VPC 对等

Amazon Virtual Private Cloud

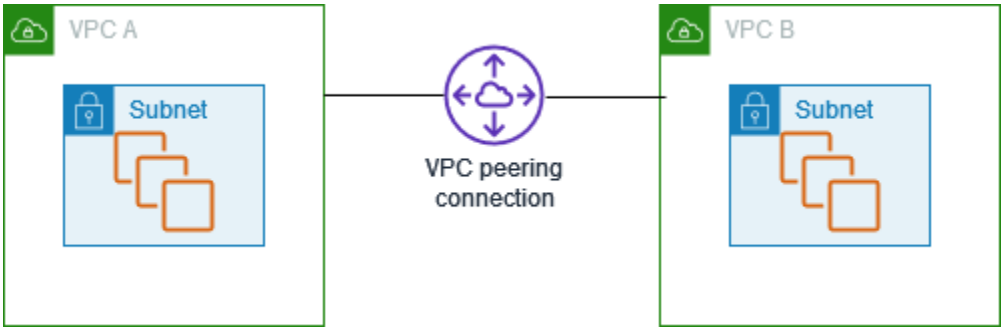
Amazon Virtual Private Cloud: VPC 对等

Table of Contents

什么是 VPC 对等？

虚拟私有云（VPC）是专用于您的 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。您可以在 VPC 内启动 AWS 资源，例如 Amazon EC2 实例。

VPC 对等连接是两个 VPC 之间的网络连接，通过此连接，您可以使用私有 IPv4 地址或 IPv6 地址在两个 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。您可以在自己的 VPC 之间创建 VPC 对等连接，或者在自己的 VPC 与其他AWS账户中的 VPC 之间创建连接。VPC 可位于不同区域内（也称为区域间 VPC 对等连接）。



AWS使用 VPC 的现有基础设施来创建 VPC 对等连接；该连接既不是网关也不是 VPN 连接，并且不依赖某一单独的物理硬件。没有单点通信故障也没有带宽瓶颈。

VPC 对等连接可以帮助您促进数据的传输。例如，如果您有多个AWS账户，则可以通过在这些账户中的 VPC 间建立对等连接来创建文件共享网络。您还可以使用 VPC 对等连接来允许其他 VPC 访问您某个 VPC 中的资源。

当您跨不同 AWS 区域在 VPC 之间建立对等关系时，不同 AWS 区域中的 VPC 中的资源（例如 EC2 实例和 Lambda 函数）可以使用私有 IP 地址相互通信，无需使用网关、VPN 连接或网络设备。这些流量保留在私有 IP 地址空间中。所有区域间流量在离开 AWS 设施前均已加密，没有单点故障或带宽瓶颈。流量一直处于全球AWS骨干网络中，不会经过公有 Internet，这样可以减少面临的威胁，例如常见攻击漏洞和 DDoS 攻击。区域间 VPC 对等连接提供了一种简单且经济高效的方式来在区域间共享资源或复制数据以实现地理冗余。

VPC 对等连接的定价

创建 VPC 对等连接，无需付费。通过保留在可用区内的 VPC 对等连接进行的所有数据传输（即使是在不同账户之间）都是免费的。通过跨可用区和区域的 VPC 对等连接进行的数据传输需支付费用。有关更多信息，请参阅 Amazon EC2 定价。

VPC 对等连接的工作原理

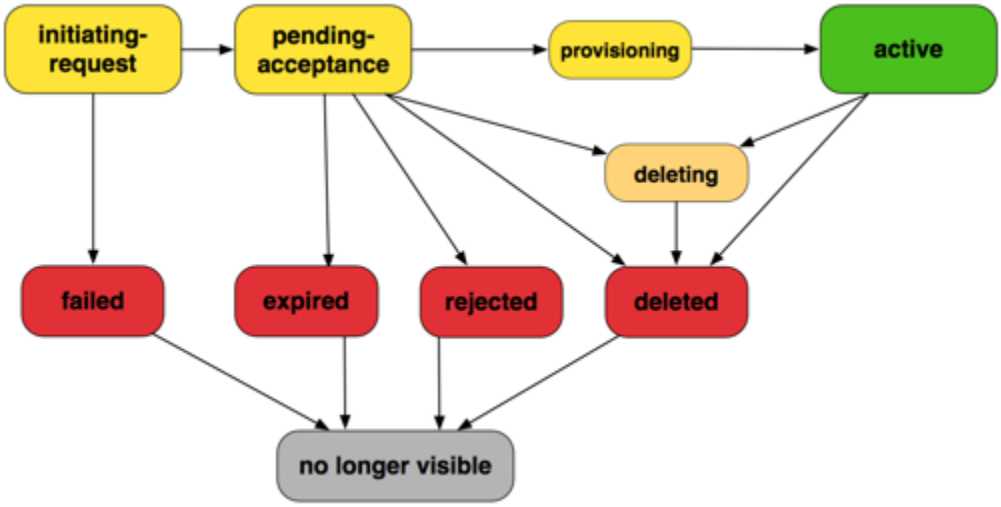
以下步骤描述了 VPC 对等连接流程：

1. 请求者 VPC 的拥有者向接受者 VPC 的拥有者发送创建 VPC 对等连接的请求。接受者 VPC 可以归您或其他 AWS 账户所有，不能包含与请求者 VPC 的 CIDR 块重叠的 CIDR 块。
2. 接受者 VPC 的拥有者接受 VPC 对等连接请求以激活 VPC 对等连接。
3. 要使用私有 IP 地址实现 VPC 之间的流量流动，VPC 对等连接中每个 VPC 的拥有者必须向一个或多个 VPC 路由表手动添加指向其他 VPC (对等 VPC) 的 IP 地址范围的路由。
4. 如果需要，请更新与您的 EC2 实例关联的安全组规则以确保进出对等 VPC 的流量不受限制。如果两个 VPC 位于相同区域内，则您可以引用对等 VPC 中的安全组作为安全组中的入站或出站规则的源或目标。
5. 通过默认 VPC 对等连接选项，如果 VPC 对等连接任一侧的 EC2 实例使用公有 DNS 主机名相互进行寻址，则主机名会解析为 EC2 实例的公有 IP 地址。要更改此行为，请为您的 VPC 连接启用 DNS 主机名解析。在启用 DNS 主机名解析后，如果 VPC 对等连接任一侧的 EC2 实例使用公有 DNS 主机名相互进行寻址，则主机名将解析为 EC2 实例的私有 IP 地址。

有关更多信息，请参阅 VPC 对等连接。

VPC 对等连接的生命周期

从发起请求时开始，VPC 对等连接会经过各个阶段。在每个阶段中，您都可以执行一些操作，在生命周期结束后，VPC 对等连接仍会在 Amazon VPC 控制台和 API 或命令行输出中继续显示一段时间。



- Initiating-request (发起请求)：已发起 VPC 对等连接请求。在这一阶段中，对等连接可能失败或可能转到 pending-acceptance。
- Failed (已失败)：VPC 对等连接请求失败。在处于此状态时，无法接受、拒绝或删除该连接。请求者仍可在 2 个小时内看到失败的 VPC 对等连接。
- Pending-acceptance：等待接受者 VPC 的拥有者接受 VPC 对等连接请求。在这一阶段中，请求者 VPC 的拥有者可以删除此请求，接受者 VPC 的拥有者可以接受或拒绝此请求。如果双方均未对此请求执行任何操作，该请求将在 7 天后过期。
- Expired (已过期)：VPC 对等连接请求已过期，任一 VPC 拥有者都无法再对该请求执行任何操作。两个 VPC 拥有者仍可以在 2 天内看到已过期的 VPC 对等连接。
- Rejected：接受者 VPC 的拥有者拒绝了 pending-acceptance VPC 对等连接请求。在处于此状态时，无法接受请求。请求者 VPC 的拥有者仍可以在 2 天内看到已拒绝的 VPC 对等连接，接受者 VPC 的拥有者仍可在 2 个小时内看到此对等连接。如果请求是在同一AWS账户内创建的，则已拒绝的请求会继续显示 2 个小时。
- Provisioning (正在预置)：VPC 对等连接请求已接受，即将处于 active 状态。
- Active：VPC 对等连接处于活动状态，而且流量可以在 VPC 之间流动 (假设您的安全组和路由表允许流量流动)。在处于此状态时，任一 VPC 拥有者都可以删除 VPC 对等连接，但是无法拒绝它。

  > **Note**
  >
  > 如果 VPC 所在的区域中的事件阻止流量流动，则 VPC 对等连接的状态将保持 Active。

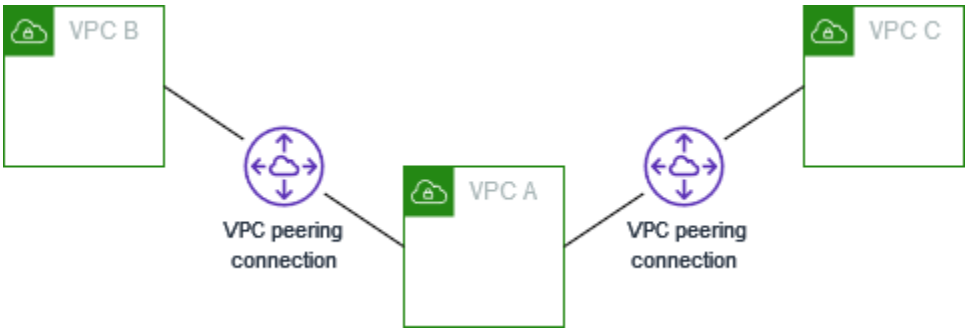
- Deleting（删除）：适用于处于删除过程中的区域间 VPC 对等连接。任一 VPC 的拥有者已提交删除 active VPC 对等连接的请求，或者请求者 VPC 的拥有者已提交删除 pending-acceptance VPC 对等连接请求的请求。
- Deleted (已删除)：任一 VPC 拥有者已删除了 active 的 VPC 对等连接，或请求者 VPC 的拥有者已删除了 pending-acceptance 的 VPC 对等连接请求。在这一阶段中，无法接受或拒绝 VPC 对等连接。VPC 对等连接仍会向其删除方继续显示 2 个小时，向另一方显示 2 天。如果 VPC 对等连接是在同一AWS账户内创建的，则已删除的请求仍将继续显示 2 个小时。

多个 VPC 对等连接

VPC 对等连接是两个 VPC 之间的一对一关系。您可以为您的每个 VPC 创建多个 VPC 对等连接，但是不支持传递的对等关系。您不会与您的 VPC 不直接对等的 VPC 形成任何对等关系。

下图举例说明一个 VPC 与两个不同的 VPC 具有对等关系。图中有两个 VPC 对等连接：VPC A 同时与 VPC B 和 VPC C 具有对等关系。VPC B 与 VPC C 不对等，并且您不能将 VPC A 用作 VPC B 和

VPC C 之间的对等中转点。如果您要在 VPC B 和 VPC C 之间支持流量路由，必须在这两者之间创建一个唯一的 VPC 对等连接。



VPC 对等限制

请考虑以下 VPC 对等连接的限制。在某些情况下，您可以使用中转网关连接代替 VPC 对等连接。有关更多信息，请参阅《Amazon VPC 中转网关》中的 Example transit gateway scenarios。

连接

- 每个 VPC 具有的活动和待定 VPC 对等连接的数量具有配额。有关更多信息，请参阅 配额。
- 两个 VPC 之间不能同时创建多个 VPC 对等连接。
- 您为 VPC 对等连接创建的任何标签仅在您创建它们的账户或区域中应用。
- 您无法连接或查询对等 VPC 中的 Amazon DNS 服务器。
- 如果 VPC 对等连接中 VPC 的 IPv4 CIDR 块不在 RFC 1918 所指定的私有 IPv4 地址范围内，则该 VPC 的私有 DNS 主机名无法解析为私有 IP 地址。要将私有 DNS 主机名解析为私有 IP 地址，您可以为 VPC 对等连接启用 DNS 解析支持。有关更多信息，请参阅 实现对 VPC 对等连接的 DNS 解析。
- 您可以允许 VPC 对等连接两端的资源通过 IPv6 通信。您必须为每个 VPC 关联一个 IPv6 CIDR 块，允许 VPC 中的实例进行 IPv6 通信，并将针对对等 VPC 的 IPv6 流量路由到 VPC 对等连接。
- 不支持在 VPC 对等连接中进行单一地址反向传输路径转发。有关更多信息，请参阅 响应流量路由。

重叠 CIDR 块

- 您无法在具有匹配或重叠的 IPv4 或 IPv6 CIDR 块的 VPC 之间创建 VPC 对等连接。
- 如果您有多个 IPv4 CIDR 块，则只要有任何 CIDR 块重叠，您都无法创建 VPC 对等连接，即使您打算仅使用不重叠的 CIDR 块或仅使用 IPv6 CIDR 块。

传递的对等

- VPC 对等不支持传递的对等关系。例如，如果 VPC A 和 VPC B 之间以及 VPC A 和 VPC C 之间有 VPC 对等连接，则您无法通过 VPC A 将流量从 VPC B 路由到 VPC C。要在 VPC B 和 VPC C 之间路由流量，您必须在两者之间创建 VPC 对等连接。有关更多信息，请参阅 相互对等的三个 VPC。

通过网关或私有连接进行的边缘到边缘路由

- 如果 VPC A 具有互联网网关，则 VPC B 中的资源无法使用 VPC A 中的互联网网关访问互联网。
- 如果 VPC A 具有为 VPC A 中的子网提供 Internet 访问的 NAT 设备，则 VPC B 中的资源无法使用 VPC A 中的 NAT 设备访问 Internet。
- 如果 VPC A 具有连接到公司网络的 VPN 连接，则 VPC B 中的资源无法使用 VPN 连接与公司网络通信。
- 如果 VPC A 具有连接到公司网络的 Direct Connect 连接，则 VPC B 中的资源无法使用 Direct Connect 连接与公司网络通信。
- 如果 VPC A 的网关端点提供与 Amazon S3 到 VPC A 中的私有子网的连接，则 VPC B 中的资源无法使用网关端点访问 Amazon S3。

区域间 VPC 对等连接

- 对于巨型帧，同一区域内的 VPC 对等连接之间的最大传输单位（MTU）为 9001 字节。区域间 VPC 对等连接的 MTU 为 8500 字节。有关巨型帧的更多信息，请参阅《Amazon EC2 用户指南》中的巨型帧（9001 MTU）。
- 您必须为 VPC 对等连接启用 DNS 解析支持才能将对等 VPC 的私有 DNS 主机名解析为私有 IP 地址，即使 VPC 的 IPv4 CIDR 位于 RFC 1918 指定的私有 IPv4 地址范围内也是如此。

共享 VPC 和子网

- 只有 VPC 所有者可以使用（描述、创建、接受、拒绝、修改或删除）对等连接。参与者无法使用对等连接。有关更多信息，请参阅 Amazon VPC 用户指南中的与其他账户共享 VPC。

VPC 对等连接

通过 VPC 对等连接，您可以连接相同或不同 AWS 区域中的两个 VPC。如此一来，一个 VPC 中的实例就能与另一个 VPC 中的实例进行通信，就像属于同一个网络一样。

VPC 对等连接通过私有 IPv4 地址或 IPv6 地址在两个 VPC 之间直接创建网络路由。在连接的 VPC 之间发送的流量不会通过互联网、VPN 连接或 AWS Direct Connect 传输。这使得 VPC 对等连接成为一种跨 VPC 边界共享资源（例如数据库或 Web 服务器）的安全方式。

要建立 VPC 对等连接，必须从一个 VPC 创建对等连接请求，且另一个 VPC 的所有者接受该请求。建立连接后，您可以更新路由表，以在 VPC 之间路由流量。如此一来，一个 VPC 中的实例就可以访问另一个 VPC 中的资源了。

VPC 对等连接是在 AWS 中构建多 VPC 架构和跨组织边界共享资源的重要工具。该功能提供了一种简单、低延迟的方式来连接 VPC，免去了配置 VPN 或其他网络服务的复杂工作。

使用以下步骤来创建和使用 VPC 对等连接。

任务

- 创建 VPC 对等连接
- 接受或拒绝 VPC 对等连接
- 为 VPC 对等连接更新路由表
- 更新您的安全组以引用对等安全组
- 实现对 VPC 对等连接的 DNS 解析
- 删除 VPC 对等连接
- 对 VPC 对等连接进行问题排查

创建 VPC 对等连接

要创建 VPC 对等连接，请首先创建要与其他 VPC 建立对等连接的请求。要激活请求，接受者 VPC 的拥有者必须接受此请求。支持以下对等连接：

- 在同一账户和区域中的 VPC 之间
- 在同一账户和不同区域中的 VPC 之间
- 在不同账户和同一区域中的 VPC 之间

- 在不同账户和区域中的 VPC 之间

对于区域间 VPC 对等连接，必须从请求者 VPC 的区域发出请求，且必须从接受者 VPC 的区域接受请求。有关更多信息，请参阅 the section called “接受或拒绝”。

任务

- 先决条件
- 使用控制台创建对等连接
- 使用命令行创建对等连接

先决条件

- 查看 VPC 对等连接的限制。
- 确保 VPC 没有重叠的 IPv4 CIDR 块。如有重叠，则 VPC 对等连接的状态将立即变为 `failed`。即使 VPC 具有唯一的 IPv6 CIDR 块，此限制依然适用。

使用控制台创建对等连接

使用以下过程创建 VPC 对等连接。

要使用控制台创建对等连接

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择 Peering Connections（对等连接）。
3. 选择 Create Peering Connection（创建对等连接）。
4. （可选）对于名称，为 VPC 对等连接指定名称。这样可创建具有 Name 键以及您指定的值的标签。
5. 对于 VPC ID（请求者），从当前账户中选择 VPC。
6. 在选择要用作对等的另一个 VPC 下，执行以下操作：
   a. 对于账户，要与其他账户中的 VPC 对等连接，选择其他账户并输入账户 ID。否则，保留我的账户。
   b. 对于区域，要与其他区域的 VPC 对等连接，请选择其他区域并选择此区域。否则，请保留此区域。
   c. 对于 VPC ID（接受者），从指定的账户和区域中选择 VPC。

7. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入标签键和标签值。
8. 选择 Create Peering Connection（创建对等连接）。
9. 接受者账户的拥有者必须接受对等连接。有关更多信息，请参阅 the section called “接受或拒绝”。
10. 更新两个 VPC 的路由表，以启用两者之间的通信。有关更多信息，请参阅 the section called “更新路由表”。

使用命令行创建对等连接

您可以使用以下命令创建 VPC 对等连接：

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

接受或拒绝 VPC 对等连接

处于 `pending-acceptance` 状态的 VPC 对等连接仅在由接受者 VPC 的拥有者接受后才能激活。有关 `Deleted` 对等连接的更多信息，请参阅 VPC 对等连接的生命周期。您无法接受您已发送至其他 AWS 账户的 VPC 对等连接请求。要在同一 AWS 账户中的 VPC 之间创建 VPC 对等连接，您可以自己创建并接受请求。

您可以拒绝您收到的处于 `pending-acceptance` 状态的任何 VPC 对等连接请求。您应仅接受来自您了解并信任的 AWS 账户的 VPC 对等连接；您可以拒绝任何不良的请求。有关 `Rejected` 对等连接的更多信息，请参阅 VPC 对等连接的生命周期。

> **Important**
>
> 请勿接受来自未知 AWS 账户的 VPC 对等连接。恶意用户可能已向您发出 VPC 对等连接请求来获取对您的 VPC 进行未经授权的网络访问的权限。这称为“对等钓鱼”。您可以安全地拒绝不必要的 VPC 对等连接请求，这样就不需要承担以下风险：请求者会访问有关您的 AWS 账户或您的 VPC 的任何信息。有关更多信息，请参阅 接受或拒绝 VPC 对等连接。您还可以忽略请求让它过期；默认情况下，请求将在 7 天后过期。

要使用控制台接受或拒绝对等连接

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 使用区域选择器选择接受者 VPC 的区域。

3. 在导航窗格中，选择 Peering Connections（对等连接）。
4. 要拒绝对等连接，先选择该 VPC 对等连接，然后依次选择操作、拒绝请求。当系统提示进行确认时，选择拒绝请求。
5. 要接受对等连接，先选择待处理的 VPC 对等连接（状态为 `pending-acceptance`），然后依次选择操作、接受请求。有关对等连接生命周期状态的更多信息，请参阅 VPC 对等连接的生命周期。

   如果没有待处理的 VPC 对等连接，则请确认您已选择接受者 VPC 的区域。
6. 当系统提示进行确认时，选择接受请求。
7. 选择立即修改我的路由表，以向 VPC 路由表添加路由，从而确保您可以通过对等连接收发流量。有关更多信息，请参阅 为 VPC 对等连接更新路由表。

要使用命令行接受对等连接

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

要使用命令行拒绝对等连接

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

为 VPC 对等连接更新路由表

要在对等 VPC 中的实例之间启用私有 IPv4 流量，您必须向与两个实例的子网关联的路由表添加路由。路由目的地为对等 VPC 的 CIDR 块（或 CIDR 块的一部分），目标为 VPC 对等连接的 ID。有关更多信息，请参阅《Amazon VPC 用户指南》中的配置路由表。

以下是路由表的示例，该路由表允许两个对等 VPC（VPC A 和 VPC B）中的实例之间的通信。每个表都有一个本地路由和将对等 VPC 的流量发送到 VPC 对等连接的路由。

路由表	目的地	目标
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-*11112222*

路由表	目的地	目标
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-*11112222*

同样，如果 VPC 对等连接中的 VPC 具有关联的 IPv6 CIDR 块，则您可以添加路由来通过 IPv6 实现与对等 VPC 的通信。

有关 VPC 对等连接支持的路由表配置的更多信息，请参阅常见 VPC 对等连接配置。

注意事项

- 如果您的某个 VPC 与多个具有重叠或匹配的 IPv4 CIDR 块的 VPC 对等，请确保路由表配置为不从您的 VPC 向不正确的 VPC 发送响应流量。AWS 当前不支持在 VPC 对等连接中进行单一地址反向传输路径转发，即检查数据包的源 IP 并将应答数据包路由回源。有关更多信息，请参阅 响应流量路由。
- 您的账号的每个路由表可以添加的条目数是有配额的。如果 VPC 中的 VPC 对等连接数超过单个路由表的路由表条目配额，请考虑使用多个子网，且每个子网都与一个自定义路由表关联。
- 您可以为处于 `pending-acceptance` 状态的 VPC 对等连接添加路由。但是，此路由的状态为 `blackhole`，并且在 VPC 对等连接变为 `active` 状态后才生效。

为 VPC 对等连接添加 IPv4 路由

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Route tables（路由表）。
3. 选中与您实例所在子网关联的路由表旁边的复选框。

   如果您未在子网与特定路由表间建立显式关联，则这个子网将与主路由表建立隐式关联。
4. 依次选择 Actions（操作）、Edit routes（编辑路由）。
5. 选择 Add route (添加路由)。
6. 对于 Destination，请输入必须将 VPC 对等连接中的网络流量定向到的 IPv4 地址范围。您可以指定对等 VPC 的整个 IPv4 CIDR 块、具体的范围或单个 IPv4 地址，例如要与之通信的实例的 IP 地址。举例来说，如果对等 VPC 的 CIDR 块为 `10.0.0.0/16`，则您可以指定 `10.0.0.0/24` 部分或具体的 IP 地址 `10.0.0.7/32`。
7. 对于目标，选择该 VPC 对等连接。

8. 选择保存更改。

对等 VPC 的拥有者还必须完成这些步骤，以添加路由来通过 VPC 对等连接将流量定向回到您的 VPC。

如果您在不同 AWS 区域中有使用 IPv6 地址的资源，则可以创建区域间对等连接。然后，您可以为资源之间的通信添加 IPv6 路由。

为 VPC 对等连接添加 IPv6 路由

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Route tables（路由表）。
3. 选中与您实例所在子网关联的路由表旁边的复选框。

> **Note**
>
> 如果您没有与该子网关联的路由表，请选择 VPC 的主路由表作为子网路由表，然后默认使用此路由表。

4. 依次选择 Actions (操作)、Edit routes (编辑路由)。
5. 选择 Add route (添加路由)。
6. 对于 Destination，输入对等 VPC 的 IPv6 地址范围。您可以指定对等 VPC 的整个 IPv6 CIDR 块、具体的范围或单个 IPv6 地址。举例来说，如果对等 VPC 的 CIDR 块为 `2001:db8:1234:1a00::/56`，则您可以指定 `2001:db8:1234:1a00::/64` 部分或具体的 IP 地址 `2001:db8:1234:1a00::123/128`。
7. 对于目标，选择该 VPC 对等连接。
8. 选择保存更改。

有关更多信息，请参阅《Amazon VPC 用户指南》中的路由表。

使用命令行添加或替换路由

- create-route 和 replace-route(AWS CLI)
- New-EC2Route 和 Set-EC2Route(AWS Tools for Windows PowerShell)

更新您的安全组以引用对等安全组

您可以更新 VPC 安全组的入站或出站规则以引用对等 VPC 的安全组。此操作将允许流量流入和流出与对等的 VPC 中的已引用安全组关联的实例。

> **Note**
>
> 不会在控制台中显示对等 VPC 中的安全组供您选择。

要求

- 要在对等 VPC 中引用安全组，VPC 对等连接必须处于`active`状态。
- 对等 VPC 可以是您的账户中的 VPC，也可以是另一AWS账户中的 VPC。要引用位于其他 AWS 账户但属于相同区域的安全组，请将账号与安全组的 ID 一起包括在内。例如 `123456789012/sg-1a2b3c4d`。
- 您无法引用位于不同区域内的对等 VPC 的安全组。而是使用对等 VPC 的 CIDR 块。
- 如果您将路由配置为通过中间设备在不同子网中的两个实例之间转发流量，则必须确保这两个实例的安全组允许流量在实例之间流动。每个实例的安全组必须引用另一个实例的私有 IP 地址或包含另一个实例的子网的 CIDR 范围作为源。如果您引用另一个实例的安全组作为源，则安全组不允许流量在实例之间流动。

使用控制台更新安全组规则

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择安全组。
3. 选择安全组，然后执行下列操作之一：
   - 要修改入站规则，请选择操作、编辑入站规则。
   - 要修改出站规则，请选择操作、编辑出站规则。
4. 要添加规则，请选择添加规则，然后指定类型、协议和端口范围。对于源（入站规则）或目的地（出站规则），请执行下列操作之一：
   - 对于同一账户和区域中的对等 VPC，请输入安全组的 ID。
   - 对于位于不同账户但位于相同区域的对等 VPC，请输入账户 ID 和安全组 ID，中间用正斜杠分隔（例如，`123456789012/sg-1a2b3c4d`）。
   - 对于位于不同区域中的对等 VPC，输入对等 VPC 的 CIDR 块。

5. 要编辑现有的规则，请更改其值（例如，源或描述）。
6. 要删除规则，请选择该规则旁的删除。
7. 选择保存规则。

使用命令行更新入站规则

- authorize-security-group-ingress 和 revoke-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress 和 Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

例如，要更新安全组 sg-aaaa1111 以允许通过 HTTP 从对等 VPC 中的 sg-bbbb2222 进行入站访问，请使用以下命令。如果对等 VPC 位于同一区域但位于不同账户，则添加 `--group-owner` *aws-account-id*。

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

使用命令行更新出站规则

- authorize-security-group-egress 和 revoke-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress 和 Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

在更新安全组规则后，使用 describe-security-groups 命令来查看安全组规则中引用的安全组。

确定引用的安全组

要确定在对等 VPC 中的安全组规则中是否正在引用您的安全组，请对账户中的一个或多个安全组使用以下命令之一。

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

在以下示例中，响应表示安全组 sg-bbbb2222 正在被 VPC vpc-aaaaaaaa 中的安全组引用：

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

如果删除 VPC 对等连接，或者对等 VPC 的拥有者删除引用的安全组，则安全组规则将过时。

查看并删除过时安全组规则

过时的安全组规则是一种引用相同 VPC 或对等 VPC 中的已删除安全组的规则，或引用 VPC 对等连接已删除的对等 VPC 中的安全组的规则。系统不会从您的安全组中自动移除过时的安全组规则，您必须手动删除它们。当安全组规则因删除了 VPC 对等连接而变得过时的时候，如果您使用相同的 VPC 创建了新的 VPC 对等连接，则安全组规则将不再标记为过时。

您可以使用 Amazon VPC 控制台查看和删除某个 VPC 的过时安全组规则。

查看和删除过时安全组规则

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择 Actions (操作)、Manage stale rules (管理过时规则)。
4. 对于 VPC，请选择具有过时规则的 VPC。
5. 选择编辑。
6. 选择您希望删除的规则旁边的 Delete（删除）按钮。选择 Preview changes (预览更改)，然后选择 Save rules (保存规则)。

使用命令行描述您的过时的安全组规则

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

在以下示例中，VPC A (vpc-aaaaaaaa) 和 VPC B 是对等的，并且已删除 VPC 对等连接。您在 VPC A 中的安全组 sg-aaaa1111 引用了 VPC B 中的 sg-bbbb2222。在为您的 VPC 运行

describe-stale-security-groups 命令时，响应表示安全组 sg-aaaa1111 具有引用了 sg-bbbb2222 的过时 SSH 规则。

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
            "Description": "Reference remote SG"
        }
    ]
}
```

找到过时的安全组规则后，您可以使用 revoke-security-group-ingress 或 revoke-security-group-egress 命令将其删除。

实现对 VPC 对等连接的 DNS 解析

VPC 对等连接的 DNS 设置确定如何解析通过 VPC 对等连接的请求的公有 DNS 主机名。如果 VPC 对等连接一端的 EC2 实例使用该实例的公有 IPv4 DNS 主机名向另一端的 EC2 实例发送请求，则解析 DNS 主机名的方法如下所示。

已禁用 DNS 解析（默认）

公有 IPv4 DNS 主机名解析为实例的公有 IPv4 地址。

已启用 DNS 解析

公有 IPv4 DNS 主机名解析为实例的私有 IPv4 地址。

要求

- 必须为 DNS 主机名和 DNS 解析启用两种 VPC。有关更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 的 DNS 属性。
- 对等连接必须处于 `active` 状态。创建对等连接时，无法启用 DNS 解析。
- 请求者 VPC 的拥有者必须修改请求者 VPC 对等连接选项，接受者 VPC 的拥有者必须修改接受者 VPC 对等连接选项。如果 VPC 位于同一账户内，则可以同时为请求者和接受者 VPC 启用 DNS 解析。这适用于同区域和跨区域 VPC 对等连接。

要使用控制台实现对对等连接的 DNS 解析

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择 Peering Connections（对等连接）。
3. 选择 VPC 对等连接。
4. 选择操作和编辑 DNS 设置。
5. 要为来自请求者 VPC 的请求启用 DNS 解析，请选择请求者 DNS 解析和允许接受者 VPC 解析请求者 VPC 的 DNS。
6. 为确保对来自接受者 VPC 的请求进行 DNS 解析，请选择接受者 DNS 解析和允许请求者 VPC 解析接受者 VPC 的 DNS。
7. 选择保存更改。

使用命令行启用 DNS 解析

- modify-vpc-peering-connection-options (AWS CLI)
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

要使用命令行描述 VPC 对等连接选项

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

删除 VPC 对等连接

对等连接中任一 VPC 的拥有者都可以随时删除 VPC 对等连接。您还可以删除您所请求的状态仍为 `pending-acceptance` 的 VPC 对等连接。

您无法删除处于 `rejected` 状态的 VPC 对等连接。我们会自动为您删除连接。

在 Amazon VPC 控制台中删除作为活动 VPC 对等连接的一部分的 VPC 也会删除该 VPC 对等连接。如果您请求了与其他账户中的 VPC 建立 VPC 对等连接，您在另一方接受此请求之前删除了您的 VPC，则 VPC 对等连接也将被删除。您无法删除其他账户中的 VPC 发出的 `pending-acceptance` 请求所涉及到的 VPC。您必须首先拒绝此 VPC 对等连接请求。

删除对等连接时，状态设置为 `Deleting`，然后将变为 `Deleted`。连接删除后将不能接受、拒绝或编辑。有关对等连接保持多长时间可见的更多信息，请参阅 VPC 对等连接的生命周期。

要删除 VPC 对等连接，请按以下步骤操作

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Peering Connections（对等连接）。
3. 选择 VPC 对等连接。
4. 依次选择 Actions（操作）、Delete peering connection（删除对等连接）。
5. 提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

使用命令行删除 VPC 对等连接

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

对 VPC 对等连接进行问题排查

如果您在从对等 VPC 中的资源连接到 VPC 中的资源时遇到问题，请执行以下操作：

- 对于每个 VPC 中的每个资源，验证其子网的路由表中是否包含将以对等 VPC 为目的地的流量发送到 VPC 对等连接的路由。此举可确保网络流量在两个 VPC 之间正常流动。有关更多信息，请参阅更新路由表。
- 对于任何涉及的 EC2 实例，验证这些实例的安全组是否允许来自对等 VPC 的入站和出站流量。安全组规则可控制允许访问 EC2 实例的流量。有关更多信息，请参阅 引用对等安全组。
- 检查包含您资源的子网的网络 ACL 是否允许来自对等 VPC 的必要流量。网络 ACL 是额外的安全层，可在子网级别过滤流量。

若仍有问题，则可使用 Reachability Analyzer。Reachability Analyzer 可以帮助识别导致两个 VPC 之间出现连接问题的特定组件（无论是路由表、安全组还是网络 ACL）。有关更多信息，请参阅 Reachability Analyzer 角色指南。

彻底验证 VPC 网络配置是排查和解决 VPC 对等连接可能出现的任何问题的关键措施。

常见 VPC 对等连接配置

本节旨在介绍可实现的两种常见 VPC 对等连接配置：

- 包含指向整个 VPC 的路由的 VPC 对等配置：在此配置中，您可以在每个 VPC 的路由表中创建一个路由，将所有目标为对等 VPC 的流量发送到 VPC 对等连接。这使得一个 VPC 中的任何资源都能与对等 VPC 中的任何资源进行通信，从而简化管理。不过，这也意味着 VPC 之间的所有流量都将流经对等连接；如果流量很大，对等连接可能会成为瓶颈。
- 具有特定路由的 VPC 对等配置：您也可以在每个 VPC 的路由表中创建更精细的路由，这些路由只能将流量发送到对等 VPC 中的特定子网或资源。这使得您可以将流经对等连接的流量限制在必要范围内，从而提高效率。不过，该操作也需要更多的维护，因为只要在对等 VPC 中添加了需要通信的新资源，就需要更新路由表。

最佳方法取决于各种因素，诸如 VPC 架构的规模和复杂性、VPC 之间的预期流量以及组织在安全和资源访问权限方面的需求。许多企业采用混合方法，为常见流量模式提供广泛路由，为更敏感或带宽密集型应用场景提供特定路由。

配置

- 包含指向整个 VPC 的路由的 VPC 对等配置
- 具有特定路由的 VPC 对等配置

包含指向整个 VPC 的路由的 VPC 对等配置

您可以配置 VPC 对等连接，以便路由表可以访问对等 VPC 的整个 CIDR 块。有关可能需要特定 VPC 对等连接配置的方案的更多信息，请参阅VPC 对等连接的联网场景。有关创建和使用 VPC 对等连接的更多信息，请参阅VPC 对等连接。

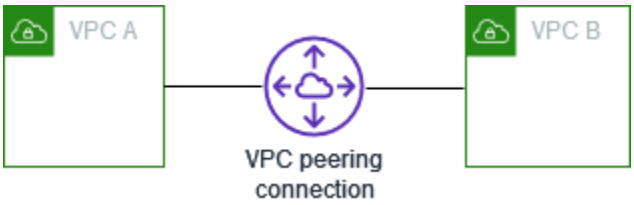
有关更新路由表的更多信息，请参阅为 VPC 对等连接更新路由表。

配置

- 相互对等的两个 VPC
- 一个 VPC 与两个 VPC 具有对等关系
- 相互对等的三个 VPC
- 相互对等的多个 VPC

相互对等的两个 VPC

在此配置中，VPC A 和 VPC B 之间具有对等连接 (pcx-11112222)。这些 VPC 处于同一 AWS 账户中，并且其 CIDR 块没有重叠。



当您有两个需要相互资源访问权限的 VPC 时，可能会用到这种类型的配置。例如，您为账户记录设置 VPC A，为财务记录设置 VPC B，现在需要这两个 VPC 能够无限制地访问相互的资源。

单个 VPC CIDR

使用将对等 VPC 的 CIDR 块的流量发送到 VPC 对等连接的路由，从而更新每个 VPC 的路由表。

路由表	目的地	目标
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-11112222

多个 IPv4 VPC CIDR

如果 VPC A 和 VPC B 有多个关联的 IPv4 CIDR 块，则可以使用对等 VPC 的部分或全部 IPv4 CIDR 块的路由来更新每个 VPC 的路由表。

路由表	目的地	目标
VPC A	*VPC A CIDR 1*	本地
	VPC A CIDR 2	本地
	VPC B CIDR 1	pcx-11112222

路由表	目的地	目标
	VPC B CIDR 2	pcx-11112222
VPC B	*VPC B CIDR 1*	本地
	VPC B CIDR 2	本地
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

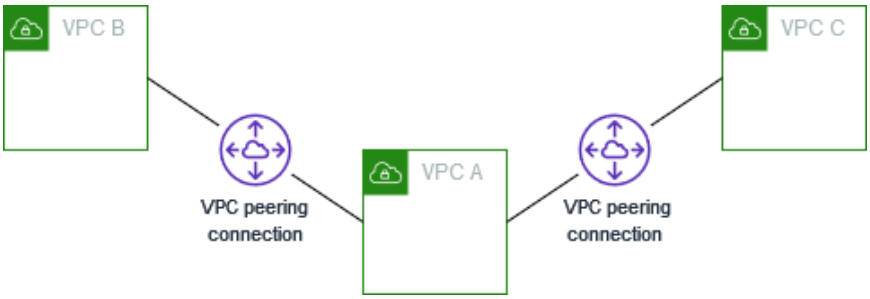
IPv4 和 IPv6 VPC CIDR

如果 VPC A 和 VPC B 有关联的 IPv6 CIDR 块，则可以使用对等 VPC 的 IPv4 和 IPv6 CIDR 块的路由来更新每个 VPC 的路由表。

路由表	目的地	目标
VPC A	*VPC A IPv4 CIDR*	本地
	VPC A IPv6 CIDR	本地
	VPC B IPv4 CIDR	pcx-11112222
	VPC B IPv6 CIDR	pcx-11112222
VPC B	*VPC B IPv4 CIDR*	本地
	VPC B IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-11112222
	VPC A IPv6 CIDR	pcx-11112222

一个 VPC 与两个 VPC 具有对等关系

此配置包含一个中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-12121212)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-23232323)。所有这三个 VPC 都处于同一 AWS 账户中，并且其 CIDR 块没有重叠。



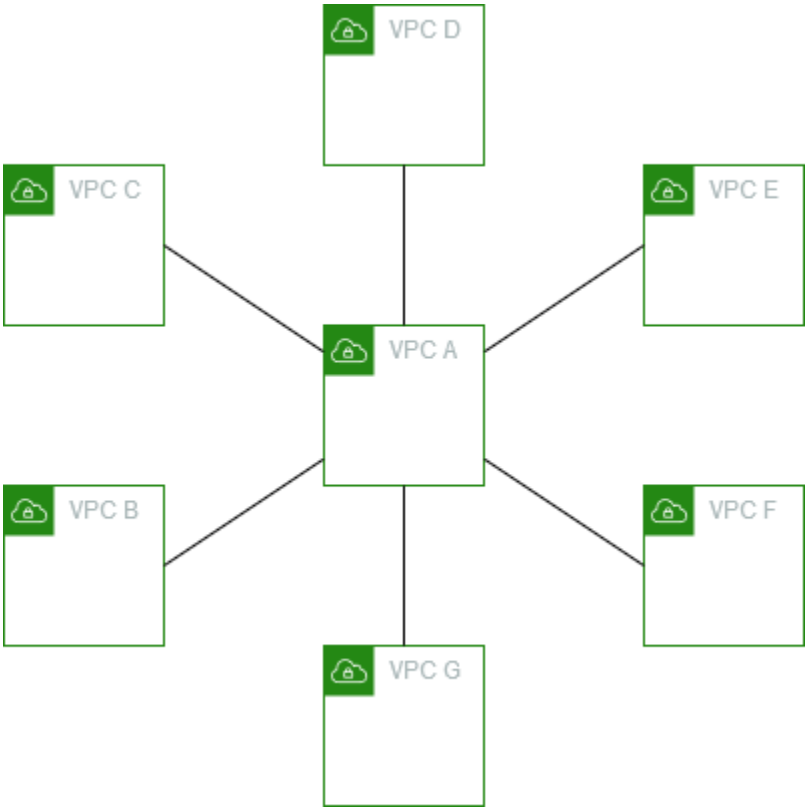
VPC B 和 VPC C 无法通过 VPC A 直接相互发送流量，因为 VPC 对等不支持传递性对等关系。您可以在 VPC B 与 VPC C 之间创建 VPC 对等连接，如 相互对等的三个 VPC 中所示。有关不支持的对等方案的更多信息，请参阅the section called “VPC 对等限制”。

当您在中心 VPC 上拥有其他 VPC 需要访问的资源（如服务存储库）时，可能需要使用这种配置。其他 VPC 无需访问相互的资源；它们只需访问中心 VPC 上的资源。

按如下方式更新每个 VPC 的路由表，以便在每个 VPC 中使用一个 CIDR 块来实现此配置。

路由表	目的地	目标
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	本地
	VPC A CIDR	pcx-23232323

您可以将此配置扩展到其他 VPC。例如，VPC A 与 VPC B 通过同时使用 IPv4 和 IPv6 CIDR 的 VPC G 进行对等，但其他 VPC 之间并未相互对等。在此图中，线条表示 VPC 对等连接。



按以下方式更新路由表。

路由表	目的地	目标
VPC A	*VPC A IPv4 CIDR*	本地
	VPC A IPv6 CIDR	本地
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee

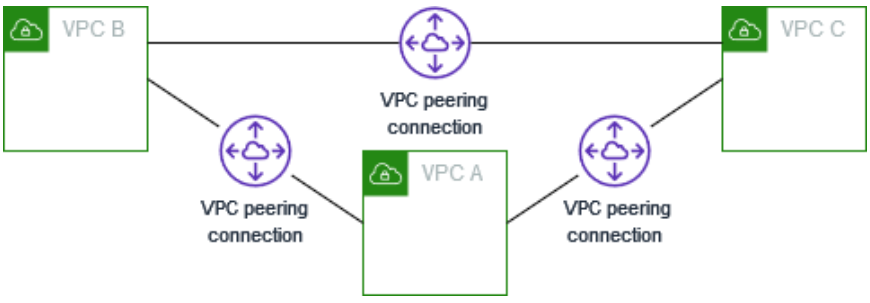
路由表	目的地	目标
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	本地
	VPC B IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPC C	*VPC C IPv4 CIDR*	本地
	VPC C IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
VPC D	*VPC D IPv4 CIDR*	本地
	VPC D IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
VPC E	*VPC E IPv4 CIDR*	本地
	VPC E IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaaeeee

路由表	目的地	目标
	VPC A IPv6 CIDR	pcx-aaaaeeee
VPC F	*VPC F IPv4 CIDR*	本地
	VPC F IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
VPC G	*VPC G IPv4 CIDR*	本地
	VPC G IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg

相互对等的三个 VPC

在此配置中，同一 AWS 账户中有三个 VPC，并且其 CIDR 块没有重叠。这些 VPC 全网格对等，具体如下：

- VPC A 通过 VPC 对等连接 pcx-aaaabbbb 与 VPC B 对等
- VPC A 通过 VPC 对等连接 pcx-aaaacccc 与 VPC C 对等
- VPC B 通过 VPC 对等连接 pcx-bbbbcccc 与 VPC C 对等



当您具有需要无限制地相互共享资源的 VPC 时，则可能需要使用这种配置。例如，作为文件共享系统。

按如下方式更新每个 VPC 的路由表，以实现此配置。

路由表	目的地	目标
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	本地
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

如果 VPC A 和 VPC B 同时具有 IPv4 和 IPv6 CIDR 块，但 VPC C 没有 IPv6 CIDR 块，请按如下方式更新路由表。VPC A 和 VPC B 中的资源可以使用 IPv6 通过 VPC 对等连接进行通信。但是，VPC C 无法使用 IPv6 与 VPC A 或 VPC B 进行通信。

路由表	目标位置	目标
VPC A	*VPC A IPv4 CIDR*	本地
	VPC A IPv6 CIDR	本地
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
VPC B	*VPC B IPv4 CIDR*	本地

路由表	目标位置	目标
	VPC B IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
VPC C	*VPC C IPv4 CIDR*	本地
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc

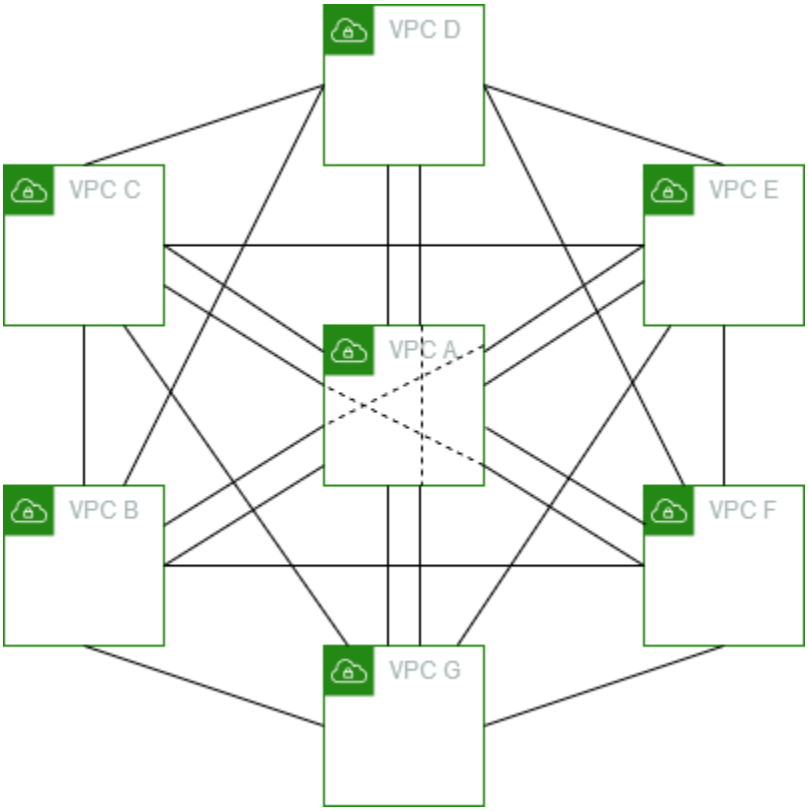
相互对等的多个 VPC

此配置包含七个具有全网格配置的对等 VPC。这些 VPC 处于同一 AWS 账户中，并且其 CIDR 块没有重叠。

VPC	VPC	VPC 对等连接
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd
B	E	pcx-bbbbeeee

VPC	VPC	VPC 对等连接
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

当您有多个 VPC 并且必须能够无限制地访问相互资源时，则可能需要使用这种配置。例如，作为文件共享网络。在此图中，线条表示 VPC 对等连接。



按如下方式更新每个 VPC 的路由表，以实现此配置。

路由表	目的地	目标
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-aaaabbbb

路由表	目的地	目标
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G CIDR	pcx-bbbbgggg
VPC C	*VPC C CIDR*	本地
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-cccceeee
	VPC F CIDR	pcx-ccccffff
	VPC G CIDR	pcx-ccccgggg
VPC D	*VPC D CIDR*	本地
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg
VPC E	*VPC E CIDR*	本地

路由表	目的地	目标
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-eeeegggg
VPC F	*VPC F CIDR*	本地
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC E CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-ffffgggg
VPC G	*VPC G CIDR*	本地
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg
	VPC D CIDR	pcx-ddddgggg
	VPC E CIDR	pcx-eeeegggg
	VPC F CIDR	pcx-ffffgggg

如果所有 VPC 都具有关联的 IPv6 CIDR 块，请按以下方式更新路由表。

路由表	目的地	目标
VPC A	*VPC A IPv4 CIDR*	本地
	VPC A IPv6 CIDR	本地
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	本地
	VPC B IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc

路由表	目的地	目标
	VPC C IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-bbbbdddd
	VPC D IPv6 CIDR	pcx-bbbbdddd
	VPC E IPv4 CIDR	pcx-bbbbeeee
	VPC E IPv6 CIDR	pcx-bbbbeeee
	VPC F IPv4 CIDR	pcx-bbbbffff
	VPC F IPv6 CIDR	pcx-bbbbffff
	VPC G IPv4 CIDR	pcx-bbbbgggg
	VPC G IPv6 CIDR	pcx-bbbbgggg
VPC C	*VPC C IPv4 CIDR*	本地
	VPC C IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc
	VPC B IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-cccceeee
	VPC E IPv6 CIDR	pcx-cccceeee
	VPC F IPv4 CIDR	pcx-ccccffff

路由表	目的地	目标
	VPC F IPv4 CIDR	pcx-ccccffff
	VPC G IPv4 CIDR	pcx-ccccgggg
	VPC G IPv6 CIDR	pcx-ccccgggg
VPC D	*VPC D IPv4 CIDR*	本地
	VPC D IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4 CIDR	pcx-bbbbdddd
	VPC B IPv6 CIDR	pcx-bbbbdddd
	VPC C IPv4 CIDR	pcx-ccccdddd
	VPC C IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-ddddeeee
	VPC E IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-ddddffff
	VPC F IPv6 CIDR	pcx-ddddffff
	VPC G IPv4 CIDR	pcx-ddddgggg
	VPC G IPv6 CIDR	pcx-ddddgggg
VPC E	*VPC E IPv4 CIDR*	本地
	VPC E IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaaeeee

路由表	目的地	目标
	VPC A IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4 CIDR	pcx-bbbbeeee
	VPC B IPv6 CIDR	pcx-bbbbeeee
	VPC C IPv4 CIDR	pcx-cccceeee
	VPC C IPv6 CIDR	pcx-cccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-eeeeffff
	VPC F IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-eeeegggg
	VPC G IPv6 CIDR	pcx-eeeegggg
VPC F	*VPC F IPv4 CIDR*	本地
	VPC F IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff
	VPC C IPv4 CIDR	pcx-ccccffff
	VPC C IPv6 CIDR	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff

路由表	目的地	目标
	VPC D IPv6 CIDR	pcx-ddddffff
	VPC E IPv4 CIDR	pcx-eeeeffff
	VPC E IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-ffffgggg
	VPC G IPv6 CIDR	pcx-ffffgggg
VPC G	*VPC G IPv4 CIDR*	本地
	VPC G IPv6 CIDR	本地
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4 CIDR	pcx-bbbbgggg
	VPC B IPv6 CIDR	pcx-bbbbgggg
	VPC C IPv4 CIDR	pcx-ccccgggg
	VPC C IPv6 CIDR	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6 CIDR	pcx-ddddgggg
	VPC E IPv4 CIDR	pcx-eeeegggg
	VPC E IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4 CIDR	pcx-ffffgggg
	VPC F IPv6 CIDR	pcx-ffffgggg

具有特定路由的 VPC 对等配置

您可以为 VPC 对等连接配置路由表，以限制对等 VPC 内子网 CIDR 块、特定 CIDR 块（如果 VPC 有多个 CIDR 块）或特定资源的访问权限。在这些示例中，一个中心 VPC 与具有重叠 CIDR 块的至少两个或更多 VPC 对等连接。

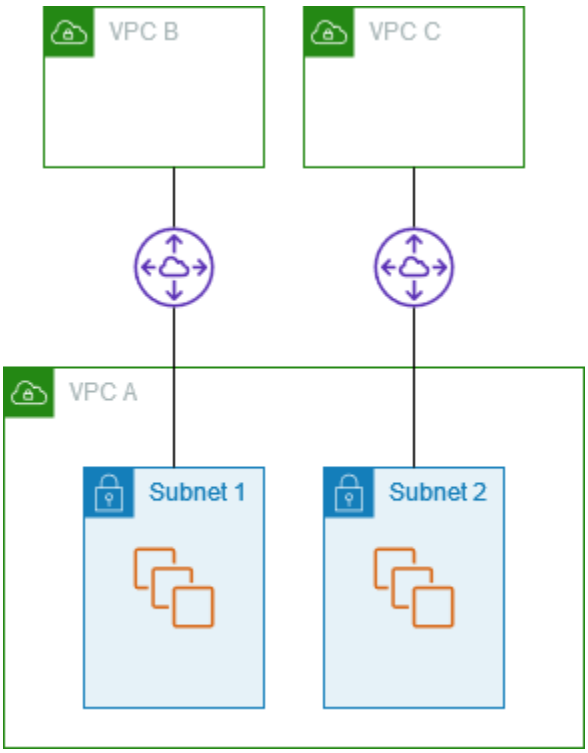
有关可能需要特定 VPC 对等连接配置的方案示例，请参阅VPC 对等连接的联网场景。有关使用 VPC 对等连接的更多信息，请参阅 VPC 对等连接。有关更新路由表的更多信息，请参阅为 VPC 对等连接更新路由表。

配置

- 访问一个 VPC 中特定子网的两个 VPC
- 访问一个 VPC 中特定 CIDR 块的两个 VPC
- 访问两个 VPC 中特定子网的一个 VPC
- 一个 VPC 中可访问两个 VPC 中特定实例的实例
- 一个使用最长前缀匹配来访问两个 VPC 的 VPC
- 多 VPC 配置

访问一个 VPC 中特定子网的两个 VPC

此配置包含一个具有两个子网的中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-aaaabbbb)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-aaaacccc)。每个 VPC 只需要访问 VPC A 中一个子网内的资源。



子网 1 的路由表使用 VPC 对等连接 pcx-aaaabbbb 来访问 VPC B 的整个 CIDR 块。VPC B 的路由表使用 pcx-aaaabbbb 来仅访问 VPC A 中子网 1 的 CIDR 块。子网 2 的路由表使用 VPC 对等连接 pcx-aaaacccc 来访问 VPC C 的整个 CIDR 块。VPC C 的路由表使用 pcx-aaaacccc 来仅访问 VPC A 中子网 2 的 CIDR 块。

路由表	目的地	Target
子网 1（VPC A）	*VPC A CIDR*	本地
	VPC B CIDR	pcx-aaaabbbb
子网 2（VPC A）	*VPC A CIDR*	本地
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	本地
	## 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	本地
	## 2 CIDR	pcx-aaaacccc

您可以将此配置扩展到多个 CIDR 块。假设 VPC A 和 VPC B 同时具有 IPv4 和 IPv6 CIDR 块，子网 1 同时具有关联的 IPv6 CIDR 块。您可以使用 VPC 对等连接使 VPC B 能够通过 IPv6 与 VPC A 中的子网 1 通信。为此，请为 VPC A 的路由表添加一条目的地为 VPC B 的 IPv6 CIDR 块的路由，并为 VPC B 的路由表添加一条目的地为 VPC A 中子网 1 的 IPv6 CIDR 块的路由。

路由表	目的地	目标	备注
VPC A 中的子网 1	*VPC A IPv4 CIDR*	本地	
	VPC A IPv6 CIDR	本地	VPC 中自动添加的用于 IPv6 通信的本地路由。
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	到 VPC B 的 IPv6 CIDR 块的路由。
VPC A 中的子网 2	*VPC A IPv4 CIDR*	本地	
	VPC A IPv6 CIDR	本地	VPC 中自动添加的用于 IPv6 通信的本地路由。
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	本地	
	VPC B IPv6 CIDR	本地	VPC 中自动添加的用于 IPv6 通信的本地路由。
	## 1 IPv4 CIDR	pcx-aaaabbbb	
	## 1 IPv6 CIDR	pcx-aaaabbbb	到 VPC A 的 IPv6 CIDR 块的路由。
VPC C	*VPC C IPv4 CIDR*	本地	
	## 2 IPv4 CIDR	pcx-aaaacccc	

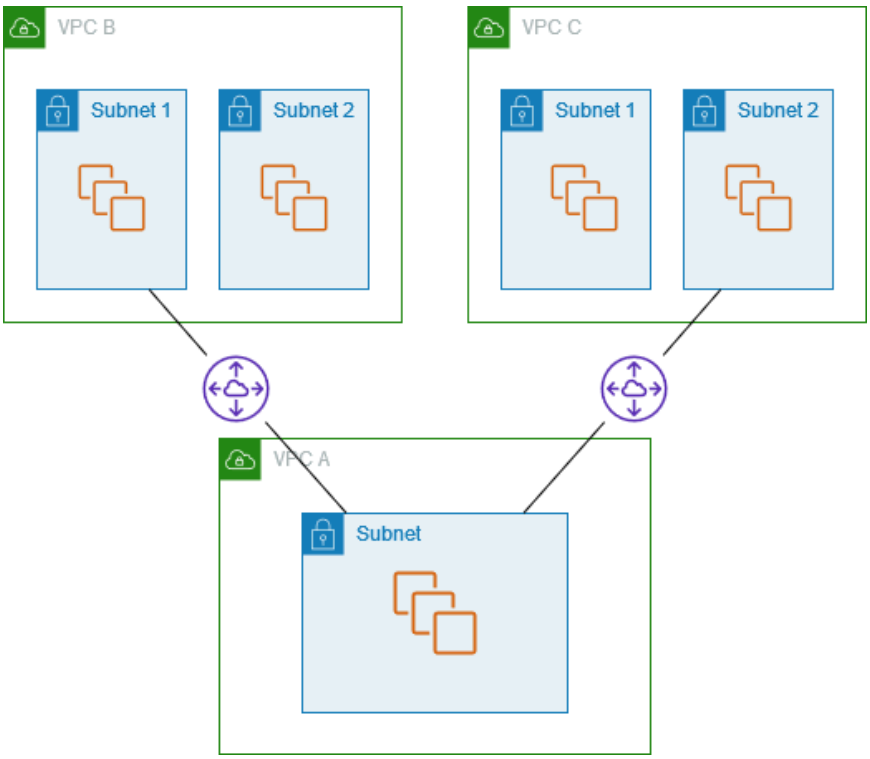
访问一个 VPC 中特定 CIDR 块的两个 VPC

此配置包含一个中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-aaaabbbb)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-aaaacccc)。VPC A 为 VPC 对等连接提供了一个 CIDR 块。

路由表	目的地	Target
VPC A	*VPC A CIDR 1*	本地
	VPC A CIDR 2	本地
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	本地
	VPC A CIDR 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	本地
	VPC A CIDR 2	pcx-aaaacccc

访问两个 VPC 中特定子网的一个 VPC

此配置包含一个具有一个子网的中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-aaaabbbb)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-aaaacccc)。VPC B 和 VPC C 分别有两个子网。VPC A 与 VPC B 之间的对等连接仅使用 VPC B 中的一个子网。VPC A 与 VPC C 之间的对等连接仅使用 VPC C 中的一个子网。



当您的中心 VPC 具有其他 VPC 需要访问的单个资源集（如 Active Directory 服务）时，请使用这种类型的配置。中心 VPC 无需可完全访问与之对等的 VPC。

VPC A 的路由表使用对等连接来仅访问对等 VPC 中的特定子网。子网 1 的路由表使用与 VPC A 的对等连接来访问 VPC A 中的子网。子网 2 的路由表使用与 VPC A 的对等连接来访问 VPC A 中的子网。

路由表	目的地	Target
VPC A	*VPC A CIDR*	本地
	## 1 CIDR	pcx-aaaabbbb
	## 2 CIDR	pcx-aaaacccc
子网 1（VPC B）	*VPC B CIDR*	本地
	VPC A CIDR ####	pcx-aaaabbbb
子网 2（VPC C）	*VPC C CIDR*	本地
	VPC A CIDR ####	pcx-aaaacccc

响应流量路由

如果您的某个 VPC 与多个 VPC 建立了对等连接，并且这些 VPC 具有重叠或匹配的 CIDR 块，请确保路由表配置不会导致将响应流量从您的 VPC 发送到错误的 VPC。AWS 不支持在 VPC 对等连接中进行单播反向传输路径转发，即检查数据包的源 IP 并将应答数据包路由回源。

例如，VPC A 与 VPC B 和 VPC C 具有对等关系。VPC B 和 VPC C 具有匹配 CIDR 块，并且其子网具有匹配 CIDR 块。VPC B 中子网 2 的路由表指向 VPC 对等连接 pcx-aaaabbbb 以访问 VPC A 的子网。VPC A 路由表配置为将目的地为 VPC CIDR 的流量发送到对等连接 pcx-aaaaccccc。

路由表	目的地	Target
子网 2（VPC B）	*VPC B CIDR*	本地
	VPC A CIDR ####	pcx-aaaabbbb
VPC A	*VPC A CIDR*	本地
	VPC C CIDR	pcx-aaaacccc

假设 VPC B 中子网 2 中的实例使用 VPC 对等连接 pcx-aaaabbbb 向 VPC A 中的 Active Directory 服务器发送流量。VPC A 向 Active Directory 服务器发送响应流量。但是，VPC A 路由表配置为将 VPC CIDR 范围中的所有流量都发送到 VPC 对等连接 pcx-aaaaccccc。如果 VPC C 中的子网 2 具有与 VPC B 的子网 2 中的实例相同的 IP 地址，则它从 VPC A 接收响应流量。VPC B 中子网 2 内的实例不接收对其到 VPC A 的请求的响应。

为了防止这种情况，您可以将某个特定路由添加到 VPC A 路由表，其目的地为 VPC B 中子网 2 的 CIDR，目标为 pcx-aaaabbbb。由于新路由更加具体，因此，目的地为子网 2 CIDR 的流量将路由至 VPC 对等连接 pcx-aaaabbbb

或者，在以下示例中，VPC A 路由表针对每个 VPC 对等连接都具有每个子网的路由。VPC A 可以与 VPC B 中的子网 2 以及 VPC C 中的子网 1 进行通信。如果您需要添加与另一子网（与 VPC B 及 VPC C 位于相同地址范围）的其他 VPC 对等连接，则此情况非常有用，您只需为该特定子网添加其他路由即可。

目标位置	目标
VPC A CIDR	本地

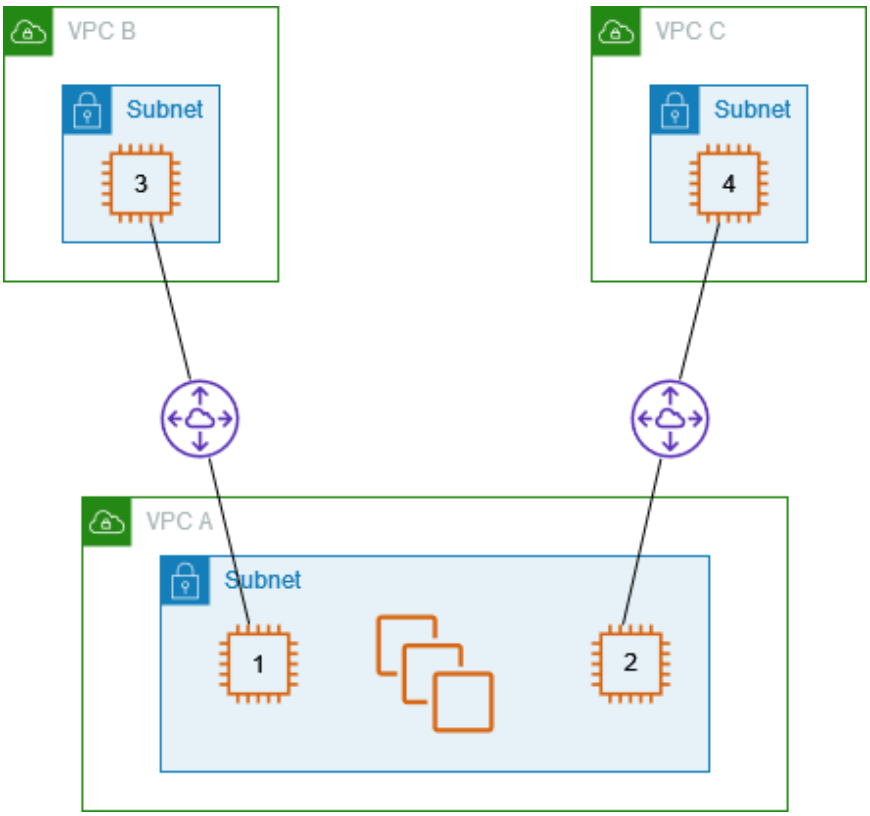
目标位置	目标
## 2 CIDR	pcx-aaaabbbb
## 1 CIDR	pcx-aaaacccc

或者，根据您的使用案例，您可以创建到 VPC B 中特定 IP 地址的路由，确保将流量路由回正确的服务器 (路由表使用最长前缀匹配来确定路由的优先级)：

目标位置	目标
VPC A CIDR	本地
## 2 #### IP ##	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

一个 VPC 中可访问两个 VPC 中特定实例的实例

此配置包含一个具有一个子网的中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-aaaabbbb)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-aaaacccc)。VPC A 有一个子网，并且每个对等连接都有一个实例。您可使用这种类型的配置将对等流量限制到特定实例。

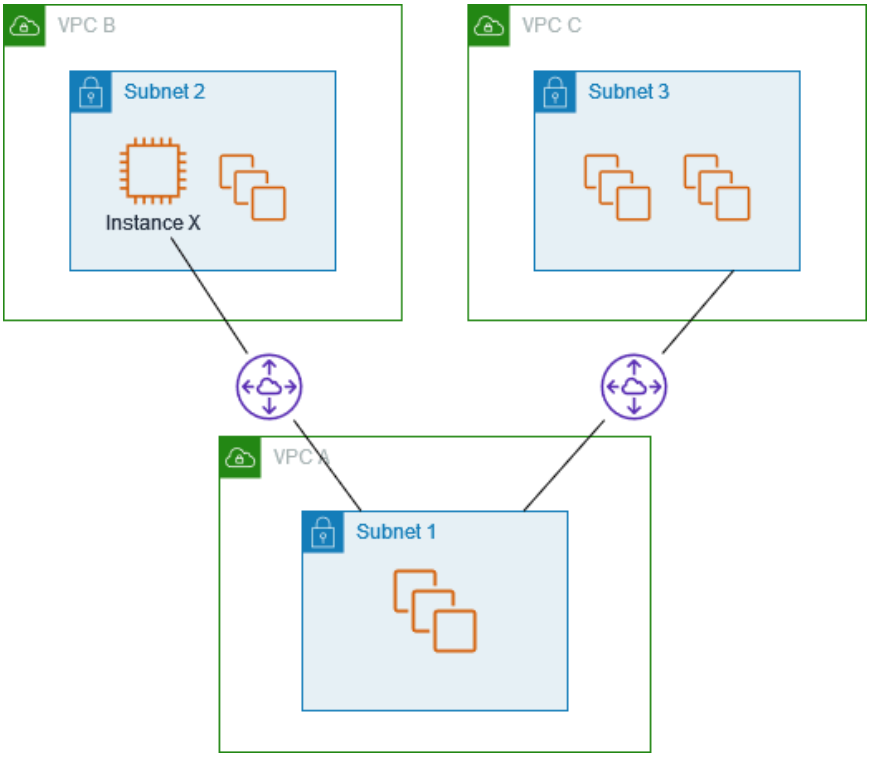


每个 VPC 的路由表都指向相关 VPC 对等连接，以访问对等 VPC 中的单个 IP 地址 (因而访问特定实例)。

路由表	目的地	Target
VPC A	*VPC A CIDR*	本地
	## 3 IP ##	pcx-aaaabbbb
	## 4 IP ##	pcx-aaaacccc
VPC B	*VPC B CIDR*	本地
	## 1 IP ##	pcx-aaaabbbb
VPC C	*VPC C CIDR*	本地
	## 2 IP ##	pcx-aaaacccc

一个使用最长前缀匹配来访问两个 VPC 的 VPC

此配置包含一个具有一个子网的中心 VPC（VPC A）、VPC A 与 VPC B 之间的 VPC 对等连接 (pcx-aaaabbbb)，以及 VPC A 与 VPC C 之间的 VPC 对等连接 (pcx-aaaacccc)。VPC B 和 VPC C 具有匹配 CIDR 块。您使用 VPC 对等连接 pcx-aaaabbbb 在 VPC A 与 VPC B 中的特定实例之间路由流量。以 VPC B 和 VPC C 共享的 CIDR 地址范围为目标的所有其他流量均通过 pcx-aaaacccc 路由到 VPC C。



VPC 路由表使用最长前缀匹配选择跨预期 VPC 对等连接的最具体路由。所有其他流量都通过下一个匹配路由 (在此例中，跨 VPC 对等连接 pcx-aaaacccc) 进行路由。

路由表	目的地	Target
VPC A	*VPC A CIDR #*	本地
	## X IP ##	pcx-aaaabbbb
	VPC C CIDR #	pcx-aaaacccc
VPC B	*VPC B CIDR #*	本地
	VPC A CIDR #	pcx-aaaabbbb

路由表	目的地	Target
VPC C	*VPC C CIDR #*	本地
	VPC A CIDR #	pcx-aaaacccc

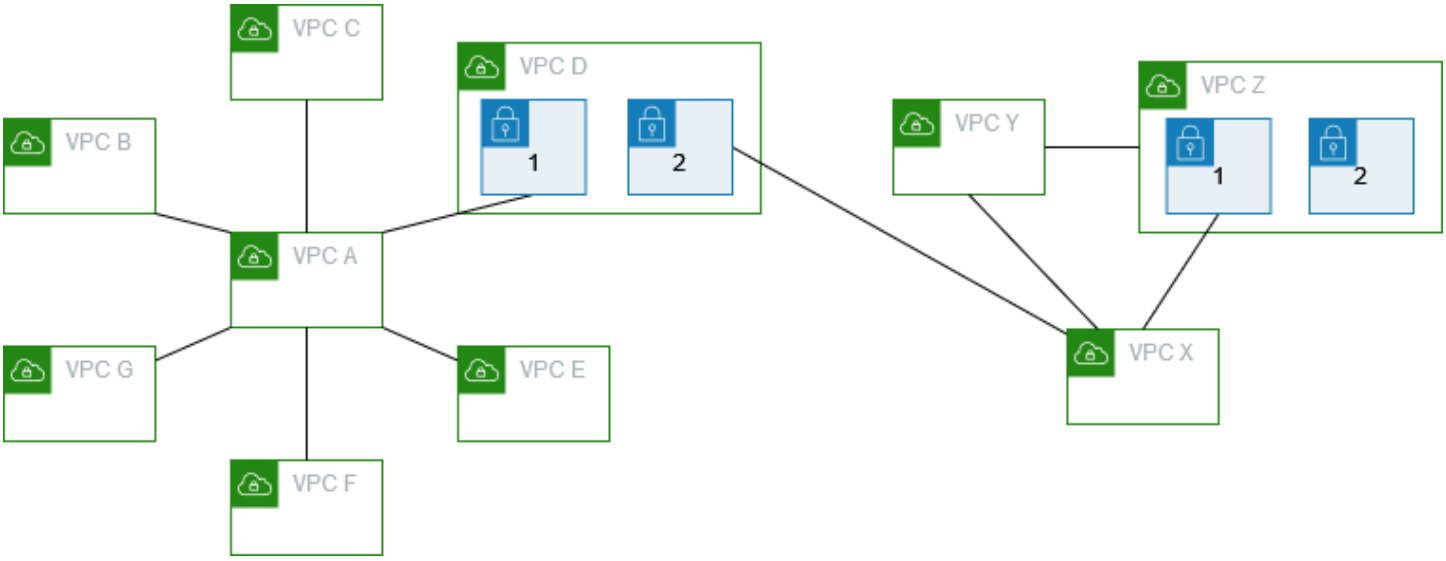
> **Important**
>
> 如果 VPC B 中除实例 X 之外的实例向 VPC A 发送流量，则响应流量可能会路由到 VPC C，而不是 VPC B。有关更多信息，请参阅 响应流量路由。

多 VPC 配置

在此配置中，一个中心 VPC (VPC A) 采用轮辐型配置与多个 VPC 建立对等连接。您还具有采用完全网状配置对等的三个 VPC（VPC X、Y 和 Z）。

VPC D 还具有与 VPC X 之间的 VPC 对等连接（`pcx-ddddxxxx`）。VPC A 和 VPC X 具有重叠 CIDR 块。这意味着 VPC A 与 VPC D 之间的对等流量仅限于 VPC D 中的特定子网（子网 1）。这是为了确保在收到来自 VPC A 或 VPC X 的请求时，VPC D 会将响应流量发送到正确的 VPC。AWS 不支持在 VPC 对等连接中进行单播反向传输路径转发，即检查数据包的源 IP 并将应答数据包路由回该源。有关更多信息，请参阅 响应流量路由。

同样，VPC D 和 VPC Z 具有重叠 CIDR 块。VPC D 与 VPC X 之间的对等流量限制为 VPC D 中的 子网 2，VPC X 与 VPC Z 之间的对等流量限制为 VPC Z 中的子网 1。这样是为了确保如果 VPC X 从 VPC D 或 VPC Z 接收对等流量，则它会将响应流量发送回正确的 VPC。



VPC B、C、E、F 和 G 的路由表指向相关对等连接以访问 VPC A 的完整 CIDR 块，VPC A 的路由表指向 VPC B、C、E、F 和 G 的相关对等连接以访问其完整 CIDR 块。对于对等连接 pcx-aaaadddd，VPC A 的路由表仅将流量路由到 VPC D 中的子网 1，而 VPC D 中子网 1 的路由表指向 VPC A 的完整 CIDR 块。

VPC Y 的路由表指向相关对等连接以访问 VPC X 和 VPC Z 的完整 CIDR 块，VPC Z 的路由表指向相关对等连接以访问 VPC Y 的完整 CIDR 块。VPC Z 中子网 1 的路由表指向相关对等连接以访问 VPC Y 的完整 CIDR 块。VPC X 的路由表指向相关对等连接以访问 VPC D 中的子网 2 和 VPC Z 中的子网 1。

路由表	目的地	Target
VPC A	*VPC A CIDR*	本地
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D #### 1 CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg

路由表	目的地	Target
VPC B	*VPC B CIDR*	本地
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	本地
	VPC A CIDR	pcx-aaaacccc
VPC D 中的子网 1	*VPC D CIDR*	本地
	VPC A CIDR	pcx-aaaadddd
VPC D 中的子网 2	*VPC D CIDR*	本地
	VPC X CIDR	pcx-ddddxxxx
VPC E	*VPC E CIDR*	本地
	VPC A CIDR	pcx-aaaaeeee
VPC F	*VPC F CIDR*	本地
	VPC A CIDR	pcx-aaaaffff
VPC G	*VPC G CIDR*	本地
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	本地
	VPC D #### 2 CIDR	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	VPC Z #### 1 CIDR	pcx-xxxxzzzz
VPC Y	*VPC Y CIDR*	本地
	VPC X CIDR	pcx-xxxxyyyy

路由表	目的地	Target
	VPC Z CIDR	pcx-yyyyzzzz
VPC Z	*VPC Z CIDR*	本地
	VPC Y CIDR	pcx-yyyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

VPC 对等连接的联网场景

您可能出于某些原因需要在您的 VPC 之间，或是在您拥有的 VPC 与不同 AWS 账户中的 VPC 之间设置 VPC 对等连接。以下方案可以帮助您确定最适合于您联网要求的配置。

场景

- 使两个或更多 VPC 具有对等关系以提供对资源的完全访问
- 与一个 VPC 对等以访问集中资源

使两个或更多 VPC 具有对等关系以提供对资源的完全访问

在此方案中，您希望您的两个或更多 VPC 具有对等关系，以便在所有 VPC 之间实现完全资源共享。下面是一些示例：

- 您的公司具有一个用于财务部门的 VPC，以及另一个用于会计部门的 VPC。财务部门需要访问会计部门中的所有资源，而会计部门需要访问财务部门中的所有资源。
- 您的公司具有多个 IT 部门，每个部门具有自己的 VPC。某些 VPC 处于同一 AWS 账户下，而其他 VPC 处于另一个 AWS 账户下。您希望所有 VPC 相互对等，以便使各个 IT 部门可以完全访问相互的资源。

有关如何为此方案设置 VPC 对等连接配置和路由表的更多信息，请参阅以下文档：

- 相互对等的两个 VPC
- 相互对等的三个 VPC
- 相互对等的多个 VPC

有关在 Amazon VPC 控制台中创建和使用 VPC 对等连接的更多信息，请参阅VPC 对等连接。

与一个 VPC 对等以访问集中资源

在此方案中，您具有一个中心 VPC，其中包含要与其他 VPC 共享的资源。中心 VPC 可能需要对等 VPC 的完全或部分访问权限，同样，对等 VPC 可能需要中心 VPC 的完全或部分访问权限。下面是一些示例：

- 您公司的 IT 部门具有一个用于文件共享的 VPC。您希望其他 VPC 与该中心 VPC 对等，但是，不希望其他 VPC 相互发送流量。
- 您的公司具有一个要与客户共享的 VPC。每个客户都可以与您的 VPC 创建 VPC 对等连接，但是，客户无法向与您 VPC 对等的其他 VPC 路由流量，也不了解其他客户的路由。
- 您具有一个用于 Active Directory 服务的 VPC。对等 VPC 中的特定实例向 Active Directory 服务器发送请求，需要中心 VPC 的完全访问权限。中心 VPC 无需对等 VPC 的完全访问权限；它只需将响应流量路由到特定实例。

有关在 Amazon VPC 控制台中创建和使用 VPC 对等连接的更多信息，请参阅VPC 对等连接。

适用于 VPC 对等连接的 Identity and Access Management

默认情况下，用户无法创建或修改 VPC 对等连接。要授予对 VPC 对等连接资源的访问权限，请将 IAM policy 附加到角等 IAM 身份。

示例

- 示例：创建 VPC 对等连接
- 示例：接受 VPC 对等连接
- 示例：删除 VPC 对等连接
- 示例：在特定账户中工作
- 示例：使用控制台管理 VPC 对等连接

有关 Amazon VPC 操作以及每个操作支持的资源和条件键的列表，请参阅《服务授权参考》中的 Actions, resources, and condition keys for Amazon EC2。

示例：创建 VPC 对等连接

以下策略授予用户权限以使用标记有 `Purpose=Peering` 的 VPC 来创建 VPC 对等连接请求。第一条语句对 VPC 资源应用条件键 (`ec2:ResourceTag`)。请注意，`CreateVpcPeeringConnection` 操作的 VPC 资源始终为请求者 VPC。

第二条语句授予用户权限以创建 VPC 对等连接资源，因此使用 * 通配符代替特定资源 ID。

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
```

```
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
    }
  ]
}
```

以下策略授予特定 AWS 账户中的用户权限，以使用指定区域中的任何 VPC 创建 VPC 对等连接，但是仅当接受对等连接的 VPC 是特定账户中的特定 VPC 时。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-
connection/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:AccepterVpc": "arn:aws:ec2:us-
east-1:111122223333:vpc/vpc-1234567890abcdef0"
                }
            }
        }
    ]
}
```

示例：接受 VPC 对等连接

以下策略授予用户权限，以接受来自特定 AWS 账户的 VPC 对等连接请求。这样有助于防止用户接受来自未知账户的 VPC 对等连接请求。语句使用 ec2:RequesterVpc 条件键强制实施此策略。

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:us-east-1:111122223333:vpc/*"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
    }
  ]
}
```

以下策略授予用户权限，以便在仅当 VPC 具有标签 Purpose=Peering 时才接受 VPC 对等请求。

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}
```

示例：删除 VPC 对等连接

以下策略授予特定账户中的用户权限以删除任何 VPC 对等连接，使用指定 VPC（处于同一账户中）的连接除外。该策略同时指定 `ec2:AccepterVpc` 和 `ec2:RequesterVpc` 条件密钥，因为 VPC 可能是原始 VPC 对等连接请求中的请求者 VPC 或对等方 VPC。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-
connection/*",
            "Condition": {
                "ArnNotEquals": {
                    "ec2:AccepterVpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0",
                    "ec2:RequesterVpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-0abcdef1234567890"
                }
            }
        }
    ]
}
```

示例：在特定账户中工作

以下策略授予用户权限以在特定账户中处理 VPC 对等连接。用户可以查看、创建、接受、拒绝和删除 VPC 对等连接，前提是他们都处于相同的 AWS 账户中。

第一条语句授予用户权限以查看所有 VPC 对等连接。在这种情况下，Resource 元素需要 * 通配符，因为此 API 操作 (DescribeVpcPeeringConnections) 当前不支持资源级权限。

第二条语句授予用户权限以创建 VPC 对等连接，并访问特定账户中的所有 VPC 以便执行此操作。

第三条语句使用 * 通配符作为 Action 元素的一部分，以便为所有 VPC 对等连接操作授予权限。条件密钥确保只能对与属于账户的 VPC 建立的 VPC 对等连接执行操作。例如，如果接受者或请求者 VPC 属于不同账户，则用户无法删除 VPC 对等连接。用户无法与属于不同账户的 VPC 建立 VPC 对等连接。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcPeeringConnections",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection"
            ],
            "Resource": "arn:aws:ec2:*:111122223333:vpc/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:*VpcPeeringConnection",
            "Resource": "arn:aws:ec2:*:111122223333:vpc-peering-connection/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:AccepterVpc": "arn:aws:ec2:*:111122223333:vpc/*",
                    "ec2:RequesterVpc": "arn:aws:ec2:*:111122223333:vpc/*"
                }
```

```
            }
        }
    ]
}
```

示例：使用控制台管理 VPC 对等连接

要在 Amazon VPC 控制台中查看 VPC 对等连接，用户必须拥有使用 `ec2:DescribeVpcPeeringConnections` 操作的权限。要使用创建对等连接页面，用户必须拥有使用 `ec2:DescribeVpcs` 操作的权限。这可授予其权限以查看和选择 VPC。您可以将资源级权限应用于所有 `ec2:*PeeringConnection` 权限 (`ec2:DescribeVpcPeeringConnections` 除外)。

以下策略授予用户权限以查看 VPC 对等连接，并使用 Create VPC Peering Connection（创建 VPC 对等连接）对话框创建仅使用特定请求者 VPC 的 VPC 对等连接。如果用户尝试创建使用不同请求者 VPC 的 VPC 对等连接，则请求会失败。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-1234567890abcdef0",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

账户的 VPC 对等连接配额

VPC 对等连接支持连接两个 VPC。如此一来，一个 VPC 中的资源就能与另一个 VPC 中的资源进行通信，就像位于同一个网络中一样。无论 VPC 位于同一 AWS 区域还是不同区域，VPC 对等连接都是用于连接 VPC 的一项实用功能。本节旨在介绍在使用 VPC 对等连接时应注意的配额。

下表列出了您 AWS 账户的 VPC 对等连接的配额（之前称为限制）。除非另有说明，否则您可以请求增加这些配额。

如果发现当前的 VPC 对等连接要求超过默认配额，建议提交请求来提高服务的限额。我们会审核您的使用情况，同您一起对配额进行相应调整，从而确保 VPC 环境能够满足不断增长的业务需求。

名称	默认值	可调整
每个 VPC 的活动 VPC 对等连接	50	是 （最多 125）
未完成的 VPC 对等连接请求	25	是
未接受的 VPC 对等连接请求的过期时间	1 周（168 小时）	否

有关使用 VPC 对等连接的规则的更多信息，请参阅 VPC 对等限制。有关 Amazon VPC 配额的更多信息，请参阅《Amazon VPC 用户指南》https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html中的 Amazon VPC 配额。

《Amazon VPC 对等连接指南》的文档历史记录

下表介绍《Amazon VPC 对等连接指南》的文档版本。

变更	说明	日期
在创建时添加标签	您可以在创建 VPC 对等连接和路由表时添加标签。	2020 年 7 月 20 日
区域间对等	亚太地区（香港）区域中的区域间 VPC 对等连接支持 DNS 主机名解析。	2019 年 8 月 26 日
区域间对等	您可以在位于不同 AWS 区域中的 VPC 之间创建 VPC 对等连接。	2017 年 11 月 29 日
用于 VPC 对等的 DNS 解析支持	您可以使本地 VPC 在通过对等 VPC 中的实例查询时将公有 DNS 主机名解析为私有 IP 地址。	2016 年 7 月 28 日
过时的安全组规则	您可以了解自己的安全组是否被对等 VPC 中的安全组规则引用，找出过时的安全组规则。	2016 年 5 月 12 日
在 VPC 对等连接上使用 ClassicLink	您可以修改 VPC 对等连接，使本地链接的 EC2-Classic 实例能够与对等 VPC 中的实例进行通信，反之亦然。	2016 年 4 月 26 日
VPC 对等连接	您可以在两个 VPC 之间创建 VPC 对等连接，这样，任一 VPC 中的实例都可以使用私有 IP 地址相互通信。	2014 年 3 月 24 日