解决方案实践

快速搭建 OpenVPN

文档版本	1.0
发布日期	2023-12-06

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OpenVPN,帮助企业之间或者个人与公司之间建立虚拟私人网络加密通道及数据安全传输隧道。有以下用途：

1，可与实现网通、电信机房快速、安全通信

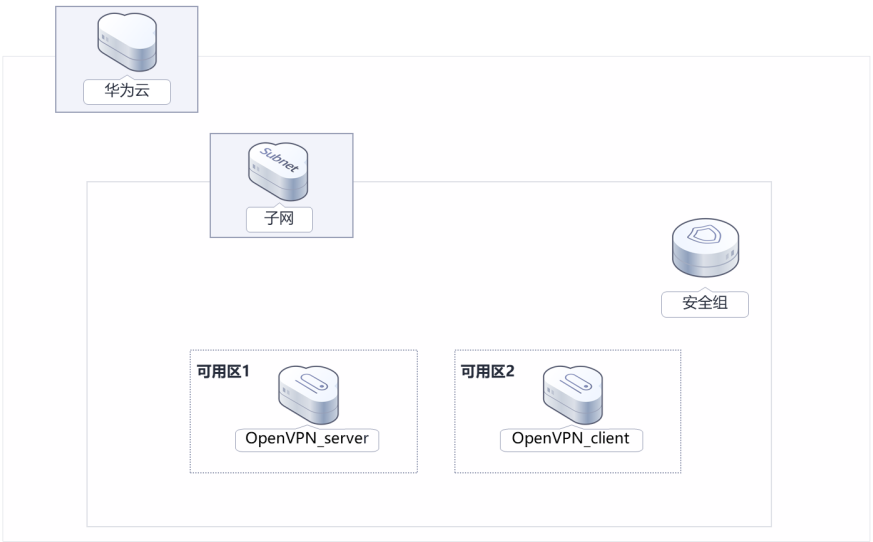
2，可以作为公司的远程办公环境，可与PPTPD服务器作为互备

3，可以穿透一些顽固型的防火墙，直接访问其后的局域网环境中的资源

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2台Linux弹性云服务器部署在不同的可用区，分别用于搭建OpenVPN的服务端和客户端。
- 创建2条弹性公网IP(EIP)，用于OpenVPN环境部署及提供访问公网和被公网访问能力。
- 创建安全组，可以保护弹性云服务器的网络安全，通过配置安全组规则，限定云服务器的访问端口。

方案优势

- 灵活自主

  提供极致性价比的云服务器，用户可以根据实际需求选择不同规格的弹性云服务器，灵活配置各类资源的大小，提升资源的利用率。
- 一键部署

  一键部署，即可完成云服务器创建和OpenVPN的安装和配置。
- 开源和定制化

  该解决方案是开源的，用户可以免费用于商业用途，并且还可以在源码基础上进行定制化开发。

约束与限制

- 部署该解决方案之前，需注册华为账号并开通华为云，完成实名认证，且账号不能处于欠费或冻结状态，请根据**表2-1**中预估价格，确保余额充足。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。
- 该解决方案部署成功后，搭建OpenVPN服务器大约用时20分钟，完成后方可参考**3.3 开始使用**进行验证。

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 资源和成本规格-弹性云服务器部署(包年包月)

华为云服务	配置示例	每月预估花费
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 | ECS | c6.large.2 | 2vCPUs | 4GiB • 镜像：Ubuntu 16.04 server 64bit • 系统盘：高IO | 100GB • 购买量：2	243.50*2=487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 • 公网带宽：按带宽计费 • 带宽大小：5Mbit/s • 购买时长：1个月 • 购买量：2	115 *2 = 230元
合计		**717元**

表 2-2 资源和成本规格-弹性云服务器部署(按需计费)

华为云服务	配置示例	每月预估花费
弹性云服务器 ECS	• 按需计费：0.51元/小时 • 区域：华北-北京四 • 计费模式：按需计费 • 规格：X86计算 | ECS | c6.large.2 | 2vCPUs | 4GiB • 镜像：Ubuntu 16.04 server 64bit • 系统盘：高IO | 100GB • 购买量：2	0.51* 24 * 30 *2=734.4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：按需计费 • 线路：动态BGP • 公网带宽：按带宽计费 • 购买量：2	0.34 * 24 * 30 *2= 489.6元
合计		**1224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界面中右上角的“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：1-54个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	openvpn-demo
secgroup_name	String	必填	安全组名称，该模板新建安全组。取值范围：1-64个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	openvpn-demo
ecs_name	String	必填	弹性云服务器名称，不允许重名。命名方式为：{ecs_name}-server（服务端），{ecs_name}-client（客户端）。取值范围：1-57个字符，支持字母、数字、中文、下划线（_）、中划线（-）、英文句号（.）。	openvpn-demo

参数名称	类型	是否必填	参数解释	默认值
ecs_flavor	String	必填	弹性云服务器规格名称，具体请参考官网**弹性云服务器规格清单**。（c6|2vCPUs|4GiB。）	c6.large.2
ecs_password	String	必填	云服务器密码，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，仅支持小写字母、数字、中划线（-）、英文句号（.）。如果修改密码，请参考**重置弹性云服务器密码**登录ECS控制台修改密码。	空
system_disk_size	String	必填	系统盘大小，以GB为单位，取值范围为40～1,024，不支持缩盘。	100
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
charging_unit	String	选填	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	选填	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，此选项为选填项。	1

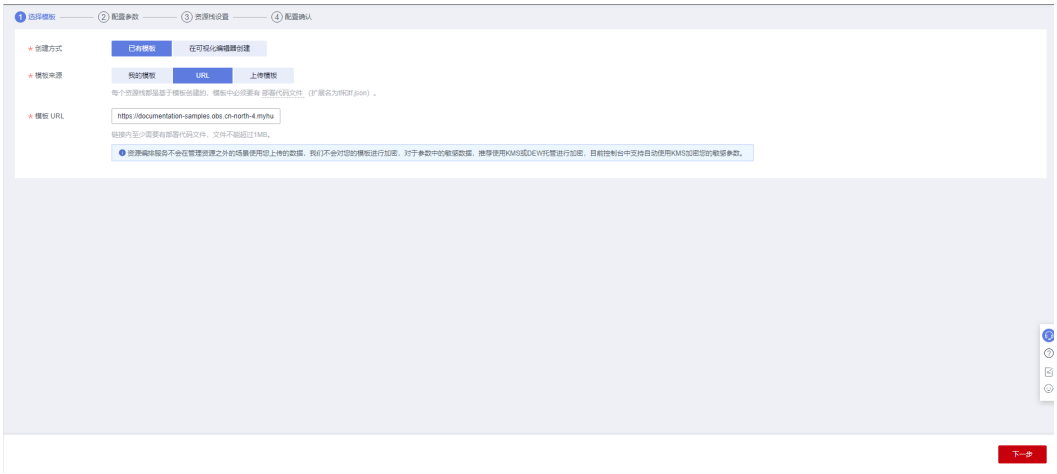
参数名称	类型	是否必填	参数解释	默认值
eip_bandwidth_size	number	必填	弹性公网IP带宽大小，该模板采用按带宽计费。取值范围为1-2,000Mbit/s。	5

步骤1 登录华为云解决方案实践，选择“**快速搭建OpenVPN**”解决方案，单击“一键部署”，跳转至解决方案创建资源栈界面。

图 3-8 解决方案实施库

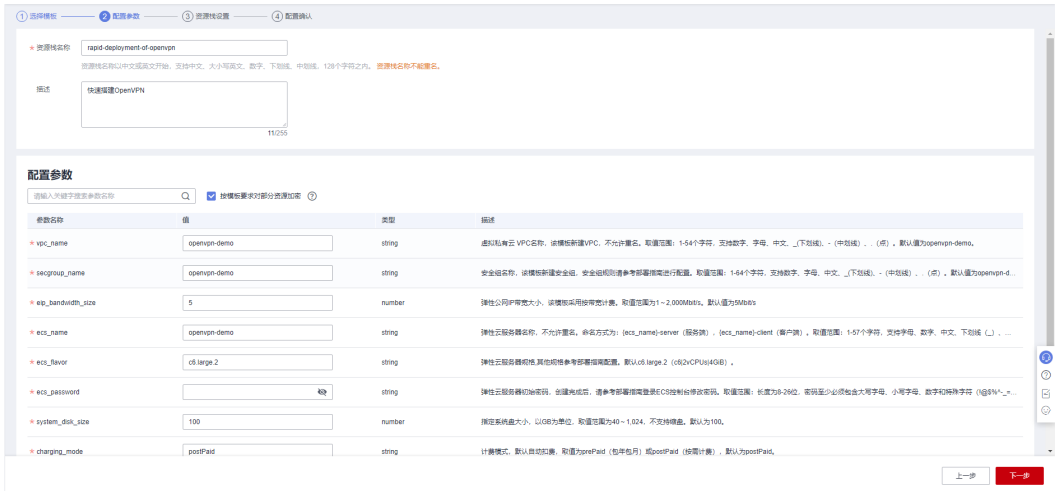
步骤2 在选择模板界面中，单击“下一步”。

图 3-9 选择模板



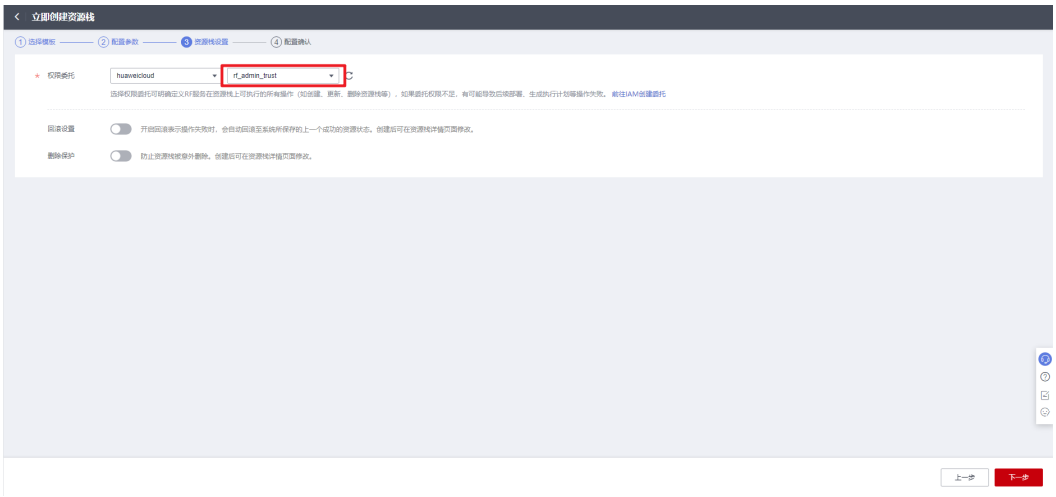
步骤3 在配置参数界面中，根据**表3-1**配置参数信息，单击“下一步”。

图 3-10 配置参数



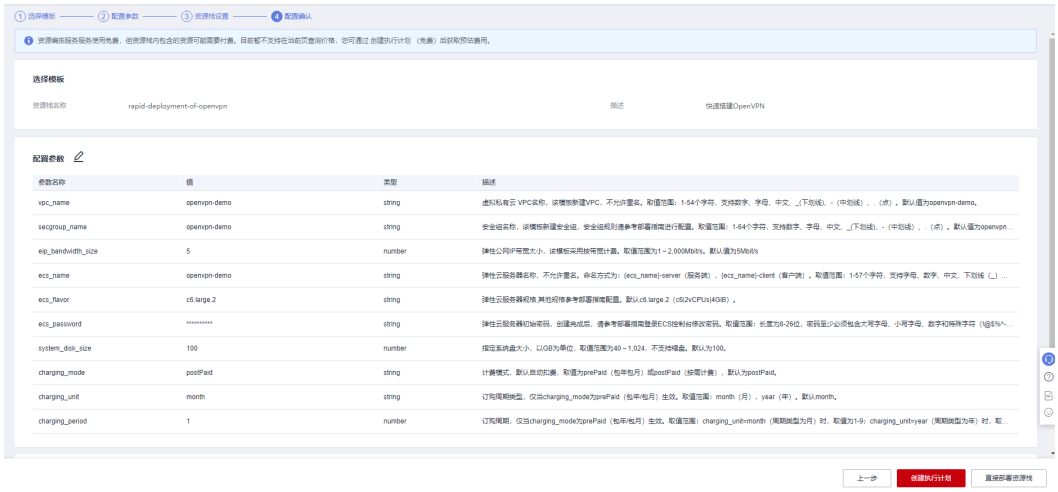
步骤4 在资源设置界面中，“权限委托”下拉框中选择“rf_admin_trust”委托，单击“下一步”。

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 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

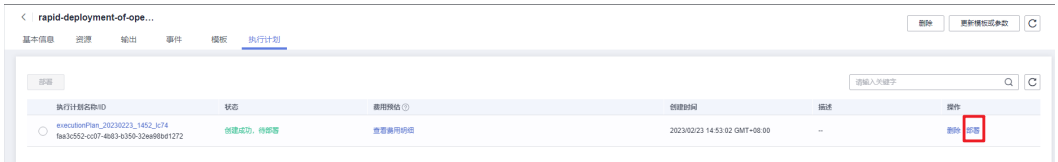


图 3-15 执行计划确认

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

----结束

3.3 开始使用

安全组规则修改（可选）

须知

- OpenVPN提供服务端口号为1194，入方向规则默认全放通，请参考修改安全组规则，配置IP地址白名单，以便能正常使用服务。
- 该解决方案使用22端口远程登录弹性云服务器ECS，默认对该方案创建的VPC子网网段放开，请参考**修改安全组规则**，配置IP地址白名单，以便能正常访问服务。

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。

登录 ECS

步骤1 登录**ECS弹性云服务器**控制平台，首先选择一台弹性云服务器，单击远程登录，或者使用其他的远程登录工具进入Linux弹性云服务器。

图 3-17 登录 ECS 云服务器控制平台

图 3-18 登录 Linux 弹性云服务器

步骤2 在Linux弹性云服务中输入账号和密码后回车进入服务器。

图 3-19 登录 Linux 弹性云服务器

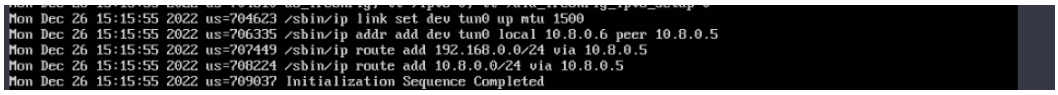
----结束

验证环境

步骤1 在客户端查看日志输入cat /var/log/openvpn.log

当返回如下信息，则表示已经成功连接VPN

图 3-20 返回信息



----结束

3.4 快速卸载

步骤1 解决方案部署成功后，进入**资源栈**，单击该方案资源栈后的“删除”。

图 3-21 一键卸载

步骤2 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 3-22 删除资源栈确认

----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 弹性云服务器ECS：是一种可随时自助获取、可弹性伸缩的云服务器，可帮助您打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。
- 弹性公网IP EIP：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。
- OpenVPN：是一种适用于建立虚拟私人网络加密通道的软件。

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2022-12-30	第一次正式发布。
2023-02-28	修订实施步骤。