e0e2db-c3f2-4a3a-a180-a0110a1885c9
sso.shareKey.timeout=60
```

说明: 修改**shterm.conf**后，需要管理员手工重启RIS才生效，RIS采用HA部署时，需要手工重启所有节点。

配置完成后，将可以在以下两个地方使用共享登录：

- 登录RIS时，Web登录界面会出现站点切换下拉框（下拉框中包含当前站点和其他站点），用户可以选择登录到哪个节点（帐号、密码要与登录的节点对应）。
- 登录RIS后，Web界面右上角都会出现站点切换下拉框（下拉框中不包含当前站点），单击目标站点后用户即可完成自动跳转。

配置授权文件

通过配置授权文件可以备份或者更新RIS软件授权。

License即“许可证”或“授权”，是供应商与客户对所销售/购买的产品功能、资产等进行授权/被授权的一种合约形式。

购买授权后，请先申请授权文件，然后将授权文件导入RIS。

如部署为HA，只需要对其中一个节点进行授权，并使用该节点进行部署。完成HA部署后再使用同样的方式更新授权，授权将同步到所有节点上。每一个节点的授权数量将单独计算。

如果已经上传过授权需要更新的，请单击**更新授权**。

1. 单击RIS右上角用户帐号**admin**，选择**系统设置**。
2. 选择**系统** > **授权管理**。
3. 在**授权管理**中单击**申请**，然后单击**请下载授权申请文件**，将**lic-XXXXXX.bin**文件保存到本地PC。
4. 将授权申请文件发送给技术支持人员。

   说明: 技术支持人员收到授权申请后，会生成授权文件**license-XXXXXX.tar.gz**文件并发送给申请者。

5. 单击**浏览**，选择原始授权文件（**不要解压缩**），单击**打开**，最后单击**确定**。

升级系统和安装补丁

RIS支持通过Web界面安装**qzp**和**bin**格式的系统升级包和补丁包，实现软件更新。

升级包是指从一个版本升级到另一个版本的软件包；补丁包是指一个版本内解决问题的软件包。升级包安装完成后需要手工重启系统，补丁包安装完成后不需要重启系统。

安装系统升级包和补丁包同时在Web和控制台下支持，请根据不同的部署场景选择安装方式：

- 对于单机，可以任意选择通过Web或者控制台安装。
- 对于**HA**，请先通过VIP登录Web开启维护模式；然后通过实IP登录**主节点**的**控制台**或者**Web**安装补丁；再通过实IP登录**备节点**的**控制台**安装补丁；最后通过VIP登录Web关闭维护模式。如果安装的是升级包需要重启系统，请在关闭维护模式后执行重启操作。

1. 选择**系统设置** > **系统** > **补丁管理**。
2. 单击**安装补丁**。
3. 单击**浏览**，选择要安装的**qzp**或**bin**格式的文件，单击**确定**。

升级操作执行完成后，Web界面上会显示已安装的升级包和补丁包 。

查看系统状态

通过系统状态可以查看当前的基本状态，并进行一些系统管理操作。

RIS系统状态包含各节点下列信息：

- 当前版本
- 系统时间
- 维护模式状态（HA部署时）
- 连续运行时间
- 活跃会话数
- 系统负载
- 内存占用
- CPU占用
- 是否存在故障未启动的服务
- 已停止的服务
- 磁盘空间使用情况
- 进程状态
- 组件版本信息

1. 选择**系统设置** > **系统** > **系统状态**。
2. 您可以进行下列操作：
   - 查看系统状态（HA部署时可以查看其他节点的状态）。
   - 单击**关机**，可以关闭当前节点的RIS。
   - 单击**重启**，可以重启当前节点的RIS。
   - HA部署时单击**设置维护模式**，启用或者关闭维护模式。

     说明:

     维护模式是指停止ping和服务状态检查，维持当前主从关系不变。设置维护模式只能在HA的主节点上执行。

     - HA部署时，如果要升级系统软件或者安装补丁，请先在主节点上开启维护模式，然后执行升级操作，结束后在主节点上关闭维护模式。
   - HA部署时单击**主从切换**，切换HA主备机。
   - 单击**设置sshd外部访问**，可以查看并设置RIS当前是否开启sshd外部访问。开启sshd外部访问表示用户能够通过SSH方式登录RIS的Console控制台。安装部署场景下，完成授权之前默认开启该功能，完成授权后将默认关闭，请根据需要在此处开启。
   - 单机部署时，可以在此处单击**恢复出厂设置**并单击**确定**，将RIS的配置恢复到出厂时的状态。HA场景下不显示此按钮。

     说明: 恢复出厂设置，将清除当前的所有配置信息（包括用户、资产、权限和系统设置）并重启设备。重启过程中，Web服务将不可用。请在恢复出厂设置前务必先备份系统配置。

配置安全证书

要消除访问RIS的Web界面时出现的证书错误提示，管理员需要配置RIS的安全证书。安全证书是RIS和客户端进行通信时所使用的服务器证书。

使用RIS自签名安全证书

如果需要HA部署，请先完成HA相关的配置工作，并保证所有节点在线。

1. 选择**系统设置** > **系统** > **安全证书**。
2. 在**制作HTTPS证书**中设置各参数，完成后单击**确定**。

参数	说明
C	标准国家代号 ，如CN，表示中国，必填，仅支持字母、数字、空格、.-_。
ST	省份，如ZheJiang，表示浙江省，必填，仅支持字母、数字、空格、.-_。
L	城市，如Hangzhou，表示杭州，必填。
O	组织名称，如您的公司英文名，必填。
OU	组织单位，如您部门的英文名，必填。
CN	访问RIS的IP地址或者域名，比如192.168.1.1，请务必和实际地址和域名保持一次。HA部署的填写HA虚地址或者对应的域名。

说明: 如果参数设置有误，可以单击**重置**来一次性清空所有已配置的内容。

3. 提示**该操作将重启WEB服务，确认执行吗?**，如果确认当前状态RIS无人使用可以单击**确定**，否则请单击**取消**。

Web服务重启完成，SSL证书将更新，您可以安装安全证书以消除证书错误提示。

使用用户自己的安全证书

通过知名CA或者自建CA为RIS生成SSL证书。

说明: 用户生成RIS的证书时，**CN**字段必须填写RIS的IP地址或者访问域名。如果RIS采用HA部署，生成证书时需要在SubjectAltNames中填写虚IP、所有实IP及访问域名。

1. 选择**系统设置** > **系统** > **安全证书**。
2. 在**上传用户证书**中设置各参数，完成后单击**确定**。

参数	说明
口令	上传的证书私钥对应的密码(PassPhrase)。如无密码则留空。
上传证书	单击**浏览**，上传pem格式的RIS的服务器证书（扩展名为**crt**）。
上传私钥	单击**浏览**，上传pem格式的RIS的服务器证书对应的私钥（扩展名为**key**）。

说明： 如果证书上传有误，可以直接重新上传证书或者单击**重置**恢复到初始状态。

用户登录RIS的Web界面，证书错误提示不再出现。

说明： 这里假设用户已安装对应的根证书。

定期任务：配置LDAP用户同步

当RIS启用了AD/LDAP身份验证后，可以配置LDAP同步，自动从LDAP中定期导入用户帐号。

要配置LDAP用户同步，请先配置AD认证或者配置LDAP认证且必须使用RIS提供的缺省名称为**AD/LDAP**中配置的的认证服务器。

如果您只需要同步一次，可以参考配置用户（LDAP导入）。如果您需要周期性同步，请按以下方法配置：

1. 选择**系统设置** > **系统** > **定期任务** > **LDAP同步**。
2. 选择**启用**，开启LDAP同步。
3. 配置LDAP相关各参数，完成后单击**测试**。

参数	说明
LDAP地址	RIS将直接读取**系统设置** > **用户** > **登录认证** > **AD/LDAP**中名称为**AD/LDAP**中配置的**服务器地址**。
baseDN	需要同步到RIS的用户DN的范围，例如"dc=mydomain,dc=org"。
objectClass	选择设置LDAP对象类。
memberOf	选择设置用户所属的分组。
过滤条件	设置过滤条件来筛选用户，过滤条件的语法请参考RFC4515。
ldap用户属性关系	设置LDAP属性和RIS中用户帐号属性的对应关系： • **帐号**：设置将LDAP服务器上的什么属性作为RIS的帐号，缺省值为AD中的用户名字段**sAMAccountName**。 **说明：** Open LDAP中用户名对应的字段为**uid**，如果是Open LDAP服务器且仍使用用户名字段作为帐号，此处就要修改为**uid**。 • **姓名**：设置将LDAP服务器上的什么属性作为RIS的姓名，缺省值为**displayName**。 • **工作邮箱**：设置将LDAP服务器上的什么属性作为RIS的工作邮箱，缺省值为**mail**。

4. 设置同步相关参数，完成后单击**确认**。

参数	说明
执行时间	任务的首次执行日期和每次执行时间。

参数	说明
执行间隔	任务的执行周期，支持按天或者按月。超过31天，只支持按月。
入组配置	选择新用户的默认用户组。选填。 **说明：** 关于用户组，可以参考配置用户组。
同步行为	当AD或者LDAP上禁用或者删除用户后，RIS上帐号的处理方式： • **禁用**，禁用RIS上的用户帐号。 • **删除**，删除RIS上的用户帐号。

5. 可选： 单击**立即同步**，可以立即同步。

定期任务：配置审计数据备份

RIS支持对审计数据进行手动和定期备份，手动或定期自动将RIS中的审计数据备份到文件服务器上。

要配置审计数据备份，请先完成配置文件服务。

表 33: 审计数据备份文件说明

文件夹名称	说明
filelog	文件留痕的留痕文件。 **说明：** 早期版本的存储留痕文件的目录名称为**filetranfer**，如果是从早期版本升级上来，该目录中的留痕文件也将会被备份。 RIS当前的**filetransfer**目录中，将仅包含网盘文件，这些文件将不会被备份。
filesesslog_es	文件传输会话ES日志。
dbsesslog_es	数据库会话ES日志。
dbsesslog_detail_es	数据库会话详情ES日志。
guisesslog_guioper_es	图形会话模拟操作ES日志。
guisesslog_guioperdetail_es	图形会话操作模拟操作详情ES日志。
desktopsesslog	桌面会话日志。
desktopsesslog_es	桌面会话ES日志。
desktopsesslog_detail_es	桌面会话详情ES日志。
guisesslog	图形会话日志。
guisesslog_es	图形会话ES日志。
guisesslog_detail_es	图形会话详情ES日志。
sesslog	字符会话日志。
sesslog_es	字符会话ES日志。

文件夹名称	说明
sesslog_detail_es	字符会话详情ES日志。

配置定期备份

1. 选择**系统设置** > **系统** > **定期任务** > **审计数据备份**。
2. 选择**启用**，开启审计数据备份。
3. 配置各参数，完成后单击**确定**。

参数	说明
定期备份	设置每天的备份时间。备份数据的时间范围是上次备份截止时间到当天凌晨0点。
文件服务器一、文件服务器二	选择备份到哪一台文件服务，可以同时选择，选择RIS会同时备份到两台文件服务器。

RIS将按照设定的时间向文件服务器备份审计数据，备份时采用增量备份方式。审计数据将被备份到文件服务器的工作目录下面，名称中包含sesslog的多个文件夹中。

审计日志备份定期任务执行后，**上次执行时间**将显示上次执行清理任务的时间和执行结果（包括失败原因）。

审计数据定期备份如果失败，所有超级管理员都将在右上角收到备份失败提醒。

执行手动备份

1. 选择**系统设置** > **系统** > **定期任务** > **审计数据备份**。
2. 配置各参数，完成后单击**确定**。

参数	说明
手动备份	设置备份起始时间。将该起始时间至今的审计数据备份到文件服务器。
文件服务器一、文件服务器二	选择备份到哪一台文件服务，可以同时选择，选择RIS会同时备份到两台文件服务器。

3. 单击**确定**执行手动备份。

RIS将立即向文件服务器备份审计数据，备份用户指定的时间范围内的审计数据。审计数据将被备份到文件服务器的以下路径：文件服务器工作目录/sesslogbk-manual。

执行手动备份后，**确定**按钮上方将显示上次执行备份任务的时间和执行结果（包括失败原因）。

定期任务：配置审计数据清理

RIS支持每天在指定时间清理N天前的审计日志。

清理的审计日志包括：

- 字符会话、图形会话和数据库会话的操作审计日志。

- 文件传输日志，如果留痕还包括传输的文件。
- 登录日志。
- 配置日志。
- 审计记录。

说明： RIS不清理在线会话的审计日志。

1. 选择**系统设置** > **系统** > **定期任务** > **审计数据清理**。
2. 选择**启用**，开启审计数据清理。
3. 设置定期清理时间（时和分）和天数（清理多少天以前的审计日志），完成后单击**确定**。
   - 假设在2018年9月17日10:00执行清理任务，如果清理1天前的日志，那么清理的是9月17日00:00之前的日志；如果清理2天前的日志，那么清理的是9月16日00:00之前的日志。
   - 清理审计日志时，以会话的开始时间判断审计日志是否符合清理条件。

   说明： 如果要禁用该功能，可以先选中**禁用**，或者单击**重置**，然后单击**确定**。

配置完成后，RIS每天在指定的时间清理N天之前的审计数据。审计日志清理定期任务执行后，**上次执行时间**将显示上次执行清理任务的时间和执行结果（包括失败原因）。审计管理员也可以在**工作台** > **审计** > **事件审计** > **配置日志**中查看到一条日志。

审计数据清理如果失败，所有超级管理员都将在右上角收到清理失败提醒。

配置问题诊断

通过使用问题诊断功能，管理员可以采集RIS的后台服务日志，或进行网络问题诊断。

日志采集

日志级别说明

日志级别由高到低分为：fatal > error > warn > info > debug > trace。

设置一个日志级别后，RIS会记录该日志级别以上的所有级别日志。例如设置info级别，RIS会记录fatal、error、warn、info的日志。RIS所有服务的日志级别默认为info。

日志采集方法

当遇见无法解决的异常问题时，可以采集后台服务的日志，进行异常问题的定位。通过Web页面采集日志，对于HA，使用VIP登录Web界面只能采集主节点的日志，备节点的日志请通过控制台采集。

- 能够复现的异常问题。
  1. 找到异常问题所涉及的服务，调整相应服务的日志级别。
  2. 进行相应操作，复现异常问题。
  3. 采集日志。

4. 将日志级别改回info级别。

- 不能够复现的异常问题。

1. 确定异常问题发生的时间。
2. 输入采集天数范围，该天数范围需要包含异常问题发生时间点。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**系统** > **问题诊断**。
3. 调整相应服务的日志级别，单击**确定**。
4. 进行相应操作，复现异常问题。

   说明: 修改shterm-webapp、shterm-common、shterm-text、shterm-agentmgr四个服务的日志级别，相应日志的产生将在一分钟后生效，请修改日志级别一分钟后进行问题的复现。

5. 输入日志采集的天数，单击**一键采集**。

   说明: 由于采集日志涉及的文件较多，采集时间会较长，请耐心等待。

6. 将采集后得到的tbx加密文件交给齐治科技工程师进行分析。

网络问题诊断

通过网络问题诊断功能，管理员可以进行ping测试、TCP/UDP端口测试、抓包等操作。

- ping：发送ICMP请求包，进行网络测试。
- telnet：使用Telnet协议，进行TCP端口测试。
- nmap：端口探测工具，进行TCP/UDP端口测试。
- tcpdump：抓包工具，进行网络流量抓取。
- traceroute：利用ICMP协议测试数据包从RIS到目的地所经过的路由器或者网关，它主要检查网络连接是否可达，以及分析网络什么地方发生了故障。

RIS基于Linux系统提供以上命令工具，所有命令的使用格式参考Linux下该命令使用规范。

1. 使用超级管理员进入**问题诊断**页面。
2. 选择相应命令工具。
3. 参数部分填写该命令对应的参数。

   说明: ping和traceroute功能，使用IPv6地址时，需要在地址前面加上-6，例如-6 fc00:1010:32::30。

4. 单击**开始**。
5. 查看输出，分析问题。
6. 单击**停止**。

说明： Tcpdump工具产生的输出，可以以文件形式下载到本地查看。单击**停止**后，出现下载按钮。

用户

本节介绍用户管理的基础设置，包括启用AD、LDAP、RADIUS等其他认证方式、调整用户认证和登录相关的参数。

登录认证：配置本地密码参数

本地用户的密码要求包括长度、复杂度、有效期等，配置本地用户的密码时需要满足这些要求。

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** > **本地密码**。
3. 设置各参数，完成后单击**确定**。

参数	说明
最小长度	密码的最小长度，整数形式，取值范围是6~14，缺省值为6。
复杂程度	密码的复杂程度要求。 • 不限 • 包含且仅包含字母和数字。 • 包含且仅包含字母、数字和特殊字符。 • 至少包含大写字母、小写字母、数字、特殊字符四类中的三类。
有效期限	密码的有效期，取值包括：不限、30天、90天、180天、1年，缺省值是不限。
过期处理	密码配置了有效期限，密码过期后的处理方式。 • 过期一周内允许修改密码：密码过期的一周内，用户可以自己修改密码；过期一周后，用户无法登录，只能联系管理员修改密码。 • 仅提醒：仅提醒用户密码过期，不影响登录。
密码相同检查	新密码不能与前面多少个历史密码相同。整数形式，取值范围是1~100，缺省值是5。

登录认证：配置AD认证

RIS支持和AD服务器对接，使用AD服务器来集中完成用户身份认证。RIS支持配置多个AD服务器。

RIS缺省提供一个名称为**AD/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AD认证服务器。本节以新建AD认证服务器为例进行介绍。

说明： LDAP用户同步只能使用RIS缺省提供的认证方式**AD/LDAP**。

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** > **AD/LDAP**。
3. 单击**添加**。
4. 单击**启用**，然后输入认证服务器名称。
5. **服务器类型**选择**微软AD**。
6. 设置服务器基本参数。

参数	说明
服务器地址	AD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**。 • 如果AD服务器存在主、备，输入的IP地址之间使用“,”分隔。
域名	AD服务器的域名，例如**example.com**。

7. 可选： 如果AD服务器要求安全连接，请选中**服务器要求安全连接(SSL)**，设置各参数。

参数	说明
CA	AD服务器的CA证书，单击**浏览**选择文件上传。
CERT	RIS的客户端证书CERT，单击**浏览**选择文件上传。
KEY	RIS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，RIS不对LDAP服务器的证书进行合法性检查；如果不选，RIS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。

8. 可选： 如果希望AD用户能够自动登录RIS，请选中**新用户自动加入系统**，然后选择新用户的角色。

   说明: 当配置了多个AD和LDAP服务器时，RIS会依次在各个选中了**新用户自动加入系统**的AD和LDAP服务器上查找新用户是否存在。RIS首先在缺省的**AD/LDAP**上查找用户，然后再在剩余的AD和LDAP服务器（根据HASH计算检查顺序）上查找，一旦找到就不再继续查找。

   用户可以直接使用AD用户名和密码登录RIS，首次登录时RIS会自动创建同名的用户帐号。
9. 完成后单击**确定**。
10. 单击**测试**，输入AD服务器的用户名和密码，测试连通性。

AD认证配置完成后，管理员在配置用户时，身份验证方式就可以选择已配置的AD认证方式；另外，配置的AD认证方式也能在双因子认证中引用。

登录认证：配置LDAP认证

RIS支持和LDAP服务器对接，使用LDAP服务器来集中完成用户身份认证。RIS支持配置多个LDAP服务器。

RIS缺省提供一个名称为**AD/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。

说明： LDAP用户同步只能使用RIS缺省提供的认证方式**AD/LDAP**。

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** > **AD/LDAP**。
3. 单击**添加**。
4. 单击**启用**，然后输入认证服务器名称。
5. **服务器类型**选择**通用LDAP服务器**。
6. 设置服务器基本参数。

参数	说明
服务器地址	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**。 • 如果LDAP服务器存在主、备，输入的IP地址之间使用“**,**”分隔。
域名	域名，例如**test.com**。
匿名访问	• 如果LDAP服务器允许匿名访问，请选中**是**。 • 如果LDAP服务器不允许匿名访问，请选中**否**，并设置**查询用户DN**和**查询用户密码**。 **说明:** 请在LDAP服务器上使用ldapsearch获取查询用户DN。
BaseDN	登录RIS的用户DN的范围，例如"dc=mydomain,dc=org"。
用户名属性	用户名的属性名称，如**uid**、**cn**等。

7. 可选： 如果LDAP服务器要求安全连接，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	RIS的客户端证书CERT，单击**浏览**选择文件上传。

参数	说明
KEY	RIS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，不对LDAP服务器的证书进行合法性检查；如果不选，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。

8. 可选： 如果希望LDAP用户能够自动登录RIS，请选中**新用户自动加入系统**，然后选择新用户的角色。

   说明: 当配置了多个AD和LDAP服务器时，RIS会依次在各个选中了**新用户自动加入系统**的AD和LDAP服务器上查找新用户是否存在。RIS首先在缺省的**AD/LDAP**上查找用户，然后再在剩余的AD和LDAP服务器（根据HASH计算检查顺序）上查找，一旦找到就不再继续查找。

   用户可以直接使用LDAP用户名和密码登录RIS，首次登录时RIS会自动创建同名的用户帐号。

9. 完成后单击**确定**。

10. 单击**测试**，输入LDAP服务器的用户名和密码，测试连通性。

LDAP认证配置完成后，管理员在配置用户时，身份验证方式就可以选择已配置的LDAP认证方式；另外，配置的LDAP认证方式也能在双因子认证中引用。

登录认证：配置RADIUS认证

RIS支持和RADIUS服务器对接，使用RADIUS服务器来集中完成用户身份认证。

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** > **RADIUS**。
3. 单击**启用**。
4. 设置各参数，完成后单击**确定**。

参数	说明
认证方式	RADIUS服务器要求使用的认证方式，包括PAP和CHAP。 • PAP：采用二次握手机制，认证过程简单，使用明文格式发送认证信息。 • CHAP：采用三次握手机制，认证过程比较复杂，使用密文格式发送认证信息。
服务器地址	RADIUS服务器的IP地址和端口，缺省端口号是1812。 **说明:** • 如果服务器的端口号是缺省的1812，仅输入IP地址即可；如果不是，输入格式为**IP地址:端口号**。 • 如果RADIUS服务器存在主、备，输入的IP地址之间使用“**,**”分隔。
有共享密钥	RADIUS服务器和RIS之间通信的共享密钥。

参数	说明
	说明： 共享密钥可以显示也可以隐藏，请单击对应的**显示密码**、**隐藏密码**按钮。

5. 单击**测试**，输入RADIUS服务器的用户名和密码，测试连通性。

RADIUS认证配置完成后，管理员在配置用户时，身份验证方式就可以选择**RADIUS**；另外，**RADIUS**也能作为一种认证方式在双因子认证中引用。

登录认证：配置动态令牌认证（TOTP）

RIS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。

- 购买动态令牌并获取对应的种子文件。
- 配置RIS系统时间，配置方法请参见基本设置：配置系统时间（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RIS之间保持网络通信，也不需要其他额外的认证服务器。

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码的长度、复杂度等参数，完成后单击确定。

   说明： PIN码使用本地密码的安全性设置，具体配置请参见配置本地密码参数。

4. 添加令牌到RIS上。

   - **手工新建令牌**

     1. 单击**新建**。
     2. 设置各参数，完成后单击**确定**。

     表 34: 动态令牌参数说明

参数	说明
SN	动态令牌的SN，由若干位数字组成，请在动态令牌实体上查看。
KEY	动态令牌的KEY，由若干位数字和字符组成，请在发货附件中查看。KEY和SN一一对应。

   - **批量导入令牌**

     1. 单击**导入**。
     2. 单击**上传文件**，选择从齐治科技接收到的后缀名为tnk的文件。

说明:

- tnk文件的内容有两列，一列是SN，一列是对应的KEY，中间用空格分隔。
- 如果不使用tnk文件导入，可以单击**下载模板**，将Excel格式的模板文件保存到本地PC；然后打开本地模板文件，填写SN和对应的KEY，完成后保存文件；最后单击**上传文件**时选择Excel文件。
- 不需要导入的动态令牌，请直接单击令牌对应的，从列表中删除该令牌。

3. 单击**开始导入**。
4. 单击**下载导入结果**，查看导入的动态令牌。

5. 可选： 同步动态令牌的时钟（单个）。

   如果动态令牌的时钟与RIS不一致，请执行以下操作同步时钟。

   a) 单击令牌对应的**同步**。

   b) 按下动态令牌的按钮，获取第一个动态密码，并填写到**动态密码1**中，在1分钟后再次按下按钮，获取第二个动态密码，并填写到**动态密码2**中，单击**同步**。

   说明: 注意两个动态密码必须是连续的。

6. 可选： 重置动态令牌的时钟（批量）。

   当RIS的系统时间发生变化时，请执行批量同步操作重置所有动态令牌的时钟，确保动态令牌时间和RIS系统时间保持同步。

   a) 单击**批量同步**。

   b) 在**时钟漂移值**中输入**0**，单击**同步**。

   时钟漂移值是指动态令牌和RIS系统时间的时间差，一般情况下请配置为0。

- 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，可以筛选出特定令牌。单击**重置**清空关键字，查看所有令牌。
- 动态令牌配置完成后，新建用户中**身份验证**就可以选择**动态令牌**。

  说明:

  如果使用双因子认证，请先配置双因子认证，并将**认证方式2**选择为动态令牌，新建用户时身份验证选择刚才配置的双因子认证方式。

  用户登录时，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**等按钮后再输入“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”。

登录认证：配置手机令牌认证

RIS支持手机令牌认证，且手机令牌认证必须和其他认证方式结合使用形成双因子认证方式。

动态口令的基本认证原理是认证双方使用同一个共享密钥对时间进行密码算法计算，之后比较计算值是否一致从而进行认证。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。

手机令牌是TOTP在手机客户端上的实现。RIS的手机令牌适用于双因子认证场景，即手机令牌和其他认证方式（例如本地密码、AD、LDAP和RADIUS认证）结合使用。

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** > **手机令牌**。
3. 单击**请配置NTP服务或手工校准服务器时间**，进入**系统时间**配置页面，可以选择手工校准服务器时间，也可以配置NTP服务（**推荐**）。
4. 配置偏移时间窗，完成后单击**确定**。

   配置时间偏移窗：配置允许的手机和RIS之间的时间偏差。整数形式，取值范围是1~30。取值每增加1，时间偏移增加30秒。缺省值是1，表示允许的时间偏移是30秒。

   说明：时间偏移设置的太小，可能会由于网络延迟等原因导致认证失败。时间偏移设置的太大，可能会降低登录认证的安全性。

手机令牌配置完成后，请配置双因子认证，并把**认证方式2**选择为手机令牌。

登录认证：配置短信认证

RIS支持短信认证，短信认证必须和其他认证方式结合使用形成双因子认证方式。

已配置HTTP短信网关。

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** > **短信认证**。
3. 单击**启用**。
4. 设置各参数，完成后单击**确定**。

参数	说明
认证类型	RIS已配置的认证类型，取值为**HTTP**。如果没有配置或者要修改配置，请单击**配置认证信息**。
消息过期时间	认证消息过期时间。整数形式，单位是分钟，取值范围是1~5，缺省值是2。

短信认证配置完成后，就可以使用包含短信认证的双因子认证方式来进行用户认证。请先配置双因子认证，并将**认证方式2**选择为短信认证。然后新建用户，并将**身份验证**选择为刚才配置的双因子认证方式，注意必须配置手机号码。

登录认证：配置双因子认证

RIS支持将两种认证方式结合使用形成双因子认证方式。

用户使用双因子认证方式登录RIS时，密码输入方式有以下两种。缺省情况下，两种密码输入方式都支持。

- 输入第一重密码后按回车或者**登录**等按钮后再输入第二重密码，这是最常见的密码输入方式。
- 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+第二重密码”，如果第二重密码是6位数字，可以直接输入“第一重密码+6位数字的第二重密码”。例如“admin123 admin456”或者“admin123456”。

对于认证方式是双因子的用户，RIS会直接将空格分隔的两个字符串识别成第一重和第二重密码，或者将最后的六位数字识别成第二重密码。这在有些情况下会出现问题，例如用户的第一重密码最后六位正好是数字时，会错误地被识别成第二重密码，导致认证失败。这类情况下，需要禁用输入组合密码功能，请在shterm.conf中将login.ignoreCombinedPassword设置为true（**系统设置** > **系统** > **基本设置** > **配置文件**）。

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** > **双因子**。
3. 单击**新建**。
4. 设置各参数，完成后单击**确定**。

参数	说明
名称	双因子认证的名称，字符串形式，长度范围是1~30个字符。
认证方式1	请选择第一认证方式，包括：本地密码、AD/LDAP、RADIUS。
认证方式2	请选择第二认证方式，包括：AD/LDAP、RADIUS、动态令牌、手机令牌、短信认证、USBKey认证。 **说明:** ：其中手机令牌、短信认证、USBKey认证只能作为双因子认证的认证方式2，不能作为单独的认证方式。

双因子认证配置完成后，管理员在配置用户时，身份验证方式就可以选择已配置的双因子认证方式。

登录认证：配置X.509证书认证

RIS支持通过X.509证书对用户进行身份认证。

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** > **X.509证书认证**。
3. 单击**启用**。
4. 设置各参数，完成后单击**确定**。

参数	说明

用户信息匹配规则	匹配用户证书Subject内容的规则，使用正则表达式表示。
	配置匹配规则时，支持使用RIS上定义的以下变量：
	• {LOGIN_NAME}：用户的帐号
	• {USER_NAME}：用户的姓名
	• {EMAIL}：用户的工作邮箱
	假设用户的个人证书的Subject内容如下：
	`Subject: C=CN, ST=AAA, O=BBB, OU=CCC, CN=user01/emailAddress=user01@test.com`
	RIS读取Subject内容并处理，处理后内容如下（各主题之间用“,”分隔）：
	`emailAddress=user01@test.com,CN=user01,OU=CCC,O=BBB,ST=AAA,C=CN`
	匹配规则示例：
	1. 证书中的**CN**与用户的姓名相同，且**emailAddress**与用户的工作邮箱相同。
	`emailAddress={EMAIL},CN={USER_NAME},.*`
	2. 证书中**CN**与用户的帐号相同，且**OU**为**CCC**。
	`.*CN={LOGIN_NAME},OU=CCC,.*`

受信任根证书	单击**浏览**，上传签发用户证书的根证书（扩展名可以为**pem**、**crt**、**cert**）。
验证深度	证书的验证深度。整数形式，取值范围是1~99，缺省值为1。如果用户证书直接由根证书签发，验证深度为1；如果用户证书由根证书的一级中间证书签发，验证深度为2；以此类推。

启用X.509证书认证后，管理员在新建/修改用户时就可以选择是否验证X.509证书。

说明: 选择了验证X.509证书的用户需要在本地PC导入个人证书。如果验证深度大于1，还需要将所有中间证书导入用户本地PC。

登录认证：配置USB Key认证

USB Key认证，可以作为单独的认证方式，也可以作为双因子认证的第二重认证方式。

配置USB Key认证的前提条件如下：

- 已获取齐治科技提供的USB Key设备。
- 已准备一台有USB 2.0及以上接口的Windows PC，安装了IE 11浏览器。
- 已安装了USB Key设备中的et199auto.exe控件。

- 已安装了**帮助** > **USBKey认证插件** > **下载**中的认证插件，并在IE浏览器中启用了该加载项，设置了允许RIS的IP。

USB Key的登录认证需要安装控件。RIS目前只提供了IE11浏览器的控件，因此超级管理员签发USB Key，也必须使用IE11浏览器。

启用USB Key认证

1. 单击右上角的用户姓名（例如admin），选择**系统设置** > **用户** > **登录认证** > **USBKey认证**。
2. 单击**启用**，并单击**确定**。启用USB Key。

设置用户使用USB Key认证

3. 选择**用户** > **用户管理** > **用户列表**。
4. 新建用户，或编辑已有用户，将**身份验证**设置为USBKey认证或包含USBKey认证的双因子认证。

签发USB Key

5. 将USB Key设备插入本地PC的USB接口中。
6. 重新选择**系统设置** > **用户** > **登录认证** > **USBKey认证**，并单击**签发新USBKey**。
7. 输入相关参数，并单击**确定**。

参数	说明
USBKey序列号	用于在RIS中唯一地标识一个USB Key，仅用于内部管理，可以不使用硬件序列号。例如180101AF02464。
持有人	必须是已存在的用户，且**身份验证**方式为为USBKey认证或包含USBKey认证的双因子认证，并且不存在已签发的USB Key，才能在此下拉选择。例如选择用户usb。
有效期	超过该有效期的USB Key将无法使用。取值范围为1 - 36500。例如取默认值1095。

8. 输入USB Key的密码，并单击**登录**，完成USB Key的签发。

   如无法使用键盘直接输入，请勾选**使用软键盘**，并使用软键盘输入密码。

完成USB Key的签发后，如该USB Key将不再使用，可以单击对应的**吊销**按钮，将该USB Key吊销。吊销后可以单击**重新签发**，将该USB Key的状态再次变成**已签发**。

登录认证：配置登录安全

为提高密码安全性，请设置密码输错多少次会导致RIS锁定IP和帐号以及锁定时长。

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** > **登录安全配置**。
3. 设置各参数，完成后单击**确定**。

参数	说明
密码错误锁定（次）	密码输错多少次时锁定用户，整数形式，取值范围是1~99，缺省值是3。
客户端锁定（次）	在同一个客户端上使用相同或不同帐号登录，密码输错多少次时锁定该客户端的IP地址。整数形式，取值范围是1~99，缺省值是10。
锁定时长（秒）	用户和IP地址的锁定时长，取值范围是1~600，缺省值是60。

配置用户角色权限

RIS缺省提供了多个用户角色并支持自定义用户角色，本节介绍如何查看各角色的授权情况、修改操作员的授权权限以及创建用户角色并授权。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**用户** > **角色权限**。
3. 可选： 单击**+**，设置各参数，完成后单击**保存授权**。

参数	说明
角色名称	用户角色的名称，字符串格式，长度范围是1~30。
角色描述	用户角色的描述。
管理授权	用户角色拥有的对RIS的管理和配置权限，包括：用户、资产、权限、工单和系统设置，选中对应的复选框即可。
服务授权	用户角色拥有的访问RIS服务的权限，包括：访问资产、审计、、高危操作、报表、自动化，选中对应的复选框即可。 **说明:** 管理员如果选中了**审计**，还可以单击左下角的，然后勾选**查看键盘记录**、**下载会话**来进一步设置用户的权限，包括全部勾选、全部不勾选和只勾选**查看键盘记录**。 • 键盘记录是指用户进行的鼠标或键盘的按键操作以及具体的操作命令，对应到审计界面后包括**按键**、**模拟操作**、**剪贴板记录**、**详情**等功能。 • 下载会话是指将会话的记录文件下载到本地计算机。

用户角色配置完成后，管理员在配置用户时，用户角色就可以选择新配置的角色。

4. 可选： 单击**超级管理员**、**配置管理员**等页签查看对应角色的授权情况。
5. 可选： 单击**操作员**，选中或者去选授权，完成后单击**更新授权**。

配置用户属性

配置用户时，如果RIS提供的预定义用户属性不满足需求时，请自定义用户属性。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**用户** > **用户属性**。
3. 单击**新建**，设置各属性，完成后单击**确定**。

参数	说明
名称	用户属性的名称，字符串格式，长度范围是1~30。
类型	用户属性的类型。 • 如果类型选择**字符串**，请设置**长度**，取值范围是1~99。 • 如果类型选择**数字**，请设置**范围**（最小值和最大值），取值为整数（支持正负值）且长度不超过9个字符。 • 如果类型选择**日期**，请设置**范围**（起始和结束日期）。 • 如果类型选择**可选值**，请设置**可选项**的标签（输入字符串后回车即可形成一个标签），每个标签的长度范围是1~25个字符。

用户属性配置完成后，管理员在配置用户时，就可以配置用户的自定义属性。

配置全局用户登录控制

为提高安全性，请设置允许或禁止用户登录RIS的时间、IP地址和MAC地址范围。

警告: 该设置全局生效，即对包括超级管理员在内的所有角色均生效，如果设置不当可能导致所有用户都无法登录，请仔细规划和配置。万一配置错误导致无法登录RIS，请联系齐治科技技术支持处理。

管理员可以配置多条登录控制策略，当有用户登录时，RIS会从上到下匹配，一旦匹配到某条策略就执行对应的动作，不再继续向下匹配。管理员可以通过单击↑和↓来调整策略的优先级。

说明: 如果需要配置单个用户的登录控制参数，请参见修改用户属性。单个用户的优先级高于全局配置。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**用户** > **登录控制**。
3. 单击**新建**，设置各参数，完成后单击**确定**。

参数	说明
时间	登录控制的时间范围，格式如下： • 周：w[1-3,5,7] • 月：m[1,3-5,12]

参数	说明
	• 天：d[1,5,7,31] • 日期：D[20180101,20180101-20180301] • 时间：T[03:30-18:00] 请根据实际需要组合多个范围使用，多个范围之间是交集的关系，即设置的几个范围要同时满足。多个范围请用空格分隔。取值为空时表示不限制。 例如，每周一到周五的8:00至18:00写作**w[1-5] T[08:00-18:00]**
IP地址	登录控制的IP地址范围，格式如下： • 具体地址：192.168.1.10 • 地址段：192.168.1.1-192.168.1.10 • 网段：192.168.1.0/24 请根据实际需要组合多个范围使用，多个范围请用英文逗号“,”分隔，最大长度为1024个字符。 取值为空时表示不限制IP地址。
MAC地址	登录控制的MAC地址范围，要求如下： • 客户端和RIS在同一网段。 • 配置时请输入完整的MAC地址，多个MAC地址使用英文逗号“,”分隔，最大长度为1024个字符。 • 取值为空时表示不限制MAC地址。
条件	包括**满足**、**不满足**和**不启用**。其中不启用表示该登录控制策略不生效。
动作	登录控制的动作，包括**允许**和**禁止**。

配置了登录控制后，RIS会强制不满足登录条件的在线用户下线。

资产

配置资产类型

管理员修改资产类型的属性，新增资产类型。

RIS中内置了常见的资产类型。如果用户设备不在这些资产类型范围内，管理员可以在此增加新的资产类型。

资产类型与新建资产时的默认参数有关，例如指定Linux资产默认使用的字符终端为SSH。管理员可以修改资产类型的参数，以满足新设备被创建时，拥有期望的默认参数的需求。

通过RIS访问的资产主要有两种类型。

- **通过RIS直接访问的资产**

  RIS作为客户端能够通过相关远程协议直接访问目标资产，用户可以通过RIS直接发起到资产的访问。访问的的路径为：**用户PC->RIS->目标资产。**

  例如：支持SSH、Telnet、RDP、VNC、Xdmcp、Xfwd协议的资产。

- **通过应用发布服务器访问的资产**

  有些资产属于Windows下的应用程序，用户通过RIS无法直接访问。如果要访问这类型的资产，需要通过应用发布服务器来访问。访问的路径为：**用户PC->RIS->应用发布服务器->目标资产。**

  例如：Chrome浏览器、Firefox浏览器、Plsqldev客户端、Navicat客户端等。

配置通过RIS直接访问的资产类型

通过RIS直接访问的资产类型存在于RIS主机、网络两个类别中。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置。**
2. 选择**资产** > **资产类型** > **主机/网络。**
3. 单击**新增**，或者**编辑**已存在的资产类型。

图 9: 直接访问的资产类型

参数	说明
名称	输入此资产类型的名称。
分类	选择此资产类型所属的分类，如果没有所属的分类，可以选择编辑新增一个分类。

参数	说明
字符终端	勾选该资产所拥有的协议。当新建该类型的资产后，可以在资产的访问协议中，选择添加这些协议。访问协议配置方法参考配置资产的访问协议。 在下拉框中选择相关协议，以作为该资产创建时的默认添加的字符协议。如果无法选择默认添加协议，请确认其后的相关协议是否勾选。 SSH和Telnet协议的高级属性中，可以修改默认端口。
图形终端	勾选该资产所拥有的协议。当新建该类型的资产后，可以在资产的访问协议中，选择添加这些协议。访问协议配置方法参考配置资产的访问协议。 在下拉框中选择相关协议，以作为该资产创建时的默认添加的图形协议。如果无法选择默认添加协议，请确认其后的相关协议是否勾选。 RDP协议的高级属性中，可以修改默认端口，指定是否默认使用Console模式（Console模式相当于mstsc的/admin或/console选项，表示是否允许普通用户连接终端服务器的控制台会话（session id=0），用于防止终端服务器授权的会话数超过后，用户无法登录目标资产的情况。）。 VNC协议的高级属性中，可以修改默认端口，指定是否默认使用商业版方式。当目标资产是商业版VNC时，需要勾选该项目。 Xdmcp协议的高级属性中，可以修改默认端口，该端口一般为UDP端口。 Xfwd协议的高级属性中，可以修改Xfwd方式启动所调用的程序。
特权帐号	输入该资产类型的特权帐号。指定特权帐号的目的是为了通过RIS执行一些针对目标资产的高权限操作，例如帐号改密等操作。
改密方式	选择该资产类型的改密方式。不同的改密方式代表着不同的改密脚本，改密方式主要用于帐号改密功能。帐号改密，配置方法参考配置改密计划。
编码类型	选择资产类型的编码。该编码主要影响**工作台** > **审计** > **字符会话**中详情页命令和输出的编码。

配置通过应用发布服务器访问的资产类型

通过应用发布服务器访问的资产类型存在于RIS数据库、应用系统两个类别中。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **资产类型** > **数据库/应用系统**。
3. **编辑**已存在的资产类型，勾选该资产类型下的客户端，远程客户端配置参考配置远程客户端。

参数	说明
特权帐号	指定该资产类型的特权帐号。指定特权帐号的目的是为了通过RIS执行一些针对目标资产的高权限操作。
默认客户端	指定该资产类型的默认客户端。该类型资产被创建时的默认添加这个客户端。

配置资产属性

新增资产的属性。

当资产被创建后，可以拥有**资产名称、资产IP、简要说明、资产类型**等系统默认属性，当资产需要拥有新的属性时，管理员可以通过配置**资产属性**方式来完成。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **资产属性**。
3. 单击**新建**。
4. 输入资产属性相应内容。

参数	说明
名称	输入资产属性的名称。
类型	选择资产属性的数据类型。有字符串、数字、日期、可选值四个选项。类型参考表 35: 资产属性类型说明
长度/范围/可选项	根据类型参数的不同，此项目会有不同的样式。可以指定该数据所能设置的范围。

表 35: 资产属性类型说明

类型	说明
字符串	字符可以是任意可显示字符，包括特殊字符，例如：~!@#$%^&*()_+{}|:"<>?~！@#￥%^。
数字	只能是整数数字。
日期	只能是日期格式的数据。
可选值	必须得预定义可选值，可预定义多个可选值。

访问设置

RIS中包含多种的会话访问方式，包括Web页面访问，字符会话访问、图形会话访问、文件传输访问。每种会话访问在启动时，都带有默认参数，例如字符会话的最大持续时间、图形会话启动默认调用的客户端等。管理员可以通过当前菜单，修改会话访问中的默认参数。

配置字符终端参数

修改访问RIS字符会话的默认参数。

ShellMenu

用户使用本地计算机的SSH客户端访问RIS时，RIS会以列表方式列出所有可访问的字符资产，该列表方式被称为ShellMenu。

用户使用字符终端访问RIS有两种形式。

- 使用Web页面，单击相应字符资产，调用本地计算机的SSH客户端。
- 使用本地计算机的SSH客户端访问RIS，在列出的ShellMemu菜单中选择目标资产。

这两种方式启动的字符会话的默认参数，都可以在此处进行修改。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **访问设置** > **字符终端**。
3. 配置字符终端默认参数。

参数	说明
终端字符编码	通过SSH客户端直连RIS时，ShellMenu的编码。 当ShellMenu出现乱码时，修改此项。
初始终端标题	通过RIS访问字符资产时，调用的SSH客户端的标题栏内容。 标题格式中可以包含变量，变量包含在{}中，默认变量：{user}代表登录用户，{account}代表帐号，{hostname}代表服务器名，{hostaddr}代表服务器IP。格式中不支持英文双引号。 RIS调用不同种类的SSH客户端时，因为兼容性问题，效果会存在差异，请以实际效果为准。SecureCRT的支持最为完善。
并发登录限制（个）	RIS所允许的全局最大字符会话数量和单用户所允许的最大字符会话数量。 该参数只对字符会话生效，图形会话、登录测试会话、回放会话、复核会话、会话共享会话都不占用这个限制。当超出最大显示，连接RIS的字符会话，RIS会显示当前登录连接数超出。默认值为0表示不限制。
终端登录提示	通过RIS访问字符会话时，会出现该登录提示。

参数	说明
	如果该内容显示乱码，请修改终端字符编码。
字符会话输入超时	字符会话无输入时间开始算起，超时将退出。 单位：时:分。0:00分表示无超时设置。使用rz、sz方式传输文件过程中不会退出。
最大持续时间	字符会话初始访问时间开始算起，超时将退出。 最长时间阈值为5天23:59分。不可以设置0天0:00。
会话访问方式	在Windows环境下，通过Web页面访问字符会话所调用的SSH客户端。 如需修改个人帐号会话访问方式，请参考修改会话配置。
会话访问方式(Mac)	在Mac环境下，通过WEB页面访问字符会话所调用的SSH客户端。 如需修改个人帐号会话访问方式，请参考修改会话配置。
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：表示不分类 • 资产组 • 资产类型 • 责任人
终端菜单超时退出（秒）	通过SSH客户端直连RIS时，ShellMenu无操作退出的超时时间。 内容为0，表示不自动退出。
切断过夜会话	切断该时间点的字符会话。 对于连接未超过5分钟的字符会话不受影响。 **说明：** 单击左下角的**重置**可以清空切换过夜会话的设置。
命令输出限制	审计中，对记录到ElasticSearch中的命令输出的长度和大小进行限制。字符会话命令输出超出范围时，不进行记录。（只影响**审计** > **操作审计** > **字符会话** > **详情**中的输出，不影响字符会话实时、回放、下载方式时的输出。） 填写输出行数和输出文件大小以进行限制，当输出内容满足以上任何一个条件，就停止记录。输出行数和输出文件大小都不能设置为0。

参数	说明
命令记录限制	审计中，对记录到会话日志文件中的命令输出进行限制。字符会话两次键盘输入之间的输出超出范围时，不进行记录。（只影响字符会话实时、回放、下载方式时的输出，不影响**审计** > **操作审计** > **字符会话** > **详情**中的输出。） 不可以设置为0。

配置图形会话参数
修改访问RIS图形会话的默认参数。

用户访问RIS的图形会话，有两种形式。

- 使用Web页面，单击相应图形资产，访问该资产。
- 使用本地计算机的Mstsc客户端访问RIS，在列出的菜单中选择图形资产。这种方式只适用于RDP方式访问的Windows资产。

这两种方式启动的图形会话的默认参数，都可以在此处进行修改。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **访问设置** > **图形会话**。
3. 配置图形会话默认参数。

参数	说明
初始终端标题	通过RIS访问图形资产时，标题栏的内容。 标题格式中可以包含变量，变量包含在{}中，默认变量：{user}代表登录用户，{account}代表帐号，{hostname}代表服务器名，{hostaddr}代表服务器IP。格式中不支持英文双引号。 通过WEB页面方式启动图形会话时，标题显示在标签页名称中。通过RemoteAPP方式启动的Rdpapp会话不显示标题。
键盘记录开关	审计是否记录图形会话的键盘事件和字符剪切板的记录。 默认选项为记录，如果不记录，**审计** > **操作审计** > **图形会话** > **详情** > **模拟操作/剪切板记录**、**审计** > **操作审计** > **图形会话** > **更多** > **按键**将不产生数据，**审计** > **操作审计** > **图形会话** > **回放**也将不显示键盘记录。
RDP启动方式	通过WEB页面启用的RDP会话，使用的启动方式。 选项Mstsc：从本地计算机打开Mstsc工具调用RDP的方式。如需修改个人帐号RDP启动方式，请参考修改会话配置。

参数	说明
图形会话输入超时	图形会话无操作时间开始算起，超时将退出。 单位：分钟。0表示无超时设置。
最大持续时间	图形会话初始访问时间开始算起，超时将退出。 最长时间阈值为7天23:59分。不可以设置0天0:00。
默认分辨率	通过web页面以Mstsc启用的RDP会话的分辨率。 默认全屏：RDP会话会以全屏的方式显示，如需退出该会话，请将鼠标移动到页面的顶部中间位置，会出现Mstsc的会话操作标题栏，点击X退出。 最大化：RDP会话在当前桌面显示，但是不会遮挡本地计算机的任务栏，方便本地计算机任务切换。此分辨率是RIS的默认初始分辨率，也是推荐使用的分辨率。 如需修改个人帐号的默认分辨率，请参考修改会话配置。
反连地址限制	使用Xdmcp服务时，是否针对所有IP开放Xdmcp协议使用的TCP6000-6009端口。 使用Xdmcp服务时，RIS会打开TCP6000-6009端口，以监听Xdmcp的反向连接，如果向所有IP开放TCP6000-6009端口，会产生安全漏洞。 选项是：XDMCP服务在连接目标资产时，针对目标资产的地址开启防火墙端口。防止非目标资产的反向连接。推荐使用这种方式。 选项否：XDMCP服务在连接目标资产时，不针对目标资产的地址开启防火墙端口。任何目标资产都可以反向连接。
会话切片大小(MB)	审计记录图形会话，会话文件在达到切片大小时，生成下一个切片。 **审计** > **操作审计** > **图形会话** > **详情** > **按大小切片**中可以看到切片文件。
按标题切片	审计记录RDP会话，如果RDP会话的当前活跃窗口的标题发生变化，生成一个切片。 开启该选项后，**审计** > **操作审计** > **图形会话** > **详情**中将出现**按标题切片**的页签。 **说明:** 只支持RDP会话，且**RDP启动方式**为**mstsc**。如果**RDP启动方式**为**web**，**按标题切片**中无内容。
是否开启tls	RIS监听的3389端口是否只允许TLS方式的连接。 该选项变更会重启RDP服务，当前在线RDP会话会被全部断开。

参数	说明
	开启TLS连接，可以规避Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness漏洞。 **说明：** 当开启了tls时，用户通过RDP访问资产时，会收到提示**无法验证此远程计算机的身份，是否仍要连接。**勾选了不再询问后，下次访问时将不再提示。
回放方式	用于控制进行图形审计回放时的回放方式，取值范围如下： • web：在浏览器中播放会话录屏。默认选项。 • java：在JAVA窗口中播放会话录屏。 **说明：** web和java方式的详细区别，请参考播放会话录屏。

配置文件传输参数
修改访问RIS文件传输的默认参数。

通过RIS，用户可以进行多种方式的文件传输。

- 通过RDP协议，以剪贴板上下行方式，进行Windows的文件传输。
- 通过rz/sz工具，进行字符会话下的文件传输。
- 通过SFTP协议，用户使用SFTP客户端直连RIS，进行字符会话下的文件传输。

以上几种方式启动的文件传输会话的默认参数，都可以在此处进行修改。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **访问设置** > **文件传输**。
3. 配置文件传输默认参数。

参数	说明
是否留痕	通过RIS进行文件传输的文件是否在RIS上保留一份副本。 留痕文件可以在**审计** > **操作审计** > **文件传输**中下载。
文件留痕阈值(单位M)	只有小于该阈值的文件会进行文件留痕操作。 此参数留空代表不设限制，所有文件都进行留痕操作。
禁用Zmodem传输	是否允许rz/sz方式，进行字符会话下的文件传输。
会话访问方式	在Windows环境下，通过WEB页面访问文件传输所调用的客户端。 如需修改个人帐号会话访问方式，请参考修改文件传输配置。

参数	说明
会话访问方式(Mac)	在Mac环境下，通过WEB页面访问文件传输所调用的客户端。 如需修改个人帐号会话访问方式，请参考修改文件传输配置。
初始终端标题	通过RIS访问文件传输时，调用客户端的标题栏内容。 标题格式中可以包含变量，变量包含在{}中，默认变量：{user}代表登录用户，{account}代表帐号，{hostname}代表服务器名，{hostaddr}代表服务器IP。 RIS调用不同种类的客户端时，因为兼容性问题，效果会存在差异，请以实际效果为准。Filezilla的支持最为完善。

配置访问通用参数
修改RIS访问的通用参数。

用户可以使用多种方式登录RIS访问目标资产，例如WEB页面，SSH客户端直连等。关于访问通用的默认参数，可以在此处进行修改。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **访问设置** > **所有会话**。
3. 配置默认参数。

参数	说明
默认备注方式	通过RIS访问目标资产时，用户是否需要填写备注信息。 通过Mstsc客户端和SFTP客户端直连RIS的会话不受此参数影响。
WEB超时时间（分）	WEB会话无操作时间开始算起，超时将退出。
会话切断策略	WEB会话退出时，是否切断从WEB页面启动的字符、图形会话。 从WEB页面启动的以WEB方式访问的RDP会话，不受此参数影响，如果WEB会话退出，WEB页面的RDP会话一定会断开。
同一用户帐号同时只允许从一个IP地址访问	只要用户帐号通过当前IP地址登录RIS的会话存在，RIS就不允许该用户帐号从其他IP地址上登录。 所登录的会话类型不光包括WEB会话，还包括TUI和GUI会话。 关于WEB会话的退出，用户需要在页面右上角，单击用户帐号，单击**退出**。如果直接关闭浏览器，并不能直接退出WEB会话。

配置负载限制

注意：一旦开启负载限制，并设定相应限制值，当全局会话或单个会话占用的资源超过限制时，将引起会话状态异常，例如异常断开连接等。请仔细考虑并针对性地设计了相应的限制值后，再开启该功能。

当RIS承载的会话过多而引起CPU或内存占用过高时，超级管理员可以开启负载限制功能，对全局或单会话占用的CPU或内存资源进行限制，在超过限制时自动断开会话。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **访问设置** > **所有会话**。
3. 如需设置全局限制，勾选全局限制对应的会话类型，并填写对应的CPU和内存限制值。

   说明：CPU和内存占用的最大限制取值范围为1~100%，请不要设置得过低，以防止无法建立任何会话。图形会话包括RDP会话和应用系统会话。字符会话不能设置内存占用的限制。

   设置后，当该类型的会话占用负载总和超过该限制时将无法创建新会话，并且旧的会话有可能异常断开。
4. 如需设置单会话限制，勾选单会话限制对应的会话类型，并填写对应的CPU和内存限制值。

   说明：VIP用户是指需要单独设置限制的用户。请单击**VIP用户**对应的**选择用户**，勾选一个或多个用户。字符会话不能设置单会话的负载限制。

   设置后，当某个会话负载超过该限制时将自动切断会话。
5. 确认设置无误后，单击**确定**，设置将立即生效。

远程客户端

应用发布服务器

用户通过RIS，使用SSH、Telnet、RDP、VNC、Xdmcp、Xfwd等远程连接协议，可以直接访问这类型的资产。但是当用户需要基于Windows图形化客户端的工具，访问远程资产（例如：通过Firefox浏览器访问防火墙的网页，通过Navicat工具访问MySQL数据库。）时，是无法通过RIS直接完成的。这时需要一台Windows机器，用户通过RIS登录这台Windows机器，通过其上的客户端，访问目标资产。这台Windows机器被称作应用发布服务器。

远程客户端

被RIS发布出来的应用发布服务器上的客户端，被称为远程客户端。用户可以通过RIS访问这些客户端资产。远程客户端的种类是丰富多彩的，甚至Chrome浏览器也可以被称为一个客户端。远程客户端在应用发布服务器上一定要是可执行的文件。

配置应用发布服务器

为了访问应用系统和数据库资产，RIS需要建立与应用发布服务器的连接。

说明：应用发布服务器的安装、部署和使用，请参见《RIS应用发布典型配置指南》。本文仅介绍RIS上的相关配置。

新建应用发布服务器

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统设置** > **资产** > **远程客户端** > **应用发布服务器**。
3. 单击**新建**，设置各参数，完成后单击**确定**。

参数	说明
地址	应用发布服务器的IP地址。
管理员帐户	应用发布服务器上的管理员帐号。
管理员密码 / 确认密码	管理员帐号对应的密码。

应用发布服务器列表中的**WinSync状态**反映了RIS与该应用发布服务器的连接状态是否良好，当Winsync状态为**正常**时，代表连接正常。

当需要修改应用发布服务器的设置时，单击对应的**编辑**。

说明: 应用发布服务器的**升级**和**批量升级**功能，当前版本暂不可用，请勿使用该功能。

登录应用发布服务器

1. 单击右上角用户帐号（例如admin），选择**系统设置**。
2. 选择**系统设置** > **资产** > **远程客户端** > **应用发布服务器**。
3. 选择应用发布服务器，单击**登录**。
4. 选择**分辨率**，勾选需要映射的磁盘，单击**启动**。

管理内置应用发布服务器

默认应用发布服务器是以KVM虚拟机方式内置在RIS上的，RIS的应用发布服务器页面就是管理员对内置应用发布服务器进行管理的入口。管理员可以进行应用发布服务器登录、开关机、用户帐号同步、快照等管理操作。

1. 使用超级管理员进入**应用发布服务器**页面。
2. 选择应用发布服务器，单击**管理**。
3. 单击**开机**、**关机**，进行物理开关机。单击**创建快照**，创建新的快照。在已存在的快照中单击**恢复快照**、**删除快照**进行快照的恢复和删除操作。

管理用户帐号同步

RIS上的不同用户在访问应用发布服务器时，需要有自己一套独立的环境。RIS默认会在用户在首次使用应用发布服务器时，将该用户的帐号、密码同步到应用发布服务器上，帐号使用用户同名帐号，密码使用RIS随机生成的密码。当用户在访问远程客户端，打开应用发布服务器时，使用同步的帐号进行登录。

1. 单击右上角用户帐号（例如admin），选择**系统设置**。

2. 选择**系统设置** > **资产** > **远程客户端** > **应用发布服务器**。

3. 可选： 单击**同步状态**，设置自动同步选项，完成后单击**确定**。

   自动同步选项包括**同步**和**不同步**，缺省为**同步**。当选择**不同步**时，RIS在用户在首次使用应用发布服务器时，不会将该用户的帐号同步到应用发布服务器上。当有远程客户端需要RIS同名帐号登录，访问会提示帐号登录失败。

4. 可选： 单击**查看帐号**，选择相应帐号后可以执行以下操作。

   - 单击**登录**，使用同步帐号登录应用发布服务器。
   - 单击**删除**，在应用发布服务器上删除该帐号。
   - 单击**重新同步**，重新同步该帐号。

     说明: 当管理员在应用发布服务器上手工修改了用户的密码，RIS由于不知道新密码，会登录失败。这时就需要重新同步帐号，RIS会将用户的帐号密码都重新同步。

配置远程客户端
添加远程客户端、修改远程客户端的启动参数。
请确保RIS与应用发布服务器连接正常。

RemoteAPP

RIS远程客户端调用的一种方式，与普通方式调用的远程客户端相比，RemoteAPP方式中打开的客户端不包含Windows背景，标题栏以应用的标题栏显示而不是远程桌面会话的标题栏显示，更像是本地客户端的打开方式。推荐远程客户端使用RemoteAPP方式。

代填脚本

RIS访问的应用发布资产通常有登录框，需要登录才能进行操作。通过管理员配置代填脚本，RIS可以实现登录框内容的代填，进行登录操作。

管理员需要通过RIS的远程客户端页面，将RIS和远程客户端进行关联。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **远程客户端** > **远程客户端**。
3. 单击**新建**，选择远程客户端的JSON格式文件，新建远程客户端。
4. 选择需要配置的远程客户端，单击**编辑**，设置各参数，完成后单击**确定**。

参数	说明
名称	输入远程客户端的名称。
执行帐号	使用什么帐号登录应用发布服务器。 同用户帐号：以登录RIS的相同帐号登录应用发布服务器。

参数	说明
	手工指定：指定一个帐号，使用当前远程客户端时都通过指定帐号登录。
RemoteAPP	远程客户端是否使用RemoteAPP方式，如果不使用，则通过普通方式打开。
代填脚本	选择代填脚本。
键盘记录开关	审计时是否记录鼠标和键盘事件信息，默认选项为记录。 如果选择**不记录**，**审计** > **操作审计** > **图形会话**中将不产生键盘记录数据。只有当配置图形会话和此处的键盘记录开关全都设置为记录时，才会记录相应会话的按键信息。

配置CS代填脚本

管理员如果希望RIS在登录CS远程客户端时，自动代填登录框内容，可以配置CS代填脚本。不同的CS远程客户端对应着不同的CS代填脚本。

请确保RIS与应用发布服务器连接正常。

1. 使用超级管理员登录RIS。单击右上角的用户帐号，单击**系统设置**。
2. 选择**资产** > **远程客户端** > **CS代填脚本**。
3. 单击代填脚本对应的**编辑**，修改代填脚本的名称、客户端标识和备注，完成后单击**确定**。
4. 单击**新增**，设置各参数，完成后单击**确定**。

参数	说明
文件上传	单击**文件上传**选择录制出的远程客户端登录过程的JSON文件，该文件是通过应用发布服务器的**APP脚本录制器**录制的。
客户端标识	选择相应的远程客户端，可以选择多个。
备注	CS脚本的备注信息。

Console控制台

13

目录:

Console控制台用于管理员完成少量RIS Web界面上不能完成的配置操作。

Console的登录请参考登录RIS的Console。为保障RIS的安全性，管理员登录RIS的Console后只能看到固定的控制台菜单界面并进行相关操作。

配置系统日期和时间（Date and Time）

系统管理员可以使用Console菜单提供的日期和时间工具修改系统时间。

配置系统日期和时间的方式有手动设置和NTP同步两种，请选择其中的一种方式进行配置。配置NTP服务器后请勿再手动修改日期和时间。

集群部署时，只能通过NTP服务器同步系统时间，不能手动设置。

1. 登录RIS的Console。
2. 在主菜单中输入**Date and Time**对应的字符，并按回车，进入**Date and Time**菜单。

```
Date and Time
   1. Date : 2019-07-01
   2. Time : 16:00:05
   3. Network Time Protocol
   0. Return
Enter selection:
```

手动配置系统时间

3. 输入**Date**对应的序号，例如1并按回车，修改系统日期。

   输入修改后的日期，并按回车。

   说明: 如要取消修改，请直接按回车。

如果提示**Ntp server is running, it is not recommeneded to update the clock manually, press enter to continue...**，说明已配置了NTP服务器。此时可以继续手动配置日期和时间，但手动配置后将清空NTP服务器的设置。

4. 输入**Time**对应的序号，例如2并按回车，修改系统时间。

   输入修改后的时间，并按回车。

   说明: 如要取消修改，请直接按回车。

5. 确认手动设置无误后，输入S，执行**Submit**，提交所有修改，使日期/时间设置生效。

```
Date and Time
   1. Date : 2019-07-01 ==> 2019-07-02
   2. Time : 16:15:35 ==> 15:15:15
   3. Network Time Protocol
   S. Submit
   0. Return
Enter selection:
```

通过NTP服务器自动同步系统时间

6. 输入**Network Time Protocol**对应的序号，例如3并按回车，配置NTP服务。

   说明: 如已配置了NTP服务，将可以看到NTP服务器的地址

7. 输入1并按回车，填写NTP服务器的主机名或IP地址。

```
Network Time Protocol:
   1. Ntp server:
   0. Return
Enter selection: 1
Please input ntp server: 192.168.8.8
```

   说明: 可以输入多个NTP服务器，不同的主机名或IP之间用英文逗号分隔，例如：**ntp1.test.com,192.168.8.8,ntp2.test.com**。只要有一个NTP服务器能够生效，同步时间就能成功。

   配置NTP服务器后，如NTP服务器连接正常，时间同步将立即生效。

配置HA（HA Management)

仅当RIS为HA部署时，Console控制台才会显示HA的配置菜单。

设置HA维护模式

系统管理员可以通过该操作，开启或关闭HA的维护模式。

维护模式是指停止ping和服务状态检查，维持当前主从关系不变。一般用于HA的升级和打补丁等维护操作。

设置维护模式可以在HA的任一节点上执行，开启/关闭后将影响所有节点。

Console菜单中无法直接查看当前是否开启维护模式，但在执行设置维护模式时会进行确认提示，请根据提示中的**enable**或**disable**确认当前的维护模式状态。

开启维护模式

1. 登录到主机或备机的控制台。
2. 输入**HA Management**对应的序号并按回车。
3. 输入**Enable/Disable Maintenance Mode**对应的序号并按回车。
4. 在收到确认开启维护模式提示后，输入y，并按回车，维护模式开启。

关闭维护模式

5. 登录到主机或备机的控制台。
6. 输入**HA Management**对应的序号并按回车。
7. 输入**Enable/Disable Maintenance Mode**对应的序号并按回车。
8. 在收到确认关闭维护模式提示后，输入y，并按回车，维护模式关闭。

请在完成维护操作后，立即关闭维护模式，确保HA遇到故障时能够自动进行主从切换。

拆除HA

系统管理员可以通过该操作，将HA拆成单独的两台RIS。仅当部署了HA的情况下，登录Console控制台时显示该菜单。

> **注意:** 该操作为高危操作，请经过充分的方案讨论，并确认当前没有用户在执行重要操作时，再执行该拆除操作。操作一旦执行，HA的部署将被破坏。操作过程中Web界面可能会不可用，并且操作完成后需要重启RIS的相关进程。建议在执行操作之前先基本设置：备份系统配置。
>
> 需要在主节点和备节点上分别执行拆除HA，建议**先拆除备节点，再拆除主节点**，以防止拆除过程中自动进行主从切换。

1. 登录到备机的控制台。
2. 输入**HA Management**对应的序号并按回车。
3. 输入**Undeploy**对应的序号并按回车。
4. 在收到确认拆除提示后，输入y，并按回车。
   系统将执行拆除脚本，请等待。
5. 登录到主机的控制台
6. 在主机上重复以上步骤，完成主机侧的HA拆除。
   拆除完成后，各台RIS重新独立正常工作，此时可以重新登录到各Web界面及控制台。

查看系统信息（System Maintenance）

系统管理员可以使用Console菜单提供的系统维护工具查看各类系统信息。

1. 登录RIS的Console。
2. 在主菜单中输入**System Maintenance**对应的字符，并按回车，进入**System Maintenance**菜单。
3. 输入以下功能对应的序号，并按回车，查看相应的信息：

序号	名称	说明
1	System Status	查看系统状态，包括CPU、内存、I/O、磁盘空间、RAID、负载等信息。
2	Service Status	包括各进程的名称、PID、内存大小、CPU使用率、进程状态和子进程数。
3	Service Restart	重启指定名称的服务。根据页面提示，输入待重启的服务名称，完成后按回车重启该服务。
4	Port Listening	查看RIS监听的端口列表。
5	Firewall Status	查看RIS的防火墙状态。
6	Product Info	查看产品ID。
7	Module Version	查看各组件的版本信息。
8	Log View	在/var/log目录中查看系统日志。只能执行执行cd、ls、sz、tail或tailf操作。
0	Return	返回上级菜单。

配置网络参数（Network Configuration）

系统管理员可以通过该操作，对RIS的各种网络配置进行调整，实现配置网口、路由、网口绑定、默认网关、主机名域名等功能。

配置网络参数中的大部分功能都可以在Web界面中直接操作，请参考基本设置：配置网络参数。建议仅当Web界面无法登录时才通过Console控制台菜单进行修改。

修改网口信息

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 查看当前存在的网口。子菜单最上方将会显示所有存在配置文件且状态为UP的网口，并按1~N进行编号，如：

```
1. eth0
2. eth1
...
```

4. 输入网口序号，如修改3中的eth1的网口信息，输入2，进入修改eth1网口信息的子菜单。

```
Network Configuration
   1. IP Address   : 10.10.33.18
   2. Netmask      : 255.255.255.0
   3. IPV6 Address :
   4. DNS1         : 192.168.8.8
   5. DNS2         :
   6. DISPLAY
   C. Clear all
```

```
0. Return
```

5. 输入1~4并按回车，修改网口的IP地址、子网掩码或DNS。

   说明：IPv4地址和掩码必须配置，IPv6地址和DNS可以选填。

6. 输入修改后的值并按回车。

7. 全部修改完毕后，输入S并按回车，执行**Submit**提交修改，使网口配置生效。

   操作完成后，系统管理员可以输入**Clear all**对应的字符，例如C，清空所有配置信息。

   也可以输入**DISPLAY**对应的序号，例如6，用于显示当使用DHCP时，自动获取的IPv4、IPv6地址。该功能不能显示通过IPv6路由通告获取的地址。

修改路由配置

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入R，执行**Routes**修改路由配置。
4. 查看当前的路由配置。子菜单最上方将会显示所有手动添加的路由，并按1~N进行编号，显示格式为“**目的网络/掩码,网关**”，如：

   ```
   1. 10.10.34.0/24,10.10.32.1
   2. 10.10.35.0/24,10.10.32.1
   ...
   ```

5. 查看所有路由配置，执行**Display Route**，查看所有路由。显示结果即为Linux的ip route命令的回显，例如：

   ```
   default via 10.10.32.1 dev eth0 proto static metric 102
   1.1.1.0/24 dev virbr0 proto kernel scope link src 1.1.1.1
   10.10.32.1 dev eth0  proto static scope link metric 102
   10.10.33.0/24 dev eth0  proto kernel scope link src 10.10.33.18 metric 102
   10.10.34.0/24 via 10.10.32.1 dev eth0
   10.10.35.0/24 via 10.10.32.1 dev eth0
   ```

6. 输入A，执行**Add**，添加路由。格式为目的网络（/掩码或掩码长度）,网关，例如10.10.36.0/24,10.10.32.1。

   可以重复执行**Add**再一并提交。

   执行**Add**后，所有已添加且并未提交的路由将被编号并显示在子菜单中。

7. 输入R，并输入路由序号，执行**Remove**，对多余的路由进行删除。路由序号即为子菜最上方显示的若干条手动添加的了路由对应的序号。

8. 执行**Add**或**Remove**后，需要输入S，执行**Submit**提交路由配置修改，使配置生效。

查看/修改网口状态

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入S，执行**Device Status**查看网口信息。子菜单中只会列出所有存在配置文件的网口。

子菜单会显示所有网口名称及网口对应的状态，状态显示为**UP**或**DOWN**，并按1~N进行编号。如设置了网口绑定，会列出绑定后的网口，其中网口名称前会加上“**bond**”，绑定状态**Bond**值为**yes**；同时也会列出绑定到该网口的所有物理网口，网口名称前会加上“**bond-slave**”，**Bond**值为绑定后的网口名称。

```
Device status:
  1. Device: bond-net01 Status: UP Bond: yes
  2. Device: bond-slave-eth0 Status: UP Bond: net01
  3. Device: bond-slave-eth1 Status: UP Bond: net01
  4. Device: eth0 Status: UP
  0. Return
```

4. 输入网口前面的序号，修改网口状态，将**UP**修改为**DOWN**，或将**DOWN**修改为**UP**。

配置网口绑定

Bonding(绑定)是一种Linux系统下的网口绑定技术，可以把服务器上多个物理网口在系统内部抽象(绑定)成一个逻辑上的网口，从而达到提升网络吞吐量、实现网络冗余、负载等功能的目的。

网口绑定需要有2个或2个以上的闲置网口，如缺少网口请添加板卡后执行添加网口，再进行网口绑定。

注意：如果被绑定的网口上原来配置了IP地址，被绑定后该IP将被清除。请确保该IP地址不被使用，再进行网口绑定。

在RIS控制台中可以使用**Device Bonding**菜单中的功能，绑定或解绑网口。

警告：配置了网口绑定后，如涉及插入或移除板卡操作，则必须先解除网口绑定并关机后，再进行板卡的插入或移除，否则配置网口时将失败并引起网络服务故障。出现故障后，请解除网口绑定并重启RIS，再重新配置网口绑定；如板卡已移除，请先插回板卡再进行以上操作。

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入B，并按回车，执行**Device Bonding**查看或修改网口绑定。
4. 输入A，并按回车，执行**Add Bonding**，添加网口绑定。
5. 输入绑定后的逻辑网口的名称，并按回车确定。

```
Please input bond name: net01
```

6. 根据提示输入网口绑定的模式编号，并按回车。

网口绑定有7种模式，分别如下：

序号	模式编号	模式名称	说明
1	bond0	balance-rr	平衡轮循策略。平衡负载模式，每块网卡轮询发包，有自动备援，但需要配置交换机。
2	bond1	active-backup	主-备份策略。自动备援模式，其中一条线若断线，其他线路将会自动备援。

序号	模式编号	模式名称	说明
3	bond2	balance-xor	平衡策略。基于指定的传输Hash策略传输数据包。
4	bond3	broadcast	广播策略。在每个slave接口上传输每个数据包，提供容错能力。
5	bond4	802.3ad	IEEE 802.3ad 动态链接聚合策略。创建一个聚合组，它们共享同样的速率和双工设定。根据802.3ad规范将多个slave工作在同一个激活的聚合体下。
6	bond5	balance-tlb	适配器传输负载均衡策略。在每个slave上根据当前的负载（根据速度计算）分配外出流量。
7	bond6	balance-alb	适配器适应性负载均衡策略。平衡负载模式，有自动备援，不必需要配置交换机，通过ARP协商实现接收负载均衡。

7. 根据提示输入待绑定的网口序号，至少两个，中间用“,”分隔，例如：

```
1. eth0
2. eth1
Please input bond device (example 1,2): 1,2
```

等待绑定完成。绑定完成后，子菜单最上方将显示所有绑定的网口，格式为“序号.bond-5中填写的网口名称”。

8. 输入绑定后的网口的IP地址和子网掩码。格式为IP地址/掩码，例如10.10.10.1/255.255.255.0，其中掩码必须为完整的格式，不能只输入掩码长度。

9. 可选： 如需解除网口绑定，在**Device Bonding**菜单中，输入绑定网口的序号，按回车键，并输入y进行确认，解除网口绑定，如：

```
Device Bonding:
   1. bond-net01
   A. Add Bonding
   0. Return
Enter selection: 1
Are you sure to delete bond name: net01?[y/n] y
```

配置默认网关

注意:

一台RIS上默认网关只能设置一个，对一个网口设置默认网关，将清空其他网口上设置默认网关。一般只需要对业务网口设置默认网关。

1. 登录RIS的Console。

2. 输入**Network Configuration**对应的的序号，例如3，并按回车。

3. 输入G，并按回车，执行**Default Gateway**查看或修改默认网关。

   序号为1的行中将显示默认网关的地址，及默认网关所在的网卡，例如：

```
Default Gateway:
  1. Gateway: 10.10.32.1 Dev: eth0
  0. Return
```

4. 输入1，修改默认网关。
5. 在列表中选择1个待设置默认网关的网口。如修改了默认网关的网口，之前设置默认网关将被清空。

```
1: bond-net01
2: eth0
Please input gateway dev: 2
```

6. 输入新的默认网关，并按回车。收到提示后输入y并按回车确定。

```
Current Gateway: 10.10.32.1
Current Gateway Device: eth0

1: bond-net01
2: eth0
Please input gateway dev: 2
Please input new gateway: 10.10.33.1
Config gateway, please wait
Restart network to make new gateway effective?[y/n] y
```

配置IPv6默认网关

仅当为网口配置了IPv6地址时需要配置IPv6默认网关。

> **注意:**
>
> 一台RIS上默认网关只能设置一个，对一个网口设置默认网关，将清空其他网口上设置默认网关。一般只需要对业务网口设置默认网关。

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入G，并按回车，执行**Default IPV6 Gateway**查看或修改IPV6默认网关。

   序号为1的行中将显示默认网关的地址，及默认网关所在的网卡，例如：

```
Default IPV6 Gateway:
  1. IPV6 Gateway: fe80::3a22:d6ff:fe71:db1 Dev: eth0
  0. Return
```

4. 输入1，修改IPv6默认网关。
5. 在列表中选择1个待设置默认网关的网口。如修改了默认网关所在的网口，之前设置的默认网关将被清空。

```
1: bond-net01
2: eth0
Please input gateway dev: 2
```

6. 输入新的IPV6默认网关，并按回车。收到提示后输入y并按回车确定。

```
Current Gateway: fe80::3a22:d6ff:fe71:db1
Current Gateway Device: eth0

1: bond-net01
2: eth0
```

```
Please input ipv6 gateway dev: 2
Please input new ipv6 gateway: fe80::3a22:d6ff:fe71:db2
Config gateway, please wait
Restart network to make new gateway effective?[y/n] y
```

关闭/开启IPv6路由通告

IPv6路由通告即无状态地址自动配置（SLAAC），通过路由器自动获得IPv6地址。区别于DHCPv6，它是另一种动态获取IPv6地址的方式。

RIS默认开启IPv6路由通告，在支持路由通告的路由器网络中将自动获取到一个IPv6动态地址。用户可以参考本节的操作关闭/开启该功能。

注意：关闭/开启IPv6自动配置后，需要重启RIS。请确保当前的系统没有承载业务，可以正常重启，再执行本节的操作。

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入C，进入**IPV6 Auto Config**菜单，修改IPv6自动配置的状态。

   说明：IPV6 Auto Config:后面会显示当前IPV6 Auto Config的状态，默认为**Enable**，即可以通过路由通告自动获取IPv6地址。
4. 如需开启IPv6 路由通告，输入**Enable ipv6 auto configuration**对应的序号，例如1，并按回车。在收到重启系统使配置生效提示后，输入y后，按回车。
5. 如需关闭IPv6 路由通告，输入**Disable ipv6 auto configuration**对应的序号，例如2，并按回车。在收到重启系统使配置生效提示后，输入y后，按回车。

配置主机名信息

系统管理员可以通过该操作，查看并修改主机名和域名。

注意：该操作完成后会重启RIS，请确保操作时允许重启RIS。

此处的主机名仅用于标识RIS所属节点的名称，一般不需要修改。部署HA时建议将不同RIS修改成不同的主机名，从而便于对HA中的不同主机进行区分。

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入H，并按回车，执行**Host Info**查看或修改主机名和域名。显示格式为**1.Hostname：主机名、2.Domain name：域名。**
4. 输入1并按回车，修改主机名。

   输入修改后的主机名，并按回车。

   说明：如要取消修改，请直接按回车。
5. 输入2并按回车，修改域名。

输入修改后的域名，并按回车。

说明: 如要取消修改，请直接按回车。

6. 确认修改无误后，输入S，并按回车，执行**Submit**提交修改，使配置生效。
7. 收到重启提示后，输入“y”，并按回车，执行重启。

   重启后，超级管理员可以登录RIS Web界面，并在**系统设置** > **系统状态中**看到修改后的主机名。

添加网口

当新加了一块物理网卡后，一般需要重启，该网口信息才会在**Network Configuration**菜单中显示。使用该功能可以无需重启就将网口信息添加到**Network Configuration**菜单中。

已执行过添加操作的网口，仅在此显示，将无法再执行添加操作。

1. 登录RIS的Console。
2. 输入**Network Configuration**对应的的序号，例如3，并按回车。
3. 输入A，并按回车，执行**Add Net Device**添加网口。
4. 在列表中选择一个待添加的网口，输入该网口的序号，并按回车，添加网口。

   收到确认提示后，输入y并按回车确认。

```
1. eth0
2. eth1
3. eth2
Please choose device: 3
Are you sure to add eth2 ? (y/n)y
```

完成添加网口后，请参照修改网口信息修改该网口的信息。

使用Shterm工具（Shterm Tools）

系统管理员可以使用控制台提供的Shterm工具完成采集日志和安装补丁包等操作。

一键采集日志

本节介绍如何在控制台采集RIS的日志。

该功能与Web界面的日志采集的功能一致，但使用时请注意以下差异：

- 通过Web采集日志可以配置日志的级别，通过控制台采集日志无法配置级别，直接使用Web上配置的级别。
- 通过控制台采集日志，只能采集当前节点的日志。对于HA，由于无法登录HA备节点的Web界面，因此备节点必须通过控制台采集。

说明:

- 请通过SSH连接控制台，SSH客户端必须使用支持ZMODEM的客户端（例如不能使用putty），因为采集过程中需要使用**sz**从RIS下载文件到本地PC。
- 采集过程中请严格按照界面提示进行操作，请勿执行 **Ctrl+C**退出控制台界面。

1. 登录RIS的Console。

2. 输入**Shterm Tools**对应的序号，然后按回车。
3. 输入**Collect Log**对应的序号，然后按回车。
4. 输入日志采集的天数，然后按回车（如果不输入天数直接按回车表示采集所有日志），采集完成后请选择本地PC保存日志的文件夹。

   说明： 由于采集日志涉及的文件较多，采集时间会较长，请耐心等待。

5. 将采集后得到的**tbx**文件交给齐治科技工程师进行解密并分析。

安装标准升级包和补丁包

RIS支持通过控制台界面安装任何格式的系统升级包和补丁包，实现软件更新，但升级包或补丁包必须是齐治科技官方发布的包且文件内容正确。

升级包是指从一个版本升级到另一个版本的软件包；补丁包是指一个版本内解决问题的软件包。升级包安装完成后需要手工重启系统，补丁包安装完成后不需要重启系统。

安装系统升级包和补丁包同时在Web和控制台下支持，请根据不同的部署场景选择安装方式：

- 对于单机，可以任意选择通过Web或者控制台安装。
- 对于**HA**，请先通过VIP登录Web开启维护模式；然后通过实IP登录**主节点**的**控制台**或者**Web**安装补丁；再通过实IP登录**备节点**的**控制台**安装补丁；最后通过VIP登录Web关闭维护模式。如果安装的是升级包需要重启系统，请在关闭维护模式后执行重启操作。

1. 通过SSH方式登录RIS的Console。

   说明： 请通过SSH连接控制台，SSH客户端必须使用支持ZMODEM的客户端（例如不能使用putty），因为安装过程中需要使用**rz**从本地PC上传文件到RIS。

2. 输入**Shterm Tools**对应的序号，然后按回车。
3. 输入**Install standard patch package**对应的序号，然后按回车。
4. 在弹出的窗口中，选择补丁包，并单击**打开**，上传补丁包到RIS中。

   说明： 安装过程中请严格按照界面提示进行操作，请勿执行 **Ctrl+C**退出控制台界面。

补丁包上传完成后，RIS会自动完成该补丁包的安装，补丁安装完成后会自动删除该安装包。

安装其他特殊补丁包

本节介绍如何在RIS上安装**zip**格式的特殊补丁包。

对于**HA**，请先通过VIP登录Web开启维护模式；然后通过实IP登录**主节点**的控制台安装补丁；再通过实IP登录**备节点**的控制台安装补丁；最后通过VIP登录Web关闭维护模式。

说明：

- 请通过SSH连接控制台，SSH客户端必须使用支持ZMODEM的客户端（例如不能使用putty），因为安装过程中需要使用**rz**从本地PC上传文件到RIS。

- 安装过程中请严格按照界面提示进行操作，请勿执行 **Ctrl+C**退出控制台界面。

1. 登录RIS的Console。
2. 输入**Shterm Tools**对应的序号，然后按回车。
3. 输入**Install special patch package**对应的序号，然后按回车。
4. 在弹出的窗口中，选择zip格式的补丁包，并单击**打开**，上传补丁包到RIS中。

补丁包上传完成后，RIS会自动完成该补丁包的安装，补丁安装完成后会自动删除该安装包。

恢复出厂设置

本节介绍如何恢复出厂设置。

恢复出厂设置，将清除当前的所有配置信息（包括用户、资产、权限和系统设置）并重启设备。

1. 登录RIS的Console。
2. 输入**Shterm Tools**对应的序号，然后按回车。
3. 输入**Restore factory settings**对应的序号，然后按回车。
4. 按照提示输入信息，恢复出厂设置。

修复RPM Database

本节介绍如何修复RPM Database。

RPM Database的修复使用rpm命令中的rpm --rebuild命令进行修复，请参考该命令的使用说明。只有当RPM Database存在问题时，Console控制台中才会有修复RPM Database的选项。

1. 登录RIS的Console。
2. 输入**Shterm Tools**对应的序号，然后按回车。
3. 输入**Fix rpm database**对应的序号，然后按回车。
4. 在收到确认修复RPM Database提示后，输入y，并按回车，系统将执行RPM数据库的重建。

重置admin用户（Reset admin）

当超级管理员admin丢失密码无法登录时，可以通过该功能重置admin帐号的密码、角色、身份验证方式、手机号、状态。

1. 登录RIS的Console。
2. 输入“R”并按下回车键，进入**Reset admin**。
3. 输入“1”并按下回车键，执行**Reset Admin**。
4. 收到要求确认提示后，输入“Y”或“y”并按下回车键。

   收到重置成功提示后，admin的帐号将进行以下修改：

   - 密码：重置为**admin**。

- 角色：重置为**超级管理员**。

  说明：其他超级管理员可以将admin帐号的角色修改为其他角色。

- 身份验证方式：重置为**本地密码**。
- 手机号：重置为空。
- 状态：重置为**活动**。

admin用户被重置后，立即使用admin登录RIS Web界面，使用密码**admin**，登录成功后立即修改密码。

如admin帐号被其他超级管理员修改为了其他角色，重置后会重新变为超级管理员。但必须登录Web界面，完成修改密码并重新登录，admin的用户角色才能正常显示为超级管理员。

配置SSHD端口状态（SSHD Management）

当管理员需要允许或禁止用户使用SSH登录RIS的Console控制台时，可以在控制台菜单中进行配置。

启用和禁用SSHD端口，表示允许或禁止用户使用SSH通过8022端口连接到RIS并操作Console控制台。

该操作可以在Console控制台中操作，也可以在Web界面的**系统设置** > **系统** > **系统状态**的**sshd外部访问**参数中设置，两处配置同源。但Web界面中仅能进行配置，看不到SSHD的实际状态。而控制台中可以查看SSHD实际状态，同时修改配置。

1. 登录RIS的Console。
2. 在主菜单输入“S”并按下回车键，进入**SSHD Management**。
3. 查看**1. SSHD port status:**后面的状态，enable表示已启用SSHD，disable表示已禁用SSHD。
4. 输入“D”，执行**Disable sshd port**，禁用SSHD；或输入“E”，执行**Enable sshd port**，启用SSHD。

禁用SSHD之后，当前通过SSH连接到Console控制台的会话不会直接断开，但退出会话之后无法再重连。

禁用SSHD之后，无法通过SSHD访问Console控制台。如需启用SSHD，可以在Web界面上修改配置，也可以通过设备的VGA或者IPMI接口修改配置。

配置Host头防护（Nginx Management）

为了保证RIS不存在HTTP Host头攻击风险，管理员可以启用HTTP Host 头攻击防护，并设置HTTP Host 头白名单。配置后，当用户访问RIS的Web界面时，将会检查用户访问请求中的Host头是否匹配白名单中的域名或IP，只有匹配成功时才能够访问Web界面。

RIS一般需要将业务网口的IP添加到白名单中；如果是HA部署，且需要使用虚IP和各节点的实IP访问Web界面，则将这些IP都添加到白名单中。如果做了域名的映射，需要将所有域名都添加到白名单中。

HA部署时，可以在任意节点的Console菜单中修改Host头防护配置，修改的都是主节点的配置文件。

1. 登录RIS的Console。

2. 在主菜单输入N并按下回车键，进入**Nginx Management**。
3. 查看**Host header defend status**后面的Host头防护的状态，enable表示开启，disable表示关闭。
4. 输入E，执行**Enable host header defend**，开启防护；或输入D，执行**Disable host header defend**。
5. 启用防护的状态下，输入U，执行**Update Server Name**，更新Nginx的Server Name名单。
6. 输入新的Server Name名单内容并按回车确定。**Current Server Name**将显示当前的名单内容。

```
Nginx Management:
   1. Host header defend status: enable
   D. Disable host header defend
   U. Update Server Name
   0. Return
Enter selection: U

Current Server Name: 10.10.33.35 10.10.33.36

Please input new server name: 10.10.33.* ~.*.fc00.1010.32.0.* *.example.com
Update nginx server name successfully.
```

说明:

- 如需配置IPv6地址，具体的地址需要加上中括号，例如[fc00:1010:32::1]。
- 域名可以使用模糊匹配或使用正则表达式，例如*.example.org、~^www\d+\.example\.net$。
- 如需配置为网段，必须使用模糊匹配或正则表达式，例如10.10.10.0/24网段，写成10.10.10.*。对于IPv6网段，只能使用正则表达式，正则表达式不加中括号，并将:用.代替，例如fc00:1010:32::/64网段，写成~.*.fc00.1010.32.0.*。
- 多个IP或域名之间用空格进行分隔。

在该菜单中执行启用/关闭该功能，或者执行**Update Server Name**，Nginx都将会自动重启。

配置访问控制（ACL Management）

通过配置ACL访问控制，可以对远程访问Console控制台的主机地址进行限制。

ACL访问控制是一个白名单，限定了哪些IP地址可以通过SSH远程访问RIS的Console控制台。若该白名单为空，则所有IP地址都可以通过SSH远程访问Console控制台。一旦该白名单中添加了控制规则，则只有白名单中的地址可以SSH访问Console控制台。

1. 登录RIS的Console。
2. 在主菜单输入A并按下回车键，进入**ACL Management**。
3. 输入A，执行**Add**，添加ACL规则，并输入y确认。

   ACL规则格式为目的网络[（/掩码或掩码长度）]，即可以为某个具体的IP地址，例如10.10.67.18，或某个网段，例如10.10.67.0/24或10.10.67.0/255.255.255.0。

```
ACL Management:
   A. Add
   R. Remove
   0. Return
Enter selection: a
```

```
Please input acl (target[/netmask or masklen]): 10.10.67.0/24
Are you sure (10.10.67.0/24) ? (y/n)y
```

添加的规则将显示在**ACL Management**菜单的最上方，并按添加顺序进行排序和标号。

4. 如需对已添加的规则进行修改，输入规则对应的序号，并重新填写规则的内容。

```
ACL Management:
   1. 10.10.67.0/24
   2. 10.10.66.15
   A. Add
   R. Remove
   S. Submit
   0. Return
Enter selection: 2
Update acl (orig: 10.10.66.15): 10.10.66.0/24
Are you sure (10.10.66.0/24) ? (y/n)Y
```

5. 如需删除某条规则，输入R，执行**Remove**，并输入规则序号进行删除。

```
ACL Management:
   1. 10.10.67.0/24
   2. 10.10.66.0/24
   A. Add
   R. Remove
   S. Submit
   0. Return
Enter selection: r
Please input id: 2
Remove (10.10.66.0/24) now, sure? (y/N)y
```

6. 完成所有规则的添加/修改/删除并确认无误后，输入S，执行**Submit**，提交对ACL规则的所有修改。

> **注意：** 如需继续使用当前PC客户端SSH登录Console控制台，请确保添加的ACL规则里已包含了该PC客户端的IP地址。否则断开连接后将无法再连接。

```
ACL Management:
   1. 10.10.67.0/24
   A. Add
   R. Remove
   S. Submit
   0. Return
Enter selection: S
```

使用系统工具（System Tools）

系统管理员可以使用Console菜单提供的系统工具进行网络调试操作。

1. 登录RIS的Console。
2. 输入**System Tools**对应的字符，并按回车，进入**System Tools**菜单。
3. 使用**Ping**工具。

   发送ICMP包给指定IP地址，检查RIS和目标地址之间的连通情况，相当于在Linux下执行ping命令。该操作要求目的IP地址的防火墙入站规则中允许ICMP回显。操作回显过程中可以使用**Ctrl+C**中断操作。

   a) 输入**Ping**对应的数字并按回车。

   b) 输入待检测连通情况的资产的IP地址，并按回车。

   将回显出3次ping操作的结果。

c) 输入**Return**对应的数字，返回上级菜单。

4. 使用**Traceroute**工具。

   跟踪从RIS到目标地址之间的路由，会显示出经过的各层路由，相当于在Linux下执行traceroute命令。操作回显过程中可以使用**Ctrl+C**中断操作。

   a) 输入**Traceroute**对应的数字并按回车。

   b) 输入待跟踪路由的IP地址，并按回车。

   将依次回显出RIS到目标地址经过的路由，如经过的路由较多，需要等待一定的执行时间。

   c) 输入**Return**对应的数字，返回上级菜单。

5. **重启系统。**

   a) 输入**Reboot**对应的数字并按回车。

   b) 按照提示输入y确认。

6. **关机。**

   a) 输入**Power off**对应的数字并按回车。

   b) 按照提示输入y确认。

7. **修改root密码**

   a) 输入**Change root password**对应的数字并按回车。

   b) 输入新的root登录密码，并按回车。

   说明: 密码长度建议至少8位。当设置长度不足8位时会提示**BAD PASSWORD**，但仍能设置成功。

   c) 根据页面提示，再输入一遍修改后的密码，完成后按回车。

8. 使用**Advanced Management**工具。

   a) 输入**Advanced Management**对应的数字并按回车。

   b) 将显示的**User Code**发送给齐治科技技术支持人员，获取**Challenge**码。

   c) 输入**Challenge**码后，按回车进入命令行菜单，并执行Linux命令。

   d) 在命令行中输入**exit**并按回车，或直接按**Ctrl**+**D**，返回Console菜单。