一、Amazon VPC 概念

1、VPC 和子网

Virtual Private Cloud (VPC) 是仅适用于您的 AWS 账户的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔绝。可在 VPC 中启动 AWS 资源，如 Amazon EC2 实例。您可以为 VPC 指定 IP 地址范围、添加子网、关联安全组以及配置路由表。

子网是您的 VPC 内的 IP 地址范围。您可以在指定子网内启动 AWS 资源。对必须连接 Internet 的资源使用公有子网，而对将不会连接到 Internet 的资源使用私有子网。

2、支持的平台

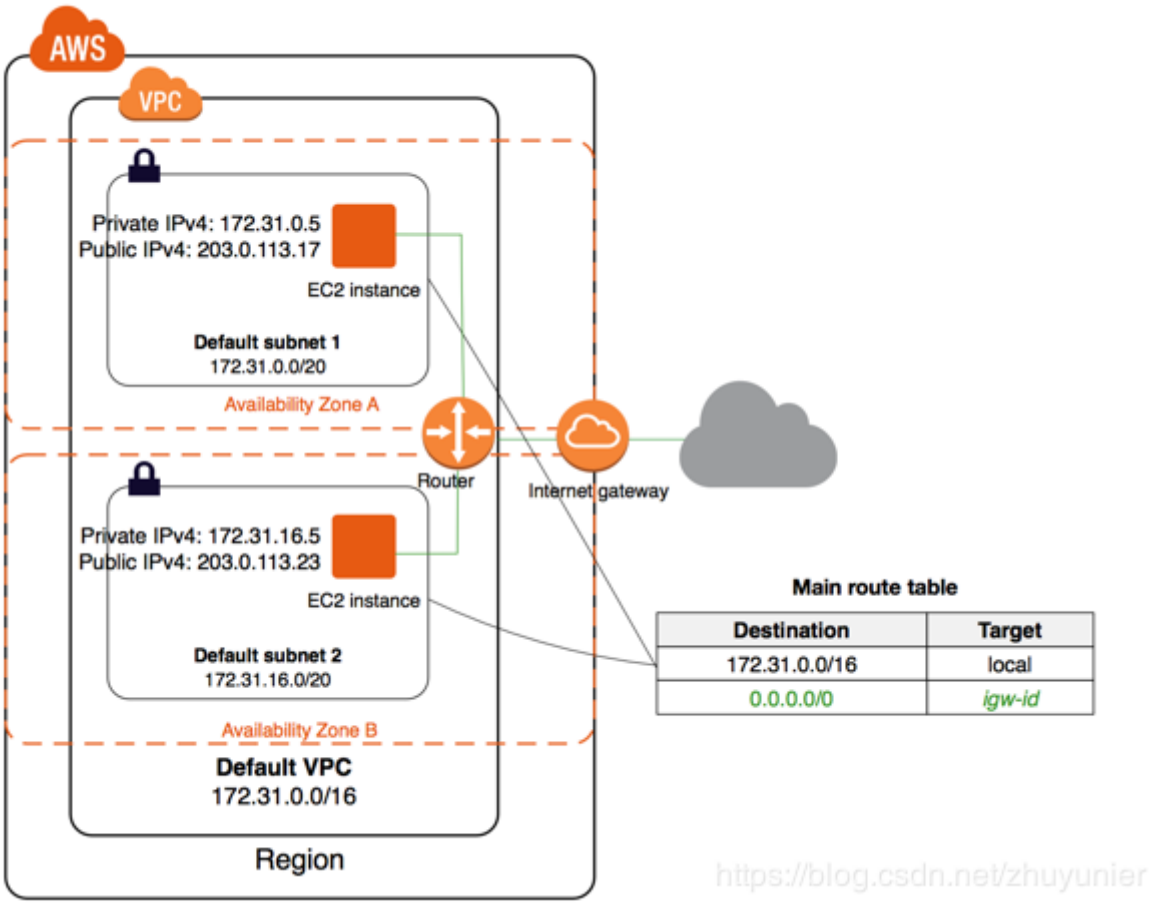
通过将实例启动到 VPC (而不是 EC2-Classic)，您能够： 为启动和停止时保持不变的实例分配静态私有 IPv4 地址

- (可选) 将 IPv6 CIDR 块与您的 VPC 关联，并为您的实例分配 IPv6 地址
- 为您的实例分配多个 IP 地址
- 定义网络接口，并将一个或多个网络接口连接到您的实例
- 在实例运行时更改其安全组成员身份
- 控制您的实例的入站流量 (入站筛选) 和出站流量 (出站筛选)
- 以网络访问控制列表 (ACL) 的方式为您的实例添加额外的访问控制层
- 在单租户硬件上运行您的实例

3、正在访问 Internet

- 您的默认 VPC 包含一个 Internet 网关，而且每个默认子网都是一个公有子网。您在默认子网中启动的每个实例都有一个私有 IPv4 地址和一个公有 IPv4 地址。这些实例可以通过 Internet 网关与 Internet 通信。通过 Internet 网关，

您的实例可通过 Amazon EC2 网络边界连接到 Internet。



- 默认情况下，您启动到非默认子网中的每个实例都有一个私有 IPv4 地址，但没有公有 IPv4 地址，除非您在启动时特意指定一个，或者修改子网的公有 IP 地址属性。这些实例可以相互通信，但无法访问 Internet。termark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3podXl1bmllcg==,size_16,color_FFFFFF,t_70)
- 您可以通过以下方式为在非默认子网中启动的实例启用 Internet 访问：将一个 Internet 网关附加到该实例的 VPC (如果其 VPC 不是默认 VPC)，然后将一个弹性 IP 地址与该实例相关联。
- 您也可以为 IPv4 流量使用网络地址转换 (NAT) 设备，以允许 VPC 中的实例发起到 Internet 的出站连接，但阻止来自 Internet 的未经请求的入站连接。NAT 将多个私有 IPv4 地址映射到一个公有 IPv4 地址。NAT 设备有一个弹性 IP 地址，并通过 Internet 网关与 Internet 相连。您可以通过 NAT 设备将私有子网中的实例连接到 Internet，NAT 设备会将来自实例的流量路由到 Internet 网关，并将所有响应路由到该实例。
- 您可以选择将 Amazon 提供的 IPv6 CIDR 块与您的 VPC 关联，并为您的实例分配 IPv6 地址。实例可以通过 Internet 网关经由 IPv6 连接到 Internet。或者，实例也可以使用仅出口 Internet 网关经由 IPv6 发起到 Internet 的出站连接。有关更多信息，请参阅 仅出口 Internet 网关。IPv6 流量独立于 IPv4 流量；您的路由表必须包含单独的 IPv6 流量路由。

4、安全组

安全组充当虚拟防火墙，为其关联的实例控制数据流。要使用安全组，您可以添加入站规则以控制进入实例的传入流量，添加出站规则以控制来自您的实例的传出流量。要将安全组与实例关联，您可以在启动实例时指定安全组。无论您是添加还是删除安全组规则，我们都会将这些变化自动应用到与安全组相关的实例中。

WebServerSG 安全组规则

下表介绍了 WebServerSG 安全组的入站和出站规则。您将自行添加入站规则。出站规则是默认规则，它允许发送到任何地址的出站通信 — 您无需自行添加此规则。

入站			
源 IP	**协议**	**端口范围**	**注释**
0.0.0.0/0	TCP	80	允许从任意 IPv4 地址进行入站 HTTP 访问。
0.0.0.0/0	TCP	443	允许从任意 IPv4 地址进行入站 HTTPS 访问。
您的家庭网络的公有 IPv4 地址范围	TCP	22	允许从您的家庭网络到 Linux/UNIX 实例的入站 SSH 访问。
您的家庭网络的公有 IPv4 地址范围	TCP	3389	允许从您的家庭网络到 Windows 实例的入站 RDP 访问。
出站			
目的地 IP	**协议**	**端口范围**	**注释**
0.0.0.0/0	全部	全部	允许所有出站 IPv4 通信的默认出站规则。

二、IP地址

1、IPv4 和 IPv6

IP 地址使 VPC 中的资源能够相互通信以及与 Internet 上的资源进行通信。Amazon EC2 和 Amazon VPC 支持 IPv4 及 IPv6 寻址协议。

默认情况下，Amazon EC2 和 Amazon VPC 使用 IPv4 寻址协议。创建 VPC 时，必须为其分配 IPv4 CIDR 块 (一系列私有 IPv4 地址)。私有 IPv4 地址无法通过 Internet 访问。要通过 Internet 连接您的实例或实现实例与其他具有公共终端节点的 AWS 服务之间的通信，您可以向实例分配全球唯一的公有 IPv4 地址。

您可以选择向 VPC 和子网关联 IPv6 CIDR 块，然后将此块中的 IPv6 地址分配给 VPC 中的资源。IPv6 地址是公有的，可通过 Internet 访问。

IPv4 和 IPv6 特性与限制

IPv4	
格式为 32 位，4 组，每组最多 3 个数字。	格式为 1
所有 VPC 的默认项和必需值；无法删除。	
VPC CIDR 块大小可以从 /16 到 /28。	
子网 CIDR 块大小可以从 /16 到 /28。	

IPv4	
您可以为您的 VPC 选择私有 IPv4 CIDR 块。	我们从 Amazon 的 IPv6 地址池
存在私有 IP 地址和公有 IP 地址之分。要与 Internet 通信，需要通过网络地址转换 (NAT) 将公有 IPv4 地址映射为主要私有 IPv4 地址。	不区分公有 I
所有实例类型都支持。	受所有最新一代的实
受 EC2-Classic 和通过 ClassicLink 与 VPC 连接的 EC2-Classic 支持。	不受 EC2-Classic 和
所有 AMI 都支持。	在针对 DHCPv6 进行了配置的 AMI 上自 Server 2008 R2 和更高版本进行了 DHC
实例会收到与其私有 IPv4 地址对应的 Amazon 提供的私有 DNS 主机名，如果适用，还会收到与其公有 IPv4 或弹性 IP 地址对应的公有 DNS 主机名。	不支
支持弹性 IPv4 地址。	
支持 VPC VPN 连接和客户网关、NAT 设备及 VPC 终端节点。	不支持 VPC VPN

2、私有 IPv4 地址

私有 IPv4 地址 (也称作私有 IP 地址) 无法通过 Internet 访问，但可用于 VPC 中实例之间的通信。当在 VPC 中启动实例时，系统会将子网地址范围中的一个主要私有 IPv4 地址分配给该实例的默认网络接口 (eth0)。另外，还为每个实例指定一个可解析为实例私有 IP 地址的私有 (内部) DNS 主机名。如果未指定主要私有 IP 地址，会在子网范围内为您选择可用的 IP 地址。

3、公有 IPv4 地址

所有子网都有一个用于确定在子网中创建的网络接口是否自动接收公有 IPv4 地址 (在本主题中也称作公有 IP 地址) 的属性。因此，当在启用了此属性的子网中启动实例时，系统会向为此实例创建的主网络接口 (eth0) 分配一个公有 IP 地址。公有 IP 地址通过网络地址转换 (NAT) 映射到主要私有 IP 地址。

如果需要向账户分配一个永久公有 IP 地址，需要改为使用弹性 IP 地址。

4、IPv6 地址

IPv6 地址具有全局唯一性，因此可通过 Internet 访问。

三、网络 ACL

网络访问控制列表 (ACL) 是 VPC 的一个可选安全层，可用作防火墙来控制进出一个或多个子网的流量。可以设置网络 ACL，使其规则与您的安全组相似，以便为 VPC 添加额外安全层。

网络 ACL 基本信息

- 您的 VPC 自动带有可修改的默认网络 ACL。默认情况下，它允许所有入站和出站 IPv4 流量以及 IPv6 流量 (如果适用)。
- 您可以创建自定义网络 ACL 并将其与子网相关联。默认情况下，每个自定义网络 ACL 都拒绝所有入站和出站流量，直至您添加规则。
- 您的 VPC 中的每个子网都必须与一个网络 ACL 相关联。如果您没有明确地将子网与网络 ACL 相关联，则子网将自动与默认网络 ACL 关联。
- 您可以将一个网络 ACL 与多个子网关联；但是，一个子网一次只能与一个网络 ACL 关联。当您将一个网络 ACL 与一个子网关联时，将删除之前的关联。
- 网络 ACL 包含规则的编号列表，以供我们按顺序评估 (从编号最小的规则开始) 以判断流量是否被允许进入或离开任何与网络 ACL 关联的子网。您可以使用的最高规则编号为 32766。我们建议您开始先以增量方式创建规则（例如，以 10 或 100 的增量增加），这样您可以在稍后需要时插入新的规则。
- 网络 ACL 有单独的入站和出站规则，每项规则都或是允许或是拒绝数据流。
- 网络 ACL 没有任何状态；对允许入站数据流的响应会随着出站数据流规则的变化而改变 (反之亦然)。

默认网络 ACL

下面是一个仅支持 IPv4 的 VPC 的示例默认网络 ACL。

入站					
规则 #	**类型**	**协议**	**端口范围**	**源**	**允许/拒绝**
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允许
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒绝
出站					
规则 #	**类型**	**协议**	**端口范围**	**目的地**	**允许/拒绝**
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允许
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒绝

自定义网络 ACL

下表显示了一个仅支持 IPv4 的 VPC 的自定义网络 ACL 示例。其中包括允许 HTTP 和 HTTPS 数据流进入的规则 (入站规则 100 和 110)。存在相应的出站规则，以允许响应入站数据流 (出站规则 120，适用于临时端口 32768-65535)。

入站						
规则 #	类型	协议	端口范围	源	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTP 流量。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTPS 流量。
120	SSH	TCP	22	192.0.2.0/24	允许	允许来自您的家庭网络的公有 IPv4 地址范围的入站 SSH 流量 (通过 Internet 网关)。
130	RDP	TCP	3389	192.0.2.0/24	允许	允许从您的家庭网络的公有 IPv4 地址范围到 Web 服务器的入站 RDP 流量 (通过 Internet 网关)。
140	自定义 TCP	TCP	32768-65535	0.0.0.0/0	允许	允许来自 Internet 的入站返回 IPv4 流量 (即源自子网的请求)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见临时端口。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则 (不可修改) 处理的入站 IPv4 流量。

出站						
规则 #	类型	协议	端口范围	目的地	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许出站 IPv4 HTTP 流量从子网流向 Internet。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许出站 IPv4 HTTPS 流量从子网流向 Internet。
120	自定义 TCP	TCP	32768-65535	0.0.0.0/0	允许	允许对 Internet 客户端的出站 IPv4 响应 (例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见临时端口。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站 IPv4 流量。

四、VPC 联网组件

1、网络接口

弹性网络接口 (本文档称为网络接口) 是可包含以下属性的虚拟网络接口：

- 一个主要私有 IPv4 地址
- 一个或多个辅助私有 IPv4 地址
- 每个私有 IPv4 地址一个弹性 IP 地址
- 一个公有 IPv4 地址，可在启动实例时自动分配给 eth0 的网络接口
- 一个或多个 IPv6 地址
- 一个或多个安全组
- MAC 地址
- 源/目标检查标记
- 说明

可以创建一个网络接口，将其连接到某个实例，将其与实例分离，再连接到另一个实例。在连接实例或断开实例连接并重新连接至另一实例时，网络接口的属性会随之变化。当您将一个网络接口从一个实例移动到另一个实例时，网络流量也会重导向到新的实例。

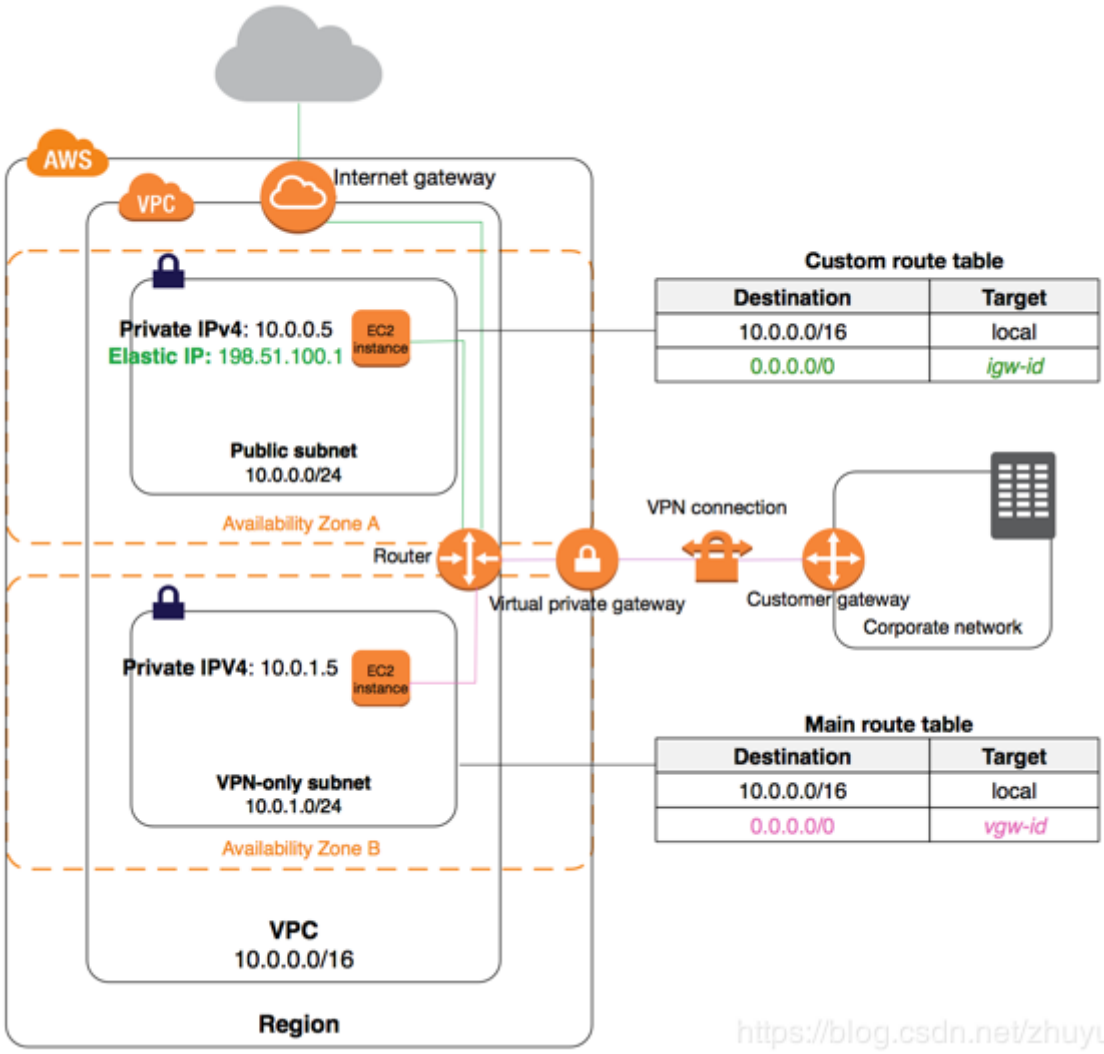
2、路由表

路由表中包含一系列被称为路由的规则，可用于判断网络流量的导向目的地。

在VPC 中的每个子网必须与一个路由表关联；路由表控制子网的路由。一个子网一次只能与一个路由表关联，但可以将多个子网与同一路由表关联。

- 主路由表:在 Amazon VPC 控制台中的 Route Tables 页面上，通过在 Main 列中查找 Yes 可以查看 VPC 的主路由表。主路由表控制未与任何其他路由表显式关联的所有子网的路由。可以在主路由表中添加、删除和修改路由。
- 自定义路由表:除了默认路由表之外， VPC 还可以有其他路由表。保护VPC 的一种方式是保留主路由表的初始默认状态 (仅包含本地路由)，并将创建的每个新建子网与已经创建的自定义路由表之一建立显式关联。这样可以确保能够显式控制每个子网的出站数据流的路由方式。

下图展示了同时有 Internet 网关和虚拟专用网关、以及一个公有子网和仅限 VPN 连接子网的 VPC 的路由。主路由表自带 VPC，同时还有仅限 VPN 的子网的路由。与公有子网关联的自定义路由表。自定义路由表内包含 Internet 网关路由 (目的地为 0.0.0.0/0，目标为 Internet 网关)。



下面的路由表

包含一条指向 Internet 网关的 IPv4 Internet 流量 (0.0.0.0/0) 路由、一条指向对等连接 (pcx-1a2b3c4d) 的 172.31.0.0/16 IPv4 流量路由。来自该子网的目标为 172.31.0.0/16 IP 地址范围的任意流量均使用对等连接，因为该路由比 Internet 网关路由更明确。目标设为 VPC (10.0.0.0/16) 中的目标的任何流量将被 Local 路由涵盖，因此将在 VPC 中路由。来自该子网的所有其他流量使用 Internet 网关。

目的地	目标
10.0.0.0/16	本地
172.31.0.0/16	pcx-1a2b3c4d
0.0.0.0/0	igw-11aa22bb

在此示例中，IPv6 CIDR 块与您的 VPC 关联。在您的路由表中，发往 VPC (2001:db8[1234]1a00::/56) 中的 IPv6 流量为 Local 路由所覆盖，在 VPC 内路由。此路由表还具有指向对等连接 (pcx-1a2b3c4d) 的 172.31.0.0/16 IPv4 流量的路由、指向 Internet 网关的所有 IPv4 流量 (0.0.0.0/0) 的路由以及指向仅出口 Internet 网关的所有 IPv6 流量 (::/0) 的路由。IPv4 和 IPv6 流量是分开处理的；因此，所有 IPv6 流量 (VPC 内流量除外) 均被路由到仅出口 Internet 网关。

目的地	目标
10.0.0.0/16	本地
2001:db8:1234:1a00::/56	本地
172.31.0.0/16	pcx-1a2b3c4d
0.0.0.0/0	igw-11aa22bb
::/0	eigw-aabb1122

3、Internet 网关

Internet 网关是一种横向扩展、支持冗余且高度可用的 VPC 组件，可实现 VPC 中的实例与 Internet 之间的通信。因此它不会对网络流量造成可用性风险或带宽限制。

Internet 网关有两个用途，一个是在 VPC 路由表中为 Internet 可路由流量提供目标，另一个是为已经分配了公有 IPv4 地址的实例执行网络地址转换 (NAT)。

Internet 网关支持 IPv4 和 IPv6 流量。

4、DHCP 选项集

动态主机配置协议 (DHCP) 提供了将配置信息传递到 TCP/IP 网络中主机的标准。DHCP 消息中的 options 字段包含配置参数。这些参数包括域名、域名服务器以及“netbios-node-type”。

DHCP 选项集概述

DHCP 选项名称	说明
domain-name-servers	最多四台域名服务器 (即 AmazonProvidedDNS) 的 IP 地址。默认 DHCP 选项集指定 AmazonProvide 管可以指定最多四个域名服务器，但请注意，某些操作系统可能会施加较低的限制。如果要让实例 name-servers 设置为自定义 DNS 服

DHCP 选项名称	说明
domain-name	如果您是在 us-east-1 中使用 AmazonProvidedDNS，请指定 ec2.internal。如果您是在其他区域中使 northeast-1.compute.internal）。否则，请指定域名 (例如 example.co
ntp-servers	最多四个网络时间协议 (NTP) 服务器的
netbios-name-servers	最多四个 NetBIOS 名称服务器的 IP
netbios-node-type	NetBIOS 节点类型 (1、2、4 或 8)。我们建议您指定 2 (点对点或

Amazon DNS 服务器

当创建 VPC 时，会自动创建 DHCP 选项集，并将它们与 VPC 相关联。此设置包括两个选项：domain-name-servers=AmazonProvidedDNS 和 domain-name=domain-name-for-your-region。AmazonProvidedDNS 是 Amazon DNS 服务器，此选项允许 DNS 使用需要通过 VPC Internet 网关进行通信的实例。字符串 AmazonProvidedDNS 映射到在预留 IP 地址 (以 VPC IPv4 网络范围“+2”为基础) 中运行的 DNS 服务器。例如，10.0.0.0/16 网络中的 DNS 服务器位于 10.0.0.2。对于包含多个 IPv4 CIDR 块的 VPC，DNS 服务器的 IP 地址位于主要 CIDR 块中。

当您在 VPC 中启动一个实例时，如果该实例接收公有 IPv4 地址，我们会为该实例提供一个私有 DNS 主机名和一个公有 DNS 主机名。如果将 DHCP 选项中的 domain-name-servers 设置为 AmazonProvidedDNS，则对于 us-east-1 区域，公有 DNS 主机名采用 ec2-public-ipv4-address.compute-1.amazonaws.com 形式，对于其他区域，则采用 ec2-public-ipv4-address.region.compute.amazonaws.com 形式。对于 us-east-1 区域，私有主机名采用 ip-private-ipv4-address.ec2.internal 形式，对于其他区域，则采用 ip-private-ipv4-address.region.compute.internal 形式。要将这些更改为自定义 DNS 主机名，您必须将 domain-name-servers 设为自定义 DNS 服务器。

5、DNS

域名系统 (DNS) 是 Internet 中名称使用的标准，以将名称解析到各自相应的 IP 地址。DNS 主机名是可以唯一并绝对区分计算机的名称；它由主机名和域名组成。DNS 服务器会将 DNS 主机名称解析到其相应的 IP 地址。

DNS 主机名

当将实例启动到默认 VPC 中时，为实例提供与其公有 IPv4 和私有 IPv4 地址对应的公有和私有 DNS 主机名。当在非默认 VPC 中启动实例时，会为实例提供私有 DNS 主机名，并根据为 VPC 指定的 DNS 属性以及您的实例是否具有公有 IPv4 地址来决定是否提供公有 DNS 主机名。

Amazon 提供的私有 (内部) DNS 主机名解析为实例的私有 IPv4 地址，并对 us-east-1 区域采用 ip-private-ipv4-address.ec2.internal 形式，对其他区域采用 ip-private-ipv4-address.region.compute.internal 形式 (其中 private-ipv4-address 是反向查找 IP 地址)。可以使用私有 DNS 主机名在同一网络中实现实例之间的通信，但无法解析实例所在网络之外的 DNS 主机名。

对于 us-east-1 区域，公有 (外部) DNS 主机名采用 ec2-public-ipv4-address.compute-1.amazonaws.com 形式，对于其他区域，则采用 ec2-public-ipv4-address.region.compute.amazonaws.com 形式。将公有 DNS 主机名解析为该实例在所在网络外的公有 IPv4 地址及其在所在网络内的私有 IPv4 地址。

不为 IPv6 地址提供 DNS 主机名。

6、VPC 对等

VPC 对等连接是两个 VPC 之间的网络连接，可通过此连接不公开地在这两个 VPC 之间路由流量。这两个 VPC 中的实例可以彼此通信，就像它们在同一网络中一样。可以在自己的 VPC 之间、自己的 VPC 与另一个 AWS 账户中的 VPC 或与其他 AWS 区域中的 VPC 之间创建 VPC 对等连接。

AWS 使用现有 VPC 基础设施创建 VPC 对等连接，既不是网关，也不是 VPN 连接，因此不依赖某个独立的实体硬件。没有单点通信故障也没有带宽瓶颈。

7、弹性 IP 地址

弹性 IP 地址 是专门用于进行动态云计算的静态、公有 IPv4 地址。可以将弹性 IP 地址与您账户中的任意 VPC 的任何实例或网络接口相关联。借助弹性 IP 地址，可以迅速将地址重新映射到 VPC 中的另一个实例，从而屏蔽实例故障。注意，将弹性 IP 地址与网络接口关联，而不直接与实例关联的优势在于，只需一步，即可将网络接口的所有属性从一个实例移至另一个。

目前不支持对 IPv6 使用弹性 IP 地址。

8、VPC 终端节点

VPC 终端节点使您能够将 VPC 私密地连接到支持的 AWS 服务和 VPC 终端节点服务（由 PrivateLink 提供支持），而无需 Internet 网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例无需公有 IP 地址便可与服务中的资源通信。VPC 和其他服务之间的通信不会离开 Amazon 网络。

终端节点是虚拟设备。这些是水平扩展、冗余且具备高可用性的 VPC 组件，通过使用这些组件，可以在 VPC 中的实例与服务之间进行通信，而不会对网络通信带来可用性风险或带宽限制。

VPC 终端节点有两种类型：接口终端节点 和 网关终端节点。创建受支持的服务所需要的 VPC 终端节点类型。