

# 深信服零信任 aTrust 华为公有云

部署手册

- **产品版本** 2.4.10 及以上
- **文档版本** 02
- 发布日期 2024-09-04

深信服科技股份有限公司

#### 版权声明

本文档版权归深信服科技股份有限公司所有,并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有 特别注明外,其著作权或其它相关权利均属于深信服科技股份有限公司。未经深信服 科技股份有限公司书面同意,任何人不得以任何方式或形式对本文档内的任何部分进 行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

### 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
2024-09-04	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	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	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。
\land 小心	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	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	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
窗口夕 苏英夕笙	<b>古托县 "[]"</b>	弹出[新建用户]窗口。
図口石 <b>、</b> 米平石守	刀拍与[]	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ii
1. 概述
1.1. 环境准备
1.1.1. 规格网络要求
2. 设备部署
2.1. 镜像上传-自行获取镜像上传
2.1.1 上传镜像
2.1.2 镜像制作
2.2. 使用市场镜像1
2.3. 创建虚拟私有云 VPC-「可跳过」12
2.4. 安全组-「可跳过」14
2.5. 创建弹性云服务器10
3. aTrust 网络配置
3.1. 配置网络
3.2. 设备授权
3.3. 基本配置
3.3.1. 新增用户
3.3.2. 发布隧道资源
3.3.3. 给用户授权
3.3.4. 验证配置效果
4. 附录

# 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. 规格网络要求

- 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 5-10 并发用户
  - 8 核 16G 500G 系统盘 10-2000 并发用户
- 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	综合控制中心控制台运维管理端口
443 端口	综合控制中心:用户接入认证和鉴权端口 443 端口可改,控制中心的 443 可更改为其它端口。
441 端口	隧道应用端口
22 端口	综合控制中心后台运维、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				
综合控制中心	需映射 443 端口到外网做远程用户接入认证用,端口可改				
综合控制中心	映射 441 端口用户访问隧道应用,不可改				
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]。

HUAWEI	华为云 / 控制台 <b>오</b> 上海	×				
≡	服务列表 >	请输入名称或者功能查找服务				
٢	弹性云服务器 ECS	最近访问的服务: 弹性云服务器 ECS	弹性	性公网IP EIP 虚拟私有云 VPC	对象存储服	鎊 OBS
	裸金属服务器 BMS	计算		存储		网络
.000	弹性伸缩 AS	弹性云服务器 ECS	Ŧ	云硬盘 EVS	Ŧ	虚拟私有云 VPC
_		云耀云服务器 HECS		专属分布式存储 DSS		弹性负载均衡 ELB
0	云硬盘 EVS	裸金属服务器 BMS	Ŧ	存储容灾服务 SDRS		云专线 DC
	云硬盘备份 VBS	云手机 CPH		云服务器备份		虚拟专用网络 VPN
Ø	库拟私有云 VPC	VR云渲游平台		云备份 CBR		云解析服务 DNS
		镜像服务 IMS		云硬盘备份 VBS	Ŧ	NAT网关 NAT
$\Phi$	弹性负载均衡 ELB	函数工作流 FunctionGraph	1	对象存储服务 OBS		弹性公网IP EIP
P	弹性公网IP EIP	弹性伸缩 AS	Ŧ	数据快递服务 DES		云连接 CC
A	一物提皮 PDS	专属云		弹性文件服务 SFS		VPC 终端节点
ŝ		专属主机 DEH		CDN		
$\bigcirc$	域名注册			云存储网关 CSG		应用服务
		容器服务				应用魔方 AppCube
		云容器引擎 CCE		管理与部署		应用管理与运维平台;

#### 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。

# 

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。

-	华为云 👘	ita		投索	Q. 费用中心	资源	Im	企业	开发工具	备宪	支持与服务	中文 (茵体)	hw11304400	
	对象存储服务		对象存储服务 ⑦ 开题声明							40	· 流程引导 - 西	9 使用旗曲	(1521M)	购买资源包
(j) (j)	対象存储 并行文件系统		① 减激型参加对象存储服务使用件检测	研,您宝贵的意见和建议是我们持续提升产品	品体验的源动力,感谢	他的参与	1							×
,AIA	我的套餐	æ	OBS Browser+ 土 下载	obsutil 上 下载	obsfs		土 下雲	9	ERENSOK					
0	数据快递服务	do.	图形化管理工具,支持批量上传大文 件,文件夫。	命令行管理工具,支持桶和对参的基 本操作。	并行文件系统团 地文件系统操作	载工具, 1 对象。	可实现在本		就取访问图1 访问OBS成计	井(AK和SK ≲地图				
0	云存储网关	o <sup>o</sup>	了解更多	了解更多	了解更多									
Ô	媒体转码服务	°6												

区域	<ul> <li>♀ 华南-广州</li> <li>▼</li> <li>不同区域的云服务产品之间内网互不指通:请就近选择靠近您业务的区域,可减少网络时延,提高访问速度。</li> </ul>
数据冗余存储策略	多AZ存储 单AZ存储 ⑦
	多AZ存儲能提高您的数据可用性,同时会采用相对较高的计费标准。价格详情 多AZ存储属性一旦启用,后续无法修改。
桶名称	sdp-atrust         命名规则:         - 需全局唯一,不能与已有的任何構名称重复。         - 删除桶或并行文件系统后,需要要特30分钟才能创建同名桶或并行文件系统。         - 长底范围为3963个字符,支持小写字母、数字、中划线(·)、英文句号()。         - 禁止使用PP地址。         - 禁止使用PP地址。         - 如果名称中包会英文句号(),访问桶或对象时可能会进行安全证书校验。
存储类别	标准存储 低频访问存储 归档存储
	适用于有大量热点文件或小文件,且需要频繁访问(平均一个月多次)并快速获取数据的业务场景。 上传对象时,对象默认与桶的存储类别相同,也可以根据适用场景修改。了解更多
桶策略	私有 公共读 公共读写
	桶的拥有者拥有完全控制权限,其他用户在未经授权的情况下均无访问权限。
默认加密	开启 关闭 ②
	推荐 密钥管理全免费,核心数据更安全。
归档数据直读	开启关闭
	通过归档数据直读,您可以直接下载存储类别为归档存储的数据,而无需提前恢复。归档数据直读会收取相应的费用。 价格详情

步骤2. 点击<确定>完成存储桶的创建。

华为云 拉制台					
对象存储服务		<ol> <li>试邀您参加对象存储服</li> </ol>	务使用体验调研,您宝贵的意	见和建议是我们持续	<sup>2</sup> 提升产品体验的源
对象存储			a . 1. 20		
并行文件系统		OBS Browser+ 图形化管理工具 支持批算		obsutil 命今行管理工具	支持桶和对象的复
我的套餐	do	了解更多		了解更多	
数据快递服务	ି				
云存储网关	er P				
媒体转码服务	d <sup>D</sup>				
CDN	do	在控制台上您还可以创建9	8个桶。		
对象存储迁移服务	e <sub>o</sub>	桶名称 ↓三	存储类别↓Ξ		区域 1三
		sdp-atrust	标准存储		华南-广州
		sangfor-atrust	标准存储		华东·上海一
	マノン     エージン       対象存储服务       対象存储       并行文件系统       我的套餐       数据快递服务       云存储网关       媒体转码服务       CDN       对象存储迁移服务	大学/女     110010       対象存储服务     パ象存储       并行文件系统     ・       我協快递服务     ・       数据快递服务     ・       支存储网关     ・       媒体转码服务     ・       CDN     ・       対象存储迁移服务     ・	対象存储服务     ①     試邀您参加对象存储服务       対象存储     并行文件系统     〇BS Browser+       并行文件系统     ②     図形化管理工具、支持批量       我的赛餐     ②     万解更多       数据快递服务     ②     〇BS Browser+       現状時码服务     ③     ○       文方储网关     ②     ○       政保快递服务     ②     ○       放露存储迁移服务     ③     ○       耐合計     ○     ○       耐合計     ○     ○       前合称     □     □       就像存储迁移服务     ③     ○       前合市     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □       」     □     □ <td< td=""><td>対象存储服务        対象存储        対象存储        并行文件系统        労務客餐        数据快递服务        公方储网关        成本時码服务        CDN        対象存储迁移服务        研索存储迁移服务        研索存储迁移服务  <!--</td--><td>中子女女     12004       対象存储服务        対象存储        対象存储        并行文件系统        労務条        数据快递服务        改留快递服务        安宿鶴风关        成本转码服务        プ解更多        在控制台上您还可以创建98个桶。       安宿道        行储类別 /=        sangfor-atrust     标准存储</td></td></td<>	対象存储服务        対象存储        対象存储        并行文件系统        労務客餐        数据快递服务        公方储网关        成本時码服务        CDN        対象存储迁移服务        研索存储迁移服务        研索存储迁移服务 </td <td>中子女女     12004       対象存储服务        対象存储        対象存储        并行文件系统        労務条        数据快递服务        改留快递服务        安宿鶴风关        成本转码服务        プ解更多        在控制台上您还可以创建98个桶。       安宿道        行储类別 /=        sangfor-atrust     标准存储</td>	中子女女     12004       対象存储服务        対象存储        対象存储        并行文件系统        労務条        数据快递服务        改留快递服务        安宿鶴风关        成本转码服务        プ解更多        在控制台上您还可以创建98个桶。       安宿道        行储类別 /=        sangfor-atrust     标准存储

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 综合控制中心 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。

并行文件系统				
桶数量	: 2			
外部桶	<b>建桶 +</b> ;碎片	⑦ 桶ACLs 更	多。	
定时上传桶名和	γ 1Ξ	存储类别↓Ξ	区域 1Ξ	存储用量↓Ξ
任务管理	dp-atrust	标准存储	华南-广州	0 byte
🥃 si	angfor-atrust	标准存储	华东-上海一	15.53 GB

NAME:	华为云 🗌 控制台						搜索	Q	费用中心
Ξ	对象存储服务		对象存储服务 ⑦ 开源	<b>国</b> 明					
6	↓ 対象存储 并行文件系统		① 或邀您参加对象存储服务	使用体验调研,您宝贵的题	原见和建议是我们持续提升产品体验的源	动力,感谢您的参	与!		
MN	我的套餐	<sub>с</sub> о	OBS Browser+	上 下载	obsutil	上 下载	obsfs	上下	载
0	数据快递服务	00	图形化管理工具,支持批量上	传大文件,文件夹。	命令行管理工具,支持桶和对象的基	体操作。	并行文件系统挂载工具 作对象。	1, 可实现在本地文件系统	提
0	テ友時回关	20	了解更多		了解更多		了解更多		
$\bigcirc$	媒体转码服务	eo eo							
4	CDN	op							
P	对象存储迁移服务	6 <sup>0</sup>							
යි			在控制台上您还可以创建98个	桶。		_			
			▲ 桶名称 ↓三	存储类别↓Ξ	区域 1三		存储用量↓Ξ	Data+ 🏦	力能
			sdp-atrust	标准存储	华南·广州		25.43 GB	该区域暫不到	支持
			sangfor-atrust	标准存储	华东-上海一	- 44 ) -	15.53 GB	该区域智不可	支持
			sangfor-atrust	标准存储	华东·上海一		15.53 GB	该区域智不到	支持

## 2.1.2 镜像制作

步骤1. 在服务列表选择镜像服务。

HUAWEI	华为云 拉制台	115					
≡	服务列表	>	请输入名称或者功	力能查找服务			
0	弹性云服务器 ECS		最近访问的服务:	镜像服务 IMS	弹性云	服务器 ECS 对象存储服务 OBS	虚拟和
යි	云数据库 RDS		计算			存储	
,000,	弹性伸缩 AS		弹性云服务器 ECS		Ŧ	云硬盘 EVS	Ŧ
6	裸金属服务器 BMS		云耀云服务器 HECS 裸金属服务器 BMS	5	¥	专属分布式存储 DSS 存储容灾服务 SDRS	
0	云硬盘 EVS		云手机 CPH			云服务器备份 CSBS	
	云硬盘备份 VBS		VR云渲游平台			云备份 CBR	
Ô	虚拟私有云 VPC		镜像服务 IMS 函数工作流 Function	電像服务 IMS	<u></u>	云硬盘备份 VBS 对象存储服务 OBS	¥
$\triangle$	弹性负载均衡 ELB		弹性伸缩 AS		¥	数据快递服务 DES	

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。

## 深信服零信任华为公有云部署手册

目前镜像服	务已进入商业化阶段,私有镜像会收取一定的存储费用。 详细计费标准可参	考镜像服务计费标准			
像类型和来源					
区域	华南-广州				
	不同区域的资源之间内网不互通。请选择靠近您客户的区域,可以降低	网络时延、提高访问速度。			
* 创建方式	系統曲鏡像整机鏡像数据曲镜像	ISO镜像			
选择镜像源	云服务器 標金庫服务器 镜像文件				
	<ul> <li>目前支持使用vhd, zvhd, vmdk, qcow2, raw, zvhd2, vhdk</li> <li>创建坑串镇像使用的文件署要先上传到对象开稿为示律供型的情報更多</li> <li>创建镇像都, 请确保镜像文件已完成相关配置, 了解更多</li> </ul>	K、qcow、vdl或qed格式镜像文件创建私有精 每中,除文件格式为zvhd2和raw外,从桶中设	總。 起取的镜像文件的实际大	小不能超过128GB。 🤇	7
	<ul> <li>目前支持使用小付, zvhd, vmdk, qcow2, raw, zvhd2, vhdk</li> <li>创建机构模像使用的文件業界上作与对象并指为市种进起的構築</li> <li>创建建像前, 请确保意像文件已先成相关犯罪。了解罪多</li> <li>价适望的机构模像的指式和大小可能描述的振动模像文件不同。</li> <li>快速望动起间代表无成模像制作, 很模像文件柔特能为rawa就</li> <li>创建模像前,请查普遍作系统已知问题。了解更多</li> </ul>	K、qcow、vdl或qed推式機像文件创建私有物 中,除文件推式为zvhd2f0raw分,从場中以 zvhd2推式并完成機像优化。了解更多	增优。 5取的損像文件的实际大	小不能超过12868。	7
	目前支持使用vhd, zvhd, vmdk, qcow2, raw, zvhd2, vhdk     创建机有模像使用的文件要是无上作与时没条件接入方电线能控的使用的文件。     创建模像前,清确保镜像文件已完成相关配置,了解要多     听信道的机械有做有关化力可能能能的能减操令文件不同。     化注意道面临时快速考虑消费利许,信赖像文件需要转换力raw或     创建模像前,清量量操作系统已知问题,了解更多      杨列表:>dp-atrust	<、qcow、vdli或qed格式機像交件创建私有精 目中、除文件格式力zvhd2和aw分、从標中U Izvhd2格式并完成简像优化、了解更多	像。 國政的損優文件的实际大 请输入文件名称前缀	小不能超过128GB。 Q	C
	日前支持使用小d、zhd、vmdk、qcow2, raw, zhd2, vhdk 创建机构模像使用为文件量表上作等可读者存进为市场模型的模 版更多 创建理像参称:清确得理像全文给已完成相关觉量。了解更多 新聞書的私精確會的形式化力可可能能可能的影响模像文件不同。 快速透道功能可快送完成编卷制作。信提像文件柔特能力raw或 创建模参新,请量着操作系统已知问题。了解更多	c. qcow, vdl或qed格式機像文件创建私有補 時中,除文件相致力zvhdz和awh,从備中 2vhd2格式并完成機像优化。了解更多 最后体改动向	10条。 国际的调像文件的实际大 请能入文件名称新疆 文件类型	小不能超过128GB。 Q 文件大小	7 C
	日前式非按照小d、	c. qcow. vdl或qed格式倒像文件创建私有描 中、使文件相致力zvhdz和awh,从博中 izvhd2格式并完成确像优化。了解更多 最后修改对问	(象. 取約項像文件的实际大 書組入文件名称前缀 文件类型	小不能超过128GB。	C
	<ul> <li>目前式性疫気小d、ためd、Ymdk、qcow2、raw、ためd2、Ymdk</li> <li>・ 创建構像使用的文件電景先上待到对象存在为你准装型软件</li></ul>	<ul> <li>c. qcow. vdl或qed格式機像文件创建私有構 時、除文件相式方zvhd2和av分,从標中2 izvhd2格式并完成機像优化。了解更多 最后條改改问 2021/04/15 04:06:04 GMT+08:00</li> </ul>	▲. ▲. ●. ●. ●. ●. ●. ●. ●. ●. ●. ●	小不能超过128G8。 Q 文件大小 9.89 GB	C

配置信息	
	☑ 进行后台自动化配置 了解更多
* 镜像用途	ECS系统盘镜像 BM/S系统盘镜象
架构类型	x86 ARM
	系统记别的镇像文件架构英型与用户设置的架构类型不同时,以系统记别的架构类型为准。系统不能记别镇像文件的架构类型时,以用户透得的架构类型为准。
启动方式	BIOS UEFI
	清确保选择的启动方式与确象文件中的启动方式一致,否则,使用该确象创建的弹性云服务器无法启动。
操作系统	CentOS v 8.0 64bit v
	系统归别的确象文件操作系统与用户设置的操作系统不同时,以系统问别的操作系统为准。系统不能识别确象文件的操作系统时,以用户选择的操作系统为准。 <b>宣君支持的操作系统。</b>
* 系统盘 (GB)	- 500 + 満時保織入的大小不小子猿像文件的系统曲大小、
	⑦ 增加一块数据曲 您还可以挂载3块数据曲。
* 名称	aTrust-SDPC
加密	─ KMS 加速 经题 ⑦
标签	如果您需要使用同一标签标识多种去资源,即所有服务均可在标签编入框下拉选择同一标签,建议在TMS中创建领定义标签。查署预定义标签 C
	<ul> <li>标签键 标签值</li> <li>标签值</li> </ul>
描述	

立即创建

步骤4. 点击提交完成镜像创建

	く 创建私有镜像						
	资源详情						
	立日夕物	2009					2048
	了 前各林 系统盘镜像	区域 镜像关型 名称 来源 强作系统 系统盘(CB) 架构类型 启动方式	广州 ECS系统曲镜像 aTrust-SDPC 镜像文件 (atru CentOS 8.0 64) 500 x86 BIOS	st.sdpc_20200527.qcow2) ilt			<b>5000</b>
						我已经阅读并同意《镜像制作承	语书》和《镜像免麦声明》 上一页 提交
镜像	服务②						
0	诚邀您参加镜像服务使用体验	调研,您宝贵的意贝	已和建议是我们持续提升	产品体验的源动力,感谢您的参与!			
	目前镜像服务已进入商业化阶段	设, 私有镜像会收取	一定的存储费用,删除管	刘建的镜像后将不再计费。详细计费	示准可参考镜像服务计费标准		
3	公共镜像 私有镜像	共享镜像					
	镜像支持云服务器快速发放,	建议您优化不支持该	功能的镜像。请在详情了	页面查看镜像是否支持快速发放。了	解更多		
感	还可以创建48个私有镜像。						
	删除 共享					所有镜像 🔻	所有攝作系统 🔻
	□ 名称 ↓Ξ	状态	操作系统类型	操作系统	镜像类型		磁盘容量 (GB) 加密
	aTrust-Proxy	⊘正常	Linux	CentOS 8.0 64bit	ECS系统自	且镜像(x86)	500 否
	aTrust-SDPC	❷正常	Linux	CentOS 8.0 64bit	ECS系统自	±鏡像(x86)	500 否

# 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-4a611a 1a8192#productid=OFFI1127135378533625856

			中国站 (1) 式構造App	p.
www.even	云商店 免费试用 商品分类 最新活动 热门子	家区 帮助中心	中心 关于第01 Q 世家	1
	云南店 > 安全 > 应用安全 > 深信服VPN网关管理软件编绘			
		<ul> <li>に</li> <li>に</li> <li>辺境</li> <li>規構</li> <li>施行加速</li> </ul>	Common Co	8 8
			◎ 指保交易 ◎ 服务全程监管 ◎ 過数換后无比 ◎ 优质等家	

# 2.3. 创建虚拟私有云 VPC-「可跳过」

步骤1. 进入控制台, 在服务列表项点击虚拟私有云VPC。

服务列表 > 请輸入名称或者功能查找服务		
③ 弹性云服务器 ECS 最近访问的服务: 虚拟私有云 VPC   弹性云服务器 ECS		
会 云数据库 RDS 计算 存储		网络
//// 弾性伸縮 AS 弾性云服务器 ECS 単 云硬盘 EVS	¥	虚拟私有云 VPC
云耀云服务器 HECS 专属分布式存储 DSS		弹性负载均衡 ELB
		云专线 DC
□ 云硬盘 EVS 云手机 CPH 云服务器备份		虚拟专用网络 VPN
マアテレンジャンジャンジャンジャンジャンジャンジャンジャンジャンジャンジャンジャンジャン		云解析服务 DNS
· · · · · · · · · · · · · · · · · · ·	Ā	NAT网关 NAT
<ul> <li>虚拟私有云 VPC 函数工作流 FunctionGraph 对象存储服务 OBS</li> </ul>		弹性公网IP EIP
		云连接 CC

步骤2. 点击<创建虚拟私有云>。

华为云 拉制台	◆ 上時	•		11.2	Q	商用中心	致源	工単	22	THIA	92	3210-148239	中文 (2044)	hw11304400	
网络控制台		虚拟私有云 ③											19 使用脑带	erate	鐵私有云
83.		國際語题 在一下的一个中心的一个中心的一个中心的一个中心的一个中心的一个中心的一个中心的一个中心	PC) 可解助您在云上经私和建简单的,私家的遗形J	9後环境,25可以完全掌握自己的虚拟网络,包括由唐津	性公网中、 東京	1. 创建子用。	设置安全组	15. 此外	exact	1过云寺城、 VP	N幅方式R	₩FC与体统数据	中心互联互通、贯浦	s. /.	
子网		网络邮署流程								助文档			/		₩¥×>
諸由家	· · ·								1	什么显出现和 创建进程私有	(荷云 🚺 (云	lot.	/		
弹性公司IP和带宽	•								1	公网连接 通过EIP追接公	39 <b>H</b>	3			
NAT同关 弹性负数均衡	:	e,			(		)		-	通过NAT同共	连接公司				
		101			1		/								

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。

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。

<	创建虚拟私有云	0
	基本信息	
	区域	<ul> <li>Q 华海,广州</li> <li>▼</li> <li>不同区域的资源之间内网不互通,请选择靠近您惹户的区域,可以降低网络时延,提举访问遗度,</li> </ul>
	名称	零信任专有网络
	IPv4网段	10       ・       243       ・       0       /       16       ▼         建议使用网段: 100.00/8-24 (透達)       172.160.01/2-24 (透達)       192.168.00/16-24 (透達)       192.168.00/16-24 (透達)
	高级配置 🔻	标签   描述
	默认子网	
	可用区	可用区3 • ⑦
	名称	零信任-业务网
	子网IPv4网段	10     ・     243     ・     0     /     24     マ     ⑦ 可用P数: 251       子网始連先成点:     子网网段无法传放
	子网IPv6网段	There ?
	关联路由表	RKA 🕜
	高级配置 ▼	网关 IDNS服务器地址 INTP服务器地址 IDHCP程约时间 I标签 I描述
免	费创建	<u></u>

步骤4. 完成创建后,可在页面查看到对应的私有云网段。

HUAWEI	华为云 控制台	♀ 广州	*	
Ξ	网络控制台		虚拟私有云 ⑦	
0	意览			
Ω	虚拟私有云		名称	IPv4网段
6	子网路由夷		零信任专有网络	10.243.0.0/16 (主网段)
0	访问控制	•		
0	VPC流日志			
$\bigcirc$	弹性公网IP和带宽			

步骤5. 点击子网,可查看到新建的子网信息。

华为云 拉制台	• ****									66) hwi
网络控制台	子网 ⑦									
0.8					全部通知私有云	1.*	28		Q	标签编集
進用私有云	名称	虚宛私有云	IPv4网段	IPV6FEER ⑦	状态		可用区 ⑦	网络ACI	路由表	操作
路由赛	零信任·业务网	零信任专有网络	10.243.0.0/24	开启中v6	可用		可用区3	373	rtb-零倍任专有 默认路由街	
iঠ/নিশ্রম	•									
VPC流日志										
弹性公网IP和带宽	•									
NAT网关										

# 2.4. 安全组-「可跳过」

**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)。

	华为云 三日 日本	<b>○</b> / H	*		[36	ě.	9 <b>8</b> 8940	) ≘ <b>2</b>	工業 合計	THIR	RE 205588	中文 (範証)	hw11304400	1 🖉
≡	网络控制台		安全组 ①									[2] 使用		1920
0	9 <b>X</b>		● 安全组基一个逻辑上的分组、为同一个VPC内具有相同安全保护需求并相同	[信任的云曆多圓過供访问篇	<b>略,安全纷纷建</b> 后,两户可	以在安全组中定义各种	防闭成时,当天服务器	8入波安全组网	. 即受到这些访问	间间隙炉、安全1	8款认远方向放行,并且9	2 全组内的云服务署	1可以相互访问。	×
100.	唐段私育云 子問		利表中"Sys-default"基系统数以创建的一个安全组、数以安全组的规则指 参冗所建立全组。	创建安全组			×	均、安全道思可	[以直接使用,译]	「清多元款以安全」	800规则,记集默以安全	8不能異足言求。日	可创建制的安全组。	*
8	BOR			* 2.17	零倍任-访问控制	_				-	:f2			C
0	(5/R)2#)	•	88	* 1815	BBX			关联共列	i side			操作		
0	死總ACL		default	捕送	人方向不放透任何調口。 模擬实际访问素求适应	STERROLLS DERROLLS		¢	Default secu	ity group		能量规则 管理	建实例 充限	
0	1P地址目 VPC流日志													2
©	弹性公司印和带宽	•				(	//255							
	NATRE:	•		重音模板成制 •	_									
	20年後後				<b>NG</b>	tow.								
					10 million - 10									8

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。

<b>0</b> #==	×
安全组创建成功,请添加安全组规则以便能正常访问该安全组关联的实例	
199.e	
配置规则	

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。

〈 零信任-访问控制						
基本信息 入方向规则 出方向规则 关联	实例					
	添加入方向规则 教我设置					3
1 允许 TCP : 4433	安全组入方向规则为白名单(允)	许),放通入方向网络流量。				
1 允许 TCP:4433	安全组 <b>零信任-访问控制</b> 如您要添加多条规则,建议单击导入规》	则以进行批量导入。				
	优先级 ⑦ 策略	协议端口 ②	类型	源地址 ②	描述	操作
	1	тср • 443	IPv4 ¥	IP地址         ▼           0.0.0.0/0		复利 删除
	1	TCP •	IPv6 ¥	IP始始止         ・           ::/0         ・		复制 删除
			④ 増加1条规则			
			确定	取消		

■ 常信任-切问控制 ■信息 入び	1 5向规则 出方1	向规则 关联实例				S 安全相等语任-0	的控制爆发规则成功
(BackRA)	他回答拉起税则	1019 一種飲酒 入方向规则: 5	較我设置				
(KRIR ()	第略 ⑦	thicking 7 (1)	类型	1946a): ①	描述	爆战时间	操作
0 1	允许	TCP: 4433	IP <sub>9</sub> 4	0.0.0.0	允许安全组内的弹性云服务器做出通信	2021/04/15 18:03:34 GMT+08:00	修改 完制 删除
□ 1	允许	TCP: 4433	IPx6	:/0	允许安全组内的弹性云服务器彼此遵信	2021/04/15 18:03:10 GMT+08:00	1922   2514   2509
1	允许	TCP: 441	1Py4	0.0.0.0 (2)	-	2021/04/15 18:01:42 GMT+08:00	(FZ) 2241 259
1	九年	TCP: 443	1Pv4	0.0.0.0/0 ②	1.00	2021/04/15 18:01:42 GMT+08:00	修改 田利 勤除
1	允许	TCP: 443	iPv6	::20	12	2021/04/15 18:01:42 GMT+08:00	修改 契利 删除

## 步骤4. 配置出方向规则,可配置为默认全放通。

零信任-访问控制					
本信息 入方向	向规则 出方	向规则 关联实例			
添加规则	央遗添加规则	删除 <b>一键放通</b> 出方向规则: 2 教我没置			
优先级 ⑦	策略 ②	协议端口 丁 ②	类型	目的地址⑦	描述
1	允许	全部	IPv6	::/0	放通全部流量
1	允许	全部	IPv4	0.0.0.0/0 ⑦	放通全部流量

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。
---------------	-------------------

HUAWEI	华为云 │ 控制台 ♀ 广州		搜索
Ξ	网络控制台	安全组 ⑦	
ම ස	总览		
M	子网	名称         安           零倍任-访问控制	·全组规则 7
0	路由表  访问控制 ▲	default	6
	安全组		
© 4	网络ACL IP地址组		

# 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。

HUAWEI	华为云	控制台	♥┌₩	*		
Ξ	ℓ 自定	€¥				
٢			-			
6	关注多	<b>&amp;源</b> [广州]	0			
M	引单性	E云服务器 EC	s	0	裸金属服务器 BMS	0
0	云硬	电台 VBS		0	虚拟私有云 VPC	1
	云数	始居库 RDS		0	域名注册	0
Ø						
$\bigtriangleup$	最近认	访问的服务				
P	弹性	云服务器 ECS	对象存储服务 OBS	虚拟私有云	VPC	

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>。

工单	企业	开发工具	备案	支持与服务	中文 (简体)	hw11304400   🗗
				☞ 最新动态	同 使用指南	购买弹性云服务器
						×
					C	
						0 Q
址		j	计费模式 「	7	标签	操作

**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,服务器配置满足1.1.1章节规格要求。

#### 深信服零信任华为公有云部署手册

弹性云服务器	自定义购买快速购买			
1 ##RE	② 网络配置 ③ 高级	配置 ——— ④ 确认配置		
计费模式	包年/包月 [2]	計畫 竟价计费	0	
区域	♥ 华南-广州 ▼	● 推荐区域 👚 西南-贵阳—(0	) 华北-北京四(0) 华南-广州(0)	华东-上海— (0) 型太-香港
可用区		但進; 请威江远洋军正恐业务的区域。 用区6 可用区3	可無少阿珀可述,提高的问题是是。如何过4世	0
CPU架构	x86计算 觀點计算 ⑦			
规格	最新系列	vCPUs 8vCPUs	▼ 内存 16GB	▼ 规格名称
	规格名称	vCPUs   内存 ↓=	CPU 1	基准 / 最大带宽(
	c6s.2xlarge.2	8vCPUs   16GB	Intel Cascade Lake 2.6GH	z 4 / 4 Gbit/s
	C c6.2xlarge.2	8vCPUs   16GB	Intel Cascade Lake 3.0GH	z 4.5 / 15 Gbit/s
	C c3.2xlarge.2	8vCPUs   16GB	Intel SkyLake 6151 3.0GH	z 2 / 5 Gbit/s
	S6.2xlarge.2	8vCPUs   16GB	Intel Cascade Lake 2.6GH	z 0.75 / 3 Gbit/s
	S3.2xlarge.2	8vCPUs   16GB	Intel SkyLake 6161 2.2GH	z 0.8 / 3 Gbit/s
	S2.2xlarge.2	8vCPUs   16GB	Intel E5-2680V4 2.4GHz	0.8 / 3 Gbit/s
	hc2.2xlarge.2 (已售罄) 可购买区域	8vCPUs   16GB	Intel E5-2690V4 2.6GHz	2 / 5 Gbit/s
	当前规格 通用计算增强型	c6s.2xlarge.2   8vCPUs   16GB		
镜像	公共镜像	私有镜像	共享镜像 市场镜像	0
	aTrust-SDPC(500GB	)		▼ C 新建私有镜像
	使用私有镜像创建弹性	t云服务器前,请查君操作系统T	己知问题。	
系统盘	通用型SSD	▼ _ 500	+ GB IOPS上限7,800, IOPS突	发上限8,000 ⑦
	(中) 営加一中数据盘	悠还可以挂载 23 块碳盘 (云硬	± 1	

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。

# 

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 VPN。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。

密级:公
------

< 弹性云服务器	自定义购买快速购买
① 基础配置 ——	2 网络配置 ————————————————————————————————————
网络	零信任考有网络(10.243.0.0/16)     ▼     C     電信任业务网(10.243.0.0/24)     ▼     ●
扩展网卡	⑦ 增加一块网卡 認近可以增加 1 块网卡
安全组	零信任-访问控制 (fdc7b774-ce7f-446d-9f8b-f906692f4fc ● ▼ C 新疆安全組 ⑦ 安全組មKI初火場功能, 是一个逻辑上的分祖,用于设置网络访问控制。 当前选择安全组年软温FCMP协议,无法PING宏振务器,您可以配置安全组现则 属开安全组观则 >
弹性公网IP	<ul> <li>● 现在购买</li> <li>● 使用已有</li> <li>● 暂不购买</li> <li>⑦</li> </ul>
线路	全动をBCP     静をBCP     ⑦       ⑤ 不低于99.95%可用性保険     ⑦
公网带宽	接着就计费 ①     流量技术就处理定的场景     描述市就比型定的场景     描述中的场景     描述中就处理定的场景     描述中就是一般实际使用的出公网流量计量,与使用时间无关。
带宽大小	5         10         20         50         100         自定义         一         10         +         希意意識: 1-300 Mbit/s           ⑤ 免费开自DDoS基础的护

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。

< 弹性云服务器	自定义购买快速购买
① 基础配置 ——	— ② 网络配置 ——— ③ 高级配置 ——— ④ 确认配置
云服务器名称	aTrust-SDPC-01 / 允许重名 购买多台云服务器时,支持自动增加数字后缀命名或者自定义规则命名。 ?
描述	
登录凭证	0/85 <b>密码 密钥对 使用脑牵宏码</b> 保留所选择镜像的密码。为了保证您的正常使用,请确保所选择镜像中已经设置了密码。
云簧份	使用云音份服务,素购买售份存储库,存储库是存放服务器产生的备份副本的容器。 现在购买 使用已有 <b>若不购买</b> ⑦
云服务贛組 (可选)	<b>反亲和性</b> ⑦ 请选择云服务器组 ▼ C 新建云服务器组
高级选项	□ 现在配置

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。

弹性云服	性云服务器 ⑦									
1 31	1思参加弹性云服务器使用体验调研,您宝贵的意见和	口建议是我们持续提升	十产品体验的源动力,感谢您的	)参与!						
开机	. 关机 重置密码 更多 ▼									
默认挂	安照名称搜索									
	名称/ID	监控	可用区 7	状态 ⑦	规格/镜像	IP地址	计费模式 ⑦			
	aTrust-SDPC-02 ad41aae9-e4b8-4e22-a7eb-ff954dac555d	Ø	可用区6	⑤ 运行中	4vCPUs   8GB   c6s.xlarge.2 aTrust-SDPC	124.71.40.37 (弹性公网) 1 10.243.0.29 (私有)	按需计器 2021/04/15 19:20:10 创			
	a Trust-SDPC-01 72c21434-7052-45a8-b774-47d7857e8af4	2	可用区6	⑤ 运行中	4vCPUs   8GB   s6.xlarge.2 aTrust-SDPC	139.9.203.223 (弹性公网) 10.243.0.85 (私有)	按需计费 2021/04/15 19:18:27 创			

# 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】

系统管理	=	路由设置				
	~	● 新増		的新		
	$\rightarrow$	原号	目的地址			子网掩码
	~	1	0.0.0.0			0.0.0.0
			编辑静态路由		×	
			*目的地址:	0.0.0.0		
			*子网掩码:	0.0.0.0		
			*下一跳网关:	10.243.0.1		
				确定	取消	
	×					

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。

#### 深信服零信任华为公有云部署手册

중信任控制中心		监控中心	业务管理	安全中心	系统管理	审计中心	
< 1/2 >						您的设备尚未进行健康检查	, 为保障设备健康运行, 请尽
系统管理	←│编辑网	10					
公 管理员配置 シン	属性						
◎ 系统配置 >	*名称:	业务口					
● 网络部署 ~	描述:	仅用于控制台	访问,内置预留管	理接口,不可删除			
网络接口	*网络接口:	eth0					
路由设置	类别:	LAN					
HOSTS							
創 集群管理	网络配置						
昰 特性中心	* 网口地址:	10.243.0.13/	24				
四 系统运维 >					1/512行	ли 4-д 11	
	首选DNS:	114.114.114	.114				
	备选DNS:						

## 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。

🕝 零信任综合	网关 V2.0	监控中	心 业务管理	UEM 安全	P心 系统管理	审计中心		
< 1/2 >				▲ 您的磁盘速度	(write:0.9MB/s read:1	1.8MB/s)不满足最低要	求 (磁盘读速度不能低于40MB	/s,写速度不能低于40ME
系统管理	⊒	日期与时间	客户端接入设置	控制台选项	隐私设置			
& 管理员配置	>	客户端接入地址						
◎ 系統配置	~	1. 接入地址 注章: 仅分	: 指终端用户登录aTrust :许诵讨接入她址或别名地	的服务器地址(互联网划 圳清求aTrust、其它地划	处或内网地址),用户 比将拒绝接入以防止HOS	在未登录aTrust时直接i T攻击。	方问业务系统,将重定向到该地	业进行登录。
通用配置		2. 用户还派 3. 为方便称	有安装客户端?可下载 动端APP用户接入,可了	客户端 进行客户端分发; 「戴二维码 分发给终端用	沪,用户扫码即可自动:	完成接入地址填写 (当)	3用第二代SPA时,将同时自动地	直写安全码) 。
证书管理		(注) ###4.	https:// 111		配署到之前	9+1F		
授权管理		按八地址:	nups,// 111.		ROEDSTAR	DAT		127
邮件服务器			客户端连接界面里	《认展开安全码输入框 (	D	· 填入VPN ECS	分配的弹性公网IP地址	<u>11-</u>
短信网关			✓ 客户端安装包文件	名携带接入地址 🚺				
消息推送配置		端口设置						
52 终端个性配置	>	HTTPS监听端[	1: 443	置多端口 ()				
● 网络部署	>	HTTP监听端口	: ☐ 启用并使用HTTP	满口 80				
			当使用HTTP访问	时,自动跳转HTTPS接)	•			
創 集群管理	>	证书认证端口:	合用证书认证端[					

#### 密级:公开

密级:	公开
-----	----

🕝 零信任综合网	关 V2.0	监控中心	业务管理	UEM 安全	全中心 🚿	统管理	审计中心		
< 1/2 >			您的磁盘速度(write:	0MB/s read:32.9MB/	s)不满足最低要求	(磁盘读道	惠度不能低于40MB/s,写透	態度不能低于40MB/s)	,请尽快更换磁盘
系统管理	Ξ	日期与时间	<b>将户端接入设置</b>	控制台选项	隐私设置				
↓ 管理员配置	>	当未填写局域 选路原理:当	网访问地址与互联网说 冬端在局域网时,aTru	5问地址时,默认使用3 ust客户端使用局域网订	客户端接入地址作; 5问地址作为隧道;	为隧道接入 接入地址;	、地址。		
◎ 系统配置	~	当终端在互联 当终端既能访问	网环境下,aTrust客户 可局域网也能访问互助	端使用互联网访问地址 网的情况下,aTrust看	L作为隧道接入地 客户端会采用接入i	址; 速度快的一	-个地址作为隧道接入地址		
通用配置		局域网访问地址:	10.1.245.157:441			<b>(i)</b>			
证书管理							填入 VPN VPC子网利	4网地址	
授权管理									
邮件服务器					1/64	ř			
短信网关		互联网方问地址:	139.159.231.34:44	41		0	▶ 插入 VPN 弹性公网	ilP地址:441保持2	不变
消息推送配置							Seven marine and	THE REAL CONTRACT.	
🖬 终端个性配置	>				2/6//=				
● 网络部署	>	选路策略配置			2/044]				
1 集群管理	>	SSL/TLS协议设置	<b>(</b> )						
昰 特 <u>性</u> 中心		♀ 1.为保障正常は	前问,当前设备不支持	禁用【国际密码标准】					

## 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

🕝 零信任综合	网关	监控中心	业务管理	UEM	安全中心	系统管理	审计中心	
业务管理	П	用户管理						
& 用户管理		●新増 Q 刷新						
🗊 认证管理	>	名称		⇒ 描述	5			目录类型
□; 应用管理	>	2 本地用户目录		平台	內置用户目录			平台内置
🗏 终端管理	>							
& 角色管理								
圆 权限基线								
日 策略管理	>							

步骤二:在组织架构处,点击<+添加>。

		• 警告:	当前设备用户	中授权即将过期,为避免影响;	2番的正常使用,请前往深信服授权中心!
<u> </u> 务管理	E	←   本地用户管理			
3 用户管理		组织架构群组	<b>〇</b> 新	増用户 🔰 🛃 批量导,	入 🛛 🔂 批量导出 👘 🗘 刷
] 认证管理	>	组织架构 +添加		/ / / / //////////////////////////////	授权
♂ 应用管理 应用列表	~			□ 名称 □ <b>1</b> user4	↓ 所屬组织架构 /ssl
应用权限审批 免认证应用		Mi 17 1000		L test1       L test1-moon	/ /部门1-moon
े 角色管理				L test3-moon	/部门1-moon
3 权限基线				L test2-moon	/部门1-moon
■ 策略管理	>				

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

密级:2	公开
------	----

2	←   新増组织	装构		
	基本属性			
>	*名称:	ITES/]	所属组织架构	×
~	描述:		搜索	Q
>	* 所置迫积滞构:		□ ► / ■ ssl ■ 即门1-moon	
				确定取消

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>

		• 警告:3	当前设备用户授权即将过期,为避免影响;	设备的正常使用,请前往深信服授权中心 https	://license.sangfor.com.cn 复制地	b) 为设备授权续费。如已续费,请及时在设备本地导入	、最新的词
业务管理	Ξ	←   本地用户管理					
& 用户管理		组织架构 群组	● 新増用户 🛃 批量导	入   💼 批量导出   🗘 刷新	● 绑定管理		
🗊 认证管理	)	组织架构 + 添加		18 11 11 11 11 11 11 11 11 11 11 11 11 1			
□ 应用管理	~		□ 名称	新属组织架构	\$ 群组	⇒ 手机号码	
应用列表		ssl					
应用权限审	甜	— <b>胎</b> 節(]1-moon					
免认证应用	3						
』。 角色管理	I.						
权限基线	a						
品 策略管理	×					留元炭振	

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。

业务管理			
	←   新瑁本地/		
A 用户管理	基本属性		
創 认证管理	* 用户名:	运维人员1	
□; 应用管理	→ 描述:	请输入用户描述信息	
应用列表	* 所屬组织架构:	/IT音阶] :三	
应用权限审批	群组:	点击选择群组	
免认证应用	*密码:		0
▲ 角色管理	*确认密码:		
圓 权限基线		随机密码并复制	
<b>品</b> 策略管理	电子邮箱:	请输入电子邮箱	
	手机号码:	请输入手机号码	
	过期时间:	● 永不过期	
		○手动设置 2021-06-25 前	当天23点59分过期
	账号状态:	● 启用 ○ 禁用	
	策略设置		
	(组内新增用户量	状认优先采用如下的认证策略和用户策略)	
	认证策略:	默认策略 😑 🕤 新增	
	保存	保存并继续添加取消	

步骤六:新增后即可在IT部门组织中看到该运维人员1。

组织架构 群组 6	)新增用户   📩 批量导入	🛃 批量导出 🔰 🗘 刷新	◎ 绑定管理	
组织架构 + 添加	IT部门 《编辑	€授权		
	名称	⇒ 所屋组织架构	↓ 群組	⇒ 手机号码
···· ••• ITAN'] ····	□ 💄 运维人员1	/IT部门	12	2
部门1-moon				

# 3.3.2. 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=viewdat abase&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>。

🕝 零信任综合	网关	监控中心	1	管理 UEM 安全中心	系统管理 审计中心	
业务管理	П	应用列表				
& 用户管理		应用分类	+	♥新増 ■計  ■計  ■計  ■計  批量等入	☆ 批量导出 ○ Q 刷新	🖥 自动采集站点
🗊 认证管理	>	国際	Q	日 名称	≑ 访问模式	≑描述
□2 应用管理	~	□· <b>&gt;&gt; 所有</b> □ <mark>&gt;&gt; </mark> 默认分类		🔲 📄 baidu	WEB模式	3
应用列表						
应用权限审批						
免认证应用						
🗏 终端管理	>					
& 角色管理						
圆 权限基线						
品 策略管理	>					

### 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、服务器地址端口

零信任控制中心 v2	0 监控中心	业务管理 UEM 安	全中心 主动防御	系统管理 审计	中心		
< 1/2 >			<b>经检测,当前设备未运行虚拟</b> 相	1.性能优化工具,可能导致	欧业务访问失败,i	清尽快退出控制台部署相关工具	
业务管理 三	←   新増应用						
& 用户与角色	应用属性						
創 认证管理 >	发布模式:	● 隧道资源 (推荐) ()	○ WEB资源 (〕	○ WEB泛域名资源	<b>○</b> ≢	面云资源 🚺	
□2 应用管理 ✓	*名称:	请输入应用名称					
应用列表	描述:	请输入描述文字					
应用授权	*所属应用分类:	集团应用	=		支持端口号。 单个端口号:	或調口范围, 如: : 35	
应用权限审批	*所属节点区域:	【虚拟ip演示完成后,请及时关闭】》	\$ <u>₩</u> \$\$\$		端口范围: 多个: 35,40	1-65535 0-50,80	
终端管理    >	*服务器地址:	序号 * 协议 ① * 服	务器地址 (1)	* it	第日 ①	操作	
品 策略管理 >		1 TCP • 1	72.22.230.200		端口 口	•	
		□ 排除部分服务器地址   配置指导图	8			1/128行	
	应用状态:						
	个性设置	代理设置安全设置	汞登点单				
	应用中心设置						
	应用可见:	✓ 允许用户可见 (显示在应用中心)					
	*应用图标:	<ul> <li>内置图标</li> <li>本地上传</li> </ul>					
	指定应用打开方式	(指定程序和系统应用功能仅支持通过客	户端工作台打开) ()				
	保存	保存并继续授权 取消					

如: 协议:TCP/ALL 服务器地址:172.22.230.200 端口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。 其他选项:可默认

步骤三:填写后保存即可在应用列表看到该发布的资源。

应用列表													
应用分类	+	0	新聞   <u>前</u> 1000	▲ 北重导入   ▲ 北重导出   (		54			全部	•   38	自入关键字	(	Q
田 医 銀素	Q		名称	○ 访问模式	: 描述	\$ 版	i調服务器地址 ÷	惹靖访问地址		状态	\$ 操作		
🖃 늘 所有			■ 注射平台2	能道模式		17	72.22.230.200:8001	http://172.22.230.200:8001		~	编辑	<b>10</b>	
第6.5章			🖬 深信服業网	WEB構式		ht	ttps://www.sangfor.com.cn	https://www.sangfor.com.cn		~	编辑	#19:	
test1			■ 深信服w3	WEBREC		ht	ttps://w3.atrust.sangfor.com.cn	https://sangfor.whitemoonfl	/.xyz	~	编辑	209	
			1 软件仓库	WEBI		ht	ttp://200.200.4.209:80	http://testapp.whitemoonfly	xyz:60202	~	编辑	<b>E</b> (1)	

# 3.3.3. 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=viewdat abase&tid=158655&highlight=

步骤1. 在[业务管理/应用管理/应用列表]中选择应用,点击后面的授权按钮。

중信任控制中心 va	2.0 监控中	U WREE	UEM 安全中心	主动防御 系统管理	审计中心			搜索	9	🛎 🕜 🤱 sdj	pdemo ·
< 1/2 >			🌲 经检测	,当前设备未运行虚拟机性能优化工具	, 可能导致业务访问失败, 请尽快退出控制	1台部署相关工具。					
业务管理 🏾 🖃	应用列表										
& 用户与角色	应用分类	+	71980 2应用	的美编辑 之应用分类授权							
同认证管理 >	71980	×Q	O #12 11 110			白动学生以点		快速篮话	全部 -	诸编入关键字	0
_	<b>∷ 71980</b>		— 名称	: 访问模式	↓ 后端服务精地址	前號访问地址	免认证设置	- ALING	状态	2 操作	
しる 应用管理 シン			🗌 🔡 平台系统	隧道模式	12.12.13.13:55				Ħ	编辑 授权 删除	
应用列表										1	
应用授权										/	
应用权限审批										/	
日 终端管理 >											
品 策略管理 >											

步骤2. 在选择授权设置, 然后点击需授权的用户/用户组。

중信任控制中心 v₂.	0) 監控中心 业务管理 UEM	vi 安全中心 主动防御 系統電	理 审计中心				搜索	۵) 🖲 🕲 🤱	sdpdemo •
< 1/2 >		自己的公司中国行应权机性能优	比工具,可能导致业务访问失败,请	尽快退出控制台部署相关工具					
业务管理 三	应用授权							🛊 授权过期	明經醴设置
名 用户与角色	血用 应用分类 🛔 平台	选择授权对象							×
	THERE XQ	▲ 组织架构与用户 △ 角色 当	藏用户目录:本地用户目录			已透 (0)			清空
Ca 应用管理 🛛 🗸 🗸		Q 请输入关键词,支持搜索组织帮助名称及用	卢全部字段信息		匙	名称	所屋组织架构	所雇用户目录	操作
应用列表	日本の	E = /	待适						
应用路权			各称	显示名	所屬組织架构 …				
应用权限审批			普勒组: 🐂 / (选择当前组数	认包含以下子组及用户)	选择本组				
			🗆 🕨 ya Talah		1				
E SCHERKE /		- 5/1 P	<ul> <li>Market</li> </ul>	×					
日 策略管理 >			- · · · ·		1200		~ 1	Ś	
		- 📁 angalaki	🗆 🕨 Tariyi		T		17.2	and the second se	
		- Jewa	Image: A set of the		and the second s		Ta A.s	KBW	
			, 🕒 🕨 1997		× .				
		- <u>-</u> - 254	10	×.					
		- 187	🗆 🕨 🛤 👘						
				-					
		- 늘 488	共12146项	2 608	> 每页 20 * 条				
		/						确定	取消

步骤3. 在弹出的窗口选择定制平台2。

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。

## 3.3.4. 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)。

중信任安全代	理网关	自然中心 新鮮	前理 审计中心	
< 1/2 >			🌲 Sideka	世行健康检查,为存殖设备健康运行,请尽快进行健康检查 立即检查
系统管理	Ξ	控制台命令 文件管理		
😑 本机管理		命令名称 help	说明 显示全部支持命令用法 三帝月41余帝中法	用法 belp manual manual and a set of the set
③ 系统配置	>	ctrl+c uptime	结束当前执行程序 握实当前执行程序 整实实法:2017多长时间	Artar web we to Sha ping "Arping - Help (社種 (ctt+c) uptime
8 Risting	>	route traceroute arp	宣會超出现會 跟踪裁据包到达网络主机所经过的路由 查看设备asp表	route -s traceroute host (M) traceroute 192.160.1.1) arp
		arping ping ifconfig	用于发送amp请求到一个相邻主机 测试设备与其他主机的连接情况 查看设备网收信息	arping (-I interface) (-3 第19) 田林19 ping hostname (-I interface or address) (-c count) ifconfio
@ 系统运输	~	ip tepdump	査督设备121信息 派取教授包命令 法市込み回り休暇 1127年1	可在ip后结合查通的内容,如ip rule tepdumg [options] [hoat IF] (別tepdumg -w a.cap hoat 192.168.1.1)
SNMP 配置备份与恢复		telnet atrust_tool	室看发着两口隔想,加以上有55 查看某个端口是否可以访问 日志导出,获取春户端日志,切换日志级别	etntoi uzvaame (mu etntool etnu) teinet ip port(Mu teinet 192,168.1.1 8080) atrust_tool export log, atrust_tool health, atrust_tool client [cmd] [cmd_args], atrust_tool log [cmd] [cmd_args]
Webconsole		grep teil wget	按条件宣挑文件中字符串 显示文件末尾的内容 从网络中下载文件的工具	<pre>grep [options] partern [file] (f0 grep -r test /bome/*) tail [-f] [-n number] file (f0 tail -f -n 10 test.log) wget [options] [UBE] (f0 were bruns/198.168.1.100)</pre>
系统开级		curl openasl	从服务器中接受成者传输数据的工具 Open SSL命令行工具	curl (URLs) (ÅD curl https://192.165.1.1:80) openssl command (command_opts) (command_args)
设备运经		ps netstat iptables	显示当前进程信息 显示网络、接口、路由等信息 查看包过滤规则	ps [options] (5] ps -mux) metstat [options], (5] metstat -n) iptables [options] (5] piptables -n)
		free df	亚看内存信息 亚看պ盘信息	free (options) (0 free -h) df (options) (0 df -h)
		ifstat 1sof	查看Cablands 查看州培推口数据 查看进程打开文件的信息	mpstu (options) (Nulmpstut = A) ifstat [options] (Nulfstat = p) laof = 1[1] (Nu laof = 14)
		tor vi 清楚入theint宫后更杂会分	压缩和解压缩工具 文本编辑工具	tar [options] filename (fültar -xxvf test.tar.gz) vi file (fülvi test.txt)
		> ping 172.22.230.200 PING 172.22.230.200 (172.22.2	30.200) 56(84) bytes of data.	
		64 bytes from 172.22.230.200: 64 bytes from 172.22.230.200: 64 bytes from 172.22.230.200:	<pre>icsp_seq=1 ttl=125 tixe=20.2 ms icsp_seq=2 ttl=125 tixe=0.652 ms icsp_seq=3 ttl=125 tixe=2.18 ms</pre>	
		> telmet 172.22.230.200 8001 Connected to 172.22.230.200		

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。

@aTrust		<b>⇒</b> - ×
◆ 温馨提示 实验使用案信任,重要会全边界	本地密码认识	E
	用户名	
	运维人员1	
	密码	
	✓ 我已阅读并同意 (用户协议)	-
"零信任	東登	
重朔空令边界"		halon.
里望女主边7	- 其他登录方式 -	
	0	
	aTrust APP扫码	

ତ	应用中心	申请权限 +	
86	默认分类		
	默认分类		
	定制平台2		

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

问题咨询支持:

1.如您有商务问题咨询,请拨打云市场用户商务专线:0755-86965494; 2.如您有售后问题咨询,请拨打云市场用户售后服务专线:0755-23832091