

JumpServer 产品手册

管理员使用手册 V3.10

2024.01

免责声明

本文档“按原样”提供。FIT2CLOUD, Inc. 不承诺与本文档相关的所有保证, 包括但不限于对适销性和特定用途适用性的默示保证。本文档可能含有技术或其他方面的错误或印刷错误。FIT2CLOUD, Inc. 保留随时修订本文档中的信息的权利, 如有更改, 恕不另行通知。本文档及本文档中介绍的软件属 FIT2CLOUD, Inc. 及其许可发放方的机密信息, 依据 FIT2CLOUD, Inc. 的许可提供。

FIT2CLOUD, Inc.、FIT2CLOUD 徽标是 FIT2CLOUD, Inc. 和或其附属公司的商标, 已在中国国专利商标局和其他国家/地区注册。所有其他商标和注册商标为各自所有者的资产。

商标

FIT2CLOUD®

商标

FIT2CLOUD®

目录

免责声明	1
前言	8
概述	8
预期读者	8
获取帮助	8
1. 快速入门	10
1.1. 资产创建	10
1.1.1. 资产示例	10
1.1.2. 编辑资产树	10
1.1.3. 创建资产	11
1.2. 创建授权规则	12
1.3. 用户登录资产	14
1.4. 系统设置	14
1.4.1. 基本设置	14
1.4.2. 邮件设置	15
1.4.3. 用户对接	15
2. 视图介绍	16
3. 个人信息	18
3.1. 用户信息	18
3.2. 认证设置	19
3.3. 偏好设置	19
3.3.1. 基本	19
3.3.2. Luna 配置设置	20
3.3.3. Koko 配置设置	21
3.4. API Key	22
3.5. 临时密码	24
3.6. 连接令牌	24
4. 系统设置	26

4.1. 概览	26
4.2. 基本设置	27
4.3. 组织管理	27
4.4. 消息通知	28
4.4.1. 邮件设置	29
4.4.2. 短信设置	30
4.4.3. 消息订阅	32
4.5. 功能设置	33
4.5.1. 公告	34
4.5.2. 工单	35
4.5.3. 任务中心	35
4.5.4. 账号存储	36
4.5.5. 智能问答	37
4.5.6. 虚拟应用	37
4.6. 认证设置	38
4.6.1. 基本	38
4.6.2. LDAP	39
4.6.3. CAS	41
4.6.4. Passkey	42
4.6.5. OIDC	42
4.6.6. SAML2	44
4.6.7. OAuth2	45
4.6.8. 企业微信	47
4.6.9. 钉钉	52
4.6.10. 飞书	56
4.6.11. Radius	62
4.7. 存储设置	63
4.7.1. 对象存储	64
4.7.2. 命令存储	65
4.8. 组件设置	67

4.8.1. 基本设置	67
4.8.2. 组件管理	70
4.8.3. 组件监控	71
4.8.4. 服务端点	71
4.8.5. 端点规则	73
4.9. 远程应用	73
4.9.1. 远程应用	74
4.9.2. 应用发布机	79
4.10. 安全设置	82
4.10.1. 认证安全	83
4.10.2. 登录限制	84
4.10.3. 密码安全	85
4.10.4. 会话安全	86
4.11. 界面设置	86
4.11.1. 基本设置	86
4.11.2. Logo	87
4.11.3. 图片	89
4.11.4. 备案	89
4.12. 系统工具	89
4.13. 系统任务	90
4.13.1. 任务列表	90
4.13.2. 定期清理	91
4.14. 许可证	92
5. 控制台	94
5.1. 仪表盘	94
5.2. 用户管理	95
5.2.1. 用户列表	95
5.2.2. 用户组	102
5.2.3. 角色列表	107
5.3. 资产管理	112

5.3.1. 资产列表	112
5.3.2. 网域列表	124
5.3.3. 平台列表	127
5.4. 账号管理	129
5.4.1. 账号列表	130
5.4.2. 账号模版	132
5.4.3. 账号推送	133
5.4.4. 账号收集	135
5.4.5. 账号改密	138
5.4.6. 账号备份	141
5.5. 权限管理	143
5.5.1. 资产授权	143
5.5.2. 用户登录	151
5.5.3. 命令过滤	152
5.5.4. 资产登录	157
5.5.5. 连接方式	158
5.6. 更多选项	159
5.6.1. 标签列表	159
6. 审计台	161
6.1. 仪表盘	161
6.2. 在线用户	162
6.3. 会话审计	162
6.3.1. 会话记录	163
6.3.2. 命令记录	166
6.3.3. 文件传输	166
6.4. 日志审计	167
6.4.1. 登录日志	167
6.4.2. 操作日志	168
6.4.3. 改密日志	169
6.4.4. 作业日志	169

7. 工作台	171
7.1. 概览	174
7.2. 我的资产	174
7.3. Web 终端	176
7.3.1. 组织切换	176
7.3.2. 批量资产连接	177
7.3.3. 会话拖拽	177
7.3.4. 会话切换	178
7.3.5. 会话分屏	178
7.3.6. 资产连接	178
7.3.7. 文件管理	193
7.3.8. 视图	194
7.3.9. 语言	194
7.3.10. 设置	194
7.3.11. 帮助	195
7.3.12. 窗口列表	196
7.4. 文件管理	196
7.4.1. 批量传输	196
7.4.2. 文件管理	197
7.5. 作业中心	200
7.5.1. 快捷命令	200
7.5.2. 作业管理	201
7.5.3. 模版管理	202
7.5.4. 执行历史	203
8. 工单	205
8.1. 我的申请	205
8.1.1. 申请工单	205
8.1.2. 查看工单	206
8.1.3. 关闭工单	207
8.2. 待我审批	207

8.3. 流程设置	209
8.3.1. 查看	209
8.3.2. 更新	210
9. 其他	211
9.1. 命令行连接	211
9.2. 命令行直连 JumpServer 纳管的资产	211
9.3. SFTP 命令行操作 JumpServer 纳管的资产	212
9.3.1. 图形化连接	213
9.3.2. 命令行连接	214
9.4. VSCode 连接 JumpServer 纳管的资产	216
9.4.1. VSCode 配置	217
9.4.2. 连接资产	217

前言

概述

感谢您选择 JumpServer 堡垒机。本手册详细描述了 JumpServer 堡垒机（以下简称“JumpServer”或“系统”）的使用方法，包括 JumpServer 快速入门、个人信息、系统设置、控制台、审计台、工作台、工单等模块。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、不同项目配置文件不相同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用 JumpServer 的人员，包括系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、HTTP 等基础网络通讯协议。
- 数据库、服务器、路由器、交换机等常见设备（系统）的基本工作原理和配置、操作。
- 堡垒机和网络安全运维工具的基本工作原理和操作。

获取帮助

当您在使用 JumpServer 过程中遇到任何问题，请联系企业微信群中的支持人员、QQ 群中的在线支持人员或者登录飞致云支持门户 <https://support.fit2cloud.com/> 提交工单、拨打 400-052-0755 寻求帮助。

公司各区域联系地址：

- 北京：北京市朝阳区东三环中路 7 号财富中心写字楼 A 座 501 室、715 室。
- 上海：上海市徐汇区宜山路 425 号光启城 1008 室。
- 深圳：广东省深圳市福田区金田路 2030 号卓越世纪中心 4 栋 1005 室。
- 广州：广东省广州市天河区华强路 9 号保利克洛维中盈 2410A 单元。

- 杭州：浙江省杭州市西湖区云栖小镇山景路 7 号 3 幢 2 楼 201 室。
- 杭州：浙江省杭州市上城区民心路 100 号万银国际 505 室。
- 南京：江苏省南京市建邺区河西大街 66 号（徐矿广场）写字楼 A 座 802 。
- 成都：四川省成都市高新区天府大道 666 号希顿国际广场 C 座 2402 室 。
- 武汉：湖北省武汉市洪山区关山大道 101 号光谷时代广场 A 座 902 室。
- 苏州：江苏省苏州市吴中区宝带东路 399 号中润中心 1222 室 。
- 西安：陕西省西安市碑林区长安大街 3 号 1 号楼 A 座 1405 室 。
- 济南：山东省济南市历下区解放东路 6-17 号中弘广场 D 座 12 层 1203 室 。
- 青岛：山东省青岛市市北区龙城路 31 号卓越世纪中心 Tower3-3205 室 。
- 郑州：河南省郑州市二七区航海中路升龙城二七中心 A 座 1320 室。
- 长沙：湖南省长沙市岳麓区桐梓坡西路 139 号长房时代天地 1411 室。
- 厦门：福建省厦门市思明区宜兰路 9 号康利金融大厦 2501 单元 。
- 合肥：安徽省合肥市包河区绿地中心 E 座 1716 室。
- 重庆：重庆市渝中区五一路 99 号平安国际金融中心 2605-2 室。

1. 快速入门

快速入门模块帮助用户快速实现通过 JumpServer 纳管资产并成功连接。JumpServer 管理员纳管一个资产的步骤如下：

- 资产创建
- 资产授权
- 资产登录

1.1. 资产创建

JumpServer 支持纳管多种类型的资产，快速入门以 Windows 资产、Linux 资产和数据库资产为例进行快速入门演示。

1.1.1. 资产示例

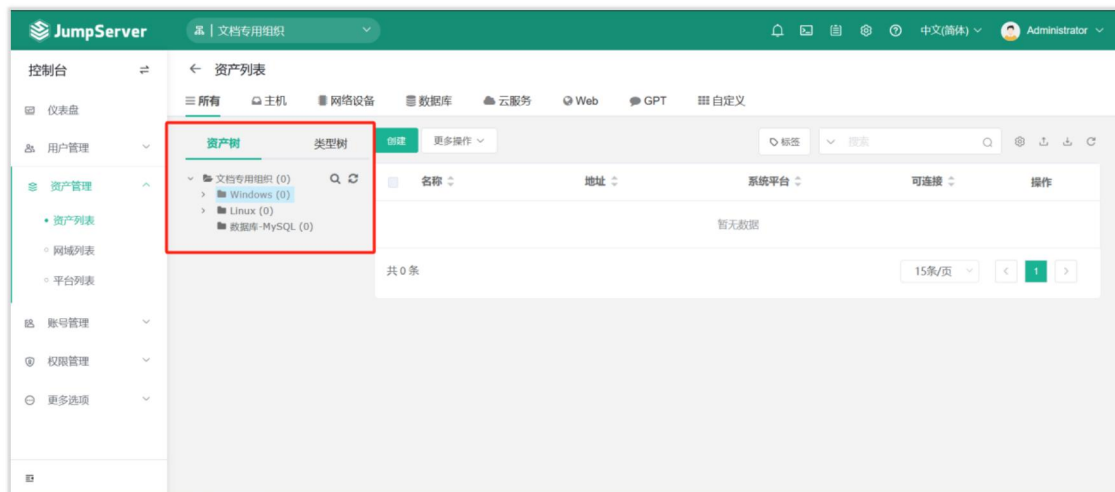
IP	主机名称	端口	系统	登录用户
10.1.12.182	Linux-SSH	22	CentOS 7	root
10.1.12.16	Windows-RDP	3389	Windows 2019	Administrator
10.1.12.116	MySQL-5.7	3306	MySQL 5.7	root

注：

- Windows 资产如果需要执行自动化任务，例如：获取硬件信息、可连接性测试等，需在 Windows 资产上安装 OpenSSH 服务。
- Windows 资产新增支持了 WINRM 协议，例如：修改账号改密等可以使用 WINRM 协议，需要在 Windows 上面开启 WINRM 协议对于端口。
- MySQL 资产连接时需要授权登录用户远程访问的权限。

1.1.2. 编辑资产树

资产树即资产分组，后续授权可按资产树节点授权。右击资产树根节点【根节点的名称为当前组织的名称】，创建资产树节点如下图所示：



注：

- 资产树根节点 **Default** 不能重命名。【根节点的名称为当前组织的名称】
- 右击资产树节点名称可以对节点进行增加、删除、修改命名等操作。
- 资产列表中的资产数量与资产树显示的资产数量不一致时，可右击资产树，执行“校对资产数量”任务。

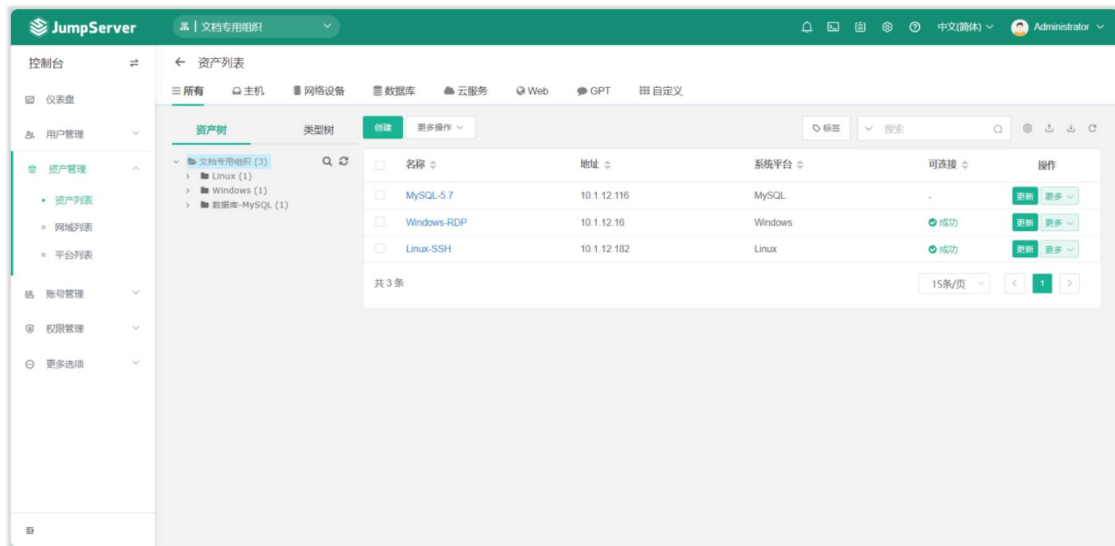
1.1.3. 创建资产

点击页面左侧的“资产管理”下拉框选择“资产列表”按钮进入资产列表页面，点击主机页签选择创建按钮，创建一台 Linux 服务器。在创建资产过程中，同步创建资产的登录用户，内容就是上面表单的账号列表。Windows 资产的创建流程同样如此。





资产创建成功即如下图所示：



1.2. 创建授权规则

点击页面左侧的“权限管理”下拉框选择“资产授权”按钮进入资产授权页面。点击创建按钮，创建一条授权规则，Windows 授权、数据库授权均如下图：

JumpServer

基 | 文档专用组织

🔔 📧 🏠 ⚙️ 🕒 中文(简体) Administrator

控制台

仪表盘

用户管理

资产管理

账号管理

权限管理

- 资产授权
- 用户登录
- 命令过滤
- 资产登录
- 连接方式

更多选项

创建资产授权规则

基本

名称Linux资产授权

用户

用户Administrator(admin) ×

用户组请选择

资产

资产Linux-SSH(10.1.12.182) ×

节点请选择

账号

账号☒ 所有账号 ☐ 指定账号 ☐ 手动账号 ☐ 同名账号 ☐ 匿名账号

JumpServer

基 | 文档专用组织

🔔 📧 🏠 ⚙️ 🕒 中文(简体) Administrator

控制台

仪表盘

用户管理

资产管理

账号管理

权限管理

- 资产授权
- 用户登录
- 命令过滤
- 资产登录
- 连接方式

更多选项

协议

协议☒ 所有 ☐ 指定协议

权限

权限☒ 全部

- ☒ 连接
- ☒ 文件传输
 - ☒ 上传
 - ☒ 下载
 - ☒ 删除
- ☒ 剪贴板
 - ☒ 复制
 - ☒ 粘贴
- ☒ 分享

各个权限作用协议不尽相同，点击权限后面的图标查看

其它

激活中☒

开始日期2024-01-29 15:07:43

授权规则创建成功后如下图所示：

JumpServer

基 | 文档专用组织

🔔 📧 🏠 ⚙️ 🕒 中文(简体) Administrator

控制台

仪表盘

用户管理

资产管理

账号管理

权限管理

- 资产授权
- 用户登录
- 命令过滤
- 资产登录
- 连接方式

更多选项

资产授权

资产授权允许您选择用户和资产，将资产授权给用户以便访问。一旦授权完成，用户便可便捷地访问这些资产。此外，您还可以设置特定的权限位，以进一步定义用户对资产的权限范围。

资产树

文档专用组织 (3)

- Linux (1)
- Windows (1)
- 数据库-MYSQL (1)

创建更多操作

标签搜索

<input type="checkbox"/>	名称	用户	用户组	资产	节点	账号	操作
<input type="checkbox"/>	Linux资产授权	1	0	1	0	1	更新 更多
<input type="checkbox"/>	MySQL资产授权	1	0	1	0	1	更新 更多
<input type="checkbox"/>	Windows资产授权	1	0	1	0	1	更新 更多

共 3 条15条/页< 1 >

1.3. 用户登录资产

授权规则创建后,用户可点击页面右上角的<Web 终端>按钮进入 Web 页面,进行资产连接。

用户仅被允许查看和操作被管理员授权过的资产。



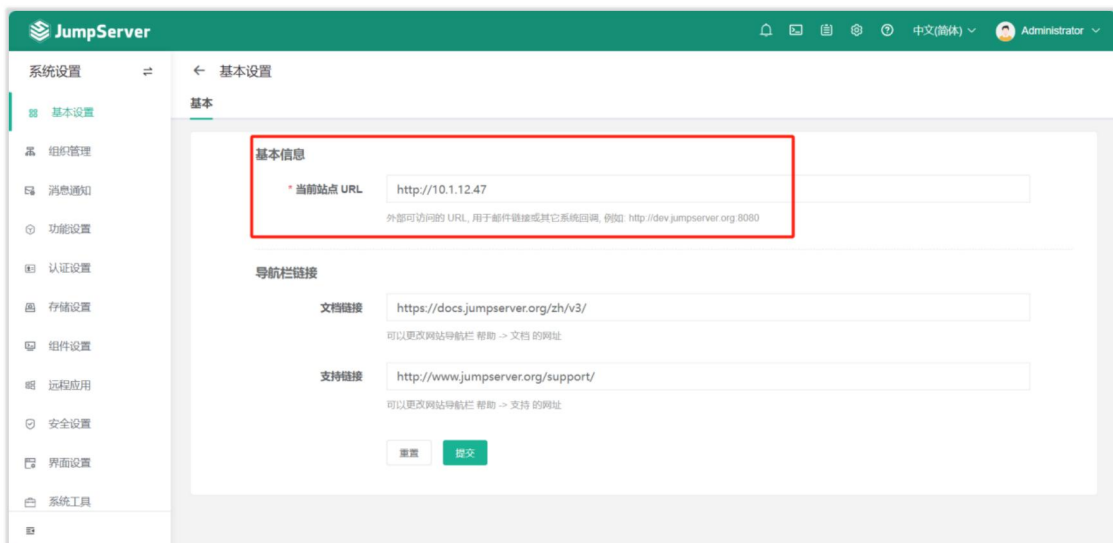
1.4. 系统设置

系统设置主要面向整个 JumpServer 平台,初次使用需配置的地方包含以下三个页面:

基本设置、邮件设置和用户对接。

1.4.1. 基本设置

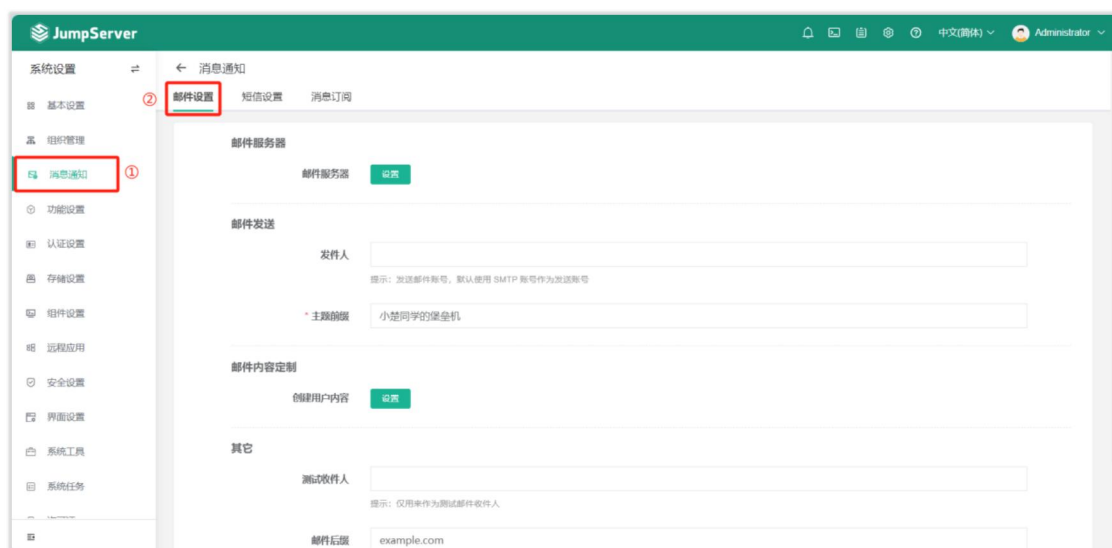
基本设置页面设置当前站点 URL,默认为 localhost,可能导致邮件等信息跳转链接错误。



其余信息可参考[正文-基本设置](#)。

1.4.2. 邮件设置

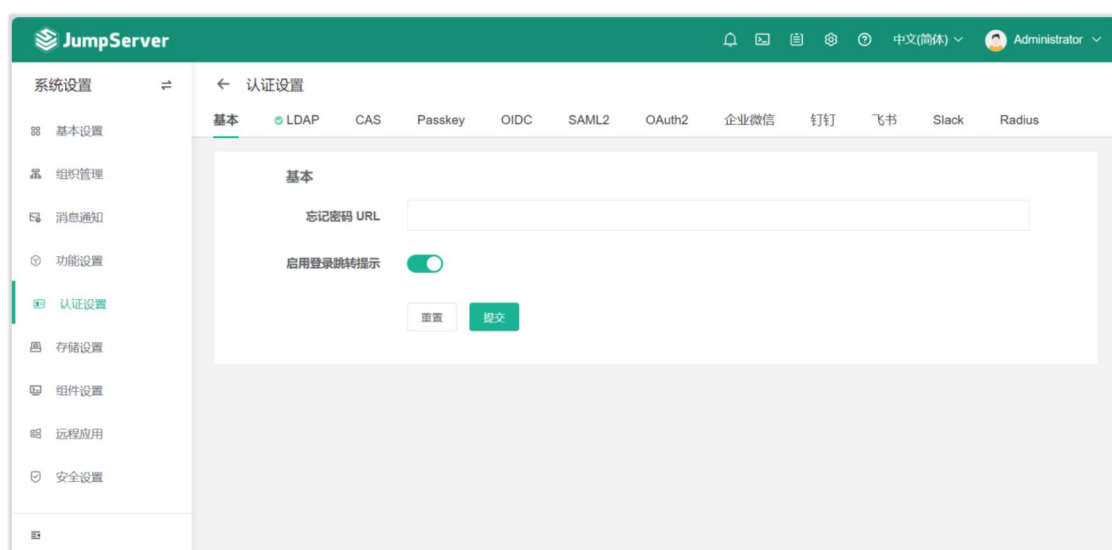
邮件为 JumpServer 系统中除站内信之外的第二大信息收发载体。



具体设置需要参考[正文-邮件设置](#)。

1.4.3. 用户对接

JumpServer 除了手动创建本地用户之外，还支持对接外部第三方系统进行用户认证。例如 LDAP、宁盾、钉钉等。



具体的用户对接配置可参考[正文-认证设置](#)。

2. 视图介绍

JumpServer 页面分为三大视图：“控制台”、“审计台”和“工作台”。点击主页左上方的控制台右侧的切换按钮，选择对应的视图进行切换。

页面右上角有工单模块、系统设置模块等，点击相应图标可进入对应的页面。



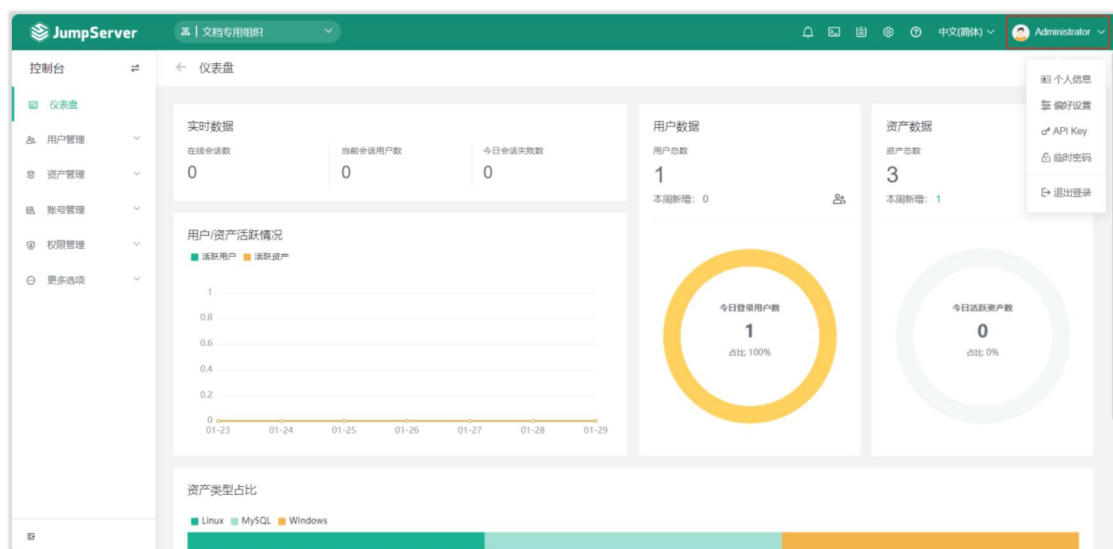
各区域功能说明：

序号	区域名称	说明
(1)	控制台	管理员操作入口。通过控制台，管理员可进行用户管理、资产管理、账号管理、权限管理等配置。
(2)	审计台	审计员操作入口。通过审计台，审计员可查看各会话的连接详细信息和 JumpServer 系统的各类型日志。 组织审计员只能够看到该组织下的审计日志信息。
(3)	工作台	普通用户操作入口。通过工作台，普通用户可以看到自己有权限操作的资产。
(4)	站内信	JumpServer 系统站内消息通知中心，接收工单处理提醒，服务告警信息等通知。
(5)	Web 终端	资产运维操作入口，通过 Web 终端进入资产连接页面，在此页面上进行连接操作。
(6)	工单	工单入口，通过该按钮进入工单页面，查看提交的工单、待审批的工单等。

(7)	系统设置	系统设置入口，通过该按钮进入系统设置中，配置系统认证，安全设置等各类型的系统参数。
(8)	帮助	帮助入口，通过该按钮进入帮助页面，可访问 JumpServer 产品知识网站和下载系统工具。
(9)	语言切换	语言切换入口，可以切换 JumpServer 页面的显示语言，包含：中文（简体）、 English 、日本語。
(10)	个人信息	个人信息入口，点击该按钮，查看个人账号信息，当前用户连接资产使用的资产令牌以及退出登录的按钮等。
(11)	组织切换	组织切换模块，可以切换至登录用户可管理的组织或用户可登录的组织。

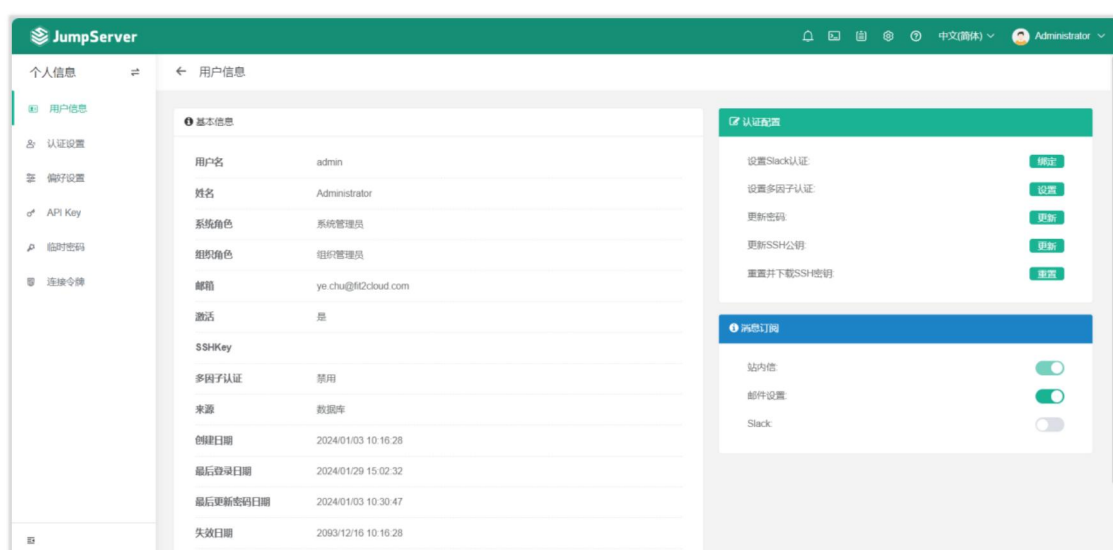
3. 个人信息

点击页面右上角的<用户名称>按钮进入个人信息界面，该页面主要查看个人账号信息，设置个人信息临时密码等等。



3.1. 用户信息

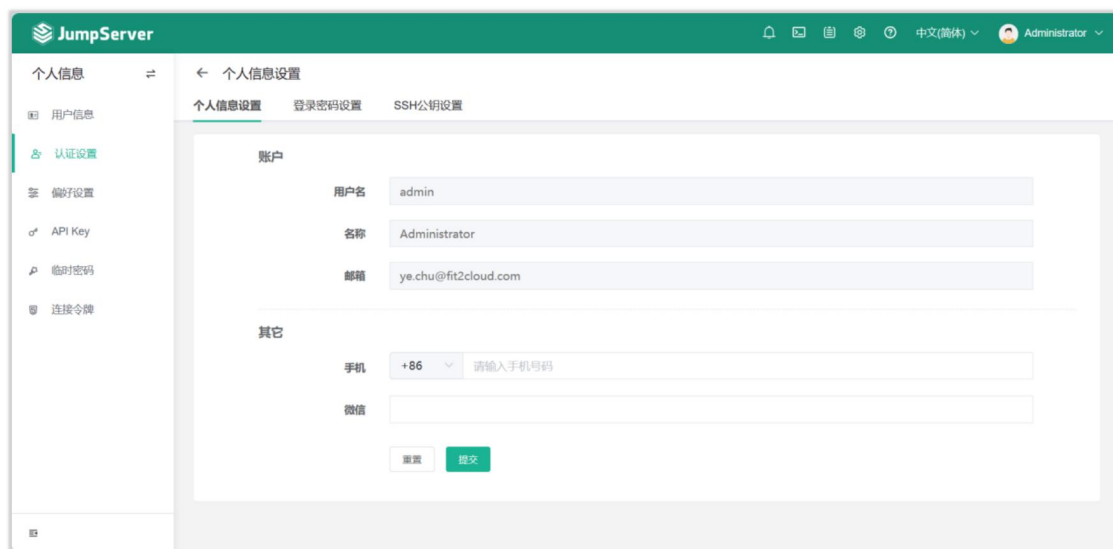
该页面可以查看用户的基本信息。该页面可以进行一些认证配置，例如多因子认证、登录密码、SSH 密钥等信息。同时可设置消息订阅，默认包含站内信和邮件设置，如果配置了企业微信或者钉钉，可以再此处配置相应的账号对接配置。



3.2. 认证设置

管理员用户在认证设置页面可对本人账号信息进行相应的认证配置和消息订阅配置。

- 个人信息设置页面：管理员用户可在此页面设置手机（手机号支持区号选择）、微信。当 JumpServer 开启短信 MFA 认证时，该手机号码用来接收短信；
- 登录密码设置页面：管理员用户可在此页面自行更新当前账户的密码；
- SSH 公钥设置页面：管理员用户可在此页面自行设置 SSH 公钥并下载，在使用 SSH 终端登录 JumpServer 时使用该公钥。



The screenshot shows the JumpServer web interface. The top navigation bar is green with the JumpServer logo and user information (Administrator). The left sidebar contains links for 'Personal Information', 'User Information', 'Authentication Settings', 'Preference Settings', 'API Key', 'One-time Password', and 'Connection Command'. The main content area is titled 'Personal Information Settings' and has three tabs: 'Personal Information Settings', 'Login Password Settings', and 'SSH Public Key Settings'. The 'Personal Information Settings' tab is active, showing a form with the following fields:

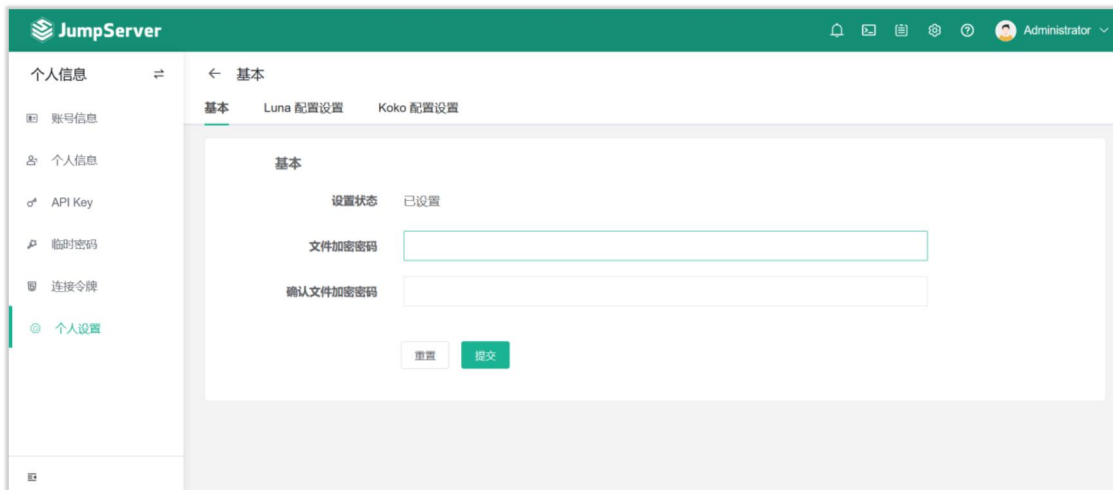
- Account:**
 - Username: admin
 - Name: Administrator
 - Email: ye.chu@fit2cloud.com
- Other:**
 - Phone: +86 (dropdown) [Please enter phone number]
 - WeChat: [Empty field]

At the bottom of the form are two buttons: 'Reset' (重置) and 'Submit' (提交).

3.3. 偏好设置

3.3.1. 基本

点击偏好设置页面中左侧页签<基本>按钮，可以对从 JumpServer 页面导出文件的加密密码进行设置。

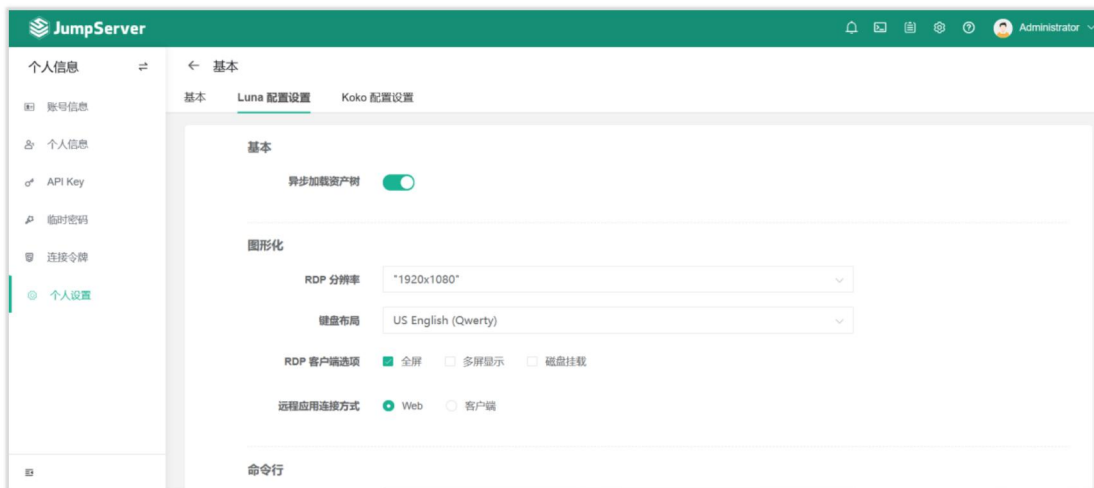


详细配置解释：

配置项	说明
文件加密密码	从 JumpServer 导出或者下载的文件中可能存在某些敏感信息，此处设置文件的加密密码。此处的文件加密密码仅适用于账号密码批量导出的场景中。

3.3.2. Luna 配置设置

点击个人设置页面中中间页签[<Luna 配置设置>](#)按钮，对 Luna 页面资产连接时的参数进行设置。



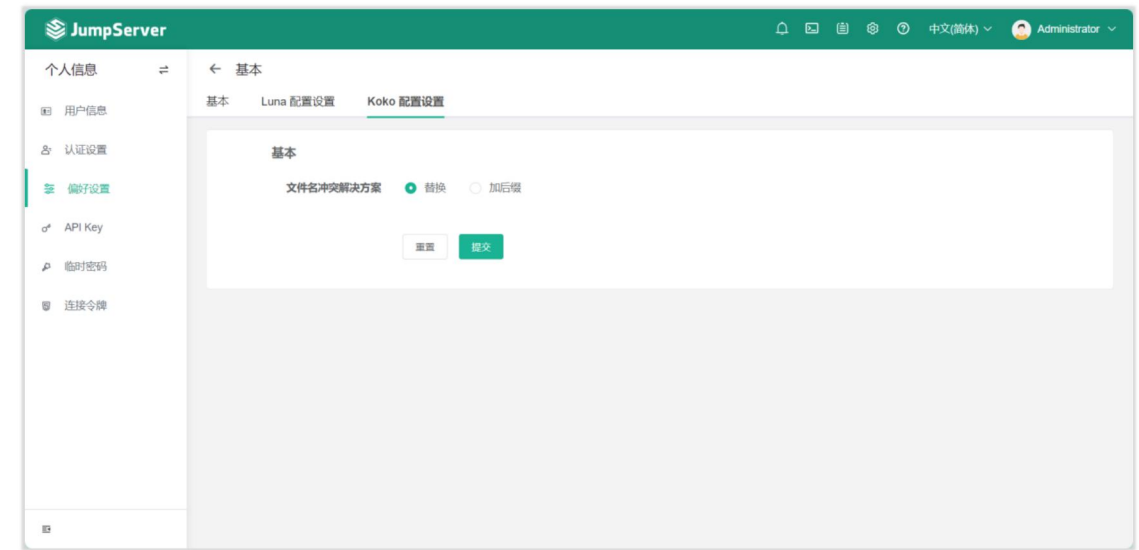
详细配置解释：

配置项	说明
异步加载资产树	资产连接中是否实时加载资产树。
RDP 分辨率	修改 RDP 分辨率，默认为 Auto。

键盘布局	选择连接 Windows 资产时使用的键盘布局。
RDP 客户端选项	RDP 客户端连接是否开启全屏与磁盘挂载。
RDP 颜色质量	选择远程会话的颜色深度。
RDP 智能大小	调整窗口大小时客户端计算机是否应缩放远程计算机上的内容以适应客户端计算机的窗口大小。
远程应用连接方式	选择远程应用的连接方式，Web 或者客户端方式。
字符终端字体大小	设置终端字体的大小显示。
字符终端 Backspace AS Ctrl+H	在命令行中是否开启快捷键 Ctrl+H 作为删除键。
右键快速粘贴	命令行是否开启右键快速粘贴。

3.3.3. Koko 配置设置

点击个人设置页面中中间页签<Koko 设置>按钮，对使用 Koko 组件进行资产连接时的参数进行设置。



详细参数解释：

配置项	说明
文件名冲突解决方案	当通过 KOKO 组件进行文件上传时，上传的文件跟原本目录中的文件冲突时选择替换原文件或者在新上传的文件中添加后缀。

3.4. API Key

JumpServer 支持多种 API 认证方式。其中使用 API key 签名请求头进行认证，每个请求的头部不一致，相对于永久 token 的认证方式，API Key 方式更加安全。点击此页面中的创建按钮，即可创建访问密钥。创建密钥时会显示创建密钥的 Secret，后续使用过程中不可再查看。以下为使用 API Key 进行认证的示例：

```
# Python 示例

# pip install requests drf-httpsig

import requests, datetime, json

from httpsig.requests_auth import HTTPSignatureAuth

def get_auth(KeyID, SecretID):

    signature_headers = ['(request-target)', 'accept', 'date']

    auth = HTTPSignatureAuth(key_id=KeyID, secret=SecretID, algorithm='hmac-sha256',
headers=signature_headers)

    return auth

def get_user_info(jms_url, auth):

    url = jms_url + '/api/v1/users/users/'

    gmt_form = '%a, %d %b %Y %H:%M:%S GMT'

    headers = {

        'Accept': 'application/json',

        'X-JMS-ORG': '00000000-0000-0000-0000-000000000002',

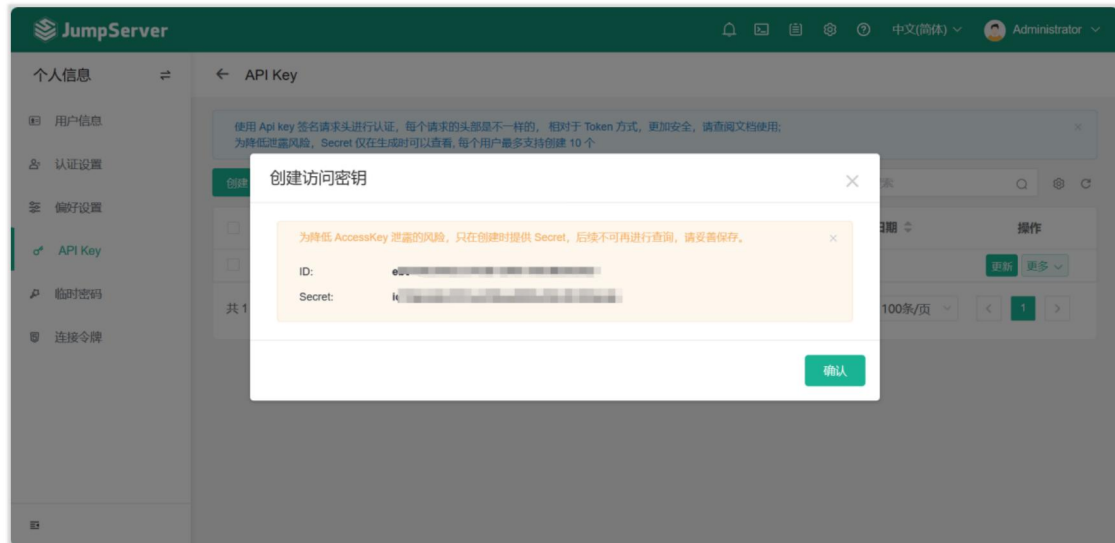
        'Date': datetime.datetime.utcnow().strftime(gmt_form)

    }

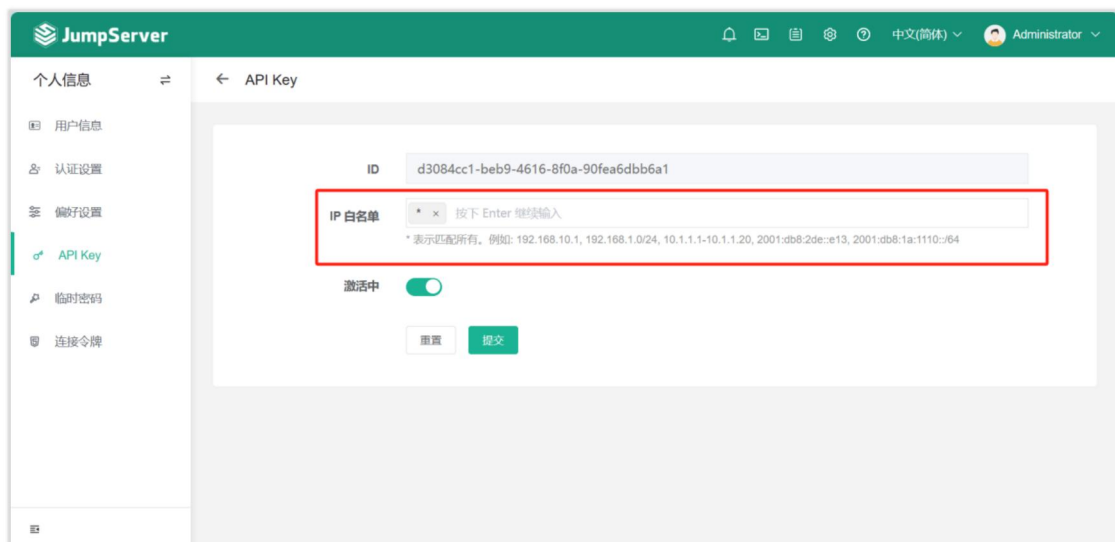
    response = requests.get(url, auth=auth, headers=headers)

    print(json.loads(response.text))
```

```
if __name__ == '__main__':  
  
    jms_url = 'https://demo.jumpserver.org'  
  
    KeyID = 'AccessKeyID'  
  
    SecretID = 'AccessKeySecret'  
  
    auth = get_auth(KeyID, SecretID)  
  
    get_user_info(jms_url, auth)
```



点击创建成功的 API Key 的<更新>按钮，可以支持配置白名单策略对非法的 IP 请求进行安全拦截，可提升 JumpServer 系统的安全性。



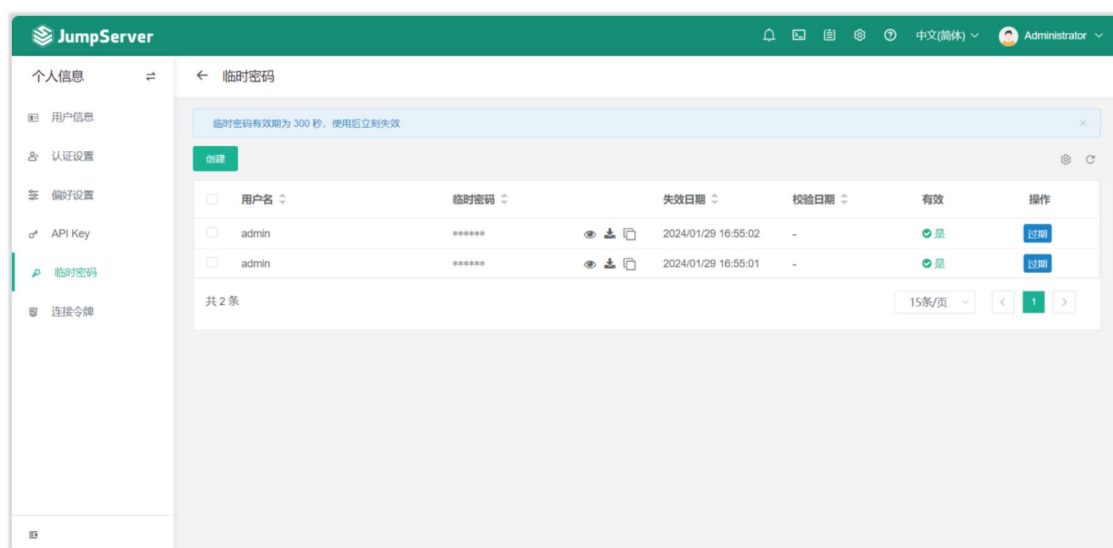
3.5. 临时密码

临时密码功能默认不开启，需管理员用户开启。开启需要在配置文件中添加选项，修改之后重启堡垒机服务生效。

JumpServer 配置文件默认位于：`/opt/jumpserver/config/config.txt`

开启临时密码功能的配置项为：`AUTH_TEMP_TOKEN=true`

JumpServer 支持使用临时密码登录 JumpServer。用户可在该页面创建一个临时密码，临时密码有效期为 300 秒，使用后临时密码立刻失效。

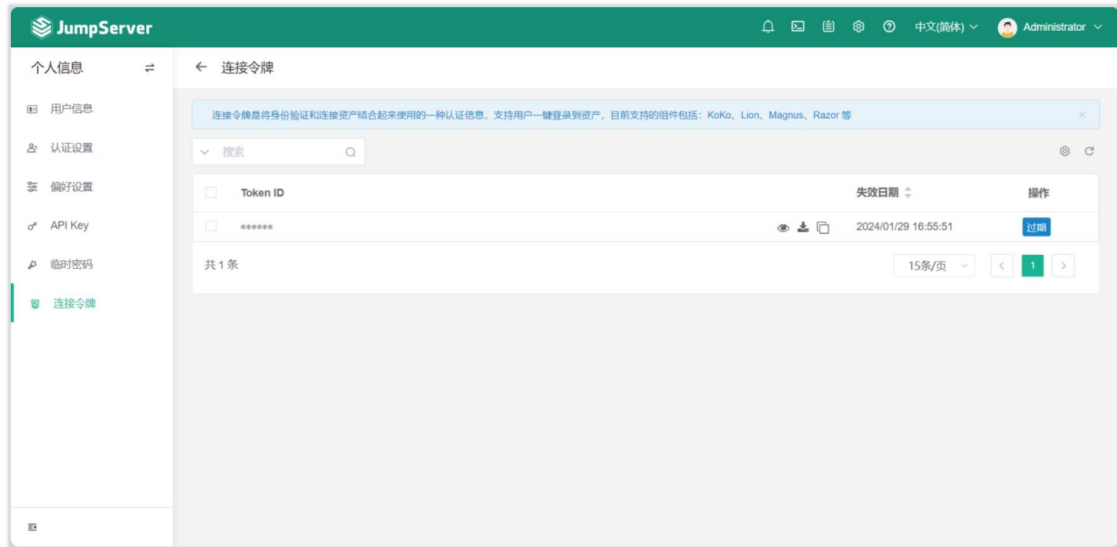


3.6. 连接令牌

连接令牌是将身份验证和连接资产结合起来使用的一种认证信息，支持用户一键登录到资产，目前支持的组件包括：Koko、Lion、Magnus、Razor 等。用户可以自行查看连接令牌信息并使令牌过期。

连接令牌的创建方式：

- 连接 SSH 协议资产：通过 Web 终端连接 Linux 资产，选择连接方式为“客户端”，即可创建令牌信息；
- 连接 RDP 协议资产：通过 Web 终端连接 RDP 资产，选择连接方式为“客户端-Remote Desktop”，即可创建令牌信息；
- 连接数据库应用：通过 Web 终端连接数据库应用，选择连接方式为“客户端”，即可创建令牌信息；
- 通过调用 API 方式创建。

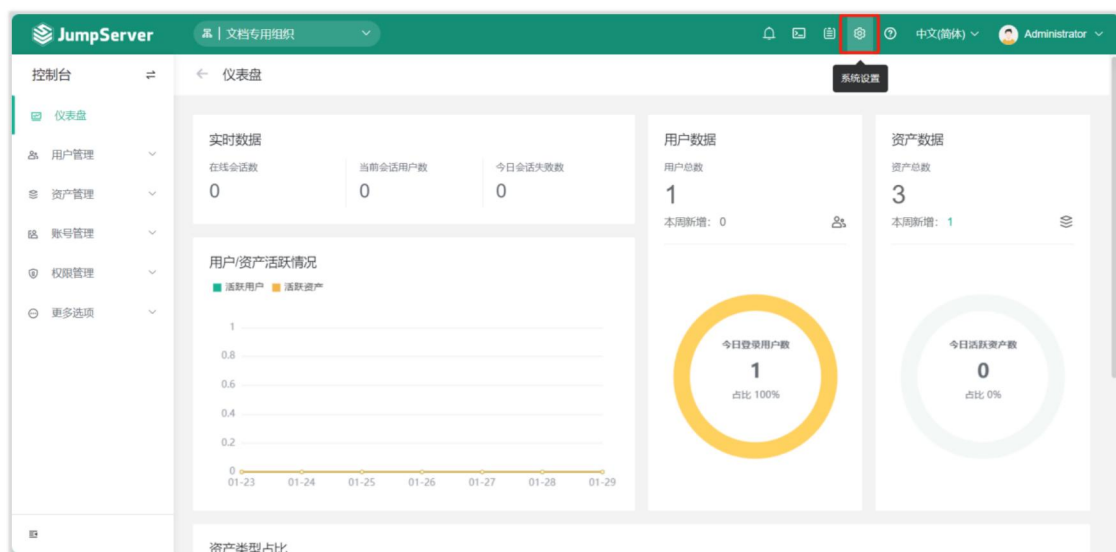


4. 系统设置

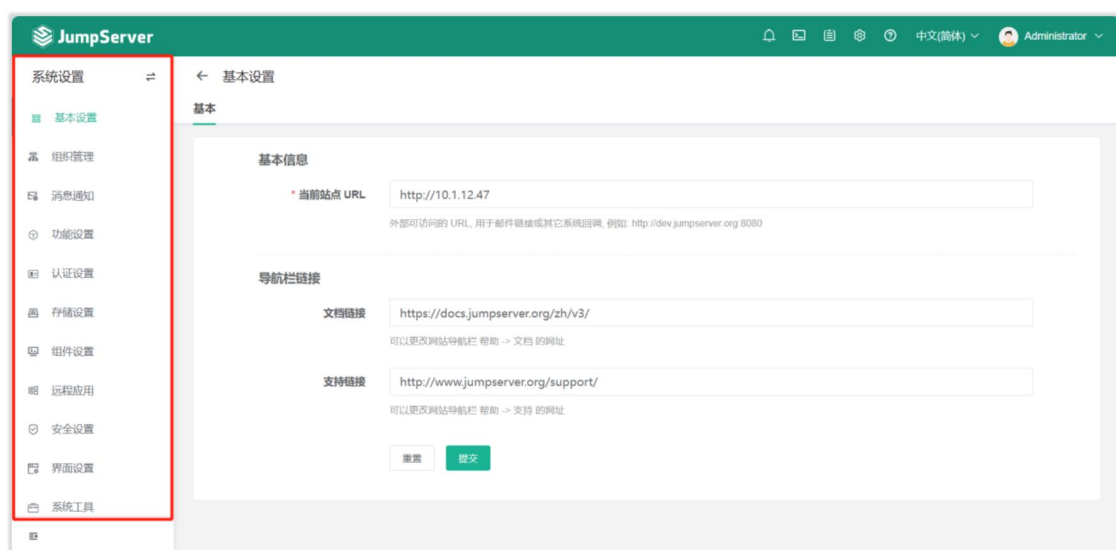
系统设置是 JumpServer 全局设置的操作入口，通过系统设置可以配置 JumpServer 用户认证、远程应用、安全设置等各类型的系统参数。

4.1. 概览

点击首页右上角<系统设置>按钮，进入系统设置页面。

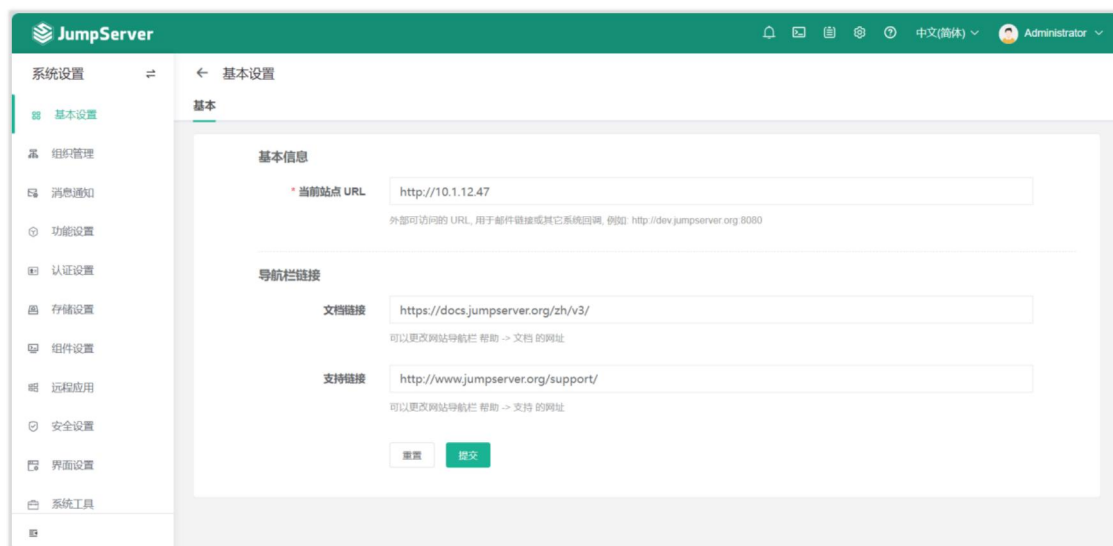


系统设置页面分为：基本设置、组织管理、消息通知、功能设置、认证设置、存储设置、组件设置、远程应用、安全设置、界面设置、系统工具、系统任务和许可证页面。



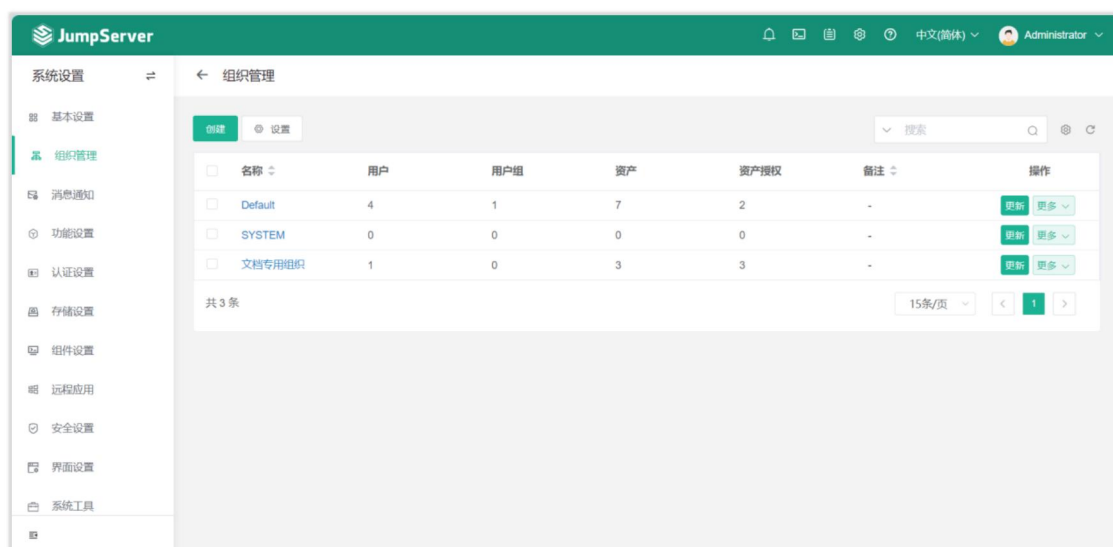
4.2. 基本设置

点击系统设置页面左侧菜单的<基本设置>按钮，进入基本设置页面，编辑基本信息。包含当前站点 URL（外部可访问的 URL，用于邮件链接或其他系统回调。此处可以填写域名或 IP）、导航栏链接。



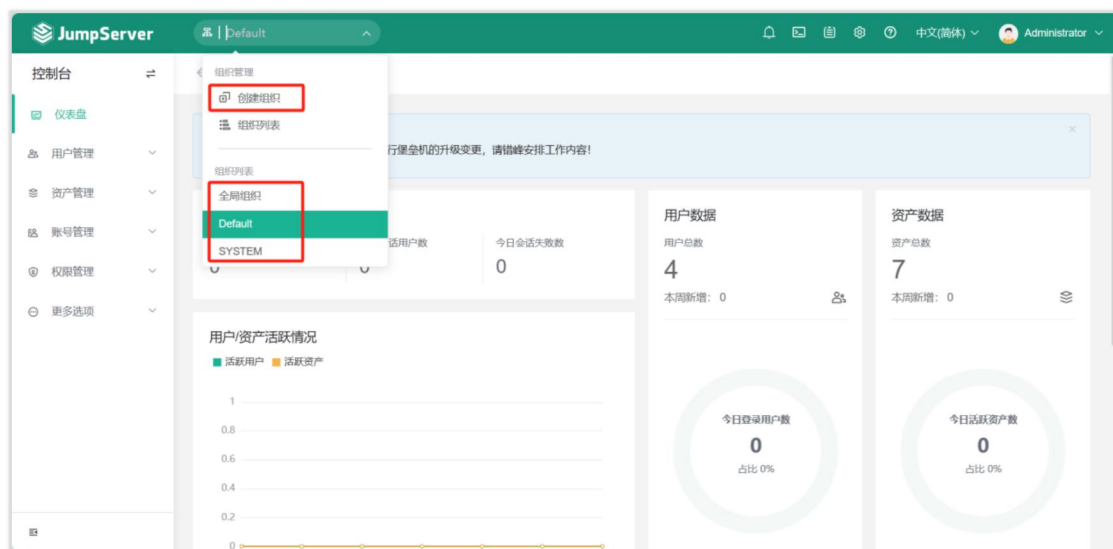
4.3. 组织管理

点击系统设置页面左侧的<组织管理>按钮，进入组织管理页面。JumpServer 支持分组织的管理方式，即不同的组织之间用户的权限、资产、权限等信息均隔离，方便管理员根据公司组织结构创建和查看不同组织环境下的信息。



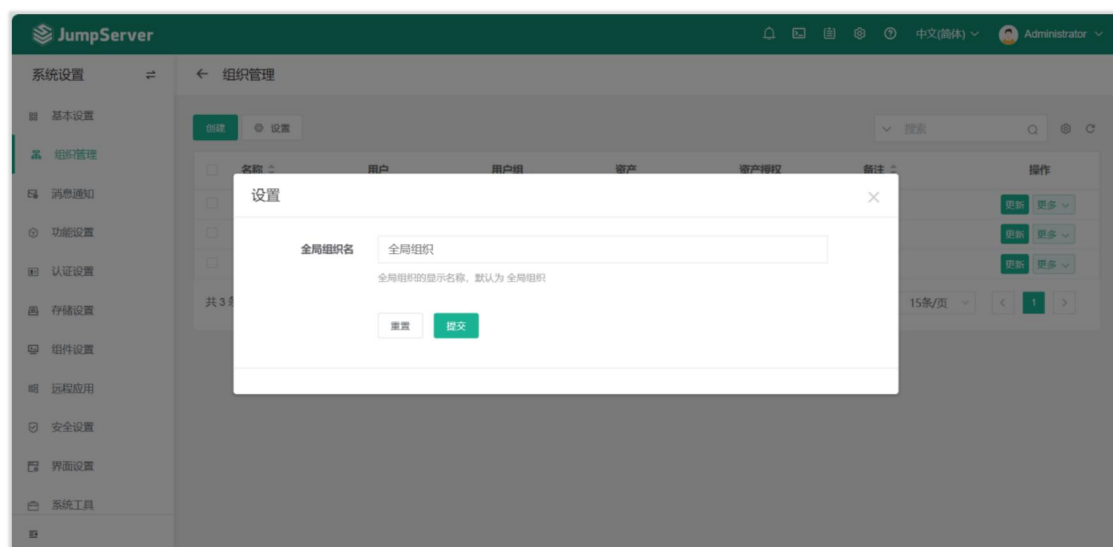
管理员登录 JumpServer 系统后，点击页面左上角的<创建组织>按钮，进入组织创建页面。

首先为创建的组织命名；创建组织成功后，组织列表显示新创建的组织信息，并且与左上方组织标识对应。组织的切换操作地点在主页的左上角。同时此按钮下也可以进行组织的创建。



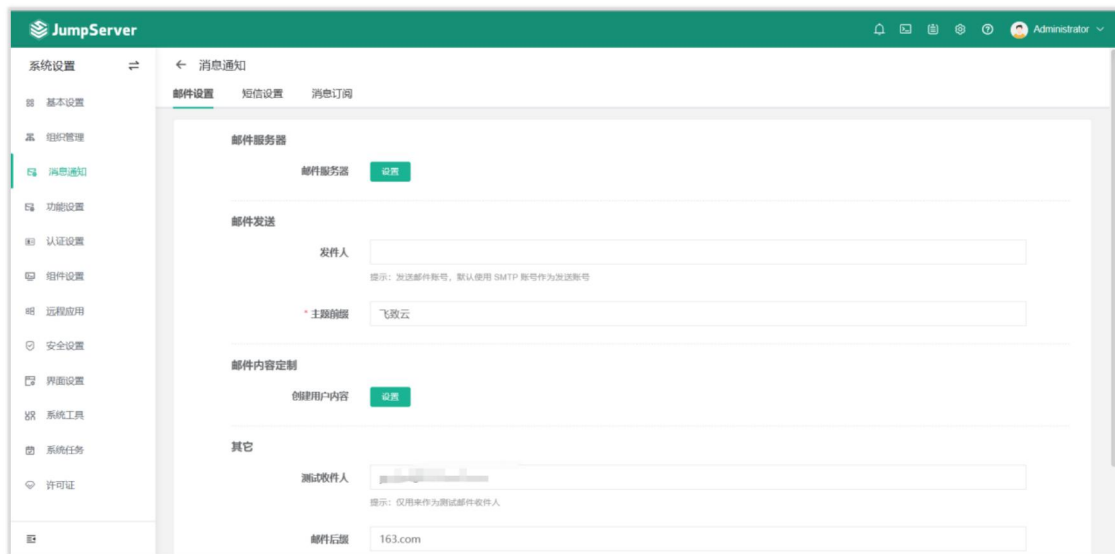
注：组织内的角色、资产、应用等都在各自的区域内，不可跨组织使用。

在系统设置→组织管理页面的左上角，点击设置可以设置全局组织名称。



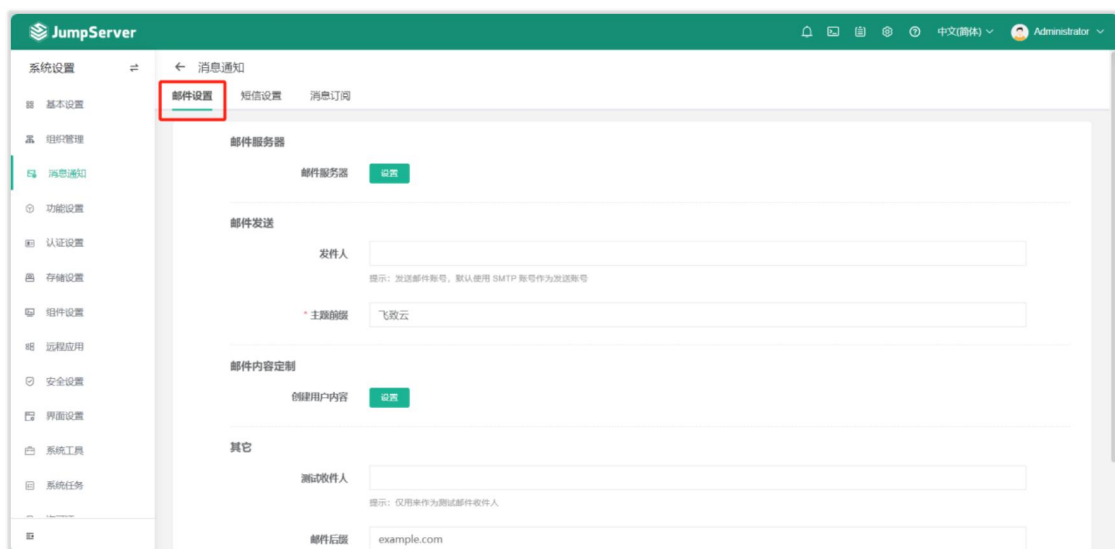
4.4. 消息通知

点击系统设置页面左侧的<消息通知>按钮，进入消息通知设置页面。

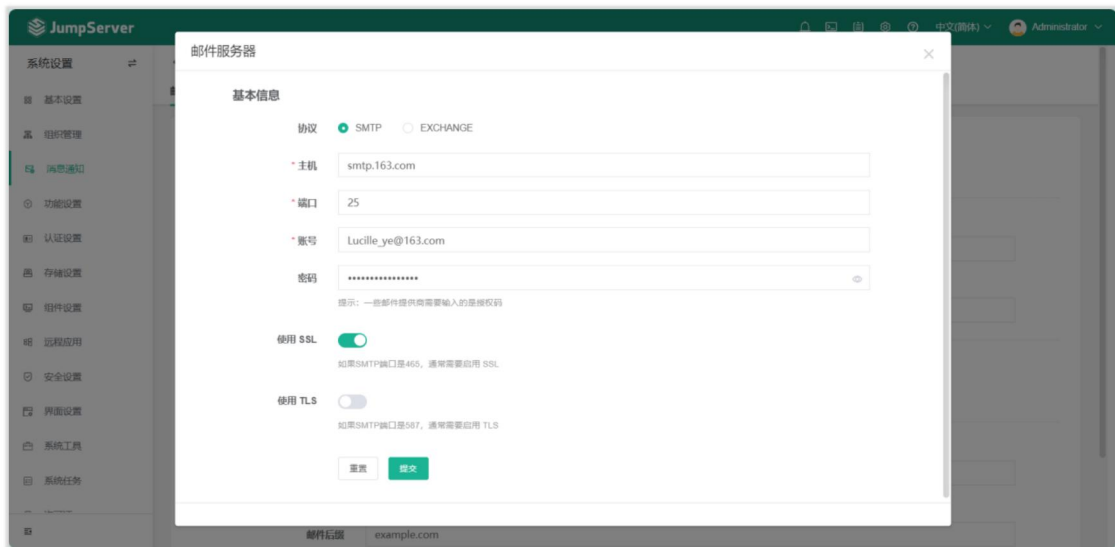


4.4.1. 邮件设置

点击消息通知页面对的左侧页签 [邮件设置](#) 按钮，即进入邮件设置页面。邮件设置界面主要配置邮件的发件邮箱信息，用于发送“创建用户密码设置邮件”、“危险命令提醒邮件”、“授权过期提醒邮件”等邮件到 JumpServer 用户的邮箱。邮件服务支持 SMTP 协议和 Exchange 协议。



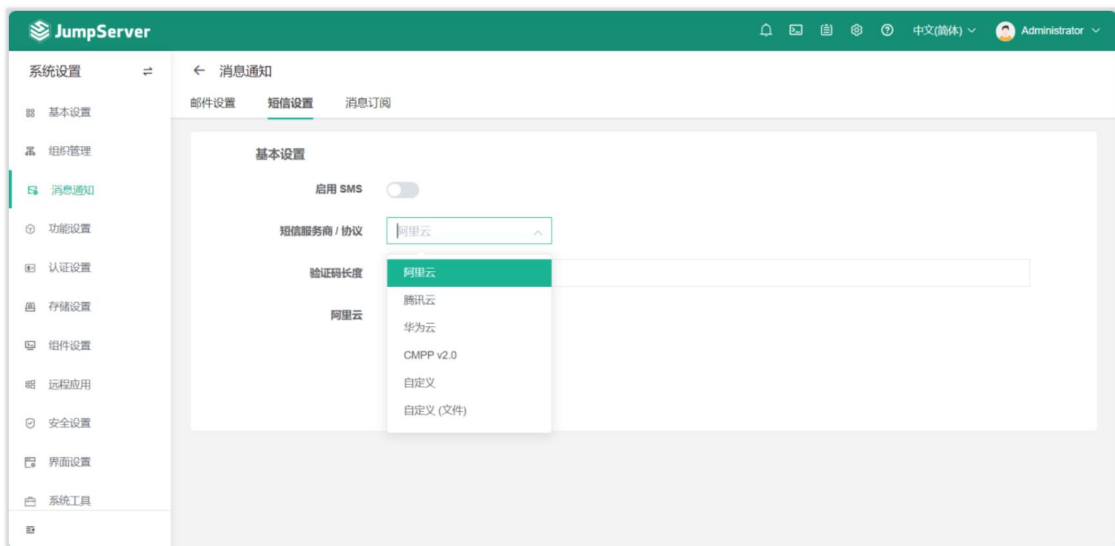
以 163 邮箱为例。SMTP 主机是 `smtp.163.com`。SMTP 端口在不使用 SSL 时是 25，使用 SSL 时是 465 或 994，使用 TLS 时是 587。SMTP 账号密码是登录邮箱的账号密码或账号授权码。



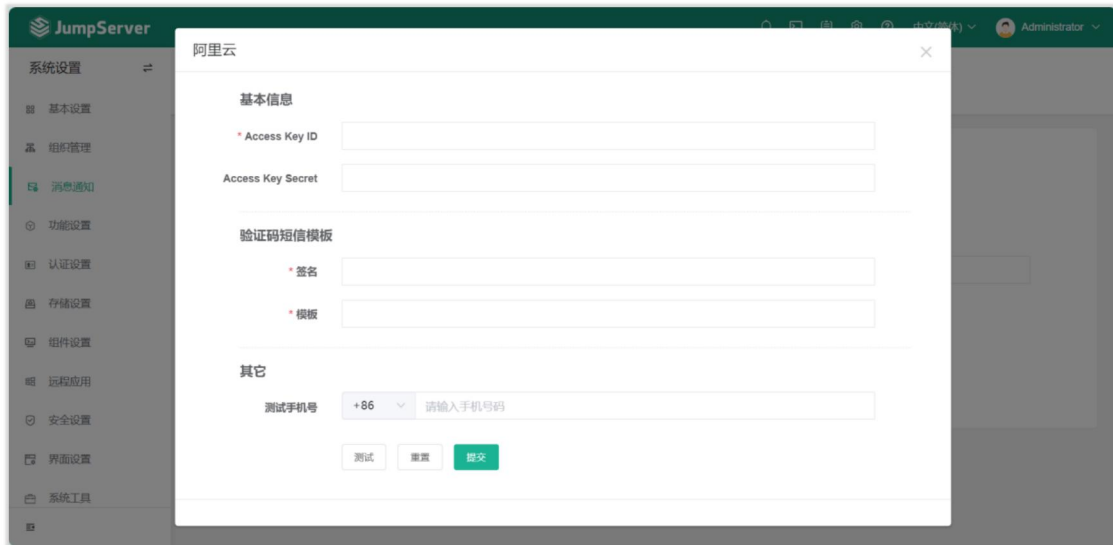
配置邮件服务器与邮件发送后，可添加测试收件人并点击[测试连接](#)按钮，如果配置正确，页面出现提示信息，同时 JumpServer 会发送一条测试邮件到测试收件人邮箱。

4.4.2. 短信设置

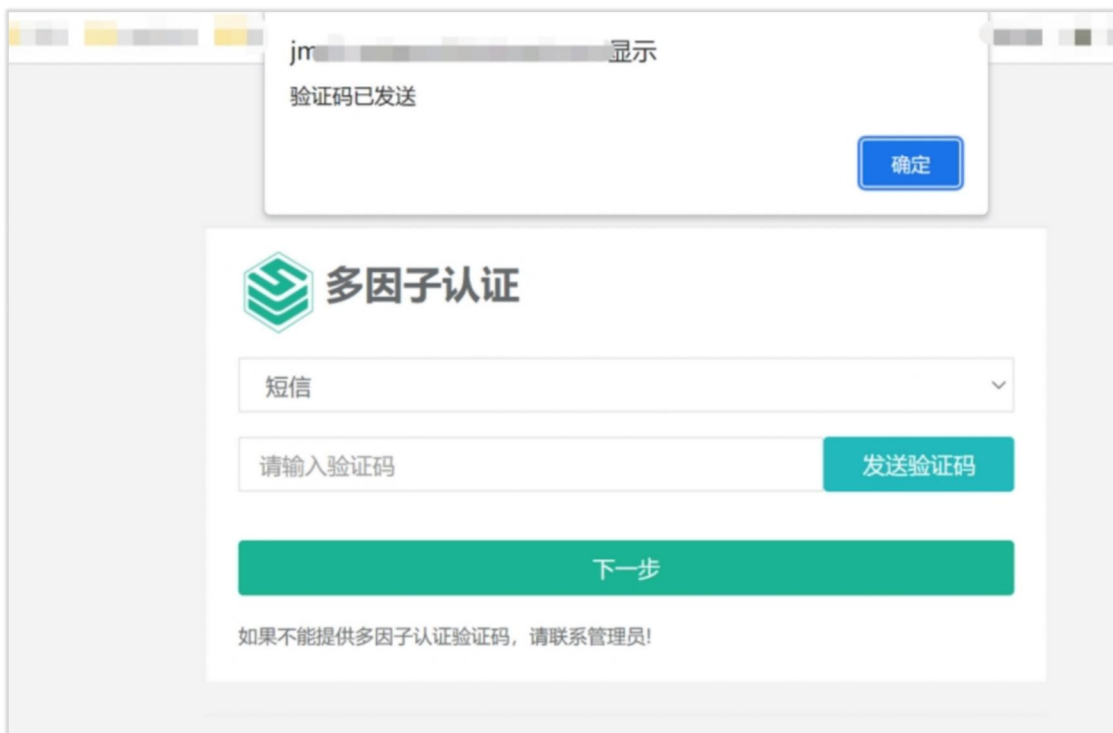
点击消息通知页面中间页签[短信设置](#)按钮，可以设置短信 MFA 认证方式（目前支持阿里云、腾讯云、华为云、CMPP v2.0、自定义、自定义【文件】）。除了 MFA 方式之外，JumpServer 还支持使用手机短信找回用户密码。管理员需要开启 SMS 服务，且用户信息需要配置手机号。



选择对应的短信服务商，以阿里云为例。填入阿里云短信服务的相关信息，点击[测试](#)按钮可测试配置是否正确。



启用双因素认证后，在下图位置中可选择 MFA 或者短信。



启用短信找回密码后，可在点击忘记密码后选择发送短信重新设置密码。

忘记密码?

输入您的手机号码，验证码将发送到您的手机

短信

180

验证码

等待: 60

提交

4.4.3. 消息订阅

点击消息通知页面中右侧页签[短信设置](#)按钮，进入消息订阅设置界面。

JumpServer

消息通知

消息订阅

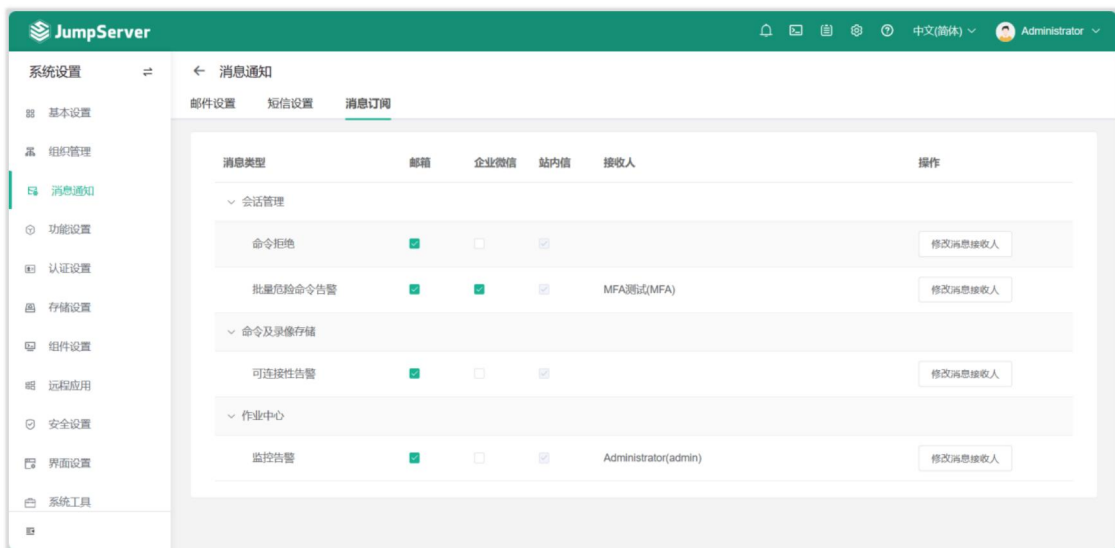
消息类型	邮箱	站内信	接收人	操作
会话管理				
命令拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		修改消息接收人
批量危险命令告警	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		修改消息接收人
命令及录像存储				
可选连接性告警	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		修改消息接收人
作业中心				
监控告警	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Administrator(admin)	修改消息接收人

该页面主要调节监控告警信息、危险命令告警信息、批量危险命令告警等信息的接收人。点击[修改消息接收人](#)按钮，进入消息接收人设置界面。



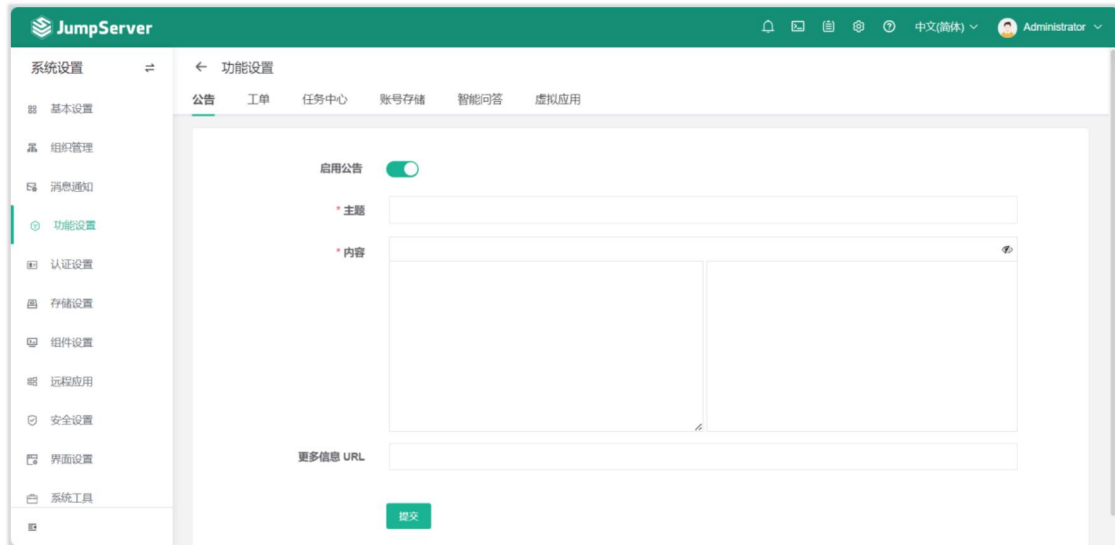
点击①框修改消息接收人，点击②框选择需要接受消息的人，点击③框加入消息接收人行列，点击④框确认。

消息订阅模式中默认只拥有“站内信”。JumpServer 与其他平台进行对接后（例如企业微信），出现企业微信的消息复选框，如下图所示：



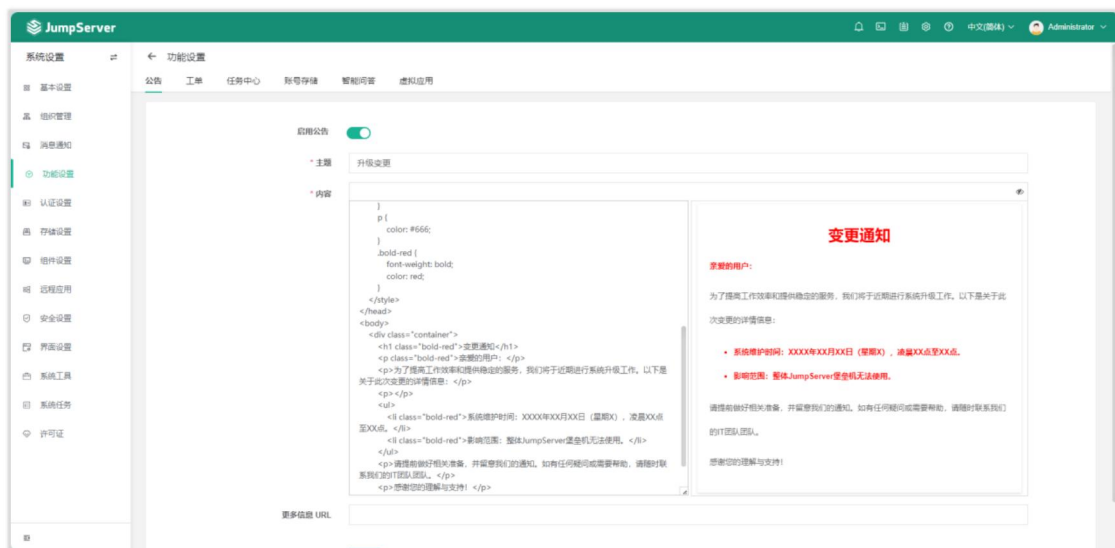
4.5. 功能设置

点击页面左侧的[功能设置](#)按钮，进入功能设置页面。



4.5.1. 公告

点击功能设置页面中[公告](#)按钮，即进入公告设置页面，配置后可以在页面首页显示公告内容。公告内容支持 Markdown 语法，更好的显示公告内容。公告内容支持显示在 SSH 方法连接堡垒机时显示，Markdown 语法的公告不支持正常展示在 SSH 页面。

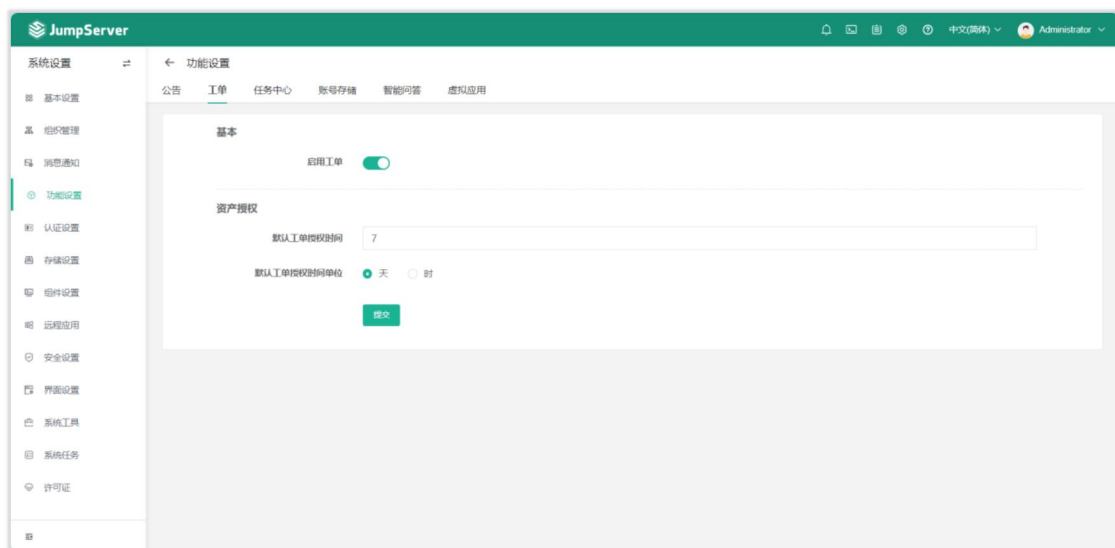


设置后效果如下：



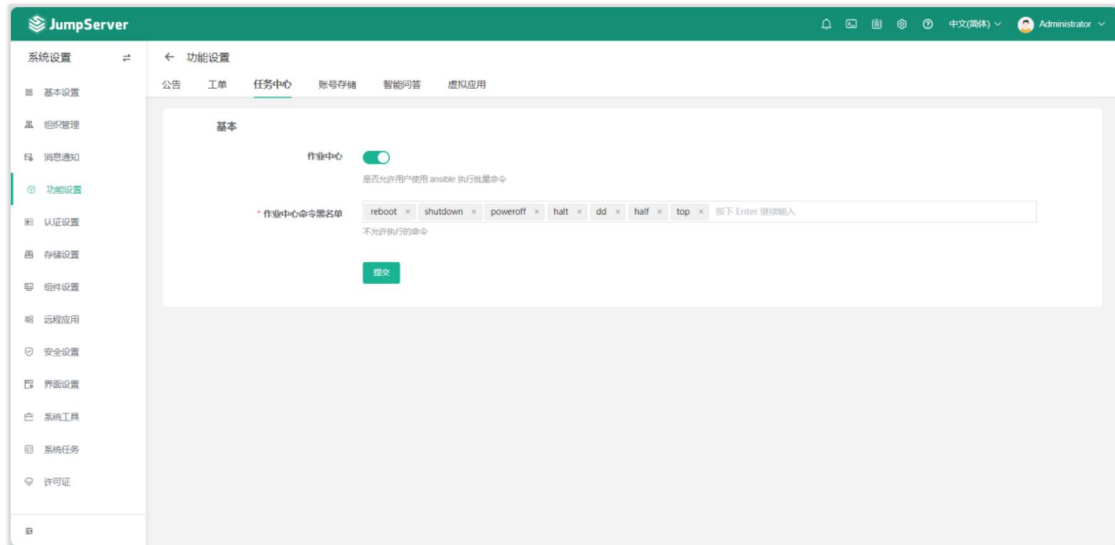
4.5.2. 工单

点击功能设置页面中[工单](#)按钮，即进入工单相关内容设置页面。工单设置页面包含是否开启工单配置项、在使用工单申请资产授权时，资产授权的默认授权时间与时间单位。



4.5.3. 任务中心

点击功能设置页面中[任务中心](#)按钮，进入工作台页面任务中心设置页面。该页面可以设置是否允许用户使用 ansible 执行批量命令以及设置作业中心命令黑名单。



4.5.4. 账号存储

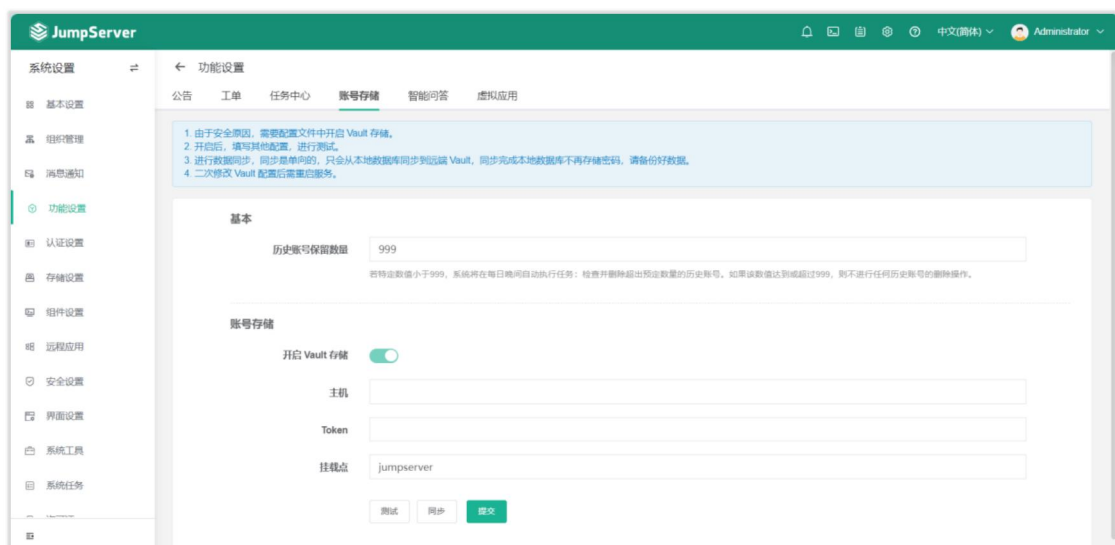
点击功能设置页面中 [<账号存储>](#) 按钮，即进入账号存储策略设置页面。

JumpServer 账号密码支持第三方密钥存储系统。该功能开启需要在配置文件中添加选项，修改之后重启 JumpServer 服务生效。

注：账号信息数据同步时，同步操作是单向的，只会从本地数据库同步到远端 Vault，同步完成后本地数据库不再存储账户信息，原存储账号信息会删除，请配置 Vault 同步之前，备份好数据。

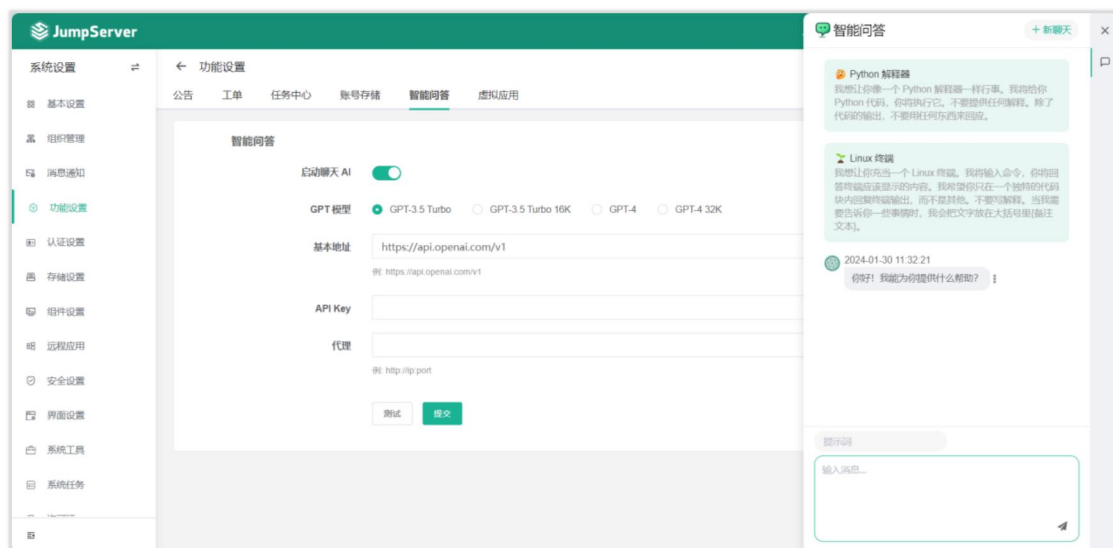
JumpServer 配置文件默认位于：/opt/jumpserver/config/config.txt

开启账号存储 Vault 功能的配置项为：VAULT_ENABLED=true



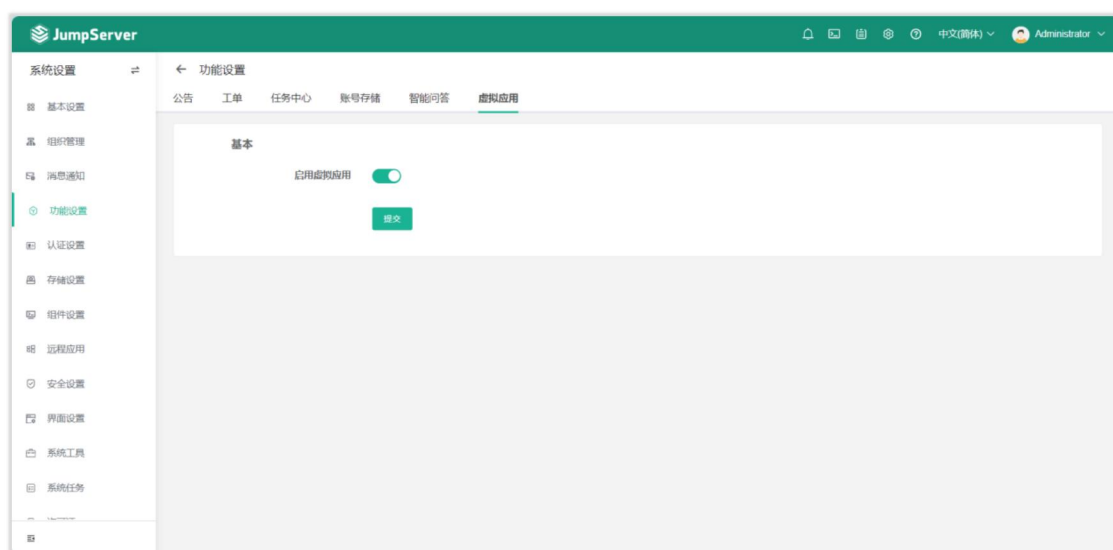
4.5.5. 智能问答

点击功能设置页面中<智能问答>按钮，即进入智能问答设置页面。管理员可以在此对接 ChatGPT 服务，启动 Chat AI 小助手功能。通过 Chat AI 小助手，用户可以直接在 JumpServer 主界面进行智能问答。



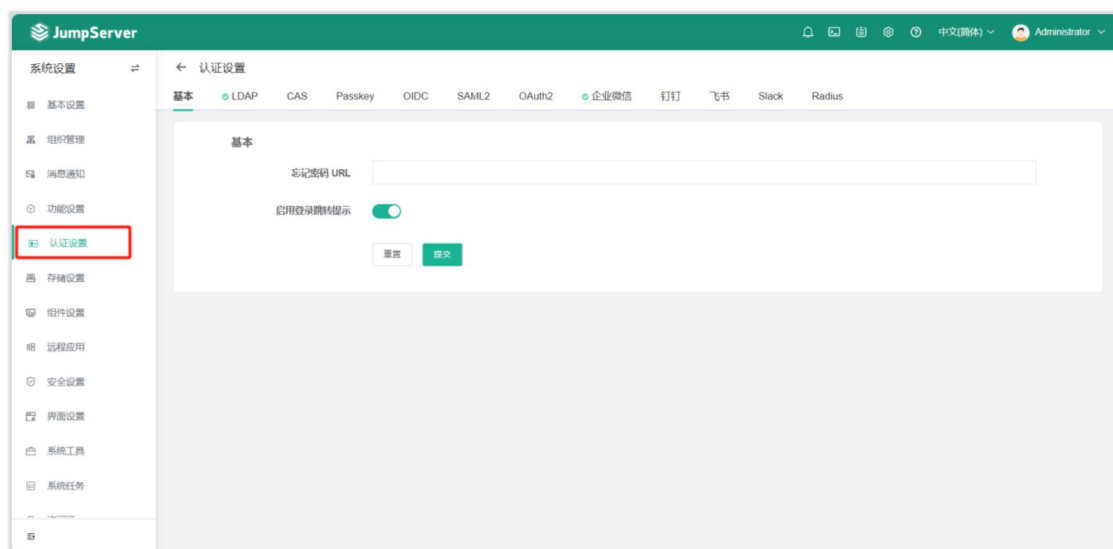
4.5.6. 虚拟应用

点击功能设置页面中<虚拟应用>按钮，即进入虚拟应用开启页面。JumpServer 支持使用 Linux 系统为远程应用功能的运行载体，在此页面开启以 Linux 系统为底层的虚拟应用功能。



4.6. 认证设置

点击页面左侧的<认证设置>按钮，进入认证设置页面。

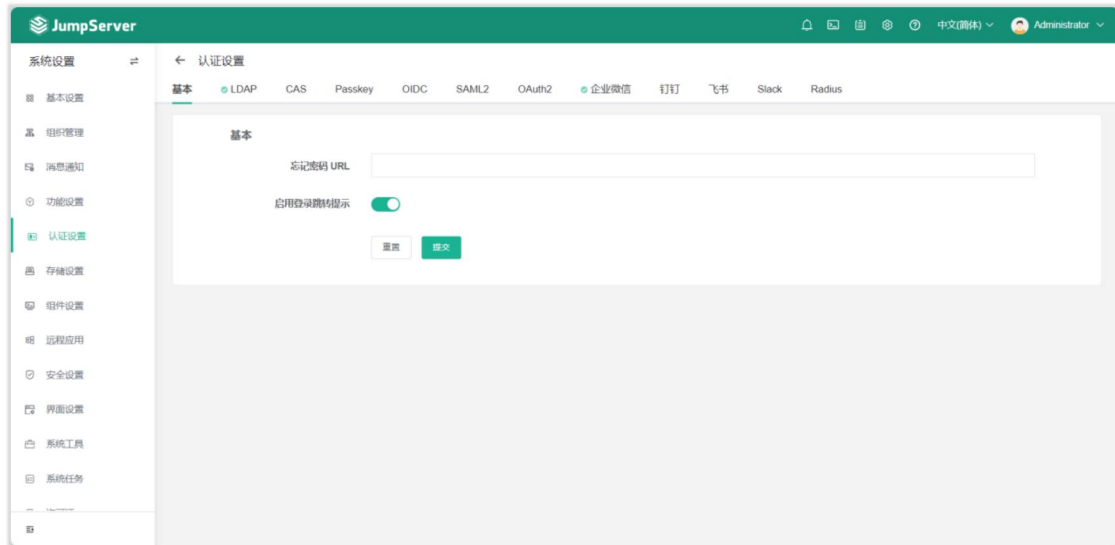


4.6.1. 基本

认证设置的基本设置是忘记密码的 URL 设置，该设置作用为：用户忘记密码时会发送重置邮件到用户邮箱，邮件内会包含此 URL 便于用户跳转到用户改密页面。

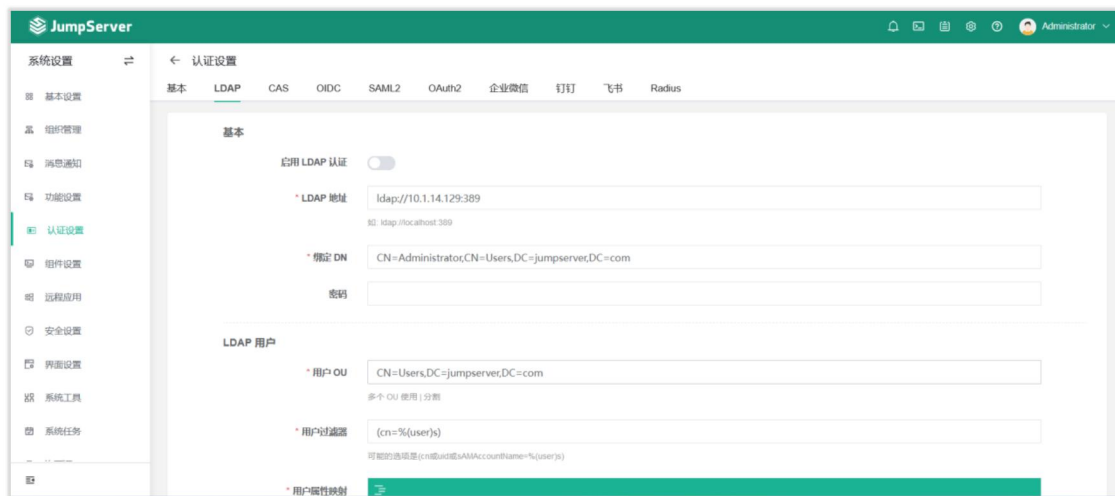
注：JumpServer 本地用户改密的 URL 默认为堡垒机的 URL。其他外部身份认证系统的密码不会托管在堡垒机；如外部认证用户需要改密，忘记密码 URL 需要填写外部身份认证系统的改密 URL。

启用登录跳转提示按钮是指：当 JumpServer 开启外部认证时，浏览器输入访问 JumpServer 的 URL 时，会跳转到认证服务的页面，此页面有倒计时按钮。关闭“登录跳转提示”即去除倒计时，直接跳转到认证服务页面。



4.6.2. LDAP

JumpServer 支持使用 LDAP 进行登录认证。点击[认证设置](#)按钮，进入“LDAP”页签，配置全局图如下所示：



详细参数说明：

配置项	说明
LDAP 地址	LDAP 地址，可以为 IP 或者域名。例如：ldap://serverurl:389。需确保 LDAP 服务器的端口 389 与 JumpServer 服务器连通。
绑定 DN	绑定的 LDAP 账号。例如：cn=admin,dc=jumpserver,dc=com
密码	绑定 LDAP 账号的密码。
用户 OU	用户查询的起始 OU。

用户过滤器	根据规则匹配指定的用户。过滤器语法参考： http://www.ldapexplorer.com/en/manual/109010000-ldap-filter-syntax.htm
用户属性映射	指 LDAP 中的属性和 JumpServer 用户的属性的对应关系，支持 memberOf 选项。其中 username,name,email 是 JumpServer 的用户必要属性。
连接超时时间	和 LDAP 服务器建立连接时的超时时间。
搜索分页数量（条）	从 LDAP 服务器中同步用户数据时每一次同步的数量。
启用 LDAP 认证	表示是否启用 LDAP 认证。

按钮说明：

按钮	说明
测试连接	该按钮可在配置信息后检测信息配置是否正常以及网络是否连通。
测试登录	该按钮可测试 LDAP 同步的用户是否可登录。
用户导入	该按钮即进入用户导入页面，选择用户导入到 JumpServer 用户列表中。
同步设置	该按钮可设置定时任务，定时同步 LDAP 用户到 JumpServer 平台中。 该按钮还可设置发送同步任务执行情况给收件人。
重置	该按钮会重置 LDAP 地址等信息。
提交	该按钮提交所有配置信息。

JumpServer 支持 LDAP 同步用户的同时同步用户组。目前支持 **memberOf**。在配置过程中，需注意：同步用户组需要在用户属性映射中添加如下图示例：

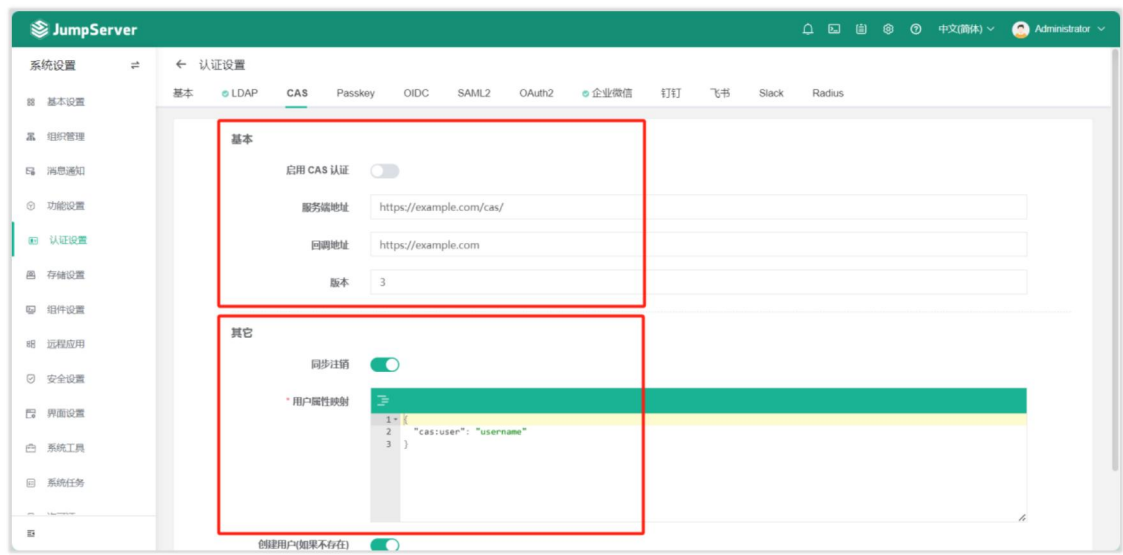


配置成功提交配置信息后，刷新 LDAP 用户信息，即可同步用户及对应的用户组。同步后的用户组以 **AD** 为开头，即 **AD+原用户组**。

4.6.3. CAS

点击页面中的“CAS”页签，进入CAS设置页面。在此页面可编辑是否启用CAS认证、服务端地址、回调地址、CAS版本、用户名与用户属性映射（可以选择是否开启），编辑完成后点击<提交>按钮，完成CAS设置。对接成功后，用户可使用CAS中的用户作为JumpServer登录用户并使用CAS用户的密码进行登录认证。

注：使用该认证方式的用户，有两种方式可以创建用户：一是用户主动登录到堡垒机平台，JumpServer自动创建用户；二是在堡垒机创建完用户后，用户来源修改为CAS，之后该用户登录时，会进入CAS的权限进行身份认证。



详细参数说明：

参数项	说明
是否启用CAS认证	表示是否启用CAS认证。
服务端地址	CAS认证地址，此项必填。例如： https://account.example.com/cas/
回调地址	CAS认证通过以后，回调JumpServer的地址。
版本	使用的CAS协议版本。可选 1、2、3、CAS_2_SAML_1_0。
同步注销	退出JumpServer时，是否注销CAS中的登录会话。
用户属性规则	CAS返回的用户信息和JumpServer中用户信息的对应关系。
创建用户（如果不存在）	当从CAS认证的资产不存在时，自动创建该用户到JumpServer用户列表中。

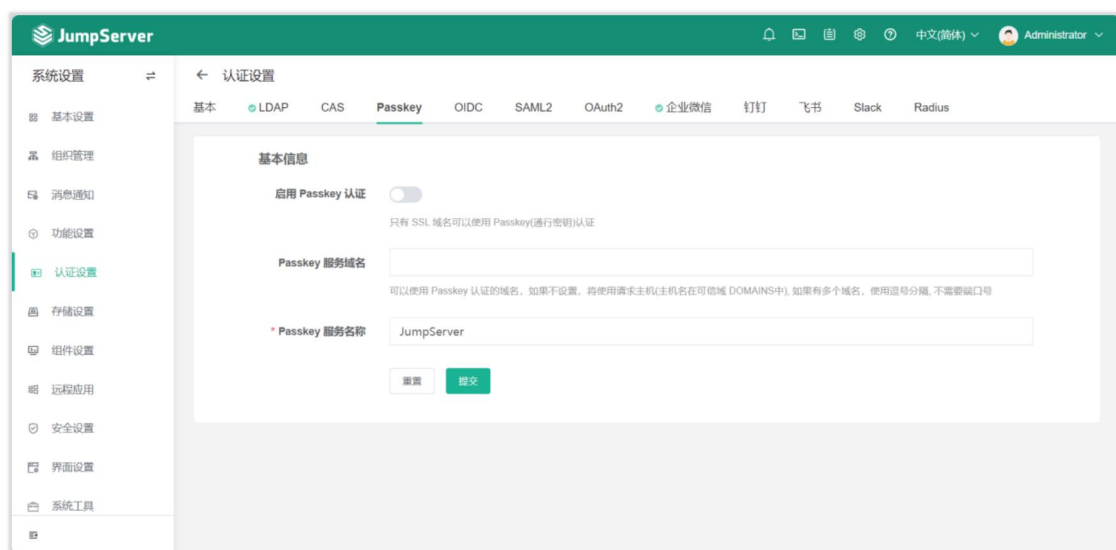
4.6.4. Passkey

选择“Passkey”页签，进入 Passkey 认证设置页面，编辑启用 Passkey 认证。

设置 Passkey 认证配置的前提条件如下：

- JumpServer 开启 HTTPS 登录，且配置安全的 SSL 证书；
- JumpServer 的配置文件中配置了可信任域名，即 DOMAINS；
- 个人 PC 或其他设备支持设备生物认证；

选择启用 Passkey 认证，填写对应的信息。完成 Passkey 认证设置。



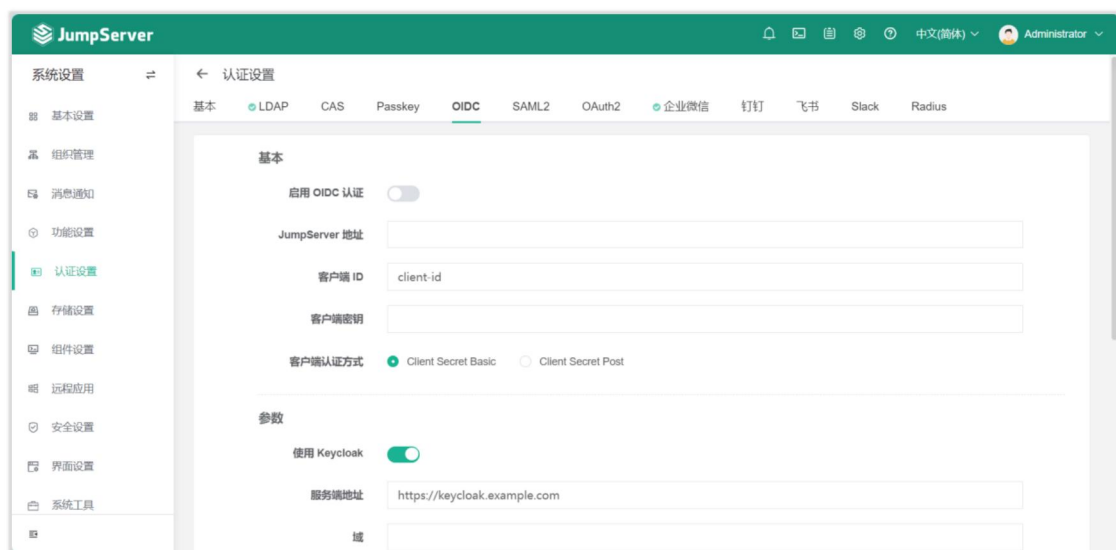
启用 Passkey 认证后，在个人信息页面录入 Passkey 凭证。即可在登录时选择 Passkey 进行认证登录。

4.6.5. OIDC

选择“OIDC”页签，进入 OIDC 设置页面，编辑是否启用 OIDC 认证、JumpServer 地址、客户端 ID 与密钥、是否使用 Keycloak 等选项，点击[提交](#)按钮，完成 OIDC 设置。

JumpServer 可自定义用户属性映射字段，实现 OpenID 中用户属性映射到 JumpServer 上的操作。

注：在属性映射中，如用户填写的属性不存在，则会使用 OpenID 中的用户的 ID 作为属性进行映射。



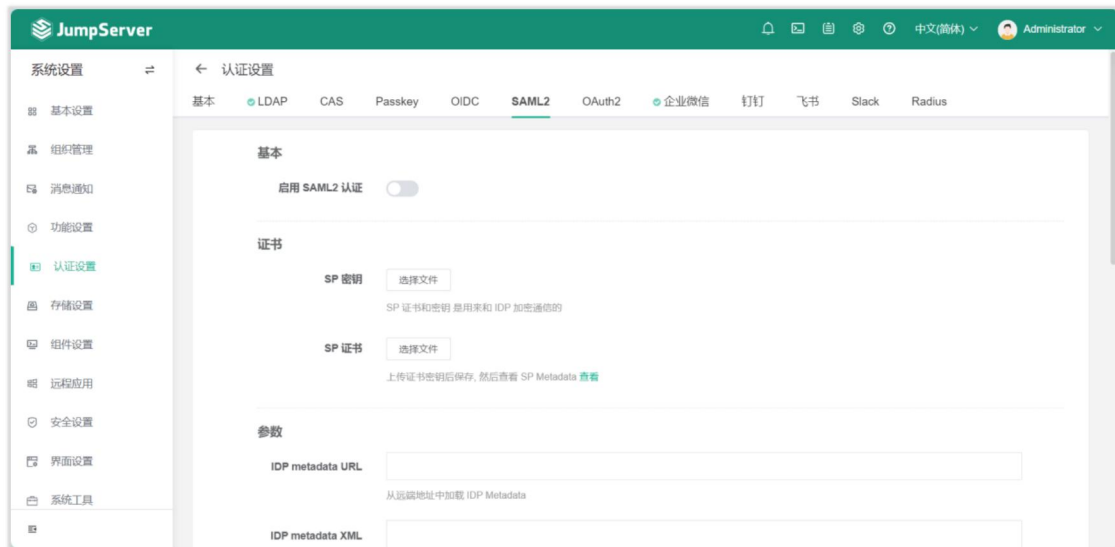
详细参数说明：

参数			说明
启用 OIDC 认证			表示是否启用 OIDC 认证。
JumpServer 访问地址			指 JumpServer 的访问地址，注意末尾加 "/" 。 例如：https://demo.jumpserver.org/
客户端 ID			Client ID。
客户端密钥			该客户端所使用的密钥。
客户端认证方式			Client Secret Basic 或者 Client Secret Post， 表示认证密钥是通过 request body 传递还是通过 request header 进行传递。
使用 Keycloak	启用	服务端地址	Keycloak 服务器地址，注意末尾加"/"。例 如： https://id.jumpserver.org/auth/
		域	Keycloak 中配置的 Realm 名称。
	不启用	端点地址	OIDC 端点地址。
		授权端点地址	OIDC 授权端点地址。
		token 端点地址	OIDC 获取 Token 的端点地址。
		jwks 端点地址	OIDC JWKS 的端点地址。
		注销会话端点地址	OIDC 注销会话的端点地址。
		签名算法	OIDC 所使用的签名算法。一般为 HS256。
	用户信息端点地址	OIDC 获取用户信息的端点地址。	

		签名 Key	OIDC 使用的签名 Key，当签名算法为 RS256 时，签名 Key 必填。
		启用 PKCE	是否启用 PKCE。默认不启用。
		验证校验码方式	启用 PKCE 后对 code_verifier 的转换算法。
		连接范围	获取的用户信息范围。一般为：email openid profile。
		令牌有效时间	id_token 的有效期。
		声明	定义 id_token 内容是否可用于检索用户信息声明和范围，以便创建和更新正在验证的用户。
		使用状态	用于维护身份验证请求和回调之间的状态数据。
		临时使用	在进行授权请求时是否应使用随机数。Nonce 用于减轻重放攻击。
		总是更新用户信息	是否始终更新用户信息（当用户每次登录并成功验证时）。
忽略 SSL 证书验证		是否忽略 SSL 证书验证， 一般选是。	
共享会话		是否共享会话，实现单点退出。	
用户属性映射		认证服务器返回的用户信息和 JumpServer 中用户属性的对应关系。	

4.6.6. SAML2

选择“SAML2”页签，进入 SAML2 设置页面，编辑是否启用 SAML2 认证、相关证书、SAML2 参数、以及其他的相关信息，点击[提交](#)按钮，完成 SAML2 设置。

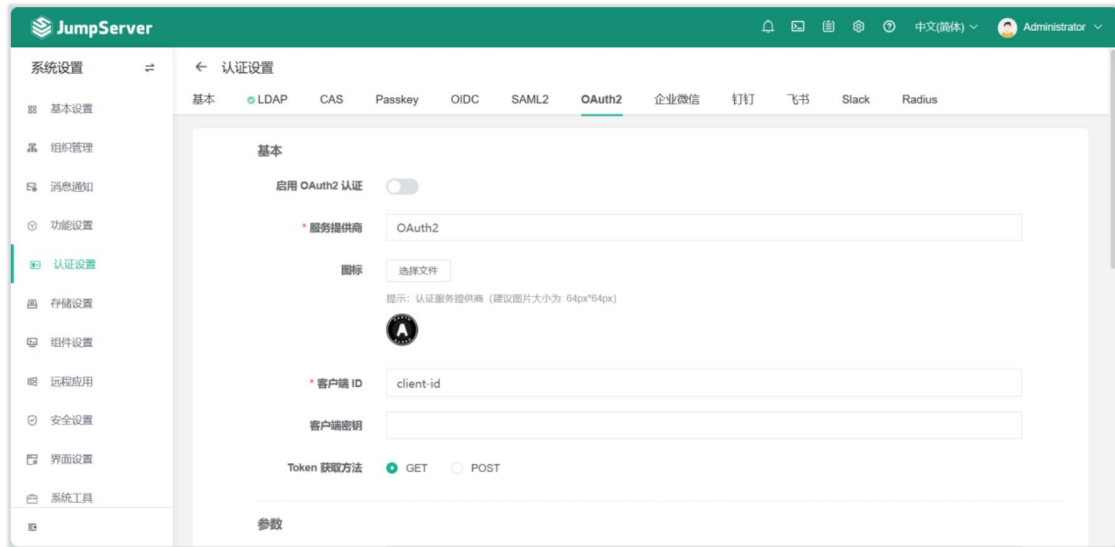


详细参数说明：

参数	说明
启用 SAML2 认证	表示是否启用 SAML2 认证。
SP 密钥	指 SP 的密钥信息，主要用来与 IDP 进行加密通信。
SP 证书	指 SP 的证书密钥信息。
IDP metadata URL	IDP 获取 metadata 的 URL。
IDP metadata XML	IDP metadata XML 的内容。
高级配置	设置一些高级配置如“OrganizationName”等参数。
同步注销	退出 JumpServer 时，是否注销 SAML2 中的登录会话。
总是更新用户信息	是否始终更新用户信息（当用户每次登录并成功验证时）。
用户属性映射	认证服务器返回的用户信息和 JumpServer 中用户属性的对应关系。

4.6.7. OAuth2

选择“ OAuth2 ”页签，进入 OAuth2 设置页面，编辑是否启用 OAuth2 认证、服务提供商、客户端 ID、客户端密钥、端点信息等相关参数，点击<提交>按钮，完成 OAuth2 设置。



详细参数说明：

参数	说明
启用 OAuth2 认证	表示是否启用 OAuth2 认证。
服务提供商	OAuth2 产品厂商。
图标	OAuth2 产品厂商的图标。
客户端 ID	Client ID。
客户端密钥	客户端密钥。
Token 获取方法	获取 Token 的方式，GET 或者是 Post 的请求方式。
范围	获取的用户信息范围，默认填写 email openid profile。
授权端点地址	授权端点地址 URL。
Token 端点地址	Token 端点地址 URL。
用户信息端点地址	用户信息端点地址 URL。
注销会话端点地址	注销会话端点地址 URL。
同步注销	退出 JumpServer 时是否同步注销在 OAuth2 中的会话。
总是更新用户信息	登录成功后是否更新用户信息。
用户属性映射	认证服务器返回的用户信息和 JumpServer 中用户属性的对应关系。

4.6.8. 企业微信

JumpServer 支持使用企业微信扫码登录，使用企业微信的用户与 JumpServer 的登录用户进行绑定实现快速登录 JumpServer 堡垒机。

注：JumpServer 配置企业微信对接前，需修改系统设置基本设置页面的当前站点 URL 为 JumpServer 访问地址。

注：需要保证堡垒机与企业微信之间的网络为双向互通，即堡垒机可以访问到企业微信，企业微信可以访问到堡垒机。

当使用企业微信扫码登录时，对于不存在的用户，JumpServer 会自动创建一个普通用户，并将该用户与企业微信认证绑定。

4.6.8.1. 企业微信端配置

打开【企业微信管理后台 <https://work.weixin.qq.com/>】，使用管理员权限用户登录；选择<应用管理>页面下的<创建应用>按钮，进入企业微信应用创建页面。选择<创建应用>按钮，创建 JumpServer 对接应用并选择应用可见范围。



进入企业微信应用详情页，查看企业微信应用凭据以及企业 ID。



设置应用主页与授权回调域（均为 JumpServer 访问域名）。



设置网页授权及 JS-SDK，配置网页授权。



在配置可信域名前需要进行域名归属认证。



将下载的文件复制到 jms_web 容器中，并配置 nginx，详细命令如下：

#临时方案

```
$ docker cp ./WW_verify_IF95X8Tagox6aZY4.txt jms_web:/opt/jumpserver/data
```

```
$ docker exec -it jms_web bash
```

```
$ vi /etc/nginx/conf.d/default.conf
```

```
location = /WW_verify_pGAIdNBz3AetOpbQ.txt {
    alias /opt/jumpserver/data/WW_verify_pGAIdNBz3AetOpbQ.txt;
}
```

```
$ nginx -t
```

```
$ nginx -s reload
```

#持久化

```
$ docker cp jms_web:/etc/nginx/conf.d /data/jumpserver/nginx/
```

```
$ vi /opt/jumpserver-offline-installer-v*-amd64/compose/dokcer-compose-lb.yml
```

```
- /data/jumpserver/nginx/conf.d/default.conf:/etc/nginx/conf.d/default.conf
```

```
$ docker restart jms_web
```

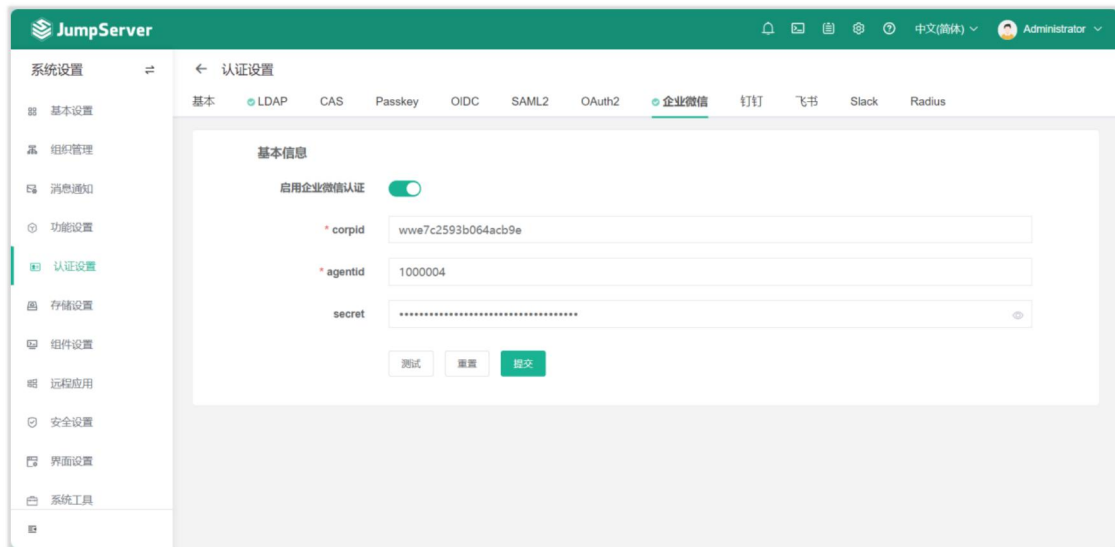
访问域名+文件名是否可访问，可访问即验证成功；

设置授权回调域。



4.6.8.2. JumpServer 端配置

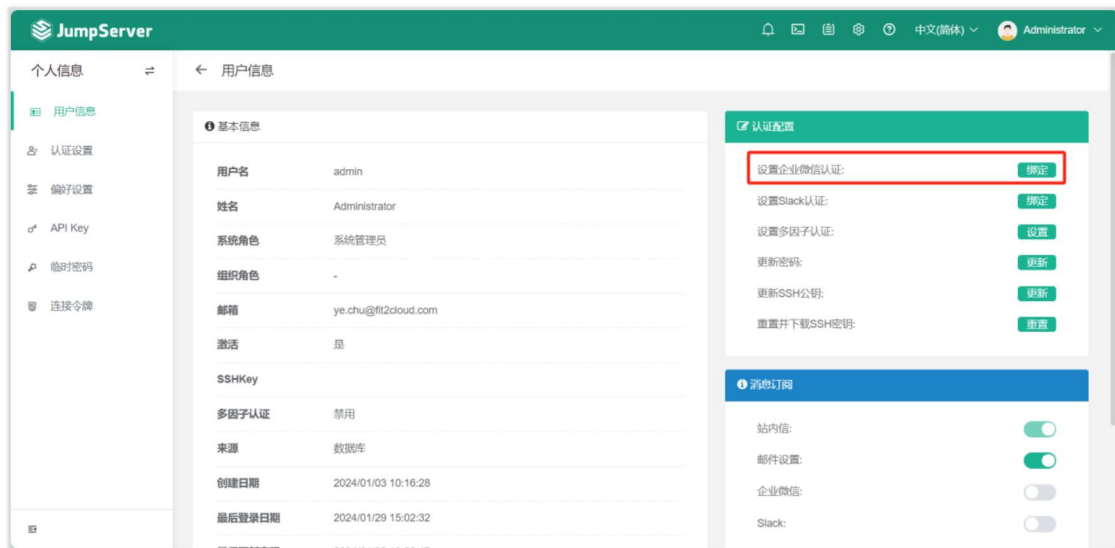
点击 JumpServer 系统设置的认证设置页面，选择“企业微信”页签，填写获取到的企业微信应用认证信息。



点击<测试>按钮测试是否成功并提交相关信息。

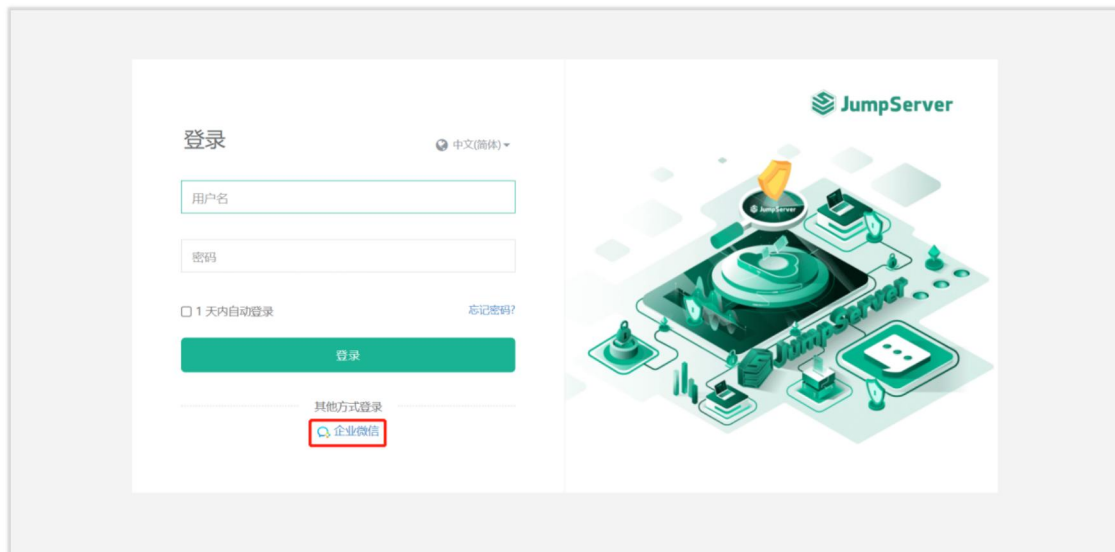
4.6.8.3. 企业微信账号登录

点击用户名称进入个人信息页面，在认证配置模块设置企业微信认证即绑定企业微信账号。



绑定企业微信账号需验证账号的密码，输入密码后跳转至企业微信操作登录页面。扫码后跳转即绑定配置成功。

在登录页面选择企业微信登录模式，使用企业微信扫码登录 JumpServer。



4.6.9. 钉钉

JumpServer 支持使用钉钉进行扫码登录，使用钉钉的用户与 JumpServer 的登录用户进行绑定实现快速登录 JumpServer 堡垒机。

注：JumpServer 配置钉钉对接前，需修改系统设置基本设置页面的当前站点 URL 为 JumpServer 访问地址。

当使用钉钉扫码登录时，对于不存在的用户，JumpServer 会自动创建一个普通用户，并将该用户与钉钉认证绑定。

4.6.9.1. 钉钉端配置

打开【钉钉开发平台 <https://developers.dingtalk.com/>】，使用管理员权限用户登录；选择<应用开发>按钮下的<企业内部开发>按钮，进入钉钉应用创建页面。选择<创建应用>按钮，创建 JumpServer 对接应用，应用类型选择“H5 微应用”或“小程序”均可。



查看钉钉应用的凭证信息。



点击<应用功能>下拉框中的<登录与分享>按钮，填写 JumpServer 回调域名（JumpServer 访问地址）。



点击<基础信息>下拉框中的<开发管理>按钮，填写“JumpServer 服务器出口 IP”和“应

用首页地址”（JumpServer 服务器出口 IP 即 JumpServer 对外的公网地址，设置此 IP 后，只能通过此 IP 与钉钉进行通信）。

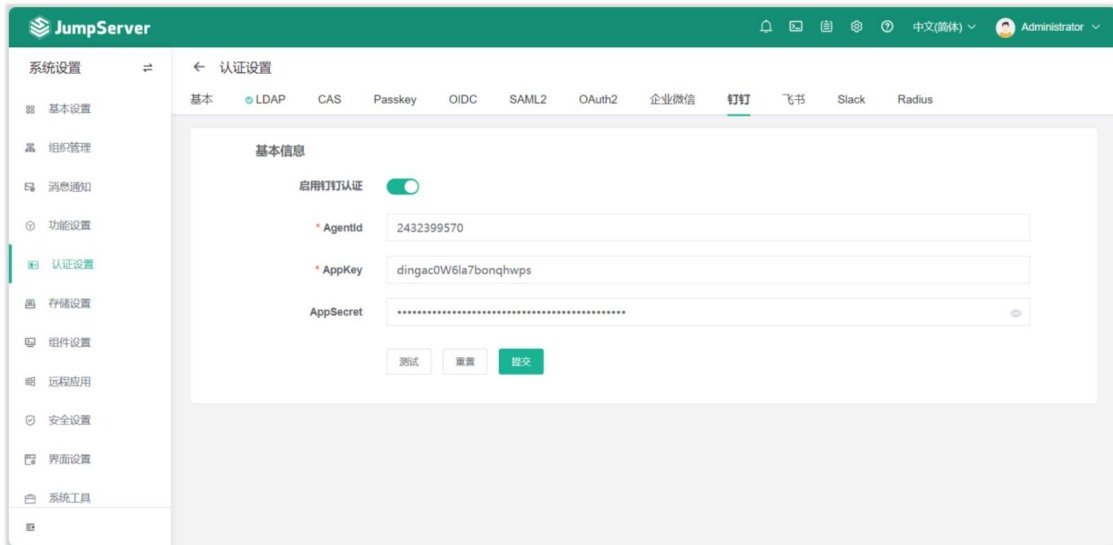


点击<基础信息>下拉框中的<权限管理>按钮，批量申请“成员信息读权限”。



4.6.9.2. JumpServer 端配置

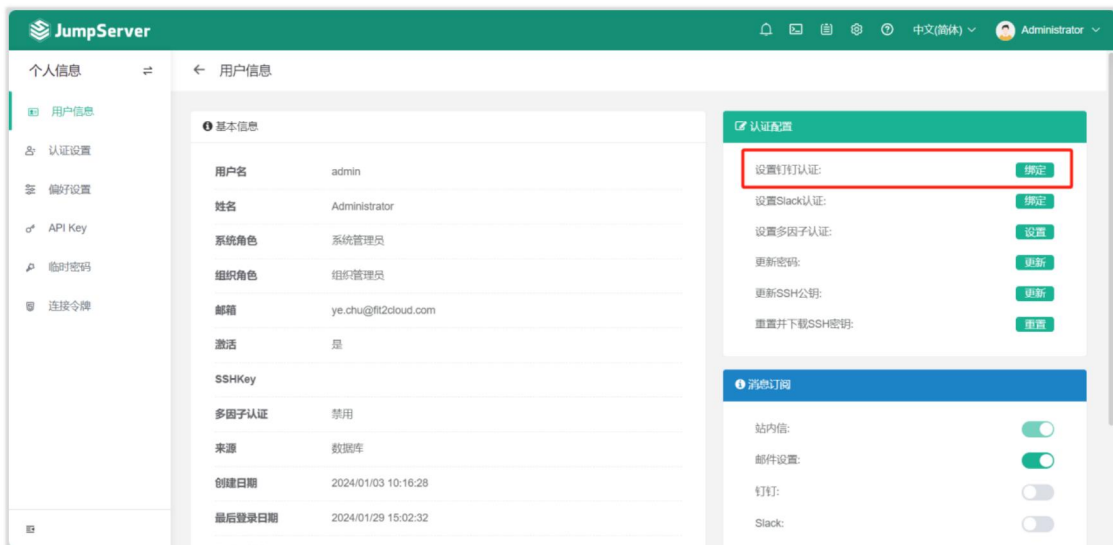
点击 JumpServer 系统设置的认证设置页面，选择“钉钉”页签，填写获取到的钉钉应用认证信息。



点击<测试>按钮测试是否成功并提交相关信息。

4.6.9.3. 钉钉账号登录

点击用户名称进入个人信息页面，在认证配置模块设置钉钉认证即绑定钉钉账号。

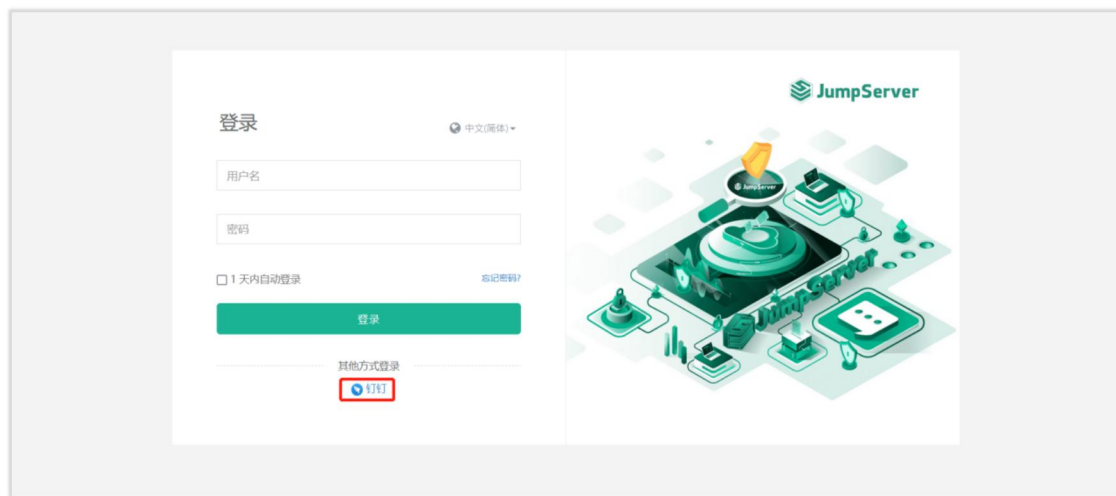


绑定钉钉账号需验证账号的密码，输入密码后跳转至钉钉操作登录页面。



扫码后跳转即绑定配置成功。

在登录页面选择钉钉登录模式，使用钉钉扫码登录 JumpServer。



4.6.10. 飞书

JumpServer 支持使用飞书扫码登录，使用飞书的用户与 JumpServer 的登录用户进行绑定实现快速登录 JumpServer 堡垒机。

注：JumpServer 配置飞书对接前，需修改系统设置基本设置页面的当前站点 URL 为 JumpServer 访问地址。

当使用飞书扫码登录时，对于不存在的用户，JumpServer 会自动创建一个普通用户，并将该用户与飞书认证绑定。

4.6.10.1. 飞书端配置

打开【飞书开放平台 <https://open.feishu.cn/app/>】，用管理员权限用户登录进入开发者后台。

点击[<创建企业自建应用>](#)按钮，创建一个新应用。



在应用详情页点击[添加应用能力](#)按钮进入添加应用能力页面，添加机器人能力。



点击左侧[安全设置](#)按钮，设置重定向 URL 以及 IP 白名单。

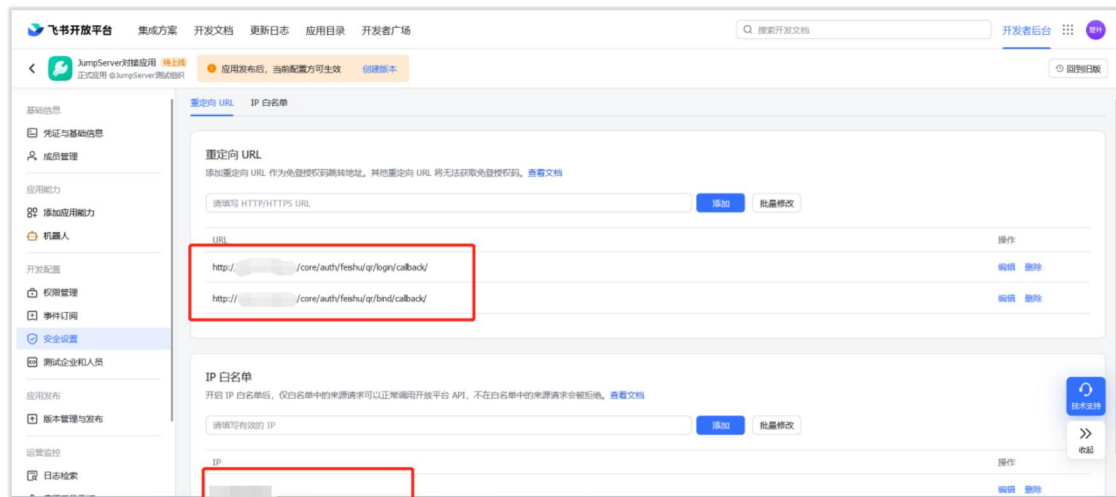
重定 URL: 【<jumpserver_host>替换为 JumpServer 域名或 IP】

http{s}://<jumpserver_host>/core/auth/feishu/qr/bind/callback/

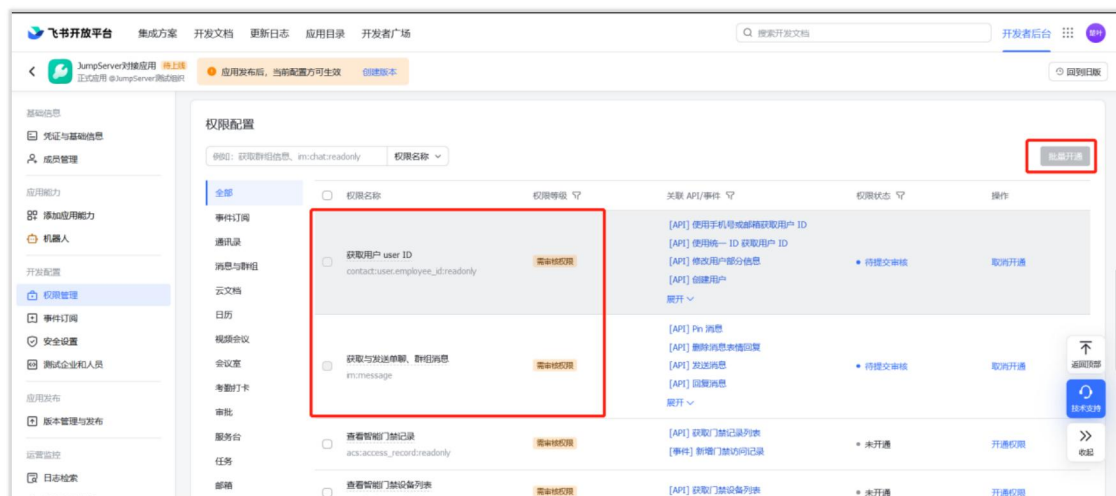
http{s}://<jumpserver_host>/core/auth/feishu/qr/login/callback/

IP 白名单:

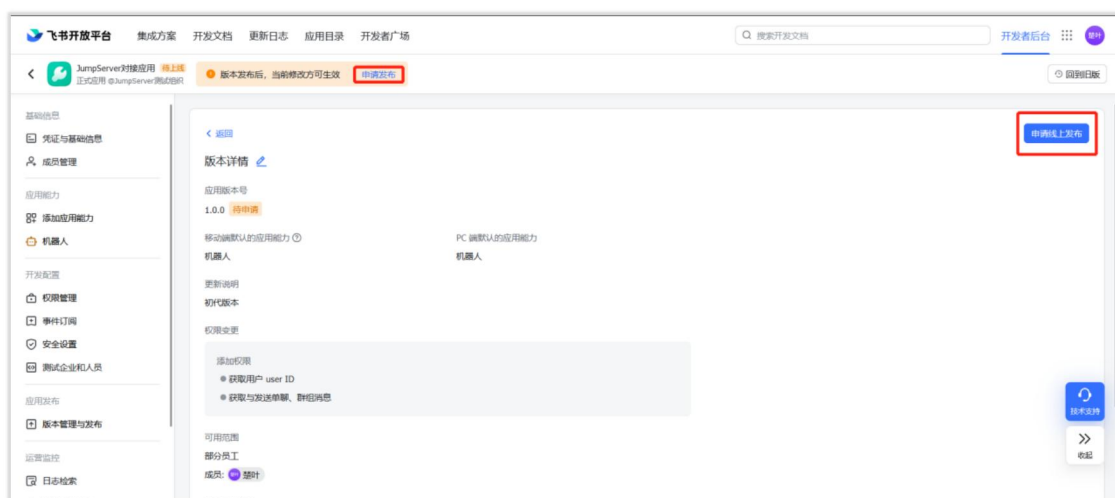
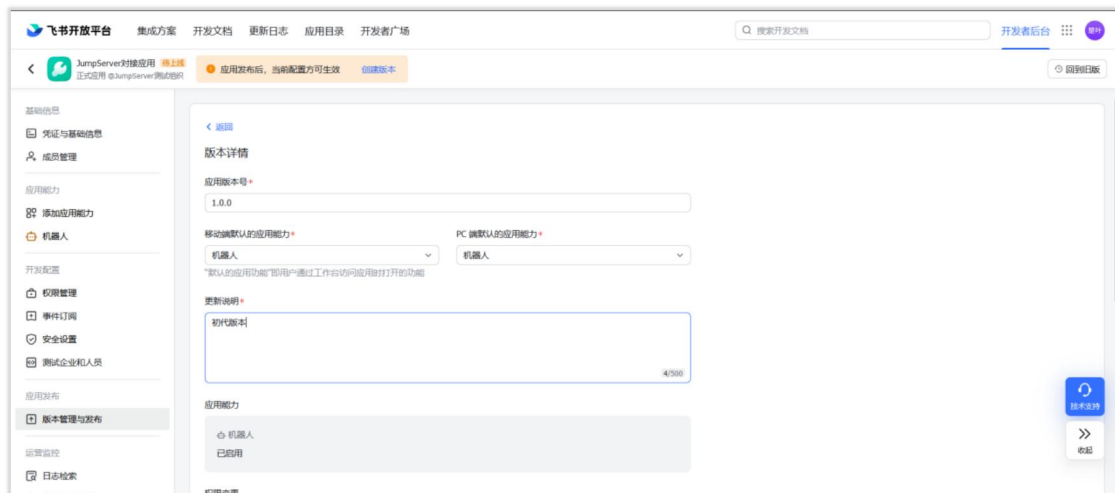
JumpServer 服务器的公网 IP。



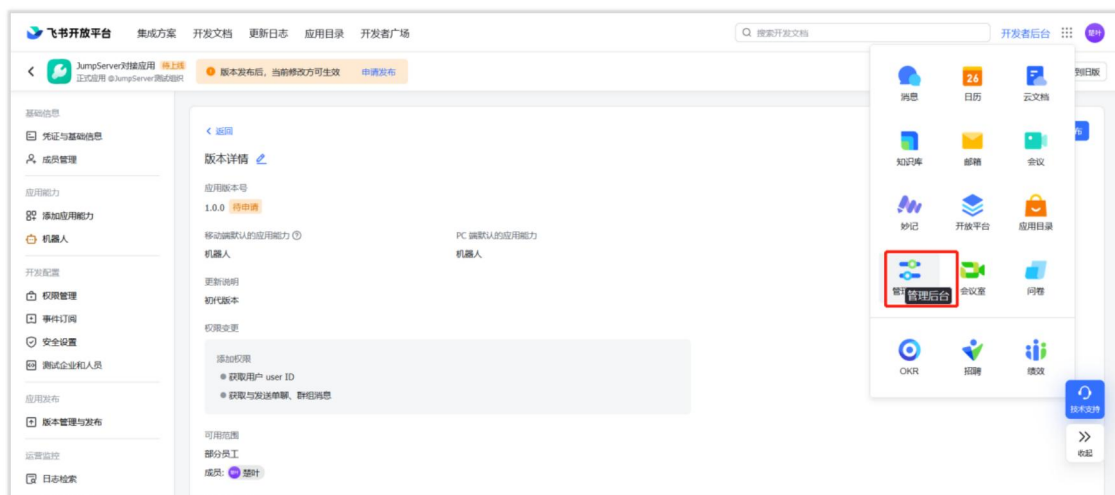
点击左侧<权限管理>添加“获取用户 userid”和“获取与发送单聊、群聊消息”权限。



点击左侧<版本管理与发布>点击右上角<创建版本>，输入应用版本号，应用功能选择<机器人>，输入更新说明，指定员工，点击保存。点击左上角，申请发布应用。



打开飞书管理后台，选择左侧<工作台>中的<应用审核>，点击<审核>按钮，通过审核信息。

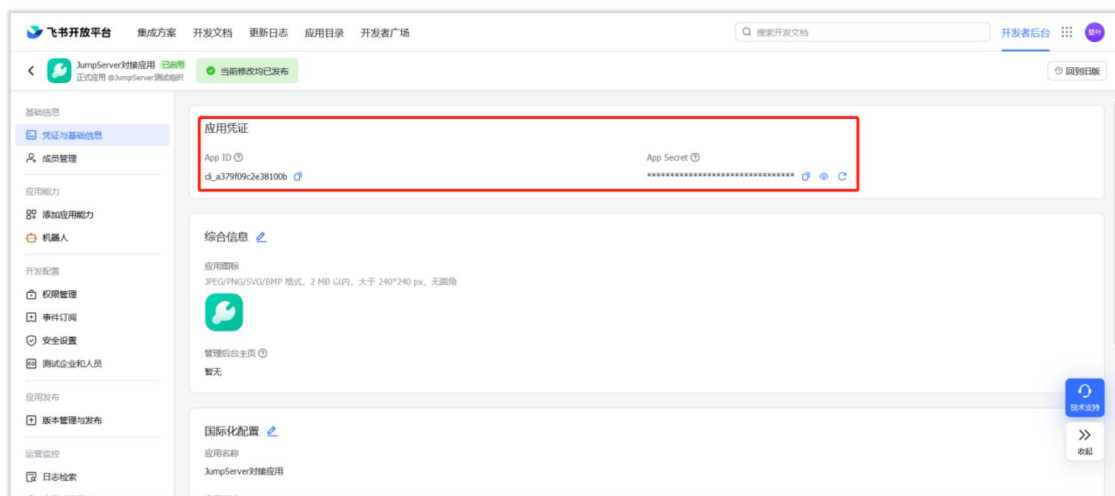




查看该应用处于“已启用”状态。

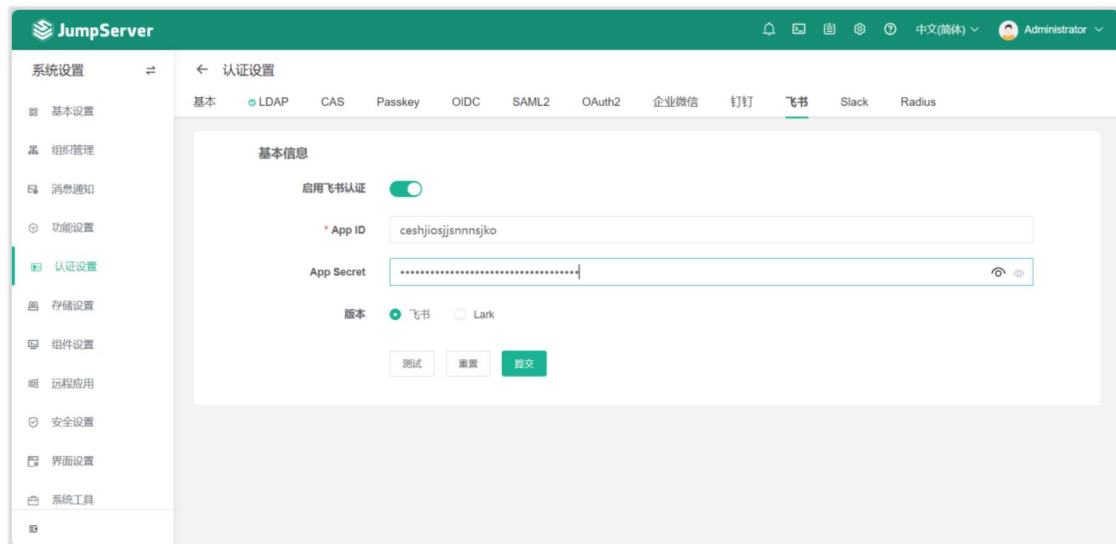


点击进入应用详情页，获取应用凭证信息。



4.6.10.2. JumpServer 端配置

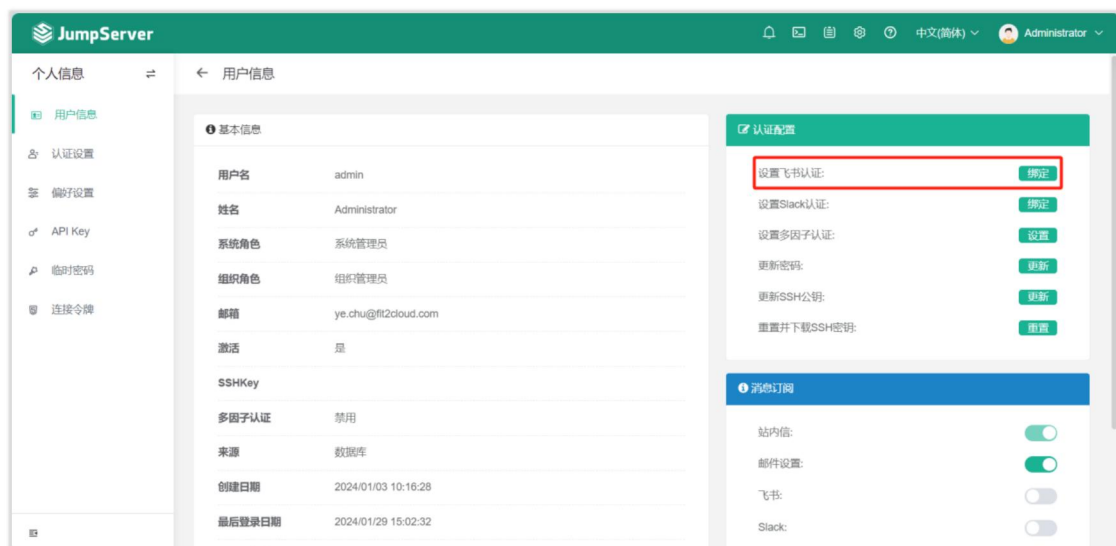
点击 JumpServer 系统设置的认证设置页面，选择“飞书”页签，填写获取到的飞书应用认证信息。



点击<测试>按钮测试是否成功并提交相关信息。

4.6.10.3. 飞书账号登录

点击用户名称进入个人信息页面，在认证配置模块设置飞书认证即绑定飞书账号。

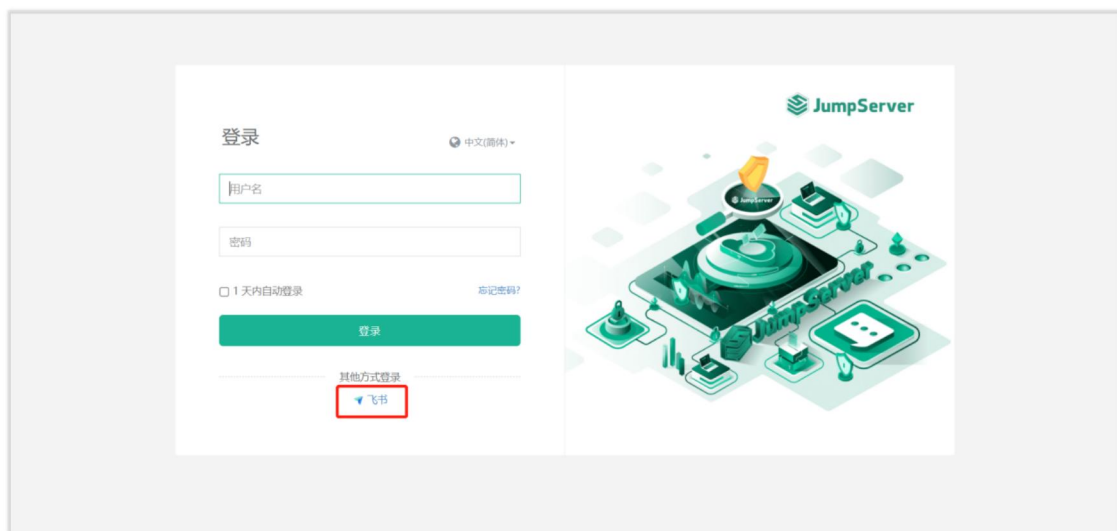


绑定飞书账号需验证账号的密码，输入密码后跳转至飞书操作登录页面。



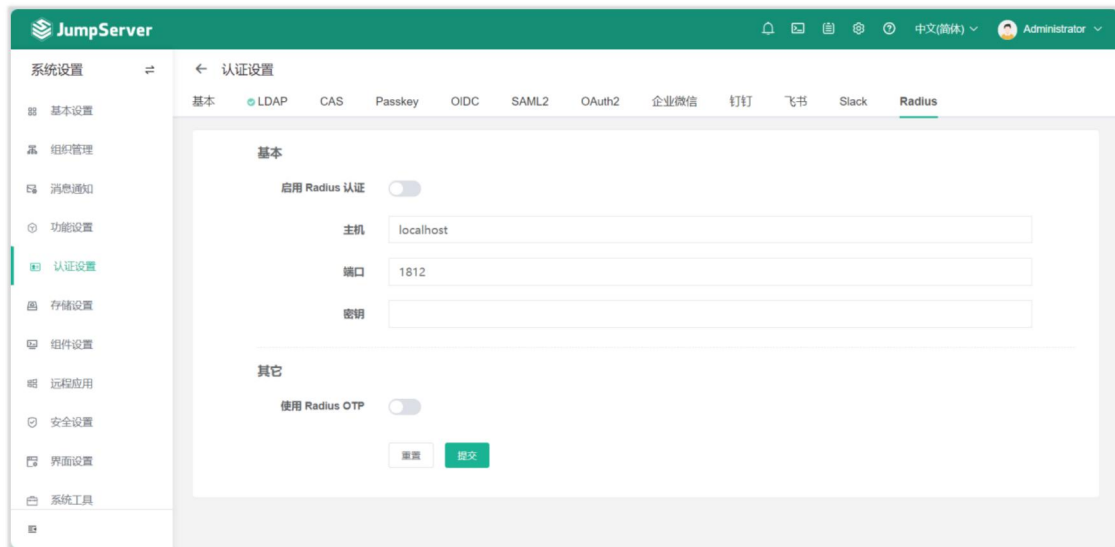
扫码后跳转即绑定配置成功。

在登录页面选择飞书登录模式，使用飞书扫码登录 JumpServer。



4.6.11. Radius

JumpServer 支持使用 Radius 进行认证。Radius 认证可直接在页面进行配置，具体配置如下图所示：



配置项参数详解：

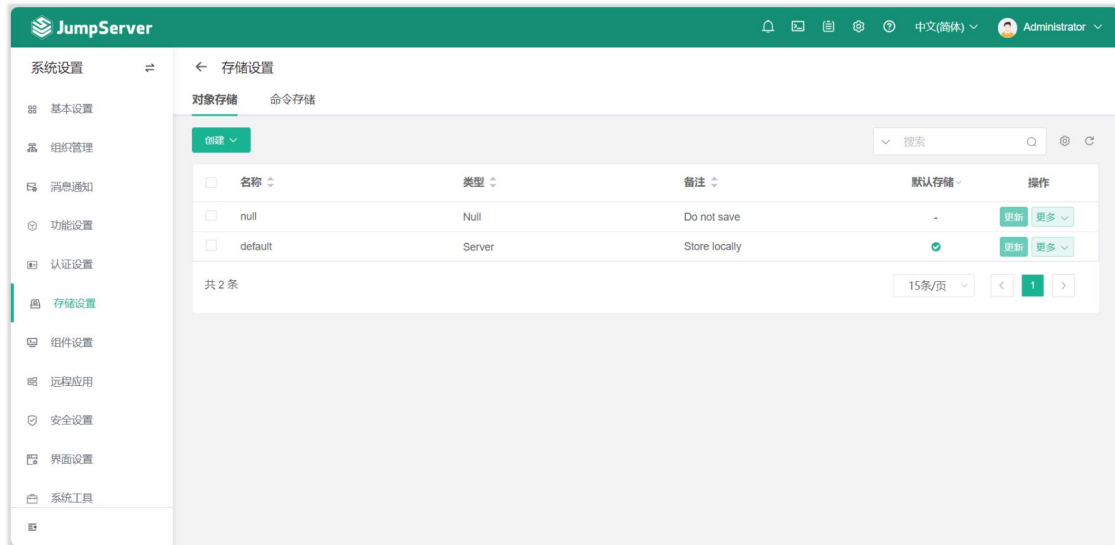
参数名称	说明
启用 Radius 认证	是否启用 Radius 认证。
主机	Radius 服务器的 IP 或域名。
端口	Radius 服务器的端口。
密钥	Radius 服务器的预共享密钥。
使用 Radius OTP	使用动态密码认证，可以配合 Ldap 使用。

注：宁盾对接时，如果宁盾架构为高可用架构且拥有虚拟 IP，主机信息填写如下所示：

- 当 JumpServer 服务与宁盾服务同在一个网段时，宁盾返回包中宁盾地址为宁盾的真实地址；此时主机选项需填写宁盾服务的真实地址才可验证通过。
- 当 JumpServer 服务与宁盾服务不处于同一个网段时，宁盾返回包中宁盾地址为宁盾虚拟 IP 地址；此时主机选项可填写宁盾虚拟 IP。

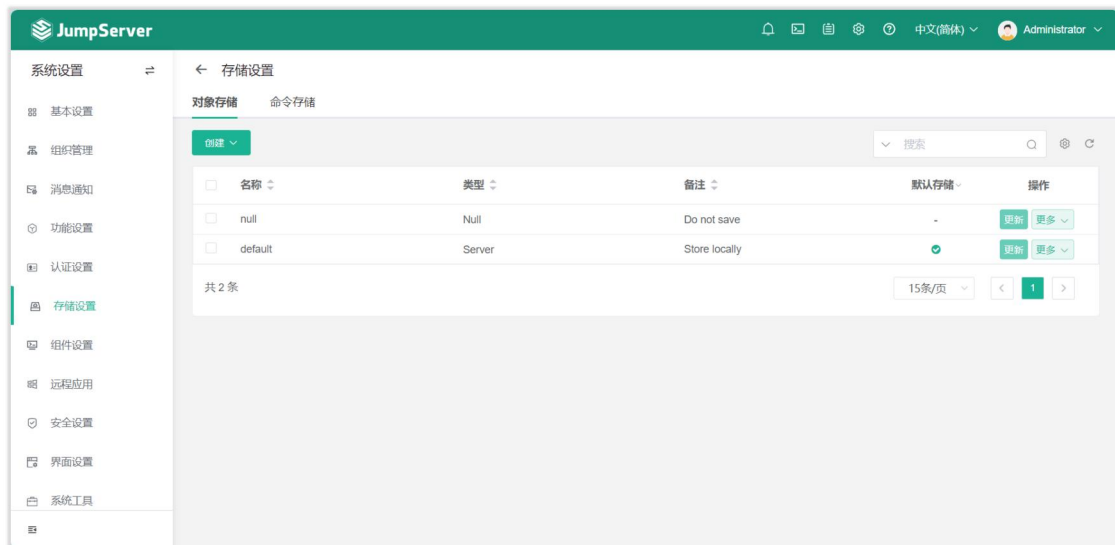
4.7. 存储设置

页面左侧点击[<存储设置>](#)按钮，进入存储设置页面。



4.7.1. 对象存储

对象存储页面可以对 JumpServer 连接资产的会话录像存储的位置进行自定义。目前支持的外部录像存储有亚马逊的 S3 云存储、Ceph、Swift、OSS、Azure、OBS、COS。



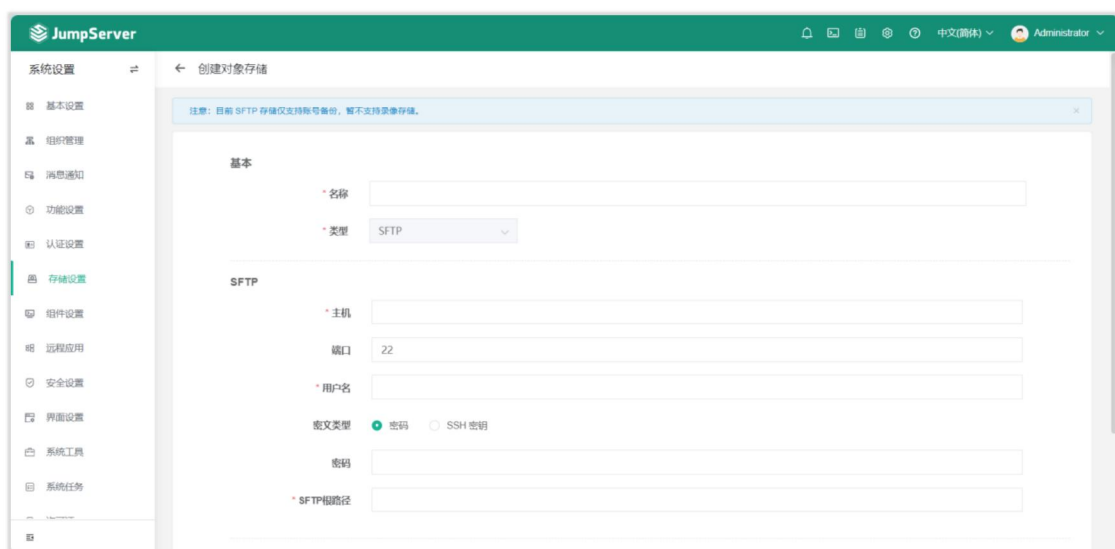
点击[创建](#)按钮，选择对应的存储类型，以华为云的 OBS 存储为例：

以下图片中红框中的信息均在华为云控制台页面获取，输入对应的字段后点击提交。创建完成后，即在终端管理中更新录像存储将录像存储在华为的 OBS 存储桶中。

JumpServer 录像存储对接外部存储后，定期清理页面中的会话日志保存时间对录像存储失效。

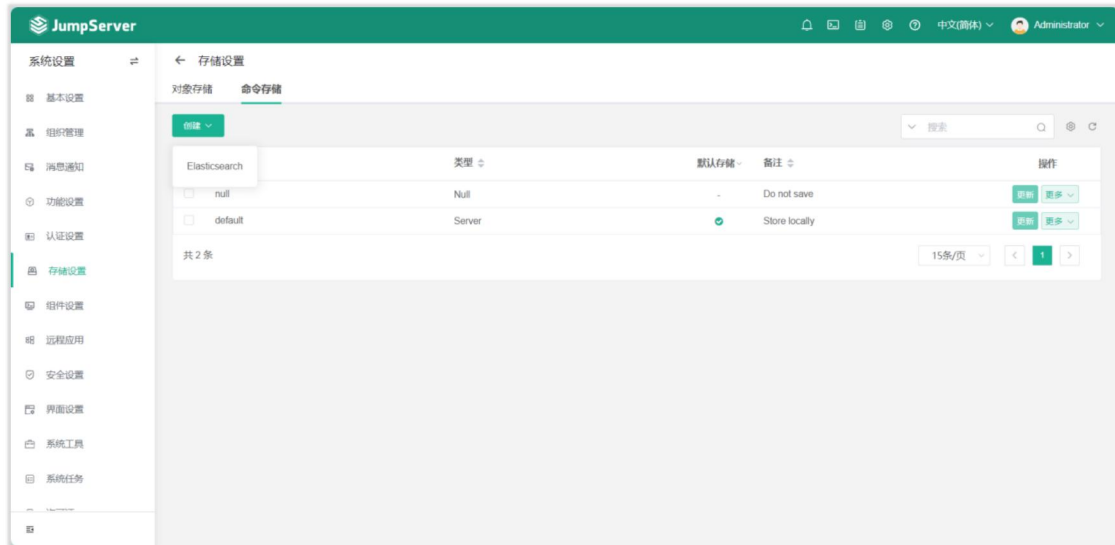


对象存储页面可以设置 SFTP 存储对账号进行备份。



4.7.2. 命令存储

命令存储页面可以更改 JumpServer 连接资产的会话命令记录存储的位置。默认的资产会话命令记录存储在 JumpServer 的数据库中，目前支持的外部命令存储有 Elasticsearch 。



点击<创建>按钮，创建一个新的命令存储，将 JumpServer 连接资产产生的会话存储到外部，减少数据库的存储用量。输入对应的字段点击提交，即创建成功。

JumpServer 支持使用 Elasticsearch 存储日志并支持根据日期建立索引，索引名为：JumpServer 页面中配置的索引名+命令记录产生的日期，方便用户根据日期进行查询与管理。使用外部命令存储后，定期清理页面中的会话日志保存时间对命令存储失效。

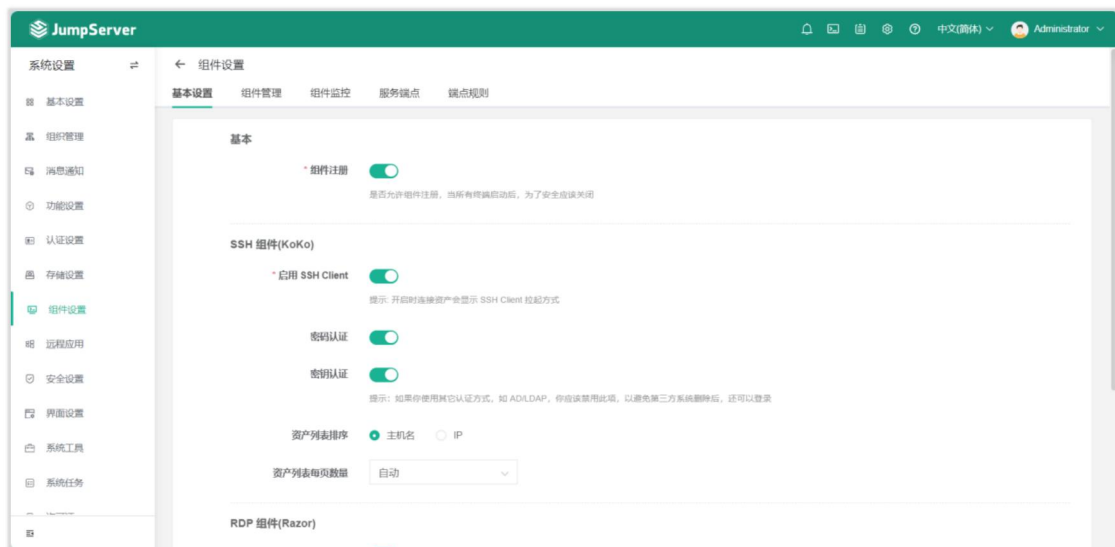


成功创建的索引如下图：



4.8. 组件设置

页面左侧点击[组件设置](#)按钮，进入组件设置页面。



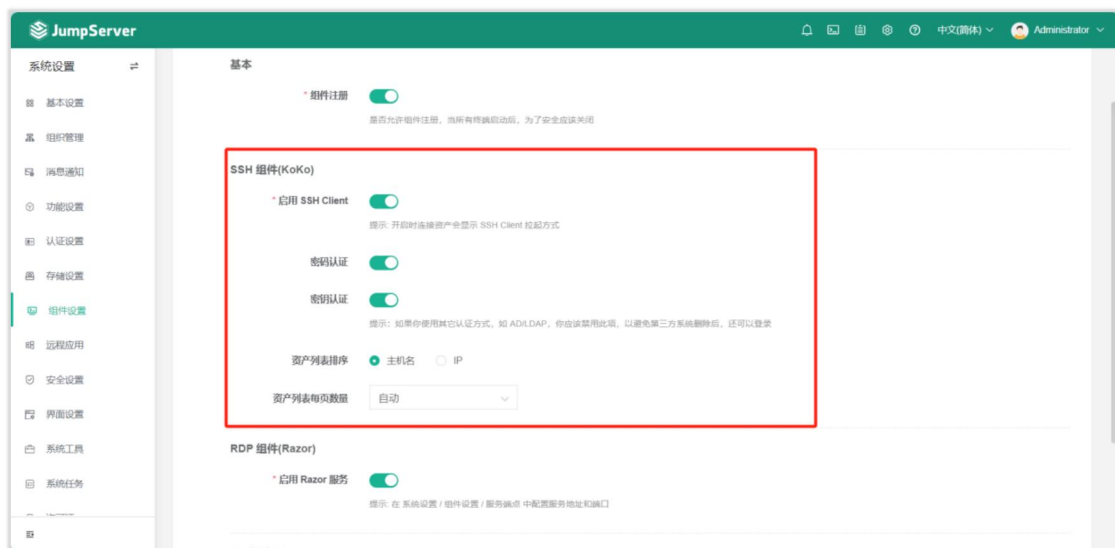
4.8.1. 基本设置

基本设置主要对四个方面进行设置：组件注册、KoKo 组件、Razor 组件、Magnus 组件。组件注册是一个安全设置。关闭终端注册后，其余组件无法正常注册到核心组件 core 中。

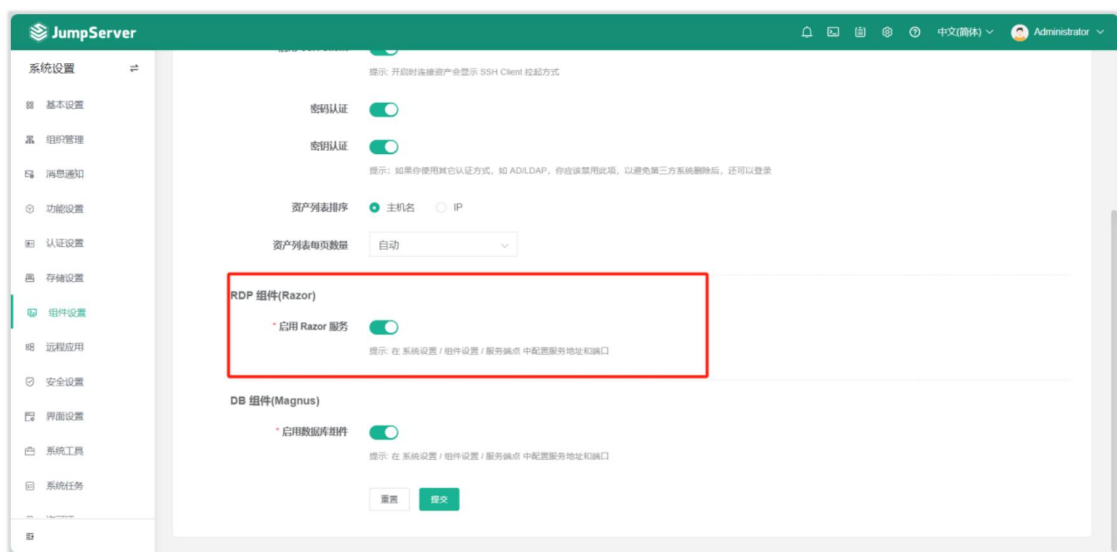


KoKo 组件是服务于类 Unix 系统平台的组件，该组件的功能主要是：

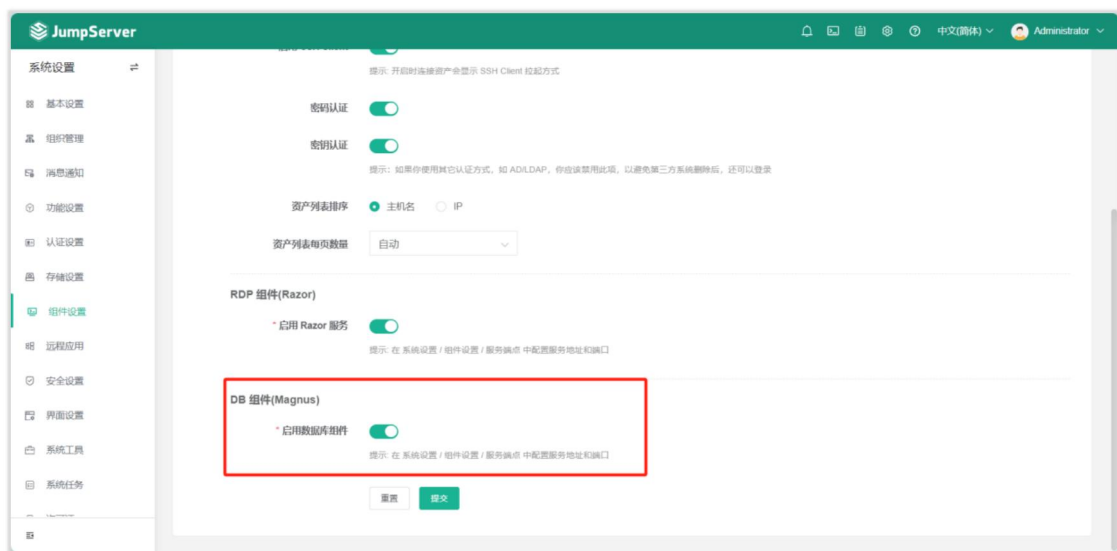
- 命令行的方式纳管 Linux、数据库、K8S 等资产；
- 作为 SSH 服务，可通过 2222 端口通过 SSH 协议或者 SFTP 协议操作资产。



Razor 组件是服务于 Windows 系统的组件，通过 JumpServer 客户端连接 Windows 资产。



Magnus 组件是服务于数据库资产的组件，主要功能是以数据库代理的方式支持用户通过原生数据库客户端（例如 Navicat、DBeaver 等）对数据库进行直连操作。



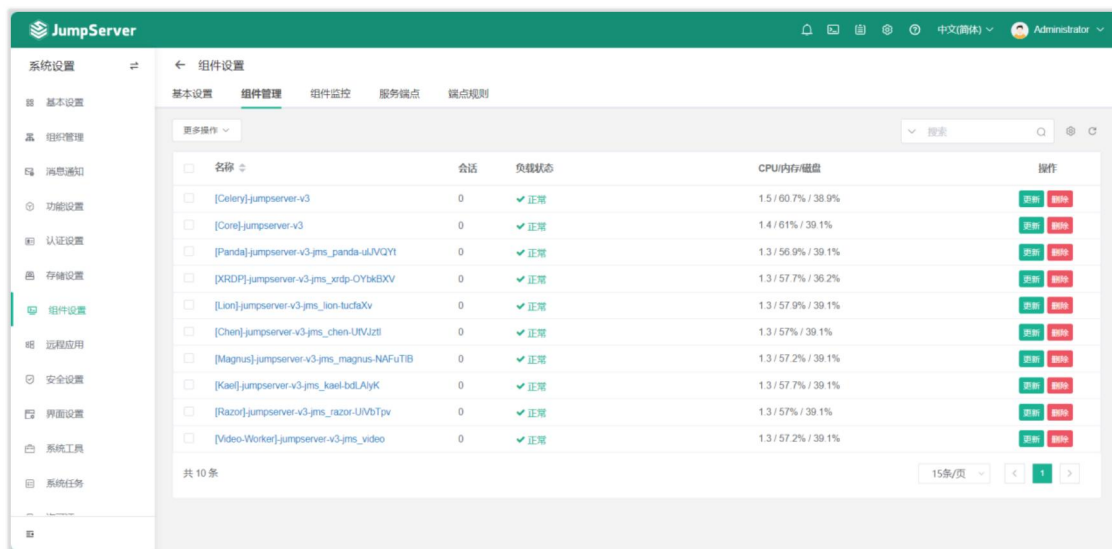
参数详细说明：

参数	说明
组件注册	是否允许其他外部的组件注册到本地的 Core 组件上。
启用 SSH Client	开启时连接 Linux 资产时可选择客户端方式连接，即通过 JumpServer Client 拉起本地的客户端连接 Linux 资产。
密码认证	该选项针对于命令行方式登录 JumpServer 堡垒机，关闭密码认证即不支持密码认证。
密钥认证	该选项针对于命令行方式登录 JumpServer 堡垒机，关闭密钥认证即不支持密钥认证。

资产列表排序	资产列表的排序规则按照“主机名”或者“IP”。
资产列表每页数量	资产列表每一页展示的资产数量。
启用 Razor 服务	是否启用 Razor 服务即使用 RDP 客户端连接 Windows 资产。
启用数据库组件	是否启用 Magnus 服务即使用外部客户端连接数据库资产。

4.8.2. 组件管理

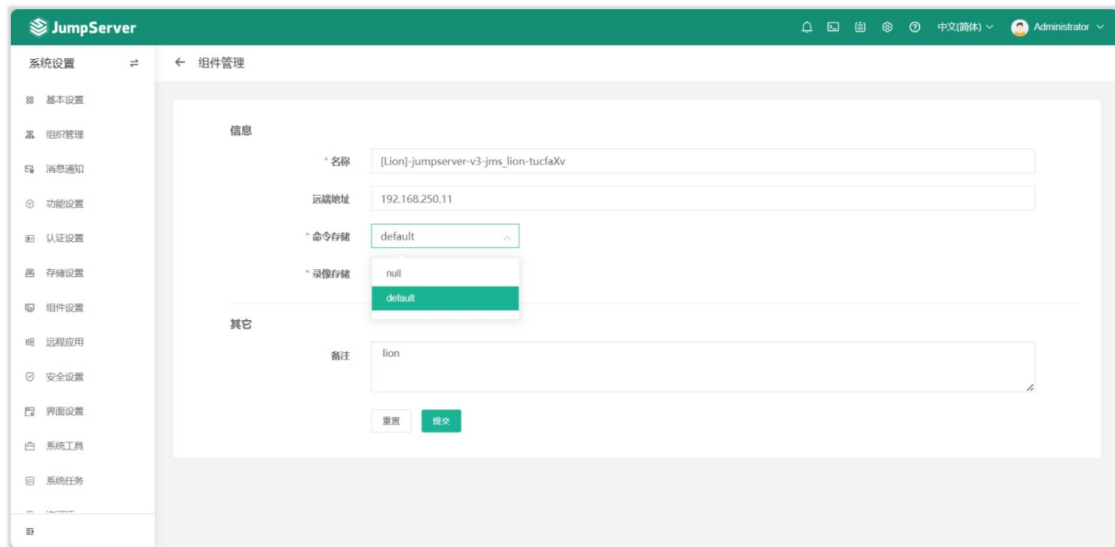
组件管理页面主要是查看 JumpServer 所有组件的使用状态，页面如下图所示：



终端管理页面主要可以查看的信息如下：

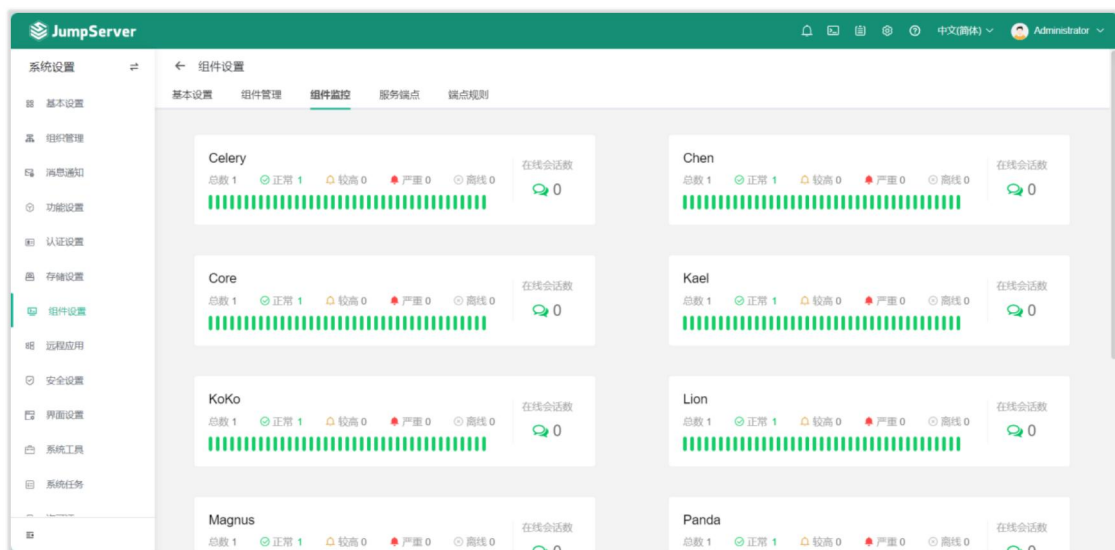
- 查看组件名，组件名称命名时会取组件所在的 **hostname** 和随机字符串的组合，当有多节点集群或者分布式部署时，可以通过该信息确定组件所在主机，便于排错处理；
- 查看 JumpServer 所有组件的 CPU 负载、内存使用率等性能信息；当使用率过高时，会产生监控告警，告警通知在消息订阅中进行配置；
- 查看会话，可以看到每个组件上实时的会话数。

点击某个组件的 [更新](#) 按钮或选择多个组件，点击更多操作可进行更新。更新组件的命令存储与录像存储，会话录像默认存放在服务器本地；会话命令默认存放在数据库中，这里可以更改会话录像与会话命令存储到外部存储。



4.8.3. 组件监控

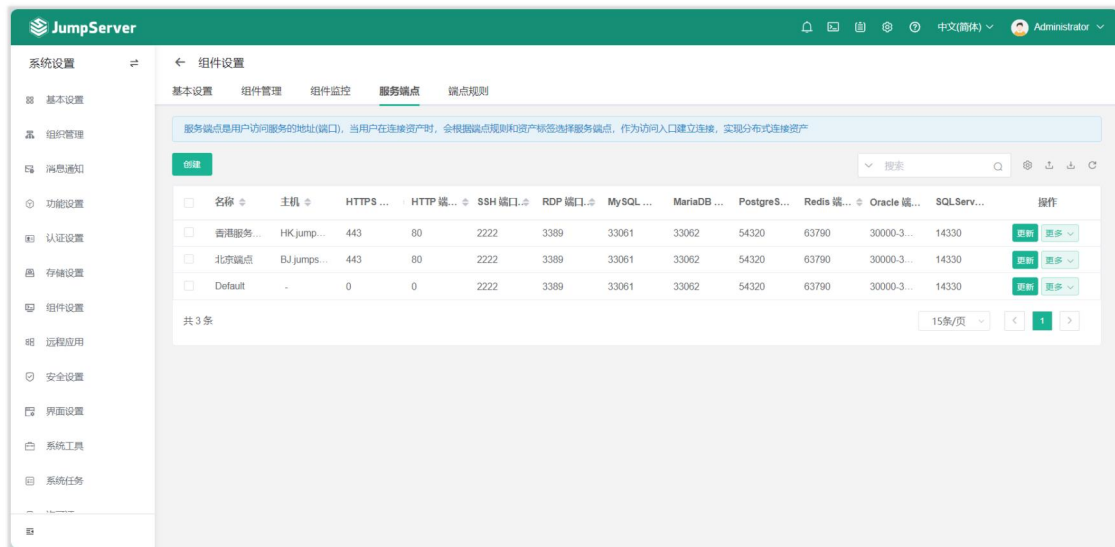
组件监控页面可以查看每个组件的状态，具体信息包含：组件的负载状态与该组件目前在线会话数。



4.8.4. 服务端点

服务端点页面主要是访问入口的相关设置。服务端点使用户访问服务的地址（端口），当用户在连接资产时，会根据端点规则和资产标签选择服务端点，作为访问入口建立连接，实现分布式连接资产。

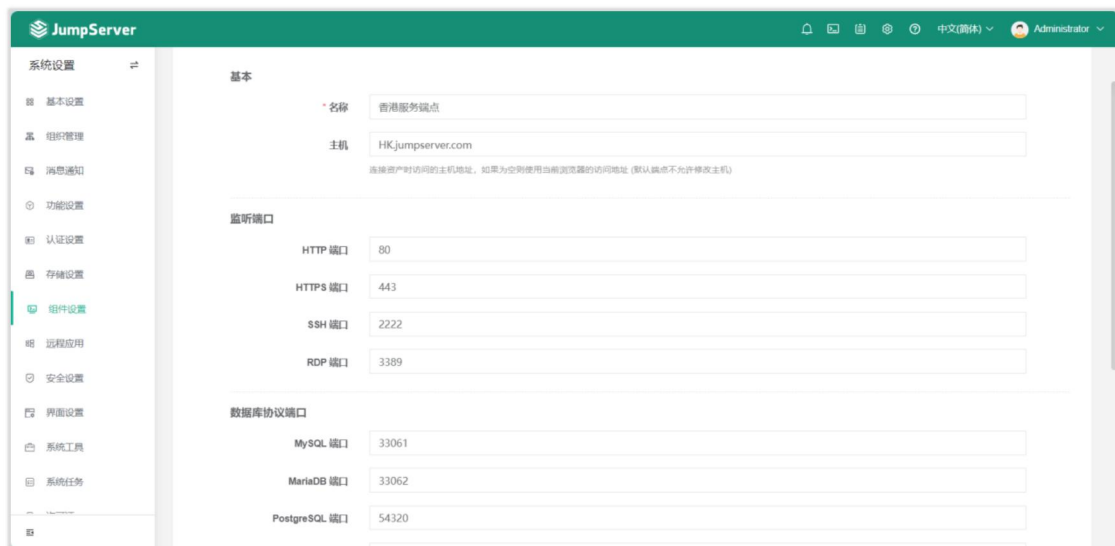
以下页面为 JumpServer 默认需要开通的端口，2222、3389 以及数据库映射端口。



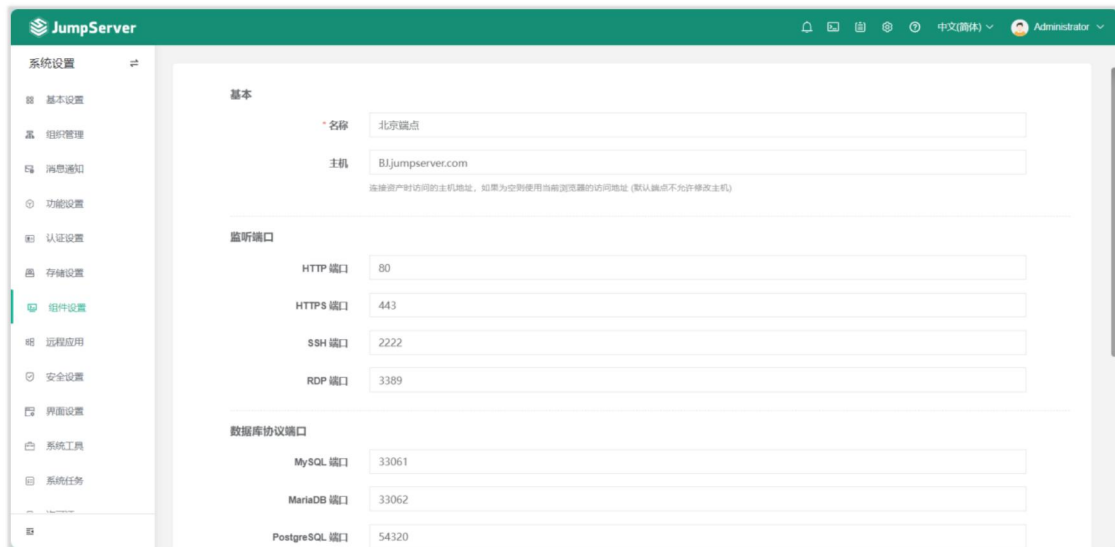
适用场景（例如）：

- 某公司在华为云上有两个区域的资产，分别处于香港与北京。需要使用同一套堡垒机对它们进行纳管，会由于网络延迟以及带宽性能的问题造成较大的困难。
- 服务端点此时即可解决以上问题。例如：使用香港的一台服务器部署一套 JumpServer 系统、北京的一台服务器部署一套 JumpServer 系统。
- 两套 JumpServer 系统共用同一个数据库。访问时，香港的资产使用香港的 JumpServer 入口进入，北京的资产使用北京的 JumpServer 入口进入，对应区域的云主机指定到对应的节点访问。

创建一个香港服务端点：



创建一个北京服务端点：

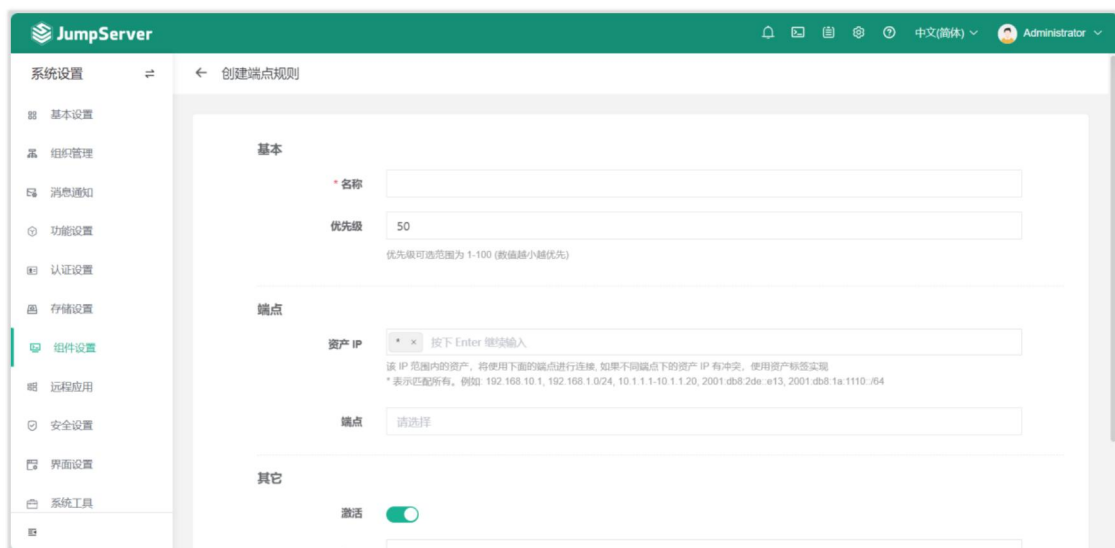


4.8.5. 端点规则

对于服务端点选择策略，目前支持两种：

- 根据端点规则指定端点(当前页面)；
- 通过资产标签选择端点，标签名固定是 **endpoint**，值是端点的名称。

两种方式优先使用标签匹配，因为 IP 段可能冲突，标签方式是作为规则的补充存在的。在端点规则中，设置哪些 IP 段，资产将对应访问到哪个服务端点。



4.9. 远程应用

JumpServer 支持以远程应用的方式创建 Web 页面访问以及使用 Navicat 等工具连接数据库。

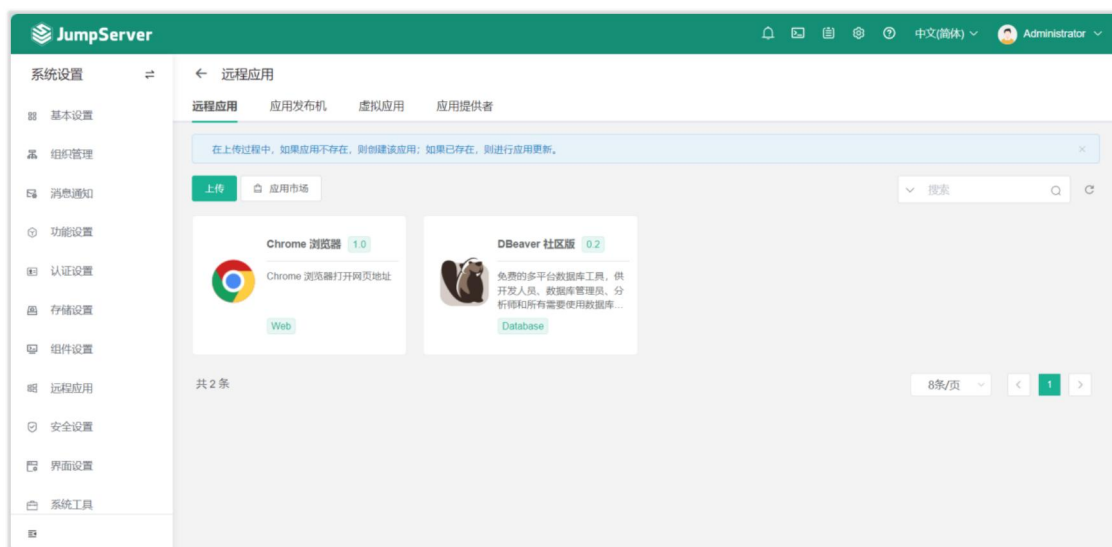
远程应用的 Web 页面配置顺序为：

- 创建应用发布机(应用发布机即一台干净的 Windows 服务器且安装了 OpenSSH 服务)。
- 部署应用发布机（该步骤会安装默认的远程应用即 Chrome 与其他远程应用到应用发布机中）。
- 创建 Web 页面资产与账号。
- 访问。

点击系统设置页面的[<远程应用>](#)按钮，进入远程应用设置页面。远程应用设置页面分为远程应用页面与应用发布机页面。

4.9.1. 远程应用

JumpServer 默认内嵌 Chrome、DBeever 远程应用，远程应用发布机部署时会默认安装远程应用。



4.9.1.1. 自定义远程应用

JumpServer 支持用户新建默认远程应用之外的应用。以下介绍如何自定义远程应用。

(一) Applet 介绍

自定义远程应用由 Applet 目录组成，Applet 是一个包含 Python 脚本的目录，其中必须包含以下文件：

- i18n.yml：对 manifest.yml 的国际化文件。
- icon.png：Applet 的图标
- main.py：Python 代填的执行脚本。
- manifest.yml：Applet 的元数据。
- setup.yml：拉起程序的安装描述。

(二) 元数据 manifest.yml

manifest.yml 定义了 Applet 的元数据，如名称、作者、版本、支持的协议。

```
name: mysql_workbench8 (required)

display_name: MySQL Workbench8

comment: A tool for working with MySQL, to execute SQL and design tables
(required)

version: 0.1 (required)

exec_type: python (reserved, 暂未使用)

author: Eric (required)

type: general (required)

update_policy: none (暂未使用)

tags: (required)

  - database

protocols: (required)

  - mysql
```

详细参数说明：

字段	说明
name	名称。优先选择字母数字，不支持特殊字符。
protocols	此 Applet 脚本支持的协议。
tags	标签信息。
type	主要包含 General、Web。
l18n.yml	对 manifest.yml 的国际化文件。

(三) 安装条件 setup.yml

setup.yml 定义了 Applet 拉起程序的安装方式。

```
type: msi # exe, zip, manual

source: https://jms-pkg.oss-cn-beijing.aliyuncs.com/windows-pkgs/mysql-workbench-community-8.0.31-winx64.msi

arguments:

  - /qn

  - /norestart
```

destination:	C:\Program Files\MySQL\MySQL Workbench 8.0 CE
program:	C:\Program Files\MySQL\MySQL Workbench 8.0 CE\MySQLWorkbench.exe
md5:	d628190252133c06dad399657666974a

详细参数说明：

参数	说明
type	定义软件的安装方式。 msi: 安装软件; exe: 安装软件; zip: 解压安装方式; manual: 手动安装方式。此种方式下, source 等保持为空, 可不校验 MD5 值。需要手动登录应用发布及安装软件。
source	软件下载地址。
arguments	msi 或者 exe 安装程序需要的参数, 使用静默安装。
destination	程序安装目录地址。
program	具体的软件地址。
md5	program 软件的 md5 值, 主要用于校验安装是否成功。

(四) 脚本执行 main.py

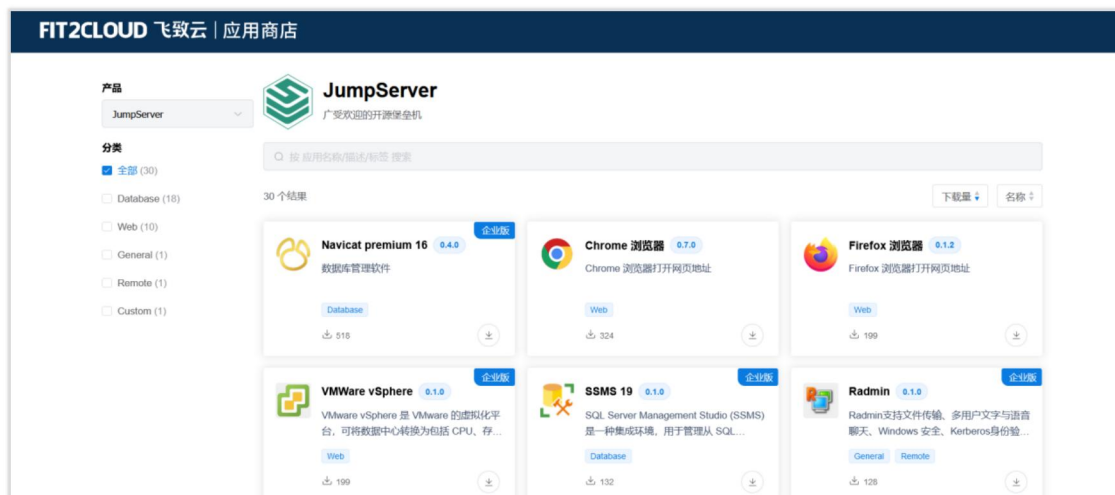
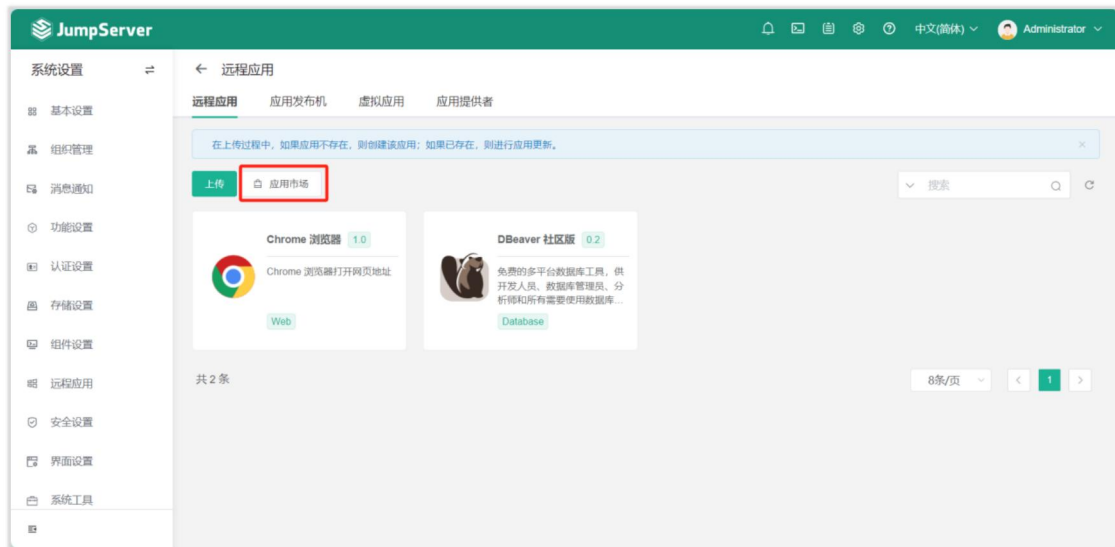
main.py 是 Python 脚本主程序。JumpServer 的 Remoteapp 程序 tinker 将通过调用 python main.py base64_json_data 的方式执行。base64_json_data 是 JSON 数据进行 base64 之后的字符串, 包含资产、账号等认证信息。数据格式大致如下, 依据 api 变化做相应调整:

<p>示例:</p> <pre>{ "app_name": "mysql_workbench8", "protocol": "mysql", "user": { "id": "2647CA35-5CAD-4DDF-8A88-6BD88F39BB30", "name": "Administrator",</pre>

```
    "username": "admin"
  },
  "asset": {
    "asset_id": "46EE5F50-F1C1-468C-97EE-560E3436754C",
    "asset_name": "test_mysql",
    "address": "192.168.1.1",
    "protocols": [
      {
        "id": 2,
        "name": "mysql",
        "port": 3306
      }
    ]
  },
  "account": {
    "account_id": "9D5585DE-5132-458C-AABE-89A83C112A83",
    "username": "root",
    "secret": "test"
  },
  "platform": {
    "charset": "UTF-8"
  }
}
```

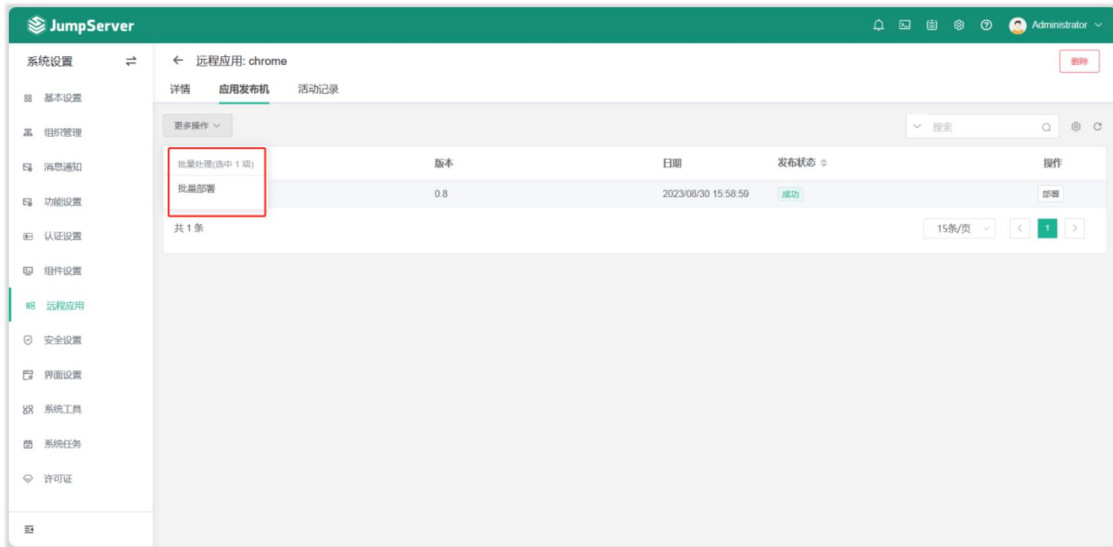
4.9.1.2. 应用商店

在远程应用页面中，点击远程应用页签中的[应用市场](#)按钮进入飞致云官网提供的应用市场页面。飞致云应用市场中包含多种远程应用，例如：**Firefox** 浏览器、**SSMS**、阿里云管理平台等。



4.9.1.3. 批量部署

JumpServer 支持将单个远程应用批量推送至纳管的远程发布机上。

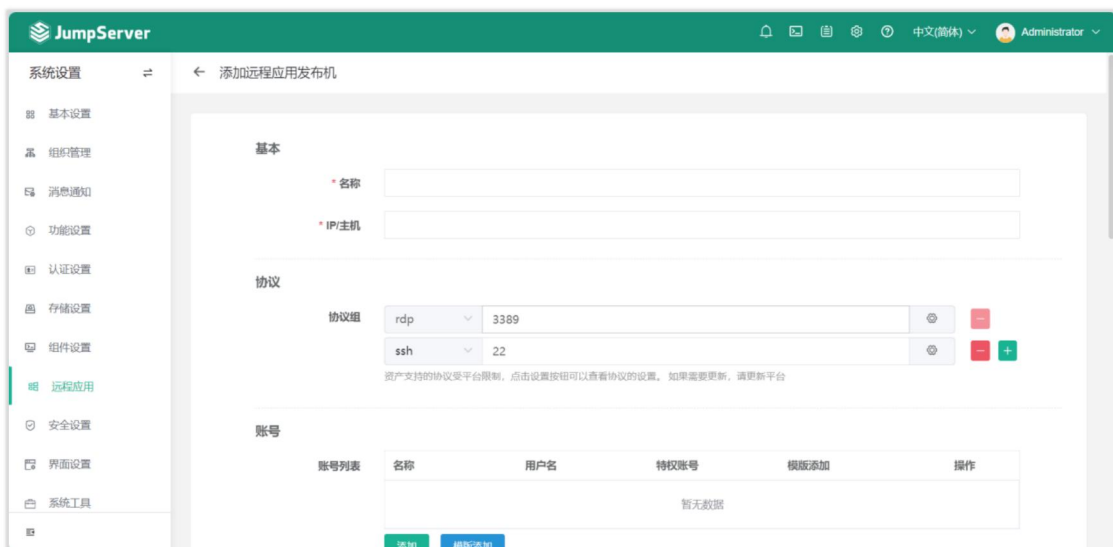


4.9.2. 应用发布机

应用发布机是用来运行 Web 页面资产或者使用远程应用 DBeaver 等连接数据的程序运行主体。应用发布机支持使用资产标签匹配机制给某个远程应用资产配置标签，指定远程应用发布机连接到此远程应用。

4.9.2.1. 创建应用发布机

点击应用发布机页面的[<创建>](#)按钮即新建一个应用发布机。



详细参数说明：

参数	说明
----	----

名称	远程应用发布机的名称，识别信息。
IP/主机	远程应用发布机的 IP 信息。
协议组	远程应用发布机支持的协议组以及协议组的端口。
账号列表	远程应用发布机的管理员连接账号信息。
使用同名账号	是否优先使用同名账号连接发布机。此功能需在配置文件中开启。
自动创建账号	创建应用时是否创建用户连接应用的账号。
创建账号数量	创建连接应用的账号的数量。
Core 服务地址	远程应用发布机的 agent 与 JumpServer 堡垒机 core 服务的通信地址。
已有 RDS 许可证	是否拥有 RDS 许可证，需到微软官方购买 RD 授权许可。
RDS 许可服务器	RDS 许可服务器信息。
RDS 授权模式	<p>选择“设备”或“用户”设置授权模式。</p> <ul style="list-style-type: none"> ● 设备：允许一台设备（任何用户使用的）连接到远程应用发布机。 ● 用户：授予一个用户从无限数目的客户端计算机或设备访问远程应用发布机。
RDS 单用户单会话	<p>选择“禁用”或“启用”设置单用户单会话模式。</p> <ul style="list-style-type: none"> ● 禁用：允许每个用户可以同时多台客户端电脑连接服务器远程桌面。 ● 启用：禁止每个用户可以同时多台客户端电脑连接服务器远程桌面。
RDS 最大断开时间	如果某个会话连接达到了此最大时间，连接即断开。
RDS 远程应用注销时间限制	远程应用会话断开后的注销时间。
网域	可选项，针对某些跨网段远程应用发布机，需要以网域网关（sshpas）为代理进行访问。

提交即可创建远程应用发布机。

4.9.2.2. 部署应用发布机

部署应用发布机前，需确认远程应用发布机上安装了 OpenSSH 服务。可从下载中心页面中

下载快捷安装方式。

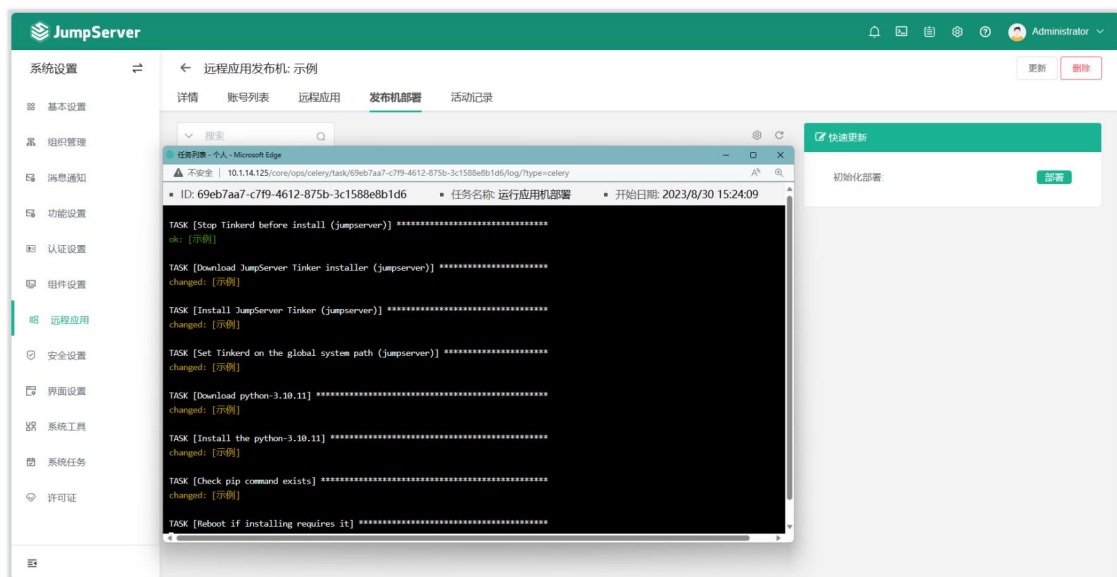
Windows 远程应用发布服务器工具

OpenSSH 是在 windows 远程应用发布服务器中用来连接远程应用的程序

- [openSSH-win64.msi](#)

创建应用发布机后需手动执行应用发布机部署，安装 Python、Chrome、Navicat、DBeaver 或自定义远程应用。

点击[<应用发布机名称>](#)按钮进入应用发布机详情页中，选择发布机部署页签，点击快速更新模块的[<初始化部署>](#)按钮，初始化应用发布机。



部署完成后即远程应用发布机部署完成。

4.9.2.3. 查看应用发布机详情

点击[<应用发布机名称>](#)按钮进入应用发布机详情页中，此页面包含应用发布机详情信息，包括：远程应用发布机帐号列表、远程应用、发布机部署记录等。



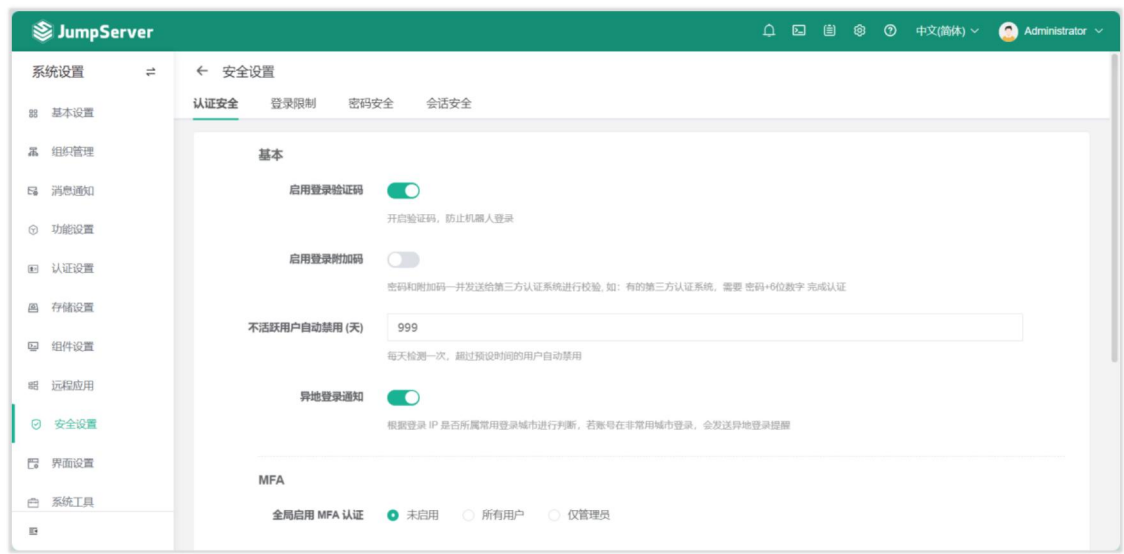
远程应用发布机详情页模块说明：

模块	说明
详情	该模块主要包含远程应用发布机的基本信息以及简单的自动化任务，更新硬件信息、测试可连接性等。
账号列表	该模块主要展示远程应用发布机的账号。默认状况下初始化远程应用发布机时 JumpServer 会创建 100 个登录用户以支持远程应用会话。
远程应用	该模块中包含默认的远程应用与自建的远程应用信息，在该模块可直接对远程应用进行部署。
发布机部署	该模块中主要用于远程应用发布机的初始化部署，以及部署日志的查看。
活动记录	该模块中记录了远程应用发布机的活动记录信息，点击可查看详情。

4.10. 安全设置

点击页面左侧的<安全设置>按钮，进入安全设置页面。安全设置页面主要配置 **JumpServer** 安全相关信息，编辑认证安全以及密码等校验规则。

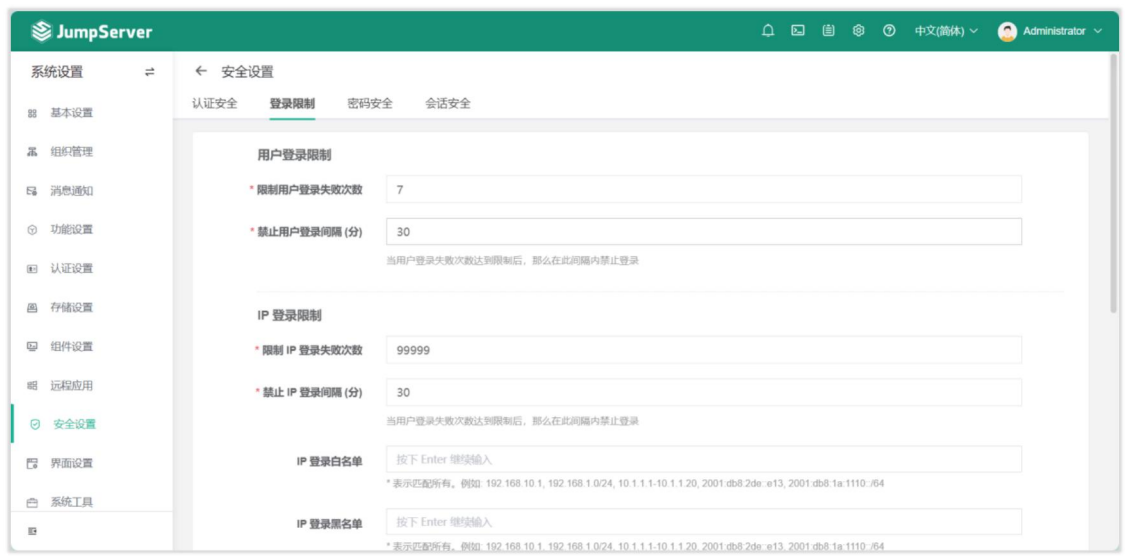
4.10.1. 认证安全



详细参数说明：

参数	说明
启用登录验证码	启用登录验证码，防止机器人登录。
启用登录附加码	密码和附加码一起发送给第三方认证系统进行校验，如：有的第三方认证系统，需要密码+6 位数字 完成认证。
不活跃用户自动禁用（天）	设置预设时间，在该时间内没有登录 JumpServer 的用户自动禁用。
异地登录通知	根据登录 IP 判断是否属常用登录城市，如果不是，会发送异地登录提醒邮件到用户邮箱。
全局启用 MFA 认证	可以设置禁用 MFA，或所有用户启用 MFA、或仅管理员启用。当全局设置启动 MFA 时，单个用户无法关闭 MFA 验证。
第三方开启 MFA	支持 OIDC、CAS、SAML2 认证方式的用户进行 MFA 认证。
MFA 有效期	当查看账号密码时，验证 MFA 之后有效期内不需要再次验证。
OTP 扫描后的名称	绑定 MFA 之后动态码在软件端的显示名称。
OTP 延迟有效次数	OTP 延迟的有效次数

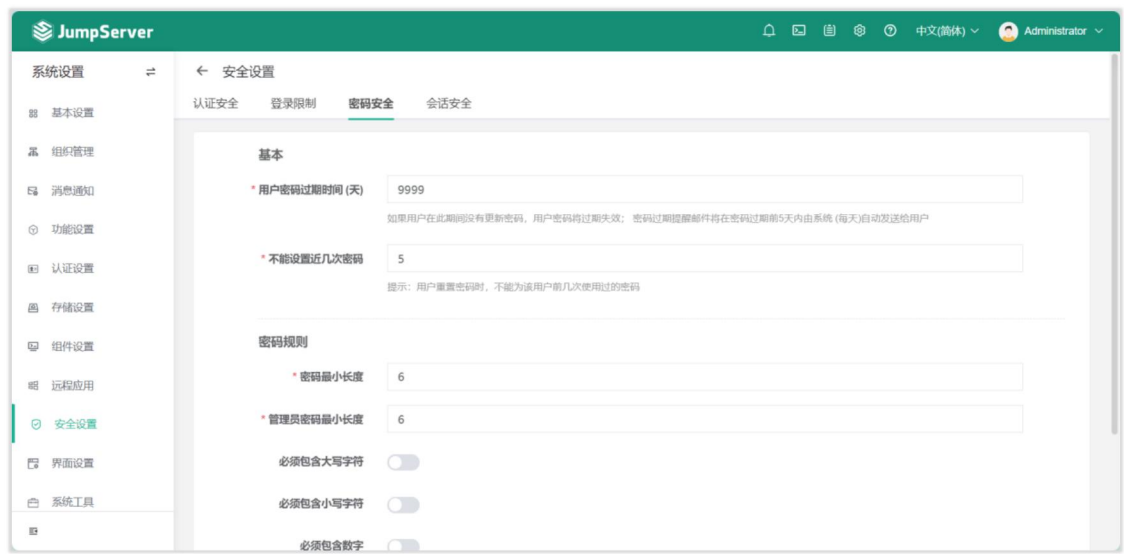
4.10.2. 登录限制



详细参数说明：

参数	说明
限制用户登录失败次数	用户输错密码最多登录失败次数，之后将会被锁定一段时间。
禁止用户登录间隔	用户锁定的时间。
限制 IP 登录失败次数	某 IP 最多登录失败次数，之后将会被禁止登录一段时间。
禁止 IP 登录间隔	IP 锁定的时间。
IP 登录白名单	允许登录堡垒机的 IP。
IP 登录黑名单	不允许登录堡垒机的 IP。
已锁定的 IP	超过设置的登录失败次数后被锁定的 IP。
仅一台设备登录	仅允许用户在一台设备上登录。下个设备登录，上一个登录设备会强制下线。
仅已存在用户登录	仅允许存在于 JumpServer 用户列表中的用户登录。
仅从用户来源登录	仅允许用户从用户列表中列出的来源处登录。

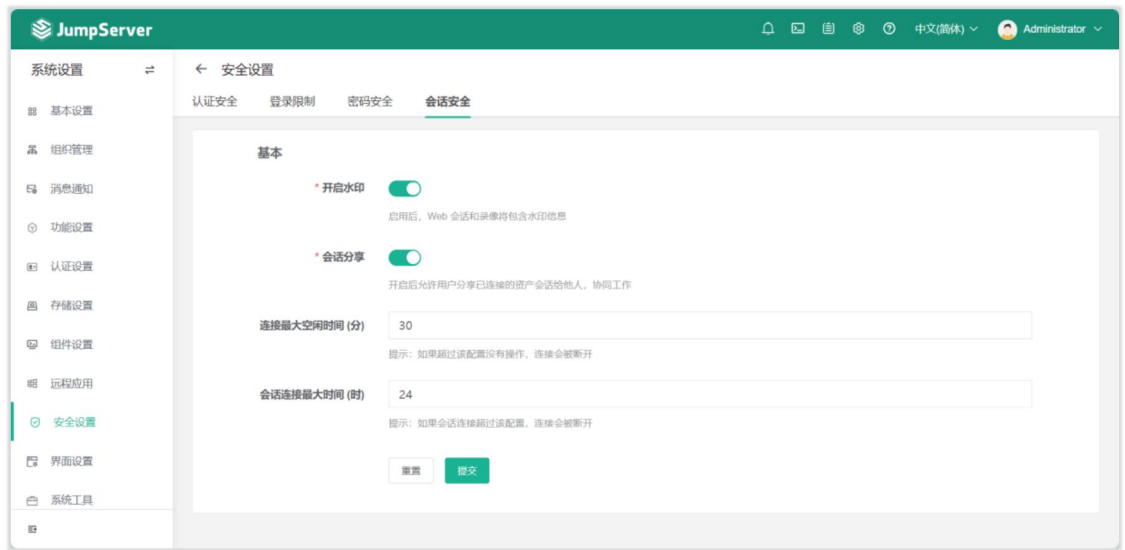
4.10.3. 密码安全



详细参数说明：

参数	说明
用户密码过期时间（天）	用户每隔多少天需要强制更新密码。单位：天，如果用户在此期间没有更新密码，用户密码将过期失效； 密码过期提醒邮件将在密码过期前 5 天内由系统（每天）自动发送给用户。
不能设置近几次密码	用户重置密码时，不能为该用户前几次使用过的密码。
密码最小长度	设置用户密码支持的最小长度。
管理员密码最小长度	设置管理员密码支持的最小长度。
必须包含大写字符	密码中必须包含大写字符。
必须包含小写字符	密码中必须包含小写字符。
必须包含数字	密码中必须包含数字字符。
必须包含特殊字符	密码中必须包含特殊字符，如#\$@%等。

4.10.4. 会话安全



详细参数说明：

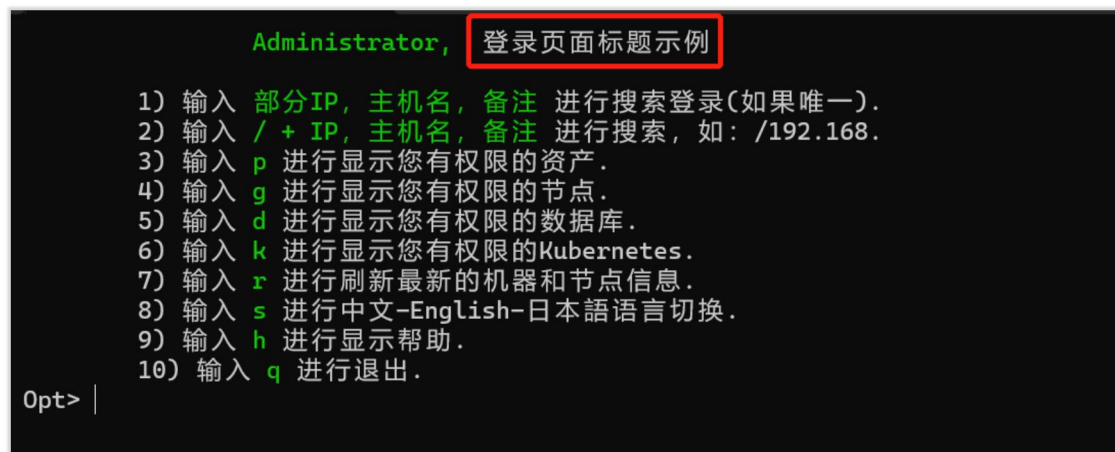
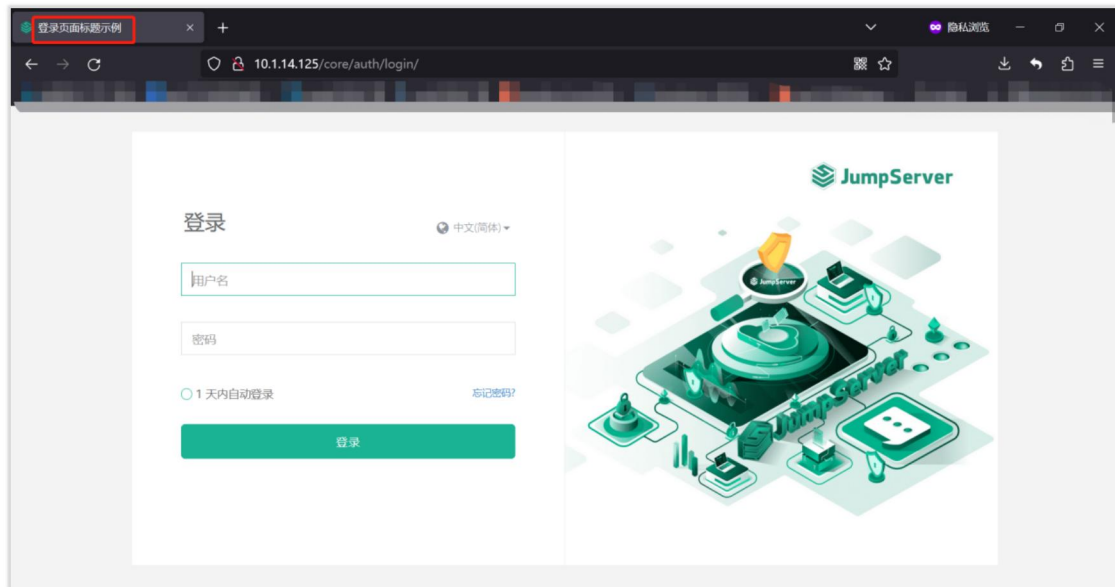
参数	说明
开启水印	会话和录像会包含访问资产的堡垒机用户水印信息。 RDP 客户端 方式的连接不支持水印。
会话分享	开启后允许用户以 URL 形式分享已连接的资产会话给他人，方便协同工作。
连接最大空闲时间（分）	资产在空闲时间达到此配置时会自动断开。
会话连接最大时间（时）	资产连接会话到达此时间后自动断开。

4.11. 界面设置

点击页面左侧的[<界面设置>](#)按钮，进入界面设置页面。界面设置主要包含：登录页面标题设置、JumpServer 整体主题设置，JumpServer 相关 Logo 设置、登录页面图片设置以及备案号设置。

4.11.1. 基本设置

基本设置包含登录页面标题与主题。登录页面标题可自定义，自定义后显示如下：



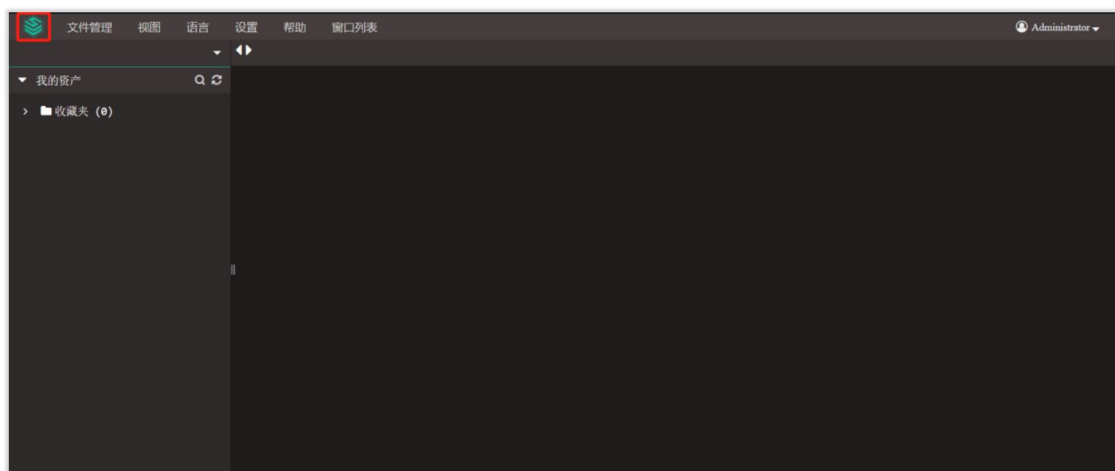
JumpServer 支持多种主题切换，目前支持的主题有：中国红、深邃黑、科技蓝、经典绿、高贵紫。

4.11.2. Logo

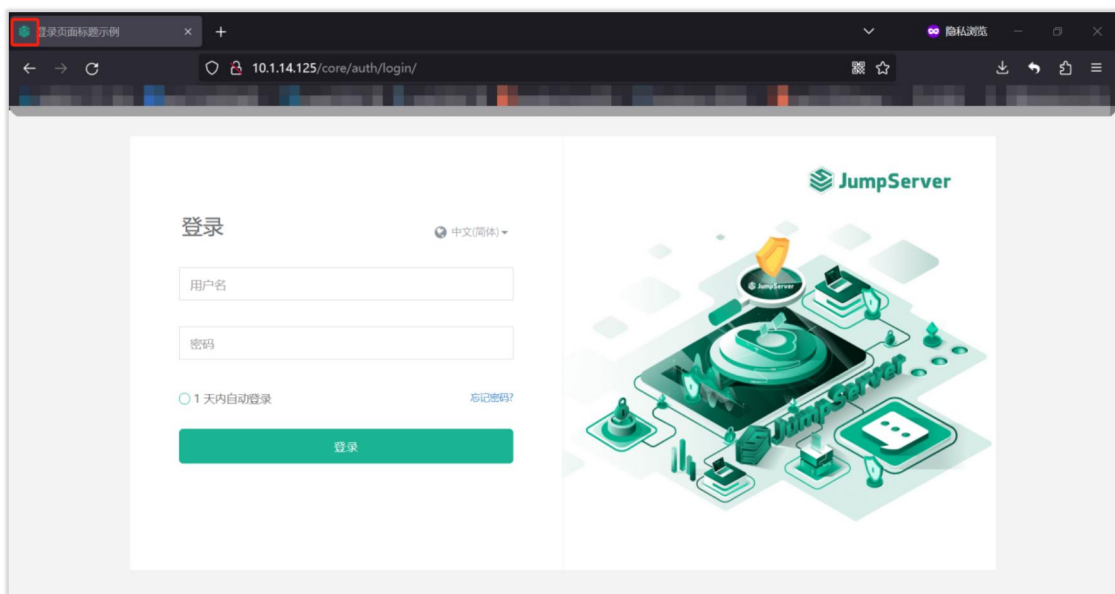
Logo(带文字)的选项调整后将会显示在管理页面左上方，如下图所示：



Logo（不带文字）的选项调整后会显示在企业版用户的 Web 终端的小图标，如下图所示：

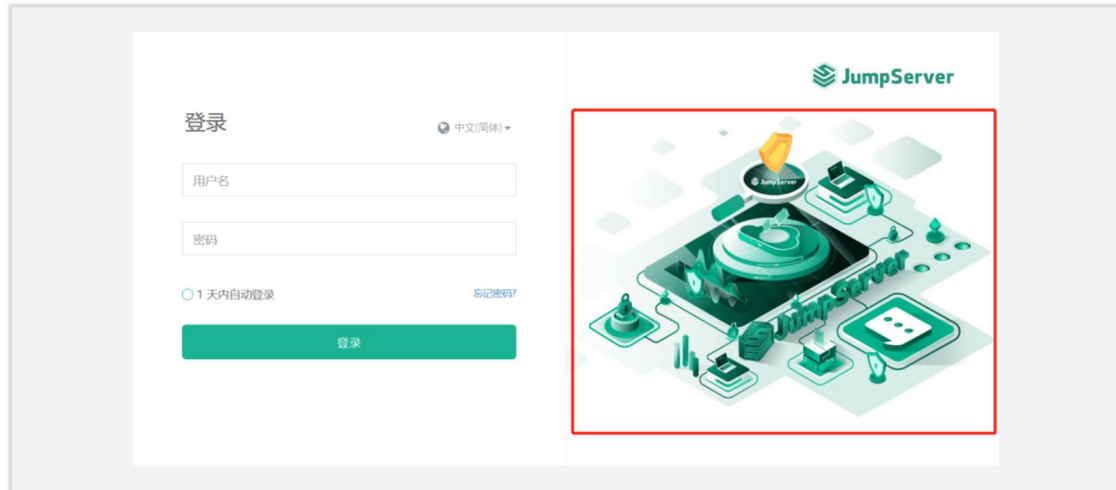


网站图标选项调整后会显示在浏览器页签左侧的小图标，如下图所示：



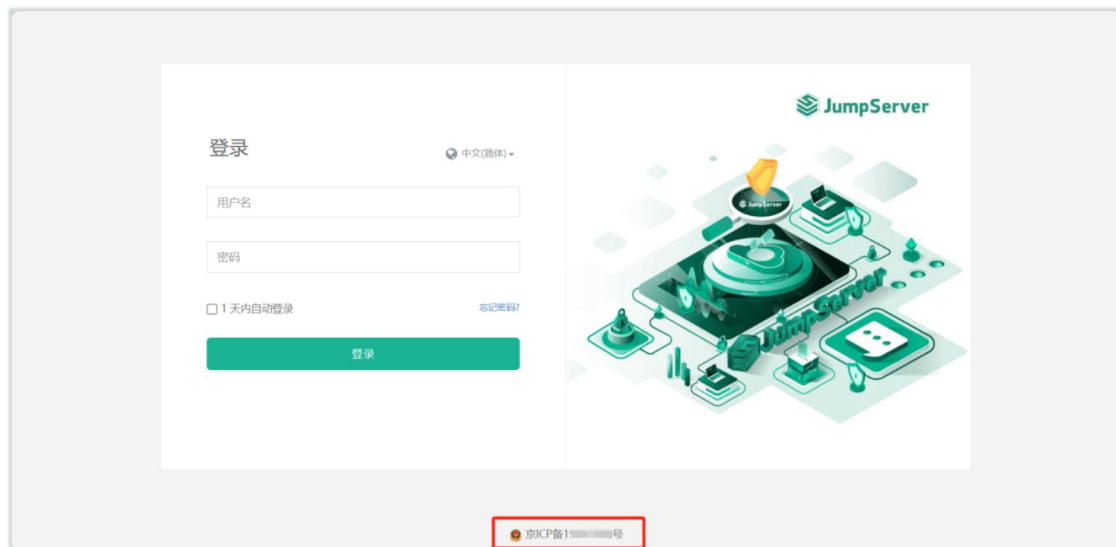
4.11.3. 图片

登录页面图片调整后显示页面位于登录输入框的右侧，如下所示：



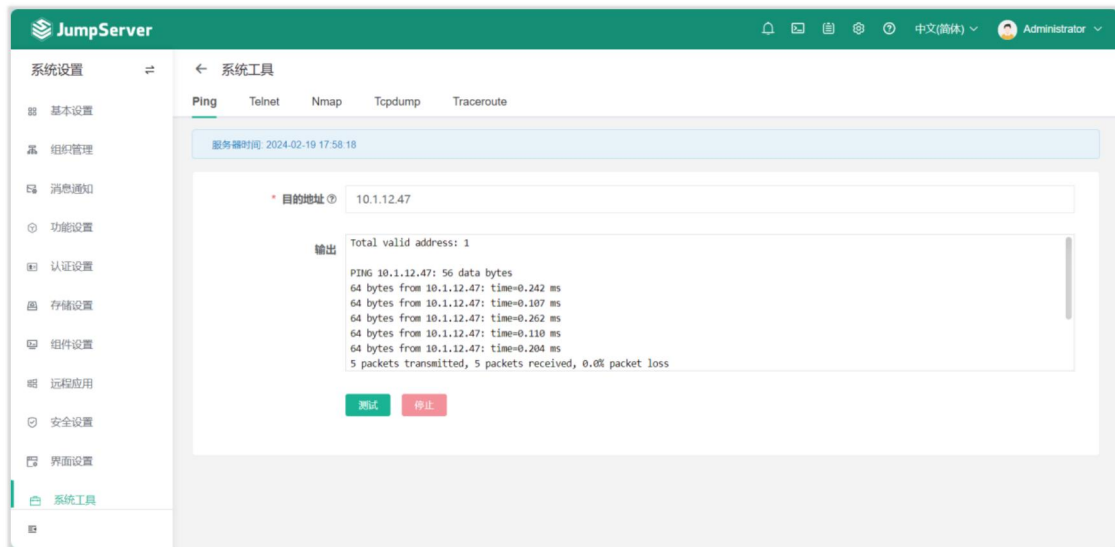
4.11.4. 备案

备案信息调整后显示页面位于登录页面下侧，如下所示：



4.12. 系统工具

点击页面左侧的[<系统工具>](#)按钮，进入系统工具页面。该页面中包含了系统工具 ping、telnet、Nmap、Tcpdump，Traceroute。方便用户检测资产与 JumpServer 服务之间的网络连接情况。



4.13. 系统任务

点击页面左侧的[系统任务](#)按钮，进入系统任务查看页面。

4.13.1. 任务列表

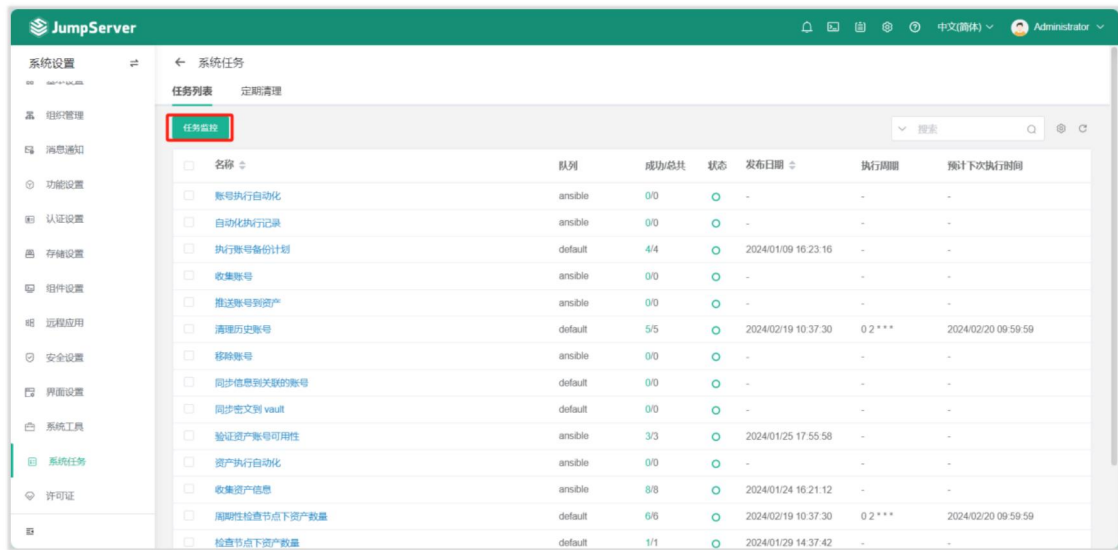
JumpServer 支持使用 Ansible 等技术实现自动化执行任务，系统任务页面可查看任务执行的日志信息以及执行自动化任务的组件 Celery 的状态与已执行任务的历史记录等。

The screenshot shows the JumpServer 'System Tasks' (系统任务) interface. The 'Task List' (任务列表) tab is selected. The table displays a list of tasks with the following columns: Name (名称), Queue (队列), Success Count (成功总), Status (状态), Publish Date (发布日期), Execution Period (执行周期), and Next Execution Time (预计下次执行时间). The tasks include various automation tasks like account backup, asset collection, and asset verification.

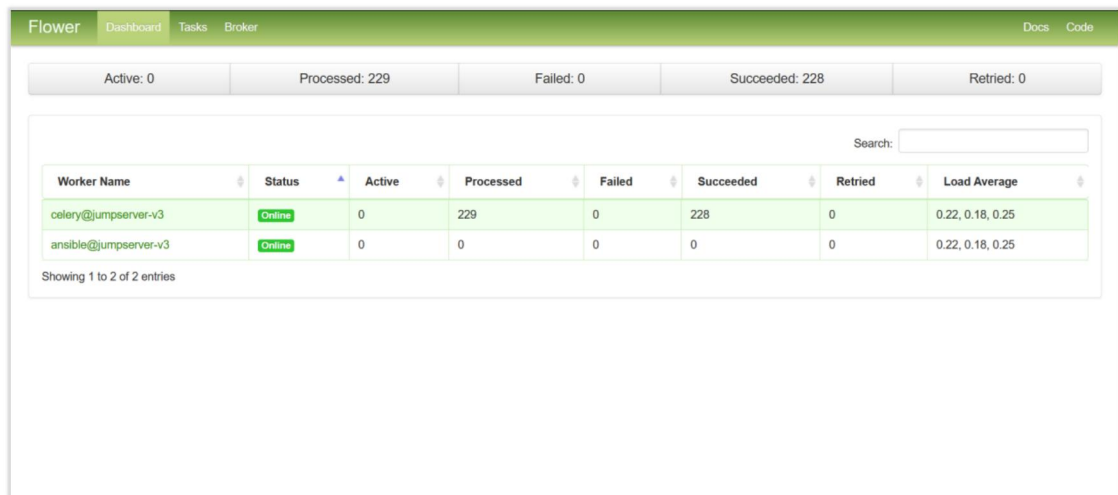
名称	队列	成功总	状态	发布日期	执行周期	预计下次执行时间
账号执行自动化	ansible	0/0	○	-	-	-
自动化执行记录	ansible	0/0	○	-	-	-
执行账号备份计划	default	4/4	○	2024/01/09 16:23:16	-	-
收集账号	ansible	0/0	○	-	-	-
推送账号到资产	ansible	0/0	○	-	-	-
清理历史账号	default	5/5	○	2024/02/19 10:37:30	0 2 ***	2024/02/20 09:59:59
转移账号	ansible	0/0	○	-	-	-
同步信息到关联的账号	default	0/0	○	-	-	-
同步密文到 vault	default	0/0	○	-	-	-
验证资产账号可用性	ansible	3/3	○	2024/01/25 17:55:58	-	-
资产执行自动化	ansible	0/0	○	-	-	-
收集资产信息	ansible	8/8	○	2024/01/24 16:21:12	-	-
周期性检查节点下资产数量	default	6/6	○	2024/02/19 10:37:30	0 2 ***	2024/02/20 09:59:59
检查节点下资产数量	default	1/1	○	2024/01/29 14:37:42	-	-

该页面可查看所有自动化任务，其中包含账号备份计划，推送账号，检查资产连接性、邮件发送自动化任务等。点击自动化任务名称即可进入该自动化任务的详情页面，在该自动化任务的详情页面可查看任务详情信息，执行历史等信息。

点击页面左上角的[任务监控](#)按钮，可查看 JumpServer 后端批量任务组件的相关状态。

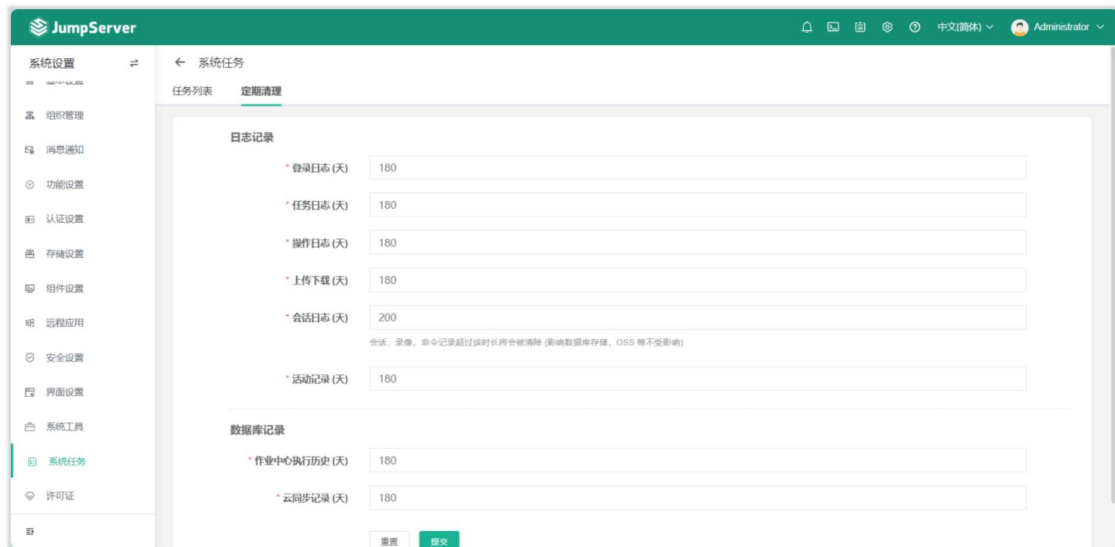


点击页面上部分的任务状态可查看成功任务的日志或失败任务的日志，查看后端 celery 组件与 ansible 服务的相关信息。



4.13.2. 定期清理

点击[定期清理](#)按钮，进入定期清理设置页面，配置登录、任务、操作、上传下载日志和数据库记录等审计任务的定时清理周期，为服务器存储减轻压力。该页面的配置主要控制本地保存的记录，当录像与日志存储到外部存储中，不受该页面配置影响。



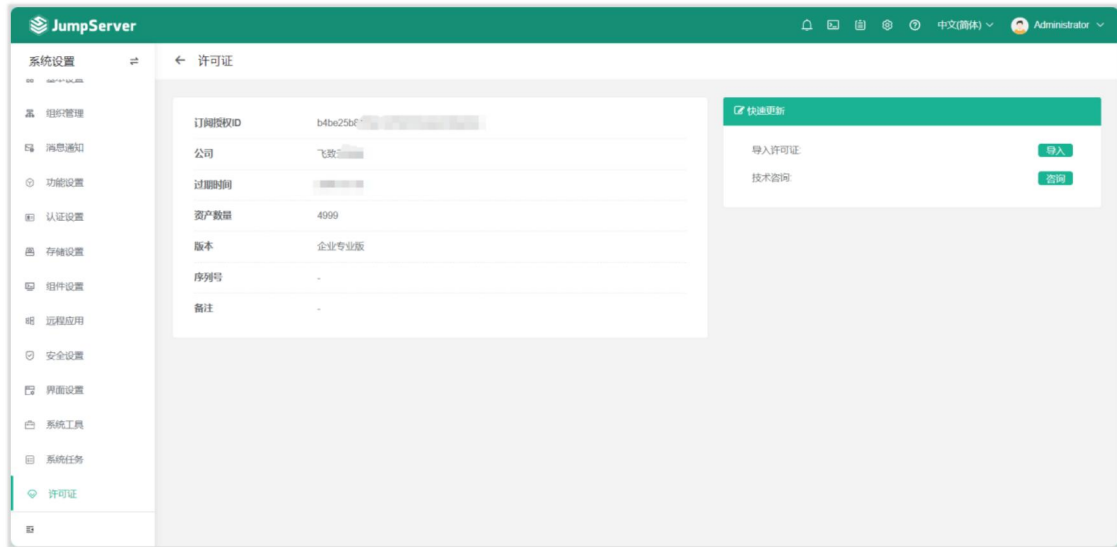
详细参数说明：

参数	说明
登录日志	登录日志主要记录 JumpServer 用户的登录信息，包括用户名、类型、Agent、登录 IP 地址、登录地点以及登录日期。
任务日志	任务日志主要记录一些批量命令等自动化的任务信息。
操作日志	操作日志主要记录用户对资产的操作动作、操作时间以及操作的资源类型和远端地址。
上传下载	上传下载主要记录用户进行 FTP 上传、下载时所留下的操作记录。
会话日志保存时间	会话日志主要记录通过 JumpServer 登录资产产生的会话日志包含录像与命令记录。
活动记录	活动记录主要记录资产、授权、账号或任务详情页的操作信息。
作业中心执行历史	作业中心主要记录作业中心的任务执行的历史信息，包括快捷命令与作业。
云同步记录	云同步记录主要记录执行云同步任务的信息。

4.14. 许可证

点击页面左侧的[许可证](#)按钮，进入许可证页面。该页面可以导入飞致云企业 License 使用企业版功能，可以查看资产授权数量以及 JumpServer 企业版 License 过期时间。

注：非企业版安装包，不能导入 License。

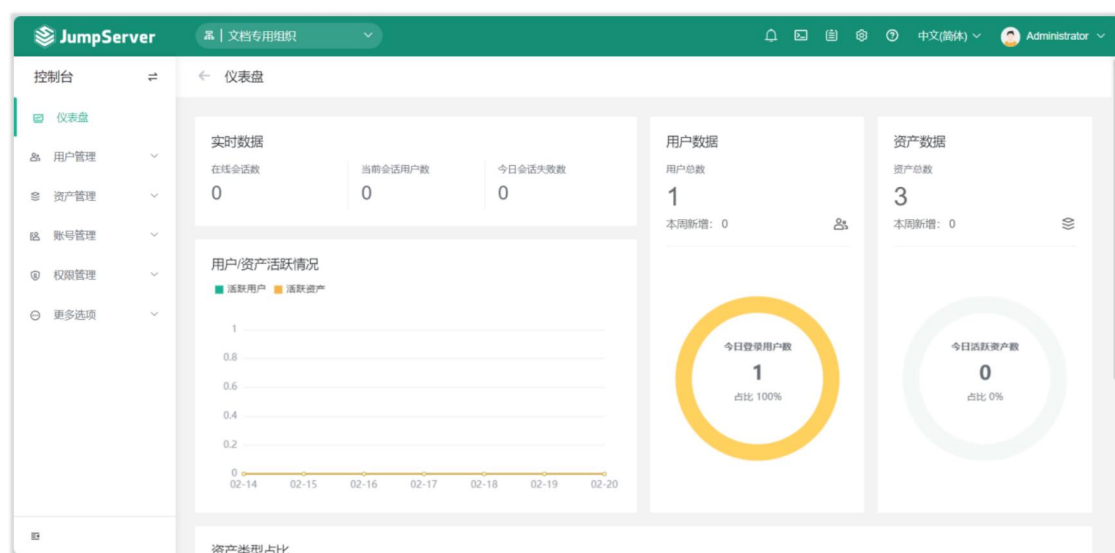


5. 控制台

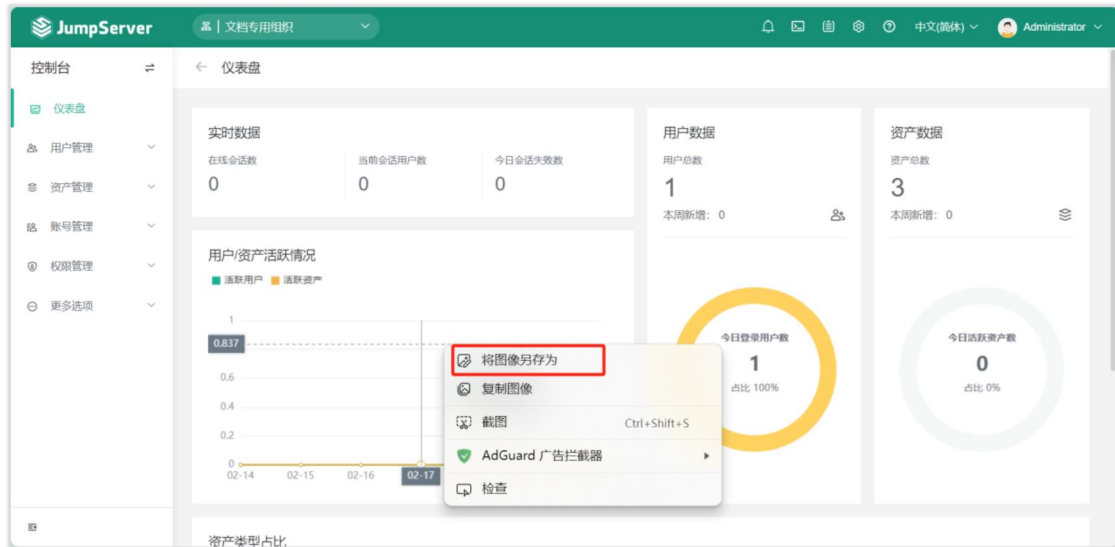
控制台页面是管理员的操作入口，通过控制台，管理员可以进行用户管理、资产管理、账号管理、权限管理、任务中心等配置。

5.1. 仪表盘

JumpServer 的仪表盘页面，主要展示用户与资产以及登录会话情况的概览数据，系统管理员可切换到各个组织下，看到该组织的用户总数、资产总数、在线用户、在线会话等。组织管理员只能看到某个组织的概览数据。JumpServer 系统内置全局组织，系统管理员通过全局组织下可看到整个 JumpServer 平台的综合数据。JumpServer 控制台仪表盘页面如下：

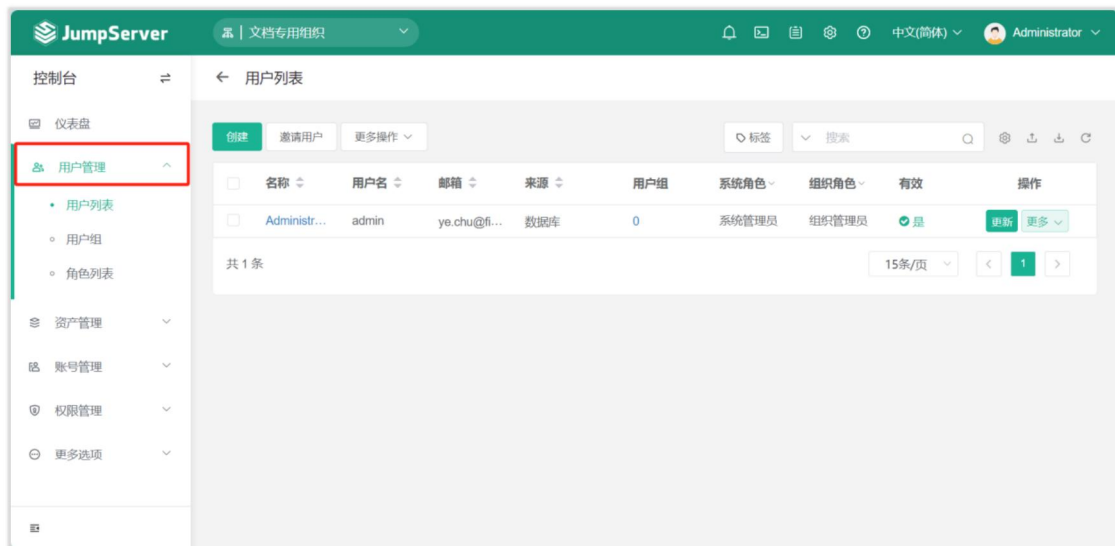


JumpServer 支持将仪表盘页面的图像（用户/资产活跃情况、用户数据库图、资产数据图、资产类型占比）导出为图片，方便保存，在该页面中空白处鼠标右击，选择[<将图片另存为>](#)按钮。



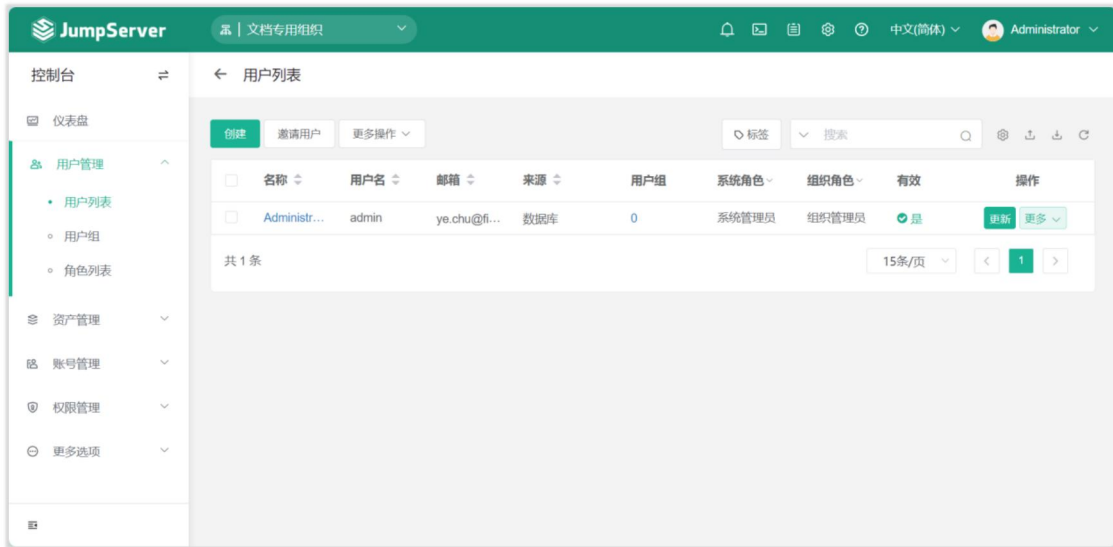
5.2. 用户管理

点击控制台页面左侧的[用户管理](#)按钮，即可打开下拉框选择进入用户管理页面。用户管理页面主要针对于 JumpServer 的登录用户的管理，包括 JumpServer 的用户列表、JumpServer 的用户组以及 JumpServer 的角色列表。



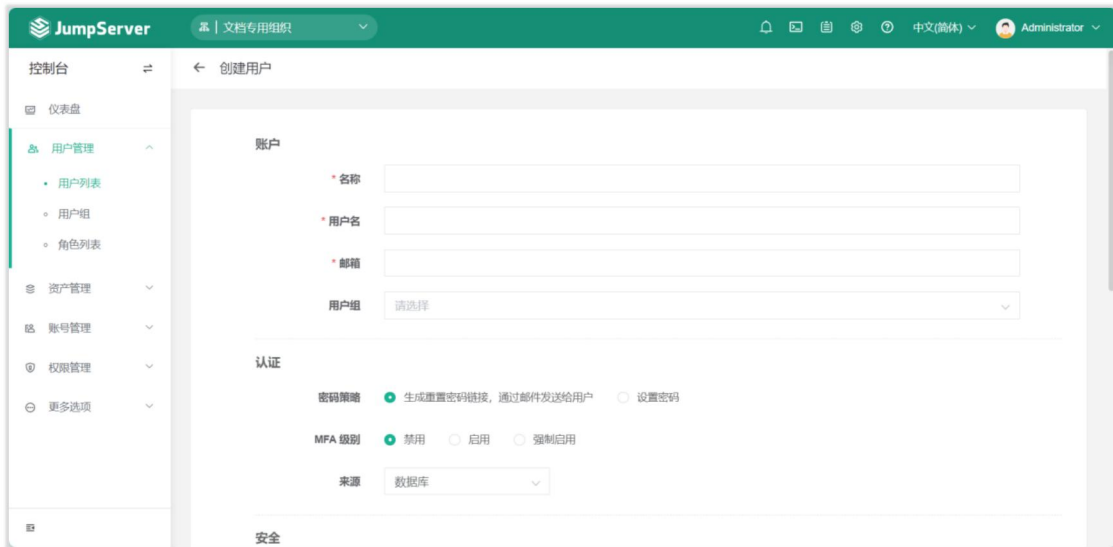
5.2.1. 用户列表

点击[用户列表](#)按钮，进入用户列表界面。该页面主要负责 JumpServer 用户的操作，包含增加、删除、更新、查看等。



5.2.1.1. 创建用户

点击“用户列表”页面的[创建](#)按钮，进入用户详细创建页面。



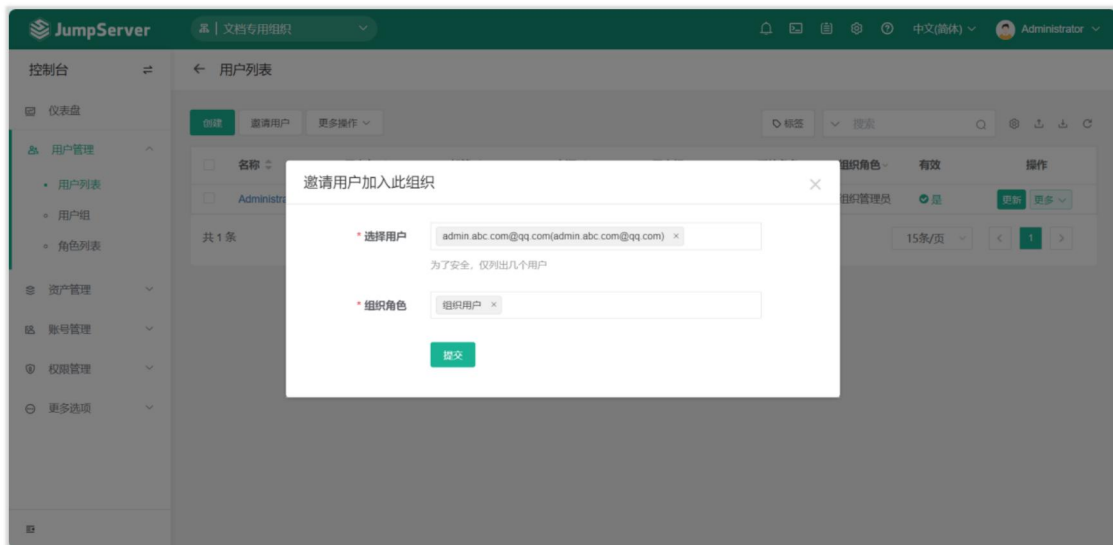
详细参数说明：

参数	说明
名称	用户识别名称，可重复。
用户名	登录 JumpServer 的登录账号，不可重复。
邮箱	登录账号对应的邮箱地址，不可重复。
用户组	将用户按组进行管理，主要用于资产授权，当某个资产对某个用户组授权时，这个用户组所有的用户都对这个资产有相应的权限。

密码策略	密码在管理员创建用户的过程中可以自主设置；也可以生成密码连接，通过邮件发送给用户。在成功提交用户信息后，JumpServer 会发送一条“设置用户密码”的邮件到所填写的用户邮箱。
MFA	多因子身份认证。启用 MFA 后，用户登录 JumpServer 系统时，系统将要求输入用户名和密码（第一安全要素），然后要求输入来自其 MFA 设备的动态验证码（第二安全要素），双因子的安全认证将为账户提供更高的安全保护。
来源	指定该用户的来源，如手动创建则为“数据库”，如从 LDAP 中导入则为“LDAP”。
系统角色	系统角色是决定一个用户在系统层面具有哪些权限（系统管理员、审计员、用户/其他自定义角色）。
组织角色	组织角色是决定一个用户在组织层面具有哪些权限（组织管理员、审计员、用户/其他自定义角色）。
激活	表示用户状态是否正常可登录，非激活状态用户不可登录。
失效日期	失效日期指用户可进行登录的最后日期，时间截至后不可登录。
手机	非必填项，配置用户的手机号，用于“MFA”手机短信的接收。
微信	非必填项，配置用户的企业微信，用于“企业微信”方式的认证登录。
备注	非必填项，管理员配置该用户的备注信息。

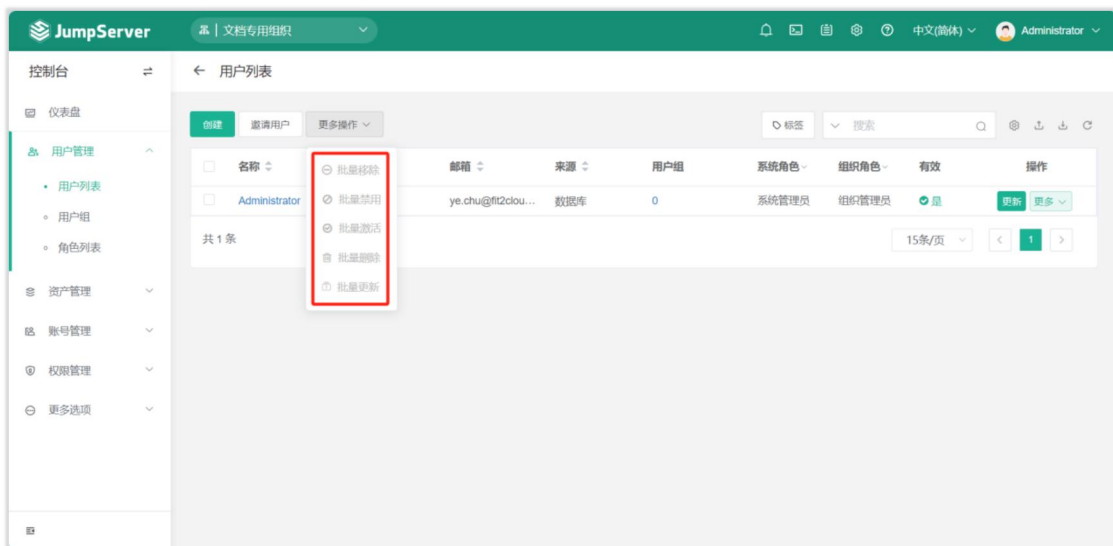
5.2.1.2. 邀请用户

点击“用户详情”页面的[邀请用户](#)按钮，使用邀请用户功能。该功能主要用于某个 JumpServer 用户已经存在于 JumpServer 系统中，但不存在于当前组织中时，邀请该用户加入到当前组织中。点击[邀请用户](#)按钮后，在弹窗中输入需要邀请的用户并设置该用户当前组织中的组织角色，点击[提交](#)按钮保存。



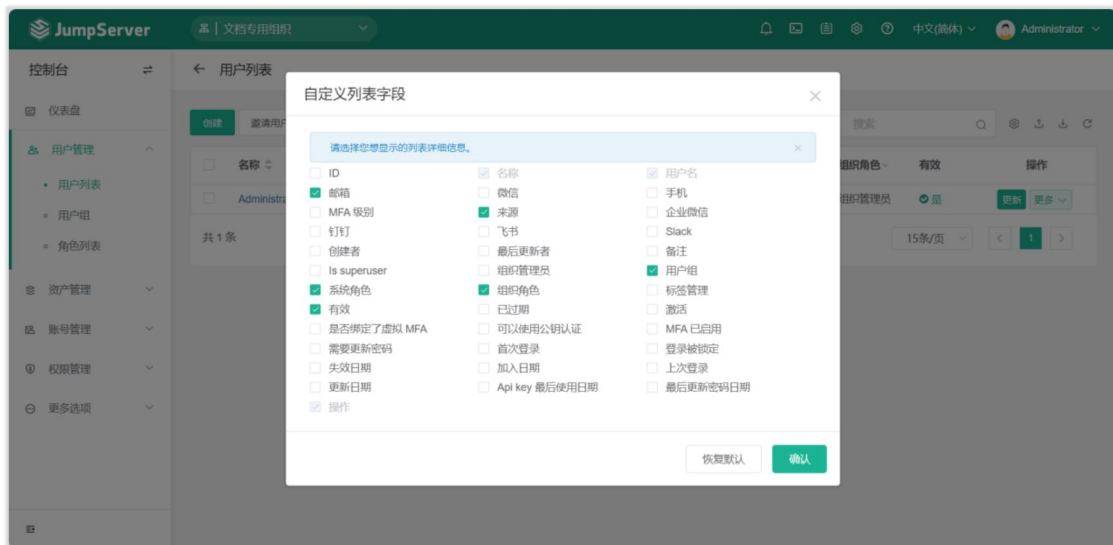
5.2.1.3. 批量操作

[<更多操作>](#)按钮主要针对于用户的批量操作，主要包括移除所选用户、禁用所选用户、激活所选用户、删除所选用户、以及更改所选用户。点击用户详情前端的“复选框”，即可进行批量操作。



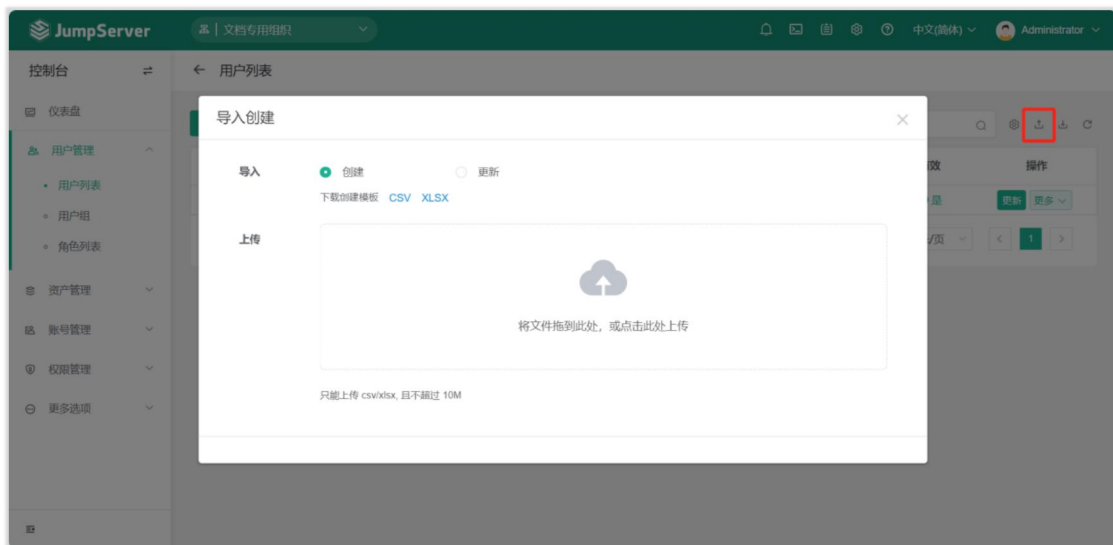
5.2.1.4. 显示设置

点击“用户列表”页面右上角的[<齿轮>](#)按钮，可进行页面显示的设置，可更详细的展示用户相关信息，例如：用户上次登录的时间、失效日期、创建日期等等。



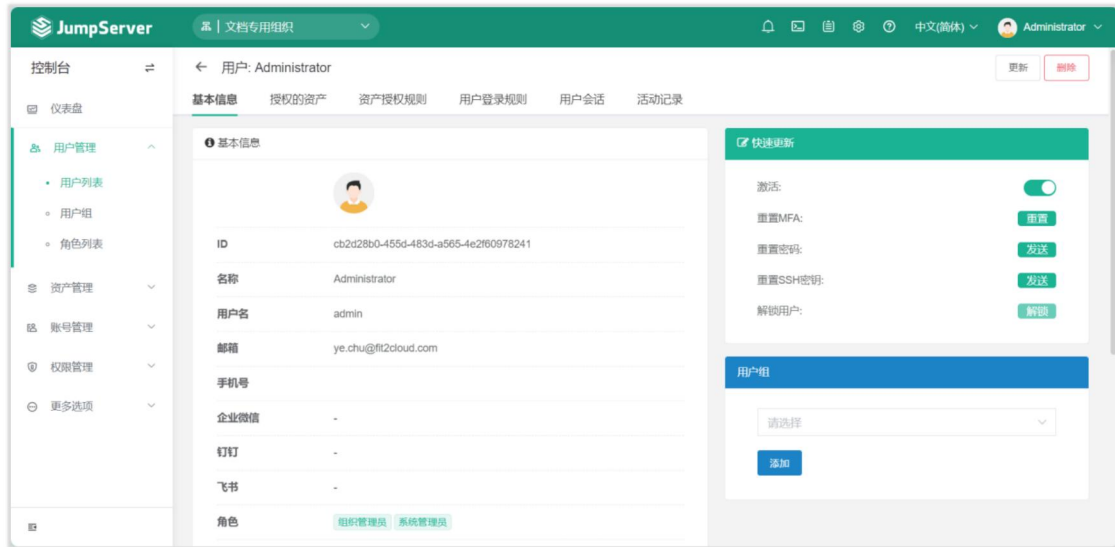
5.2.1.5. 用户导入导出

用户支持导入创建、更新和将已存在用户信息导出，支持的表格方式有 **xlsx**、**csvs**。首次导入，可点击[<导入>](#)按钮下载模板后根据提示填写信息后导入。



5.2.1.6. 用户详情

在“用户列表”页面点击[<用户名称>](#)按钮，进入用户详情页面。用户详情页包含的信息包括基本信息、授权的资产、资产授权规则、用户授权规则以及活动记录。



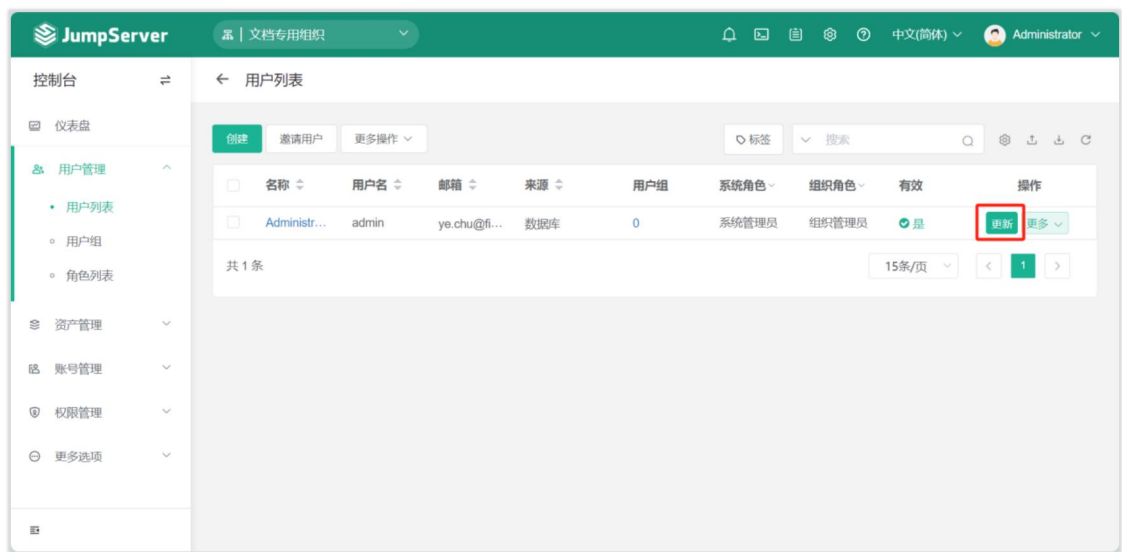
详细参数说明：

参数	说明
基本信息	基本信息页面显示该用户的详细信息，包括 ID、名称、用户名、邮件、角色、创建者等信息。
授权的资产	显示出当前组织下授权给该用户的资产列表。
资产授权规则	显示出包含该用户的资产授权规则列表。
用户登录规则	该用户的登录策略配置详情。可通过配置登录规则限制某用户只允许在某个时间段或使用某个 IP 登录等。
用户会话	显示当前组织下该用户正在操作的会话信息。
活动记录	该用户的登录记录与操作记录。
激活	快速操作按钮，允许或禁止该用户进行登录。
重置 MFA	快速操作按钮，还原用户的 MFA 到初始状态，用户下次登录需要再次进行绑定操作。
重置密码	快速操作按钮，向该用户的邮箱发送重置密码的邮件。
重置 SSH 密钥	快速操作按钮，向该用户的邮箱发送重置用户的 SSH Key 的邮件。
解锁用户	快速操作按钮，如该用户因为密码多次输入错误导致账号锁定，可通过此按钮进行解锁。
用户组	快速操作按钮，可在输入框中选择某个用户组进行加入或点击已加入用户组列表右侧删除按钮进行删除。

点击用户详情页面的[<用户登录规则>](#)按钮，跳转至“权限管理”模块设置“用户登录”规则。

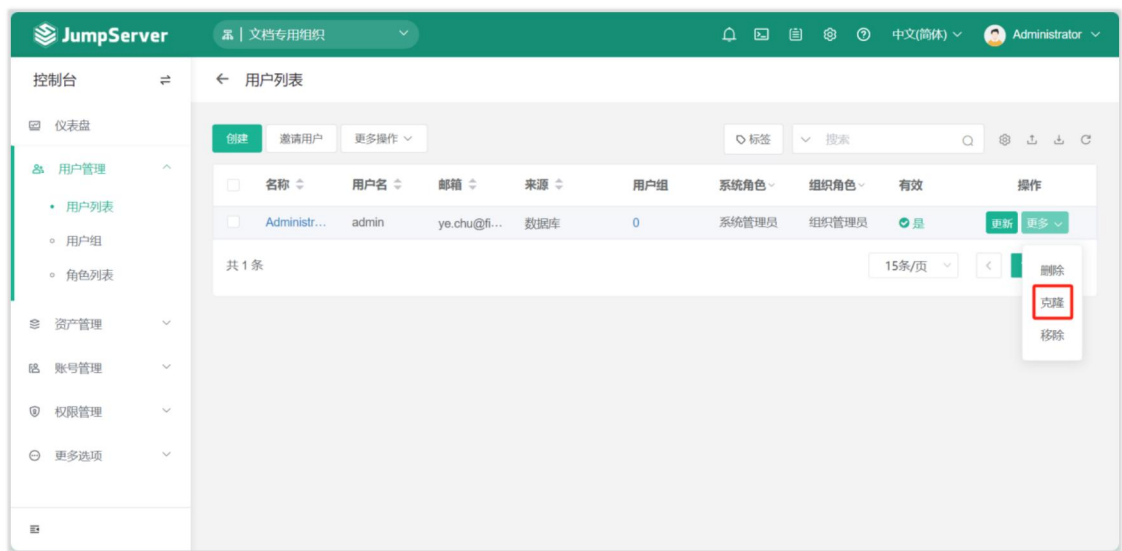
5.2.1.7. 用户信息更新

当需要对某个用户的信息进行更新时，可点击“用户列表”页面用户后方的[<更新>](#)按钮进行用户信息更新，详细参数说明可参考创建用户详细说明。



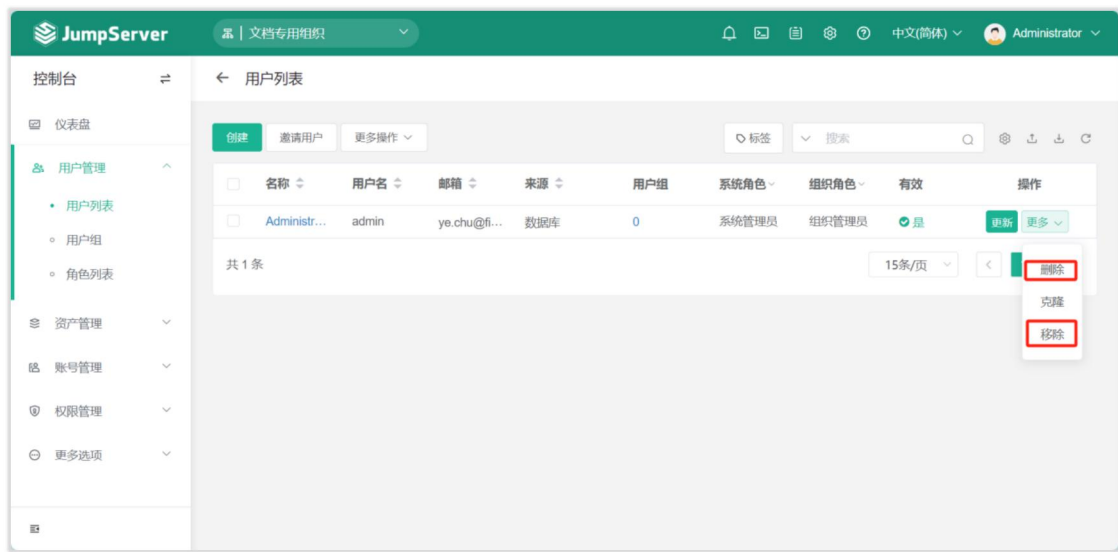
5.2.1.8. 用户克隆

针对于用户信息相同，或大部分相同的情况，可以点击用户后方的[<更多>](#)按钮，选择[<克隆>](#)按钮，进入用户信息更改界面，修改相关信息后，提交即可。



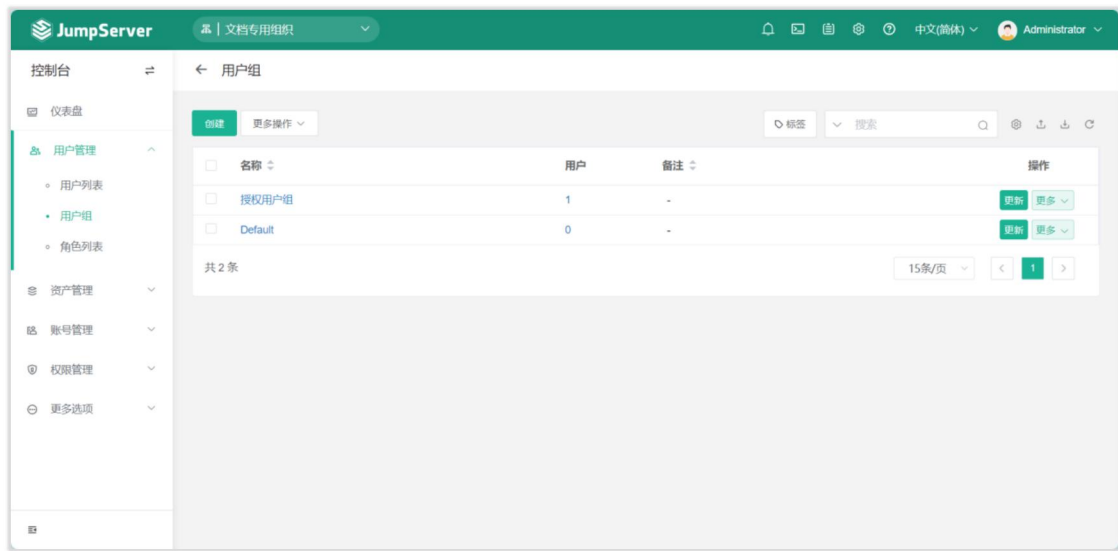
5.2.1.9. 用户删除/移除

当需要将用户从当前组织中移除，点击用户后方的<更多>按钮，选择<移除>按钮（此操作可通过邀请用户重新将用户加入到当前组织中）；当需要将用户从整个 JumpServer 系统中删除，点击用户后方的<更多>按钮，选择<删除>按钮（该操作将在数据库层面删除此用户数据，操作结果不可逆）。



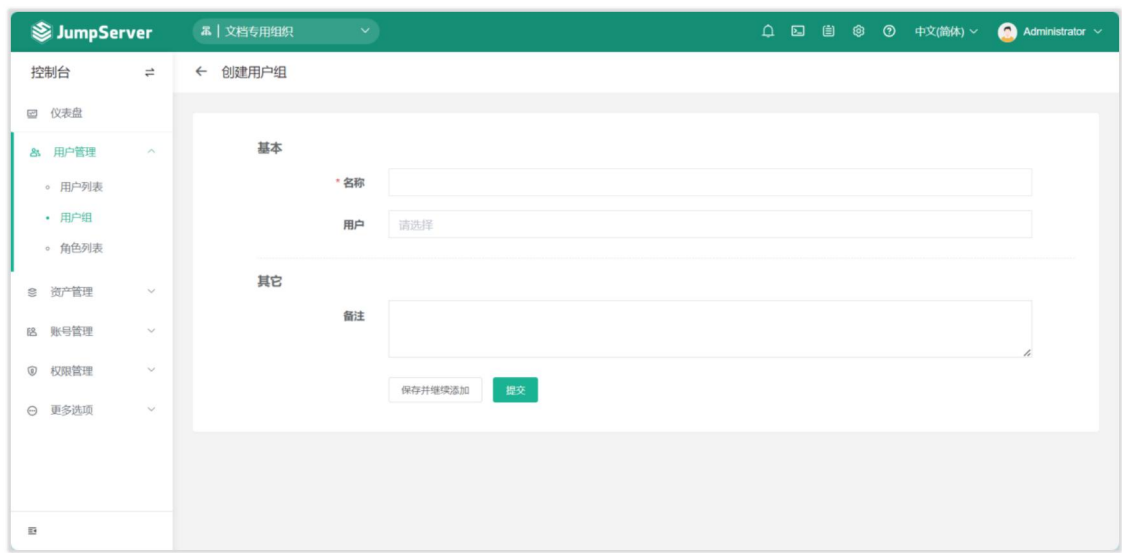
5.2.2. 用户组

点击控制台页面左侧的<用户组>按钮，即可进入用户组页面。该页面主要针对用户组，包括用户组的创建、删除、更新、查看。用户组是对用户进行分组管理。在分配资产权限的时候，可针对用户组进行授权，一个用户支持加入多个用户组。



5.2.2.1. 创建用户组

点击“用户组”页面的<创建>按钮，进入用户组的创建页面。填写用户组的相关信息，点击<提交>按钮后创建用户组完成。

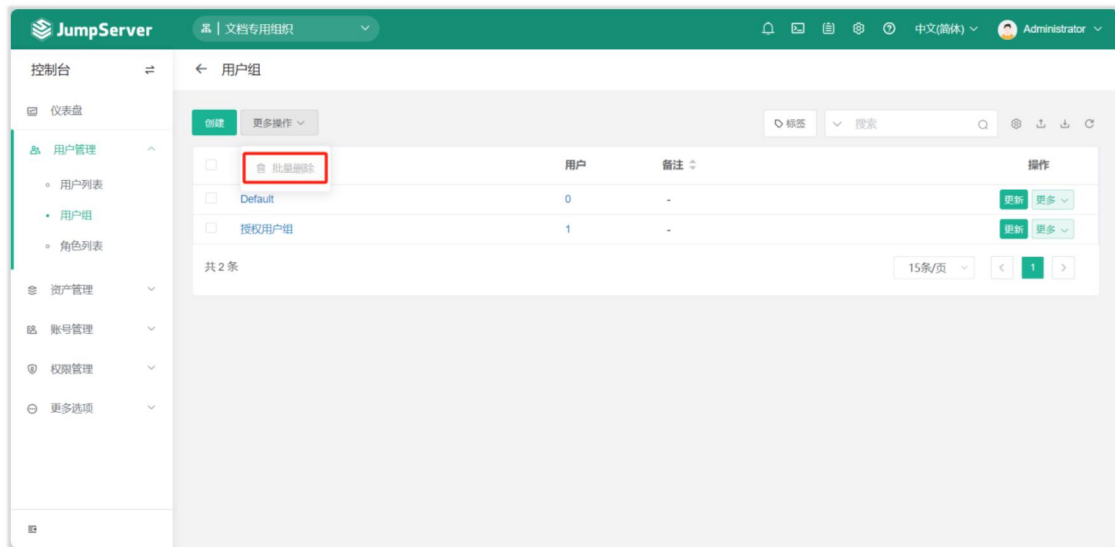


详细参数说明：

参数	说明
名称	用户组名称。
用户	将用户添加到该用户组中。

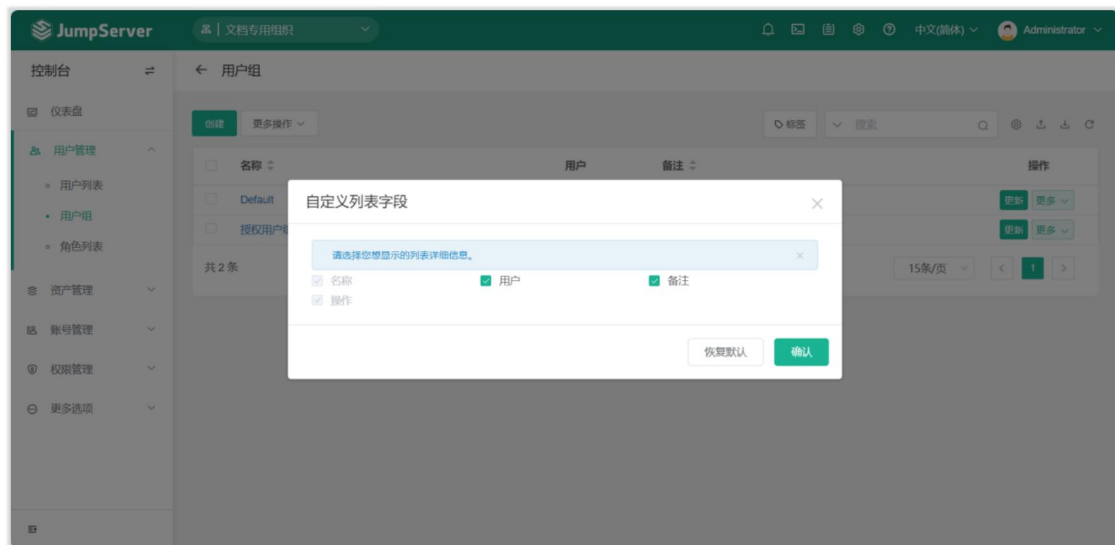
5.2.2.2. 批量操作用户组

<更多操作>按钮针对于批量删除用户组的场景。当需求批量删除用户组时，选择用户组前方的复选框，点击<更多操作>按钮，选择<删除所选>的按钮操作批量删除用户组。



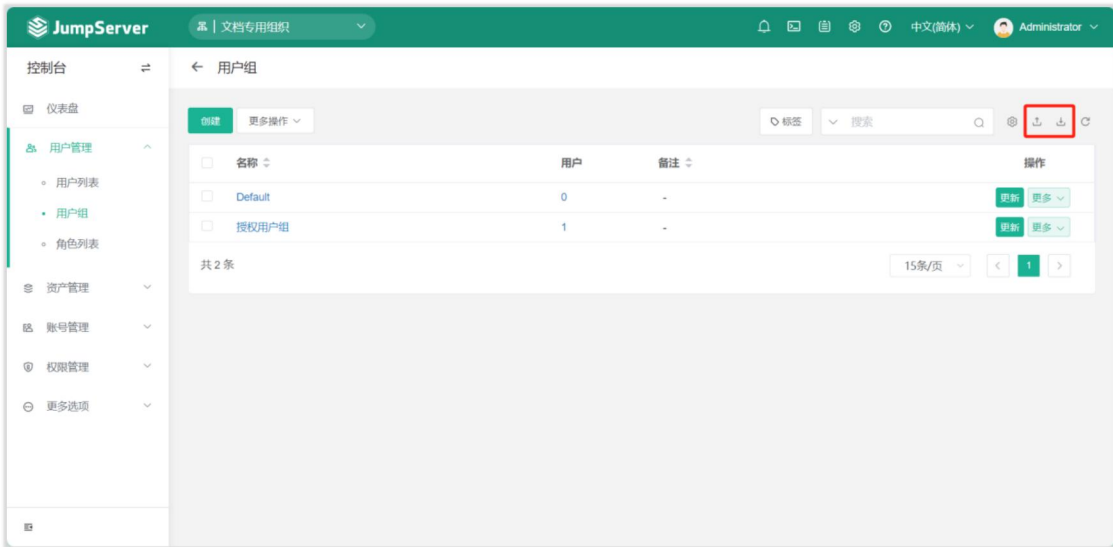
5.2.2.3. 显示设置

点击“用户组”列表页右上角的^{<齿轮>}按钮，可进行页面显示的设置，可更详细的展示用户组相关信息，例如：用户组包含的用户数等等。



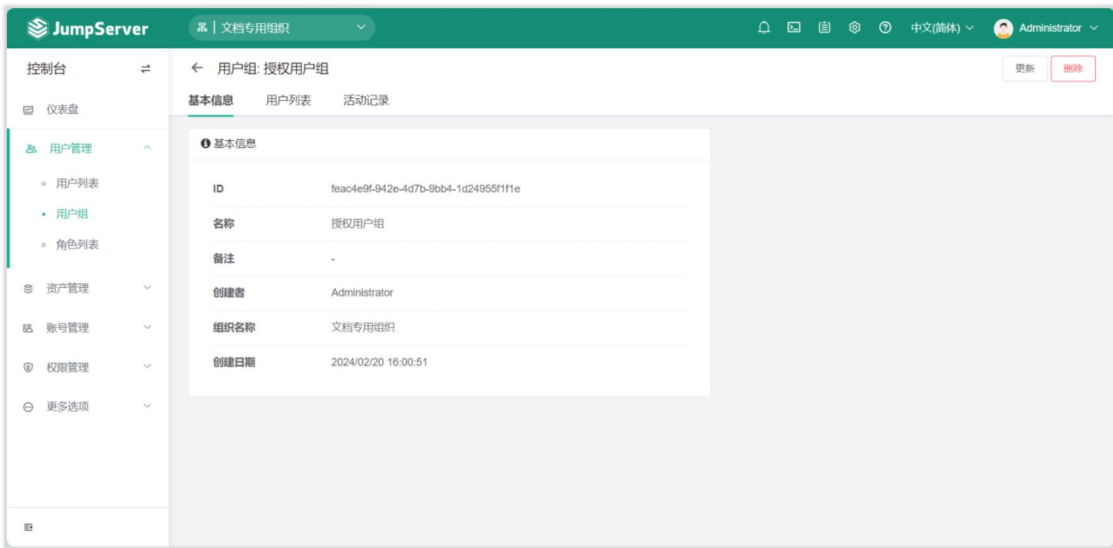
5.2.2.4. 用户组导入导出

用户组支持导入创建用户组和将已存在用户组导出，支持的表格方式有 **xlsx**、**cvs**。首次导入，可点击^{<导入>}按钮下载模板后根据提示填写信息后导入。



5.2.2.5. 用户组详情页

在“用户组”列表页面点击[<用户组名称>](#)，进入用户组详情页面。用户组详情页包含的信息包括用户组的基本信息、用户列表以及活动记录。



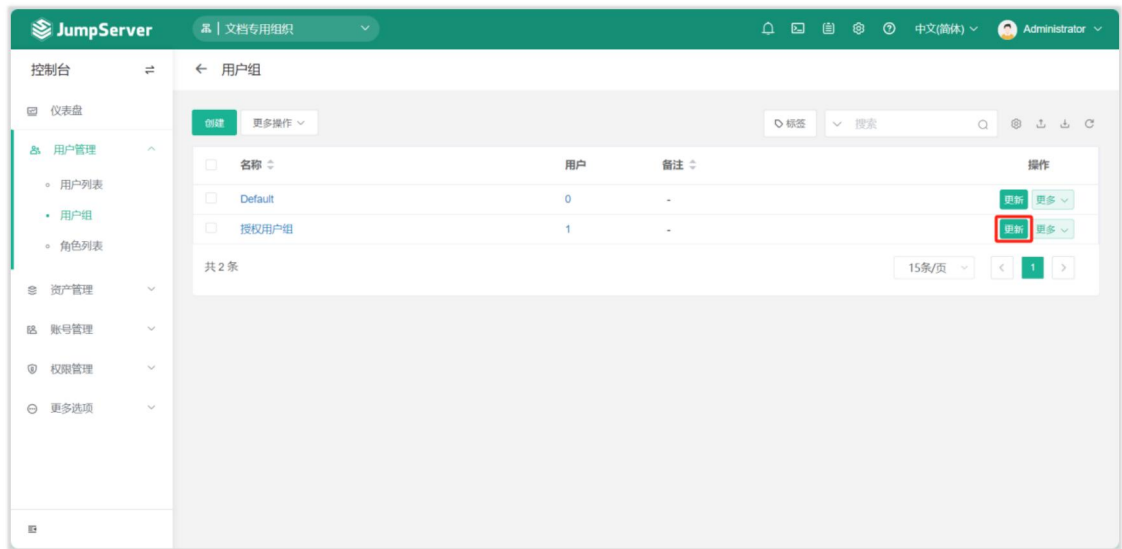
详细参数说明如下：

参数	说明
基本信息	基本信息页面显示该用户组的详细信息，包括 ID、名称、用户数量、创建者等信息。
用户列表	用户列表页面显示哪些用户属于该用户组。该页面可以删除某个用户，可以快捷的将全部成员添加到该用户组中，可以选择性的

	添加用户到该用户组中。
活动记录	该选项记录该用户组的活动记录，创建时间、创建人等等信息。

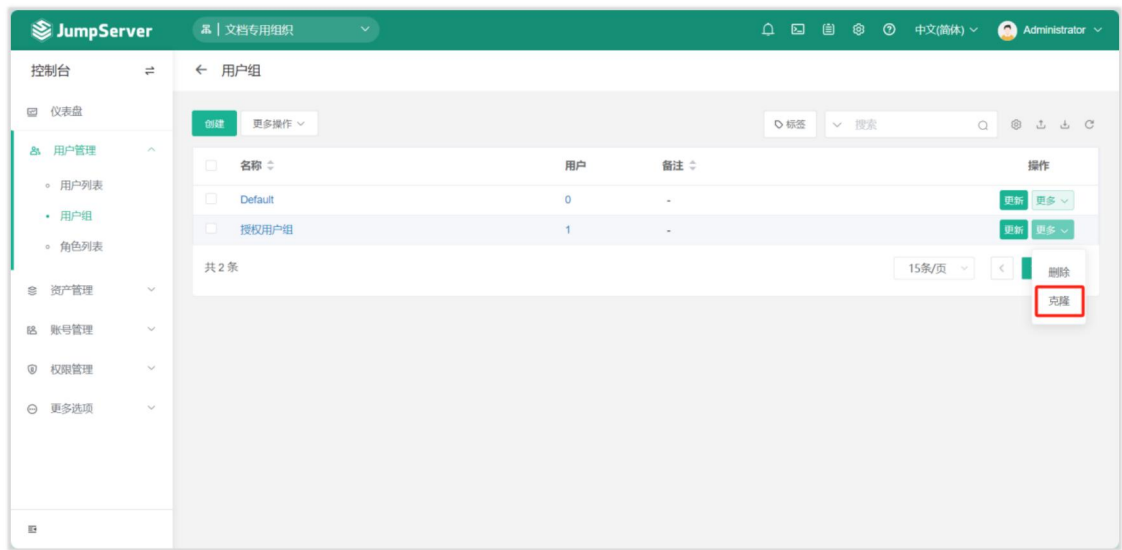
5.2.2.6. 更新用户组

对于用户组的信息变动情况，可以对用户组的信息进行更新。点击对应用户组后方的[更新](#)按钮，进入用户信息页，改动后点击[提交](#)按钮即可。



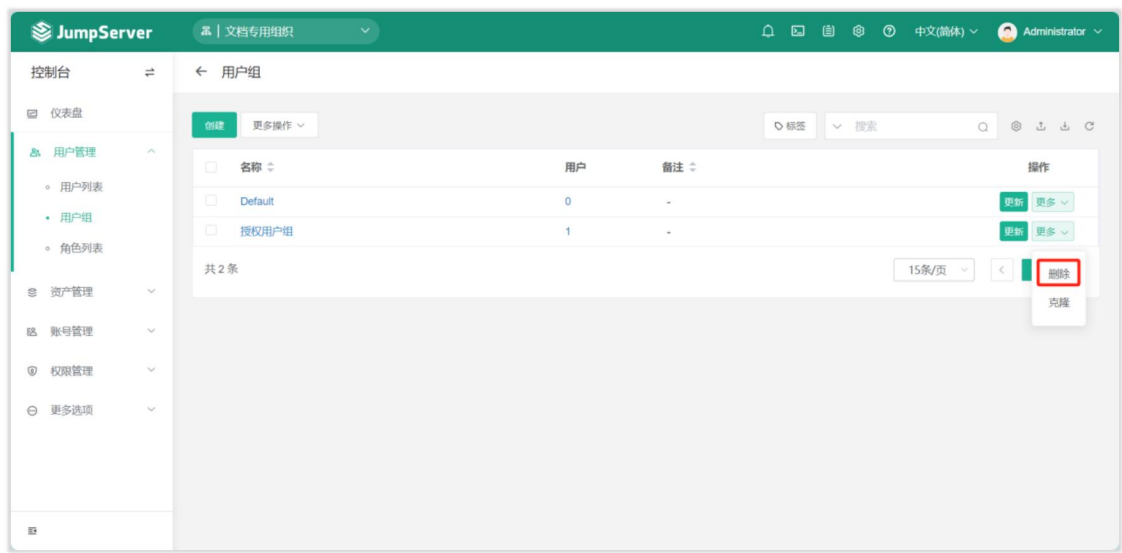
5.2.2.7. 克隆用户组

对于用户组大部分信息相同的情况，可通过克隆功能快速添加，点击用户组后方的[更多](#)按钮，选择[克隆](#)按钮，进入用户组的信息更改界面，修改相关信息后，提交即可。



5.2.2.8. 删除用户组

当需求删除用户组时，可以点击相应的用户组后方的[<更多>](#)按钮，选择[<删除>](#)按钮，点击删除即可。

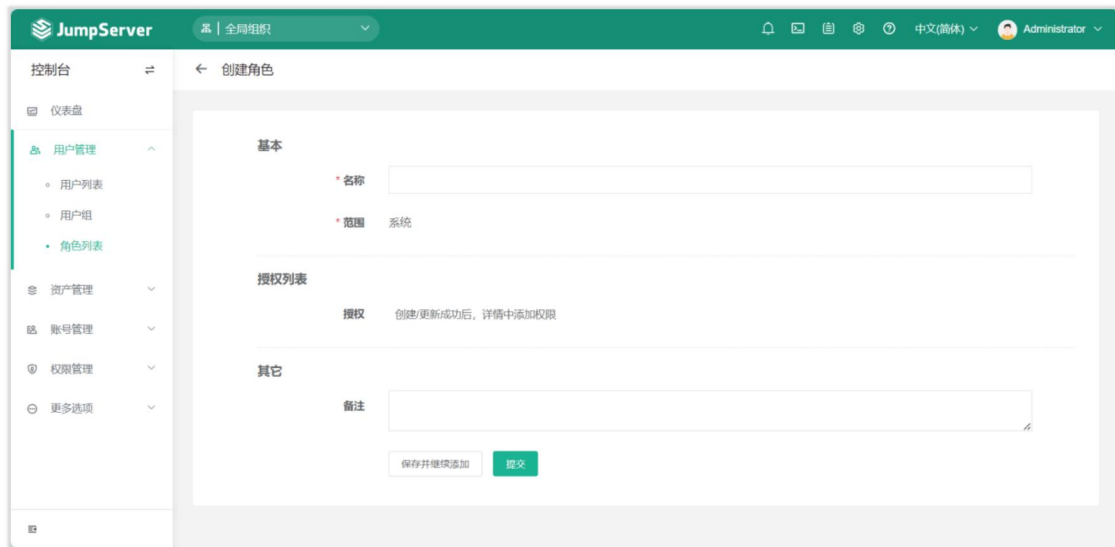


5.2.3. 角色列表

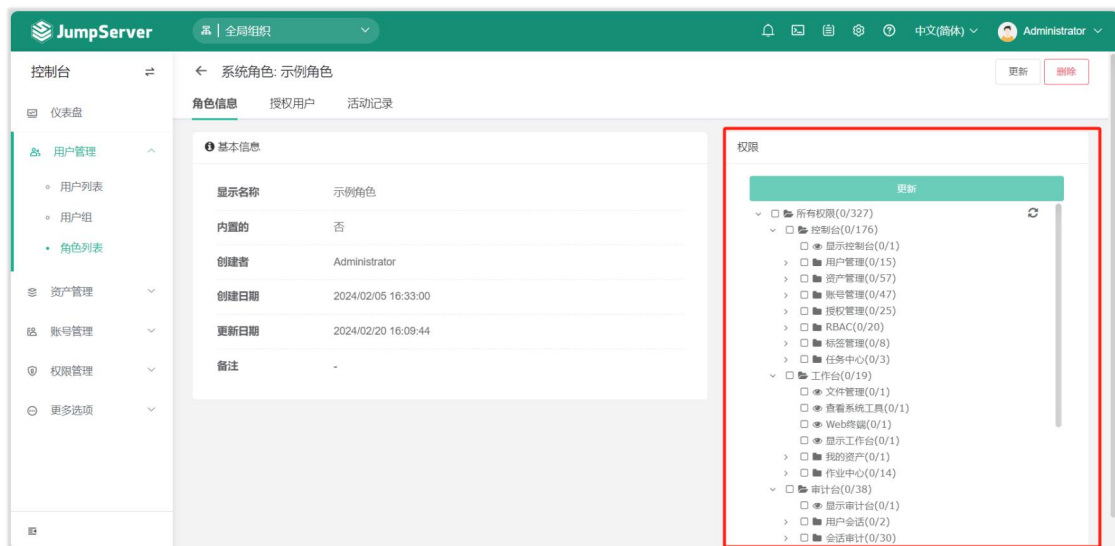
JumpServer 系统中角色可以分为系统角色和组织角色。系统角色默认有系统管理员、系统审计员、用户与系统组件；组织角色默认有组织管理员、组织审计员、组织用户。默认角色都不可以进行删除，更新等操作。

5.2.3.1. 创建角色

系统角色与组织角色均可新建。点击页面左侧上方的[<创建>](#)按钮，进入角色创建页面。

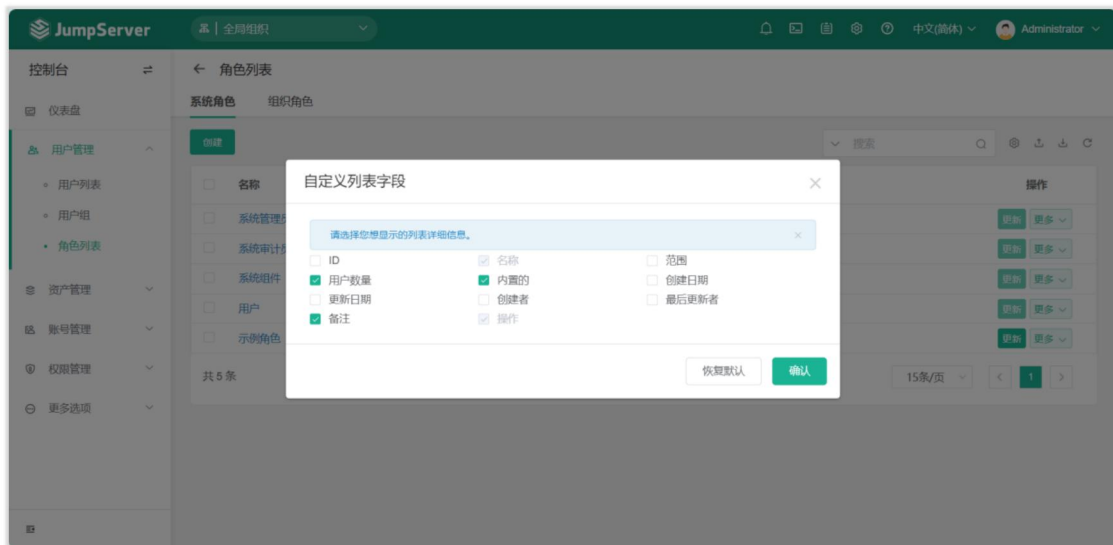


创建角色成功后，进入新创建的角色详情页，可以对该角色进行权限设置。如下图，右边部分为角色的权限设置。根据需求的权限更新设置后，点击[更新](#)按钮提交。



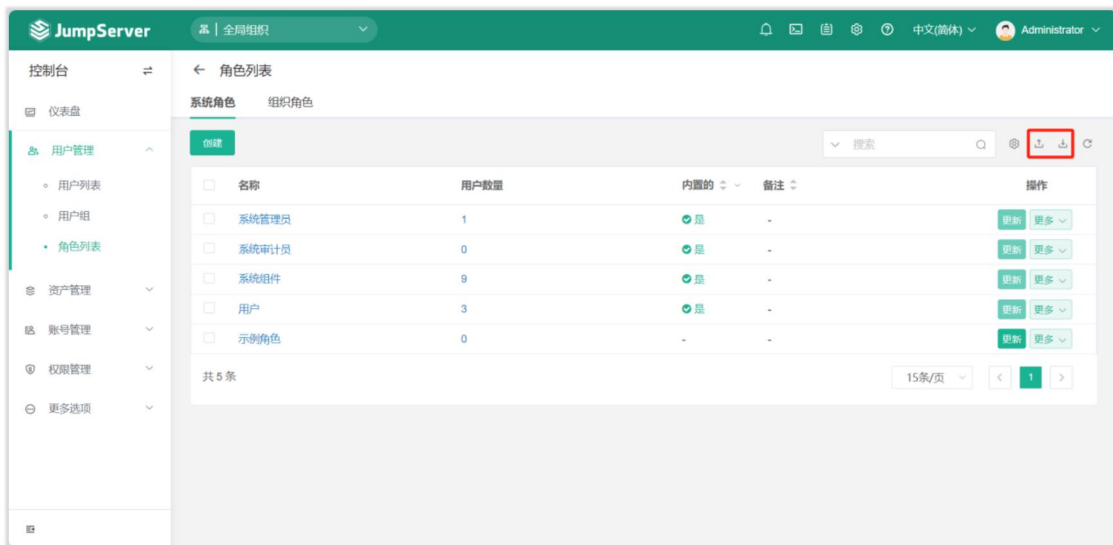
5.2.3.2. 显示设置

点击角色列表页右上角的[<齿轮>](#)按钮，可进行页面显示的设置，可更详细的展示角色相关信息，例如：角色创建者、角色创建日期等等。



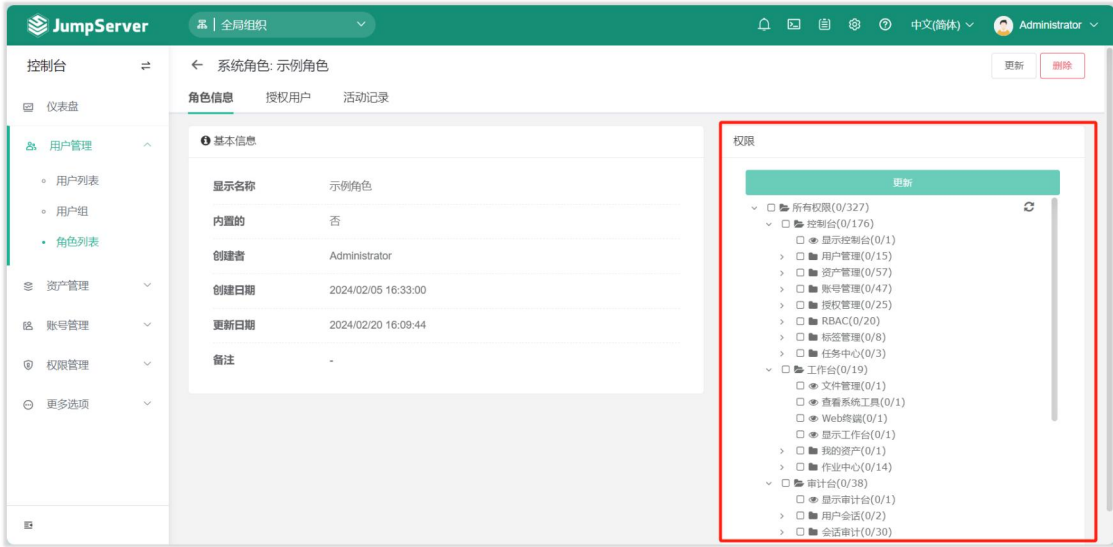
5.2.3.3. 角色导入导出

角色支持导入创建和已存在角色信息导出，支持的表格方式有 **xlsx**、**csvs**。首次导入角色时，点击 [<导入>](#) 按钮下载模板后根据提示填写信息后导入。



5.2.3.4. 角色详情

在角色列表页面点击 [<角色名称>](#)，进入角色详情页面。角色详情页包含的信息包括角色基本信息、角色权限、授权用户以及角色活动记录。

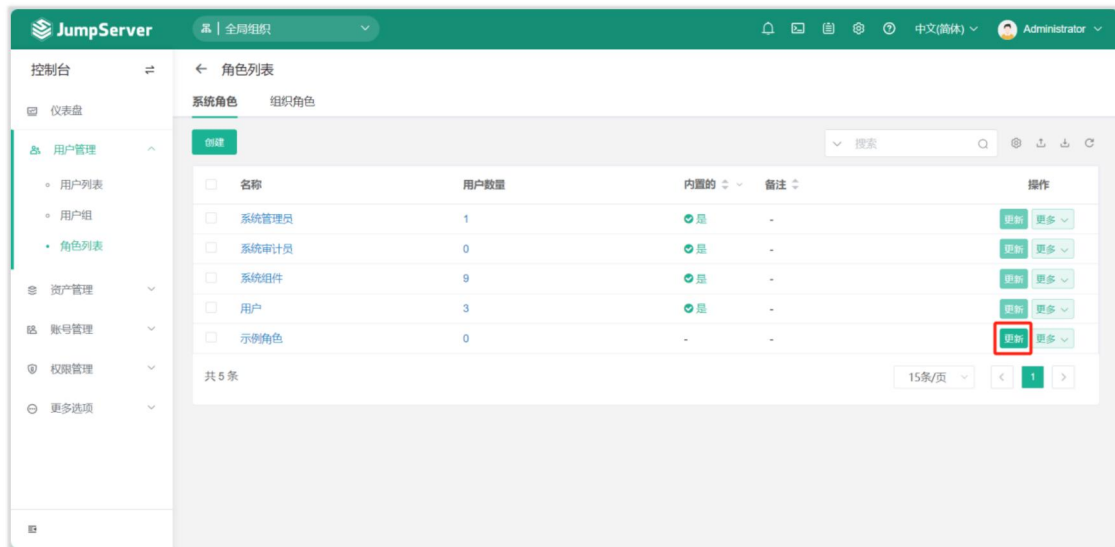


详细参数说明：

参数	说明
基本信息	基本信息页面显示该角色的详细信息，包括名称、是否内置、创建者等信息。
权限	该选项用来设置当前角色的权限，是否可以使用目前这些功能。
授权用户	该页面用来绑定角色与用户，即给某个用户赋该角色的权限。
活动记录	该页面显示当前角色的活动记录。

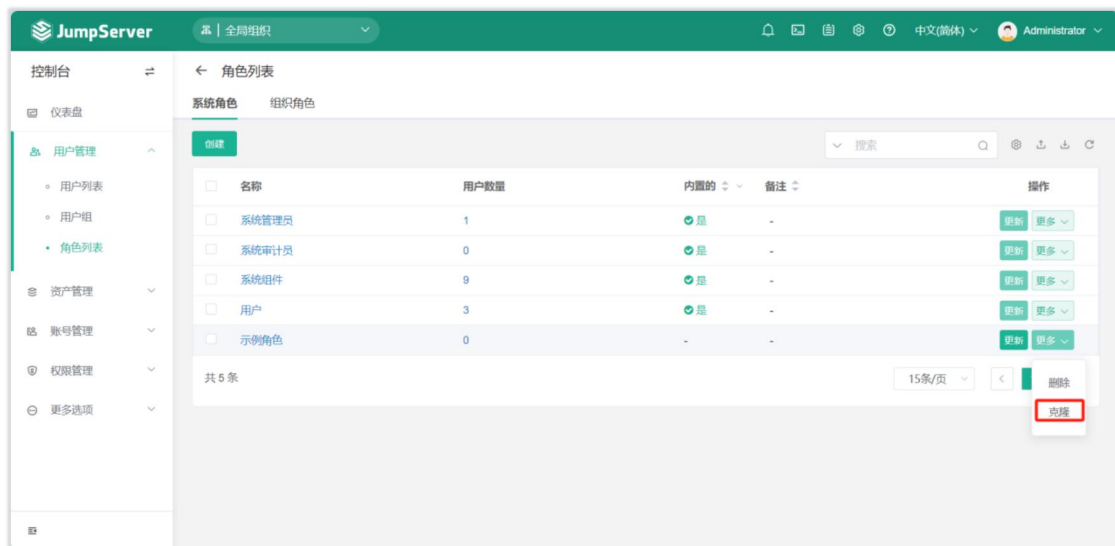
5.2.3.5. 更新角色

角色信息需求进行变动时，可以更新角色相关信息。需求更新角色权限时，点击[角色名称](#)按钮进入角色详情页，在右侧权限模块更新角色的权限。需求更新角色名称等信息时，点击对应角色后方的[更新](#)按钮修改对应信息提交。



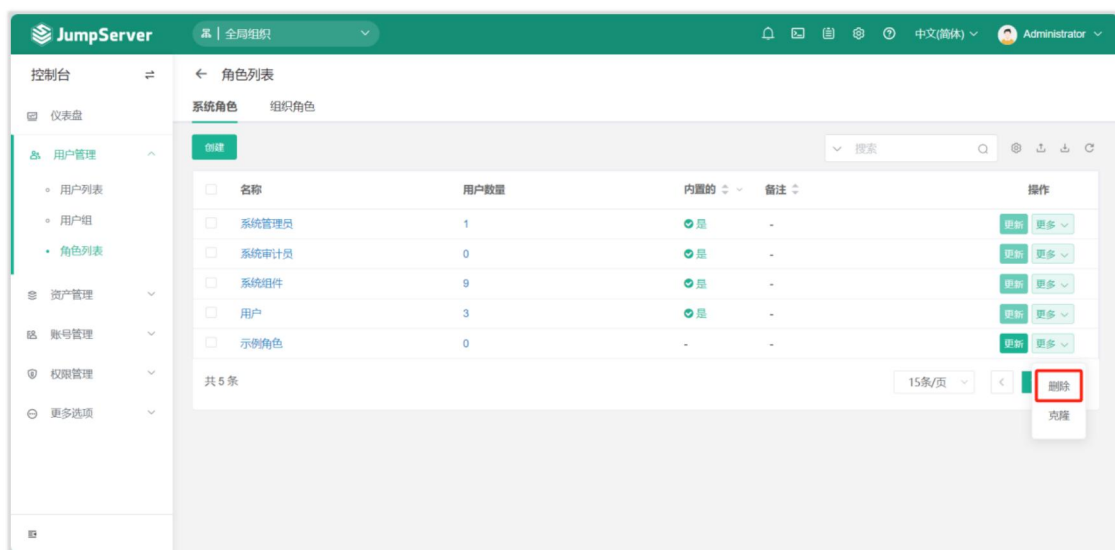
5.2.3.6. 克隆角色

所有角色均支持克隆。克隆后，在角色详情页中可以选择修改该角色的权限。点击角色后方的<更多>按钮选择<克隆>按钮，进入角色创建界面，修改相关信息后，提交修改角色权限即克隆完成。



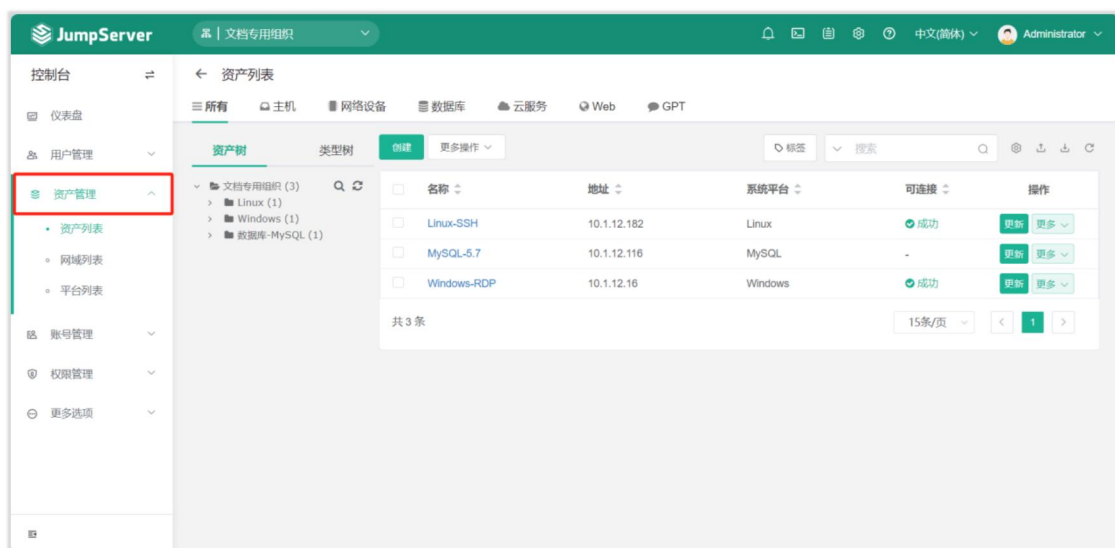
5.2.3.7. 删除角色

系统默认角色不允许删除，非内置角色可进行删除。点击角色后方的<删除>按钮，删除角色。



5.3. 资产管理

点击页面左侧的[资产管理](#)按钮，即可打开下拉框选择进入资产管理页面。资产管理页面主要针对于 JumpServer 的纳管资产的管理，包括 JumpServer 纳管的资产列表、网域列表、平台列表以及标签列表。



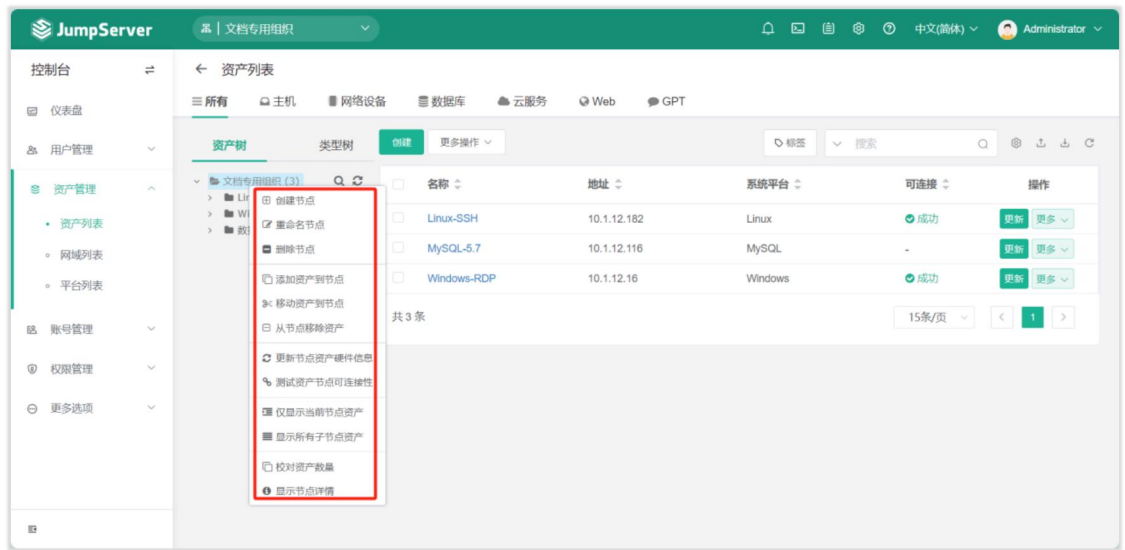
5.3.1. 资产列表

5.3.1.1. 资产树与类型树

资产树是对资产类别的一个划分。对于每个资产，可以按照不同维度进行划分，同一资产可

以存在多维度的划分，例如：按照组织划分、按照项目划分、按照协议划分等等。划分节点后，可以灵活的分配用户权限，达到高效管理主机的目的。

资产树根节点不能重名，右击节点可以添加、删除和重命名节点，以及资产的相关操作。

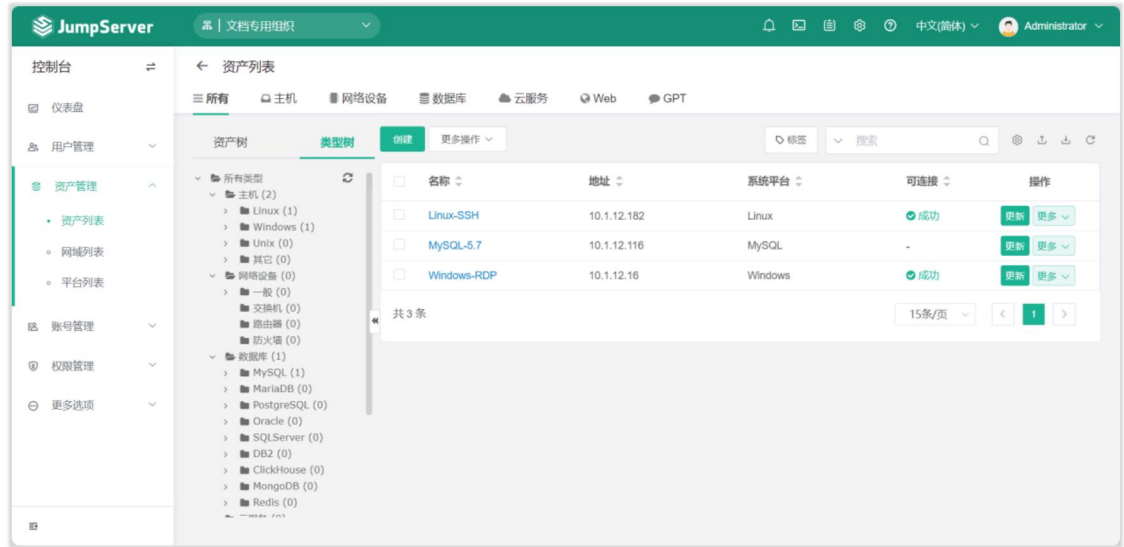


选项详细说明：

参数	说明
创建节点	在当前节点下创建一个新的子节点。
重命名节点	重命名当前节点，根节点不可重命名。
删除节点	删除当前节点。
添加资产到节点	将其他节点的资产添加到当前节点下，原节点下资产不会被移除。
移动资产到节点	将其他节点的资产移动到当前节点下，原节点下的资产会被移除。
更新节点资产硬件信息	拉起自动化任务，批量更新当前节点下资产硬件信息。注：需当前节点下的资产开启了自动化任务并配置正确的特权用户，该功能只支持 SSH 协议。
测试资产节点可连接性	拉起自动化任务，批量更新当前节点下资产的可连接性。注：需当前节点下的资产开启了自动化任务并配置正确的特权用户，该功能只支持 SSH 协议。
仅显示当前节点资产	只显示当前节点下的资产，不显示子节点下的资产。
显示所有子节点资产	当前节点下和所有子节点下的资产都显示出来，不论子节点下是否还有多层子节点。
校对资产数量	校对当前节点下的资产数量。

显示节点详情	显示当前节点的详细信息，包含节点 ID、名称与全称。
--------	----------------------------

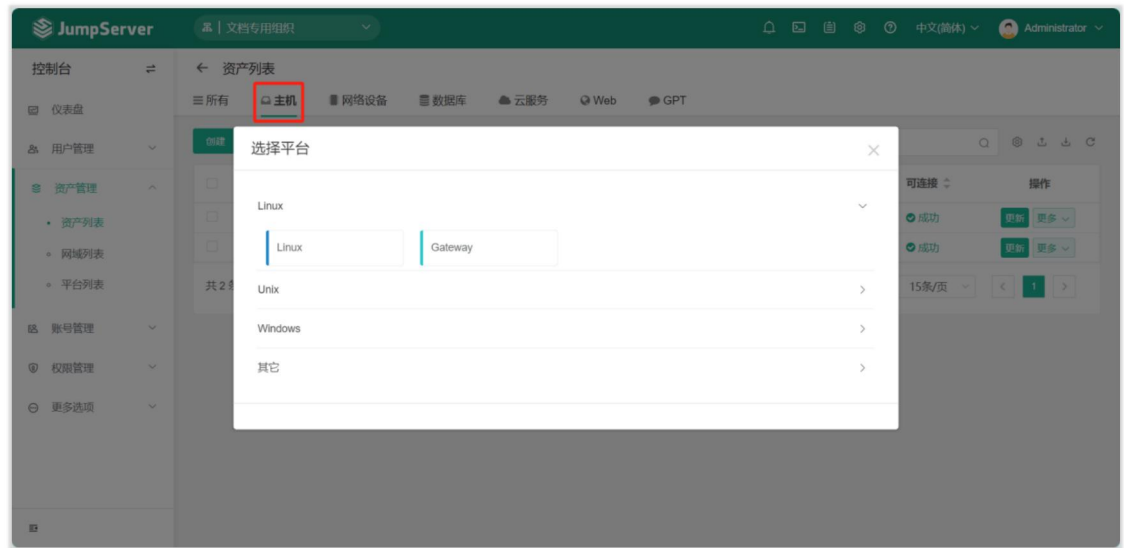
类型树是对资产的另一种区分，JumpServer 将主机、网络设备、数据库等均归类于 JumpServer 资产，类型树主要统计每一种类型的资产数量更直观的查看资产分布。



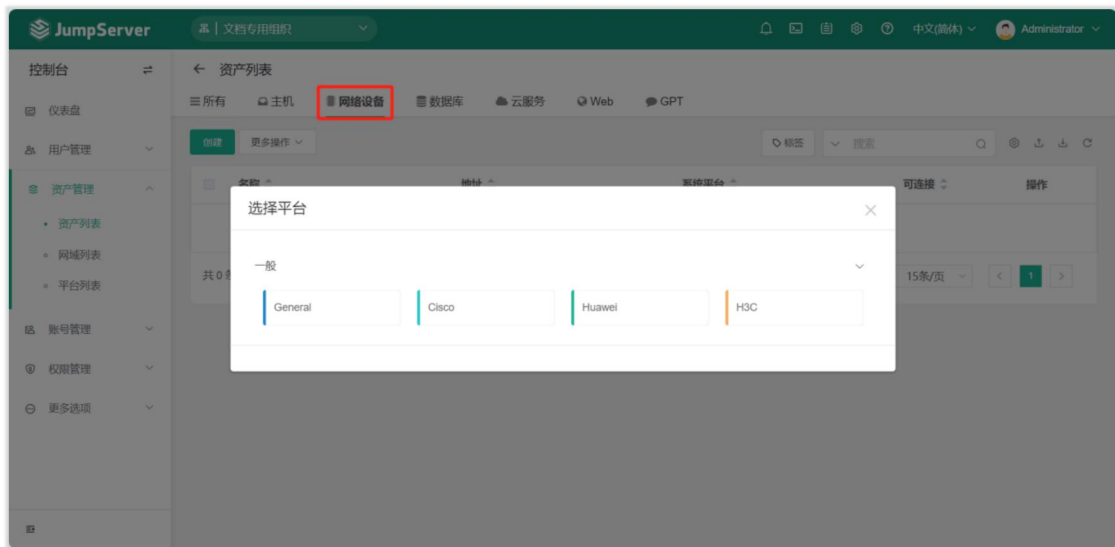
5.3.1.2. 资产类型

JumpServer 将主机、网络设备、数据库等等均归类于 JumpServer 资产。管理员用户可以自行在平台列表中自定义平台类型。

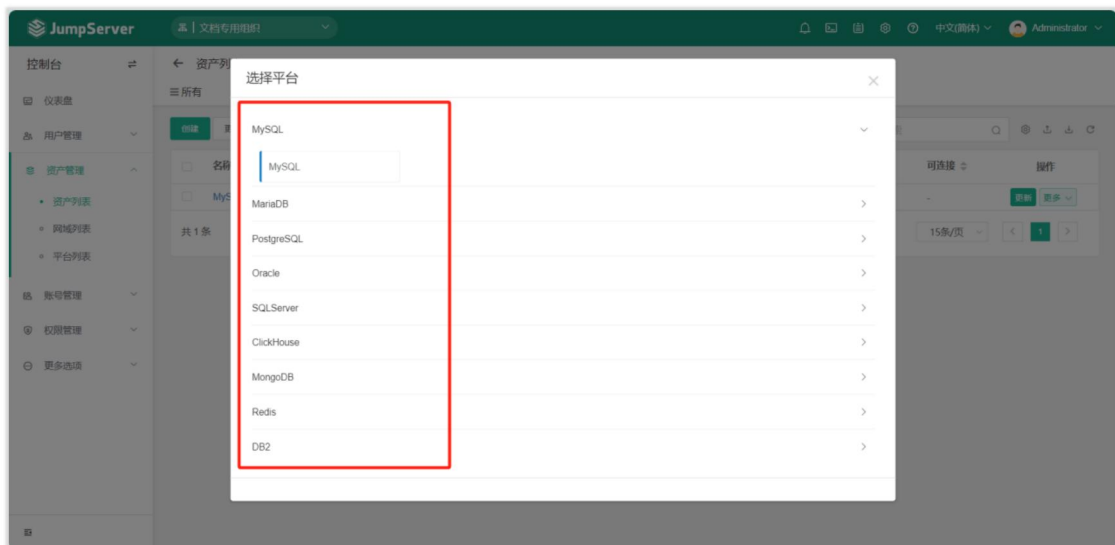
主机类型中默认包含 Linux 资产、Windows 资产、Unix 资产等。



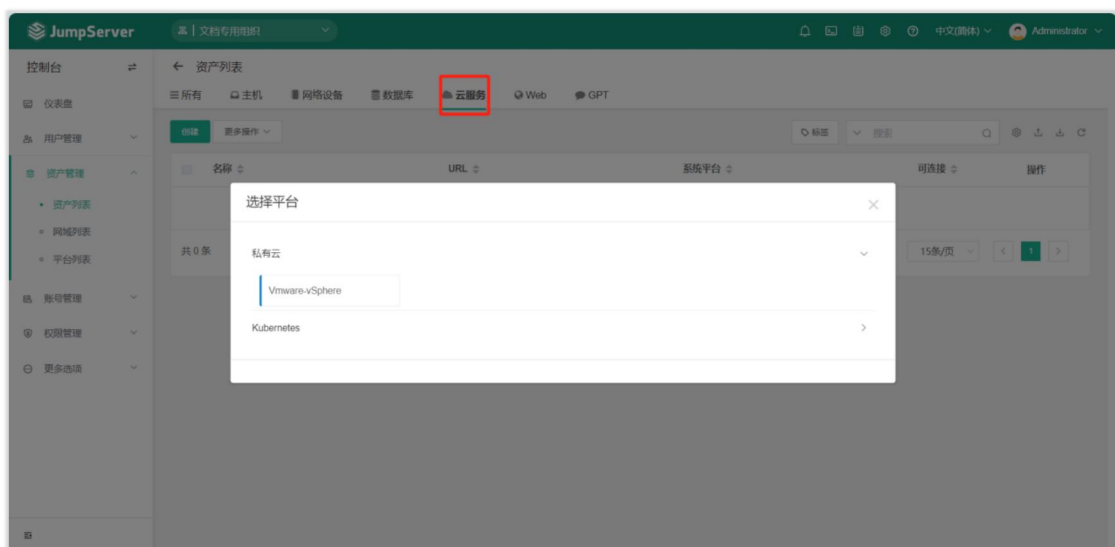
网络设备类型中默认包含 General、Cisco 等。



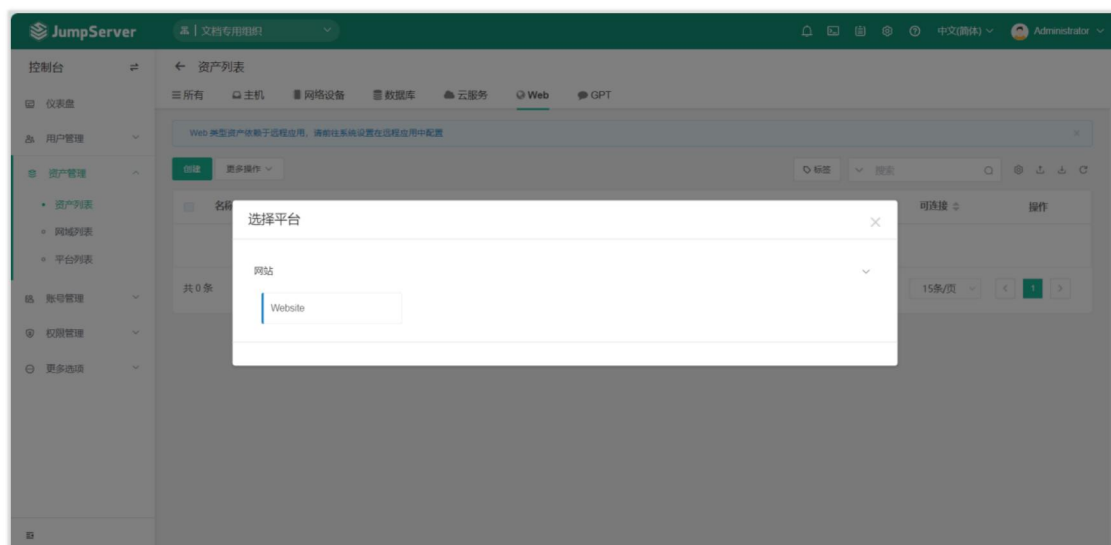
数据库类型中默认包含 MySQL、MariaDB、Oracle、Redis 等。



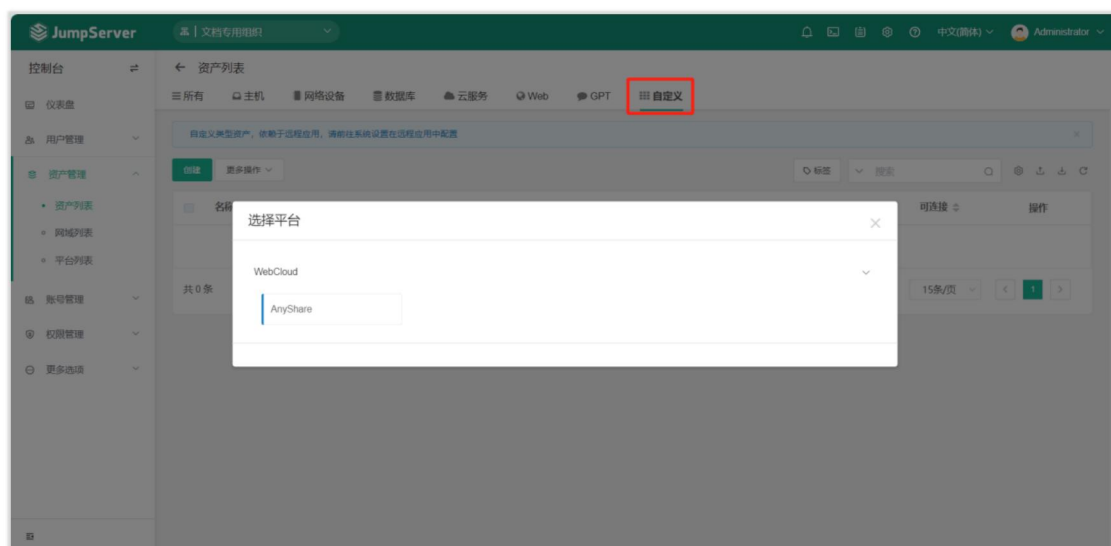
云服务类型中默认包含私有云与 Kubernetes。



Web 类型中默认包含网站。可在远程应用中自定义其他 Web 网站。



除堡垒机内置的资产类型之外，JumpServer 支持以远程应用的方式自定义资产类型，例如：测试软件，笔记软件等等。



5.3.1.3. 资产创建

JumpServer 支持多种方式创建资产。例如：手动创建单个资产，克隆资产、表格导入批量创建资产、云同步批量创建资产。

- 手动创建单个资产

JumpServer 支持手动创建资产。资产的创建需要填入资产的基本信息，登录用户信息，节点信息等必要信息。点击资产分类进入具体的分类页面（以主机为例）。点击页面左上角的 [<创建>](#) 按钮，进入资产创建页面，填写资产详细信息。

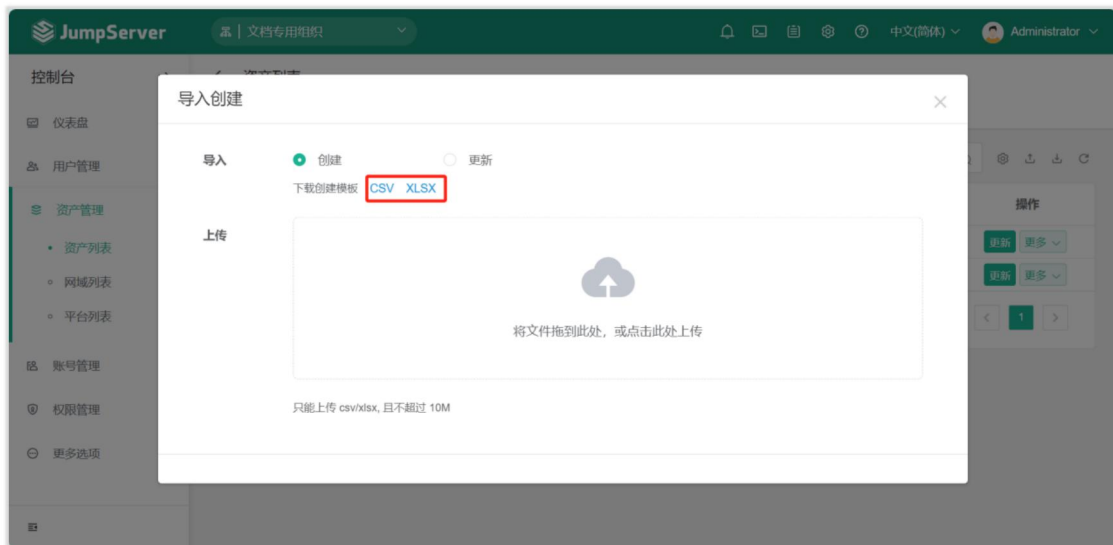


详细参数解释：

参数	解释
名称	必填项，该资产在 JumpServer 中的名称，与资产本身计算机名无关。不可重名。
IP/主机	必填项，资产的真实 IP 或 VIP 或域名。允许重名。
系统平台	默认项，资产的系统平台，各个平台可以设置不同的字符编码、连接参数等。
节点	必填项，该资产所属于的节点。
协议组	必填项，资产访问时用到的协议，可选一个或多个。默认协议组为系统平台中设置的协议组。
账号列表	必填项，该资产的登录用户，可创建多个账号。账号与资产绑定。
网域	可选项，针对某些跨网段资产，需要以网域网关（ sshpas ）为代理进行访问。
标签	可选项，给该资产添加的标签，方便管理。
激活	必填项，该资产是否可使用。

● 通过 Excel 批量导入资产

JumpServer 支持通过 **Excel** 表格导入进行批量创建、更新资产。**JumpServer** 提供两种模板信息，**CSV** 与 **XLSX** 模板。首次导入资产，可点击资产列表的右上角 [<导入>](#) 按钮，下载导入模板后根据模板提示填写需要导入或更新的信息，填写完成后在导入页面导入文件即可。

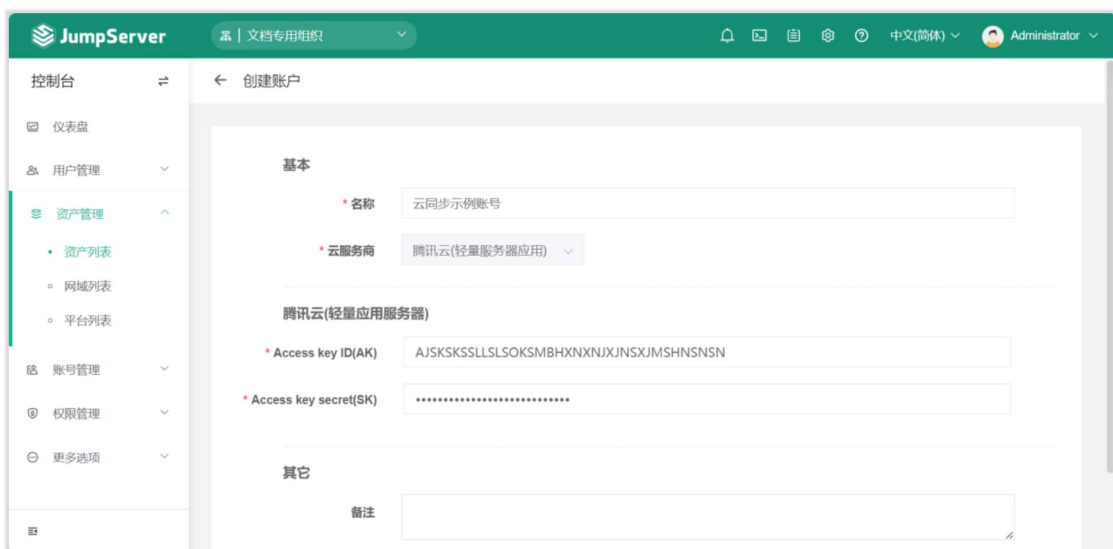


● 云同步

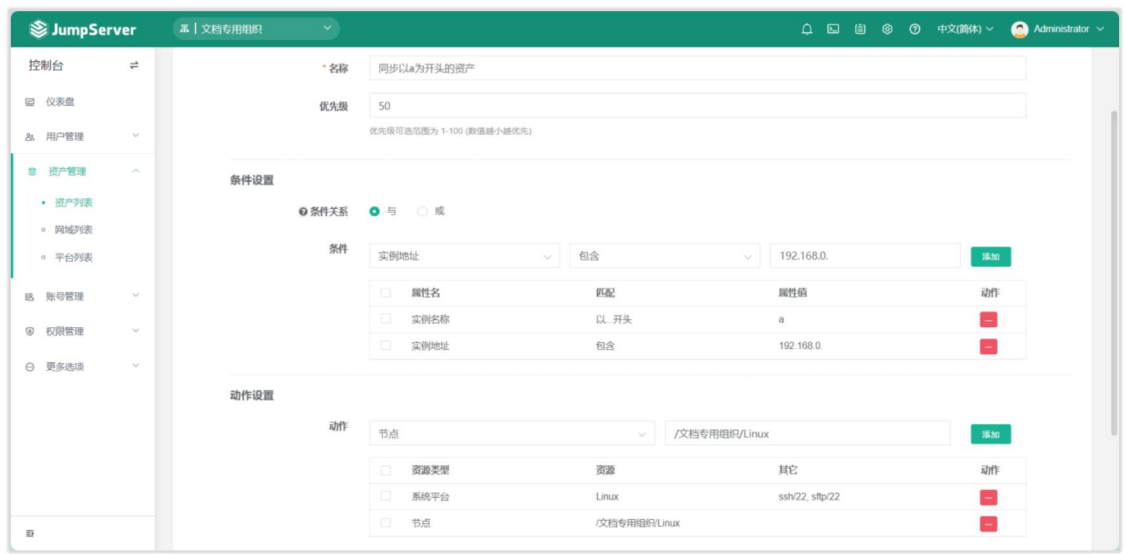
JumpServer 堡垒机提供云主机同步功能。云同步功能支持将云资产同步到 JumpServer 堡垒机中。通过创建云账号和同步实例将阿里云、腾讯云、腾讯云（轻量应用服务器）、华为云、百度云、京东云、金山云、AWS(中国)、AWS(国际)、Azure(中国)、Azure(国际)、谷歌云、UCloud 云、VMware、青云私有云、华为私有云、天翼私有云、OpenStack、ZStack、Nutanix、Fusion Compute、深信服云平台、阿里云专有云、局域网等的云资产同步到 JumpServer 资产列表。

点击页面左侧的<资产列表>按钮，进入资产列表页面。点击资产列表页面的主机页签，点击<云同步>按钮，进入云同步页面。

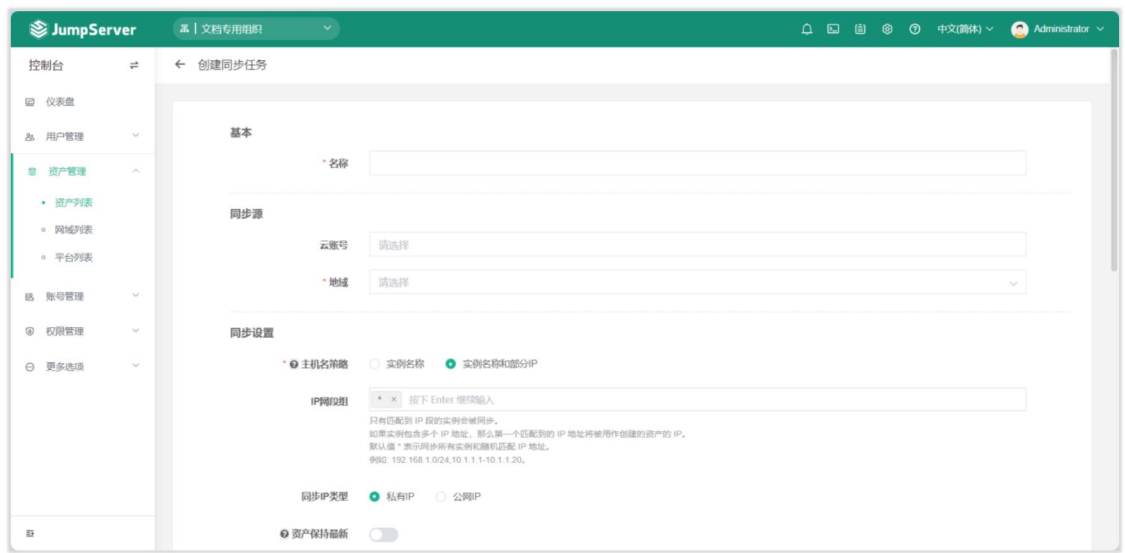
点击云同步页面的账号列表页签，在此页面上创建云账号，以腾讯云为例(在腾讯云的账号页面获取腾讯云的相关密钥):



点击云同步页面的同步策略页签，在此页面上创建同步策略。



点击云同步页面的同步实例任务列表页签，在此页面上创建同步任务实例。



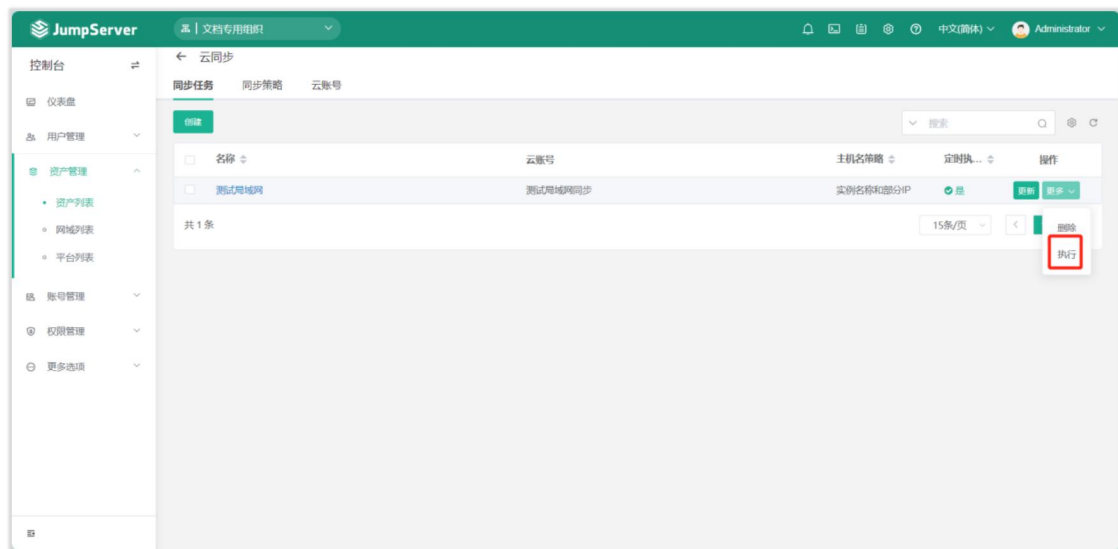
详细参数说明：

参数	说明
名称	该同步任务的名称。
账号	同步源的账号，即账号列表中的账号。
地域	账号列表中可识别的地域，即需求同步的资产所处的地域。
主机名策略	同步资产的主机名，选择‘实例名称’或‘实例名称+部分 IP’。
IP 网段组	同步资产被匹配的 IP 网段组。如果匹配成功，资产即可被同步。

同步 IP 类型	同步资产被同步的 IP 类型，私有 IP 或者公网 IP。
资产信息保持最新	每次执行同步任务时，是否更新资产的所有信息。
资产完全同步	当资产条件不满足匹配资产策略时，是否继续同步此类资产。
策略	选择需要匹配的策略。
定时执行	是否开启定时执行。

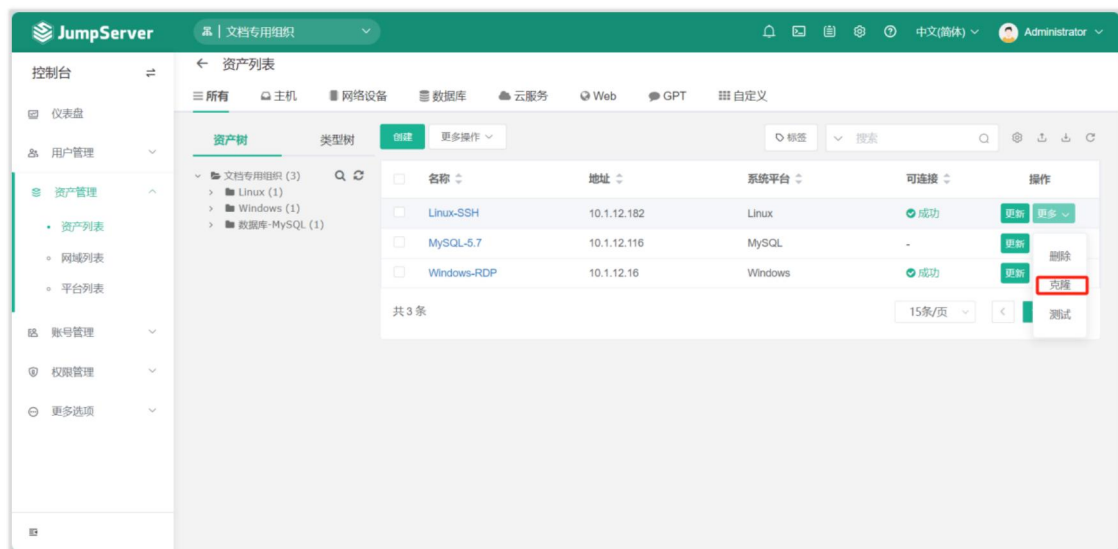
点击[提交](#)按钮后，同步实例任务创建完成。

同步任务可定时执行也可手动执行。手动执行即点击同步任务实例后方的[更多](#)按钮，选择[执行](#)按钮，即可执行同步任务。



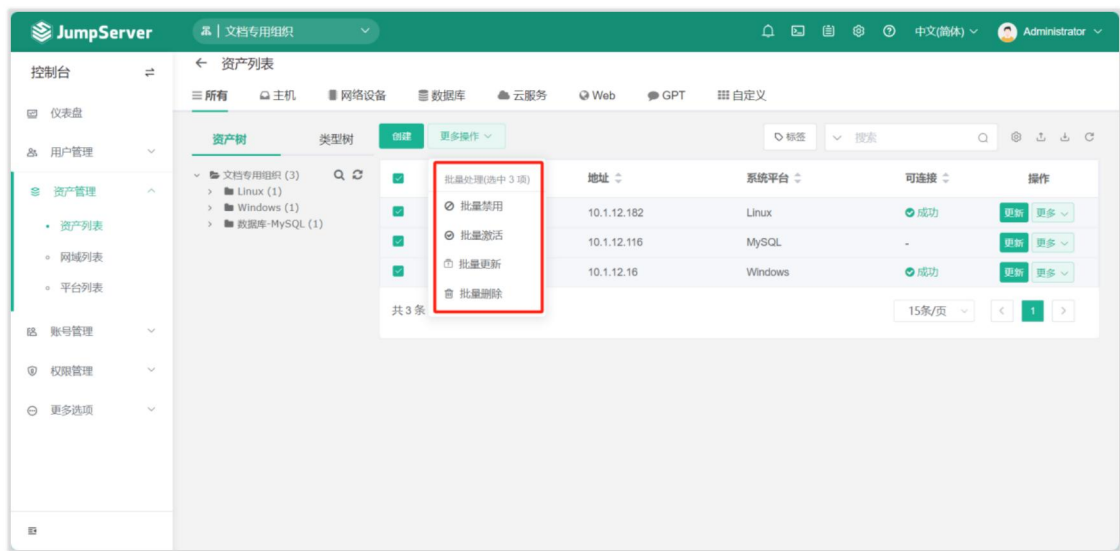
● 克隆资产

对于资产大部分信息相同的情况，可通过克隆功能快速添加资产，点击资产后方的[更多](#)按钮，选择[克隆](#)按钮，进入资产信息界面，修改相关信息后，提交即可。



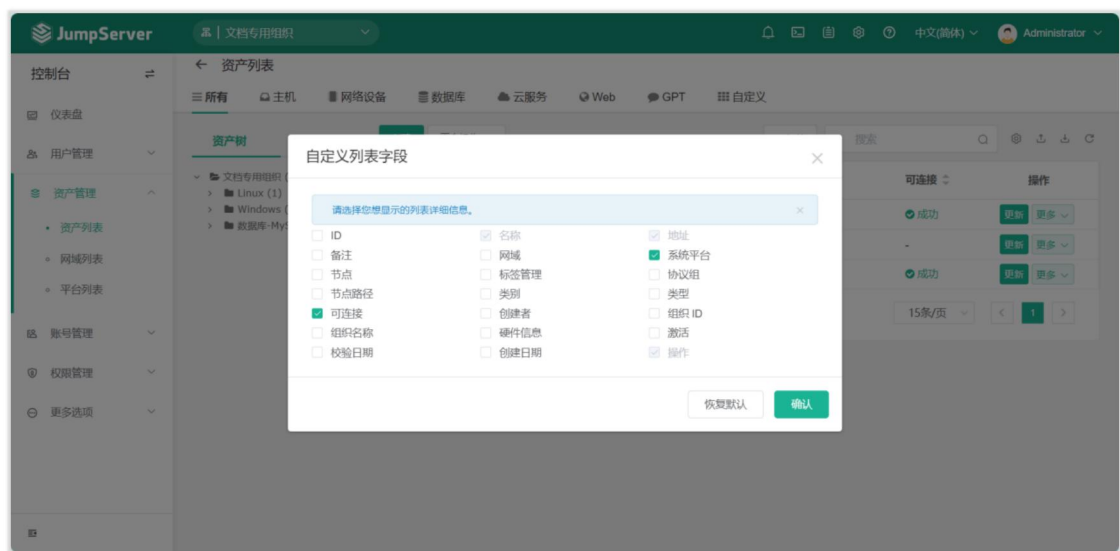
5.3.1.4. 批量操作

[更多操作](#)按钮针对于批量操作资产的场景。当需求批量操作资产时，选择用户组前方的复选框，点击[更多操作](#)按钮，选择对应按钮操作对应的资产。



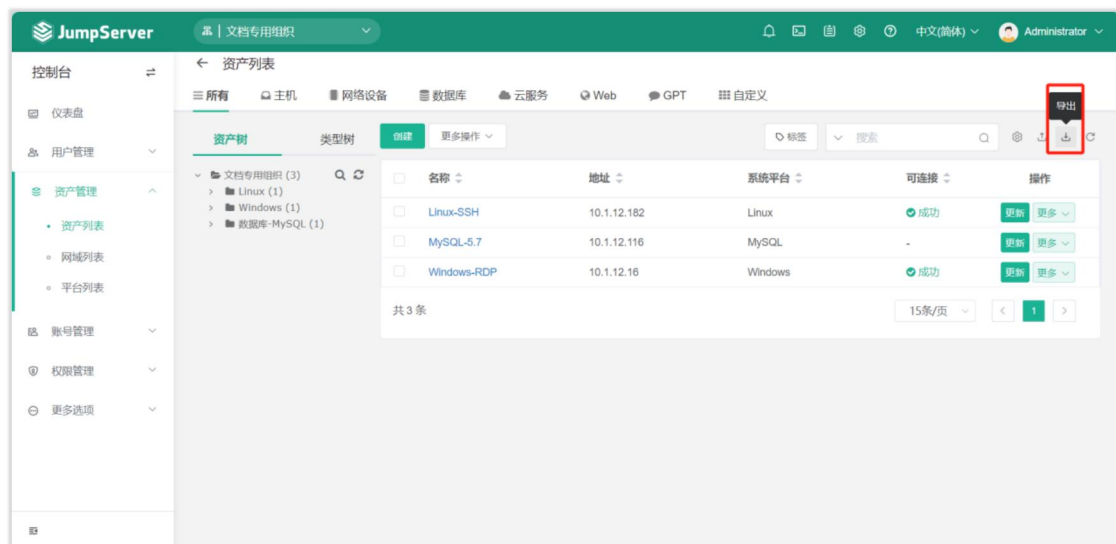
5.3.1.5. 显示设置

点击资产列表页右上角的[齿轮](#)按钮，可进行页面显示的设置，可更详细的展示资产相关信息，例如：资产协议组、资产节点、资产所处组织等。



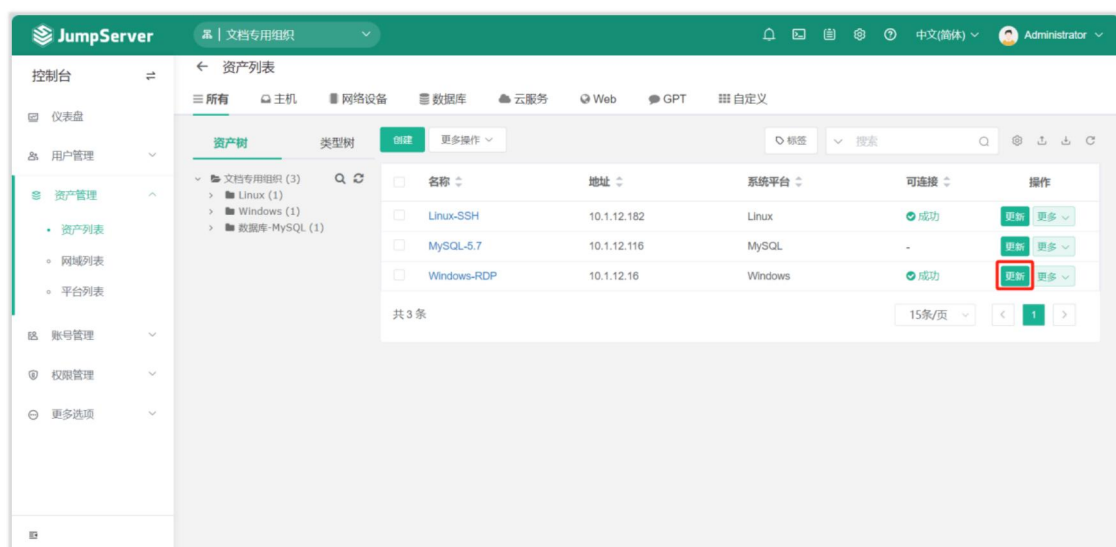
5.3.1.6. 资产导出

资产支持已存在资产信息导出，支持的表格方式有 **xlsx**、**csvs**。点击页面右上角的 **<导出>** 按钮，导出需要的资产信息。



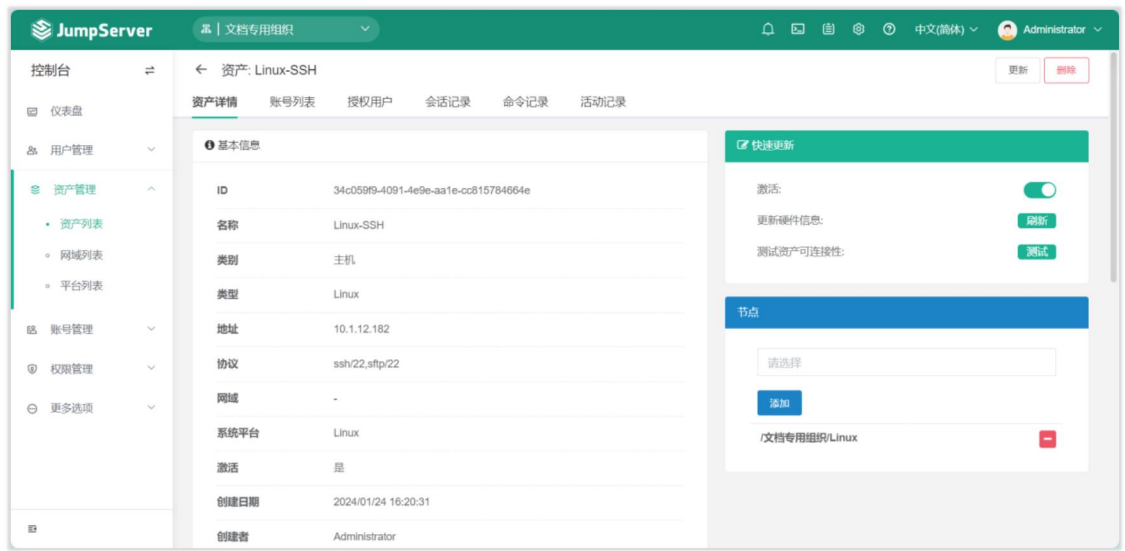
5.3.1.7. 资产更新

当需求对某一个资产的信息进行更新时，可点击资产后方的 **<更新>** 按钮，进入资产信息更新页面，更新资产相关信息。当需求更改该资产对应的账号的信息时，点击 **<资产名称>** 按钮进入资产详情页面，在账号列表模块对账号信息更新。



5.3.1.8. 资产详情

在资产列表页面点击<资产名称>，进入资产详情页面。资产详情页包含的信息包括资产基本信息、资产账号列表、授权用户以及资产活动记录。



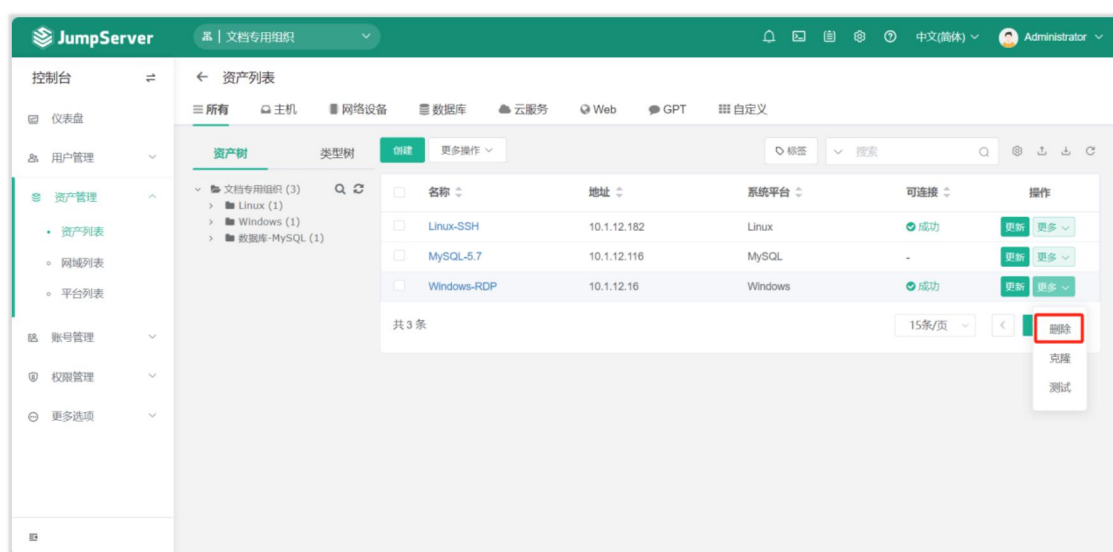
详细参数说明：

参数	说明
基本信息	基本信息模块主要介绍资产的信息，包括资产名称、协议、系统平台等。
硬件信息	硬件信息模块主要查看该资产的硬件信息，包含 CPU 信息、内存、硬盘信息等。此模块信息通过自动化任务获取硬件信息。
快速更新	快速更新模块主要进行资产的自动化任务执行，例如：更新资产硬件信息与资产可连接性。
节点	节点模块可以调整资产所属的模块。
标签	标签模块可以查看资产所属的标签。
账号列表	账号列表模块主要包含资产绑定的系统账号信息，在此模块进行账号的增加、删除、查看、修改。
授权用户	授权用户模块主要展示资产被授权的用户、用户组；此页面还查看该资产对应的授权规则。
会话记录	会话记录模块记录该资产的会话信息，包括连接用户、连接

	时间等等。
命令记录	命令记录模块主要记录该资产上执行过的命令记录。
活动记录	活动记录模块主要查看资产最近 30 次的日志, 包含更新日志和会话记录。

5.3.1.9. 资产删除

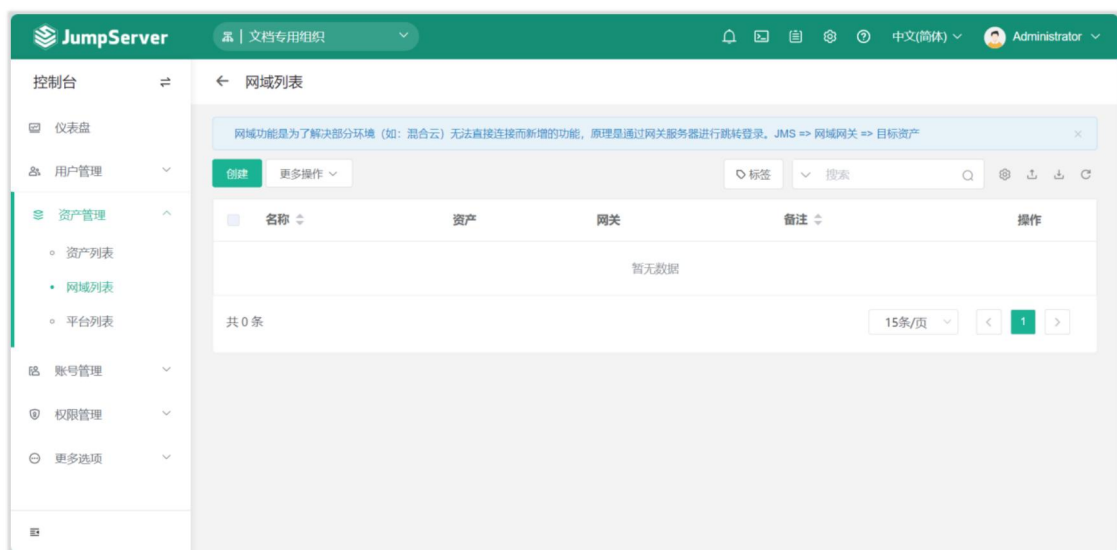
当需求删除某个资产时, 可以点击相应的资产后方的<更多>按钮, 选择<删除>按钮, 点击删除即可。



5.3.2. 网域列表

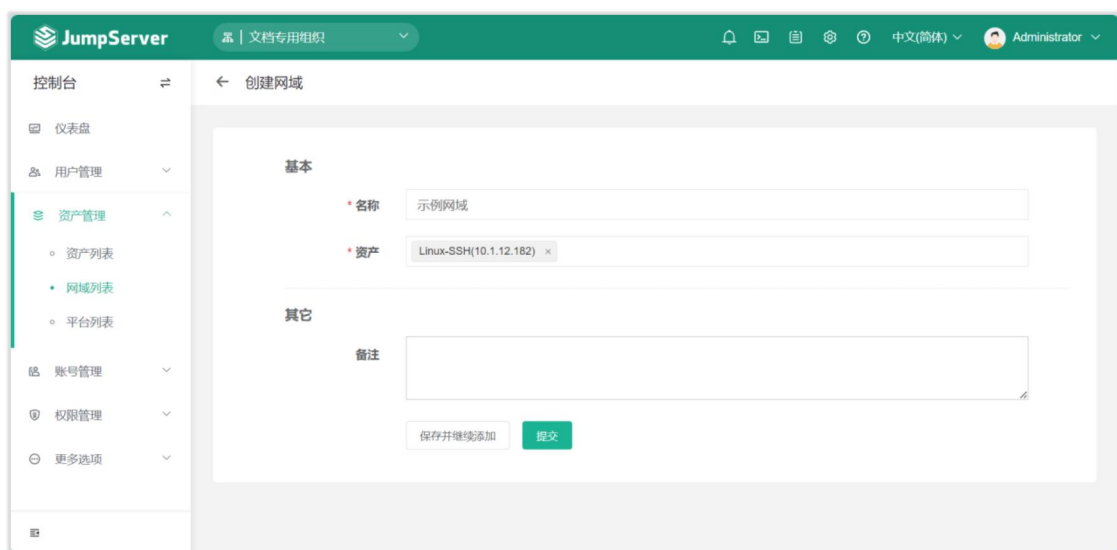
JumpServer 支持网域功能。网域是为了解决 JumpServer 与部分资产之间网络无法连通的问题, 原理是通过网关服务器进行 SSH 隧道进行流量转发。

点击页面左侧的<网域列表>按钮, 进入网域列表界面。网域列表界面主要针对于 JumpServer 的网域列表进行增加、删除、更改、查看。



5.3.2.1. 网域创建

点击“网域列表”页面的[创建](#)按钮，进入网域列表信息设置页面，填写网域的相关信息。

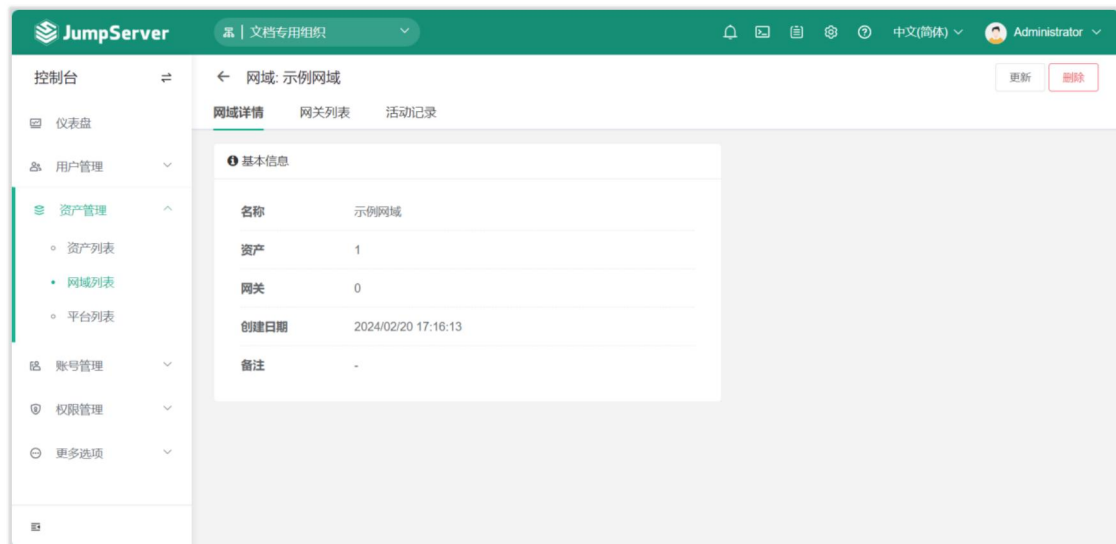


详细参数说明：

参数	说明
名称	网域识别名称。
资产	资产选项为需要使用网域与 JumpServer 通信的资产。

5.3.2.2. 网域详情

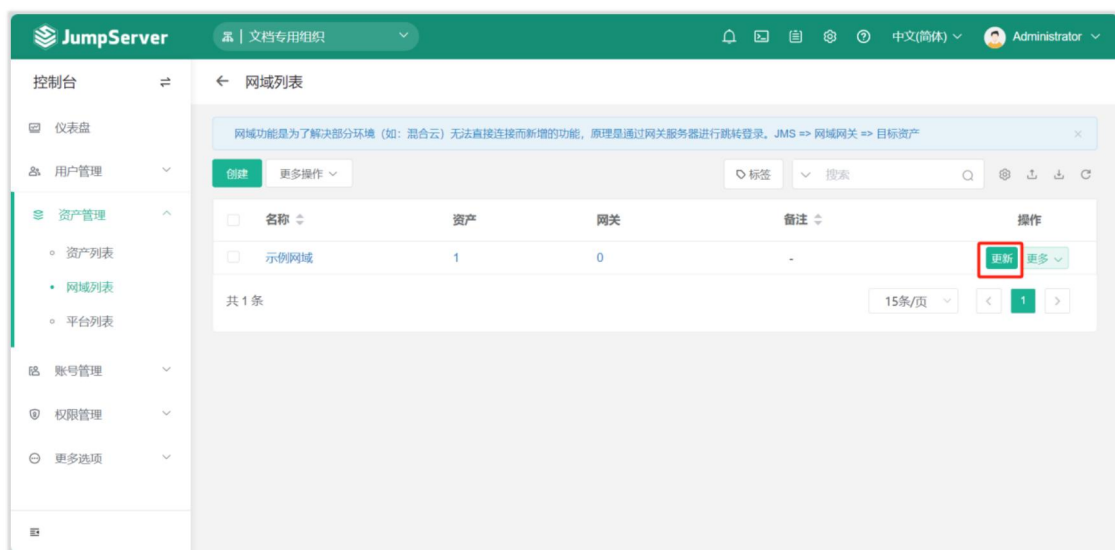
在网域列表页面点击[网域名称](#)按钮，进入网域详情页面，该页面主要包含网域详情页面、网关列表页面、活动记录页面。



- 网域详情：该模块主要包含网域的详细信息，包含名称、创建日期等等。
- 网关列表：该模块主要进行网关的增加、删除、更新、查询。
- 活动记录：该模块主要记录网域的相关日志。

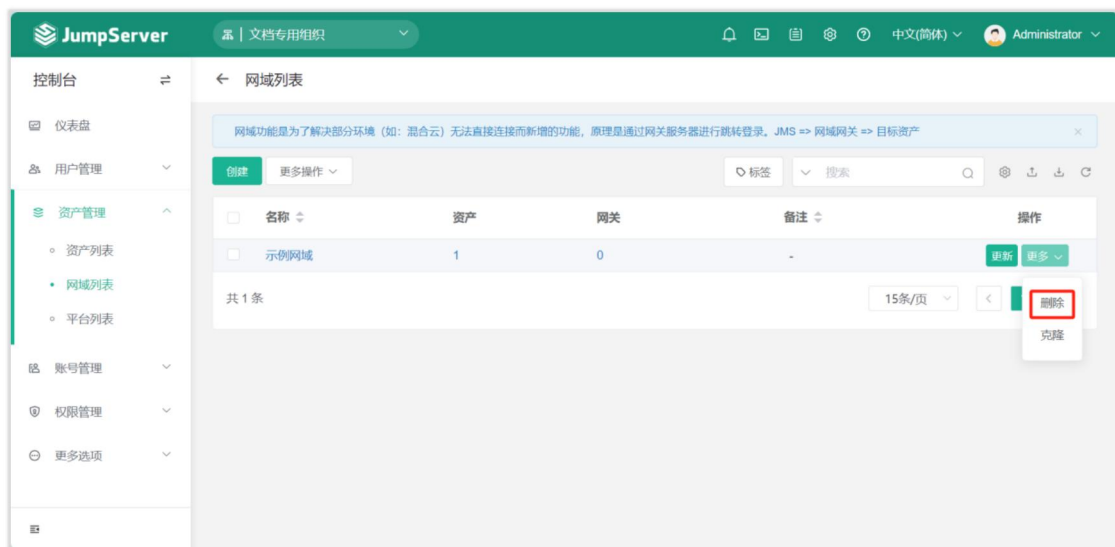
5.3.2.3. 网域更新

当需求对某一个网域的信息进行更新时，可点击资产后方的[更新](#)按钮，进入资产信息更新页面，更新资产相关信息。当需求更改该网域对应的网关的信息时，点击[网域名称](#)按钮进入网域详情页面，在网关模块对网关信息更新。



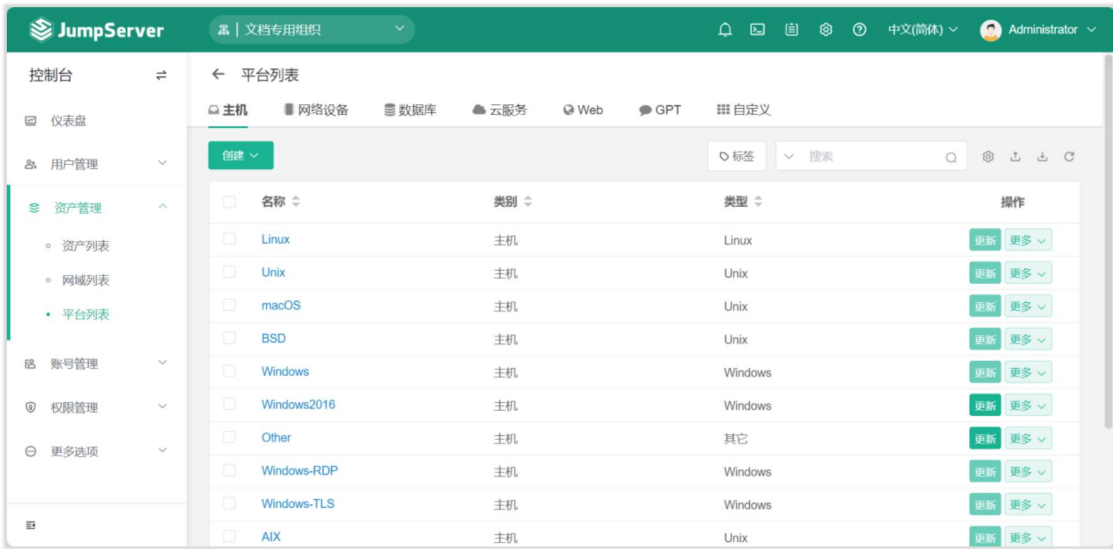
5.3.2.4. 网域删除

当需求删除某个网域时，可以点击相应的网域后方的<更多>按钮，选择<删除>按钮，点击删除即可。

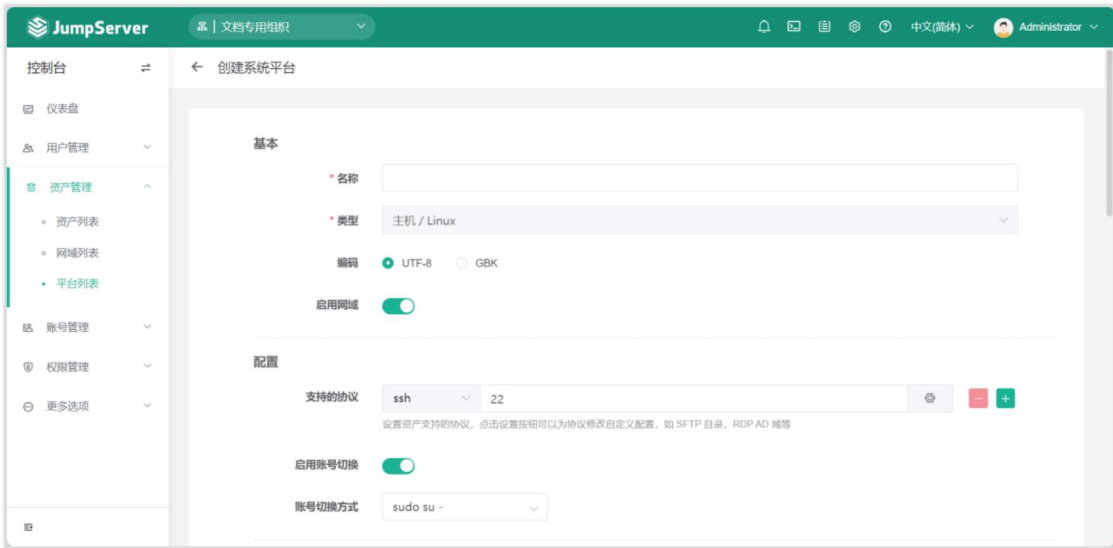


5.3.3. 平台列表

JumpServer 支持用户自定义平台列表。平台列表在创建资产时供用户选择，用户可以在创建资产时为资产选择不同的系统类型，如 Linux、Windows 等，用户也可以新建一个平台类型，并选择指定的基础平台，就可在创建资产中指定新建的平台类型。不同的平台类型决定改密计划中的改密脚本。



点击平台列表页面的[<创建>](#)按钮，填写系统平台的信息即可创建新的系统平台。



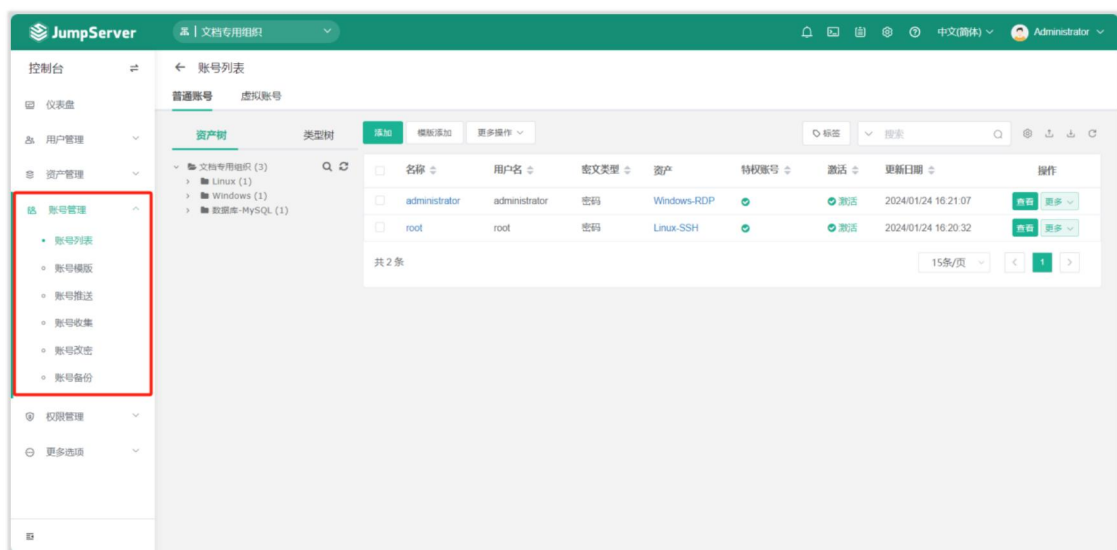
详细参数说明：

参数	说明
名称	系统平台的名称。
类型	系统平台的类型，不同的系统类型决定不同的编码与自动化方式。
编码	系统平台选择的编码方式，可选择“UTF8”或“GBK”。
启用网域	是否启用网域，如果此按钮无法选择即该平台类型不支持启用网域。
支持的协议	设置系统平台支持的协议，每个平台中默认的协议不可删除。协议的默认端口号支持修改。点击设置按钮可以

		为协议修改自定义配置，例如： SFTP 目录， RDP 的 AD 网域。
启用切换账号	启用	启用切换账号，并设置切换方式。
	不启用	不启用切换账号功能。如果此按钮无法选择即表示该系统平台不支持切换账号功能。
启用自动化	Ansible 配置	Ansible 连接等信息配置。一般不进行修改。
	启用资产探测	是否启用资产探测，即获取资产连接性。
	资产探测方式	设置资产的探测方式。
	收集资产信息	是否启用资产信息，即获取资产硬件信息等。
	收集信息方式	设置收集信息的方式。
	启用账号改密	是否启用账号改密。
	账号改密方式	设置账号改密的方式。
	启用推送账号	是否开启推送账号。
	推送账号方式	设置推送账号的方式。账号推送中可更改推送账号的默认参数。
	启用校验账号	是否开启校验账号。
	校验账号方式	设置校验账号的方式。
	启用账号收集	是否启用账号收集功能。
	收集账号方式	设置收集账号的方式。
	不启用	不启用自动化任务。

5.4. 账号管理

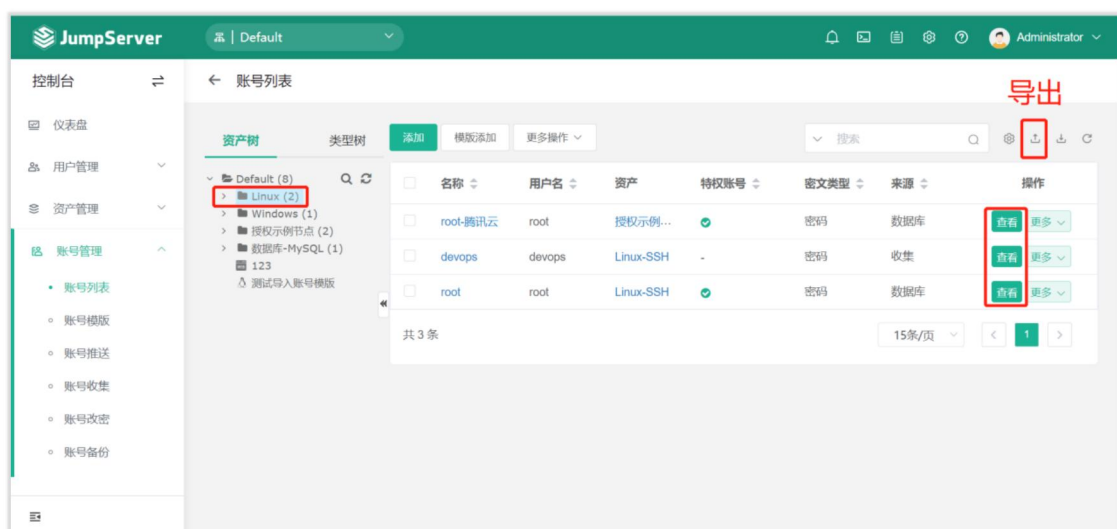
点击页面左侧的<账号管理>按钮，即可打开下拉框选择进入账号管理页面。资产管理页面主要针对于 **JumpServer** 的资产账号的管理，包括账号查看、账号模版、账号推送、账号收集、账号改密、账号备份等。



5.4.1. 账号列表

5.4.1.1. 普通账号

JumpServer 支持对已托管资产的账号进行管理。点击页面左侧的资产树或者类型树选择需要查看的节点或者资产，可以查看相关资产关联的账号信息（需要查看管理员账户的 MFA），可以针对账户信息批量导出，JumpServer 支持导出所有资产关联账号的详细信息与账号密码。

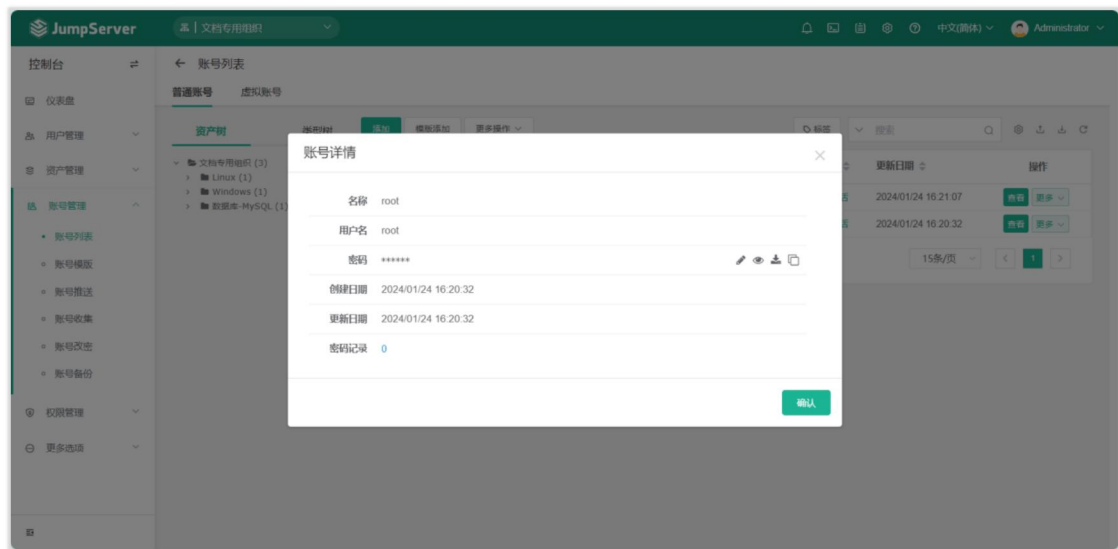


查看账号详细信息例如账号密码时需要验证用户的 MFA。

JumpServer 为提高安全性，默认查看密码需要校验 MFA；如需取消验证 MFA，可以在 JumpServer 的配置文件中添加配置项，修改后重启堡垒机服务生效。

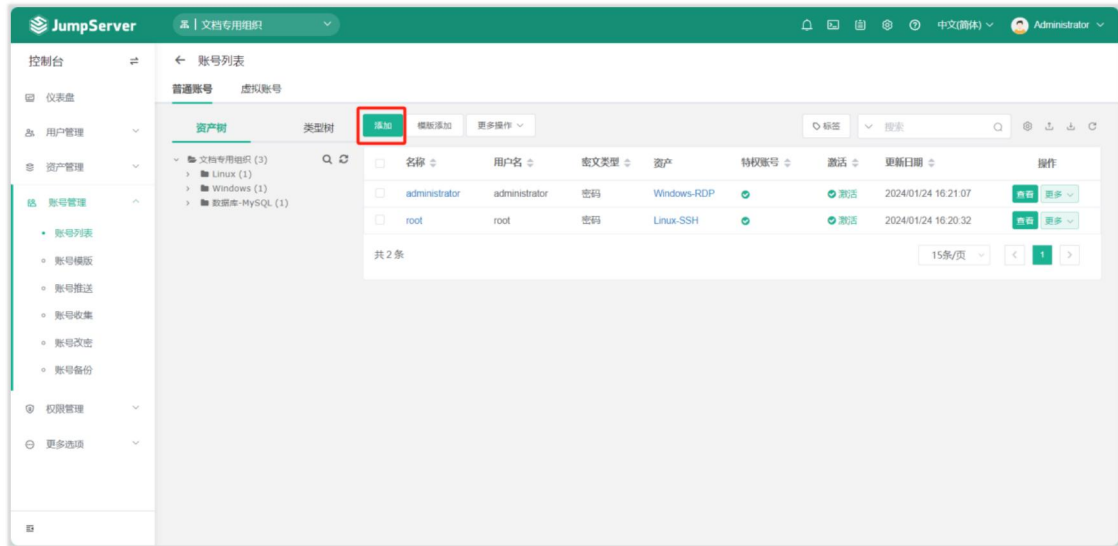
JumpServer 的配置文件默认位于：/opt/jumpserver/config/config.txt

关闭账号查看时 MFA 验证的配置项为：SECURITY_VIEW_AUTH_NEED_MFA=False



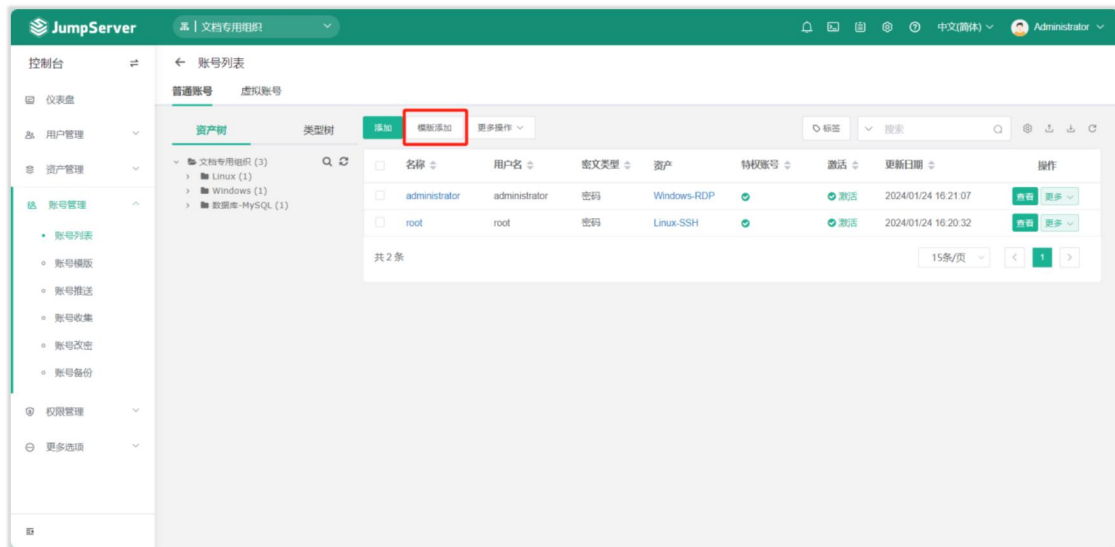
(一)账号添加

JumpServer 支持将一个账号批量关联给多个资产，即账号添加功能。点击账号列表页面的 [<添加>](#) 按钮，选择需要将账号关联的资产，填写需要关联的账号相关信息，即可批量的关联账号给资产。



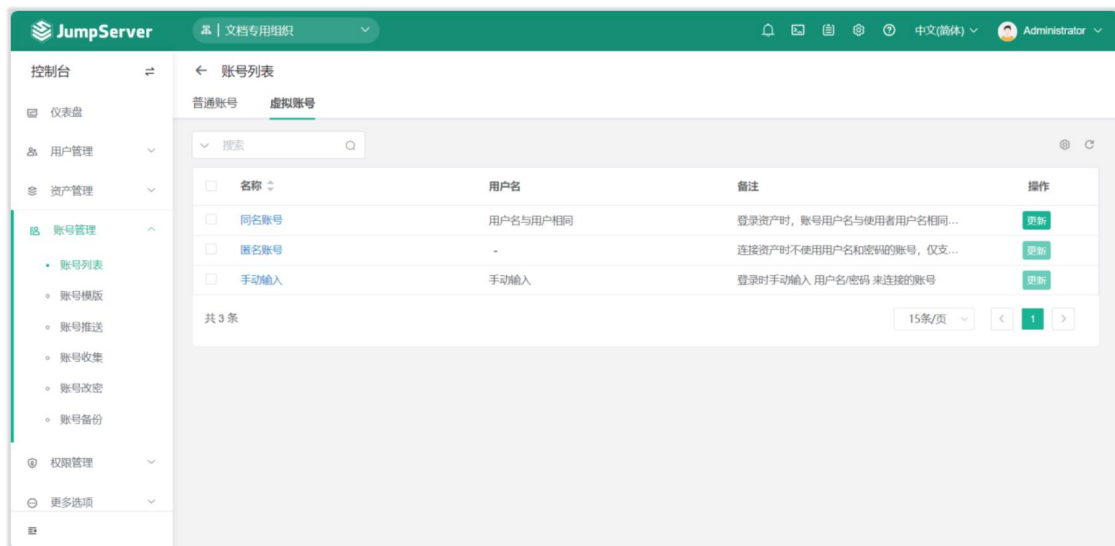
(二)账号模版添加

JumpServer 支持将账号模版批量关联给多个资产，即账号模版添加功能。点击账号列表页面的 [<模版添加>](#) 按钮，选择需要将资产关联给的资产，选择需要管理的账号模版，即可批量的关联账号模版给资产。



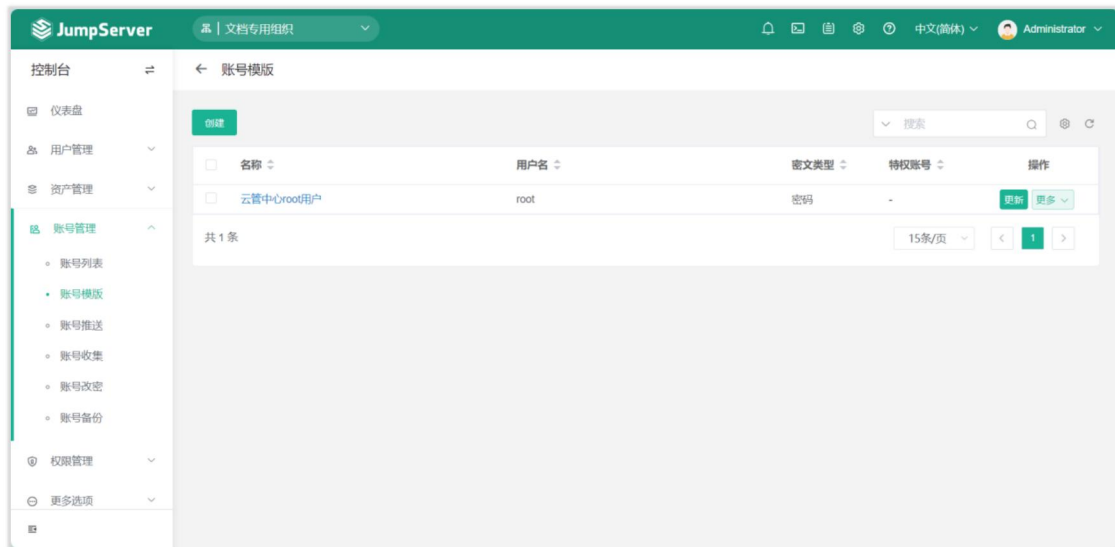
5.4.1.2. 虚拟账号

在授权规则创建时，某些场景下会使用虚拟账号登录资产。虚拟账号页面支持对虚拟账户的详情进行查看。JumpServer 支持当授权规则中授权了同名账户时，AD/LDAP 用户使用 JumpServer 用户密码登录资产。



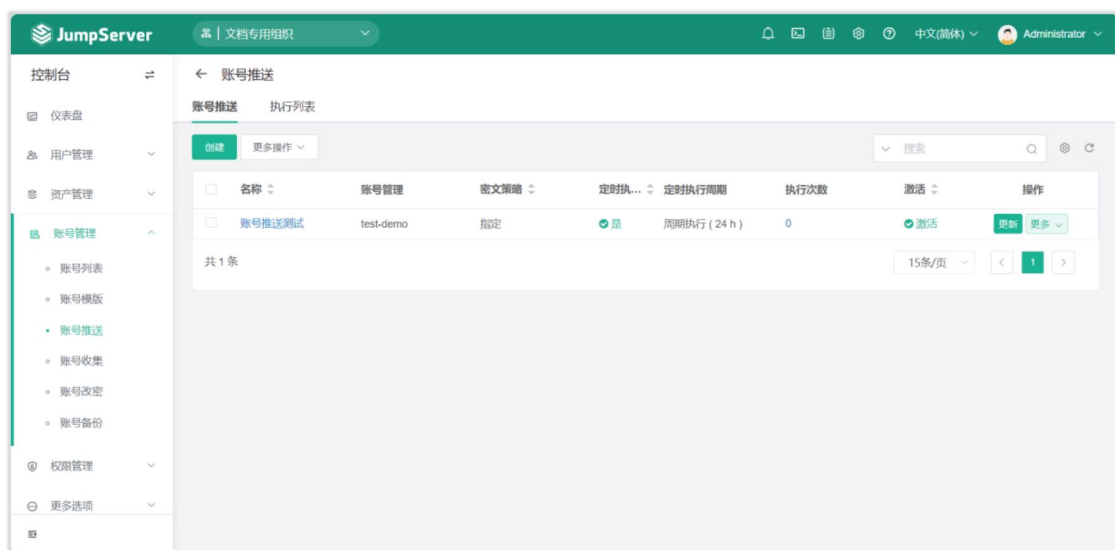
5.4.2. 账号模版

在纳管资产中，可能会出现多个资产账户与密码相同的情况。账号模版功能可以简化每一次创建资产时创建账号的步骤，创建资产时直接关联账号模版即可。授权时选择账号模版。账号模版即一个账户信息。



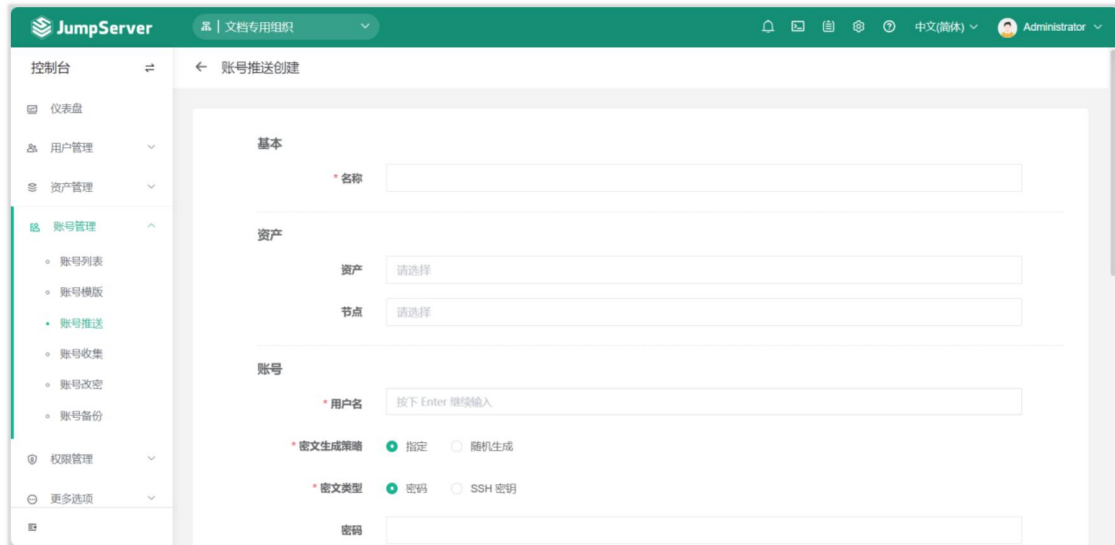
5.4.3. 账号推送

JumpServer 支持自动化推送用户到纳管的资产中。



5.4.3.1. 账号推送

点击账号推送页面的[<创建>](#)按钮，创建一个账户推送任务。

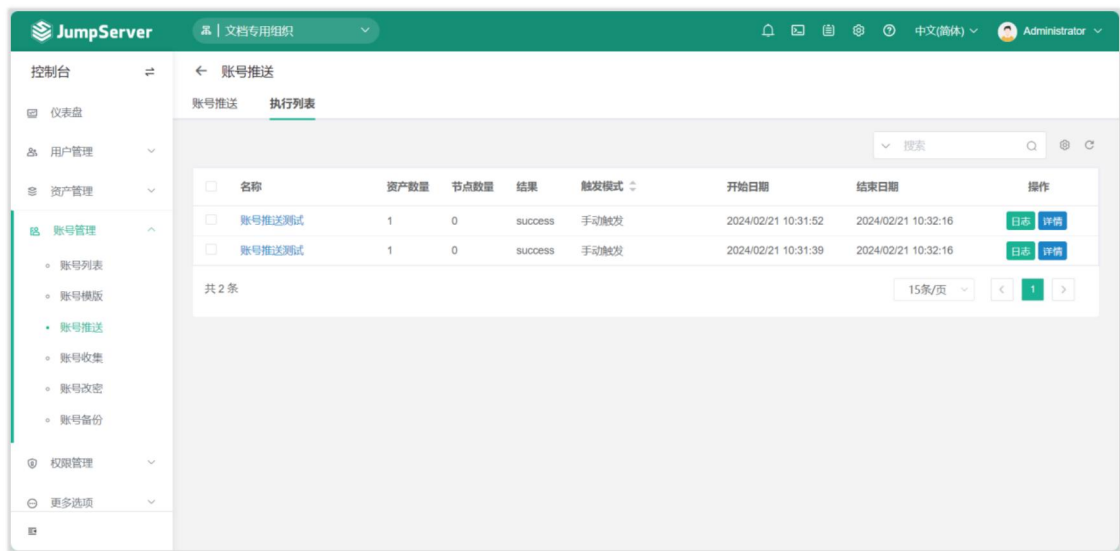


详细参数说明：

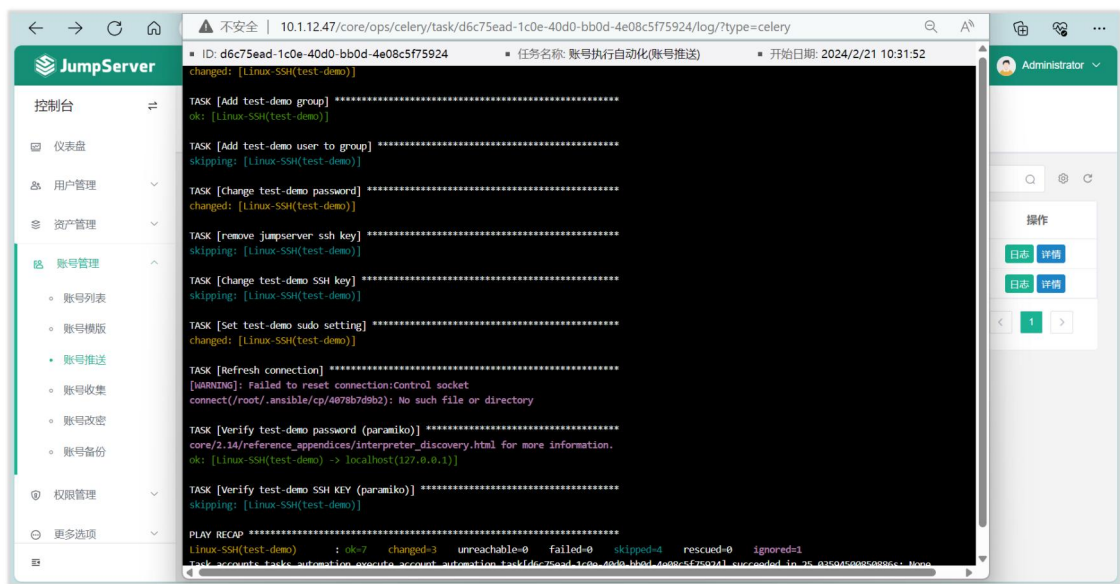
参数	说明
名称	账号推送任务的名称。
资产	需要被推送账户的资产。
节点	需要被推送账户的节点。
用户名	需要被推送到资产的账号名称。
密码策略-密文生成策略	选择被推送的用户的密码策略。 <ul style="list-style-type: none"> ● 指定：管理员用户手动输入密码。 ● 随机：JumpServer 自行生成密码。
密码策略-密文类型	被推送的用户密文的类型。
密码	选择密文生成策略为指定，管理员用户输入密码。 选择密文生成策略为随机，管理员用户设置密码生成规则，例如：密码长度、密码强弱规则等等。
推送参数	<ul style="list-style-type: none"> ● 当资产系统为 Windows 操作系统时，账号推送支持配置推送账号的用户组； ● 当资产系统为类 UNIX 操作系统时，账号推送支持配置推送账号的 Sudo、Shell、用户组； 目前仅对平台种类为主机的资产生效。
定时执行	选择该自动化任务是否定时执行，设置定时任务执行时间。

5.4.3.2. 执行列表

该页面主要查看账号推送计划任务的执行日志、任务详情等详细信息。



点击任务执行列表后的日志，可以查看账号推送任务的详细日志信息。

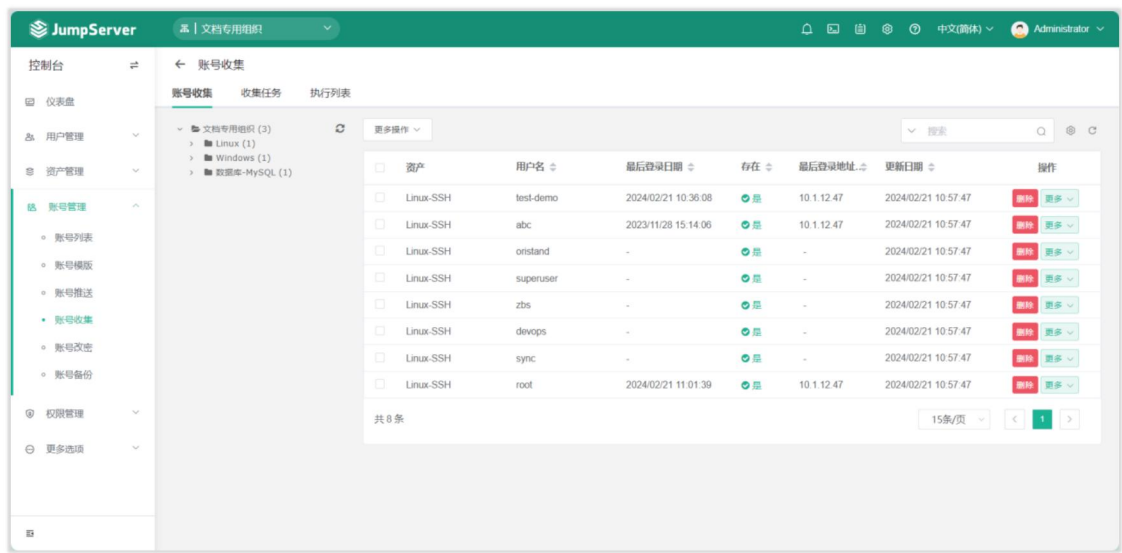


5.4.4. 账号收集

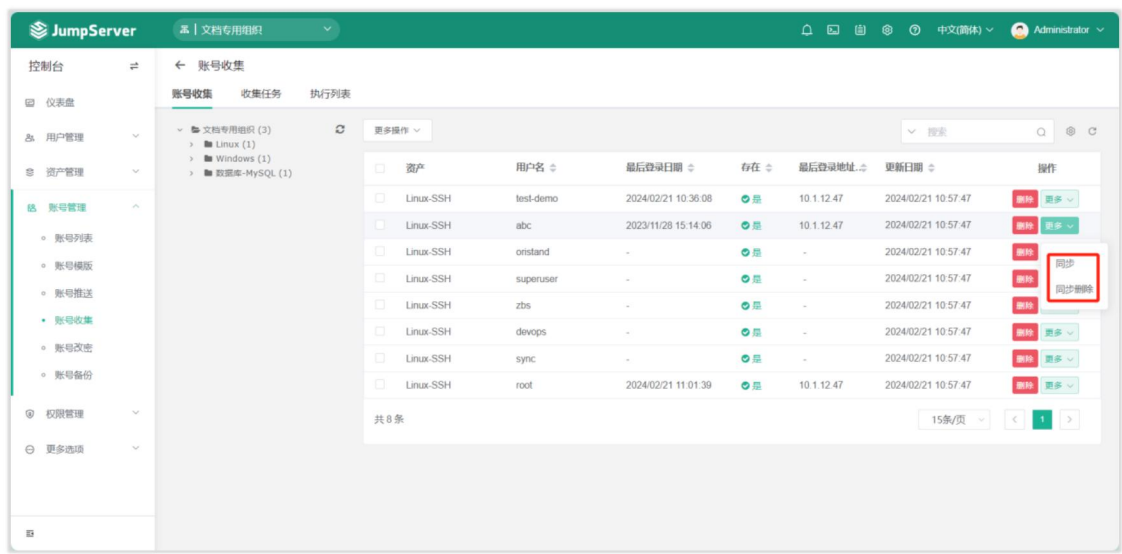
账户收集功能可以收集 JumpServer 纳管的资产上的账户，通过执行任务收集资产账户信息。JumpServer 支持将收集到的账户信息与 JumpServer 纳管的资产绑定，减少人工操作。

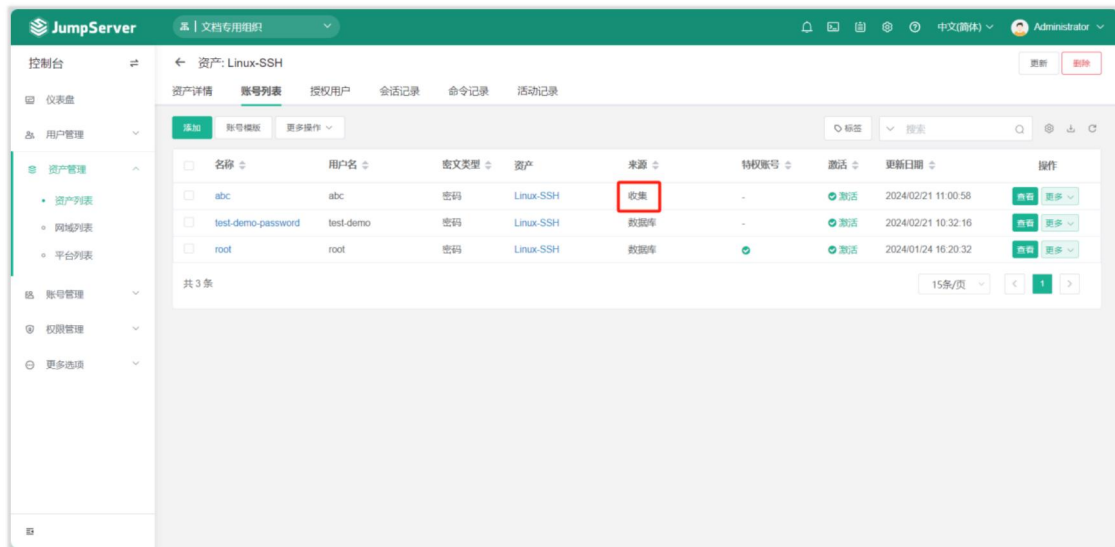
5.4.4.1. 账号收集

账户收集页面可以查看到执行账户收集任务后同步到的所有相关用户。



点击收集到的账户后方的<同步>按钮可以把收集到的用户与对应资产进行绑定。点击收集到的账号后方的<同步删除>按钮可以在服务器上将该账号删除。



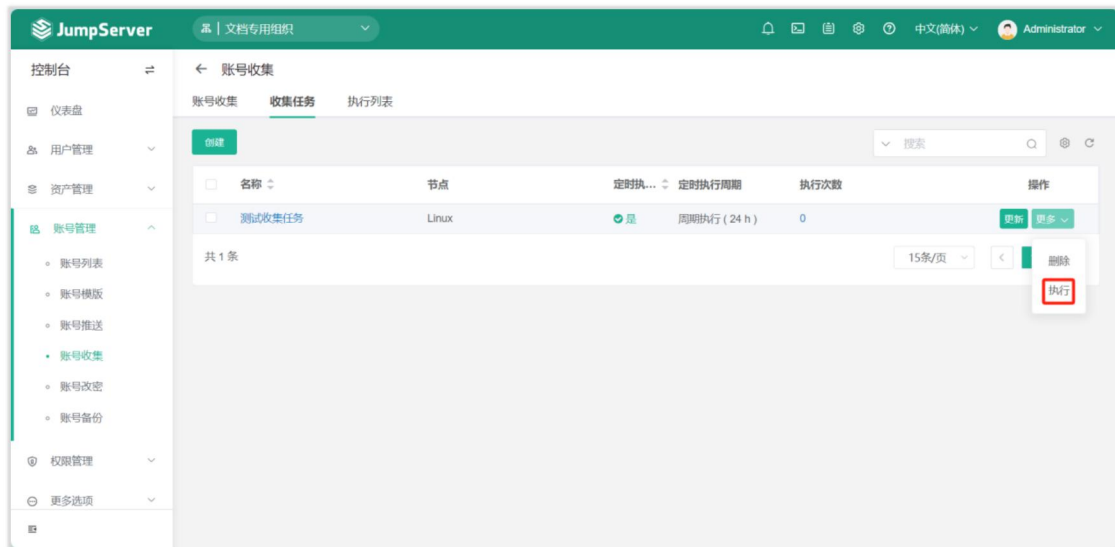


5.4.4.2. 收集任务

点击账户收集页面的收集任务页签中的[创建](#)按钮，创建收集用户任务。根据节点收集资产的用户。JumpServer 支持将收集到的用户自动同步到对应的资产账号下，在创建收集任务时，打开“同步到资产”选项。

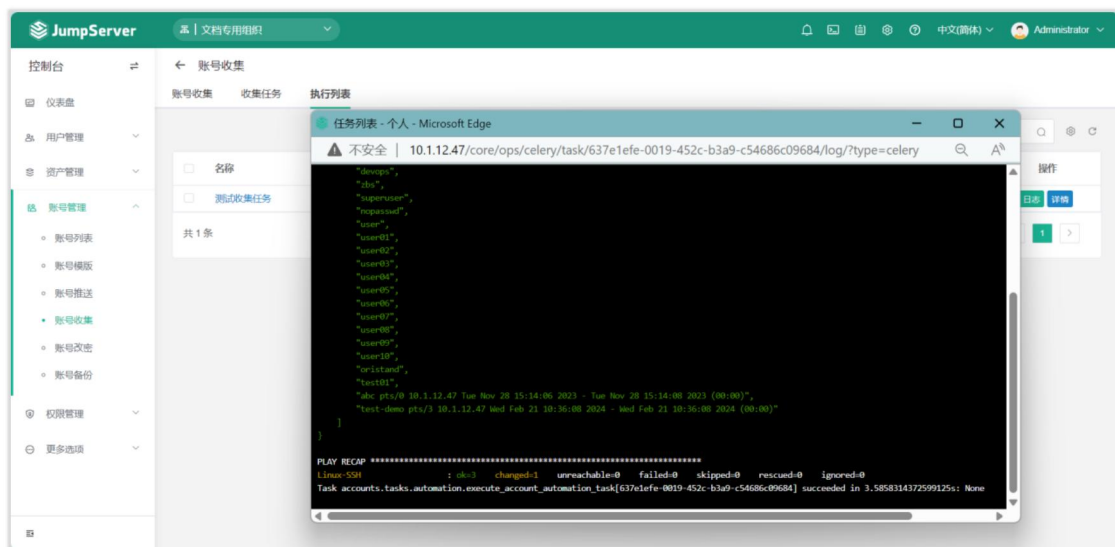


创建成功后，点击收集用户任务后方的更多下拉框选择[执行](#)按钮，即可执行收集用户任务。



5.4.4.3. 执行列表

执行列表页面主要查看收集用户任务执行的详细信息和日志信息。点击对应执行过的日志后方的<日志>按钮或<详情>按钮即可查看任务执行的详细信息。



5.4.5. 账号改密

账号改密是为了满足用户的安全需求，定期修改资产中的用户密码，减少人力操作。账号改密任务更改资产上的用户密码使用该资产的特权账号进行操作【此操作需要资产的账号列表中有特权账号】；账号改密目前不支持更改 Windows 域账号密码。由于修改特权用户的密码为高风险操作，所以 JumpServer 默认不允许修改特权用户的密码；

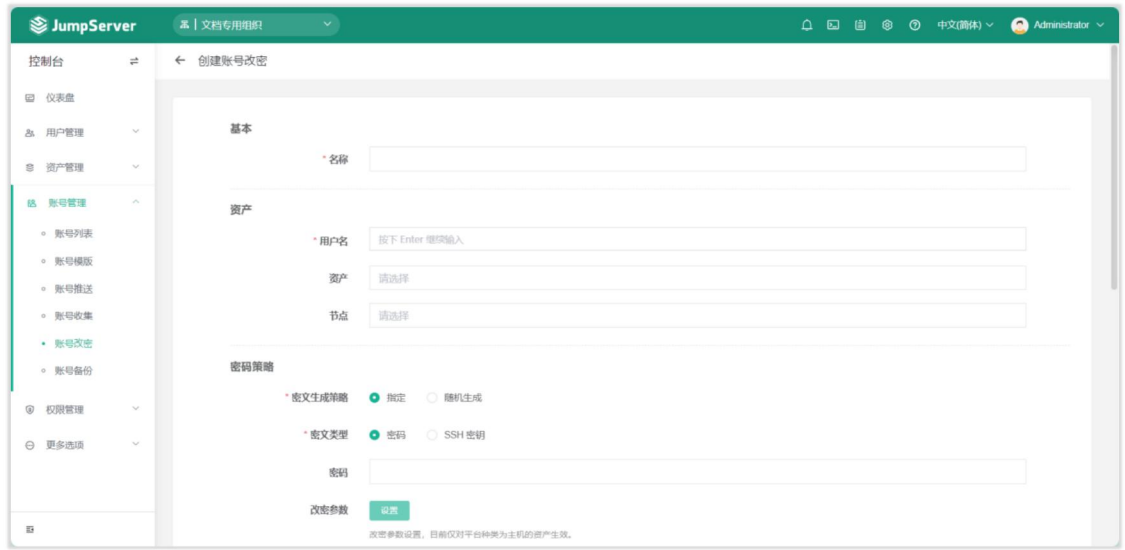
修改资产的特权账号密码的功能默认不开启，需管理员用户在配置文件中添加选项，重启堡垒机后生效。

JumpServer 配置文件默认位于：/opt/jumpserver/config/config.txt

开启修改特权账号密码功能的配置项为：
CHANGE_AUTH_PLAN_SECURE_MODE_ENABLED=false

5.4.5.1. 账号改密

点击账号改密页面的<创建>按钮，创建账号改密自动化任务。

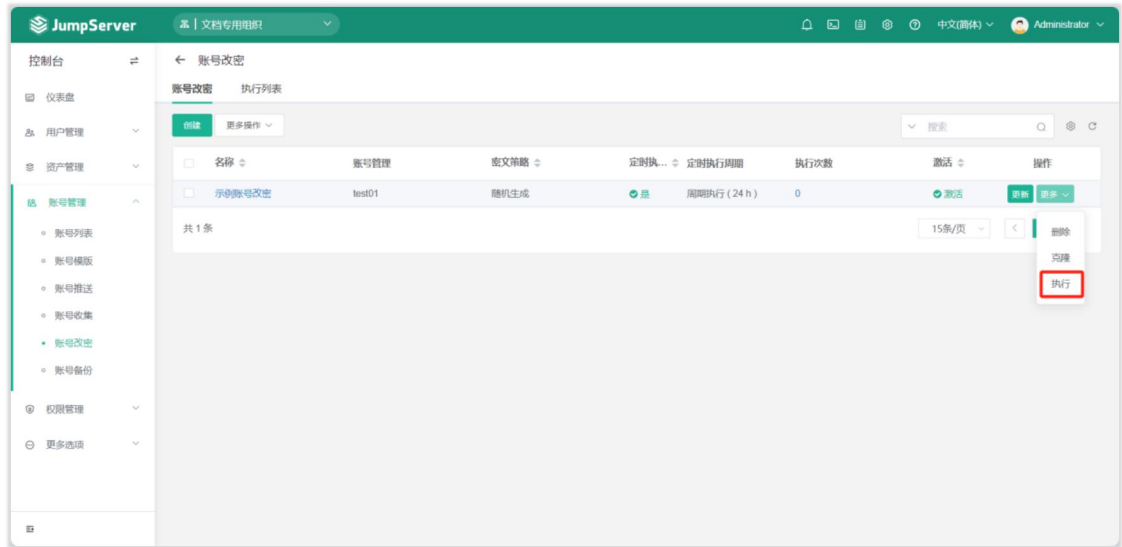


详细参数说明：

参数	说明
名称	账号改密自动化任务的名称
用户名	被改密的用户。
资产	需要被改密的资产。
节点	需要被改密的资产节点组。
密码策略-密文生成策略	选择被改密的用户的密码策略。 <ul style="list-style-type: none">● 指定：管理员用户手动输入密码。● 随机：JumpServer 自行生成密码。
密码策略-密文类型	被修改的用户密文的类型。
密码	选择密文生成策略为指定，管理员用户输入密码。 选择密文生成策略为随机，管理员用户设置密码生成规则，

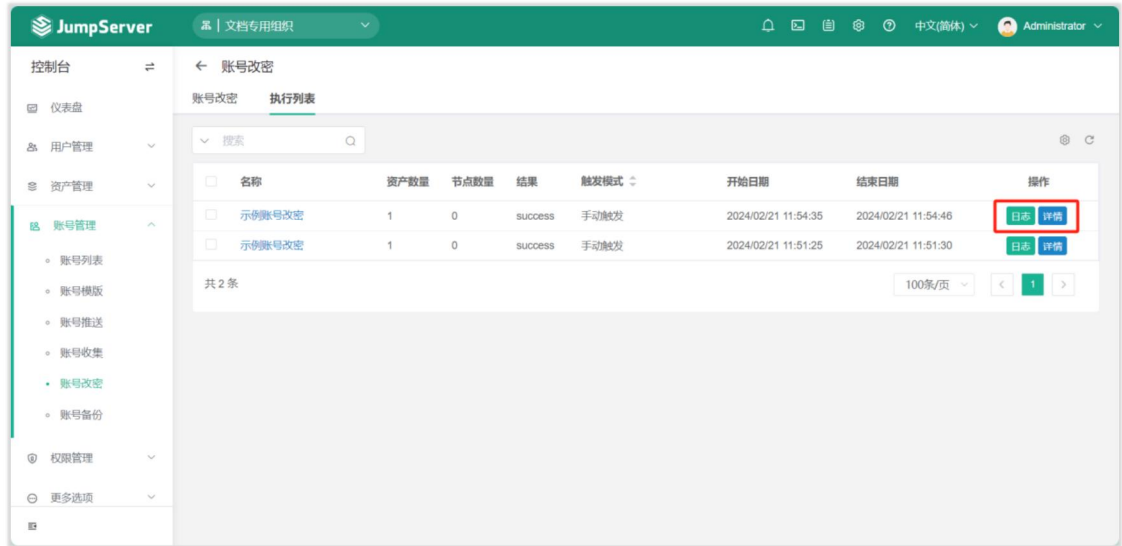
	例如：密码长度、密码强弱规则等等。
定时执行	选择该自动化任务是否定时执行，设置定时任务执行时间。
收件人	选择用户接受改密后的邮件通知信息。

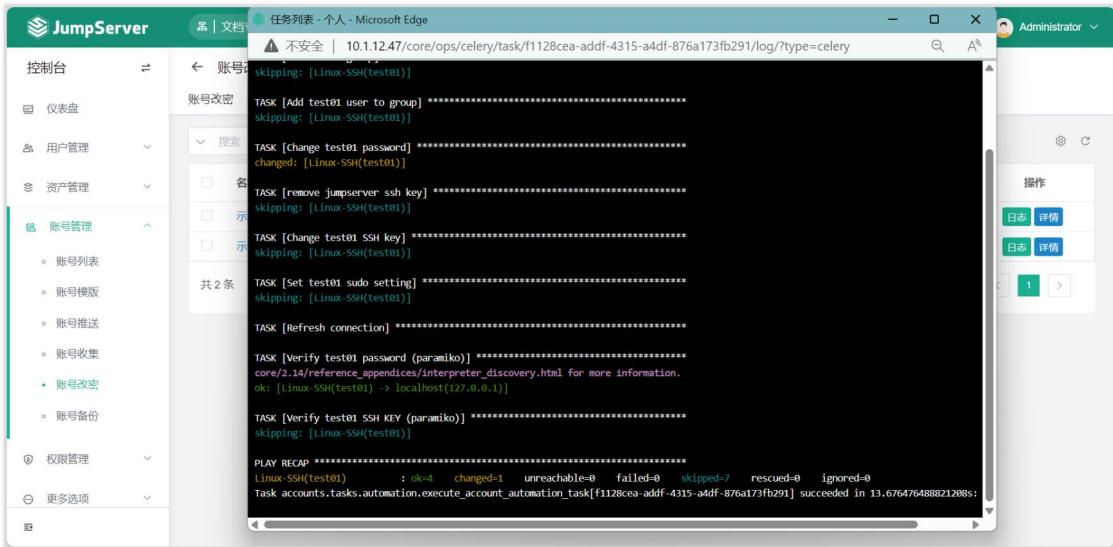
点击账号改密自动化任务后方的<更多>按钮，选择执行即可立即执行自动化任务。



5.4.5.2. 执行列表

该页面主要查看账号改密计划任务的执行日志、任务详情等详细信息。



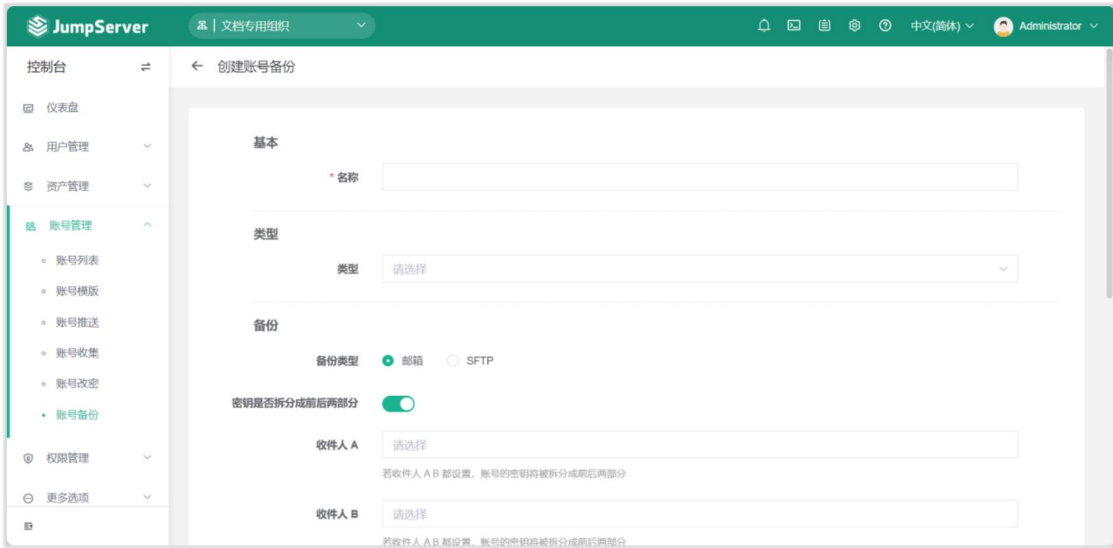


5.4.6. 账号备份

为了防止不可控因素导致服务器出现数据损坏、资产账户丢失等问题，环境无法正常运行的情况，JumpServer 支持了账户备份功能，该功能可备份 JumpServer 上所有的资产账户。备份策略可选择即时备份和定时备份。

5.4.6.1. 账户备份

在账号备份页面点击<创建>按钮，即可创建账号备份自动化任务。

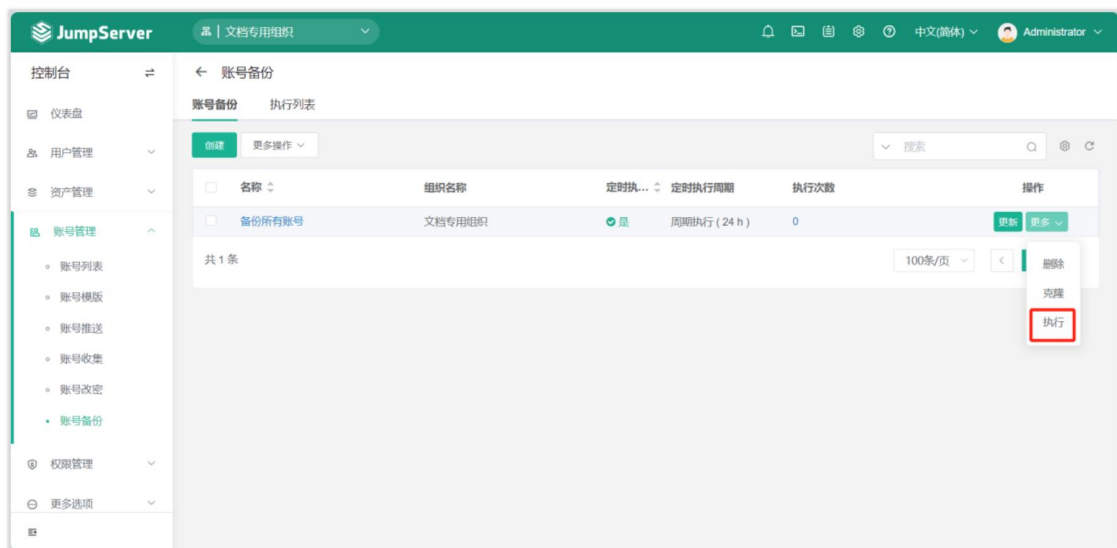


详细参数说明：

参数	说明
----	----

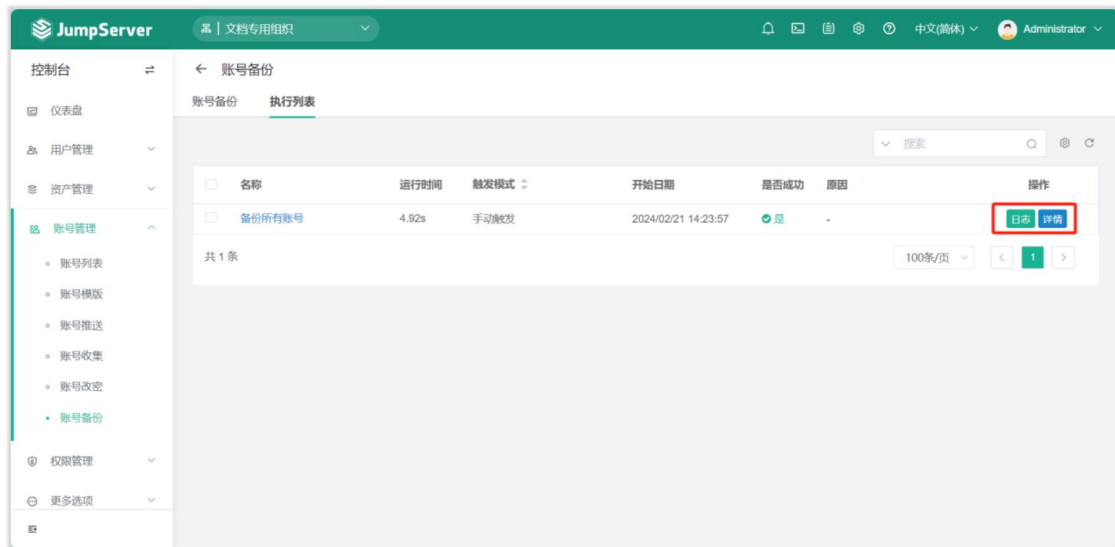
名称	账号备份任务的名称。
类型	需要备份账号的类型，可以根据账号类型创建备份任务。
备份类型	JumpServer 支持将账号通过表格的方式备份到邮箱中，或通过 SFTP 的方式备份。
密钥是否拆分成前后两部分	是否将账号的密钥拆分，保证安全。
收件人 A	备份后的账号会发送一封邮件给用户，设置接收邮件的用户。账号的密钥会被拆分成前后两部分。
收件人 B	备份后的账号会发送一封邮件给用户，设置接收邮件的用户。账号的密钥会被拆分成前后两部分。
定时执行	设置该备份任务是否定时任务，备份任务支持定时执行或手动执行。

点击账号备份任务后方的<更多>按钮，选择<执行>按钮即可立即执行该账号备份任务。



5.4.6.2. 执行列表

该页面主要查看账号备份任务执行的历史记录、执行日志以及账号备份的详细信息。



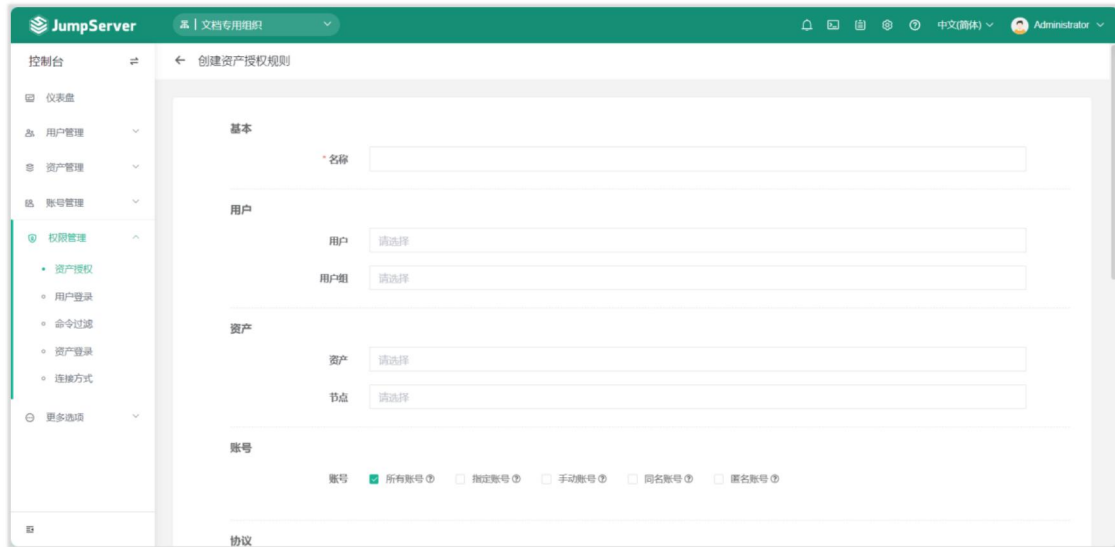
5.5. 权限管理

5.5.1. 资产授权

资产的授权规则通过以下几个维度确定用户能使用那种协议、哪些账号访问哪些资产并且拥有什么样的权限。维度分别如下：

- 用户：用户维度主要包括用户与用户组（代表该用户组下所有的用户）；
- 资产：资产维度主要包括资产、节点（资产组的概念，代表该节点下的所有资产）、账号（登录资产的账号）；
- 账号：账号维度主要区分用户可以用哪些账号登录资产。
- 协议：协议维度主要区分用户登录资产可以使用的协议。
- 动作：动作维度主要包括连接权限、上传、下载、删除权限、复制粘贴权限（仅支持 RDP 协议和 VNC 协议）。

点击资产授权页面的[<创建>](#)按钮，即进入资产授权创建页面。



详细参数说明：

参数	说明
名称	授权规则的名称。
用户	JumpServer 登录用户，即给该用户授权资产的连接或其它权限。
用户组	JumpServer 登录用户组，即给该用户组授权资产的连接或其它权限。
资产	授权的资产，即用户需求连接的资产。
节点	授权的节点，即用户需求连接的资产组。
账号	<p>授权资产登录的账号。</p> <ul style="list-style-type: none"> ● 所有账号：资产上添加的所有账号都授权； ● 指定账号：手动输入需要授权的账号名称； ● 手动输入：授权用户连接时自行输入用户名/密码； ● 同名账号：授权用户连接时使用与 JumpServer 登录用户同名的账号； ● 匿名账号：授权用户连接时不代填任何认证信息，仅拉起应用本身。（适用于 Web 和自定义类型的资产）
协议	<p>授权用户可用的协议。</p> <ul style="list-style-type: none"> ● 所有：用户可以使用堡垒机支持的任意协议登录资产； ● 指定协议：用户可以使用指定协议登录资产。
动作	授权的动作，即用户对资产可以做什么。剪切板权限控制目前仅支持 RDP/VNC 协议的连接。
开始日期	该授权规则开始的时间，默认为该授权规则创建的时间。

失效日期	该授权规则失效的时间。
------	-------------

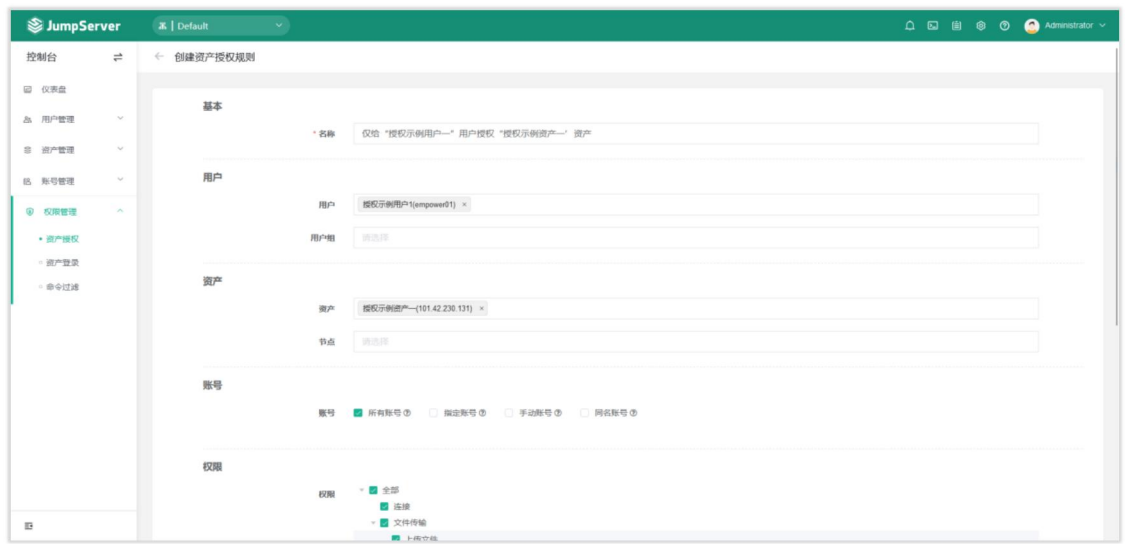
以下示例每一次新的授权规则创建前都会删除原授权规则，原授权规则对新创建的授权规则无影响。

5.5.1.1. 仅给某个用户授权某资产

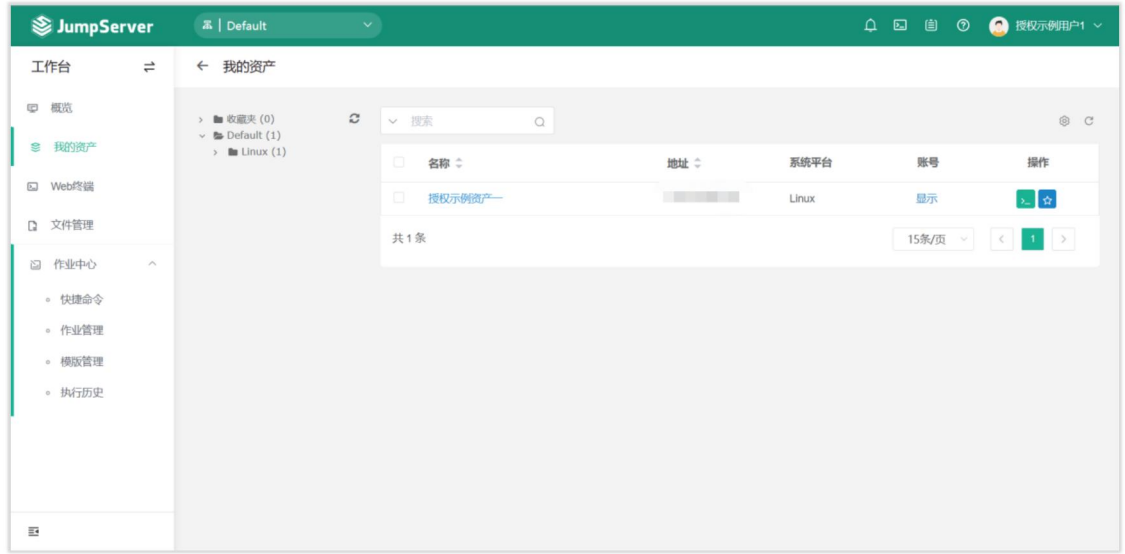
当需求仅给某个用户授权某资产时：

- ◆ 选择将【用户模块】中的“用户”选项选择为需要授权的用户，“用户组”选项置空；
- ◆ 选择将【资产模块】中的“资产”选项为需要登录的资产，“节点”选项为空，“账号”选择授权的账号，示例选择“所有账号”。

授权规则如下：



授权结果：

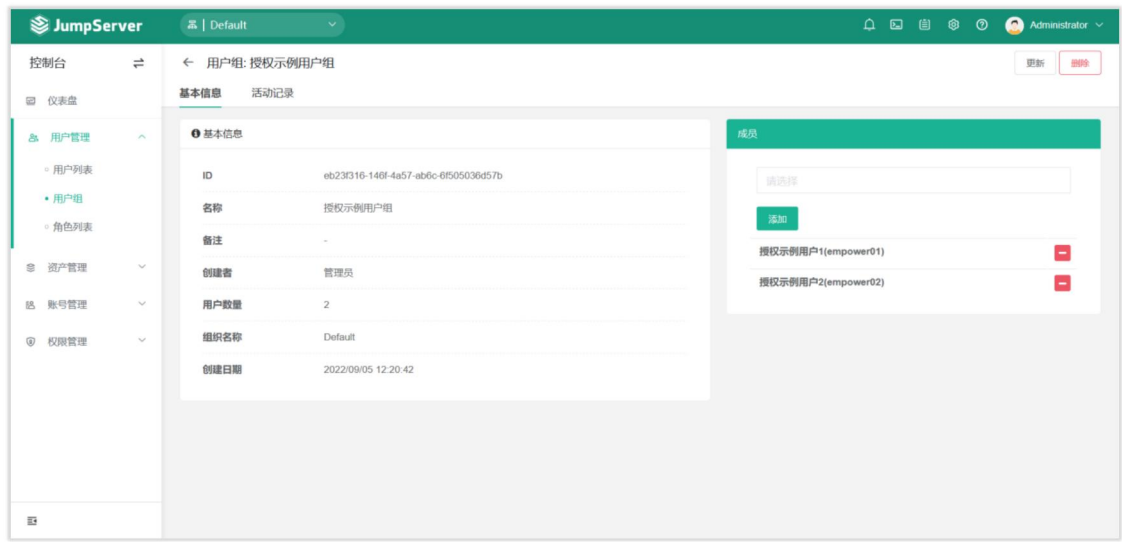


5.5.1.2. 给某个用户组授权某资产

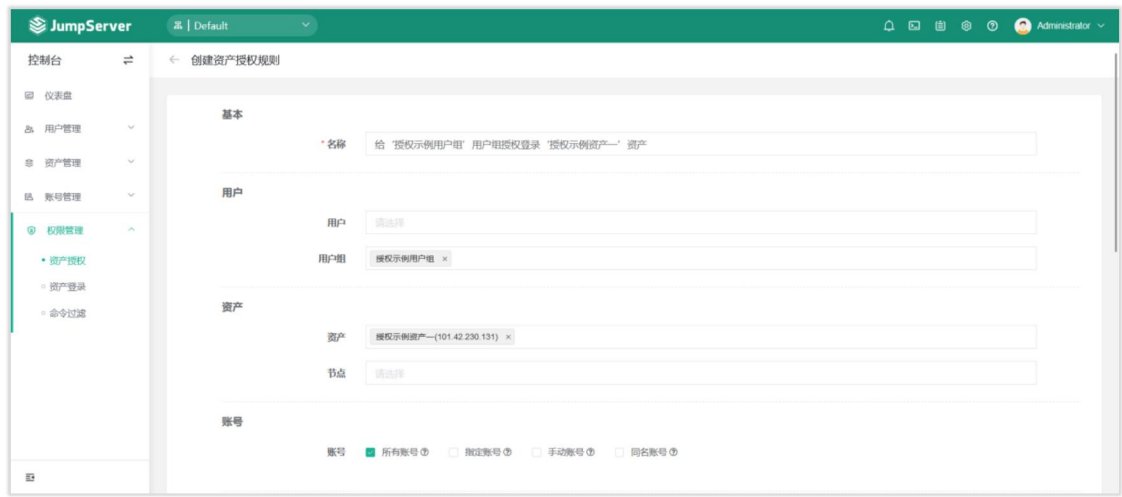
当针对与允许某个用户组登录一个资产时：

- ◆ 选择将【用户模块】中“用户组”选项选择为需要授权的用户组，“用户”选项为空；
- ◆ 将【资产模块】中的“资产”选项选择为需要登录的资产，“节点”选项为空，账号”选择授权的账号，示例选择“所有账号”。

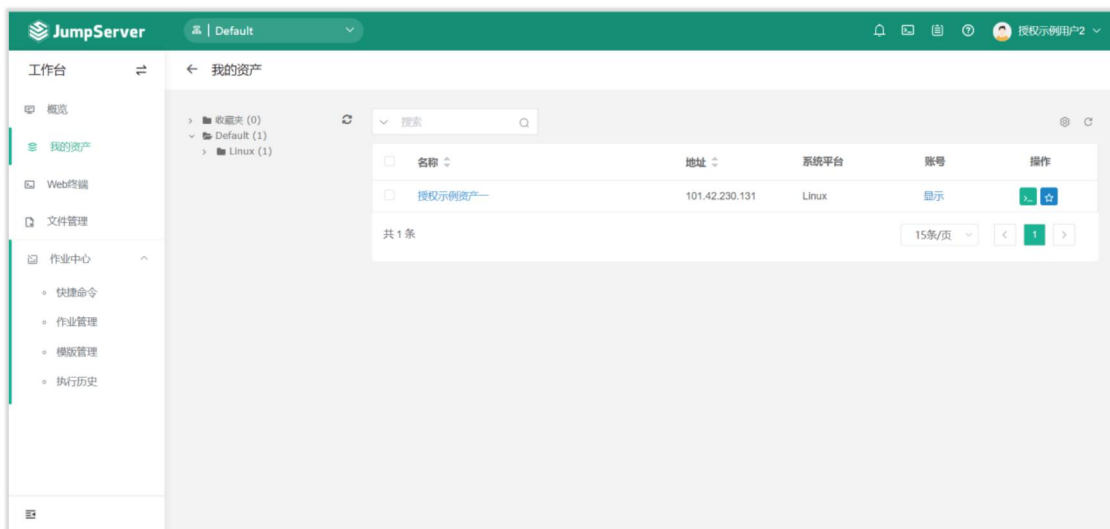
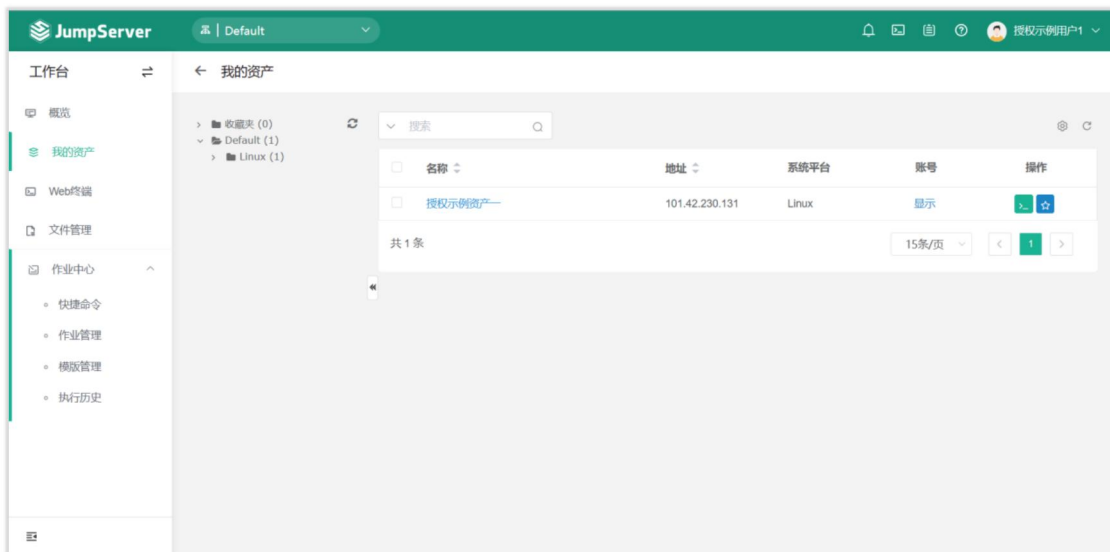
授权用户组拥有的用户：



授权规则如下：



授权结果如下：

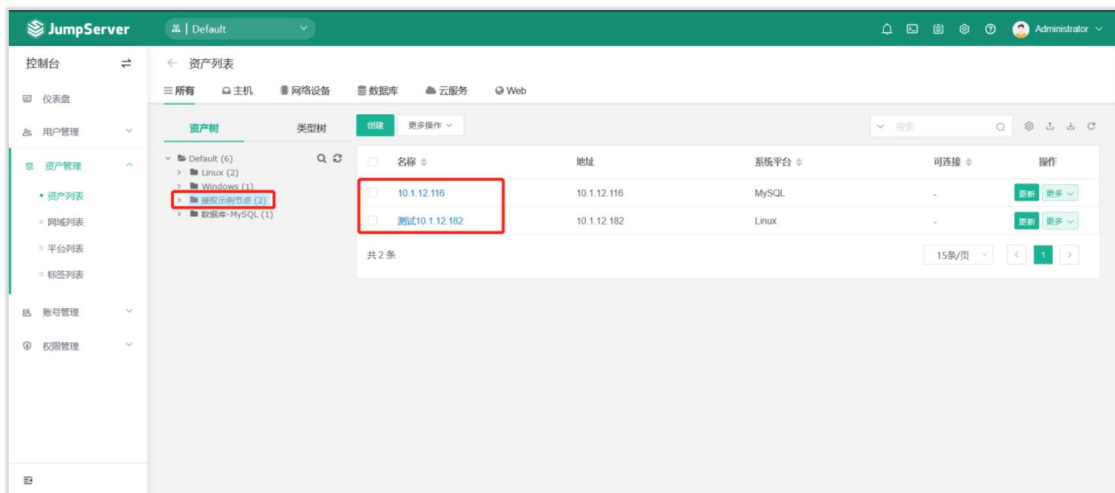


5.5.1.3. 给某个用户授权某节点

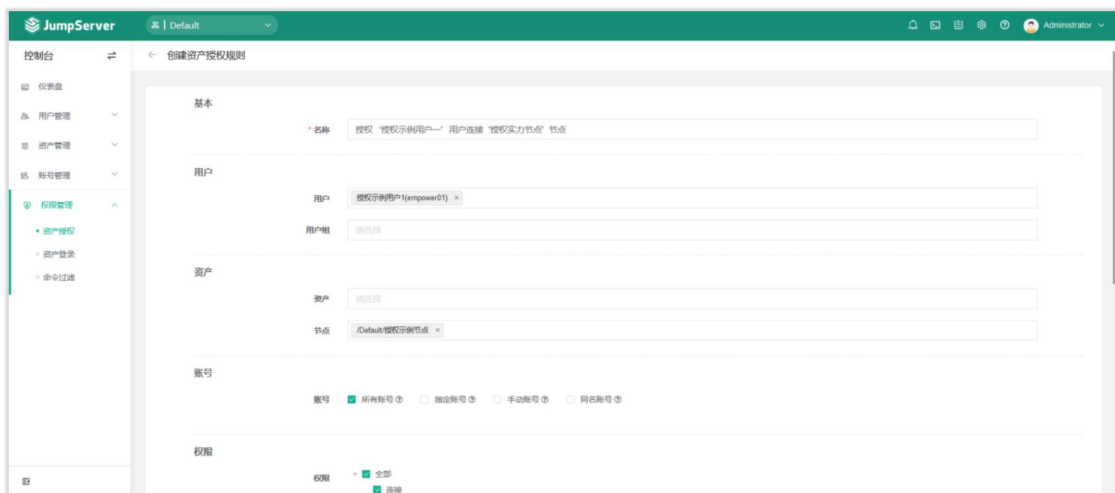
当针对与允许某个用户登录某一组资产时：

- ◆ 选择将【用户模块】中“用户”选项选择为需要授权的用户，“用户组”选项为空；
- ◆ 将【资产模块】中的“节点”选项选择为需要登录的资产组，“资产”选项为空，账号”选择授权的账号，示例选择“所有账号”。

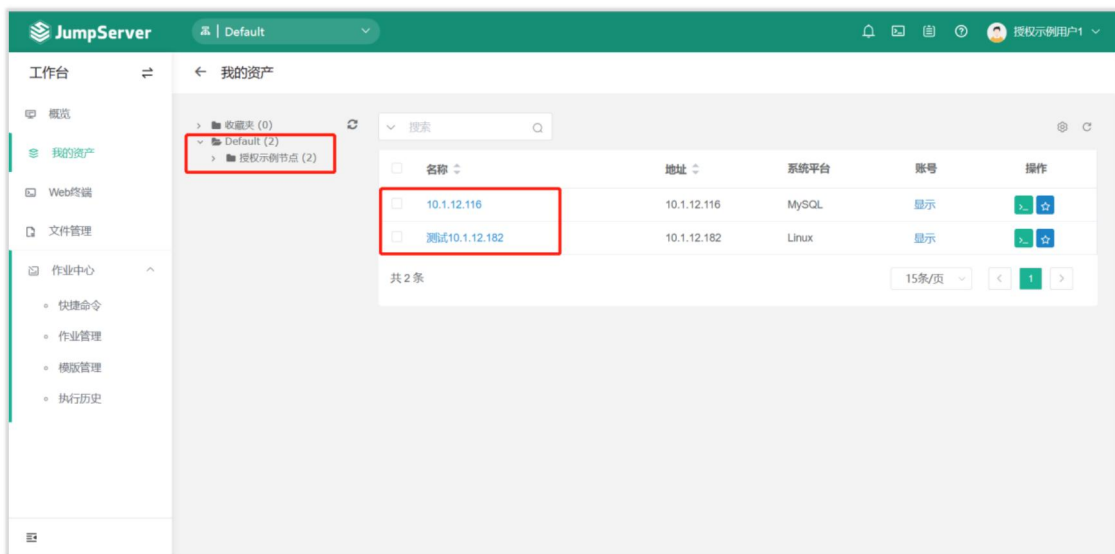
授权示例节点中包含的资产如下：



授权规则如下：



授权结果如下：

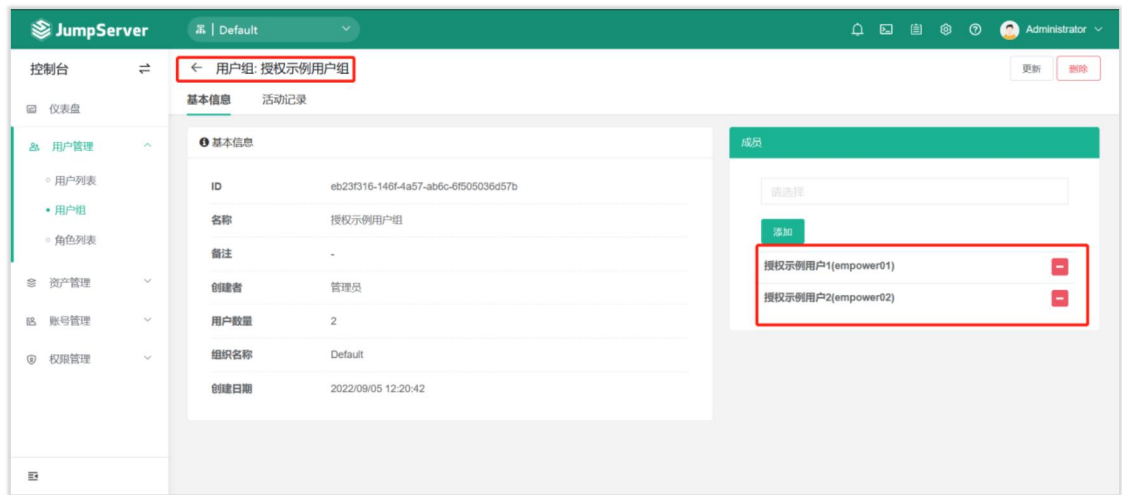


5.5.1.4. 给某个用户组授权某节点

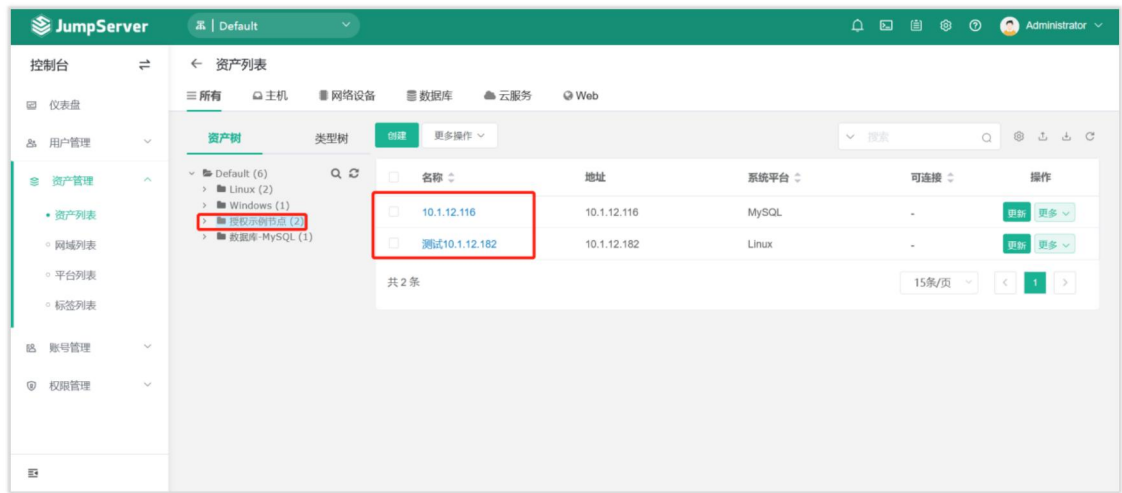
当允许某个用户组登录某一组资产时：

- ◆ 选择将【用户模块】中“用户组”选项选择为需要授权的用户组，“用户”选项为空；
- ◆ 将【资产模块】中的“节点”选项选择为需要登录的资产组，“资产”选项为空，账号”选择授权的账号，示例选择“所有账号”。

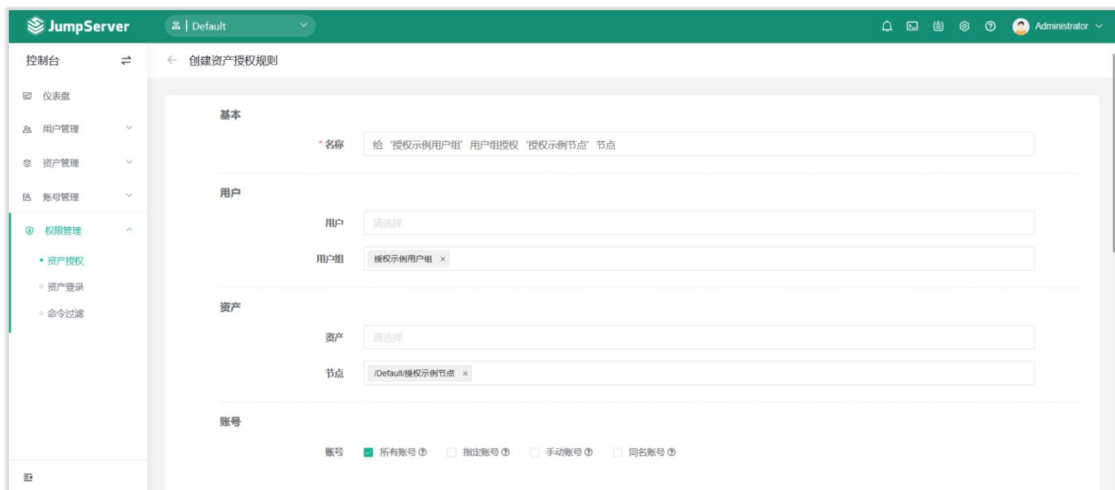
用户组包含的用户如下：



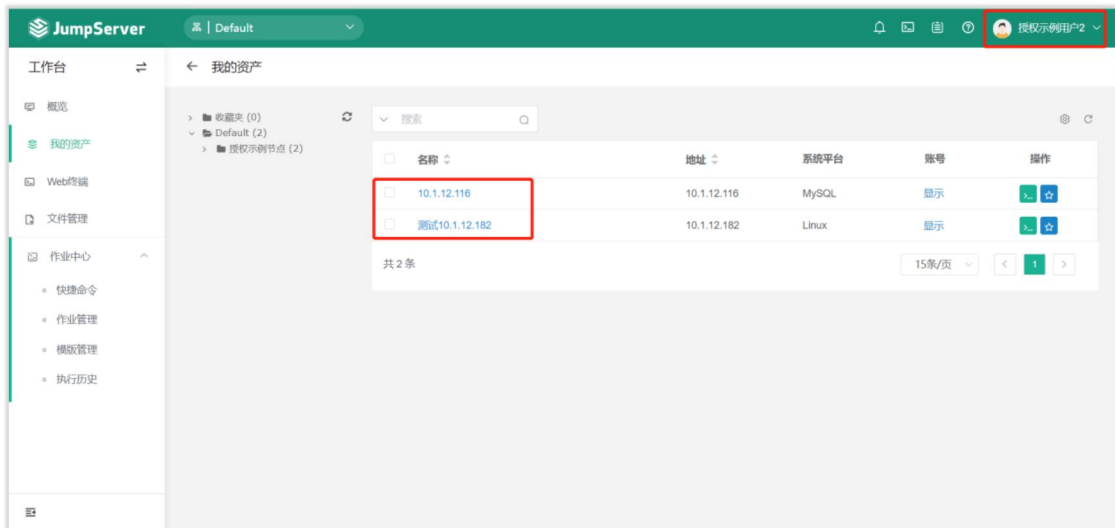
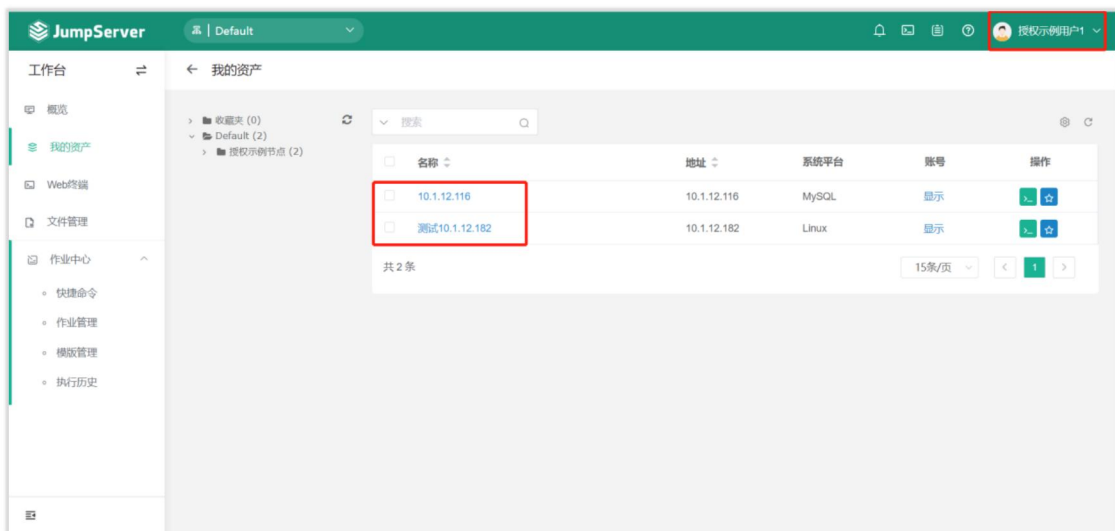
授权示例节点包含的资产如下：



授权规则如下：



授权结果如下：

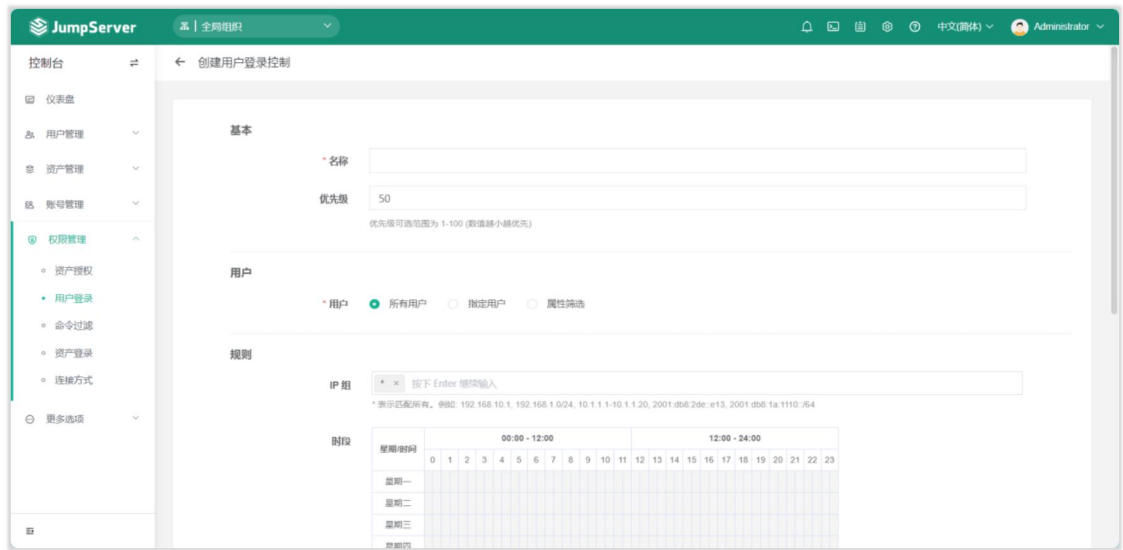


5.5.1.5. 其它

- A. 授权规则模块中的任何选项都为空的情况下，该授权规则不起任何作用。
- B. 授权规则模块中的任一模块选项都为空的情况下，该授权规则不起任何作用。
- C. 授权规则不能使用“*”进行全匹配。

5.5.2. 用户登录

JumpServer 支持在用户登录 JumpServer 时, 针对用户的登录 IP 段与登录时间段设置用户登录规则。用户登录规则可以针对所有用户、指定用户以及属性匹配到的用户。用户登录规则可以在用户详情页中进行设置，也可以在权限管理模块进行设置。当 JumpServer 用户登录匹配到某一条用户登录规则时，会根据该规则的动作执行，如果没有匹配到对应规则，用户即正常执行。用户登录规则在全局组织中设置生效。



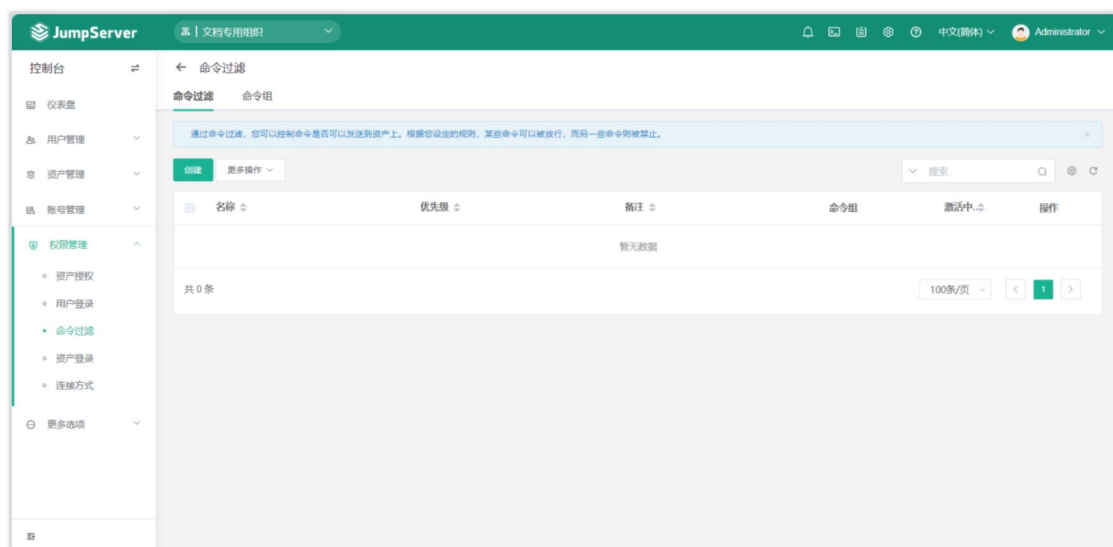
详细参数说明：

参数	说明
名称	指定该登录规则的名称。
优先级	指定该登录规则生效的优先级，优先值可选范围为 1~100，数字越小优先级越高。
用户	指定该登录规则匹配的用户。 <ul style="list-style-type: none">● 所有用户：该登录规则匹配所有用户。● 指定用户：该登录规则匹配指定用户。● 属性筛选：该登录规则匹配属性规则匹配到的用户。

IP 组	指定该登录规则生效所限制的登录 IP，格式为逗号分隔的字符串，*表示匹配所有。例如:192.168.10.1, 192.168.1.0/24, 10.1.1.1-10.1.1.20, 2001:db8:2de::e13, 2001:db8:1a:1110::/64。该 IP 是指用户登录时的 IP。
时段	指定该登录规则所限制的用户登录时间段。
动作	指定该登录规则被执行时的动作。 <ul style="list-style-type: none"> ● 拒绝：当用户登录匹配到上述规则拒绝该用户登录。 ● 接受：当用户登录匹配到上述规则接受该用户登录。 ● 审批：当用户登录匹配到上述规则发送工单给审批人员，审批人员通过后允许用户登录。 ● 通知：当用户登录匹配到上述规则时，发送通知信息给指定的用户。
激活中	指定该登录规则是否生效。

5.5.3. 命令过滤

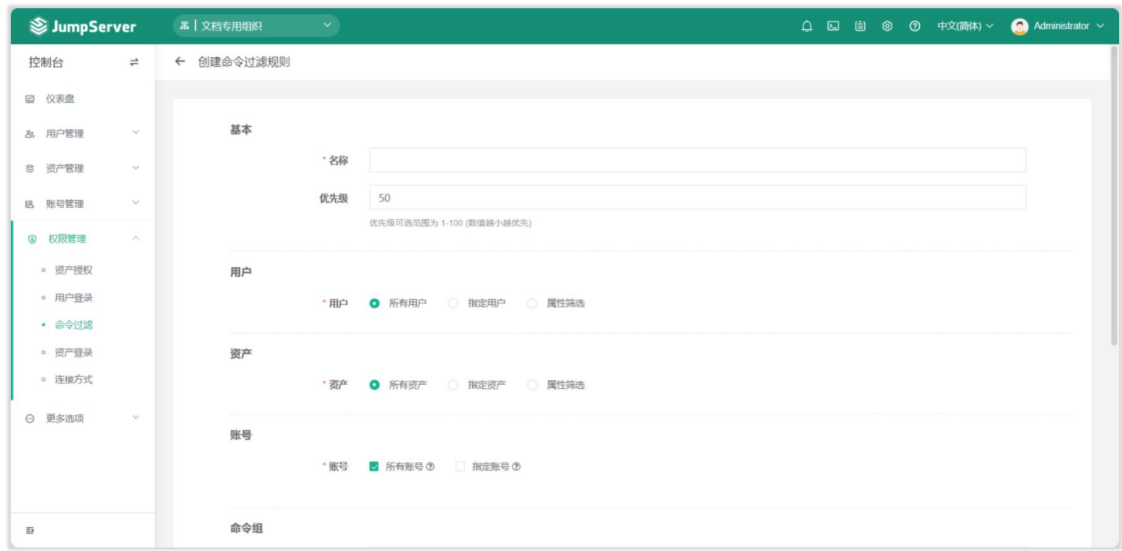
JumpServer 支持对会话过程中使用的命令进行过滤，设置命令过滤规则。命令过滤器可以绑定 JumpServer 用户、资产、连接资产使用的用户，一个命令过滤可以绑定多个命令组。当绑定的用户用资产绑定账号去连接绑定的资产执行命令时，这个命令需要被绑定过滤器的所有命令组进行匹配，高优先级先被匹配；当某一条规则被匹配到后，会根据该规则的动作执行，如果没有匹配到对应的规则，命令即正常执行。



5.5.3.1. 命令过滤

该页面可以针对命令过滤器进行创建、删除、更新、查看。点击命令过滤页面中的命令过滤页签进入命令过滤器设置页面。

创建：点击该页面左上角的<创建>按钮，即可创建命令过滤器。

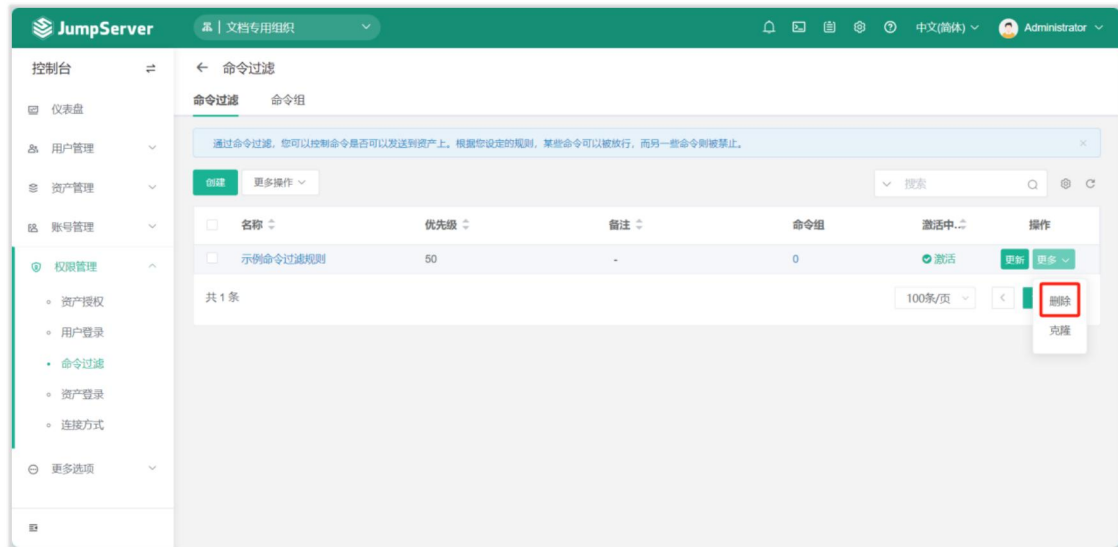


详细参数说明：

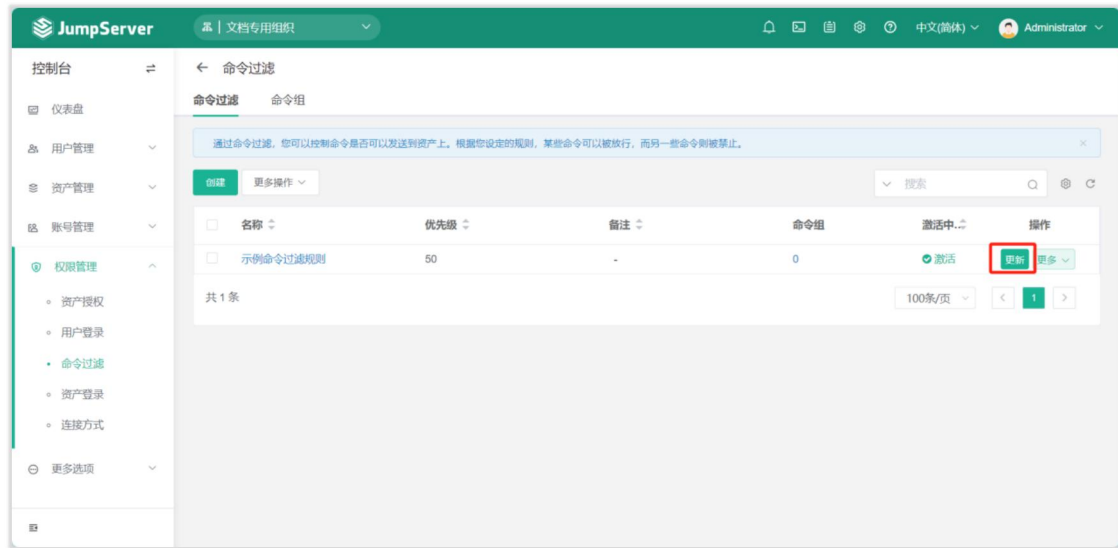
参数	说明
名称	命令过滤器的名称
优先级	命令过滤器的优先级，优先级可选范围为 1~100，数值越小规则匹配越优先，默认为 50。
用户	该命令过滤器匹配的 JumpServer 用户。 <ul style="list-style-type: none">● 所有用户：该命令过滤器匹配所有 JumpServer 用户；● 指定用户：该命令过滤器匹配指定 JumpServer 用户；● 属性筛选：该命令过滤器匹配属性过滤规则匹配的用户；
资产	该命令过滤器匹配的资产信息。 <ul style="list-style-type: none">● 所有资产：该命令过滤器匹配所有资产；● 指定资产：该命令过滤器匹配指定资产；● 属性筛选：该命令过滤器匹配属性过滤规则匹配的资产；
账户	该命令过滤器匹配的资产账号。 <ul style="list-style-type: none">● 所有账号：该命令过滤器匹配到的资产所有账号；● 指定账号：该命令过滤器匹配到的资产指定账户；
命令组	该命令过滤器关联的命令组，当匹配到的 JumpServer 使用匹配到的账号登录匹配到的资产执行这些命令时执行相应的动

	作。
动作	<p>匹配到该命令过滤器规则时做出的动作。</p> <ul style="list-style-type: none">● “拒绝”：拒绝执行命令；● “接受”：允许执行命令；● “审批”：经过设置的审批人审批允许或者拒绝命令。● “告警”：当匹配导指令时，发送告警信息给指定人员。

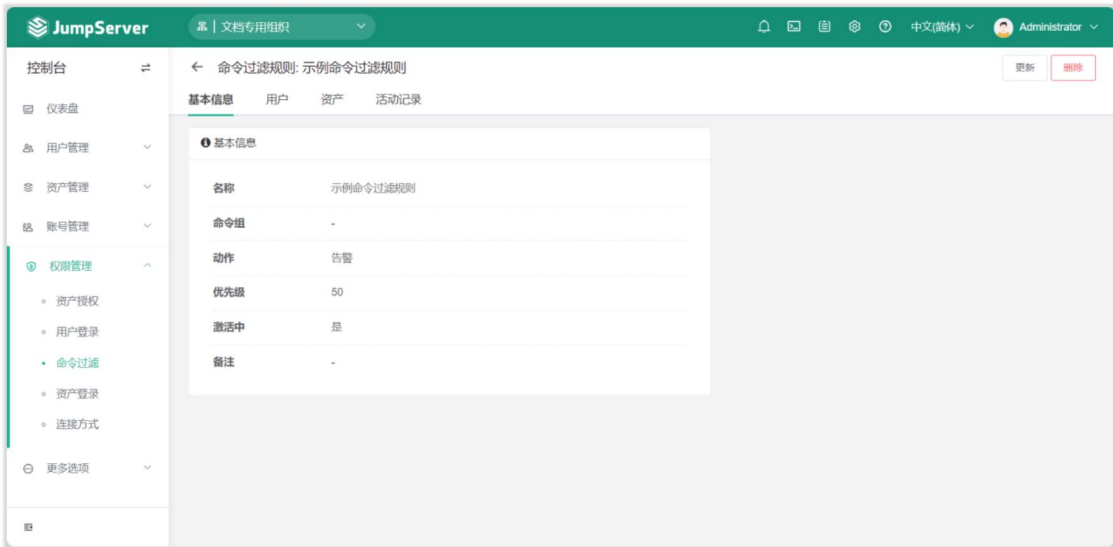
删除： 点击需要删除的命令过滤器后方的<更多>按钮，选择<删除>按钮，即可删除命令过滤器。



更新： 点击需要更新的命令过滤器后方的<更新>按钮，填写对应需要更新的信息，即可更新命令过滤器信息。



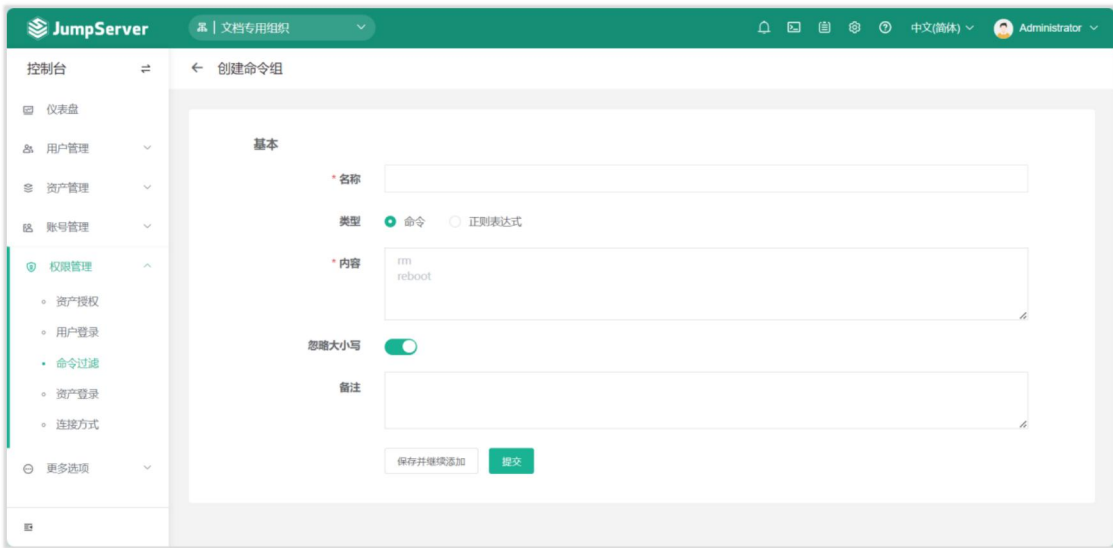
查看： 点击命令过滤器的名称，可查看该命令过滤器的具体信息，包括该命令过滤器基本信息、绑定的用户信息、绑定的资产信息与该命令过滤器的活动记录。



5.5.3.2. 命令组

命令组可以绑定到命令过滤器中，命令组中可以创建两种命令组，分别是正则表达式和命令。

创建： 点击该页面左上角的<创建>按钮，即可创建命令过滤器。

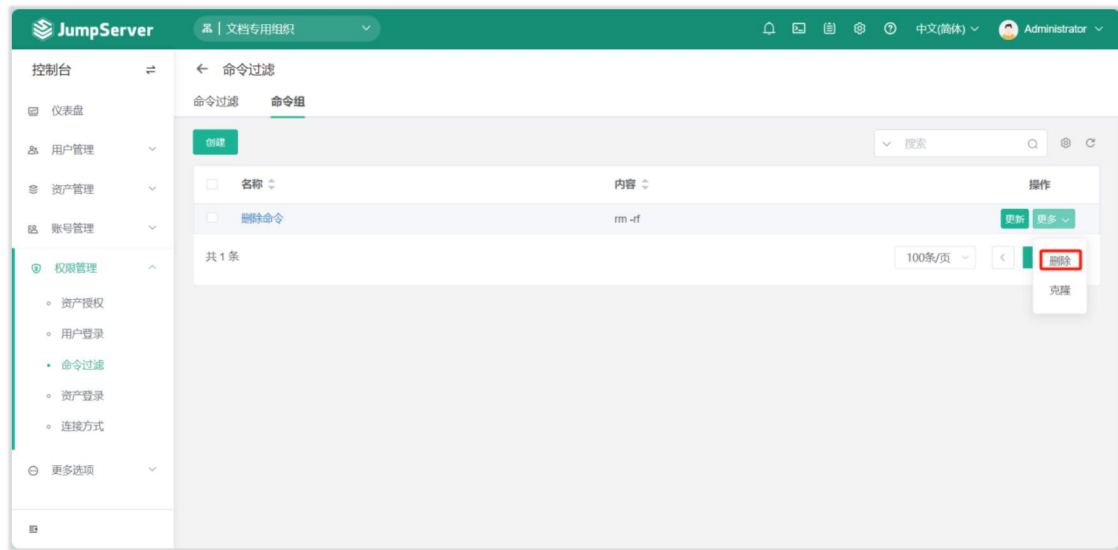


详细参数说明：

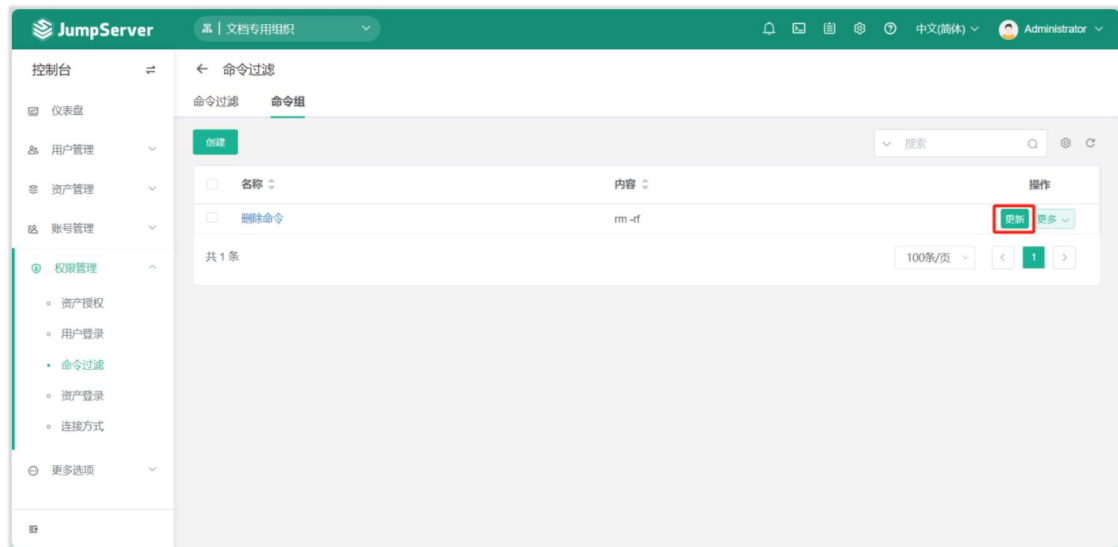
参数	说明
名称	命令组的名称。
类型	正则表达式表示通过正则表达式进行命令匹配，命令则表示过滤某固定命令。
内容	内容可以是多行文本，每一行代表一条匹配规则。

忽略大小写	指将填入的命令不论大小写，一律按规则进行筛选。
-------	-------------------------

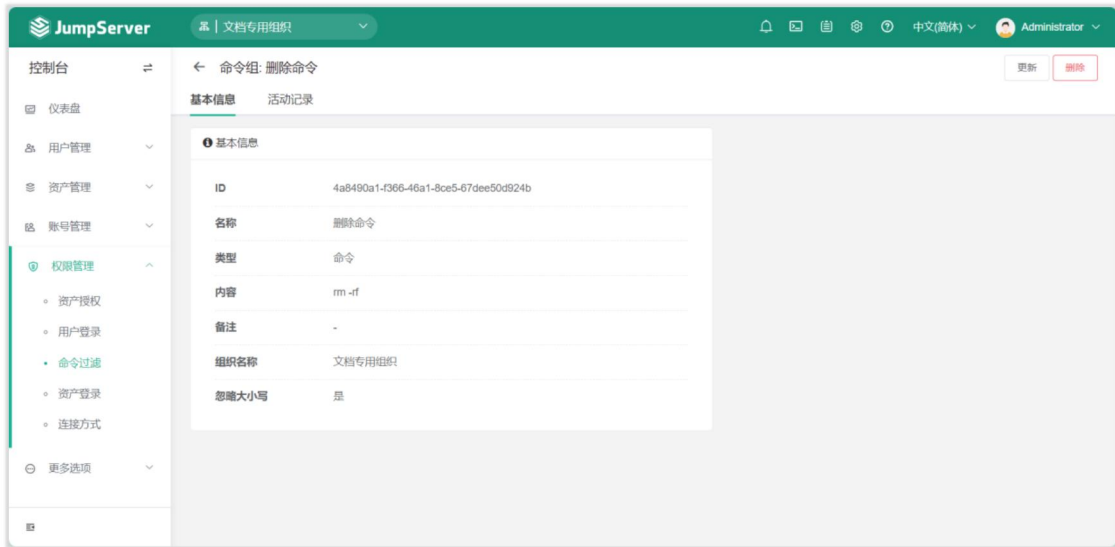
删除： 点击需要删除的命令组后方的<更多>按钮，选择<删除>按钮，即可删除命令组。



更新： 点击需要更新的命令组后方的<更新>按钮，填写对应需要更新的信息，即可更新命令组信息。

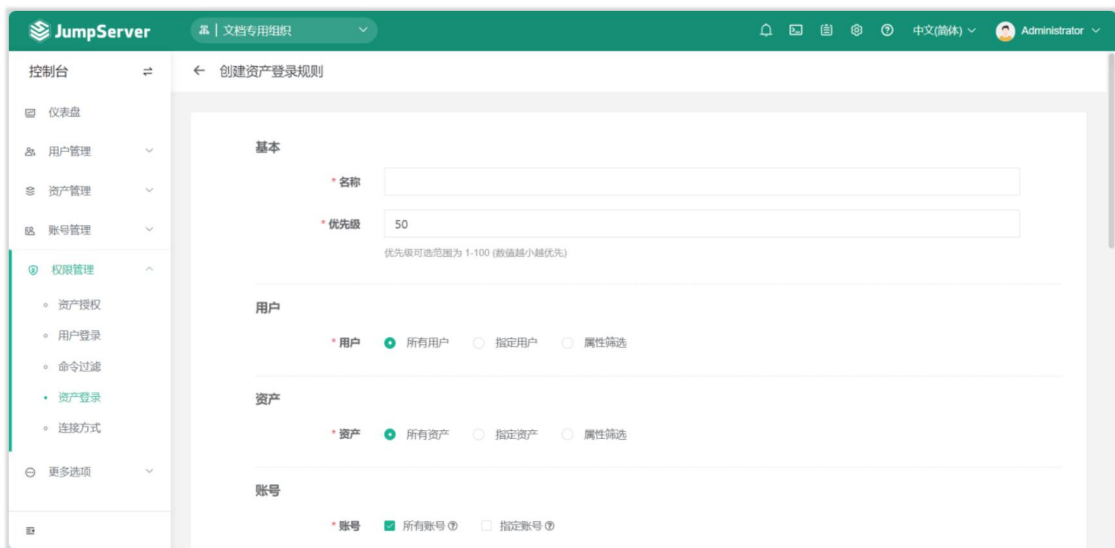


查看： 点击命令组的名称，可查看该命令组的具体信息，包括该命令组的基本信息与活动记录。



5.5.4. 资产登录

JumpServer 支持对资产登录进行二次复核功能。依据安全策略，系统可以针对 JumpServer 登录用户、资产信息、账号信息、匹配规则四个维度对资产的登录设置动作限制，当设置二次复核动作时，审批人审批资产登录。JumpServer 登录用户、资产信息、账号信息、规则信息、动作五种限制可以组合使用。



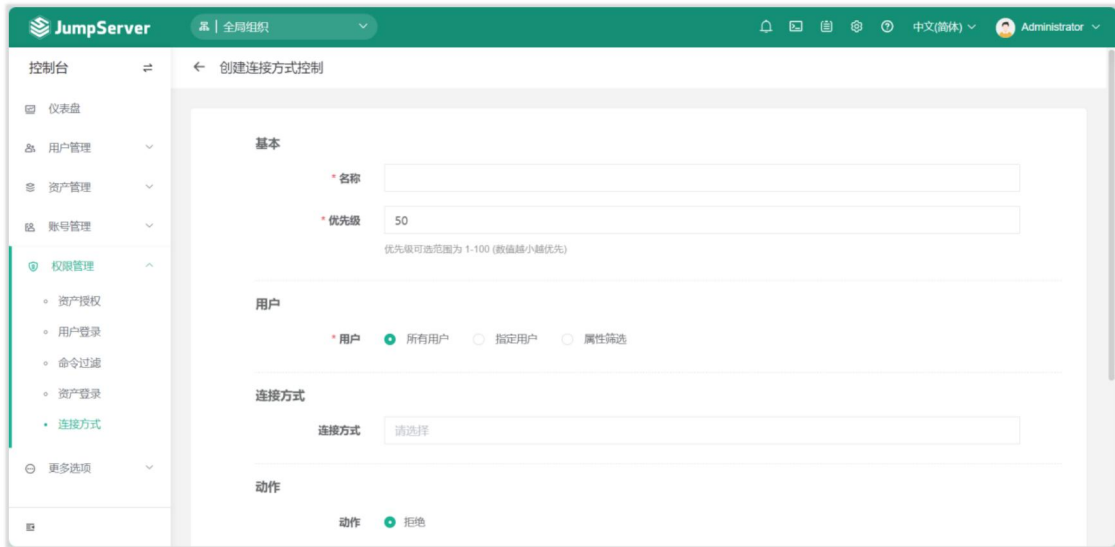
详细参数说明：

参数	说明
名称	资产登录规则的名称。
优先级	资产登录规则的优先级，优先级可选范围为 1~100，数值越

	小规则匹配越优先，默认为 50。
用户	<p>当使用该用户登录 JumpServer 堡垒机连接下面选项的资产时匹配该资产登录规则。</p> <ul style="list-style-type: none"> ● 所有用户：所有用户均匹配该资产登录规则； ● 指定用户：指定某些用户匹配该资产登录规则； ● 属性筛选：创建属性筛选规则，匹配筛选规则的用户匹配该资产登录规则；
资产	<p>当连接该资产时匹配该资产登录规则。</p> <ul style="list-style-type: none"> ● 所有资产：连接所有资产时匹配该资产登录规则； ● 指定资产：连接指定资产时匹配该资产登录规则； ● 属性筛选：创建属性筛选规则，匹配筛选规则的资产匹配该资产登录规则；
账号	<p>当 JumpServer 使用该账号登录资产时匹配该资产登录规则。</p> <ul style="list-style-type: none"> ● 所有账户：匹配到的资产使用任何账号登录都匹配该资产登录规则； ● 执行账户：匹配到的资产使用指定账号登录都匹配该资产登录规则；
规则-登录 IP	当匹配到上述 JumpServer 用户、资产、账户时，匹配 JumpServer 用户的登录 IP。
规则-时段	当匹配到上述 JumpServer 用户、资产、账户时，匹配 JumpServer 用户的登录时间段。
动作	<p>匹配到该资产登录规则时做出的动作。</p> <ul style="list-style-type: none"> ● “拒绝”：拒绝登录资产； ● “接受”：允许登录资产； ● “审批”：经过设置的审批人审批允许或者拒绝登录。该方式生成的会话信息，工单审批人可以在工单中对会话进行控制，例如暂停，恢复，终端，监控。 ● “通知”：当匹配到上述规则时，发送消息给审批人。

5.5.5. 连接方式

JumpServer 针对于不同的资产类型，提供多种连接方式，例如：命令行方式（Web CLI）、图形界面（Web GUI）、客户端方式、远程应用方式。JumpServer 支持控制用户使用某种连接方式登录到资产上。



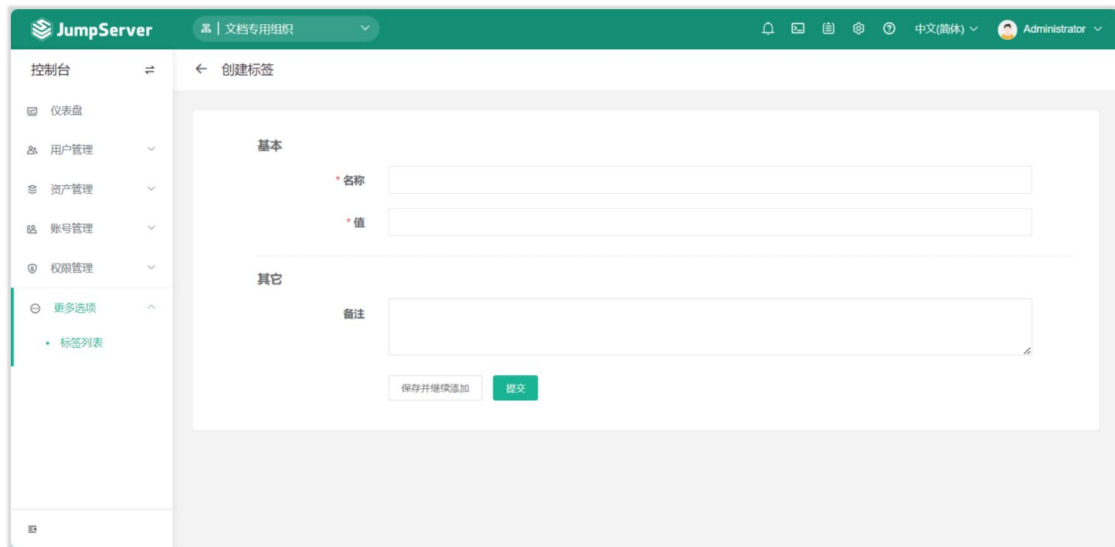
详细参数说明：

参数	说明
名称	控制连接方式规则的名称。
优先级	控制连接方式的规则的优先级。优先级可选范围为 1~100，数值越小规则匹配越优先，默认为 50。
用户	该规则匹配的用户信息： <ul style="list-style-type: none">● 所有用户：该规则适配所有用户；● 指定用户：该规则适配指定用户；● 属性筛选：该规则适配符合属性筛选的用户；
连接方式	选择匹配该规则的资产连接方式。
动作	匹配到该资产登录规则时做出的“拒绝”动作。

5.6. 更多选项

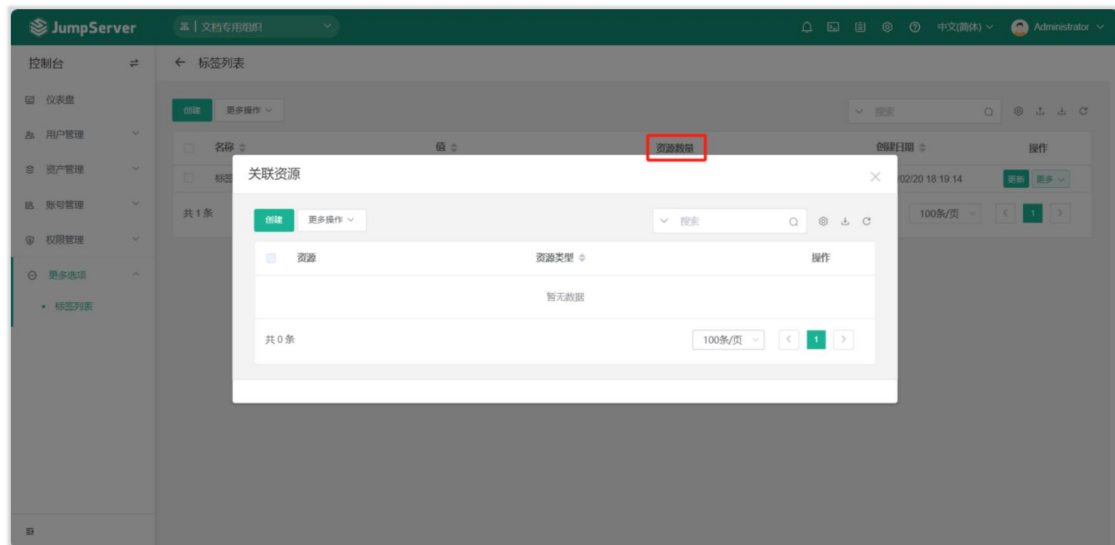
5.6.1. 标签列表

JumpServer 支持标签功能。将资产、用户、账号打上标签便于查询和管理，可以由用户自定义资源的各种属性作为标签，方便归类汇总分析。点击页面左上角[创建](#)按钮，进入标签创建页面。



标签信息有名称和值：名称可以是描述功能信息，例如：用途；值则可以是具体信息，例如：组织，1-部门，1-研发。

点击标签列表中的资源数量值可以将已存在的资源打上标签。



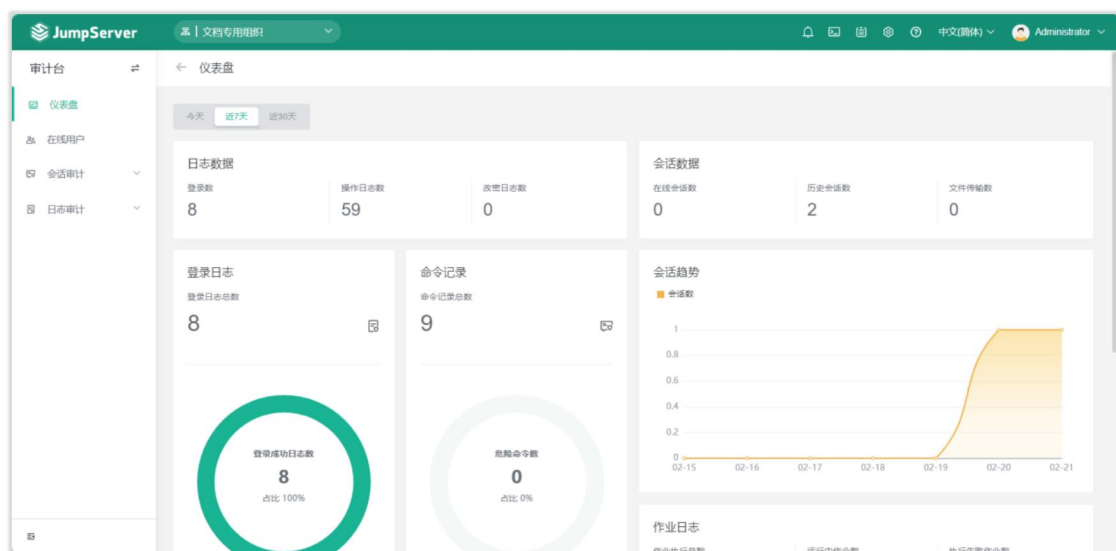
标签名称可以重名，一个资源可以有多个标签。标签删除，资产上的标签信息会自动消失。其他按钮的使用方式可参考用户管理中的按钮详解。

6. 审计台

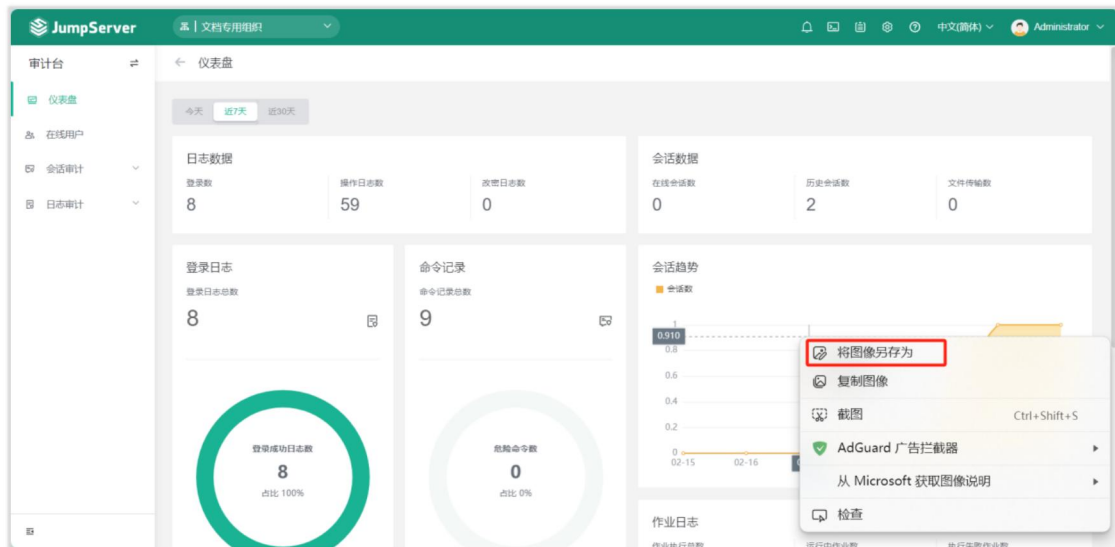
审计台主要面向审计人员，主要分为三个部分：在线用户、会话审计与日志审计。在线用户主要面向 JumpServer 系统上的登录在线用户；会话审计主要面向 JumpServer 连接资产时产生的会话日志审计信息；日志审计主要面向 JumpServer 平台本身的日志包括登录日志、操作日志等。

6.1. 仪表盘

审计台初始页面如下所示，可以查看当前组织的日志详情。仪表盘页面可查看日志数量、会话数量、会话登录趋势、用户登录趋势等。



JumpServer 支持将仪表盘页面的图像（登录日志占比、会话趋势、用户登录趋势等）导出为图片，方便保存，在该页面中空白处鼠标右击，选择<将图片另存为>按钮。



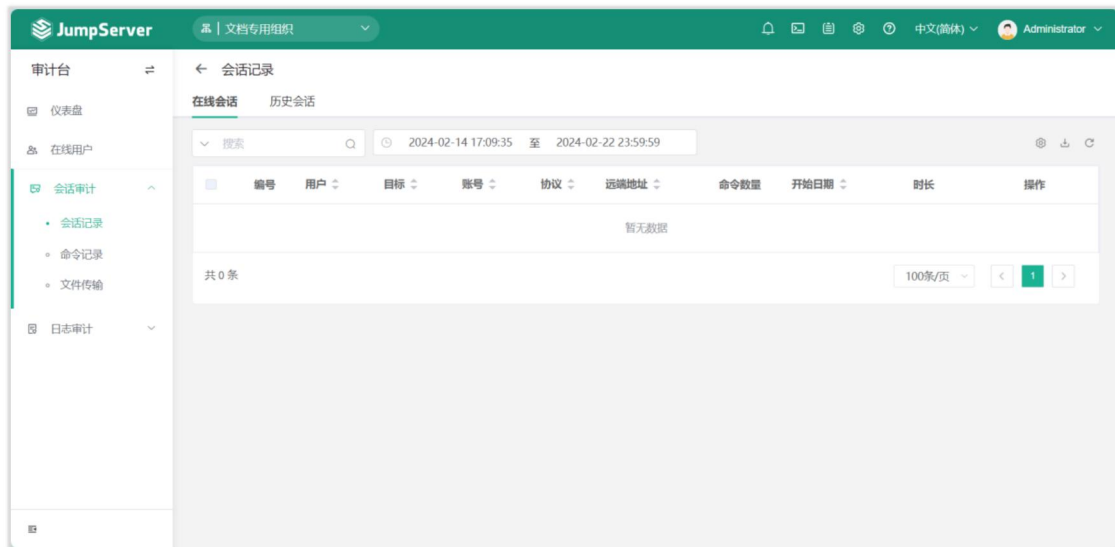
6.2. 在线用户

在线用户页面可以查看当前登录 JumpServer 系统的用户信息（当前仅记录以 Web 方式登录的用户），且可以控制用户下线。

The screenshot shows the '在线用户' (Online Users) page in JumpServer. It features a table with columns: 用户 (User), 认证方式 (Authentication Method), 登录 IP (Login IP), 登录城市 (Login City), 用户代理 (User Agent), 创建时间 (Creation Time), 活跃 (Active), and 操作 (Action). The table lists three users, all named 'Administrator', who have logged in via '密码' (Password) from IP '10.1.10.35' using 'Mozilla/5.0 (Windows ...)' as the user agent. The '操作' column contains a '下线' (Offline) button for each user. A message at the top states: '无法下线当前会话，因为该会话是当前用户的在线会话。当前只记录以 Web 方式登录的用户。' (Cannot offline the current session because it is the current user's online session. Currently, only users logged in via Web are recorded.)

6.3. 会话审计

会话审计即用户连接资产、传输文件的记录。会话审计模块包含会话记录、命令记录和文件传输记录。

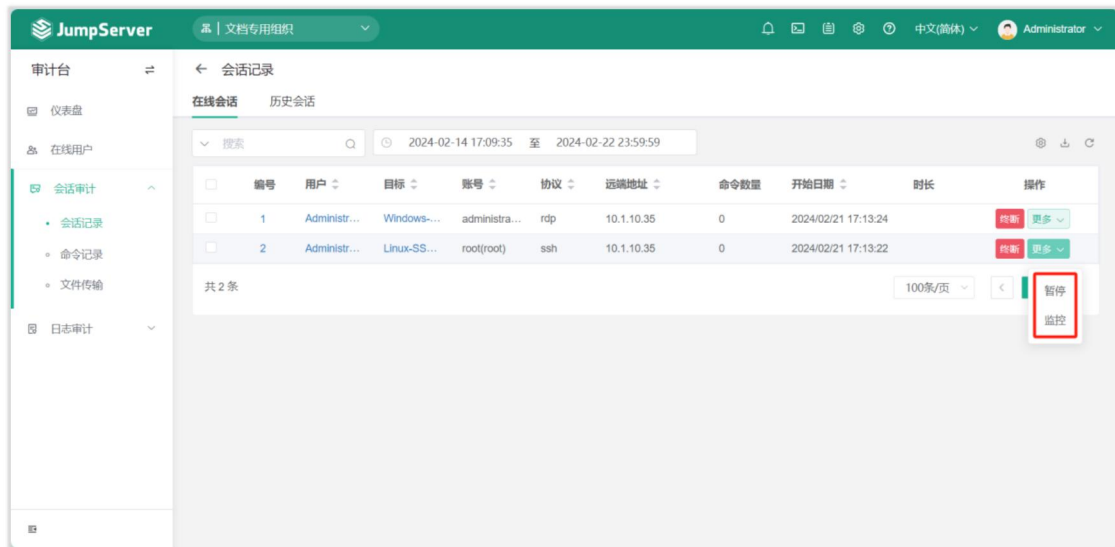


6.3.1. 会话记录

会话记录包含在线会话与历史会话两部分，主要展示的信息有登录资产的会话详细记录，包含用户、协议、远端地址、会话时间以及会话录像等。

6.3.1.1. 在线会话

在线会话可以查看到所有目前正在使用 **JumpServer** 登录其他资产的会话。**JumpServer** 在线会话可以实时监控，当用户进行违规的操作时，管理员可直接终结该会话。**JumpServer** 在线会话可以实时监控，管理员可以对当前在线会话执行“暂停”和“恢复”操作，被“暂停”的会话用户无法继续操作，管理员选择“恢复”后用户可继续操作。**JumpServer** 实时监控支持 **SSH** 协议与 **RDP** 协议的会话连接，**RDP** 客户端方式会话与数据库协议会话暂不支持实时监控。



6.3.1.2. 历史会话

历史会话可以查看所有 JumpServer 连接资产的详细信息以及操作录像，方便进行回溯与追责。JumpServer 可以在线查看录像或者下载录像到本地 PC 通过 JumpServer 离线录像播放器播放录像。

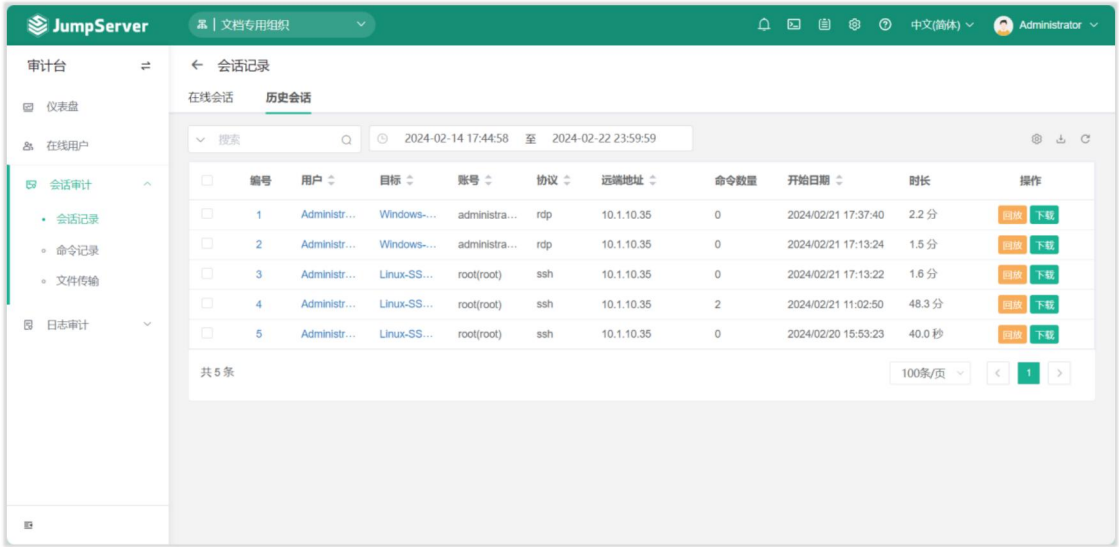
JumpServer 支持将 Razor 组件与 Lion 组件产生会话录像转换成 MP4 格式，支持录像的进度条拖动和倍速播放。该功能需要使用 JumpServer 新增的 Video-Worker 组件。开启需要在配置文件中添加选项，修改之后重启 JumpServer 堡垒机服务生效。

JumpServer 配置文件默认位于：/opt/jumpserver/config/config.txt

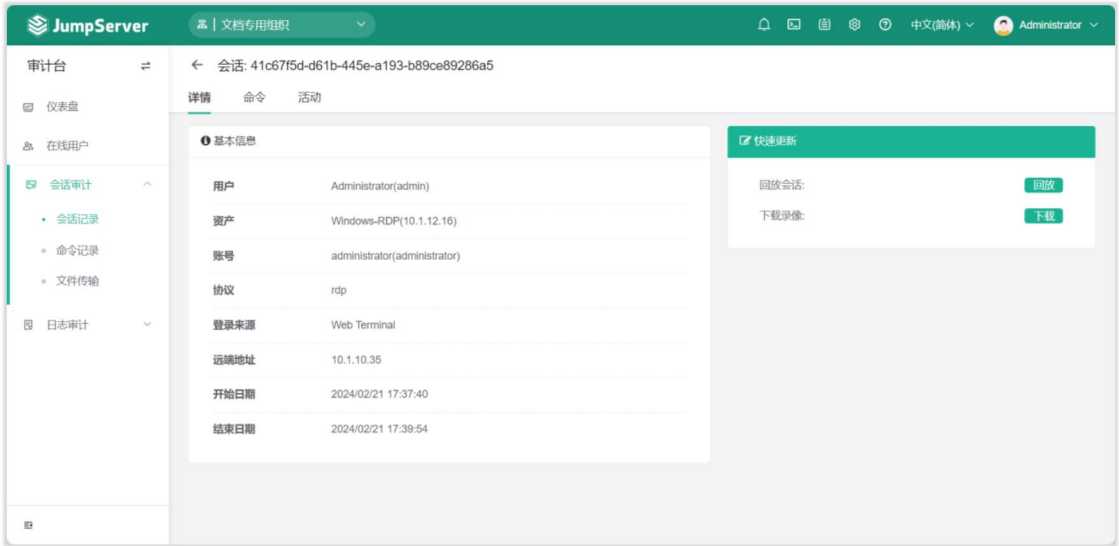
开启 Windows 录像转换成 MP4 格式的配置项如下：

```
USE_VIDEO=1
ENABLE_VIDEO_WORKER=True
VIDEO_WORKER_HOST=http://jms_video:9000
```

注：转码的相关组件主要依赖 ffmpeg 相关库，运行过程中会大量消耗 CPU，不建议与 JumpServer 部署在同一台机器上。详情可咨询 JumpServer 售后工程师。



点击历史会话页面的<编号>按钮，可进入会话的详细信息页面。

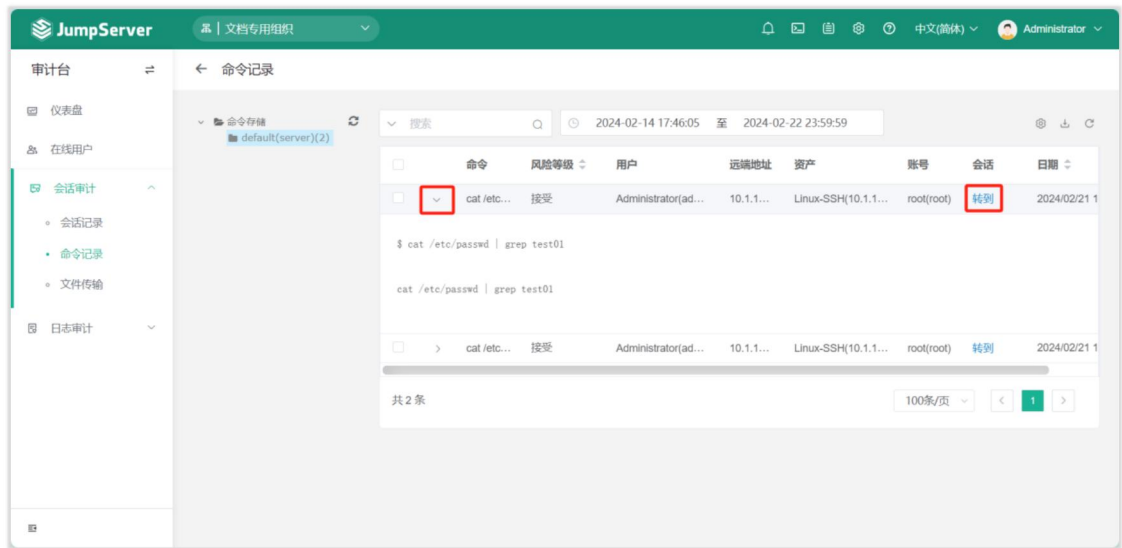


模块详细说明：

模块	说明
基本信息	基本信息模块主要介绍该会话的基础信息，包含登录用户、登录来源、远端地址、会话开始时间与结束时间等。
快速更新	快速更新模块主要针对录像的播放，包含直接播放与下载录像后播放。
命令	命令模块可以查询到该会话连接过程中用户执行的命令记录。
活动	JumpServer 支持会话分享，即分享已连接的会话给其它用户。活动模块即可查看分享记录。

6.3.2. 命令记录

命令记录主要显示用户在资产连接后执行的命令，单击某一行记录，可以查看命令执行的详细结果。



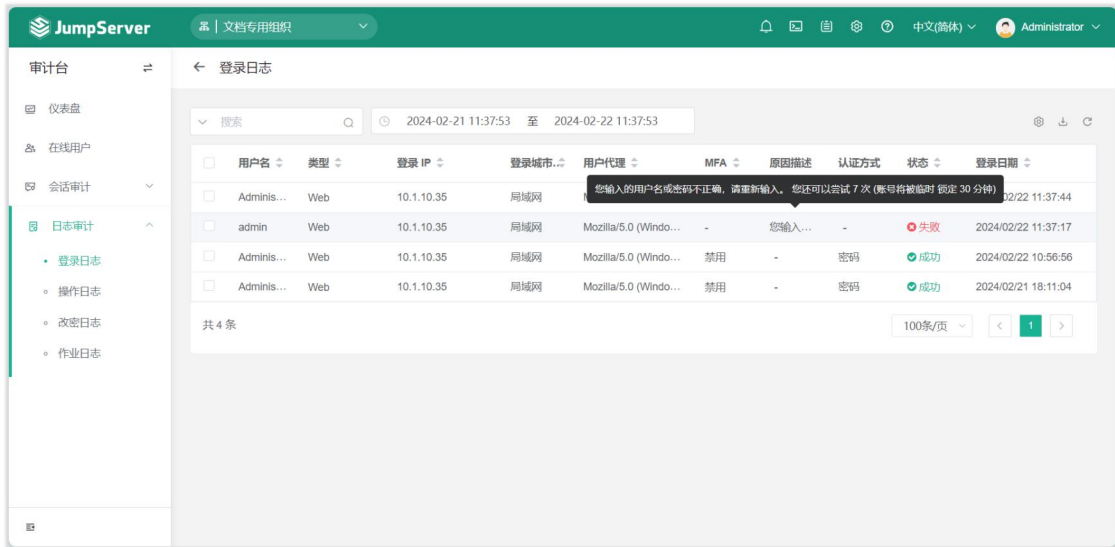
点击对应命令后方的[<转到>](#)按钮，JumpServer 会跳转到详细的会话列表页面，如果会话已结束可直接查看会话录像。

6.3.3. 文件传输

文件传输可以查看所有上传/下载文件到资产上的历史记录。JumpServer 支持对文件上传/下载的文件内容进行审计，管理员可以在文件传输页面查看文件传输的文件内容。JumpServer 默认备份文件的大小阈值为 100MB。当需要保存 100MB 以上的文件时，需要管理员在配置文件中添加参数：

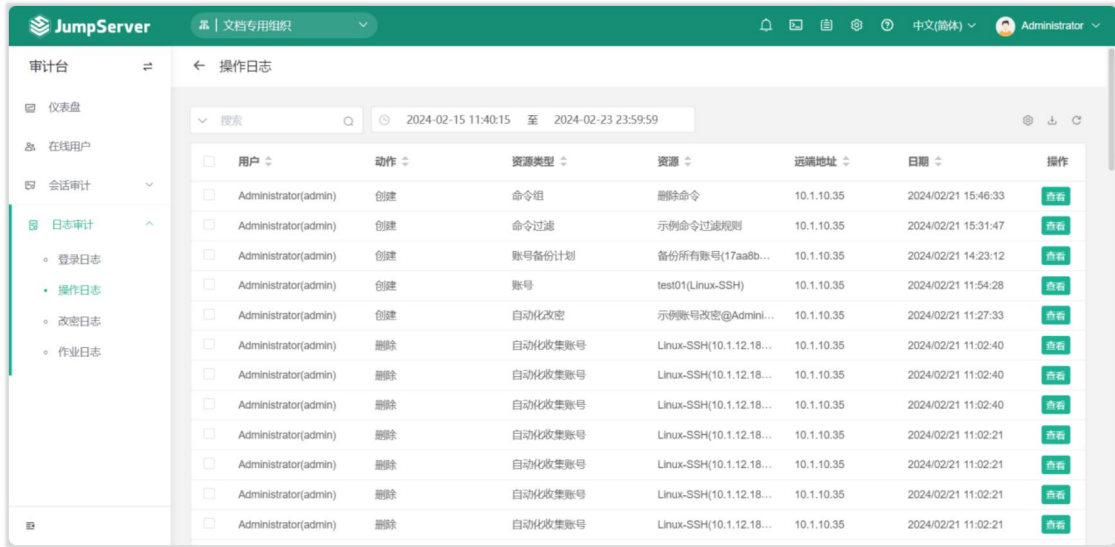
JumpServer 配置文件默认位于：/opt/jumpserver/config/config.txt

配置备份文件的大小阈值的配置项为: FTP_FILE_MAX_STORE #该参数配置单位为 MB，当此配置项的值小于或等于零时，不开启文件备份功能。JumpServer 版本大于等于 3.10.3 版本，默认不开启文件备份功能。

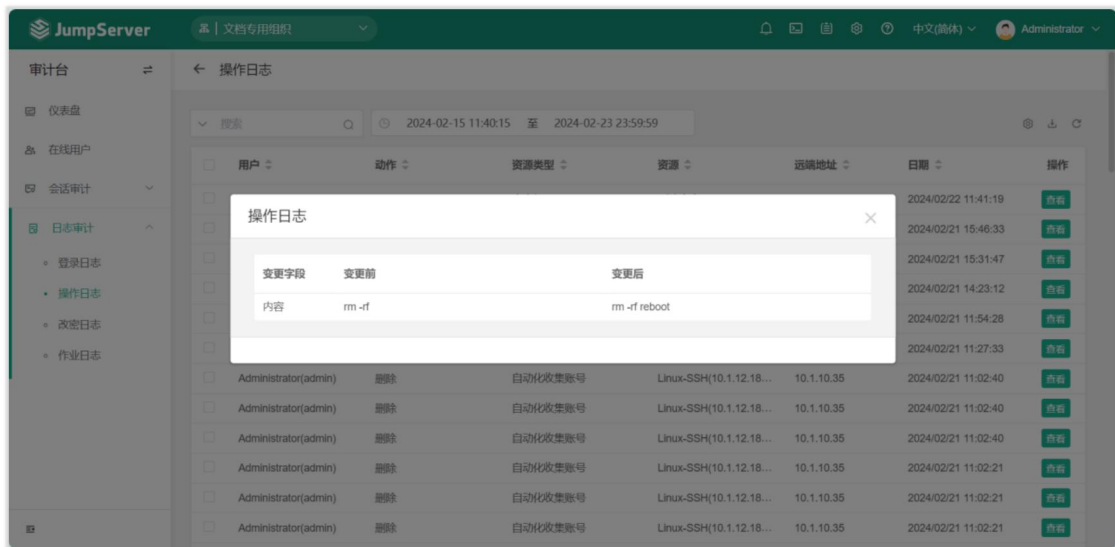


6.4.2. 操作日志

操作日志是指整个 JumpServer 平台的管理操作日志，在此页面可以查看操作的用户、资产类型、操作的日志。

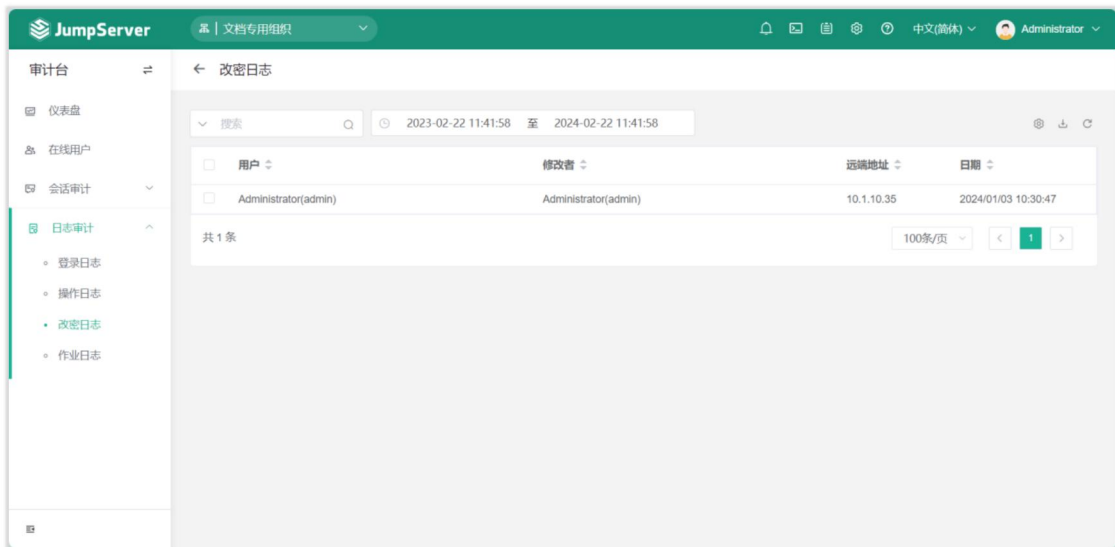


具体的变更可以点击操作日志后方的[查看](#)按钮。



6.4.3. 改密日志

改密日志是指 JumpServer 系统中的登录用户的改密日志信息。



6.4.4. 作业日志

作业任务是针对于用户的作业中心的任务执行的日志信息。

JumpServer

基 | 文档专用组织

🔔

📧

👤

⚙️

🕒

中文(简体)

Administrator

审计台

仪表盘

在线用户

会话审计

日志审计

- 登录日志
- 操作日志
- 改密日志
- 作业日志

← 作业日志

搜索

🕒 2024-02-15 11:45:02 至 2024-02-23 23:59:59

⚙️ ⬇️ 🔍

<input type="checkbox"/>	创建者	命令	是否完成	成功	时间	开始日期	结束日期	操作
<input type="checkbox"/>	Administrator	shell:free -h	✓	✓	1.83s	2024/02/22 11:44:44	2024/02/22 11:44:46	输出
<input type="checkbox"/>	Administrator	shell:df -h	✓	✓	1.92s	2024/02/22 11:44:34	2024/02/22 11:44:36	输出
<input type="checkbox"/>	Administrator	shell:ls	✓	✓	2.17s	2024/02/22 11:44:22	2024/02/22 11:44:24	输出

共 3 条

100条/页<1>

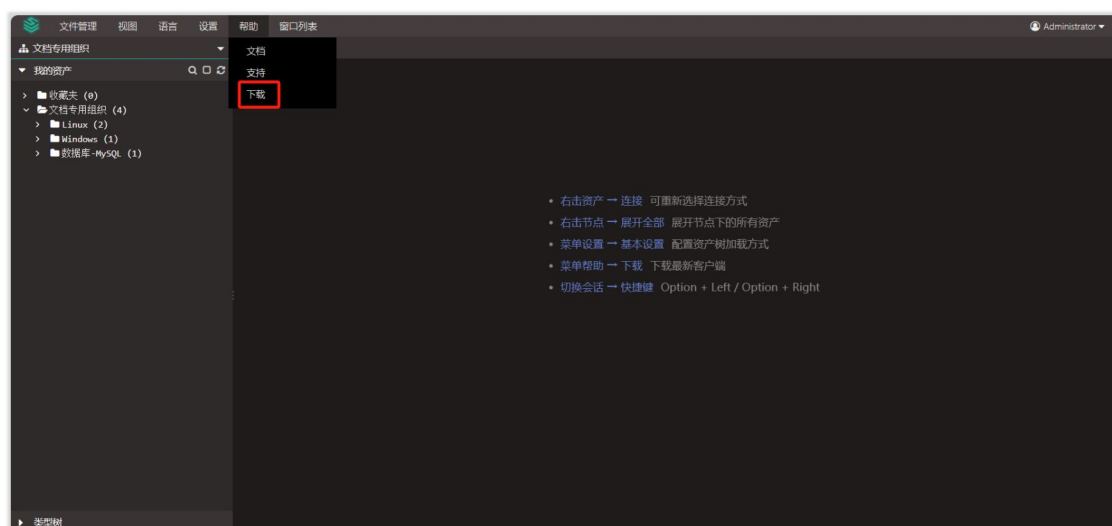
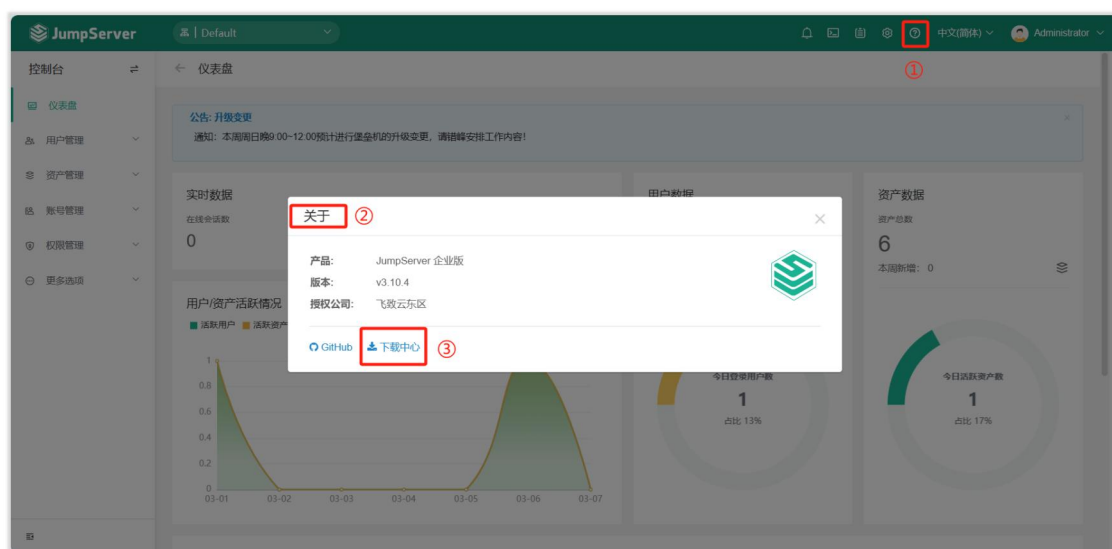
7. JumpServer 下载中心

7.1. 概述

JumpServer 的下载中心中包含 JumpServer 服务中提供的所有服务中需要用到的一些程序。其中包含：JumpServer 的客户端、微软 RDP 官方客户端、Windows 远程应用发布服务器 工具、JumpServer 离线播放器。

JumpServer 客户端的安装包下载地址如下：

- 工作台页面的“关于”模块中的下载中心页面中下载；
- Web 终端页面中的“帮助”模块中的下载页面中下载。下载中心的页面如下所示：



下载中心的页面如下所示：



4.2. JumpServer 客户端

JumpServer 客户端的使用场景如下：

- Linux 资产使用客户端方式连接时通过 JumpServer 客户端拉起个人 PC 的 Linux 资产连接程序。例如：SecureCRT；
- Windows 资产使用客户端方式连接时通过 JumpServer 客户端拉起个人 PC 的 mstsc 程序。例如：mstsc ；
- 数据库资产使用客户端方式连接时通过 JumpServer 客户端拉起个人 PC 的数据库资产连接程序。例如：PLSQL、DBeaver、RDM 等；



JumpServer 客户端支持安装到 Windows、MAC 与 Linux 系统的个人 PC 上。

4.3. 微软 RDP 官方客户端

微软 RDP 官方客户端的使用场景如下：

- 当用户的个人 PC 为 MAC 时,使用客户端方式连接 Windows 时无法提供 mstsc 程序； 可下载该客户端并将其安装到个人 PC 上实现 Windows 的客户端连接。

微软 RDP 官方客户端 v10.6.7

macOS 需要下载客户端来连接 RDP 资产，Windows 系统默认安装了该程序

- [microsoft-remote-desktop-installer.pkg](#)

4.4. Windows 远程应用发布服务器工具

Windows 远程应用发布服务器工具的使用场景如下：

- Windows 远程应用发布机在目前版本中使用程序自动化部署，该 Windows 需要支持 OpenSSH 协议，该工具可快速在 Windows 机器上安装 SSH 协议并开放对应端口。

Windows 远程应用发布服务器工具

OpenSSH 是在 windows 远程应用发布服务器中用来连接远程应用的程序

- [openSSH-win64.msi](#)

4.5. JumpServer 离线录像播放器

JumpServer 离线录像播放器的使用场景如下：

- 当将 JumpServer 的录像下载到个人 PC 本地进行播放时，需要安装录像播放器播放录像。

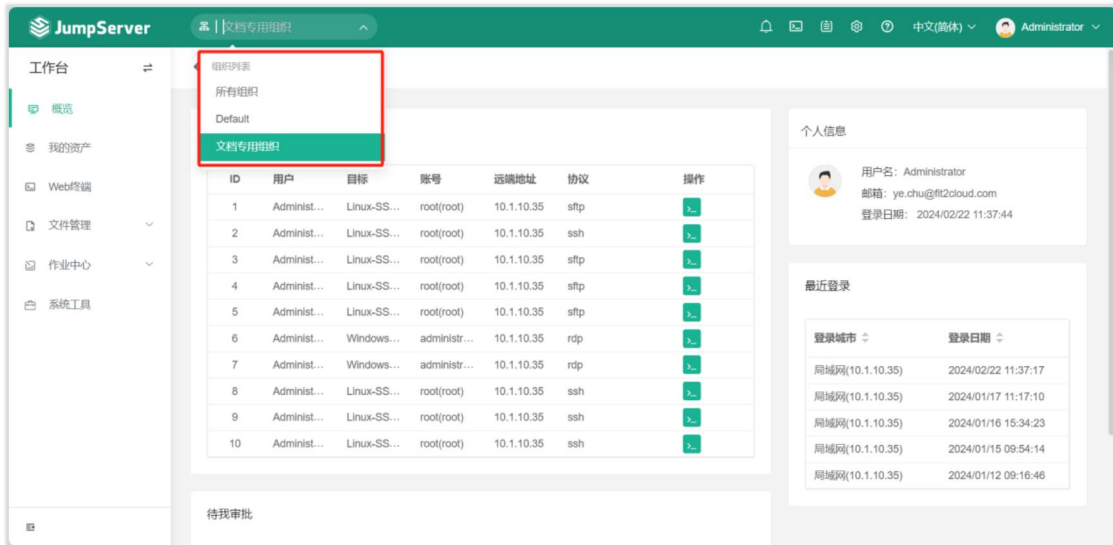
JumpServer 离线录像播放器 v0.1.5

- [jumpserver-video-player.dmg](#)
- [jumpserver-video-player.exe](#)

8. 工作台

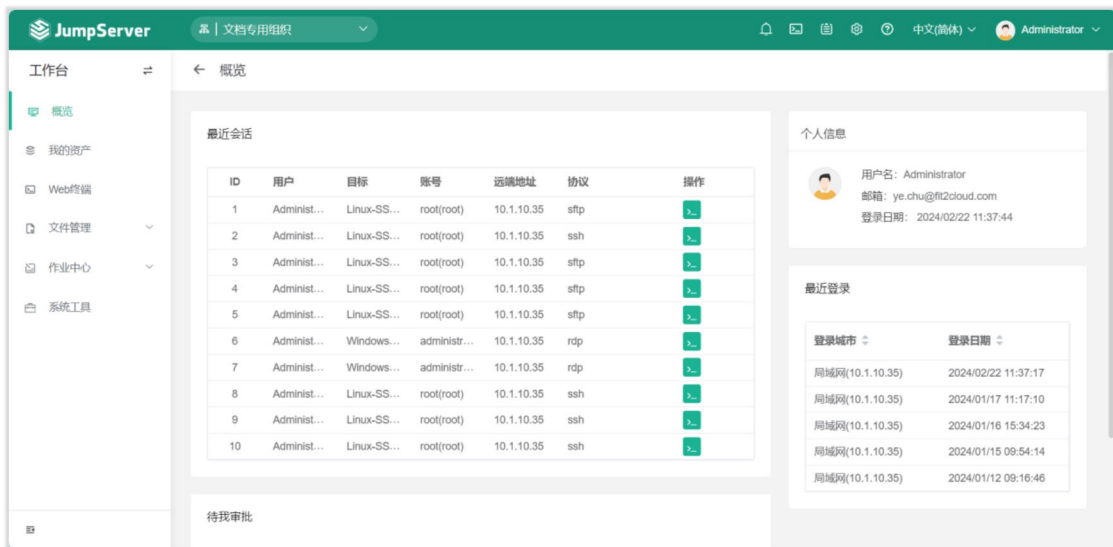
工作台页面主要面向普通用户，主要分为五个部分：信息概览、我的资产、Web 终端、文件管理、作业中心。

JumpServer 工作台支持区分组织，即切换不同的组织，获取不同的组织授权。



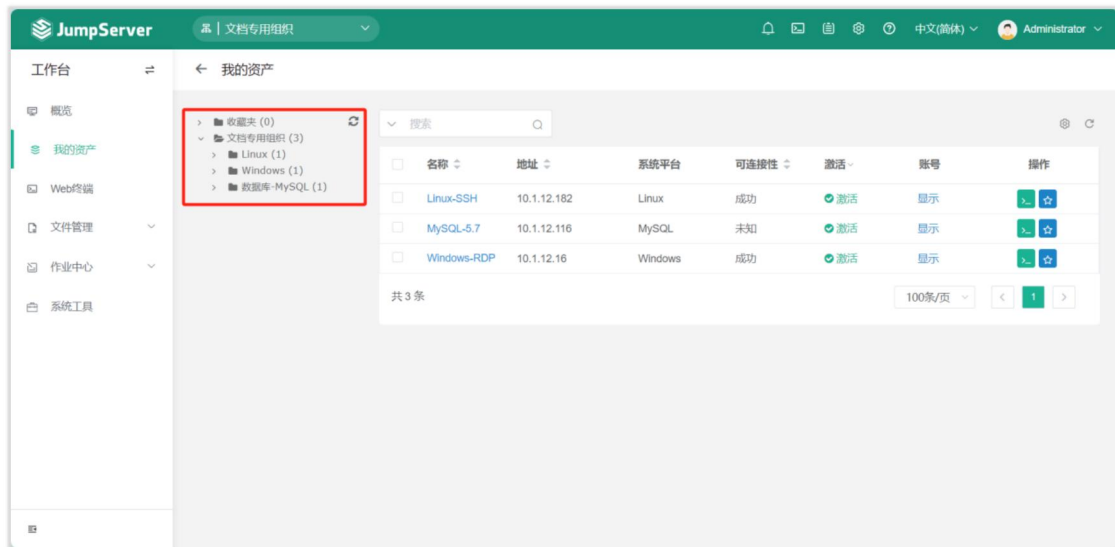
8.1. 概览

概览页面为用户登录后显示的首个页面，主要包含的信息：管理员用户设置的公告信息、最近连接的会话信息、个人信息介绍、个人最近登录信息、工单审批信息。

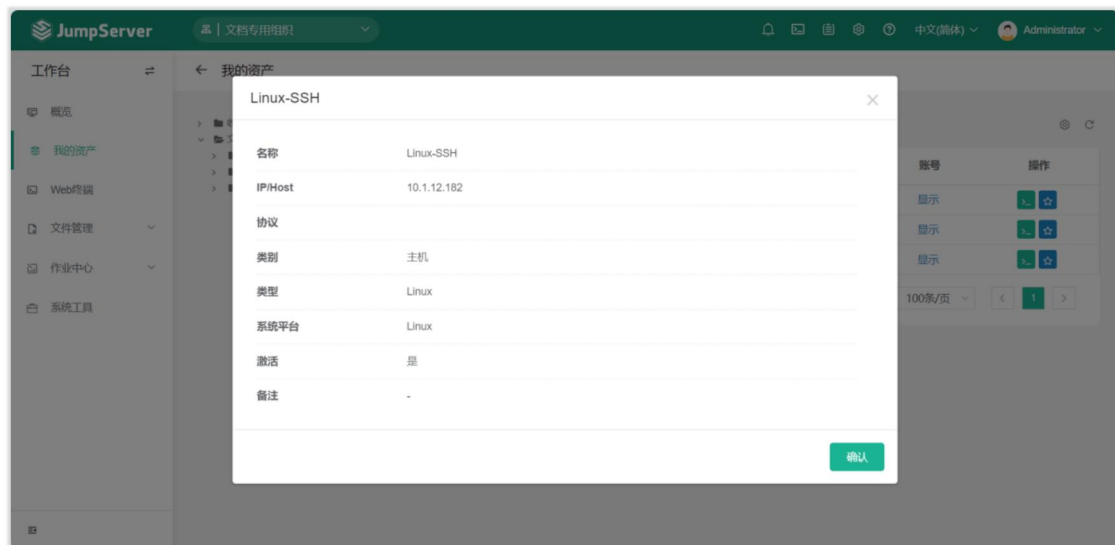


8.2. 我的资产

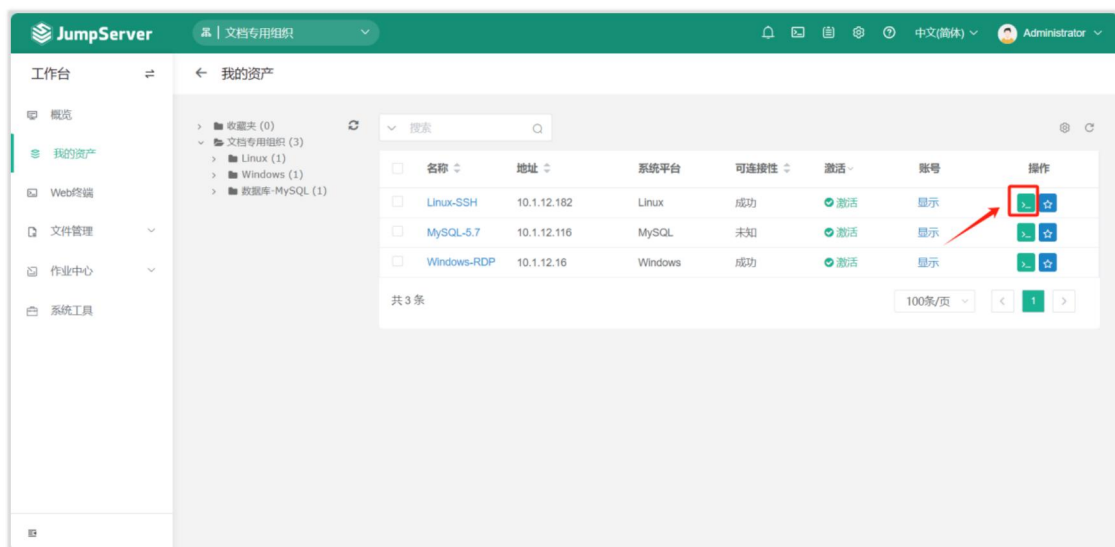
我的资产页面主要包含的是管理员已经授权给当前用户的资产信息。页面左侧为管理员用户授权给当前用户的资产所处的节点树，页面右侧为管理员用户授权给当前用户的所有资产。



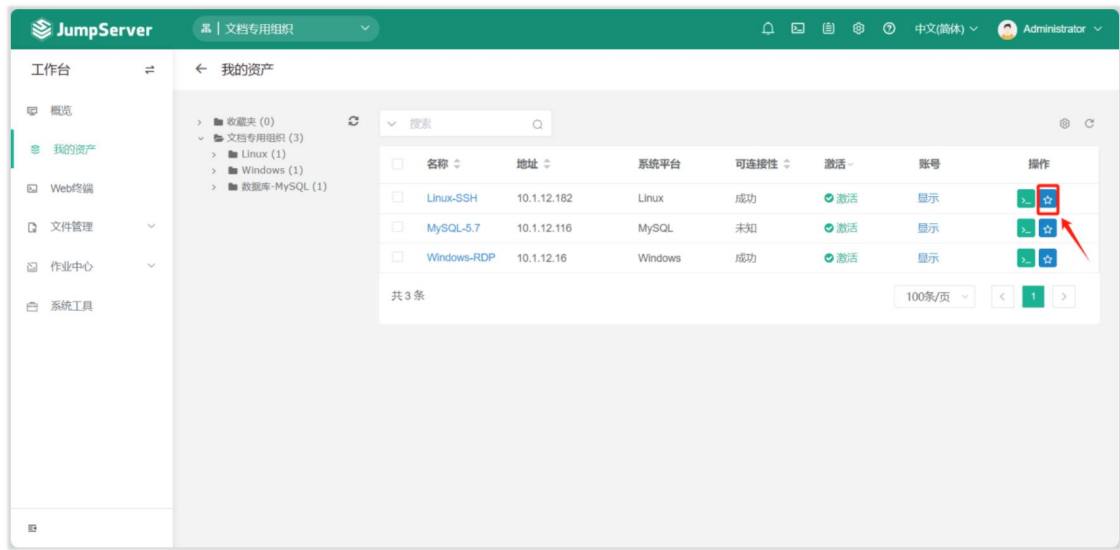
点击资产名称可以进入资产详情页面，查看资产详细信息。



点击资产后方的第一个按钮，可以快速跳转到 Web 终端页面并连接对应资产。

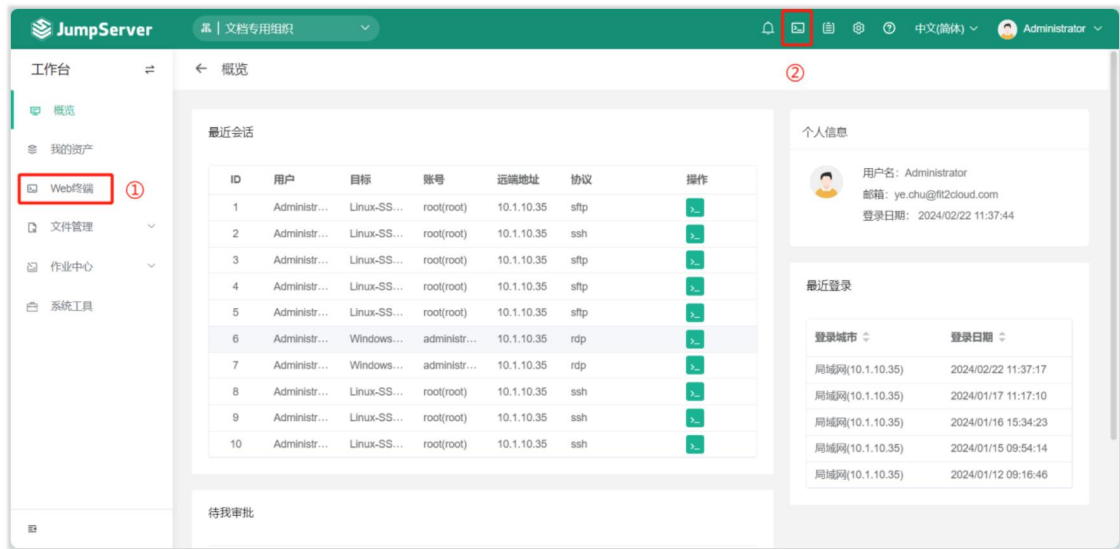


点击资产后方的第二个按钮，可以将当前资产添加到收藏夹之中，便于在 Web 终端中快速找到并连接该资产。



8.3. Web 终端

Web 终端页面主要用于资产连接。点击工作台页面的 [Web 终端](#) 按钮或者右上角图标，均可跳转到 Web 终端页面，并在此页面发起资产访问。



8.3.1. 组织切换

JumpServer 支持在 Web 终端页面按照组织显示授权给用户的资产。当某一个用户在多组织下都拥有资产授权时，可在如图示中按钮切换组织并获取该组织的授权资产；在需求连接

资产时，可以在左侧资产树列表中选择需要访问的资产，也可以通过资产名称或 IP 进行模糊搜索，快速找到访问目标，点击即可登录。



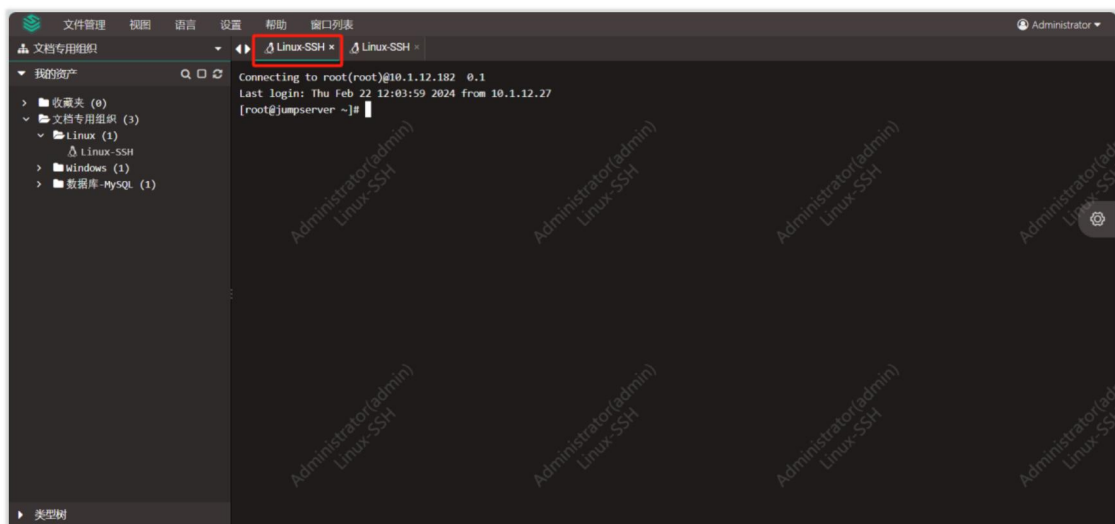
8.3.2. 批量资产连接

Web 终端页面支持用户批量连接资产。通过页面左上角的批量选项选择需要连接的资产，对资产批量发起连接操作。



8.3.3. 会话拖拽

用户使用 Web Terminal 方式连接资产时，支持对相应的 Tab 窗口手动拖拽，调整排列位置。

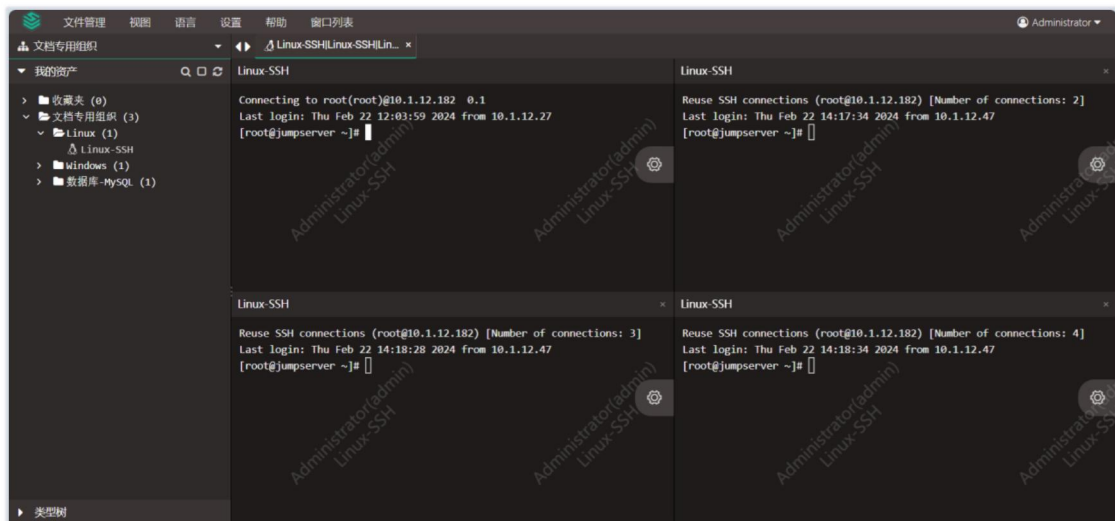


8.3.4. 会话切换

用户连接多个资产时，可以使用“ALT+Left/Right”组合快捷键快速跳转至下一个会话。

8.3.5. 会话分屏

用户连接资产时，可以在一个浏览器界面打开多个会话，并对批量命令的执行结果进行实时查看，方便用户对会话中的内容进行对比操作。（目前单个会话最多支持 4 个分屏）。



8.3.6. 资产连接

Web 终端页面主要功能为资产连接，不同类型的资产支持的连接方式也不同。

8.3.6.1. Linux 资产连接

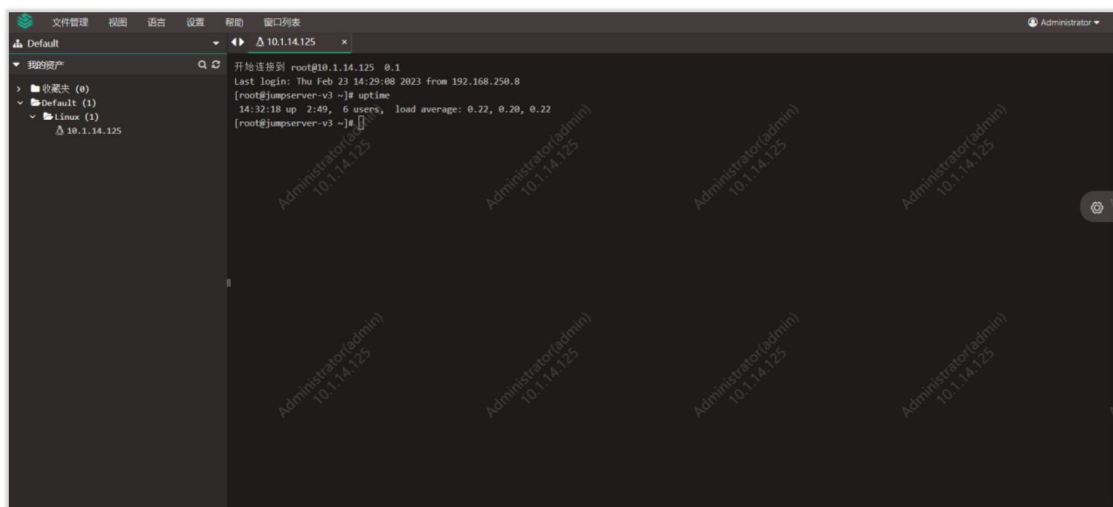
Linux 资产连接支持两种连接方式，包含 Web CLI 和客户端方式。

(一) Web CLI

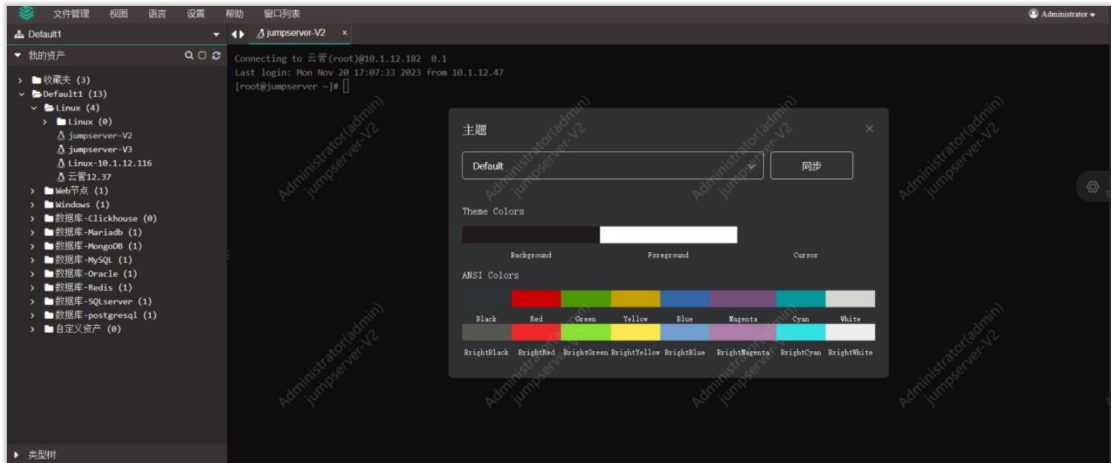
Web CLI 即命令行连接方式，如下图所示：



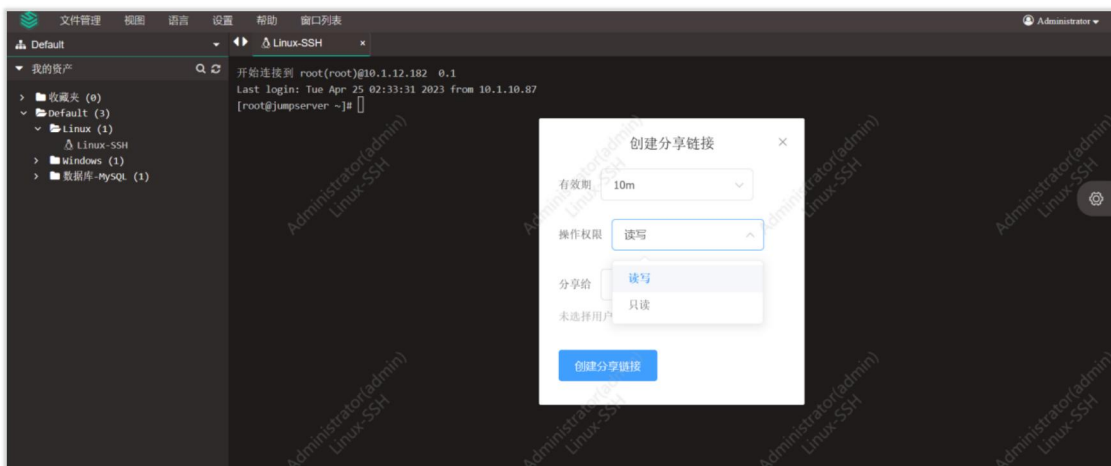
连接结果如下图所示：

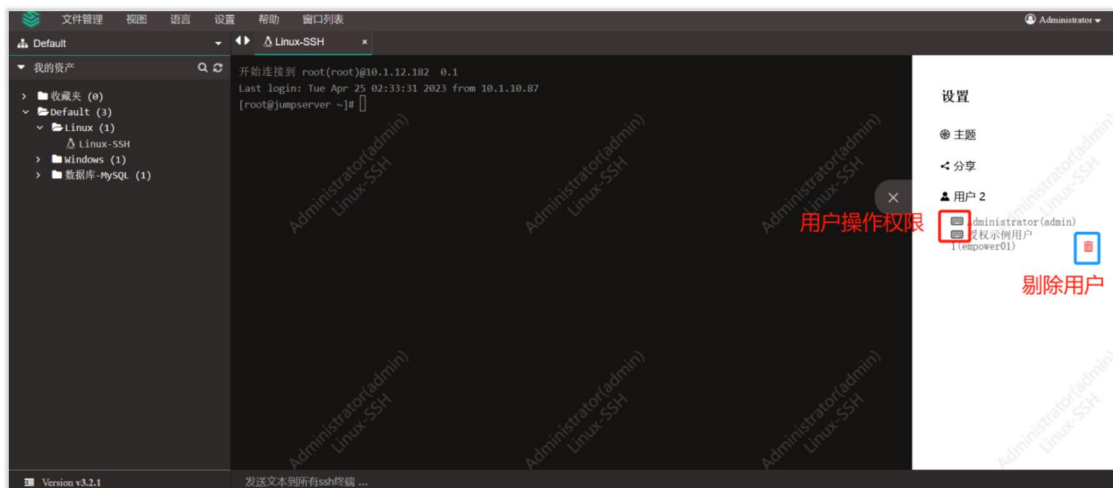


JumpServer 支持多种命令行主题，在此页面可以更改 Web 端显示的背景颜色，让用户更舒适的使用（目前仅支持 SSH/Telnet 会话）。当连接到某一个资产后，点击页面右侧 [<主题>](#) 按钮即可切换多种主题。用户可以点击“同步”按钮对主题进行持久化配置。



JumpServer 支持将 Linux 资产分享给其他用户即协作者，多人同时操作一个会话。当连接到某一个资产后，点击会话右侧^{<齿轮>}按钮中的^{<分享>}按钮即可设置分享链接有效期、被分享者的操作权限（读写、只读）、被分享的用户名称，点击^{<创建分享链接>}按钮，自动生成验证码，将该链接地址和验证码分享给其他堡垒机用户，则对方打开分享的 URL 并登录堡垒机后，输入验证码登录到当前会话（登录之后是当前登录资产的用户，并且页面是实时共享的，可协同操作），当会话分享链接创建时，被分享人的站内信会收到分享会话的站内信通知。当未选择被分享用户时，即允许所有人加入此会话链接。在会话共享过程中，分享者可以断开被分享者的会话，提交会话共享性。会话过程中，所有用户均可查看该会话共享中所有人的操作权限。

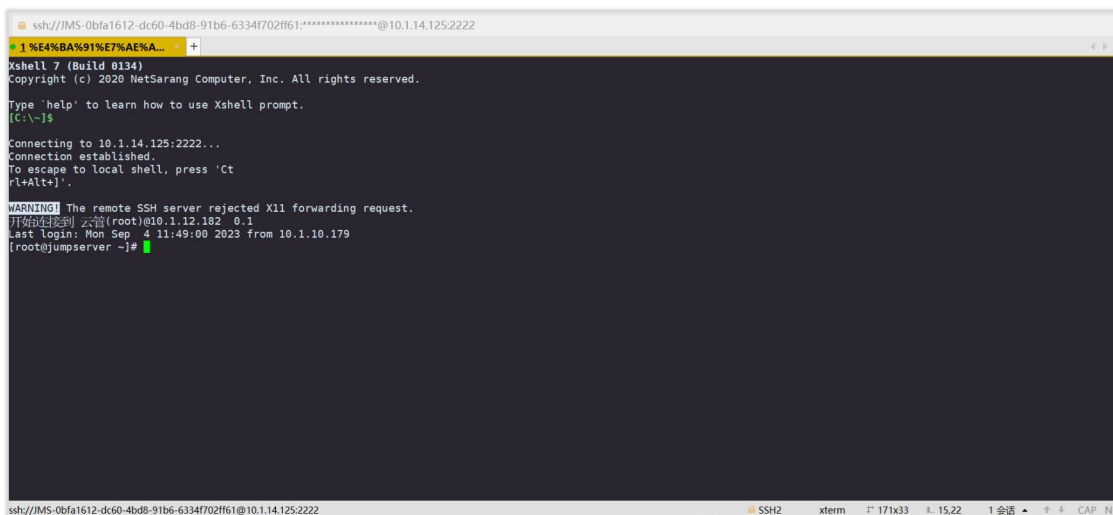
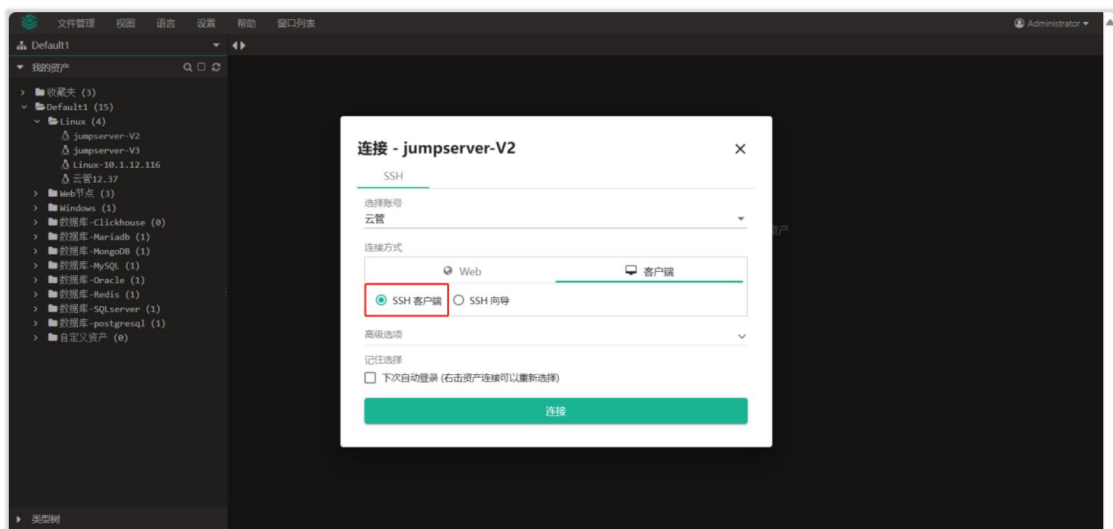




(二) 客户端

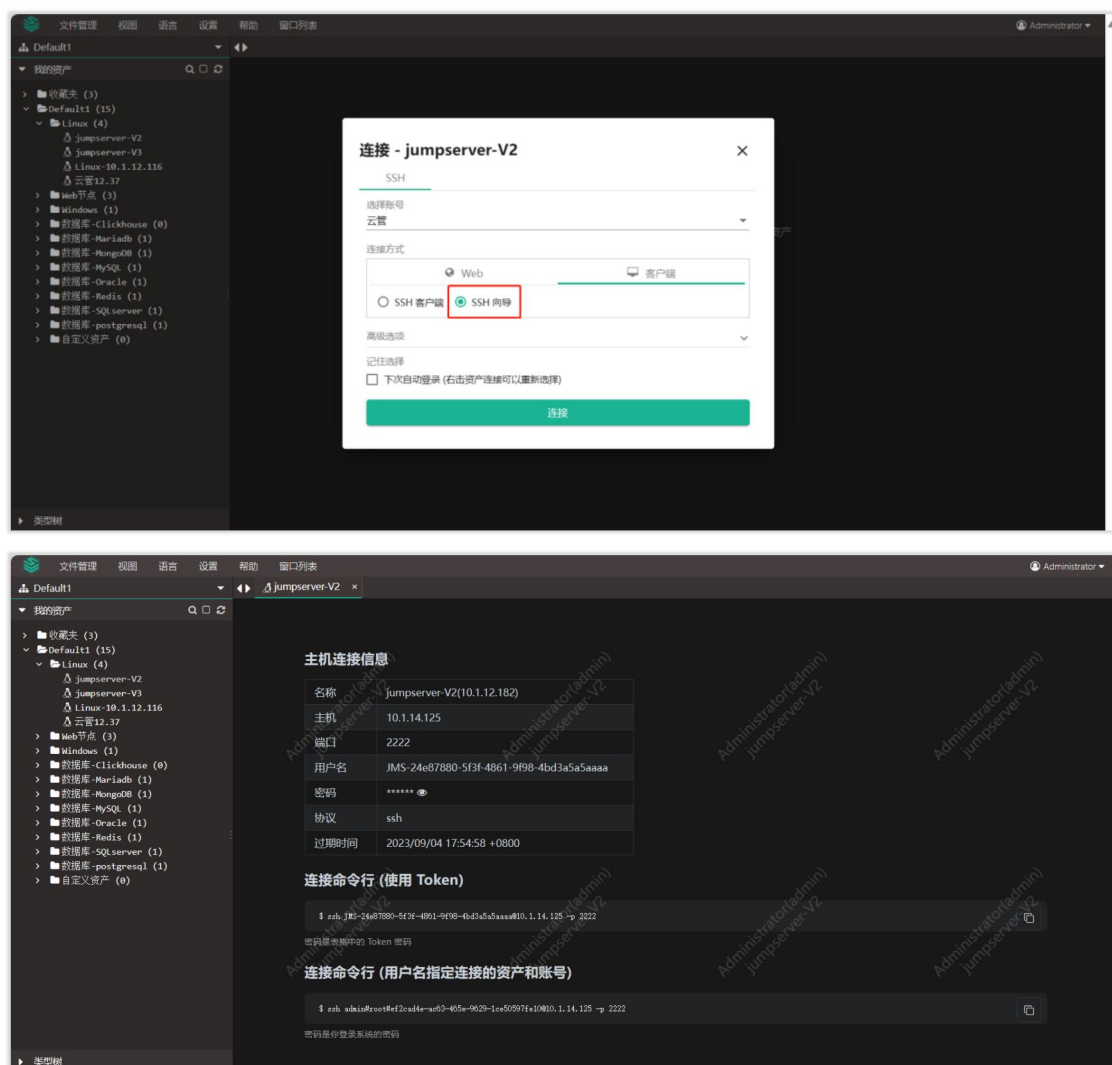
① SSH 客户端

JumpServer 支持通过拉起 SSH 客户端的方式连接 Linux 资产。用户选择“客户端-SSH 客户端”方式连接,即可拉起 JumpServer 客户端, JumpServer 客户端拉起本地的 SecureCRT 客户端或其他客户端并代填连接数据,即可连接。



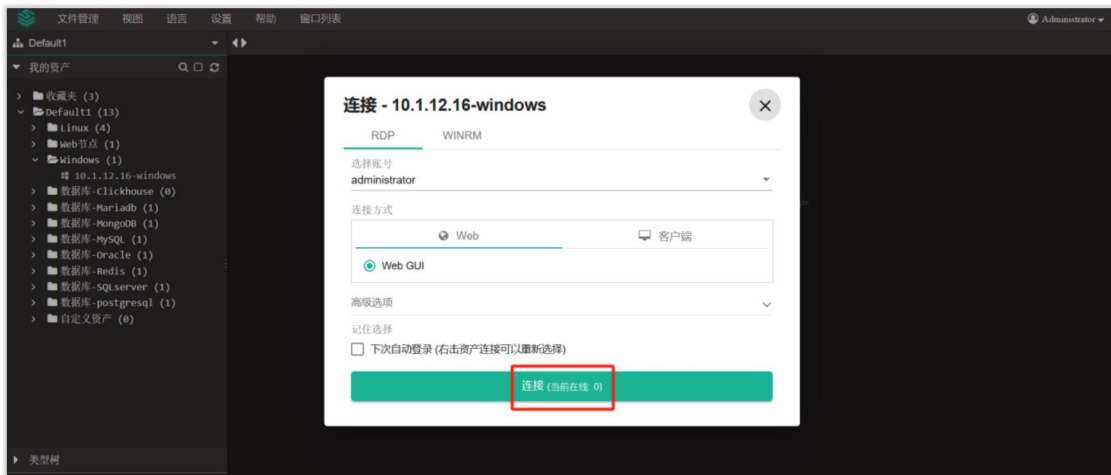
② SSH 向导

JumpServer 支持通过生成加密信息的方式连接 Linux 资产。用户选择“客户端-SSH 向导”方式连接，即可生成加密的连接信息。用户可复制此处的加密信息到任意命令行执行连接对应的资产。



8.3.6.2. Windows 资产连接

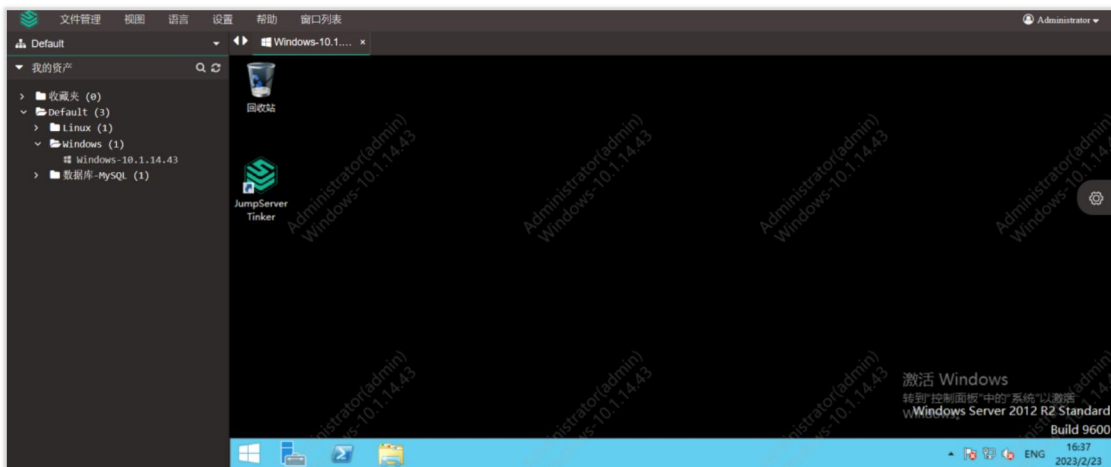
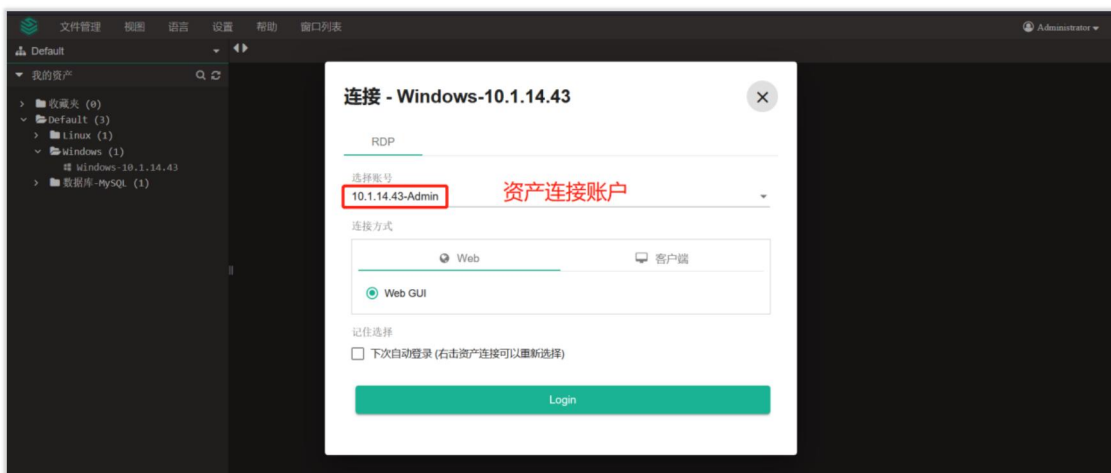
Windows 资产在连接按钮中显示该资产当前已连接的用户数量。



Windows 资产 JumpServer 支持三种连接方式，分别为“Web GUI”、“Remote Desktop（原 RDP 客户端）”、“Click to download rdp file（原 RDP 文件）”。

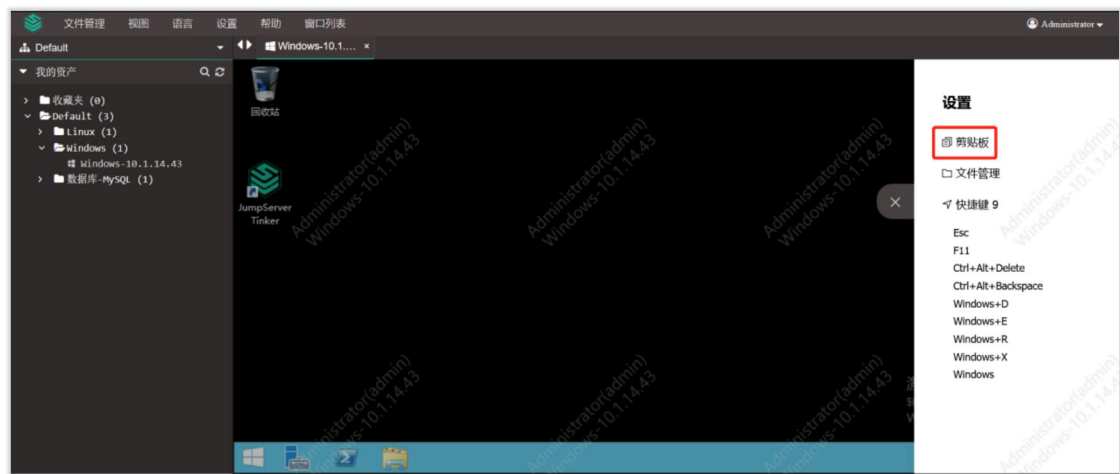
(一) Web GUI

Web GUI 方式即在 JumpServer 页面对 Windows 进行连接，如下图所示：



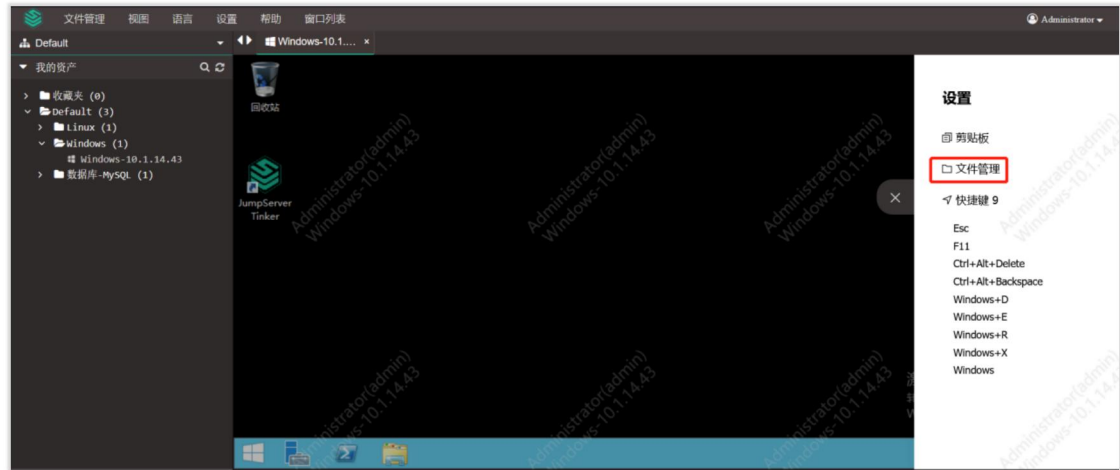
Web GUI 的方式复制粘贴需要通过页面右侧的<齿轮>按钮中的剪切板实现。当需要复制本地 PC 的文字到 Windows 资产中时，本地 PC 上选择复制后，点击连接页面右侧的<齿轮>

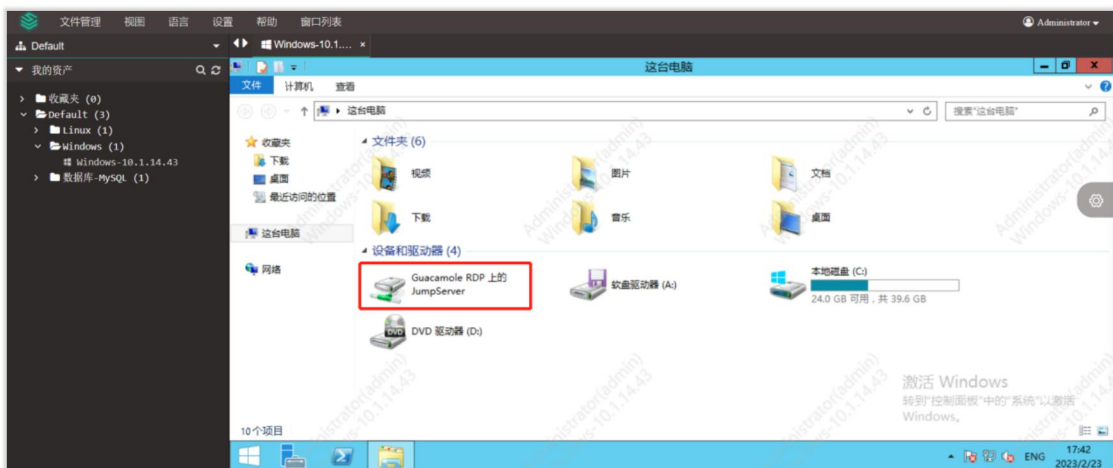
按钮，选择<剪切板>按钮，复制剪切板中的内容就可以复制本地 PC 的文字到 Windows 资产中。Windows 资产复制文字到本地 PC 同理。



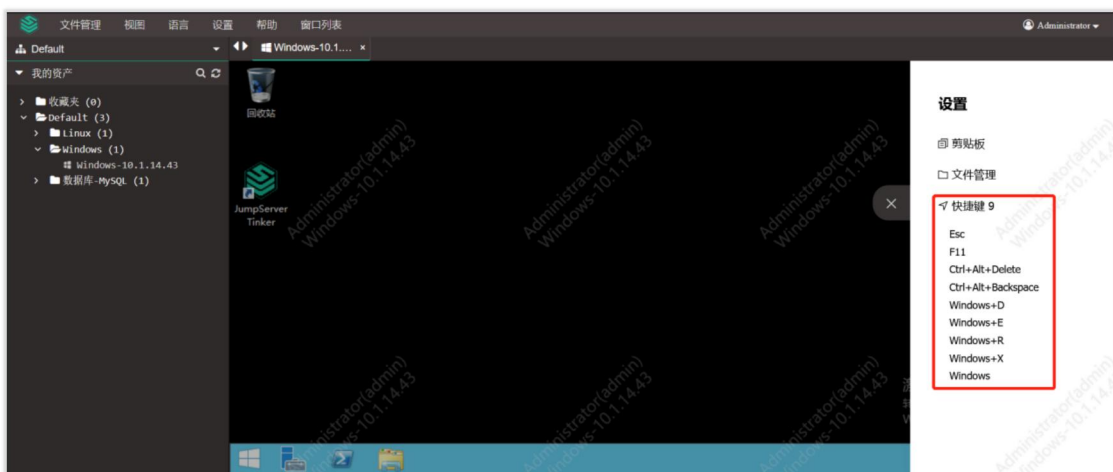
Web GUI 的方式上传下载文件通过页面右侧的<齿轮>按钮中的文件管理实现。

- 当需要在使用 Web GUI 连接方式连接 Windows 的情况下上传文件时，点击连接页面右侧的<齿轮>按钮，选择<文件管理>按钮，在弹出的文件管理页面中点击<上传文件>按钮，选择需要上传的文件，文件上传成功后到 Windows 资产的文件资产管理器中寻找共享盘（Guacamole RDP 上的 JumpServer）中寻找上传成功的文件并移动到其他位置。
- 当需要在使用 Web GUI 连接方式连接 Windows 的情况下下载文件时，将需要下载的文件移动到 Windows 资产的文件资产管理器中的共享盘（Guacamole RDP 上的 JumpServer）中的 Download 目录下，即可实现文件的下载。



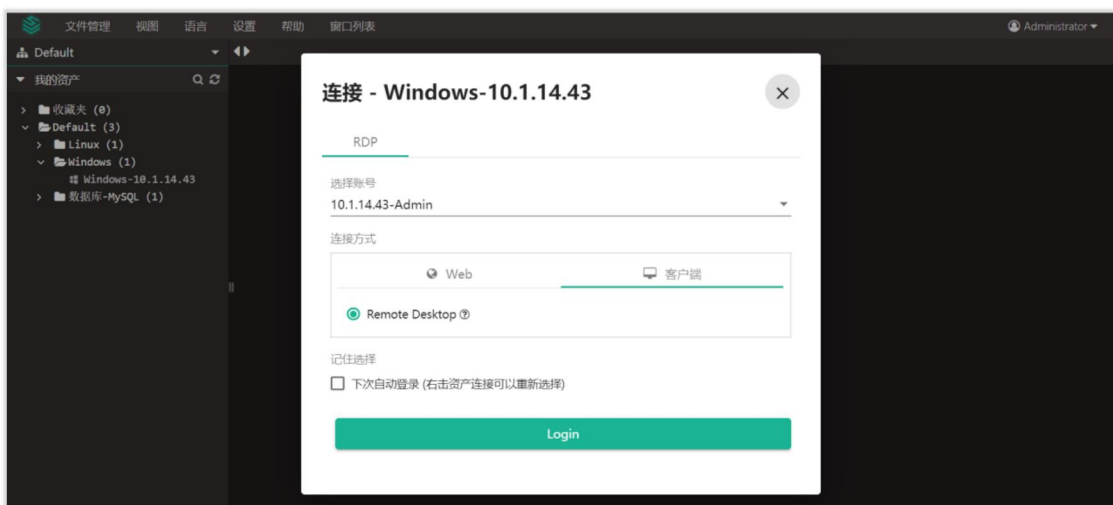


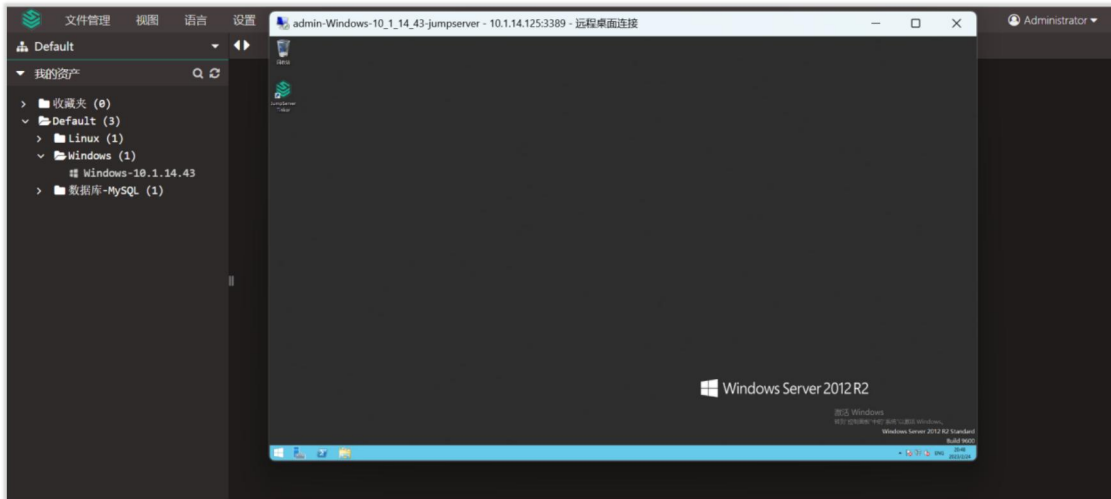
Web GUI 的方式的快捷键通过页面右侧的<齿轮>按钮中的快捷键实现。



(二) Remote Desktop

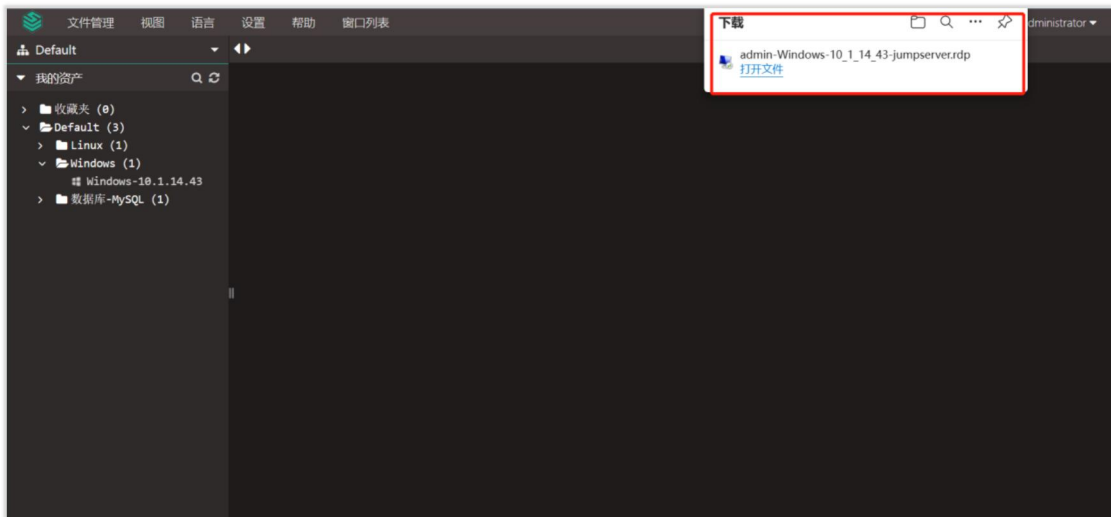
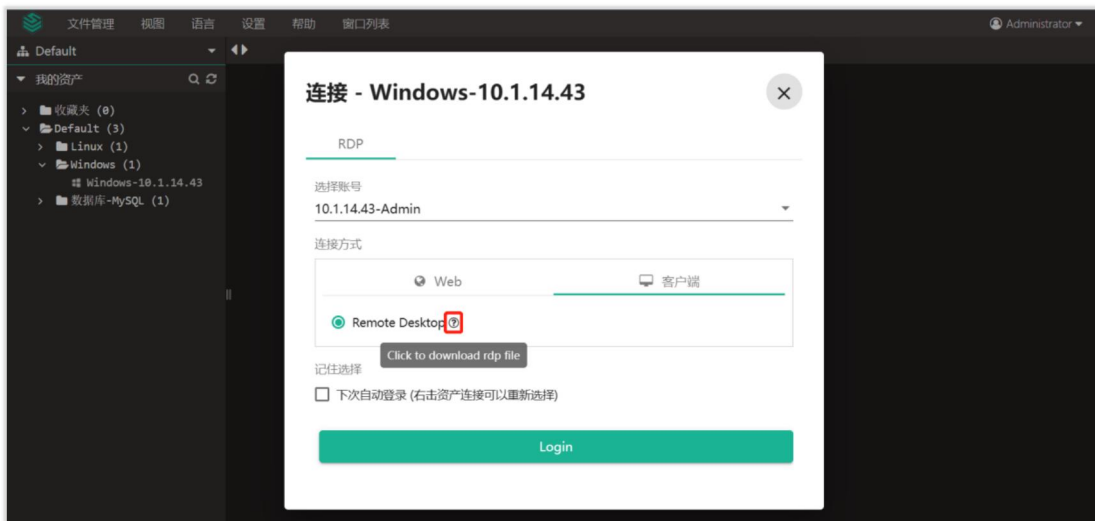
“Remote Desktop”方式会拉起 JumpServer 客户端，JumpServer 客户端拉起 Windows 本地的 Mstsc 程序连接 Windows 资产，Mac 系统需下载微软 RDP 官方客户端（点击 Web 终端中的帮助模块中的<下载>按钮跳转后的页面中）。



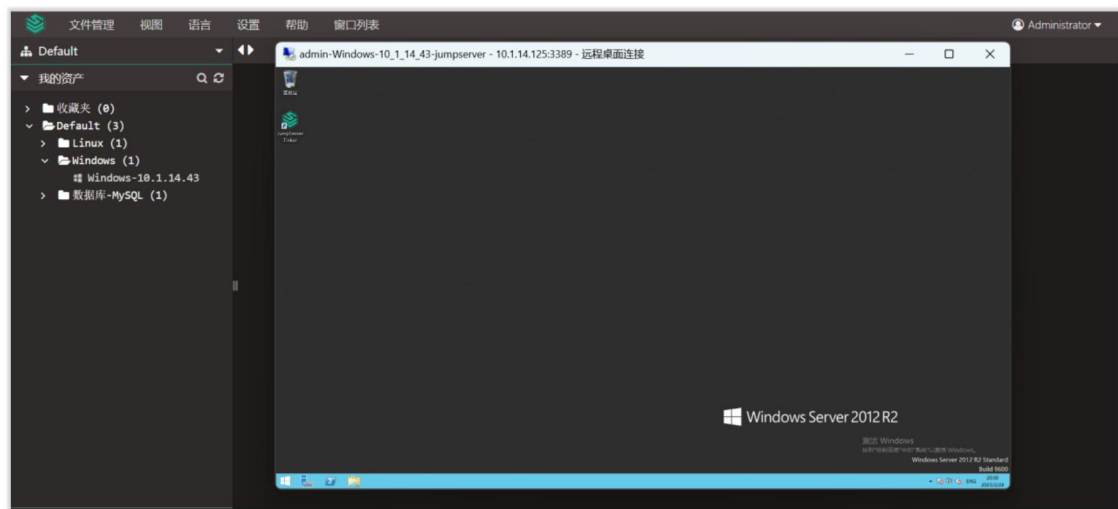


(三) RDP File

“RDP File”方式会下载一个 RDP 文件，点击 RDP 文件后拉起 Windows 本地的 Mstsc 程序连接 Windows 资产，Mac 系统需下载微软 RDP 官方客户端（点击 Web 终端中的帮助模块中的[<下载>](#)按钮跳转后的页面中）。



连接成功如下图所示：



8.3.6.3. 数据库资产连接

JumpServer 提供多种方式登录数据库。例如命令行的方式 Web CLI，图形化方式 Web GUI，数据库代理直连数据库方式 DB Client，远程应用方式拉起 Navicat。

连接方式 数据库	Web CLI	Web GUI	数据库客户 端	DB 连接向 导	远程应用方 式
MySQL	√	√	√	√	√
MariaDB	√	√	√	√	√
PostgreSQL	√	√	√	√	√
Oracle	×	√	√	√	√
SQL Server	×	√	√	√	√
Redis	√	×	√	√	√
MongoDB	√	×	-	-	√
ClickHouse	√	×	×	×	√

- √：该符号表示 JumpServer 使用该种连接方式连接数据库已实现
- ×
- ：该符号表示这种连接方式 JumpServer 计划支持，根据排期开发中。

(三)Web CLI 方式

在 Web 终端页面点击数据库，选择“Web CLI”方式连接数据库。连接结果如下图所示：

```
开始连接数据库 阿里云rds (mysql5.7) (rm-uf6i3t...) 0.1

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 201593
Server version: 5.7.35-log Source distribution

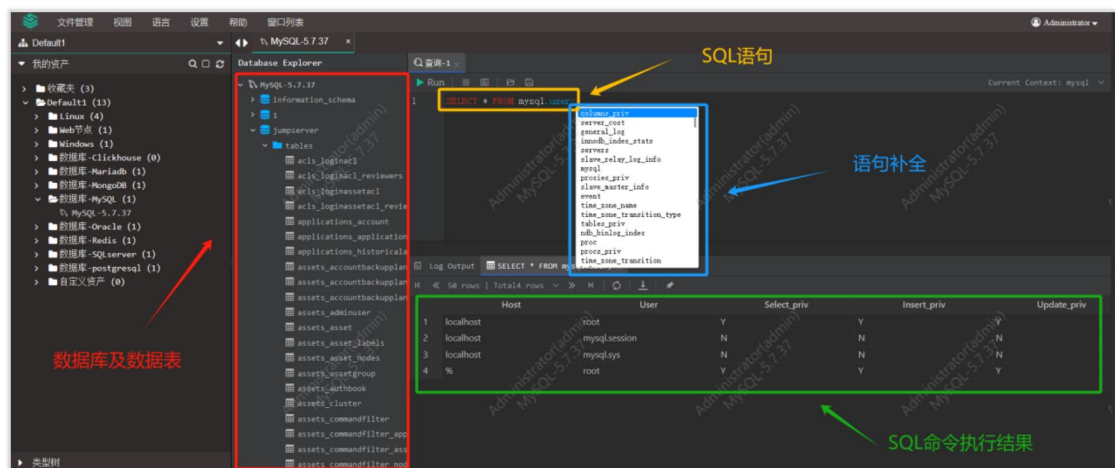
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

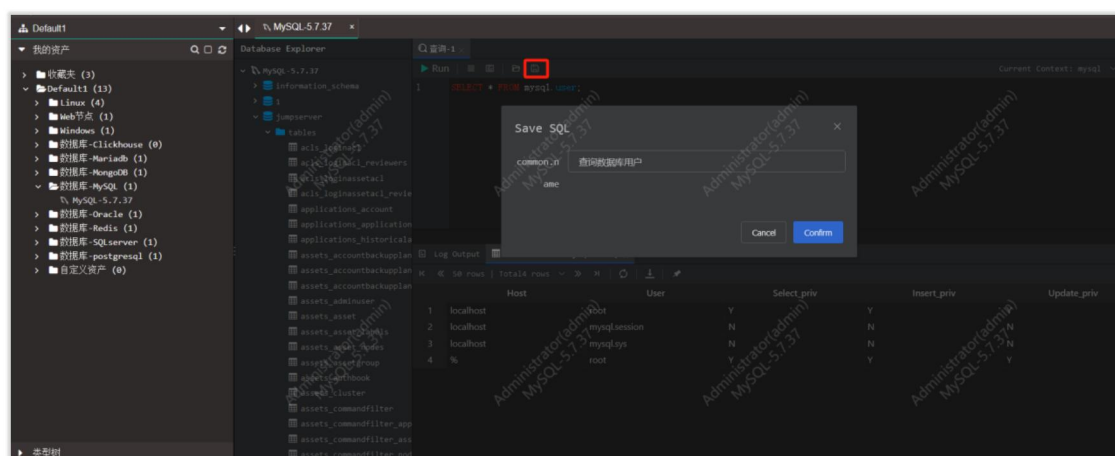
MySQL [(none)]>
```

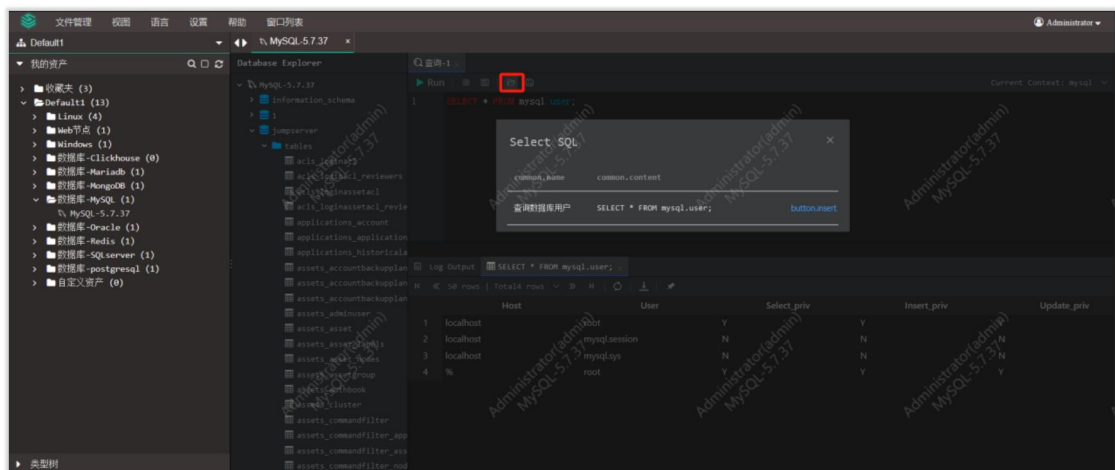
(四)Web GUI 方式

在 Web 终端页面点击数据库，选择“Web GUI”方式连接数据库，“Web GUI”方式支持对表名称与列名称自动补全。连接结果如下图所示：

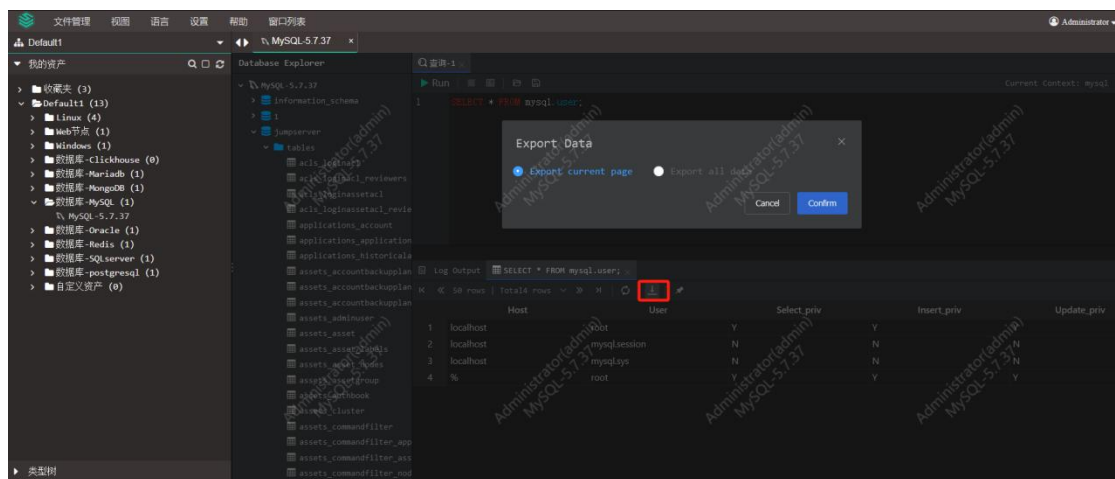


使用 Web GUI 方式连接数据库时，JumpServer 支持选中执行部署的 SQL 命令，将查询面板中的 SQL 命令收藏，方便下次继续执行：





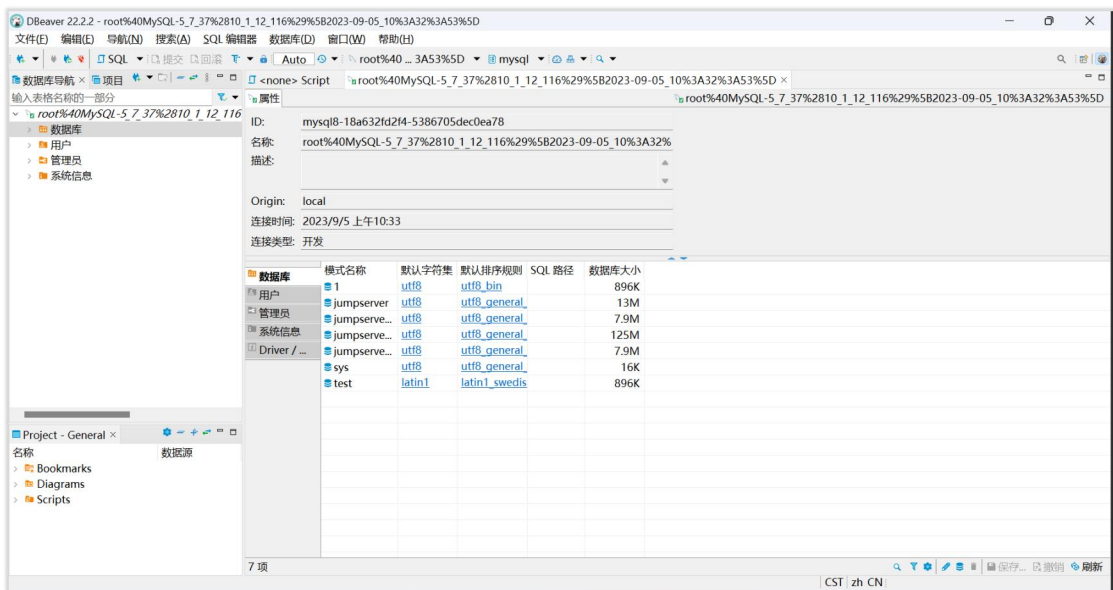
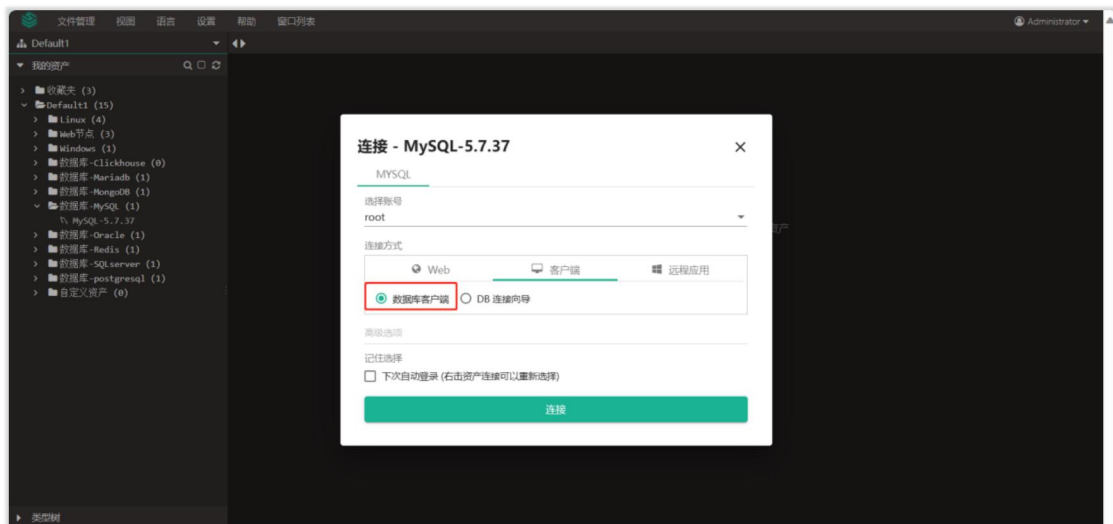
使用 Web GUI 方式连接数据库时，JumpServer 支持将 SQL 语句查询到的结果以 CVS 格式导出到本地，方便用户保存执行结果；



(五)客户端方式

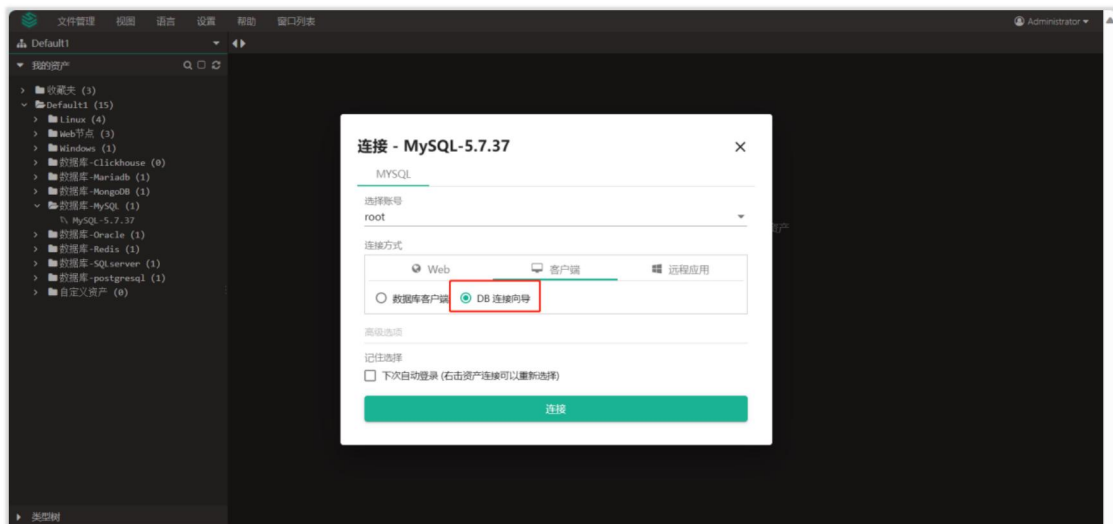
① 数据库客户端

此功能需要提前配置 JumpServer 客户端。在 Web 终端页面点击数据库，选择“客户端”方式“数据库客户端”连接数据库，该操作会拉起个人 PC 机中的客户端 DBeaver【已经配置的前提下】进行连接。



② DB 连接向导

在 Web 终端页面点击数据库，选择“客户端”方式“DB 连接向导”连接数据库生成的数据库连接信息如下所示：（“客户端”方式生成的信息提供两种连接方式连接数据库）



JumpServer 支持使用令牌连接资产时，在令牌未过期前不限制次数地使用相同的令牌来连接资产；开启需要在配置文件中添加选项，修改之后重启堡垒机服务生效。

JumpServer 配置文件默认位于：/opt/jumpserver/config/config.txt

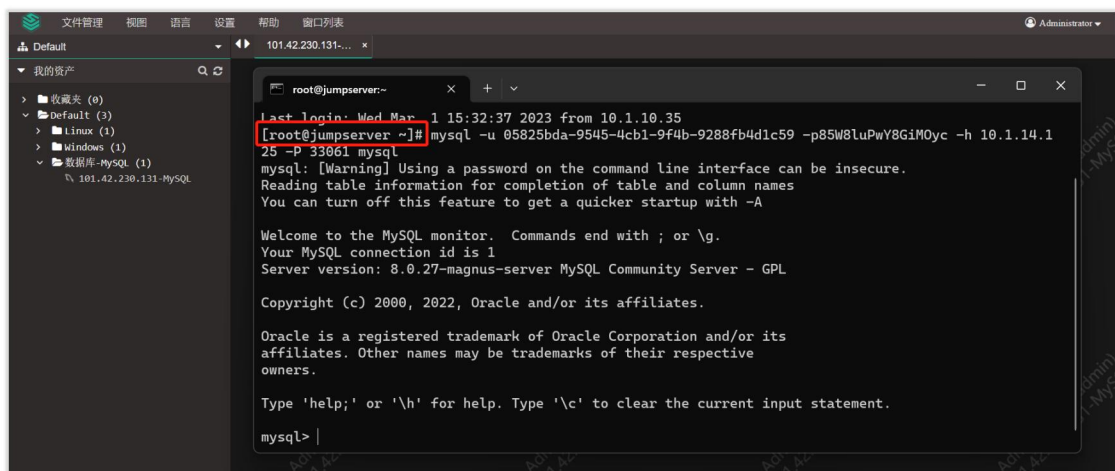
开启临时密码功能的配置项为：CONNECTION_TOKEN_REUSABLE=true



方法一：复制生成的连接信息，到 Terminal 中执行命令连接数据库；此种连接方式需要在 Terminal 中安装客户端。此处以 Linux 为例，需要打开命令行并安装 MySQL 客户端。



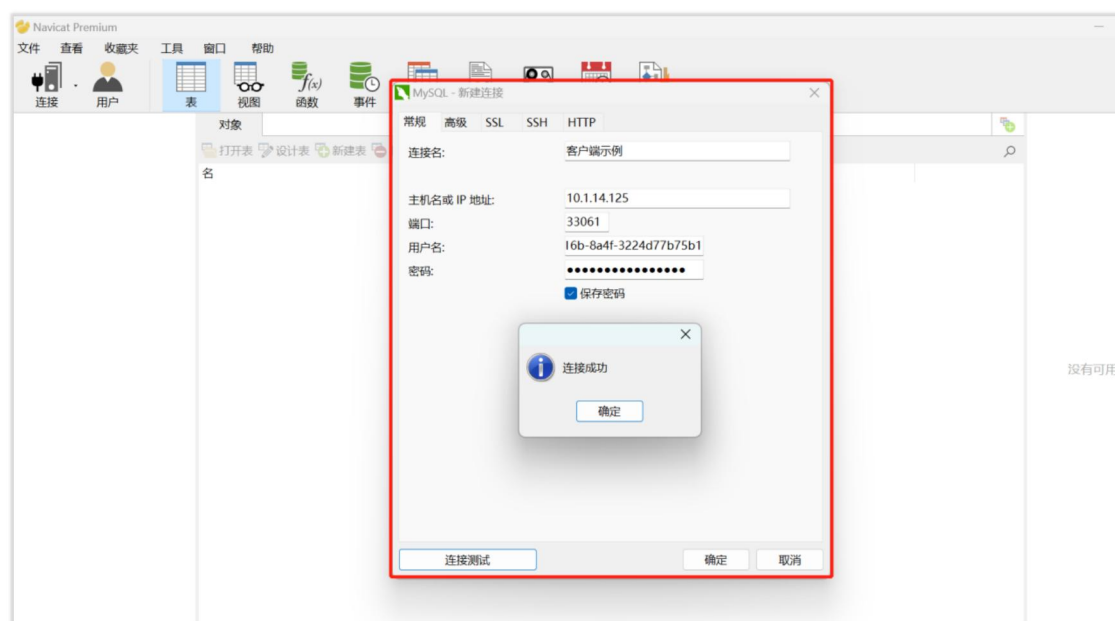
连接成功如下图：



方法三：使用数据库管理工具（例如 Navicat、SQLyog 等）连接数据库，此种连接方式不限制数据库客户端类型，复制 JumpServer 提供的加密信息，直接打开 Navicat 等连接软件输入相应参数即可连接成功。

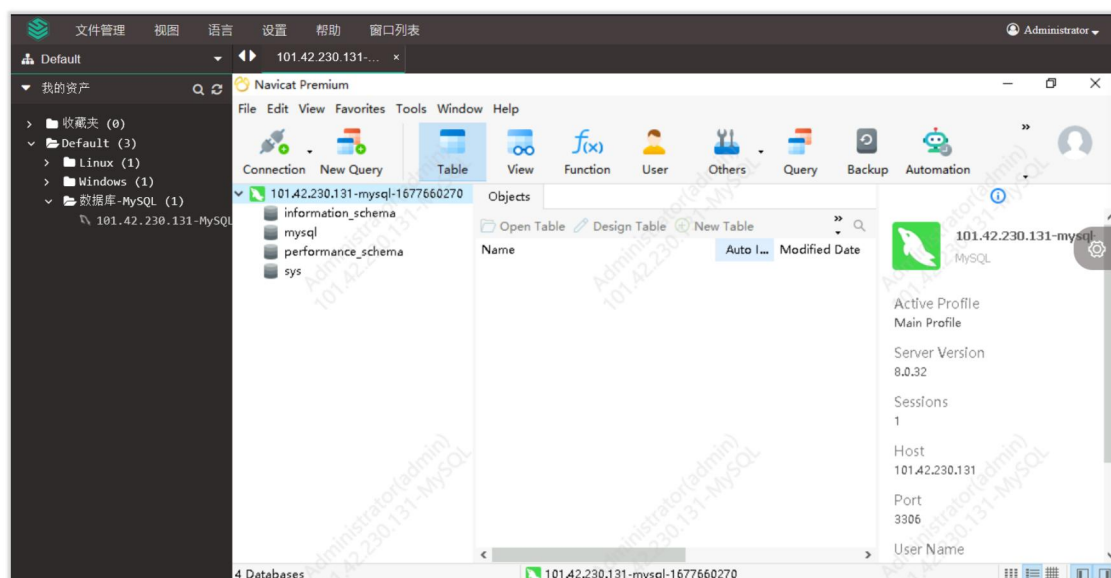


连接成功如下图所示：



(六) 远程应用方式

在 Web 终端页面点击数据库，选择“远程应用”方式连接数据库。使用此方式的前提，需要管理员提前设置了远程应用并发布了远程应用 Navicat 或者 DBeaver（管理员设置远程应用参考：[正文-远程应用配置](#)）。连接结果如下图所示：

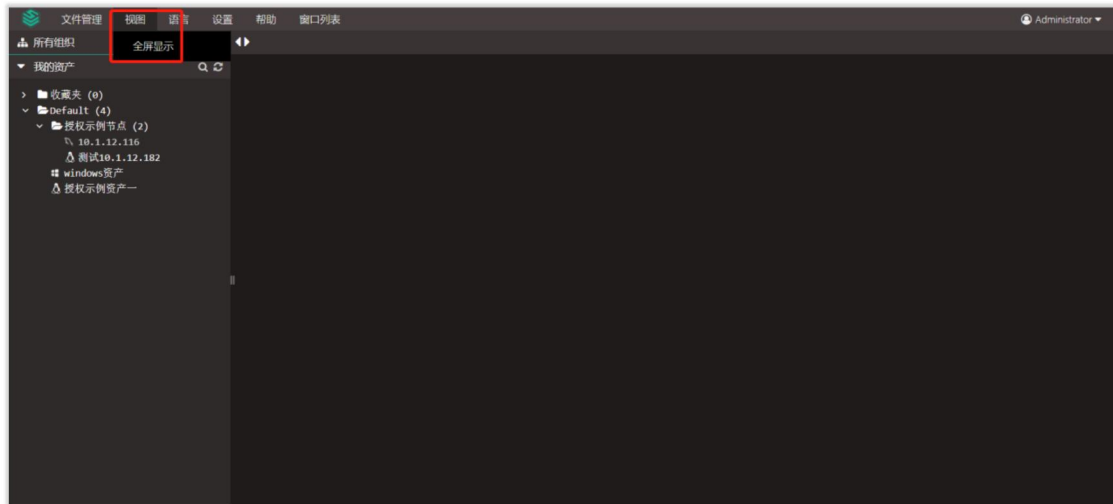


8.3.7. 文件管理

在 Web 终端页面，点击<文件管理>按钮，选择<连接>按钮即可进入文件管理模块。文件管理模块具体解释可参考 7.4 文件管理

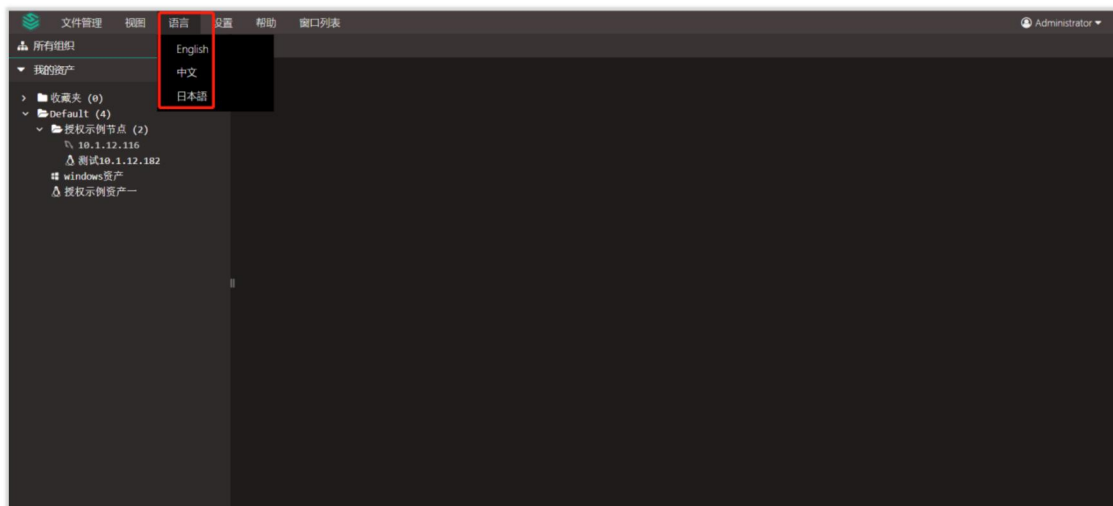
8.3.8. 视图

[<视图>](#)按钮主要用来全屏显示资产连接（连接资产时）。



8.3.9. 语言

JumpServer 支持多种语言，包含英语、中文、日语。[<语言>](#)按钮可以切换 JumpServer 系统的显示语言。



8.3.10. 设置

[<设置>](#)按钮主要针对于 JumpServer 资产连接过程中的设置信息。包含：基本配置、图形化、命令行。

基本配置：

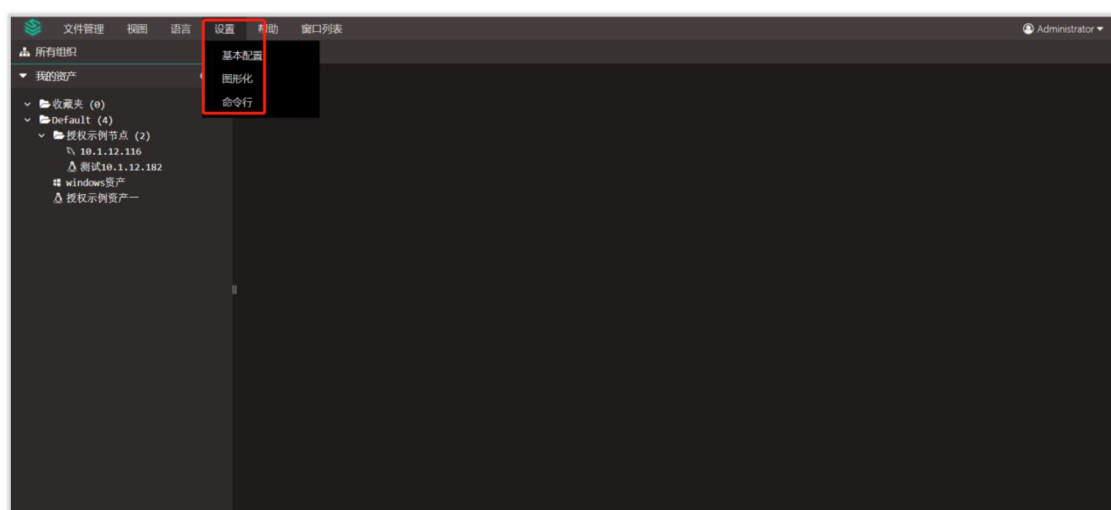
- 异步加载资产树：资产连接中是否实时加载资产树。

图形化：

- RDP 分辨率：修改 RDP 分辨率，默认为 Auto；
- RDP 智能大小：是否开启 RDP 智能大小，开启后可自动计算匹配出本地窗口大小与远程窗口大小的缩放比例。
- 键盘布局：选择连接 Windows 资产时使用的键盘布局。
- RDP 客户端选项：RDP 客户端连接是否开启全屏与磁盘挂载；
- 远程应用连接方式：选择远程应用的连接方式，Web 或者客户端方式。

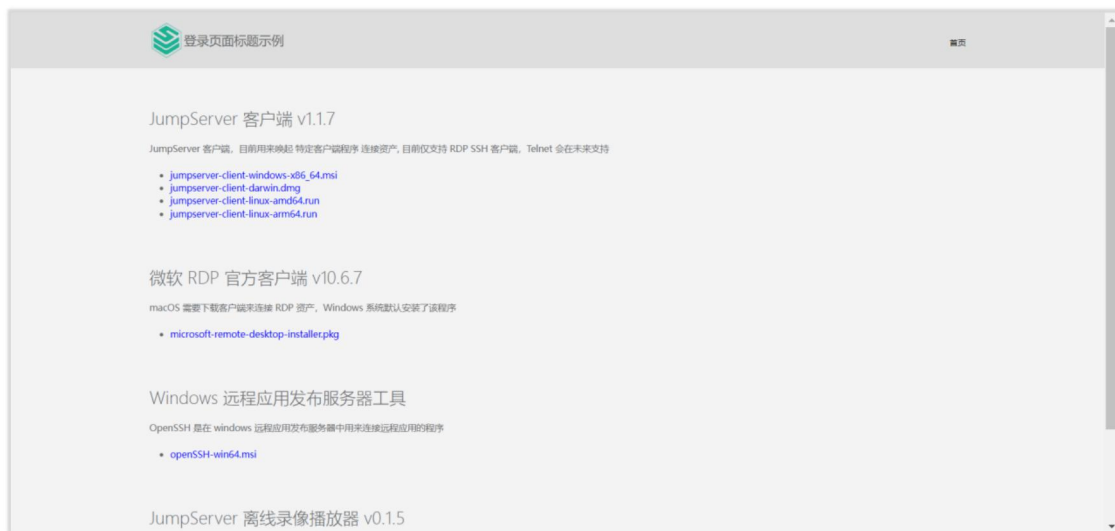
命令行：

- 字符终端字体大小：设置终端字体的大小显示；
- 字符终端 Backspace As Ctrl+H：在命令行中是否开启快捷键 Ctrl+H 作为删除键；
- 右键快速粘贴：命令行是否开启右键快速粘贴。



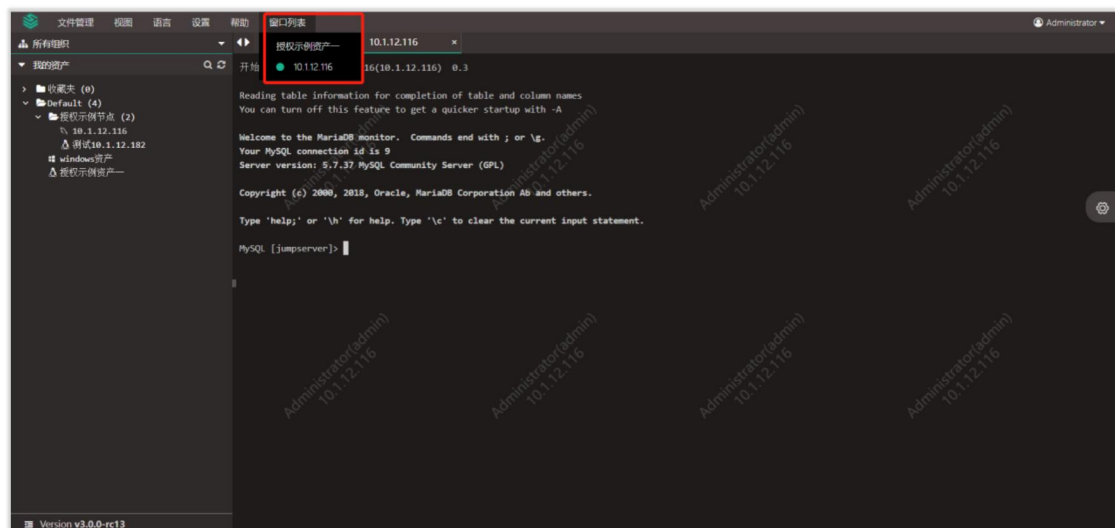
8.3.11. 帮助

[<帮助>](#)按钮主要分为三个模块，文档、支持、下载三个模块。文档与支持跳转链接可进行修改，修改按钮位于：系统设置→其它设置→导航栏链接模块。下载链接跳转至 JumpServer 系统周边工具下载，包含：JumpServer 客户端、微软 RDP 客户端、JumpServer 离线录像播放器等。



8.3.12. 窗口列表

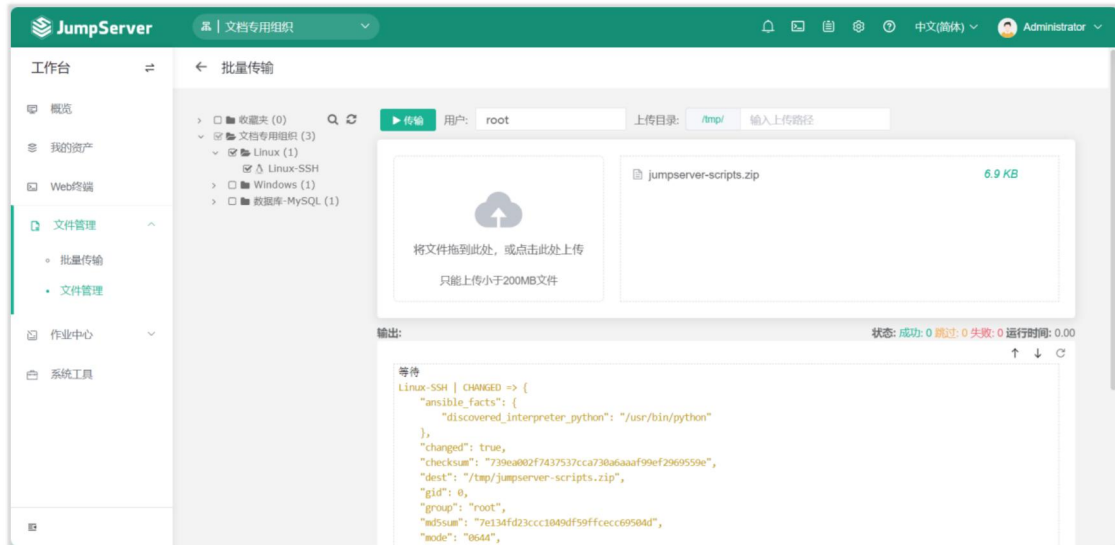
<窗口列表>按钮可查看正在连接的所有会话并进行切换。



8.4. 文件管理

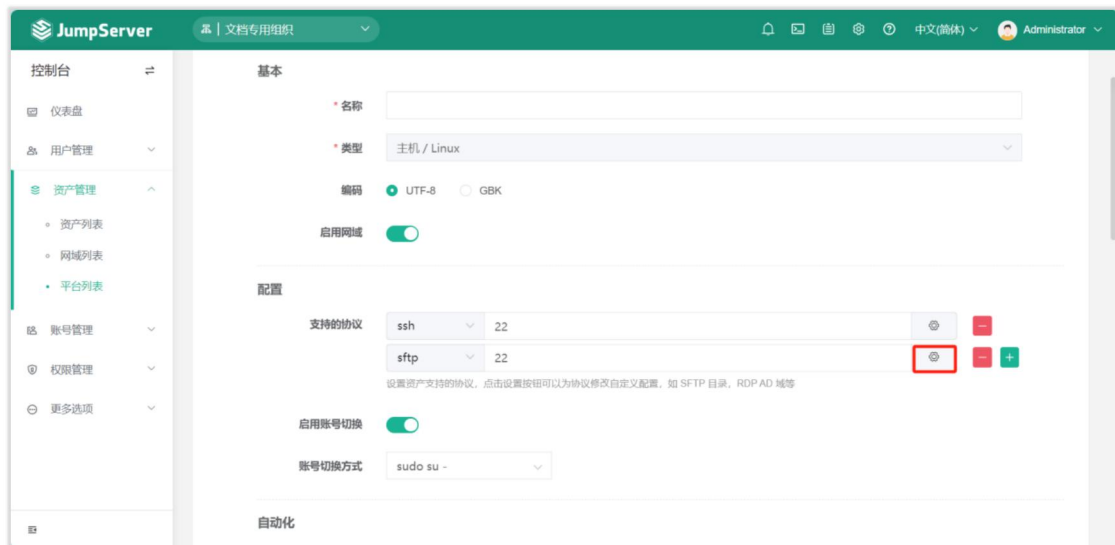
8.4.1. 批量传输

JumpServer 支持对文件的批量发送功能，即将本地文件批量的上传到多个 JumpServer 纳管的资产中。



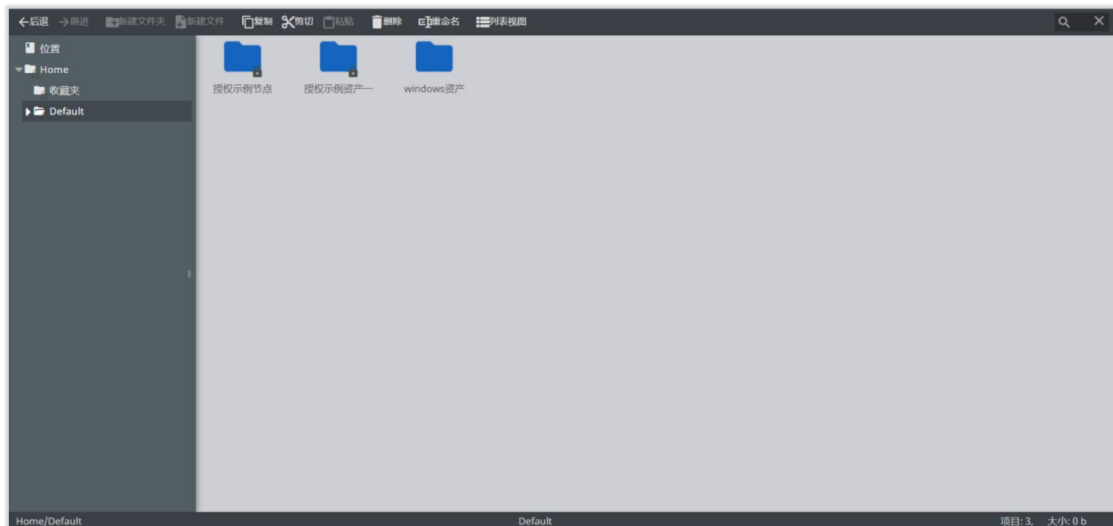
8.4.2. 文件管理

上传下载默认的 SFTP 目录默认为 `/tmp` 路径。SFTP 目录与资产平台进行绑定。JumpServer 默认平台的 SFTP 目录无法修改，如需修改需要新建一个系统平台，然后进行调整。





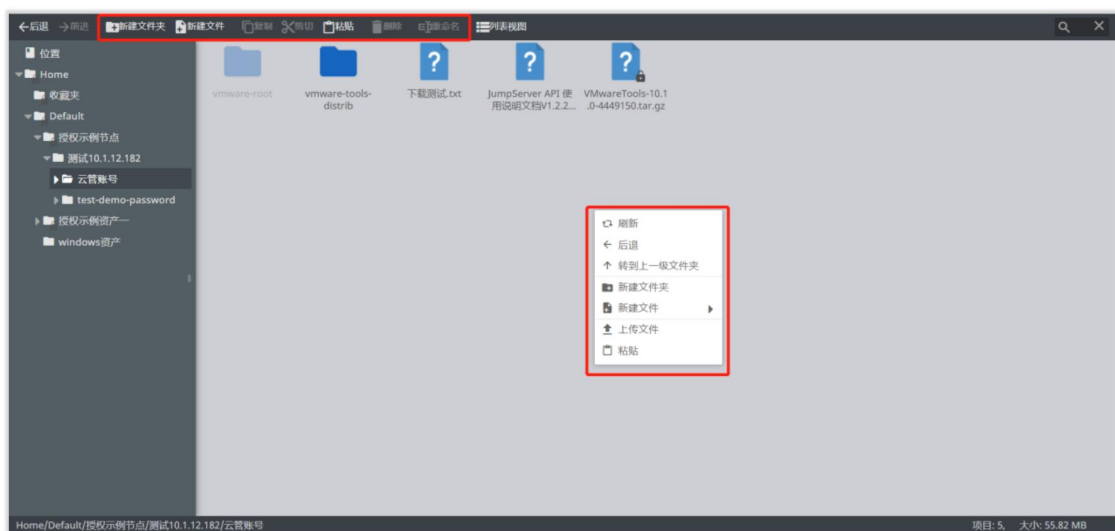
文件管理页面如下图所示，右击上方黑色区域选择文本标签可显示标签含义：



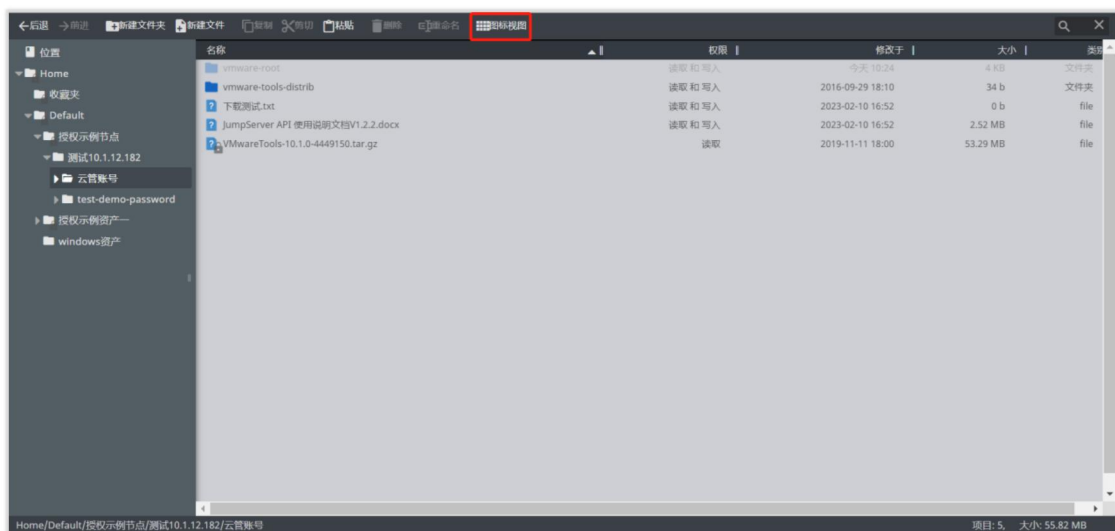
点击右侧节点树对应信息，即可进入资产中的 **SFTP** 目录。当某个资产有且仅有一个账号授权时，点击资产名称即可直接进入该资产对应授权用户的 **SFTP** 目录，当某个资产拥有多个账号授权时，需点击资产名称后选择资产对应的账号才能进入对应的 **SFTP** 目录。



进入 SFTP 目录后，即可对文件夹或文件对应操作。操作方式支持两种：第一种方式：直接在右侧页面右击唤出操作菜单；第二种方式：上方黑色部分的按钮进行对应的操作。



JumpServer 支持调整展示文件的视图。调整按钮与调整之后的视图如下所示：

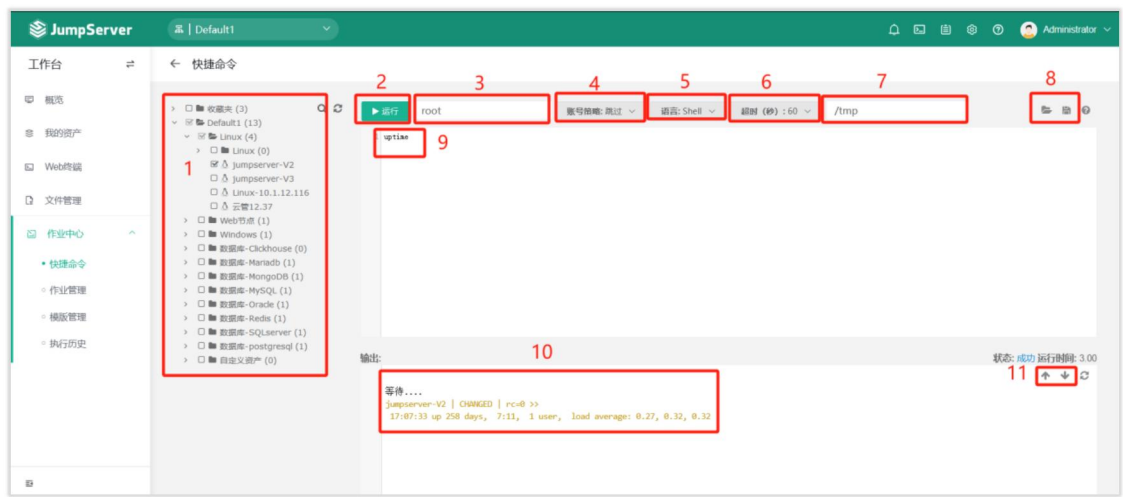


8.5. 作业中心

作业中心是 JumpServer 针对于资产执行批量命令的自动化模块，目前仅支持 SSH 协议的资产自动化，建议每次任务的并发数不超过 50，以保证 JumpServer 系统与其他自动化任务稳定运行。

8.5.1. 快捷命令

快捷命令是对用户有权限的资产进行批量命令处理。在资产树中选择需要执行快捷命令的资产，选择账号信息、超时信息 etc。



详细模块说明：

序号	名称	说明
● 1	资产树	选择执行命令的资产。
● 2	运行	运行命令的按钮。
● 3	运行用户	目标资产运行命令的用户。
● 4	账号策略	<ul style="list-style-type: none">● 跳过● 优先特权账号● 仅特权账号
● 5	语言	目前支持的语言类型有：Shell、PowerShell、Raw、Python、MySQL、PostgreSQL、SQL Server。
● 6	超时（秒）	执行命令超时时效，目前支持：10、30、60，单位为秒。
● 7	运行目录	执行该快捷命令的目录。

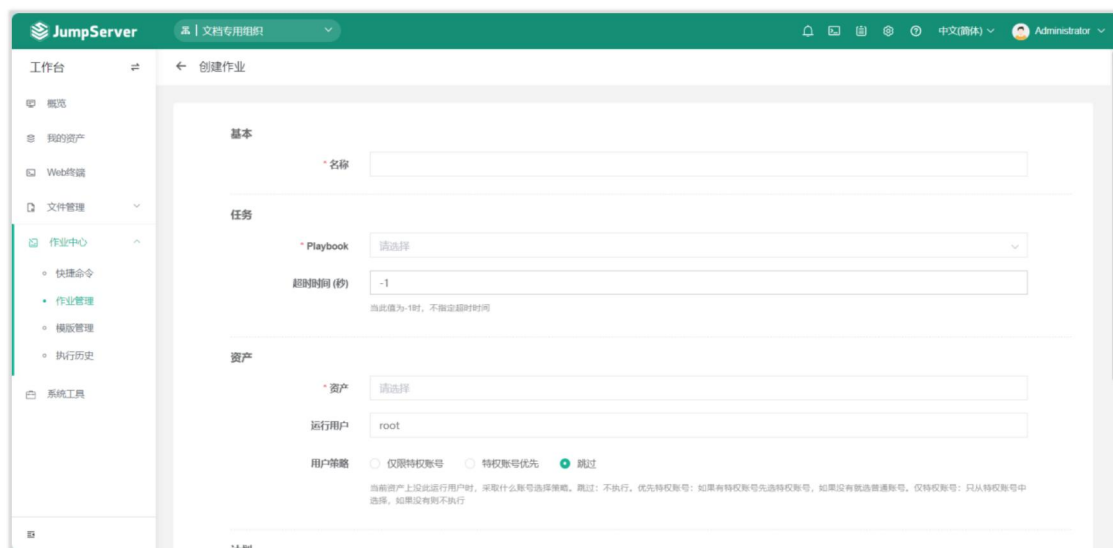
● 8	打开命令	打开模版管理模块中的命令进行使用。
	保存命令	保存当前命令到模版管理模块中。
● 9	命令输入区域	需要执行的命令。
● 10	结果输出区域	执行命令的结果。
11	清屏与滚动	清除所有命令执行的结果。

8.5.2. 作业管理

作业管理功能主要针对命令、Playbook 两种作业类型创建作业任务，并设置定期执行作业任务或手动执行作业任务。

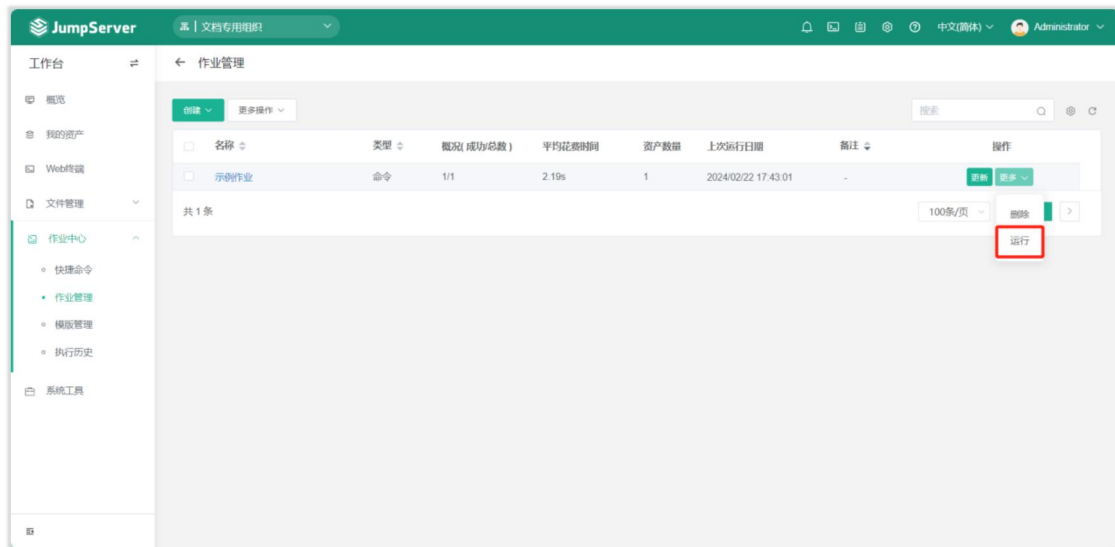
8.5.2.1. 创建作业

以 Playbook 类型作业任务为示例。作业任务中的 Playbook 参数需要在模版管理功能中提前创建好 Playbook 模版后进行选择。点击作业中心下拉框选择作业管理按钮进入作业管理页面，点击<创建>按钮，创建一个 Playbook 作业。



8.5.2.2. 执行作业

点击创建好的 Playbook 示例作业后方的更多下拉框，选择<运行>按钮，即执行 Playbook 作业。



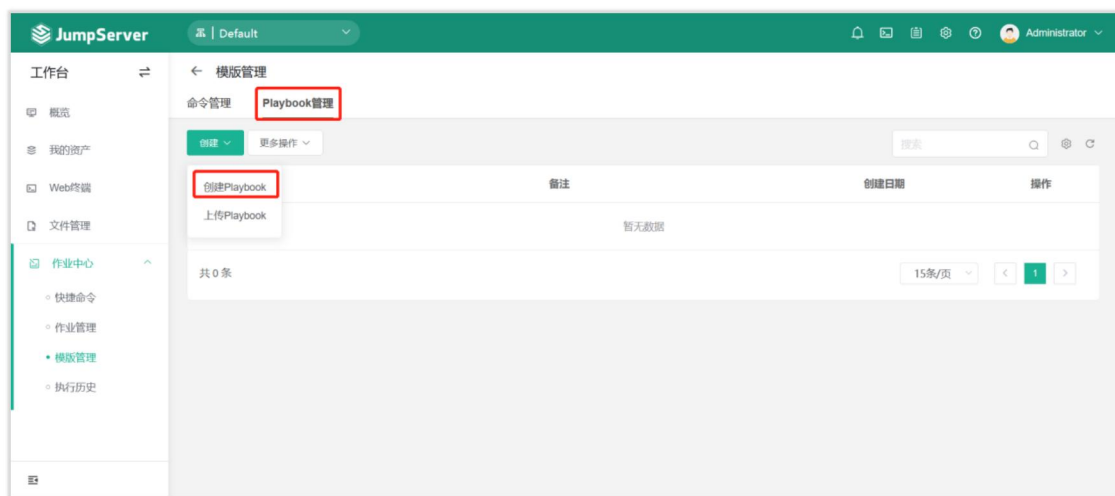
8.5.3. 模版管理

模版管理功能主要针对命令与 Playbook 两种类型来创建模版，方便用户在快捷命令和作业管理功能中快速创建自动化任务。

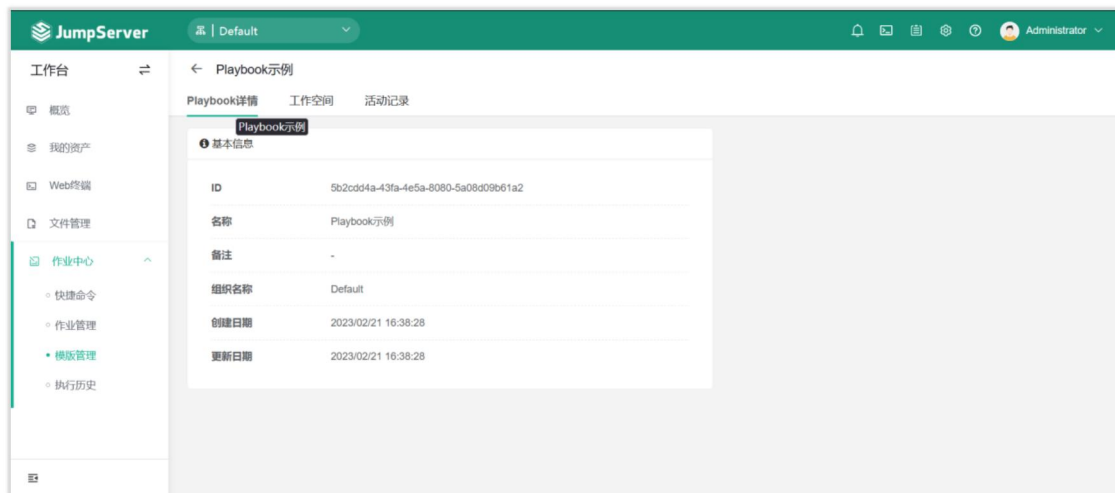
8.5.3.1. 创建模版

以 Playbook 类型模版为示例，在目标资产中创建一个 UID 为 4000 的用户。

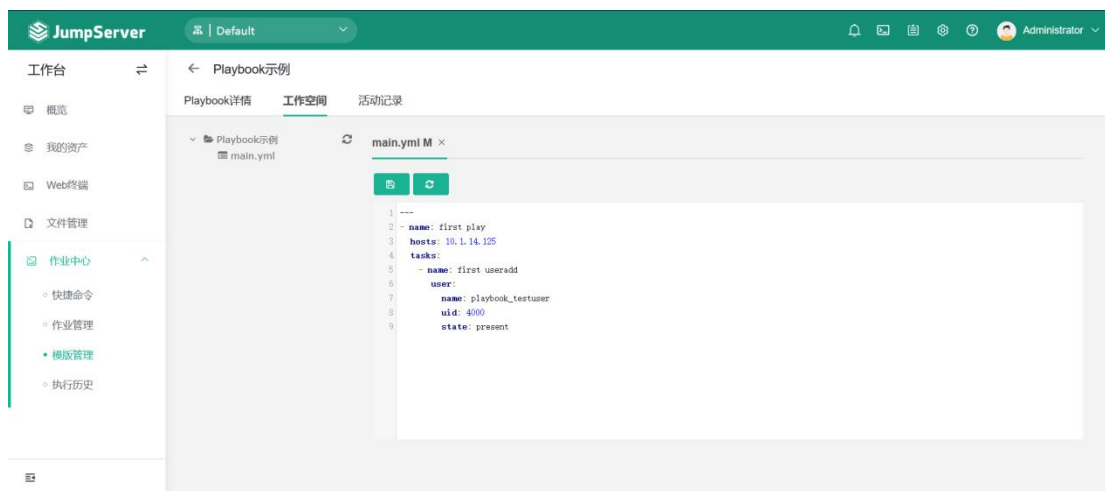
点击作业中心下拉框选择<模版管理>按钮进入模版管理页面，选择“Playbook 管理”页签，点击创建按钮，创建一个 Playbook 模版。



填写 Playbook 模版的名称即可创建成功。创建成功后点击 Playbook 模版名称进入详情页中。



点击“工作空间”页签创建 main.yml 如下图所示：



点击<保存>按钮，保存创建的 main.yml。

8.5.3.2. 模版执行

模版执行请参考[正文-作业管理](#)。

8.5.4. 执行历史

执行历史页面主要是针对作业中心模块中的任务进行历史记录，可以在该页面查看任务执行的详情和具体输出信息。

JumpServer

Default

Administrator

工作台

概览

我的资产

Web终端

文件管理

作业中心

快捷命令

作业管理

模板管理

执行历史

执行历史

搜索

清除

ID	命令	任务类型	是否完成	成功	时间	创建日期	操作
dd8e89d0-0120-42e5-9dec-b2981d40c41f	Default Administrator...	playbook	✓	✓	2.21s	2023/02/21 16:58:04	详情 输出
94a00daa-fe2c-4b1e-9a3e-be58b78ecce	Default Administrator...	playbook	✓	✓	2.28s	2023/02/21 16:58:04	详情 输出
a05cea08-1828-4306-a5d5-7a0f7e138e11	shell uptime	adhoc	✓	✓	3.35s	2023/02/21 16:16:51	详情 输出
ctb6b0ce-4740-41e4-b0bc-1d9022aa68ce	shell ls	adhoc	✓	✓	8.41s	2023/02/21 16:14:54	详情 输出

共 4 条

Celery任务日志 - JumpServer 开源堡垒机 - Mozilla Firefox

10.1.14.125/ui/#/ops/celery/task/d6eb44db-0b0d-4c90-8590-357514abb8c0/log?tab=80%

Linux SSH | CHANGED | rc=0 >>
sudoedit -ks.cfg
rmv.sh
oracle
oraeditg_root
package
templates
Videos
Task ops.tasks.run_ops_job_execution[d6eb44db-0b0d-4c90-8590-357514abb8c0] succeeded in 8.472747958025561s: None

9. 工单

工单功能主要负责授权工单的申请与审核、命令过滤与资产登录的审核。JumpServer 授权申请支持二级审批流程；工单功能支持对用户登录请求行为以及命令过滤功能进行控制。用户点击申请、申请授权工单信息，根据设置完成的流程对应的审批人审批通过后，用户即可获得申请资产的权限或用户登录请求与命令过滤。

9.1. 我的申请

我的申请页面主要进行资产授权的申请、查看资产授权工单详情。

9.1.1. 申请工单

在我的申请页面点击[<申请工单>](#)按钮。选择[<申请资产授权>](#)按钮，进入资产授权申请页面如下所示：

The screenshot shows the JumpServer web interface for creating a ticket. The top navigation bar is green with the JumpServer logo and user information (Administrator). The left sidebar contains links for 'Ticket List', 'My Applications', 'Pending Approval', and 'Workflow Settings'. The main content area is titled 'Create Ticket' and contains two main sections: 'Basic' and 'Authorization Request'. The 'Basic' section has input fields for 'Title' and 'Organization ID'. The 'Authorization Request' section has dropdown menus for 'Node' and 'Asset', both with search functionality. Below these are radio buttons for 'Request Account' and a dropdown for 'Action'.

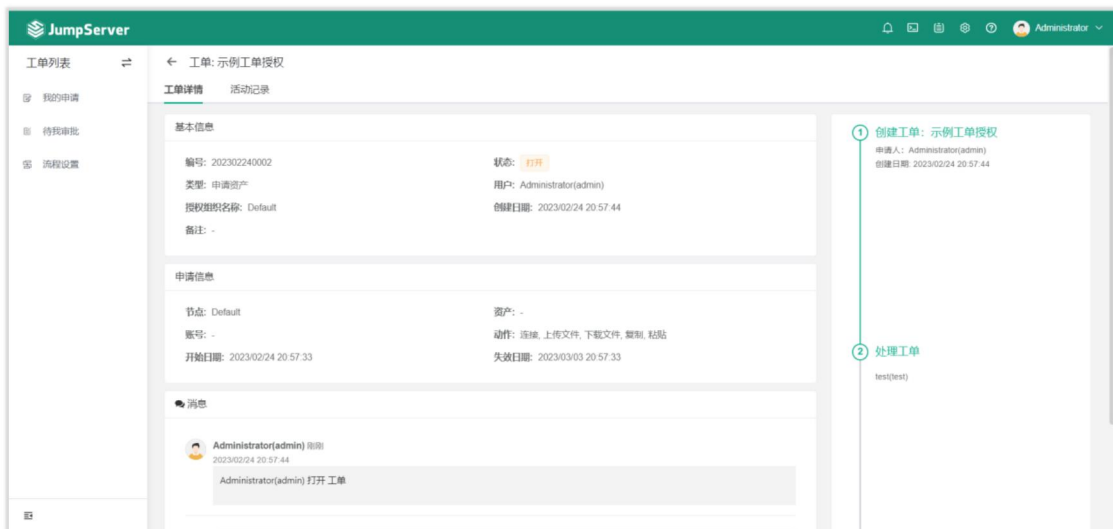


参数详细说明：

参数	说明
标题	该工单的标题。
组织 ID	该工单所申请的权限以及 JumpServer 用户所处的组织。
节点	JumpServer 用户申请的资产，节点指申请整个节点下所有资产的权限。
资产	JumpServer 用户申请的资产。
申请账号	JumpServer 用户申请的资产所使用的登录账号。
动作	JumpServer 用户申请拥有的动作权限。
开始日期、失效日期	用户申请的权限使用的期限。

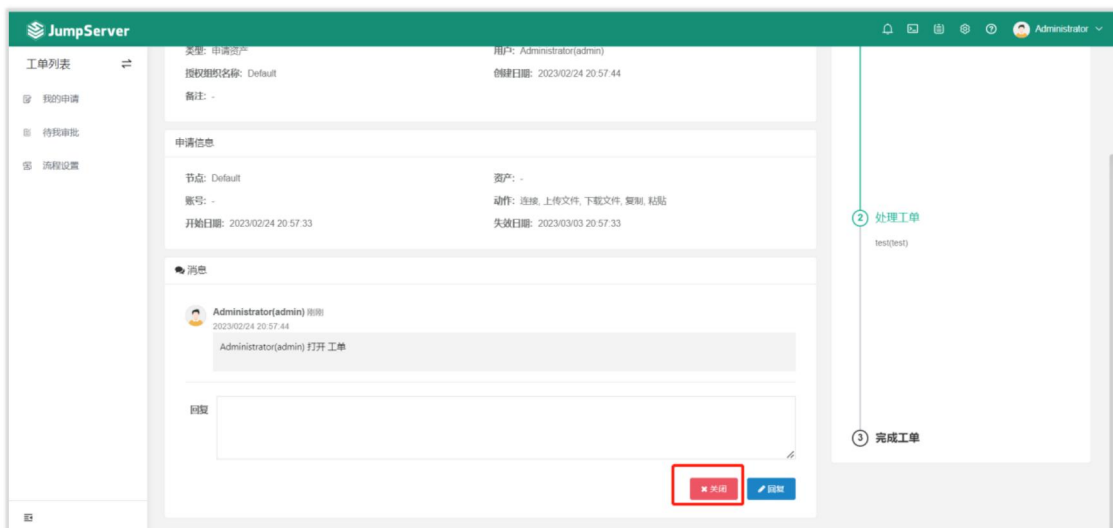
9.1.2. 查看工单

点击创建好的[工单标题](#)按钮，可进入工单详情页中。工单详情页中包含该工单的基本信息、申请信息以及审批人，同时该页面可以与审批人进行对话。



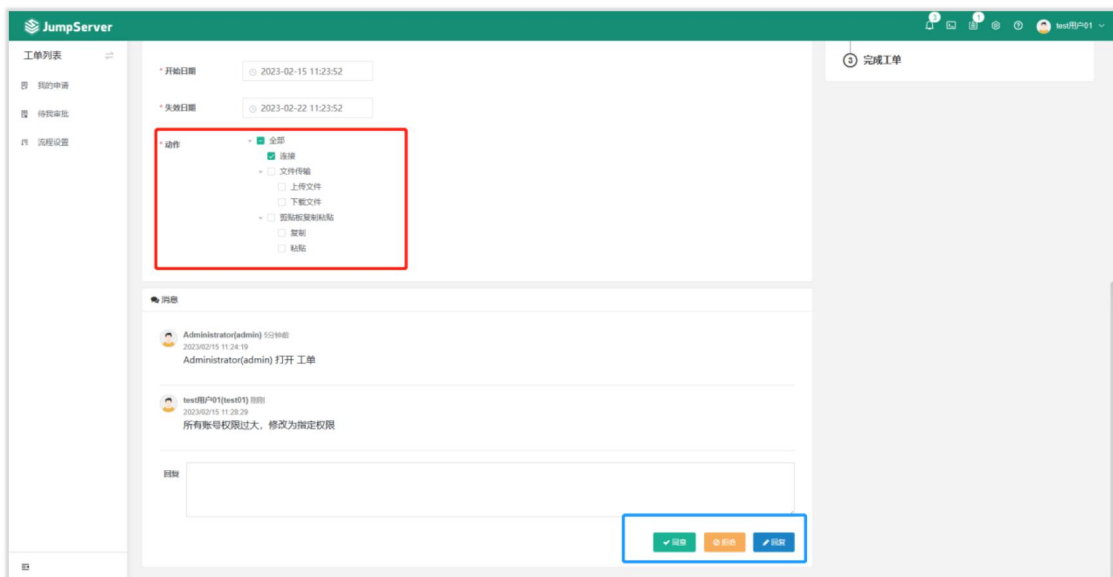
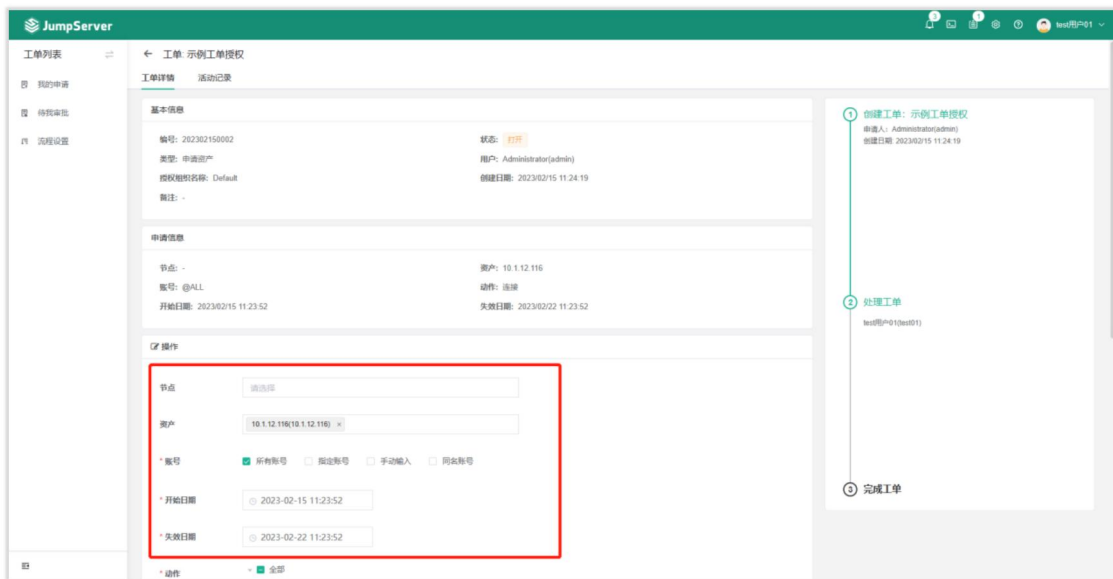
9.1.3. 关闭工单

申请人在审批人未审批前可自行关闭工单，关闭入口位于工单详情页下方。

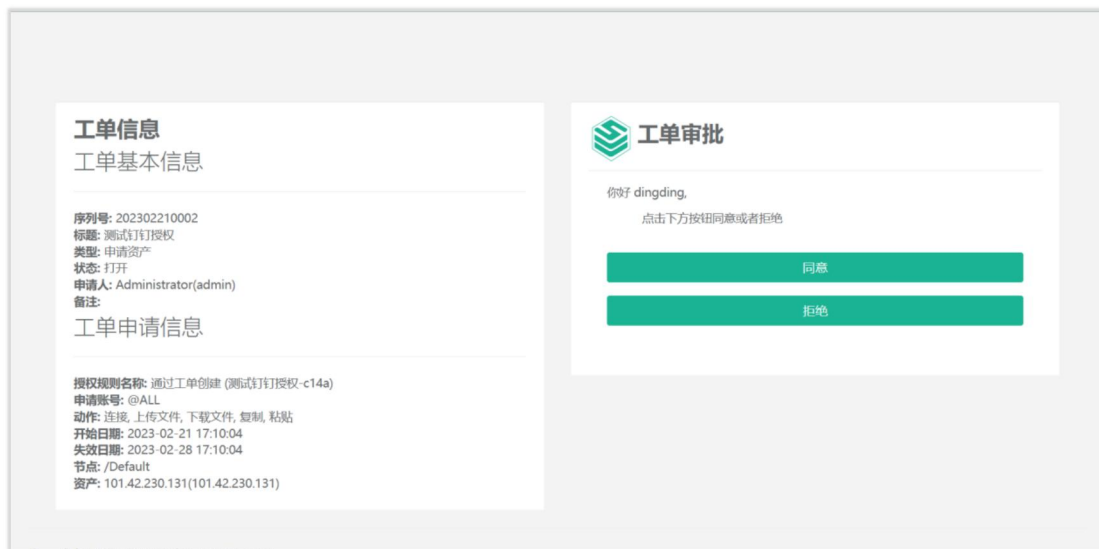
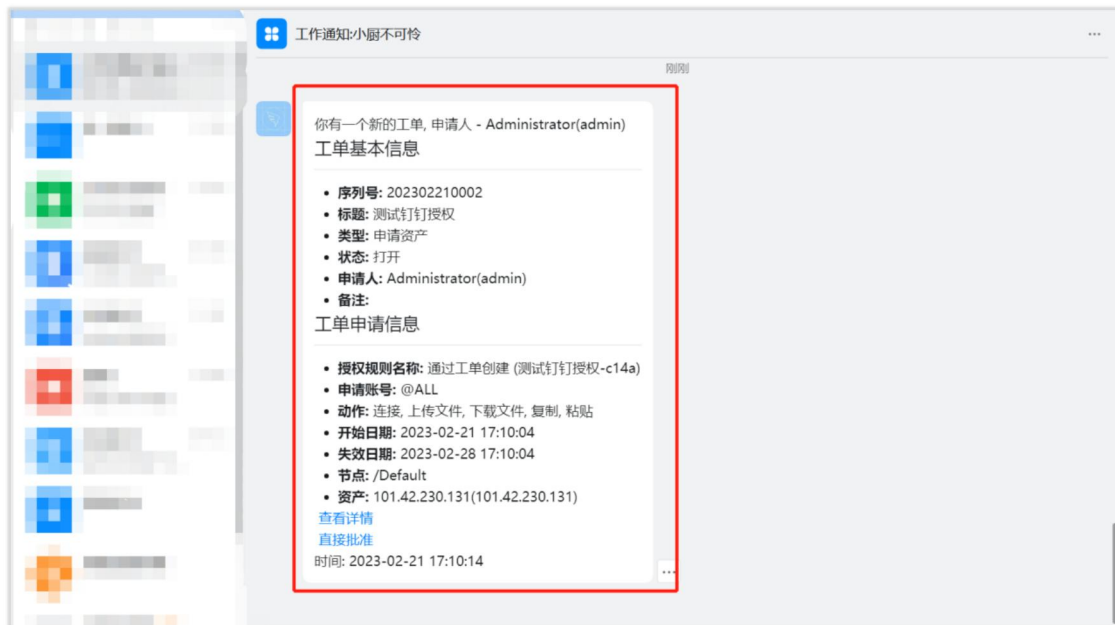


9.2. 待我审批

在待我审批页面，点击<工单名称>按钮，对工单进行查阅审批。审批人查看工单时，可修改申请人申请的资产、账号、动作等权限。



除了在 JumpServer 页面进行审批外，JumpServer 还支持企业微信、钉钉直接审批工单信息。当审批人的企业微信或者钉钉绑定后，审批人可实时在企业微信或者钉钉上对申请人的工单进行审批。

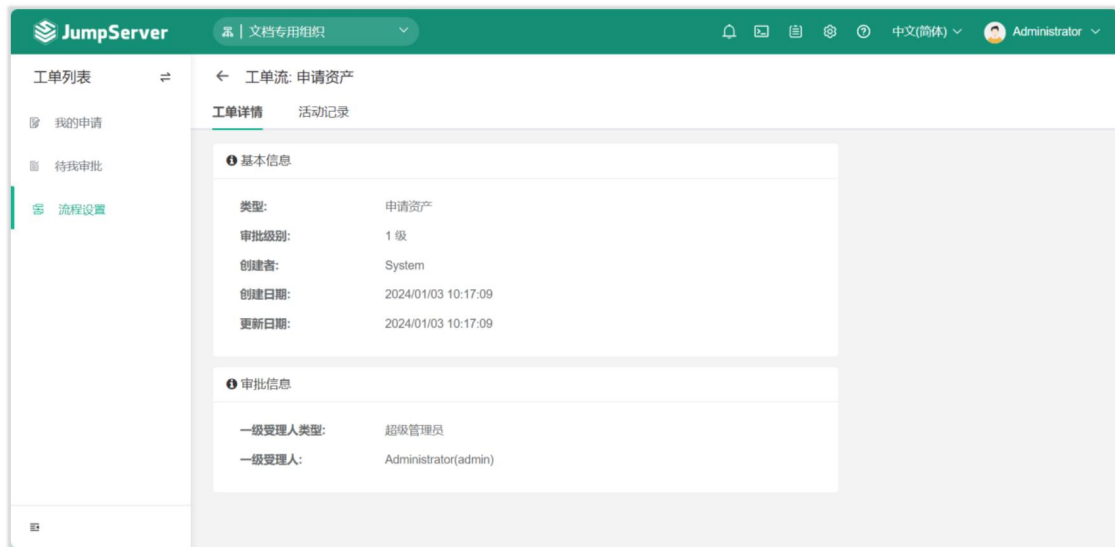


9.3. 流程设置

流程设置页面主要包含两个方面：查看申请资产的流程和更新资产的流程。

9.3.1. 查看

点击<申请资产>按钮即可进入申请资产得流程详情页，查看申请资产工单的基本信息以及审批信息。

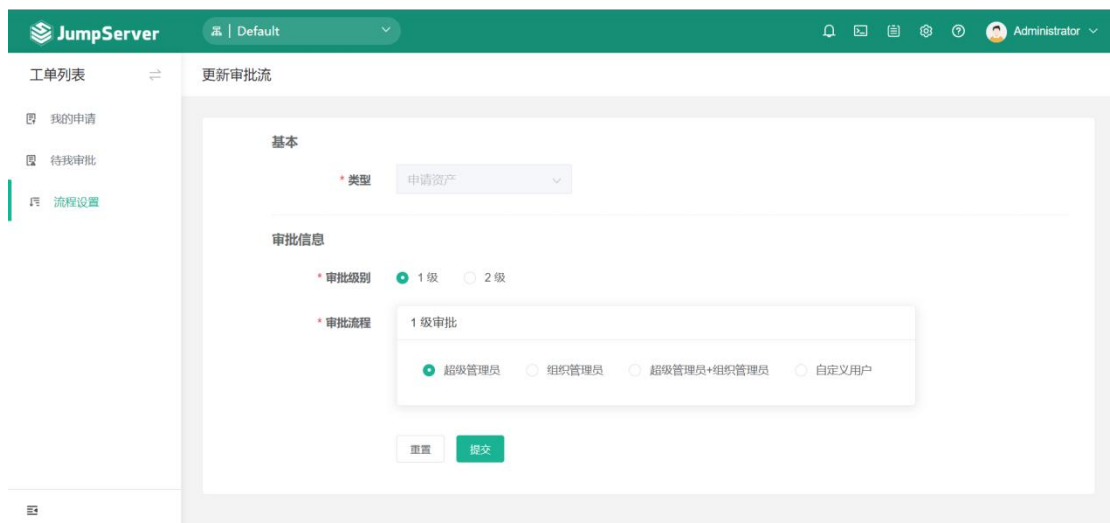


审批人流转规则如下：

- 审批人为超级管理员，申请人为普通用户时正常流转；
- 审批人为两个用户时，当其中一个用户申请工单时，审批流程只会流转到另一个用户；
- 审批人并不局限于组织内，某一个用户不存在于当前组织但只要条件符合也会流转到用户。

9.3.2. 更新

点击申请资产流程后方的<更新>按钮，即可进入流程更新页面，调整审批的级别与审批流程信息。



10. 其他

10.1. 命令行连接

JumpServer 支持使用命令行的方式连接 JumpServer 并进行操作。

命令示例如下：

命令格式：

```
ssh -p2222 jumpserverUsername@jumpserverHostIP
```

解释：

- 2222 : JumpServer 提供命令行连接的端口，默认为 2222 端口。
- jumpserverUsername : 登录 JumpServer 的用户。
- jumpserverHostIP : JumpServer 的访问地址，IP 与域名均可。

下图示例未开启 MFA 演示，如开启 MFA 验证需要在验证密码成功后输入 6 位动态码。连接成功如下图所示：

```
C:\Users\fit2cloud>ssh -p2222 admin@10.1.14.125
admin@10.1.14.125's password:
Administrator, JumpServer开源堡垒机

1) 输入 部分IP, 主机名, 备注 进行搜索登录(如果唯一).
2) 输入 / + IP, 主机名, 备注 进行搜索, 如: /192.168.
3) 输入 p 进行显示您有权限的主机.
4) 输入 g 进行显示您有权限的节点.
5) 输入 d 进行显示您有权限的数据库.
6) 输入 k 进行显示您有权限的Kubernetes.
7) 输入 r 进行刷新最新的机器和节点信息.
8) 输入 s 进行中英日语言切换.
9) 输入 h 进行显示帮助.
10) 输入 q 进行退出.

Opt>
```

连接成功后可根据命令行提示进行资产连接等操作。

注：目前该种方式暂不支持 RDP 协议的资产连接登录。

10.2. 命令行直连 JumpServer 纳管的资产

JumpServer 支持使用 SSH 工具直连 JumpServer 纳管的资产。命令格式如下所示：

命令格式：

```
ssh jumpserverUsername@systemUsername@AssetIP@jumpserverHostIP -p2222
```

解释：

- jumpserverUsername ：登录 JumpServer 的用户。
 - systemUsername ：连接资产使用的账号名称。
 - AssetIP ：被连接的资产 IP。
-
- jumpserverHostIP ：JumpServer 的访问地址，IP 与域名均可。
 - 2222 ：JumpServer 提供命令行连接的端口，默认为 2222 端口。
-

下图示例未开启 MFA 演示，如开启 MFA 验证需要在验证密码成功后输入 6 位动态码。连接成功如下图所示：

```
C:\Users\fit2cloud>ssh -p2222 admin@root@101.42.230.131@10.1.14.125
admin@root@101.42.230.131@10.1.14.125's password:
开始连接到 root@101.42.230.131 0.5
Last failed login: Sun Jan 29 17:57:55 CST 2023 from 43.134.227.248 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Sun Jan 29 17:57:45 2023 from 43.254.45.83
[root@VM-24-7-centos ~]# |
```

注：以上示例中 root 用户与 101.42.230.131 均可匹配到唯一的资产和唯一的登录名，即可直接登录到目标资产。如果该资产 IP 匹配到多个值，即需要用户手动选择资产进行登录。以上示例中，账号的密码托管至 JumpServer 中，即可直接登录到目标资产；账号的密码策略为手动输入，验证堡垒机密码后需要输入账号的密码。

10.3. SFTP 命令行操作 JumpServer 纳管的资产

JumpServer 支持通过 SFTP 协议直连 JumpServer 纳管的资产，进行文件的上传下载。命令格式如下所示：

命令行格式：

```
sftp jumpserverUsername@systemUsername@AssetIP@jumpserverHostIP -p2222
```

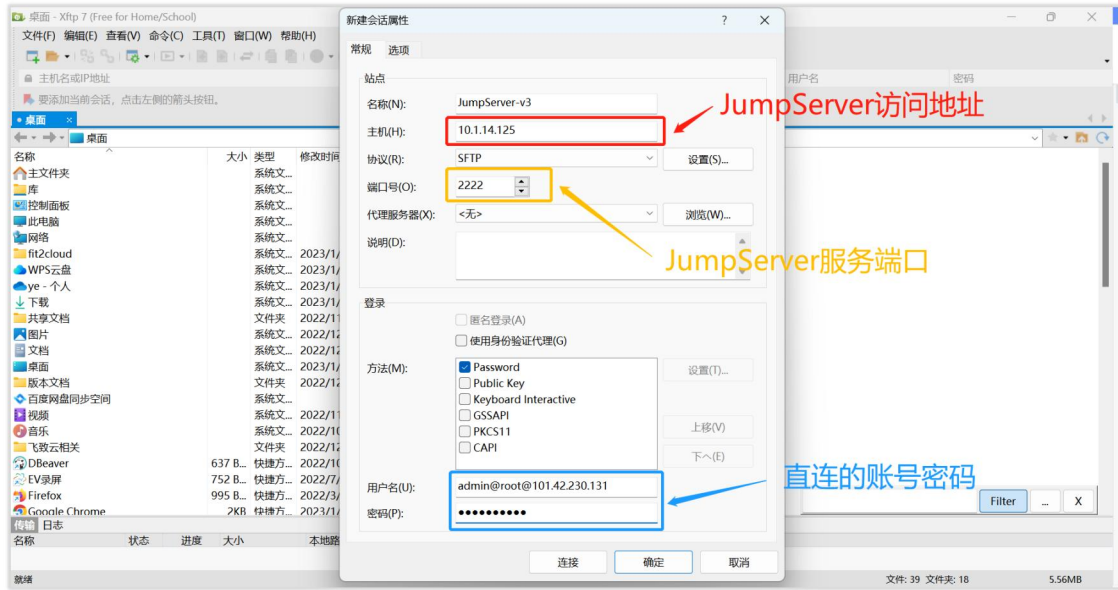
解释：

- jumpserverUsername ：登录 JumpServer 的用户。
 - systemUsername ：连接资产使用的账号名称。
 - AssetIP ：被连接的资产 IP。
-
- jumpserverHostIP ：JumpServer 的访问地址，IP 与域名均可。
-

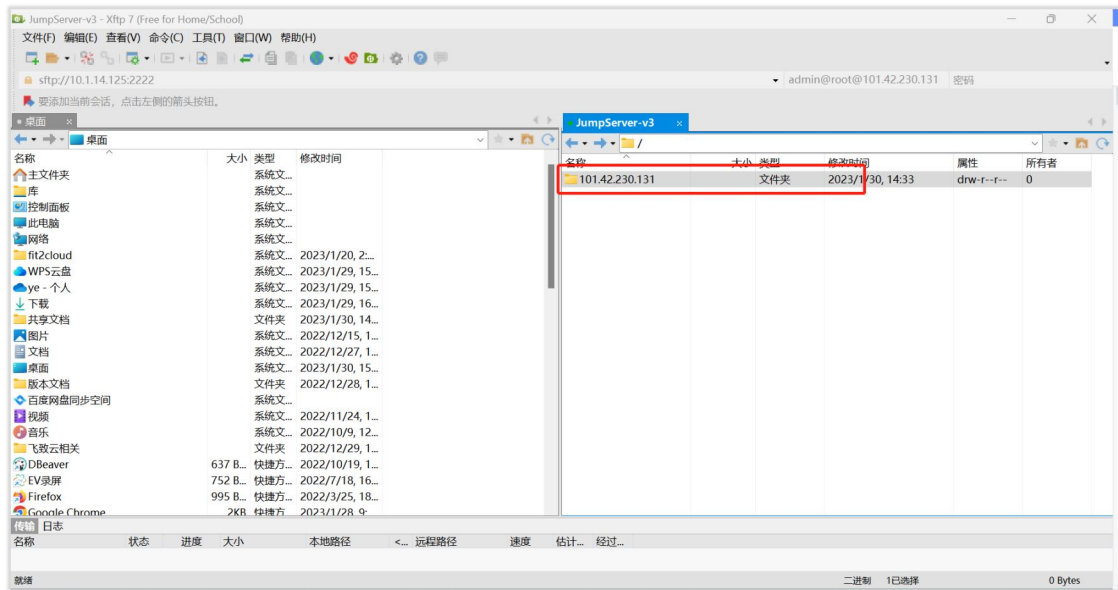
- 2222 : JumpServer 提供命令行连接的端口，默认为 2222 端口。

10.3.1. 图形化连接

JumpServer 支持通过图像化的方式进行 SFTP 操作，以上操作以 Xftp 软件进行示例，相关参数填写如下图：

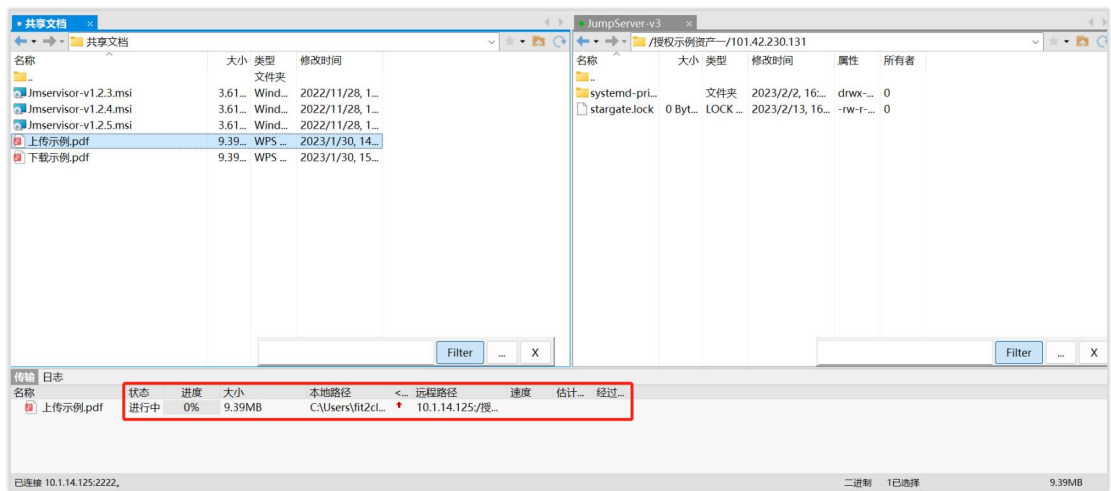


连接成功后即可在此界面进行文件的上传和下载。点击即可进入被链接资产的 SFTP 目录，默认连接成功时被连接的资产的目录只能显示连接使用系统平台设置的 SFTP 目录，默认为/tmp 目录。



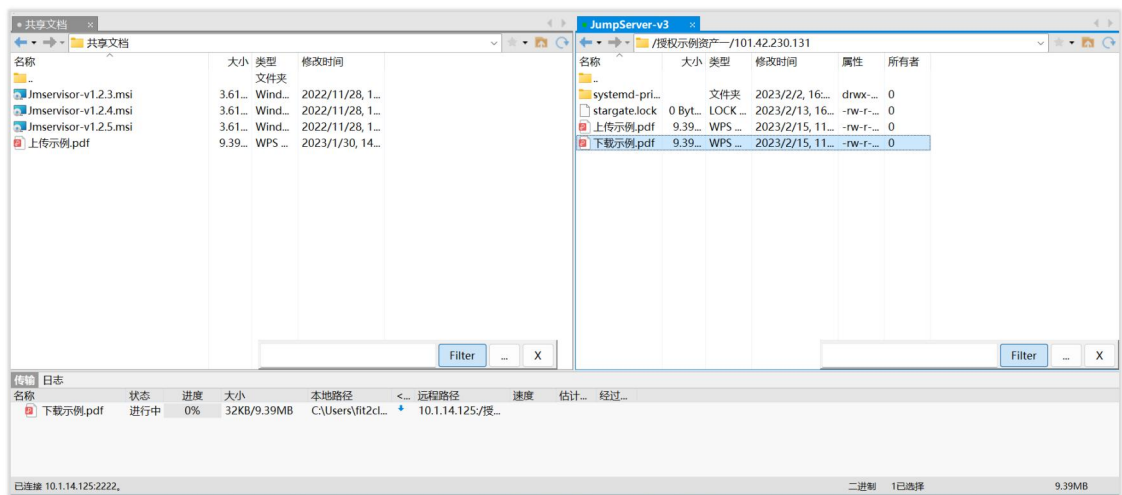
10.3.1.1. 上传文件

将本地 PC 的文件拖动到资产的模块中，即可将本地 PC 的文件进行上传。上传后的位置默认位于资产的/tmp 目录下。



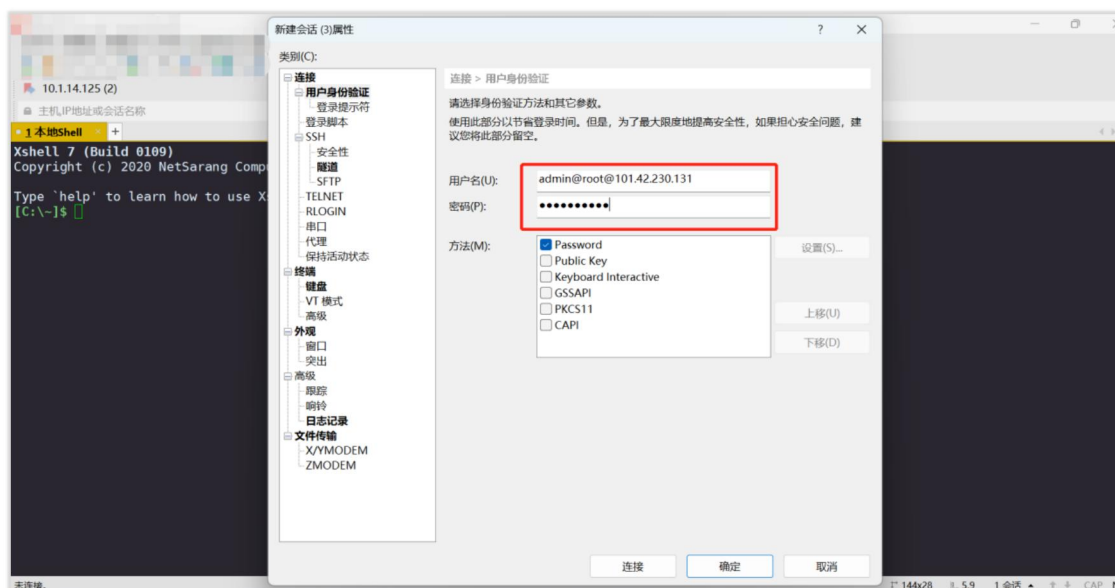
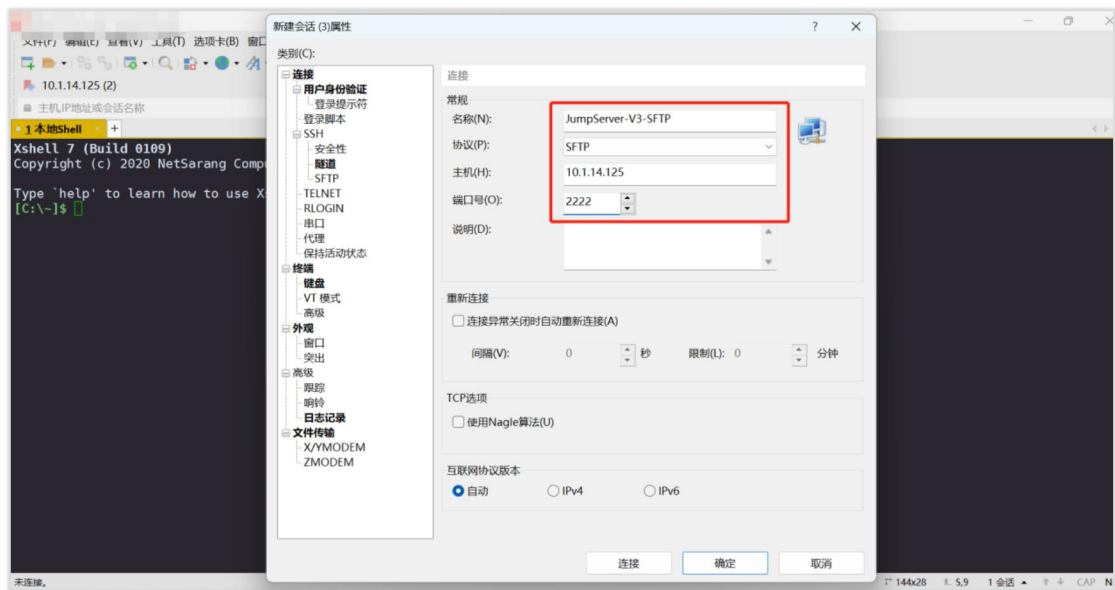
10.3.1.2. 下载文件

将资产中需要下载的文件移动到 SFTP 目录下，拖动文件到本地 PC 模块即可实现文件下载。

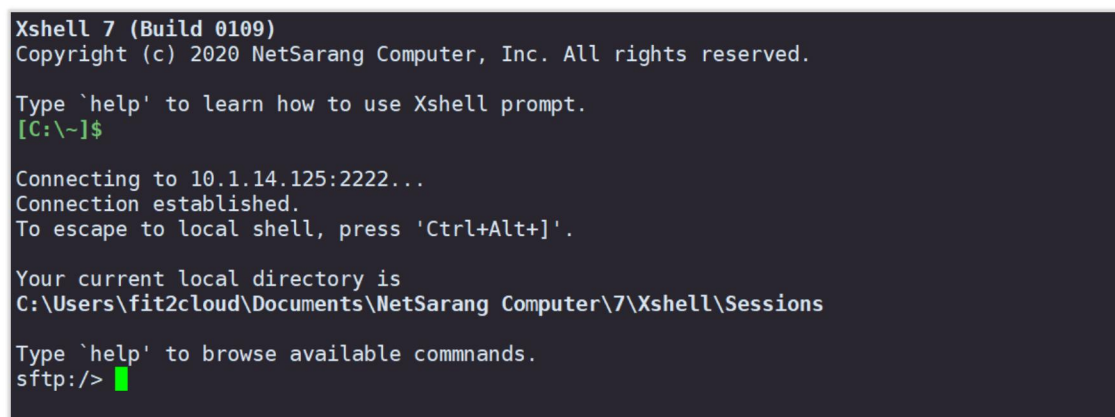


10.3.2. 命令行连接

JumpServer 支持通过命令行的方式进行 SFTP 操作，以上操作以 XShell 软件进行示例，相关参数填写如下图：



连接成功后的页面如下图所示：

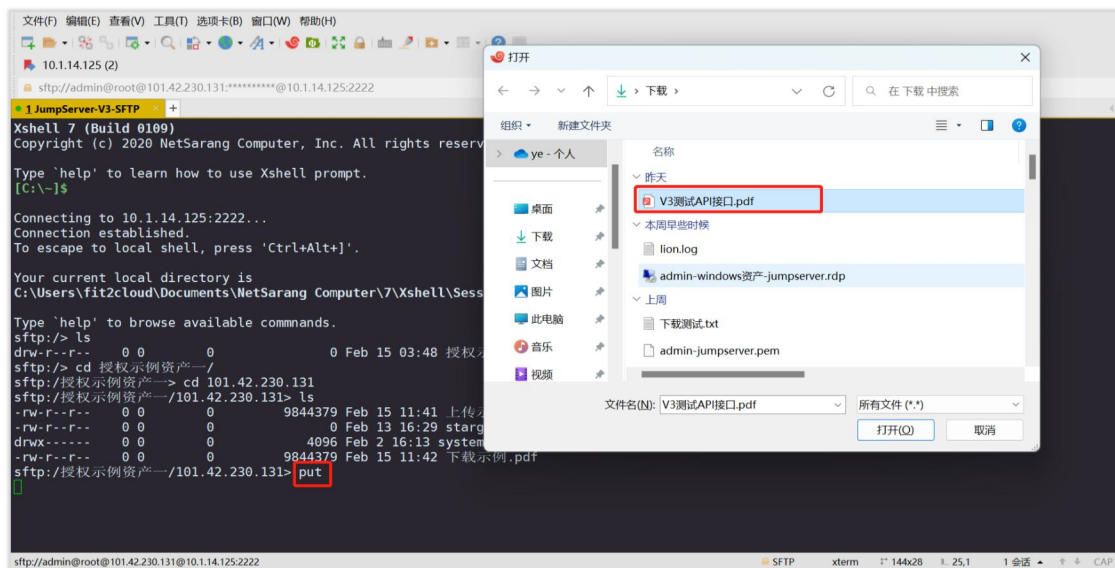


切换到需要上传下载文件的资产的 SFTP 目录下：

```
sftp:/> ls
drw-r--r--    0 0      0      0 Feb 15 03:48 授权示例资产一/
sftp:/> cd 授权示例资产一/
sftp:/授权示例资产一> cd 101.42.230.131
sftp:/授权示例资产一/101.42.230.131>
```

10.3.2.1. 上传文件

在当前目录下执行 put 命令，选择需要上传的文件确定即可上传文件。



10.3.2.2. 下载文件

在当前目录下执行切换目录的命令，并下载文件到 D 盘，具体命令如下图所示：

```
sftp:/授权示例资产一/101.42.230.131> lcd D:\
Local directory is now D:\
sftp:/授权示例资产一/101.42.230.131> get 下载示例.pdf
Fetching /授权示例资产一/101.42.230.131/下载示例.pdf to 下载示例.pdf
sftp: received 9.38 MB in 16.74 seconds
```

10.4. VScode 连接 JumpServer 纳管的资产

JumpServer 支持通过 VScode (Visual Studio Code) 的 Remote-SSH 插件直连 JumpServer 纳管的 Linux-SSH 协议的资产，进行远程开发。

JumpServer 支持 VSCode 连接纳管的资产，需要提前在配置文件 config.txt 中添加如下配置：

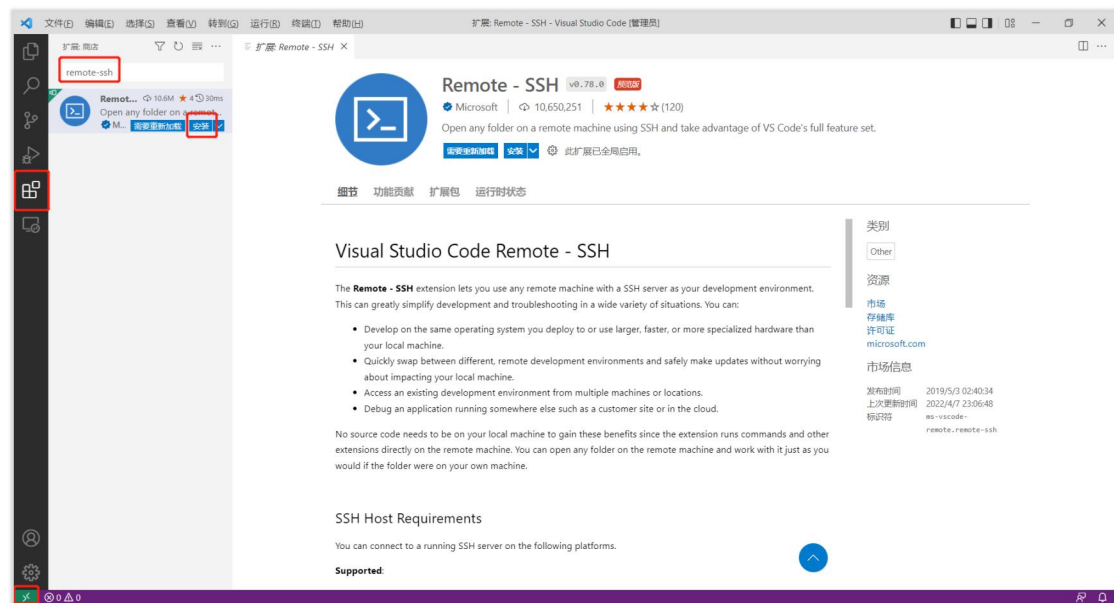
ENABLE_LOCAL_PORT_FORWARD=true

ENABLE_VSCODE_SUPPORT=true

10.4.1. VSCode 配置

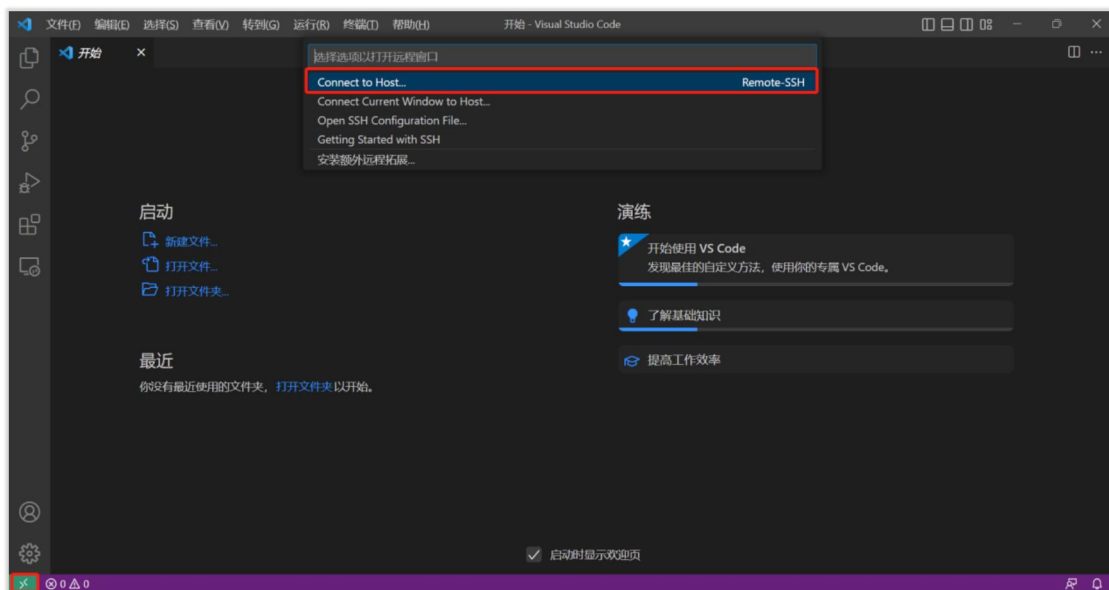
VScode 的下载地址: <https://code.visualstudio.com/download>

VSCode 连接 JumpServer 纳管的资产主要使用 Remote-SSH 插件进行连接,需要提前下载并安装 Remote-SSH 插件。在“扩展”中搜索“Remote-SSH”,得到插件进行安装。安装后左下角出现绿色小标,如下图所示。

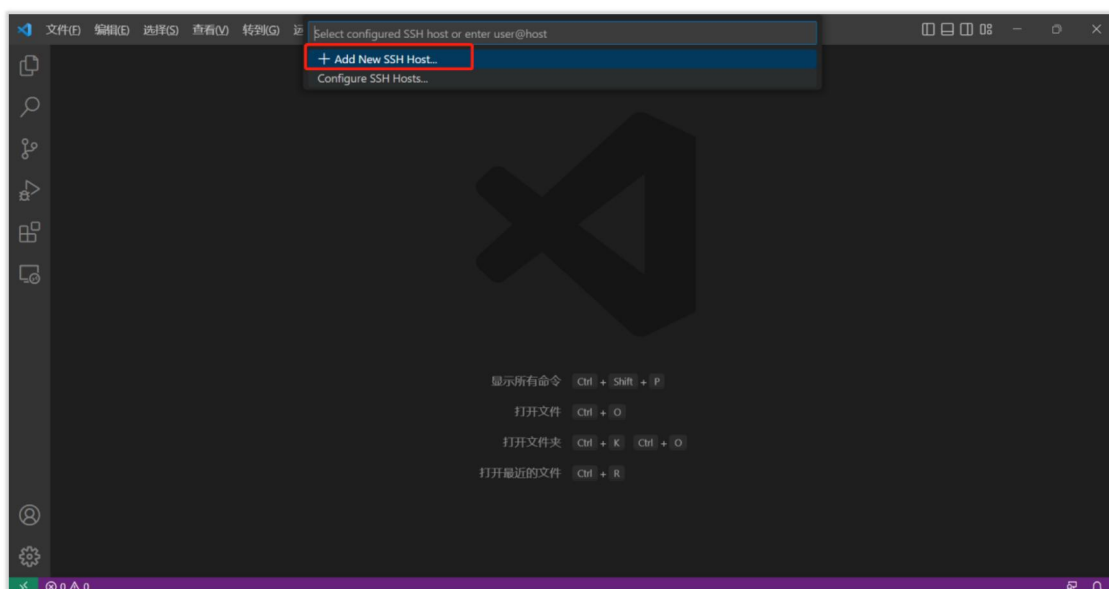


10.4.2. 连接资产

点击左下角绿色标识,中间上方选择“Connect to Host”。



下一步选择“Add New SSH Host”。



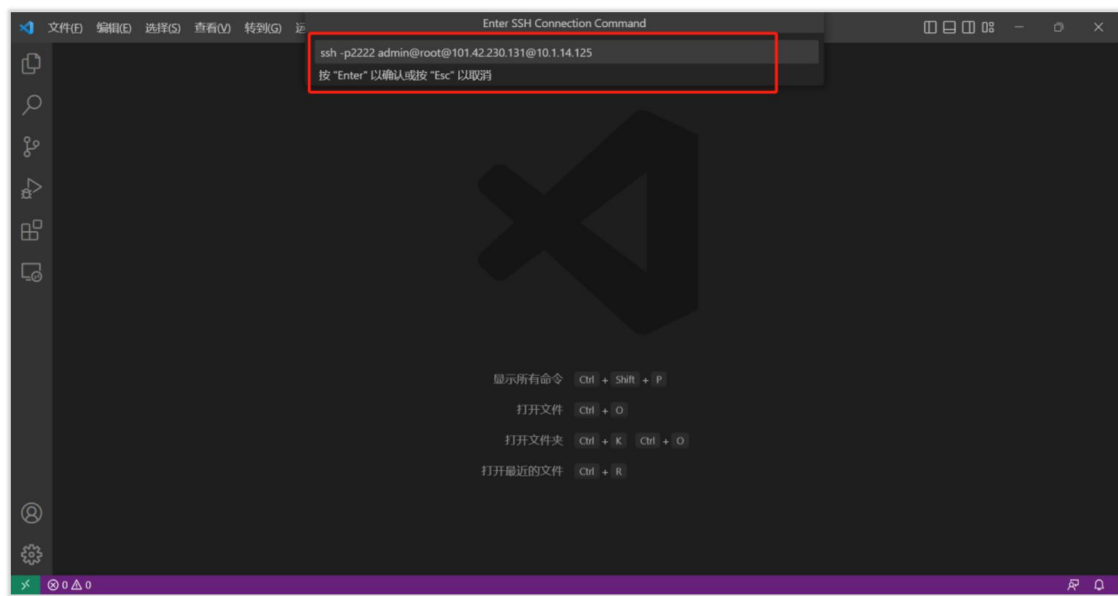
输入命令行直连 JumpServer 纳管的资产命令：

```
ssh jumpserverUsername@systemUsername@AssetIP@jumpserverHostIP -p2222
```

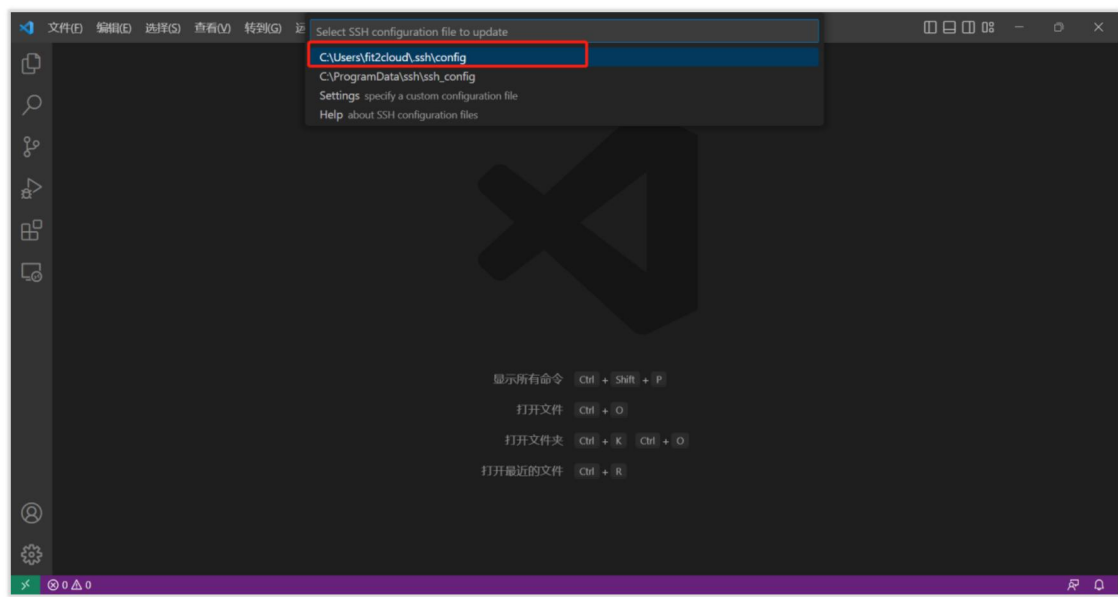
解释：

- jumpserverUsername ： 登录 JumpServer 的用户。
 - systemUsername ： 连接资产使用的账号名称。
 - AssetIP ： 被连接的资产 IP。
-
- jumpserverHostIP ： JumpServer 的访问地址，可以填写 IP 或域名。
 - 2222 ： JumpServer 提供命令行连接的端口，默认为 2222 端口。
-

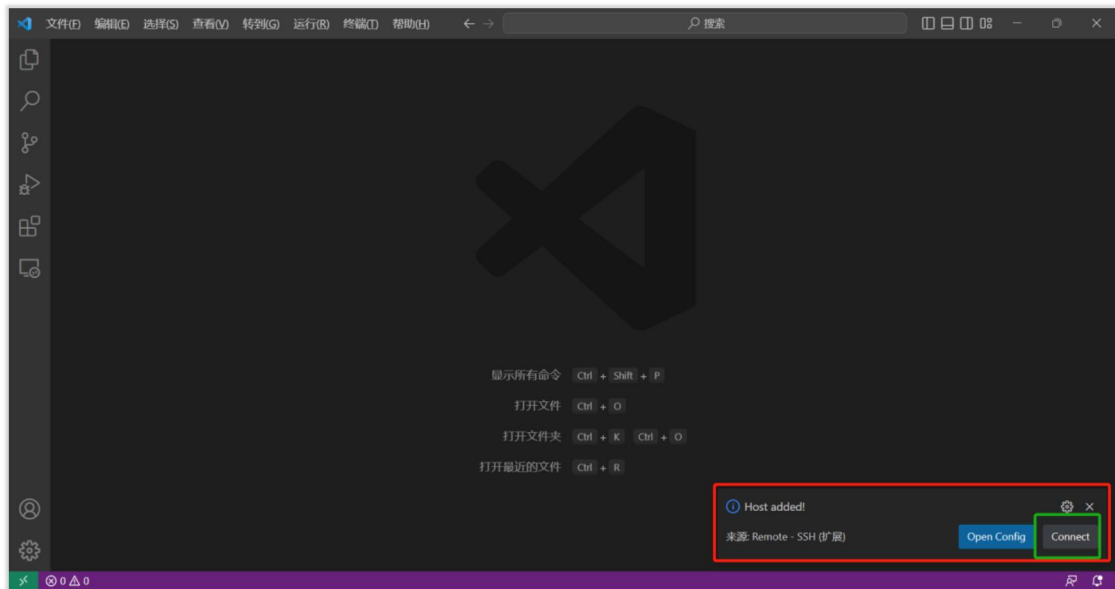
示例如下图：



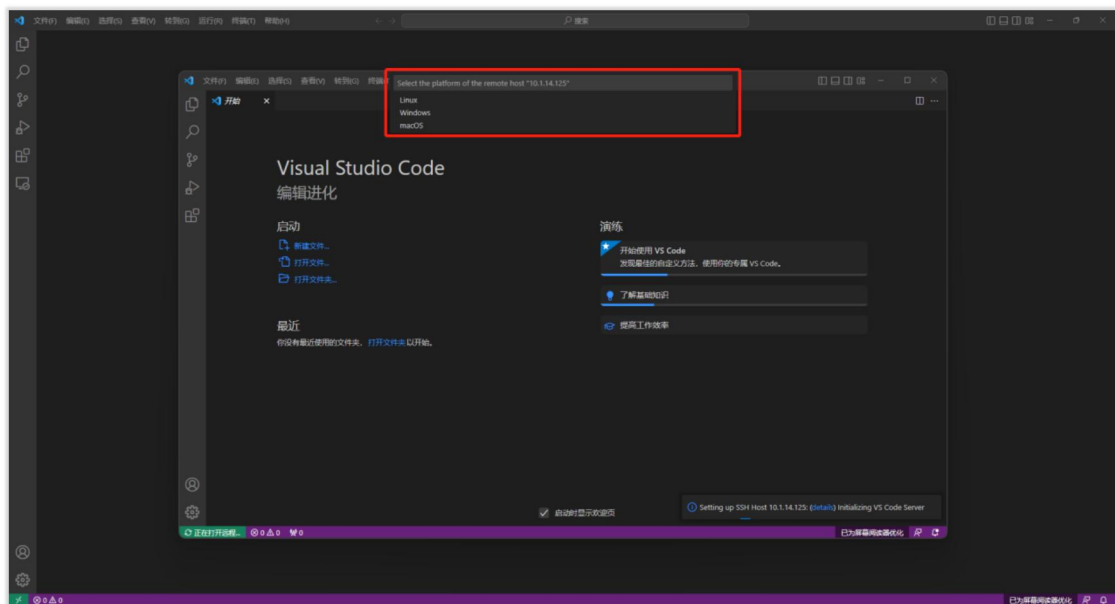
选择 SSH 配置更新存储的文件位置。如下图所示：



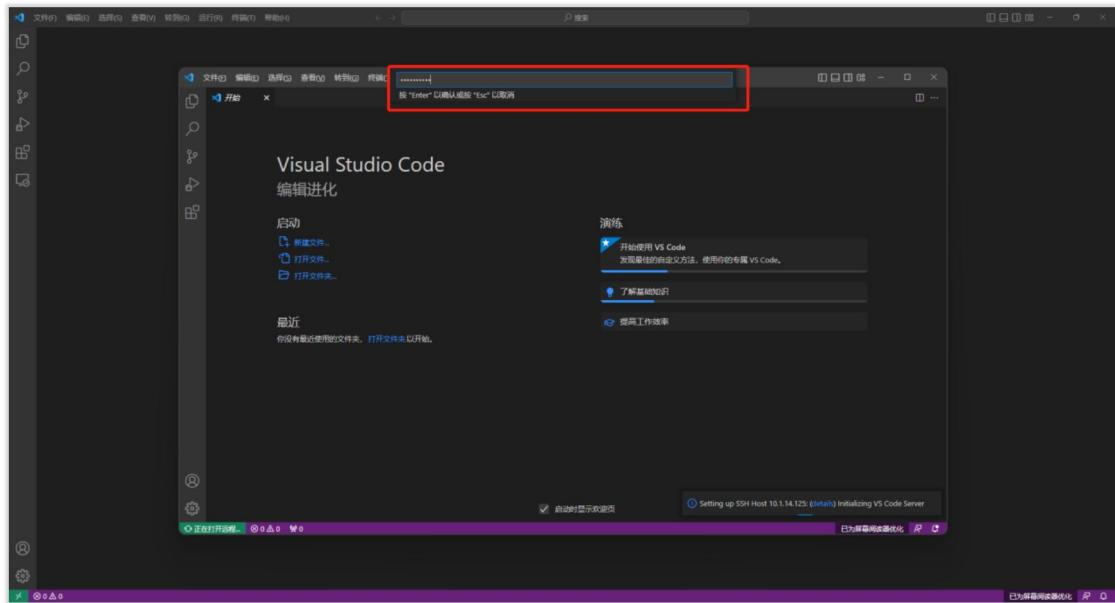
下图表示该连接信息已经存储到配置文件中，点击 [Connect](#) 按钮连接资产。



选择需要连接的资产的系统类型。



输入登录 JumpServer 的账号密码。



连接资产成功。