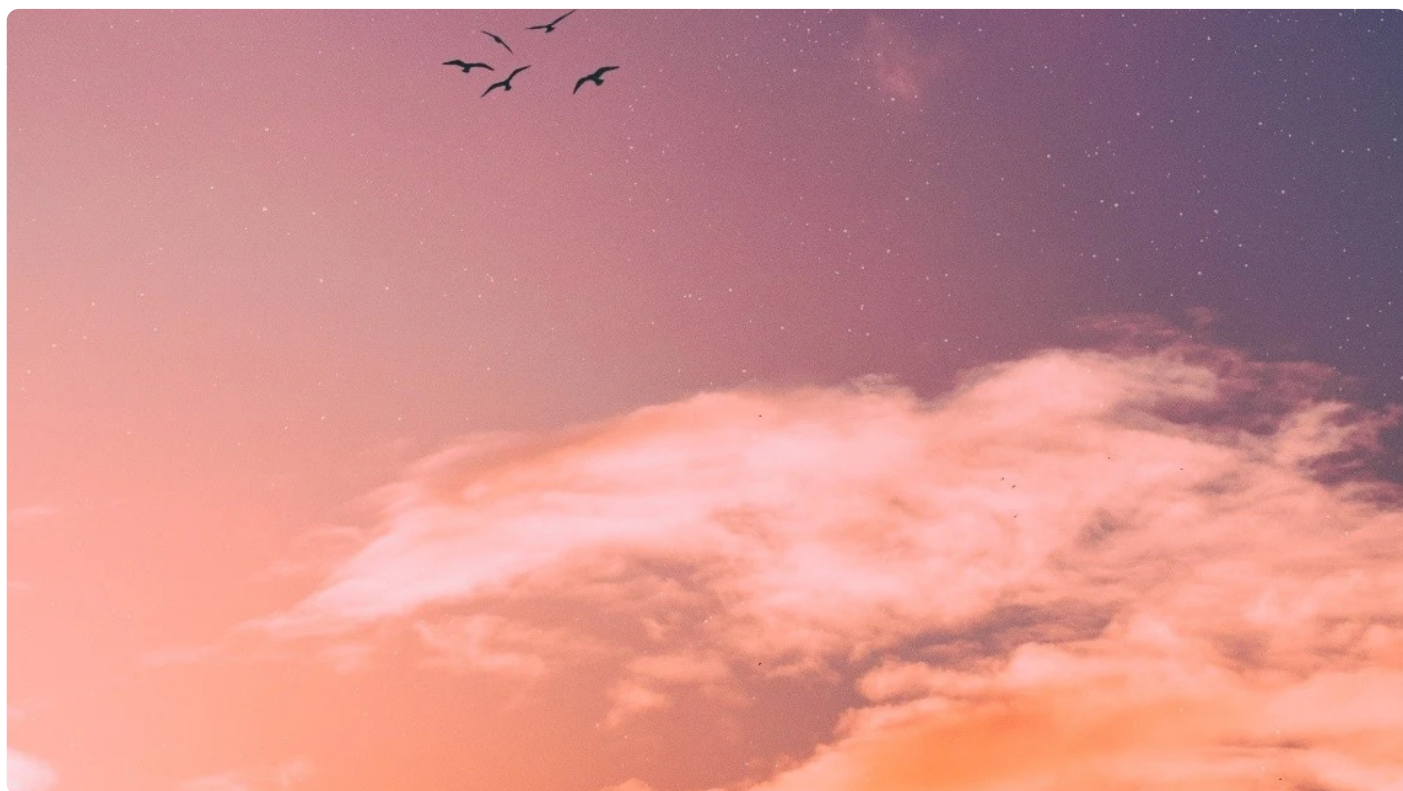


06 | 云上虚拟网络：开合有度，编织无形之网

2020-03-16 何恺铎 来自北京

《深入浅出云计算》



你好，我是何恺铎。

我们对于 IaaS 的介绍已经渐入佳境了。前面，我们主要涉及了与云虚拟机相关的计算和存储方面的内容。今天这一讲，我想要和你讨论的，则是“计算 / 存储 / 网络”三要素中的最后一项：**网络**。

在互联网时代，网络的重要性不言而喻，我们必须好好掌握。通过合理的网络拓扑设置，既能够帮助我们实现架构上的隔离性和安全性，又能够让各组件互联互通、有序配合。

不过网络对于许多开发者而言，有时会让人感觉是一个挺困难的话题。它复杂的设置、晦涩的术语，尤其是各种连而不通的场景，可能让你望而生畏。

请你不要担心，云上的网络经过了一定程度的抽象以后，已经为我们屏蔽了一定的复杂度。只要宏观的思路梳理得足够清晰，你很快就能够理解云上的网络组件，并让它们听你指挥、投入

使用。

什么是虚拟私有网络？

虚拟私有网络（Virtual Private Cloud，简称 VPC），是云计算网络端最重要的概念之一，它是指构建在云上的、相互隔离的、用户可以自主控制的私有网络环境。虚拟私有网络有时也称为专有网络（阿里云）或虚拟网络（Virtual Network 或 VNet，Azure 的叫法）。

上面的概念解释也许不太好理解，其实用通俗的话来讲，**私有网络就是一张属于你自己的内网**。内网之中的服务器和设备，可以比较自由地互相通信，与外界默认是隔离的。如果外部互联网，或者其他虚拟网络需要连接，则需要额外的配置。

所以说，虚拟私有网络，就是你在云上的保护网，能够有效地保护网内的各种设施。有的时候，你可能还要同时创建多个虚拟网络，让它们各司其职，实现更精细的隔离。

小提示：在一些云上，除了私有网络，你可能还会看到“经典网络”的选项。这是上一代的云上内网基础设施，虽然它配置起来相对简单，但在隔离性、可配置性上有许多局限。现在已不推荐使用了。

虚拟私有网络麻雀虽小，但五脏俱全。在传统数据中心里，经典网络架构中的概念和组件，在虚拟网络中你几乎都能找到对应。这里比较重要的一些概念包括：

网段，私有网络的内部 IP 区段，通常用 CIDR 形式来表达，如 192.168.0.0/16。

子网，私有网络的下级网络结构，一个私有网络可以划分多个子网，这和通常意义上的子网也是对应和一致的。阿里云中把子网形象地称为“交换机”。

路由表，用于定义私有网络内流量的路由规则，决定着数据包的“下一跳”去向何方。每个子网都必须有一张关联的路由表，通常情况下，系统会自动帮你创建一个默认的路由表。

网关，是对进出私有网络的流量进行把守和分发的重要节点，根据用途的不同，有多种类型，后面我们还会讲到。

安全组，私有网络里虚拟机进出流量的通行或拦截规则，可以起到虚拟机网络防火墙的作用，我们曾经在 [🔗 第 2 讲](#)中提到过它。

所以在创建虚拟网络时，你就需要对上面这些重要属性进行按需设定。

下面，我就以**阿里云 VPC** 为例，来带你实际操作体验一下。

首先，我们来到阿里云的专有网络管理控制台，选择新建一个 VPC，这里的**网段**我们选择 **192.168.0.0/16**：

专有网络

地域
华东2（上海）

● **名称** ?

test-vpc1 9/128 ✓

● **IPv4网段** ?

☒ 推荐网段
☐ 高级配置网段

192.168.0.0/16 ▼

⚠ 一旦创建成功，网段不能修改

描述 ?

极客时间测试vpc 9/256

资源组

默认资源组 ▼

注意：VPC 属于局域网，按照 RFC 规范，能够使用的 IPv4 区段必须为 192.168.0.0/16、172.16.0.0/12、10.0.0.0/8 这三个或它们的子集。

同时，我们还**至少要创建一个子网**，也就是交换机。我们选择一个子 IP 段 192.168.0.0/24，并且设置所属可用区为 “**可用区 D**”：

交换机

名称 ?

test-vpc1-vsw1

14/128 ✓

可用区 ?

上海 可用区D



可用区资源 ?

ECS ✓

RDS ✓

SLB ✓

IPv4网段

192

.

168

.

0

.

0

/

24



⚠ 一旦创建成功，网段不能修改

可用IP数

252

描述 ?

测试vpc下的交换机1

11/256

我们再来创建另外一个交换机，网段设置为 192.168.1.0/24。这里的关键在于，我们可以让第二个交换机位于另外一个可用区 E：

创建交换机 ② 如何创建交换机

资源组

全部

• 专有网络

test-vpc1/vpc-uf6irhi8124x59al68761

网段

192.168.0.0/16

IPv6网段 ?

[开通IPv6](#)

• 名称 ?

test-vpc1-vsw2

14/128

• 可用区 ?

上海 可用区E

可用区资源 ?

ECS

RDS

SLB

• IPv4网段

192

.

168

.

1

.

0

/

24

一旦创建成功，网段不能修改

可用IP数

252

这就说明，**我们可以建立跨可用区，也就是跨同区域内不同数据中心的私有网络**。这是 VPC 的一个强大的特性，能够为我们私有网络的高可用性提供保障。比如，你可以让主力集群在一个可用区工作，备用集群在另一个可用区随时待命，需要时迅速切换；你也可以把流量同时分发到不同的可用区，动态控制分发策略。

就这样，我们收获了一个包含两个交换机的 VPC。

实例ID/名称	网段	状态	默认专有网络	路由表	交换机
vpc-uf6irhi8124x59al68761  test-vpc1	192.168.0.0/16	● 可用 ● 未绑定云企...	否	1	2

实例ID/名称	所属专有网络	状态	IPv4网段	可用IP数
vsw-uf6ls7t8l8lpt35c6a37u  test-vpc1-vsw2	vpc-uf6irhi8124x59al68761  test-vpc1	● 可用	192.168.1.0/24	251
vsw-uf6nbt7032jedor7jbnnf  test-vpc1-vsw1 	vpc-uf6irhi8124x59al68761  test-vpc1	● 可用	192.168.0.0/24	252

查看一下它的路由表，你可以发现，它自动为我们包含了两个子网的路由信息：

路由条目列表						已绑定交换机
<div> <div>添加路由条目</div> <div>刷新</div> <div>导出</div> </div>						
目标网段	状态	下一跳	类型	描述	操作	
192.168.0.0/24	● 可用	-	系统			
192.168.1.0/24	● 可用	-	系统			
100.64.0.0/10	● 可用	-	系统			

你看，创建 VPC 其实并不困难。这里的关键还是要规划好 VPC 和各子网的网段，需要让它们既有足够的地址空间以供资源拓展，又不要安排得范围过大，以免和其他 VPC 或公司内部网络产生地址冲突，为后续的网间互联带来不必要的麻烦。

如果你在没有 VPC 的情况下直接创建虚拟机，公有云一般都会为你自动生成 VPC。在生产环境中，我强烈地建议你**不要让系统自动建立 VPC**，而是像我们上面的做法，先自行建立好 VPC，配置好子网和网段等重要参数，然后再创建云虚拟机“入住”。**因为这样，你会事先让自己有一个明确的网络规划，对整个 VPC 的把控和理解也会更强。**

私有网络中的虚拟机

让我们回到虚拟机的视角。当一个虚拟网络已经存在时，我们就可以将新创建的虚拟机放置在这个虚拟网络中。

那么，这个所谓的“放置”是怎么真正产生的呢？虚拟机和专有网络的连接点在哪里呢？

答案就在于虚拟机的**网卡**，又称弹性网卡（Elastic Network Interface，简称 ENI）。虚拟机的网卡一方面是和虚拟机的本体进行绑定，另一方面则嵌入某个私有网络的子网，也会拥有至少一个私网 IP。

云上的网卡，之所以被称为“弹性”网卡，是因为它具备以下特征：

1. 一个虚拟机可以绑定多块网卡，有主网卡和辅助网卡之分；
2. 一块网卡隶属于一个子网，可以配置同一子网内的多个私有 IP；
3. 辅助网卡可以动态解绑，还能够绑定到另一台虚拟机上。

这再次体现了云计算的解耦特征，在某些场景下是非常有用的。比如，有一台服务线上流量的机器，而且线上流量导向的是它的辅助网卡，那么当这台机器因故无法正常工作时，你在排查问题的同时可以考虑这样一个应急的办法：将这台机器的辅助网卡迅速解绑，并重新绑定到待命的备用机上。这样就能够比较快地先恢复对外服务。

当你在创建虚拟机的时候，向导会询问你，这台虚拟机属于哪个 VPC，以及 VPC 下的哪个子网？现在你就理解了，**这个选项的实质性结果，就是新虚拟机自动生成的主网卡，接入了所选 VPC 的所选子网。**

好了，网卡和私有 IP 的部分你应该已经比较清楚了。那么你可能会问，**公有 IP 呢？**这正是我想说的另一个比较关键的部分。

在绝大多数的云上，创建虚拟机时都会有一个选项，问你“是否同时为虚拟机分配一个公网 IP 地址”。如果你选择“是”，这样机器启动后，就会拥有一个自动分配的公网地址，便于你从自己的电脑连接到这个实例。这在很多时候都是最方便的选择。

公网 IP

公网带宽计费

✓ 分配公网IPv4地址

系统会分配公网 IP，也可采用更加灵活的弹性公网 IP 方案。

但对于生产环境，我的推荐是，**尽量不要使用和依赖这个自动生成的公有 IP**。因为它本质上是一个从公有云的 IP 池中**临时租用**给你的 IP。如果你的机器关闭或重启，下次获得的 IP 可能就完全不同了。

这时，我们真正应该用到的是**弹性 IP**（Elastic IP），有些云称为 eIP。弹性 IP 一旦生成，它所对应的 IP 是固定、不会变化的，而且完全属于你所有。这非常适合需要稳定 IP 的生产环境。

请不要被它的名字迷惑，它所谓的弹性，其实是指可以**非常自由地解绑和再次绑定到任意目标**。你本质上是买下了这个 IP 的所有权，将这个 IP 赋予谁，是你的权利，而且你还可以动态按需切换。

所以，当你有一个域名，需要让 DNS 服务解析到某个外部 IP，你就应该建立一个弹性 IP，绑定到相关资源后，让域名解析到这个弹性 IP，而不应该使用虚拟机自动匹配的公有 IP。因为后者是不稳定的。

好，让我们继续进入实验的部分。我们在刚才的 VPC 内来建立一台虚拟机，起名为 vm1-in-vpc1，把它放置到位于可用区 E 的第二个交换机中，并且选择**不自动生成公有 IP**。

<input type="checkbox"/> 实例ID/名称	可用区 ▾	IP地址	状态 ▾	网络类型 ▾	配置	专有网络属性
<input type="checkbox"/> i-uf67dkl0049u0sm2vdqs vm1-in-vpc1  	  华东 2 可用区 E	192.168.1.80(私有)	 运行中	专有网络	2 vCPU 8 GiB (I/O优化) ecs.g6.large 0Mbps (峰值)	vpc-uf6irhi8124x59a168761 vsw-uf6ls7t8l8lpt35c6a37u

注意，**这时它只有私有 IP，我们怎么连接它呢？**我们可以创建一个弹性 IP，然后绑定到这台实例：

<input type="checkbox"/> 实例ID/名称	IP地址	监控	带宽	线路类型	状态(全部) ▾	操作
<input type="checkbox"/> eip-uf6026fr8c0w3amydydwa eip1-for-vpc1 	 47.102.139.39		1 Mbps 按使用流量计费	BGP (多线)	 可用	绑定 解绑 更多操作 ✓

IP地址:

47.102.139.39

● 实例类型

ECS实例

资源组

全部

● ECS实例 ?

vm1-in-vpc1/i-uf67dkl0049u0sm2vdqs

只有处于运行中和已停止状态的云服务器实例可以绑定弹性公网IP

绑定之后，就自然可以连上刚才的这台虚拟机了。注意 VM 列表界面会有相应的显示：

<input type="checkbox"/> 实例ID/名称	可用区 ▼	IP地址
<input type="checkbox"/> i-uf67dkl0049u0sm2vdqs	华东 2 可用区 E	47.102.139.39(弹性)
<input type="checkbox"/> vm1-in-vpc1		192.168.1.80(私有)

尝试 SSH 连接一下，一切正常：

[复制代码](#)

```
1 client@clientVM:~$ ssh root@47.102.139.39
2 root@47.102.139.39's password:
3 Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)
4 * Documentation:  https://help.ubuntu.com
5 * Management:    https://landscape.canonical.com
6 * Support:       https://ubuntu.com/advantage
7 Welcome to Alibaba Cloud Elastic Compute Service !
8 root@vm1-in-vpc1:~#
```

如何让私有网络对外“开口子”？

在阿里云上，如果一台云虚拟机没有被赋予公有 IP，默认情况下它就失去了访问外网的能力，只能进行内网通信，这在很多时候，的确是我们想要的安全控制。但也有一些情况，我们希望内网的机器和外界并不完全隔离，一些互联网流量需要有序地引进来，一些内网机器也需要访问外网。

这就是一个如何在 VPC 上“开口子”的问题了。

当然，你可以使用前面提到的弹性 IP，绑定到相关虚拟机上。不过，如果我们需要访问外网的虚拟机数量有很多，这种办法就需要很多弹性 IP，管理上就太麻烦了，成本也不划算。还有一个问题是，弹性 IP 带来的是双向的开放，有时我们只想允许单向的连接。

这就是**网关**可以大显身手的场景了，它正是用来统一协调管理私有网络与外部通信的组件。随着各个公有云的发展，云上也延伸出了许多不同形式、解决不同目的的网关产品。

我们这里讨论一个常见的场景，即**如何允许多台没有公有 IP 的虚拟机访问外网**。这时需要使用到的网关叫做 **NAT** (Network Address Translation) 网关，是一种常见的用来给 VPC 开口的手段。

我们继续以阿里云为例，来看下**如何通过 NAT 网关让虚拟机访问外网**。

我们可以事先把弹性 IP 从刚才那台虚拟机解绑，这下它现在又无法访问外网了：

复制代码

```
1 root@vm1-in-vpc1:~# curl myip.ipip.net
2 curl: (7) Failed to connect to myip.ipip.net port 80: Connection timed out
```

接着我们创建一个 NAT 网关实例，并选择它对应的 VPC，然后把刚才解绑的弹性 IP(47.102.139.39) 绑定到 NAT 网关上：

实例ID/名称	监控	最大带宽	规格/类型	专有网络	状态	付费类型	计费方式	弹性公网IP
ngw-uf67sm234nlzw641chy15 nat-for-vpc1		不涉及	小型普通型	vpc-uf6irhi8124x59al68761 test-vpc1	可用	后付费	按规格计费	47.102.139.39

这里的关键之处在于**接下来我们要添加的 SNAT 条目**。

SNAT 是“源地址转换”的意思，它非常适合让私有网络的主机共享某个公网 IP 地址接入 Internet。注意，**这是一种从内向外的、单向的连通形式**。

创建SNAT条目

① 如何管理与创建 SNAT

X

i

SNAT条目帮助您构建VPC内云产品访问互联网的二维度：
1. 交换机 粒度：指定交换机下的ECS通过配置的公网IP访问互联网
2. ECS 粒度：指定的ECS通过配置的公网IP访问互联网

使用须知：

1.用于创建DNAT条目的公网IP地址，将不能用来创建SNAT条目
2.NAT网关配置的公网IP数限制NAT网关的最大并发数，绑定单个IP最大连接数为55000，当通过NAT网关访问公网上同一个目的IP和端口的带宽大于2Gbps时，建议您为NAT网关绑定4-8个公网IP并构建SNAT IP池，避免单IP的端口数量限制可能产生的丢包
3.SNAT规则配置后，ECS没有优先使用SNAT IP主动访问互联网，请参考[统一公网出口IP](#)来优化您的网络架构

交换机粒度

ECS粒度

* 交换机

test-vpc1-vsw2

▼

指定交换机下的ECS将通过配置的公网IP访问互联网

交换机网段

192.168.1.0/24

* 公网IP地址

47.102.139.39

X

▼

选择多个IP地址配置SNAT IP地址池时，请确保每个IP地址在一个共享带宽中

条目名称 ②

snat-for-vsw2

13/128

确定

取消

⊞

上面我们添加了一个 SNAT 条目，让整个交换机 “test-vpc1-vsw2” 下的网段都共享一个出口公网 IP。你要注意，**我们的虚拟机是位于这个网段内的。**

接着再回到这台虚拟机内，我们通过 curl 命令，尝试对外访问：

 复制代码

```
1 root@vm1-in-vpc1:~# curl myip.ipip.net
2 当前 IP: 47.102.139.39 来自于: 中国 上海 上海 阿里云/电信/联通/移动/铁通/教育网
```

很棒，这回成功地连通了。而且外部网站也显示，我们正在使用的外网 IP 正是那个弹性 IP(47.102.139.39)。这就是对于 NAT 网关的一个小小实验了。

还有一种网关被称为 **VPN 网关**，也可以帮助外界连接到 VPC，它本质上是基于你所熟知的 VPN 技术。由于 VPN 能够基于互联网提供私有加密的通信，因此非常适合用来从任意其他私有设施安全地连接到 VPC。这些私有设施可以小到一台个人电脑或手机终端，也可以大到是你本地的数据中心，还可以是另一个 VPC。

多网连接有哪些方式？

前面我们主要是从单个 VPC 的角度来进行讨论的，那么最后，我们再来讨论一下多 VPC 的场景。**公有云上允许你同时使用多个 VPC 的，这样你可以构建更加复杂的网络架构，实现模块隔离和跨区域扩展等高级需求。**

如果是云端 VPC 和 VPC 的互联，我首先推荐的就是**对等连接**（VPC Peering）的方式。它能够在不添加额外设备的情况下，让两个 VPC 无缝地互联起来，而且操作非常简单，对等连接甚至还能够支持跨区域的私有网络互联。当然，对等连接的实施前提，是这两个 VPC 的网段没有交集，不存在冲突。

这里你需要注意对等连接的一个特点，就是它不具备传递性。也就是说，如果 A 和 B 建立了对等连接，B 和 C 建立了对等连接，那么 A 和 C 是不相通的。这是对等连接的一个局限。

如果你真的需要多个 VPC 间任意路径的互联互通，那么可以考虑使用比对等连接更为复杂和强大的**专用网络设施**，比如 AWS 的 Transit Gateway，和阿里云的云企业网，它们能够帮助搭建更为复杂的多 VPC 网络拓扑结构，也允许进行更精细的路由设置。如有需要，建议你仔细阅读厂商的文档进行学习和研究。

公有云中的私有网络，还可以和企业本地数据中心进行互联，形成**混合云架构**。你可以先考虑使用 VPN 这种轻量化的方式，通过公网线路为两边建立连接渠道。但如果应用场景要求保证延迟和带宽，一般就需要专线进行连接了。绝大多数的云厂商，都提供了云端区域和本地数据中心进行高速互联的服务和解决方案，比如 AWS 的 Direct Connect、Azure 的 ExpressRoute 和阿里云的“高速通道”（云下 IDC 专线接入）等等。一般专线还会和 VPN 一起组合使用，来保证通道的高可用性。

小提示：与较为易用的 VPC 互联相比，混合云的构建是一项较为复杂的工程，通常需要由本地机房、云厂商、电信运营商三方配合进行，也牵涉到本地数据中心端的网络规划和路由设备适配。这超出了我们开发者课程的范畴。如需实施，建议你仔细咨询云厂商工作人员。

课堂总结与思考

今天，我主要为你介绍了云上虚拟网络，包括它的具体组成、使用场景和连接性问题。我还给你推荐了一些在生产环境下的最佳实践。

从某种程度上来说，虚拟私有网络的“仿真度”非常高，在软件定义网络（SDN）技术的加持下，甚至比物理网络还要更加灵活高效，更易于扩展。所以，**通过合理的规划和设置，云端的网络基础设施能够让我们拥有一个健壮而强大的网络拓扑结构，对于流量的引导和控制，也完全能够做到因势利导、开合有度。**

需要特别说明的是，在主体理念保持一致的情况下，各个云厂商在具体实现上，其实是各显神通的，会有一些细节存在差异。这是正常的现象，请你在实践时注意。比如说，和阿里云不同，AWS 的 VPC 中访问外网，需要经由专门的 Internet Gateway 来通行流量，路由表中也需要进行相应的设置。

好了，今天我给你留下的思考题是：

在虚拟私有网络的内部，两机互联的带宽有多大呢？可能受到哪些因素的影响？

在今天的实验中，我们通过 NAT 网关实现了流量“出网”的目的。那么，如果是反过来需要引导外界流量进入 VPC，应该使用什么方式呢？

欢迎你在留言区和我互动，我会一起参与讨论。如果觉得有收获，也欢迎你把这篇文章分享给你的朋友。感谢阅读，我们下期再见。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

精选留言 (25)



何恺铎 置顶

2020-04-18

[上讲问题参考回答]

1. 在一些云平台上，已经能够支持云硬盘的在线扩容了，所属VM可以不用停机。但需要注意，扩容操作不会直接改变文件系统和分区等设置，扩容后一般需要在操作系统内进行分区的扩展或新增。
2. EFS/NAS类云产品也能够以磁盘形式挂载到云虚拟机。这类存储产品的特点，在于虚拟出的磁盘可以跨多个虚拟机进行文件共享，同时容量上限很高，可以轻松突破原来的单盘极限。

共 1 条评论 >

👍 8



我来也 置顶

2020-03-17

我把弹性网卡和辅助私网IP用起来了.可以解决我工作中的一个实际问题.

我测试用的k8s工作节点,由于都是抢占付费模式按需购买,所以IP经常会发生变动.

如果k8s中的部分服务要对外暴露, 就会遇到IP地址经常发生变动的情况.

之前我的解决方案是给k8s中的Service配置为LoadBalancer的方式,这样服务对外暴露的IP地址就不会变化了.

但是一个阿里云账户,默认创建的上限是50个负载均衡.

而我测试的服务,完全没有必要用这种额度.

我现在就用辅助私网IP, 实现了每次新建k8s工作节点时,都可以用同一个IP访问到k8s集群服务.

这样我就可以指定k8s中的Service配置为NodePort的方式.不用再占负载均衡的额度.
k8s集群外一样可以用固定的IP和端口,访问k8s里面的服务了.

作者回复: 赞!

共 3 条评论 >

👍 8



leslie 置顶

2020-03-16

目前云计算的很多概念确实让我们在使用的时候会难以弄清,通过课程的学习梳理应当可以达到与私有云思维的对比和学习,课程听到现在觉得不少核心的思路与原理还是有相似之处。两机互联的带宽应当很大-相当于两台设备之间拉了一根网线。影响的因素应当在网卡,虚拟交换机。

至于第二个问题在课程中有"AWS 的 Direct Connect、Azure 的 ExpressRoute 和阿里云的"高速通道"不知道是否是相应的答案,这块自己还待更多的实践去摸索提升。
谢谢老师今天的分享,期待后续课程的学习。

作者回复: 影响的因素在于机器的配置,一般来说机器配置越高,其内网带宽也越大。你可以仔细留心,很多云都会给出机型的内网带宽。

第二个问题主要依靠负载均衡等手段,下一讲我们会涉及。高速通道等主要用于私网连通,和外网没有关系。



👍 1



怀朔

2020-03-16

1、

1.1 两机之间 小的那台机器带宽情况

1.2 其影响因素:

两台机器同时发送和接收情况

不同可用区网络抖动?

2、“入网”方式

2.1 通过dnat进来

2.2 文中介绍绑定eip (弹性ip)

2.3 通过slb 引流

作者回复: 堪称完美的回答!

共 2 条评论 >

👍 11



我来也

2020-03-16

刚才在手机上编辑的一大段,因为提示有敏感词,大部分都丢失了,现在在电脑上再手敲一下.😭

自从本专栏出来后, 每天都是盼着更新! 😊

vpc内两机互联, 带宽和影响因素。

首先的瓶颈在购买的云主机可支持的最大网络带宽。

(我看到的云主机网络上限有0.8G、1G、1.5G这些规格。)

其次看两机所处的网络位置。

如果两机处在同区域的可可用区, 那爽歪歪, 很容易达到网卡上限, scp速度可以到100MB/s+。(这里是大写的B)

如果是同区域不同可用区, 网络速度也还行, 能不能到机器上限还不确定, 收不收费也不确定。

如果是不同可用区, 可能带宽和速度又会降低些。好像还收费。

再次看"邻居"

在云上, 毕竟是共享的。

如果同网络设备(如交换机)中的其他用户也是大量的占用带宽, 也可能会影响你的速度。

导入流量到vpc, 应该就是靠nat网关的dnat功能了。

关于阿里的nat网关我有话说

阿里云的nat网关, 我也是最近两三天才有所了解, 原因是他对个人不太友好。最低规格的按量付费都是每天12元, 个人平常尝试的少。

但是它的功能确实强大, 可以跨可用区, 单IP的带宽可以达到200Mb/s。

还可以很方便的添加和绑定弹性ip。

现在云厂商的文档是真的详细, 还都是中文的, 哈哈。

个人疑问

虚拟弹性网卡

之前只见有些虚拟机可以绑定数十张辅助网卡, 不知有何用。

看了老师的文章, 发现这里原来还可以这么用. 我再去研究系按官方的文档。

不同用户的vpc互联

之前只见阿里有提到,不同用户的vpc也可以互联,没实操过.
看了老师的文章,说还可以用VPX代理的方式打通不同vpc.
那就说明这个打通还真是可行的了.

我的场景是这样的,老师先来帮忙分析下整体的可行性.只需要最终的结果,不需要分析过程.
我想自己账户下的vpc,与公司的vpc能互联.如果能复用公司的nat网关就更好了.

我的应用场景是:

自己购买云主机,加入到企业的k8s测试集群中.以便在不需要的时候可以随时释放.
用企业的子账号购买云主机,需要有相关的权限,怕BOSS不放心.
自己搭建的k8s测试集群,除了需要支付nat网关的费用,还无法与其他依赖服务互相通讯,没有实际的意义.

看了老师的文章,才去尝试云主机的抢占付费模式,真的是爽歪歪.
阿里云4CPU32G的配置,0.2元/小时不到的价格,持续用了周末的两个白天.

作者回复: 回答得非常好, 赞一个!

关于你的场景, 跨账号的VPC互联, 在阿里云上是能够通过“云企业网”实现的, 参见 https://help.aliyun.com/document_detail/65901.html 。但如果想复用NAT网关, 可能还需要额外的转发或路由设置。你可以实操一下, 必要时可以联系阿里云客服确认。

共 2 条评论 >

👍 8



我来也

2020-03-28

今天周末,趁机在阿里云上体验了一把<云企业网>,确实方便和强大.
可以跨账号私网互通.
本身不收费,同地区还免流量费!

确实可以实现之前的愿望:

自己账号下的实例加入到企业账户下的k8s集群.
由于涉及企业账户,所以小试了一把后就移除了<云企业网>.

有了它,可玩的方式确实多起来了.
还可以异地跨账号互通.就是要购买流量包了.



5



一天到晚游泳的鱼

2020-03-25

看到ip, 会变吓了我一跳, 第一次注意这个问题, 我们公司现在用腾讯云有十几台云主机, 没有用弹性ip, 只用买的时候固定分配的, 三年来, 重启了几十次, ip并没有有变化过, 查了下资料, 也说不会主动释放, 您说的这个包括腾讯云吗

作者回复: 不同云的公有IP调度策略细节可能有不同, 当然一般来说如果只是重启, 换IP的可能性还是相当小的。但大多数云如果是机器关机一段时间再启动, 就很有可能换IP了。是否更换IP还可能会和你的机器是包年包月, 还是按量付费有关系。

腾讯云的具体行为可以再咨询一下客服, 以官方回复为准。但无论如何, 依赖弹性IP一定是最安全的。可以考虑把你们公司环境中最关键的几个IP转化为弹性IP。

共 4 条评论 >

2



我来也

2020-03-18

说个糗事.

今天测试辅助私网IP, 换了个系统, 之前是在CentOS上弄的, 今天是在Ubuntu 18.04上弄的. 官方的文档只支持Ubuntu 14/16. 结果我自己折腾时, 可能配置配错了. 重启网卡后, 与服务器就失去了相应, 重启了也无法恢复. 最后只能重置服务器.

幸好这个服务器在昨天晚上把上面的东西弄走了, 要不然就悲剧了. 哈哈.

作者回复: "上面的东西"一般丢不了的, 即便机器无法启动或无法连接, 可以把云盘卸下来, 挂载到其他正常机器来挽救。

共 2 条评论 >

2



Helios

2020-03-16

1. 申请虚拟机的时候能指定需要多少带宽的虚拟机 (1 Gbps、1 .5Gbps...10Gbps) , 影响的因素个人觉得主要有两个: 一、云虚拟机的带宽是独占的还是共享的, 明显独占的是更快的;

二、虚拟机之间的距离，是同可用区 > 同区域不同可用区 > 不同区域

2. 可以使用DNAT网关，也可以找一台有公网ip的虚拟机作为堡垒机，通过这台机器去进去VPC，还有直接给绑定个eip算么👤

作者回复：几个点都说得很对，除了内网带宽并没有独占共享之说。



👍 2



我来也

2020-03-16

今天在阿里云上实操了下弹性网卡和辅助私网IP，确实方便和强大。

辅助网卡可以随便切换绑定的实例。

辅助私网IP也是可以随便的增删。

绑定或增加后，只需要在实例中执行简单的几个命令或配置，就可以生效了。

也就是说，某一实例的网络出状况时，可以先把网卡指向到备用实例，继续提供服务。原先的现场还能保留。

作者回复：是的，实操之后印象会更加深刻。



👍 2



戴斌

2020-03-20

内网带宽受机器配置影响

作者回复：没错，配置越强悍，内网带宽越高。



👍 1



上山砍柴

2020-03-17

老师，能不能讲一下，云计算网络他们是怎么构造的，深层次的原理。或者推介一下资料也是好的

作者回复：你可以参考一下极客时间上另一门课程刘超老师《趣谈网络协议》中的相关章节。



👍 1



安排

2020-03-16

云提供商这一块的vpc是不是通过路由器接入公网的？一台云上虚拟机接入公网，这之间还有哪些设备呢？如果我们申请的云上虚拟机不配置公网ip和弹性ip，那控制这台虚拟机只能通过阿里云的网页来控制吗？网上有说通过ssh连到跳板机可以控制的？跳板机的原理是啥？如何申请呢

作者回复：虚拟机的流量进入公网，的确会经过数据中心的路由层，但这里面实际牵涉到的设备和算法，会比通常意义上的“路由器”要复杂精密得多。

跳板机可以是一台普通虚拟机，通过公共ip对外暴露部分端口，外界可以直接连接（一般会限制连接ip）。因为它位于内网中，所以能通过它访问内网其他机器。另外，云上跳板机在不需要使用的时候，也可以关机下线。



1



潘政宇

2020-03-16

- 1.VPC两机器互联的带宽，主要受虚拟网卡限制吧
- 2.需要DNAT

作者回复：注意虚拟网卡本身没有性能级别，一般是取决于虚拟机本身的配置档次。



1



Nothing Is Impossi...

2021-10-19

这样子是不是就没有mac的概念了？看起来好像都是用IP在通信



熊猫

2021-06-26

老师，弹性IP会和公网上的IP会重吗？



lifebread

2020-06-21

老师，没有完全读懂SNAT和NAT之间的关系，为什么要先创建一个NAT再创建SNAT呢？从文中只看到了SNAT绑定在了EIP上，并没有看到比如说SNAT绑定在了特定的NAT上

作者回复：谢谢你的问题，这里的确可以说得更清楚些：NAT网关是一个实例，SNAT条目本质上是NAT网关实例上的一种配置或者说导流规则。我们是在NAT网关界面中创建SNAT条目的，所以它们天生是关联的，不需要额外“绑定”。

共 2 条评论 >



分清云淡

2020-05-12

请教老师：

- 1) 阿里云的vpc跨城的话就没法多个ecs重用一個vpc了吧？
- 2) 阿里云上多个vpc怎么打通好呢？

作者回复：嗯，跨地域场景，可以使用阿里云的云企业网，进行多个vpc间的互联，参见 <https://help.aliyun.com/product/59006.html>



胖子

2020-04-11

每个子网都有路由表怎么理解呢？VPC下的子网属于同一局域网何需路由器层级的路由功能。

作者回复：只要身处网络之中，为了知道下一跳往何处去，就要有路由表的指引。云上这样设计子网和路由表的对应关系，是为了在某些情况下，允许子网级别的细粒度路由控制，是有意义和价值的。

另外，注意文中说子网是和路由表进行“关联”，意味着路由表实例是可以共享的，并非指每个子网一定要有自己独立的路由表。



胖子

2020-04-11

请老师解惑1、网段与子网的关系与区别？2、同一VPC可以跨区域设置吗？

作者回复：网段就是IP区段，是VPC或者子网的地址段属性。同一个VPC一般只能限定在一个区域，如果要跨区域内部通信，就需要用到文中提到的多VPC互联了。

