欢迎学习模块 7：连接网络。

本模块包含以下章节：

1. 架构需求
2. 使用 AWS Site-to-Site VPN 连接到远程网络
3. 使用 AWS Direct Connect 连接到远程网络
4. 使用 VPC 对等连接在 AWS 中连接 VPC
5. 使用 AWS Transit Gateway 扩展 VPC 网络
6. 将 VPC 连接到受支持的 AWS 服务

本模块还包括：

- 一项活动，您将在此活动中讨论如何使用 AWS Transit Gateway 连接三个 Virtual Private Cloud (VPC)
- 一个指导实验，您将在此实验中创建 VPC 对等连接

最后，您需要完成一个知识测验，以测试您对本模块中涵盖的关键概念的理解程度。

模块目标

学完本模块后，您应该能够：

- 描述如何将本地网络连接到 Amazon Web Services (AWS) 云
- 描述如何在 AWS 云中连接 VPC
- 使用 VPC 对等连接在 AWS 云中连接 VPC
- 描述如何在 AWS 云中扩展 VPC
- 描述如何将 VPC 连接到受支持的 AWS 服务

学完本模块后，您应该能够：

- 描述如何将本地网络连接到 Amazon Web Services (AWS) 云
- 描述如何在 AWS 云中连接 VPC
- 使用 VPC 对等连接在 AWS 云中连接 VPC
- 描述如何在 AWS 云中扩展 VPC
- 描述如何将 VPC 连接到受支持的 AWS 服务

模块 7：连接网络

第 1 节：架构需求

介绍第 1 节：架构需求。

咖啡馆业务要求

咖啡馆的工作负载越来越复杂。该架构必须支持多个 VPC 之间的连接，
并且具有高可用性和容错能力。

咖啡馆启动了忠诚度奖励计划，客户在购买 10 件或更多类似商品后可获得免费饮料或甜点。客户在线订购时，他们必须提供一些个人身份信息 (PII)，例如电子邮件地址和信用卡号码。出于合规性原因，咖啡馆不能将这些信息存储在云中。因此，Sofía 和 Nikhil 需要使用一种方法将其本地数据库（存储敏感客户信息）连接到其云系统（存储交易数据）。然后，他们必须对两个系统之间的数据进行映射，以提供客户获得的奖励。

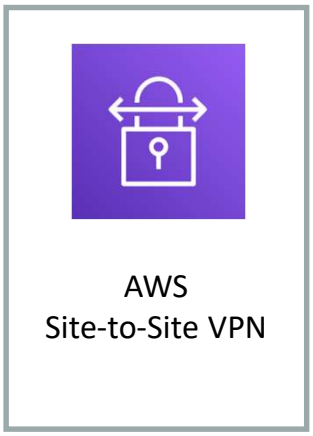
此外，出于安全考虑，Sofía 告诉 Olivia，她希望将开发环境隔离在一个 VPC 中，将生产环境隔离在另一个 VPC 中，但两者之间仍然互相连接。Olivia 认为这是个好主意，并建议 Sofía 在设计网络环境时使其具有高可用性和容错能力。

模块 7：连接网络

第 2 节：使用 AWS Site-to-Site VPN 连接到远程网络

介绍第 2 节：使用 AWS Site-to-Site VPN 连接到远程网络。

AWS Site-to-Site VPN



AWS Site-to-Site 是一种高度可用的解决方案，可让您安全地将本地网络或分支机构站点连接到 VPC。

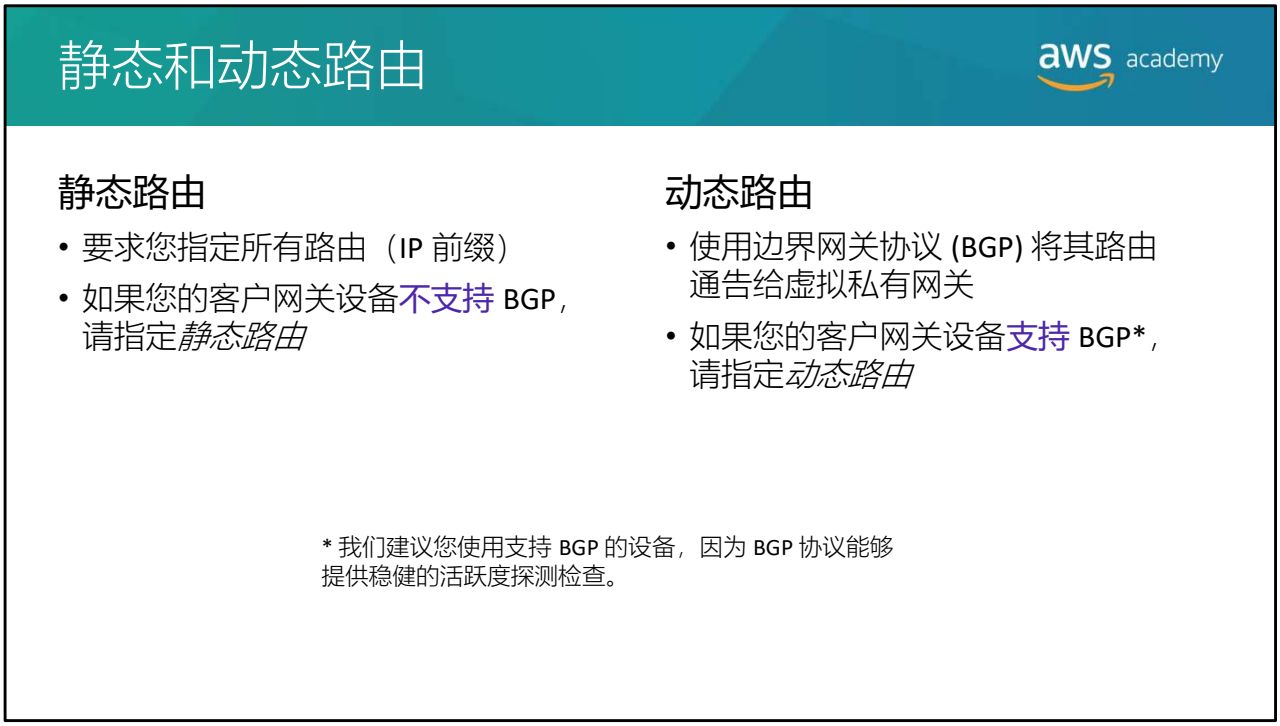
- 使用互联网协议安全 (IPSec) 通信创建加密的虚拟私有网络 (VPN) 隧道
- 为每个 VPN 连接提供两个加密隧道
- 按 VPN 连接小时收费

默认情况下，您在 AWS 上的 Virtual Private Cloud (VPC) 中启动的实例无法与本地网络通信。

您可以使用 AWS Site-to-Site Virtual Private Network (AWS Site-to-Site VPN) 将本地网络或分支机构站点安全地连接到 VPC。每个 AWS Site-to-Site VPN 连接都使用互联网协议安全 (IPSec) 通信在两个位置之间创建加密的 VPN 隧道。*VPN 隧道*是用于在客户网络和 AWS 之间传输数据的加密链接。连接的 AWS 端是*虚拟私有网关*。（请注意，您还可以在中转网关上创建 Site-to-Site VPN 连接，而不使用虚拟私有网关。稍候您将在本模块中了解有关 AWS Transit Gateway 的更多信息。）连接的本地端是*客户网关*。

AWS Site-to-Site VPN 提供两个跨多个可用区的 VPN 隧道，您可以同时使用这两条 VPN 隧道来实现高可用性。您可以通过第一个隧道流式传输主要流量，使用第二个隧道进行冗余。如果一条隧道发生故障，流量仍会传输到 VPC。

如果创建与 VPC 相连的 Site-to-Site VPN 连接，您需要为 VPN 连接已预置且可用的 VPN 连接小时付费。有关定价的更多信息，请参阅 AWS Site-to-Site VPN 和 Accelerated Site-to-Site VPN 连接定价。



在创建 Site-to-Site VPN 连接时，必须指定计划使用的路由类型，而且必须更新子网的路由表。

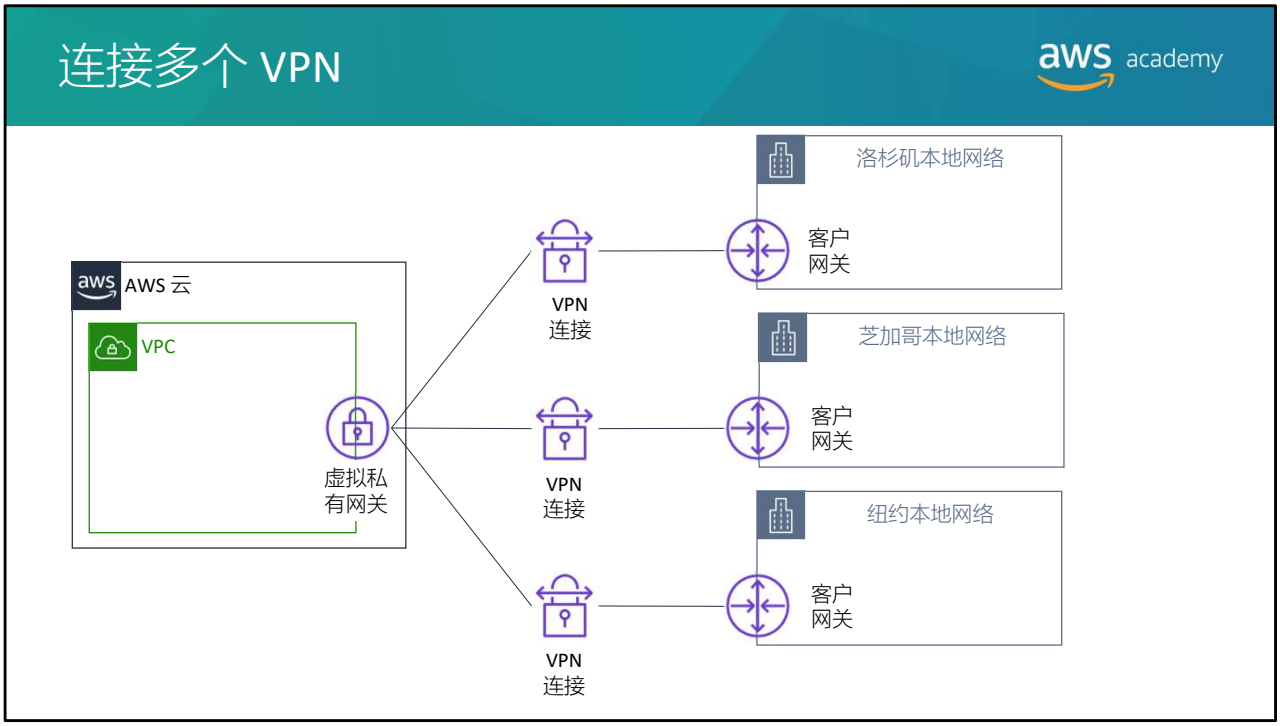
AWS Site-to-Site VPN 支持两种类型的路由。您选择的路由类型取决于您的 VPN 设备的品牌和型号：

- 如果您的 VPN 设备支持边界网关协议 (BGP)，您可以在配置 Site-to-Site VPN 连接时指定*动态路由*方式。*动态路由*使用 BGP 向虚拟私有网关通告路由。动态路由每个路由表最多支持 100 个传播路由。（有关当前限制，请参阅 AWS Site-to-Site VPN 限制。）
- 如果您的 VPN 设备不支持 BGP，请指定*静态路由*。*静态路由*要求您为网络指定应与虚拟私有网关通信的路由（即 IP 前缀）。默认情况下，静态路由支持每个路由表 50 个非传播路由，最多可支持 1000 个非传播路由。（有关当前限制，请参阅 AWS Site-to-Site VPN 限制。）

我们建议您使用支持 BGP 的设备，因为 BGP 协议可提供稳健的活性探测检查，可以在第一条隧道出现故障时协助故障转移到第二条 VPN 隧道。不支持 BGP 的设备也可执行运行状况检查，以便在需要时协助故障转移到第二条隧道。

有关已使用 Amazon VPC 测试的静态和动态路由设备的列表，请参阅 *AWS Site-to-Site VPN 网络管理员指南*中的我们已测试的客户网关设备。

有关 Site-to-Site VPN 路由选项的详细信息，请参阅静态路由和动态路由选项。



为了保持客户网关的高可用性，您可以设置冗余客户网关设备。如果您有冗余客户网关设备，则每个设备都会通告相同的前缀（例如 *0.0.0.0/0*）给虚拟私有网关。AWS 使用 BGP 路由确定流量的路径。如果一个客户网关设备发生故障，则虚拟私有网关会将所有流量定向到正常工作的客户网关设备。

您可以使用 AWS VPN CloudHub 建立从多个客户网关设备到单个虚拟私有网关的多个 VPN 连接。此配置可在不同的方式中用于在 VPN 连接侧实现冗余和故障转移。

AWS VPN CloudHub 以轮辐模式运行，使多个站点能够访问您的 VPC 或安全地相互访问。您可以在包含或不包含 VPC 的情况下使用它。您配置各个客户网关设备以通告具体站点相关的前缀（例如 *10.0.0.0/24*、*10.0.1.0/24*）给虚拟私有网关。虚拟私有网关将所有流量导向适当的站点，并将该站点的可到达性通告给所有其他站点。

有关使用 AWS Site-to-Site VPN 的更多信息，请参阅以下资源：

- Site-to-Site VPN 单一连接和多个连接示例
- 使用冗余 Site-to-Site VPN 连接以提供故障转移

第 2 节要点

- AWS Site-to-Site VPN 是一种高度可用的解决方案，可让您安全地将本地网络或分支机构站点连接到 VPC
- AWS Site-to-Site VPN 支持静态和动态路由
- 您可以建立从多个客户网关设备到单个虚拟私有网关的多个 VPN 连接

本模块中这节内容的要点包括：

- AWS Site-to-Site VPN 是一种高度可用的解决方案，可让您安全地将本地网络或分支机构站点连接到 VPC
- AWS Site-to-Site VPN 支持静态和动态路由
- 您可以建立从多个客户网关设备到单个虚拟私有网关的多个 VPN 连接

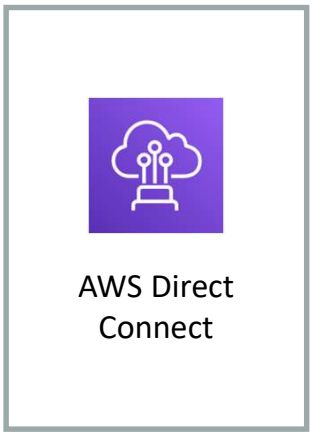
模块 7：连接网络

第 3 节：使用 AWS Direct Connect 连接到远程网络

aws academy

介绍第 3 节：使用 AWS Direct Connect 连接到远程网络。

AWS Direct Connect (DX)



AWS Direct Connect（也称为DX）可为您提供容量为 1Gbps 或10Gbps 的专用私有网络

降低数据传输成本

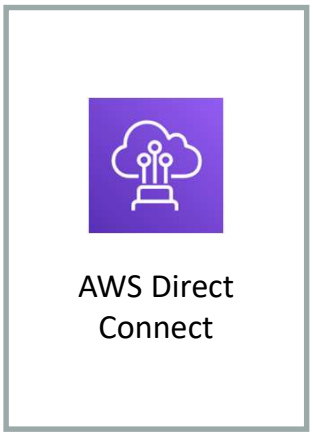
通过可预测的指标提高应用程序性能

如您所知，AWS Site-to-Site VPN 是用于将本地网络连接到 AWS 全球网络的一个选项。使用这个选项，您的数据将经由公共互联网通过加密的隧道传输。

AWS Direct Connect（即 DX）是另一种超越简单互联网连接的解决方案。DX 使用开放标准 802.1q 虚拟局域网 (VLAN)，因此您可以建立从本地到 AWS 的专用私有网络连接。这种私有连接可以降低网络成本，增加带宽吞吐量，同时提供优于互联网连接的稳定网络体验。

可提供 1Gbps 和 10Gbps 容量的专用连接。

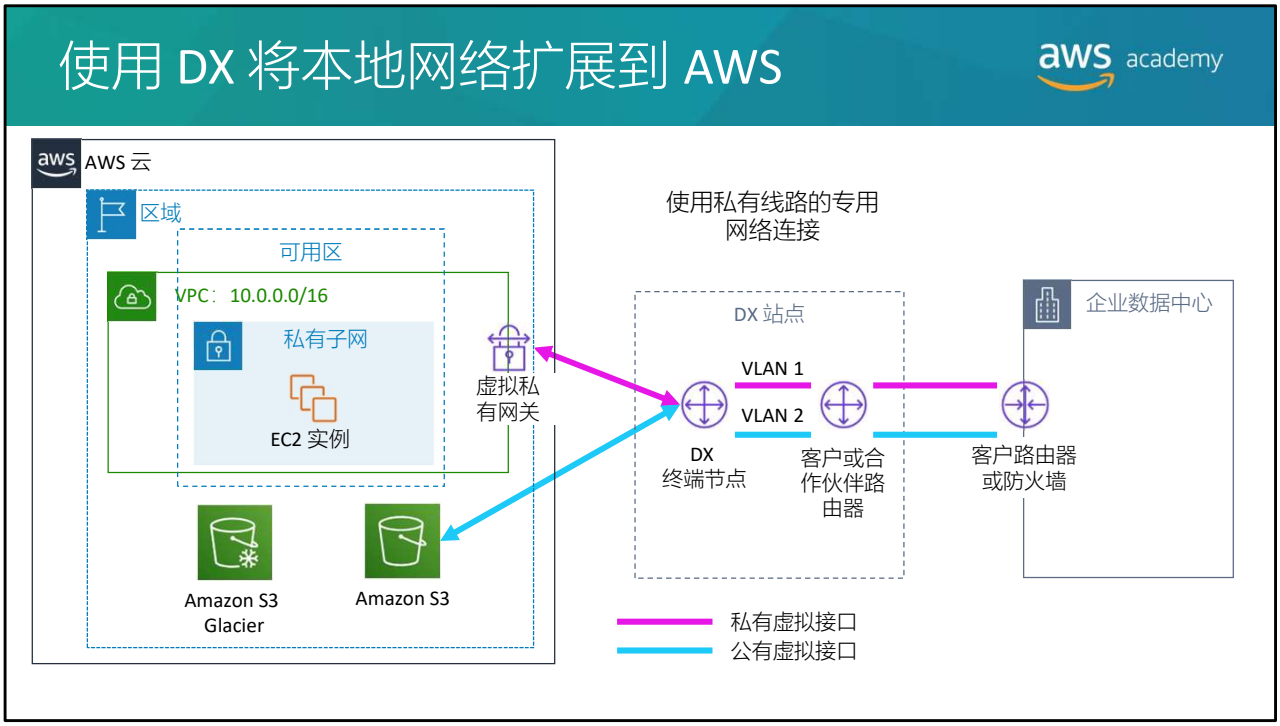
DX 使用案例



- 混合环境
- 传输大型数据集
- 可预测的网络性能
- 安全性与合规性

DX 在几种场景中非常有用，例如：

- *混合环境* – 对于需要访问现有数据中心设备（例如本地数据库）的应用程序，DX 使您能够创建一个混合环境，从而使您能够利用 AWS 的弹性和经济效益。
- *传输大型数据集* – 对于在大型数据集上运行的应用程序（例如高性能计算 (HPC) 应用程序），通过互联网在数据中心和 AWS 云之间传输大型数据集既耗时又昂贵。对于此类应用程序，使用 DX 连接到 AWS 云是个很好的解决方案，其原因在于：
  - 网络传输不会争用数据中心的互联网带宽。
  - 高带宽链路可降低网络拥塞和应用程序性能下降的可能性。
  - 通过限制应用程序使用的互联网带宽，您可以减少支付给 Internet 服务提供商 (ISP) 的网络费用，同时避免为增加的互联网带宽承诺或新合同付费。此外，通过 DX 传输的所有数据会按照降低后的 DX 数据传输费率（而非互联网数据传输费率）收费，这可以降低您的网络成本。
- *提升应用程序性能* – DX 对需要可预测的网络性能的应用程序也很有用。其中包括处理实时数据源（如音频流或视频流）的应用程序。在这种情况下，专用网络连接可以提供一致性比标准互联网连接更强的网络性能。
- *安全与合规性* – 有时候，企业安全或监管政策要求托管在 AWS 云上的应用程序只能通过私有网络线路进行访问。DX 自然而然成为针对此要求的一种解决方案，因为您的数据中心与应用程序之间的流量会流经专用的私有网络连接。

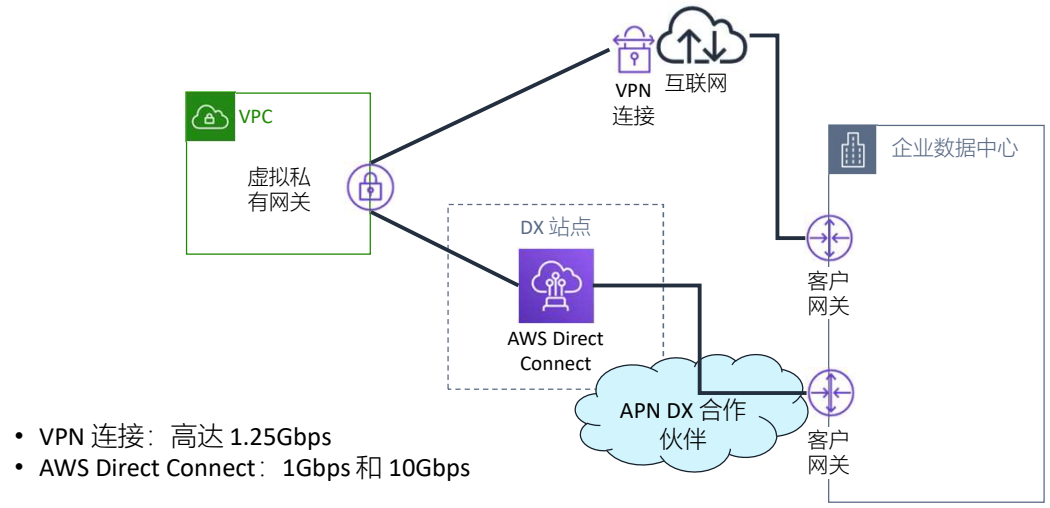


DX 通过标准的以太网光纤电缆将您的内部网络链接到 DX 站点。缆线的一端连接到您的路由器。另一端连接到 DX 路由器。通过此连接，您可以创建允许直接访问 AWS 服务的*虚拟接口*。公有虚拟接口允许访问公有 AWS 服务，例如 Amazon Simple Storage Service (Amazon S3)。私有虚拟接口允许对您的 VPC 进行访问。

您可以从任何受支持的 DX 位置访问任何区域（中国除外）的任何 VPC 或公有 AWS 服务。如果您的 DX 站点没有设备，则可以在 DX AWS 合作伙伴网络 (APN) 合作伙伴的协助下访问 DX。

有关 DX 的信息，请参阅什么是 AWS Direct Connect?

实现高可用性：具有备份 VPN 连接的 DX



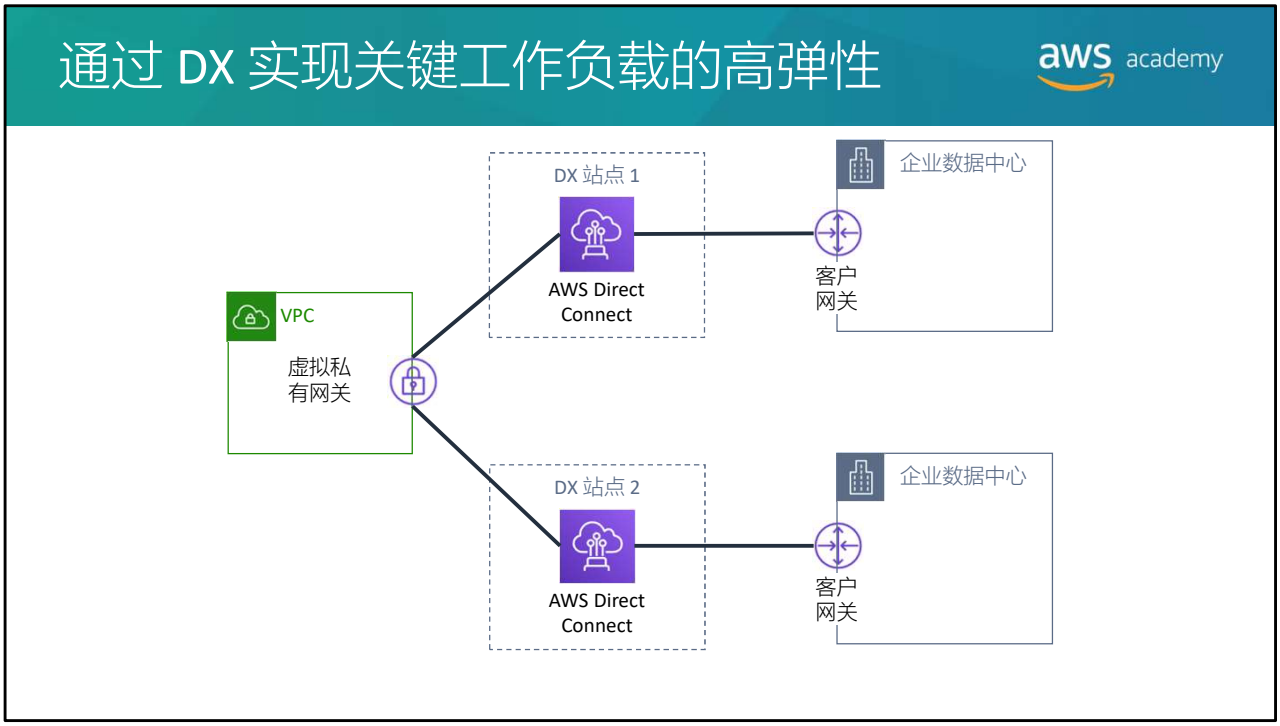
通过将用于主连接的一个或多个 DX 连接与成本较低的备份 VPN 连接相结合，您可以在数据中心和 VPC 之间实现高可用性连接。

在此示例中，配置包含两个动态路由连接，一个使用 DX，另一个使用两个来自不同客户设备的 VPN 连接。AWS 提供了示例路由器配置，帮助您建立 DX 连接和动态路由 VPN 连接。默认情况下，AWS 始终优先通过 DX 连接发送流量，因此不需要其他特定于 AWS 的配置来定义主连接和备份连接。但是，您应该配置 DX 和 VPN 特定的内部路由传播，以确保内部系统选择适当的路径。

这种方法让您可以为 AWS 流量选择主网络路径和网络提供商，还让您可以选择使用其他提供商来备份 VPN 连接。您应该选择符合组织风险承受能力、财务预期和数据中心连接策略的网络提供商和 DX 站点。

最后，您可以在分开部署的私有 IP 地址空间之间使用多个 DX 线路和多个 VPN 隧道。您还可以使用多个 DX 站点来实现高可用性。如果您使用多个 AWS 区域，您还需要在至少两个区域中使用多个 DX 站点。您可能需要考虑使用 AWS Marketplace 设备作为 VPN 的端点。

通过 DX 实现关键工作负载的高弹性



高弹性且具备容错能力的网络连接是构建架构完善的系统的关键。AWS 建议从多个数据中心进行连接以实现物理位置冗余。在设计远程连接时，可以考虑使用冗余硬件和电信提供商。

此外，最佳实践是使用动态路由、主动/主动连接在冗余网络连接之间实现自动负载均衡和故障转移。预置足够的网络容量，确保在一个网络连接发生故障时，不会使冗余连接遭到摧毁和性能降低。

对于需要高弹性的关键生产工作负载，AWS 建议您在多个位置建立一个连接。如架构图所示，这种拓扑可确保在因硬件故障或整个位置故障而导致连接故障时具有弹性。您可以使用 Direct Connect Gateway 从任何 DX 站点访问任何 AWS 区域（中国境内的 AWS 区域除外）。

要详细了解连接到 AWS 时需要牢记的其他拓扑指南，请参阅 AWS Direct Connect 弹性建议。

第 3 节要点

- AWS Direct Connect 使用开放标准 802.1q VLAN，使您能够建立从本地到 AWS 的专用私有网络连接
- 您可以从任何受支持的 DX 站点访问任何区域（中国除外）的任何 VPC 或公有 AWS 服务
- 通过将用于主连接的一个或多个 DX 连接与成本较低的备份 VPN 连接相结合，您可以在数据中心和 VPC 之间实现高度可用的连接
- 为了实现高弹性且具备容错能力的架构，请从多个数据中心连接到 AWS 网络，以便实现物理位置冗余

本模块中这节内容的要点包括：

- AWS Direct Connect 使用开放标准 802.1q VLAN 允许您建立从本地到 AWS 的专用私有网络连接
- 您可以从任何受支持的 DX 站点访问任何区域（中国除外）的任何 VPC 或公有 AWS 服务
- 通过将用于主连接的一个或多个 DX 连接与成本较低的备份 VPN 连接相结合，您可以在数据中心和 VPC 之间实现高度可用的连接
- 为了实现高弹性且具备容错能力的架构，请从多个数据中心连接到 AWS 网络，以便实现物理位置冗余

模块 7：连接网络

第 4 节：使用 VPC 对等连接在 AWS 中连接 VPC

aws academy

介绍第 4 节：使用 VPC 对等连接在 AWS 中连接 VPC。

连接 VPC

- 隔离一些工作负载通常是一种很好的做法。
- 但是，您可能需要在两个或更多 VPC 之间传输数据

将工作负载隔离在单独的 VPC 中通常是一种很好的做法。例如，当您的业务或架构规模过大时，您可能需要出于安全性、架构目的或简单性而将逻辑元素隔开。但是，当需要在 VPC 之间传输数据时，最好在 VPC 之间建立连接。

VPC 对等连接

- 两个 VPC 之间的一对一网络连接
- 无需网关、VPN 连接和单独的网络设备
- 高度可用的连接
- 没有单点故障或带宽瓶颈
- 流量始终保留在全球 AWS 骨干网上

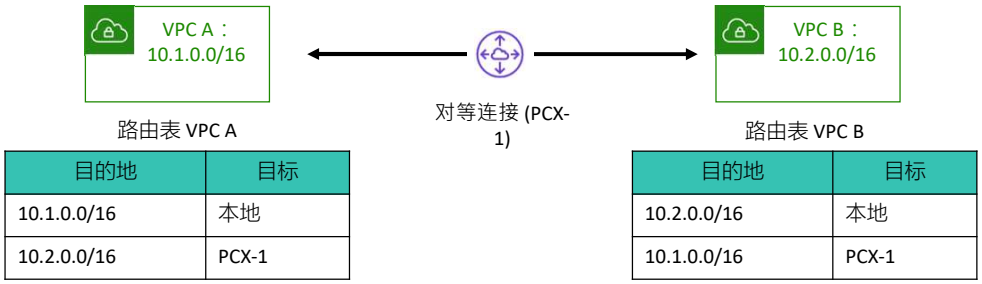
*VPC 对等连接*是两个 VPC 之间的一对一网络连接，让您可以私下在它们之间路由流量。这两个 VPC 中的实例可以彼此通信，就像它们位于同一网络中一样。您可以在您自己的 VPC 之间创建 VPC 对等连接：可以与其他 AWS 账户中的 VPC 建立连接，也可以与其他 AWS 区域中的 VPC 建立连接。

您可以在不同 AWS 区域的 VPC 之间建立对等连接关系。区域间 VPC 对等连接提供了一种简单经济的方式，可在区域间共享资源或为实现地理冗余性而复制数据。通过区域间 VPC 对等连接传输的数据将按标准的区域间数据传输费率收费。

区域间 VPC 对等连接使 VPC 资源能够使用私有 IP 地址相互通信，而无需网关、VPN 连接或独立的网络设备。VPC 资源的一些示例包括 Amazon Elastic Compute Cloud (Amazon EC2) 实例、Amazon Relational Database Service (Amazon RDS) 数据库以及在不同区域运行的 AWS Lambda 函数。

流量仍保留在私有 IP 地址空间中。所有区域间流量都经过加密，没有单点故障或带宽瓶颈。流量始终保留在全球 AWS 骨干网上。流量永远不会经过公共互联网，这样可以减少面临的威胁，例如常见漏洞和分布式拒绝服务 (DDoS) 攻击。

建立 VPC 对等连接



路由表 VPC A

目的地	目标
10.1.0.0/16	本地
10.2.0.0/16	PCX-1

路由表 VPC B

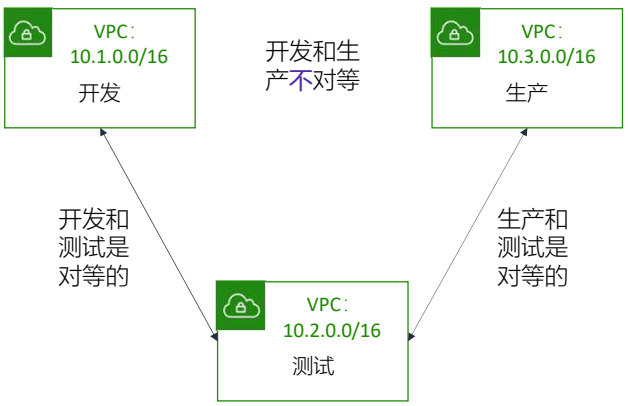
目的地	目标
10.2.0.0/16	本地
10.1.0.0/16	PCX-1

要建立 VPC 对等连接，请求者 VPC（或本地 VPC）的所有者应向对等 VPC 的所有者发送一个请求。要激活连接，对等 VPC 的所有者必须接受 VPC 对等连接请求。

要通过使用私有 IP 地址启用对等 VPC 之间的流量流，您必须向 VPC 的一个或多个路由表添加路由。此路由必须指向对等 VPC 的 IP 地址范围。然后，对等 VPC 的所有者会向其任一 VPC 路由表添加一条指向您的 VPC IP 地址范围的路由。

您可能还需要更新与您的实例关联的安全组规则，以便进出对等 VPC 的流量不受限制。

VPC 对等连接限制



- 使用私有 IP 地址
- 可以在不同的 AWS 账户之间建立
- 不能有重叠的 CIDR 块
- 任何两个 VPC 之间只能有一个对等资源
- 不支持传递对等关系

在建立 VPC 对等连接时，您应该注意一些限制：

- VPC 对等连接使用私有 IP 地址。
- 可以在不同的 AWS 账户之间建立 VPC 对等连接。对等 VPC 的 CIDR 块不能与请求者的 CIDR 块重叠。
- 您在任何两个 VPC 之间只能有一个对等资源。
- 不支持可传递对等互连。例如，在图示中，开发 VPC 和测试 VPC 之间已建立对等连接，生产 VPC 和测试 VPC 之间已建立对等连接。但是，这并不意味着生产 VPC 已连接到开发 VPC。默认情况下，VPC 对等连接不允许生产 VPC 连接到开发 VPC，除非它们*明确建立了对等连接*。因此，您可以控制哪些 VPC 可以相互通信。

要了解有关 VPC 对等连接限制的更多信息，请参阅 VPC 对等连接限制。

有关对等连接多个 VPC 的注意事项

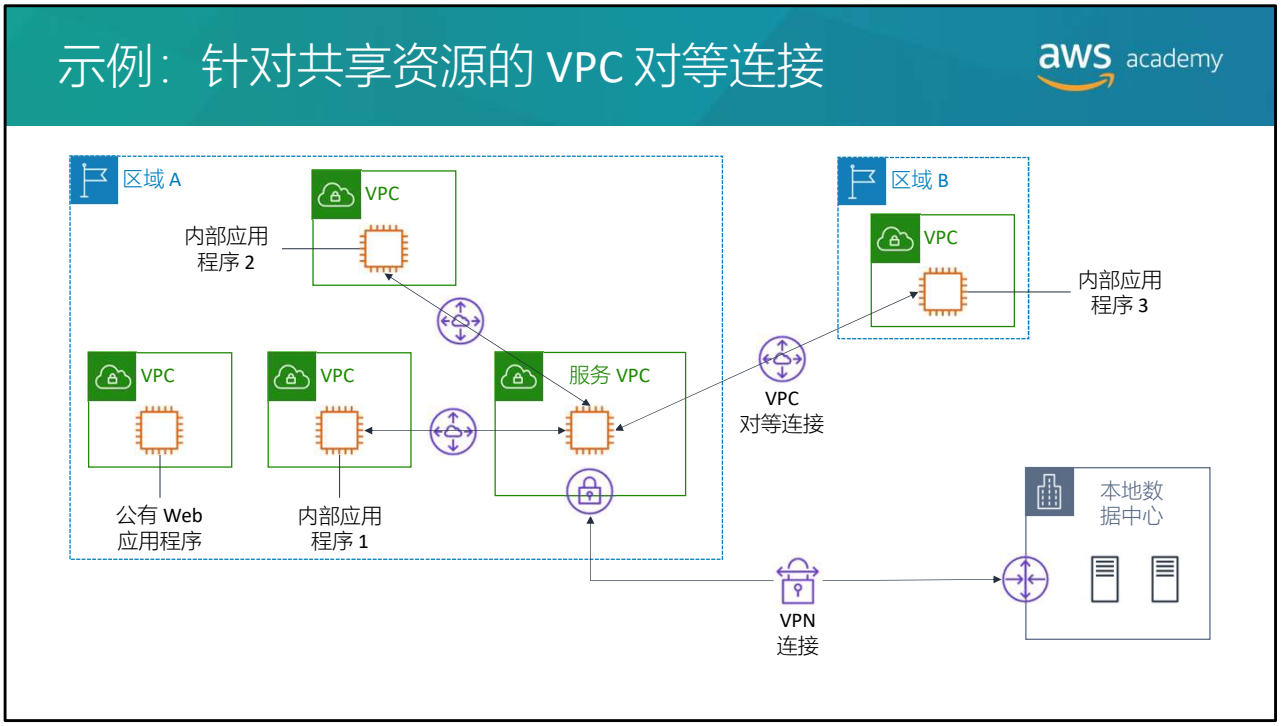
在连接多个 VPC 时，请考虑以下网络设计原则：

仅连接必要的 VPC

确保解决方案可以扩展

在单个 AWS 区域中连接多个 VPC 时，请考虑以下网络设计原则：

- 仅连接那些真正必须彼此通信的 VPC
- 确保您选择的解决方案可以根据您当前和未来的 VPC 连接需求进行扩展



本示例展示了如何将 VPC 对等连接用于共享资源。

在本示例中，公司中的每个部门 VPC 都与共享*服务 VPC* 建立了对等连接。此 VPC 包含与 Microsoft Active Directory 的连接、安全扫描工具、监控和日志记录工具以及其他各种功能。它还提供了一个代理，通过该代理，部门 VPC 可以访问一些本地资源。VPC 对等连接使处于不同 VPC 中的公司应用程序能够访问共享服务 VPC，但彼此间仍保持隔离。在本示例中，还请注意 VPC 对等连接是在不同区域的 VPC 之间建立的。

第 4 节要点

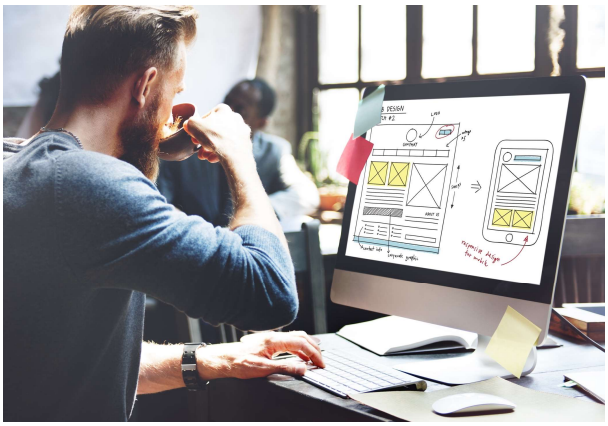
- VPC 对等连接是两个 VPC 之间的一对一网络连接，使您可以私下在它们之间路由流量
- 您可以在不同 AWS 区域的 VPC 之间建立对等关系
- VPC 对等连接 –
  - 使用私有 IP 地址
  - 可以在不同的 AWS 账户之间建立
  - 不能有重叠的 CIDR 块
  - 任何两个 VPC 之间只能有一个对等资源
  - 不支持传递对等关系

本模块中这节内容的要点包括：

- VPC 对等连接是两个 VPC 之间的一对一网络连接，使您可以私下在它们之间路由流量
- 您可以在不同 AWS 区域的 VPC 之间建立对等关系
- VPC 对等连接 –
  - 使用私有 IP 地址
  - 可以在不同的 AWS 账户之间建立
  - 不能有重叠的 CIDR 块
  - 任何两个 VPC 之间只能有一个对等资源
  - 不支持传递对等关系

模块 7 – 指导实验：创建 VPC 对等连接

aws academy



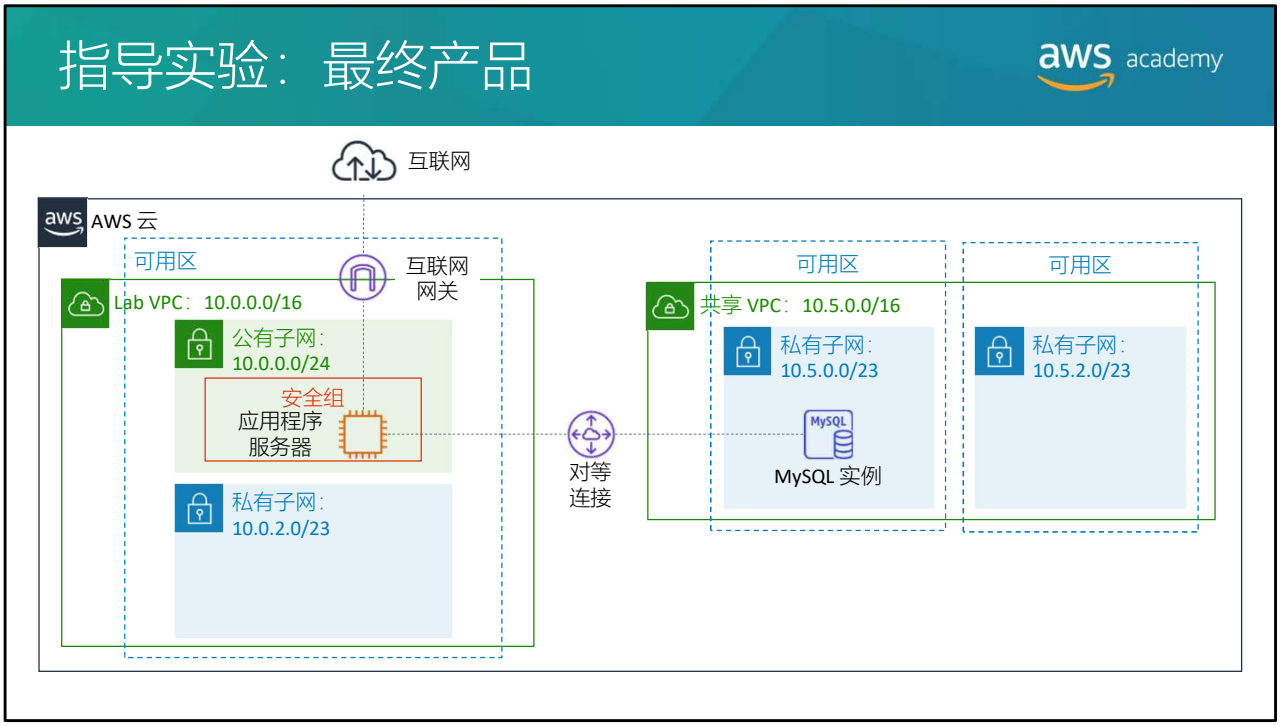
您现在将完成模块 7 – 指导实验：创建 VPC 对等连接。

指导实验：任务

1. 在两个 VPC 之间建立对等连接
2. 配置路由表以将流量发送到对等连接
3. 测试对等连接

在本指导实验中，您将完成以下任务：

1. 在两个 VPC 之间建立对等连接
2. 配置路由表以将流量发送到对等连接
3. 测试对等连接



该图总结了您完成实验后将会构建的内容。

大约 20 分钟

现在可以开始指导实验了。

指导实验总结：要点

完成这个指导实验之后，您的讲师可能会带您讨论此指导实验的要点。

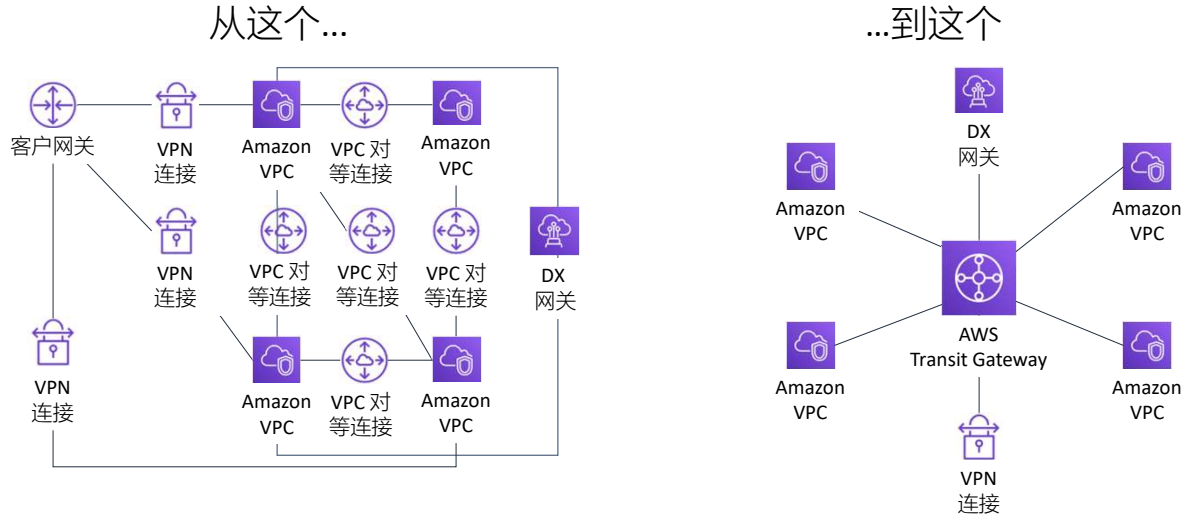
模块 7：连接网络

第 5 节：使用 AWS Transit Gateway 扩展 VPC 网络

aws academy

介绍第 5 节：使用 AWS Transit Gateway 扩展 VPC 网络。

需要跨多个 VPC 扩展网络



随着 AWS 上运行的工作负载数量增加，您必须能够跨多个账户和 VPC 扩展网络，才能跟上增长速度。您可以使用 VPC 对等连接来连接任意两个 VPC。但是，如果无法集中管理连接策略，那么就会造成运营成本高昂，且难于跨多个 VPC 管理点对点连接。对于本地连接，必须将 VPN 连接到每个单独的 VPC。当 VPC 数量增长到数百个时，此解决方案的构建可能非常耗时，而且难以管理。

思考以下几个问题非常重要：在经过一段时间后，您的环境会达到多大规模？环境的扩展能力如何？以及您如何管理 VPC？要解决此问题，您可以使用 AWS Transit Gateway 来简化联网模型。

AWS Transit Gateway

AWS Transit Gateway 是一项服务，使您可以将 VPC 和本地网络连接到单个网关。

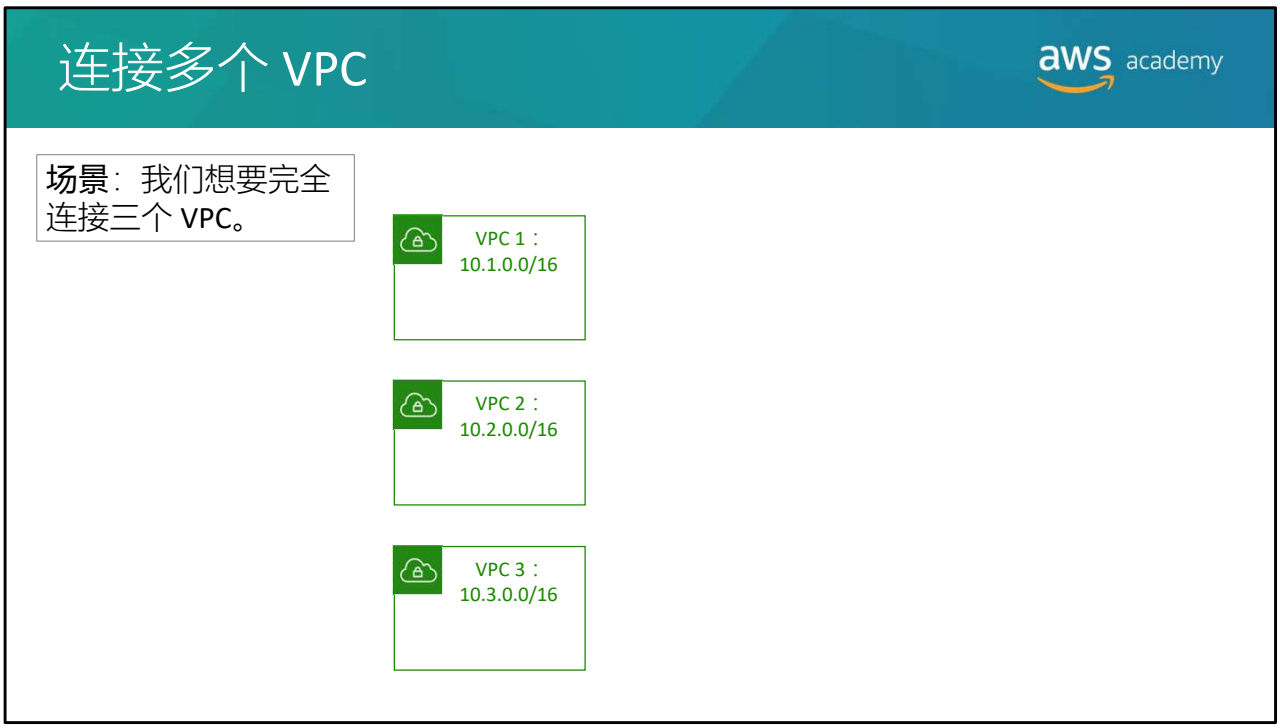
- 完全托管、高度可用且灵活的路由服务
- 充当所有流量流经您网络的枢纽
- 使用单个网关连接多达 5000 个 VPC 和本地环境

借助 AWS Transit Gateway 这项服务，您能够将 VPC 和本地网络连接到单个网关（称为中转网关）。借助 AWS Transit Gateway，只需创建和管理从中央网关到网络中每个 VPC、本地数据中心或远程办公室的一条连接。

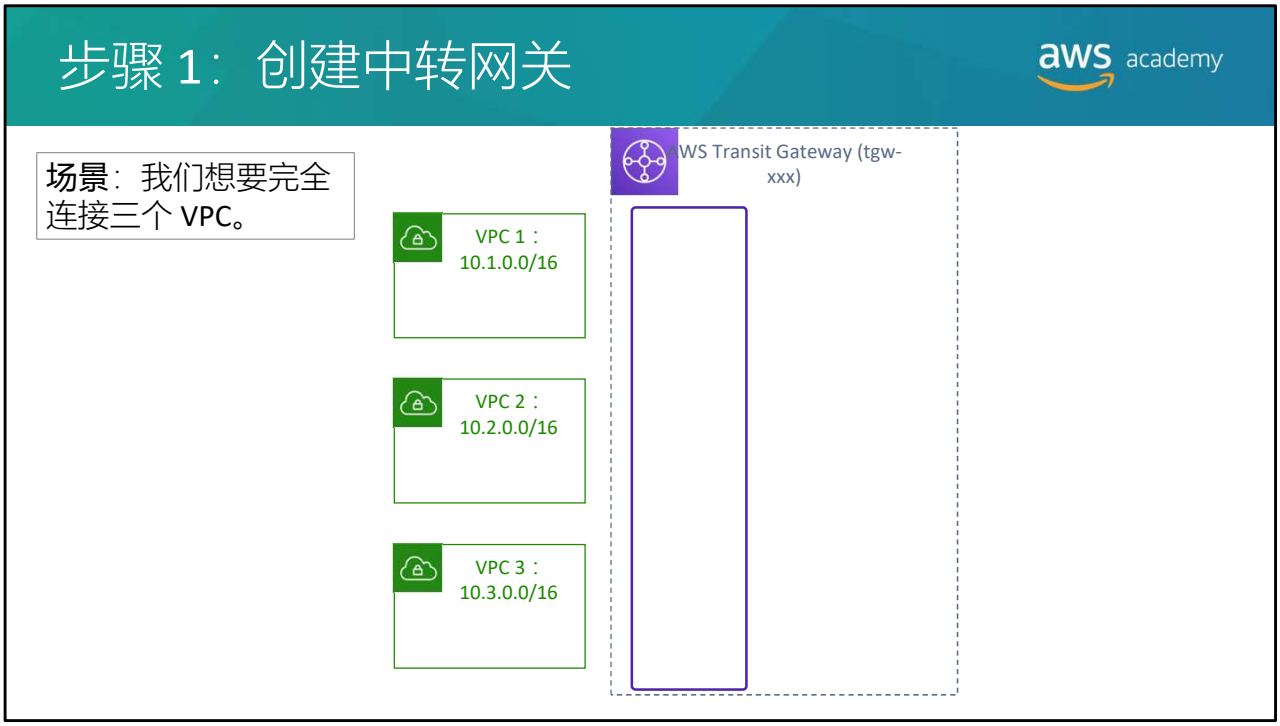
AWS Transit Gateway 使用轮辐模型。这种模型可以大大简化管理工作并降低运营成本，因为每个网络只需连接到中转网关，而不是连接到所有其他网络。将任何新的 VPC 连接到中转网关，然后它就会自动向连接到中转网关的所有其他网络开放。这种易连接性使您可以随着需求的增长更轻松地扩展网络。

您可以使用 AWS Transit Gateway 连接多达 5000 个 VPC 和本地网络。

连接多个 VPC



要了解如何使用 AWS Transit Gateway 连接多个 VPC，请考虑此场景。您想要完全连接网络中的三个 VPC。在此场景中，您将学习如何在单个区域中部署 AWS Transit Gateway 和三个具有非重叠 IP 地址空间的 VPC。然后，您将中转网关连接到这些 VPC。

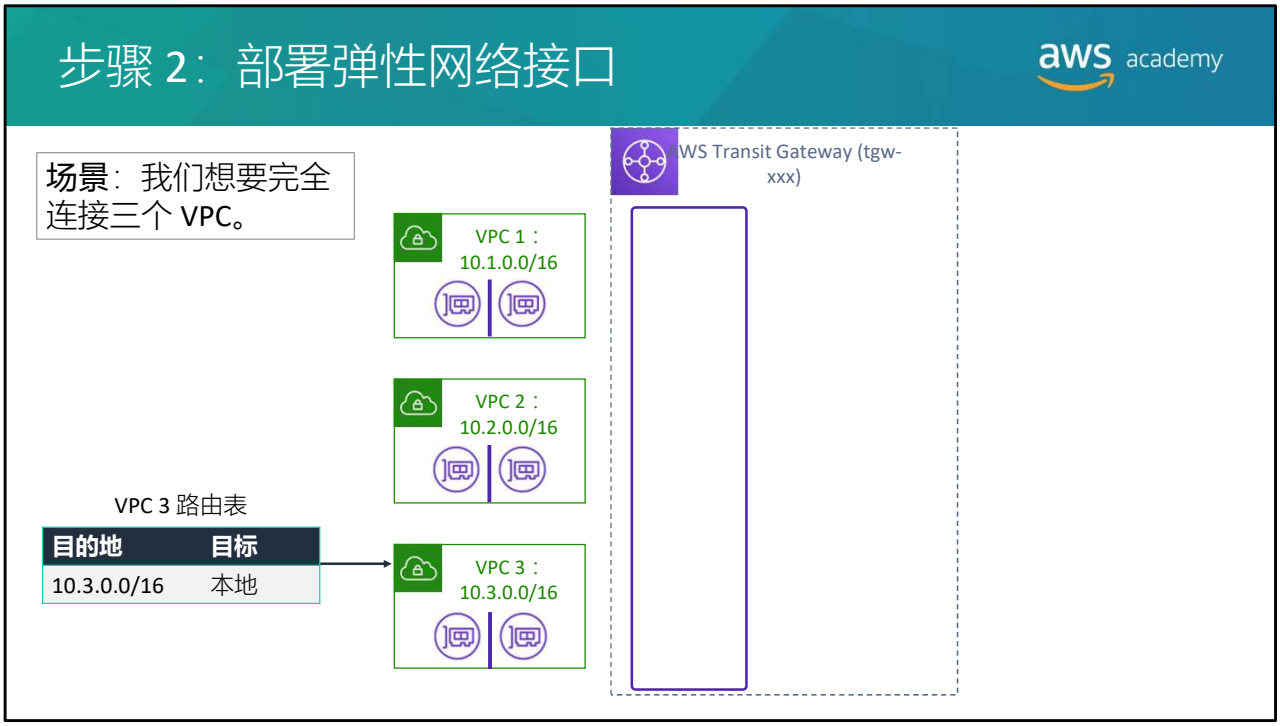


连接多个 VPC 的第一步是创建中转网关。*中转网关*是中转中心，您可用它来互连 VPC 和本地网络。它充当区域虚拟路由器，用于路由在您的 VPC 和 VPN 连接之间流动的流量。中转网关根据网络流量的规模灵活地进行扩展。

您可以通过 Amazon VPC 控制面板设置中转网关。使用 AWS Transit Gateway 需要支付各种费用，因此请确保您的架构和预算能够支持使用中转网关。

有关详细信息，请参阅什么是中转网关？

步骤 2：部署弹性网络接口

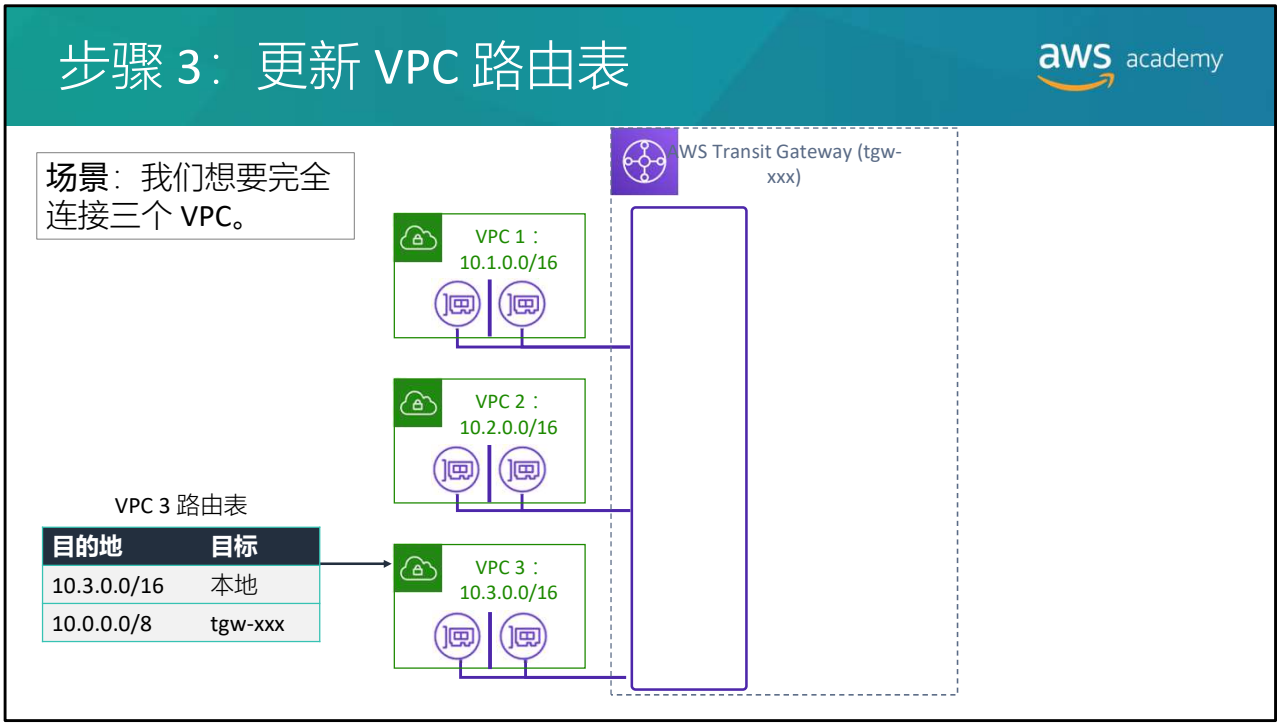


AWS Transit Gateway 通过弹性网络接口（即 ENI）连接到 VPC，这些接口部署到子网中。

您必须确保属于 VPC 的每个可用区都有一个将 VPC 连接到中转网关的 ENI。您可以通过从每个可用区中为 ENI 选择至少一个子网来实现此目的。

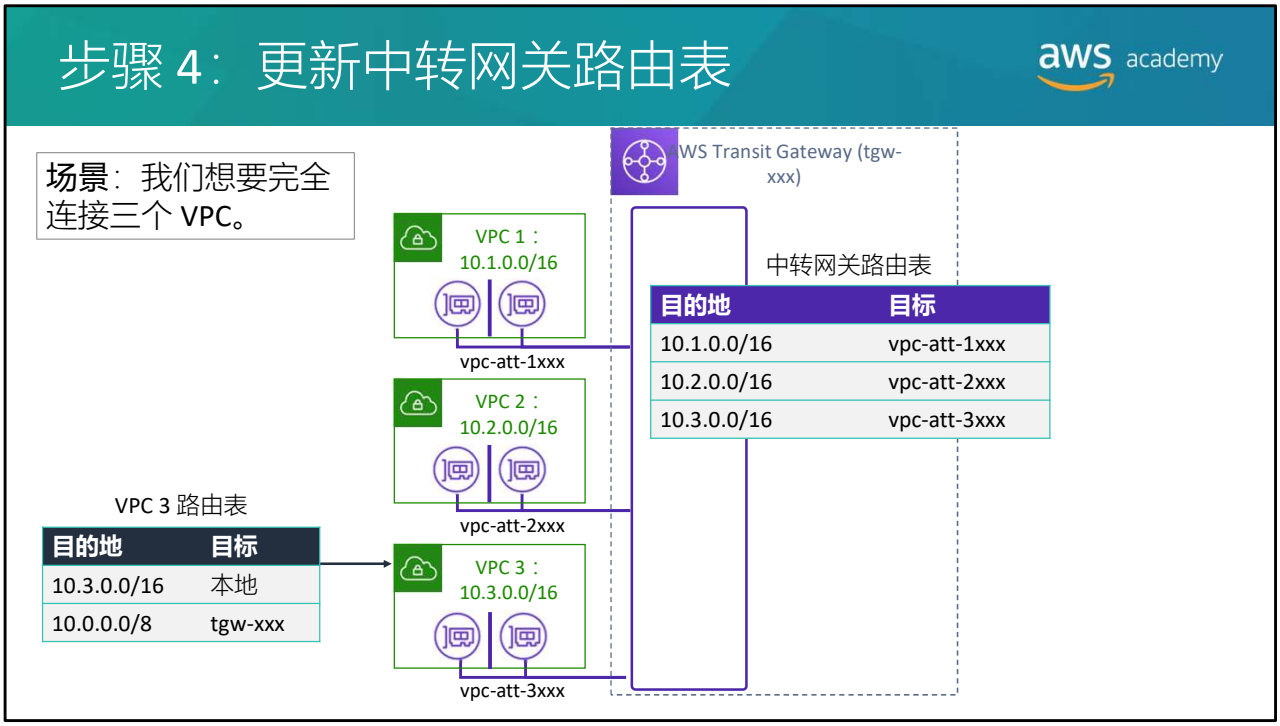
请注意，在此示例中，VPC 3 的路由表具有使用 10.3.0.0/16 网络的 VPC 3 的本地目的地路由。

步骤 3：更新 VPC 路由表



在连接 ENI 后，下一步是在 VPC 路由表中添加一个路由，以将发往网络中其他 VPC 的流量发送到中转网关。

在此示例中，VPC 3 路由表的第二行显示，发往 10.0.0.0/8 网络的流量被发送到中转网关。此路由使从 VPC 3 到 VPC 1 或 VPC 2 的任何流量都可以发送到中转网关，因为 CIDR 块 10.0.0.0/8 包括 10.X.0.0/16 CIDR 块（由单独 VPC 使用）。



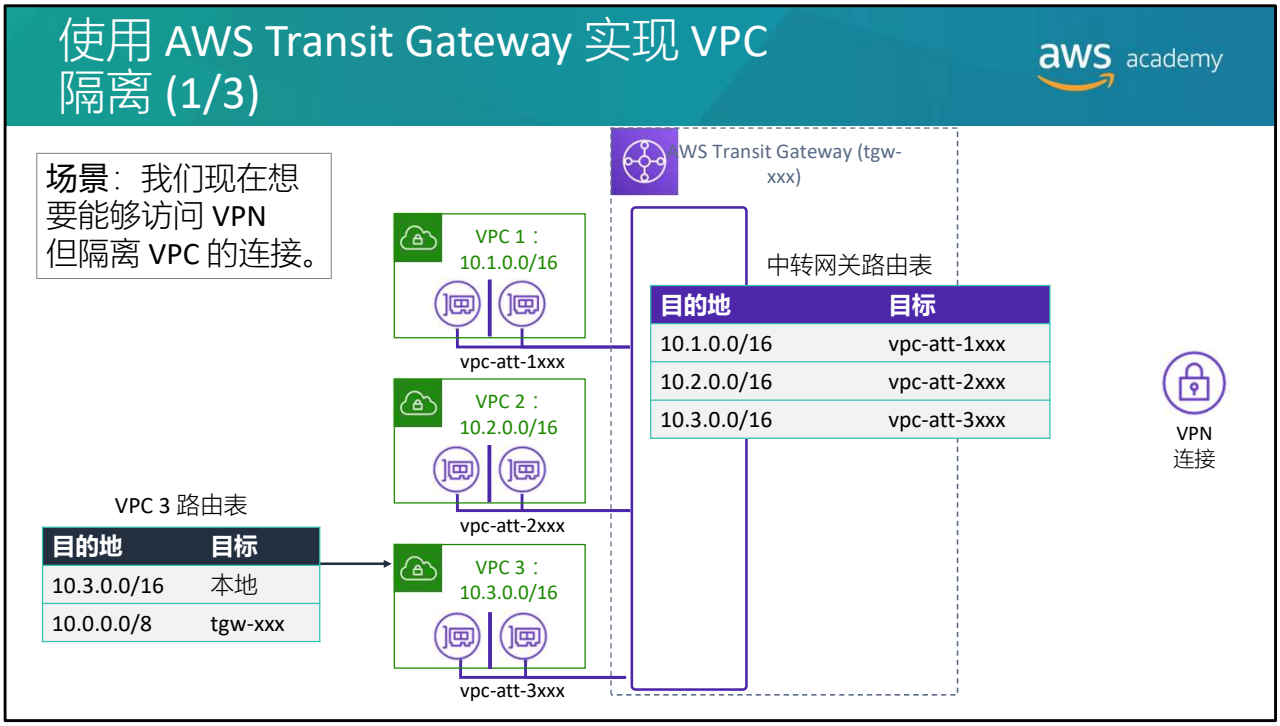
接下来，您必须配置中转网关路由表，以将流量路由到所连接的 VPC。

在创建中转网关时，将创建默认的中转网关路由表。中转网关路由表中的每条路由使中转网关能够将发往其中一个 VPC 的流量发送到相应的附件（这是对连接到 VPC 本身的 ENI 的引用）。

在此示例中，中转网关路由表中有一条路由，该路由将任何发往 10.1.0.0/16 网络的流量发送到 vpc-att-1xxx（VPC 1 的附件）。同样，任何发往其他 VPC 网络的流量都会发送到相应的附件。

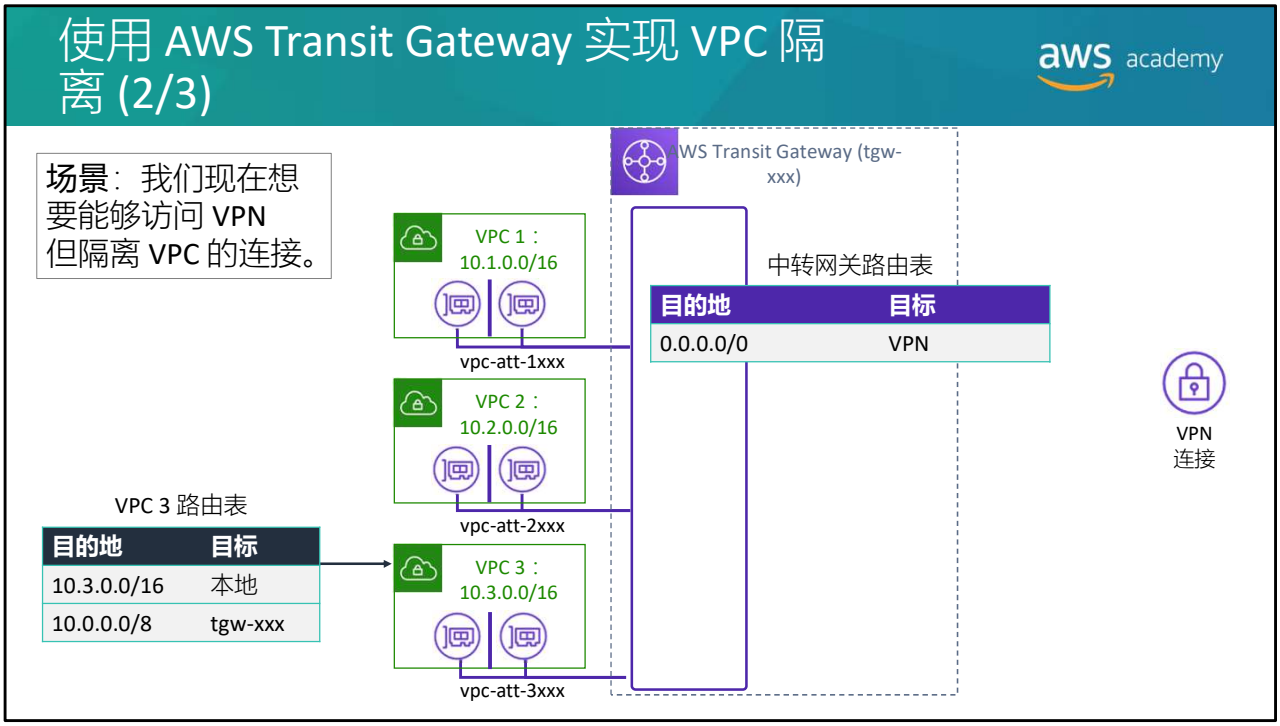
有关如何使用 AWS Transit Gateway 创建互连环境的更多信息，请参阅 Transit Gateways 入门。

使用 AWS Transit Gateway 实现 VPC 隔离 (1/3)



尽管可以使用 AWS Transit Gateway 连接多个 VPC，但也可以使用它在 VPC 环境中实现隔离。在这个场景中，您想要将 VPN 源连接到 VPC 环境。您还希望阻止 VPC 直接连接彼此，让 VPN 来决定是否必须将来自一个 VPC 的流量转发到另一个 VPC。

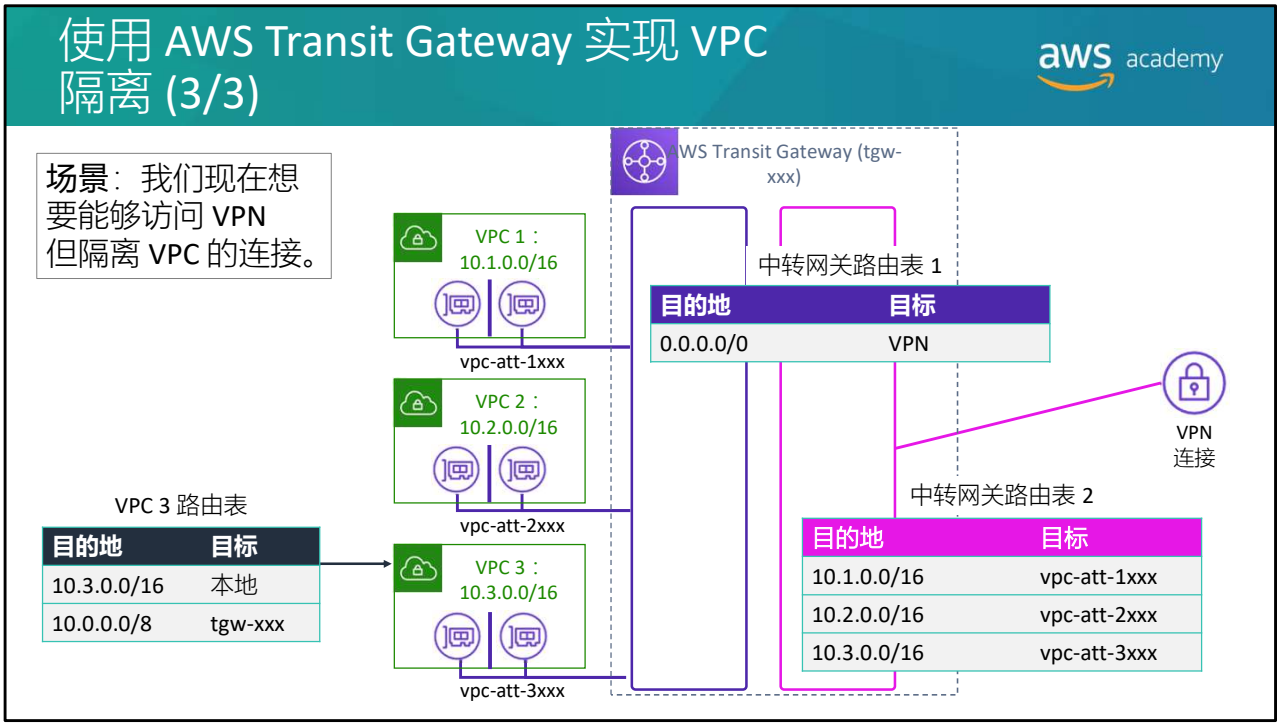
通过适当地为中转网关设置路由表，您可以阻止 VPC 之间的信息共享。



要实施此解决方案，请更新中转网关路由表中的路由，以将所有已知流量发送到 VPN 连接。

在此示例中，当 10.0.0.0/8 网络中任何 VPC 的流量从 VPC 3 发送到中转网关时，中转网关会将流量转发到 VPN（如幻灯片所示）。中转网关不会将流量发送到任何其他 VPC，因为没有指向任何 VPC 附件的路由。

现在，您具有了对 VPC 环境的隔离且安全的 VPN 访问，而 VPC 之间没有交叉通信。

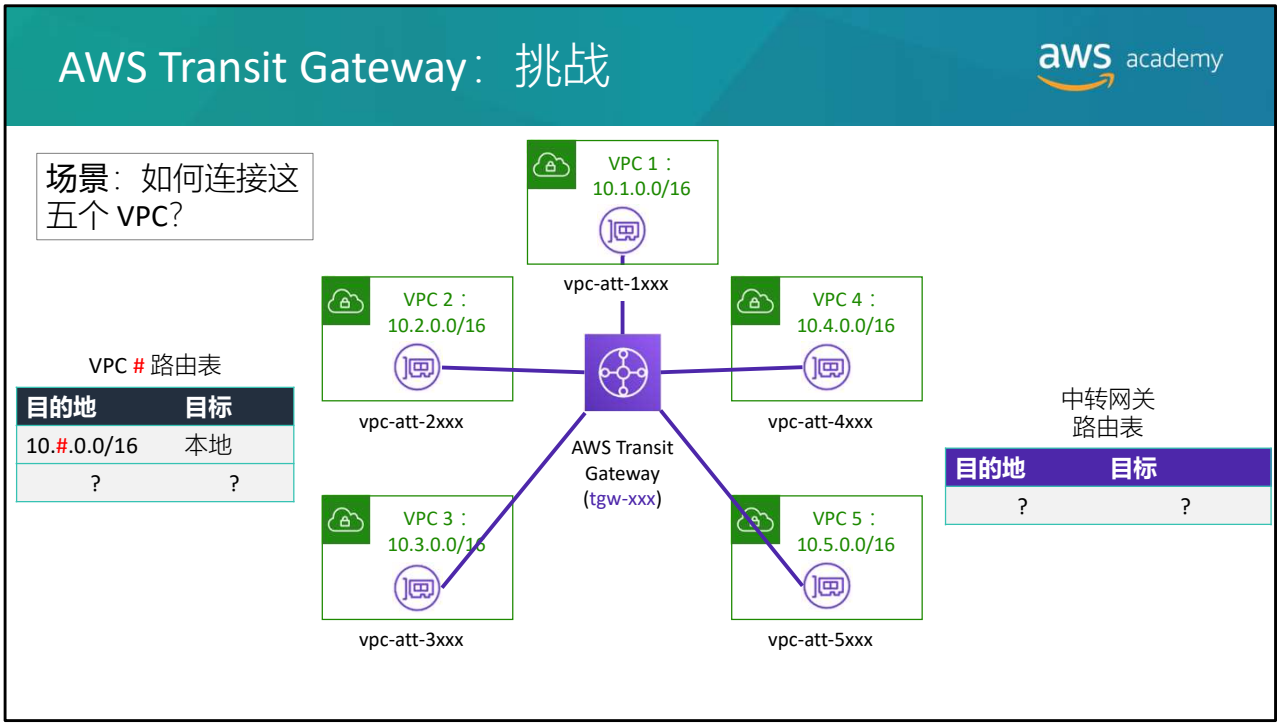


您可以根据需要创建多个针对特定交互的中转网关路由表来定向流量。

在此示例中，第二个路由表将来自 VPN 的入站流量定向到连接到中转网关的其中一个 VPC。

活动：AWS Transit Gateway

您现在将完成以下活动：AWS Transit Gateway。

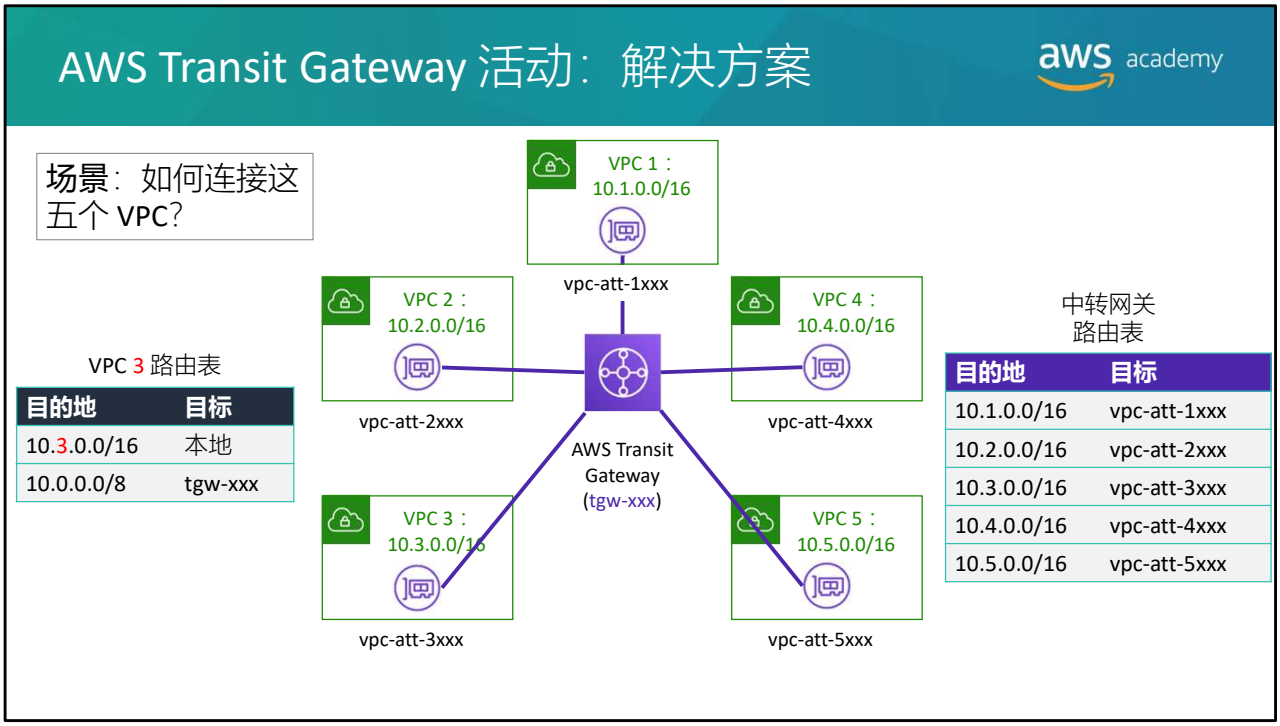


在本活动中，您有五个要通过 AWS Transit Gateway 相互连接的 VPC。

回答以下问题：

- 为了实现完全连接，需要向每个 VPC 路由表添加哪些路由?
- 为了实现完全连接，需要向中转网关路由表添加哪些路由?

AWS Transit Gateway 活动：解决方案



为了实现完全连接，必须在每个 VPC 路由表中添加哪些路由？

- 请参阅为 VPC 3 路由表提供的解决方案。您要以类似方式更新其他 VPC 路由表。

为了实现完全连接，必须向中转网关路由表添加哪些路由？

- 为每个 VPC 附件添加路由，以将流量定向到每个 VPC。

第 5 节要点

- 借助 AWS Transit Gateway，您能够将 VPC 和本地网络连接到单个网关（称为中转网关）
- AWS Transit Gateway 使用轮辐模型来简化 VPC 管理并降低运营成本

本模块中这节内容的要点包括：

- 借助 AWS Transit Gateway，您能够将 VPC 和本地网络连接到单个网关（称为中转网关）
- AWS Transit Gateway 使用轮辐模型来简化 VPC 管理并降低运营成本

模块 7：连接网络

第 6 节：将 VPC 连接到受支持的 AWS 服务

介绍第 6 节：将 VPC 连接到受支持的 AWS 服务。

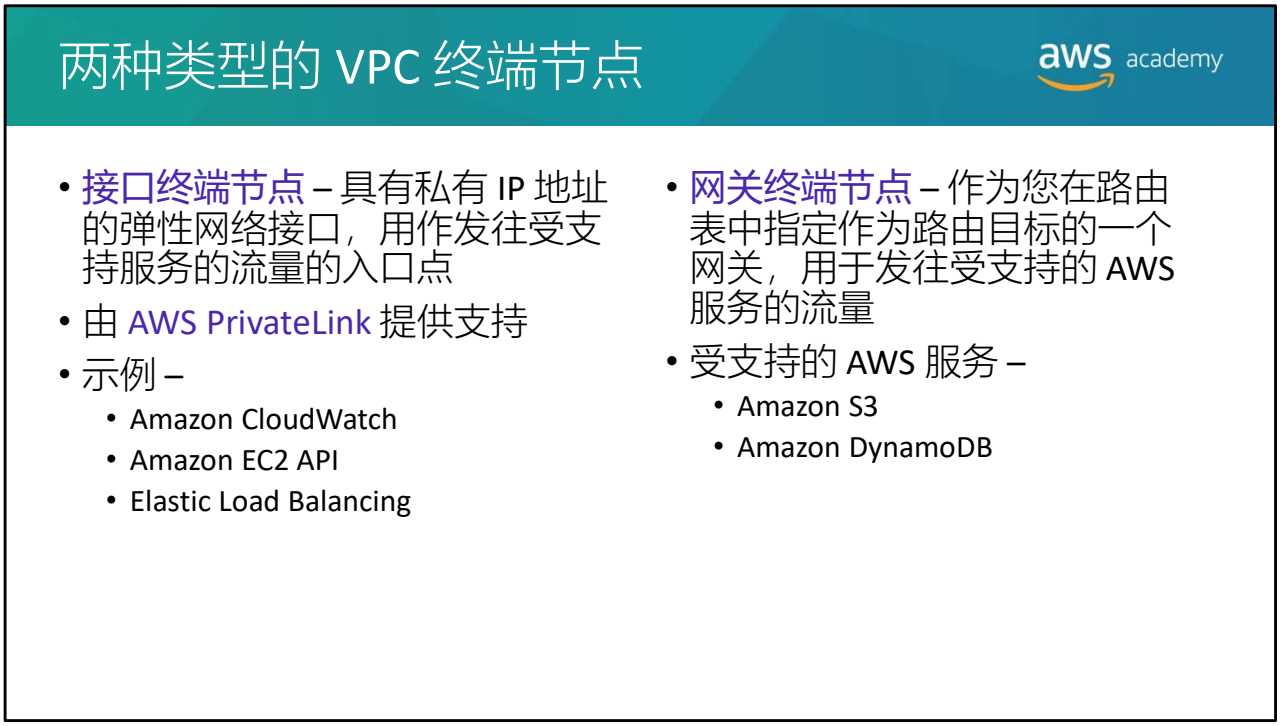
VPC 终端节点

- 让您能够将 VPC 以私密方式连接到受支持的 AWS 服务和由 AWS PrivateLink 提供支持的 VPC 终端节点服务
- 支持 VPC 和其他服务之间的流量而不脱离 Amazon 网络
- 无需互联网网关、VPN、网络地址转换 (NAT) 设备或防火墙代理
- 可水平扩展、冗余且高度可用

借助 *VPC 终端节点*，您能够将 VPC 以私密方式连接到受支持的 AWS 服务和由 AWS PrivateLink 提供支持的 VPC 终端节点服务。由 AWS PrivateLink 提供支持的 VPC 终端节点服务包括一些 AWS 服务、由其他 AWS 客户和 AWS 合作伙伴网络 (APN) 合作伙伴在其自己的 VPC 中托管的服务（称为*终端节点服务*）以及受支持的 AWS Marketplace APN 合作伙伴服务。

VPC 终端节点不需要互联网网关、NAT 设备、VPN 连接或 DX 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 和其他服务之间的流量不会脱离 Amazon 网络。

终端节点是虚拟设备。它们是水平扩展、冗余且高度可用的 VPC 组件。通过终端节点，VPC 中的实例与服务之间可以进行通信，而不会对网络通信带来可用性风险或带宽约束。



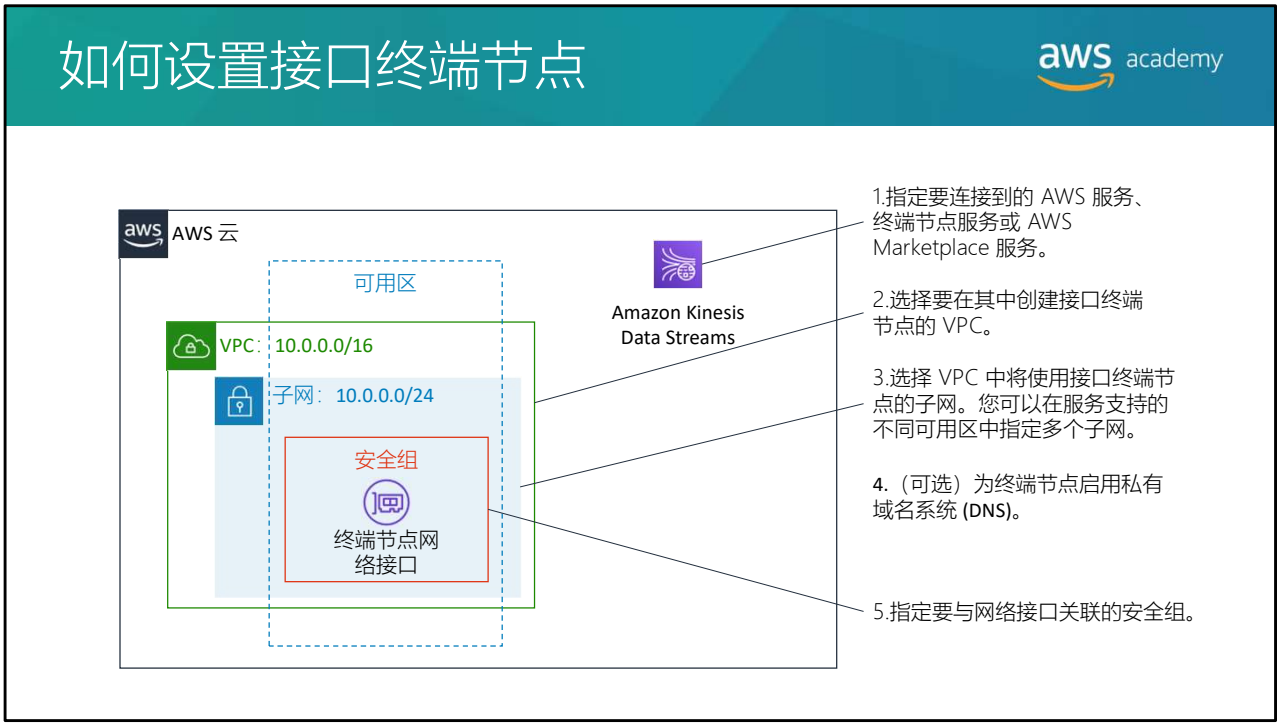
有两种类型的 VPC 终端节点：

- *接口终端节点*是具有私有 IP 地址的弹性网络接口。此 IP 地址作为发往受支持服务的流量的入口点。接口终端节点使您能够连接到由 AWS PrivateLink 提供支持的服务。服务的所有者是*服务提供商*。作为创建接口终端节点的委托人，您是*服务使用者*。有关接口终端节点支持的服务的完整列表，请参阅 VPC 终端节点 – 接口终端节点。

- *网关终端节点*是一个您在路由表中指定为某个路由的目标的网关。该路由适用于发往受支持的 AWS 服务的流量。网关终端节点支持 Amazon S3 和 Amazon DynamoDB。

使用网关 VPC 终端节点不会产生数据处理费用或按小时计算的费用。但是，我们将按照 VPC 终端节点在没个可用区中保持已预置状态的小时数收费，无论其与服务的关联状态如何。当您删除 VPC 终端节点时，我们就会停止这种按小时计费。如果终端节点服务拥有者拒绝让您的 VPC 终端节点与其服务连接，我们也会停止按小时计费。该服务随后会被删除。有关接口终端节点定价的更多信息，请参阅 AWS PrivateLink 定价。

要了解有关 VPC 终端节点的更多信息，请参阅 AWS 文档中的 VPC 终端节点。



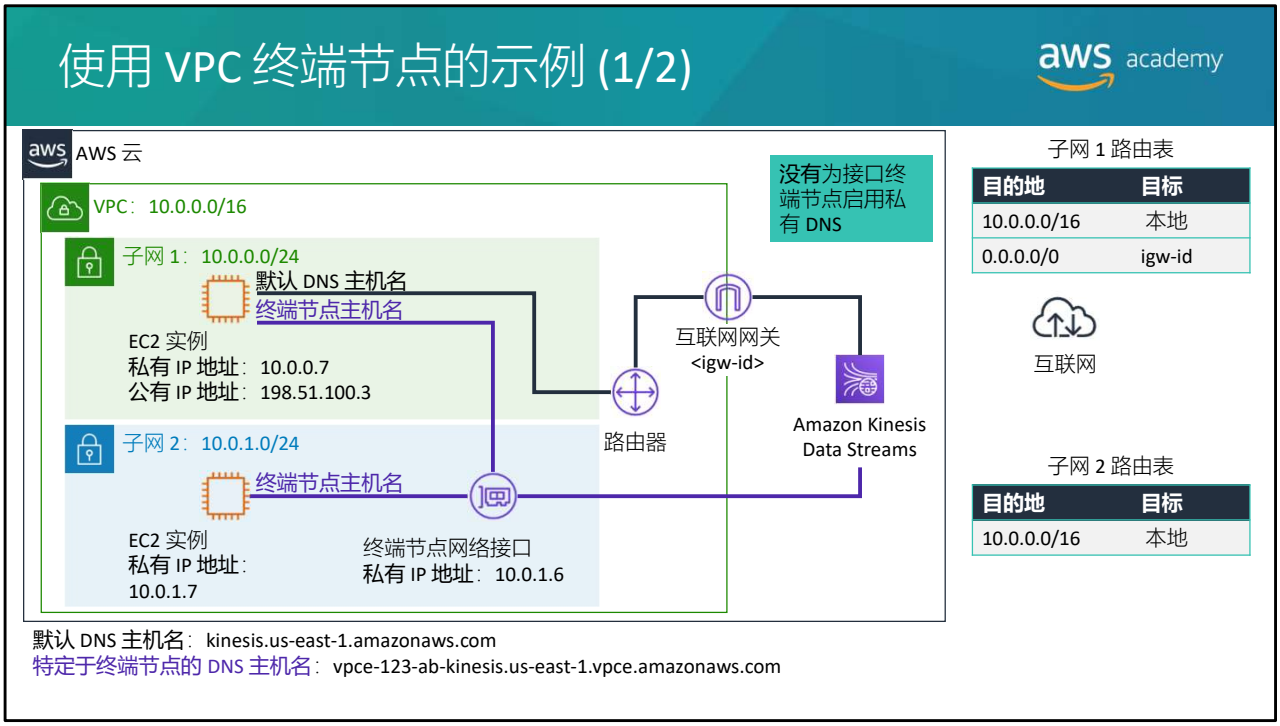
要设置接口终端节点，请从 Amazon VPC 控制台执行以下常规步骤：

1. 指定要连接的 AWS 服务、终端节点服务或 AWS Marketplace 服务的名称。
2. 选择要在其中创建接口终端节点的 VPC。您可以在服务支持的不同可用区中指定多个子网。这样做有助于确保接口终端节点在遇到可用区故障时能够恢复。在此情况下，将在您指定的每个子网中创建一个终端节点网络接口。
3. 选择 VPC 中将使用接口终端节点的子网。当您在 VPC 中为某项服务创建接口终端节点时，将在所选子网中创建*终端节点网络接口*。终端节点网络接口具有私有 IP 地址，可用作发往该服务的流量的入口点。
4. （可选）为终端节点启用私有域名系统 (DNS)。这样一来，您可以使用它的默认 DNS 主机名向服务发出请求（默认情况下，已针对为 AWS 服务和 AWS Marketplace 合作伙伴服务创建的终端节点启用）。
5. 指定要与网络接口关联的安全组。安全组规则将控制从 VPC 中的资源发送到终端节点网络接口的流量。如果您未指定安全组，将使用 VPC 的默认安全组。

服务无法通过终端节点向您 VPC 中的资源发起请求。终端节点仅针对从您 VPC 中的资源发起的流量返回响应。

有关如何创建接口终端节点的详细信息，请参阅：

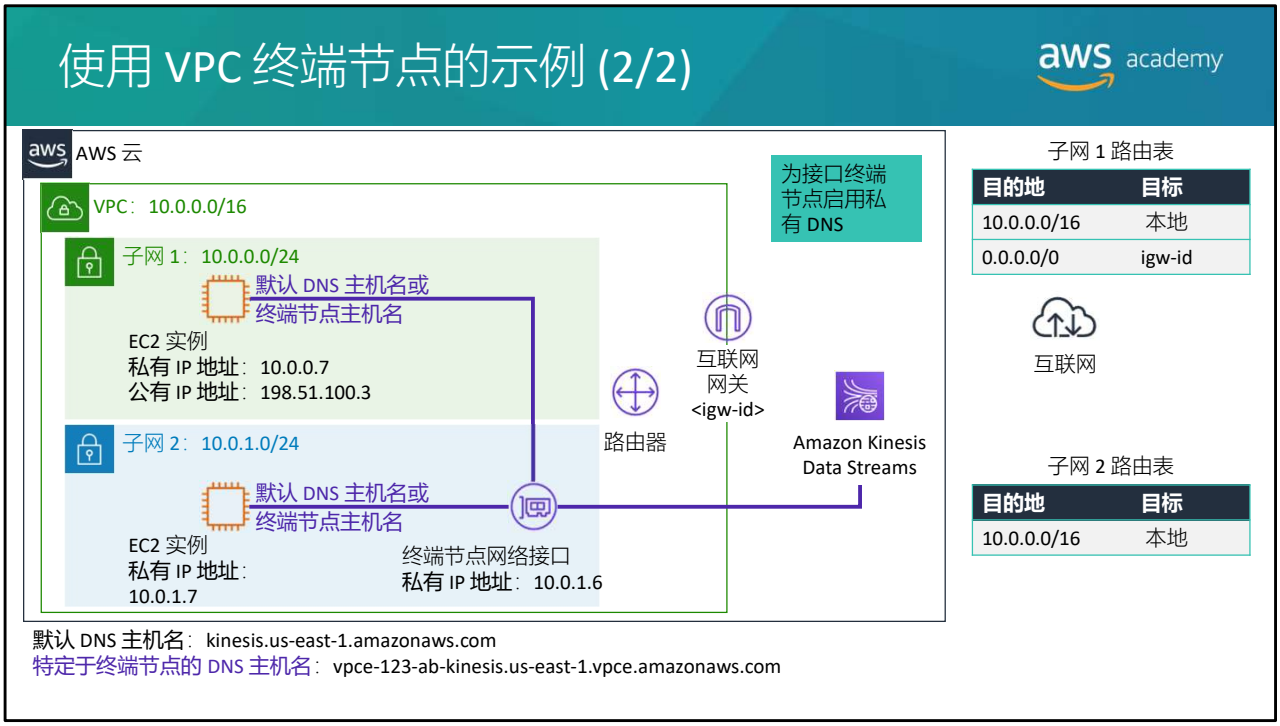
- 创建接口终端节点
- 什么是接口 VPC 终端节点，如何为我的 VPC 创建接口终端节点？



当您创建接口终端节点时，将生成您可用于与服务通信的特定于终端节点的 DNS 主机名。对于 AWS 服务和 AWS Marketplace 合作伙伴服务，私有 DNS 选项（默认启用）会将私有托管区域与您的 VPC 相关联。托管区域包含用于服务的默认 DNS 名称的记录集（例如，kinesis.us-east-1.amazonaws.com），该记录集解析为您的 VPC 中终端节点网络接口的私有 IP 地址。这样您的应用程序就能够使用服务的默认 DNS 主机名而不是特定于终端节点的 DNS 主机名来向服务发出请求。这允许您的现有应用程序通过接口终端节点向 AWS 服务发出请求，而无需任何配置更改。

在此示例中，子网 2 中有一个针对 Amazon Kinesis Data Streams 的接口终端节点和一个终端节点网络接口。**尚未**为接口终端节点启用私有 DNS。任一子网中的实例都可以使用特定于终端节点的 DNS 主机名通过接口终端节点向 Amazon Kinesis Data Streams 发送请求。子网 1 中的实例可以使用服务的默认 DNS 主机名，通过 AWS 区域中的公有 IP 地址空间与 Amazon Kinesis Data Streams 通信。

使用 VPC 终端节点的示例 (2/2)



在此示例中，已为终端节点启用私有 DNS。任一子网中的实例都可以使用默认的 DNS 主机名或特定于终端节点的 DNS 主机名，通过接口终端节点向 Amazon Kinesis Data Streams 发送请求。

有关此示例的更多信息，请参阅接口终端节点的私有 DNS。

第 6 节要点

- VPC 终端节点使您能够将 VPC 以私密方式连接到受支持的 AWS 服务和由 AWS PrivateLink 提供支持的 VPC 终端节点服务
- VPC 终端节点不需要互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接
- VPC 终端节点有两种类型：接口终端节点和网关终端节点

本模块中这节内容的要点包括：

- VPC 终端节点使您能够将 VPC 以私密方式连接到受支持的 AWS 服务和由 AWS PrivateLink 提供支持的 VPC 终端节点服务
- VPC 终端节点不需要互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接
- VPC 终端节点有两种类型：接口终端节点和网关终端节点

模块 7：连接网络

模块总结

现在来回顾下本模块，并对知识测验和对实践认证考试问题的讨论进行总结。

模块总结

aws academy

总体来说，您在本模块中学习了如何：

- 描述如何将本地网络连接到 AWS 云
- 描述如何在 AWS 云中连接 VPC
- 使用 VPC 对等连接在 AWS 云中连接 VPC
- 描述如何在 AWS 云中扩展 VPC
- 描述如何将 VPC 连接到受支持的 AWS 服务

总体来说，您在本模块中学习了如何：

- 描述如何将本地网络连接到 AWS 云
- 描述如何在 AWS 云中连接 VPC
- 使用 VPC 对等连接在 AWS 云中连接 VPC
- 描述如何在 AWS 云中扩展 VPC
- 描述如何将 VPC 连接到受支持的 AWS 服务

完成知识测验

现在可以完成本模块的知识测验。

样题

一个在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上运行的应用程序处理存储在 Amazon Simple Storage Service (Amazon S3) 上的敏感信息。此信息可以通过互联网访问。安全团队担心 Amazon S3 的互联网连接会带来安全风险。

哪种解决方案可以解决这个安全担心？

A. 通过互联网网关访问数据。
B. 通过 VPN 连接访问数据。
C. 通过 NAT 网关访问数据。
D. 通过 Amazon S3 的 VPC 终端节点访问数据。

请查看答案选项，并根据之前突出显示的关键字排除错误选项。

正确答案是 D： *“通过 Amazon S3 的 VPC 终端节点访问数据。”* 选项 A （“通过互联网网关访问数据”）可以排除，因为将 Amazon S3 中存储的数据公开会带来安全风险。选项 B （“通过 VPN 连接访问数据”）也可以排除，因为您无法通过 VPN 连接到 Amazon S3。虽然选项 C （“通过 NAT 网关访问数据”）也没错，但您只能选择一个正确的答案。选项 D 更合适，因为其无需额外的成本，也没有性能限制。

其他资源

- AWS re:Invent 2018 视频：AWS VPN 解决方案
- AWS 知识中心视频：如何使用 Amazon VPC 创建 VPN？
- 如何通过 AWS Direct Connect 配置 VPN？
- AWS re:Invent 2019 视频：从一个到多个：Amazon VPC 设计的演进
- 构建可扩展的安全多 VPC AWS 网络基础设施白皮书
- AWS 知识中心视频：什么是 AWS 对等连接？
- AWS re:Invent 2019 视频：适用于多 VPC 的 AWS Transit Gateway 参考架构
- AWS 知识中心视频：什么是接口 VPC 终端节点，如何为我的 VPC 创建接口终端节点？

如果您想了解有关本模块所涵盖主题的更多信息，下面这些其他资源可能会有所帮助：

- AWS re:Invent 2018 视频：AWS VPN 解决方案
- AWS 知识中心视频：如何使用 Amazon VPC 创建 VPN？
- 如何通过 AWS Direct Connect 配置 VPN？
- AWS re:Invent 2019 视频：从一个到多个：Amazon VPC 设计的演进
- 构建可扩展的安全多 VPC AWS 网络基础设施白皮书
- AWS 知识中心视频：什么是 AWS 对等连接？
- AWS re:Invent 2019 视频：适用于多 VPC 的 AWS Transit Gateway 参考架构
- AWS 知识中心视频：什么是接口 VPC 终端节点，如何

感谢您完成本模块的学习。