



SANGFOR
深信服科技

深信服云安全中心（CSC）端点安全 软件服务器版 aES 部署实施指导书 V1.0.0

深信服科技股份有限公司

2023 年 11 月

版权声明

深信服科技股份有限公司版权所有, 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。

信息反馈

如果您有任何宝贵意见, 请反馈至:

地 址: 深圳市南山区学苑大道 1001 号南山智园 A1 栋

邮 编: 518055

电 话: 0755-86627888

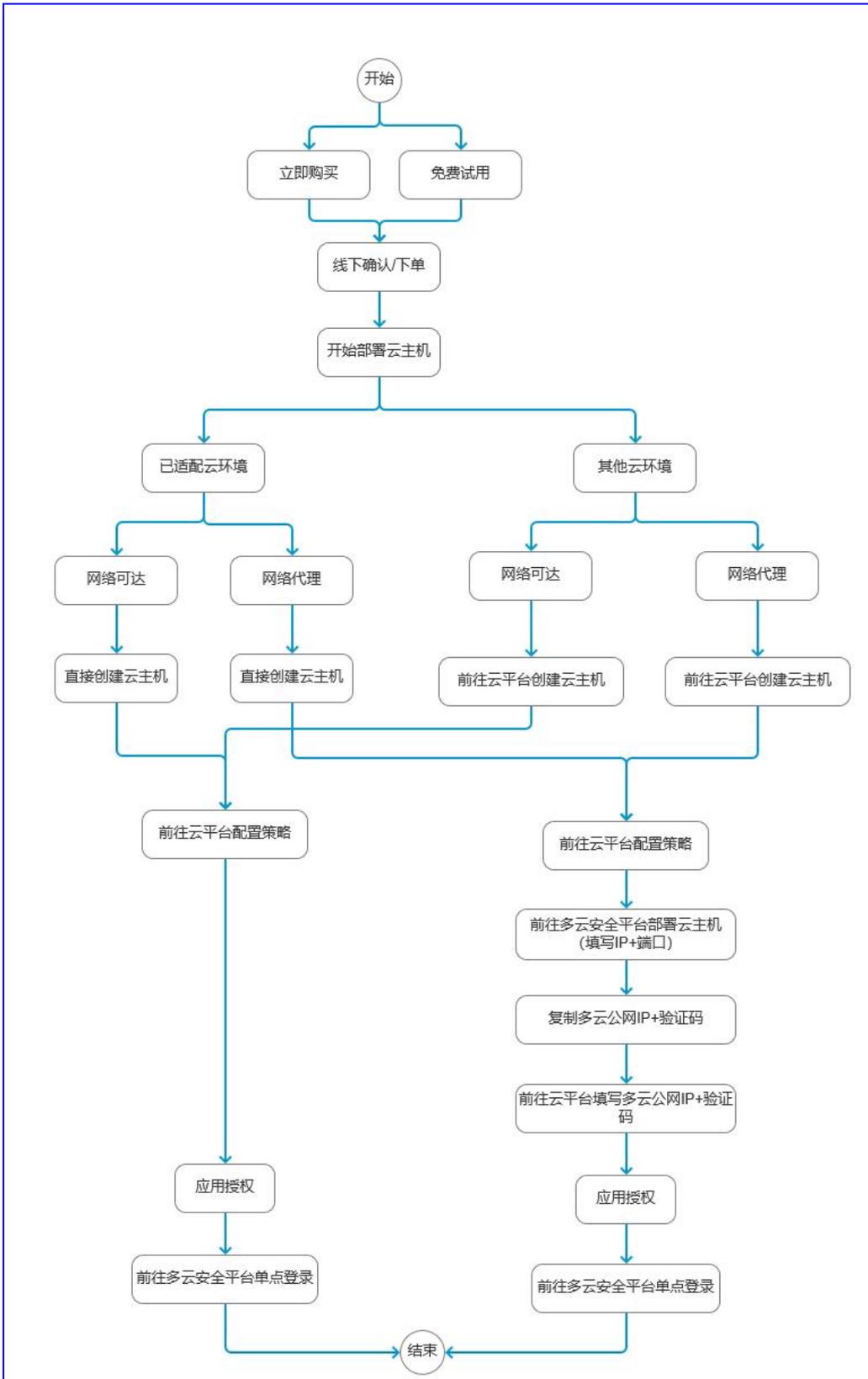
传 真: 0755-86627999

您也可以访问深信服科技股份有限公司官方网站: www.sangfor.com.cn 获得最新技术、产品和方案信息。

目 录

1 流程介绍	1
2 操作步骤	2
2.1 部署云主机	2
2.1.1 已适配云环境	3
2.1.2 其他云环境	8
2.2 配置策略及授权	9
2.2.1 网络可达方式一：云主机绑定公网 IP 方案	9
2.2.2 网络可达方式二：使用 DNAT 方案	11
2.2.3 网络代理方式：使用 SNAT 方案	17
2.3 单点登录	21
2.4 应用组件规格及资源消耗表	22
2.5 云平台链接汇总	22

1 流程介绍



2 操作步骤

2.1 部署云主机

云环境选择说明

1、未创建云主机：

(1) 云安全中心已适配“阿里云”“腾讯云”“华为云”，您可通过云安全中心创建这三个云环境的云主机。

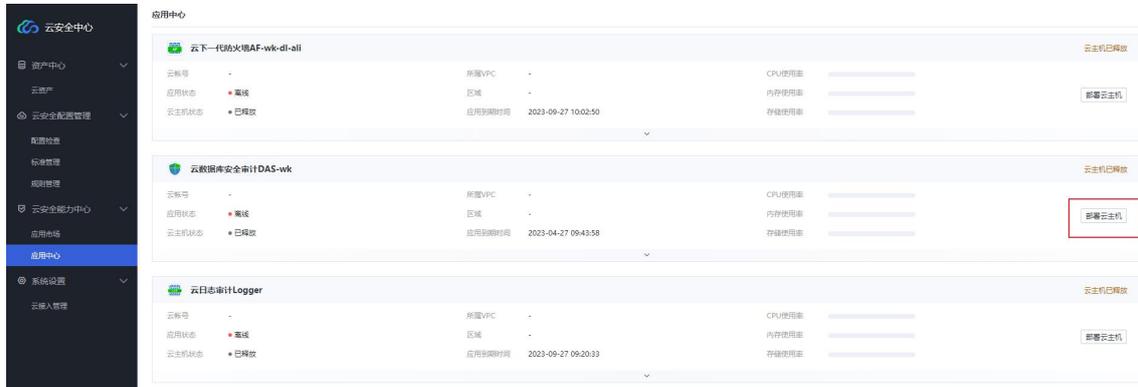
(2) 若在云安全中心购买的应用组件需要部署到“阿里云”“腾讯云”“华为云”以外的云环境，请先联系云安全中心客户经理分享镜像，通过该镜像在云平台创建云主机并配置安全组、NAT 等相关策略后，再在云安全中心选择“其他云环境”并填写公网/私网 IP 和端口信息。

2、**已创建云主机：**若您已创建了云主机（包括阿里云、腾讯云、华为云等云环境），在云安全中心统一管理时，请先配置安全组、NAT 等相关策略，再在云安全中心选择“其他云环境”并填写相关信息。

说明：可前往云平台查看 NAT。查看[阿里云 NAT 说明文档](#)

2.1.1 已适配云环境

在[云安全能力中心-应用中心](#)找到待部署的应用，点击“部署云主机”进行部署。



1、选择云环境与应用授权方式

选择云环境：支持选择“阿里云”“腾讯云”“华为云”。

选择云帐号：选择已接入的云帐号。若没找到合适的云帐号请先接入。接入说明请查看《连接云环境说明文档》

主帐号 ID：选择“阿里云”“腾讯云”时，需提供所选云帐号的主帐号 ID 用于创建云主机。可前往云平台-帐号信息复制主帐号 ID。

说明：主帐号 ID 填写错误会导致镜像分享失败。

(1) 获取阿里云主帐号 ID，主帐号[登录阿里云控制台](#)时，鼠标悬浮 hover 用户头像并复制下图的账号 ID 即可。



(3) 获取腾讯云主帐号 ID，主帐号[登录腾讯云控制台](#)时，鼠标悬浮 hover 用户头像并复制下图的账号 ID 即可。



(4) 获取腾讯云主帐号 ID，子帐号[登录腾讯云控制台](#)时，鼠标悬浮 hover 用户头像并复制下图@后的主帐号 ID 即可。



应用上线方式：包括网络可达、网络代理。

(1) 网络可达

适用场景：有对外提供服务的公网 IP 或允许云安全中心主动连接您应用组件的公网 IP。

方案：需您提供公网 IP 及端口信息。您可选择主机直接绑定公网 IP 或通过 DNAT 配置。详情查看 [2.2.1 网络可达方式一](#)及 [2.2.2 网络可达方式二](#)。

(2) 网络代理

适用场景：没有对外提供服务的公网 IP 或不允许云安全中心主动连接您应用组件的公网 IP。

方案：通过您的应用组件连接云安全中心的公网 IP，需您前往云平台登录云主机填写云安全中心公网 IP 及验证码信息。详情查看 [2.2.3 网络代理方式](#)。

2、创建云主机

付费模式：可选包年包月、按量付费，建议选择和应用一致的付费模式。

购买时长：建议购买和应用一致的时长。免费试用结束的应用重新购买后，请前往云平台将云主机的到期时长更改成与应用一致或更长。

地域：选择业务所在私有网络的地域。

网络：选择业务所在的私有网络及子网。

项目 ID：云环境选择“华为云”时，需要填写项目 ID。

性能参数：云安全中心根据应用选型自动计算出对应的实例规格、存储。

公网 IP：选择网络可达方式需提供公网 IP，如应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成并进行 DNAT 网关相关配置后，再前往云安全中心找到应用填写绑定在 DNAT 上的公网 IP。

端口：默认选择 443。

安全组：第一次连通必须将 443 端口的访问策略设置为允许云安全中心（42.193.174.234）访问。

2.1.2 其他云环境

1、选择云环境与应用上线方式

需要选择“其他云环境”的情况如下：

1、若您需在“阿里云”“腾讯云”“华为云”以外的云环境部署，请先联系云安全中心客户经理分享镜像，通过该镜像在云平台创建云主机并配置安全组、NAT 等相关策略后，再在云安全中心选择“其他云环境”并填写公网/私网 IP 和端口信息。

2、已创建云主机：若您已在阿里云、腾讯云、华为云创建云主机，在云安全中心统一管理时，请先配置安全组、NAT 等相关策略，再在云安全中心选择“其他云环境”并填写相关信息。

应用上线方式：包括网络可达、网络代理。

(1) 网络可达

适用场景：有对外提供服务的公网 IP 或允许云安全中心主动连接您应用组件的公网 IP。

方案：需您提供公网 IP 及端口信息。您可选择主机直接绑定公网 IP 或通过 DNAT 配置。详情查看 [2.2.1 网络可达方式一](#)及 [2.2.2 网络可达方式二](#)。

(2) 网络代理

适用场景：没有对外提供服务的公网 IP 或不允许云安全中心主动连接您应用组件的公网 IP。

方案：通过您的应用组件连接云安全中心的公网 IP，需您前往云平台登录云主机填写云安全中心公网 IP 及验证码信息。详情查看 [2.2.3 网络代理方式](#)。

2、创建云主机

付费模式： 可选包年包月、按量付费，建议选择和应用一致的付费模式。

购买时长： 建议购买和应用一致的时长。免费试用结束的应用重新购买后，请前往云平台将云主机的到期时长更改成与应用一致或更长。

地域： 选择业务所在私有网络的地域。

网络： 选择业务所在的私有网络及子网。

性能参数： 根据云安全中心提供的应用选型选择云主机规格及存储。点击查看 [应用组件规格及资源消耗表](#)

公网 IP： 选择网络可达方式需提供公网 IP。若应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成进行 DNAT 网关相关配置后，再前往 [云安全中心-云安全能力中心-应用中心](#)找到应用填写绑定在 DNAT 上的公网 IP。

端口： 默认选择 443。

安全组： 第一次连通必须将 443 端口的访问策略设置为允许云安全中心（42.193.174.234）访问。

2.2 配置策略及授权

2.2.1 网络可达方式一：云主机绑定公网 IP 方案

2.2.1.1 配置策略

确认安全组策略： 云主机绑定的安全组 443 端口允许云安全中心（42.193.174.234）访问。

说明：

- 1、若云主机所关联的安全组不符合要求，请前往云平台-安全组创建安全组并绑定云主机。
- 2、若需换成其他的端口，请在第一次授权成功后再修改。

2.2.1.2 应用授权

网络可达模式配置正确，会自动发起第一次授权，请前往[云安全中心-云安全能力中心-应用中心](#)查看，当应用状态更新为“正常”即为授权成功。后续应用离线后需您主动“发起连接”才能再次连通。

说明：云环境为“其他云环境”时，完成以上配置后请前往[云安全中心-云安全能力中心-应用中心](#)找到该应用，点击“部署云主机”填写云主机的公网IP及端口信息，当应用状态更新为“正常”即为授权成功。

(1) 填写公网IP及端口并点击立即部署

* 选择云环境

阿里云 腾讯云 HUAWEI 其他云环境

* 应用上线方式

网络可达
通过公网IP进行网络通信

网络代理
通过登录主机填写服务器IP和验证码进行反向网络通信

[查看说明文档](#)

连接云主机

公网IP

端口

应用验证 修改登录应用的用户名/密码
用户名和密码默认都为admin，若您修改过该信息，请重新录入

[立即部署](#) [保存信息](#) ⓘ

(2) 查看应用状态

云日志审计Logger

云账号	所属VPC	xxxx	CPU使用率	4.00%	进入应用
应用状态	区域	华北地区(北京)	内存使用率	46.00%	登录云主机
云主机状态	应用到期时间	2021-10-28 15:55:33	存储使用率	1.00%	

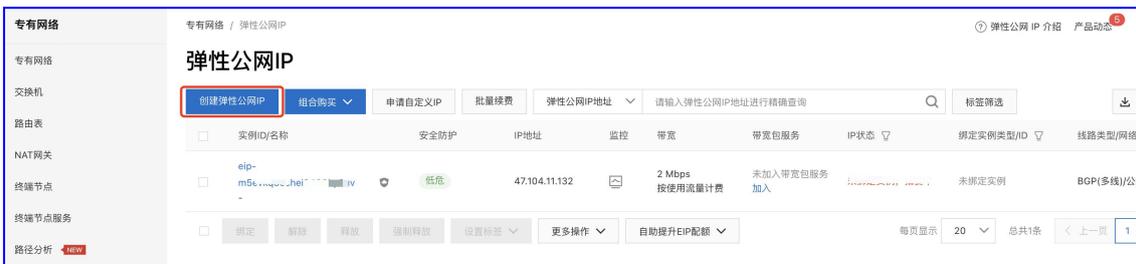
2.2.2 网络可达方式二：使用 DNAT 方案

选择网络可达方式需提供公网 IP，如应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成并进行 DNAT 网关相关配置后，再前往[云安全中心-云安全能力中心-应用中心](#)找到应用填写绑定在 DNAT 上的公网 IP。

2.2.2.1 配置策略

2.3.2.1.1 创建弹性公网 IP

1、前往弹性公网 IP 控制台-创建公网 IP。如您已创建请直接往下配置 DNAT。



2、填写相关信息，其中地域需选择与云主机、NAT 相同的地域。



2.2.2.1.2 配置 DNAT

1、前往专有网络控制台-NAT 网关-进入 NAT 网关详情



说明：若创建新的 NAT 网关，需选择与主机相同的地域及 VPC。

2、在“DNAT”页面创建 DNAT

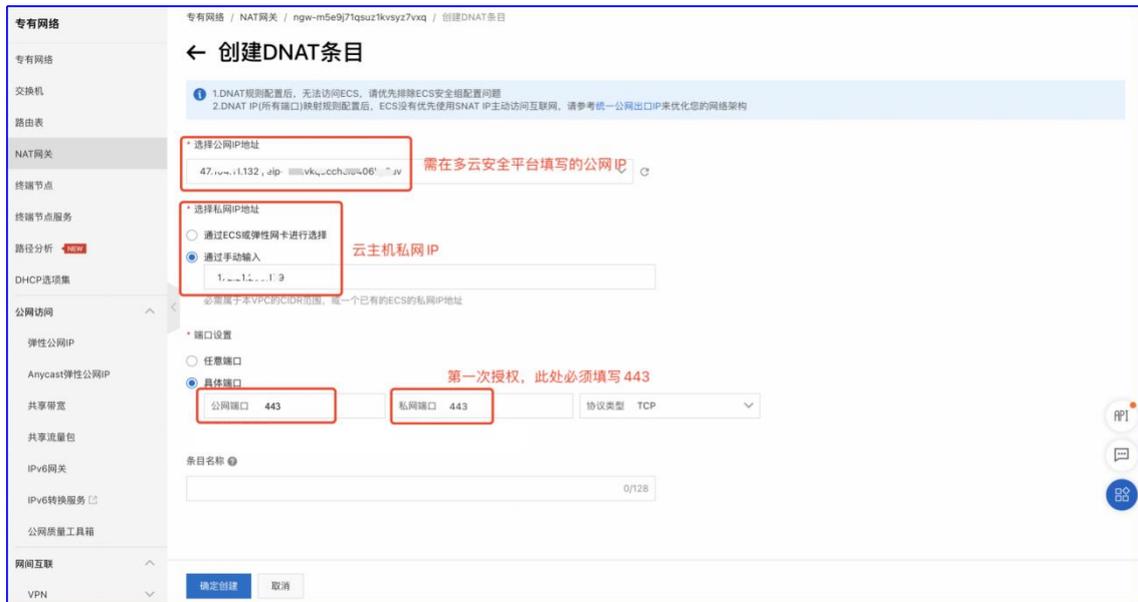


3、填写 DNAT 条目信息并点击确定创建

选择公网 IP 地址：选择弹性公网 IP，该公网 IP 需在云安全中心填写

选择私网 IP 地址：选择刚刚创建云主机的私网 IP。

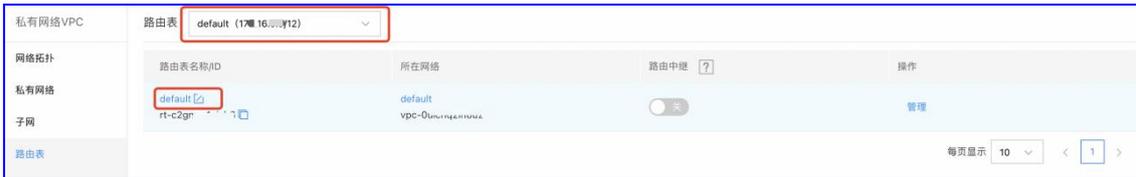
端口设置：公网端口可自定义，该端口需在云安全中心填写；第一次授权时必须填写 443。



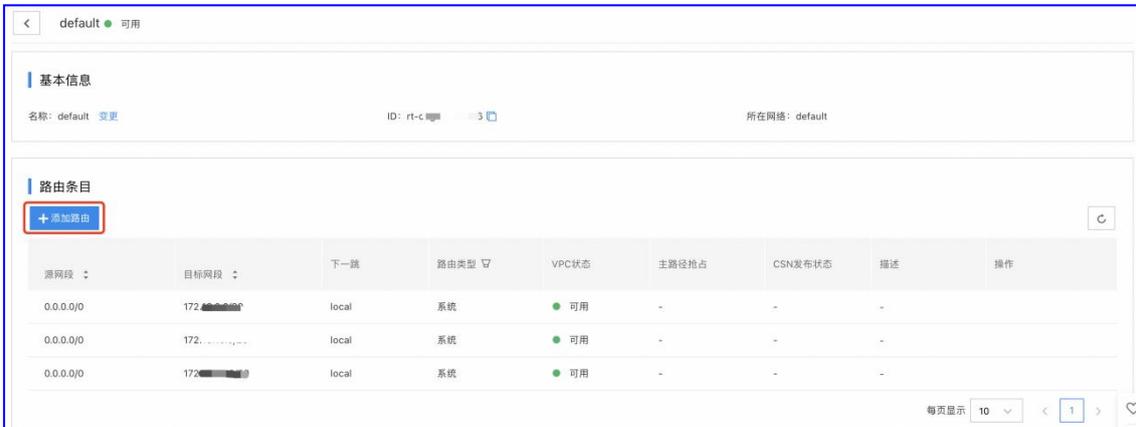
2.2.2.1.3 配置路由表

说明：阿里云不需要配置路由表，腾讯云、华为云、百度云需要配置路由表。

1、选择路由表并点击进入路由表详情页



2、添加路由



3、填写路由信息并点击确定

源网段：当前云主机所在的网段

目标网段：云主机需要访问的网段

路由类型：选择“NAT 网关”

下一跳实例：选择刚刚配置的“DNAT 实例”

添加路由 ×

网段类型： IPV4 IPV6

* 源网段：

* 目标网段：

路由类型：

* 下一跳实例：

描述：

2.2.2.1.4 确认安全组策略

第一次授权需设置云主机绑定的安全组 443 端口允许云安全中心(42.193.174.234)访问。

说明：

1、若云主机所关联的安全组未符合要求，请前往云平台-安全组创建安全组并绑定云主机。

2、若需换成其他的端口，请在第一次授权成功后再修改。

2.2.2.2 应用授权

网络可达模式配置正确，会自动发起第一次授权，请前往云安全中心-云安全能力中心-应用中心查看，当应用状态更新为“正常”即为授权成功。后续应用离线后需您主动“发起连接”才能再次连通。

说明：云环境为“其他云环境”时，完成以上配置后请前往[云安全中心-云安全能力中心-应用中心](#)找到该应用点击“部署云主机”或“更改信息”并填写 DNAT 绑定的公网 IP 及端口信息，当应用状态更新为“正常”即为授权成功。

(1) 填写公网 IP 及端口并点击立即部署



* 选择云环境

阿里云 腾讯云 HUAWEI 其他云环境

* 应用上线方式

网络可达
通过公网IP进行网络通信

网络代理
通过登录主机填写服务器IP和验证码进行反向网络通信

查看说明文档 ↓

连接云主机

公网IP 1.2.3.4

端口 443

应用验证 修改登录应用的用户名/密码
用户名和密码默认都为admin，若您修改过该信息，请重新录入

立即部署 保存信息 ⓘ

(2) 查看应用状态



云日志审计Logger

云账号	xxxx	所属VPC	xxxx	CPU使用率	4.00%	进入应用
应用状态	● 正常	区域	华北地区(北京)	内存使用率	46.00%	登录云主机
云主机状态	● 正常	应用到期时间	2021-10-28 15:55:33	存储使用率	1.00%	

2.2.3 网络代理方式：使用 SNAT 方案

2.2.3.1 配置策略

2.2.3.1.1 创建弹性公网 IP

1、前往弹性公网 IP 控制台-创建公网 IP。如您已创建请直接往下配置 DNAT。



2、填写相关信息，其中地域需选择与云主机、NAT 相同的地域。



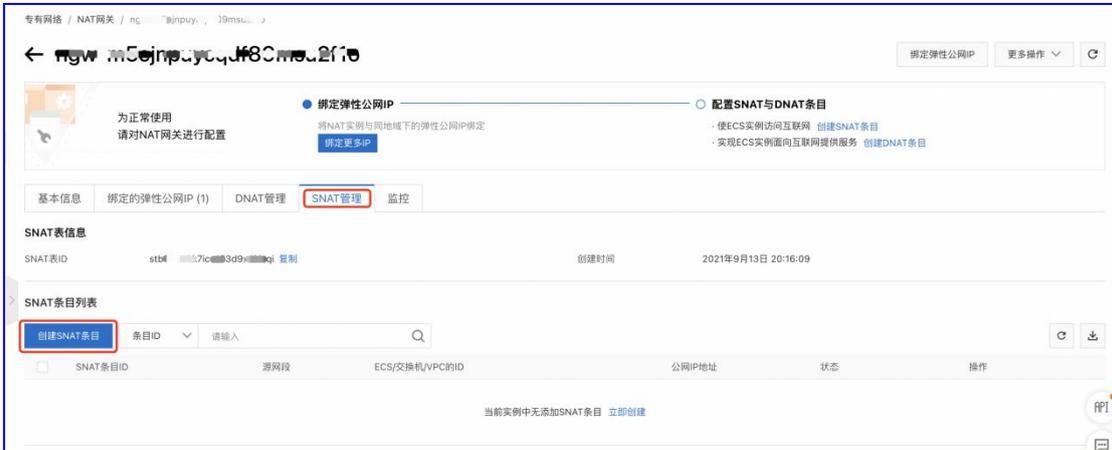
2.2.3.1.2 配置 SNAT

1、前往专有网络控制台-NAT 网关-进入 NAT 网关详情

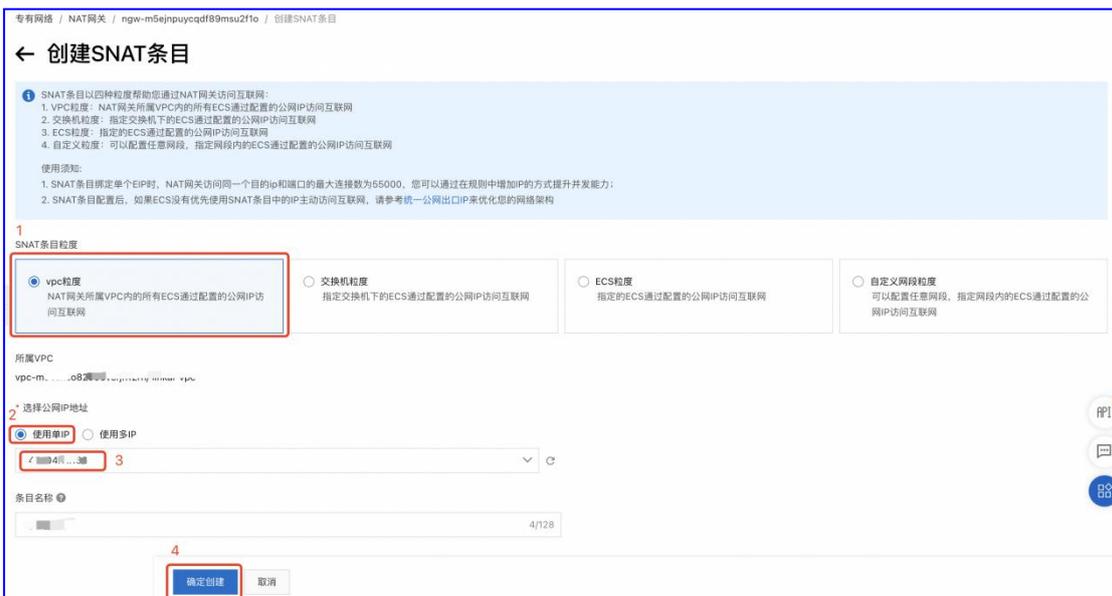


说明：若创建新的 NAT 网关，需选择与云主机相同的地域及 VPC。

2、在“SNAT”页面创建 SNAT



3、选择 vpc 粒度及刚刚创建的公网 IP 并点击“确定创建”



2.2.3.2 填写验证码

第一步：前往[云安全中心-云安全能力中心-应用中心](#)查看应用的验证码

说明：云环境选择其他云环境时，在云平台创建云主机后，需在[云安全中心-云安全能力中心-应用中心](#)找到该应用订单点击“部署云主机”，填写云主机的私网 IP 及端口信息，部署完成应用同步成功即可查看验证码。

(1) 部署云主机

*选择云环境

阿里云 腾讯云 HUAWEI 其他云环境

*应用上线方式

网络可达
通过公网IP进行网络通信

网络代理
通过登录主机填写服务器IP和验证码进行反向网络通信

查看说明文档 ↓

连接云主机

私网IP 12...1

端口 443

应用验证 修改登录应用的用户名/密码
用户名和密码默认都为admin，若您修改过该信息，请重新录入

立即部署 保存信息 ⓘ

(2) 查看并复制验证码

云下一代防火墙AF 部署成功，请完成其他配置并登录云主机进行验证

云帐号	其他云环境	所属VPC	-	CPU使用率	██████████	更改信息
应用状态	未上线	区域	-	内存使用率	██████████	查看验证码
云主机状态	-	应用到期时间	2022-09-28 17:48:43	存储使用率	██████████	发起连接

第二步：在云服务器-实例列表找到该主机，并登录/远程连接该主机

ID/名称	监控	状态	可用区	实例类型	实例配置	主IPV4地址	实例计费模式	操作
搜索“所属项目:默认项目”，找到 1 条结果 返回原列表								
<input type="checkbox"/> ins-17f8cyeas 未命名		运行中	南京一区	标准型SA2	1核 1GB 1Mbps 系统盘: 高性能云硬盘 网络: Default-VPC	10.10.1.1 (公) 16.0.0.0 (内)	按量计费 2021-09-17 17:38:17创建	登录 更多

第三步：在“SANGFOR NFV”界面找到“NFV ONLINE SETTING”并点击“OK”



第四步：在“NFV ONLINE”界面的“Ip Or Domain”、“Uerify Code”分别填写云安全中心的公网 IP（42.193.174.234）和应用的验证码。

说明：如未能正常打开“NFV ONLINE”界面，请按 alt+F8 或 option+F8。



2.2.3.3 应用授权

网络代理模式配置正确后将自动授权，请前往云安全中心-云安全能力中心-应用中心查看，当应用状态更新为“正常”即为授权成功。



2.3 单点登录

前往云安全能力中心-应用中心，当应用状态为“正常”时，点击“进入应用”即可单点登录至应用的控制台。



2.4 应用组件规格及资源消耗表

产品名称	应用规格	所需要资源（虚拟核心数、内存、硬盘）	网络可达方式-主机绑定公网 IP 带宽性能
endpoint安全软件 aES 服务器全量版	2 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器全量版	10 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器全量版	100 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器全量版	1000 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器全量版	2000 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器旗舰版	3 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器旗舰版	9 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器旗舰版	90 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器旗舰版	900 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求
endpoint安全软件 aES 服务器旗舰版	1800 个资产授权	4vCPU, 8GiB, 330G 系统盘	无要求

2.5 云平台链接汇总

云平台	分类	链接
阿里云	安全组	立即前往
阿里云	NAT 网关	立即前往
阿里云	弹性公网 IP	立即前往
阿里云	云服务器	立即前往
腾讯云	安全组	立即前往
腾讯云	NAT 网关	立即前往
腾讯云	弹性公网 IP	立即前往
腾讯云	云服务器	立即前往
华为云	安全组	立即前往
华为云	NAT 网关	立即前往
华为云	弹性公网 IP	立即前往
华为云	云服务器	立即前往

百度云	安全组	立即前往
百度云	NAT 网关	立即前往
百度云	弹性公网 IP	立即前往
百度云	云服务器	立即前往