解决方案实践

# 基于 VPCEP 实现跨 VPC 连接 ELB

| | |
|---|---|
| 文档版本 | 1.0.3 |
| 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

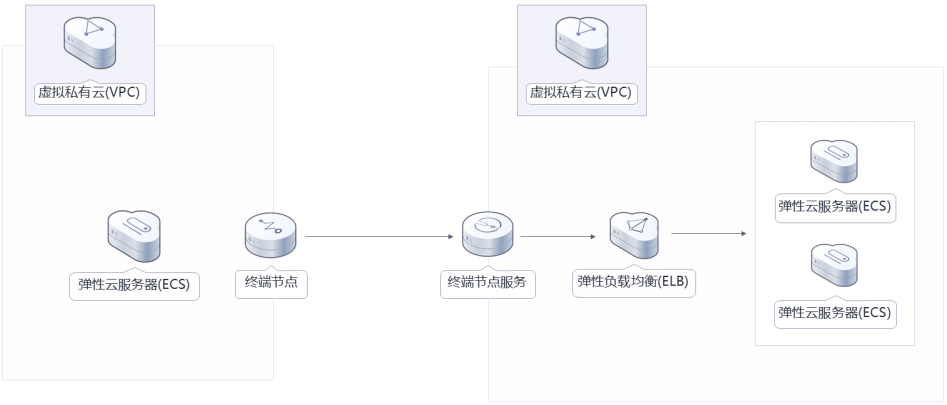
## 应用场景

该解决方案基于终端节点和终端节点服务，帮助用户快速实现同一区域不经过公网跨VPC的ELB后端服务访问。

## 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：

- 创建弹性云服务器 ECS，用于访问和提供业务服务。
- 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。
- 创建一个终端节点 VPCEP，用于私密连接终端节点服务。

- 创建一个终端节点服务，用于将云服务或用户私有服务配置为VPC终端节点支持的服务，可以被终端节点连接和访问。
- 创建弹性负载均衡 ELB，为终端节点服务提供业务保障。

## 方案优势

- 高安全性

  用户能够通过终端节点私密地连接到终端节点服务，避免泄漏服务端相关信息所带来不可知的风险。

- 灵活易用

  无需弹性公网IP，直连内网，使用更加灵活。连接负载均衡，确保业务高可用。

- 性能强劲

  每个网关节点可提供百万级对话，满足多种应用场景需求。

## 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**。
- 一个终端节点仅支持连接一个终端节点服务，一个终端节点服务仅支持对应一个后端资源实例。

# 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<br>• 计费模式：免费创建<br>• 购买量：2 | 0 |
| 弹性云服务器 ECS | • 区域：华北-北京四<br>• 计费模式：包年包月<br>• 规格：X86计算 \| 通用计算型 \| s6.small.1 \| 1vCPUs \| 1 GiB<br>• 镜像：CentOS 8.2 64bit<br>• 系统盘：通用性SSD \| 40GB<br>• 购买量：3 | 60.2 * 3 = 180.60元 |
| 弹性负载均衡 EIB | 共享型负载均衡(性能保障模式)<br>• 按需计费：0.32元/小时<br>• 区域：华北-北京四<br>• 计费模式：按需计费<br>• 购买量：1 | 0.32 * 24 * 30 = 230.4元 |
| 终端节点 VPCEP | • 区域：华北-北京四<br>• 服务类别：基础版<br>• 购买时长：1个月<br>• 购买量：1 | 0.1*24*30 = 72元 |
| 合计 | | 483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<br>• 计费模式：免费创建<br>• 购买量：2 | 0 |
| 弹性云服务器 ECS | • 按需计费：0.11元/小时<br>• 区域：华北-北京四<br>• 计费模式：包年包月<br>• 规格：X86计算 \| 通用计算型 \| s6.small.1 \| 1vCPUs \| 1 GiB<br>• 镜像：CentOS 8.2 64bit<br>• 系统盘：通用性SSD \| 40GB<br>• 购买量：3 | 0.11 * 24 * 30 * 3 = 237.6元 |
| 弹性负载均衡 EIB | 共享型负载均衡(性能保障模式)<br>• 按需计费：0.32元/小时<br>• 区域：华北-北京四<br>• 计费模式：按需计费<br>• 购买量：1 | 0.32 * 24 * 30 = 230.4元 |
| 终端节点 VPCEP | • 区域：华北-北京四<br>• 服务类别：基础版<br>• 购买时长：1个月<br>• 购买量：1 | 0.1*24*30 = 72元 |
| 合计 | | 540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） | cross-vpc-based-on-vpcep-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） | cross-vpc-based-on-vpcep-demo |
| ecs_name | string | 必填 | 弹性云服务器名称，不允许重名。取值范围：1-59个字符组成，包括字母、数字、下划线(_)、连字符 (-) 和句点 (.) | cross-vpc-based-on-vpcep-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<br>(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 |

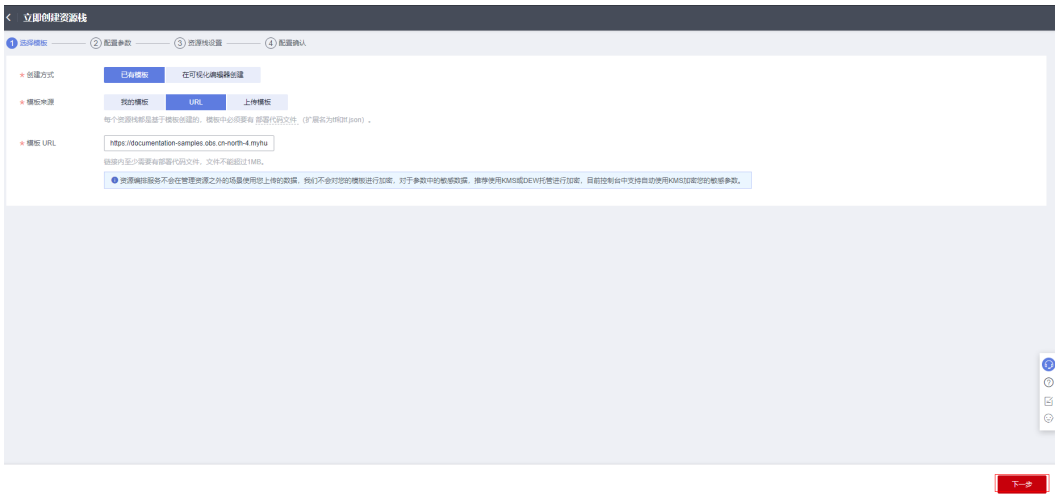
| 参数名称 | 类型 | 是否必填 | 参数解释 | 默认值 |
| --- | --- | --- | --- | --- |
| charging_unit | String | 必填 | 有效值为“year”或“month”。当charging_mode（计费模式）为prePaid时，此选项为必填项。 | month |
| charging_period | number | 必填 | 包年包月时长，当charging_unit取值为“year”，取值范围为1～3；当charging_unit取值为“month”,取值范围为1～9。当charging_mode（计费模式）为prePaid时，此选项为必填项。 | 1 |

**步骤1** 登录**华为云解决方案实践**，选择“基于VPCEP实现跨VPC连接ELB”，跳转至该解决方案一键部署界面。

**图 3-8** 解决方案实施库

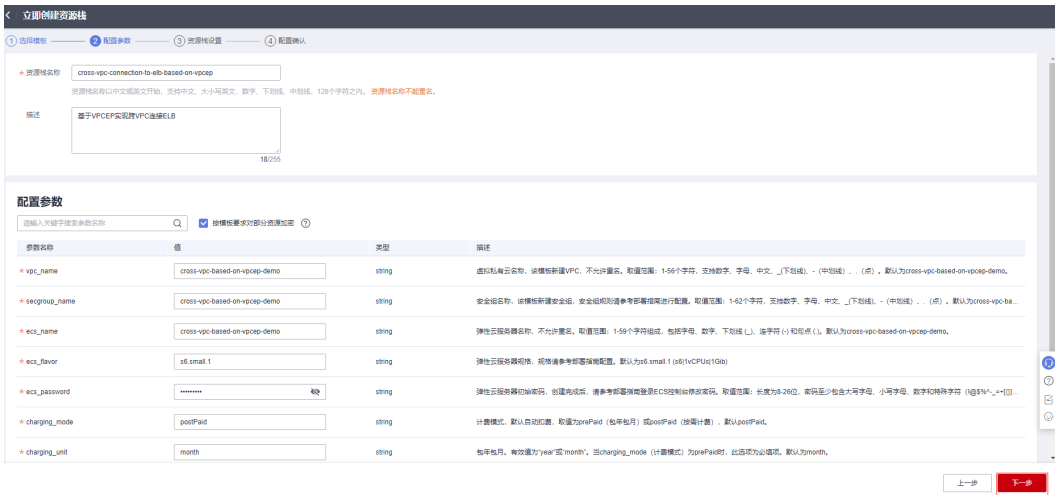

**步骤2** 在选择模板界面中，单击“下一步”。

**图 3-9** 选择模板



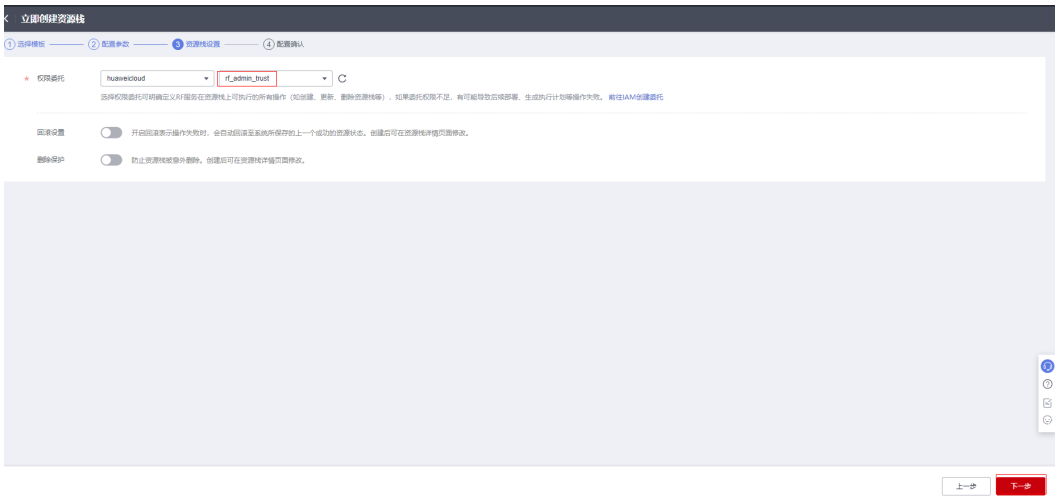

**步骤3** 在配置参数界面中，自定义填写堆栈名称，参考**表 参数填写说明**完成自定义参数填写，单击“下一步”。

**图 3-10** 配置参数



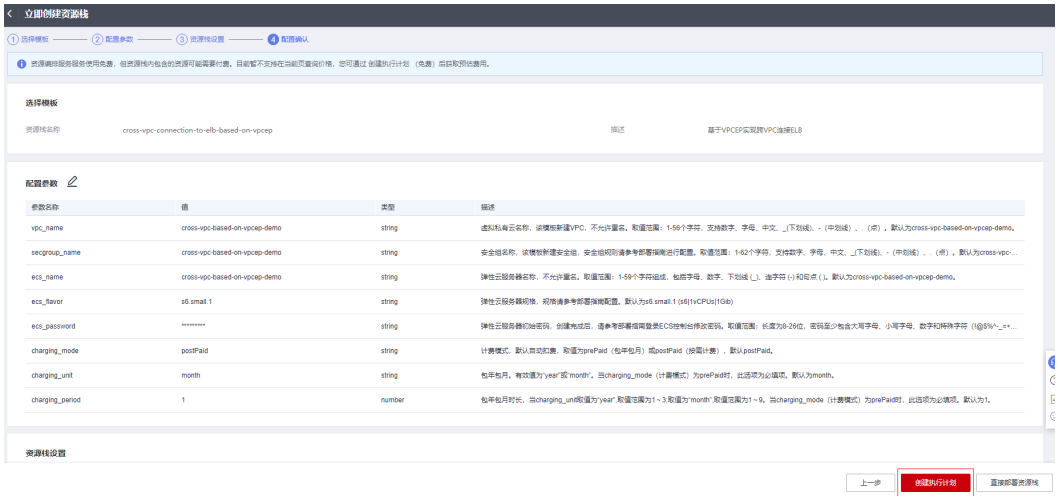

**步骤4** 在资源栈设置页面中，权限委托选择“rf_admin_trust”,单击“下一步”。

**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

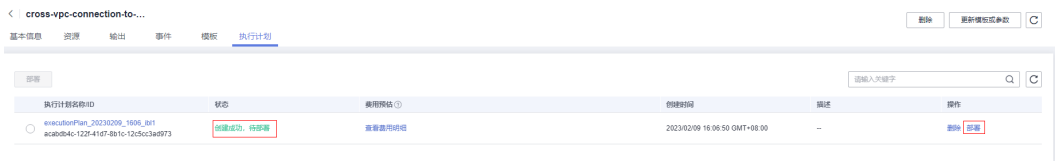


**图 3-15** 执行计划确认


**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

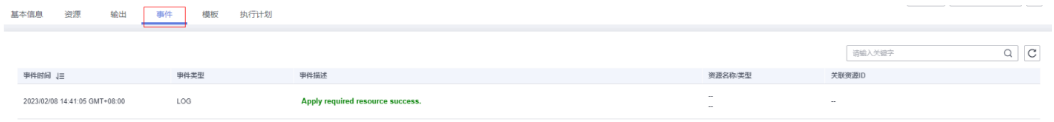
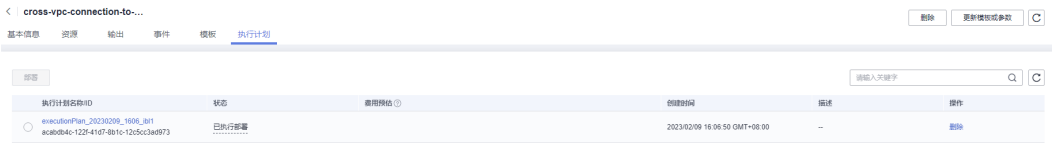



**图 3-17** 执行完成




**----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** 修改初始密码。打开**华为云服务器控制台**，勾选**3.1快速部署-步骤3**中创建的弹性云服务器，单击“关机”，关机成功后，单击“重置密码”，根据提示重置密码，单击“确定”后，开机即可正常使用。

**图 3-18** 重置密码


**----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**，区域选择“北京四”。

**图 3-19** 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 3-20** 虚拟私有云 VPC 控制台

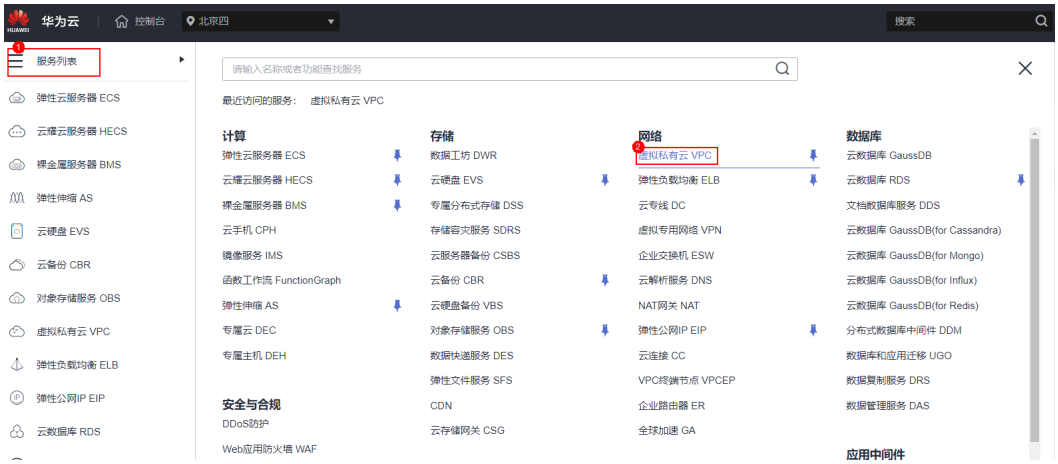
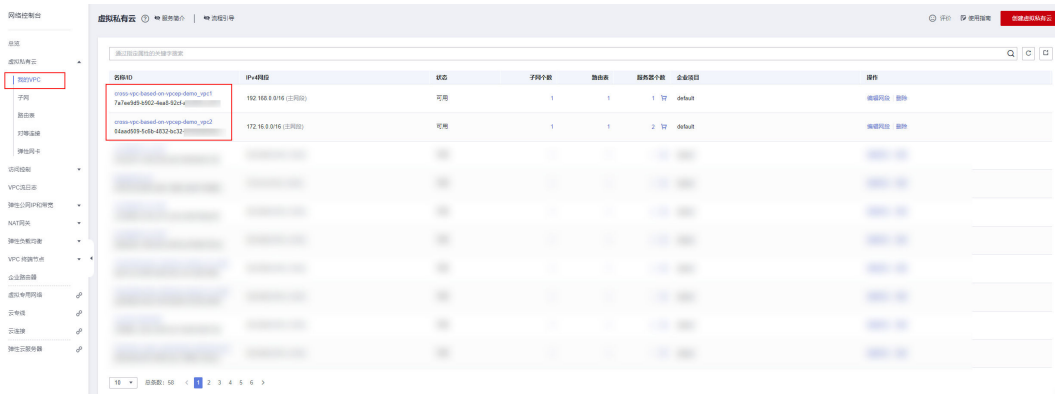
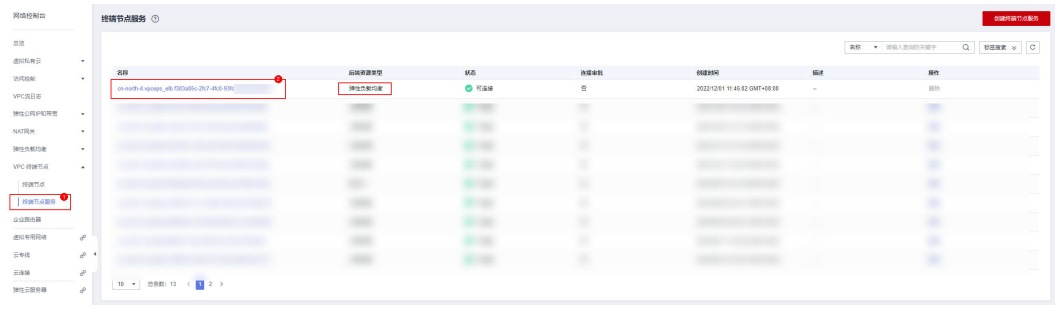



**图 3-21** VPC 实例



**步骤3** 在VPC终端节点服务中，可查看该方案一键部署生成的终端节点服务。

**图 3-22** 终端节点服务实例

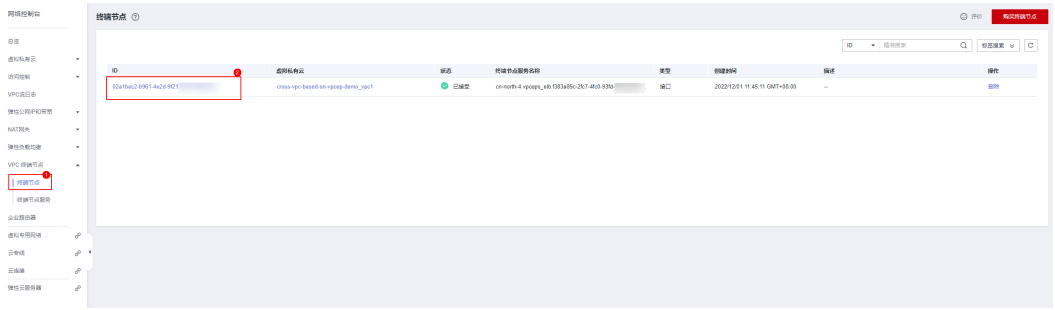


**步骤4** 单击对应的终端节点服务名称，可查看该服务关联的后端资源、连接管理等具体信息。

**图 3-23** 终端节点服务详情

**步骤5** 在VPC终端节点中，可查看该方案一键部署生成的终端节点 。

**图 3-24** 终端节点实例

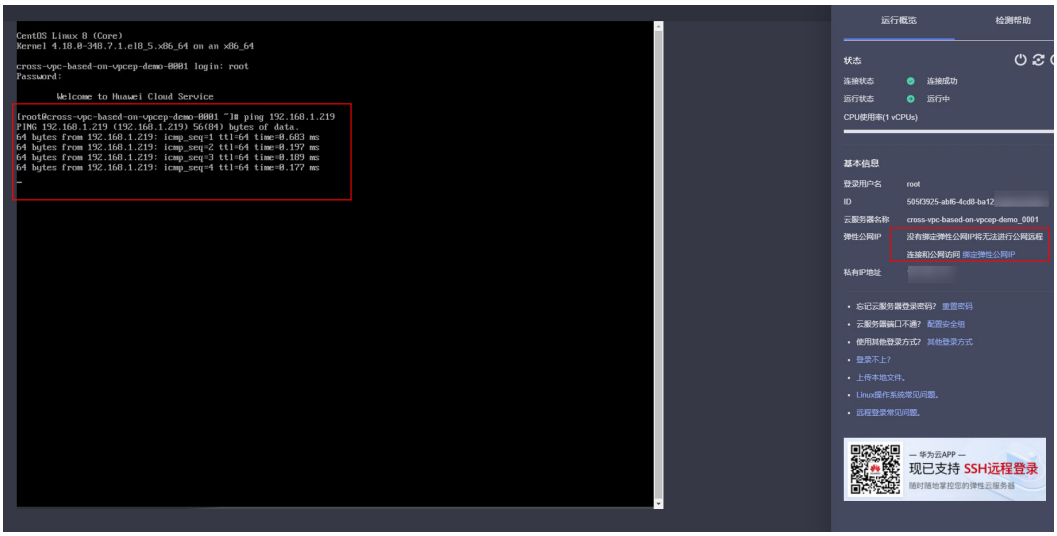


**步骤6** 单击对应的终端节点ID，可查看该节点IP、内网域名等具体信息。

**图 3-25** 终端节点详情

**步骤7** 远程登录VPC1中的弹性云服务器， 访问VPC终端节点的节点IP或内网域名。

**图 3-26** 登录云服务器访问 VPC 终端节点



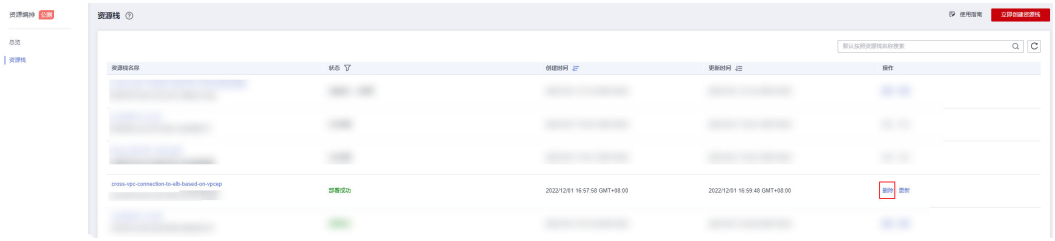

**----结束**

# 3.4 快速卸载

## 一键卸载

**步骤1** 解决方案部署成功后，单击该方案堆栈后的“删除”。

**图 3-27** 一键卸载



**步骤2** 在弹出的删除堆栈确认框中，输入Delete，单击“确定”，即可卸载解决方案。

**图 3-28** 删除堆栈确认


**----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。
- **VPC终端节点VPCEP**：能够将VPC私密地连接到终端节点服务（云服务、用户私有服务），使VPC中的云资源无需弹性公网IP就能够访问终端节点服务，提高了访问效率，为您提供更加灵活、安全的组网方式。
- **弹性负载均衡ELB**：是将访问流量根据分配策略分发到后端多台服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。

# 5 修订记录

| 发布日期 | 修订记录 |
| --- | --- |
| 2022-11-30 | 第一次正式发布。 |
| 2023-02-28 | 修订实施步骤。 |