

解决方案实践

快速部署高可用七层负载均衡

文档版本 1.0.1
发布日期 2023-02-28



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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	1
2 资源和成本规划	3
3 实施步骤	5
3.1 准备工作.....	5
3.2 快速部署.....	9
3.3 开始使用.....	15
3.4 快速卸载.....	18
4 附录	20
5 修订记录	21

1 方案概述

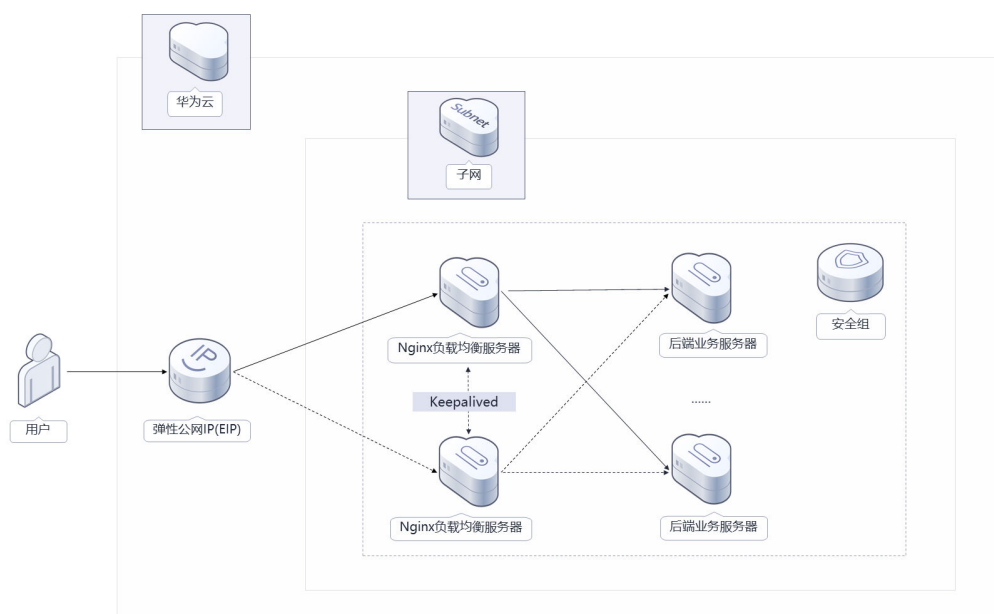
应用场景

该解决方案基于开源软件Nginx+Keepalived构建，快速帮助用户在华为云弹性云服务器上部署七层高可用负载均衡。Nginx节点主备部署，提供负载均衡能力，支持HTTP/HTTPS协议，并做一些分流策略，用户可以通过主机IP、域名等快速访问业务服务器。Keepalived提供健康检查和故障转移能力，提高系统的可用性。

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：

- 创建两台Linux弹性云服务器，用于部署负载均衡业务系统。
- 创建虚拟IP，并分别绑定到两台弹性云服务器上，用于Nginx节点主备切换。

- 创建弹性公网EIP，并绑定到虚拟IP上，用于提供对外访问服务。
- 在两台Linux弹性云服务器分别完成Nginx和Keepalive软件的自动安装，以及高可用负载均衡环境配置。

方案优势

- 高性能
Nginx工作在OSI的第七层，是一个具有高并发、高稳定、开源免费（弹性负载均衡器ELB成本最低为0.32元/小时/实例），省带宽的HTTP/HTTPS反向代理Web服务器。
- 高可靠
Nginx节点主备部署，支持请求重发。通过Keepalived自动检测健康状态，并进行故障转移，提高自建负载均衡系统的可用性。
- 一键部署
一键轻松部署，即可完成资源的快速发放以及高可用七层负载均衡环境的部署。

约束与限制

- 部署该解决方案之前，您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。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。
- 已有虚拟私有云VPC、子网、安全组以及业务虚拟机。
- 使用中国大陆节点服务器部署的Web网站，您需要注册域名，并在开通网站前按照工信部要求办理网站备案，以确保您的网站可以通过域名正常访问。华为云支持一站式完成域名注册、实名认证、网站备案和网站解析等操作，详细操作请参考[流程指引](#)。
- 该解决方案安装Nginx默认监听80和443端口，如未开通请参考[添加安全组规则](#)添加加入方向规则，打开指定的TCP端口。

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，具体请参考华为云[官网价格](#)，实际以收费账单为准：

表 2-1 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
弹性云服务器 ECS	<ul style="list-style-type: none">● 按需计费：0.41元/小时● 区域：华北-北京四● 计费模式：按需计费● 规格：X86计算 ECS s6.large.2 2vCPUs 4GiB● 镜像：CentOS 7.6 64bit● 系统盘：高IO 100GB● 购买量：2	$0.41 * 24 * 30 * 2 = 590.4$ 元
弹性公网IP EIP	<ul style="list-style-type: none">● 按需计费：0.34元/MBit/s/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● 带宽大小：5Mbit/s● 购买量：3(配置完成后可手动释放2个，将不再计费)	$0.34 * 24 * 30 * 3 = 734.4$ 元
合计	-	1324.8元

表 2-2 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
弹性云服务器 ECS	<ul style="list-style-type: none">● 区域：华北-北京四● 计费模式：包年包月● 规格：X86计算 ECS s6.large.2 2vCPUs 4GiB● 镜像：CentOS 7.6 64bit● 系统盘：高IO 100GB● 购买量：2	$187.2 * 2 = 374.4$ 元
弹性公网IP EIP	<ul style="list-style-type: none">● 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● 购买量：3(配置完成后可手动释放2个，将返还部分费用)	$115 * 3 = 345$ 元
合计	-	719.4元

3 实施步骤

- 3.1 准备工作
- 3.2 快速部署
- 3.3 开始使用
- 3.4 快速卸载

3.1 准备工作

本章节主要帮助用户在快速部署该解决方案之前，获取部分依赖的资源，以供一键部署时使用。

创建 rf_admin_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

获取资源 ID

步骤1 登录[华为云官网控制台](#)，单击[虚拟私有云VPC](#)，打开后端业务服务器所属VPC，单击该VPC下的[子网](#)，单击任一子网或后端业务服务器所属子网，获取网络ID。

图 3-8 VPC 下的子网



图 3-9 子网列表

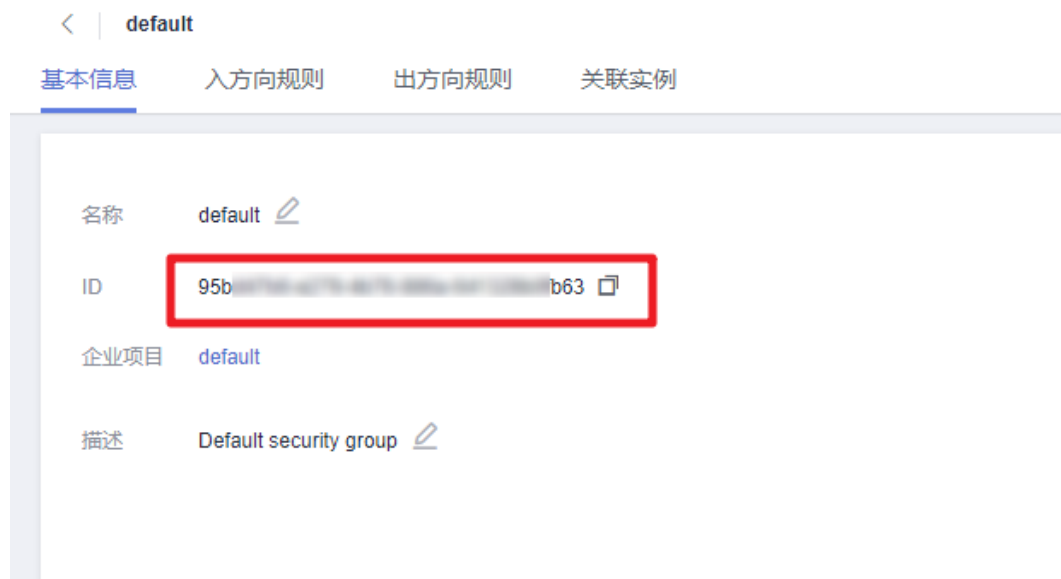


图 3-10 子网网络 ID



步骤2 在网络控制台查看[安全组](#)，打开业务虚拟机所配置的安全组，获取安全组ID。

图 3-11 安全组 ID



----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
subnet_id	String	必填	子网ID，该模板使用已有子网，请选择后端业务服务器所在虚拟私有云VPC内子网，查询并获取子网ID请参考 3.1准备工作步骤1 。	空
security_group_id	String	必填	安全组ID，该模板使用已有安全组，建议选择后端业务服务器相同安全组，查询并获取安全组ID请参考 3.1准备工作步骤2 。	空
ecs_name	String	必填	负载均衡主、备云服务器前缀，服务器命名方式为 {ecs_name}-master, {ecs_name}-backup，不支持重名。取值范围：1-54个字符组成，包括字母、数字、下划线（_）、连字符（-）和句点（.）。	highly-available-seven-layer-load-balancer-demo

参数名称	类型	是否必填	参数解释	默认值
ecs_flavor	String	必填	负载均衡主、备云服务器规格，具体请参考官网 弹性云服务器规格清单 。	s6.large.2 (s6 2vCPU 4GiB)
ecs_password	String	必填	负载均衡主、备云服务器初始化密码，创建完成后请参考 3.3 开始使用步骤1 重置密码。取值范围：长度为8-26位，密码至少包含大写字母、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
bandwidth_size	Number	必填	带宽大小，该模板计费方式为按带宽计费。取值范围：1-2,000Mbit/s。	5Mbit/s
ip_port_list	String	必填	用户后端业务服务器的私有IP地址及Web服务访问端口，格式为：IP1:端口1,IP2:端口2，所有符号均为英文半角符号。例如： 192.168.0.1:8080,192.168.0.2:8081,192.168.0.3:8083（在浏览器中访问该环境时，请选择后端端口对应的HTTP协议或者HTTPS协议访问）。	空
ssl_certificate	String	必填	用户已有SSL证书(公钥)文件名称，包含后缀名。该模板部署完成后，请使用远程连接工具登录两台负载均衡服务器，在指定目录下（/etc/nginx/ssl/）分别上传该证书文件，具体请参考 3.3开始使用步骤2 。	空
ssl_certificate_key	String	必填	用户已有SSL证书(私钥)文件名称，包含后缀名。该模板部署完成后，请使用远程连接工具登录两台负载均衡服务器，在指定目录下（/etc/nginx/ssl/）分别上传该证书文件，具体请参考 3.3开始使用步骤2 。	空
charge_mode	String	必填	计费模式，默认自动扣费，可选值为：prePaid（包年包月）或postPaid（按需计费）。	postPaid

参数名称	类型	是否必填	参数解释	默认值
charge_period_unit	String	必填	订购周期类型，仅当charge_mode为prePaid（包年/包月）生效。取值范围：month（月），year（年）。	month
charge_period	Number	必填	订购周期，仅当charge_mode为prePaid（包年/包月）生效。取值范围：charge_period_unit=month（周期类型为月）时，取值为1-9；charge_period_unit=year（周期类型为年）时，取值为1-3。	1

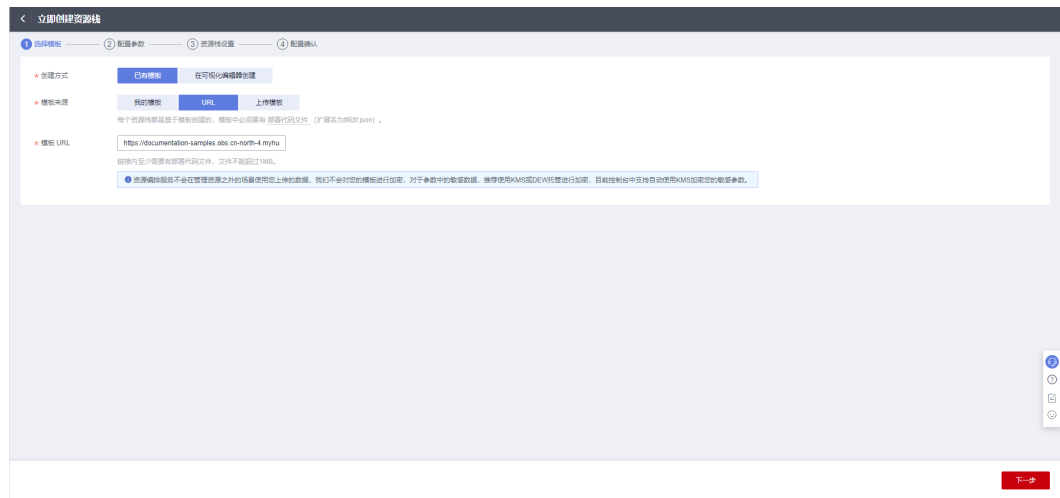
步骤1 登录华为云解决方案实践，选择“快速部署高可用七层负载均衡”并单击，跳转至该解决方案一键部署界面，数据中心下拉菜单可以选择需要部署的区域。

图 3-12 解决方案实施库



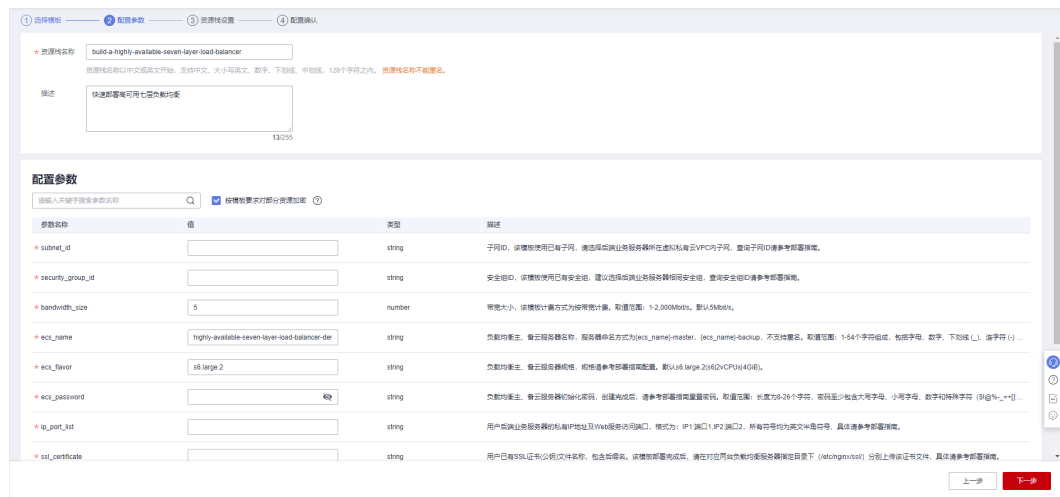
步骤2 单击“一键部署”，跳转至该解决方案创建资源栈部署界面。

图 3-13 创建资源栈



步骤3 单击“下一步”，参考表3-1完成自定义参数填写。

图 3-14 参数配置



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。

图 3-17 创建执行计划



步骤7 单击“部署”，在弹窗中再次单击“执行”确认执行。

图 3-18 执行计划确认

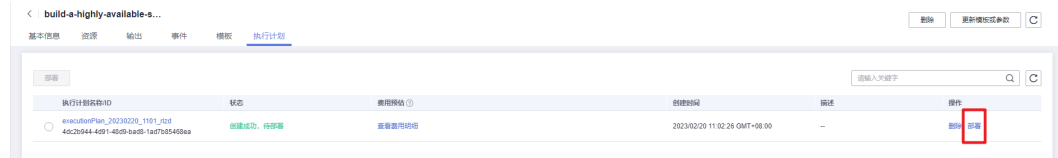


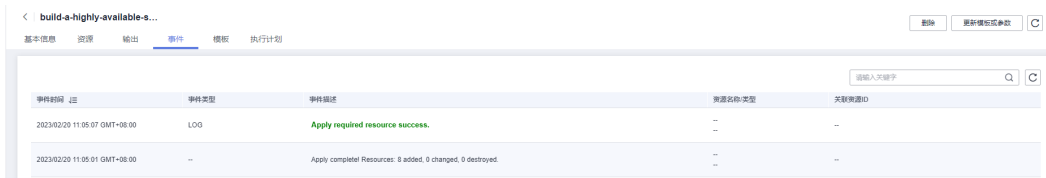
图 3-19 执行计划确认



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(所需总费用请参考表2-2)请及时登录[费用中心](#), 手动完成待支付订单的费用支付。

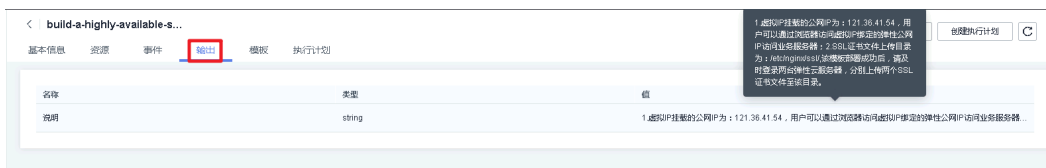
步骤9 待“事件”中出现“Apply required resource success”, 表示该解决方案已经部署完成。

图 3-20 资源创建成功



步骤10 单击“输出”, 查看虚拟IP挂载的弹性公网IP等信息。

图 3-21 VIP 挂载 EIP



----结束

3.3 开始使用

步骤1 修改初始密码。登录[华为云服务器控制台](#), 参考[在控制台重置弹性云服务器密码](#), 进行密码重置。

步骤2 使用远程连接工具, 登录两台负载均衡服务器, 上传已有SSL证书(公钥、私钥)文件至指定目录: /etc/nginx/ssl/, 上传请参考[上传文件到云服务器方式概览](#)。

图 3-22 SSL 证书

```
Welcome to Huawei Cloud Service
[root@nginx-keepalived-master ~]# ls /etc/nginx/ssl/
server.crt server.key
[root@nginx-keepalived-master ~]# _
```

步骤3 上传证书到指定路径后，需要用户重新启动Nginx服务，输入如下命令：
systemctl restart nginx

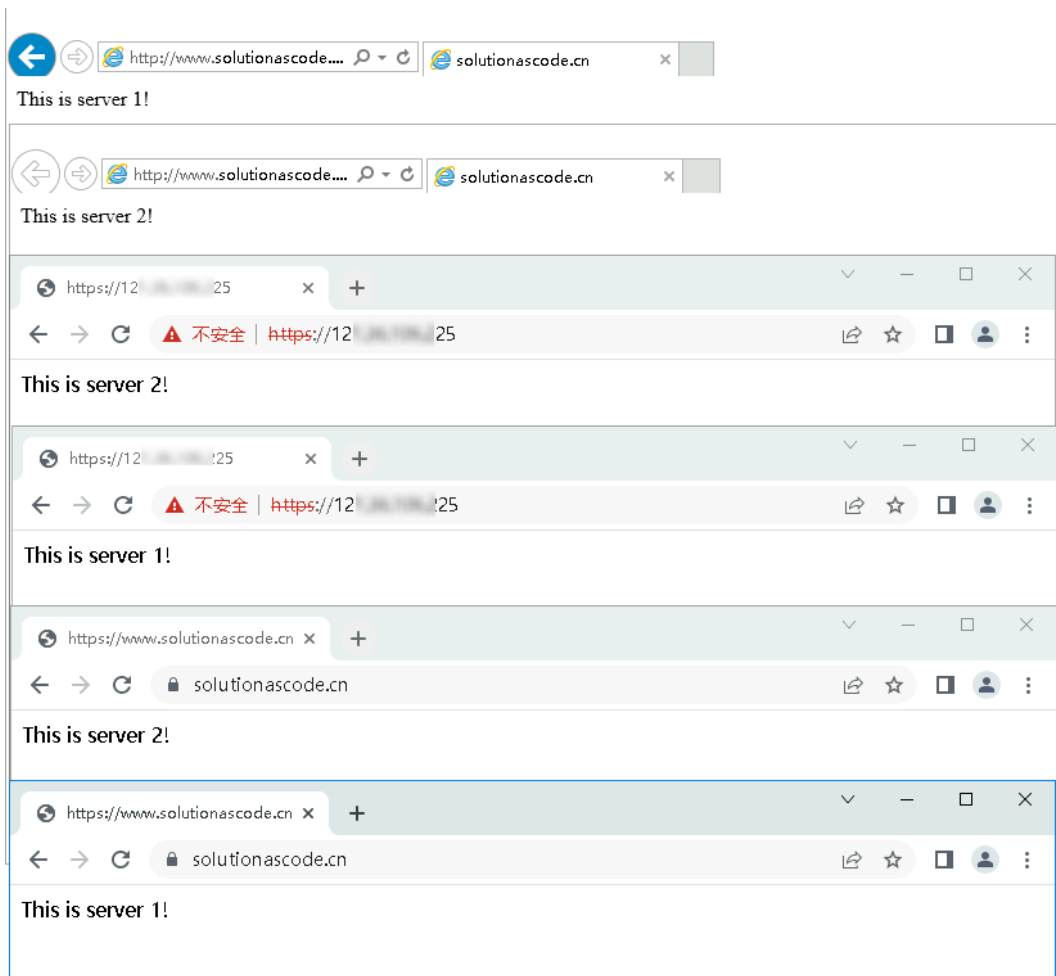
图 3-23 重启 Nginx 服务

```
[root@highly-available-seven-layer-load-balancer-demo-master ~]# systemctl restart nginx
[root@highly-available-seven-layer-load-balancer-demo-master ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-10-25 15:00:42 CST; 5s ago
     Process: 13116 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
    Process: 13111 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 13109 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
   Main PID: 13116 (nginx)
   CGroup: /system.slice/nginx.service
           └─13116 nginx: master process /usr/sbin/nginx
             └─13117 nginx: worker process
               └─13118 nginx: worker process
```

步骤4 配置域名解析。通过网站解析将SSL证书绑定的域名与3.2快速部署步骤9中虚拟IP绑定的公网IP关联，即可实现通过在浏览器中直接输入域名访问网站，具体解析流程参考[快速添加域名解析](#)。

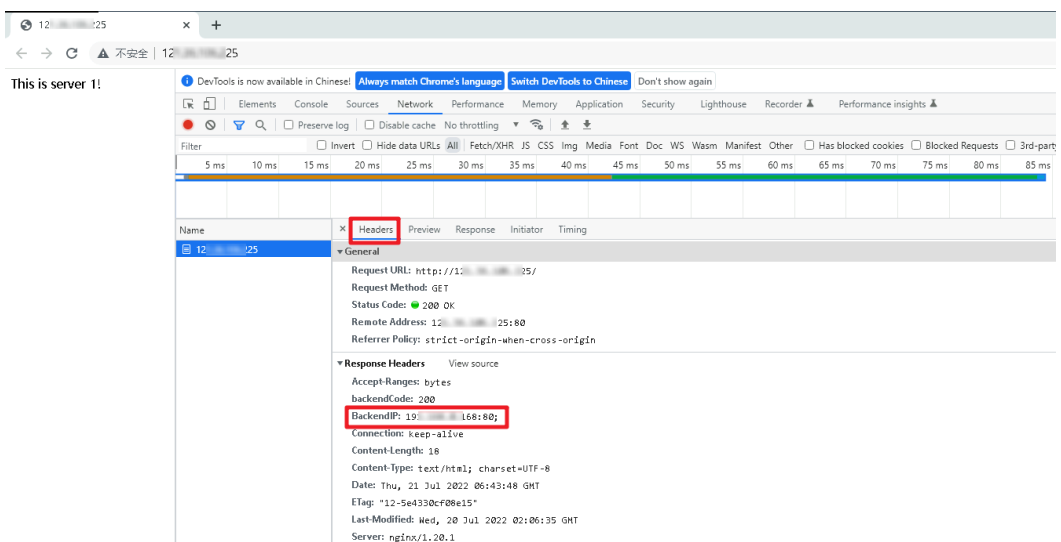
步骤5 在浏览器中多次使用HTTP协议或HTTPS协议访问虚拟IP绑定的弹性公网IP或者域名，即可实现轮询访问后端业务服务器。如HTTP协议使用http://EIP、http://域名或直接输入域名，HTTPS协议使用https://EIP，https://域名。

图 3-24 访问 VIP 挂载的 EIP



步骤6 在键盘按下F12键，可以查看Nginx将请求发送到后端哪个服务器。

图 3-25 查看 Nginx 请求转发

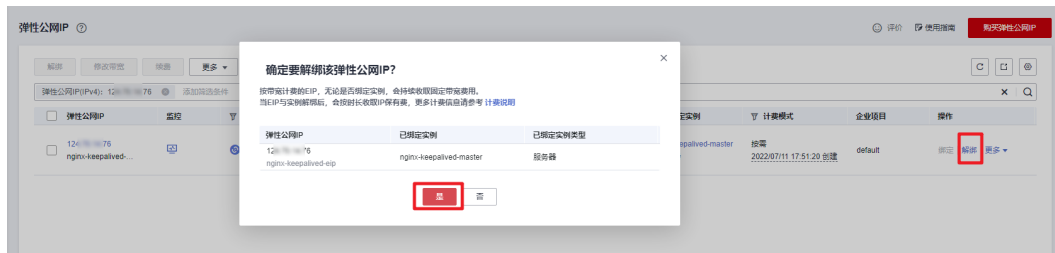


步骤7 解绑弹性公网IP。登录[华为云服务器控制台](#)，选择以负载均衡服务器名称为前缀的两台弹性云服务器，分别单击其绑定的弹性公网IP，单击“解绑>是”进行解绑。

图 3-26 查看 EIP



图 3-27 解绑 EIP



步骤8 释放弹性公网IP。分别单击两台弹性云服务器弹性公网IP右侧“更多>释放>是”，释放弹性公网IP。

图 3-28 释放 EIP



----结束

3.4 快速卸载

一键卸载

步骤1 登录[应用编排服务AOS](#)资源栈，找到该解决方案创建的资源栈，单击资源栈名称最右侧“删除”按钮，在弹出的“删除资源栈”提示框输入“Delete”，单击“确定”进行解决方案卸载。

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

- 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VIP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- 虚拟VIP：虚拟IP（Virtual IP Address，简称VIP）是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。同时，虚拟IP地址拥有私有IP地址同样的网络接入能力，包括VPC内二三层通信、VPC之间对等连接访问，以及弹性公网IP、VPN、云专线等网络接入。
- Nginx：Nginx是一款十分轻量级的HTTP服务器，Nginx，是一个高性能的HTTP和反向代理服务器，同时也是一个IMAP/POP3/SMTP代理服务器。具体请参考官网<http://nginx.org/en/>。
- Keepalived：是一个检测服务器的状态的开源软件，如果有一台web服务器宕机，或工作出现故障，Keepalived将检测到，并将有故障的服务器从系统中剔除，同时使用其他服务器代替该服务器的工作，当服务器工作正常后Keepalived自动将服务器加入到服务器群中，这些工作全部自动完成，不需要人工干涉，需要人工做的只是修复故障的服务器。具体请参考官网<https://www.keepalived.org/>。

5 修订记录

发布日期	修订记录
2022-07-30	第一次正式发布。
2023-02-28	修订实施步骤。