保密级别：□绝密 □机密 □秘密 □内部公开 ■公开

旗舰版堡垒机-UHAS
用户手册

优刻得科技股份有限公司

文档修订记录

版本编号或者更改记录编号	*变化状态	简要说明（变更内容和变更范围）	日期	变更人	审核日期	审核人
V1.0	A	旗舰版堡垒机 3.4.8.0 版本	2021.4.11	薛姣	2020.4.21	安全产品部

*变化状态：A——增加，M——修改，D——删除

目 录

1 前言

1.1 名称解释

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。

1.2 适用范围和先决条件

优刻得旨在为 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

1.3 支持信息

优刻得科技股份有限公司

网址：http://www.yunanbao.com.cn

技术支持：4000188133

2 产品简介

2.1产品概要

堡垒机是优刻得科技股份有限公司经过多年研发，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。

堡垒机系统为政府部门、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。

部署堡垒机，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。

2.2应用场景

满足政策、法规需求：堡垒机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。部署堡垒机后，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，部署堡垒机，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：堡垒机能对 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：堡垒机的应用托管功能，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。

3 桌面

桌面由不同的控制板组成，控制版的数据来源于对应权限的模块，当有相应控制板权限时则显示对应的控制板内容。Admin 拥有最高权限。如图 3-1

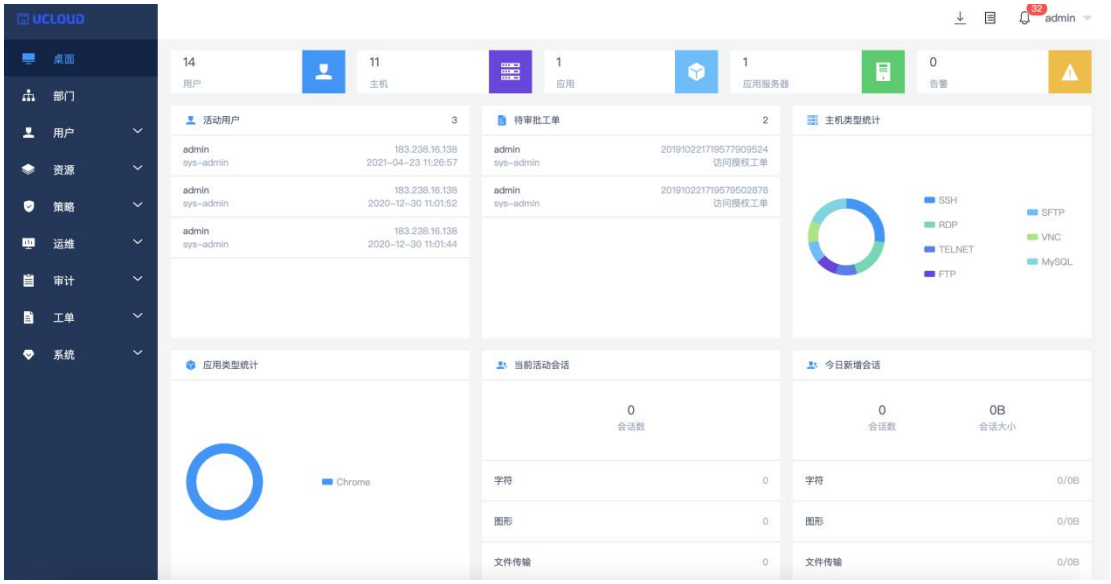


图 3-1

4 部门

部门用于划分组织结构，可在每个部门下创建多个部门，以树状图结构展示出。如图 4-1

注意事项：

1 主机资源或者用户被添加到任何一个新建的部门后，此时删除该部门，该部门中的用户和资源会一并删除。

2 总部为默认部门无法删除。

3 当设置部门的安全码之后，部门的管理员在进行导出资源、用户等数据时，会自动使用部门安全码进行加密

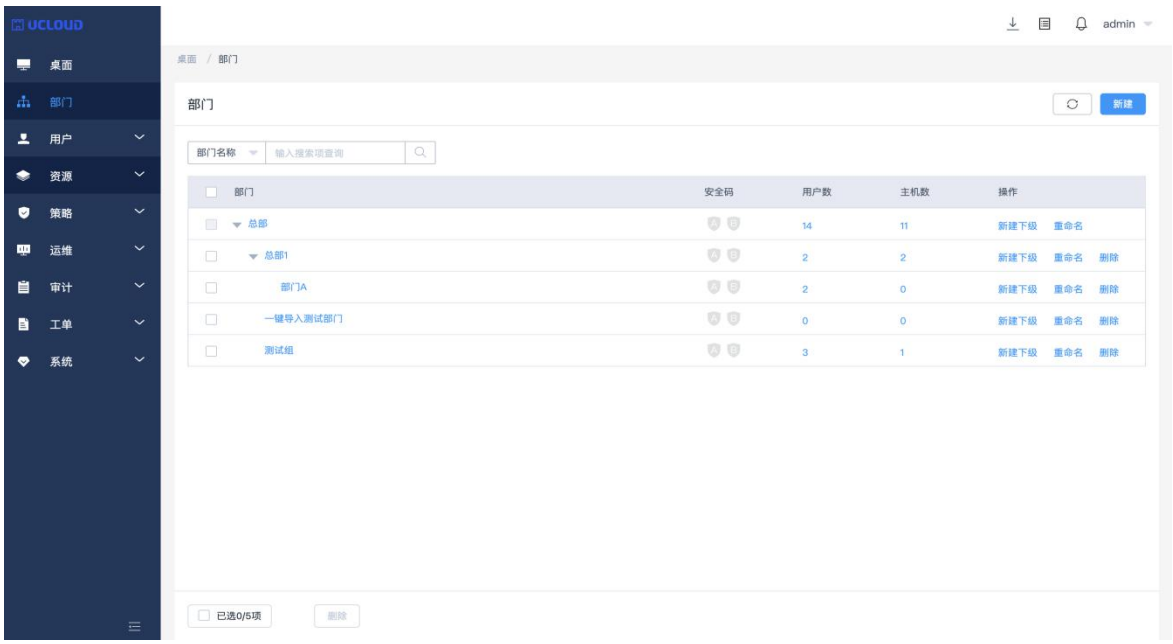


图 4-1

5 用户

5.1 用户管理

5.1.1 用户配置

在用户管理页面可为堡垒机添加用户并分配角色，创建完成后点击用户后方的管理，可为该用户配置多因子登录方式，用户的有效期，登录的时间段限制，登录时的 IP 地址限制，Mac 地址限制。如图 5-1

当用户开启多因子登录时，该用户不可使用密码登录方式登录，支持开启多个多因子方式登录。

图 5-1

5.1.2 批量配置

堡垒机支持批量配置用户，勾选需要配置的用户后，点击更多，可批量更改。可支持批和单个禁用用户。用户为禁用状态时，该用户无法登陆堡垒机。如图 5-2

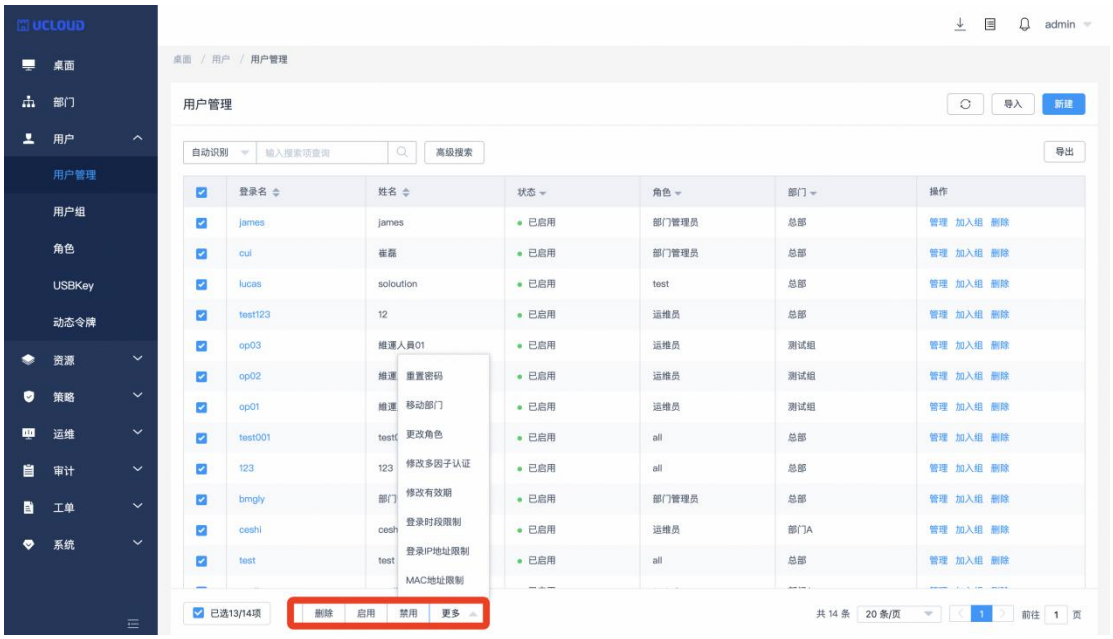


图 5-2

5.1.3 用户导入

支持用户导入，导出用户模板后按照模板格式添加用户可成功导入，目前导入用户的格式支持 xls，xlsx，csv 格式文件。如图 5-3

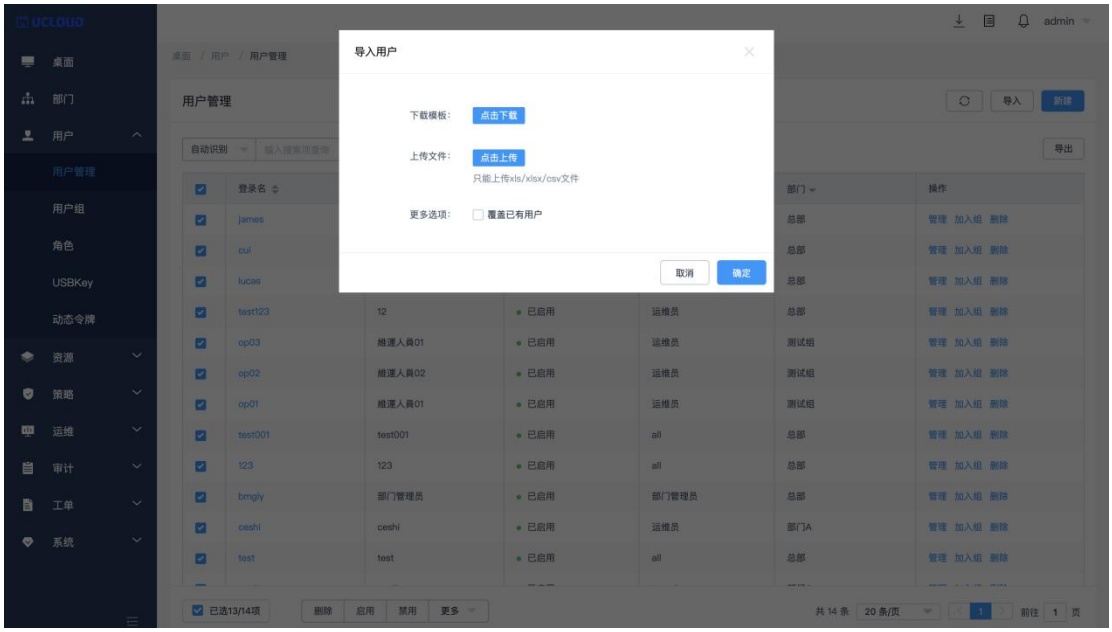


图 5-3

5.2 用户组

用户组用于把用户分组后，实现批量授权的功能，可创建多个组，点击编辑组成员可为该组添加用户。如图 5-4

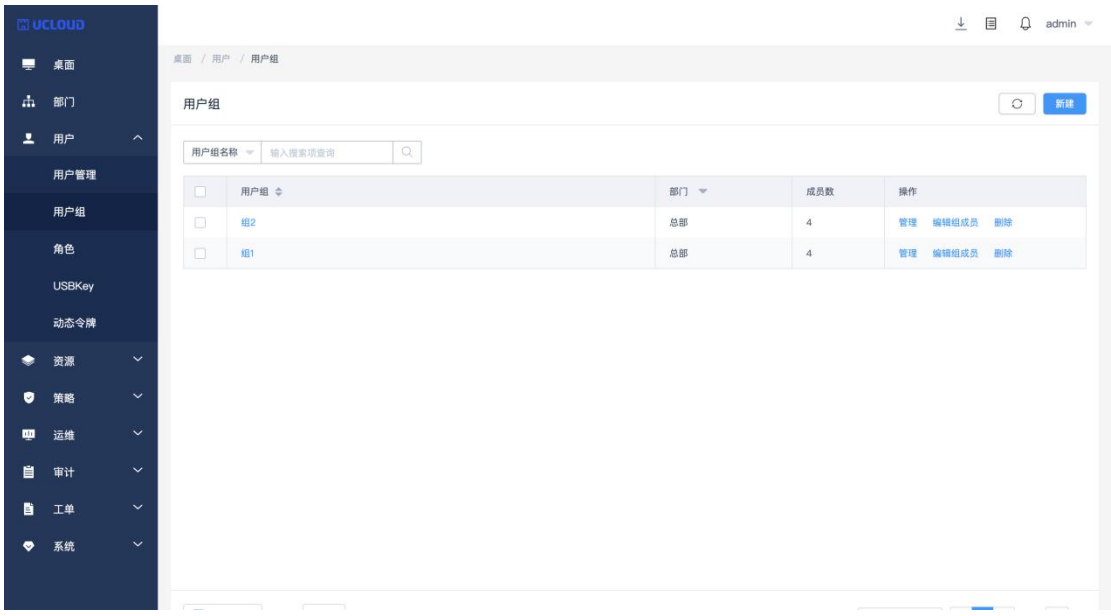


图 5-4

5.3 角色

进入用户-角色模块，可查看到当前拥有的所有角色，堡垒机默认角色为 4 个，部门管理员，审计管理员，策略管理员和运维员，角色拥有不同的权限，可新建自定义角色，并可随意分配给该角色权限。如图 5-5

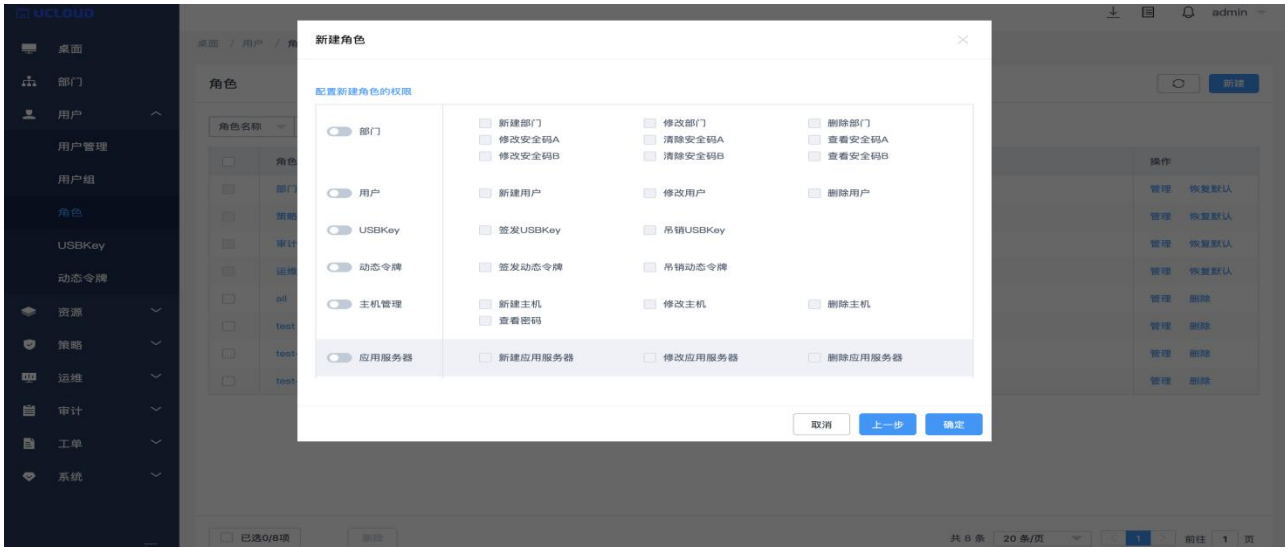


图 5-5

【角色控制范围】

新建角色的时候可以根据实际情况自行设置角色管理者，即如下图所示：

图 5-6

角色管理者支持多选，且下拉备选项的显示范围即“功能权限开启新建用户或修改用户权限的角色”。

若已开启了设置角色管理者，角色详情页面显示设置角色管理者为开启状态，并显示角色管理者，如下图：

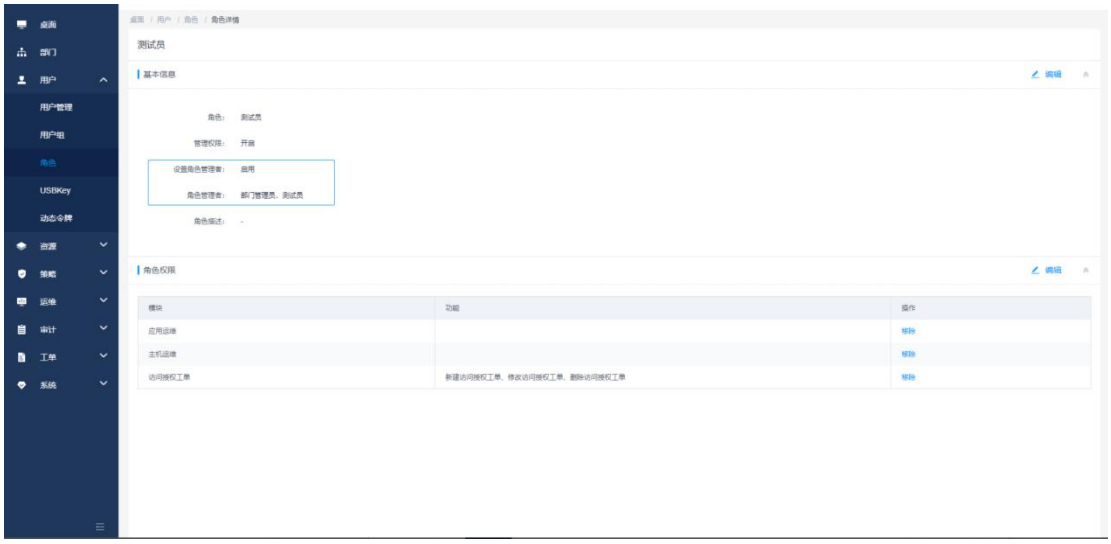


图 5-7

若未开启了设置角色管理者，角色详情页面显示角色管理者为禁用状态，且不显示角色管理者，如下图：

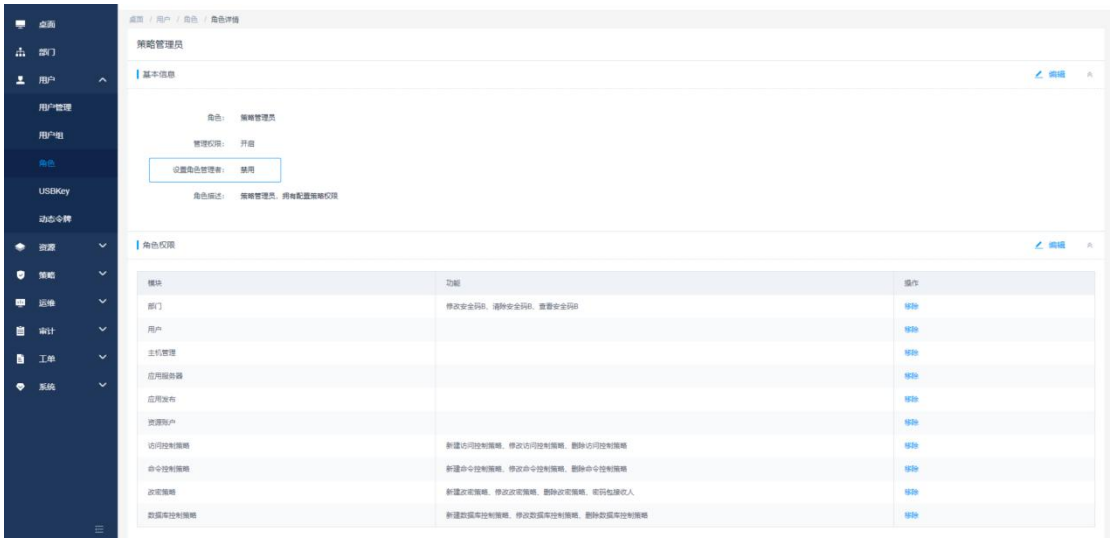


图 5-8

【注】

- 如果不开启角色管理者，则表示不限制角色管理者，那么当用户创建（或修改）用户时，可以设置（或修改）用户为该角色；
- 如果开启角色管理者，则表示仅角色为角色管理者的用户（在用户有“新建用户”功能权限的情况下）能够创建该角色的用户，或者是（在用户有“修改用户”功能权限的情况下）将其他用户修改为该角色。

5.4 多因子 USB key

当用户配置好可用多因子 USBkey 登录时，可在 USBkey 模块中中为该用户签发 USBksy，插入 USBkey 后，选择需要签发的用户和正确 PIN 码，签发成功后，被签发的用户可正常使用 USBkey 方式登录堡垒机。如图 5-9、图 5-10

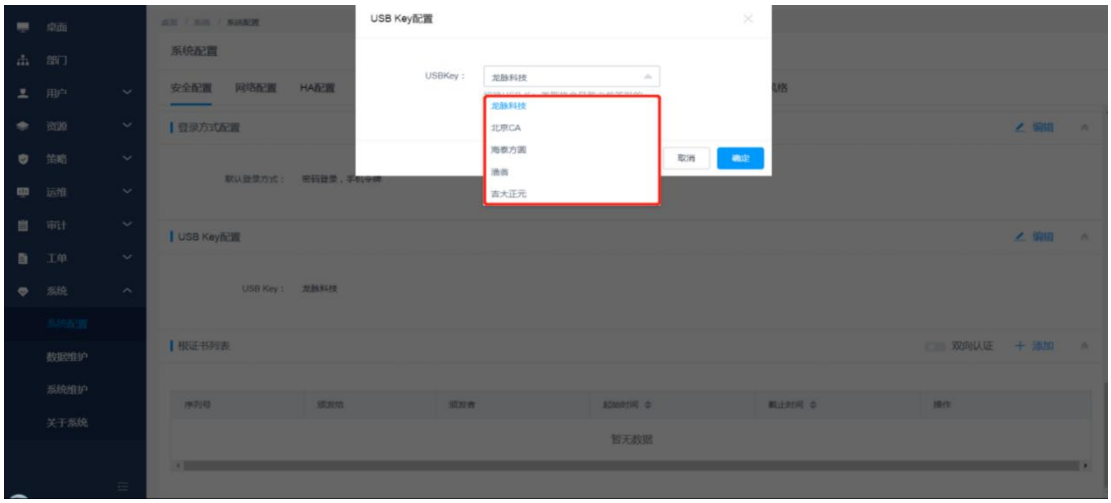


图 5-9

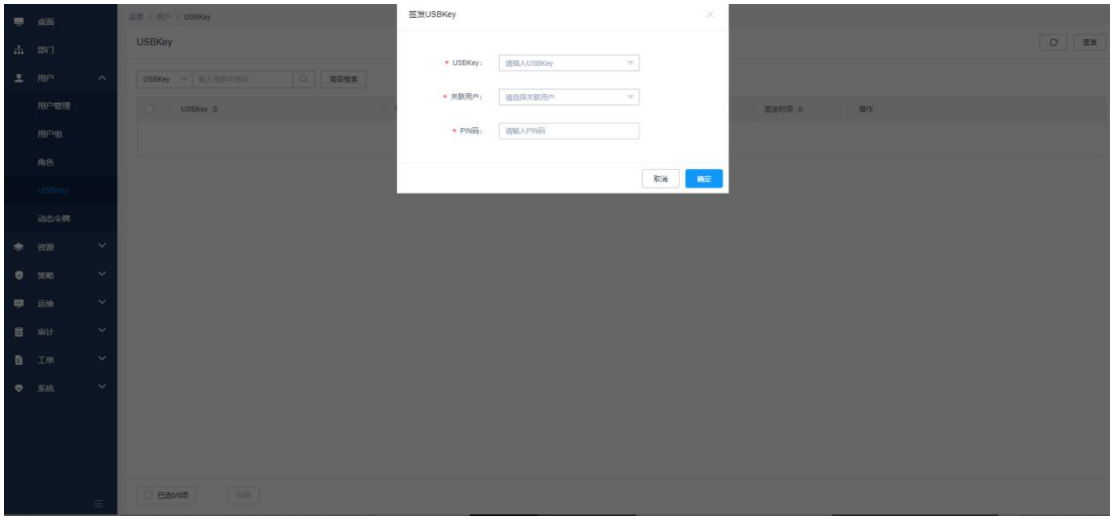


图 5-10

吉大正元 USBKey 签发登录需要选择证书，证书必须与关联用户一直才能登录成功。如图 5-11

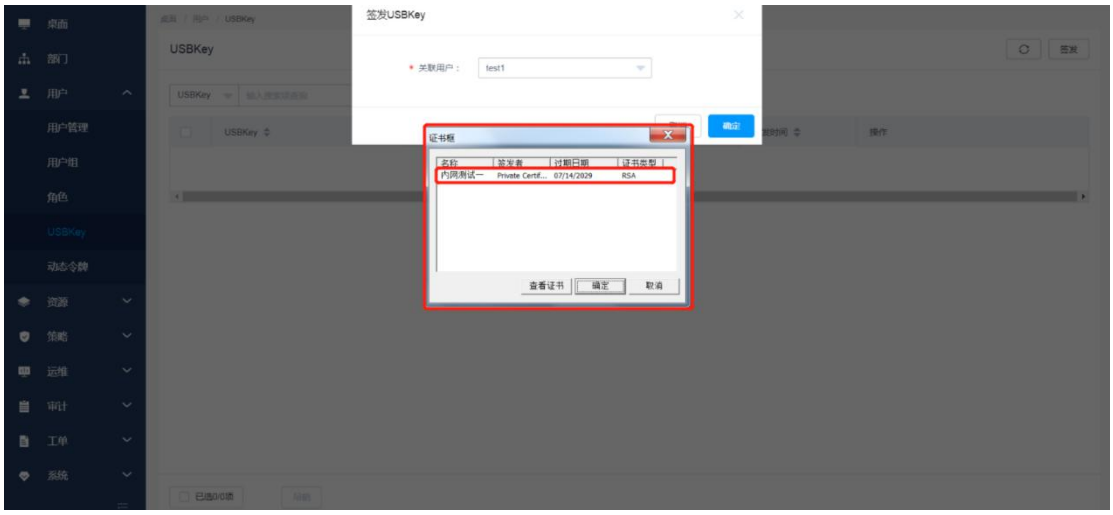


图 5-11

5.5 多因子动态令牌

当用户配置好可使用多因子动态令牌登录时，可在动态令牌中为该用户签发动态令牌。点击签发后输入标识和正确的秘钥并选择要关联的用户，点击确定，被签发的用户登录堡垒机时可使用多因子动态令牌方式登录。且动态令牌支持导出导入的方式添加保存。如图 5-12

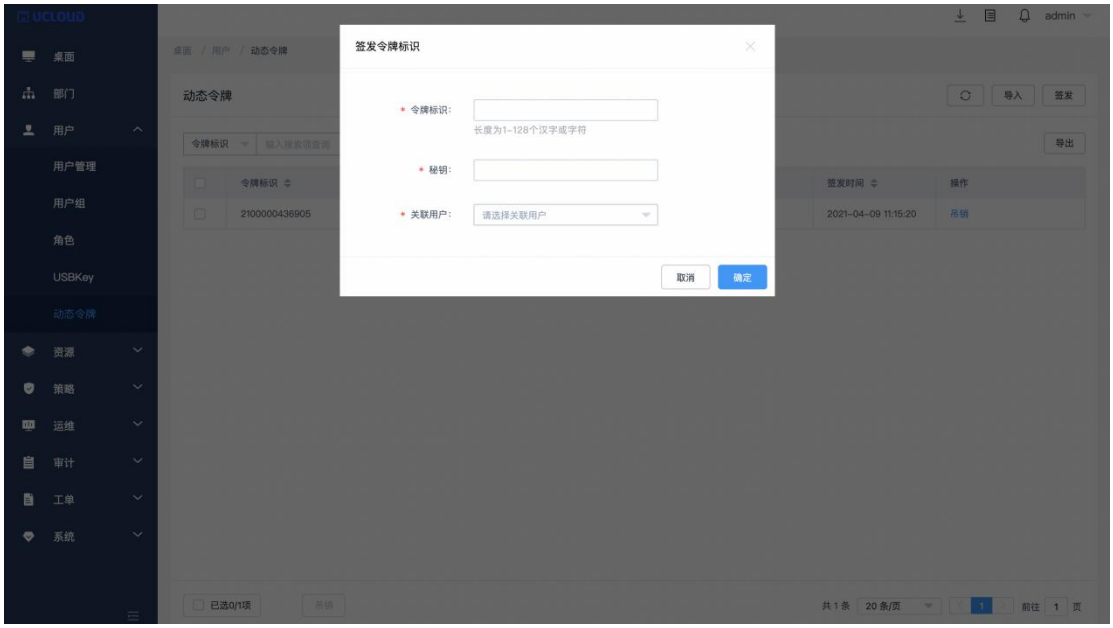


图 5-12

5.6 多因子手机令牌

手机令牌登录做为登录堡垒机的登录方式之一，用户可在个人中心-手机令牌中按照步骤绑定，绑定成功后可使用手机令牌登录方式登录堡垒机中。如图 5-13

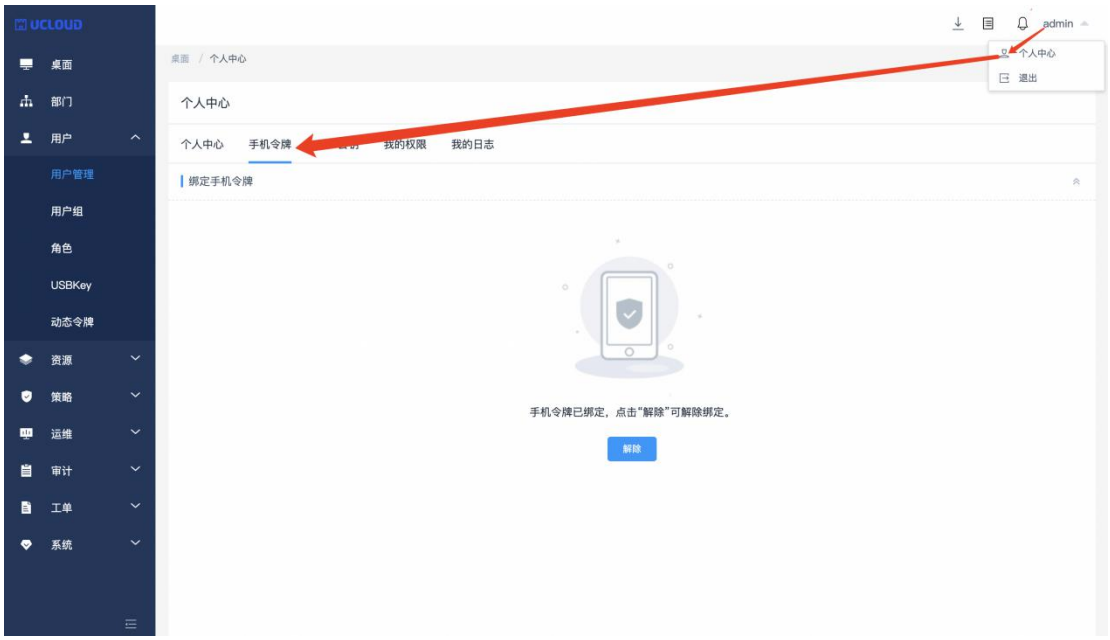


图 5-13

5.7 手机短信登录

在创建用户时为用户添加手机号码（该号码用户登录堡垒机之后可在个人中心自己设置）或者点击已创建的用户后方的管理为用户添加手机号码，并在登录配置中配置可以使用多因子手机短信即可。如图 5-14

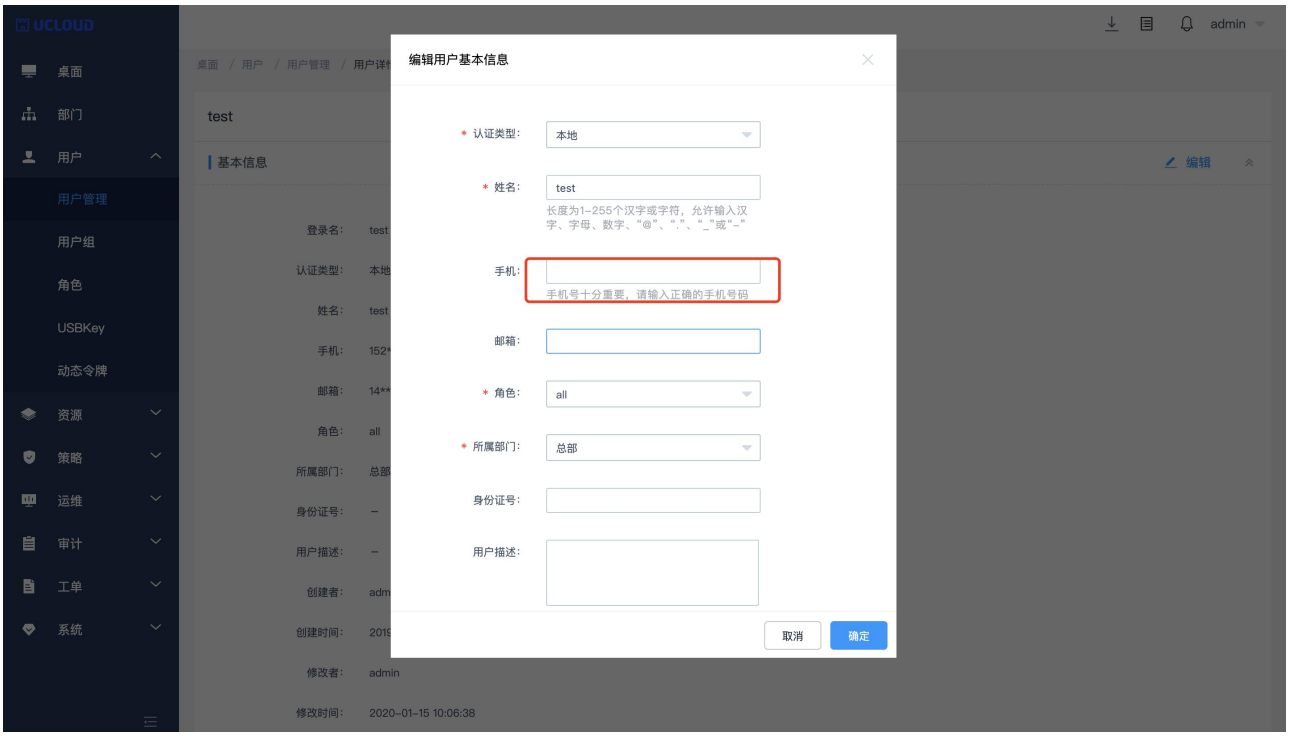


图 5-14

6 资源

6.1 主机管理

6.1.1 新建主机

进入资源-主机管理，可展示当前所被堡垒机管控的所有主机，点击新建后可添加新的资源主机。如图 6-1

图 6-1

新建主机资源时涉及主机地址为 IPv6 以及 IPv4 主机地址协议为 MySQL，DB2，Oracle，SQL Server 时不支持账户的验证，即隐藏验证按钮，如下图 6-2，图 6-3：

图 6-2

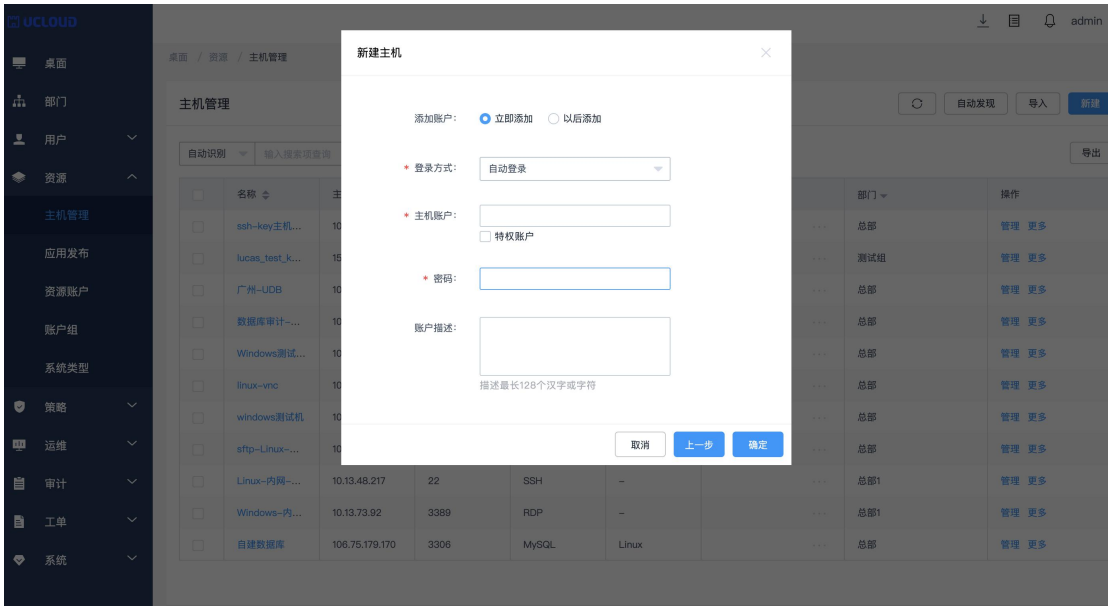


图 6-3

6.1.2 主机导出/导入

堡垒机支持批量导出/导入用户，可点击导出后按照导出的模板规范填写参数，正确填写后可批量导入主机，目前支持导入的文件格式有 xsl/xlsx/csv。当进行导出的主机所在部门有安全

密码时，则在本地打开的时候需要输入正确的加密密码。勾选验证账户时，则可在任务中心查看主机账户正常/异常数。导入界面如图 6-4

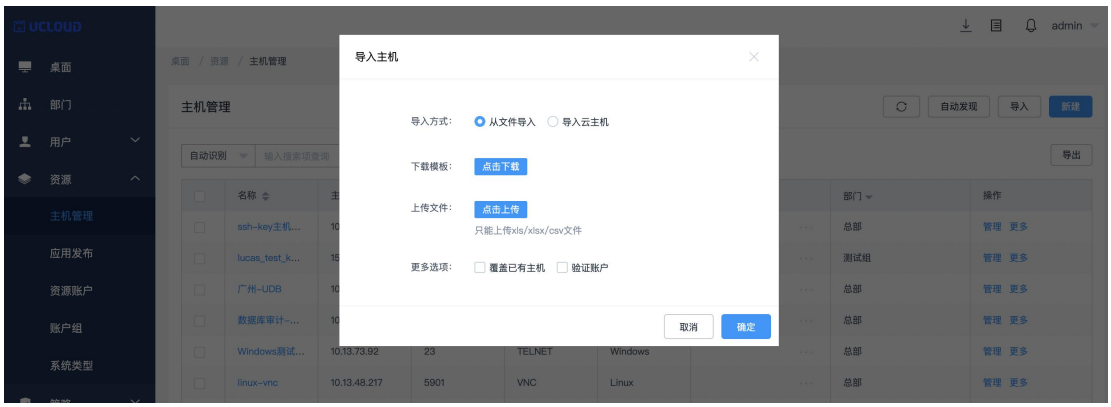


图 6-4

堡垒机支持云主机导入，选择云平台后，输入正确的 public_key 和 private_key 后，当点击全部导入时则导入全部主机到堡垒机，点击让我选择时可手动选择要导入的主机，导入后可在主机管理中查看该主机。如图 6-5

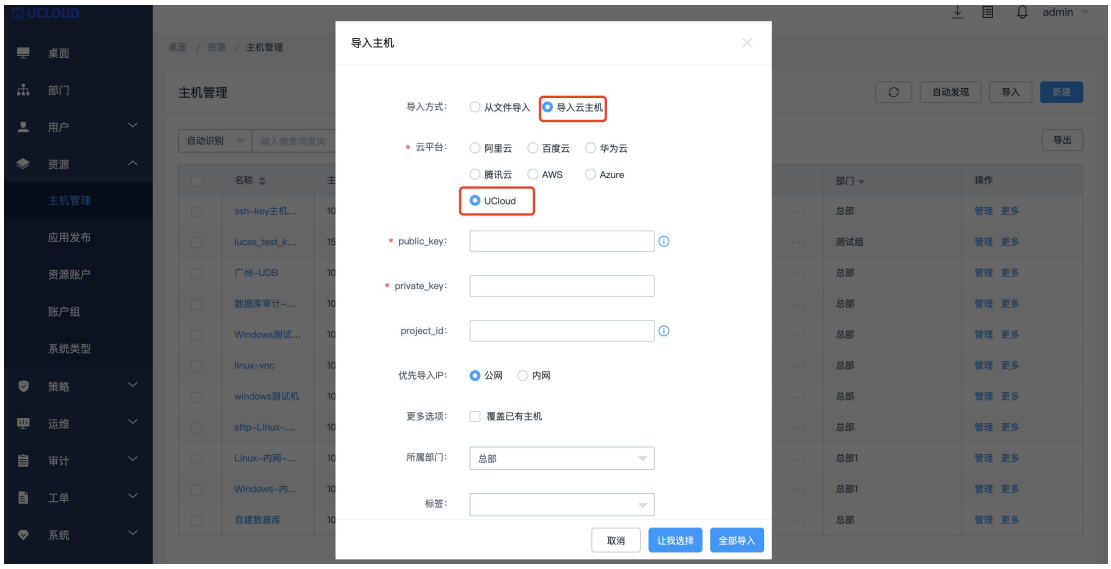


图 6-5

6.2 应用发布

6.2.1 应用服务器

创建应用发布之前，需要为该应用创建应用发布服务器，需要输入正确的服务器地址，选择服务器类型，当服务器类型选择完成后，程序启动路径会自动填写。如图 6-6

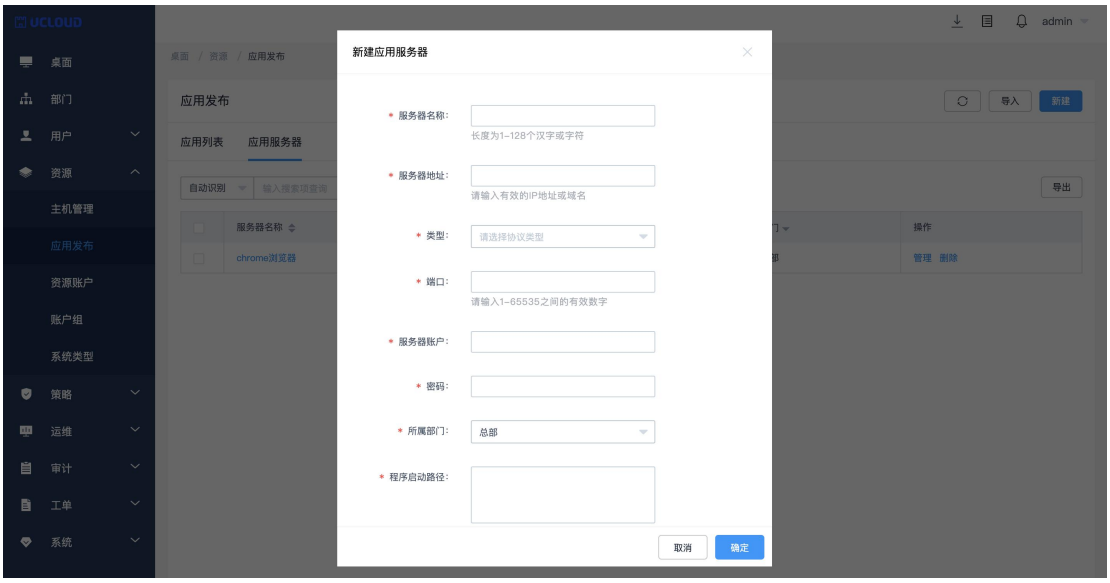


图 6-6

6.2.2 应用

应用发布服务器创建完成后，可创建应用并且关联应用服务器，输入正确的应用地址和端口后点击下一步添加账户即可。如图 6-7

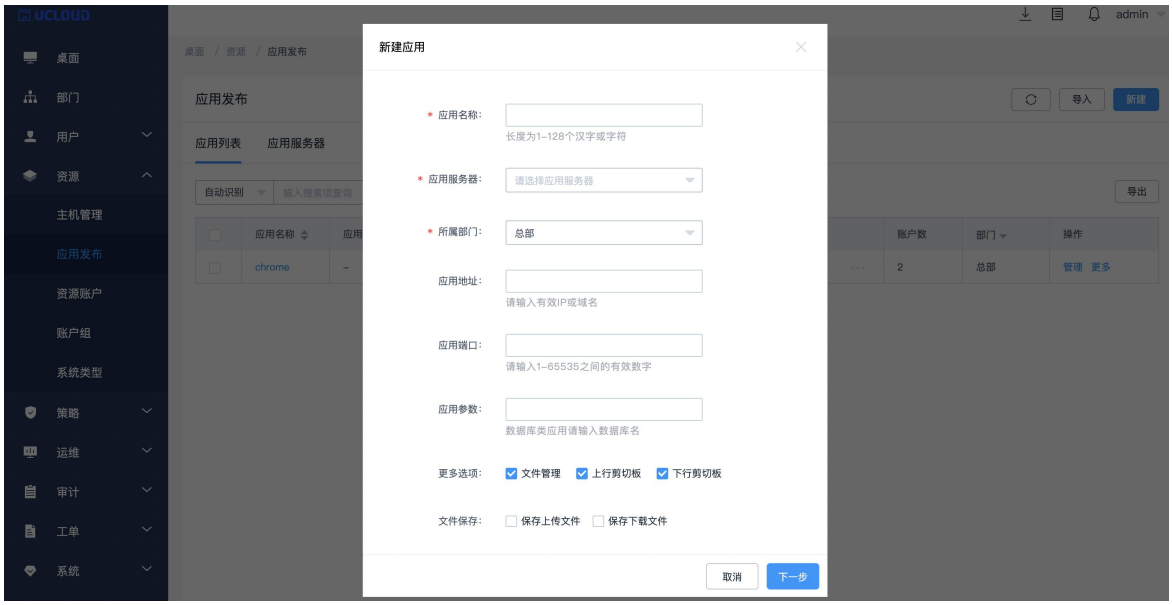


图 6-7

6.2.3 应用导出/导入

支持应用发布服务器和应用导出/导入，可导出模板后按照模板格式填写正确参数后导入，导入应用时，前提需要有对应的应用发布服务器，否则无法直接导入应用。目前支持的导入文件格式有 xls/xlsx/csv。当进行导出的用户所在部门设置了安全码时，则在本地打开的时候需要输入正确的部门安全码。如图 6-8

图 6-8

6.3 资源账户

每创建一个主机或应用后，主机中会自带一个空账户【Empty】，该账户用于手动登录。除此之外，可为主机创建多个账户，点击新建，选择关联的资源主机和登录方式后输入正确账户密码即可。当添加和配置好正确的 sshkey 时，可直接使用 sshkey 免密码登录。支持批量删除可批量验证所选择的账户正常/异常状态。如图 6-9

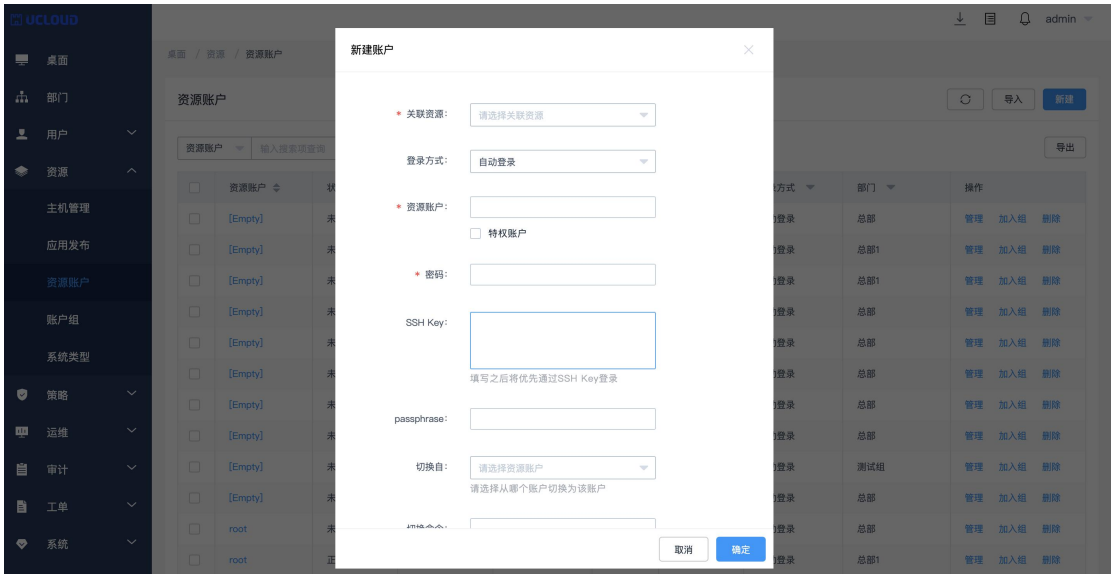


图 6-9

注：

登录方式可选择自动登录，手动登录，提权登录。当选择提权登录时，需要选择提权到那个账户，提权时的切换命令，最后输入正确密码即可。

特权账户用户改密策略改密，勾选特权账户时，该账户属于特权账户。

账户导出/导入与应用导入操作相同。

若资源账户关联的主机资源涉及主机地址为 IPv6 以及 IPv4 主机地址协议为 MySQL，DB2，Oracle，SQL Server 时不支持账户的验证，即隐藏验证按钮，如下图 6-10：

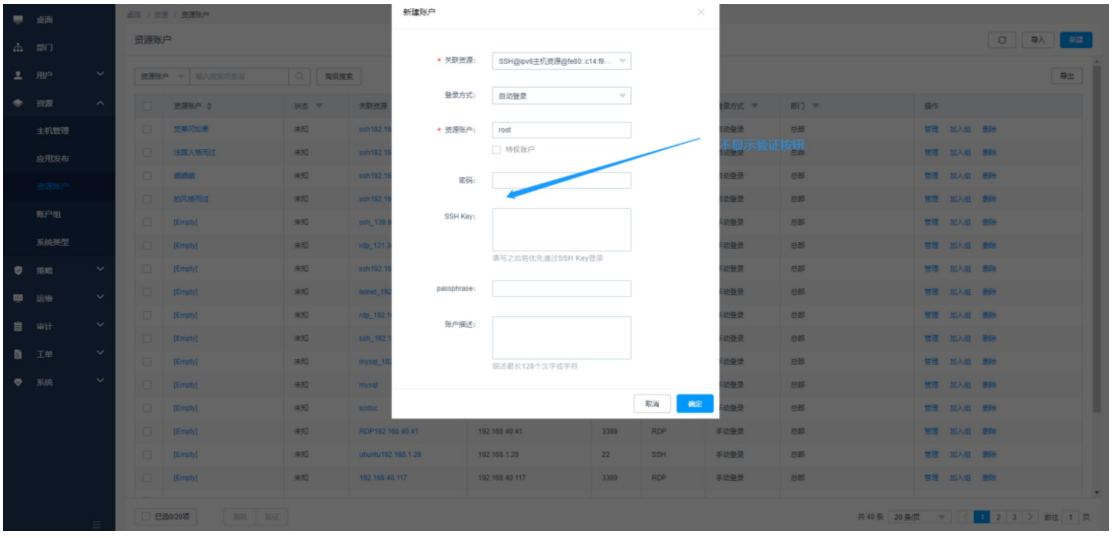


图 6-10

6.4 账户组

账户组可将账户打包分组，实现批量授权的功能，可创建多个账户组，创建完成后可为该组增加/删除账户，支持批量删除组和批量验证账户组中账户正常/异常的状态。如图 6-11

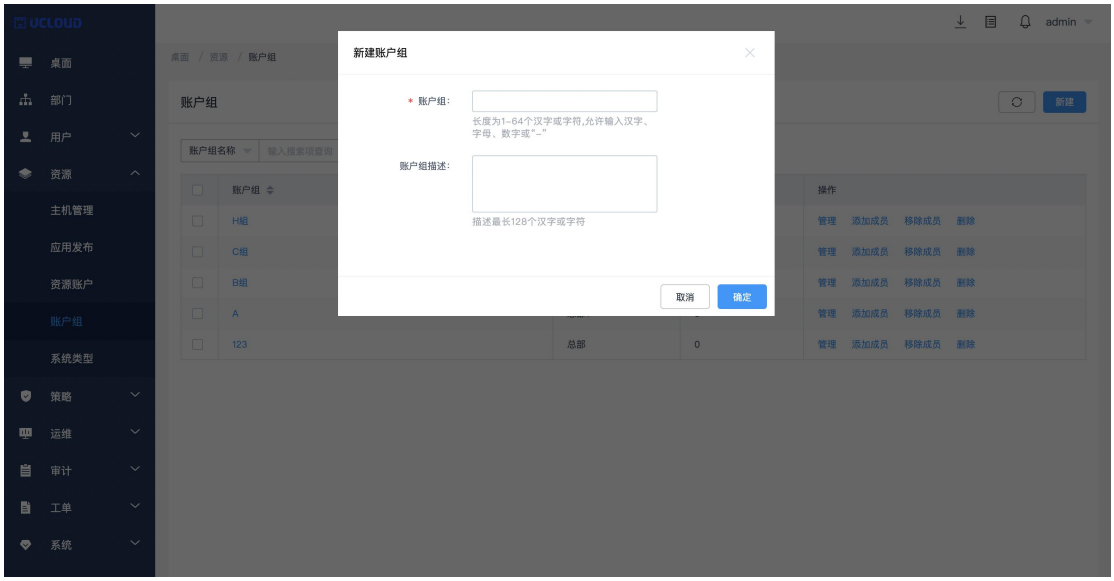


图 6-11

6.5 系统类型

进入资源-系统类型，可查看到堡垒机内置系统类型，点击新建后可创建新的系统类型，如图 6-12

图 6-12

说明：

参数为非必填，每个参数最多添加 5 个。

改密参数：设置改密的命令和成功返回。

提权账户改密参数：设置提权账户改密的命令和成功返回。

配置备份参数：设置配置备份的命令和成功返回。

7 策略

7.1 访问控制策略

7.1.1 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，可以让指定的用户在指定的时间内访问指定的主机资源。且支持 IP 地址限制，文件传输，剪切板上下行，水印显示等。选择完成后关联用户和资源，所关联的用户就能使用关联的资源进行运维。如图 7-1

图 7-1

当账户存在于多个策略时，并且策略中选择的功能不同，可通过拖动策略，更改优先级。支持策略启用/禁用功能。如图 7-2

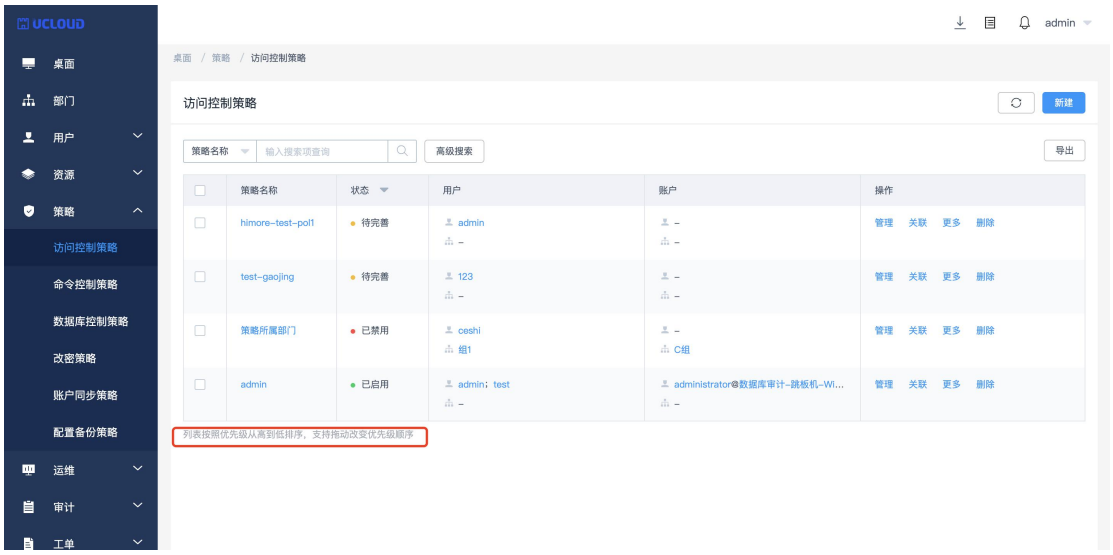


图 7-2

7.1.2 访问控制策略双人授权

添加双人授权候选人后，当策略内的用户访问策略内的资源时，需要候选人现场输入密码。可在访问控制模块点击策略后的更多选项添加双人授权候选人。如图 7-3

图 7-3

7.2 命令控制策略

7.2.1 命令控制策略

命令控制策略用于控制指定的用户登录指定的字符类型协议后，当执行策略指定的命令时，会触发相应的执行动作限制，执行动作分为：允许执行，拒绝执行，断开连接（断开运维会话），动态授权（生成工单申请授权）。可配置该策略有效期，不在有效期内时，策略状态为未生效。如图 7-4

图 7-4

配置完成后添加命令或命令集，添加命令支持通配符，最后关联用户和资源即可。如图 7-5

图 7-5

7.2.2 命令集

命令集可添加堡垒机内置的一些命令，用于方便添加。可直接关联到命令控制策略中。如图 7-6

图 7-6

7.3 数据库控制策略

7.3.1 数据库控制策略

数据库控制策略用于控制指定的用户登录到指定的数据库类型资源后执行的一些操作，当登录数据库资源且执行策略中关联的规则时，会触发相应的执行动作限制，执行动作分为：允许执行，拒绝执行，断开连接（断开运维会话），动态授权（生成工单授权）。可配置该策略有效期，不在有效期内时，策略不会拦截。如图 7-7

目前数据库控制策略只支持 MySQL，Oracle 两种数据库。

图 7-7

7.3.2 规则集

规则集可添加堡垒机内置的一些 sql 命令，规则集创建完成后可为规则集添加规则，关联到数据库控制策略中。如图 7-8

图 7-8

7.4 改密策略

7.4.1 改密策略

改密策略用于对主机内资源账户定时，定期进行改密，改密方式可选择生成不同密码（多个账户生成不同密码），生成相同密码（多个账户使用相同密码）和自定义相同密码（多个账户指定密码），改密方式为生成不同密码和生成相同密码时，可以指定生成密码的策略，如图 7-9。当选择定时执行和周期执行时可在指定的时间自动执行改密策略；改密策略执行完毕后，会将密码修改结果分开发给指定的用户，

图 7-9

注意：

1）支持改密策略改密的协议有：SSH ,MySQL，sql server，Oracle，RDP，Telnet。

2）选中允许修改特权账户密码时，才能修改特权账户的密码，否则特权账户密码不会修改，默认不选中

3）选中使用特权账户改密时，系统自动寻找账户对应资源的特权账户，通过特权账户修改密码，无特权账户时，自己修改自己密码，该选项默认选中

4）手动执行改密策略需要输入当前用户的登录密码

5）使用自定义改密策略时按照自定义改密策略创建密码；否则会生成 20 位的包含大小写字母、数字、特殊符号的密码

7.4.2 改密日志

改密策略执行完成后可在改密日志中查看改密详情。用户（具有下载改密日志权限）可通过下载日志到本地查看改密策略改密之后的密码（其他用户只能查看大致信息，无法看到具体的密码），下载与手动执行策略类似，需要输入操作用户的登录密码。如图 7-10

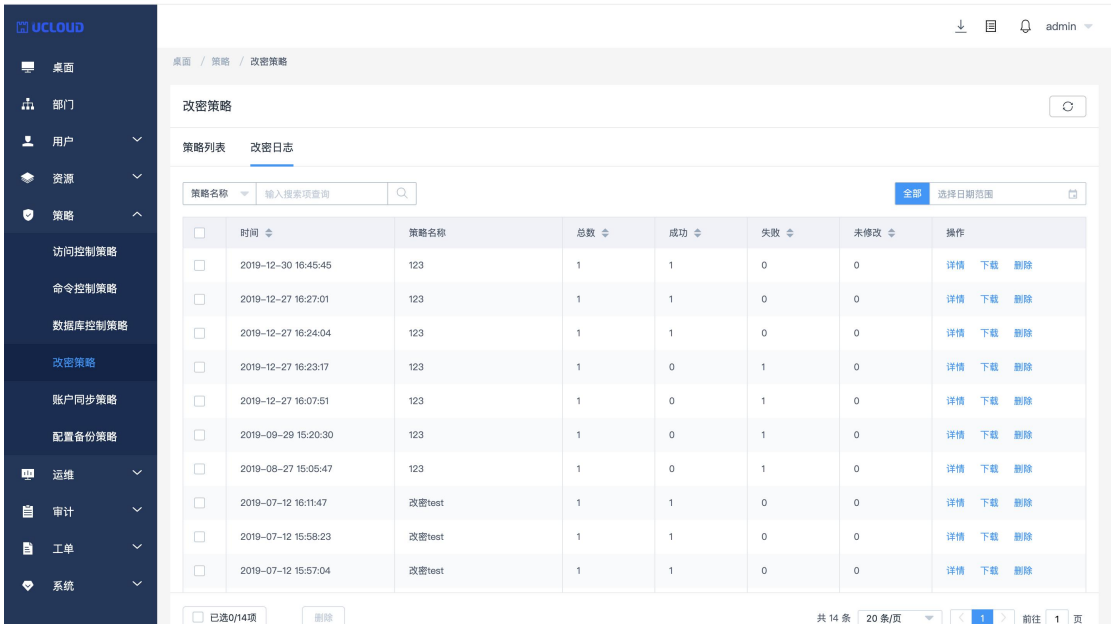


图 7-10

7.5 账户同步策略

7.5.1 账户同步策略

账户同步用户拉取或推送账户，当选择拉取账户时，会扫描主机内的所有账户，统计正常、非正常信息。选择推送账户时，将堡垒机录入的资源账户同步到目标主机，可进行更新主机密码，新建主机密码，或删除非堡垒机纳管账户的操作。如图 7-11

图 7-11

注意：

1）当选择同步动作为推送账户时，除选择执行账户时，还需要选择推送账户。

2）非纳管账户说明：主机内的账户没有添加到堡垒机内，该账户会被识别为非纳管账户。

3）账户同步策略只支持 SSH 协议。

7.5.2 执行日志

账户同步策略执行后，可在执行日志中查看详情。如图 7-12

图 7-12

7.6 配置备份策略

7.6.1 配置备份策略

为了方便网络设备上配置文件的备份，堡垒机支持网络设备配置备份策略。创建时执行方式可选择为手动执行，定时执行和周期执行，最后关联要执行的账户即可。执行完成后可在执行账户所在主机下的配置备份中查看该文件（支持下载到本地）。且支持外置存储，使网络设备能够备份到用户自定义的 FTP/TFTP 服务器上（对应的设备需要支持 FTP/TFTP 命令）。如图 7-13

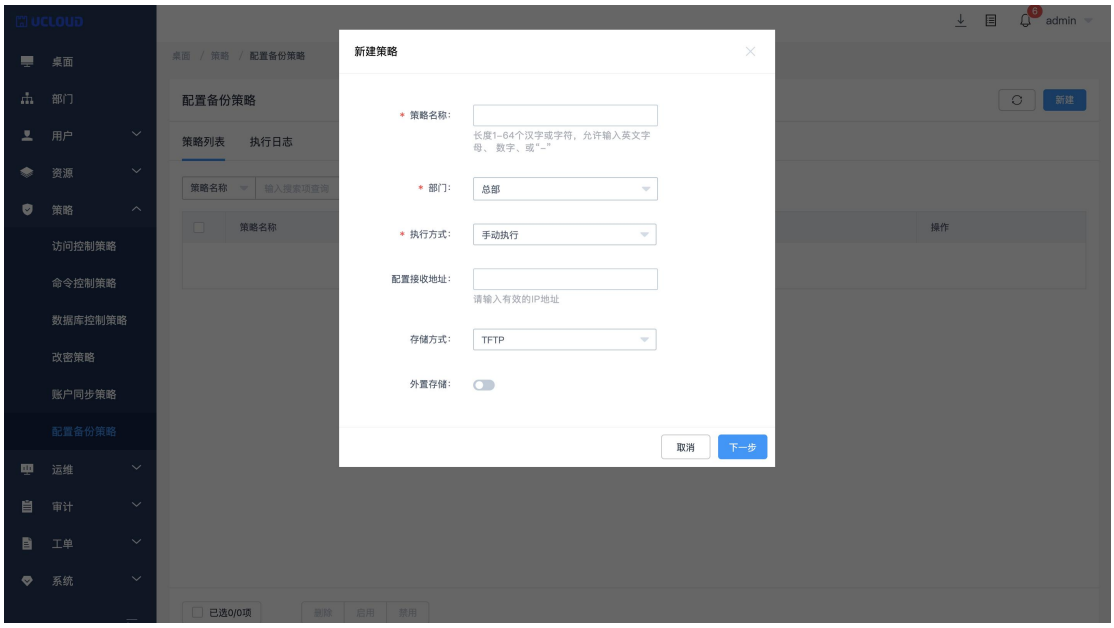


图 7-13

7.6.2 执行日志

配置备份策略执行完成后，可在执行日志中查看详情，查看备份文件的的完成情况。如图 7-14

图 7-14

8 运维

8.1 主机运维

8.1.1 登录配置下载

进入[运维/主机运维]，点击<登录配置下载>，可将运维资源导出成 xshell 或者是 secure CRT 配置，如图 8-1。详细操作流程可查看登录配置下载文件中的 readme.txt 文件。

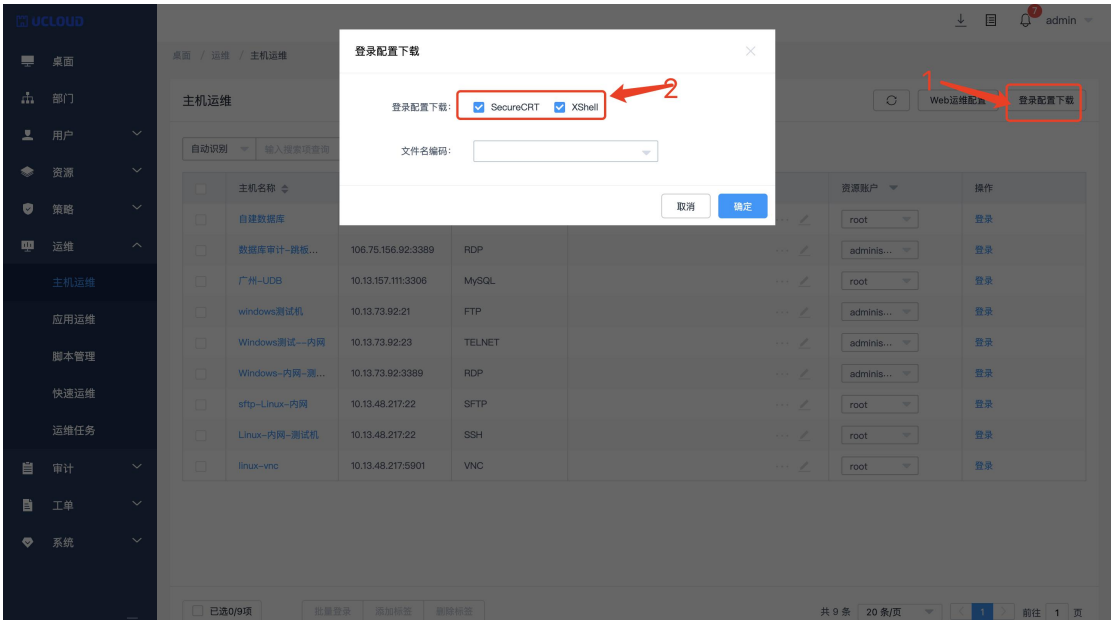


图 8-1

8.1.2 页面批量登录

进入[运维/主机运维]，点击<登录>，会登录主机资源进入 H5 会话，且支持批量登录，勾需要登录的主机，点击下方的<批量登录>，便可登录成功。当没有勾选主机时，批量登录为灰色，不可点击。如图 8-2。

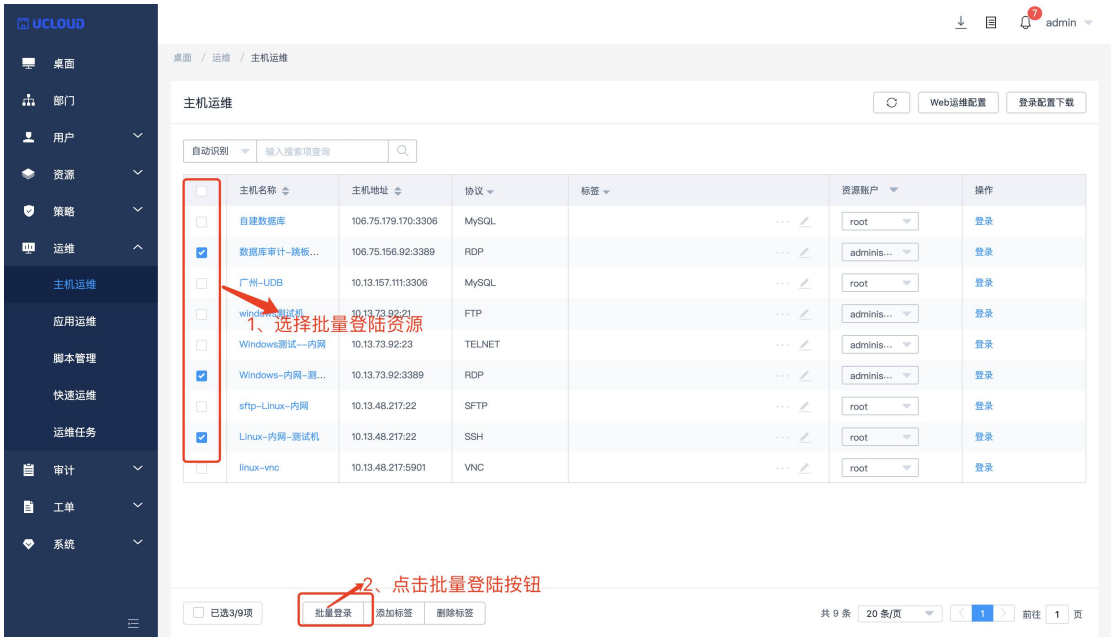


图 8-2

注意

不支持批量登录的协议有：FTP/SFTP/SCP/DB2/MYSQL/Oracle/SQL Server，手动登录和双人授权账户。

8.1.3 H5 登录字符协议主机

进入[运维/主机运维]，登录 SSH 或 TELNET 协议主机进入 h5 会话页面，根据所拥有权限可执行相应操作，（如：管理员如没有给予运维员下载权限，则在 H5 页面下载按钮不可使用）如图 8-3。

图 8-3

说明：

1.可上传本地文件和网盘文件。

2.可将该主机内文件下载到本地可网盘。

3.网盘属于堡垒机用户的个人空间，仅本人可见，用户可以将网盘文件上传到多个主机。

4.如果主机开启了文件保存，运维时与主机进行了文件传输，符合要求的文件在审计中能保留下载

SSH 或 TELNET 协议主机 h5 会话的登录，支持协同分享。如图 8-4，创建者可以将当前会话的链接复制，发送给堡垒机用户。

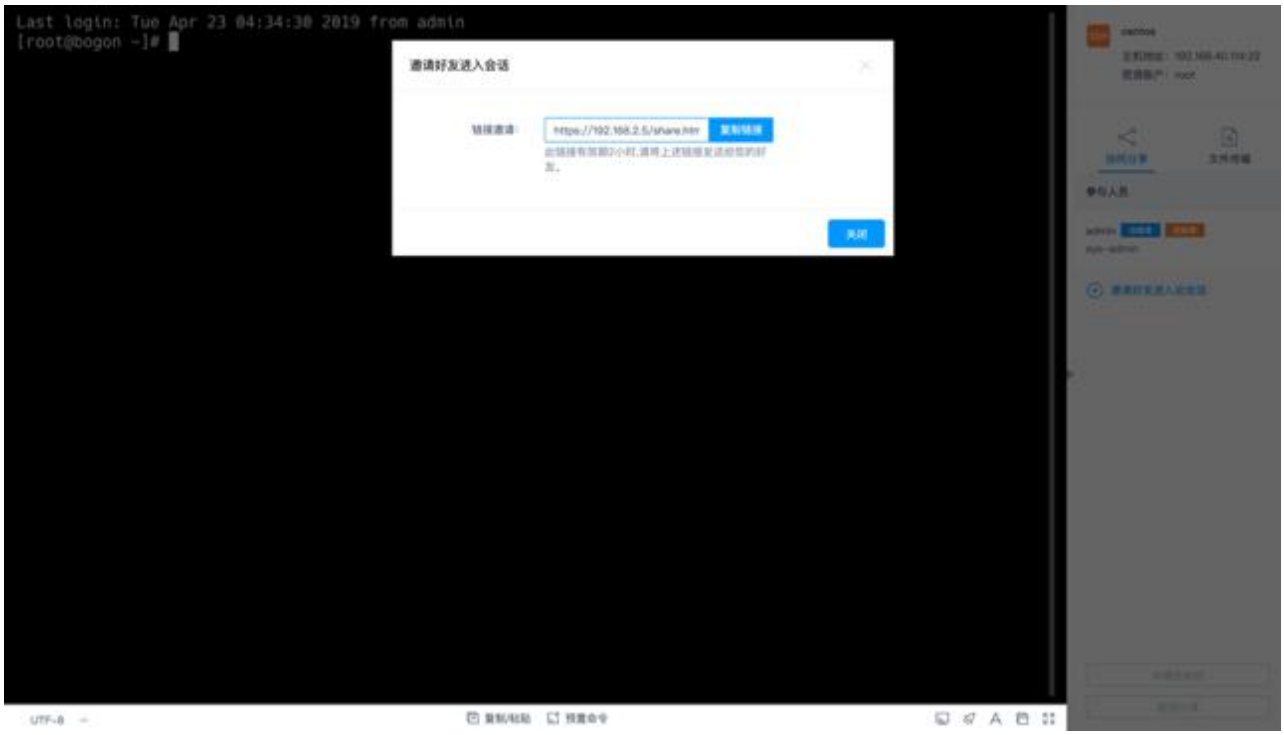


图 8-4

堡垒机用户可通过该链接登录创建者的会话中，如图 8-5。

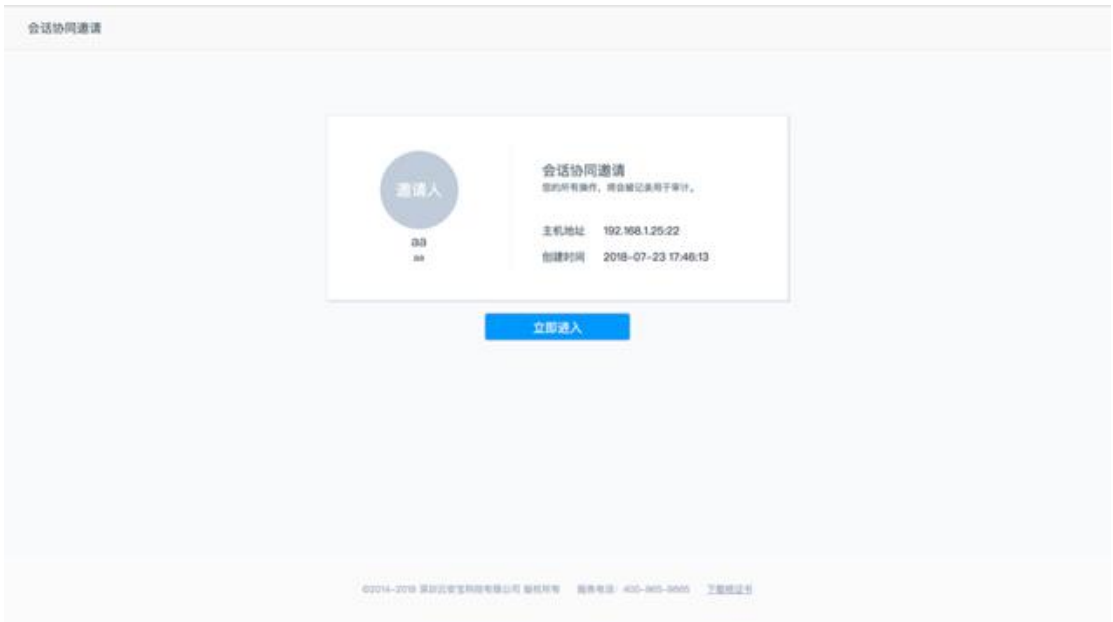


图 8-5

点击立即进入后可进入回话，在会话协同中，可像分享人申请控制权，分享人同意后，便可对该会话进行操作。如图 8-6。

图 8-6

注意事项：

1. 当没有控制权的用户申请并且获得会话控制权，此时分享者可强制获取控制权。

2. 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，且之前的会话链接失效。

3. 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。

8.1.4 H5 登录图形协议主机

进入主机运维，登录 RDP、VNC 或应用发布资源，图形协议类型主机 h5 会话的登录，支持文件传输。与 SSH 类似，区别在于 RDP 的目标地址只有：主机网盘，支持下载网盘文件到本地，支持上传本地文件到网盘。如图 8-7。

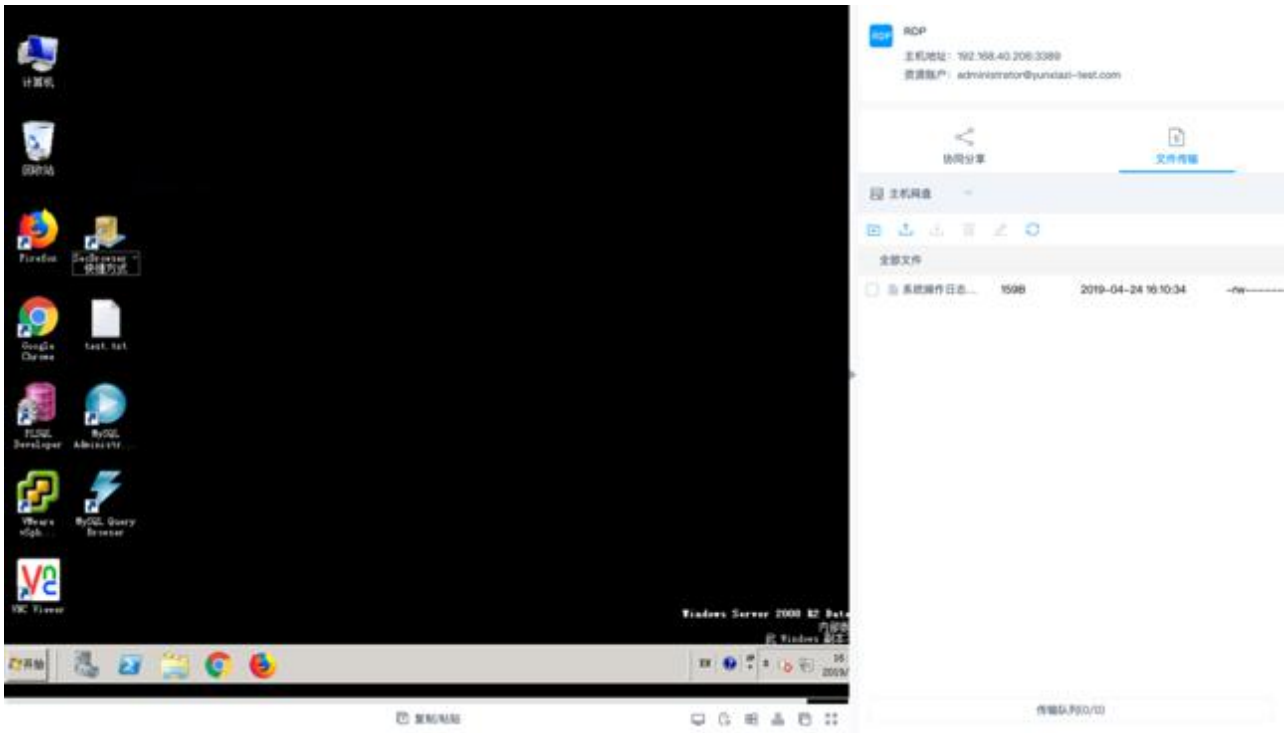


图 8-7

注：图形协议会话的协同分享与字符类型协议的会话协同操作相同。

8.1.5 SSH 客户端登录

通过 SSH 客户端登录堡垒机，此处以 xshell 为例。可新建会话如图 1-8，主机为堡垒机 IP 地址，默认端口为 22222，点击连接后输入堡垒机账户密码即可登录成功。

可通过命令行输入登录堡垒机，登录用户名格式为【堡垒机用户@IP 地址 端口号】登录密码为堡垒机密码，登录到堡垒机后可选择资源标号登录堡垒机纳管内的账户。如图 8-8

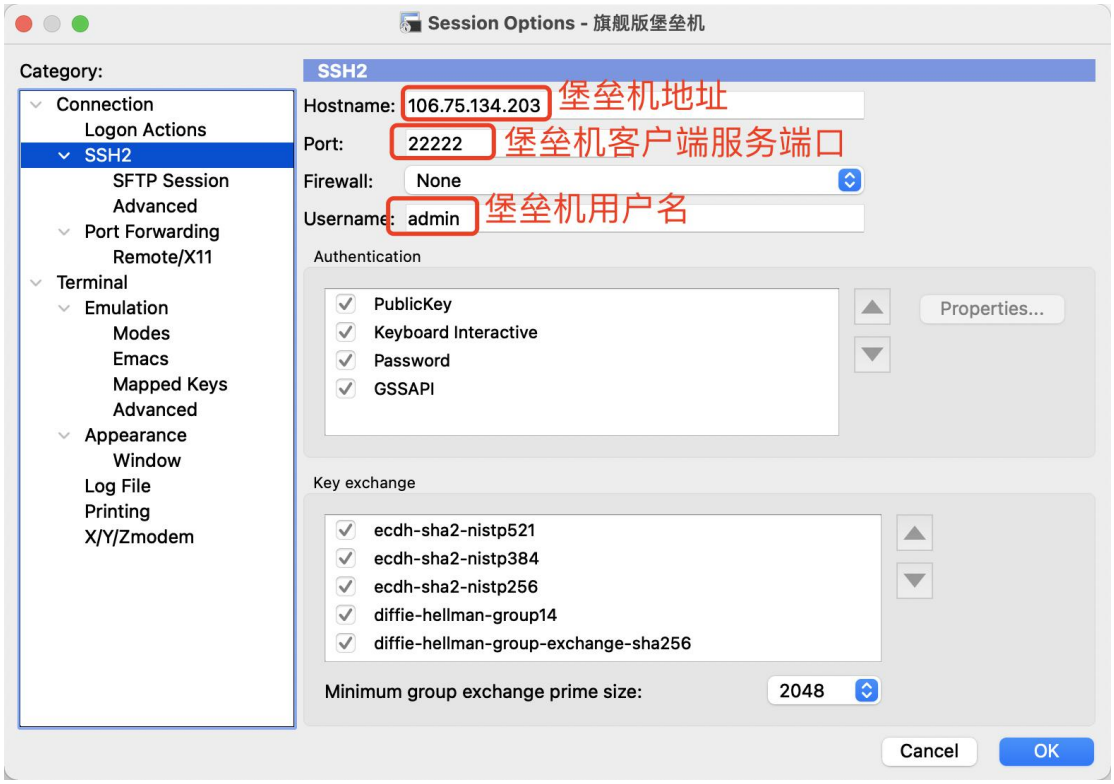


图 8-8

注意事项：

支持使用 API 的登录方式登录堡垒机指定的资源登录账户，可直接通过命令行输入：堡垒机账号@从账号@从账号 IP@堡垒机 IP 端口号，例如 admin@root@192.168.1.1@192.168.1.2 端口号，最后输入堡垒机密码，即可通过堡垒机登录到指定的主机资源内。

8.1.6 SFTP/FTP 客户端登录

堡垒机支持登录 SFTP/FTP 协议类型主机，登录信息在主机运维中点击 SFTP/FTP 主机登录弹窗获取，在 SFTP/SFTP 客户端填写该登录信息即可成功登陆。此处以 FTP 为例,SFTP 类似，区别是 SFTP 使用的是堡垒机密码，非明文密码，且无 URL 链接。如图 8-9。

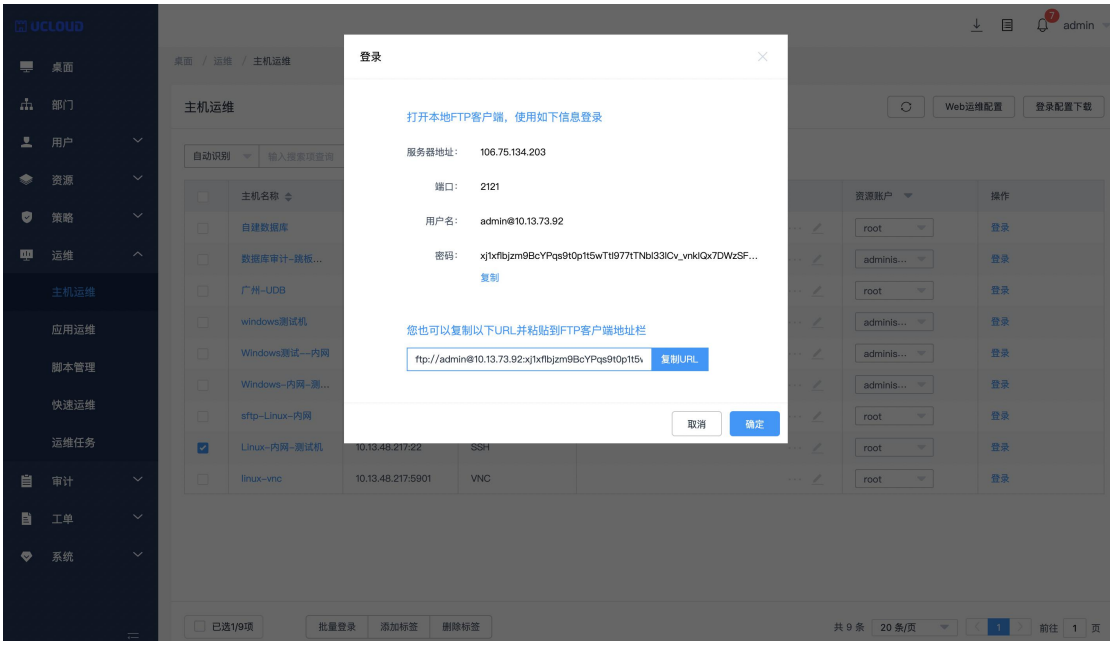


图 8-9

注意：

1 支持的 SFTP/FTP 客户端种类：Xftp，WinSCP,FlashFXP，FileZilla。

2 其中 FTP 可复制 URL 到 FTP 客户端直接登录。

8.1.7 数据库客户端登录

用户被授权数据库资源后，进入到主机运维的列表页面，点击数据库资源的登录按钮，会出现代理程序的询问弹窗，如图 8-10。

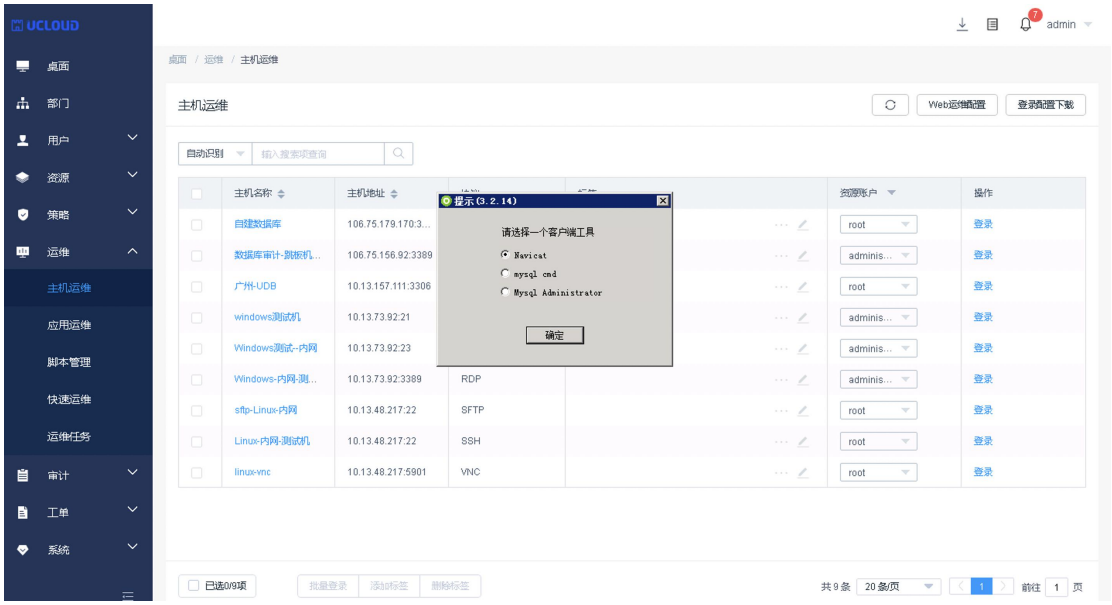


图 8-10

选择要使用登录的客户端工具即可完成数据库资源的登录进行运维，见图 8-11。

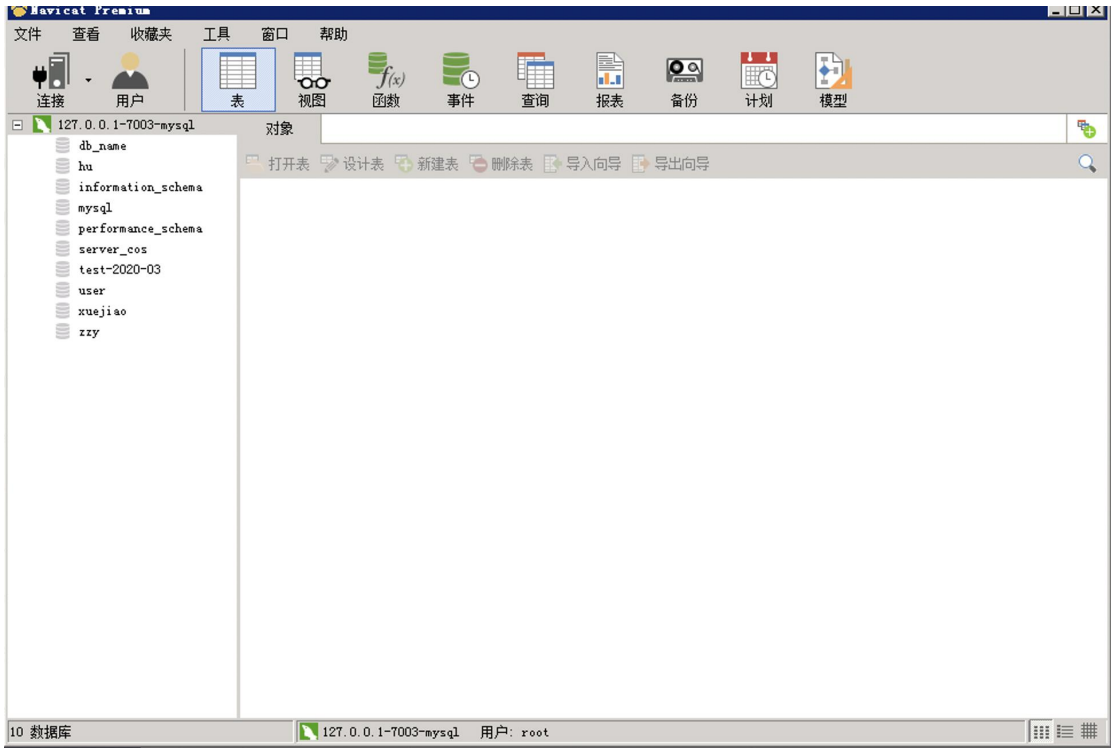


图 8-11

8.1.8 MSTSC 登录

堡垒机上添加 Windows 资源，用户被授权该资源后，支持在本地电脑上使用 mstsc 客户端能连接运维资源。填写方式，计算机名：堡垒机 IP 地址：53389。用户名：堡垒机用户名@运维的 windows 资源账户名@运维资源 IP 地址：3389。然后在资源新弹窗页面输入堡垒机密码。

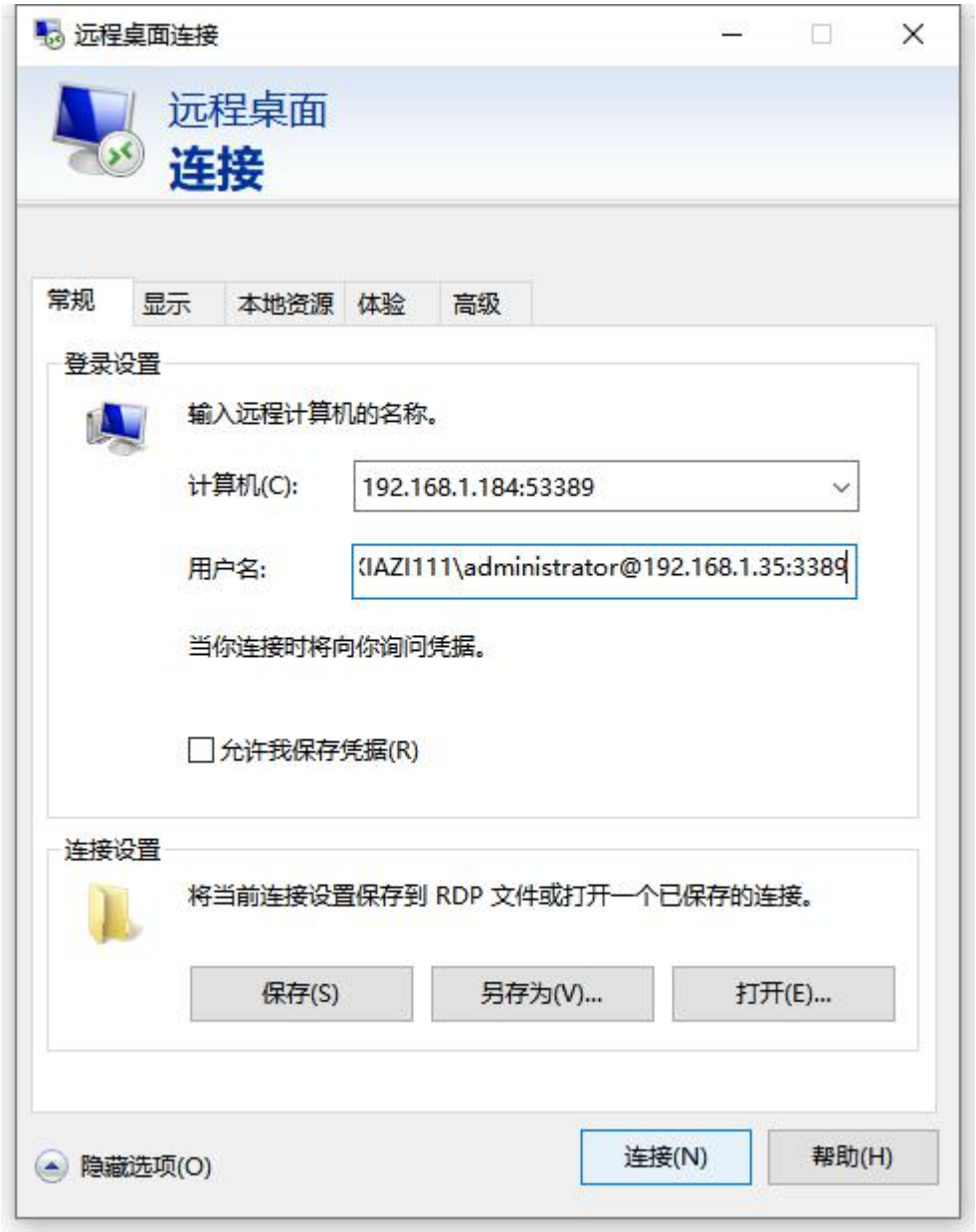


图 8-12

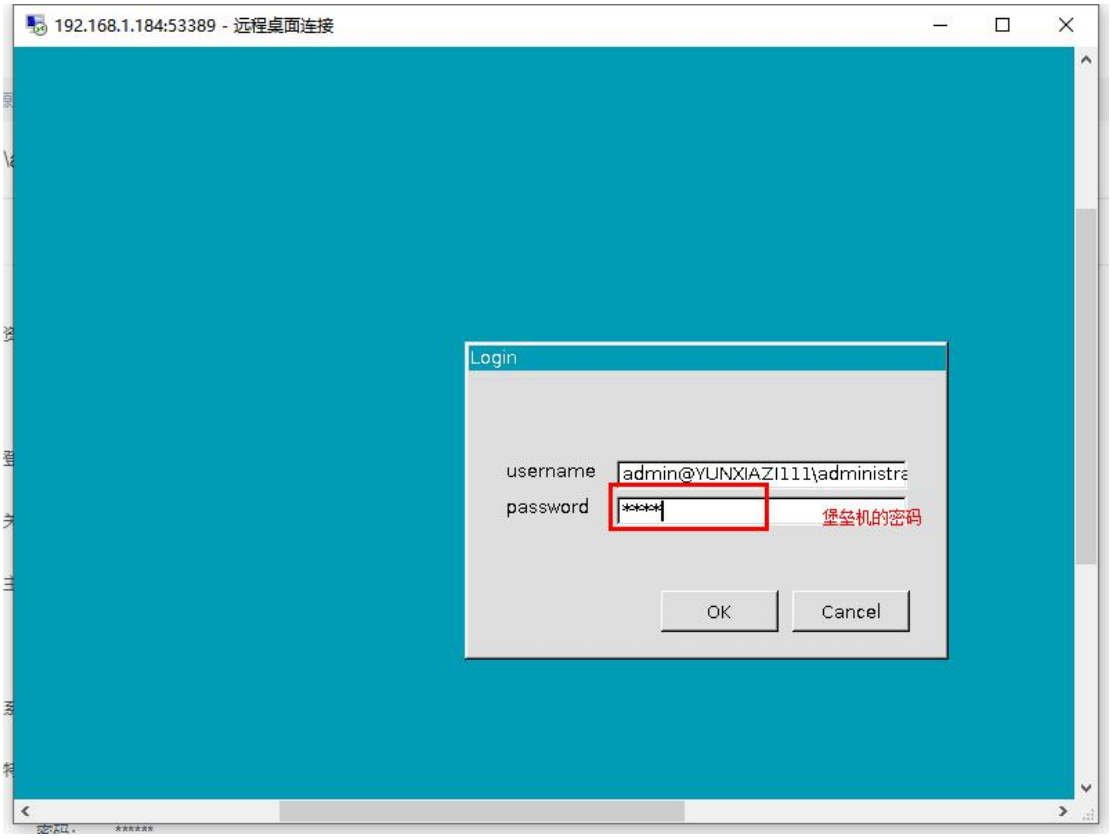


图 8-13

正常运维，见下图：

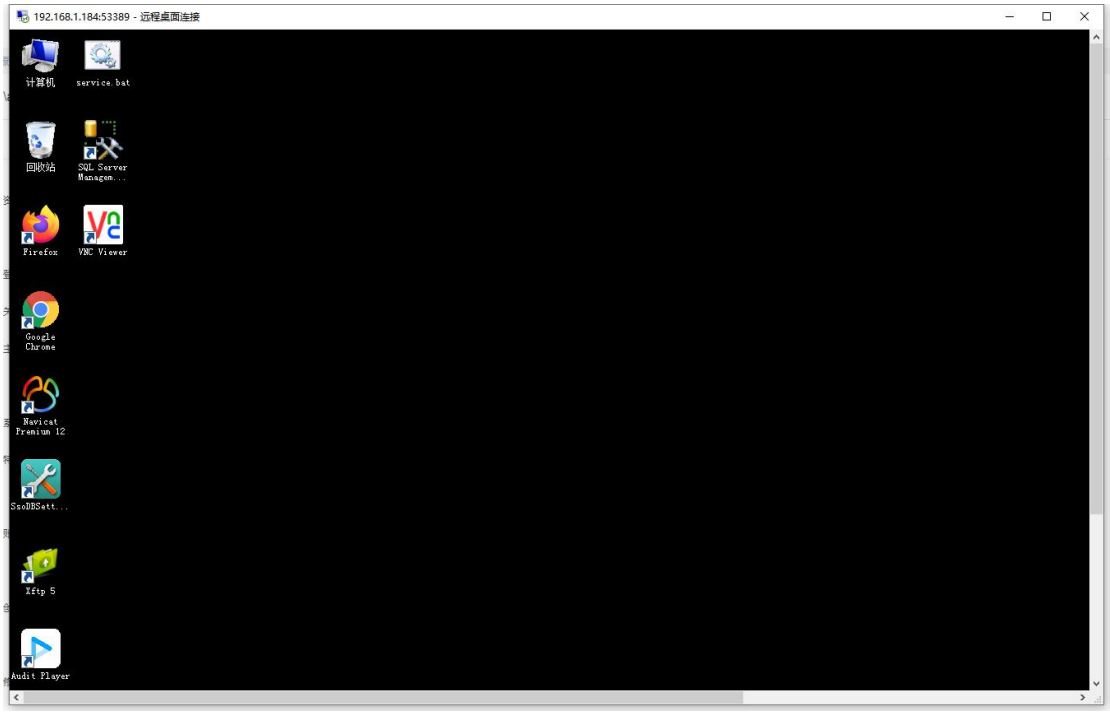


图 8-14

审计页面查看：

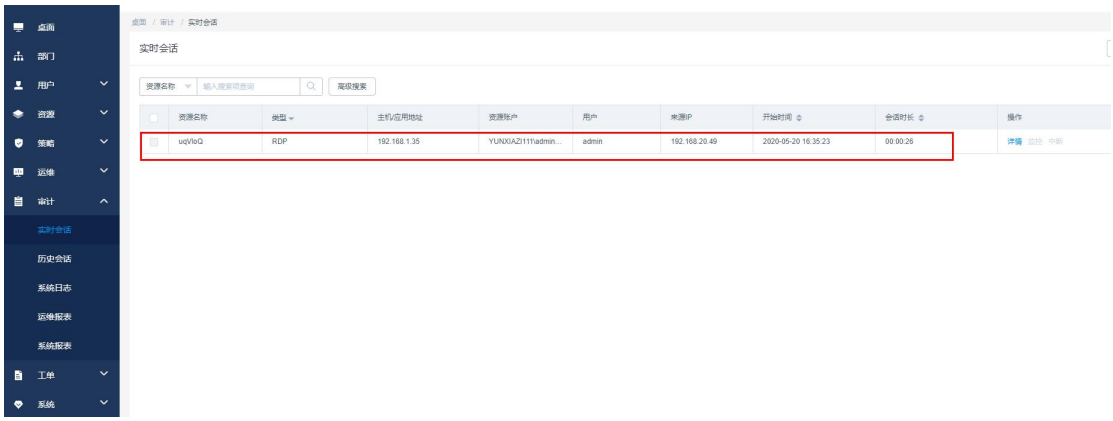


图 8-15

8.1.9 Web 运维配置

Web 运维配置支持一些特殊设定，支持的设定项有：admin console 选项，当 rdp 资源上的的远程服务器授权过期时无法登陆，勾选此选项能够强制登录进入资源，如图 8-16 所示；

图 8-16

8.2 应用运维

进入[运维/应用运维]，点击<登录>，可直接登录应用发布进入 H5 会话页面。如图 8-17。

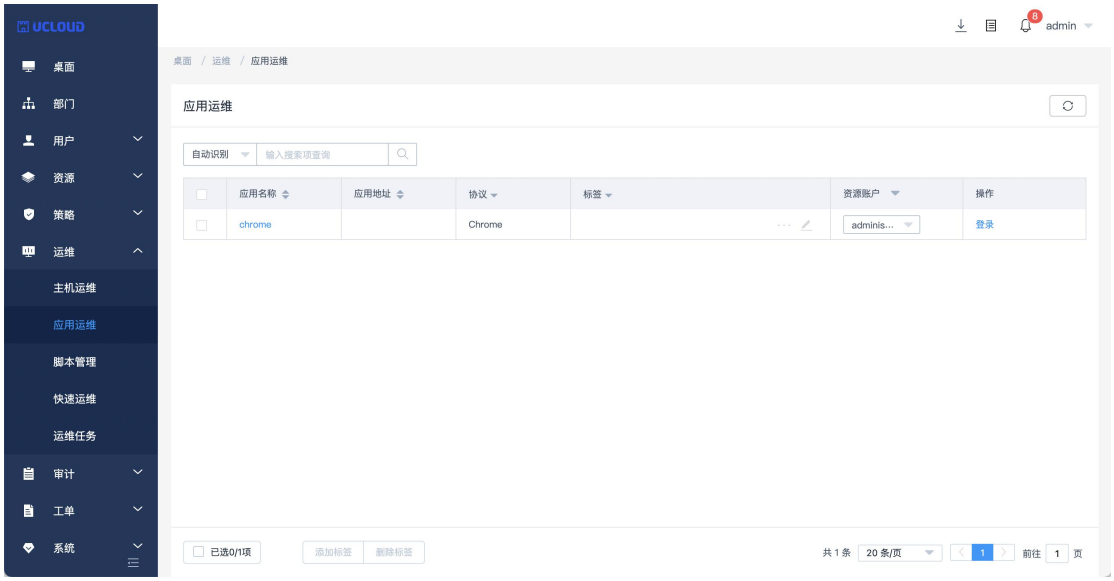


图 8-17

注意事项：支持回话协同分享，此处会话协同操作与字符类型会话协同操作相同。

8.3 脚本管理

脚本用于执行快速运维和运维任务时添加脚本使用，进入脚本管理页面，可查看当前用户所创建的脚本，支持在线编辑或导入格式为 Python 和 shell 格式的脚本。如图 8-18。

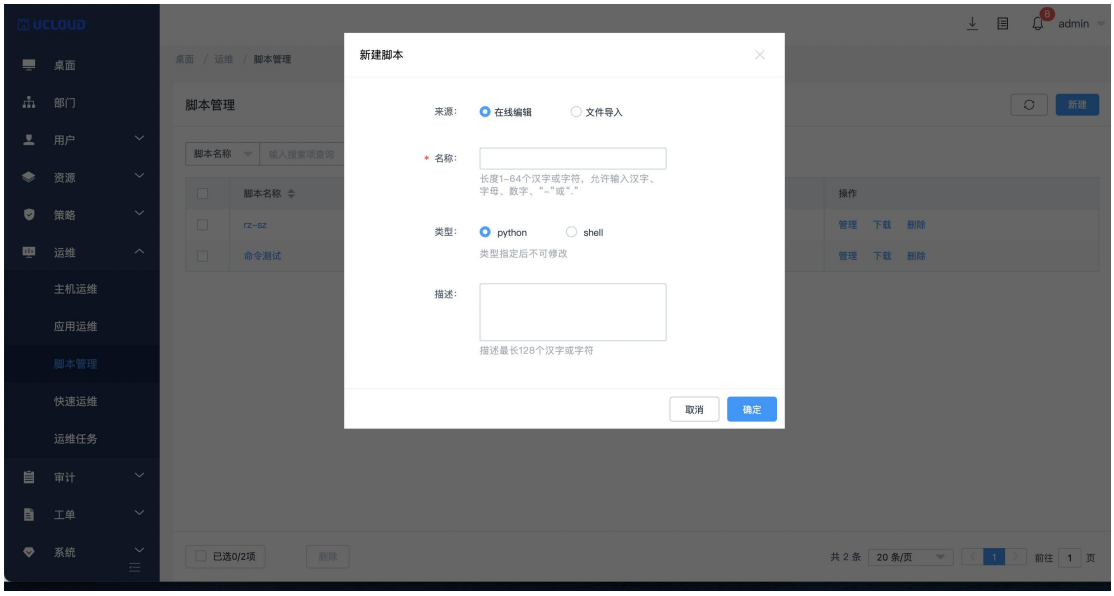


图 8-18

注意事项：脚本属于个人空间，所有的脚本详情仅限创建者可见。

8.4 快速运维

进入快速运维模块，可看到相应的 tab，选择需要执行的账户，便可在该账户快速执行命令，脚本和传输文件，执行完成后可在执行日志中查看详情信息。如图 8-19。

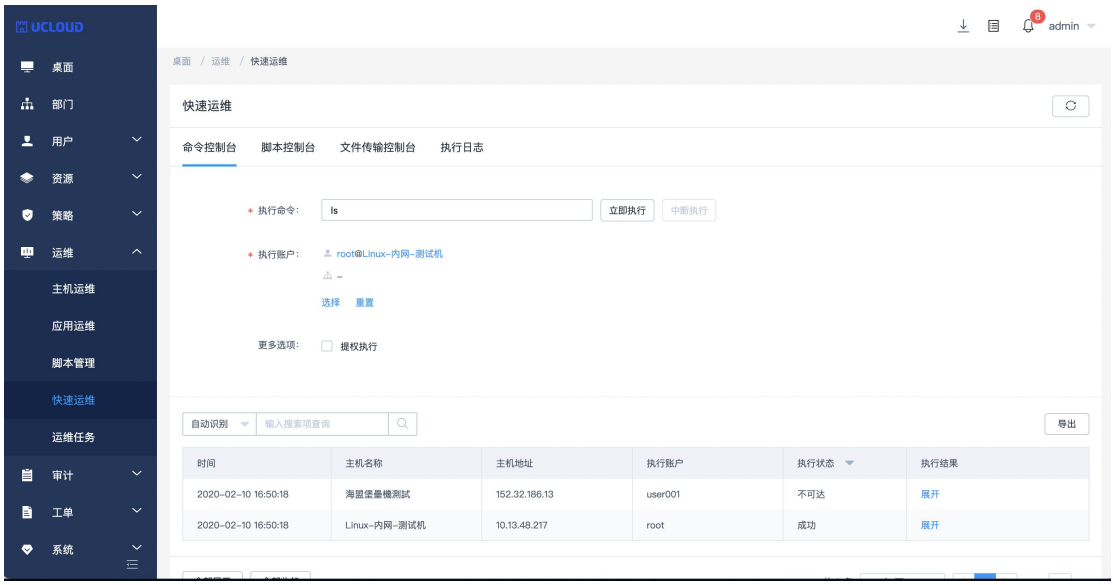


图 8-19

注意：

当该执行账户在主机的 sudoers 文件夹中时，便可勾选提权执行，执行相应命令。

8.5 运维任务

进入运维任务模块，可新建运维任务，执行方式可选择手动执行，定时执行，周期执行，更多选项可勾选提权执行，点击<下一步>选择要执行的账户。如图 8-20。

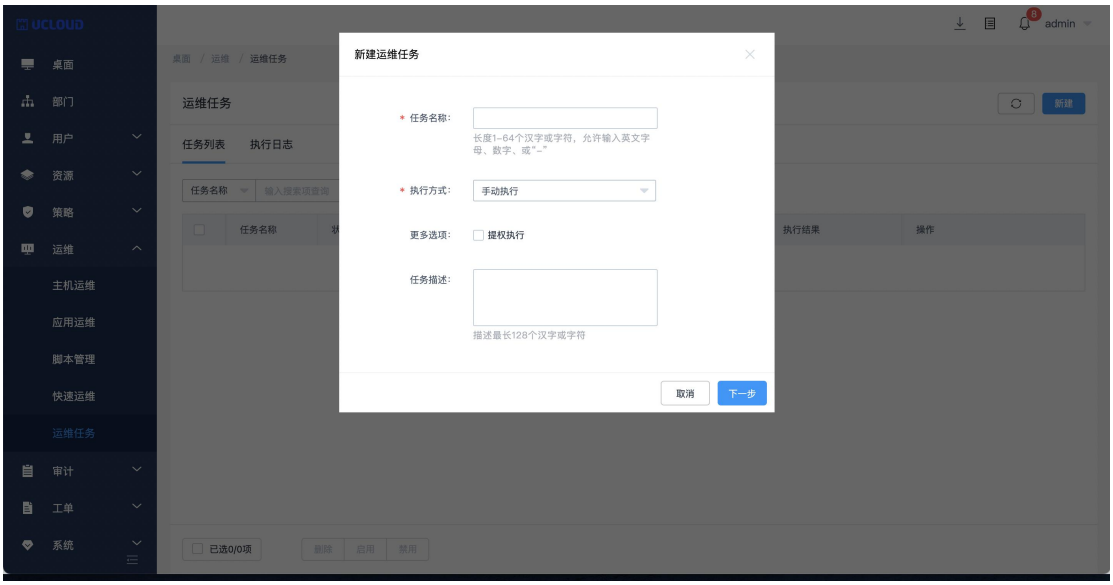


图 8-20

执行账户选择完成之后可添加任务步骤，步骤可选择执行命令，执行脚本，文件传输。支持添加多个步骤。如图 8-21。

图 8-21

9 审计

9.1 实时会话

实时会话可查看当前时间正在运维的会话，对于字符类型协议和图形协议的 H5 运维可进行实时监控，对于客户端登录的协议，可在详情中查看运维记录（SSH 协议客户端运维可查看实时会话），在会话过程中，管理员可以强制中断该回话。如图 9-1

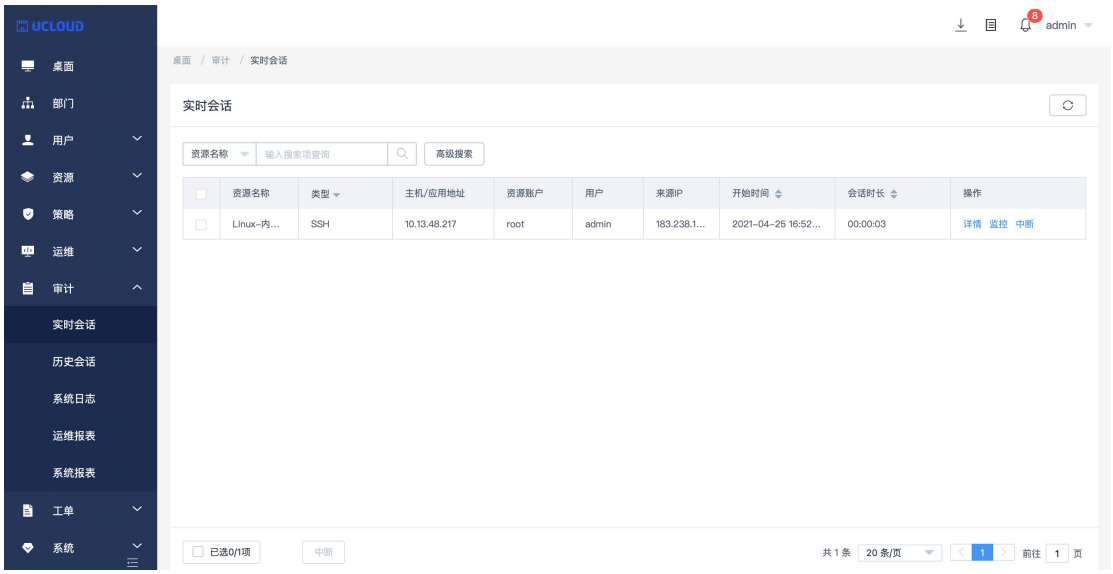


图 9-1

9.2 历史会话

当会话结束后，可在历史会话中查看该会话中所有操作，字符类型协议和图形协议可播放视频，且支持将会话文件下载到本地进行播放。对于在客户端登录的会话， SSH 客户端同样支持下载会话文件进行播放，其他客户端会话不支持播放，仅能在详情查看运维。如图 9-2

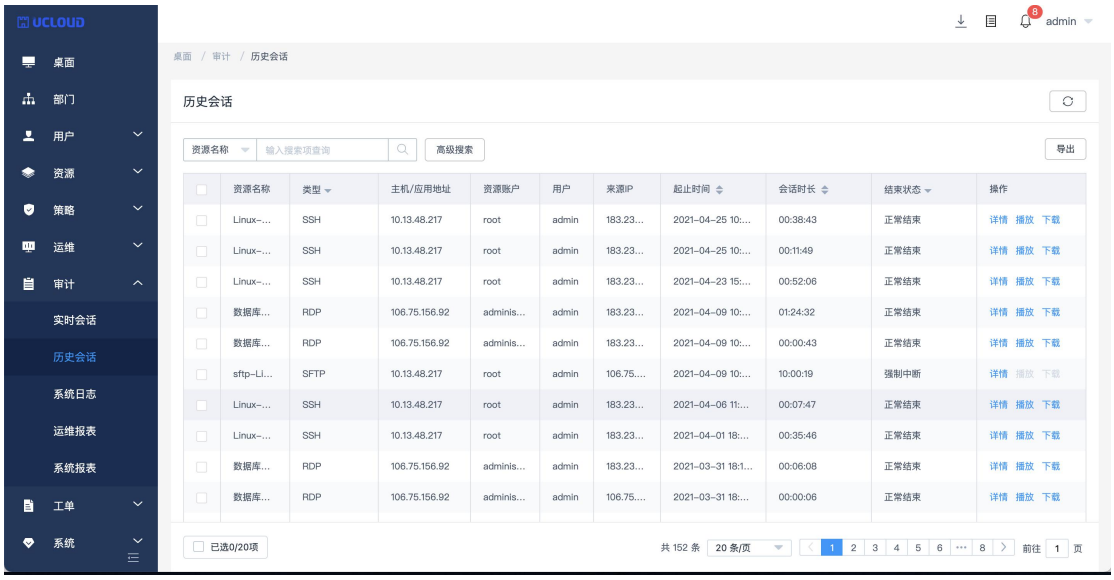


图 9-2

9.3 系统日志

系统日志可查看用户登录系统的日志以及所有操作的日志，进入系统日志页面后，可看到两个 tab。系统登录日志可查看堡垒机用户的登录日志。系统操作日志可查看堡垒机用户的操作日志。可导出日志。如图 9-3

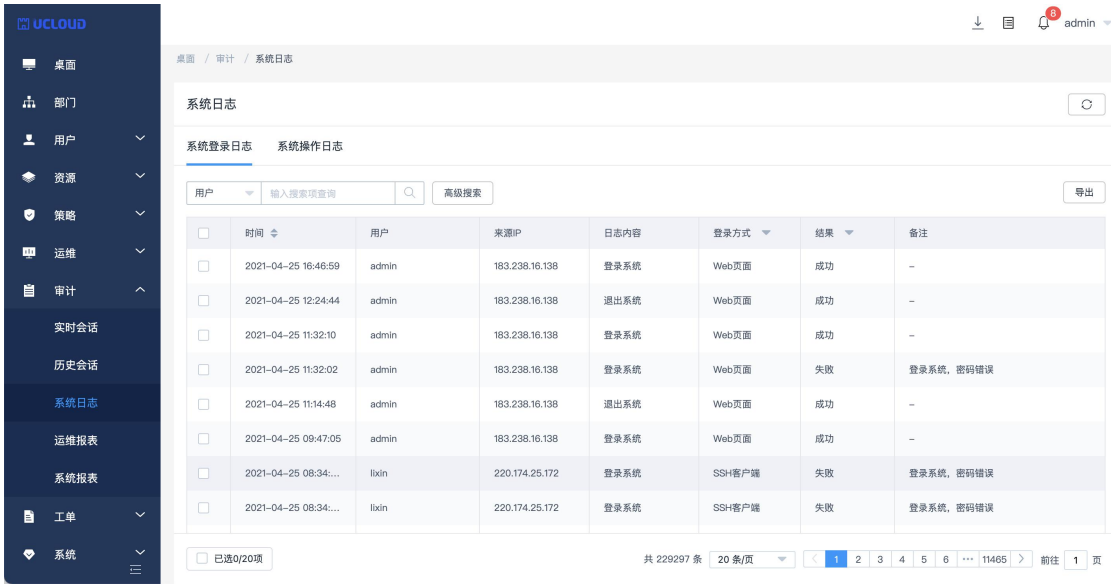


图 9-3

系统日志导出包括系统登录日志导出和系统操作日志导出，系统日志导出时间限制在 180 天以内，支持导出时间范围选择，如图 9-4

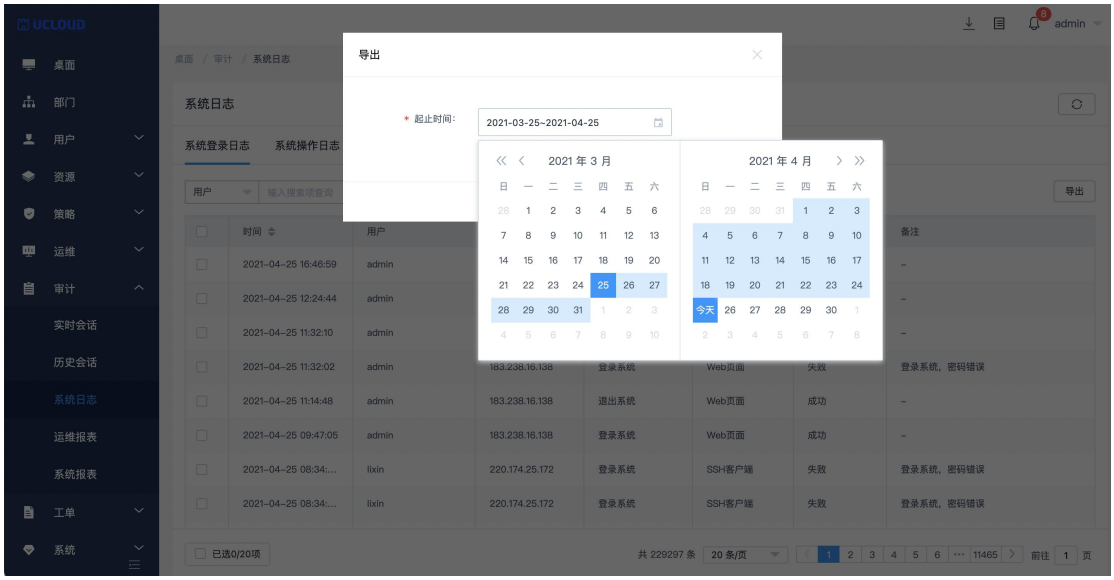


图 9-4

9.4 运维报表

进入运维报表，点击要查看的 tab，可查看运维相关报表内容。支持导出报表到本地。如图 9-5

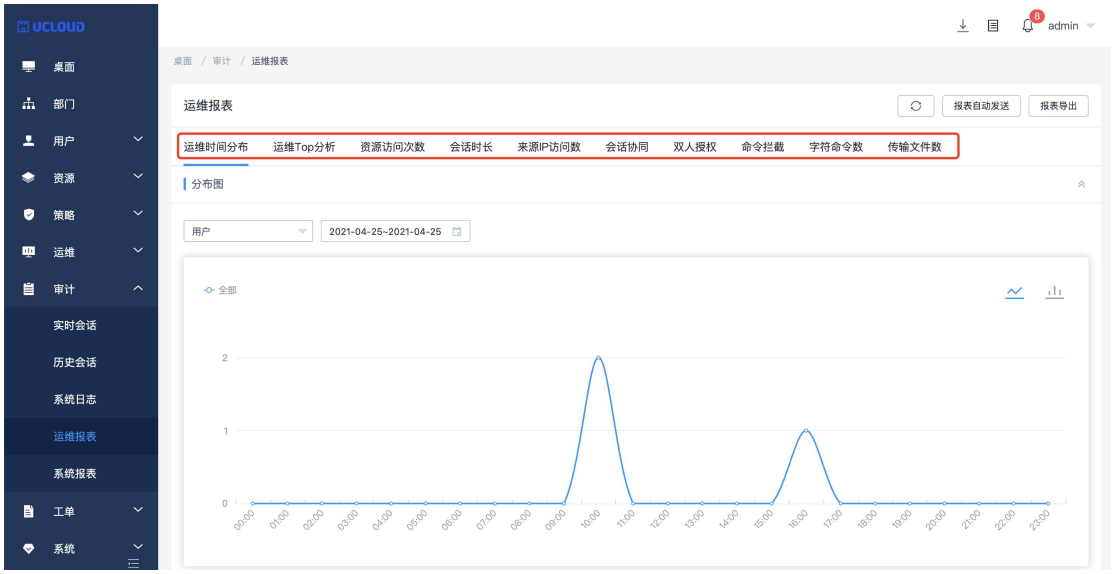


图 9-5

9.5 系统报表

进入系统报表，点击要查看的 tab，可查看系统相关报表内容。支持导出报表到本地。如图 9-5

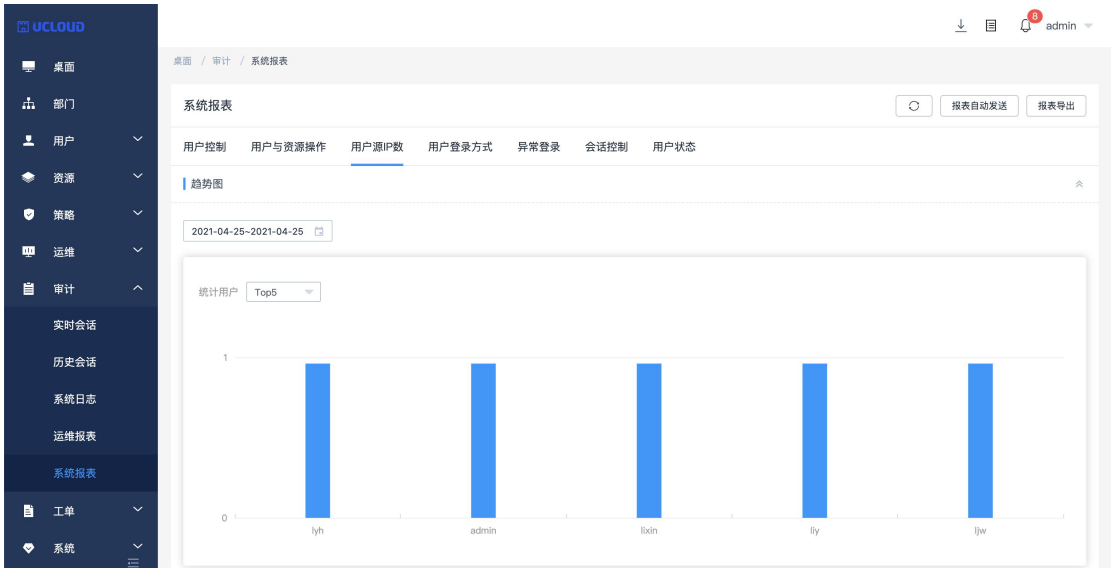


图 9-5

9.6 报表自动发送

当开启报表自动发送，会按勾选的发送时间定时发送报表至邮件。如图 9-6

图 9-6

10 工单

10.1 访问授权工单

访问授权工单用于运维员不具备运维某台主机资源权限，且又需要运维该资源时，可通过访问授权工单申请访问资源。点击新建访问授权工单，可选择自己要运维的时间和自己需要的功能。如图 10-1

图 10-1

最后选择要运维的资源主机，勾选立即提交后该工单会自动提交，否则需要在访问授权工单模块进行手动提交。管理员审批通过后该工单生效。如图 10-2

图 10-2

【工单克隆】
如果需要再次使用申请过得资源，可以使用工单克隆功能快速复制工单，如图 10-3，点击更多即可看到克隆功能

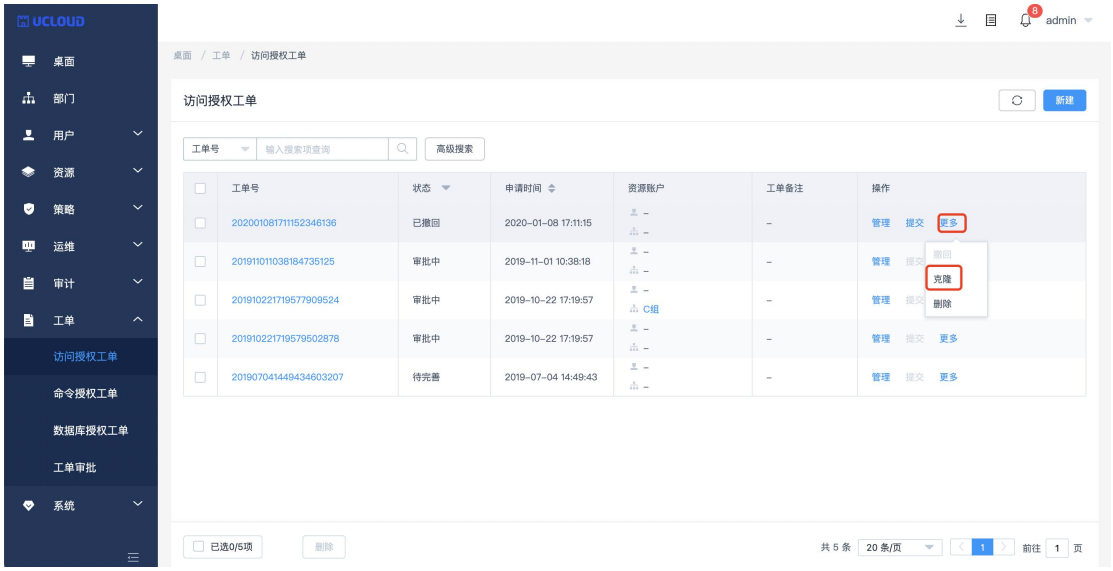


图 10-3

注意：
除了待完善状态的工单都能进行复制

10.2 命令授权工单

管理员为用户配置命令控制策略后，当用户登录该资源并执行了策略中的命令，命令授权工单列表中就会自动生成一个命令授权工单。如图 10-4。

图 10-4

如果 admin 在系统配置中的命令授权工单提交方式配置为手动提交，则需要在命令授权工单中手动点击提交，管理员审批同意后，刷新页面，该工单生效。如图 10-5。

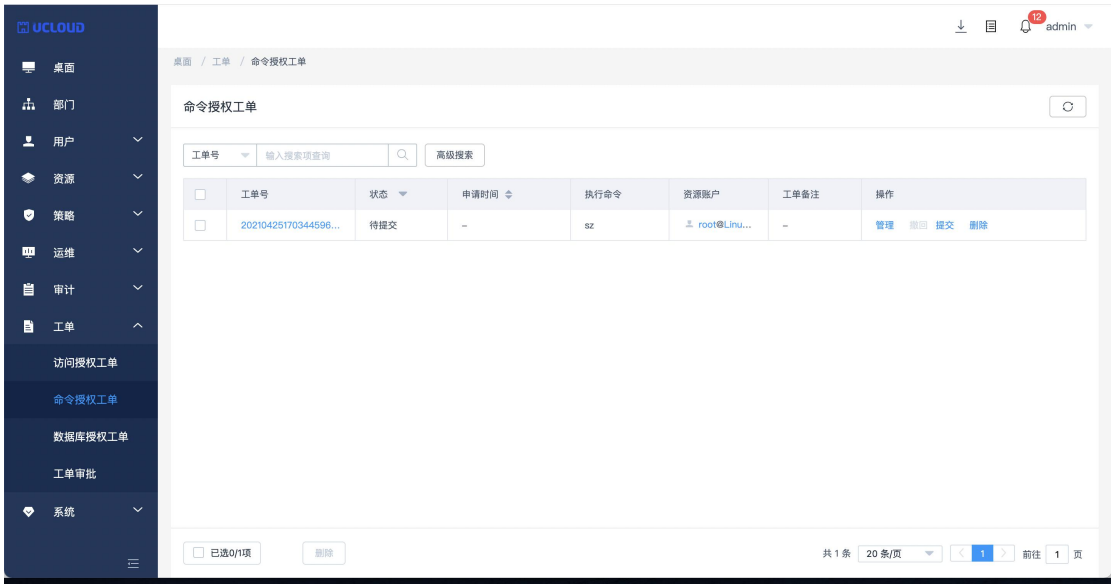


图 10-5

注意事项：

命令授权工单由用户触发“动态授权”命令策略时自动创建，无法手动创建命令授权工单。

10.3 数据库授权工单

管理员为用户配置数据库控制策略并添加相应的规则后，当用户登录该资源并执行了策略中的规则，数据授权工单列表中就会自动生成工单，点击提交，管理员审批通过后状态为生效。如图 10-6。

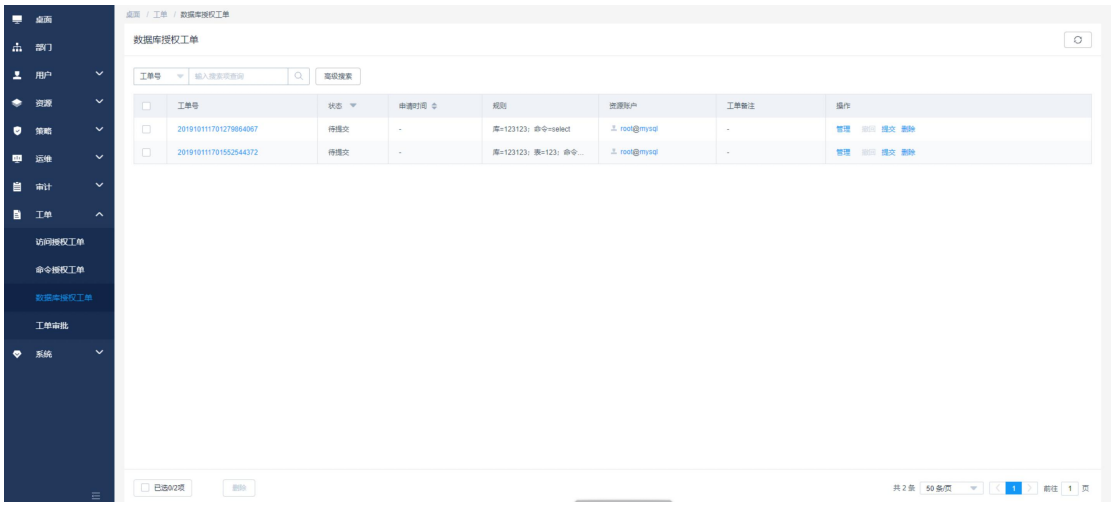


图 10- 6

注意事项：

1 如果系统配置中命令授权工单配置为手动提交，则需要手动提交给管理员，管理员同意后，该工单生效。

2 目前数据库授权工单只支持 MySQL 和 oracle 两种数据库。

3 数据库授权工单由用户触发“动态授权”命令策略时自动创建，无法手动创建数据库授权工单。

10.4 工单审批

工单审批用于对堡垒机用户提交后的工单进行审批，进入工单审批后可查看当前需要审批和审批后的工单，点击管理可查看审批人节点，和审批内容。支持勾选后批量审批。如图 10-7

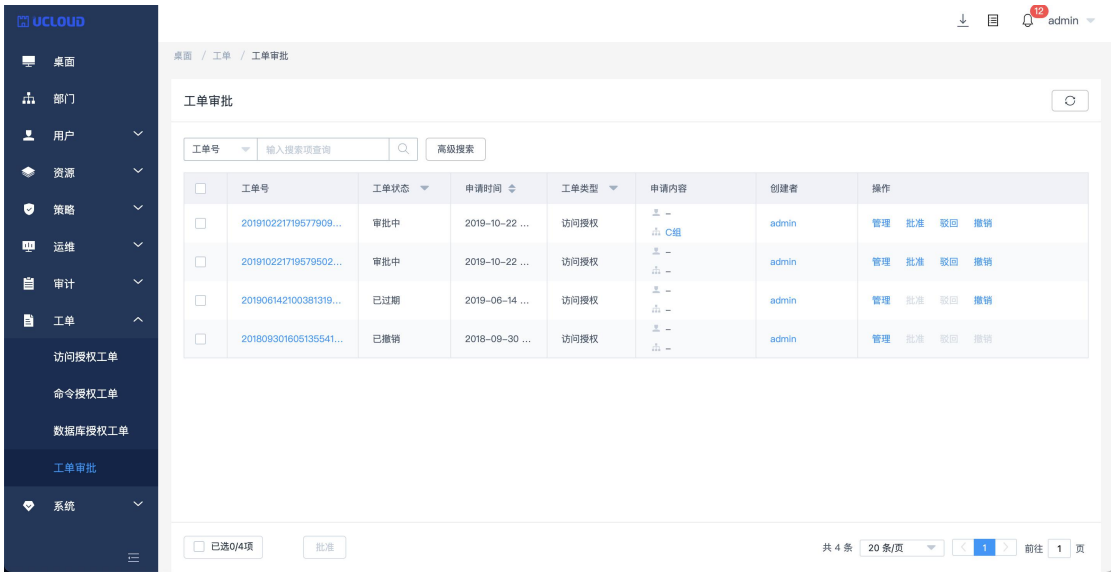


图 10- 7

11 系统

11.1 安全配置

11.1.1 用户锁定配置

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，如果设置为 0，则不锁定账户/来源 IP，默认值 5 次。锁定时长是指用户输错密码被锁定的时长，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，默认值 5 分钟。如图 11-1

图 11-1

11.1.2 密码策略配置

密码策略配置中密码强度校验开启后更改密码时不得更改为简单密码。新用户强制改密打开后，当用户第一次登陆到堡垒机时，系统强制用户更改堡垒机密码。密码相同校验是指，更改密码时不得与前 x 次的密码相同，默认为 5 次。密码修改周期默认为 30 天，当到达 30 天后系统会强制堡垒机用户更改密码。如图 11-2

图 11-2

11.1.3 web 登录配置

Web 登录配置中登录超时默认为 30 分钟，当登录堡垒机 30 分钟后页面无任何操作则需要重新登录堡垒机，短信验证码过期时间默认为 60 秒，当使用手机短信登录接收的验证码在 60 秒之内有效。支持更改 USBkey 类型。当开启图形验证码为自动时，web 登录页面输入密码错误超过 3 次则会出现验证码，验证码过期时间默认为 60 秒。当开启域控校验时用户登录时需要进行域控校验，且用户的新建和编辑弹窗增加“更多选项：域控校验”复选框的展示。如图 11-3

图 11-3

11.1.4 web 证书配置

在 web 证书配置中可上传正确格式的证书文件，输入密码后即可。如图 11-4

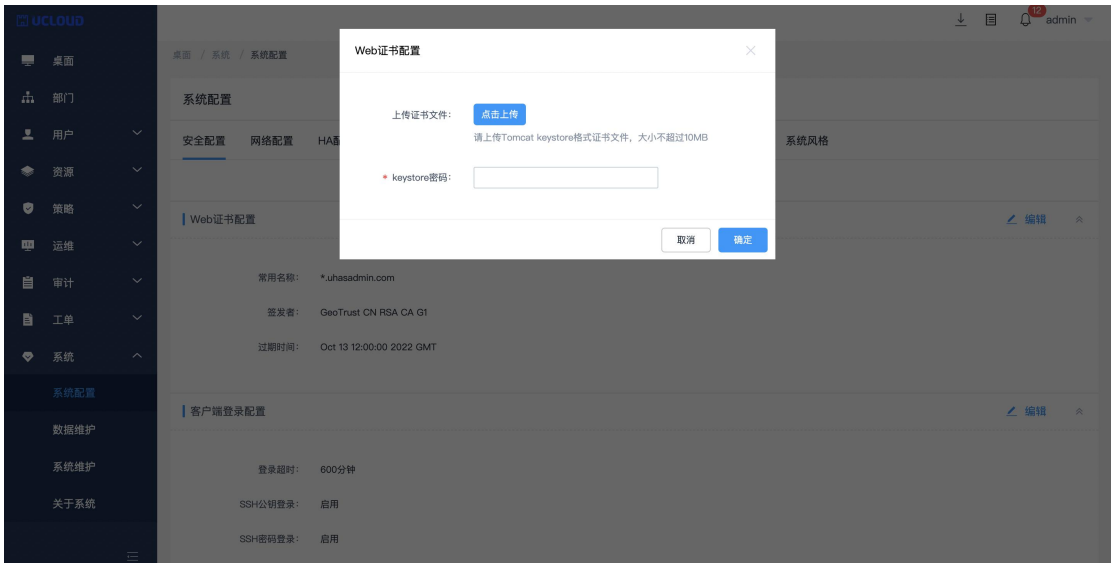


图 11-4

11.1.5 客户端登录配置

SSH 登录超时默认为 30 分钟，当在客户端登录堡垒机之后 30 分钟无操作，再次操作需要重新登录。当开启 SSH 公钥登录并用户配置了 SSH 公钥即可免密码登录。密码登录开启后在 SSH 客户端登录时只能输入密码登录，如公钥登录和密码登录全部开启，则优先使用公钥登录。如图 11-5

图 11-5

11.1.6 USB Key 配置

USB Key 类型包含龙脉科技、北京 CA、海泰方圆、鱼翁、吉大正元可配置。更改之后用户签发 USB Key、用户使用 USB Key 方式登录也做相应的变化。如图 11-6、图 11-7

图 11-6

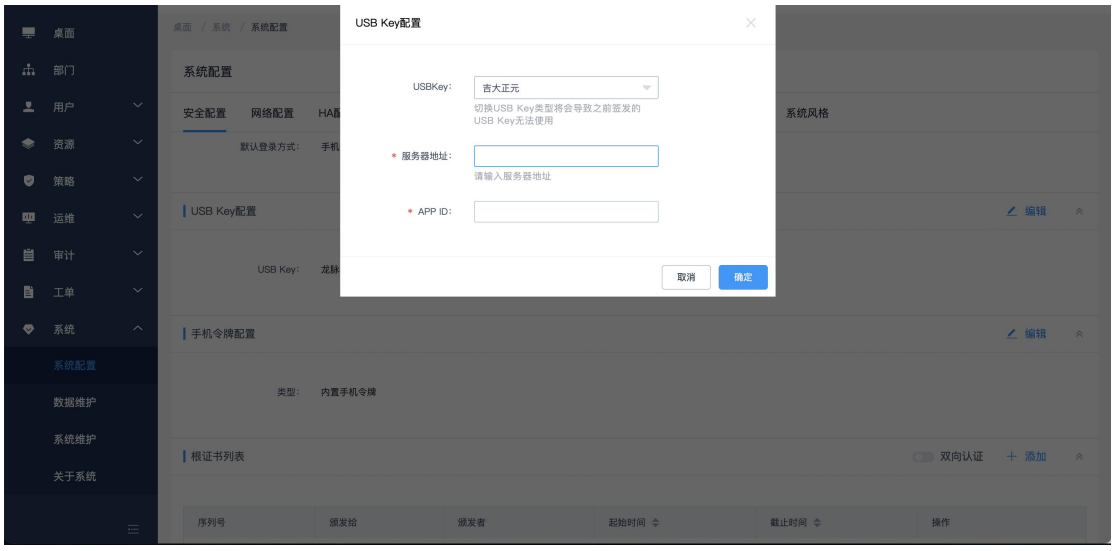


图 11-7

11.1.7 手机令牌配置

堡垒机除了使用内置的手机令牌，还支持使用奇安信 ID 或 Radius 令牌，见图 11-8 和图 11-9,选取对应的类型后将数据填写进入并保存，用户就可以在登录时使用对应的手机令牌服务。

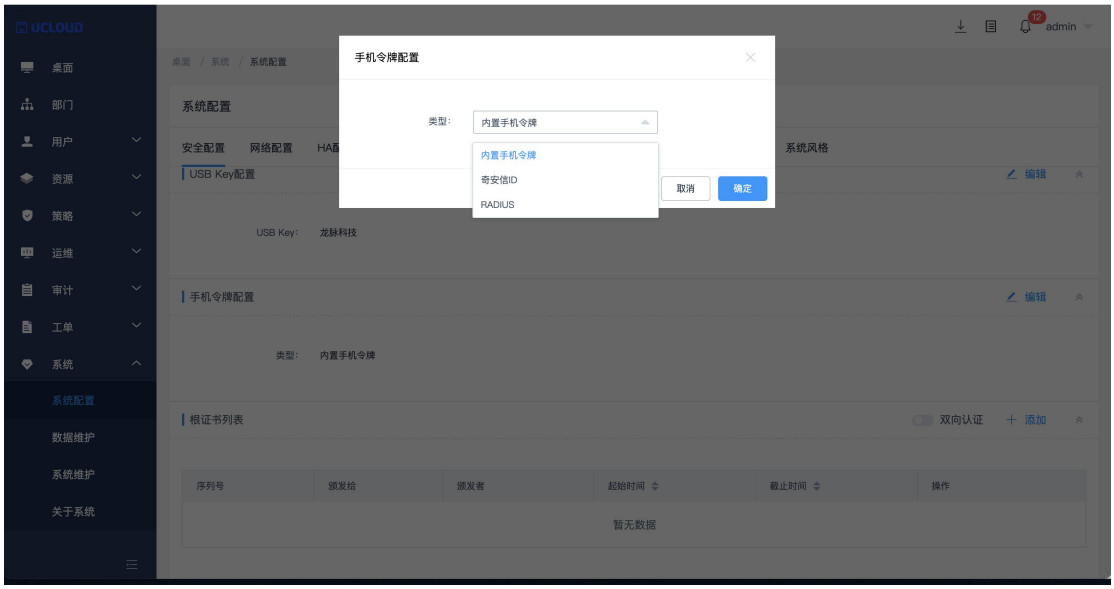


图 11-8

11.2 网络配置

11.2.1 网络接口列表

其中网络接口列表可以编辑、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 11-10

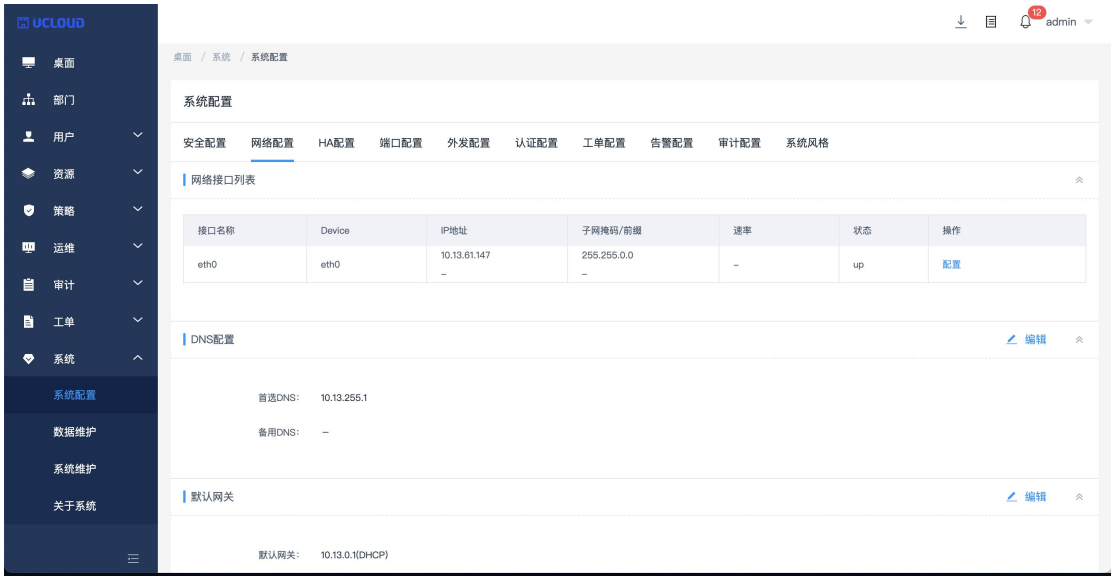


图 11-10

11.2.2 DNS 配置

可修改当前机器的首选 DNS 和备用 DNS，输入正确的 DNS 地址即可。如图 11-11

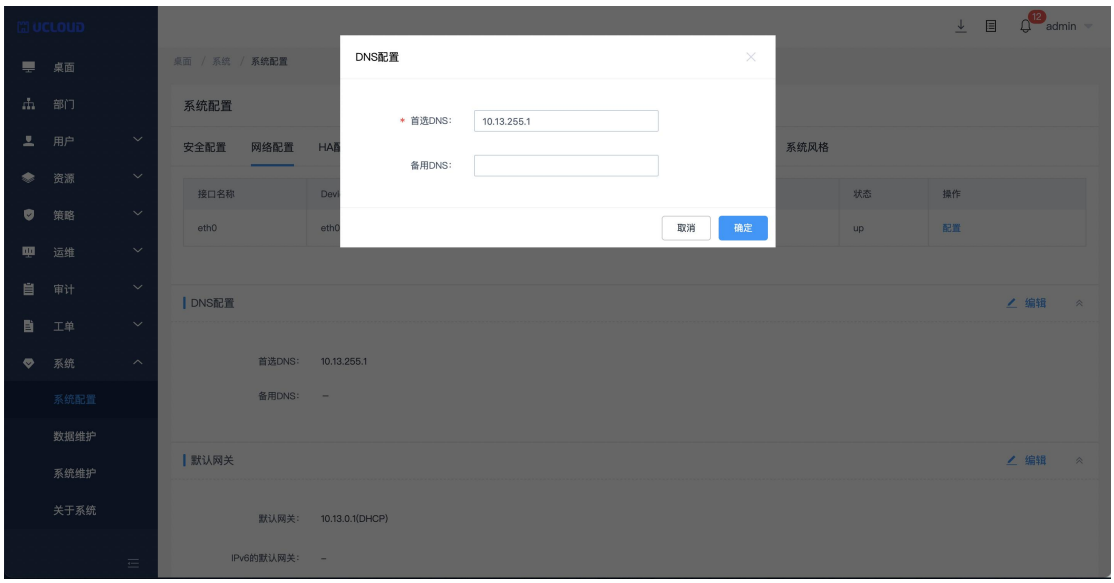


图 11-11

11.2.3 默认网关

可在默认网关处修改 IPv4 和 IPv6 的默认网关。如图 11-12

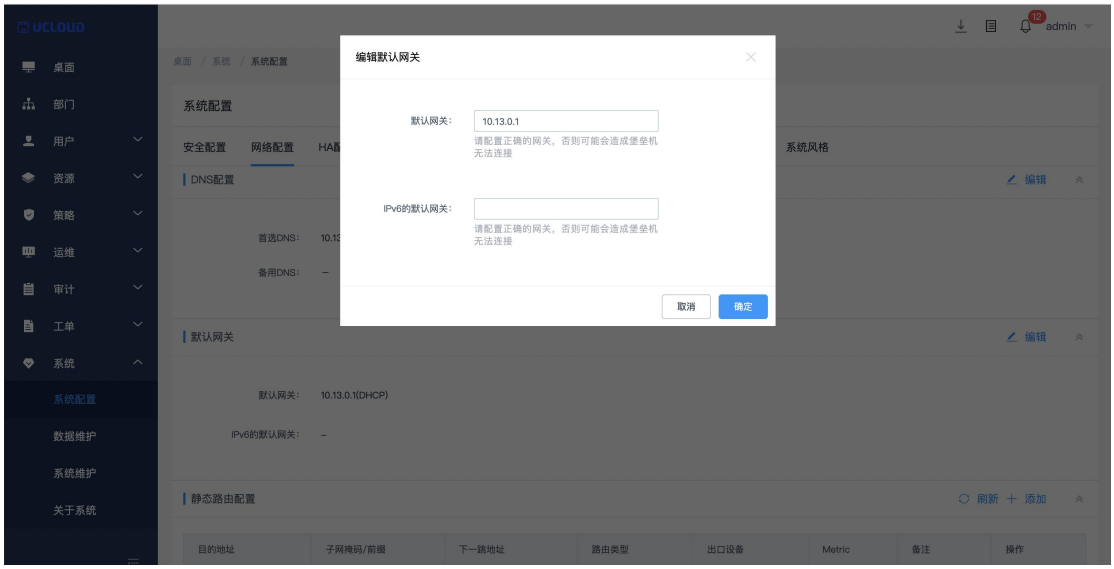


图 11-12

11.2.4 静态路由配置

可为当前机器添加静态路由，使当前机器可以访问到其他网段的机器。如图 11-13

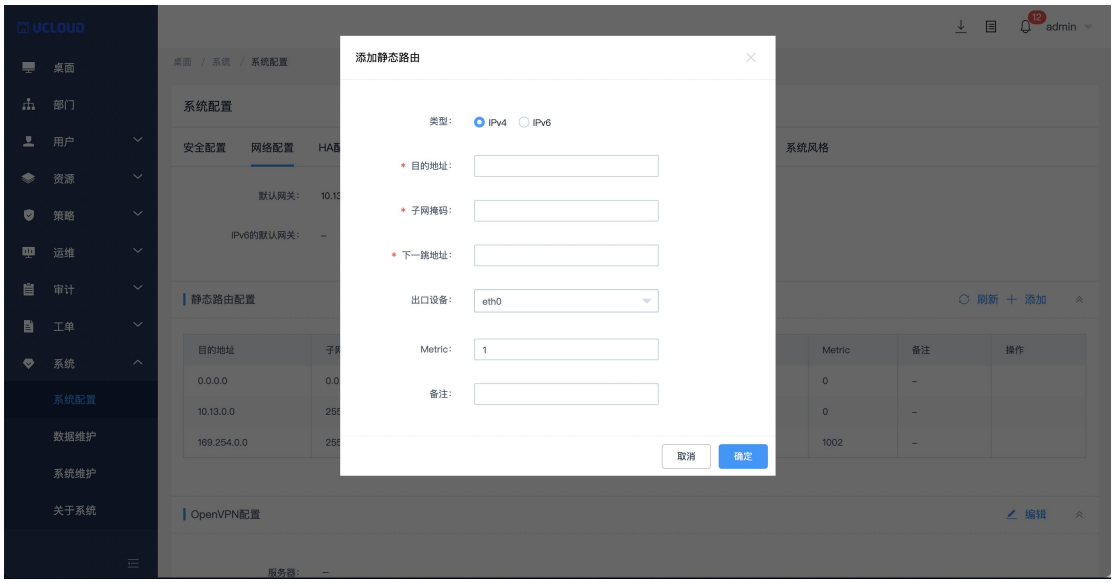


图 11-13

11.2.5 OpenVPN 配置

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。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，填

写完成后即可将堡垒机添加到堡垒机服务器，用户可对 VPN 内部资源运维，审计等操作。如图 11-14

图 11-14

11.3 HA 配置

进入 HA 配置页面后可查看当前 HA 状态，开启 HA 需要两台堡垒机，并且版本一致，点击启用后需要先配置主节点，在备节点 IP 栏输入需要作为备节点的 IP，HAkey 可在堡垒机的系统-关于系统中查看，在浮动 IP 栏输入未被使用的 IP 地址，浮动 IP 格式为地址/掩码，选择浮动 IP 网口和 HA 心跳接口点击确定后重启主节点（未重启时状态为单机状态）。重启完成后配置备节点，配置完成后重启备节点即可。如图 11-15

图 11-15

11.4 端口配置

进入端口配置页面可查看当前端口，共分为三种，运维端口，web 控制台端口，SSH 控制台端口，运维段口配置主要针对 SSH/SFTP 和 FTP，端口配置完成后重新启动堡垒机即可。如图 11-16

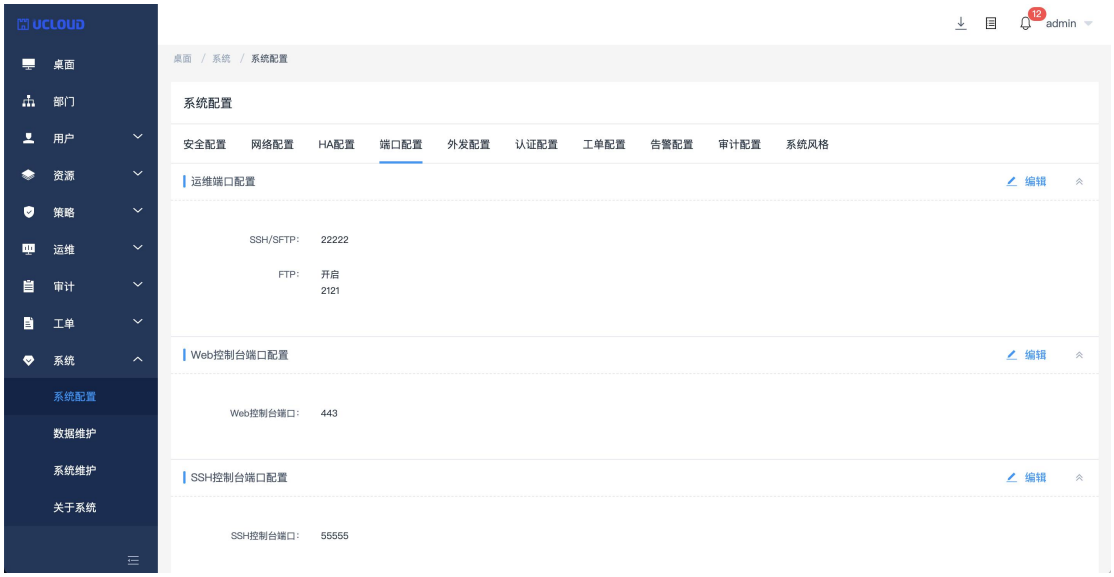


图 11-16

11.5 外发配置

11.5.1 邮件配置

邮件配置用于配置邮件服务器，为报表自动发送功能和账户验证等通知提供邮件发送服务。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，目前支持两种发送方式 — SMTP 、 Exchange 。如图 11-17

图 11-17

11.5.2 短信配置

短信配置支持两种，一种是堡垒机内置的短信网关，由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 11-18

图 11-18

11.5.3 SNMP Agent 配置

SNMP Agent 配置分为 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 11-19

图 11-19

11.6 认证配置

11.6.1 AD 域认证配置

当企业网络中计算机和用户数量较多时，可实现高效管理。进入 AD 域认证配置页面，点击添加 AD 域，可选择认证模式和同步模式。填写正确的 AD 域服务器名称，端口，域，Base DN，和登录名密码后，同步方式可选为手动/自动同步。如图 11-20

图 11-20

输入正确参数点击下一步可选择导入源，选择完成后即可导入。如图 11-21

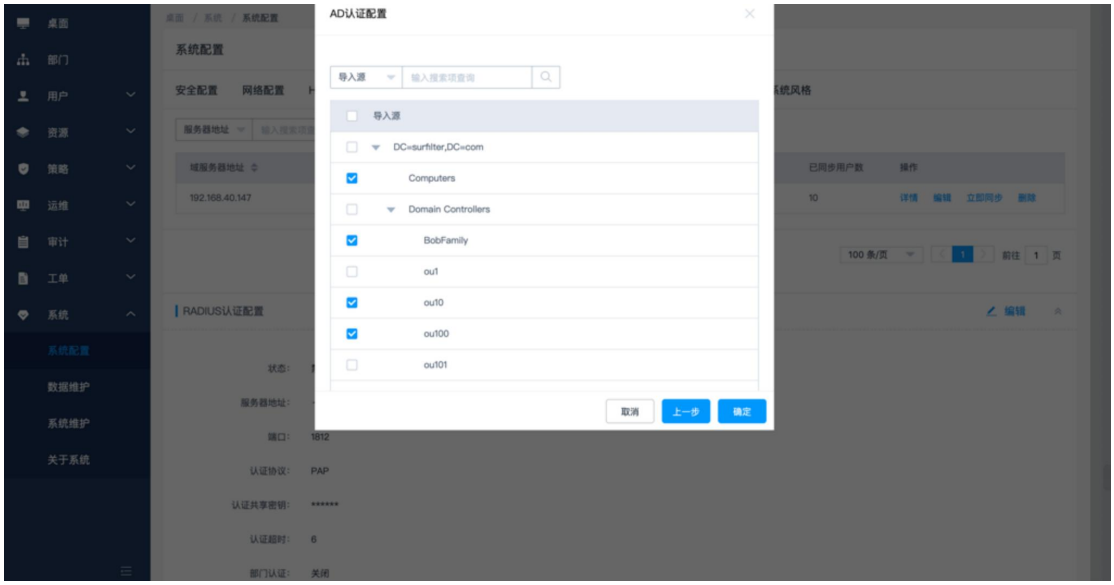


图 11-21

注：

域认证模式是指新建用户时认证类型为 AD 域认证，使用域服务器进行认证机制。

域同步模式是直接同步域服务器上的用户到堡垒机，然后进行认证。

11.6.2 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 11-22

图 11-22

11.6.3 LDAP 认证配置

云堡垒还支持 LDAP 认证。进入 LDAP 认证配置页面，点击添加 LDAP 服务器，填写正确的 LDAP 服务器地址，端口，OU，选择过滤器类型，点击确定可添加。如图 11-23

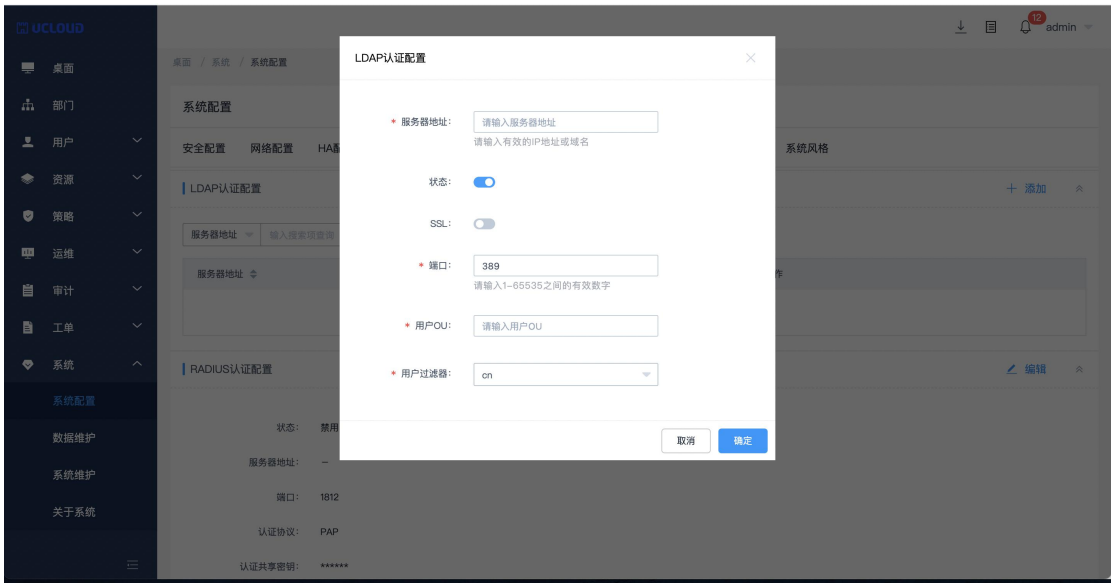


图 11-23

11.6.4 CAS 配置

第三方 CAS 服务器配置信息在 CAS 配置点编辑，状态开启，填写正确的 CAS 登录服务地址，CAS 服务器部署地址，redirect_url 等信息。如图 11-24

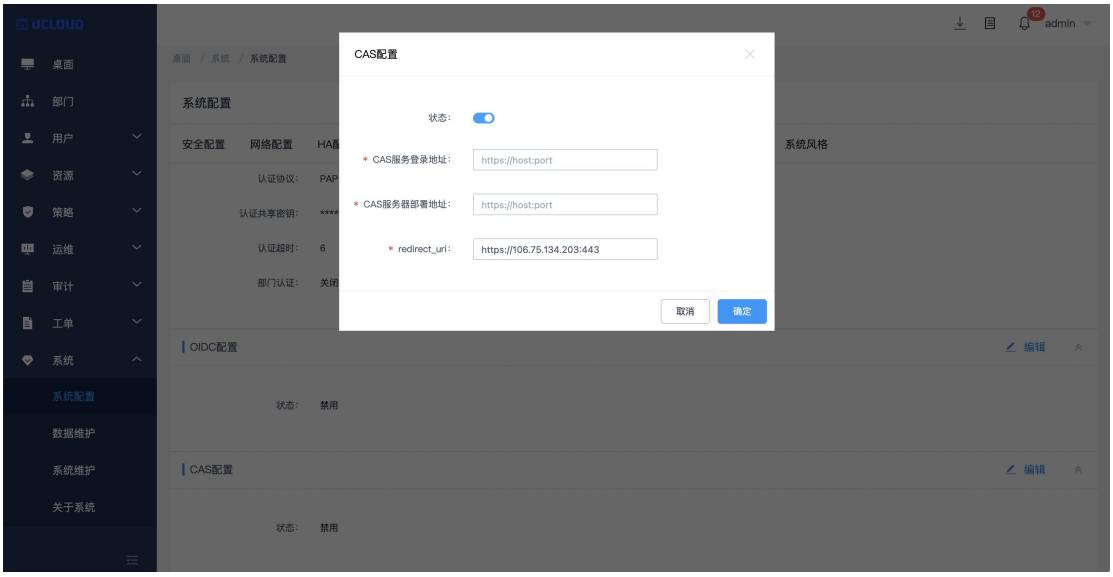


图 11-24

11.7 工单配置

11.7.1 基本模式

基本模式中可配置访问授权工单申请时的申请范围和命令授权工单的提交方式。如图 11-25

图 11-25

11.7.2 高级模式

高级模式中可配置指定部门的用户、角色可以申请指定部门的资源。为用户池和资源池添加用户所属部门和资源所属部门。如图 11-26

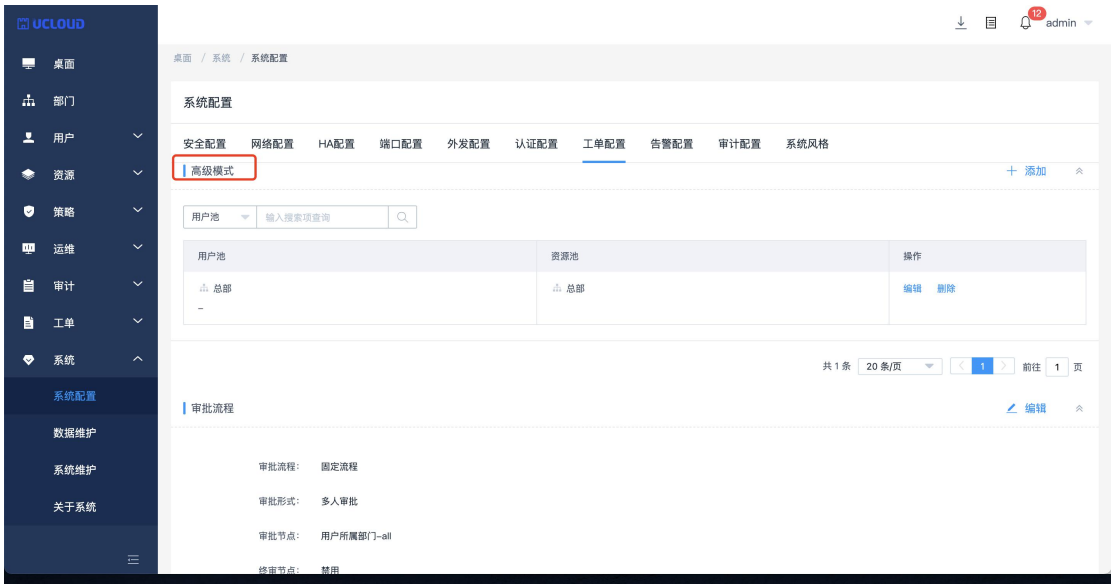


图 11-26

11.7.3 审批流程

审批流程设置为分级流程时，系统将自动按照指定的审批节点设置到指定的所属部门寻找对应的角色用户作为节点，设置为固定流程时，则按照配置寻找节点用户，上限添加 5 个用户。审批形式设置为多人审批时，每级仅需一个节点进行批准就能通过审批。设置为会签审批时，则需要同一级的所有节点都批准了工单，工单才能进入下一级审批。审批节点由两部分属性决定，分别为部门属性和角色属性，部门属性固定有用户所属部门和资源所属部门，角色需要有管理权限和工单审批权限，只要在指定的部门里的指定角色的用户会自动成为审批节点，如果用户或资源所在的部门没有对应角色的用户，则自动往上级部门寻找，直到找到总部为止。审批级数指的是通过工单需要的最大次数，设置为 1 时，则需要一个节点进行审批，如果开启了终审，则还需要 admin 用户进行一次审批，级数仅在分级流程时开启，如工单无节点，那么无论有没有开启终审，都由 admin 审批。如图 11-27

图 11-27

11.8 告警配置

11.8.1 告警方式配置

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 11-28

图 11-28

11.8.2 告警等级配置

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 11-29

图 11-29

11.9 审计配置

进入审计配置可查看到当前 OCR 的状态，启用 OCR 后可对图形协议进行文字识别。只对图形协议有效。输入正确的 OCR 地址即可。如图 11-30

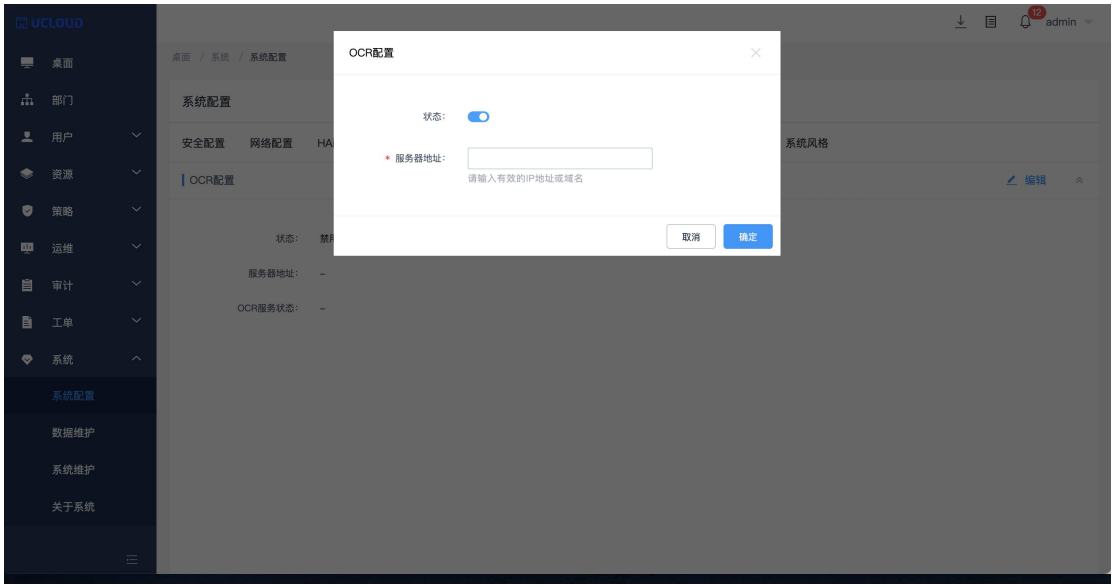


图 11-30

11.10 系统风格

进入系统风格后，可更改系统语言，和企业图标。如图 11-31

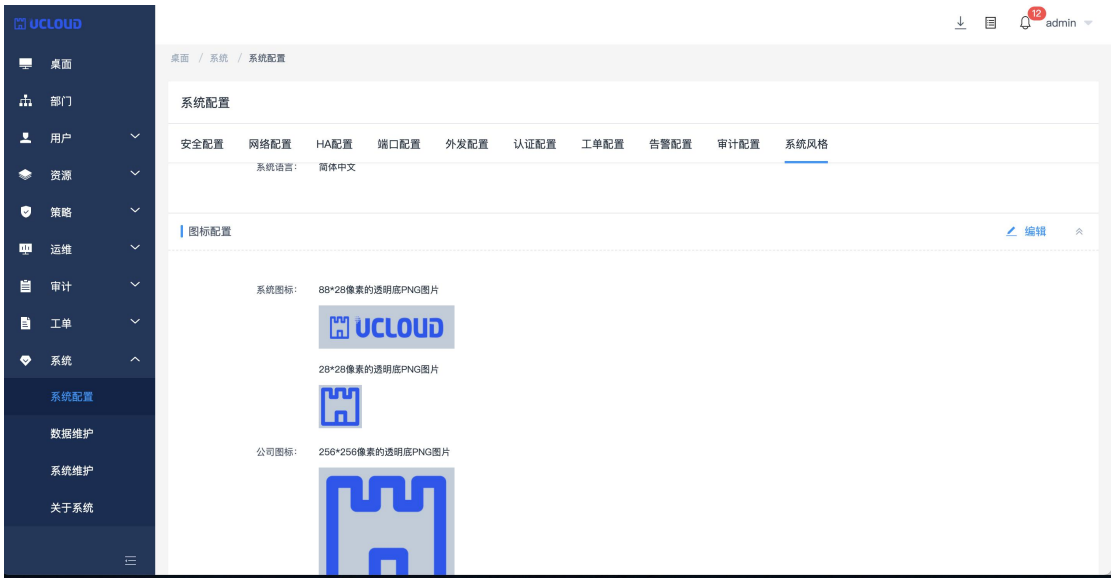


图 11-31

11.11 数据维护-存储配置

11.11.1 存储概览

存储概览主要展示当前堡垒机系统的系统分区和数据分区的空间使用量。如图 11-32

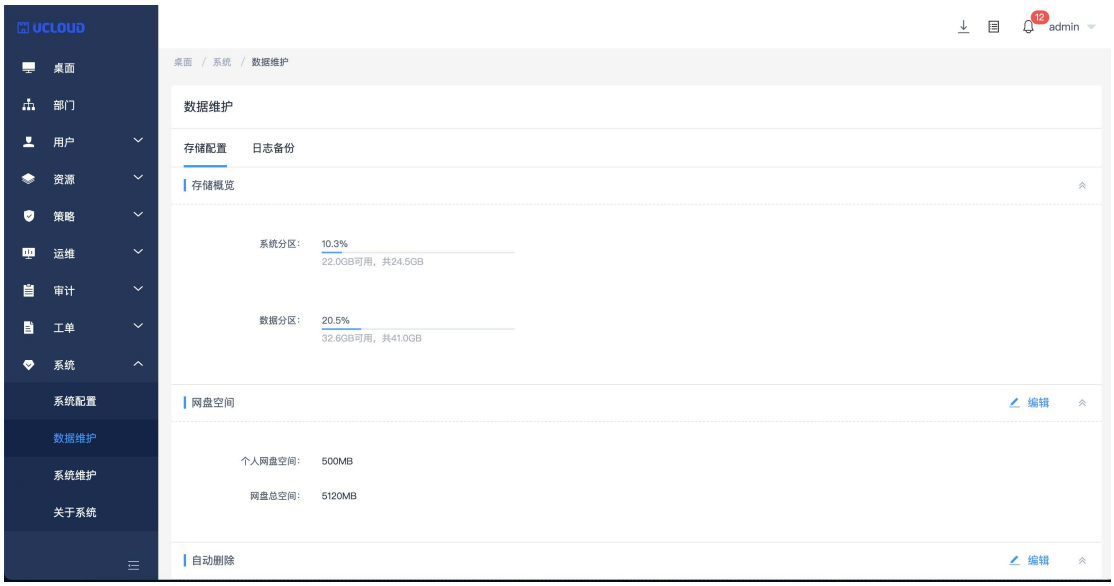


图 11-32

11.11.2 网盘空间

网盘空间可查看更改个人网盘空间和总空间。如图 11-33

图 11-33

11.11.3 自动删除

自动删除用户是否开启磁盘自动清除，和空间满是自动覆盖最早的数据，自动删除默认为删除 180 天前的数据，如 180 天前的数据删除完后磁盘还是无空间，则继续一天一天往前自动删除。配置如图 11-34

图 11-34

11.11.4 手动删除

支持手动删除选择日期天前的数据。如图 11-35

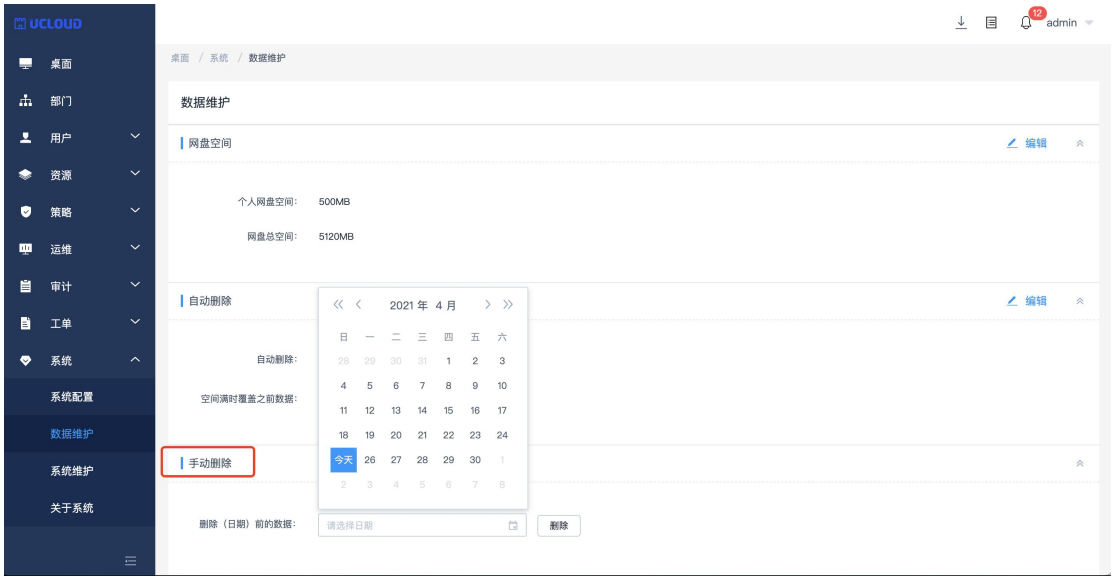
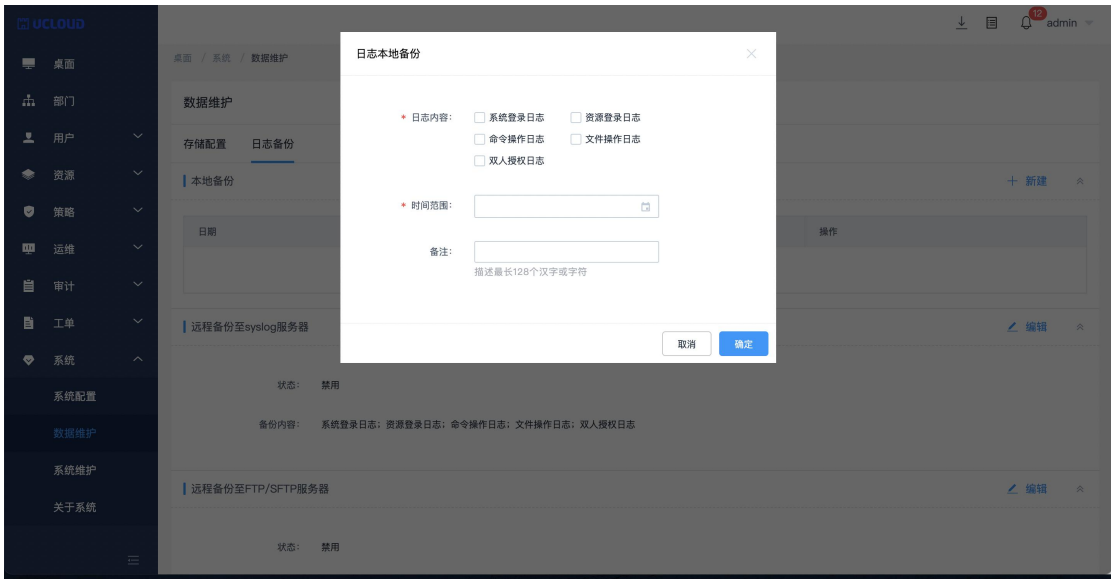


图 11-3



11.12 数据维护-日志备份

11.12.1 本地备份

进入日志备份，点击本地备份右边的新建，选择要备份的日志内容，和时间范围，点击确定即可完成备份。如图 11-36

图 11- 36

11.12.2 远程备份至 syslog 服务器

点击编辑配置 syslog 服务器，填写标识后输入正确的 syslog 服务器地址，勾选备份内容后，当执行了备份内容中的操作时，会自动备份到 syslog 服务器中。配置如图 11-37

图 11-37

11.12.3 远程备份至 FTP/SFTP 服务器

点击编辑将状态改为开启状态后可选择 FTP/SFTP 服务器，输入正确的参数后可选择备份内容，支持系统配置和会话回放日志。支持手动备份今天之前的日志到 FTP/SFTP 服务器上。配置如图 11-38

图 11-38

11.13 系统维护-系统状态

进入系统状态可查看 CPU/内存使用率，磁盘读写状态和网络收发状态，点击可展开。如图 11-39

图 11- 39

11.14 系统维护-系统管理

进入系统管理可查看到当前系统地址，系统时间（输入正确的时间服务器地址可同步时间），系统升级（点击升级后上传正确的升级包，点击确认升级，系统即可自动升级），系统工具（具有重启，关机和恢复出厂设置功能）。如图 11-40

图 11- 40

11.15 系统维护-配置备份与还原

11.15.1 备份列表

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。可将备份文件下载到本地。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 11-41

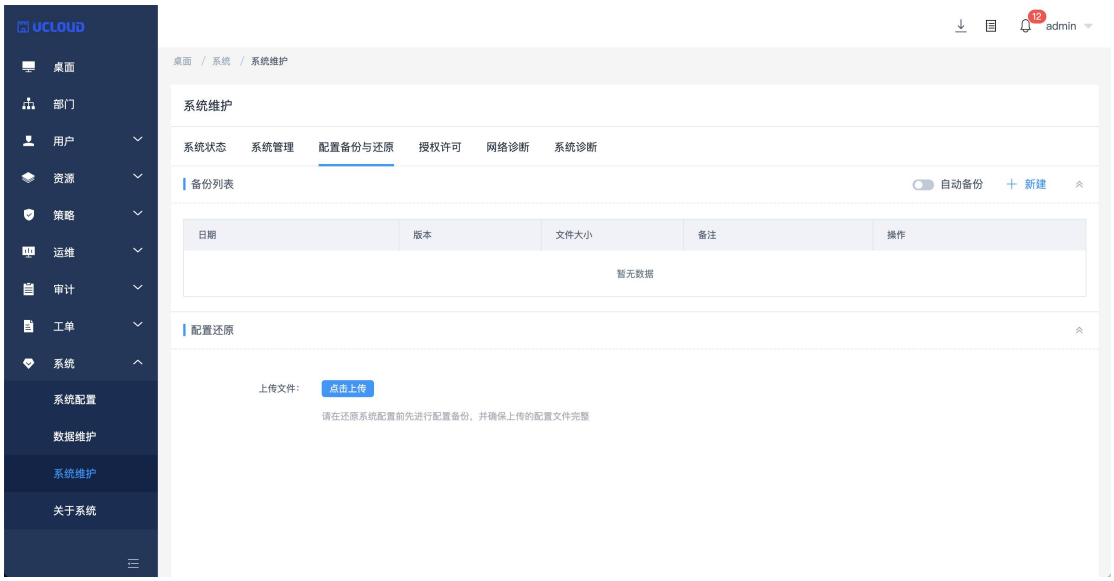


图 11-41

11.15.2 配置还原

点击上传文件后，上传备份文件即可看到弹窗：是否还原配置，点击确定后可还原。如图 11-42

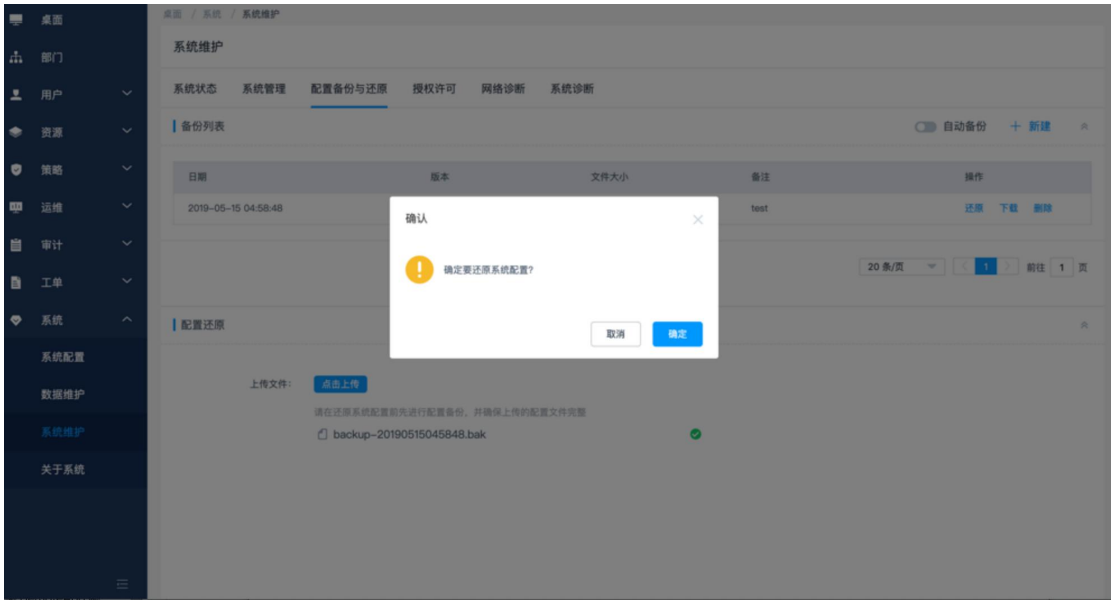


图 11-42

11.16 系统维护-授权许可

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，上传售后人员发来的授权文件，完成更新授权。如图 11-43

图 11-43

11.17 系统维护-网络诊断

进入网络诊断后，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 11-44

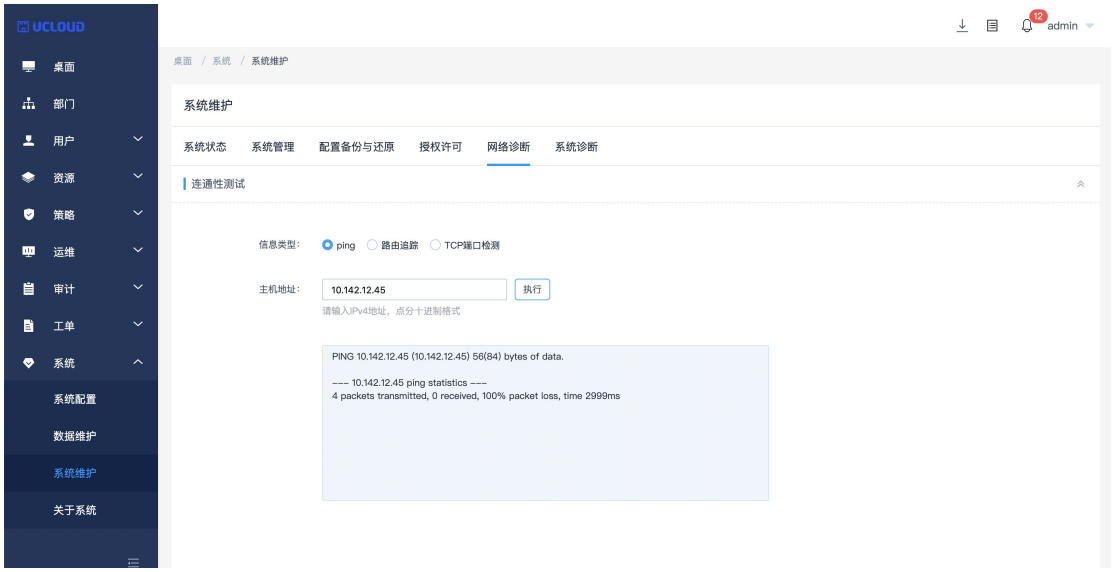


图 11-44

11.18 系统维护-系统诊断

进入系统诊断后，可选择信息类型获取信息。如图 11-45

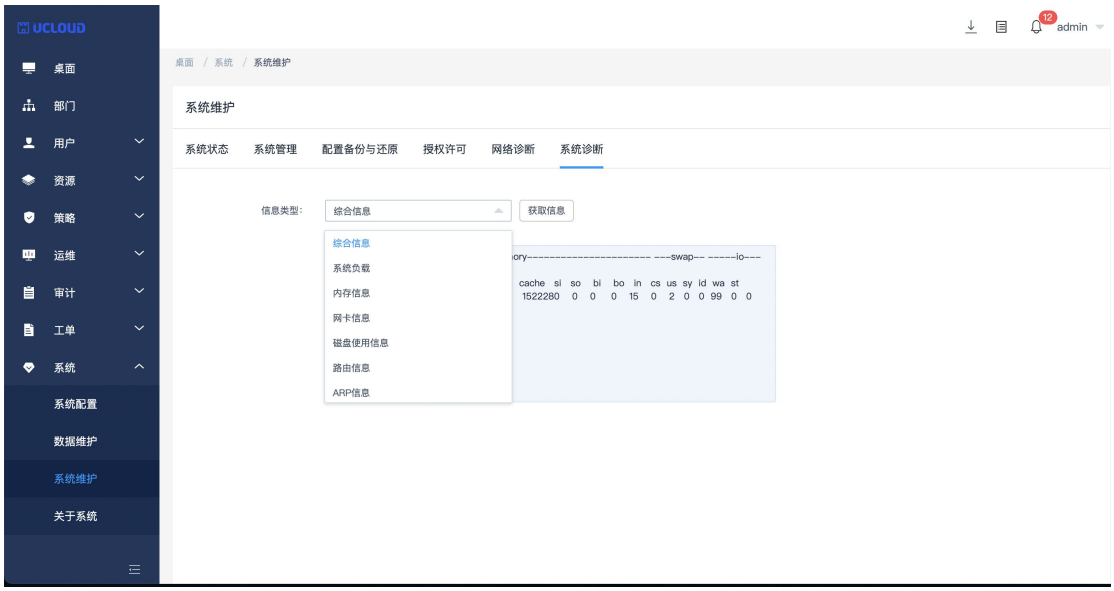


图 11-45

11.19 关于系统

进入系统-关于系统可查看当前系统相关内容。如图 11-46

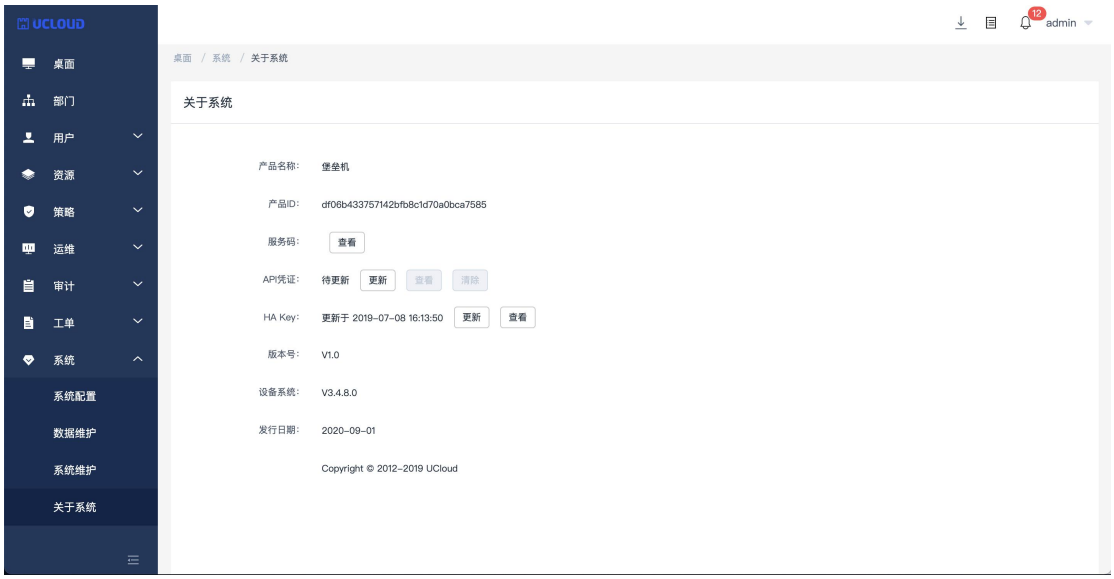


图 11-46

12 附录

12.1 应用发布服务安装配置

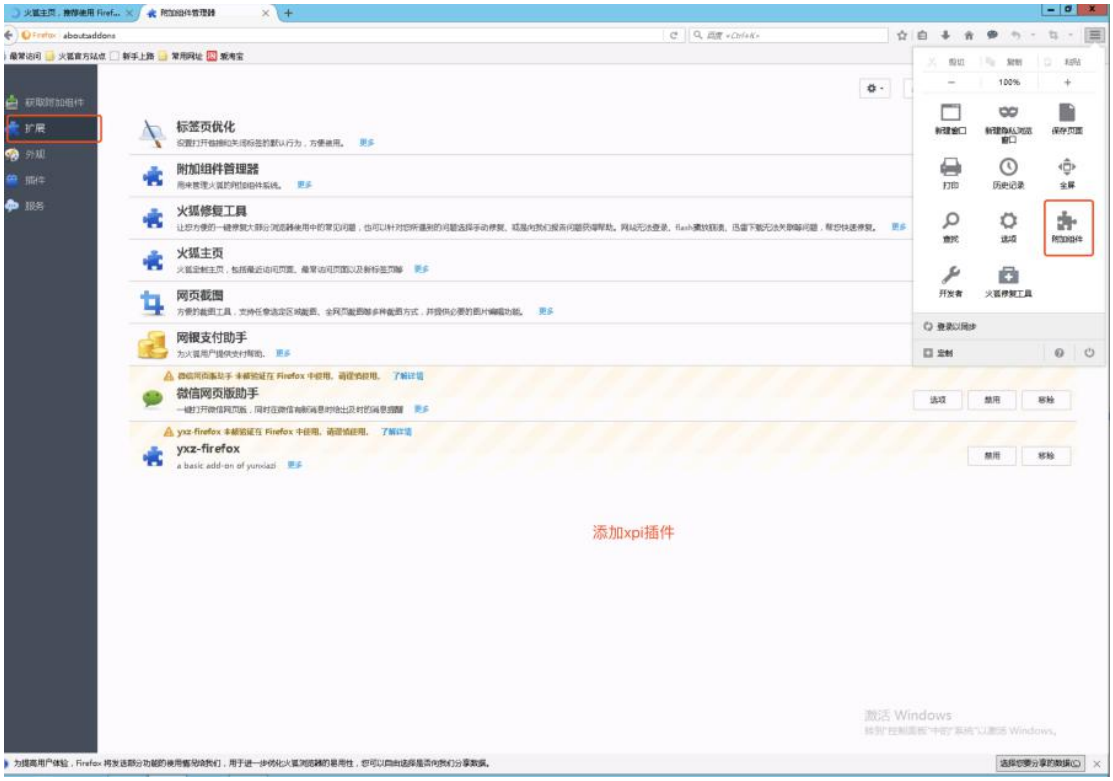
应用发布服务器要完成自动代填，需要进行配置才可以；以下附上配置方法：

12.1.1 安装 RemoteApp 跳板程序

(前提需要微软的.Net 框架)，程序请向售后人员等索要；

12.1.2 配置 FireFox

配置 FireFox；首先安装 FireFox，然后在命令行中执行命令 "FireFox 安装目录\firefox.exe" -no-remote -p default，执行完命令后会启动 Firefox 浏览器，这时候找到"附加组件-扩展-从文件中安装附加组件"将插件（该插件由售后人员提供）安装到浏览器，



拖放并安装好插件后，打开 C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles，检查是否存在一个*.default 的文件夹，并将该文件夹下的内容拷贝到 C:\DevOpsTools\RemoteAPPProxy\Browser\Firefox\fc4fa298.default 替换

（先将 fc4fa298.default 目录下文件清空再粘贴），在目录 C:\DevOpsTools 下创建文件夹 Firefox，文件夹包含文件有 firefox.bat、firefox.exe、firefox.vbs、md5.vbs（请向售后人员等索要），确保 vbs 脚本编码格式是 ANSI，通过另存为可以看到编码格式，如果是其他编码格式请修改为 ANSI 格式保存

12.1.3 配置 Chrome

配置 Chrome，与 FireFox 类似，首先安装 Chrome，在 cmd 命令行执行 start chrome.exe --user-data-dir=C:\User\chromeaccounts\default，执行完命令后会打开 Chrome 浏览器，打开拓展程序安装界面,拖拽代填插件 chrome.crx 插件（售后人员提供）到 chrome 浏览器中进行安装，然后到文件目录 C:\User\chromeaccounts 查看是否有 default 文件夹，并将 default 文件夹下的内容拷贝到 C:\DevOpsTools\RemoteAPPProxy\Browser\Chrome\Default 替换，在目录 C:\DevOpsTools 下创建文件夹 Chrome，文件夹包含文件有 chrome.bat、chrome.exe、chrome.vbs（请向售后人员等索要），确保 vbs 脚本编码格式是 ANSI，通过另存为可以看到编码格式，如果是其他编码格式请修改为 ANSI 格式保存