Amazon Virtual Private Cloud

User Guide

API Version 2013-02-01

Amazon Web Services

Amazon Virtual Private Cloud: User Guide

Amazon Web Services

Amazon VPC 是什么？

Amazon Virtual Private Cloud (Amazon VPC) 允许您在已经定义的虚拟网络内启动 Amazon Web Services (AWS) 资源。这个虚拟网络与您在数据中心中运行的传统网络极其相似，并会为您提供使用 AWS 的可扩展基础设施的优势。

Topics

Amazon VPC 概念

在您熟悉 Amazon VPC 时，您应了解这个虚拟网络的主要概念，以及它与您的自有网络有哪些相似或差异之处。此部分提供对于 Amazon VPC 主要概念的简要描述。

Amazon VPC 是 Amazon EC2 的网络化阶层。 如果您是 Amazon EC2 的新用户，请参阅 What is Amazon EC2?以获取简要概述，该部分位于 *Amazon Elastic Compute Cloud User Guide* 中。

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。您可以在您的 VPC 内启动您的 AWS 资源，例如 Amazon EC2 实例。 您可以配置您的 VPC、选择 IP 地址范围、创建子网以及配置路由表、网络网关和安全设置。

*子网*是您的 VPC 内的 IP 地址范围。您可以在您选定的子网内启动 AWS 资源。使用必须连接 Internet 的资源的公用子网，以及无法连接到 Internet 的资源的私有子网。

如需保护您在每个子网中的 AWS 资源，您可以使用多安全层，包括安全组和访问控制列表 (ACL)。 有关更多信息，请参见 您的 VPC 安全性 (p. 57)。

支持平台

有两个支持平台可供你启动您的实例： EC2-Classic 和 EC2-VPC。有关更多信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Supported Platforms部分。

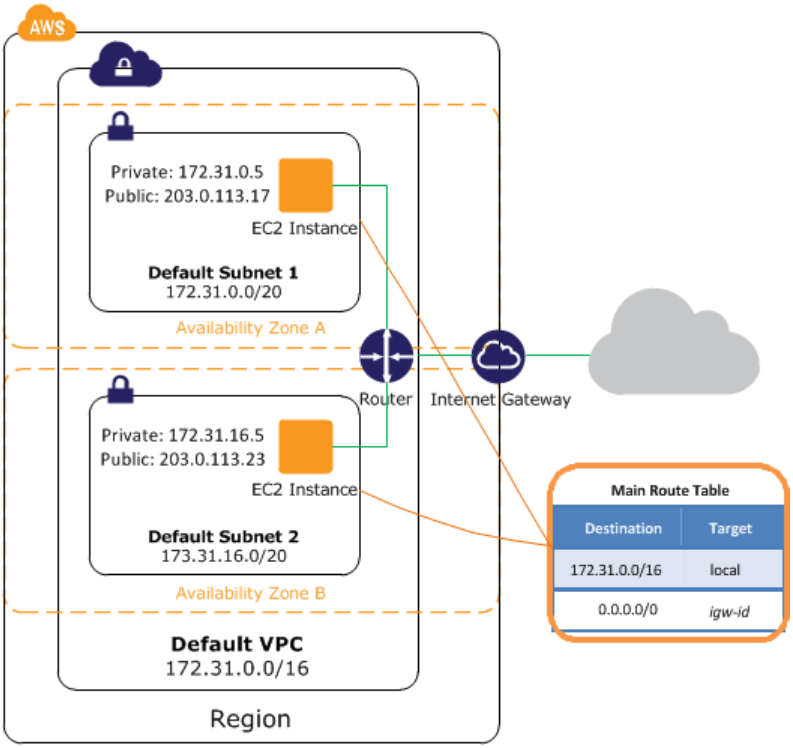
默认 VPC 将 EC2-VPC 提供的高级网络化功能优势与 EC2-Classic 的易于使用性结合在一起。 If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.

有关更多信息，请参见 您的默认 VPC 和子网 (p. 51)。

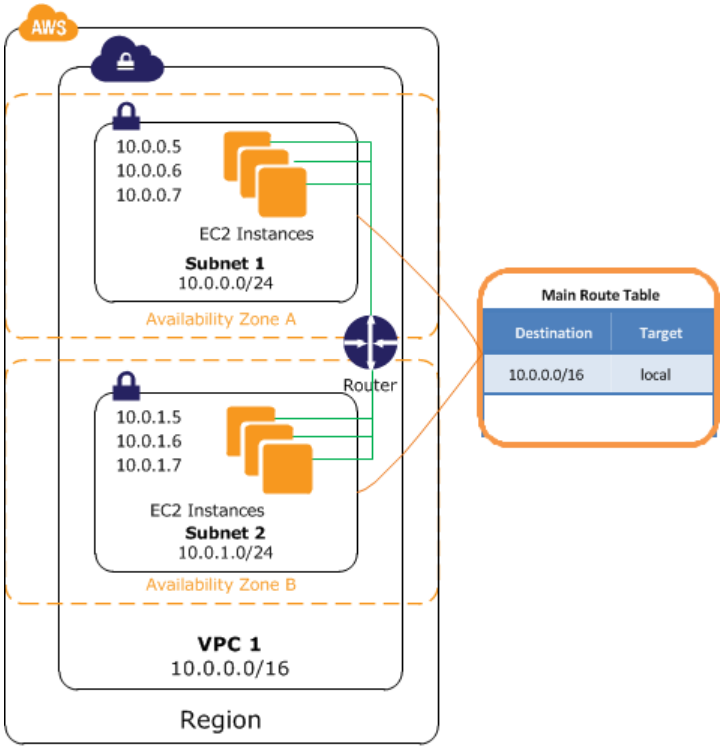
正在访问 Internet

您可以控制在 VPC 之外的 VPC 访问资源中启动实例的方式。

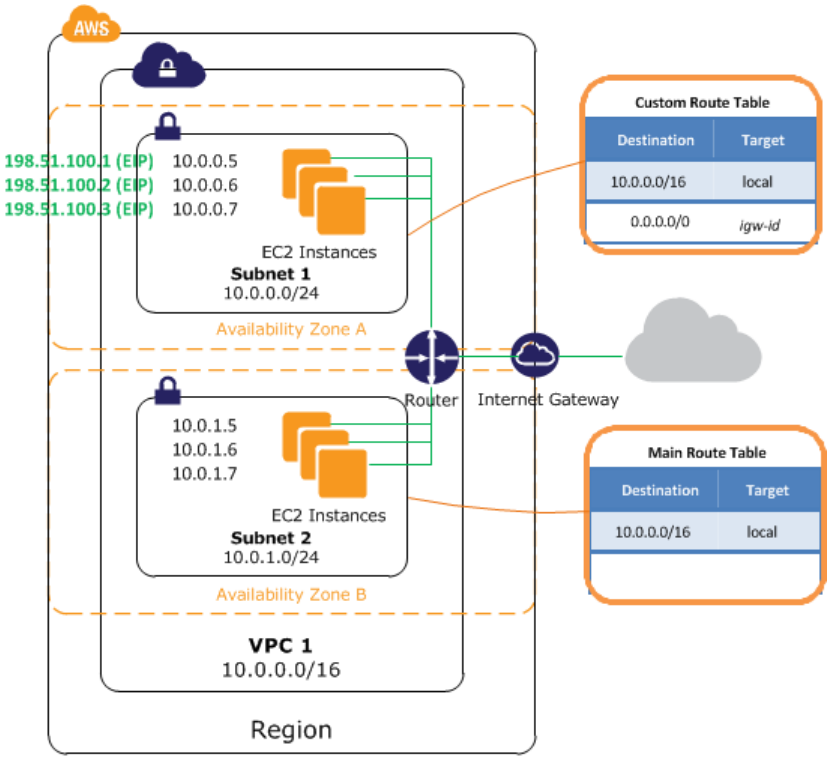
您在默认子网中启动的每项实例都有一个私有 IP 地址和一个公有 IP 地址。这些实例可以通过 Internet 网关与 Internet 通信。Internet 网关允许您的实例通过 Amazon EC2 网络边界连接 Internet。您的默认 VPC 内包含一个 Internet 网关。



您在非默认子网中启动的每项实例都有一个私有 IP 地址，但没有公有 IP 地址。这些实例可以彼此通信，但是不可访问 Internet 或其他 AWS 产品，例如 Amazon Simple Storage Service (Amazon S3)。



您可以非默认子网中启动的实例启用 Internet 访问功能，步骤如下：将 Internet 网关与其 VPC 关联（如果其 VPC 不是默认 VPC），然后将弹性 IP 地址与该实例相关联。



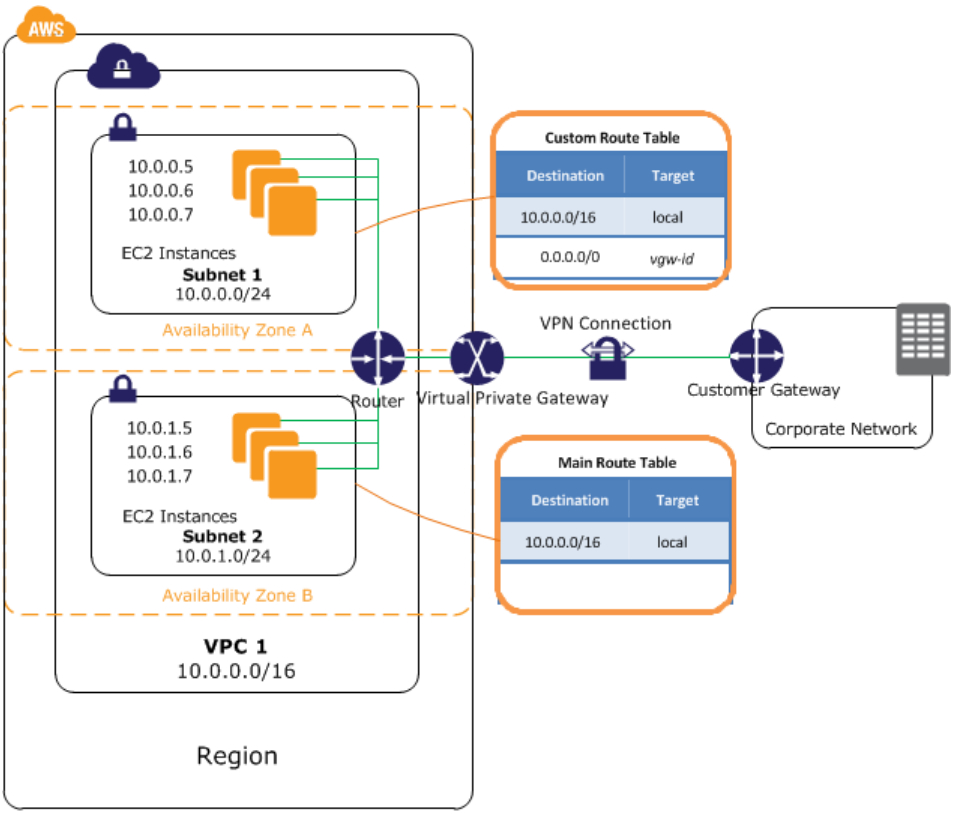
或者，您可以使用网络地址转换 (NAT) 实例，以允许 VPC 中的一项实例启动到 Internet 的出站连接，并阻止来自 Internet 的未经请求的入站连接。 NAT 会将多个私有 IP 地址映射到一个公有 IP 地址。NAT 实例有一个弹性 IP 地址，并通过 Internet 网关与 Internet 相连。 您可以通过 NAT 实例连接私有子网的实例和 Internet，它会将来自实例的数据流路由到 Internet 网关，并将响应路由到实例。

有关您 VPC 的路由和 NAT 的更多信息，请参见路由表 (p. 89)和NAT 实例 (p. 104)。

正在访问企业或家庭网络

您可以选择使用 IPsec 硬件 VPN 连接、并将 AWS 云设置为您的数据中心扩展，以将您的 VPC 与您自己的公司数据中心相连。

VPN 连接由附属在您的 VPC 上的 VPG 以及位于您的数据中心的客户网关组成。VPG 是在 VPN 连接的 Amazon 端的 VPN 集线器。 客户网关是在您的 VPN 连接端的实体设备或软件设备。



有关更多信息，请参见 在您的 VPC 中添加硬件虚拟专用网关 (p. 117)。

使用 Amazon VPC

AWS 提供多种使用 Amazon VPC 的方式：

- AWS 管理控制台
- 命令行接口
- API 操作

AWS 管理控制台

您可以使用 AWS 管理控制台来执行与 Amazon VPC 相关的任务，例如创建和删除 VPC、子网和网关。有关 Amazon VPC 控制台的更多信息，请参见Getting Started with Amazon VPC。

命令行接口

Amazon VPC 的命令行接口提供一系列使用 Java 运行环境的简单命令。Amazon VPC 命令是 Amazon EC2 API 工具接口的一部分。 有关命令行接口入门的更多信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Setting Up the Amazon EC2 Command Line Tools部分。有关 Amazon EC2 和 Amazon VPC 命令的更多信息，请参见*Amazon Elastic Compute Cloud Command Line Reference*的List of API Tools by Function部分。

API

Amazon VPC 操作是 Amazon EC2 WSDL 的一部分，Amazon VPC 使用 Amazon EC2 Web 服务终端节点。请求 Amazon VPC 身份验证；API 操作的运行方式与 Amazon EC2 API 操作的运行方式相同。有关如何使用 API 操作的更多信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Making API Requests部分。有关 Amazon EC2 和 Amazon VPC API 操作的更多信息，请参见*Amazon Elastic Compute Cloud API Reference*的List of Actions by Function部分。

Amazon VPC 的收费方式

您无需承担额外的 Amazon VPC 使用费用。您需要为您使用的实例和其他 Amazon EC2 功能支付标准费用。如果您选择创建硬件 VPN 连接，您需要按小时支付 VPN 与 VPC 的连接费用。有关更多信息，请参见Amazon VPC Pricing 和 Amazon EC2 Pricing。

Amazon VPC 限制

您可以提供的 Amazon VPC 组成部分数目有限。您可以请求提高这些限制。有关这些限制、以及如何申请提高限制的更多信息，请参见Amazon VPC 限制 (p. 135)。

接下来做什么？

如需获得有关 Amazon VPC 的实践介绍，完成教程Getting Started with Amazon VPC。

如需了解 Amazon VPC 的基本情景，请参见使用 Amazon VPC 情景 (p. 7)。您可以通过其他满足您的需求的方式配置您的 VPC 和子网。 有关其他情景的更多信息，请参见Amazon Virtual Private Cloud Connectivity Options。

如需了解与其他 AWS 产品一同使用 Amazon VPC 的信息，请参见以下文件。

产品	相关主题
Amazon EC2	Amazon EC2 和 Amazon VPC
Amazon RDS	Amazon RDS 和 Amazon VPC
Auto Scaling	在 Amazon VPC 中启动 Auto Scaling 实例

产品	相关主题
Elastic Load Balancing	在 Amazon VPC 内部署 ELB
Amazon EMR	在 Amazon VPC 中运行 EMR 作业流
Elastic Beanstalk	在 Amazon VPC 中使用 AWS Elastic Beanstalk

下表列出了在您使用此服务时可为您提供帮助的相关资源。

资源	描述
Amazon Virtual Private Cloud 连接性选项	提供对于网络连接性选项概览的白皮书。
AWS Developer Resources	A central starting point to find documentation, code samples, release notes, and other information to help you create innovative applications with AWS.
Amazon VPC Discussion Forum	A community-based forum for discussing technical questions related to Amazon VPC.
Amazon VPC Release Notes	A high-level overview of the current release.
AWS Support Center	The home page for AWS Support.
Contact Us	A central contact point for inquiries concerning AWS billing, accounts, and events.

使用 Amazon VPC 情景

此部分将描述使用 Amazon VPC 的基本情景。我们针对每个情景提供以下各项：

- 此表显示了基本组成部分
- 有关 VPC 和子网的信息
- 有关子网路由表的信息
- 有关推荐安全组规则的信息
- 实施情景的分步骤指示

下表描述了基本情景。

情景	用途
情景 1：仅带公有子网的 VPC (p. 7)	运行单层、面向公众使用的 Web 应用程序，例如博客或简单网站。
情景 2：带有公有子网和私有子网的 VPC (p. 13)	运行面向公众的 Web 应用程序，同时仍旧在第二个子网中保持非公开访问的后端服务器。
情景 3：带有公有和私有子网以及硬件 VPN 访问的 VPC (p. 24)	将您的数据中心扩展至云，并从您的 VPC 直接访问 Internet。
情景 4：仅带有私有子网和硬件 VPN 访问的 VPC (p. 35)	将您的数据中心扩展至云，无需将您的网络连接到 Internet 即可使用 Amazon 基础设备。

情景 1：仅带公有子网的 VPC

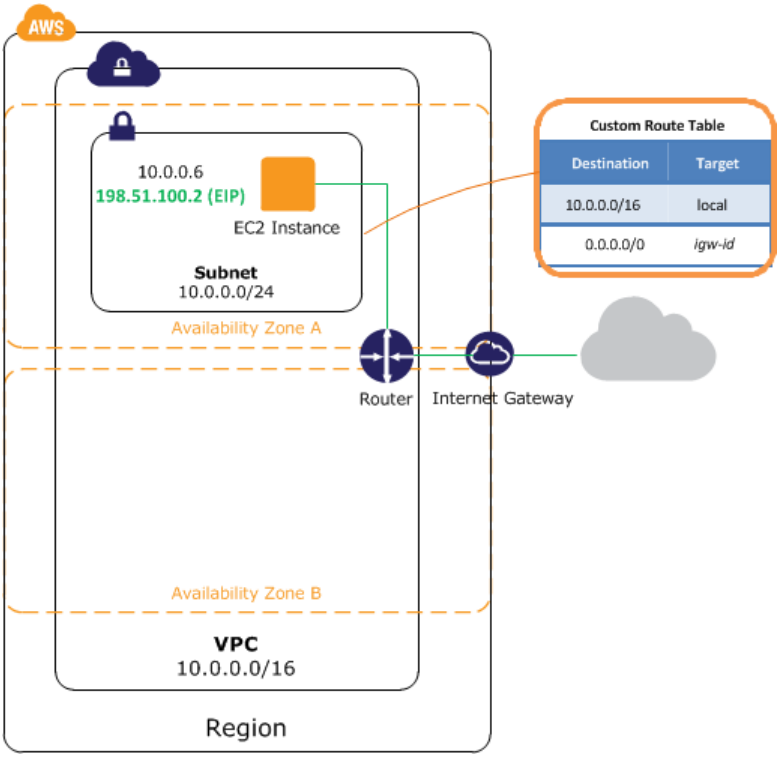
此情景的配置包含一个有单一公有子网的 Virtual Private Cloud (VPC)，以及一个 Internet 网关以启用 Internet 通信。如果您要运行单一层级且面向公众的 Web 应用程序，如博客或简单的网站，则我们建议您使用此配置。

Topics

- 情景 1 配置 (p. 36)
- 情景 1 的基本组成部分 (p. 36)
- 情景 1 路由 (p. 9)
- 情景安全性 1 (p. 9)

情景 1 配置

下表展示了此情景配置的主要组成部分。



Note

如果您已经完成了*Amazon Virtual Private Cloud Getting Started Guide*中的练习，然后您已经使用 Amazon VPC 控制台中的 VPC 向导实施过此情景。

情景 1 的基本组成部分

下表描述了在这个情景的配置图中呈现的基本组成部分：

- 大小为 /16 的 Virtual Private Cloud (VPC)（示例 CIDR：10.0.0.0/16）。提供 65,536 个私有 IP 地址。
- 大小为 /24的子网（示例 CIDR：10.0.0.0/24）。提供 256 个私有 IP 地址。
- Internet 网关。它可以将 VPC 与 Internet 以及其他 AWS 产品连接，例如 Amazon Simple Storage Service (Amazon S3)。
- 实例有处于子网范围之内（例如 10.0.0.6）的私有 IP 地址，这使实例可以与 VPC 中的其他实例建立通信；以及一个弹性 IP 地址（例如“198.51.100.2”），可允许实例连接 Internet。
- 允许子网中的实例与 VPC 中的其他实例通信的路由表条目；以及允许子网中的实例直接通过 Internet 建立通信的路由表条目。

有关子网的更多信息，请参见您的 VPC 和子网 (p. 44)和您的 VPC 中的 IP 地址 (p. 86)。有关 Internet 网关的更多信息，请参见在您的 VPC 中添加 Internet 网关 (p. 100)。

Tip

如果您希望在无需为每项实例分配弹性 IP 地址的情况下，使 VPC 中的实例可以通过 Internet 通信，您可以使用 NAT 实例。有关配置 NAT 实例的更多信息，请参见情景 2：带有公有子网和私有子网的 VPC (p. 13)或NAT 实例 (p. 104)。

情景 1 路由

您的 VPC 有隐藏路由器（显示在此情景的配置表中）。在这个情景中，VPC 向导创建路由表，以将所有目标为 VPC 外的地址的数据流路由到 Internet 网关，并将此路由表与子网关联。否则，您将需要自行创建和关联路由表。

下表显示了可在这个情景的配置表中使用的示例地址的路由表形式。第一行显示 VPC 中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间建立通信。第二行显示的条目可将所有其他子网数据流路由到 Internet 网关，即通过其 AWS 指定标识符分配的 Internet 网关。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-*xxxxxxxx*

情景安全性 1

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see 您的 VPC 安全性 (p. 57).

对于情景 1，您可以使用安全组而不是网络 ACL。有关安全组的更多信息，请参见您的 VPC 的安全组 (p. 58)。

推荐安全组规则

您的 VPC 会生成默认安全组，它的初始设置将拒绝所有入站数据流、允许所有出站数据流、以及允许在分配到您的安全组的实例间的所有数据流。如果您在启动实例时没有指定安全组，实例会自动分配到VPC 的默认安全组。我们可以修改默认安全组的规则，但是您的 Web 服务器需要的规则可能并不适用于您在 VPC 中启动的其他实例。因此，我们建议您创建一个安全组，以供您的公有子网 Web 服务器使用。

您将以`WebServerSG`作为名称创建一个安全组，添加您需要的规则，然后当您在 VPC 中启动实例时指定安全组。

下表描述了您应在 WebServerSG 组内添加的入站和出站规则。这些规则允许分配到这个安全组的实例接收 Internet 数据流，以及从您的网络接收 SSH 和 RDP 数据流。这些实例还可以启动到 Internet 的数据流。

入站			
源	协议	端口范围	注释

0.0.0.0/0	TCP	80	允许从任何地方对 Web 服务器进行入站 HTTP 访问
0.0.0.0/0	TCP	443	允许从任何地方对 Web 服务器进行入站 HTTPS 访问
您的网络的公有 IP 地址范围	TCP	22	（Linux 实例）允许来自您的网络的入站 SSH 访问
您的网络的公有 IP 地址范围	TCP	3389	（Windows 实例）允许来自您的网络的入站 RDP 访问
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许对 Internet 上的服务器进行出站 HTTP 访问（例如，软件更新）
0.0.0.0/0	TCP	443	允许对 Internet 上的服务器进行出站 HTTPS 访问（例如，软件更新）

VPC 的安全组带有默认规则，可自动允许指定实例在彼此之间建立通信。如需允许在您的子网 Web 服务器之间进行的此类通信，您必须在 WebServerSG 安全组内添加下列规则。

入站			
源	协议	端口范围	注释
WebServerSG	全部	全部	允许来自分配到 WebServerSG 的实例的入站数据流{
出站			
目的地	协议	端口范围	注释
WebServerSG	全部	全部	允许来自分配到 WebServerSG 的实例的出站数据流

实施情景 1

使用以下步骤以通过 VPC 向导实施情景。

Tip

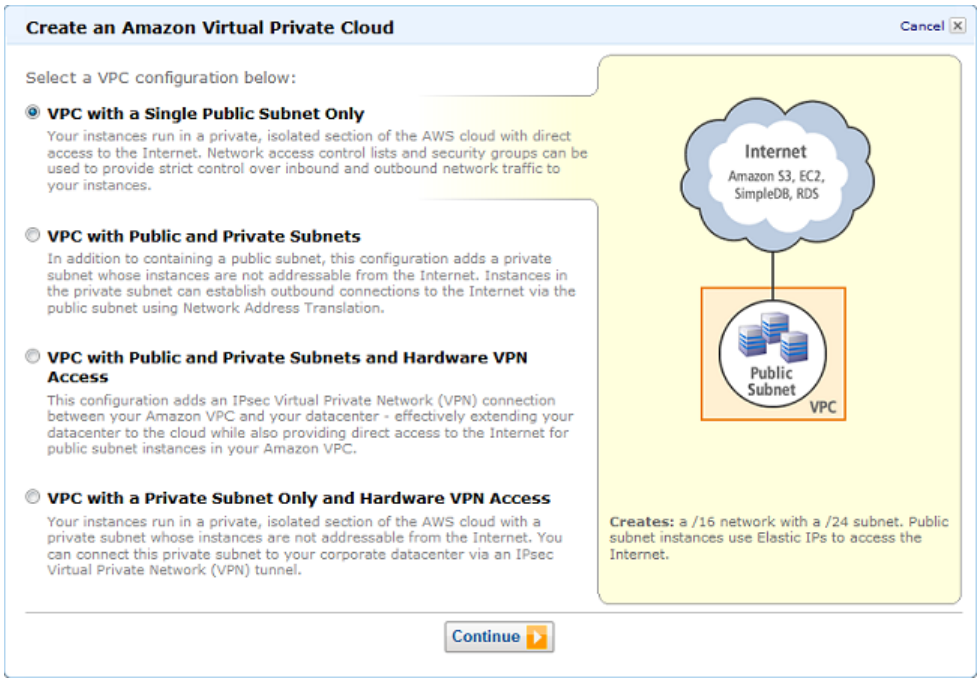
Amazon Virtual Private Cloud Getting Started Guide描述了相同的步骤，但会提供关于某些步骤的更多详细信息。

使用 VPC 向导实施情景 1

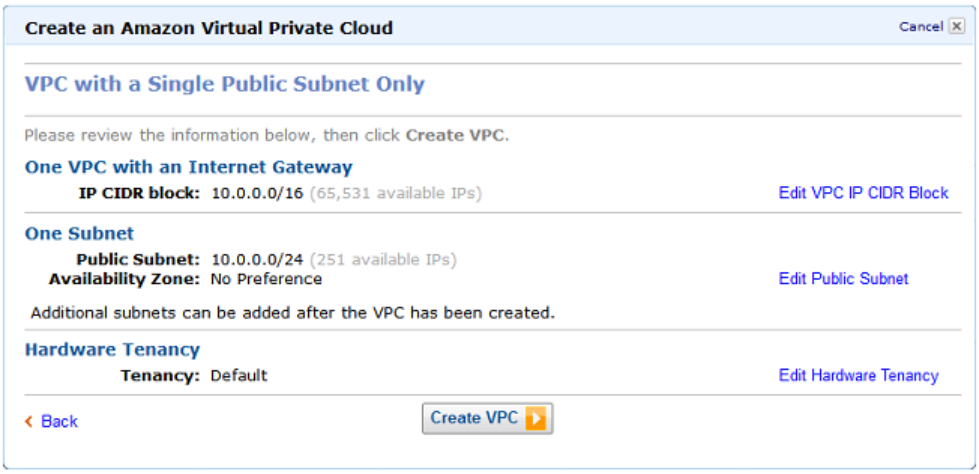
1. 设置 VPC、子网和 Internet 网关:
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. 单击导航窗格中的“VPC Dashboard”。

c. 查找控制面板的“Your Virtual Private Cloud”区域，单击“Get started creating a VPC”，如果您没有 VPC 资源，您也可以单击“Start VPC Wizard”。

d. 选择第一个选项“VPC with a Single Public Subnet Only”，并单击“Continue”。



e. 配置页面显示了您已经选择的 CIDR 范围和设置。对这些设置进行任何需要的更改，然后单击“Create VPC”以创建 VPC、子网、Internet 网关和路由表。



2. 创建 WebServerSG 安全组并添加规则：

a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

b. 单击导航窗格中的“Security Groups”。

c. 单击“Create Security Group”按钮。

d. 指定`WebServerSG`作为安全组名称，然后提供描述。从“VPC”菜单中选择您 VPC 的 ID，然后单击“Yes, Create”。

e. 选择您刚刚创建的 WebServerSG 安全组。详细信息窗格内会显示此安全组的信息，以及可供您使用入站规则和出站规则的选项卡。

f. 在Inbound选项卡中，进行以下操作：

- 从“Create a new rule”列表中选择HTTP，确保“Source”为0.0.0.0/0，然后单击“Add Rule”。
- 从“Create a new rule”列表中选择HTTPS，确保“Source”为0.0.0.0/0，然后单击“Add Rule”。
- 从“Create a new rule”列表中选择“SSH(Linux)” 或“RDP (Windows)” 。在“Source”方框中，指定您的网络的公用 IP 地址范围，然后单击“Add Rule”。
- 单击“Apply Rule Changes”以应用这些入站规则。

g. 在“Outbound”选项卡中，进行以下操作：

- 查找可以启用所有出站数据流的默认规则，然后单击“Delete”。
- 从“Create a new rule”列表中选择HTTP，确保“Destination”为0.0.0.0/0，然后单击“Add Rule”。
- 从“Create a new rule”列表中选择HTTPS，确保“Destination”为0.0.0.0/0，然后单击“Add Rule”。
- 单击“Apply Rule Changes”以应用这些出站规则。

3. 在 VPC 中启动实例：

a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

b. 在控制面板中单击“Launch Instance”按钮。

c. 在创建新实例页面中，选择“Quick Launch Wizard”，然后单击“Continue”。按照向导中的指示操作。为您的实例指定名称，选择密钥对，选择 AMI，然后单击“Continue”。

d. 单击“Edit Details”。在“Instance Details”项下，选择“Launch into a VPC”并指定一个子网。在“Security Settings”下，选择您在第 2 步中创建的 WebServerSG 安全组。

e. 单击“Save Details”。

f. 检视您已经选择的设置。根据需要进行更改，随后单击“Launch”。

4. 为实例分配弹性 IP 地址：

a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

b. 单击导航窗格中的“Elastic IPs”。

c. 单击“Allocate New Address”按钮。

d. 从“EIP used in”列表中，选择VPC并单击“Yes, Allocate”。

e. 从列表中选择弹性 IP 地址，然后单击“Associate Address”按钮。

f. 在“Associate Address”对话框中，选择要与地址关联的实例，然后单击“Yes, Associate”。

现在您可以连接您的 VPC 中的实例。有关如何连接 Linux 实例的信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Connect to Your Linux Instance部分。有关如何连接 Windows 实例的信息，请参见*Amazon Elastic Compute Cloud Microsoft Windows Guide*中的Connect to Your Windows Instance部分。

情景 2：带有公有子网和私有子网的 VPC

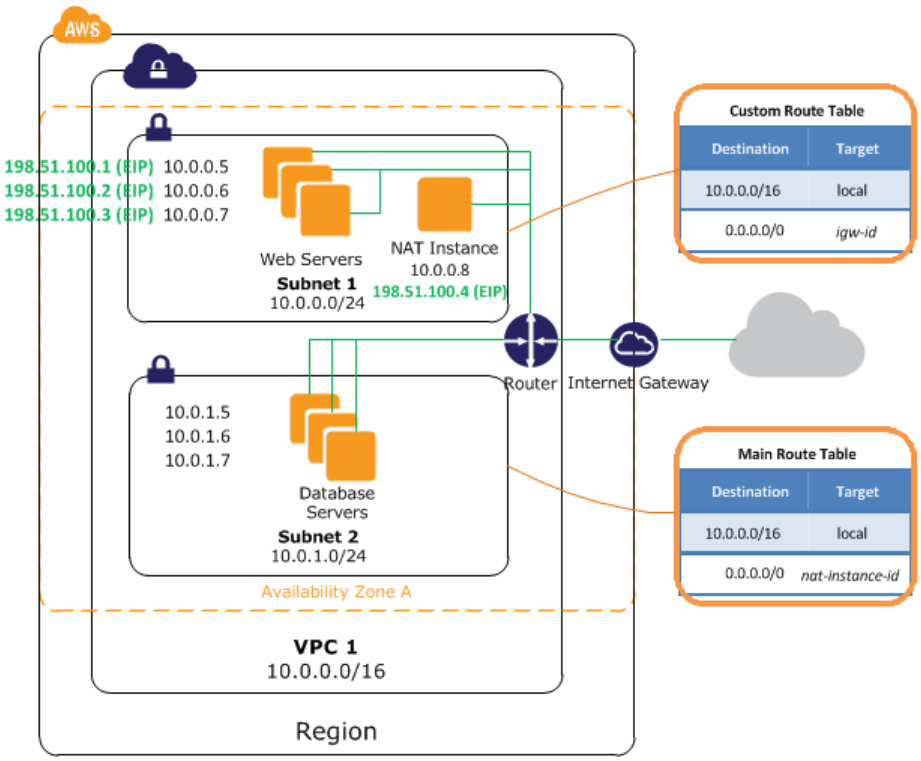
这个情景的配置包括一个有公有子网和私有子网的 Virtual Private Cloud (VPC)。如果您希望运行面向公众的 Web 应用程序，并同时保留不可公开访问的后端服务器，我们建议您使用此情景。常用例子是一个多层网站，其 Web 服务器位于公有子网之内，数据库服务器则位于私有子网之内。您可以设置安全性和路由，以使 Web 服务器能够与数据库服务器建立通信。

公有子网中的实例可以直接从 Internet 接收入站数据流，私有子网中的实例则不可。公有子网中的实例可以直接向 Internet 发送出站数据流，私有子网中的实例则不可。但是，私有子网中的实例可以使用您在公有子网中启动的网络地址转换 (NAT) 实例访问 Internet。

Topics

情景 2 配置

下表展示了此情景配置的主要组成部分。



Important

在这个情景中，Amazon Virtual Private Cloud Network Administrator Guide描述了您的网络管理员需要完成的任务，以配置在您的 VPN 连接端的 Amazon VPC 客户网关。

情景 2 的基本组成部分

下表描述了在这个情景的配置图中呈现的基本组成部分：

- 大小为 /16 的 Virtual Private Cloud (VPC)（示例 CIDR：10.0.0.0/16）。提供 65,536 个私有 IP 地址。
- 大小为 /24 的公有子网（示例 CIDR：10.0.0.0/24）。提供 256 个私有 IP 地址。
- 大小为 /24 的私有子网（示例 CIDR：10.0.1.0/24）。提供 256 个私有 IP 地址。
- Internet 网关。它可以将 VPC 与 Internet 以及其他 AWS 产品连接，例如 Amazon Simple Storage Service (Amazon S3)。
- 实例有处于子网范围之内（例如 10.0.0.5、10.0.1.5）的私有 IP 地址，这使它们可以在彼此之间以及与 VPC 中的其他实例建立通信。公有子网中的实例还有弹性 IP 地址（例如198.51.100.1），这些弹性 IP 地址允许它们连接 Internet。私有子网中的实例是后端服务器，它们不需要接收来自 Internet 的传入数据流；但是，它们可以使用 NAT 实例向 Internet 发送请求（请参阅下一个重点内容）。
- 有自己的弹性 IP 地址的网络地址转换 (NAT) 实例。这将允许私有子网中的实例向 Internet 发送请求（例如软件更新）。
- 与公有子网关联的自定义路由表。此路由表中包含一项条目允许子网中的实例与 VPC 中的其他实例建立通信，另一项条目则允许子网中的实例直接与 Internet 建立通信。
- 与私有子网关联的主路由表。路由表中包含允许子网中的实例与 VPC 中的其他实例通信的条目；以及允许子网中的实例直接与您的网络通信的条目。

有关子网的更多信息，请参见您的 VPC 和子网 (p. 44)和您的 VPC 中的 IP 地址 (p. 86)。有关 Internet 网关的更多信息，请参见在您的 VPC 中添加 Internet 网关 (p. 100)。有关 NAT 的更多信息，请参见NAT 实例 (p. 104)。

Tip

如果您希望帮助管理私有子网中的实例，您可以在公有子网中设置防御服务器，以作为代理服务器使用。例如，您可以在公有子网中设置 SSH 端口转发器或 RDP 网关，以代理从您自己的网络流向数据库服务器的数据流。

情景 2 路由

您的 VPC 有一个隐藏路由器（显示在此情景的配置图中）。在这个情景中，VPC 向导更新了使用私有子网的主路由表，并创建了一个自定义路由表并将其与公有子网关联。否则，您将需要自行创建和关联路由表。

在这个情景中，从每个子网前往 AWS（例如，到 Amazon EC2 或 Amazon S3 终端节点）的所有数据流都会经过 Internet 网关。私有子网中的数据库服务器无法直接接收来自 Internet 的数据流，因为它们没有弹性 IP 地址。但是，数据库服务器可以通过公有子网中的 NAT 实例发送和接收 Internet 数据流。

任何您使用默认主路由表创建的额外子网，也就是默认的私有子网。如果您希望将子网设置为公有子网，您可以随时更改与其相关的路由表。

下表描述了此情景的路由表。

主路由表

第一行描述 VPC 中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间进行通信。 第二行描述的条目可将所有其他子网数据流发送到 NAT 实例，即通过其 AWS 指定标识符分配的 NAT 实例（例如，网络接口`eni-1a2b3c4d`和实例`i-1a2b3c4d`）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	eni-*xxxxxxxx* / i-*xxxxxxxx*

自定义路由表

第一行描述 VPC 中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间建立通信。第二行描述的条目可通过 Internet 网关将所有其他子网数据流路由到 Internet，即通过其 AWS 指定标识符分配的 Internet 网关（例如igw-1a2b3d4d）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-*xxxxxxxx*

情景 2 安全性

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see 您的 VPC 安全性 (p. 57).

在情景 2 中，您可以使用安全组而不是网络 ACL。有关安全组的更多信息，请参见您的 VPC 的安全组 (p. 58)。

推荐安全组

您的 VPC 会生成一个默认安全组，其初始规则会拒绝所有入站数据流、允许所有出站数据流以及允许所有在组内实例之间交换的数据流。如果您在启动实例时未指定安全组，实例将自动关联到默认安全组。如果您需要分配实例，以便从 VPC 外部接收数据流，您必须更改默认安全组的规则。

在这个情景中，我们建议您创建以下安全组，而不是使用默认安全组：

- WebServerSG – 适用于公有子网中的 Web 服务器
- NATSG – 适用于公有子网中的 NAT 实例
- DBServerSG – 适用于私有子网中的数据库服务器

分配到同一个安全组的实例可以位于不同的子网之中。 但是，在这个情景中，每个安全组都对应一项实例承担的角色类型，每个角色则要求实例处于特定的子网内。因此，在这个情景中，所有分配到一个安全组的实例都位于相同的子网之中。

即使部分实例被分配到相同的安全组中（例如 Web 服务器被分配到 WebServerSG），它们仍无法在彼此之间进行通信。只有默认安全组中才包含允许不同实例彼此间通信的规则（默认规则）。如需允许在归属于相同的安全组的实例之间进行的此类通信，除了推荐规则之外，您还必须在每个安全组内添加下列规则。

入站

源	协议	端口范围	注释
安全组 ID	全部	全部	允许来自分配到此安全组的其他实例的入站数据流
出站			
目的地	协议	端口范围	注释
安全组 ID	全部	全部	允许来自分配到此安全组的其他实例的出站数据流

创建 WebServerSG、NATSG 和 DBServerSG 安全组

创建 WebServerSG、NATSG 和 DBServerSG 安全组

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 单击“Create Security Group” 按钮。
4. 在“Create Security Group”对话框中，指定`WebServerSG`作为安全组的名称，并提供描述。从“VPC”列表中选择您 VPC 的 ID，然后单击“Yes, Create”。
5. 再次单击“Create Security Group”按钮 。
6. 在“Create Security Group”对话框中，指定`NATSG`作为安全组的名称，并提供描述。从“VPC”列表中选择您 VPC 的 ID，然后单击“Yes, Create”。
7. 再次单击“Create Security Group”按钮 。
8. 在“Create Security Group”对话框中，指定`DBServerSG`作为安全组的名称，并提供描述。从“VPC”列表中选择您 VPC 的 ID，然后单击“Yes, Create”。

下一部分将描述每个安全组的推荐规则，并为您展示如何添加这些规则。

向 WebServerSG 安全组中添加规则

WebServerSG 安全组是指当您在公有子网中启动 Web 服务器时指定的安全组。 下表描述了此安全组的推荐规则，这些规则允许 Web 服务器接收 Internet 数据流，以及来自您的网络的 SSH 和 RDP 数据流。Web 服务器也可以启动到 Internet 的数据流，以及读取和写入发送至私有子网的数据库服务器的请求。

WebServerSG：推荐规则

入站			
源	协议	端口范围	注释
`0.0.0.0/0`	TCP	80	允许从任何地方对 Web 服务器进行入站 HTTP 访问
`0.0.0.0/0`	TCP	443	允许从任何地方对 Web 服务器进行入站 HTTPS 访问
您网络的公有 IP 地址范围	TCP	22	允许从您的网络对 Linux 实例进行入站 SSH 访问（通过 Internet 网关）
您网络的公有 IP 地址范围	TCP	3389	允许从您的网络对 Windows 实例进行入站 RDP 访问（通过 Internet 网关）

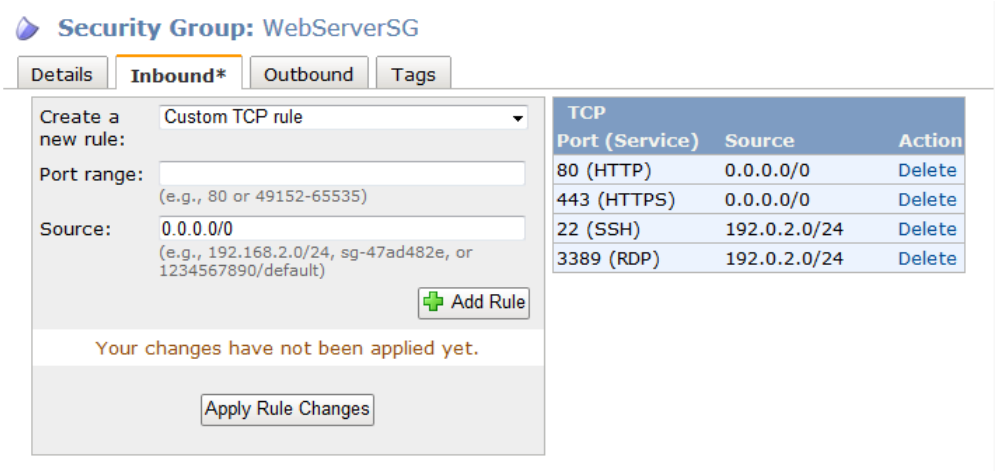
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许 Web 服务器启动对 Internet 的出站 HTTP 访问（例如软件更新）
0.0.0.0/0	TCP	443	允许 Web 服务器启动对 Internet 的出站 HTTPS 访问（例如软件更新）
您的 DBServerSG 安全组 ID	TCP	1433	允许对分配到 DBServerSG 的数据库服务器进行出站 Microsoft SQL Server 访问
您的 DBServerSG 安全组 ID	TCP	3306	允许对归属于 DBServerSG 的数据库服务器进行出站 MySQL 访问

Note

组内包括 SSH 和 RDP 访问，以及 Microsoft SQL Server 和 MySQL 访问。根据您的情况，您可能仅需要 Linux（SSH 和 MySQL）或 Windows（RDP 和 Microsoft SQL Server）规则。

向 WebServerSG 安全组中添加规则

1. 选择您刚刚创建的 WebServerSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
2. 如下所示使用“Inbound”选项卡添加入站数据流规则：
   a. 从“HTTPCreate a new rule”列表中选择 。确保“Source”一项为0.0.0.0/0，然后单击“Add Rule”。请注意“Apply Rules Changes”按钮已经启用，并且显示出“Your changes have not been applied yet”文本。在您添加了所有您需要的入站数据流规则之后，您可以单击“Apply Rule Changes”以添加这些规则。
   b. 从“HTTPSCreate a new rule”列表中选择 。确保“Source”一项为0.0.0.0/0，然后单击“Add Rule”。
   c. 从“SSHCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围（在这个例子中使用的是192.0.2.0/24），然后单击“Add Rule”。
   d. 从“RDPCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围，然后单击“Add Rule”。
   e. 单击“Apply Rule Changes”。



3. 如下所示使用“Outbound”选项卡添加出站数据流规则：

   a. 查找可以所有出站规则的默认规则，然后单击“Delete”。

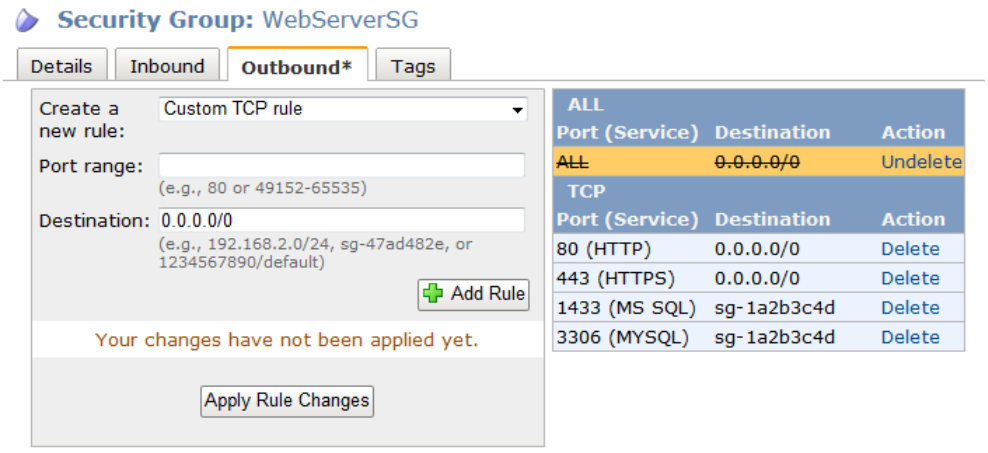
   b. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。

   c. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。

   d. 从“MS SQLCreate a new rule”列表中选择 。在“Destination”方框中，指定 DBServerSG 安全组的 ID，然后单击“Add Rule”。

   e. 从“MySQLCreate a new rule”列表中选择 。在“Destination”方框中，指定 DBServerSG 安全组的 ID，然后单击“Add Rule”。

   f. 单击“Apply Rule Changes”。



向 NATSG 安全组中添加规则

NATSG 安全组是指当您在公有子网中启动 NAT 实例时将指定的安全组。下表描述了此安全组的推荐规则，这些规则允许 NAT 实例从私有子网中的实例接收 Internet 绑定数据流，以及来自您的网络的 SSH 数据流。NAT 实例也可以向 Internet 发送数据流，因此私有子网中的实例便可以接收软件更新。

NATSG：推荐规则

入站			
源	协议	端口范围	注释
10.0.1.0/24	TCP	80	允许来自私有子网的数据库服务器的入站 HTTP 数据流
10.0.1.0/24	TCP	443	允许来自私有子网的数据库服务器的入站 HTTPS 数据流
您网络的公有 IP 地址范围	TCP	22	允许从您的网络对 NAT 实例进行入站 SSH 访问（通过 Internet 网关）
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许对 Internet 进行出站 HTTP 访问（通过 Internet 网关）
0.0.0.0/0	TCP	443	允许对 Internet 进行出站 HTTPS 访问（通过 Internet 网关）

向 NATSG 安全组中添加推荐规则

1. 选择您刚刚创建的 NATSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
2. 如下所示使用“Inbound”选项卡添加入站数据流规则：

a. 从“HTTPCreate a new rule”列表中选择 。在“Source”方框中，指定您的私有子网的 IP 地址范围，然后单击“Add Rule”。
b. 从“HTTPSCreate a new rule”列表中选择 。在“Source”方框中，指定您的私有子网的 IP 地址范围，然后单击“Add Rule”。
c. 从“SSHCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围，然后单击“Add Rule”。
d. 单击“Apply Rule Changes”。

3. 如下所示使用“Outbound”选项卡添加出站数据流规则：

a. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
b. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
c. 单击“Apply Rule Changes”。

向 DBServerSG 安全组中添加规则

DBServerSG 安全组是指当您在您的私有子网中启动数据库服务器时将指定的安全组。 下表描述了此安全组的推荐规则，即允许从 Web 服务器读取或写入数据库请求。数据库服务器还可以启动绑定到 Internet 的数据流（您的路由表将数据流发送到 NAT 实例，NAT 实例随后通过 Internet 网关将其转发至 Internet）。

DBServerSG：推荐规则

入站			
源	协议	端口范围	注释
您的 WebServerSG 安全组 ID	TCP	1433	允许分配到 WebServerSG Microsoft SQL Server 的 Web 服务器访问分配到 DBServerSG 的数据库服务器
您的 WebServerSG 安全组 ID	TCP	3306	允许分配到 WebServerSG MySQL 的 Web 服务器访问分配到 DBServerSG 的数据库服务器
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许对 Internet 进行出站 HTTP 访问（例如，软件更新）
0.0.0.0/0	TCP	443	允许对 Internet 进行出站 HTTPS 访问（例如，软件更新）

在 DBServerSG 安全组中添加推荐规则

1. 选择您刚刚创建的 DBServerSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
2. 如下所示使用“Inbound”选项卡添加入站数据流规则：

a. 从“MS SQLCreate a new rule”列表中选择 。在“Source”方框中，指定您的 WebServerSG 安全组的 ID，然后单击“Add Rule”。
b. 从“MYSQLCreate a new rule”列表中选择 。在“Source”方框中，指定您的 WebServerSG 安全组的 ID，然后单击“Add Rule”。
c. 单击“Apply Rule Changes”。

3. 如下所示使用“Outbound”选项卡添加出站数据流规则：

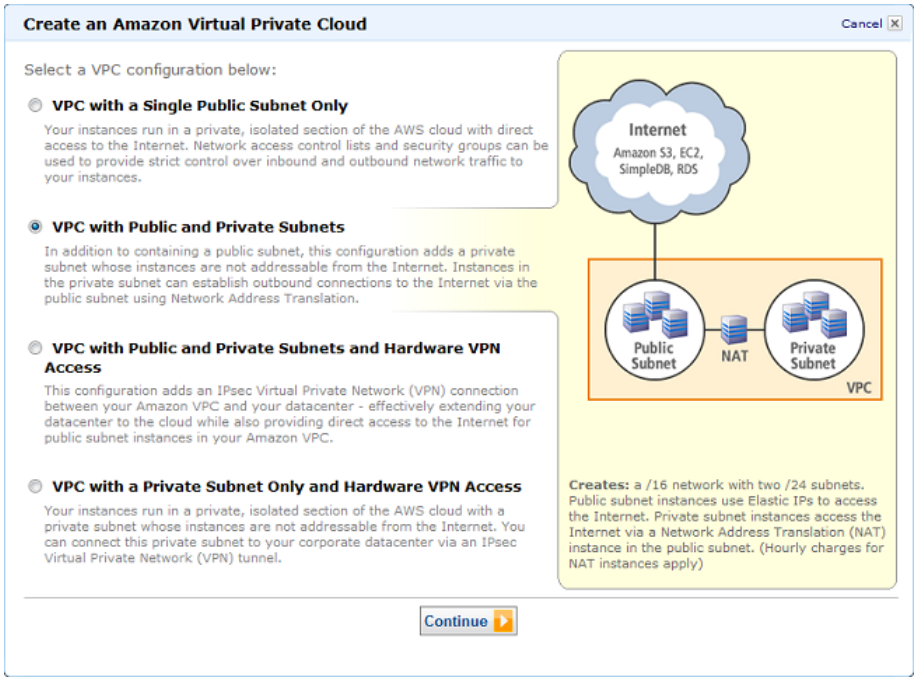
a. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
b. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
c. 单击“Apply Rule Changes”。

实施情景 2

使用以下步骤以通过 VPC 向导实施情景 2。

使用 VPC 向导实施情景 2

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“VPC Dashboard”。
3. 查找控制面板的“Your Virtual Private Cloud”区域，单击“Get started creating a VPC”，如果您没有 VPC 资源，您也可以单击“Start VPC Wizard”。
4. 选择第二个选项 – “VPC with Public and Private Subnets”，然后单击“Continue”。

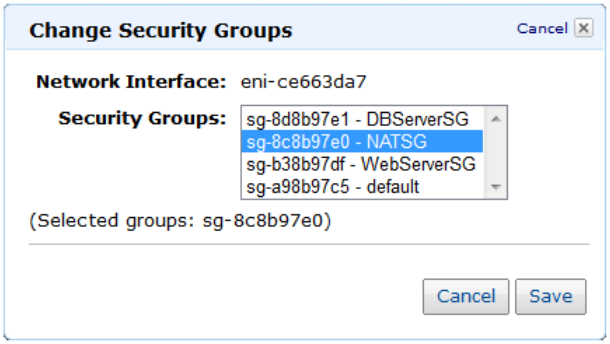


5. 验证配置页面中的信息。根据您的需要进行修改，然后单击“Create VPC”以创建您的 VPC、子网、Internet 网关和路由表，并在公有子网内启动 NAT 实例。

当 VPC 向导启动 NAT 实例时，它会在 VPC 内使用默认安全组。相反的是，您需要将 NAT 实例与 NATSG 安全组关联。

更改 NAT 实例的安全组

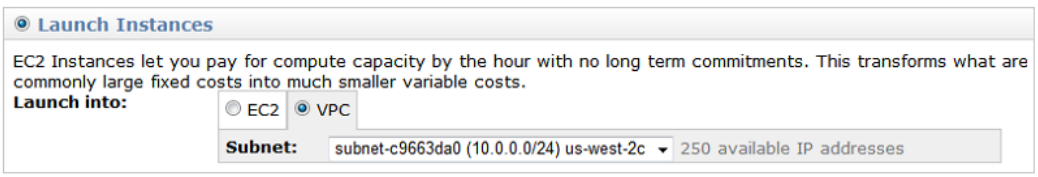
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 单击导航窗格中的“Network Interfaces”。
3. 从列表中选择 NAT 实例的网络接口，然后从“Actions”列表中选择“Change Security Groups”。
4. 在“Change Security Groups”对话框中，从“Security Groups”列表中选择您创建的 NATSG 安全组（参阅情景 2 安全性 (p. 15)），然后单击“Save”。



您可以在您的 VPC 内启动实例。如果您已经熟悉了在 VPC 外启动实例的流程，您便已经大概了解应如何在 VPC 内启动实例。

启动实例

1. 如果您尚未创建 WebServerSG 和 DBServerSG 安全组，现在创建 WebServerSG 和 DBServerSG 安全组（参见情景 2 安全性 (p. 15)）。您应在启动实例时指定以下一个安全组。
2. 启动 Classic 向导：
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 单击控制面板中的“Launch Instance”按钮。
   c. 在创建新实例页面中，选择“Classic Wizard”，然后单击“Continue”。
3. 在选择 AMI页面中，“Quick Start”选项卡显示了名称为“亚马逊系统映像”(AMI)的基本配置列表。选择您要使用的 AMI，然后单击它的“Select”按钮。
4. 在实例详细信息页面中，在“Launch Instances”项下，选择需要启动实例的子网。保留此页面中的其他默认设置，并单击“Continue”。



5. 如需使用接下来的INSTANCE DETAILS页面中描述的默认设置，您只需单击每页的“Continue”即可。
6. 在CREATE A KEY PAIR页面中，您可以从您已经创建的现有密钥对中进行选择，或者根据向导的指示创建新的密钥对。

7. 在Configure Firewall页面中，选择您希望用于实例的安全组（WebServerSG 或 DBServerSG），然后单击Continue。
8. 检视您的设置。如果您的选择无误之后，单击“Launch”。

您必须先指定一个弹性 IP 地址，然后才能够访问公有子网中的实例。

To allocate an Elastic IP address and assign it to an instance

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

现在您可以连接您的 VPC 中的实例。有关如何连接 Linux 实例的信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Connect to Your Linux Instance部分。有关如何连接 Windows 实例的信息，请参见*Amazon Elastic Compute Cloud Microsoft Windows Guide*中的Connect to Your Windows Instance部分。

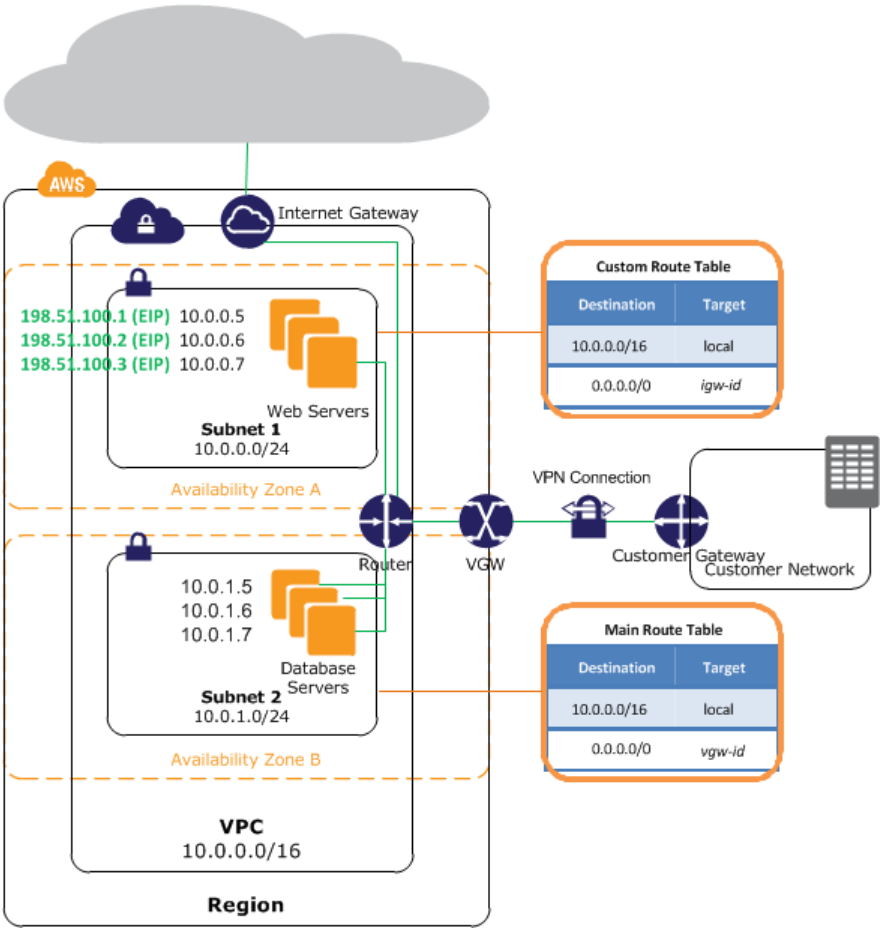
情景 3：带有公有和私有子网以及硬件 VPN 访问的 VPC

此情景的配置包括一个包含公有子网和私有子网的 Virtual Private Cloud (VPC)，以及一个虚拟专用网关，以允许您自己的网络可以通过 IPsec VPN 隧道进行通信。如果您想将您的网络扩展到云并且直接从您的 VPC 访问 Internet，则我们建议您采用此方案。在此情景中，您可以在公有子网中运行有可扩展 Web 前端的多层应用程序，还能够将您的数据储存在通过 IPsec VPN 连接与您的网络相连的私有子网中。

Topics

情景 3 配置

下表展示了此情景配置的主要组成部分。



Important

在这个情景中，*Amazon Virtual Private Cloud Network Administrator Guide描述了您的网络管理员需要完成的任务，以配置在您这端的 VPN 连接的 Amazon VPC 客户网关。*

情景 3 的基本配置

下表描述了在这个情景的配置图中呈现的基本组成部分：

- 大小为 /16 的 Virtual Private Cloud (VPC)（示例 CIDR：10.0.0.0/16）。提供 65,536 个私有 IP 地址。
- 大小为 /24 的公有子网（示例 CIDR：10.0.0.0/24）。提供 256 个私有 IP 地址。
- 大小为 /24 的仅限 VPN 是子网（示例 CIDR：10.0.1.0/24）。提供 256 个私有 IP 地址。
- Internet 网关。它可以将 VPC 与 Internet 以及其他 AWS 产品连接，例如 Amazon Simple Storage Service (Amazon S3)。
- 在您的 VPC 和网络之间的 VPN 连接。VPN 连接由位于 VPN 连接的 Amazon 一端的虚拟专用网关、以及位于您的一端的客户网关组成。
- 有私有 IP 地址的实例，这些 IP 地址处于子网范围之内（例如 10.0.0.5 和 10.0.1.5），它们允许实例在彼此之间、以及和 VPC 中的其他实例建立通信。公有子网中的实例还有弹性 IP 地址（例如 198.51.100.1”），这些弹性 IP 地址允许它们连接 Internet。在仅限 VPN 的子网中的实例是后端服务器，它们不需要从 Internet 接收传入数据流，但是可以从您的网络发送和接受数据流。
- 与公有子网关联的自定义路由表。此路由表中包含一项条目允许子网中的实例与 VPC 中的其他实例建立通信，另一项条目则允许子网中的实例直接与 Internet 建立通信。
- 与仅限 VPN 的子网关联的主路由表。路由表中包含允许子网中的实例与 VPC 中的其他实例通信的条目；以及允许子网中的实例直接与您的网络通信的条目。

有关子网的更多信息，请参见您的 VPC 和子网 (p. 44)和您的 VPC 中的 IP 地址 (p. 86)。有关 Internet 网关的更多信息，请参见在您的 VPC 中添加 Internet 网关 (p. 100)。有关您的 VPN 连接的更多信息，请参见在您的 VPC 中添加硬件虚拟专用网关 (p. 117)。有关配置客户网关的更多信息，请参见*Amazon Virtual Private Cloud Network Administrator Guide*。

情景 3 路由

您的 VPC 有一个隐藏路由器（显示在此情景的配置图中）。在这个情景中，VPC 向导更新了在仅限 VPN 的子网中使用的主路由表，并创建了一个自定义路由表并将其关联到公有子网。否则，您将需要自行创建和关联路由表。

仅限 VPN 的子网中的实例无法直接连接 Internet；所有 Internet 绑定的数据流必须首先通过虚拟专用网关到达您的网络，随后数据流会接受您的防火墙和公司安全策略检测。如果实例发送任何 AWS 绑定数据流（例如，请求 Amazon S3 或 Amazon EC2 API），则请求必须经过虚拟专用网关通向您的网络，并在到达 AWS 之前进入 Internet 。

Tip

任何来自您的网络、前往公有子网中实例的弹性 IP 地址的数据流量都会流经 Internet，而不是流经虚拟专用网关。您也可以设置路由和安全组规则，以允许来自您的网络的数据流可通过虚拟专用网关到达公有子网。

VPN 可被配置为静态路由 VPN 连接或动态路由 VPN 连接（使用 BGP）。 如果您选择静态路由，您将收到提示，要求您在创建 VPN 连接时手动输入您的网络的 IP 前缀。如果您选择动态路由，IP 前缀会使用 BGP，自动发布到您的 VPC 的虚拟专用网关。

下表描述了此情景的路由表。

主路由表

第一行描述 VPC 中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间进行通信。 第二行描述的条目可通过虚拟专用网关将来自私有子网的所有其他子网数据流路由到您的网络，即通过其 AWS 指定标识符分配的虚拟专用网关（例如`vgw-1a2b3c4d`）。

目的地	目标
`10.0.0.0/16`	本地
`0.0.0.0/0`	`vgw-`*`xxxxxxxx`*

自定义路由表

第一行描述 VPC 中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间进行通信。 第二行描述的条目可通过 Internet 网关将来自公有子网的所有其他子网数据流路由到 Internet，即通过其 AWS 指定标识符分配的 Internet 网关（例如`igw-1a2b3c4d`）。

目的地	目标
`10.0.0.0/16`	本地
`0.0.0.0/0`	`igw-`*`xxxxxxxx`*

替代路由

或者，如果您希望私有子网的实例可以访问 Internet，您可以设置路由，以使子网的 Internet 绑定数据流能够通向公有子网中的网络地址转换 (NAT) 实例。NAT 实例允许仅限 VPN 的子网通过 Internet 网关发送请求（例如软件更新）。 如需允许私有子网的 Internet 绑定数据流到达 NAT 实例，您必须对主路由表进行如下更新。

主路由表

第一行描述 VPC 中的本地路由条目。第二行描述的条目可将通往您的网络的子网数据流路由到虚拟专用网关，即通过其 AWS 指定标识符分配的虚拟专用网关（例如`vgw-1a2b3c4d`）。第三行将所有其他子网数据流发送到 NAT 实例，即通过其 AWS 指定标识符分配的 NAT 实例（例如`i-1a2b3c4d`）。

目的地	目标
`10.0.0.0/16`	本地
`172.16.0.0/12`	`vgw-`*`xxxxxxxx`*
`0.0.0.0/0`	`i-`*`xxxxxxxx`*

有关手动设置 NAT 实例的信息，请参见NAT 实例 (p. 104)。有关使用 VPC 向导以设置 NAT 实例的信息，请参见情景 2：带有公有子网和私有子网的 VPC (p. 13)。

情景 3 的安全性

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone

can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see 您的 VPC 安全性 (p. 57).

在情景 3 中，您可以使用安全组而不是网络 ACL。有关安全组的更多信息，请参见您的 VPC 的安全组 (p. 58)。

Topics

推荐安全组

您的 VPC 会生成默认安全组，它的初始设置将拒绝所有入站数据流、允许所有出站数据流、以及允许在分配到您的安全组的实例间的所有数据流。如果您在启动实例时未指定安全组，实例将自动关联到默认安全组。如果您需要分配实例，以便从 VPC 外部接收数据流，您必须更改默认安全组的规则。

在这个情景中，我们建议您创建以下安全组，而不是使用默认安全组：

- WebServerSG – 适用于公有子网中的 Web 服务器。
- DBServerSG – 适用于仅限 VPN 的子网中的数据库服务器

分配到同一个安全组的实例可以位于不同的子网之中。 但是，在这个情景中，每个安全组都对应一项实例承担的角色类型，每个角色则要求实例处于特定的子网内。因此，在这个情景中，所有分配到一个安全组的实例都位于相同的子网之中。

即使部分实例被分配到相同的安全组中（例如 Web 服务器被分配到 WebServerSG），它们仍无法在彼此之间进行通信。只有默认安全组中才包含允许不同实例彼此间通信的规则（默认规则）。如需允许在归属于相同的安全组的实例之间进行的此类通信，除了推荐规则之外，您还必须在每个安全组内添加下列规则。

入站			
源	协议	端口范围	注释
安全组 ID	全部	全部	允许来自分配到此安全组的其他实例的入站数据流
出站			
目的地	协议	端口范围	注释
安全组 ID	全部	全部	允许来自分配到此安全组的其他实例的出站数据流

正在创建 WebServerSG 和 DBServerSG 安全组

创建 WebServerSG 和 DBServerSG 安全组

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。

3. 单击“Create Security Group” 按钮。
4. 在“Create Security Group”对话框中，指定`WebServerSG`作为安全组的名称，并提供描述。从“VPC”列表中选择您 VPC 的 ID，然后单击“Yes, Create”。
5. 再次单击“Create Security Group”按钮 。
6. 在“Create Security Group”对话框中，指定`DBServerSG`作为安全组的名称，并提供描述。从“VPC”列表中选择您 VPC 的 ID，然后单击“Yes, Create”。

下一部分将描述每个安全组的推荐规则，并为您展示如何添加这些规则。

向 WebServerSG 安全组中添加规则

WebServerSG 安全组是指当您在公有子网中启动 Web 服务器时指定的安全组。 下表描述了此安全组的推荐规则，这些规则允许 Web 服务器接收 Internet 数据流，以及来自您的网络的 SSH 和 RDP 数据流。Web 服务器也可以启动到 Internet 的数据流，以及读写通向仅限 VPN 的子网中的数据库服务器的请求。

WebServerSG：推荐规则

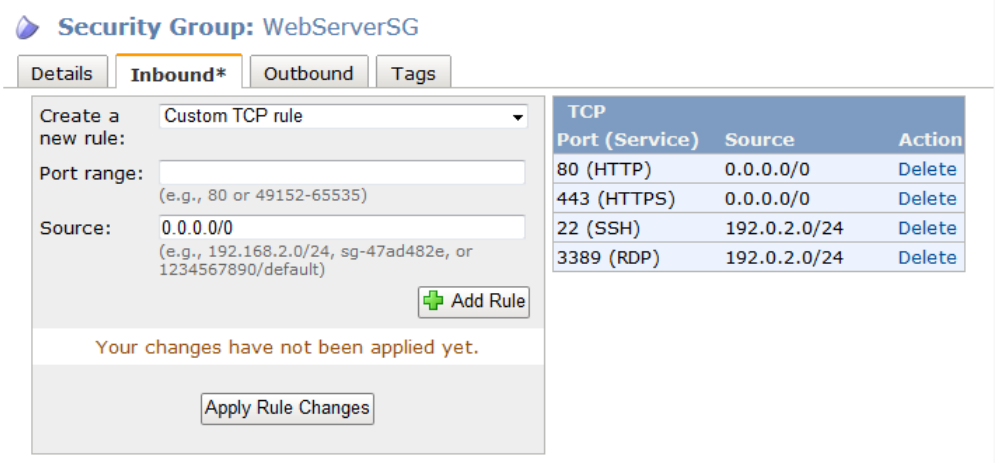
入站			
源	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许从任何地方对 Web 服务器进行入站 HTTP 访问
0.0.0.0/0	TCP	443	允许从任何地方对 Web 服务器进行入站 HTTPS 访问
您网络的公有 IP 地址范围	TCP	22	允许从您的网络对 Linux 实例进行入站 SSH 访问（通过 Internet 网关）
您网络的公有 IP 地址范围	TCP	3389	允许从您的网络对 Windows 实例进行入站 RDP 访问（通过 Internet 网关）
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许 Web 服务器启动对 Internet 的出站 HTTP 访问（例如软件更新）
0.0.0.0/0	TCP	443	允许 Web 服务器启动对 Internet 的出站 HTTPS 访问（例如软件更新）
您的 DBServerSG 安全组 ID	TCP	1433	允许对分配到 DBServerSG 的数据库服务器进行出站 Microsoft SQL Server 访问
您的 DBServerSG 安全组 ID	TCP	3306	允许对归属于 DBServerSG 的数据库服务器进行出站 MySQL 访问

Note

组内包括 SSH 和 RDP 访问，以及 Microsoft SQL Server 和 MySQL 访问。根据您的情况，您可能仅需要 Linux（SSH 和 MySQL）或 Windows（RDP 和 Microsoft SQL Server）规则。

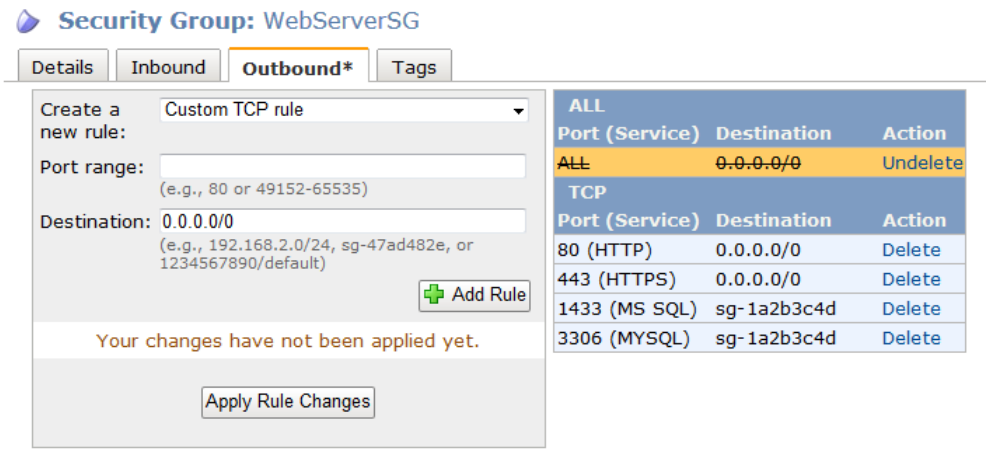
在 WebServerSG 安全组中添加推荐规则

1. 选择您刚刚创建的 WebServerSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
2. 如下所示使用“Inbound”选项卡添加入站数据流规则：
   a. 从“HTTPCreate a new rule”列表中选择 。确保“Source”一项为`0.0.0.0/0`，然后单击“Add Rule”。请注意“Apply Rules Changes”按钮已经启用，并且显示出“Your changes have not been applied yet”文本。在您添加了所有您需要的入站数据流规则之后，您可以单击“Apply Rule Changes”以添加这些规则。
   b. 从“HTTPSCreate a new rule”列表中选择 。确保“Source”一项为`0.0.0.0/0`，然后单击“Add Rule”。
   c. 从“SSHCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围（这个例子使用的是 192.0.2.0/24），然后单击Add Rule。
   d. 从“RDPCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围，然后单击“Add Rule”。
   e. 单击“Apply Rule Changes”。



3. 如下所示使用“Outbound”选项卡添加出站数据流规则：
   a. 查找可以所有出站规则的默认规则，然后单击“Delete”。

b. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
c. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
d. 从“MS SQLCreate a new rule”列表中选择 。在“Destination”方框中，指定 DBServerSG 安全组的 ID，然后单击“Add Rule”。
e. 从“MySQLCreate a new rule”列表中选择 。在“Destination”方框中，指定 DBServerSG 安全组的 ID，然后单击“Add Rule”。
f. 单击“Apply Rule Changes”。



向 DBServerSG 安全组中添加规则

DBServerSG 安全组是指当您在仅限 VPN 连接的子网中启动数据库服务器时指定的安全组。下表描述了此安全组的推荐规则，这些规则允许 Microsoft SQL Server 和 MySQL 读取和书写 Web 服务器请求以及来自您的网络的 RDP 数据流。 数据库服务器也可以启动通往 Internet 的数据流（您的路由表会通过虚拟专用网关发送数据流）。

DBServerSG：推荐规则

入站			
源	协议	端口范围	注释
您的 WebServerSG 安全组 ID	TCP	1433	允许分配到 WebServerSG Microsoft SQL Server 的 Web 服务器访问分配到 DBServerSG 的数据库服务器
您的 WebServerSG 安全组 ID	TCP	3306	允许分配到 WebServerSG MySQL 的 Web 服务器访问分配到 DBServerSG 的数据库服务器
您网络的公有 IP 地址范围	TCP	22	允许从您的网络到 Linux 实例的入站 SSH 数据流（通过虚拟专用网关）
您网络的公有 IP 地址范围	TCP	3389	允许从您的网络对 Windows 实例进行入站 RDP 访问（通过虚拟专用网关）

出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许通过虚拟专用网关对 Internet 进行出站 HTTP 访问（例如软件更新）
0.0.0.0/0	TCP	443	允许通过虚拟专用网关对 Internet 进行出站 HTTPS 访问（例如软件更新）

在 DBServerSG 安全组中添加推荐规则

1. 选择您刚刚创建的 DBServerSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
2. 如下所示使用“Inbound”选项卡添加入站数据流规则：
   a. 从“SSHCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的 IP 地址范围，然后单击“Add Rule”。
   b. 从“RDPCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的 IP 地址范围，然后单击“Add Rule”。
   c. 从“MS SQLCreate a new rule”列表中选择 。在“Source”方框中，指定您的 WebServerSG 安全组的 ID，然后单击“Add Rule”。
   d. 从“MYSQLCreate a new rule”列表中选择 。在“Source”方框中，指定您的 WebServerSG 安全组的 ID，然后单击“Add Rule”。
   e. 单击“Apply Rule Changes”。
3. 如下所示使用“Outbound”选项卡添加出站数据流规则：
   a. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
   b. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
   c. 单击“Apply Rule Changes”。

正在实施情景 3

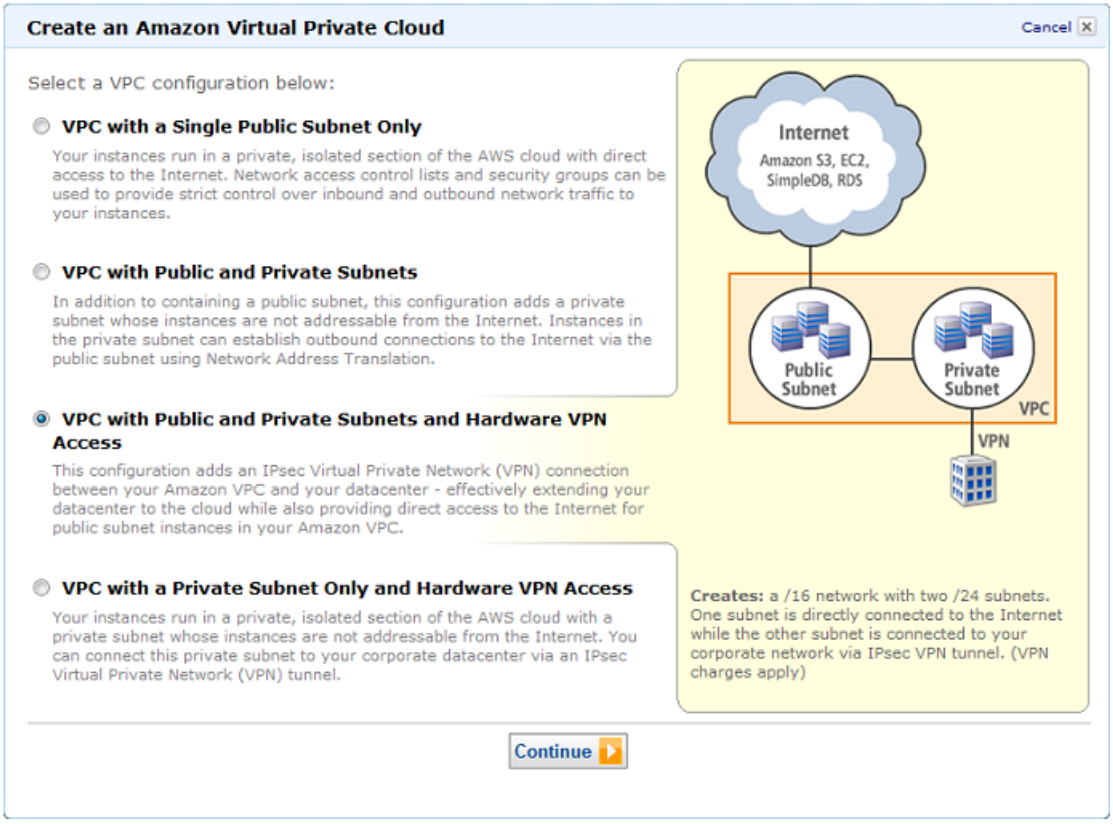
按照以下步骤，使用 VPC 向导实施情景 3。

准备您的客户网关

1. 正在确定将作为您的客户网关使用的设备。有关我们已经测试过的设备的更多信息，请参见Amazon Virtual Private Cloud 常见问题。有关对您的客户网关的要求的更多信息，请参见Amazon Virtual Private Cloud Network Administrator Guide。
2. 为客户网关的外部接口获取 Internet 可路由的 IP 地址。地址必须为静态，并且不可属于任何执行网络地址转换 (NAT) 任务的设备。
3. 收集应通过 VPN 连接传播到虚拟专用网关的内部 IP 范围列表（在 CIDR 符号内）（如果您使用的是静态路由 VPN 连接）。有关更多信息，请参见 VPN 路由选项 (p. 119)。

使用 VPC 向导实施情景 3

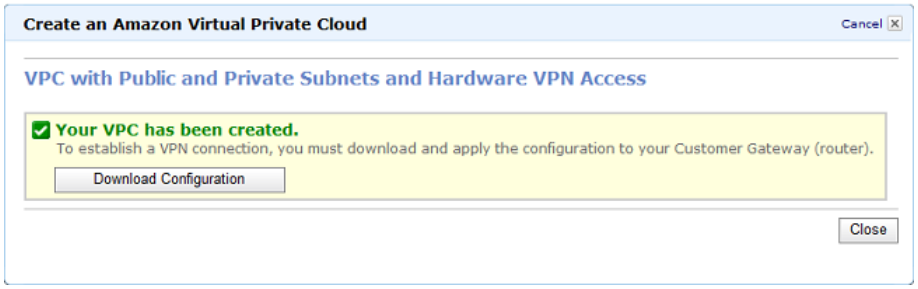
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“VPC Dashboard”。
3. 查找控制面板的“Your Virtual Private Cloud”区域，然后单击“Get started creating a VPC”，如果您没有 VPC 资源，您也可以单击“Start VPC Wizard”。
4. 选择第三个选项 – “VPC with Public and Private Subnets and Hardware VPN Access”– 然后单击“Continue”。



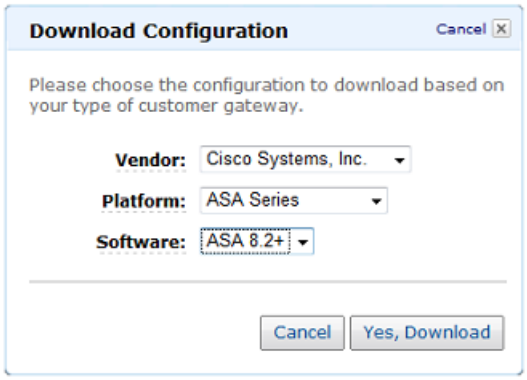
5. 在“Create an Amazon Virtual Private Cloud”对话框中，执行以下操作，然后单击“Continue”：
   - 在“IP Address”中，指定您的 VPN 路由器的公有 IP 地址。
   - 在“Specify the routing for the VPN Connection”中，从以下路由选项中选择一项：
     - 如果您的 VPN 路由器支持边界网关协议 (BGP)，选择“Use dynamic routing (requires BGP)”。
     - 如果您的 VPN 路由器不支持 BGP，单击“Use static routing”。在“IP Prefix”中，添加您的网络的每项 IP 前缀。

   有关适用选项的更多信息，请参见Amazon Virtual Private Cloud 常见问题。有关动态与静态路由的更多信息，请参见VPN 路由选项 (p. 119)。

6. 验证配置页面中的信息。根据您的需要进行更改，然后单击“Create VPC”以创建 VPC、子网、路由表、Internet 网关和 VPN 连接。
7. 在您关闭向导之后，屏幕中会显示一个确认对话框和一个下载按钮，以供您下载您的客户网关的配置。单击“Download Configuration”。



8. 在“Download Configuration”对话框中，选择客户网关、平台和软件版本的供应商，然后单击“Yes, Download”。

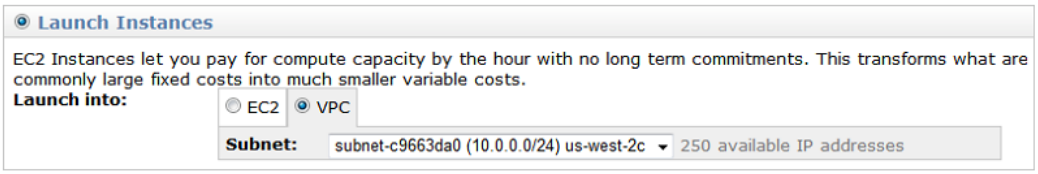


9. 保存包含 VPN 配置的文本文件，并连同本指南Amazon Virtual Private Cloud Network Administrator Guide一起将其提供给网络管理员。在网络管理员完成客户网关配置之前，VPN 将无法使用。

在您的网络管理员完成您的客户网关配置之后，您可以在您的 VPC 内启动实例。如果您已经熟悉了在 VPC 外启动实例的流程，您便已经大概了解应如何在 VPC 内启动实例。

启动实例

1. 如果您尚未创建 WebServerSG 和 DBServerSG 安全组，现在创建 WebServerSG 和 DBServerSG 安全组（参见情景 3 的安全性 (p. 26)）。您应在启动实例时指定以下一个安全组。
2. 启动 Classic 向导：
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 单击控制面板中的“Launch Instance”按钮。
   c. 在创建新实例页面中，选择“Classic Wizard”，然后单击“Continue”。
3. 在选择 AMI页面中，“Quick Start”选项卡显示了名称为“亚马逊系统映像”(AMI)的基本配置列表。选择您要使用的 AMI，然后单击它的“Select”按钮。
4. 在实例详细信息页面中，在“Launch Instances”项下，选择需要启动实例的子网。保留此页面中的其他默认设置，并单击“Continue”。



5. 如需使用接下来的实例详细信息页面中描述的默认设置，您只需单击每页的“Continue”即可。
6. 在CREATE A KEY PAIR页面中，您可以从您已经创建的现有密钥对中进行选择，或者根据向导的指示创建新的密钥对。
7. 在Configure Firewall页面中，选择您希望用于实例的安全组（WebServerSG 或 DBServerSG），然后单击Continue。
8. 检视您的设置。在您确认选择无误之后，单击“Launch”。

对于在仅限 VPN 的子网中运行的实例，您可以从您的网络对其进行检测，以测试实例的连接性。有关更多信息，请参阅 测试实例的端至端连接 (p. 124)。

您必须先指定一个弹性 IP 地址，然后才能够访问公有子网中的实例。

To allocate an Elastic IP address and assign it to an instance

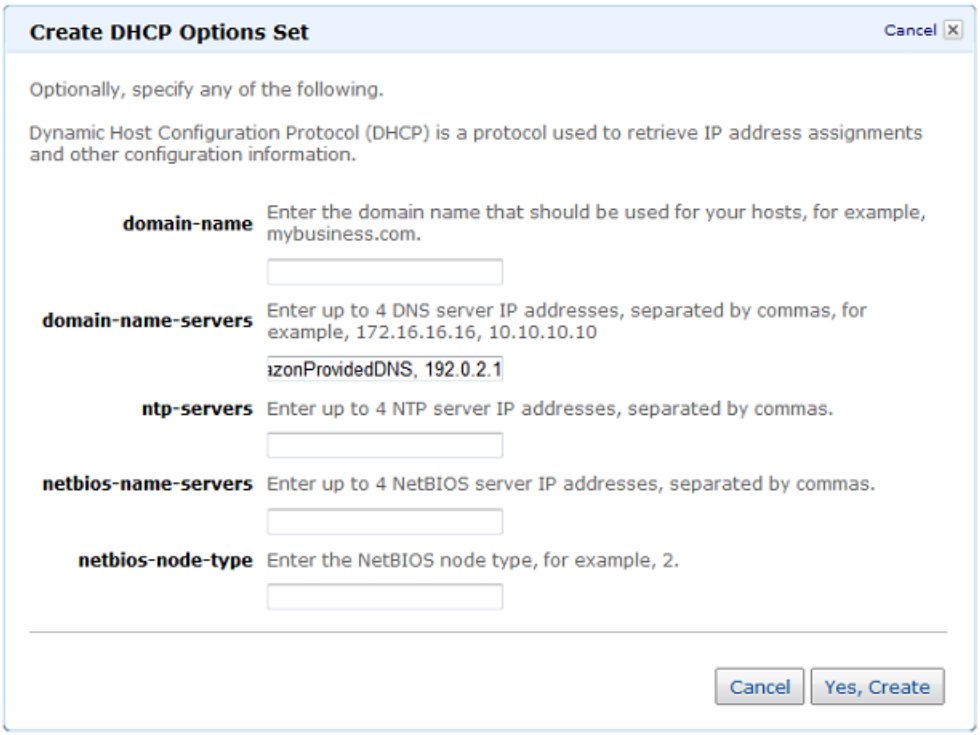
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

在情景 3 中，您需要一个 DNS 服务器以允许您的公有子网与 Internet 中的服务器通信，您还需要另一个 DNS 服务器，以允许您的仅限 VPN 的子网与您的网络中的服务器进行通信。

您的 VPC 会自动生成有 domain-name-servers=AmazonProvidedDNS 的 DHCP 选项集。这是 Amazon 提供的 DNS 服务器，以帮助您启动 VPC 中的公有子网，从而通过 Internet 网关与 Internet 通信。您必须提供您自己的 DNS 服务器，并将其添加至您的 VPC 使用的 DNS 服务器列表中。DHCP 选项集不可更改，因此您必须创建包含您的 DNS 服务器和 Amazon DNS 服务器的 DHCP 选项集，您必须更新 VPC，方可使用新建的 DHCP 选项集。

更新 DHCP 选项

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“DHCP Options Sets”。
3. 单击“Create DHCP Options Set”按钮。
4. 在“Create DHCP Options Set”对话框中，在“domain-name-servers”方框中指定 Amazon DNS 服务器 (AmazonProvidedDNS) 的地址以及您的 DNS 服务器的地址，以逗号隔开，然后单击“Create”。在这个例子中，您的 DNS 服务器是 192.0.2.1。



5. 单击导航窗格中的“Your VPCs”。
6. 选择 VPC，然后单击“Change DHCP Options Set”按钮。
7. 在“Change DHCP Options Set”对话框中，从列表中选择新的选项集 ID，然后单击“Yes, Change”。
8. （可选）VPC 现在使用新建的 DHCP 选项集，并因此可以访问两个 DNS 服务器。 如果您需要，您可以删除 VPC 使用的初始选项集。

现在您可以连接您的 VPC 中的实例。有关如何连接 Linux 实例的信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Connect to Your Linux Instance部分。有关如何连接 Windows 实例的信息，请参见*Amazon Elastic Compute Cloud Microsoft Windows Guide*中的Connect to Your Windows Instance部分。

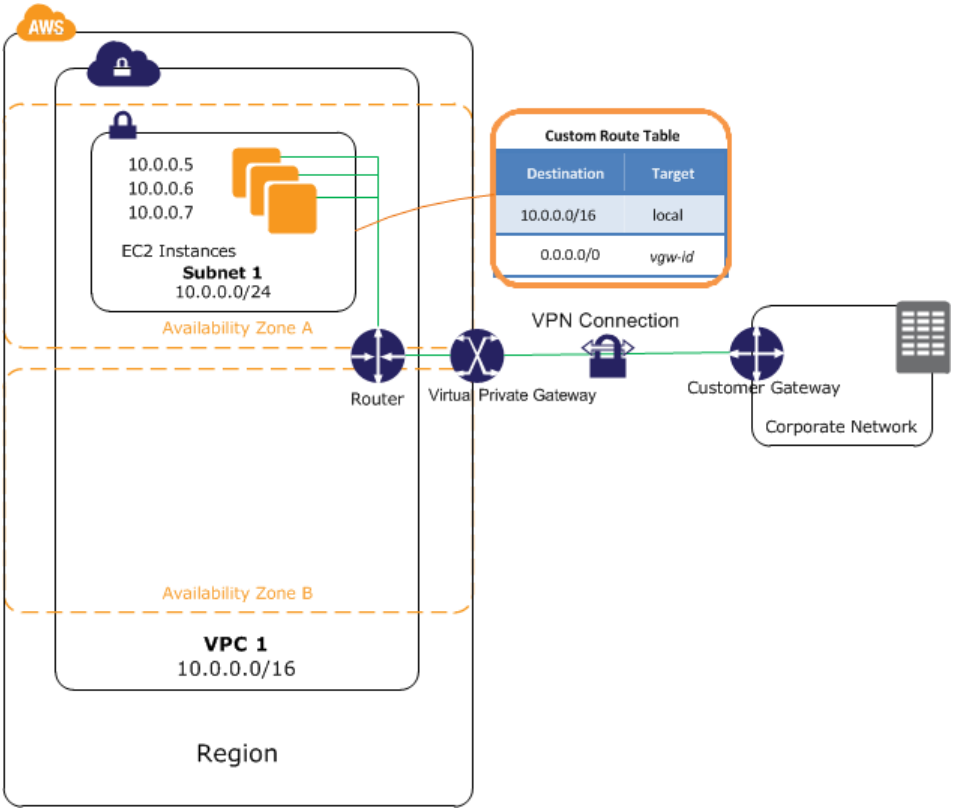
情景 4：仅带有私有子网和硬件 VPN 访问的 VPC

此情景的配置包括一个有单一私有子网的 Virtual Private Cloud (VPC)，以及一个虚拟专用网关，以允许您自己的网络可以通过 IPsec VPN 隧道进行通信。没有 Internet 网关可进行 Internet 通信。如果您希望利用 Amazon 的基础设施将您的网络扩展到云，并且不将您的网络公开到 Internet，我们建议您采用此情景。

Topics

情景 4 配置

下表展示了此情景配置的主要组成部分。



Important

在这个情景中，*Amazon Virtual Private Cloud Network Administrator Guide*描述了您的网络管理员需要完成的任务，以便在您的 VPN 连接一端配置 Amazon VPC 客户网关。

情景 4 的基础组成部分

下表描述了在这个情景的配置图中呈现的基本组成部分：

- 大小为 /16 的 Virtual Private Cloud (VPC)（示例 CIDR：10.0.0.0/16）。提供 65,536 个私有 IP 地址。
- 大小为 /24 的仅限 VPN 子网（示例 CIDR：10.0.0.0/24）。提供 256 个私有 IP 地址。
- 在您的 VPC 和网络之间的 VPN 连接。VPN 连接由位于 VPN 连接的 Amazon 一端的虚拟专用网关、以及位于您的一端的客户网关组成。

- 有私有 IP 地址的实例处于子网范围之内（例如 10.0.0.5、10.0.0.6 和 10.0.0.7），这使它们可以在彼此之间以及与 VPC 中的其他实例建立通信。
- 允许子网中的实例与其他 VPC 中的实例通信的路由表条目；以及允许子网中的实例与您的网络直接建立通信的路由表条目。

有关子网的更多信息，请参见您的 VPC 和子网 (p. 44)和您的 VPC 中的 IP 地址 (p. 86)。有关您的 VPN 连接的更多信息，请参见在您的 VPC 中添加硬件虚拟专用网关 (p. 117)。有关配置客户网关的更多信息，请参阅 *Amazon Virtual Private Cloud Network Administrator Guide*。

情景 4 路由

您的 VPC 有隐藏路由器（显示在此情景的配置图中）。在这个情景中，VPC 向导创建路由表，以将所有目标为 VPC 外的地址的数据流路由到 VPN 连接，并将此路由表与子网关联。否则，您将需要自行创建和关联路由表。

下表显示了可在这个情景的配置表中使用的示例地址的路由表形式。第一行描述VPC中的本地路由条目；这项条目允许 VPC 中的实例在彼此之间建立通信。第二行描述的条目可将所有其他子网数据流路由到虚拟专用网关，即通过其 AWS 指定标识符分配的虚拟专用网关（例如`vgw-1a2b3c4d`）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	vgw-*xxxxxxxx*

VPN 连接可被配置为静态路由 VPN 连接或动态路由 VPN 连接（使用 BGP）。如果您选择静态路由，您将收到提示，要求您在创建 VPN 连接时手动输入您的网络的 IP 前缀。如果您选择动态路由，IP 前缀会通过 BGP 自动传播到您的 VPC。

在您的 VPC 中的实例无法直接连接 Internet；Internet 绑定的数据流必须首先经过虚拟专用网关到达您的网络，在您的网络中，数据流会接受您的防火墙和公司安全策略的检测。如果实例发送任何 AWS 绑定数据流（例如对 Amazon S3 或 Amazon EC2 的请求），则请求必须经过虚拟专用网关通向您的网络，并在最终到达 AWS 之前流经 Internet。

情景 4 安全性

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see 您的 VPC 安全性 (p. 57).

在情景 4 中，您将在 VPC 中使用默认安全组。

推荐安全组规则

您的 VPC 会生成一个默认安全组，其初始规则会拒绝所有入站数据流、允许所有出站数据流以及允许所有在安全组内实例之间交换的数据流。我们建议您更改默认安全组的规则，以仅允许来自您的网络的入站 SSH 数据流 (Linux) 和远程桌面数据流 (Windows)。

下表描述了您需要为您的 VPC 的默认安全组设置的推荐入站和出站规则。

默认安全组：推荐规则

入站			
源	协议	端口范围	注释
您网络的私有 IP 地址范围	TCP	22	（Linux 实例）允许来自您的网络的入站 SSH 数据流
您网络的私有 IP 地址范围	TCP	3389	（Windows 选项）允许来自您网络的入站 RDP 数据流
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	全部	全部	允许来自实例的所有出站数据流

Important

默认安全组会自动允许指定的实例进行彼此间通信，因此您无需添加规则以允许此操作。如果您使用另一个安全组，而且希望指定实例之间可以相互通信，则您必须添加相关规则。

实施情景 4

使用以下步骤以通过 VPC 向导实施情景 4。

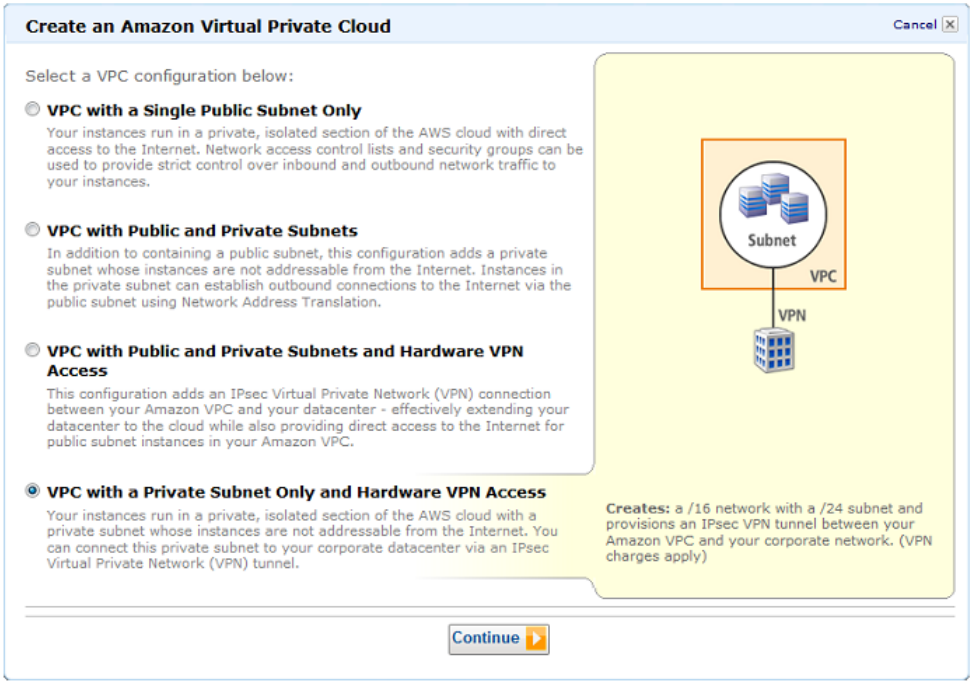
准备您的客户网关

1. 正在确定将作为您的客户网关使用的设备。有关我们已经测试的设备的信息，请参见Amazon Virtual Private Cloud 常见问题。有关对您的客户网关的要求的更多信息，请参见*Amazon Virtual Private Cloud Network Administrator Guide*。
2. 为客户网关的外部接口获取 Internet 可路由的 IP 地址。地址必须为静态，并且不可属于任何执行网络地址转换 (NAT) 任务的设备。
3. 收集应通过 VPN 连接传播到虚拟专用网关的内部 IP 范围列表（在 CIDR 符号内）（如果您使用的是静态路由 VPN 连接）。有关更多信息，请参见 VPN 路由选项 (p. 119)。

下一步，根据以下步骤中的描述使用 VPC 向导来创建您的 VPC 和 VPN 连接。

使用 VPC 向导实施情景 4

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“VPC Dashboard”。
3. 查找控制面板的“Your Virtual Private Cloud”区域，然后单击“Get started creating a VPC”，如果您没有 VPC 资源，您也可以单击“Start VPC Wizard”。
4. 选择第四个选项 – “VPC with a Private Subnet Only and Hardware VPN Access”，然后单击“Continue”。



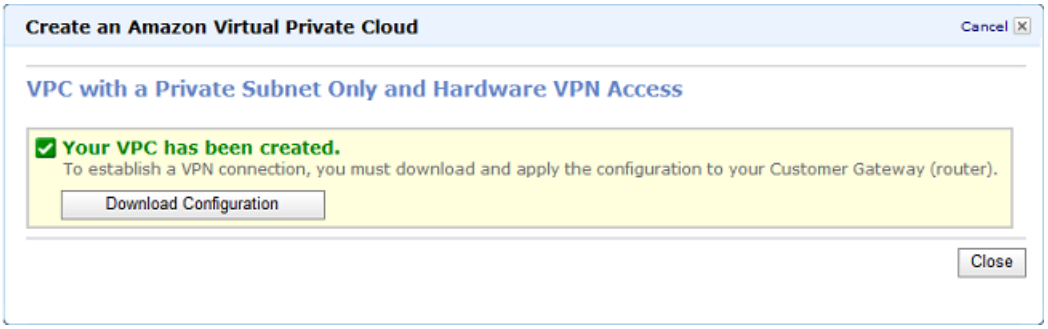
5. 在“Create an Amazon Virtual Private Cloud”对话框中，执行以下操作，然后单击“Continue”：

   - 在“IP Address”中，指定您的 VPN 路由器的公有 IP 地址。
   - 在“Specify the routing for the VPN Connection”中，从以下路由选项中选择一项：
     - 如果您的 VPN 路由器支持边界网关协议 (BGP)，选择“Use dynamic routing (requires BGP)”。
     - 如果您的 VPN 路由器不支持 BGP，选择“Use static routing”。在“IP Prefix”中，添加您的网络的每个 IP 前缀。

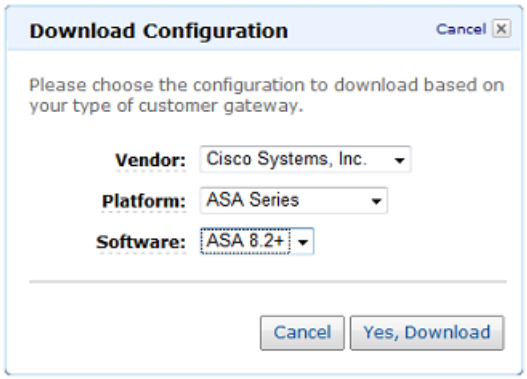
   有关适用选项的更多信息，请参见Amazon Virtual Private Cloud 常见问题。有关动态和静态路由的更多信息，请参见VPN 路由选项 (p. 119)。

6. 验证配置页面中的信息。根据您的需要进行更改，然后单击“Create VPC”以创建 VPC、子网、路由表和 VPN 连接。

7. 在您关闭向导之后，屏幕中会显示一个确认对话框和一个下载按钮，以供您下载您的客户网关的配置。单击“Download Configuration”。



8. 在“Download Configuration”对话框中，选择客户网关的供应商、平台和软件版本，然后单击“Yes, Download”。

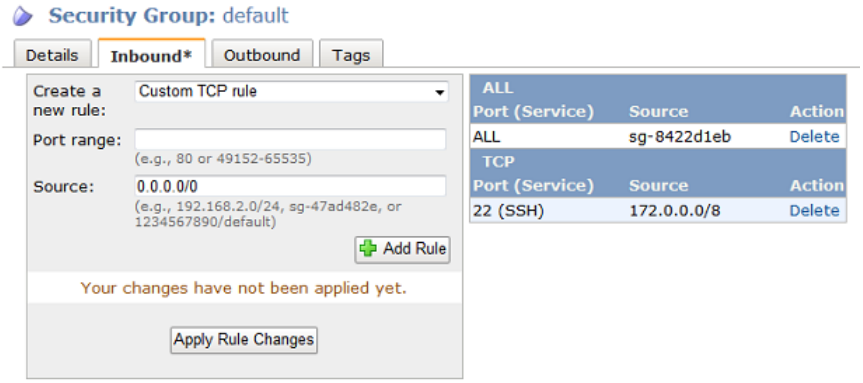


9. 保存包含 VPN 配置的文本文件，并将其连同指南 *Amazon Virtual Private Cloud Network Administrator Guide* 一起提供给您的网络管理员。在网络管理员完成客户网关配置之前，VPN 将无法使用。

在这个情景中，您需要更新默认安全组，添加新的入站规则，以允许从您的网络进行 SSH 和远程桌面 (RDP) 访问。提示：默认安全组的初始设置会阻塞所有入站数据流、允许所有出站数据流、以及允许归属于组的实例彼此之间建立通信。

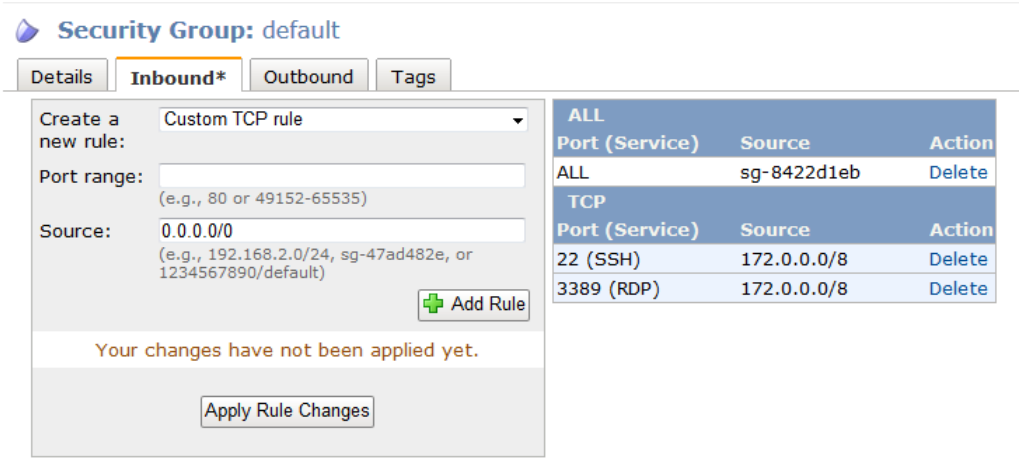
更新默认安全组的规则

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”，然后选择 VPC 的默认安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
3. 添加适用于从您的网络对组进行入站 SSH 访问的规则：
   a. 在“Inbound”选项卡上，从“Create a new rule”下拉列表中选择 SSH。
   b. 在“Source”方框中，输入您的网络的私有 IP 地址范围。
   c. 单击“Add Rule”。
   规则已被添加到“Inbound”选项卡中。不过，要等到您单击“Apply Rule Changes”后该规则才会应用到该安全组，您在添加完所有出站规则后也应单击此按钮。



4. 添加适用于从您的网络对组进行入站 RDP 访问的规则：

   a. 在Inbound选项卡上，从“RDPCreate a new rule”下拉列表中选择 。
   b. 在“Source”方框中，输入您的网络的私有 IP 地址范围。
   c. 单击“Add Rule”。



5. 单击“Apply Rule Changes”。

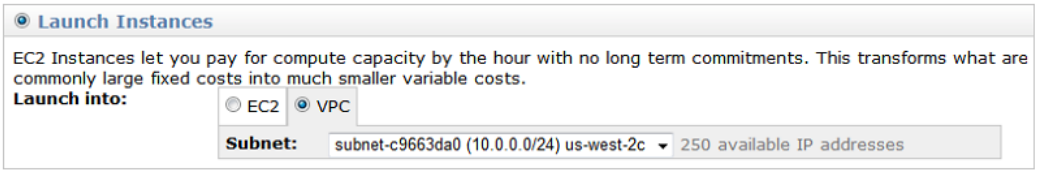
在您的网络管理员完成您的客户网关配置之后，您可以在您的 VPC 内启动实例。如果您已经熟悉了在 VPC 外启动实例的流程，您便已经大概了解应如何在 VPC 内启动实例。

启动实例

1. 启动 Classic 向导：

   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 单击控制面板中的“Launch Instance”按钮。
   c. 在创建新实例页面中，选择“Classic Wizard”，然后单击“Continue”。

2. 在“CHOOSE AN AMI”页面中，“Quick Start”选项卡显示了称为“亚马逊系统映像”(AMI) 的基本配置列表。选择您要使用的 AMI，然后单击它的“Select”按钮。
3. 在实例详细信息页面中，在“Launch Instances”项下，选择需要启动实例的子网。保留此页面中的其他默认设置，并单击“Continue”。



4. 如需使用接下来的INSTANCE DETAILS页面中描述的默认设置，您只需单击每页的Continue即可。
5. 在CREATE A KEY PAIR页面中，您可以从您已经创建的现有密钥对进行选择，或根据向导指示创建新的密钥对。
6. 在CONFIGURE FIREWALL页面中，选择默认安全组，然后单击“Continue”。
7. 检视您的设置。在您确认选择无误之后，单击“Launch”。

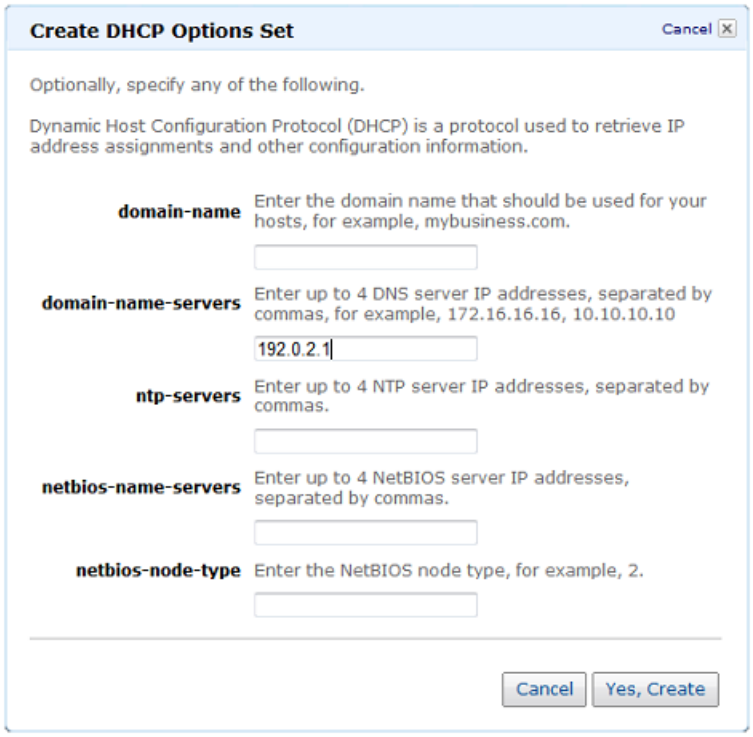
在情景 4 中，您需要一个 DNS 服务器来支持您的子网（仅限 VPN），使其与您的网络中的服务器进行通信。您必须创建新的 DHCP 选项集，在其中添加您的 DNS 服务器，并随后配置 VPC 以使用此选项集。

Note

您的 VPC 会自动生成 domain-name-servers=AmazonProvidedDNS 的 DHCP 选项。这是 Amazon 提供的 DNS 服务器，以帮助您启动 VPC 中的公有子网，从而通过 Internet 网关与 Internet 通信。情景 4 没有任何公有子网，因此您不需要这个 DHCP 选项集。

更新 DHCP 选项

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“DHCP Options Sets”。
3. 单击“Create DHCP Options Set”按钮。
4. 在“Create DHCP Options Set”对话框中，在“domain-name-servers”方框中输入您的 DNS 服务器地址，然后单击“Yes, Create”。在这个例子中，您的 DNS 服务器是 192.0.2.1。



5. 单击导航窗格中的“Your VPCs”。
6. 选择 VPC，然后单击“Change DHCP Options Set”按钮。
7. 在“Change DHCP Options Set”对话框中，从列表中选择新的选项集 ID，然后单击“Yes, Change”。
8. （可选）VPC 现在使用这套新的 DHCP 选项，并因此开始使用您的 DNS 服务器。如果您需要，您可以删除 VPC 使用的初始选项集。

您现在可以使用 SSH 或 RDP 来连接您 VPC 中的实例。有关如何连接 Linux 实例的信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Connect to Your Linux Instance部分。有关如何连接 Windows 实例的信息，请参见*Amazon Elastic Compute Cloud Microsoft Windows Guide*中的Connect to Your Windows Instance部分。

您的 VPC 和子网

要开始使用 Amazon Virtual Private Cloud (Amazon VPC)，您需要创建一个 VPC 和多个子网。有关 VPC 和子网的总体概览，请参见Amazon VPC 是什么？ (p. 1)。

Topics

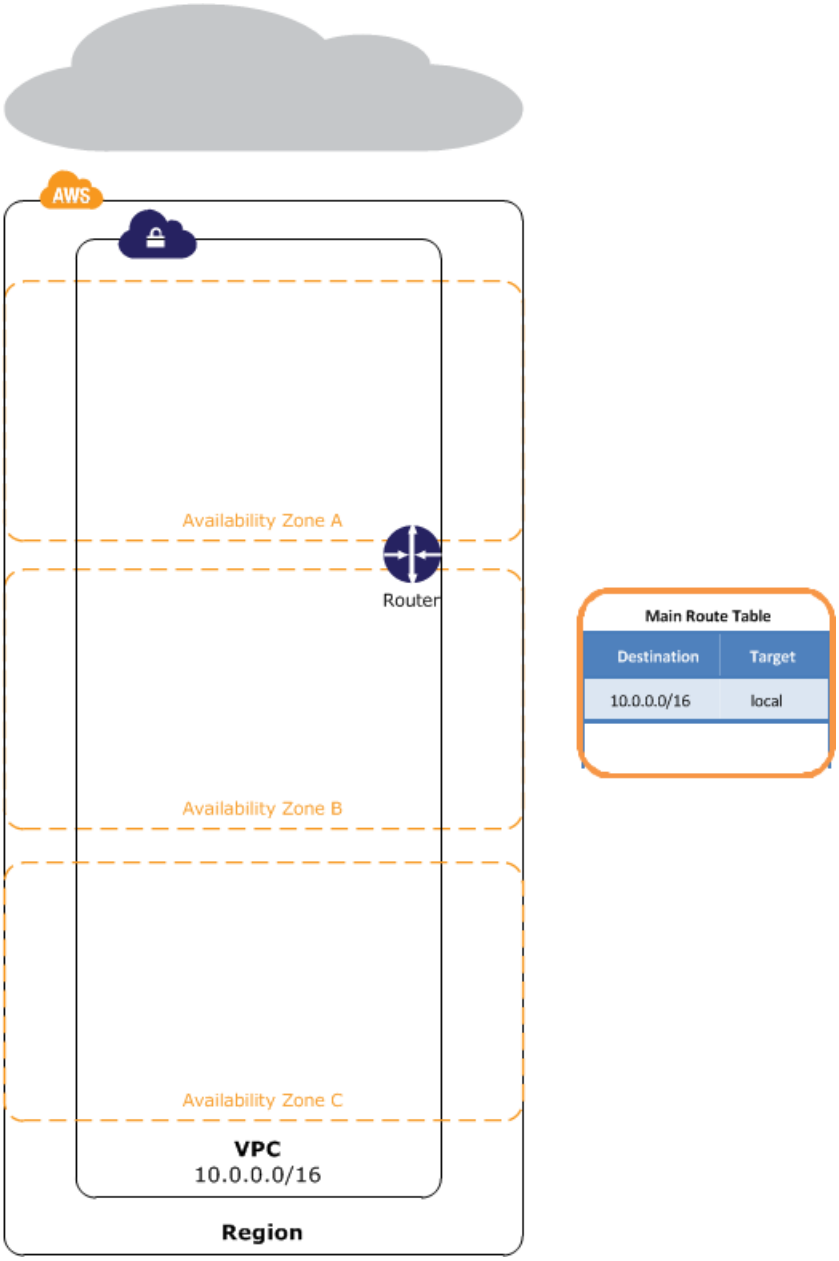
您的 VPC

在创建 VPC 时，您以无类域间路由 (CIDR) 块的形式为您的 VPC 指定 IP 地址集（例如，10.0.0.0/16）。有关 CIDR 注释和 "/16" 含义的更多信息，请参阅 Wikipedia 上的 Classless Inter-Domain Routing。

Topics

您的新 VPC

下图显示了具有默认路由表的新 VPC。



您需要先添加一个子网，然后才能在您的 VPC 中启动实例。

VPC 大小调整

您可以为 VPC 指定单一 CIDR 块。 允许块大小在 /28 网络掩码和 /16 网络掩码之间。换句话说，这个 VPC 可以包含 16 到 65,536 个 IP 地址。在您创建 VPC 之后，您便无法更改 VPC 的大小。 如果您的 VPC 容量过小无法满足您的需求，您必须终止在这个 VPC 中的所有实例，删除 VPC 并随后创建一个容量较大的新 VPC。有关更多信息，请参阅 正在删除您的 VPC (p. 47)。

您的 VPC 与您的公司或家庭网络之间的连接

您可以选择设置从您 VPC 到您的公司或家庭网络之间的连接。如果您在 VPC 中有一个 IP 地址，并且这个 IP 地址的前缀与您的网络前缀重叠，则任何通往这个网络前缀的数据流都将被停止。例如，让我们假设您有以下各项：

- VPC 的 CIDR 块为 10.0.0.0/16
- VPC 中的一个子网的 CIDR 块为 10.0.1.0/24
- 在 IP 地址为 10.0.1.4 和 10.0.1.5 的子网中运行的实例。
- 使用 CIDR 块 10.0.37.0/24 和 10.1.38.0/24 的内部主机网络

当 VPC 中的实例尝试与 10.0.37.0/24 地址空间内的主机通信时，因为 10.0.37.0/24 是分配给 VPC 的较大前缀 (10.0.0.0/16) 的一部分，因此实例和主机间的数据流将被中止。 实例可以与 10.1.38.0/24 空间内的主机通信，因为实例的块不是 10.0.0.0/16 的一部分。

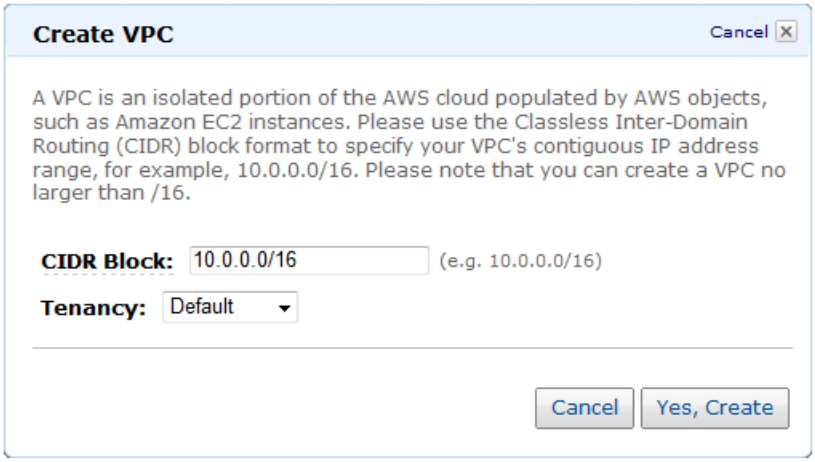
因此，我们建议您在创建 VPC 的 CIDR 范围时，使其足以满足未来的预期增长需求、并且不会与您的公司或家庭网络内任何现有或未来预期子网重叠。

正在创建 VPC

您可以通过两种方式使用 Amazon VPC 控制台创建 VPC：“Create VPC”对话框和 VPC 向导。以下步骤中会使用到“Create VPC”对话框，您只可用其创建 VPC；您需要随后自行添加子网、网关和路由表。 有关使用 VPC 向导，以便一步创建 VPC 及其子网、网关和路由表的信息，请参见使用 Amazon VPC 情景 (p. 7)。

创建 VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Your VPCs”。
3. 单击“Create VPC”。
4. 在“Create VPC”对话框中，根据需要指定以下 VPC 详细信息，然后单击“Yes, Create”。
   - 为 VPC 指定一个 CIDR 块。
   - 选择一个租期选项，例如，确保您的实例在单一租户硬件上运行的专用租期。有关专用实例的更多信息，请参阅 使用 EC2 专用实例 (p. 130)。



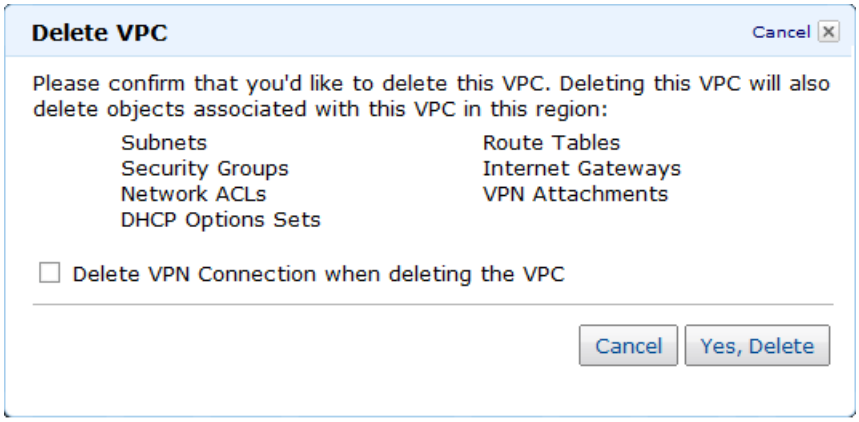
正在删除您的 VPC

您可以随时删除 VPC（例如，在您决定 VPC 容量过小的时候）。但是，请注意我们删除了与 VPC 相关的所有其他组件，例如实例、子网、安全组、网络 ACL、路由表、Internet 网关和 DHCP 选项。

如果您有VPN连接，您便无需删除此连接或与VPN相关的其他组件（例如客户网关和虚拟专用网关）。如果您计划在另一个 VPC 中使用客户网关，我们建议您保留 VPN 连接和网关。或者，您的网络管理员必须在您创建新的 VPN 连接之后配置再次配置网关。

删除您的 VPC

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 终止 VPC 中的所有实例。
3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
4. 在导航窗格中，单击“Your VPCs”。
5. 选择要删除的 VPC，然后单击“Delete”。
6. 如果您需要删除 VPN 连接，选择适用选项；或者您也可不选择此项。单击“Yes, Delete”。



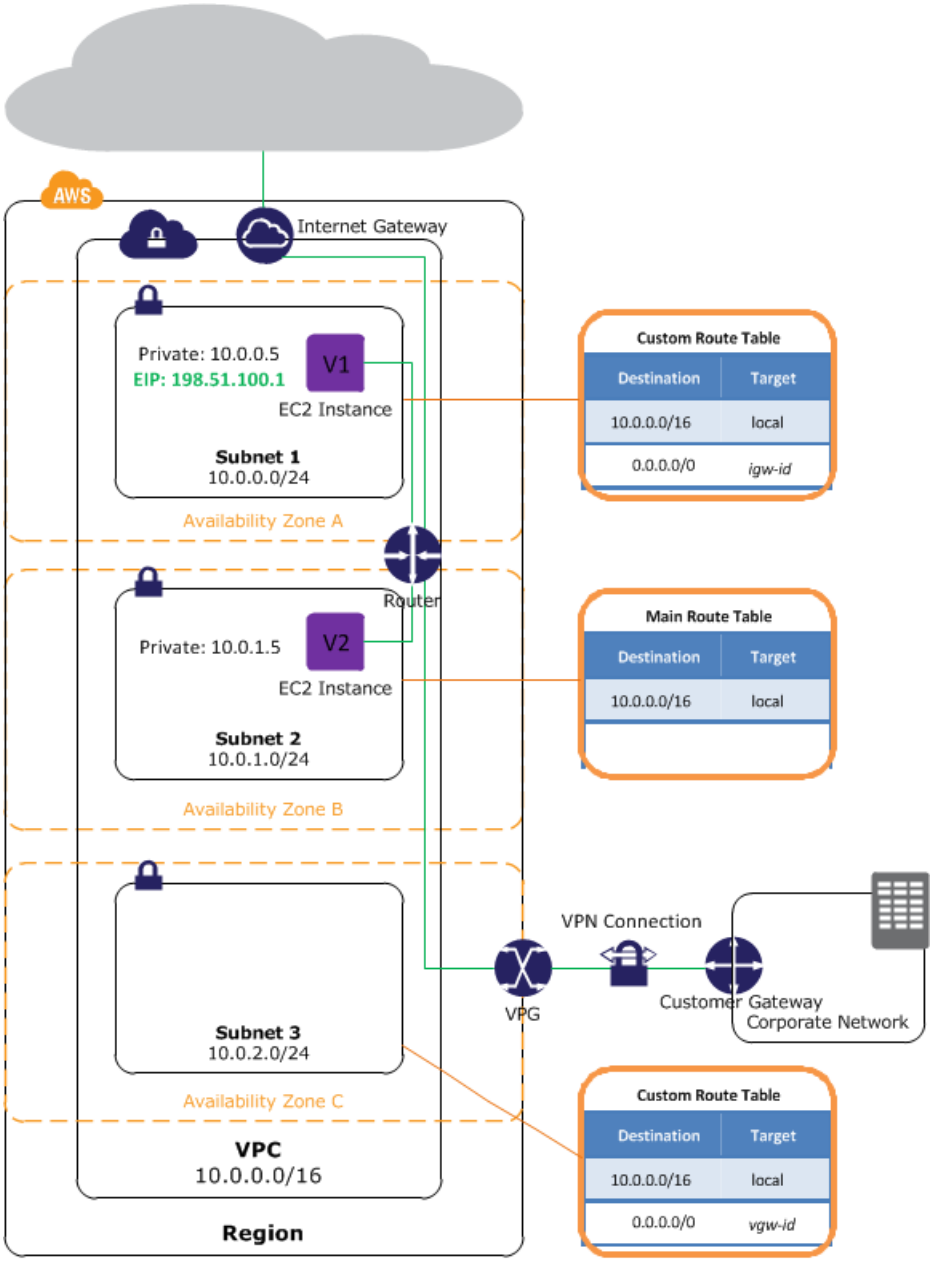
您的 VPC 中的子网

您可以创建跨越多个可用区域的 VPC。有关更多信息，请参阅 正在创建 VPC (p. 46)。在创建 VPC 之后，您可以在每个可用区域中添加一个或多个子网。每个子网都必须完全位于一个可用区域之内，不能跨越多个可用区域。可用区域是被设计为可以隔离其他可用区域的故障的不同位置。通过启动独立可用区域内的实例，您可以保护您的应用程序不受某一位置故障的影响。AWS 会为每个子网指定一个独特的 ID。

Topics

带子网的 VPC

下图展示了一个在多个可用区域内配置子网的 VPC。您可以根据需要添加 Internet 网关，以启用通过 Internet 的通信，或者添加一个虚拟私有网络 (VPN) 连接以启用与网络的通信。有关更多信息，请参见 使用 Amazon VPC 情景 (p. 7)、在您的 VPC 中添加 Internet 网关 (p. 100) 或 在您的 VPC 中添加硬件虚拟专用网关 (p. 117)。



子网大小调整

当您创建子网时，您即为这个子网指定了 CIDR 块。 子网的 CIDR 块可以与 VPC 的 CIDR 块（适用于 VPC 中的单一子网）或子网的 CIDR 块（启用多子网）相同。如果您在 VPC 中创建多于一个子网，切勿使子网的 CIDR 块重叠。

例如，如果您创建一个 CIDR 块为 10.0.0.0/24 的 VPC，它将支持 256 个 IP 地址。 您可以将这个 CIDR 块分散到两个子网，每个子网支持 128 个 IP 地址。 一个子网使用 CIDR 块 10.0.0.0/25（适用于 10.0.0.0 – 10.0.0.127 地址），另一个子网则使用 CIDR 块 10.0.0.128/25（适用于 10.0.0.128 – 10.0.0.255 地址）。

Important

AWS 将保留每个子网的 CIDR 块中的前四个 IP 地址和最后一个 IP 地址。您目前尚无法使用它们。

您可以借助许多工具来计算子网的 CIDR 块。有关常用工具的信息，请参阅 http://www.subnet-calculator.com/cidr.php。此外，您的网络工程组可以帮助您判断可为您的子网指定哪些具体 CIDR 块。

子网路由

通过设计，每个子网都必须关联一个路由表，这个路由表可指定允许出站数据流离开子网的可用路由。您创建的每个子网都会自动关联 VPC 的主路由表。 您可以更改关联，以及更改主路由表的内容。有关更多信息，请参见 路由表 (p. 89)。

如果一个子网的数据流可被路由到 Internet 网关，这个子网便是*公有子网*。在上一张图表中，子网 1 是公有子网。与子网 1 相关的路由表会将所有数据流 (0.0.0.0/0) 路由到一个 Internet 网关（例如 igw-1a2b3c4d）。因为实例 V1 有弹性 IP 地址，因此它可以连接 Internet。

如果一个子网没有通向 Internet 网关的路由，这个子网便是*私有子网*。在上一张图表中，子网 2 是私有子网。实例 V2 无法连接 Internet，但可以连接 VPC 中的其他实例。 您可以通过网络地址转换 (NAT) 实例，允许 VPC 中的一项实例启动到 Internet 的出站连接，并阻止来自 Internet 的未经请求的入站连接。有关更多信息，请参见 NAT 实例 (p. 104)。

如果一个子网没有通向 Internet 网关的路由，但其数据流会被路由到虚拟专用网关，这个子网便是*仅限 VPN 子网*。在上一张图表中，子网 3 是仅限 VPN 子网。与子网 3 相关的路由表会将所有数据流 (0.0.0.0/0) 路由到一个虚拟专用网关（例如ivgw-1a2b3c4d）。

子网安全性

通过设计，每个子网都必须关联一个网络 ACL，这个网络 ACL 可为子网中的实例提供子网级别的安全性。 您创建的每个新建子网都会自动关联 VPC 的默认网络 ACL。 您可以更改关联，以及更改默认网络 ACL 的内容。有关更多信息，请参见 网络 ACL (p. 64)。

正在向您的 VPC 中添加子网

当您在 VPC 中添加新子网时，您必须为子网设置您需要的路由和安全性。您可以根据此部分的描述手动进行此操作，或者由 VPC 向导为完成设置，如使用 Amazon VPC 情景 (p. 7)所述。

为您的 VPC 添加子网

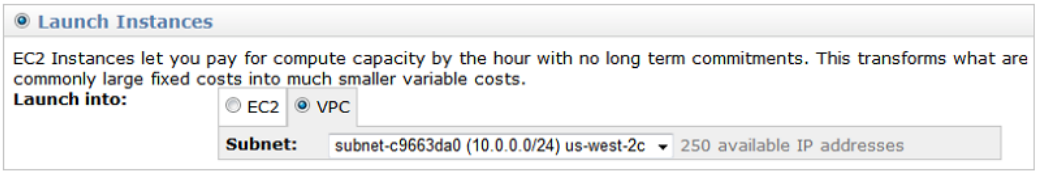
1. 创建子网。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. 在导航窗格中，单击“Subnets”。
   c. 单击“Create Subnet”。
   d. 在“Create Subnet”对话框中，选择 VPC，选择可用区域，指定子网的 CIDR 范围，然后单击“Yes, Create”。

2. 设置子网路由。例如，您可以在 Internet 网关或 NAT 实例中添加一个路由。有关更多信息，请参见路由表 (p. 89)。
3. （可选）根据需要创建或修改您的安全组。有关更多信息，请参见 您的 VPC 的安全组 (p. 58)。
4. （可选）根据需要创建或修改您的网络 ACL。有关网络 ACL 的更多信息，请参见网络 ACL (p. 64)。

在您的子网中启动一项实例

在您的子网中启动实例

1. 启动 Classic 向导：
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 在控制面板上，单击“Launch Instance”。
   c. 在创建新实例页面中，选择“Classic Wizard”，然后单击“Continue”。
2. 在选择 AMI页面中，“Quick Start”选项卡显示了名称为“亚马逊系统映像”(AMI)的基本配置列表。选择要使用的 AMI，然后单击对应的“Select”按钮。
3. 在实例详细信息页面中，在“Launch Instances”项下，选择需要启动实例的子网。保留此页面中的其他默认设置，并单击“Continue”。



4. 如需使用接下来几个INSTANCE DETAILS页面中的默认设置，只需在每页上单击“Continue”即可。
5. 在CREATE A KEY PAIR页面中，您可以从您已经创建的现有密钥对中进行选择，或根据向导的指示创建新的密钥对。
6. 在配置防火墙页面中，您可以从您已经有的安全组中进行选择，或根据向导的指示创建新的安全组。
7. 检视您的设置。如果您的选择无误之后，单击“Launch”。

删除您的子网

您必须先终止子网中的任何实例。

删除您的子网

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 终止子网中的所有实例。
3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
4. 在导航窗格中，单击“Subnets”。
5. 选择要删除的子网，然后单击“Delete”。
6. 在“Delete Subnet”对话框中，单击“Yes, Delete”。

您的默认 VPC 和子网

默认 VPC 将 EC2-VPC 平台提供的高级网络化功能优势与 EC2-Classic 平台的易于使用结合在一起。

有关 EC2-Classic 和 EC2-VPC 平台的更多信息，请参见Supported Platforms。

Topics

默认 VPC 基本信息

这个部分将提供关于您的 Virtual Private Cloud (VPC) 及其子网的信息。

可用性

有关在您的 AWS 账户的每个区域内检测平台支持的信息，请参见正在检测您的支持平台以及您是否有默认 VPC (p. 52)。

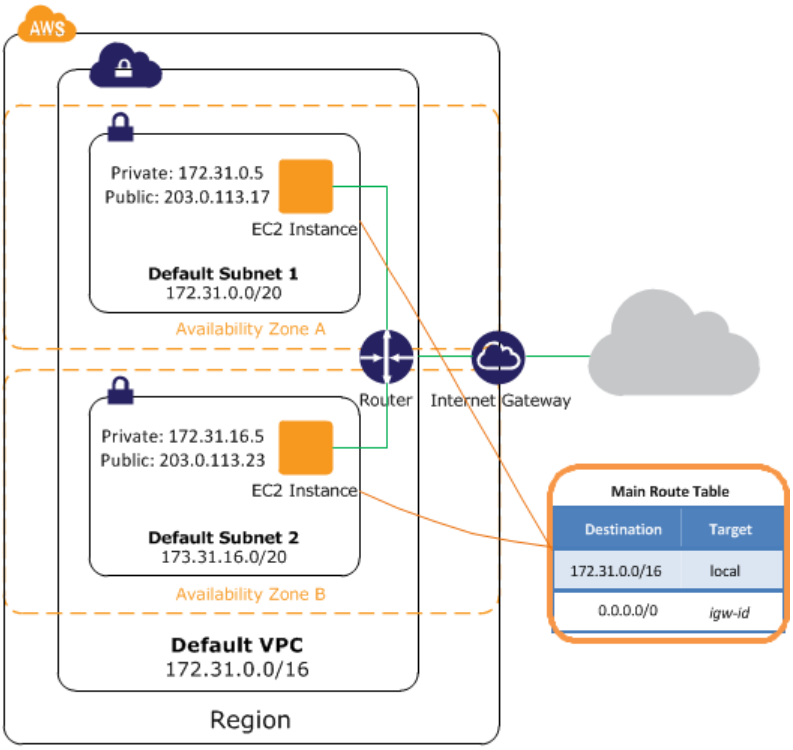
如果一个 AWS 账户仅支持 EC2-VPC，则与这个 AWS 账户相关的 IAM 账户也将仅支持 EC2-VPC，并会与 AWS 账户使用相同的默认 VPC。

组成部分

当我们创建默认 VPC 时，我们会通过以下操作为您完成设置：

- 在每个可用区域内创建默认子网。
- 创建 Internet 网关并将其连接到您的默认 VPC。
- 为您的默认 VPC 创建主路由表，并设置允许向 Internet 网关发送所有被指定到 Internet 的数据流。
- 创建默认安全组并将其与您的默认 VPC 关联。
- 创建默认网络访问控制列表 (ACL)，并将其与您的默认 VPC 关联。
- 将您的 AWS 账户的默认 DHCP 选项与您的默认 VPC 相关联。

下图表明了我们为默认 VPC 设置的关键组件。



您在默认 VPC 中启动的每项实例都可同时接收公有 IP 地址和私有 IP 地址。 每项实例同时还会接收公有和私有 DNS 主机名称。

默认 VPC 与其他任何 VPC 相同；您可以在其中添加子网、修改主路由表、添加额外路由表、关联额外安全组、更新默认安全组的规则以及添加 VPN 连接。您可以创建额外 VPC。

默认子网与任何其他子网相同，您可以在其中添加自定义路由表和设置网络 ACL。您还可以在启动 EC2 实例时指定默认子网。

默认子网

默认 VPC 的 CIDR 块将始终是 172.31.0.0/16。 最多可提供 65,536 个私有 IP 地址。默认子网的网络掩码始终都是 /20，它最多可为每个子网提供 4,096 个地址，其中部分地址将被预留以供我们使用。

默认子网通常都是公用子网，因为主路由表会将指定的 Internet 的子网数据流发送到 Internet 网关。您可以从到 Internet 网关的目标 0.0.0.0/0 中删除路由，以将私有子网设置为默认子网。 但是，如果您如此操作，在该子网中运行的 EC2 实例便无法访问 Internet 或其他 AWS 产品，例如 Amazon Simple Storage Service (Amazon S3)。

正在检测您的支持平台以及您是否有默认 VPC

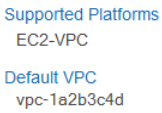
您可以在默认 VPC 内启动 EC2 实例并使用 Elastic Load Balancing、Amazon Relational Database Service (Amazon RDS) 以及 Amazon Elastic MapReduce (Amazon EMR)而不需了解任何有关 Amazon VPC 的任何信息。无论您使用的是默认 VPC 还是 EC2-Classic，您将获得相同的服务体验。 但是，您可以了解您的 AWS 账户是否支持两个平台，以及您是否有默认 VPC。下一个部分将为您展示应如何使用 Amazon EC2 控制台、Amazon EC2 命令行接口以及 Amazon EC2 API 操作。

AWS 管理控制台

Amazon EC2 控制台将表明您可以启动 EC2 实例的具体平台，以及您是否有默认 VPC。

Verify that the region you'll use is selected in the navigation bar. On the Amazon EC2 console dashboard, look for Supported Platforms under Account Attributes. If there are two values, EC2 and VPC, you can launch instances into either platform. If there is one value, VPC, you can launch instances only into EC2-VPC.

例如，以下示例表明账户仅支持 EC2-VPC 平台，默认 VPC 的标识符为`vpc-1a2b3c4d`。



如果您删除默认 VPC，Default VPC将显示为`None`。有关更多信息，请参见 正在删除您的默认 VPC (p. 55)。

命令行接口

`supported-platforms`属性表明您可以在其中启动 EC2 实例的平台。如需获取您的账户此属性值，使用如下所示`ec2-describe-account-attributes`命令。

```
ec2-describe-account-attributes supported-platforms
```

如果属性有两个值，`EC2-Classic`和`EC2-VPC`，则账户可以在任何一个平台内启动 EC2 实例。如果您在启动实例时未指定 VPC，它将在 EC2-Classic 平台内启动。

如果这个属性有一个值，`EC2-VPC`，则账户仅可以在 EC2-VPC 中启动实例。如果您在启动实例时未指定 VPC，它将在您的默认 VPC 内启动。

以下是输出示例，表明您始终在 EC-VPC 内启动实例。

```
ACCOUNTATTRIBUTE    supported-platforms
VALUE     EC2-VPC
```

`default-vpc`属性会表明您是否有默认 VPC，（如果您有）并显示它的标识符。如需获取此属性值，使用`ec2-describe-account-attributes`命令。您可以在同一个命令行中指定两项属性，`supported-platforms`和`default-vpc`，或者您也可以如此处所示分别使用它们。

```
ec2-describe-account-attributes default-vpc
```

以下是输出示例，表明您有 ID 为“vpc-1a2b3c4d”的默认 VPC。

```
ACCOUNTATTRIBUTE    default-vpc
VALUE     vpc-1a2b3c4d
```

此外，当您使用`ec2-describe-vpcs`命令显示您的 VPC 时，我们会在输出中表明默认 VPC。当您使用`ec2-describe-subnets`命令显示您的子网时，我们会在输出中表明每个可用区域的默认子网。

有关更多信息，请参见*Amazon Elastic Compute Cloud Command Line Reference*中的 ec2-describe-account-attributes、ec2-describe-vpcs和ec2-describe-subnets部分。

API

`supported-platforms`属性表明您可以在其中启动 EC2 实例的平台。`default-vpc` 属性会指明您是否有默认 VPC，（如果您有）并显示它的标识符。如需为您的账户获取这些属性值，请使用`DescribeAccountAttributes`API 操作。

此外，当您使用`DescribeVpcs`API 操作显示您的 VPC 时，我们会在响应中表明默认 VPC。当您使用`DescribeSubnets`API 操作显示您的子网时，我们会在响应中表明每个可用区域的默认子网。

有关更多信息，请参见*Amazon Elastic Compute Cloud API Reference*中的DescribeAccountAttributes、DescribeVpcs和DescribeSubnets部分。

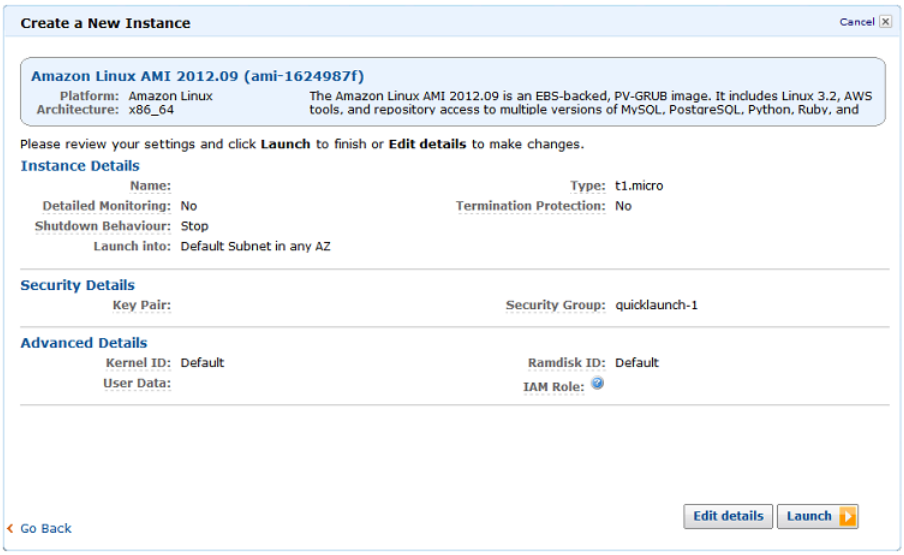
在您的默认 VPC 内启动 EC2 实例。

当您启动 EC2 实例但却未指定相关子网时，实例会自动在您的默认 VPC 的默认子网内启动。我们会默认为您选择一个可用区域，并在该可用区域的相应子网内启动实例。 或者，您可以通过在控制台选择与实例对应的默认子网、或在 CLI 中指定子网或可用区域，从而为您的实例选择可用区域。

AWS 管理控制台

在您的默认 VPC 内启动 EC2 实例

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 在 Amazon EC2 控制台控制面板中，单击Launch Instance。
3. 在Create a New Instance页面中，单击Quick Launch Wizard。按照向导中的指示操作。 为您的实例指定名称、创建密钥对并选择一项 AMI。使用默认安全组。
4. 检视您的设置。Launch into的默认值是Default Subnet in any AZ。这意味着这项实例会在我们选定的可用区域的默认子网中启动。 或者，您可以单击Edit details以为特定的可用区域选择默认子网。



5. 单击Launch以启动实例。

命令行接口

如需在您的默认 VPC 中启动 EC2 实例，您可以使用`ec2-run-instances`命令以启动您的实例，并且无需指定子网或可用区域。例如：

```
ec2-run-instances ami-b232d0db
```

如需在您的默认 VPC 的指定子网内启动一项 EC2 实例，您需要指定一个可用区域。

```
ec2-run-instances ami-b232d0db --availability-zone us-east-1a
```

或者，使用`ec2-describe-subnets`命令列出您的子网，同时显示可用区域的默认子网。

```
ec2-describe-subnets
SUBNET  subnet-9d4a7b6c   available   vpc-1a2b3c4d  10.0.1.0/24   250   us-east-
1a  true true
```

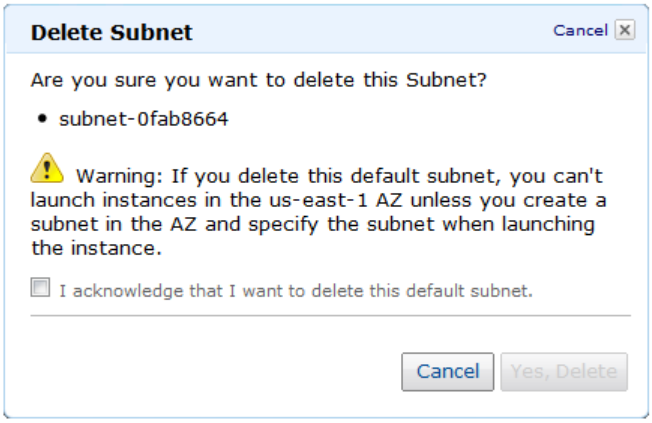
随后，使用`ec2-run-instances`在可用区域的默认子网中启动您的实例。例如：

```
ec2-run-instances ami-b232d0db -s subnet-9d4a7b6c
```

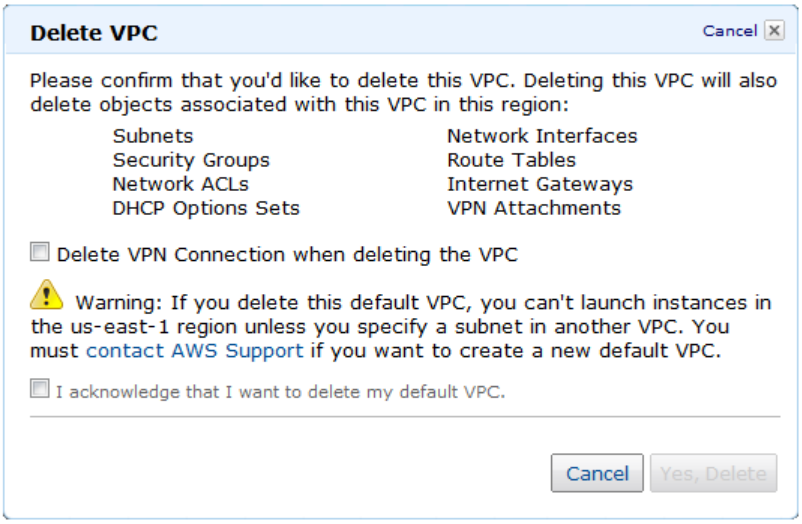
正在删除您的默认 VPC

您可以像删除其他任何子网一样删除一个或多个默认子网。 但是，在您删除默认子网之后，默认子网便会消失。现在，您无法在默认 VPC 内的这个可用区域内启动 EC2 实例，除非您在这个可用区域内创建子网，并明确地在这个子网内启动实例。 如果您删除默认 VPC 的所有默认子网，则您必须在启动 EC2 实例时在其他 VPC 内指定一个子网，因为您无法在 EC2-Classic 内启动实例。

如果您尝试删除默认子网，Delete Subnet对话框内会显示警告，并要求您确认您知道您正在删除默认子网。



您可以像删除任何其他 VPC 一样删除您的默认 VPC。 但是，在您删除默认 VPC 之后，默认 VPC 便会消失。 现在，您必须在启动 EC2 实例时在另一个 VPC 中启动子网，因为您无法在 EC2-Classic 启动实例。如果您尝试删除默认 VPC，Delete Subnet对话框内会显示警告，并要求您确认您知道您正在删除默认 VPC。



如果您删除了默认 VPC，并随后需要恢复这个默认 VPC，您可以联系 AWS Support 以重新设置您的账户，以使我们可以为您创建新的默认 VPC。

您的 VPC 安全性

Amazon VPC 提供两种功能，以供您提高 VPC 的安全性：

- 安全组 – 作为相关 Amazon EC2 实例的防火墙，可在实例级别控制入站和出站的数据流。
- 网络访问控制列表 (ACL) – 作为关联子网的防火墙，在子网级别控制入站和出站数据流

当您在 VPC 中启动一项实例时，您可以为其关联一个或多个您已经创建的安全组。在您的 VPC 中的每项实例都可能属于不同的安全组集合。如果您在启动实例时未指定安全组，实例会自动归属到 VPC 的默认安全组。有关安全组的更多信息，请参见您的 VPC 的安全组 (p. 58)。

您可以仅利用安全组来确保您的 VPC 实例安全；但是，您可以添加网络 ACL 以作为第二防御层。有关网络 ACL 的更多信息，请参见网络 ACL (p. 64)。

您可以使用 AWS Identity and Access Management 来控制可以创建和管理安全组及网络 ACL 的组织成员。例如，您可以仅授予您的网络管理员此许可，而非将许可授予需要启动实例的人员。有关更多信息，请参见 控制 VPC 管理 (p. 81)。

Note

Amazon 安全组和网络 ACL 不会过滤通向或来自本地链接地址 (169.254.0.0/16) 的数据流。VPC 中的本地链接地址支持以下服务：域名服务 (DNS)、动态主机配置协议 (DHCP)、Amazon EC2 实例特定元数据以及密钥管理服务器（KMS – Windows 实例的许可管理）。
您可以在您的实例中实施额外的防火墙解决方案，以阻断与本地链接地址间的网络通信。

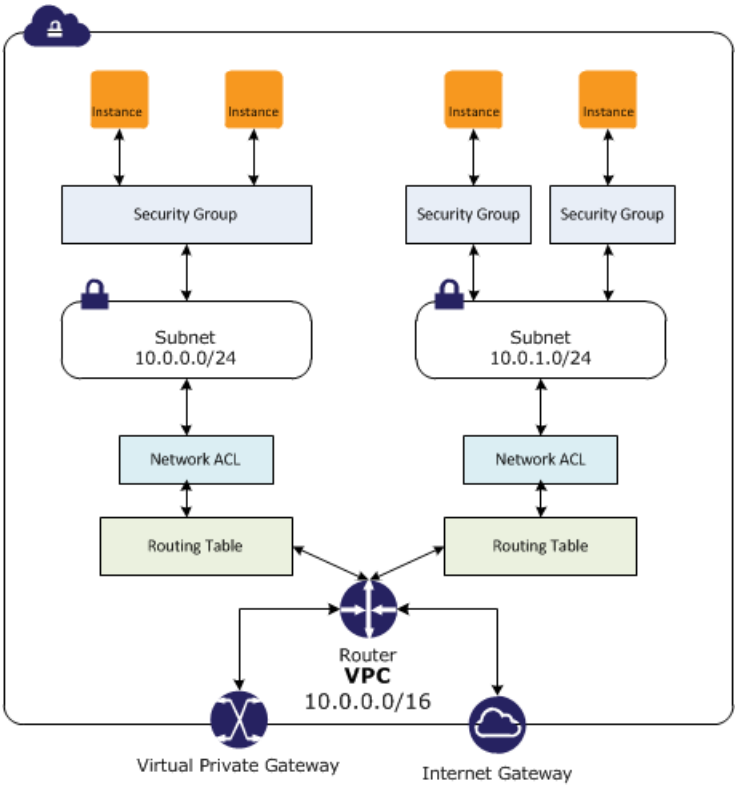
安全组与网络 ACL 的比较

下表概述了安全组和网络 ACL 之间的基本差异。

安全组	网络 ACL
在实例级别操作（第一防御层）	在子网级别操作（第二防御层）
仅支持允许规则	支持允许规则和拒绝规则
有状态：返回数据流会被自动允许，不受任何规则的影响	无状态：返回数据流必须被规则明确允许

安全组	网络 ACL
我们会在决定是否允许数据流前评估所有规则	我们会在决定是否允许数据流时按照数字顺序处理所有规则
只有在启动实例的同时指定安全组、或稍后将安全组与实例关联的情况下，操作才会被应用到实例	自动应用到关联子网内的所有实例（备份防御层，因此您便不需要依靠别人为您指定安全组）

下图展示了由安全组和网络 ACL 提供的安全层。例如，来自 Internet 网关的数据流会通过路由表中的路径被路由到合适的子网。与子网相关的网络 ACL 规则控制允许进入子网的数据流。与实例相关的安全组规则控制允许进入实例的数据流。



您的 VPC 的安全组

*安全组*充当虚拟防火墙，控制允许进入和离开相关实例的流量。当您在 VPC 内中启动实例时，您可以为该实例指定最多五个 VPC 安全组。安全组在实例级别运行，而不是子网级别。因此，在您的 VPC 的子网中的每项实例都归属于不同的安全组集合。如果您在启动时没有指定具体的安全组，实例会自动归属到 VPC 的默认安全组。

对于每个安全组，您可以添加*规则*以控制到实例的入站数据流，以及另外一套单独规则以控制出站数据流。此部分描述了您需要了解的有关您的 VPC 安全组的基本信息以及它们的规则。

您可以设置网络 ACL，使其规则与您的安全组相似，以便为您的 VPC 添加额外安全层。有关安全组和网络 ACL 之间的不同之处的更多信息，请参见安全组与网络 ACL 的比较 (p. 57)。

Topics

安全组基本信息

以下是您的 VPC 安全组的基本特征：

- 您最多可以为每个 VPC 创建 100 个安全组。您最多可以为每个安全组添加 50 条规则。如果您需要向一个实例应用超过 50 条规则，则最多可以为每个实例指定 5 个安全组。
- 您可以指定允许规则，但不可指定拒绝规则。
- 您可以为入站和出站流量指定单独规则。
- 在您向安全组中添加入站规则之前，所有入站数据流都默认不被允许。
- 在您向安全组中添加出站规则之前，所有出站数据流都会被默认允许（此后将由您指定允许的出站数据流）。
- 如果是为响应已允许的入站数据流量，则该响应可以出站，此时可忽略出站规则，反之亦然（安全组会相应地显示状态）。
- 与安全组关联的实例无法彼此通信，除非您添加了相应的允许规则（已有此类默认规则的默认安全组除外）。
- 在您启动实例之后，您可以更改与实例关联的具体安全组。

您的 VPC 的默认安全组

您的 VPC 会自动带有默认的安全组。如果您在启动实例时未指定其他安全组，则您在 VPC 内启动的每项 EC2 实例都会自动与默认安全组关联。

以下是默认安全组的默认设置：

- 不允许入站流量流入实例（来自同一安全组中的实例的流量除外）
- 允许从实例流出的所有出站流量
- 允许同一安全组的实例之间的入站和出站流量。

您可以更改默认安全组的规则。

安全组规则

您可以添加或删除安全组规则（又被称为*授权*或*撤销*入站或出站访问）。适用于入站数据流（进入）或出站数据流（离开）的规则。您可以授予访问特定 CIDR 范围、或您的 VPC 内的另一个安全组的权限。

以下是您的安全组规则的基本部分：

- （仅限入站规则）数据流源（CIDR 范围或安全组）以及目标端口或端口范围
- （仅限出站规则）数据流目的地（CIDR 范围或安全组）以及目标端口或端口范围
- 任何有标准协议编号的协议（有关具体列表，请参见Protocol Numbers）

  如果您指定 ICMP 作为协议，您可以指定任意或全部 ICMP 类型和代码。

当您添加或删除一项规则时，您的修改会自动应用到所有与该安全组相关的实例。

Note

有些设置防火墙的系统会让您在源端口进行过滤。安全组可帮助您仅在目标端口进行过滤。

以下是一个安全组规则示例。

入站			
源	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许来自任何地方的入站 HTTP 访问
0.0.0.0/0	TCP	443	允许来自任何地方的入站 HTTPS 访问
出站			
目的地	协议	端口范围	注释
DBServerSG	TCP	1433	允许对 DBServerSG 组内的实例进行出站 MS SQL 访问
0.0.0.0/0	TCP	80	允许对 Internet 上的服务器进行出站 HTTP 访问（例如，软件更新）
0.0.0.0/0	TCP	443	允许对 Internet 上的服务器进行出站 HTTPS 访问（例如，软件更新）

EC2-Classic 和 EC2-VPC 安全组之间的差异

如果您已经是 Amazon EC2 用户，则可能对这些安全组很熟悉。但是，您无法将创建用于 EC2-Classic 的安全组用于 VPC 中的实例。您必须专门为 VPC 中的实例创建安全组。您为 VPC 安全组创建的规则无法参考在 EC2-Classic 安全组中使用的规则，反之亦然。

下表概述了在 EC2-Classic 和 EC2-VPC 中使用的安全组的不同之处。

EC2-Classic	EC2-VPC
您最多可以为每个地区创建 500 个安全组。	您最多可以为每个 VPC 创建 100 个安全组。
您最多可以为一个安全组添加 100 条规则。	您最多可以为一个安全组添加 50 条规则。
您只能为入站流量添加规则。	您可以为入站和出站流量添加规则。
您可以为一个实例分配无限个安全组。	您最多可以为一个实例分配 5 个安全组。
您可以参考其他 AWS 账户的安全组。	您只能参考您的 VPC 的安全组。
启动实例后，您就不能再更改为其分配的安全组。	您可以在启动实例后更改为其分配的安全组。
当您向安全组添加规则时，无需指定某项协议，并且仅有 TCP、UDP 或 ICMP 可供您使用。	当您向安全组添加规则时，必须指定协议，您可以指定任何有标准协议编号的协议或所有协议（参见 Protocol Numbers）。
当您向安全组添加规则时，必须指定端口号（适用于 TCP 或 UDP）。	当您向安全组添加规则时，可以指定端口号（只有在规则是 TCP 或 UDP 规则时，您才可以指定全部端口号）。

使用安全组

此部分为您展示如何用 AWS 管理控制台使用安全组。

Topics

正在修改默认安全组

您的 VPC 包含一个默认安全组，其初始规则为拒绝所有入站数据流、允许所有出站数据流以及允许所有在组内实例之间的数据流。您无法删除此安全组；但是，您可以更改安全组的规则。此过程与修改任何其他安全组的过程相同。 有关更多信息，请参见 添加和删除规则 (p. 61)。

正在创建安全组

尽管您可以为实例指定默认安全组，您可能仍希望创建自己的安全组，以反映实例在您的系统中扮演的不同角色。本指南中提出的多个情景都包括创建您自己的安全组。有关更多信息，请参见 使用 Amazon VPC 情景 (p. 7)。

创建安全组

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 单击“Create Security Group”按钮。
4. 输入安全组名称，并提供描述。 从“VPC”菜单中选择您 VPC 的 ID，然后单击“Yes, Create”。

在默认情况下，新安全组起初只有一条出站规则，即允许所有通信离开实例。您必须添加规则，以便允许任何入站数据流或限制出站数据流。

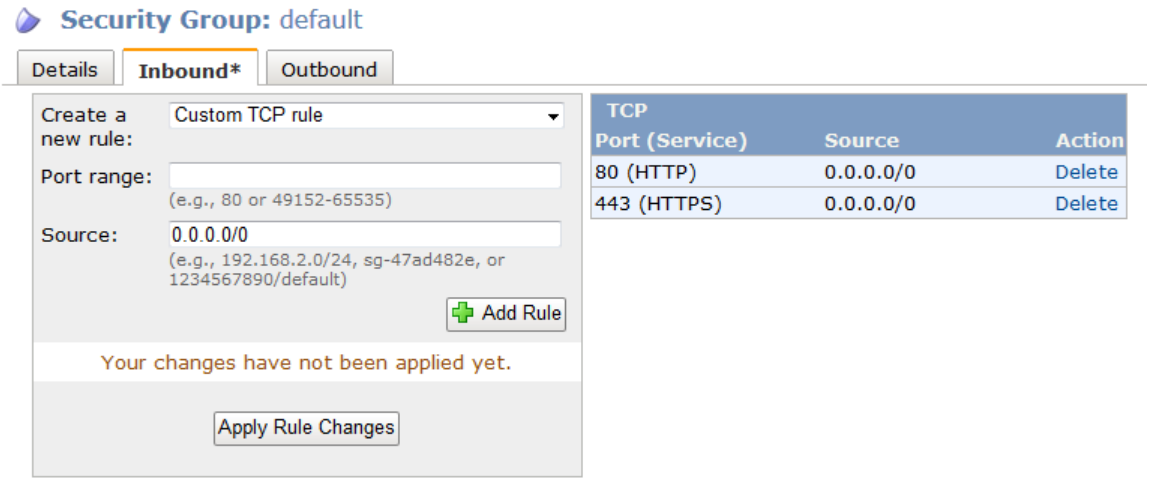
添加和删除规则

当您添加或删除一项规则时，任何已经指定到该安全组的实例都会随之发生变化。您无法修改规则；您仅可以添加和删除规则。

本指南中提出的多个情景都包括有关在安全组内添加规则的说明。有关更多信息，请参见 使用 Amazon VPC 情景 (p. 7)。

添加一项规则

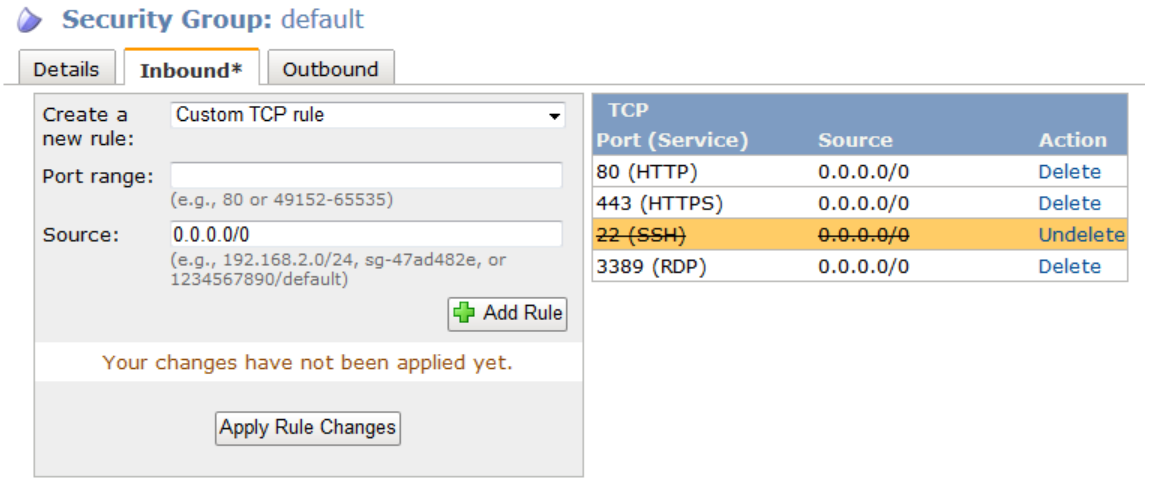
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 选择需要更新的安全组。 详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
4. 使用“Inbound”选项卡，从“Create a new rule”中选择一个入站数据流规则选项，填写必填信息，然后单击“Add Rule”。例如，选择HTTP或HTTPS，并保留“Source”的设置为0.0.0.0/0。请注意“Apply Rule Changes”按钮已经启用，按钮上方将显示“Your changes have not been applied yet”文本。在添加完所有您需要的入站数据流规则之后，单击“Apply Rule Changes”以添加规则。



5. 重复上一步中描述的步骤，以使用“Outbound”选项卡添加出站数据流规则。

删除一项规则

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 选择需要更新的安全组。 详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
4. 对于您希望删除的规则，单击“Delete”。请注意“Apply Rule Changes”按钮已经启用，按钮上方将显示“Your changes have not been applied yet”文本。
5. 单击“Apply Rule Changes”以删除规则。

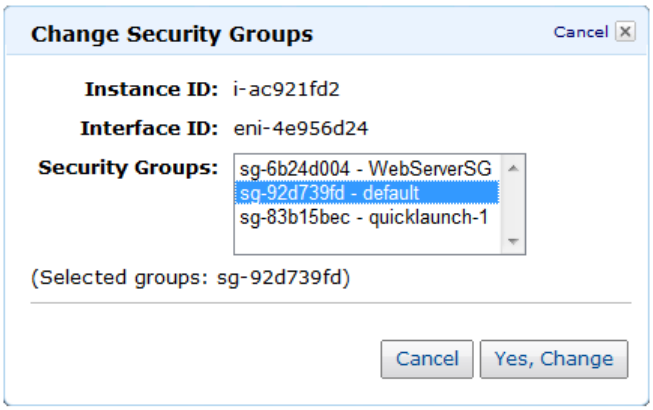


正在更改实例的安全组

您可以在启动 VPC 实例之后，更改该实例归属的安全组。当您进行此更改时，实例可以处于运行或停止状态。

更改实例的安全组

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 单击导航窗格中的“Instances”。
3. 右键单击实例，然后选择“Change Security Groups”。
4. 在“Change Security Groups”对话框中，从“Security Groups”中选择一个或多个安全组，然后单击“Yes, Change”。



正在删除安全组

只有在某一安全组中没有任何实例时（无论是运行还是停止实例），您方可删除此安全组。您可以在删除安全组之前将实例指定到另一个安全组（参阅正在更改实例的安全组 (p. 62)）。

删除安全组

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 选择安全组，然后单击“Delete”。
4. 在“Delete Security Group”对话框中，单击“Yes, Delete”。

删除“2009-07-15-default”安全组

任何使用晚于 2011-01-01 的 API 版本创建的 VPC 都有`2009-07-15-default`安全组。除了这个安全组之外，每个 VPC 还自带了常规`default`安全组。您无法将 Internet 网关与具有 `2009-07-15-default` 安全组的 VPC 关联。因此，您必须先删除此安全组，然后才能将 Internet 网关与 VPC 关联。

Note

如果您已将此安全组分配给任何实例，则必须先将这些实例分配给其他安全组，然后才能删除所分配的安全组。

删除**`2009-07-15-default`**安全组

1. 确保此安全组未分配给任何实例。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 单击导航窗格中的Network Interfaces。

c. 从列表中选择实例的网络接口，然后从“Actions”列表中选择“Change Security Groups”。
d. 在“Change Security Groups”对话框中，从“Security Groups”列表中选择新的安全组，然后单击“Save”。

Tip

在更改实例的安全组时，您可以从列表中选择多个安全组。您选定的安全组会替换实例现有的安全组。

e. 为每个实例重复上一步骤。

2. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
3. 单击导航窗格中的“Security Groups”。
4. 选择`2009-07-15-default`安全组，然后单击“Delete”按钮。
5. 在“Delete Security Group”对话框中，单击“Yes, Delete”。

API 和命令概览

下表概述了可用安全组命令和相应的 API 操作。

描述	命令	API 操作
创建安全组	ec2-create-group	CreateSecurityGroup
在安全组中添加规则。	ec2-authorize	AuthorizeSecurityGroupIngress AuthorizeSecurityGroupEgress
描述您的一个或多个安全组。	ec2-describe-group	DescribeSecurityGroups
修改与实例相关的安全组。	ec2-modify-instance-attribute	ModifyInstanceAttribute
从安全组中删除规则。	ec2-revoke	RevokeSecurityGroupIngress RevokeSecurityGroupEgress
删除安全组	ec2-delete-group	DeleteSecurityGroup

网络 ACL

*网络访问控制列表 (ACL)*是一个可选安全层，可作为防火墙，以控制进出子网的数据流。您可以设置网络 ACL，使其规则与您的安全组相似，以便为您的 VPC 添加额外安全层。 有关安全组和网络 ACL 之间的差别的更多信息，请参见安全组与网络 ACL 的比较 (p. 57)。

Topics

- API 和命令概览 (p. 108)

网络 ACL 基本信息

以下是您需要了解的有关网络 ACL 的基本信息:

- 网络 ACL 是规则的编号列表，以供我们按顺序评估（从编号最小的规则开始）以判断数据流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。我们建议您从创建规则编号为 100 的倍数的规则开始，以使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。
- 您的 VPC 会自动带有可以修改的默认网络 ACL；这个网络 ACL 会默认允许所有入站和出站数据流。
- 您可以创建自定义网络 ACL；每个自定义网络 ACL 最初都为关闭状态（不允许任何数据流），直至您添加规则为止。
- 每项子网都必须与一个网络 ACL 关联；如果您的未在子网与一个网络 ACL 之间建立显式关联，子网将自动与默认网络 ACL 关联。
- 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）。

有关您可以创建的网络 ACL 数目的信息，请参见Amazon VPC 限制 (p. 135)。

网络 ACL 规则

您可以在默认网络 ACL 中添加或删除规则，或为您的 VPC 创建额外网络 ACL。当您在网络 ACL 中添加或删除规则时，更改也会自动应用到与其相关联的子网。

以下为部分网络 ACL 规则：

- 规则编号。规则评估从编号最低的规则起开始进行。
- 协议。您可以指定任何有标准协议编号的协议。 有关更多信息，请参见Protocol Numbers。如果您指定 ICMP 作为协议，您可以指定任意或全部 ICMP 类型和代码。
- [仅限入站规则]数据流源（CIDR 范围）和目标端口（监听）或端口范围。
- [仅限出站规则]数据流目标（CIDR 范围）以及目标端口或端口范围。
- 允许或拒绝选项。

默认网络 ACL

为帮助您理解 ACL 规则的形式，以下是默认网络 ACL 在其初始状态时可能呈现的形式。它经配置以允许所有数据流流进和流出每个子网。每个网络 ACL 都包含一项以星号作为规则名称的规则。此规则会确保在数据包不匹配任何其他规则时拒绝此数据包。您可以修改或删除此规则。

入站				
规则 #	源 IP	协议	端口	允许/拒绝
100	0.0.0.0/0	全部	全部	允许
*	0.0.0.0/0	全部	全部	拒绝
出站				
规则 #	目的 IP	协议	端口	允许/拒绝
100	0.0.0.0/0	全部	全部	允许

*	0.0.0.0/0	全部	全部	拒绝

自定义网络 ACL 示例

下表展示了一个自定义网络 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 49152-65535）. 有关如何选择适当的临时端口范围的更多信息，请参见临时端口 (p. 67)。

网络 ACL 还包括允许 SSH 和 RDP 数据流进入子网的入站规则。出站规则 120 允许离开子网的响应。

网络 ACL 出站规则（100 和 110）允许离开子网的 HTTP 和 HTTPS 数据流。存在相应的入站规则，以允许响应出站数据流（入站规则 140，适用于临时端口 49152-65535）。

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许来自任何地方的入站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许来自任何地方的入站 HTTP 数据流
120	192.0.2.0/24	TCP	22	允许	允许来自您的家庭网络的公有 IP 地址范围内的入站 SSH 数据流（通过 Internet 网关）。
130	192.0.2.0/24	TCP	3389	允许	允许从您的家庭网络的公有 IP 地址范围内，到 Web 服务器的入站 RDP 数据流（通过 Internet 网关）。
140	0.0.0.0/0	TCP	49152-65535	允许	允许来自 Internet 的入站返回数据流（即生成自子网的请求）。 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 (p. 67)。
150	0.0.0.0/0	UDP	32768-61000	允许	允许入站返回 UDP 流量。 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 (p. 67)。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流。
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流。

110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流。
120	0.0.0.0/0	TCP	49152-65535	允许	允许对 Internet 客户端进行出站响应（例如，向访问子网中 Wed 服务器的人员开放网页）。 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 (p. 67)。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流。

随着数据包流向子网，我们会根据与子网关联的 ACL 的进入规则评估数据包（从规则列表的顶端开始向下移动）。 信息包被指定发往 SSL 端口 (443)。数据包不匹配第一项评估规则（规则 100）。它匹配第二条规则 (110)，即允许数据包进入子网。如果数据包的目的地已经指定为端口 139 (NetBIOS)，则最初两项规则可能无法匹配，但是“*”规则最终可能会拒绝这个数据包。

在您需要开放一系列端口、同时在此部分端口内您想拒绝部分窗口，您可能希望添加一项拒绝规则。您只需确保将拒绝规则放在表的较前端，先于一系列的端口数据流的规则。

临时端口

上一个部分中的网络 ACL 实例使用了临时端口范围 49152-65535。但是，您可能希望为网络 ACL 设置不同的范围。此部分将为您解释原因。

发起请求的客户端会选择临时端口范围。根据客户端的操作系统不同，范围也随之更改。许多Linux内核（包括 Amazon Linux 内核）使用端口 32768-61000。生成自 Elastic Load Balancing 的请求使用端口 1024-65535。Windows 操作系统通过 Windows Server 2003 使用端口 1025-5000。Windows Server 2008 使用端口 49152-65535。因此，如果一项来自 Internet 上的 Windows XP 客户端的请求到达您的 VPC 的 Web 服务器，则您的网络 ACL 必须有相应的出站规则，以启用目标为端口 1025-5000 的数据流。

如果在您的 VPC 中的一项 EC2 实例是客户发起的请求，则您的网络 ACL 必须有入站规则以启动目标为仅适用于此类实例的临时端口的数据流（Amazon Linux、Windows Server 2008 等）。

实际上，为涵盖不同客户端类型可能启动的进入到您 VPC 中的公有实例的数据流，您需要开放临时端口 1024-65535。但是，您也可以在 ACL 中添加规则以拒绝任何在此范围内的来自恶意端口的数据流。您只需确保将拒绝规则放在表的较前端，先于允许一系列临时端口数据流的规则。

使用网络 ACL

此部分为您展示如何在 AWS 管理控制台中使用网络 ACL。

Topics

- 正在删除网络 ACL (p. 73)

判断与子网关联的网络 ACL

判断与子网关联的特定网络 ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Subnets”，然后选择子网。

   与子网相关联的网络 ACL 已包含在详细信息页面中，连同网络 ACL 的规则一起。

Subnet: subnet-161db57c

CIDR: 10.0.0.0/24 **VPC:** vpc-071db56d **Availability Zone:** us-east-1d

Route Table: rtb-ed1db587 (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-041db56e

Network ACL: Default (replace)
Inbound:

Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

判断与网络 ACL 关联的子网

判断与网络 ACL 关联的特定子网

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”。

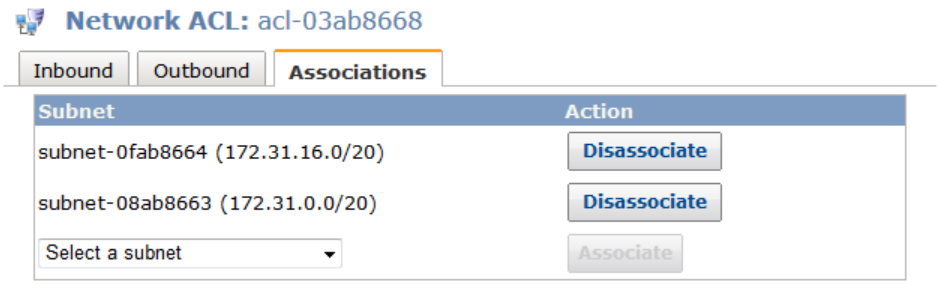
   控制台会显示您的网络 ACL。Associated With一栏显示相关子网的数目。

Viewing: All Network ACLs 1 to 2 of 2 Items

	Network ACL ID	Associated With	Default	VPC
☐	acl-03ab8668	2 Subnets	Yes	vpc-09ab8662 (172.31.0.0/16)
☐	acl-051db56f	1 Subnet	Yes	vpc-071db56d (10.0.0.0/16)

3. 选择网络 ACL。

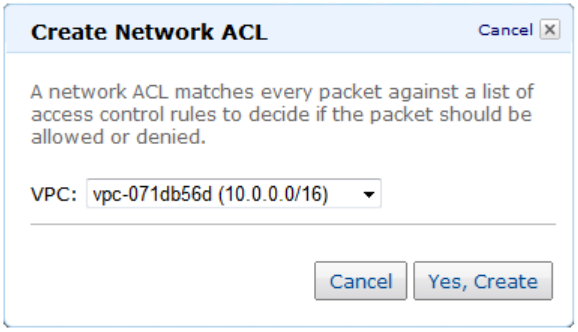
4. 在详细信息窗格中，单击“Associations”选项卡以显示与网络 ACL 相关联的子网。



正在创建网络 ACL

创建网络网络 ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”。
3. 单击“Create Network ACL”按钮。
4. 在“Create Network ACL”对话框中，从“VPC”列表中选择您的 VPC 的 ID，但后单击“Yes, Delete”。



网络 ACL 的初步设定会阻塞所有入站和出站数据流。除了在每个 ACL 中展示的“*”规则之外，网络 ACL 再无其他规则。

新增 ACL 未与任何子网相关联。

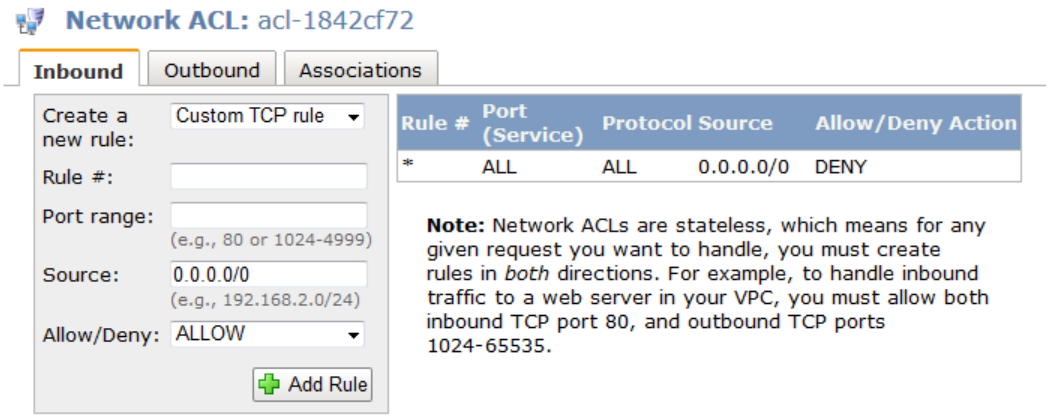
正在添加和删除规则

当您在网络 ACL 中添加或删除规则时，与其相关联的子网也会随之更改。您不需要在子网中终止和重新启动实例；更改将稍后生效。

您无法修改规则，您仅可以添加和删除规则。如果您需要更改 ACL 中的规则顺序，您必须添加有新规则编号的新规则，并随后删除最初的规则。

为网络 ACL 添加规则

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”，然后选择网络 ACL。
3. 在详细信息窗格中，根据您需要添加的规则类型，“Inbound”或“Outbound”选项卡。



4. 从“Create a new rule”下拉列表中选择选项 。例如，如需添加 HTTP 规则，您可以选择HTTP选项。如需添加规则以允许所有 TCP 数据流，选择All TCP。对于部分选项（例如 HTTP）我们会在端口中为您提供。如需使用未列出的规则，您可以选择“Custom protocol rule”。
5. 提供规则详细信息：

   a. 在Rule #中输入一个规则编号（例如 100）。规则编号必须不是存在于网络 ACL 中。我们会按顺序处理规则，以编号最低的规则开始。

   Tip

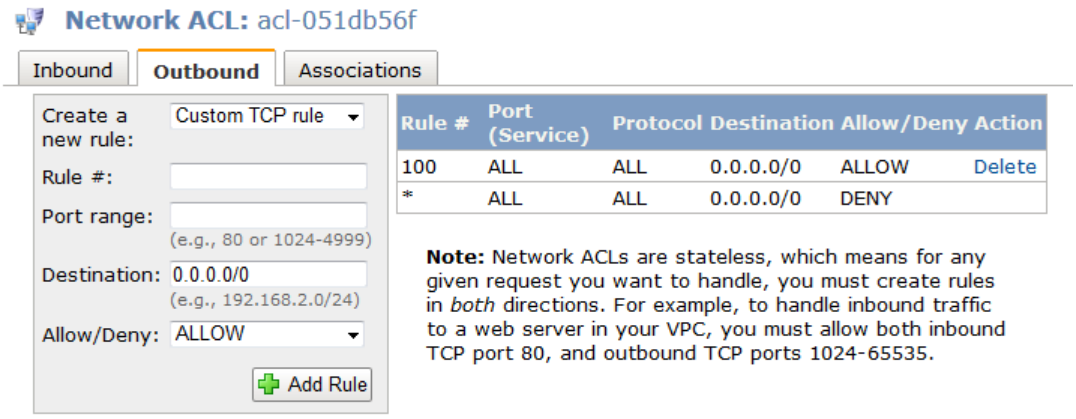
   我们建议您使用跳跃的规则编号（例如 100、200、300）而不是使用顺序编号（例如 101、102、103）。这会让在目标中添加新规则变得更加简单，无需您记住现有规则。

   b. （可选）如果您正在创建自定义协议规则，您可以在Protocol方框中输入协议编号 (47) 或名称 (GRE)。有关更多信息，请参见IANA List of Protocol Numbers。
   c. （可选）如果您已经选定的协议要求提供端口号，您可以输入由连字符分隔的端口号或端口范围（例如 49152-65535）。
   d. 在Source或Destination方框中（根据是入站规则还是出站规则），输入规则适用的 CIDR 范围。

6. 从“Allow/Deny”列表中，选择“ALLOW”以允许指定数据流或选择“DENY”以拒绝指定数据流。
7. 单击“Add Rule”。

从网络 ACL 删除规则

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”，然后选择网络 ACL。
3. 在详细信息窗格中，选择“Inbound”或“Outbound”选项卡，然后单击“Delete”。



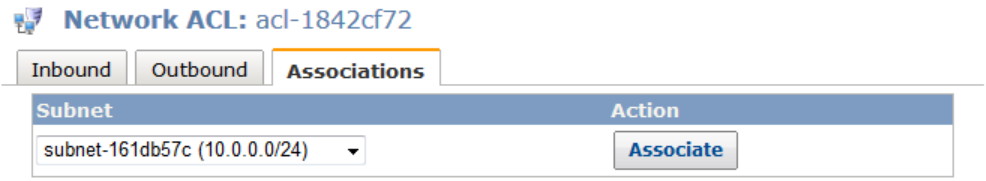
4. 在“Delete Network ACL Rule”对话框中，单击“Yes, Delete”。

正在将子网与网络 ACL 关联

如需对特定子网应用特定的网络 ACL 规则，您必须首先将子网与网络 ACL 关联。您可以将一个网络 ACL 与多个子网关联；但是，一个子网仅可以与一个网络 ACL 关联。任何未与特定 ACL 关联的子网都与会默认与默认网络 ACL 关联。

将子网与网络 ACL 关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”，然后选择网络 ACL。
3. 在详细信息窗格中，在“Associations”选项卡中，选择需要与表关联的子网，然后单击“Associate”。



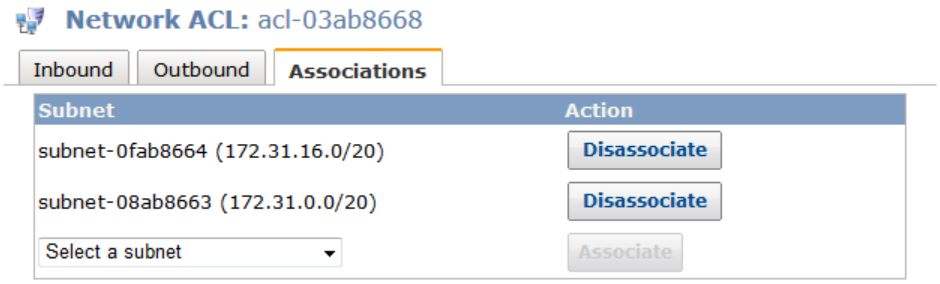
4. 在“Associate Network ACL”对话框中单击“Yes, Associate”。

解除网络 ACL 与子网的关联

您可以需要解除子网与其网络 ACL 的关联。例如，您可能有与自定义网络 ACL 关联的子网，但是您希望将其与默认网络 ACL 关联。通过解除子网与自定义网络 ACL 的关联，子网将与默认网络 ACL 建立关联。

解除子网与网络 ACL 的关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”，然后选择网络 ACL。
3. 在详细信息窗格中，单击“Associations”选项卡。
4. 单击“Disassociate”。



5. 在“Disassociate Network ACL”对话框中，单击“Yes, Disassociate”。

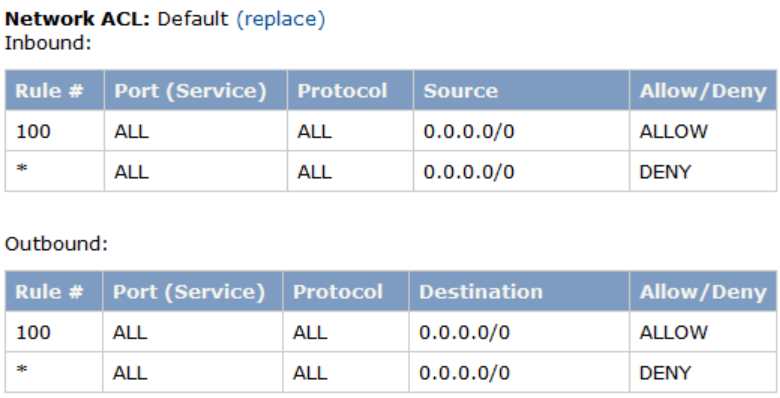
更改子网的网络 ACL

您可以更改子网关联的具体网络 ACL。例如，当您创建一个子网时，这个子网会最初与主路由表关联。相反，您可能需要将其与您创建的自定义网络 ACL 相关联。

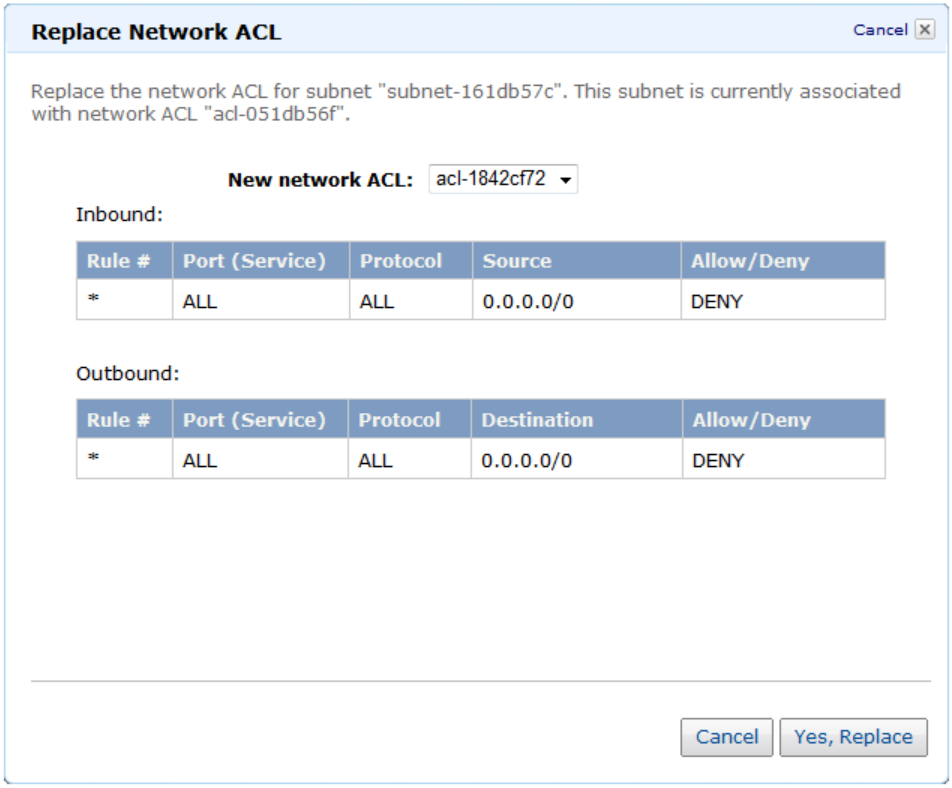
在更改子网的网络 ACL 之后，您不需要终止和重新启动子网中的实例；您的更改会在稍后生效。

更改子网的网络 ACL 关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Subnets”，然后选择子网。
3. 在详细信息窗格中，在与子网相关的网络 ACL 的 ID 旁，单击Replace。



4. 在“Replace Network ACL”对话框的下拉列表中，选择需要与子网关联的网络 ACL，然后单击“Yes, Replace”。



正在删除网络 ACL

您只可以删除未与任何子网关联的网络 ACL。您无法删除默认网络 ACL。

删除网络 ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Network ACLs”。
3. 选择网络 ACL，但后单击“Delete”按钮。
4. 在“Delete Network ACL”对话框中，单击“Yes, Delete”。

API 和命令概览

下表概述了可用的网络 ACL 命令和相应的 API 操作。

描述	命令	API 操作
为您的 VPC 创建网络 ACL	ec2-create-network-acl	CreateNetworkAcl
描述一项或多项您的网络 ACL。	ec2-describe-network-acls	DescribeNetworkAcls
删除网络 ACL。	ec2-delete-network-acl	DeleteNetworkAcl
在网络 ACL 中添加规则。	ec2-create-network-acl-entry	CreateNetworkAclEntry

描述	命令	API 操作
从网络 ACL 中删除规则。	ec2-delete-network-acl-entry	DeleteNetworkAclEntry
替换网络 ACL 中的现有规则。	ec2-replace-network-acl-entry	ReplaceNetworkAclEntry
更改与子网相关联的网络 ACL	ec2-replace-network-acl-association	ReplaceNetworkAclAssociation

您的 VPC 的推荐网络 ACL 规则

Topics

此指南在之前部分展示的情景可引导您使用默认规则下的默认网络 ACL。这些规则允许所有进出子网的数据流量，这意味着实际上您已经无需再使用 ACL 来为您的 VPC 提供任何额外安全性。

如果您希望额外安全层，此附录描述了我们推荐在本指南情景中使用的网络 ACL 规则。有关网络 ACL 和如何使用网络 ACL 的更多信息，请参见网络 ACL (p. 64)。

Important

下方的示例 ACL 列出了临时端口范围为 49152-65535。您可能希望使用不同范围。有关更多信息，请参见临时端口 (p. 67)。

情景 1 的推荐规则

在情景 1 中，您的单一子网中的实例可以接收和发送 Internet 数据流。有关情景 1 的完整讨论，请参见情景 1：仅带公有子网的 VPC (p. 7)。

下表显示了推荐规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许来自任何地方的入站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许来自任何地方的入站 HTTPS 数据流
120	您的家庭网络的公有 IP 地址范围	TCP	22	允许	允许来自您的家庭网络的入站 SSH 数据流（通过 Internet 网关）
130	您的家庭网络的公有 IP 地址范围	TCP	3389	允许	允许来自您的家庭网络的入站 RDP 数据流（通过 Internet 网关）

140	0.0.0.0/0	TCP	49152-65535	允许	允许从源于子网的请求返回的入站数据流 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流
120	0.0.0.0/0	TCP	49152-65535	允许	允许对 Internet 中的客户端进行出站响应（例如向访问子网 Web 服务器的人员开放网页） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

情景 2 的推荐规则

在情景 2 中，您的公有子网中的实例可以接收和发送 Internet 数据流，私有子网无法从 Internet 直接接收数据流。但是，它会通过公有子网中的 NAT 实例，启动到 Internet 的数据流量（并接收响应）。有关情景 2 的完整讨论，请参见情景 2：带有公有子网和私有子网的 VPC (p. 13)。

在这个情景中，您的公有子网有网络 ACL，私有子网有另一个单独的网络 ACL。下表显示了推荐给每个 ACL 的规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。它们大多会在情景中模拟安全组规则。

公有子网的 ACL 规则

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许来自任何地方的入站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许来自任何地方的入站 HTTPS 数据流

120	您的家庭网络的公有 IP 地址范围	TCP	22	允许	允许来自您的家庭网络的入站 SSH 数据流（通过 Internet 网关）
130	您的家庭网络的公有 IP 地址范围	TCP	3389	允许	允许来自您的家庭网络的入站 RDP 数据流（通过 Internet 网关）
140	0.0.0.0/0	TCP	49152-65535	允许	允许从源于子网的请求返回的入站数据流 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流
120	10.0.1.0/24	TCP	1433	允许	允许对私有子网中的数据库服务器进行出站 MS SQL 访问
130	10.0.1.0/24	TCP	3306	允许	允许对私有子网中的数据库服务器进行出站 MySQL 访问
140	0.0.0.0/0	TCP	49152-65535	允许	允许对 Internet 中的客户端进行出站响应（例如向访问子网 Web 服务器的人员开放网页） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

私有子网的 ACL 规则

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释

100	10.0.0.0/24	TCP	1433	允许	允许公有子网中的 Web 服务器读写私有子网中的 MySQL 服务器
110	10.0.0.0/24	TCP	3306	允许	允许公有子网中的 Web 服务器读写私有子网中的 MySQL 服务器
120	10.0.0.0/24	TCP	22	允许	允许来自公有子网的 SSH 防御的入站 SSH 数据流
130	10.0.0.0/24	TCP	3389	允许	允许公有子网的 Microsoft Terminal Services 网关的入站 RDP 数据流（通过虚拟专用网关）
140	10.0.0.0/24	TCP	49152-65535	允许	允许从公有子网中的 NAT 实例返回的入站数据流，以处理源于私有子网的请求 参阅本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流
120	10.0.0.0/24	TCP	49152-65535	允许	允许对公有子网进行出站响应（例如响应正在与私有子网中的 DB 服务器通信的公有子网中的 Web 服务器） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

情景 3 的推荐规则

在情景 3 中，您的公有子网中的实例可以接收和发送 Internet 数据流，一个仅限 VPN 连接的子网中的实例仅可以通过 VPN 连接与您的家庭网络通信。有关情景 3 的完整讨论，请参见情景 3：带有公有和私有子网以及硬件 VPN 访问的 VPC (p. 24)。

在这个情景中，您的公有子网有网络 ACL，以及仅限 VPN 连接的子网的另一个单独的网络 ACL。下表显示了推荐给每个 ACL 的规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。

公有子网的 ACL 规则

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从任何地方到 Web 服务器的入站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许从任何地方到 Web 服务器的入站 HTTPS 数据流
120	您的家庭网络的公有 IP 地址范围	TCP	22	允许	允许从您的家庭网络到 Web 服务器的入站 SSH 数据流（通过 Internet 网关）
130	您的家庭网络的公有 IP 地址范围	TCP	3389	允许	允许从您的家庭网络到 Web 服务器的入站 RDP 数据流（通过 Internet 网关）
140	0.0.0.0/0	TCP	49152-65535	允许	允许从源于子网的请求返回的入站数据流 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流
120	10.0.1.0/24	TCP	1433	允许	允许对仅限 VPN 连接的子网中的数据库服务器进行出站 MS SQL 访问
130	10.0.1.0/24	TCP	3306	允许	允许对仅限 VPN 连接的子网中的数据库服务器进行出站 MySQL 访问
140	0.0.0.0/0	TCP	49152-65535	允许	允许对 Internet 中的客户端进行出站响应（例如向访问子网 Web 服务器的人员开放网页） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。

*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

仅限 VPN 的子网的 ACL 设置

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	10.0.0.0/24	TCP	1433	允许	允许公有子网中的 Web 服务器读写仅限 VPN 连接的子网中的 MS SQL 服务器
110	10.0.0.0/24	TCP	3306	允许	允许公有子网中的 Web 服务器读写仅限 VPN 连接的子网中的 MySQL 服务器
120	您的家庭网络的私有 IP 地址范围	TCP	22	允许	允许来自家庭网络的入站 SSH 数据流（通过虚拟专用网关）
130	您的家庭网络的私有 IP 地址范围	TCP	3389	允许	允许来自家庭网络的入站 RDP 数据流（通过虚拟专用网关）
140	您的家庭网络的私有 IP 地址范围	TCP	49152-65535	允许	允许从家庭网络客户端返回的入站数据流（通过虚拟专用网关） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	您的家庭网络的私有 IP 地址范围	全部	全部	允许	允许从子网到您的家庭网络的所有出站数据流（通过虚拟专用网关）
110	10.0.0.0/24	TCP	49152-65535	允许	允许对公有子网中的 Web 服务器进行出站响应 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。

120	您的家庭网络的私有 IP 地址范围	TCP	49152-65535	允许	允许对家庭网络中的客户端进行出站响应（通过 Internet 网关） 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

情景 4 的推荐规则

在情景 4 中，您的单一子网中的实例仅可以通过 VPN 连接与您的家庭网络通信。有关情景 4 的完整讨论，请参见情景 4：仅带有私有子网和硬件 VPN 访问的 VPC (p. 35)。

下表显示了推荐规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。

入站					
规则 #	源 IP	协议	端口	允许/拒绝	注释
100	您的家庭网络的私有 IP 地址范围	TCP	22	允许	允许从您的家庭网络到子网的入站 SSH 数据流
110	您的家庭网络的私有 IP 地址范围	TCP	3389	允许	允许从您的家庭网络到子网的入站 RDP 数据流
120	您的家庭网络的私有 IP 地址范围	TCP	49152-65535	允许	允许从源于子网的请求返回的入站数据流 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。
*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流
出站					
规则 #	目的 IP	协议	端口	允许/拒绝	注释
100	您的家庭网络的私有 IP 地址范围	全部	全部	允许	允许从子网到您的家庭网络的所有出站数据流
120	您的家庭网络的私有 IP 地址范围	TCP	49152-65535	允许	允许对家庭网络中的客户端进行出站响应 参见本主题开始部分的重要注释，以了解如何指定正确的临时端口。

*	0.0.0.0/0	全部	全部	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流

控制 VPC 管理

您是否希望控制哪些用户可以设置和管理您的 Virtual Private Cloud (VPC)？您是否希望控制哪些用户可以关联 Internet 网关或定义安全组和网络 ACL？您可以使用 AWS Identity and Access Management (IAM) 来创建和管理在您的账户中的用户。*用户*是指需要与 AWS 互动的人员或应用程序。利用 IAM，您可以集中管理您的账户用户、他们的安全证书（例如访问密钥）以及控制用户可以访问 AWS 资源的许可。

对于 Amazon VPC 和 Amazon EC2，您可以使用 IAM 来控制用户可以访问的 API 操作。例如，您可以在 IAM 中创建用户网络管理员组，并仅向该组授予相应权限，使其能够调用创建和管理 VPC 的 Amazon EC2 API 操作。因此，您的组织成员便无法自行更改 VPC 的布局、路由和安全性。

Note

目前，您尚无法使用 IAM 来限制用户访问特定 Amazon EC2 或 Amazon VPC 资源的权限。您可以只限制用户访问单项 API 操作的权限。例如，您无法使用 IAM 来阻止用户访问特定实例、子网或安全组；IAM 权限适用于该类型的所有资源。

IAM 使用 JSON 格式的策略以指定用户许可。您创建一项策略，并将您希望对其应用许可的用户组添加到策略中。下一部分会展示对您有用的策略示例。

Note

IAM 策略可控制访问权限，并且不受接口影响。例如，您可以允许一个用户登录 AWS 管理控制台，并且适用于该用户的策略可以控制其在控制台内的操作权限。或者，您可以为用户提供 AWS 访问密钥，以向 AWS 进行 API 调用，策略可控制用户能够使用这些访问密钥通过身份验证、进而通过库或客户端请求的具体操作。

有关设置账户中的用户、策略和 IAM 的详细信息，请访问 Using IAM。

在 Amazon VPC 中使用 AWS IAM

利用 IAM，您可以使用 JSON 格式或通过 AWS 管理控制台以编程方式管理组和它们对您的 VPC 资源访问权限。借助两种工具，您可以创建一个组，例如“管理员”，并赋予其访问您的 VPC 的完全权限。组可以执行全套任务，例如创建和删除 VPC 和子网、关联和取消关联路由表以及撤销安全组访问权限。或者，您可以创建只能访问确定的 VPC 资源集的组。

Amazon VPC 的亚马逊资源名称 (ARN)

Amazon VPC 没有亚马逊资源名称 (ARN)，因为您无法在 IAM 策略中指定特定的 Amazon VPC 资源。在编写策略以控制对 Amazon VPC API 操作的访问权限时，您可以将通配符 * 指定为资源。

有关 ARN 的详细信息，请参阅 *Amazon Web Services General Reference* 中的 Amazon Resource Names (ARN) and AWS Service Namespaces。

Amazon VPC API 操作

在 IAM 策略中，您可以指定任何一项 Amazon VPC API 操作。每个操作名称都必须以小写字符串 `ec2:` 为前缀。例如：`ec2:CreateCustomerGateway`、`ec2:*VpnGateway*`、`ec2:*`（适用于所有 Amazon

VPC 和 Amazon EC2 操作）。有关 Amazon VPC 操作的列表，请参阅 *Amazon Elastic Compute Cloud API Reference* 中的 Actions。

Amazon VPC 策略密钥

您可以在 IAM 策略中指定控制策略生效时间的条件。每个条件都包含一个或多个密钥值对。AWS 定义条件和密钥，各项服务可以定义其他针对特定服务的密钥。

Amazon EC2 实施 AWS 范围内的策略密钥，但没有针对特定服务的策略密钥。

有关 AWS 范围内的策略密钥，请参阅 *Using IAM* 中的 Available Keys。

Amazon VPC 的示例策略

此部分将展示您可以使用 JSON 和 AWS 管理控制台定义的 IAM 策略示例。此外，此部分还将讨论您可以和不可以进行的操作，以及如何应对当前的限制。

管理 VPC

以下是您可以为需要创建和管理您的 VPC 的网络管理员组提供的策略示例。此策略允许组访问与 VPC、子网、Internet 网关、客户网关、虚拟专用网关、VPN 连接、路由表、弹性 IP 地址、安全组、网络 ACL 以及 DHCP 选项集相关的 API 操作。策略还会允许组运行、停止、开始和终止示例。此操作可允许组显示账户的资源。有关适用于 Amazon EC2 和 Amazon VPC 的可行操作完整列表，请访问Amazon Elastic Compute Cloud API Reference。

Note

策略使用通配符（例如`*SecurityGroup*`）指定适用于不同类别目标的所有操作。您也可以明确地列出每项操作。如果您使用通配符，请注意如果我们在策略中添加任何名称包含在通配符字符串内的新操作，策略将自动允许组访问这些新增操作。

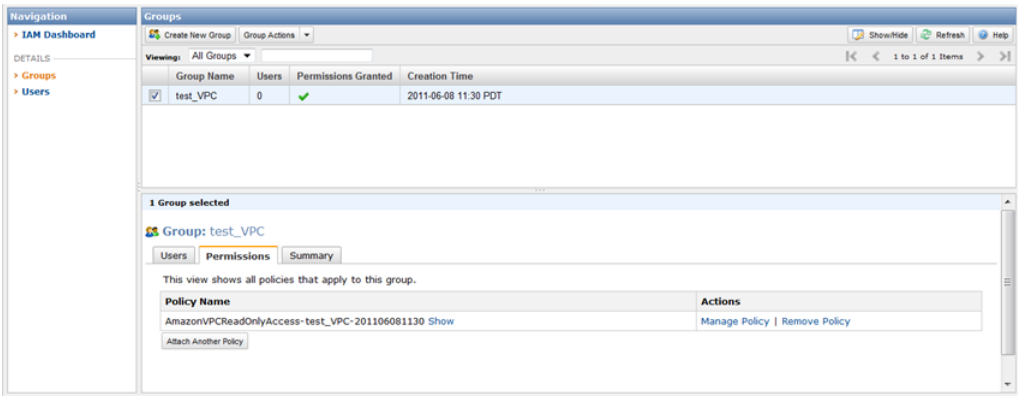
使用 JSON 管理 VPC

- 使用以下示例代码 – 根据需要将“*”通配符替换为具体操作，例如“create”、“delete”、“describe”等。

```
{
    "Statement":[{
    "Effect":"Allow",
    "Action":["ec2:*Vpc*",
              "ec2:*Subnet*",
              "ec2:*Gateway*",
              "ec2:*Vpn*",
              "ec2:*Route*",
              "ec2:*Address*",
              "ec2:*SecurityGroup*",
              "ec2:*NetworkAcl*",
              "ec2:*DhcpOptions*",
              "ec2:RunInstances",
              "ec2:StopInstances",
              "ec2:StartInstances",
              "ec2:TerminateInstances",
              "ec2:Describe*"],
    "Resource":"*"
    }
  ]
  }
```

使用 AWS 管理控制台管理 VPC

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. 在导航窗格中，单击“Groups”，然后选择相应的 IAM 组，向其授予您的 VPC 的完全访问权限。
3. 在底部窗格中，进入Permissions选项卡然后单击Manage Policy。



4. 在管理组许可页面中，在“Policy Name”下拉菜单中，选择“AmazonVPCFullAccess”然后单击“Apply Policy”。

Note

如果您仅希望向您的用户开放一个子集的策略权限，您可以编辑“Policy Document”方框中的列表，然后单击“Apply Policy”。

Amazon VPC 的只读策略

在下方的策略中，您给予用户许可，以在 AWS 管理控制台中查看 Amazon VPC 控制台。他们不可进行任何更改；他们只可以查看与您的 VPC 及其组成部分相关的信息。

使用 JSON 对您的 VPC 授予只读访问权限

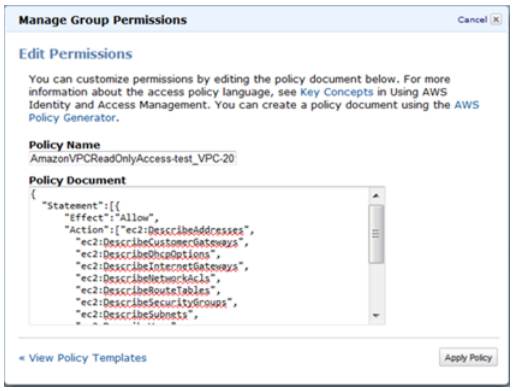
- 使用以下示例代码以允许组查看关于您的 VPC 的信息。

```
{
    "Statement":[{
    "Effect":"Allow",
    "Action":["ec2:DescribeVpcs",
              "ec2:DescribeSubnets",
              "ec2:DescribeInternetGateways",
              "ec2:DescribeCustomerGateways",
              "ec2:DescribeVpnGateways",
              "ec2:DescribeVpnConnections",
              "ec2:DescribeRouteTables",
              "ec2:DescribeAddresses",
              "ec2:DescribeSecurityGroups",
              "ec2:DescribeNetworkAcls",
              "ec2:DescribeDhcpOptions",
              "ec2:DescribeTags",
              "ec2:DescribeInstances"],
    "Resource":"*"
```

```
    }
  ]
}
```

使用 AWS 管理控制台对您的 VPC 授予只读访问权限

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. 在导航窗格中，单击“Groups”，然后选择相应的组，向其授予您的 VPC 的只读权限。
3. 在底部窗格中，进入“Permissions”选项卡然后单击“Manage Policy”。显示管理组许可页面。



4. 在“Policy Name”下拉菜单中，选择“AmazonVPCReadOnlyAccess”然后单击“Apply Policy”。

> **Note**
>
> 如果您仅希望向您的用户开放一个子集的策略权限，您可以编辑“Policy Document”方框中的列表，然后单击“Apply Policy”。

Amazon VPC 的自定义策略

您可以定制访问策略，以授予您的 VPC 用户。在下方的策略中，您给予一个用户组许可，以启动实例、以及显示可用的 Amazon EC2 和 Amazon VPC 资源。此策略可阻止用户对您的 VPC 布局、路由或安全性进行任何更改。

使用 JSON 授予启动您的 VPC 实例的权限

- 下方的策略允许组访问预期操作，同时拒绝组访问任何其他操作。用户可以启动实例、停止实例、开始实例、终止示例以及描述账户内的任何资源（即建立资源列表）。策略中的第二句可防止其他任何策略授予用户访问大部分 API 操作的权限。

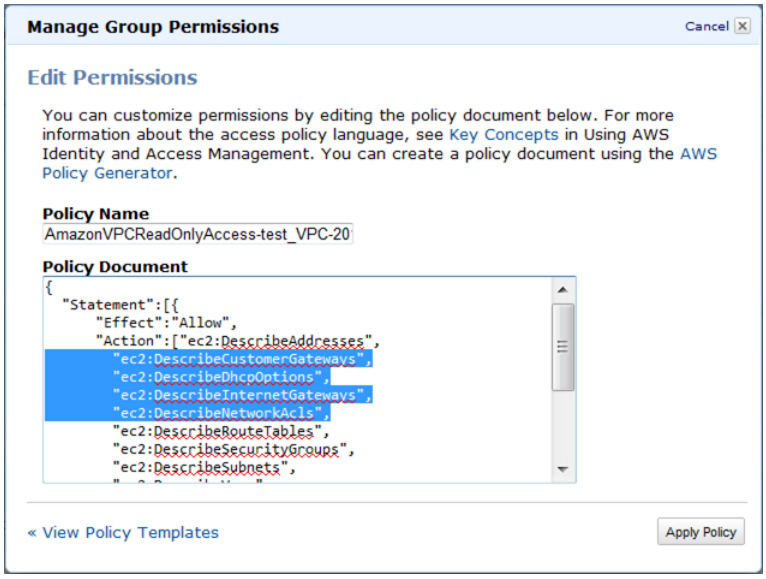
> **Note**
>
> 以下策略会阻止用户创建或在实例中添加 Amazon EBS 卷，或创建卷的快照。还可阻止弹性 IP 地址与实例相关联。如果用户需要这些功能，您可以在策略中添加相关的 API 操作。

```
{
  "Statement":[{
```

```
    "Effect":"Allow",
    "Action":["ec2:RunInstances",
              "ec2:StopInstances",
              "ec2:StartInstances",
              "ec2:TerminateInstances",
              "ec2:Describe*"],
     "Resource":"*"
     },
     {
     "Effect":"Deny",
     "NotAction":["ec2:RunInstances",
                  "ec2:StopInstances",
                  "ec2:StartInstances",
                  "ec2:TerminateInstances",
                  "ec2:Describe*"],
     "Resource":"*"
     }
  ]
}
```

使用 AWS 管理控制台授予启动您的 VPC 实例的权限

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. 在导航窗格中，单击“Groups”，然后选择相应的 IAM 组，向其授予您的 VPC 的已定义访问权限集。
3. 在底部窗格的“Permissions”选项卡中，单击“Manage Policy”。显示管理组许可页面。
4. 单击“View Policy Templates”，选择“Custom Policy”，然后单击“Select”。显示Manage Group Permissions页面。



Note

如果您希望仅向您的用户开放一个子集的策略权限，您可以编辑“Policy Document”方框中的列表，然后单击“Policy Document”。

您的 VPC 联网

您可以使用以下组件配置您的 VPC 网络化：

您的 VPC 中的 IP 地址

本主题将描述适用于您 VPC 中的 Amazon EC2 实例的 IP 地址。

公用和私有 IP 地址

您可以使用私有 IP 地址在 VPC 实例间进行通信。您可以使用公用 IP 地址在您的实例和 Internet 之间进行通信。

VPC 中的每个实例都有一个默认的网络接口，而且都分配了一个处于子网地址段内的主私有 IP 地址。如果您未指定主要私有 IP 地址，我们会在子网范围内为您选择可用的 IP 地址。有关网络接口的更多信息，请参阅 *Amazon Elastic Compute Cloud User Guide* 中的 Elastic Network Interfaces。

对于默认子网，我们会在您启动实例时为每个网络接口分配两个 IP 地址：主要私有 IP 地址和可通过网络地址转换 (NAT) 映射到主要私有 IP 地址的公有 IP 地址。

。如果您需要非默认子网中的实例与 Internet 通信，则必须为其分配一个弹性 IP 地址以在 VPC 中使用，然后将该 EIP 与私有 IP 地址（由连接至实例的网络接口指定）相关联。有关更多信息，请参阅 弹性 IP 地址 (p. 87)。

您可以为 VPC 中运行的实例指定其他 IP 地址（又被称为“次要私有 IP 地址”）。与主要私有 IP 地址不同，您可以将一个网络接口或实例的次要私有 IP 地址重新分配给另一个网络接口或实例。有关主要和次要 IP 地址的更多信息，请参见 *Amazon Elastic Compute Cloud User Guide* 中的 Multiple IP Addresses。

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 IP 地址。您可以将弹性 IP 地址与 VPC 中的任何实例或网络接口相关联。借助 EIP，您可以迅速将地址重新映射到 VPC 中的另一项实例，从而掩饰实例故障。请注意，将弹性 IP 地址与网络接口关联，而非直接与实例关联的优势在于，您通过一个步骤就可以将网络接口的所有属性从一个实例移动到另一个实例。

Topics

弹性 IP 地址基础信息

以下是您需要了解的关于弹性 IP 地址的基本信息:

- 首先分配一项 EIP 以便在 VPC 中使用，随后将其与 VPC 中的实例关联（每次仅可以将 EIP 指定给一个实例）。
- EIP 是网络接口的一项属性。您可以更新与实例相关联的网络接口，进而将 EIP 与实例相关联。
- 在 VPC 中使用的 EIP 与在 EC2-Classic 中使用的 EIP 并不相同。有关更多信息，请参阅 *Amazon Elastic Compute Cloud User Guide* 中的 Differences Between EC2-Classic and Amazon EC2-VPC。
- 您可以将EIP从一个实例移动到另一个。实例可以来自同一VPC或其他VPC，但不可来自EC2-Classic。
- 您的 EIP 会保留与您的 AWS 账户的关联，直至您明确解除 EIP 为止。
- 为确保 EIP 的有效使用，当这些 IP 地址未与运行的实例关联或它们关联到了已停止的实例或未连接的网络接口时，我们将强制收取小额的小时费用。当您的实例正在运行时，对于与该实例相关的一项EIP您无需支付相关费用，但对于其他与实例相关的 EIP 您则应承担相关费用。
- 您仅可以拥有 5 个弹性 IP 地址；为保存这些弹性 IP 地址，您可以使用 NAT 实例（参见NAT 实例 (p. 104)）。

使用弹性 IP 地址

您可以分配弹性 IP 地址，并随后将其与 VPC 中的实例相关联。

分配弹性 IP 地址以在 VPC 中使用

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Elastic IPs”。
3. 单击“Allocate New Address”按钮。
4. 从“EIP used in”列表中，选择 VPC 并单击“Yes, Allocate”。

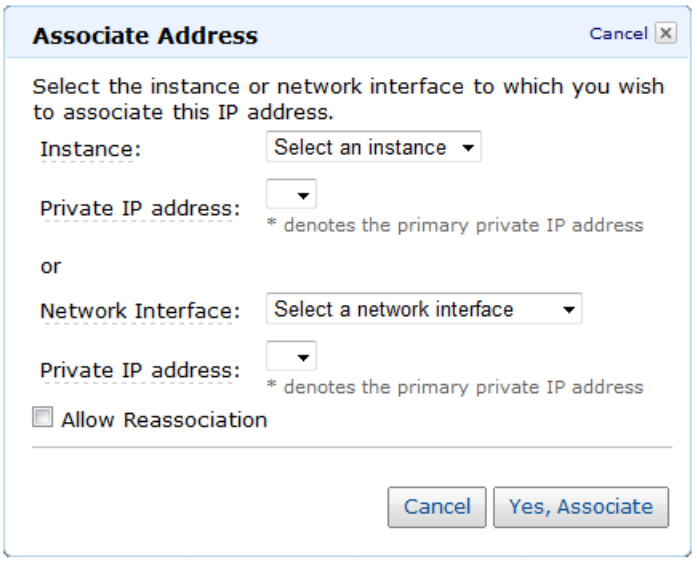
查看您的 EIP

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Elastic IPs”。
3. 如需过滤显示列表，您可以在搜索方框中输入指定给实例的部分 EIP 或 ID。

将弹性 IP 地址与运行的 VPC 实例相关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Elastic IPs”。

3. 选择弹性 IP 地址，然后单击“Associate Address”。
4. 在“Associate Address”对话框的“Network Interface”列表中选择网络接口，或从“Instance”列表中选择实例。从相应的“Private IP Address”列表中选择要与 EIP 关联的地址，然后单击“Yes, Associate”。



5. （可选）如果 DNS 主机名称已启用，则您将弹性 IP 地址与您的实例关联后，将获得一个 DNS 主机名称。有关更多信息，请参阅 在您的 VPC 中使用 DNS (p. 113)。

如需更改与弹性 IP 地址相关联的实例，您可撤销该地址与目前实例的关联，并随后将其关联到 VPC 中的新实例。

撤销弹性 IP 地址的关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Elastic IPs”。
3. 选择弹性 IP 地址，然后单击“Disassociate Address”。
4. 在出现提示时，单击“Yes, Disassociate”。

如果您不再需要弹性 IP 地址，我们建议您解除此弹性 IP 地址（地址不可与实例相关联）。对于被分配在 VPC 中使用、却未与实例相关联的 EIP，您也需承担相应费用。

解除弹性 IP 地址

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Elastic IPs”。
3. 选择弹性 IP 地址，然后单击按钮。
4. 在出现提示时，单击“Yes, Release”。

API 和命令概览

下表概述了适用于弹性 IP 地址的命令和 API 操作。

描述	命令	API 操作
获取弹性 IP 地址，以与您的实例一同使用。	ec2-allocate-address	AllocateAddress
将弹性 IP 地址与实例或网络接口相关联	ec2-associate-address	AssociateAddress
显示并描述一项或多项弹性 IP 地址。	ec2-describe-addresses	DescribeAddresses
解除弹性 IP 地址和与其相关的实例或网络接口的关联	ec2-disassociate-address	DisassociateAddress
解除分配给您的 AWS 账户的弹性 IP 地址。	ec2-release-address	ReleaseAddress

在您的 VPC 中使用弹性网络接口

在您的 VPC 中的每项实例都有一个默认的网络接口，并会被指定一个属于您的 VPC IP 地址范围内的私有 IP 地址。您可以为 VPC 内的任何实例创建和连接其他网络接口，即“弹性网络接口”(ENI)。您可以连接的 ENI 数目根据实例类型有所不同。有关更多信息，请参见*Amazon Elastic Compute Cloud User Guide*中的Private IP Addresses Per ENI Per Instance Type部分。

ENI 是包含以下属性的虚拟网络接口：

- 主要私有 IP 地址
- 一个或多个次要私有 IP 地址
- 弹性 IP 地址
- MAC 地址
- 一个或多个关联安全组
- 源/目标检查标记
- 描述

您可以创建 ENI，将其连接到一项实例，将其与实例断开以及再次连接到其他实例。ENI 属性会跟随 ENI 与一项实例连接或断开，以及再次连接到另一项实例而变化。当您将一个 ENI 从一项实例移动到另一项实例时，网络流量也会被重新导向新的实例。

当您希望进行以下操作时，您可以为一项实例连接多个 ENI：

- 创建管理网络。
- 在您的 VPC 中使用网络和安全性设备。
- 创建双归属实例，并在不同子网间分配工作负载/任务。
- 创建低预算、高可用性的解决方案。

有关 ENI、以及在 Amazon EC2 控制台中使用 ENI 的分步骤说明的更多信息，请参见*Amazon Elastic Compute Cloud User Guide*的Elastic Network Interfaces部分。

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。

在您的 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。您可以为同一个路由表关联多个子网，但是您仅可以为一个子网关联一个路由表。

Topics

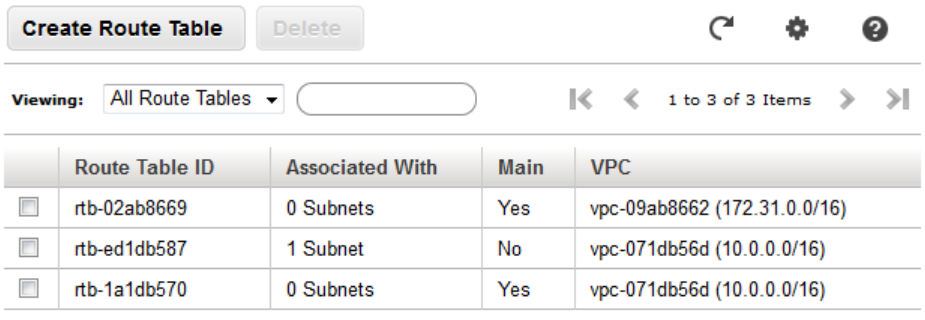
路由表基本信息

以下是您需要了解的关于路由表的基本信息：

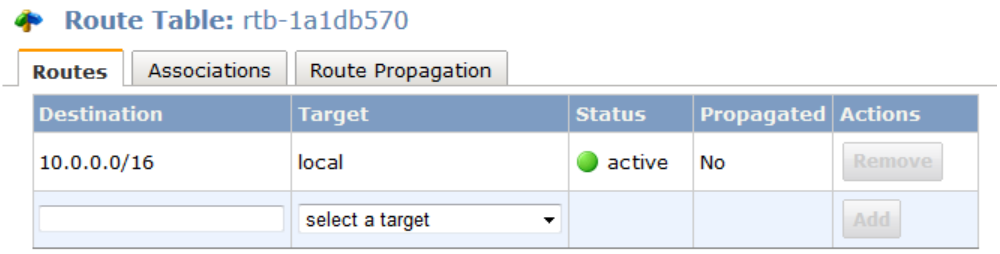
- 您的 VPC 有一个隐式路由器。
- 您的 VPC 会自动生成主路由表，以供您修改。
- 您可以为您的 VPC 创建额外的自定义路由表。
- 每个子网必须与一个路由表关联，这个路由表控制子网的路由。 如果您未在子网与特定路由表间建立显式关联，这个子网将使用主路由表。
- 您可以将主路由表替换为您创建的自定义路由表（以使这个路由表成为默认路由表，并可与每个新增子网存在关联）。
- 路由表中的每项路由都指定了一个目的 CIDR 和目标（例如，指向 172.16.0.0/12 的数据流将通向虚拟专用网关）；我们使用与数据流匹配的最明确路由以判断数据流的路由方式。

主路由表

当您创建 VPC 时，它会自动生成主路由表。 下方来自 VPC 控制台的图表展示了每个 VPC 的主路由表（Main一栏为Yes）。



最初，主路由表（以及VPC中的每一项路由表）中仅会包含一项路由：可启动VPC内通信的本地路由。

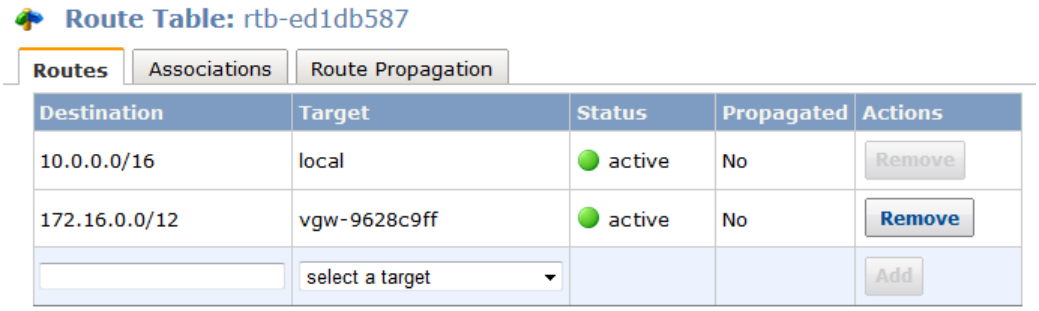


您无法修改路由表中的本地路由。无论您何时在 VPC 中启动实例，本地路由都会自动应用到这个实例；您无需在路由表中添加新的实例。

如果您未在子网与路由表间建立显式关联，这个子网将与主路由表建立隐式关联。但是，您仍可以在子网与主路由表间建立显式关联。如果您更改了作为主路由表的路由表，您可以进行此操作（参见正在替换主路由表 (p. 98)）。

控制台会显示出与每个路由表关联的子网数目。只有显式关联会被包含在这个编号中（参见正在判断与表显式关联的子网 (p. 95)）。

当您在 VPC 中添加一个网关时（无论是 Internet 网关还是虚拟专用网关），您必须为任何使用此网关的子网更新路由表。例如，下图显示了对主路由表的更新，以将数据流路由到虚拟专用网关。



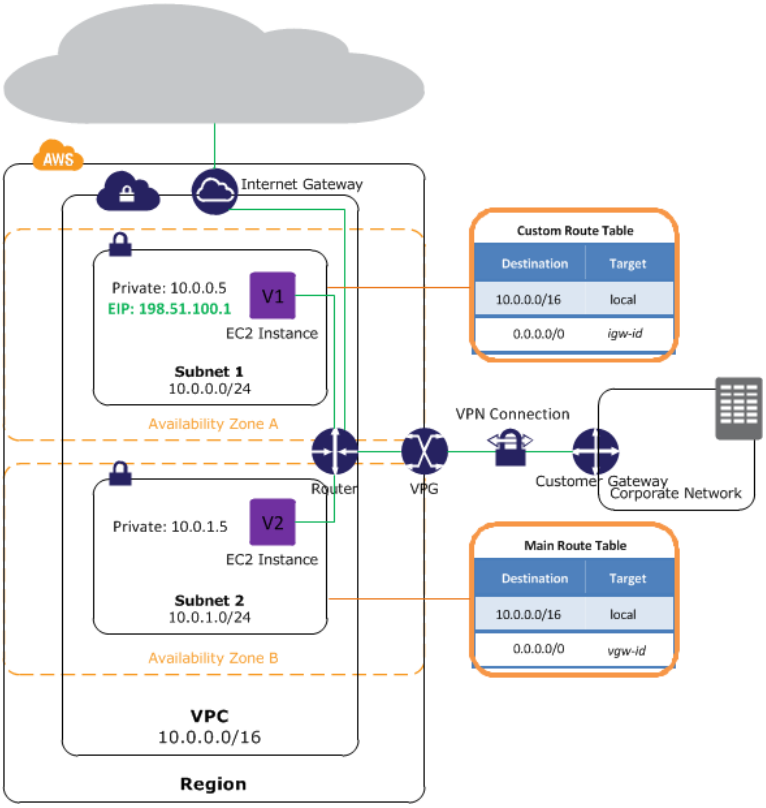
如果您已经将一个虚拟专用网关与您的 VPC 相连，并且启用了路由表中的路由传播，代表您的 VPN 连接的路由会在您的路由表的路由列表中自动显示为已传播路由。

自定义路由表

除了默认路由表之外，您的 VPC 还可以有其他路由表。保护您的 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），并将您创建的每个新建子网与您已经创建的自定义路由表之一建立显式关联。这样可以确保您能够明确地控制每个子网的出站数据流的路由方式。

有关您可以创建的路由表数目限制的信息，请参见Amazon VPC 限制 (p. 135)。

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。公有子网（子网 1）有一个自定义路由表。自定义路由表内包含公有子网的 Internet 网关路由（目的地为 0.0.0.0/0，目标为 Internet 网关）。



如果您在此 VPC 内创建一个新的子网，它将自动与主路由表关联，而主路由表会将数据流路由到虚拟专用网关。 如果您设置反向配置（主路由表内包含通往 Internet 网关的路由，自定义路由表内包含通往虚拟专用网关的路由），并且如果您创建了一个新子网，这个子网会自动生成通往 Internet 网关的路由。

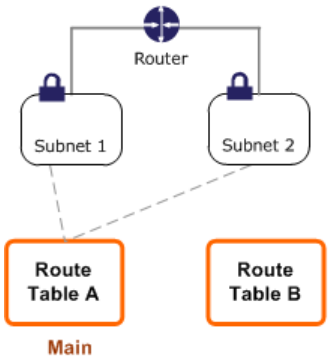
路由表关联

主路由表是子网使用的默认路由表（如果它们位于另一个路由表有显式关联）。当您添加新的子网时，它会自动使用在主路由表中指定的路由。您可以更改作为主路由表的路由表，并随之更改额外新增子网的默认设置。

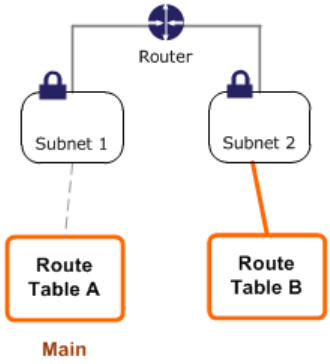
子网可以与主路由表建立显式或隐式关联。子网通常不会与主路由表建立显式关联，尽管当您替换主路由表时可能会临时生成显式关联。

您可以能想要更改主路由表，但是为避免使您的数据流出现中断，您决定首先使用自定义路由表测试路由更改。 当您满意测试结果之后，您便可以将主路由表替换为新的自定义路由表。

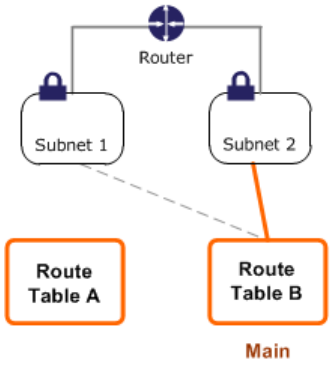
下图展示的是一个有两个子网的 VPC，并且这些子网都与主路由表（路由表 A）有隐式关联，自定义路由表（路由表 B）则未与任何子网相关。



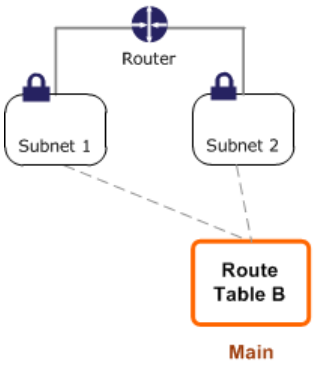
您可以在子网 2 和路由表 B 之间建立显式关联。



在您测试完路由表 B 之后，您可以将其设定为主路由表。请注意子网 2 仍与路由表 B 有显式关联，而子网 1 与路由表 B 有隐式关联，因为路由表 B 是新的主路由表。 路由表 A 已经不再使用。



如果您解除子网 2 与路由表 B 的关联，在子网 2 与路由表 B 之间仍将存在隐式关联。如果您不再需要路由表 A，您可以将其删除。



使用路由表

此部分将为您展示如何使用路由表。

Note

当您使用控制台向导创建带有网关的 VPC 时，向导会自动为您更新使用网关的路由表。如果您正在使用命令行工具或 API 来设置您的 VPC，您必须自行更新路由表。

Topics

正在判断与子网关联的具体路由表。

您可以在 Amazon VPC 控制台中查看子网的详细信息，以判断与子网关联的具体路由表。

判断与子网关联的路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的Subnets，然后选择子网。

   子网详细信息已显示在详细信息窗格中。与子网关联的路由表的 ID 已包含在详细信息之中（参见下图）。如果它是主路由表，控制台便无法表明关联为隐式或是显式。 如需判断与主路由表的关联是否为显式关联，请参见正在判断与表显式关联的子网 (p. 95)。

正在判断与表显式关联的子网

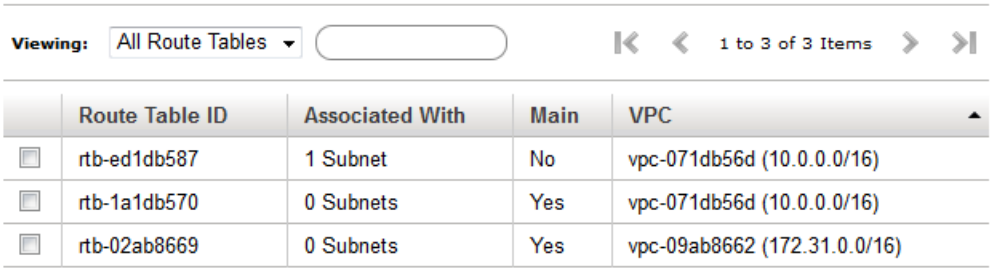
您可以判断与路由表显式关联的子网数目以及存在关联的具体子网。

主路由表可以有显式和隐式关联。 自定义路由表只有显式关联。

未与任何路由表建立显式关联的子网都与主路由表有隐式关联。您可以在子网和主路由表中建立显式关联（有关您为何建立显式关联的原因，请参见正在替换主路由表 (p. 98)）。

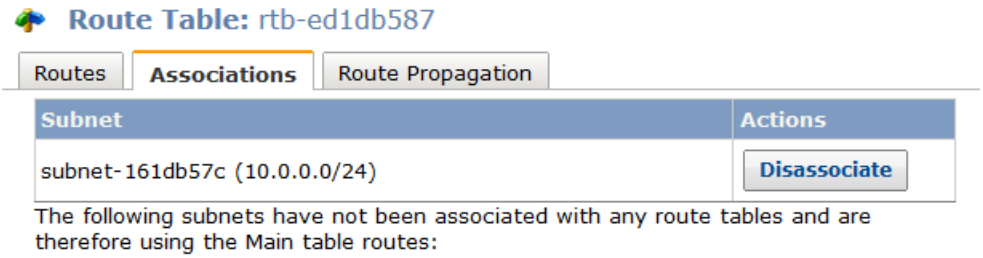
判断具有显式关联的子网数目

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的Route Tables。
   检查Associated With一栏以判断具有显式关联的子网的数目。



判断显式关联的子网

1. 选择适用的路由表。
2. 单击详细信息窗格中的Associations选项卡。与路由表有显式关联的子网已经列于选项卡之中。所有未与任何路由表关联的子网（并因此与主路由表隐式关联）也将被列出。



创建自定义路由表

根据您的具体情况，您可能需要创建自己的路由表。

创建自定义路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”。
3. 单击“Create Route Table”按钮。
4. 在“Create Route Table”对话框中，从VPC下拉列表中选择您的 VPC，然后单击“Yes, Associate”。

在路由表中添加和删除路由

您无法修改表中的路由；您仅可以添加和删除路由。

在路由表中添加路由

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 在详细信息窗格的“Routes”选项卡中，输入路由的目的地和目标，然后单击“Add”。
4. 在“Create Route”对话框中，单击“Yes, Associate”。

从路由表中删除路由

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 右击您要删除的路由，然后单击“Delete”。
4. 在“Delete Route”对话框中，单击“Yes, Delete”。

启用和禁用路由传播

路由传播允许虚拟专用网关自动传播路由至路由表，所以您便无需再手动向您的路由表中输入VPN路由。您可以启用或禁用路由传播。

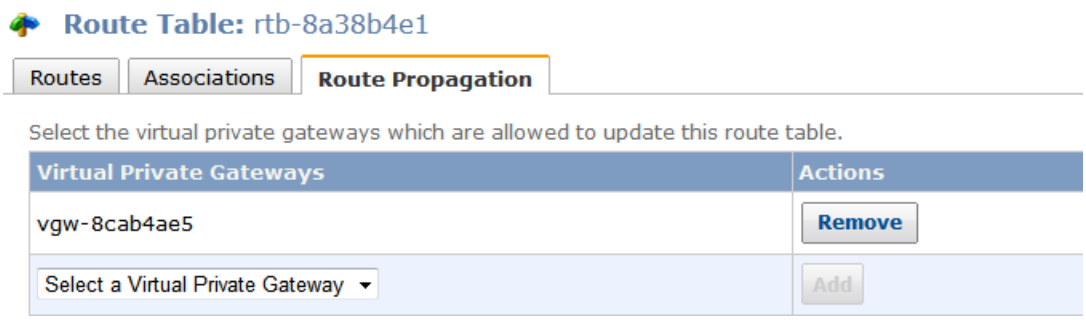
有关 VPN 路由选项的更多信息，请参见 VPN 路由选项 (p. 119)。

启用路由传播

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 在详细信息窗格中，单击“Route Propagation”选项卡。
4. 从下拉列表中选择虚拟专用网关，但后单击“Add”。

禁用路由传播

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 在详细信息窗格中，在“Route Propagation”选项卡中，在 VGW 的 ID 旁边，单击“Remove”。



4. 在“Remove Virtual Private Gateway”对话框中，单击“Yes, Disable”。

正在将子网与路由表关联

如需对特定子网应用路由表路由，您必须将路由表与子网关联。路由表可以与多个子网关联；但是一个子网仅可以与一个路由表关联。任何未与路由表显式关联的子网都默认与主路由表隐式关联。

将表与子网关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 在详细信息窗格中，在“Associations”选项卡中，选择与表关联的子网，并单击“Associate”。
4. 在“Associate Route Table”对话框中，单击“Yes, Associate”。

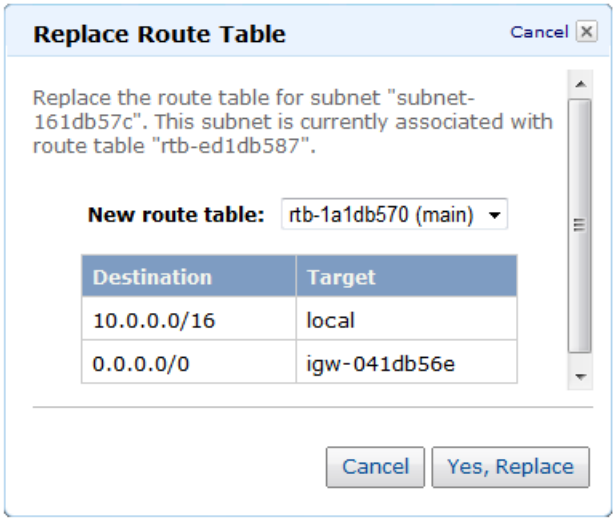
正在更改子网的路由表

您可以更改与子网关联的路由表。 例如，当您创建一个子网时，这个子网与主路由表为隐式关联。 您可能希望将其与您创建的自定义路由表关联。

更改子网的路由表关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Subnets”，然后选择子网。
3. 在详细信息窗格中，在与子网关联的路由表的 ID 旁边，单击“Replace”。

4. 在“Replace Route Table”对话框中，从“New Route Table”中选择与子网关联的路由表，然后单击“Yes, Replace”。



正在解除子网与路由表的关联

您可能希望解除子网与路由表的关联。例如，您可能有与自定义路由表关联的子网，但是您希望将其与主路由表关联。通过解除子网与自定义路由表的关联，子网与主路由表将变为隐式关联。

解除子网与路由表的关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”，然后选择路由表。
3. 在详细信息窗格中，选择“Associations”选项卡，并验证子网目前是否与路由表关联。
4. 单击“Disassociate”。
5. 在“Disassociate Route Table”对话框中，单击“Yes, Disassociate”。

正在替换主路由表

以下步骤描述如何更改作为您的 VPC 主路由表的路由表。

替换主路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”。
3. 查找您希望作为新的主路由表的路由表，右键单击表，然后选择“Set as Main Table”。
4. 在“Set Main Route Table”对话框中，单击“Yes, Set”。

以下步骤描述如何删除子网与主路由表之间的显式关联。结果是在子网和主路由之间生成隐式关联。这个步骤与解除任何子网与任何路由表的步骤相同。

删除与主路由表的显式关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”。
3. 选择主路由表，然后单击它的“Associations”选项卡。
4. 单击“Disassociate”。

5. 在“Disassociate Route Table”对话框中，单击“Yes, Disassociate”。

正在删除路由表

您只可以删除未与任何子网关联的路由表。您无法删除主路由表。

删除路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Route Tables”。
3. 选择路由表，然后单击“Delete”按钮。
4. 在“Delete Route Table”对话框中，单击“Yes, Delete”。

API 和命令概览

下表概述了可用路由表命令和相应的 API 操作。

描述	命令	API 操作
为您的 VPC 创建自定义路由表。	ec2-create-route-table	CreateRouteTable
描述您的一项或多项路由表	ec2-describe-route-tables	DescribeRouteTables
从 VPC 中删除一项路由表。	ec2-delete-route-table	DeleteRouteTable
在路由表中添加新的路由。	ec2-create-route	CreateRoute
从路由表中删除一项路由。	ec2-delete-route	DeleteRoute
替换路由表中的现有路由。	ec2-replace-route	ReplaceRoute
将子网与路由表关联	ec2-associate-route-table	AssociateRouteTable
解除子网与路由表的关联	ec2-disassociate-route-table	DisassociateRouteTable
更改与子网关联的路由表。同时更改作为主路由表的路由表。	ec2-replace-route-table-association	ReplaceRouteTableAssociation
启用虚拟专用网关 (VGW) 以将路由传播至 VPC 的路由表。	ec2-enable-vgw-route-propagation	EnableVgwRoutePropagation
禁止 VGW 传播路由到 VPC 的路由表。如果您禁用路由传播选项，您必须手动在路由表内输入与 VPN 连接关联的路由。	ec2-disable-vgw-route-propagation	DisableVgwRoutePropagation
创建与 VPN 连接相关的静态路由。	ec2-create-vpn-connection-route	CreateVPNConnectionRoute
删除与 VPN 连接关联的静态路由。	ec2-delete-vpn-connection-route	DeleteVPNConnectionRoute

在您的 VPC 中添加 Internet 网关

您的默认 VPC 带有一个 Internet 网关，而且默认情况下，在默认子网内启动的实例会获得一个公有 IP 地址。因此，您在默认子网中启动的实例可以自动与 Internet 通信。有关更多信息，请参阅 您的默认 VPC 和子网 (p. 51)。

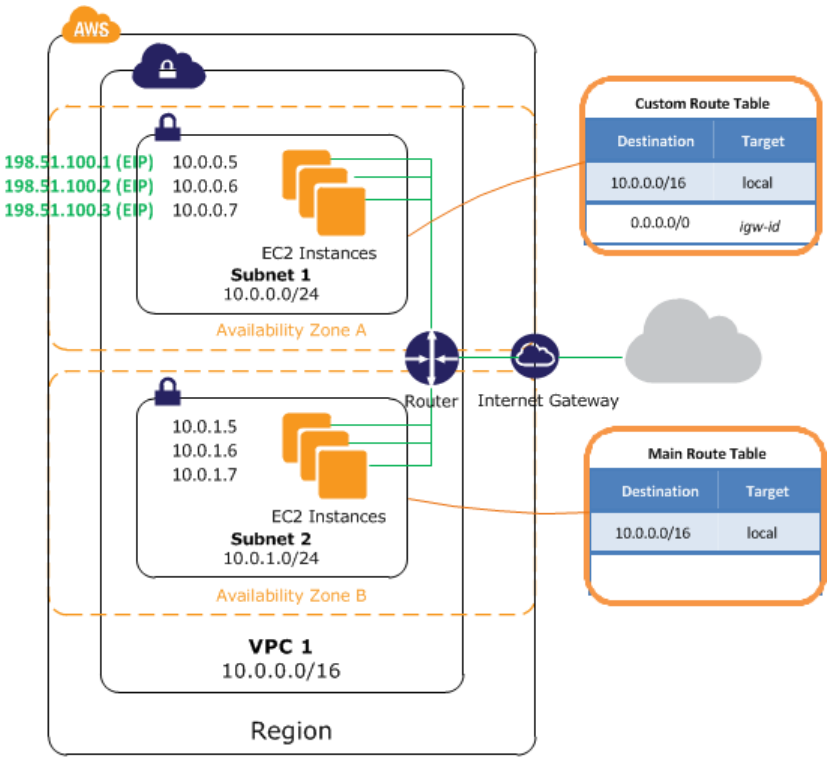
除非您在启动时特意分配了一个地址，否则默认情况下，在非默认子网中启动的实例不会获得公有 IP 地址，而且无法与 Internet 通信。您可以为在非默认子网内启动的实例启用 Internet 访问功能，步骤如下：为 VPC 连接 Internet 网关、创建自定义路由表、更新您的安全组规则以及为每项实例关联相应的弹性 IP 地址。

当您在 VPC 中添加新子网时，您必须为子网设置您需要的路由和安全性。您可以根据此页的描述，手动完成此步骤，或使用 VPC 向导以简化流程。例如，根据您选择的选项，VPC 向导会在您的 VPC 中添加一个 Internet 网关，并更新路由表，以使您的实例可以与 Internet 通信。有关使用 VPC 向导以创建有 Internet 网关的子网的更多信息，请参见情景 1：仅带公有子网的 VPC (p. 7)或情景 2：带有公有子网和私有子网的 VPC (p. 13)。

以下部分描述了如何手动设置子网，以支持 Internet 访问。

Topics

当您完成子网设置时，您的 VPC 便已如下图所示配置。



创建子网

为您的 VPC 添加子网

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Subnets”，然后单击“Create Subnet”。
3. 在“Create Subnet”对话框中，选择 VPC，选择可用区域，指定子网的 CIDR 范围，然后单击“Yes, Create”。

有关子网的更多信息，请参见您的 VPC 和子网 (p. 44)。

连接 Internet 网关

创建 Internet 网关，并将其连接至您的 VPC

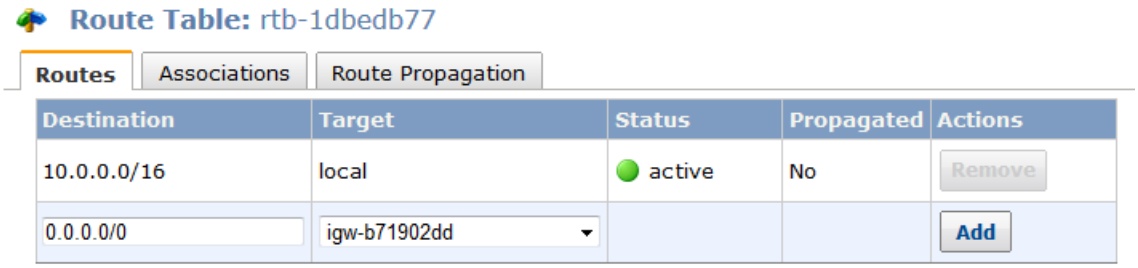
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Internet Gateways”，然后单击“Create Internet Gateway”。
3. 在“Create Internet Gateway”对话框中，单击“Yes, Create”。
4. 选择您刚刚创建的 Internet 网关，然后单击“Attach to VPC”。
5. 在“Attach to VPC”对话框中，从列表中选择您的 VPC，然后单击“Yes, Attach”。

创建自定义路由表

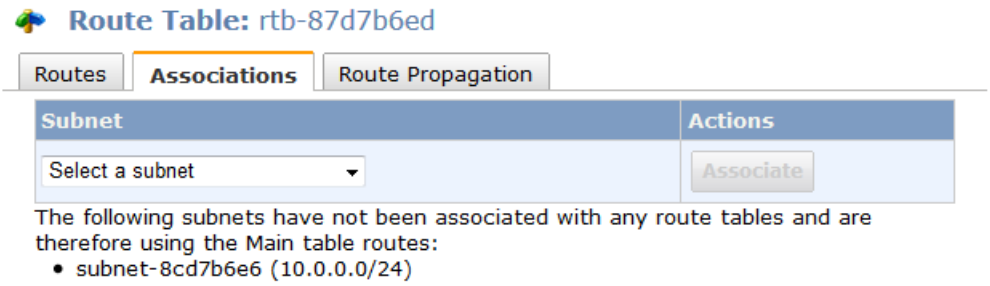
当您创建子网时，我们会自动将其与 VPC 的主路由表关联。主路由表在默认情况下不会包含通往 Internet 网关的路径。以下步骤为您演示如何创建自定义路由表，使其中有可以将目标为 VPC 外的数据流发送到 Internet 网关的路由，以及如何将自定义路由表与您的子网相关联。

创建自定义路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Route Tables”，然后单击“Create Route Table”。
3. 在“Create Route Table”对话框中，选择您的 VPC，然后单击“Yes, Create”。
4. 选择您刚刚创建的自定义路由表。详细信息窗格中会显示选项卡，以供您使用其路径、关联和路线传播。
5. 在“Routes”选项卡中，在“Destination”方框中指定`0.0.0.0/0`，从“Target”列表中选择 Internet 网关 ID，然后单击“Add”。



6. 在“Associations”选项卡中，选择子网的 ID，然后单击“Associate”。



有关路由表的更多信息，请参见路由表 (p. 89)。

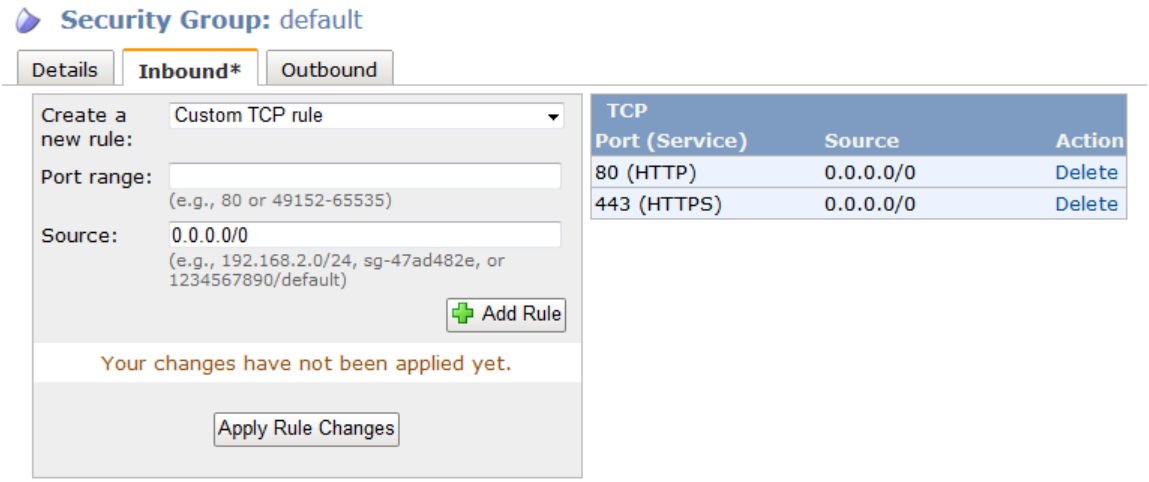
更新安全组规则

您的 VPC 带有默认的安全组。您在 VPC 中启动的每项实例都会自动与其默认安全组关联。默认安全组的默认设置不允许来自 Internet 的任何入站数据流量，但允许通往 Internet 的所有出站数据流量。因此，为使您的实例能够与 Internet 通信，您需要创建允许公用实例访问 Internet 的新安全组。

创建新的安全组，并将其与您的实例关联

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Security Groups”，然后单击“Create Security Group”。

3. 在“Create Security Group”对话框中，为您的安全组指定名称和描述。从VPC列表中选择您 VPC 的 ID，然后单击“Yes, Create”。
4. 选择安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
5. 在“Inbound”选项卡中，从“Create a new rule”列表中选择规则类型，填入所需的信息，然后单击“Add Rule”。例如，选择HTTP或HTTPS，并保留“Source”的设置为0.0.0.0/0。请注意“Apply Rule Changes”按钮已经启用，按钮上方将显示“Your changes have not been applied yet”文本。在添加完所有您需要的入站数据流规则之后，单击“Apply Rule Changes”以添加规则。



6. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
7. 在导航窗格中，单击“Instances”。
8. 右键单击实例，然后选择“Change Security Groups”。
9. 在“Change Security Groups”对话框中，从“Security Groups”列表中选择新的安全组，然后单击“Yes, Change”。

有关安全组的更多信息，请参见您的 VPC 的安全组 (p. 58)。

添加弹性 IP 地址

当您在子网中启动实例之后，若您希望可以从 Internet 中访问该实例，则必须为其分配一个 弹性 IP 地址。

To allocate an Elastic IP address and assign it to an instance

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

有关弹性 IP 地址的更多信息，请参见弹性 IP 地址 (p. 87)。

将 Internet 网关与您的 VPC 断开

如果您不再需要通过 Internet 访问在非默认 VPC 中启动的实例，则可将 Internet 网关与 VPC 断开。如果该 VPC 的某些实例具有关联的弹性 IP 地址，则无法断开 Internet 网关。

断开 Internet 网关

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 单击导航窗格中的 Elastic IPs。
3. 选择 IP 地址，单击“Disassociate Address”，然后单击“Yes, Disassociate”。
4. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
5. 单击导航窗格中的“Internet Gateways”。
6. 选择相应的 Internet 网关，然后单击“Detach from VPC”。
7. 在“Detach from VPC”对话框中的“VPC”列表中选择要断开的 VPC，然后单击“Yes, Detach”。

删除 Internet 网关

若您不再需要某一 Internet 网关，则可将其删除。您无法删除仍与 VPC 关联的 Internet 网关。

删除 Internet 网关

1. 选择相应的 Internet 网关，然后单击“Delete”。
2. 在“Delete Internet Gateway”对话框中，单击“Yes, Delete”。

API 和命令概览

下表概述了可用 Internet 网关命令和相应的 API 操作。

描述	命令	API 操作
将 Internet 网关与指定 VPC 关联。	ec2-attach-internet-gateway	AttachInternetGateway
创建一个与 VPC 配合使用的新 Internet 网关。	ec2-create-internet-gateway	CreateInternetGateway
从您的 AWS 账户中删除一个 Internet 网关。	ec2-delete-internet-gateway	DeleteInternetGateway
描述您的一个或多个 Internet 网关。	ec2-describe-internet-gateways	DescribeInternetGateways
将 Internet 网关与指定的 VPC 断开。	ec2-detach-internet-gateway	DetachInternetGateway

NAT 实例

您在 Virtual Private Cloud (VPC) 内的私有子网内启动的实例无法与 Internet 通信。您可以选择使用在您的 VPC 的公有子网内的网络地址转换 (NAT) 实例来启动私有子网中的实例，以启动到 Internet 的出站数据流，以及拒绝接收由 Internet 中其他用户启动的入站数据流。

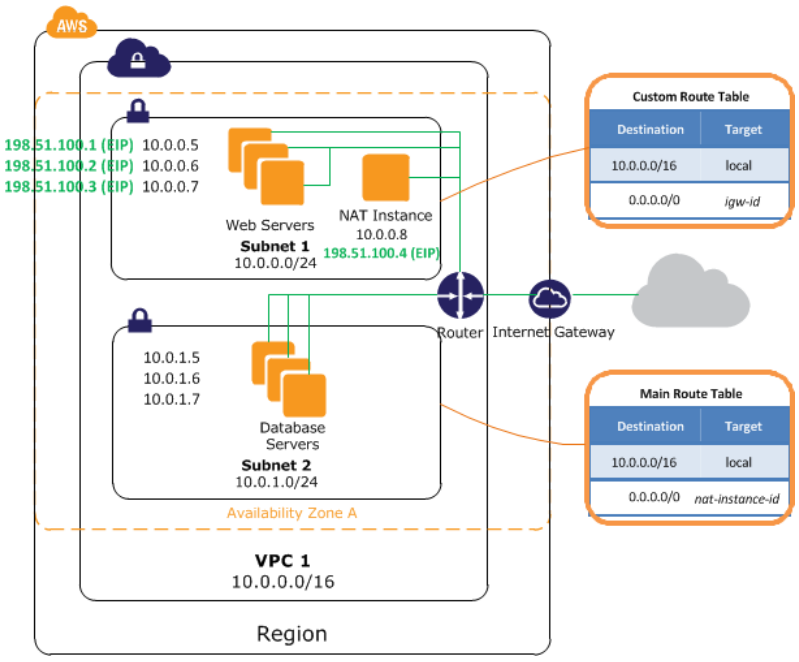
Note

我们使用术语*NAT 实例*；但是，NAT 实例的主要任务实际则是进行端口地址转换 (PAT)。我们选择使用更广为人知的术语“NAT”。有关 NAT 和 PAT 的更多信息，请参见Wikipedia article about network address translation。

Topics

NAT 实例基本信息

下图展示了 NAT 实例的基本信息。主路由表可将流量从私有子网中的实例发送到公有子网中的 NAT 实例中。NAT 实例可将流量发送到 VPC 的 Internet 网关。流量由 NAT 实例的弹性 IP 地址产生。NAT 实例为响应指定了一个较高的端口号；响应返回后，NAT 实例会根据响应的端口号将其发送给私有子网中的相应实例。



有关 VPC 和子网总体概览，请参见Amazon VPC 是什么？ (p. 1)。

设置 NAT 实例

您可以使用 VPC 向导以设置有 NAT 实例的 VPC；有关更多信息，请参见情景 2：带有公有子网和私有子网的 VPC (p. 13)。或者，您也可以根据以下步骤手动设置 NAT 实例：

1. 创建带有两个子网的 VPC。

a. 创建 VPC（参见 正在创建 VPC (p. 46)）
b. 创建两个子网（参见 创建子网 (p. 101)）
c. 将 Internet 网关与一个子网关联（参见 连接 Internet 网关 (p. 101)），使其成为公有子网
d. 为公有子网创建一个自定义主路由表（参见 创建自定义路由表 (p. 102)）

2. 创建 NATSG 安全组（参见正在创建 NATSG 安全组 (p. 107)）。您应在启动 NAT 实例时指定此安全组。
3. 将实例从已经配置为作为 NAT 实例运行的 AMI 推送到您的公有子网。Amazon 提供 Amazon Linux AMI，并会将其配置作为 NAT 实例运行。这些 AMI 在名称中包含`ami-vpc-nat`字符串，因此您可以在 AWS 管理控制台中进行搜索。

   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. 单击导航窗格中的“Instances”。
   c. 单击“Launch Instance”按钮。
   d. 在创建新实例页面中，单击“Quick Launch Wizard”。按以下说明完成向导。

      i. 为您的 NAT 实例指定一个名称。
      ii. 选择或创建一个密钥对。
      iii. 在“Choose a Launch Configuration”下，选择“More Amazon Machine Images”，然后单击“Continue”。
      iv. 在“Public AMIs”选项卡中，搜索 `ami-vpc-nat`。从结果列表中选择一个 NAT AMI，然后单击“Continue”。
      v. 单击“Edit Details”。
      vi. 在“Instance Details”下，选择“Launch into a VPC”并指定您的公有子网。
      vii. 在“Security Settings”下，选择已创建的 NATSG 安全组，然后单击“Save Details”。
      viii. 检视您已经选择的设置。根据需要进行更改，然后单击“Launch”。

4. [可选]登录 NAT 实例，根据您的需要进行修改，然后创建您自己的 AMI，对其进行配置，以作为 NAT 实例运行。您可以在下次您需要启动 NAT 实例时使用此 AMI。有关创建您自己的 AMI 的更多信息，请参见*Amazon Elastic Compute Cloud User Guide*的Creating Amazon EBS-Backed AMIs部分。

   Note

   Amazon Linux AMI 登录是`ec2-user`，而不是`root`。

5. 禁用 NAT 实例的`SrcDestCheck`属性（参见正在禁用源/目标检查 (p. 108)）
6. 将弹性 IP 地址与 NAT 实例相关联。

   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. 单击导航窗格中的“Elastic IPs”。
   c. 单击“Allocate New Address”按钮。
   d. 在“Allocate New Address”对话框中，从“EIP used in”列表中选择VPC，但后单击“Yes, Allocate”。
   e. 从列表中选择弹性 IP 地址，然后单击“Associate Address”按钮。
   f. 在“Associate Address”对话框中，选择 NAT 实例的网络接口。从“Private IP Address”列表中选择与 EIP 相关联的地址，然后单击“Yes, Associate”。

7. 更新主路由表以将流量发送至 NAT 实例。有关更多信息，请参阅 更新主路由表 (p. 108)。

正在创建 NATSG 安全组

根据下表的描述定义 NATSG 安全组，以允许您的 NAT 实例从私有子网实例接收 Internet 绑定的数据流、以及来自您的网络 SSH 数据流。NAT 实例也可以向 Internet 发送数据流，即允许私有子网中的实例接收软件更新。

NATSG：推荐规则

入站			
源	协议	端口范围	注释
10.0.1.0/24	TCP	80	允许来自私有子网服务器的入站 HTTP 数据流
10.0.1.0/24	TCP	443	允许来自私有子网服务器的入站 HTTPS 数据流
您的网络的公有 IP 地址范围	TCP	22	允许从您的网络对 NAT 实例进行入站 SSH 访问（通过 Internet 网关）
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许对 Internet 的出站 HTTP 访问
0.0.0.0/0	TCP	443	允许对 Internet 的出站 HTTP 访问

创建 NATSG 安全组

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Security Groups”。
3. 单击“Create Security Group” 按钮。
4. 在“Create Security Group”对话框中，指定NATSG作为安全组的名称，并提供描述。从VPC列表中选择您的 VPC 的 ID，然后单击“Yes, Create”。
5. 选择您刚刚创建的 NATSG 安全组。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
6. 如下所示使用“Inbound”选项卡添加入站数据流规则：
   a. 从“HTTPCreate a new rule”列表中选择 。在“Source”方框中，指定您的私有子网的 IP 地址范围，然后单击“Add Rule”。
   b. 从“HTTPSCreate a new rule”列表中选择 。在“Source”方框中，指定您的私有子网的 IP 地址范围，然后单击“Add Rule”。
   c. 从“SSHCreate a new rule”列表中选择 。在“Source”方框中，指定您的网络的公有 IP 地址范围，然后单击“Add Rule”。
   d. 单击“Apply Rule Changes”。
7. 如下所示使用“Outbound”选项卡添加出站数据流规则：
   a. 从“HTTPCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。
   b. 从“HTTPSCreate a new rule”列表中选择 。确保“Destination”一项为0.0.0.0/0，然后单击“Add Rule”。

c. 单击“Apply Rule Changes”。

有关安全组的更多信息，请参阅 您的 VPC 的安全组 (p. 58)。

正在禁用源/目标检查

每项 EC2 实例都会默认执行源/目标检查。这意味着实例必须为其发送或接收的数据流的源头或目标。但是，NAT 实例必须能够在源或目标并非其本身时发送和接收数据流。因此，您必须禁用 NAT 实例的源/目标检查。

按照以下步骤禁用正在运行或已经停止的 NAT 实例的`SrcDestCheck`属性。

To disable source/destination checking on a NAT instance

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Click Instances in the navigation pane.
3. Right-click the NAT instance, and then select Change Source / Dest Check.
4. For a NAT instance, this attribute should be disabled. Click Yes, Disable.

更新主路由表

按照以下程序中的说明更新主路由表。默认情况下，主路由表使您的 VPC 中的实例能够互相通信。我们将添加一个路由，将所有子网发送至 NAT 实例。

更新主路由表

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 为您的 VPC 选择主路由表。详细信息窗格中会显示选项卡，以供您使用其路径、关联和路线传播。
3. 在“Routes”选项卡中，从“Destination”框中指定 `0.0.0.0/0`，在“Target”框中指定 NAT 实例的实例 ID，然后单击“Add”。
4. 在“Associations”选项卡中，选择子网的 ID，然后单击“Associate”。

有关路由表的更多信息，请参见路由表 (p. 89)。

API 和命令概览

下表概述了可用的 EC2 实例以及与 NAT 实例相关的 API 操作。

描述	命令	API 操作
启用或禁用 EC2 实例的`SrcDestCheck`属性，以判断是否可以执行网络地址转换 (NAT)。	ec2-modify-instance-attribute	ModifyInstanceAttribute

DHCP 选项集

此主题将描述 DHCP 选项集以及如何为您的 VPC 指定 DHCP 选项集。

Topics

DHCP 选项集概述

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 选项集与您的 AWS 账户相关联，因此您可以在所有 Virtual Private Cloud (VPC) 内使用这些选项。

您在非默认 VPC 内启动的 Amazon EC2 实例属于私有实例；它们未分配公有 IP 地址，。AWS 会为非默认 VPC 中的所有实例默认分配一个无法解析的主机名称（例如，ip-10-0-0-202）。您可以为您的实例指定您自己的域名，并可最多使用四个您自己的 DNS 服务器。如需完成此操作，您必须指定特别 DHCP 选项集，以在 VPC 中使用。这种选项集中可以包含其他常用的 DHCP 选项（参阅下表以了解支持选项的完整列表）。有关这些选项的更多信息，请参见RFC 2132。

DHCP Option Name	Description
domain-name-servers	The IP addresses of up to four domain name servers, or AmazonProvidedDNS. The default DHCP option set specifies AmazonProvidedDNS.
domain-name	If you're using AmazonProvidedDNS in US East (Northern Virginia) Region, specify compute-1.amazonaws.com. If you're using AmazonProvidedDNS in another region, specify *region*.compute.amazonaws.com. Otherwise, specify a domain name (for example, `MyCompany.com`).
ntp-servers	The IP addresses of up to four Network Time Protocol (NTP) servers.
netbios-name-servers	The IP addresses of up to four NetBIOS name servers.
netbios-node-type	The NetBIOS node type (1, 2, 4, or 8). We recommend that you specify 2 (broadcast and multicast are not currently supported). For more information about these node types, see RFC 2132.

Amazon DNS 服务器

当您创建 VPC 时，我们会自动创建 DHCP 选项集，并将它们与 VPC 相关联。这个选项集中只包含一个选项：`domain-name-servers=AmazonProvidedDNS`。这是 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 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。

Note

您还可以使用 Amazon DNS 服务器 IP 地址 169.254.169.253，尽管部分服务器不允许其使用。例如，Windows Server 2008 禁止使用位于 169.254.x.x 网络范围内的 DNS 服务器。

更改 DHCP 选项

在您创建 DHCP 选项集之后，您便无法再修改这些选项。如果您希望 VPC 使用不同的 DHCP 选项集，您必须创建新的选项集，并将其与您的 VPC 相关联。您还可以设置 VPC，让其不使用任何 DHCP 选项。

您可以有多个 DHCP 选项集，但每次您仅可以将一个选项集与 VPC 相关联。如果您删除 VPC，与该 VPC 相关联的 DHCP 选项集也会被随之删除。

在您将新的 DHCP 选项集与 VPC 关联之后，任何现有实例以及您在 VPC 内启动的所有新增实例都将使用这些选项。 You don't need to restart or relaunch the instances. They automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. If you want, you can explicitly renew the lease using the operating system on the instance.

使用 DHCP 选项集

此部分将为您展示如何使用 DHCP 选项集。

Topics

正在创建 DHCP 选项集

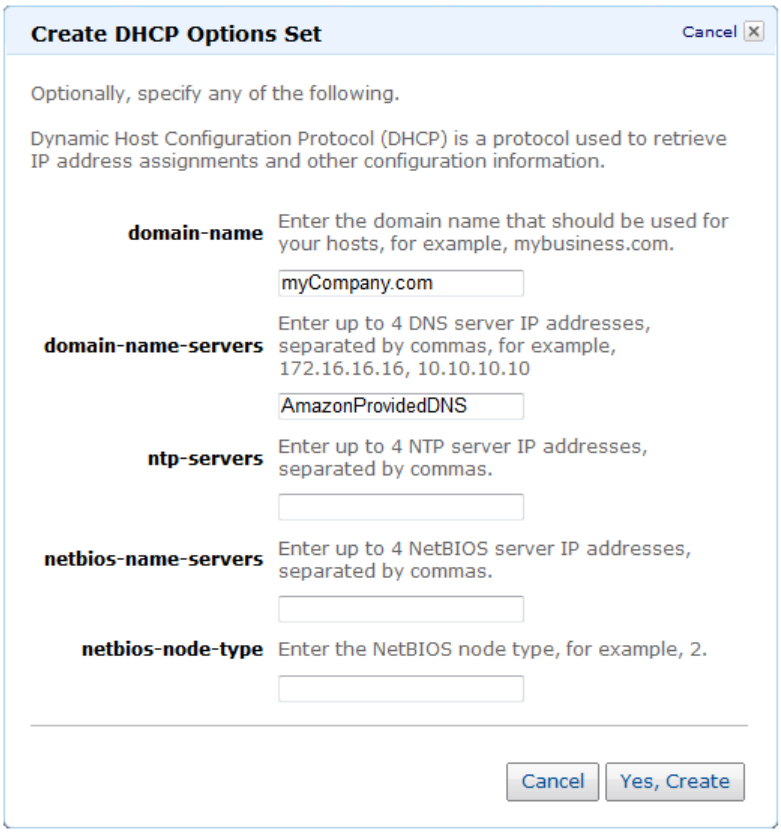
您可以根据需要，任意创建额外 DHCP 选项集。但是，每次您仅可以将一个 DHCP 选项集与一个 VPC 相关联。在您创建 DHCP 选项集之后，您必须配置使用这些选项的 VPC。有关更多信息，请参见 更改 DHCP 选项集以供 VPC 使用 (p. 111)。

创建 DHCP 选项集

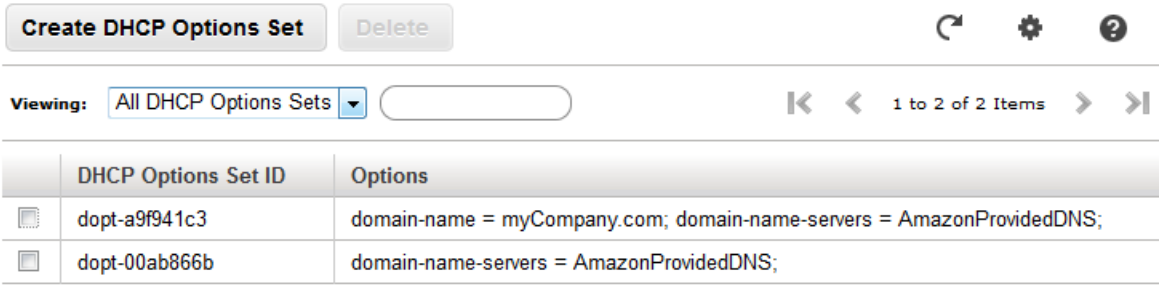
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“DHCP Options Set”，然后单击“Create DHCP Options Set”按钮。
3. 在“Change DHCP Options Set”对话框内，输入您希望使用的选项值，然后单击“Yes, Create”。

Important

如果您的 VPC 有 Internet 网关，确保指定您自己的 DNS 服务器或 Amazon 的 DNS 服务器 (AmazonProvidedDNS) 作为domain-name-servers值。否则，需要使用 Internet 通信的实例将无法访问 DNS。



新的 DHCP 选项集会出现在您的 DHCP 选项列表中。下图中便是此类列表示例，图中展示了您刚刚创建的 DHCP 选项集以及与您的 VPC 一同自动生成的选项集（其中的唯一选项便是 domain-name-servers=AmazonProvidedDNS）。



4. 记录新增 DHCP 选项集的 ID (dopt-*xxxxxxxx*)。您需要利用它将您的新增选项集和 VPC 相关联。

尽管您已经创建了 DHCP 选项级，您必须将其与您的 VPC 相关联，以使选项生效。您可以创建多个 DHCP 选项集，但每次您仅可以将一个选项集与 VPC 相关联。

更改 DHCP 选项集以供 VPC 使用

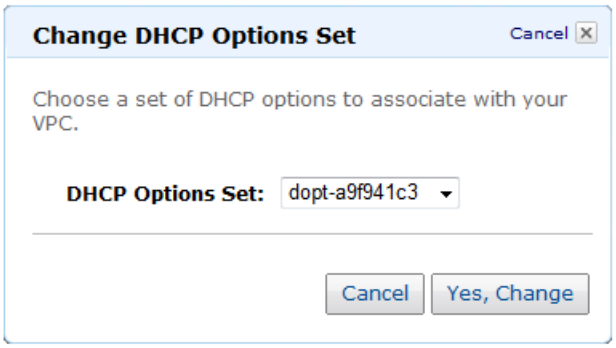
您可以更改 VPC 使用的 DHCP 选项集。如果您不希望 VPC 使用 DHCP 选项，请参见更改 VPC 以使用 NO DHCP 选项 (p. 112)。

Note

下列步骤是在假设您已经创建了您希望更改的 DHCP 选项集后进行。如果您尚未创建，请立即创建选项集。有关更多信息，请参见正在创建 DHCP 选项集 (p. 110)。

更改与 VPC 相关联的 DHCP 选项集。

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的Your VPCs。
3. 选择 VPC 然后单击Change DHCP Options Set按钮。
4. 在Change DHCP Options Set对话框中，从下拉列表中选择一个选项集，然后单击Yes, Change。

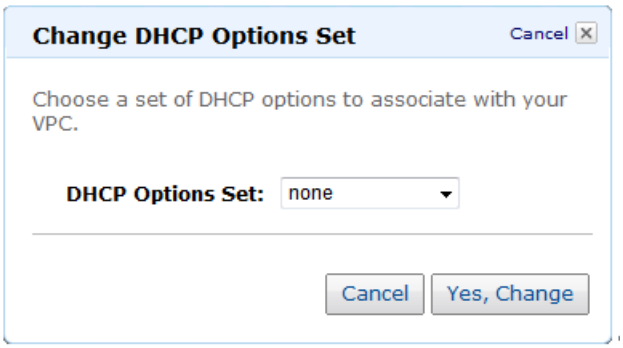


在您将新的 DHCP 选项集与 VPC 关联之后，任何现有实例以及您在 VPC 内启动的所有新增实例都将使用这些选项。无需重新开始或重新启动实例。根据实例更新 DHCP 租赁权的频率，它们会在几个小时内自动拾取更改。如果您愿意，您也可以使用实例上的操作系统，直接更新租赁权。

更改 VPC 以使用 NO DHCP 选项

您可以设置您的 VPC，使其不使用任何 DHCP 选项。

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的Your VPCs。
3. 选择 VPC 然后单击“Change DHCP Options Set”按钮。
4. 在“Change DHCP Options Set”对话框中，从下拉列表中选择“none”，然后单击“Yes, Change”。



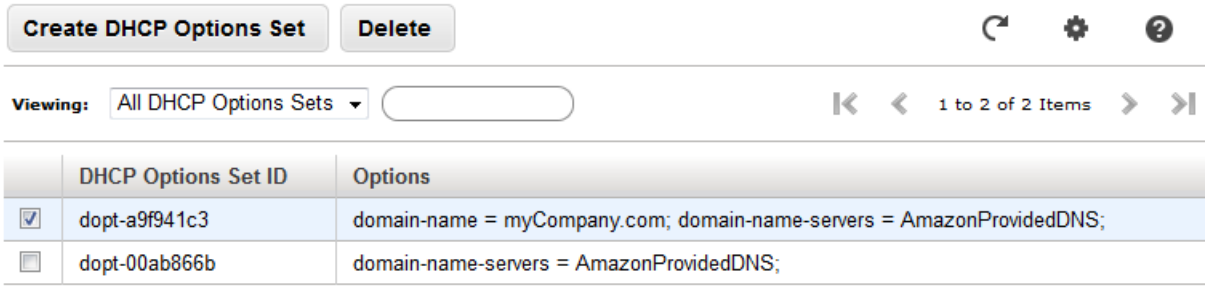
You don't need to restart or relaunch the instances. They automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. If you want, you can explicitly renew the lease using the operating system on the instance.

正在删除 DHCP 选项集

当您不再需要 DHCP 选项集时，您可以使按照以下步骤删除 DHCP 选项集。VPC 必须未在使用选项。

删除 DHCP 选项集

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“DHCP Options Set”。
3. 选择需要删除的 DHCP 选项集，然后单击“Delete”。



4. 在“Change DHCP Options Set”对话框中，单击“Yes, Delete”。

API 和命令概览

下表概述了可用的 DHCP 选项集命令和相应的 API 操作。

描述	命令	API 操作
为您的 VPC 创建 DHCP 选项集。	ec2-create-dhcp-options	CreateDhcpOptions
将 DHCP 选项集与指定 VPC 相关联，或更改 VPC 以便不使用 DHCP 选项。	ec2-associate-dhcp-options	AssociateDhcpOptions
描述您的一项或多项 DHCP 选项集	ec2-describe-dhcp-options	DescribeDhcpOptions
删除 DHCP 选项集	ec2-delete-dhcp-options	DeleteDhcpOptions

在您的 VPC 中使用 DNS

Amazon EC2 实例需要 IP 地址以进行通信。公有 IP 地址可实现 Internet 间的通信，私有 IP 地址可实现网络内实例（EC2-Classic 或 VPC）之间的通信。

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 主机名称是可以唯一并绝对区分计算机的名称；它由主机名称和域名组成。DNS 服务器会将 DNS 主机名称解析到其相应的 IP 地址。

我们提供 Amazon DNS 服务器。如需使用您自己的 DNS 服务器，更新您 VPC 的 DHCP 选项。有关更多信息，请参见 DHCP 选项集 (p. 108)。

要使 EC2 实例可供公开访问，则必须为其提供一个公有 IP 地址、一个 DNS 主机名称以及 DNS 解析。

查看您的 EC2 实例的 DNS 主机名称

当您在 EC2-Classic 平台中或默认 VPC 中启动实例时，我们会为实例提供公有和私有 DNS 主机名称。根据您的 AWS 账户支持的平台，您在非默认 VPC 中启动的实例可能获得公用和私有 DNS 主机名称。

您可以使用 Amazon EC2 控制台或 Amazon EC2 命令行接口查看运行实例或网络接口的 DNS 主机名称。

AWS 管理控制台

使用控制台查看实例的 DNS 主机名称

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 在导航窗格中，单击 Instances。
3. 从列表中选择实例。
4. 在详细信息窗格的“Description”选项卡中，检视“Public DNS”和“Private DNS”字段的值。

使用控制台查看网络接口的 DNS 主机名称

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 在导航窗格中，单击“Network Interfaces”。
3. 从列表中选择网络接口。
4. 在网络接口的“Details”选项卡中，检视“Public DNS”和“Private DNS”字段的值。

命令行接口

如需使用命令行接口查看实例的 DNS 主机名称，您可以使用ec2-describe-instances命令。例如，下方命令会显示出有关这个 ID 的实例的信息，例如 DNS 主机名称`i-1a2b3c4d`。

```
ec2-describe-instances i-1a2b3c4d
```

下方示例摘录自此命令结果，命令结果显示出公有 DNS 主机名称为 `ec2-203-0-113-12.compute-1.amazonaws.com`，私有 DNS 主机名称为 `ip-172-31-14-29.ec2.internal`。这些只是示例名称；根据实例启动的地点和方式的不同，您的实例的 DNS 主机名称可能会采取不同的格式。

```
RESERVATION     r-6482711d      880185128111    quicklaunch-2
INSTANCE  i-1a2b3c4d  ami-1624987f  ec2-203-0-113-12.compute-1.amazonaws.com

ip-172-31-14-29.ec2.internal  running
```

如需使用命令行接口查看网络接口的 DNS 主机名称，您可以使用ec2-describe-network-interfaces命令以显示指定网络接口的 DNS 主机名称。例如，下方命令会显示出有关这个 ID 的网络实例的信息，例如 DNS 主机名称`eni-1a2b3c4d`。

```
ec2-describe-network-interfaces eni-1a2b3c4d
```

下方示例摘录自此命令结果，命令结果显示出公有 DNS 主机名称为 `ec2-203-0-113-12.compute-1.amazonaws.com`，私有 DNS 主机名称为 `ip-172-31-14-29.ec2.internal`。请注意示例的名称；根据实例启动的地点和方式的不同，您的实例的 DNS 主机名称可能会采取不同的格式。

```
NETWORKINTERFACE    eni-1a2b3c4d    subnet-73ba071a vpc-1a2b3c4d  us-east-1b
 false   in-use
172-31-14-29 ip-172-31-14-29.ec2.internal   true
...
ASSOCIATION    203-0-113-12   amazon  172-31-14-29   ec2-203-0-113-12.compute-
1.amazonaws.com
PRIVATEIPADDRESS 172-31-14-29   ip-172-31-14-29.ec2.internal
```

更新您的 VPC 的 DNS 支持

当您在 VPC 内启动实例时，我们仅会在 VPC 已启用 DNS 主机名称的情况下，为实例提供公有和私有 DNS 主机名称。默认情况下，DNS 主机名称仅向默认 VPC 和由您使用 VPC 控制台创建的 VPC 启用。如果您在 VPC 中的实例没有 DNS 主机名称和 DNS 解析，则无法通过 Internet 进行访问。

我们支持以下 VPC 属性以控制 DNS 支持。如果您希望具有公有 IP 地址的实例可通过 Internet 访问，请务必将这两个属性都设置为 `true`。

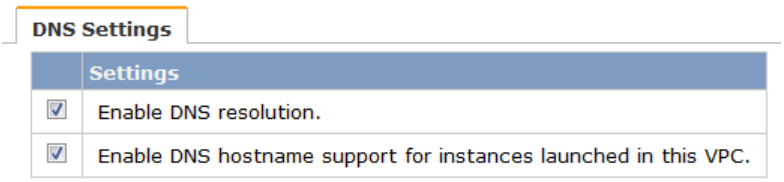
属性	描述
`enableDnsHostnames`	指明在 VPC 内启动的实例是否可获得 DNS 主机名称。如果该属性为 `true`，则 VPC 内的实例可获得 DNS 主机名称，否则将无法获得。除非 `enableDnsSupport` 为 `true`，否则您无法将此属性设置为 `true`。
`enableDnsSupport`	指明 VPC 是否支持 DNS 解析。如果该属性为 `true`，则 Amazon DNS 服务器会将您实例的 DNS 主机名称解析为相应的 IP 地址，否则不会解析。

如果您在之前不支持 DNS 主机名称的 VPC 中启用 DNS 主机名称，则您已经在该 VPC 中启动的一项实例将会获得一个 DNS 主机名称（如果这个实例有公有 IP 地址或弹性 IP 地址）。

AWS 管理控制台

使用 Amazon VPC 控制台更新 VPC 的 DNS 支持

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“Your VPCs”。
3. 从列表中选择 VPC。
4. 检视“DNS Settings”选项卡中的信息。在这个例子中，两项设置都已被启用。



5. 根据需要更新这些设置。

命令行接口

使用ec2-describe-vpc-attribute命令以判断指定 VPC 是否支持 DNS 解析和 DNS 主机名称。

```
ec2-describe-vpc-attribute -H vpc-id
```

下方示例输出表明 DNS 解析和 DNS 主机名称都支持指定的 VPC。

```
TYPE            EnableDnsSupport   EnableDnsHostnames
VPCATTRIBUTES   true               true
```

使用ec2-modify-vpc-attribute命令以根据需要更新这些设置。例如，下方命令可禁用 DNS 主机名称支持。

```
ec2-modify-vpc-attribute vpc-id --dns-hostnames false
```

在您的 VPC 中添加硬件虚拟专用网关

在默认情况下，您在 Virtual Private Cloud (VPC) 中启动的实例无法与您自己的网络进行通信。您可以启用从 VPC 访问网络的权限，为完成此操作您需要在 VPC 中附加虚拟专用网关、创建自定义路由表并更新您的安全组规则。

您可以根据本页的描述手动完成此过程，或由 VPC 创建向导为您完成其中大部分步骤。有关使用 VPC 创建向导以设置虚拟专用网关的更多信息，请参见情景 3：带有公有和私有子网以及硬件 VPN 访问的 VPC (p. 24)或情景 4：仅带有私有子网和硬件 VPN 访问的 VPC (p. 35)。

尽管术语 *VPN 连接*是一项泛指性术语，但是在 Amazon VPC 文档中，“VPN 连接”是指在您的 VPC 和您自己的网络之间的连接。

Topics

有关在 VPC 中使用 VPN 连接的相关费用的信息，请参见 Amazon VPC 产品页面。

VPN 组成部分

一项 VPN 连接由以下部分组成。

虚拟专用网关

*虚拟专用网关*是 VPN 连接在 Amazon 一端的 VPN 集线器。

有关您可以在每个地区设置的虚拟专用网关数目，以及 VPC 的其他组成部分限制的信息，请参见Amazon VPC 限制 (p. 135)。

客户网关

*客户网关*是指 VPN 连接在您这一端的实体设备或软件应用程序。

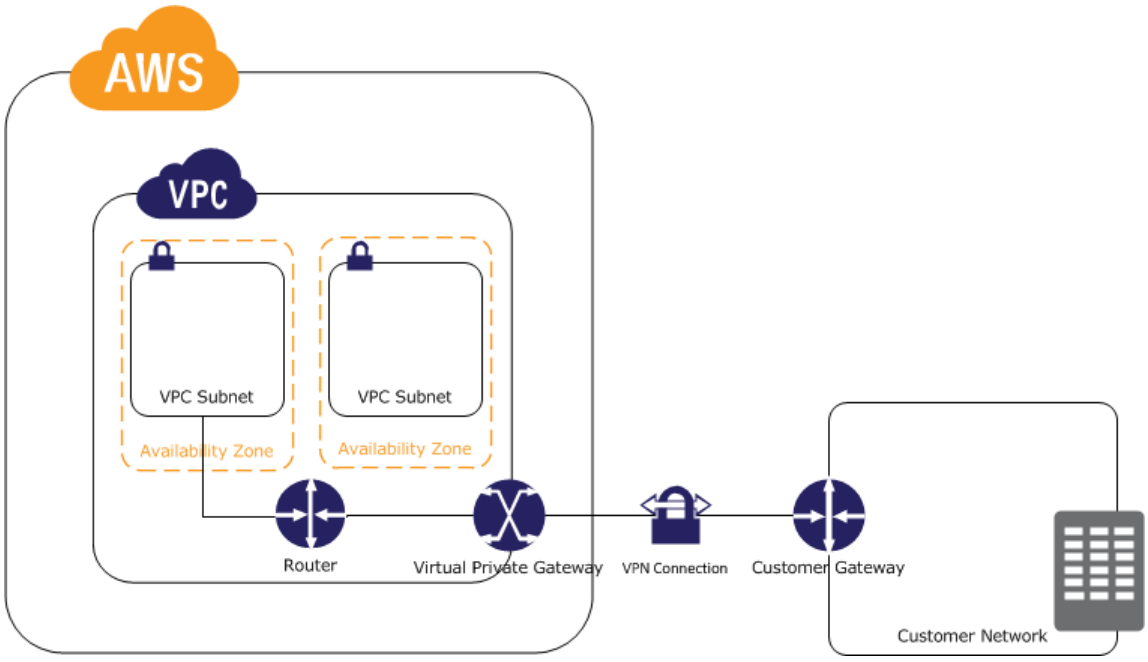
有关已经过 Amazon VPC 测试的客户网关列表，请参见Amazon Virtual Private Cloud 常见问题。

VPN 配置示例

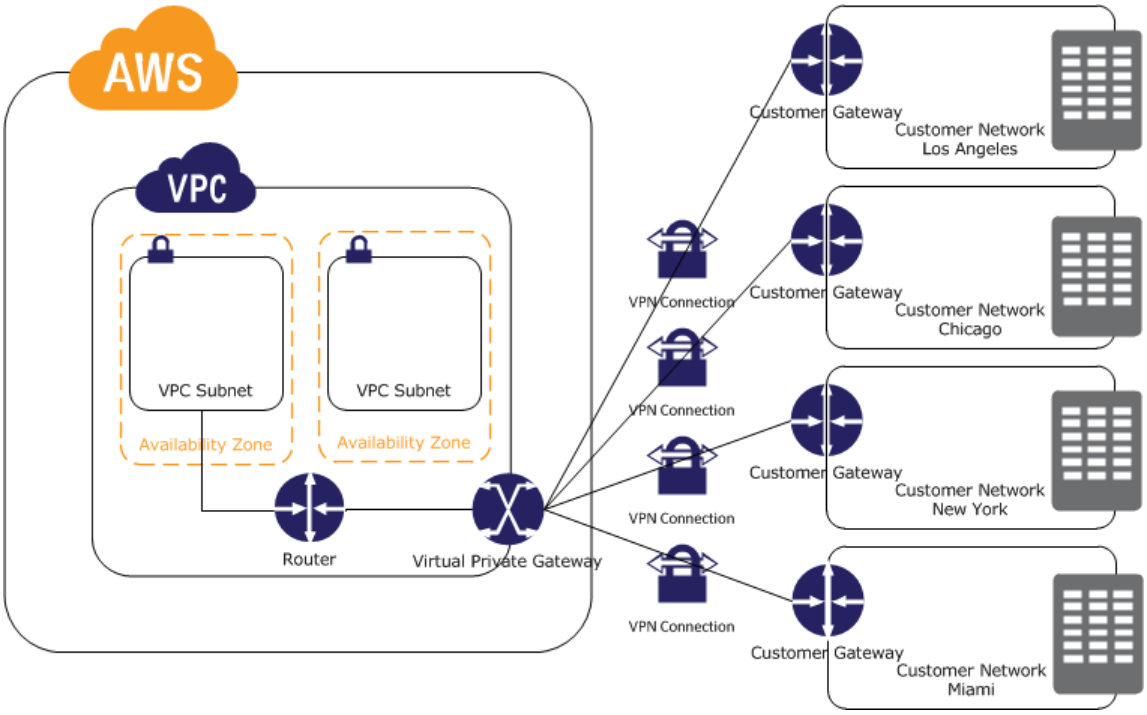
下图展示的是单一和多 VPN 连接。VPC 有附属的虚拟专用网关，您的网络内包括一个客户网关，您必须配置以启用 VPN 连接。您可以设置路由，以使从您的 VPC 通向您的网络的数据流可以被路由到虚拟专用网关中。

当您为单一 VPC 创建多项 VPN 连接时，您可以配置第二客户网关，以创建到同一外部地点的冗余连接。您还可以使用它来创建到多个地理位置的 VPN 连接。

单一 VPN 连接



多 VPN 连接



VPN 路由选项

当您创建 VPN 连接时，您必须指定您计划使用的路由类型。您选择的路由类型可由您的 VPN 设备构造和型号决定。如果您的 VPN 支持边界网关协议 (BGP)，您可以在配置 VPN 连接时指定动态路由方式。如果您的设备不支持 BGP，您便需要指定静态路由。有关已经过 Amazon VPC 测试的静态和动态路由设备列表，请参阅 Amazon Virtual Private Cloud 常见问题。

当您使用 BGP 设备时，您不需要为 VPN 连接指定静态路由，因为设备会使用 BGP 将其路由通告虚拟专用网关。如果您的设备不支持 BGP，您必须选择静态路由，并输入您的网络的路径（IP 前缀），以便与虚拟专用网关建立通信。只有虚拟专用网关已知的 IP 前缀可从您的 VPC 接收数据流量（无论是通过 BGP 通告还是静态路由条目）。

我们建议您在适用的情况下使用支持 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对第二条 VPN 隧道进行故障转移。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。

建立 VPN 连接所需的步骤

如需在 VPN 连接中使用 Amazon VPC，您或您的网络管理员必须指定一台实体设备以作为您的客户网关，并对其进行配置。我们会为您提供规定配置信息，包括 VPN 预共享密钥和其他与设置 VPN 连接相关的参数。您的网络管理员通常会执行此项配置。有关客户网关要求和配置的信息，请参阅Amazon Virtual Private Cloud Network Administrator Guide。

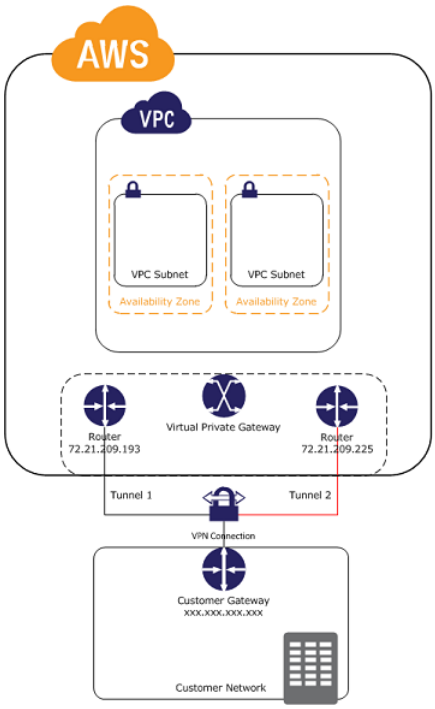
下表列出了您必须掌握的信息，以帮助我们为您建立 VPN 连接。

项目	如何使用	注释	
客户网关类型（例如 Cisco ASA、Juniper J-Series、Juniper SSG、Yamaha）	指定如何规定返回信息的格式，以供您配置客户网关		
客户网关外部接口的 Internet 可路由 IP 地址（静态）	用于创建和配置您的客户网关（又被称为“YOUR_UPLINK_ADDRESS”）	这个值必须为静态值，并且不可位于执行网络地址转换 (NAT) 设备的值范围内。	
（可选）客户网关的边界网关协议 (BGP)自治系统编号 (ASN)（如果您创建的是动态路由的 VPN 连接）。	用于创建和配置您的客户网关（又被称为“YOUR_UPLINK_ADDRESS”）。 如果您在控制台中使用向导以设置您的 VPC，我们会自动使用 65000 作为 ASN。	您可以使用指定给您的网络的现有 ASN。如果您没有 ASN，您可以使用专用 ASN（在 64512–65534 范围内）。有关 ASN 的更多信息，请参见Wikipedia 条目。 Amazon VPC 支持双字节的 ASN 编号。	
您希望通过 VPN 连接传播到 VPC 的内部网络 IP 范围。	用于指定静态路由。		

为您的 VPN 连接配置两条 VPN 隧道

您使用 VPN 连接以将您的网络连接到 VPC。每项 VPN 连接都有两条隧道，每条隧道都会使用一个独特的虚拟专用网关公有 IP 地址。配置两条隧道以提供冗余能力是重要的步骤。当一条隧道无法使用时（例如，因维护而关闭），网络流量会自动路由到指定 VPN 连接的其他可用隧道。

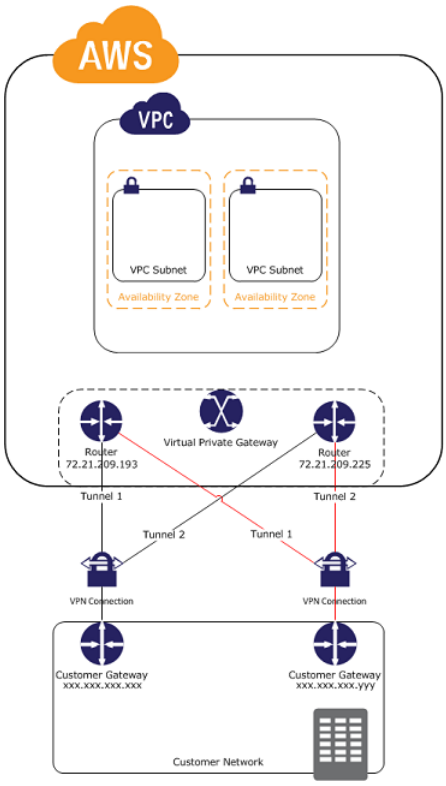
下图展示了 VPN 连接的两条隧道。



使用冗余 VPN 连接以提供故障转移

如上所述，VPN 连接配有两条隧道以帮助确保连接性，以防止出现 VPN 连接不可用的情况。如需避免因您的客户网关不可用而造成连接中断，您可以使用第二个客户网关为您的 VPC 设置第二项 VPN 连接。通过使用冗余 VPN 连接和网关，您可以在对其中一个客户网关进行维护时保证数据流量可以继续流经第二个客户网关的 VPN 连接。如需在您的网络中建立冗余 VPN 连接和客户网关，您需要设置第二项 VPN 连接。第二项 VPN 连接的客户网关 IP 地址必须可供公开访问，并且不能与您在第一项 VPN 连接中使用的公有 IP 地址相同。

下图展示了 VPN 连接的两条隧道和两个客户网关。



动态路由的 VPN 连接使用边界网关协议 (BGP) 在您的客户网关和虚拟专用网关之间交换路由信息。静态路由的 VPN 连接要求您输入在您这一端的客户网关的网络静态路由。已通告 BGP 和静态输入的路由信息可以帮助两端的网关在出现故障时判断可用隧道，进而重新路由数据流量。我们建议您配置您的网络，使其使用 BGP 提供的路由信息（若适用）以选择可用路径。精确配置取决于您的网络架构。

设置 VPN 连接

按照以下步骤以手动设置 VPN 连接。或者，您可以创建 VPC 和子网，并使用 VPC 向导完成此程序的前四个步骤。有关更多信息，请参见正在实施情景 3 (p. 31)或实施情景 4 (p. 38)。

该 程序 假设您已经具有一个包含一个或多个子网的 VPC，并且具有所需的网络信息（参见 建立 VPN 连接所需的步骤 (p. 119)）。

1. 创建客户网关。

   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. 在导航窗格中，单击“Customer Gateways”，然后再单击“Create Customer Gateway”。
   c. 指定您的客户网关设备的路由类型和静态 IP 地址，然后单击“Yes, Create”。

2. 创建虚拟专用网关并将其连接到您的 VPC。

   a. 在导航窗格中，单击“Virtual Private Gateways”，然后再单击“Create Virtual Private Gateway”。
   b. 在出现提示时单击“Yes, Create”。
   c. 选择您刚刚创建的虚拟专用网关，然后单击“Attach to VPC”。
   d. 在“Attach to VPC”对话框中，从列表中选择 VPC，然后单击“Yes, Attach”。

3. 在路由表中添加路由，然后启用路由传播。

   a. 在导航窗格中，单击“Route Tables”，然后选择与子网关联的路由表；默认情况下，该路由表为 VPC 的主路由表。
   b. 在详细信息窗格的“Routes”选项卡上，执行以下一项操作，然后单击“Add”：

      - 如果您要对您的 VPN 连接使用静态路由，请在“Destination”框中添加该 VPN 连接所使用的静态路由，然后从“Target”列表中选择虚拟私有网关 ID。
      - 如果您要对您的 VPN 连接使用动态路由，请在“Destination”框中输入您的客户网络的 IP 前缀，然后从“Target”列表中选择虚拟私有网关 ID。

   c. 在详细信息窗格的“Route Propagation”选项卡中，从列表中选择与 VPC 相关的虚拟专用网关，然后单击“Add”。

      Note

      如果您将 VPN 连接配置为使用动态路由，并且已经启用了路由传播，源自您的客户网关的 BGP 通告路由便不会出现在路由表中，除非 VPN 连接的状态为 UP。

4. 向安全组添加规则，以允许从您的网络进行 SSH 和 RDP 访问。有关添加入站规则的更多信息，请参阅 添加和删除规则 (p. 61)。

   a. 在导航窗格中，单击“Security Groups”，然后选择 VPC 的默认安全组。
   b. 在详细信息窗格的“Inbound”选项卡上，添加从您的网络向组进行入站 SSH 访问的规则和进行入站 RDP 访问的规则，然后单击“Apply Rule Changes”。

5. 创建 VPN 连接。

   a. 在导航窗格中，单击“VPN Connections”。
   b. 单击“Create VPN Connection”。
   c. 在“Add VPN Connection”对话框中，执行以下操作，并随后单击“Yes, Create”：

      - 指定您的客户网关的 IP 地址。
      - 根据您的 VPN 路由器是否支持边界网关协议 (BGP)，选择一个路由选项：
        - 如果您的 VPN 路由器支持 BGP，选择“Use dynamic routing (requires BGP)”。
        - 如果您的 VPN 路由器不支持 BGP，选择“Use static routing”。在“IP Prefix”框中，指定您的 VPN 连接的私有网络的每项 IP 前缀，然后单击“Add”。

6. 配置客户网关。

   a. 在导航窗格中，单击“VPN Connections”。
   b. 选择您的 VPN 连接，然后单击“Download Configuration”。
   c. 为您的网络管理员提供配置信息和指南：Amazon Virtual Private Cloud Network Administrator Guide。在网络管理员配置客户网关之后，VPN 连接便已可以操作。

7. 在子网中启动实例。

   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

b. 在导航窗格中，单击 Instances。
c. 单击“Launch Instance”。
d. 在“Create a New Instance”页，单击“Quick Launch Wizard”并按照指示操作。为您的实例指定名称，选择密钥对，选择 AMI，然后单击“Continue”。
e. 单击“Edit Details”，选择“Instance Details”下的“Launch into a VPC”，指定一个子网，然后单击“Save Details”。
f. 检视您已经选择的设置。根据需要进行更改，随后单击“Launch”。

测试实例的端至端连接

在您设置 VPN 连接并启动实例之后，您可以通过检测实例以测试连接。您只需要使用可以回应检测请求的 AMI。我们建议您使用 Amazon Linux AMI 之一。如果您使用的实例在 Windows Server 中允许，您将需要登录实例，并在 Windows 防火墙中启用 ICMPv4，方可检测实例。

Important

您必须对 VPC 中负责过滤实例流量的任何安全组或网络 ACL 进行配置，以允许入站和出站 ICMP 流量。

您可以使用 Amazon VPC 控制台或使用 Amazon EC2 API/CLI 来监控 VPN 连接的状态。您可以查看有关您的 VPN 连接的信息，包括状态、自上一次状态更改后持续的时间以及描述性错误文本。

测试端至端连接

1. 当实例开始运行后，获取其私有 IP 地址（例如`10.0.0.4`）。Amazon EC2 控制台显示的地址是实例详细信息的一部分。
2. 对于在您的网络中、位于客户网关背后的计算机，您可以使用Ping命令侦测实例的私有 IP 地址。成功响应的形式与下方类似：

```
PROMPT> ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

您现在可以使用 SSH 或 RDP 来连接您 VPC 中的实例。有关如何连接 Linux 实例的更多信息，请参阅 *Amazon Elastic Compute Cloud User Guide* 中的 Connect to Your Linux Instance。有关如何连接 Windows 实例的更多信息，请参阅 *Amazon Elastic Compute Cloud Microsoft Windows Guide* 中的 Connect to Your Windows Instance。

替换受损的证书

如果您认为 VPN 连接的隧道证书已经受损，您可以更改 IKE 预共享密钥。如需测试受损证书，取消 VPN 连接，使用相同的虚拟专用网关创建一项新的证书，并在您的客户网关中配置新的密钥。您还需要确认隧道的内部和外部地址可以相互匹配，因为在您重新建立 VPN 连接时这些地址可能也会随之更改。在您执行此步骤时，与您的 VPC 实例的通信将会停止，但实例仍会继续不受干扰地运行。在网络管理员执行新配置信息之后，您的 VPN 连接便可使用新证书，而到您的 VPC 实例的网络连接也将恢复正常。

Important

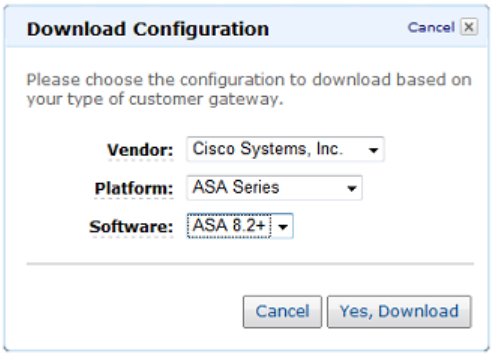
此步骤要求您的网络管理员组的协助。

更改 IKE 预共享密钥

1. 删除 VPN 连接。您不需要删除 VPC 或虚拟专用网关。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. 在导航窗格中，单击“VPN Connections”。
   c. 选择 VPN 连接，然后单击“Delete”。
   d. 在“Delete VPN Connection”对话框中，单击“Yes, Delete”。

2. 创建新的 VPN 连接。
   a. 在同一VPN 连接页面中，单击“Create VPN Connection”。注意您的虚拟专用网关和客户网关都已被选定。
   b. 根据您的 VPN 路由器是否支持边界网关协议 (BGP)，选择一个路由方案。如果您无法确定，请参见Amazon Virtual Private Cloud 常见问题。
      - 如果您的 VPN 路由器支持边界网关协议 (BGP)，单击“Use dynamic routing (requires BGP)”。
      - 如果您的 VPN 路由器不支持 BGP，单击“Use static routing”。在“IP Prefix”框中，输入您网络的每项 IP 前缀，然后单击“Add”。
   c. 单击“Yes, Create”。

3. 下载新的客户网关配置，您的网络管理员必须执行此配置。这项新的配置会替换之前在 IKE 预共享密钥中使用的网关配置。
   a. 选择您刚刚创建的 VPN 连接，然后单击“Download Configuration”。
   b. 选择客户网关的供应商、平台和软件版本，然后单击“Yes, Download”。



c. 保存文本文件，并连同 Amazon Virtual Private Cloud Network Administrator Guide 一起提供给您的网络管理员。

删除 VPN 连接

若您不再需要某一 VPN 连接，则可将其删除。

Important

如果您删除了 VPN 连接并创建了一个新连接，则需要下载新配置信息，然后让您的网络管理员重新配置客户网关。

删除 VPN 连接

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在导航窗格中，单击“VPN Connections”。
3. 选择 VPN 连接，然后单击“Delete”。
4. 在“Delete VPN Connection”对话框中，单击“Yes, Delete”。

若您不再需要某一客户网关，则可将其删除。您无法删除正在 VPN 连接中使用的客户网关。

删除客户网关

1. 在导航窗格中，单击“Customer Gateways”。
2. 选择要删除的客户网关，然后单击“Delete”。
3. 在“Delete Customer Gateway”对话框中，单击“Yes, Delete”。

如果您不再需要 VPC 的某一虚拟私有网关，则可将其断开。

断开虚拟私有网关

1. 在导航窗格中，单击“Virtual Private Gateways”。
2. 选择相应的虚拟私有网关，然后单击“Detach from VPC”。
3. 在“Detach from VPC”对话框中，单击“VPC”列表，选择要断开的 VPC，然后单击“Yes, Detach”。

如果您不再需要某一虚拟私有网关，则可将其删除。您无法删除仍与 VPC 关联的虚拟私有网关。

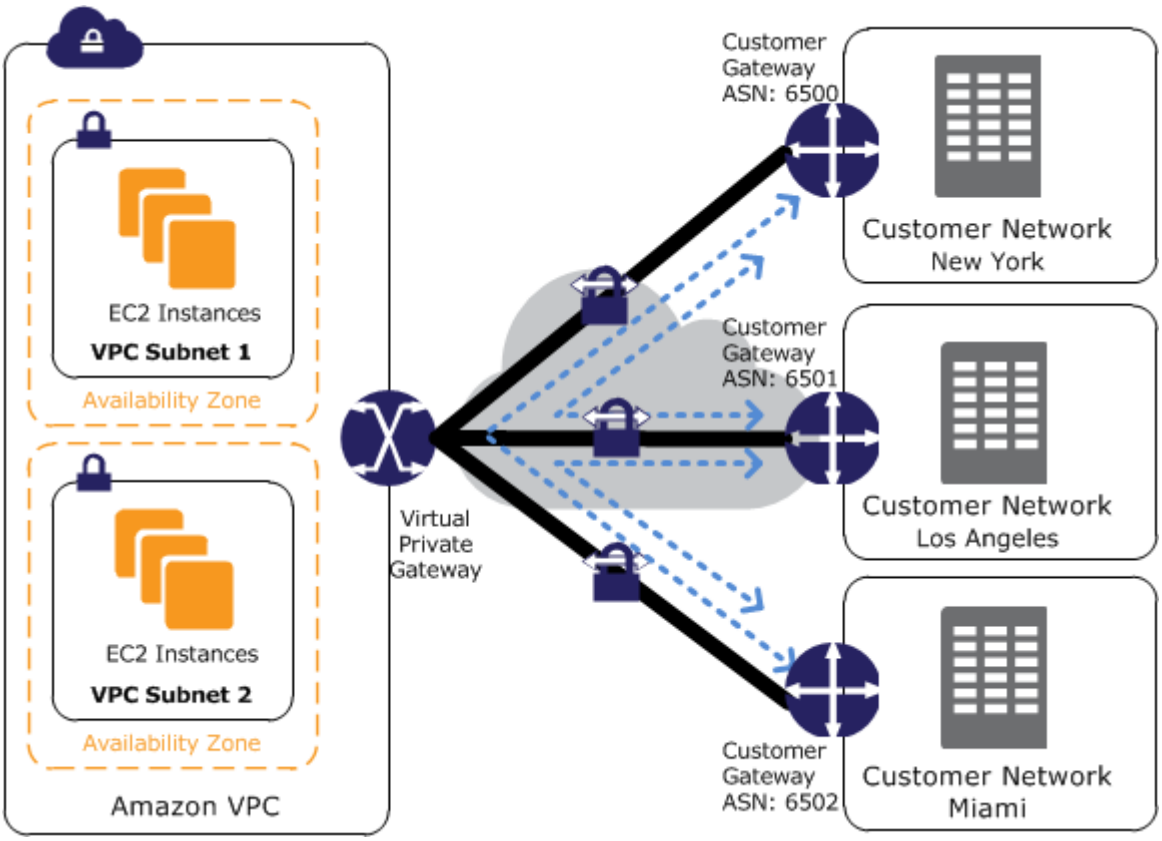
删除虚拟私有网关

1. 选择要删除的虚拟私有网关，然后单击“Delete”。
2. 在“Delete Virtual Private Gateway”对话框中，单击“Yes, Delete”。

使用 VPN CloudHub 在各个站点之间建立安全通信

如果您有多项 VPN 连接，您可以使用 AWS VPN CloudHub 在各个站点之间建立安全通信。VPN CloudHub 在简单的星型拓扑连接模型上操作，您可以在使用或不使用 VPC 的情况下操作 VPN CloudHub。这种设计适合有多间分公司和现有 Internet 连接的客户，帮助他们实施方便、潜在低成本的星型拓扑连接模型，以便在这些远程办公室之间建立主要或备用连接。

下图展示了 VPN CloudHub 架构，蓝色虚线表明远程站点之间的网络流量（通过 VPN 连接路由）。



如需使用 AWS VPN CloudHub，您必须创建有多个客户网关的虚拟专用网关，并且每个网关都有独特的 Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs)。客户网关可通过它们的 VPN 连接传播适当的路由（BGP 前缀）。路由通告会被每个 BGP 对等体接收并重新通告，使每个站点都可以向其他站点发送或接受数据。每个轮辐必须有唯一的 ASN，并且站点不可与 IP 范围重叠。每个站点还可以发送和从 VPC 接收数据（与使用标准 VPN 连接的方式相同）。

使用 AWS Direct Connect 连接来连接虚拟专用网关的站点也可以是 AWS VPN CloudHub 的一部分。例如，您在纽约的公司总部有到 VPC 的 AWS Direct Connect 连接，您的分公司可以使用 VPN 连接以连接 VPC。洛杉矶和迈阿密的分公司可以使用 AWS VPN CloudHub 在彼此以及您的公司总部之间发送和接收数据。

如需配置 AWS VPN CloudHub，您可以使用 AWS 管理控制台创建多个客户网关，并且每个网关都有独特的网关公用 IP 地址和独特的 ASN。 接下来，您可以创建从每个客户网关到通用虚拟专用网关的 VPN 连接。每项 VPN 连接必须传播其指定的 BGP 路由。您可以使用 VPN 连接的 VPN 配置文件内的网络声明完成此操作。根据您使用的路由类型，网络声明可能会有稍许不同。

在使用 AWS VPN CloudHub 时，您需要支付标准的 Amazon VPC VPN 连接费用。 您需要按小时承担 VPN 与虚拟专用网关的连接费用。当您使用 AWS VPN CloudHub 从一个站点向另一个站点发送数据，从您的站点向虚拟专用网关发送数据不会产生任何费用。对于从虚拟专用网关转继到您的终端节点的数据您仅需支付标准 AWS 数据传输费用即可。 例如，如果您在洛杉矶设有一个站点、在纽约设有第二个站点，并且两个站点都有通向虚拟专用网关的 VPN 连接，您应为每个 VPN 连接支付每小时 0.05 美元的费用（两项 VPN 连接的总费用为每小时 0.10 美元）。您还需要为所有经过 VPN 连接从洛杉矶发送到纽约（或从纽约发送到洛杉矶）的数据支付标准 AWS 数据传输费用；通过 VPN 连接发送到虚拟专用网关的数据流量不会产生任何费用，但是通过 VPN 从虚拟专用网关发送到终端节点的网络流量将按照标准 AWS 数据传输费用产生相应的费用。有关更多信息，请参见VPN Connection Pricing。

使用 EC2 专用实例

您的 Amazon EC2 专用实例在单租户硬件上运行。它们与您的其他实例、以及属于其他 AWS 账户的其他实例在主机硬件级别便已实体隔离。您必须在 Virtual Private Cloud (VPC) 中启用专用实例。

此主题将讨论有关专用实例的基本信息，并为您展示如何实施专用实例。

Topics

专用实例基本信息

您在 VPC 内启动的每项实例都有一个租期属性。此属性有以下值。

值	描述
`default`	您的实例在共享硬件上运行。
`dedicated`	您的实例在单租户硬件上运行。

在您启动实例之后，您便无法更改实例的租期。如果在启动时您未将实例的租期设置为`dedicated`，您必须停止运行实例、设置租期并重新启动实例。

每个 VPC 都有相关的实例租期属性。此属性有以下值。

值	描述
`default`	如果在 VPC 内启动的实例的租期属性是`dedicated`，则该实例为专用实例。
`dedicated`	所有在 VPC 内启动的实例都是专用实例，无论该实例的租期属性值是什么。

在您创建 VPC 实例之后，您便无法更改实例的租期。相反，您必须终止 VPC 内的所有实例，删除 VPC，以新的实例租期属性值创建新的 VPC，然后重新启动实例。

如果您计划使用专用实例，则可以通过以下任一方式实施实例：

- 创建一个实例租期设置为 `dedicated` 的 VPC（在该 VPC 内启动的所有实例都是专用实例）。
- 创建一个实例租期设置为 `default` 的 VPC，然后在启动时为应该作为专用实例的任何实例指定专用租期。

Amazon EBS 与专用实例

当您启动 Amazon EBS 支持的专用实例时，EBS 卷不会在单一租户硬件中运行。

有专用租期的预留实例

为确保您在启动专用实例时拥有足够的容量，您可以购买专用预留实例。有关预留实例的更多信息，请参阅 On-Demand and Reserved Instances。

如果您购买专用预留实例，也就意味着您同时购买容量并以较低的使用费在 VPC 内启动专用实例；小时费用的价格折扣仅在您启动具有专用租期实例的情况下才生效。但是，如果您购买具有默认租期值的预留实例，则在启动租期为 `dedicated` 的实例时，将不会获得专用预留实例。

此外，您在购买之后，便无法更改预留实例的租期。

专用实例的 Auto Scaling

如果您计划对您的专用实例实施 Auto Scaling，这些实例必须是在实例租期属性设置为 `dedicated` 的 VPC 内启动的。

专用实例定价

我们为专用实例指定了单独的定价模式。有关更多信息，请参见Amazon EC2 专用实例产品页面。

使用专用实例

此部分将为您展示如何完成以下任务。

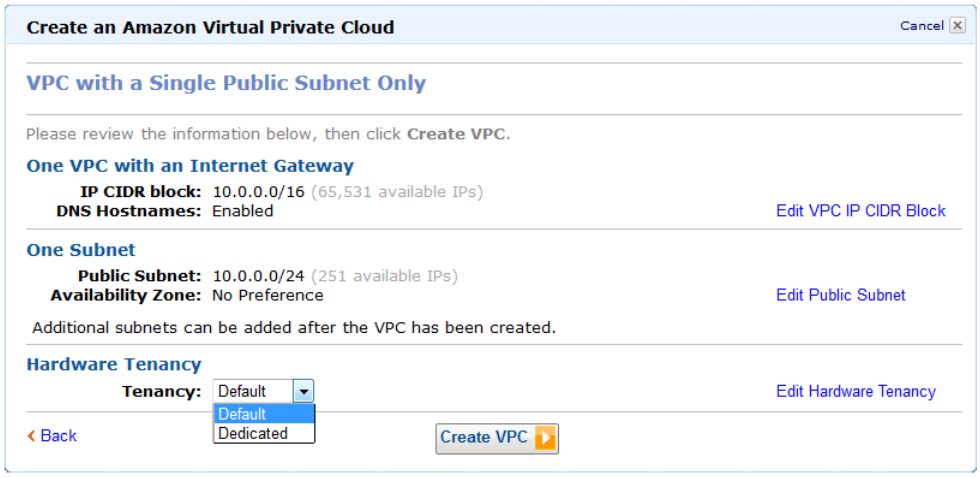
Topics

创建有专用实例租期的 VPC

当您创建 VPC 时，您可以选择指定它的实例租期。您可以接受默认设置，或者为您的 VPC 指定实例租期`dedicated`。在此部分中，我们将为您展示如何创建实例租期为`dedicated`的 VPC。

创建指定了专用实例租期的 VPC（VPC 向导）

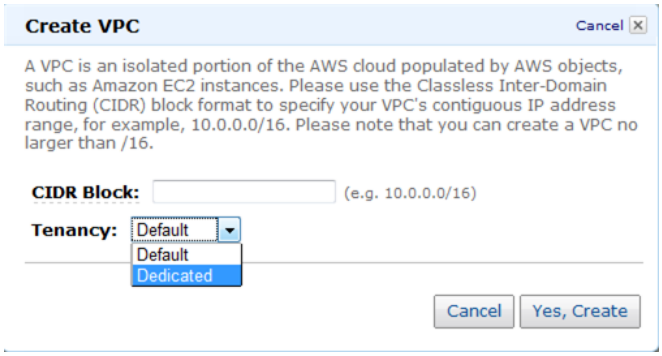
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 在控制面板中，单击“Start VPC Wizard”按钮。
3. 选择 VPC 配置，然后单击“Continue”。
4. 在确认页面中，单击“Edit Hardware Tenancy”然后单击“Dedicated”。



5. 单击“Create VPC”按钮以创建 VPC。

创建指定了专用实例租期的 VPC（创建 VPC 对话框）

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的“Your VPCs”，然后单击“Create VPC”按钮。
3. 在“Create VPC”对话框中，从“Tenancy”下拉列表中选择“Dedicated”。指定“CIDR Block”，然后单击“Yes, Create”。



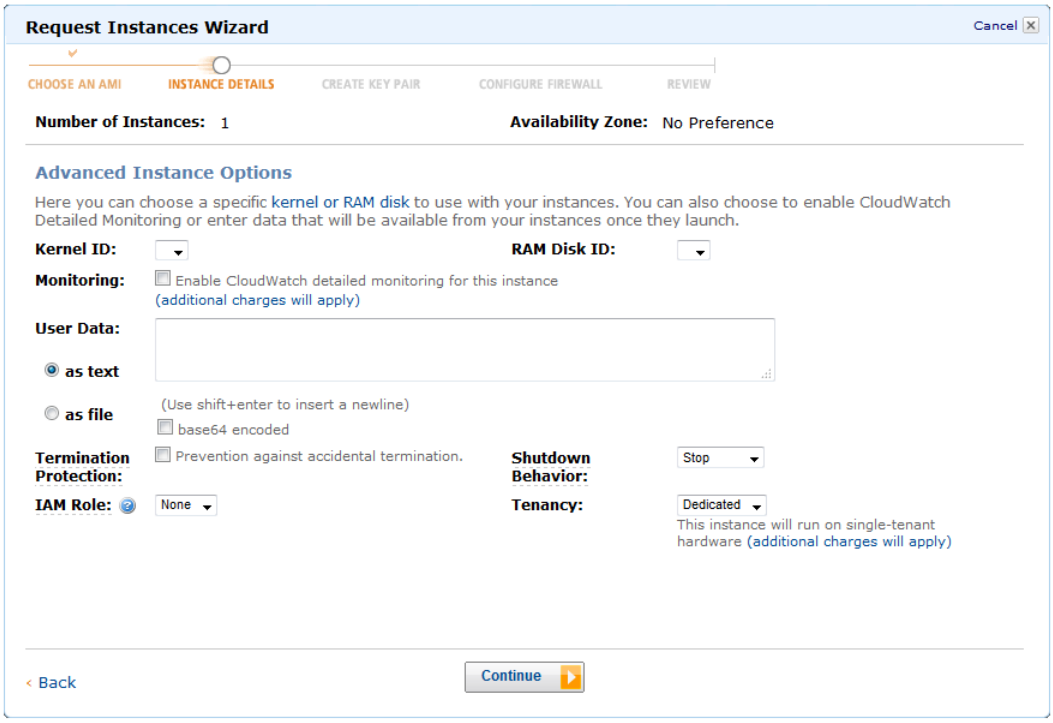
在 VPC 内启动专用实例

如果您在实例租期为`dedicated`的 VPC 内启动实例，您的实例会自动成为专用实例，无论该实例的租期是什么。接下来的步骤将为您演示如何在有默认实例租期设置的 VPC 内启动专用实例。

在默认实例租期内，在 VPC 内启动专用实例

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 创建 VPC，或决定使用现有 VPC。
3. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
4. 单击“Launch Instance”按钮，选择“Classic Wizard”按钮，然后单击“Continue”。
5. 在选择 AMI页面中，选择 AMI。

6. 在实例详细信息页面中，从“Instance Type”列表中选择“M1 small (m1.small)”。在“Launch Instances”选项下，选择 VPC 的子网以启动实例。单击“Continue”。
7. 在“Advanced Instance Options”选项下，从“Tenancy”下拉列表中选择“Dedicated”，然后单击“Continue”。

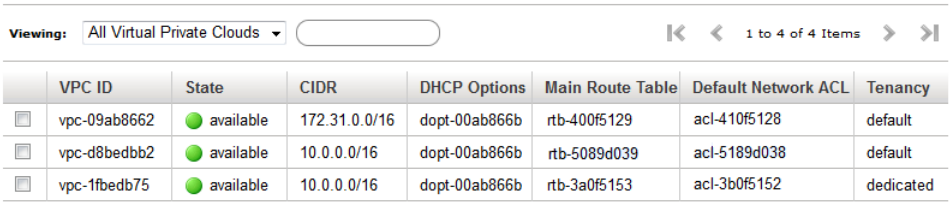


8. 根据 VPC 向导的提示继续。当您完成在REVIEW页面中检视选项的步骤之后，单击Launch按钮以启动专用实例。

显示租期信息

显示 VPC 的租期信息

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. 单击导航窗格中的Your VPCs。
3. 在Tenancy一栏中查看您的 VPC 实例的租期。

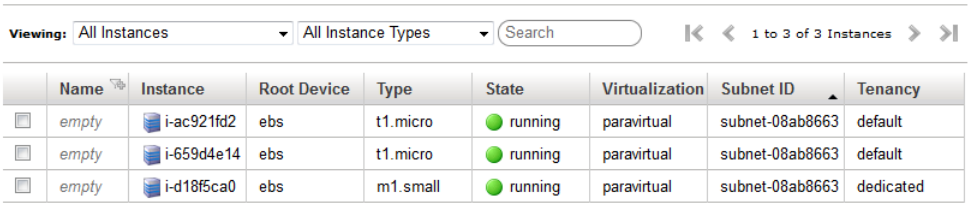


VPC ID	State	CIDR	DHCP Options	Main Route Table	Default Network ACL	Tenancy
vpc-09ab8662	available	172.31.0.0/16	dopt-00ab866b	rtb-400f5129	acl-410f5128	default
vpc-d8bedbb2	available	10.0.0.0/16	dopt-00ab866b	rtb-5089d039	acl-5189d038	default
vpc-1fbedb75	available	10.0.0.0/16	dopt-00ab866b	rtb-3a0f5153	acl-3b0f5152	dedicated

4. 如果“Tenancy”栏未能显示，单击“Show/Hide”按钮，并从“Show/Hide Columns”对话框中选择“Tenancy”，然后单击“Close”。

显示实例的租期信息

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. 单击导航窗格中的“Instances”。
3. 在“Tenancy”一栏中查看您的实例的租期。



	Name	Instance	Root Device	Type	State	Virtualization	Subnet ID	Tenancy
☐	empty	i-ac921fd2	ebs	t1.micro	running	paravirtual	subnet-08ab8663	default
☐	empty	i-659d4e14	ebs	t1.micro	running	paravirtual	subnet-08ab8663	default
☐	empty	i-d18f5ca0	ebs	m1.small	running	paravirtual	subnet-08ab8663	dedicated

4. 如果“Tenancy”栏未能显示，您可以执行以下操作：
   - 单击“Show/Hide”按钮，从“Show/Hide Columns”对话框中选择“Tenancy”，然后单击“Close”。
   - 选择实例。详细信息页面中的“Description”选项卡中会显示关于实例的信息，包括它的租期。例如：

API 和命令概览

下表概述了适用于专用实例的命令和 API 操作。

描述	命令	API 操作
您可以为在 VPC 中启动的实例指定支持租期选项。`default`值代表您可以在任何租期内，在 VPC 内启动实例；`dedicated`值代表您必须以专用实例形式，在 VPC 内启动所有实例。	ec2-create-vpc	CreateVpc
描述在 VPC 内启动的实例支持的租期选项（`default`或`dedicated`）。	ec2-describe-vpcs	DescribeVpcs
您可以为在 VPC 中启动的实例指定租期选项。（`default`或`dedicated`）	ec2-run-instances	RunInstances
描述实例的租期值（`default`或`dedicated`）。	ec2-describe-instances	DescribeInstances
描述预留实例的租期值（`default`或`dedicated`）。	ec2-describe-reserved-instances	DescribeReservedInstances
描述预留实例选项的租期值（`default`或`dedicated`）。	ec2-describe-reserved-instances-offerings	DescribeReservedInstancesOfferings

Amazon VPC 限制

下表列出了与 Amazon VPC 相关的限制。如需请求提高任何限制，请访问 Amazon VPC Limits form。

组成部分	限制	注释
每个地区的 VPC 数量	5	
每个 VPC 的子网数量	200	
每个地区的 Internet 网关数量	5	每个 VPC 一个
每个地区的虚拟私有网关数量	5	每个 VPC 一个
每个地区的客户网关数	50	
每个地区的 VPN 连接数	50	每个虚拟专用网关十个
每个 VPC 的路由表数	10	包括主路由表
每个路由表的条目数	20	
每个 AWS 账户内每个地区的弹性 IP 地址数	5	Amazon EC2 针对每个 AWS 账户为每个地区可以拥有的弹性 IP 地址设定了单独限制
每个 VPC 的安全组数	100	
每个安全组的规则数	50	
可分配给 VPC 中的实例的安全组数	5	
每个 VPC 的网络 ACL 数	50	
每个网络 ACL 的规则数	20	
每个 VPN 连接的 BGP 推荐转接数	100	

文档历史记录

下表描述此 Amazon VPC 指南每次发行时进行的重要修改。

功能	API 版本	描述	发行日期
启用 DNS 主机名称并禁用 DNS 解析	2013-02-01	DNS 解析默认已启用。现在，您可以通过 Amazon VPC 控制台、Amazon EC2 命令行接口或 Amazon EC2 API 操作禁用 DNS 解析。 非默认 VPC 的 DNS 主机名称默认已禁用。现在，您可以通过 Amazon VPC 控制台、Amazon EC2 命令行接口或 Amazon EC2 API 操作启用 DNS 主机名称。 有关更多信息，请参阅 在您的 VPC 中使用 DNS (p. 113)。	2013 年 3 月 11 日
VPN 连接使用静态路由配置。	2012-08-15	您可以使用静态路由配置在 IPsec VPN 和 Amazon VPC 之间建立连接。之前，VPN 连接要求使用边界网关协议 (BGP)。现在我们支持两种类型的连接，并激动地宣布现在您已经可以与不支持 BGP 的设备建立连接，包括 Cisco ASA 和 Microsoft Windows Server 2008 R2。	2012 年 9 月 13 日
自动路由传播	2012-08-15	现在您可以配置从您的 VPN 出发的路径、以及到您的 VPC 路由表的 Direct Connect 链接的自动传播。此功能简化了创建与维护到 Amazon VPC 的连接的过程。	2012 年 9 月 13 日
AWS VPN CloudHub 和冗余 VPN 连接		无论是否通过 VPC，您都可以在两个站点之间安全通信。您可以使用冗余 VPN 连接为您的 VPC 提供容错连接。	2011 年 9 月 29 日
VPC 无处不在	2011–07–15	五个 AWS 地区的多个可用区域支持 VPC，每个 AWS 账户可具有多个 VPC，Microsoft Windows Server 2008 R2 和 Microsoft SQL Server 预留实例的每个 VPC 都可以有多个 VPN 连接。	2011 年 8 月 03 日

功能	API 版本	描述	发行日期
专用实例	2011 年 2 月 28 日	专用实例是在您的 VPC 内启动的 Amazon EC2 实例，它们运行单一用户专用的硬件。专用实例不仅让您可以充分利用 Amazon VPC 和 AWS 弹性预置的优势，仅为实际用量付费，还让您能够享受到私有隔离虚拟网络 – 所有这些优势都在保证您的实例在硬件级别隔离的环境下实现。	2011 年 3 月 27 日