深信服 SASE-VPN 快速上架手册

文档版本 02

发布日期 2022-06-14

深信服科技股份有限公司

注意

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

关于本文档

本文档针对深信服安全接入平台SASE- AC 产品，介绍了 SASE-VPN 成功上线的每一个步骤及每一步骤的成功上线的说明，以客户视角明确SASE-VPN在客户端的成功交付。

读者对象

本上线手册建议适用于以下对象：

- 网络设计工程师
- 运维人员

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布时间	更新说明
01	2022-04-07	本文档第一次发布。
02	2022-06-25	修改部分内容。

资料获取

您可以通过深信服官方网站获取产品的最新资讯：

www.sangfor.com.cn

获取安装/配置资料、软件版本及升级包、常用工具地址如下：

bbs.sangfor.com.cn

深信服科技

深信服技术服务

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服科技服务商及服务有效期查询：

https://bbs.sangfor.com.cn/plugin.php?id=service:query

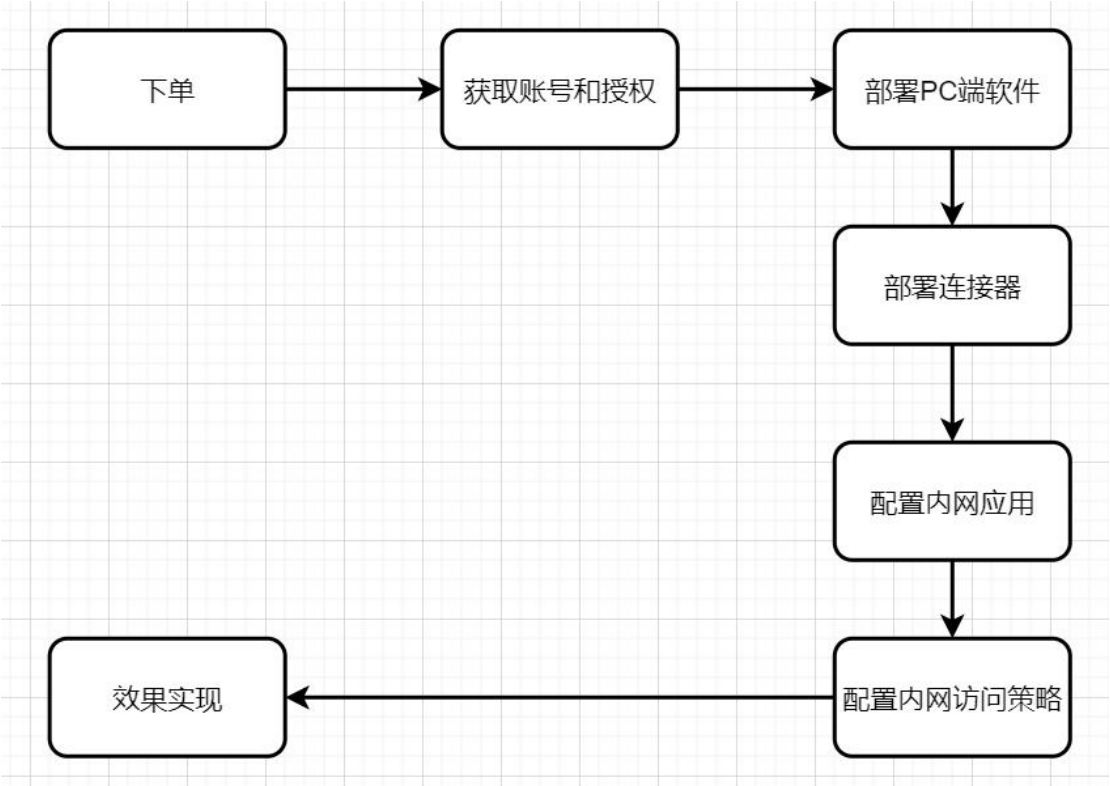
意见反馈

如果您在使用过程中发现任何产品资料的问题，可以通过以下方式联系我们。

- bbs.sangfor.com.cn
- 通过联系当地办事处电话反馈
- 售后服务电话 400-630-6430

目录

1. 交付整体流程



2. SASE-VPN 上线账号和授权获取流程

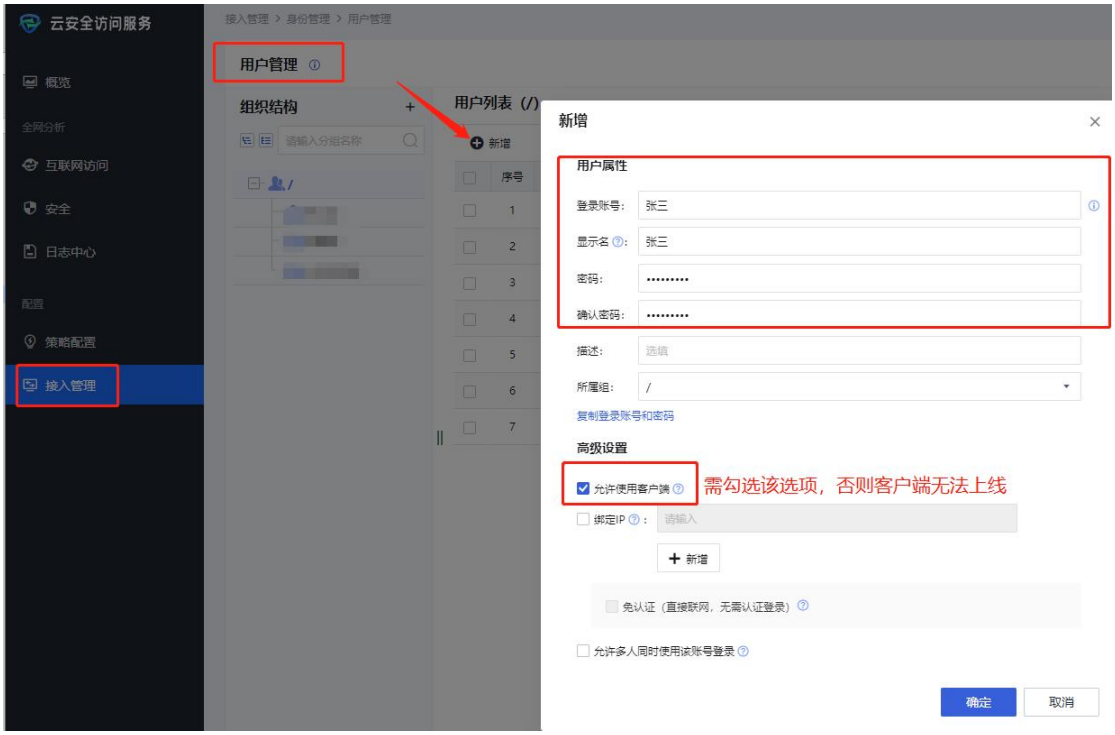
SASE-VPN 线上授权功能暂未上线，需要交付时请拨打 400-630-6430 转 5 或者是云图在线客服进行人工开工

3. SASE-VPN 部署

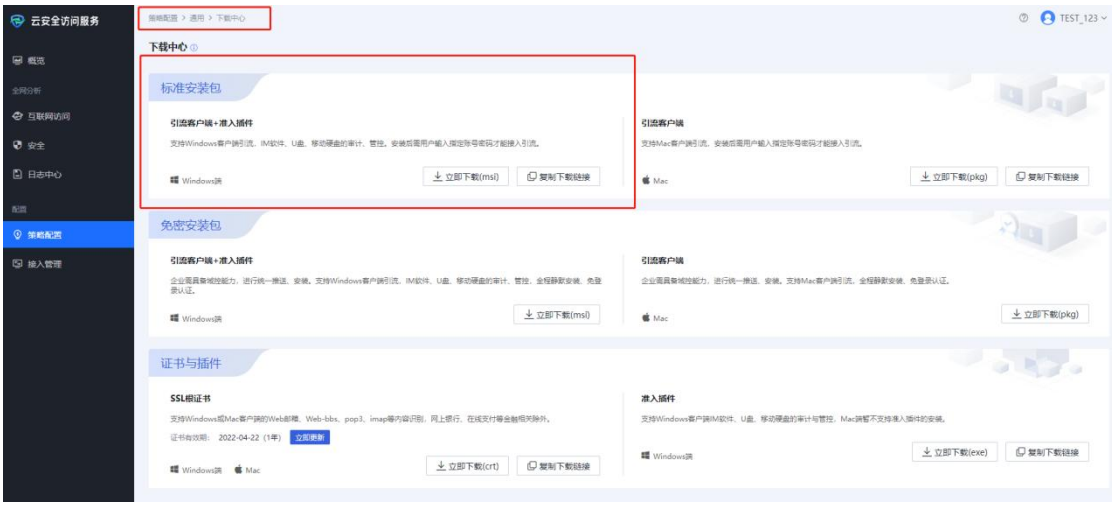
3.1 部署 PC 端软件

登录云图，选择产品服务页面，找到【云安全访问服务】“点击进入”。

（1）接入管理-->用户管理，点击新增，定义**账号密码**



（2）策略配置-->通用-->下载中心，选择“标准安装包”点击下载，双击安装



（3）安装后到达登录页面，使用（1）中的自定义的账号密码登录

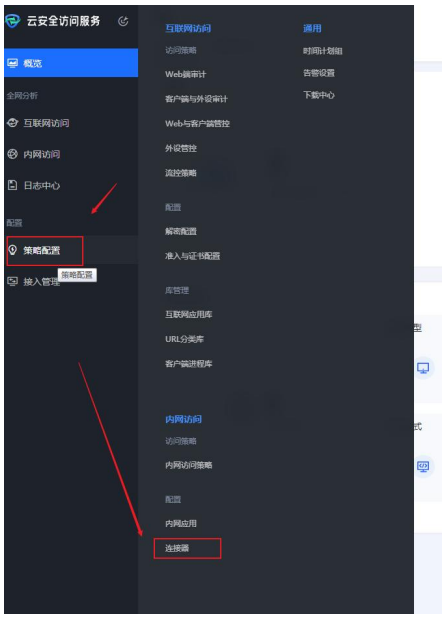
（4）【成功标志1】登录成功后，首页看到用户在线

【成功标志2】 PC使用浏览器打开http://127.0.0.1:30001/也可以查看到客户端接

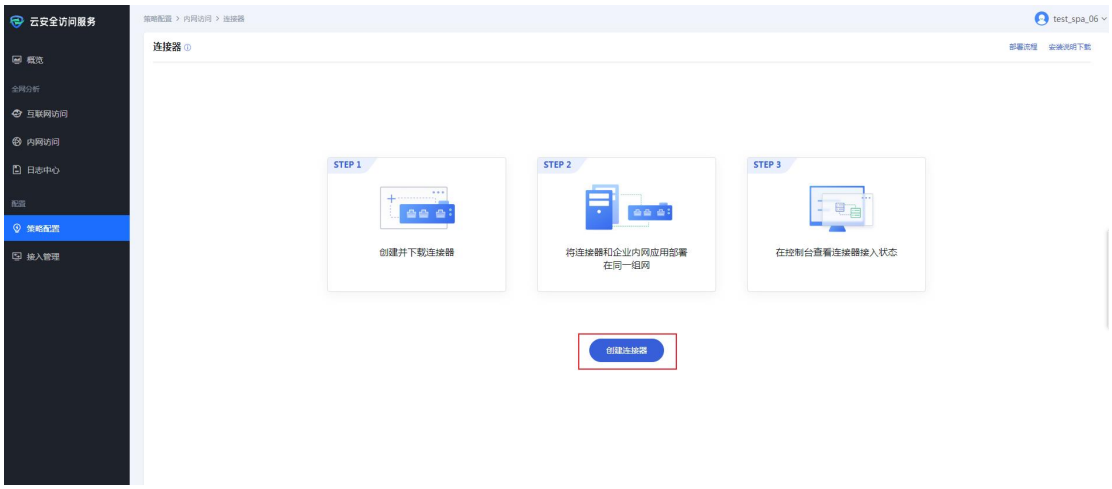
入情况，并且可以在这个页面重新登录或者临时注销

3.1 部署连接器

（1）进入导航-->策略配置-->连接器



首次进入连接器功能页面如下图，点击创建连接器



（2）弹出新增连接器输入框，连接器名称输入“newcon” （名字可任取）

（3）新增成功后即可看到我们新增的连接器“newcon”，除了连接器名称，还有软件版本、关联应用数量、操作（下载连接器、删除）

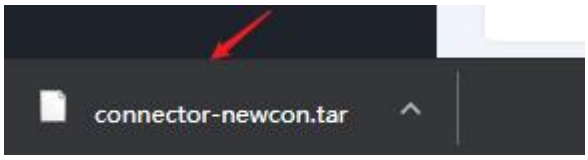
（4）点击操作中的下载连接器

等待下载完成后，将刚下载的压缩包，导入提前准备的服务器中

注：

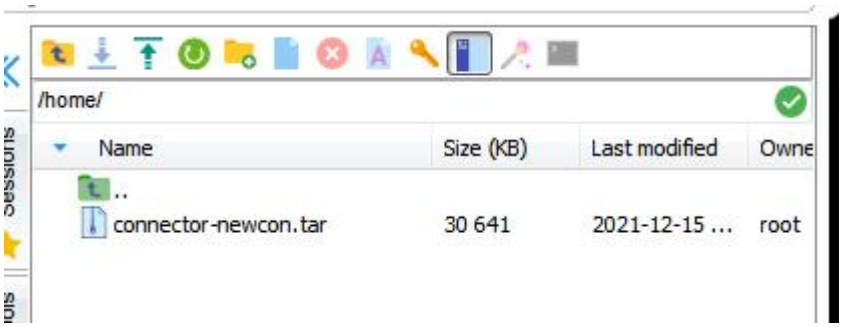
（1）服务器版本要求：centos 7.9 及以上；ubuntu 支持 5.2.1 及以上（建议 ubuntu-16.04.7）；目前仅支持 64 位系统

（2）服务器硬件要求：4 核 8G 起



（5）上传安装包

将连接器安装包上传到 Linux 服务器，放在 /home 路径下。

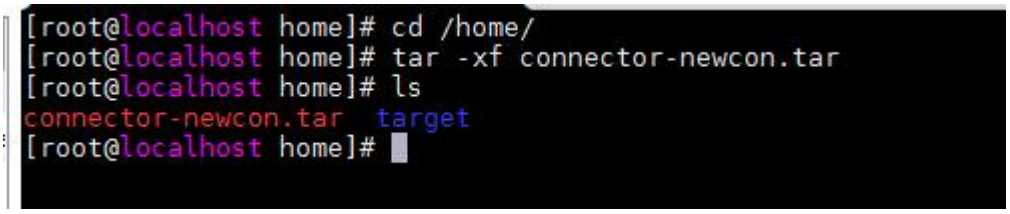


（6）解压安装包

输入命令：cd /home

输入命令：tar -xf connector-xxx.tar （xxx 为连接器名称）输入命令：ls

示例：



（7）进入安装目录

输入命令：cd target

输入命令：ls

示例：

```
[root@centos8base testConn]# cd target
[root@centos8base target]# ls
conf  connector  connector.service  install.sh  mdbg  README.md  update.sh
```

（8）执行安装

输入命令：./install.sh

示例：

```
[root@centos8base target]# ./install.sh
mkdir -p /opt/sangfor/spa-connector/connector/conf
cp -rf ./conf/* /opt/sangfor/spa-connector/connector/conf/
```

（9）安装成功

查看连接器运行状态，状态为 active(running) 表示安装成功。

输入命令：systemctl status connector

```
[root@centos8base target]# systemctl status connector
● connector.service
   Loaded: loaded (/etc/systemd/system/connector.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-12-10 22:34:35 CST; 15s ago
 Main PID: 3961034 (connector)
    Tasks: 8 (limit: 49514)
   Memory: 18.3M
   CGroup: /system.slice/connector.service
           └─3961034 /opt/sangfor/spa-connector/connector/connector

Dec 10 22:34:35 centos8base systemd[1]: Starting connector.service...
Dec 10 22:34:35 centos8base systemd[1]: Started connector.service.
```

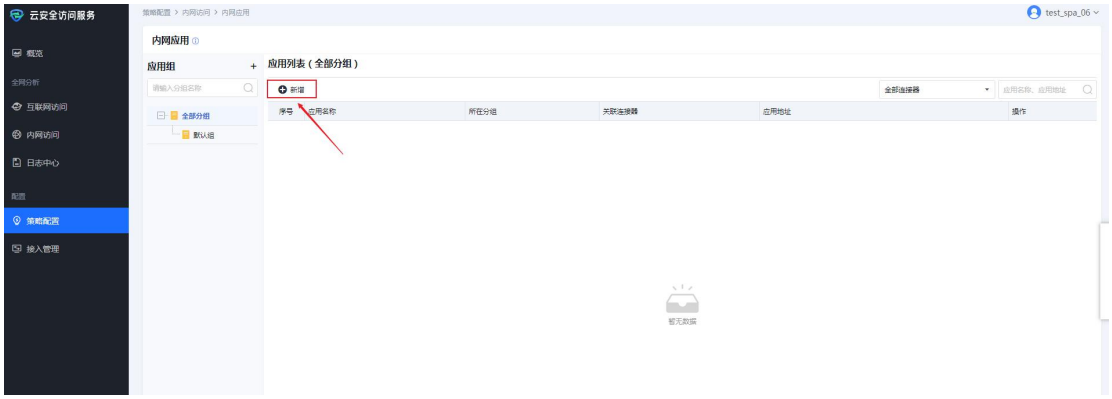
4. SASE-VPN 策略配置

4.1 内网应用管理

功能 1：新增内网应用

使用 SPA 租户登录租户平台，进入导航》策略配置》配置》内网应用

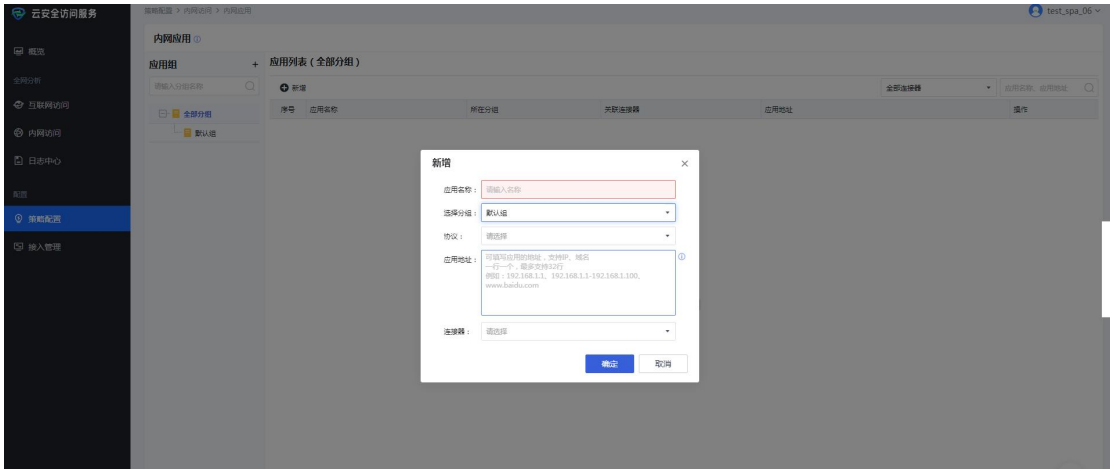
进入内网应用配置界面，点击新增



弹出新增界面输入

应用名称：任意取名

选择分组：默认为默认组；如需要选择其他分组需要手动先创建分组，创建分组方法可以参考功能 2：创建分组



协议：支持 http、https、tcp、udp 协议；http 协议默认端口 80、https 默认端口为 443；选择 tcp 和 udp 协议支持自定义端口号

应用地址：支持配置 iP、ip 端 或域名；如选择协议为 tcp 及 udp 协议，则不支持配置域名

端口：一行输入一个，最多可支持 128 行，支持设定端口范围，如 1-65535；（注：仅在协议选择 tcp 或 udp 时展示）

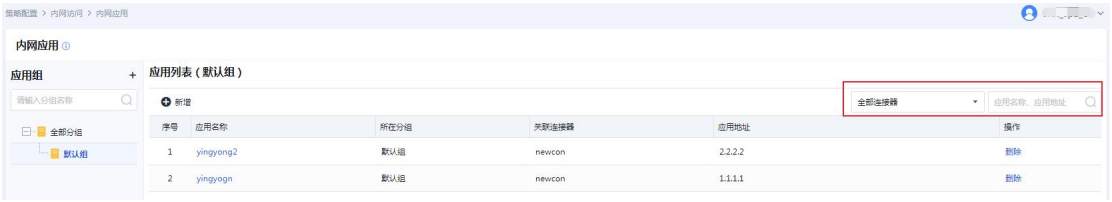
连接器：选择我们刚创建的连接器即可

功能 2：创建分组

点击应用组右边“+”即可新增分组

功能 3：搜索内网应用

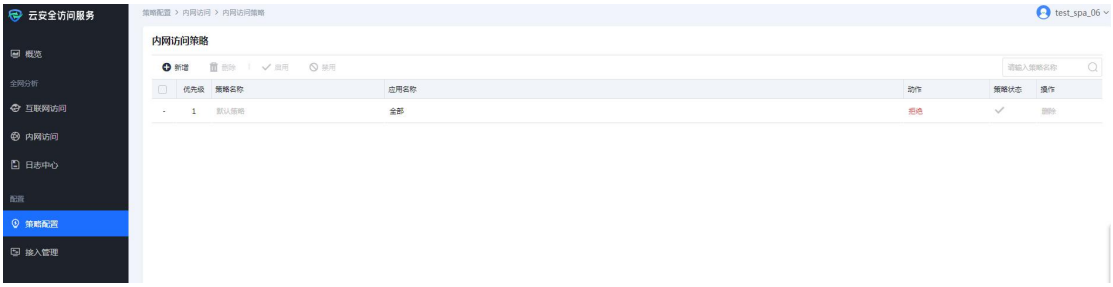
支持通过选择指定连接器或全部连接器，输入应用名称或应用地址检索内网应用



4.2 内网访问策略

功能 1：添加内网访问策略

使用 SPA 租户登录租户平台，进入导航》策略配置》内网访问》内网访问策略界面



点击新增，填写策略信息

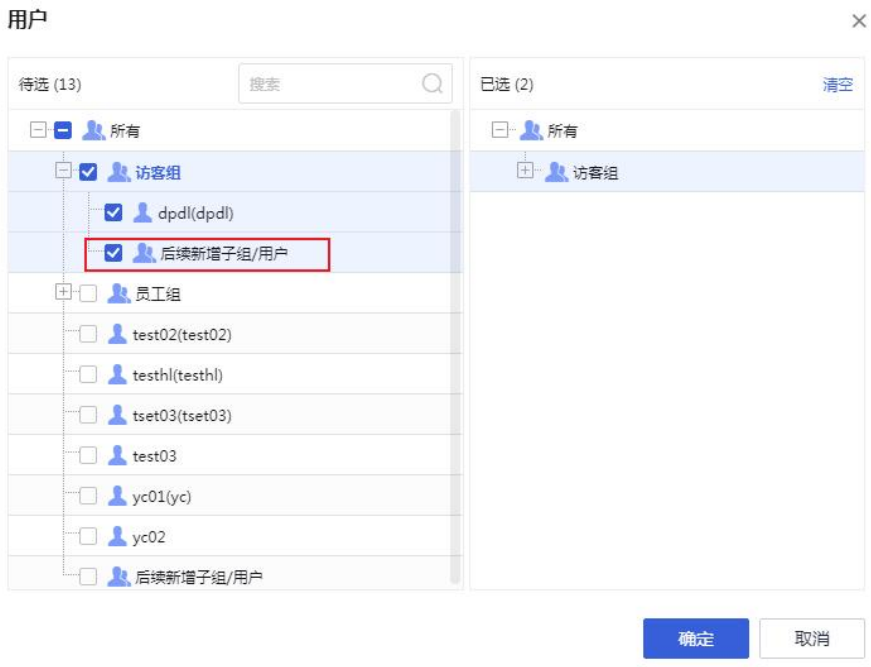
策略名称：任取，支持中英数字，最长字符数；

描述信息：按需选填；

启/禁用：选择启用，即为启用这条访问策略；选择禁用即为禁用此策略，策略不生效；

动作：选择允许，即允许此策略的适用用户访问选择的内网应用；选择拒绝，即不允许此策略的适用用户访问选择的内网应用；

适用用户：选择指定的用户，支持选择单用户、多用户及用户组；当你选择后续新增子组/用户项，如下选择访客组后续新增子组/用户，后续在访客组中新增的用户及分组都会自动继承该访问策略



选择应用：支持选个单个应用、多个应用、应用组；

注：如下图，当你全选默认组的内网应用，后续在默认组中新增的应用自动继承该访问策略

注：内网访问策略中存在一条默认策略，默认禁止所有用户访问，

功能 2：优先级

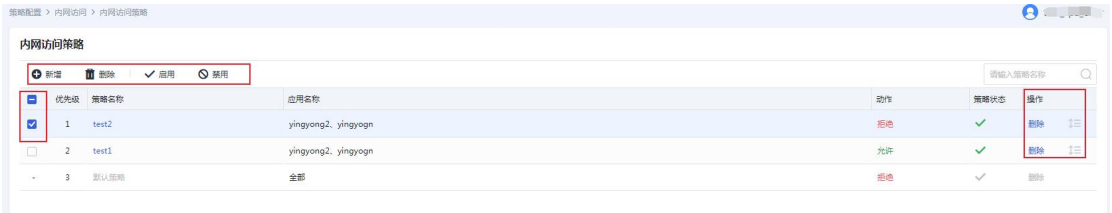
当你内网访问策略同时设置多条访问策略时，优先执行的访问策略优先级 1 的访问策略

可以通过拖拽操作列项中的 修改访问策略优先级

注：无法修改默认访问策略的优先级

功能 3：编辑策略

可以通过勾选访问策略进行编辑操作，或点击策略名称进行编辑修改访问策略

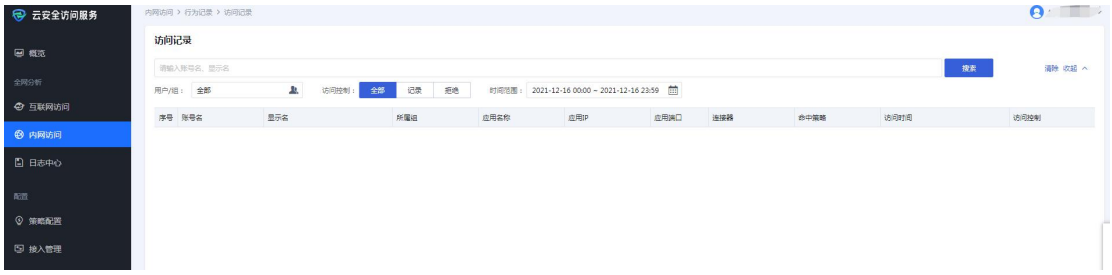


4.3 内网访问日志

功能 1：查看内网访问日志

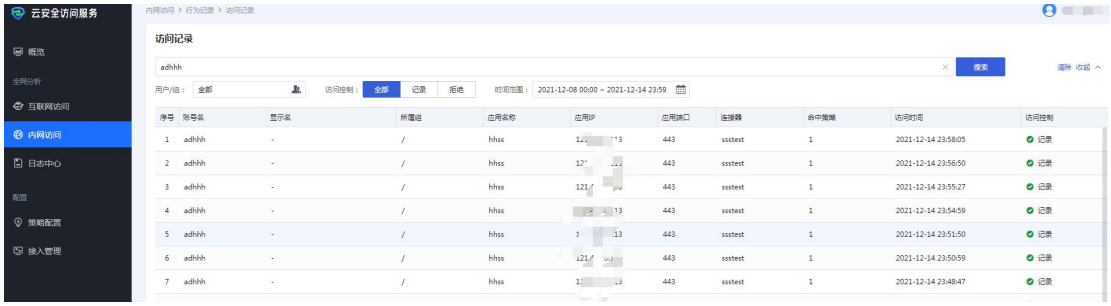
进入导航》内网访问》行为记录》访问记录

可以查看用户访问内网应用的记录



功能 2：筛选日志

支持通过输入框输入账号名、显示名检索指定用户的内网访问日志

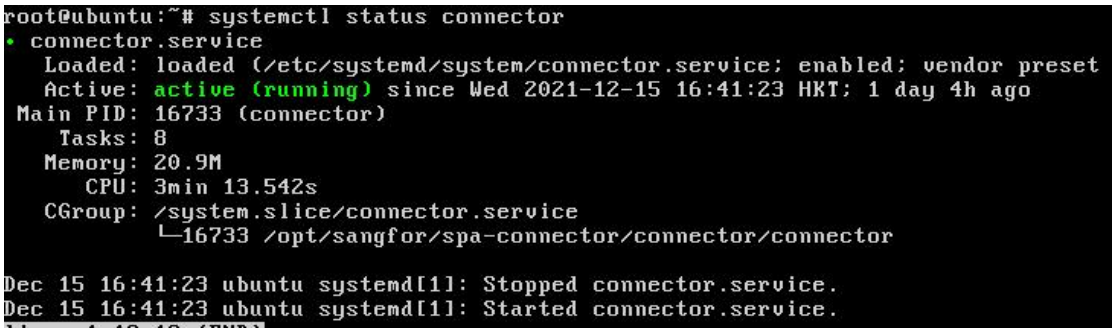


通过用户/组、访问控制、时间范围筛选日志

5.常见连接器排障方法

FAQ 1:如何查看连接器是否正常

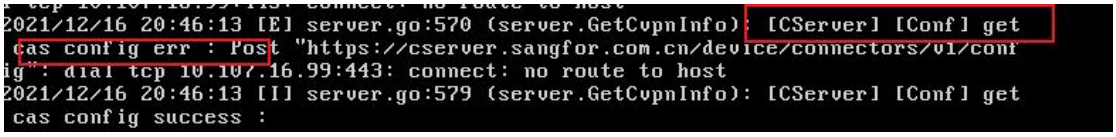
（1）执行 systemctl status connetor，查看状态是否正常，显示 active （running）即为正常



（2）查看连接器日志

执行 tail -100f /var/logs/spa/connector/conns.log

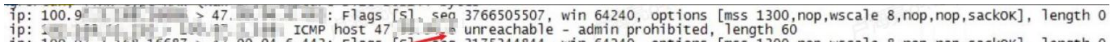
检查是否与 CServer 连接器异常，如提示 get cas config err；检查域名 cserver.sangfor.com.cn 是否能 ping 通



FAQ 2:内网应用无法访问，连接器能抓到包但没有回包

（1）在连接器执行：tcpdump -i sangfortun -nne host 目的 IP

查看提示 unreachable



（2）检查 iptables；回包被 iptables 拦截

执行：iptables -t nat -F 删除 nat 表所有规则即可解决

注意：注意备份手动添加的 iptables 规则

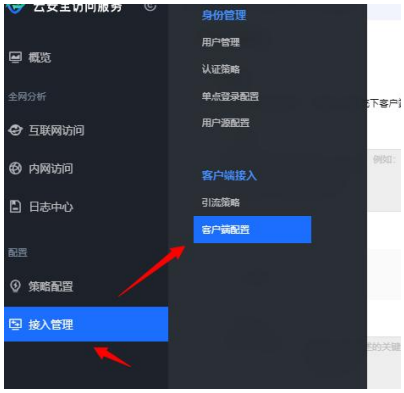
FAQ 3:内网应用无法访问，连接器无法抓到包

（1）检查租户是否开通了多个 POP 节点

（2）通过访问百度搜索 ip；查看当前 ip 归属地，确认当前归属地的 pop 节点是否上线 SPA 业务

FAQ 4:内部应用域名引流失败

（1）域名引流需要手动在 sase 平台开启 DNS 引流；开启路径：导航》接入管理》高级设置；找到开启 DNS 引流



FAQ5:服务器回包到了连接器物理网口没有回到sangfortun口

（1）需要开启服务器转发功能，开启命令是：iptables -P FORWARD ACCEPT