云堡垒机 用户手册

文档版本：V 3.0.0.0
发布日期：2018 年 9 月

目 录

本书约定

1、 图形界面格式约定

格式	意　义
<>	带尖括号“<>”表示按钮名，如“请按<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名、数据表和字段名等，如“弹出[新增用户]窗口”。
/	多级菜单用“/”隔开，如“[资源管理/主机/独立主机]”多级菜单表示[资源管理]菜单下的[主机]子菜单下的[独立主机]菜单项。

2、 鼠标操作约定

操作	意　义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标的一个按钮不放，移动鼠标。

3、 各类标志

本书还采用各种醒目的标志来表示需要特别注意的地方，这些标志的含义如下：

注意：提醒应该注意的事项。

说明：对内容进行必要的补充和说明。

4、 本书名词解释

角色名称	主要权限
部门管理员	本部门的系统管理员，拥有管理权限。
策略管理员	策略管理员，拥有配置策略的权限。
审计管理员	拥有查阅、管理系统审计数据的权限。
运维员	拥有对资源的运维操作权限。

注：预置系统管理员 admin 不属于以上任何角色，拥有最高权限

前言

适用范围和先决条件

云堡垒机旨在为 IT 审计员、IT 顾问和安全专家提供可靠的服务器和应用发布管理安全解决方案，帮助 IT 决策者应对各类法令法规（如 SOX、PCI、企业内控管理、等级保护、ISO/IEC27001 等），同时帮助 IT 运维人员更高效地执行自动化运维和资源监控操作。本手册编写以帮助用户了解系统使用、根据使用场景构建出属于自己的云计算安全管控系统。

要成为一个合格的云堡垒机系统管理员，必须具备以下技能：

- 基本的系统管理（Windows、Linux、Unix 以及各类网络设备）知识
- 熟悉计算机网络、TCP/IP 协议以及常用网络术语

支持信息

成都西维数码科技有限公司

网址：http://www.west.cn

电话：+86-028- 62778877

企业 QQ：800019263

地址：四川省成都市金牛区一环路北一段 99 号 环球广场 24 楼

第一章 产品简介

1.1 产品概要

云堡垒机管理系统是用于提供云计算安全管控的系统和组件，实现对运维资源的 4A 全面安全管控。系统包含用户管理、资源管理、策略、审计、工单等模块，支持对 Windows 主机、Linux 主机等诸多主机的安全管控保护。是集统一资产管理与单点登录，多种终端访问协议，文件传输功能于一体的运维安全管理与审计产品，产品特色及优势主要体现以下几个方面：

- 无需客户端，在登录资源，或对其实时监控和上传下载文件时无需安装任何客户端软件。
- 集中账号管理，统一维护主机、网络设备和应用发布等资源。
- 记录与审计，支持访问历史记录回放和操作指令搜索功能，可随时查看每个用户对所属主机、主机和网络设备的访问情况。
- 细粒度的权限划分及对用户的动态授权功能。
- 敏感命令拦截，对云堡垒机所管控的主机进行实时命令拦截。
- 协同运维功能，可邀请其他运维人员或专家对同一会话进行协同操作或问题定位。

云堡垒机管理系统为政府部门、电信运营商、金融机构、企事业单位、商业组织等提供了完整的统一安全管理平台解决方案，使客户在面对高复杂度的内控授权、运维操作审计、法律法规合规性审查时，能够实施完善的解决方案。

部署云堡垒机管理系统，能够极大的保护客户内部网络设备及主机资源的安全性，提高运维效率，使得客户的网络管理更加统一、安全和便捷。

1.2 应用场景

满足政策、法规需求：云堡垒机管理系统能满足各类法令法规（如 SOX、PCI、企业内控管理、等级保护、ISO/IEC27001 等）对运维审计的要求。能够细粒度地划分不同角色的权限，达到控制管理员对服务器的访问，并且提供大数据智能审计功能，对所有运维操作能达到很好的审计、监控、控制和历史回放效果。

管理外部 IT 运维人员：许多公司聘请了外部 IT 运维人员来进行各类主机和设备的配置、维护和管理，这些主机中可能包含着重要的邮件、客户信息和关键业务服务，这种行为实际上意味着公司需要绝对信任外部 IT 运维人员。在这种情况下，拥有可靠的外部设备来监控、审计运维操作就显得至关重要。部署云堡垒机管理系统后，既能满足对 IT 运维人员所有操作的记录

和回放，又能实时监控与阻断在线 IT 运维人员，达到对外部 IT 运维人员操作的全监控。

会话协同：通过分享 URL，邀请其他用户共同查看同一会话，并且参与者在会话发起者批准的前提下可对会话进行操作，可应用于远程演示、对运维疑难问题”会诊”等场景。

远程管理的控制：许多公司都拥有需要在互联网上远程管理的主机和设备，部署云堡垒机管理系统，更好的强化对主机或设备的安全管理，追踪每次运维操作的具体细节。

SSH、TELNET、RDP、VNC、SFTP、FTP 协议控制：云堡垒机管理系统能对 SSH、TELNET 等字符控制协议提供支持，利用自身技术优势，无论对加密协议（如 SSH、RDP、SFTP）或非加密协议（如 TELNET、VNC、FTP）都能实现完全的监控和事后审计。让用户对支持不同协议的设备监控和审计操作更加简单和易用。

应用中心：云堡垒机管理系统的应用托管功能，可以实现 RemoteApp 应用程序的托管，同其他协议一样，可以对其进行完全的实时监控、历史回放和审计功能。使用应用托管，将可以进行更多，更大范围的运维审计，如 MySQL 数据库、浏览器等多种应用程序。

第二章 部署安装

2.1 部署方式

2.1.1 云平台上部署

在云平台上创建主机，其中硬盘指定为分发的云堡垒机镜像文件，直接启动主机。各类其他虚拟化平台对主机镜像启动运行的具体方法参考各大虚拟化平台官方提供的使用手册。

2.2 证书导入

进入云堡垒机登录界面，首先下载根证书，以确保浏览器可以正常稳定的访问云堡垒机，点击<下载根证书>，如图 2-2-1 所示。

图 2-2- 1

然后打开下载的证书，点击<安装证书>进行安装，如图 2-2-2 所示。

图 2-2- 2

点击<下一步>，进入证书导入向导界面，如图 2-2-3 所示，点击<完成>即可安装根目录到本地计算机，如图 2-2-4 所示。

图 2-2- 3

图 2-2- 4

第三章 登录云堡垒机

3.1 Web 方式登录

3.1.1 密码方式登录

云堡垒机基于 Web 界面登录的方式，支持各种主流浏览器: IE10 浏览器及以上版本，Chrome 浏览器，Firefox 浏览器，Safari 浏览器等。

请首先启动浏览器，并且输入云堡垒机的 IP 地址和端口（例如 https://192.168.0.254:443）到地址栏，然后按下<Enter> 键，进入登录界面；如图 3-1-1 所示。输入“admin”（云堡垒机默认系统管理员账号） 到用户名输入栏里，输入密码，最后单击<登录>按钮。

图 3-1- 1

3.1.2 手机短信方式登录

输入“admin”（云堡垒机默认系统管理员账号） 到用户名输入栏里，并且输入 admin 的密码，此时点击获取验证码，admin 绑定的手机号码就会收到短信验证码，将收到的短信验证码输入到输入框中，单击<登录>按钮即可登录进云堡垒机，如图 3-1-3 所示。

图 3-1- 3

3.1.3 手机令牌方式登录

使用密码方式直接登录进云堡垒机后，我们可以为用户绑定手机令牌，更好的保证账号安全。如图 3-1-2 所示，输入“admin”（云堡垒机默认系统管理员账号） 到用户名输入栏里，并且输入已经改过的密码，此时还要多加一步，输入手机令牌的动态码（每隔一段时间就会变化），最后单击<登录>按钮即可登录进云堡垒机。

图 3-1- 2

说明：

1）云堡垒机登录采用 Web 方式，使用目前主流操作系统下的常见浏览器（Chrome、Firefox、

Safari 等）都可访问云堡垒机，个别浏览器的新版本可能会出现无法登录的问题，如果出现请换用其他常见浏览器或联系售后人员。
2）为用户开启手机令牌登录方式时，系统管理员须保证系统时间与北京标准时间保持一致，否则用户将无法通过手机令牌方式登录。

3.2 SSH 客户端登录

3.2.1 密码方式登录

云堡垒机也可以使用 SSH 客户端登录的方式，打开 SSH 客户端（比如 Xshell），新建一个会话，在主机栏中输入云堡垒机的 IP 地址（例如 192.168.0.254），在端口号栏中填写默认的端口号 2222，然后点击<确定> 按钮，选择刚刚新建的会话，点击<连接>按钮或是双击刚刚新建的会话，进入登录界面；输入用户名，点击<确定>按钮，并输入密码点击<确定>按钮即可登录成功，如图 3-2-1，3-2-2，3-2-3，3-2-4 所示。

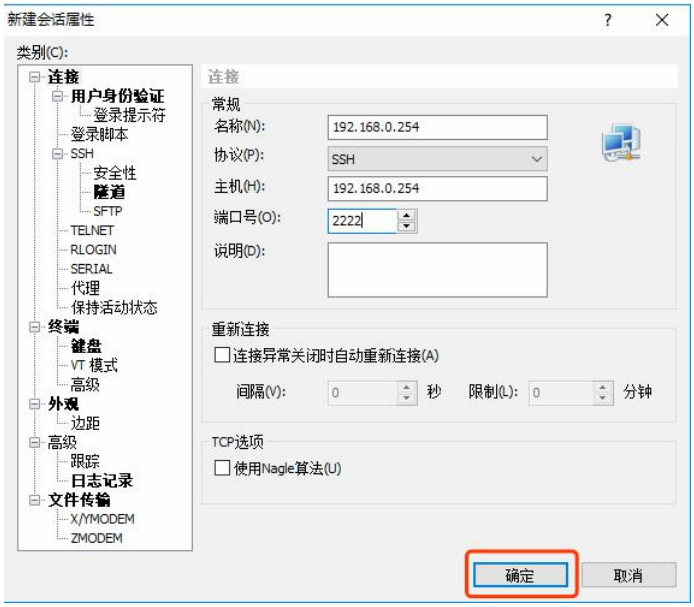


图 3-2- 1

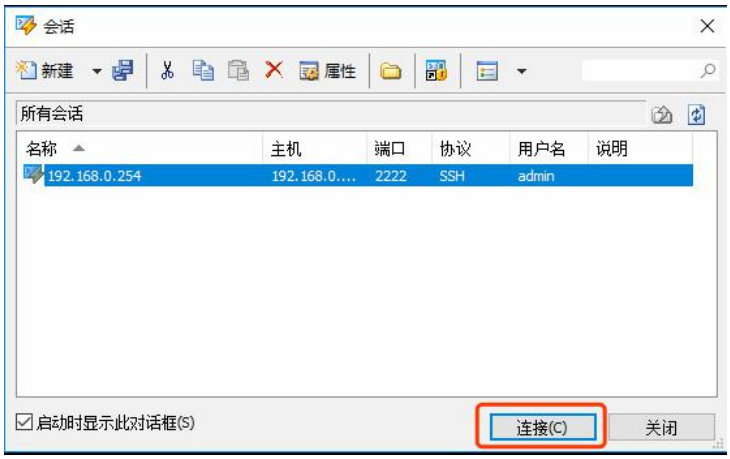


图 3-2- 2

图 3-2- 3

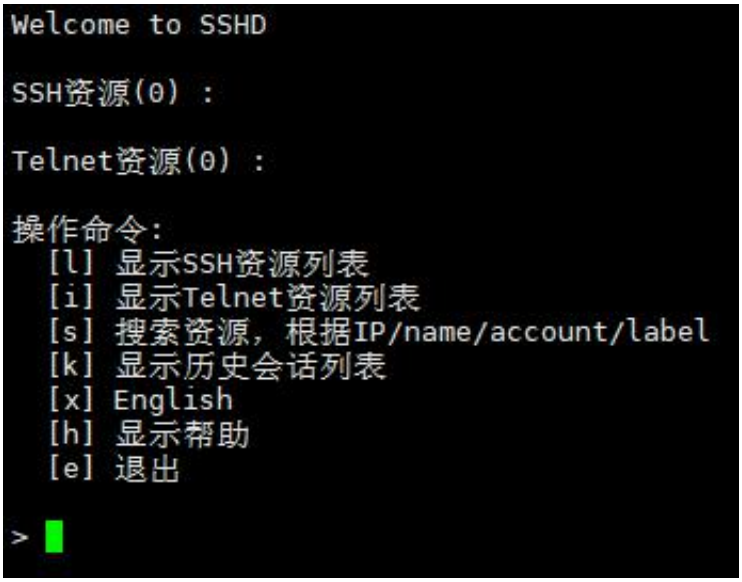


图 3-2- 4

3.2.2 手机短信方式登录

设置用户多因子认证方式为“手机短信”，用户在登录界面输入用户名和密码后，选择短信验证码方式，此时用户绑定的手机号码会收到一条短信验证码，输入正确短信验证码即可成功登录云堡垒机，如图 3-2-5 所示。

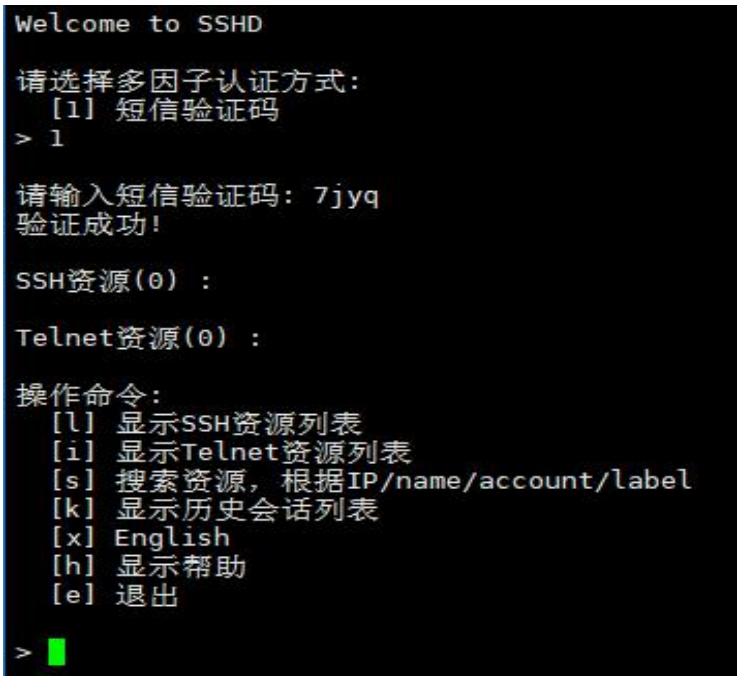


图 3-2- 5

3.2.3 手机令牌方式登录

在用户通过其他登录方式登录系统并已经在个人中心绑定手机令牌后，由管理员设置用户多因子认证方式为“手机令牌”，用户在登录界面选择手机令牌 OTP 方式，输入登录名和密码后，在手机上查看该用户已经绑定过的手机令牌动态密码，输入手机令牌的动态密码即可成功登录云堡垒机，如图 3-2-6 所示。

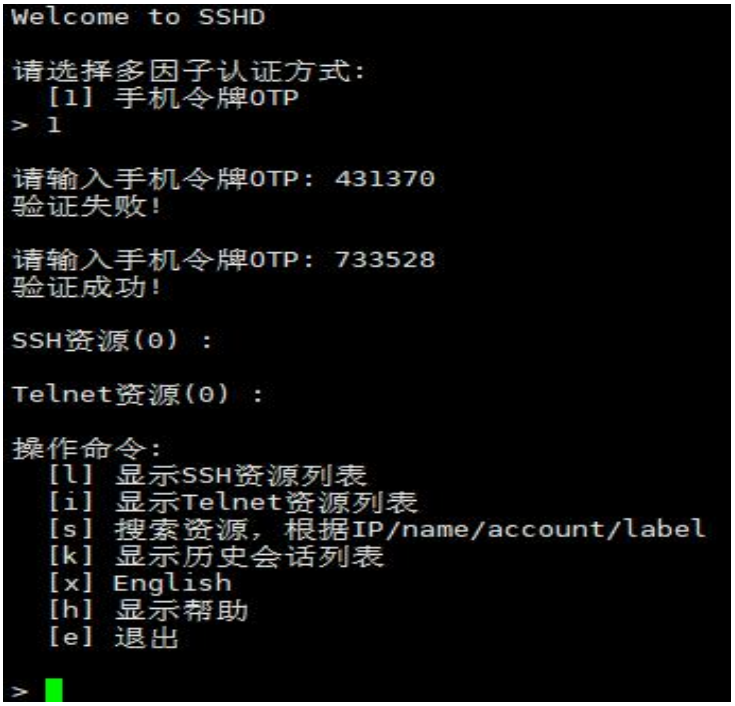


图 3-2- 6

3.3 找回密码

系统管理员创建用户或是用户自行登录系统后，如果填写过正确移动电话号码，在之后的使用过程中用户如果忘记系统登录密码，可以通过登录首页的找回密码功能对密码进行重置。点击登录页面的<忘记密码?>，填写登录账号、手机号和验证码，如图 3-3-1 所示，填写正确信息后，进入重置密码页面，如图 3-3-2 所示，填写符合密码强度要求的新密码，完成密码重置。

图 3-3- 1

图 3-3- 2

第四章 桌面

下面以系统管理员为例讲解其登录后系统桌面的各项含义。

4.1 任务中心

进入[桌面/任务中心]，将会看到正在进行中的任务或已经完成的任务或已经停止的任务（任务共有 9 种，分别是导入用户、导入主机、导入云主机、导入应用、导入应用服务器、导入账户、账户改密、AD 域同步、系统维护，其中系统维护又分为升级和还原），如图 4-1-1 所示。

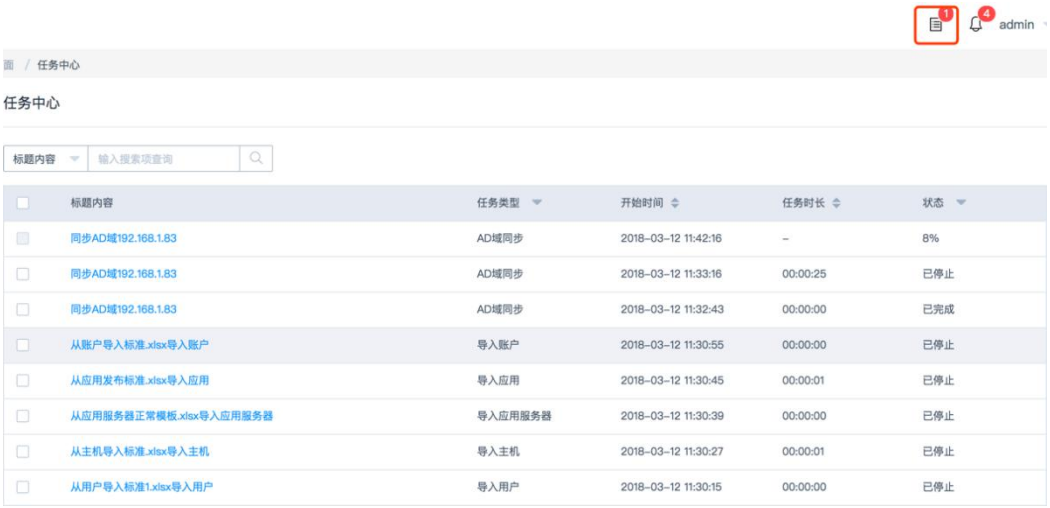


图 4-1- 1

4.2 消息中心

进入[桌面/消息中心]，将会看到各种类型的消息（系统消息、业务消息、任务消息、命令告警、工单消息），并且这些消息还分为高、中、低三个级别，级别越高，在消息中心的按钮小弹窗中颜色就越深，如图 4-2-1 所示。

图 4-2- 1

4.3 个人中心

进入[桌面/个人中心]，将会看到 5 个 tab，分别是个人中心、手机令牌、SSH 公钥、我的权限、我的日志，其中个人中心可以修改当前用户的基本信息和登录密码；手机令牌可以为当前用户绑定手机令牌，用户开启手机令牌登录方式时，就可以使用手机令牌生成的 6 位动态密码成功登录云堡垒机；添加 ssh 公钥后，用户在 ssh 客户端可以免密登录云堡垒机；用户可以在我的权限中查看当前用户角色所拥有的权限；在我的日志中，用户可以查看到自己的系统登录日志、系统操作日志、资源登录日志，如图 4-3-1、4-3-2、4-3-3、4-3-4、4-3-5 所示。

图 4-3-1

图 4-3-2

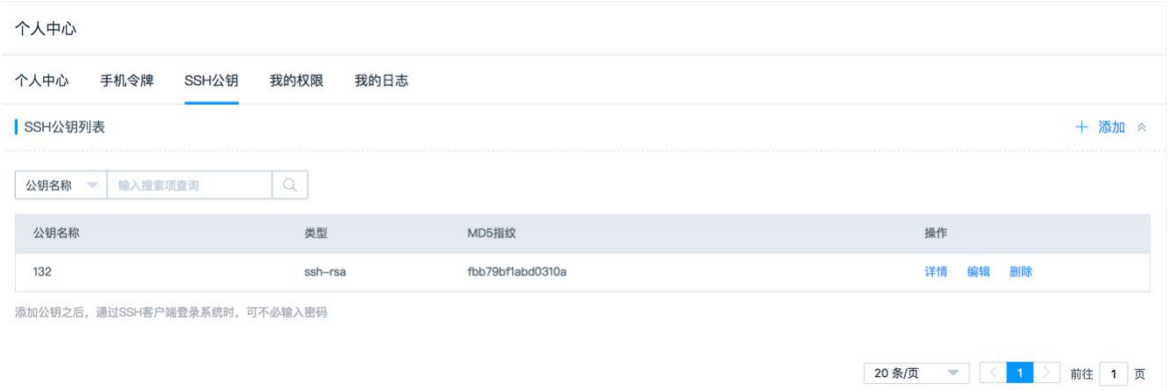


图 4-3-3

图 4-3-4

图 4-3-5

4.4 统计控制板

进入[桌面]，可以查看到关于用户、主机、应用、应用服务器、告警的统计控制板，点击这些统计控制板，即可跳转到相对应的列表页面进行相关操作，该统计控制板是否显示由用户角

色是否拥有用户管理模块权限、主机管理模块权限、应用发布模块权限、应用服务器模块权限和管理权限决定，当权限导致统计控制板只有一个时，默认不显示，如图 4-4-1、4-4-2、4-4-3、4-4-4、4-4-5、4-4-6 所示。

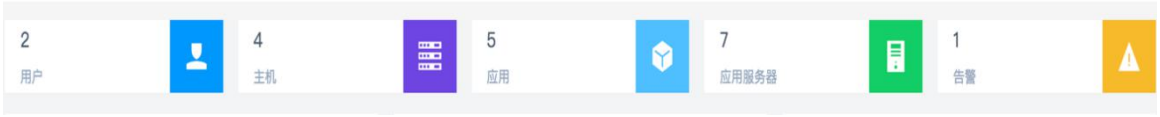


图 4-4-1

图 4-4-2

图 4-4-3

图 4-4-4

图 4-4-5

图 4-4-6

4.5 活动用户

进入[桌面]，查看[活动用户]控制板，可显示用户角色权限范围内的在线用户，点击列表中的用户名可跳转到用户详情。该控制板是否显示由用户角色是否拥有用户管理模块权限和管理权限决定，如图 4-5-1、4-5-2 所示。

图 4-5-1

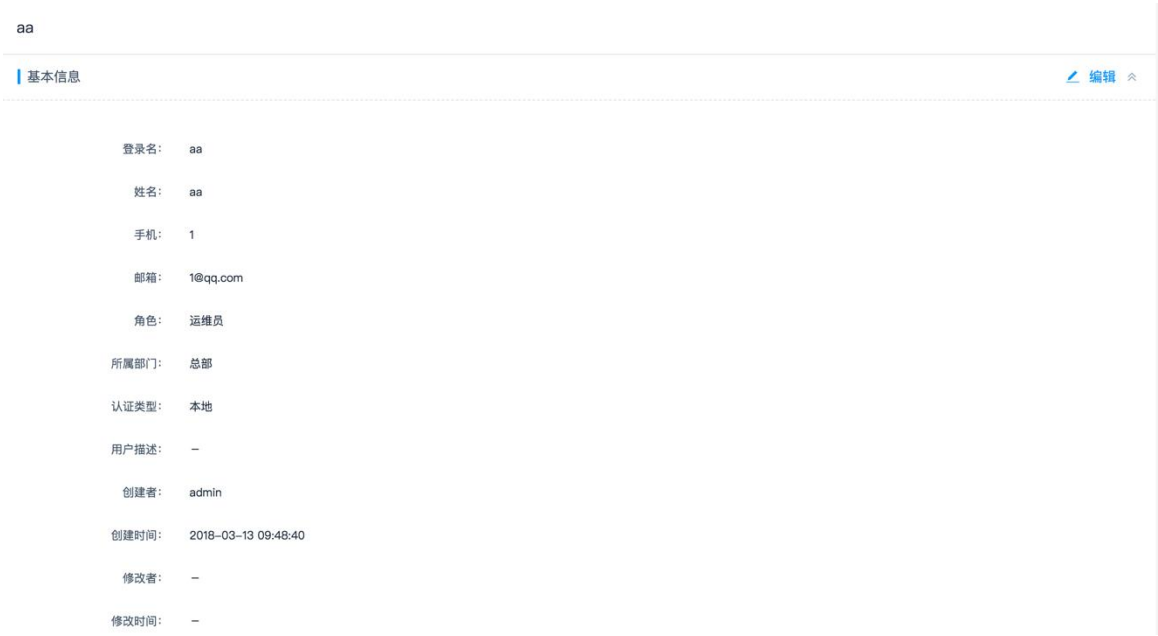


图 4-5-2

4.6 待审批工单

进入[桌面]，查看[待审批工单]控制板，可显示用户角色权限范围内的待审批工单，点击可跳转工单详情。该控制板是否显示由用户角色是否拥有工单审批模块权限和管理权限决定，如图 4-6-1、4-6-2 所示。

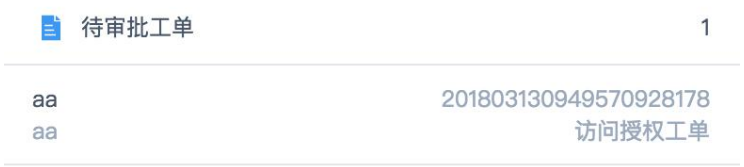


图 4-6-1

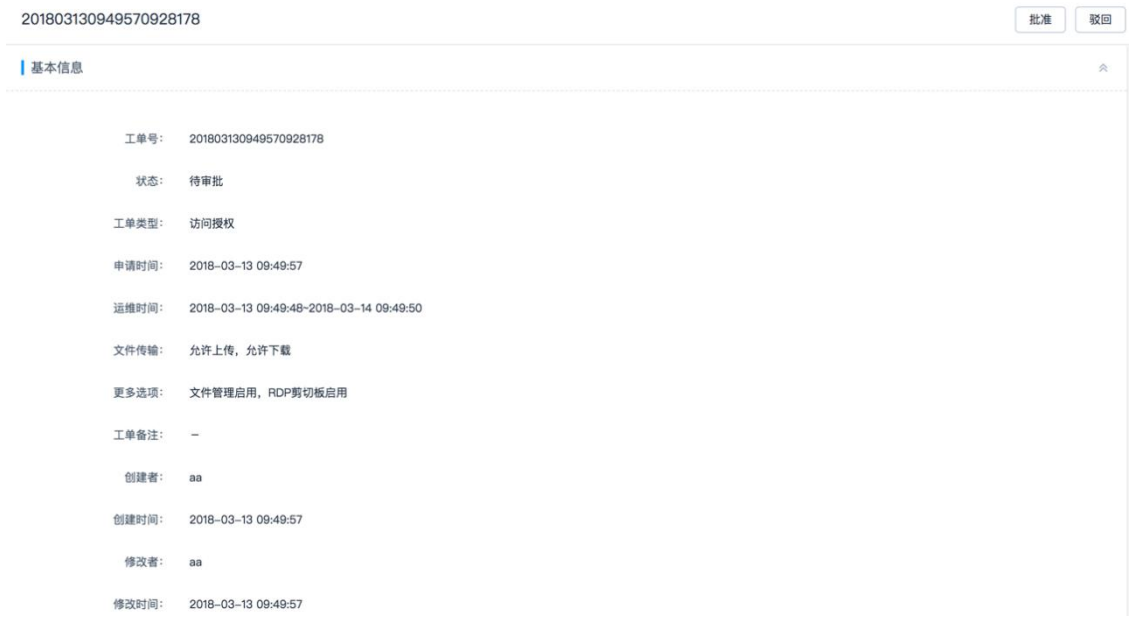


图 4-6-2

4.7 主机类型统计

进入[桌面]，查看[主机类型统计]控制板，可显示用户角色权限范围内的主机类型统计，将鼠标放在统计数据上会有数据显示，点击可跳转到主机管理模块。该控制板是否显示由用户角色是否拥有主机管理模块权限和管理权限决定，如图 4-7-1、4-7-2 所示。

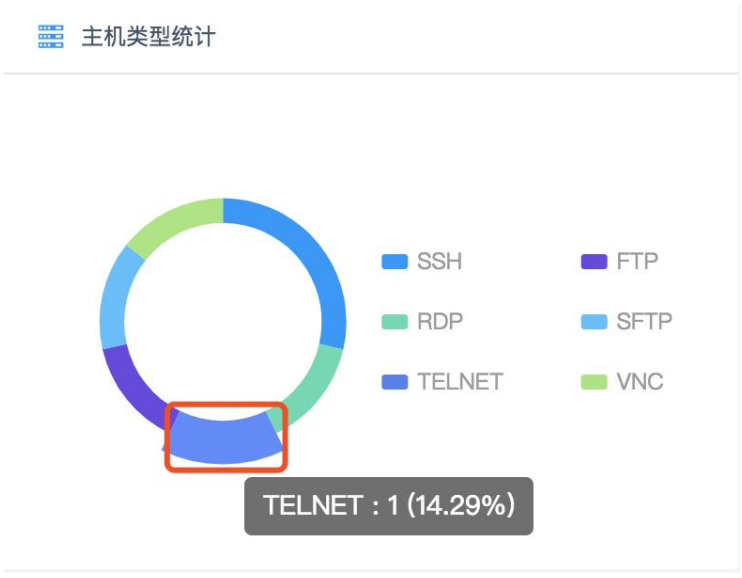


图 4-7-1

图 4-7-2

4.8 应用类型统计

进入[桌面]，查看[应用类型统计]控制板，可显示用户角色权限范围内的应用发布类型统计，将鼠标放在统计数据上会有数据显示，点击可跳转到应用户发布模块。该控制板是否显示由用户角色是否拥有应用发布模块权限和管理权限决定，如图 4-8-1、4-8-2 所示。

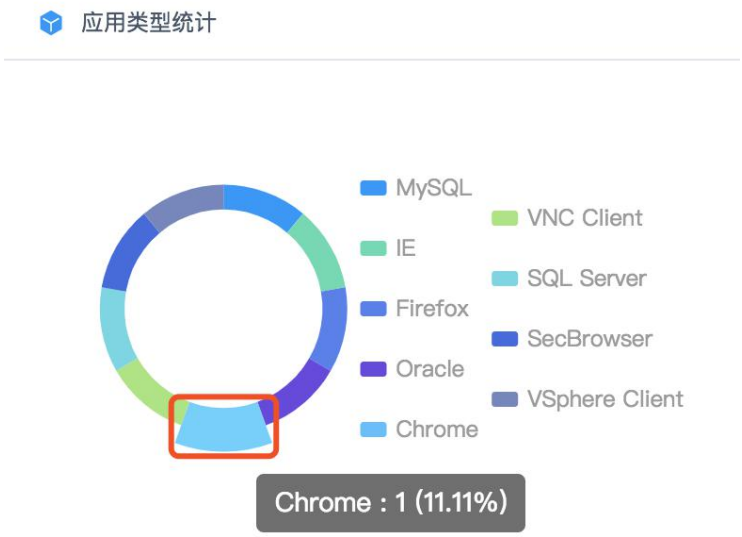


图 4-8-1

图 4-8-2

4.9 当前活动会话

进入[桌面]，查看[当前活动会话]控制板，可显示用户角色权限范围内的实时会话统计，点击对应类型的统计数据可跳转到实时会话模块并进行监控。该控制板是否显示由用户角色是否拥有实时会话模块权限和管理权限决定，如图 4-9-1、4-9-2 所示。

图 4-9-1

图 4-9-2

4.10 今日新增会话

进入[桌面]，查看[今日新增会话]控制板，可显示用户角色权限范围内的历史会话统计，点击对应类型的统计数据可跳转到历史会话模块并进行回放。该控制板是否显示由用户角色是否拥有历史会话模块权限和管理权限决定，如图 4-10-1、4-10-2 所示。

图 4-10-1

图 4-10-2

4.11 登录次数统计

进入[桌面]，查看[登录次数统计]控制板，可显示用户角色权限范围内的用户登录系统次数的周统计和月统计，将鼠标放在某天上，会有对应的数值显示。该控制板是否显示由用户角色是否拥有用户管理模块权限和管理权限决定，如图 4-11-1 所示。

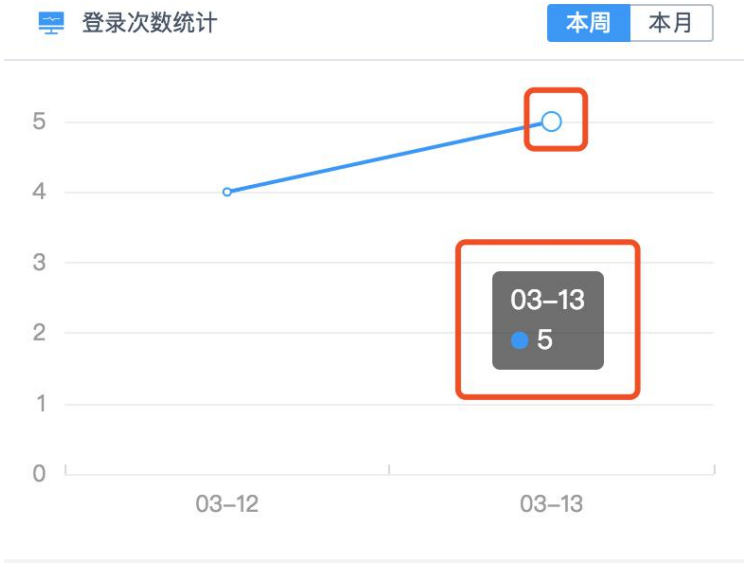


图 4-11-1

4.12 运维次数统计

进入[桌面]，查看[运维次数统计]控制板，可显示用户角色权限范围内的用户登录系统次数的周统计和月统计，将鼠标放在某天上，会有对应的数值显示。该控制板是否显示由用户角色是否拥有历史会话模块权限和管理权限决定，如图 4-12-1 所示。

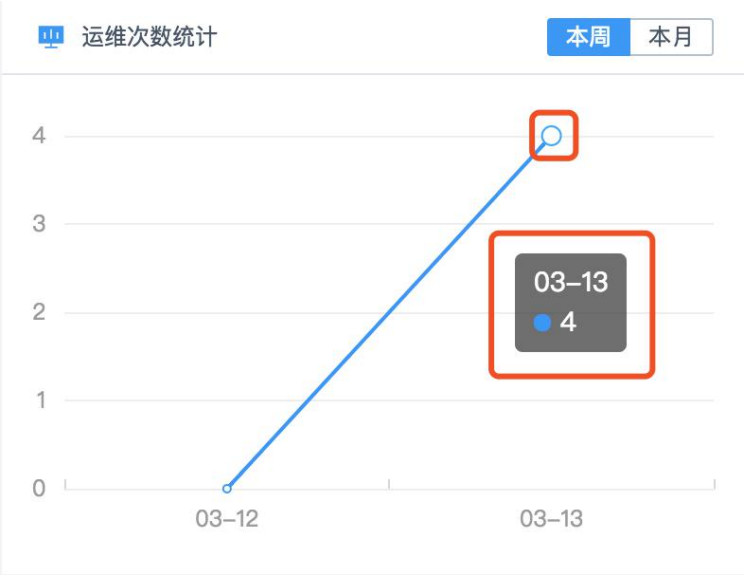


图 4-12-1

4.13 运维用户 Top5

进入[桌面]，查看[运维用户 Top5]控制板，可显示用户角色权限范围内的登录资源次数最多的 5 位用户的周统计和月统计，点击用户，会跳转到对应用户的详情页面。该控制板是否显示由用户角色是否拥有历史会话模块权限和管理权限决定，如图 4-13-1、4-13-2 所示。

图 4-13-1

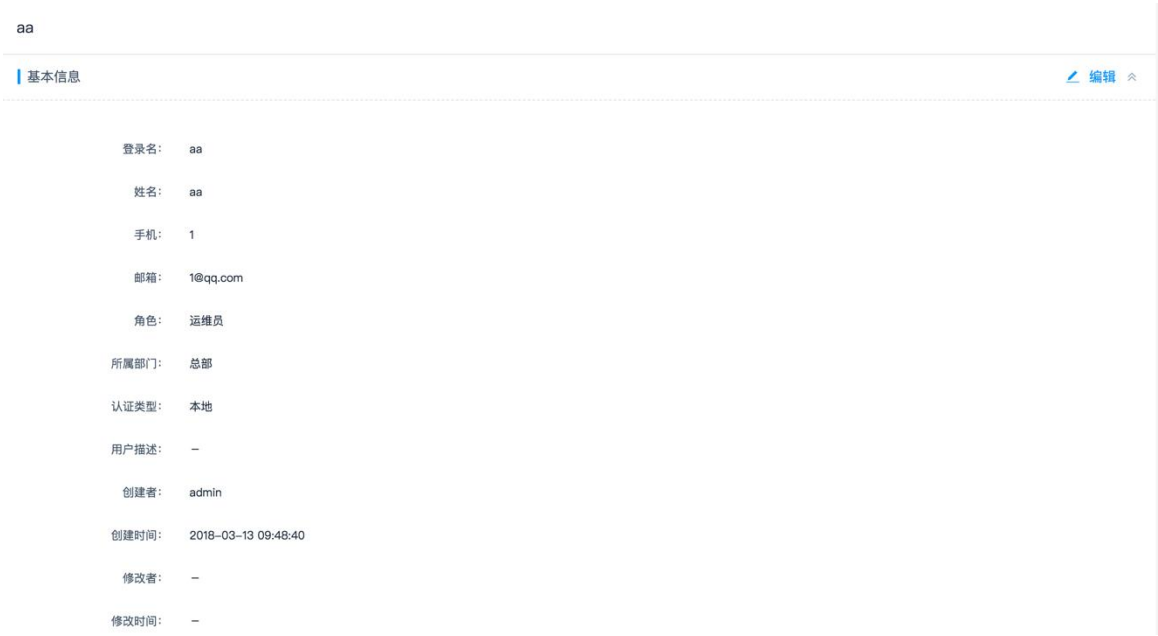


图 4-13-2

4.14 运维资源 Top5

进入[桌面]，查看[运维资源 Top5]控制板，可显示用户角色权限范围内的被登录资源次数最多的 5 个资源的周统计和月统计，点击资源，会跳转到对应资源的详情页面。该控制板是否显示由用户角色是否拥有历史会话模块权限和管理权限决定，如图 4-14-1、4-14-2 所示。

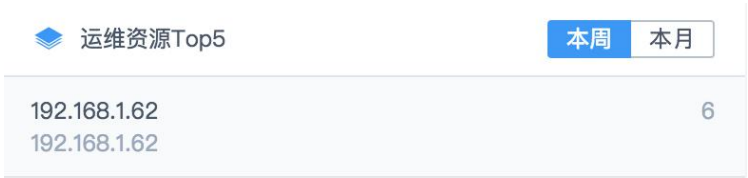


图 4-14-1

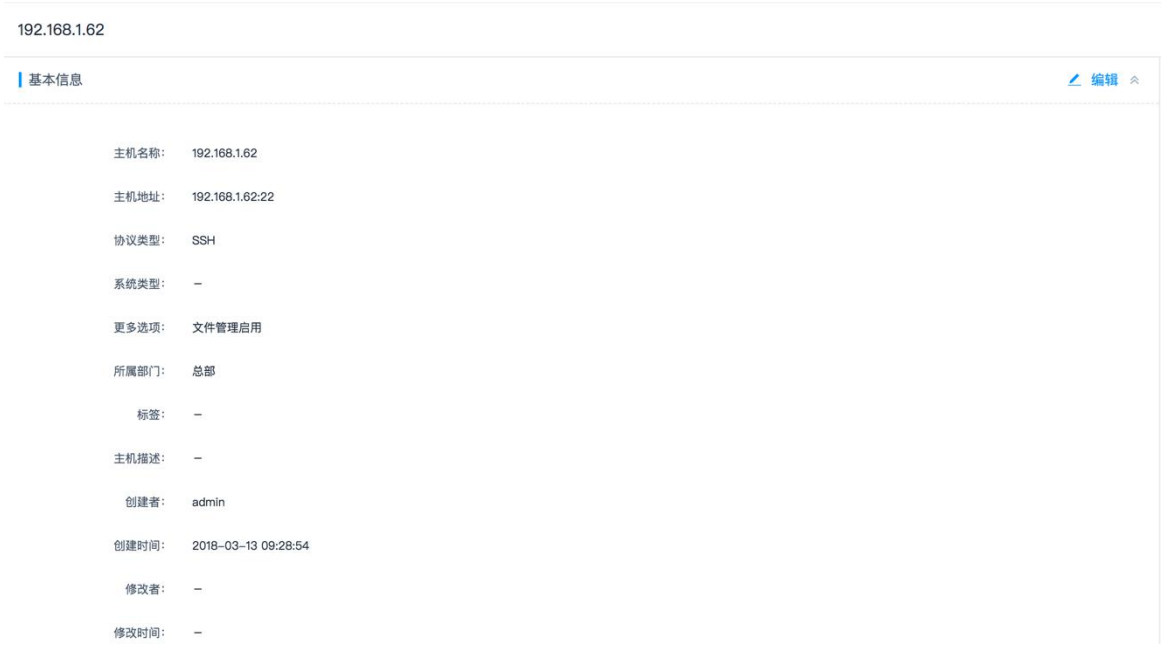


图 4-14-2

4.15 系统状态

进入[桌面]，查看[系统状态]控制板，可显示当前系统的 CPU、内存、磁盘的使用量。该控制板是否显示由用户角色是否拥有系统模块权限和管理权限决定，如图 4-15-1 所示。

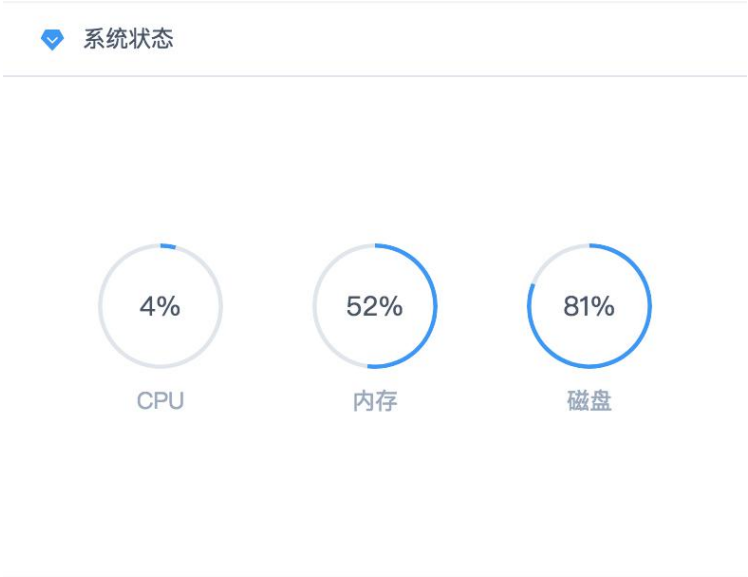


图 4-15-1

4.16 系统信息

进入[桌面]，查看[系统信息]控制板，可显示当前系统的基本信息。该控制板是否显示由用户角色是否拥有系统模块权限和管理权限决定，如图 4-16-1 所示。

图 4-16-1

4.17 最近登录主机

进入[桌面]，查看[最近登录主机]控制板，可显示当前用户最近登录过的主机资源。该控制板是否显示由用户角色是否拥有主机运维模块权限决定，如图 4-17-1 所示。

图 4-17-1

4.18 最近登录应用

进入[桌面]，查看[最近登录应用]控制板，可显示当前用户最近登录过的应用发布资源。该控制板是否显示由用户角色是否拥有应用运维模块权限决定，如图 4-18-1 所示。

图 4-18-1

第五章 部门

部门用于划分组织结构，标识用户、资源等数据的组织归属。

5.1 部门新建

进入[部门]，点击<新建>，进入新建部门界面，如图 5-1-1 所示。

图 5-1- 1

图 5-1- 2

其中“*”标记的红色部分为必填必选项，“上级部门”可以选择管理员能查看到的其他部门作为上级部门，“部门名称”允许填写中文、数字、英文字母等，需要同时创建多个部门时，用”，”分隔部门名称。此外，新建部门支持快速操作，鼠标悬停到部门行时，显示快捷操作按钮，如图 5-1-3、5-1-4 所示：

图 5-1- 3

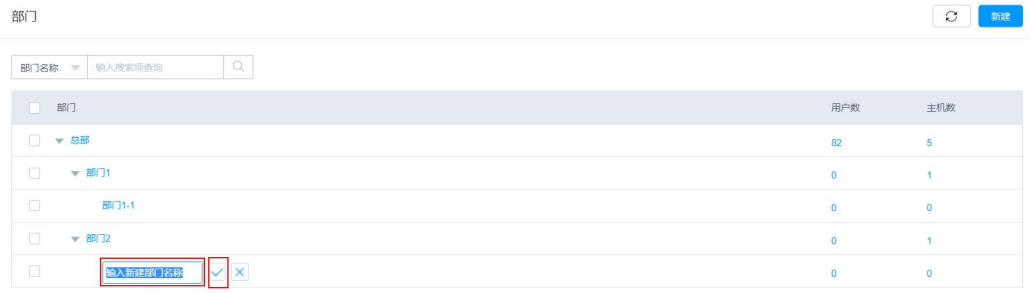


图 5-1- 4

点击所选部门右边的 按钮，在新弹出框内输入新建部门名称，点击 或页面其他区域，完成在所选部门下新建部门的操作。

5.2 部门详情

进入[部门]，点击部门名称进入详情页面，详情信息包括上级部门、部门名称、部门描述等如图 5-2-1 所示。

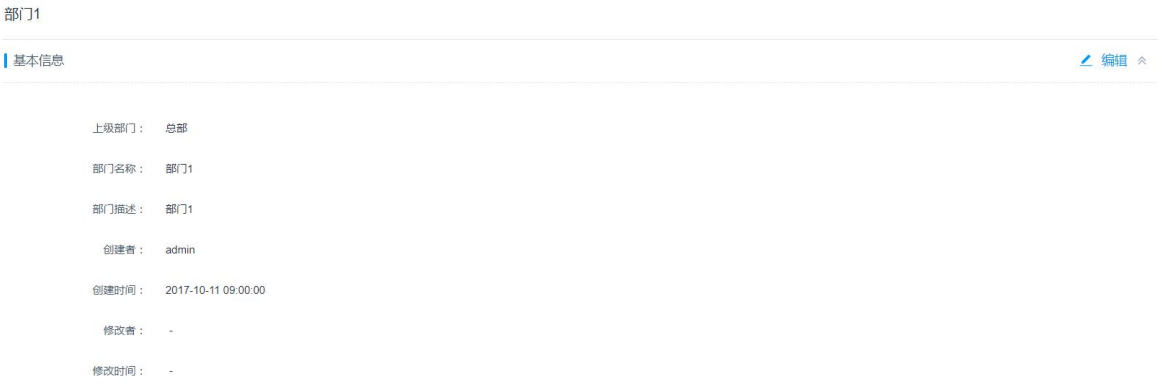


图 5-2- 1

5.3 部门修改

进入[部门]，点击部门名称进入详情页面，点击页面右上方的<编辑>按钮，进入修改部门页面，如图 5-3-1 所示。

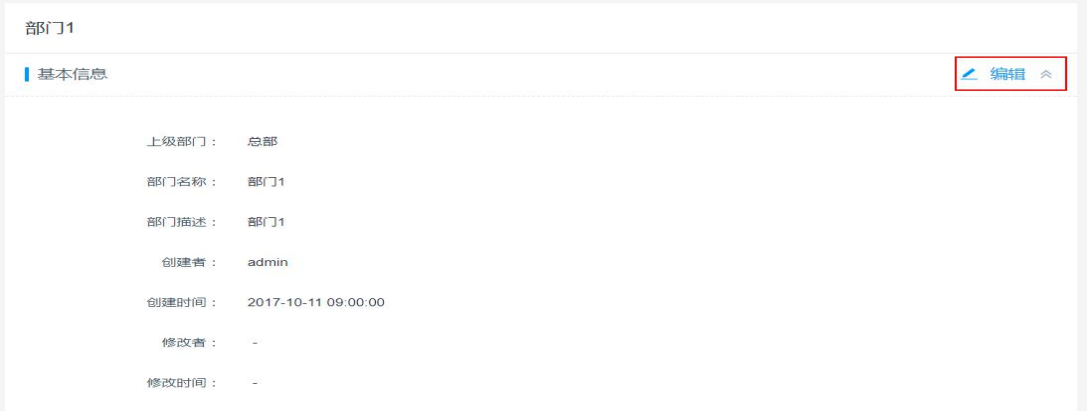


图 5-3- 1

此外，修改部门名称支持快速操作，鼠标悬停到部门行时，显示快捷操作按钮，如图 5-3-2 所示：

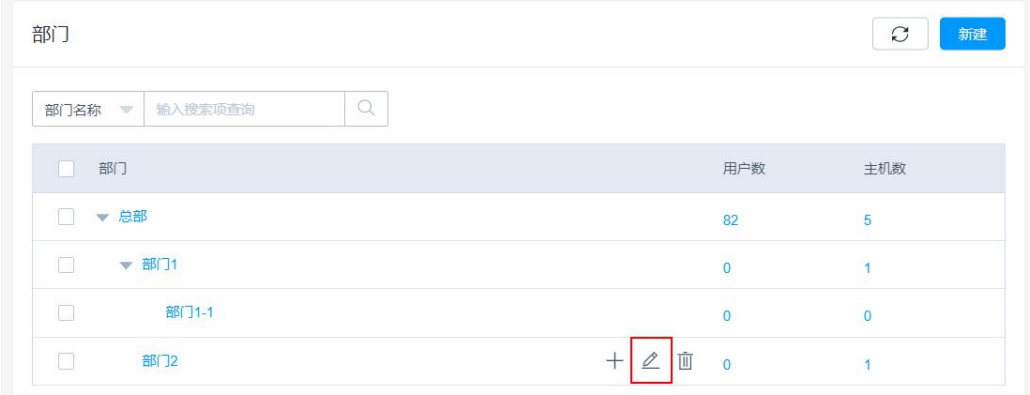


图 5-3-2

点击所选部门右边的 按钮，在编辑框内修改部门名称，点击 或页面其他区域，完成所选部门的名称修改操作。

5.4 部门删除

进入[部门]，快捷删除部门，如图 5-4-1 所示：

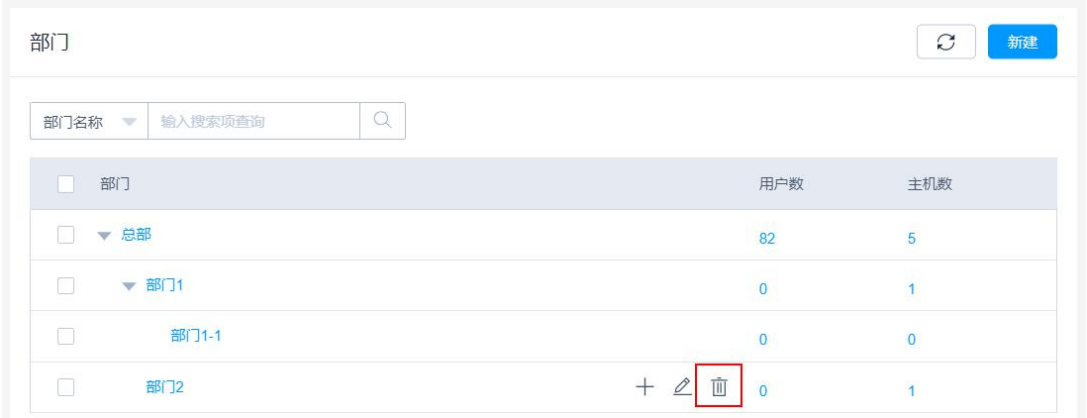


图 5-4-1

支持批量删除部门，勾选部门，点击部门树下方的<删除>按钮，可完成部门的批量删除，如图 5-4-2 所示。部门删除时其下级部门和所有部门下的用户和资源会被同时删除。

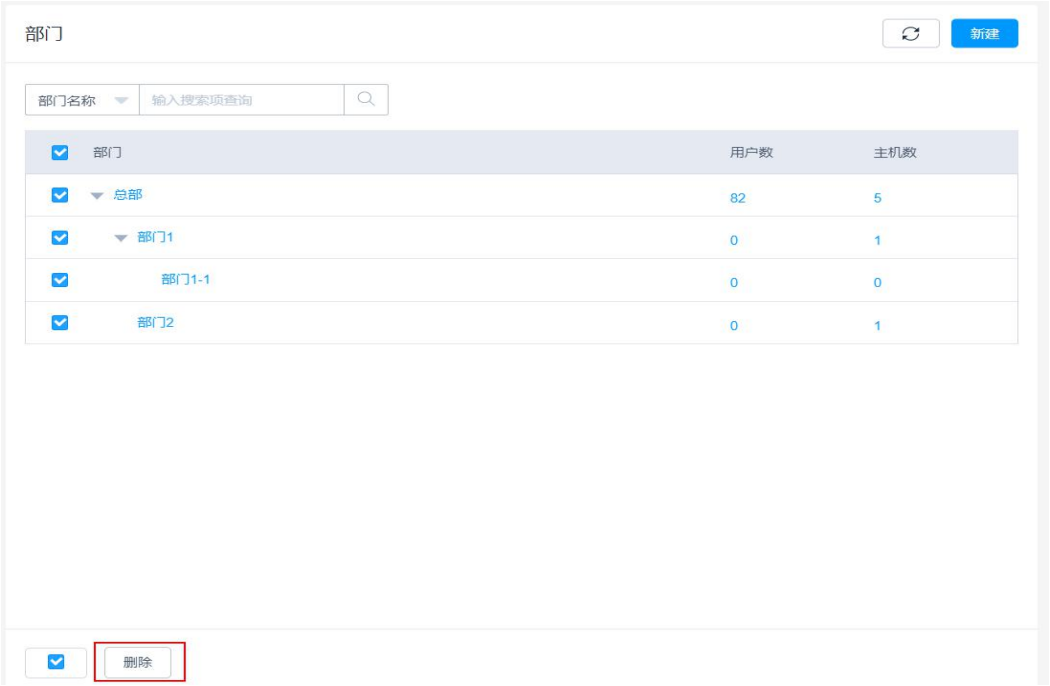


图 5-4-2

5.5 部门查询

进入[部门]，可显示管理员权限范围内的部门树结构，可通过”部门名称”对部门进行查询，如图 5-5-1 所示。

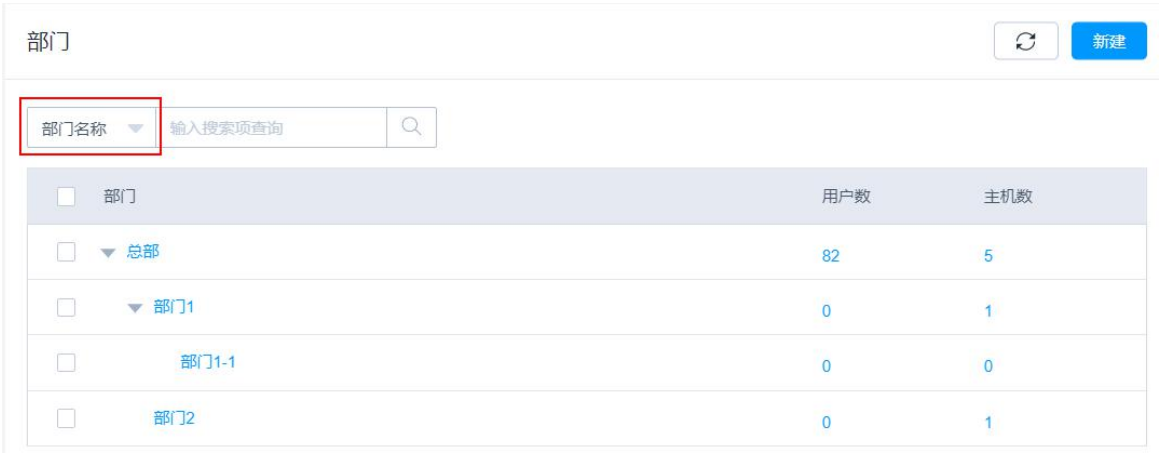


图 5-5- 1

第六章 用户

6.1 用户管理

6.1.1 用户新建

进入[用户/用户管理]，点击页面右上方的<新建>按钮，进入新建用户页面，如图 6-1-1 所示。

图 6-1-1

进入[用户新建]界面，编辑用户信息，其中“*”标记的红色部分为必填项。其中需要注意的是新密码和确认密码的填写需要保存一致；点击<随机生成>，可以自动生成随机密码；点击复制密码，可以将密码复制到粘贴板。填写好所有必填项信息后，点击<确定>按键完成创建。如图 6-1-2 所示。

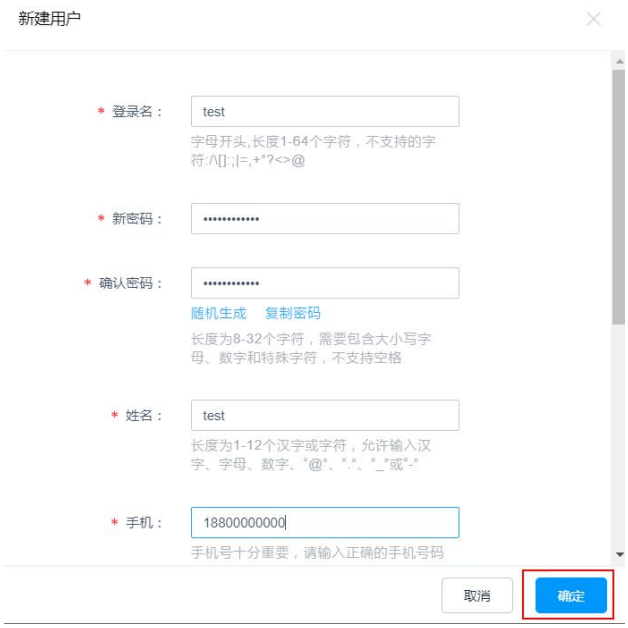


图 6-1-2

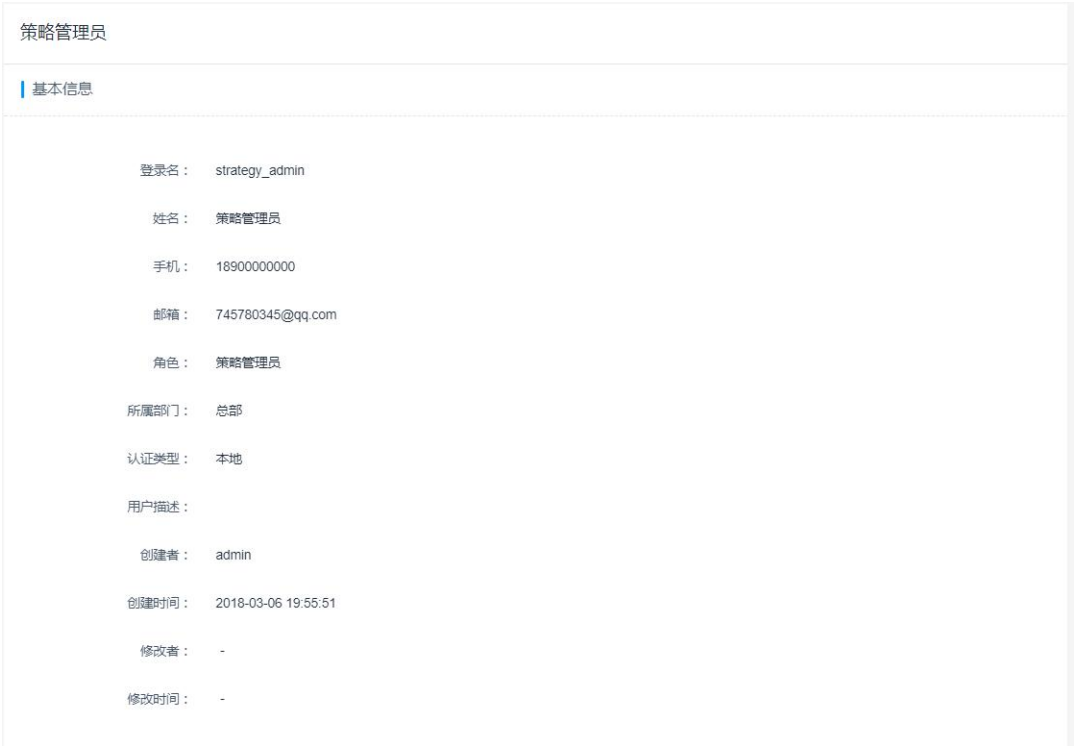
当用户认证类型选择“AD 域”或“RADIUS”时，请参考[系统/系统配置/认证配置]相关章节，进行 AD 域或 RADIUS 服务器的配置操作。

6.1.2 用户详情

进入[用户/用户管理]，点击指定用户的登录名或者是操作中的<管理>按钮，进入用户详情页面，如图 6-1-3 所示

图 6-1-3

进入[用户详情]界面后，可以查看和编辑用户的基本信息、用户配置信息和用户加入的组，如图 6-1-4、6-1-5 所示。



图

6-1-4

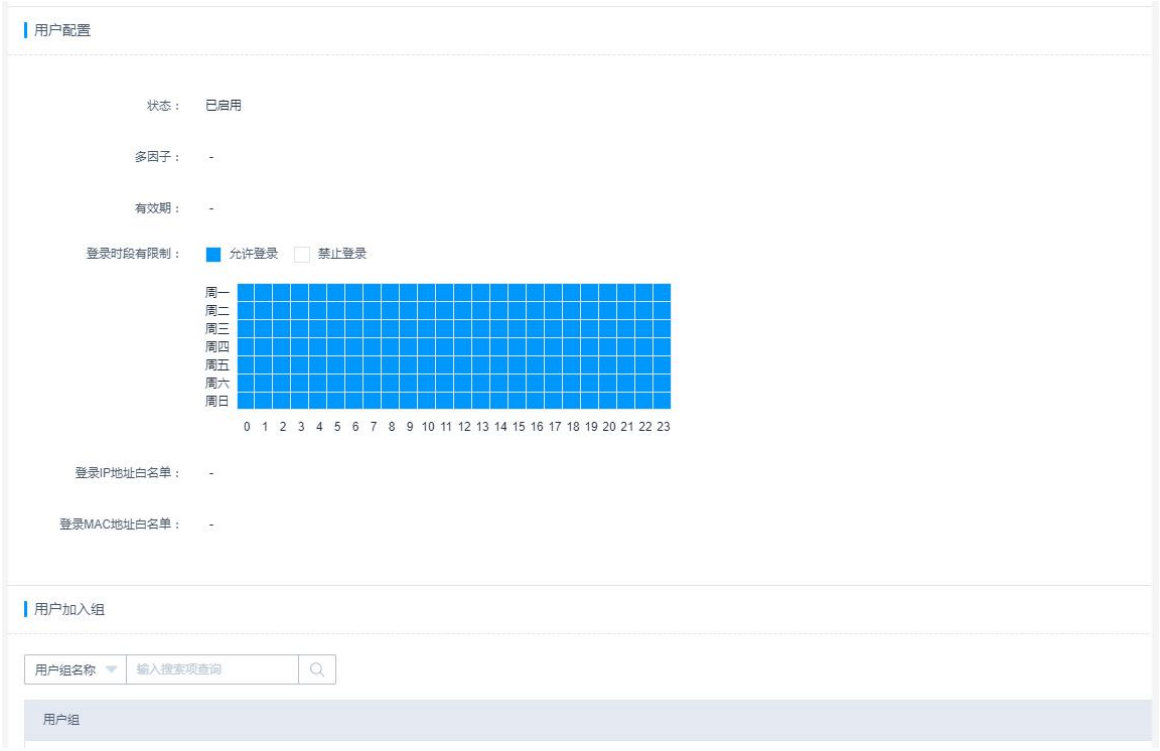


图 6-1-5

6.1.3 用户修改—编辑基本信息

进入[用户详情]界面后，点击基本信息的<编辑>按钮，如图 6-1-6 所示。

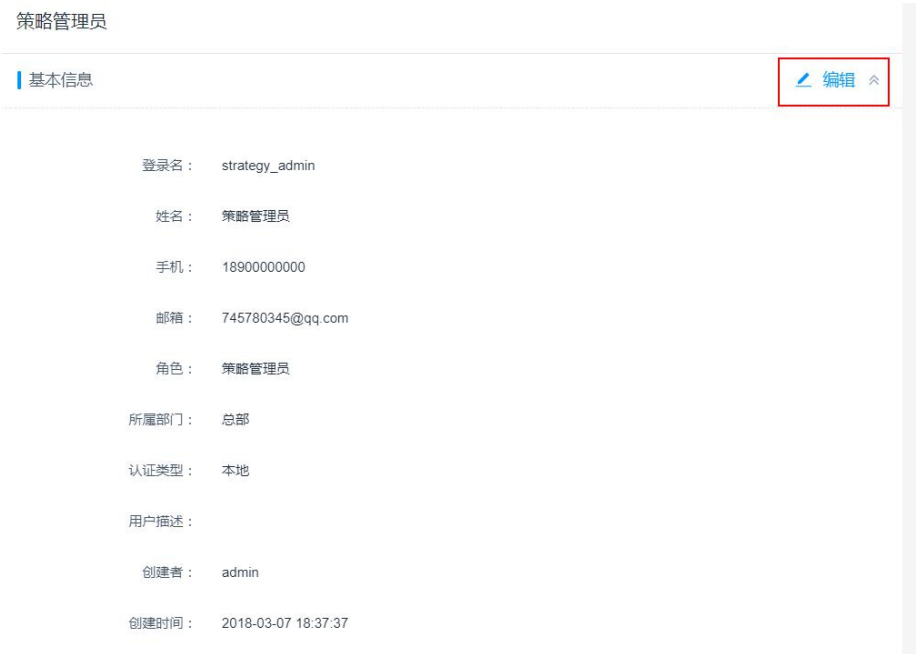


图 6-1-6

进入编辑[基本信息]界面后，可以进行相关操作，修改基本信息，点击<确定>按键保存修改信息，如图 6-1-7 所示。

图 6-1-7

6.1.4 用户修改—编辑用户配置信息

进入[用户详情]界面后，点击用户配置的<编辑>按钮，如图 6-1-8 所示。

图 6-1-8

进入编辑[用户配置]界面后，可以编辑用户的状态、多因子认证、有效期、登录限制等配置，

点击<确定>按键保存修改信息，如图 6-1-9 所示。

图 6-1-9

6.1.5 用户修改—编辑用户组信息

进入[用户详情]界面后，点击用户加入组的<编辑>按钮，如图 6-1-10 所示。

图 6-1-10

进入编辑[编辑用户组]界面后，可以将用户加入组、移出组，点击<确定>按键保存修改信息，如图 6-1-11 所示。

图 6-1-11

6.1.6 用户删除

进入[用户/用户管理]，点击指定用户对应操作中的<删除>按键，可以删除单个指定用户，如图 6-1-12 所示。

图 6-1-12

在用户列表中，同时勾选多个用户，然后点击列表下方的<删除>，可以一次性删除多个用户组，如图 6-1-13 所示。

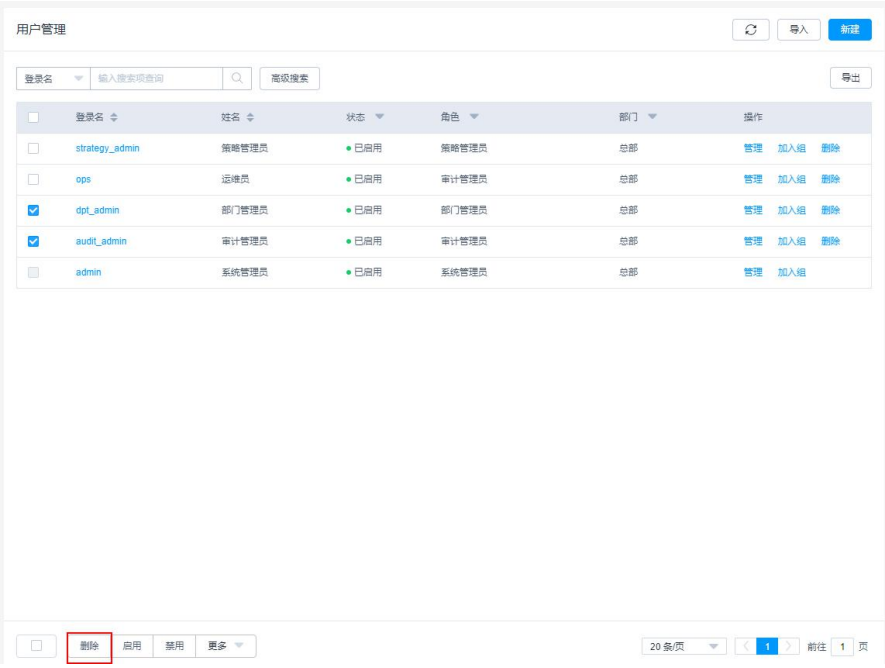


图 6-1-13

注意：系统管理员 admin 无法被删除。

6.1.7 用户查询

进入[用户/用户管理]，如图 6-1-14 所示，可以对登录名、姓名、手机、邮箱进行快速查询。

图 6-1-14

进入[用户/用户管理/高级搜索，]如图 6-1-15、6-1-16，可使用组合条件进行高级搜索。

图 6-1-15

图 6-1-16

6.1.8 加入用户组

进入[用户/用户管理]，点击指定用户对应操作中的<加入组>按键，可以将用户加入或者移除组，如图 6-1-17 所示。

图 6-1-17

6.1.9 用户导入

进入[用户/用户管理]，点击<导入>进行批量导入用户，如图 6-1-18 所示。

图 6-1- 18

进入导入用户界面后，首先点击<点击上传>，选择要导入的文件进行上传，如图 6-1-19 所示。

图 6-1-19

下一步，在弹出的本地目录中选择需要导入的文件，如图 6-1-20 所示。

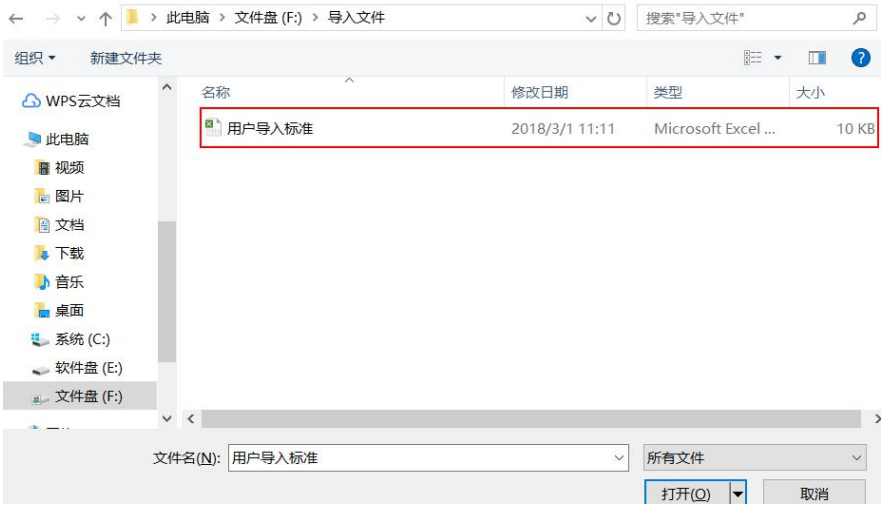


图 6-1-20

注意：

1. 支持上传的文件类型：CSV、xls、xlsx
2.点击覆盖已有用户：a.选中时，当登录名重复时会覆盖用户
覆盖用户将会更新现有用户的用户信息，不会删除用户重新创建
b.未选中，则跳过登录名重复的用户

6.1.10 用户导出

进入[用户/用户管理]，点击<导出>进行批量导出用户（注：如果未选中任何用户，点击【导出用户】，则导出全部用户；如有选中用户，点击【导出用户】，则导出选中用户），如图 6-1-21 所示。

图 6-1-21

6.1.11 批量操作

进入[用户/用户管理]，在用户列表中勾选多个要批量操作的用户，如图 5-1-22 所示，进入用户批量操作界面。

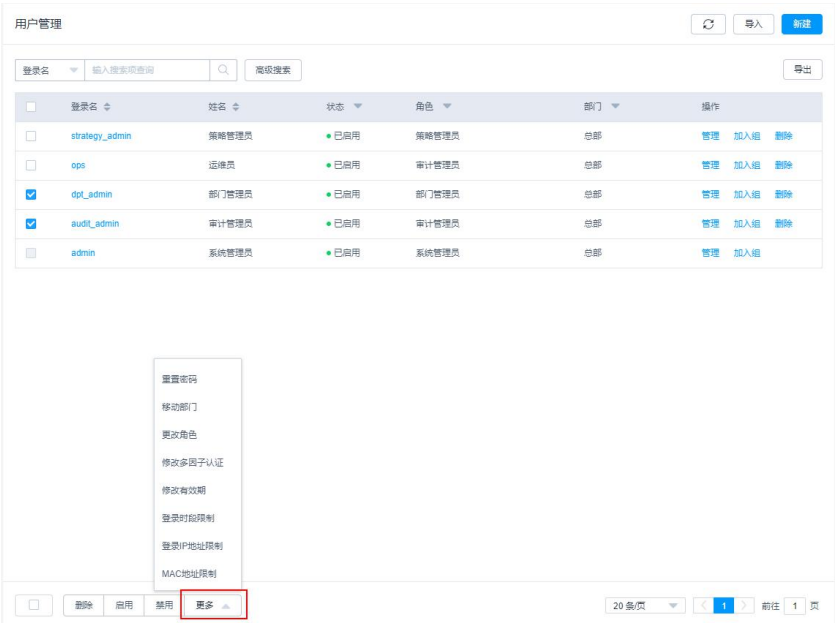


图 5-1- 22

注意：

1. 批量操作包括：删除、启用（可解锁锁定用户）、禁用、重置密码、移动部门、更改角色等

2.当没有用户被选中时，<更多>按键是被禁用的

6.2 用户组

6.2.1 用户组新建

进入[用户/用户组]，点击<新建>，进入新建用户组界面，如图 6-2-1 所示。

图 6-2-1

编辑用户组信息，其中“*”标记的为必填项。点击<确定>完成保存。

6.2.2 用户组详情

进入[用户/用户组]，点击指定用户组名称或者是用户组的列表操作<管理>，进入用户组详情，如图 6-2-2、6-2-3 所示。

图 6-2-2

图 6-2-3

6.2.3 用户组修改

进入[用户组详情]，点击基本信息的<编辑>，可以修改用户的基本信息；点击用户组成员的<编辑>，可以将用户移除或者加入组，如图 6-2-4 所示。

图 6-2-4

6.2.4 用户组删除

进入[用户/用户组]，点击指定用户组的列表操作<删除>，如图 6-2-5 所示。

图 6-2-5

在用户组列表中，同时勾选多个用户组，然后点击列表下方的<删除>，可以一次性删除多

个用户组，如图 6-2-6 所示。

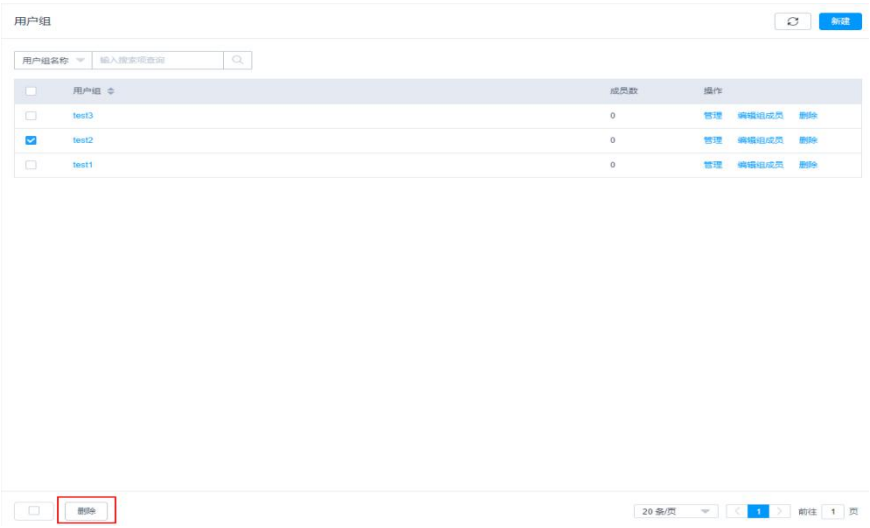


图 6-2-6

6.2.5 用户组查询

进入[用户/用户组]，如图 6-2-7 所示，可以对用户组名称进行快速查询。

图 6-2-7

6.2.6 编辑组成员

进入[用户/用户组]，点击<编辑组成员>按钮，批量将用户加入或移出用户组，如图 6-2-8 所示。

图 6-2-8

进入添加组成员界面，勾选左侧列表中的用户移动到右侧列表中，如图 6-2-9 所示。

图 6-2-9

6.3 角色

6.3.1 角色新建

进入[用户/角色]，点击<新建>按钮，如图 6-3-1 所示。

图 6-3-1

编辑用户组信息，其中“*”标记的为必填项。点击<确定>完成保存。

注意：

1. 管理权限:

a.选择【开启】，则该角色具有管理权限，能够查看本部门及下级部门的数据

b.选择【关闭】，则该角色没有管理权限，默认选择【关闭】

6.3.2 角色详情

进入[用户/角色]，点击指定角色名称或者是列表操作<管理>，如图 6-3-2、6-3-3 所示。

图 6-3-2

图 6-3-3

6.3.3 角色修改

进入角色详情，点击基本信息<编辑>按钮，编辑角色的基本信息；点击角色权限<编辑>，编辑角色的模块权限和功能权限，如图 6-3-4 所示。

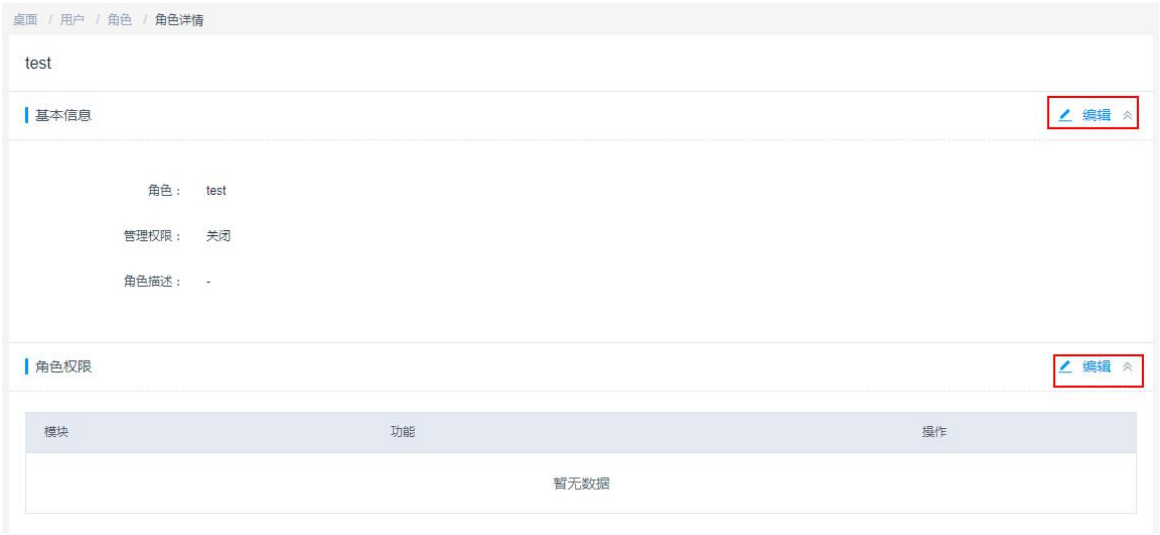


图 6-3-4

编辑基本信息，可以修改角色的名称、管理权限、角色描述，如图 6-3-5 所示。

图 6-3-5

编辑角色权限，可以修改角色的模块权限和功能权限，如图 6-3-6 所示。

图 6-3-6

6.3.4 角色删除

进入[用户/角色]，点击自定义角色列表项后的<删除>按钮，如图 6-3-7 所示。

图 6-3-7

支持批量删除，勾选自定义角色，点击下方的<删除>按钮，如图 6-3-8 所示。

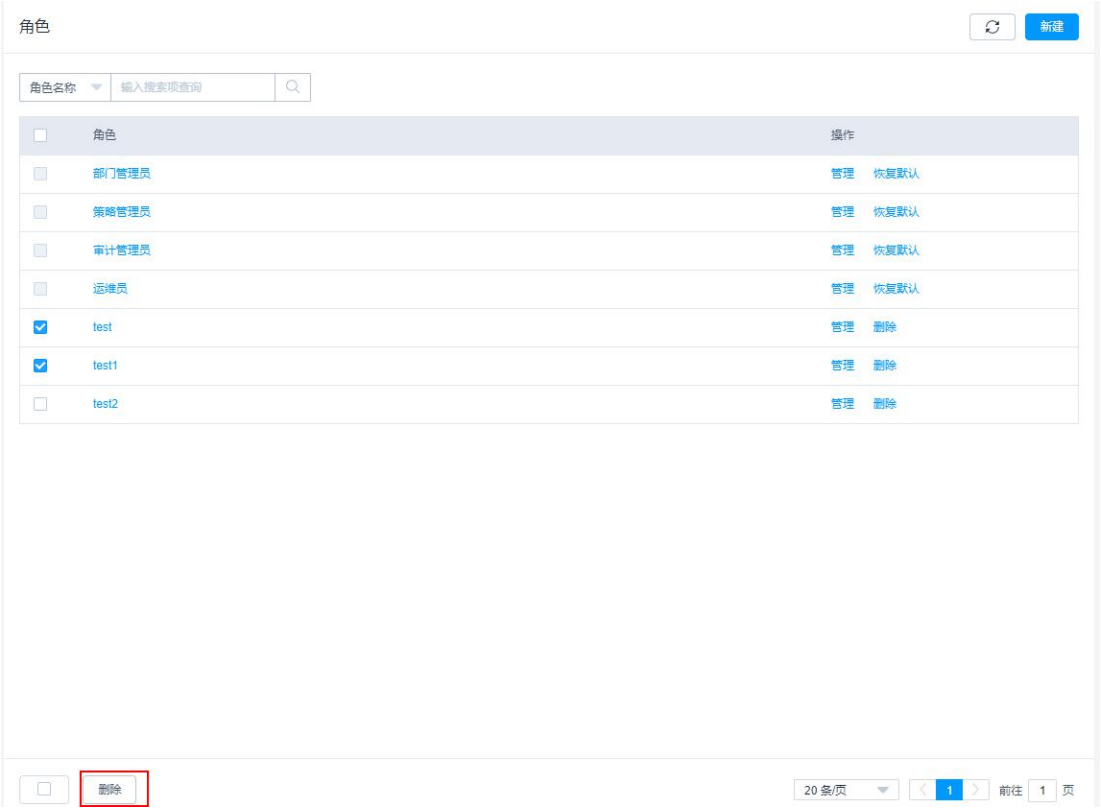


图 6-3-8

注意：

1. 预置角色无法被删除。
2. 预置角色有：超级管理员、部门管理员、策略管理员、审计管理员、运维员
3. 当没有角色被选中时，批量删除按键被禁用

6.3.5 角色查询

进入[用户/角色]，可以通过搜索角色名称查询角色，如图 6-3-9 所示。

图 6-3-9

6.3.6 恢复默认

预置角色可恢复默认设置，进入[用户/角色]，点击列表项后的<恢复默认>按钮，如图 6-3-10 示。

图 6-3-10

第七章 资源

7.1 主机管理

7.1.1 主机新建

进入[资源/主机管理]，点击<新建>，如图 7-1-1 所示。

图 7-1-1

进入新建主机，其中“*”为必填项，编辑主机的基本信息，进入[新建主机]界面，首先填写主机基本信息，输入主机参数，其中“*”标记的红色部分为必填项，“主机名称”允许填写中文、数字、英文字母等，“协议类型”可选 SSH、RDP、VNC、TELNET、FTP、SFTP，“主机 IP”填写需要被云堡垒机管控的主机 IP 地址，“端口”根据所选主机类型可自动填写，也可修改，“所属部门” 为主机归属部门。其余为非必填项，如图 7-1-2 所示。

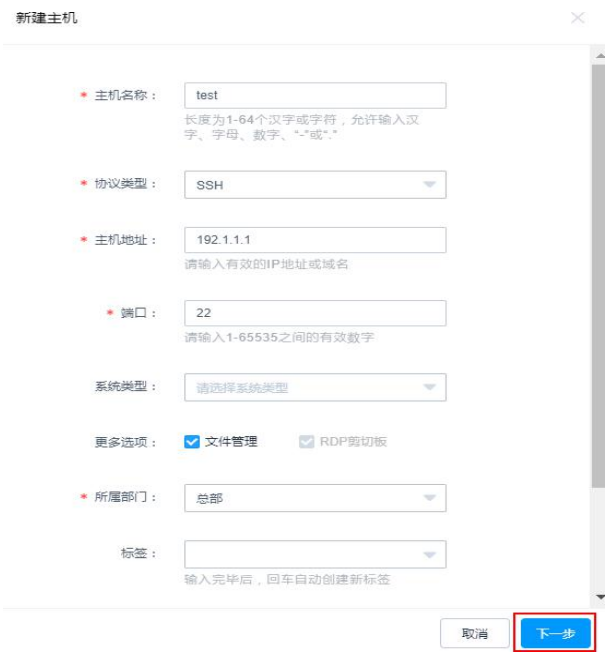


图 7-1-2

如果新建 RDP 主机，选择 RDP 协议后，会出现 RDP 剪切板选项，该选项用于在登录 RDP 资源之后，决定是否允许用户将远程 RDP 主机里的文本复制到本地，RDP 剪切板未开启时，禁止远程和本地之间的数据传输，见图 7-1-3。

图 7-1-3

如果新建的是 RDP 和 SSH 主机，会出现文件管理选项，见图 7-1-4。

图 7-1-4

填写好主机基本信息后，点击<下一步>，添加主机账户信息，如图 7-1-5 所示，

图 7-1-5

除了密码登录方式，云堡垒机对 Linux 主机还支持 SSH Key 秘钥代理登录方式，用户可通过第三方工具（例如 putty）或 Linux 系统命令 ssh-keygen 生成秘钥对。将生成的公钥导入被管控主机的登录账户目录下的 authorized_keys 文件内（如/root/.ssh/authorized_keys），私钥内容和私钥对应的 passphrase 填写到云堡垒机系统中的资源账户内，如图 7-1-6 所示。

图 7-1-6

注意：

1. 选中【以后添加】时，点击【确定】，自动创建一个[空账户]（一个主机仅包含一个[空账户]），例外：FTP/SFTP 不创建空账户
2. 选中【立即添加】时，账户信息填写正确，点击【确定】，如果无[空账户]，则创建一个[空账户]
3. 当选择的资源为 VNC 协议时，提示：如果没有账户，请自定义一个账户名用于标识
4. 特权账户，用于改密策略当中的使用特权账户改密功能，特权账户仅有一个
5. 文件管理例外情况：当文件管理开启，而实际上主机并不支持时，文件管理 tab 依旧显示，下方空白，并提示当前主机不支持文件管理功能；如果云主机无法使用文件管理，则主机网盘和云主机文件都无法使用
6. 每个主机最多绑定 10 个标签

7.1.2 主机详情

进入[资源/主机管理]，点击主机名称或<管理>按钮进入详情页面，可以查看到主机的基本信息和资源账户信息，如图 7-1-7 所示。

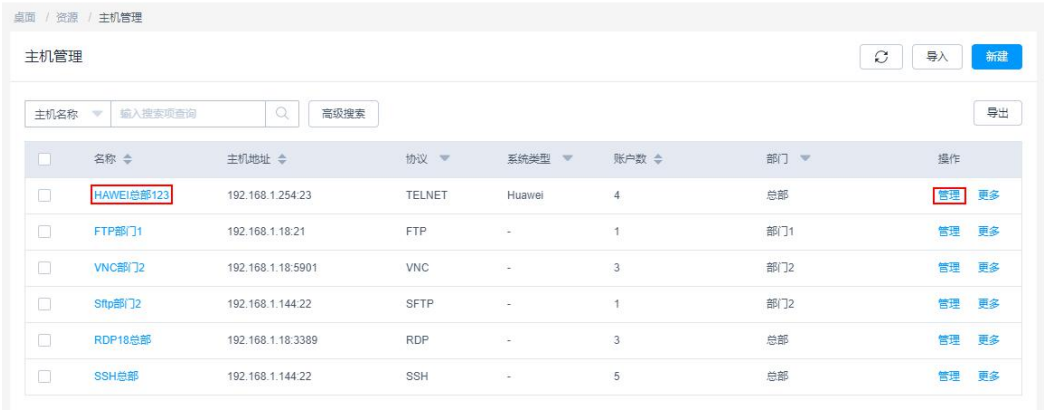


图 7-1-7

7.1.3 主机修改

进入主机详情，点击基本信息的<编辑>，修改主机的基本信息，如图 7-1-8 所示；点击资源账户的<添加>，添加资源账户，如图 7-1-9 所示。

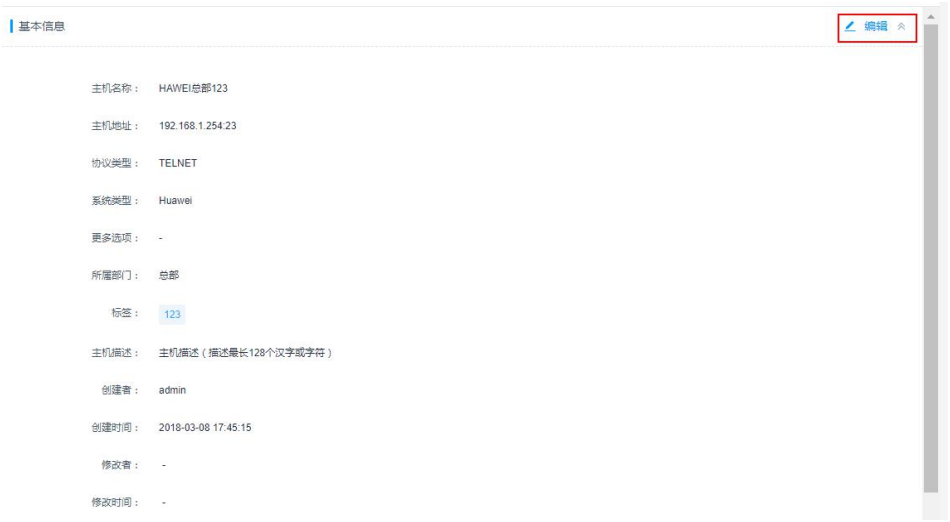


图 7-1-8

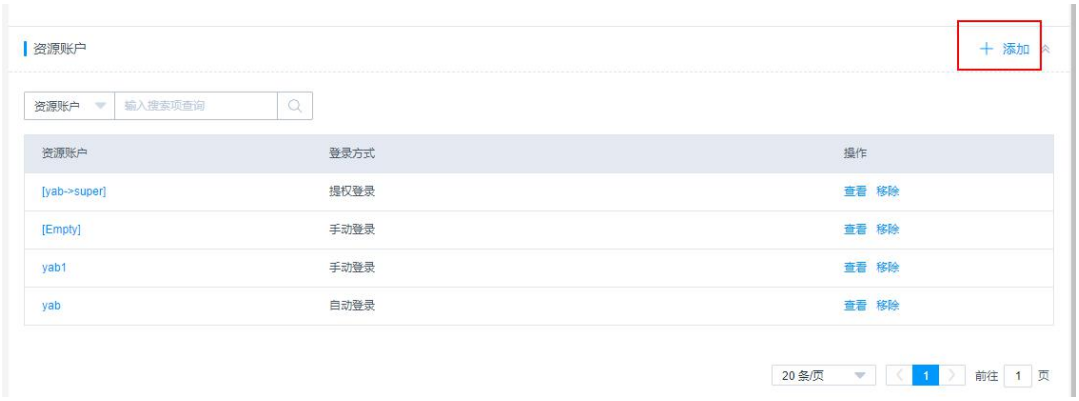


图 7-1-9

注意：

1. 在主机详情的资源账户列表，点击【查看】，跳转到资源账户模块，打开账户详情页面
2. 点击【移除】，移除主机账户

7.1.4 主机删除

进入[资源/主机管理]，选择指定机器，点击<更多/删除>按钮，如图 7-1-10 所示。

图 7-1-10

支持批量删除主机，勾选需要删除的主机，点击下方的<删除>按钮，如图 7-1-11 所示。

图 7-1-11

7.1.5 主机查询

进入[资源/主机管理]，选择搜索项（支持搜索主机名称、主机地址、标签名称），在搜索输入框内输入关键词，点击查询结果，如图 7-1-12 所示。

图 7-1-12

除了普通搜索，还支持高级搜索。点击高级搜索，可以搜索同时匹配多个条件的主机，如图 7-1-13、7-1-14 所示。

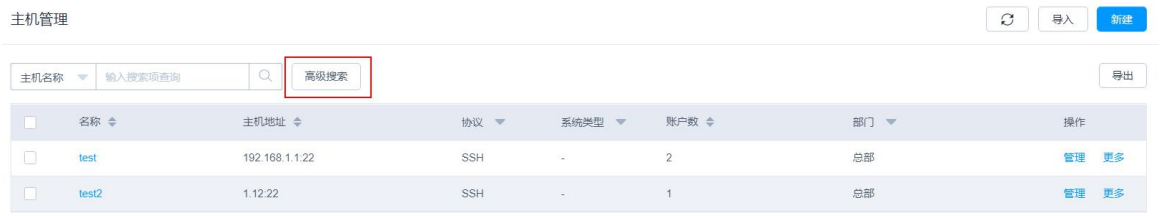


图 7-1-13

图 7-1-14

7.1.6 添加账户

除了在新建主机时添加账户，也可以对已经存在的主机添加账户。进入主机详情页面，点击资源账户<添加>按钮，如图 7-1-15 所示。

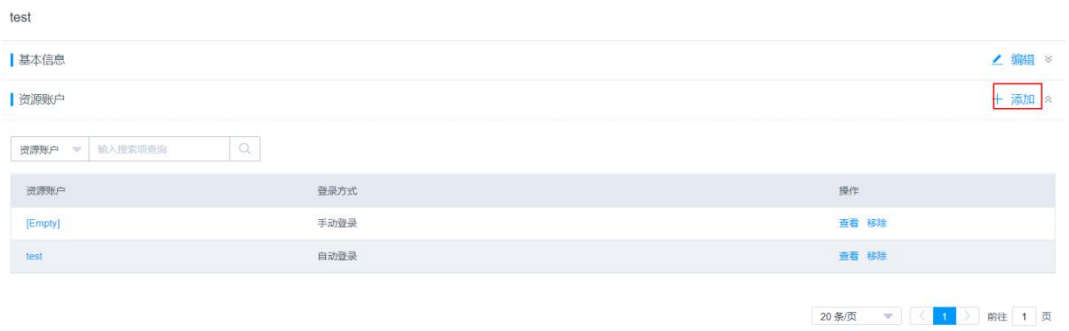


图 7-1- 15

此外，进入[资源/主机管理]列表，通过点击<更多/添加账户>按钮，也可快速添加账户，

如图 7-1-16 所示。

图 7-1- 16

7.1.7 编辑标签

除了在新建主机时编辑标签，也可以对已经存在的主机编辑标签。进入主机主机详情，编辑主机基本信息里面的标签，如图 7-1-17 所示。

图 7-1-17

此外，进入[资源/主机管理]列表，通过点击<更多/编辑标签>按钮，也可快速编辑标签，如图 7-1-18 所示。

图 7-1-18

7.1.8 主机导入

进入[资源/主机管理]，点击<导入>，如图 7-1-19 所示。

图 7-1-19

从文件导入：进入导入页面，选择文件导入主机方式，点击<点击上传>，选择本地文件导入，如图 7-1-20 所示。

图 7-1-20

导入云主机：进入导入页面，选择导入云主机方式，如图 7-1-21 所示。

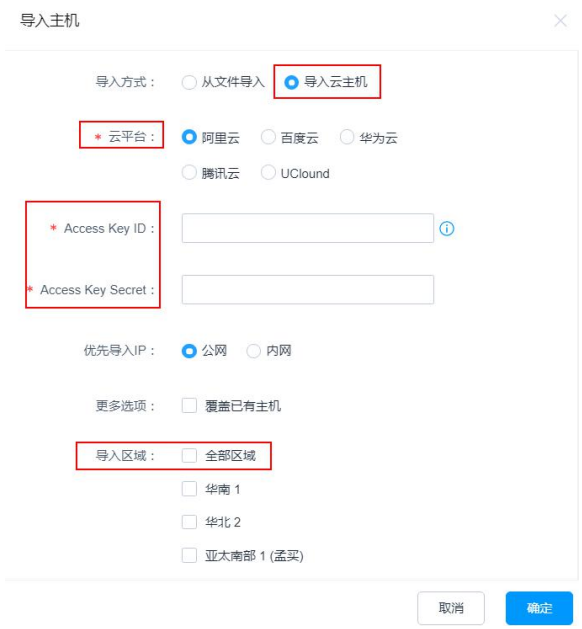


图 7-1-21

云主机导入方式，除了标注“*”的是必填选项外，还需要勾选需要导入区域。

文件导入：

1. 支持上传的文件类型：CSV、xls、xlsx
2. 覆盖已有主机：选中时，当主机地址、端口和协议重复时会覆盖主机（更新主机信息）

导入云主机：

1. 阿里云、百度云、华为云、腾讯云、UCloud
2. 覆盖已有主机：选中时，当主机地址、端口和协议重复时会覆盖主机（更新主机信息）

7.1.9 主机导出

进入[资源/主机管理]，点击<导出>，如图 7-1-22 所示。

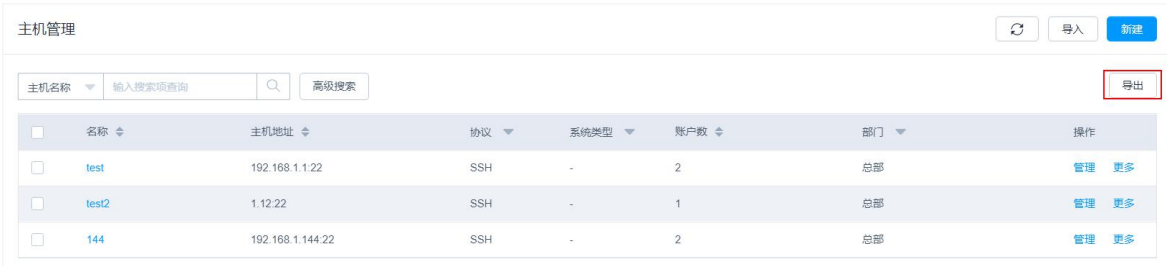


图 7-1-22

1. 如果未选中任何主机，点击【导出主机】，则导出当前筛选的全部主机
2. 如有选中主机，点击【导出主机】，则导出选中主机
3. 导出主机会同时导出主机的账户，当无权限查看账户密码时，导出密文密码（导出的列表中有两列：明文密码和密文密码）

a.查看账户密码的权限在系统设置进行配置

7.1.10 批量操作

批量操作支持批量添加标签和删除标签，进入[资源/主机管理]，选中主机，点击<添加标签>或者<删除标签>，如图 7-1-23 所示。

图 7-1-23

1. 当没有主机被选中时，禁用<添加标签>和<删除标签>按键
2. 删除标签将去除所选主机上的所有标签

7.2 应用发布

7.2.1 应用服务器新建

进入[资源/应用发布/应用服务器]，点击<新建>，如图 7-2-1、7-2-2 所示。

图 7-2-1

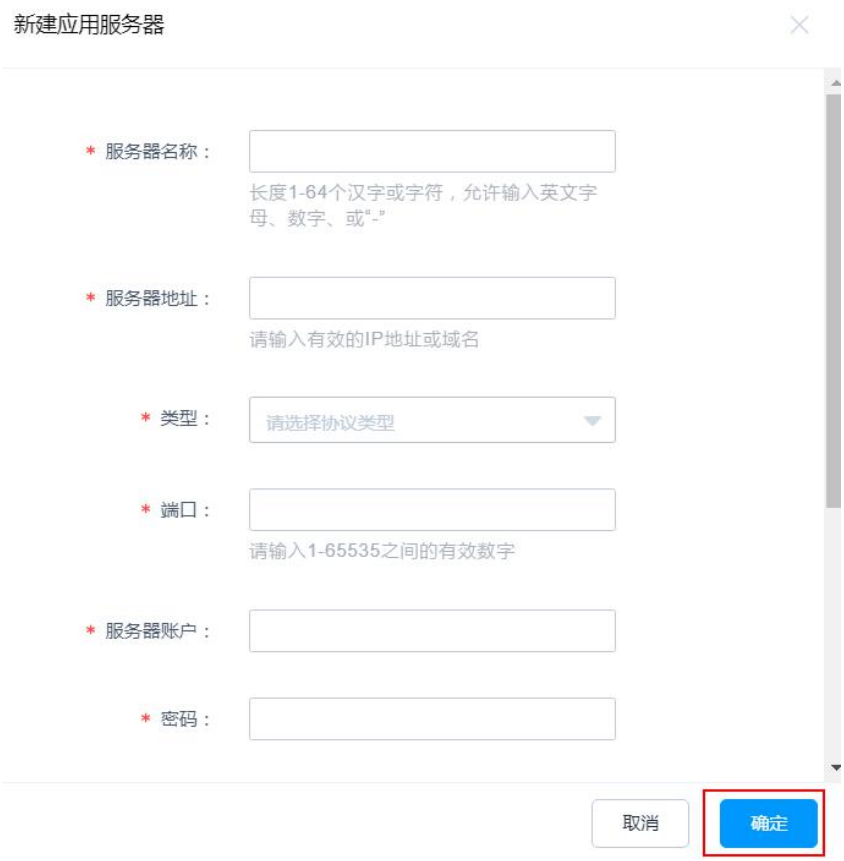


图 7-2-2

其中带“*”的为必填选项，填写完必填选项后，点击确定保存信息。

7.2.2 应用服务器详情

进入[资源/应用发布/应用服务器]，点击名称或<管理>按钮进入详情页面，如图 7-2-3 所示。

图 7-2-3

7.2.3 应用服务器修改

进入[资源/应用发布/应用服务器]，进入详情页面，点击<编辑>按键进入修改基本信息，如图 7-2-4 所示。

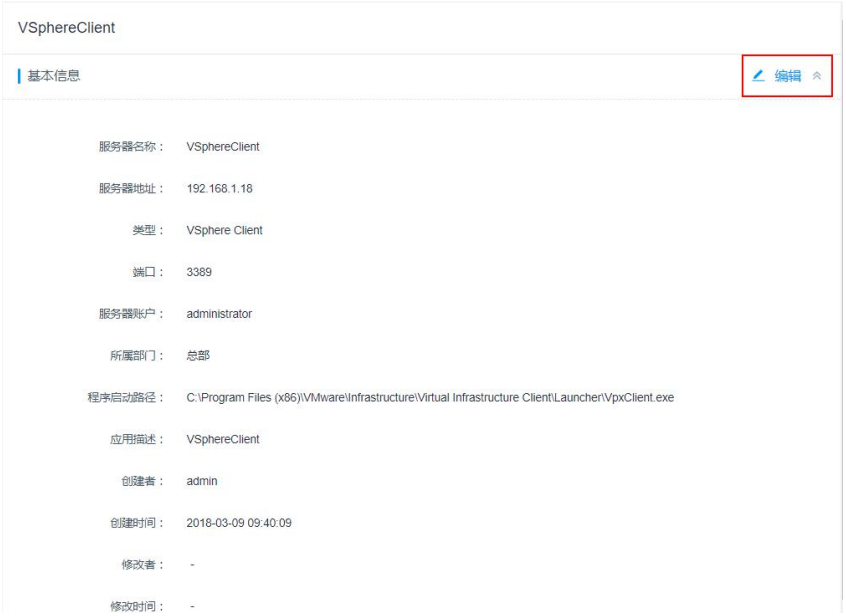


图 7-2-4

注意：

1. 账户不变时，密码为空不填则不修改密码

7.2.4 应用服务器删除

进入[资源/应用发布/应用服务器]，点击指定应用服务器的<删除>按钮，如图 7-2-5 所示。

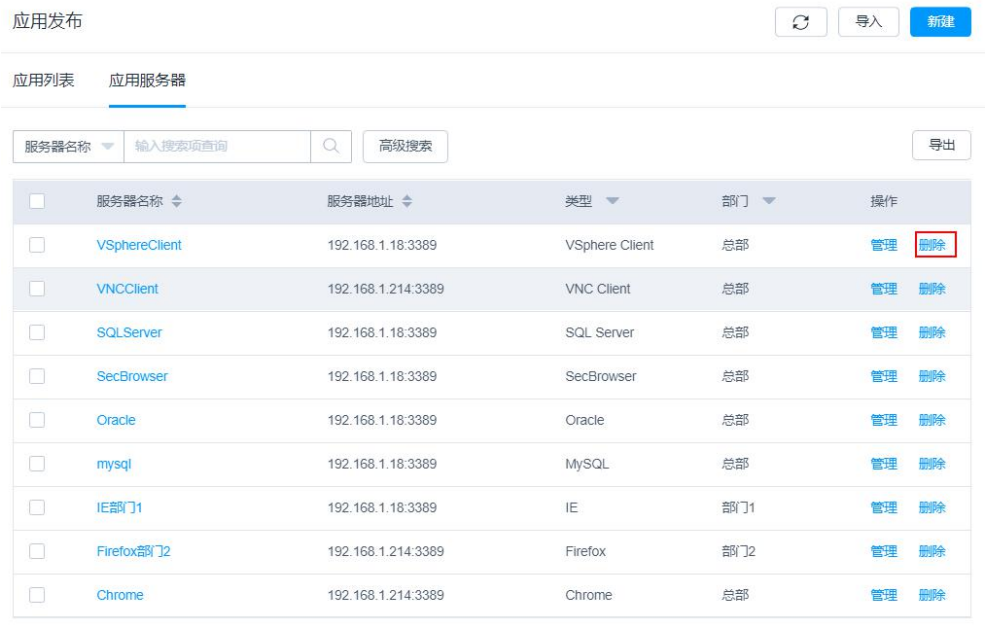


图 7-2-5

除了可以单个删除应用发布服务器之外，还支持批量删除应用发布服务器。勾选需要删除的应用发布服务器，点击下方的<删除>按钮，如图 7-2-6 所示。

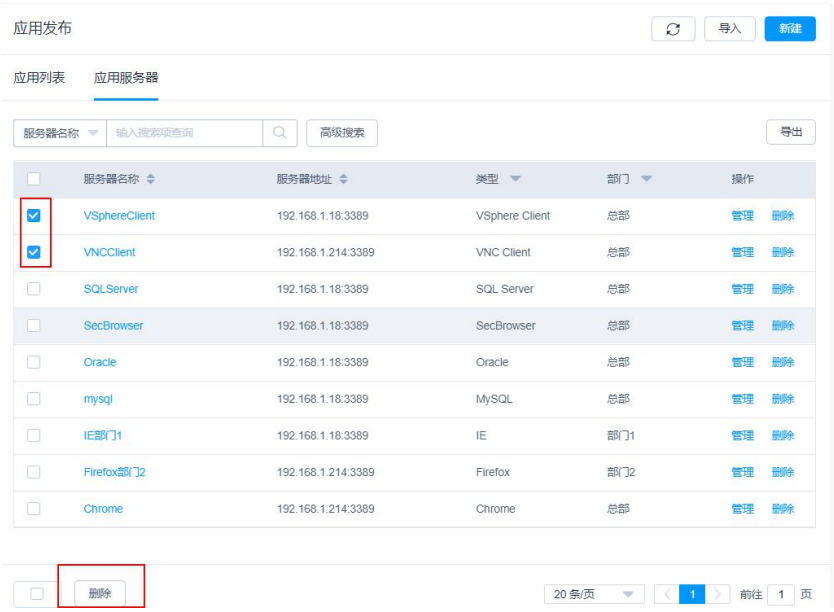


图 7-2-6

注意：

1. 当没有应用服务器被选中时，批量删除被禁用

7.2.5 应用服务器查询

进入[资源/应用发布/应用服务器]，选择搜索项（支持搜索服务器名称、服务器地址、端口），然后在搜索输入框内输入关键词进行查询，如图 7-2-7 所示。

图 7-2-7

除了普通搜索，还支持高级搜索。点击高级搜索，可以搜索同时匹配多个条件的应用服务器，如图 7-2-8、7-2-9 所示。

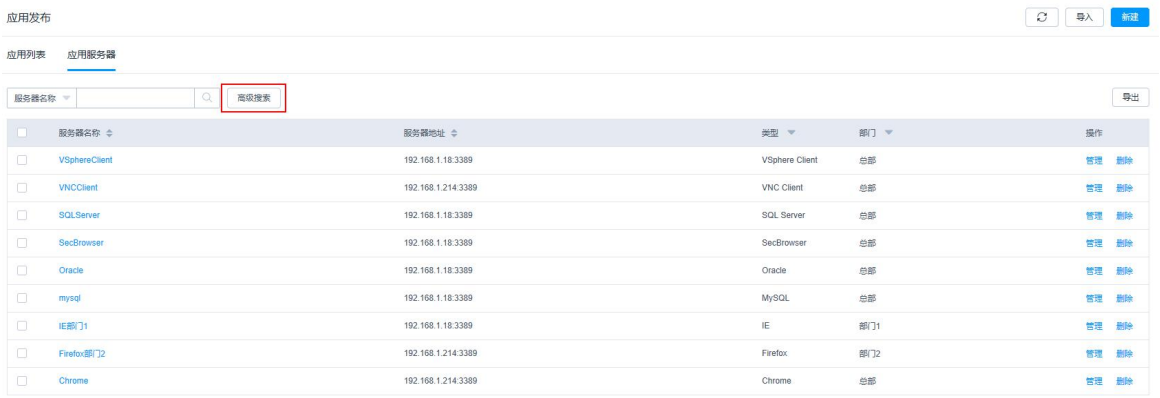


图 7-2-8

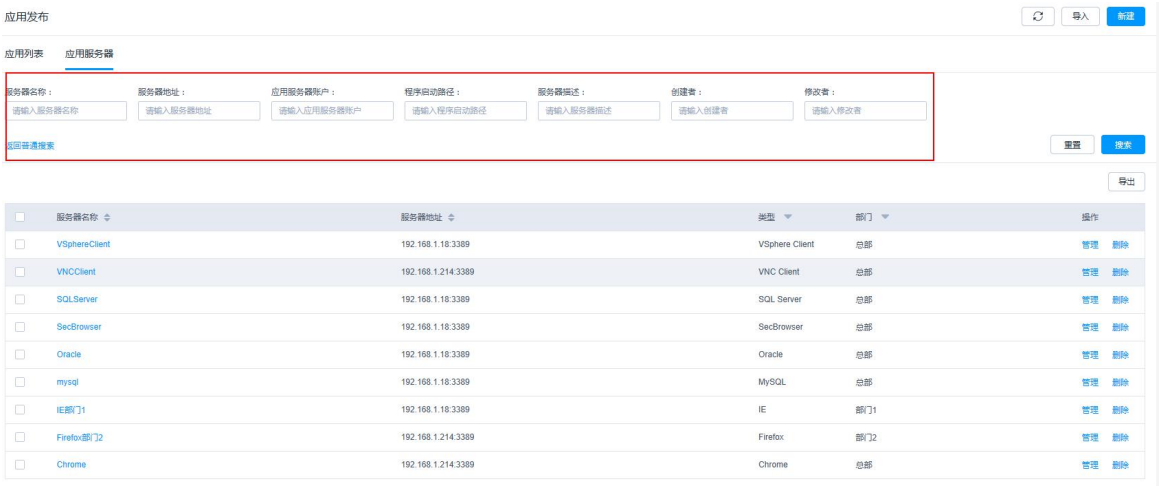


图 7-2-9

7.2.6 应用服务器导入

进入[资源/应用发布/应用服务器]，点击<导入>，导入应用发布服务器，如图 7-2-10 所示。

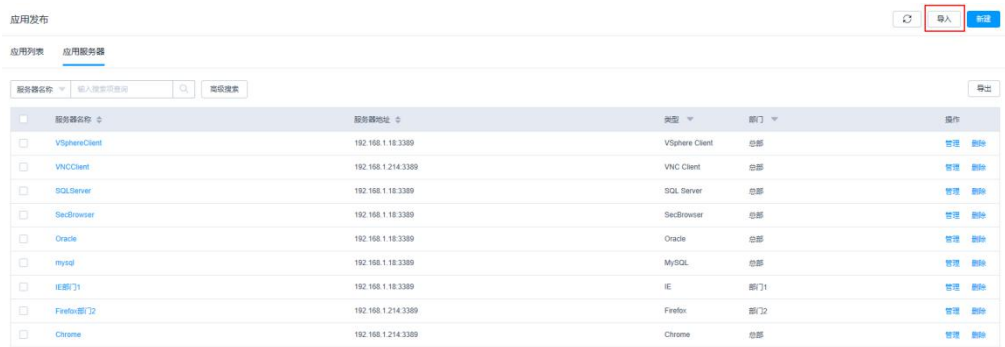


图 7-2-10

注意：

1. 文件导入目前支持导入只能上传 CSV/xls/xlsx 文件
2. 覆盖已有应用服务器：选中时，当应用服务器名称相同时，将覆盖应用服务器

7.2.7 应用服务器导出

进入[资源/应用发布/应用服务器]，点击<导出>，导出应用发布服务器，如图 7-2-11 所示。

图 7-2-11

注意：

1. 如果未选中任何应用服务器，点击【导出应用服务器】，则导出当前筛选的全部应用服务器
2. 如有选中应用服务器，点击【导出应用服务器】，则导出选中应用服务器

7.2.8 应用新建

进入[资源/应用发布/应用列表]，点击<新建>，创建应用发布，如图 7-2-12、7-2-13 所示。

图 7-2-12

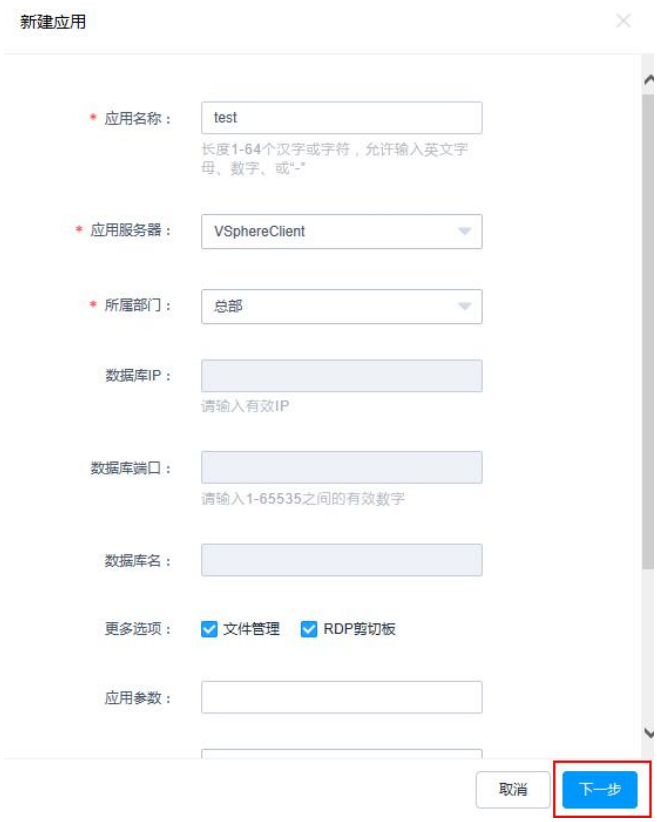


图 7-2-13

进入[应用发布新建]界面，首先填写应用发布资源基本信息，输入应用发布资源参数，其中“*”标记的红色部分为必填项，“名称”允许填写中文字、数字、英文字母等，“发布服务器”请选择已创建的应用发布服务器。填写完毕后，点击<下一步>，进入账户填写界面，如图 7-2-14 所示。

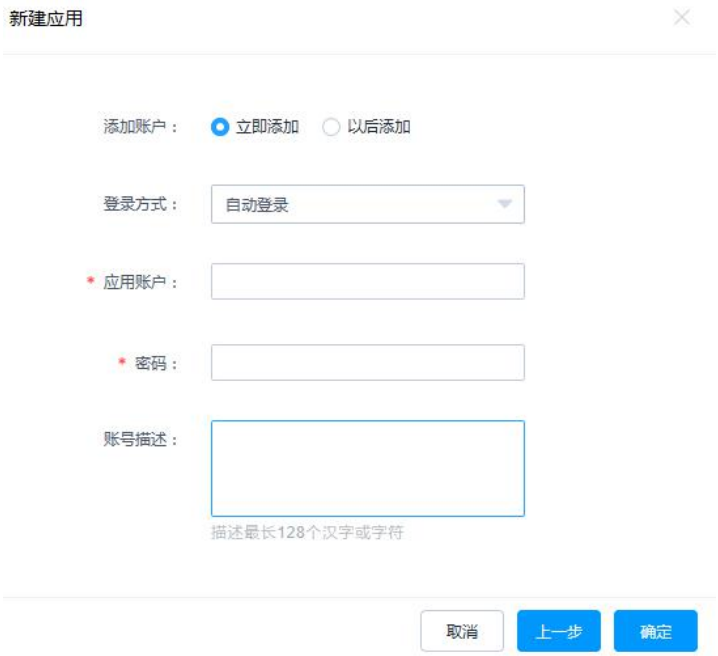


图 7-2-14

注意：

1. 选中文件管理，则开启文件管理功能
2. 选中 RDP 剪切板，则开启 RDP 剪切板功能
3. 选中【以后添加】时，点击【确定】，自动创建一个[空账户]（一个应用仅包含一个[空账户]）
4. 选中【立即添加】时，账户信息填写正确时，点击【确定】，如果无[空账户]，则创建一个[空账户]
5. 手动登录：如果账户未填，则创建一个[空账户]；如果已经有一个空账户，则判定为重复
6. IE 无自动登录账户

7.2.9 应用详情

进入[资源/应用发布/应用列表]，点击应用名称或<管理>按钮进入详情页面，如图 7-2-15 所示。

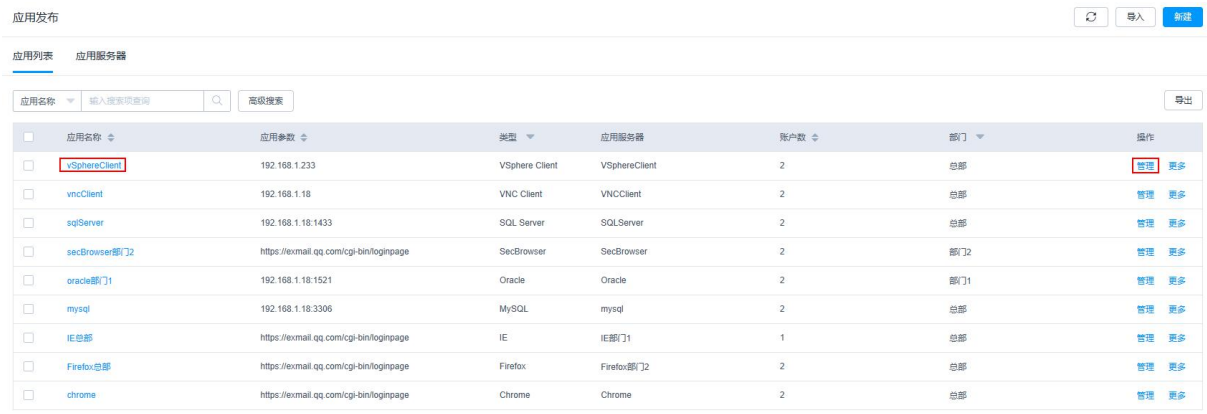


图 7-2-15

7.2.10 应用修改

进入[资源/应用发布/应用列表]，进入应用发布详情页面，点击基本信息的<编辑>按钮，修改应用发布基本信息，如图 7-2-16、7-2-17 所示。

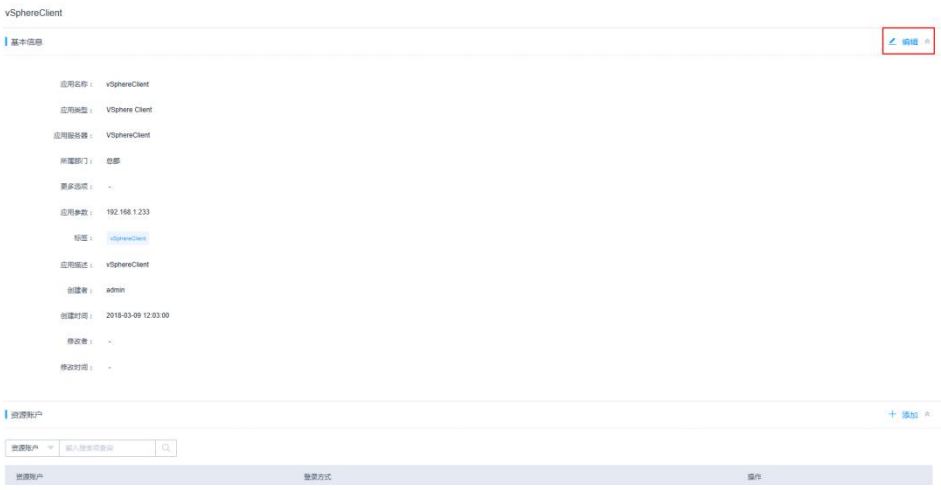


图 7-2-16

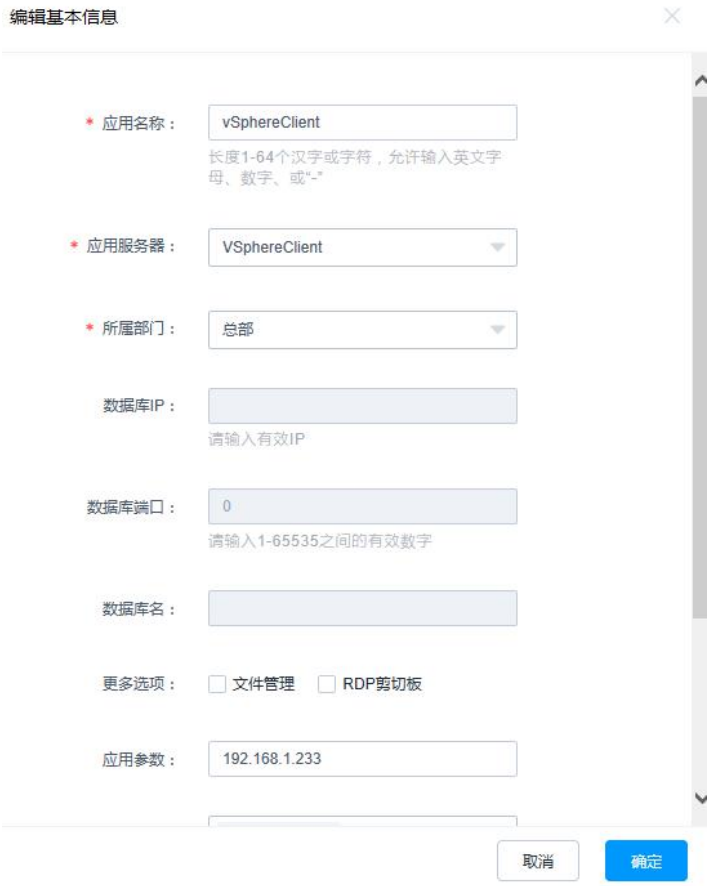


图 7-2-17

7.2.11 应用删除

进入[资源/应用发布/应用列表]，点击指定应用发布的<更多/删除>按钮，删除单个应用发布，如图 7-2-18 所示。

图 7-2-18

除了删除单个应用发布，还支持批量删除多个应用发布，勾选需要删除的应用发布，点击下方的<删除>按键，如图 7-2-19。

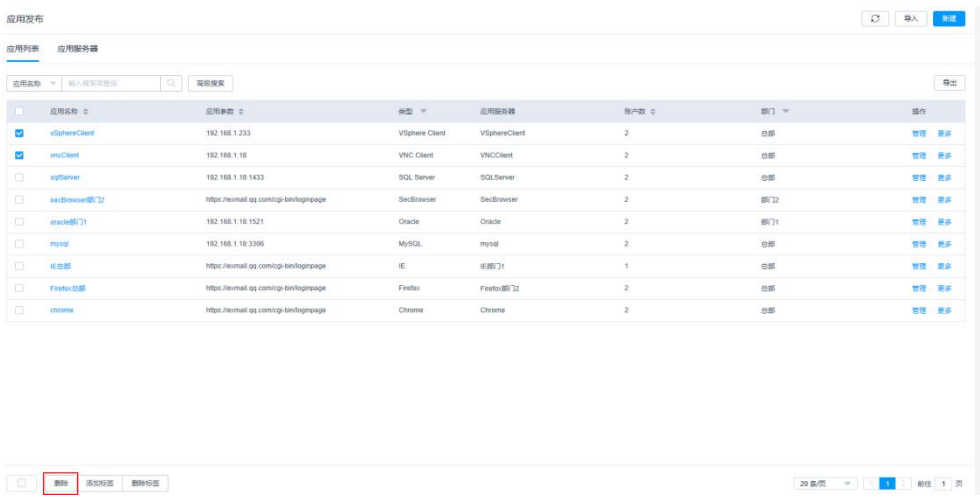


图 7-2-19

7.2.12 应用查询

进入[资源/应用发布/应用列表]，选择搜索项（搜索项可选应用名称、应用参数、标签），在搜索输入框内容输入关键词，点击搜索应用发布，如图 7-2-20 所示。

图 7-2-20

除了普通搜索，还支持高级搜索。点击高级搜索，可以搜索同时匹配多个条件的应用发布，如图 7-2-21、7-2-22 所示。

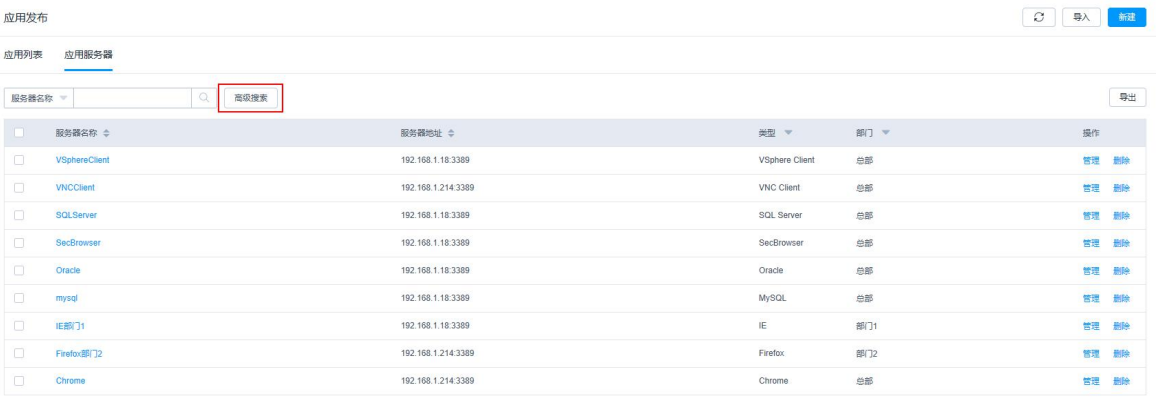


图 7-2-21

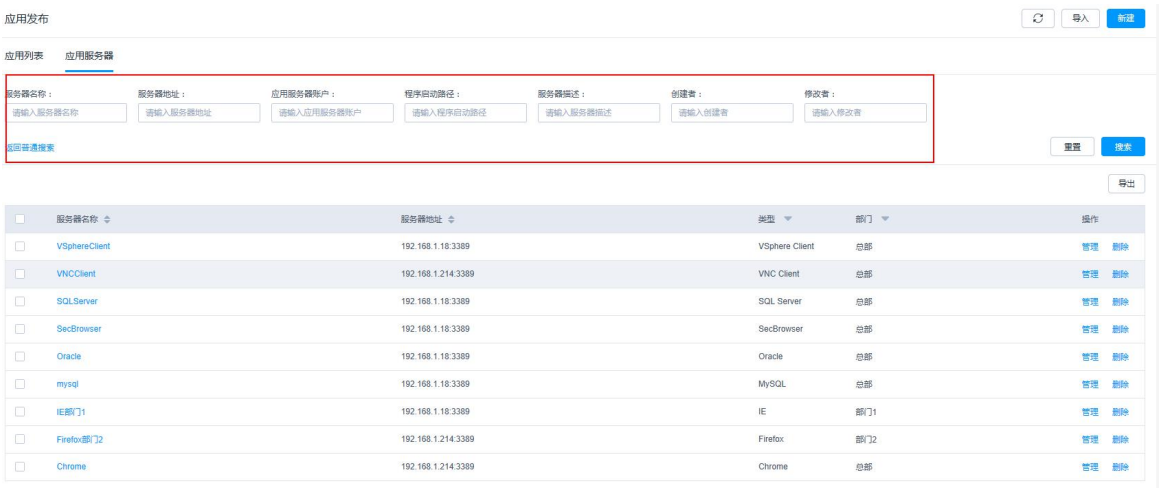


图 7-2-22

7.2.13 添加账户

除了在新建应用时添加账户，也可以对已经存在的应用添加账户，进入详情页面，点击资源账户的<添加>，如图 7-2-23 所示。

图 7-2-23

此外，进入[资源/应用发布/应用列表]，通过点击<更多/添加账户>按钮，也可快速添加账户，如图 7-2-24 所示。

图 7-2-24

7.2.14 编辑标签

除了在新建应用时编辑标签，也可以对已经存在的应用编辑标签，进入详情页面，在编辑应用基本信息同时编辑标签，如图 7-2-25 所示。

图 7-2-25

此外，进入[资源/应用发布/应用列表]，通过点击<更多/编辑标签>按钮，也可快速编辑标签，如图 7-2-26 所示。

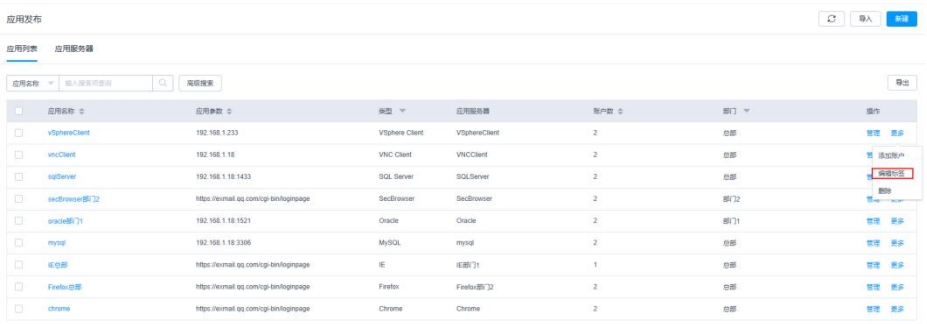


图 7-2-26

7.2.15 应用导入

进入[资源/应用发布/应用列表]，点击<导入>，导入应用发布，如图 7-2-27 所示。

图 7-2-27

注意：

1. 文件导入目前支持导入只能上传 CSV/xls/xlsx 文件
2. 覆盖已有应用发布：选中时，当应用发布名称相同时，将覆盖应用

7.2.16 应用导出

进入[资源/应用发布/应用列表]，点击<导出>，导出应用发布，如图 7-2-28 所示。

图 7-2-28

注意：

1. 如果未选中任何应用，点击【导出应用】，则导出当前筛选的全部应用
2. 如有选中应用，点击【导出应用】，则导出选中应用
3. 导出应用会同时导出应用的账户，当无权限查看账户密码时，导出密文密码（导出的列表中有两列：明文密码和密文密码）

a.查看账户密码的权限在系统设置进行配置

7.3 资源账户

7.3.1 账户新建

进入[资源/资源账户]，点击<新建>，如图 7-3-1、7-3-2 所示。

图 7-3-1

图 7-3-2

账户主要有以下几种类型：

1.自动登录账户:账户、密码必填

2.手动登录账户: 账户非必填，密码输入框禁用

3.提权登录账户: 账户输入框禁用，密码必填

7.3.2 账户详情

进入[资源/资源账户]，点击名称或<管理>按钮进入详情页面，如图 7-3-3 所示。

图 7-3-3

7.3.3 账户修改

进入[资源/资源账户]，进入账户详情，点击基本信息的<编辑>，修改账户基本信息，如图 7-3-4 所示。

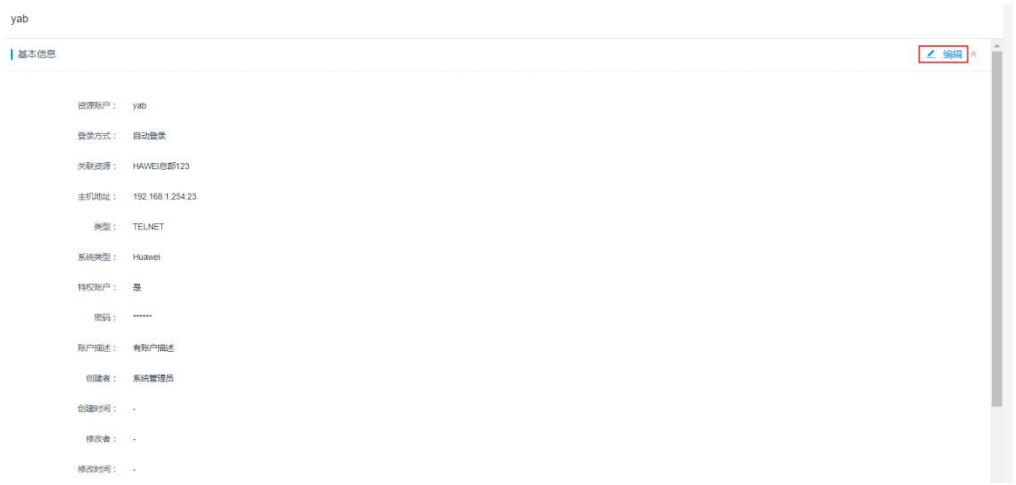


图 7-3-4

在账户详情里，也可以编辑账户组信息，如图 7-3-5、7-3-6 所示。

图 7-3-5

图 7-3-6

注意：

1. 编辑基本信息：ssh key 和密码、passphrase 展示为空，不是必填项，如果为空则不修改
2. 特权账户：标记该账户为特权账户，用于改密策略当中的使用特权账户改密功能，特权账户仅有一个

7.3.4 账户删除

进入[资源/资源账户]，点击指定账户的<更多/删除>按钮，删除指定的账户如图 7-3-7 所示。

图 7-3-7

除了支持单个删除账户，还支持批量删除账户。勾选需要删除的账户，点击下方的<删除>按键，批量删除账户，如图 7-3-8 所示。

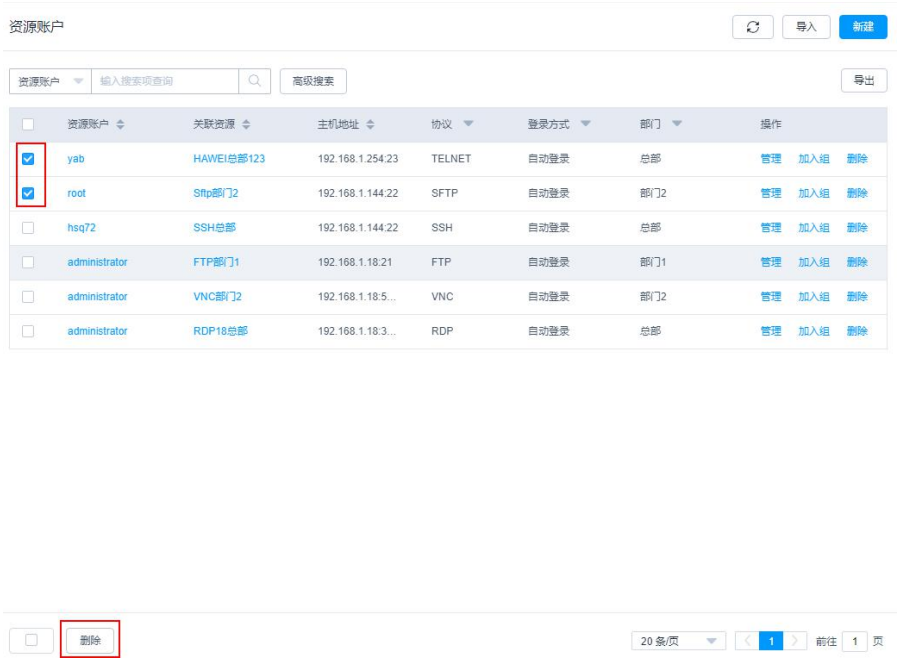


图 7-3-8

7.3.5 账户查询

进入[资源/资源账户]，选择搜索项（搜索项可选资源账户名称、关联资源名称、特权账户、SSH Key 账户、使用 passphrase），在搜索输入框内容输入关键词，点击搜索资源账户，如图 7-3-9 所示。

图 7-3-9-

除了普通搜索，还支持高级搜索。点击高级搜索，可以搜索同时匹配多个条件的资源账户，如图 7-3-10 所示。

图 7-3-10

7.3.6 加入组

进入[资源/资源账户]，点击<加入组>按钮，可以将账户加入或者移除出账户组，如图 7-3-11 所示。

图 7-3-11

7.3.7 账户导入

进入[资源/资源账户]，点击<导入>，导入账户，如图 7-3-12 所示。

图 7-3-12

注意：

1. 文件导入目前支持导入只能上传 CSV/xls/xlsx 文件
2. 覆盖已有应用发布：选中时，当应用发布名称相同时，将覆盖账户

7.3.8 账户导出

进入[资源/资源账户]，点击<导出>，导出资源账户，如图 7-3-13 所示。

图 7-3-13

注意：

1. 如果未选中任何账户，点击【导出账户】，则导出当前筛选的全部账户
2. 如有选中账户，点击【导出账户】，则导出选中账户

7.4 账户组

7.4.1 账户组新建

进入[资源/账户组]，点击<新建>，进入新建界面，如图 7-4-1、7-4-2 所示。

图 7-4-1

图 7-4-2

编辑组信息，其中“*”标记的为必填项。点击<确定>完成保存。

7.4.2 账户组详情

进入[资源/账户组]，点击账户组名称或者管理，进入账户组详情，如图 7-4-3 所示。

图 7-4-3

7.4.3 账户组修改

进入[资源/账户组]，在账户组详情页面，点击<编辑>，编辑账户组信息，如图 7-4-4、7-4-5 所示。

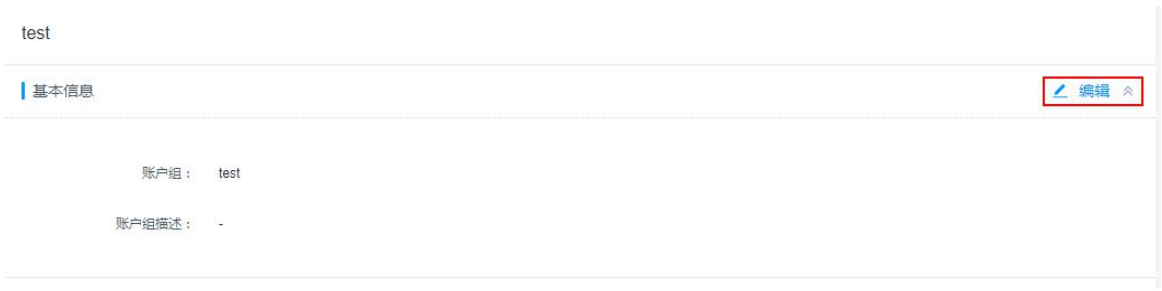


图 7-4-4

图 7-4-5

7.4.4 账户组删除

进入[资源/账户组]，点击指定账户组对应的管理<删除>按键，删除指定账户组，如图 7-4-6 所示。

图 7-4-6

在账户组列表中，同时勾选多个账户组，点击列表下方的<删除>，可以一次性删除多个账户组，如图 7-4-7 所示。

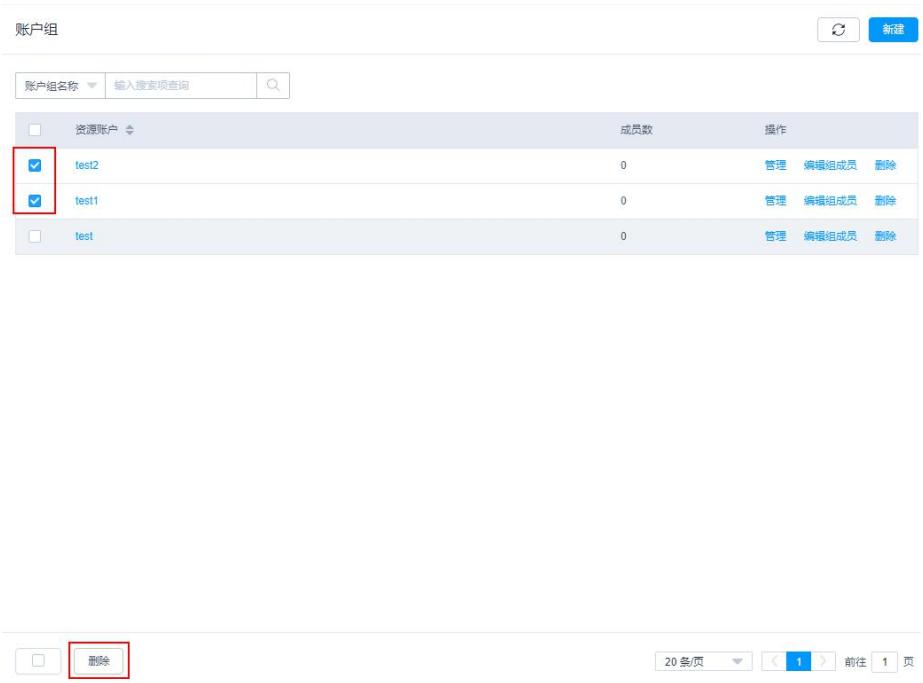


图 7-4-7

7.4.5 账户组查询

进入[资源/账户组]，选择搜索项（搜索项可选账户组 mc ），在搜索输入框内容输入关键词，点击搜索账户组，如图 7-4-8 所示。

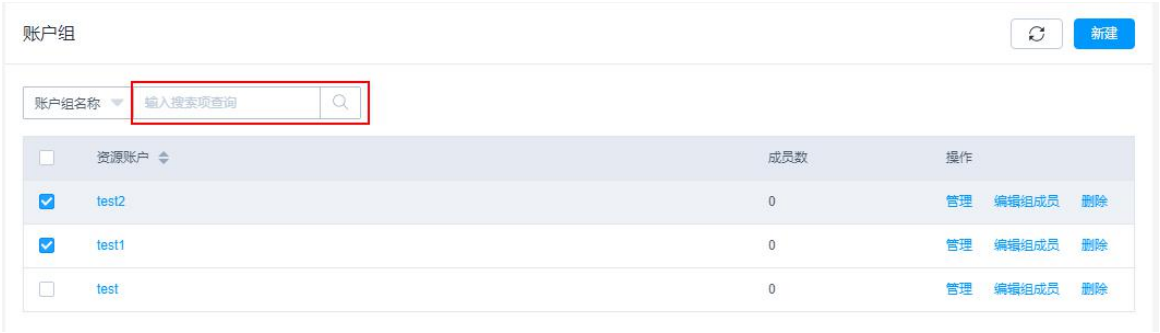


图 7-4-8

7.4.6 编辑组成员

进入[用户/用户组]，点击<编辑组成员>按钮，如图 7-4-9 所示。

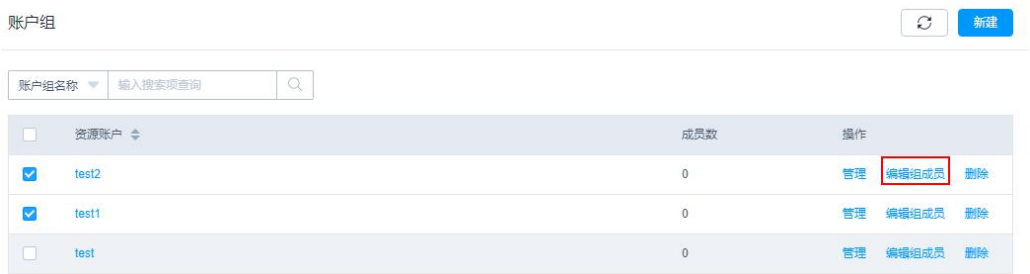


图 7-4-9

进入添加组成员界面，勾选左侧列表中的用户移动到右侧列表中，如图 7-4-10 所示。

图 7-4-10

在账户组详情页面，点击账户组成员的<编辑>按键，也可以编辑账户组成员，如图 7-4-11 所示。

图 7-4-11

第八章 策略

8.1 访问控制策略

访问控制策略用于控制用户访问资源的权限。

8.1.1 新建访问控制策略

进入[策略/访问控制策略]，点击<新建>，如图 8-1-1 所示。弹出新建访问控制策略弹窗。

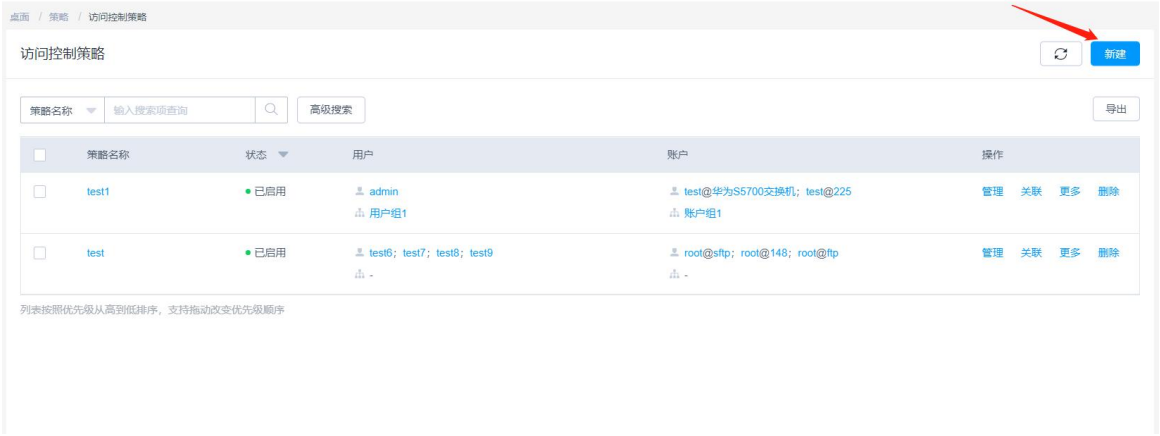


图 8-1-1

图 8-1-2

在新建访问控制策略弹窗中输入策略名称，可设置策略有效期、上传、下载、文件管理、

RDP 剪切板、登录时段限制、IP 限制，设置完成后，点击下一步进行关联用户用户组，如图 8-1-3。关联用户或用户组后点击下一步进行关联账户或账户组，如图 8-1-4。关联完成后点击确定完成新建策略。

图 8-1-3

关联用户时可以输入用户的登录名、姓名、手机、邮箱、角色、部门进行查询；关联用户组时可以输入用户组名称进行查询。

图 8-1-4

关联账户时可以使用账户的账户名、关联资源、主机地址、数据库 IP、启动参数、类型、登录方式、部门进行查询；关联账户组时可以使用账户组名称进行查询。

进入[策略/访问控制策略]，选择某策略，点击<更多>，弹出下拉列表，如图 8-1-5。点击<插入>，弹出新建访问控制策略弹窗，该新建策略的优先级在选择策略的上方。

图 8-1-5

点击双人授权候选人，弹出编辑双人授权候选人弹窗，如图 8-1-6。可选的用户为当前操作用户本部门及上级部门的部门管理员，admin 也包含在可选范围。可以输入用户的登录名、姓名、手机、邮箱进行查询。

图 8-1-6

8.1.2 编辑访问控制策略关联对象

进入[策略/访问控制策略]，点击<关联>，弹出下拉列表，如图 8-1-7。选择对应编辑项，弹出对应编辑弹窗。之后操作与新建策略时关联类似。

图 8-1-7

8.1.3 访问控制策略详情

进入[策略/访问控制策略]，点击<管理>或策略名称，进入对应策略详情页面，如图 8-1-8。

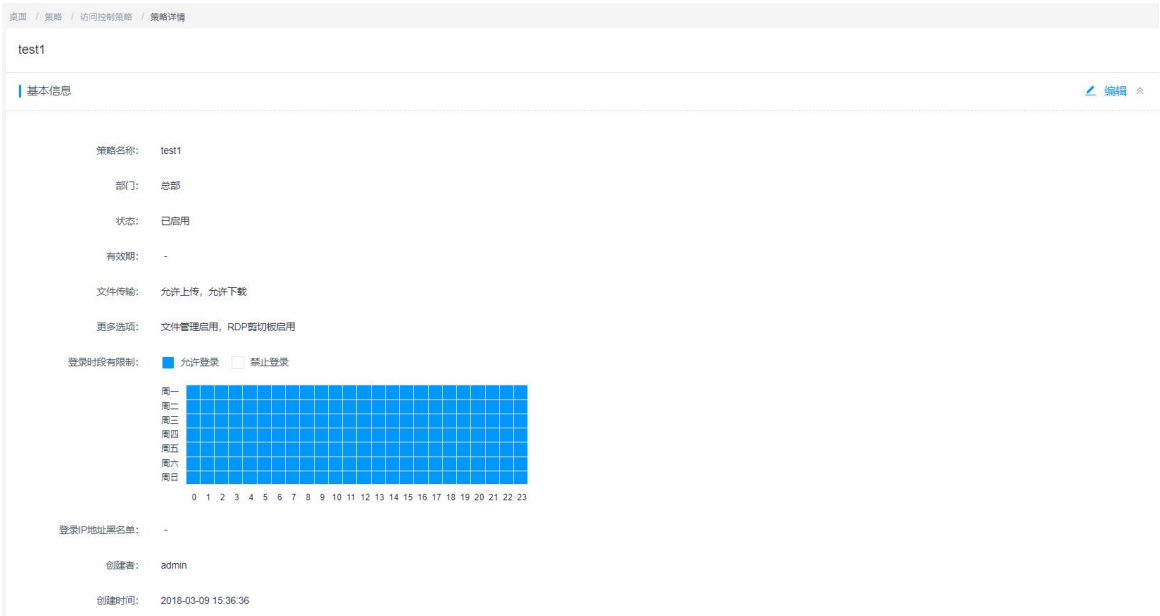


图 8-1-8

[基本信息]中展示对应策略的基本信息。

点击<编辑>，弹出编辑访问控制策略弹窗，如图 8-1-9，其操作与新建改密策略类似。

图 8-1-9

[用户]中展示对应策略所关联的用户，如图 8-1-10 所示。点击<编辑>，弹出编辑关联用户弹窗，操作与新建策略类型。点击<移除>，可移除对应关联用户。

图 8-1-10

[用户组]中展示对应策略所关联的用户组，如图 8-1-11 所示。点击<编辑>，弹出编辑关联用户组弹窗，操作与新建策略类型。点击<移除>，可移除对应关联用户组。

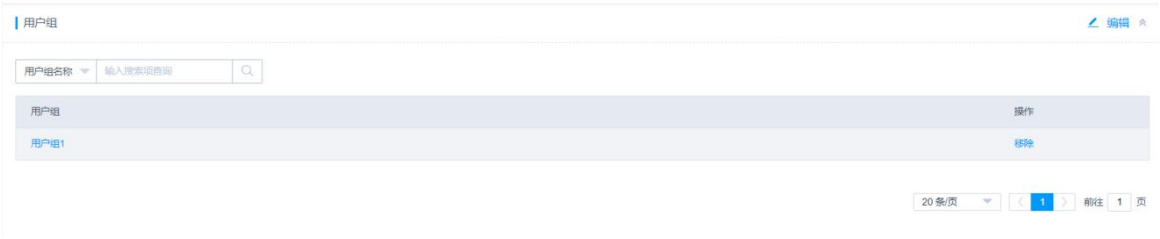


图 8-1-11

[资源账户]中展示对应策略所关联的账户，如图 8-1-12 所示。点击<编辑>，弹出编辑关联账户弹窗，操作与新建策略类型。点击<移除>，可移除对应关联账户。

图 8-1-12

[账户组]中展示对应策略所关联的账户组，如图 8-1-13 所示。点击<编辑>，弹出编辑关联账户组弹窗，操作与新建策略类型。点击<移除>，可移除对应关联账户组。

图 8-1-13

[双人授权候选人] 中展示对应策略所关联的双人授权候选人，如图 8-1-14 所示。点击<编辑>，弹出编辑双人授权候选人弹窗，操作与编辑策略类型。点击<移除>，可移除对应关联双人授权候选人。

图 8-1-14

8.1.4 访问控制策略搜索

进入[策略/访问控制策略]，点击搜索项，弹出搜索项下拉列表，如图 8-1-15 所示。可选择策略名称、用户、资源名称、主机地址、资源账户、时间限制和 IP 限制进行搜索。

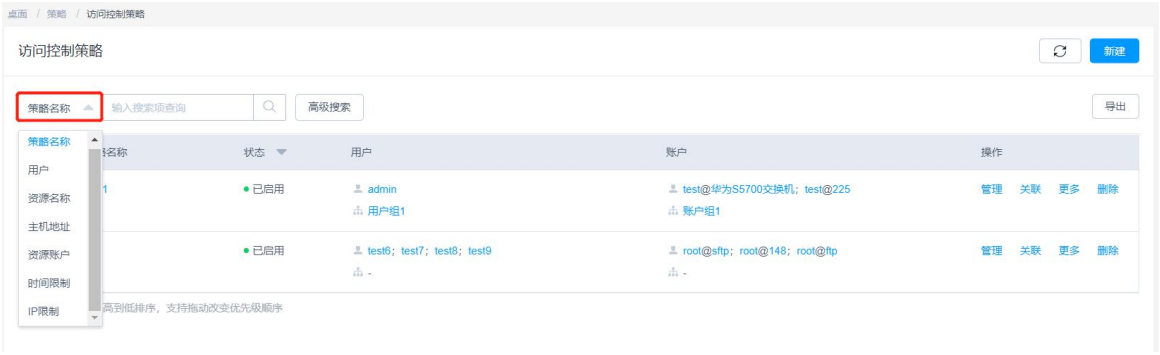


图 8-1-15

点击<高级搜索>，显示高级搜索搜索框，如图 8-1-16 所示。可使用策略名称、用户、资源名称、主机地址、资源账户、时间限制、IP 限制、生效时间、失效时间、上传、下载、RDP 剪切板、文件管理、创建者和修改者进行搜索。点击<重置>后将列表重置为显示所有策略。

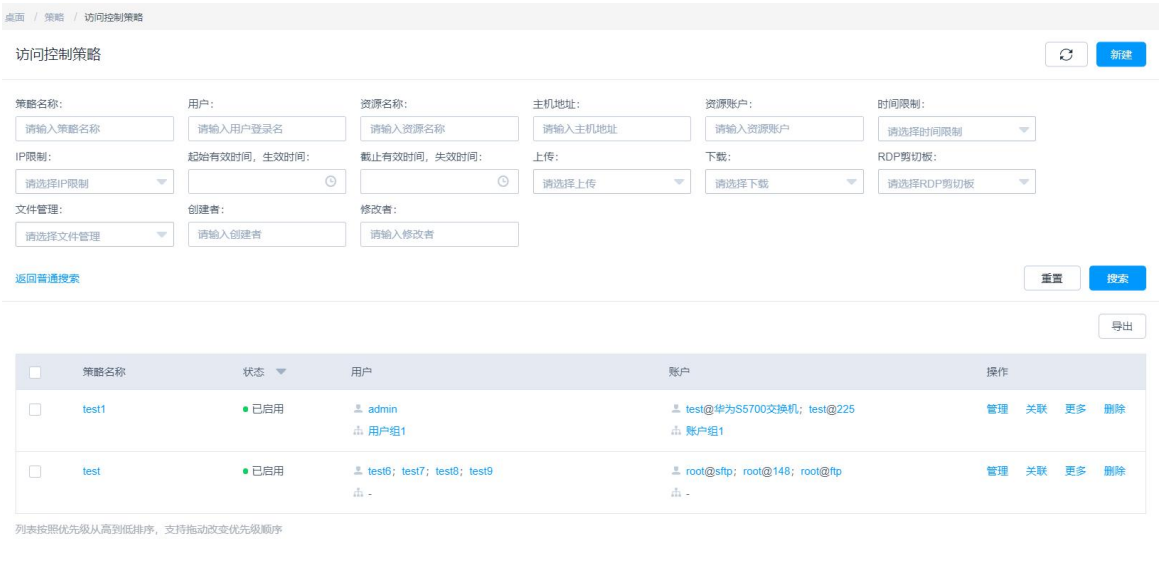


图 8-1-16

8.1.5 访问控制策略导出

进入[策略/访问控制策略]，点击<导出>，如图 8-1-17 所示。即可导出策略授权关系表。默认导出所有策略，若选中某些策略，则导出所选中的策略的授权关系表。

图 8-1-17

8.1.6 访问控制策略列表

进入[策略/访问控制策略]，如图 8-1-18。选中某些策略，点击<启用>，所选中的策略都被启用；点击<禁用>，所选中的策略都被禁用；点击列表下方<删除>，则所选中的策略都被删除。点击列表中策略对应的<删除>，删除对应策略。点击策略名称，进入对应策略详情页面；点击列表中的用户登录名、用户组名称、账户名、主机名、账户组名称，分别进入对应对象的详情页面。

列表按优先级排序，可拖动改变优先级，优先级高的策略优先生效；可使用策略状态进行筛选。

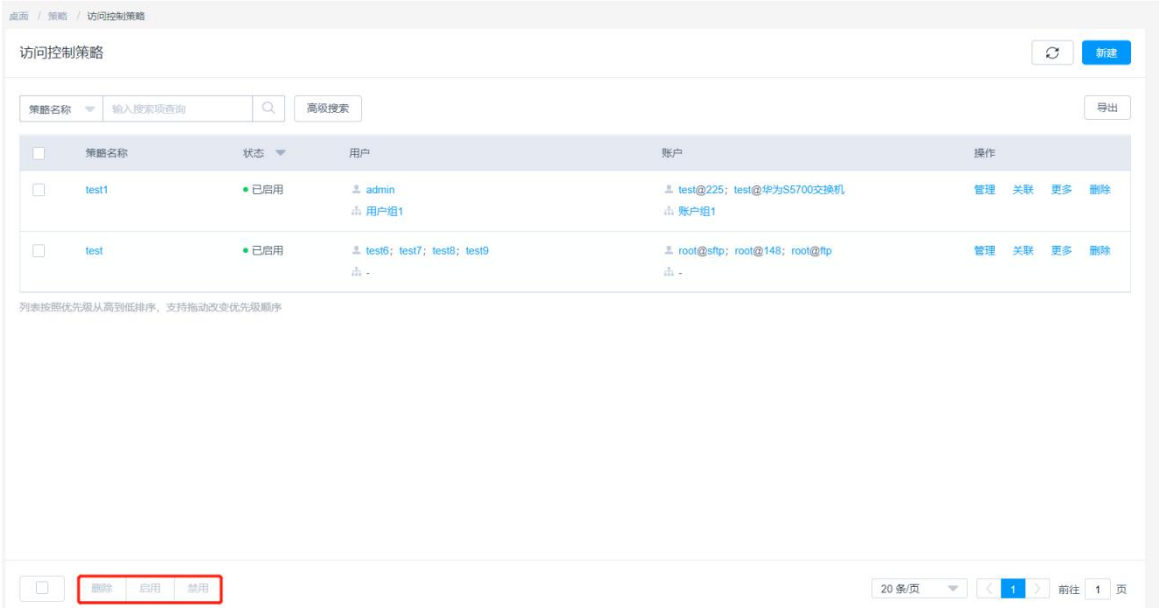


图 8-1-18

8.2 命令控制策略

8.2.1 新建命令控制策略

进入[策略/命令控制策略/策略列表]，如图 8-2-1。点击<新建>，弹出新建策略弹窗，如图 8-2-2 所示。输入策略名称和执行动作，执行动作包含：断开连接、拒绝执行、动态授权、允许执行。可输入有效期和时间限制。点击下一步，进入关联命令命令集弹窗，如图 8-2-3。关联命令支持通配符（*代表任意字符，?代表任意一个字符，[]代表匹配中括号内字符、范围或取反），每行输入一条命令。

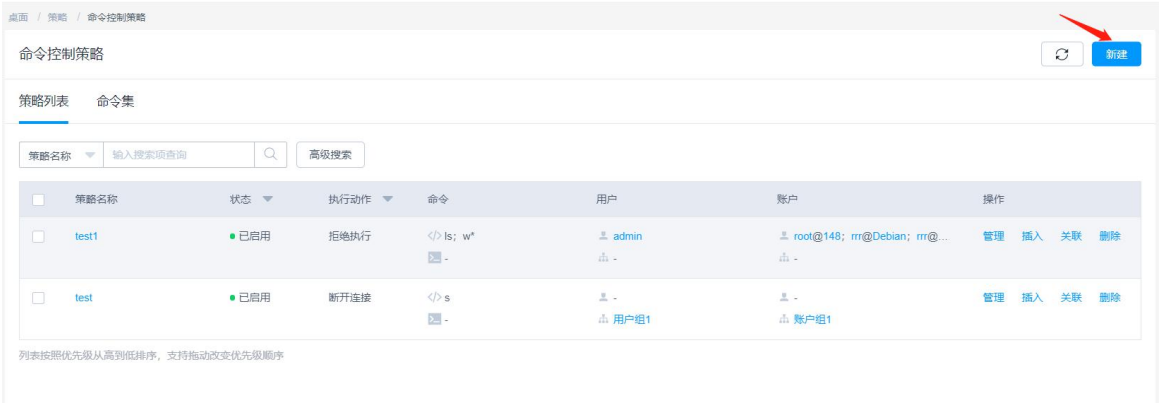
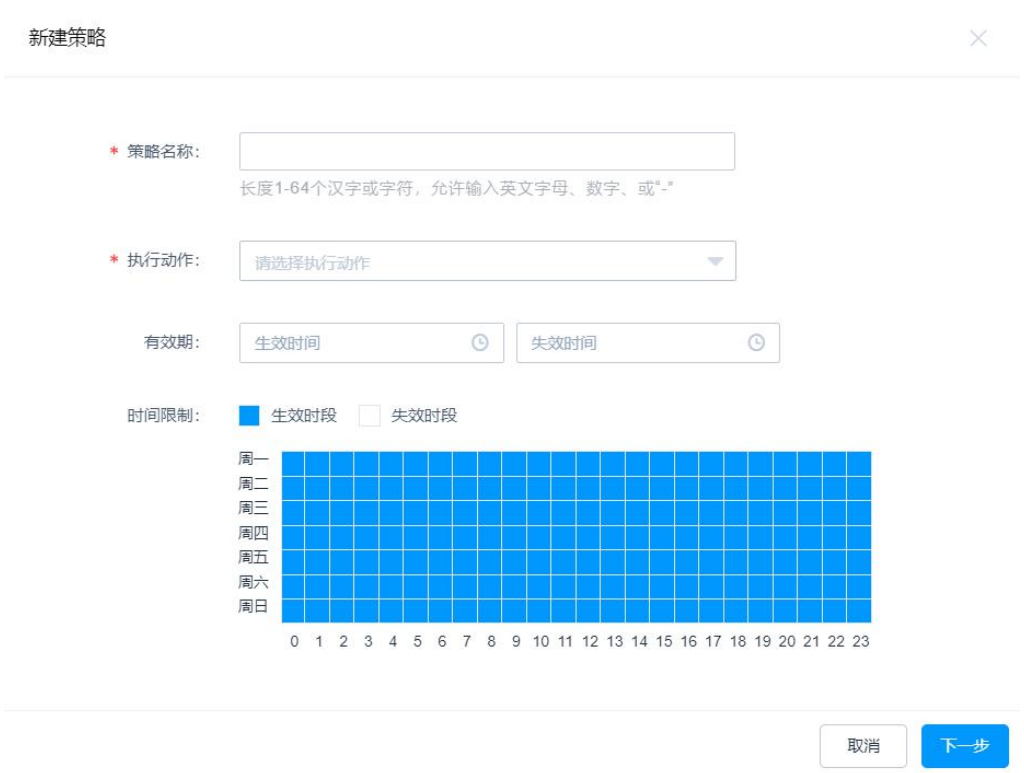


图 8-2-1



图

8-2-2

图 8-2-3

关联命令集中可选择已新建的命令集，如图 8-2-4。点击下一步，进行关联用户用户组，账户账户组，操作与新建访问控制策略类似。

注意：

1） 关联资源账户为 SSH 或 TELNET 协议类型的账户。

图 8-2-4

8.2.2 新建命令集

进入[策略/命令控制策略/命令集]，如图 8-2-5。点击<新建>，弹出新建命令集弹窗，如图 8-2-6，输入命令集名称，点击确定。

图 8-2-5

图 8-2-6

8.2.3 命令控制策略列表

进入[策略/命令控制策略/策略列表]，如图 8-2-7。点击<管理>，进入命令策略详情页面；点击<插入>，在对应策略前插入一条新建策略；点击<关联>，编辑对应策略关联对象，操作同访问控制策略类似；点击<删除>，删除对应命令控制策略；点击策略名称，进入对应策略详情页面；点击列表中的用户登录名、用户组名称、账户名、主机名、账户组名称，分别进入对应对象的详情页面。

选中策略后，点击列表下方<启用>，所选策略被批量启用；点击列表下方<禁用>，所选策略被批量禁用，点击列表下方<删除>，所选策略被批量删除。

列表可使用策略状态，执行动作进行筛选。

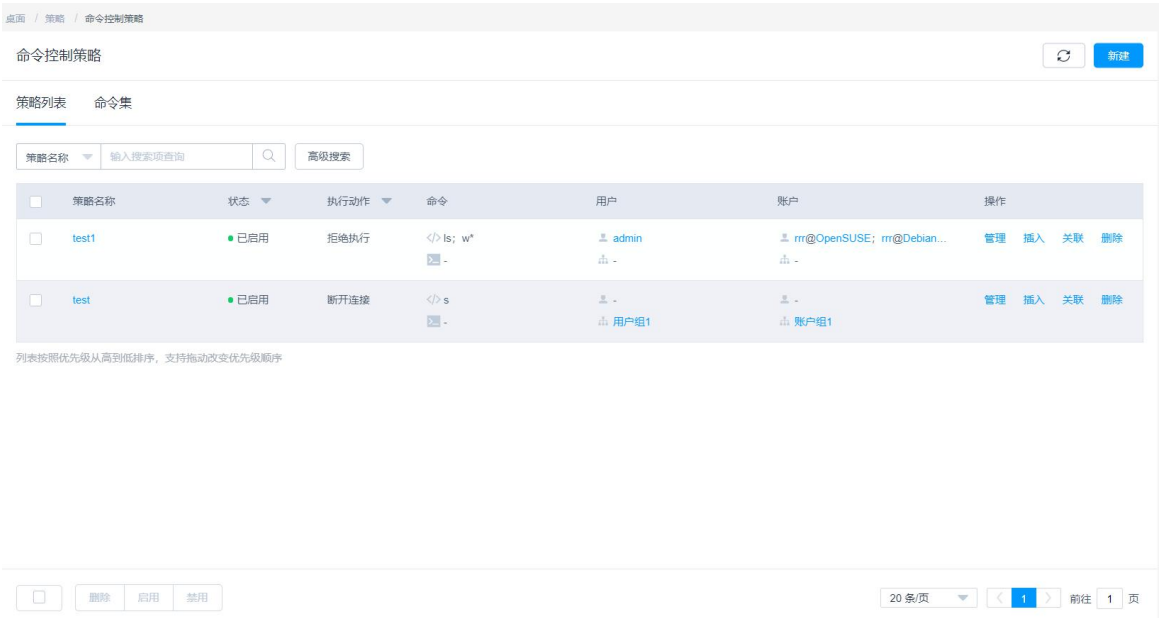


图 8-2-7

8.2.4 命令集列表

进入[策略/命令控制策略/命令集]，如图 8-2-8。点击<管理>进入命令集详情列表；点击添加命令>，弹出添加命令弹窗，如图 8-2-9 所示。在[命令/参数]中输入命令名即可对命令进行搜索；点击<删除>删除对应命令集；点击列表下方<删除>可批量删除所有选中命令集。

列表可使用命令集名称进行排序；使用命令集名称，命令/参数进行搜索。

图 8-2-8

图 8-2-9

8.2.5 命令控制策略详情

进入[策略/命令控制策略/策略列表]，点击<管理>或策略名称，进入命令策略详情页面，如图 8-2-10 所示，点击<编辑>弹出编辑策略信息弹窗。

图 8-2-10

[命令]中展示了对应策略所关联的命令，点击<编辑>弹出编辑关联命令弹窗；点击<移除>可移除对应命令。可使用[命令/参数]对命令进行查询。

图 8-2-11

[命令集]中展示了对应策略所关联的命令集，点击<编辑>弹出编辑关联命令集弹窗；点击<移除>可移除对应命令集。可使用[命令集名称]对命令集进行查询。

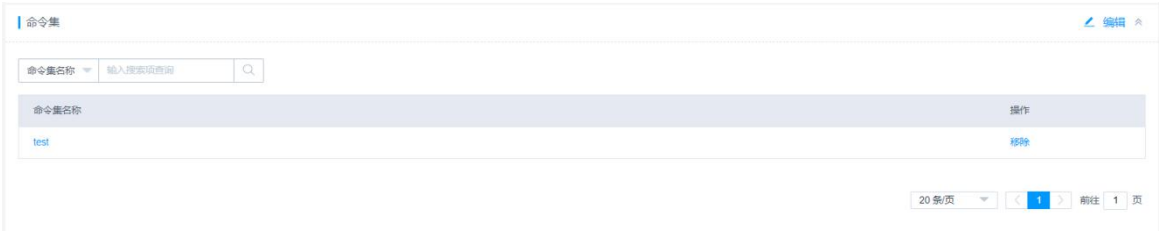


图 8-2-12

[用户][用户组][账户][账户组]详情中展示与访问控制策略相似。

8.2.6 命令集详情

进入[策略/命令控制策略/命令集]，点击<管理>或命令集名称，进入命令集详情页面，如图 8-2-13 所示，点击<编辑>，弹出编辑命令集弹窗，操作与新建命令集类似；

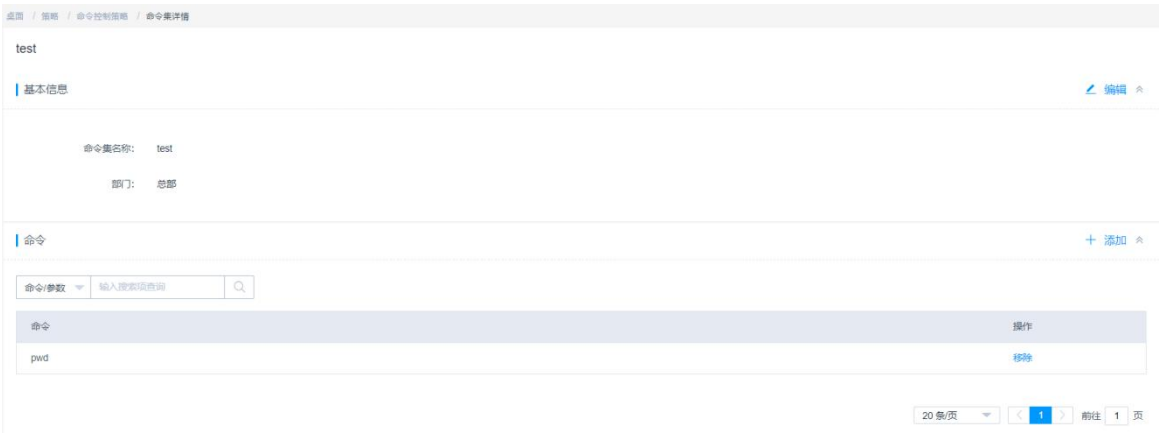


图 8-2-13

8.2.7 命令控制策略搜索

进入[策略/命令控制策略/策略列表]，点击搜索项，弹出搜索项下拉列表，如图 8-2-14，可使用策略名称，用户登录名，资源名称，主机地址，资源账户，命令集名称，命令/参数进行搜索。

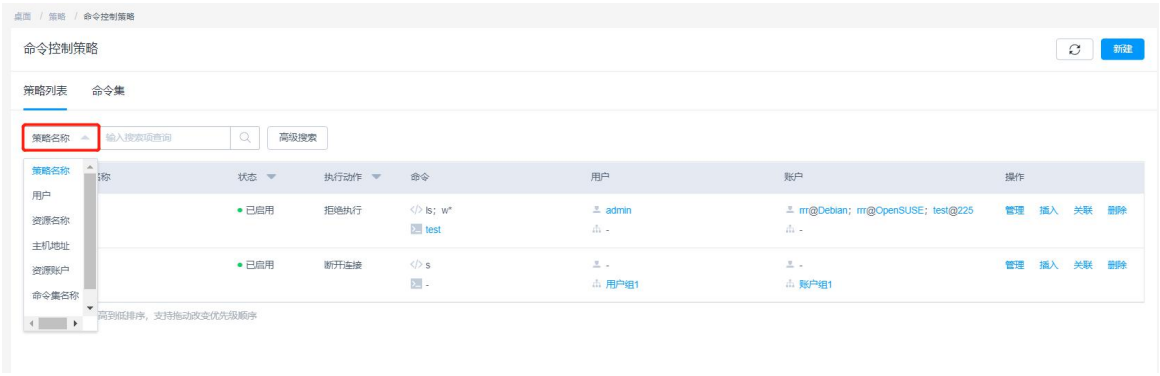


图 8-2-14

点击<高级搜索>，弹出高级搜索框，如图 8-2-15 所示，可使用策略名称，用户登录名，资源名称，主机地址，资源账户，命令集名称，命令/参数，生效时间，失效时间，告警方式，时间

限制，创建者，修改者进行搜索。

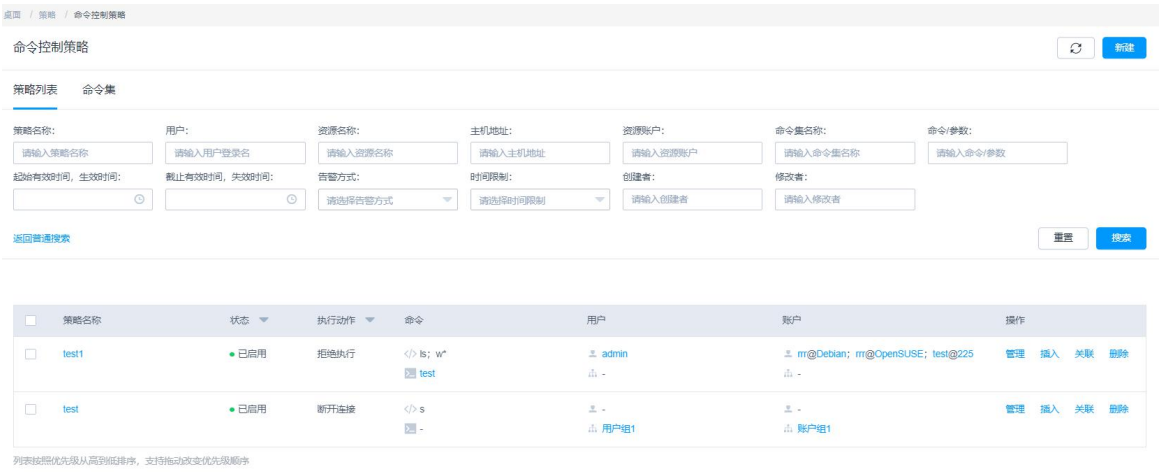


图 8-2-15

8.3 改密策略

8.3.1 改密策略新建

进入[策略/改密策略/策略列表]，如图 8-3-1。点击<新建>，弹出新建策略弹窗，如图 8-3-2，填入策略名称、执行方式、改密方式，可选择优先使用特权账户改密和允许修改特权账户密码。执行方式包含：手动执行、定时执行和周期执行，选择定时执行时需要填写执行时间，选择周期执行时需要填写执行时间和执行周期。改密方式包含：生成不同密码、生成相同密码、指定相同密码，选择指定相同密码时，需要输入密码和确认密码。点击下一步，进入关联账户账户组弹窗，操作与新建访问控制策略类似。

图 8-3-1

图 8-3-2

注意：

1. 选择定时执行时，执行时间可选择至时分秒；选择周期执行时，执行时间只可选择至天，同时执行周期为正整数。
2. 周期执行的执行时间为每天 0 点。

8.3.2 改密策略列表

进入[策略/改密策略/策略列表]，如图 8-3-3。点击<管理>进入对应策略详情页面；点击<立即执行>执行对应改密策略；点击<关联>弹出关联资源账户和账户组下拉列表，操作与新建策略类似；点击<删除>删除对应改密策略。点击列表左下方<启用>启用批量所选改密策略；点击<禁用>禁用批量所选改密策略；点击<删除>批量删除所选改密策略。

列表可使用状态、执行方式、改密方式进行筛选。

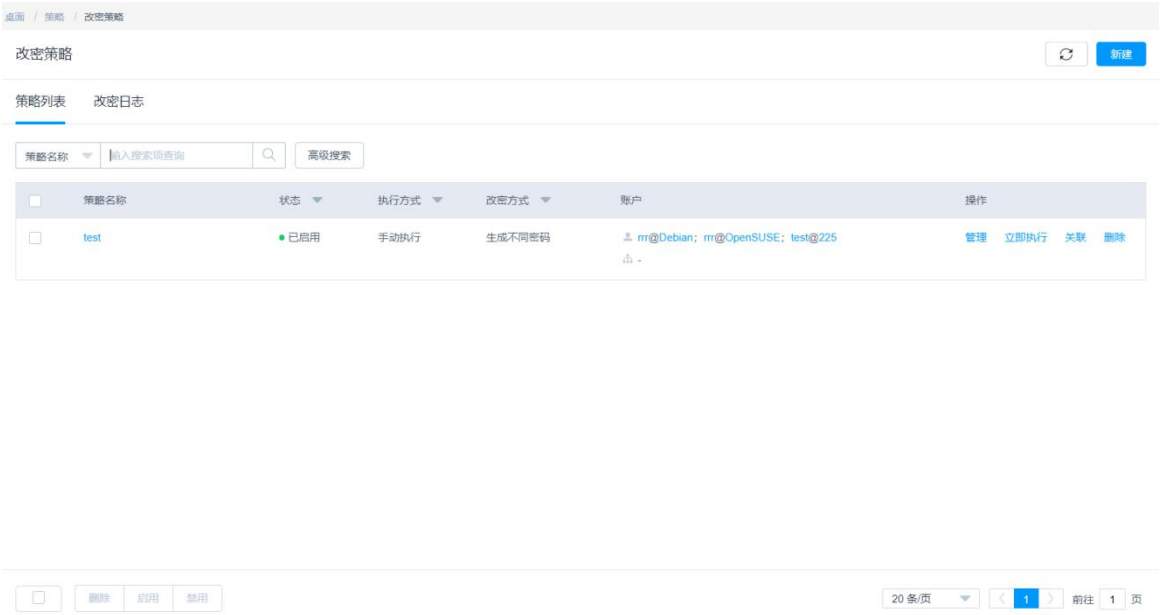


图 8-3-3

8.3.3 改密日志列表

进入[策略/改密策略/改密日志]，如图 8-3-4。点击列表右上方[选择日期范围]，可选择列表展示的改密日志时间范围；可使用时间、总数、成功数、失败数、未修改数进行排序，使用策略名称进行查询；点击<详情>进入改密日志详情页面；点击<下载>下载 xlsx 格式的改密日志；点击<删除>删除当前改密日志。点击列表下方<删除>，批量删除所有选中的改密日志。

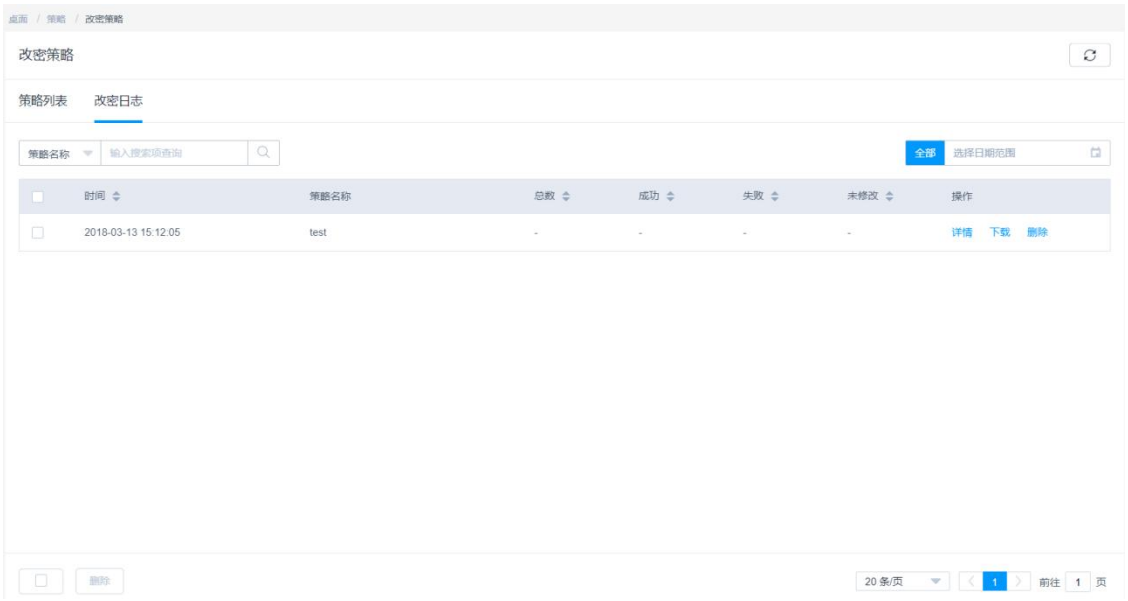


图 8-3-4

8.3.4 改密策略详情

进入[策略/改密策略/策略列表]，点击<管理>或策略名称可进入对应改密策略详情，如图 8-3-5 所示。[基本信息]展示了策略名称、部门、创建者、创建时间、修改者、修改时间、状态、执行方式、改密方式，更多选项。点击<编辑>弹出编辑改策略弹窗，操作与新建改密策略类似。

[资源账户][账户组] 详情中展示与访问控制策略相似。

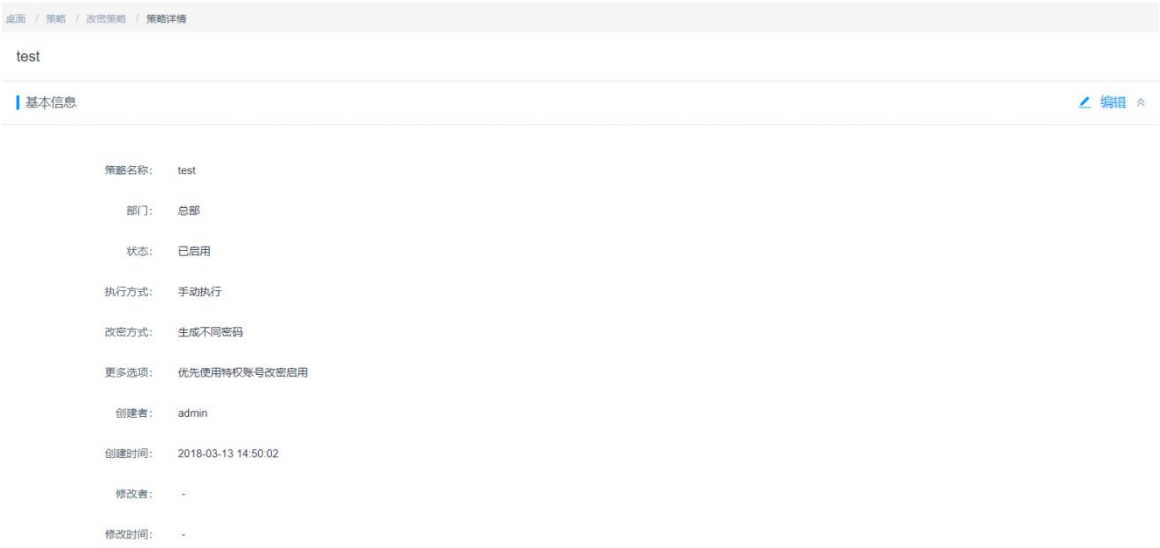


图 8-3-5

8.3.5 改密日志详情

进入[策略/改密策略/改密日志]，点击<详情>可进入对应改密日志详情，如图 8-3-6 所示。

[基本信息]展示了改密策略执行时间，策略名称，总账户数，修改成功账户数，修改失败账户数，未修改账户数。[改密结果]展示了每个资源账户的详细改密结果，通过点击账户名和资源名可以跳转至对应对象详情页面；可使用类型、改密结果进行列表筛选，使用账户，关联资源、主机地址进行搜索。

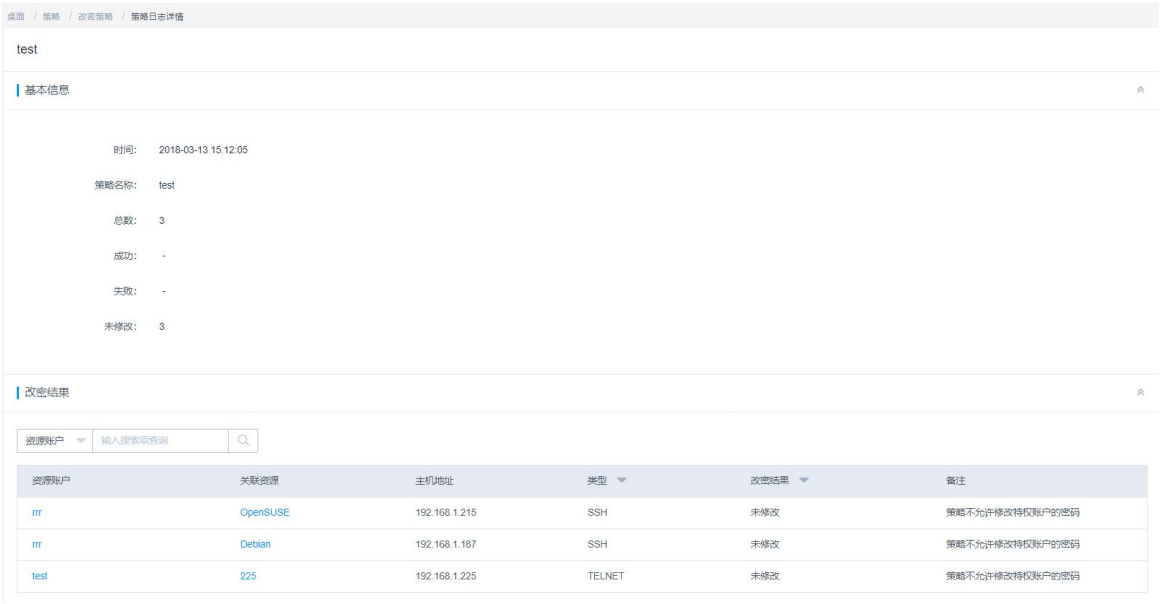


图 8-3-6

8.3.6 改密策略搜索

进入[策略/改密策略/策略列表]，点击搜索项，弹出搜索项下拉列表，如图 8-3-7 所示。可使用策略名称、资源名称、资源账户进行搜索。

图 8-3-7

点击<高级搜索>，弹出高级搜索搜索框，如图 8-3-8 所示。可使用策略名称、资源名称、资源账户、主机地址、执行方式、改密方式、使用特权账户改密、允许修改特权账户密码、执行时间、结束时间、创建者、修改者进行搜索。


桌面 / 策略 / 改密策略
改密策略
新建
策略列表
改密日志
策略名称:
请输入策略名称
资源名称:
请输入资源名称
资源账户:
请输入资源账户
主机地址:
请输入主机地址
执行方式:
请选择执行方式
改密方式:
请选择改密方式
使用特权账户改密:
请选择使用特权账户改密
允许修改特权账户密码:
请选择允许修改特权账...
执行时间:
结束时间:
创建者:
请输入创建者
修改者:
请输入修改者
返回普通搜索
重置
搜索
策略名称
状态
执行方式
改密方式
账户
操作
test
已启用
手动执行
生成不同密码
rr@OpenSUSE; rr@Debian; test@225
-
管理
立即执行
关联
删除

图 8-3-8

第九章 运维

9.1 主机运维

9.1.1 主机运维列表

进入[运维/主机运维]，选择搜索项（可选的搜索项主机名称、主机地址），在输入框内输入关键词点击搜索，如图 9-1-1 所示。

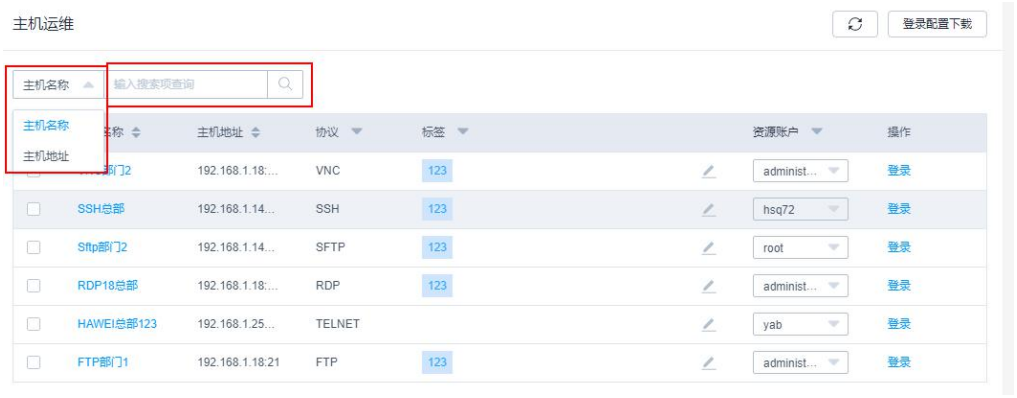


图 9-1-1

进入[运维/主机运维]，点击<登录配置下载>，将运维资源导出成 xshell 或者是 secure CRT 配置，如图 9-1-2 所示。

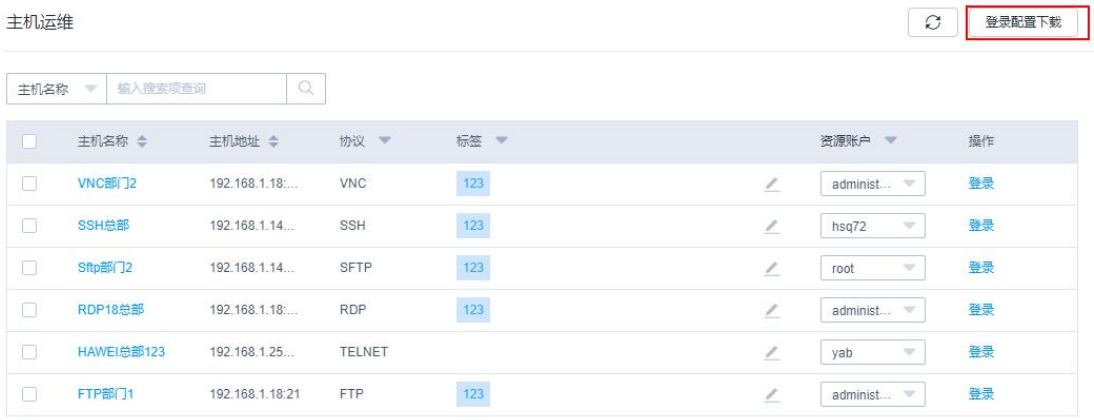


图 9-1-2

进入[运维/主机运维]，点击<登录>，登录主机资源的 H5 会话，如图 9-1-3 所示。

图 9-1-3

除了支持单个登录，还支持多台主机同时登录，勾选几台需要批量登录的主机，点击下方的<批量登录>，如图 9-1-4 所示。

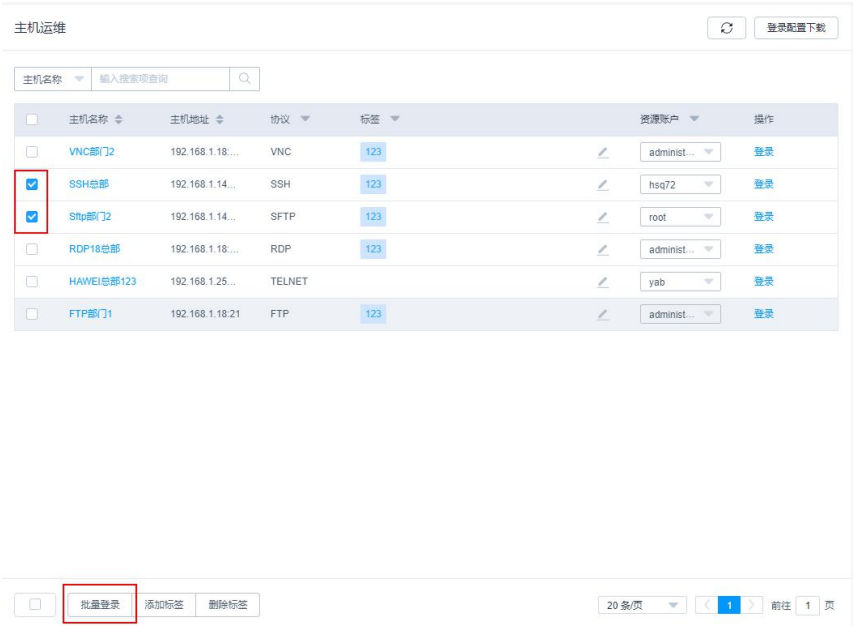


图 9-1-4

进入[运维/主机运维]，勾选几台主机，点击下方的<添加标签>或者是<删除标签>，可以批量添加或者批量删除标签，如图 9-1-5 所示。

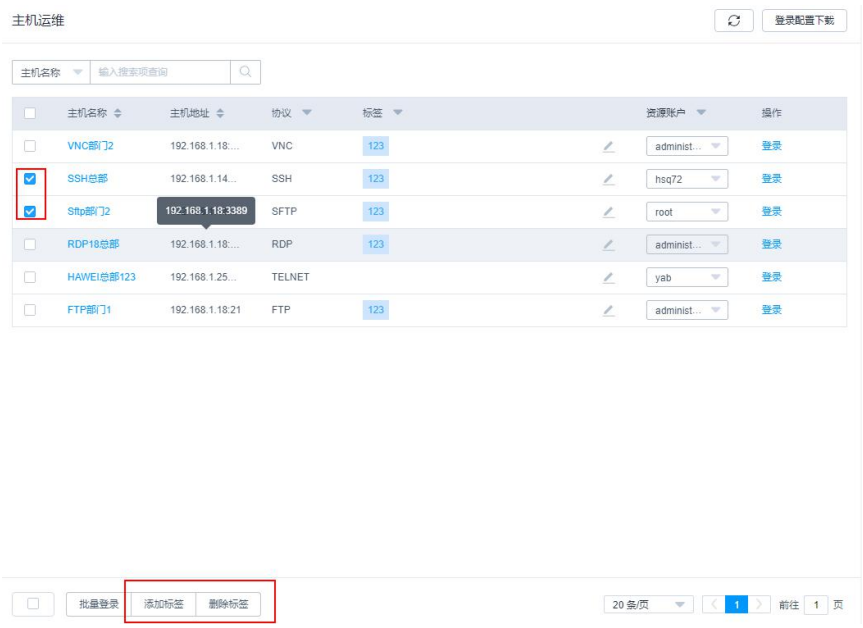


图 9-1-5

9.1.2 H5 页面登录—登录字符协议类型主机

进入[运维/主机运维]，登录 SSH 或 TELNET 协议主机，如图 9-1-6 所示。

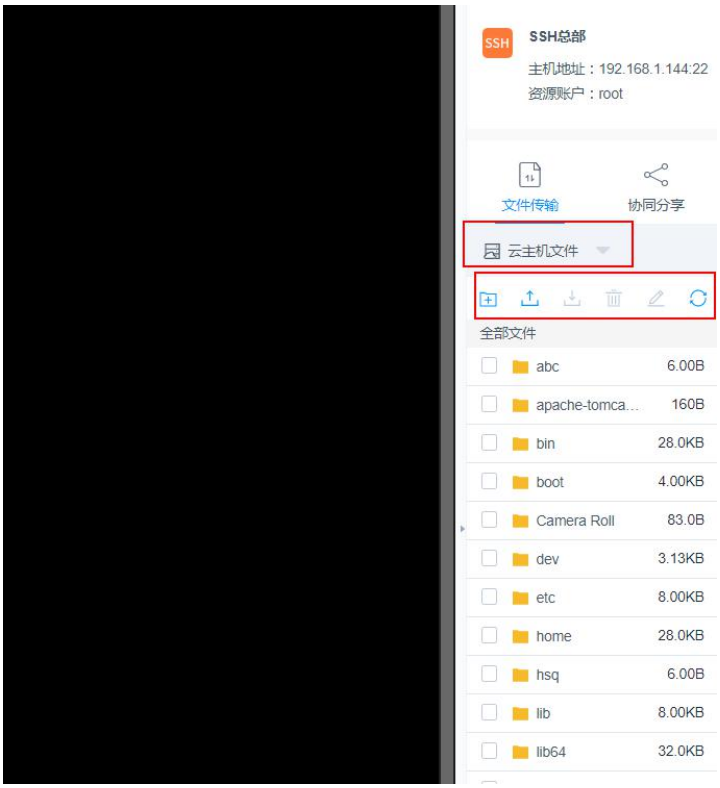


图 9-1-6

SSH 或 TELNET 协议主机 h5 会话的登录，支持文件传输。支持在云主机上上传、下载、编辑、删除文件或者文件夹；支持新建文件夹；也支持在主机网盘的上传、下载、新建、编辑、修改文件夹和文件。

注意：

1. 当目标地址为：云主机文件
点击【上传】图标，下拉展示：上传本地文件、上传网盘文件
点击【上传本地文件】，调用浏览器自带的上传功能，支持：上传多个文件
点击【上传网盘文件】，支持：上传多个文件
点击【下载】图标，下拉展示：下载到本地、下载到网盘
点击【下载到本地】，调用浏览器自带的下载功能，将选中文件保存到本地
点击【下载到网盘】，将选中文件保存到网盘
2. 当目标地址为：主机网盘
点击【上传】图标，下拉展示：上传本地文件、上传本地文件夹
点击【上传本地文件】，调用浏览器自带的上传功能，支持：上传多个文件
点击【上传本地文件夹】，调用浏览器自带的上传功能，支持上传一个文件夹
点击【下载】图标，调用浏览器自带的下载功能，将选中文件保存到本地
3. 支持批量删除
4. 不支持批量编辑文件或者文件夹

SSH 或 TELNET 协议主机 h5 会话的登录，支持协同分享。如图 9-1-7 所示，创建者可以将当前会话的链接复制，发送给协助者。协助者可以通过该链接登录创建者的会话中，如图 9-1-8 所示。

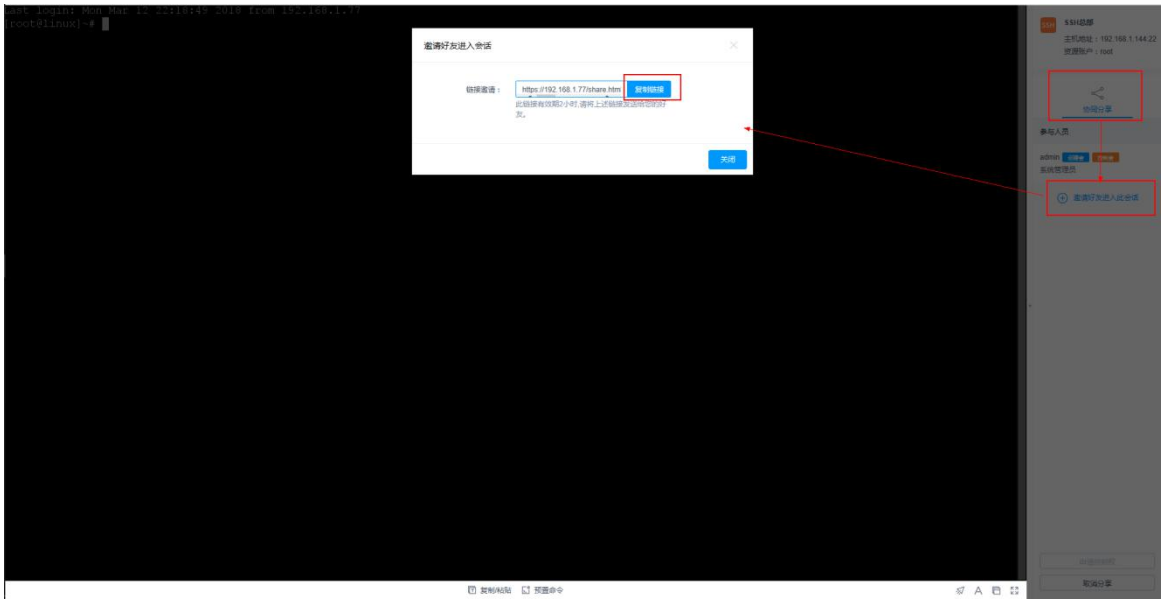


图 9-1-7

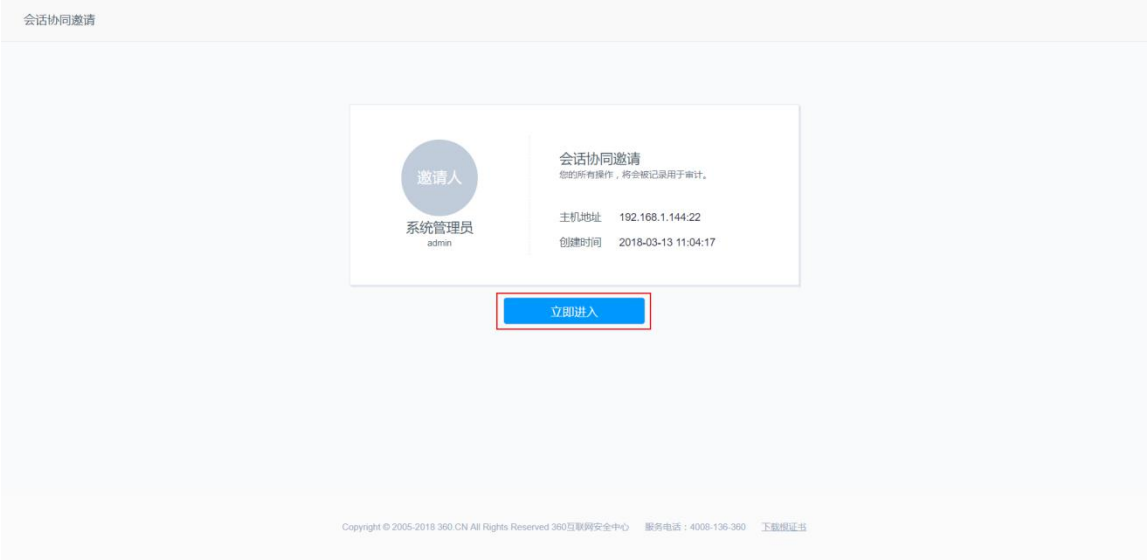


图 9-1-8

在会话协同中，没有会话控制权限的用户可以点击【申请控制】，向当前的控制者发送控制申请，申请控制当前会话的权限，如图 9-1-9 所示。

图 9-1-9

注意：

1. 当控制者申请获得会话控制权。此时点击提示的【强制获取】，会强制获取控制权
2. 当有用户申请控制时，当前会话控制者有权可以拒绝、关闭、同样申请
3. 当创建者取消分享或者是退出当前会话时候，协同用户被踢出会话，并且不能通过之前的链接再次进入
4. 当协同者拥有控制权限时，可以点击【释放控制】，会话的控制权限会回到创建者手中
5. 协同用户退出会话之后，当分享会话还有效且链接未过期时，可以通过之前的链接再次进入会话
6. 协同用户如果当前有控制器，退出会话之后，控制器转移到创建者

SSH 或 TELNET 协议主机 h5 会话的登录，支持设置预置命令，如图 9-1-10 所示。输入命令名称，命令内容，点击添加保存预置命令，如图 9-1-11 所示。

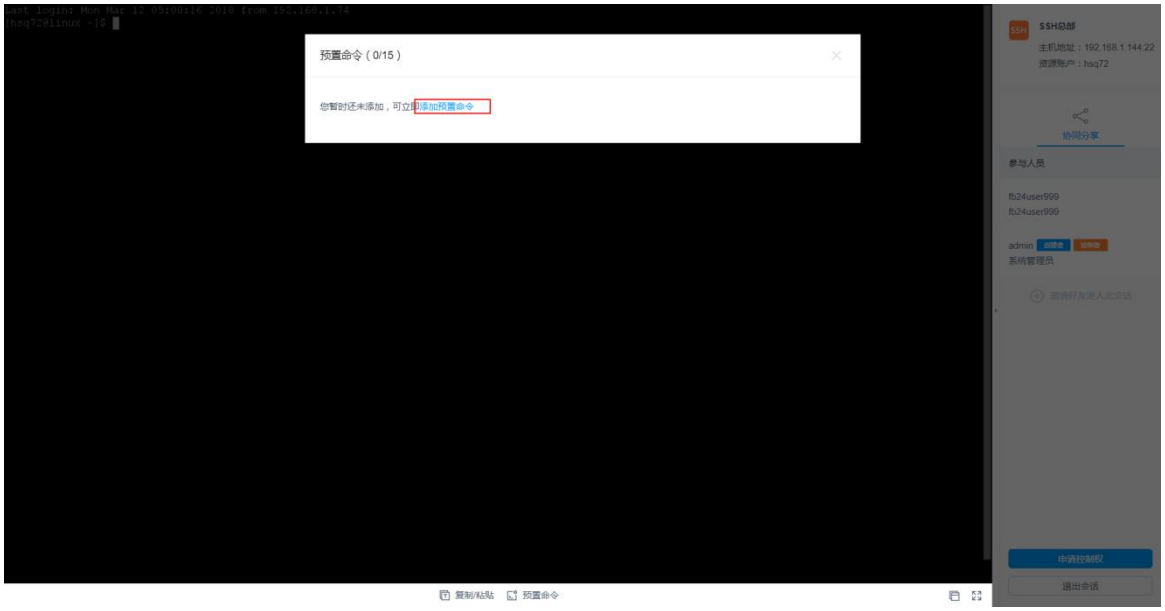


图 9-1-10

图 9-1-11

点击某个预设命令，命令填写到远端机器，按回车执行命令，如图 9-1-12。

图 9-1-12

9.1.3 H5 页面登录—登录图像协议类型主机

进入[运维]，登录 RDP、VNC 或应用发布资源，如图 9-1-13 所示。

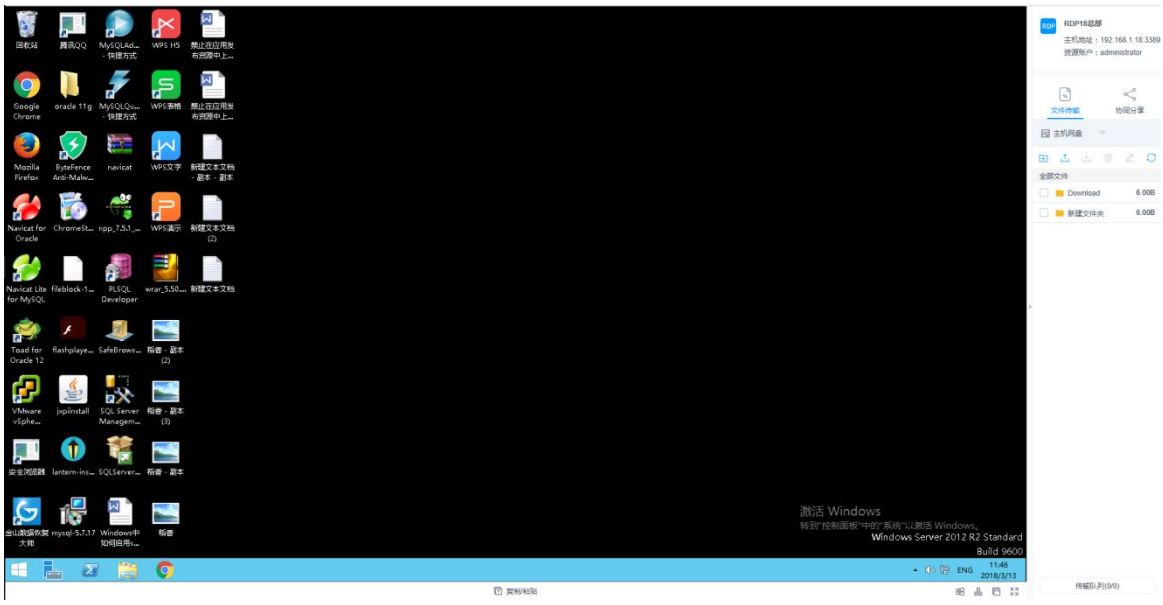


图 9-1-13

图像协议类型主机 h5 会话的登录，支持文件传输。如图 9-1-14 所示，与 SSH 类似，区别在于 RDP 的目标地址只有：主机网盘。

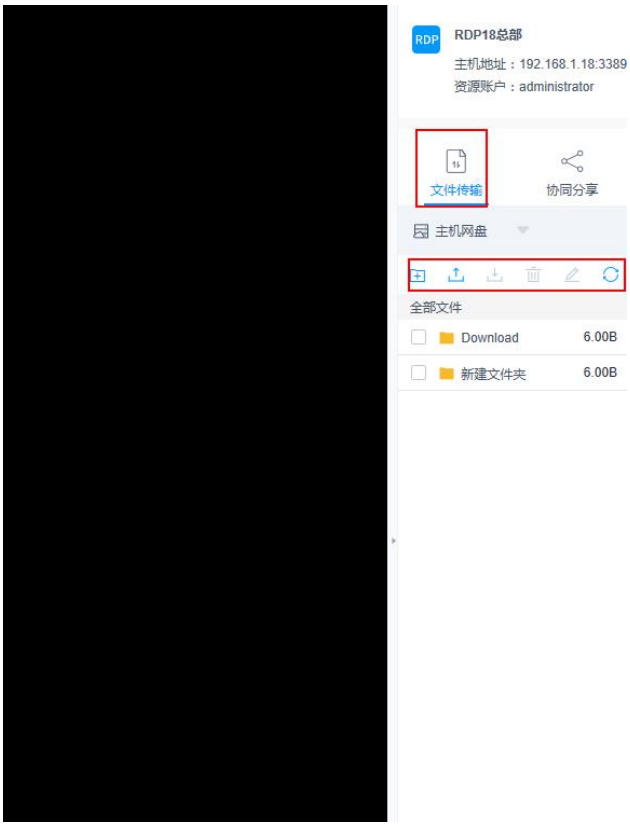


图 9-1-14

图像协议类型主机 h5 会话的协同分享，参考 H5 登录字符协议类型主机的协同分享。

9.1.4 SSH 客户端登录

通过 SSH 客户端(putty，SecureCRT、xshell、MAC terminal、linux terminal、secure shell client)登录云堡垒机，可以在不改变用户原来使用 SSH 客户端习惯的前提下对授权资源进行运维管理，并且支持云堡垒机系统的命令拦截策略和运维审计功能。如图 9-1-15，主机 IP 填写堡垒机地址，端口为 2222，登录用户名写堡垒机账户，登录密码写的是堡垒机密码。

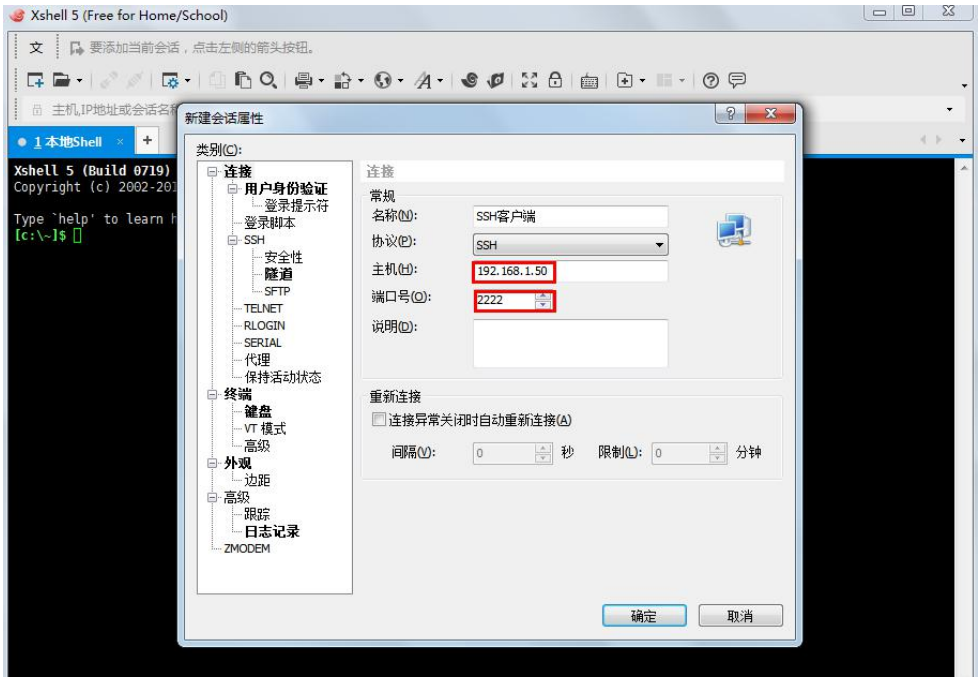


图 9-1-15

除了使用密码登录之外，还支持公钥方式登录堡垒机。用户可以先在堡垒机登录个人中心，添加公钥，如图 9-1-16。然后用户可以通过私钥登录堡垒机而无需再记住密码。在登录客户端时，选择在用户身份验证设置中，选择 Public Key，输入云堡垒机用户名，选择对应的私钥登录堡垒机，如图 9-1-17。

图 9-1-16

图 9-1-17

除了使用堡垒机账户密码直接登录的方式外，还支持使用 API 的登录方式登录堡垒机指定的资源登录账户，如图 9-1-18 所示。登录用户名输入：主账号@从账号@主机地址:端口，例如说 admin@root@192.168.1.100:22，登录密码输入堡垒机密码。除了使用密码登录之外，还支持公钥方式登录堡垒机。公钥登录方式如同上面的非 API 登录方式所示。

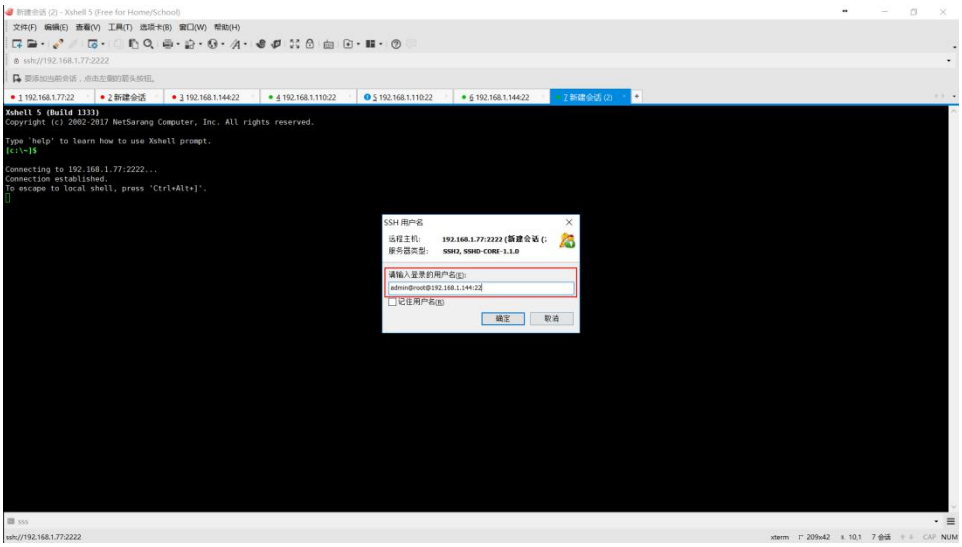


图 9-1-18

修改堡垒机 SSH 运维端口，可在系统->系统配置->端口配置->SSH/SFTP 端口中更改，如图 9-1-19 所示。配置完端口后需要重启堡垒机。

图 9-1-19

进入非 API 登进堡垒机的界面，可以使用快捷命令操作堡垒机，如图 9-1-20 所示。输入命令：l，列举 ssh 资源；输入命令：i，列举 telnet 资源；输入命令：s，搜索资源的 IP、名称、标签；输入命令：k，展示最近登录的 10 个历史会话；输入命令：x，语言切换；输入命令：h，展示帮助信息；输入命令：e，退出登录。

图 9-1-20

注意：

1. 使用非 API 方式登录堡垒机，使用 Space 键显示下一页，使用 Enter 键显示全部，使用 ESC 退出当前列表

9.1.5 SFTP 客户端登录

堡垒机支持使用 API 的登录方式登录 sftp 协议类型主机，如图 9-1-21 所示。登录 IP 填写堡垒机 IP，登录端口填写：2222（端口可以在后面修改），登录用户名输入：主账号@从账号@主机地址:端口，例如说 admin@root@192.168.1.144:22，登录密码输入堡垒机密码。除了使用密码登录之外，还支持公钥方式登录堡垒机。公钥登录方式同上面的 ssh 客户端公钥登录方式所

示。

图 9-1-21

修改 sftp 登录端口，可在系统->系统配置->端口配置->SSH/SFTP 端口中更改，如图 9-1-22 所示。配置完端口后需要重启堡垒机。

图 9-1-22

SFTP 在根目录上，可以通过特殊的列表项“!UTF-8”或“!gb18030”来进行切换使用不同的编码，如图 9-1-23 所示。

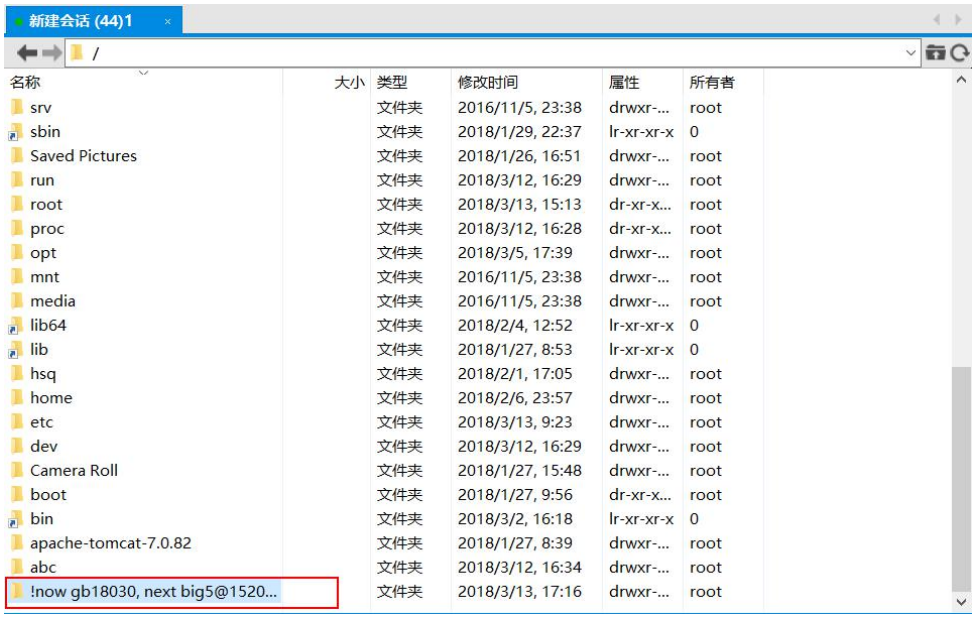


图 9-1-23

注意：

1. 支持的 SFTP 客户端种类：Xftp、WinSCP、FlashFXP

9.1.6 FTP 客户端登录

堡垒机支持登录 FTP 协议类型主机，如图 9-1-24 所示。主机 IP、用户名、密码在登录 FTP 主机运维的登录弹窗获取，如图 9-1-25 所示。

图 9-1-24

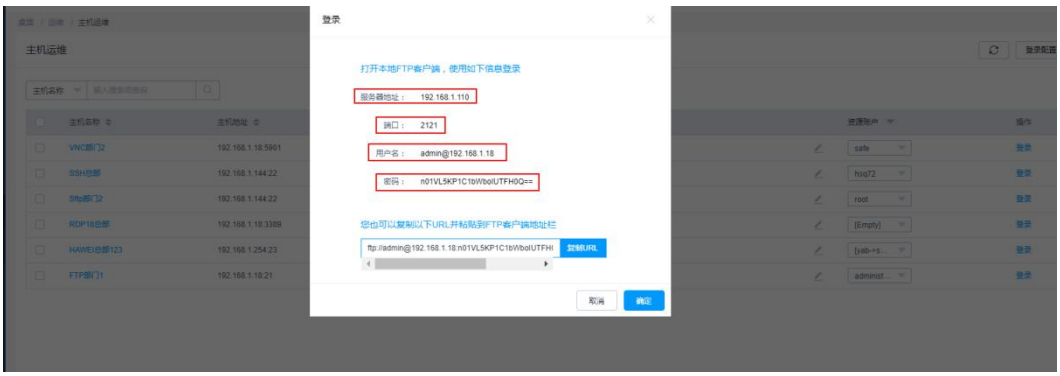


图 9-1-25

修改 FTP 登录端口，可在系统->系统配置->端口配置-> FTP 端口中更改，如图 9-1-26 所示。配置完端口后需要重启堡垒机。

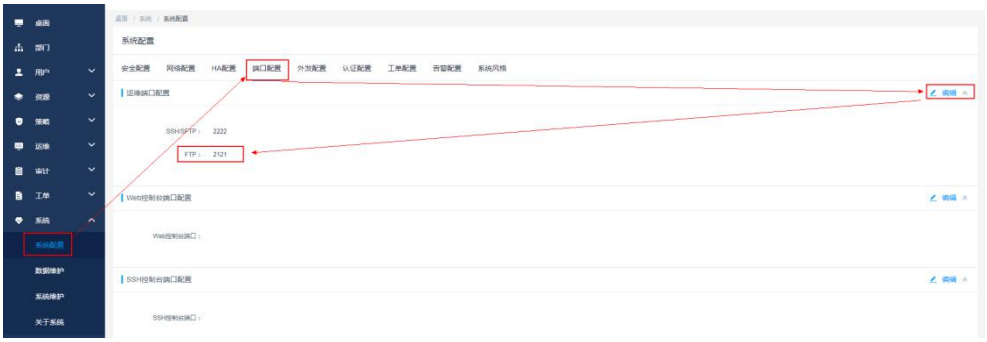


图 9-1-26

FTP 在根目录上，可以通过特殊的列表项“!UTF-8”或“!gb18030”来进行切换使用不同的编码，如图 9-1-27 所示。

图 9-1-27

注意：

1. 支持的 FTP 客户端种类：Xftp、WinSCP、FlashFXP、FileZilla

9.2 应用运维

9.2.1 应用运维列表

进入[运维/应用运维]，选择搜索项（可选的搜索项有应用名称、应用参数），在输入框内输入关键词点击搜索，如图 9-2-1 所示。

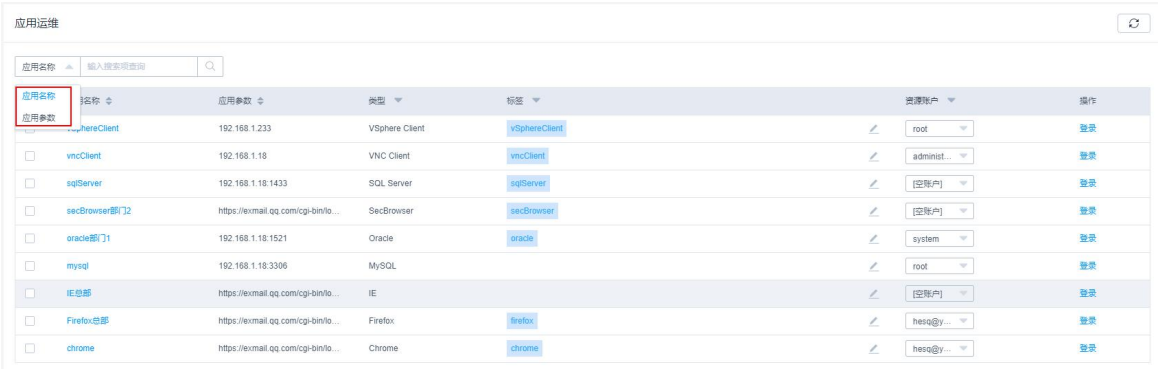


图 9-2-1

进入[运维/应用运维]，点击<登录>，登录应用发布的 H5 会话，如图 9-2-2 所示。

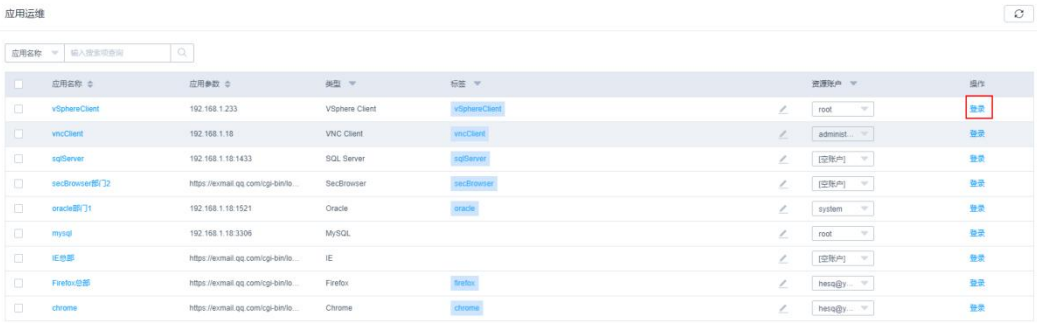


图 9-2-2

进入[运维/应用运维]，勾选几台主机，点击下方的<添加标签>或者是<删除标签>，可以批量添加或者批量删除标签，如图 9-2-3 所示。

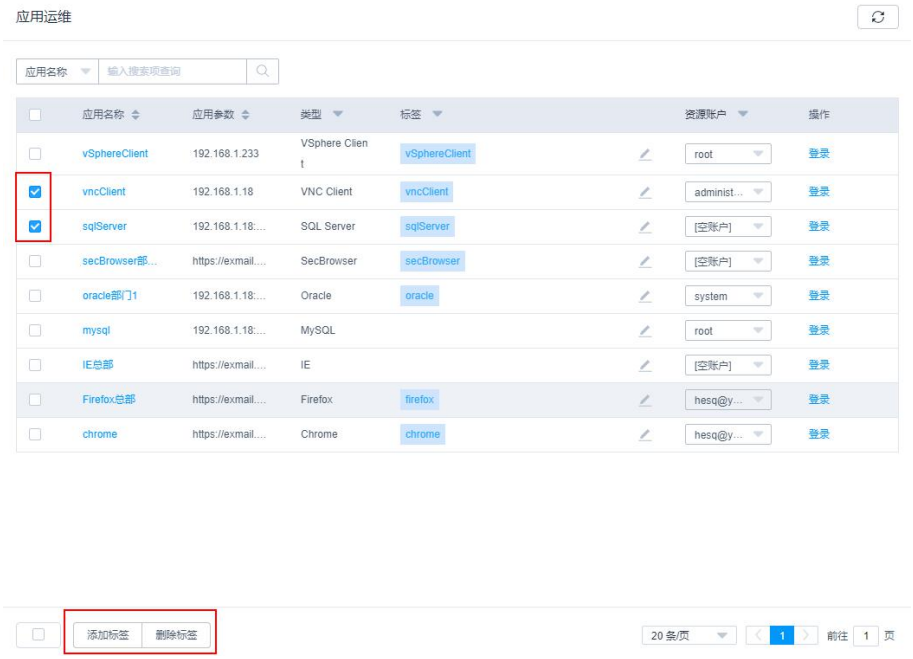


图 9-2-3

第十章 审计

10.1 实时会话

10.1.1 实时会话列表

进入[审计/实时会话]，如图 10-1-1 所示。点击搜索项，弹出搜索项下拉列表，可使用资源名称、资源账户、用户、来源 IP 进行搜索。点击<详情>，进入对应会话详情页面；点击<监控>，进入实时会话监控页面；点击<中断>，中断对应会话。点击列表下方<中断>，批量中断所有选中的会话。

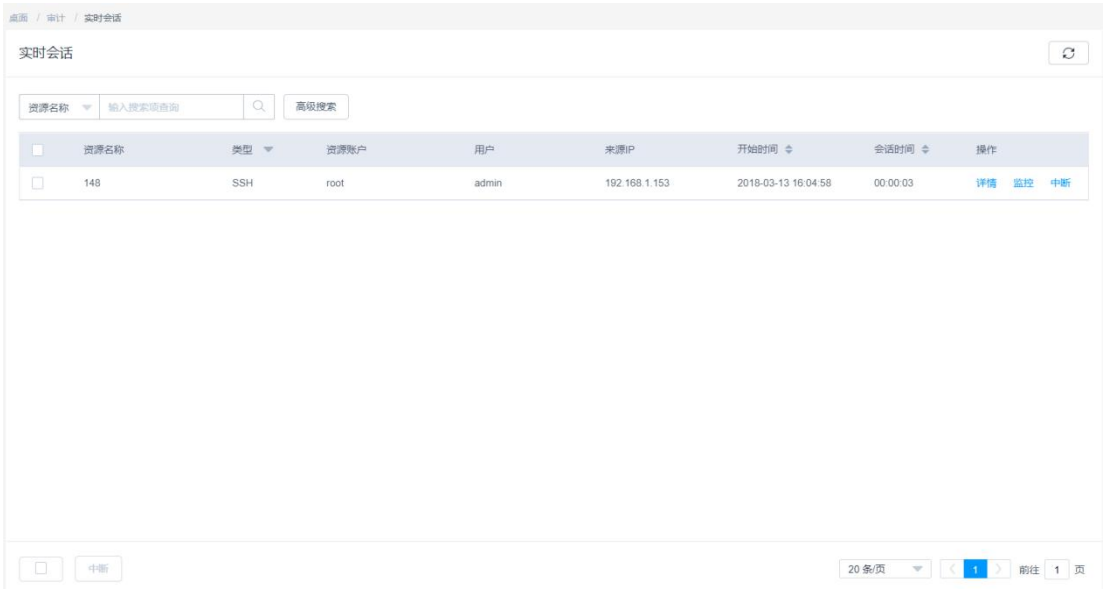


图 10-1- 1

点击<高级搜索>，弹出高级搜索搜索框，如图 10-1- 2 所示。可使用资源名称、资源账户、用户、来源 IP、主机地址、起始时间、截止时间、会话时长范围、操作指令、双人授权、双人授权用户、会话协同、会话协同用户进行搜索。

列表可使用协议类型进行筛选；可使用开始时间和会话时长进行排序。

图 10-1- 2

10.1.2 实时监控

进入[审计/实时会话]，点击<监控>，如图 10-1-3 所示为字符协议实时监控。

监控页面右上方展示会话相关信息：资源名称、主机类型、主机地址、资源账户、运维用户、开始时间。[运维记录]中展示运维用户操作指令的记录，可用命令进行查询，可用允许执行、动态授权、拒绝执行进行筛选。[文件传输]中展示运维用户上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)的操作，可用文件(夹)名称进行查询，可用上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)进行筛选。[参与用户]中展示监控用户和协同用户的登录名、姓名、开始监控(协同)时间。

下方工具栏中，点击<截屏>图标，将页面截屏并保存为 PNG 格式下载；点击<中断>图标，中断当前会话；点击<全屏>图标，页面变为全屏显示。

图 10-1- 3

注意：

1) SSH 客户端实时监控无监控文件传输与参与用户。

图 10-1-4 展示图形协议实时监控

监控页面右上方展示会话相关信息：资源名称、主机类型、主机地址、应用参数、资源账户、运维用户、开始时间。[运维记录]中展示键盘输入和剪贴板复制粘贴操作，可用键盘输入、剪切板内容进行查询，可用键盘输入、剪切板进行筛选。[文件传输]中展示上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)，可用文件(夹)名称进行查询，可用上传文件、下

载文件、创建文件夹、重命名文件(夹)、删除文件(夹)进行筛选。[参与用户]中展示监控用户和协同用户的登录名、姓名、开始监控(协同)时间。

下方工具栏中，点击<截屏>图标，将页面截屏并保存为 PNG 格式下载；点击<中断>图标，中断当前会话；点击<全屏>图标，页面变为全屏显示。[鼠标左键][鼠标中键][鼠标右键][Control 键][Shift 键][Alt 键]等图标，当运维用户点击对应按键时，相应的图标会亮起。

图 10-1-4

注意：

1) 应用参数仅当登录应用资源时显示，数据库应用时，展示：数据库 IP:端口；非数据库应用，展示：启动参数

10.1.3 会话详情

进入[审计/实时会话]，点击<详情>进入对应实时会话详情页面，如图 10-1-5 所示为字符协议会话详情。点击<监控>进入实时会话监控页面；点击<中断>中断此会话。[资源会话信息]展示资源名称、协议类型、主机地址、资源账户、开始时间、会话时长、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、登录时间、会话时长、认证类型、多因子认证、登录方式。

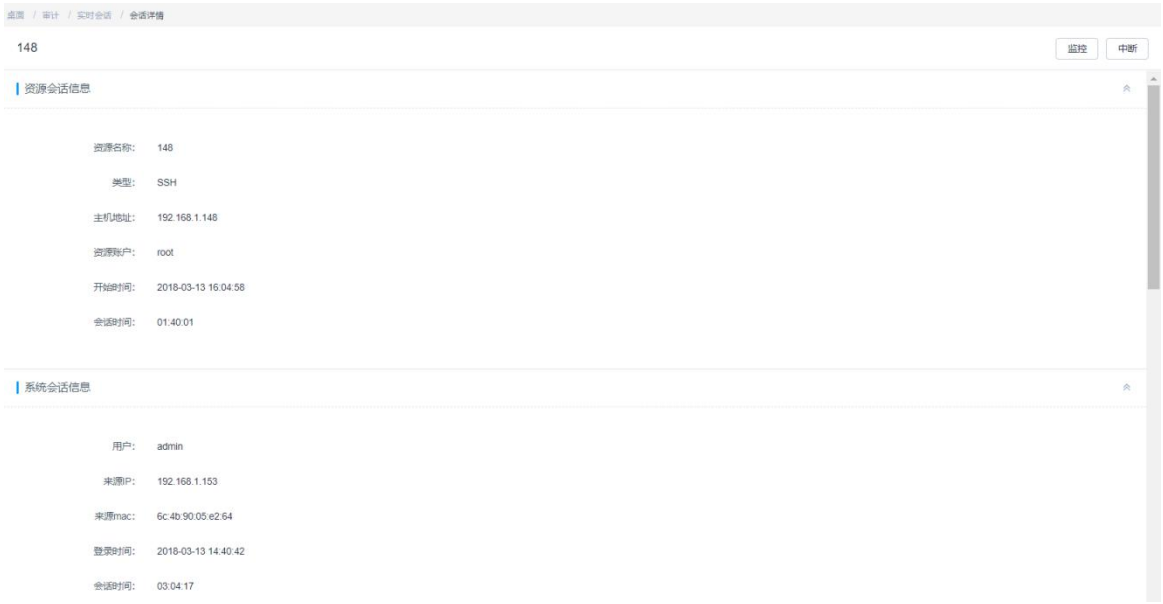


图 10-1- 5

[运维记录]展示用户执行的操作指令，如图 10-1- 6 所示。点击<展开>后，展示字符命令输出结果。可使用用户登录名、操作指令进行查询；可使用时间进行排序；可用执行动作进行筛选。

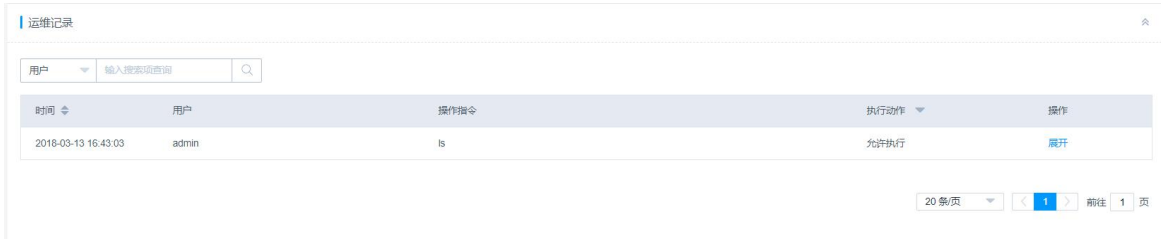


图 10-1- 6

[文件传输]展示用户对文件进行的操作，如图 10-1- 7 所示。可用文件名称、来源路径、目标路径进行搜索；可用时间、文件大小、传输时间进行搜索；可用类型、结果进行筛选。

图 10-1- 7

[会话协同]展示会话中产生协同会话的信息，如图 10-1- 8 所示。可用用户登录名进行查询；可用加入时间、退出时间进行排序。

图 10-1- 8

如图 10-1- 9 显示为图形协议会话详情页面。[资源会话信息]展示资源名称、协议类型、主机地址、数据库 IP，数据库端口，数据库名，启动参数，资源账户、开始时间、会话时长、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、登录时间、会话时长、认证类型、多因子认证、登录方式。

注意：

1) 当资源为应用发布时，主机地址隐藏。

2) 当资源为主机或非数据库应用时，数据库 IP、数据库端口、数据库名隐藏。

3) 当资源为主机或数据库应用时，启动参数隐藏。

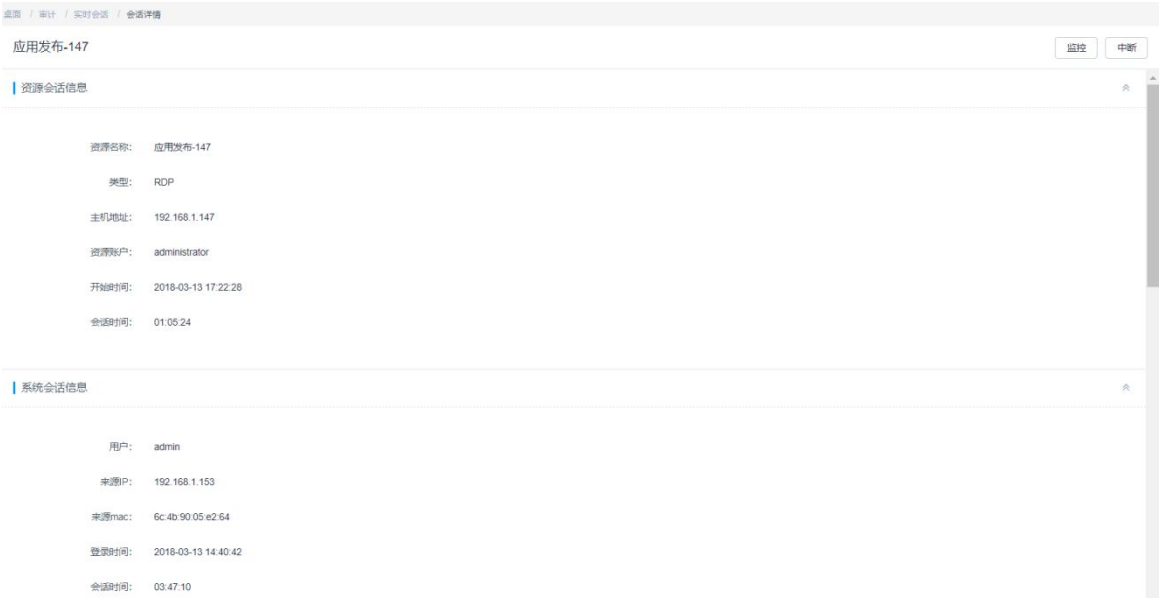


图 10-1-9

[运维记录]展示用户键盘输入和剪切板复制粘贴，如图 10-1- 10 所示。可使用用户登录名、操作指令进行查询；可使用时间进行排序；可用类型进行筛选。

[文件传输][会话协同]展示与字符协议会话详情类似。

图 10-1- 10

如图 10-1- 11 显示为文件传输协议会话详情页面。[资源会话信息]展示资源名称、协议类型、主机地址、资源账户、开始时间、会话时长、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、登录时间、会话时长、认证类型、多因子认证、登录方式。

[文件传输]展示与字符协议会话详情类似。

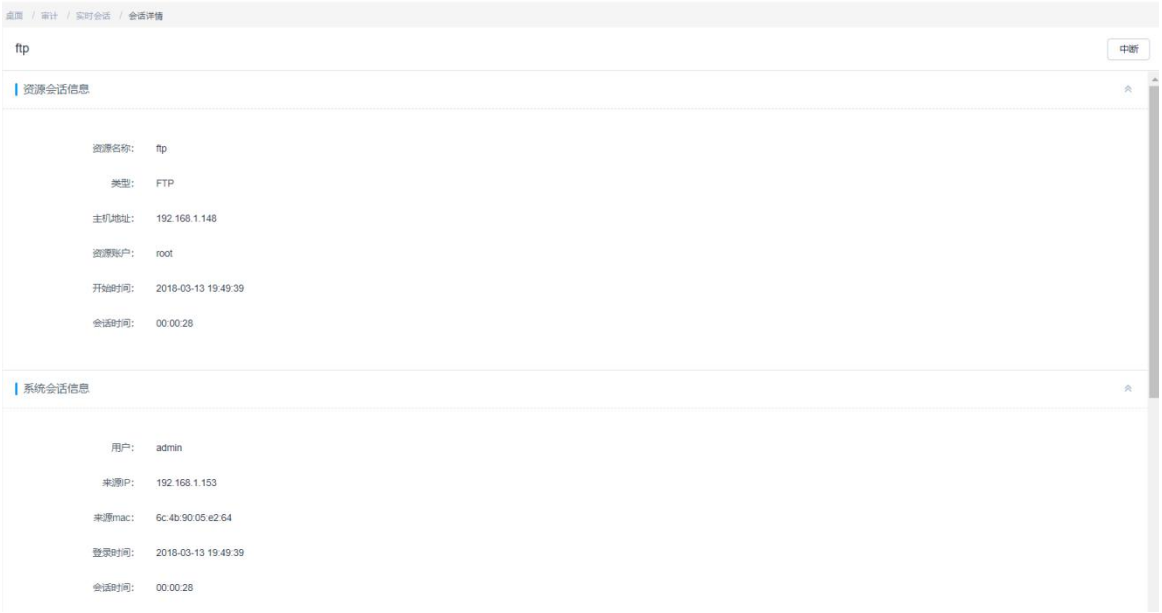


图 10-1- 11

10.2 历史会话

10.2.1 历史会话列表

进入[审计/历史会话]，如图 10-2-1 所示。点击<详情>进入历史会话详情页面；点击<播放>进入历史会话播放页面；点击<下载>下载 M4V 格式的审计视频文件。点击<导出>导出 XLSX 格式历史会话记录。

使用类型和结束状态进行列表筛选；使用起止时间、会话时长进行列表排序。

点击搜索项弹出搜索项下拉列表；点击<高级搜索>弹出高级搜索搜索框，可使用资源名称、资源账户、用户、来源 IP、主机地址、起始时间、截止时间、会话时长范围、操作指令、双人授权、双人授权用户、会话协同、会话协同用户进行搜索。

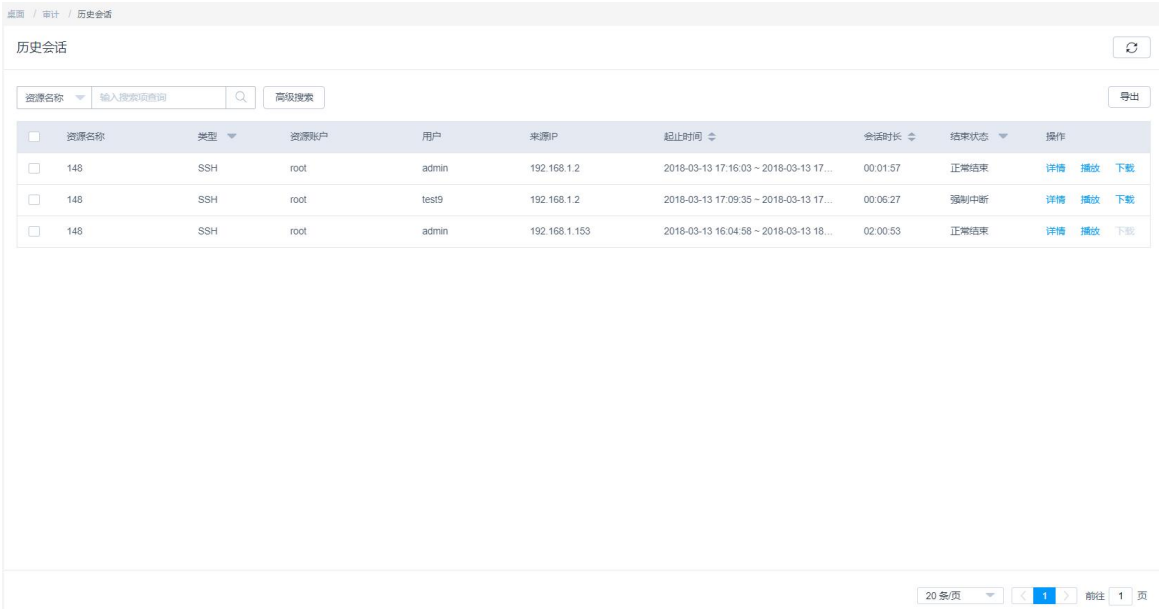


图 10-2- 1

注意：

1) 当登录方式为 SSH 客户端时，无法下载审计视频文件。

2) 当协议为文件传输协议时，无法播放和下载审计文件。

10.2.2 历史会话播放

可以播放不同资源（包括图形协议主机或者应用发布资源）的历史会话。

进入[审计/历史会话]，点击<播放>，如图 10-2-2 所示，为字符协议历史会话播放页面。

图 10-2- 2

[运维记录]中展示运维用户操作指令的记录，可用命令进行查询，可用允许执行、动态授权、拒绝执行进行筛选；点击<定位>图标后，可定位到当前操作指令进行播放。[文件传输]中展示运维用户上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)的操作，可用文件(夹)名称进行查询，可用上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)进行筛选。[参与用户]中展示监控用户和协同用户的登录名、姓名、开始监控(协同)时间。

下方工具栏中，点击<截屏>图标，将页面截屏并保存为 PNG 格式下载；点击<播放列表>图标，右侧切换为播放列表；点击<全屏>图标，页面变为全屏显示。点击<暂停/播放>图标，暂停或播放视频；点击<上一个>图标，播放上一个视频；点击<下一个>图标，播放下一个视频；点击<播放速度>图标，选择播放速度，包括：正常速度、2X 速度、4X 速度、8X 速度、16X 速度。[播放时间]显示格式为当前时间/会话时长。

如图 10-2-3 所示，为图形协议历史会话播放页面。

图 10-2-3

监控页面右上方展示会话相关信息：资源名称、主机类型、主机地址、应用参数、资源账户、运维用户、开始时间。[运维记录]中展示键盘输入和剪贴板复制粘贴操作，可用键盘输入、剪切板内容进行查询，可用键盘输入、剪切板进行筛选；点击<定位>图标后，可定位到当前操作指令进行播放。[文件传输]中展示上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)，可用文件(夹)名称进行查询，可用上传文件、下载文件、创建文件夹、重命名文件(夹)、删除文件(夹)进行筛选。[参与用户]中展示监控用户和协同用户的登录名、姓名、开始监控(协同)时间。

下方工具栏中，点击<截屏>图标，将页面截屏并保存为 PNG 格式下载；点击<播放列表>图标，右侧切换为播放列表；点击<全屏>图标，页面变为全屏显示。[鼠标左键][鼠标中键][鼠标右键][Control 键][Shift 键][Alt 键]等图标，当当前时间运维用户点击对应按键时，相应的图标会亮起。点击<暂停/播放>图标，暂停或播放视频；点击<上一个>图标，播放上一个视频；点击<下一个>图标，播放下一个视频；点击<播放速度>图标，选择播放速度，包括：正常速度、2X 速度、4X 速度、8X 速度、16X 速度。[播放时间]显示格式为当前时间/会话时长。

10.2.3 历史会话详情

进入[审计/历史会话]，点击<详情>，如图 10-2-4 所示，为字符协议历史会话详情。

[资源会话信息]展示资源名称、协议类型、主机地址、资源账户、起止时间、会话时长、会话大小、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、起止时间、会话时长、认证类型、多因子认证、登录方式。

注意：

1) 当未进行双人授权时，资源会话信息中双人授权用户和双人授权时间隐藏。

2) 会话大小中显示的大小为日志文件大小而非下载的视频文件大小。

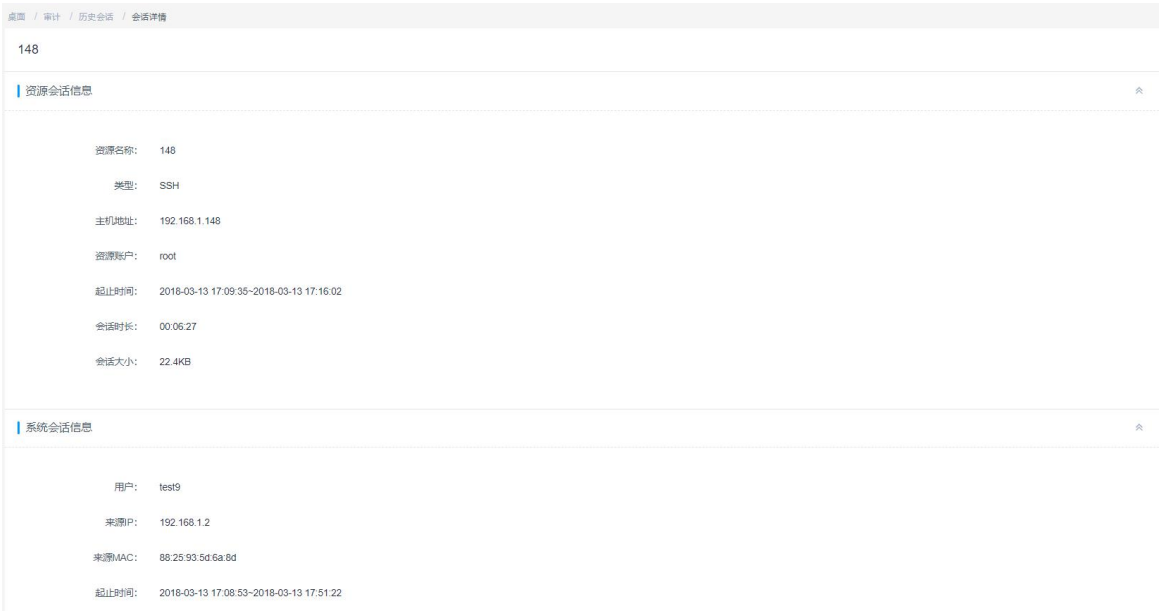


图 10-2- 4

[运维记录]展示用户执行的操作指令，如图 10-2-5 所示。点击<展开>后，展示字符命令输出结果。可使用用户登录名、操作指令进行查询；点击<播放>后，跳转到历史会话播放页面，定位当前操作开始播放视频。可使用时间进行排序；可用执行动作进行筛选。

[文件传输][会话协同]列表与实时会话字符协议详情类似。

图 10-2- 5

如图 10-2-6 所示，为图形协议历史会话详情。

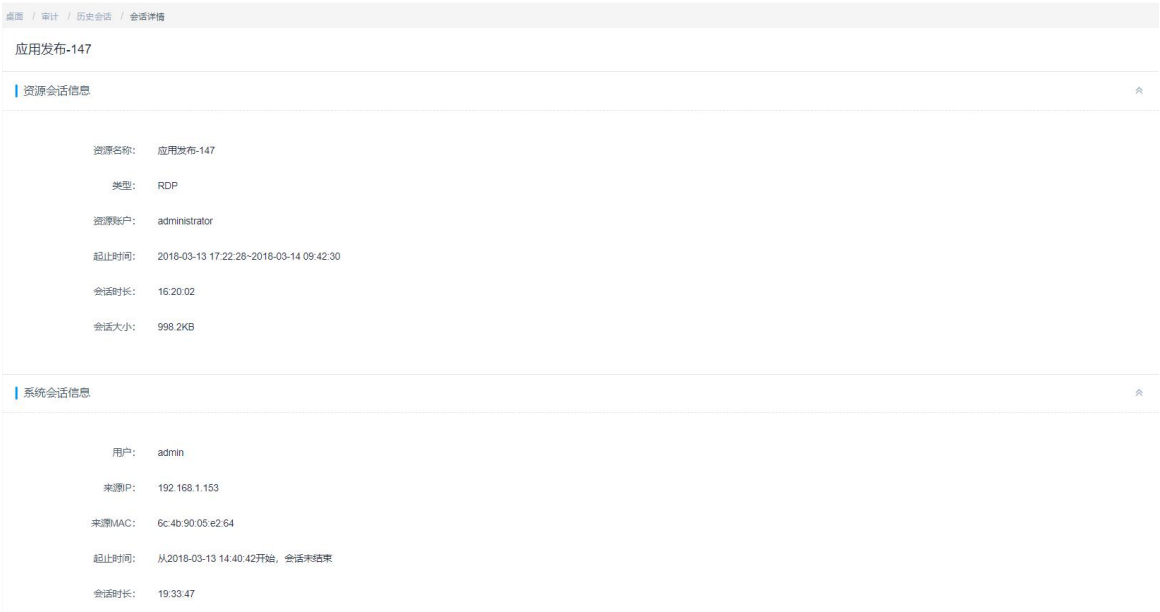


图 10-2- 6

[资源会话信息]展示资源名称、协议类型、主机地址、数据库 IP，数据库端口，数据库名，启动参数，资源账户、开始时间、会话时长、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、登录时间、会话时长、认证类型、多因子认证、登录方式。

[运维记录]展示用户键盘输入和剪切板复制粘贴，如图 10-2- 7 所示。点击<播放>后，跳转到历史会话播放页面，定位当前操作开始播放视频。可使用用户登录名、操作指令进行查询；可使用时间进行排序；可用类型进行筛选。

[文件传输][会话协同]展示与字符协议会话详情类似。

图 10-2- 7

如图 10-2-8 所示，为文件传输协议历史会话详情。

[资源会话信息]展示资源名称、协议类型、主机地址、资源账户、起止时间、会话时长、会话大小、双人授权用户、双人授权时间；[系统会话信息]展示用户登录名、来源 IP、来源 MAC、起止时间、会话时长、认证类型、多因子认证、登录方式。

[文件传输]列表与字符协议历史会话详情类似。

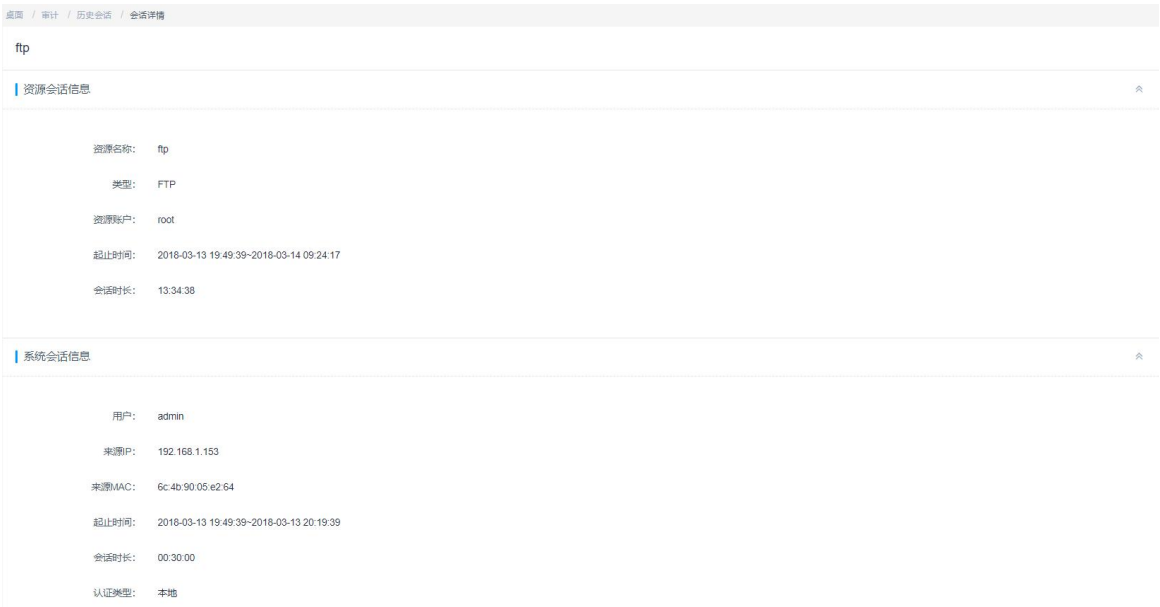


图 10-2-8

10.2.4 历史会话导出

进入[审计/历史会话]，点击<导出>导出全部 XLSX 格式历史会话记录；选中会话后点击<导出>，则导出全部选中会话。如图 10-2- 9 所示。

图 10-2- 9

10.3 系统日志

10.3.1 系统登录日志

系统登录日志记录用户登录云堡垒机的日志信息。

进入[审计/系统日志/系统登录日志]，如图 10-3-1。点击<导出>导出全部 XLSX 格式系统登录

日志；选中日志后点击<导出>，则导出全部选中日志。可用时间进行列表排序；可用登录方式、结果进行筛选。

点击搜索项，弹出搜索项下拉列表，可使用用户、来源 IP、日志内容进行搜索。点击<高级搜索>，弹出高级搜索搜索框，可用用户、来源 IP、日志内容、备注进行搜索。

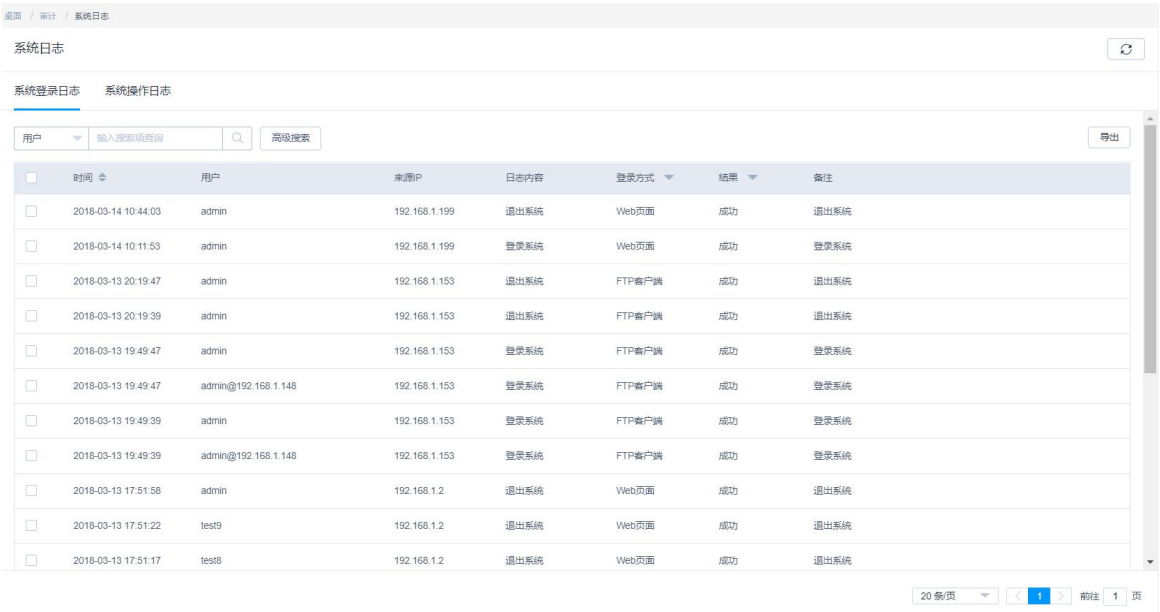


图 10-3-1

10.3.2 系统操作日志

系统操作日志记录用户在云堡垒机中的各种操作日志。

进入[审计/系统日志/系统操作日志]，如图 10-3-2。点击<导出>导出全部 XLSX 格式系统操作日志；选中日志后点击<导出>，则导出全部选中日志。可用时间进行列表排序；可用模块、结果进行筛选。

点击搜索项，弹出搜索项下拉列表，可使用用户、来源 IP、日志内容进行搜索。点击<高级搜索>，弹出高级搜索搜索框，可用用户、来源 IP、日志内容、备注进行搜索。

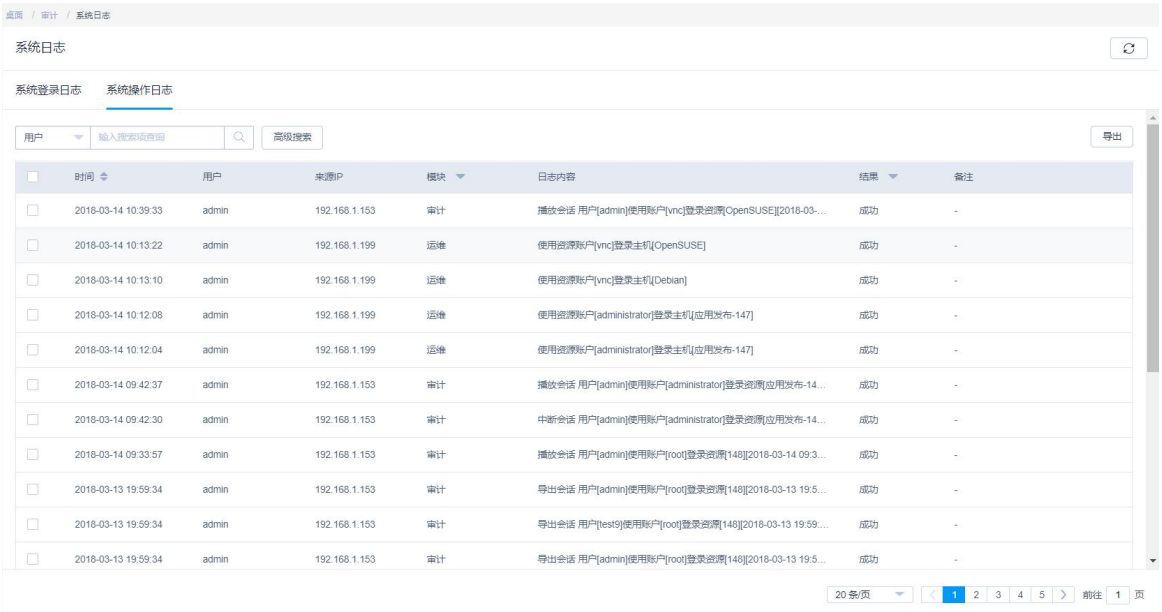


图 10-3-2

10.4 运维报表

10.4.1 运维时间分布

统计在 1 天（24 小时）范围内，用户登录资源情况分布或资源被登录分布情况。

进入[审计/运维报表/运维时间分布]，如图 10-4-1 所示。

点击<折线图>图标切换为折线图显示；点击<堆积图>图标切换为堆积图显示。点击<用户>图标切换为显示用户；点击<资源>图标切换为显示资源。报表左上方可选择对应用户或对应资源，选择后一条折线(或色块)对应一个用户(或资源)；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

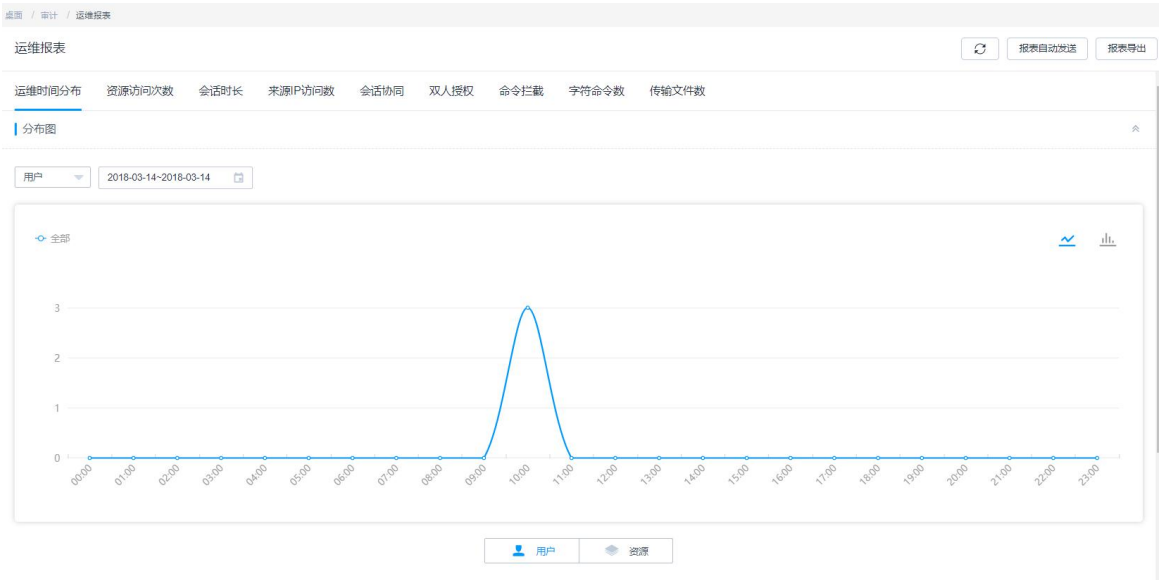


图 10-4-1

[详细数据]展示会话起止时间、用户登录名、协议类型、资源账户，如图 10-4-2 所示。

图 10-4-2

10.4.2 资源访问次数

资源访问次数统计用户(或资源)所属历史会话的数量，按会话开始时间统计。

进入[审计/运维报表/资源访问次数]，如图 10-4-3 所示。点击<折线图>图标切换为折线图显示；点击<堆积图>图标切换为堆积图显示。点击<用户>图标切换为显示用户；点击<资源>图标切换为显示资源。报表左上方可选择对应用户或对应资源，选择后一条折线(或色块)对应一个用户(或资源)；点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。当所选日志范围为 2 天到 30 天时，可选展示粒度为按天与按周；当所选日志范围为 31 天到 180 天时，可选展示粒度为按周与按月。

[详细数据]展示与运维时间分布类似。

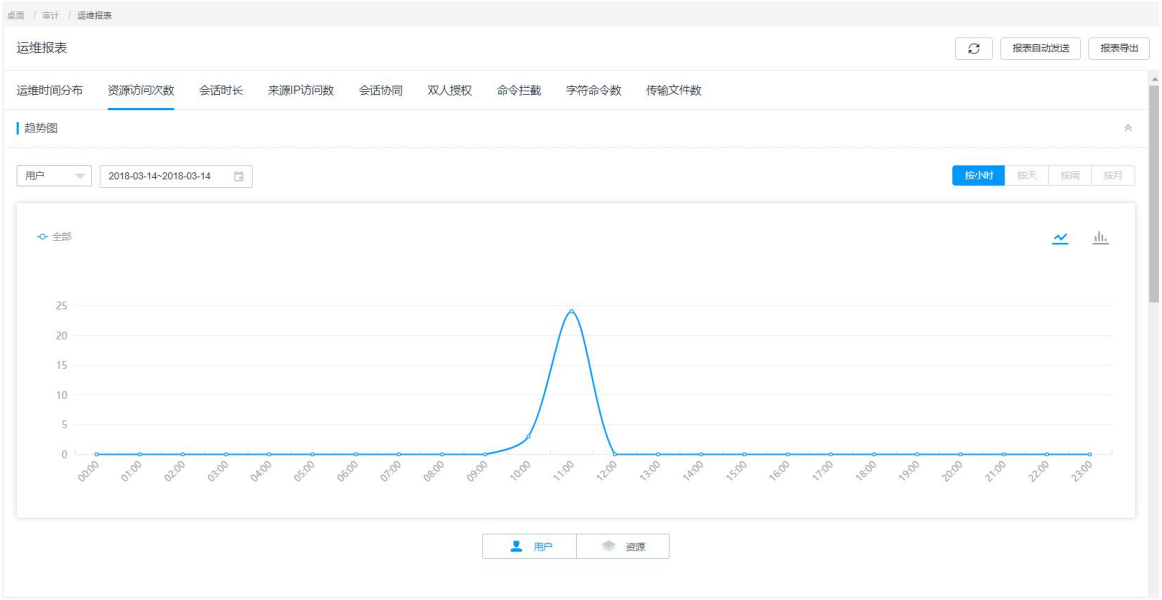


图 10-4-3

10.4.3 会话时长

会话时长统计用户(或资源)所属历史会话的会话时长。

进入[审计/运维报表/会话时长]，如图 10-4-4 所示。操作与资源访问次数类似。

[详细数据]展示会话起止时间、用户登录名、协议类型、资源账户、会话时长。

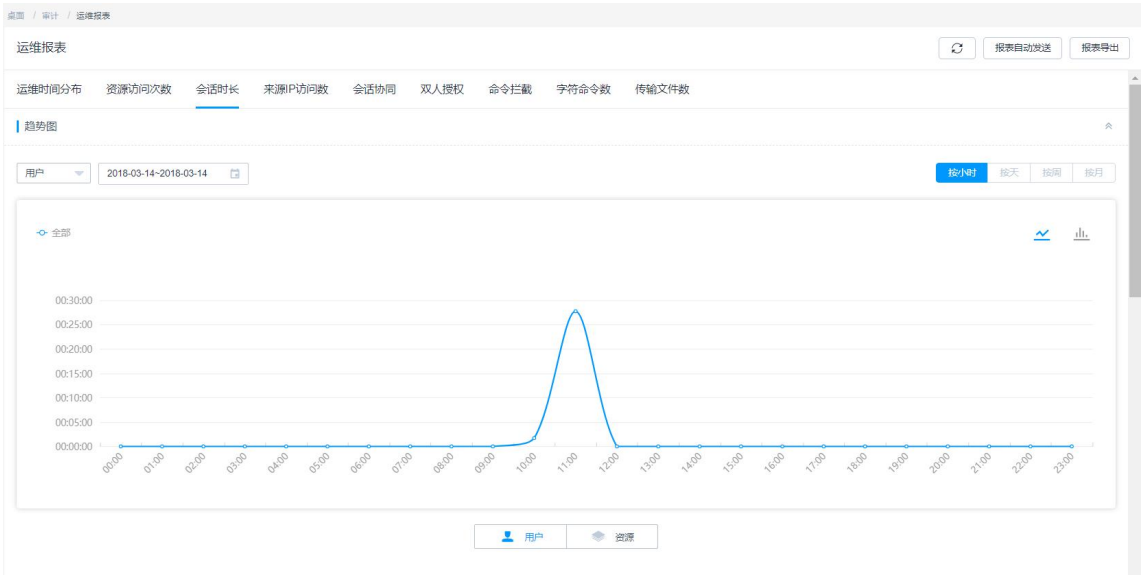


图 10-4-4

10.4.4 来源 IP 访问数

来源 IP 访问数统计用户(或资源)所属会话的不同来源 IP 数量。

进入[审计/运维报表/来源 IP 访问数]，如图 10-4-5 所示。操作与资源访问次数类似。

[详细数据]展示会话起止时间、用户登录名、资源名称、协议类型、资源账户、来源 IP。

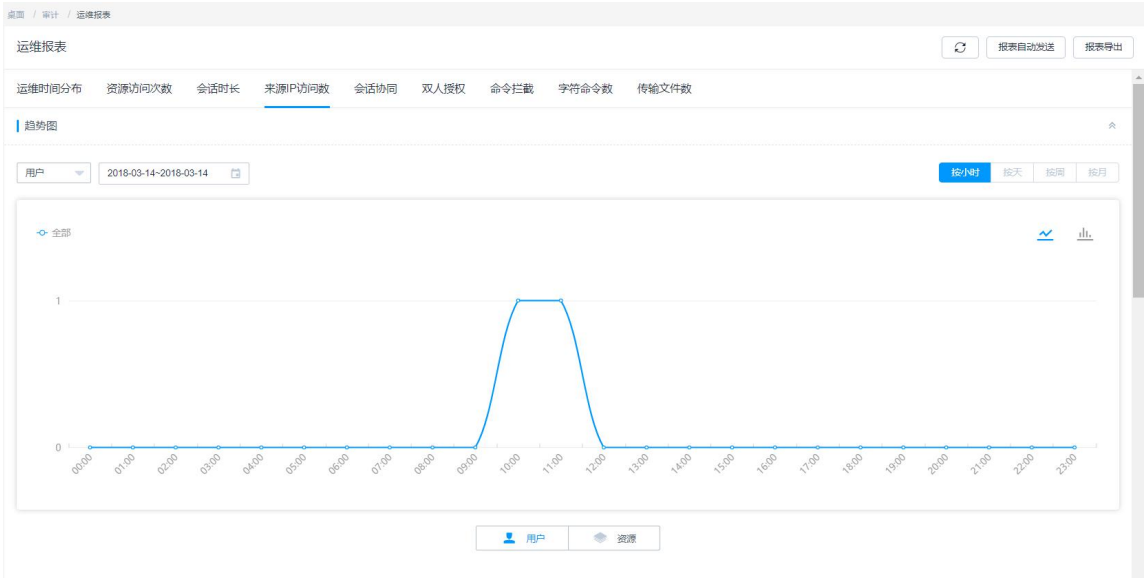


图 10-4-5

10.4.5 会话协同

会话协同统计用户(或资源)所属会话的会话协同参与用户数量。

进入[审计/运维报表/会话协同]，如图 10-4-6 所示。操作与资源访问次数类似。

[详细数据]展示会话起止时间、用户登录名、资源名称、协议类型、资源账户、协同用户。

图 10-4-6

10.4.6 双人授权

双人授权统计用户(或资源)进行双人授权的数量。

进入[审计/运维报表/双人授权]，如图 10-4-7 所示。操作与资源访问次数类似。

[详细数据]展示双人授权用户授权时间、运维用户登录名、资源名称、协议类型、资源账户、双人授权用户登录名。

图 10-4-7

10.4.7 命令拦截

命令拦截统计用户(或资源上)触发的拦截命令（断开连接、拒绝执行和动态授权）的命令数量。

进入[审计/运维报表/命令拦截]，如图 10-4-8 所示。点击<动作>图标，切换统计对象为执行动作，展示为饼图。点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏。其他操作与资源访问次数类似。

[详细数据]显示为操作指令执行时间、用户登录名、资源名称、协议类型、资源账户、操作指令、执行动作。

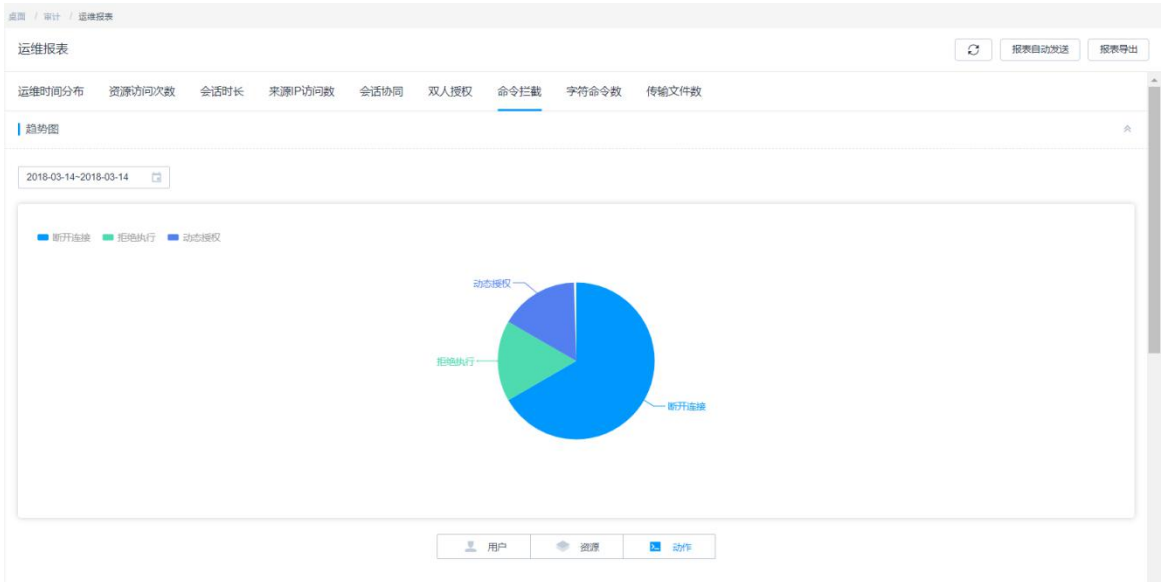


图 10-4-8

10.4.8 字符命令数

字符命令数统计用户(或资源上)执行的字符命令数量。

进入[审计/运维报表/字符命令数]，如图 10-4-9 所示。操作与资源访问次数类似。

[详细数据]中展示操作指令执行时间、用户登录名、协议类型、资源账户、操作指令。

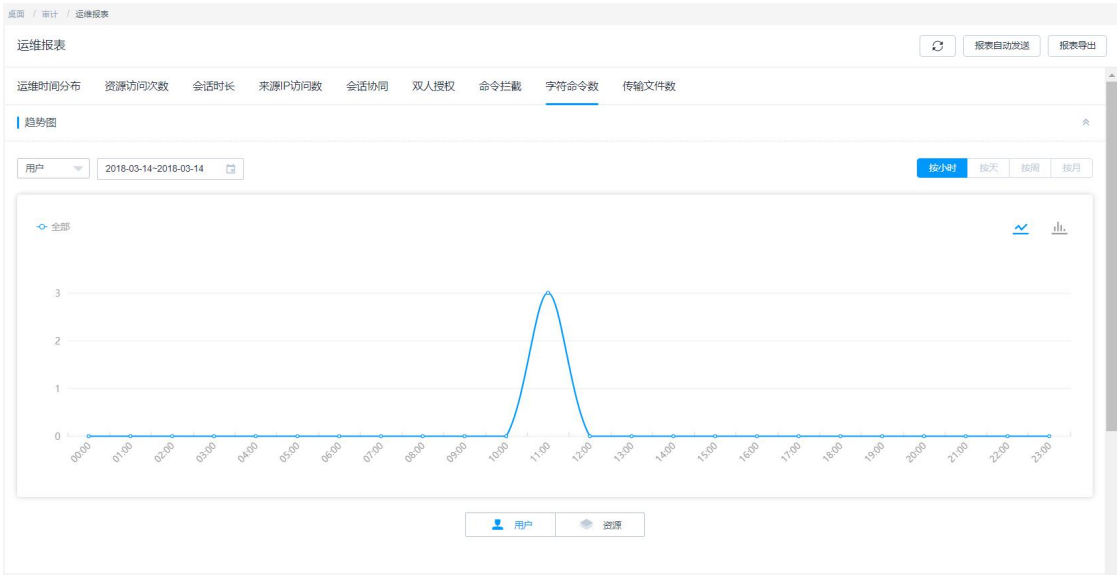


图 10-4-9

10.4.9 传输文件数

传输文件数统计用户(或资源上)上传、下载文件的数量。

进入[审计/运维报表/传输文件数]，如图 10-4-10 所示。操作与资源访问次数类似。

[详细数据]中展示文件操作时间、用户登录名、资源名称、协议类型、资源账户、操作类型、文件名称。

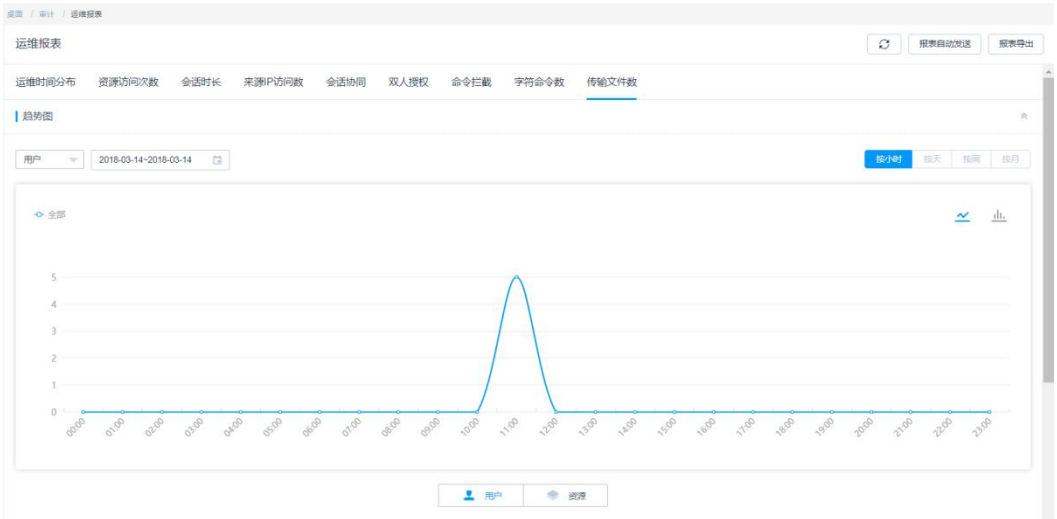


图 10-4-10

10.4.10 报表自动发送

进入[审计/运维报表]，点击<报表自动发送>，弹出报表自动发送弹窗，如图 10-4-11 所示。

默认关闭，设置定时发送后，会在所选中的发送周期中发送对应报表到当前用户邮箱（需要在系统中配置了发送邮箱）。其中，每日发送的报表中展示粒度为按小时；每周发送的报表中展示粒度为按天；每月发送的报表中展示粒度为按周。

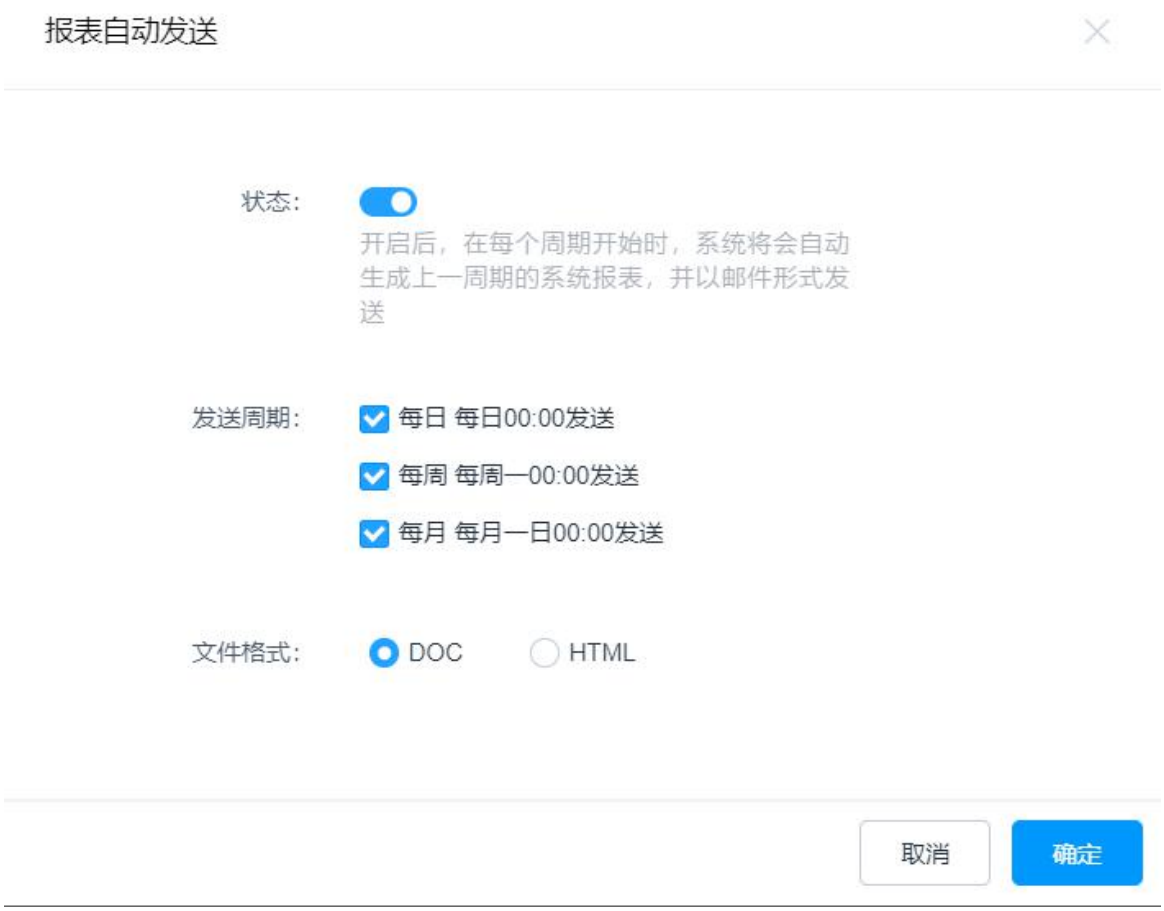


图 10-4-11

10.4.11 报表导出

进入[审计/运维报表]，点击<报表导出>，弹出报表导出弹窗，如图 10-4-12 所示。

可选展示粒度为按小时、按天、按周、按月；起止时间设置报表统计的日期范围；报表类型设置导出的报表；文件格式设置导出的报表的文件格式。

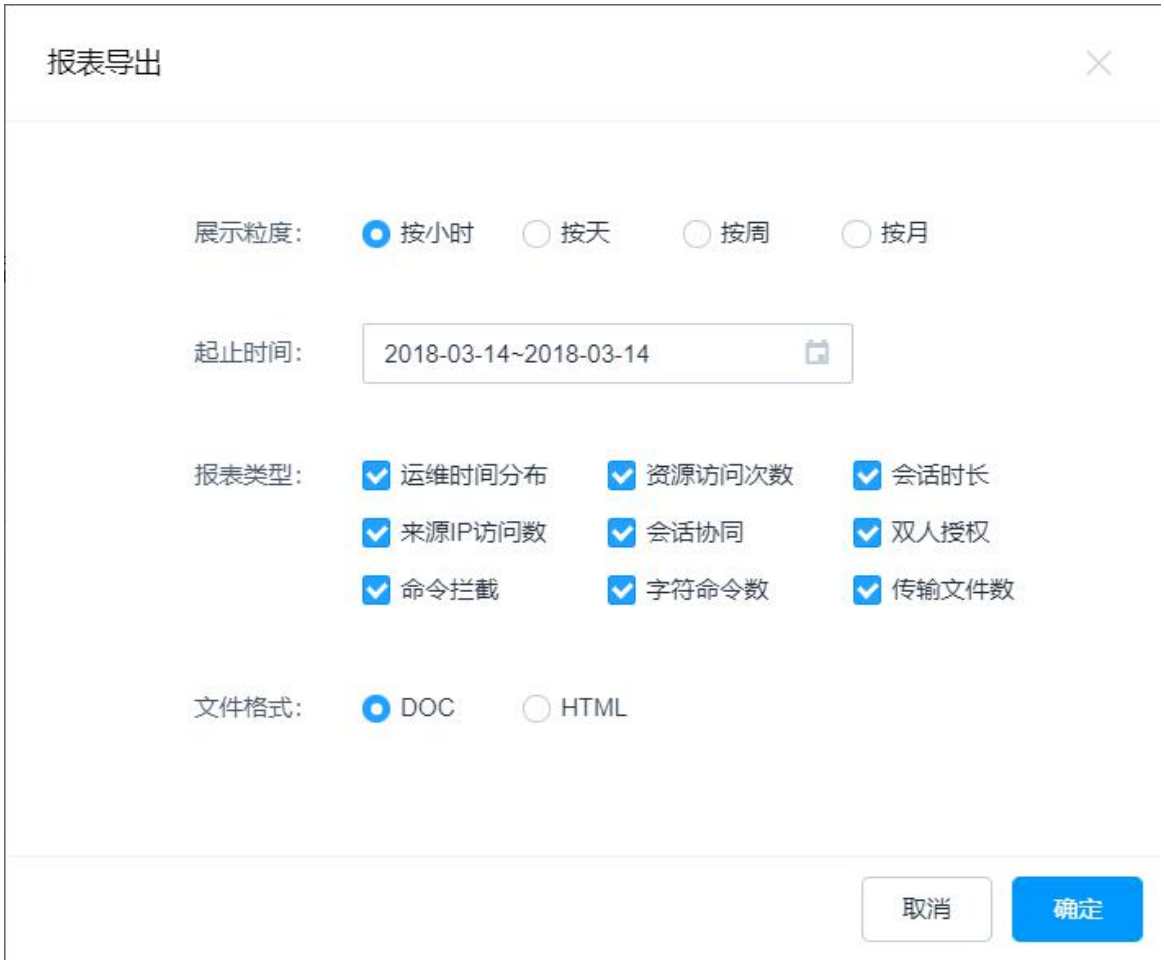


图 10-4-12

10.5 系统报表

10.5.1 用户控制

用户控制统计启用和禁用用户操作。

进入[审计/系统报表/用户控制]，如图 10-5-1 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。当所选日志范围为 2 天到 30 天时，可选展示粒度为按天与按周；当所选日志范围为 31 天到 180 天时，可选展示粒度为按周与按月。

[详细数据]显示操作时间、操作用户登录名、来源 IP、操作、操作结果。

图 10-5-1

10.5.2 用户与资源操作

用户与资源操作统计用户、用户组、主机、应用、应用服务器、资源账户、账户组的新建和删除操作。

进入[审计/系统报表/用户与资源操作]，如图 10-5-2 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

[详细数据]显示操作时间、操作用户登录名、来源 IP、操作、操作结果。

图 10-5-2

10.5.3 用户源 IP 数

用户源 IP 数统计用户登录云堡垒机的不同来源 IP 数量。

进入[审计/系统报表/用户源 IP 数]，如图 10-5-3 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击<统计用户>，选择统计用户数量，包含: Top5（默认）、Top10、Top20；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

[详细数据]显示用户登录时间、用户登录名、来源 IP、操作、操作结果。

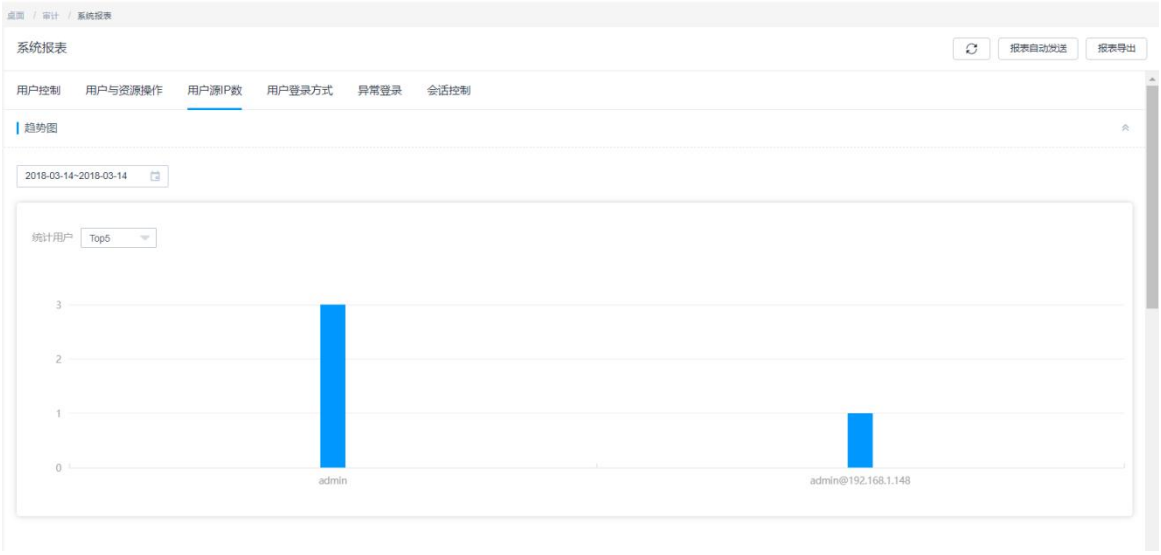


图 10-5-3

10.5.4 用户登录方式

用户登录方式统计用户登录云堡垒机的登录方式（Web 页面、SSH 客户端、FTP 客户端、SFTP 客户端）。

进入[审计/系统报表/用户登录方式]，如图 10-5-4 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

[详细数据]显示用户登录时间、用户登录名、来源 IP、操作、操作结果。

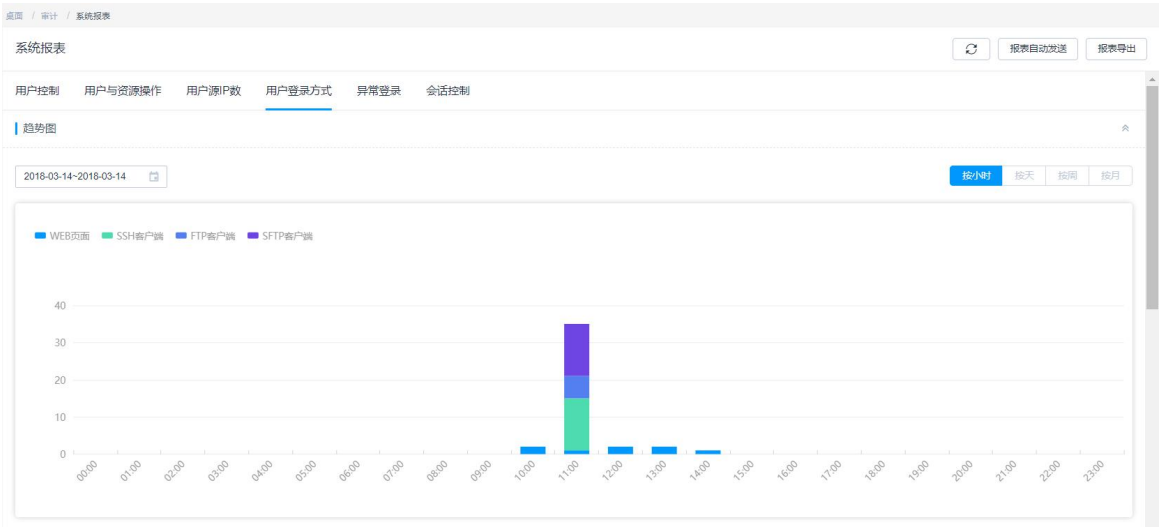


图 10-5-4

10.5.5 异常登录

异常登录统计用户的异常登录次数。

进入[审计/系统报表/异常登录]，如图 10-5-5 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击<统计用户>，选择统计用户数量，包含: Top5（默认）、Top10、Top20；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

[详细数据]显示用户登录时间、用户登录名、来源 IP、操作、操作结果。

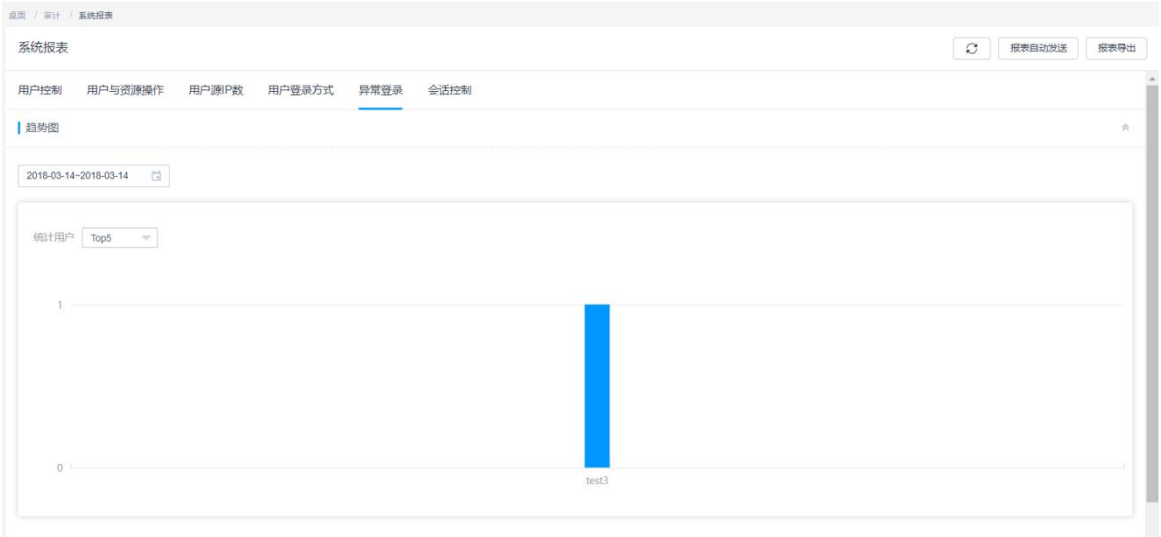


图 10-5-5

10.5.6 会话控制

会话控制统计中断和监控会话数量。

进入[审计/系统报表/会话控制]，如图 10-5-6 所示。

点击图例，切换对应报表的显示或隐藏，同时切换对应详细数据的显示或隐藏；点击[日期范围]可选择报表统计的日期范围，最大可选择 180 天。

[详细数据]显示用户登录时间、用户登录名、来源 IP、操作、操作结果。

图 10-5-6

10.5.7 报表自动发送

进入[审计/系统报表]，点击<报表自动发送>，弹出报表自动发送弹窗，如图 10-5-7 所示。操作与运维报表的报表自动发送类似。

图 10-5-7

10.5.8 报表导出

进入[审计/系统报表]，点击<报表导出>，弹出报表导出弹窗，如图 10-5-8 所示。

操作与运维报表的报表导出类似。

图 10-5-8

第十一章 工单

11.1 访问授权工单

如当用户需要使用某个未授权过的资源时，可以通过线上提交工单的方式向系统管理员和该资源所属部门的部门经理提交申请，申请被批准后，该用户即可获得该资源的授权，而当管理员撤销授权或工单失效时间到期后，则用户失去该资源的授权。如需再次使用，可再提交工单申请。

11.1.1 访问授权工单新建

用户点击访问授权工单列表页面右上方的新建按钮，选择自己要运维的时间，对一些自己需要的功能进行勾选，完成之后点击下一步，选择自己要运维的资源账户，如果需要再点击确定的时候立即提交，则勾选上立即提交按钮，如果不需要，则不勾选立即提交按钮。点击确定，工单保存成功或已经提交，如图 11-1-1、11-1-2、11-1-3 所示。

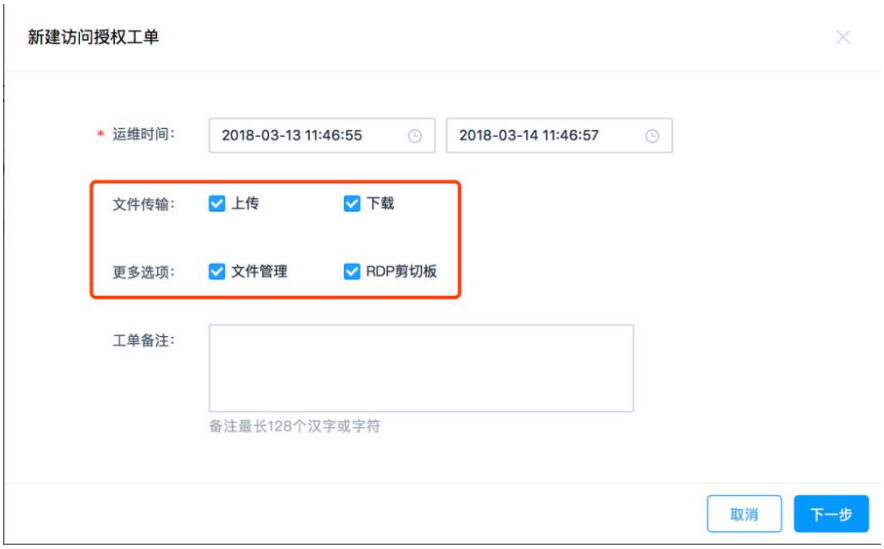


图 11-1-1

图 11-1-2

图 11-1-3

11.1.2 访问授权工单详情

点击访问授权工单的工单号或后方的管理按钮，即可进入工单详情页面。对于未提交的工单或已经被管理员驳回的工单，可以对其进行修改（基本信息、资源账户）并点击右上方的提交的按钮提交该工单；对于已经提交的工单，可以点击工单详情页面右上方的撤回按钮，撤回工单后，依旧可以对工单进行修改（基本信息、资源账户）并提交，如图 11-1-4、11-1-5、11-1-6、11-1-7 所示。

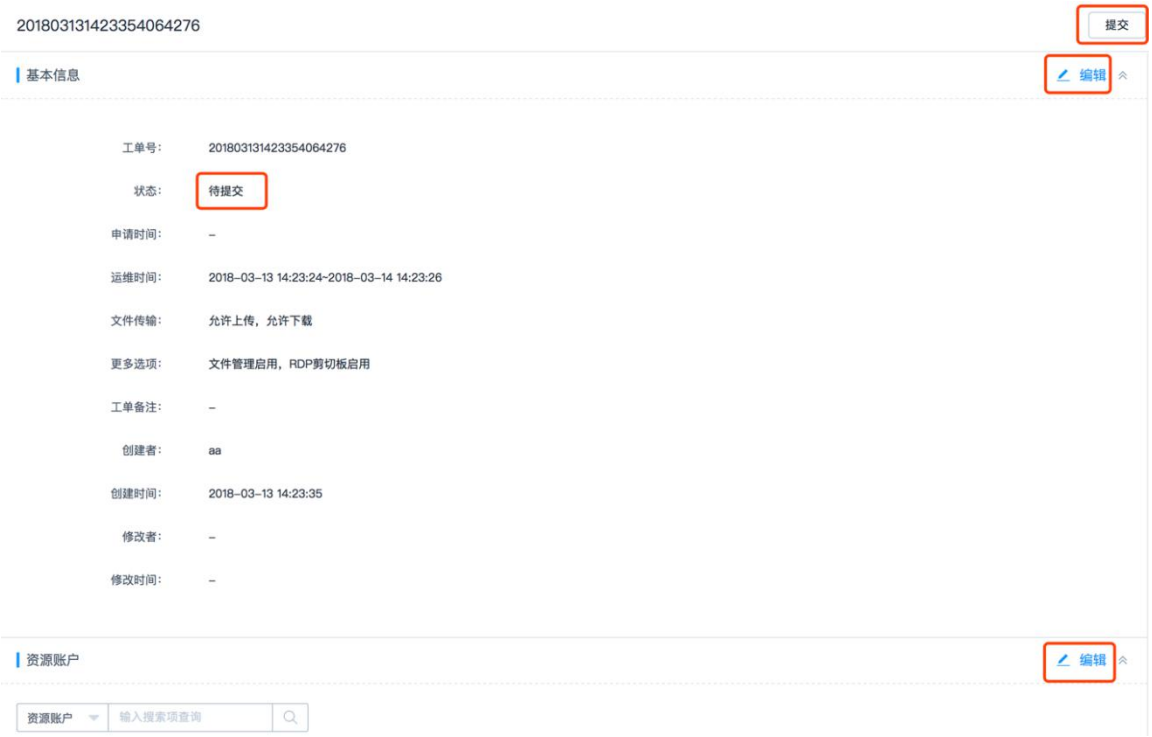

20180313142335406427 6
提交
基本信息
编辑
工单号:
20180313142335406427 6
状态:
待提交
申请时间:
-
运维时间:
2018-03-13 14:23:24~2018-03-14 14:23:26
文件传输:
允许上传，允许下载
更多选项:
文件管理启用，RDP剪切板启用
工单备注:
-
创建者:
aa
创建时间:
2018-03-13 14:23:35
修改者:
-
修改时间:
-
资源账户
编辑
资源账户
输入搜索项查询

图 11-1- 4


20180313114819620717 1
提交
基本信息
编辑
工单号:
20180313114819620717 1
状态:
已驳回
申请时间:
2018-03-13 14:22:25
运维时间:
2018-03-13 11:46:55~2018-03-14 11:46:57
文件传输:
允许上传，允许下载
更多选项:
文件管理启用，RDP剪切板启用
工单备注:
-
创建者:
aa
创建时间:
2018-03-13 11:48:19
修改者:
admin
修改时间:
2018-03-13 14:22:40
资源账户
编辑
资源账户
输入搜索项查询

图 11-1- 5

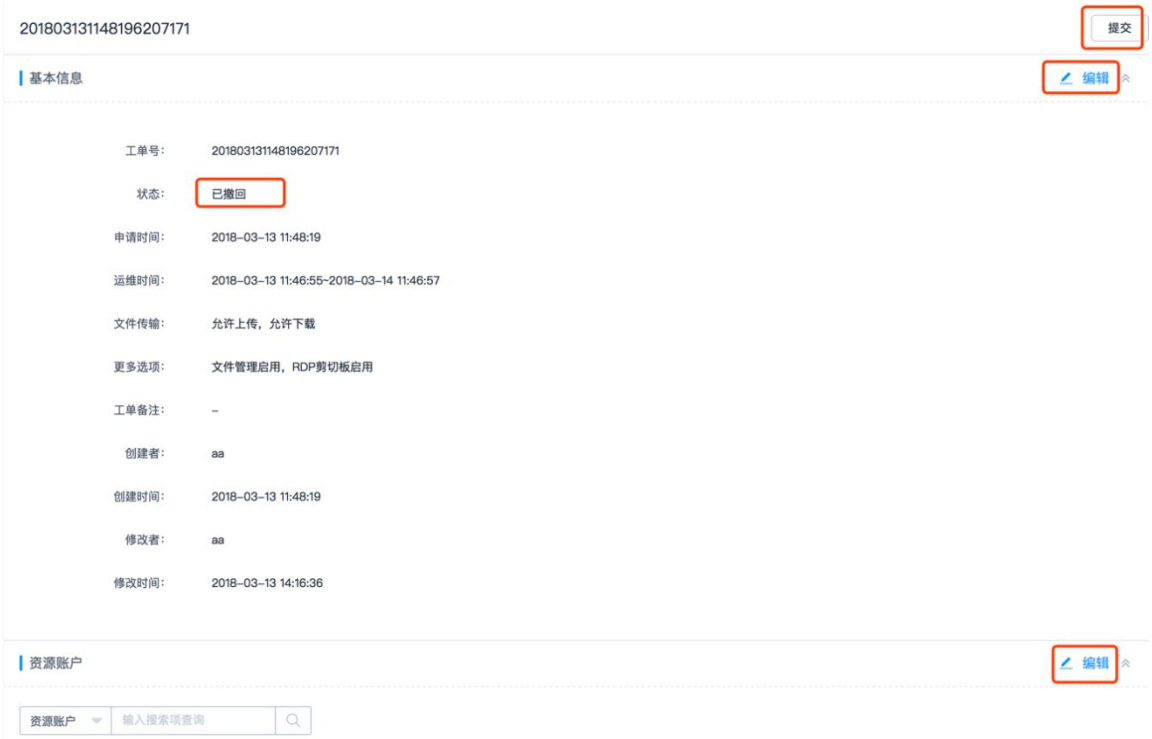


图 11-1-6

图 11-1-7

11.1.3 访问授权工单修改

用户提交工单申请后，系统管理员和申请资源所属部门的部门经理在工单列表中可以查看到待审批的工单，可以对工单申请进行批准或驳回操作。在工单被批准后管理员还可以执行撤

销操作来收回资源的授权；另外如果工单被驳回，用户可以修改后再次发出申请，如图 11-1-8、11-1-9 所示。

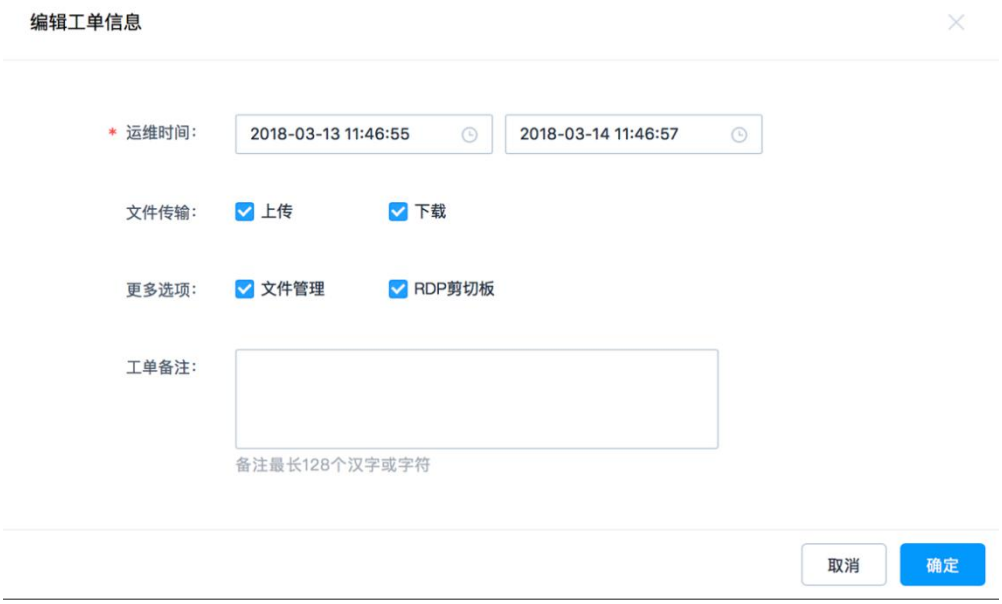


图 11-1-8

图 11-1-9

11.2 命令授权工单

11.2.1 命令授权工单触发生成

系统管理员或部门管理员可以为用户配置命令控制策略，当用户登录该资源并执行了命令控制策略中的命令，命令授权工单列表中就会自动生成一个命令授权工单，如果在系统配置中命令授权工单配置为自动提交，则触发生成的命令授权工单会自动提交到系统管理员或对该资源有管理权限和工单审批模块权限的用户处；如果系统配置中命令授权工单配置为手动提交，则触发生成的命令授权工单需要用户手动点击提交，如图 11-2-1、11-2-2、11-2-3 所示。

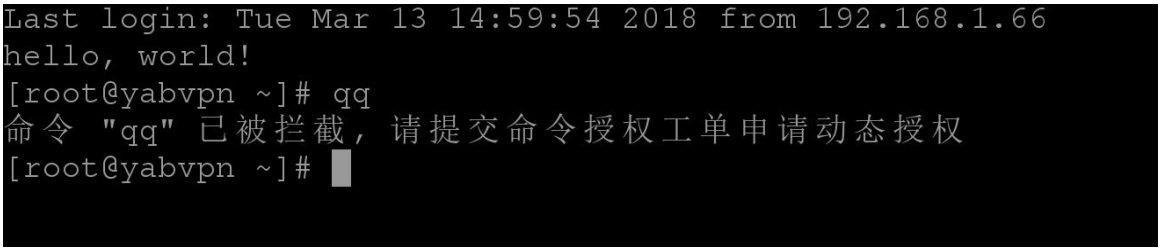


图 11-2-1

图 11-2-2

图 11-2-3

11.2.2 命令授权工单详情

点击命令授权工单的工单号或后方的管理按钮，即可进入工单详情页面。对于未提交的工单或已经被管理员驳回的工单，可以对其基本信息进行修改，并点击右上方的提交的按钮提交该工单；对于已经提交的工单，可以点击工单详情页面右上方的撤回按钮，撤回工单后，依旧可以对工单基本信息进行修改并提交，如图 11-2-4、11-2-5、11-2-6、11-2-7 所示。

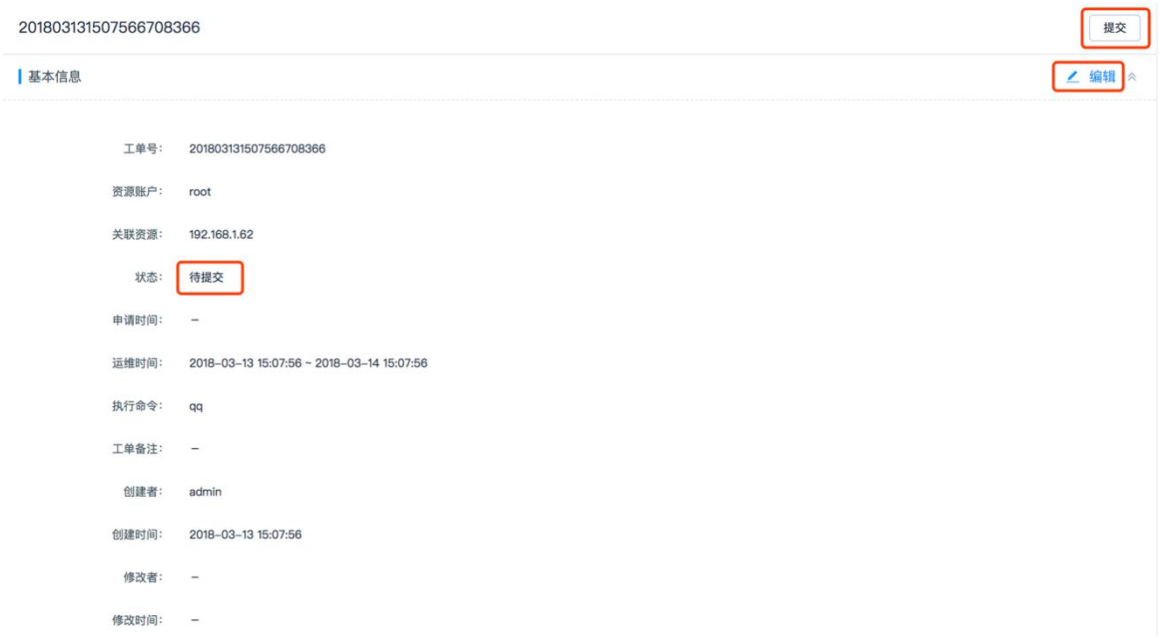

20180313150756670836 6
提交
基本信息
编辑
工单号：
20180313150756670836 6
资源账户：
root
关联资源：
192.168.1.62
状态：
待提交
申请时间：
–
运维时间：
2018-03-13 15:07:56 ~ 2018-03-14 15:07:56
执行命令：
qq
工单备注：
–
创建者：
admin
创建时间：
2018-03-13 15:07:56
修改者：
–
修改时间：
–

图 11-2-4

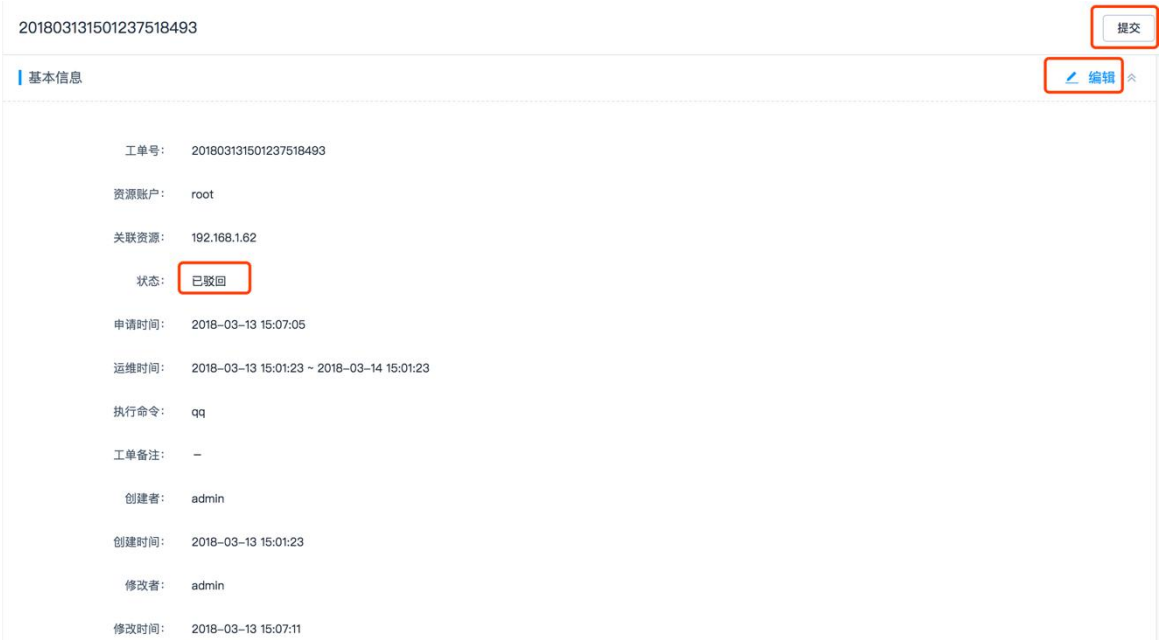

20180313150123751849 3
提交
基本信息
编辑
工单号：
20180313150123751849 3
资源账户：
root
关联资源：
192.168.1.62
状态：
已驳回
申请时间：
2018-03-13 15:07:05
运维时间：
2018-03-13 15:01:23 ~ 2018-03-14 15:01:23
执行命令：
qq
工单备注：
–
创建者：
admin
创建时间：
2018-03-13 15:01:23
修改者：
admin
修改时间：
2018-03-13 15:07:11

图 11-2-5

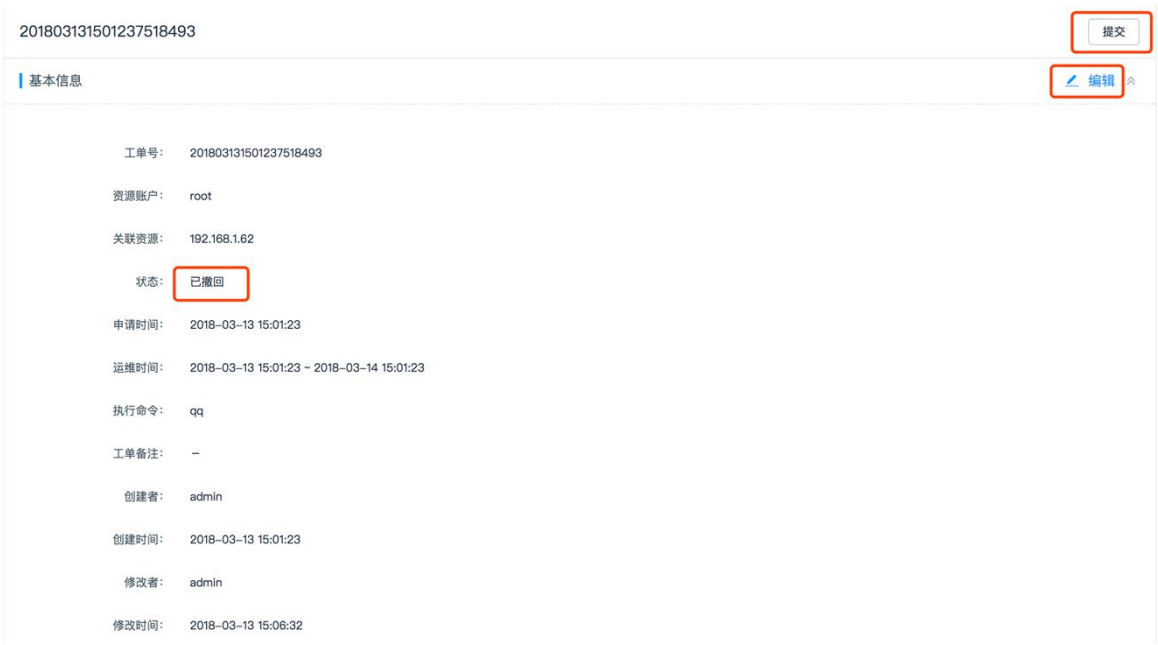


图 11-2-6

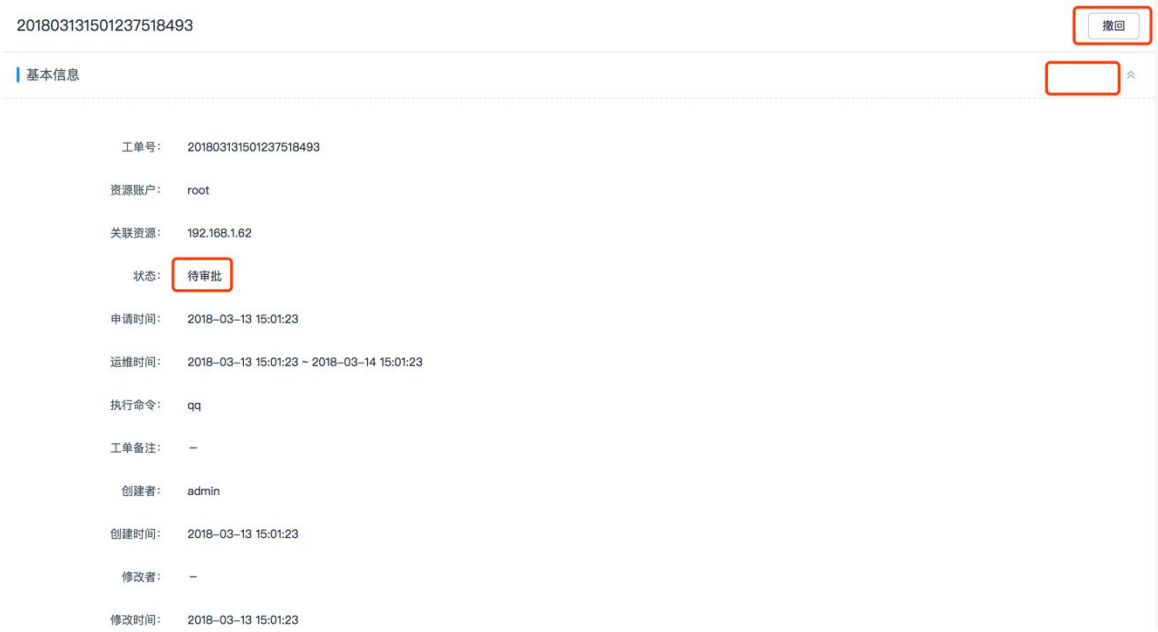


图 11-2-7

11.2.3 命令授权工单修改

用户提交工单申请后，系统管理员和申请资源所属部门的部门经理在工单列表中可以查看到待审批的工单，可以对工单申请进行批准或驳回操作。在工单被批准后管理员还可以执行撤销操作来收回资源的授权；另外如果工单被驳回，用户可以修改后再次发出申请，如图 11-2-8 所示。

图 11-2-8

11.3 工单审批

用户提交工单申请后，系统管理员和申请资源所属部门的部门管理员在工单审批列表中可以查看到待审批的工单（对于命令授权工单来说，提交之后系统管理员和对该资源有管理权限并有工单审批模块权限的用户会在工单审批列表中看到），可以对工单申请进行批准或驳回操作。在工单被批准后管理员还可以执行撤销操作来收回资源的授权；另外如果工单被驳回，用户可以修改后再次发出申请，如图 11-3-1 所示。

图 11-3-1

第十二章 系统

12.1 系统配置

12.1.1 安全配置

进入[系统/系统配置/安全配置]，显示当前安全配置信息，一共包含 5 种配置，分别是用户锁定配置、密码策略配置、Web 登录配置、Web 证书配置、SSH 登录配置，其中“用户锁定配置”的锁定方式是指输错密码达到尝试密码次数被锁定的方式，有账户和来源 IP 两种方式；尝试密码次数是指可以输错密码的次数，有效值 0-999，如果设定为 0，则不锁定账户/来源 IP，默认值 5；锁定时长是指用户输错密码被锁定的时间值，有效值 0-10080，如果设置为 0，则锁定账户/来源 IP 直到管理员解除；重置计数器时长指的是登录尝试密码失败后，将登录尝试失败计数器重置为 0 次所需要的时间，有效值 1-10080，默认值 5，如图 12-1-1 所示。

图 12-1- 1

“密码策略配置”的密码强度校验是指是否强制用户使用强密码；密码相同校验是指修改的密码不能跟前 N 次相同（用户首次登录的密码不记录在内），有效值 1-30，默认 5；新用户强制改密是指是否强制新用户首次登录时改密；密码修改周期指云堡垒机账号密码修改周期，当达到修改周期时，登录后将自动弹出修改密码框，有效值 0-90，如果设置为 0，则密码永远不过期，默认值 30，如图 12-1-2 所示。

图 12-1- 2

“Web 登录配置”的登录超时指在 web 页面无操作，再次操作时会退出重新登录的时间，有效值 1-43200，默认 30；短信验证码过期时长指通过云堡垒机发出的短信验证码的过期时间，有效值 15-3600，如果设置为 0，则不过期，默认 60；图形验证码可配置为启用、禁用、自动，当配置为启用时，登录页面上的图形验证码会一直显示，图形验证码过期时长是指出现的图形验证码的过期时间，有效值 15-3600，如果设置为 0，则不过期，默认 60；当配置为禁用时，登录不管输错多少次密码，图形验证码都不会出现；当配置为自动时，输错密码达到尝试次数，图形验证码就会出现，登录尝试次数的有效值为 1-30，默认 3，如图 12-1-3 所示。

图 12-1- 3

“Web 证书配置”需要上传符合格式要求的.jks 文件，并且还要输入 keystore 密码，配置完成后，在页面可以查看到证书的相关信息，重启系统即可生效，如图 12-1-4、12-1-5 所示。

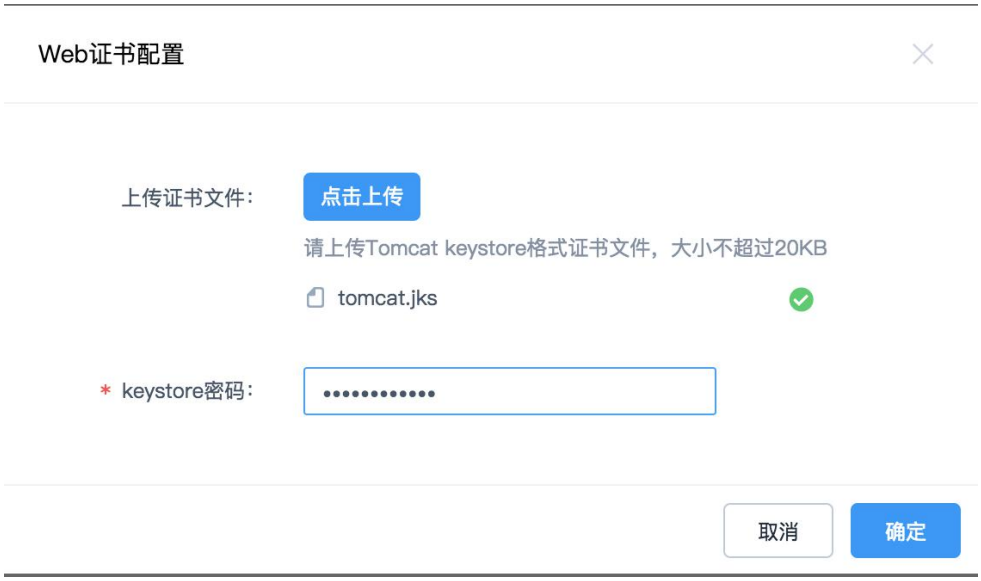


图 12-1-4

图 12-1-5

“SSH 登录配置”的登录超时指登录成功后在 SSH 客户端无操作退出登录的时间，有效值 1-43200，默认 30；公钥登录指用户使用 SSH 客户端登录云堡垒机时，如果添加了 SSH 公钥，可以免密登录；密码登录指用户使用 SSH 客户端登录云堡垒机时，只能输入密码登录；如果两种方式都打开了，则优先使用公钥登录方式，如图 12-1-6 所示。

图 12-1- 6

12.1.2 网络配置

进入[系统/系统配置/网络配置]，显示当前网络配置信息，一共包含 4 种配置，分别是网络接口列表、DNS 配置、静态路由配置、Open VPN 配置，其中“网络接口列表”可以添加、编辑、删除当前机器的相关网络接口，为后续相关操作用到网络接口做准备（删除不会删除机器中的相关接口,默认显示的网络接口不可以删除），如图 12-1-7 所示。

图 12-1- 7

“DNS 配置”可以修改当前机器的首选 DNS 和备用 DNS，当然一定要时有用的，否则解析不了，如图 12-1-8 所示。

图 12-1- 8

“静态路由配置”可以为当前机器添加静态路由，使当前机器可以访问其他网段的机器，如图 12-1-9 所示。

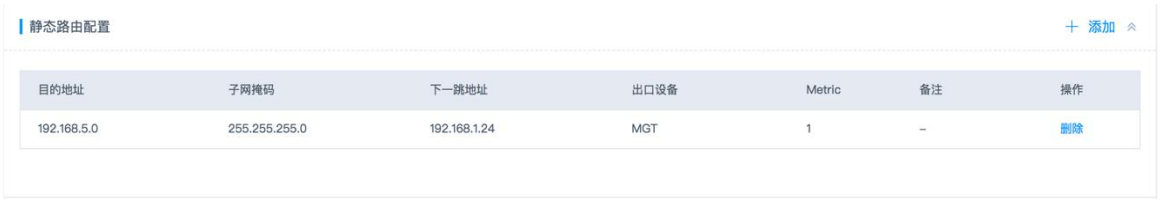


图 12-1-9

云堡垒机支持作为客户端连接到 OpenVPN 服务器，从而实现操作运维 VPN 内部资源的目的。OpenVPN 设置中，点击开启并选择与本地 OpenVPN 服务器相同配置的协议、IP、端口、是否压缩、验证 nsCertType 等信息，并上传 OpenVPN 服务器生成的 CA 证书，客户端证书和客户端私钥，点击<确定>即可将云堡垒机连接至 OpenVPN 服务器，在云堡垒机中添加 VPN 内部资源并授权后，用户即可对 VPN 内部资源进行登录、运维、审计等操作，如图 12-1-10 所示。

图 12-1-10

12.1.3 HA 配置

进入[系统/系统配置/HA 配置]页面，在双机热备配置中可以查看当前 HA 状态，默认为禁用。开启双机热备需要两台云堡垒机，点击<启用>按钮后，选择主节点或从节点（必须要先配置主节点），在备节点 IP 栏内输入作为备节点云堡垒机的 IP，在浮动 IP 一栏输入未被使用的 IP 地址（注意：浮动 IP 地址后面需要加上掩码），选择要作为 HA 接口使用的网络接口，点击确

定后重启主节点（未重启时，当前运行状态还是会显示单机），等重启完毕后服务 IP 备检测到的时候，当前运行状态就处于在线状态，服务 IP 即可登录。此时主节点断开从节点也可提供服务。（注意：配置 HA 并不一定非得要两台干净的云堡垒机，主节点配置好后，配置备节点，不管备节点有没有数据，都会被清空，同步主节点的数据）

关闭双机热备直接在主从节点的 HA 状态后面点击禁用即可，保存设置后重启两台云堡垒机，重启完成后双机热备即设为关闭状态，如图 12-1-11 所示。

图 12-1- 11

12.1.4 端口配置

进入[系统/系统配置/端口配置]，显示当前端口配置信息，一共包含 3 种配置，分别是运维端口配置、Web 控制台端口配置、SSH 控制台端口配置，其中“运维端口配置”主要是针对 SSH/SFTP、FTP 类型资源端口进行修改，包括通过 SSH 客户端登录云堡垒机的端口，配置好后点击<确定>，系统自动重启，重启完成后登录 SSH/SFTP、FTP 类型资源和通过 SSH 客户端登录云堡垒机时，都需要使用修改过的端口，有效值 1-65535 之间的有效数字，如图 12-1-12 所示。

图 12-1-12

“Web 控制台端口配置”针对的是登录 web 页面云堡垒机的端口配置，配置好后点击<确定>，系统将会自动重启，重启完成后，再次登录 web 页面的云堡垒机时，需要使用修改过的端口，有效值 1-65535 之间的有效数字，如图 12-1-13 所示。

图 12-1-13

“SSH 控制台端口配置”针对的是登录 SSH 管理控制台的端口配置，配置好后点击<确定>，系统将会自动重启，重启完成后，再次登录 SSH 管理控制台时，需要使用修改过的端口，有效值 1-65535 之间的有效数字，如图 12-1-14 所示。

图 12-1-14

12.1.5 外发配置

进入[系统/系统配置/外发设置]，显示当前外发配置信息，一共包含 3 中配置，分别是邮件配置、短信网关配置、SNMP Agent 配置，其中“邮件配置”可以配置邮件服务器，为改密计划功能和消息告警提供邮件发送服务。用户可根据需求设置私有邮箱服务器或是公共邮箱服务器，并可测试所填写服务器信息是否有效，如图 12-1-15 所示。

图 12-1-15

“短信网关配置”包含两种，一种是云堡垒机内置的短信网关，由云堡垒机本身的短信网关来提供短信服务；另一种是自定义短信网关，输入正确的 URL 地址和 API 参数后，还可测试所填写服务器信息是否有效，如图 12-1-16、12-1-17 所示。

图 12-1-16

图 12-1-17

“SNMP Agent 配置”有两种配置方式，V2 和 V3 方式，输入正确的相关信息点击<确定>（注：类型为 V3 时，认证密码和隐私秘密为必填项），配置完成后用户可以通过 SNMP 客户端或 mac 终端执行相关命令获取到云堡垒机系统的某些信息（可以点击 OID 信息表获取相关信息的 OID），如图 12-1-18、12-1-19、12-1-20 所示。

图 12-1-18

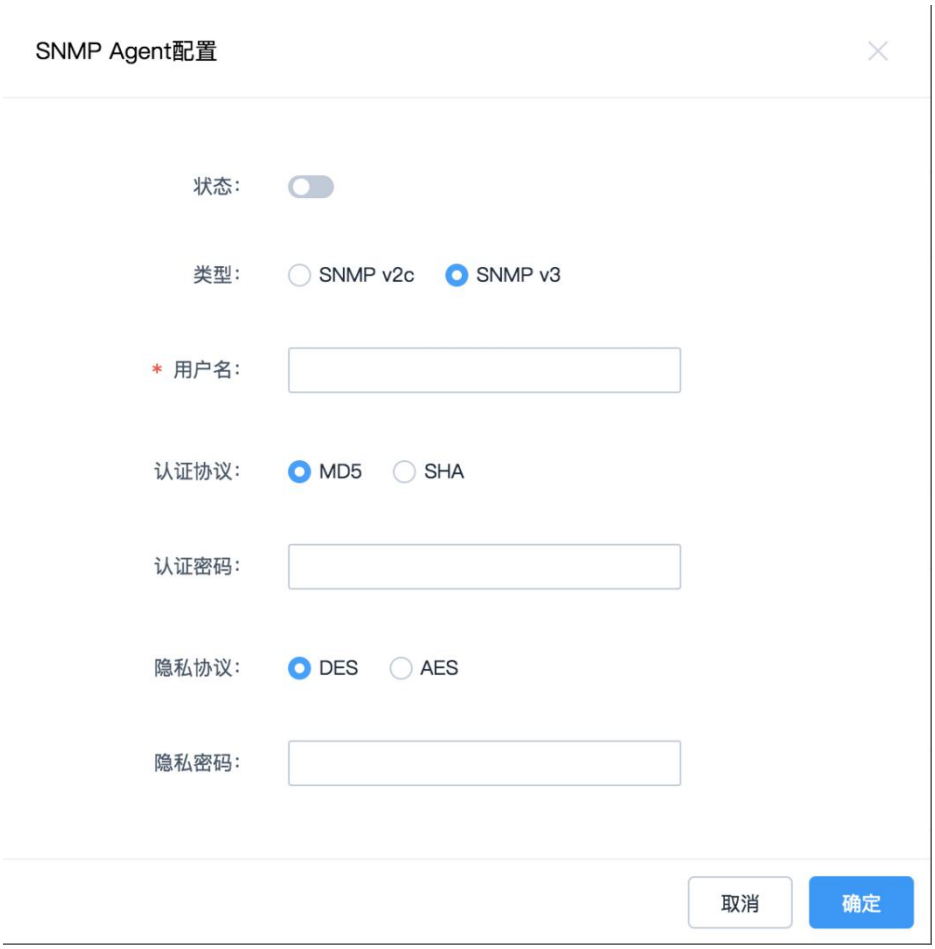


图 12-1-19

图 12-1-20

12.1.6 认证配置

进入[系统/系统配置/认证配置]，点击<+添加>，如图 12-1-21 所示。

图 12-1- 21

进入 AD 域新建页面，填写 AD 域服务器的名称、IP、域、baseDN 等信息，部门过滤和用户过滤的内容为默认，可以不做修改。如图 12-1-22 所示。

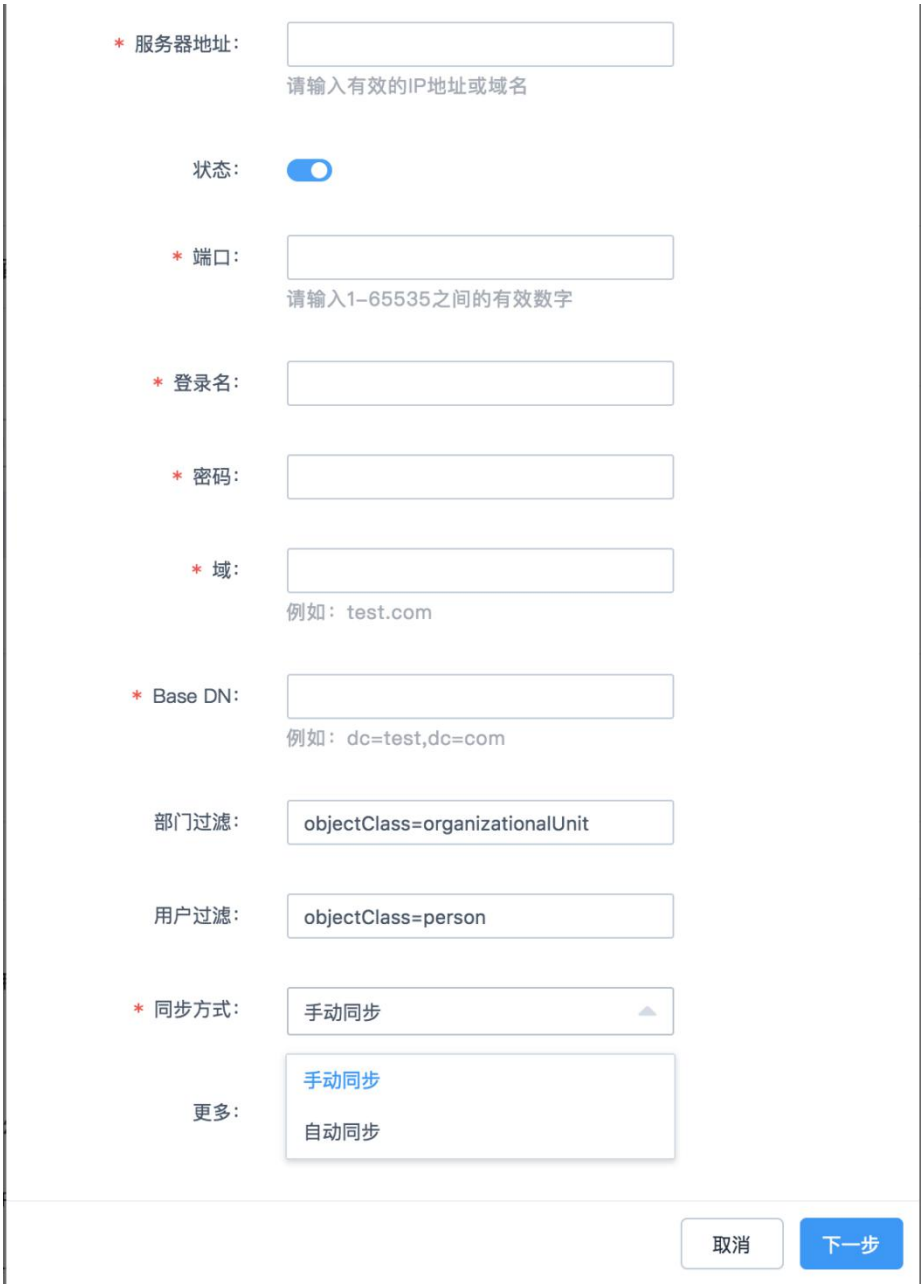


图 12-1- 22

AD 域服务器的同步方式分为“手动同步”和“自动同步”两种，选择自动同步时，需要填写同步时间、同步周期、结束时间，当时间到达同步时间，AD 域会立即开始同步，同步结束后，达到同步周期又会立即开时同步；如果勾选更多选项中的覆盖已有用户或创建新部门，则在导入时，系统将会覆盖用户列表中已有的跟 AD 域用户同名的用户，在部门列表中会创建新的导入源部门，点击<下一步>，选择导入源和目的部门，点击<确定>，AD 域完成配置，如图 12-1-23 所示。

图 12-1- 23

同步开始后状态显示为“同步中”，同时可以显示已同步的用户数。可以在云堡垒机认证配置页面点击<停止同步>来终止同步，终止同步后状态显示为“已停止”，如图 12-1-24 所示。

图 12-1- 24

删除 AD 域后，用户列表中的 AD 域用户也会同步的被删除，但是已经创建的导入源部门不会被删除；如果删除的是部门，系统会同步的删除该部门及其子部门下的所有 AD 域用户等资源。

“RADIUS 认证配置”，按照第三方 RADIUS 服务器的配置信息在 RADIUS 服务器设置页面填写正确的 IP、端口、共享秘钥等信息，并可对 RADIUS 用户进行有效性测试。如图 12-1-25 所示。

图 12-1- 25

用户通过有效性测试后，可通过手工或文件导入的方式添加 RADIUS 用户，开启 RADIUS 认证开关后，则用户在登录时需要输入与 RADIUS 服务器端一致的密码才能成功登录。其他本地认证方式的用户仍然可以通过输入本地密码完成云堡垒机登录。

12.1.7 工单配置

进入[系统/系统配置/工单配置]页面，如图 12-1-26 所示。

图 12-1- 26

在基本模式-访问授权工单申请范围中设置用户在工单申请时可以查看的资源，分为全部、本部门、本部门及下级部门，默认申请范围为本部门，此时用户在工单申请时只能查看到自己部门下面的资源；在基本模式-命令授权工单提交方式中设置命令授权工单触发生成后是自动提交或手动提交，默认是手动提交；改变访问授权工单申请范围和命令授权工单提交方式后，点击<确定>可以完成更改保存，如图 12-1-27 所示。

图 12-1- 27

在高级模式中配置用户池，用户池下部门的角色用户可以申请资源池下资源部门的资源，只针对于访问授权工单，如果用户的角色未选择，则用户池下的部门所有角色用户可以申请资源池下资源部门的所有资源，如图 12-1-28、12-1-29 所示。

图 12-1- 28

图 12-1- 29

12.1.8 告警配置

进入[系统/系统配置/告警配置]，如图 12-1-30 所示。

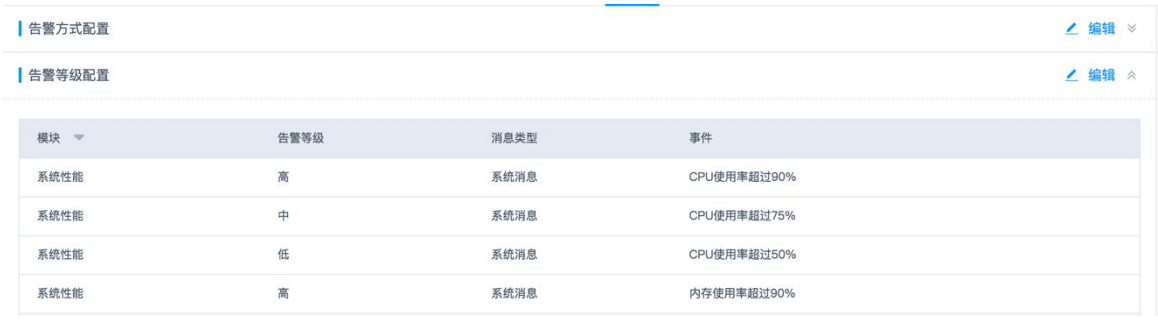


图 12-1- 30

“告警方式配置”可以修改系统消息、业务消息、任务消息、命令告警、工单消息各级别

消息是否告警和告警方式，包括消息中心、邮件通知、短信通知，默认低级消息不告警；中级消息告警，只记录消息中心；高级消息告警，记录消息中心和发送邮件，如图 12-1-31 所示。

图 12-1-31

“告警等级配置”可以修改各模块各类型消息的告警级别，如图 12-1-32 所示。

图 12-1-32

12.1.9 系统风格

进入[系统/系统配置/系统风格]，如图 12-1-33 所示。

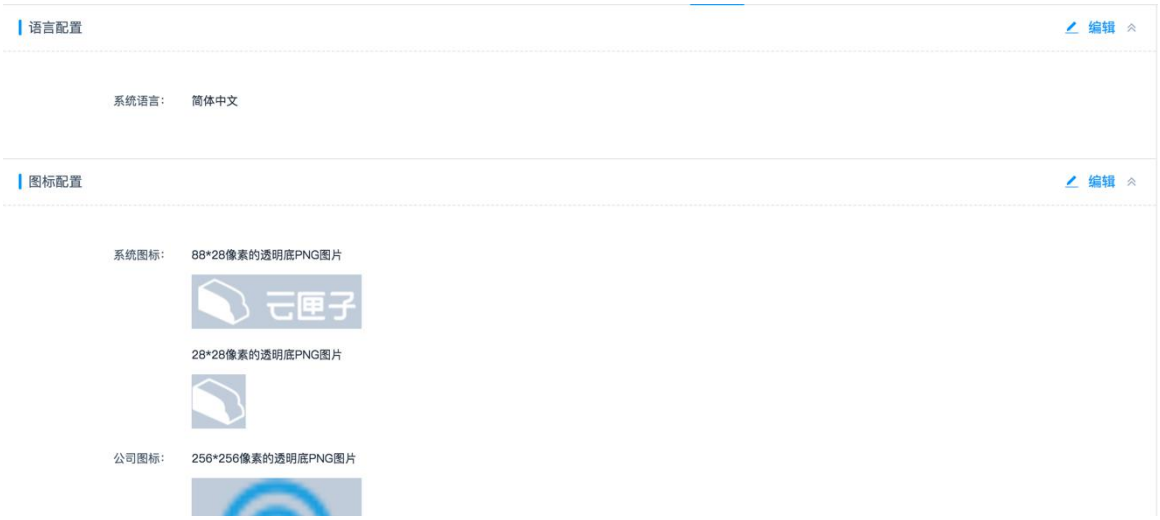


图 12-1-33

“语言配置”可以修改整个云堡垒机系统的语言配置，有中文和英文两个选择；在登录页面的右上方也有修改语言配置的选项（注：此处设置的语言，将影响浏览器首次登录云堡垒机时的默认语言配置，而在登录页面配置的语言会影响每次在该浏览器登录云堡垒机时的语言配置），如图 12-1-34、12-1-35 所示。

图 12-1-34

图 12-1-35

点击上传大的系统图标可以自定义系统登录页和系统顶部左栏的图片，上传小的系统图标可以自定义系统左侧栏收缩起来时的图片，点击上传公司图标可以自定义浏览器显示的图标，点击重置所有图片将所有图片恢复到初始图片，如图 12-1-36 所示。

图 12-1- 36

12.2 数据维护

12.2.1 存储配置

进入[系统/数据维护/存储配置]，如图 12-2-1 所示。

图 12-2-1

“存储概览”主要展示当前云堡垒机系统的系统分区和数据分区的空间使用量，如图 12-2-2 所示。

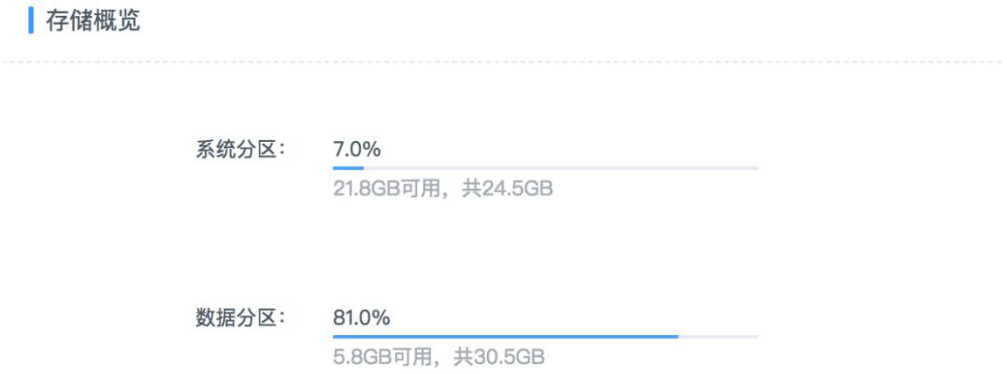


图 12-2-2

“自动删除”是指是否开启自动清除磁盘；“自动删除（天）前的数据”是指当系统数据自创建后超过一定时长时会被自动清除，有效值 1-10000 天，默认值 180 天；“空间满时自动覆盖最早的数据”可以选择开启或关闭来确定是否在磁盘使用量超过 90%的时候自动进行数据清理，检查空间剩余的间隔为 30 分钟。清理后的空间达到阈值 90%以下即停止删除）。删除的数据默认为 180 天之前的数据，如果 180 天前的数据删除之后，使用率还是高于 90%，则一天一天往前删除，直到使用率低于 90%，不会删除当天的数据，如图 12-2-3 所示。

图 12-2-3

“手动删除”可删除指定日期前的数据，如图 12-2-4 所示。

图 12-2-4

12.2.2 日志备份

进入[系统/数据维护/日志备份]，如图 12-2-5 所示。

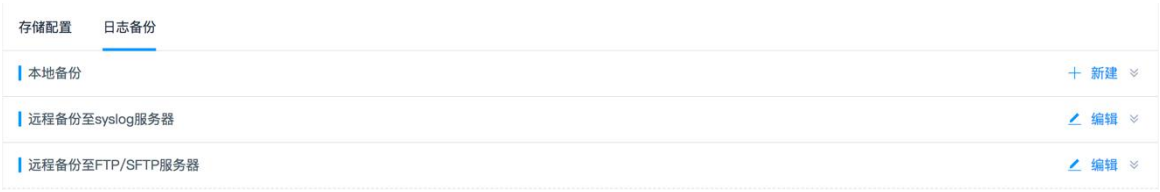


图 12-2-5

“本地备份”，点击新建，选择要备份的日志内容（包括系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志）和需要备份的时间范围，点击确定，即可完成本地备份，如图 12-2-6 所示。

图 12-2-6

“远程备份至 syslog 服务器”，点击编辑，将 syslog 状态改为开启状态，在页面中填写发送者标识，用于在 syslog 日志服务器中区分所接收的日志来自于哪个云堡垒机服务器；服务器地址和端口为 syslog 服务器端的地址和端口；选择要备份的日志内容（包括系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志），如图 12-2-7 所示。

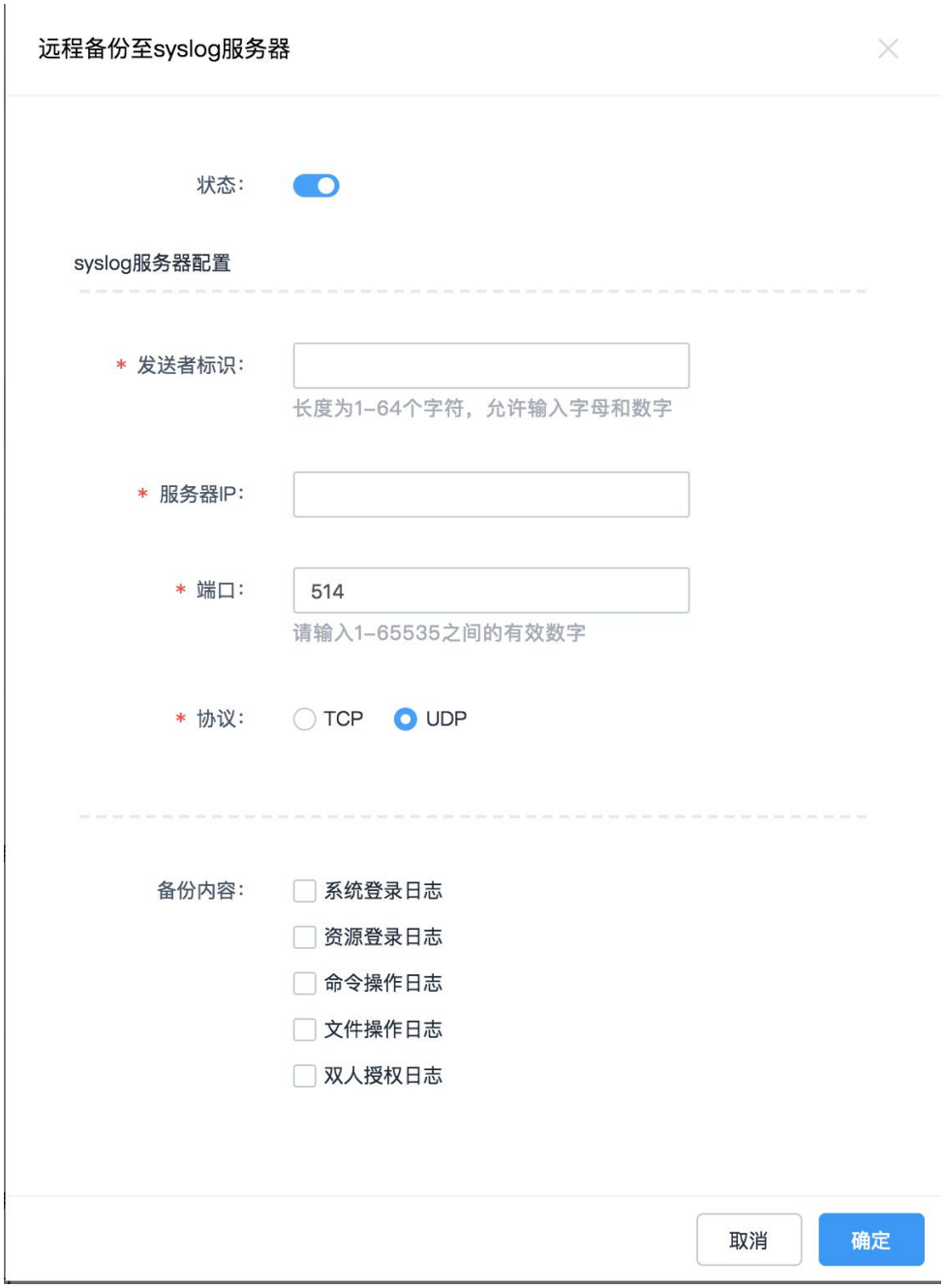


图 12-2-7

“远程备份至 FTP/SFTP 服务器”，点击编辑，将状态改为开启状态，选择备份的传输方式；服务器 IP、端口和用户名为 FTP/SFTP 服务器端的地址、端口和用户名，填写好后可以点击测试连通性确认服务器是否可达；选择要备份的日志内容（包括会话回放日志、系统配置），配置好后，系统会每天定时在零点进行前一日的数据备份并上传至远程 FTP/SFTP 服务器，如图 12-2-8 所示。

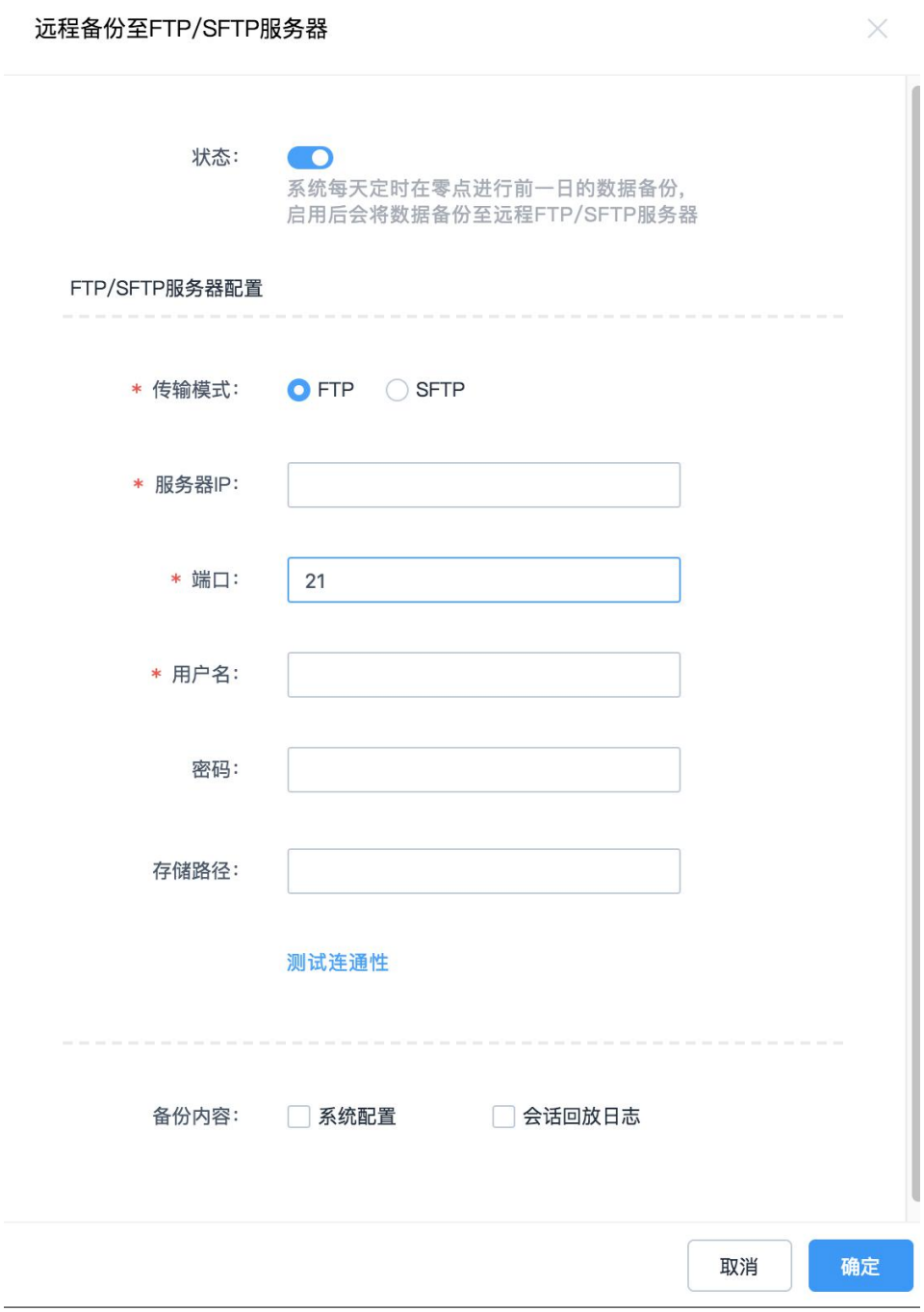


图 12-2-8

12.3 系统维护

12.3.1 系统状态

进入[系统/系统维护/系统状态]，可以查看当前云堡垒机系统的 CPU/内存使用率、磁盘读写状态、网络收发状态；其中可以自己选择时间段来查看，包括 5 分钟、15 分钟、1 小时三个阶段，将鼠标放在某个时间上会有数值显示，如图 12-3-1、12-3-2、12-3-3 所示。

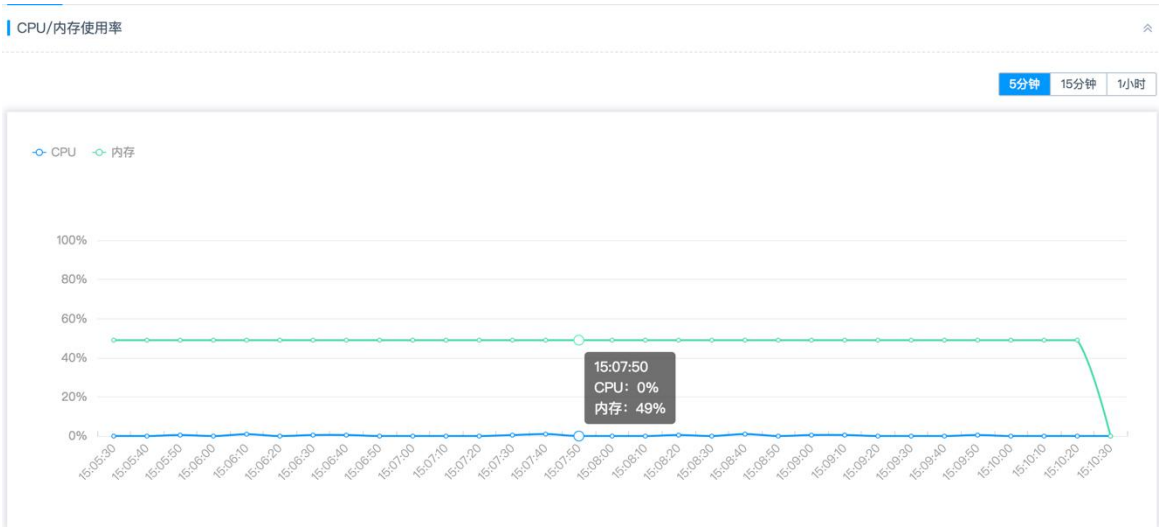


图 12-3-1

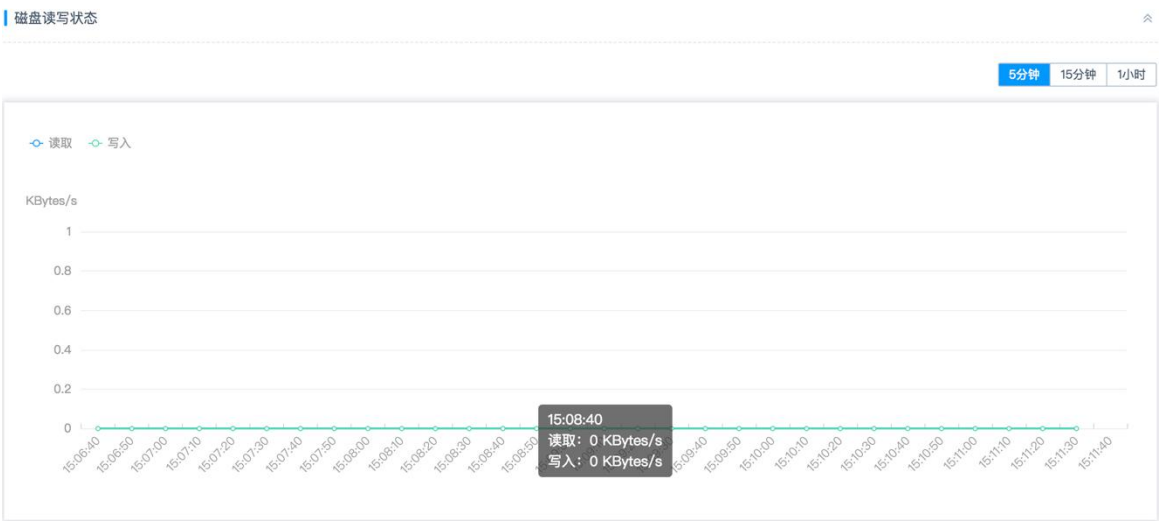


图 12-3-2

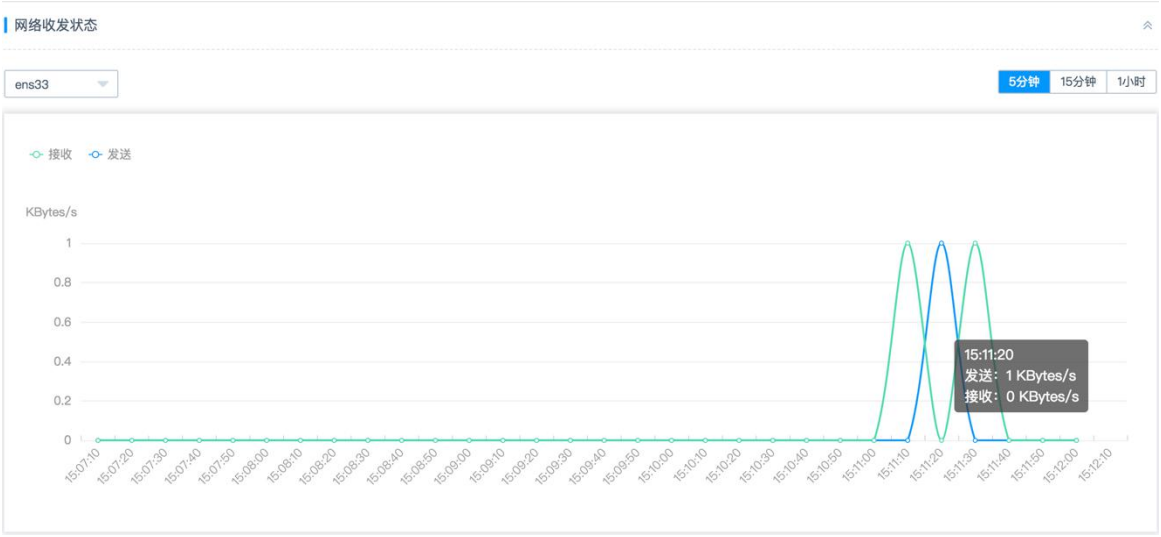


图 12-3-3

12.3.2 系统管理

进入[系统/系统维护/系统管理]页面，如图 12-3-4 所示。

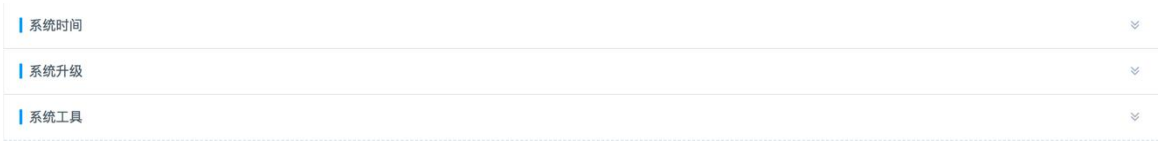


图 12-3-4

“系统时间”可以直接在页面上手动修改当前系统的时间或使用时间服务器同步当前系统的时间，使用时间服务器同步系统时间时，可以选择系统默认自带的时间服务器，也可以自己输入时间服务器点击<同步时间>（时间服务器列表最多显示 5 条记录），如图 12-3-5 所示。

图 12-3-5

在“系统升级”中点击<升级>将通过线下方式获取的升级包，上传到云堡垒机中，上传成功后会出现提示框显示该升级包的版本号，点击<确定>即可开始系统升级过程，升级过程中系统会自动重启，等重启完毕后即可完成升级过程，如图 12-3-6 所示。

图 12-3-6

在“系统工具”中点击<重启>或<关机>按钮后输入正确的云堡垒机登录密码，可以对云堡垒机服务器进行重启或关机操作；点击恢复出厂设置后输入正确的云堡垒机登录密码，即可恢复到云堡垒机的初始状态，所有的数据都会被清空（注意：license 不会变），如图 12-3-7 所示。

图 12-3-6

12.3.3 配置备份与还原

进入[系统/系统维护/配置备份与还原]页面，如图 12-3-7 所示。

图 12-3-7

点击<+新建>，弹出确认备份弹窗，可以输入备注信息来区分备份文件，点击备份开始备份，备份成功后，页面提示系统配置备份成功；打开自动备份按钮后，系统将在每天零点自动进行配置备份，如图 12-3-8 所示。

图 12-3-8

系统配置备份内容：

部门、用户模块、资源模块、运维模块中的主机标签和应用标签、策略模块、审计模块中的系统报表（报表自动发送）配置、运维报表（报表自动发送）配置、访问授权工单、安全配置中除 web 证书不备份其余配置都备份、网络配置中的 Open VPN、外发配置、认证配置、工单申请范围配置、告警配置、系统风格、存储配置中的自动删除配置、日志备份中的 syslog、FTP/SFTP 备份配置、配置备份与还原中的自动备份配置

点击<点击上传>，选择本地的备份文件上传到云堡垒机服务器中。上传完成后，还原文件会显示在页面上，出现确认还原的提示弹窗，点击<确定>，系统开始还原配置，如图 12-3-9 所示。

图 12-3-9

12.3.4 授权许可

进入[系统/系统维护/授权许可]页面，显示系统当前授权信息。“授权资源数”显示当前系统最多可添加资源数（包含：主机、应用发布资源），“授权并发连接数”指可同时登录资源数（包含：主机、应用发布资源）如图 12-3-10 所示。

图 12-3-10

点击<更新许可证>，弹出弹窗，点击<下载>，下载许可申请文件，发送给售后人员，由售后人员生成授权文件，点击<上传>，上传授权文件，完成更新授权，如图 12-3-11 所示。

图 12-3-10

12.3.5 网络诊断

进入[系统/系统维护/网络诊断]页面，连通性测试可以执行 ping、路由追踪、TCP 端口检测操作，输入正确格式的 IP 地址和端口，点击执行，会有结果信息显示，如图 12-3-11 所示。

图 12-3-11

12.3.6 系统诊断

进入[系统/系统维护/系统诊断]页面，可以获取当前系统的相关信息，选择要获取的信息，点击<获取信息>即可（获取的系统信息包括：综合信息、系统负载、内核信息、内存信息、网卡信息、磁盘使用信息、路由信息、ARP 信息），如图 12-3-12 所示。

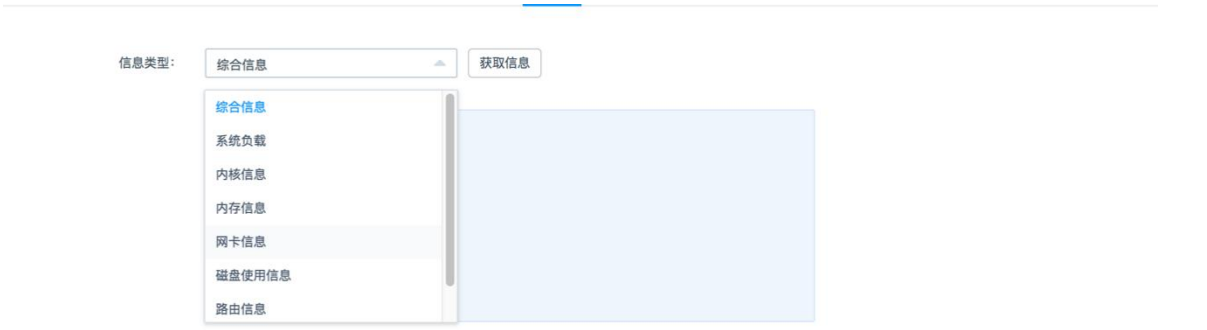


图 12-3-12

12.4 关于系统

进入[系统/系统维护/关于系统]页面，可以查看当前系统的相关信息，如图 12-4-1 所示。

图 12-4-1

附录 A FTP 服务器安装与配置

安装环境介绍

本文档安装 FTP 服务的环境为：Windows server 2012R2。

A.1 FTP 安装

A.1.1 修改服务器 IP

先修改服务器的基础信息。如主机名、IP 等。该文档服务器信息如图 A-1 所示。

图 A-1

A.1.2 安装 FTP 服务

进入服务器管理界面，选择仪表盘，仪表盘快速启动中会有配置本地服务器的选项。点击<添加角色和功能>，如图 A-2 所示。

图 A-2

A.1.3 添加角色和功能向导

添加角色和功能向导是 windowsserver 帮助安装或删除角色，角色服务以及服务功能。此页面可以跳过。点击<下一步>，如图 A-3 所示。

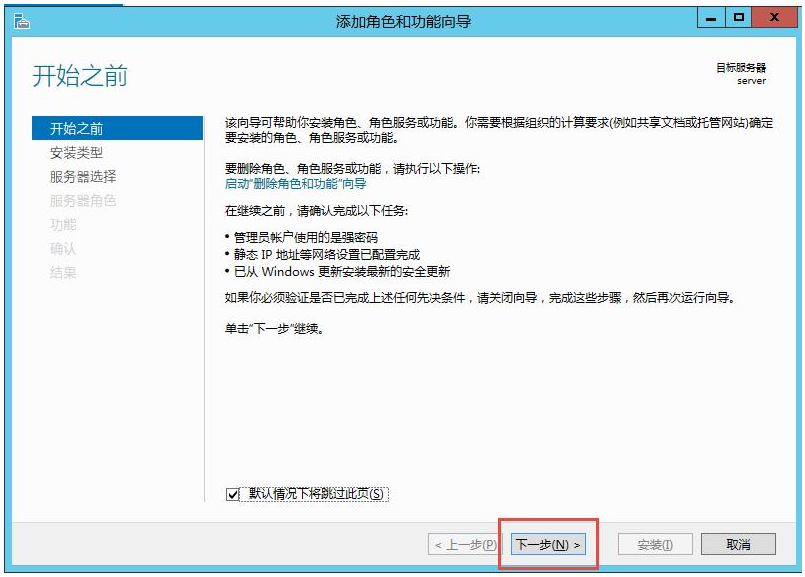


图 A-3

A.1.4 选择安装类型

选择基于角色或基于功能的安装。点击<下一步>，如图 A-4 所示。

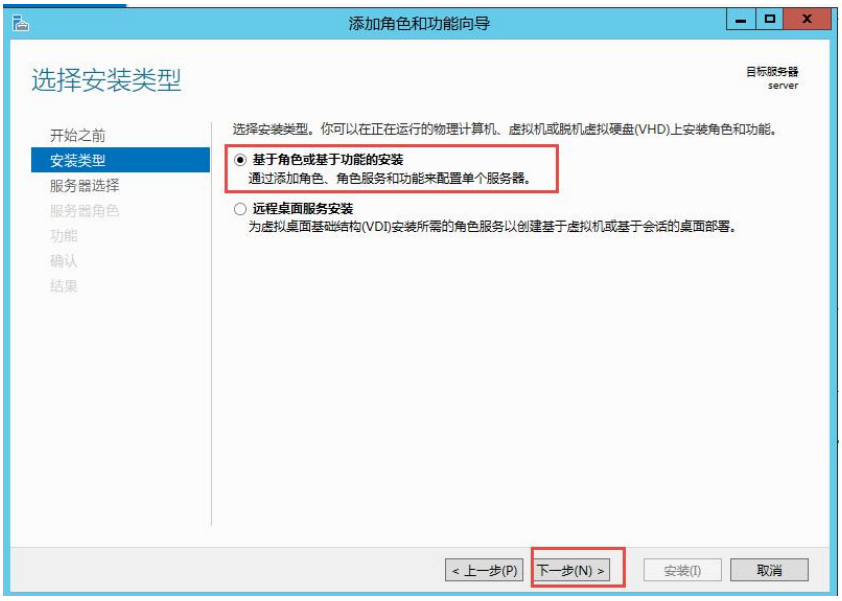


图 A-4

A.1.5 选择目标服务器

选择安装到那台服务器上或是虚拟硬盘。该环境只有 server 一台主机，选择该主机。点击<下一步>，如图 A-5 所示。

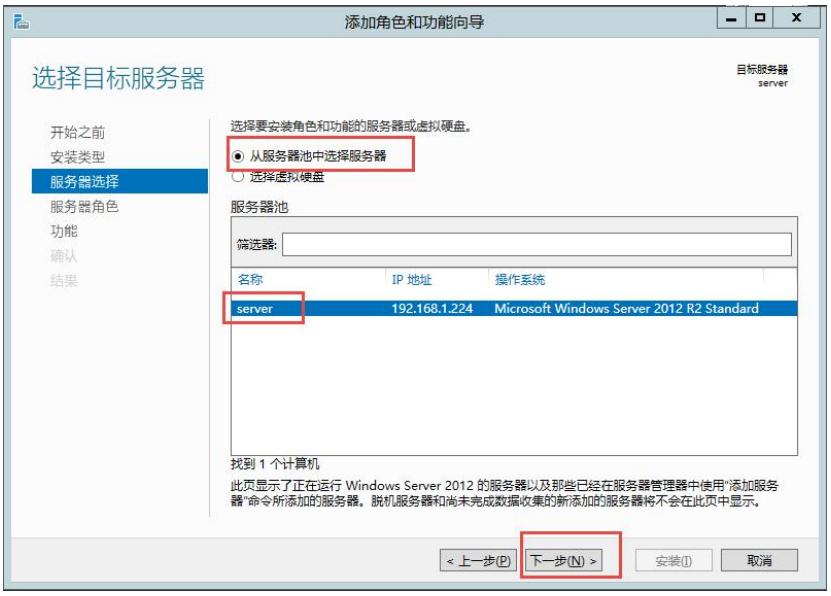


图 A-5

A.1.6 选择安装服务器角色

选择安装 Web 服务器（IIS）。选择 Web 服务器时会弹出选择管理工具。点击<添加功能>，再点击<下一步>。如图 A-6 所示。

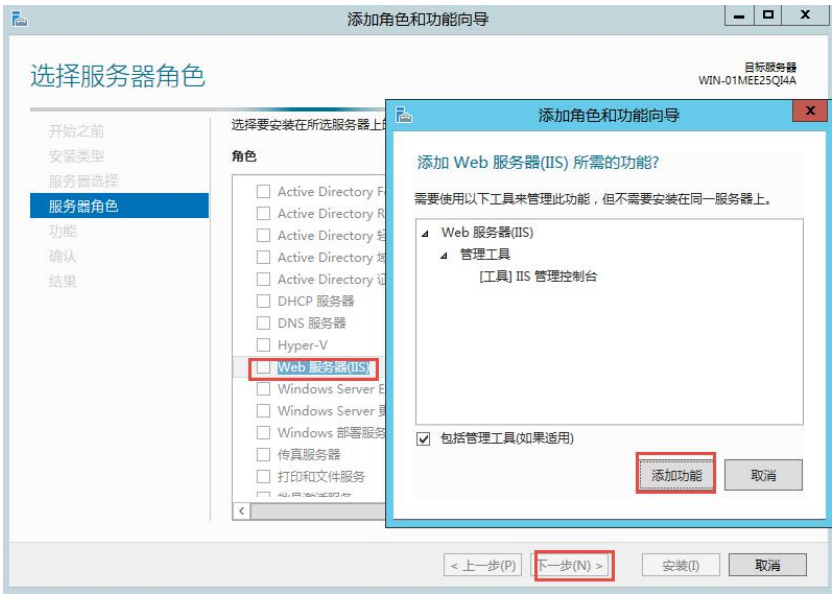


图 A-6

A.1.7 选择功能

选择该服务器所需要的其它功能（该环境为默认）。点击<下一步>。如图 A-7 所示。

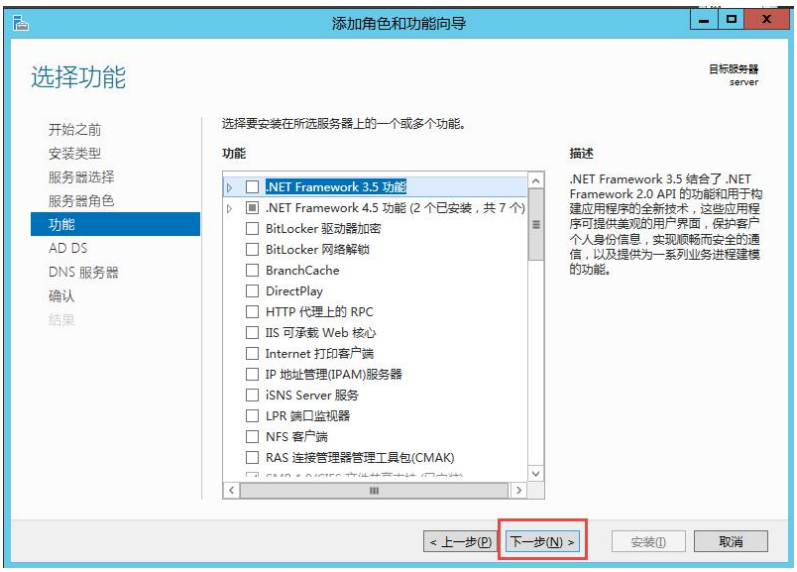


图 A-7

A.1.8 Web 服务器角色（IIS）

选择功能之后是 Web 服务器角色，点击<下一步>到服务角色的页面。选择 FTP 服务器的 FTP 服务。如图 A-8 所示。

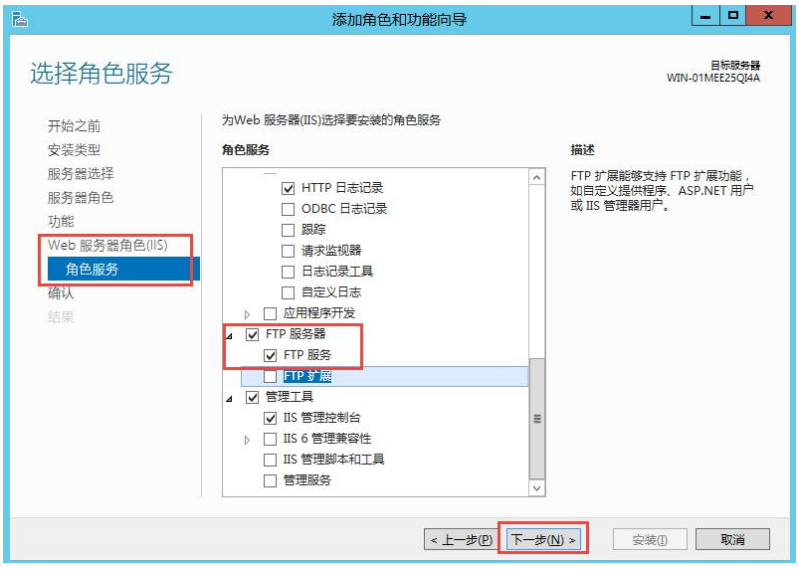


图 A-8

A.1.9 确认安装所选内容

确认在所选服务器上安装选取的角色，角色服务，或功能。点击<安装>开始安装所选服务器内容。如图 A-9 所示。

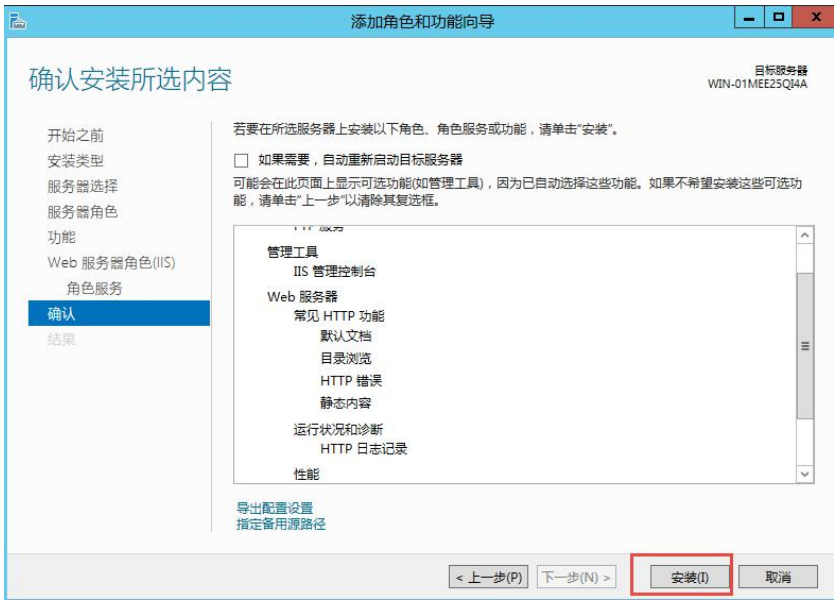


图 A-9

A.1.10 IIS 和 FTP 服务安装完成

等待服务器安装 IIS 和 FTP 服务。如图 A-10 所示，IIS 和 FTP 服务安装完成。

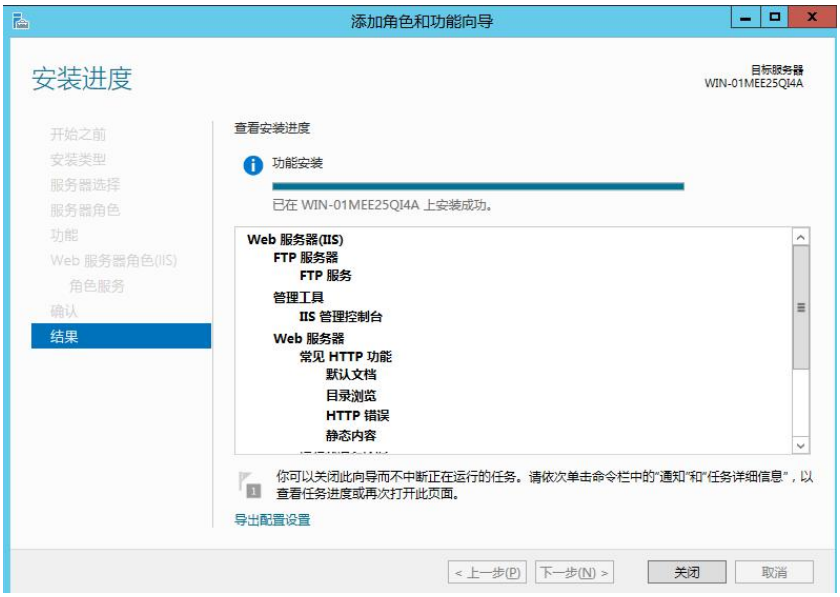


图 A-10

A.2 配置 FTP 服务

A.2.1 服务器管理器

FTP 服务器安装成功后，打开服务器管理器，选择 IIS，点击<工具>，点击<IIS 管理器>，如图 A-11 所示。

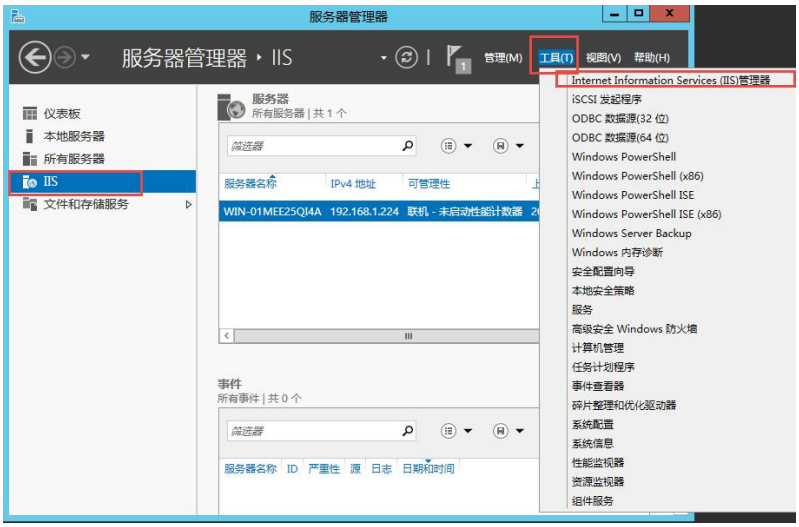


图 A-11

A.2.2 添加 FTP 站点

打开 IIS 管理器，选择网站，点击<添加 FTP 站点>。如图 A-12 所示。

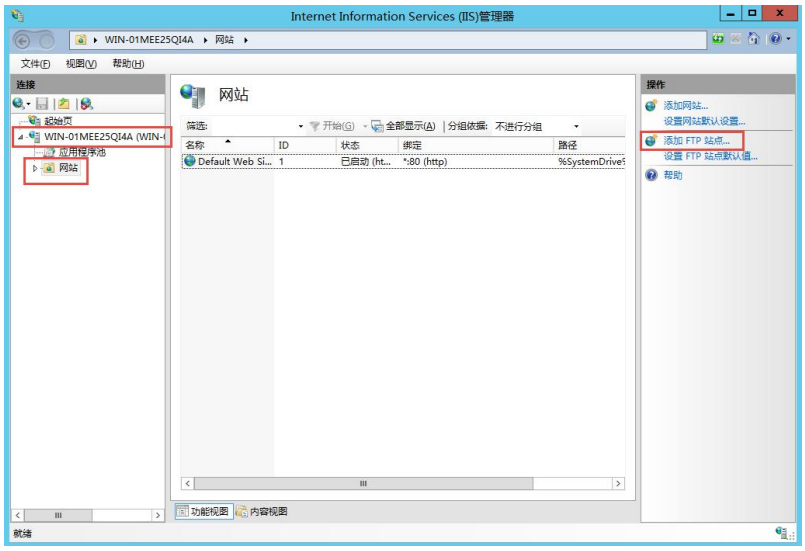


图 A-12

A.2.3 站点信息

添加 FTP 站点信息。FTP 名称，以及 FTP 对应的物理路径。然后点击<下一步>，如图 A-13 所示。

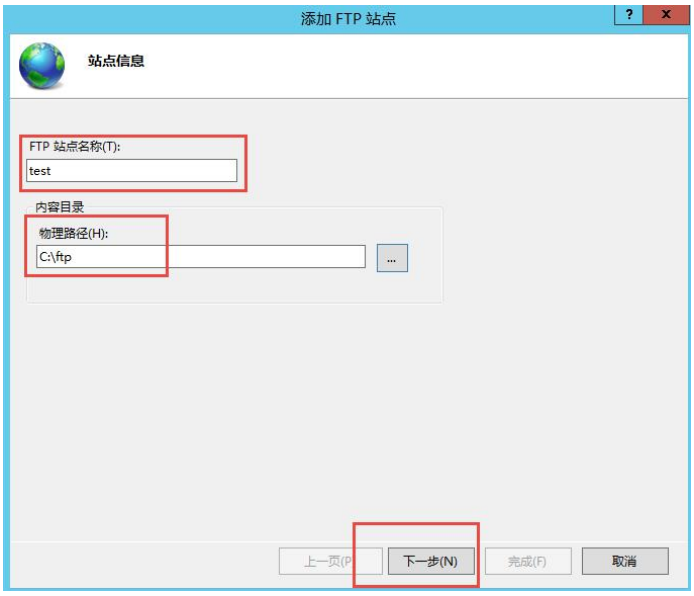


图 A-13

A.2.4 绑定和 SSL 设置

绑定 FTP 服务对应的 IP 以及端口，也可以使用虚拟主机名。SSL 证书可以通过上传，也可以自己生成（当前环境没有生成 SSL 证书，所以选择无 SSL），点击<下一步>，如图 A-14 所示。

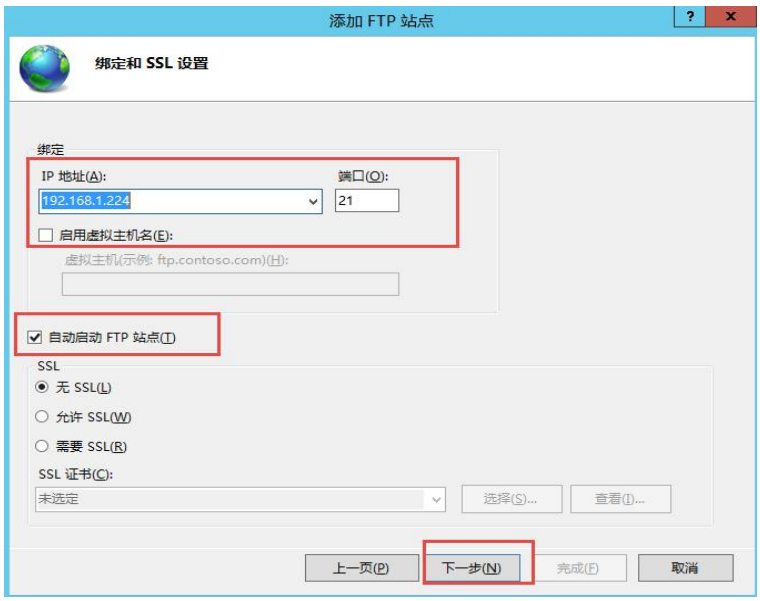


图 A-14

A.2.5 身份验证和授权信息

为当前 FTP 站点设置身份验证，以及授权用户和权限。点击<完成>，如图 A-15 所示。

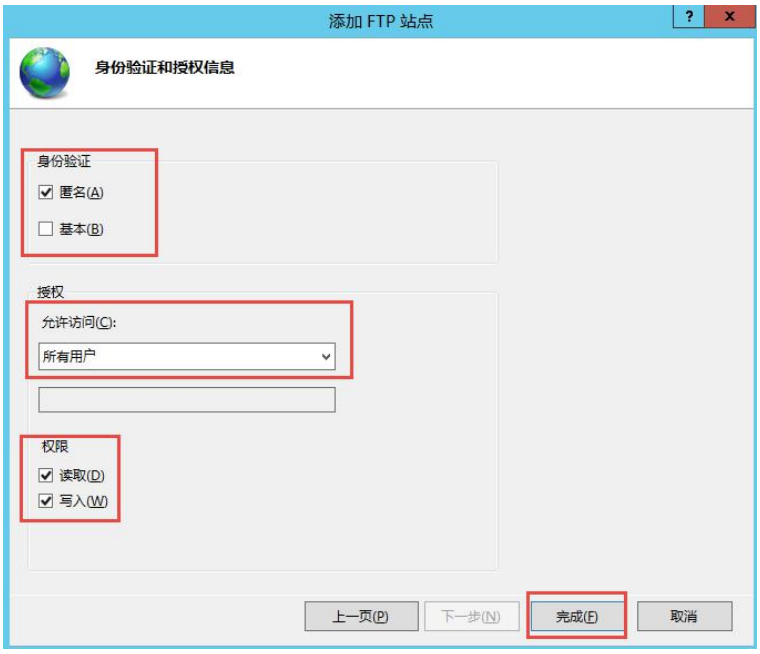


图 A-15

A.2.6 查看 FTP 站点

在 IIS 管理器的网站页面，能看到我们刚才添加的 FTP 站点已经启动。如图 A-16 所示。

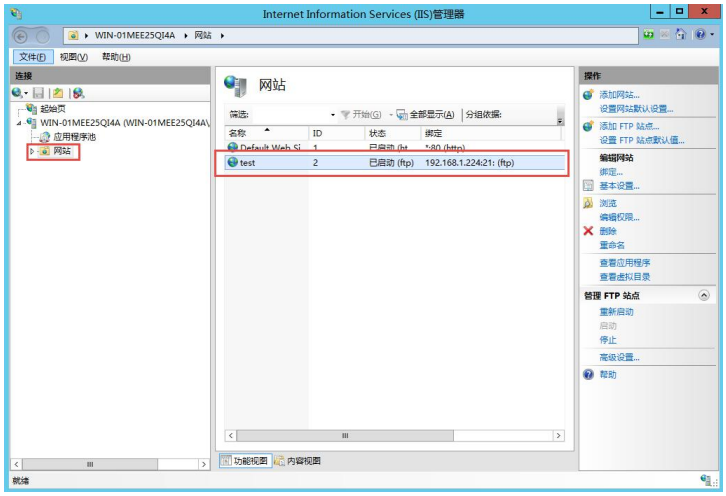


图 A-16

A.2.7 连接 FTP 站点

打开浏览器，输入 FTP://ip:端口 可以登入到 FTP 站点，可以下载文件。如果需要上传，则需要通过 FTP 工具来上传。如果访问不了 FTP 站点，请查看防火墙规则。如图 A-17 所示。

图 A-17

A.2.8 FTP 其它设置

通过服务器管理器打开 IIS 管理器，选择当前服务器主页，里面还有其它 FTP 相关设置，权限，防火墙规则等，可以根据实际环境修改。如图 A-18 所示。

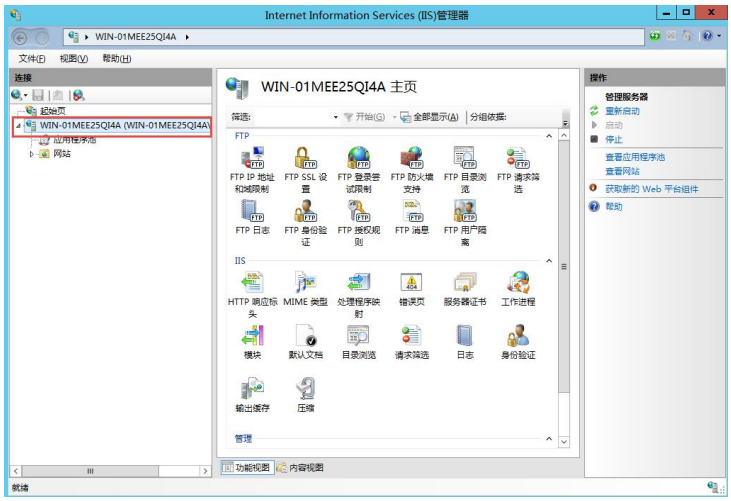


图 A-18

附录 B SNMP 安装与配置

简单网络管理协议（SNMP：Simple Network Management Protocol）是由互联网工程任务组（IETF：Internet Engineering Task Force ）定义的一套网络管理协议。该协议基于简单网关监视协议（SGMP：Simple Gateway Monitor Protocol）。利用 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

B.1 CentOS7 安装 SNMP

B.1.1 服务器信息

先修改服务器的基础信息。如主机名、ip 等。该文档服务器信息以及使用软件包信息。如图 B-1 所示。

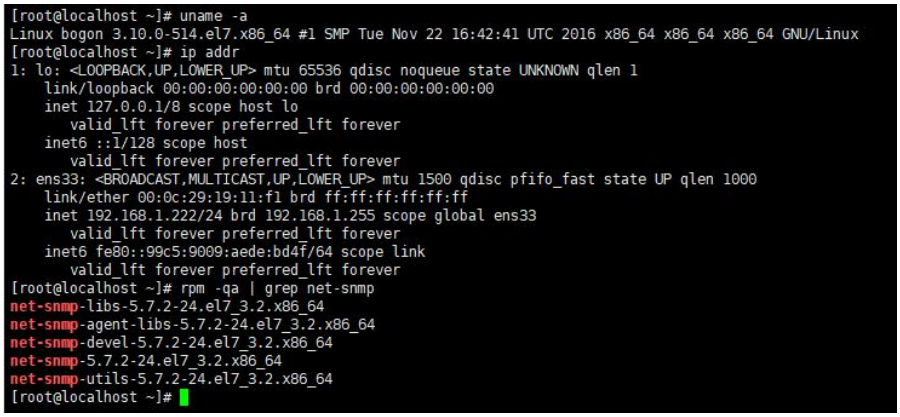


图 B-1

B.1.2 更新 yum 源并安装 SNMP

yum update &&yum install -y net-snmp net-snmp-devel net-snmp-libs net-snmp-utils php-snmp 更新 yum 源并安装 snmp 服务，如图 B-2 所示。

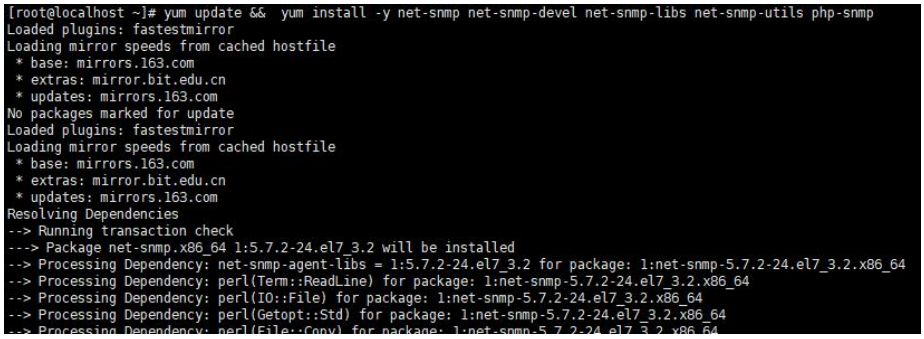


图 B-2

B.1.3 配置 SNMP

通过 yum 安装的 snmp 配置文件为：/etc/snmp/snmpd.conf。配置 snmpd.conf 文件需要更改以下几个地方（默认配置基础上）。如图 B-3 所示。public 为默认的团体名，将它修改为自己确定的字符串，红线内容为增加行，systemview 改为 all，其它几行去掉注销#。

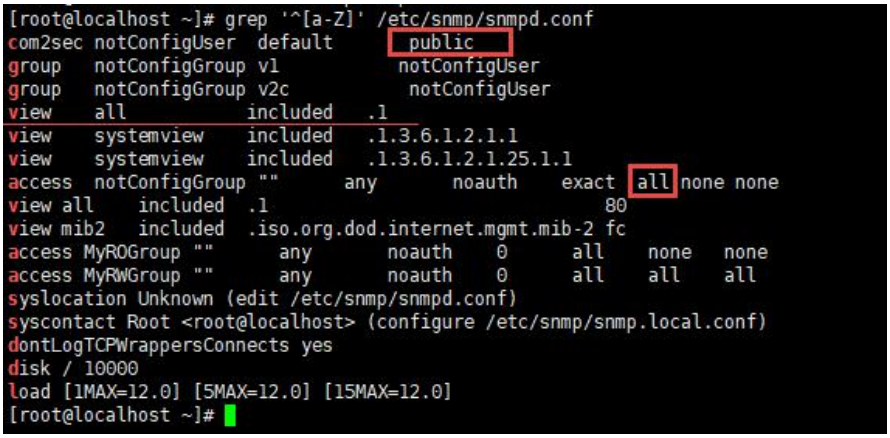


图 B-3

B.1.4 修改防火墙

iptables -I INPUT -p udp --dport 161 -j ACCEPT　　#对外开放 udp 的 161 端口

echo "iptables -I INPUT -p udp --dport 161 -j ACCEPT">> /etc/rc.d/rc.local　#将防火墙规则写入开机文件，开机自动加载防火墙配置，如图 B-4 所示。

```
[root@localhost ~]# iptables -I INPUT -p udp --dport 161 -j ACCEPT
[root@localhost ~]# echo "iptables -I INPUT -p udp --dport 161 -j ACCEPT" >> /etc/rc.d/rc.local
[root@localhost ~]# chmod +x /etc/rc.d/rc.local
[root@localhost ~]# cat /etc/rc.d/rc.local
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local
iptables -I INPUT -p udp --dport 161 -j ACCEPT
```

图 B-4

B.1.5 启动 snmp 服务

如图 B-5 所示。

systemctl start snmpd　　#启动 snmp 服务

systemctl enable snmpd　#设置 snmp 服务开机启动

systemctl status snmpd #查看 snmp 服务状态

```
[root@localhost ~]# systemctl start snmpd
[root@localhost ~]# systemctl enable snmpd
[root@localhost ~]# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2017-08-25 02:55:21 EDT; 27s ago
 Main PID: 31489 (snmpd)
   CGroup: /system.slice/snmpd.service
           └─31489 /usr/sbin/snmpd -LS0-6d -f

Aug 25 02:55:20 bogon systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
Aug 25 02:55:21 bogon snmpd[31489]: /etc/snmp/snmpd.conf: line 94: Error: bad prefix match parame
Aug 25 02:55:21 bogon snmpd[31489]: /etc/snmp/snmpd.conf: line 95: Error: bad prefix match parame
Aug 25 02:55:21 bogon snmpd[31489]: net-snmp: 2 error(s) in config file(s)
Aug 25 02:55:21 bogon snmpd[31489]: NET-SNMP version 5.7.2
Aug 25 02:55:21 bogon systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]#
```

图 B-5

B.2 Ubuntu 下安装 SNMP

B.2.1 服务器信息

先修改服务器的基础信息。如主机名、IP 等。该文档服务器信息以及使用软件包信息。如图 B-6 所示。

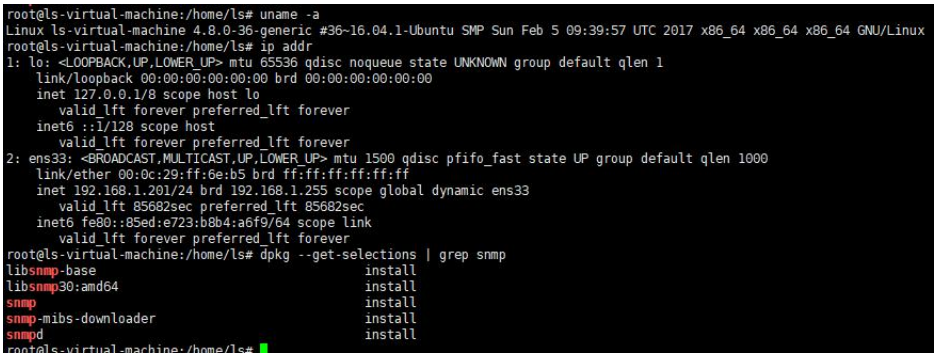


图 B-6

B.2.2 安装 SNMP

apt-get -y install snmpd snmp snmp-mibs-downloader 安装 SNMP 服务包。如图 B-7 所示。

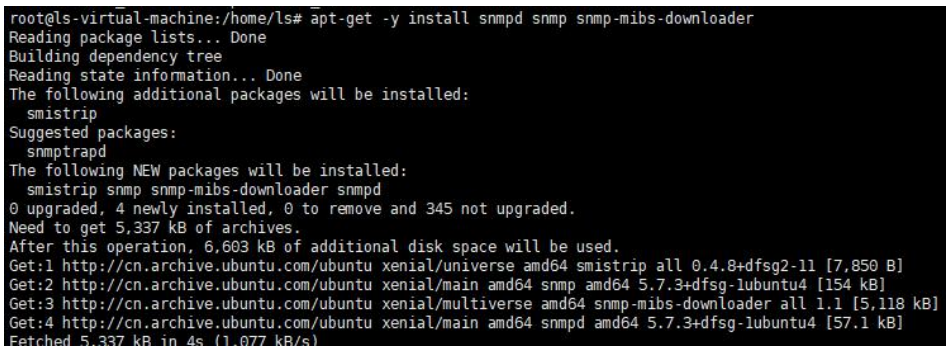


图 B-7

B.2.3 配置 SNMP

通过 yum 安装的 snmp 配置文件为：/etc/snmp/snmpd.conf。配置 snmpd.conf 文件需要更改以下几个地方（默认配置基础上）。如图 B-8 所示。public 为默认的团体名，将它修改为自己确定的字符串。

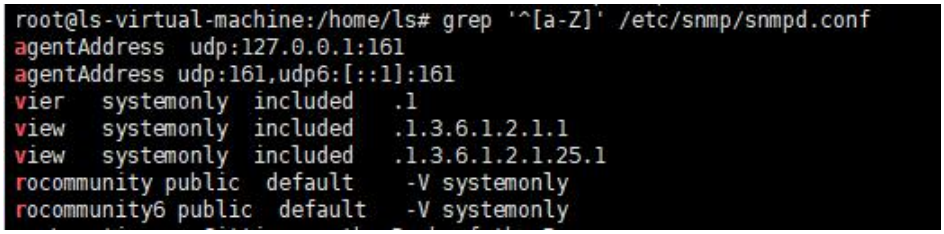


图 B-8

B.2.4 修改防火墙

iptables -I INPUT -p udp --dport 161 -j ACCEPT #对外开放 udp 的 161 端口

在/etc/rc.local 中增加一行：iptables -I INPUT -p udp --dport 161 -j ACCEPT 如图 B-9 所示。

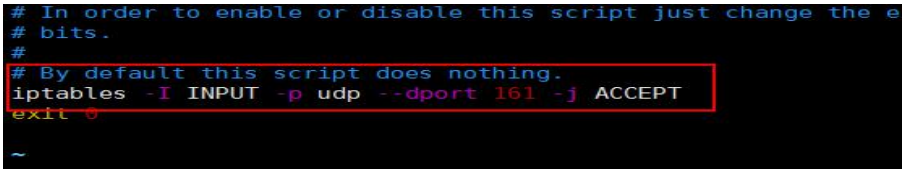


图 B-9

B.2.5 启动 SNMP 服务

systemctl start snmpd　　#启动 snmp 服务
systemctl enable snmpd　#设置 snmp 服务开机启动
systemctl status snmpd　#查看 snmp 服务状态
如图 B-10 所示。

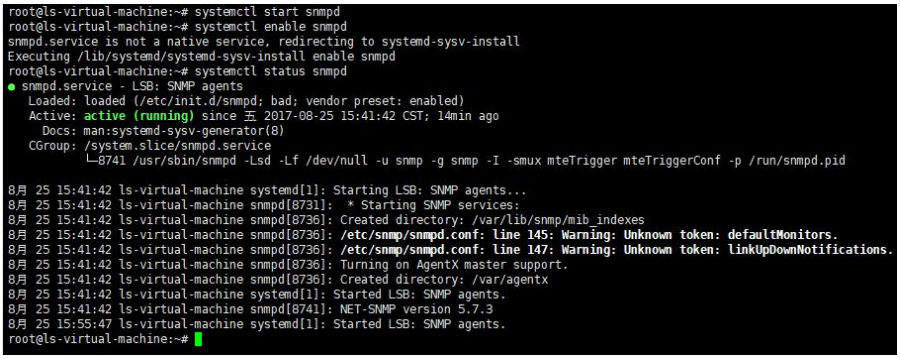


图 B-10

B.3 Windows server 2008 安装 SNMP

B.3.1 打开服务器管理器

打开开始菜单，点击<管理工具>，点击<服务器管理器>。如图 B-11 所示。

图 B-11

B.3.2 添加功能

打开服务器管理器，选择功能，点击<添加功能>。如图 B-12 所示。

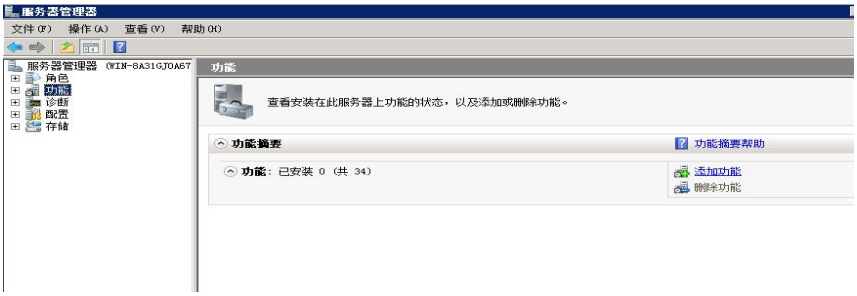


图 B-12

B.3.3 选择功能

进入添加功能页面，选择 SNMP 服务，点击<下一步>。如图 B-13 所示。

图 B-13

B.3.4 安装 SNMP 服务

选择 SNMP 服务，提示是否安装以下角色角色服务。点击<安装>，如图 B-14 所示。

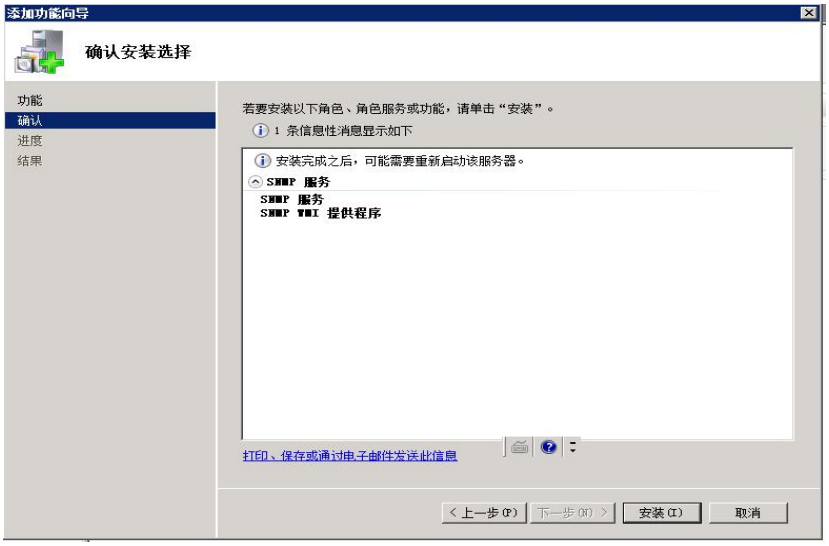


图 B-14

B.3.5 SNMP 服务安装完成

等待安装完成之后点击<关闭>。如图 B-15 所示。

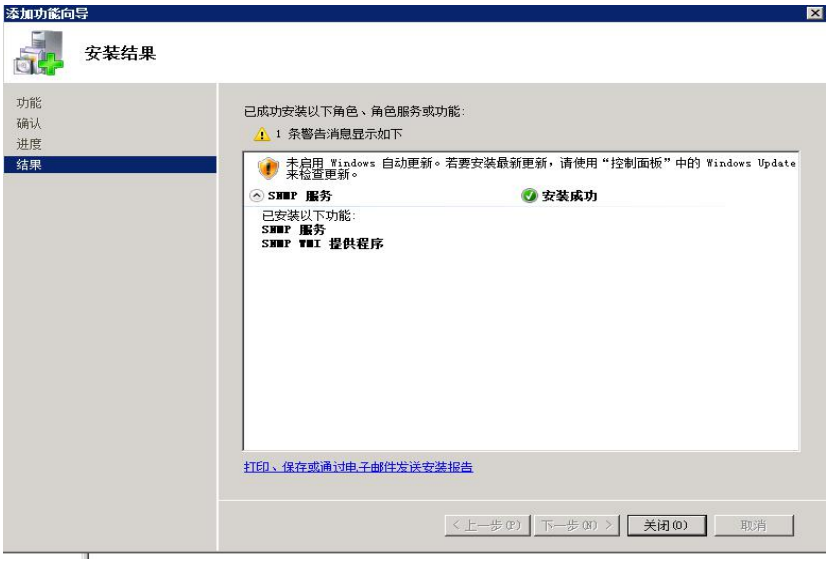


图 B-15

B.3.6 SNMP 属性

打开服务器管理器，配置—服务—SNMP 服务（右键）--属性。如图 B-16 所示。

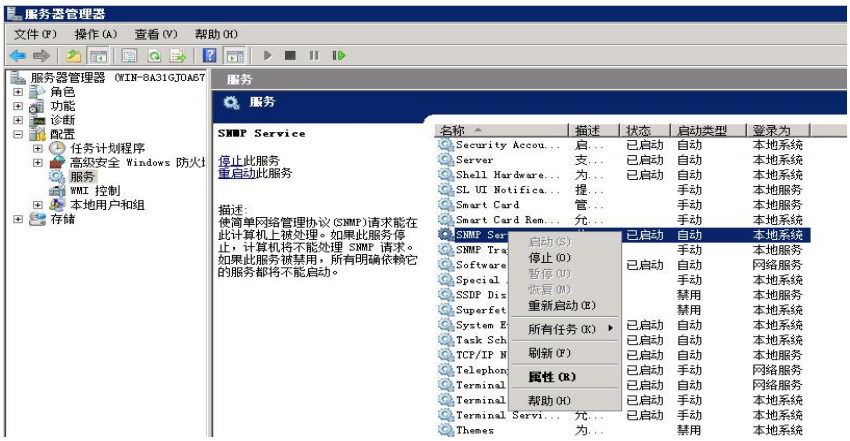


图 B-16

B.3.7 修改 SNMP 配置

切换到“安全”选项，接受的社区名称-添加（团体权限：只读；团体名称：自己定义的字符串）。接受来自下列主机的 SNMP 数据包，填写云堡垒机等监控主机的的 IP 地址（该环境以 192.168.1.123 为例），也可以选择“接受来自任何主机的 SNMP 数据包”。为了安全，建议配置为监控主机的 IP 地址。如图 B-17 所示。

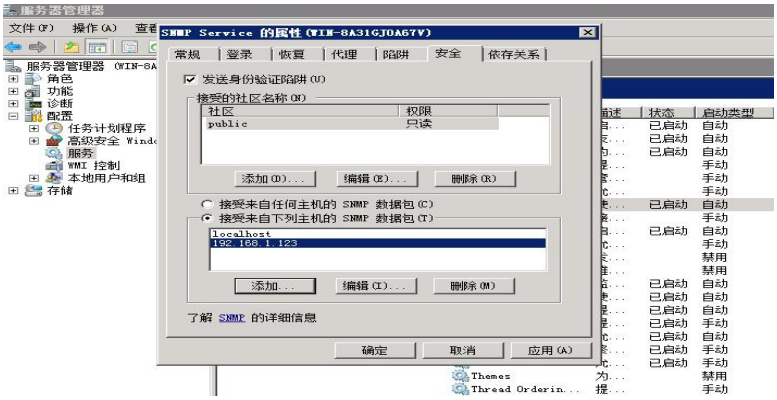


图 B-17

B.3.8 启动 SNMP 服务

右键 SNMP 服务。点击<重新启动>，重启该服务。如图 B-18 所示。

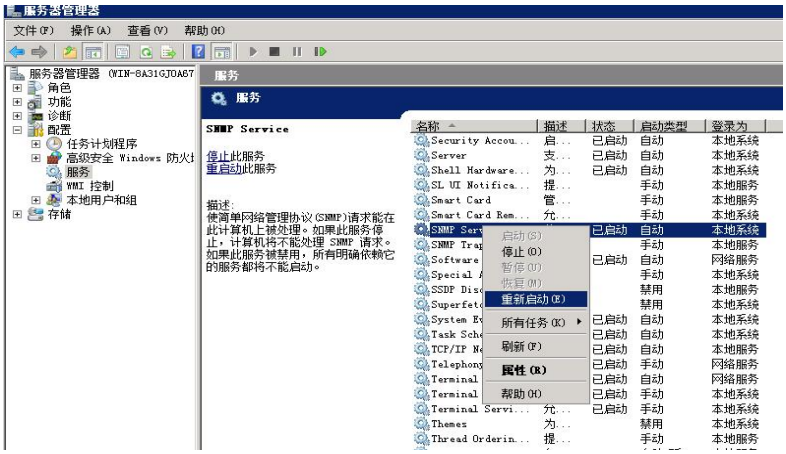


图 B-18

附录 C Radius 服务器安装与配置

Freeradius 是一个世界范围内广泛开发的 Radius 服务器。它是多样化 Radius 商业产品的基础部分。它为许多世界 500 强的公司和顶级的 ISP 服务商提供 AAA 认证服务。Freeradius 服务器高速，功能丰富，模块化，扩展性。本章以 Freeradius 的安装配置为例进行讲解。Freeradius 一般用来进行账户认证管理，记账管理，常见的电信运营商的宽带账户，上网账户管理，记账。

Freeradius 包含一个 Radius 服务器，一个 BSD 协议授权的客户端库，一个 PAM 库，还一个 Apache 的模块。大多数时候，Freeradius 就是指 radius 服务器。 作为第一款开源发布的 Radius 程序，同时作为一个普通安装包，被许多种操作系统内置。还有二进制的包给其它系统使用，并且有源码几乎可以被任何系统编译安装。

安装环境介绍

以下服务器信息为例安装 RADIUS 服务环境。

服务器信息：CentOS7

内核版本：3.10.0-514.el7.x86_64

IP：192.168.1.223/24

网关：192.168.1.1

安装软件版本

freeradius-utils-3.0.4-8.el7_3.x86_64

freeradius-3.0.4-8.el7_3.x86_64

freeradius-mysql-3.0.4-8.el7_3.x86_64

C.1 Radius 安装

C.1.1 修改服务器信息

先修改服务器的基础信息。如主机名、IP 等。该文档服务器信息如图 C-1 所示。

```
[root@bogon ~]# uname -a
Linux bogon 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
[root@bogon ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:19:11:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.222/24 brd 192.168.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::99c5:9009:aede:bd4f/64 scope link
       valid_lft forever preferred_lft forever
[root@bogon ~]#
```

图 C-1

C.1.2 更新 yum 源

Yumupdate 更新 yum 源，如图 C-2 所示。

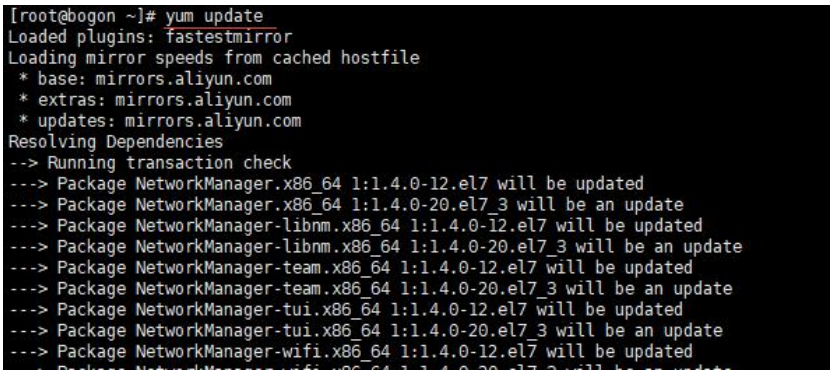


图 C-2

C.1.3 查看软件安装包

查看是否有需要安装的软件包，如果没有，就下载 epel 源，或者通过下载其它源来安装。如图 C-3 所示。

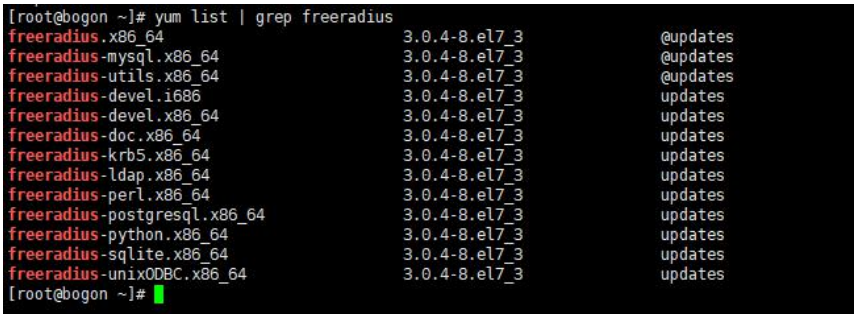


图 C-3

C.1.4 安装软件包

通过 yum 安装 freeradius，freeradius-utils。如图 C-4 所示。

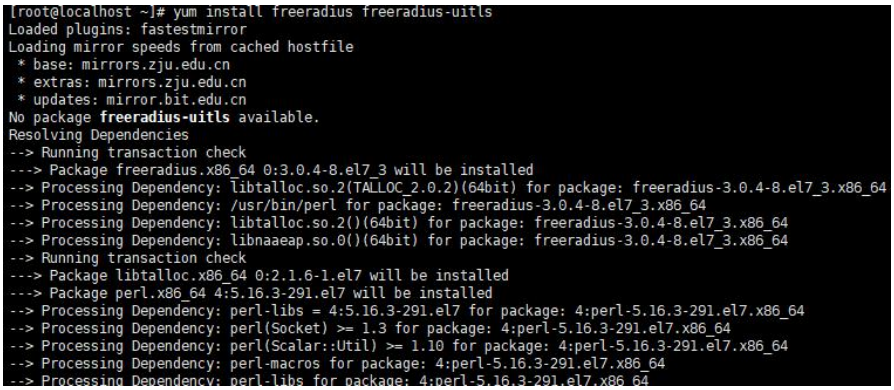


图 C-4

C.1.5 查看包是否安装

通过 rpm-qa|grep freeradius 查询 freeradius 包是否安装。如图 C-5 所示。

Freeradiusfreeradius-utils 安装完成。

```
[root@localhost ~]# rpm -qa | grep freeradius
freeradius-3.0.4-8.el7_3.x86_64
freeradius-utils-3.0.4-8.el7_3.x86_64
[root@localhost ~]#
```

图 C-5

C.2 配置 Freeradius

C.2.1 修改 client 配置文件

编辑/etc/raddb/clients.conf 配置文件。将文件 241-244 行取消注销，将 radius 对当前网段开放，修改共享密钥（该文档配置密钥为 yunanbao）如图 C-6 所示。

```
240 #
241 client private-network-1 {
242         ipaddr          = 192.168.1.0/24
243         secret          = yunanbao
244 }
245
```

图 C-6

C.2.2 修改 users 配置文件

编辑/etc/raddb/clients.users，添加用户信息。将文件 87-88 行取消注销，或者自己新增，（bob 为测试用户，hello 为测试密码）如图 C-7 所示。

```
87 bob      Cleartext-Password := "hello"
88          Reply-Message := "Hello, %{User-Name}"
89 #
```

图 C-7

C.2.3 启动服务

systemctlstartradiusd 启动 radius 服务， systemctlenableradiusd 将 radius 服务设置开机启动，systemctlstatusradiusd 查看 radius 服务状态。如图 C-8 所示。

```
[root@localhost ~]# systemctl start radiusd
[root@localhost ~]# systemctl enable radiusd
Created symlink from /etc/systemd/system/multi-user.target.wants/radiusd.service to /usr/lib/systemd/system/radiusd.service.
[root@localhost ~]# systemctl status radiusd
● radiusd.service - FreeRADIUS high performance RADIUS server.
   Loaded: loaded (/usr/lib/systemd/system/radiusd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-08-24 23:24:13 EDT; 10s ago
 Main PID: 2866 (radiusd)
   CGroup: /system.slice/radiusd.service
           └─2866 /usr/sbin/radiusd -d /etc/raddb

Aug 24 23:24:13 bogon systemd[1]: Starting FreeRADIUS high performance RADIUS server....
Aug 24 23:24:13 bogon systemd[1]: Started FreeRADIUS high performance RADIUS server..
[root@localhost ~]#
```

图 C-8

C.2.4 查看端口

netstat-naup 查看当前开放的 udp 端口，可以看到 18121813 端口开放，如图 C-9 所示。

图 C-9

C.2.5 修改防火墙

iptables -I INPUT -p udp --dport 1812 -j ACCEPT 防火墙对外开放 udp 协议的 1812 端口

iptables -I INPUT -p udp --dport 1813 -j ACCEPT 防火墙对外开放 udp 协议的 1813 端口

如图 C-10 所示。

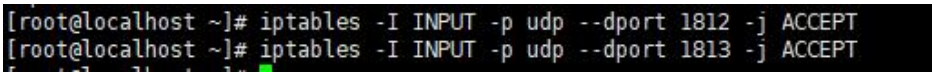


图 C-10

C.2.6 Radius 调试

到此为止基本的 Radius 服务就可以正常工作了。如果 radius 启动出现问题，可以将 radius 进程停止，然后以参数-X 的方式临时启动调试模式。如图 C-11 所示。

radius-X 进入调试模式。

图 C-11

附录 D AD 域服务器安装与配置

活动目录（Active Directory）是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。（Active Directory 不能运行在 Windows Web Server 上，但是可以通过它对运行 Windows Web Server 的计算机进行管理。）Active Directory 存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。Active Directory 使用了一种结构化的数据存储方式，并以此作为基础对目录信息进行合乎逻辑的分层组织。

安装环境介绍

以下服务器信息为该文档安装 AD 域环境。

Windowsserver 版本：Windowsserver2012R2

IP：192.168.1.224/24

网关：192.168.1.1

DNS：192.168.1.224

域名：yunanbao.com

创建域的必要环境

DNS 域名：创建 AD 域之前，需要一个符合 DNS 格式的域名，如 yunanbao.com（本文档以 yunanbao.com 为例）。

DNS 服务器：AD 域服务需要 DNS 服务的支持，其它计算机通过 DNS 服务解析找到该域服务器。因此需要一台支持 AD 的 DNS 服务器，并且支持动态更新。如果现在没有 DNS 服务器，则可以在创建 AD 域的过程中，选择这台域控制器上安装 DNS 服务器（该文档是 AD 域和 DNS 服务一起安装）。AD 需要一个 SYSVOL 文件夹来存储域共享文件（例如域组策略有关的文件），该文件夹必须位于 NTFS 磁盘，系统默认创建在系统盘，为了性能建议存储到其它分区。

D.1 AD 域安装

D.1.1 修改主机名和 IP

修改服务 IP 地址，并且将 DNS 指向本机，修改计算机名（该文档计算机名为 server）。安装 AD 域服务之后，机器名称变成主机名+域名 （例：server.yunanbao.com）。如图 D-1 所示。

图 D-1

D.1.2 安装 AD 域

进入服务器管理界面，选择仪表盘，仪表盘快速启动中会有配置本地服务器的选项。点击<添加角色和功能>，如图 D-2 所示。

图 D-2

D.1.3 添加角色和功能向导

添加角色和功能向导是 windowsserver 帮助安装或删除角色，角色服务以及服务功能。此页面可以跳过。点击<下一步>，如图 D-3 所示。

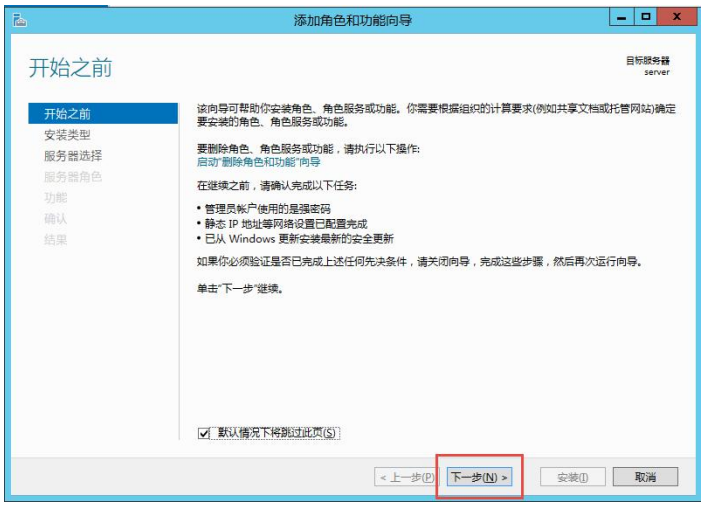


图 D-3

D.1.4 选择安装类型

选择基于角色或基于功能的安装。点击<下一步>，如图 D-4 所示。

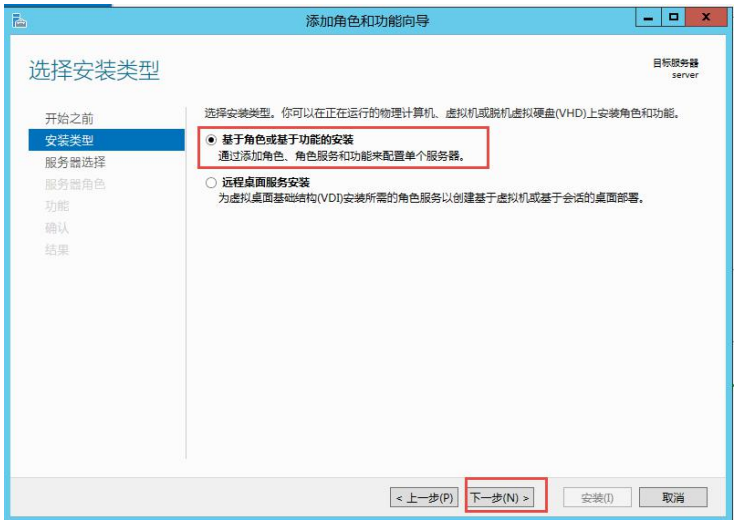


图 D-4

D.1.5 选择目标服务器

选择安装到那台服务器上或是虚拟硬盘。该环境只有 server 一台主机，选择该主机。点击<下一步>，如图 D-5 所示。

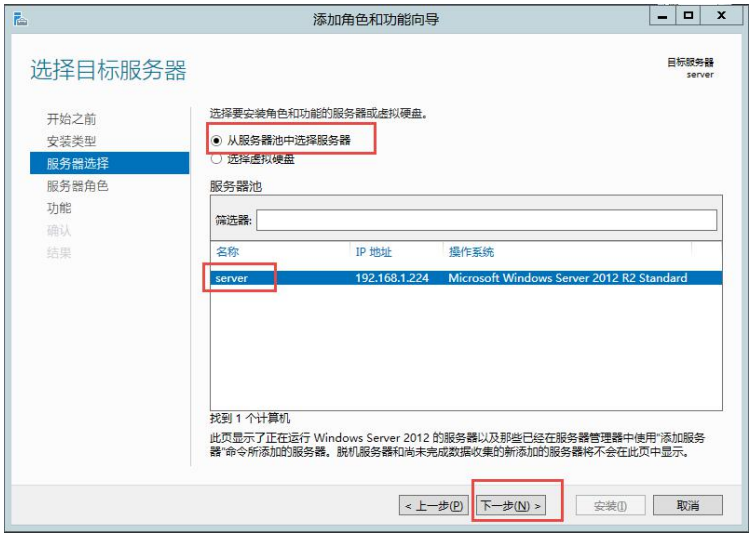


图 D-5

D.1.6 选择安装 AD 域

选择服务器 ActiveDirectory 域服务。会弹出一个安装 AD 域服务所需的功能，以及 AD 域管理工具。如果不需要管理工具，也可以不安装管理工具，然后点击添加功能，如图 D-6 所示。

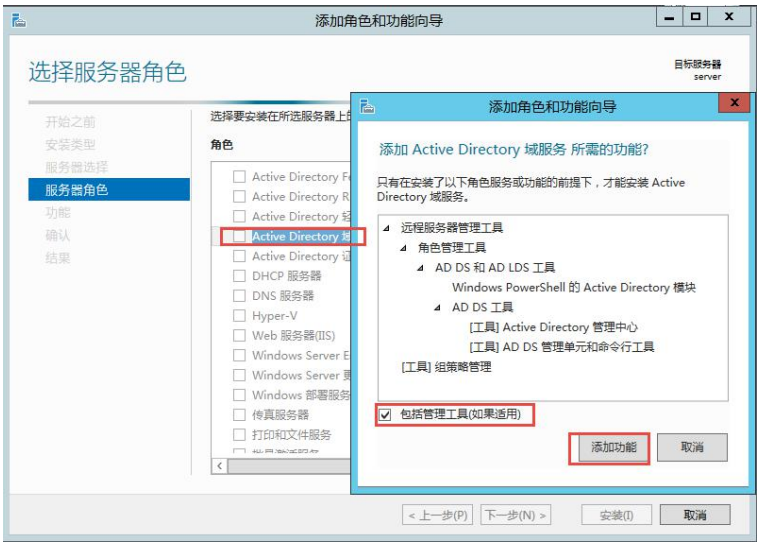


图 D-6

D.1.7 选择安装 DNS 服务

AD 域服务需要 DNS 服务的支持。如果当前环境没有一台可以支持 AD 域的 DNS 服务器，那就需要安装 DNS 服务（该环境没有其它 DNS 服务，所以在 AD 域上安装 DNS 服务），如果当前环境有可用的 DNS 服务器，则可以不用安装 DNS 服务。步骤与 AD 域一样。然后点击<下一步>。

如图 D-7 所示。

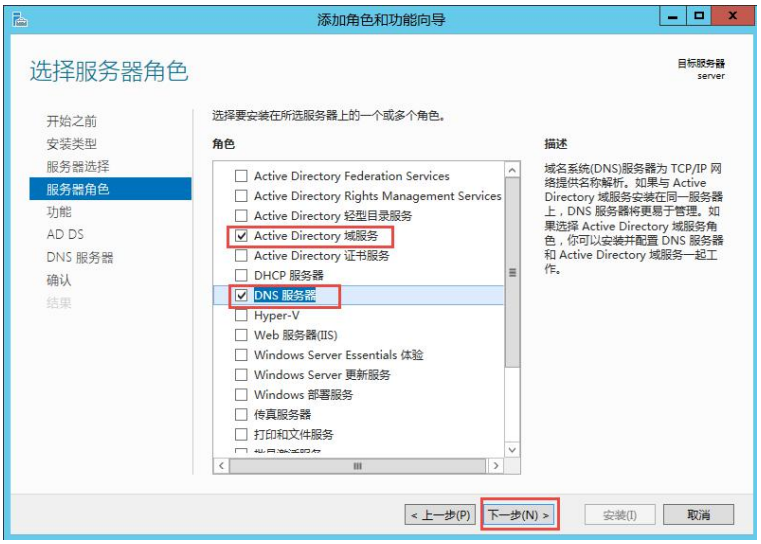


图 D-7

D.1.8 选择功能

选择该服务器所需要的其它功能（该环境为默认）。点击<下一步>。如图 D-8 所示。

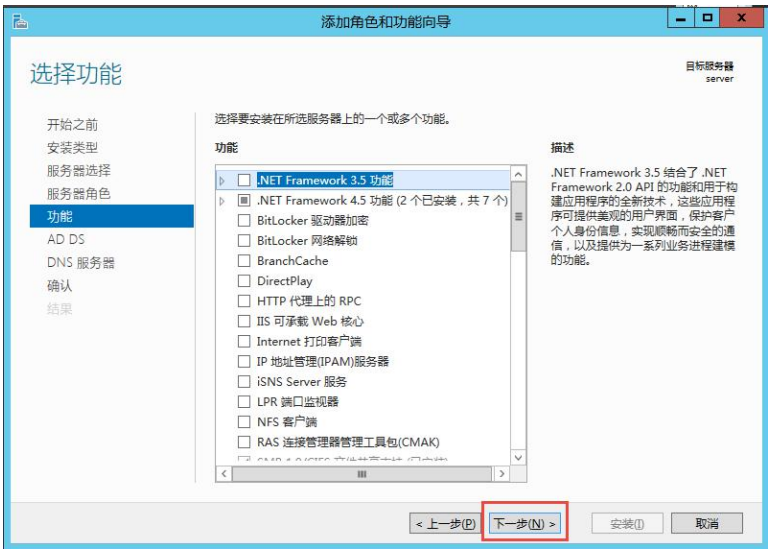


图 D-8

D.1.9 确认安装所选内容

选择功能之后是 AD 域和 DNS 的介绍。点击<下一步>到缺认安装所选内容的页面。点击<安装>开始安装 AD 域服务和 DNS 服务。如图 D-9 所示。

图 D-9

D.1.10 AD 域服务和 DNS 服务安装完成

等待服务器安装好 AD 域服务和 DNS 服务。安装完成了的 AD 域和 DNS 服务并不能直接提供服务，AD 域需要配置之后才能提供服务。如图 D-10 所示，AD 域和 DNS 服务安装完成。

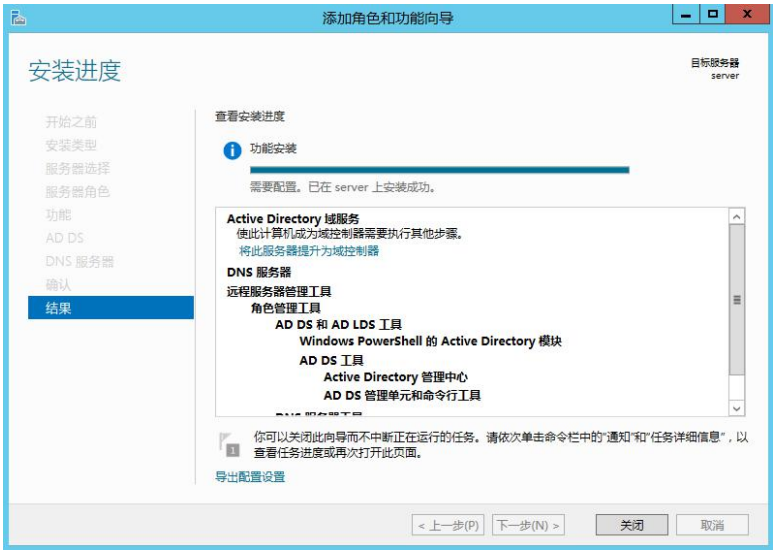


图 D-10

D.2 配置 AD 域

D.2.1 服务器管理器

AD 域服务和 DNS 服务安装完成后。在服务器管理器中可以看到 ADDS 和 DNS 的选项。选择 AD DS。管理页面会提示需要配置 AD 域。选择通知栏。点击<将此服务器提升为域控制器>。如图 D-11 所示。

图 D-11

D.2.2 AD 域部署配置

如果当前环境已经是域环境，那就加入现有域或者加入到现有林。如果是一个新的环境，则选择新林。填写根域名（例：yunanbao.com）。点击<下一步>，如图 D-12 所示。

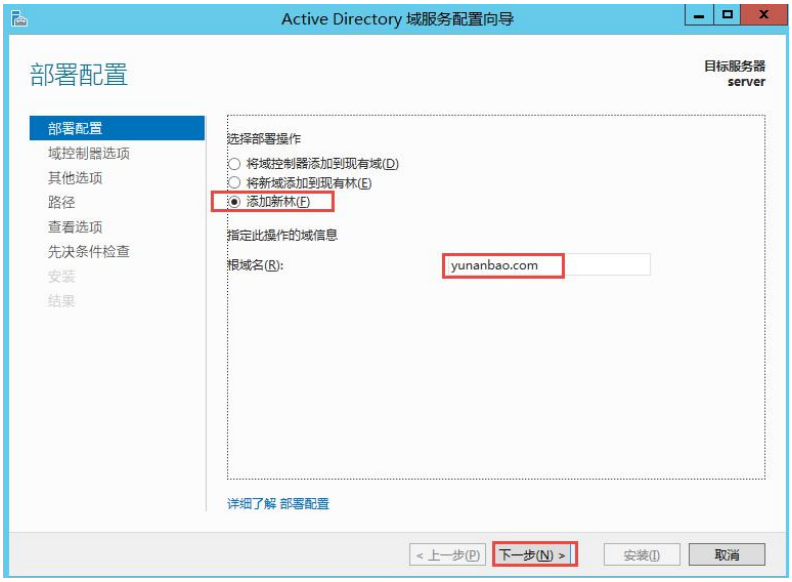


图 D-12

D.2.3 域控制器选项

域控制器选项，根据需求选择林功能级别，和域功能级别。

需要目录服务还原模式（DSRM）密码才能登入未运行 ADDS 的域控制器。指定的密码必须满足密码策略的密码复杂性要求。强密码需要大小写字母、数字和服务的组合。然后点击<下一步>，如图 D-13 所示。

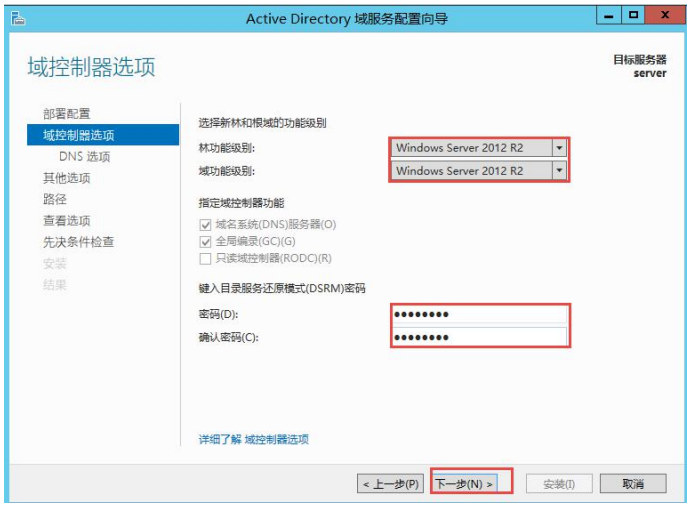


图 D-13

D.2.4 DNS 选项

安装 DNS 服务器时，应该在父域名系统 (DNS) 区域中创建指向 DNS 服务器且具有区域权限的委派记录。委派记录将传输名称解析机构和提供对授权管理新区域的新服务器对其它 DNS 服务器和客户端的正确引用。由于本机父域指向的是自己，无法进行 DNS 服务器的委派，不用创建 DNS 委派。点击<下一步>，如图 D-14 所示。

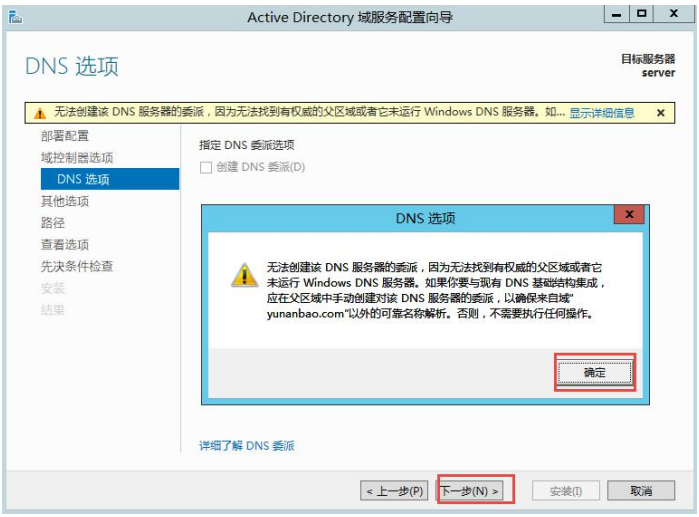


图 D-14

D.2.5 其它选项

确保为域分配了 NetBIOS 名称，并在必要时修改该名称。点击<下一步>，如图 D-15。

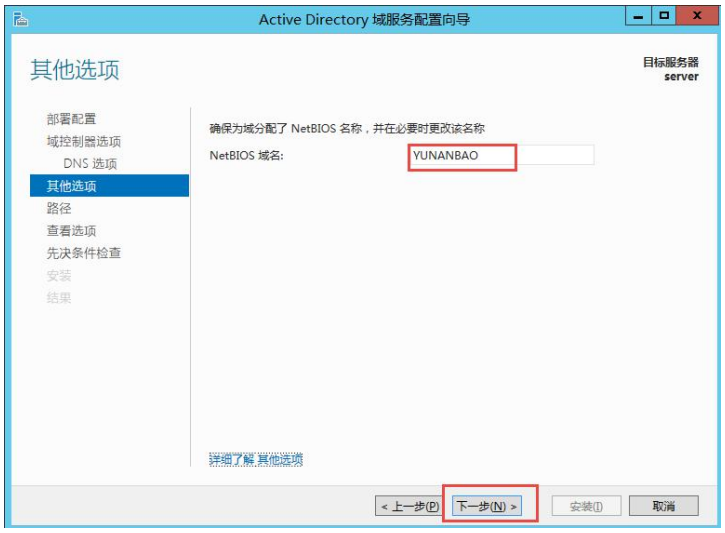


图 D-15

D.2.6 路径配置

指定 ADDS 的数据库，日志文件和 SYSVOL 的位置。点击<下一步>，如图 D-16 所示。

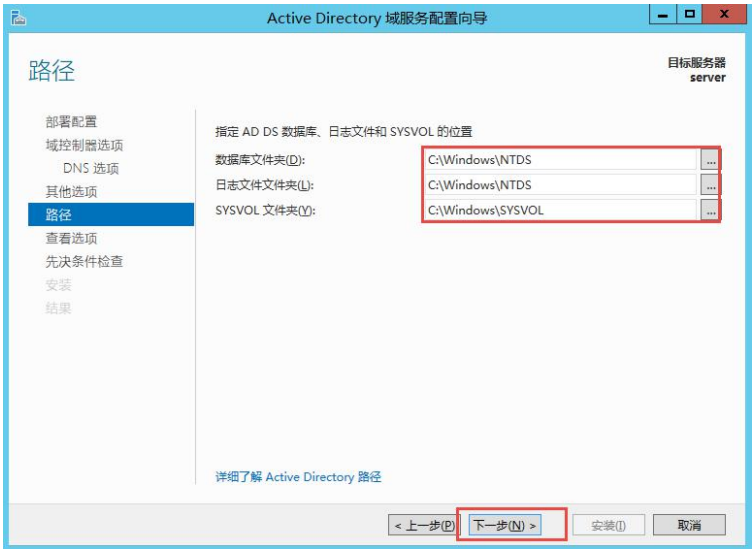


图 D-16

D.2.7 查看选项

检查为 AD 域配置的信息。点击<下一步>，如图 D-17 所示。

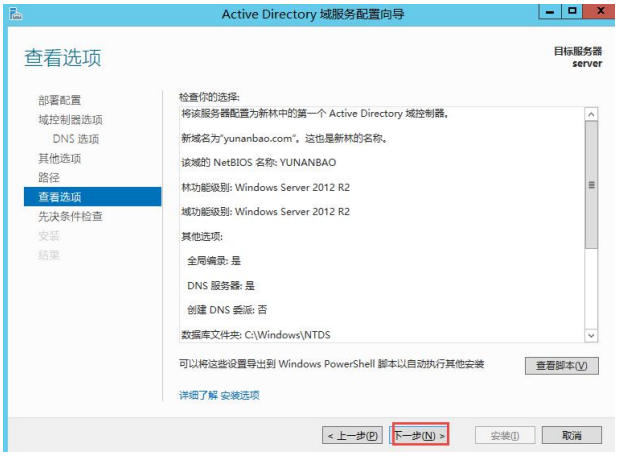


图 D-17

D.2.8 先决条件检查

等待服务器检查，先决条件检查成功通过。点击<安装>开始安装 AD 域。如图 D-18 所示。

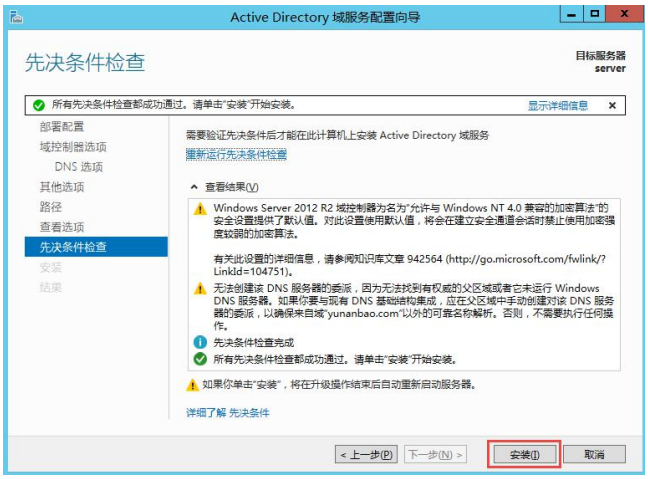


图 D-18

D.2.9 安装完成

安装完成之后，服务器会要求重启。如图 D-19 所示。

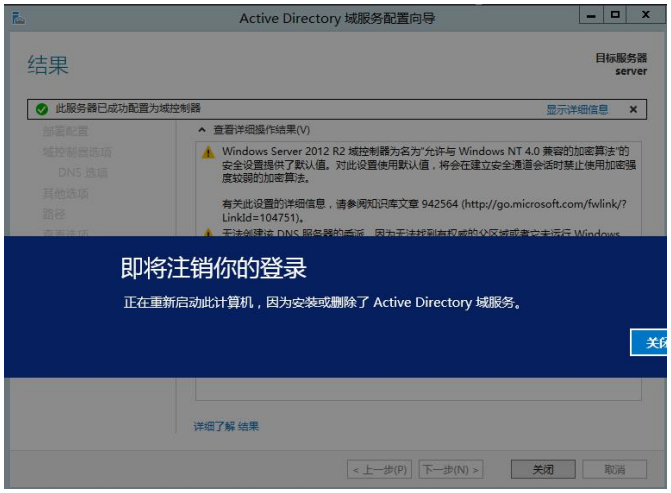


图 D-19

D.2.10 登入 AD 域

安装 AD 域之后，该服务以域用户登入服务器。登入之后服务器信息如图 D-20 所示。

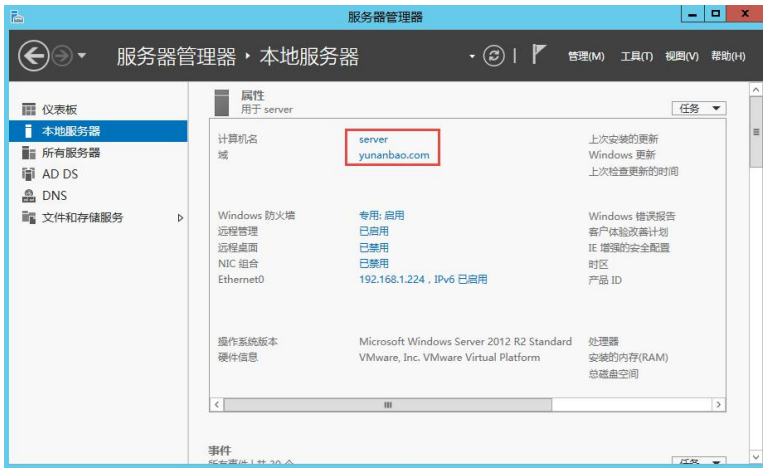


图 D-20

D.2.11 AD 域管理中心

通过服务器管理器，选择 ADDS，点击<工具>,点击 <ActiveDirectory 管理中心>进入 AD 域管理中心。如图 D-21 所示。

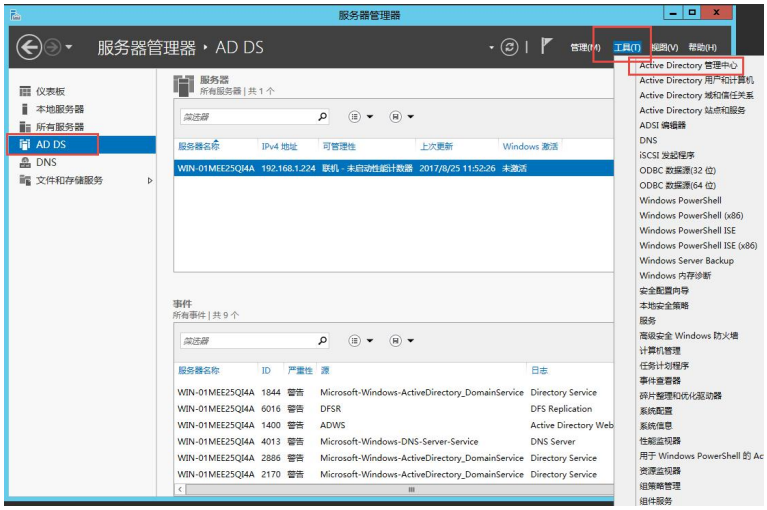


图 D-21

D.2.12 新建组织单位

打开 AD 域管理中心。选择（本地），点击<新建>，点击<组织单位>新建组织单位。如图 D-22 所示。

图 D-22

D.2.13 组织单位信息

新建组织单位，名称（该文档以成都西维数码科技有限公司为例）。该组织单位的 DN 为 OU 成都西维数码科技有限公司，DC=west，DC=cn。如图 D-23 所示。

图 D-23

附录 E Rsyslog 服务器安装与配置

对于包括 Linux 系统，Windows 服务器，路由器，交换机及其它主机能在网络上发送日志信息的这类设备，日志服务器都可以用作于它们在网络上的重要日志监控点。通过日志服务器，你能从不同的主机及设备过滤和合并日志信息于一个单一的位置，所以你能很容易的查看及存档日志信息。

在大多数据的 Linux 发行版中，rsyslog 是一个预先安装的标准日志后台进程。在客户端/服务端的系统配置中，rsyslog 能扮演两个角色;作为一个日志服务器能从其它设备收集日志信息，而作为一个日志客户端，rsyslog 发送自己内部日志信息到远程日志服务器。

E.1 Rsyslog 安装配置

E.1.1 syslog 基础

当通过 syslog 机制来收集日志时，有 3 个必须要考虑到的重要事情：

（1）设备: 监听何种类型的进程

设备定义了一种用来对内部系统进程进行分类的方法，linux 中的一些常见的设备包括:

auth: 身份验证相关的消息（登录时）

cron: 进程或应用调度相关的消息

daemon: 守护进程相关的消息（内部服务器）

kernel: 内核相关的消息

mail: 内部邮件服务器相关的消息

syslog: syslog 守护进程本身相关的消息

lpr: 打印服务相关的消息

local0 - local7: 用户自定义的消息 （local7 通常被 Cisco 和 Windows 服务器 使用）

（2）严重性 （优先） 级别: 收集何种级别的日志消息

严重性（优先）级别有固定的标准缩写和指代的值，其中的数字 7 具有最高的级别，这些级别包含了：

emerg: Emergency（紧急）- 0

alert: Alerts （报警）- 1

crit: Critical (关键）- 2

err: Errors （错误）- 3

warn: Warnings （警告）- 4

notice: Notification （通知）- 5

info: Information （消息）- 6

debug: Debugging （调试）- 7

（3）目标: 发送或记录日志消息到何处

目标语句会让一个 syslog 客户端来执行以下三个任务之一：

保存日志消息到一个本地文件；

通过 TCP/UDP 将消息路由到远程的 syslog 服务器中；

将其发送到一个标准输出中，例如控制台。

E.1.2 配置 syslog

rsyslog 一般是预先就安装于 linux 系统的发行版上的，rsyslog 后台进程默认不能接受外部信息的，但可以通过配置它的配置文件/etc/rsyslog.conf 来配置。

打开/etc/rsyslog.conf 文件，去掉红色划出两行行首的#字符，如图 E-1 所示。

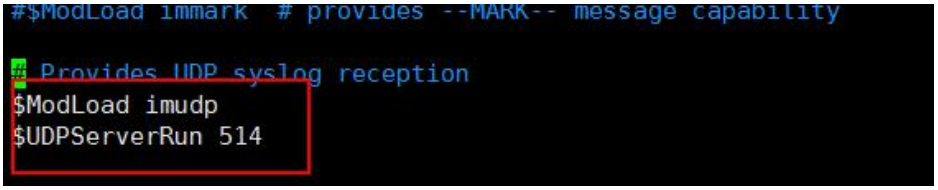


图 E-1

创建一个模板，告诉 rsyslog 后台进程怎样记录从其它客户端接收的信息

在 GLOBAL DIRECTIVES 内容块的前面追加如下模板，如图 E-2 所示。

图 E-2

$template RemoteLogs 指令（“RemoteLogs” 可以为其它的描述的名字）迫使 rsyslog 后台进程隔开本地/var/log/下文件去写日志信息。而日志文件名则依据发送远程日志的机器名及应用程序名来定义。第二行（*.* ?RemoteLogs）暗含运行用模板 RemoteLogs 于所有的接收日志。& ~则告诉 rsyslog 后台进程停止进一步的去处理日志信息,即不对它们进行本地化写入，它是代表一个重定向规则。如果没有这一行，则意味着接收到的日志会写入两次，一次如前两行写的方式写，第二次则以本地日志记录的方式写入。运行这个规则的另一个结论则是日志服务器自己的日志信息只会写入到依照机器主机名命名的文件中。

E.1.3 配置防火墙

iptables -I INPUT -p udp --dport 514 -j ACCEPT#对外开放 udp514 端口
echo "iptables -I INPUT -p udp --dport 514 -j ACCEPT">> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local#将防火墙配置写入开机文件，启动时加载防火墙配置
如图 E-3 所示。

图 E-3

E.1.4 设置开机自启 rsyslog 服务

systemctl enable rsyslog #开机启动 rsyslog 服务
systemctl start rsyslog #启动 rsyslog 服务
systemctl status rsyslog#查看 rsyslog 启动状态
如图 E-4 所示。

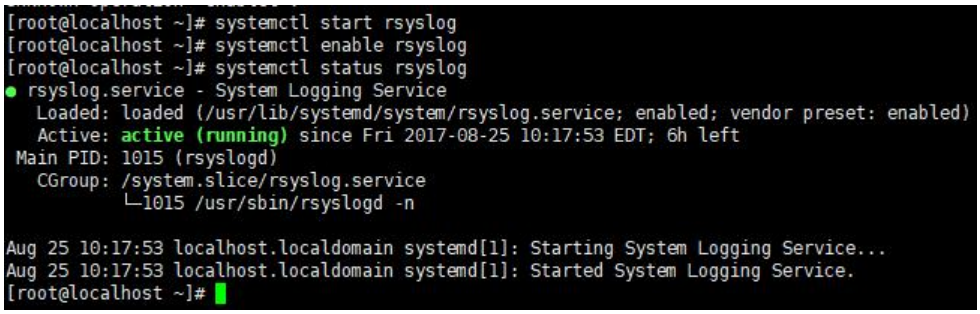


图 E-4