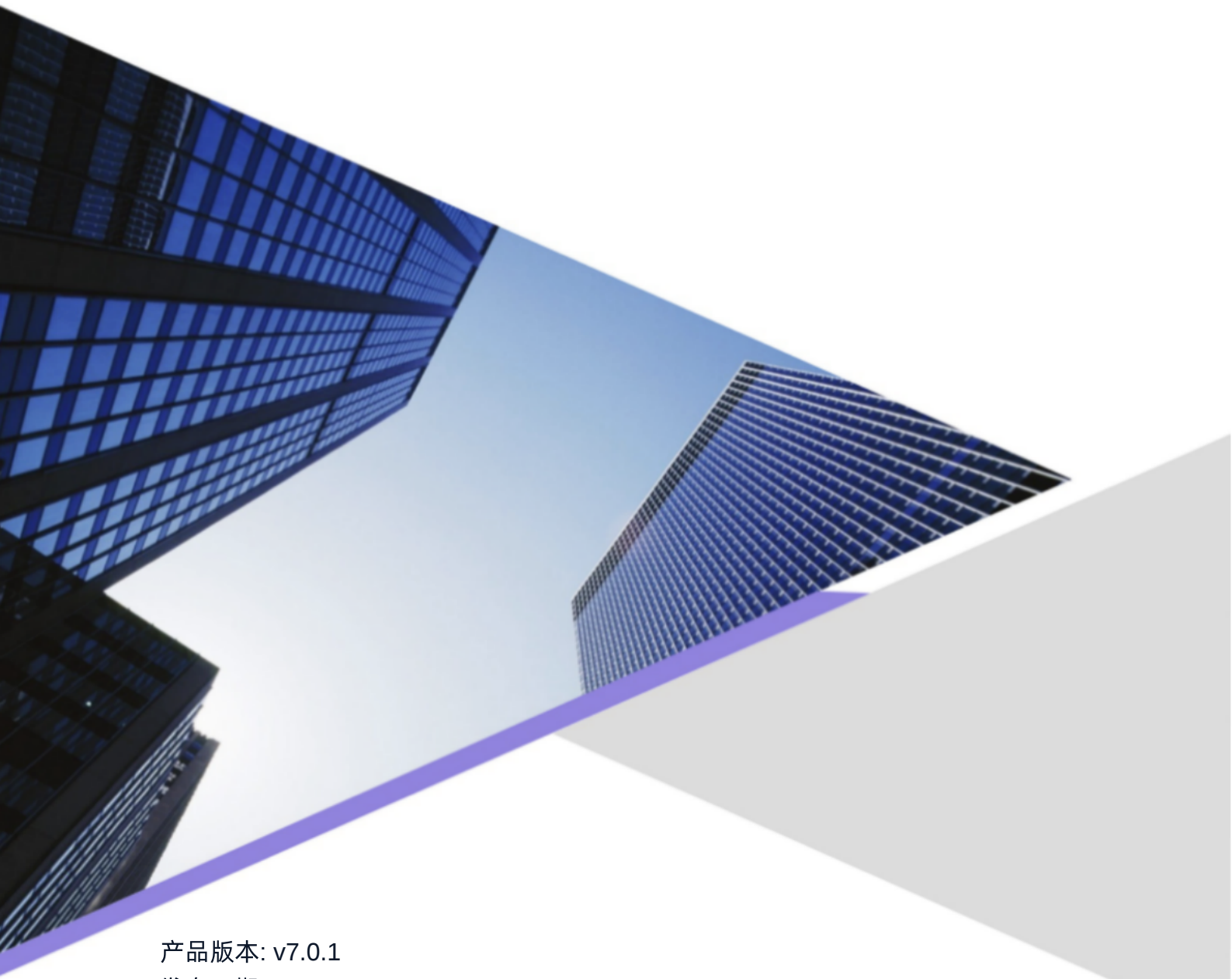
EasyStack
易捷行云

独享型负载均衡服务

最佳实践



产品版本: v7.0.1

发布日期: 2026-08-18

目录

1 最佳实践

1.1 构建具备四层负载均衡能力的TCP服务

背景描述

负载均衡器可以将来自公网地址的访问流量分发到多个资源上，并支持自动检测并隔离不可用的资源，提高业务的服务能力和可用性。用户可以灵活调整资源池中的资源，而不影响业务的正常访问，并且，负载均衡器通过将所收到的网络流量转发到工作负载较低的资源上，从而使整个资源集群以高效的方式快速处理访问流量。本文将以构建具备四层负载均衡能力的TCP服务为例，介绍如何借助三台云主机托管TCP服务以便支持生产工作负载，同时尽可能减少用户的运维工作。

前提条件

- 已完成 前置条件准备。
- 已创建三台规格相同的云主机，用于托管TCP服务。
- 已准备一个可供外部访问的公网IP地址。

操作步骤

1. 创建负载均衡器。
   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。
   2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。
   3. “子网”选择云主机所在子网，并配置其他参数后，单击 `创建` ，完成操作。其中，各参数的具体说明，请参考 创建负载均衡器。
2. 创建监听器。
   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。
   2. 在“监听器配置”页面中，“协议”选择“TCP（性能模式）”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“22”，并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。
   3. 在“资源池配置”页面中，“资源池”选择“新建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”选择“TCP（性能模式）”，“负载方式”选择“轮询”，并配置其他参数后，单击

确认 ，完成操作。其中，各参数的具体说明，请参考 创建监听器。

3. 配置资源池资源。
   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[资源池]页签中，单击上述新建资源池的名称 ，进入其详情页面。
   2. 在“资源列表”区域框中，单击 添加云内资源 ，弹出“添加云内资源”对话框。
   3. 在“添加云内资源”页面中，选择上述三台云主机后，单击 下一步：资源配置 ，进入“资源配置”页面。
   4. 在“资源配置”页面中，配置参数后，单击 下一步：确认信息 ，进入“确认信息”页面。
   5. 在“确认信息”页面中，确认各资源的配置信息后，单击 添加 ，完成操作。
4. 绑定公网IP。
   1. 在“独享型负载均衡”页面中，勾选上述负载均衡器后，单击 绑定公网IP ，弹出“绑定公网IP”对话框。
   2. 配置参数后，单击 绑定 ，完成操作。

结果验证

1. 通过远程客户端访问上述公网IP地址，确认当前成功登录的云主机。具体命令如下:

```
ssh root@<公网IP地址>
```

2. 退出远程访问访问。具体命令如下:

```
exit
```

3. 重新访问上述公网IP地址，确认当前已成功登录另一台云主机。

```
(client) [root@node-1 ~]# ssh root@172.70.0.167
Warning: Permanently added '172.70.0.167' (ECDSA) to the list of known hosts.
root@172.70.0.167's password:
Last login: Wed Aug 11 14:17:56 2021
[root@qlq-mem-vm1 ~]#
[root@qlq-mem-vm1 ~]#
[root@qlq-mem-vm1 ~]# exit
登出
Connection to 172.70.0.167 closed.
(client) [root@node-1 ~]#
(client) [root@node-1 ~]# ssh root@172.70.0.167
Warning: Permanently added '172.70.0.167' (ECDSA) to the list of known hosts.
root@172.70.0.167's password:
Last login: Wed Jul 21 19:32:39 2021
[root@qlq-mem-vm2 ~]# Connection to 172.70.0.167 closed by remote host.
Connection to 172.70.0.167 closed.
(client) [root@node-1 ~]# ^C
(client) [root@node-1 ~]#
```

1.2 构建具备七层负载均衡能力的基础Web应用程序

背景描述

负载均衡器可以将来自公网地址的访问流量分发到多个资源上，并支持自动检测并隔离不可用的资源，提高业务的服务能力和可用性。用户可以灵活调整资源池中的资源，而不影响业务的正常访问，并且，负载均衡器通过将所收到的网络流量转发到工作负载较低的资源上，从而使整个资源集群以高效的方式快速处理访问流量。此外，通过为HTTP/HTTPS负载均衡监听器配置L7策略，可以对流入负载均衡器的流量进行高级控制，使不同客户端在连接到同一负载均衡器的情况下，能够依据所配置的L7策略进行自定义转发。本文将以构建具备七层负载均衡能力的基础Web应用程序为例，介绍如何借助三台云主机托管Web应用程序以便支持生产工作负载，同时实现对流量的高级管控。

前提条件

- 已完成 前置条件准备。
- 已创建三台规格相同的云主机，用于托管Web应用程序。
- 已准备一个可供外部访问的公网IP地址。

操作步骤

1. 配置Web应用程序。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[云主机]，进入“云主机”页面。

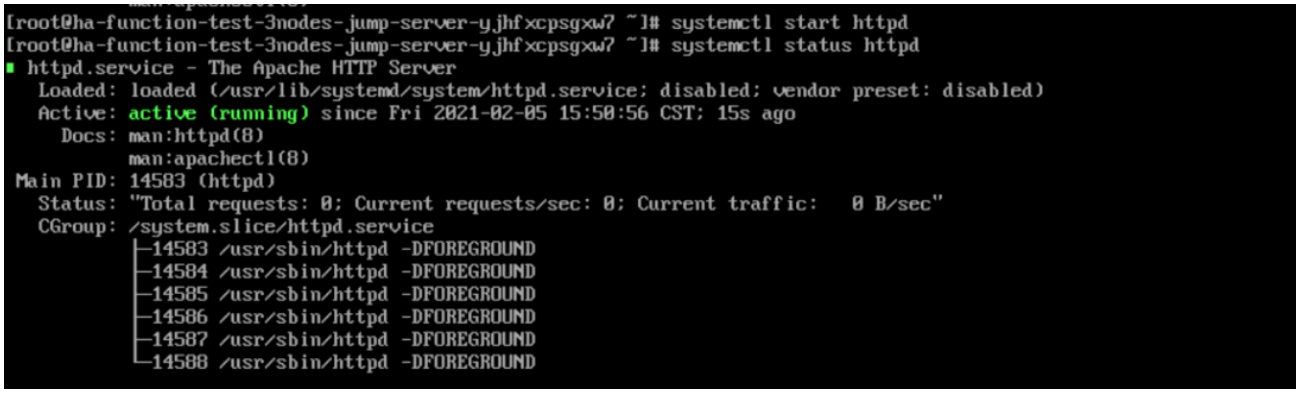
    2. 单击各云主机所在行的VNC图标，访问其控制台并登录云主机。

    3. 安装并启动Apache服务器。具体命令如下:

        ```
        yum install httpd
        systemctl start httpd
        ```

    4. 确认Apache服务器启动成功。具体命令如下:

```
systemctl status httpd
```



2. 创建负载均衡器。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。

    2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。

    3. “子网”选择云主机所在子网，并配置其他参数后，单击 `创建` ，完成负载均衡器创建。其中，各参数的具体说明，请参考 创建负载均衡器。

    4. 绑定公网IP。

        1. 在“独享型负载均衡”页面中，勾选上述负载均衡器后，单击 `绑定公网IP` ，弹出“绑定公网IP”对话框。

        2. 配置参数后，单击 `绑定` ，完成操作。

3. 创建监听器和资源池。

    由于在本实践方案中，将采用配置重定向到资源池的L7策略方式，实现对流量的高级管控。所以在创建监听器时，除为其新建默认资源池外，还将为其另创建一个重定向资源池。其中，各参数的具体说明，请参考创建监听器。

    1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。

    2. 在“监听器配置”页面中，“协议”选择“HTTP”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“80”，并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。

3. 在“资源池配置”页面中，“资源池”选择“新建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”选择“HTTP”，“负载方式”选择“轮询”，并配置其他参数后，单击 `确认` ，完成监听器和默认资源池的创建。

4. 创建重定向资源池。

   1. 在上述负载均衡器详情页面的[资源池]页签中，单击 `创建资源池` ，进入“创建资源池”页面。

   2. 配置参数后，单击 `创建` ，完成操作。

4. 配置L7策略。

   在本实践方案中，将对请求URL路径（ **PATH** ）中包含 **zh-cn** 的流量，采取重定向到重定向资源池的L7策略。其中，各参数的具体说明，请参考 创建监听器。

   1. 创建L7策略。

      1. 在上述负载均衡器详情页面的[监听器]页签中，单击监听器名称 ，进入其详情页面。在详情页的“七层负载均衡策略”区域框中，单击 `创建七层负载均衡策略` ，弹出“创建七层负载均衡策略”对话框。

      2. “动作”选择“重定向到资源池”，“资源池”选择上述重定向资源池，并配置其他参数后，单击 `保存` ，完成操作。

   2. 创建L7规则。

      1. 在“七层负载均衡策略”区域框中，单击待操作L7策略名称后的展开箭头，展开L7规则区域框。

      2. 单击 `创建` ，弹出“创建规则”对话框。

      3. “匹配内容类型”选择“PATH”，“匹配规则类型”选择“包含”，“匹配内容”输入“zh-cn”，并配置其他参数后，单击 `保存` ，完成操作。

5. 分别配置默认资源池和重定向资源池中资源。

   在本实践方案中，将为默认资源池配置两台云主机，为重定向资源池配置一台云主机。具体配置步骤如下：

   1. 在上述负载均衡器详情页面的[资源池]页签中，单击待操作资源池的名称 ，进入其详情页面。

   2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。

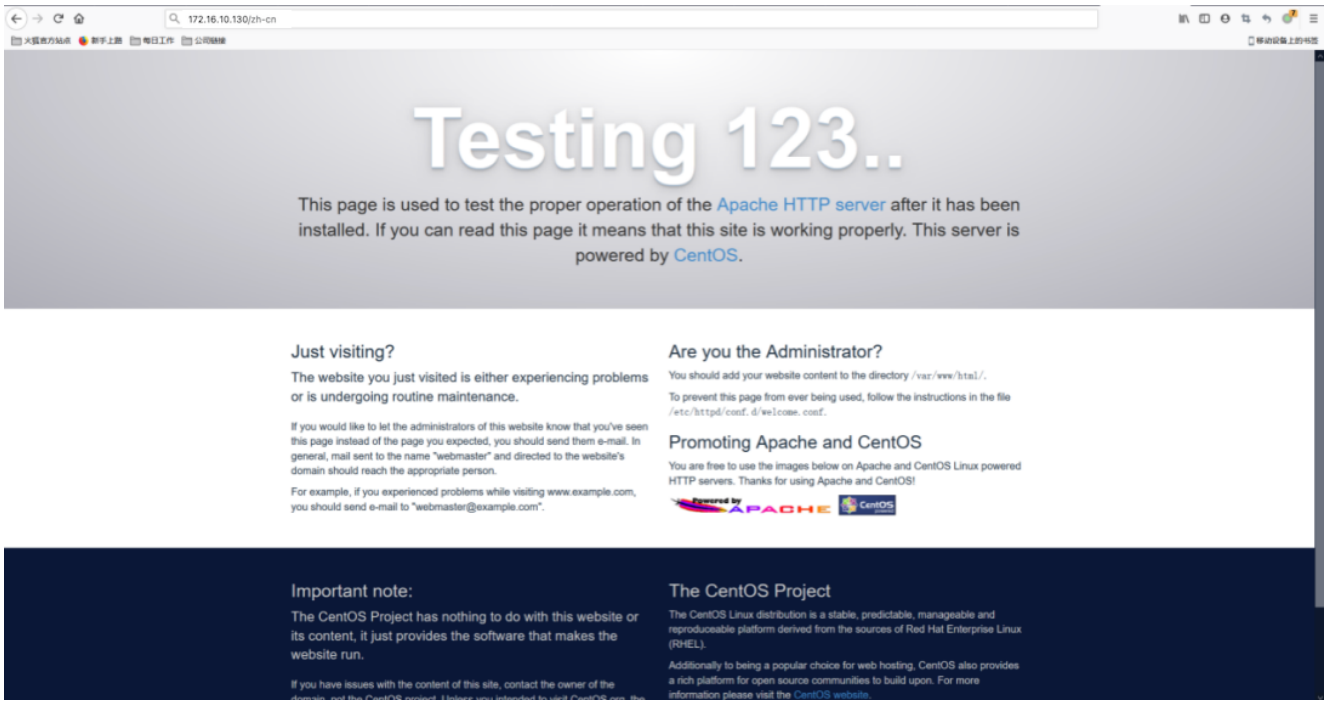
   3. 在“添加云内资源”页面中，选择对应云主机后，单击 `下一步：资源配置` ，进入“资源配置”页面。

4. 在“资源配置”页面中，配置参数后，单击 `下一步：确认信息` ，进入“确认信息”页面。

5. 在“确认信息”页面中，确认各资源的配置信息后，单击 `添加` ，完成操作。

结果验证

- 通过浏览器访问公网IP地址，确认可以正常进入到Apache服务器页面中。



- 通过远程客户端多次访问公网IP地址，确认当路径包含 **zh-cn** 时只能访问到指定IP地址的云主机。具体命令如下:

```
curl -s <公网IP地址>/zh-cn
```

1.3 构建双栈多VIP的负载均衡服务

背景描述

负载均衡器在创建完成后，除了自身携带的VIP地址外，还支持通过 `绑定VIP` 功能为其绑定其他子网的VIP地址。当为负载均衡器绑定一个IPv6地址后，该负载均衡器便同时具备IPv4和IPv6两种类型的VIP地址，即双栈VIP，可以同时对外提供IPv4和IPv6的访问入口。同时，由于在创建监听器时可以指定监听器所使用的VIP地址，所以可以在同一个负载均衡器上分别创建IPv4监听器和IPv6监听器，并为其配置不同IP类型的资源池和资源，从而将IPv4和IPv6的访问流量分别转发至对应IP类型的后端服务，在不改造现有IPv4业务的前提下平滑支持IPv6访问。本文将以构建具备双栈VIP的Web服务为例，介绍如何为负载均衡器绑定IPv6地址，并通过两个监听器分别访问IPv4和IPv6的后端服务。

前提条件

- 已完成 前置条件准备。
- 已创建一个IPv4子网和一个IPv6子网，且两个子网属于同一个网络。
- 已创建四台规格相同的云主机，用于托管Web应用程序。其中，两台云主机连接IPv4子网并已分配IPv4地址，另外两台云主机连接IPv6子网并已分配IPv6地址。
- 上述四台云主机中的Web应用程序已启动，且分别监听对应IP类型地址的80端口。

操作步骤

1. 创建负载均衡器。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。
    2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。
    3. “子网”选择IPv4子网，“VIP地址”选择“自动分配VIP”，并配置其他参数后，单击 `创建` ，完成负载均衡器创建。其中，各参数的具体说明，请参考 创建负载均衡器。

2. 绑定VIP，构建双栈VIP。

    在本实践方案中，负载均衡器创建时已自带一个IPv4类型的VIP地址，此处再为其绑定一个IPv6类型的VIP地址，使该负载均衡器同时具备IPv4和IPv6两个访问入口。 1. 在“独享型负载均衡”页面中，勾选上述负载均

衡器后，单击 `绑定VIP` ，弹出“绑定VIP”对话框。 2. “子网”选择上述IPv6子网，“VIP地址”选择“自动分配VIP”（如需使用指定的IPv6地址，则选择“手动指定VIP”并输入该IPv6地址），单击 `绑定` ，完成操作。 3. 单击上述负载均衡器名称，进入其详情页面，确认在“VIP地址”中已同时显示IPv4和IPv6两个VIP地址。

> 说明：
>
> 一个负载均衡器支持绑定多个VIP地址，且各VIP地址所属子网需要属于同一个网络。当不再需要某个VIP地址时，可以通过 `解绑VIP` 将其解绑，但负载均衡器创建时自带的VIP地址不支持解绑。

3. 创建IPv4监听器和IPv4资源池。

   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。
   2. 在“监听器配置”页面中，“协议”选择“HTTP”，“VIP”选择上述IPv4类型的VIP地址，“协议端口”输入“80”，并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。
   3. 在“资源池配置”页面中，“资源池”选择“新建”，“名称”输入便于识别的名称（如“pool-ipv4”），“IP类型”选择“IPv4”，“协议”选择“HTTP”，“负载方式”选择“轮询”，并配置其他参数后，单击 `确认` ，完成监听器和IPv4资源池的创建。其中，各参数的具体说明，请参考 创建监听器。

4. 创建IPv6监听器和IPv6资源池。

   1. 在上述负载均衡器详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。
   2. 在“监听器配置”页面中，“协议”选择“HTTP”，“VIP”选择上述IPv6类型的VIP地址，“协议端口”输入“80”，并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。
   3. 在“资源池配置”页面中，“资源池”选择“新建”，“名称”输入便于识别的名称（如“pool-ipv6”），“IP类型”选择“IPv6”，“协议”选择“HTTP”，“负载方式”选择“轮询”，并配置其他参数后，单击 `确认` ，完成监听器和IPv6资源池的创建。

5. 分别配置IPv4资源池和IPv6资源池中的资源。

在本实践方案中，将为IPv4资源池添加两台使用IPv4地址的云主机，为IPv6资源池添加两台使用IPv6地址的云主机。具体配置步骤如下： 1. 在上述负载均衡器详情页面的[资源池]页签中，单击待操作资源池的名称，进入其详情页面。 2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。 3. 在“添加云内资源”页面中，选择与该资源池IP类型对应的子网（IPv4资源池选择IPv4子网，IPv6资源池选择IPv6子网），并选择对应的云主机后，单击 `下一步：资源配置` ，进入“资源配置”页面。 4. 在“资源配置”页

面中，配置端口号80，权重100后，单击 `下一步：确认信息` ，进入“确认信息”页面。 5. 在“确认信息”页面中，确认各资源的IP地址类型和配置信息后，单击 `添加` ，完成操作。 6. 参考上述步骤，为另一个资源池添加对应IP类型的云内资源。

结果验证

1. 登录一台与负载均衡器同网络且支持双栈访问的云主机，多次执行以下命令访问IPv4的VIP地址，确认请求被轮流转发至IPv4资源池中的两台云主机。具体命令如下:

```
curl http://:80
```

2. 在该云主机上多次执行以下命令访问IPv6的VIP地址，确认请求被轮流转发至IPv6资源池中的两台云主机，且与IPv4的访问结果互不影响。具体命令如下:

```
curl -g -6 http://[]:80
```

1.4 利用七层负载均衡策略构建HTTPS域名映射服务

背景描述

负载均衡器可以将来自公网地址的访问流量分发到多个资源上，并支持自动检测并隔离不可用的资源，提高业务的服务能力和可用性。用户可以灵活调整资源池中的资源，而不影响业务的正常访问，并且，负载均衡器通过将所收到的网络流量转发到工作负载较低的资源上，从而使整个资源集群以高效的方式快速处理访问流量。此外，通过为HTTP/HTTPS负载均衡监听器配置L7策略，可以对流入负载均衡器的流量进行高级控制，使不同客户端在连接到同一负载均衡器的情况下，能够依据所配置的L7策略进行自定义转发。本文通过利用七层负载均衡策略来构建https域名映射服务为例，介绍如何借助四台云主机托管Web应用程序以便支持生产工作负载，同时实现对流量的高级管控。

前提条件

- 已完成 前置条件准备。
- 已申请一个 **Let's Encrypt** 证书。
- 已创建四台规格相同的云主机，用于托管Web应用程序。
- 已准备一个可供外部访问的公网IP地址。

操作步骤

1. 配置Web应用程序。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[云主机]，进入“云主机”页面。

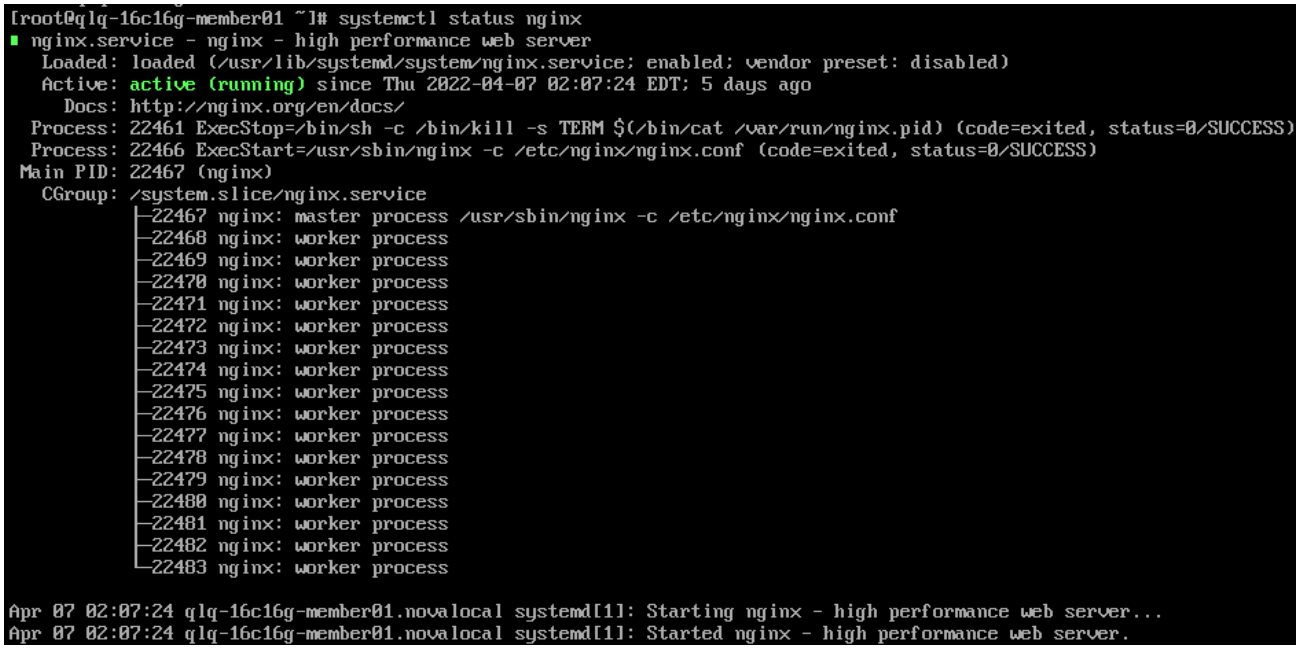
    2. 单击各云主机所在行的VNC图标，访问其控制台并登录云主机。

    3. 安装并启动nginx服务器。具体命令如下:

        ```
        yum install nginx
        systemctl start nginx
        ```

    4. 确认nginx服务器启动成功。具体命令如下:

```
systemctl status nginx
```



5. 请参考下图，依次修改四台云主机的nginx index文件，方便对每台云主机进行标识。

```
[root@qlq-16c16g-member01 ~]# cat /usr/share/nginx/html/index.html
<!DOCTYPE html>
<html>
<head>
<title>Welcome to test2.example.cn member01!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to test2.example.cn member01!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
[root@qlq-16c16g-member01 ~]# _
```

2. 创建负载均衡器。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。
    2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。
    3. “子网”选择云主机所在子网，并配置其他参数后，单击 `创建` ，完成负载均衡器创建。其中，各参数的具体说明，请参考 创建负载均衡器。
    4. 绑定公网IP。
        1. 在“独享型负载均衡”页面中，勾选上述负载均衡器后，单击 `绑定公网IP` ，弹出“绑定公网IP”对话框。
        2. 配置参数后，单击 `绑定` ，完成操作。

3. 创建监听器和资源池。

    由于在本实践方案中，将采用配置重定向到资源池的L7策略方式，实现对流量的高级管控。所以在创建监听器时，除为其新建默认资源池外，还将为其另创建一个重定向资源池。其中，各参数的具体说明，请参考

创建监听器。

1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。

2. 在“监听器配置”页面中，“协议”选择“HTTPS”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“443”，选择证书（如何托管证书，参考证书管理服务说明文档。）并配置其他参数后，单击 `下一步: 资源池配置` ，进入“资源池配置”页面。

3. 在“资源池配置”页面中，“资源池”选择“新建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”选择“HTTP”，“负载方式”选择“轮询”，并配置其他参数后，单击 `确认` ，完成监听器和默认资源池的创建。

4. 创建重定向资源池。

    1. 在上述负载均衡器详情页面的[资源池]页签中，单击 `创建资源池` ，进入“创建资源池”页面。

    2. 配置参数后，单击 `创建` ，完成操作。

4. 配置L7策略。

    在本实践方案中，将对请求域名中包含 **test1.example.cn** 和 **test2.example.cn** 的流量，采取重定向到重定向资源池的L7策略。其中，各参数的具体说明，请参考 创建监听器。

    1. 创建L7策略。

        1. 在上述负载均衡器详情页面的[监听器]页签中，单击监听器名称 ，进入其详情页面。在详情页的“七层负载均衡策略”区域框中，单击 `创建七层负载均衡策略` ，弹出“创建七层负载均衡策略”对话框。

        2. “动作”选择“重定向到资源池”，“资源池”选择上述重定向资源池，并配置其他参数后，单击 `保存` ，完成操作。

    2. 创建L7规则。

        1. 在“七层负载均衡策略”区域框中，单击待操作L7策略名称后的展开箭头，展开L7规则区域框。

        2. 单击 `创建` ，弹出“创建规则”对话框。“匹配内容类型”选择“HOST_NAME”，“匹配规则类型”选择“正则”，“匹配内容”输入“test1.example.cn”，并配置其他参数后，单击 `保存` ，完成针对 **test1.example.cn** 流量的规则创建。

3. 重复上一步，创建针对 **test2.example.cn** 流量的规则。即“匹配内容”请输入“test2.example.cn”。

5. 分别配置默认资源池和重定向资源池中资源。

在本实践方案中，将为默认资源池配置两台云主机，为重定向资源池配置另外两台云主机。具体配置步骤如下：

1. 在上述负载均衡器详情页面的[资源池]页签中，单击待操作资源池的名称，进入其详情页面。
2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。
3. 在“添加云内资源”页面中，选择对应云主机后，单击 `下一步：资源配置` ，进入“资源配置”页面。
4. 在“资源配置”页面中，配置参数后，单击 `下一步：确认信息` ，进入“确认信息”页面。
5. 在“确认信息”页面中，确认各资源的配置信息后，单击 `添加` ，完成操作。

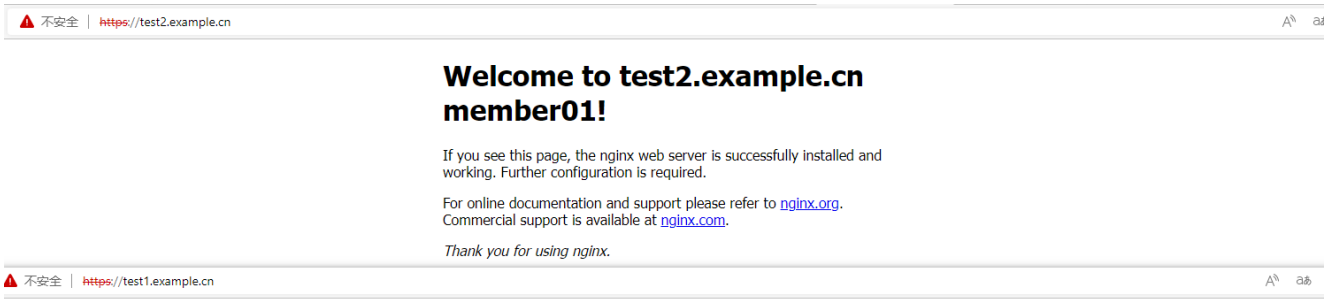
结果验证

1. 在本地计算机的 **hosts** 文件中，添加对公网IP地址的域名访问映射。

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
172.49.0.157 test1.example.cn
172.49.0.157 test2.example.cn
```

2. 在本地计算机的浏览器地址栏中输入 **https://test1.example.cn** 或 **https://test2.example.cn**，访问对应内容。


不安全 | https://test2.example.cn
Welcome to test2.example.cn member01!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.
不安全 | https://test1.example.cn
Welcome to test1.example.cn member02!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.

1.5 启用HTTP1.1版本健康检查器并使用云主机域名进行健康检查

背景描述

健康检查是指在负载均衡器中，对后端服务器进行定期检查，以确定其是否能够正常接受并处理流量。如果后端服务器被检测为不健康状态，则流量将不会被转发到该服务器，以确保流量的可靠性和服务的高可用性。独享型负载均衡健康检查器支持TCP、PING、HTTP等三种类型的健康检查，HTTP类型扩展了对HTTP1.1协议的支持，提供更加丰富的健康检查策略。本文即是验证通过主机域名进行健康检查的实践。

前提条件

- 已完成 前置条件准备。
- 已创建三台规格相同的云主机，用于托管Web应用程序。

操作步骤

1. 配置Web应用程序。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[云主机]，进入“云主机”页面。

   2. 使用nginx镜像，创建3台云主机vm1，vm2，vm3。在vm1，vm2，vm3中分别执行以下命令：

      ```
      echo "exampleX">/usr/share/nginx/example.com/index.html
      注：X对应每台云主机的索引。
      ```

   3. 在nginx.conf文件中增加server配置。具体配置如下:

      ```
      server {
         listen 80;
         listen [::]:80;

         server_name example.com;

         root /usr/share/nginx/example.com;
      ```

```
    index index.html;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

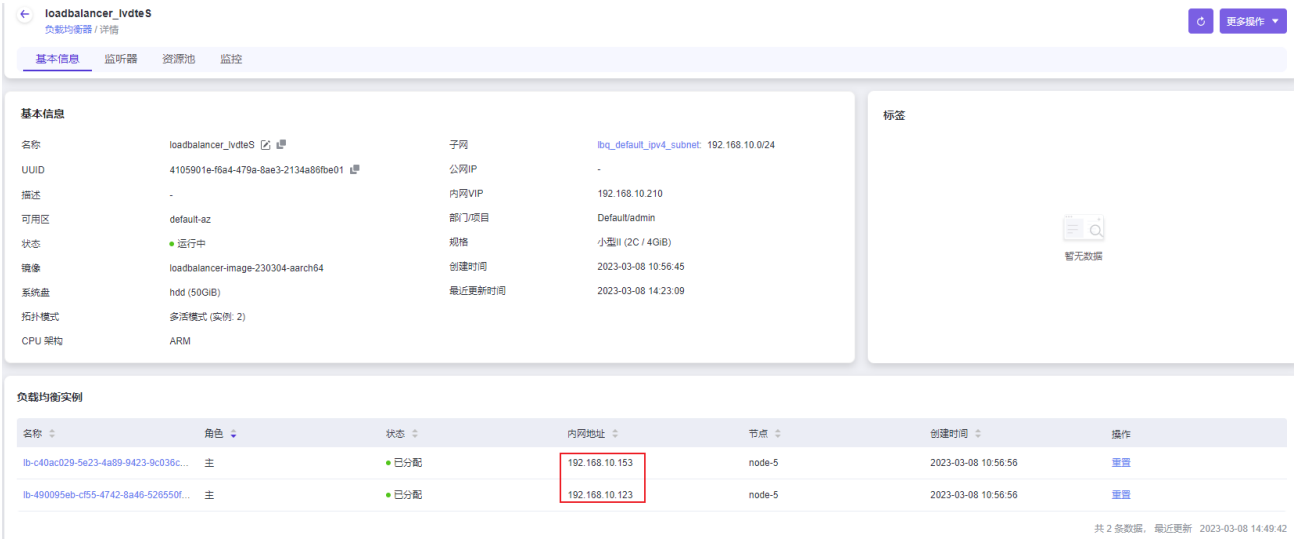
2. 使用命令systemctl restart nginx重启nginx。

3. 创建多活负载均衡器。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。

   2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。

   3. 拓扑模式选择多活模式，实例数量保持默认，“子网”选择云主机所在子网，并配置其他参数后，单击 `保存` ，完成操作。其中，各参数的具体说明，请参考 创建负载均衡器。



4. 创建监听器。

   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。

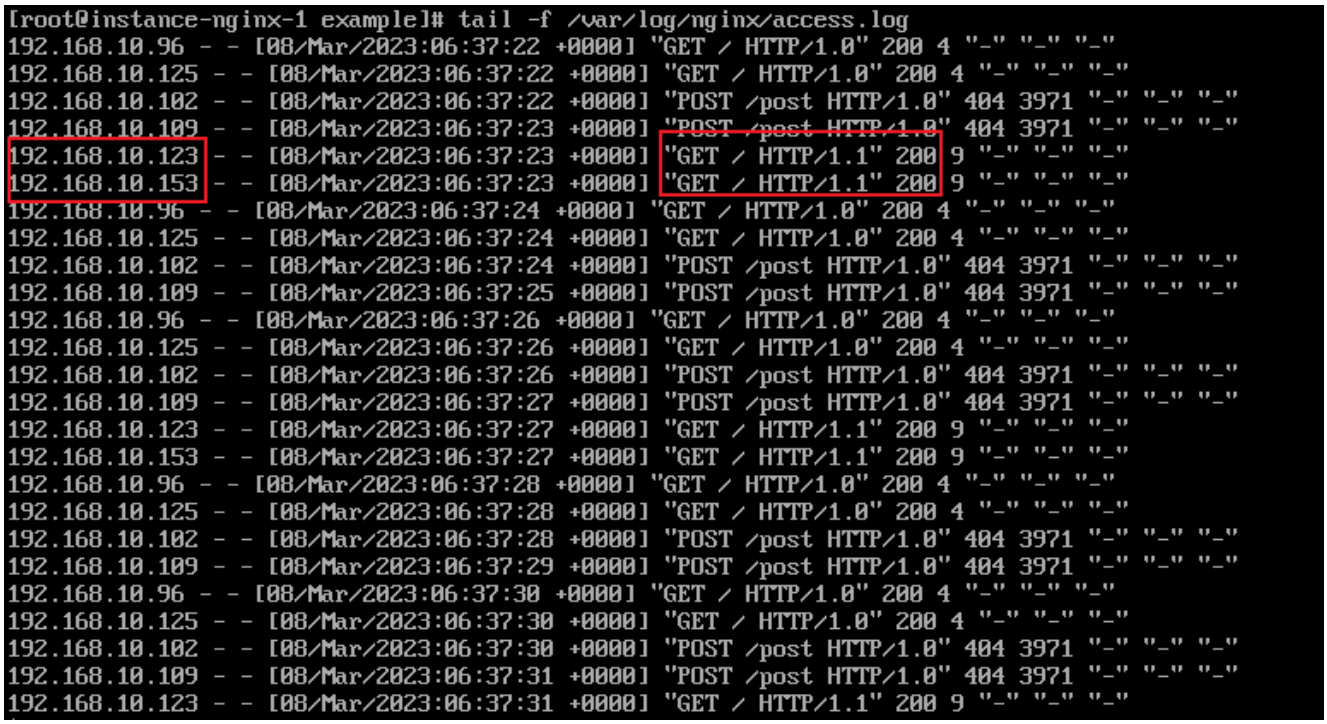
   2. 在“监听器配置”页面中，“协议”选择“HTTP”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“80”，其他参数默认，单击 `下一步：资源池配置` ，进入“资源池配置”页面。

3. 在“资源池配置”页面中，“资源池”保持默认选择“新创建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”默认选择“HTTP”，“负载方式”默认选择“轮询”，然后启用健康检查器。
4. 健康检查器配置：类型选择HTTP，HTTP协议版本选择HTTP 1.1，主机域名填写example.com，最大尝试次数、检测超时时间、检查间隔时间依次设置为2、3、4。
5. 待所有配置完成后，单击 `确认` ，完成操作。其中，各参数的具体说明，请参考 创建监听器。

5. 配置资源池资源。
   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[资源池]页签中，单击上述新建资源池的名称 ，进入其详情页面。
   2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。
   3. 在“添加云内资源”页面中，选择上述三台云主机后，单击 `下一步：资源配置` ，进入“资源配置”页面。
   4. 在“资源配置”页面中，填写端口号80、检查端口80、权重100，单击 `下一步：确认信息` ，进入“确认信息”页面。
   5. 在“确认信息”页面中，确认各资源的配置信息后，单击 `添加` ，完成操作。

结果验证

1. 通过vnc成功登录到后端云主机。查看其日志有HTTP 1.1的GET请求:



2. 在资源列表页查看三个后端云主机的检查状态为在线。

1.6 构建HTTP透明代理生效场景

背景描述

PROXY（代理协议）是一种 Internet 协议，代理协议激活后，客户端的IP地址会包含在发送到后端服务器的请求的头中，您可以在使用负载均衡时识别客户端的连接信息，但需要接收请求的服务端也支持代理协议，如nginx、apache 等，否则不能识别包头，导致无法成功建立连接。

前提条件

- 已完成 前置条件准备。
- 已创建两台规格相同的云主机，用于托管Web应用程序。

操作步骤

1. 配置Web应用程序。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[云主机]，进入“云主机”页面。
    2. 单击已创建的云主机所在行的VNC图标，访问其控制台并登录云主机。
    3. 安装并启动nginx服务器。具体命令如下:

```
yum install nginx
systemctl start nginx
```

    4. 修改nginx透明代理配置文件。具体配置如下:

```
server {
  listen  80 default_server proxy_protocol;
  server_name  _;
  root         /usr/share/nginx/html;
  # Load configuration files for the default server block.
  include /etc/nginx/default.d/*.conf;

  location / {
```

```
    }

    error_page 404 /404.html;
    location = /404.html {
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
```

}

5. 重启并确认nginx服务器启动成功。具体命令如下:

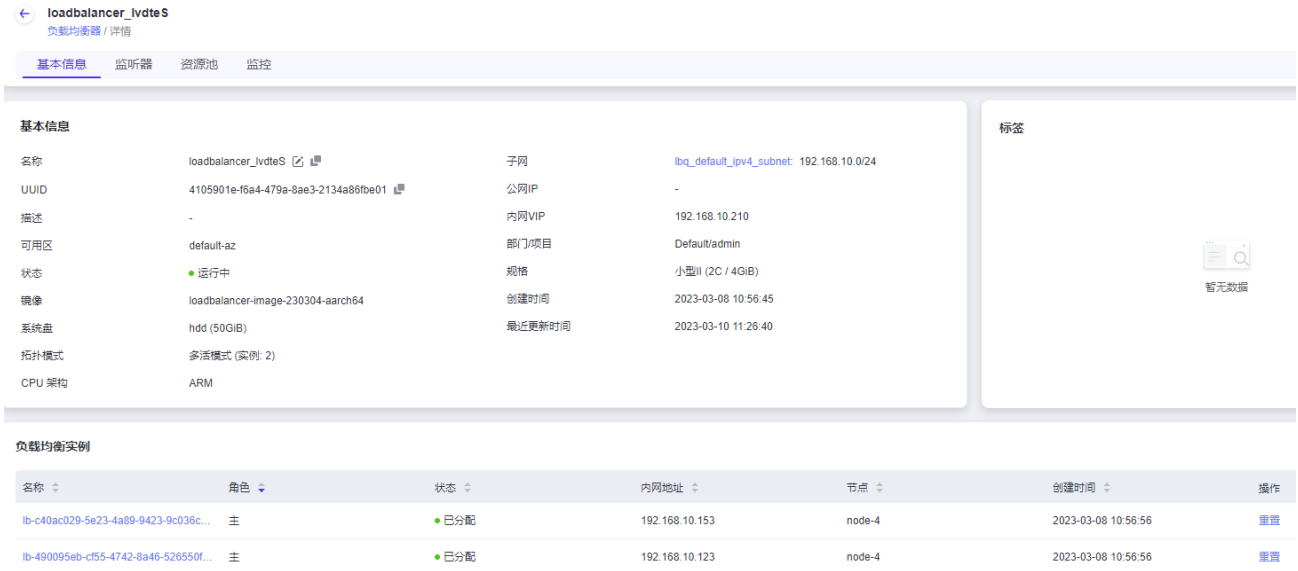
```
systemctl restart nginx; systemctl status nginx
```

6. 依次修改两台云主机的nginx index文件，方便对每台云主机进行标识。

```
echo "this is nginx-1{对应主机名,方便标识是哪个云主机}" >
/usr/share/nginx/html/index.html
```

2. 创建负载均衡器。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。
2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。
3. “子网”选择云主机所在子网，并配置其他参数后，单击 `创建` ，完成负载均衡器创建。其中，各参数的具体说明，请参考 创建负载均衡器。



3. 创建监听器和资源池。

   1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。

   2. 在“监听器配置”页面中，“协议”选择“HTTP”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“80”，并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。

   3. 在“资源池配置”页面中，“资源池”选择“新建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”选择“PROXY”，“负载方式”选择“轮询”。

   4. 激活健康检查器，类型选择HTTP，最大尝试次数、检测超时时间、检查间隔时间依次填写2、3、4，单击 `创建` ，完成监听器和默认资源池的创建。

4. 添加云内资源。

   具体配置步骤如下：

   1. 在上述负载均衡器详情页面的[资源池]页签中，单击待操作资源池的名称，进入其详情页面。

   2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。

   3. 在“添加云内资源”页面中，选择连接资源的子网，选择云内资源后，单击 `下一步：资源配置` ，进入“资源配置”页面。

   4. 在“资源配置”页面中，配置端口号80，权重100后，单击 `下一步：确认信息` ，进入“确认信息”页面。

5. 在“确认信息”页面中，确认各资源的配置信息后，单击 `添加` ，完成操作。

结果验证

1. 登录另一台跟DLB同子网的云主机（192.168.10.22），多次执行以下命令

curl vip:80（本例中vip为192.168.10.210）

```
[root@instance-nginx-3 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:74:33:55 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.22/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe74:3355/64 scope link
       valid_lft forever preferred_lft forever
[root@instance-nginx-3 ~]#
[root@instance-nginx-3 ~]# curl 192.168.10.210
nginx-1
[root@instance-nginx-3 ~]# curl 192.168.10.210
nginx-1
[root@instance-nginx-3 ~]# curl 192.168.10.210
nginx-2
```

2. 登录添加的云内资源，查看其access.log日志：

```
[root@instance-nginx-1 nginx]# tail -f access.log
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:03 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.22 - 192.168.10.123 - - [10/Mar/2023:03:27:03 +0000] "GET / HTTP/1.1" 200 8 "-" "curl/7.61.1" "-"
192.168.10.123 - 192.168.10.123 - - [10/Mar/2023:03:27:04 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:05 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.22 - 192.168.10.123 - - [10/Mar/2023:03:27:05 +0000] "GET / HTTP/1.1" 200 8 "-" "curl/7.61.1" "-"
192.168.10.123 - 192.168.10.123 - - [10/Mar/2023:03:27:06 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:07 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.123 - 192.168.10.123 - - [10/Mar/2023:03:27:08 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:09 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.123 - 192.168.10.123 - - [10/Mar/2023:03:27:10 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:11 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.123 - 192.168.10.123 - - [10/Mar/2023:03:27:12 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
192.168.10.153 - 192.168.10.153 - - [10/Mar/2023:03:27:13 +0000] "GET / HTTP/1.0" 200 8 "-" "-" "-"
```

1.7 利用HTTP重定向功能重定向到HTTPS服务

背景描述

根据现代Web安全标准和最佳实践，推荐所有网站使用HTTPS来保护用户隐私和数据安全。这也是许多网络安全标准和框架的要求。所以负载均衡器提供HTTP重定向功能，可以实现将对HTTP监听器的访问重定向至HTTPS监听器。确保数据在传输过程中是加密的，从而防止中间人攻击和窃听。这对于网站处理敏感信息（如登录凭据、支付信息等）至关重要。

前提条件

- 已完成 前置条件准备。
- 已申请一个 **Let's Encrypt** 证书。
- 已创建三台规格相同的云主机，用于托管Web应用程序。
- 已准备一个可供外部访问的公网IP地址。

操作步骤

1. 配置Web应用程序。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[云主机]，进入“云主机”页面。

    2. 单击各云主机所在行的VNC图标，访问其控制台并登录云主机。

    3. 安装并启动nginx服务器。具体命令如下:

    ```
    yum install nginx
    systemctl start nginx
    ```

    4. 确认nginx服务器启动成功。具体命令如下:

    ```
    systemctl status nginx
    ```

```
[root@qlq-16c16g-member01 ~]# systemctl status nginx
● nginx.service - nginx - high performance web server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-04-07 02:07:24 EDT; 5 days ago
     Docs: http://nginx.org/en/docs/
  Process: 22461 ExecStop=/bin/sh -c /bin/kill -s TERM $(/bin/cat /var/run/nginx.pid) (code=exited, status=0/SUCCESS)
  Process: 22466 ExecStart=/usr/sbin/nginx -c /etc/nginx/nginx.conf (code=exited, status=0/SUCCESS)
 Main PID: 22467 (nginx)
   CGroup: /system.slice/nginx.service
           ├─22467 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
           ├─22468 nginx: worker process
           ├─22469 nginx: worker process
           ├─22470 nginx: worker process
           ├─22471 nginx: worker process
           ├─22472 nginx: worker process
           ├─22473 nginx: worker process
           ├─22474 nginx: worker process
           ├─22475 nginx: worker process
           ├─22476 nginx: worker process
           ├─22477 nginx: worker process
           ├─22478 nginx: worker process
           ├─22479 nginx: worker process
           ├─22480 nginx: worker process
           ├─22481 nginx: worker process
           ├─22482 nginx: worker process
           └─22483 nginx: worker process

Apr 07 02:07:24 qlq-16c16g-member01.novalocal systemd[1]: Starting nginx - high performance web server...
Apr 07 02:07:24 qlq-16c16g-member01.novalocal systemd[1]: Started nginx - high performance web server.
```

5. 请参考下图，依次修改3台云主机的nginx index文件，方便对每台云主机进行标识。

```
[root@qlq-16c16g-member01 ~]# cat /usr/share/nginx/html/index.html
<!DOCTYPE html>
<html>
<head>
<title>Welcome to test2.example.cn member01!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to test2.example.cn member01!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
[root@qlq-16c16g-member01 ~]# _
```

2. 创建负载均衡器。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[独享型负载均衡]，进入“独享型负载均衡”页面。
2. 单击 `创建负载均衡器` ，弹出“创建负载均衡器”对话框。
3. “子网”选择云主机所在子网，并配置其他参数后，单击 `创建` ，完成负载均衡器创建。其中，各参数的具体说明，请参考 创建负载均衡器。
4. 绑定公网IP。
    1. 在“独享型负载均衡”页面中，勾选上述负载均衡器后，单击 `绑定公网IP` ，弹出“绑定公网IP”对话框。
    2. 配置参数后，单击 `绑定` ，完成操作。

3. 创建监听器和资源池。

    由于在本实践方案中，将采用配置HTTP重定向到HTTPS的方式，对请求进行重定向访问。

    1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[监听器]页签中，单击 `创建监听器` ，进入“创建监听器”的“监听器配置”页面。
    2. 在“监听器配置”页面中，“协议”选择“HTTPS”，“VIP”任选一个负载均衡器的VIP地址，“协议端口”输入“443”，选择证书（如何托管证书，参考证书管理服务说明文档。）并配置其他参数后，单击 `下一步：资源池配置` ，进入“资源池配置”页面。
    3. 在“资源池配置”页面中，“资源池”选择“新建”，“IP类型”选择符合监听器VIP要求的IP类型（如“IPv4”或“IPv6”），“协议”选择“HTTP”，“负载方式”选择“轮询”，并配置其他参数后，单击 `确认` ，完成监听器和默认资源池的创建。
    4. 重新回到此负载均衡器详情页面，单击 `创建监听器` ，在“监听器配置”页面中，“协议”选择“HTTP”，“协议端口”输入“80”，开启“重定向”，选择步骤2中创建的HTTPS监听器，并配置其他参数后，单击 `确认` ，完成监听器的创建。

4. 配置资源池资源。

    1. 在“独享型负载均衡”页面中，单击上述负载均衡器名称，进入其详情页面。在该详情页面的[资源池]页签中，单击上述新建资源池的名称 ，进入其详情页面。
    2. 在“资源列表”区域框中，单击 `添加云内资源` ，弹出“添加云内资源”对话框。
    3. 在“添加云内资源”页面中，选择上述三台云主机后，单击 `下一步：资源配置` ，进入“资源配置”页面。

4. 在“资源配置”页面中，配置参数后，单击 `下一步：确认信息` ，进入“确认信息”页面。

5. 在“确认信息”页面中，确认各资源的配置信息后，单击 `添加` ，完成操作。

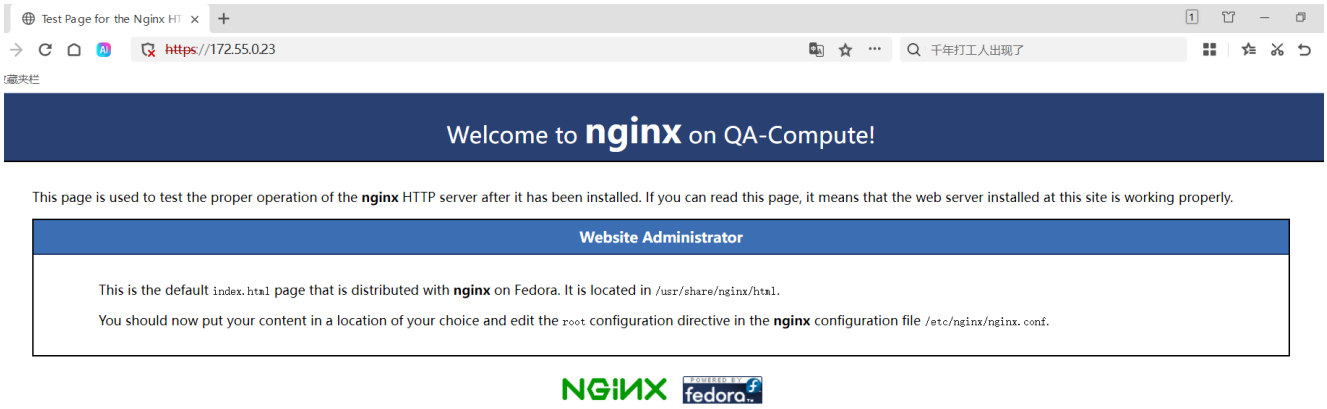
5. 绑定公网IP。

1. 在“独享型负载均衡”页面中，勾选上述负载均衡器后，单击 `绑定公网IP` ，弹出“绑定公网IP”对话框。

2. 配置参数后，单击 `绑定` ，完成操作。

结果验证

- 通过浏览器访问http://<公网IP地址>，确认可以自动跳转到https://<公网IP地址>，并正常进入到Nginx服务器页面中。



- 通过远程客户端多次访问http://<公网IP地址>，确认http状态码返回301并重定向至443端口，并成功访问到Nginx服务器。

```
[root@test ~]# curl http://172.55.0.23 -k  -L -v
* About to connect() to 172.55.0.23 port 80 (#0)
*   Trying 172.55.0.23...
* Connected to 172.55.0.23 (172.55.0.23) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 172.55.0.23
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< content-length: 0
< location: https://172.55.0.23:443/
<
* Connection #0 to host 172.55.0.23 left intact
* Issue another request to this URL: 'https://172.55.0.23:443/'
* Found bundle for host 172.55.0.23: 0x3da03fe0
* About to connect() to 172.55.0.23 port 443 (#1)
*   Trying 172.55.0.23...
* Connected to 172.55.0.23 (172.55.0.23) port 443 (#1)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate:
*       subject: CN=123,OU=312,O=12,L=beijing,ST=beijing,C=CN
*       start date: Sep 10 11:44:40 2024 GMT
*       expire date: Sep 09 11:44:40 2027 GMT
*       common name: 123
*       issuer: CN=fxj,OU=321,O=321,L=beijing,ST=beijing,C=CN
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 172.55.0.23
> Accept: */*
>
< HTTP/1.1 200 OK
< server: nginx/1.12.2
< date: Tue, 10 Sep 2024 12:37:59 GMT
< content-type: text/html
```

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区23号楼华胜天成科研大楼一层东侧120-123
南京分公司：
江苏省南京市雨花台区软件大道168号润和创智中心B栋一楼西101
上海office：
上海黄浦区西藏中路336号华旭大厦22楼2204
成都分公司：
成都市高新区天府五街168号德必天府五街WE602

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)
training@easystack.cn (培训咨询)
hr@easystack.cn (招聘咨询)