云堡垒机

产品文档

文档目录

产品简介

产品概述

最近更新时间: 2022-11-17 10:26:23

云堡垒机通过轻量级的安全运维产品为客户提供用户认证、访问控制、权限管理、操作行为审计等服务。免客户端安装，支持移动运维。

功能优势

最近更新时间: 2022-11-17 10:26:23

-满足合规要求

满足多因素认证、操作监控和审计等合规要求。

-移动运维

除普通PC之外，支持通过手机、PAD等移动设备终端进行管理和运维，解放运维人员和管理人员对工作环境的依赖。

-免客户端

无需安装专门的运维客户端工具和APP，只需要有浏览器即可，解放对运维工具的依赖。

-易于掌握和学习

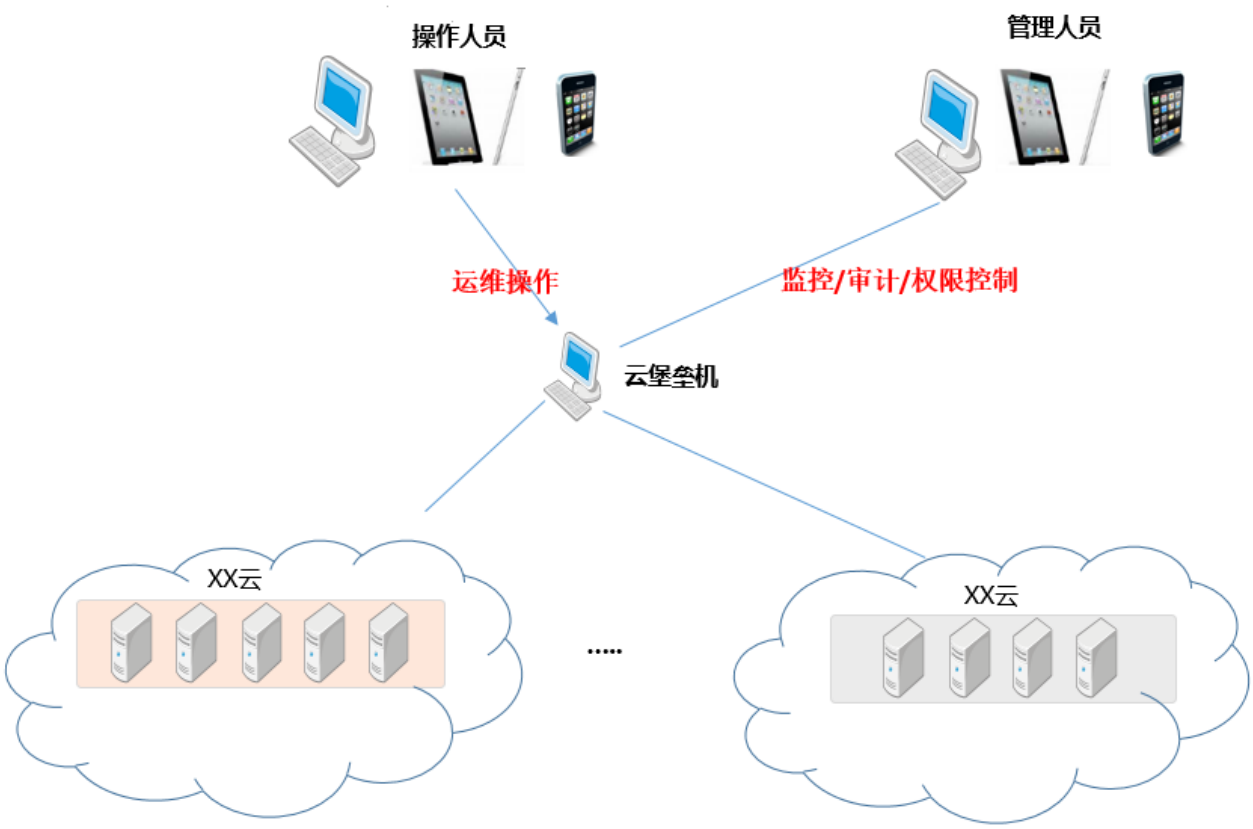
所见即所得，学习成本低，普通用户无需专业技能即可管理使用，解放对于专业人员的过度依赖和打扰。

应用场景

最近更新时间: 2019-11-27 16:43:05

运维人员通过云堡垒机进行用户认证、登录转接后完成运维操作；

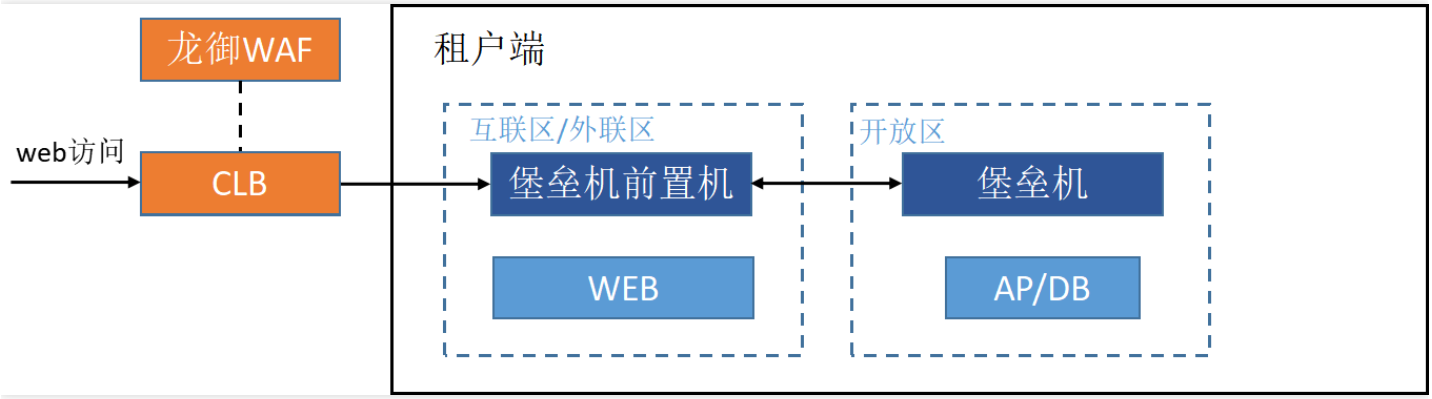
管理员通过云堡垒机进行用户管理、运维用户权限管控、操作监控、事后审计等。



产品架构

最近更新时间: 2022-11-17 10:26:23

堡垒机前置机部署在互联区/外联区，堡垒机部署在开放区



推荐解决方案

最近更新时间: 2022-11-17 10:26:23

用户0-200、纳管资产0-500，推荐使用：

CPU/内存	硬盘	用户	资产	并发数
4核/8G	400G	0以上	0以上	100

说明：

1.资产，此处指属于用户的云服务器（Linux、Windows等主机）等；

2.并发数，指同时在线使用云堡垒机连接目标资产的连接个数，每增加100并发数，需要增加一台“4核/8G/、400G硬盘”的云堡垒机；

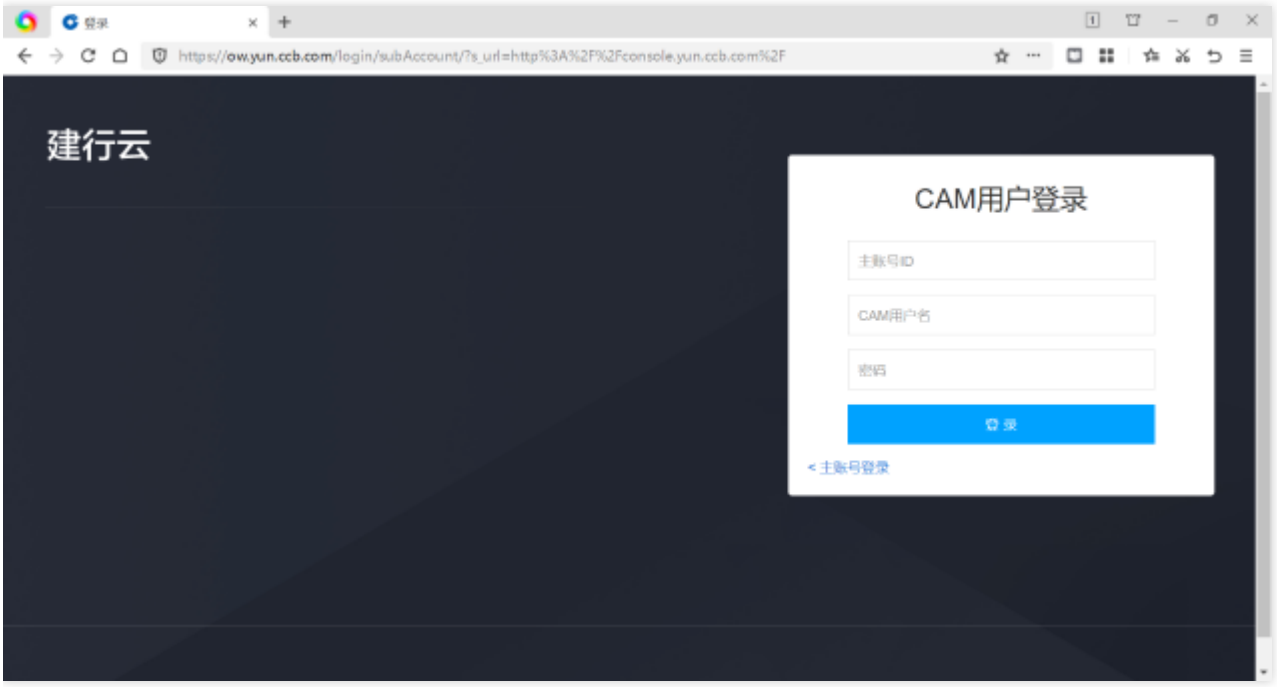
3.存储空间，取决于用户的操作量，以50个用户、平均每天运维操作2小时为例，平均每秒产生5k的日志，则平均每天约产生2G的日志，申请400G的硬盘可在线保存200天。如果操作日志需要保存更长时间，请按以下公式计算所需存储空间并申请扩容：

用户数×平均每天运维时间（秒）×5k（平均每秒产生的日志大小）×保存时间（天）/（1024×1024）=所需存储空间（G）

快速入门
用户登录

最近更新时间: 2023-01-05 14:24:15

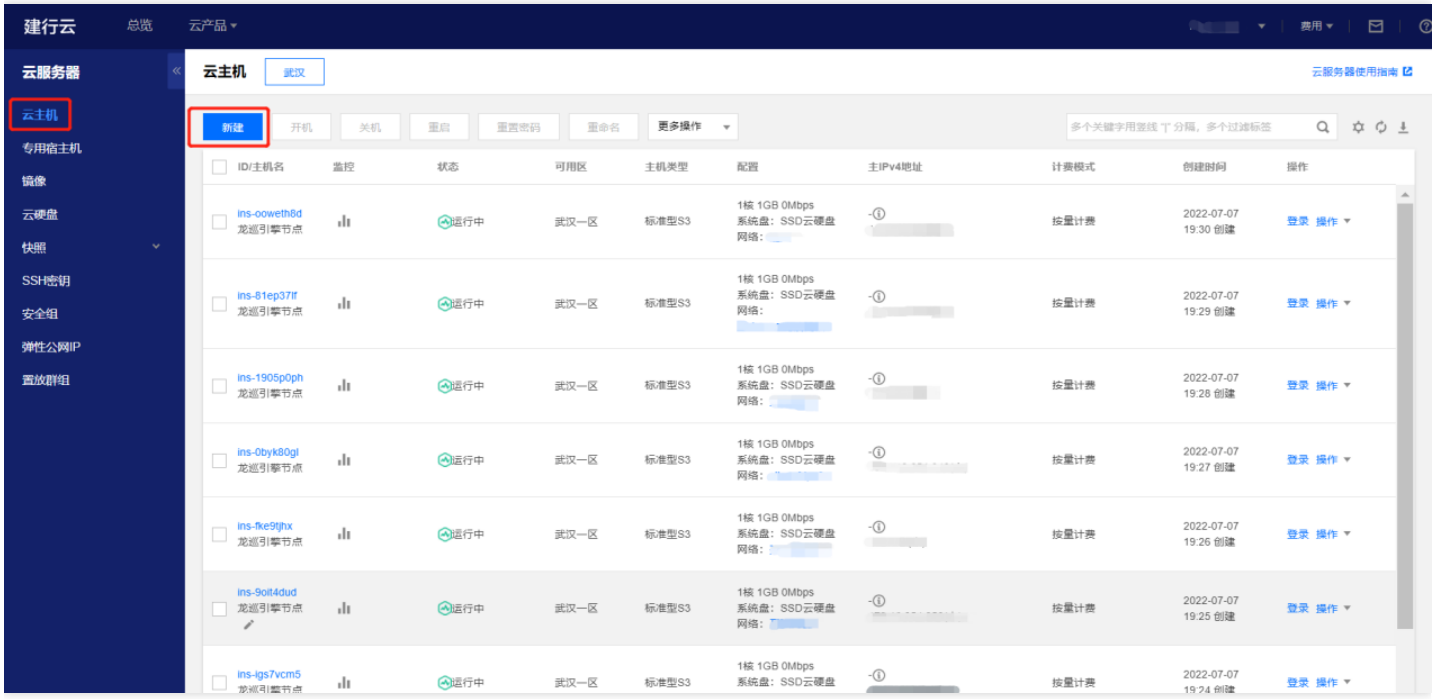
用户登录到云官网。



创建前置机

最近更新时间: 2023-01-11 11:34:00

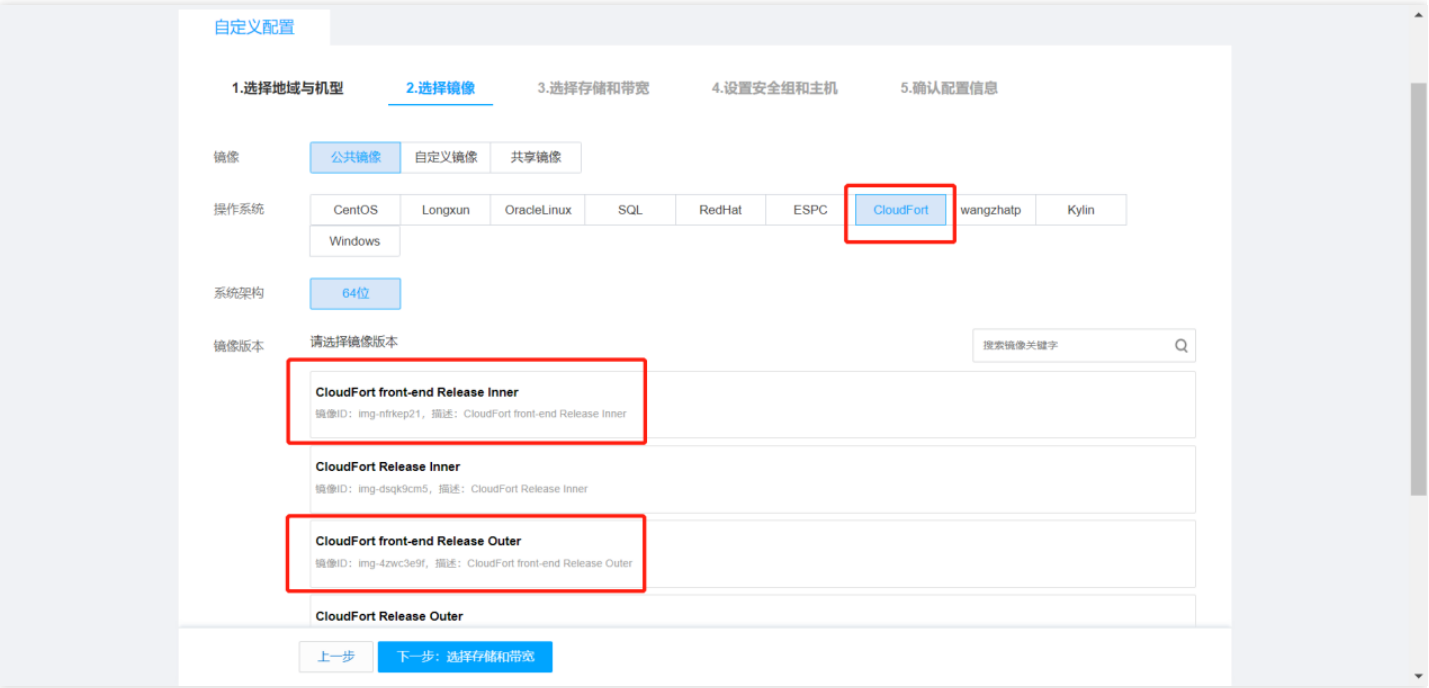
进入云服务器。



点击新建，选择地域和机型，在“自定义配置”页面，选择“地域”、“可用区”、“网络（选择互联区/外联区，不与堡垒机在同一个网络区域）”、“实例”，完成后点击“下一步：选择镜像”。

实例按照自身情况申请适当的前置机配置。前置机需安装龙防，龙防基本配置要求2C4G。前置机推荐配置4C8G。

为实现内外部租户的隔离管控，降低安全风险，目前从机器互联网安全暴露风险角度考虑，前置机镜像分为了外部租户前置机镜像（镜像名称：CloudFort front-end Release Outer）和内部租户前置机镜像（镜像名称：CloudFort front-end Release Inner），内外部租户定义详见本文档“常见问题-内外部租户定义？”，各租户在新建前置机时需要依据实际情况选择相应的镜像进行创建。



完成后点击“下一步：选择存储和带宽”。

完成后点击“下一步：设置安全组和主机”。

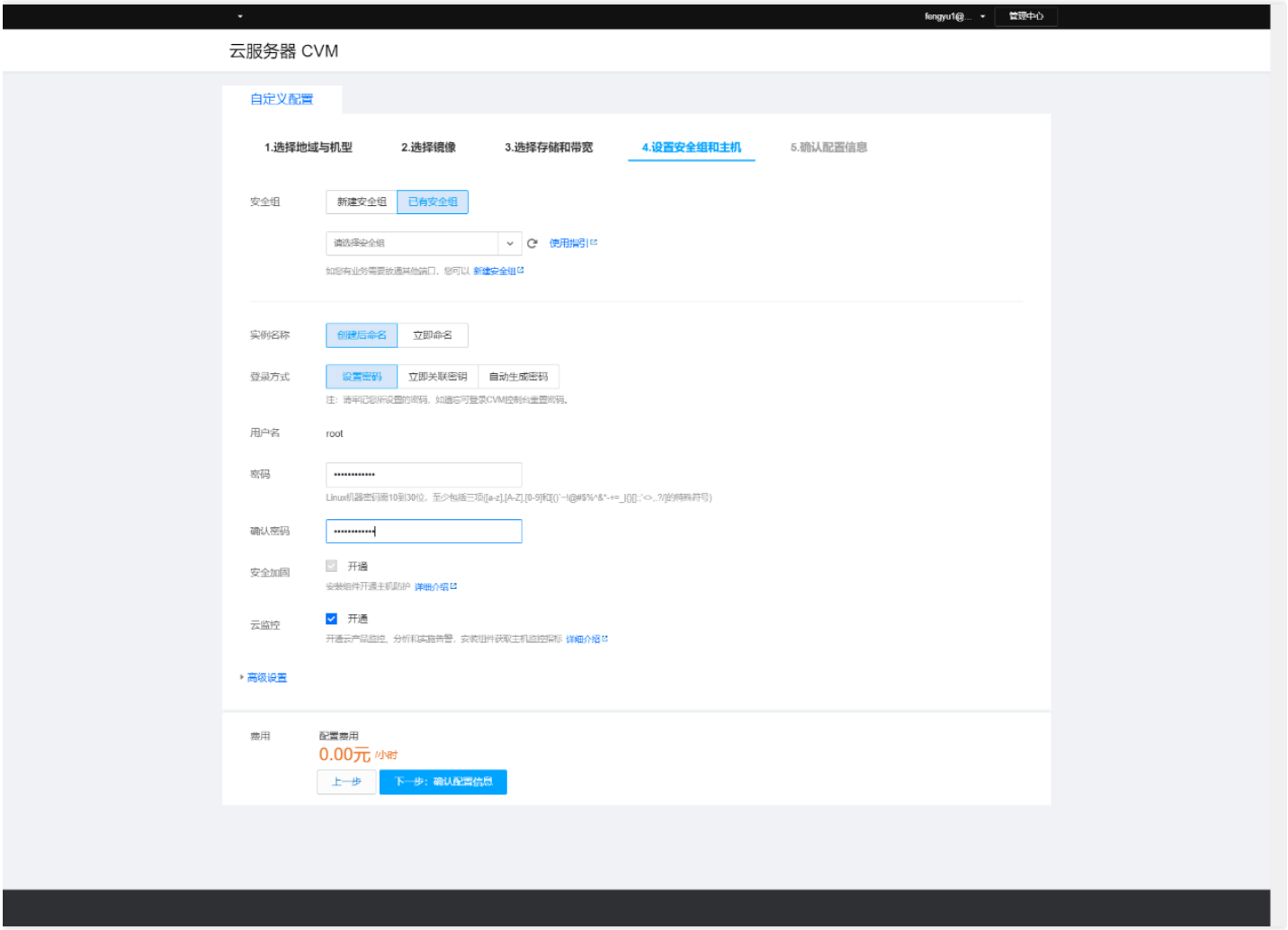
前置机安全组设置

入站规则：

来源	协议端口	策略	备注
堡垒机IP	TCP:8119	允许	
0.0.0.0/0	ALL	拒绝	
堡垒机IP	TCP:22	允许	
0.0.0.0/0	ALL	拒绝	

出站规则：

来源	协议端口	策略	备注
0.0.0.0/0	TCP:80	允许	
龙巡服务器IP	ALL	允许	



完成后点击“下一步：确认配置信息”。

请展开每个子区域，仔细核对配置信息，确认无问题后点击“开通”

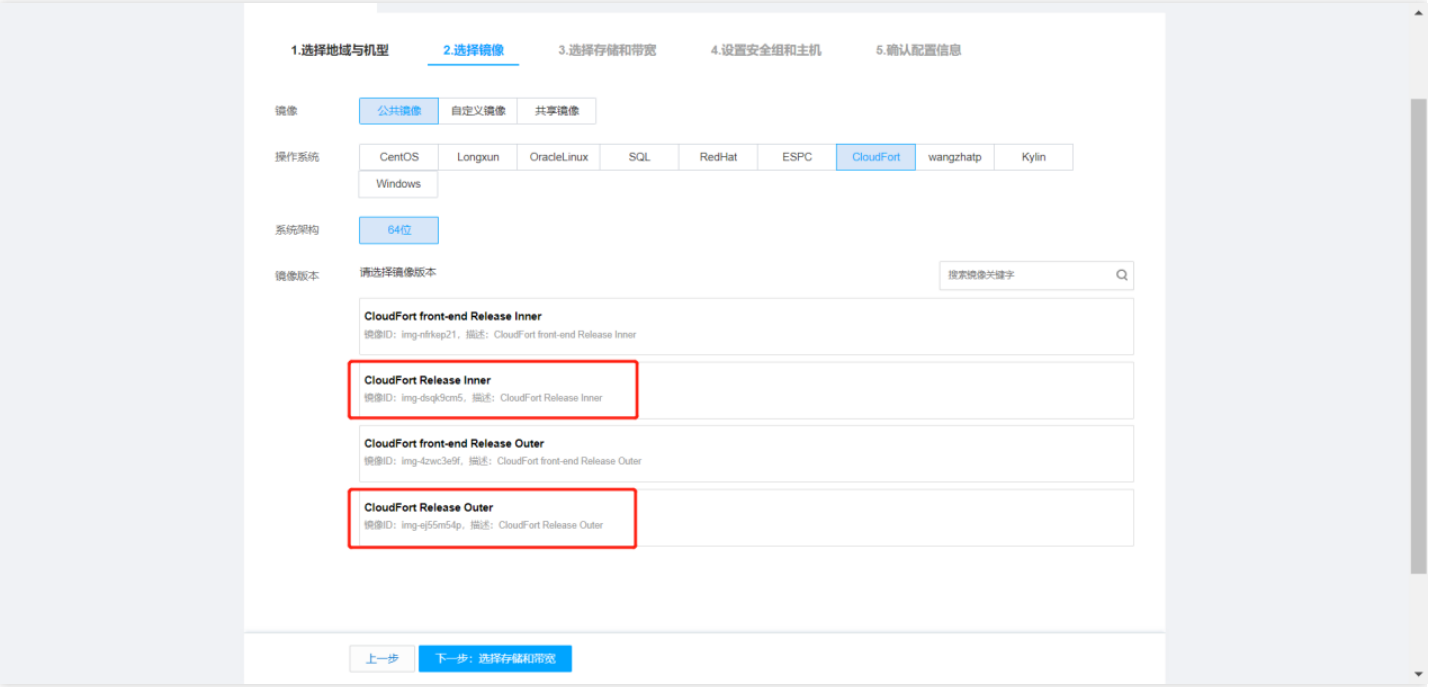
创建堡垒机

最近更新时间: 2023-01-11 11:34:00

点击新建，选择地域和机型，在“自定义配置”页面，选择“地域”、“可用区”、“网络（选择开放区，不与前置机在同一个网络区域）”、“实例”，完成后点击“下一步：选择镜像”。
实例按照自身情况申请适当的堡垒机配置。堡垒机需安装龙防，龙防基本配置要求2C4G。堡垒机推荐配置4C8G。

为实现内外部租户的隔离管控，降低安全风险，目前从机器互联网安全暴露风险角度考虑，堡垒机镜像分为了外部租户堡垒机镜像（镜像名称：CloudFort Release Outer）和内部租户堡垒机镜像（镜像名称：CloudFort Release Inner），内外部租户定义详见本文档“常见问题-内外部租户定义？”，各租户在新建堡垒机时时需要依据实际情况

选择相应的镜像进行创建。



完成后点击“下一步：选择存储和带宽”。

“数据盘”，用于存储用户操作录像文件，大小主要取决于用户的操作量，以50 个用户、平均每天运维2 小时为例，平均每秒产生 5k 的日志，则平均每天约产生 2G 的日志，申请 400G 的硬盘可在线保存 200 天。如果操作日志需要保存更长时间，请按以下公式计算所需存储空间进行申请或以后扩容：用户数×平均每天运维时间（秒）×5k（平均每秒产生的日志大小）×保存时间（天）/（1024×1024）=所需存储空间（G）

完成后点击“下一步：设置安全组和主机”。

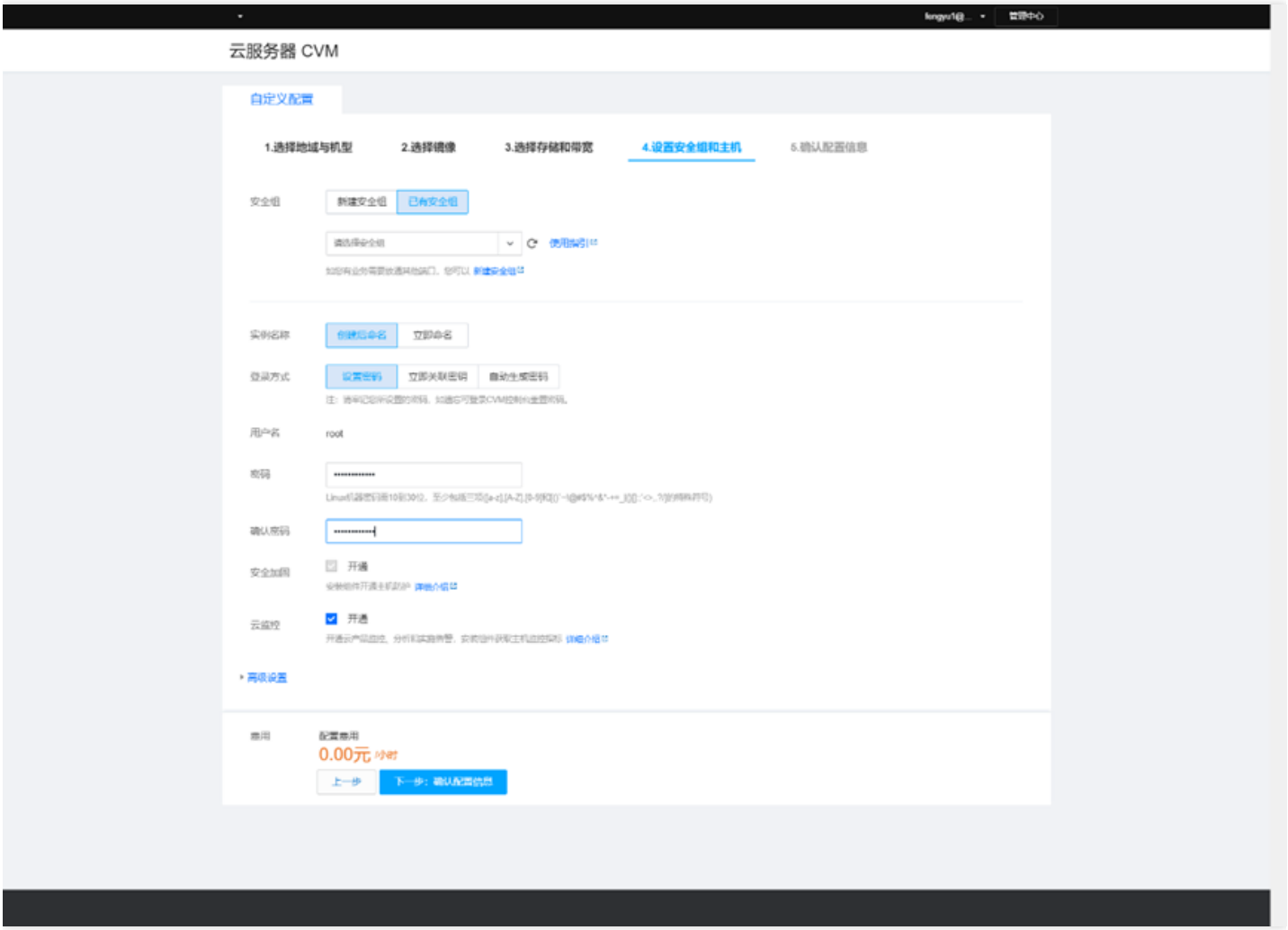
堡垒机安全组设置：

入站规则：

来源	协议端口	策略	备注
前置机IP	TCP:8119	允许	
龙巡服务器IP	ALL	允许	
堡垒机IP	TCP:22	允许	
0.0.0.0/0	ALL	拒绝	

出站规则：

来源	协议端口	策略	备注
0.0.0.0/0	TCP:22	允许	
Windows服务器IP	TCP:13389,10800	允许	
裸金属服务器	TCP:36000	允许	
0.0.0.0/0	ALL	拒绝	



完成后点击“下一步：确认配置信息”。

请展开每个子区域，仔细核对配置信息，确认无问题后点击“开通”

挂载云硬盘

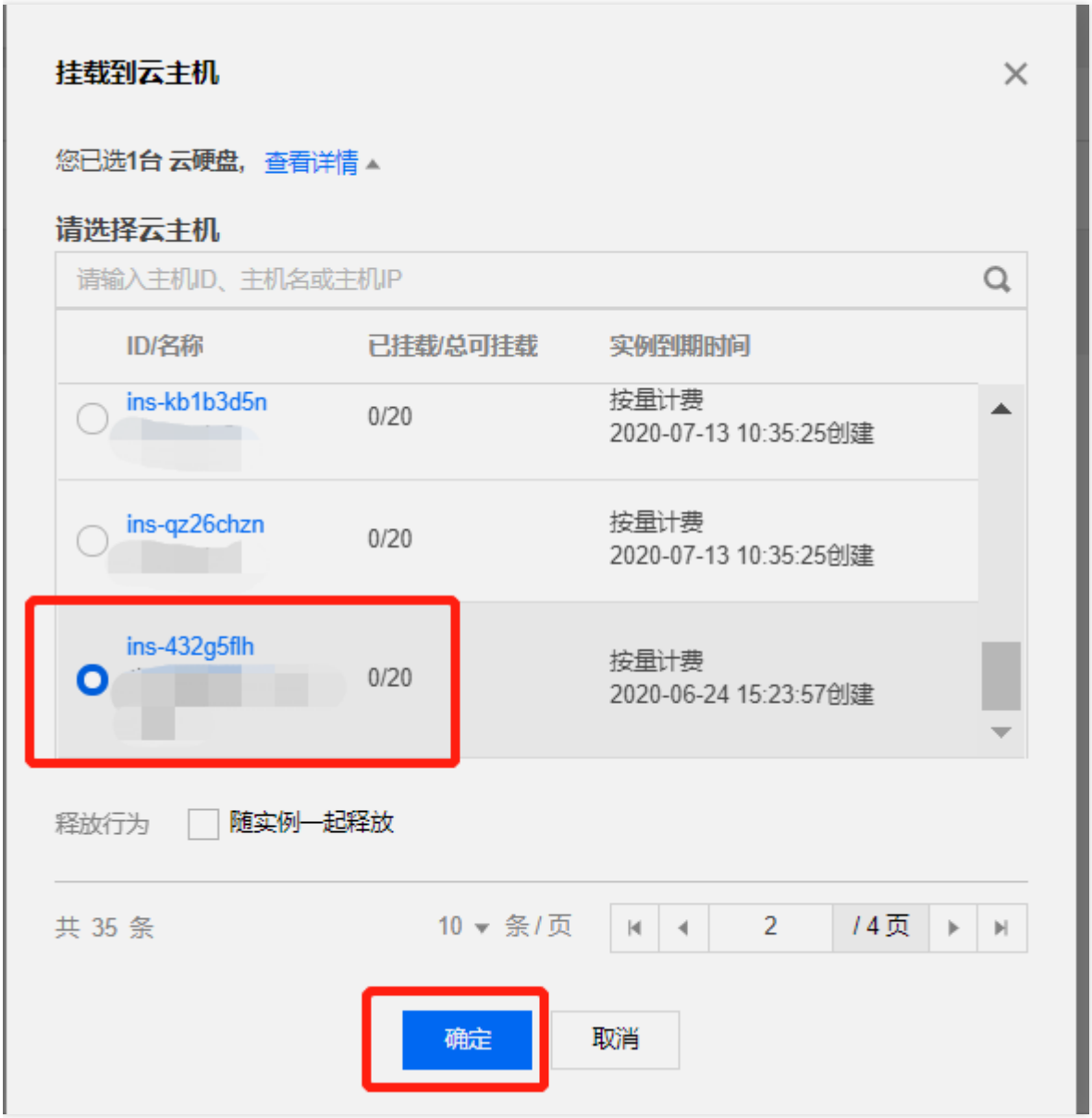
最近更新时间: 2023-01-11 11:34:00

1、进入云硬盘点击新建创建云硬盘

2、填写云硬盘容量和磁盘名称

3、将云硬盘挂载到堡垒机，勾选新创建的云硬盘点击挂载

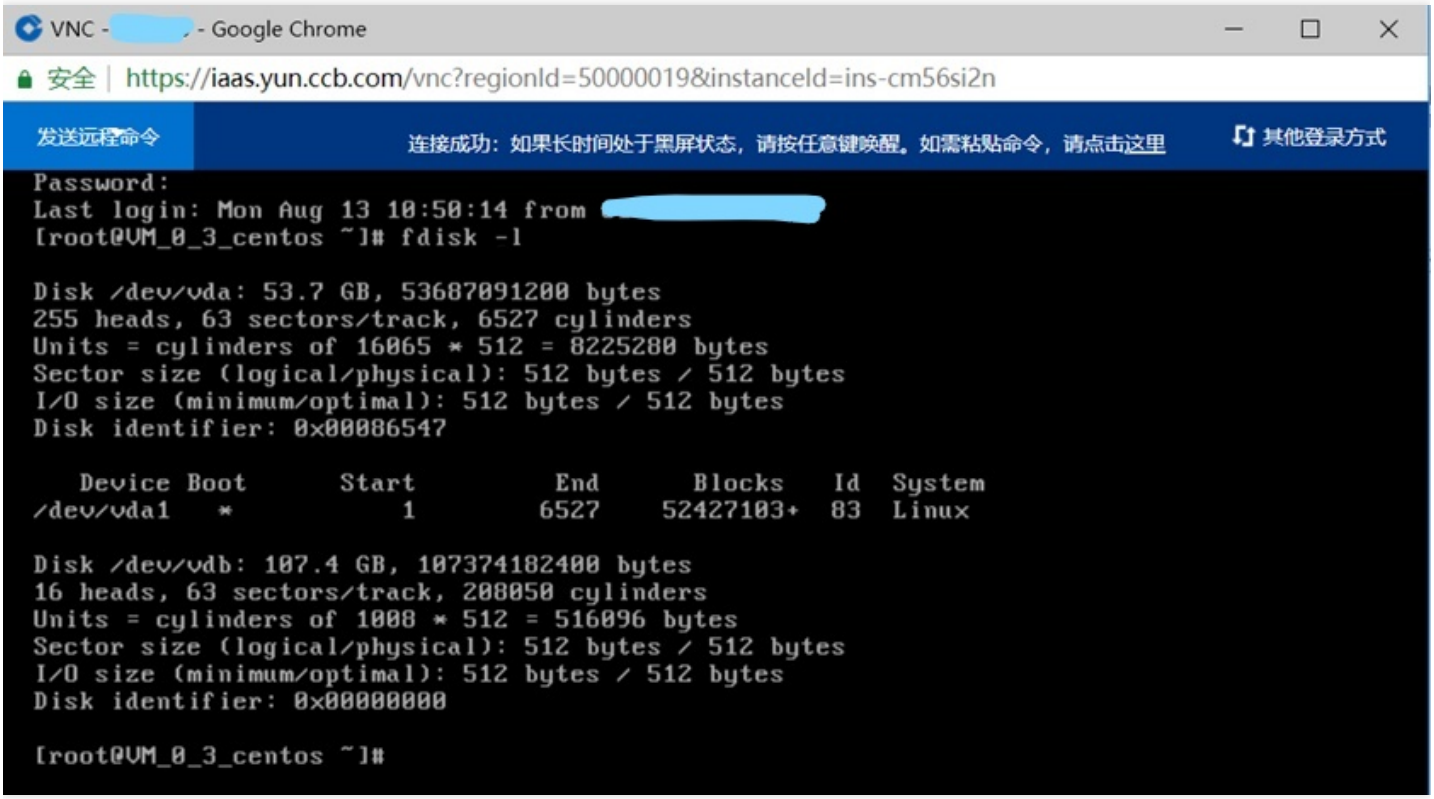
4、勾选对应堡垒机，点击确定



5、新建云硬盘状态显示已挂载，如下图所示

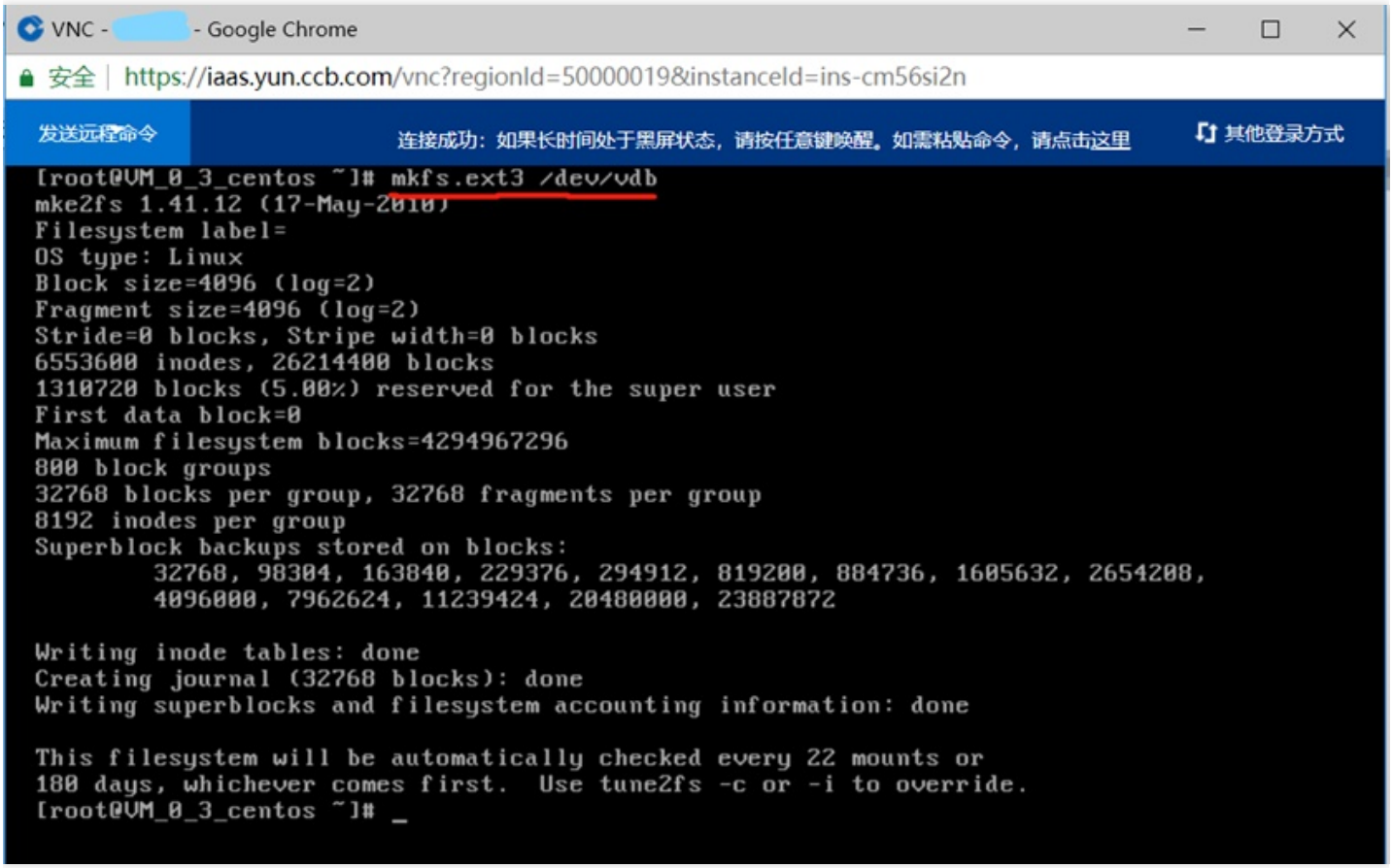
6、通过VNC登录云堡垒机操作系统

7、fdisk –l 查看云硬盘磁盘名称



如上图示例，操作系统盘/dev/vda 待挂载的云硬盘磁盘名 /dev/vdb

8、格式化云硬盘:mkfs.ext3 /dev/vdb



9、 执行mkdir /somdata创建挂载点

10、 执行mount /dev/vdb /somdata 把云硬盘挂载somdata

11、 修改/etc/fstab 云主机开机挂载云硬盘

echo ”/dev/vdb /somdata ext3 defaults 0 0”>>/etc/fstab

12、 云堡垒机数据迁移到云盘

在VNC窗口输入 sh /usr/local/splatmon/splat_mount.sh

配置前置机与堡垒机访问关系

最近更新时间: 2023-01-11 11:34:00

前置机和堡垒机的访问关系通过修改前置机的nginx配置实现。登录前置机，修改前置机的nginx配置文件，编辑/usr/local/nginx/conf/nginx.conf配置文件，将相应的端口服务转向对应的堡垒机ip和8119端口，执行命令sh /usr/local/nginx/sbin/nginx –t检查nginx.conf配置文件内容格式结果为successful，执行命令nginx –s reload重新加载nginx配置,执行命令ps –ef |grep nginx检查nginx启动时间为当前时间。

```
server {
       listen  443 ssl http2 ;
       listen   80;
       ssl_certificate "/usr/local/nginx/certs/nginx.crt";
       ssl_certificate_key "/usr/local/nginx/certs/nginx.key";
       proxy_redirect http:// https:// ;
       client_max_body_size 1024000m;
       if ($time_iso8601 ~ "(\d{4}-\d{2}-\d{2})")
       {
       {
       }
       access_log logs/host.access.$tttt.log  main;
#        ssl_session_cache shared:SSL:1m;
#        ssl_session_timeout  10m;
#        ssl_ciphers HIGH:!aNULL:!MD5;
#        ssl_prefer_server_ciphers on;
#
#        # Load configuration files for the default server block.
#        include /usr/local/nginx/default.d/*.conf;
       location /api {
             deny all;
               }

       location / {
           proxy_pass http://172.[redacted]:8119;

           proxy_set_header Host $http_host;
           proxy_set_header X-Real-IP $remote_addr;
           proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
           proxy_set_header Upgrade $http_upgrade;
           proxy_set_header Connection $connection_upgrade;
       }
```

显示工具栏

```
[root@VM_0_85_centos nginx]# vi /usr/local/nginx/conf/nginx.conf
[root@VM_0_85_centos nginx]# nginx -t
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok
nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful
[root@VM_0_85_centos nginx]# nginx -s reload
[root@VM_0_85_centos nginx]# ps -ef |grep nginx
root      5452 23583  0 09:13 ?        00:00:00 nginx: worker process
root      5453 23583  0 09:13 ?        00:00:00 nginx: worker process
root      5459  4193  0 09:13 pts/0    00:00:00 grep --color=auto nginx
root     23583     1  0 Oct10 ?        00:00:00 nginx: master process /usr/local/nginx/sbin/nginx
[root@VM_0_85_centos nginx]#
```

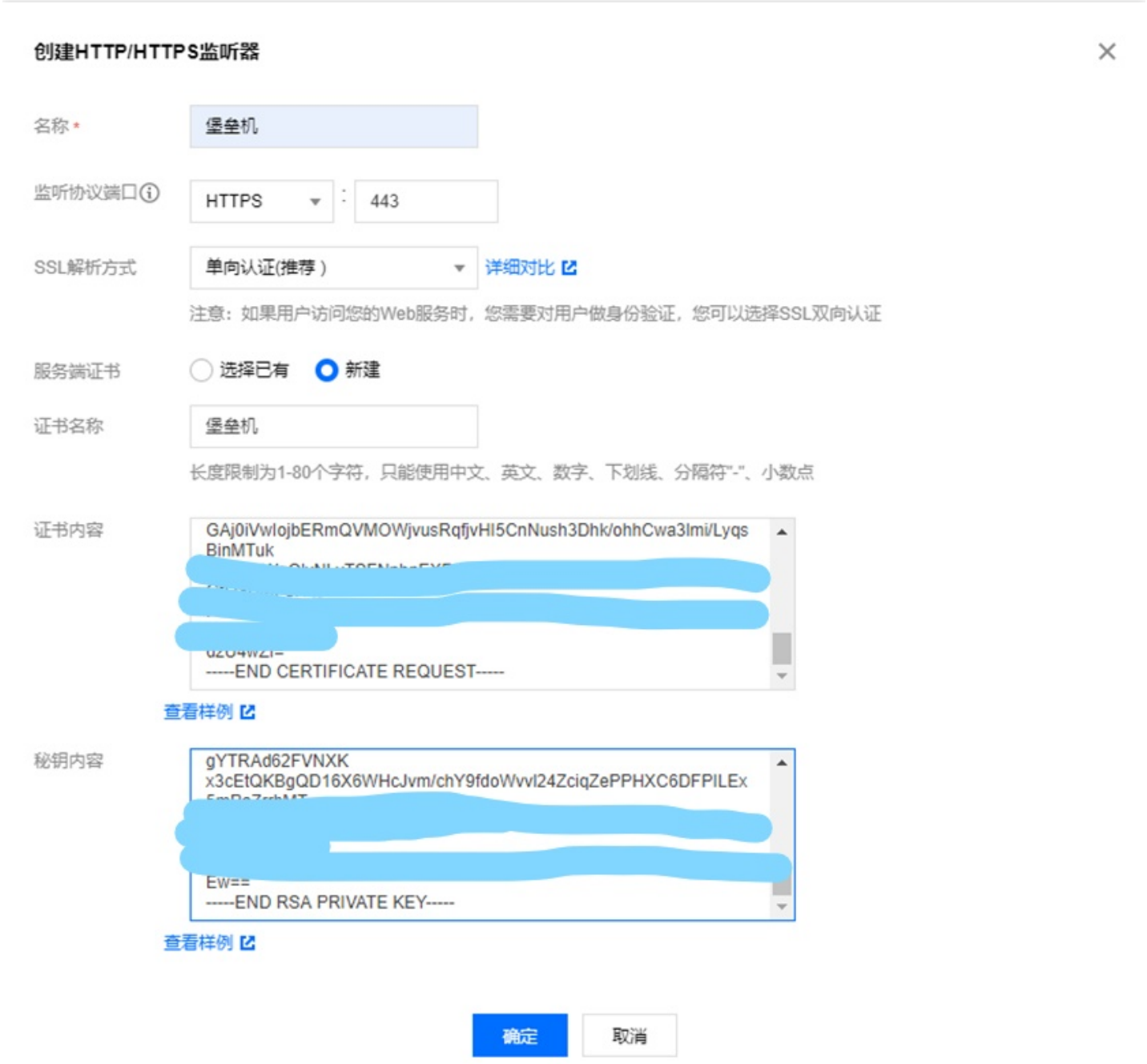
设置域名访问堡垒机并通过WAF监控流量

最近更新时间: 2023-01-11 11:34:00

行方规定使用ECC机房环境访问堡垒机，使用内网负载创建域名并且绑定前置机，由于特殊原因需要通过互联网访问堡垒机，需要申请互联网访问（需要提前联系运营一线报备加白，运营一线联系电话：87815199-29827），此配置需要在互联网区外网负载进行操作，具体步骤与内网负载一致。

创建负载均衡https监听器，端口号默认选择443，如多个堡垒机，可在该端口下多建立几个域名，如果创建其他端口，访问时需要域名加端口号，例如：https://堡垒机域名:端口号，在新建的域名后绑定前置机的80端口。

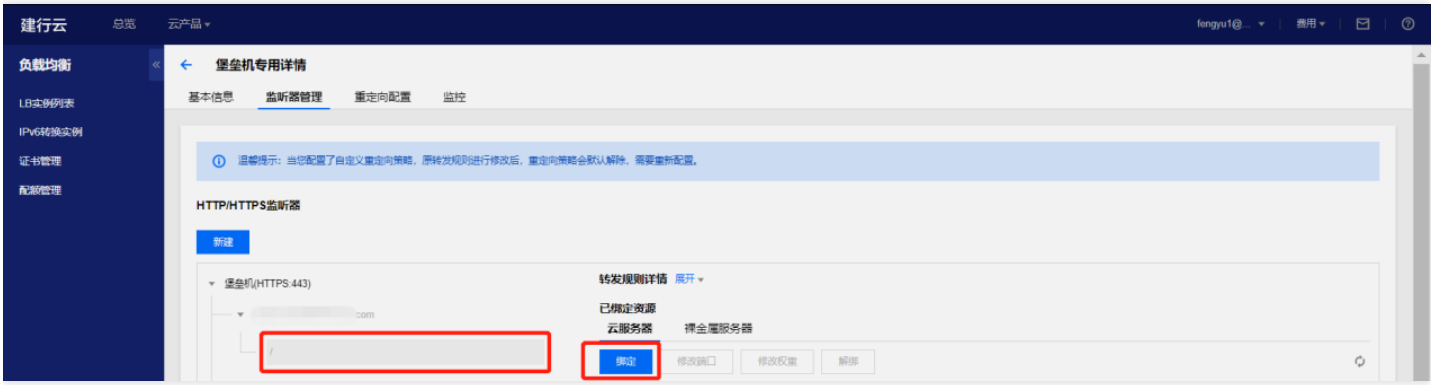
1、进入负载均衡点击新建创建HTTPS监听器，填写监听器信息后点击确定。（堡垒机证书使用云堡垒机-安装手册附件cert.tar.gz中的文件，nginx.crt为证书，nginx.key为秘钥，然后将内容分别复制到相应的位置。堡垒机-安装手册联系我们获取，联系邮箱fxglb_sp2.zh@ccb.com。）

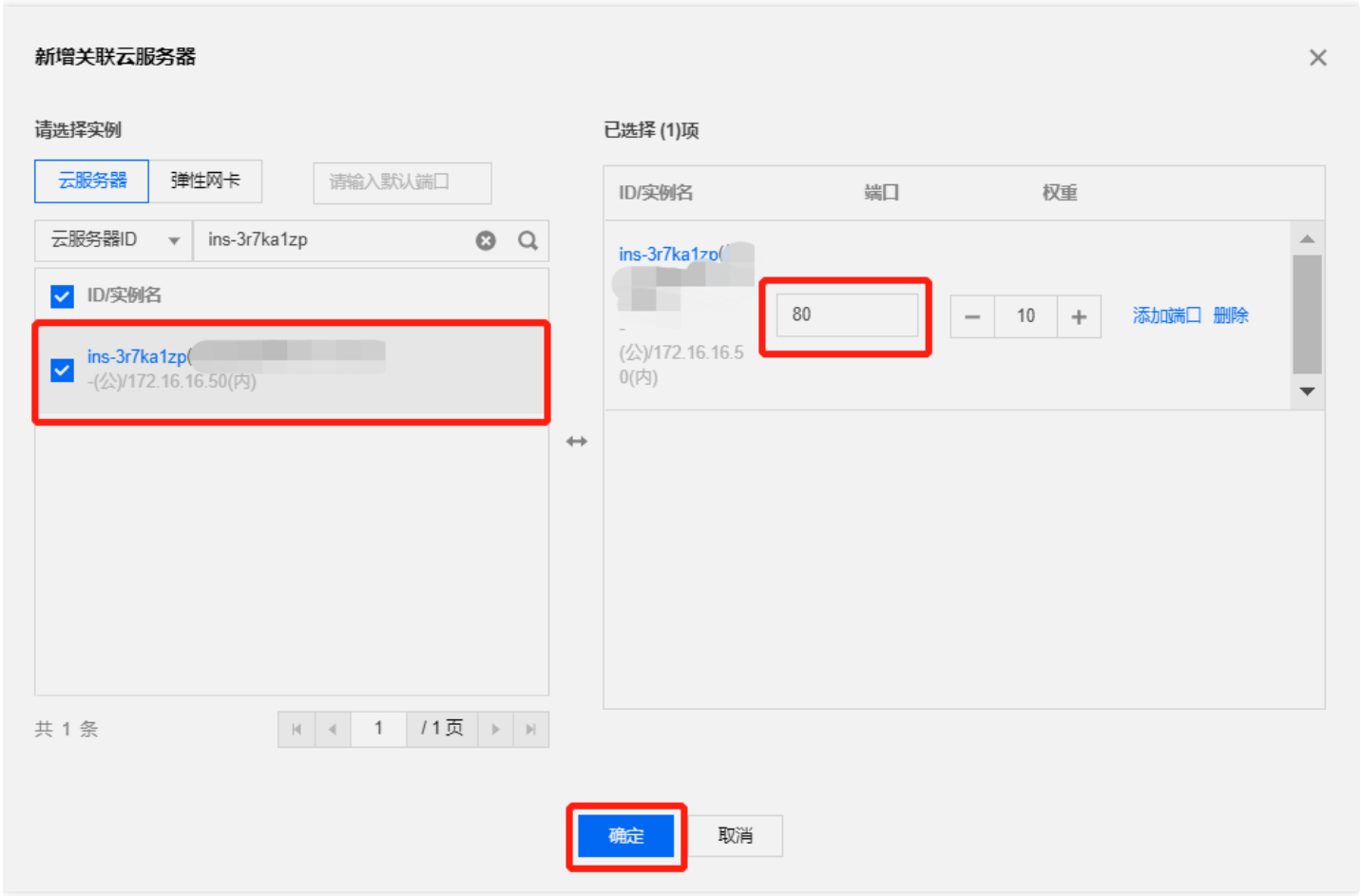


创建HTTP/HTTPS转发规则

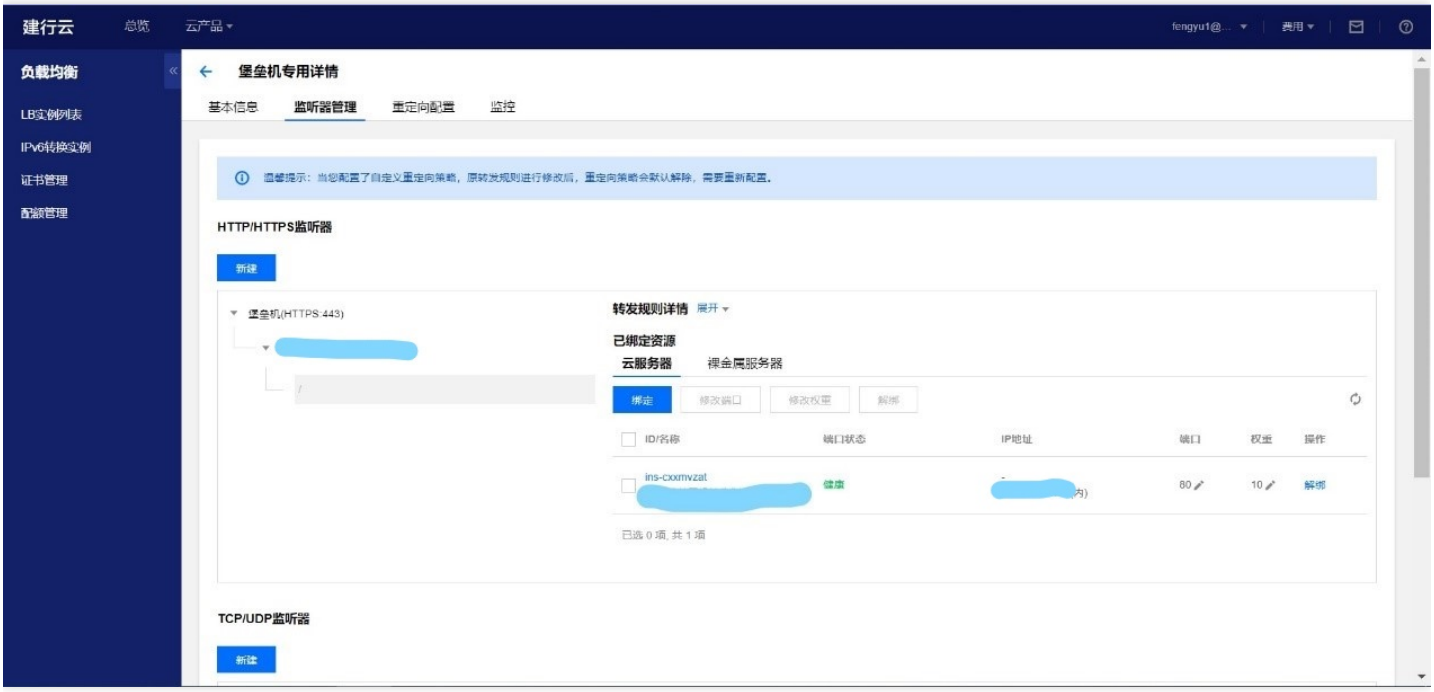

创建HTTP/HTTPS转发规则
1 基本配置
2 健康检查
3 会话保持
域名
URL路径
/
均衡方式
按权重轮询
当后端CVM的权重都设置为同一个值时，权重属性将不生效，将按照简单的轮询策略分发请求
获取客户端IP
已启用
Gzip压缩
已启用
下一步：健康检查
取消

绑定前置机的80端口

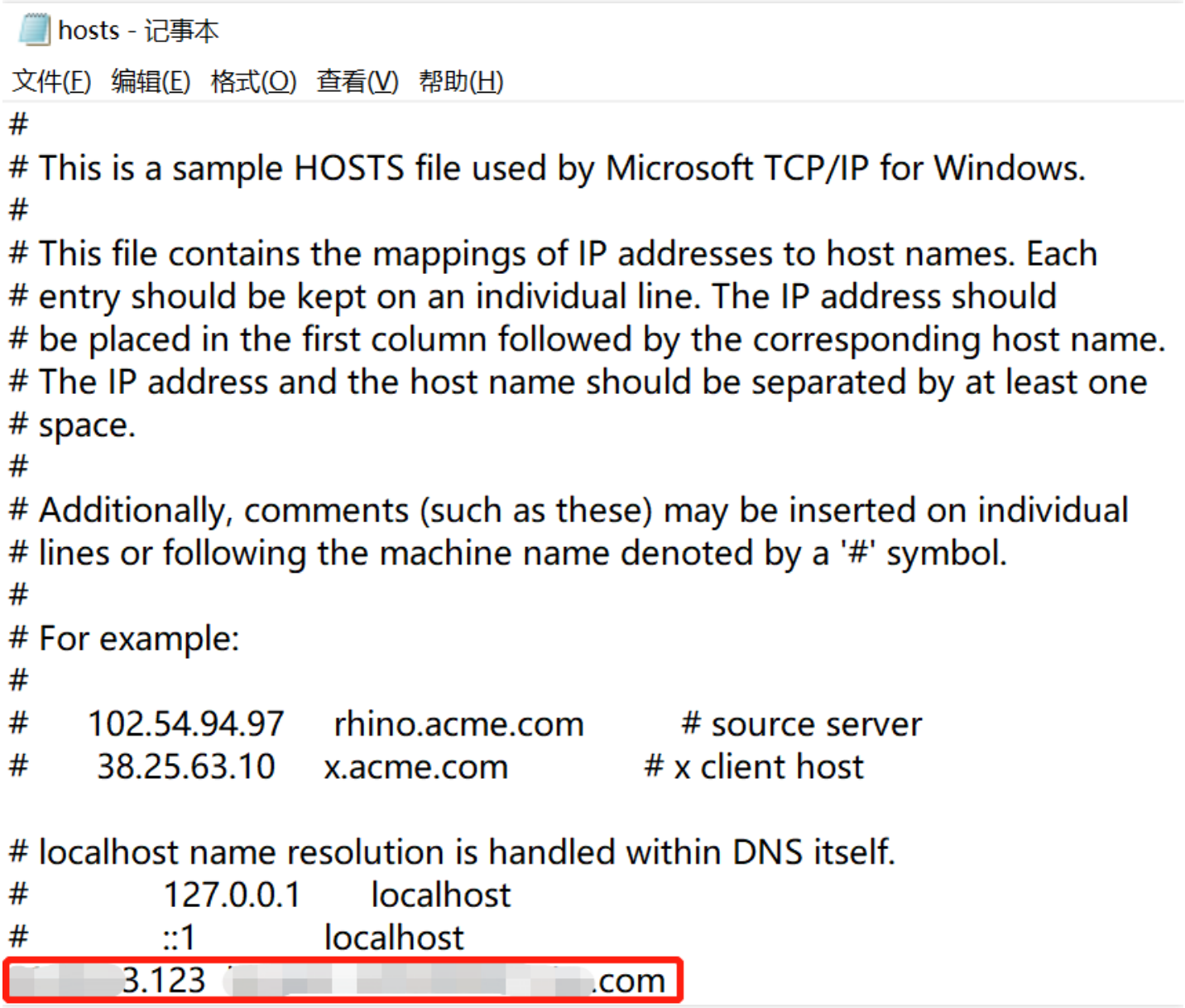

建行云
总览
云产品
负载均衡
LB实例列表
IPv6转换实例
证书管理
配额管理
堡垒机专用详情
基本信息
监听器管理
重定向配置
监控
HTTP/HTTPS监听器
新建
堡垒机(HTTPS:443)
转发规则详情
已绑定资源
云服务器
裸金属服务器
绑定
修改端口
修改权重
解绑


新增关联云服务器
请选择实例
云服务器
弹性网卡
请输入默认端口
云服务器ID
ins-3r7ka1zp
ID/实例名
ins-3r7ka1zp(
-(公)/172.16.16.50(内)
已选择 (1)项
ID/实例名
端口
权重
ins-3r7ka1zp(
80
10
添加端口
删除
(公)/172.16.16.50(内)
共 1 条
1
/ 1 页
确定
取消

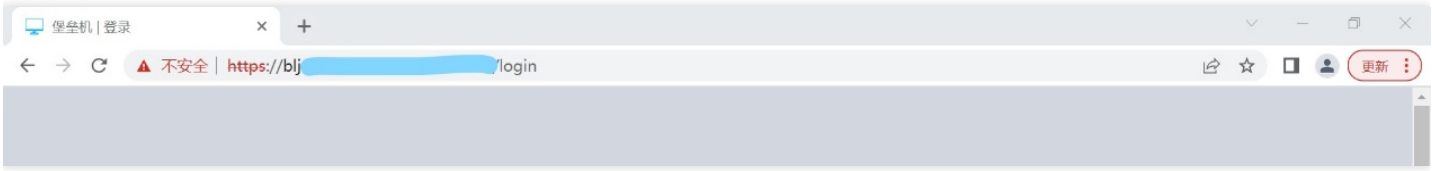
绑定成功后如下图所示


建行云
总览
云产品
负载均衡
LB实例列表
IPv6转换实例
证书管理
配额管理
堡垒机专用详情
基本信息
监听器管理
重定向配置
监控
HTTP/HTTPS监听器
新建
堡垒机(HTTPS:443)
转发规则详情
已绑定资源
云服务器
裸金属服务器
绑定
修改端口
修改权重
解绑
ID/名称
端口状态
IP地址
端口
权重
操作
TCP/UDP监听器
新建

配置本地host，在本地windows机器的hosts文件中添加配置好的域名和对应的负载均衡VIP地址，如下图中IP地址为负载均衡VIP，域名为负载均衡配置的堡垒机域名



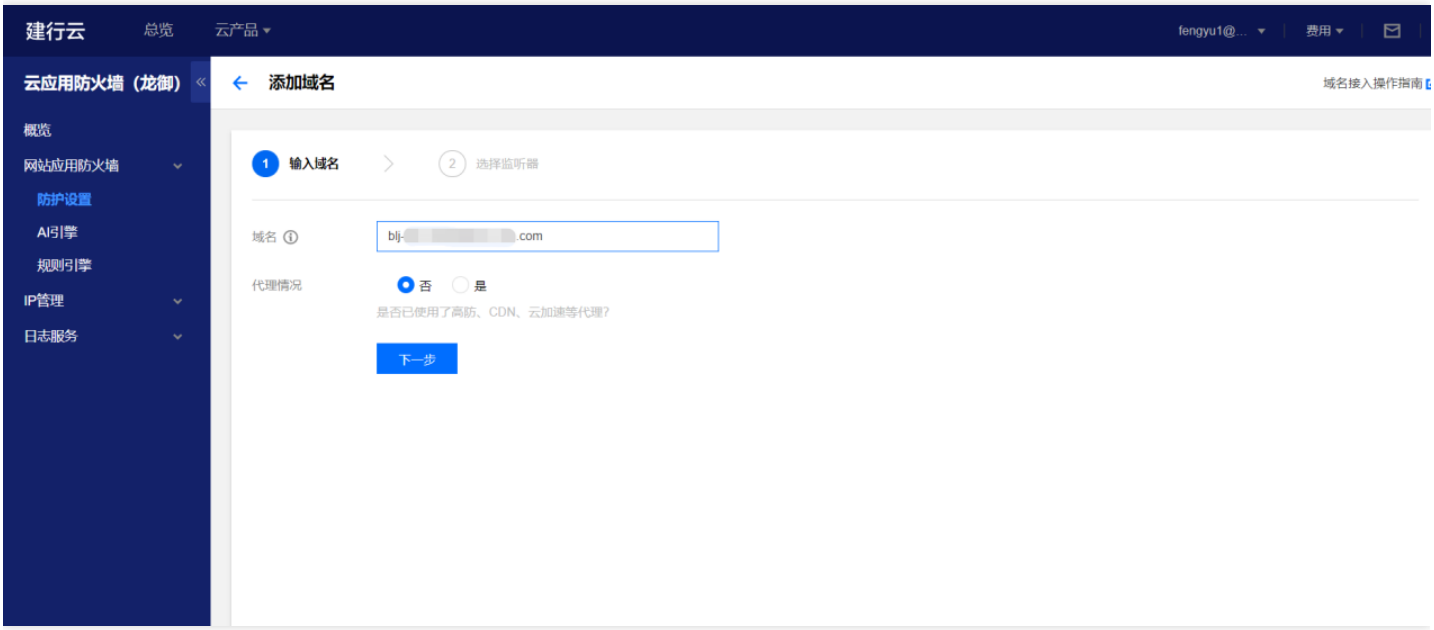
浏览器访问https://堡垒机域名:端口号，打开登录页面。



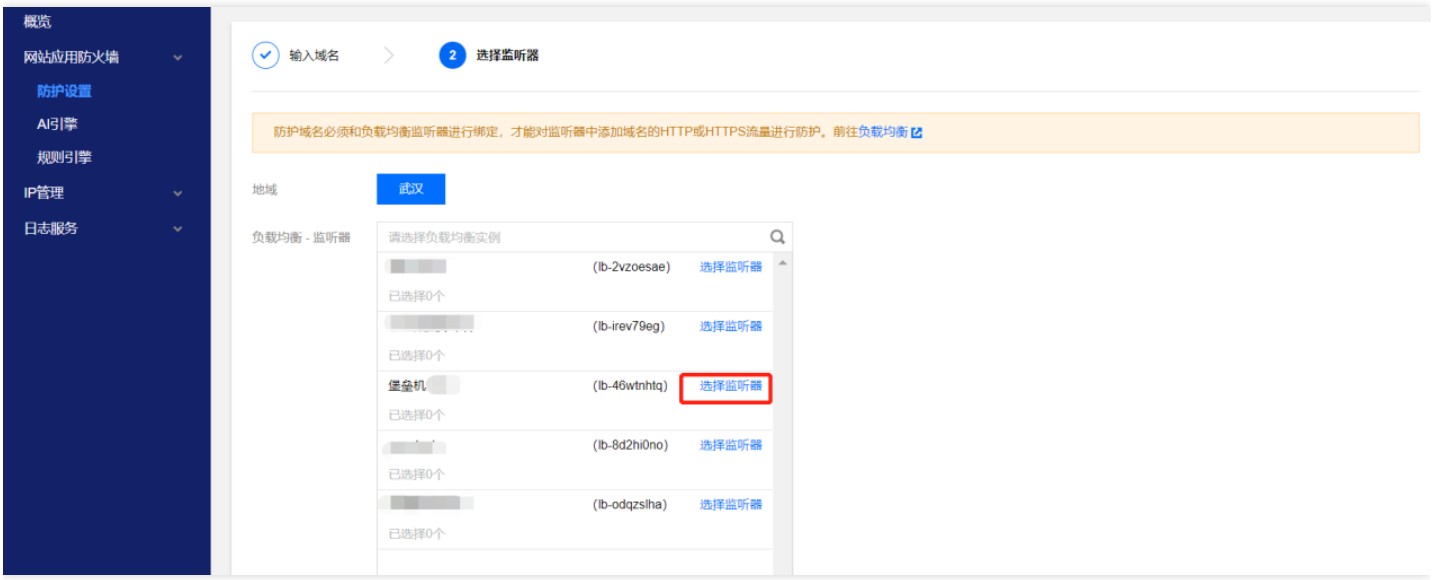
2、堡垒机域名配置WAF防护

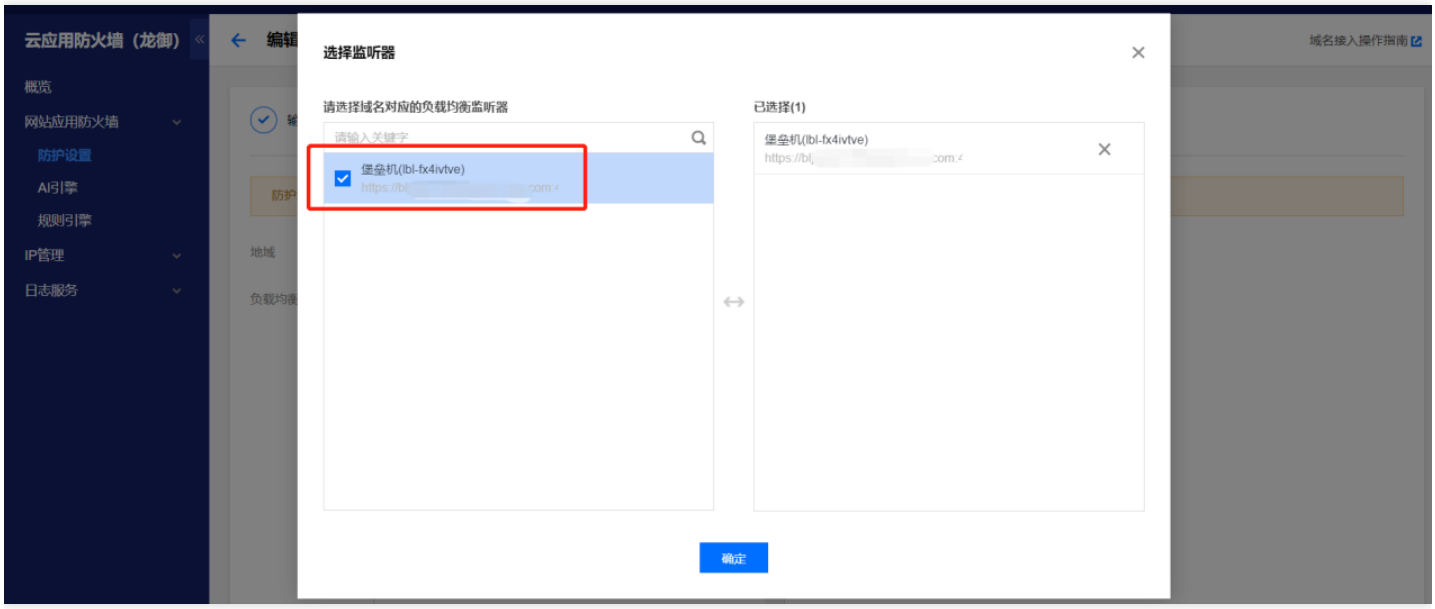

建行云
总览
云产品
云产品
使用中
全部
云计算与网络
云服务器
负载均衡
弹性伸缩
裸金属服务器
私有网络
专线接入
云数据库
云数据库Oracle版
云数据库Oracle专用版
云数据库MySQL标准版
云数据库MySQL增强版
云数据库Redis标准版
云数据库Redis增强版
智能DBA
SQL审核
存储
云硬盘
对象存储
文件存储
安全
微隔离服务
主机安全（龙卫士）
云应用防火墙（龙御）
容器安全（龙巢）
内容安全（龙鉴）
基线核查(龙检)
虚拟化入侵检测（龙防）
虚拟化漏扫(龙巡)
威胁情报

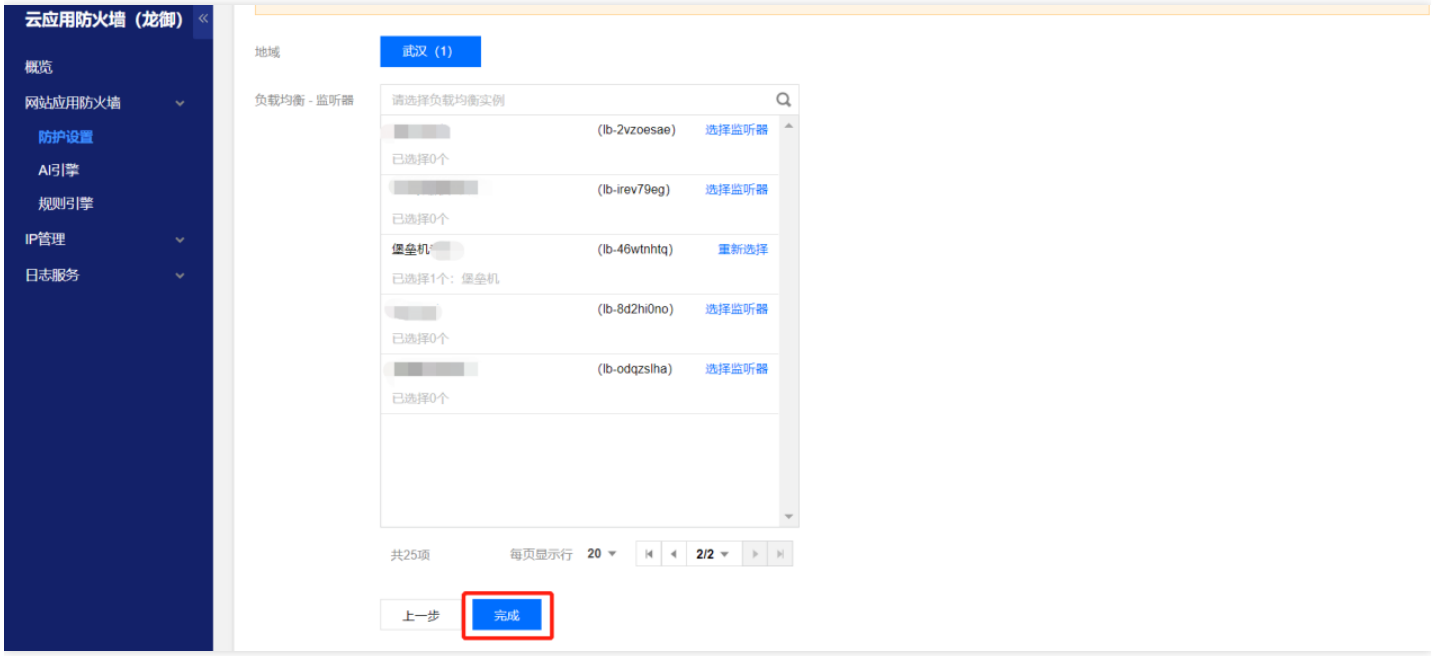

建行云
总览
云产品
fengyu1@...
费用
云应用防火墙（龙御）
概览
网站应用防火墙
防护设置
AI引擎
规则引擎
IP管理
日志服务
负载均衡型
域名接入操作指南
防护设置
域名列表
添加域名
开启
关闭
删除
支持域名、负载均衡名称、监听器名称模糊搜索
域名/ID
流量模式
区域
负载均衡（ID）
负载均衡VIP
监听器
WAF开关
操作
清洗模式
武汉
删除 编辑 防护配置
清洗模式
武汉
删除 编辑 防护配置



选择创建域名的负载均衡



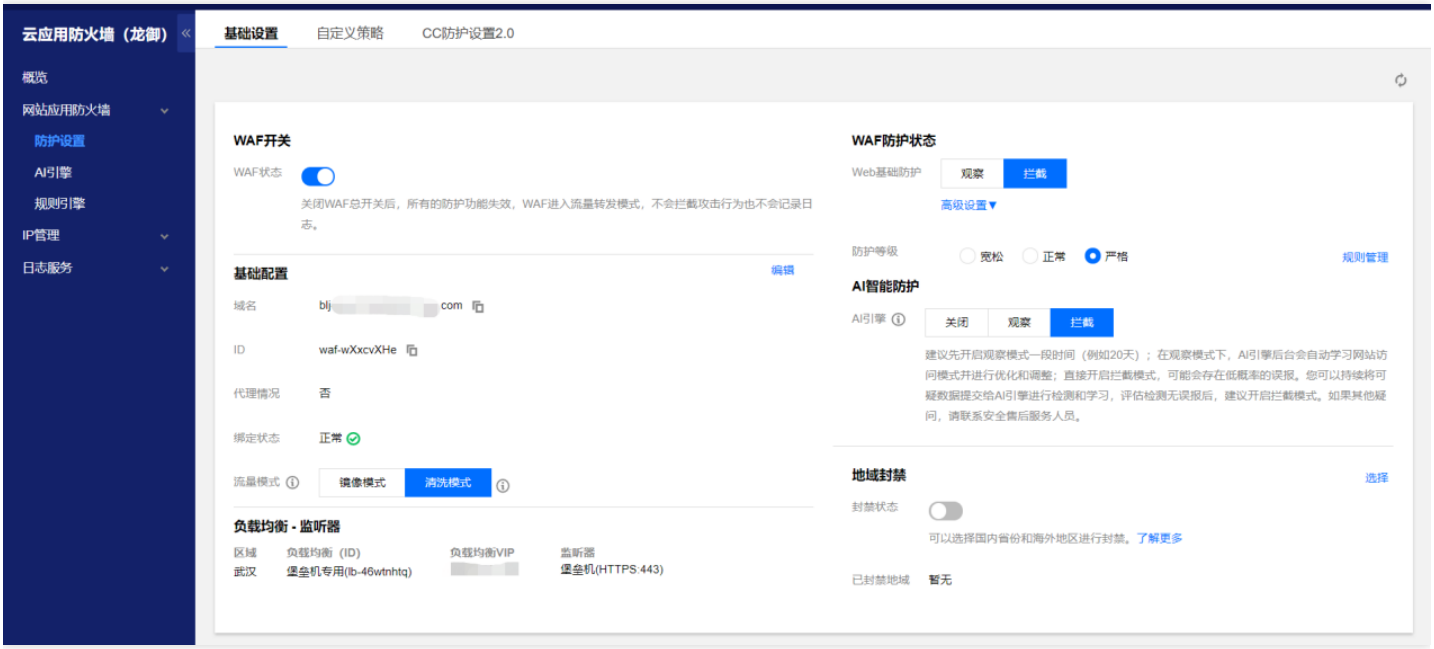

云应用防火墙（龙御）
概览
网站应用防火墙
防护设置
AI引擎
规则引擎
IP管理
日志服务
编辑
选择监听器
请选择域名对应的负载均衡监听器
请输入关键字
堡垒机(lbl-fx4ivtve)
已选择(1)
堡垒机(lbl-fx4ivtve)
确定
域名接入操作指南


云应用防火墙（龙御）
概览
网站应用防火墙
防护设置
AI引擎
规则引擎
IP管理
日志服务
地域
武汉（1）
负载均衡 - 监听器
请选择负载均衡实例
(lb-2vzoesae) 选择监听器
已选择0个
(lb-irev79eg) 选择监听器
已选择0个
堡垒机 (lb-46wtnhtq) 重新选择
已选择1个：堡垒机
(lb-8d2hi0no) 选择监听器
已选择0个
(lb-odqzslha) 选择监听器
已选择0个
共25项
每页显示行 20
2/2
上一步
完成

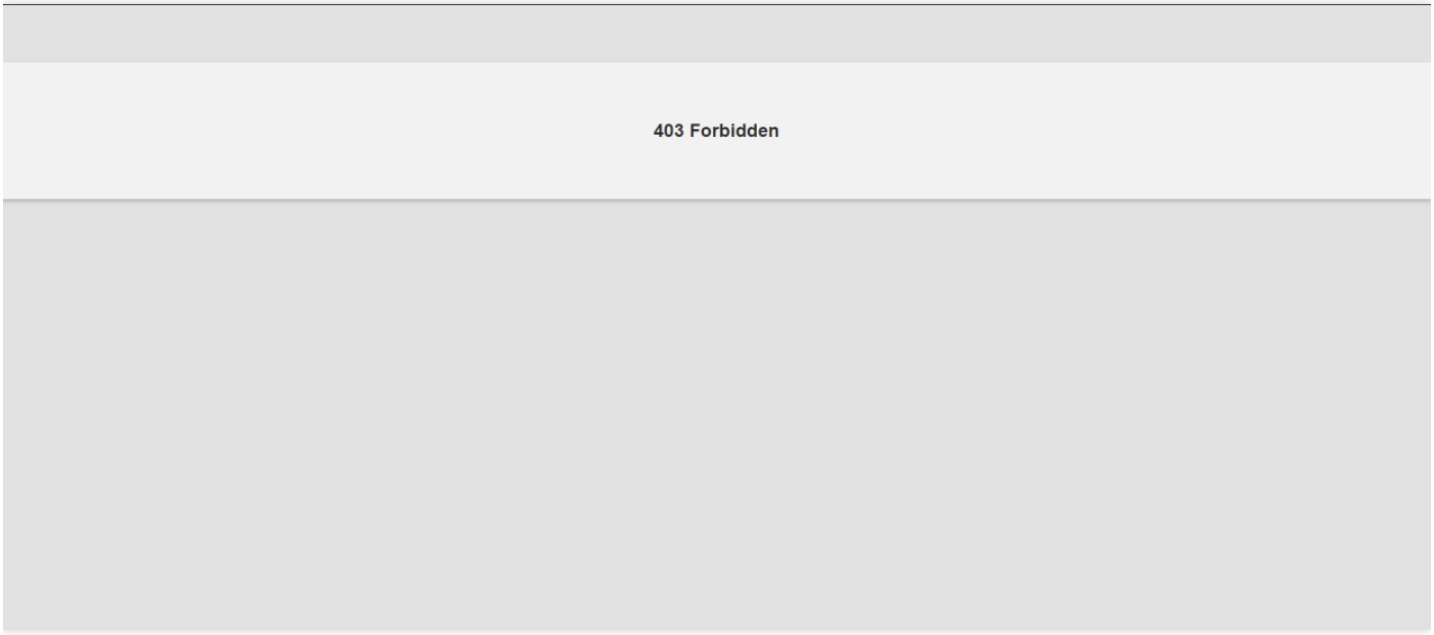
配置防护规则


建行云
总览
云产品
云应用防火墙（龙御）
概览
网站应用防火墙
防护设置
AI引擎
规则引擎
IP管理
日志服务
负载均衡型
防护设置
域名接入操作指南
域名列表
添加域名
开启
关闭
删除
堡垒机专用
域名/ID
流量模式
区域
负载均衡（ID）
负载均衡VIP
监听器
WAF开关
操作
清洗模式
武汉
堡垒机(HTTPS:443)
删除
编辑
防护配置

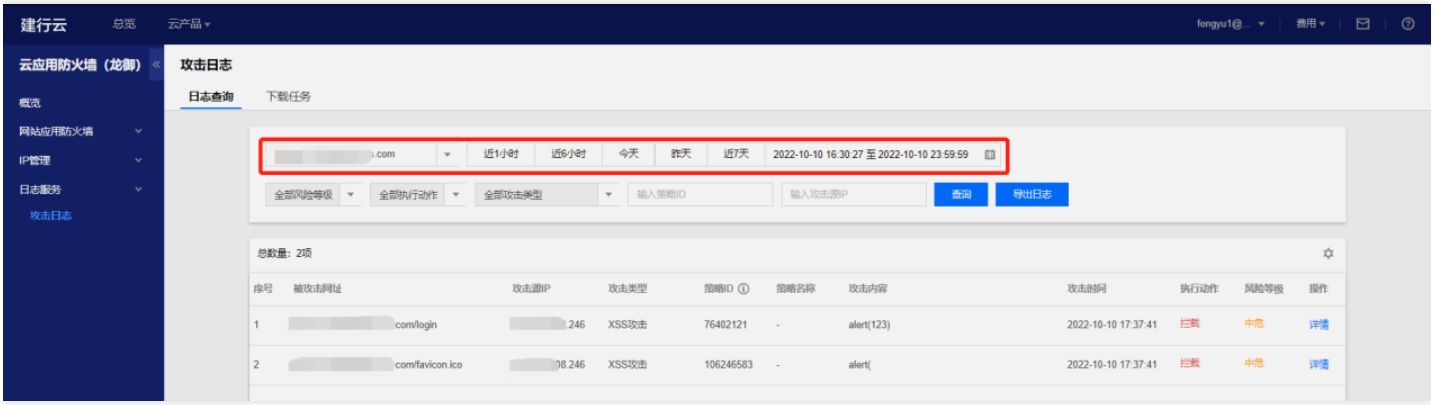
防护设置中WAF开关开启、Web基础防护为拦截、流量模式为清洗模式、AI引擎为拦截



日志查看，访问堡垒机域名返回403如下图所示则为WAF拦截



需要根据堡垒机域名和访问堡垒机域名时间查询拦截日志分析拦截原因

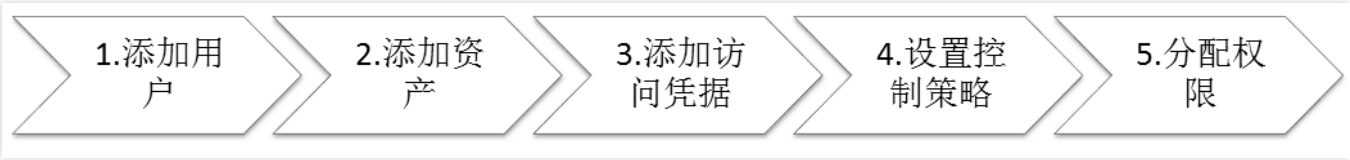


操作指南
操作说明

最近更新时间: 2019-11-27 16:44:13

1. 管理

   运维人员使用云堡垒机进行运维操作，需要管理员配置用户、设置权限后才能使用。操作主要步骤如下；



1. 添加用户

   维护配置使用云堡垒机进行操作的管理人员、运维人员；

2. 添加资产

   维护配置需要纳入云堡垒机管理的云服务器、网络设备等云资源，以IP为单位，每个IP地址为一个资产；

3. 添加访问凭据

   维护配置登录目标资产（云服务器等）使用的账户、连接方式、密码等凭据；

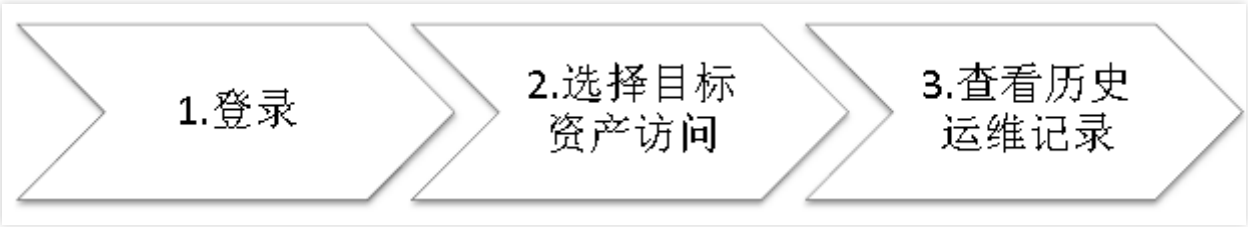
4. 设置控制策略

   维护配置登录到目标资产（云服务器等）后可使用的操作，实现基于操作命令级的操作；

5. 分配权限

   将资产、凭据、策略等权限分配给具体的运维人员；只有分配了权限后，运维人员登录后才能通过云堡垒机使用这些资产（云服务器等）。

2. 运维



1. 登录

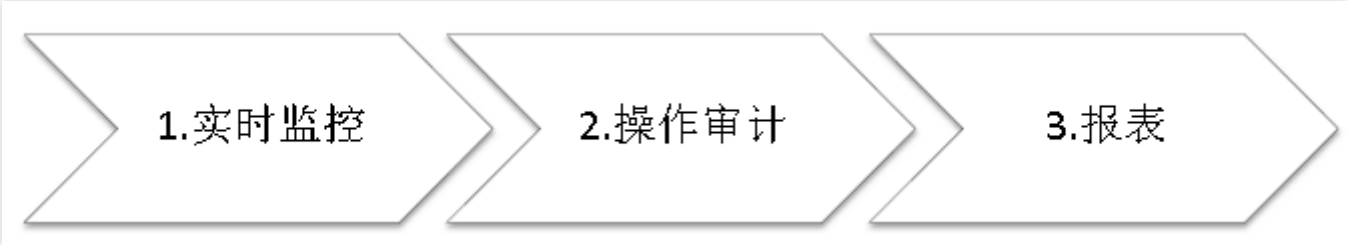
   以运维人员身份登录后，显示该运维人员可访问的资产列表；

2. 选择目标资产访问

   选择需要维护的目标资产（云服务器等）打开，并选择本次操作使用的访问凭据（账户等）进行登录；

3. 查看历史运维记录
   查看运维人员自身历史运维记录。

3. 审计



1. 实时监控
   对在线运维人员操作，实时监控同步显示运维人员操作过程；
2. 操作审计
   事中事后对用户所有操作进行审计，重现当时操作过程；
3. 报表
   运维人员登录访问情况、权限配置权限等形成统计分析报表，及时掌握系统运行情况。

功能界面展示如下

登录

最近更新时间: 2023-01-11 14:04:44

用户通过自己配置的堡垒机域名，在浏览器中直接访问“https://堡垒机域名:端口号”登录。

首次登录请联系我们获取默认管理员及密码，登录后请及时修改密码。

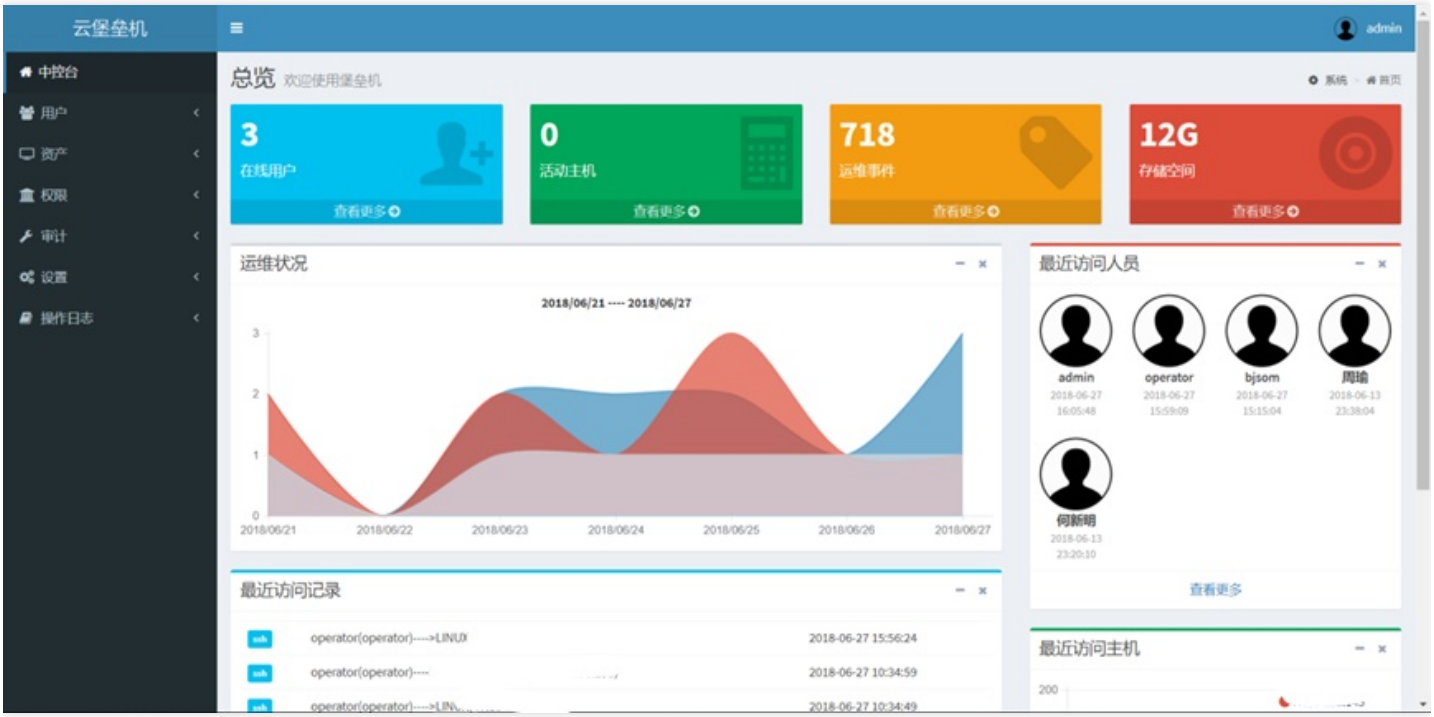
管理员登录后，可以新增其他管理员和运维用户。

用户

用户

最近更新时间: 2023-02-08 11:41:15

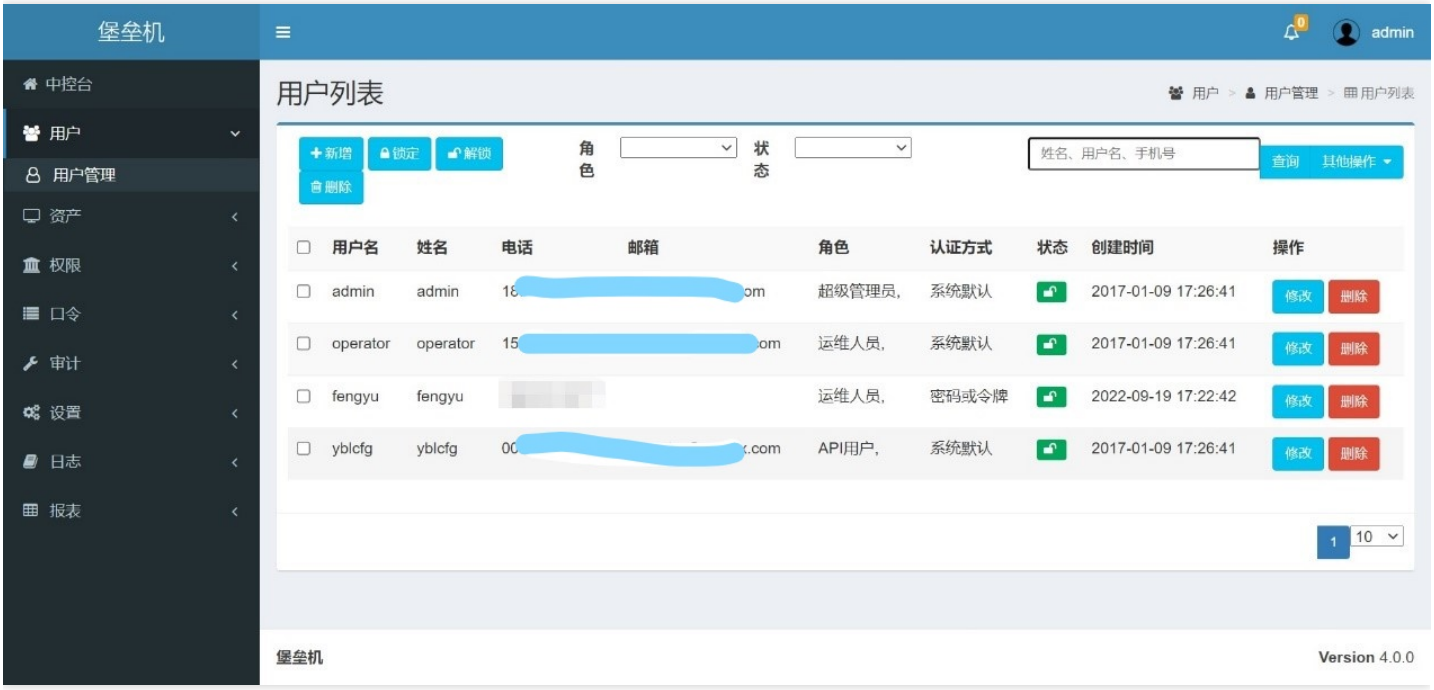
管理员登录后，首页是管理员的中控台，显示云堡垒机当前状态，包括在线用户、资源使用情况、以及运维相关的各种统计图表等。



用户管理

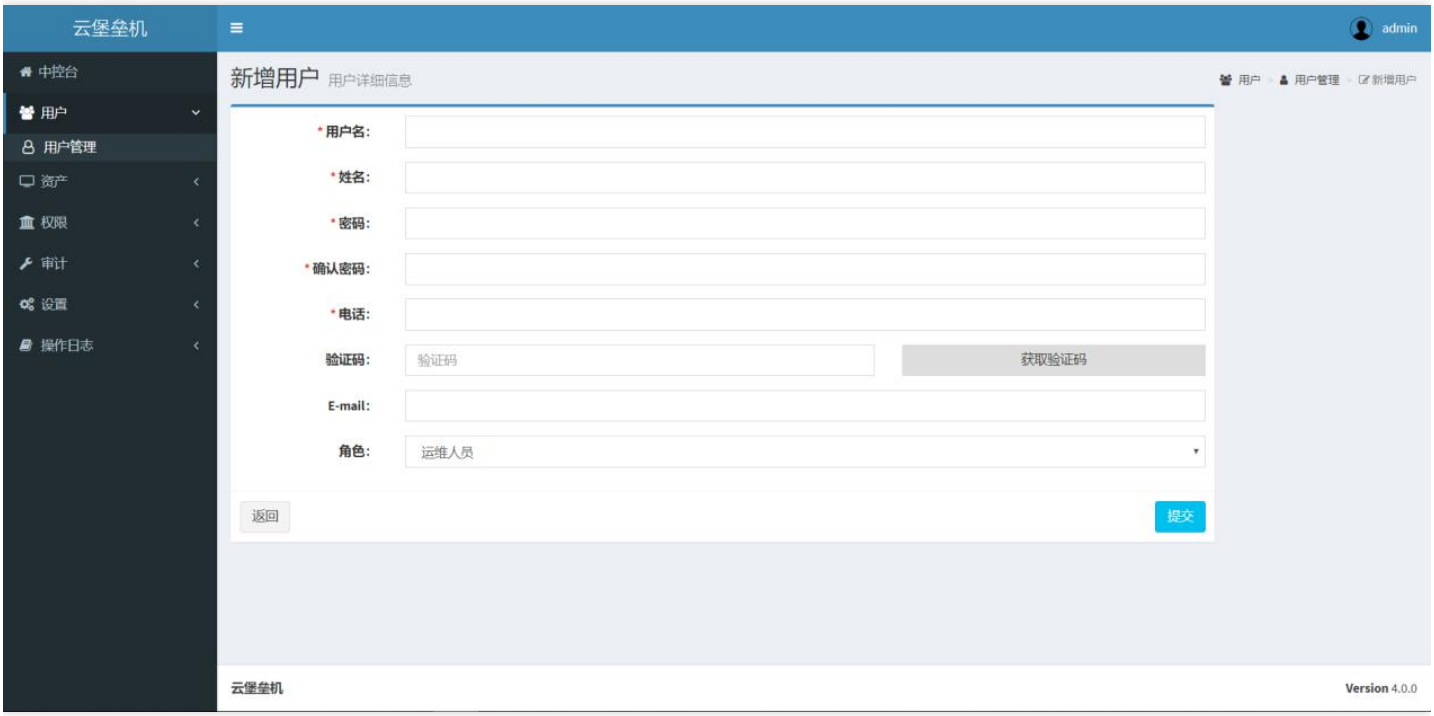
最近更新时间: 2023-02-08 11:41:14

点击主菜单“用户”>“用户管理”，打开用户管理页面，如下图所示：

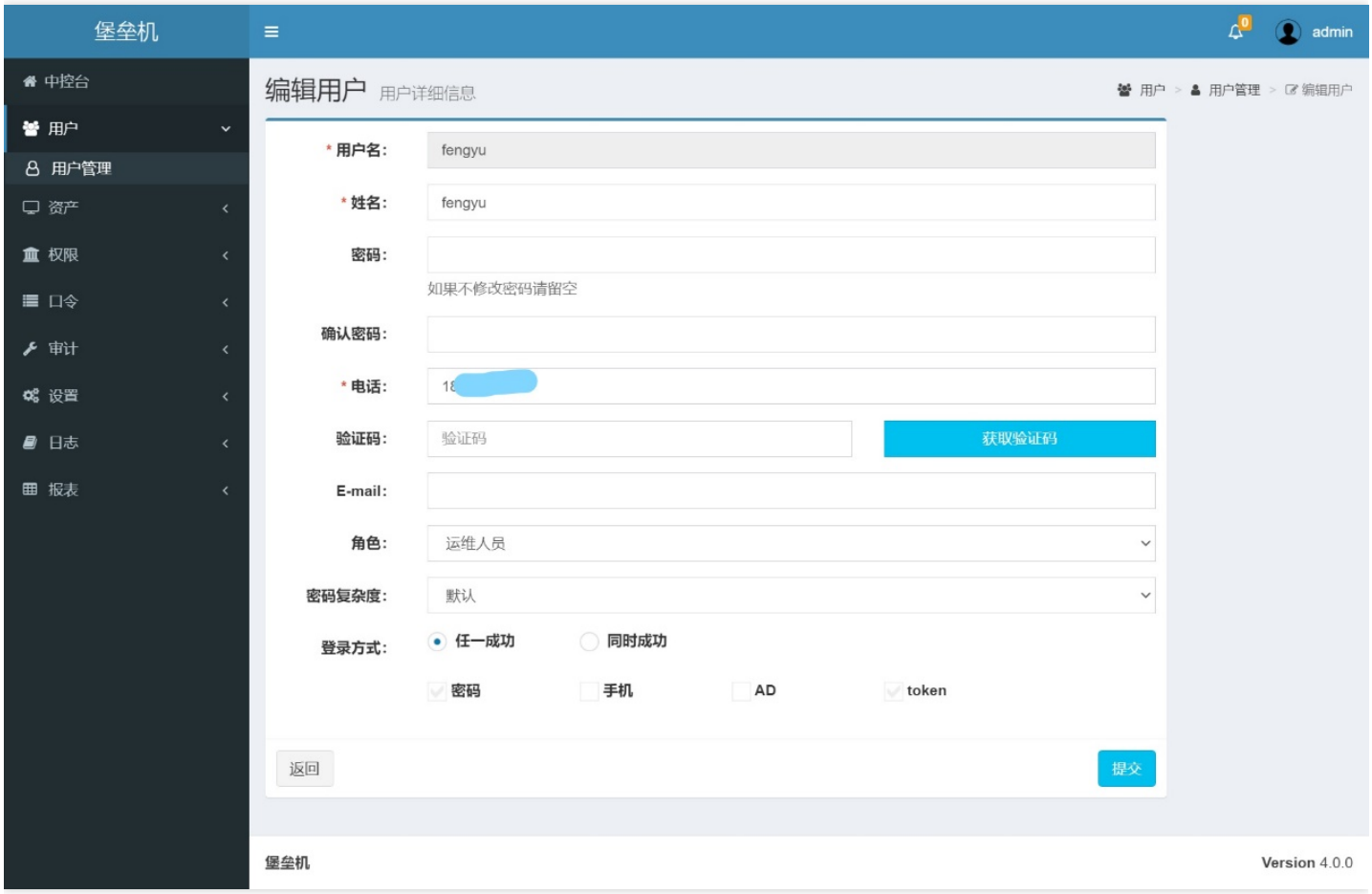


点击下方的“新增”、“锁定”、“解锁”、“删除”，对进行增删查改操作。

- 新增用用户
  对使用云堡垒机的用户身份进行管理，实现增加、删除、锁定和解锁用户等，以及按用户身份分配访问权限等。参数说明如下：
- 用户名：用户用于登录到系统的用户标识；
- 姓名： 用户的真实姓名；
- 密码： 用户登录系统时所用的密码；
- 确认密码： 再次输入密码；
- 电话： 用户的电话，用于验证用户；
- 验证码： 短信发送到用户的手机；
- E-mail： 用户的Email，可为空；
- 角色： 用户的角色，决定用户的基础权限，分为运维人员、超级管理员、审计员、特权审计员、口令管理员、开发人员、API用户。系统管理员：能管理所有的系统信息，运维人员和开发人员：只具有运维服务器的功能。审计员：只能实时监控审计以及查询统计报表操作。特权审计员：只能实时监控审计以及查询统计报表操作，并在操作录像中查看执行的命令。口令管理员：只能对设备口令及访问凭据进行管理与维护，同时还可以进行与访问凭据相关的查询统计操作。API用户：未使用系统保留。

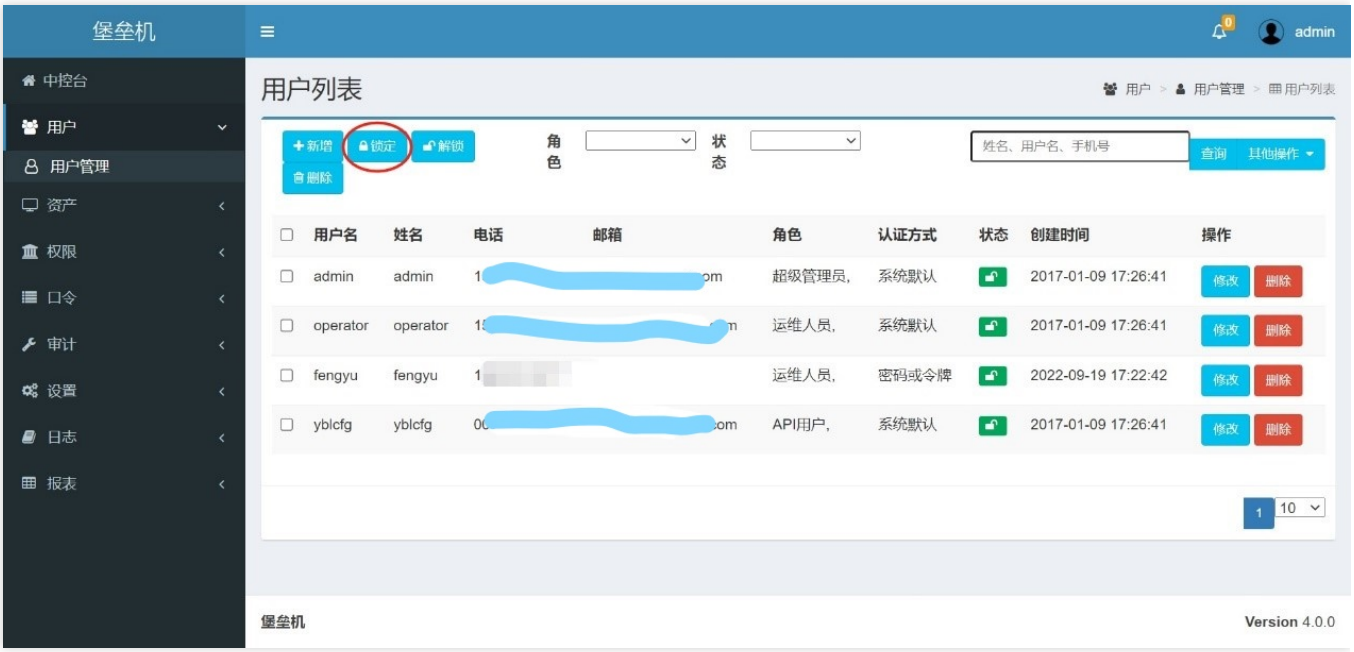


- 修改用户 点击需要修改信息用户所在行的“修改”按钮，跳转到修改页面：



- 锁定和解锁 锁定用户是指将用户的状态变为锁定，使之无法登录，也不能使用。锁定用户可通过如下的方式：

  一：勾选需要锁定的用户后点击上方按钮组的“锁定”按钮，并在弹出的对话框中选择“确定”，即可锁定一组用户。勾选后点击“解锁”即可解锁一组用户。如下图所示：



【注意】锁定用户后，用户无法登录系统。

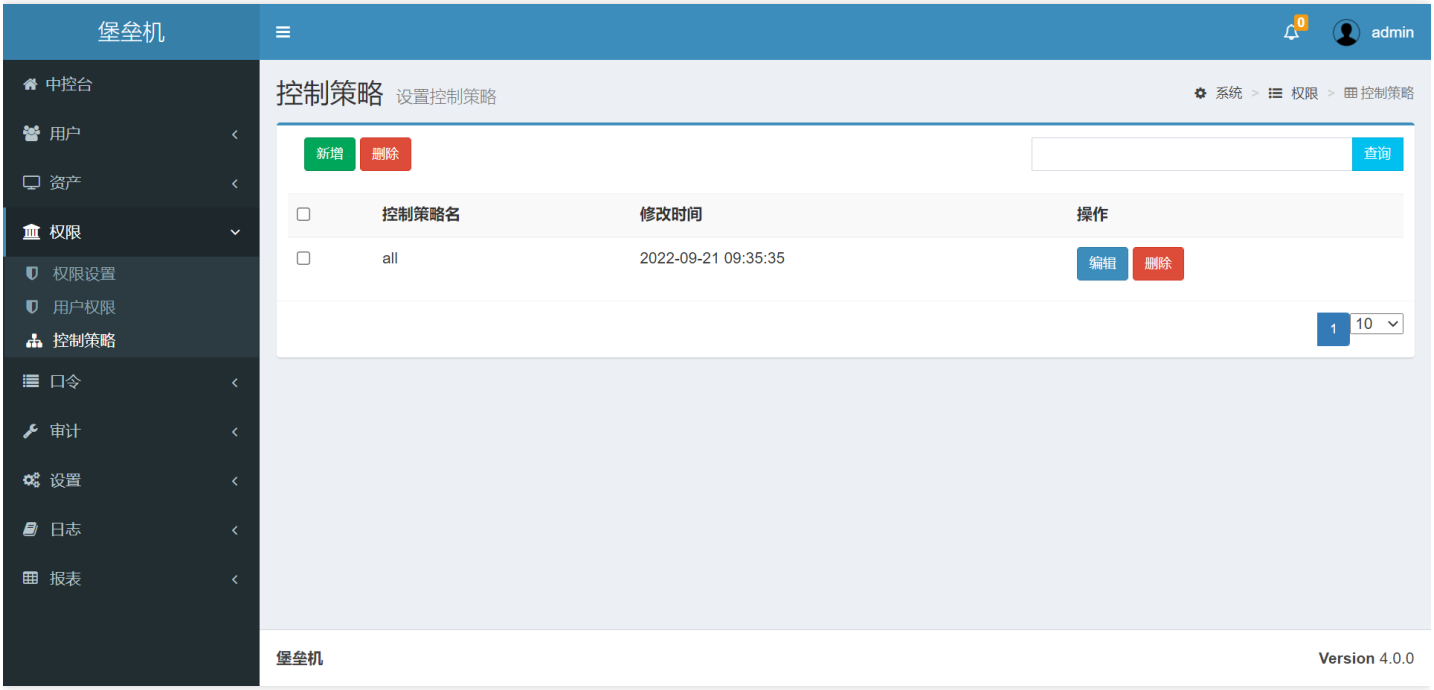
权限中重新添加该用户时，无法找到该用户。

二：点击的用户中状态栏的锁图标，即可变更用户的状态。如果是未锁定的用户，点击后将会变为已锁定状态；如果是已锁定的用户，点击后将会变为为锁定的状态。

权限
控制策略

最近更新时间: 2023-02-08 13:49:47

控制策略，实现对用户连接目标服务器的操作行为进行精细控制，包括控制用户的IP范围、可访问的时间段、协议、禁止执行的命令、上传下载文件的权限等。 对控制策略进行配置管理，实现添加、删除等操作。需要在配置权限设置前设置，否则无法在权限设置中进行控制策略设置。
通过“权限”->“控制策略”来进入控制策略管理页面:



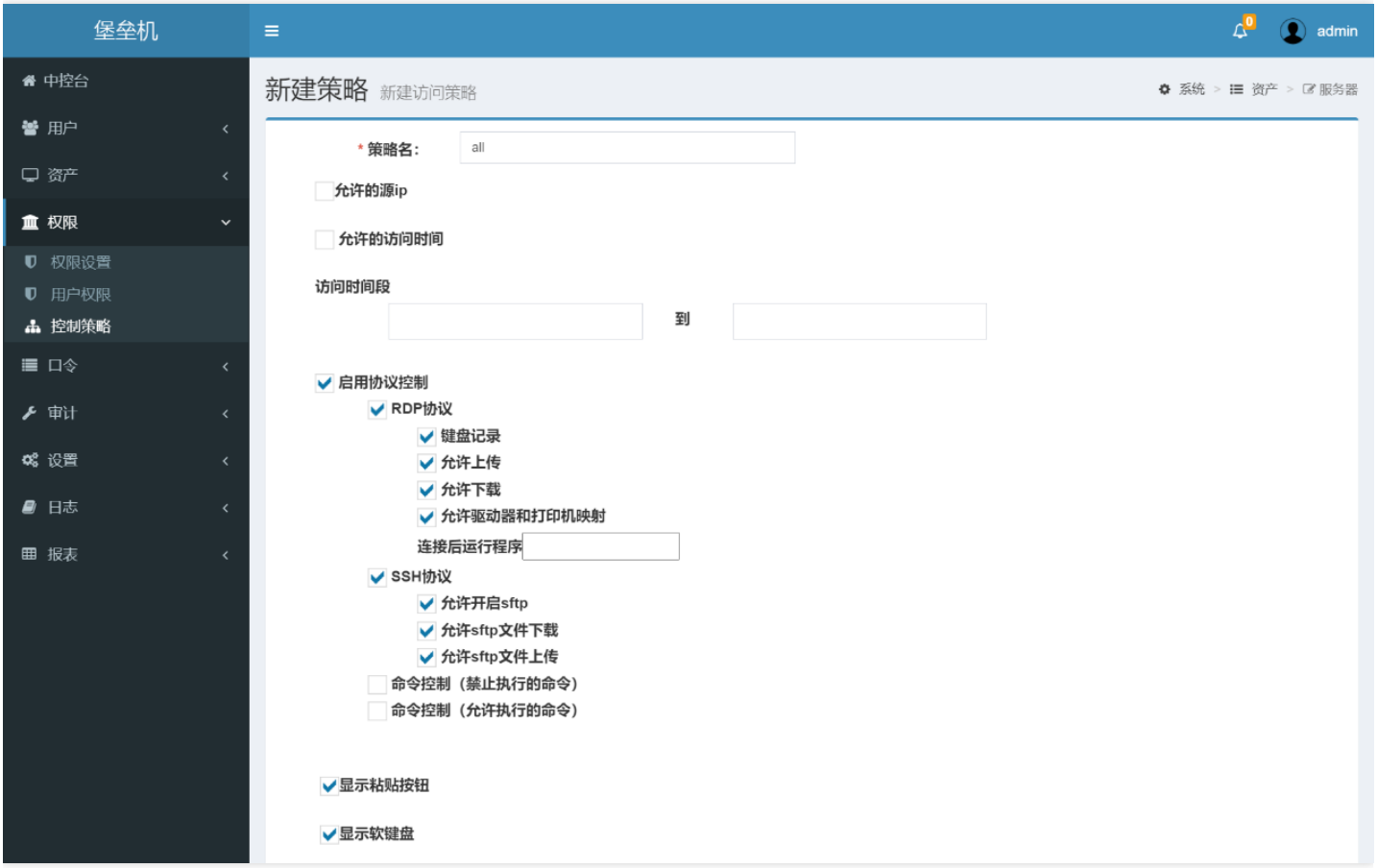
- 新增控制策略 点击左上按钮区域的“新增”按钮，进入新增控制策略页面，以下是对具体参数的说明：
  - 允许的源IP：用户登录进入时允许的ip地址，如果不符合将无法登录。
  - 允许的访问时间：用户允许登录进入的时间，可以按照工作日和时间来进行限定。
  - 启用协议控制：对用户的操作进行限制；勾选后以下选项才会出现 RDP协议 面向目标服务器为windows操作系统。其中：
    键盘记录

目标服务器连接以后，记录所有的键盘操作 允许上传 允许客户端上传文件到目标服务器(windows操作系统)。此项不选不能上传文件 允许下载 允许客户端从目标服务器(windows操作系统)上下载文件。此项不选不能上传文件 允许驱动器和打印机映射 要上传和下载文件到windows服务器，必须选定此选项。 连接后运行程序 连接后运行的程序绝对路径 SSH协议 面向目标服务器为linux操作系统。其中： 允许开启sftp 允许开启sftp协议。此处不勾选表示未开启sftp，无法上传和下载 允许sftp文件下载 允许从目标服务器(linux操作系统)下载文件到客户端。

此选项不勾选，在连接到目标终端后界面上不显示下载链接。 □ 允许sftp文件上传 允许客户端向目标服务器(linux操作系统)上传文件。此选项不勾选，在连接到目标终端后界面上不显示上传链接。

命令控制 此处输入禁止连接到客户端时执行的命令。多个命令通过“换行”区分。 选择合适的参数后，点击确定即可新增。 □ 显示粘贴按钮：登录服务器显示粘贴按钮 □ 显示软键盘：登录服务器显示软键盘

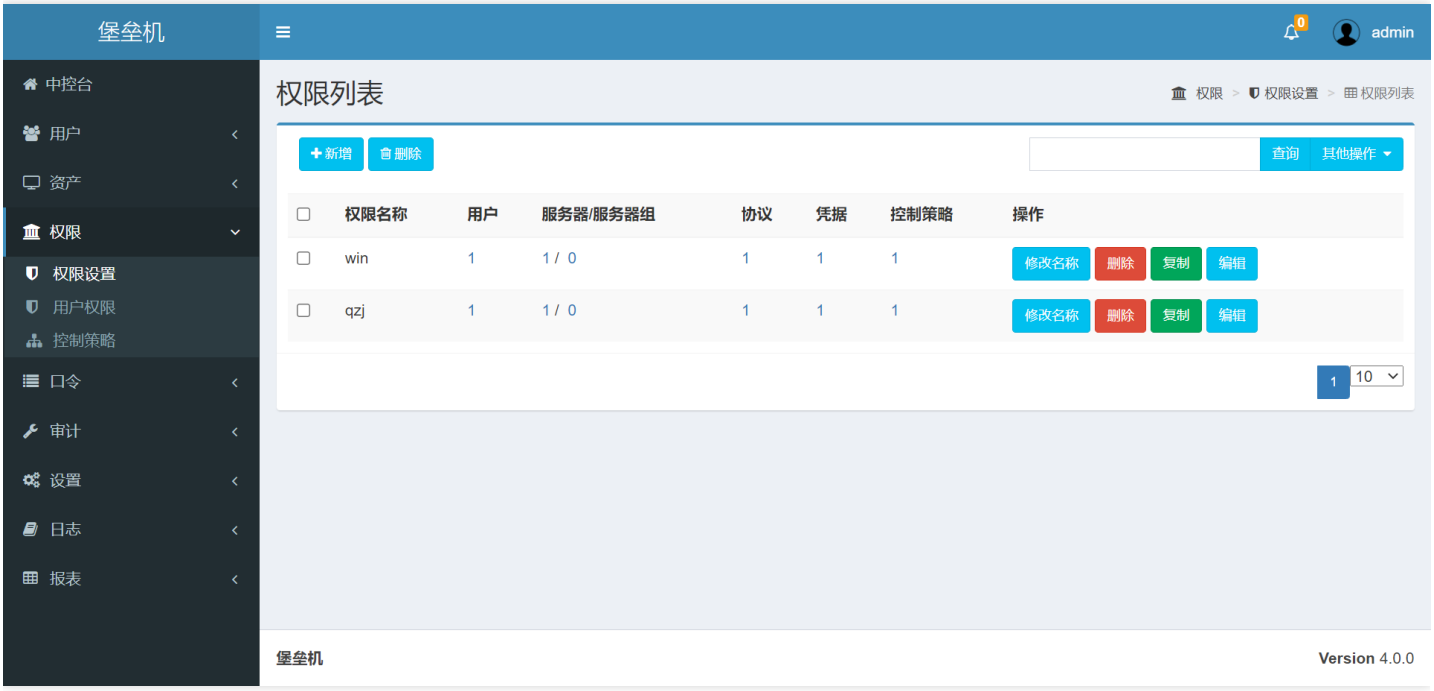
 编辑控制策略 编辑控制策略可以进入编辑界面，重新设置控制策略的属性值：



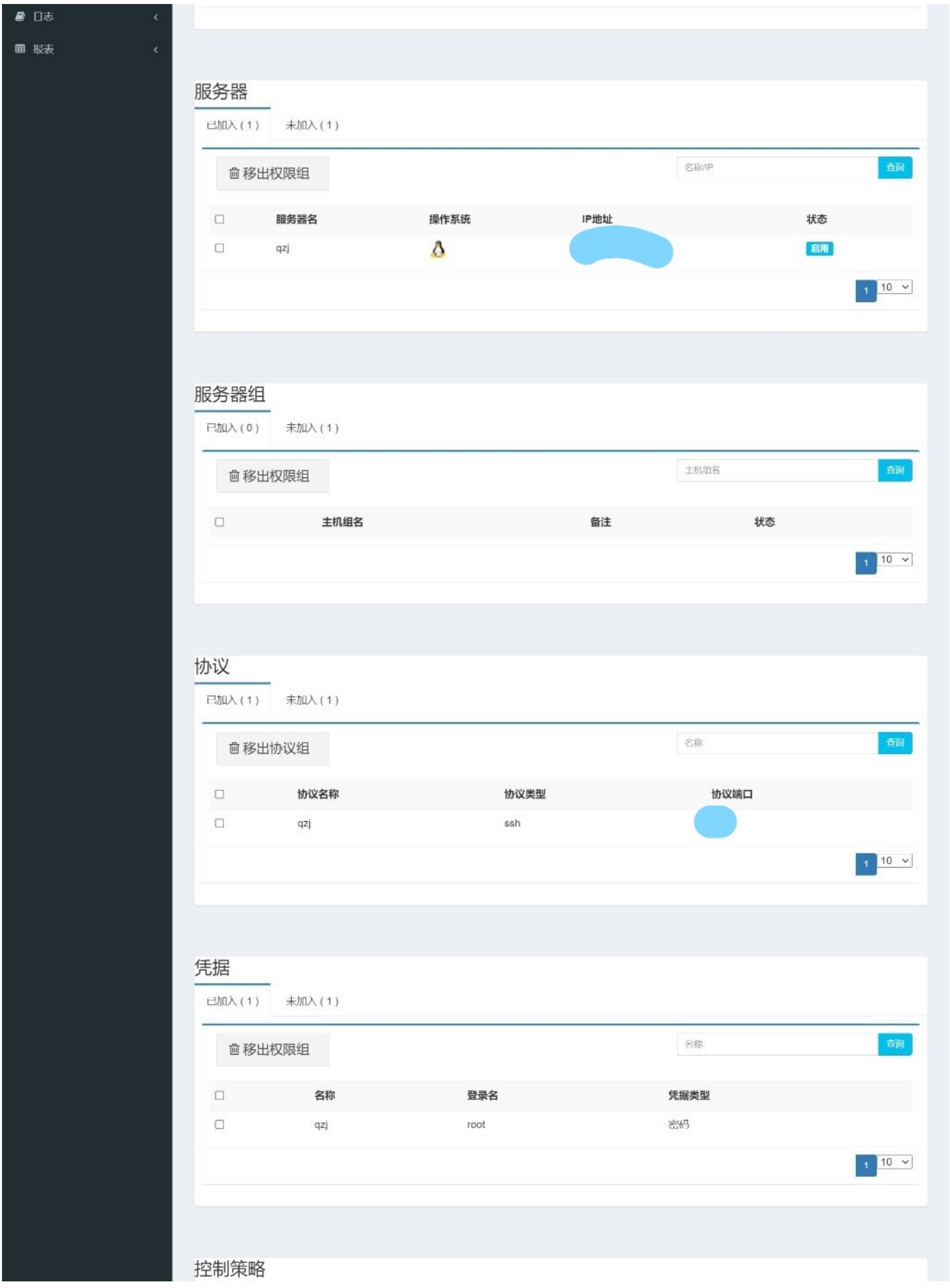
权限设置

最近更新时间: 2023-02-08 13:49:47

将权限分配给运维人员，设置运维人员允许访问的目标服务器（或组）、使用的凭据、控制策略等。 运维人员只有在分配了权限后，才能使用云堡垒机登录目标服务器进行操作。 通过“权限”->“权限设置”来进入控制策略管理页面:



 新增权限 点击上方按钮组的新增按钮，在弹出的对话框中输入权限的名称，即可创建一个新的权限。 对表格的说明： 权限名称： 权限的独立标识。 用户： 指定了该权限的用户。 服务器/服务器组： 该权限允许远程运维的服务器/服务器组。 凭据： 用户远程访问时使用的凭据。 控制策略： 用户访问时的限定行为。 通过点击对应列的数字可以增添或移除对应的项。


日志
报表
服务器
已加入 (1)
未加入 (1)
移出权限组
名称/IP
查询
服务器名
操作系统
IP地址
状态
qzj
启用
1
10
服务器组
已加入 (0)
未加入 (1)
移出权限组
主机组名
查询
主机组名
备注
状态
1
10
协议
已加入 (1)
未加入 (1)
移出协议组
名称
查询
协议名称
协议类型
协议端口
qzj
ssh
1
10
凭据
已加入 (1)
未加入 (1)
移出权限组
名称
查询
名称
登录名
凭据类型
qzj
root
密码
1
10
控制策略

- 修改权限名称
  点击对应权限的“修改名称”按钮，在弹出的对话框中输入修改后的名称即可修改权限的名称；
- 删除权限
  点击对应权限所在行的“删除”按钮，在弹出的对话框中选择确定删除的权限记录。
- 复制权限
  复制功能用于复制一份权限的配置，用于简化用户的新增操作。点击对应权限所在行的“复制”按钮，再弹出的对话框中输入复制后的名称即可新增一条具有相同配置，但是名称不同的记录。

用户权限

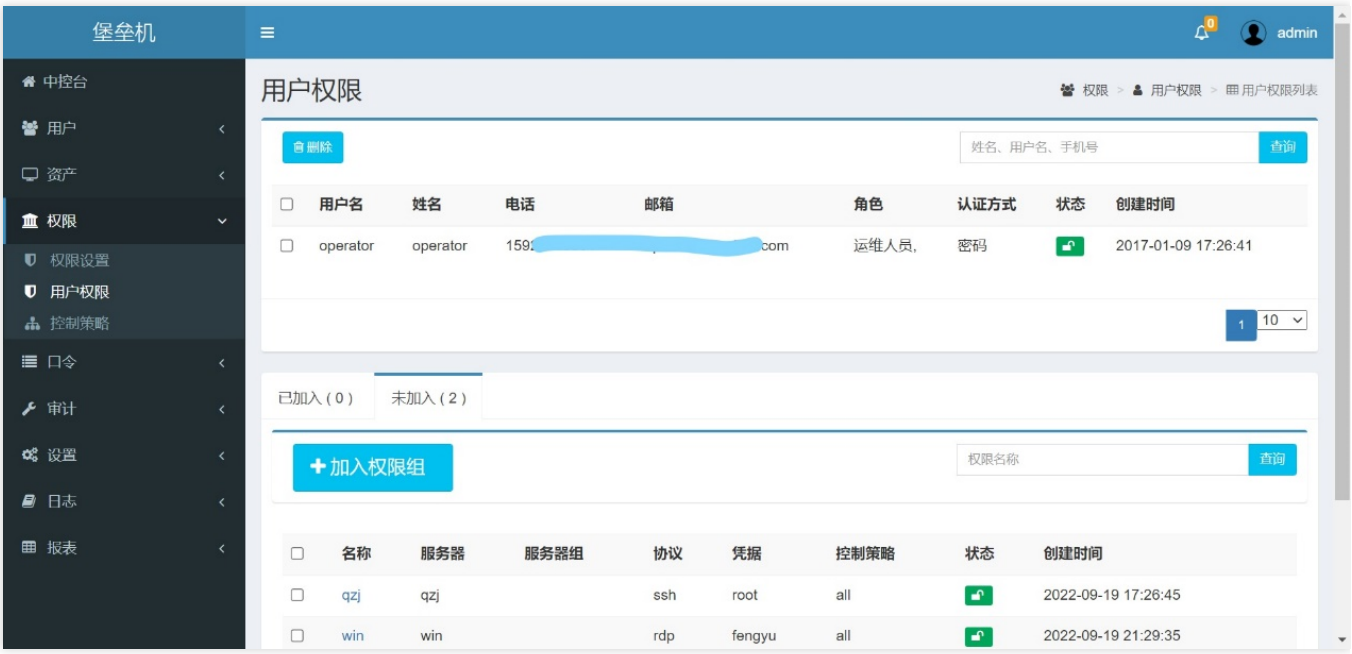
最近更新时间: 2023-02-08 13:49:47

用户权限对用户所能访问的服务器、控制策略进行管理，可以新增、查询和修改权限。 通过“权限”->“用户权限”菜单即可进入用户权限界面，如下图所示：

- 新增用户权限

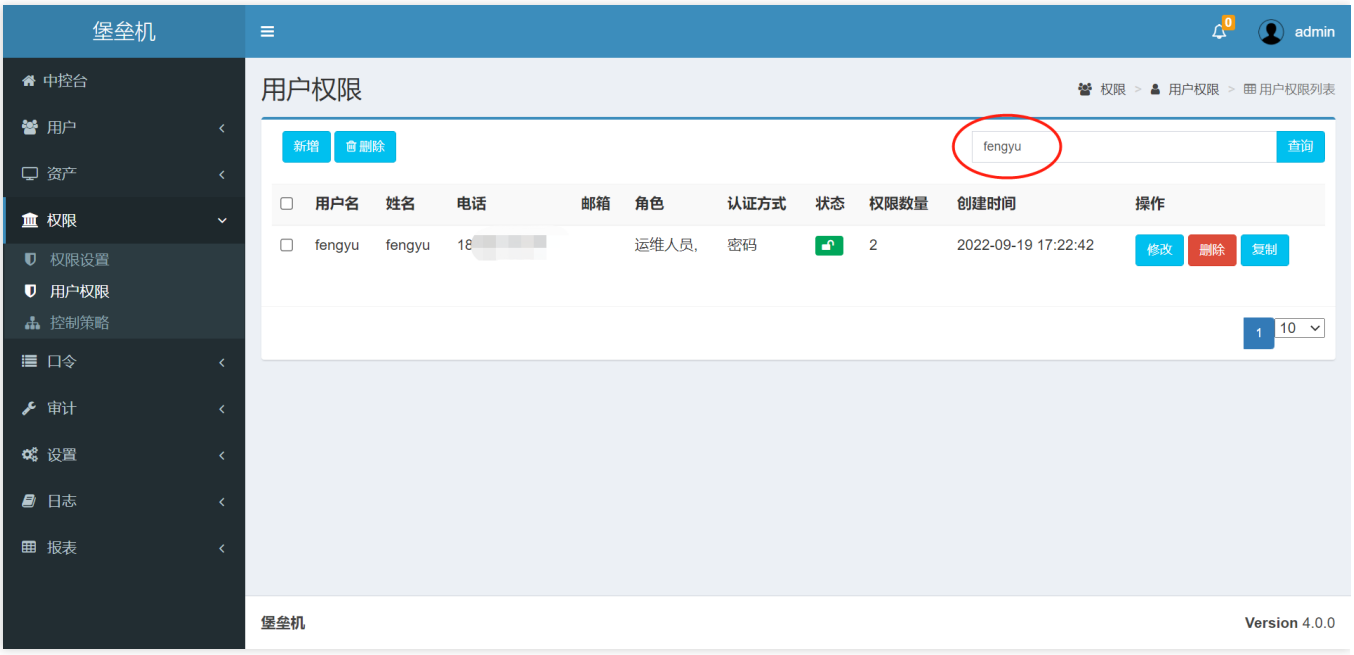
  点击左上角的“新增”按钮，进行新增用户权限功能，在未加入选择要管理的服务器，加入权限组。如下图，

所示：



- 查询用户权限

  在右上角输入姓名、用户名、手机号，点击查询，可以对用户权限进行查询。如下图所示：



- 修改用户权限

  点击权限旁边的“修改”按钮，可以对用户权限进行修改，移除或者加入。如下图所示：

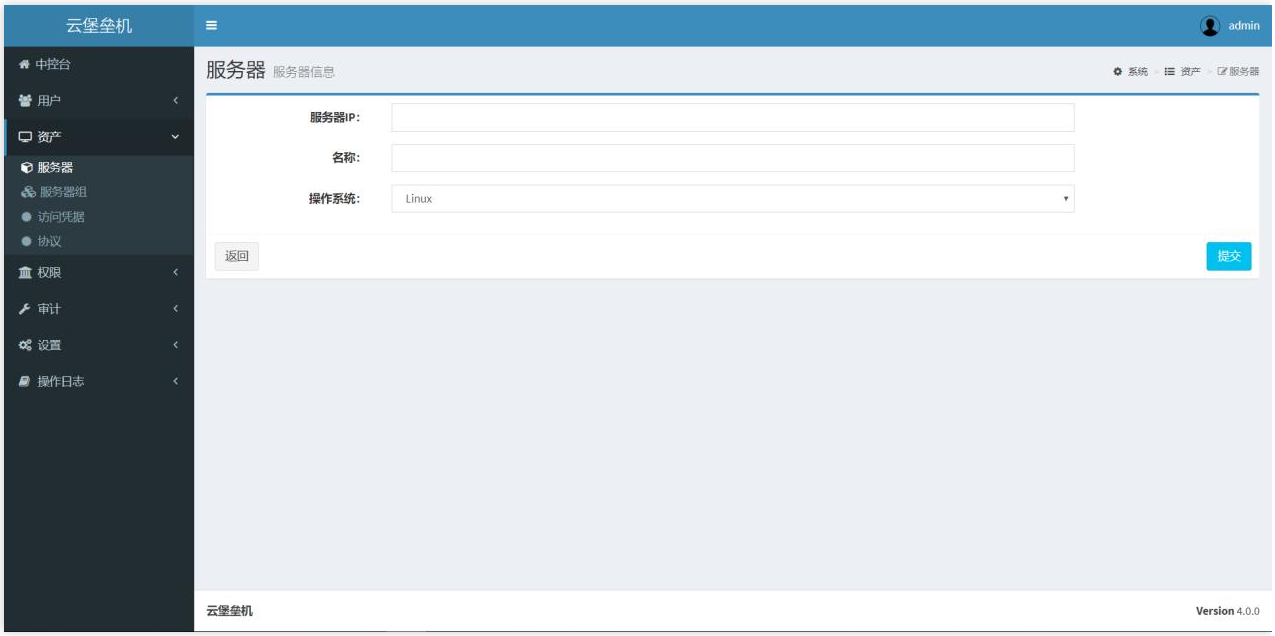

堡垒机
admin
中控台
用户
资产
权限
权限设置
用户权限
控制策略
口令
审计
设置
日志
报表
fengyu:用户
权限 > 用户权限 > 用户权限列表
已加入 (2)
未加入 (0)
移出权限
权限名
查询
名称 服务器 服务器组 协议 凭据 控制策略 创建时间
qzj qzj ssh root all 2022-09-19 17:26:45
win win rdp fengyu all 2022-09-19 21:29:35
返回
1
10
堡垒机
Version 4.0.0

资产
服务器管理

最近更新时间: 2023-02-08 11:41:14

服务器即能通过云堡垒机运维的机器。服务器管理功能能增添，删除，锁定，解锁服务器，对服务器进行有效的管理。
在主界面依次点击菜单栏“资产”-->“服务器”按钮，进入服务器管理页面。如下图所示：

- 新增服务器 点击左上按钮区域的“新增”按钮，进入新增服务器页面。参数说明如下：
    - 服务器IP： 服务器的IP地址，用于远程连接的IP。
    - 名称： 独立的服务器名称标识，长度限制60位。
    - 操作系统： 指服务器上运行的操作系统类型，决定连接的方式，如果是Windows，将会进行RDP连接，Linux则使用SSH方式进行连接。



- 锁定和解锁 锁定服务器是指将服务器的状态变为锁定，从而变为当前不可用的状态。锁定服务器可通过如下的方式：

  i：勾选需要锁定的服务器后点击上方按钮组的“锁定”按钮，并在弹出的对话框中选择“确定”，即可锁定一组用户。勾选后点击“解锁”即可解锁一组用户。如下图所示：

ii：点击的服务器行所在状态栏的锁定图标，即可变更服务器的状态。如果是未锁定的服务器，点击后将会变为已锁定状态；如果是已锁定的服务器，点击后将会变为为锁定的状态。

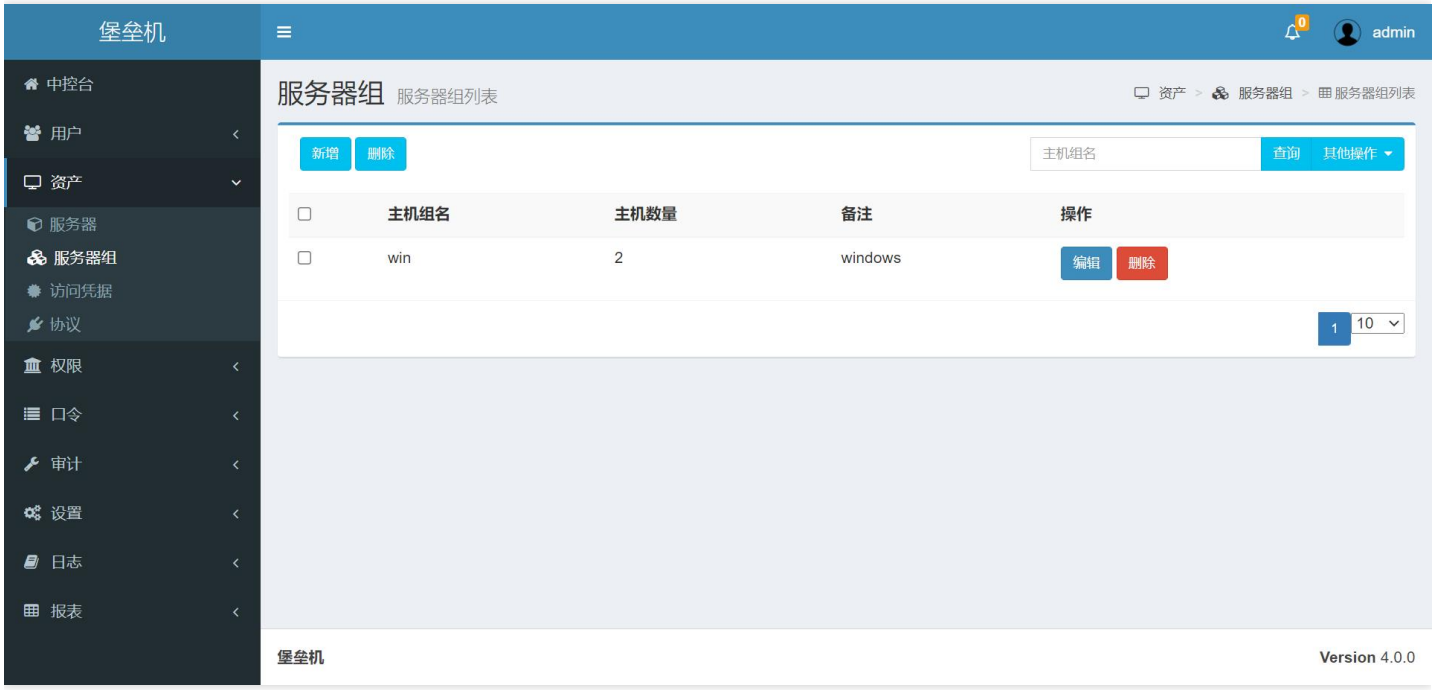
【注】

锁定的服务器会从相关的“服务器组”、“权限”中清除，如果重新引用该服务器，需要解锁后，重新添加服务器到相应服务器组和权限中

服务器组管理

最近更新时间: 2023-02-08 11:41:14

服务器组管理允许将多个服务器设定为一组，进行统一的管理的操作：



- 新增服务器组

  点击左上按钮区域的“新增”按钮，进入新增服务器组页面，如下图所示：

跳转到新增服务器组页面后，输入相关的参数即可新建服务器组记录。参数说明如下：

- 组名：用以标注服务器组的标识名
- 备注：对服务器组相关说明。

- 编辑 服务器编辑功能即将服务器添加和移除到服务器组。

点击服务器组所在行的编辑按钮进入编辑界面

i：添加服务器：

在服务器编辑界面，选中未选tab页

此处列出未锁定未删除的所有服务器。点选列表前边的复选框，选中需要添加到组中的服务器，点击左下角

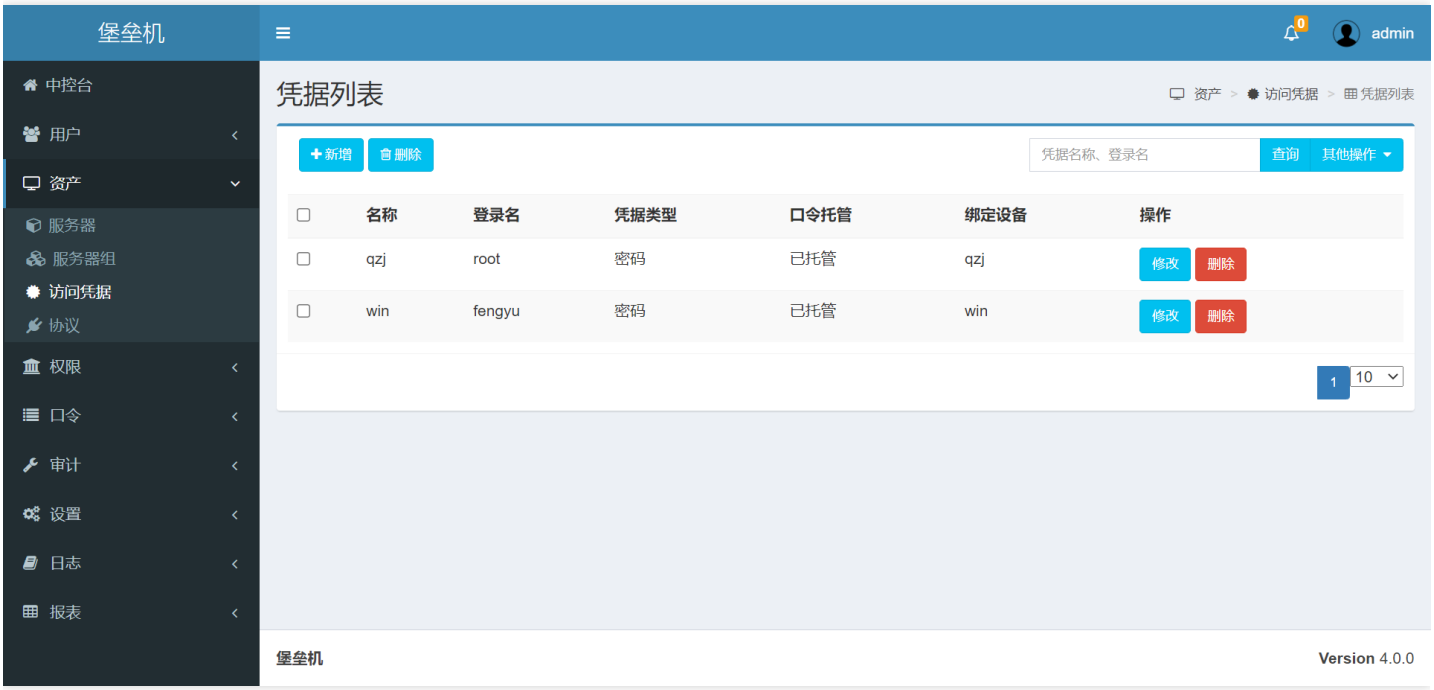
的“添加所选服务器”按钮，添加成功后到“已选”Tab页，可以看到刚才选择的服务器，如下图所示：

ii：移除服务器 在服务器编辑界面，选中已选tab页签后，依次选中需要移除的服务器，点击左下角的“移走所选服务器”的按钮，进行移除，如下图所示：

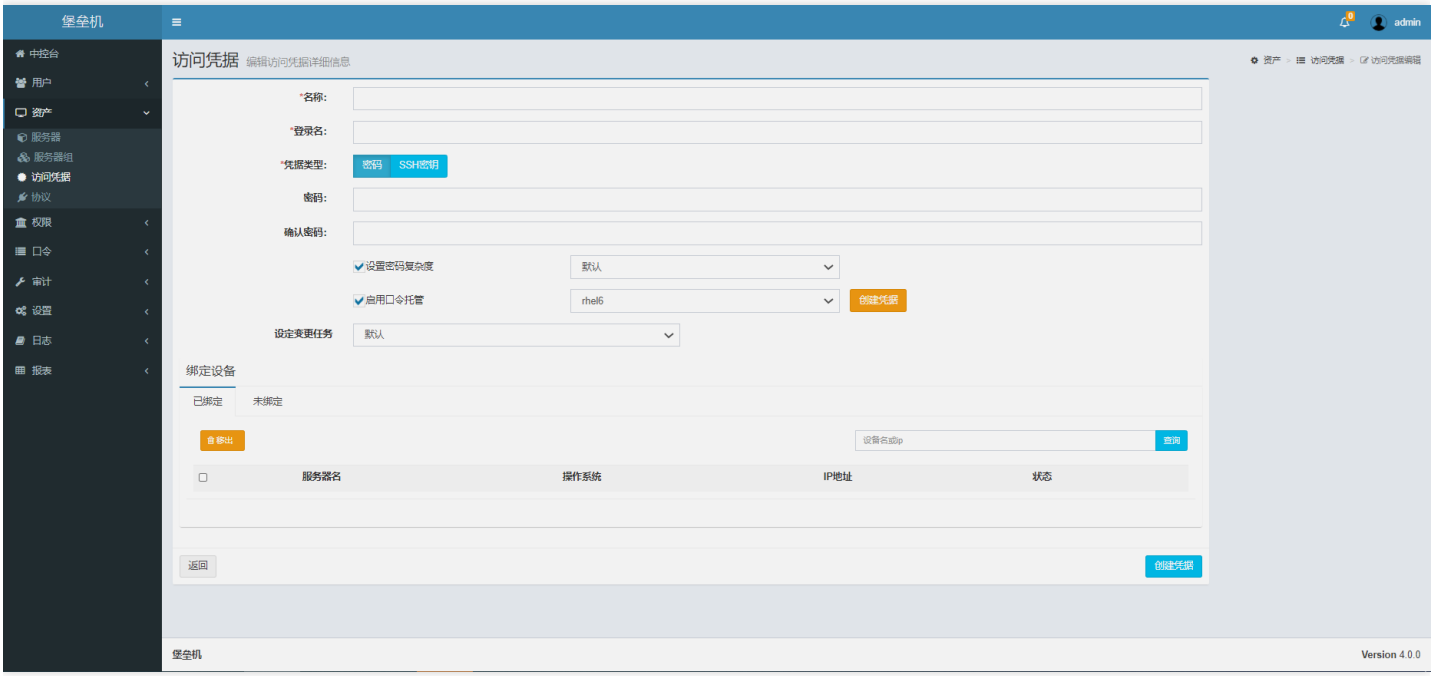
访问凭据

最近更新时间: 2023-02-08 11:41:14

问凭据是用来管理登录服务器的口令的功能，具有新增，删除和修改的功能。
通过“资产”->“访问凭据”来进入访问凭据管理页面



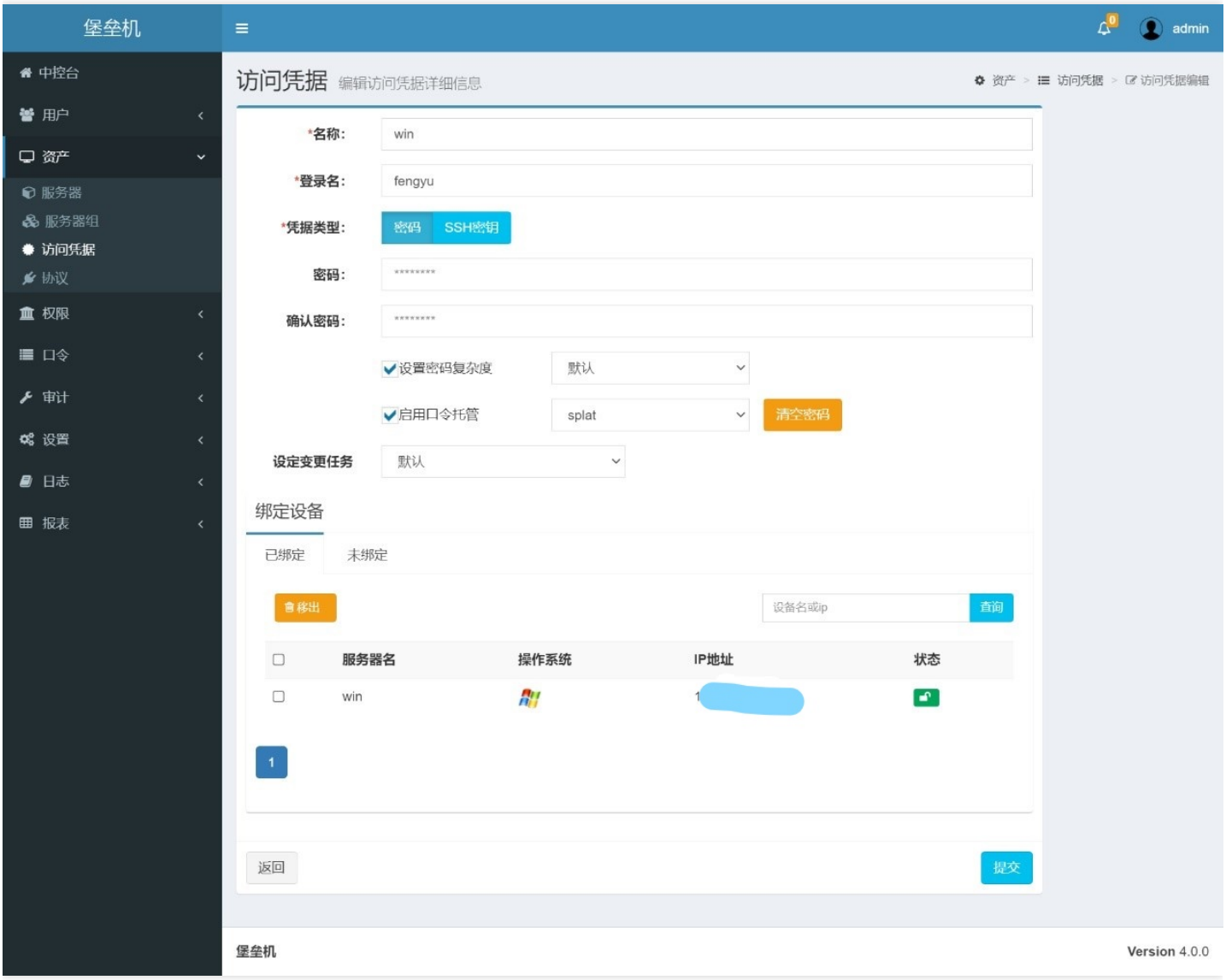
- 新增访问凭据
  点击左上按钮区域的“新增”按钮，进入新增访问凭据页面。访问凭据是指登录目标服务器使用的账户、口令等信息，主要由账户名和口令构成。对访问凭据进行管理，实现添加、删除等操作，设置的访问凭据必须绑定目标服务器。参数说明如下：
  - 名称： 该凭据的独立标识。
  - 登录名：登录到系统中的用户名。
    - 凭据类型： 有两种方式：密码或者SSH私钥。
  - 密码： 登录名对应的密码；
  - 设置密码复杂度： 选择默认
  - 启用口令托管： windows系统选择splat；red hat系统选择rhel6；CentOS系统选择CentOS6。
  - 设定变更任务：选择口令任务中设置的变更任务方案。选到对应的口令任务，才能在口令任务设置中找到对应的服务器
  - 绑定设备：在先提交密码后选择要绑定的设备。在未绑定中选择设备，点击绑定，绑定成功后，点击提交。



注意：此处录入的口令只用于自动登录，系统不修改口令，请用户自行保管好口令。

- 修改访问凭据

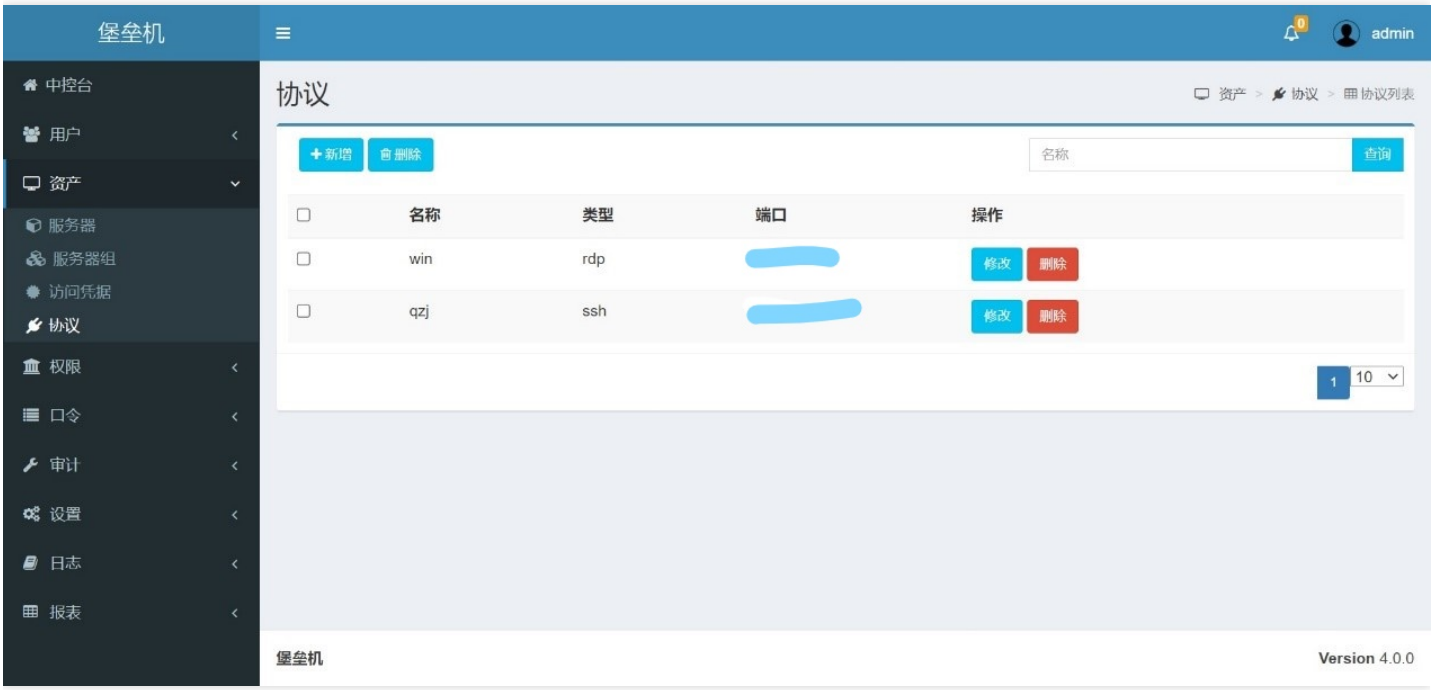
  点击所需修改的访问凭据所在行的修改按钮，进入修改页面，如下所示：


堡垒机
admin
中控台
用户
资产
服务器
服务器组
访问凭据
协议
权限
口令
审计
设置
日志
报表
访问凭据 编辑访问凭据详细信息
资产 > 访问凭据 > 访问凭据编辑
*名称: win
*登录名: fengyu
*凭据类型: 密码 SSH密钥
密码: ********
确认密码: ********
设置密码复杂度 默认
启用口令托管 splat 清空密码
设定变更任务 默认
绑定设备
已绑定 未绑定
移出 设备名或ip 查询
服务器名 操作系统 IP地址 状态
win
1
返回 提交
堡垒机 Version 4.0.0

协议

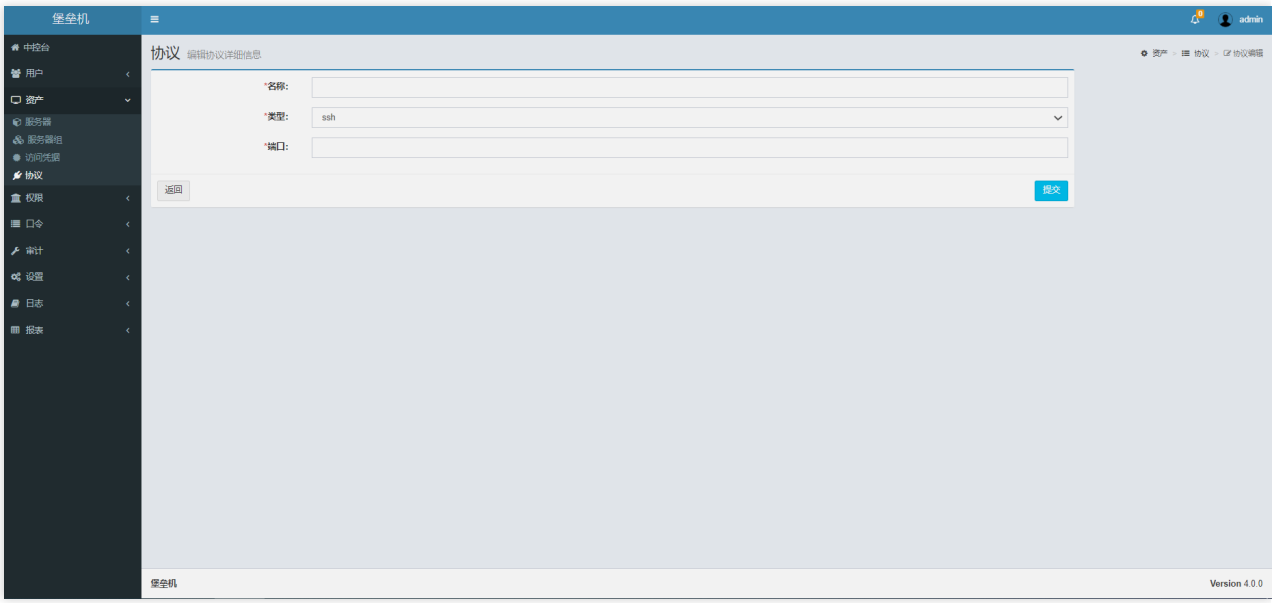
最近更新时间: 2023-02-08 11:41:14

协议是用来管理登录服务器使用的协议的功能，具有查询、新增、删除和修改的功能。
通过“资产”->“协议”来进入协议管理页面:

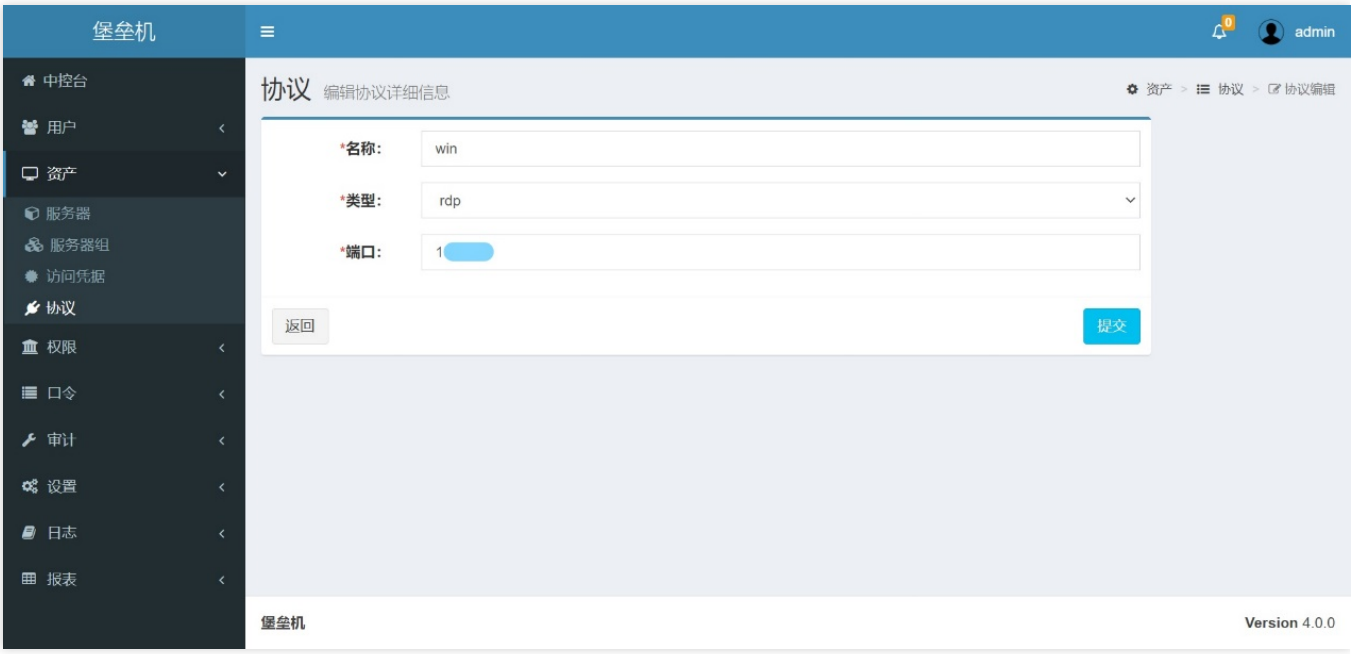


- 新增协议 点击左上按钮区域的“新增”按钮，进入新增协议页面，参数说明如下：
  - 名称：协议的独立标识。
  - 类型：有两种方式：SSH、RDP。

- 端口：使用该协议访问目标设备时连接的目标设备端口，例如：SSH使用22，RDP使用13389。



- 协议修改 点击所需修改的协议所在行的修改按钮，进入修改页面，如下所示：



口令

口令

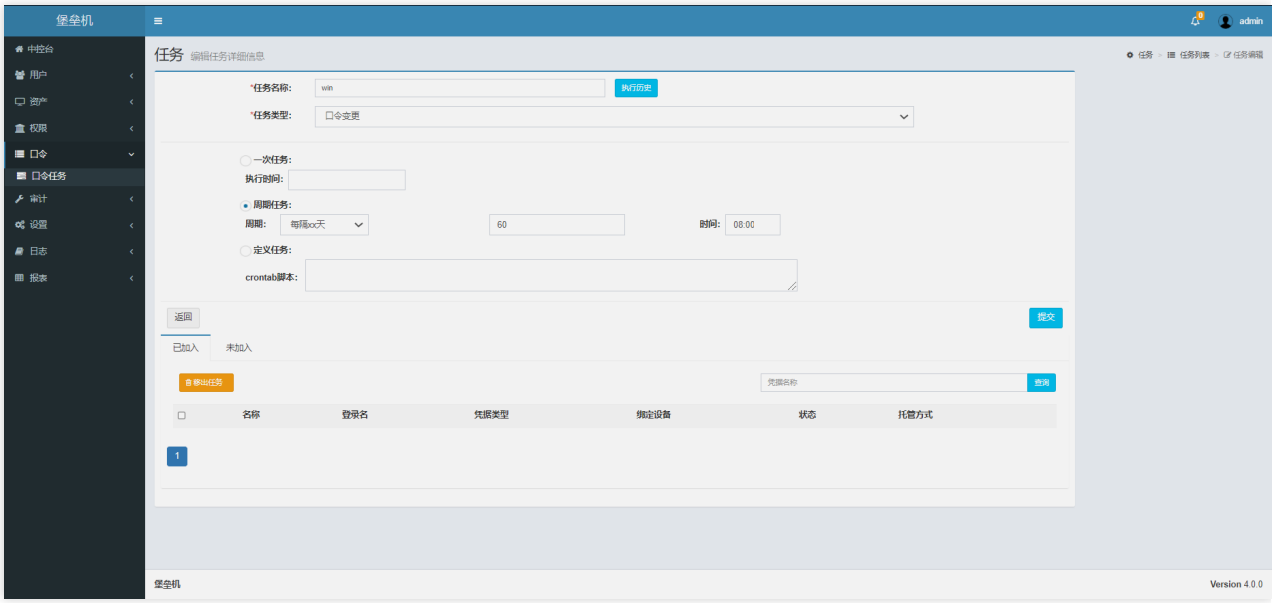
最近更新时间: 2023-02-08 13:49:46

通过“口令”->“口令任务”菜单即可进入用户权限界面，如下图所示：

口令任务

最近更新时间: 2023-02-08 13:49:46

- 新增口令任务
  设置口令任务执行时间，绑定口令任务对应的访问凭据（注：在权限中需将对应的服务器、访问凭据、协议相关联，否则会导致口令任务变更失败），以下是对参数的具体说明：
  - 任务名称：编写自定义名称。 * 任务类型：口令变更。 * 一次任务：只执行一次变更口令任务，填写变更指定的执行时间（修改为指定口令）。
    * 周期任务：每隔一段时间周期性执行变更任务（堡垒机通过算法修改为随机密码）。
    * 定义任务：目前不需要填写。
    * 加入任务：点击提交后，在未加入处选择要加入的访问凭据，点击加入任务。



- 立即执行
  第一次设置口令任务时先点击立即执行测试口令是否成功，再编辑修改成定时口令上收。行内要求所有纳管账号都要进行口令上收，特例除外。 通过勾选任务的选框，选择执行的任务，然后点击上方按钮处的按钮“立即

执行”，开始执行任务。

- 启用

  通过勾选任务的选框，选择启用的任务，然后点击上方按钮处的按钮“启用”，启用任务。

- 停止 通过勾选任务的选框，选择停止的任务，然后点击上方按钮处的按钮“停止”，启用任务。

审计

审计

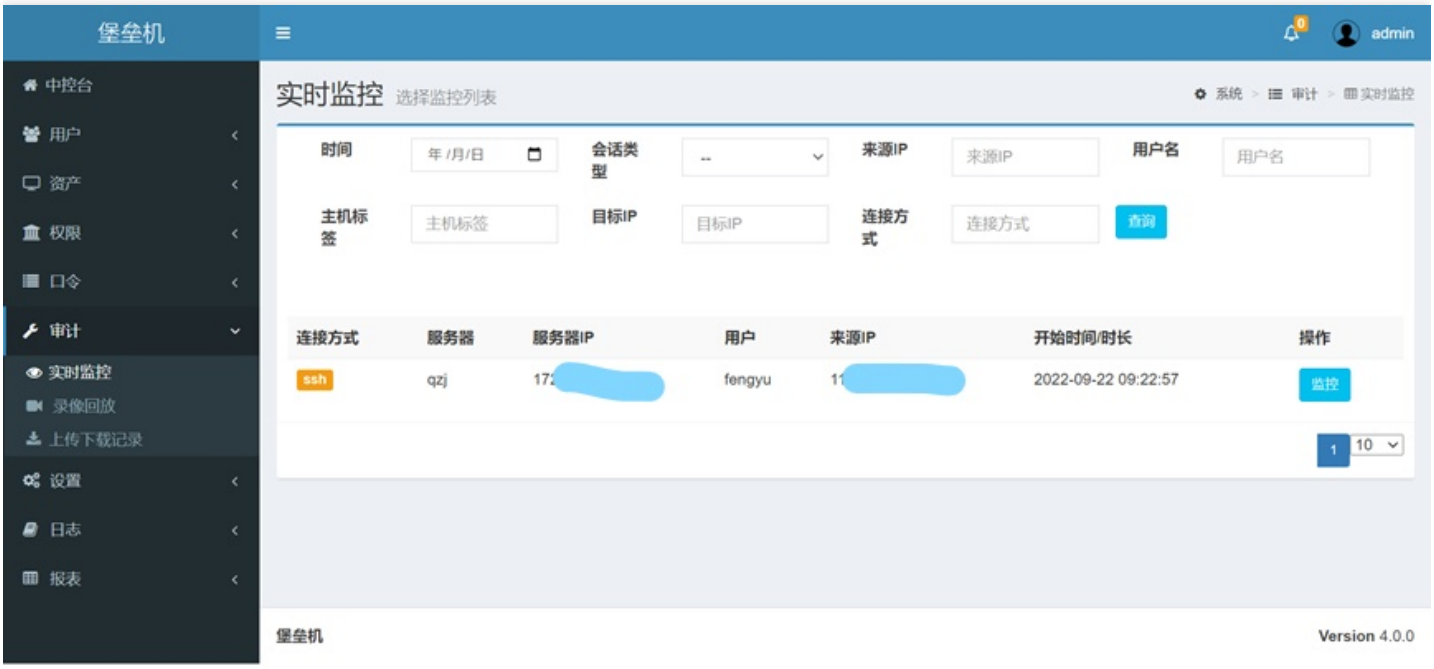
最近更新时间: 2023-01-11 14:48:54

运维人员通过云堡垒机进行的所有操作均有记录，对在线用户可实时监控用户远程连接的操作，监控画面实时同步展示运维人员终端操作。 对于历史操作记录，通过查看录像，重现运维人员当时的所有操作过程。

实时监控

最近更新时间: 2023-02-08 16:17:55

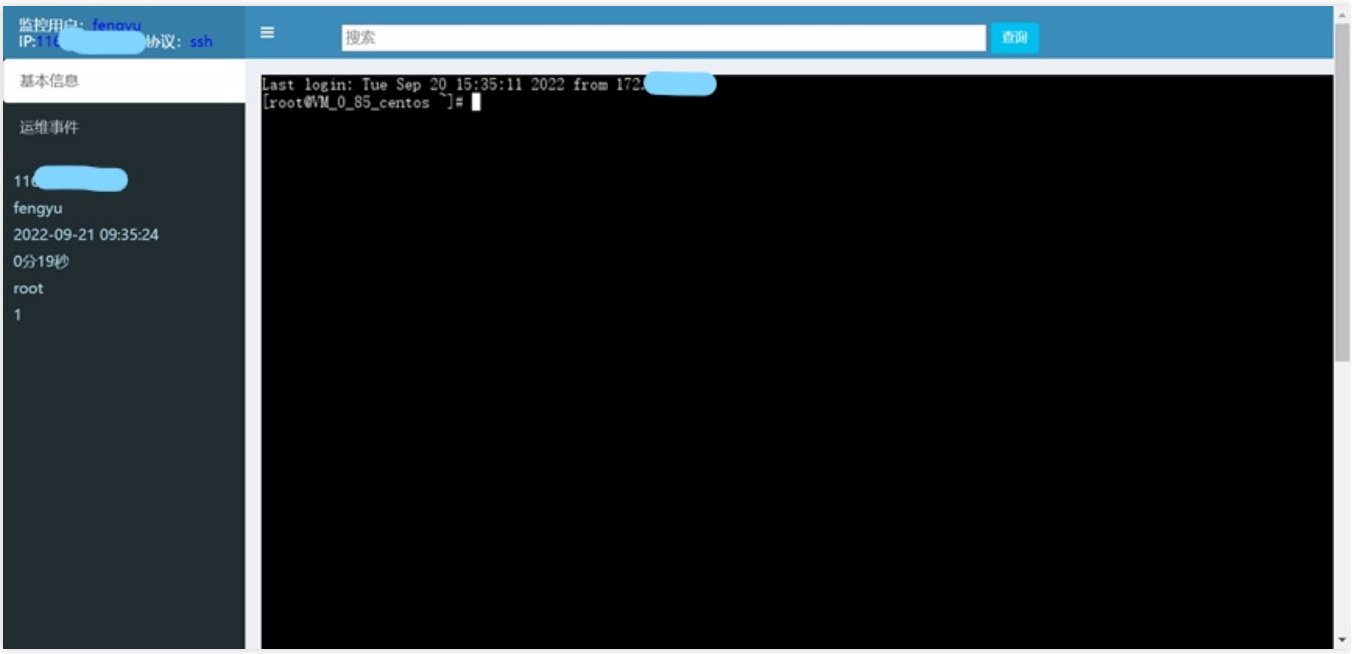
对当前通过云堡垒机进行操作的在线连接进行监控，实时展示运维人员在目标服务器上的操作情况。
通过菜单栏“审计”-->“实时监控”进入实时监控页面，如下图所示：



在界面上将出现当前远程运维的连接。上方的搜索区域可以根据条件搜索给出条件搜索符合条件的连接。

- 监控
  选择对应的连接记录后，点击监控即可进入监控界面，实时查看远程连接的操作，通过视频流的方式展示，如

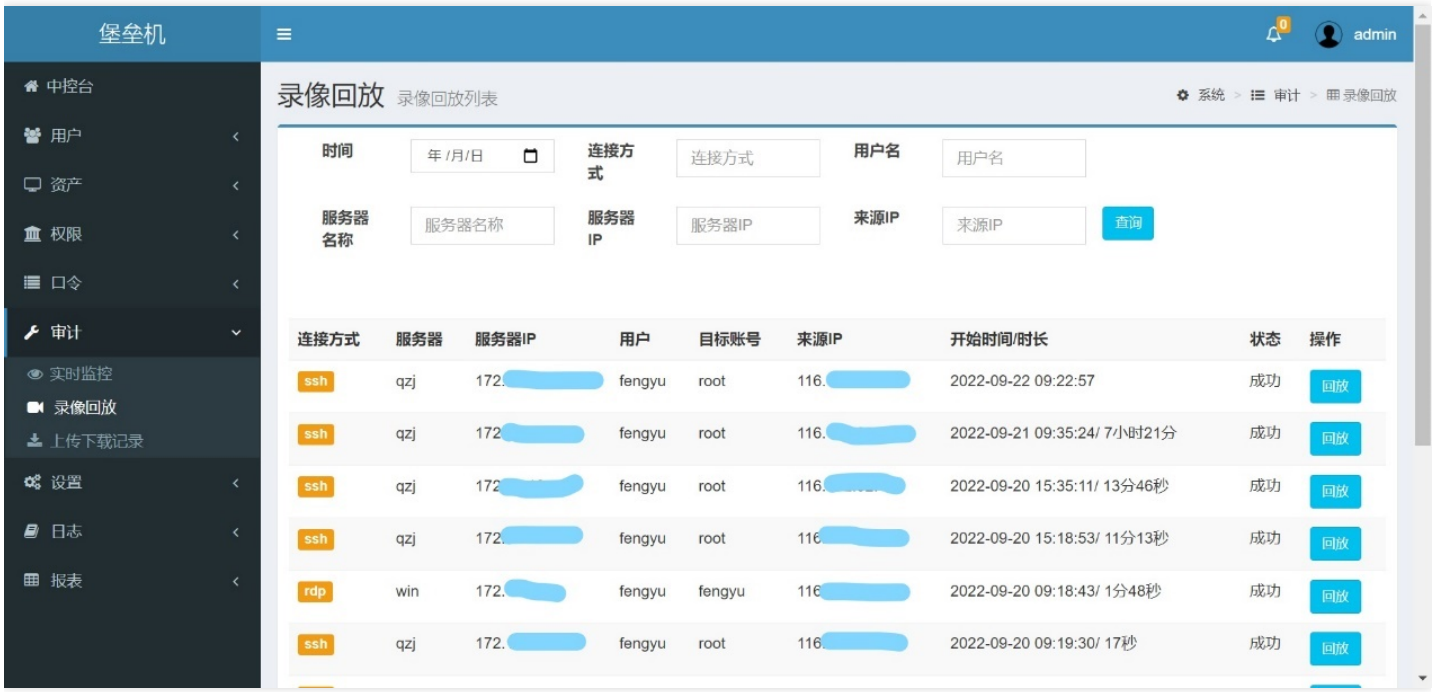
下图所示：


搜索
查询
基本信息
运维事件
fengyu
2022-09-21 09:35:24
0分19秒
root
1
Last login: Tue Sep 20 15:35:11 2022 from
[root@VM_0_85_centos ~]#

录像回放

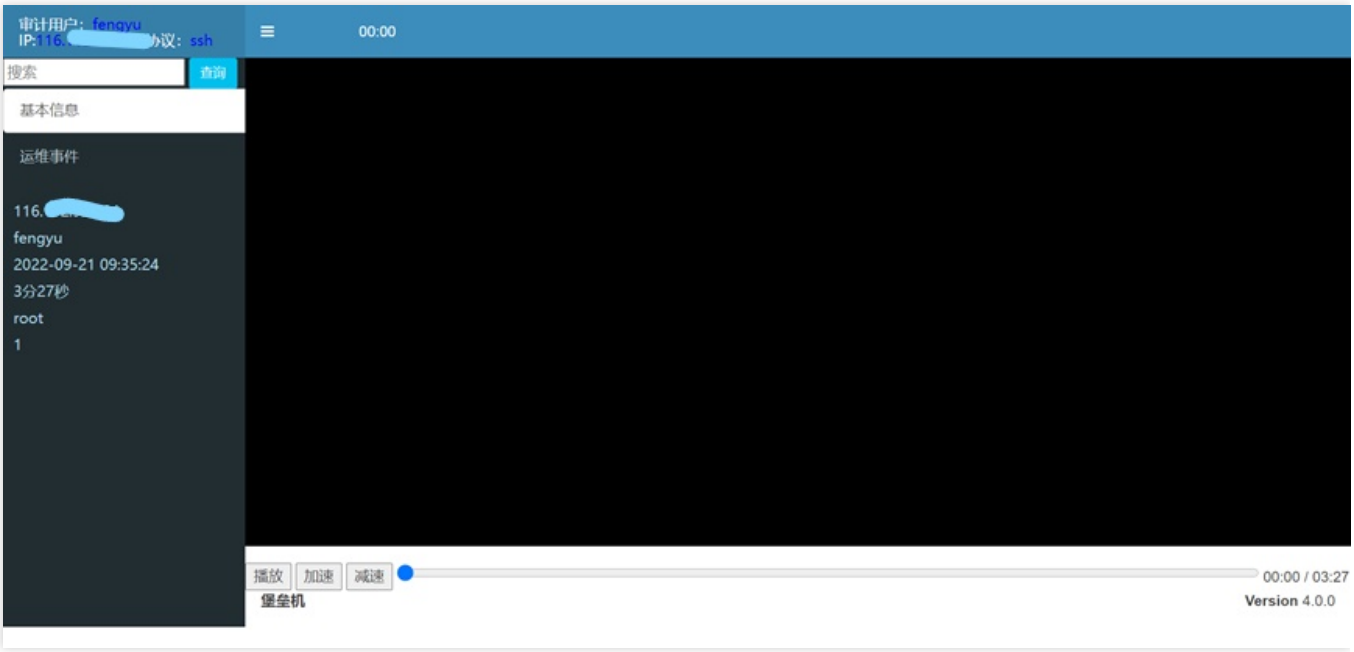
最近更新时间: 2023-02-08 16:17:55

运维人员访问目标服务器的所有操作均有记录，在运维人员结束操作后，管理员通过录像回放可以重现运维人员当时的操作过程。
对于通过堡垒机的远程连接，系统将会自动记录，生成视频文件在，再录像回放页面即可统一查看：
通过菜单“审计”->“录像回放”进入录像回放界面，如下图所示：



可以通过上方的查询区域输入对应的值查询查看的录像内容。

- 回放
  通过点击对应记录的“回放”按钮，即可进入回放页面，如下图所示：



在页面中点击“播放”和“取消”按钮即可播放和暂停视频。

上传下载记录

最近更新时间: 2023-02-08 16:17:55

通过堡垒机的远程连接功能上传和下载的文件，系统会自动记录并保存，管理员审计时可以到此功能查看运维人员。 通过“审计”→“上传下载记录”，进入上传下载记录的页面。

可以通过上方的查询区域输入对应的值查询查看的上传下载文件内容。

设置

设置

最近更新时间: 2023-01-11 14:48:49

对云堡垒机运行参数进行配置，包括配置系统的认证方式(密码、双因子等)、默认端口、备份策略等，以及对云堡垒机立即进行备份和恢复

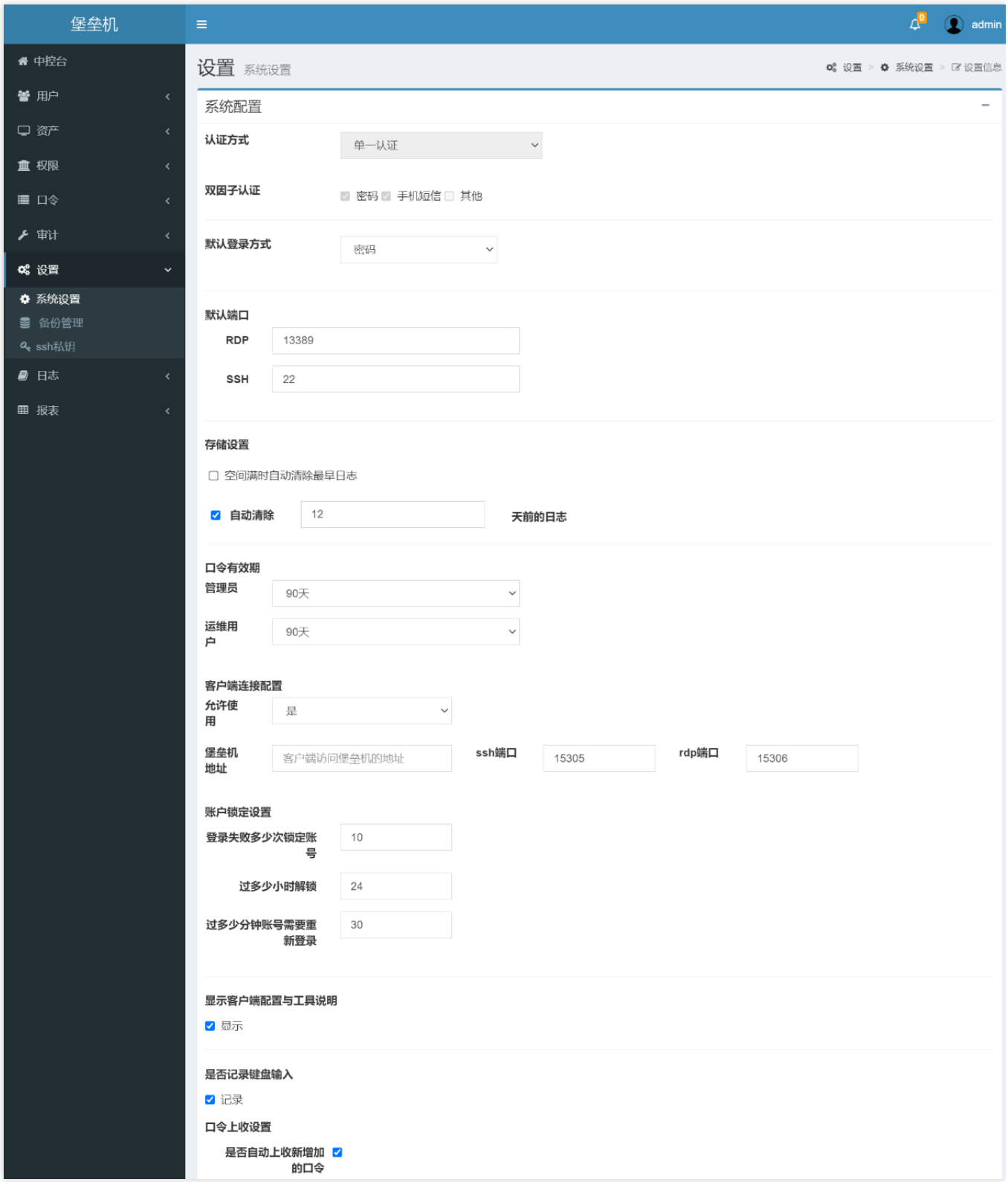
系统设置

最近更新时间: 2023-02-08 16:35:52

通过“设置”->“系统设置”菜单即可进入用户权限界面，以下是对参数的具体说明：

- 双因子认证：设置登录进入云堡垒机的方式，默认设定密码，手机方式登录。界面无法修改。
- 默认端口： 设置通过SSH和RDP客户端远程连接服务器时的默认使用端口。系统初始化RDP为3389，SSH为22.
- 存储设置： 系统自动清除功能的设定。可以设置自动清除的时间间隔，同时也可以设置是否在空间满之后自动删除最早的备份记录。
- 再进入设置页面输入参数后，点击提交保存结果，否则将不会保存修改记录。
- 口令有效期：管理员口令和运维用户口令分别设置，在间隔多少天以后无效，要求用户定期修改密码。
- 账户锁定设置：该项配置了账户锁定策略
- 显示客户端配置与工具说明：网页显示客户端配置与工具说明

- 口令上收设置：自动上收新增加的口令

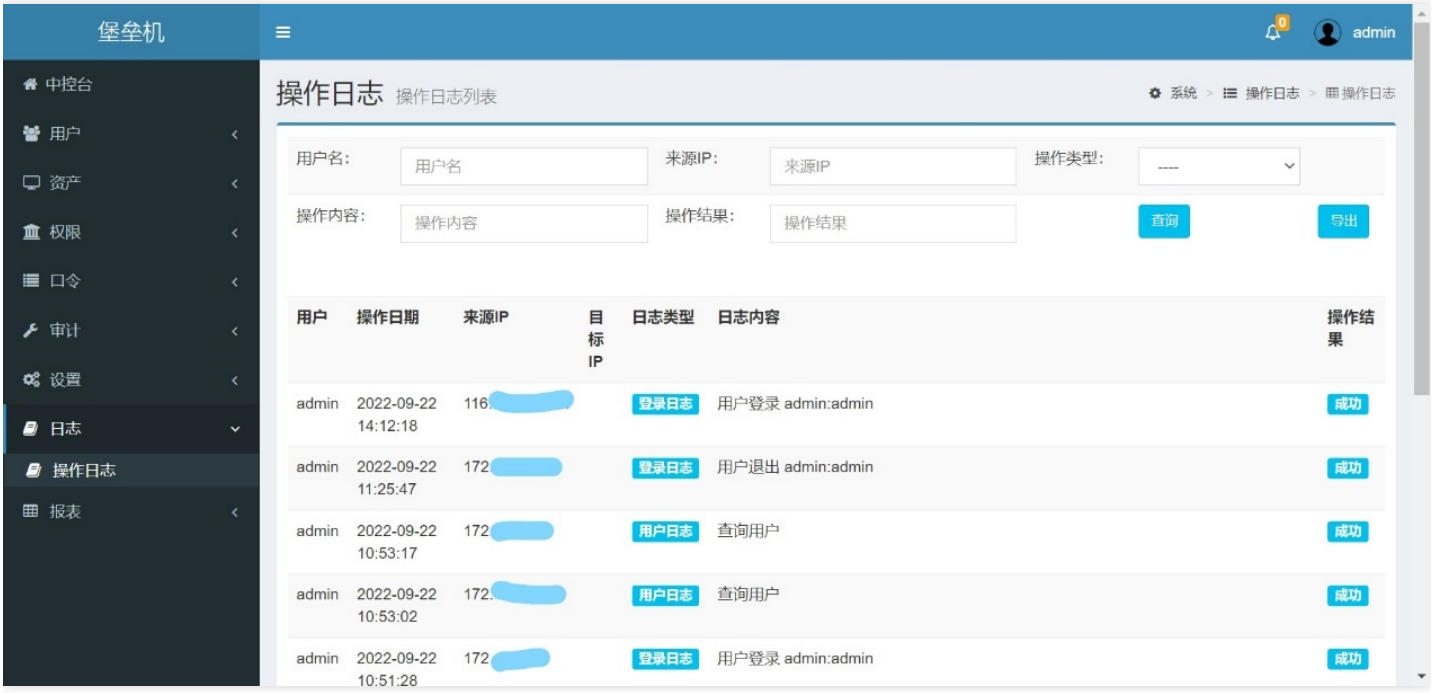


日志
操作日志

最近更新时间: 2023-02-08 16:35:52

系统记录了所有用户通过云堡垒机进行操作的日志，包括但不限于用户登录、远程访问的日志。 点击“操作日志”，以列表方式展示用户所有操作记录，通过菜单“日志”->“操作日志”对当前堡垒机的所有状态进行管理，以下是对参数的具体说明：

- 用户： 即进行操作的用户的用户名；
- 操作日期： 即操作发生的详细时间；
- 来源IP： 用户进行操作时本地IP；
- 目标IP： 如果用户操作远程的服务器，则显示远程服务器的IP地址，否则为空；
- 日志类型： 用户进行操作的类型划分，目前分为登录日志和权限日志；
- 日志内容： 用户操作的详细内容；
- 操作结果： 显示操作的成功或失败状态；



报表

权限报表

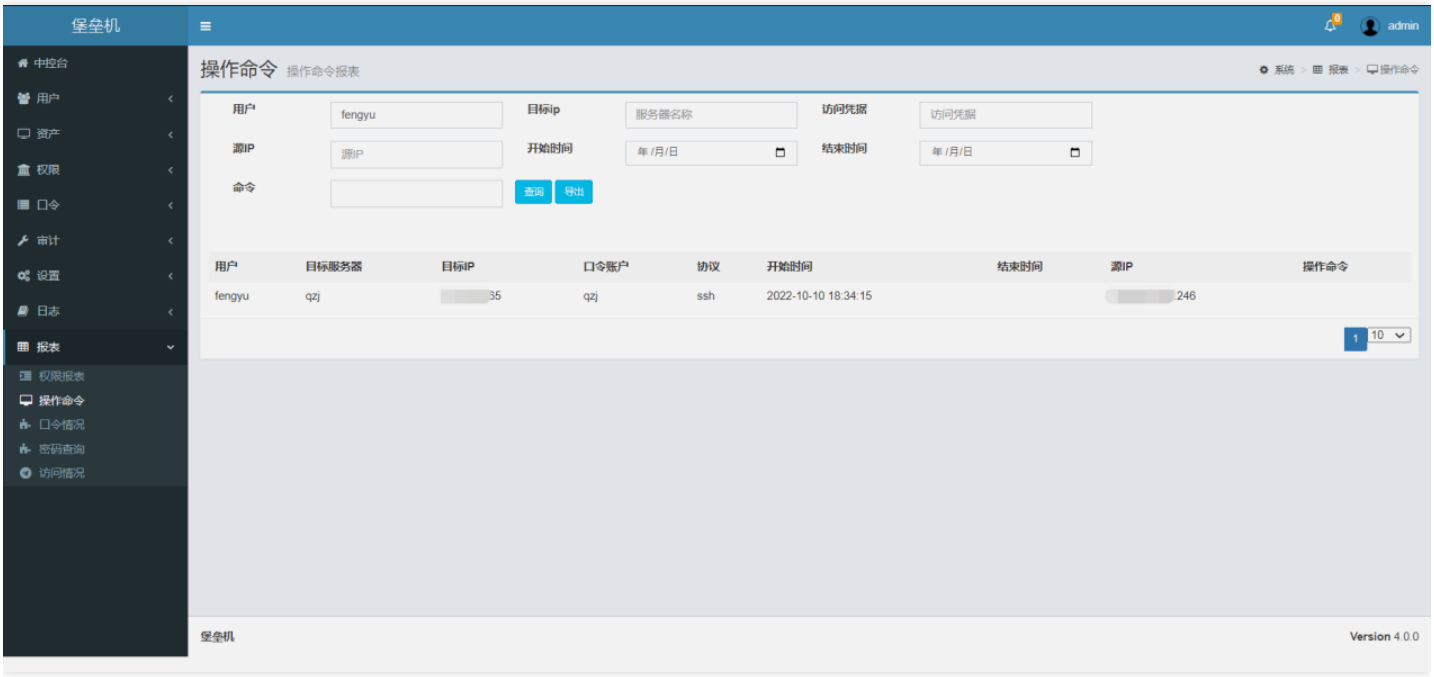
最近更新时间: 2023-02-08 16:35:52

根据服务器名称或IP查询相关的用户、协议、访问凭据、服务器名称、服务器IP、控制策略权限。通过菜单“报表”->“权限报表”对当前堡垒机的所有权限配置进行查询

操作命令

最近更新时间: 2023-02-08 16:35:52

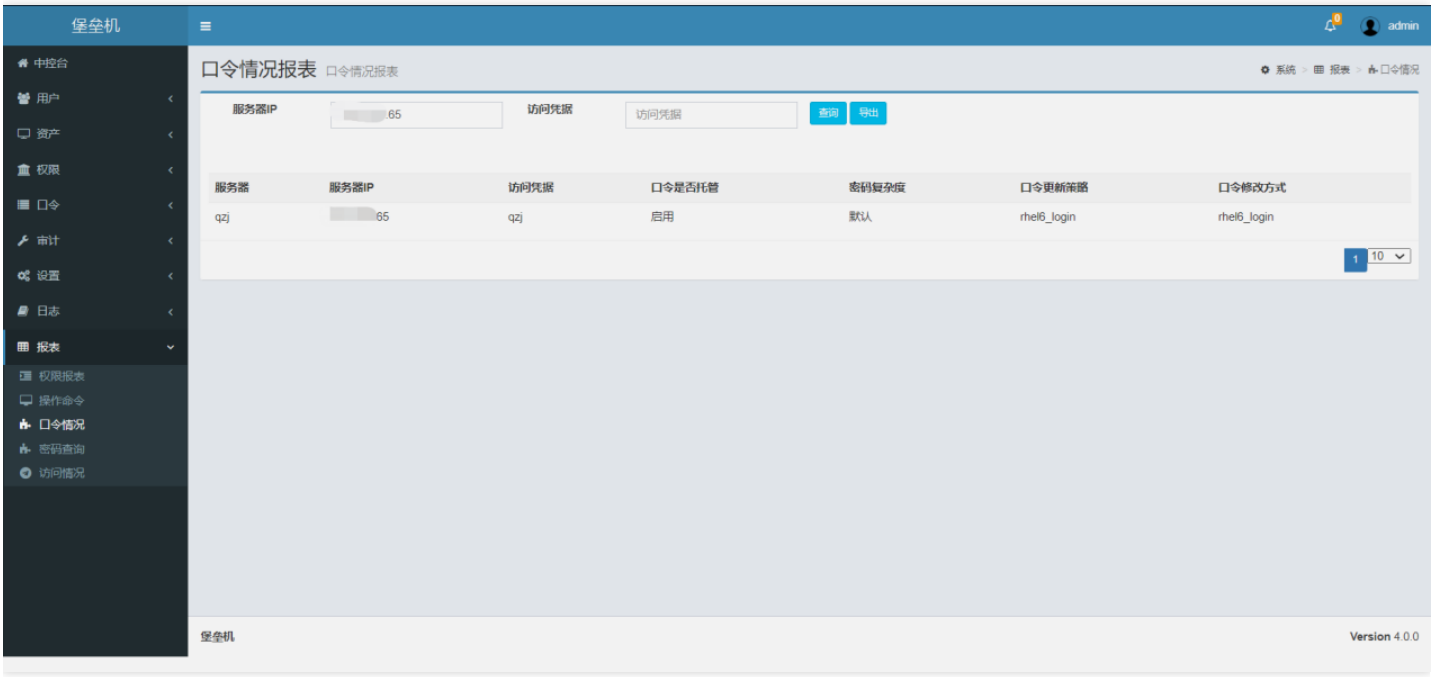
根据用户或IP查询相关的服务器的操作情况。通过菜单“报表”->“操作命令”对当前堡垒机纳管服务器的操作情况进行查询



口令情况

最近更新时间: 2023-02-08 16:35:52

根据服务器IP或访问凭据查询相关服务器口令任务的执行变更情况。通过菜单“报表”->“口令情况”对当前堡垒机口令任务的执行变更情况进行查询，行内要求密码复杂度为默认，口令托管为启用。



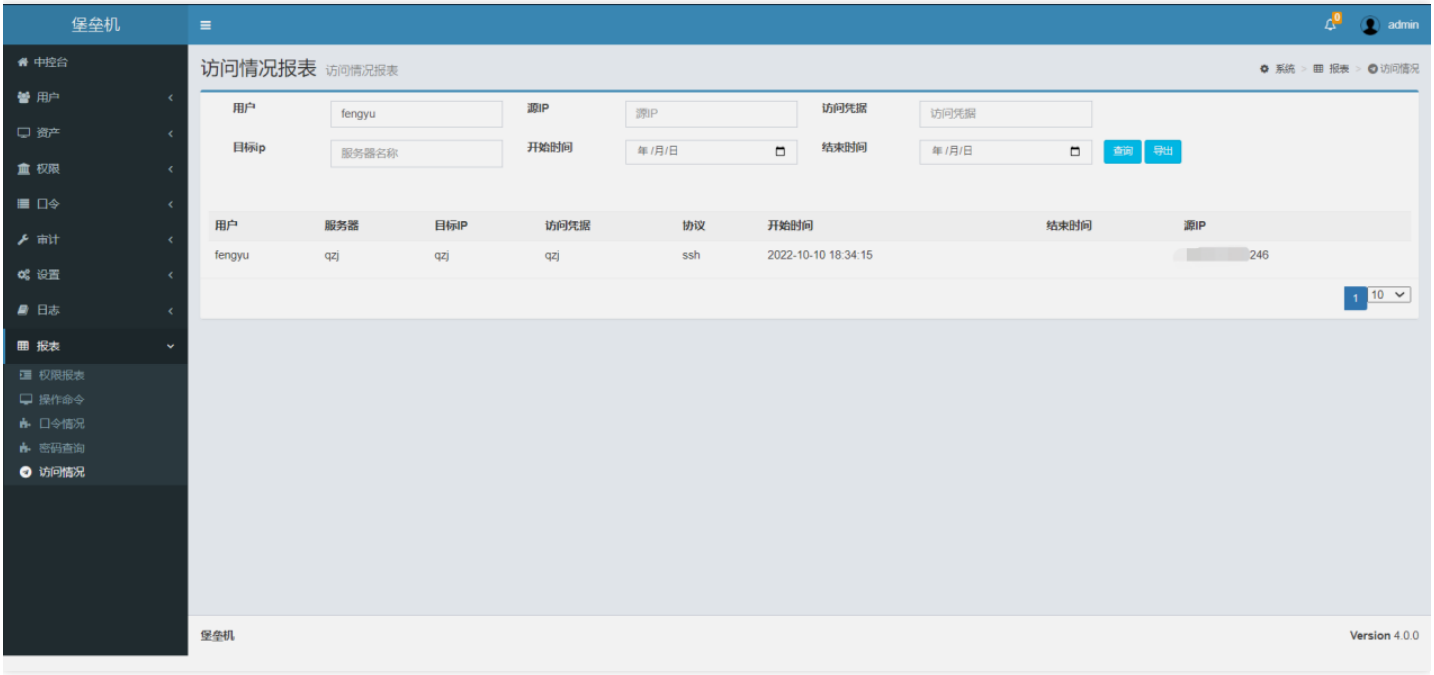
密码查询

最近更新时间: 2023-02-08 16:35:52

根据服务器IP或访问凭据查询相关服务器执行变更后的新密码情况。通过菜单“报表”->“密码查询”对当前堡垒机纳管服务器密码变更情况进行查询

访问情况：根据用户或源IP查询纳管服务器的访问情况。通过菜单“报表”->“访问情况”对当前堡垒机纳管服务器访

问情况进行查询


堡垒机
admin
中控台
用户
资产
权限
口令
审计
设置
日志
报表
权限报表
操作命令
口令情况
密码查询
访问情况
访问情况报表
访问情况报表
系统 > 报表 > 访问情况
用户
fengyu
源IP
源IP
访问凭据
访问凭据
目标ip
服务器名称
开始时间
年/月/日
结束时间
年/月/日
查询
导出
用户
服务器
目标IP
访问凭据
协议
开始时间
结束时间
源IP
fengyu
qzj
qzj
qzj
ssh
2022-10-10 18:34:15
246
1
10
堡垒机
Version 4.0.0

运维

运维

最近更新时间: 2023-01-11 14:48:49

运维人员登录云堡垒机，通过云堡垒机连接目标服务器运行运维操作。

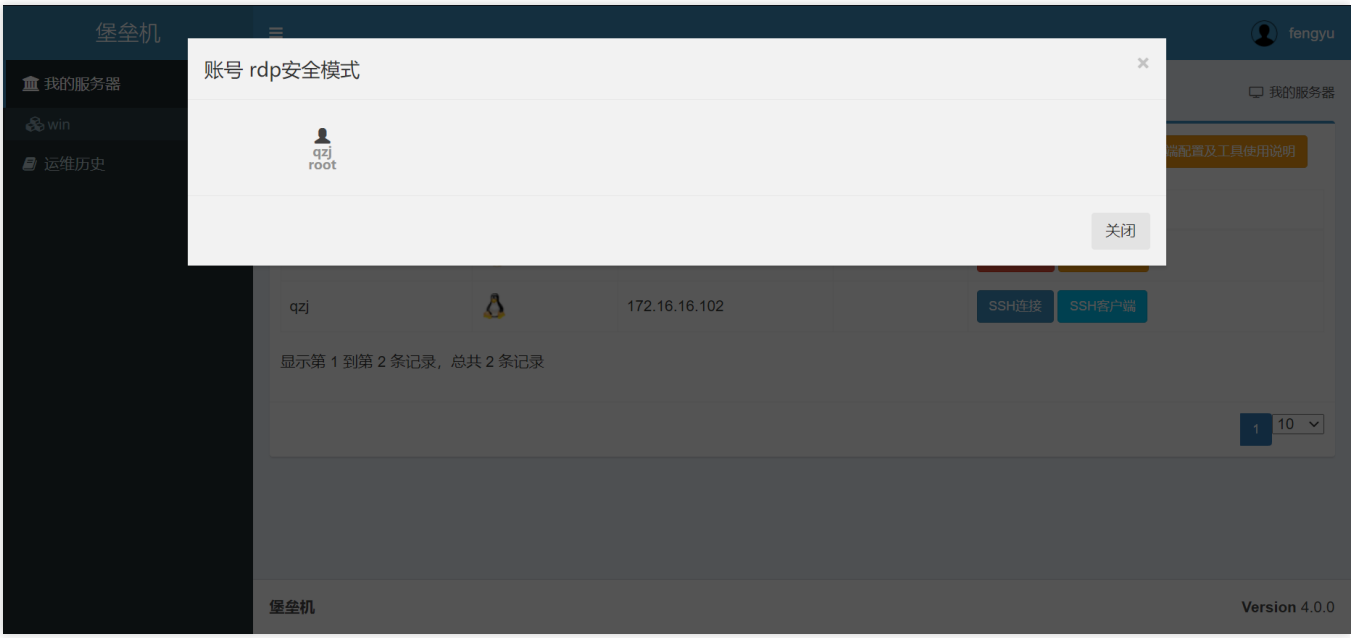
远程访问

最近更新时间: 2023-02-08 16:35:52

运维人员登录后，在“我的权限”菜单显示该运维人员拥有的访问权限，如下图所示：

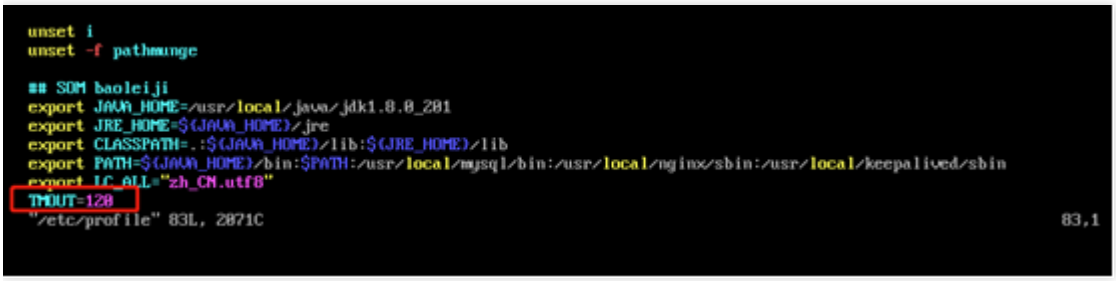
在该界面中，展示用户具有权限的服务器的列表，并能正式连接。

- 远程连接
  在“我的权限”列表中选择需要访问的目标服务器，通过点击操作列中的按钮“SSH连接”/“RDP连接”，进行登录。在弹出的页面，选择本次连接使用的“账户”，如下图所示：



直接点击选择的“账户”即可进入目标服务器进行操作，如下图所示：

点击右侧的按钮显示“工具栏”，然后点击“SFTP上传下载”和“打开键盘”分别开启文件传输和键盘输入功能。



访问目标服务器长时间无操作自动会断开，这个断开时间在目标服务器设置用户自动登出时间不是在堡垒机里设置，编辑/etc/profile文件，搜索TMOUT，修改后面的数值

最佳实践

最近更新时间: 2023-01-11 14:04:44

1. 最小授权

   用户管理服务器时，包括且不限于对防火墙、端口、访问用户权限的配置应按照最小授权原则，保证每个用户和程序在操作时使用尽可能少的特权。以限制事故、错误或攻击带来的危害。

运维指南

最近更新时间: 2023-01-11 14:04:44

1. 云堡垒机重启

   云堡垒机支持开机自启动，会随着云服务器的启动同时启动云堡垒机。

2. 监控告警

   建议在购买的云服务器列表设置CPU、内存、硬盘空间、网络响应等告警指标，在收到告警后，根据告警提示选择进行资源扩容或清理日志以释放磁盘空间。

常见问题
堡垒机需要安装客户端吗，是否支持移动设备?

最近更新时间: 2021-10-09 14:27:41

您的操作系统安装了WEB浏览器就可以使用龙堡垒机机。无需安装其他客户端，支持所有移动设备。

通过堡垒机访问目标服务器时，提示失败

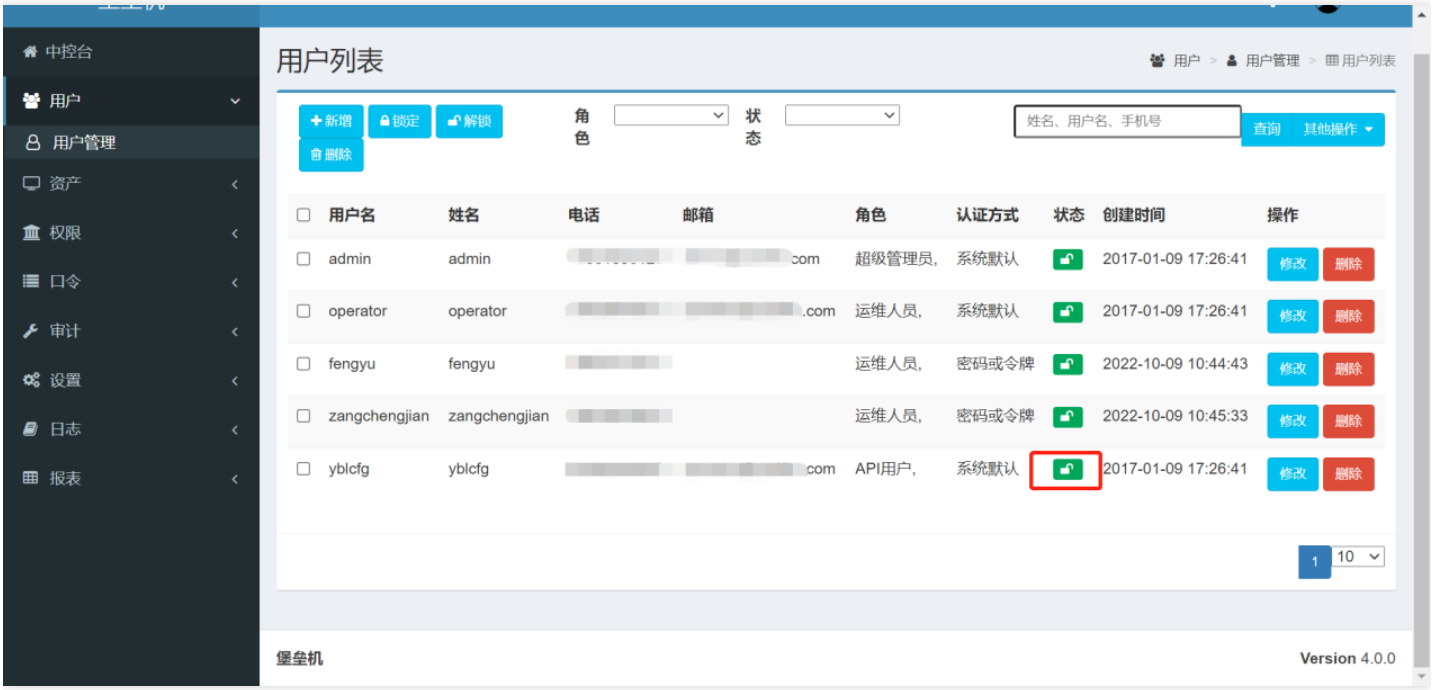
最近更新时间: 2023-01-11 14:04:34

首先需要检查目标服务器的安全组规则配置、服务器本身防火墙配置，确认没有限制堡垒机访问服务器的端口；然后检查堡垒机对服务器的权限、协议、控制策略，是否允许连接。

通过堡垒机上收口令时上收失败

最近更新时间: 2023-01-11 14:04:34

1、管理员用户登陆堡垒机检查yblcfg用户是否正常，用户状态正常为未锁定状态如下图所示，如锁定需要点击yblcfg用户右侧的锁形按钮解锁。



2、管理员用户登陆堡垒机检查设置–系统设置，确认允许客户端登录，如果时否则改为是。

3、登录租户控制台VNC登录堡垒机，检查堡垒机后台配置文件cat /usr/local/somapp/application-noncluster.propername |grep yblcfg,确认有配置cclientusername=yblcfg

```
[root@VM_16_50_centos ~]# cat /usr/local/somapp/application-noncluster.properties |grep yblcfg
cclientusername=yblcfg
[root@VM_16_50_centos ~]#
```

4、 管理员用户登陆堡垒机检查口令任务纳管设置的访问凭据中登录名、密码、口令托管模板是否正确，口令托管模板windows系统选择splat；red hat系统选择rhel6；CentOS系统选择CentOS6。

5、 管理员用户登陆堡垒机检查权限设置是否正确，点击下图协议处的“1”，检查协议类型和协议端口是否正确

6、 如果上面检查配置都没有问题VNC登录堡垒机执行命令etlog set etpass2 4打开口令上收日志

```
[root@VM_16_50_centos ~]# etlog set etpass2 4
[root@VM_16_50_centos ~]# etlog
etlog is ready.
[root@VM_16_50_centos ~]#
```

再执行一遍口令上收，执行命令$LOG_DIR/etpass2.log查看日志路径，查看日志报错信息定位问题原因cat /var/log/et-smplat/etpass2.log，如下图所示

```
[root@VM_16_50_centos ~]# $LOG_DIR/etpass2.log
-bash: /var/log/et-smplat/etpass2.log: 权限不够
[root@VM_16_50_centos ~]# cat /var/log/et-smplat/etpass2.log
[root@VM_16_50_centos ~]#
```

如无法定位问题联系我们提供技术支持，联系邮箱fxglb_sp2.zh@ccb.com

登录堡垒机无法收到验证码

最近更新时间: 2023-01-11 14:04:34

1、 检查手机号是否正确，手机号是否存在欠费、停机等问题。

2、 登录租户控制台VNC登录堡垒机，执行命令netstat -nltp |grep 8000检查8000端口是否被监听，如未监听vi /usr/local/nginx/conf/nginx.conf检查nginx配置文件是否正常，正常server配置如下图所示

```
server {
        listen  8000;
        proxy_redirect http:// $scheme://;
        client_max_body_size 1024M;
        if ($time_iso8601 ~ "(\d{4}-\d{2}-\d{2})")
        {
            set $tttt $1;
        }
        access_log  logs/host.access.$tttt.log  main;
        server_name  localhost  127.0.0.1;
        location / {
            proxy_pass         http://mysite1;
            #proxy_set_header X-Forward-For $remote_addr;
            proxy_set_header X-Real-IP $remote_addr;
            #proxy_set_header Host $host;
            proxy_set_header Host $http_host;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto https;
            proxy_http_version 1.1;
            proxy_set_header   Upgrade $http_upgrade;
            proxy_set_header   Connection "upgrade";
            proxy_buffering off;
                }
        location ~/\. {
            deny all;
                }
        }
    server_tokens off;
}
```

如与图片中server配置不一致则修改nginx.conf配置，然后nginx -s reload重新加载nginx配置

```
[root@VM_16_50_centos ~]# vi /usr/local/nginx/conf/nginx.conf
[root@VM_16_50_centos ~]# nginx -s reload
[root@VM_16_50_centos ~]#
```

如果上面检查都没有问题联系我们提供技术支持，联系邮箱fxglb_sp2.zh@ccb.com

登陆堡垒机提示页面正在维护中

最近更新时间: 2023-01-11 14:04:34

登录租户控制台VNC登录堡垒机，df -h检查磁盘使用情况，如果磁盘满了则需要清理堡垒机日志

/baoleijidata/目录中A开头的为用户操作日志，records为录屏日志，租户根据自身情况自行清理

内外部租户如何定义?

最近更新时间: 2023-01-11 14:04:34

内外部租户定义如下:
内部租户：与建行相关，运维系统上有建行logo的租户
外部租户：1）与建行无关，系统上没有建行相关logo的租户，需要申请互联网访问（需要提前联系运营一线报备加白）；2）属于建行内部租户，但是由于没有ECC机房权限，需要申请互联网访问（需要提前联系运营一线咨询报备加白流程），运营一线联系电话：87815199-29827

通过堡垒机，使用SSH访问目标服务器时是否支持使用密钥的方式

最近更新时间: 2023-01-11 14:04:34

支持，用户可以使用用户名密码和密钥两种方式访问服务器。

堡垒机连接云服务器时的空闲时长是多少?

最近更新时间: 2023-01-11 14:04:34

依赖于目标服务器设置的连接空闲时长。目标服务器空闲时长修改需要编辑/etc/profile文件，搜索TMOUT，修改后面的数值，如下图所示

/baoleijidata/目录中A开头的为用户操作日志，records为录屏日志，租户根据自身情况自行清理

通过堡垒机文件上传失败

最近更新时间: 2023-01-11 14:04:34

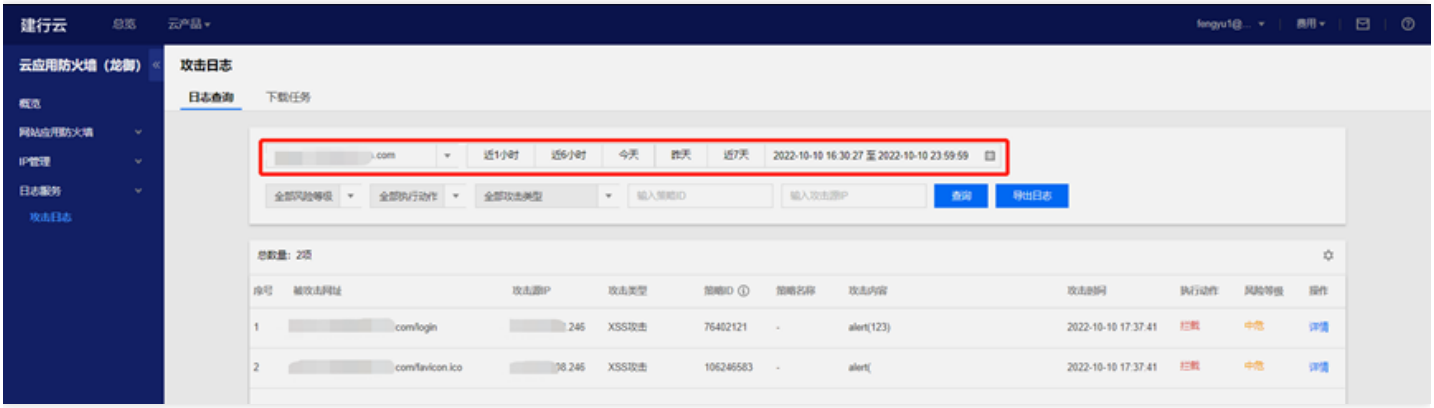
1、用户没有文件上传目录的读写权限，会导致上传失败。正确的做法选择登陆用户有读写权限的目录做为文件上传目录。

2、检查磁盘是否满了，df –h检查磁盘使用情况，如果磁盘满了则需要清理堡垒机日志

```
[root@VM_16_50_centos baoleijidata]# ll /baoleijidata
总用量 40
drwx------  3 root  root  4096 9月   23 17:17 A000000004
drwx------  3 root  root  4096 9月   30 16:00 A000000007
drwxr-xr-x  2 root  root  4096 10月  11 00:30 backupfile
lrwxrwxrwx  1 root  root    21 10月  10 15:07 baoleijidata -> /somdata/baoleijidata
drwxr-xr-x  3 mysql mysql 4096 8月   22 2019 db
drwxr-xr-x  5 root  root  4096 9月   30 16:18 fileTempPath
drwxr-xr-x  2 root  root  4096 10月  11 02:00 logs
drwxr-xr-x 14 root  root  4096 10月  10 23:30 records
drwxr-xr-x  3 root  root  4096 8月   22 2019 redis
drwxr-xr-x 19 root  root  4096 9月   30 14:07 release
drwxr-xr-x  8 root  root  4096 8月   22 2019 somlog
[root@VM_16_50_centos baoleijidata]#
```

/baoleijidata/目录中A开头的为用户操作日志，records为录屏日志，租户根据自身情况自行清理

3、检查是否被WAF拦截，登录租户控制台–云应用防火墙，输入堡垒机域名选择上传文件时间段查询是否有拦截日志

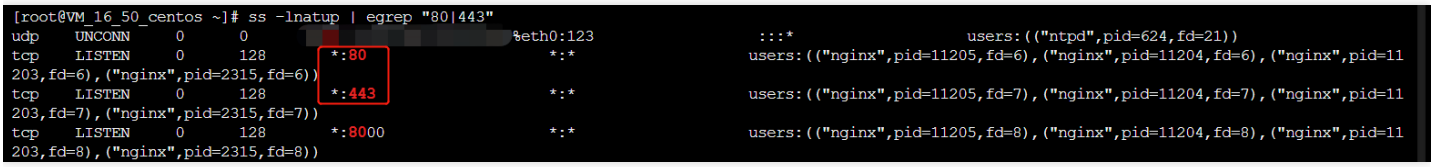


登录堡垒机报502和504错误

最近更新时间: 2023-01-11 14:04:34

1、 检查堡垒机和前置机的安全组配置是否正确，前置机入站放通80端口、堡垒机ip22端口，出站放通堡垒机8119端口，堡垒机入站放通堡垒机ip22端口、8119端口，出站放通22(ssh协议)、10800（windows口令上收）、13389（rdp协议）端口。如有未放通修改堡垒机和前置机安全组配置添加放行规则。

2、 检查堡垒机和前置机的nginx服务是否启动ps –ef |grep nginx,如未启动，执行命令启动nginx服务sh /usr/local/nginx/sbin/nginx;检查80、443端口开启ss –lnatup | egrep “80|443”，命令执行结果如下图所示则为nginx启动成功。



3、 检查数据库是否启动service mysqld status如未启动，执行命令service mysqld start。

4、 检查磁盘是否满了df –h，如果满了，按需清理/baoleijidata/目录中A开头的运维日志和records中的录屏日志。

5、 检查java进程 ps –ef |grep xjar如果java进程没有启动，输入以下命令启动进程sh /usr/local/somapp/startapp.sh。

堡垒机其他常见问题如何处理?

最近更新时间: 2023-01-11 14:04:34

联系我们获取常见问题处理手册，按照手册进行解锁。联系邮箱fxglb_sp2.zh@ccb.com