



弹性公网 IPv6 (EIPv6)

产品文档





文档目录

- 产品简介
 - 产品概述
 - 产品优势
 - 应用场景
 - 配额说明
- 快速入门
- 操作指南
 - 私有网络分配与释放 IPv6 CIDR
 - 子网分配与释放 IPv6 CIDR
 - 弹性网卡申请与释放 IPv6 地址
 - 管理 IPv6 公网
- 常见问题
 - 通用类
 - IPv6连通性故障排查
- 词汇表

产品简介

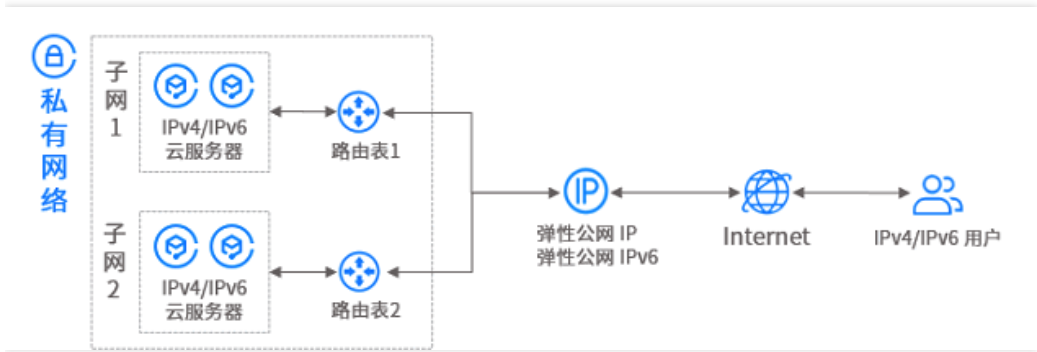
产品概述

最近更新时间: 2024-08-23 15:08:00

弹性公网 IPv6 (Elastic IPv6 , EIPv6) 是云服务器 IPv6 的公网网关。通过弹性公网 IPv6 , 您可以为每一个云服务器的 IPv6 地址开通或者关闭公网 , 并设置公网带宽。

说明 :

本文档中的弹性公网 IP , 均指弹性公网 IPv4。



产品功能

弹性网卡申请了 IPv6 地址后 , 默认关闭了公网访问能力 , 仅支持 VPC 内的 IPv6 地址通信。通过弹性公网 IPv6 , 支持单个 IPv6 地址或者多个 IPv6 地址开通公网或者关闭公网。

VPC 内通信

同一 VPC 下不同的弹性网卡获取并启用 IPv6 地址后 , 即默认支持 VPC 内的 IPv6 地址相互通信。

开通公网

未开通公网的 IPv6 地址 , 可通过弹性公网 IPv6 开通公网并设置公网带宽上限 , 开通公网支持单个开通与批量开通。

关闭公网

已开通公网通信能力的 IPv6 地址 , 可通过弹性公网 IPv6 关闭公网 , 关闭公网支持单个关闭与批量关闭。



产品优势

最近更新时间: 2024-08-23 15:08:00

操作简便

您可以通过弹性公网 IPv6 随时为您的 IPv6 云服务器开启或者关闭公网接入，并且灵活设置 IPv6 公网带宽峰值。提供批量开通和关闭操作，易于管理。

安全可靠

弹性公网 IPv6 通过多种方式保证的 IPv6 通信访问安全性和可靠性，例如，默认关闭公网访问。同时通过跨机架容灾、跨机房容灾的底层架构能力，实现整体架构的高可用。

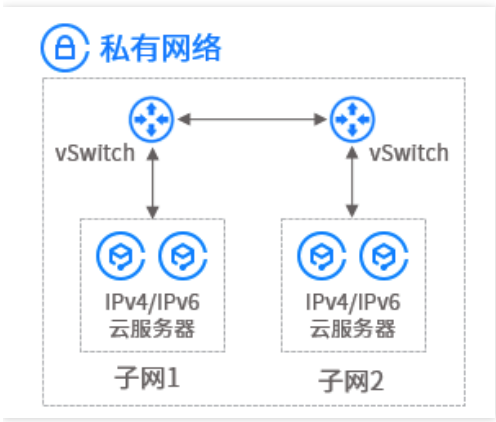
应用场景

最近更新时间: 2024-08-23 15:08:00

场景一：构建 VPC 内部的 IPv4/IPv6 双栈通信

您可以通过开通 IPv6 快速搭建 IPv4/IPv6 双栈私有网络。

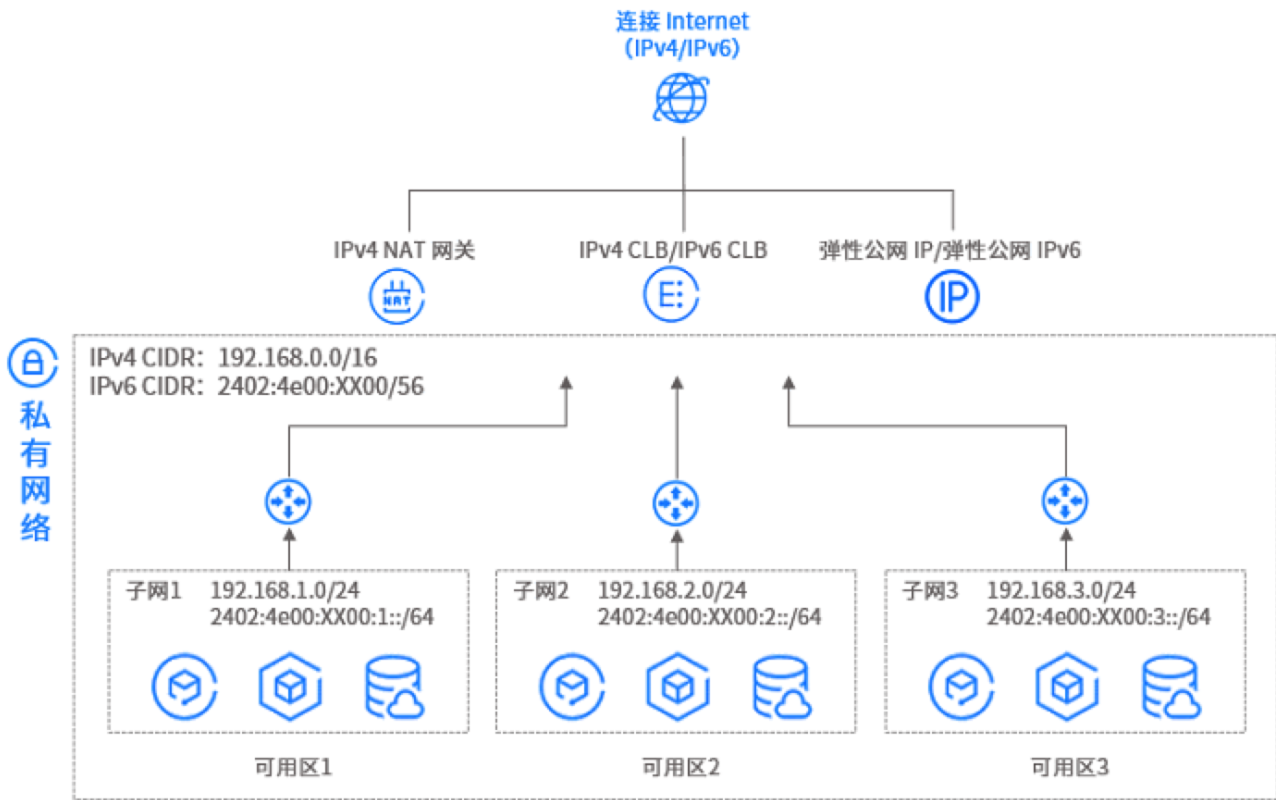
- VPC 获取到 IPv6 CIDR 后，VPC 将同时支持 IPv4 和 IPv6 双协议栈。
- 云服务器获取到 IPv6 后，也将同时支持 IPv4 和 IPv6 双协议栈。
- 默认条件下，支持同一 VPC 下的云服务器 IPv6 通信，但不支持跨 VPC 下的云服务器 IPv6 通信。
- 默认条件下，云服务器无法访问 IPv6 公网，您需要为云服务器手动开启 IPv6 公网带宽后才能够访问 IPv6 公网。



场景二：构建云服务器的 IPv6 公网通信

云服务器获取到 IPv6 后，将同时运行 IPv4 和 IPv6 双协议栈。

- 您可以通过弹性公网 IPv6 为云服务器开通 IPv6 公网访问能力，而云服务器访问 IPv4 公网仍然可以选择通过 IPv4 EIP 或者 IPv4 NAT 网关。
- IPv6 的公网访问设置和 IPv4 EIP 的设置不会相互影响，所以在只设置 IPv6 开通公网，而没有设置 IPv4 EIP 的条件下，云服务器无法访问 IPv4 公网。
- 您可为云服务器 IPv6 公网设置最大带宽，通过精细化的 IPv6 公网带宽阈值和默认的 DDoS 基础防护策略，可以有效提升安全防护能力。





配额说明

最近更新时间: 2024-08-23 15:08:00

IPv6 基础配额

资源	限制 (个)
每个 VPC 的 IPv6 CIDR 个数	1
每个 VPC 可开通 IPv6 的子网个数	256
每个子网的 IPv6 CIDR 个数	1
每个弹性网卡的 IPv6 地址个数	1
每个 VPC 可开通 IPv6 的弹性网卡个数	10000
每个 VPC 可开通 IPv6 公网的个数	1000

说明：

一个 VPC 内仅允许1000个 IPv6 地址开通公网，如果需要开通更多 IPv6 的公网能力，请提交 [工单申请](#)。

IPv6 公网带宽上限

每个 IPv6 的公网带宽上限为0 - 100Mbps。

说明：

每个 IPv6 公网带宽设置和 IPv4 公网带宽设置相互独立。不同云服务器机型的 IPv6 公网带宽峰值不同，如果需要开通更大的公网带宽，请提交 [工单申请](#)。

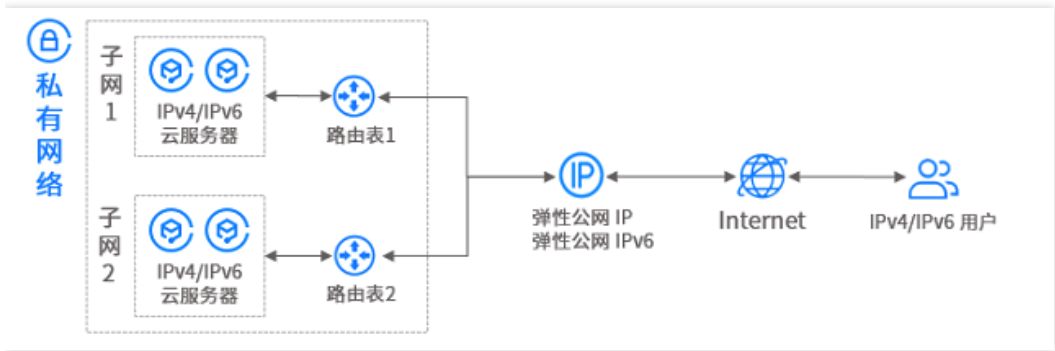
快速入门

最近更新时间: 2024-08-23 15:08:00

本教程将帮助您搭建一个具有 IPv6 CIDR 的私有网络（VPC），并为 VPC 内的云服务器开启 IPv6，实现 IPv6 的内外网通信。

操作场景

- 1. 云服务器启用 IPv6，和 VPC 内其他云服务器的 IPv6 内网互通。
- 2. 云服务器启用 IPv6，和 Internet 的 IPv6 用户进行双向通信。



操作须知

- 1. IPv6 地址为GUA地址，每个 VPC 分配1个 /56 的 IPv6 CIDR，每个子网分配1个 /64 的 IPv6 CIDR，每个弹性网卡分配1个 IPv6 地址。
- 2. 主网卡、辅助网卡均支持申请 IPv6 地址。想要了解更多云服务器和弹性网卡的关系，请参见 [弹性网卡](#) 产品文档。

操作步骤

步骤一：VPC 分配 IPv6 CIDR

- 1. 登录 [私有网络控制台](#)。
- 2. 选择支持 IPv6 的地域，并在 VPC 所在行的操作栏下，单击[获取 IPv6 地址](#)。



私有网络(VPC)

网络拓扑

私有网络

子网

路由表

IP与网卡

NAT网关

对等连接

VPN连接

私有网络

新建

搜索私有网络的名称/ID

ID/名称	IPv4 CIDR	IPv6 CIDR	外部用扩展C...	组播	子网	路由表	云主机	默认私有网络	操作
vpc-6zk1uns7 TomVPC	192.168.0.0/16		无	☐	1	1	0	否	编辑扩展CIDR 释放IPv6地址 删除
vpc-2d0k582x vpc-test	10.0.0.0/24		无	☐	1	1	0	否	编辑扩展CIDR 获取IPv6地址 删除

[私有网络与子网帮助文档](#)

系统将为 VPC 分配一个 /56 的 IPv6 地址段，您可以在列表里看到 IPv6 地址段的详细信息。

私有网络

新建

搜索私有网络的名称/ID

ID/名称	IPv4 CIDR	IPv6 CIDR	外部用扩展CIDR	组播	子网	路由表	云主机	默认私有网络	操作
vpc-6zk1uns7 TomVPC	192.168.0.0/16	2002:::0/56	无	☐	1	1	0	否	编辑扩展CIDR 释放IPv6地址 删除

[私有网络与子网帮助文档](#)

步骤二：为子网分配 IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择子网，进入管理页面。
3. 在 [步骤一](#) 中的 VPC 中的子网所在行的操作栏下，单击分配 Ipv6 CIDR。

子网

TomVPC

新建

搜索子网的名称/ID

ID/名称	所属网络	IPv4 CIDR	IPv6 CIDR	类型	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-dxy94sa8 A	vpc-6zk1uns7 TomVPC	192.168.0.0/16		普通子网	可用区1	rtb-15nctyt2 default	0	253	否	分配IPv6 CIDR 删除

[私有网络与子网帮助文档](#)

4. 在弹出的对话框中，为子网分配IPv6 CIDR并单击确定。



为子网分配IPv6 CIDR

子网

A (subnet-dvy94sa8)

IPv4 CIDR

IPv6 CIDR

2002:c000:0000:0000:0000:0000:0000:0000

确定

取消

系统将从 VPC 的 /56 IPv6 CIDR 分配一个 /64 的 IPv6 CIDR。

子网

TomVPC

私有网络与子网帮助文档

新建

搜索子网的名称/ID

ID/名称	所属网络	IPv4 CIDR	IPv6 CIDR	类型	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-dvy94sa8 A	vpc-6zk1uns7 TomVPC	10.0.0.0/24	2002:c000:0000:0000:0000:0000:0000:0000 /64	普通子网	cn-hangzhou	rtb-l5nc4yb2 default	0	253	否	释放IPv6 CIDR 更换路由表 删除

共 1 条

20 条 / 页

1 / 1 页

步骤三：购买云服务器并配置云服务器的 IPv6

为 VPC 和子网分配 IPv6 CIDR 后，您可在该子网下创建一个具有 IPv6 地址的云服务器，也可以为该子网下运行中的云服务器获取 IPv6 地址。因为 IPv6 地址目前还不支持自动下发到网卡，所以从在控制台获取 IPv6 地址后，您还需要登录云服务器进行 IPv6 的配置。

1. 登录 [云服务器购买页](#)。
2. 在云服务器购买页上方，选择**自定义配置**。
3. 在**选择地域与机型**页签，选择已分配IPv6 CIDR的私有网络和子网，设置实例类型，并单击**下一步：选择镜像**。
4. 在**选择镜像**页签，设置镜像、操作系统、系统架构、及镜像版本，并单击**下一步：选择存储和带宽**。
5. 在**选择存储和带宽**页签，选择系统盘类型、指定是否现在分配公网IP，勾选分配IPv6地址，并单击**下一步：设置安全组和主机**。
6. 在**设置安全组和主机**页签，设置安全组及实例登录密码等相关参数，并单击**下一步：确认配置信息**。
7. 在**确认配置信息**页签，确认云服务器信息无误后，单击**开通**。
8. 云服务器购买成功后，即可在云服务器列表查看到 IPv6 地址信息。



ID名称	监控	状态	可用区	实例类型	实例配置	主IPv4地址	主IPv6地址	实例计费模式	操作
		运行中		大数据型D2	8核 32GB 1Mbps 系统盘: 高性能云硬盘 网络: 1	1 (公) 1 (内)	2402	按量计费 2020-03-12 11:45:24创建	登录 更多

说明：

- 如果云服务器在购买时未分配 IPv6 地址，可在对应云服务器实例所在行的操作栏下，选择[更多](#) > [弹性 IP](#) > [管理 IPv6地址](#)，为主网卡分配 IPv6 地址。
- 如果想要给云服务器的其他弹性网卡也分配 IPv6 地址，请参见[申请和释放 IPv6](#) 进行操作。

9. 登录云服务器配置 IPv6，由于各类云服务器操作系统配置 IPv6 的方式不同，详细操作方法请参见[Linux 云服务器配置 IPv6](#) 和 [Windows 云服务器配置 IPv6](#)。

步骤四：为云服务器的 IPv6 地址开通公网（可选）

- 登录[私有网络控制台](#)。
- 在左侧目录下选择 [IP 与网卡](#) > [弹性公网 IPv6](#)。
- 选择云服务器的所在地域，单击[申请](#)，进入管理页面。
- 勾选云服务器的 IPv6 地址、设置目标带宽上限，单击[提交](#)即可。

说明：

- 云服务器申请了 IPv6 地址后，默认关闭了公网访问能力，可通过弹性公网 IPv6 [管理 IPv6 公网能力](#)。
- 当运营商类型为 BGP 时，弹性公网 IPv6 地址即为云服务器获取到的 IPv6 地址，所以请确保云服务器已经获取到 IPv6 地址。
- 单次操作可支持最多100个 IPv6 地址同时开通公网，如果超过100个 IPv6 地址需要开通公网，请分多次操作。



← 申请弹性公网IPv6

① 运营商类型为BGP时，弹性公网IPv6地址即为网卡的IPv6地址。所以使用弹性公网IPv6前，请确保弹性网卡已经获取到IPv6地址。

地域

IP地址类型 普通IPv6 ①

运营商 BGP

计费模式 按流量

IP列表 请选择需要开通公网的IPv6地址 ①

请输入IP

☒ IPv6地址

所属网络

绑定资源

☒ 2002:...

vpc-6zk1uns7

ins-cz8f31cv

已选择 (1)

IPv6地址	所属网络	绑定资源
2002:...	vpc-6zk1uns7	ins-cz8f31cv

目标带宽上限

1 Mbps

25 Mbps

50 Mbps

75 Mbps

100 Mbps

1

+

Mbps

提交

取消

步骤五：配置 IPv6 的安全组规则

说明：

出入方向的安全组规则支持配置来源为单个 IPv6 地址或者 IPv6 CIDR，其中 `::/0` 代表所有的 IPv6 源地址。

1. 登录 [私有网络控制台](#)。

2. 在左侧目录下选择**安全 > 安全组**，在列表页中单击云服务器绑定的安全组 ID，进入详情页。

3. 选择**入站规则**并单击**添加规则**，添加 IPv6 的入方向安全组规则，单击**完成**即可。

添加入站规则

类型	来源 ①	协议端口 ①	策略	备注
自定义	::/0	all	允许	
+ 新增一行				

完成

取消

4. 选择**出站规则**并单击**添加规则**，添加 IPv6 的出方向安全组规则，单击**完成**即可。

版权所有：尚航云_V1

第12 页 共52页



添加出站规则

类型

目标 ①

协议端口 ①

策略

备注

自定义

::/0

all

允许

删除

+ 新增一行

完成

取消

步骤六：测试 IPv6 的连通性

说明：

- 如果是测试公网连通性，请确保已经开通公网。
- 如果是未开通公网使用 ssh 或远程桌面测试 IPv6 的连通性，可使用另一台处于同一私有网络的云服务器 ssh 或远程桌面被测试的云服务器。

Linux 云服务器

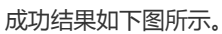
Linux 云服务器可通过 Ping 或 ssh 等操作来测试 IPv6 的连通性。

- 方式1：**通过 Ping 进行测试，操作如下：在云服务器中执行 ping6 IPv6地址 进行测试，例如， ping6 240c::6666 、 ping6 www.qq.com 、 ping6 同一私有网络下的 IPv6 地址 ，成功结果如下图所示：

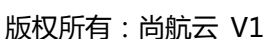
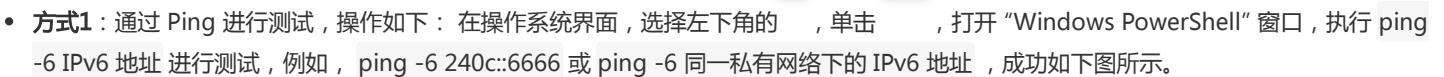
```
[root@VM_24_8_centos ~]# ping6 240c::6666
PING 240c::6666(240c::6666) 56 data bytes
64 bytes from 240c::6666: icmp_seq=1 ttl=53 time=29.1 ms
64 bytes from 240c::6666: icmp_seq=2 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=3 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=4 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=5 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=6 ttl=53 time=29.0 ms
^C
--- 240c::6666 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 29.011/29.055/29.162/0.049 ms
[root@VM_24_8_centos ~]# ping -6 www.qq.com
PING www.qq.com(2402:4e00:8010::154 (2402:4e00:8010::154)) 56 data bytes
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=1 ttl=56 time=3.49 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=2 ttl=56 time=3.48 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=3 ttl=56 time=3.49 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=4 ttl=56 time=3.50 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=5 ttl=56 time=3.49 ms
^C
--- www.qq.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 3.489/3.494/3.501/0.074 ms
[root@VM_24_8_centos ~]#
```

- 方式2：**通过 IPv6 地址 ssh 云服务器，操作如下：执行如下命令查看 IPv6 地址，并用 PuTTY 或者 Xshell 等软件，测试能否通过 IPv6 地址 ssh 到云服务器。

```
ifconfig
```



Windows 云服务器可通过 Ping 或远程桌面测试 IPv6 连通性。





- 方式2：通过 IPv6 地址进行远程桌面，远程桌面操作详情请参见使用远程桌面连接登录 Windows 实例。

附录

Linux 云服务器配置 IPv6

Linux 云服务器配置 IPv6 有两种方式：工具配置 和 手动配置。

- 工具配置通过工具一键配置 IPv6。
- 手动配置需要您对 Linux 命令有一定的熟练掌握程度。

请根据您的实际情况选择对应的方式，推荐您使用更高效的自动配置工具配置 IPv6 地址。

镜像类型	购买时间	是否已开启 IPv6	工具配置 (推荐)	手动配置
CentOS 7.5/CentOS 7.6	2019-06-30前购买	否	enable_ipv6 工具	如下列举了四种常用镜像的操作方法，若不满足您的需求，请提交 [工单申请] (http://console.cloud.sunhongs.com/workorder/category?step=0 target="_blank")： - 新购 CentOS 7.5/新购 CentOS 7.6 配置 IPv6 - CentOS 6.8 配置 IPv6 - CentOS 7.3/存量 CentOS 7.5/存量 CentOS 7.6 配置 IPv6 - Debian 8.2 配置 IPv6
	2019-06-30后购买	是	config_ipv6 工具	
CentOS 6/CentOS 7 (不含7.5/7.6) Ubuntu14.04/Ubuntu 12.04 Debian 8/Debian 9 CoreOS 17 Tencent Linux	2019-11-13 01:00前购买	否	enable_ipv6 工具	
	2019-11-13 01:00后购买	是	config_ipv6 工具	
FreeBSD、Suse、Ubuntu18	2019-11-13 01:00前购买	否	不支持	
	2019-11-13 01:00后购买	是		

工具配置



请根据云服务器是否已开启 IPv6 选择对应的配置方式：

- 未开启 IPv6 的云服务器：enable_ipv6 工具配置。
- 已开启 IPv6 的云服务器：config_ipv6 工具配置。

enable_ipv6 工具配置

enable_ipv6 工具可以为已分配 IPv6 地址的 CVM 实例一键配置 IPv6 地址。

使用限制

- enable_ipv6 工具仅适用于 VPC 网络环境下。
- enable_ipv6 工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

操作步骤

1. 登录云服务器，在云服务器中直接执行如下命令下载 enable_ipv6 工具：

```
wget https://iso-1251783334.cos.ap-guangzhou.myqcloud.com/scripts/enable_ipv6.sh
```

2. 赋予执行权限后使用管理员权限执行：

```
chmod +x ./enable_ipv6.sh
./enable_ipv6.sh [网卡名称]
# 示例 1：./enable_ipv6.sh eth0
# 示例 2：./enable_ipv6.sh eth1
```

3. （此步骤仅适用于 CoreOS 操作系统）重启云服务器，使上述配置生效。

config_ipv6 工具配置

config_ipv6 工具可以为已开启 IPv6 且已分配 IPv6 地址的 CVM 实例一键配置 IPv6 地址。

使用限制

- config_ipv6 工具仅适用于 VPC 网络环境下。
- config_ipv6 工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

操作步骤

1. 登录云服务器，在云服务器中直接执行如下命令下载 config_ipv6 工具：

```
wget https://iso-1251783334.cos.ap-guangzhou.myqcloud.com/scripts/config_ipv6.sh
```

2. 赋予执行权限后使用管理员权限执行：

```
chmod +x ./config_ipv6.sh
./config_ipv6.sh [网卡名称]
# 示例 1 : ./config_ipv6.sh eth0
# 示例 2 : ./config_ipv6.sh eth1
```

3. (此步骤仅适用于 CoreOS 操作系统) 重启云服务器, 使上述配置生效。

对于需要自动化配置 IPv6 实例的需求, 例如, 大批量配置, 建议您使用实例自定义数据配合脚本的方式来调用。详情请参见 [实例自定义数据](#)。如下为脚本示例 (假设是 RHEL 系列, Bash Shell 脚本)。

说明 :

该示例仅对 eth0 进行配置, 实际操作时注意修改为实际使用的网卡名。

```
#!/bin/sh
install_dir=/usr/sbin
install_path="$install_dir/config-ipv6
if [ ! -f "$install_path" ]; then
tool_url="https://iso-1251783334.cos.ap-guangzhou.myqcloud.com/scripts/config_ipv6.sh"
# download the tool
if ! wget "$tool_url" -O "$install_path"; then
echo "[Error] download tool failed, code $?"
exit "$?"
fi
fi
# chmod the tool
if ! chmod +x "$install_path"; then
echo "[Error] chmod tool failed, code $?"
exit "$?"
fi
# run the tool
$install_path eth0
```

手动配置

如下列举了四种常用的 Linux 云服务器的操作方法 :

- 新购 CentOS 7.5/新购 CentOS 7.6 配置 IPv6
- CentOS 6.8 配置 IPv6
- CentOS 7.3/存量 CentOS 7.5/存量 CentOS 7.6 配置 IPv6
- Debian 8.2 配置 IPv6

说明 :

- 新购 CentOS 7.5/新购 CentOS 7.6 指2019年06月30日后购买的云服务器。
- 存量 CentOS 7.5/存量 CentOS 7.6 指2019年06月30日前购买的云服务器。

新购 CentOS7.5 /新购 CentOS7.6 配置 IPv6

1. 进入 [云服务器控制台](#) 并登录实例。

新建

开机

关机

重启

续费

重置密码

更多操作

关键字用“”分隔，过滤标签用回车键分隔

Q

☐ 只看待回收实例

☐ ID/实例名	监控	状态	可用区	主机类型	配置	主IP地址	实例计费模式	网络计费模式	操作
☐ i-...	山	运行中		标准型S1	1 核 1 GB 1 Mbps 系统盘：高性能云盘 网络：andy-ipv6...	1	按量计费 2019-08-29 10:54创建	按流量计费	登录 更多

2. 执行如下命令，打开 /etc/sysconfig/network-scripts/ 文件夹下的 ifcfg-eth0 文件。

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

3. 按 “i” 切换至编辑模式，增加如下内容。

```
DHCPV6C=yes
```

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=52:54:00:06:d5:57
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
DHCPV6C=yes
```

4. 按 “Esc”，输入 “:wq”，保存文件并返回。

5. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
# 若云服务器有多个网卡，请执行 dhclient -6 网卡名称，如 dhclient -6 eth0
dhclient -6 或 dhclient -6 网卡名称
ifconfig
```

```
[root@VM_23_16_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 1 netmask 255.255.255.0 broadcast 1
    inet6 fe prefixlen 64 scopeid 0x20<link>
    inet6 2fe prefixlen 64 scopeid 0x0<global>
    ether 52:54:00:06:d5:b7 txqueuelen 1000 (Ethernet)
    RX packets 5581952 bytes 567752177 (541.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4779345 bytes 683082390 (651.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 18 bytes 1936 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1936 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

6. 执行如下命令，打开 `/etc/ssh/` 文件夹下的 `sshd_config` 文件。

```
vim /etc/ssh/sshd_config
```

7. 按 “i” 切换至编辑模式，删除对 `AddressFamily any` 的注释（即删除前面的 `#`），为 `ssh` 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

#Port 22
AddressFamily any
AddressFamily inet
ListenAddress 10.0.0.1
ListenAddress 10.0.0.2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

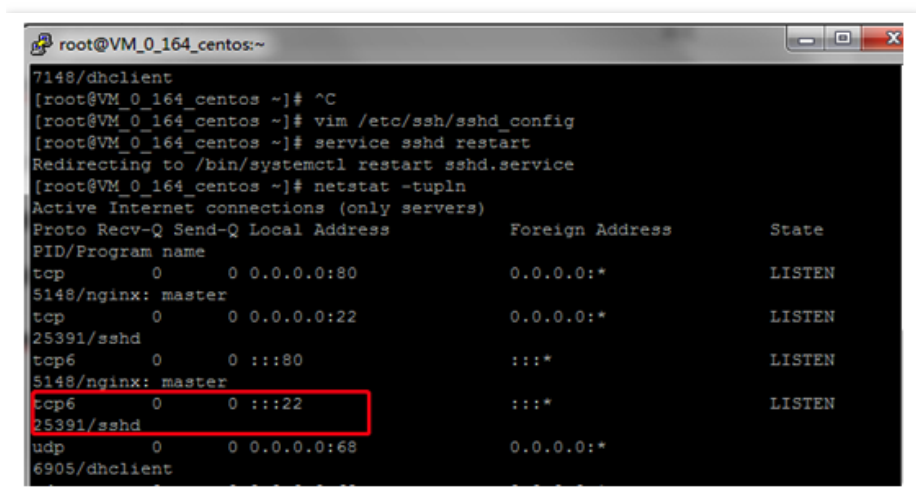
8. 按“Esc”，输入“:wq”，保存文件并返回。

9. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

10. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```

```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_centos ~]# netstat -tupln  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address          Foreign Address         State  
PID/Program name  
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                  :::*                     LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                  :::*                     LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68             0.0.0.0:*  
6905/dhclient
```

CentOS 6.8 配置 IPv6

1. 远程连接实例。具体操作，请参见[登录及远程连接](#)。

2. 检查实例是否已开启 IPv6 服务，执行如下命令：

```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

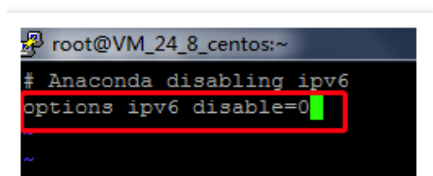
- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
- 若返回 inet6 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 第9步 继续操作。

3. 执行如下命令，打开 /etc/modprobe.d/ 文件夹下的 ipv6.conf 文件。

```
vi /etc/modprobe.d/ipv6.conf
```

4. 按 “i” 切换至编辑模式，将如下的内核参数设置为0。

```
options ipv6 disable=0
```



```
root@VM_24_8_centos:~  
# Anaconda disabling ipv6  
options ipv6 disable=0
```

5. 按 “Esc”，输入 “:wq”，保存文件并返回。

6. 执行如下命令，打开 etc 文件夹下的 sysctl.conf.first 文件。

```
vim /etc/sysctl.conf.first
```

7. 按 “i” 切换至编辑模式，将如下的配置文件参数设置为0。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
# Controls the console_loglevel for dmesg by tlinux team <t_os@tencent.com>
kernel.printk = 2

# disable ipv6 default by tlinux team <t_os@tencent.com>
net.ipv6.conf.all.disable_ipv6 = 0

net.ipv4.conf.all.promote_secondaries = 1
net.ipv4.conf.default.promote_secondaries = 1
net.ipv6.neigh.default.gc_thresh3 = 4096
net.ipv4.neigh.default.gc_thresh3 = 4096
kernel.sysrq = 1
kernel.shmmax = 68719476736
```

8. 按 “Esc”，输入 “:wq”，保存文件并返回。

9. 执行如下命令，打开 /etc/sysconfig/ 文件夹下的 network 文件。

```
vi /etc/sysconfig/network
```

0. 按 “i” 切换至编辑模式，增加如下内容。

```
NETWORKING_IPV6=yes
DHCPV6C=yes
```

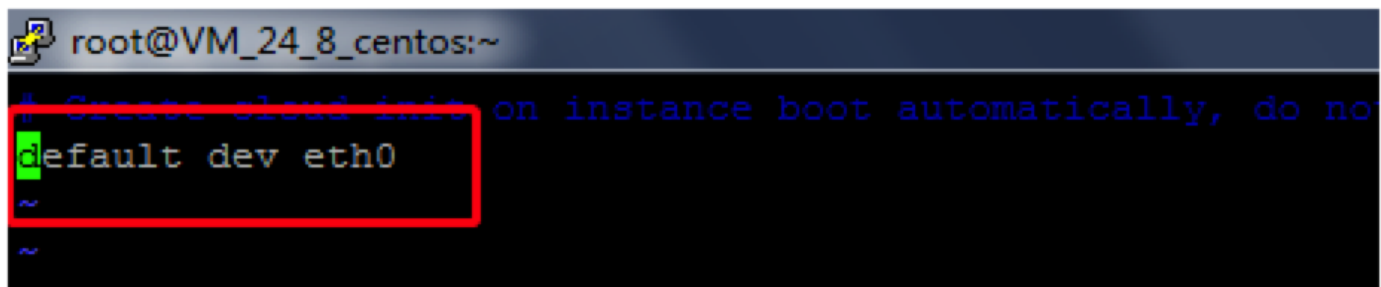
```
root@VM_24_8_centos:~
# Created by cloud-init on instance boot automatically, do not edit.
#
NETWORKING=yes
HOSTNAME=VM_24_8_centos
NETWORKING_IPV6=yes
DHCPV6C=yes
~
~
```

1. 按 “Esc”，输入 “:wq”，保存文件并返回。
2. 执行如下命令，打开或创建 `/etc/sysconfig/network-scripts/` 文件夹下的 `route6-eth0` 文件。

```
vim /etc/sysconfig/network-scripts/route6-eth0
```

3. 按 “i” 切换至编辑模式，增加如下内容，为网卡的 IPv6 添加默认出口。

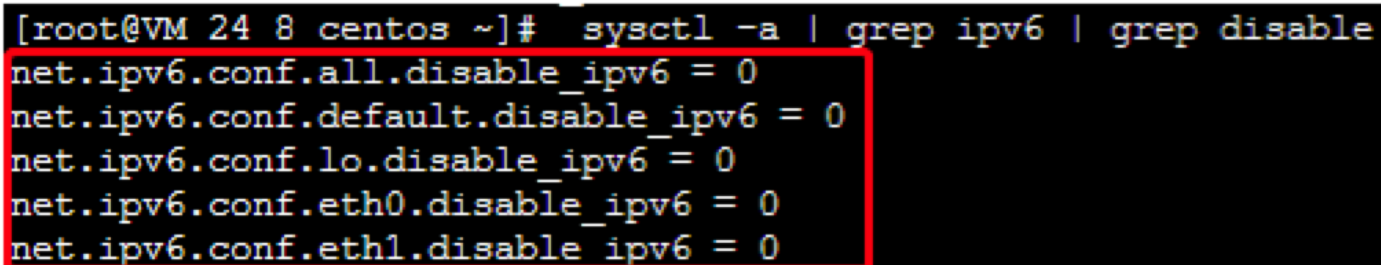
```
default dev eth0
```



```
root@VM_24_8_centos:~  
# Create cloud-init on instance boot automatically, do not  
default dev eth0  
~  
~
```

4. 按 “Esc”，输入 “:wq”，保存文件并返回。
5. 重启云服务器，仅通过 `service network restart`，IPv6 无法正常加载。
6. 执行如下命令查看重启后 IPv6 是否已经正常加载。

```
sysctl -a | grep ipv6 | grep disable
```



```
[root@VM 24 8 centos ~]# sysctl -a | grep ipv6 | grep disable  
net.ipv6.conf.all.disable_ipv6 = 0  
net.ipv6.conf.default.disable_ipv6 = 0  
net.ipv6.conf.lo.disable_ipv6 = 0  
net.ipv6.conf.eth0.disable_ipv6 = 0  
net.ipv6.conf.eth1.disable_ipv6 = 0
```

7. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
# 若云服务器有多个网卡，请执行 dhclient -6 网卡名称，如 dhclient -6 eth0  
dhclient -6 或 dhclient -6 网卡名称  
ifconfig
```

```
[root@VM_24_8_centos ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:75:F2:C0
          inet addr:10.23.24.8  Bcast:10.23.24.255  Mask:255.255.255.0
          inet6 addr: fe80::5c...:f2c0/64 Scope:Link
          inet6 addr: 2402::...:2be8/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4074 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2772 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:274150 (267.7 KiB)  TX bytes:260211 (254.1 KiB)

eth1      Link encap:Ethernet  HWaddr 20:90:6f:74:53:d7
          inet6 addr: 2402::...:575e/64 Scope:Global
          inet6 addr: fe80::...:3d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16124 (15.7 KiB)  TX bytes:696 (696.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

8. 执行如下命令，打开 `/etc/ssh/` 文件夹下的 `sshd_config` 文件。

```
vim /etc/ssh/sshd_config
```

9. 按 “i” 切换至编辑模式，删除对 `AddressFamily any` 的注释（即删除前面的 `#`），为 `ssh` 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
AddressFamily any
#AddressFamily inet
#ListenAddress 10.0.0.1
#ListenAddress 10.0.0.2
HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

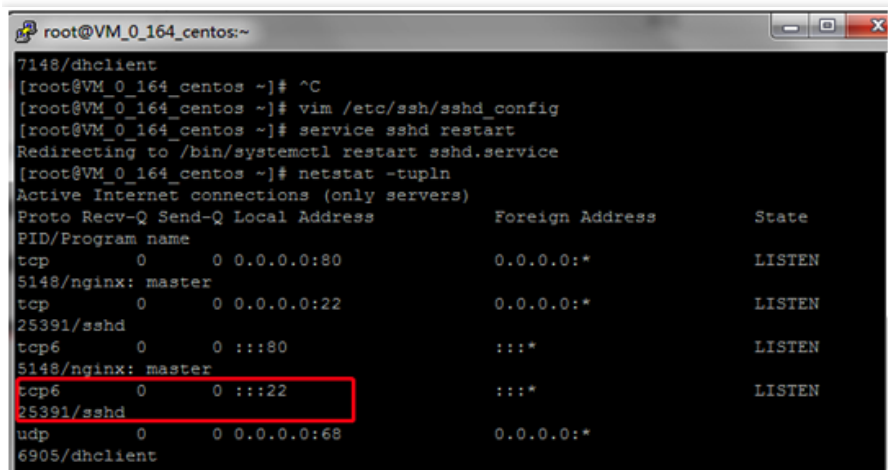
0. 按“Esc”，输入“:wq”，保存文件并返回。

1. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

2. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```



```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_centos ~]# netstat -tupln  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
PID/Program name  
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                  :::*                     LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                  :::*                     LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68             0.0.0.0:*  
6905/dhclient
```

CentOS 7.3/存量 CentOS 7.5/存量 CentOS 7.6 配置 IPv6

1. 远程连接实例。具体操作，请参见[登录及远程连接](#)。
2. 检查实例是否已开启 IPv6 服务，执行如下命令：

```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
- 若返回 `inet6` 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 第8步 继续操作。

3. 执行如下命令，打开 `etc` 文件夹下的 `sysctl.conf` 文件。

```
vim /etc/sysctl.conf
```

4. 按 “i” 切换至编辑模式，将如下的 IPv6 相关参数设置为0。

```
net.ipv6.conf.all.disable_ipv6 = 0  
net.ipv6.conf.default.disable_ipv6 = 0  
net.ipv6.conf.lo.disable_ipv6 = 0
```

```
# disable ipv6 default
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0

net.ipv4.conf.all.promote_secondaries = 1
net.ipv4.conf.default.promote_secondaries = 1
net.ipv6.neigh.default.gc_thresh3 = 4096
net.ipv4.neigh.default.gc_thresh3 = 4096

kernel.softlockup_panic = 1
kernel.sysrq = 1
vm.overcommit_memory = 1
```

5. 按“Esc”，输入“:wq”，保存文件并返回。

6. 执行如下命令，对参数进行加载。

```
sysctl -p
```

7. 执行如下命令，查看是否修改成功。

```
sysctl -a | grep ipv6 | grep disable
```

显示结果如下，则已成功修改。

```
"/etc/sysctl.conf" 45L, 1385C written
[root@VM_23_16_centos ~]# sysctl -a | grep ipv6 | grep disable
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.eth0.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.eth0.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0
[root@VM_23_16_centos ~]#
```

8. 执行如下命令，打开或创建 `/etc/sysconfig/network-scripts/` 文件夹下的 `ifcfg-eth0` 文件。

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

9. 按 “i” 切换至编辑模式，增加如下内容。

```
DHCPV6C=yes
```




2. 按 “i” 切换至编辑模式，增加如下内容，为网卡的 IPv6 添加默认出口。

```
default dev eth0
```



```
default dev eth0
```

```
~
~
~
~
"/etc/sysconfig/network-scripts/route6-eth0" 1L, 17C
```

3. 按“Esc”，输入“:wq”，保存文件并返回。

4. 执行如下命令，重新启动网卡。

```
service network restart
或者
systemctl restart network
```

5. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
# 若云服务器有多个网卡，请执行 dhclient -6 网卡名称，如 dhclient -6 eth0
dhclient -6 或 dhclient -6 网卡名称
ifconfig
```

```
[root@VM_23_16_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::208:5efe::1 prefixlen 64 scopeid 0x20<link>
    inet6 2001::18e prefixlen 64 scopeid 0x0<global>
    ether 52:54:00:06:d5:57 txqueuelen 1000 (Ethernet)
    RX packets 7400400 bytes 738255010 (704.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6293549 bytes 875070585 (834.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 18 bytes 1936 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1936 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@VM_23_16_centos ~]#
```

6. 执行如下命令，打开 /etc/ssh/ 文件夹下的 sshd_config 文件。

```
vim /etc/ssh/sshd_config
```

7. 按 “i” 切换至编辑模式，删除对 AddressFamily any 的注释（即删除前面的 #），为 ssh 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

#Port 22
AddressFamily any
AddressFamily inet
ListenAddress 10.0.0.1
ListenAddress 10.0.0.2

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

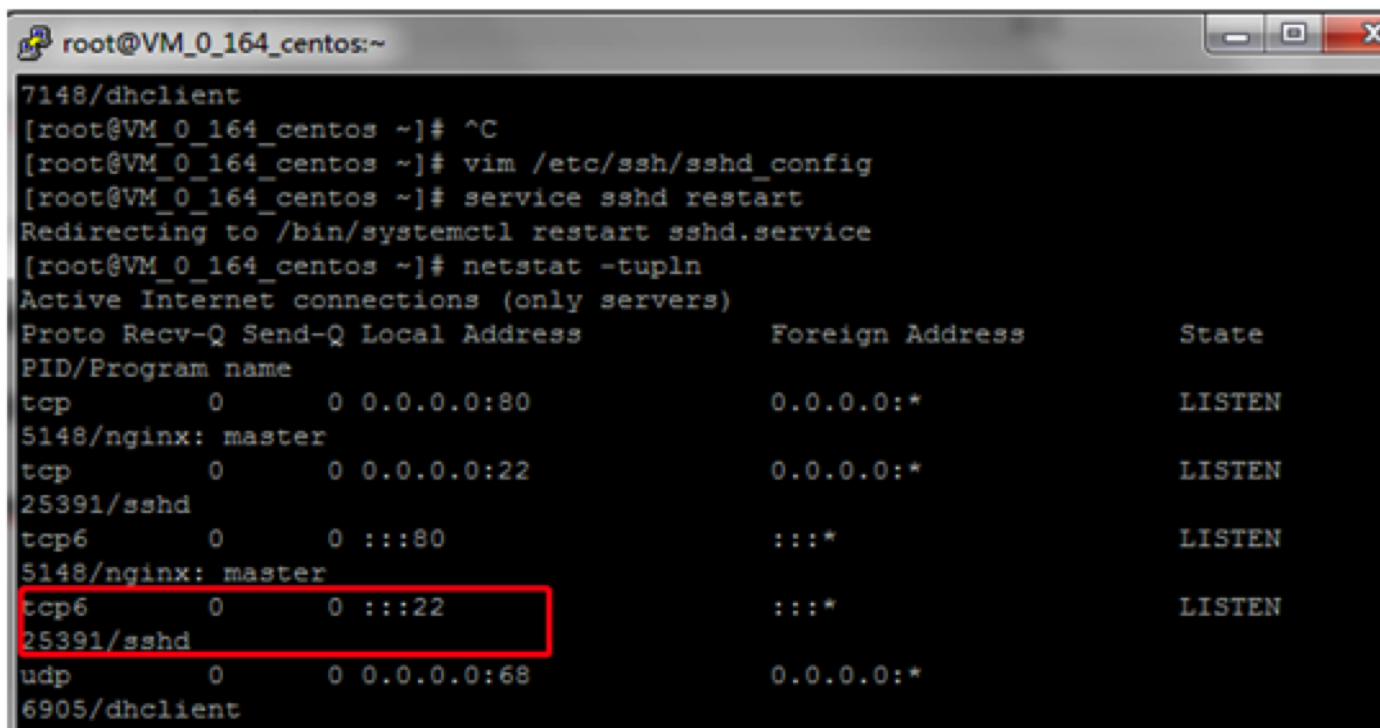
8. 按 “Esc”，输入 “:wq”，保存文件并返回。

9. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

10. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```



```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_centos ~]# netstat -tupln  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
PID/Program name  
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                 :::*                    LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                 :::*                    LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68            0.0.0.0:*  
6905/dhclient
```

Debian 8.2 配置 IPv6

1. 远程连接实例。具体操作，请参见[登录及远程连接](#)。

2. 检查实例是否已开启 IPv6 服务，执行如下命令：

```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
- 若返回 inet6 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 第6步 继续操作。

3. 执行如下命令，打开 etc 文件夹下的 sysctl.conf。

```
vim /etc/sysctl.conf
```

4. 按 “i” 切换至编辑模式，将如下的 IPv6 相关参数设置为0。

```
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
```

5. 按 “Esc”，输入 “:wq”，保存文件并返回。

6. 执行如下命令，对参数进行加载。

```
sysctl -p
```

7. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
# 若云服务器有多个网卡，请执行 dhclient -6 网卡名称，如 dhclient -6 eth0
dhclient -6 或 dhclient -6 网卡名称
ifconfig
```

```
root@VM-24-10-debian:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:bf:8a:4a
          inet addr:10.10.10.10  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::219:0:0:0/64 Scope:Link
          inet6 addr: 2001:::2/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12457 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11235 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1404471 (1.3 MiB)  TX bytes:1213697 (1.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

8. Debian 8.2 系统默认为 ssh (22端口) 开启 IPv6 监听，无需特殊配置，您可执行如下命令，进行查看。

```
netstat -tupln
```

```
root@VM-24-11-debian:~# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      349/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      664/exim4
tcp6       0      0 :::22                   :::*                     LISTEN      349/sshd
tcp6       0      0 :::1:25                  :::*                     LISTEN      664/exim4
udp        0      0 0.0.0.0:68              0.0.0.0:*               254/dhclient
udp        0      0 0.0.0.0:25284            0.0.0.0:*               4189/dhclient
udp        0      0 0.0.0.0:24313            0.0.0.0:*               254/dhclient
```

9. 执行如下命令，配置默认路由。

```
ip -6 route add default dev eth0
```

Windows 云服务器配置 IPv6

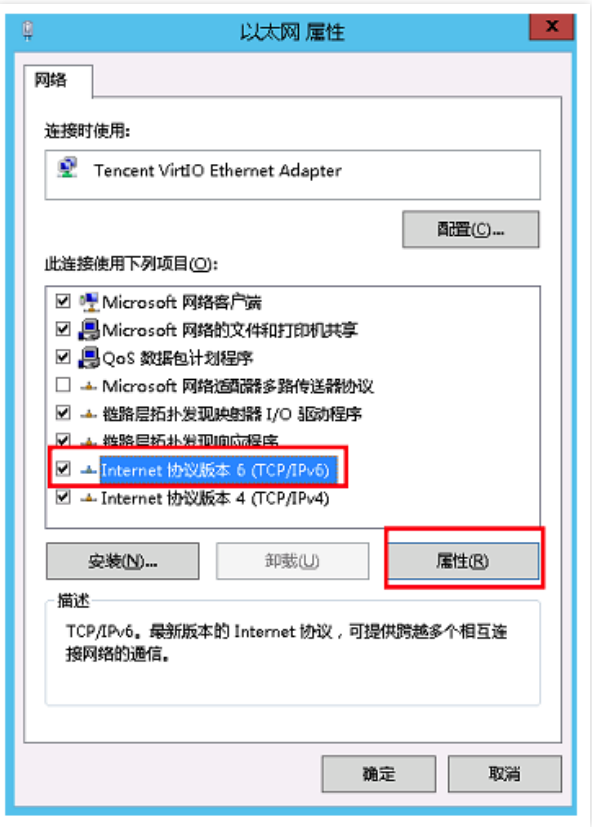
如下操作以 Windows 2012 为例：

1. 登录云服务器实例，进入操作系统的**控制面板** > **网络和 Internet** > **网络和共享中心**，单击命名为“以太网”的网卡进行编辑。

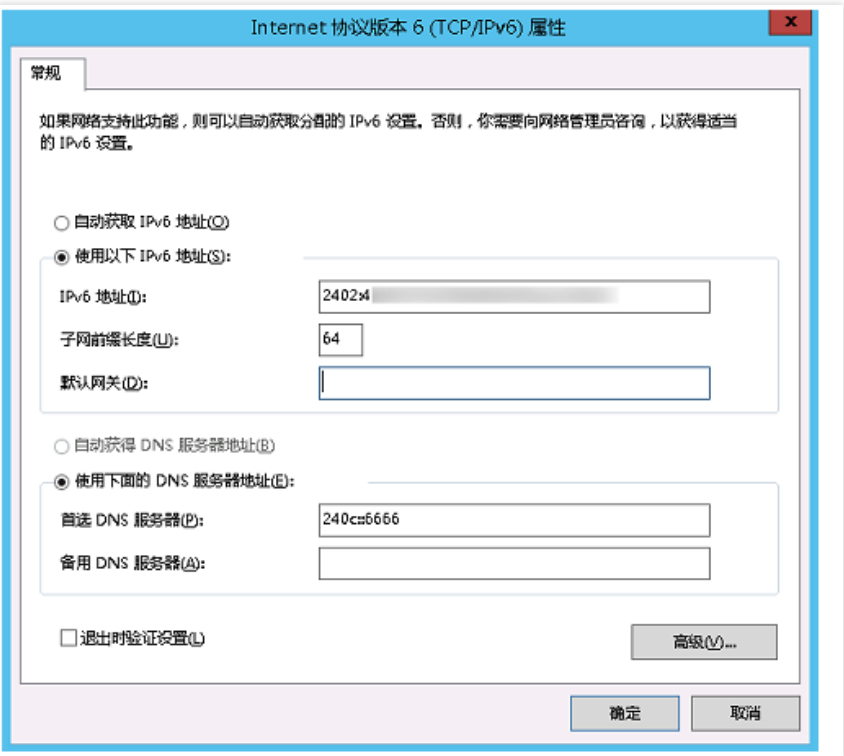


2. 在“以太网状态”弹窗中，单击**属性**。

3. 在“以太网属性”弹窗中，选中 **Internet 协议版本 6 (TCP/IPv6)** 并单击**属性**。



4. 在“Internet 协议版本 6 (TCP/IPv6) 属性”弹窗中，手工输入 步骤三 中云服务器获取到的 IPv6 地址并设置 DNS（推荐使用 240c::6666 ），单击**确定**。





5. 在操作系统界面，选择左下角的 ，单击 ，打开“Windows PowerShell”窗口，依次执行如下命令配置默认路由以及查看 IPv6 地址。

```
netsh interface ipv6 add route ::/64295985640140800 "以太网"  
ipconfig
```

```
PS C:\Users\Administrator> netsh interface ipv6 add route ::/0 "以太网"  
确定。  
PS C:\Users\Administrator> ipconfig  
Windows IP 配置  
  
以太网适配器 以太网：  
连接特定的 DNS 后缀 . . . . . :  
IPv6 地址 . . . . . : 240  
本地链接 IPv6 地址. . . . . : fe8  
IPv4 地址 . . . . . : 10  
子网掩码 . . . . . : 255.255.255.0  
默认网关. . . . . : ::  
10.23  
  
隧道适配器 isatap.{A971A  
媒体状态 . . . . . : 媒体已断开  
连接特定的 DNS 后缀 . . . . . :
```



操作指南

私有网络分配与释放 IPv6 CIDR

最近更新时间: 2024-08-23 15:08:00

1. 登录 [私有网络控制台](#)。
2. 在“私有网络”列表上方，选择【地域】，将会展示所属地域下的所有私有网络信息。
3. 在需要开启 IPv6 的 VPC 所在行的操作栏下，单击【获取IPv6地址】，系统将为该 VPC 分配1个 /56 的 IPv6 CIDR。
4. 如该IPv6地址处于闲置状态，则可以单击操作列中的【释放IPv6地址】，系统将释放该 VPC 的 IPv6 CIDR。

私有网络 									
新建 搜索私有网络的名称/ID									
ID/名称	IPv4 CIDR	IPv6 CIDR	外部扩展CIDR	组播	子网	路由表	云主机	默认私有网络	操作
vpc-6zk1uns7 TomVPC		2002:c... 	无		1	1	1 	否	编辑扩展CIDR 释放IPv6地址 删除



子网分配与释放 IPv6 CIDR

最近更新时间: 2024-08-23 15:08:00

1. 登录 [私有网络控制台](#)。
2. 在左侧目录单击【子网】，在“子网”列表上方，选择【地域】和【私有网络】，将会展示所属地域和私有网络下的所有子网信息。
3. 选择一个子网，单击【分配 IPv6 CIDR】，系统将为该子网分配1个 /64 的 IPv6 CIDR。

子网 TomVPC										
新建 搜索子网名称/ID										
ID/名称	所属网络	IPv4 CIDR	IPv6 CIDR	类型	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-dvy94sa8 A	vpc-6zk1uns7 TomVPC			普通子网		rtb-l5nc4yb2 default	0	253	否	分配IPv6 CIDR 删除

4. 选择一个已获取到 IPv6 CIDR 的子网，单击【释放 IPv6 CIDR】并确定操作，系统将回收该子网的 IPv6 CIDR。

子网 全部私有网络										
新建 搜索子网名称/ID										
ID/名称	所属网络	IPv4 CIDR	IPv6 CIDR	类型	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-dvy94sa8 A	vpc-6zk1uns7 TomVPC		2002:::1:::1	普通子网		rtb-l5nc4yb2 default	1	252	否	释放IPv6 CIDR 删除



弹性网卡申请与释放 IPv6 地址

最近更新时间: 2024-08-23 15:08:00

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 单击需要查看的实例 ID，进入详情页。
4. 选择【IPv6 地址管理】标签页，单击【分配 IP】申请 IPv6 地址。



5. 在弹窗中单击【确定】。



6. 在“IPv6 地址管理”标签页中，您可看到系统已为弹性网卡分配一个 IPv6 地址。



←

ENI

基本信息

IPv4 地址管理

IPv6 地址管理

关联安全组

i

IPv6地址不占用弹性网卡的内网IP配额,每个弹性网卡最多支持一个IPv6地址

分配IP

IP	操作
2002: :bcee	释放

7. 您可以通过单击操作栏下的【释放】，释放 IPv6 地址。

说明：

释放前，请先关闭该 IPv6 地址的公网。

←

j

基本信息

IPv4 地址管理

IPv6 地址管理

关联安全组

分配IP

IP	备注	操作
2:	-	释放



管理 IPv6 公网

最近更新时间: 2024-08-23 15:08:00

开通 IPv6 公网

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【IP 与网卡】>【弹性公网 IPv6】。
3. 选择需要开通 IPv6 公网的地域单击【申请】，进入“申请弹性公网IPv6”页面。
4. 勾选云服务器的 IPv6 地址、设置目标带宽上限，单击【提交】即可。

说明：

- 云服务器申请了 IPv6 地址后，默认关闭了公网访问能力，可通过弹性公网 IPv6 [管理 IPv6 公网](#) 能力。
- 当运营商类型为 BGP 时，弹性公网 IPv6 地址即为云服务器获取到的 IPv6 地址，所以请确保云服务器已经获取到 IPv6 地址。
- 单次操作可支持最多100个 IPv6 地址同时开通公网，如果超过100个 IPv6 地址需要开通公网，请分多次操作。

← 申请弹性公网IPv6

① 运营商类型为BGP时，弹性公网IPv6地址即为网卡的IPv6地址，所以使用弹性公网IPv6前，请确保弹性网卡已经获取到IPv6地址。

地域

IP地址类型

运营商

计费模式

IP列表

普通IPv6 ①

BGP

按流量

请选择需要开通公网的IPv6地址 ①

请输入IP

☒ IPv6地址

所属网络

绑定资源

2002:...

vpc-6zk1uns7

ins-cz8f31cv

已选择 (1)

IPv6地址

所属网络

绑定资源

2002:...

vpc-6zk1uns7

ins-cz8f31cv

目标带宽上限

1 Mbps

25 Mbps

50 Mbps

75 Mbps

100 Mbps

1

Mbps

提交

取消

关闭 IPv6 公网

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【IP 与网卡】>【弹性公网 IPv6】。

版权所有：尚航云_V1

第42 页 共52页



3. 在弹性公网 IPv6 列表页，勾选需要关闭公网的 IPv6 地址，并单击【释放】。

弹性公网IPv6

弹性公网IPv6帮助文档

申请

释放

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

☒ ID	IP地址	监控	运营商	EIP状态	私有网络	弹性网卡	绑定资源	计费模式	带宽上限	操作
☒ eip-ga4r6dyz	2aa0...		BGP	BIND_ENI		eni-4		按流量	2 Mbps	调整宽带

共 1 条

20 条 / 页

1

/ 1 页

4. 在弹窗中核对信息并单击【确定】，即可释放弹性公网 IPv6。释放弹性公网 IPv6 后，对应的 IPv6 地址将关闭公网访问。

关闭公网

您已选择1个IPv6地址关闭公网访问，执行此操作后所选择的IPv6将无法访问公网，但内网通信不受影响。

序号	IPv6地址	绑定资源
1	2aa0...	-

确定

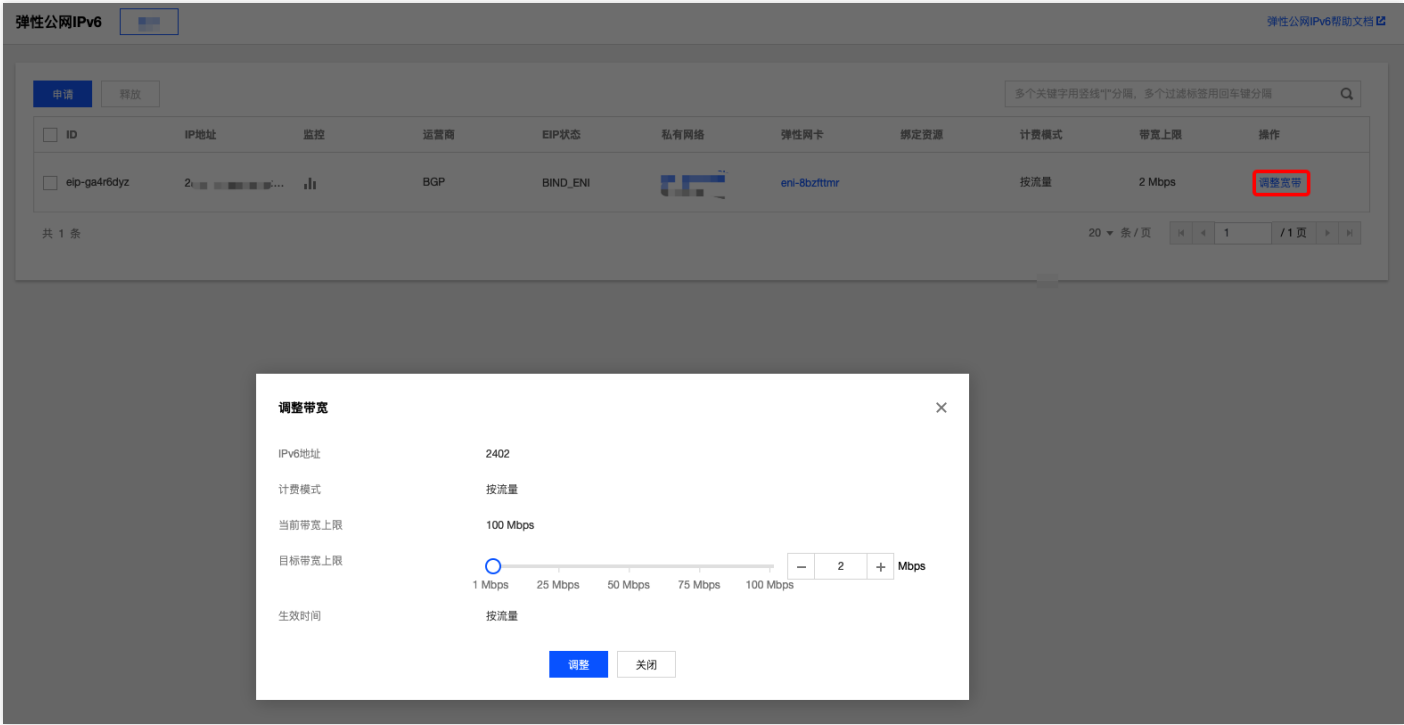
取消

调整 IPv6 公网带宽

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【IP 与网卡】>【弹性公网 IPv6】。



3. 在单个弹性公网 IPv6 的操作栏下，单击【调整带宽】。



4. 在弹出的【调整带宽】对话框中，修改该弹性公网 IPv6 的公网带宽上限并单击【调整】即可。



常见问题

通用类

最近更新时间: 2024-08-23 15:08:00

什么是弹性公网 IPv6 ?

云服务器或者弹性网卡获取到 IPv6 地址后，默认关闭了 IPv6 公网能力。通过弹性公网 IPv6，您可以：

- 实时管理云服务器或者弹性网卡提供 IPv6 公网接入。
- 选择单个 IPv6 地址开通公网，也可以批量选择多个 IPv6 地址开通公网。
- 在开通公网后，设置公网带宽、查看监控、关闭公网等。

弹性公网 IPv6 和弹性公网 IP (EIP) 有何区别 ?

云服务器可以同时获取 IPv6 和 IPv4 地址，并运行 IPv6 和 IPv4 双栈。

- 通过绑定 EIP 来开通 IPv4 公网，IPv4 EIP 是独立的公网地址，使用 NAT 来实现公网访问。
- 通过弹性公网 IPv6 来开通 IPv6 公网，弹性公网 IPv6 是基于弹性网卡上的 IPv6 内网地址实现，不使用 NAT。

云服务器开通 IPv6 公网需要具备哪些条件 ?

云服务器开通 IPv6 公网需要具备如下条件：

1. 云服务器所在的 VPC 和子网分别获取 IPv6 CIDR。
2. 云服务器所关联的弹性网卡（包括主网卡和辅助网卡）获取 IPv6 地址。
3. 为弹性网卡的 IPv6 开启公网。

IPv6 公网通信是否已默认支持 DDoS 防护 ?

所有开通 IPv6 公网的云服务器都默认支持 IPv6 DDoS 防护。

IPv6连通性故障排查

最近更新时间: 2024-08-23 15:08:00

操作场景

本文将为您提供云服务器的 IPv6 连通性问题的基本排障思路。

操作步骤

首先通过如下四个步骤检查云服务器是否已经完成 IPv6 配置：

1. 执行如下命令，查看云服务器的网卡（通常是 eth0）是否已经获取到“fe80”开头的 link-local IPv6 地址。

- 若已获取表明该镜像已经开启了 IPv6 功能，请执行 [步骤2](#)。
- 若未获取，请参见 [解决思路-步骤1](#)。

说明：

“fe80”开头的 IPv6 地址并非是由于通信的 IPv6 地址。

ifconfig

```
[root@VM_27_11_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.1 netmask 255.255.255.0 broadcast 10.1.1.255
    inet6 fe80::50cc: prefixlen 64 scopeid 0x20<link>
    ether 52:54:00:bf:40:cc txqueuelen 1000 (Ethernet)
    RX packets 6532919 bytes 605487045 (577.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6530588 bytes 804198603 (766.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@VM_27_11_centos ~]#
```

2. 执行如下命令，查看云服务器的网卡（通常是 eth0）是否已经获取到“2402”开头的 IPv6 地址（不是“fe80”开头的地址）。

- 若已获取，请执行 [步骤3](#)。
- 若未获取，请参见 [解决思路-步骤2](#)。

```
ifconfig
```

```
[root@VM_0_8_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 17.17.17.1 netmask 255.255.255.0 broadcast 17.17.17.255
    inet6 fe80::5054:1:1:1 prefixlen 64 scopeid 0x20<link>
    inet6 2402:4e1::1::1 e0 prefixlen 64 scopeid 0x0<global>
    ether 52:54:00:63:13:96 txqueuelen 1000 (Ethernet)
    RX packets 4055775 bytes 363959444 (347.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4059357 bytes 564490360 (538.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@VM_0_8_centos ~]#
```

3. 执行如下命令，查看网卡的默认路由。

- 若已配置默认路由且能 Ping 通公网，请执行 [步骤4](#)。
- 若看不到默认路由，或无法 Ping 通公网，请参见 [解决思路-步骤3](#)。

```
ip -6 route show
```

```
[root@VM_23_16_centos ~]# ip -6 route show
unreachable :::/96 dev lo metric 1024 error -113 mtu 65536
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:a00::/24 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:7f00::/24 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:a9fe::/32 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:ac10::/28 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:c0a8::/32 dev lo metric 1024 error -113 mtu 65536
unreachable 2002:e000::/19 dev lo metric 1024 error -113 mtu 65536
2402:4e00:1400:1240::/64 dev eth0 proto kernel metric 256 mtu 1464
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -113 mtu 65536
fe80::/64 dev eth0 proto kernel metric 256 mtu 1464
default dev eth0 metric 1024 mtu 1464
```

通过 ping6 240c::6666 或者 ping -6 240c::6666 来测试公网连通性。

```
[root@VM_24_8_centos ~]# ping6 240c::6666
PING 240c::6666(240c::6666) 56 data bytes
64 bytes from 240c::6666: icmp_seq=1 ttl=53 time=45.8 ms
64 bytes from 240c::6666: icmp_seq=2 ttl=53 time=45.3 ms
64 bytes from 240c::6666: icmp_seq=3 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=4 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=5 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=6 ttl=53 time=45.3 ms
```

4. 执行如下命令，确认是否22端口和80端口都已经监听了 IPv6。如果22端口和80端口没有监听 IPv6，请参见 [解决思路-步骤4](#)。

```
netstat -tupln
```

```
[root@VM_23_4_centos ~]# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      3204/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1159/sshd
tcp6       0      0 0 :::80                  :::*                   LISTEN      3204/nginx: master
tcp6       0      0 0 :::22                  :::*                   LISTEN      1159/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*               *          914/dhclient
udp        0      0 10.24.23.4:123          0.0.0.0:*               *          636/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*               *          636/ntpd
udp6       0      0 fe80::5054:ff:fe:fa::546 :::*                   *          3066/dhclient
udp6       0      0 2402:4e00:1400:1240:123 :::*                   *          636/ntpd
udp6       0      0 fe80::5054:ff:fe:fa::123 :::*                   *          636/ntpd
udp6       0      0 ::1:123                 :::*                   *          636/ntpd
[root@VM_23_4_centos ~]#
```

解决思路

1. 如果通过 `ifconfig`，没有看到“fe80”开头的 IPv6 地址，则说明云服务器没有开启 IPv6 功能。请参见 [快速入门 - 云服务器配置 IPv6](#)，选择您所需的镜像开启 IPv6 的方式重新配置，可以通过执行 `sysctl -a | grep ipv6 | grep disable` 来确认。

2. 如果通过 `ifconfig`，没有看到“2402”开头的 IPv6 地址，则有两种可能性：

i. 控制台云服务器的弹性网卡没有分配 IPv6 地址，解决方法是进入控制台为弹性网卡分配 IPv6 地址，详情请参见 [弹性网卡申请与释放 IPv6 地址](#)。

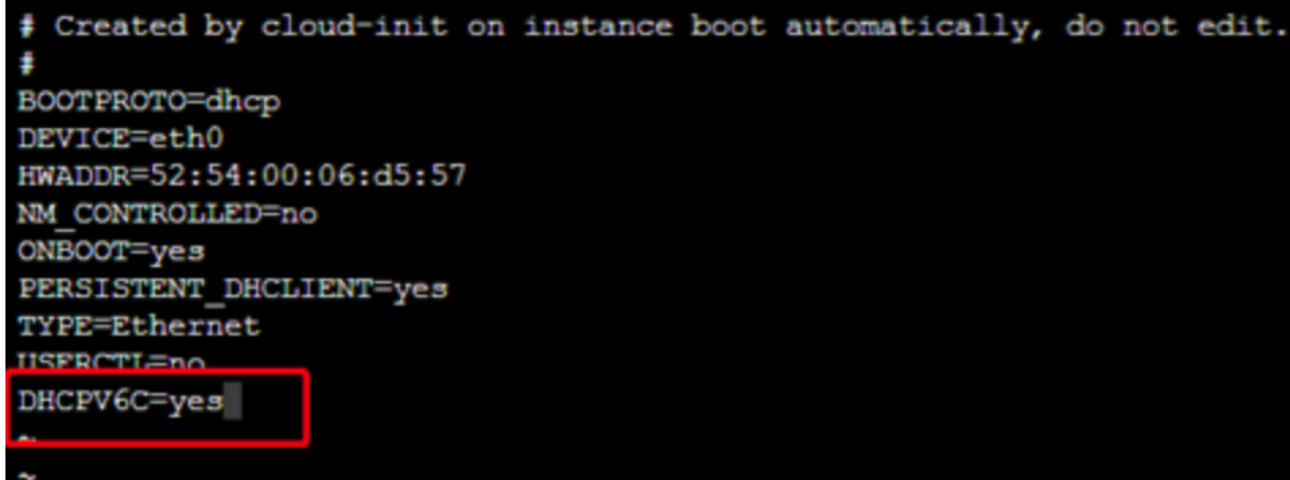
ii. 云服务器内的 `dhcpcv6` 相关配置没有配置好或者没有执行 `dhclient -6`。请登录云服务器：

a. 执行如下命令，打开 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件。

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

b. 按 “i” 切换至编辑模式，增加如下内容。

```
dhcpcv6=yes
```



```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=52:54:00:06:d5:57
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
DHCPV6C=yes
```

c. 按 “Esc”，输入 “:wq”，保存文件并返回，重启云服务器。

d. 依次执行如下命令，查看是否已经获取到“2402”开头的 IPv6 地址。

```
# 若云服务器有多个网卡，请执行 dhclient -6 网卡名称，如 dhclient -6 eth0
dhclient -6 或 dhclient -6 网卡名称
ifconfig
```

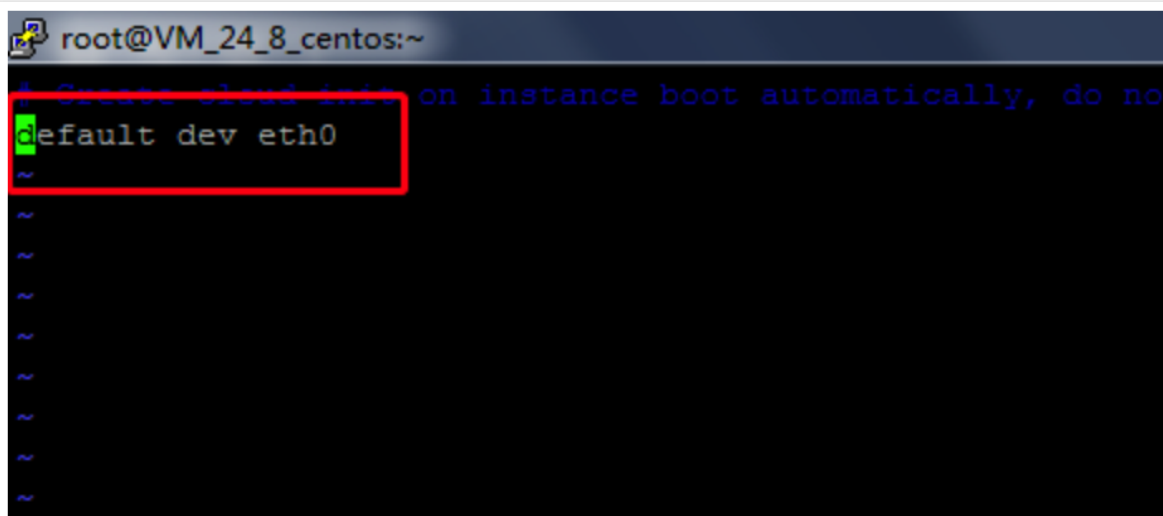
3. 如果已经获取到 IPv6 地址，但是无法 Ping 通公网，则有两种可能性：

- i. 没有为 IPv6 地址开启公网，解决方法是进入控制台为 IPv6 地址开启公网，详情请参见 [管理 IPv6 公网](#)。
- ii. 没有配置默认路由，通过 `ip -6 route show` 查看是否已经配置默认路由。如果看不到默认路由，则需要：
 - a. 执行如下命令，打开 `/etc/sysconfig/network-scripts/` 文件夹下的 `route6-eth0` 文件。

```
vim /etc/sysconfig/network-scripts/route6-eth0
```

- b. 按 “i” 切换至编辑模式，增加如下内容。

```
default dev eth0
```



- c. 按 “Esc”，输入 “:wq”，保存文件并返回，执行如下命令重启网络服务，或者重启云服务器。

```
service network restart  
或者  
systemctl restart network
```

- 4. 如果 IPv6 公网可以 Ping 通，但是无法通过22或者80端口来访问，则通常是 sshd 和 Nginx 等文件配置问题，需要修改 sshd 和 Nginx 配置，使22或者80等端口监听 IPv6。配置完成后：

- i. 依次执行如下命令，重启 sshd 和 Nginx 服务。

```
service sshd restart  
service nginx restart
```



```
[root@VM_23_9_centos ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@VM_23_9_centos ~]# service nginx restart
Redirecting to /bin/systemctl restart nginx.service
[root@VM_23_9_centos ~]#
```

- ii. 通过执行 `netstat -tupln` 查看22或者80等端口是否已监听 IPv6，可参见上文 [操作步骤-步骤4](#)。



词汇表

最近更新时间: 2024-08-23 15:08:00

私有网络

私有网络 (Virtual Private Cloud , VPC) 是一块您在云平台上自定义的逻辑隔离网络空间，与您在数据中心运行的传统网络相似。私有网络可以同时开通 IPv4 和 IPv6 双栈。

子网

一个私有网络由至少一个子网组成，子网的 CIDR 必须在私有网络的 CIDR 内。私有网络中的所有云资源（如云服务器、云数据库等）都必须部署在子网内。子网可以同时开通 IPv4 和 IPv6 双栈。

弹性网卡

弹性网卡是绑定私有网络 (Virtual Private Cloud , VPC) 内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡可以同时获取 IPv4 地址和 IPv6 地址。

云服务器

云服务器 (Cloud Virtual Machine , CVM) 为您提供安全可靠的弹性计算服务。云服务器可以运行 IPv4 和 IPv6 双栈，云服务器的 IPv6 地址通过关联的弹性网卡获取。

全球单播地址

全球单播地址 (Global Unicast Address , GUA) 等同于 IPv4 中的公网地址，可以在 IPv6 Internet 上进行全局路由和访问。这种地址类型允许路由前缀的聚合，从而限制了全球路由表项的数量。