中科云量
ZKQCLOUD

中科云量运维安全管理系统

操作手册

广东中科云量信息安全技术有限公司

地址：广州市天河区天慧路10号粤港澳大湾区创新基地 电话：020-29029607 传真：020-29029607

版权声明

免责条款

1、本文档是广东中科云量信息安全技术有限公司相关工作人员依据现有信息制作，在编写该文档时候已尽最大努力保证其内容准确可用，广东中科云量信息安全技术有限公司及其员工将不对本文档中任何内容直接或间接导致第三方的损失和损害承担任何责任。

2、本文档是用户实际安装过程中的指南和使用参考手册，本文档的部分内容可能随产品型号和规格的不同而略有区别，不会影响对本文档的理解。中科云量有权利在不通知用户的情况下对产品和手册进行修改，请以实际设备为准。相关问题请咨询中科云量全国服务热线 400-618-6058。

信息反馈

全国服务热线：020-29029607

公司网址：http://www.zkqcloud.com

总公司邮编：510000

总公司地址：广州市天河区天慧路 10 号粤港澳大湾区创新基地

目 录

第一章 产品概述

广东中科云量信息安全技术有限公司长期致力于各行业用户在安全建设、安全运维、安全综合管理中所遇到的各种问题的研究，为用户提供安全解决方案，安全服务和产品，协助用户在进行自身的信息安全建设时迅速有效的解决问题，并有效保持需达到的安全保障水平。本文中所介绍的中科云量运维安全管理系统作为中科云量公司统一身份管理（4A）解决方案中的重要组成部分，同时可作为单独的安全产品，为用户提供网络主机安全管理安全保障。

该产品主要帮助用户对服务器、网络设备、安全设备、关键应用、数据库的访问行为进行管控，通过部署该产品使得相关操作、管理和运行更加可视、可控、可管理、可跟踪、可鉴定，解决系统级别的安全问题、安全威胁，为国家重要部门和企业信息系统的正常有序运行，提供可靠的安全保障。

第二章 WEB 管理

中科云量运维安全管理系统可以通过用WEB界面进行配置管理，也可以通过ssh或串口超级终端登录系统，用命令行方式进行管理。本用户手册主要介绍如何使用中科云量运维安全管理系统的 WEB 界面进行配置管理。

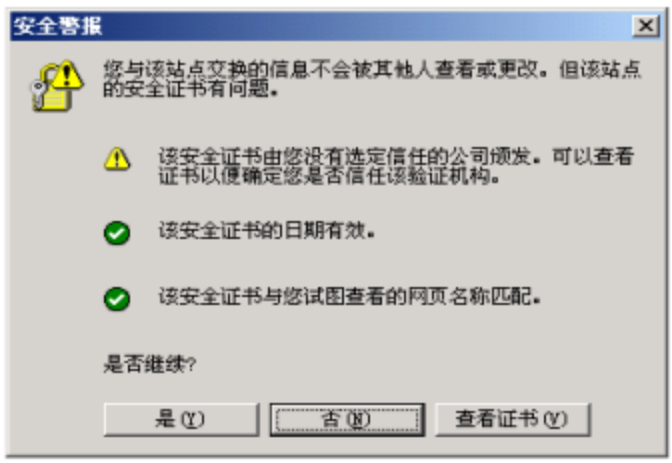
2.1 登录管理

为了能够使用中科云量运维安全管理系统上的 WEB 管理界面，需要使用您工作站上的浏览器。由于超文本传输协议（HTTP）以非加密的明文形式进行网络传输，为了建立一个安全的从工作站到中科云量运维安全管理系统之间的连接，中科云量运维安全管理系统需要您使用安全套接字（SSL）协议 2.0 或 3.0 版，安全套接字加密了所有和中科云量运维安全管理系统之间交换的信息。

注意：为了建立一个 SSL 连接，需要您的工作站和中科云量运维安全管理系统之间进行相互认证，如果无法进行认证将无法建立连接。当您访问中科云量运维安全管理系统时，安全认证会弹出警告信息。当您接受了认证，中科云量运维安全管理系统和工作站之间就能建立持续的安全、加密的连接。

下面为登录步骤：

1. 默认管理口：LAN2，地址：192.168.1.1。
2. 在您的管理工作站上运行 IE 浏览器（或火狐浏览器）。
3. 在[地址]栏中，输入 https:// 192.168.1.1，弹出一个安全警告框，显示如下：



4. 选择下列一项：
   - 点击[是]接受登录进程的认证
   - 点击[否]拒绝登录进程的认证
   - 如果您想使用安装认证向导在您的工作站上永久安装认证，点击[查看证书]，再点击[安装证书]即可为此您的计算机安装证书。
   - 若输入服务器 IP 地址不正确系统会显示下图所示的出错信息：

2.2 登录

登录界面共包括两部分内容：登录信息和控制按钮，输入信息包括：用户名称、登录密码；控制按钮包括：登录、退出，如下图：

注意：系统支持三员分立，为了确保中科云量运维安全管理系统的安全，不同角色的授权管理员只有一个，程序启动以后管理员应及时修改口令，以免被他人非法登

录。

缺省的管理员用户和密码：

- **系统管理员**

用户名：sysadmin，密码：Sysadmin@2017

负责系统运行维护，可以进行系统配置管理，包括系统的重启、关机；日志下载与删除；配置管理；系统重置；系统升级；磁盘告警设置；时间设置；网络配置，查看系统状态等功能。

- **安全保密管理员**

用户：admin 密码：Bluedon@2017

负责用户帐号管理、设备管理、部门管理、访问控制、命令防火墙、参数设置，审计员操作日志和登录日志的审查分析等功能。

- **审计员**

用户：auditor 密码：Auditor@2017

负责对系统管理员、安全保密员的操作行为进行审计和对操作日志进行管理。

- **普通用户**

通过帐号集中管理与审计系统管理设备的普通用户是通过安全管理员创建，创建不同的普通用户，根据不同的协议对设备进行管理，协议包括 7 个协议，分别为：ssh、telnet、ftp、sftp、rdp、vnc、db。

2.3 快捷操作

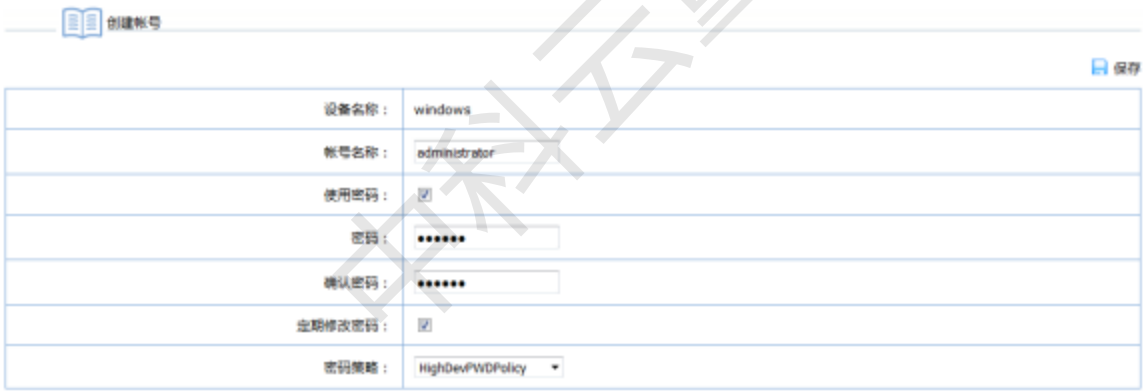
1.登录安全保密管理员 admin，配置帐号集中管理的设备。

第一步：在基础管理→部门管理，右键点击右侧部门名称，在弹出的菜单中点击“修改”按钮，修改默认部门为您所需要的部门名称。

第二步：在设备管理→设备管理，点击“添加设备”，输入设备名称、描述、

IP 地址、协议、端口等参数，创建帐号集中管理与审计系统管理的设备。

第三步：添加设备成功后，给该设备添加帐号，输入该设备的帐户名称、密码，是否定期修改帐户的密码等参数。



2.登录安全保密管理员 admin，添加授权管理设备的用户，该用户为帐号集中管理与审计系统的普通用户。

第一步：在基础管理→用户管理，点击“创建”按钮，输入登录名称、开始时间、结束时间、状态，选择角色为：用户、部门的等参数，创建授权管理设备的用户。

第二步：创建用户成功后，用初始密码登录普通用户，也可以修改用户的密码，用修改后的新密码登录。

3.登录安全保密管理员 admin，授权用户与帐号集中管理与审计系统管理的设备之间的访问控制。

第一步：在设备管理→访问控制，点击“授权”，在授权管理界面，选择部门、用户、勾选授权的设备，点击“授权”，创建用户可以管理设备的授权关系。

第二步：在设备管理→访问控制，查看已经建立用户的授权管理关系。

第三步：用浏览器，输入帐号集中管理系统的地址，登录已授权的普通用户。登录成功，点击“连接”，根据授权的不同协议，访问授权的设备。

注意：

- **添加到帐号集中管理与审计系统的设备必须要与帐号集中管理与审计系统网络互通。**
- **添加到帐号集中管理与审计系统的设备已开启相应协议的服务，例如 telnet、VNC 等服务。**

第三章 系统操作

中科云量运维安全管理系统的配置管理主要通过 WEB 界面来实现，首页界面主要包括页面左边区域的菜单栏，页面右边区域的中科云量运维安全管理系统说明页面。

3.1 基础管理

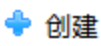
中科云量运维安全管理系统的基础管理是对设备的基本参数设置，使其能够正常工作。包括“用户管理”、“设备管理”、“部门管理”、“访问控制”、“命令防火墙”、“命令集管理”等选项。用鼠标单击页面左边菜单栏的“基础管理”菜单可以看到它所包含的子菜单项。

3.1.1 用户管理

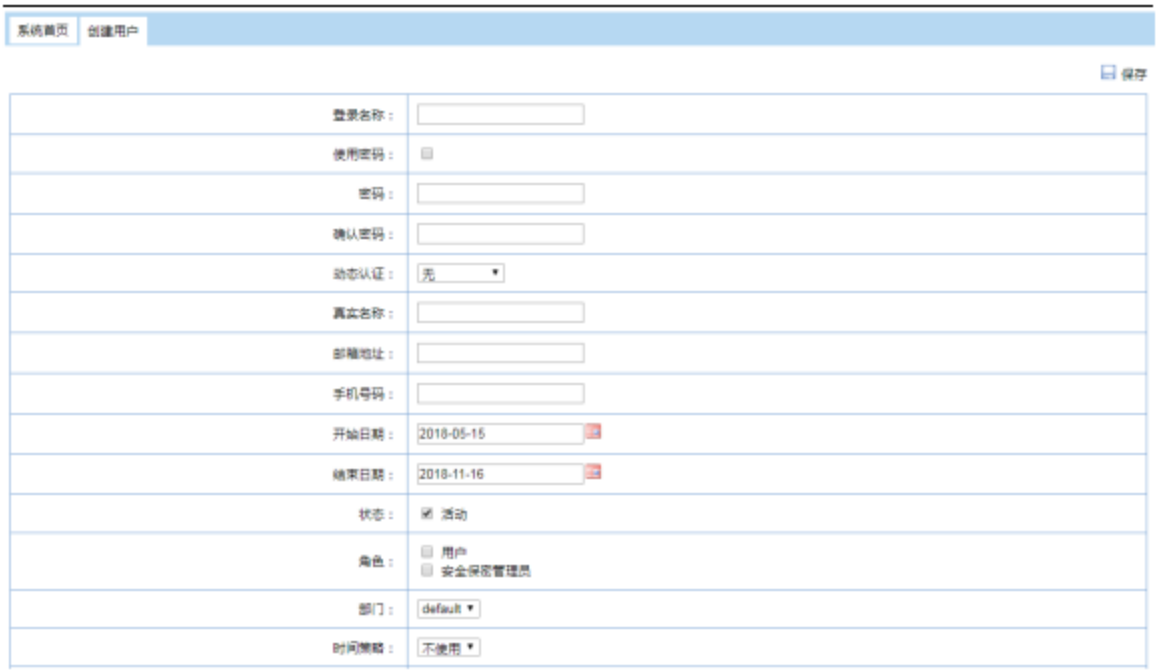
在用户管理模块，添加对授权管理设备进行访问控制的用户，功能包括查看角色，创建用户、导出用户列表、修改用户属性、重置密码、访问控制权限，删除用户。可以根据实际情况，管理不同的用户。

1.查询用户，在用户列表的  文本框输入登录名称进行查询。

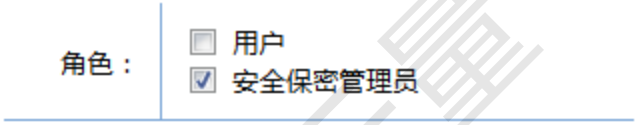
2.查看角色：点击“查看角色”，用户列表显示用户的所属角色。

3.创建用户：点击“  ”按钮，进入创建用户界面。

如设定角色为“用户”。则具有使用系统分配的设备资源及修改用户信息（密码、邮箱地址）的权限。



如设定角色为“安全保密管理员”，如下图：



说明：

“**登录名称**”是指用户的名字，只能使用用户的英文名，这样方便审计报表显示实名制，如 zhangdaqian；

“**动态认证**”指定动态认证的类型，包括：短信验证码，动态口令，数字证书，USB KEY，在登录时，需要输入相关的短信认证码、动态口令或导入数字证书，插入 USB KEY 才能登录系统；

“**真实名称**”是指用户的真实姓名，如张大千；

“**邮箱地址**”是指用户的电子邮箱，如 zhdq@bluedon.com，通过该邮箱，用户可以收到相关信息，例如其密码等；

“**手机号码**”指定接收短信验证码的手机号；

“**开始日期**”是指用户活动/失效的开始时间；

“**结束日期**”是指用户活动/失效的结束时间；

“**状态**”是指用户当前是否处于激活状态；

“**角色**”分两种，指明用户是哪种角色。‘用户’指普通用户；‘安全保密管理员’指负责用户帐号管理、参数设置和日志的审查分析。

“**部门**”是配合现实管理工作的项，可以采用部门的上下级关系，配合行政上

的管理。

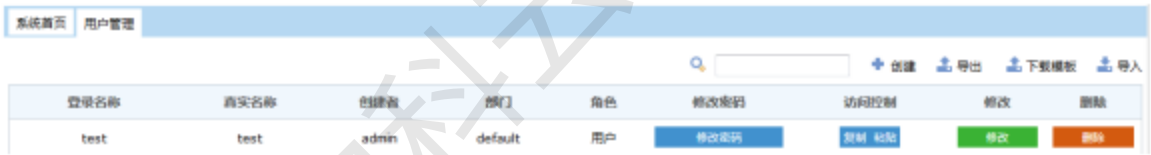
“**时间策略**”是指用户访问管理设备的时间限制设置，详细设置在参数设置里。

“**IP 策略**”是指用户访问管理设备的 IP 限制设置，详细设置在参数设置里。

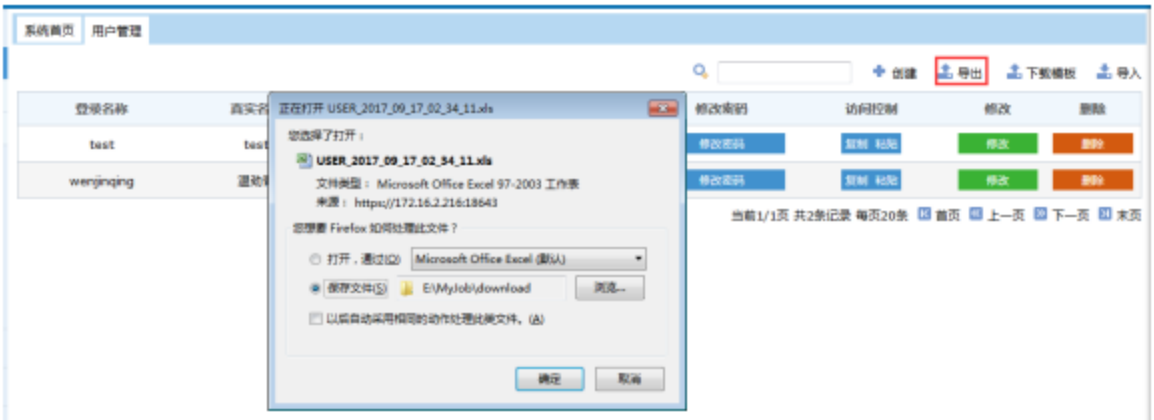
编辑完成，点击“保存”后，提示创建用户成功，如下图：

4.修改用户属性、修改密码、访问控制权限，删除用户。

在用户管理界面，可以显示用户属于哪种角色，忘记密码的用户可以修改其密码，也可以对用户相关属性进行修改、粘贴或者复制用户的访问控制权限、删除用户，如下图：



5.导出：可以以 excle、html 格式导出用户列表，点击“ 导出 ”，弹出保存文件对话框，选择保存文件目录，点击确定。



6.下载模板：下载导入用户的模板，点击“ 下载模板 ”，弹出保存文件对话框，选择保存文件目录，点击确定。

7.导入：导入用户，点击“ 导入 ”，进入导入配置文件页面，点击浏览按钮，选择要导入的数据（导出的用户数据或下载模板后添加的用户数据），点击导入。

8.复制、粘贴：点击“ 复制 ”，复制某用户管理的设备的权限；在需要授予设备权限的用户中点击“ 粘贴 ”，将点击“ 复制 ”复制出来的访问设备的权限粘贴给该用户。

3.1.2 部门管理

部门管理是将访问控制管理映射到设备上的管理关系，列出了部门里面含有的用户和设备，可进行修改和删除、添加、查询部门，默认的部门根节点为：default，如下图所示。

1.查询部门，在 文本框输入部门名称进行查询。

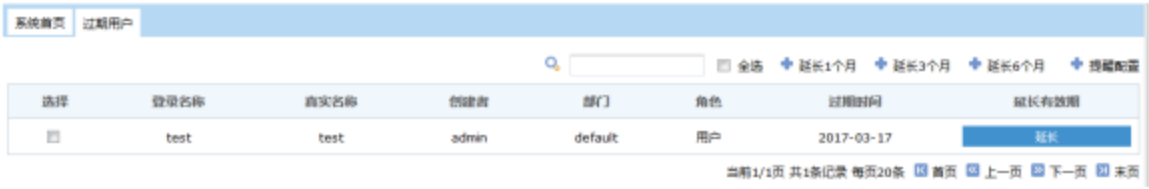
2.用户列表页，显示、管理帐号集中管理与审计系统的普通用户，包括授权、修改、删除、添加等。

3.设备列表页，显示帐号集中管理与审计系统的所有设备，包括授权、修改、删除、添加等。

4.添加部门，点击页面左侧的“ 添加部门 ”，输入部门名称，选择上级部门，点击保存。也可直接右键点击左侧列表的部门名称，在弹出的菜单中点击“添加”，输入部门名称后点击保存。

3.1.3 失效用户

失效用户用于管理已过期的用户，可延长用户的使用时长，如下图所示。



1.查询用户，在  文本框输入部门名称进行查询。

2.延长 1 个月：延长用户的使用时间从当前时间往后顺延一个月。勾选用户，点击“延长 1 个月”。

3.延长 3 个月：延长用户的使用时间从当前时间往后顺延三个月。勾选用户，点击“延长 3 个月”。

4.延长 6 个月：延长用户的使用时间从当前时间往后顺延一个月。勾选用户，点击“延长 6 个月”。

5.延长：延长用户的使用时间到选择的结束日期。点击数据条目中的“延长”，选择结束日期，点击确定。

6.提醒配置：针对用户的过期时间，通知相关的人员。

3.2 设备管理

3.2.1 配置向导

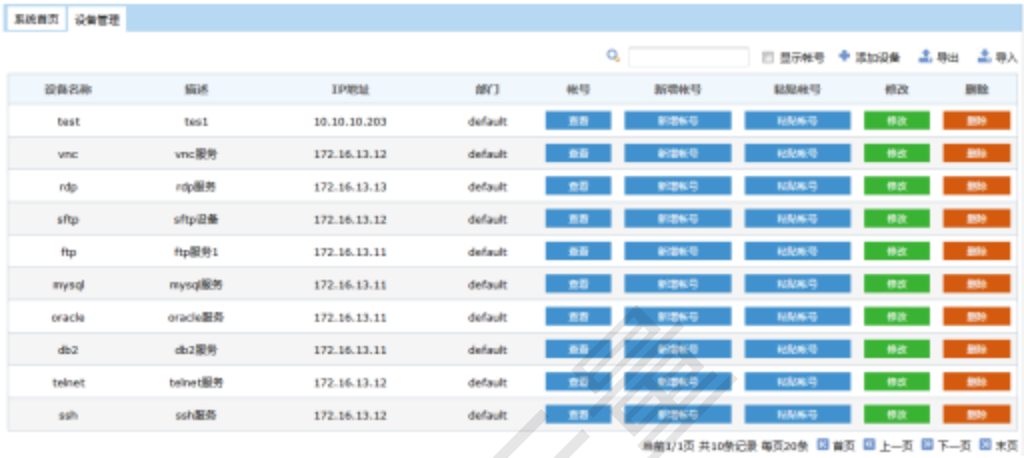
以引导用户的方式，添加设备、账号，授权访问设备。

1.添加设备，添加访问设备和账号。

2.添加授权，添加用户访问当前添加的设备的权限。

3.2.2 设备管理

设备管理可对设备和设备里面的帐号和帐户密码进行管理，能直观显示设备所属的组、部门和设备里面开设的帐号，并对这些信息进行修改。

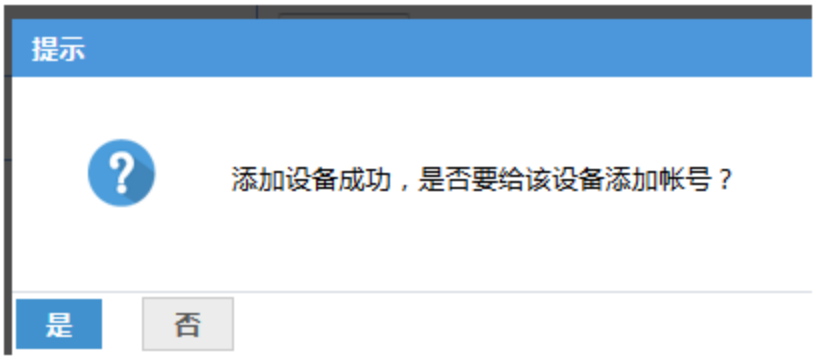


1.查询设备，在  文本框输入设备名称进行查询。

2.显示帐号，点击“显示帐号”，显示可以管理访问设备的帐号。

3.“添加设备”指增加需要保护的设备主机。如下图：

点击“保存”，出现如下对话框：



点击“是”，添加帐号，如下图：

同上步骤添加：可以根据管理的实际情况，添加相应的设备及其用户。

在设备管理界面，可以显示设备的帐号，也可以对设备相关属性进行修改、新增或者粘贴设备的帐号、删除设备。

说明：

“**设备名称**”指设备的管理名称，例如“核心交换机 C6500”；

“**描述**”指对设备的一些说明、备注；

“**IP 地址**”指设备远程管理的 IP 地址，如“10.243.21.83”；

“**部门**”指设备行政上属于哪个部门，一般不需要修改；

“**端口**”指相应协议所使用的 tcp 端口，一般使用默认值；

“**设备类型**”指设备是哪种 Unix Like 系统，有 Cisco、Huawei 网络设备，通用 Unix 和 Linux 等；

“**协议**”用来设置该设备上已存在的服务协议；

协议目前支持支持 ssh、telnet、vnc、rdp、ftp、sftp、db 协议，注意 db 协议目前支持 oralce 数据库、mysql 数据库，添加数据库对应的端口和数据库名，当数据库为 oracle 时，数据库名是服务号或者 ID 号、实例名。

“**时间策略**”是指用户访问管理设备的时间限制设置，详细设置在参数设置里，默认不使用。

“**IP 策略**”是指用户访问管理设备的 IP 限制设置，详细设置在参数设置里，默认不使用。

4、导出，指以 excel、html 的格式导出设备的信息列表，包括设备名称、设备 IP、

设备类型、服务类型等。

3.2.3 设备授权

中科云量运维安全管理系统策略控制主要是通过组对用户、设备和设备里的帐户进行授权配置来实现的，用户对授权给它的资源具有使用的权限。

1.查询授权管理，在  文本框输入用户、设备、帐号、协议进行查询。

2.设备授权，进去访问控制界面，点击“授权”，在授权管理界面，选择部门、用户、勾选授权的设备，点击“授权”，创建用户可以管理设备的授权关系。

说明：

“**部门**”可筛选出我们所要建立授权关系的部门和设备；

“**用户**”指我们要授以权限的用户，可以勾选多个；

“**设备**”是用来选择要授权给用户的设备、使用的帐号和服务协议；

4. 选择完后点击‘创建’按钮完成创建的任务。

5. 授权的删除，在授权管理界面可以删除授权。

3.2.4 设备扫描

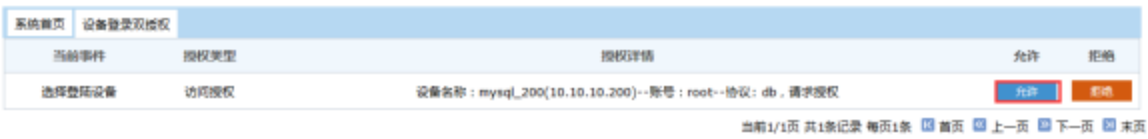
设备可以扫描同个网段的启用了 ssh、ftp、sftp、telnet、rdp、vnc 设备，扫描的内容包括：网卡名称、IP 地址、协议名称、端口后，操作系统，方便用户添加管理设备。如下图所示：

1. 输入 IP，点击“ 一键扫描 ”按钮，进行网络扫描。扫描时，会显示扫描进度，扫描结束后，会显示最后扫描时间。

2. 点击“ 清空扫描信息 ”，可以清空扫描信息。

3.2.5 设备登录双授权

用户发起访问申请，在双授权管理中配置的“授权者”登录系统后，即可在该页面中看到用户发起的访问申请，该页面可允许、拒绝双授权登录申请。



1. 允许，点击列表中的允许，通过用户的访问申请，用户登录设备成功。

2. 拒绝，点击列表中的拒绝，拒绝用户的访问申请，用户登录设备失败。

3.3 应用管理

应用管理模块可让被授权用户通过 web 直接在本地计算机中访问远程计算机的应用。用安全保密管理员（admin）登录系统，在应用管理模块中添加应用跳板机、应用资源，创建应用实例并将实例授权给系统用户，用户即可使用相应的应用。

3.3.1 配置向导

以引导用户的方式，添加资源实例，授权访问应用。

1. 创建实例，添加资源实例。选择下拉菜单，选择资源，点击创建实例。
2. 添加授权，添加用户访问当前添加的应用实例的权限。

3.3.2 应用资源

应用资源能对应用资源进行管理，可添加、查询、删除应用资源，可创建应用实例。

1. 添加资源

打开应用管理-应用资源页面，在该页面中点击“ 添加资源 ”，在应用代填中输入名称，选择代填应用类型（如果为 C/S 应用，请点击“ ... ”选择相应的应用），根据应用的实际情况勾选不需要录制自动完成（如果不勾选，则进入录制自动完成

页面），点击确定。

录制过程分三个步骤：

一、选择需要录制的控件（如果没有，则在自定义类型中输入自定义控件的名称，点击添加）

二、鼠标左键点击左上角图标不放

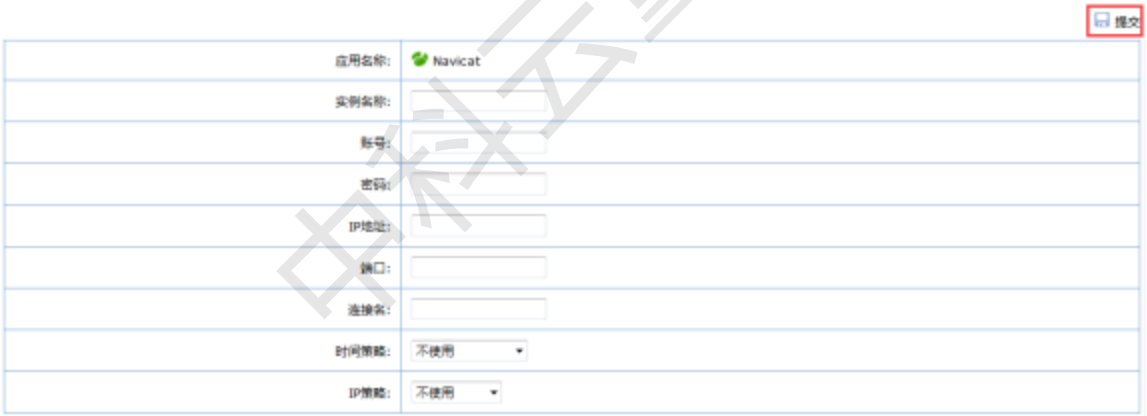
三、移动到相对应的控件中，松开鼠标左键

录制完成后，启用保存按钮，点击保存按钮后，成功将相应的控件保存到应用资源中。

2. 查询资源，在  文本框输入资源名称进行查询。

3. 删除资源，在应用资源数据条目中点击“  ”

4. 创建实例，在需要创建实例的应用资源中点击“  ”，在创建实例页面中输入实例属性，点击“提交”，如下图：



3.3.3 应用实例

应用实例能对资源实例进行管理，可查询、修改、删除资源实例。

1.查询实例，在  文本框输入实例名称进行查询。

2.修改实例，点击数据条目中的“ 修改 ”，在编辑界面中编辑应用实例属性，编辑完成后点击“提交”。

3.删除实例，在应用实例数据条目中点击“ 删除 ”。

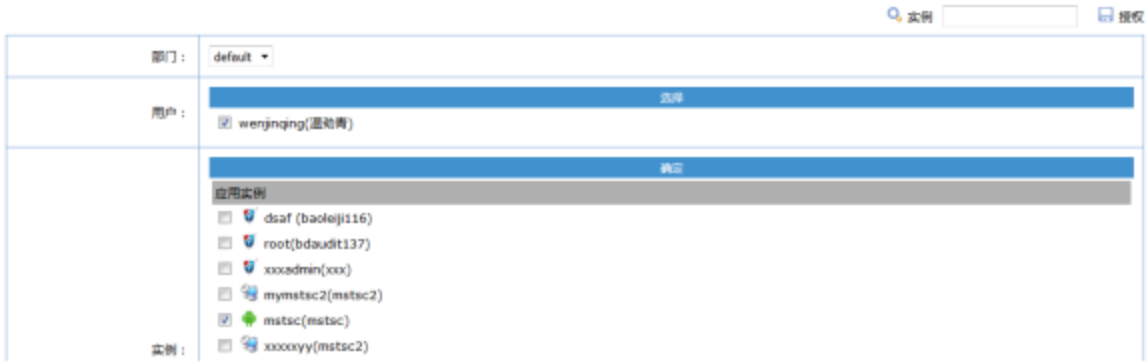
3.3.4 应用授权

应用授权可对应用资源的权限进行管理，可查询、删除、配置用户应用实例权限。

1.查询授权，在  文本框输入授权属性进行查询。

2.删除授权，在资源授权数据条目中点击“ 删除 ”。

3.配置授权，点击“ 配置 ”，在访问配置页面中勾选用户和实例，点击“授权”，如下图所示：



3.3.5 应用跳板机

应用跳板机用于添加和访问应用资源的跳板，通过访问它可以实现应用资源的添加和访问。应用跳板机页面可查询、修改、删除、添加应用跳板机。

1.查询应用跳板机，在  文本框输入跳板机属性进行查询。

2.修改应用跳板机，点击数据条目中的“ 修改 ”，在编辑界面中编辑应用跳板机属性，编辑完成后点击“保存”。

3.删除应用跳板机，在应用跳板机数据条目中点击“ 删除 ”。

4.添加应用跳板机，点击“ 添加跳板机 ”，在创建跳板机页面中输入跳板机属性，点击保存，如下图所示：

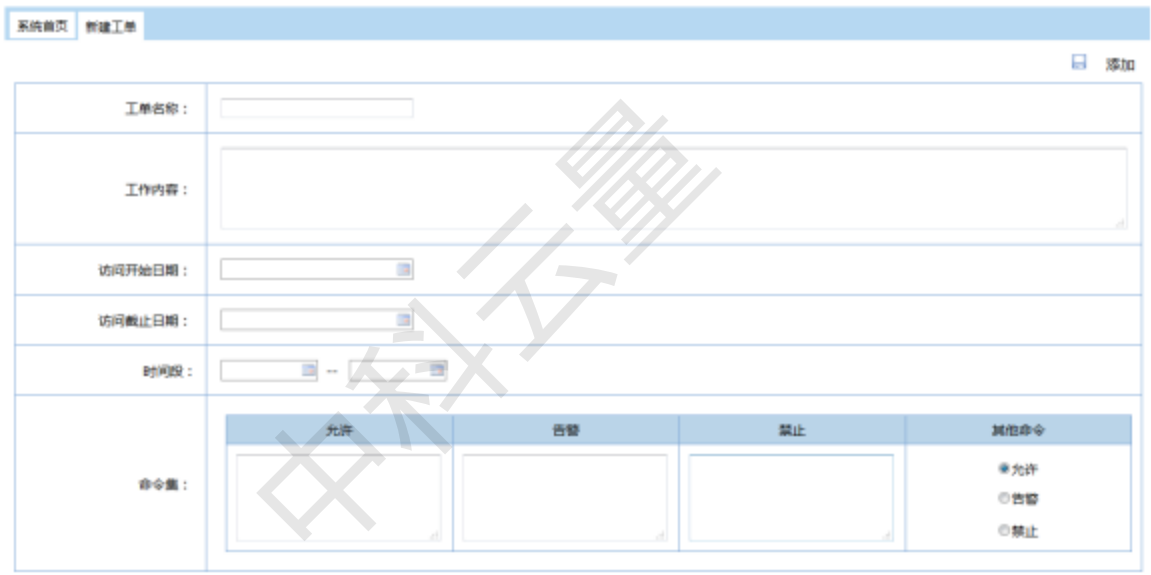
3.4 工单管理

通过“工单管理”，管理员可创建普通用户访问设备的工单，工单创建后，授权用户可在工单管理中访问相应的设备。普通用户可发起访问设备的申请，待管理员审核通过后，用户可在已完成审批中访问申请的设备。

3.4.1 工单管理

管理员可在工单管理中添加工单，定义工单的访问时间段，访问工单执行的命令。分配设备资源供用户访问。

1.添加工单，点击“ 添加工单 ”，在新建工单页面中输入工单名称，工作内容，访问开始时间、访问结束时间等信息，点击“添加”，如下图：



2.分配资源，点击“ 分配资源 ”，在分配资源页面中勾选用户和设备，点击保存。

3.删除用户，点击数据条目中的“⊞”展开工单，点击用户中的“ 删除 ”，删除用户访问工单的权限。

4.删除设备，点击数据条目中的“⊞”展开工单，点击设备中的“ 删除 ”，删除用户访问工单中的设备。

5.删除工单，点击数据条目中的 “ 删除 ” 。

3.4.2 待处理审批

管理员可在待处理审批中同意或拒绝普通用户的访问设备申请，可删除多余的访问设备。

1. 同意，点击“ 同意 ”，通过审批，申请人可连接审批中对应的设备。

2. 拒绝，点击“ 拒绝 ”，拒绝审批，申请人在审批拒绝后不能访问审批中对应的设备。

3. 删除设备，点击数据条目中的“ ⊞ ”展开审批，点击设备中的“ 删除 ”，删除审批中不希望被申请人访问的设备。

3.4.3 已完成审批

管理员可在已完成审批中查看审批记录，包括审批详情、访问时间段、申请人、状态等。

3.5 自动运维

通过“自动运维”，管理员可创建并配置设备的自动运维策略，以达到在指定设备中定期执行命令或脚本的目的。

3.5.1 运维策略

管理员可在运维策略中添加运维策略及配置运维设备，以达到定时在目标设备上执行命令或脚本的目的。

1.添加策略，点击“ ✚ 添加策略 ”，在创建自动化页面中输入策略名称，执行任务的时间、策略类型、自动化运维策略内容等信息，点击“保存”，如下图：

2.配置，点击“ ✚ 配置 ”，在策略授权页面中勾选需要自动运维的设备，点击“授权”。

3.修改，点击数据条目中的“ 修改 ”，修改自动运维策略。

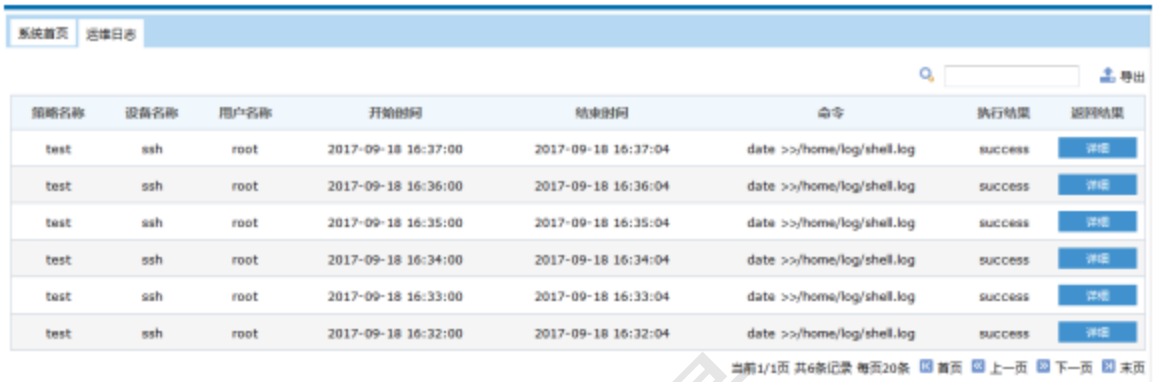
4.删除设备，点击数据条目中的“ ⊞ ”展开自动化运维策略，点击设备中的“ 删除 ”，删除设备后，该自动化运维策略在删除的设备中不会执行。

5.删除自动化运维策略，点击数据条目中的“ 删除 ”，删除自动化

运维策略。

3.5.2 运维日志

管理员可在运维日志查看自动化运维的执行历史，包括设备名称、执行命令、执行结果、返回结果等。



1.返回结果详情，点击返回结果列中的“ 详细 ”，查看自动化运维执行后返回的结果。

3.6 安全防护

通过“安全防护”，管理员可以进行策略管理、密码策略、时间策略、IP 策略、批量修改密码等。

3.6.1 策略管理

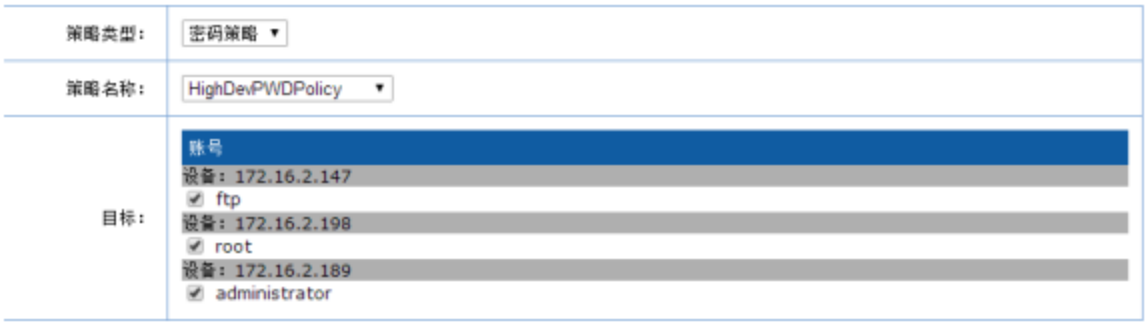
策略管理是定时修改设备的用户密码策略、时间策略、IP 策略的统一管理，同时可以配置策略的应用范围。

1.策略列表显示策略名称、策略类型、所有者、详情，点击“ 查看所有者 ”能显示出所有策略名称及策略应用访问。

2.选择策略，点击“查看”可显示该策略的所有者。

3.选择策略，点击“详情”可查看该策略对应的相关设置。

4.点击“配置”，可以根据策略类型配置策略的应用范围。例如：密码策略，选择策略名称、目标设备以及对应的帐号。

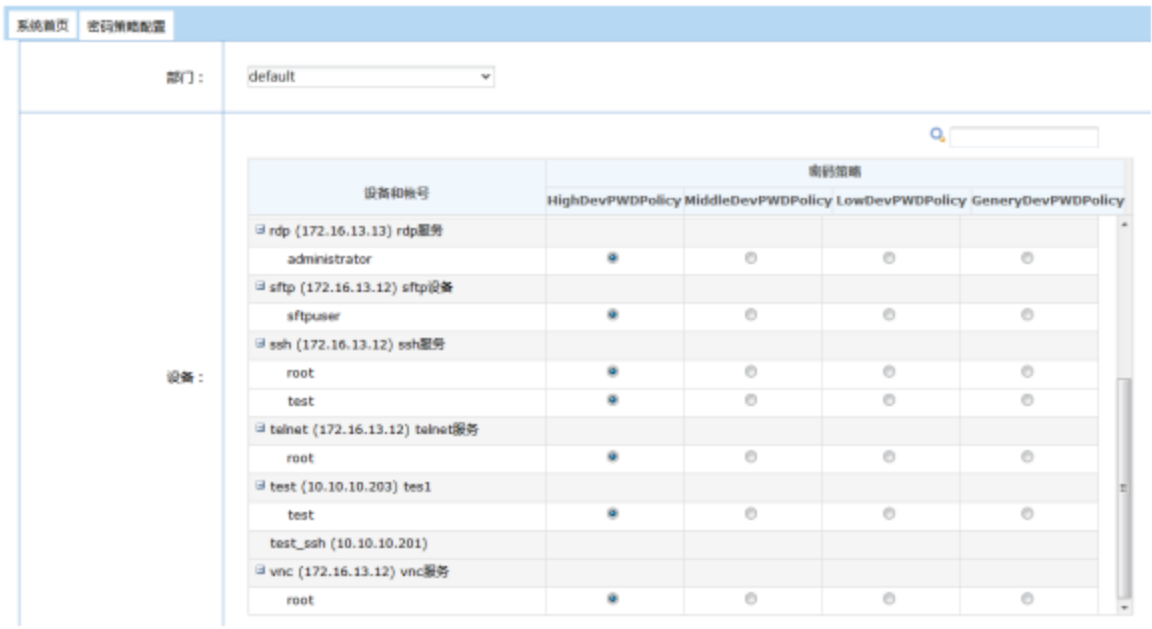


3.6.2 密码策略

密码策略包括两种密码策略，一种用户密码策略，是指系统在创建新用户时，可以自动为用户生成随机密码；另外一种是帐号密码策略，是指被保护的设备资源中的帐号定期修改密码的策略，默认包括：策略的应用在设备的帐号设置中。

1.选择密码策略，点击“修改”可设定密码修改策略，包括：策略名称、策略类型、有效日期、最小长度、包含数字位数等参数，策略的应用是在策略管理中。如下图所示：

2.配置，点击“ 配置 ”，进入密码策略的配置页面，选择设备与密码策略的对应关系，配置密码策略，如下图：



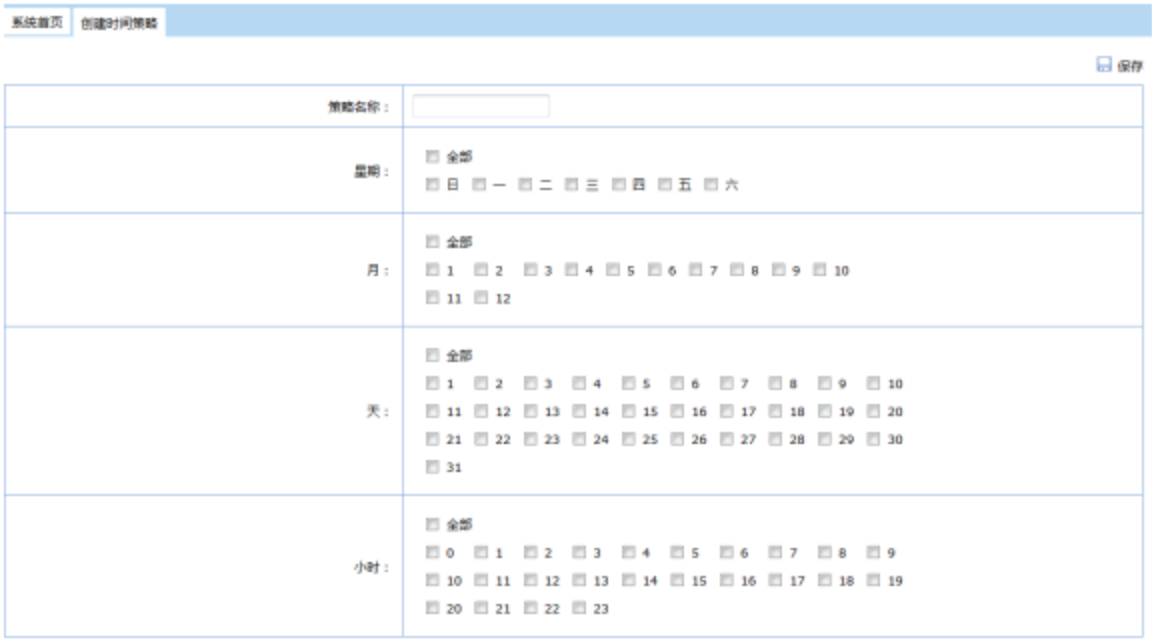
3.6.3 时间策略

通过“时间策略”，可以设置用户在哪个时间段可以管理、访问设备。可以对策略进行修改、删除。

1.点击“ ⊞ ”可显示该策略的所有者。

2.创建时间策略。

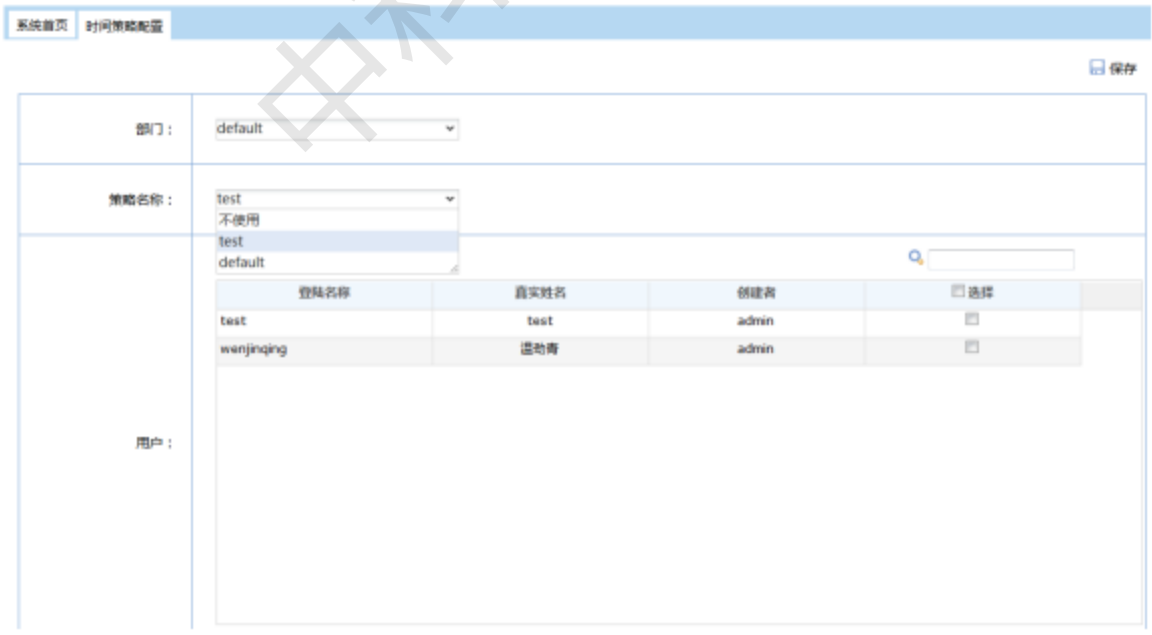
“策略名称”可自定义；时间细分为“星期”、“月”、“天”、“小时”、“分钟”；每个时间可以选择“全部”，也可以根据具体时间选择单项或多项，如下图所示。



3.修改、删除策略。

点击“修改”，可以修改时间策略；点击“删除”，可以删除时间策略。

4.配置，点击配置按钮，进入时间策略配置页面，在策略名称下拉框中选择需要配置的策略，如果需要配置用户的时间策略，则勾选用户；如果需要配置设备的时间策略，则勾选设备，勾选完毕后，点击保存，如下图：



3.6.4 防绕策略

管理员可在防绕策略中创建、配置防绕策略，用于针对设备的访问进行记录、

阻断等。

1.创建，点击 “ ✚ 创建 ”，进入创建防绕策略页面，输入策略名称、规则、阻断、日志等，点击保存。

2.配置，点击配置按钮，进入防绕策略配置页面，在策略名称下拉框中选择需要配置的策略，勾选设备，勾选完毕后，点击保存，如下图：

3. 删除设备，点击数据条目中的“ ⊞ ”展开防绕策略，点击设备中的“ 删除 ”，删除设备后，该防绕策略在删除的设备中不会执行。

4. 修改防绕策略，点击数据条目中的“ 修改 ”，修改防绕策略。

5. 删除防绕策略，点击数据条目中的“ 删除 ”，删除防绕策略。

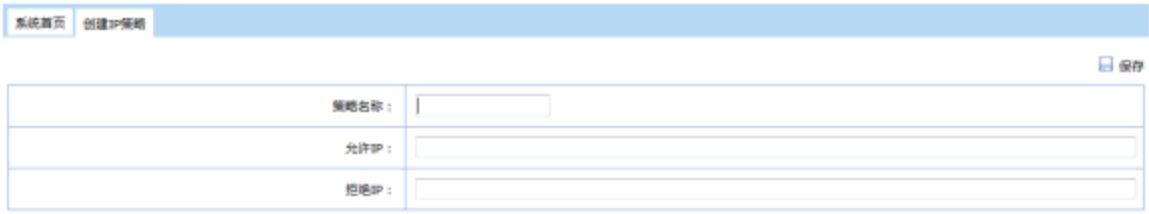
3.6.5 IP 策略

通过“IP 策略”，可以设置指定 IP 可以允许或者进行管理、访问设备资源。

1. 点击 IP 策略中的“ ⊞ ”可显示该策略的所有者。

2. 创建 IP 策略

‘策略名称’可自定义；‘允许 IP’、‘拒绝 IP’可根据需要设定。



3.修改、删除策略。

点击“修改”，可以修改 IP 策略；点击“删除”，可以删除 IP 策略。

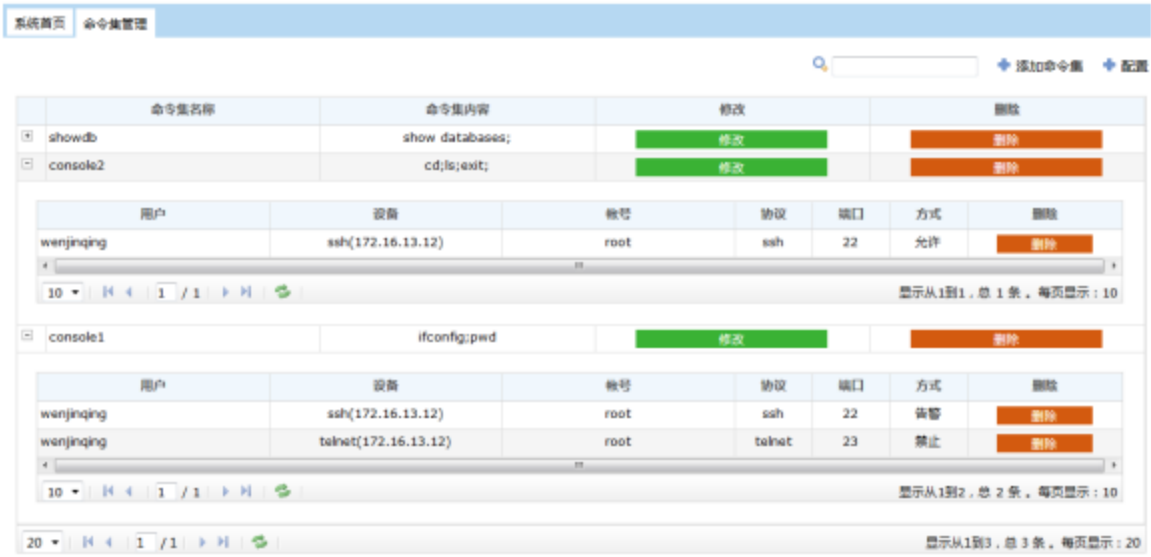
4.配置，点击配置按钮，进入 IP 策略配置页面，在策略名称下拉框中选择需要配置的策略，如果需要配置用户的时间策略，则勾选用户；如果需要配置设备的时间策略，则勾选设备，勾选完毕后，点击保存，如下图：

5.删除用户的 IP 策略，点击 IP 策略中的“ ⊞ ”，展开 IP 策略配置详情，点击用户对应的“ 删除 ”

6. 删除设备的 IP 策略，点击 IP 策略中的“ ⊞ ”，展开 IP 策略配置详情，点击设备对应的“ 删除 ”

3.6.6 命令防火墙

命令防火墙可添加命令集、配置命令防火墙，可以对已创建访问关系的用户操作进行命令级的过滤，实现每个用户在不同设备上实现不同帐号的细节控制。如下图：



1.查询命令防火墙，在  文本框输入用户、设备、帐号、协议、命令集进行查询。

2.添加命令集，点击“ ✚ 添加命令集 ”，进入添加命令集页面，输入命令集属性后点击“保存”。

3.配置命令防火墙，点击“ ✚ 配置 ”，进入命令集的配置页面，选择命令集，展开授权关系，勾选授权关系,如下图：

如果“允许”栏勾上，表示只能执行“命令集”所选中的命令集中配置的命令。

如果“禁止”栏勾上，表示不能执行“命令集”所选中的命令集中配置的命令。

如果“告警”栏勾上，表示执行“命令集”所选中的命令集中配置的命令时有拦截告警日志。

如果“取消”栏勾上，表示不启用执行“命令集”所选中的命令集中配置的命令。

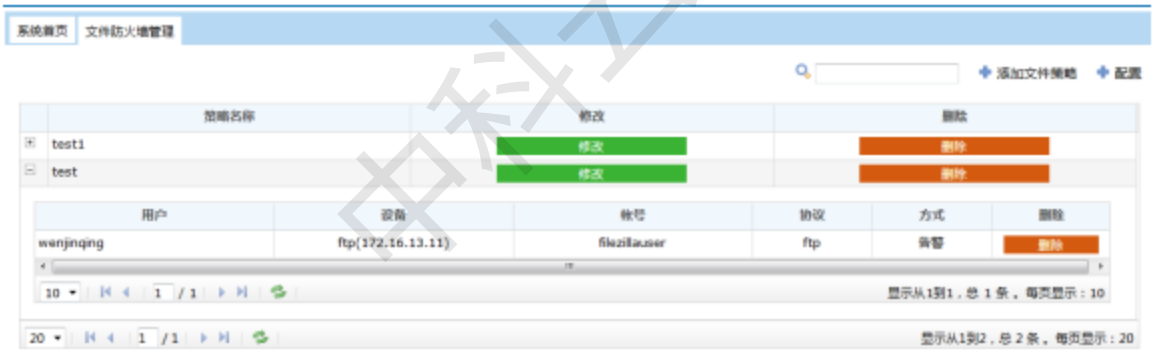
4.修改命令集，点击数据条目中的“修改”，可修改命令集。

5.删除命令集，点击数据条目中的“删除”，可删除命令集（如果命令集正在使用，则不能删除）。

6.删除设备，点击命令集中的“ ⊞ ”，展开命令集配置，点击设备中的“删除”，删除设备，删除设备后访问该设备将不再执行命令防火墙规则。

3.6.7 文件防火墙

文件防火墙可添加文件策略、配置文件防火墙。配置文件防火墙规则后，可以对已创建关系的 ftp、sftp、rdp、vnc 设备传输的文件进行告警、拦截。



1.查询文件防火墙，在  文本框输入策略名称进行查询。

2.添加文件策略，点击“ ✚ 添加文件策略 ”，进入添加文件防火墙策略页面，编辑文件防火墙策略属性，点击“保存”。

3.配置文件防火墙，点击“ ✚ 配置 ”，进入文件防火墙配置页面，选择文件策略、授权关系，如下图：

4. 修改文件策略，点击数据条目中的“ 修改 ”，修改文件策略。

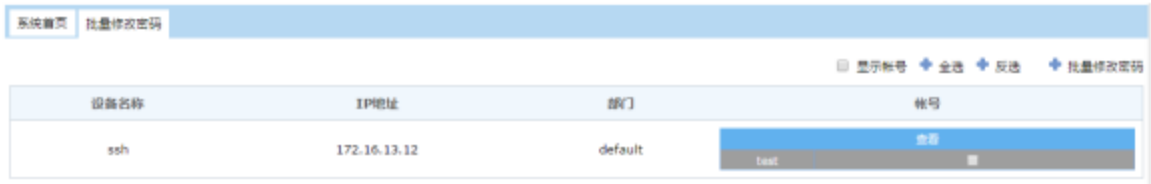
5. 删除文件策略，点击数据条目中的“ 删除 ”，删除文件策略。

6. 删除设备，点击数据条目中的“ ⊞ ”，展开文件防火墙配置，点击“ 删除 ”。

3.6.8 批量修改密码

批量修改密码，是指添加设备的帐号时，如果选择定期修改密码，那么设备的帐户会根据密码策略定期修改密码，同时也可以批量修改设备的帐号密码。

1. 点击“ ☑ 显示账号 ”显示定期修改密码的设备帐号。



2. 点击“ ✚ 全选 ”可以全选所有设备的所有帐号；点击“ ✚ 反选 ”可以反选所有设备的所有帐号，也可以单选、多选设备的帐号，然后点击“ ✚ 批量修改密码 ”，修改设备的帐号密码。密码修改成功后或者失败，有对应的提示。

注意：

- **定期修改密码的帐号，才可以在批量修改密码才有效。**
- **当定期修改或者批量修改设备帐号的密码时，修改后的密码会发送到管理员的邮箱。**

只有 linux、windows、还有网络设备，能够定时、批量修改密码，同时这些设备还必须要启动了 telnet 或者 ssh。

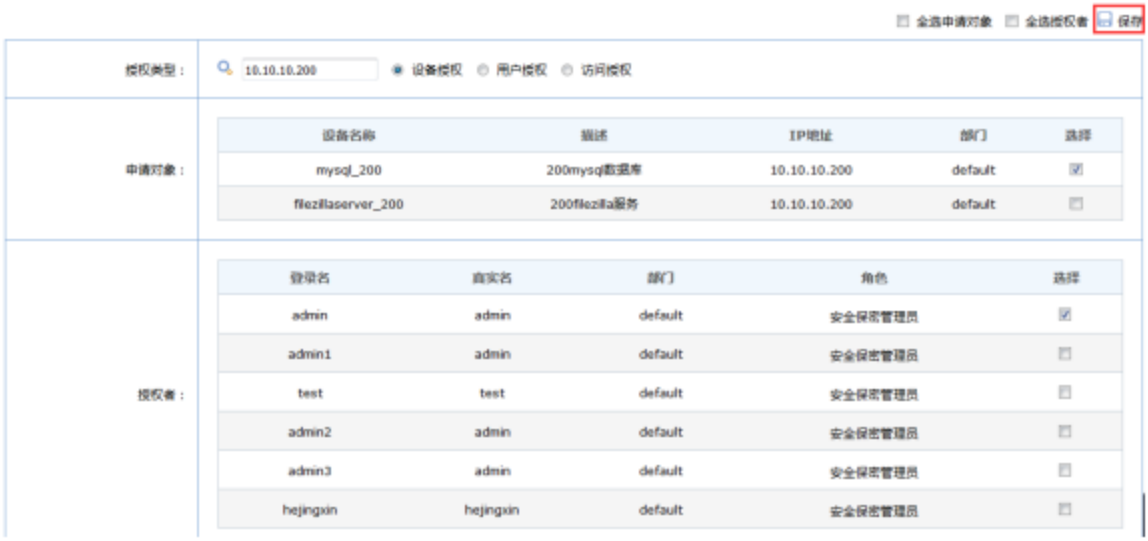
3.6.9 双授权管理

双授权管理用于配置用户访问设备的双授权规则，在添加设备并对设备授权后，可添加“设备”、“用户”、“访问”三种类型的双授权规则，在配置该规则后，相应规则内的用户访问设备时，将发起访问设备的请求，由相应规则指定的安全保密管理员通过请求后，用户才能正常访问相应的设备。双授权管理页面可查询、删除、配置双授权规则。

1.查询双授权，点击选择设备类型，在  文本框输入双授权属性进行查询。

2.删除双授权，在双授权数据条目中点击“ 删除 ”。

3.配置授权，点击“ 配置 ”，进入双授权配置页面，选择授权类型，勾选“申请对象”和“授权者”，点击“ 保存 ”，如下图：



3.6.10 证书管理

证书管理用于配置用户登录系统时使用的证书，可创建、删除、下载、证书，也可将证书发送到该用户的邮箱上。

1. 查询证书，在  文本框输入证书属性进行查询。

2. 删除证书，在证书数据条目中点击“ 删除 ”。

3. 创建证书，点击证书数据条目中的“ 创建 ”，系统生成该用户对应的证书。

4. 下载证书，点击证书数据条目中的“ 下载 ”，下载该证书到本地。

5. 发送证书，点击证书数据条目中的“ 发送 ”，发送该证书到用户对应的邮箱中。

3.6.11 动态口令管理

动态口令管理用于配置用户登录系统时使用的动态口令，可生成、查看、下

载动态口令二维码，也可将动态口令二维码发送到该用户的邮箱上。

1.查询动态口令，在  文本框输入动态口令属性进行查询。

2.生成/更新动态口令，在动态口令数据条目中点击“ 生成 ”，可生成动态口令，也可更新动态口令（让旧的口令失效，使用新的动态口令）。

3.查看动态口令，点击证书数据条目中的“ 查看 ”，可查看该动态口令的二维码。

4.下载动态口令，点击动态口令数据条目中的“ 下载 ”，下载该动态口令到本地。

5.发送动态口令，点击动态口令数据条目中的“ 发送 ”，发送该动态口令到用户对应的邮箱中。

3.7 日志审计

3.7.1 会话浏览

“会话浏览”默认浏览最新的会话，状态分为完成或中止，点击“中止”则可以中止活动的会话；点击“详细”可以浏览会话的详细内容。

会话在活动中，点击“监控”按钮，可以监控会话的操作情况。

如果会话类型是字符类，如 SSH、TELNET、DB，则可以点击“详细”或“下载”查看操作内容；进入“详细”点击“播放”，可回放 SSH、TELNET、DB 操作。

如果会话类型是图形类，如 RDP、VNC，点击“播放”，可查看操作录像。

注意：查看详情、播放操作录像、监控操作录像时，如果浏览器阻止弹出的窗口，请允许所有弹窗。

3.7.2 应用浏览

“应用浏览”默认浏览最新的会话，状态分为完成或中止，点击“中止”则可以中止活动的会话；点击“播放”可以浏览应用会话的详情。

会话在活动中，点击“监控”按钮，可以监控会话的操作情况。

点击“播放”，可回放应用会话操作。

点击“下载”，可将应用会话操作保存到本地。

注意：查看详情、播放操作录像、监控操作录像时，如果浏览器阻止弹出的窗口，请允许所有弹窗。

3.7.3 拦截日志

对已启用命令防火墙的用户设备，所有触发命令防火墙的命令集中命令都会在拦截记录体现，包括禁止的拦截记录、告警记录、除了允许命令外其他命令的禁止记录。

1.日志拦截记录的显示方式，在拦截记录界面的显示方式有按时间排、按用户排、按帐号排、按源 IP 排、按目标 IP 排、按状态排、是否触发规则；拦截记录包括拦截时间、用户、帐号、源 IP、目标 IP、登录方式、类型，触发规则，触发命令。

说明：

“拦截时间”是指触发命令防火墙命令集中命令，受拦截的实时时间。

“用户”是指授权访问设备资源的用户。

“帐号”是指设备资源的帐户。

“源 IP”是指访问设备资源的客户端 IP 地址。

“目标 IP”是指被访问的设备资源地址。

“类型”是指命令防火墙的拒绝方式，包括允许、告警、拦截、禁止。

“触发规则”是指触发到命令防火墙的规则名称。

“触发命令”是指触发到命令防火墙的规则里面具体的命令。

2.导出拦截记录，点击“ 导出 ”，可以用 excel、html 的格式导出拦截记录。

3.7.4 防绕日志

启用防绕后，防绕规则中阻断、记录的日志可在该界面查询。

1.“显示”用于筛选界面显示的防绕类型对应的数据，包括网络防绕、会话防绕。勾选后显示该类型的防绕日志。

2.“排序”，用于对日志结果进行排序，默认按时间排序，勾选相应的排序方式后，日志将按相应的方式进行排序。

说明：

“防绕时间”是指用户不通过堡垒机连接防绕规则中的设备，触发防绕的时间。

“客户 IP”是指用户访问防绕规则中设备所使用的计算机 IP。

“设备”是指用户使用的客户端。

“登录时间”是指用户访问设备发起连接的时间。

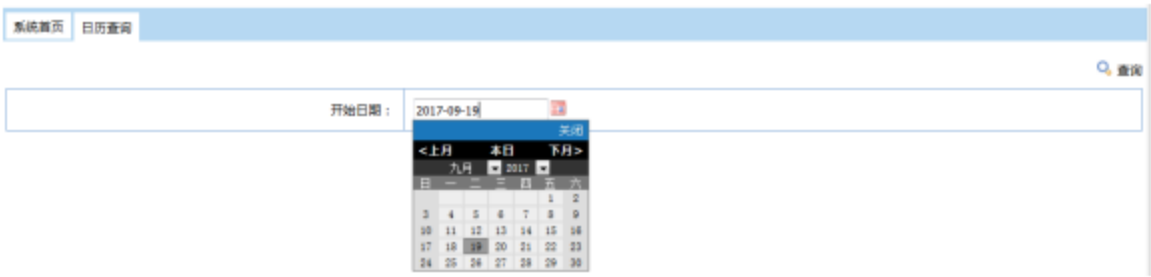
“操作”是指触发防绕规则后执行的动作，包括阻断、记录。

“状态”是指执行防绕的结果。

3.“导出”用户将防绕日志导出到本地。

3.7.5 日历查询

可很方便的通过日历查询会话。查询时需指定‘开始日期’，如下图所示：



3.7.6 命令查询

命令查询，可很方便的查询执行过的指令及其输出等相关命令的会话。查询时需指定“开始日期”和“结束日期”，“用户”、“帐号”、“源 IP”和“关键字”的选项可填单个或多个，它们之间为与关系。如下图所示：

说明：

“**开始日期**”是指会话的开始时间。

“**结束日期**”是指会话的结束时间。

“**用户**”是指访问设备资源的用户。

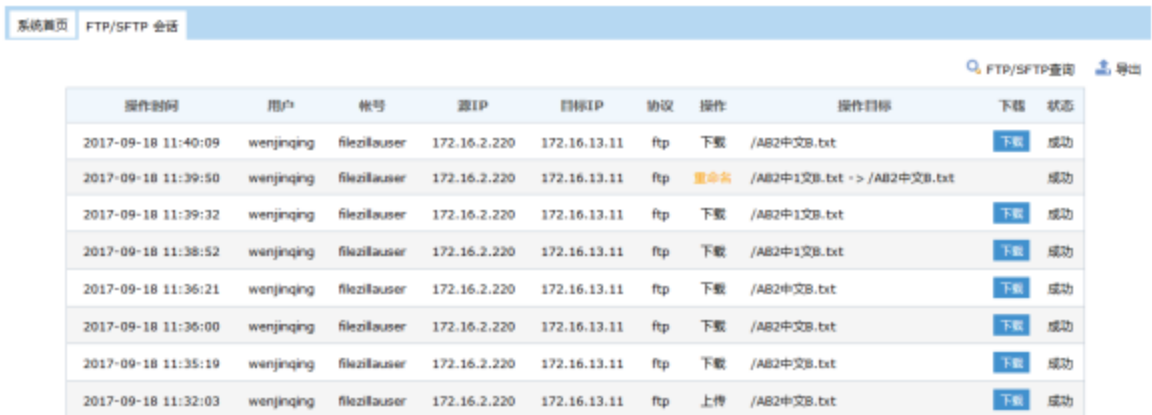
“**帐号**”是指设备的资源的帐号。

“**源 IP**”是指访问设备资源的用户的 IP 地址。

“**关键字**”是指访问设备资源的用户执行相关命令的关键字。

3.7.7 FTP 会话

“FTP 会话”可以浏览最新的 FTP/SFTP 会话信息，用以查看某用户授权的访问关系登录到 FTP 服务器后的下载、上传、删除、重命名的操作记录。FTP/SFTP 的会话信息包括：操作时间、用户、帐号、源 IP、目标 IP、协议、操作、操作目标、状态，如下图所示：



1.点击“ FTP/SFTP查询 ”，可以跳转进入 FTP/SFTP 查询页面，详细查询

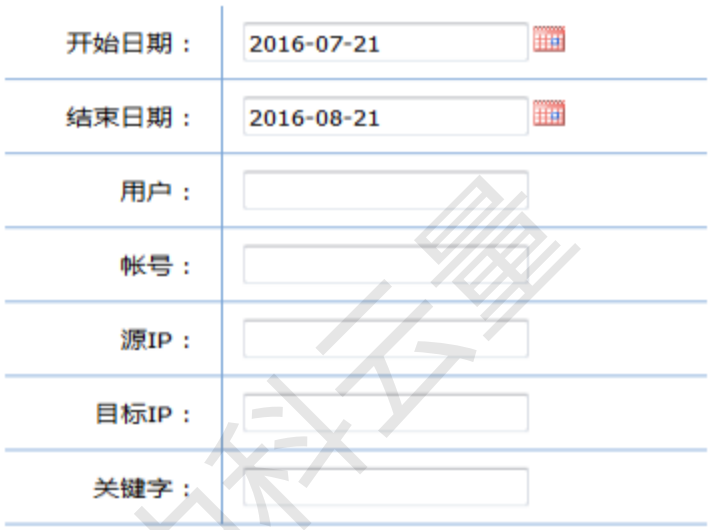
方法请参考下一节的《3.7.8 FTP 查询》。

2.导出操作日志。

点击“导出”，以 excel、html 格式导出 FTP 会话日志。

3.7.8 FTP 查询

可很方便查询用户登录 FTP/SFTP 后的操作。查询时需指定‘开始日期’和‘结束日期’，‘用户’、‘帐号’、‘源 IP’和‘关键字’的选项可填单个或多个，它们之间为与关系。如下图所示：



说明：

“**开始日期**”是指 FTP/SFTP 会话的开始时间。

“**结束日期**”是指 FTP/SFTP 会话的结束时间。

“**用户**”是指登录 FTP/SFTP 会话的授权管理设备资源的用户，

“**帐号**”是指被访问的设备资源的帐号。

“**源 IP**” 是指授权管理设备资源用户的 IP 地址。

“关键字”是指操作目标的目录名或者文件名中的任何字眼，例如上传 test.txt 文件，关键字为“test”。

3.7.9 登录日志

通过浏览“登录日志”，可以了解所有用户的登录情况，在  文本框输入用户名称、IP 地址、登录类型、登录时间

进行查询，如下图所示。

用户名称	IP地址	登录类型	登录时间	登录状态
auditor	172.16.2.220	web	2017-09-18 15:55:29	成功
auditor	172.16.2.220	web	2017-09-18 15:11:59	成功
test1111	172.16.2.220	web	2017-09-18 14:41:25	成功
auditor	172.16.2.220	web	2017-09-18 14:30:53	成功
auditor	172.16.2.220	web	2017-09-18 14:00:06	成功
auditor	172.16.2.220	web	2017-09-18 11:33:32	成功
auditor	172.16.2.220	web	2017-09-18 09:17:39	成功
auditor	172.16.2.220	web	2017-09-18 09:09:45	成功
auditor	172.16.2.220	web	2017-09-18 09:04:38	成功
auditor	172.16.2.220	web	2017-09-16 17:08:51	成功
auditor	172.16.2.220	web	2017-09-16 17:04:15	成功
auditor	172.16.2.220	web	2017-09-16 16:42:29	成功
auditor	172.16.2.220	web	2017-09-16 16:41:29	成功

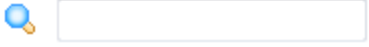
注意：三权分立，安全保密员可以看到安全审计员的登录日志；系统管理员没有查看登录日志的权限；安全审计员可以查看到系统管理员、安全保密员和普通用户的登录日志。

3.7.10 操作日志

通过“操作日志”可以审计系统管理员、安全保密管理员、审计管理员等用户的活动情况，操作日志列表包括：用户、操作时间、操作 IP、操作类型、操作对象。如下图所示：

用户	操作时间	操作IP	操作类型	操作对象
auditor	2017-09-18 16:10:12	172.16.2.220	修改	用户：test1111
test1111	2017-09-18 14:43:10	172.16.2.220	导出	Ftp信息
auditor	2017-09-18 14:41:09	172.16.2.220	修改密码	用户：test1111
auditor	2017-09-18 14:41:01	172.16.2.220	新增	用户：test1111
auditor	2017-09-18 14:40:42	172.16.2.220	删除	用户：test1111
auditor	2017-09-18 14:40:36	172.16.2.220	修改	用户：test1111
auditor	2017-09-18 14:36:16	172.16.2.220	修改密码	用户：test1111
auditor	2017-09-18 14:32:38	172.16.2.220	重置密码	用户：test1111
auditor	2017-09-18 14:32:30	172.16.2.220	重置密码	用户：test1111
auditor	2017-09-18 14:31:30	172.16.2.220	重置密码	用户：test1111
auditor	2017-09-18 14:31:16	172.16.2.220	新增	用户：test1111
auditor	2017-09-18 14:00:22	172.16.2.220	导出	防火墙日志记录
auditor	2017-09-16 17:09:24	172.16.2.220	修改密码	用户：auditor
auditor	2017-09-16 17:04:50	172.16.2.220	修改密码	用户：auditor

当前1/1页 共14条记录 每页20条 首页 上一页 下一页 末页

1.查询操作日志，在  文本框输入用户、操作时间、操作 IP、操作类型、操作对象进行查询。

2.导出操作日志。

点击“导出”，以 excel、html 格式导出操作日志。

注意：

- **三权分立，安全保密员可以看到安全审计员的操作日志；系统管理员没有查看操作日志的权限；安全审计员可以查看到系统管理员和安全保密员的操作日志。授权管理员的操作日志不包括：FTP/SFTP 文件操作；WEB 登录日志；SSH、Telnet 退出日志；远程 rdp、vnc 的登录日志、，命令防火墙的日志。**

3.7.11 双授权日志

通过浏览“双授权日志”，可以了解所有用户的双授权情况，在  输入双授权日志属性进行查询，如下图所示。

3.7.12 访问统计

通过访问统计，可以统计用户访问设备的统计数，内容包括：用户名、开始时间、结束时间、访问次数。同时可以对用户的访问统计进行筛选、导出用户访问统计日志。

1.用户访问统计筛选

选择‘开始时间’和‘结束时间’，点击“筛选”，便可对用户访问统计进行筛选。

2.导出用户访问统计日志，以 excel、html 格式导出用户访问统计日志。

3.7.13 密码查询

定期修改和批量修改设备帐号的密码，可以在密码查询，查询到相应的密码。内容包括：设备名称、帐号名、原密码、新密码、修改时间、修改状态，如下图所示。

报表查询是历史会话或当前会话管理的入口，是安全审计员（auditor）主要的查询和报表工具。查询的内容包括会话浏览、拦截日志、日历查询、命令查询、FTP 查询、登录日志、操作日志。

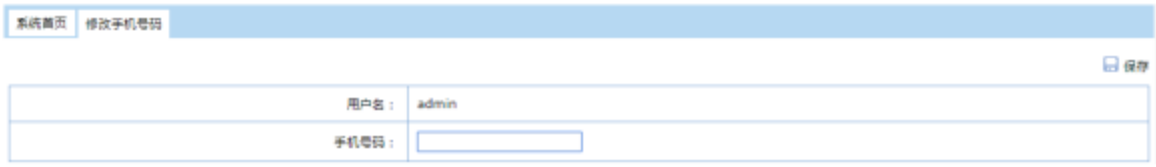
3.8 信息配置

3.8.1 修改邮箱

系统支持用户修改邮箱地址。

3.8.2 修改手机号码

系统支持用户修改手机号码。



3.8.3 密码修改

系统支持用户自行修改自身帐户的密码，如下图：

3.8.4 动态认证

系统支持用户修改自身帐户的动态认证方式，如下图：

“短信验证码”指定用户登录时验证短信验证码，验证通过后才能进入系统；
“动态口令”指定用户登录时验证用户的动态口令，选择该动态认证方式保存后，可查看、生成密钥，查看二维码，发送二维码（发送二维码到用户邮箱），用户登录时，输入的密码为：“静态密码+动态口令值”，验证通过后才能进入系统；
“数字证书”指定用户登录时验证用户的数字证书，选择该动态认证方式保存后，可创建、删除、下载证书，也可发送证书到用户的邮箱，用户必须在浏览器中导入了该证书文件后才能成功登录系统。
“USB KEY”指定用户登录时验证用户的 USB KEY，插入了 USB KEY 的计算机才能使用该用户登录。

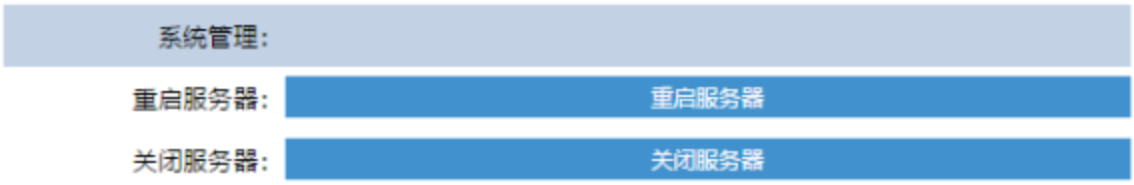
3.9 系统管理

用系统管理员（sysadmin）登录系统管理界面，系统管理由系统维护、时间设置、系统状态、邮件配置、网络配置、注册授权、退出系统组成。

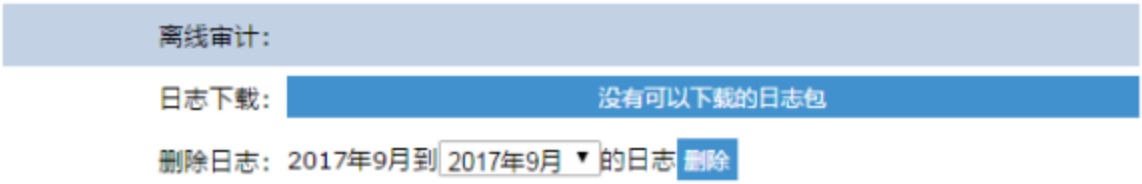
3.9.1 系统维护

通过“系统维护”可以进行系统管理、离线审计、配置管理、系统重置、系统升级、SOC、导出配置的格式设置、磁盘告警阈值。

1.系统管理：点击“重启服务器”的按钮， 可重新启动设备；点击的“关闭服务器”的按钮，可以关闭设备。

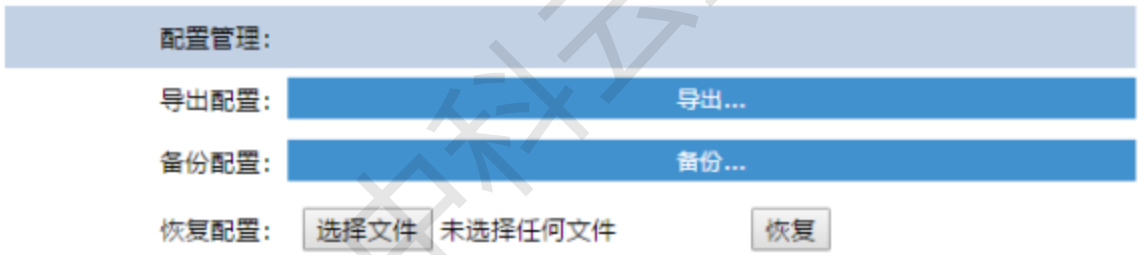


2.离线审计：点击“日志下载”，可以下载已有的日志包；选择日志的时间，点击“删除”可以删除月份的日志。



注意：日志下载是下载所有日志，删除日志是删除整月的日志。

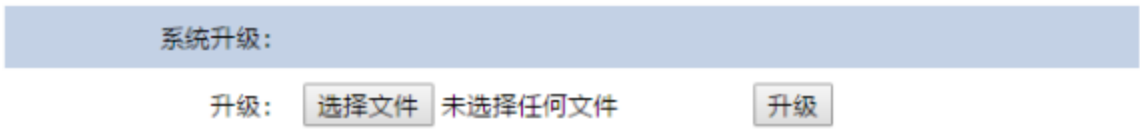
3.配置管理：点击“导出配置”，可以以 excle、html 格式导出配置数据，导出到客户端 PC 指定的存储地点，导出配置数据的格式在导出格式进行设置；点击“备份配置”，可以备份配置；选择已备份的配置文件，点击“恢复”，可以恢复配置。



4.系统重置：点击“系统重置”可将系统恢复到原始数据，现有数据会丢失。

注意：系统重置时，网络设置不会恢复到默认设置。

5.系统升级：点击“浏览”按钮，选择升级包，点击“升级”按钮，可以升级系统，升级成功后，有相应的提示。

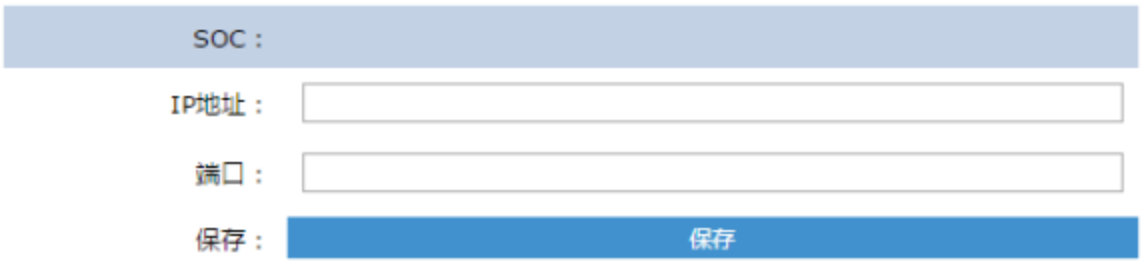


注意：升级包升级会自动校验文件内容，只有符合的文件内容，才能够升级成功。

6.系统超时设置：设置登录系统的超时时间，当达到设置的时间后将退出用

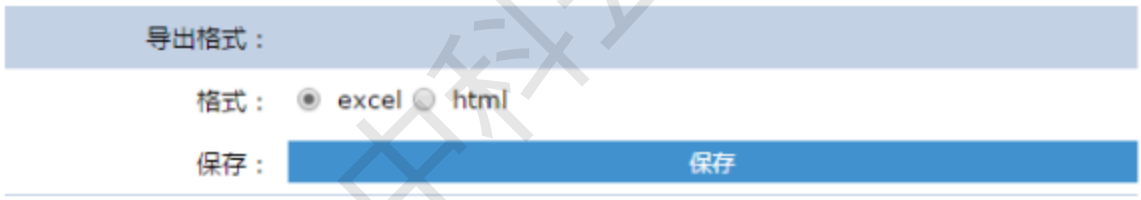
户的登录状态。

7.SOC：输入 SOC 系统的 IP 地址、端口，然后点击“保存”。设备可与 SOC 系统联动，让 SOC 管理。



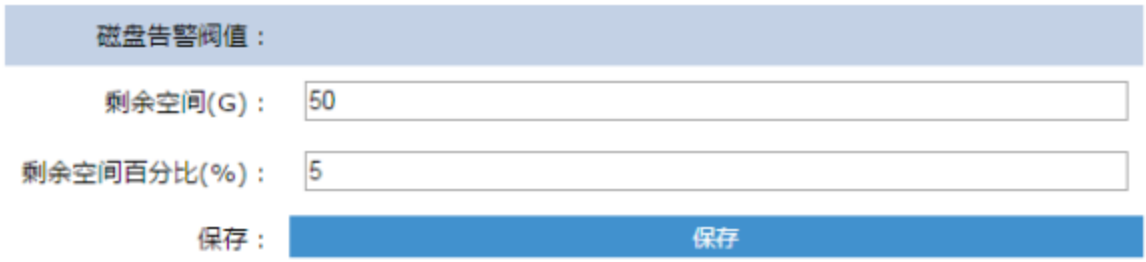
注意：SOC 的联动，是指帐号集中管理与审计系统中授权管理员的操作日志可以通过 syslog 上传到 SOC 设备，另外 SOC 可以通过 BDSEC 协议对帐号集中管理与审计系统进行关机、重启等管控操作。

8.导出格式：这里为导出配置设置、用户列表、设备列表、日志等报表导出的格式，包括 excel、html 两种格式。



9.登录验证码：选择禁用或启用登录时的验证码。

10.磁盘告警阈值：设置磁盘剩余空间容量大小，达到指定的剩余容量阈值时会报警；设置磁盘剩余空间容量的百分比，达到指定的剩余容量百分比阈值时会报警。报警的方式是通过发送邮件信息到系统管理员用户。



注意：设置磁盘告警阈值时，可以通过查看系统状态，查看磁盘空间容量的大小。

11.自动删除日志阈值：勾选删除记录，设置磁盘剩余空间容量大小，达到指定的剩余容量阈值时会自动删除日志；勾选删除记录，设置磁盘剩余空间容量的百分比，达到指定的剩余容量百分比阈值时会自动删除日志。保存日志时间，可以设置日志的时间，包括一个月、两个月、三个月、半年、一年。

注意：

- **保存日志是保存最近的时间，例如：保存一个月，即是保存最近一个月时间的日志。**
- **当同时设置剩余空间和剩余空间百分比时，系统读取较小值，进行删除日志。**
- **删除日志时，只是删除会话日志，而且会保存指当前时间之前的一天的日志。**

12.动态认证方式：选择启用或禁用指定的动态认证方式，勾选相应的动态认证方式保存后，启用相应类型的动态认证方式。

3.9.2 时间设置

通过“时间设置”可以设置帐号集中管理与审计系统的时间，输入系统时间，点击“同步”按钮，便可同步实时时间，包括与 NTP 时间服务器的设置，如下图所示；

3.9.3 系统状态

通过“系统状态”可以了解设备的运行情况，包括系统时间、cup 使用率、物理内存总量、使用的物理内存总量、空闲内存总量、用作内核缓存的内存量、磁盘总空间、磁盘已用空间、硬盘剩余空间。如下图所示：

注意：查看磁盘空间可以设置磁盘告警阈值。

3.9.4 邮件配置

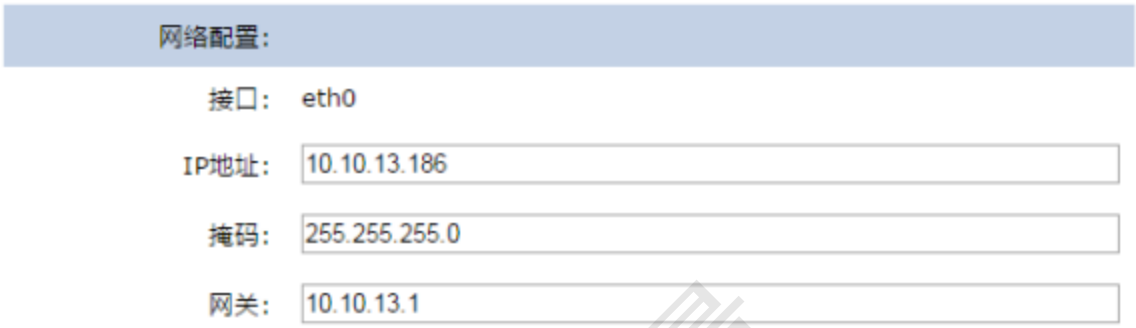
“邮件配置”能显示 SMTP 服务器、用户名和相关接收用户信息。

注意：邮件接收用户，勾选“用户”时，如果用户忘记登录密码，可以接收到新密码的邮件；勾选“安全保密管理员”时，当设备资源的帐号开启定期修改密码或者

批量修改密码时，修改后的密码，可以发送到安全保密管理的邮箱；磁盘空间告警是发送到系统管理员的邮箱。

3.9.5 网络配置

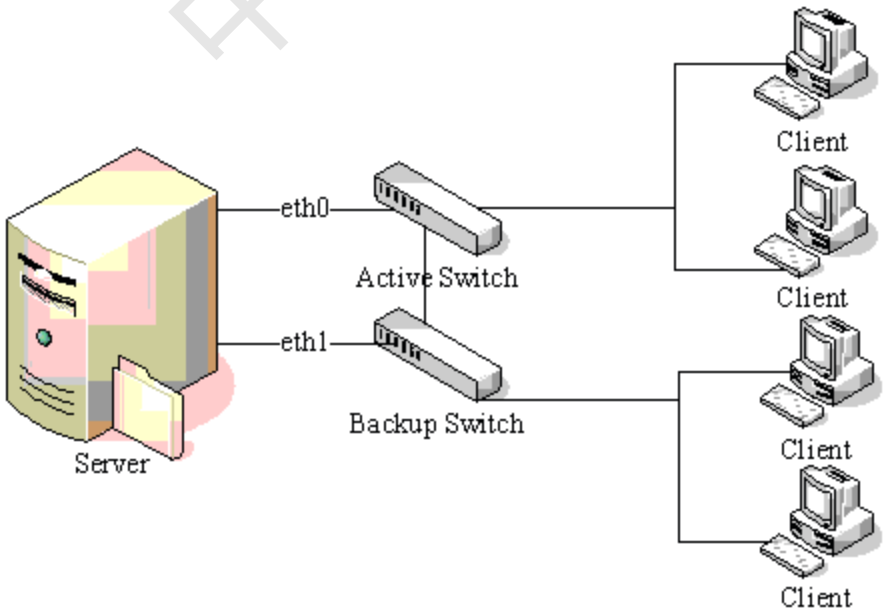
1.1.通过网络配置可以了解网络相关状态，包括设置网口的 IP、掩码、网关，默认管理口为 eth1，网络配置如下图所示：



注意：

- **修改网口后，点击“应用”按钮，会自动提示“修改网络配置后将重启设备，继续？”，点击“是”后，重新系统后，网口配置生效。**
- **网口不支持多个默认网关，只要设置一个默认网关即可。**

1.2.帐号集中管理与审计系统主备 IP（又叫冗余 IP，聚合 IP）模式配置。

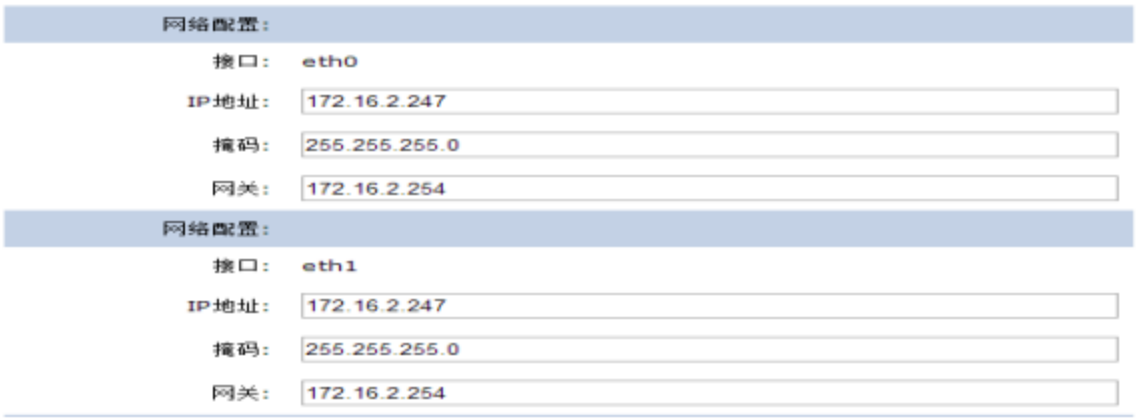


主备模式网络拓补图

帐号集中管理与审计系统通过 bond 技术，将系统设备中的两块物理网卡虚拟

为一块网卡，在平时只有一个设备处于活动状态，当一个宕掉（如主交换机断电等）另一个马上由备份设备转换为主设备，确保网络不会中断。

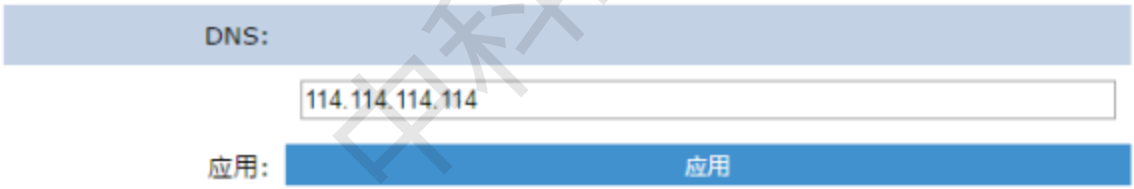
系统支持一组网口 IP 冗余（聚合），如下图 eth0 和 eth1。



注意：

- **配置冗余（聚合）IP 后，其它网口不能配置与冗余（聚合）IP 相同网段的 IP**
- **如果冗余（聚合）IP 中配置了网关，则其它网口都不能配置网关，否则冗余（聚合）IP 中配置的网关将失效，会导致冗余（聚合）IP 所在网段与其它网段不可达。**

2.配置 DNS,设置完 DNS 后，点击“应用”便可生效。



3.可信主机配置，可以设置允许、拒绝的 IP 地址或者网段，访问帐号集中管理及审计系统的管理界面，设置成功，点击“应用”，即可生效。

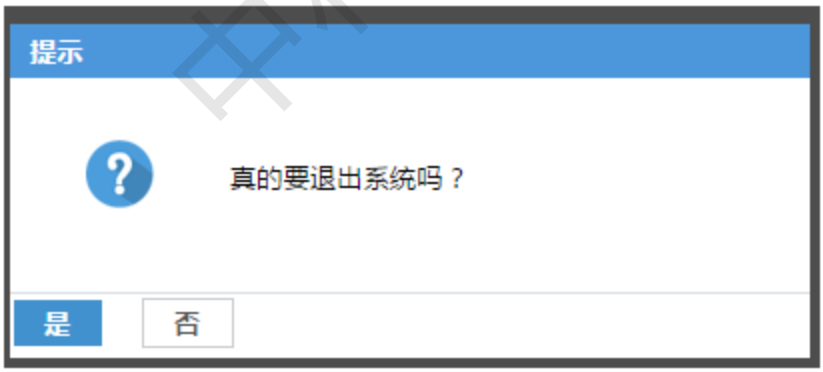
3.9.6 注册授权

通过“注册授权”了解设备的授权信息，如下图所示。

当没有授权时，下载授权申请，授权申请发给技术人员；收到授权证书后，导入授权证书进行授权。

3.9.7 退出系统

通过“退出系统”，可以从当前登录用户，退出系统登录。点击“退出系统”，提示“真的要退出系统吗”，点击确定后，退出系统，如下图所示。



3.9.8 域管理

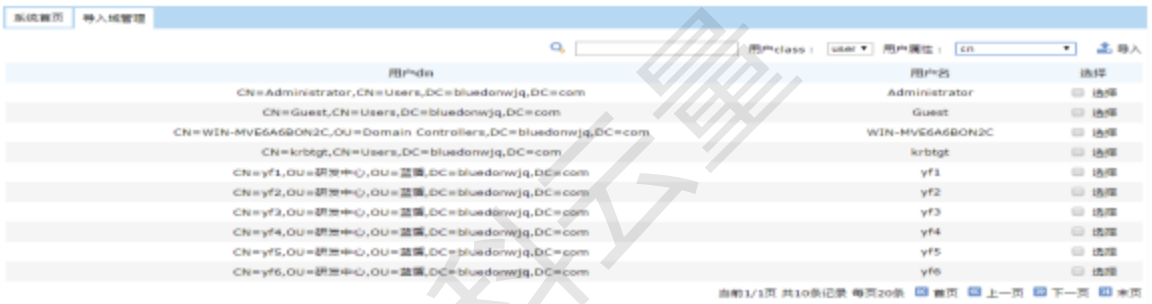
通过“域管理”，系统“安全保密管理员”可配置 AD、LDAP 域的相关信息，可将域用户导入到系统中。

1.添加域，点击“ 添加 ”，进入添加域页面，编辑域的属性后，点击“保存”。

2.修改域，点击“ 修改 ”，进入修改域页面，编辑域的属性后，点击“保存”。

3.删除域，点击“ 删除 ”，在弹出的对话框中点击“确定”。

4.导入域用户，点击“ 导入 ”，进入导入域管理页面，勾选域用户，点击“ 导入 ”，如下图：

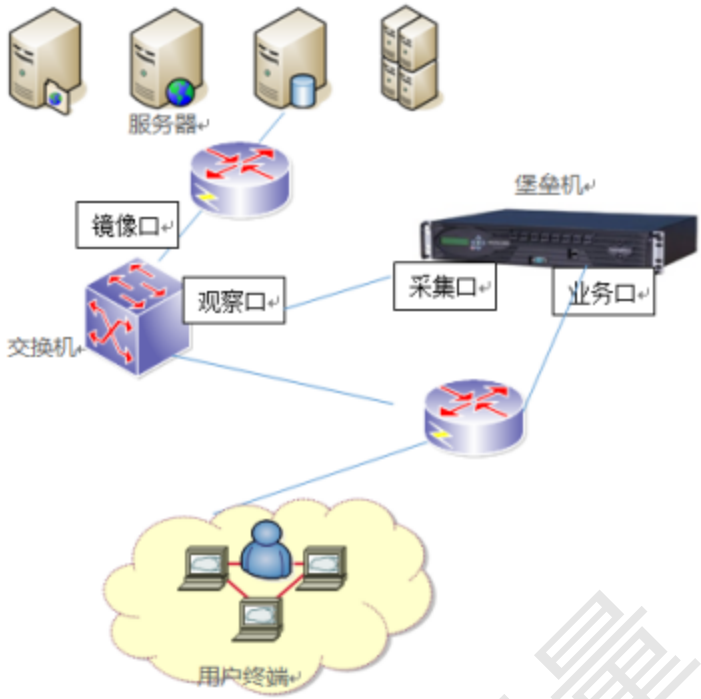


3.9.9 防绕管理

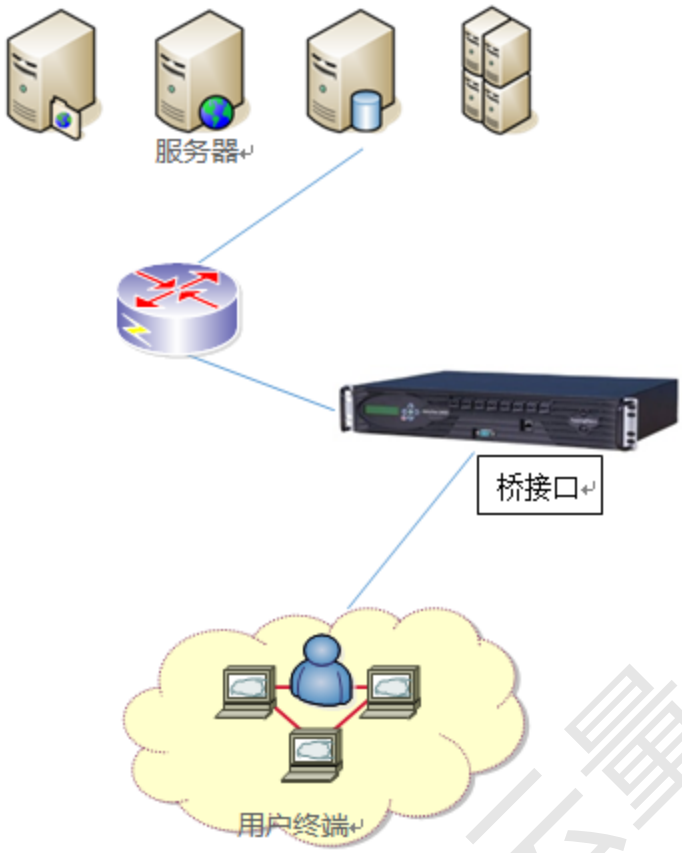
通过“防绕管理”，系统“安全保密管理员”可通过该页面禁用、启用镜像模式或桥模式防绕。

1.启用镜像模式，点击运行状态中的“ 启用 ”，防绕模式中的“ 镜像模式 ”，选择 1 个网口作为镜像包采集口，点击保存。网络拓补图如下

所示：



2. 启用桥模式，点击运行状态中的“ 启用 ”，防绕模式中的“ 桥模式 ”，勾选 2 个网口作为镜像包采集口，点击保存。网络拓补图如下所示：



第四章 用户登录

4.1 Web 登录

客户端的本地化可以让“用户”通过登录 WEB 端，在 WEB 界面输入用户名、密码直接登录到所授权的设备上。登录后，在左侧菜单栏的基础管理，点击“访问控制”，可以查看到用户授权管理访问的设备资源，根据不同的协议，点击“连接”按钮，直接登录到设备资源上。如下图所示：

1.终端命令操作：Telnet、SSH、DB 协议，登录成功后，直接在命令字符界面操作设备。

- Telnet 连接

注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要在 web 弹出框输入设备的密码才可正常登录。

➢ SSH 连接

注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要在 web 弹出框输入设备的密码才可正常登录。

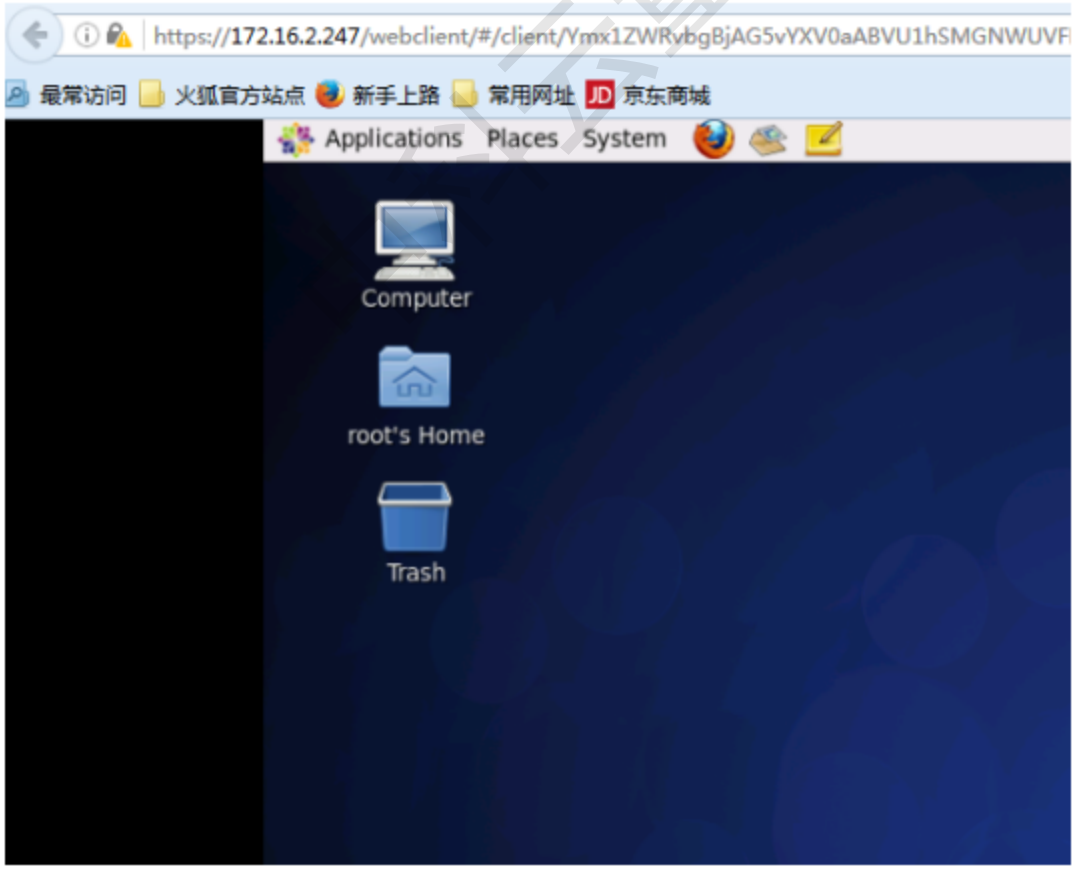
➢ 数据库连接

2. 远程桌面操作：RDP、VNC 协议，登录成功后，直接 WEB 界面操作远程桌面。

➢ RDP 连接

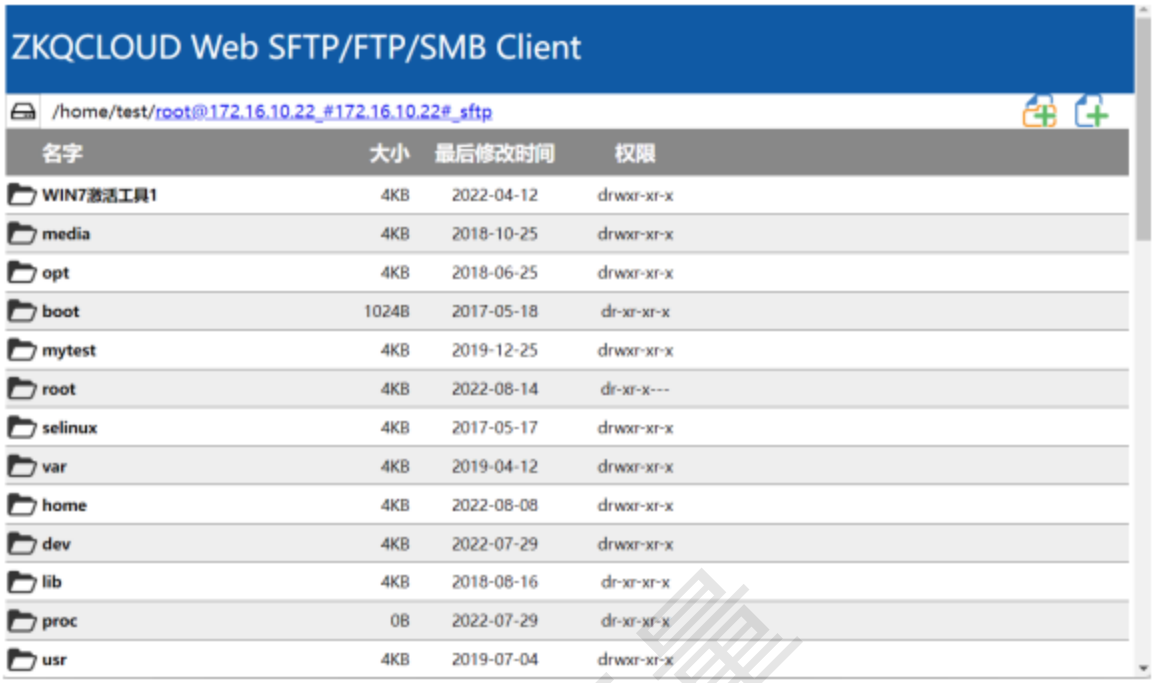
注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要输入设备的密码才可正常登录。

➢ VNC 连接



注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要在 web 弹出框输入设备的密码才可正常登录。

3.文件上传和下载：FTP、SFTP 协议，登录成功后，直接在 WEB 界面操作 FTP 服务器共享的文件。包括删除、上传、下载、重命名文件/目录。



新建目录：点击“  ”，输入新建目录的名称，可以新建目录。

上传文件：点击“  ”，在本地电脑选择需要上传的文件，点击“打开”进行上传，上传成功后，会有相应的提示。

下载文件：选择文件，选择文件名，便可下载文件到本地电脑上。

删除文件：选择文件，点击“  ”，有相应的删除提示，点击“确定”后，删除文件或者目录。

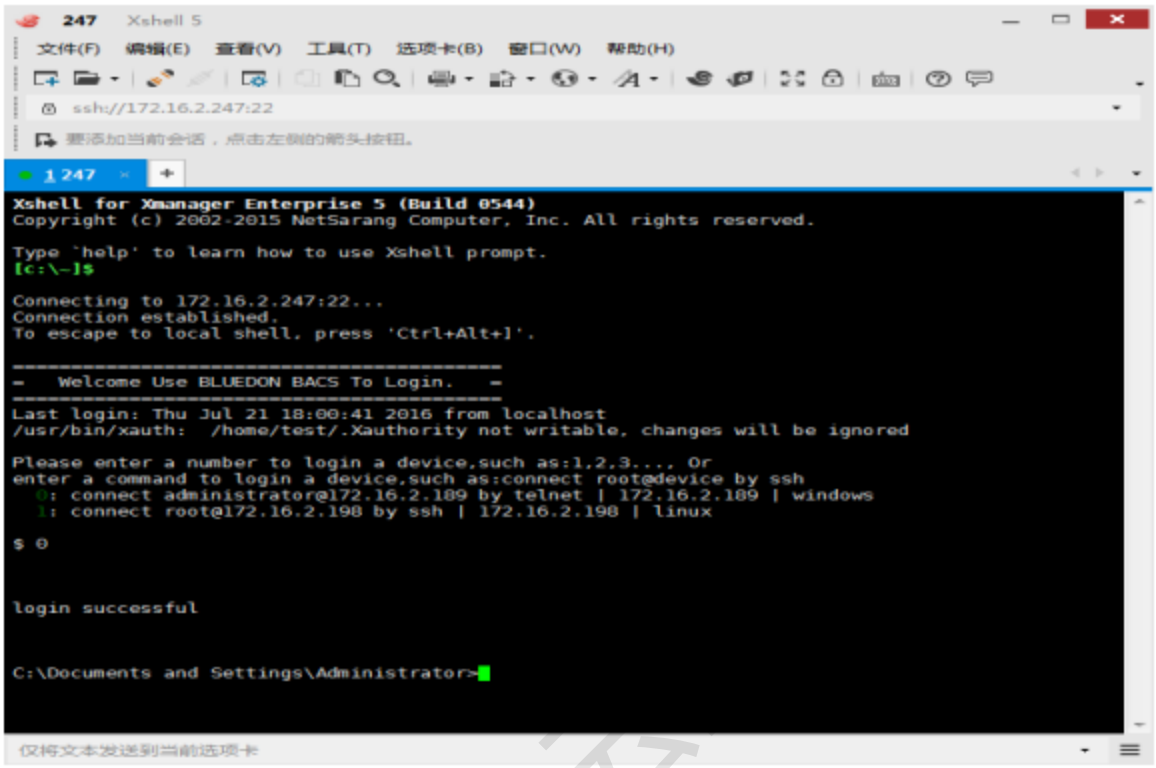
重命名：选择文件，点击“  ”，输入新的名字，修改文件或者目录的名字。

注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要在 web 弹出框输入设备的密码才可正常登录。

4.2 客户端工具登录

授权管理设备资源的用户，除了可以通过登录 web 端访问设备资源外，还可以保持用户原有运维习惯，利用已有的运维工具访问设备资源。

1.终端命令操作：SSH、Telnet、db 协议，可以通过 xshell、putty 等远程连接工具连接。如下图所示：



注意：

- **SSH 登录的地址为帐号集中管理与审计系统的地址，登录的用户为授权管理设备资源的用户。登录成功后，如果用户授权的终端命令操作的设备资源比较多，可以通过选择序号进行访问，数据库客户端登录也是通过 ssh 登录。**
- **当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要输入设备的密码才可正常登录。同时，数据库不支持无密码登录。**

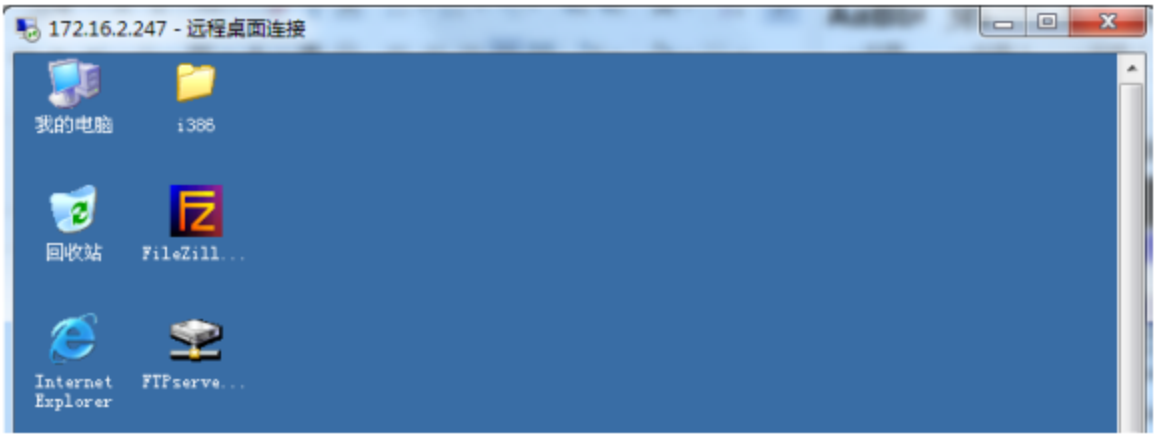
2.远程桌面操作：rdp、vnc 协议，可以通过远程桌面就可以直接连接，如下图所示。

第一步：远程桌面的地址为帐号集中管理与审计系统的地址，登录的用户为授权管理设备资源的用户。

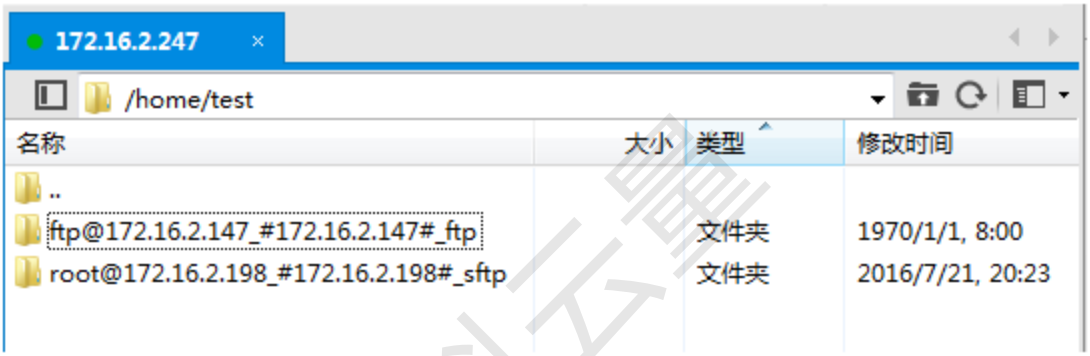
第二步：点击“ LOGIN ”登录后，选择需要登录的设备，包括 IP 地址、用户名、协议。

注意：当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要输入设备的密码才可正常登录。

第三步：选择设备后，点击“ OK ”，远程桌面设备资源。



文件上传和下载：ftp、sftp 协议，可以通过 xftp、winscp 等远程连接工具连接，如下图所示：



注意：

- **FTP/SFTP 登录的地址为帐号集中管理与审计系统的地址，登录的用户为授权管理设备资源的用户。登录成功后，如果用户授权的终端命令操作的设备资源比较多，可以通过选择对应设备目录进行访问。**
- **当添加设备时，被管设备没有添加设备帐号的密码时，连接时需要在 web 弹出框输入设备的密码才可正常登录。**

4.3 发起双授权访问申请

双授权访问申请可由第三方客户端工具发起，也可由 web 发起。

第三方客户端发起访问申请时，“用户授权”在连接设备时即发起，“设备授权”、“访问授权”在选择连接相应的设备时发起，如下图：

```
=   Welcome Use BLUEDON BACS To Login.    =
==========================================
Last login: Mon Jun 19 15:37:30 2017 from localhost
```

发起用户授权

```
=========================================
=   Welcome Use BLUEDON BACS To Login.   =
=========================================
Last login: Mon Jun 19 15:37:30 2017 from localhost
该用户(wenjinqing)被admin授权允许访问

Please enter a number to login a device,such as:1,2,3..., Or
enter a command to login a device,such as:connect root@device by ssh
  0: connect root@ssh_201 by ssh | 10.10.10.201 | 201SSH协议
  1: connect root@mysql_200 by db | 10.10.10.200 | 200mysql数据库

$ 1
```

发起设备授权或访问授权

web 发起访问申请时，“用户授权”在用户登录系统时发起，“设备授权”、“访问授权”在用户点击访问控制-设备访问页面中的连接时发起。

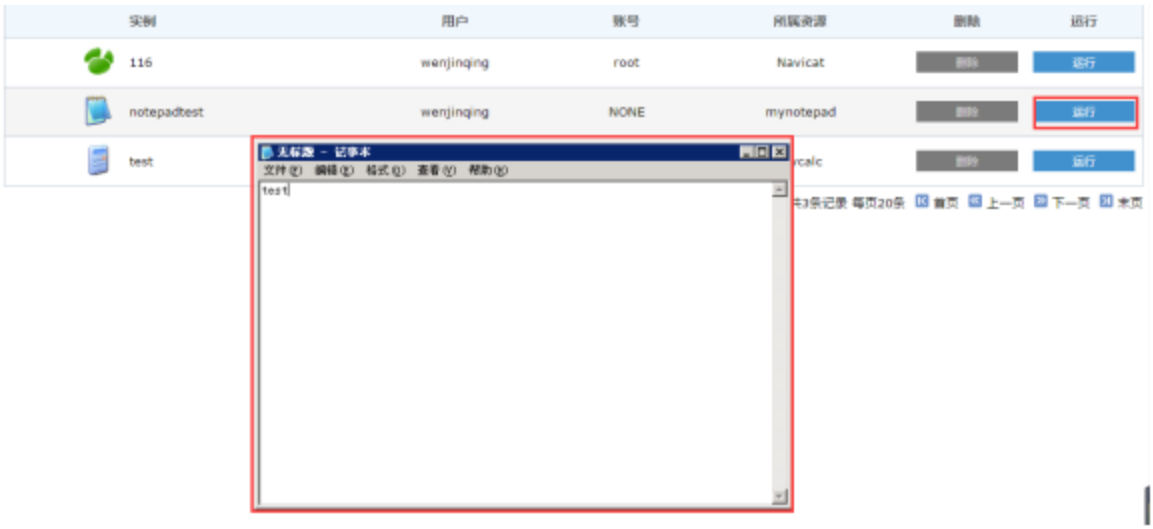
4.4 访问管理

4.4.1 设备访问

以被授权用户登录 web，点击“ 连接 ”，打开应用实例，如下图所示：

4.4.2 应用访问

以被授权用户登录 web，点击“ 运行 ”，打开应用实例，如下图所示：

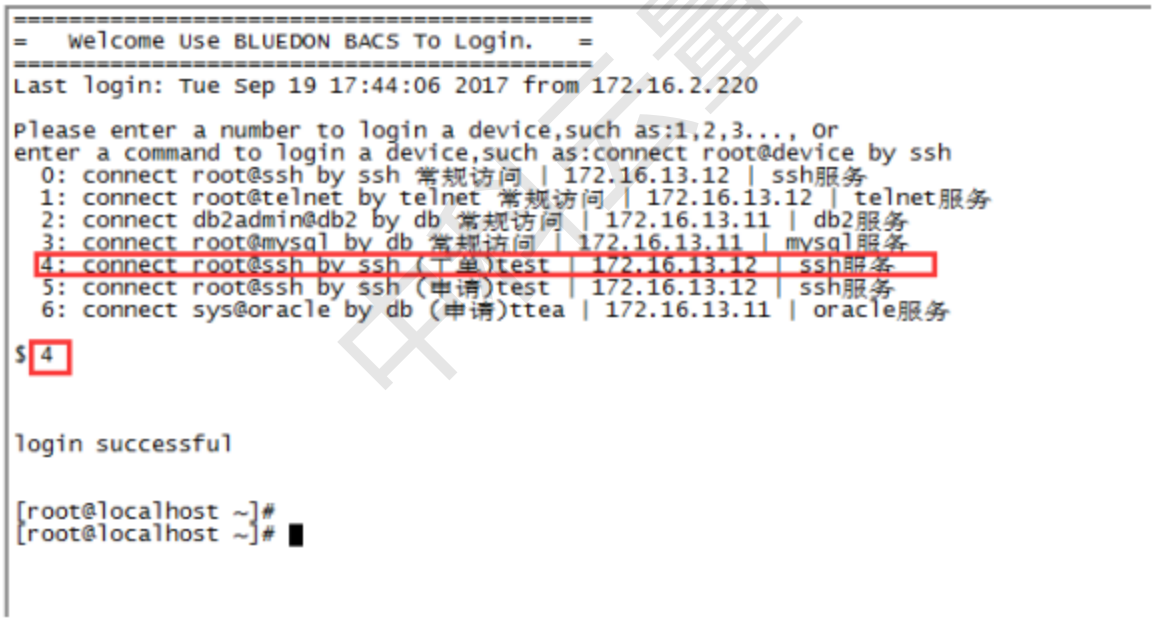


4.5 工单任务访问

4.5.1 我的任务

1.web 访问，以被授权用户登录 web，进入工单管理-我的任务，点击数据条目中的“⊞”展开设备，点击“ 连接 ”，如下图所示：

2.第三方客户端访问，具体操作过程请参考《4.2 客户端工具登录》，操作截图如下：



4.5.2 申请设备访问

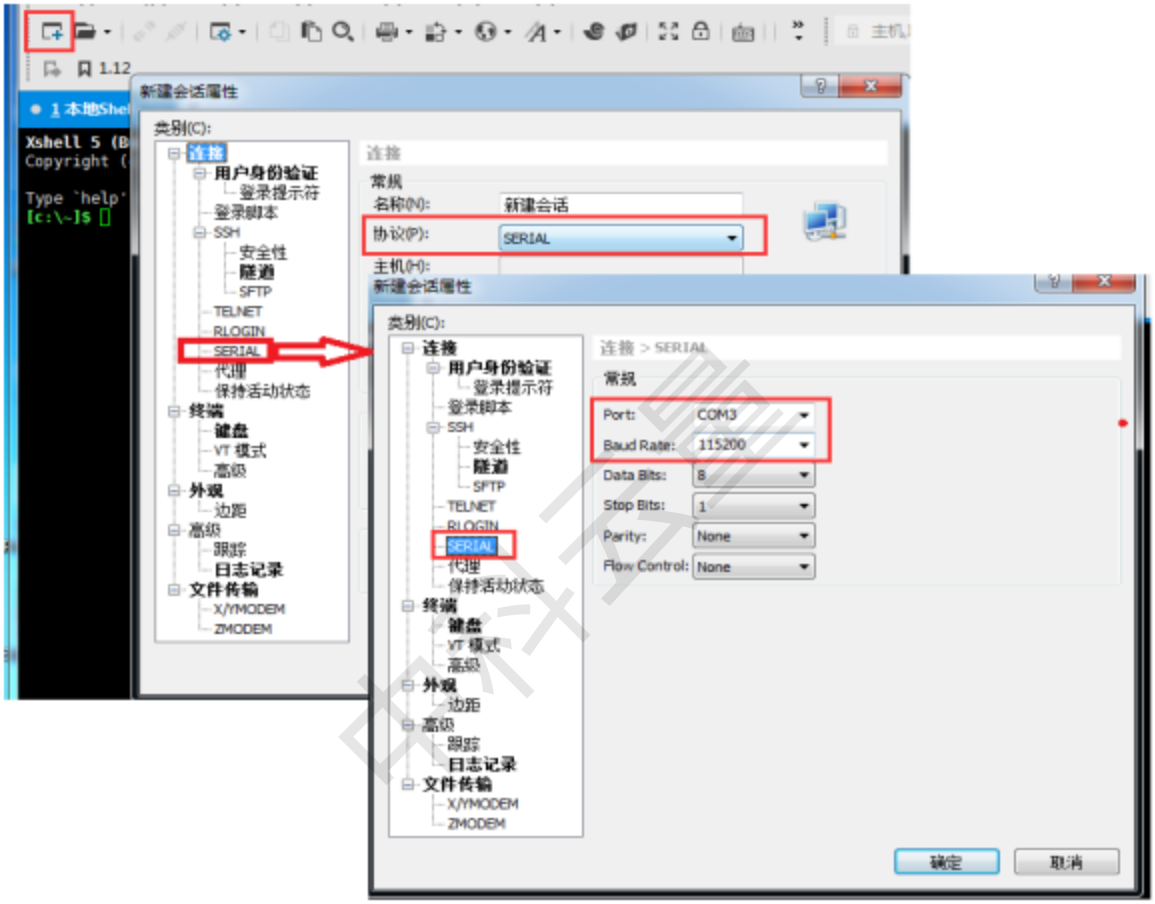
1.web 访问，以被授权用户登录 web，进入工单管理-已完成申请，点击数据条目中的“⊞”展开设备，点击“ 连接 ”，如下图所示：

2.第三方客户端访问，具体操作过程请参考《4.2 客户端工具登录》，操作截图如下：

```
==========================================
=   Welcome Use BLUEDON BACS To Login.   =
==========================================
Last login: Tue Sep 19 17:49:50 2017 from 172.16.2.220

Please enter a number to login a device,such as:1,2,3..., Or
enter a command to login a device,such as:connect root@device by ssh
  0: connect root@ssh by ssh 常规访问 | 172.16.13.12 | ssh服务
  1: connect root@telnet by telnet 常规访问 | 172.16.13.12 | telnet服务
  2: connect db2admin@db2 by db 常规访问 | 172.16.13.11 | db2服务
  3: connect root@mysql by db 常规访问 | 172.16.13.11 | mysql服务
  4: connect root@ssh by ssh (工单)test | 172.16.13.12 | ssh服务
  5: connect root@ssh by ssh (申请)test | 172.16.13.12 | ssh服务
  6: connect sys@oracle by db (申请)ttea | 172.16.13.11 | oracle服务

$ 5


login successful


[root@localhost ~]#
[root@localhost ~]#
```

第五章 CONSOLE 操作指南

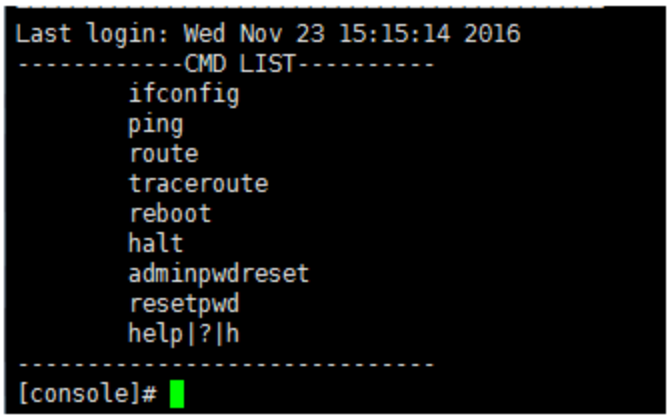
用串口线连接 console 口，在 xshell 中新建串口连接，如下图选择 serial 协议，点击左侧 serial，选择 com 口（在电脑的设备管理中查看当前连接使用的串口），波特率：115200；确定连接。用户名：console；密码:Console@2017。




```
Last login: Wed Nov 23 15:15:14 2016
-----------CMD LIST----------
        ifconfig
        ping
        route
        traceroute
        reboot
        halt
        adminpwdreset
        resetpwd
        help|?|h
-----------------------------
[console]#
```

5.1 查看串口下命令

“help”、“?”或者“h”：可以查看串口下所有的命令。



5.2 ifconfig

使用 ifconfig 查看网口的 IP 地址、临时性配置网口 IP 地址。

#查看所有网口的 IP 信息

[console]#ifconfig -a |more

#查看指定网口的 IP 信息，如 eth0

[console]#ifconfig eth0

#配置临时性 IP 地址，如为 eth0 配置 172.16.2.188/24

[console]#ifconfig eth0 172.16.2.188/24

注意：使用 ifconfig 配置 IP 地址为临时性的，服务器重启即恢复为原来 IP，通过登录 web 页面下发则为永久性配置。

5.3 ping

使用 ping 命令诊断网络连通性，ping 后面可以加 IP 或者加域名（前提 DNS 能成功解析）。

[console]#ping 172.16.2.88

[console]#ping www.bluedon.cn

5.4 route

使用 route 命令可以查看路由表，增加、删除路由。

#查看命令帮助

[console]#route -h

#查看路由表

[console]#route -n

#添加静态路由，如指定默认网关为 172.16.2.254

[console]#route add -net 0.0.0.0 netmask 0.0.0.0 gw 172.16.2.254

或者

[console]#route add default gw 172.16.2.254

#删除静态路由，如删除上面添加的默认网关

[console]#route delete -net 0.0.0.0 netmask 0.0.0.0

5.5 traceroute

使用 traceroute 命令跟踪主机到目的地址的路由走向。

#用法：traceroute hostname（域名、IP）

[console]#traceroute 202.96.128.166

[console]#traceroute www.baidu.com

5.6 reboot

使用 reboot 命令重启服务器。

[console]#reboot

5.7 adminpwdreset

#使用 adminpwdreset 重置 admin 管理员的初始密码 Bluedon@2017。

[console]#adminpwdreset

```
[console]# adminpwdreset
        Are you sure you want to reset the password for admin? (yes|no)
        yes
        *Password has been reset successfully!
[console]#
```

5.8 resetpwd

#使用 resetpwd重置 sysadmin 的初始密码为 Sysadmin@2017;auditor 的初始密码为 Auditor@2017。

[console]#resetpwd

```
[console]# resetpwd
       Are you sure you want to reset the password for auditor and sysadmin? (yes|no)
       yes
       *Password has been reset successfully!
```

5.9 halt

使用 halt 命令关闭服务器。

[console]#halt

5.10 exit

使用 exit、quit 退出 console 管理界面。

第六章 必要软件安装

用户在使用中科云量运维安全管理系统时，需调用相关联的软件，这些软件需要预先安装好，否则将出现相关系统功能不能正常运行的现象。

6.1 远程桌面服务（RemoteApp）

远程桌面服务（RemoteApp）用于应用管理模块中，应用资源的添加、应用实例的调用。该服务安装在应用跳板机中，建议跳板机的系统版本为：Windows Server 2008(如果被帐号集中管理与审计系统管理的 Windows Server 2008 设备需要定时修改密码，也需要安装该服务。)。操作步骤如下：

在应用跳板机服务器上打开服务器管理器，如图 1 所示，右键点击"角色"，选择"添加角色"。

图 1

如图 2 所示，出现角色向导，点击"下一步"继续。

图 2

如图 3 所示，在服务器角色中选择"远程桌面服务器"，如果操作系统是 Windows Server 2008，就要选择"终端服务"角色。

图 3

选择了远程桌面服务角色后，接下来就要选择角色服务了。如图 4 所示，我们选择的角色服务是"远程桌面会话主机"。远程桌面会话主机就是 Windows Server 2008 中的终端服务器，我们在远程桌面会话主机中可以实现 RemoteApp。其他的角色服务我们在后续文章中会进行部署及配置。

图 4

如图 5 所示，角色向导提示我们某些应用程序在终端服务器下可能无法正常工作，需要在终端服务器下重新安装才能运行。其实很多应用程序无需修改或者只需要稍作修改，就可以在终端服务器上完美运行了。

图 5

如图 6 所示，接下来要选择身份验证方式，我们可以选择"需要使用网络级别身份验证"或"不需要使用网络级别身份验证"。如果选择使用网络级别身份验证，那么客户机需要先进行身份验证才可以连接到终端服务器，安全性会更好一些。我们在测试环境下选择的是不需要使用网络级别身份验证，这样客户机可以连接到终端服务器之后再进行身份验证。虽然降低了一些安全性，但可以使更多的客户机来使用这项服务。

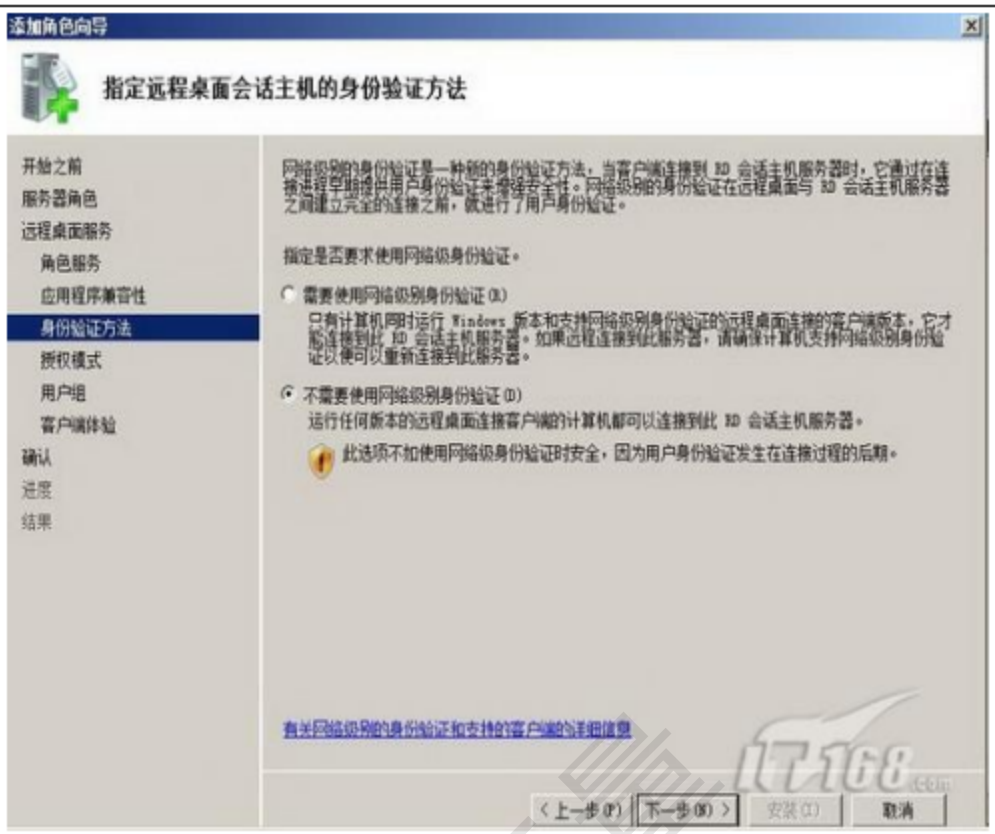


图 6

如图 7 所示，我们要为终端服务选择合适的授权模式。在测试环境下，我们选择"以后配置，这意味着我们有 120 天的测试使用时间。

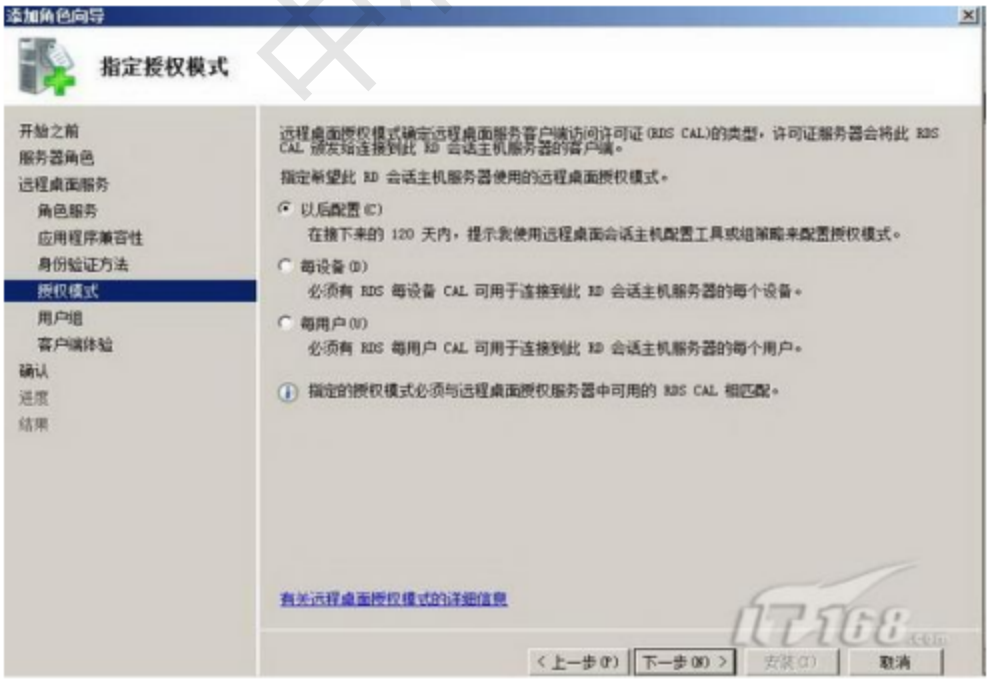


图 7

如图 8 所示，接下来要配置的是允许连接到终端服务器的用户或组。默认本地管理员组被授权访问终端服务器，我们添加了 Domain Users 组，让所有的域用户都可以访问终端服务器。

图 8

如图 9 所示，在配置客户端体验中我们可以让客户机连接到终端服务器后使用 Aero 桌面，音频或视频资源。考虑到这些资源需要更多的网络带宽，我们没有选择这些附加功能。

图 9

如图 10 所示，确认我们要安装的角色及各项参数配置无误，点击"安装"按钮开始角色安装。安装完毕后重启计算机，我们就完成了 RemoteApp 服务器的部署。

图 10

如图 11 所示，我们就完成了 RemoteApp 服务器的配置。

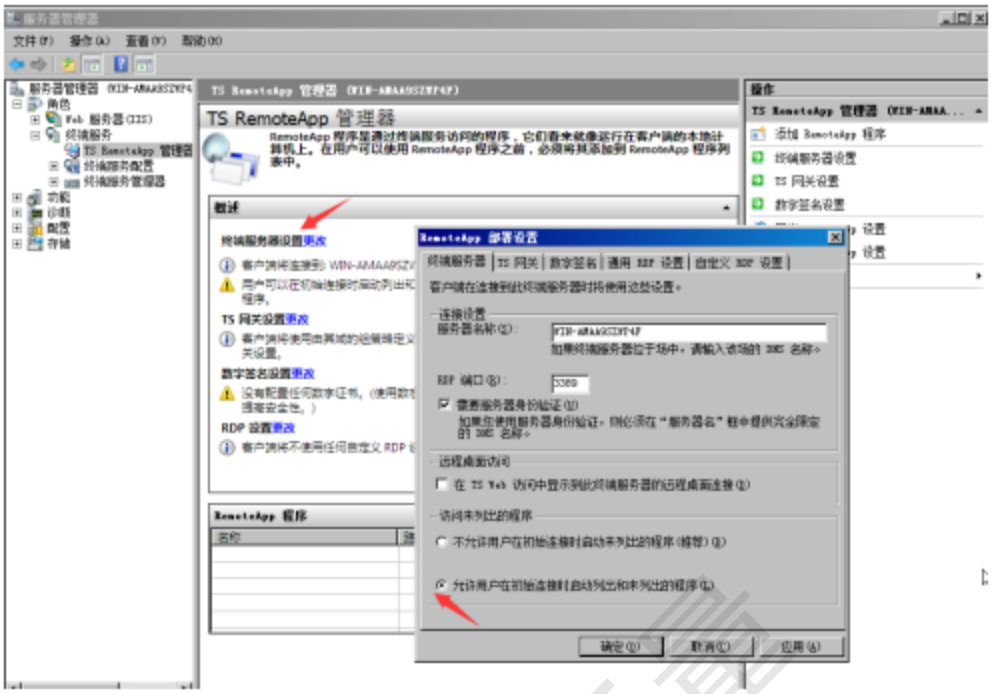


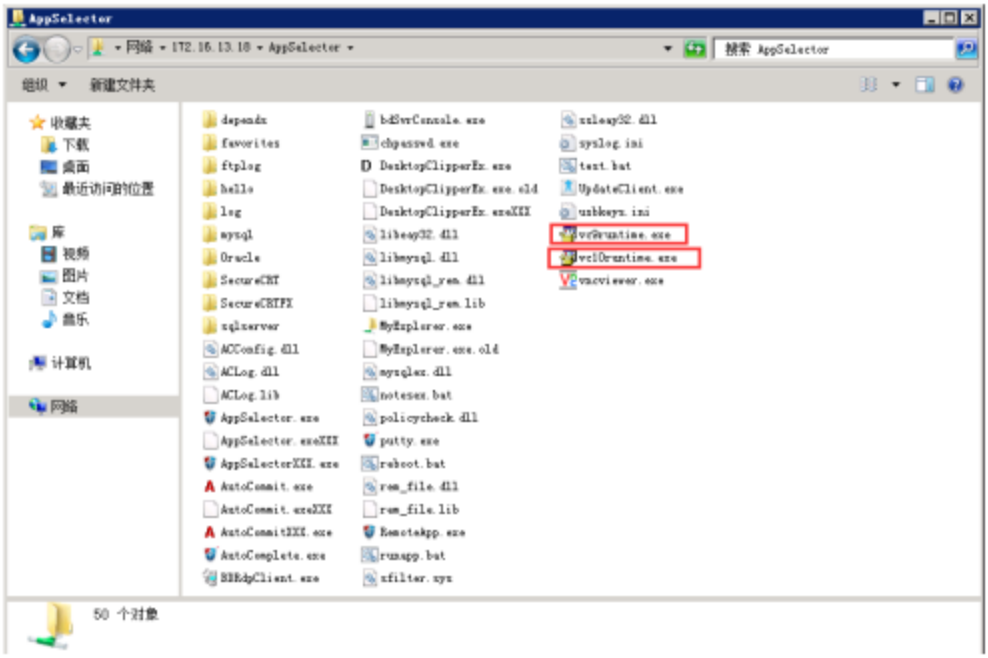
图 11

6.2 C 语言运行库

使用应用管理模块功能，除需要安装远程桌面服务外，还需要安装应用发布控件，安装步骤如下：

1.安装 vc2008 和 vc2010 运行库，步骤如下：

使用应用跳板机服务器，访问帐号集中管理与审计系统的共享目录“AppSelector”，URL：\\IP\AppSelector。如跳板机的 IP 地址为 192.168.249.7，则共享目录地址为：\\192.168.249.7\AppSelector，共享目录文件如下图所示：



分别双击“vc9runtime.exe”、“vc10runtime.exe”完成运行库的安装。

注意：如果需要将远程桌面访问的视频下载到本地审计，则本地客户端的计算机也需要安装该运行库。

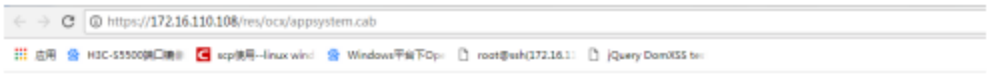
6.3 应用发布控件

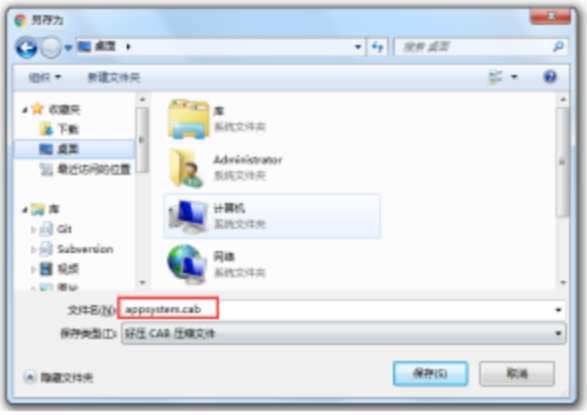
要使用应用发布模块的计算机都需要安装应用发布（ActiveX）控件。

1. 安装应用发布控件，可通过下载 appsystem.cab 到本地安装，也可通过设置 IE 对 ActiveX 控件的支持后，直接安装。

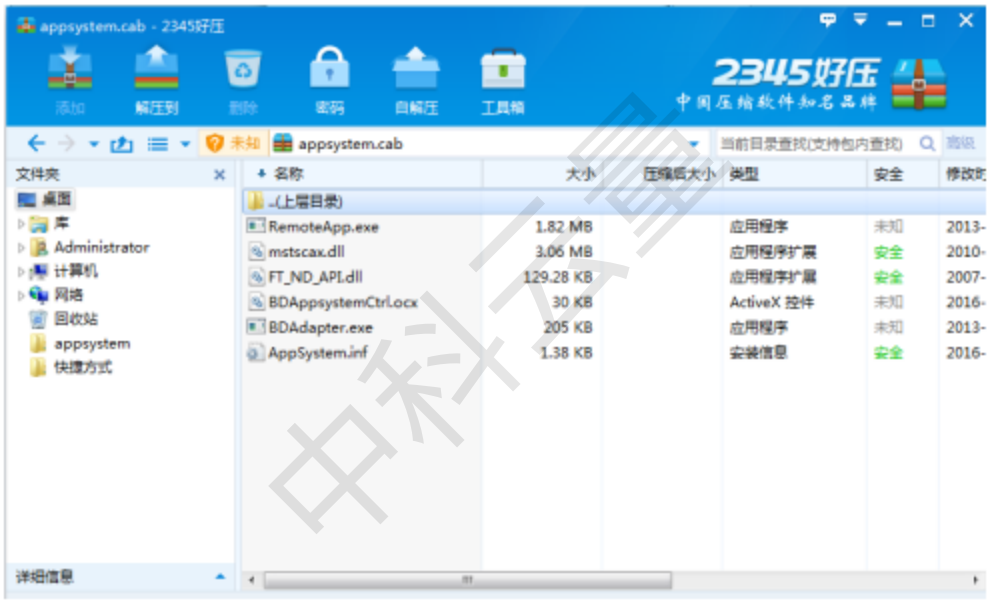
1.1、下载 appsystem.cab 到本地安装应用发布控件，步骤如下：

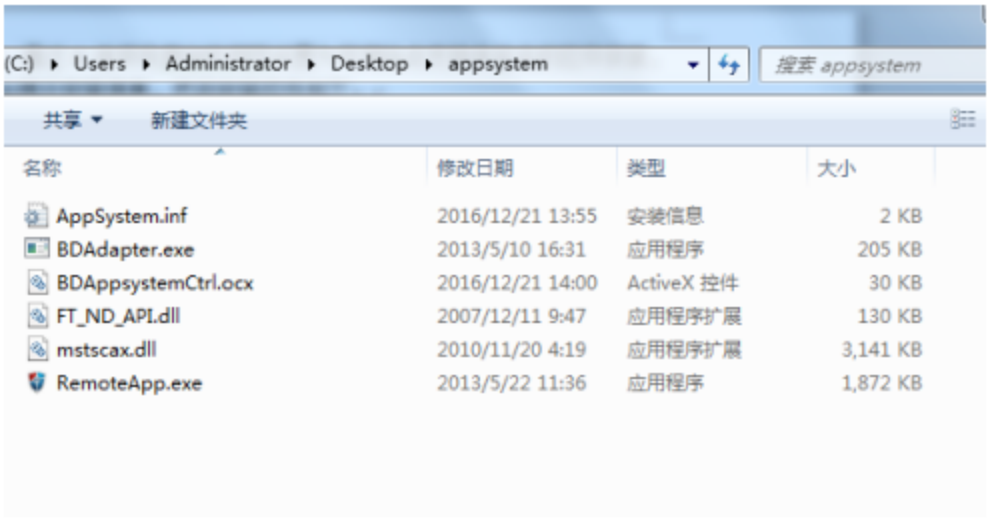
1.1.1、使用网页浏览器，访问 URL：https://IP/res/ocx/appsystem.cab，IP 为帐号集中管理与审计系统对应的 IP 地址，如系统的 IP 地址为“172.16.21.174”，则访问的 URL 为：https://172.16.110.108/res/ocx/appsystem.cab。





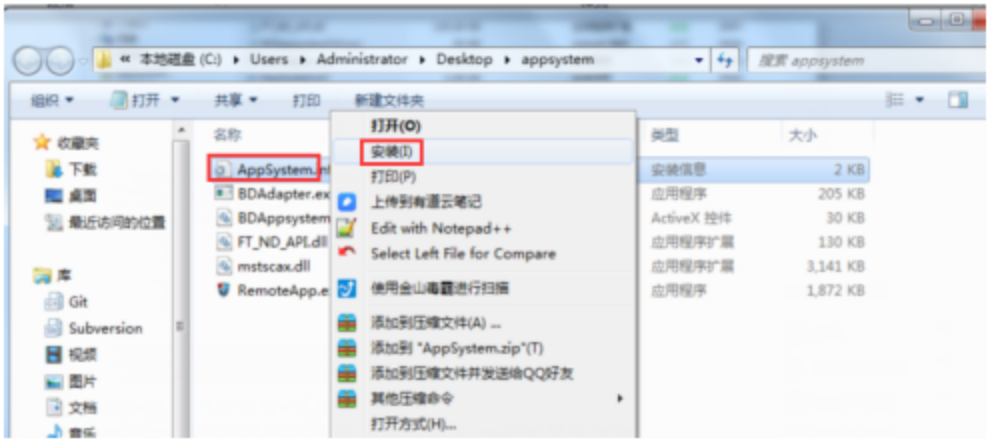
1.1.2、将 appsystem.cab 文件保存到本地后，解压该文件。





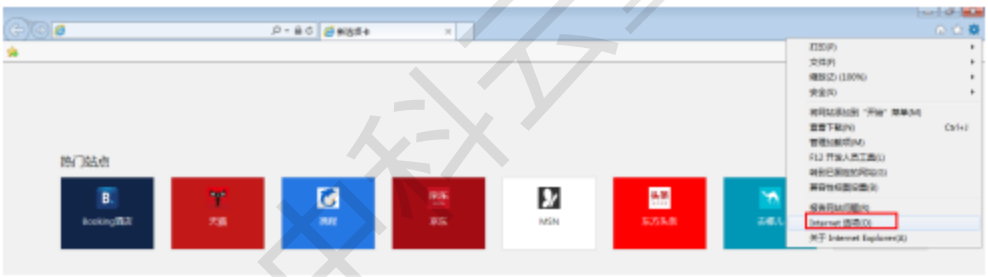
1.1.3、鼠标右键点击“AppSystem.inf”文件，在列出的菜单中左键点击“安

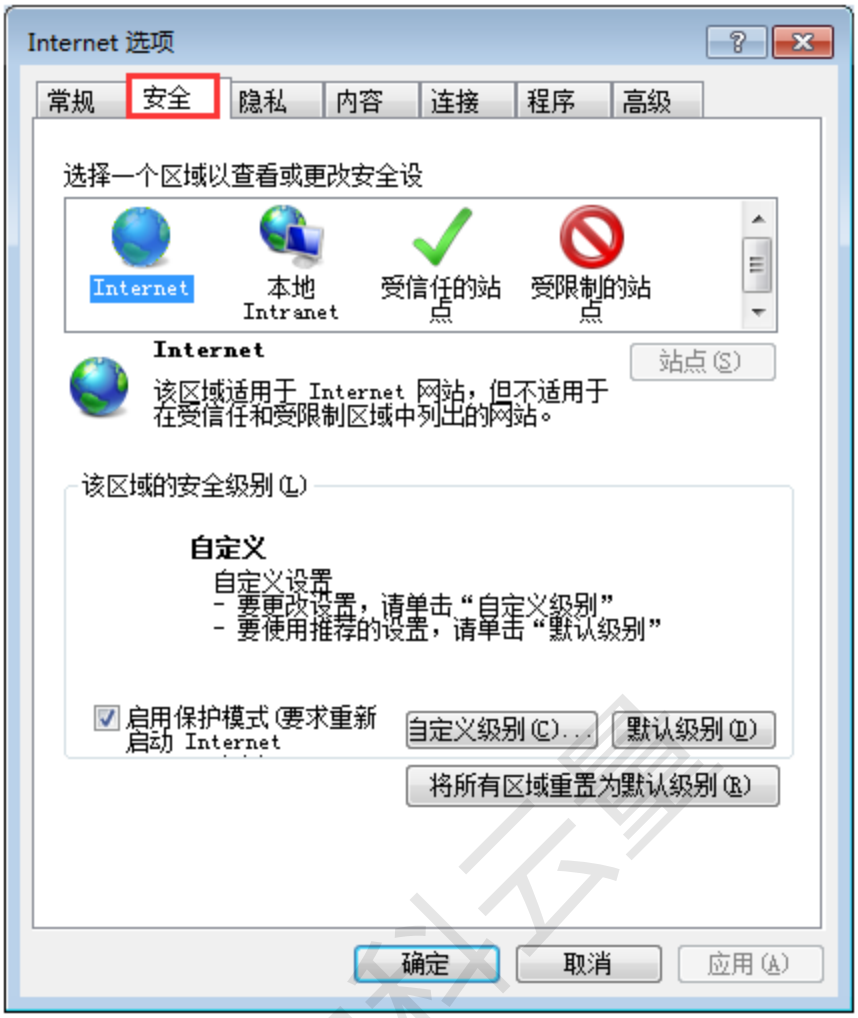
装”，



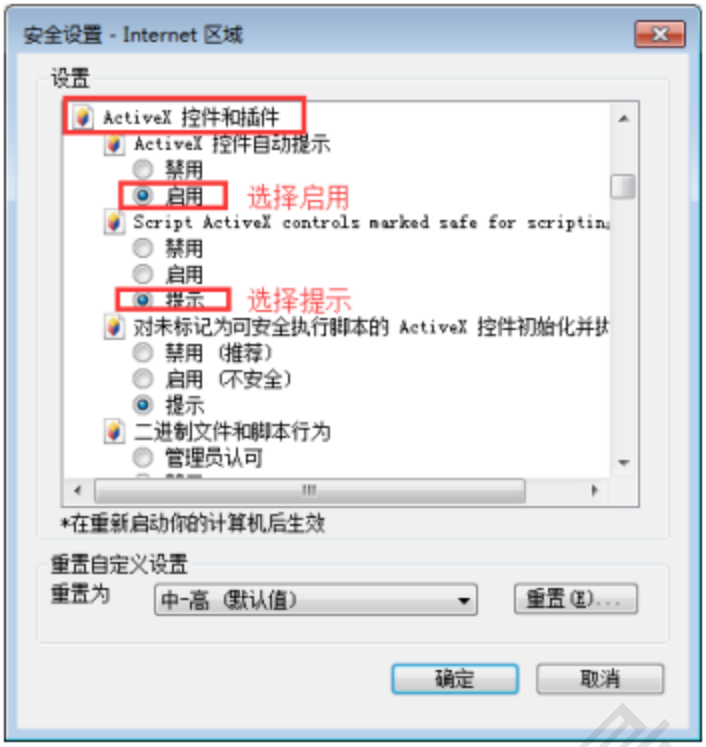
1.2、在需要使用应用管理模块功能的计算机中，通过 IE 浏览器（只支持 IE10 以上版本）安装 appsystem.cab，先设置 IE 对 ActiveX 控件的支持（分别在"Internet","本地 Internet","受信任的站点"中的“ActiveX 控件和插件”项中选择启用/提示-有提示选项选提示，没提示选项选启用），如下：

1.2.1、打开 IE 选项，切换到“安全”。

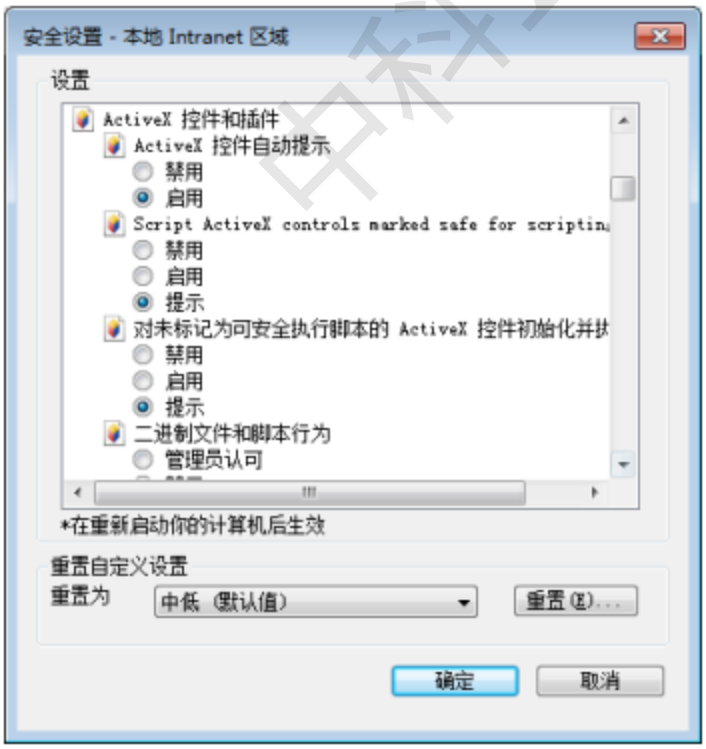




1.2.2、依次点击“Internet”，“自定义级别”，打开“安全设置-Internet区域”，下拉滚动条，定位到“ActiveX 控件和插件”，在该项中，有提示的选择提示，没提示的选择启用（所有 ActiveX 控件和插件中的项都需选择）。

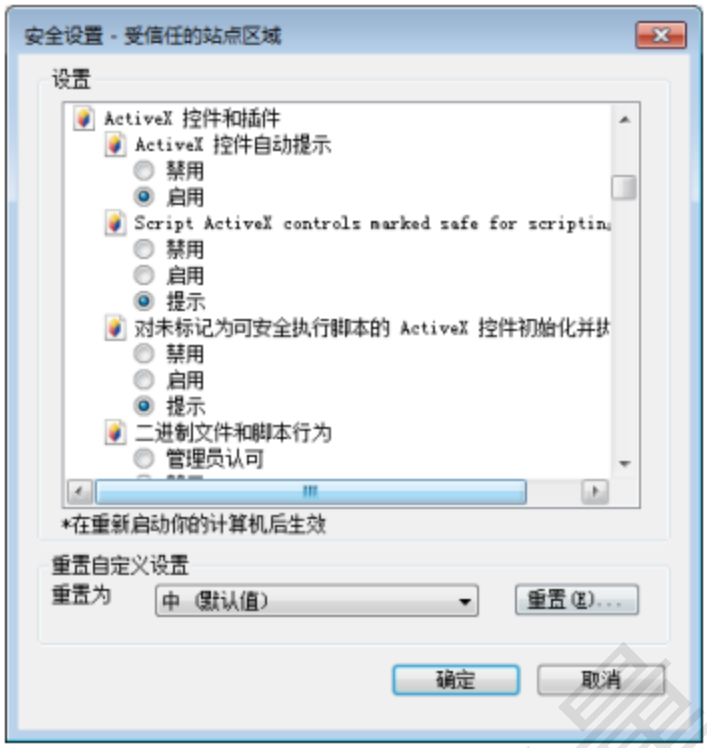


1.2.3、依次点击“本地 Internet”，“自定义级别”，打开“安全设置-本地 Internet 区域”，下拉滚动条，定位到“ActiveX 控件和插件”，在该项中，有提示的选择提示，没提示的选择启用（所有 ActiveX 控件和插件中的项都需选择）。

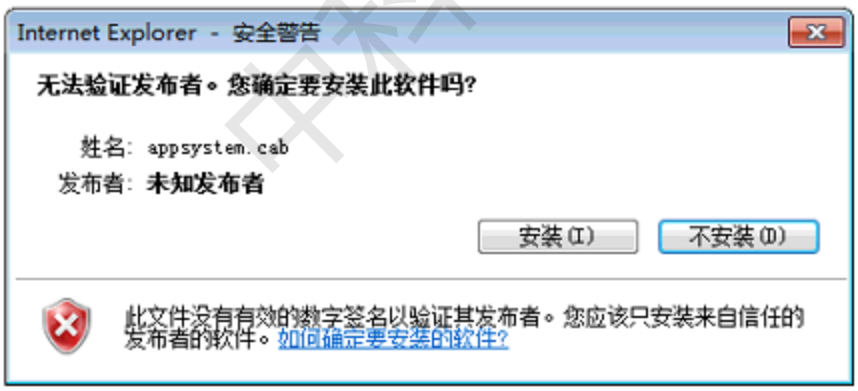


1.2.4、依次点击“受信任的站点”，“自定义级别”，打开“安全设置-受信任的站点区域”，下拉滚动条，定位到“ActiveX 控件和插件”，在该项中，有提

示的选择提示，没提示的选择启用（所有 ActiveX 控件和插件中的项都需选择）。

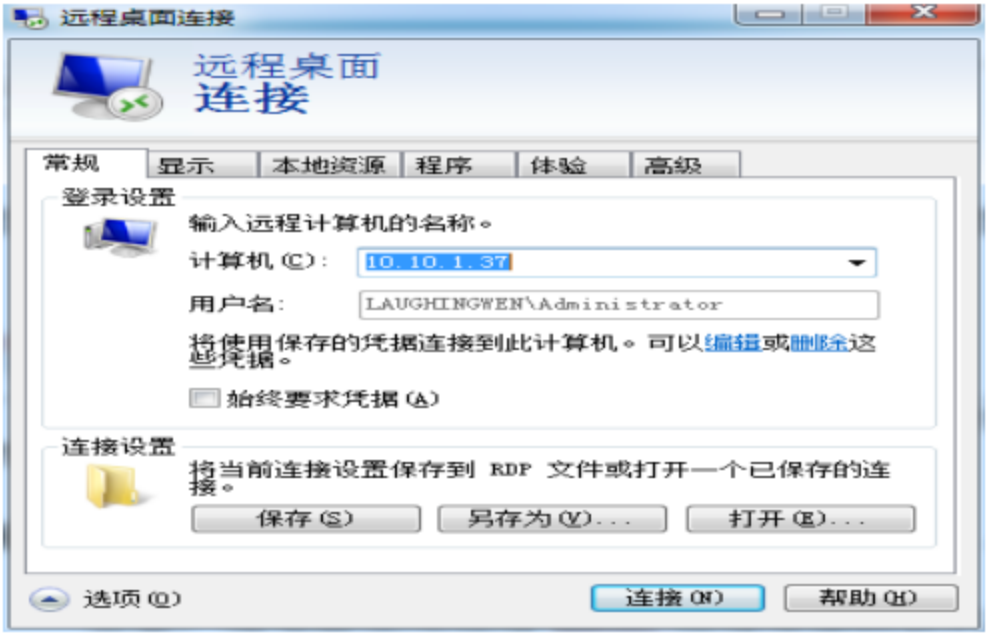


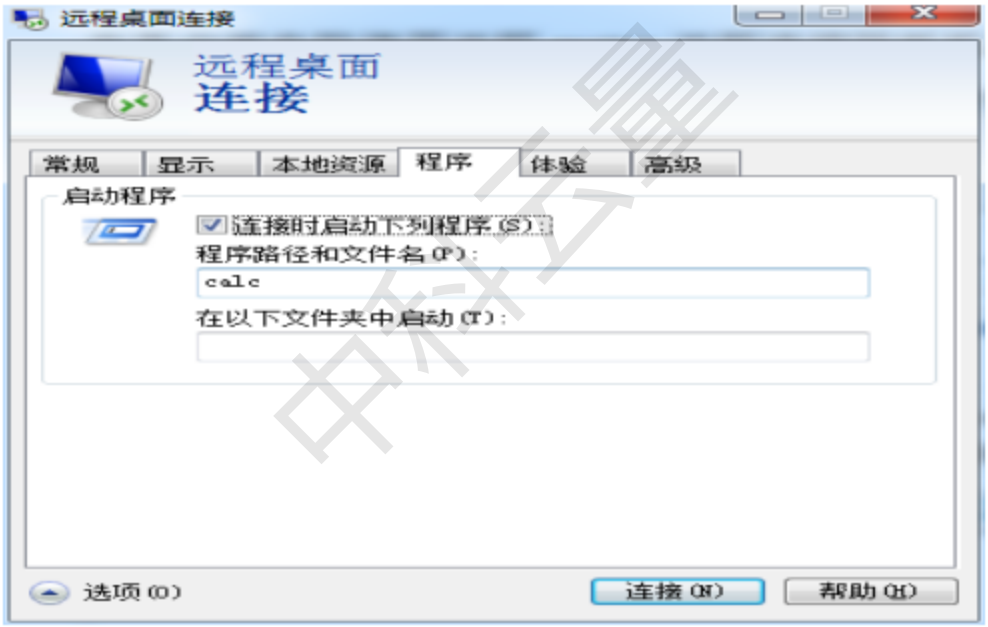
1.2.5、重启 IE，打开堡垒机网页，使用 admin 用户登录后会提示安装信息，然后点击安装。



6.4 测试远程桌面服务（RemoteApp）

在客户端电脑使用 mstsc 连接跳板机，发起多次（相同用户两次以上）连接打开跳板机的计算器应用：


远程桌面连接
远程桌面
连接
常规
显示
本地资源
程序
体验
高级
登录设置
输入远程计算机的名称。
计算机(C):
10.10.1.37
用户名:
LAUGHINGWEN\Administrator
将使用保存的凭据连接到此计算机。可以编辑或删除这些凭据。
始终要求凭据(A)
连接设置
将当前连接设置保存到 RDP 文件或打开一个已保存的连接。
保存(S)
另存为(V)...
打开(E)...
选项(O)
连接(N)
帮助(H)


远程桌面连接
远程桌面
连接
常规
显示
本地资源
程序
体验
高级
启动程序
连接时启动下列程序(S):
程序路径和文件名(P):
calc
在以下文件夹中启动(T):
选项(O)
连接(N)
帮助(H)

如上图，远程连接到跳板机能直接打开跳板机中的计算器，并且跳板机允许相同用户发起多个远程会话连接，则说明跳板机已满足帐号集中管理与审计系统的应用发布模块使用要求。

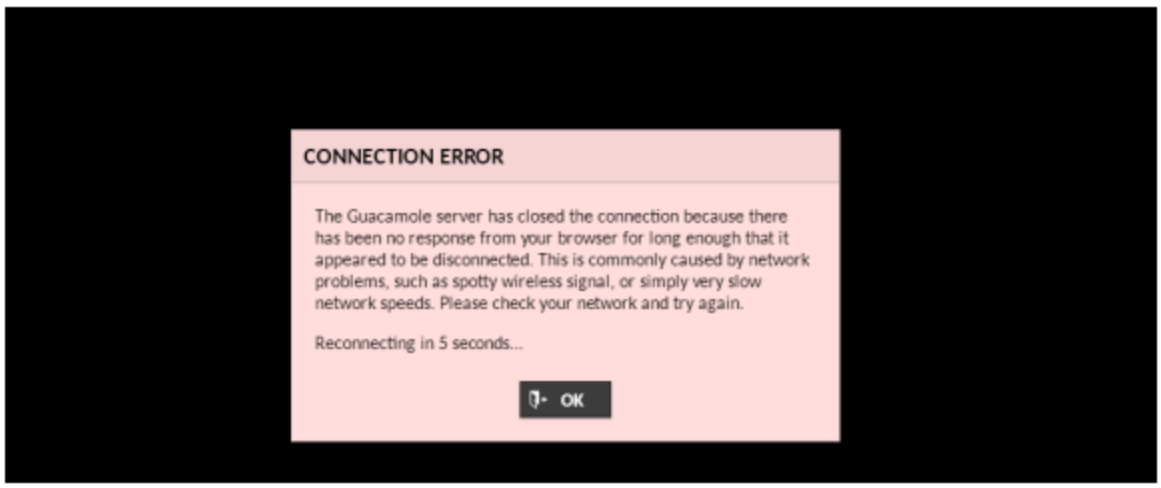
第七章 常见问题排查

7.1 连接被管理的资产时失败

7.1.1. 无法正常连接设备

7.1.1.1. 问题现象

连接设备时，无法正常连接



7.1.1.2. 排查过程

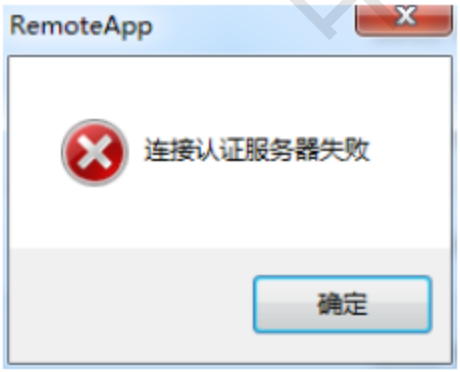
排查步骤	成功现象	失败现象分析及解决方案
1.使用串口线，连接到设备的串口，使用 console/Console@2017 登录。 2. 执行 ping 命令，看网络是否可达网关，资产设备 IP 等。 3.执行 route,查看网关配置 4.如果能 ping 通堡垒机所在的网关却不能 ping 通资产设备所在的网关，则检查网络配置 5.能 ping 通资产设备，则 telnet 需要访问的端口 6.检查保存在设备中的用户名和密码，确保其准确性并进行测试	1. 成功登录 console 用户 2.成功 ping 通网关或资产设备 IP 3.已经正确添加网关，且网关只有一个 4.相同网段的 IP 只有一个 5.能 telnet 成功 6.保存的账号密码正确，直接访问能正常连接	1.用户名或密码输入错误，确认用户名或密码的准确性，重新输入 2.资产设备 IP 不通时，ping 资产设备所在的网关，资产设备的网关不通时，执行步骤 3 3.网关出现多个，使用 sysadmin 用户登录系统，修改网络配置，确保网关只有一个 4.相同网段的 IP 存在多个，修改网络配置，确定相同网段的 IP 只有一个 5.不能 telnet 资产设备的端口，则检查网络链路上的防火墙配置，看是否有拦截该端口，如果有，则解除拦截。 6.设备保存的账号或密码错误，修改账号或密码。

7.2 无法添加资源或访问应用时打不开应用

7.2.1.点击添加资源或运行应用时提示连接认证服务器失败

7.2.1.1. 问题现象

在应用资源页面点击添加资源>启动应用按钮或在应用访问页面点击运行>启动应用按钮，弹出提示“连接认证服务器失败”



7.2.1.2. 排查过程

排查步骤	成功现象	失败现象分析及解决方案
1.从客户端 telnet 堡垒机的 33334 端口	1.能成功连接	1.检查网络链路中的防火墙，看是否有拦截该端口，放开对该端口的拦截

7.2.2.点击添加资源或运行应用时界面停留在连接远程桌面成功

7.2.2.1. 问题现象

添加资源或连接设备时，不能打开应用，界面停留在连接远程桌面成功

7.2.2.1. 排查过程

排查步骤	成功现象	失败现象分析及解决方案
1.执行《7.1.2 排查过程》中的步骤，确保保存的跳板机信息及网络都没问题 2.连接到跳板机，打开跳板机的windows任务管理器，切换到用户标签页，查看发起连接时是否有新的连接 3. 从跳板机telnet堡垒机的33334端口 3.从跳板机访问堡垒机的共享目录或telnet堡垒机的139端口	1.网络可达，跳板机信息准确 2.有新的用户连接进来 3.能正常连接 4.能正常打开共享目录或连接	1.修复网络连接，更新保存的跳板机信息 2.确保远程桌面服务正确部署并安装了VC运行库，执行《6.5 测试远程桌面服务（RemoteApp）》的测试能访问跳板机中的应用；用户名和密码配置正确 3.检查网络链路，看是否有拦截该端口，放开对该端口的拦截 4.检查网络链路，看是否有拦截该端口，放开对该端口的拦截