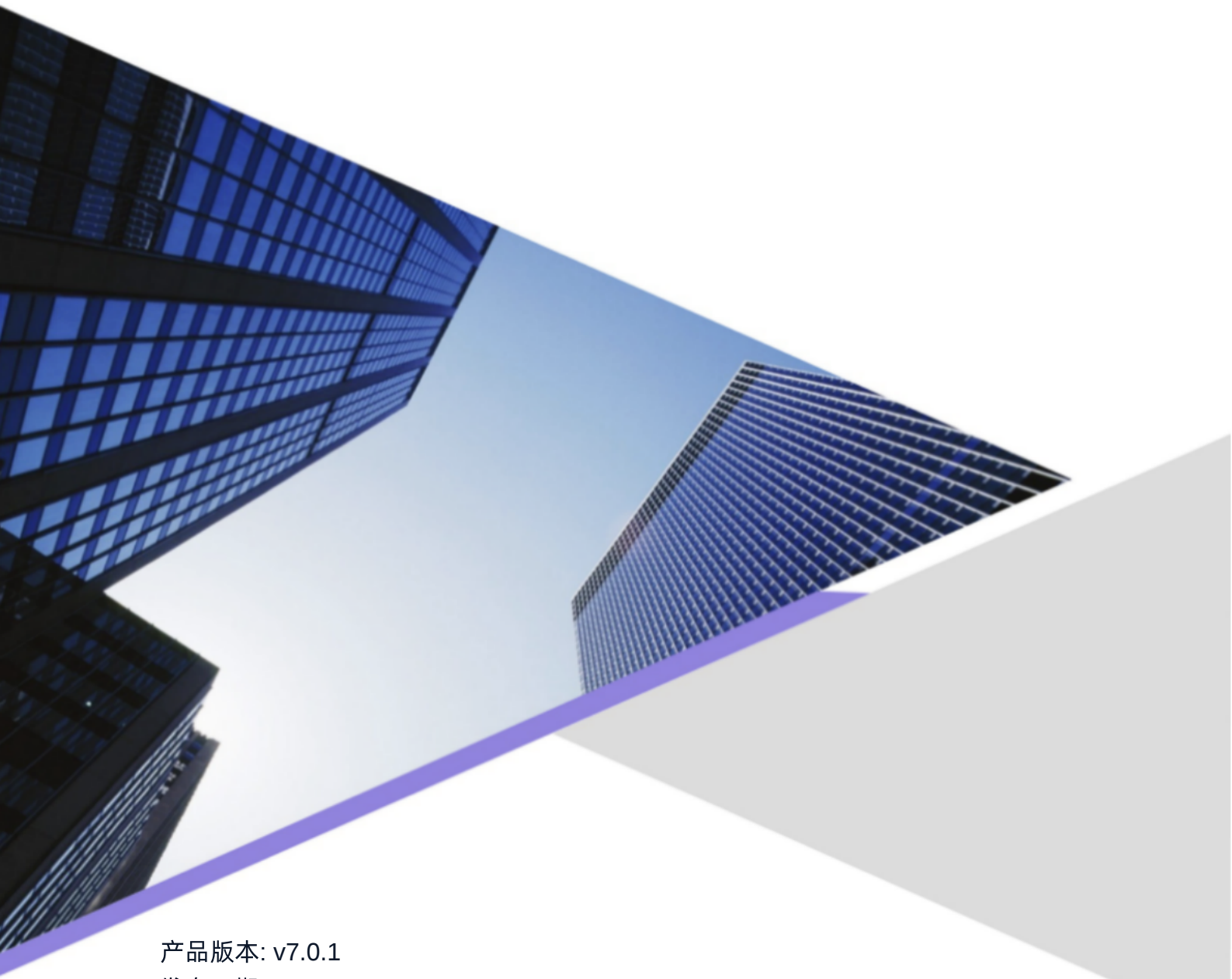
EasyStack
易捷行云

SDN网络服务

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 通过Keepalived与虚拟IP结合配置云主机网络高可用

背景描述

通过为多个云主机的多个虚拟网卡配置同一虚拟IP（VIP），可以自定义其作为高可用服务的可漂移网络入口，保障业务应用的高可用性。典型的应用场景是将此虚拟IP与Keepalived相结合使用。

本文将以在两个CentOS 7云主机中配置Keepalived虚拟IP为例，详细介绍如何在该云平台中配置Keepalived与虚拟IP结合使用，以保障业务连续性。

前提条件

- 已参考“计算”帮助中“云主机”的相关内容，完成两个CentOS 7云主机的创建。

操作步骤

1. 分别为各云主机的虚拟网卡配置同一虚拟IP。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[虚拟网卡]，进入“虚拟网卡”页面。
    2. 勾选待操作虚拟网卡后，`更多` - `管理虚拟IP` ，弹出“管理虚拟IP”对话框。
    3. 如果虚拟IP不存在，则点击 `创建虚拟IP` 完成虚拟IP的创建，如果虚拟IP已存在，直接选择即可。
2. 在各云主机中安装Keepalived。
    1. 下载keepalived的rpm安装包。具体命令如下::

```
wget
http://www.rpmfind.net/linux/centos/7.6.1810/os/x86_64/Packages/keepalive
d-1.3.5-6.el7.x86_64.rpm
```

2. 配置EPEL源。

   通过yum命令，配置EPEL源。具体命令如下::

```
yum -y
install http://dl.fedoraproject.org/pub/epel/7Server/x86_64/e/epel-
release-7-8.noarch.rpm
```

3. 安装keepalived的rpm安装包。具体命令如下::

```
yum localinstall keepalived-1.3.5-6.el7.x86_64.rpm -y
```

3. 配置各云主机的Keepalived。

   1. 通过VIM编辑器，打开并编辑各云主机的Keepalived配置文件（即/etc/keepalived/keepalived.conf文件）。

      Master云主机Instance A（**node 1**）的配置示例::

```
global_defs {
     router_id rt1
}
vrrp_instance VI_1 {
     state MASTER
     interface eth0
     unicast_peer {
         $node2   #Fixed IP for Instance B.
     }
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
         auth_type PASS
         auth_pass 1234
    }
    virtual_ipaddress {
         $vip dev eth0    #Use the VIP address you configured.
    }
 }
```

Backup云主机Instance B（**node 2**）的配置示例::

```
global_defs {
     router_id rt1
}
vrrp_instance VI_1 {
     state BACKUP
     interface eth0
     unicast_peer {
         $node1   #Fixed IP for Instance A.
     }
    virtual_router_id 51
    priority 80
    advert_int 1
    authentication {
         auth_type PASS
         auth_pass 1234
    }
    virtual_ipaddress {
         $vip dev eth0    #Use the VIP address you configured.
    }
 }
```

2. 启动Keepalived服务。具体命令如下::

```
service keepalived start
```

结果验证

1. 在Master云主机（**node 1**）中，查询其IP信息，确认虚拟IP已配置成功。查询IP信息的具体命令如下::

```
ip a
```

2. 停止Master云主机（**node 1**）的Keepalived服务。具体命令如下::

```
service keepalived stop
```

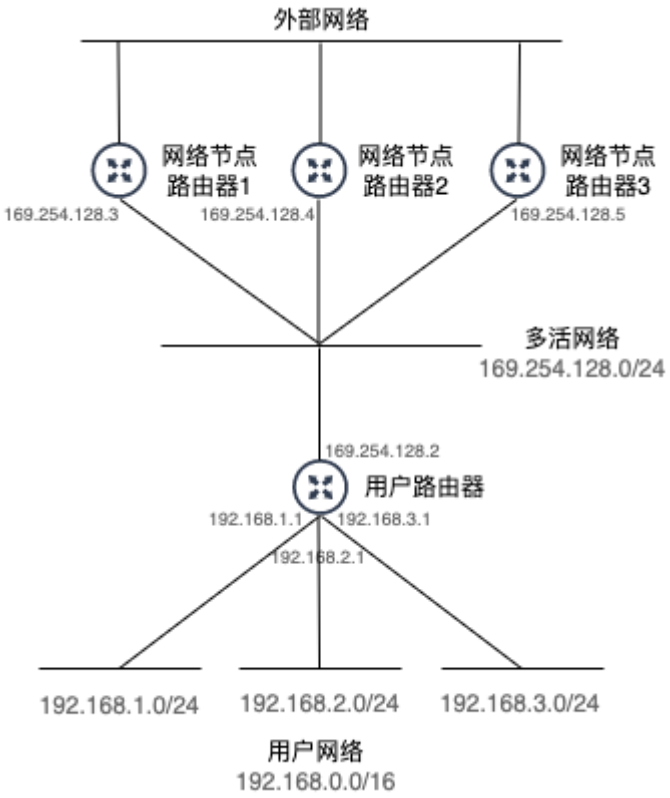
3. 查询Master云主机（**node 1**）和Backup云主机（**node 2**）的IP信息，确认虚拟IP成功漂移到Backup云主机（**node 2**）上。

1.2 配置多活网络方案(IPv4)

背景描述

通过配置多活网络，可以横向提升网络性能，保障业务应用的高性能访问。本文将以配置三个网络节点路由器为例，介绍如何在该云平台中配置多活网络方案，以提升业务的网络性能。

> 说明：
> 多活网络方案仅支持纯路由模式的路由器，即此方案中使用的用户路由器不支持公网IP和SNAT功能。



本实践方案中，具体网络规划信息如下：

类型	说明

类型	说明
用户网络	* 名称：user_network * 网络类型：内部网络 * 网络模式：Geneve * 子网1： - 名称：user_network_default_ipv4_subnet - 网段：192.168.1.0/24 - 网关地址：设置网关（192.168.1.1） - DHCP服务：开启 * 子网2： - 名称：user_network_default_ipv4_subnet2 - 网段：192.168.2.0/24 - 网关地址：设置网关（192.168.2.1） - DHCP服务：开启 * 子网3： - 名称：user_network_default_ipv4_subnet3 - 网段：192.168.3.0/24 - 网关地址：设置网关（192.168.3.1） - DHCP服务：开启
多活网络	* 名称：multi_net_169_254_128 * 网络类型：内部网络 * 网络模式：Geneve * 子网： - 名称：multi_net_169_254_128_default_ipv4_subnet - 网段：169.254.128.0/24 - 网关地址：不设置 - DHCP服务：关闭

类型	说明
用户路由器	* 名称：user_router * 路由器连接： - 子网：multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24；子网IP：169.254.128.2 - 子网：user_network_default_ipv4_subnet:192.168.1.0/24；子网IP：192.168.1.1 - 子网：user_network_default_ipv4_subnet2:192.168.2.0/24；子网IP：192.168.2.1 - 子网：user_network_default_ipv4_subnet3:192.168.3.0/24；子网IP：192.168.3.1 * 静态路由： - 目的CIDR：0.0.0.0/0；下一跳：169.254.128.3 - 目的CIDR：0.0.0.0/0；下一跳：169.254.128.4 - 目的CIDR：0.0.0.0/0；下一跳：169.254.128.5
网络节点路由器1	* 名称：multi_ex_router_lb_1 * 可用区：与网络节点的可用区一致 * 路由器网关：172.16.10.3（不开启SNAT） * 路由器连接： - 子网：multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24；子网IP：169.254.128.3 * 静态路由： - 目的CIDR：192.168.0.0/16；下一跳：169.254.128.2
网络节点路由器2	* 名称：multi_ex_router_lb_2 * 可用区：与网络节点的可用区一致 * 路由器网关：172.16.10.4 （不开启SNAT） * 路由器连接： - 子网：multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24；子网IP：169.254.128.4 * 静态路由： - 目的CIDR：192.168.0.0/16；下一跳：169.254.128.2

类型	说明
网络节点路由器3	* 名称：multi_ex_router_lb_3 * 可用区：与网络节点的可用区一致 * 路由器网关：172.16.10.5 （不开启SNAT） * 路由器连接： - 子网：multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24；子网IP：169.254.128.5 * 静态路由： - 目的CIDR：192.168.0.0/16；下一跳：169.254.128.2

操作步骤

1. 创建用户网络和多活网络。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户网络和多活网络。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
   2. 单击 `创建网络` ，进入“创建网络”页面。
   3. 配置参数后，单击 `创建网络` ，完成操作。其中，各参数的具体说明，请参考 创建二层基础网络。

2. 创建用户路由器和网络节点路由器。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器和网络节点路由器。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
   2. 单击 `创建路由器` ，弹出“创建路由器”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，各参数的具体说明，请参考 创建路由器。

3. 设置网络节点路由器的网关。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置各网络节点路由器的网关。

1. 在“路由器”页面中，勾选待操作的网络节点路由器后，单击 `更多` - `设置网关` ，弹出“设置路由器网关”对话框。
2. 配置参数后，单击 `设置` ，完成操作。其中，各参数的具体说明，请参考 设置路由器网关。

4. 设置用户路由器和网络节点路由器的子网连接。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的子网连接。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

5. 设置用户路由器和网络节点路由器的静态路由。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的静态路由。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[静态路由]页签中，单击 `添加静态路由` ，弹出“添加静态路由”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

6. 设置外网网关的ECMP静态路由。

   请在外部网关处，设置从外网网关回内网的静态路由。以Linux服务器网关为例，说明本实践方案中的静态路由配置命令::

```
  ip route add 192.168.1.0/24 nexthop via 172.16.10.3 weight 1 nexthop via
172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
  ip route add 192.168.2.0/24 nexthop via 172.16.10.3 weight 1 nexthop via
172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
  ip route add 192.168.3.0/24 nexthop via 172.16.10.3 weight 1 nexthop via
172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
```

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

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

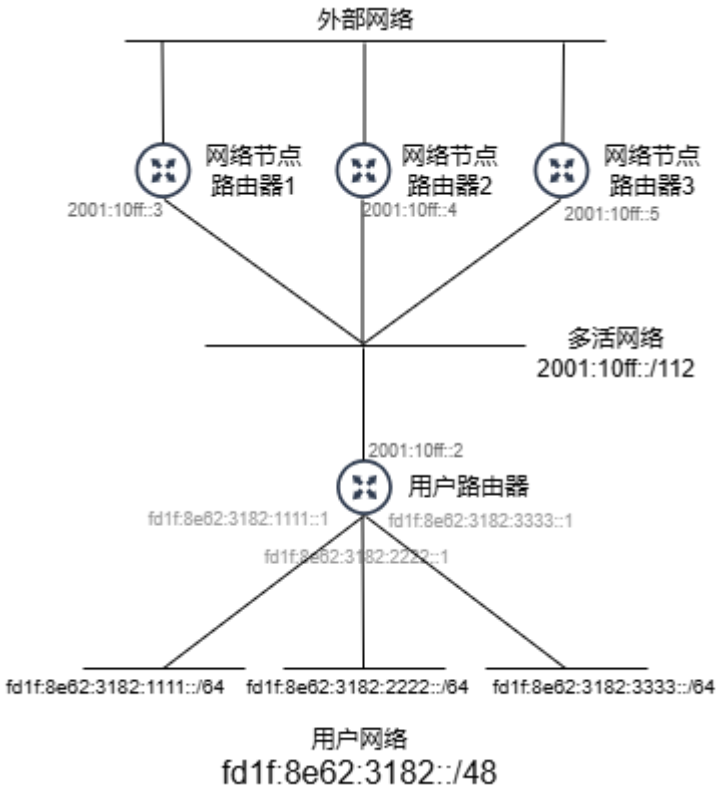
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.3 配置多活网络方案(IPv6)

背景描述

通过配置多活网络，可以横向提升网络性能，保障业务应用的高性能访问。本文将以配置三个网络节点路由器为例，介绍如何在该云平台中配置多活网络方案，以提升业务的网络性能。

> 说明：
> 多活网络方案仅支持纯路由模式的路由器，即此方案中使用的用户路由器不支持SNAT功能。



本实践方案中，具体网络规划信息如下：

类型	说明

类型	说明
用户网络	* 名称：user_network * 网络类型：内部网络 * 网络模式：Geneve * 子网1： - 名称：user_network_default_ipv6_subnet - 网段：fd1f:8e62:3182:1111::/64 - 网关地址：设置网关（fd1f:8e62:3182:1111::1） - DHCP服务：开启 * 子网2： - 名称：user_network_default_ipv6_subnet2 - 网段：fd1f:8e62:3182:2222::/64 - 网关地址：设置网关（fd1f:8e62:3182:2222::1） - DHCP服务：开启 * 子网3： - 名称：user_network_default_ipv6_subnet3 - 网段：fd1f:8e62:3182:3333::/64 - 网关地址：设置网关（fd1f:8e62:3182:3333::1） - DHCP服务：开启
多活网络	* 名称：multi_net_ipv6 * 网络类型：内部网络 * 网络模式：Geneve * 子网： - 名称：multi_net_ipv6_default_ipv6_subnet - 网段：2001:10ff::/112 - 网关地址：不设置 - DHCP服务：关闭

类型	说明
用户路由器	* 名称：user_router * 路由器连接： - 子网：multi_net_ipv6_default_ipv6_subnet： 2001:10ff::/112；子网IP：2001:10ff::2 - 子网：user_network_default_ipv6_subnet： fd1f:8e62:3182:1111::/64；子网IP：fd1f:8e62:3182:1111::1 - 子网：user_network_default_ipv6_subnet2： fd1f:8e62:3182:2222::/64；子网IP：fd1f:8e62:3182:2222::1 - 子网：user_network_default_ipv6_subnet3： fd1f:8e62:3182:3333::/64；子网IP：fd1f:8e62:3182:3333::1 * 静态路由： - 目的CIDR：::/0；下一跳：2001:10ff::3 - 目的CIDR：::/0；下一跳：2001:10ff::4 - 目的CIDR：::/0；下一跳：2001:10ff::5
网络节点路由器1	* 名称：multi_ex_router_lb_1 * 可用区：与网络节点的可用区一致 * 路由器网关：2400::3（不开启SNAT） * 路由器连接： - 子网：multi_net_ipv6_default_ipv6_subnet:2001:10ff::/112；子网IP：2001:10ff::3 * 静态路由： - 目的CIDR：fd1f:8e62:3182::/48；下一跳：2001:10ff::2
网络节点路由器2	* 名称：multi_ex_router_lb_2 * 可用区：与网络节点的可用区一致 * 路由器网关：2400::4 （不开启SNAT） * 路由器连接： - 子网：multi_net_ipv6_default_ipv6_subnet:2001:10ff::/112；子网IP：2001:10ff::4 * 静态路由： - 目的CIDR：fd1f:8e62:3182::/48；下一跳：2001:10ff::2

类型	说明
网络节点路由器3	* 名称：multi_ex_router_lb_3 * 可用区：与网络节点的可用区一致 * 路由器网关：2400::5 （不开启SNAT） * 路由器连接： - 子网：multi_net_ipv6_default_ipv6_subnet:2001:10ff::/112；子网IP：2001:10ff::5 * 静态路由： - 目的CIDR：fd1f:8e62:3182::/48；下一跳：2001:10ff::2

操作步骤

1. 创建用户网络和多活网络。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户网络和多活网络。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
   2. 单击 `创建网络` ，进入“创建网络”页面。
   3. 配置参数后，单击 `创建网络` ，完成操作。其中，各参数的具体说明，请参考 创建二层基础网络。

2. 创建用户路由器和网络节点路由器。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器和网络节点路由器。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
   2. 单击 `创建路由器` ，弹出“创建路由器”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，各参数的具体说明，请参考 创建路由器。

3. 设置网络节点路由器的网关。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置各网络节点路由器的网关。

1. 在“路由器”页面中，勾选待操作的网络节点路由器后，单击 `更多` - `设置网关` ，弹出“设置路由器网关”对话框。
2. 配置参数后，单击 `设置` ，完成操作。其中，各参数的具体说明，请参考 设置路由器网关。

4. 设置用户路由器和网络节点路由器的子网连接。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的子网连接。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

5. 设置用户路由器和网络节点路由器的静态路由。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的静态路由。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[静态路由]页签中，单击 `添加静态路由` ，弹出“添加静态路由”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

6. 设置外网网关的ECMP静态路由。

   请在外部网关处，设置从外网网关回内网的静态路由。以Linux服务器网关为例，说明本实践方案中的静态路由配置命令:

```
  ip -6 r add fd1f:8e62:3182:1111::/64 nexthop via 2400::3 weight 1 nexthop
via 2400::4 weight 1 nexthop via 2400::5 weight 1
  ip -6 r add fd1f:8e62:3182:2222::/64 nexthop via 2400::3 weight 1 nexthop
via 2400::4 weight 1 nexthop via 2400::5 weight 1
  ip -6 r add fd1f:8e62:3182:3333::/64 nexthop via 2400::3 weight 1 nexthop
via 2400::4 weight 1 nexthop via 2400::5 weight 1
```

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

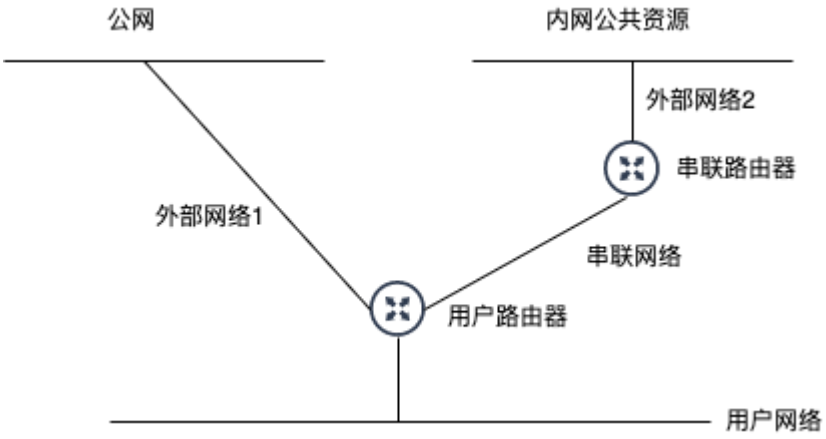
1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。

2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.4 配置路由器连接多个外网

背景描述

通过配置路由器连接多个外部网络，可以实现云主机、容器或裸金属主机等计算资源访问安全隔离的多个网络环境，保障业务应用的安全可靠访问。本文将以配置一个用户路由器连接两个外部网络（一个用于连接公网，一个用于连接内网公共资源）为例，介绍如何在该云平台中配置路由器连接多个外部网络，以提升业务的高可靠性。



本实践方案中，具体网络规划信息如下：

类型	配置	说明
用户网络	* 名称：user_network * 网络类型：内部网络 * 网络模式：Geneve * 子网： - 名称：user_network_default_ipv4_subnet - 网段：10.0.0.0/24 - 网关地址：设置网关（10.0.0.1） - DHCP服务：开启	用于建立用户路由器与用户的云主机、容器或裸金属主机等计算资源之间的连接。

类型	配置	说明
外部网络1	* 名称：ex_net_1 * 网络类型：外部网络 * 网络模式：VLAN * 子网： - 名称：ex_net_1_default_ipv4_subnet - 网段：172.17.0.0/24 - 网关地址：设置网关（172.17.0.1）	用于建立用户路由器与公网之间的连接。
外部网络2	* 名称：ex_net_2 * 网络类型：外部网络 * 网络模式：VLAN * 子网： - 名称：ex_net_2_default_ipv4_subnet - 网段：172.16.0.0/24 - 网关地址：设置网关（172.16.0.1）	用于建立串联路由器与内网公共资源（如对象存储、公共rpm源等）之间的连接。
串联网络	* 名称：series_network * 网络类型：内部网络 * 网络模式：Geneve * 子网： - 名称：series_network_default_ipv4_subnet - 网段：169.254.128.0/24 - 网关地址：不设置 - DHCP服务：关闭	用于建立用户路由器与串联路由器之间的连接。
用户路由器	* 名称：user_router * 路由器网关：172.17.0.10（开启SNAT） * 路由器连接： - 子网：user_network_default_ipv4_subnet:10.0.0.0/24；子网IP：10.0.0.1 - 子网：series_network_default_ipv4_subnet:169.254.128.0/24；子网IP：169.254.128.2 * 静态路由： - 目的CIDR：172.16.0.0/24；下一跳：169.254.128.3	用于建立用户网络、公网与内网公共资源之间的连接。

类型	配置	说明
串联路由器	* 名称：series_router * 可用区：如需保证两个外部网络的访问物理隔离，请指定单独的可用区，并确保该可用区已配置独立的网络节点。 * 路由器网关：172.16.0.10（开启SNAT） * 路由器连接： - 子网：series_network_default_ipv4_subnet: 169.254.128.0/24；子网IP：169.254.128.3 * 静态路由： - 目的CIDR：10.0.0.0/24；下一跳：169.254.128.2	用于建立用户网络与内网公共资源（如对象存储、公共rpm源等）之间的连接。

操作步骤

1. 创建用户网络、外部网络和串联网络。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户网络、外部网络1、外部网络2和串联网络。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
   2. 单击 `创建网络` ，进入“创建网络”页面。
   3. 配置参数后，单击 `创建网络` ，完成操作。其中，各参数的具体说明，请参考 创建二层基础网络。

2. 创建用户路由器和串联路由器。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器和串联路由器。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
   2. 单击 `创建路由器` ，弹出“创建路由器”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，各参数的具体说明，请参考 创建路由器。

3. 设置串联路由器的网关。

请依据本实践方案中的网络规划信息，参考以下操作步骤，设置串联路由器的网关。

1. 在“路由器”页面中，勾选待操作的网络节点路由器后，单击 `更多` - `设置网关` ，弹出“设置路由器网关”对话框。
2. 配置参数后，单击 `设置` ，完成操作。其中，各参数的具体说明，请参考 设置路由器网关。

4. 设置用户路由器和串联路由器的子网连接。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和串联路由器的子网连接。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

5. 设置用户路由器的静态路由。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，设置用户路由器的静态路由。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[静态路由]页签中，单击 `添加静态路由` ，弹出“添加静态路由”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

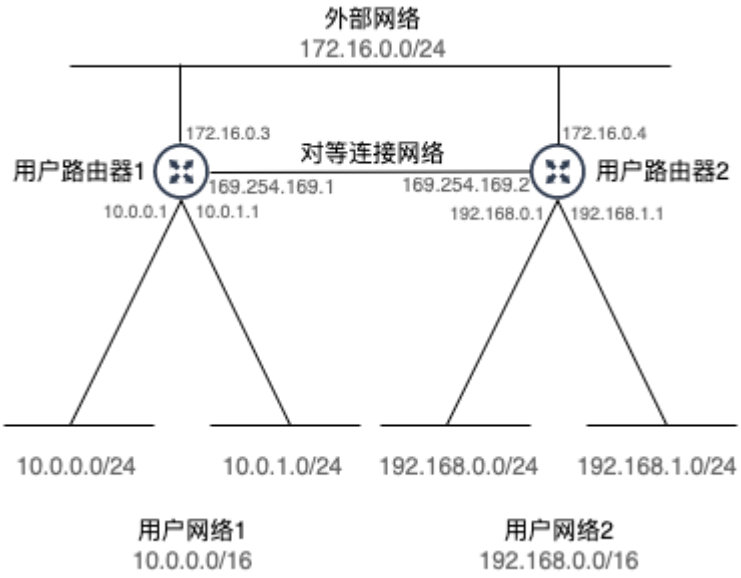
1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.5 配置云内对等连接

背景描述

通过配置用户内部网络中多个路由器之间的对等连接，可以实现云内路由器下各子网之间的三层网络互通。本文将以配置两个用户路由器的对等连接为例，介绍如何在该云平台中配置内部网络的对等连接，实现云内三层网络互通。

> 警告：
> 在配置多个用户路由器之间的云内对等连接时，请确保各路由器的子网不发生冲突。



本实践方案中，具体网络规划信息如下（其中，用户网络与外部网络假定已完成相关配置，具体信息如上图所示，下表仅展示需另添加的信息）：

类型	配置	说明

类型	配置	说明
对等连接网络	* 名称：peer_network * 网络类型：内部网络 * 网络模式：Geneve * 子网： - 名称：peer_network_default_ipv4_subnet - 网段：169.254.169.0/29 - 网关地址：不设置 - DHCP服务：关闭	用于建立两个用户路由器之间的对等连接。
用户路由器1	* 名称：user_router_1 * 路由器连接： - 子网：peer_network_default_ipv4_subnet:169.254.169.0/29；子网IP：169.254.169.1 * 静态路由： - 目的CIDR：192.168.0.0/16；下一跳：169.254.169.2	用于建立用户网络、外部网络与其他内部网络之间的连接。
用户路由器2	* 名称：user_router_2 * 路由器连接： - 子网：peer_network_default_ipv4_subnet:169.254.169.0/29；子网IP：169.254.169.2 * 静态路由： - 目的CIDR：10.0.0.0/16；下一跳：169.254.169.1	用于建立用户网络、外部网络与其他内部网络之间的连接。

操作步骤

1. 创建对等连接网络。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，创建对等连接网络。

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

   2. 单击 `创建网络` ，进入“创建网络”页面。

3. 配置参数后，单击 `创建网络` ，完成操作。其中，各参数的具体说明，请参考 创建二层基础网络。

2. 创建用户路由器。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器1和用户路由器2。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
   2. 单击 `创建路由器` ，弹出“创建路由器”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，各参数的具体说明，请参考 创建路由器。

3. 设置用户路由器的子网连接。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器1和用户路由器2的子网连接。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

4. 设置用户路由器的静态路由。

   请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器1和用户路由器2的静态路由。

   1. 在“路由器”页面中，单击待操作路由器的名称 ，进入其详情页面。
   2. 在[静态路由]页签中，单击 `添加静态路由` ，弹出“添加静态路由”对话框。
   3. 配置参数后，单击 `连接` ，完成操作。

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

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

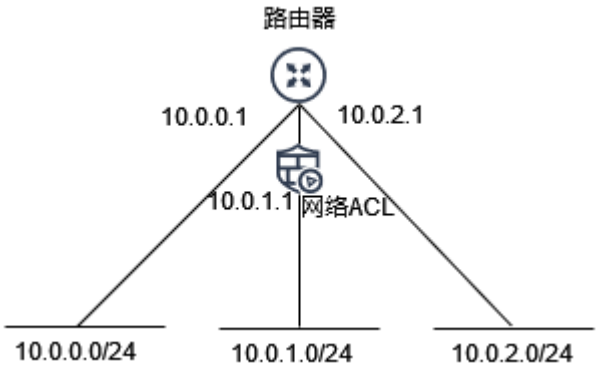
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.6 同VPC下限制子网间互访

背景描述

在VPC没有绑定网络ACL情况下，VPC内子网可以互通。通过配置网络ACL限制同VPC下子网间流量。

如图所示拓扑，VPC内网段 `10.0.1.0/24` 禁止与除 `10.0.0.0/24` 外的其它网段互通。



本实践方案通过配置网络ACL完成上述需求。

前提条件

路由器绑定了上述网段子网，子网间的云主机可以互通。

操作步骤

1. 创建网络ACL。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网络ACL]，进入“网络ACL列表”页面。
    2. 单击 `创建网络ACL` ，弹出“创建网络ACL”对话框。
    3. 配置参数后，单击 `创建` ，完成操作。

参数	说明

参数	说明
名称	网络ACL的名称。
描述	网络ACL的描述。

2. 配置网络ACL出入方向规则。

   1. 在网络ACL的详情页面，单击 `入方向规则` - `添加规则` ，出现规则编辑框。

   2. 添加如下规则，单击 `确认` ，完成操作。

方向	类型	策略	协议	源地址
入方向	ipv4	允许	全部	10.0.0.0/24

> 说明：网络ACL规则是无状态的，所以配置了一个方向的允许策略，还需要配置回复方向的允许策略，才能达到流量放行的需求。

   3. 单击 `出方向规则` - `添加规则` ，出现规则编辑框。

   4. 配置如下规则，单击 `确认` ，完成操作。

方向	类型	策略	协议	源地址
出方向	ipv4	允许	全部	0.0.0.0/0

3. 关联子网。

   1. 点击已经创建的网络ACL，进入该网络ACL的详情页面，单击 `关联子网` - `关联` ，弹出“关联子网”对话框。

   2. 选择上述网段为 `10.0.1.0/24` 的子网，点击 `关联` 。

> 说明：关联子网后，网络ACL默认拒绝所有出入子网网关的流量，直至添加放通规则。

结果验证

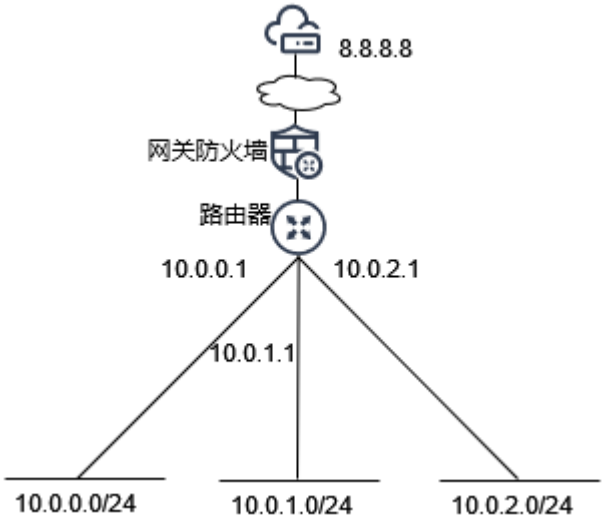
进入网段 `10.0.0.0/24` 的云主机，能正常访问网段 `10.0.1.0/24` 的云主机； 进入网段 `10.0.2.0/24` 的云主机，无法访问网段 `10.0.1.0/24` 的云主机。

1.7 限制VPC的出口流量

背景描述

在VPC没有绑定网关防火墙的情况下，VPC内云主机访问外网没有限制。通过配置网关防火墙可以限制VPC下的出口流量。

如图所示拓扑，禁止VPC内所有云主机访问外网，放行所有云主机访问外网 `8.8.8.8` 的主机。



本实践方案通过配置网关防火墙完成上述需求。

前提条件

路由器绑定了外部网关，以及云主机所在的子网，并且云主机可以访问外网。

操作步骤

1. 创建网关防火墙。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网关防火墙]，进入“网关防火墙”页面。
    2. 单击 `创建网关防火墙` ，弹出“创建网关防火墙”对话框。
    3. 配置参数后，单击 `创建` ，完成操作。

参数	说明
名称	网关防火墙的名称。
描述	网关防火墙的描述。

2. 配置网关防火墙出方向规则。

   1. 单击 `出方向规则` - `添加规则` ，出现规则编辑框。
   2. 配置如下规则，单击 `确认` ，完成操作。

   > 说明：网关防火墙规则是带状态的，所以只需要配置一个方向的允许策略，回复报文也会被允许通过。

方向	类型	策略	协议	源地址	源
出方向	ipv4	允许	全部	0.0.0.0/0	全

3. 关联路由器。

   1. 点击已经创建的网关防火墙，进入该网关防火墙的详情页面，单击 `关联路由器` - `关联` ，弹出“关联路由器”对话框。
   2. 选择上述路由器，点击 `关联` 。

   > 说明：关联路由器后，网关防火墙默认拒绝所有出入路由器网关的流量，直至添加放通规则。

结果验证

进入VPC内任意一台云主机， `ping` 访问 `114.114.114.114` 失败，能正常访问 `8.8.8.8` 。

1.8 同VPC下云主机间通过配置无状态安全组实现SSH

背景描述

安全组默认是有状态的，我们在一些场景可以使用无状态安全组，本实践方案通过配置无状态安全组完成云主机A和云主机B互相SSH。

> 说明：无状态安全组的典型使用场景包括
> - 无状态安全组性能比有状态性能好，在裸金属场景下，如果对网络性能有要求，考虑使用无状态安全组。
> - 在LVS负载均衡的DR模式下，云主机的虚拟网卡需要使用无状态安全组。

操作步骤

1. 创建无状态安全组。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[安全组]，进入“安全组列表”页面。
    2. 单击 `创建安全组` ，弹出“创建安全组”对话框。
    3. 选择状态为 `否` ，配置完参数后，单击 `创建` ，完成操作。

参数	说明
名称	安全组的名称。
描述	安全组的描述。
状态	安全组是否带状态。

> 说明：创建完无状态安全组后，默认会创建一条入方向放行metadata流量的规则，以及出方向放行 `0.0.0.0/0` 的规则。除非入向全部放开，无状态安全组无法做到云主机访问任意公网，因为回复包无

> 法添加入向的具体规则，包括源IP，目的端口都无法确定。

方向	类型	协议和端口	源地址
入方向	ipv4	TCP:全部	169.254.169.254/32
出方向	ipv4	全部	0.0.0.0/0
出方向	ipv6	全部	::/0

2. 配置安全组出入方向规则。
    1. 在安全组列表，点击上述安全组的 `配置规则` ，进入安全组详情页面的规则列表。
    2. 添加如下规则，单击 `确认` ，完成操作。

方向	类型	协议和端口	源地址
入方向	ipv4	TCP:全部	10.0.0.0/24

> 说明：由于无状态安全组规则是无状态的，所以配置了一个方向的允许策略，需要配置回复方向的允许策略，以达到流量放行的需求。

3. 虚拟网卡关联安全组。
    1. 进入虚拟网卡列表，选择云主机A和云主机B的虚拟网卡，点击页面上方 `更多` - `编辑安全组` ，弹出“编辑安全组”对话框。
    2. 选择上述安全组，点击 `保存` 。

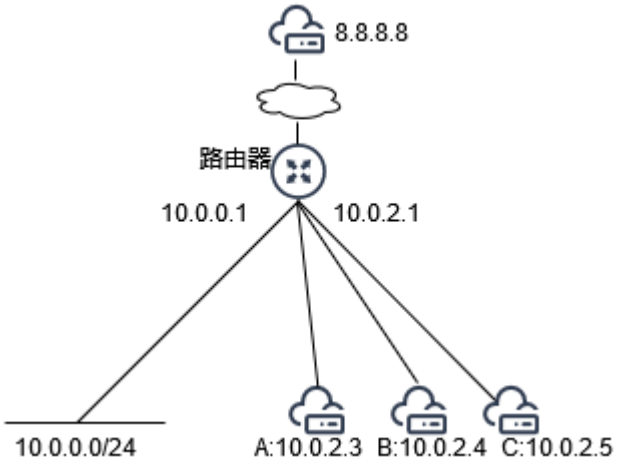
结果验证

进入云主机A，能正常SSH访问云主机B；进入云主机B，能正常SSH访问云主机A。

1.9 配置策略路由

背景描述

静态路由是根据报文的目的地址查找路由表，然后进行转发，不能满足用户自定义的策略进行报文转发和选路。如图所示拓扑，VPC内网段 `10.0.0.0/24` 访问 `8.8.8.8` 的流量需要通过ECMP引流到云主机A，B，C上进行处理。



本实践方案通过配置策略路由完成上述需求。

前提条件

路由器绑定了上述网段子网，子网间的云主机可以互通。

操作步骤

1. 分别进入云主机A，B，C的VNC，执行如下步骤。

   网卡开启路由转发功能：

   ```
   sudo sysctl -w net.ipv4.ip_forward=1
   ```

2. 进入安全组列表，创建一个 `无状态` 安全组，配置出入方向 `0.0.0.0/0` 全放通的规则。

3. 分别为云主机A，B，C的网卡配置 `无状态` 安全组和关闭 `源/目的检查` 。

   1. `虚拟网卡列表` 选择云主机的网卡，点击进入详情。

2. 点击 `更多操作` - `编辑安全组` ，选择上述 `无状态` 安全组，点击保存。

3. 点击关闭 `源/目的检查` 按钮。

> 说明：由于 `10.0.0.0/24` 虚机访问 `8.8.8.8` 的流量来回路径不一致，为了避免conntrack对云主机A，B，C网卡的影响，需要配置 `无状态` 的安全组。

4. 进入路由器，配置策略路由。

优先级	IP类型	协议和端口	策略	下一跳	
10	IPv4	全部	重路由	10.0.2.3,10.0.2.4,10.0.2.5	10.0

> 说明：源接口 `10.0.0.1` 必须配置，因为引流到云主机A，B，C的流量出来时源IP、目的IP都没有变化，再次路由后源接口变为了 `10.0.2.1` ，所以流量不会匹配这条策略路由，会正常访问到目的IP地址； `重路由` 多个下一跳地址表示 ECMP 路由，地址间用逗号隔开。

结果验证

进入网段 `10.0.0.0/24` 的云主机，能正常访问 `8.8.8.8` ； 进入云主机A，B，C的VNC，通过tcpdump能够正常抓到 `10.0.0.0/24` 访问 `8.8.8.8` 的报文。

1.10 配置二层组播

背景描述

越来越多的应用场景需要支持高效的多点通信，包括券商普通组播业务，以及IP语音组播业务。传统的单播和广播模式虽然可以完成点对点和一对全网的通信，但在多点传输中存在很多问题，尤其是在带宽、网络延迟和网络资源的使用上。因此，二层组播可用于满足特定应用对多点通信的需求。

本实践方案通过配置网络组播完成上述需求。

前提条件

1. 参考“计算”帮助中“云主机”的相关内容，提前制作并上传镜像好云主机需要的“镜像”。

操作步骤

1. 配置物理交换机（以盛科E580交换机为例）。

    1. 启用 Igmp Snooping。

    ```
    # 可以全局开启，也可以指定vlan开启
    ip igmp snooping ( vlan VLAN_ID | )
    ```

    2. 指定运行的 IGMP 版本。

    ```
    # VER 取值 1-3，推荐配置为3
    ip igmp snooping ( vlan VLAN_ID | ) version VER
    ```

    3. 在 VLAN 上使能组播查询器功能。

    ```
    # 开启组播查询器
    ip igmp snooping vlan VLAN_ID querier
    # 设置组播查询器的源地址
    ip igmp snooping vlan VLAN_ID querier address IP_ADDR
    ```

    4. 关闭 IGMP snooping 成员快速离开功能

```
no ip igmp snooping ( vlan VLAN_ID | ) fast-leave
```

5. 丢弃未知的组播流量（可选）。

```
ip igmp snooping ( vlan VLAN_ID | ) discard-unknown
```

6. 使用 ipv6 组播

```
# ipv6 组播侦听者发现协议 MLD，需要使用ipv6相关命令
如：启用 MLD Snooping
ipv6 mld snooping ( vlan VLAN_ID | )
```

7. 恢复配置

```
# 可以在命令开头使用关键字 no 恢复
如：关闭 Igmp Snooping
no ip igmp snooping ( vlan VLAN_ID | )
```

2. 创建开启组播的网络。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
   2. 单击 `创建网络` ，进入“创建网络”页面。
   3. 网络模式选择“VLAN”后，配置开启“组播”，单击 `创建网络` ，完成操作。其中，各参数的具体说明，请参考 创建二层基础网络。

3. 使用组播网络创建云主机。

   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 `创建云主机` ，进入“创建云主机”的“基础配置”页面，云主机数量输入“3”。其余配置参考“计算”帮助中“云主机”的相关内容。
   3. 单击 `下一步：网络配置` ，进入“网络配置”页面。“虚拟网卡”选择步骤1创建的组播网络，配置其他参数后，单击 `确认配置` 。其余配置参考“计算”帮助中“云主机”的相关内容。

4. 在云主机上启动IGMP。

   1. 使用开源软件SMCRoute来管理IGMP，实现IGMP组播组的加入离开。

2. 三台云主机vm1、vm2、vm3，其中vm1作为点播者，使用SMCRoute加入组播组；vm2作为对照不加入组播组；vm3作为组播源，使用iperf发送组播UDP报文。

3. 进入云主机vm1的VNC，执行如下步骤。

   1. 编译SMCRoute

```
$ wget
https://github.com/troglobit/smcroute/releases/download/2.5.7/smcroute-
2.5.7.tar.gz
$ tar xvf smcroute-2.5.7.tar.gz
$ cd ./smcroute-2.5.7
$ ./autogen.sh
$ ./configure --prefix=/usr --localstatedir=/var --sysconfdir=/etc
$ make && make install
```

   2. 启动SMCRoute

```
# 在网卡eth0上加入组播组225.1.2.3
$ cat ./smcroute.conf
mgroup from eth0 group 225.1.2.3
$ systemctl restart smcroute
```

   3. 查看组播组关系表

```
$ smcroutectl show groups

Group Memberships Table
GROUP (S,G)                                IIF
(*, 225.1.2.3)                             eth0
```

   4. 动态加入和离开组播组

```
$ smcroutectl join eth0 225.0.0.3
$ smcroutectl leave eth0 225.0.0.3
```

   5. 使用tcpdump抓包，验证加入组播组的成员可以收到组播流量

```
$ tcpdump -i eth0 -nne -vvv udp
```

4. 进入云主机vm2的VNC，使用tcpdump抓包，验证没有加入组播组的成员收不到组播流量。

```
$ tcpdump -i eth0 -nne -vvv udp
```

5. 进入云主机vm3的VNC，使用iperf发送组播流量

```
$ iperf -c 225.1.2.3 -u -t 3000 -T32  -b 1M
```

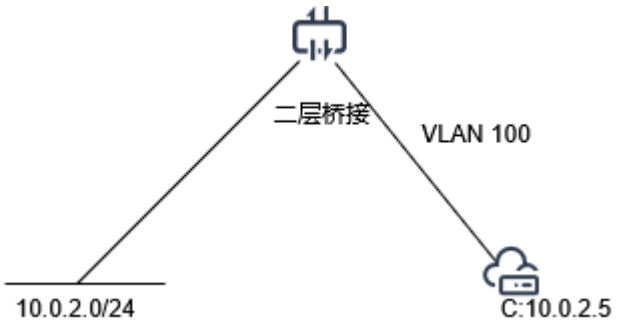
结果验证

查看云主机vm1和vm2的抓包结果，vm1可以收到来自vm3的组播流量，vm2则收不到。

1.11 云外资源通过二层桥接访问同网段云内资源

背景描述

如图所示拓扑，云外VLAN 100下的服务器C的IP `10.0.2.5` 希望访问云内 `share_net` 下同网段 `10.0.2.0/24` 的资源。



本实践方案通过配置二层桥接完成上述需求。

前提条件

已部署好二层桥接节点，并且放开节点上联交换机口的VLAN 100，配置好节点可用域比如 `leaf1` 。

> 说明：
> 二层桥接节点承载二层桥接服务，负责将云平台内部的隧道网络和云外的 VLAN 网络二层连通，实现云外服务器不改变网络二层接入云内，从而使用云内的丰富网络功能。

操作步骤

1. 创建二层桥接。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[二层桥接]，进入“二层桥接”页面。
    2. 单击 `创建二层桥接` ，弹出“创建二层桥接”对话框。
    3. 配置参数后，单击 `创建` ，完成操作。

名称	项目	描述	可用区	网络	V
l2br	Default:admin	-	leaf1	share_net	1(

2. 配置云内虚机网卡的安全组。

    1. 创建安全组，并且配置放开云外服务器C的IP `10.0.2.5` 的规则。

    2. 云内虚机网卡关联上述安全组。

结果验证

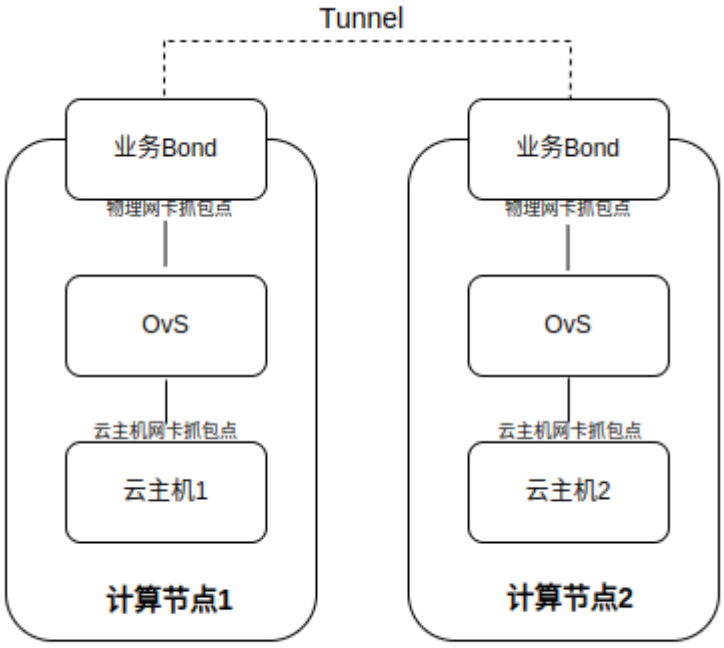
云外服务器C和云内 `10.0.2.0/24` 可以互相访问。

1.12 网络抓包

1.12.1 云主机到云主机的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



云主机到云主机的网络抓包

本实践方案中，将按云主机1流向云主机2的流量的路径，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
计算节点	* 计算节点1名称：node-1 * 计算节点2名称：node-2	创建的两个云主机分别位于这两个计算节点上。

类型	配置	说明
云主机	* 云主机1名称：test-vm1，IP地址：192.168.101.101 * 云主机2名称：test-vm2，IP地址：192.168.101.102	在云主机1上ping云主机2的IP，然后进行网络抓包。

> 说明：
> 网络抓包不支持在SR-IOV虚拟机虚拟网卡上抓包。

操作步骤

1. 创建Geneve网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
    2. 单击 `创建网络` ，进入“创建网络”页面。
    3. 配置参数后，单击 `创建网络` ，完成操作。
2. 创建云主机。
    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 `创建云主机` ，弹出“创建云主机”对话框。
    3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。
3. 在云主机1执行ping云主机2的IP。
    1. 在“云主机”页面中，单击云主机1的vnc按钮，进入云主机1的vnc页面。
    2. 在云主机1的终端中，执行ping云主机2的IP的命令。
4. 创建抓包任务。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。

2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。
3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：云主机1的虚拟网卡，计算节点1的隧道物理网卡，计算节点2的隧道物理网卡，云主机2的虚拟网卡。各参数的具体说明，请参考 配置网络抓包。
4. 这里我们在创建时，选择的 `过滤条件` ，使用 `模板` 模式，基于我们这个例子，我们选择 `IP类型` 为IPv4，`协议` 为ICMP， `源IP` 选择云主机1对应的IP地址， `目的IP` 选择云主机2对应的IP地址，且 `源端口` 和 `目的端口` 不填写， `双向` 选择 `是` 。

5. 查看抓包任务时延。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。
6. 下载抓包结果文件。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

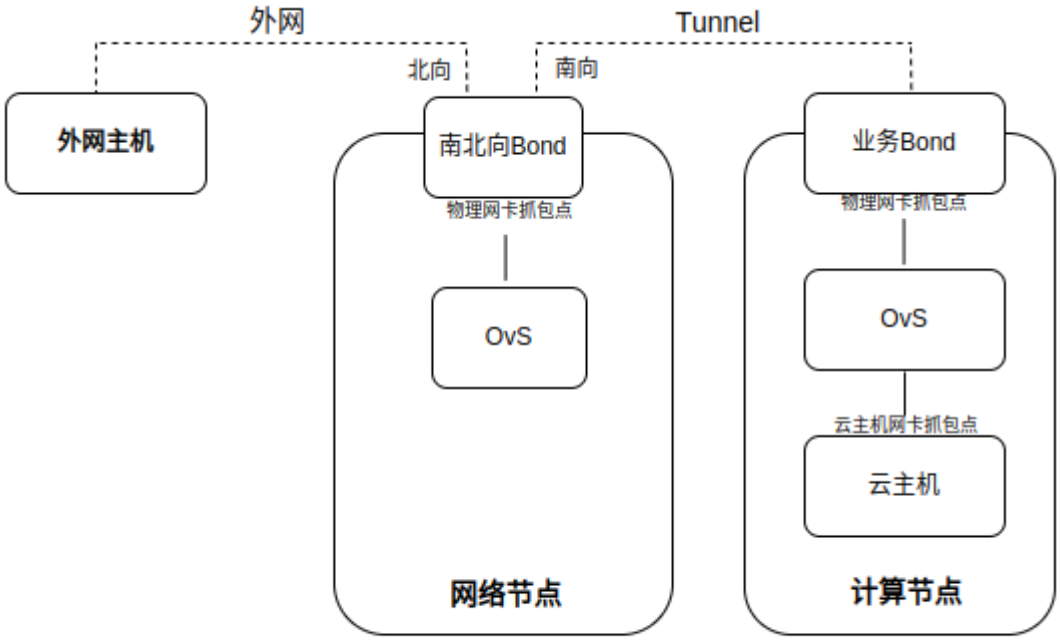
结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.12.2 外网主机到云主机的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



外网主机到云主机的网络抓包

本实践方案中，将按外网主机流向云主机的流量的路径，顺序的选择物理网卡和虚拟网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
计算节点	* 计算节点名称：node-1	创建的云主机位于该计算节点上。
网络节点	* 网络节点名称：node-2	外网主机访问云主机服务需要通过网络节点，然后通过计算节点到达云主机。

类型	配置	说明
云主机	* 云主机名称：test-vm，内部IP地址：192.168.111.144，公网IP地址：172.35.0.94	外网主机将ping该云主机的公网IP地址。
外网主机	* 外网主机名称：ext-host，IP地址：172.35.0.200	外网主机将ping该云主机的公网IP地址。

> 说明：
> 进出网络节点的北向Bond流量经过了NAT转换，所以时延的计算需要选择除网络节点的北向Bond的其他抓包点进行计算。

操作步骤

1. 创建Geneve网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
    2. 单击 `创建网络` ，进入“创建网络”页面。
    3. 配置参数后，单击 `创建网络` ，完成操作。
2. 创建路由器
    1. 在“路由器”页面中，单击 `创建路由器` ，弹出“创建路由器”对话框。
    2. 配置参数后，单击 `创建` ，完成操作。
3. 路由器连接子网
    1. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
    2. 选择步骤1创建的子网，单击 `连接` ，完成操作。
4. 创建云主机。

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 `创建云主机` ，弹出“创建云主机”对话框。
3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。

5. 配置公网IP地址。
   1. 在“云主机”页面中，选择步骤4创建的云主机，点击[更多]-[绑定公网IP]。
   2. 在弹出的 `云主机绑定公网IP` 页面，选择对应 `云主机网卡` ，选择一个对应的 `公网IP` 进行绑定。
6. 创建抓包任务。
   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。
   2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：网络节点的北向Bond物理网卡，网络节点的南向Bond物理网卡，计算节点的业务Bond物理网卡，云主机的虚拟网卡。各参数的具体说明，请参考 配置网络抓包。
   4. 这里我们在创建时，选择的 `过滤条件` ，使用 `自定义` 模式，基于我们这个例子，我们填写 `icmp and ((host 192.168.111.144) or (host 172.35.0.94) or (host 172.35.0.200))` 自定义过滤条件。
   5. 其中，网络节点的南向Bond和北向Bond是同一个Bond物理网卡。
7. 查看抓包任务时延。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。
8. 下载抓包结果文件。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。

3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

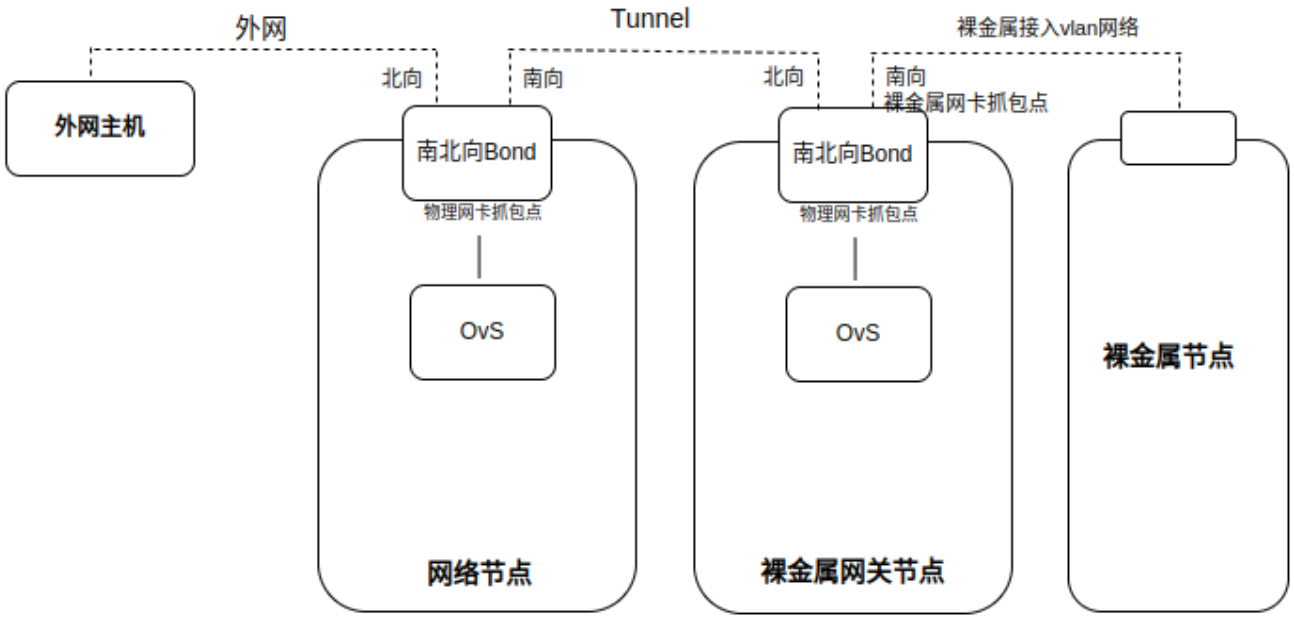
结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.12.3 外网主机到裸金属节点的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



外网主机访问裸金属节点的网络抓包

本实践方案中，将按外网主机流向裸金属节点的流量的路径，顺序的选择物理网卡和虚拟网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
裸金属网关节点	* 裸金属网关节点名称：node-1	与裸金属节点交互的流量需要通过裸金属网关节点。
网络节点	* 网络节点名称：node-2	外网主机访问裸金属节点上的服务需要通过网络节点，然后通过裸金属网关节点到达裸金属节点。

类型	配置	说明
裸金属节点	* 裸金属节点名称：test-bm，内部IP地址：192.168.111.144，公网IP地址：172.35.0.94	外网主机将ping该裸金属节点的公网IP地址。
外网主机	* 外网主机名称：ext-host，IP地址：172.35.0.200	外网主机将ping该裸金属节点的公网IP地址。

> 说明：
> 1. 网络抓包不支持在使用VLAN网络的裸金属的虚拟网卡上抓包。
> 2. 进出网络节点的北向Bond流量经过了NAT转换，所以时延的计算需要选择除网络节点的北向Bond的其他抓包点进行计算。

操作步骤

1. 创建Geneve网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
    2. 单击 `创建网络` ，进入“创建网络”页面。
    3. 配置参数后，单击 `创建网络` ，完成操作。
2. 创建路由器
    1. 在“路由器”页面中，单击 `创建路由器` ，弹出“创建路由器”对话框。
    2. 配置参数后，单击 `创建` ，完成操作。
3. 路由器连接子网
    1. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。
    2. 选择步骤1创建的子网，单击 `连接` ，完成操作。
4. 创建云主机。

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 `创建云主机` ，弹出“创建云主机”对话框。
3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。

5. 配置公网IP地址。
   1. 在“云主机”页面中，选择步骤4创建的云主机，点击[更多]-[绑定公网IP]。
   2. 在弹出的 `云主机绑定公网IP` 页面，选择对应 `云主机网卡` ，选择一个对应的 `公网IP` 进行绑定。
6. 部署裸金属节点。
7. 创建抓包任务。
   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。
   2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：网络节点的北向Bond物理网卡，网络节点的南向Bond物理网卡，裸金属网关节点的北向Bond物理网卡，裸金属网关节点的南向Bond物理网卡。各参数的具体说明，请参考 配置网络抓包。
   4. 这里我们在创建时，选择的 `过滤条件` ，使用 `自定义` 模式，基于我们这个例子，我们填写 `icmp and ((host 192.168.111.144) or (host 172.35.0.94) or (host 172.35.0.200))` 自定义过滤条件。
   5. 其中，网络节点的南向Bond和北向Bond是同一个Bond物理网卡。
8. 查看抓包任务时延。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。
9. 下载抓包结果文件。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。

2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。

3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

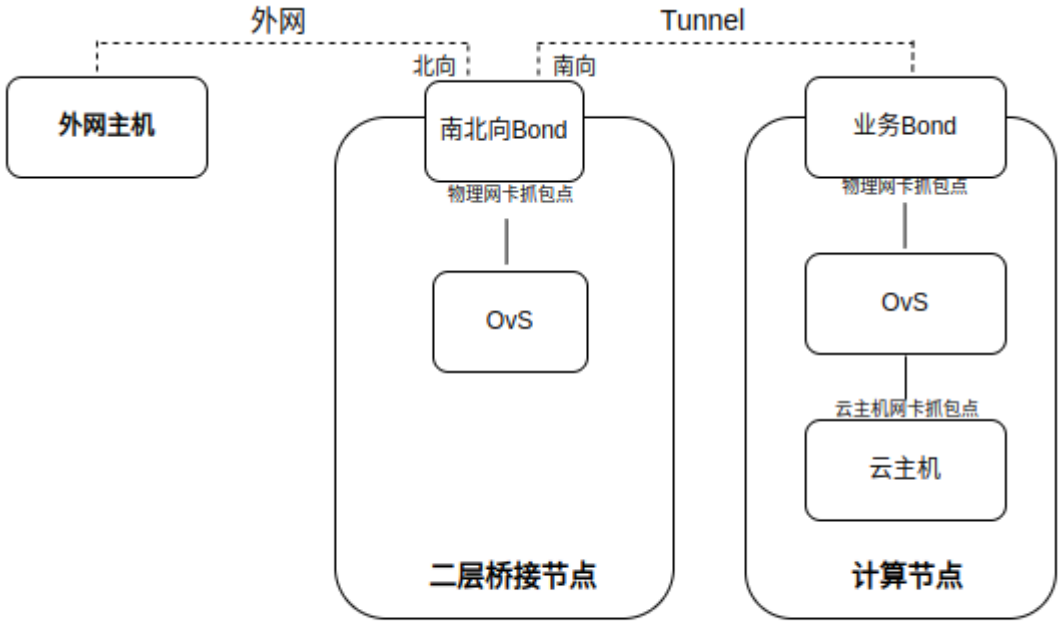
结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.12.4 外网主机通过二层桥接到云主机的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



外网主机通过二层桥接访问云主机的网络抓包

本实践方案中，将按外网主机通过二层桥接流向云主机的流量的路径，顺序的选择物理网卡和虚拟网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
计算节点	* 计算节点名称：node-1	创建的云主机位于该计算节点上。

类型	配置	说明
二层桥接节点	* 二层桥接节点名称：node-2	外网主机访问云主机服务需要通过二层桥接节点，然后通过计算节点到达云主机。
云主机	* 云主机名称：test-vm，内部IP地址：192.168.111.144	外网主机将ping该云主机的内部IP地址。
外网主机	* 外网主机名称：ext-host，IP地址：192.168.111.200	外网主机与云主机通过二层桥接，ping该云主机的内部IP地址。

操作步骤

1. 创建Geneve网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
    2. 单击 `创建网络` ，进入“创建网络”页面。
    3. 配置参数后，单击 `创建网络` ，完成操作。
2. 创建云主机。
    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 `创建云主机` ，弹出“创建云主机”对话框。
    3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。
3. 创建二层桥接
    1. 在“二层桥接”页面中，单击 `创建二层桥接` ，弹出“创建二层桥接”对话框。
    2. 配置参数后，单击 `创建` ，完成操作。其中，选择的网络为步骤1创建的网络。vlan选择对应的能与外网主机的互通的vlan ID。
4. 创建抓包任务。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。

2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。
3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：网络节点的北向Bond物理网卡，二层桥接节点的南向Bond物理网卡，计算节点的业务Bond物理网卡，云主机的虚拟网卡。各参数的具体说明，请参考 配置网络抓包。
4. 这里我们在创建时，选择的 `过滤条件` ，使用 `模板` 模式，基于我们这个例子，我们选择 `IP类型` 为IPv4，`协议` 为ICMP， `源IP` 填写外网主机对应的IP地址， `目的IP` 选择云主机对应的IP地址，且 `源端口` 和 `目的端口` 不填写， `双向` 选择 `是` 。
5. 其中，网络节点的南向Bond和北向Bond是同一个Bond物理网卡。

5. 查看抓包任务时延。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。
6. 下载抓包结果文件。
   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

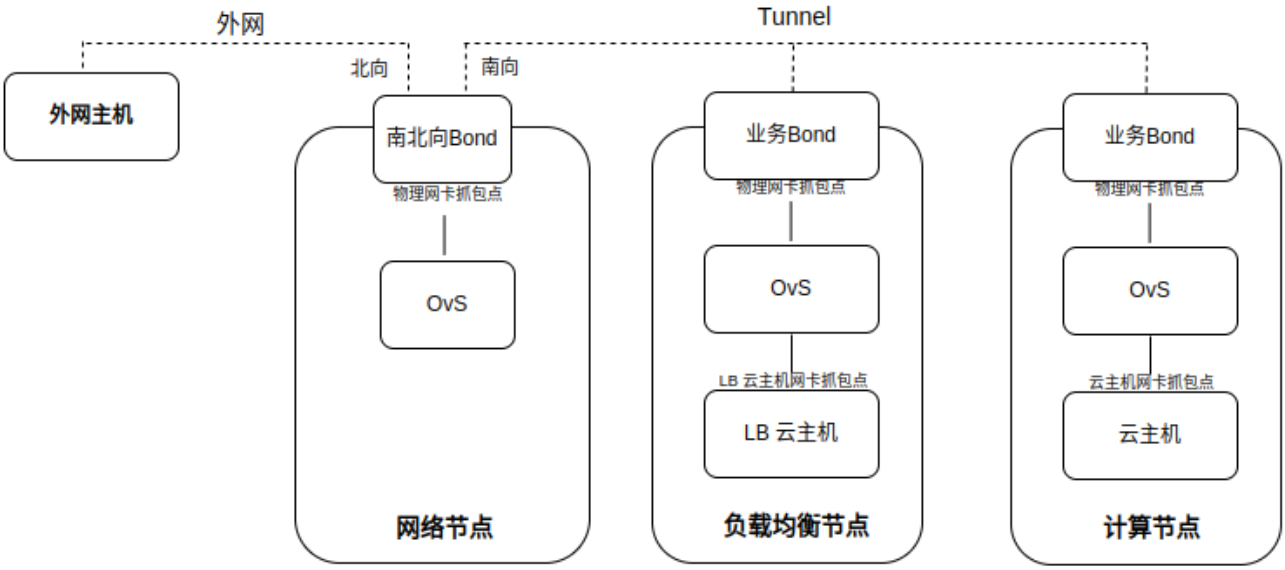
结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.12.5 外网主机通过负载均衡到云主机的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



外网主机通过云内负载均衡访问云内业务的网络抓包

本实践方案中，将按外网主机通过负载均衡节点流向云主机的流量的路径，顺序的选择物理网卡和虚拟网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
计算节点	* 计算节点名称：node-1	负载均衡的提供的后端服务的云主机位于该计算节点上。
负载均衡节点	* 负载均衡节点名称：node-2	LB云主机位于负载均衡节点上。

类型	配置	说明
网络节点	* 网络节点名称：node-3	外网主机访问负载均衡后端服务需要通过网络节点，然后通过负载均衡节点到达提供后端服务的计算节点上。
LB云主机	* LB云主机默认会创建两台 * LB云主机1的内部IP地址：192.168.111.203 * LB云主机2的内部IP地址：192.168.111.223 * 分配的内网VIP为192.168.111.19，分配的公网IP为172.46.0.194	本实践中，外网主机将通过ssh访问LB云主机的公网IP地址。
云主机	* 云主机名称：test-vm，内部IP地址：192.168.111.144	外网主机将通过负载均衡节点ssh到该云主机的上。
外网主机	* 外网主机名称：ext-host，IP地址：172.46.0.201	外网主机将通过负载均衡节点ssh到该云主机的上。

> 说明：
> 进出网络节点的北向Bond流量经过了NAT转换，所以时延的计算需要选择除网络节点的北向Bond的其他抓包点进行计算。
> 进入LB云主机的流量经过了地址转换，转换后的源端口是随机端口，抓包时无法指定，建议抓包过滤条件里只指定目的端口即可。

操作步骤

1. 创建Geneve网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
    2. 单击 `创建网络` ，进入“创建网络”页面。
    3. 配置参数后，单击 `创建网络` ，完成操作。

2. 创建路由器

   1. 在“路由器”页面中，单击 `创建路由器` ，弹出“创建路由器”对话框。

   2. 配置参数后，单击 `创建` ，完成操作。

3. 路由器连接子网

   1. 在[路由器连接]页签中，单击 `连接子网` ，弹出“连接子网”对话框。

   2. 选择步骤1创建的子网，单击 `连接` ，完成操作。

4. 创建云主机。

   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 `创建云主机` ，弹出“创建云主机”对话框。

   3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。

5. 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` ，进入“创建负载均衡器”页面。

   3. 配置参数后，单击 `创建` ，完成操作。

   4. 进入详情，点击右上角 `更多操作` ，点击 `绑定公网IP` ，选择一个公网IP进行绑定。

   5. 这里创建的负载均衡是2副本的多活模式。

6. 配置监听器和资源池。

   1. 点击步骤5创建的负载均衡器，点击 `监听器` ，进入页面，点击 `创建监听器` ，进入页面。

   2. 选择 `协议` 为 `TCP（标准模式）` ， `协议端口` 输入 `22` 。点击 `下一步：资源配置`

   3. 进入 `资源池` 配置页面，点击 `确认` 。

   4. 进入创建的 `资源池` 详情页面，点击 `添加云内资源` ，选择步骤4创建云主机，选择 `端口号` 为22。点击 `下一步：确认信息` ，最后点击 `确认` ，完成添加。

7. 创建抓包任务。

   1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。
   2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。
   3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：网络节点的北向Bond物理网卡，网络节点的南向Bond物理网卡，负载均衡节点的业务Bond物理网卡，LB云主机1的虚拟网卡，LB云主机2的虚拟网卡，计算节点的业务Bond物理网卡，云主机的虚拟网卡。各参数的具体说明，请参考 配置网络抓包。
   4. 这里我们在创建时，选择的 `过滤条件` ，使用 `自定义` 模式，基于我们这个例子，我们填写 `tcp and ((host 192.168.111.144) or (host 192.168.111.19) or (host 192.168.111.203) or (host 192.168.111.223) or (host 172.46.0.201) or (host 172.46.0.194)) and port 22` 自定义过滤条件。
   5. 其中，网络节点的南向Bond和北向Bond是同一个Bond物理网卡。

8. 查看抓包任务时延。

   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。
   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。
   4. 其中，查看网络节点到负载均衡节点上的LB云主机之间的时延，可选择网络节点的南向Bond物理网卡，负载均衡节点的业务Bond物理网卡，LB云主机1的虚拟网卡，LB云主机2的虚拟网卡这4个抓包点进行时延查看。
   5. 查看负载均衡节点到计算节点上的云主机之间的时延，可选择LB云主机1的虚拟网卡，LB云主机2的虚拟网卡，计算节点的业务Bond物理网卡，云主机的虚拟网卡这4个抓包点进行时延查看。

9. 查看抓包任务时延。

   1. 在抓包任务完成后，进入对应的抓包任务详情页面。
   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。

3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

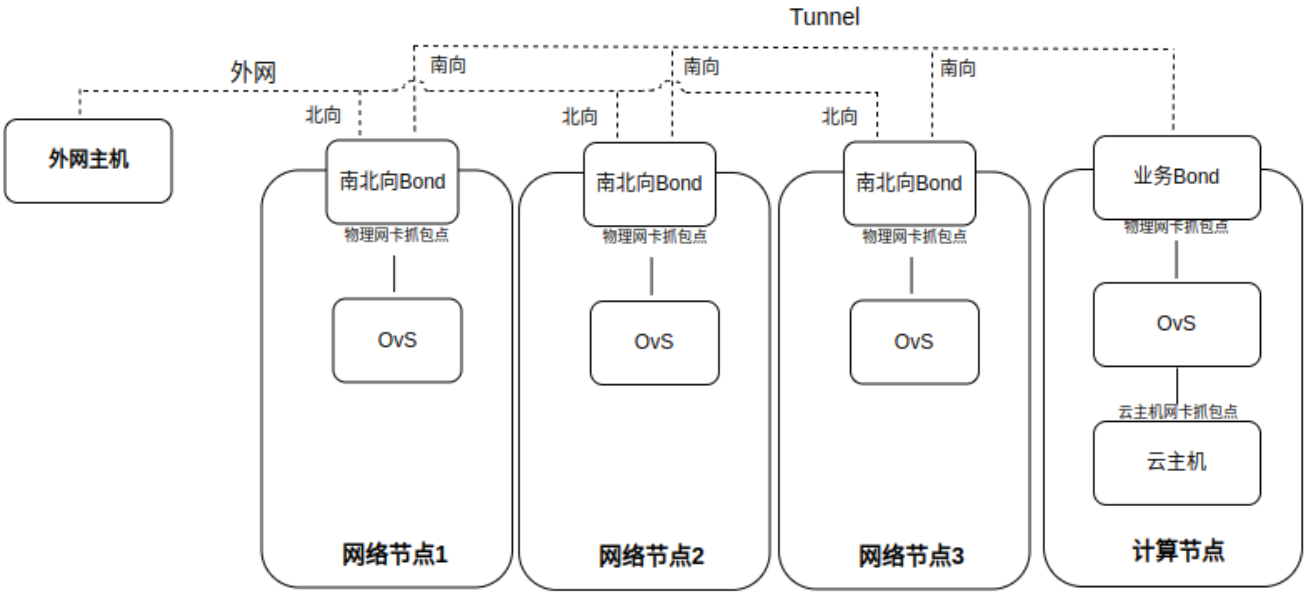
结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.12.6 外网主机通过多活网络到云主机的网络抓包

背景描述

通过手动指定虚拟网卡和物理网卡实现网络抓包。在已知流量路径的条件下，顺序的选择虚拟网卡和物理网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。当然，也可以按照任意顺序捕获期望的虚拟网卡和物理网卡的流量。



外网主机通过多活网络访问云主机的网络抓包

本实践方案中，将按外网主机通过多活网络流向云主机的流量的路径，顺序的选择物理网卡和虚拟网卡进行抓包，在抓包任务完成后，能够根据抓包结果，实现报文的下载和时延分析。具体规划信息如下：

类型	配置	说明
计算节点	* 计算节点名称：node-1	创建的云主机位于该计算节点上。

类型	配置	说明
网络节点	* 网络节点1名称：node-2 * 网络节点2名称：node-3 * 网络节点3名称：node-4	外网主机访问云主机服务的流量会通过该网络节点，然后通过计算节点到达云主机。
云主机	* 云主机名称：test-vm，内部IP地址：192.168.1.210	外网主机将ping该云主机的内部IP地址。
外网主机	* 外网主机名称：ext-host，IP地址：172.46.0.201	外网主机将ping该云主机的内部IP地址。

> 说明：
> 从云外来的流量通过外部路由器的ECMP最终选择一个网络节点进入，从云内来的流量经过云内路由器的ECMP最终也选择一个网络节点进入，由于这2个网络节点无法确定是哪一个（ECMP一般通过五元组HASH选择一个网络节点），并且这2个网络节点也不一定是同一个网络节点，所以抓包时我们需要抓所有的网络节点。

操作步骤

1. 创建多活网络相关网络和路由器，各参数和配置的具体说明，请参考 配置多活网络方案(IPv4)。

2. 创建云主机。

    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 `创建云主机` ，弹出“创建云主机”对话框。

    3. 配置参数后，单击 `创建` ，完成操作。其中，选择的子网为步骤1创建的子网。

3. 创建抓包任务。

    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络运维]，进入“网络抓包”页面。

    2. 单击 `创建网络抓包` ，弹出“创建网络抓包”对话框。

3. 配置参数后，单击 `创建` ，完成操作。其中，选择的抓包点顺序为：网络节点1的北向Bond物理网卡，网络节点1的南向Bond物理网卡，网络节点2的北向Bond物理网卡，网络节点2的南向Bond物理网卡，网络节点3的北向Bond物理网卡，网络节点3的南向Bond物理网卡，计算节点的业务Bond物理网卡，云主机的虚拟网卡。各参数的具体说明，请参考 配置网络抓包。

4. 这里我们在创建时，选择的 `过滤条件` ，使用 `模板` 模式，基于我们这个例子，我们选择 `IP类型` 为IPv4, `协议` 为ICMP， `源IP` 填写外网主机对应的IP地址， `目的IP` 选择云主机对应的IP地址，且 `源端口` 和 `目的端口` 不填写， `双向` 选择 `是` 。

5. 其中，网络节点的南向Bond和北向Bond是同一个Bond物理网卡。

4. 查看抓包任务时延。

   1. 在抓包任务完成后，进入对应的抓包任务详情页面。

   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。

   3. 选择抓包成功的报文列后，点击 `查看时延` ，在弹出的对话框中，选择对应的 `过滤条件` 后，点击 `计算时延` 按钮，将显示前10条大时延数据。其中选择的 `过滤条件` 是IPv4协议下的ICMP协议中的五元组数据。

   4. 这里发送报文和回复报文的路径可能不一致，比如发送报文走的是网络节点1到计算节点，回复报文走的计算节点到网络节点2。如果是这种路径不一致的情况，只能分别选择网络节点1的南北向Bond物理网卡，计算节点的业务Bond物理网卡和云主机的虚拟网卡计算发送报文的时延，而选择选择网络节点2的南北向Bond物理网卡，计算节点的业务Bond物理网卡和云主机的虚拟网卡计算回复报文的时延。如果发送报文和回复报文的路径一致，则按照常规选择路径上的抓包点进行时延计算即可。

5. 下载抓包结果文件。

   1. 在抓包任务完成后，进入对应的抓包任务详情页面。

   2. 在抓包任务详情页面， `抓包结果文件` 显示的抓包任务捕获的所有报文。

   3. 选择抓包成功的报文列后，点击 `下载` ，将下载抓包成功的报文文件。

结果验证

1. 在查看抓包时延页面，可以看到时延数据。
2. 下载抓包结果文件后，可以看到抓包结果文件且文件中的报文个数与页面上统计的个数相同。

1.13 SRIOV虚机使用ntopng监控流量

背景描述

创建信任模式的SRIOV网卡，该类型网卡可以接收任意IP/MAC，VLAN报文，可以用于监控网络中的流量。

本文将详细介绍如何通过SRIOV网卡虚机，结合ntopng软件来监控网络流量。

前提条件

- 计算节点安装了支持信任模式的SRIOV网卡，比如Mallenox cx4 cx5 cx6。
- 已创建监控虚机，并给虚机绑定了公网IP。

操作步骤

1. 创建FLAT网络。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[创建网络]，进入“创建网络”页面。
    2. 注意： `网络类型` 选择 `内部网络` ， `网络模式` 选择 `Flat` ， `物理网络` 选择 `physnet2` 。
2. 计算节点SRIOV网卡虚拟化切割。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[计算节点]，点击进入SRIOV网卡的节点页面。
    2. 点击 `网卡` 列表， 选择支持信任模式的SRIOV网卡比如enP4s3f0，然后 `绑定物理网络` 选择physnet2，再进行 `虚拟化切割` 按需设置切割VF的数目。
3. 创建信任模式的SRIOV网卡。
    1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[创建虚拟网卡]，进入“创建虚拟网卡”页面。
    2. 注意： `IPv4子网` 选择 上述创建的flat网络子网 ，选择 `启用SR-IOV` 并开启 `信任模式` 。
    3. 将SRIOV网卡挂载给虚机，点击 `绑定到资源` 选择虚机绑定。
4. 在云主机中安装ntopng软件。以Ubuntu虚机为例。
    1. 安装步骤，ntopng安装配置可以参考ntopng官网。

```
apt-get install software-properties-common wget
add-apt-repository universe
wget https://packages.ntop.org/apt/22.04/all/apt-ntop.deb
apt install ./apt-ntop.deb
```

2. 安装完成后，启动ntopng软件，能成功访问ntopng的web界面： `虚机公网IP:3000` 。

5. 交换机配置流量镜像，将流量镜像到SRIOV网卡。 注意：根据实际需求，以及交换机的配置方式，配置流量镜像到SRIOV网卡上联交换机端口。

结果验证

登录 `虚机公网IP:3000` ，web界面切换到SRIOV网卡，可以查看到监控的网络流量数据。

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)