



Jumpserver

FIT2CLOUD 飞致云 旗下品牌

堡垒机用户使用手册（普通用户）

2020.2 修订

目 录

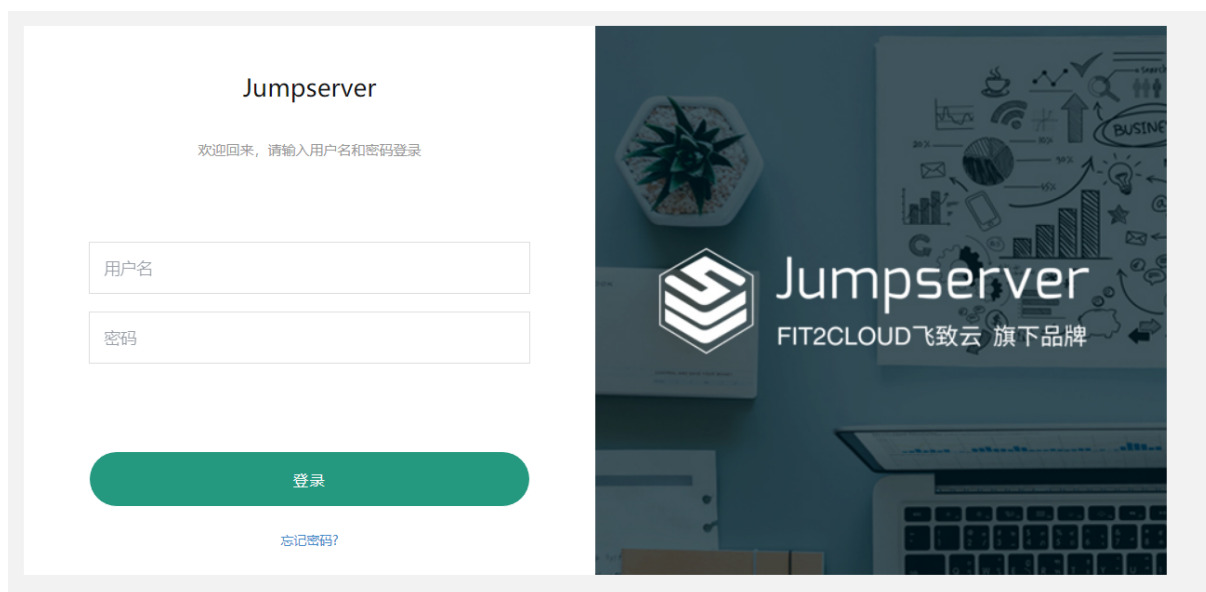
一、用户登入	4
1.1 用户登入	4
1.2 密码重置	6
1.3 绑定 MFA 认证	8
1.4 用户信息完善	11
二、我的资产	13
2.1 管理资产树	13
2.2 资产连接	14
我的应用	16
3.1 查看应用	16
3.2 访问应用	16
3.3 查看数据库	18
3.4 访问数据库	18
四、个人信息	19
4.1 个人信息显示	19
4.2 个人信息快速修改	19
4.3 密码修改	20
4.4 MFA 认证修改	21
4.6 个人信息修改	25
	2

五、 Web 终端	26
5.1 Luna 页面	26
5.2 资产树管理	27
5.3 Linux 资产连接	29
5.4 连接失败	31
5.5 Linux 资产文件管理	32
5.6 Windows 资产连接	35
5.7 Windows 资产文件管理	39
5.8 映射网络驱动	43
六、 shell 端登录	46
6.1 shell 端登录简介	46
6.2 SSH 端登录	46
七、 文件管理	49
7.1 页面传输	49

一、用户登入

1.1 用户登入

输入 jumpserver 界面地址，直接登录。



如果管理员绑定了 MFA 二次认证，需要先绑定 MFA，详见 1.3 章节。绑定 MFA 成功后，返回登入页面，输入用户名密码，来到二次认证页面，同样使用认证客户端，输入 6 位认证数字，即可登入成功

欢迎使用

全球首款完全开源的堡垒机，使用GNU GPL v2.0开源协议，是符合 4A 的专业运维审计系统。

使用Python / Django 进行开发，遵循 Web 2.0 规范，配备了业界领先的 Web Terminal 解决方案，交互界面美观、用户体验好。

采纳分布式架构，支持多机房跨区域部署，中心节点提供 API，各机房部署登录节点，可横向扩展、无并发访问限制。

改变世界，从一点点开始。

MFA认证

账号保护已开启，请根据提示完成以下操作



请打开手机Google Authenticator应用，输入6位动态码

下一步

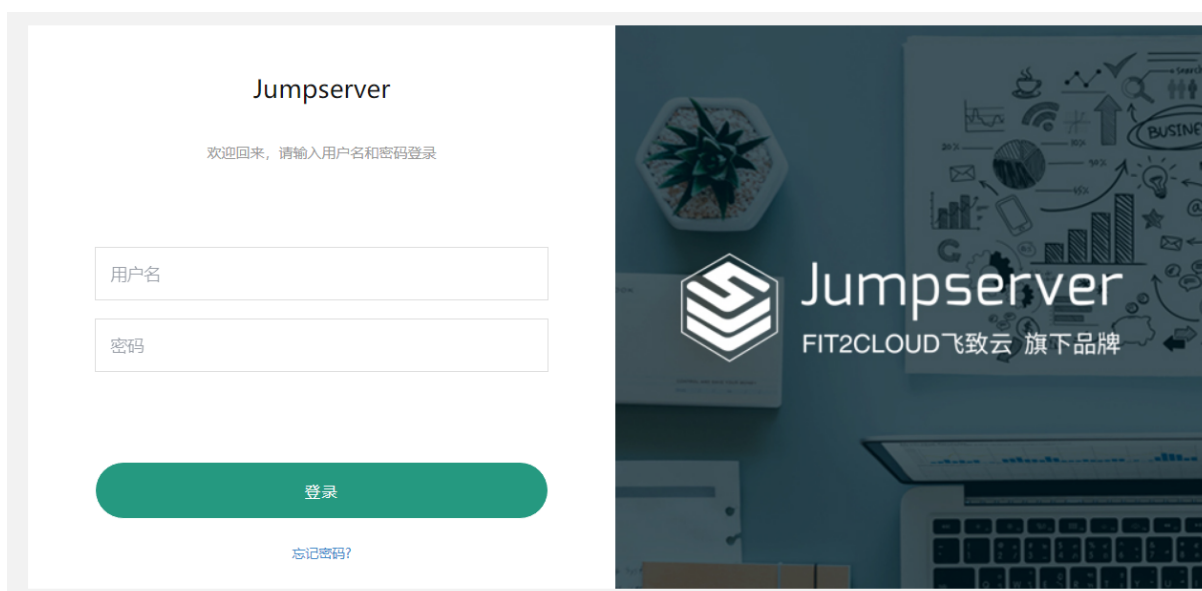
如果不能提供MFA验证码，请联系管理员!

淘
转

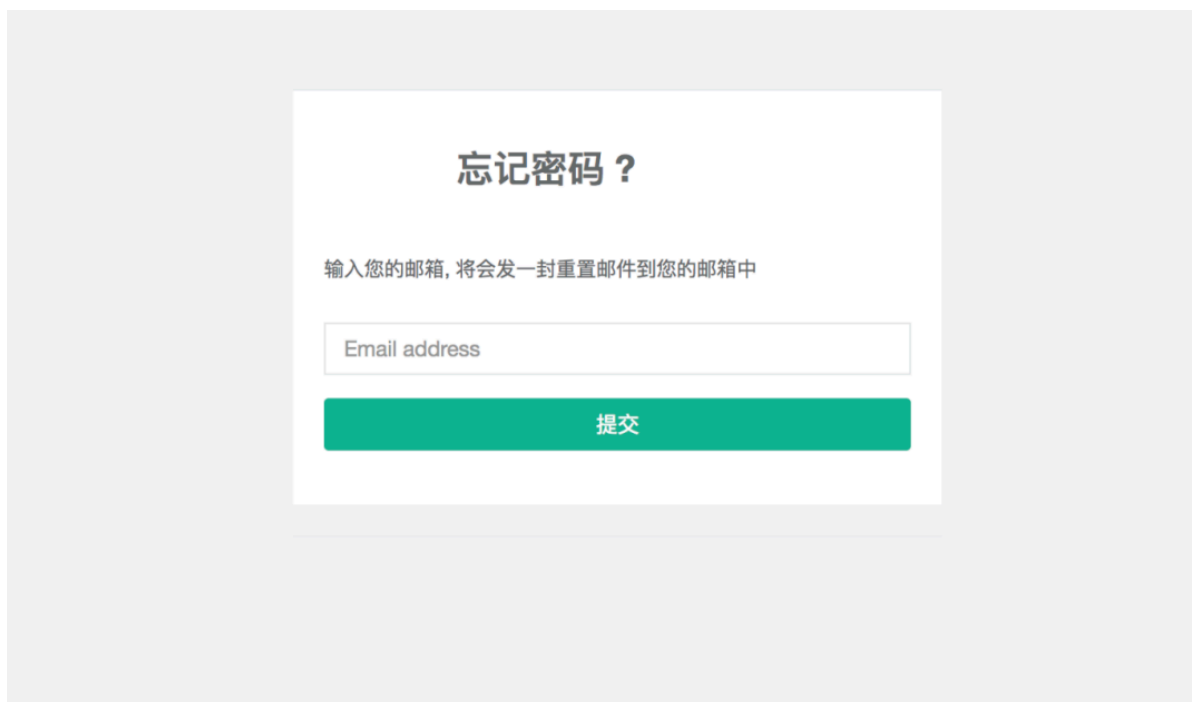
1.2 密码重置

1. 重置密码：输入堡垒机地址：<https://jms.crc.com.cn> 进入登入页面，若未初始化密码，请点击忘记密码，跳转至密码重置页面。

注：（堡垒机不支持 IE 浏览器，推荐使用 Chrome ，也可使用火狐浏览器）



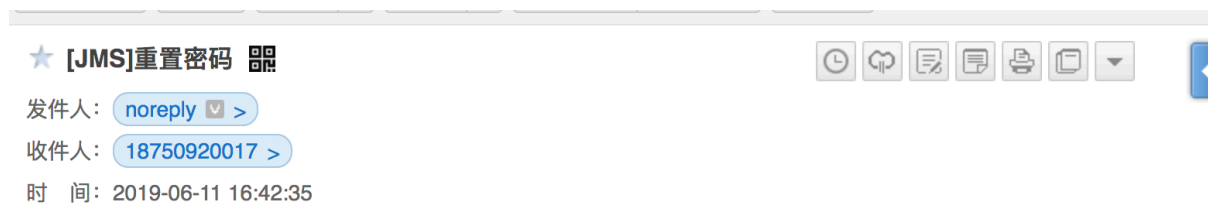
2. 发送密码重置邮件：输入该用户的邮箱信息，发送密码重置邮件。



说明：

由于用户初始化数据是参考旧版本堡垒机的用户信息，若提示邮箱错误，可能是原来堡垒机用户的用户信息中无邮箱，或邮箱和其他账号的邮箱重复，请联系管理员重置密码。

3. 密码重置：按邮件指示完成密码重置



4. 重新登入：重置成功后，进入登入页面，输入账号密码进行登入

1.3 绑定 MFA 认证

1. 二次密码验证：若管理员设置了 MFA 二次认证，首次登入时需要绑定 MFA 进行二次认证，登入页面输入用户名密码，跳转至身份验证页面，再次输入密码验证，点击下一步。

验证身份

安全令牌验证 账户 **test** 请按照以下步骤完成绑定操作

下一步

2. 认证客户端安装：扫码下载认证客户端，或搜索 MinaOTP 微信小程序，认证客户端安装完成后点击下一步

安装应用

安全令牌验证 账户 **test** 请按照以下步骤完成绑定操作

请在手机端下载并安装 Google Authenticator 应用



Android手机下载



iPhone手机下载

安装完成后点击下一步进入绑定页面（如已安装，直接进入下一步）

下一步

2020-11-11 14:41

3. 绑定 MFA：使用认证客户端扫二维码，或者手动输入 key，将账号绑定 MFA，扫码完成后输入显示的 6 位认证数字即可绑定成功

绑定 MFA

安全令牌验证 账户 test2 请按照以下步骤完成绑定操作

使用手机 Google Authenticator 应用扫描以下二维码，获取6位验证码



Secret: K33OMNPVZJZ4OP77

6位数字

下一步

激活 W
转到“设置”

说明：

若已绑定 MFA，需要再绑定一个认证客户端或者需要更换手机，可以登录后，在个人信息页面点击更改 MFA，重新登录后保留绑定二维码，使用多个客户端扫码绑定，即可绑定多个认证客户端。

1.4 用户信息完善

1. 基础信息完善：登入成功后，提示完善个人信息，微信和手机信息为选填项。

你的信息不完整, 请点击 [链接](#) 补充完整

首次登录

1. 个人信息 2. ssh公钥 3. MFA 4. 完成

Username *
jianxing

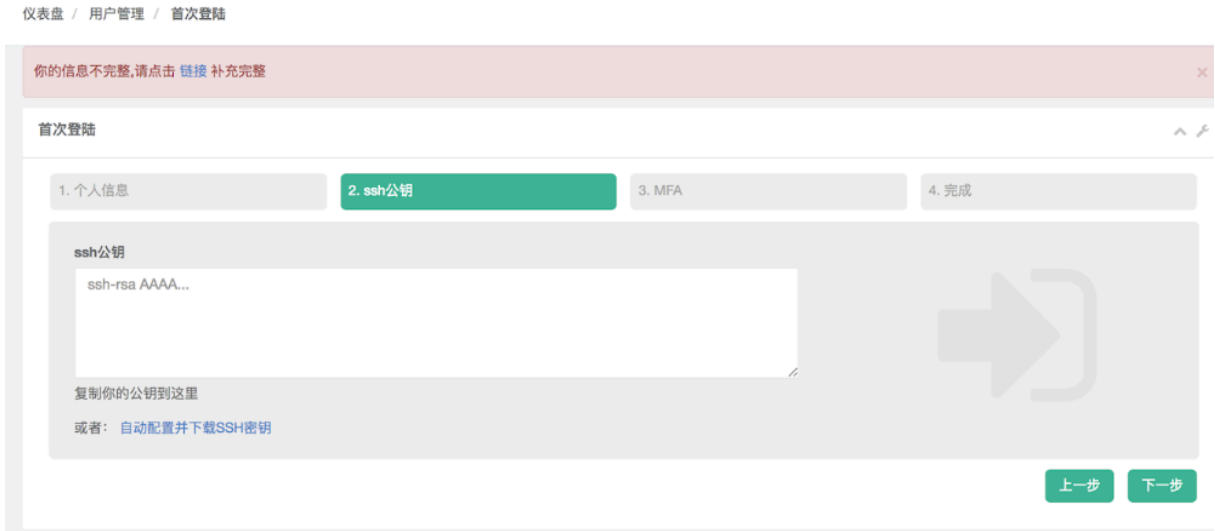
Name *
jianxing

Email *
jianxing.chen@fit2cloud.com

微信
手机

激活 Windows 下一步

2. ssh 公钥修改：ssh 公钥项为 shell 端登入堡垒机时使用的公钥，若需使用 shell 端免密登入 Linux 资产可选填，或者由系统自动帮您生成，然后再下载即可，shell 端登入请参考第六章。



3. MFA 设置：用户可以设定是否启用 MFA 功能，前提是管理员已经启用了该用户的 MFA 功能，若管理员配置为强制启用，则默认只允许设置启用状态。



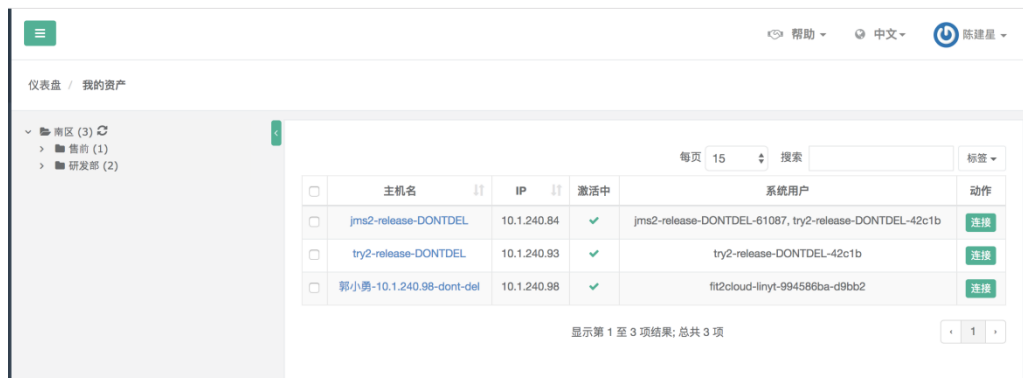
说明：

其中 MFA 认证选项为用户级别的可选设置，若系统管理员已启用全局 MFA 配置，登入时必须进行二次认证，当管理员关闭全局配置时，用户级别设置生效。

二、我的资产

2.1 管理资产树

1. 资产列表：点击“我的资产”，可以查看被划分到各资产树节点的资产信息，包括主机名、IP、状态、系统用户等信息。



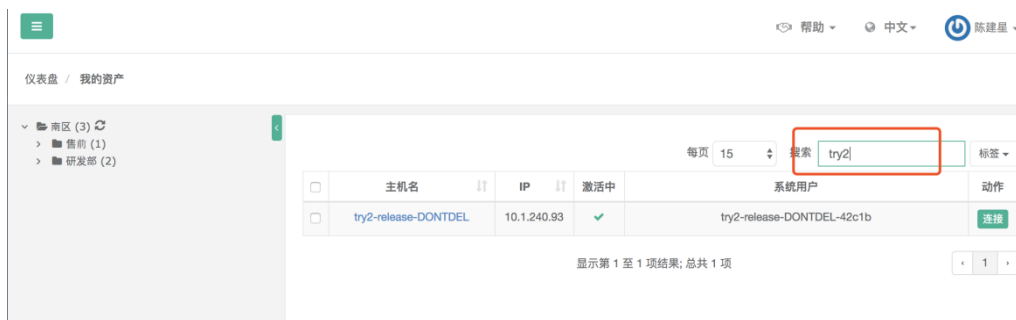
The screenshot shows a web interface for managing assets. On the left is a navigation tree with categories like '南区 (3)', '售前 (1)', and '研发部 (2)'. The main area displays a table of assets. The table has columns for '主机名' (Hostname), 'IP', '激活中' (Activated), '系统用户' (System User), and '动作' (Action). Three assets are listed, each with a '连接' (Connect) button. The table also includes a search bar, a '每页' (Items per page) dropdown set to 15, and a '显示第 1 至 3 项结果: 总共 3 项' (Showing results 1 to 3 of 3 total) footer.

主机名	IP	激活中	系统用户	动作
jms2-release-DONTDEL	10.1.240.84	✓	jms2-release-DONTDEL-61087, try2-release-DONTDEL-42c1b	连接
try2-release-DONTDEL	10.1.240.93	✓	try2-release-DONTDEL-42c1b	连接
郭小勇-10.1.240.98-dont-del	10.1.240.98	✓	fit2cloud-linyt-994586ba-d9bb2	连接

2. 显示资产详情：点击各资产的主机名，会显示该资产的详细信息。

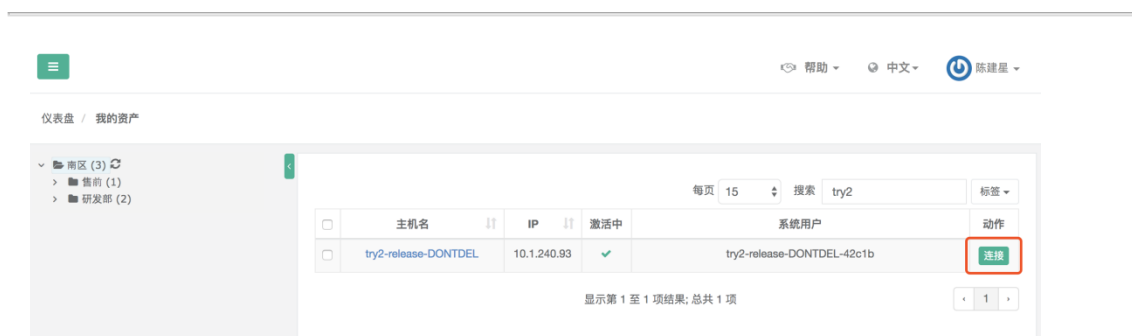


3. 搜索资产：在搜索栏输入主机名或 IP 地址，可查询相关资产列表。

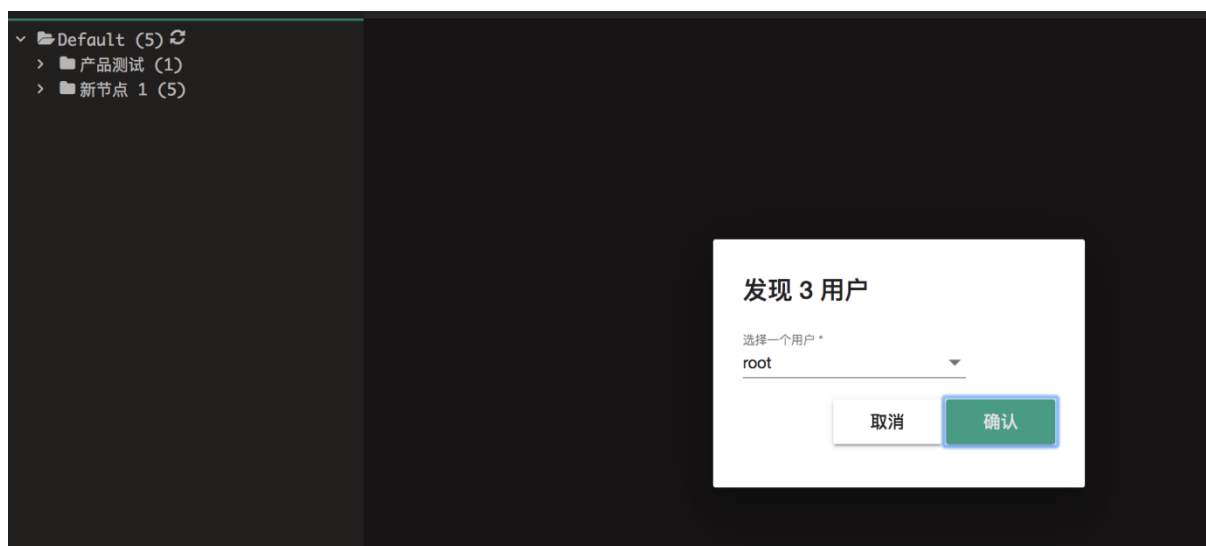


2.2 资产连接

1. 资产连接：选择资产，点开连接，跳转至 Luna 资产登入页面。



2. 资产登入：选择登入的用户，输入用户名密码进行登入。

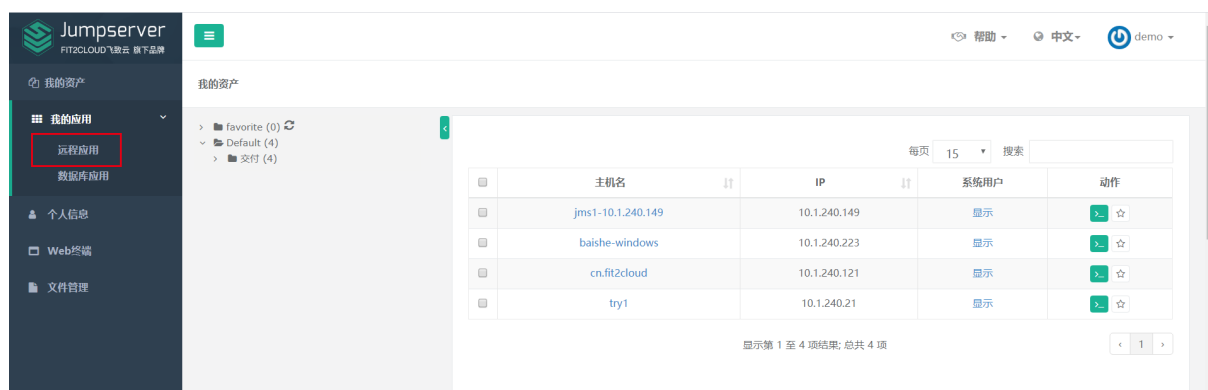


说明：登入账号为管理员设置的系统用户，若该系统用户为自动登入，则不需要填写密码，当只有自动登入的系统用户时，会选择管理员设置的优先级最高的用户自动登入，若登入用户为手动，则需要输入用户密码。

三、我的应用

3.1 查看应用

应用列表：点击“我的应用” -> “远程应用”，可以查看拥有权限的远程应用。



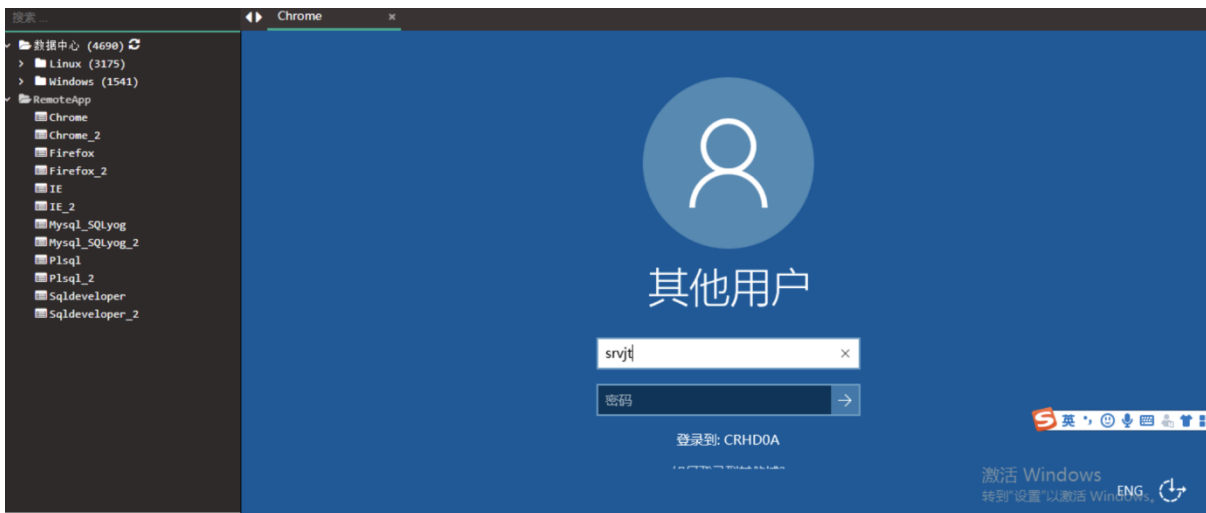
3.2 访问应用

1. 连接应用：选择需要访问的应用，点击“连接”。



名称	应用类型	资产	系统用户	备注	动作
Chrome	Chrome	10.0.14.183	appadmin		连接
Chrome_2	Chrome	10.0.14.184	appadmin		连接
Firefox	自定义	10.0.14.183	appadmin		连接
Firefox_2	自定义	10.0.14.184	appadmin		连接
IE	自定义	10.0.14.183	appadmin		连接
IE_2	自定义	10.0.14.184	appadmin		连接
Mysql_SQLyog	自定义	10.0.14.183	appadmin		连接
Mysql_SQLyog_2	自定义	10.0.14.184	appadmin		连接
Pisql	自定义	10.0.14.183	appadmin	激活 Windows	连接

2. 登入应用：输入域账号用户名密码即可访问该远程应用。



说明：

由于目前多个应用部署在同一台应用服务器上，经过验证用户首次访问应用时，需要初始化用户信息，首次连接会阻塞会话，如果访问多个应用，后续开启的应用会等待首次登入的会话过期，方可访问；如果该用户账号首次登入，并需要访问多个应用，请先关闭首次登入的应用，并等待一分钟会话过期之后，可访问多个应用。

3.3 查看数据库

应用列表：点击“我的应用” -> “数据库应用”，可以查看拥有权限的数据库应用。



3.4 访问数据库

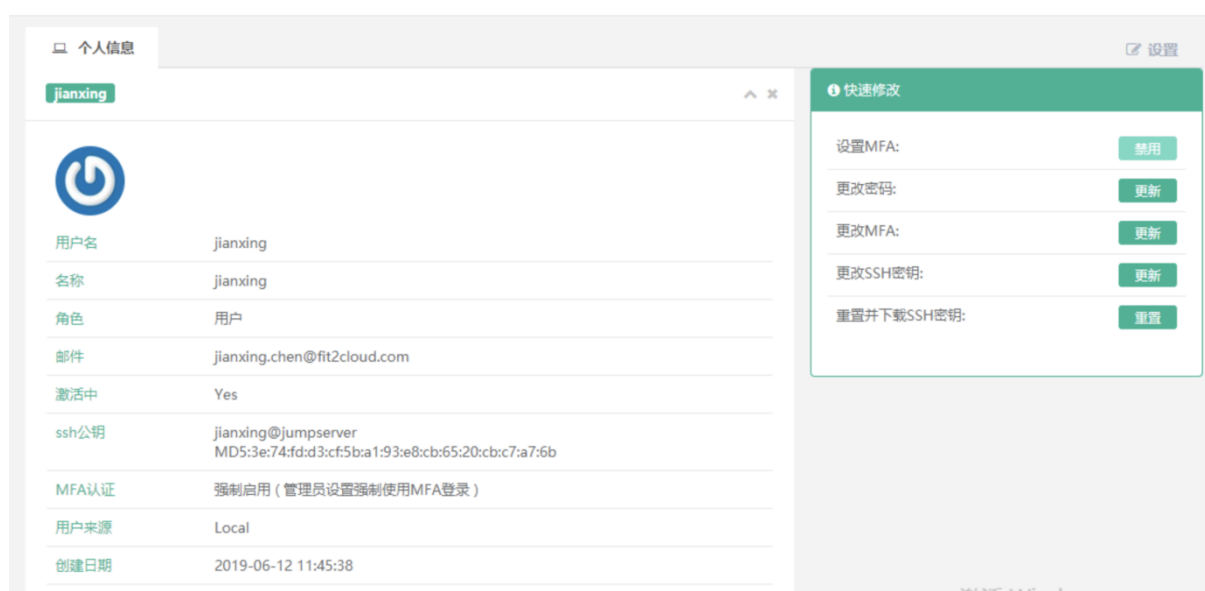
连接数据库应用：选择需要访问的数据库，点击“连接”。



四、个人信息

4.1 个人信息显示

个人信息显示：点击个人信息菜单，页面显示用户名、角色、邮箱、ssh 公钥、MFA 认证等个人信息。



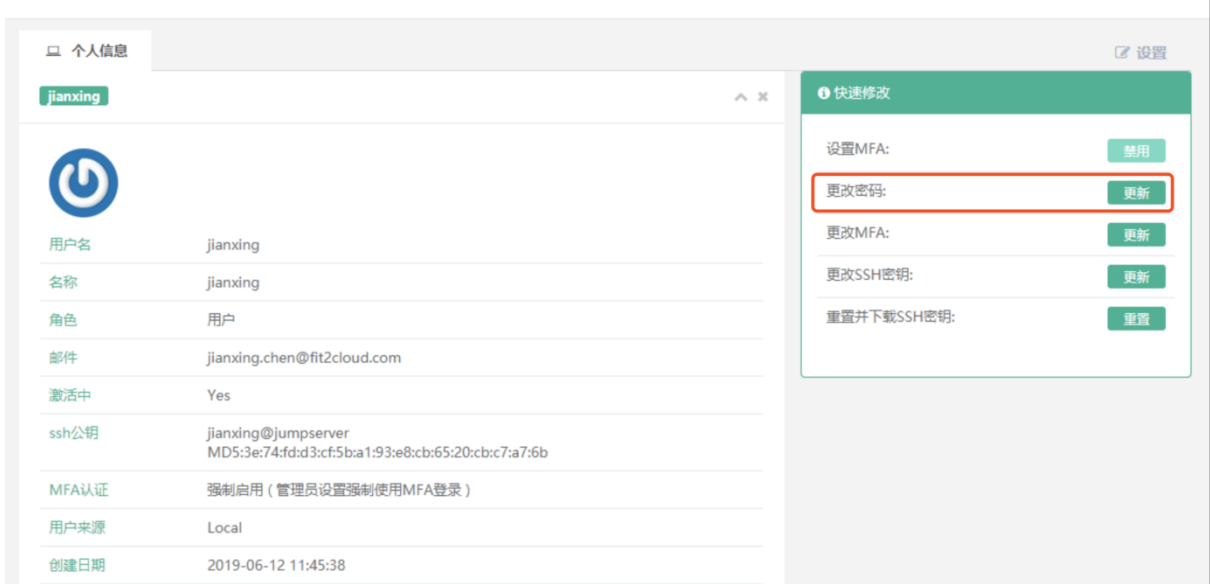
4.2 个人信息快速修改

快速修改：点击个人信息菜单，页面右方提供更改密码、更改 MFA 设置、更改 ssh 密钥、重置并下载 ssh 密钥等设置。

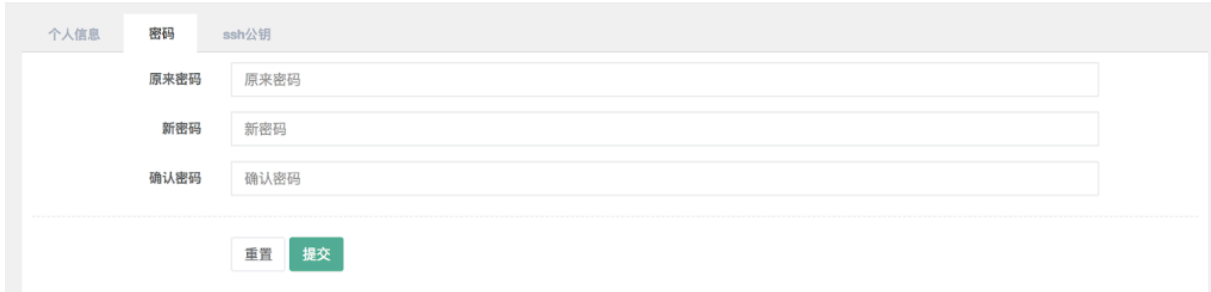


4.3 密码修改

密码修改：点击“更改密码”，依次输入原密码和新密码，完成用户密码的修改。



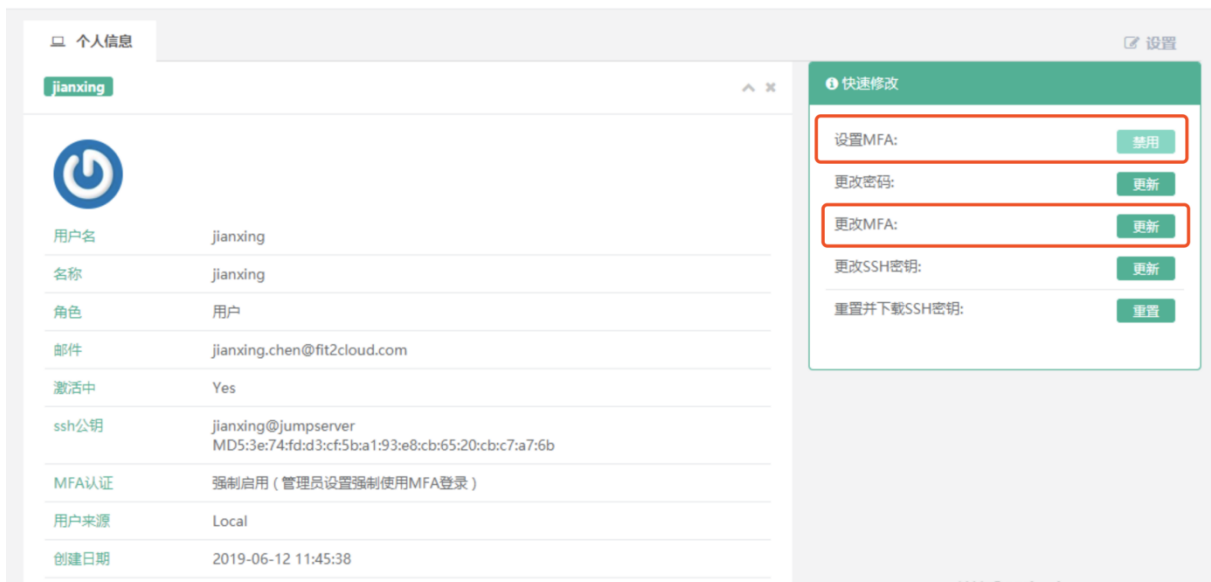
仪表盘 / 用户管理 / 密码更新



原来密码	<input type="text" value="原来密码"/>
新密码	<input type="text" value="新密码"/>
确认密码	<input type="text" value="确认密码"/>

4.4 MFA 认证修改

1. MFA 认证修改：点击“设置 MFA”，可以修改 MFA 认证禁用或启用状态，若管理员配置为强制启用，则默认只允许为启用状态。点击“修改 MFA”可修改 MFA 认证。



用户名	jianxing
名称	jianxing
角色	用户
邮件	jianxing.chen@fit2cloud.com
激活中	Yes
ssh公钥	jianxing@jumpserver MD5:3e:74:fd:d3:cf:5b:a1:93:e8:cb:65:20:cb:c7:a7:6b
MFA认证	强制启用 (管理员设置强制使用MFA登录)
用户来源	Local
创建日期	2019-06-12 11:45:38

快速修改

- 设置MFA:
- 更改密码:
- 更改MFA:
- 更改SSH密钥:
- 重置并下载SSH密钥:

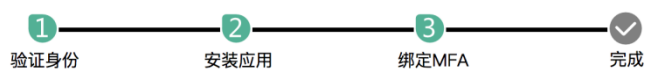
2. 密码认证：输入密码进行验证身份。



3. 安装认证客户端：然后安装 Google Authenticator 应用或使用 MinaOTP 微信小程序，其他支持标准 OTP 协议的软件同样支持。



4. 绑定 MFA 认证客户端：扫码二维码获取 6 位验证码，绑定 MFA，完成 MFA 认证。



安全令牌验证 账户 zho 请按照以下步骤完成绑定操作

使用手机 Google Authenticator 应用扫描以下二维码，获取6位验证码



6位数字

下一步

说明：

其中 MFA 认证选项为用户级别的可选设置，若系统管理员已启用全局 MFA 配置，登入时必须进行二次认证，当管理员关闭全局配置时，用户级别设置生效。

4.5 ssh 密钥修改

说明：

ssh 公钥项为 shell 端登入堡垒机时使用的公钥，若需使用 shell 端免密登入 Linux 资产可选填，或者由系统自动帮您生成，然后再下载即可，shell 端登入请参照：1.6。

1. 重置密钥：可以点击“重置”，重置并下载密钥到本地。



2. 更改密钥：点击“更改 ssh 密钥”，可以点击“重置”，重置并下载密钥到本地，也可以通过复制公钥的方式，完成 ssh 密钥更改。



4.6 个人信息修改

个人信息修改：点击“设置”，可以对用户名、邮箱等账户信息以及手机、微信等个人信息进行修改。

仪表盘 / 个人信息

个人信息

zho

快速修改

更改密码:	更新
更改MFA设置:	启用
更改SSH密钥:	更新
重置并下载SSH密钥:	重置

用户名	zho
名称	zho
角色	用户
邮件	hong@fit2cloud.com
激活中	Yes
ssh公钥	
MFA认证	禁用
用户来源	Local
创建日期	2018-08-15 17:45:53

仪表盘 / 用户 / 个人信息设置

个人信息 密码 ssh公钥

账户

Username * admin

Name * 管理员

Email * admin@fit2cloud.com

个人信息

手机

微信

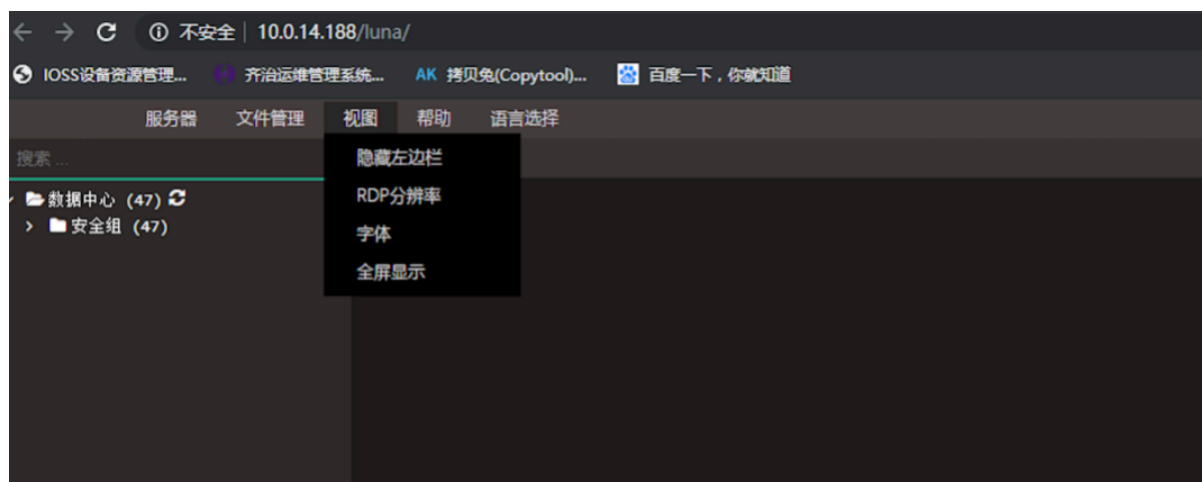
五、Web 终端

5.1 WEB 登录页面

1. Luna 资产登入页面：点击 Web 终端，跳转至 Luna 资产登入页面。

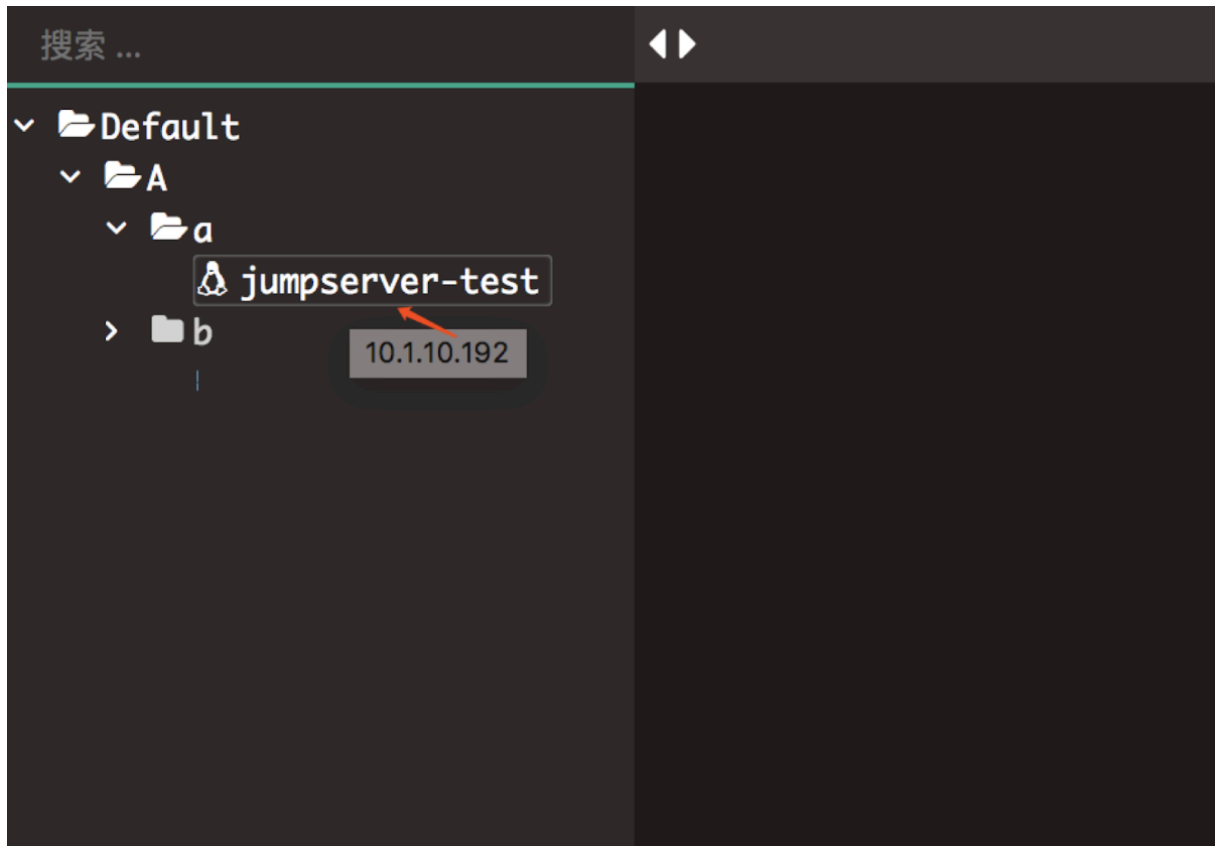


2. 视图修改：点击视图选项，可更改分辨率，显示全屏的功能，修改分辨率后，已连连接的资产需要断开连接才会生效。

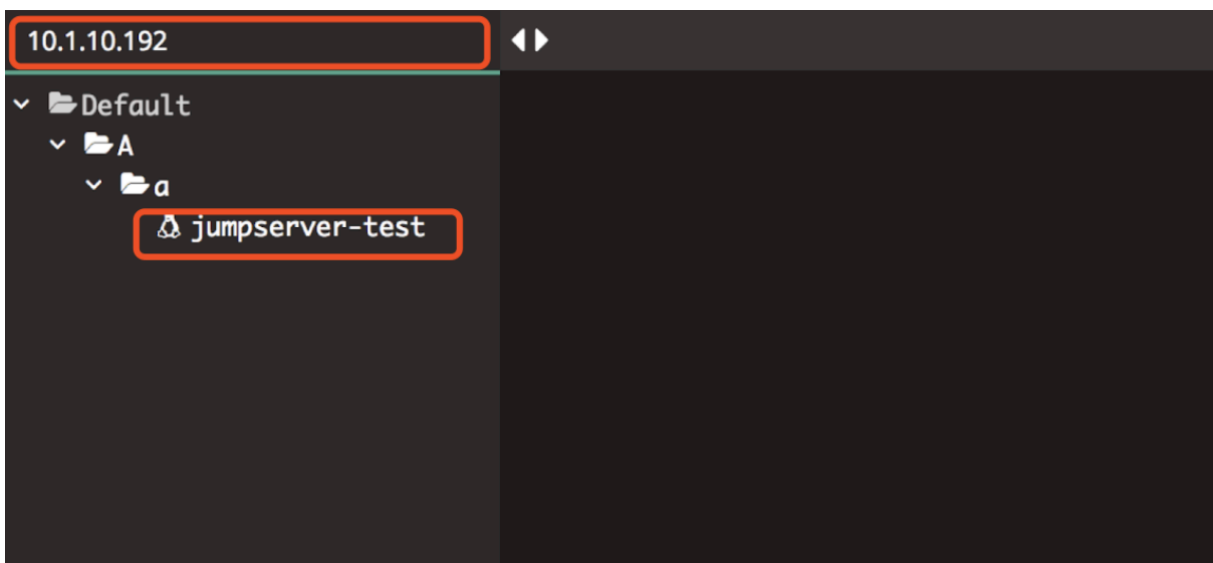
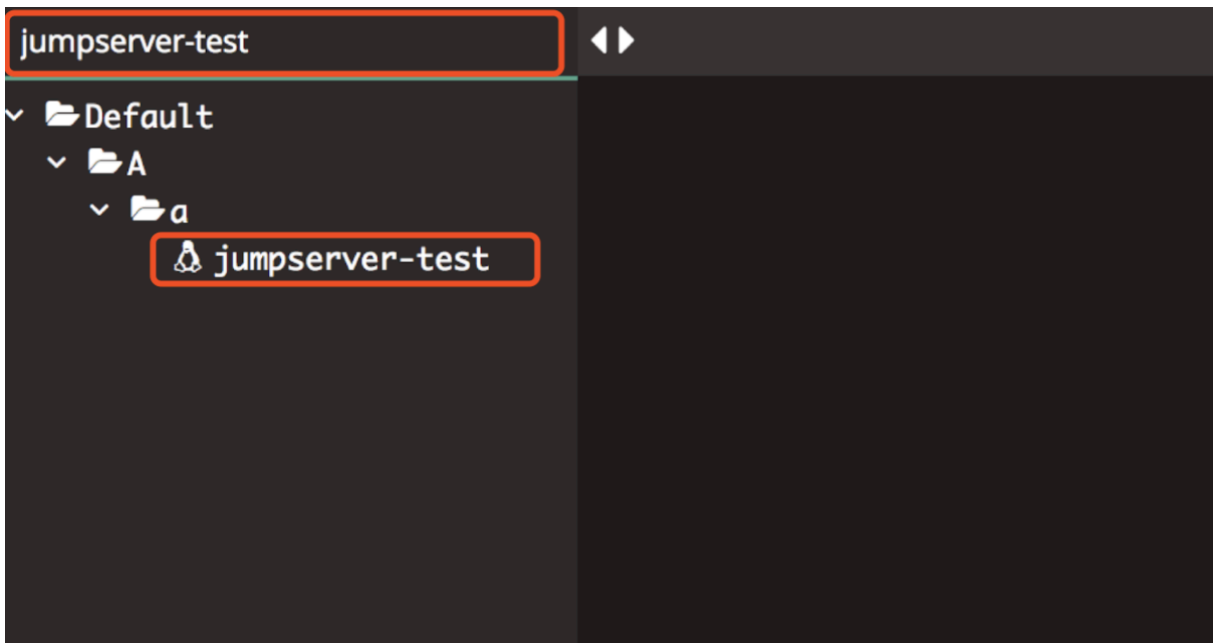


5.2 资产树管理

1. 资产显示：鼠标悬停到某个资产可以显示主机 ip。

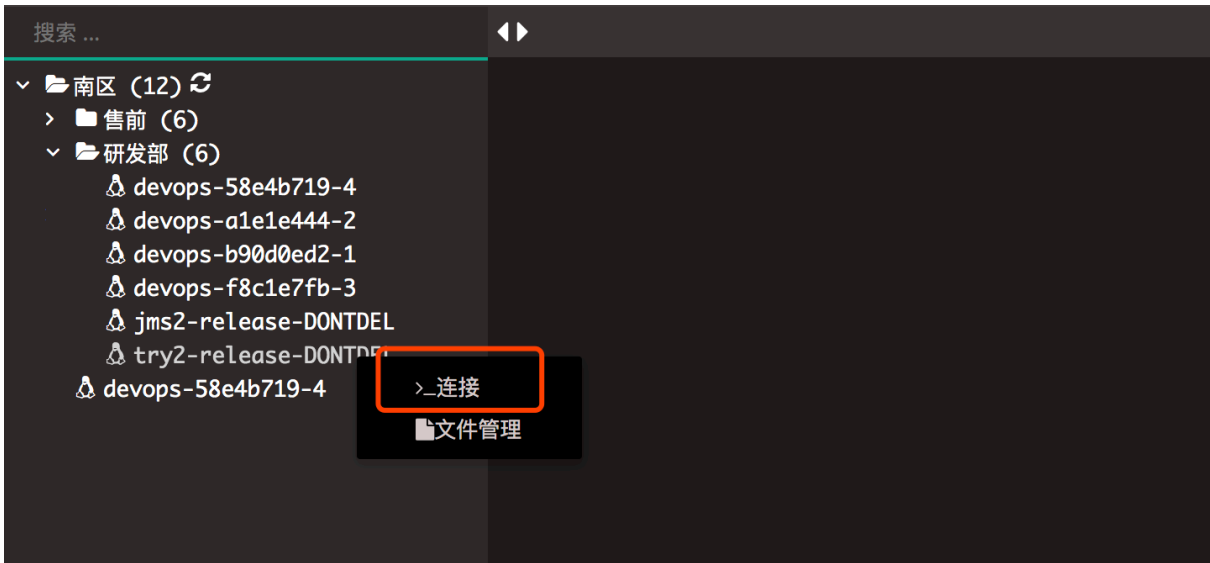


2. 搜索资产：支持根据主机名搜索资产，也支持根据主机 ip 搜索资产。

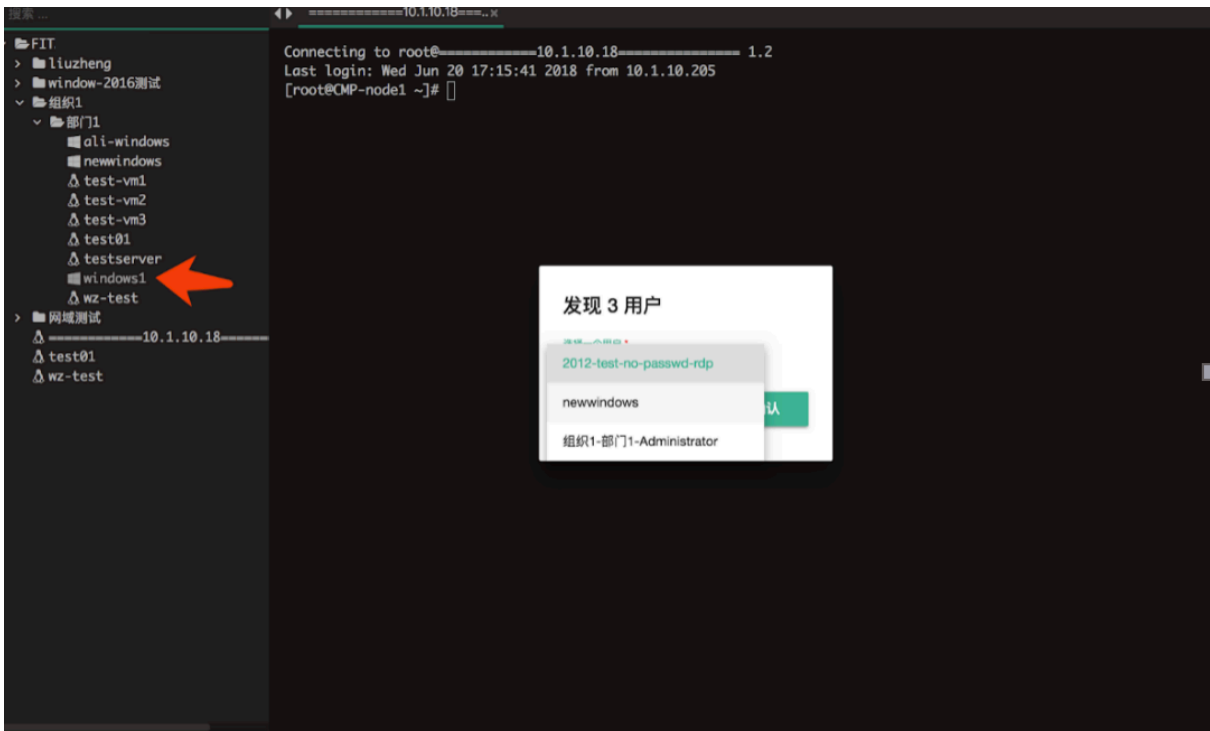


5.3 Linux 资产连接

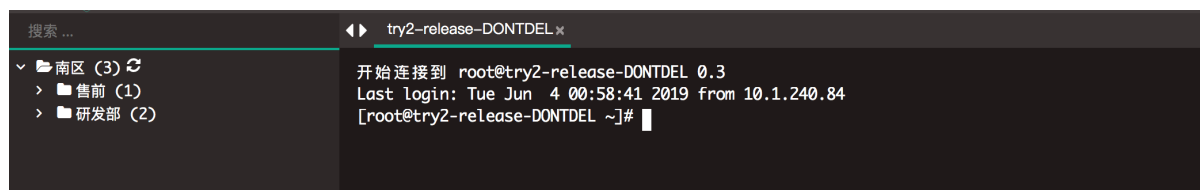
1. 连接资产：选择需要登入的资产，鼠标右键，选择连接，或直接鼠标左键点击资产。



2. 选择系统用户：当选择的资产授权了多个系统用户时，则需要手动选择系统用户，会弹出如下弹框：



3. 输入密码：输入密码后，登入成功，若该系统用户为管理员设置的自动登入用户，则不需要输入密码：



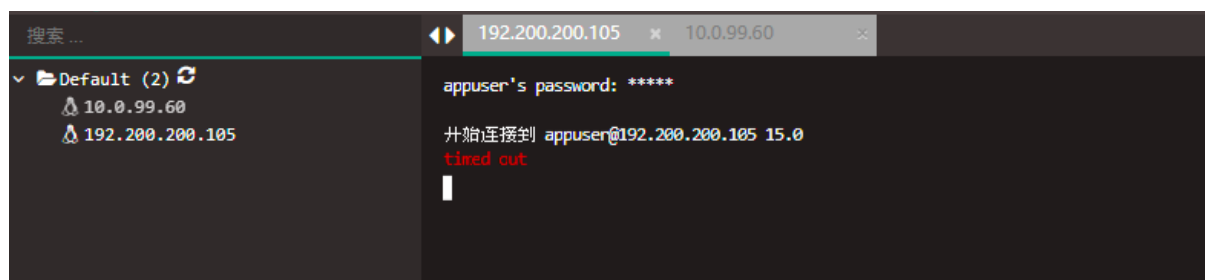
```
try2-release-DONTDEL x
开始连接到 root@try2-release-DONTDEL 0.3
Last login: Tue Jun  4 00:58:41 2019 from 10.1.240.84
[root@try2-release-DONTDEL ~]#
```

说明：

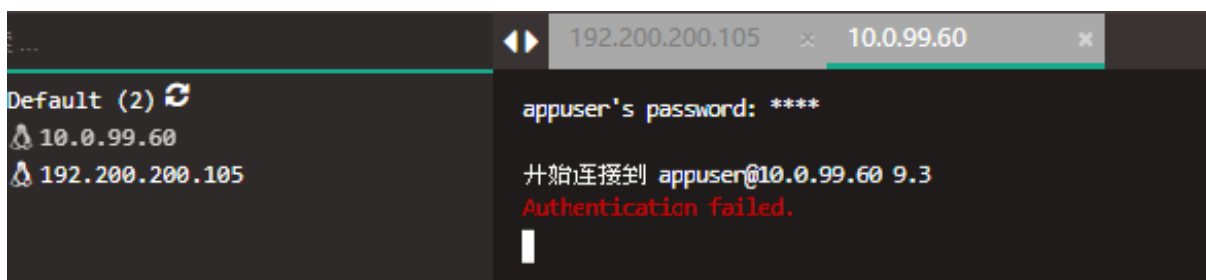
目前管理员预置的系统用户均为手动登入用户，若系统用户为自动登入则会选择优先级最高的系统用户自动登入，若优先级相同，则需要用户选择系统用户进行登入。

5.4 Linux 连接失败

连接失败：若连接失败，返回相应提示，例如，提示“time out”，则说明资产不存在或网络不通，提示“Authentication failed”，则密码输入错误，若页面无反应，可能为网络问题，或会话失效，刷新页面重试，重试后无反应请确认资产的网络环境等信息。

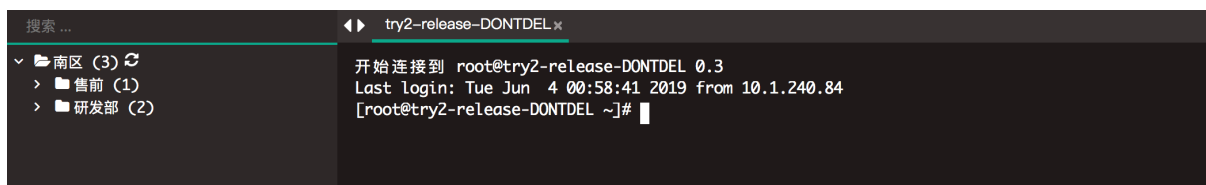
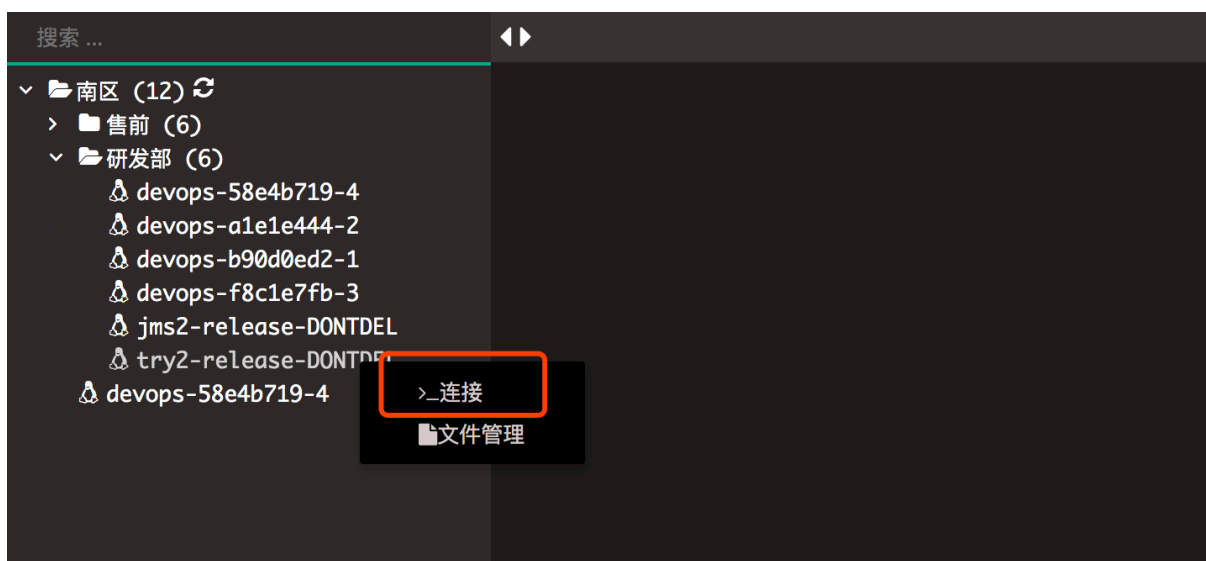


```
192.200.200.105 x 10.0.99.60
appuser's password: *****
开始连接到 appuser@192.200.200.105 15.0
timed out
```

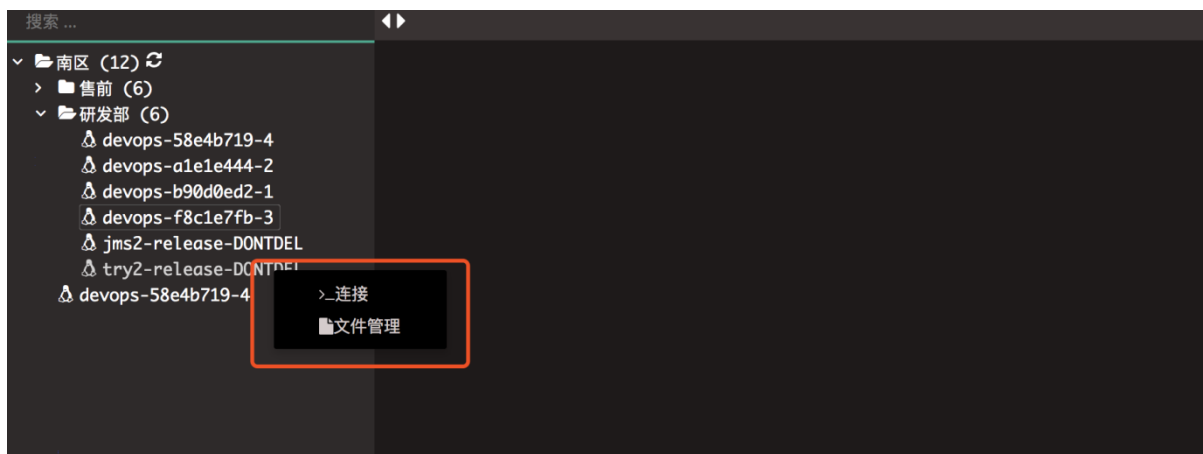


5.5 Linux 资产文件管理

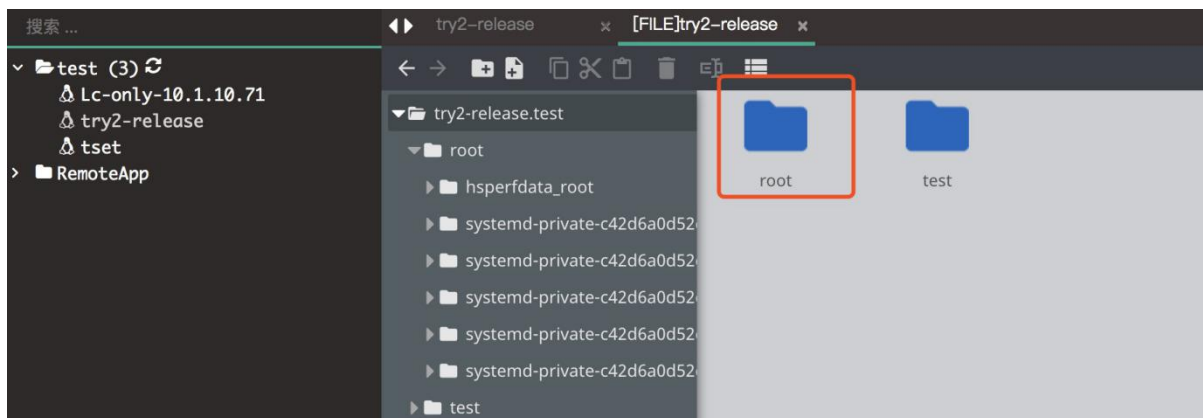
1. 连接资产：按照 1.5.2 中的步骤登入资产。



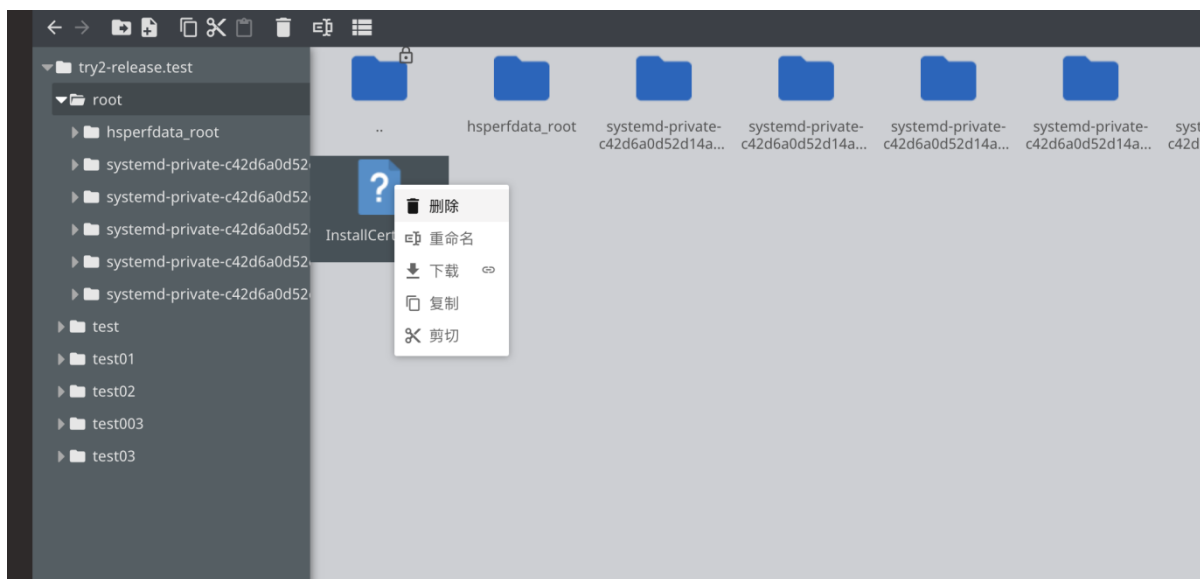
2. 登入文件管理：登入成功后，在左侧资产树中选择已连接的资产，鼠标右击，选择文件管理，进入文件管理页面。



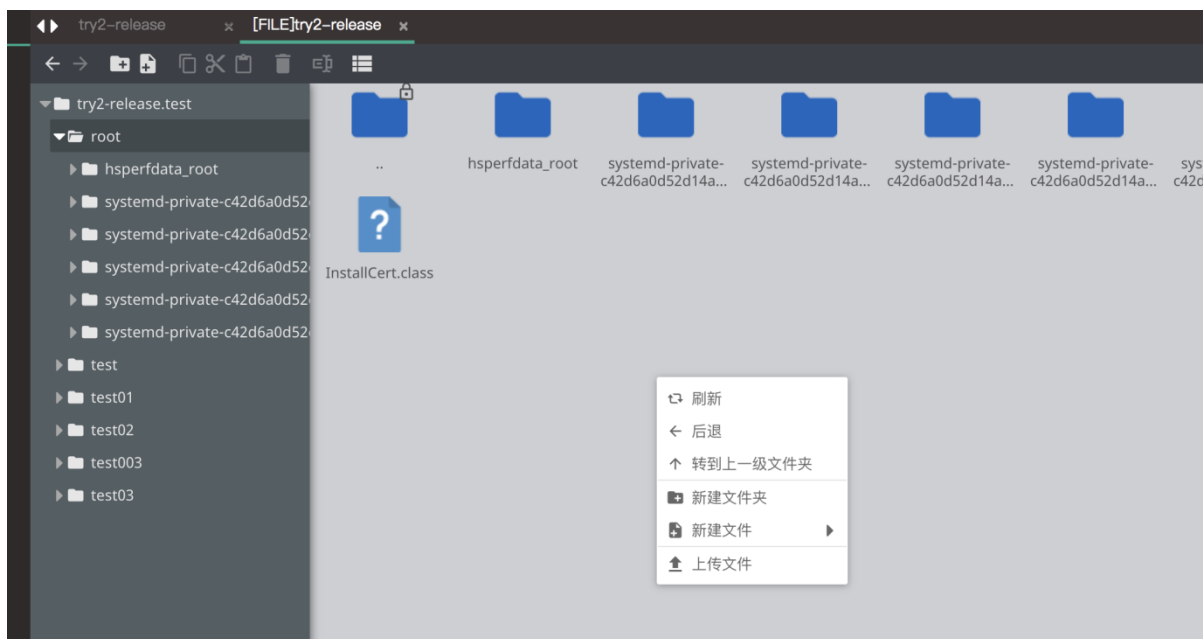
3. 访问资产/tmp 目录：选择已登入用户的相应目录（例如使用 root 用户登入，则选择 root 文件夹），即可使用该系统用户访问到目标资产的/tmp 目录。



4. 文件下载：需先将文件拷贝到/tmp 目录下，方可下载。选择需要操作的文件右键点击，即可完成文件下载等操作，双击文件也可实现下载功能。



5. 文件上传：鼠标右击页面空白处，点击上传文件，或将文件拖入页面，完成文件上传功能

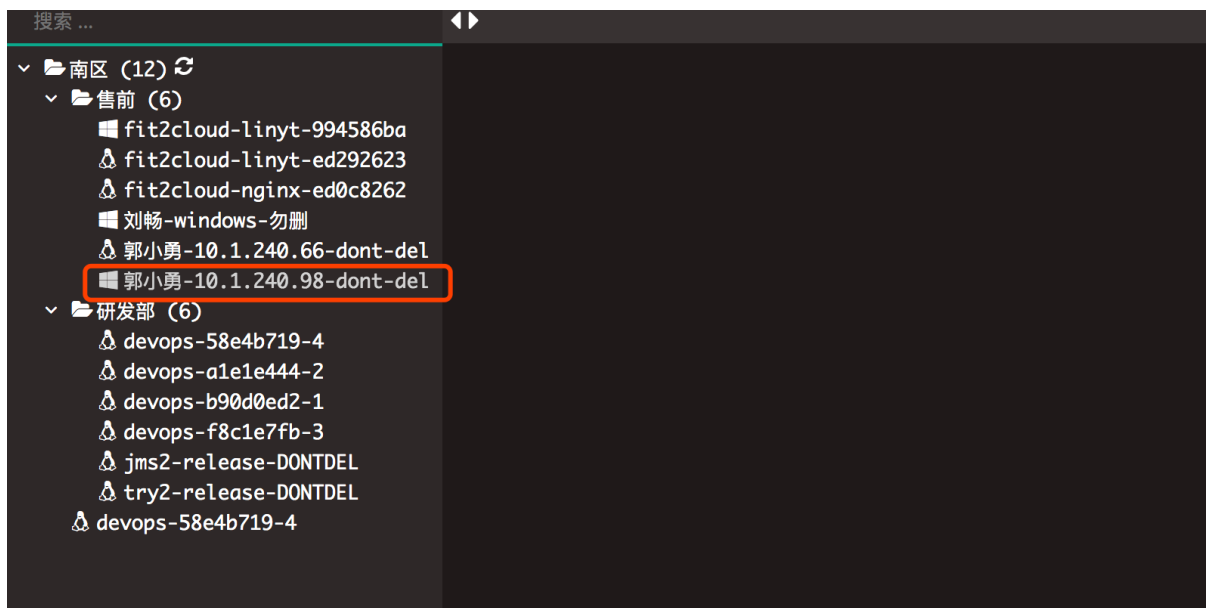


说明：

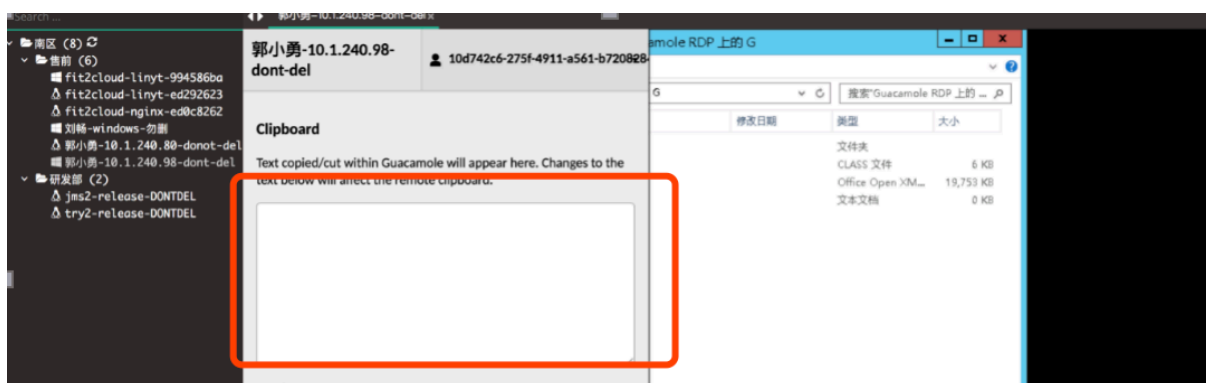
Linux 文件管理暂不支持上传下载文件夹，请先压缩再上传。

5.6 Windows 资产连接

1. 连接资产：鼠标左键点击需要访问的 Windows 资产，即可访问到 Windows 资产的登入页面，输入用户名密码登入资产。



2. 复制粘贴功能：目前支持资产中文字可向外复制粘贴，若需复制文字粘贴进资产，可以使用 Ctrl + Alt + Shift 快捷键，弹出功能界面，将需要粘贴的文字，拷贝进空白出，即可使用粘贴快捷键或右键粘贴实现文字粘贴进资产，该功能面板相当于剪切板。

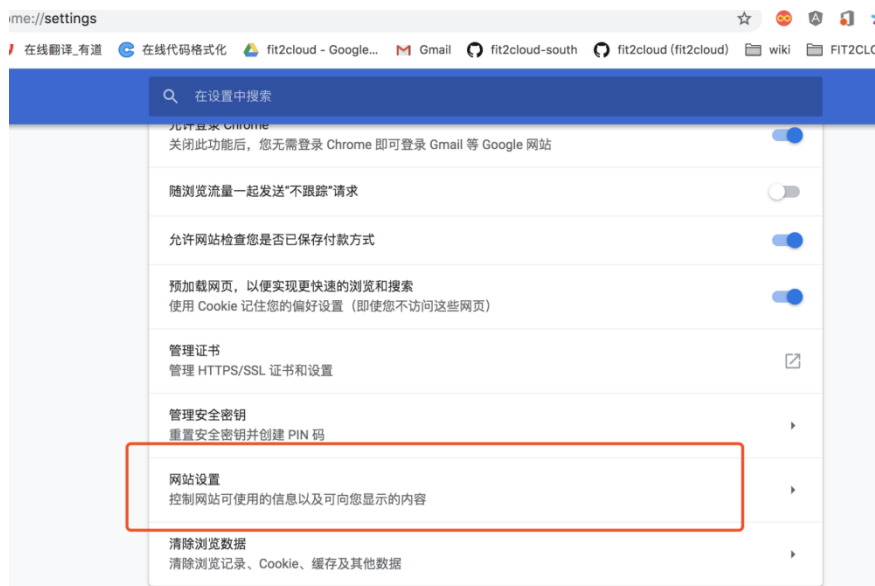


3. 直接复制粘贴功能：新版本中可以支持 Chrome 的直接复制粘贴，可以不需要使用 Ctrl + Alt + Shift 快捷键，但需要做如下配置：

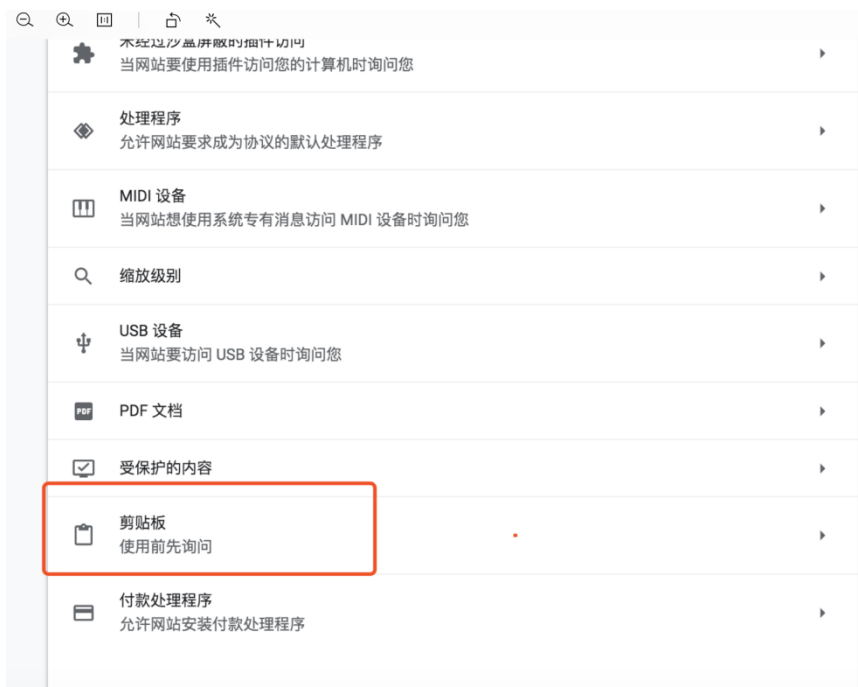
3.1 点击 Chrome 的菜单栏，点击设置



3.2 选择网站设置



3.3 选择剪贴板



3.4 添加堡垒机地址，注意地址必须是 https 的：

<https://jms.crc.com.cn>



3.5 设置完成即可直接复制粘贴文字进入 Windows 设备或远程应用中。

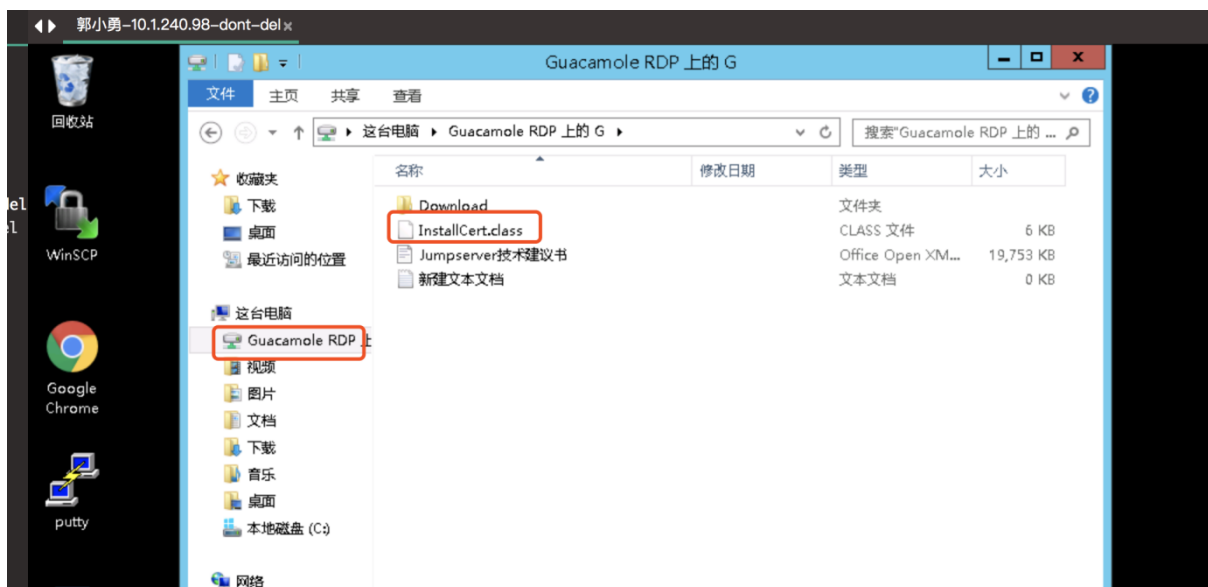
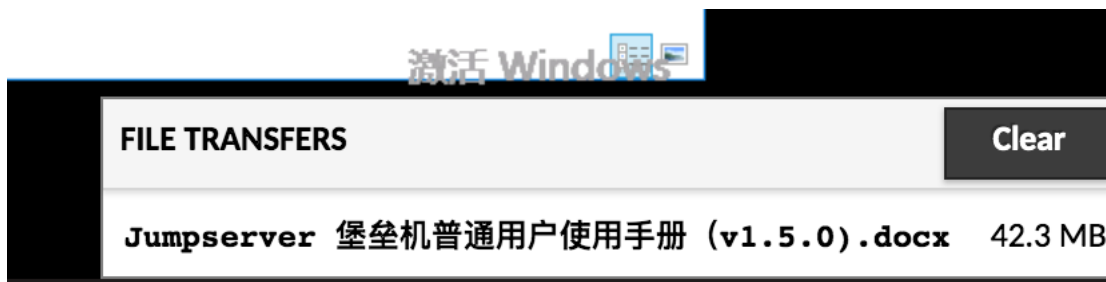
5.7 Windows 资产文件管理

1. 文件上传方式一：

- a) 直接将文件拖拽至 Windows 窗口，即开始上传文件。



b) 绿色进度条消失后，上传完成，请在虚拟设备 Guacamole RDP 中查看文件已上传文件。

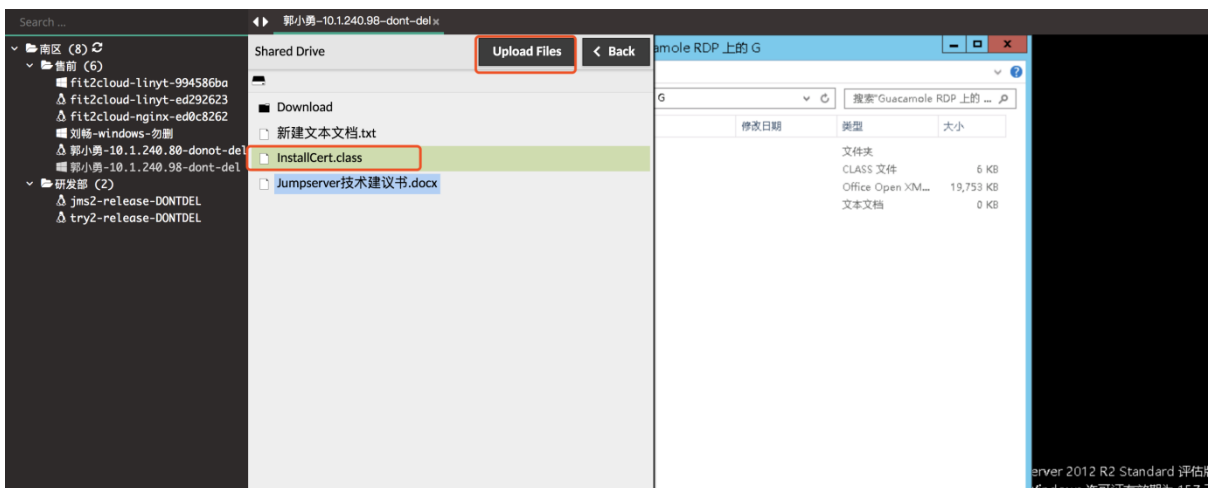


2. 文件上传方式二：

a) Share Drive：登入 Windows 资产，按住 Ctrl + Alt + Shift 快捷键，弹出共享设备界面

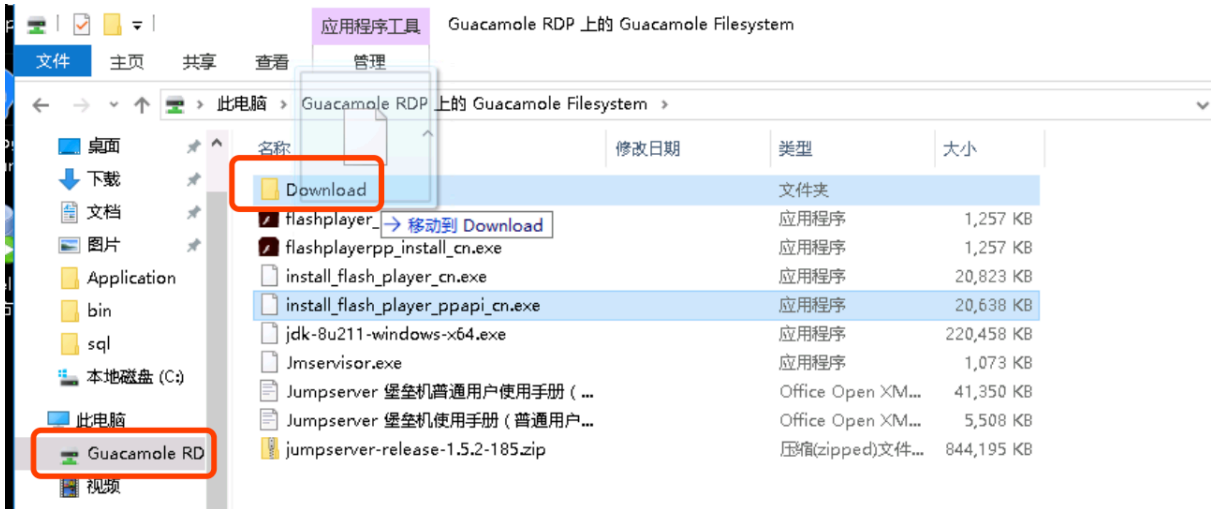


b) 文件上传下载：点击 Share Drive，进入共享的虚拟设备，双击文件，即可实现文件下载，点击 Upload Files，可实现文件上传。



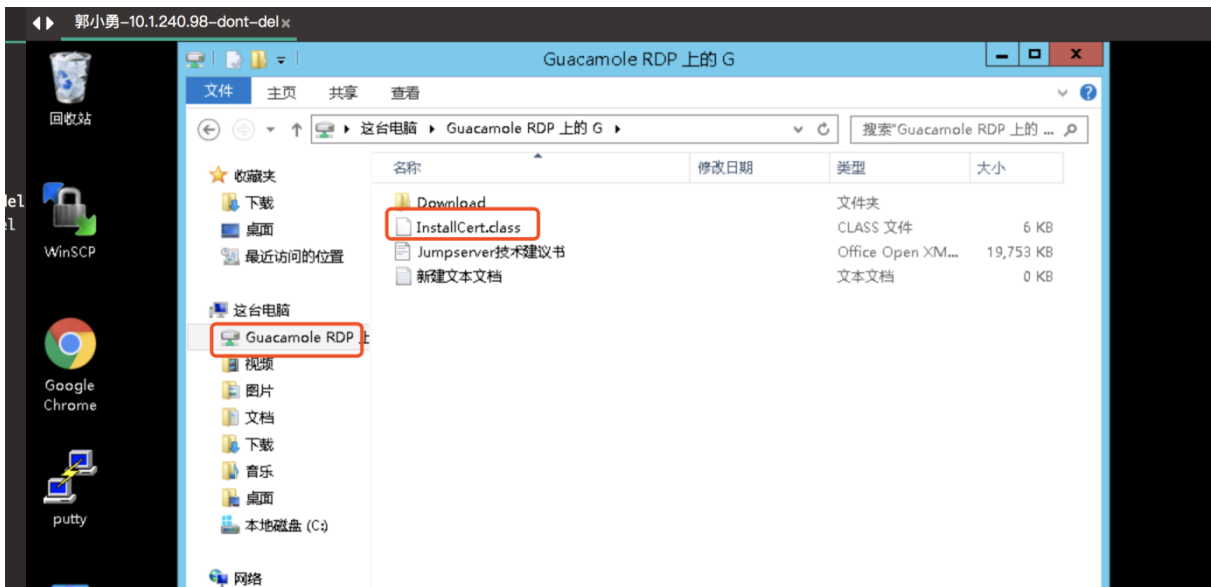
3. 文件下载方式一：

a) 将文件拖入虚拟设备 Guacamole RDP 中的 Download 目录，即可下载文件

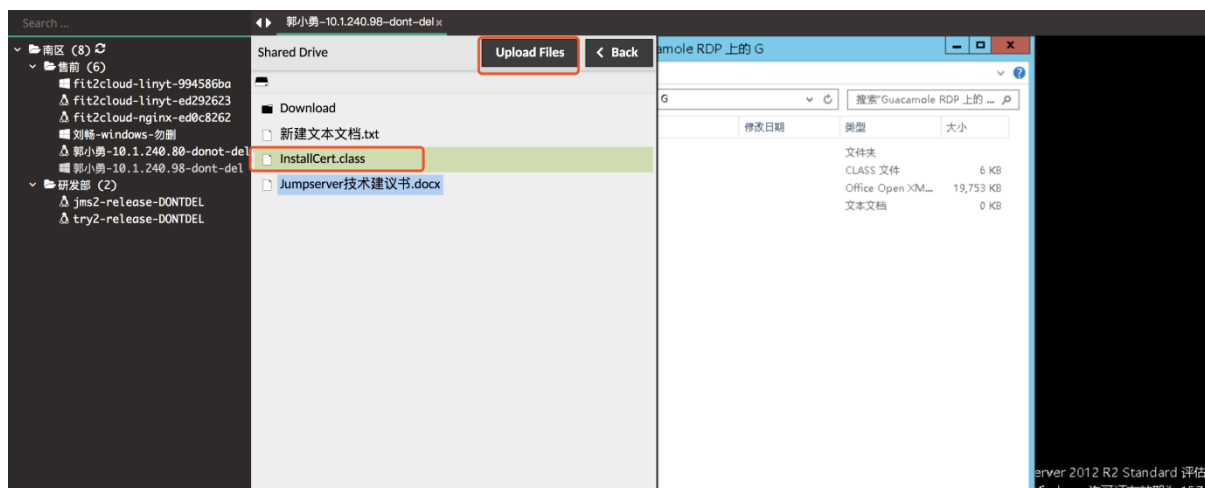


4. 文件下载方式二：

a) 将需要下载的文件拷贝进 虚拟设备 Guacamole RDP 中。



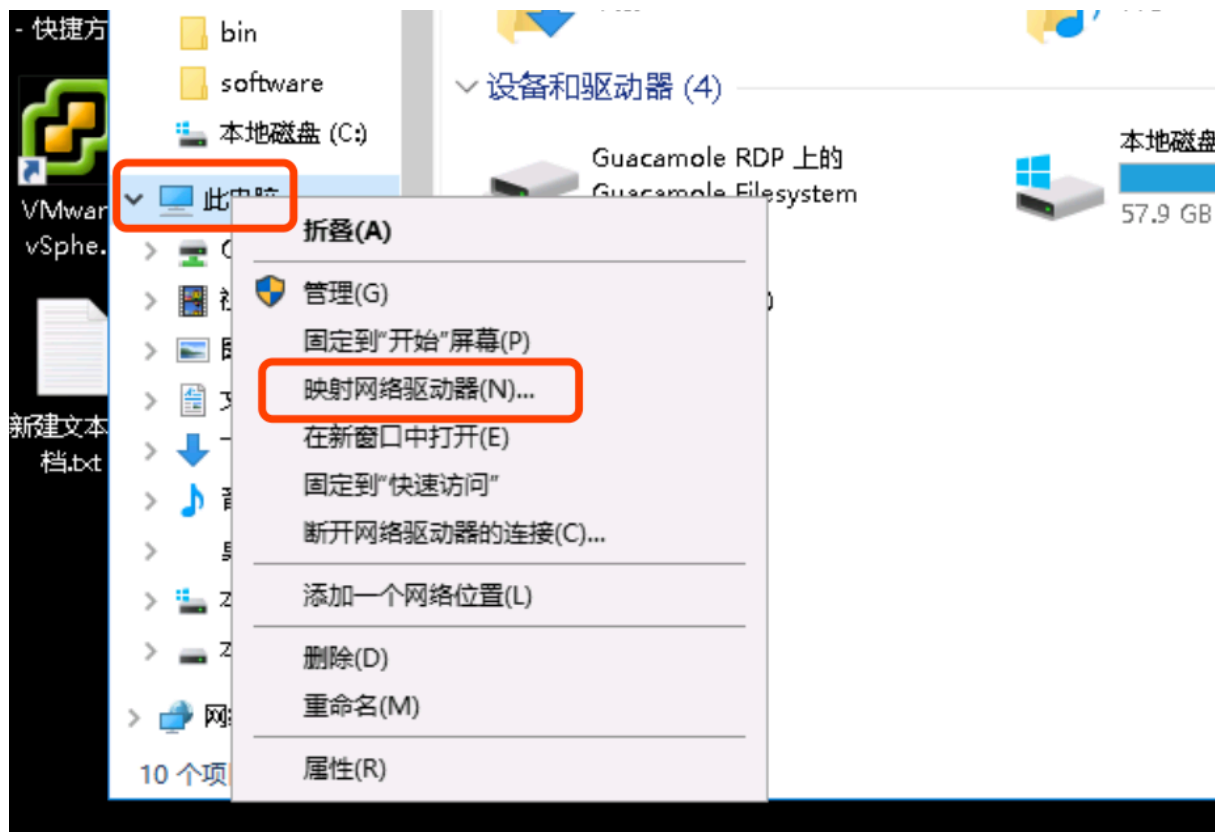
b) 按住 Ctrl + Alt + Shift 快捷键，弹出共享设备界面，点击 Share Drive，查看文件，双击文件可下载。



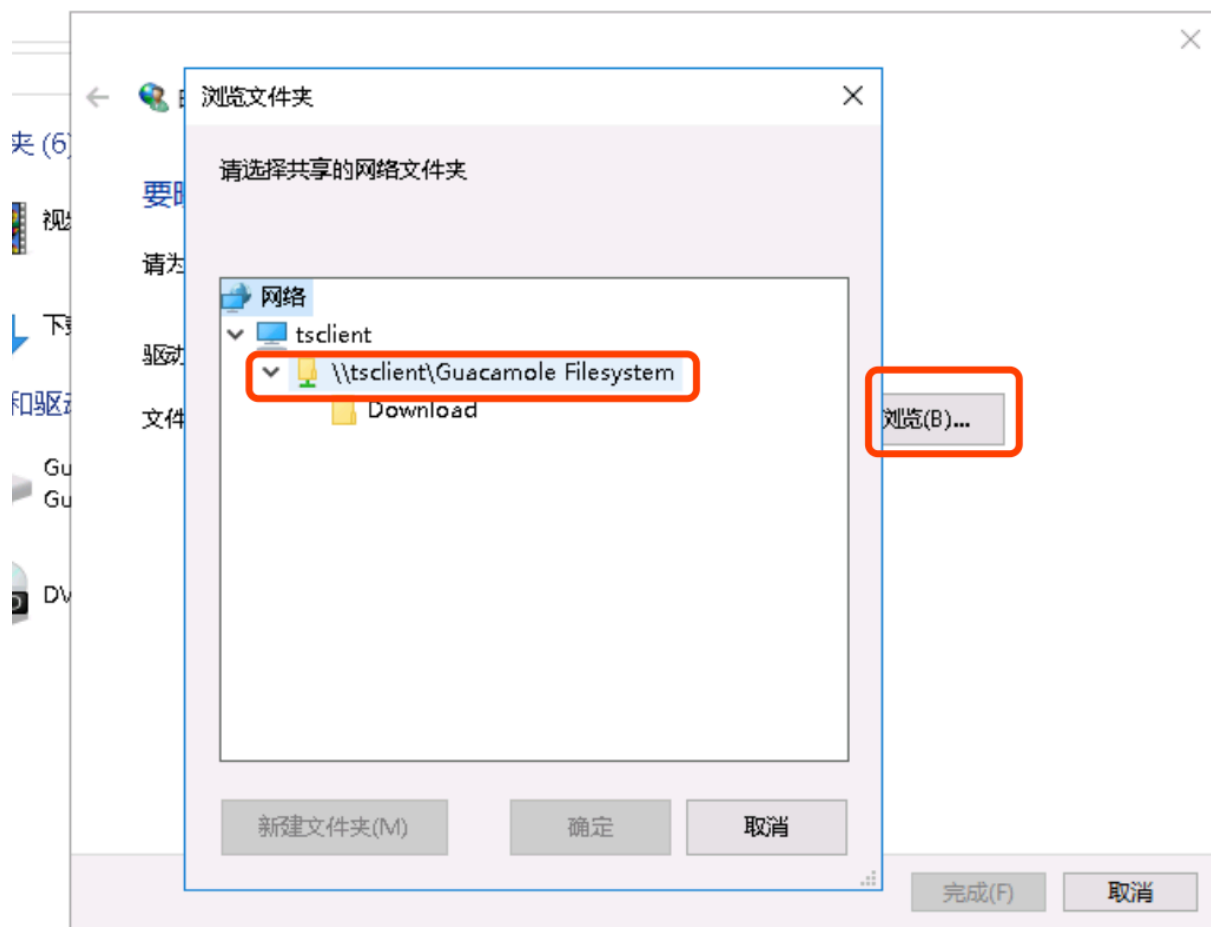
5.8 Windows 映射网络驱动

若发现 Window 设备中没有虚拟设备 Guacamole RDP，请参考以下内容，手动添加：

1. 点击“此电脑”右键，选择映射网络驱动器。



2. 点击“浏览”，选择 Guacamole Filesystem，点击确定，即可映射成功。



3. 若发现目录中没有 Guacamole Filesystem ，请参考这设置开启网络发现功能：

<https://jingyan.baidu.com/article/4853e1e5a1e3b41908f7266b.html>

说明：

Windows 上传下载目录为虚拟设备 Guacamole RDP。

Windows 文件管理暂不支持上传下载文件夹，请先压缩再上传。

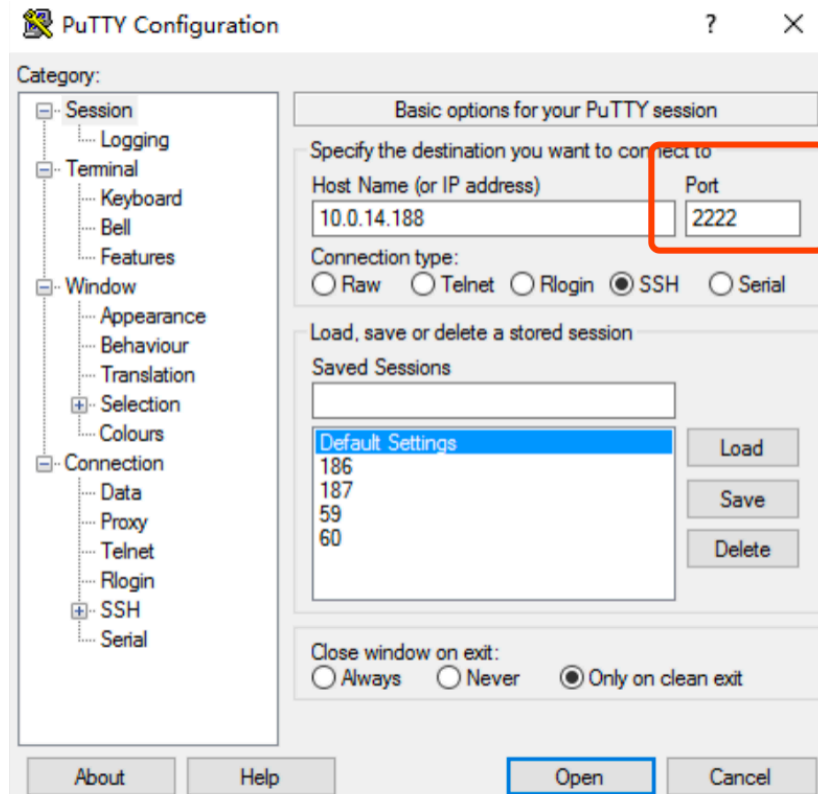
六、 shell 端登录

6.1 shell 端登录简介

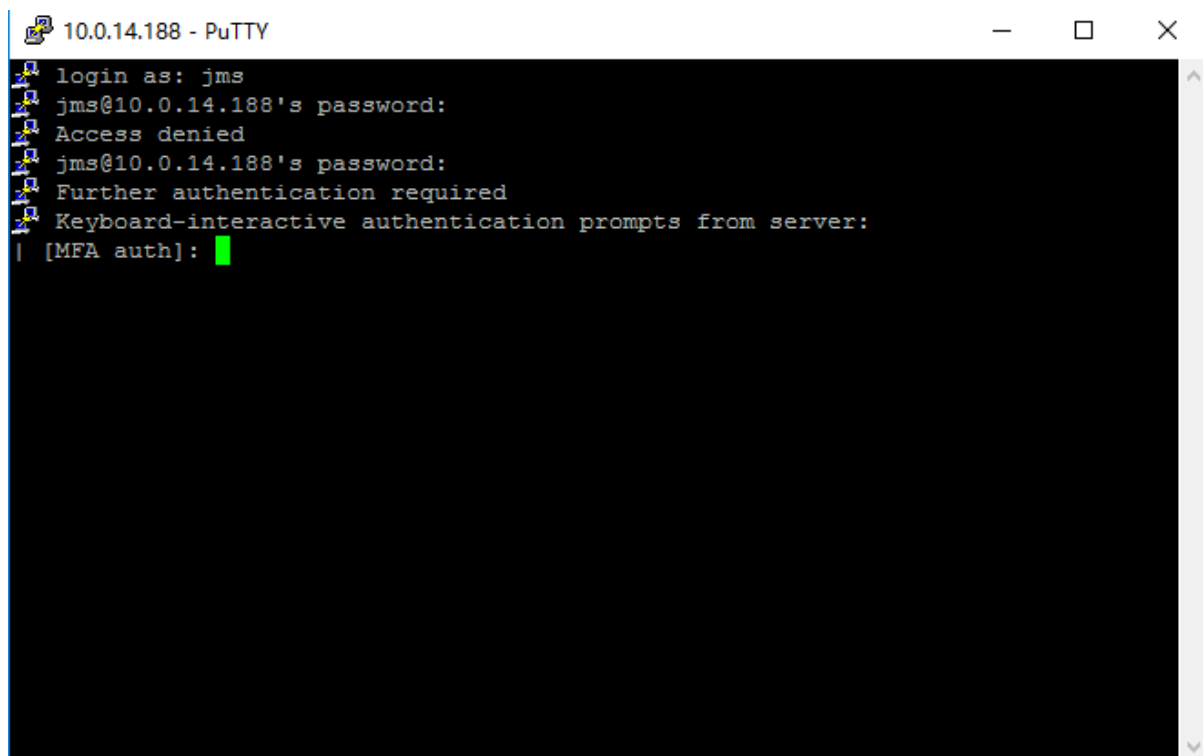
堡垒机除了内置的 Web 终端登陆资产的方式外，还提供了 shell 登录方式，用户可以使用自己惯用的终端工具如：Xshell，putty 等，或在 Shell 终端中输入命令 “ssh -p 2222 [用户名]@[堡垒机 IP] ” 或者 “ssh -p 2223 [用户名]@[堡垒机 IP] ” 进行连接。

6.2 SSH 端登录

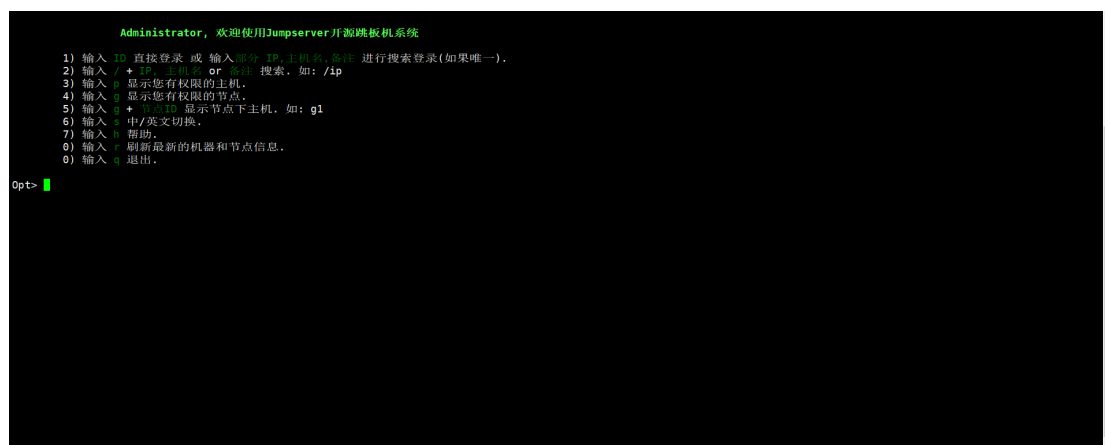
1. 终端登入：在 Shell 终端中输入命令 “ssh -p2222 [用户名]@[堡垒机 IP] ” 进行连接，或在 putty 等远程访问工具中连接堡垒机的 2222 端口，连接资产。如在账户中添加过公钥的情况下，可以使用对应的私钥进行免密登录：



2. MFA 认证：输入堡垒机账号、密码及 MFA 二次认证 6 位认证数字



3. 登入成功：登入成功后，来到欢迎页面，熟悉操作命令，特别是帮助命令，按命令说明进行操作



4. 访问资产：输入需要登入的资产编号或 IP，选择对应系统用户访问资产


```
1 ..... [w1z, zh1chi, test, root, appuser, any]
页码: 1, 数量: 1, 总页数: 1, 总数量: 1
Opt> 1
选择一个登录:
0 w1z
1 zh1chi
2 test
3 root
4 appuser
5 any
ID> aocuser
选择一个登录:
0 w1z
1 zh1chi
2 test
3 root
4 appuser
5 any
ID> 4
appuser's password: *****
开始连接到 appuser@..... 0.2
Last login: Tue Jun 4 10:15:49 2019 from 172.18.0.10
[appuser@Jtjumpvpc01 ~]$
```

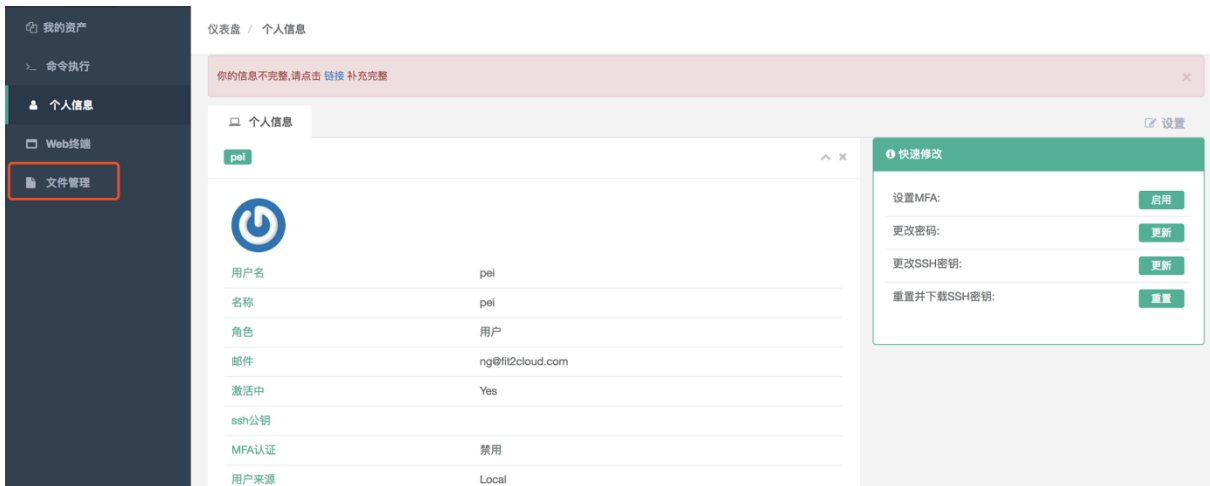
七、文件传输管理 (LIUNIX)

7.1 页面传输

说明：

该功能只针对 Linux 资产，并只支持由管理员配置好的自动登入的系统用户访问，若系统用户为手动登入用户请参照 2.5.3 进行文件管理。

1. 文件管理：点击“文件管理”，跳转至 Linux 文件管理页面，文件管理实现了针对自动登入的系统用户，对被授的 Linux 资产进行便捷地管理文件。



2. 文件管理页面：左侧显示被授权的资产，资产目录下显示登录该资产的系统用户，系统用户目录下显示该系统用户在资产上的 /tmp 目录。右侧显示登录该资产的系统用户的 /tmp 目录。点击自动登入的系统用户，即可使用该用户访问该资产的/tmp 目录。



7.2 终端传输

以 FileZilla 为例说明。

