深信服零信任 aTrust 华为公有云

部署手册

产品版本	2.1.3 及以上
文档版本	02
发布日期	2021-09-04

深信服科技股份有限公司

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

联系我们

售前咨询热线：400-860-6868

售后服务热线：400-630-6430 （中国大陆）

香港：(+852) 3427 9160

英国：(+44) 8455 332 371

新加坡：(+65) 9189 3267

马来西亚：(+60) 3 2201 0192

泰国：(+66) 2 254 5884

印尼：(+62) 21 5695 0789

您也可以访问深信服科技官方网站：www.sangfor.com.cn获得最新技术和产品信息

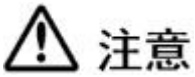
修订记录

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。

日期	文档版本	修改内容
2021-09-04	02	本文当格式优化。

符号说明

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。。
	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[ ]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“< >”	单击<确定>按钮。

目录

1. 概述

本文介绍了如何在华为公有云平台部署零信任aTrust控制中心SDPC和代理网关Proxy的安装、部署、联动和集群组建等。

现场环境准备：

1. 非集群环境

- 准备好 qcow2 格式的 aTrust 基础镜像包，并下载好最新版本文件。
- 客户环境准备好足够的钱租用虚拟机，配置最低为 8 核 16G500G。
- 给 aTrust 控制中心和代理网关分配网络地址。

2. 控制中心集群部署环境

- 准备好 qcow2 格式的 aTrust 基础镜像包，并下载好最新版本文件。
- 客户环境准备好足够的钱租用虚拟机，配置最低为 8 核 16G500G。
- 给 aTrust 控制中心和代理网关分配网络地址。

1.1. 环境准备

1.1.1. 非集群环境

- 准备好 qcow2 格式的 aTrust 基础镜像包，并下载好最新版本文件。
- 客户环境准备足够的钱租用 ECS 云服务器和公网地址，云服务器配置为
  - 4 核 8G 500G 系统盘
  - 8 核 16G 500G 系统盘
- 1 个 VPC 专有网络和子网，给 aTrust 控制中心和代理网关分配业务网络地址。

安全组策略如下：

入站规则	说明
4433 端口	控制中心和代理网关控制台运维管理端口
443 端口	控制中心：用户接入认证和鉴权端口 代理网关：用户访问 web 应用所需端口 443 端口可改，控制中心和代理网关的 443 可更改为其它端口。
441 端口	隧道应用端口
22 端口	控制中心和代理网关后台运维、升级端口

出站规则	说明
默认全放通	建议规则做全放通，也可根据客户业务情况配置规则

- 端口映射：

设备	端口说明
控制中心	需映射 443 端口到外网做远程用户接入认证用，端口可改
代理网关	映射 441 端口用户访问隧道应用，不可改 映射 443 端口用户访问 web 应用，可改
外网远程接入环境下，控制中心和代理网关都需映射 4433 和 22 端口，做设备前期部署功能。后续可通过 aTrust 平台使用隧道应用域名形式发布运维。	

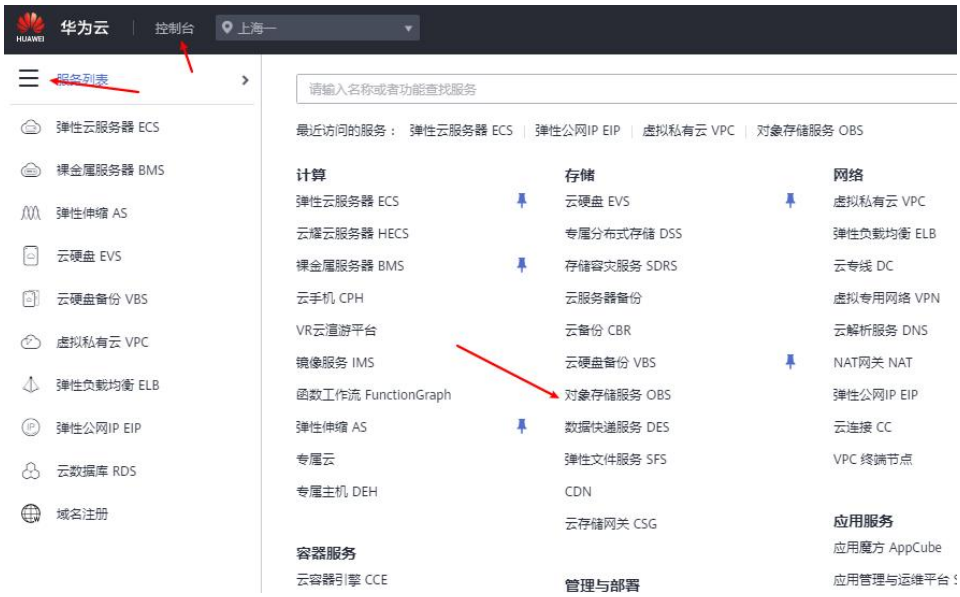
2. 设备部署

介绍零信任aTrust VPN网关华为公有云平台部署安装。

2.1. 镜像上传-自行获取镜像上传

2.1.1 上传镜像

1. 用户登录华为云，在[控制台/对象存储服务OBS]。



2. 创建存储桶

步骤1. 用户登录成功后，在[对象存储服务/对象存储]进入已创建的存储桶或点击<创建桶>新建存储桶，此处选择新创建存储桶。

⚠ 注意：

此处注意存储桶的地域选择，所有的操作都需在相同的地域操作，否则将服务器将无法读取和创建。

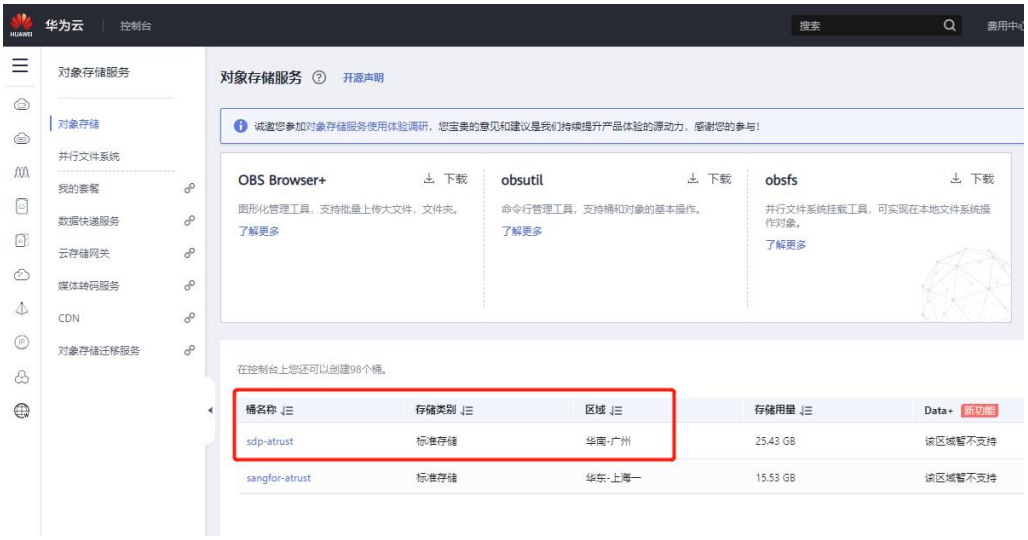
步骤2. 点击<确定>完成存储桶的创建。

步骤3. 将aTrust控制中心和代理网关的镜像，上传至新建的存储桶。点击新创建的存储，进入存储桶界面，点击<上传文件>。此时无法正常上传，需借用华为OBS Browser+工具完成镜像上传。

📖 说明：

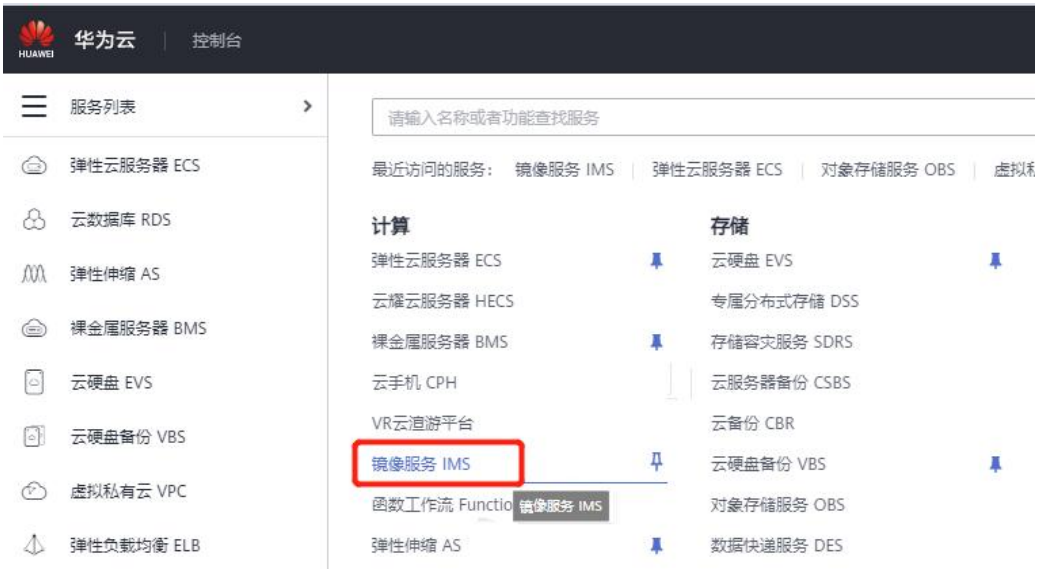
因 aTrust 控制中心和代理网关的 qcow2 镜像大于 5G，无法使用云平台直接上传至平台。可下载使用华为的 OBS Browser+工具进行上传，具体操作步骤见如下附件。

步骤4. 使用华为OBS Browser+工具上传完成镜像后，可在华为云平台对应的存储桶查看到上传的控制中心和代理网关镜像文件。

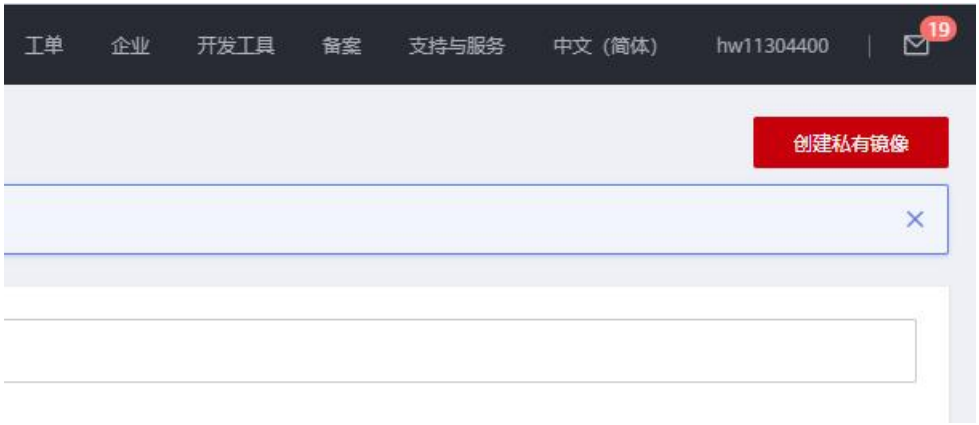


2.1.2 镜像制作

步骤1. 在服务列表选择镜像服务。



步骤2. 步骤3.进入镜像服务 IMS页面，右上角点击<创建私有镜像>。

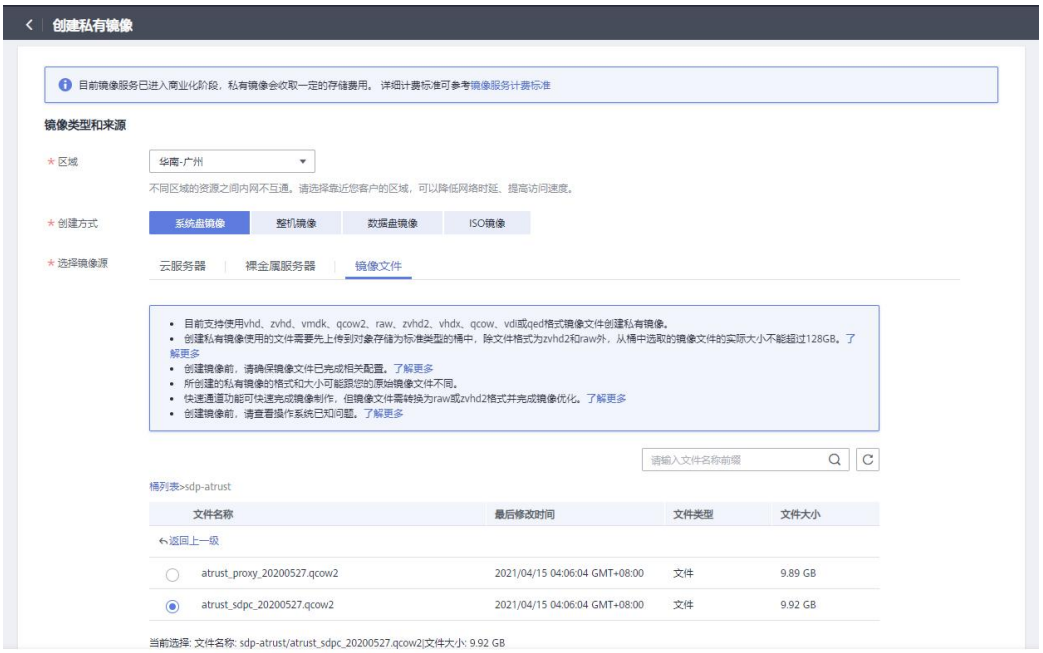


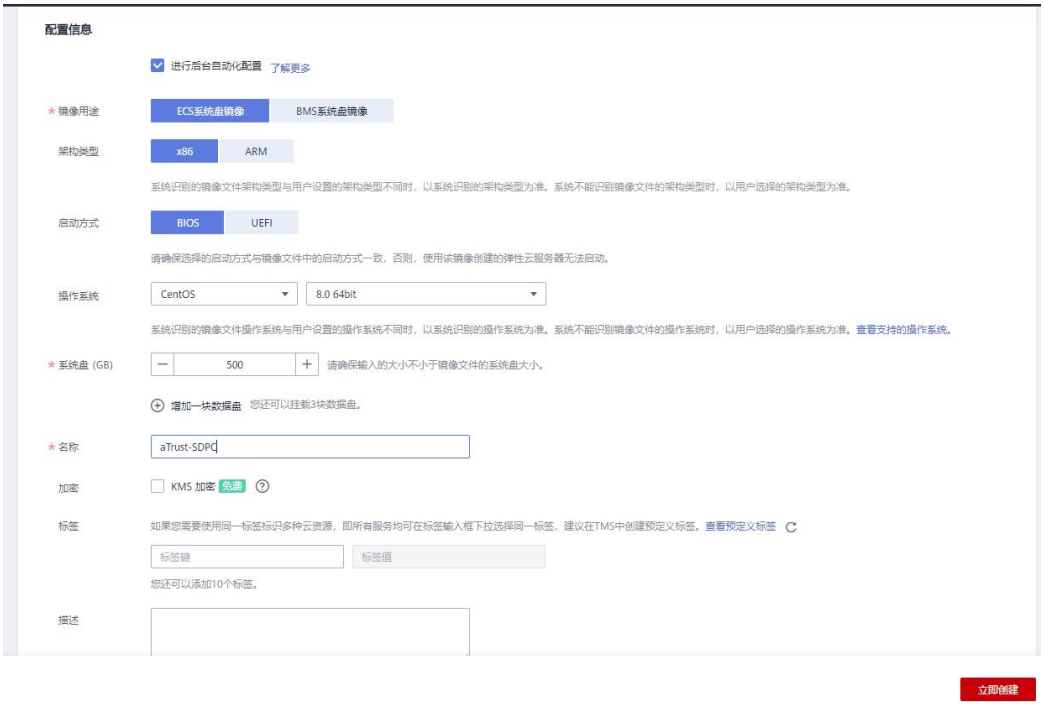
步骤3. 进入私有镜像配置页面，按需配置相关项，点击<立即创建>完成镜像配置。

区域：选择与存储桶所在的区域一致。

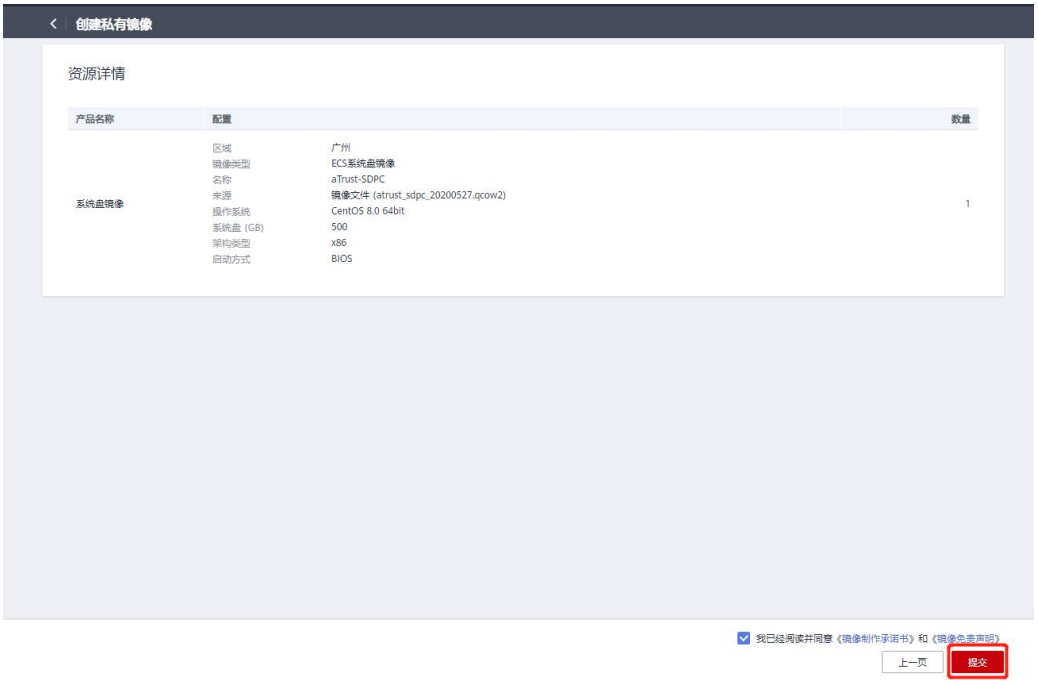
创建方式：选择系统盘镜像。

选择镜像源：选择镜像文件，选择上传的对应镜像文件。





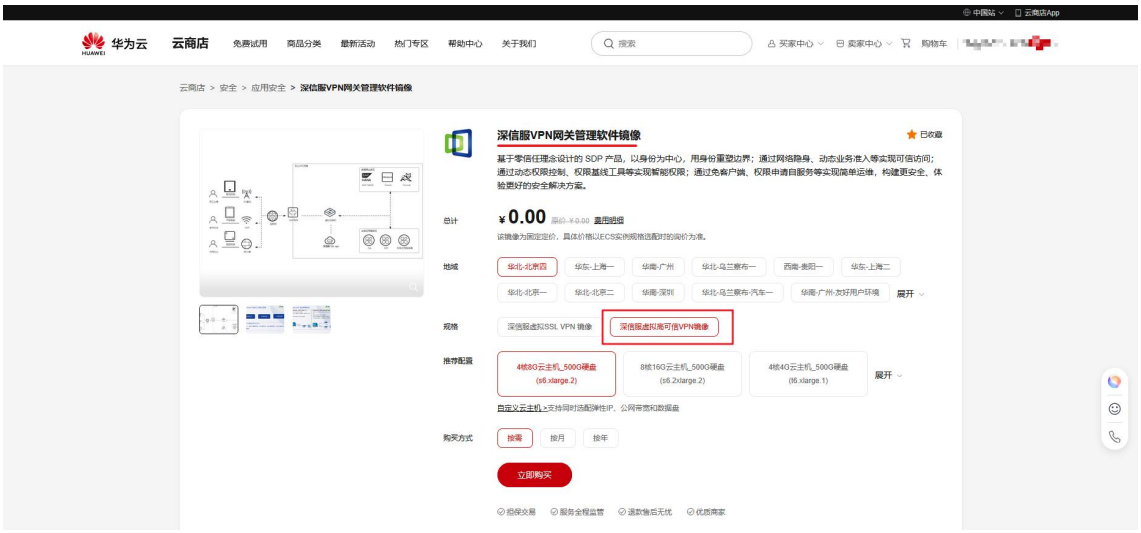
步骤4. 点击提交完成镜像创建



2.2. 使用市场镜像

深信服aTrust零信任VPN已上传至市场镜像，访问华为云市场搜索VPN管理软件

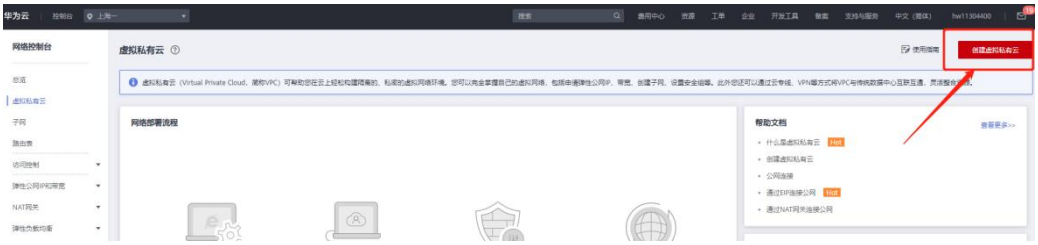
https://marketplace.huaweicloud.com/contents/5a4e4795-c116-4536-885a-4a611a1a8192#productid=OFFI1127135378533625856



2.3. 创建虚拟私有云 VPC

步骤1. 进入控制台，在服务列表项点击虚拟私有云VPC。

步骤2. 点击<创建虚拟私有云>。



步骤3. 完成虚拟私有网络的配置，点击<确定>完成配置。

区域：选择与之前选择的区域一致。

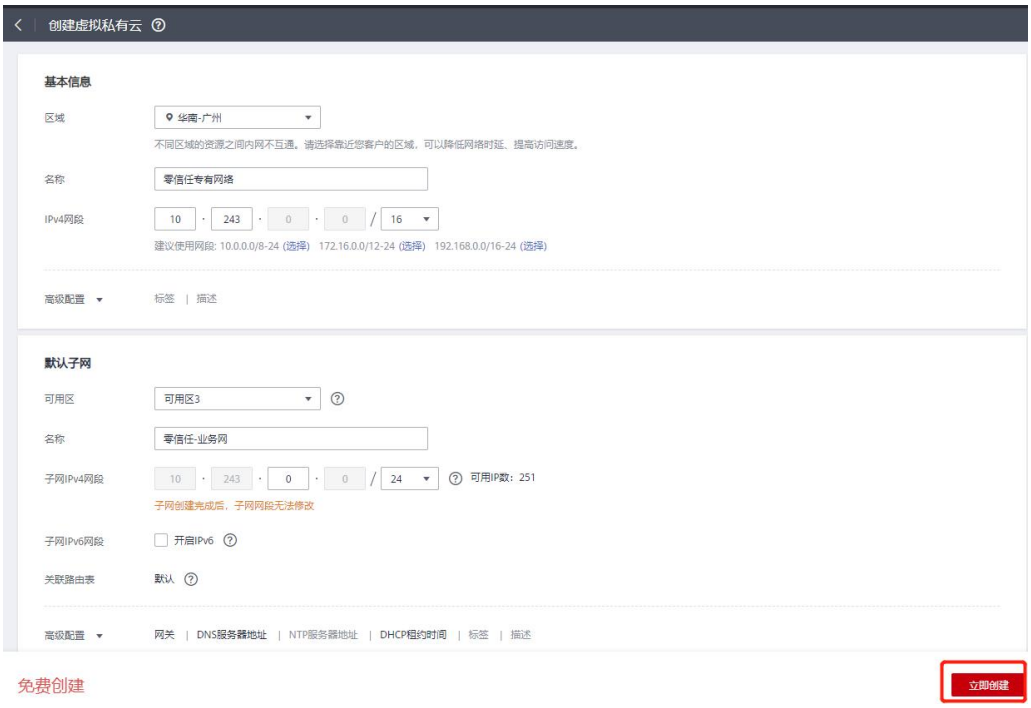
名称：设置改私有云网络的名称。

ipv4网段：设置私有云网络的业务网段。

可用区：根据实际业务选择，可默认。

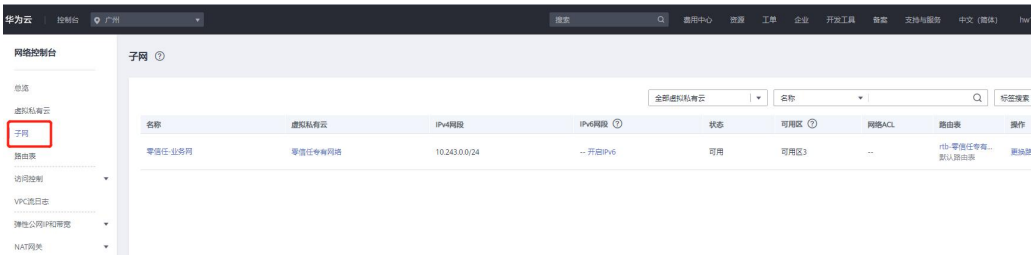
名称：可根据子网承载的业务类型进行设置。

子网IPV4：设置子网所在的网络网段。



步骤4. 完成创建后，可在页面查看到对应的私有云网段。

步骤5. 点击子网，可查看到新建的子网信息。

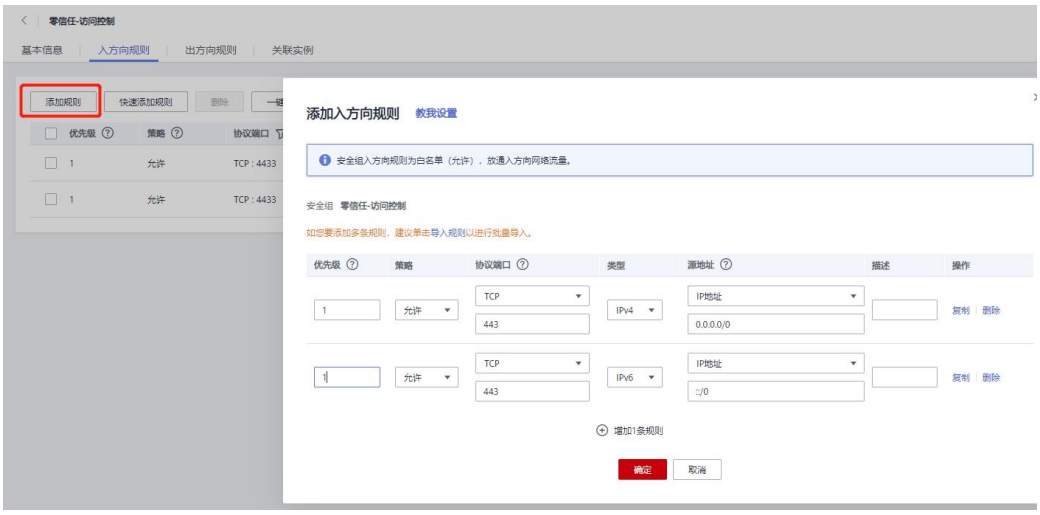


2.4. 安全组

步骤1. 在[网络控制台/访问控制/安全组]点击<创建安全组>，配置安全组相关信息包括名称和模板（选择自定义）。

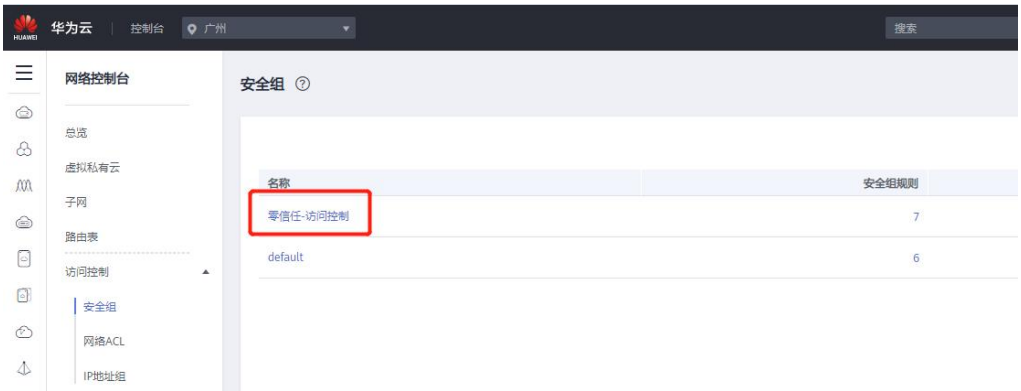
步骤2. 点击确定后，提示配置安全组规则，点击配置规则，进入配置页面。

步骤3. 配置入方向规则，放通设备的22/443/441/4433/442（其中442和4433是集群组建所需端口）端口，源地址建议添加ipv4和ipv6的所有地址。



步骤4. 配置出方向规则，可配置为默认全放通。

步骤5. 完成上述配置后，可在安全组页面查看到新建的安全组。

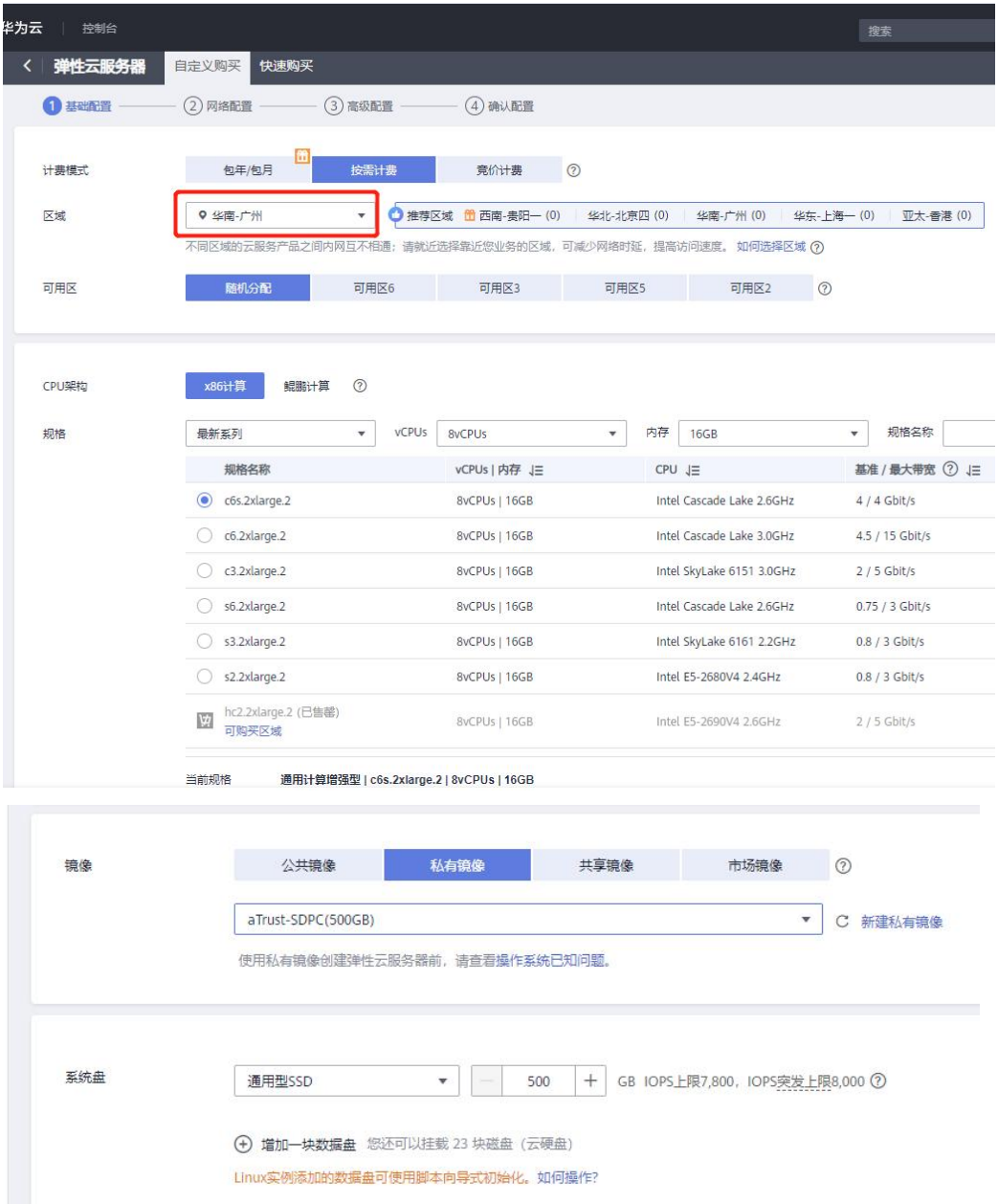


2.5. 创建弹性云服务器

步骤1. 点击控制台选择弹性云服务器ECS。

步骤2. 进入弹性云服务器ECS页面，点击右上角<购买弹性云服务器>。

步骤3. 在[自定义购买/基础配置]选择区域、规格、镜像，区域和镜像所在区域一致，规格要保证满足可扩展3张网卡，服务器配置为8核16G500G。



步骤4. 点击下一步，配置服务器网络配置

网络：选择为零信任配置的业务网段

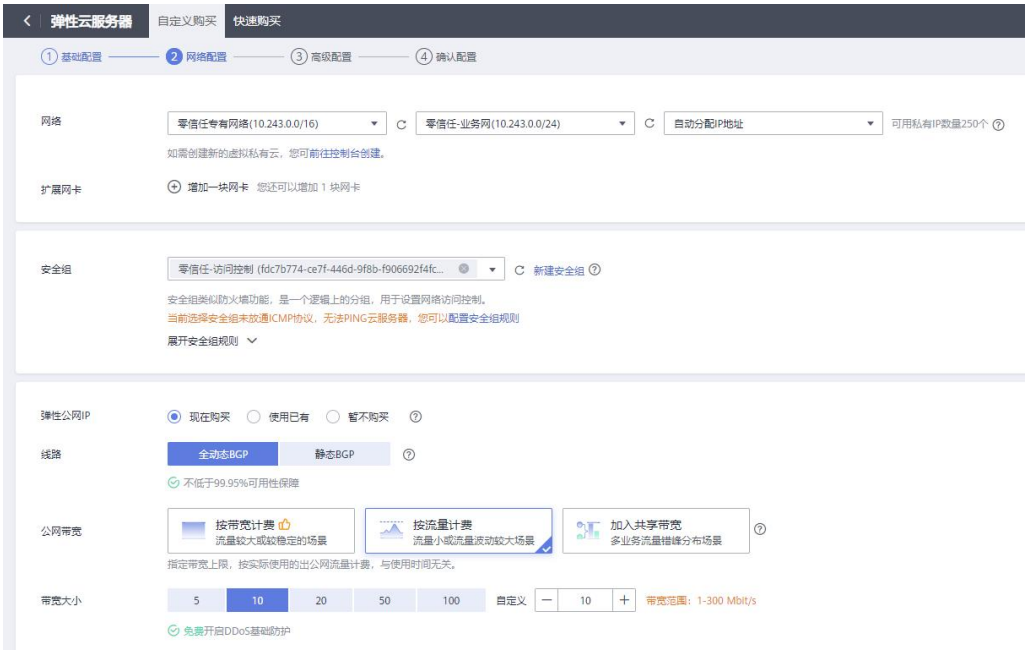
安全组：选择对应的零信任安全组。

弹性公网IP：选择现在勾选，可直接给云服务器分配对应的公网IP地址，用户访问云服务器时在外网直接输入分配的公网地址即可。

公网带宽和带宽大小可按实际需求进行配置。

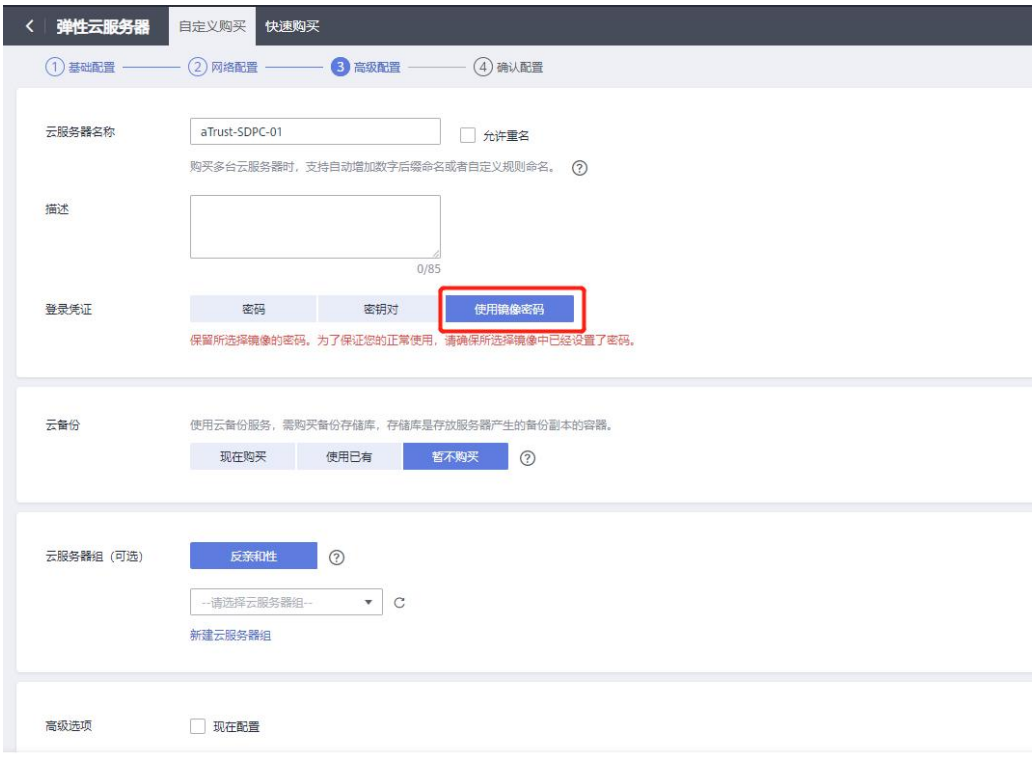
⚠ 注意：

在申请云服务器时，网络和安全组必须提前为分配给零信任设备。弹性公网 IP 可在申请云服务器时一并申请，也可利用现有的弹性公网 IP，也可使用 NAT 网关做端口映射，映射的运维端口为 22 和 4433 端口，用于后续的网络配置和设备部署。



步骤5. 点击<下一步>，完成服务器高级配置

登录凭证：选择使用镜像密码登录设备后台。



步骤6. 点击下一步确认配置，点击立即购买完成配置。

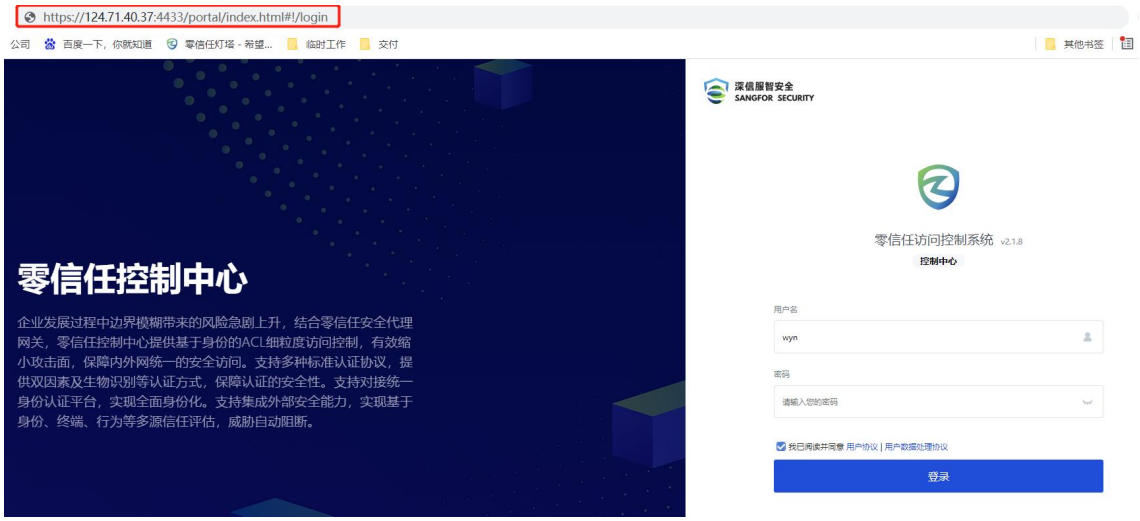
步骤7. 创建成功后，默认会绑定一个弹性公网ip到主网卡。

步骤8. 使用相同的操作，完成另一台控制中心设备和代理网关的配置申请。

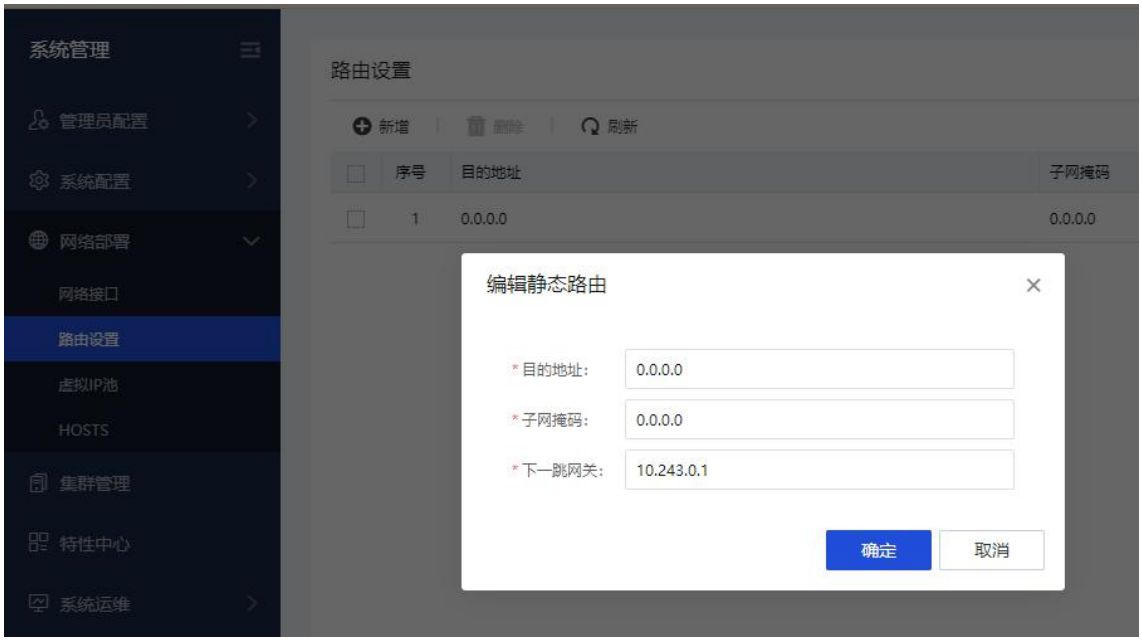
3. aTrust 网络配置

3.1. 配置网络

步骤1. 浏览器使用公网IP（https://124.71.40.37:4433）登录设备控制台，使用默认密码admin/SangforSDP@1220登录设备。



步骤2. 进入[系统管理/网络部署/路由设置]配置设备默认路由。【查看华为云VPC子网网关】



步骤3. 完成设备的默认路由配置后，进入[系统管理/网络部署/网络接口]点击网络名称为<管理口>的接口，进入配置页面完成设备的接口IP地址配置（该地址必须为华为云上分配的私有地址），点击<保存>完成设备网络配置。

步骤4. 完

完成客户端接入配置，进入[系统管理/系统配置/通用配置/客户端接入设置]，配置接入地址、隧道接入地址。

3.2. 设备授权

授权分为测试授权和正式授权

联系云市场商务获取订单激活正式授权

联系云市场商务获取测试授权

3.3. 基本配置

以上步骤即可完成服务端和客户端的部署，本节主要介绍从新增用户到发布资源并进行授权的配置过程。主要的步骤如下：

1、新增用户

2、配置认证策略

3、发布隧道资源

4、给用户授权

3.3.1. 新增用户

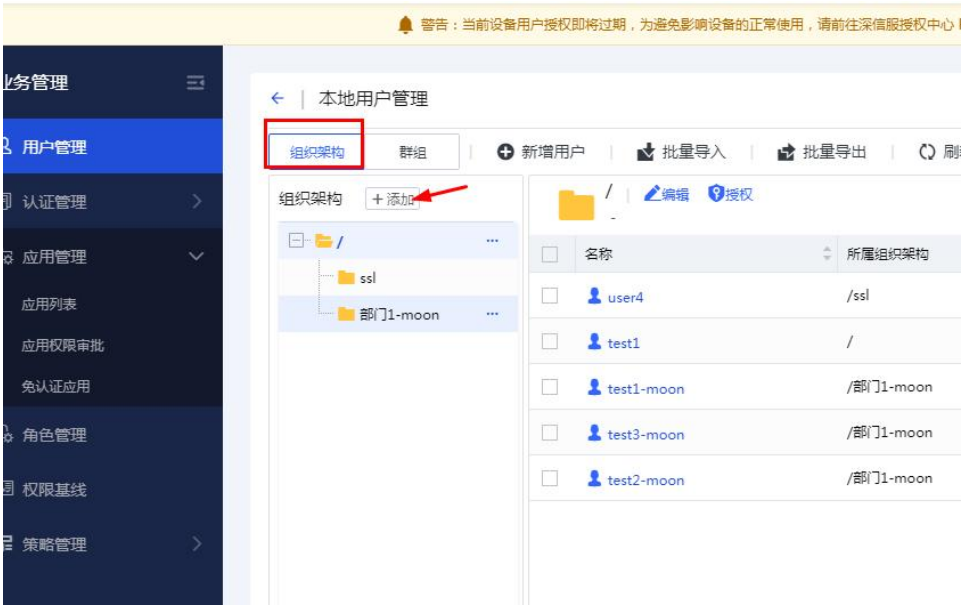
新增用户包含本地和外部用户两种方式，本次以本地用户为例进行介绍。当然部分客户外部已有统一的用户管理系统，此类用户的管理可点击<新增>在页面的右上角查看帮助资料，或参考用户手册链接：

https://support.sangfor.com.cn/productDocument/read?product_id=19&version_id=1008&category_id=270047

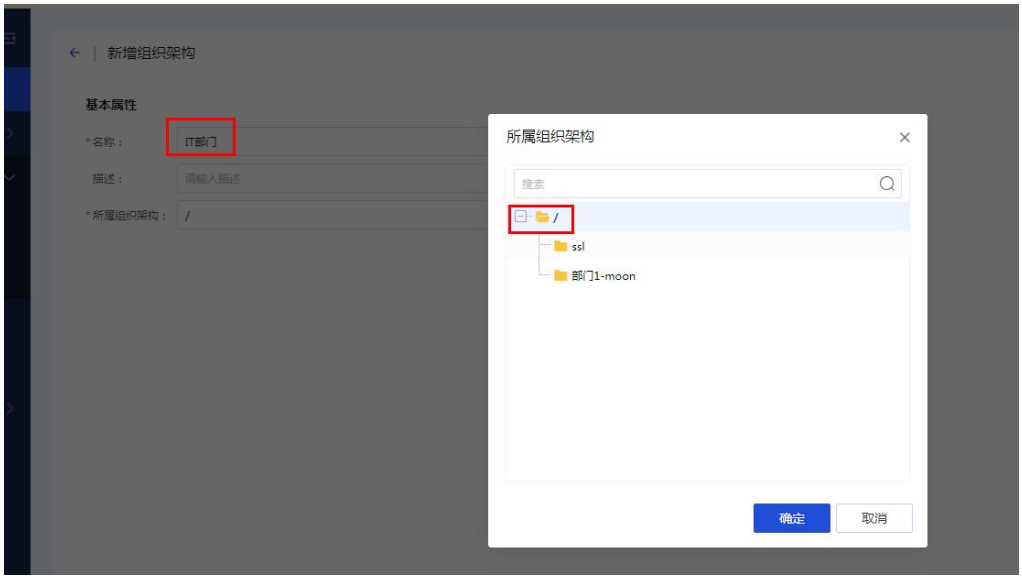
本地用户是指aTrust数据保存在综合网关的用户，认证时通过本地用户列表进行匹配。

步骤一：在[业务管理/用户管理/本地用户目录]点击本地用户目录

步骤二：在组织架构处，点击<+添加>。

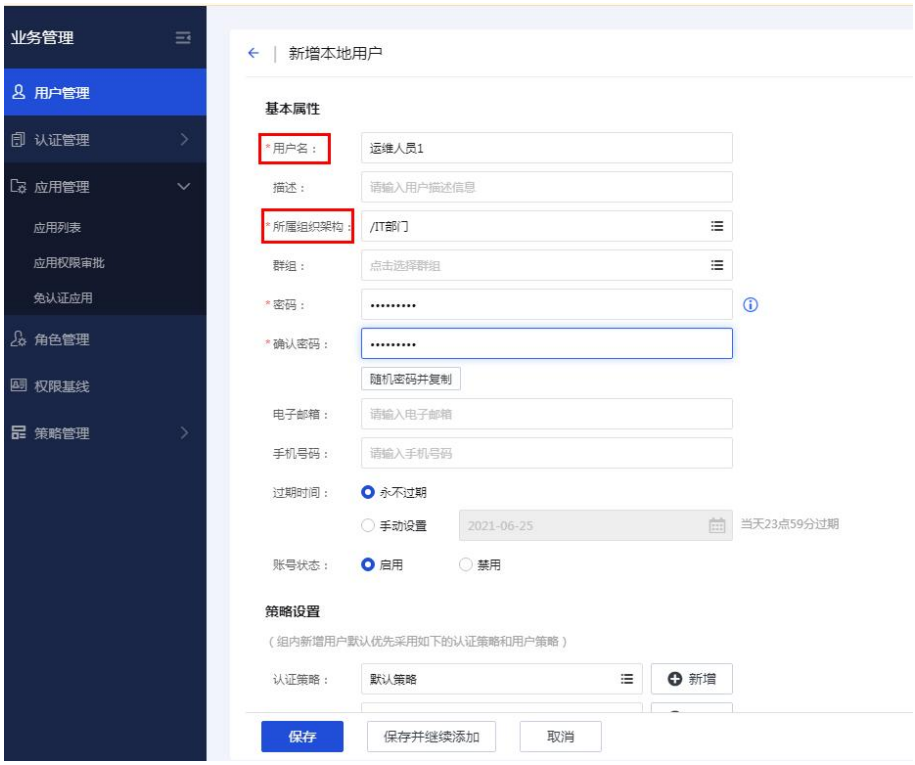


步骤三：本案例新增一个“IT部门”的组织，选择所属的组织架构/目录



步骤四：在[业务管理/用户管理/本地用户目录]本地用户管理，点击<新增>

步骤五：新增一个用户：运维人员1，选择所属的组织架构，配置密码。



步骤六：新增后即可在IT部门组织中看到该运维人员1。

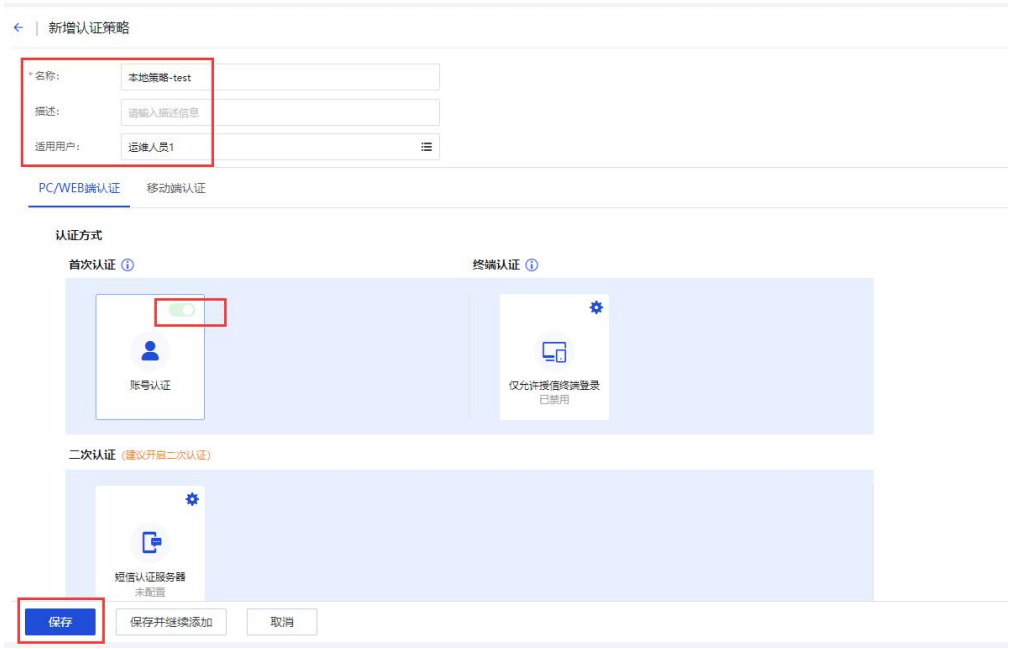
3.3.2. 配置认证策略

用户新增好后则需要配置相应的认证策略，aTrust提供了多种认证方式，为了测试效果下面以本地认证为例，其他认证方式请参考用户手册链接：

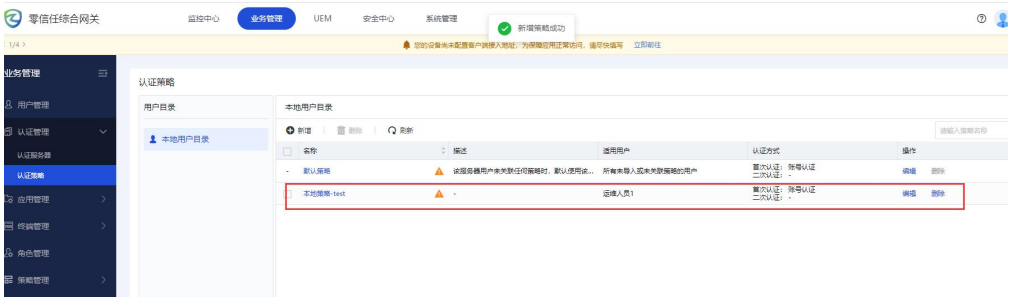
https://support.sangfor.com.cn/productDocument/read?product_id=19&version_id=1008&category_id=270047

步骤1. 在[系统管理/认证策略/本地用户目录]点击<新增>或编辑已有的默认策略。

步骤2. 新建一个认证策略：本地策略-test，适用用户选择运维人员1，然后勾选账号认证，点击保存。



步骤3. 配置成功后即可在认证策略中看到本地策略-test以及适用的用户。



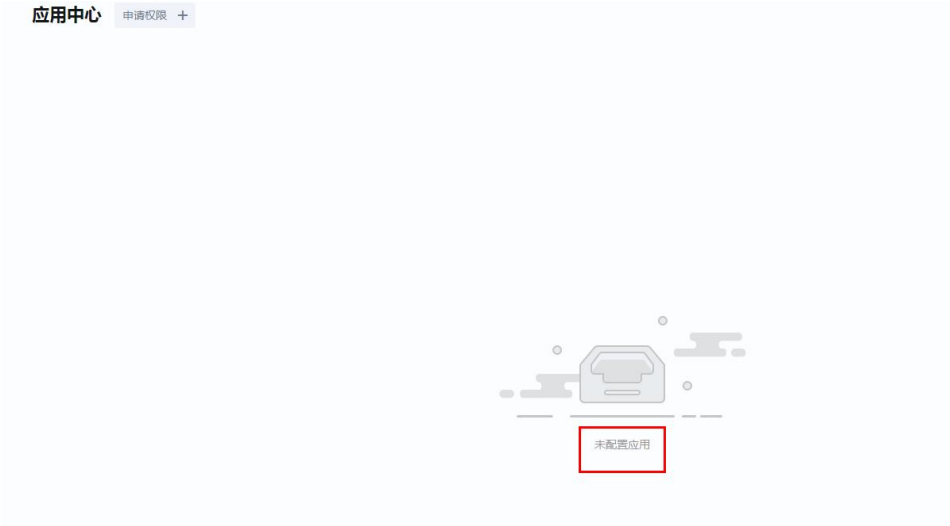
步骤4. 通过登录综合网关认证界面验证用户本地策略是否配置成功。

右键点击atrust客户端，右下角会弹出客户端登录界面，点击前往登录。

在零信任客户端软件的认证界面输入运维人员1的账号密码进行登录。

登录成功则说明认证策略没有问题。

登录后可以发现应用中心为空，因为运维人员1此时并未授权应用。下一步则需要发布隧道资源，然后再授权给该用户。

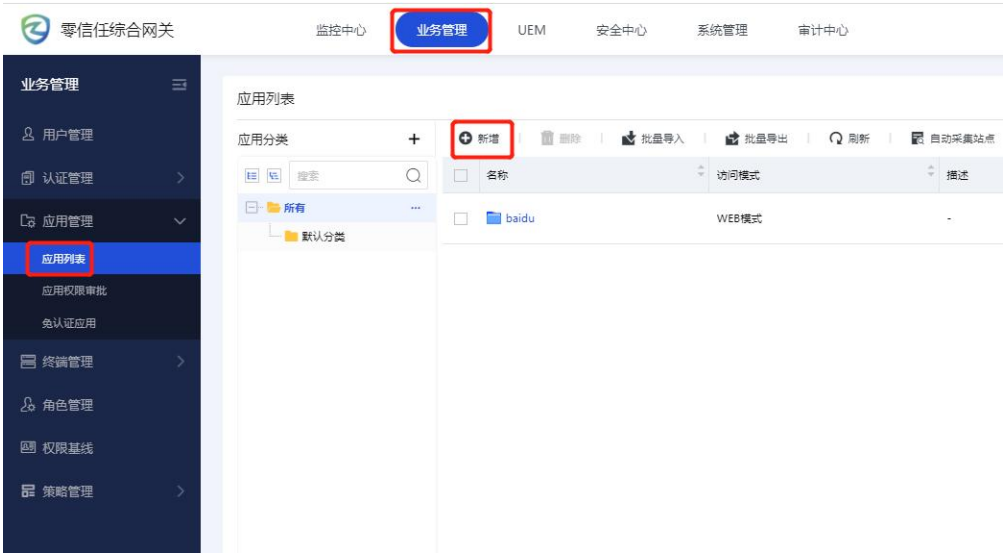


3.3.3. 发布隧道资源

应用的发布分为隧道资源配置和WEB资源配置。隧道方式发布应用更简单快捷，且覆盖的场景也更全面，在大部分场景下，更推荐使用隧道模式发布应用。本次以隧道资源发布为例，如果确实需要采用WEB资源发布的方式，请参考WEB资源配置相关手册，或参考用户手册链接：

https://bbs.sangfor.com.cn/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=158655&highlight=

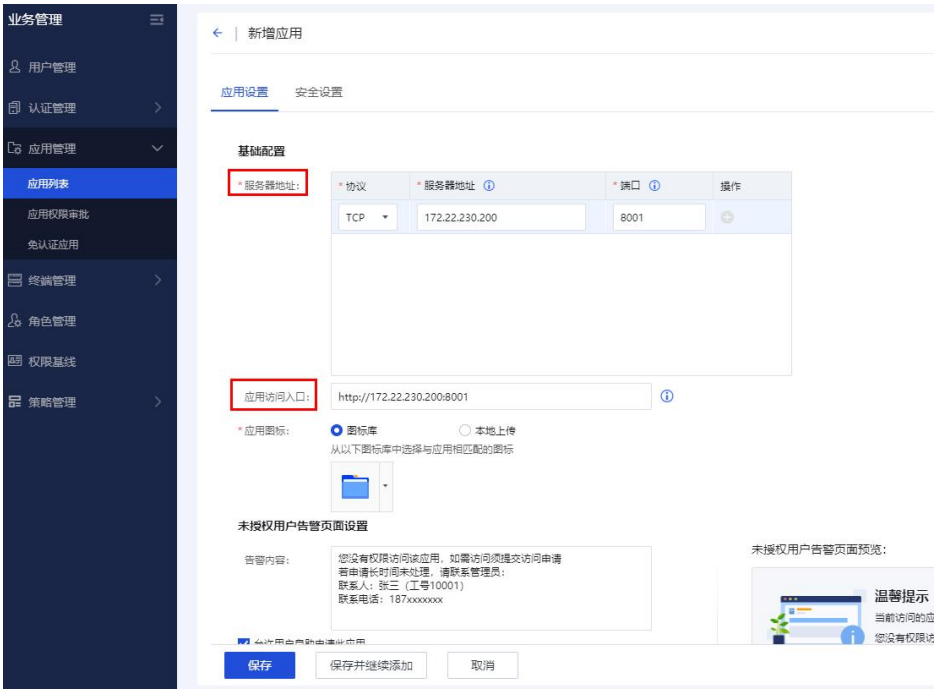
步骤1. 管理进入综合网关的控制台，在[业务管理/应用管理/应用列表]点击<新增>。



步骤2. 根据需要填写应用属性

访问模式选择隧道模式，填写好名称、描述、应用分类、节点区域等信息，应用状态选择启用。

填写定制平台2的服务器地址:172.22.230.200端口8001，应用访问入口地址同样填写：http://172.22.230.200:8001



服务器地址：支持发布通配符、单个IP、IP段和IP范围等资源，端口支持单个端口，多个端口和端口范围。隧道应用支持一个应用里面，配置可多个IP/域名资源应用。

应用访问入口：配置与服务器地址的IP/域名相同，否则可能导致访问出错，配置后可在应用中心点击直接访问。

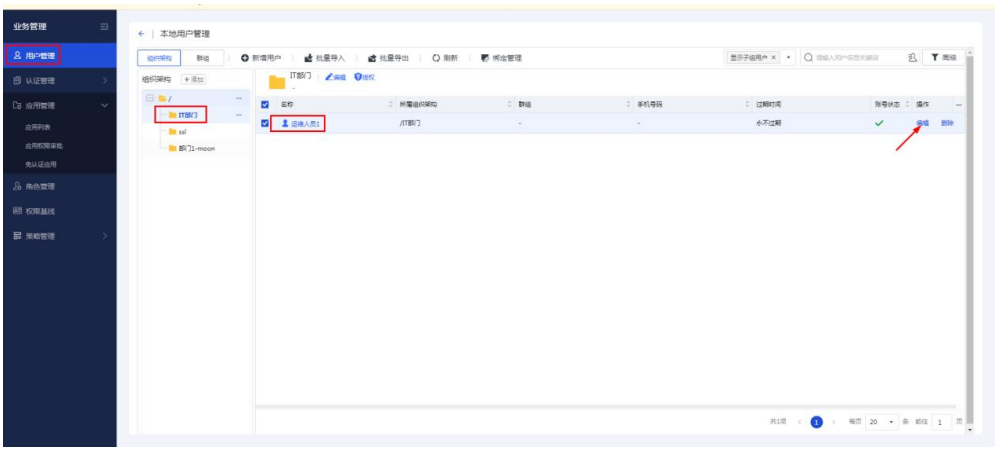
步骤三：填写后保存即可在应用列表看到该发布的资源。

3.3.4. 给用户授权

资源发布后则需要给用户进行授权。用户授权的维度比较多，包括用户、组织架构、群组、角色几个方面，本次为了测试效果以用户的维度进行授权。其他基于组织架构、群组和角色的授权方式请参考用户手册链接：

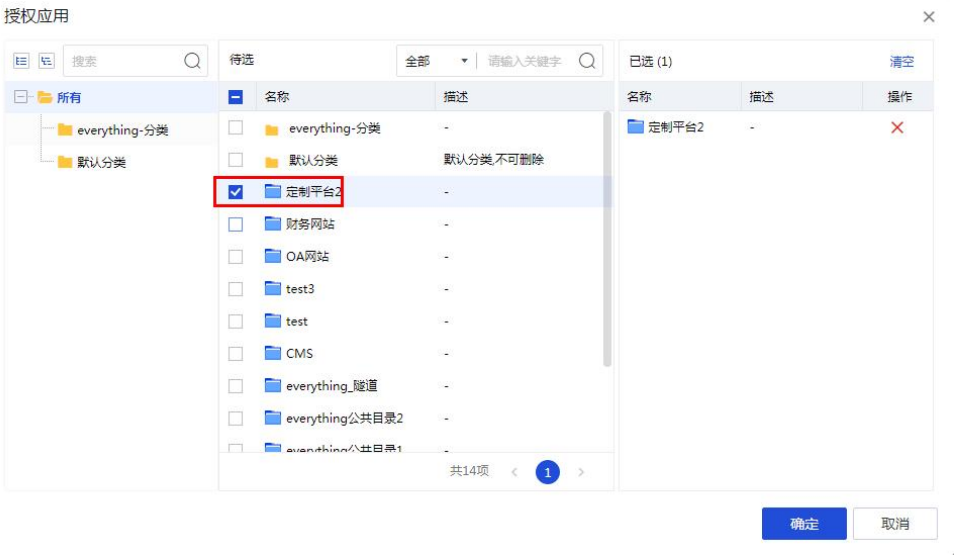
https://bbs.sangfor.com.cn/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=158655&highlight=

步骤1. 在[业务管理/用户管理/IT部门]中选择运维人员1，点击后面的编辑按钮。

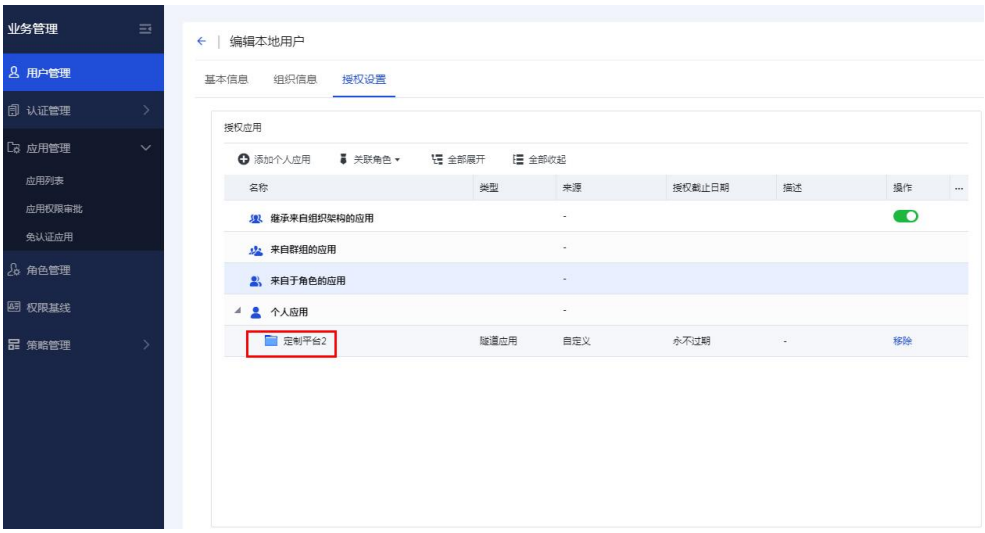


步骤2. 在选择授权设置，然后点击添加个人应用。

步骤3. 在弹出的窗口选择定制平台2。



步骤4. 选择后即可在授权设置中看到该应用已经添加。



至此，用户已配好一个隧道资源并进行了授权，下一步验证配置后的效果。

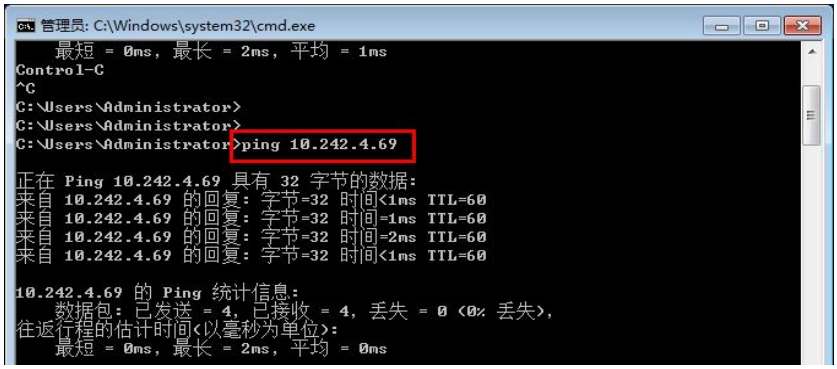
3.3.5. 验证配置效果

前面已经完成用户新增、策略配置、隧道资源发布并且对用户授权，下面验证一下资源访问的效果。验证前，需要确保客户已将访问被保护资源的流量引流到综合网关，包括网络路由的配置以及DNS的解析。验证步骤如下：

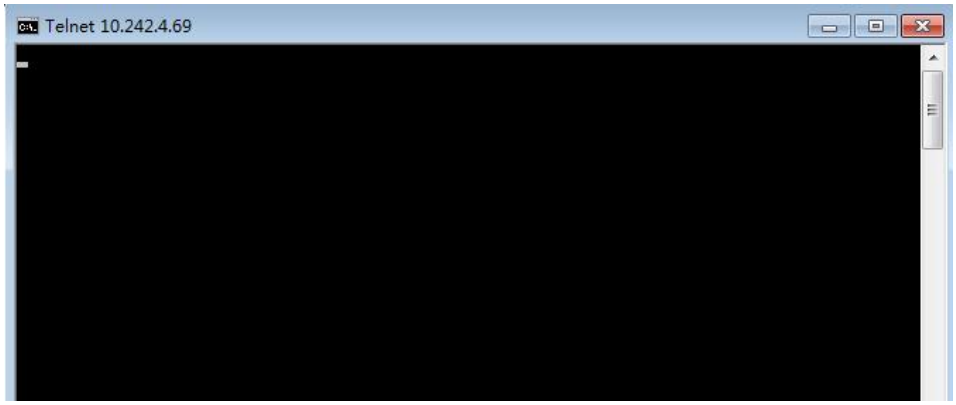
步骤1. 检查网络联通性。

包括检查本机到综合网关的网络是否可达，检查综合网关到应用资源的网络是否可达。

打开电脑的cmd，使用Ping 10.242.4.69验证，若无法访问则说明网络出现问题。

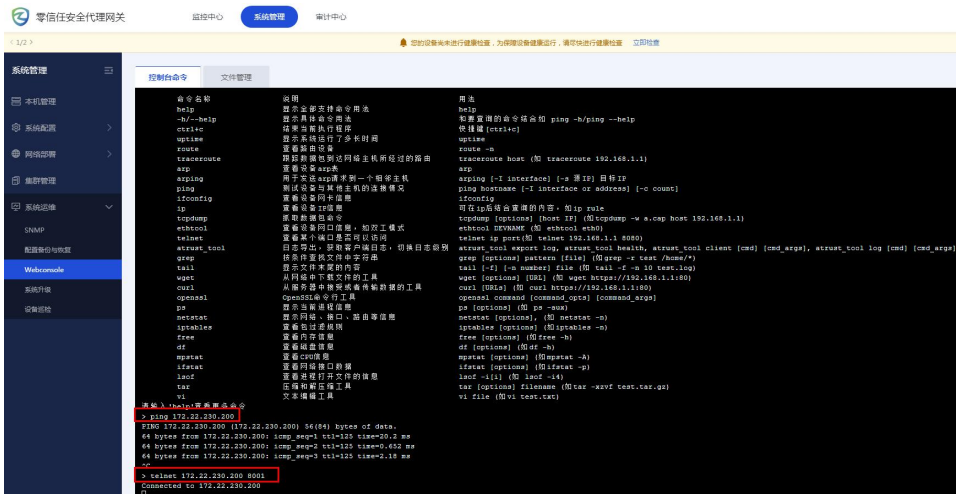


使用telnet 10.242.4.69 443和10.242.4.70 441进行查看，可以正常跳转则说明客户端接入地址和端口开放正常，不能正常跳转说明端口开放出现问题。



检查综合网关到需要发布的资源的网络是否可达。

在综合网关[系统管理/系统运维/WEBconsole]页面，然后使用网络检测命令ping 172.22.210.208 和telnet172.22.230.208:8001命令进行验证（telnet成功会有connect success的字样）。



步骤2. 查看用户能否认证登录并查看授权的资源。

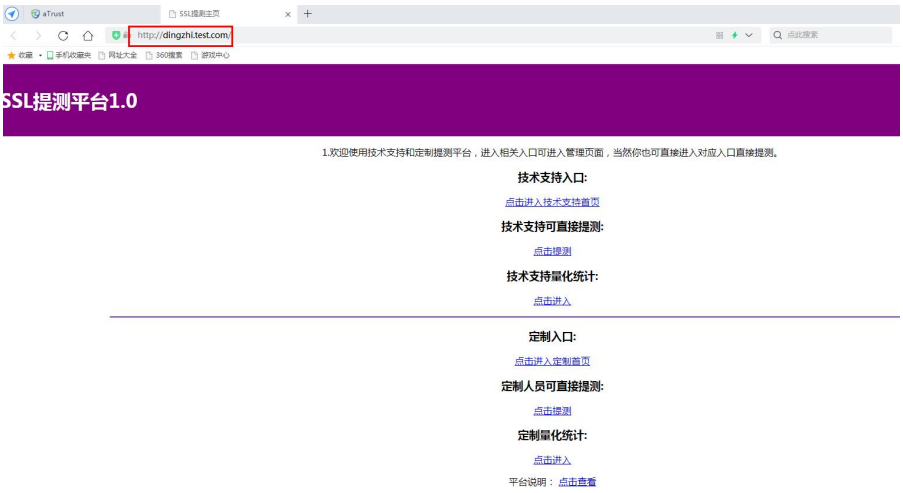
1、双击打开atrust客户端。右下角即会弹出客户端登录界面。

2、点击前往登录按钮，跳转到客户端登录界面。

3、输入运维人员1的账号密码，登录后即可查看该用户所对应的应用资源权限。

步骤三：检查用户能否正常访问应用中心的资源。

在用户的应用中心点击定制平台2，若能正常跳转则说明隧道资源配置没有问题，若无法正常跳转则说明配置有误，可参考第7章常见问题进行排查。



至此，从环境准备、服务端、客户端部署到基本配置，整个分离式部署硬件部署已部署完毕并可在内网验证访问，此步骤的内容对后续部分具有很大的关联参照意义，请按需参考。

4. 附录

如果弹性公网 ip 不够，则需要购买（购买路径：网络控制台-弹性公网 IP 和带宽）

完成弹性公网 IP 的申请，点击完成提交后完成申请