解决方案实践

基于 SNAT 公网访问解决方案

文档版本	1.0.1
发布日期	2024-04-26

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为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，华为公司对本文档内容不做任何明示或暗示的声明或保证。

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

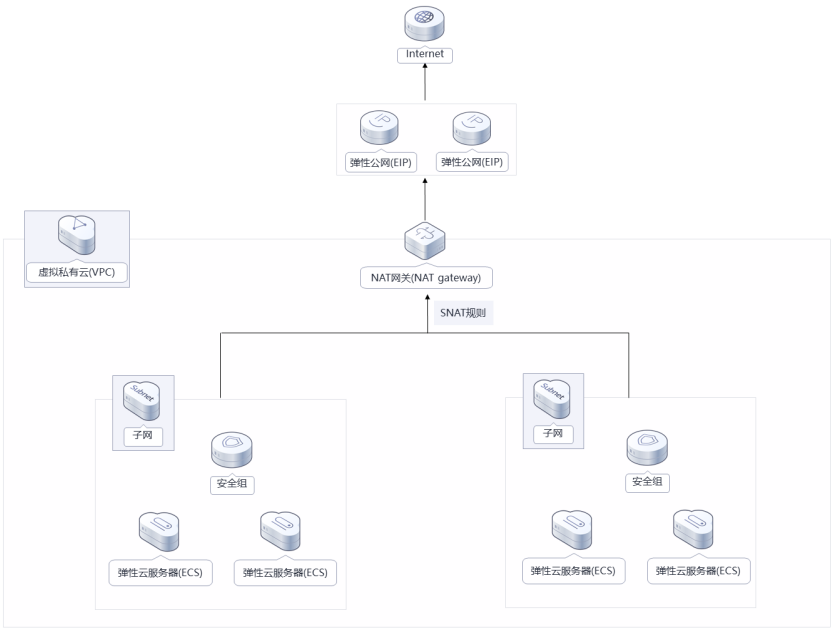
应用场景

该解决方案能帮您快速实现多个无弹性公网IP的云主机安全访问互联网，使用公网NAT网关服务共享弹性公网IP，节省弹性公网IP资源，同时按子网配置SNAT规则，轻松构建VPC的公网出口，避免云主机IP直接暴露在公网上。

方案架构

该解决方案部署架构如下图所示：

图 1-1 方案架构



该解决方案会部署如下资源：

- 创建两个子网Subnet，用于部署不同业务。
- 创建四台弹性云服务器ECS，并绑定安全组，用于主动访问公网资源。

- 创建安全组，通过配置安全组规则，为弹性云服务器提供安全防护。
- 创建两个弹性公网IP，用于提供访问公网的能力。
- 创建一个公网NAT网关，并配置SNAT规则，构建VPC中ECS的公网出口。

方案优势

- 高安全性

  SNAT有安全防护规则，只支持VPC内的ECS实例主动访问公网进行通信，而外部无法主动访问VPC的ECS实例，

- 灵活易用

  支持跨子网部署和跨可用区域部署。公网NAT网关的规格、弹性公网IP，均可以随时调整。配置简单，快速发放，即开即用，运行稳定可靠。

- 低成本

  用户无需为云主机访问Internet购买多余的弹性公网IP和带宽资源，多个云主机共享使用弹性公网IP，有效降低成本。

约束与限制

- 部署该解决方案之前，您需注册华为云账户，完成实名认证，且账号不能处于欠费或冻结状态。如果计费模式选择“包年包月”，请确保账户余额充足以便一键部署资源的时候可以自动支付；或者在一键部署的过程进入费用中心，找到“待支付订单”并手动完成支付。请根据**2 资源和成本规划**中预估价格。
- 确保租户配额充足，在“资源 > 我的配额”中查看配额是否充足，如配额不够，请提前工单申请增加配额。
- 该解决方案部署完成后，需用户登录华为云**弹性云服务器控制台**进行密码重置，请参考**弹性云服务器密码重置指南**。

2 资源和成本规划

该解决方案主要部署如下资源，不同产品的花费仅供参考，实际以收费账单为准，具体请参考华为云**官网价格**：

表 2-1 资源和成本规划(包年包月)

华为云服务	配置示例	每月预估花费
虚拟私有云 VPC	• 区域：华北-北京四 • 计费模式：免费创建 • 购买量：1	0
弹性云服务器 ECS	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：X86计算 | 通用计算型 | s6.small.1 | 1vCPUs | 1 GiB • 镜像：CentOS 8.2 64bit • 系统盘：通用性SSD | 40GB • 购买量：4	60.2 * 4 = 240.80元
弹性公网IP EIP	• 区域：华北-北京四 • 计费模式：包年包月 • 线路：动态BGP • 计费方式：按带宽计费 • 带宽大小：5Mbit/s • 购买时长：1个月 • 购买量：2	115.00 * 2 = 230元
公网NAT网关	• 区域：华北-北京四 • 规格：小型 • 购买时长：1个月 • 购买量：1	306元

合计	776.8元

表 2-2 资源和成本规划(按需计费)

华为云服务	配置示例	每月预估花费
虚拟私有云 VPC	• 区域：华北-北京四 • 计费模式：免费创建 • 购买量：1	0
弹性云服务器 ECS	• 按需计费：0.11元/小时 • 区域：华北-北京四 • 计费模式：包年包月 • 规格：X86计算 | 通用计算型 | s6.small.1 | 1vCPUs | 1 GiB • 镜像：CentOS 8.2 64bit • 系统盘：通用性SSD | 40GB • 购买量：4	0.11 * 24 * 30 * 4 = 316.8元
弹性公网IP EIP	• 按需计费：0.34元/5M/小时 • 区域：华北-北京四 • 计费模式：按带宽计费 • 线路：动态BGP • 公网带宽：按带宽计费 • 购买时长：1个月 • 购买量：1	0.34 * 24 * 30 * 2= 489.60元
公网NAT网关	• 按需计费：12元/天 • 区域：华北-北京四 • 规格：小型 • 购买时长：1个月 • 购买量：1	12*30=360元
合计		1166.4元

3 实施步骤

3.1 准备工作

创建 rf_amdin_trust 委托

步骤1 进入华为云官网，打开**控制台管理**界面，鼠标移动至个人账号处，打开“统一身份认证”菜单。

图 3-1 控制台管理界面

图 3-2 统一身份认证菜单

步骤2 进入“委托”菜单，搜索“rf_admin_trust”委托。

图 3-3 委托列表

- 如果委托存在，则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托

步骤3 单击步骤2界面中的“创建委托”按钮，在委托名称中输入“rf_admin_trust”，选择“普通账号”，委托的账号，输入“op_svc_IAC”，单击“下一步”。

图 3-4 创建委托

步骤4 在搜索框中输入”Tenant Administrator”权限，并勾选搜索结果。

图 3-5 选择策略

步骤5 选择“所有资源”，并单击下一步完成配置。

图 3-6 设置授权范围

步骤6 “委托”列表中出现“rf_admin_trust”委托则创建成功。

图 3-7 委托列表

----结束

3.2 快速部署

本章节主要帮助用户快速部署该解决方案。

表 3-1 参数填写说明

参数名称	类型	是否必填	参数解释	默认值
vpc_name	string	必填	虚拟私有云名称，该模板新建VPC，不允许重名。取值范围：1-56个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）	SNAT_base_public_network_connection_demo
secgroup_name	string	必填	安全组名称，该模板新建安全组，安全组规则请参考安全组规则修改（可选）进行配置。取值范围：1-62个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）	SNAT_base_public_network_connection_demo
ecs_name	string	必填	弹性云服务器名称，不允许重名。取值范围：1-53个字符组成，包括字母、数字、下划线(_)、连字符 (-) 和句点 (.)	SNAT_base_public_network_connection_demo
ecs_flavor	string	必填	弹性云服务器规格，规格请参考官网**弹性云服务器规格清单**。	s6.small.1 (s6|1vCPUs|1Gib)
ecs_password	string	必填	弹性云服务器初始密码，创建完成后，请参考重置ECS实例密码登录ECS控制台修改密码。取值范围：长度为8-26位，密码至少必须包含大写字母、小写字母、数字和特殊字符（!@$%^-_=+[{}]:,./?）中的三种，密码不能包含用户名或用户名的逆序。管理员账户为root	空
charging_mode	string	必填	计费模式，默认自动扣费，取值为prePaid（包年包月）或postPaid（按需计费），默认postPaid。	postPaid

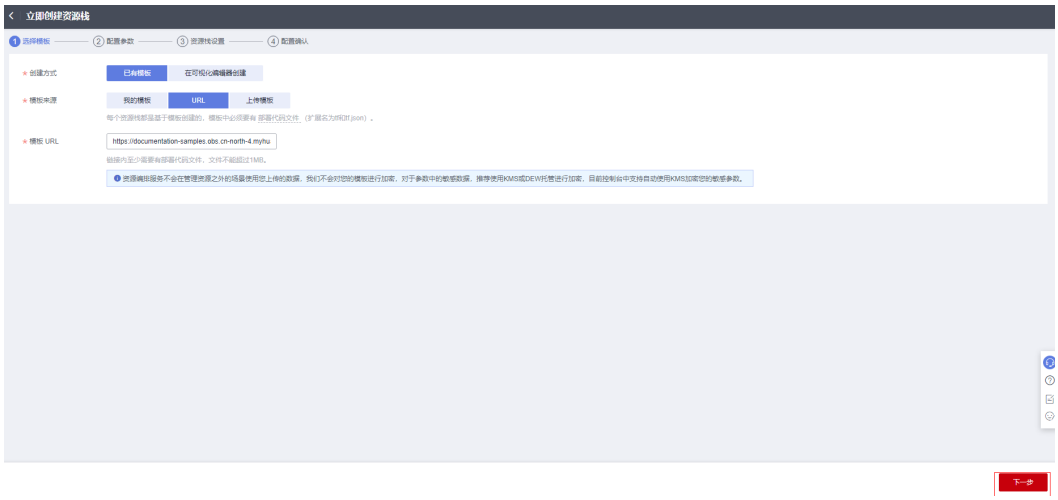
参数名称	类型	是否必填	参数解释	默认值
charging_unit	string	必填	有效值为“year”或“month”。当charging_mode（计费模式）为prePaid时，此选项为必填项。	month
charging_period	number	必填	包年包月时长，当charging_unit取值为“year”，取值范围为1～3；当charging_unit取值为“month”,取值范围为1～9。当charging_mode（计费模式）为prePaid时，此选项为必填项。	1
eip_size	number	必填	弹性公网IP带宽大小，该模板采用按带宽计费。取值范围为1-2000Mbit/s。	5

步骤1 登录**华为云解决方案实践**，选择“基于SNAT公网访问解决方案”，跳转至该解决方案一键部署界面。

图 3-8 解决方案实施库

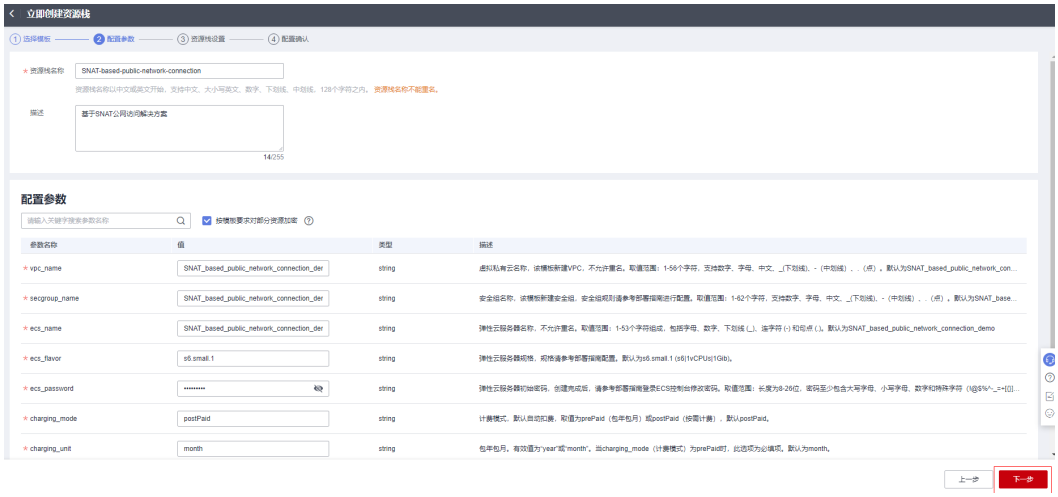
步骤2 在选择模板界面中，单击“下一步”。

图 3-9 选择模板



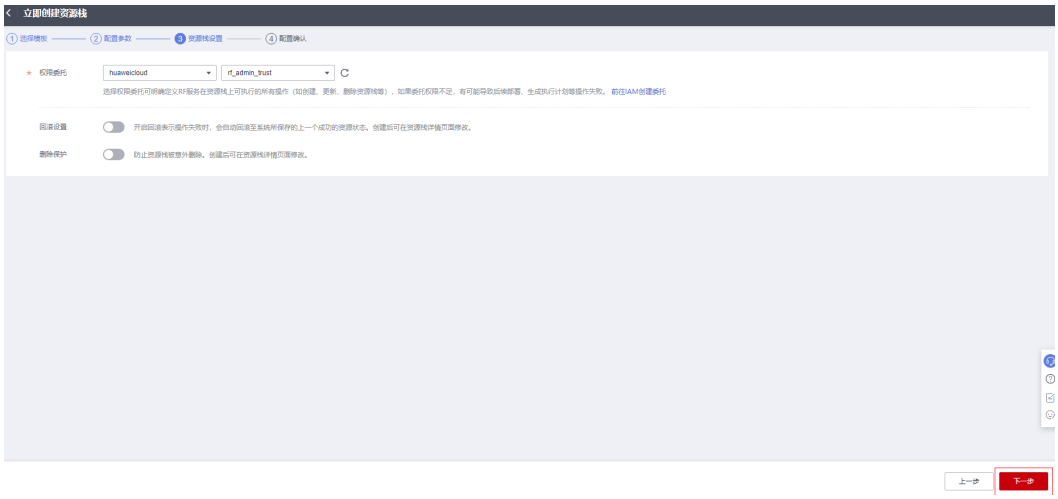
步骤3 在配置参数界面中，自定义填写堆栈名称，参考**表 参数填写说明**完成自定义参数填写，单击“下一步”。

图 3-10 配置参数



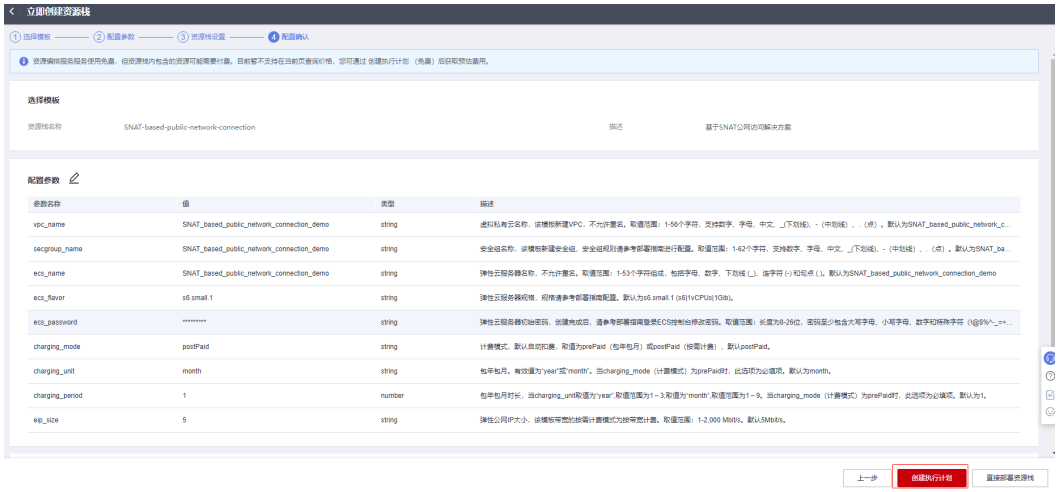
步骤4 在资源栈设置页面中，权限委托选择“rf_admin_trust”,单击“下一步”。

图 3-11 资源栈设置



步骤5 在配置确认页面中，单击“创建执行计划”。

图 3-12 配置确认



步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-13 创建执行计划

步骤7 等待执行计划状态为“创建成功，待部署”后，单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-14 执行计划创建成功

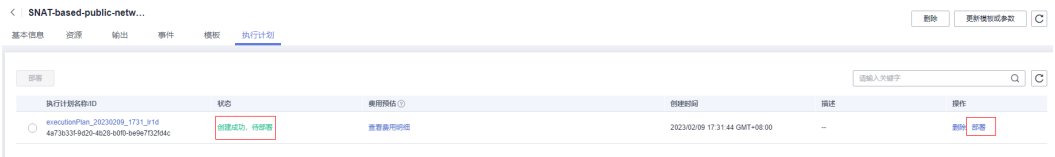


图 3-15 执行计划确认

步骤8 （可选）如果计费模式选择“包年包月”，在余额不充足的情况下（所需总费用请参考2-表 资源和成本规划（包年包月））请及时登录费用中心，手动完成待支付订单的费用支付。

步骤9 等待解决方案自动部署。部署成功后，单击“事件”，回显结果如下:

图 3-16 资源创建成功

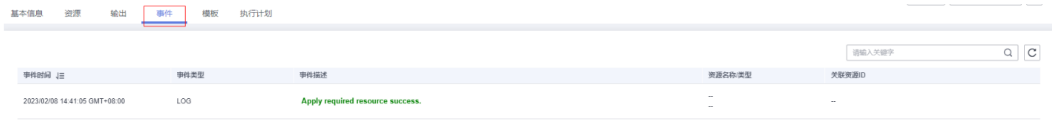
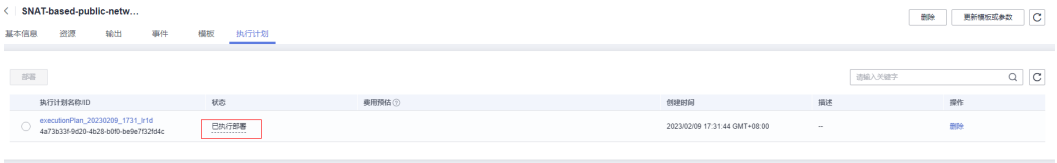


图 3-17 执行完成



----结束

3.3 开始使用

安全组规则修改（可选）

安全组实际是网络流量访问策略，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器、云数据库等实例提供安全保护。

如果您的实例关联的安全组策略无法满足使用需求，比如需要添加、修改、删除某个TCP端口，请参考以下内容进行修改。

- 添加安全组规则：根据业务使用需求需要开放某个TCP端口，请参考**添加安全组规则**添加入方向规则，打开指定的TCP端口。
- 修改安全组规则：安全组规则设置不当会造成严重的安全隐患。您可以参考**修改安全组规则**，来修改安全组中不合理的规则，保证云服务器等实例的网络安全。
- 删除安全组规则：当安全组规则入方向、出方向源地址/目的地址有变化时，或者不需要开放某个端口时，您可以参考**删除安全组规则**进行安全组规则删除。

重置 ECS 实例密码

步骤1 登录华为云控制台，通过“服务列表 > 弹性云服务器ECS”，进入到**ECS控制台**

图 3-18 华为云控制台

步骤2 重置密码。选择对应的弹性云服务器ECS实例，通过“更多 > 重置密码”来进行操作。

图 3-19 重置密码

详细请参考**弹性云服务器密码重置指南**。

----结束

查看部署资源并测试网络连接

步骤1 登录**华为云控制台**，添加以“北京四”为例。

图 3-20 华为云控制台

步骤2 在虚拟私有云VPC控制台，可查看该方案一键生成的VPC和对应的子网/路由表/弹性服务器ECS。

图 3-21 虚拟私有云 VPC 控制台

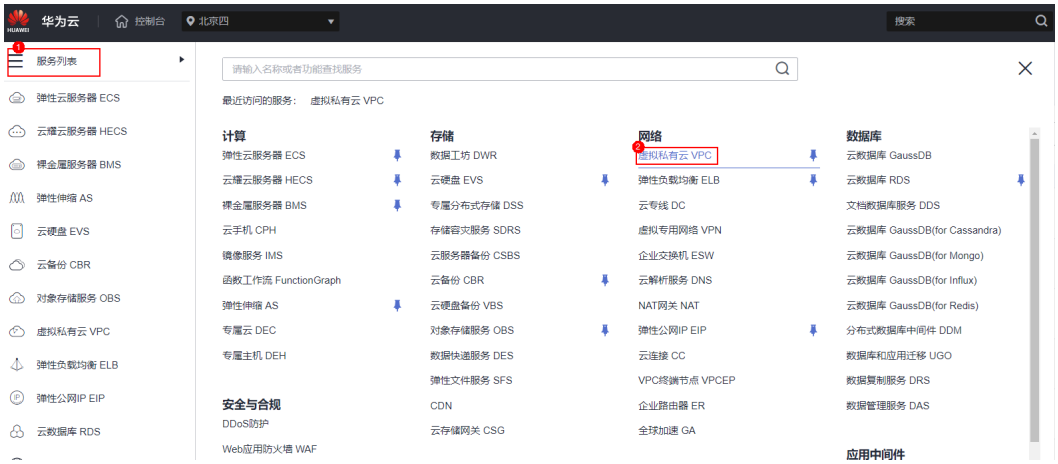
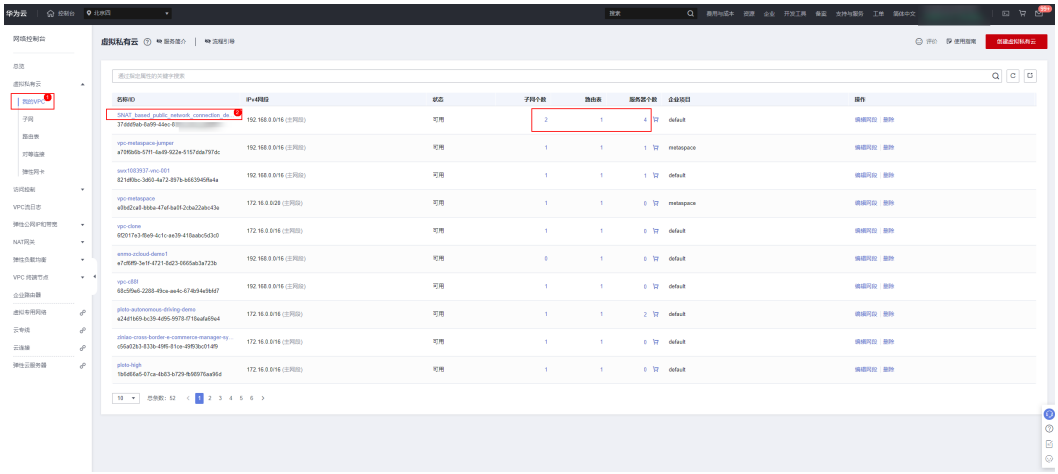


图 3-22 VPC 实例

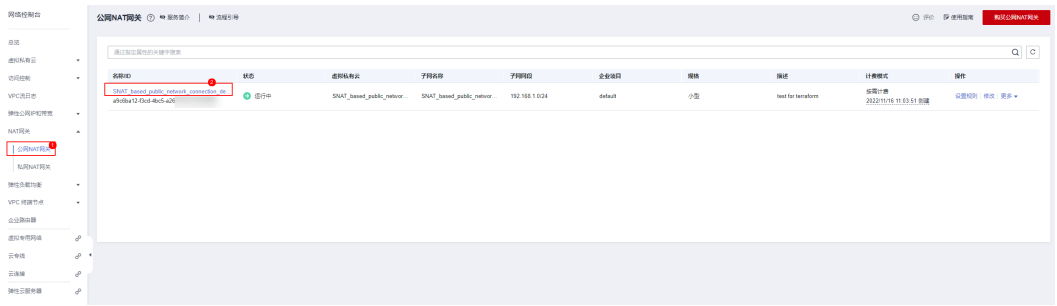


步骤3 在弹性公网IP控制台，可查看该方案一键部署生成的弹性公网IP实例。

图 3-23 弹性公网 IP 实例

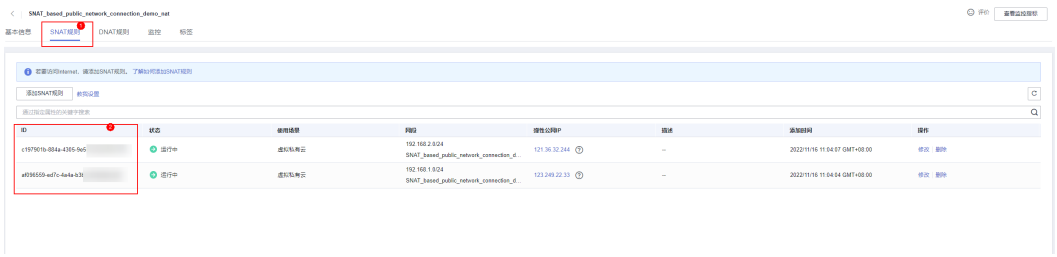
步骤4 在NAT网关控制台，可查看该方案一键部署生成的公网NAT网关实例。

图 3-24 公网 NAT 网关实例



步骤5 单击公网NAT网关实例，单击SNAT规则，查看一键部署生成的SNAT规则已成功添加。

图 3-25 NAT 网关的 SNAT 规则



步骤6 验证未绑定EIP的服务器是否可以通过NAT网关访问公网。

图 3-26 远程登录不同子网中的 ECS 实例（这里以 SNAT_based_public_network_connection_0001 和 SNAT_based_public_network_connection_0011 为例）

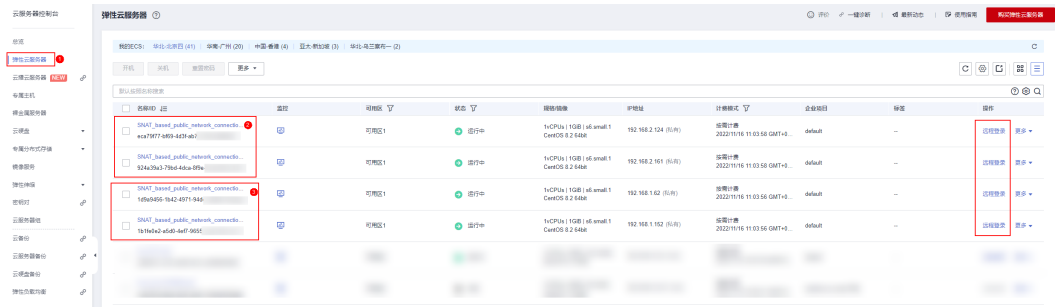


图 3-27 SNAT_based_public_network_connection_0001 测试与公网流量互通

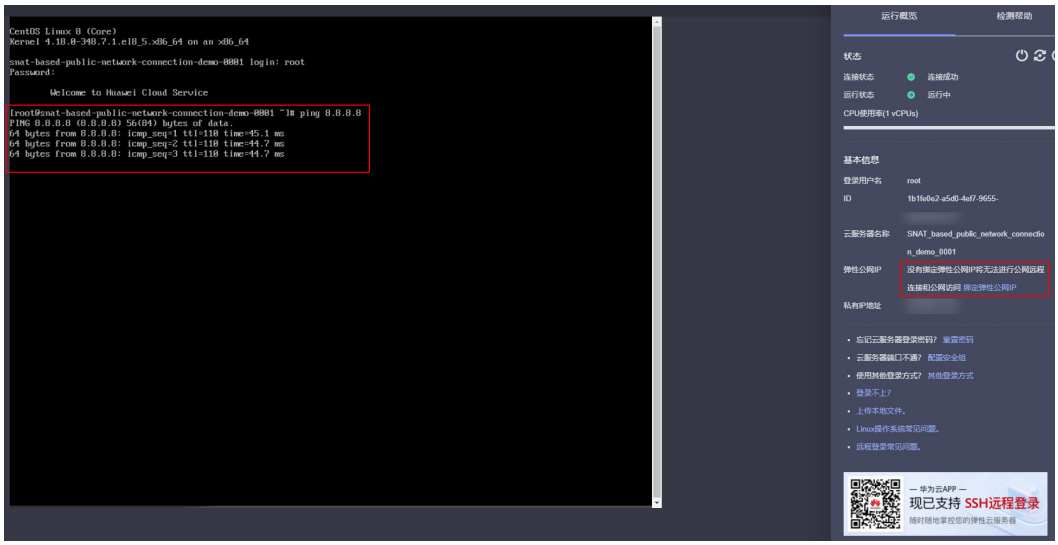
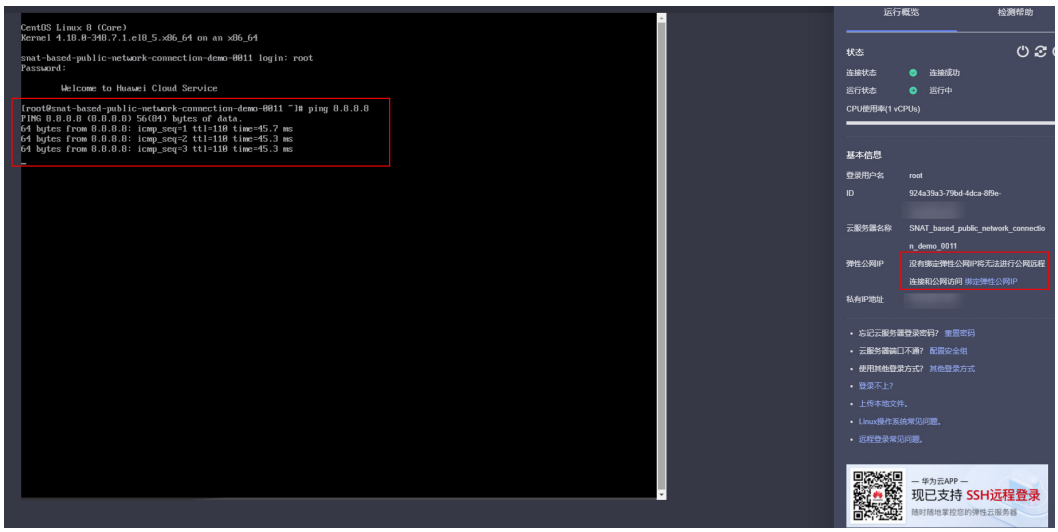


图 3-28 SNAT_based_public_network_connection_0011 测试与公网流量互通



----结束

3.4 快速卸载

步骤1 一键卸载

登录**资源编排服务RFS**，进入“资源栈”，选择**3.1快速部署步骤3**中创建的资源栈名称，单击“删除”，在弹出的“删除资源栈”确认框中输入Delete，单击“确定”即可卸载解决方案。

图 3-29 一键卸载

----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 虚拟私有云 VPC：是用户在华为云上申请的隔离的、私密的虚拟网络环境。用户可以基于VPC构建独立的云上网络空间，配合**弹性公网IP**、**云连接**、**云专线**等服务实现与Internet、云内私网、跨云私网互通，帮您打造可靠、稳定、高效的专属云上网络。
- 弹性云服务器 ECS：是一种云上可随时自助获取、可弹性伸缩的计算服务，可帮助您打造安全、可靠、灵活、高效的应用环境。
- 弹性公网IP：提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- 公网NAT网关：支持将私网IP转换为公网IP，转换后，云上资源即可安全地访问公网或对外提供服务，并且保护私有网络信息不直接对公网暴露。

5 修订记录

发布日期	修订记录
2022-10-30	第一次正式发布。
2023-02-28	修订实施步骤。