欢迎学习模块 6：创建联网环境。

本模块包含以下章节：

1. 架构需求
2. 创建网络环境
3. 将网络环境连接到互联网
4. 保护网络环境

该模块还包括：

- 一个演示，将向您展示如何手动创建 Virtual Private Cloud (VPC)
- 一个指导实验，您将在其中自行创建 VPC
- 一个挑战实验，您将在其中创建 VPC、将私有资源连接到互联网，以及创建安全层来控制进出 VPC 中私有资源的流量。

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：

- 说明 Amazon Web Services (AWS) 云联网中的 Virtual Private Cloud (VPC) 的基本功能
- 确定如何将 AWS 联网环境连接到互联网
- 描述如何在 AWS 联网环境中隔离资源
- 创建包含子网、互联网网关、路由表和安全组的 VPC

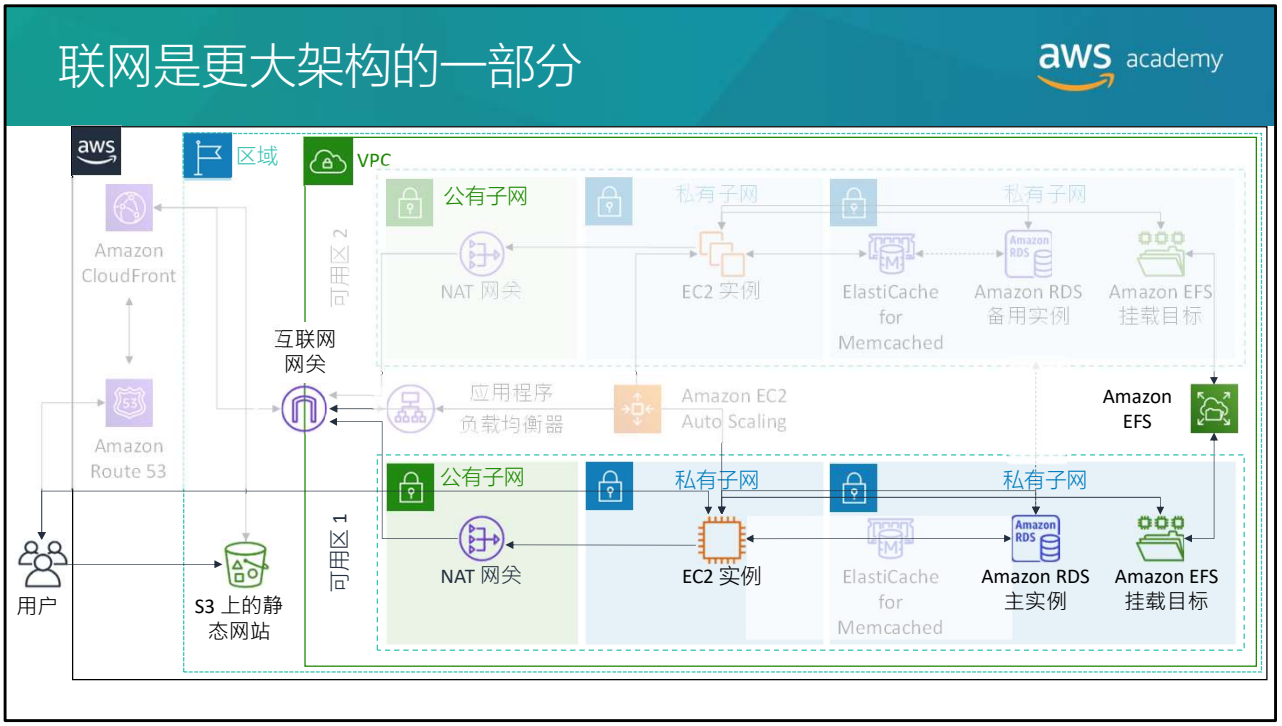
学完本模块后，您应该能够：

- 说明 Amazon Web Services (AWS) 云联网中的 Virtual Private Cloud (VPC) 的基本功能
- 确定如何将 AWS 联网环境连接到互联网
- 描述如何在 AWS 联网环境中隔离资源
- 创建包含子网、互联网网关、路由表和安全组的 VPC

模块 6：创建联网环境

第 1 节：架构需求

介绍第 1 节：架构需求。



在本模块中，您将学习如何在 AWS 上设计网络以及如何构建包含子网的 VPC。您还将学习如何将公有子网和私有子网中的实例连接到互联网。

咖啡馆业务要求

咖啡馆必须在安全、隔离的网络环境中部署和管理 AWS 资源。

该咖啡馆的业务一直在稳步增长。Sofía 和 Nikhil 已经与一些担任 AWS 顾问的咖啡馆常客成为朋友，他们开始讨论咖啡馆当前的架构。其中有一位常客是 AWS 解决方案架构师 Olivia，他认为需要扩展咖啡馆的在线业务。扩展需要额外的服务器来运行在线下单应用程序，但当前的子网规模太小，无法支持这种增长。因此，他们需要重新构建运行应用程序的网络的某些方面。

在进一步审查咖啡馆的架构时，Olivia 还发现了一个漏洞：用于管理应用程序服务器的 TCP 端口可以通过互联网访问。Sofía 解释说，她和 Nikhil 必须能够管理和维护服务器。Olivia 建议他们设置堡垒主机，以减少对服务器的公开访问，提高服务器的安全性。

模块 6：创建联网环境

第 2 节：创建 AWS 联网环境

介绍第 2 节：创建 AWS 联网环境。

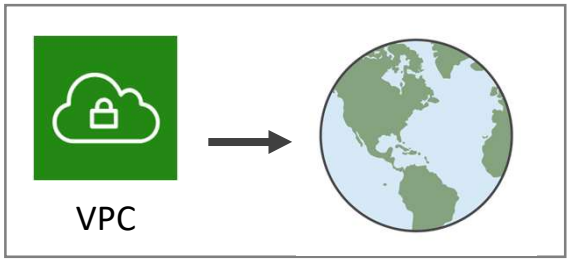
Amazon Virtual Private Cloud (Amazon VPC) 是一项服务，可让您在 AWS 云中预置一个逻辑隔离部分（称为 Virtual Private Cloud 或 VPC），您可以在其中启动您的 AWS 资源。

Amazon VPC 让您能够控制您的虚拟联网资源。例如，您可以选择自己的 IP 地址范围、创建子网以及配置路由表和网络网关。您可以在 VPC 中同时使用 IPv4 和 IPv6，实现资源和应用程序安全访问。

您还可以自定义 VPC 的网络配置。例如，您可以为可访问公有互联网的 Web 服务器创建一个公有子网。您可以将后端系统（例如数据库或应用程序服务器）放在不能通过公有互联网访问的私有子网中。

最后，您可以使用多个安全层，帮助控制对每个子网中的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的访问。这些安全层包括安全组和网络访问控制列表（网络 ACL）。

VPC 部署



您可以在任何 AWS 区域中部署 VPC。

VPC 可以托管其所在区域中任何可用区的受支持的资源。

VPC 属于单个 AWS 区域。VPC 跨越区域中的所有可用区，因此它可以托管来自其所在区域内任何可用区的受支持的资源。

无类域间路由 (CIDR)

0.0.0.0/0	= 所有 IP 地址
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	总 IP 地址数
/28	16
...	...
/20	4096
/19	8192
/18	16384
/17	32768
/16	65536

在创建 VPC 时，您可以提供您希望 VPC 中的实例使用的私有 IP 地址集。您以无类域间路由 (CIDR) 块的形式指定此地址集，例如 10.0.0.0/16。这是您的 VPC 的主要 CIDR 块。您可以指定 /28（16 个 IP 地址）到 /16（65536 个 IP 地址）之间的块大小。

Amazon VPC 支持 IPv4 和 IPv6 地址分配，并为它们设定了不同的 CIDR 块大小限制。默认情况下，所有 VPC 和子网都必须具有 IPv4 CIDR 块，您不能更改此行为。您可以选择将 IPv6 CIDR 块与您的 VPC 关联。

您的 VPC 可在双堆栈模式下运行：您的资源可通过 IPv4 和/或 IPv6 进行通信。IPv4 和 IPv6 地址是相互独立的，因此您必须在 VPC 中分别针对 IPv4 和 IPv6 配置路由和安全设置。

子网：划分 VPC

- 子网是 VPC 的 IP 地址范围的分段或分区，您可以在其中分配一组资源
- 子网不是隔离边界
- 子网是 VPC CIDR 块的子集
- 子网 CIDR 块不能重叠
- 每个子网完全位于一个可用区内
- 您可以在每个可用区或本地扩展区中添加一个或多个子网
- AWS 在每个子网中预留五个 IP 地址

例如：具有 CIDR /22 VPC 共包含 1024 个 IP 地址。

您可以将 VPC 划分为一个或多个子网。子网是 VPC 的 IP 地址范围的分段或分区，您可以在其中分配一组资源。请务必记住，子网不是应用程序的隔离边界。相反，它们是存储路由策略的容器，您将在本模块的下一节中了解这些内容。

在创建子网时，需要为子网指定 CIDR 块，它是 VPC CIDR 块的子集。子网的 CIDR 块不能重叠。

尽管每个子网都必须完全位于一个可用区内且不能跨越区域，但每个可用区都可以有一个或多个子网。您可以选择在本地扩展区中添加子网。当您在本地扩展区中创建子网时，VPC 也会扩展到该本地扩展区。有关如何将 VPC 资源扩展到本地扩展区的更多信息，请参阅 AWS 文档中的将 VPC 资源扩展到 AWS 本地扩展区。

由于 VPC 子网映射到特定可用区，因此子网置放是用以确保 Amazon EC2 实例恰当分布在多个位置的一种方式。

AWS 将预留每个子网 CIDR 块中的前四个 IP 地址和最后一个 IP 地址。例如，在 CIDR 块

为 10.0.0.0/24 的子网中，AWS 将预留以下五个 IP 地址：

- 10.0.0.0：网络地址
- 10.0.0.1：VPC 本地路由器
- 10.0.0.2：域名系统 (DNS) 解析
- 10.0.0.3：未来使用
- 10.0.0.255：网络广播地址

有关 VPC 和子网的更多信息，请参阅 AWS 文档中的 VPC 和子网。

VPC 设计最佳实践

- 为具有唯一路由要求的每组主机的每个可用区创建一个子网。
- 在一个区域内的所有可用区中平均划分 VPC 网络范围。
- 不要一次分配所有网络地址。相反，请确保预留一些地址空间以备将来使用。
- 调整 VPC CIDR 和子网的大小，以支持预期工作负载的显著增长 。
- 确保 VPC 网络范围（CIDR 块）不会与组织的其他私有网络范围重叠。

在配置任何计算机网络时，请考虑以下通用网络设计原则：

- 为具有唯一路由要求的每组主机的每个可用区创建一个子网。
- 在一个区域内的所有可用区中平均划分 VPC 网络范围。
- 不要一次分配所有网络地址。相反，请确保预留一些地址空间以备将来使用。
- 调整 VPC CIDR 和子网的大小，以支持预期工作负载的显著增长。
- 确保 VPC 网络范围（CIDR 块）不会与组织的其他私有网络范围重叠。

有关设计和调整单个 VPC 大小的更多信息，请参阅 AWS 单个 VPC 设计。

单个 VPC 部署

在有限的使用案例中，部署一个 VPC 可能是合适的做法：

- 由小型团队管理的小型单一应用程序
- 高性能计算 (HPC)
- 身份管理

在大多数使用案例中，组织基础设施主要使用两种模式：多 VPC 和多账户。

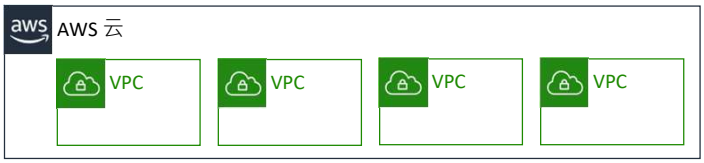
在设计和创建网络环境时，可能适合使用单个 VPC 环境的使用案例数量有限：

- 由小型团队管理的小型单一应用程序
- 高性能计算 (HPC) 环境（例如物理模拟）– 相比跨越多个 VPC 的环境，单个 VPC 环境的延迟更低
- 身份管理环境 – 单个 VPC 可能提供最佳安全性。

但是，对于大多数使用案例而言，都需要多 VPC 环境。您可以在同一区域或不同区域创建多个 VPC。您还可以在同一 AWS 账户或不同 AWS 账户中创建多个 VPC。

多个 VPC

- 最适合 –
  - 单个团队或单个企业或组织，例如托管服务提供商
  - 有限团队，更便于保持标准和管理访问
- 例外 –
  - 监管和合规性标准可能需要更大规模的工作负载隔离，与企业或组织复杂程度无关



多 VPC 最适合对每个应用程序环境中所有资源的预置和管理保持完全掌控的单一团队或组织。例如，假设有一个开发大型电子商务应用程序的团队。当开发人员能够完全访问开发和生产环境时，他们可能会使用此模式。管理测试和生产环境中所有资源的托管服务提供商 (MSP) 也通常使用这种模式。

要了解有关多 VPC 部署的服务和最佳实践的更多信息，请参阅：

- 单区域多 VPC 连接
- 多区域多 VPC 连接

多个账户

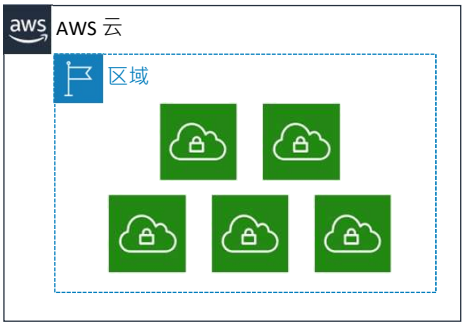
- 最适合 –
  - 大型企业或组织和拥有多个 IT 团队的企业或组织
  - 预计发展迅速的中型企业或组织
- 为什么?
  - 在较为复杂的企业或组织中，管理访问和标准的难度会更大。

如前所述，您可以在同一 AWS 账户或不同账户中创建多个 VPC。

多账户模式最适合企业客户或跨多个团队部署应用程序的组织。例如，假设某个组织要支持两个或多个团队。他们可能会使用此模式来支持以下开发人员：能够完全访问开发环境资源，但对生产环境的访问权限有限或根本没有权限。

Amazon VPC 配额

默认配额：每账户每区域 5 个 VPC *



* 默认配额为每区域 5 个 VPC，但可以申请增加配额。

注意 Amazon VPC 配额。默认配额为每个区域 5 个 VPC。但是，您可以请求增加此配额。

有关 Amazon VPC 服务限制的更多信息，请参阅 AWS 文档中的 Amazon VPC 配额。

第 2 节要点

- 使用 Amazon VPC，您可以预置 VPC，这些 VPC 是 AWS 云中的逻辑隔离部分，您可以在其中启动 AWS 资源。
- 一个 VPC 只属于一个区域，并且被划分为子网。
- 一个子网属于一个可用区或本地扩展区。它是 VPC CIDR 块的子集。
- 您可以在相同区域或不同区域以及相同或不同账户中创建多个 VPC。
- 在设计 VPC 时，请遵循最佳实践。

本模块中这节内容的要点包括：

- 使用 Amazon VPC，您可以预置 VPC，这些 VPC 是 AWS 云中的逻辑隔离部分，您可以在其中启动 AWS 资源。
- 一个 VPC 只属于一个区域，并且被划分为子网。
- 一个子网属于一个可用区或本地扩展区。它是 VPC CIDR 块的子集。
- 您可以在相同区域或不同区域以及相同账户或不同账户中创建多个 VPC。
- 在设计 VPC 时，请遵循以下最佳实践：
    - 为具有唯一路由要求的每组主机的每个可用区创建一个子网。
    - 在一个区域内的所有可用区中平均划分 VPC 网络范围。
    - 不要一次分配所有网络地址。相反，请确保预留一些地址空间以备将来使用。
    - 调整 VPC CIDR 和子网的大小，以支持预期工作负载的显著增长。
    - 确保 VPC 网络范围不会与企业或组织的其他私有网络范围重叠。

模块 6：创建联网环境

第 3 节：将 AWS 联网环境连接到互联网

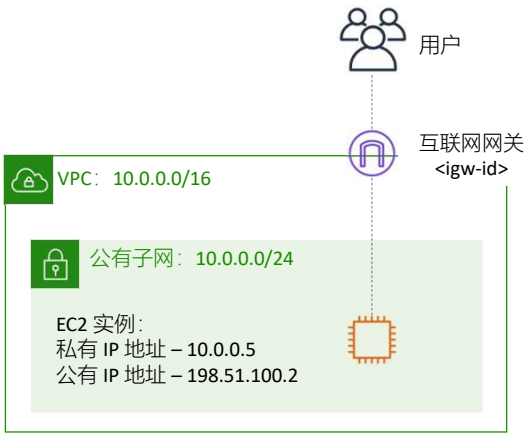
介绍第 3 节：将 AWS 联网环境连接到互联网。

创建公有子网

aws academy

互联网网关

- 允许 VPC 中的资源与互联网之间的通信
- 在默认情况下，水平扩展、具有冗余且高度可用
- 在子网路由表中为 Internet 可路由流量提供一个目标



现在，您已经知道如何为工作负载设计和创建隔离的网络环境，您希望将其连接到互联网。

互联网网关*是一种 VPC 组件，可允许 VPC 中的资源与互联网之间进行通信。*它可水平扩展、冗余且高度可用。互联网网关支持 IPv4 和 IPv6 流量。互联网网关有两种用途：首先，它在 VPC 路由表中为互联网可路由流量提供一个目标。其次，互联网网关为已分配公有 IPv4 地址的实例执行网络地址转换 (NAT)。

要将子网设为*公有*，您必须首先创建一个互联网网关并将其连接到 VPC。

定向 VPC 资源之间的流量

- 需要使用路由表来定向 VPC 资源之间的流量
- 每个 VPC 有一个主（默认）路由表
- 所有子网都必须与路由表关联
- 您可以创建自定义路由表

最佳实践：针对每个子网使用自定义路由表。

公有路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	<igw-id>

接下来，您必须更新与要连接到互联网的子网关联的路由表。路由表*包含一组称为*路由*的规则*。路由 用于确定将网络流量的目标去向。

当您创建 VPC 时，它会自动具有一个主路由表。主路由表（以及 VPC 中的每个路由表）最初仅包含一项支持 VPC 中所有资源通信的本地路由。您无法修改路由表中的本地路由。当您在 VPC 中启动实例时，本地路由会自动覆盖该实例。您不需要将新实例添加到路由表。您可以为您的 VPC 创建额外的自定义路由表。

VPC 中的每个子网必须与一个路由表相关联，该路由表会控制此子网的路由。如果您未将子网明确关联到特定路由表，则该子网将与主路由表建立隐式关联。一个子网一次只能与一个路由表关联，但您可以将多个子网与同一个路由表关联。

您可以针对每个子网创建自定义路由表，以实现对目标位置的精细路由。

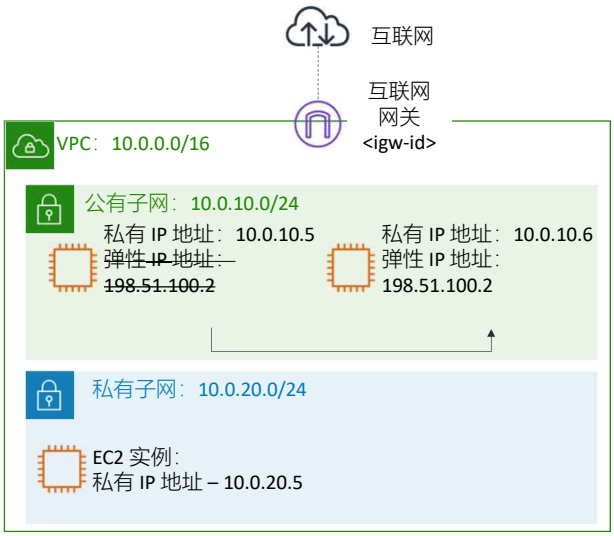
要通过互联网网关将非本地流量发送到互联网，请在与子网关联的路由表中创建一个目的地为 **0.0.0.0/0**、目标为 **<igw-id>** 的路由。

将 IP 地址从一个实例重新映射到另一个实例

aws academy

弹性 IP 地址

- 与您的 AWS 账户关联的静态公有 IPv4 地址
- 可与实例或弹性网络接口相关联
- 可以重新映射到账户中的另一个实例
- 当负载均衡器不可用时对实现冗余非常有用



接下来，您必须确保您的实例具有公有 IP 地址或弹性 IP 地址。

弹性 IP 地址*是专用于动态云计算的静态公有 IPv4 地址*。您可以将弹性 IP 地址与您账户中的任意 VPC 的任何实例或弹性网络接口相关联。借助弹性 IP 地址，您可以迅速将地址重新映射到 VPC 中的其他实例，从而屏蔽实例故障。与将弹性 IP 地址与实例直接关联相比，将弹性 IP 地址与网络接口关联具有一个优势。您可以通过一个步骤将网络接口的所有属性从一个实例移动到另一个实例。

将私有子网连接到互联网

aws academy

NAT 网关

- 使私有子网中的实例可以发起到互联网或其他 AWS 服务的出站流量
- 防止私有实例接收来自互联网的入站连接请求

公有路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	<igw-id>

私有路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	<nat-id>

要将私有子网中的实例连接到互联网或其他 AWS 服务，您需要一个*网络地址转换 (NAT)* 网关。利用 NAT 网关，私有子网中的实例可以连接到互联网或其他 AWS 服务，但会阻止互联网发起与这些实例的连接。

要创建 NAT 网关，您必须指定 NAT 网关所处的公有子网。同时，还必须指定与该 NAT 网关关联的弹性 IP 地址。创建 NAT 网关之后，必须更新与您的一个或多个私有子网关联的路由表，以便将流向互联网的流量指向该 NAT 网关。这样，您的私有子网中的实例便可以与互联网通信。

子网使用案例示例（第 1 个，共 2 个）

数据存储实例

批处理实例

后端实例

Web 应用程序实例

花点时间思考下，这些示例中的实例是应该放入公有子网还是私有子网中。

子网使用案例示例（第 2 个，共 2 个）

数据存储实例 → 私有子网

批处理实例 → 私有子网

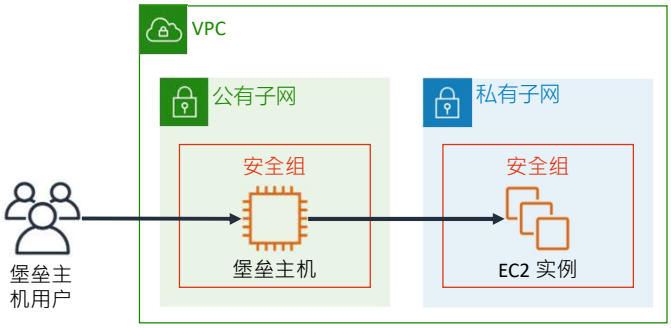
后端实例 → 私有子网

Web 应用程序实例 → 公有子网或私有子网

数据存储实例、批处理实例和后端实例应放入私有子网中。您可以将 Web 层实例放入公有子网中。但是，AWS 建议您将 Web 层实例放入*私有*子网中，并将其置于公有子网中的负载均衡器之后。在某些环境中，您必须将 Web 应用程序实例直接挂载到弹性 IP 地址（不过您也可以将弹性 IP 地址挂载到负载均衡器）。在这些情况下，Web 应用程序实例必须放入公有子网。

堡垒主机

- 用于从外部网络访问私有网络的服务器
- 必须尽量减少渗透的可能性



堡垒主机*是用于从外部网络（例如互联网）访问私有网络的服务器*。您可以使用堡垒主机最大限度地降低渗透和潜在攻击私有网络中的资源的可能性。

例如，假设您希望允许通过 Secure Shell 或 SSH 从外部网络连接到 VPC 私有子网中的 Linux 实例。

您可以使用堡垒主机来降低允许这些外部 SSH 连接到私有子网中实例的风险。堡垒主机通常在 VPC 的公有子网中的 EC2 实例上运行，如本示例所示。私有子网中的 Linux 实例位于安全组中，允许从附加到堡垒主机的安全组进行 SSH 访问。堡垒主机用户连接到堡垒主机，以便他们可以连接到 Linux 实例。

尽管您可以调整此架构来满足自己的要求，但堡垒主机应该是 Linux 实例的唯一 SSH 流量来源。

有关此架构的更多信息，请参阅博客文章 How to Record SSH Sessions Established Through a Bastion Host。要了解如何在 AWS 上的 VPC 环境中部署 Linux 堡垒主机，请完成 AWS 中的 Linux 堡垒主机 Quick Start。

演示：
创建 Virtual Private Cloud

现在，您的讲师可能会选择演示如何使用 Amazon VPC 手动创建包含子网、互联网网关和路由表的 VPC。

第 3 节要点

- 互联网网关允许 VPC 中的实例与互联网进行通信。
- 路由表 控制来自子网或网关的流量。
- 弹性 IP 地址是静态公有 IPv4 地址，可以与实例或弹性网络接口关联。它们可以重新映射到您账户中的另一个实例。
- NAT 网关使私有子网中的实例可以发起到互联网或其他 AWS 服务的出站流量。
- 堡垒主机是用于从外部网络（例如互联网）访问私有网络的服务器。

本模块中这节内容的要点包括：

- 互联网网关允许 VPC 中的实例与互联网进行通信。
- 路由表控制来自子网或网关的流量。
- 弹性 IP 地址是静态公有 IPv4 地址，可以与实例或弹性网络接口关联。它们可以重新映射到您账户中的另一个实例。
- NAT 网关使私有子网中的实例可以发起到互联网或其他 AWS 服务的出站流量。
- 堡垒主机是用于从外部网络（例如互联网）访问私有网络的服务器。

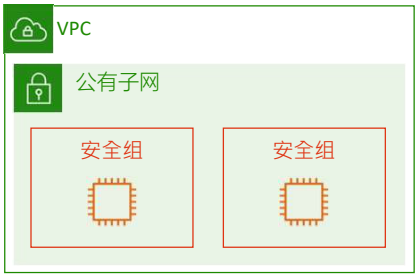
模块 6：创建联网环境

第 4 节：保护 AWS 联网环境

介绍第 4 节：保护 AWS 联网环境

安全组

- 有状态防火墙，可控制出入 AWS 资源的入站和出站流量
- 在实例或网络接口级别运行



现在，您已经知道如何设计和部署网络环境并将其连接到互联网，您必须隔离您的应用程序和工作负载。

您可以通过来实现隔离：将托管您应用程序或工作负载的 EC2 实例部署到附加到您 VPC 的安全组中。

安全组是在实例或网络接口级别运行的有状态防火墙。

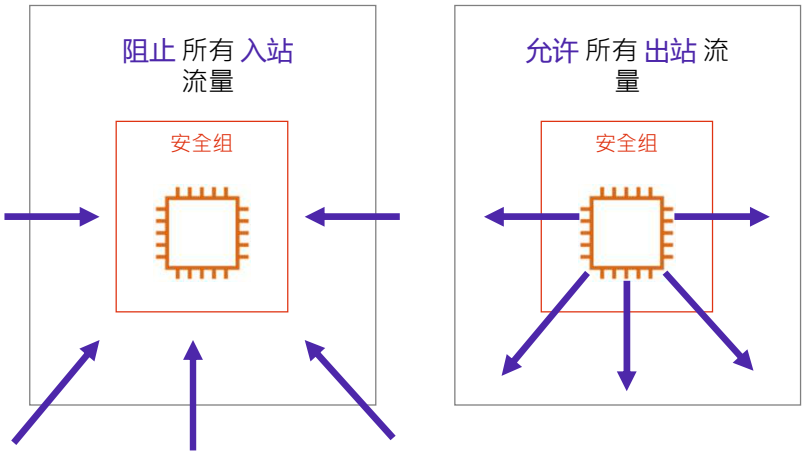
有状态意味着，自动允许返回流量，不受规则影响。例如，假设您通过家庭计算机对您的实例发起了互联网控制消息协议 (ICMP) *ping* 命令。如果入站安全组规则允许 ICMP 流量，则系统会跟踪有关连接的信息（包括端口信息）。实例对 ping 命令的响应流量不会作为新请求进行跟踪，而是作为已建立的连接进行跟踪。即使出站安全组规则限制了出站 ICMP 流量，也将允许从实例流出。

安全组规则控制出入您的 AWS 资源的入站和出站流量。您应该严格配置这些规则，以限制流量并仅在需要时允许访问。流量可以受任何互联网协议、服务端口以及源或目标 IP 地址（单个 IP 地址或 CIDR 块）的限制。

并非所有的流量流都会被跟踪。假设一个安全组规则允许所有流量（即 0.0.0.0/0）的传输控制协议 (TCP) 或用户数据报协议 (UDP) 流。另一个方向还有一个允许响应流量的相

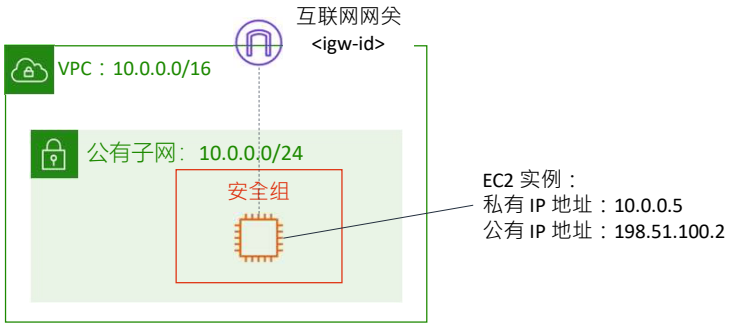
应规则。在这种情况下，不会跟踪该流量流。因此，允许响应流量基于允许响应流量的入站或出站规则流动，而不是基于跟踪信息流动。

默认安全组



当您创建一个安全组时，它没有入站规则。这意味着，您必须向安全组添加入站规则，以允许来自另一台主机的入站流量进入您的实例。默认情况下，安全组包含*允许所有出站流量*的出站规则。您可以删除该规则并添加只允许特定出站流量的出站规则。如果您的安全组没有出站规则，则系统将不允许来自您实例的任何出站流量。

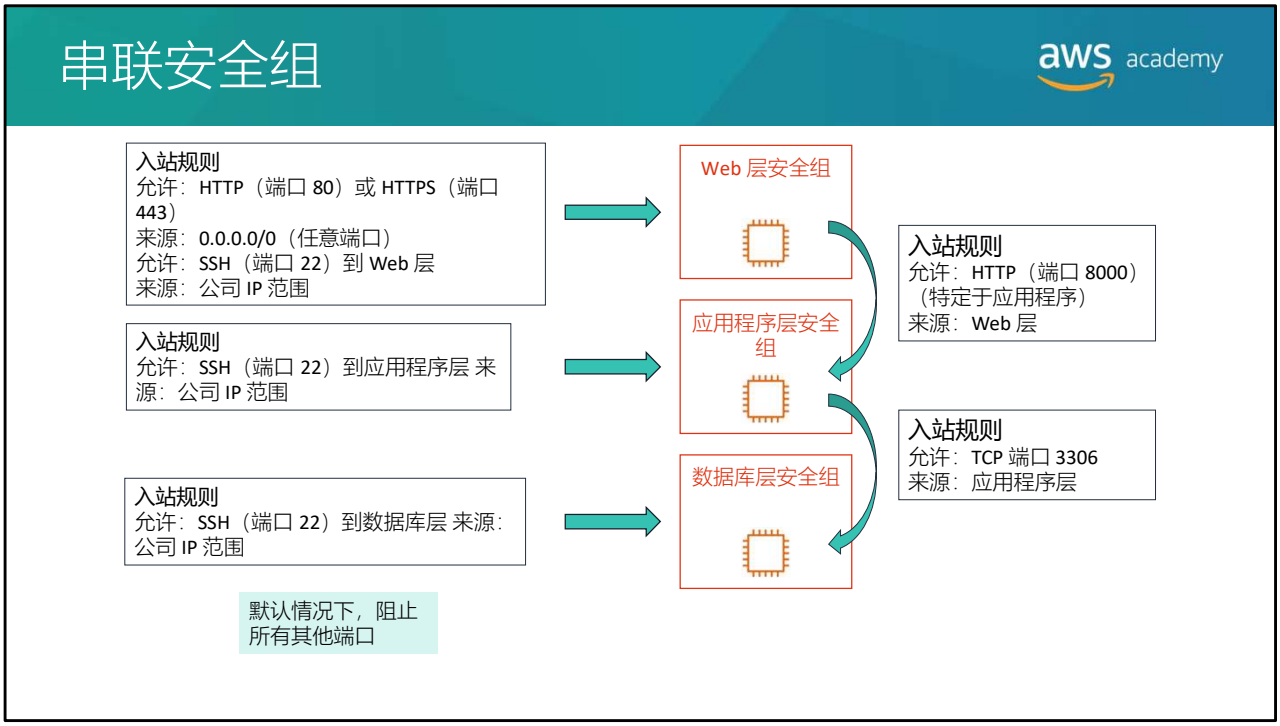
自定义安全组



入站				
类型	协议	端口范围	源	目的地
HTTP	TCP	80	任何位置	允许 Web 访问

创建自定义安全组时，您可以指定*允许*规则，但不可以指定*拒绝*规则。例如，当您为托管 Web 应用程序的实例创建公有子网时，最后一步是创建允许向这些实例发送 HTTP 流量的安全组。

在做出允许流量的决定之前评估所有规则。

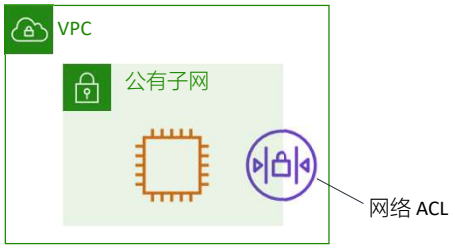


大多数云组织创建的安全组都会为每个功能层设置入站规则。此示例显示了典型的三层应用程序中的安全组链。入站和出站规则的设置方式为，仅允许流量从顶层流向底层，然后再流回。安全组将充当防火墙，防止分层中的安全漏洞自动为受影响的客户端提供针对所有资源的子网范围访问权限。

安全组可以配置为针对不同类别的实例设置不同的规则。思考下这个 Web 应用程序的传统三层架构的示例。用于 Web 服务器的组将具有对互联网开放的端口 80 (HTTP) 或端口 443 (HTTPS)。用于应用程序服务器的组将具有仅供 Web 服务器组访问的端口 8000（特定于应用程序）。用于数据库服务器的组将具有仅对应用程序服务器组开放的端口 3306 (MySQL)。这三个组均允许端口 22 (SSH) 上的管理访问，但只能从客户的公司网络访问。此机制可以实现高度安全应用程序的部署。

网络访问控制列表（网络 ACL）

- 在子网级别运行
- 默认情况下允许所有入站和出站流量
- 无状态防火墙，要求针对入站和出站流量设置显式规则



网络访问控制列表（网络 ACL）*是 VPC 的可选安全层*。它充当防火墙，用于控制进出一个或多个子网的流量。 要向您的 VPC 添加额外的安全层，您可以使用类似于安全组的规则设置网络 ACL。

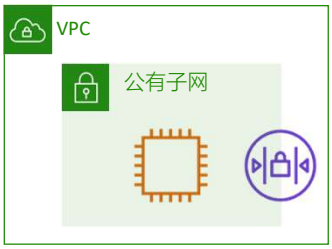
您的 VPC 中的每个子网都必须与一个网络 ACL 相关联。如果您没有将某个子网与一个网络 ACL 显式关联，则该子网将自动与默认网络 ACL 关联。您可以将网络 ACL 与多个子网关联。但是，一个子网一次只能与一个网络 ACL 关联。当您将一个网络 ACL 与一个子网关联时，之前的关联将被删除。

网络 ACL 有单独的入站和出站规则，每项规则都可以允许或拒绝流量。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）。

网络 ACL 是*无状态的*，这意味着在处理请求后，不会保留有关请求的信息。必须通过规则显式允许返回流量。

自定义网络 ACL

建议
仅限特定网络安全要求



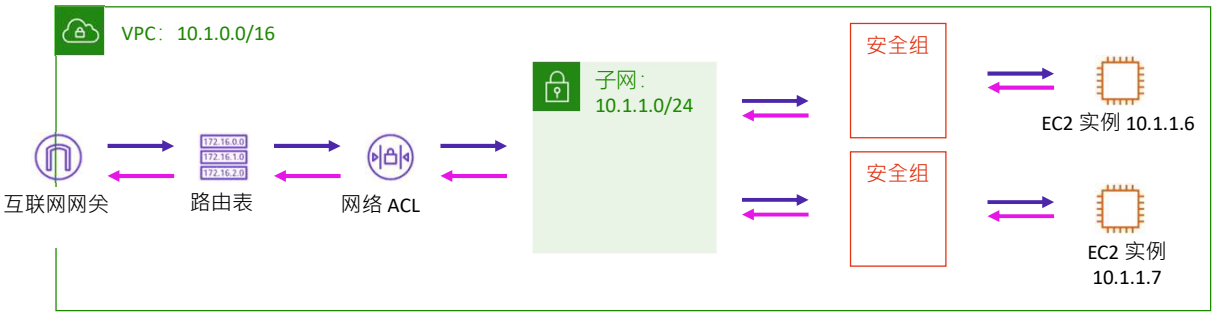
Nacl-11223344

入站：
规则 # 100：SSH 172.31.1.2/32 允许
规则 # *：所有流量 0.0.0.0/0 拒绝

出站：
规则 # 100：自定义 TCP 172.31.1.2/31 允许
规则 # *：所有流量 0.0.0.0/0 拒绝

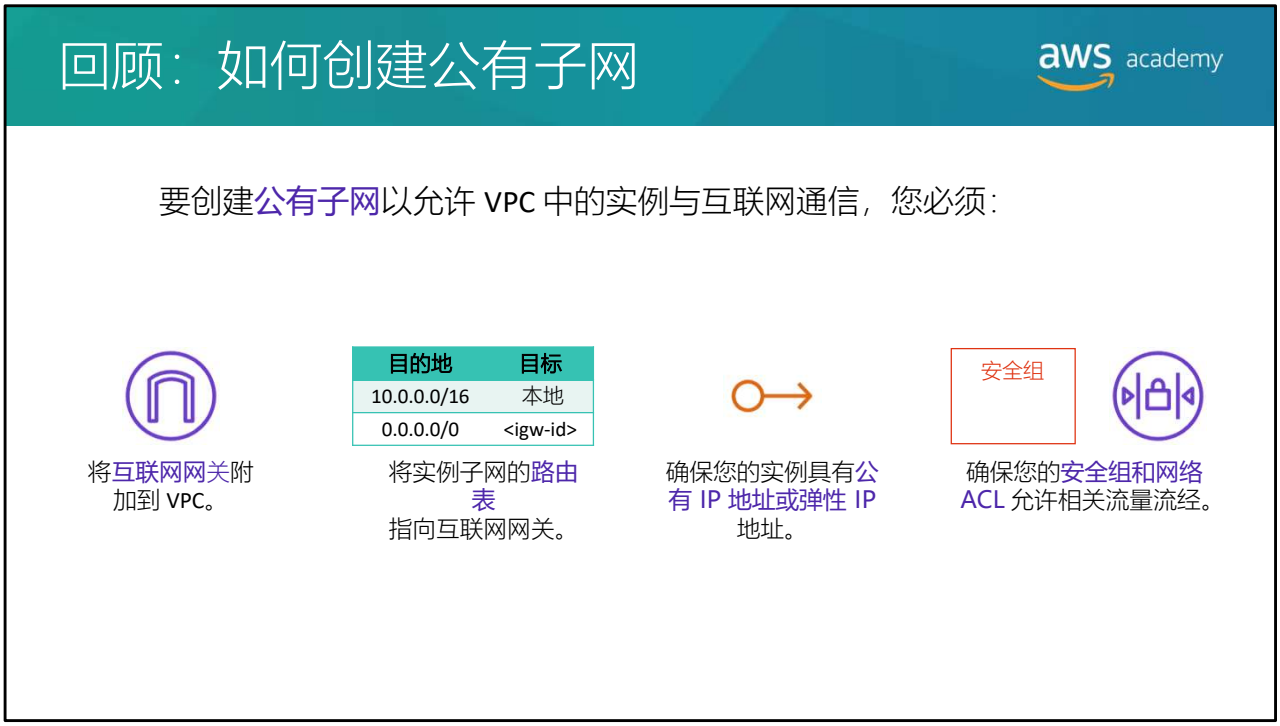
您可以创建*自定义*网络 ACL 并将其与子网相关联。默认情况下，每个自定义网络 ACL 将拒绝所有入站和出站流量，直至您添加相关规则。

使用多层防护构建基础设施



作为最佳实践，您应该使用多层防护保障您的基础设施安全。通过在 VPC 中运行基础设施，您可以控制将哪些实例对互联网开放。您可以定义安全组和网络 ACL，以便分别在基础设施和子网级别进一步保护您的基础设施。此外，您应该使用防火墙在操作系统级保障您的实例安全，并遵循其他安全性最佳实践。

在同时实施网络 ACL 和安全组作为控制流量的深度防御方法时，即使某项控制措施的配置出现错误的情况下，主机也不会遭遇不需要的流量。



回顾一下，要创建公有子网以允许 VPC 中的实例与互联网进行通信，您必须：

- 将互联网网关附加到 VPC。
- 将路由添加到您子网的路由表，该路由表将流向互联网的流量定向到互联网网关
- 确保您的实例具有公有 IP 地址或弹性 IP 地址
- 确保您的安全组和网络 ACL 允许相关流量流经

第 4 节要点

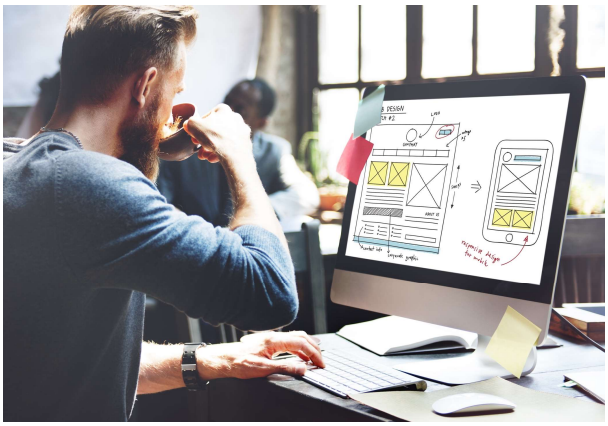
- 安全组是在实例级别运行的有状态防火墙
- 网络 ACL 是在子网级别运行的无状态防火墙
- 当您设置入站和出站规则以允许流量从架构的顶层流向底层时，您可以将安全组串联在一起来隔离安全漏洞
- 您应使用多层防护构建基础设施

本模块中这节内容的要点包括：

- 安全组是在实例级别运行的有状态防火墙
- 网络 ACL 是在子组级别运行的无状态防火墙
- 当您设置入站和出站规则以允许流量从架构的顶层流向底层时，您可以将安全组串联在一起来隔离安全漏洞
- 您应使用多层防护构建基础设施

模块 6 – 指导实验：创建 Virtual Private Cloud

aws academy



您现在将完成模块 6 – 指导实验：创建 Virtual Private Cloud。

指导实验：任务

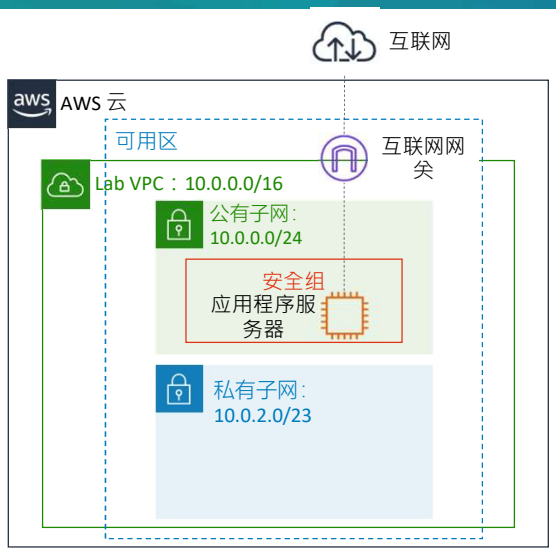
使用 Amazon VPC 手动创建 VPC，其中包括：

- 公有子网和私有子网
- 一个互联网网关
- 一个路由表，包含将流向互联网的流量定向至互联网网关
- 一个针对公有子网中 EC2 实例的安全组
- 一个测试 VPC 的应用程序服务器

在本实验中，您将使用 Amazon VPC 手动创建具有以下组件的 VPC：

- 公有子网和私有子网
- 一个互联网网关
- 一个路由表，包含将流向互联网的流量定向至互联网网关
- 一个针对公有子网中 EC2 实例的安全组
- 一个测试 VPC 的应用程序服务器

指导实验：最终产品



该图总结了您完成实验后将会构建的内容。

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 6 – 挑战实验：为咖啡馆创建 VPC 联网环境

您现在将完成模块 6 – 挑战实验：为咖啡馆创建 VPC 联网环境。

业务需求：安全的联网环境

Sofía 和 Nikhil 已将咖啡馆的数据库层与 Web 应用程序层分开。他们还将数据库资源从公有子网移动到了私有子网。

Mateo 建议他们通过与数据库实例相互独立的私有子网中运行咖啡馆的应用程序服务器，以便增强安全性。

Sofía 和 Nikhil 成功创建了一个双层架构，他们在这个架构中将咖啡馆的数据库层与 Web 应用程序层分开。他们还将数据库资源从公有子网移动到了私有子网。

Mateo 建议他们在与数据库实例相互独立的私有子网中运行咖啡馆的应用程序服务器，来增强 VPC 的安全性。

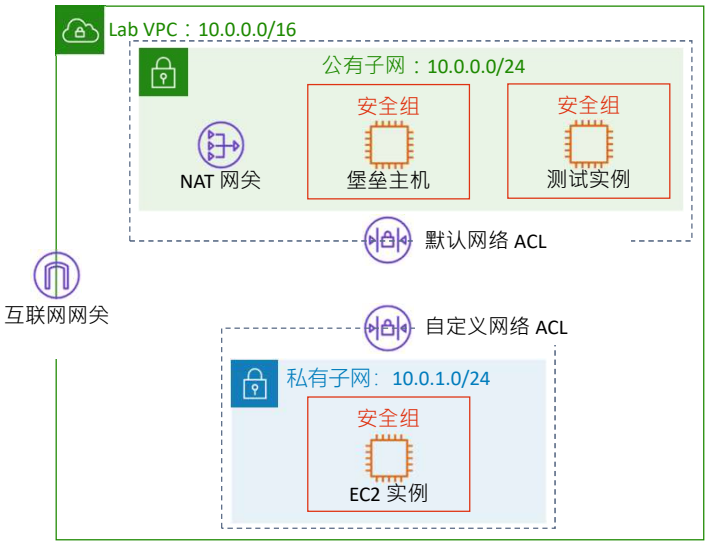
挑战实验：任务

1. 创建公有子网
2. 创建堡垒主机
3. 为堡垒主机分配弹性 IP 地址
4. 测试与堡垒主机的连接
5. 创建私有子网
6. 创建 NAT 网关
7. 在私有子网中创建 EC2 实例
8. 为 SSH 传递配置 SSH 客户端
9. 测试与堡垒主机的 SSH 连接
10. 创建网络 ACL
11. 测试自定义网络 ACL

在本挑战实验中，您将完成以下任务：

1. 创建公有子网
2. 创建堡垒主机
3. 为堡垒主机分配弹性 IP 地址
4. 测试与堡垒主机的连接
5. 创建私有子网
6. 创建 NAT 网关
7. 在私有子网中创建 EC2 实例
8. 为 SSH 传递配置 SSH 客户端
9. 测试与堡垒主机的 SSH 连接
10. 创建网络 ACL
11. 测试自定义网络 ACL

挑战实验：最终产品



该图总结了您完成实验后将会构建的内容。

现在可以开始挑战实验了。

挑战实验总结：要点

完成这个挑战实验之后，您的讲师可能会带您讨论此挑战实验的要点。

模块 6：创建联网环境

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

总体来说，您在本模块中学习了如何：

- 说明 AWS 云联网中 VPC 的基本功能
- 确定如何将 AWS 联网环境连接到互联网
- 描述如何在 AWS 联网环境中隔离资源
- 创建包含子网、互联网网关、路由表和安全组的 VPC

总体来说，您在本模块中学习了如何：

- 说明 AWS 云联网中 VPC 的基本功能
- 确定如何将 AWS 联网环境连接到互联网
- 描述如何在 AWS 联网环境中隔离资源
- 创建包含子网、互联网网关、路由表和安全组的 VPC

完成知识测验

现在可以完成本模块的知识测验。

样题

aws academy

您有一个应用程序，在单个可用区中的多个 Amazon Elastic Compute Cloud (Amazon EC2) 实例上运行。该应用程序通过互联网调用第三方应用程序编程接口 (API)。

如何为第三方 API 提供单个 IP 地址以添加到访问安全列表中？

A. 为实例分配弹性 IP 地址。
B. 为实例分配公有 IP 地址。
C. 将实例置于 NAT 网关之后。
D. 将实例置于 Network Load Balancer 之后。

思考答案选项，并根据之前突出显示的关键字排除错误选项。

正确答案是 C： *“将实例置于 NAT 网关之后。”* 可以排除选项 A 和 B，因为应用程序最终将拥有多个公有 IP 地址，而安全列表只需要一个 IP 地址。也可以排除选项 D，因为 Network Load Balancer 也将拥有多个 IP 地址。选项 C 是正确的，因为 NAT 网关可以通过单个 IP 地址访问。

其他资源

- VPC 和子网
- 从一个到多个：VPC 设计的演进
- AWS 单个 VPC 设计
- AWS re:Invent 2018：您的虚拟数据中心：VPC 基础知识和连接选项
- AWS 联网基础知识

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：

- VPC 和子网
- 从一个到多个：VPC 设计的演进
- AWS 单个 VPC 设计
- AWS re:Invent 2018：您的虚拟数据中心：VPC 基础知识和连接选项
- AWS 联网基础知识

感谢您完成本模块的学习。