

解决方案实践

快速构建高可用四层负载均衡

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.....	10
3.3 开始使用.....	17
3.4 快速卸载.....	20
4 附录	22
5 修订记录	23

1 方案概述

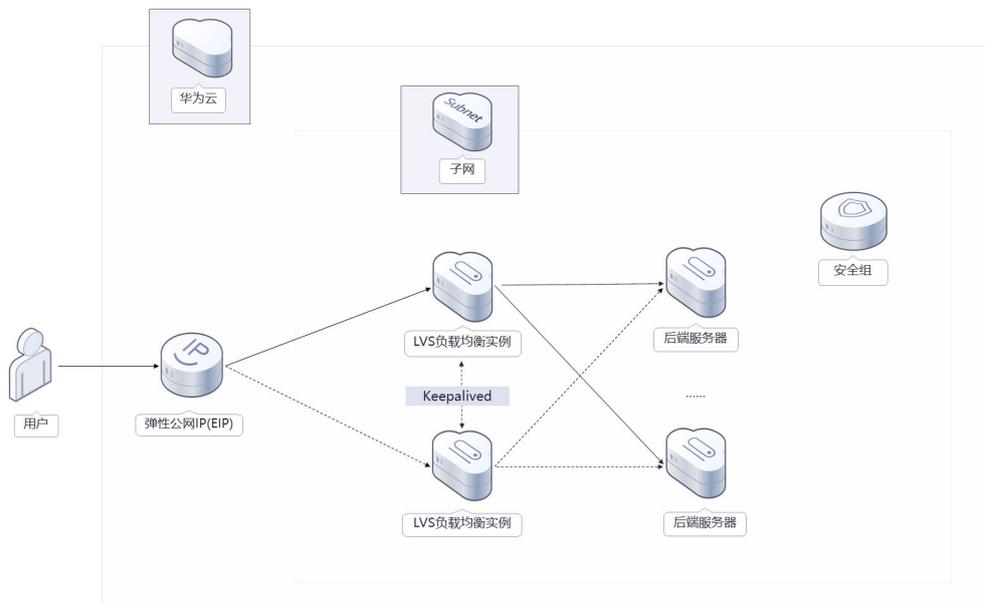
应用场景

该解决方案基于开源软件LVS+Keepalived构建，快速帮助用户在华为云（或边缘小站）弹性云服务器上完成高可用负载均衡部署。LVS节点主备部署，提供负载均衡能力，Keepalived提供健康检查和故障转移能力，提高系统的可用性。通过消除单点故障提升应用系统的可用性，是构建集群的核心，例如Web集群、数据库集群、分布式缓存服务器集群等。

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LVS云服务器主备切换。
- 创建弹性公网IP EIP，并绑定到虚拟IP上，用于提供对外访问服务（智能边缘小站 IES部署无需使用弹性公网，使用虚拟IP内网地址）。
- 在两台Linux弹性云服务器分别完成LVS和Keepalive软件的自动安装，以及高可用负载均衡环境配置。该方案采用LVS的FULLNAT模式配置。

方案优势

- 高性能
LVS抗负载能力强，该方案采用FULLNAT模式，工作在传输层上仅作分发之用，可以实现高性能的自建负载均衡。
- 高可靠
LVS云服务器主备部署，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负载均衡环境部署。

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。
- 使用“边缘小站”一键部署前，需已购买[智能边缘小站 CloudPond](#)。需要确保DNS服务器地址为华为云默认DNS地址，如已修改默认DNS服务器地址，请参考[3.1准备工作步骤3](#)进行重置。
- 已有虚拟私有云VPC、子网、安全组以及后端业务虚拟机。

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（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：1	$0.34 * 24 * 30 = 244.8$ 元
合计	-	835.2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：1	115 元
合计	-	489.4元

 说明

- “一键部署（边缘小站）”模板，仅适用于已经购买了边缘小站服务的用户。
- 在边缘小站部署该解决方案时所部署的全部资源均不涉及收费。

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“快速构建高可用四层负载均衡”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



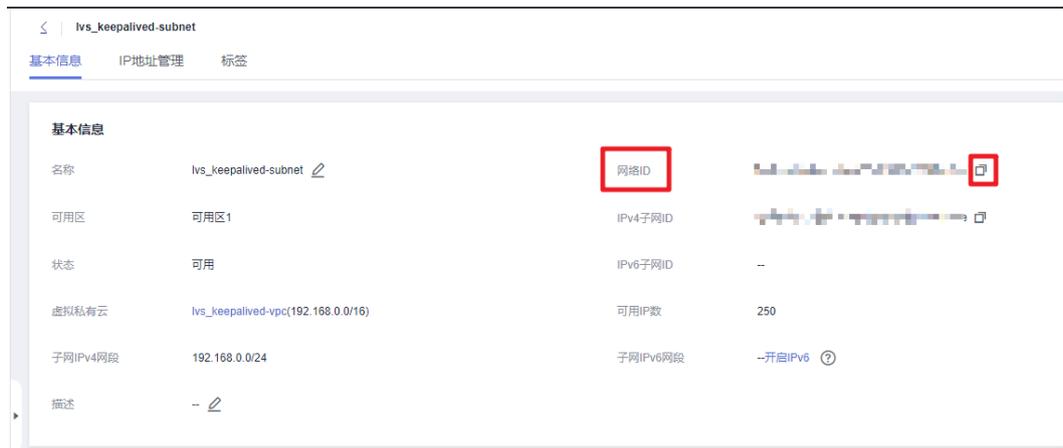
----结束

获取资源 ID

非边缘小站一键部署，只需参考完成步骤1-3；边缘小站部署需参考完成所有步骤1-4。

步骤1 登录[华为云官网控制台](#)，打开[虚拟私有云VPC](#)查看子网，打开业务虚拟机所属的子网，获取网络ID。

图 3-8 子网网络 ID



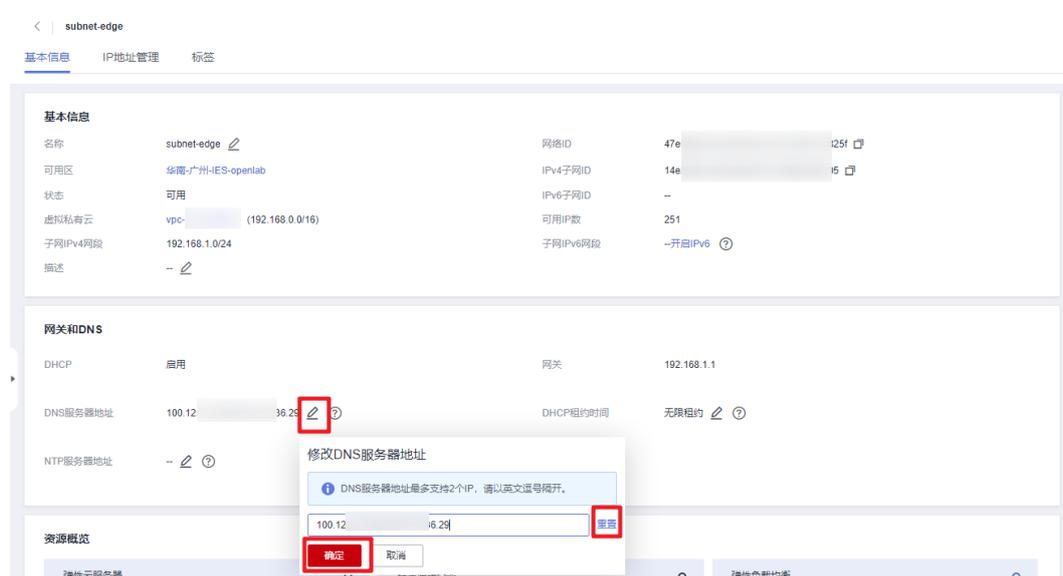
步骤2 在[网络控制台](#)，查看[安全组](#)，打开业务虚拟机所配置的安全组，获取安全组ID。

图 3-9 安全组 ID



步骤3 重置DNS服务器地址。如后端服务器所在子网下已修改默认DNS服务器地址为用户内部自定义地址，则需要重置DNS地址为华为默认地址，待解决方案部署完成后，方可修改为用户自定义地址（如用户未修改则跳过该步骤）。登录[华为云官网控制台](#)，打开[虚拟私有云VPC](#)查看子网，打开业务虚拟机所属的子网，重置DNS服务器地址。

图 3-10 重置 DNS 服务器地址



步骤4 打开[边缘小站](#)，在可用列表中，查看“状态”为可用的小站名称，单击名称打开此站点，获取边缘可用区ID（仅边缘小站部署适用）。

图 3-11 边缘可用区列表

名称	状态	区域	地点	vCPU资源使用	内存资源使用	存储资源使用	操作
IES-test-01	待部署	华南-广州	IES-test-01 四川省成都市新都区	--	--	--	订购 删除
dst1	待部署	华北-北京四	dst1 北京市 朝阳区	--	--	--	订购 删除
ERP-小站01	待部署	华北-北京四	北京-东三环 北京市 东城区	--	--	--	订购 删除
site_0XKID_test	待部署	华南-广州	0XKID_demo 广东省 佛山市 禅城区	--	--	--	订购 删除
ies_site_0XKID_test	待部署	华南-广州	0XKID_佛山_test 广东省 佛山市 禅城区	--	--	--	订购 删除
site-01	待部署	华南-广州	hawaii-01 广东省 深圳市 龙岗区	--	--	--	订购 删除
测试环境可用边缘可用区列表	待部署	华南-广州	测试环境可用边缘可用区列表 广东省 东莞市 东莞市	--	--	--	订购 删除
ies-openlab-001	可用	华南-广州	ies-openlab-001 广东省 东莞市 东莞市	24.20%	25.00%	5.49%	删除

图 3-12 边缘可用区 ID

ies-openlab-001

基本信息 资源信息 场地详情 镜像缓存

基本信息

名称 ies-openlab-001 状态 可用

场地 华南-广州-IES-openlab 区域 华南-广州

ID cf79ab56-1a02-4fff-ab0d-d9df4dda11ca 可用区ID **cn-south-1-ies-fstxz**

注册时间 2021/06/23 14:13:49 GMT+08:00 描述 中心侧: 华南-广州 边缘侧: 东莞蓝区实验室 (东莞G6-2-30R-A24)

----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。华为云上部署请参考表3-1，边缘小站部署请参考表3-2。

表 3-1 公有云一键部署参数填写说明

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

参数名称	类型	是否必填	参数解释	默认值
ecs_name	String	必填	负载均衡主、备云服务器名称前缀，服务器命名方式为{ecs_name}-master, {ecs_name}-backup, 不支持重名。取值范围：1-57个字符组成，包括字母、数字、下划线(_)、连字符(-)和句点(.)。	high-availability-four-layer-load-balancing-demo
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 2vCPUs 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。	5
ip_list	String	必填	用户后端业务服务器的私有IP地址，多个IP之间以英文半角逗号(,) 隔开。	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
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

参数名称	类型	是否必填	参数解释	默认值
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

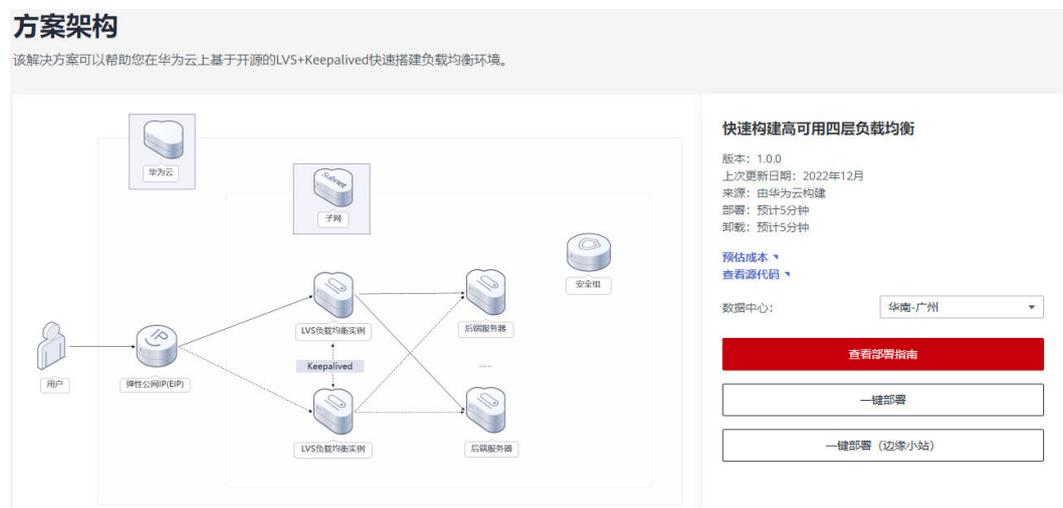
表 3-2 边缘小站一键部署参数填写说明

参数名称	类型	是否必填	参数解释	默认值
subnet_id	String	必填	边缘子网ID，该模板使用已有子网，请选择后端业务服务器同一虚拟私有云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、备云服务器名称前缀，服务器命名方式为{ecs_name}-master, {ecs_name}-backup，不支持重名。取值范围：1-57个字符组成，包括字母、数字、下划线（_）、连字符（-）和句点（.）。	空
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 。	c6s.large.2 (c6s 2vCPUs 4GiB)

参数名称	类型	是否必填	参数解释	默认值
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
availability_zone	String	必填	边缘可用区，查询并获取请参考 3.1准备工作步骤3 。	空
ip_list	String	必填	用户后端业务服务器的私有IP地址，多个IP之间以英文半角逗号（,）隔开。	空

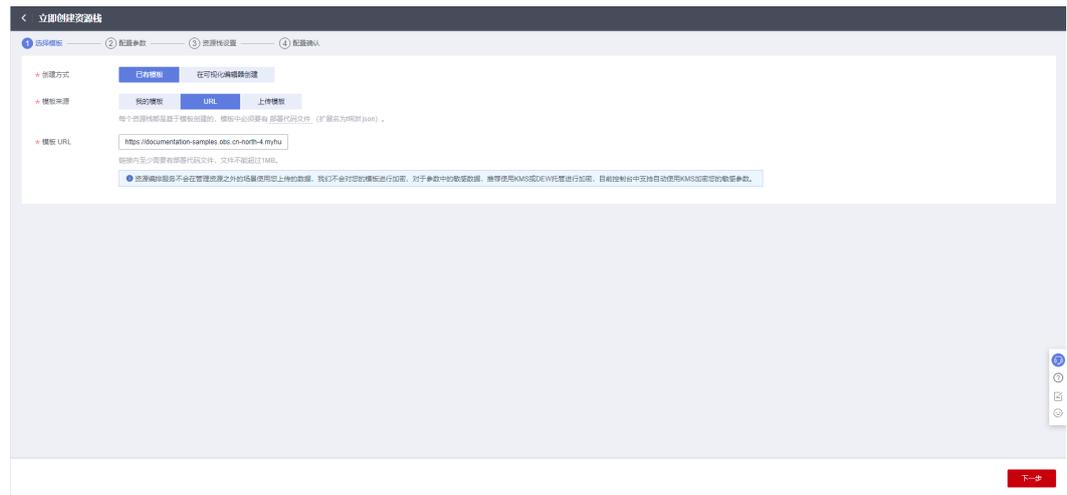
步骤1 登录华为云解决方案实践，选择“[快速构建高可用四层负载均衡](#)”，跳转至解决方案一键部署界面，数据中心下拉菜单可以选择需要部署的区域。

图 3-13 解决方案实施库



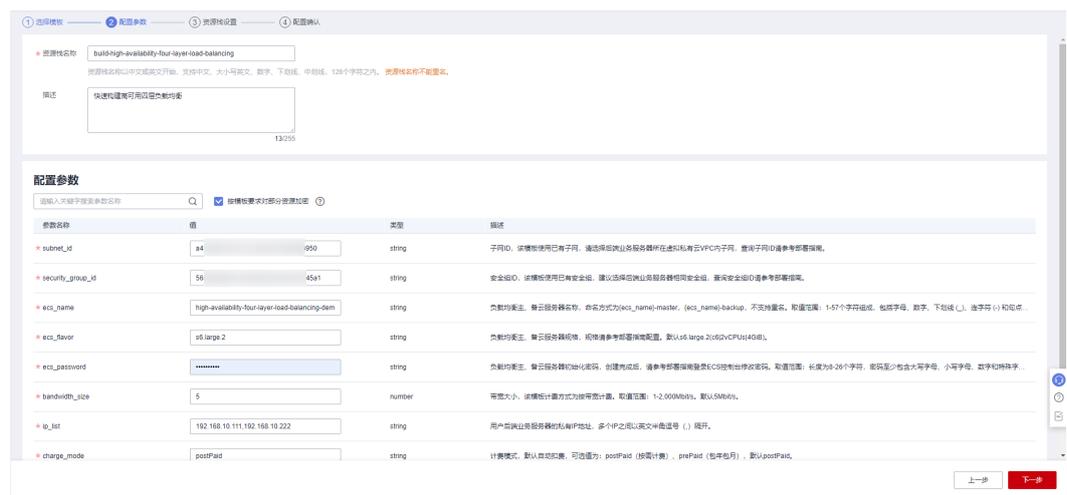
步骤2 在一键部署页面，单击“一键部署”或“一键部署（边缘小站）”，跳转至该解决方案创建资源栈部署界面。

图 3-14 创建资源栈



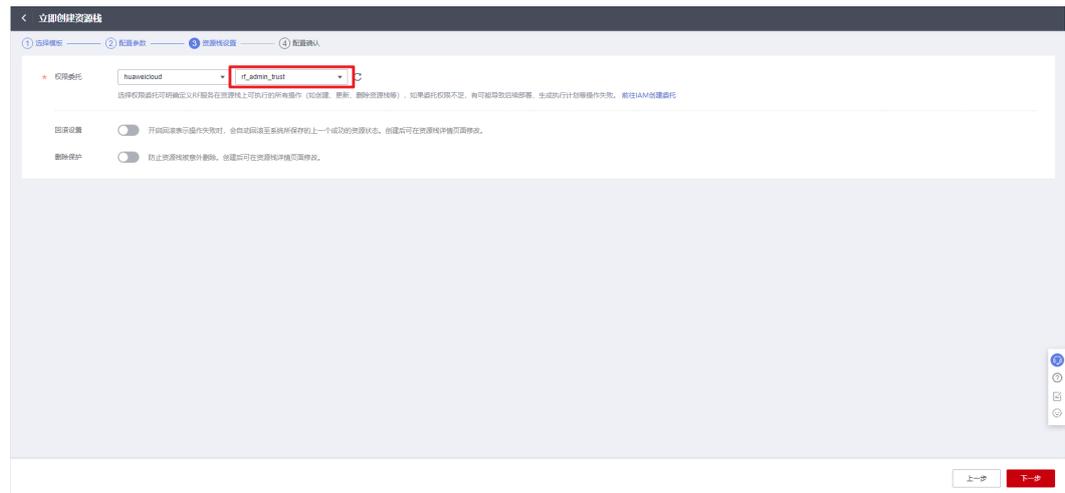
步骤3 单击“下一步”，分别参考对应模板的表1 公有云一键部署参数填写说明或表2 边缘小站一键部署参数填写说明完成自定义参数填写。

图 3-15 参数配置



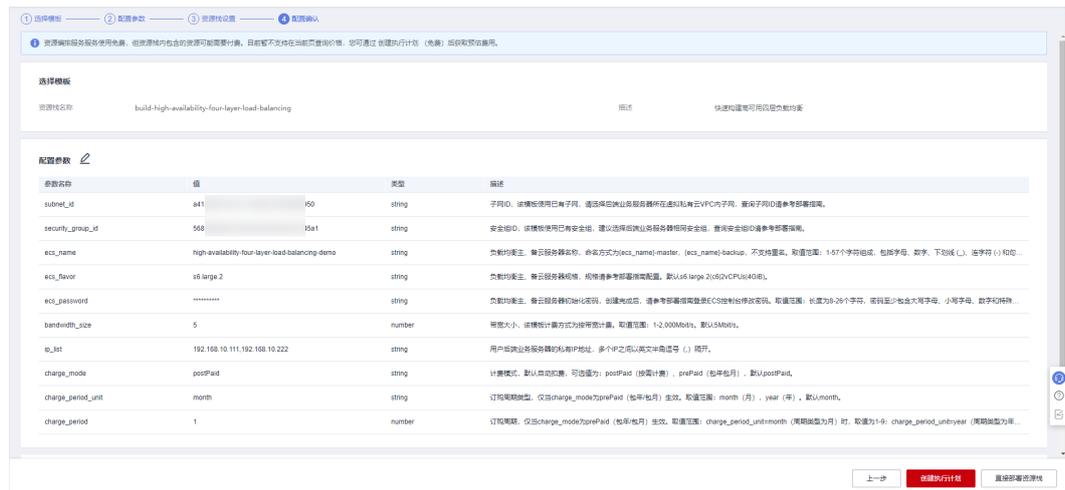
步骤4 在资源设置界面中，“权限委托”下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-16 资源栈设置



步骤5 在配置确认界面中，单击“创建执行计划”。

图 3-17 确认配置



步骤6 单击“创建执行计划”，根据提示输入执行计划名称等，单击“确定”。

图 3-18 创建执行计划



步骤7 单击右侧“部署”按钮，在弹窗上再次单击“执行”，进行方案部署。

图 3-19 创建资源



图 3-20 资源下发



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。

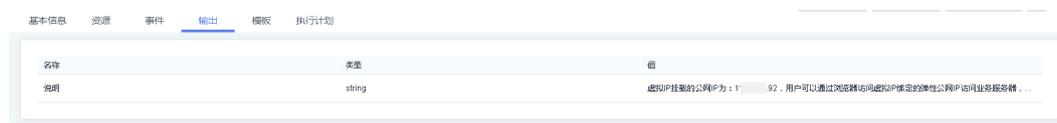
步骤9 待“事件”中出现“Apply required resource success”，表示该解决方案已经部署完成。

图 3-21 执行计划完成



步骤10 单击“输出”，查看负载均衡服务器绑定的虚拟IP地址或其绑定的弹性公网IP地址。

图 3-22 输出



----结束

3.3 开始使用

📖 说明

两台主备弹性负载均衡服务器的Keepalived配置文件路径为：`/etc/keepalived/keepalived.conf`

一键部署模板

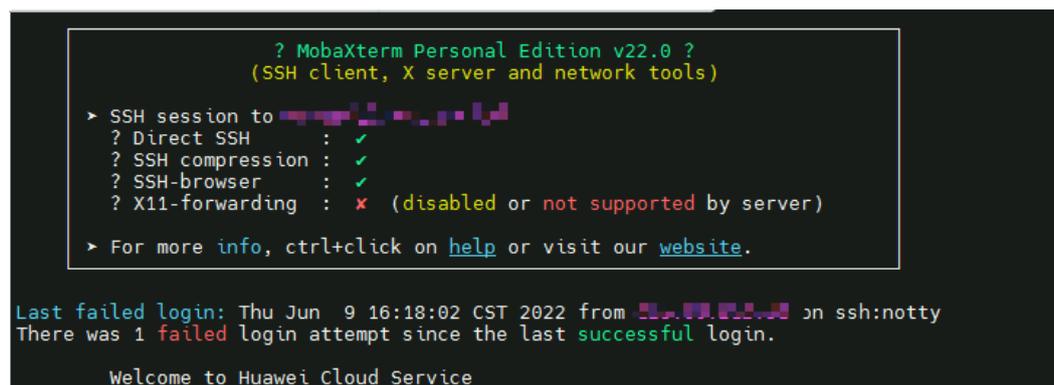
- 步骤1** 修改初始化密码。登录[华为云服务器控制台](#)，参考[在控制台重置弹性云服务器密码](#)，进行密码重置。
- 步骤2** 查看子网，打开业务虚拟机所属的子网，单击“IP地址管理”查看虚拟IP以及其绑定的弹性公网IP。

图 3-23 VIP 及绑定 EIP



- 步骤3** 打开[华为云服务器控制台](#)，查看两台服务器绑定弹性公网IP，远程登录两台弹性云服务器。管理员账户为root。

图 3-24 使用远程连接软件登录



- 步骤4** 或者通过[华为云服务器控制台](#)，选择以弹性云服务器名称为前缀的弹性云服务器，选择“远程登录”。

图 3-25 VNC 远程登录



步骤5 打开用户业务部署所在服务器，在所有服务器分别安装httpd服务，执行以下命令。注意第二行命令双引号中内容可以设置不一样，便于直观查看结果。

```
yum -y install httpd
echo "www.test01.com" > /var/www/html/index.html
chmod 777 /var/www/html/index.html
systemctl start httpd
systemctl enable httpd
curl localhost
```

步骤6 登录该解决方案创建的两台主备负载均衡弹性云服务器，执行以下命令查看被纳管的业务服务器状态（如果ipvsadm返回的服务器数量和实际不符，请排查监听后端服务器端口是否放通）。

```
ipvsadm -Ln
```

图 3-26 纳管业务服务器

```
[root@lvs-kpa-master ~]# ipvsadm -Ln
IP Virtual Server version 1.2.1 (size=4194304)
Prot LocalAddress:Port[,Subnet] Scheduler Established(Sec.) Flags
-> RemoteAddress:Port[,Oif] Forward Weight ActiveConn InactConn UtepAddr:uteport UniId Mac
TCP 192.168.0.243:80 rr
-> 192.168.0.7:80 FullNat 1 0 0
-> 192.168.0.206:80 FullNat 1 0 0
[root@lvs-kpa-master ~]#
```

步骤7 在有公网访问能力的服务器多次curl**步骤2中获取的虚拟VIP绑定的弹性公网EIP**虚拟VIP绑定的弹性公网IP，两个后端云服务器web应用内容会轮询展示：查看响应结果，两个后端云服务器web应用内容会轮询展示：

www.test01.com 或 www.test02.com

图 3-27 curl VIP 绑定的 EIP

```
[root@lvs-user ~]# curl 120.46.164.15
www.test01.com
[root@lvs-user ~]# curl 120.46.164.15
www.test02.com
[root@lvs-user ~]# _
```

步骤8 在浏览器多次访问VIP挂载的EIP：http://EIP，查看响应结果：两个后端云服务器web应用内容会随机展示：

www.test01.com 或 www.test02.com

图 3-28 访问 VIP 绑定的 EIP

The image shows two browser windows side-by-side. Both have the address bar set to 120.46.164.15. The left window displays the content of www.test02.com, and the right window displays the content of www.test01.com, demonstrating load balancing.

----结束

一键部署（边缘小站）

步骤1 打开**子网控制台**，选择该解决方案使用的子网，选择IP地址管理查看虚拟IP。

图 3-29 虚拟 IP



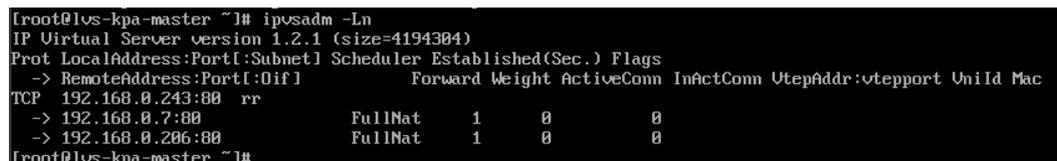
步骤2 登录已存在业务虚拟机服务器，在所有服务器分别安装httpd服务，执行以下命令。注意第二行命令双引号中内容可以设置不一样，便于直观查看结果。

```
yum -y install httpd
echo "www.test01.com" > /var/www/html/index.html
chmod 777 /var/www/html/index.html
systemctl start httpd
systemctl enable httpd
curl localhost
```

步骤3 登录两台主备弹性云服务器，执行以下命令查看被纳管的业务服务器状态（如果ipvsadm返回的服务器数量和实际不符，请排查监听后端服务器端口是否放通）。

```
ipvsadm -Ln
```

图 3-30 纳管业务服务器



步骤4 登录其他服务器，多次curl VIP（或在浏览器中访问虚拟IP地址：http://VIP），查看响应结果，两个后端云服务器web应用内容会轮询展示：

```
www.test01.com 或 www.test02.com
```

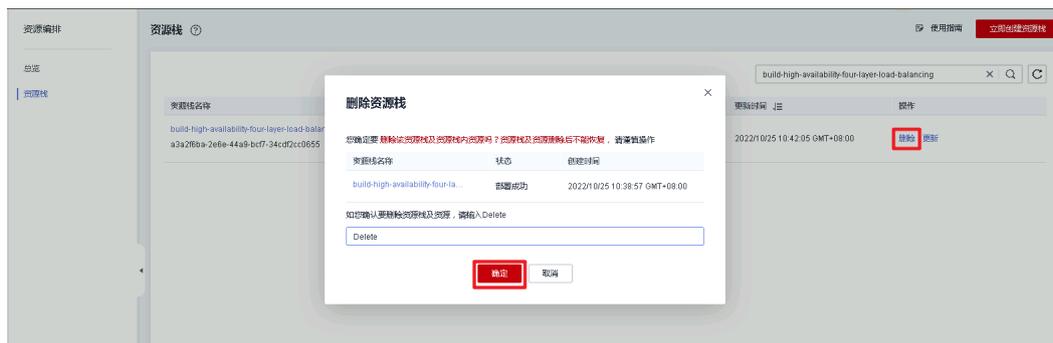
----结束

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 3-31 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。
- LVS：是Linux Virtual Server的简称，是一款开源Linux虚拟服务器软件。Linux虚拟服务器是一个高度可扩展和高度可用的服务器，构建在真实服务器集群上，[负载均衡器](#)在Linux操作系统上运行。服务器集群的架构对最终用户是完全透明的，用户之间的交互就像一个高性能的虚拟服务器一样。Linux虚拟服务器作为一种高级[负载均衡](#)解决方案，可用于构建高度可扩展且高度可用的网络服务，例如可扩展的Web、缓存、邮件、FTP、媒体和VoIP服务。
- 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。

5 修订记录

发布日期	修订记录
2022-06-30	第一次正式发布。
2023-02-28	修订实施步骤。