
Amazon Virtual Private Cloud

用户指南



Amazon Virtual Private Cloud: 用户指南

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

什么是 Amazon VPC ?	1
Amazon VPC 概念	1
VPC 和子网	1
支持的平台	1
默认和非默认 VPC	2
访问 Internet	2
访问企业或家庭网络	4
通过 AWS PrivateLink 访问服务	5
AWS 私有全球网络注意事项	6
如何开始使用 Amazon VPC	6
访问 Amazon VPC	7
Amazon VPC 定价	7
Amazon VPC 限制	7
PCI DSS 合规性	8
入门	9
IPv4 入门	9
步骤 1 : 创建 VPC	10
步骤 2 : 创建安全组	12
步骤 3 : 将实例启动到 VPC 中	13
步骤 4 : 为您的实例分配弹性 IP 地址	15
第 5 步 : 清除	16
IPv6 入门	16
步骤 1 : 创建 VPC	17
步骤 2 : 创建安全组	19
步骤 3 : 启动实例	21
场景和示例	23
场景 1 : 带单个公有子网的 VPC	23
概述	23
路由选择	25
安全性	26
实施场景 1	27
场景 2 : 带有公有子网和私有子网 (NAT) 的 VPC	29
概述	30
路由选择	32
安全性	33
实施场景 2	36
通过 NAT 实例实现场景 2	39
场景 3 : 具有公有和私有子网和 AWS Site-to-Site VPN 访问权限的 VPC	41
概述	41
路由选择	44
安全性	46
实施场景 3	49
场景 4 : 仅具有一个私有子网以及 AWS Site-to-Site VPN 访问权限的 VPC	53
概述	53
路由选择	54
安全性	55
实施场景 4	56
示例 : 使用 AWS CLI 创建 IPv4 VPC 和子网	58
第 1 步 : 创建 VPC 和子网	58
第 2 步 : 使您的子网成为公有子网	59
第 3 步 : 在您的子网中启动实例	61
步骤 4 : 清除	62
示例 : 使用 AWS CLI 创建 IPv6 VPC 和子网	63
第 1 步 : 创建 VPC 和子网	63

第 2 步：配置公有子网	64
第 3 步：配置仅出口私有子网	66
第 4 步：修改子网的 IPv6 寻址行为	67
第 5 步：在公有子网中启动实例	67
第 6 步：在私有子网中启动实例	68
步骤 7：清除	70
示例：共享公有子网和私有子网	71
示例：使用 AWS PrivateLink 和 VPC 对等连接的服务	71
示例：服务提供商配置服务	72
示例：服务使用者配置访问	72
示例：服务提供商将服务配置为跨区域	73
示例：服务使用者配置跨区域访问	74
VPC 和子网	75
VPC 和子网基础知识	75
VPC 和子网大小调整	78
针对 IPv4 的 VPC 和子网大小调整	78
向 VPC 中添加 IPv4 CIDR 块	79
针对 IPv6 的 VPC 和子网大小调整	81
子网路由	82
子网安全性	82
与本地网络和其他 VPC 的连接	83
使用 VPC 和子网	83
创建 VPC	83
在 VPC 中创建子网	84
将辅助 IPv4 CIDR 块与 VPC 关联	85
向 VPC 关联 IPv6 CIDR 块	86
向子网关联 IPv6 CIDR 块	86
在您的子网中启动一项实例	86
删除您的子网	87
取消 IPv4 CIDR 块与 VPC 的关联	87
取消 IPv6 CIDR 块与 VPC 或子网的关联	88
删除 VPC	89
使用共享 VPC	89
共享 VPC 的先决条件	89
共享子网	90
将共享的子网取消共享	90
确定共享子网的拥有者	90
共享子网权限	91
拥有者和参与者的计费和计量	91
共享子网不支持的服务	91
限制	91
默认 VPC 和默认子网	93
默认 VPC 组件	93
默认子网	94
可用性和支持的平台	95
检测支持的平台以及您是否有默认 VPC	95
查看您的默认 VPC 和默认子网	96
在您的默认 VPC 内启动 EC2 实例。	96
使用控制台启动 EC2 实例	97
使用命令行启动 EC2 实例	97
删除您的默认子网和默认 VPC	97
创建默认 VPC	97
创建默认子网	98
IP 地址	100
私有 IPv4 地址	101
公有 IPv4 地址	101
IPv6 地址	102

子网的 IP 寻址行为	102
使用 IP 地址	102
修改子网的公有 IPv4 寻址属性	103
修改子网的 IPv6 寻址属性	103
在实例启动期间分配公有 IPv4 地址	103
在实例启动期间分配 IPv6 地址	104
向实例分配 IPv6 地址	105
取消分配给实例的 IPv6 地址	105
API 和命令概览	105
迁移到 IPv6	106
示例：在具有公有和私有子网的 VPC 内启用 IPv6	107
步骤 1：将 IPv6 CIDR 块与您的 VPC 和子网关联	109
步骤 2：更新路由表	110
步骤 3：更新安全组规则	110
步骤 4：更改实例类型	111
步骤 5：为实例分配 IPv6 地址	111
步骤 6：(可选) 在实例中配置 IPv6	112
安全性	118
安全组与网络 ACL 的比较	118
安全组	119
安全组基本信息	119
您的 VPC 的默认安全组	120
安全组规则	121
EC2-Classic 和 EC2-VPC 安全组之间的差异	122
使用安全组	122
网络 ACL	126
网络 ACL 基本信息	126
网络 ACL 规则	127
默认网络 ACL	127
自定义网络 ACL	128
临时端口	131
使用网络 ACL	131
示例：控制对子网中实例的访问	134
API 和命令概览	137
您的 VPC 的推荐网络 ACL 规则	138
场景 1 的推荐规则	138
场景 2 的推荐规则	140
场景 3 的推荐规则	145
场景 4 的推荐规则	150
控制访问	151
针对 AWS CLI 或软件开发工具包的策略示例	152
控制台的策略示例	158
VPC 流日志	165
流日志基础知识	165
流日志记录	166
流日志限制	168
发布到 CloudWatch Logs	168
发布到 Amazon S3	171
使用流日志	175
故障排除	178
VPC 联网组件	180
网络接口	180
路由表	181
路由表基本信息	181
路由优先级	184
路由选项	185
使用路由表	188

API 和命令概览	191
Internet 网关	192
启用 Internet 访问	193
创建带有 Internet 网关的 VPC	194
仅出口 Internet 网关	197
仅出口 Internet 网关基础知识	198
使用仅出口 Internet 网关	198
API 和 CLI 概述	200
NAT	200
NAT 网关	200
NAT 实例	216
NAT 实例与 NAT 网关的比较	223
DHCP 选项集	224
DHCP 选项集概述	224
Amazon DNS 服务器	225
更改 DHCP 选项	226
使用 DHCP 选项集	226
API 和命令概览	227
DNS	228
DNS 主机名	228
VPC 中的 DNS 支持	229
DNS 限制	230
查看您的 EC2 实例的 DNS 主机名称	230
更新您的 VPC 的 DNS 支持	231
使用私有托管区域	231
VPC 对等	232
弹性 IP 地址	232
弹性 IP 地址基础信息	232
使用弹性 IP 地址	233
API 和 CLI 概述	234
VPC 终端节点	235
接口终端节点	237
网关终端节点	249
使用 VPC 终端节点 控制对服务的访问	262
删除集群VPC 终端节点	263
VPC 终端节点服务	263
概述	264
终端节点服务可用区注意事项	266
终端节点服务限制	266
创建 VPC 终端节点服务配置	267
为您的终端节点服务添加和删除权限	268
更改网络负载均衡器和接受设置	269
接受和拒绝接口终端节点连接请求	270
为终端节点服务创建和管理通知	271
对连接信息使用代理协议	272
添加或删除 VPC 终端节点服务标签	273
删除终端节点服务配置	273
ClassicLink	274
VPN 连接	275
限制	276
VPC 和子网	276
DNS	276
弹性 IP 地址 (IPv4)	276
网关	277
网络 ACL	277
网络接口	277
路由表	278

安全组	278
VPC 对等连接	279
VPC 终端节点	279
AWS Site-to-Site VPN 连接	279
VPC 共享	279
文档历史记录	281

什么是 Amazon VPC ?

Amazon Virtual Private Cloud (Amazon VPC) 允许您在已定义的虚拟网络内启动 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。

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。如果您是首次使用 Amazon EC2，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [什么是 Amazon EC2 ?](#) 以获取简要概述。

内容

- [VPC 和子网 \(p. 1\)](#)
- [支持的平台 \(p. 1\)](#)
- [默认和非默认 VPC \(p. 2\)](#)
- [访问 Internet \(p. 2\)](#)
- [访问企业或家庭网络 \(p. 4\)](#)
- [通过 AWS PrivateLink 访问服务 \(p. 5\)](#)
- [AWS 私有全球网络注意事项 \(p. 6\)](#)

VPC 和子网

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

子网是您的 VPC 内的 IP 地址范围。您可以在指定子网内启动 AWS 资源。对必须连接 Internet 的资源使用公有子网，而对将不会连接到 Internet 的资源使用私有子网。有关公有子网和私有子网的更多信息，请参阅[VPC 和子网基础知识 \(p. 75\)](#)。

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，请参阅[安全性 \(p. 118\)](#)。

支持的平台

Amazon EC2 的原始版本支持一个与其他客户共享的扁平化网络，这个网络称为 EC2-Classic 平台。早期的 AWS 账户仍支持此平台，并且可在 EC2-Classic 或 VPC 内启动实例。2013 年 12 月 4 日之后创建的账户仅支持 EC2-VPC。有关更多信息，请参阅[检测支持的平台以及您是否有默认 VPC \(p. 95\)](#)。

通过将实例启动到 VPC (而不是 EC2-Classic)，您能够：

- 为启动和停止时保持不变的实例分配静态私有 IPv4 地址
- (可选) 将 IPv6 CIDR 块与您的 VPC 关联，并为您的实例分配 IPv6 地址

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

默认和非默认 VPC

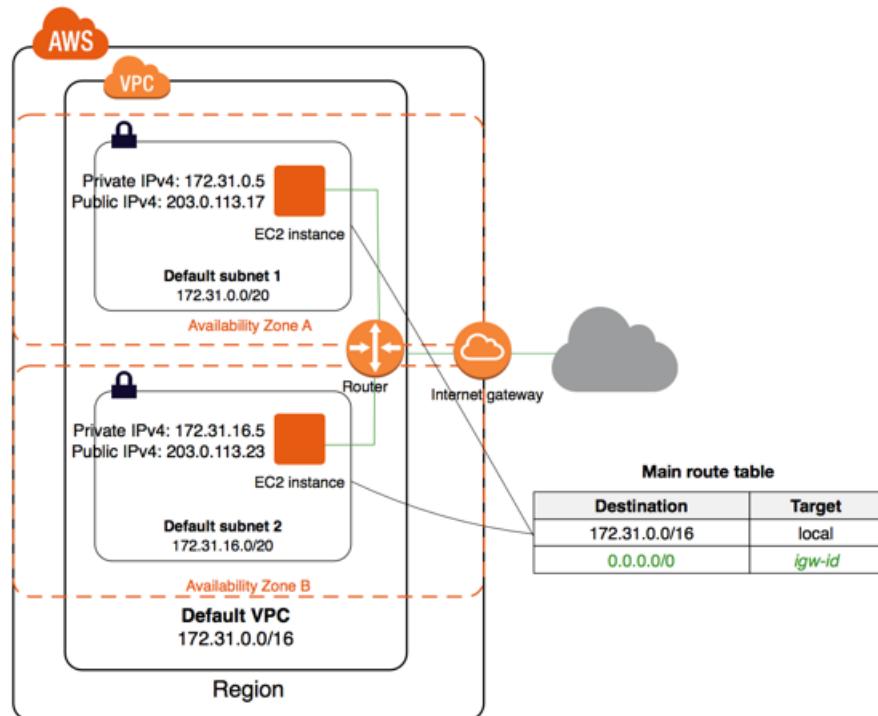
如果您的账户仅支持 EC2-VPC 平台，则它附带有一个默认 VPC，该 VPC 在每个可用区中都有一个默认子网。默认 VPC 具有 EC2-VPC 提供的高级功能所带来的种种好处，并且已准备好供您使用。如果您有默认 VPC 并且在启动实例时未指定子网，该实例就会启动到您的默认 VPC 中。您可以将实例启动到默认 VPC 中，而无需对 Amazon VPC 有任何了解。

不论您的账户支持哪种平台，您都可以创建您自己的 VPC 并根据需要对其进行配置。这称为非默认 VPC。您在非默认 VPC 中创建的子网和您在默认 VPC 中创建的额外子网称为非默认子网。

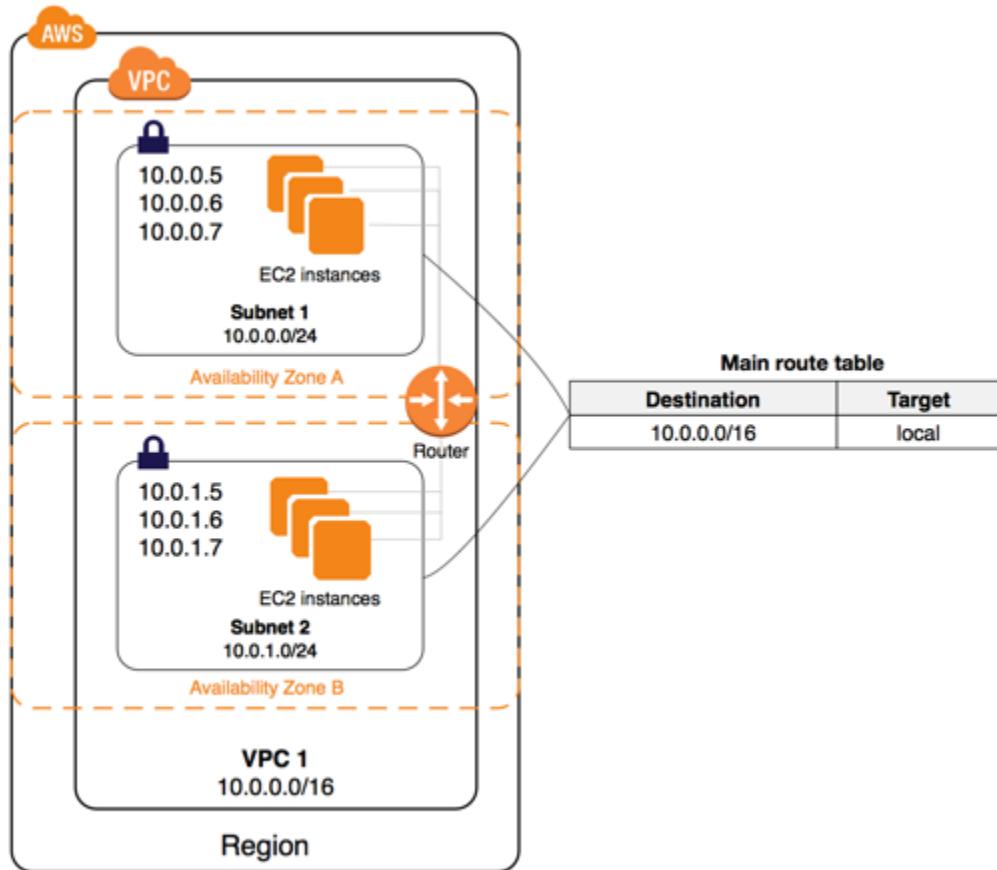
访问 Internet

您可以控制在 VPC 之外的 VPC 访问资源中启动实例的方式。

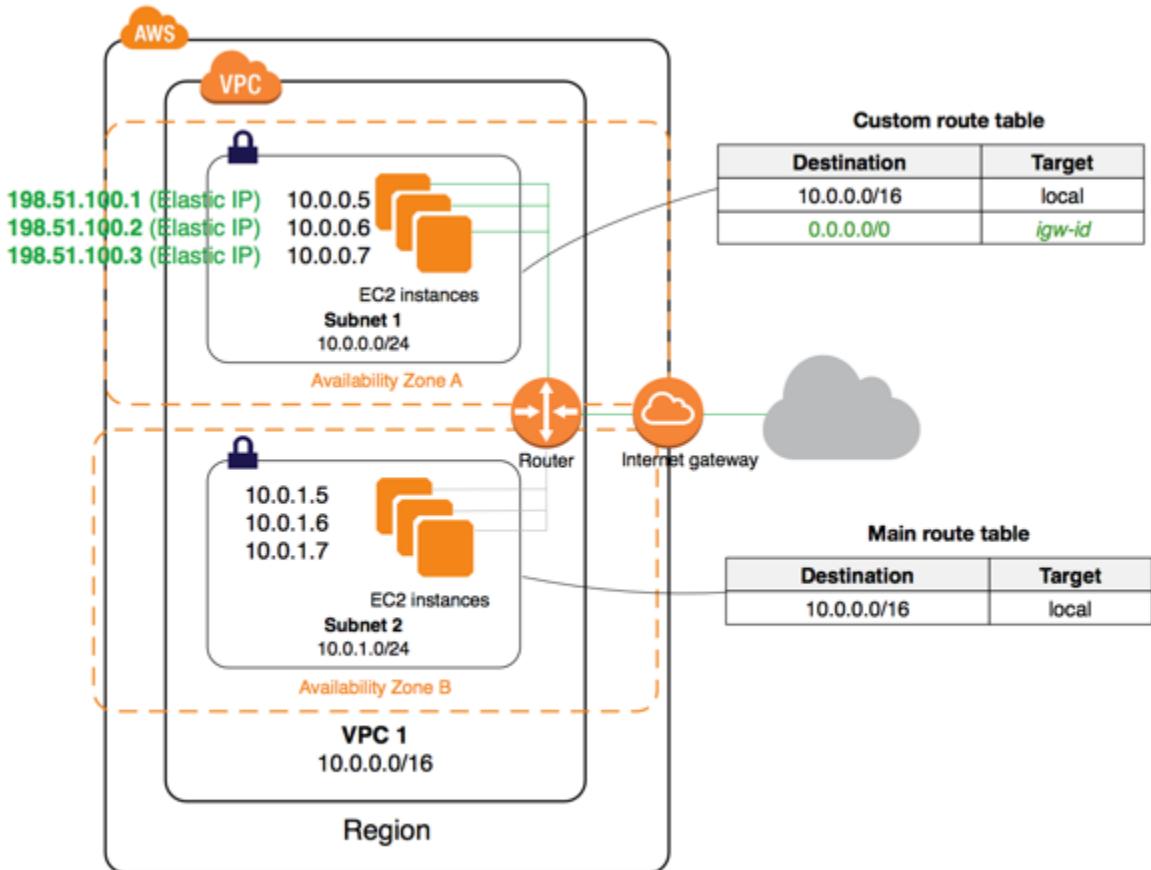
您的默认 VPC 包含一个 Internet 网关，而且每个默认子网都是一个公有子网。您在默认子网中启动的每个实例都有一个私有 IPv4 地址和一个公有 IPv4 地址。这些实例可以通过 Internet 网关与 Internet 通信。通过 Internet 网关，您的实例可通过 Amazon EC2 网络边界连接到 Internet。



默认情况下，您启动到非默认子网中的每个实例都有一个私有 IPv4 地址，但没有公有 IPv4 地址，除非您在启动时特意指定一个，或者修改子网的公有 IP 地址属性。这些实例可以相互通信，但无法访问 Internet。



您可以通过以下方式为在非默认子网中启动的实例启用 Internet 访问：将一个 Internet 网关附加到该实例的 VPC (如果其 VPC 不是默认 VPC)，然后将一个弹性 IP 地址与该实例相关联。



或者，您也可以为 IPv4 流量使用网络地址转换 (NAT) 设备，以允许 VPC 中的实例发起到 Internet 的出站连接，但阻止来自 Internet 的未经请求的入站连接。NAT 将多个私有 IPv4 地址映射到一个公有 IPv4 地址。NAT 设备有一个弹性 IP 地址，并通过 Internet 网关与 Internet 相连。您可以通过 NAT 设备将私有子网中的实例连接到 Internet，NAT 设备会将来自实例的流量路由到 Internet 网关，并将所有响应路由到该实例。

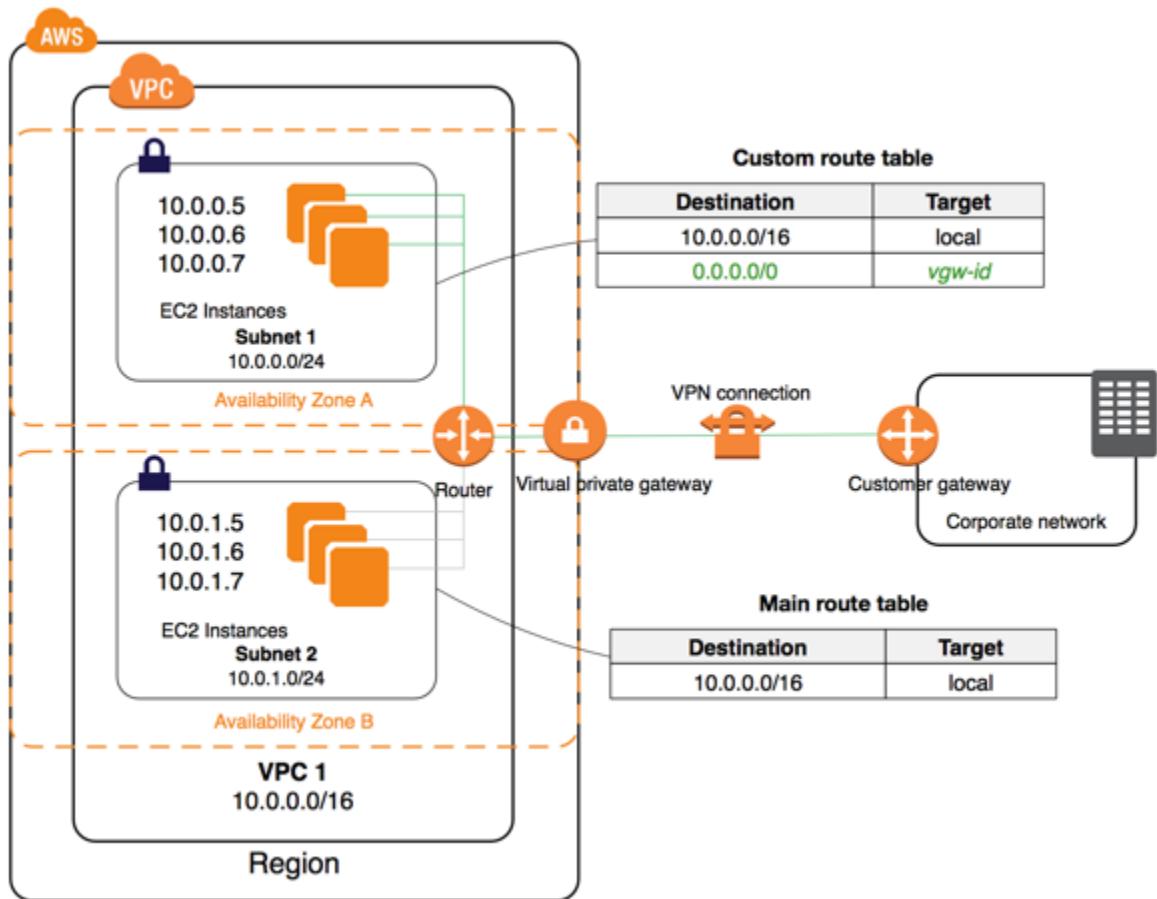
有关更多信息，请参阅 [NAT \(p. 200\)](#)。

您可以选择将 Amazon 提供的 IPv6 CIDR 块与您的 VPC 关联，并为您的实例分配 IPv6 地址。实例可以通过 Internet 网关经由 IPv6 连接到 Internet。或者，实例也可以使用仅出口 Internet 网关经由 IPv6 发起到 Internet 的出站连接。有关更多信息，请参阅 [仅出口 Internet 网关 \(p. 197\)](#)。IPv6 流量独立于 IPv4 流量；您的路由表必须包含单独的 IPv6 流量路由。

访问企业或家庭网络

您可以选择使用 IPsec AWS Site-to-Site VPN 连接将您的 VPC 与公司的数据中心相连，并将 AWS 云作为数据中心的延伸。

Site-to-Site VPN 连接由附加到您的 VPC 的虚拟专用网关和位于您的数据中心的客户网关组成。虚拟专用网关是 Site-to-Site VPN 连接在 Amazon 一端的 VPN 集线器。客户网关是 Site-to-Site VPN 连接在您这一端的实体设备或软件设备。

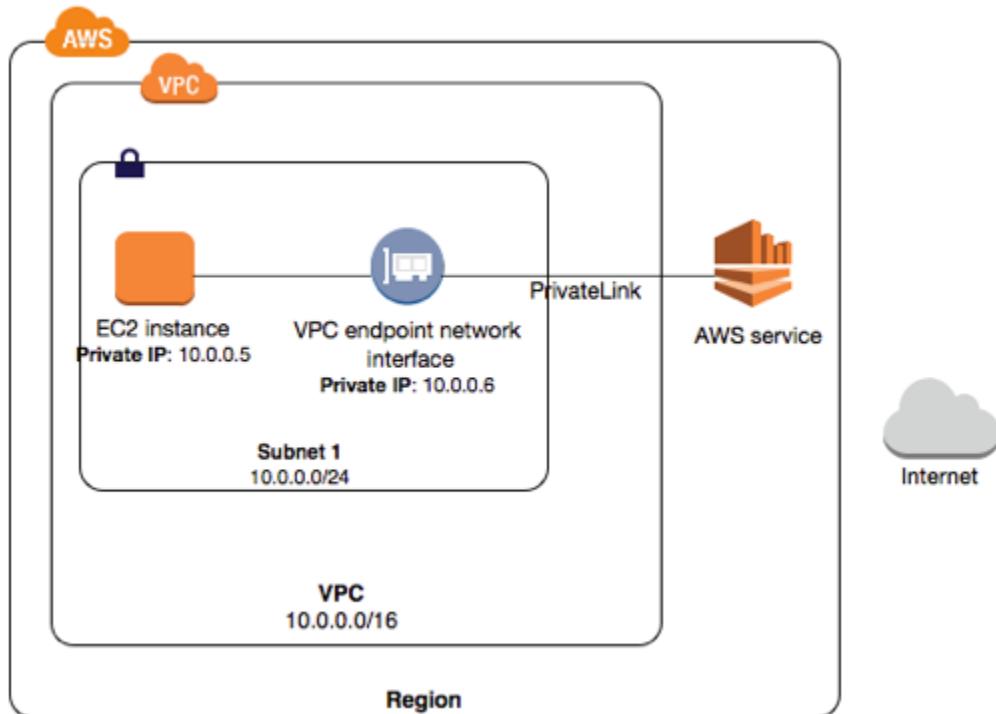


有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的[什么是 AWS Site-to-Site VPN？](#)。

通过 AWS PrivateLink 访问服务

AWS PrivateLink 是一项具有高可用性的可扩展技术，使您能够将您的 VPC 私密地连接到支持的 AWS 服务、由其他 AWS 账户托管的服务（VPC 终端节点服务）以及支持的 AWS Marketplace 合作伙伴服务。您无需 Internet 网关、NAT 设备、公有 IP 地址、AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接就能与该服务通信。您的 VPC 和服务之间的流量不会脱离 Amazon 网络。

要使用 AWS PrivateLink，请在您的 VPC 中为服务创建接口 VPC 终端节点。此操作将在您的子网中创建一个带有私有 IP 地址的弹性网络接口，用作发送到服务的流量的入口点。有关更多信息，请参阅[VPC 终端节点 \(p. 235\)](#)。



您可以创建自己的 AWS PrivateLink 支持的服务（终端节点服务）并使其他 AWS 客户能够访问您的服务。有关更多信息，请参阅[VPC 终端节点服务 \(AWS PrivateLink\) \(p. 263\)](#)。

AWS 私有全球网络注意事项

AWS 以其高性能、低延迟的私有全球网络，提供安全的云计算环境以支持您的网络需求。AWS 区域连接到多个 Internet 服务提供商 (ISP) 以及私有全球网络主干，从而为客户发送的跨区域流量提供改进的网络性能。

请注意以下事项：

- 可用区中的流量或所有区域中可用区之间的流量通过 AWS 私有全球网络路由。
- 区域之间的流量始终通过 AWS 私有全球网络路由，但 中国区域 除外。

网络数据包丢失可能因多种因素导致，包括网络流碰撞、低级（第 2 层）错误和其他网络故障。我们设计并运行我们的网络以最大限度地减少数据包丢失。我们跨连接 AWS 区域的全球骨干网衡量数据包丢失率 (PLR)。我们运营我们的骨干网络，目标是使 p99 达到每小时 PLR 低于 0.0001%。

如何开始使用 Amazon VPC

要获得有关 Amazon VPC 的实践介绍，请完成[Amazon VPC 入门 \(p. 9\)](#)。此练习将指导您完成创建带有公有子网的非默认 VPC 并在您的子网内启动实例的步骤。

如果您有默认 VPC，且希望在不对您的 VPC 进行任何额外配置的情况下开始将实例启动到 VPC 中，请参阅[在您的默认 VPC 内启动 EC2 实例。 \(p. 96\)](#)。

要了解 Amazon VPC 的基本方案，请参阅[场景和示例 \(p. 23\)](#)。您可以通过其他满足您的需求的方式配置您的 VPC 和子网。

下表列出了在您使用此服务时可能为您提供帮助的相关资源。

资源	描述
Amazon Virtual Private Cloud 连接性选项	提供了网络连接性选项概览。
Amazon VPC forum	社区论坛，在这里可以讨论关于 Amazon VPC 的技术性问题。
AWS 开发人员资源	这是一个帮助您入门的资源整合点，您可以在这里找到相关的文档、代码示例、发行说明和其他信息，帮助您使用 AWS 构建创新的应用程序。
AWS 支持中心	AWS Support 主页。
联系我们	这是一个有关查询的资源整合点，可帮助您查询有关 AWS 计费、账户、事件方面的信息。

访问 Amazon VPC

Amazon VPC 提供基于 Web 的用户界面，即 Amazon VPC 控制台。如果您已注册 AWS 账户，可以通过登录 AWS 管理控制台并选择 VPC 来访问 Amazon VPC 控制台。

如果倾向于使用命令行界面，您可使用以下选项：

AWS Command Line Interface (AWS CLI)

提供大量 AWS 服务的相关命令，并支持 Windows、macOS 和 Linux/Unix。要了解其用法，请参阅 [AWS Command Line Interface 用户指南](#)。有关 Amazon VPC 的命令的更多信息，请参阅 [ec2](#)。

适用于 Windows PowerShell 的 AWS 工具

为在 PowerShell 环境中编写脚本的用户提供大量 AWS 服务的相关命令。要了解其用法，请参阅 [适用于 Windows PowerShell 的 AWS 工具 用户指南](#)。

Amazon VPC 提供查询 API。这些请求属于 HTTP 或 HTTPS 请求，需要使用 HTTP 动词 GET 或 POST 以及一个名为 Action 的查询参数。有关更多信息，请参阅 Amazon EC2 API Reference 中的 [操作](#)。

为了使用特定语言的 API 而非通过 HTTP 或 HTTPS 提交请求来构建应用程序，AWS 为软件开发人员提供了库文件、示例代码、教程和其他资源。这些库文件提供可自动执行任务的基本功能，例如以加密方式对请求签名、重试请求和处理错误响应。有关更多信息，请参阅 [AWS SDKs and Tools](#)。

Amazon VPC 定价

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。使用 Site-to-Site VPN 连接和 NAT 网关需要支付一定的费用。有关更多信息，请参阅 [Amazon VPC 定价](#) 和 [Amazon EC2 定价](#)。

Amazon VPC 限制

您可以提供的 Amazon VPC 组成部分数目有限。您可以请求增加部分限制的值。有关更多信息，请参阅 [Amazon VPC 限制 \(p. 276\)](#)。

PCI DSS 合规性

Amazon VPC 支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。有关 PCI DSS 的更多信息，包括如何请求 AWS PCI Compliance Package 的副本，请参阅 [PCI DSS 第 1 级](#)。

Amazon VPC 入门

以下教程将帮助您快速设置非默认 VPC。如果 VPC 中的资源需要通过 IPv6 进行通信，则可以为 VPC 设置关联的 IPv6 CIDR 块。否则，使用关联的 IPv4 CIDR 块设置 VPC。

如果您已经有一个默认 VPC，则可以开始将实例启动到您的默认 VPC，而不必创建或配置新的 VPC。有关更多信息，请参阅 [在您的默认 VPC 内启动 EC2 实例。 \(p. 96\)](#)。

教程

- [适用于 Amazon VPC 的 IPv4 入门 \(p. 9\)](#)
- [适用于 Amazon VPC 的 IPv6 入门 \(p. 16\)](#)

适用于 Amazon VPC 的 IPv4 入门

在本练习中，您将创建一个具有 IPv4 CIDR 块的 VPC，创建一个具有 IPv4 CIDR 块的子网，并将一个面向公众的实例启动到您的子网中。您的实例将能够与 Internet 通信，并且您将能够使用 SSH (如果您的实例为 Linux 实例) 或远程桌面 (如果您的实例为 Windows 实例) 从本地计算机访问您的实例。在真实应用环境下，您可以使用此方案创建面向公众的 Web 服务器；例如，托管一个博客。

Note

本练习旨在帮助您快速设置您自己的非默认 VPC。如果您已有一个默认 VPC 并希望在其中开始启动实例 (同时不创建或配置新 VPC)，请参阅 [在您的默认 VPC 中启动 EC2 实例](#)。如果您要开始设置支持 IPv6 的非默认 VPC，请参阅 [适用于 Amazon VPC 的 IPv6 入门](#)。

要完成本练习，您将执行以下操作：

- 创建一个带单个公有子网的非默认 VPC。子网可以让您根据自己的安全和运营需要，对实例进行分组。公有子网是可以通过 Internet 网关访问 Internet 的子网。
- 为您的实例创建仅允许流量通过特定端口的安全组。
- 将 Amazon EC2 实例启动到您的子网中。
- 将弹性 IP 地址与您的实例相关联。这将允许您的实例访问 Internet。

在首次使用 Amazon VPC 之前，您必须先注册 Amazon Web Services (AWS)。在您注册时，您的 AWS 账户会自动注册 AWS 中的所有服务，包括 Amazon VPC。如果您尚未创建 AWS 账户，请转至 <https://aws.amazon.com/>，然后选择创建免费账户。

Note

本练习假设您的账户仅支持 EC2-VPC 平台。如果您的账户还支持较旧的 EC2-Classic 平台，则您仍然可以按照本练习中的步骤操作；不过，您的账户中将不会有与非默认 VPC 进行比较的默认 VPC。有关更多信息，请参阅 [支持的平台 \(p. 1\)](#)。

任务

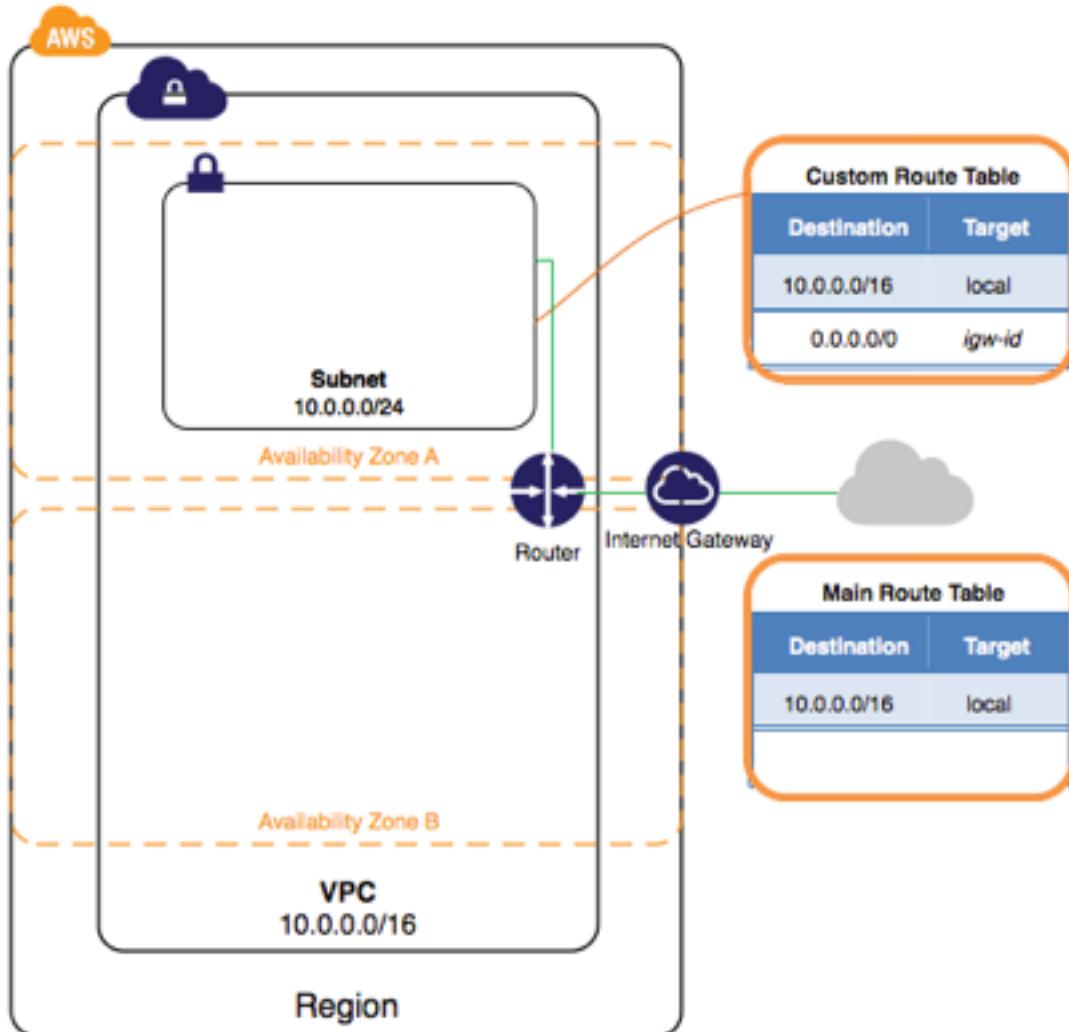
- [步骤 1：创建 VPC \(p. 10\)](#)
- [步骤 2：创建安全组 \(p. 12\)](#)
- [步骤 3：将实例启动到 VPC 中 \(p. 13\)](#)
- [步骤 4：为您的实例分配弹性 IP 地址 \(p. 15\)](#)
- [第 5 步：清除 \(p. 16\)](#)

步骤 1：创建 VPC

在此步骤中，您将在 Amazon VPC 控制台中使用 Amazon VPC 向导创建 VPC。本向导为您执行以下步骤：

- 创建一个具有 /16 IPv4 CIDR 块 (一个包含 65536 个私有 IP 地址的网络) 的 VPC。有关 CIDR 表示法和 VPC 大小的更多信息，请参阅[您的 VPC](#)。
- 将 Internet 网关连接到 VPC。有关 Internet 网关的更多信息，请参阅[Internet 网关](#)。
- 在 VPC 中创建一个大小为 /24 的 IPv4 子网 (一个包含 256 个私有 IP 地址的网络范围)。
- 创建一个自定义路由表，并将其与您的子网相关联，以便在子网与 Internet 网关之间进行通信。有关路由表的更多信息，请参阅[路由表](#)。

下图表示了您的 VPC 在您完成此步骤之后的架构。



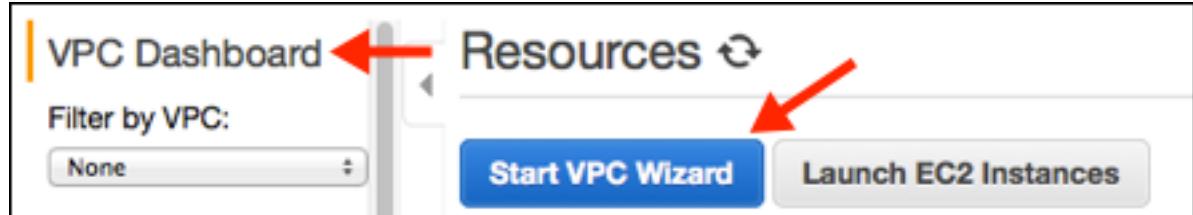
Note

本练习介绍 VPC 向导的第一个方案。有关其他方案的更多信息，请参阅[Amazon VPC 方案](#)。

使用 Amazon VPC 向导创建 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在右上角的导航栏中，记下您要在其中创建 VPC 的区域。确保继续在相同区域中操作本练习的剩余部分，因为您无法将实例启动到不同区域的 VPC 中。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[区域和可用区](#)。
3. 在导航窗格中，选择 VPC 控制面板。在控制面板中，选择 Launch VPC Wizard（启动 VPC 向导）。



Note

请勿在导航窗格中选择 Your VPCs（您的 VPC）；您无法使用该页面上的 Create VPC（创建 VPC）按钮访问 VPC 向导。

4. 选择第一个选项，即 VPC with a Single Public Subnet，然后选择 Select。
5. 在配置页面上的 VPC name 字段中输入您的 VPC 的名称（例如，my-vpc），并在 Subnet name 字段中输入您的子网的名称。这可帮助您在创建 VPC 和子网后在 Amazon VPC 控制台中识别它们。在本练习中，您可以保留页面上的其余配置设置，并选择 Create VPC。
(可选) 如果您愿意，可按如下所示修改配置设置，然后选择 Create VPC。
 - IPv4 CIDR block 显示您将用于 VPC 的 IPv4 地址范围 (10.0.0.0/16)，Public subnet's IPv4 CIDR 字段显示您将用于子网的 IPv4 地址范围 (10.0.0.0/24)。如果您不想使用默认 CIDR 范围，可以指定您自己的范围。有关更多信息，请参阅[VPC 和子网大小调整](#)。
 - Availability Zone 列表可让您选择要在其中创建子网的可用区。您可以保留 No Preference 以便让 AWS 为您选择可用区。有关更多信息，请参阅[区域和可用区](#)。
 - 在服务终结点部分中，您可以选择要在其中创建连接到相同区域的 Amazon S3 的 VPC 端点的子网。有关更多信息，请参阅[VPC 端点](#)。
 - 将 Enable DNS hostnames 选项设置为 Yes 可确保启动到您的 VPC 中的实例接收 DNS 主机名称。有关更多信息，请参阅[在您的 VPC 中使用 DNS](#)。
 - Hardware tenancy 选项可让您选择启动到您的 VPC 中的实例是在共享硬件上运行还是在专用硬件上运行。选择专用租户将产生额外费用。有关硬件租赁的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[专用实例](#)部分。
6. 状态窗口会显示工作的进度。工作完成后，选择 OK 关闭状态窗口。
7. Your VPCs 页面将显示您的默认 VPC 和您刚创建的 VPC。您创建的 VPC 是非默认 VPC，因此 Default VPC 列将显示 No。

	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy
<input type="checkbox"/>	vpc-6f71e...		available	172.31.0.0/16	dopt-6271ed0e	rtb-6071ed0c	acl-6771ed0b	Default
<input checked="" type="checkbox"/>	my-vpc	vpc-cd65...	available	10.0.0.0/16	dopt-6271ed0e	rtb-b77befd2	acl-0b931c6e	Default

查看有关您的 VPC 的信息

创建了 VPC 之后，您可以查看关于子网、Internet 网关和路由表的信息。您创建的 VPC 有两个路由表——一个所有 VPC 默认都会有的主路由表，一个由向导创建的自定义路由表。自定义路由表与您的子网相关联，这

意味着该表中的路由将确定子网数据流的传输方式。如果您向您的 VPC 添加一个新的子网，那么它默认使用主路由表。

查看有关您的 VPC 的信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。记下您创建的 VPC 的名称和 ID（查看 Name 和 VPC ID 列）。您将使用此信息确定与您的 VPC 关联的组件。
3. 在导航窗格中，选择 Subnets。控制台将显示您创建 VPC 时创建的子网。您可以通过 Name 列中的子网名称来识别子网，或者您可以使用上一步骤中获取的 VPC 信息并查看 VPC 列。
4. 在导航窗格中，选择 Internet Gateways。您可以通过查看 VPC 列找到与您的 VPC 连接的 Internet 网关，该列显示了 VPC 的 ID 和名称（如果适用）。
5. 在导航窗格中，选择 Route Tables。有两个路由表与 VPC 关联。选择自定义路由表（Main 列显示 No），然后选择 Routes 选项卡以便在详细信息窗格中显示路由信息：
 - 该表格中的第一行是本地路由，可允许 VPC 内的实例进行通信。此路由默认情况下存在于每个路由表中，您不能删除它。
 - 第二行显示了 Amazon VPC 向导添加的路由，它允许目标为 VPC (0.0.0.0/0) 外部的 IPv4 地址的流量从子网流向 Internet 网关。
6. 选择主路由表。主路由表拥有一个本地路由，但没有其他路由。

步骤 2：创建安全组

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

您的 VPC 带有默认的安全组。所有启动时未与其他安全组关联的实例都将与默认安全组相关联。在本练习中，您将创建一个新的安全组 WebServerSG，并在您将实例启动到您的 VPC 中时指定此安全组。

WebServerSG 安全组规则

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

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

0.0.0.0/0	全部	全部	允许所有出站 IPv4 通信的默认出站规则。
-----------	----	----	------------------------

创建 WebServerSG 安全组

您可以使用 Amazon VPC 控制台创建安全组。

创建 WebServerSG 安全组并添加规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 在 Group name 字段中，输入 WebServerSG 作为安全组的名称，并提供说明。您可以选择使用 Name tag 字段来为具有密钥 Name 和指定的值的安全组创建标记。
5. 从 VPC 菜单中选择您 VPC 的 ID，然后选择 Yes, Create。
6. 选择您刚刚创建的 WebServerSG 安全组（可在 Group Name 列中查看其名称）。
7. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 从 Type (类型) 列表中选择 HTTP，然后在 0.0.0.0/0Source (源) 字段中输入。
 - b. 选择 Add another rule，从 Type 列表中选择 HTTPS，然后在 Source 字段中输入 0.0.0.0/0。
 - c. 选择 Add another rule。如果您要启动 Linux 实例，请从 Type 列表中选择 SSH，如果您要启动 Windows 实例，则从 Type 列表中选择 RDP。在 Source (源) 字段中输入您网络的公有 IP 地址范围。如果您不知道地址范围，则可以使用 0.0.0.0/0 来完成此练习。

Important

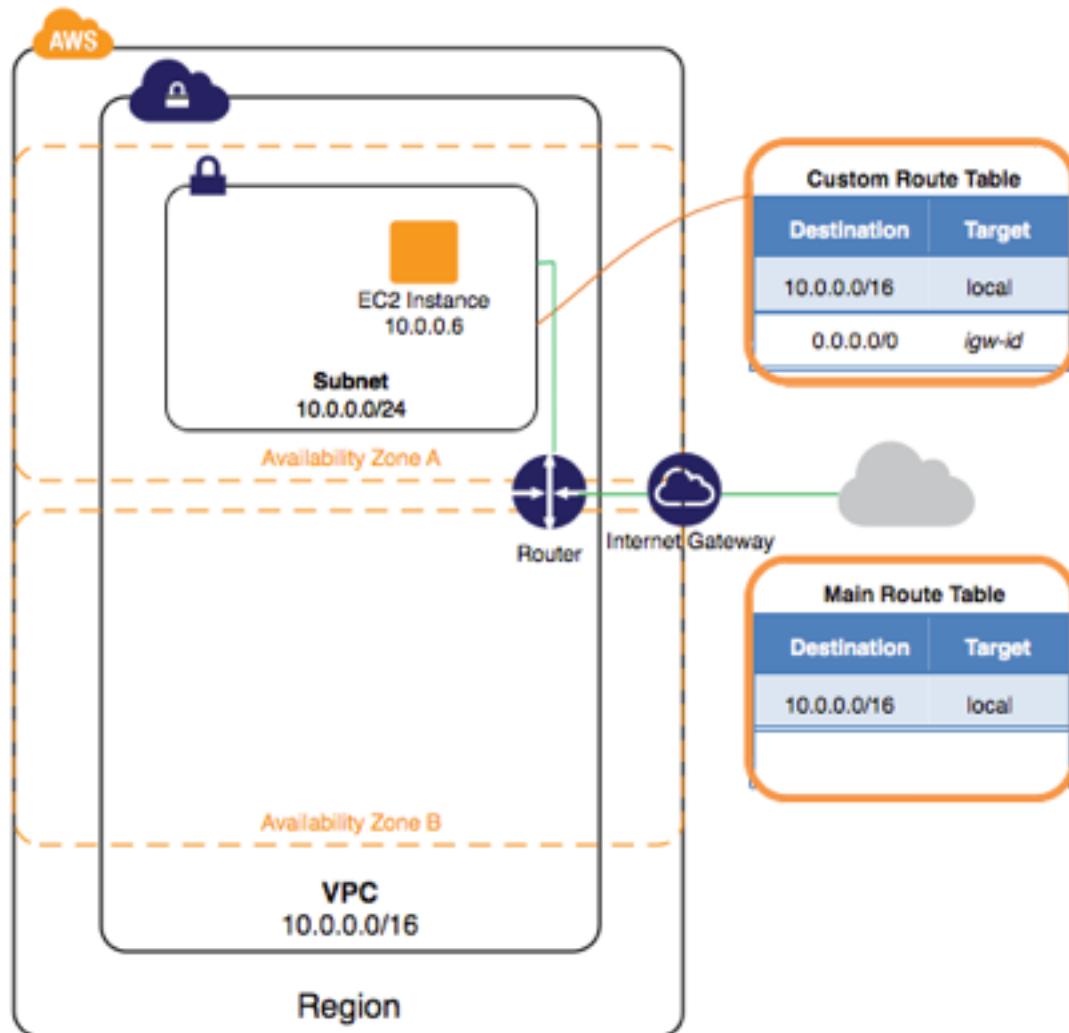
如果您使用的是 0.0.0.0/0，则可以允许所有 IP 地址使用 SSH 或 RDP 访问您的实例。您可以在本次简短的练习中使用此方法，但是在生产环境中使用其安全性有所欠缺。在生产中，您将仅授权特定 IP 地址或地址范围访问您的实例。

- d. 选择 Save (保存)。

步骤 3：将实例启动到 VPC 中

当您将 EC2 实例启动到 VPC 中时，您必须指定要在其中启动实例的子网。在这种情况下，您会将实例启动到您创建的 VPC 的公有子网中。您将在 Amazon EC2 控制台中使用 Amazon EC2 启动向导来启动您的实例。

下图表示了您的 VPC 在您完成此步骤之后的架构。



如何将一个 EC2 实例推送到 VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在右上角的导航栏中，确保选择您在其中创建了 VPC 和安全组的同一区域。
3. 在控制面板中，选择 Launch Instance。
4. 在向导的第一页上，选择您要使用的 AMI。在本练习中，我们建议您选择 Amazon Linux AMI 或 Windows AMI。
5. 在 Choose an Instance Type (选择一种实例类型) 页面上，您可以选择要启动的实例的硬件配置和大小。默认情况下，向导会基于您选择的 AMI 选择第一个可用实例类型。您可以保留默认选择，然后选择 Next: Configure Instance Details。
6. 在 Configure Instance Details 页上，从 Network 列表中选择您创建的 VPC，然后从 Subnet 列表中选择子网。保留默认设置的其余部分，然后完成向导中的后续页面，直至到达 Add Tags 页面。
7. 在 Add Tags 页面上，您可以为实例添加 Name 标签；例如 Name=MyWebServer。这有助于您启动实例后在 Amazon EC2 控制台中识别您的实例。完成时选择 Next: Configure Security Group。
8. 在 Configure Security Group (配置安全组) 页面上，向导会自动定义 launch-wizard-x 安全组，从而让您可以连接到您的实例。而是选择 Select an existing security group 选项，选择您之前创建的 WebServerSG 组，然后选择 Review and Launch。
9. 在 Review Instance Launch 页面上，检查您的实例的详细信息，然后选择 Launch。

10. 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，您可以选择现有密钥对，也可以创建新的密钥对。如果要创建新的密钥对，请确保您将文件下载并保存在安全的位置。实例启动后，您需要使用私有密钥的内容连接到实例。

要启动您的实例，请选中确认复选框，然后选择 Launch Instances。

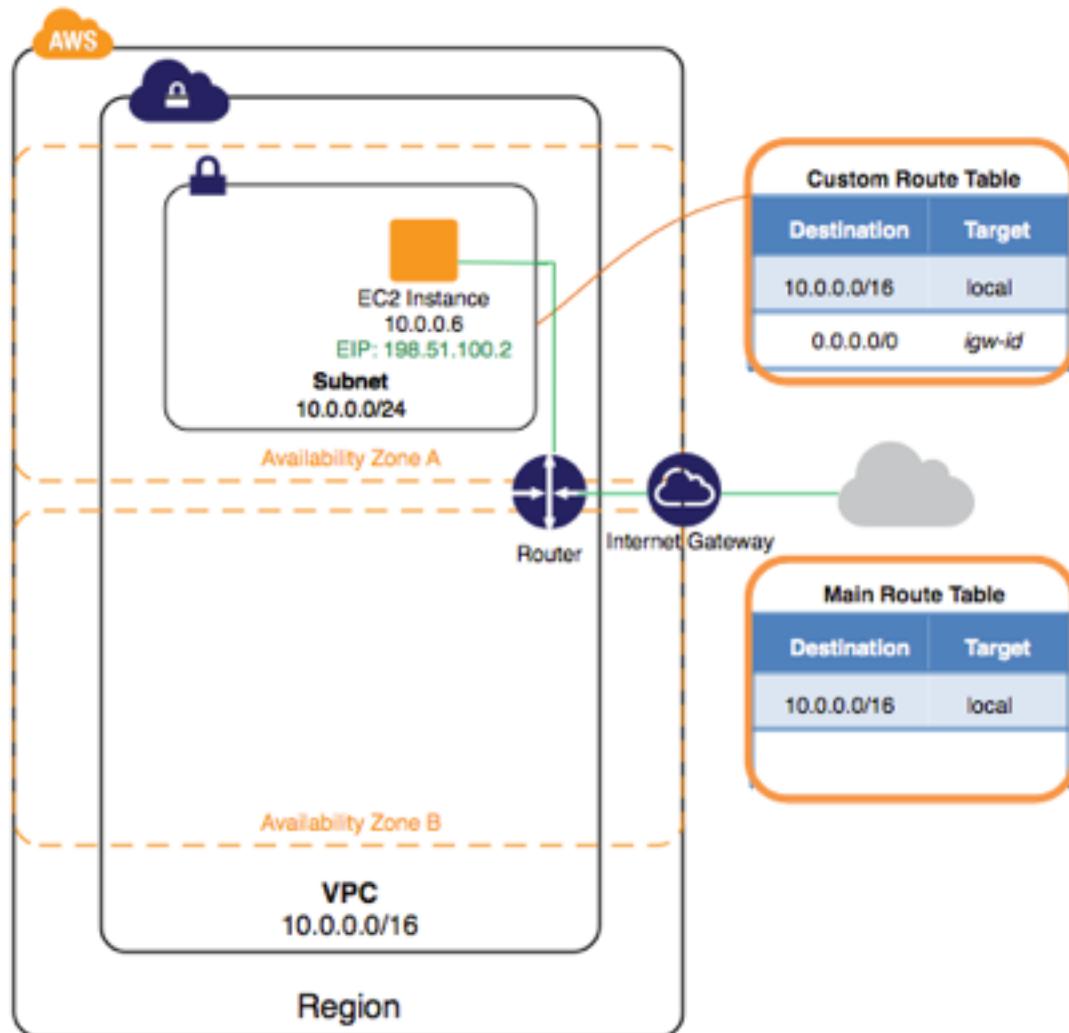
11. 在确认页面上，选择 View Instances 可在 Instances 页面上查看您的实例。选择您的实例，然后在 Description 选项卡中查看其详细信息。Private IPs 字段显示从您的子网中的 IP 地址范围分配给您的实例的私有 IP 地址。

有关 Amazon EC2 启动向导中的可用选项的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[启动实例](#)。

步骤 4：为您的实例分配弹性 IP 地址

在上一步中，您已将您的实例启动到一个公有子网（带有到 Internet 网关的路由的子网）中。不过，您的子网中的实例还需要一个公有 IPv4 地址才能与 Internet 通信。默认情况下，非默认 VPC 中的实例不会分配到公有 IPv4 地址。在此步骤中，您将向您的账户分配一个弹性 IP 地址，然后将它与您的实例关联。有关弹性 IP 地址的更多信息，请参阅[弹性 IP 地址](#)。

下图表示了您的 VPC 在您完成此步骤之后的架构。



如何指定和分配一个弹性 IP 地址

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address (分配新地址)，然后选择 Allocate (分配)。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

4. 从列表中选择弹性 IP 地址，选择 Actions，然后选择 Associate Address。
5. 对于 Resource type (资源类型)，请确保选择 Instance (实例)。从 Instance (实例) 列表中选择实例。完成后，选择 Associate (关联)。

现在就可以通过 Internet 访问您的实例了。您可以使用 SSH 或远程桌面从您的家庭网络通过您的实例的弹性 IP 地址连接到该实例。有关如何连接到 Linux 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[连接到 Linux 实例](#)。有关如何连接到 Windows 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[使用 RDP 连接到 Windows 实例](#)。

这样就完成了本次练习；您可以选择继续在 VPC 中使用您的实例，如果您不需要该实例，则可以将其终止并释放它的弹性 IP 地址以避免产生费用。您也可以删除 VPC — 请注意，您无需为本练习中创建的 VPC 和 VPC 组件（如子网和路由表）付费。

第 5 步：清除

在删除一个 VPC 之前，您必须终止在该 VPC 中正在运行的任何实例。然后，您可以使用 VPC 控制台删除 VPC。VPC 控制台还会自动将与 VPC 关联的任何资源取消关联并删除这些资源，例如子网、安全组、网络 ACL、DHCP 选项集、路由表和 Internet 网关。

终止实例、释放弹性 IP 地址并删除 VPC

1. 打开 Amazon EC2 控制台 [https://console.aws.amazon.com/ec2/。](https://console.aws.amazon.com/ec2/)
2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Instance State 和 Terminate。
4. 在对话框中，展开 Release attached Elastic IPs 部分，然后选中弹性 IP 地址旁边的复选框。选择 Yes, Terminate。
5. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
6. 在导航窗格中，选择 Your VPCs。
7. 选择 VPC，选择 Actions，然后选择 Delete VPC。
8. 在提示进行确认时，请选择 Delete VPC (删除 VPC)。

适用于 Amazon VPC 的 IPv6 入门

在本练习中，您将创建一个具有 IPv6 CIDR 块的 VPC，创建一个具有 IPv6 CIDR 块的子网，并将一个面向公众的实例启动到您的子网中。您的实例将能够通过 IPv6 与 Internet 通信，并且您将能够使用 SSH（如果您的实例为 Linux 实例）或远程桌面（如果您的实例为 Windows 实例）通过 IPv6 从本地计算机访问您的实例。在真实应用环境下，您可以使用此方案创建面向公众的 Web 服务器，例如，托管一个博客。

要完成本练习，请执行以下操作：

- 创建一个具有 IPv6 CIDR 块的非默认 VPC 和一个公有子网。子网可以让您根据自己的安全和运营需要，对实例进行分组。公有子网是可以通过 Internet 网关访问 Internet 的子网。
- 为您的实例创建仅允许流量通过特定端口的安全组。

- 将一个 Amazon EC2 实例启动到您的子网中，并在启动期间将一个 IPv6 地址与您的实例关联。IPv6 地址全局唯一，使您的实例能够与 Internet 通信。

有关 IPv4 和 IPv6 地址的更多信息，请参阅[您的 VPC 中的 IP 寻址](#)。

在首次使用 Amazon VPC 之前，您必须先注册 Amazon Web Services (AWS)。在您注册时，您的 AWS 账户会自动注册 AWS 中的所有服务，包括 Amazon VPC。如果您尚未创建 AWS 账户，请转至 <https://aws.amazon.com/>，然后选择创建免费账户。

任务

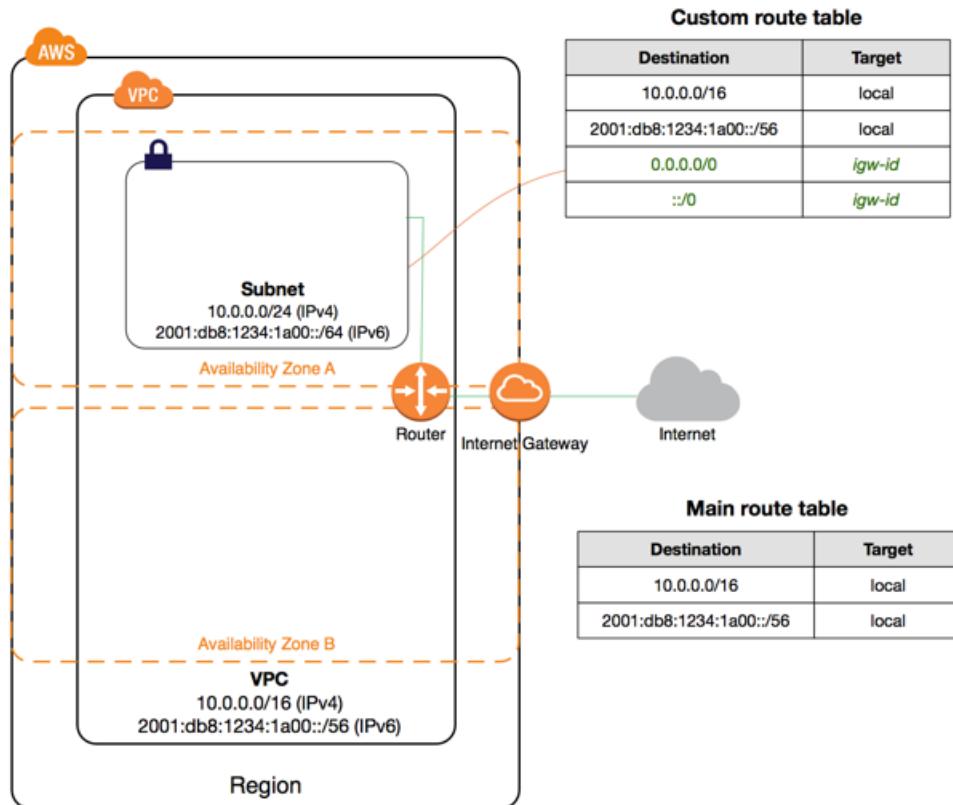
- [步骤 1：创建 VPC \(p. 17\)](#)
- [步骤 2：创建安全组 \(p. 19\)](#)
- [步骤 3：启动实例 \(p. 21\)](#)

步骤 1：创建 VPC

在此步骤中，您将在 Amazon VPC 控制台中使用 Amazon VPC 向导创建 VPC。本向导为您执行以下步骤：

- 创建一个具有 /16 IPv4 CIDR 块的 VPC 并将一个 /56 IPv6 CIDR 块与该 VPC 关联。有关更多信息，请参阅[您的 VPC](#)。IPv6 CIDR 块的大小是固定的 (/56)，IPv6 地址的范围是从 Amazon 的 IPv6 地址池中自动分配的 (您不能自选范围)。
- 将 Internet 网关连接到 VPC。有关 Internet 网关的更多信息，请参阅[Internet 网关](#)。
- 在 VPC 中创建一个具有 /24 IPv4 CIDR 块和 /64 IPv6 CIDR 块的子网。IPv6 CIDR 块的大小是固定的 (/64)。
- 创建一个自定义路由表，并将其与您的子网相关联，以便在子网与 Internet 网关之间进行通信。有关路由表的更多信息，请参阅[路由表](#)。

下图表示了您的 VPC 在您完成此步骤之后的架构。

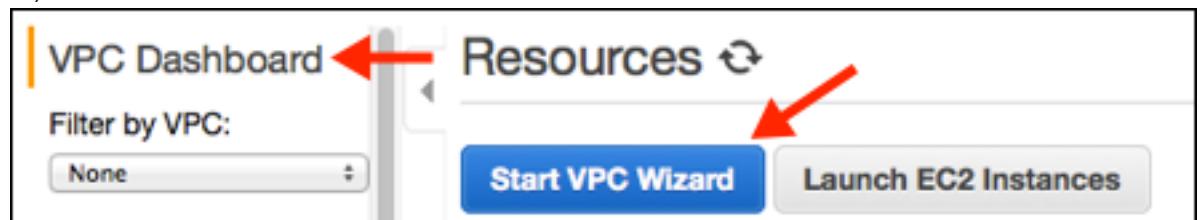


Note

本练习介绍 VPC 向导的第一个方案。有关其他方案的更多信息，请参阅 [Amazon VPC 方案](#)。

使用 Amazon VPC 向导创建 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在右上角的导航栏中，记下您要在其中创建 VPC 的区域。确保继续在相同区域中操作本练习的剩余部分，因为您无法将实例启动到不同区域的 VPC 中。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[区域和可用区](#)。
3. 在导航窗格中，选择 VPC dashboard (VPC 控制面板)，然后选择 Launch VPC Wizard (启动 VPC 向导)。



Note

请勿在导航窗格中选择 Your VPCs (您的 VPC)；您无法使用该页面上的 Create VPC (创建 VPC) 按钮访问 VPC 向导。

4. 选择第一个选项，即 VPC with a Single Public Subnet，然后选择 Select。
5. 在配置页面上，在 VPC name 字段中为您的 VPC 输入一个名称（例如，my-vpc），并在 Subnet name 字段中为您的子网输入一个名称。这可帮助您在创建 VPC 和子网后在 Amazon VPC 控制台中识别它们。

6. 对于 IPv4 CIDR block，您可以保留默认设置 (10.0.0.0/16) 或指定自己的设置。有关更多信息，请参阅 [VPC 大小调整](#)。
- 对于 IPv6 CIDR block，选择 Amazon-provided IPv6 CIDR block。
7. 对于 Public subnet's IPv4 CIDR，保留默认设置或指定您自己的设置。对于 Public subnet's IPv6 CIDR，选择 Specify a custom IPv6 CIDR。您可以保留 IPv6 子网的默认十六进制对值 (00)。
8. 保留页面上的其余默认配置，然后选择 Create VPC。
9. 状态窗口会显示工作的进度。工作完成后，选择 OK 关闭状态窗口。
10. Your VPCs 页面将显示您的默认 VPC 和您刚创建的 VPC。

查看有关您的 VPC 的信息

创建 VPC 之后，您就可以查看关于子网、Internet 网关和路由表的信息。您创建的 VPC 有两个路由表——一个所有 VPC 默认都会有的主路由表，一个由向导创建的自定义路由表。自定义路由表与您的子网相关联，这意味着该表中的路由将确定子网数据流的传输方式。如果您向您的 VPC 添加一个新的子网，那么它默认使用主路由表。

查看有关您的 VPC 的信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。记下您创建的 VPC 的名称和 ID (查看 Name 和 VPC ID 列)。您将使用此信息确定与您的 VPC 关联的组件。
3. 在导航窗格中，选择 Subnets。控制台将显示您创建 VPC 时创建的子网。您可以通过 Name 列中的子网名称来识别子网，或者您可以使用上一步骤中获取的 VPC 信息并查看 VPC 列。
4. 在导航窗格中，选择 Internet Gateways。您可以通过查看 VPC 列找到与您的 VPC 连接的 Internet 网关，该列显示了 VPC 的 ID 和名称 (如果适用)。
5. 在导航窗格中，选择 Route Tables。有两个路由表与 VPC 关联。选择自定义路由表 (Main 列显示 No)，然后选择 Routes 选项卡以便在详细信息窗格中显示路由信息：
 - 表中前两行是本地路由，可允许 VPC 中的实例通过 IPv4 和 IPv6 通信。您不能删除这些路由。
 - 下一行显示了 Amazon VPC 向导添加的路由，它允许目标为 VPC (0.0.0.0/0) 外部的 IPv4 地址的流量从子网流向 Internet 网关。
 - 再下一行显示的路由允许目标为 VPC (::/0) 外部的 IPv6 地址的流量从子网流向 Internet 网关。
6. 选择主路由表。主路由表拥有一个本地路由，但没有其他路由。

步骤 2：创建安全组

安全组充当虚拟防火墙，为其关联的实例控制数据流。要使用安全组，可以添加入站规则以控制进入实例的传入流量，添加出站规则以控制来自您的实例的传出流量。要将安全组与实例关联，可以在启动实例时指定安全组。

您的 VPC 带有默认的安全组。所有启动时未与其他安全组关联的实例都将与默认安全组相关联。在本练习中，您将创建一个新的安全组 WebServerSG，并在您将实例启动到您的 VPC 中时指定此安全组。

WebServerSG 安全组规则

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

入站

源 IP	协议	端口范围	注释
::/0	TCP	80	允许从所有 IPv6 地址进行入站 HTTP 访问。
::/0	TCP	443	允许来自所有 IPv6 地址的入站 HTTPS 流量。
您的家庭网络的 IPv6 地址范围	TCP	22 或 3389	允许从您的家庭网络中的 IPv6 地址范围到 Linux/UNIX 实例进行入站 SSH 访问（端口 22）。如果您的实例是 Windows 实例，则需要允许 RDP 访问（端口 3389）的规则。
出站			
目的地 IP	协议	端口范围	注释
0.0.0.0/0	All	全部	允许所有出站 IPv4 通信的默认出站规则。对于本练习，您无需修改此规则。
::/0	All	全部	允许所有出站 IPv6 通信的默认出站规则。对于本练习，您无需修改此规则。

Note

如果您也要对 IPv4 流量使用您的 Web 服务器实例，则必须添加允许通过 IPv4 访问的规则；在本例中，就是来自所有 IPv4 地址 (0.0.0.0/0) 的 HTTP 和 HTTPS 流量以及来自您的家庭网络 IPv4 地址范围的 SSH/RDP 访问。

创建 WebServerSG 安全组

您可以使用 Amazon VPC 控制台创建安全组。

创建 WebServerSG 安全组并添加规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，然后选择 Create Security Group。
3. 对于 Group name，输入 WebServerSG 作为安全组的名称，并提供说明。您可以选择使用 Name tag 字段来为具有密钥 Name 和指定的值的安全组创建标记。
4. 从 VPC 菜单中选择您 VPC 的 ID，然后选择 Yes, Create。
5. 选择您刚刚创建的 WebServerSG 安全组（可在 Group Name 列中查看其名称）。
6. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 对于 Type，选择 HTTP 并在 Source 字段中输入 ::/0。
 - b. 选择 Add another rule，对于 Type 选择 HTTPS，然后在 Source 字段中输入 ::/0。
 - c. 选择 Add another rule。如果您启动的是 Linux 实例，请为 Type 选择 SSH，如果您启动的是 Windows 实例，请选择 RDP。在 Source 字段中输入您网络的公有 IPv6 地址范围。如果您不知道地址范围，则可以使用 ::/0 来完成此练习。

Important

如果您使用的是 ::/0，则可以允许所有 IPv6 地址使用 SSH 或 RDP 访问您的实例。您可以在本次简短的练习中使用此方法，但是在生产环境中使用其安全性有所欠缺。在生产中，请仅授权特定 IP 地址或地址范围访问您的实例。

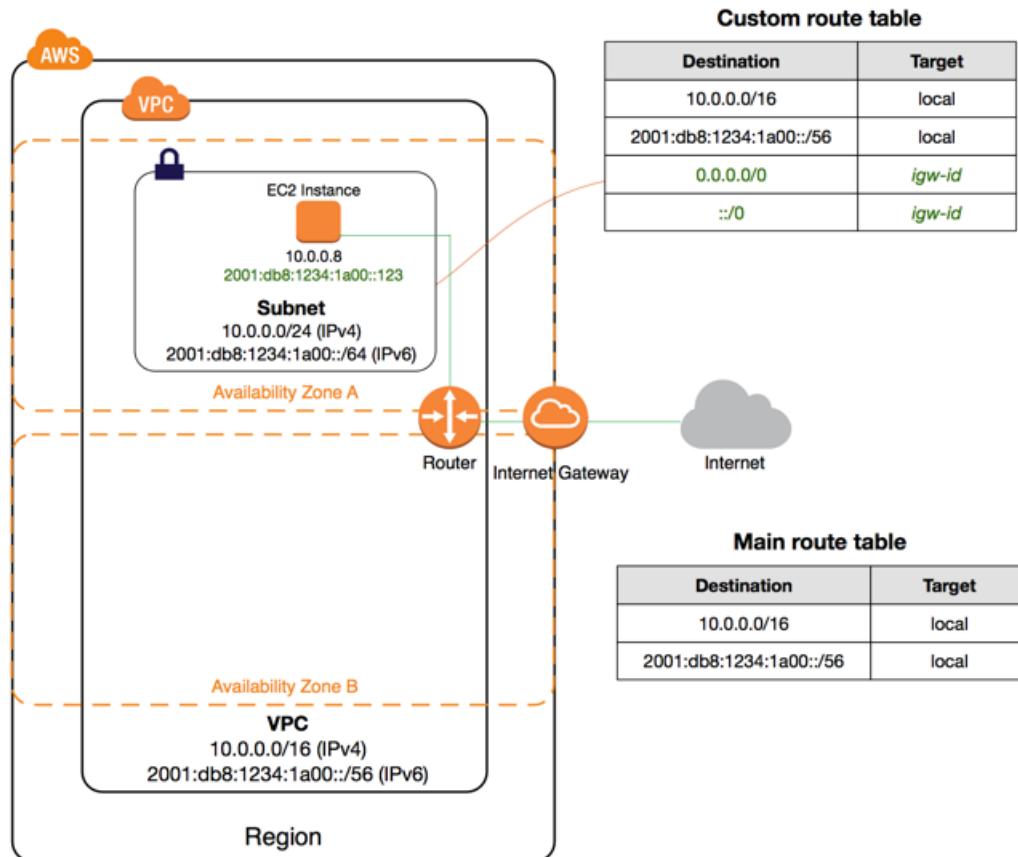
- d. 选择 Save (保存)。

步骤 3：启动实例

当您将 EC2 实例启动到 VPC 中时，您必须指定要在其中启动实例的子网。在这种情况下，您会将实例启动到您创建的 VPC 的公有子网中。在 Amazon EC2 控制台中使用 Amazon EC2 启动向导启动您的实例。

为确保您的实例可从 Internet 访问，请在启动期间为实例分配一个子网范围内的 IPv6 地址。这可以确保您的实例可以通过 IPv6 与 Internet 通信。

下图表示了您的 VPC 在您完成此步骤之后的架构。



如何将一个 EC2 实例推送到 VPC

在 VPC 中启动 EC2 实例前，请将 VPC 的子网配置为自动分配 IPv6 IP 地址。有关更多信息，请参阅[the section called “修改子网的 IPv6 寻址属性” \(p. 103\)](#)。

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在右上角的导航栏中，确保选择您在其中创建了 VPC 和安全组的同一区域。
3. 在控制面板中，选择 Launch Instance。
4. 在向导的第一页上，选择要使用的 AMI。在本练习中，我们建议您选择 Amazon Linux AMI 或 Windows AMI。
5. 在 Choose an Instance Type (选择一种实例类型) 页面上，您可以选择要启动的实例的硬件配置和大小。默认情况下，向导会基于您选择的 AMI 选择第一个可用实例类型。您可以保留默认选择，然后选择 Next: Configure Instance Details。
6. 在 Configure Instance Details 页上，从 Network 列表中选择您创建的 VPC，然后从 Subnet 列表中选择子网。

7. 对于 Auto-assign IPv6 IP，选择 Enable。
8. 保留默认设置的其余部分，然后完成向导中的后续页面，直至到达 Add Tags 页面。
9. 在 Add Tags 页面上，您可以为实例添加 Name 标签；例如 Name=MyWebServer。这有助于您启动实例后在 Amazon EC2 控制台中识别您的实例。完成时选择 Next: Configure Security Group。
10. 在 Configure Security Group (配置安全组) 页面上，向导会自动定义 launch-wizard-x 安全组，从而让您可以连接到您的实例。而是选择 Select an existing security group 选项，选择您之前创建的 WebServerSG 组，然后选择 Review and Launch。
11. 在 Review Instance Launch 页面上，检查您的实例的详细信息，然后选择 Launch。
12. 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，您可以选择现有密钥对，也可以创建新的密钥对。如果要创建新的密钥对，请确保您将文件下载并保存在安全的位置。您需要知道私钥的内容，以便在启动实例后与实例相连。

要启动您的实例，请选中确认复选框，然后选择 Launch Instances。

13. 在确认页面上，选择 View Instances 可在 Instances 页面上查看您的实例。选择您的实例，然后在 Description 选项卡中查看其详细信息。Private IPs 字段显示从您的子网中的 IPv4 地址范围分配给您的实例的私有 IPv4 地址。Private IPs 字段显示从您的子网中的 IPv6 地址范围分配给您的实例的 IPv6 地址。

有关 Amazon EC2 启动向导中的可用选项的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[启动实例](#)。

您可以使用 SSH 或远程桌面从您的家庭网络通过您的实例的 IPv6 地址连接到该实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。有关如何连接到 Linux 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[连接到 Linux 实例](#)。有关如何连接到 Windows 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的[使用 RDP 连接到 Windows 实例](#)。

Note

如果您还希望您的实例可通过 IPv4 地址在 Internet、SSH 或 RDP 上访问，则必须将一个弹性 IP 地址（静态公有 IPv4 地址）与您的实例关联，而且必须调整您的安全组规则以允许通过 IPv4 访问。有关更多信息，请参阅 [Amazon VPC 入门 \(p. 9\)](#)。

场景和示例

此部分提供了创建和配置 VPC 的示例，包括讲解如何在 Amazon VPC 控制台中使用 VPC 向导的场景。

场景	用量
场景 1：带单个公有子网的 VPC (p. 23)	使用 VPC 向导创建用于运行单层、面向公众的 Web 应用程序 (如博客或简单网站) 的 VPC。
场景 2：带有公有子网和私有子网 (NAT) 的 VPC (p. 29)	使用 VPC 向导创建用于运行面向公众的 Web 应用程序的 VPC，同时仍在第二个子网中保留非公开访问的后端服务器。
场景 3：具有公有和私有子网和 AWS Site-to-Site VPN 访问权限的 VPC (p. 41)	使用 VPC 向导创建用于将数据中心扩展到云中的 VPC，并实现从 VPC 直接访问 Internet。
场景 4：仅具有一个私有子网以及 AWS Site-to-Site VPN 访问权限的 VPC (p. 53)	使用 VPC 向导创建用于将数据中心扩展到云中的 VPC，无需将您的网络连接到 Internet 即可使用 Amazon 基础设备。
示例：使用 AWS CLI 创建 IPv4 VPC 和子网 (p. 58)	使用 AWS CLI 创建具有公有和私有子网的 VPC。
示例：使用 AWS CLI 创建 IPv6 VPC 和子网 (p. 63)	使用 AWS CLI 创建具有关联 IPv6 CIDR 块的 VPC 以及每个都具有关联 IPv6 CIDR 块的公有子网和私有子网。
the section called “示例：共享公有子网和私有子网” (p. 71)	与账户共享私有和公有子网。
the section called “示例：使用 AWS PrivateLink 和 VPC 对等连接的服务” (p. 71)	了解如何结合使用 VPC 对等连接和 AWS PrivateLink 将对私有服务的访问权限扩展到使用者。

场景 1：带单个公有子网的 VPC

此场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。

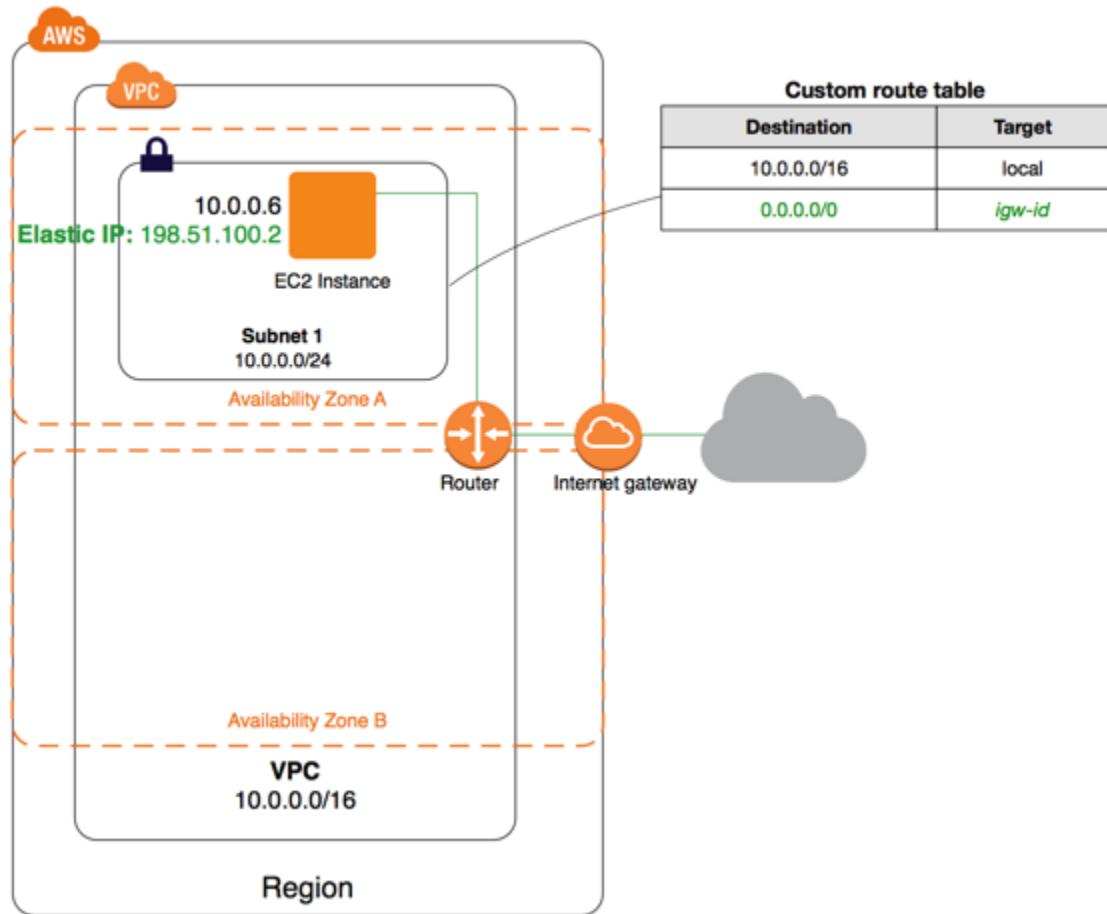
也可以选择为 IPv6 配置此场景，您可以使用 VPC 向导创建关联有 IPv6 CIDR 块的 VPC 和子网。启动到公有子网中的实例可以接收 IPv6 地址并使用 IPv6 通信。有关 IPv4 和 IPv6 寻址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

内容

- [概述 \(p. 23\)](#)
- [路由选择 \(p. 25\)](#)
- [安全性 \(p. 26\)](#)
- [实施场景 1 \(p. 27\)](#)

概述

下表展示了此场景配置的主要组成部分。



Note

如果您完成了 [Amazon VPC 入门 \(p. 9\)](#)，则实际上您已使用 Amazon VPC 控制台中的 VPC 向导实现了本场景。

此情景的配置包括：

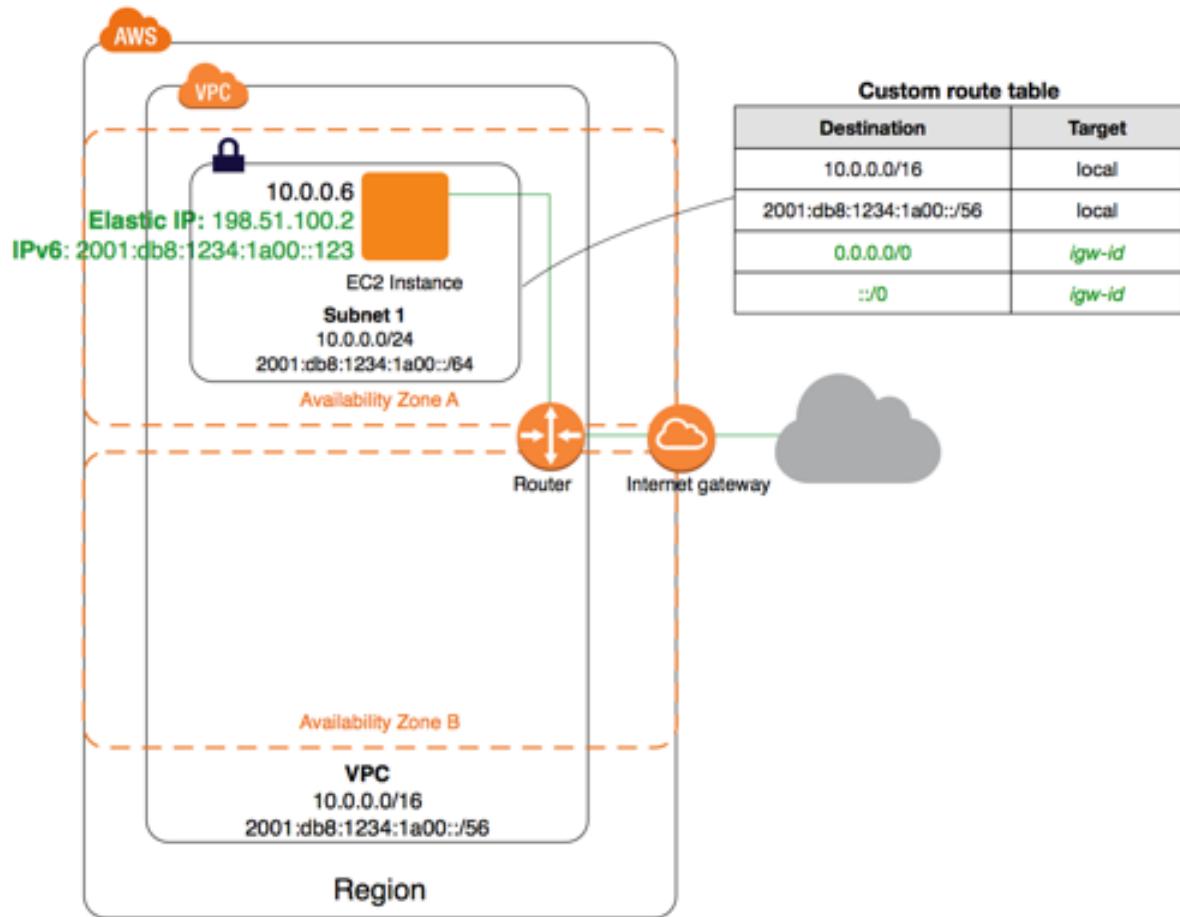
- 具有 /16 IPv4 CIDR 块的 Virtual Private Cloud (VPC) (示例：10.0.0.0/16)。提供 65536 个私有 IPv4 地址。
- 具有 /24 IPv4 CIDR 块的子网 (示例：10.0.0.0/24)。提供 256 个私有 IPv4 地址。
- Internet 网关。它将 VPC 连接到 Internet 和其他 AWS 服务。
- 具有子网范围内 (示例：10.0.0.6) 私有 IPv4 地址的实例，这使该实例可以与 VPC 中的其他实例通信；以及一个弹性 IPv4 地址 (示例：198.51.100.2)，这是使该实例能够从 Internet 访问的公有 IPv4 地址。
- 与子网关联的自定义路由表。路由表条目使得子网中的实例能够使用 IPv4 与 VPC 中的其他实例通信以及在 Internet 上直接通信。与包含指向 Internet 网关的路由的路由表关联的子网称作公有子网。

有关子网的更多信息，请参阅[VPC 和子网 \(p. 75\)](#)。有关 Internet 网关的更多信息，请参阅[Internet 网关 \(p. 192\)](#)。

IPv6 概述

您可以选择为此场景启用 IPv6。除了上面列出的组件外，还包括以下配置：

- 与 VPC 关联的 /56 IPv6 CIDR 块 (示例 : 2001:db8:1234:1a00::/56)。Amazon 会自动分配 CIDR；您不能自选范围。
- 与公有子网关联的 /64 IPv6 CIDR 块 (示例 : 2001:db8:1234:1a00::/64)。您可以从分配给 VPC 的范围内选择您的子网范围。您不能选择子网 IPv6 CIDR 块的大小。
- 子网范围内分配给实例的 IPv6 地址 (示例 : 2001:db8:1234:1a00::123)。
- 自定义路由表中的路由表条目，其允许 VPC 中的实例使用 IPv6 相互通信和直接通过 Internet 通信。



路由选择

您的 VPC 有一个隐藏路由器 (显示在上面的配置图中)。在这个情景中，VPC 向导创建了一个自定义路由表，以将所有目标为 VPC 外的地址的所有流量路由到 Internet 网关，并将此路由表与子网关联。

下表显示了在上面的配置图中用作示例的路由表。第一个条目是 VPC 中本地 IPv4 路由的默认条目；此条目允许此 VPC 中的实例相互通信。第二个条目将所有其他 IPv4 子网流量路由到 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-id

IPv6 路由

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则您的路由表必须包含适用于 IPv6 流量的单独路由。下表显示了当您选择在 VPC 中启用 IPv6 通信时此场景的自定义路由表。第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。第四个条目将所有其他 IPv6 子网流量路由到 Internet 网关。

目的地	目标
10.0.0.0/16	本地
2001:db8:1234:1a00::/56	本地
0.0.0.0/0	igw-id
::/0	igw-id

安全性

AWS 提供了可以用于在 VPC 中提高安全性的两个功能：安全组 和 网络 ACL。安全组可以控制您的实例的入站和出站数据流，网络 ACL 可以控制您的子网的入站和出站数据流。多数情况下，安全组即可满足您的需要；但是，如果您需要为您的 VPC 增添额外一层安全保护，您也可以使用网络 ACL。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

对于此场景，您可以使用安全组而不是网络 ACL。如果希望使用网络 ACL，请参阅 [场景 1 的推荐规则 \(p. 138\)](#)。

您的 VPC 带有[默认的安全组 \(p. 120\)](#)。如果您在启动期间没有指定其他安全组，在该 VPC 中启动的实例会与默认安全组自动关联。您可以向默认安全组添加规则，但这些规则可能不适用于您在该 VPC 中启动的其他实例。我们建议您为 Web 服务器创建自定义安全组。

对于该情景，请创建一个名为 webServerSG 的安全组。当您创建安全组时，它包含一条允许所有流量离开该实例的出站规则。您必须修改规则来允许入站流量，并根据需要限制出站流量。您可在 VPC 中启动实例时指定此安全组。

以下是 WebServerSG 安全组的 IPv4 流量入站和出站规则。

入站			
源	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许从任意 IPv4 地址对 Web 服务器进行入站 HTTP 访问。
0.0.0.0/0	TCP	443	允许从任意 IPv4 地址对 Web 服务器进行入站 HTTPS 访问。
您的网络的公有 IPv4 地址范围。	TCP	22	(Linux 实例) 允许您的网络通过 IPv4 进行入站 SSH 访问。您可以使用 http://checkip.amazonaws.com 或 https://checkip.amazonaws.com 等服务获取本地计算机的公有 IPv4 地址。如果您正通过 ISP 或从防火墙后面连接，没有静态 IP 地址，您需要找出客户端计算机使用的 IP 地址范围。
您的网络的公有 IPv4 地址范围。	TCP	3389	(Windows 实例) 允许您的网络通过 IPv4 进行入站 RDP 访问。

安全组 ID (sg-xxxxxxxx)	全部	全部	(可选) 允许与该安全组相关联的其他实例的入站流量。该规则会自动添加到 VPC 的默认安全组中；对于您创建的任意自定义安全组，您必须手动添加规则来允许此类通信。
Outbound (可选)			
目的地	协议	端口范围	注释
0.0.0.0/0	All	全部	允许针对任意 IPv4 地址的所有出站访问的默认规则。如果希望您的 Web 服务器启动出站流量（例如用于获取软件更新），您可以保留默认出站规则。否则，您可以删除该规则。

IPv6 安全性

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则必须向安全组中添加单独的规则来控制您的 Web 服务器实例的入站和出站 IPv6 流量。在此场景中，Web 服务器能够接收通过 IPv6 的所有 Internet 流量以及来自您的本地网络通过 IPv6 进行的 SSH 或 RDP 流量。

以下是针对 WebServerSG 安全组的特定于 IPv6 的规则（是上面所列规则的补充）。

入站			
源	协议	端口范围	注释
::/0	TCP	80	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTP 访问。
::/0	TCP	443	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTPS 访问。
您的网络的 IPv6 地址范围	TCP	22	(Linux 实例) 允许您的网络通过 IPv6 进行入站 SSH 访问。
您的网络的 IPv6 地址范围	TCP	3389	(Windows 实例) 允许您的网络通过 IPv6 进行入站 RDP 访问。
Outbound (可选)			
目的地	协议	端口范围	注释
::/0	All	全部	允许针对任意 IPv6 地址的所有出站访问的默认规则。如果希望您的 Web 服务器启动出站流量（例如用于获取软件更新），您可以保留默认出站规则。否则，您可以删除该规则。

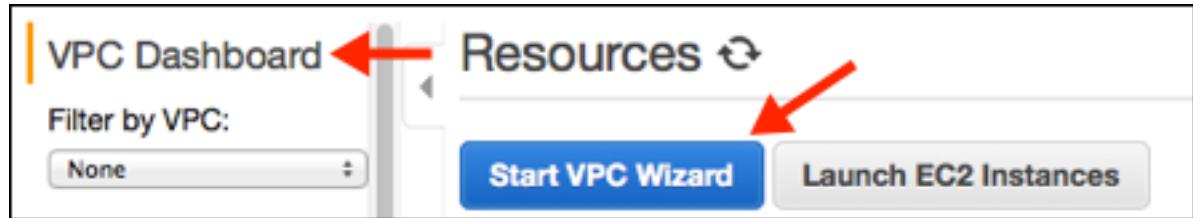
实施场景 1

要实现情景 1，请使用 VPC 向导创建一个 VPC，创建并配置 WebServerSG 安全组，然后在 VPC 中启动一个实例。

这些过程包括用于为您的 VPC 启用和配置 IPv6 通信的可选步骤。如果您不想在 VPC 上使用 IPv6，则不必执行这些步骤。

创建 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在控制面板上，选择 Launch VPC Wizard (启动 VPC 向导)。



3. 选择第一个选项，即 VPC with a Single Public Subnet，然后选择 Select。
4. (可选) 您可以命名 VPC 和子网，以便稍后在控制台中识别它们。您可以为 VPC 和子网指定自己的 IPv4 CIDR 块范围，也可以保留默认值 (分别为 10.0.0.0/16 和 10.0.0.0/24)。
5. (可选，仅 IPv6) 对于 IPv6 CIDR block，选择 Amazon-provided IPv6 CIDR block。对于 Public subnet's IPv6 CIDR (公有子网的 IPv6 CIDR)，选择 Specify a custom IPv6 CIDR (指定自定义 IPv6 CIDR) 并指定您的子网的十六进制对值或保留默认值 (00)。
6. 保留其余默认设置，然后选择 Create VPC (创建 VPC)。

要创建 WebServerSG 安全组，请执行以下操作

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 提供安全组的名称和描述。在本主题中，使用名称 WebServerSG 作为示例。从 VPC 菜单中选择您 VPC 的 ID，然后选择 Yes, Create。
5. 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。
6. 在入站规则选项卡上，选择 编辑规则，然后执行以下操作：
 - 从 Type (类型) 列表中选择 HTTP，然后在 0.0.0.0/0Source (源) 字段中输入。
 - 选择添加规则，从类型列表中选择 HTTPS，然后在 Source (源) 字段中输入 0.0.0.0/0。
 - 选择添加规则，然后从类型列表中选择 SSH (对于 Linux) 或 RDP (对于 Windows)。在 Source (源) 字段中输入您网络的公有 IP 地址范围。(如果不知道此地址范围，则可使用 0.0.0.0/0 作测试用途；在生产环境下，您将仅授权特定 IP 地址或地址范围访问您的实例。)
 - (可选) 选择添加规则，然后从类型列表中选择所有流量。在 Source (源) 字段中，输入 WebServerSG 安全组的 ID。
 - (可选，仅 IPv6) 选择添加规则，从类型列表中选择 HTTP，然后在 Source (源) 字段中输入 ::/0。
 - (可选，仅 IPv6) 选择添加规则，从类型列表中选择 HTTPS，然后在 Source (源) 字段中输入 ::/0。
 - (可选，仅 IPv6) 选择添加规则，然后从类型列表中选择 SSH (对于 Linux) 或 RDP (对于 Windows)。在 Source (源) 字段中输入您的网络的 IPv6 地址范围。(如果不知道此地址范围，则可使用 ::/0 作测试用途；在生产环境下，您将仅授权特定 IPv6 地址或地址范围访问您的实例。)
7. 选择 Save (保存)。
8. (可选) 在 Outbound Rules 选项卡上，选择 Edit。找到启用所有出站流量的默认规则，选择 Remove，然后选择 Save。

在 VPC 中启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从控制面板中选择 Launch EC2 Instances (启动 EC2 实例)。
3. 按照向导中的指示操作。选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

如果您要使用您的实例进行 IPv6 通信，则必须选择支持的实例类型，例如 T2。有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

4. 在 Configure Instance Details (配置实例详细信息) 页上，从 Network (网络) 列表中选择您在第 1 步中创建的 VPC，然后指定子网。
5. (可选) 默认情况下，在非默认 VPC 中启动的实例未分配公有 IPv4 地址。为能连接到您的实例，您可以现在分配公有 IPv4 地址，也可以分配弹性 IP 地址并在启动您的实例后向其分配该地址。要现在分配公有 IPv4 地址，请确保从 Auto-assign Public IP 列表中选择 Enable。

Note

您只能为设备索引为 eth0 的单个新网络接口使用自动分配公有 IP 功能。有关更多信息，请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)。

6. (可选，仅 IPv6) 您可以从子网范围内为您的实例自动分配 IPv6 地址。对于 Auto-assign IPv6 IP，选择 Enable。
7. 在向导的后两页上，可为您的实例配置存储并添加标签。在 Configure Security Group 页上，选择 Select an existing security group 选项，然后选择您在第 2 步中创建的 WebServerSG 安全组。选择 Review and Launch。
8. 检视您已经选择的设置。执行所需的任何更改，然后选择 Launch 以选择一个密钥对并启动您的实例。
9. 如果您没有按照第 5 步中的说明为您的实例分配公有 IPv4 地址，则无法通过 IPv4 与其连接。为实例分配弹性 IP 地址：
 - a. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
 - b. 在导航窗格中，选择 Elastic IPs。
 - c. 选择 Allocate new address。
 - d. 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

- e. 从列表中选择弹性 IP 地址，选择 Actions，然后选择 Associate address。
- f. 选择要与该地址关联的实例，然后选择 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，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Connect to Your Linux Instance](#) 部分。有关如何连接 Windows 实例的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Windows 实例\)](#) 中的 [Connect to Your Windows Instance](#) 部分。

场景 2：带有公有子网和私有子网 (NAT) 的 VPC

这个场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，我们建议您使用此场景。常用例子是一个多层次网站，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，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直接将出站流量发往 Internet，而私有子网中的实例不能这样做。但是，私有子网中的实例可使用位于公有子网中的网络地址转换 (NAT) 网关访问 Internet。数据库服务器可以使用 NAT 网关连接到 Internet 进行软件更新，但 Internet 不能建立到数据库服务器的连接。

Note

您还可以使用 VPC 向导配置有 NAT 实例的 VPC；不过，我们建议您使用 NAT 网关。有关更多信息，请参阅 [NAT 网关 \(p. 200\)](#)。

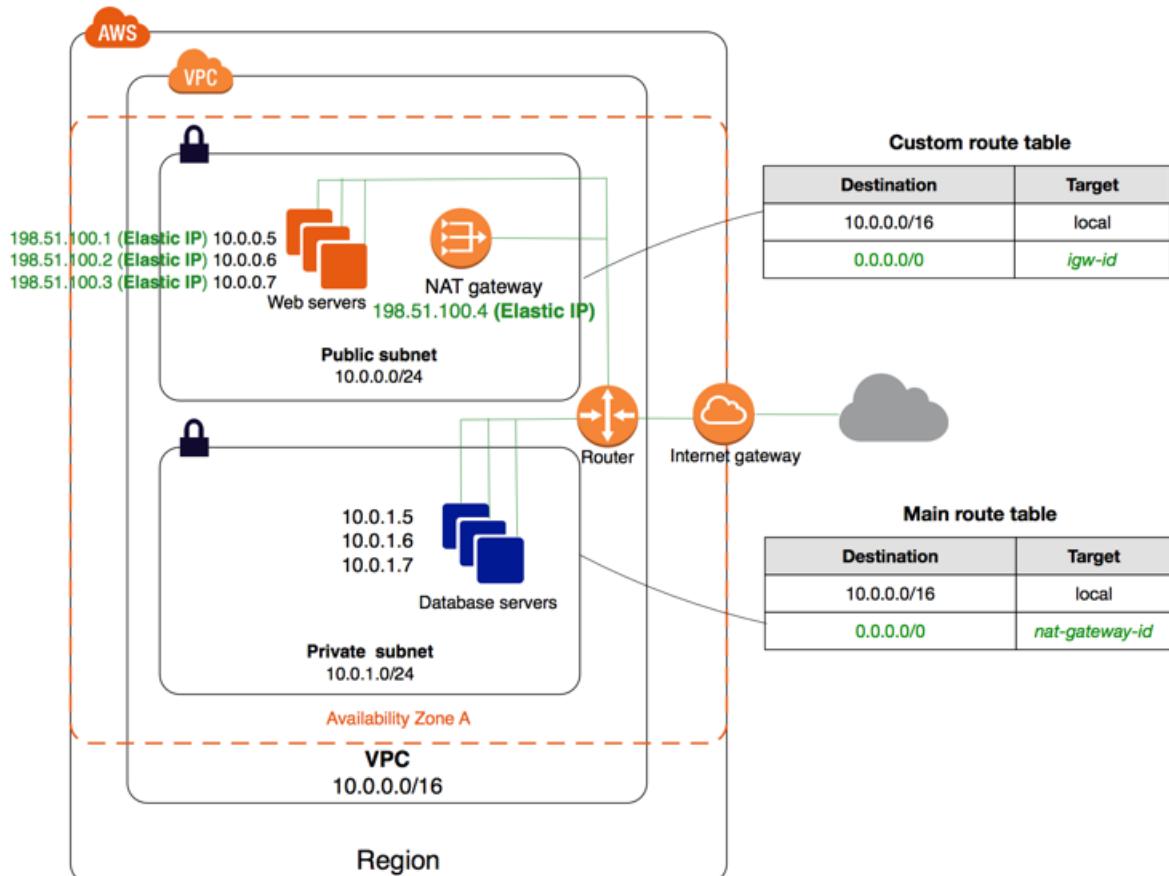
也可以选择为此场景配置 IPv6：您可以使用 VPC 向导创建关联有 IPv6 CIDR 块的 VPC 和子网。启动到子网中的实例可以接收 IPv6 地址并使用 IPv6 进行通信。私有子网中的实例可以使用仅出口 Internet 网关通过 IPv6 连接到 Internet，但 Internet 不能通过 IPv6 与私有实例建立连接。有关 IPv4 和 IPv6 寻址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

内容

- [概述 \(p. 30\)](#)
- [路由选择 \(p. 32\)](#)
- [安全性 \(p. 33\)](#)
- [实施场景 2 \(p. 36\)](#)
- [通过 NAT 实例实现场景 2 \(p. 39\)](#)

概述

下表展示了此场景配置的主要组成部分。



此情景的配置包括：

- 具有 /16 IPv4 CIDR 块的 VPC (示例：10.0.0.0/16)。提供 65536 个私有 IPv4 地址。

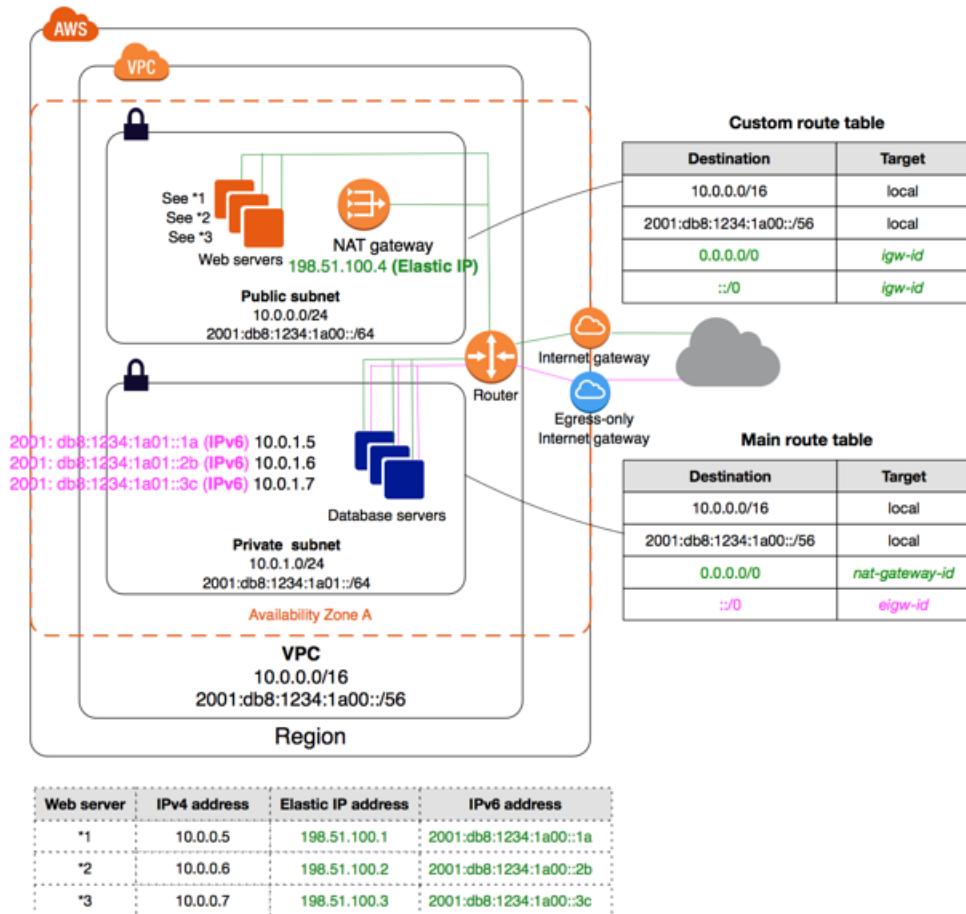
- 具有 /24 IPv4 CIDR 块的公有子网 (示例 : 10.0.0.0/24)。提供 256 个私有 IPv4 地址。公有子网是指与包含指向 Internet 网关的路由的路由表关联的子网。
- 具有 /24 IPv4 CIDR 块的私有子网 (示例 : 10.0.1.0/24)。提供 256 个私有 IPv4 地址。
- Internet 网关。它将 VPC 连接到 Internet 和其他 AWS 服务。
- 具有子网范围内私有 IPv4 地址 (示例 : 10.0.0.5、10.0.1.5) 的实例。这样实例之间可相互通信，也可与 VPC 中的其他实例通信。
- 具有公有子网内弹性 IPv4 地址 (示例 : 198.51.100.1) 的实例，这些弹性 IP 地址是使其能够从 Internet 访问的公有 IPv4 地址。可在启动时为实例分配公有 IP 地址而不是弹性 IP 地址。私有子网中的实例是后端服务器，它们不需要接受来自 Internet 的传入流量，因此，没有公有 IP 地址；但是，它们可以使用 NAT 网关向 Internet 发送请求 (请参阅下一要点)。
- 具有自己的弹性 IPv4 地址的 NAT 网关。私有子网中的实例可使用 IPv4 通过 NAT 网关向 Internet 发送请求 (例如，针对软件更新的请求)。
- 与公有子网关联的自定义路由表。此路由表中包含的一个条目允许子网中的实例通过 IPv4 与 VPC 中的其他实例通信，另一个条目则允许子网中的实例通过 IPv4 直接与 Internet 通信。
- 与私有子网关联的主路由表。路由表中包含的一个条目使子网中的实例可通过 IPv4 与 VPC 中的其他实例通信，另一条目使子网中的实例可通过 NAT 网关和 IPv4 与 Internet 通信。

有关子网的更多信息，请参阅[VPC 和子网 \(p. 75\)](#)。有关 Internet 网关的更多信息，请参阅[Internet 网关 \(p. 192\)](#)。有关 NAT 网关的更多信息，请参阅[NAT 网关 \(p. 200\)](#)。

IPv6 概述

您可以选择为此场景启用 IPv6。除了上面列出的组件外，还包括以下配置：

- 与 VPC 关联的 /56 IPv6 CIDR 块 (示例 : 2001:db8:1234:1a00::/56)。Amazon 会自动分配 CIDR；您不能自选范围。
- 与公有子网关联的 /64 IPv6 CIDR 块 (示例 : 2001:db8:1234:1a00::/64)。您可以从分配给 VPC 的范围内选择您的子网范围。您不能选择 VPC IPv6 CIDR 块的大小。
- 与私有子网关联的 /64 IPv6 CIDR 块 (示例 : 2001:db8:1234:1a01::/64)。您可以从分配给 VPC 的范围内选择您的子网范围。您不能选择子网 IPv6 CIDR 块的大小。
- 子网范围内分配给实例的 IPv6 地址 (示例 : 2001:db8:1234:1a00::1a)。
- 仅出口 Internet 网关。这允许私有子网中的实例通过 IPv6 向 Internet 发送请求 (例如软件更新)。如果您希望私有子网中的实例能够通过 IPv6 与 Internet 发起通信，则仅出口 Internet 网关是必需的。有关更多信息，请参阅[仅出口 Internet 网关 \(p. 197\)](#)。
- 自定义路由表中的路由表条目，允许公有子网中的实例使用 IPv6 相互通信和直接通过 Internet 通信。
- 主路由表中的路由表条目，允许私有子网中的实例使用 IPv6 相互通信和通过仅出口 Internet 网关与 Internet 通信。



路由选择

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。

在这个场景中，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 设备发送和接收 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。

下表描述了此场景的路由表。

主路由表

第一个条目是 VPC 中本地路由的默认条目；这项条目允许 VPC 中的实例在彼此之间进行通信。第二个条目将所有其他子网流量发送到 NAT 网关（例如 nat-12345678901234567）。

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

自定义路由表

第一个条目是 VPC 中本地路由的默认条目；这项条目允许该 VPC 中的实例在彼此之间进行通信。第二个条目将所有其他子网流量通过 Internet 网关（例如 `igw-1a2b3d4d`）路由到 Internet。

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

IPv6 路由

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则您的路由表必须包含适用于 IPv6 流量的单独路由。下面的表显示了当您选择在 VPC 中启用 IPv6 通信时此场景的自定义路由表。

主路由表

第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。第四个条目将所有其他 IPv6 子网流量路由到仅出口 Internet 网关。

目的地	目标
<code>10.0.0.0/16</code>	本地
<code>2001:db8:1234:1a00::/56</code>	本地
<code>0.0.0.0/0</code>	<code>nat-gateway-id</code>
<code>::/0</code>	<code>egress-only-igw-id</code>

自定义路由表

第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。第四个条目将所有其他 IPv6 子网流量路由到 Internet 网关。

目的地	目标
<code>10.0.0.0/16</code>	本地
<code>2001:db8:1234:1a00::/56</code>	本地
<code>0.0.0.0/0</code>	<code>igw-id</code>
<code>::/0</code>	<code>igw-id</code>

安全性

AWS 提供了可以用于在 VPC 中提高安全性的两个功能：安全组和网络 ACL。安全组可以控制您的实例的入站和出站数据流，网络 ACL 可以控制您的子网的入站和出站数据流。多数情况下，安全组即可满足您的需要；但是，如果您需要为您的 VPC 增添额外一层安全保护，您也可以使用网络 ACL。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

在场景 2 中，您可以使用安全组而不是网络 ACL。如果希望使用网络 ACL，请参阅 [场景 2 的推荐规则 \(p. 140\)](#)。

您的 VPC 带有[默认的安全组 \(p. 120\)](#)。如果您在启动期间没有指定其他安全组，在该 VPC 中启动的实例会与默认安全组自动关联。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：在公有子网中启动 Web 服务器时指定该安全组。
- DBServerSG：在私有子网中启动数据库服务器时指定该安全组。

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，在这个场景中，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，在这个场景中，所有分配到一个安全组的实例都位于相同的子网之中。

下表描述了 WebServerSG 安全组的推荐规则，这些规则允许 Web 服务器接收 Internet 流量，以及来自您的网络的 SSH 和 RDP 流量。Web 服务器也可发起对私有子网中的数据库服务器的读取和写入请求，并向 Internet 发送数据流；例如获取软件更新。由于 Web 服务器不发起任何其他出站通信，因此将删除默认出站规则。

Note

这些建议包括 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。

WebServerSG：推荐规则

入站			
源	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许从任意 IPv4 地址对 Web 服务器进行入站 HTTP 访问。
0.0.0.0/0	TCP	443	允许从任意 IPv4 地址对 Web 服务器进行入站 HTTPS 访问。
您的家庭网络的公有 IPv4 地址范围	TCP	22	允许从您的家庭网络对 Linux 实例进行入站 SSH 访问 (通过 Internet 网关)。您可以使用 http://checkip.amazonaws.com 或 https://checkip.amazonaws.com 等服务获取本地计算机的公有 IPv4 地址。如果您正通过 ISP 或从防火墙后面连接，没有静态 IP 地址，您需要找出客户端计算机使用的 IP 地址范围。
您的家庭网络的公有 IPv4 地址范围	TCP	3389	允许从您的家庭网络对 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
您的 DBServerSG 安全组 ID	TCP	1433	允许对归属于 DBServerSG 安全组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 安全组的数据库服务器进行出站 MySQL 访问。
0.0.0.0/0	TCP	80	允许对任意 IPv4 地址进行出站 HTTP 访问。

0.0.0.0/0	TCP	443	允许对任意 IPv4 地址进行出站 HTTPS 访问。
-----------	-----	-----	-----------------------------

下表描述了 DBServerSG 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 的流量 (路由表将流量发送到 NAT 网关，NAT 网关随后通过 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	允许与 WebServerSG 安全组关联的 Web 服务器进行入站 Microsoft SQL Server 访问。
您的 WebServerSG 安全组 ID	TCP	3306	允许与 WebServerSG 安全组关联的 Web 服务器进行入站 MySQL Server 访问。
出站			
目的地	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许通过 IPv4 对 Internet 进行出站 HTTP 访问 (例如，进行软件更新)。
0.0.0.0/0	TCP	443	允许通过 IPv4 对 Internet 进行出站 HTTPS 访问 (例如，进行软件更新)。

(可选) 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。要允许自定义安全组进行此类通信，您必须添加下列规则：

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	允许到分配到该安全组的其他实例的出站流量。

(可选) 如果您启动公有子网中的堡垒主机来用作从家庭网络到私有子网的 SSH 或 RDP 流量的代理，请向 DBServerSG 安全组添加一个规则，以允许来自堡垒实例或其关联安全组的入站 SSH 或 RDP 流量。

IPv6 安全性

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则必须向 WebServerSG 和 DBServerSG 安全组添加单独的规则来控制您的实例的入站和出站 IPv6 流量。在此场景中，Web 服务器能够接收通过 IPv6 的所有

Internet 流量以及来自您的本地网络的通过 IPv6 的 SSH 或 RDP 流量。它们也可以发起到 Internet 的 IPv6 流量。数据库服务器可以发起到 Internet 的出站 IPv6 流量。

以下是针对 WebServerSG 安全组的特定于 IPv6 的规则 (是上面所列规则的补充)。

入站			
源	协议	端口范围	注释
::/0	TCP	80	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTP 访问。
::/0	TCP	443	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTPS 访问。
您的网络的 IPv6 地址范围	TCP	22	(Linux 实例) 允许您的网络通过 IPv6 进行入站 SSH 访问。
您的网络的 IPv6 地址范围	TCP	3389	(Windows 实例) 允许您的网络通过 IPv6 进行入站 RDP 访问。

出站			
目的地	协议	端口范围	注释
::/0	TCP	HTTP	允许对任意 IPv6 地址进行出站 HTTP 访问。
::/0	TCP	HTTPS	允许对任意 IPv6 地址进行出站 HTTPS 访问。

以下是针对 DBServerSG 安全组的特定于 IPv6 的规则 (是上面所列规则的补充)。

出站			
目的地	协议	端口范围	注释
::/0	TCP	80	允许对任意 IPv6 地址进行出站 HTTP 访问。
::/0	TCP	443	允许对任意 IPv6 地址进行出站 HTTPS 访问。

实施场景 2

您可以使用 VPC 向导创建 VPC、子网、NAT 网关和仅出口 Internet 网关 (可选)。必须为 NAT 网关指定一个弹性 IP 地址；如果没有弹性 IP 地址，则您必须先为自己的账户分配一个。如果需要使用现有的弹性 IP 地址，请确保它当前不与其他实例或网络接口关联。NAT 网关是在您的 VPC 的公有子网中自动创建的。

这些过程包括用于为您的 VPC 启用和配置 IPv6 通信的可选步骤。如果您不想在 VPC 上使用 IPv6，则不必执行这些步骤。

(可选) 为 NAT 网关分配弹性 IP 地址 (IPv4)

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

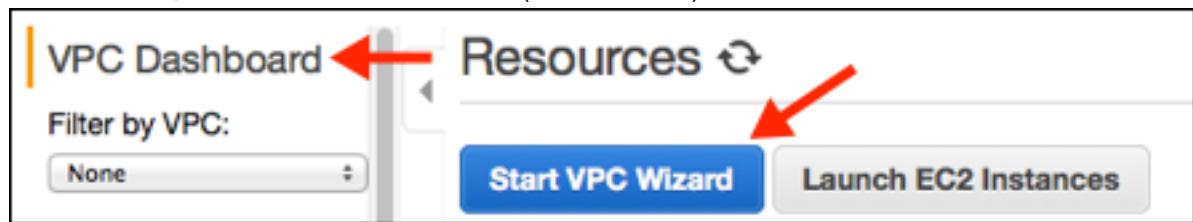
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

创建 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 选择您的 VPC，然后选择 Launch VPC Wizard (启动 VPC 向导)。



3. 选择第二个选项 VPC with Public and Private Subnets (带有公有子网和私有子网的 VPC)，然后选择 Select (选择)。
4. (可选) 您可以命名 VPC 和子网，以便稍后在控制台中识别它们。您可以为 VPC 和子网指定自己的 IPv4 CIDR 块范围，也可以保留默认值。
5. (可选，仅 IPv6) 对于 IPv6 CIDR block，选择 Amazon-provided IPv6 CIDR block。对于 Public subnet's IPv6 CIDR (公有子网的 IPv6 CIDR)，选择 Specify a custom IPv6 CIDR (指定自定义 IPv6 CIDR) 并指定您的子网的十六进制对值或保留默认值。对于 Private subnet's IPv6 CIDR，选择 Specify a custom IPv6 CIDR。指定 IPv6 子网的十六进制对值或保留默认值。
6. 在 Specify the details of your NAT gateway 部分，指定您账户中弹性 IP 地址的分配 ID。
7. 您可以保留页面上的其余默认值，然后选择 Create VPC (创建 VPC)。

由于 WebServerSG 和 DBServerSG 安全组互相引用，因此先创建本场景所需的所有安全组，然后再向其添加规则。

创建 WebServerSG 和 DBServerSG 安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，然后选择 Create Security Group。
3. 提供安全组的名称和描述。在本主题中，使用名称 WebServerSG 作为示例。对于 VPC，选择您创建的 VPC 的 ID，然后选择 Yes, Create。
4. 再次选择 Create Security Group。
5. 提供安全组的名称和描述。在本主题中，使用名称 DBServerSG 作为示例。对于 VPC，选择您的 VPC 的 ID，然后选择 Yes, Create。

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. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 选择 Type、HTTP。对于 Source，输入 0.0.0.0/0。
 - b. 选择 Add another rule、Type、HTTPS。对于 Source，输入 0.0.0.0/0。

- c. 选择 Add another rule、Type、SSH。对于 Source，输入您的网络的公有 IPv4 地址范围。
 - d. 选择 Add another rule、Type、RDP。对于 Source，输入您的网络的公有 IPv4 地址范围。
 - e. (可选，仅 IPv6) 选择 Add another rule、Type、HTTP。对于 Source，输入 ::/0。
 - f. (可选，仅 IPv6) 选择 Add another rule、Type、HTTPS。对于 Source，输入 ::/0。
 - g. (可选，仅 IPv6) 选择 Add another rule、Type、SSH (对于 Linux) 或 RDP (对于 Windows)。对于 Source，输入您的网络的 IPv6 地址范围。
 - h. 选择 Save (保存)。
3. 在 Outbound Rules 选项卡上，选择 Edit，然后添加出站流量规则，如下所示：
 - a. 找到启用所有出站流量的默认规则，然后选择 Remove。
 - b. 选择 Type、MS SQL。对于 Destination，指定 DBServerSG 安全组的 ID。
 - c. 选择 Add another rule、Type、MySQL。对于 Destination，指定 DBServerSG 安全组的 ID。
 - d. 选择 Add another rule、Type、HTTPS。对于 Destination，输入 0.0.0.0/0。
 - e. 选择 Add another rule、Type、HTTP。对于 Destination，输入 0.0.0.0/0。
 - f. (可选，仅 IPv6) 选择 Add another rule、Type、HTTPS。对于 Destination，输入 ::/0。
 - g. (可选，仅 IPv6) 选择 Add another rule、Type、HTTP。对于 Destination，输入 ::/0。
 - h. 选择 Save (保存)。

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. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 选择 Type、MS SQL。对于 Source，指定您的 WebServerSG 安全组的 ID。
 - b. 选择 Add another rule、Type、MYSQL。对于 Source，指定您的 WebServerSG 安全组的 ID。
 - c. 选择 Save (保存)。
3. 在 Outbound Rules 选项卡上，选择 Edit，然后添加出站流量规则，如下所示：
 - a. 找到启用所有出站流量的默认规则，然后选择 Remove。
 - b. 选择 Type、HTTP。对于 Destination，输入 0.0.0.0/0。
 - c. 选择 Add another rule、Type、HTTPS。对于 Destination，输入 0.0.0.0/0。
 - d. (可选，仅 IPv6) 选择 Add another rule、Type、HTTP。对于 Destination，输入 ::/0。
 - e. (可选，仅 IPv6) 选择 Add another rule、Type、HTTPS。对于 Destination，输入 ::/0。
 - f. 选择 Save (保存)。

您现在可以在您的 VPC 内启动实例。

启动实例 (Web 服务器或数据库服务器)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板中，选择 Launch Instance。
3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

如果您要使用您的实例进行 IPv6 通信，则必须选择支持的实例类型，例如 T2。有关更多信息，请参阅 [Amazon EC2 实例类型](#)。

4. 在 Configure Instance Details 页上，对于 Network，选择您之前创建的 VPC，然后选择一个子网。例如，在公有子网中启动 Web 服务器，在私有子网中启动数据库服务器。

5. (可选) 默认情况下，在非默认 VPC 中启动的实例未分配公有 IPv4 地址。要能连接到公有子网中的实例，您可以现在分配公有 IPv4 地址，也可以分配弹性 IP 地址并在实例启动后将其分配给实例。要现在分配公有 IPv4 地址，请确保从 Auto-assign Public IP 列表中选择 Enable。您无需为私有子网中的实例分配公有 IP 地址。

Note

您只能为设备索引为 eth0 的单个新网络接口使用自动分配公有 IPv4 功能。有关更多信息，请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)。

6. (可选，仅 IPv6) 您可以从子网范围内为您的实例自动分配 IPv6 地址。对于 Auto-assign IPv6 IP，选择 Enable。
7. 在向导的后两页上，可为您的实例配置存储并添加标签。在 Configure Security Group 页上，选择 Select an existing security group 选项，然后选择您之前创建的一个安全组 (对于 Web 服务器选择 WebServerSG，对于数据库服务器选择 DBServerSG)。选择 Review and Launch。
8. 检视您已经选择的设置。做出所需的任何更改，然后选择 Launch 以选择密钥对并启动您的实例。

如果未按第 5 步中的说明为公有子网中的实例分配公有 IPv4 地址，您将无法与其连接。在您能够访问公有子网中的实例之前，您必须指定一项弹性 IP 地址。

分配弹性 IP 地址并将其指定给一个实例 (IPv4)

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

5. 从列表中选择弹性 IP 地址，然后选择 Actions、Associate address。
6. 选择网络接口或实例。对于 Private IP，选择要与弹性 IP 地址关联的相应地址，然后选择 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，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Connect to Your Linux Instance](#) 部分。有关如何连接 Windows 实例的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Windows 实例\)](#) 中的 [Connect to Your Windows Instance](#) 部分。

通过 NAT 实现实风景 2

您可以使用 NAT 实例而不是 NAT 网关实现实风景 2。有关 NAT 实例的更多信息，请参阅 [NAT 实例 \(p. 216\)](#)。

您可以使用与上面相同的过程；不过，在 VPC 向导的 NAT 部分，应选择 Use a NAT instance instead 并指定 NAT 实例的详细信息。您还需要为 NAT 实例 (NATSG) 提供一个安全组，使 NAT 实例能够接收来自私有子网实例的 Internet 绑定的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。

在使用 NAT 实例创建 VPC 后，您必须将与 NAT 实例关联的安全组更改为新的 NATSG 安全组 (默认情况下，NAT 实例是使用默认安全组启动的)。

NATSG：推荐规则

入站			
源	协议	端口范围	注释

10.0.1.0/24	TCP	80	允许来自私有子网中的数据库服务器的入站 HTTP 流量
10.0.1.0/24	TCP	443	允许来自私有子网中的数据库服务器的入站 HTTPS 流量
您网络的公有 IP 地址范围	TCP	22	允许从您的网络到 NAT 实例的入站 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)

创建 NATSG 安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，然后选择 Create Security Group。
3. 为安全组指定名称和描述。在本主题中，使用名称 NATSG 作为示例。对于 VPC，选择您的 VPC 的 ID，然后选择 Yes, Create。
4. 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。
5. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 选择 Type、HTTP。对于 Source，输入您的私有子网的 IP 地址范围。
 - b. 选择 Add another rule、Type、HTTPS。对于 Source，输入您的私有子网的 IP 地址范围。
 - c. 选择 Add another rule、Type、SSH。对于 Source，输入您的网络的公有 IP 地址范围。
 - d. 选择 Save (保存)。
6. 在 Outbound Rules 选项卡上，选择 Edit，然后添加出站流量规则，如下所示：
 - a. 找到启用所有出站流量的默认规则，然后选择 Remove。
 - b. 选择 Type、HTTP。对于 Destination，输入 0.0.0.0/0。
 - c. 选择 Add another rule、Type、HTTPS。对于 Destination，输入 0.0.0.0/0。
 - d. 选择 Save (保存)。

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. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 从列表中选择 NAT 实例，然后依次选择 Actions (操作)、Networking (网络) 和 Change Security Groups (更改安全组)。
4. 选择您创建的 NATSG 安全组 (请参阅 [安全性 \(p. 33\)](#))，然后选择 Assign Security Groups (分配安全组)。

场景 3：具有公有和私有子网和 AWS Site-to-Site VPN 访问权限的 VPC

此场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。在此场景中，您可以在公有子网中运行有可扩展 Web 前端的多层次应用程序，还能够将您的数据储存在通过 AWS Site-to-Site VPN 连接与您的网络相连的私有子网中。

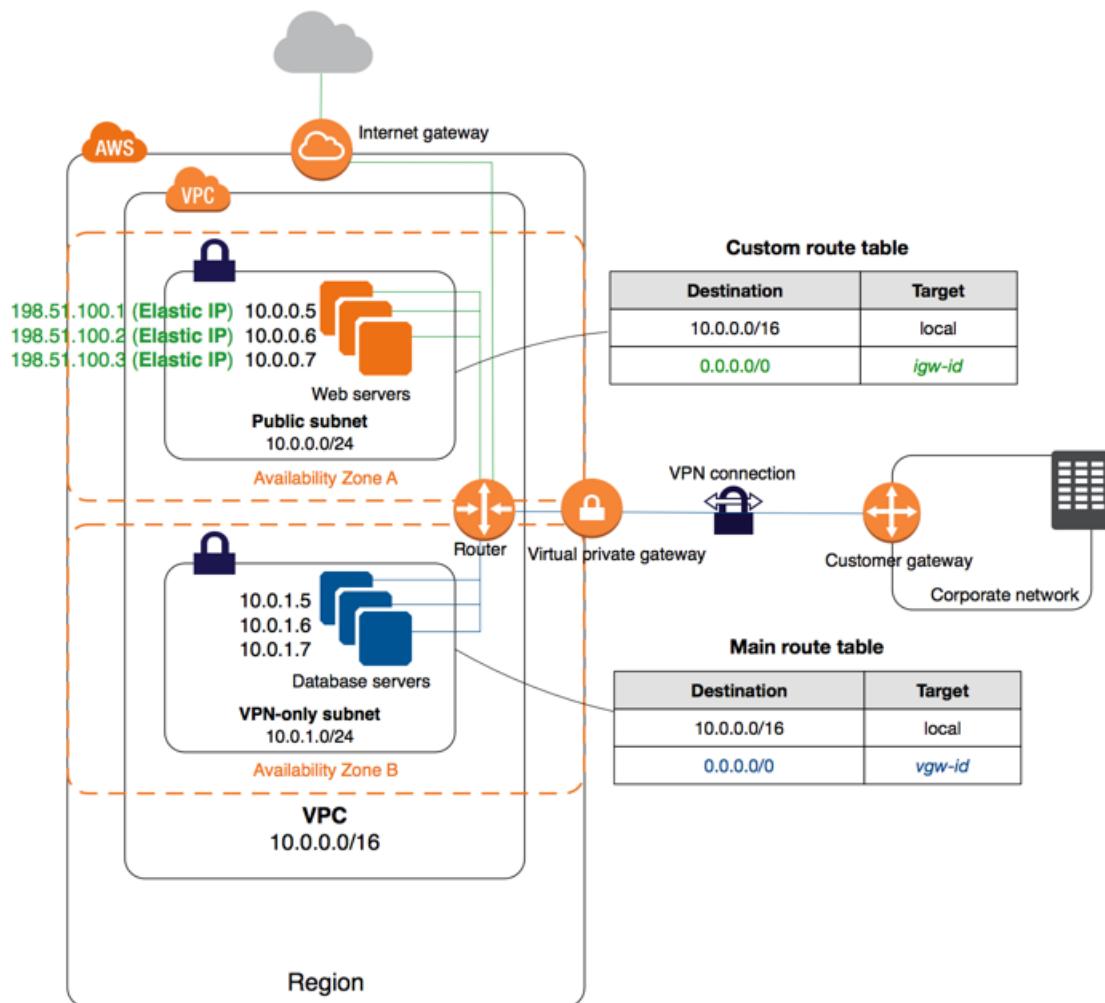
也可以选择为此场景配置 IPv6：您可以使用 VPC 向导创建关联有 IPv6 CIDR 块的 VPC 和子网。在子网中启动的实例可接收 IPv6 地址。目前，我们还不支持通过 Site-to-Site VPN 连接进行 IPv6 通信；但是，VPC 中的实例可通过 IPv6 彼此通信，公有子网中的实例可以通过 IPv6 进行 Internet 通信。有关 IPv4 和 IPv6 寻址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

内容

- [概述 \(p. 41\)](#)
- [路由选择 \(p. 44\)](#)
- [安全性 \(p. 46\)](#)
- [实施场景 3 \(p. 49\)](#)

概述

下表展示了此场景配置的主要组成部分。



Important

对于本场景，[Amazon VPC 网络管理员指南](#)介绍了您的网络管理员需要执行什么操作以在 Site-to-Site VPN 连接的您这一端上配置 Amazon VPC 客户网关。

此情景的配置包括：

- IPv4 CIDR 大小为 /16 的 Virtual Private Cloud (VPC) (示例：10.0.0.0/16)。提供 65536 个私有 IPv4 地址。
- IPv4 CIDR 大小为 /24 的公有子网 (示例：10.0.0.0/24)。提供 256 个私有 IPv4 地址。公有子网是指与包含指向 Internet 网关的路由的路由表关联的子网。
- IPv4 CIDR 大小为 /24 的仅 VPN 子网 (示例：10.0.1.0/24)。提供 256 个私有 IPv4 地址。
- Internet 网关。它将 VPC 连接到 Internet 和其他 AWS 产品。
- 在您的 VPC 和网络之间的 Site-to-Site VPN 连接。Site-to-Site VPN 连接由位于 Site-to-Site VPN 连接的 Amazon 一端的虚拟专用网关和位于 Site-to-Site VPN 连接的您这一端的客户网关组成。
- 子网范围内具有私有 IPv4 地址的实例 (例如 10.0.0.5 和 10.0.1.5)，该范围允许实例彼此通信并与 VPC 中的其他实例通信。
- 公有子网中具有弹性 IP 地址的实例 (示例：198.51.100.1)，这些弹性 IP 地址是使其能够从 Internet 访问的公有 IPv4 地址。可在启动时为实例分配公有 IPv4 地址而不是弹性 IP 地址。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。

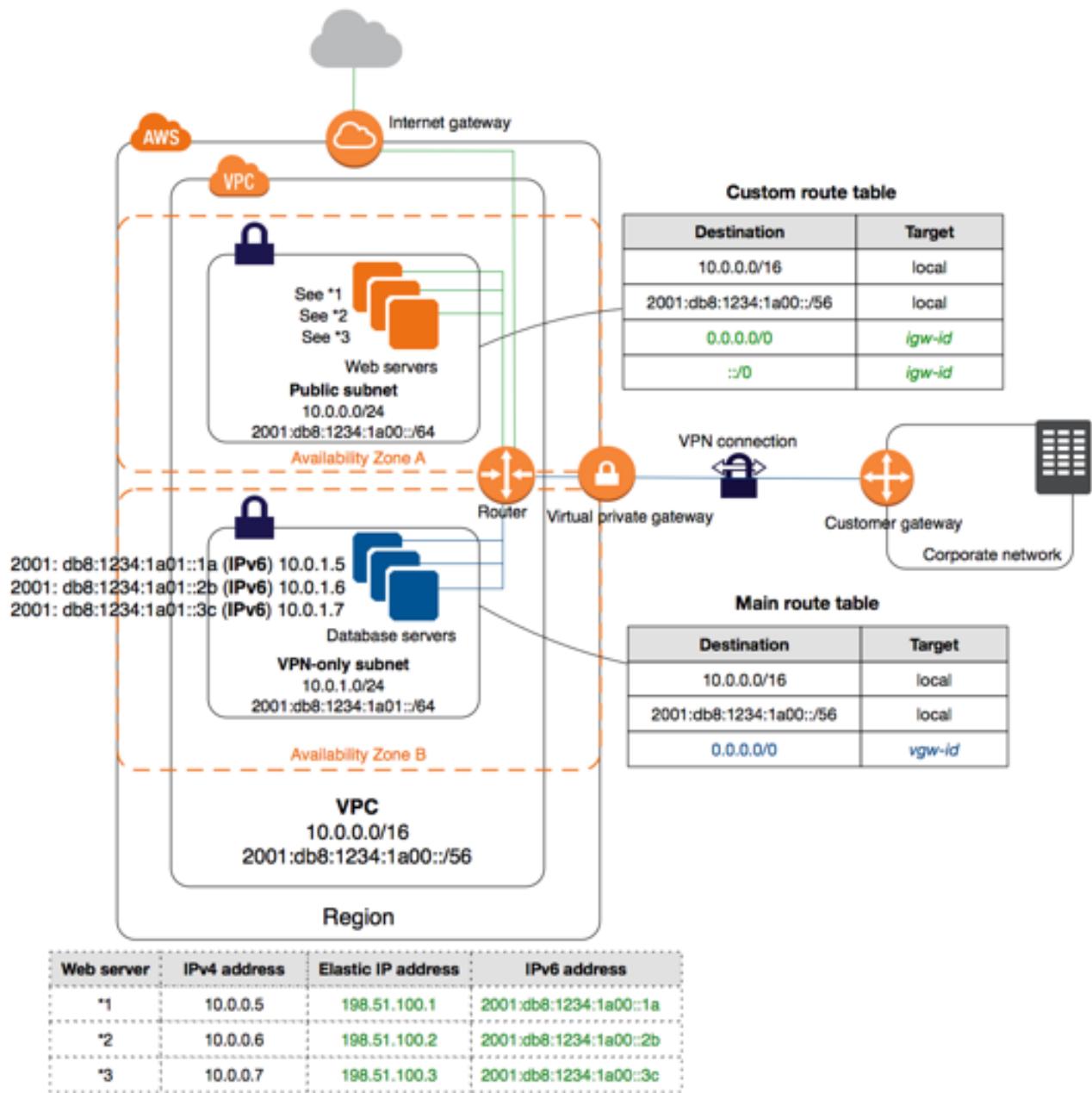
- 与公有子网关联的自定义路由表。此路由表中包含一项条目允许子网中的实例与 VPC 中的其他实例建立通信，另一项条目则允许子网中的实例直接与 Internet 建立通信。
- 与仅限 VPN 的子网关联的主路由表。路由表中包含允许子网中的实例与 VPC 中的其他实例通信的条目；以及允许子网中的实例直接与您的网络通信的条目。

有关子网的更多信息，请参阅[VPC 和子网 \(p. 75\)](#)和[您的 VPC 中的 IP 地址 \(p. 100\)](#)。有关 Internet 网关的更多信息，请参阅[Internet 网关 \(p. 192\)](#)。有关您的 AWS Site-to-Site VPN 连接的更多信息，请参阅[AWS Site-to-Site VPN 用户指南](#)中的[什么是 AWS Site-to-Site VPN](#)？有关配置客户网关的更多信息，请参阅[Amazon VPC 网络管理员指南](#)。

IPv6 概述

您可以选择为此场景启用 IPv6。除了上面列出的组件外，还包括以下配置：

- 与 VPC 关联的 /56 IPv6 CIDR 块（示例：2001:db8:1234:1a00::/56）。AWS 自动分配 CIDR；您不能自选范围。
- 与公有子网关联的 /64 IPv6 CIDR 块（示例：2001:db8:1234:1a00::/64）。您可以从分配给 VPC 的范围内选择您的子网范围。您无法选择 IPv6 CIDR 大小。
- 与仅 VPN 子网关联且大小为 /64 的 IPv6 CIDR 块（示例：2001:db8:1234:1a01::/64）。您可以从分配给 VPC 的范围内选择您的子网范围。您无法选择 IPv6 CIDR 大小。
- 子网范围内分配给实例的 IPv6 地址（示例：2001:db8:1234:1a00::1a）。
- 自定义路由表中的路由表条目，允许公有子网中的实例使用 IPv6 相互通信和直接通过 Internet 通信。
- 主路由表中的一个路由表条目，它允许仅 VPN 子网内的实例使用 IPv6 彼此进行通信。



路由选择

您的 VPC 有一个隐藏路由器 (显示在此场景的配置图中)。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。

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。目前，我们还不支持将 IPv6 用于 Site-to-Site VPN 连接。

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。

可将Site-to-Site VPN 连接配置为静态路由Site-to-Site VPN 连接或动态路由Site-to-Site VPN 连接（使用 BGP）。如果您选择静态路由，则将收到提示，要求您在创建Site-to-Site 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。

下表描述了此场景的路由表。

主路由表

第一个条目是 VPC 中本地路由的默认条目；此条目允许此 VPC 中的实例通过 IPv4 相互通信。第二个条目将来自私有子网的所有其他 IPv4 子网流量通过虚拟专用网关（例如 vgw-1a2b3c4d）路由到您的网络。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	vgw-id

自定义路由表

第一个条目是 VPC 中本地路由的默认条目；这项条目允许 VPC 中的实例在彼此之间进行通信。第二个条目将来自公有子网的所有其他 IPv4 子网流量通过 Internet 网关（例如 igw-1a2b3c4d）路由到 Internet。

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

替代路由

或者，如果您希望私有子网中的实例能够访问 Internet，您可以在公有子网中创建一个网络地址转换 (NAT) 网关或实例，然后设置路由，以使该子网的 Internet 绑定流量能够通向 NAT 设备。这使得仅 VPN 子网中的实例能够通过 Internet 网关发送请求（例如软件更新）。

有关手动设置 NAT 设备的更多信息，请参阅 [NAT \(p. 200\)](#)。有关使用 VPC 向导来设置 NAT 设备的信息，请参阅 [场景 2：带有公有子网和私有子网 \(NAT\) 的 VPC \(p. 29\)](#)。

若要使私有子网的 Internet 绑定数据流能够通向 NAT 设备，您必须对主路由表进行如下更新。

第一个条目是 VPC 中本地路由的默认条目。第二行条目用于将绑定到您的客户网络（在该示例中，假设您的本地网络的 IP 地址为 172.16.0.0/12）的子网流量路由到虚拟专用网关。第三个条目将所有其他子网流量发送到 NAT 网关。

目的地	目标
10.0.0.0/16	本地
172.16.0.0/12	vgw-id
0.0.0.0/0	nat-gateway-id

IPv6 路由

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则您的路由表必须包含适用于 IPv6 流量的单独路由。下面的表显示了当您选择在 VPC 中启用 IPv6 通信时此场景的自定义路由表。

主路由表

第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。

目的地	目标
10.0.0.0/16	本地
2001:db8:1234:1a00::/56	本地
0.0.0.0/0	vgw-id

自定义路由表

第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。第四个条目将所有其他 IPv6 子网流量路由到 Internet 网关。

目的地	目标
10.0.0.0/16	本地
2001:db8:1234:1a00::/56	本地
0.0.0.0/0	igw-id
::/0	igw-id

安全性

AWS 提供了可以用于在 VPC 中提高安全性的两个功能：安全组 和 网络 ACL。安全组可以控制您的实例的入站和出站数据流，网络 ACL 可以控制您的子网的入站和出站数据流。多数情况下，安全组即可满足您的需要；但是，如果您需要为您的 VPC 增添额外一层安全保护，您也可以使用网络 ACL。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

在场景 3 中，您可以使用安全组而不是网络 ACL。如果希望使用网络 ACL，请参阅 [场景 3 的推荐规则 \(p. 145\)](#)。

您的 VPC 带有[默认的安全组 \(p. 120\)](#)。如果您在启动期间没有指定其他安全组，在该 VPC 中启动的实例会与默认安全组自动关联。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：在公有子网中启动 Web 服务器时指定该安全组。
- DBServerSG：在仅 VPN 子网中启动数据库服务器时指定该安全组。

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，在这个场景中，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，在这个场景中，所有分配到一个安全组的实例都位于相同的子网之中。

下表描述了 WebServerSG 安全组的推荐规则，这些规则允许 Web 服务器接收 Internet 流量，以及来自您的网络的 SSH 和 RDP 流量。Web 服务器也可发起对仅限 VPN 的子网中的数据库服务器的读取和写入请求，并向 Internet 发送数据流；例如获取软件更新。由于 Web 服务器不发起任何其他出站通信，因此将删除默认出站规则。

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。

WebServerSG : 推荐规则

入站			
源	协议	端口范围	注释
0.0.0.0/0	TCP	80	允许从任意 IPv4 地址对 Web 服务器进行入站 HTTP 访问。
0.0.0.0/0	TCP	443	允许从任意 IPv4 地址对 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			
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。
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 HTTPS 访问。

下表描述了 DBServerSG 安全组的推荐规则，这些规则允许 Microsoft SQL Server 和 MySQL 读和写 Web 服务器请求以及来自您的网络的 SSH 和 RDP 流量。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	允许与 WebServerSG 安全组关联的 Web 服务器进行入站 Microsoft SQL Server 访问。
您的 WebServerSG 安全组 ID	TCP	3306	允许与 WebServerSG 安全组关联的 Web 服务器进行入站 MySQL Server 访问。
您的网络的 IPv4 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)。
您的网络的 IPv4 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 IPv4 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 IPv4 HTTPS 访问 (例如软件更新)。

(可选) 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。要允许自定义安全组进行此类通信，您必须添加下列规则：

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	允许到分配到该安全组的其他实例的出站流量。

IPv6 安全性

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则必须向 WebServerSG 和 DBServerSG 安全组添加单独的规则来控制您的实例的入站和出站 IPv6 流量。在此场景中，Web 服务器能够接收通过 IPv6 的所有 Internet 流量以及来自您的本地网络的通过 IPv6 的 SSH 或 RDP 流量。它们也可以发起到 Internet 的 IPv6 流量。数据库服务器无法启动到 Internet 的出站 IPv6 流量，因此，它们不需要任何附加的安全组规则。

以下是针对 WebServerSG 安全组的特定于 IPv6 的规则 (是上面所列规则的补充)。

入站			
源	协议	端口范围	注释
::/0	TCP	80	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTP 访问。
::/0	TCP	443	允许从任意 IPv6 地址对 Web 服务器进行入站 HTTPS 访问。
您的网络的 IPv6 地址范围	TCP	22	(Linux 实例) 允许您的网络通过 IPv6 进行入站 SSH 访问。
您的网络的 IPv6 地址范围	TCP	3389	(Windows 实例) 允许您的网络通过 IPv6 进行入站 RDP 访问。
出站			

目的地	协议	端口范围	注释
::/0	TCP	HTTP	允许对任意 IPv6 地址进行出站 HTTP 访问。
::/0	TCP	HTTPS	允许对任意 IPv6 地址进行出站 HTTPS 访问。

实施场景 3

要实现情景 3，请获取有关客户网关的信息，然后使用 VPC 向导创建 VPC。VPC 向导会为您创建 Site-to-Site VPN 连接，并提供客户网关和虚拟专用网关。

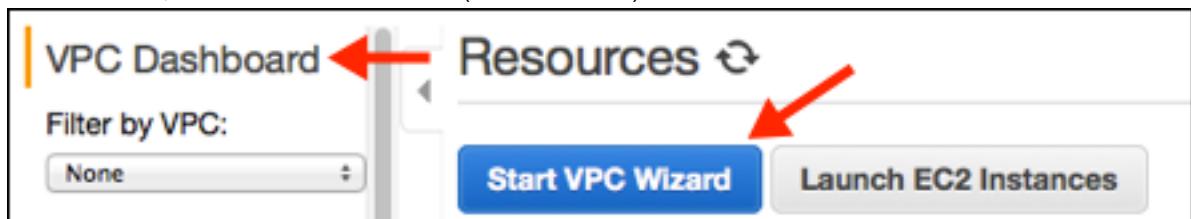
这些过程包括用于为您的 VPC 启用和配置 IPv6 通信的可选步骤。如果您不想在 VPC 上使用 IPv6，则不必执行这些步骤。

准备您的客户网关

- 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，请参阅 [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，请参阅 [Amazon VPC 网络管理员指南](#)。
- 为客户网关的外部接口获取 Internet 可路由的 IP 地址。地址必须是静态的，可位于执行网络地址转换 (NAT) 任务的设备之后。
- 如果需要创建静态路由 Site-to-Site VPN 连接，请获取应通过 Site-to-Site VPN 连接传播到虚拟专用网关的内部 IP 范围列表（以 CIDR 表示）。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的 [路由表和 VPN 路由优先级](#)。

使用 VPC 向导创建 VPC

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在控制面板上，选择 Launch VPC Wizard (启动 VPC 向导)。



- 选择第三个选项 VPC with Public and Private Subnets and Hardware VPN Access (带有公有子网和私有子网以及硬件 VPN 访问的 VPC)，然后选择 Select (选择)。
- 在 VPC with Public and Private Subnets and Hardware VPN Access (带有公有和私有子网以及硬件 VPN 访问的 VPC) 页面上，执行以下操作：
 - (可选) 根据需要修改 VPC 和子网的 IPv4 CIDR 块范围，或保留默认值。
 - (可选) 命名您的 VPC 和子网。这可帮助您以后在控制台中识别它们。
 - (可选，仅 IPv6) 对于 IPv6 CIDR block，选择 Amazon-provided IPv6 CIDR block。对于 Public subnet's IPv6 CIDR (公有子网的 IPv6 CIDR)，选择 Specify a custom IPv6 CIDR (指定自定义 IPv6 CIDR) 并指定您的子网的十六进制对值或保留默认值。对于 Private subnet's IPv6 CIDR，选择 Specify a custom IPv6 CIDR。指定 IPv6 子网的十六进制对值或保留默认值。
 - 选择 Next (下一步)。
- 在 Configure your VPN (配置 VPN) 页面上，执行以下操作：
 - 对于 Customer Gateway IP (客户网关 IP)，指定 VPN 路由器的公有 IP 地址。

- b. (可选) 命名您的客户网关和 Site-to-Site VPN 连接。
 - c. 对于 Routing Type (路由类型)，选择一个路由选项。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的 [Site-to-Site VPN 路由选项](#)。
 - 如果您的 VPN 路由器支持边界网关协议 (BGP)，请选择 Dynamic (requires BGP) (动态(需要 BGP))。
 - 如果您的 VPN 路由器不支持 BGP，请选择 Static。对于 IP Prefix (IP 前缀)，添加网络的各个 IP 范围 (以 CIDR 表示)。
 - d. 选择 Create VPC (创建 VPC)。
6. 完成向导后，在导航窗格中选择 Site-to-Site VPN Connections (站点到站点连接)。选择向导已创建的 Site-to-Site VPN 连接，然后选择 Download Configuration (下载配置)。在对话框中，选择客户网关供应商、平台和软件版本，然后选择 Yes, Download。
 7. 保存包含 VPN 配置的文本文件，并连同本指南 [Amazon VPC 网络管理员指南](#) 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。

创建 WebServerSG 和 DBServerSG 安全组。这些安全组会互相引用，因此，您必须先创建它们，然后再向其中添加规则。

创建 WebServerSG 和 DBServerSG 安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 提供安全组的名称和描述。在本主题中，使用名称 WebServerSG 作为示例。从 VPC 中选择您 VPC 的 ID，然后选择 Yes, Create (是，创建)。
5. 再次选择 Create Security Group。
6. 提供安全组的名称和描述。在本主题中，使用名称 DBServerSG 作为示例。从 VPC 中选择您 VPC 的 ID，然后选择 Yes, Create (是，创建)。

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. 在 Inbound Rules 选项卡上，选择 Edit，然后添加入站流量规则，如下所示：
 - a. 从 Type (类型) 中选择 HTTP，然后在 Source (源) 中键入 0.0.0.0/0。
 - b. 选择 Add another rule (再添加一条规则)，然后从 Type (类型) 中选择 HTTPS，并为 Source (源) 键入 0.0.0.0/0。
 - c. 选择 Add another rule (再添加一条规则)，然后从 Type (类型) 中选择 SSH。在 Source (源) 中键入您的网络的公有 IP 地址范围。
 - d. 选择 Add another rule (再添加一条规则)，然后从 Type (类型) 中选择 RDP。在 Source (源) 中键入您的网络的公有 IP 地址范围。
 - e. (可选，仅 IPv6) 选择 Add another rule、Type、HTTP。对于 Source，键入 ::/0。
 - f. (可选，仅 IPv6) 选择 Add another rule、Type、HTTPS。对于 Source，键入 ::/0。
 - g. (可选，仅 IPv6) 选择 Add another rule、Type、SSH (对于 Linux) 或 RDP (对于 Windows)。对于 Source (源)，键入您的网络的 IPv6 地址范围。
 - h. 选择 Save (保存)。
3. 在 Outbound Rules 选项卡上，选择 Edit，然后添加出站流量规则，如下所示：
 - a. 找到启用所有出站流量的默认规则，然后选择 Remove。
 - b. 从 Type (类型) 中选择 MS SQL。对于 Destination (目标)，键入 DBServerSG 安全组的 ID。

- c. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 MySQL。对于 Destination , 指定 DBServerSG 安全组的 ID。
- d. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 HTTPS。对于 Destination , 键入 0.0.0.0/0。
- e. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 HTTP。对于 Destination , 键入 0.0.0.0/0。
- f. 选择 Save (保存)。

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. 在 Inbound Rules 选项卡上 , 选择 Edit , 然后添加入站流量规则 , 如下所示 :
 - a. 从 Type (类型) 中选择 SSH , 然后在 Source (源) 中键入您的网络的 IP 地址范围。
 - b. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 RDP , 然后在 Source (源) 中键入您的网络的 IP 地址范围。
 - c. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 MS SQL。在 Source (源) 中键入您的 WebServerSG 安全组的 ID。
 - d. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 MySQL。在 Source (源) 中键入您的 WebServerSG 安全组的 ID。
 - e. 选择 Save (保存)。
3. 在 Outbound Rules 选项卡上 , 选择 Edit , 然后添加出站流量规则 , 如下所示 :
 - a. 找到启用所有出站流量的默认规则 , 然后选择 Remove。
 - b. 从 Type (类型) 中选择 HTTP。对于 Destination , 键入 0.0.0.0/0。
 - c. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 HTTPS。对于 Destination , 键入 0.0.0.0/0。
 - d. 选择 Save (保存)。

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。

启动实例 (Web 服务器或数据库服务器)

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上 , 选择 Launch Instance。
3. 按照向导中的指示操作。选择 AMI 和实例类型 , 然后选择 Next: Configure Instance Details。

Note

如果您要使用您的实例进行 IPv6 通信 , 则必须选择支持的实例类型 , 例如 T2。有关更多信息 , 请参阅 [Amazon EC2 实例类型](#)。

4. 在 Configure Instance Details (配置实例详细信息) 页面上 , 从 Network (网络) 中选择您早先创建的 VPC , 然后选择一个子网。例如 , 在公有子网中启动 Web 服务器 , 在私有子网中启动数据库服务器。
5. (可选) 默认情况下 , 在非默认 VPC 中启动的实例未分配公有 IPv4 地址。要能连接到公有子网中的实例 , 您可以现在分配公有 IPv4 地址 , 也可以分配弹性 IP 地址并在实例启动后将其分配给实例。要现在分配公有 IP 地址 , 请确保从 Auto-assign Public IP (自动分配公有 IP) 中选择 Enable (启用)。您无需为私有子网中的实例分配公有 IP 地址。

Note

您只能为设备索引为 eth0 的单个新网络接口使用自动分配公有 IP 地址功能。有关更多信息 , 请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)。

6. (可选，仅 IPv6) 您可以从子网范围内为您的实例自动分配 IPv6 地址。对于 Auto-assign IPv6 IP，选择 Enable。
7. 在向导的后两页上，可为您的实例配置存储并添加标签。在 Configure Security Group 页上，选择 Select an existing security group 选项，然后选择您创建的一个安全组 (对于 Web 服务器实例选择 WebServerSG，对于数据库服务器实例选择 DBServerSG)。选择 Review and Launch。
8. 检视您已经选择的设置。执行所需的任何更改，然后选择 Launch 以选择一个密钥对并启动您的实例。

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Site-to-Site VPN 连接](#)。

如果未按第 5 步中的说明为公有子网中的实例分配公有 IPv4 地址，您将无法与其连接。在您能够访问公有子网中的实例之前，您必须指定一项弹性 IP 地址。

使用控制台分配弹性 IP 地址并将其分配给一个实例

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

5. 从列表中选择弹性 IP 地址，然后选择 Actions、Associate address。
6. 选择网络接口或实例。从相应的 Private IP (私有 IP) 中选择要与弹性 IP 地址关联的地址，然后选择 Associate (关联)。

在场景 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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 DHCP Options Sets。
3. 选择 Create DHCP options set。
4. 在创建 DHCP 选项集对话框的域名服务器中，指定 Amazon DNS 服务器 (AmazonProvidedDNS) 的地址以及您的 DNS 服务器的地址（例如 192.0.2.1）并以逗号隔开，然后选择是，创建。
5. 在导航窗格中，选择 Your VPCs。
6. 选择 VPC，然后选择 Actions、Edit DHCP Options Set。
7. 从 DHCP options set (DHCP 选项集) 中选择新选项集的 ID，然后选择 Save (保存)。
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，请参阅Amazon EC2 用户指南（适用于 Linux 实例）中的[Connect to Your Linux Instance](#)部分。有关如何连接 Windows 实例的信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的[Connect to Your Windows Instance](#)部分。

场景 4：仅具有一个私有子网以及 AWS Site-to-Site VPN 访问权限的 VPC

此场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，我们建议您采用此方案。

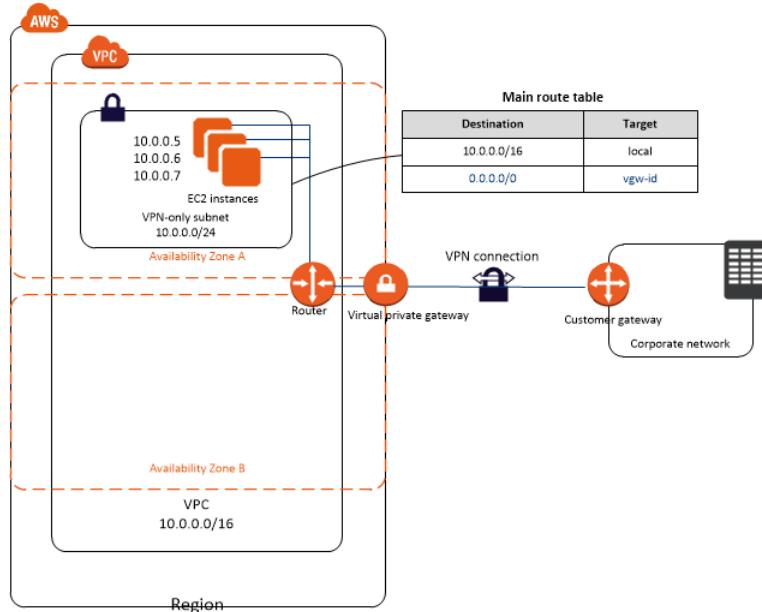
也可以选择为 IPv6 配置此场景，您可以使用 VPC 向导创建关联有 IPv6 CIDR 块的 VPC 和子网。在子网中启动的实例可接收 IPv6 地址。我们目前不支持通过 AWS Site-to-Site VPN 连接进行 IPv6 通信；但 VPC 中的实例可以通过 IPv6 彼此通信。有关 IPv4 和 IPv6 寻址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

内容

- [概述 \(p. 53\)](#)
- [路由选择 \(p. 54\)](#)
- [安全性 \(p. 55\)](#)
- [实施场景 4 \(p. 56\)](#)

概述

下表展示了此场景配置的主要组成部分。



Important

对于本场景，[Amazon VPC 网络管理员指南](#)介绍了您的网络管理员需要执行什么操作以在 Site-to-Site VPN 连接的您这一端上配置 Amazon VPC 客户网关。

此情景的配置包括：

- 大小为 /16 CIDR 的 Virtual Private Cloud (VPC) (示例：10.0.0.0/16)。提供 65536 个私有 IP 地址。
- 大小为 /24 CIDR 的仅 VPN 子网 (示例：10.0.0.0/24)。提供 256 个私有 IP 地址。

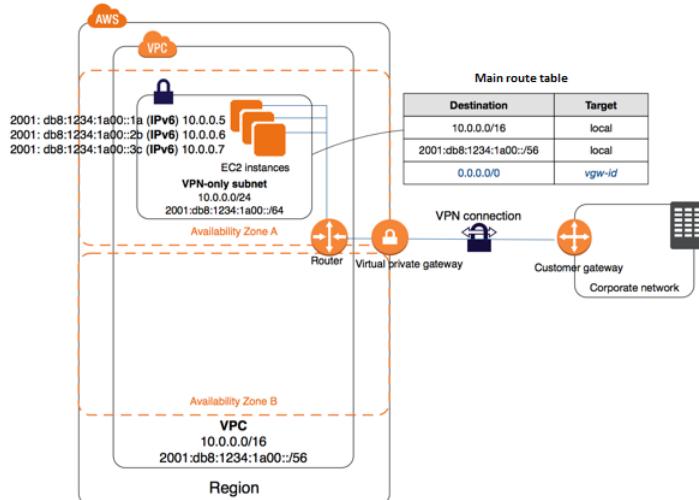
- 在您的 VPC 和网络之间的 Site-to-Site VPN 连接。Site-to-Site VPN 连接由位于 Site-to-Site VPN 连接的 Amazon 一端的虚拟专用网关和位于 Site-to-Site VPN 连接的您这一端的客户网关组成。
- 有私有 IP 地址的实例处于子网范围之内（例如 10.0.0.5、10.0.0.6 和 10.0.0.7），这使它们可以在彼此之间以及与 VPC 中的其他实例建立通信。
- 主路由表包含允许子网中的实例与 VPC 中的其他实例通信的路由。路由传播已启用，因此，允许子网中的实例与网络直接通信的路由在主路由表中显示为传播路由。

有关子网的更多信息，请参阅[VPC 和子网 \(p. 75\)](#)和[您的 VPC 中的 IP 地址 \(p. 100\)](#)。有关您的 Site-to-Site VPN 连接的更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的[什么是 AWS Site-to-Site VPN？](#)。有关配置客户网关的更多信息，请参阅[Amazon VPC 网络管理员指南](#)。

IPv6 概述

您可以选择为此场景启用 IPv6。除了上面列出的组件外，还包括以下配置：

- 与 VPC 关联的 /56 IPv6 CIDR 块（示例：2001:db8:1234:1a00::/56）。AWS 自动分配 CIDR；您不能自选范围。
- 与仅 VPN 子网关联且大小为 /64 的 IPv6 CIDR 块（示例：2001:db8:1234:1a00::/64）。您可以从分配给 VPC 的范围内选择您的子网范围。您无法选择 IPv6 CIDR 大小。
- 子网范围内分配给实例的 IPv6 地址（示例：2001:db8:1234:1a00::1a）。
- 主路由表中的路由表条目，它允许私有子网中的实例使用 IPv6 相互通信。



路由选择

您的 VPC 有一个隐藏路由器（显示在此场景的配置图中）。在此场景中，VPC 向导创建一个路由表，将所有目标为 VPC 外某个地址的流量路由到 AWS Site-to-Site VPN 连接，并将该路由表与子网关联。

以下内容说明了此情景的路由表。第一个条目是 VPC 中本地路由的默认条目；这项条目允许该 VPC 中的实例在彼此之间进行通信。第二个条目将所有其他子网流量路由到虚拟专用网关（例如 vgw-1a2b3c4d）。

目的地	目标
10.0.0.0/16	本地

目的地	目标
0.0.0.0/0	vgw-id

可将 AWS Site-to-Site VPN 连接配置为静态路由 Site-to-Site VPN 连接或动态路由 Site-to-Site VPN 连接 (使用 BGP)。如果您选择静态路由，则将收到提示，要求您在创建 Site-to-Site 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。目前，我们还不支持将 IPv6 用于 Site-to-Site VPN 连接。

IPv6 路由

如果将 IPv6 CIDR 块与您的 VPC 和子网关联，则您的路由表包含适用于 IPv6 流量的单独路由。以下内容说明了此场景的自定义路由表。第二个条目是自动为 VPC 中通过 IPv6 的本地路由添加的默认路由。

目的地	目标
10.0.0.0/16	本地
2001:db8:1234:1a00::/56	本地
0.0.0.0/0	vgw-id

安全性

AWS 提供了可以用于在 VPC 中提高安全性的两个功能：安全组 和 网络 ACL。安全组可以控制您的实例的入站和出站数据流，网络 ACL 可以控制您的子网的入站和出站数据流。多数情况下，安全组即可满足您的需要；但是，如果您需要为您的 VPC 增添额外一层安全保护，您也可以使用网络 ACL。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

对于场景 4，将对您的 VPC 使用默认安全组而非网络 ACL。如果希望使用网络 ACL，请参阅 [场景 4 的推荐规则 \(p. 150\)](#)。

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。对于该情景，我们建议您向默认安全组添加入站规则以允许来自您的网络的入站 SSH 流量 (Linux) 和远程桌面流量 (Windows)。

Important

默认安全组自动允许所分配的实例彼此之间进行通信，因此您不必添加规则以允许此项。如果您使用不同的安全组，则必须添加一条规则以允许此项。

下表介绍应向您的 VPC 的默认安全组添加的入站规则。

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 IPv4 地址范围	TCP	22	(Linux 实例) 允许来自您的网络的入站 SSH 流量。

您网络的私有 IPv4 地址范围	TCP	3389	(Windows 选项) 允许来自您网络的入站 RDP 流量。
------------------	-----	------	---------------------------------

IPv6 安全性

如果将 IPv6 CIDR 块与您的 VPC 和子网关联，则必须向安全组中添加单独的规则来控制您的实例的入站和出站 IPv6 流量。在此场景中，无法通过使用 IPv6 的 Site-to-Site VPN 连接访问数据库服务器；因此，不需要设置额外的安全组规则。

实施场景 4

要实现场景 4，请获取有关客户网关的信息，然后使用 VPC 向导创建 VPC。VPC 向导会为您创建 Site-to-Site VPN 连接，并提供客户网关和虚拟私有网关。

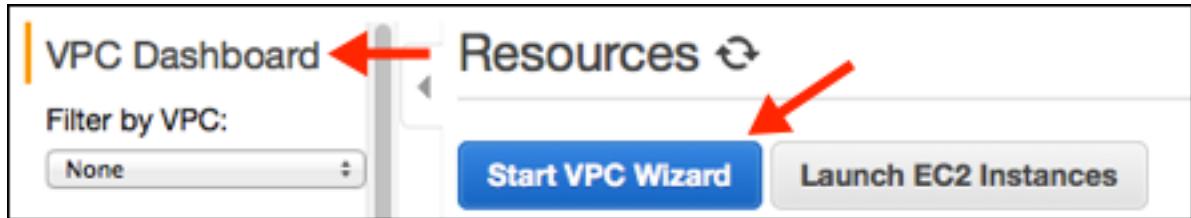
准备您的客户网关

1. 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，请参阅 [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，请参阅 [Amazon VPC 网络管理员指南](#)。
2. 为客户提供外部接口以获取 Internet 可路由的 IP 地址。地址必须是静态的，可位于执行网络地址转换 (NAT) 任务的设备之后。
3. 如果需要创建静态路由 Site-to-Site VPN 连接，请获取应通过 Site-to-Site VPN 连接传播到虚拟专用网关的内部 IP 范围列表（以 CIDR 表示）。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南中的 [Site-to-Site VPN 路由选项](#)。

使用 VPC 向导创建您的 VPC 和 Site-to-Site VPN 连接。

使用 VPC 向导创建 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在控制面板上，选择 Launch VPC Wizard (启动 VPC 向导)。



3. 选择第四个选项 VPC with a Private Subnet Only and Hardware VPN Access (仅带有私有子网和硬件 VPN 访问的 VPC)，然后选择 Select (选择)。
4. 在 VPC with a Private Subnet Only and Hardware VPN Access (仅带有私有子网和硬件 VPN 访问的 VPC) 页面上，执行以下操作：
 - a. (可选) 根据需要修改 VPC 和子网的 IPv4 CIDR 块范围，或保留默认值。
 - b. (可选) 命名您的 VPC 和子网。这可帮助您以后在控制台中识别它们。
 - c. (可选，仅 IPv6) 对于 IPv6 CIDR block，选择 Amazon-provided IPv6 CIDR block。对于 Private subnet's IPv6 CIDR，选择 Specify a custom IPv6 CIDR。指定 IPv6 子网的十六进制对值或保留默认值 (00)。
 - d. 选择 Next (下一步)。
5. 在 Configure your VPN (配置 VPN) 页面上，执行以下操作：
 - a. 对于 Customer Gateway IP (客户网关 IP)，指定 VPN 路由器的公有 IP 地址。

- b. (可选) 命名您的客户网关和Site-to-Site VPN 连接。
 - c. 对于 Routing Type (路由类型) , 选择一个路由选项。有关更多信息 , 请参阅 AWS Site-to-Site VPN 用户指南 中的[Site-to-Site VPN 路由选项](#)。
 - 如果您的 VPN 路由器支持边界网关协议 (BGP) , 请选择 Dynamic (requires BGP) (动态(需要 BGP))。
 - 如果您的 VPN 路由器不支持 BGP , 请选择 Static。对于 IP Prefix (IP 前缀) , 添加网络的各个 IP 范围 (以 CIDR 表示)。
 - d. 选择 Create VPC (创建 VPC)。
6. 完成向导后 , 在导航窗格中选择 Site-to-Site VPN Connections (站点到站点连接)。选择向导已创建的 Site-to-Site VPN 连接 , 然后选择 Download Configuration (下载配置)。在对话框中 , 选择客户网关供应商、平台和软件版本 , 然后选择 Yes, Download。
7. 保存包含 VPN 配置的文本文件 , 并连同本指南[Amazon VPC 网络管理员指南](#)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。

在这个场景中 , 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。如果不想要让实例发起出站通信 , 也可删除默认出站规则。

更新默认安全组的规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中选择 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. 在 Inbound Rules 选项卡上 , 选择 Edit , 然后添加入站流量规则 , 如下所示 :
 - a. 从 Type (类型) 中选择 SSH , 然后在 Source (源) 中键入您的网络的私有 IP 地址范围 (例如 172.0.0.0/12)。
 - b. 选择 Add another rule (再添加一条规则) , 然后从 Type (类型) 中选择 RDP , 并在 Source (源) 中键入您的网络的私有 IP 地址范围。
 - c. 选择 Save (保存)。
4. (可选) 在 Outbound Rules 选项卡上 , 选择 Edit , 找到启用所有出站流量的默认规则 , 选择 Remove , 然后选择 Save。

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. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上 , 选择 Launch Instance。
3. 按照向导中的指示操作。选择 AMI 和实例类型 , 然后选择 Next: Configure Instance Details。

Note

如果您要使用您的实例进行 IPv6 通信 , 则必须选择支持的实例类型 , 例如 T2。有关更多信息 , 请参阅[Amazon EC2 实例类型](#)。

4. 在 Configure Instance Details 页上 , 从 Network 列表中选择您早先创建的 VPC , 然后选择一个子网。选择 Next: Add Storage。
5. 在向导的后两页上 , 可为您的实例配置存储并添加标签。在 Configure Security Group (配置安全组) 页上 , 选择 Select an existing security group (选择一个现有的安全组) 选项 , 然后选择默认安全组。选择 Review and Launch。
6. 检视您已经选择的设置。执行所需的任何更改 , 然后选择 Launch 以选择一个密钥对并启动您的实例。

在场景 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。场景 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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 DHCP Options Sets。
3. 选择 Create DHCP Options Set。
4. 在 Create DHCP Options Set 对话框中，在 Domain name servers 框中输入您的 DNS 服务器的地址，然后选择 Yes, Create。在这个例子中，您的 DNS 服务器是 192.0.2.1。
5. 在导航窗格中，选择 Your VPCs。
6. 选择 VPC，然后在 Summary 选项卡中选择 Edit。
7. 从 DHCP options set 列表中选择新选项集的 ID，然后选择 Save。
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，请参阅Amazon EC2 用户指南（适用于 Linux 实例）中的[Connect to Your Linux Instance](#)部分。有关如何连接 Windows 实例的信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的[Connect to Your Windows Instance](#)部分。

示例：使用 AWS CLI 创建 IPv4 VPC 和子网

以下示例使用 AWS CLI 命令来创建具有 IPv4 CIDR 块的非默认 VPC，以及 VPC 中的公有和私有子网。在您创建了 VPC 和子网后，您可以在公有子网中启动实例，然后连接到该实例。要开始此操作，您必须首先安装和配置 AWS CLI。有关更多信息，请参阅[使用 AWS 命令行界面进行设置](#)。

任务

- 第 1 步：创建 VPC 和子网 (p. 58)
- 第 2 步：使您的子网成为公有子网 (p. 59)
- 第 3 步：在您的子网中启动实例 (p. 61)
- 步骤 4：清除 (p. 62)

第 1 步：创建 VPC 和子网

第一步是创建 VPC 和两个子网。此示例对 VPC 使用 CIDR 块 10.0.0.0/16，但您可以选择其他 CIDR 块。有关更多信息，请参阅[VPC 和子网大小调整 \(p. 78\)](#)。

使用 AWS CLI 创建 VPC 和子网

1. 创建具有 10.0.0.0/16 CIDR 块的 VPC。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

在返回的输出中，记录 VPC ID。

```
{  
    "Vpc": {  
        "VpcId": "vpc-2f09a348",  
        ...  
    }  
}
```

2. 使用上一步中的 VPC ID 创建具有 10.0.1.0/24 CIDR 块的子网。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24
```

3. 在具有 10.0.0.0/24 CIDR 块的 VPC 中创建另一个子网。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24
```

第 2 步：使您的子网成为公有子网

在创建 VPC 和子网后，您可以将 Internet 网关连接到您的 VPC，创建自定义路由表，并为子网配置到 Internet 网关的路由，从而使其中一个子网成为公有子网。

使您的子网成为公有子网

1. 创建 Internet 网关。

```
aws ec2 create-internet-gateway
```

在返回的输出中，记录 Internet 网关 ID。

```
{  
    "InternetGateway": {  
        ...  
        "InternetGatewayId": "igw-1ff7a07b",  
        ...  
    }  
}
```

2. 使用上一步中的 ID 将 Internet 网关连接到您的 VPC。

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-  
id igw-1ff7a07b
```

3. 为您的 VPC 创建自定义路由表。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

在返回的输出中，记录路由表 ID。

```
{  
    "RouteTable": {  
        ...  
        "RouteTableId": "rtb-c1c8faa6",  
        ...  
    }  
}
```

4. 在路由表中创建一个将所有流量 (0.0.0.0/0) 指向 Internet 网关的路由。

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0  
--gateway-id igw-1ff7a07b
```

5. 要确认您的路由已创建并且处于活动状态，您可以描述路由表并查看结果。

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{  
    "RouteTables": [  
        {  
            "Associations": [],  
            "RouteTableId": "rtb-c1c8faa6",  
            "VpcId": "vpc-2f09a348",  
            "PropagatingVgws": [],  
            "Tags": [],  
            "Routes": [  
                {  
                    "GatewayId": "local",  
                    "DestinationCidrBlock": "10.0.0.0/16",  
                    "State": "active",  
                    "Origin": "CreateRouteTable"  
                },  
                {  
                    "GatewayId": "igw-1ff7a07b",  
                    "DestinationCidrBlock": "0.0.0.0/0",  
                    "State": "active",  
                    "Origin": "CreateRoute"  
                }  
            ]  
        }  
    ]  
}
```

6. 路由表当前未与任何子网相关联。您需要将它与您 VPC 中的子网进行关联，以便将来自该子网的流量路由到 Internet 网关。首先，使用 `describe-subnets` 命令获取您的子网 ID。您可以使用 `--filter` 选项仅返回新 VPC 的子网，使用 `--query` 选项仅返回子网 ID 及其 CIDR 块。

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query  
'Subnets[*].{ID:SubnetId,CIDR:CidrBlock}'
```

```
[  
    {  
        "CIDR": "10.0.1.0/24",  
        "ID": "subnet-b46032ec"  
    },  
    {  
        "CIDR": "10.0.0.0/24",  
        "ID": "subnet-a46032fc"  
    }  
]
```

7. 您可以选择将哪个子网与自定义路由表进行关联，例如 `subnet-b46032ec`。此子网将是您的公有子网。

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-  
c1c8faa6
```

8. 您可以选择修改您子网的公有 IP 寻址行为，以便在该子网中启动的实例可自动接收公有 IP 地址。否则，在启动后您应将弹性 IP 地址与您的实例进行关联，以便可从 Internet 访问该实例。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --map-public-ip-on-launch
```

第 3 步：在您的子网中启动实例

要测试您的子网是公有子网并且其中的实例可通过 Internet 访问，请在您的公有子网中启动一个实例，然后连接到该实例。首先，您必须创建一个与您实例进行关联的安全组，以及在您连接到该实例时将使用的密钥对。有关安全组的更多信息，请参阅 [您的 VPC 的安全组 \(p. 119\)](#)。更多有关密钥对的信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 Amazon EC2 密钥对。

在您的公有子网中启动并连接到一个实例

1. 创建一个密钥对，使用 `--query` 选项和 `--output` 文本选项将您的私有密钥通过管道直接发送到扩展名为 `.pem` 的文件中。

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text > MyKeyPair.pem
```

在此示例中，您可以启动 Amazon Linux 实例。如果您在 Linux 或 Mac OS X 操作系统上使用 SSH 客户端连接到您的实例，请使用以下命令设置您的私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 MyKeyPair.pem
```

2. 在您的 VPC 中创建一个安全组，然后添加一个允许从任何地方进行 SSH 访问的规则。

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
    "GroupId": "sg-e1fb8c9a"  
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --protocol tcp --port 22 --cidr 0.0.0.0/0
```

Note

如果使用 `0.0.0.0/0`，则允许所有 IPv4 地址使用 SSH 访问您的实例。对于这个简短练习来说，这是可接受的，但在生产中，请只向特定 IP 地址或地址范围授权。

3. 使用您创建的安全组和密钥对在您的公有子网中启动一个实例。在输出中，记录您实例的实例 ID。

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-b46032ec
```

Note

在此示例中，AMI 是美国东部（弗吉尼亚北部）区域中的 Amazon Linux AMI。如果您在其他区域，您需要适合您区域的 AMI 的 AMI ID。有关更多信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [查找 Linux AMI](#)。

4. 您的实例必须处于 `running` 状态才能连接到该实例。描述您的实例并确认其状态，然后记录其公有 IP 地址。

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{  
    "Reservations": [  
        {  
            ...  
            "Instances": [  
                {  
                    ...  
                    "State": {  
                        "Code": 16,  
                        "Name": "running"  
                    },  
                    ...  
                    "PublicIpAddress": "52.87.168.235",  
                    ...  
                }  
            ]  
        }  
    }  
}
```

5. 当您的实例处于运行状态时，您可以通过使用以下命令，在 Linux 或 Mac OS X 计算机上使用 SSH 客户端连接到该实例：

```
ssh -i "MyKeyPair.pem" ec2-user@52.87.168.235
```

如果您从 Windows 计算机连接，请遵循以下说明：[使用 PuTTY 从 Windows 连接到您的 Linux 实例](#)。

步骤 4：清除

在确认能够连接到您的实例后，如果不再需要该实例，您可以将其终止。要执行此操作，请使用 `terminate-instances` 命令。要删除您在此示例中创建的其他资源，请按列出的顺序使用以下命令：

1. 删除您的安全组：

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

2. 删除您的子网：

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. 删除您的自定义路由表：

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

4. 将您的 Internet 网关与您的 VPC 分离：

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. 删除您的 Internet 网关：

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. 删除您的 VPC：

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

示例：使用 AWS CLI 创建 IPv6 VPC 和子网

以下示例使用 AWS CLI 命令创建具有 IPv6 CIDR 块的非默认 VPC、公有子网和只有出站 Internet 访问权限的私有子网。在您创建了 VPC 和子网后，您可以在公有子网中启动实例，然后连接到该实例。您可以在私有子网中启动实例，并验证其能否连接到 Internet。要开始此操作，您必须首先安装和配置 AWS CLI。有关更多信息，请参阅[使用 AWS 命令行界面进行设置](#)。

任务

- 第 1 步：创建 VPC 和子网 (p. 63)
- 第 2 步：配置公有子网 (p. 64)
- 第 3 步：配置仅出口私有子网 (p. 66)
- 第 4 步：修改子网的 IPv6 寻址行为 (p. 67)
- 第 5 步：在公有子网中启动实例 (p. 67)
- 第 6 步：在私有子网中启动实例 (p. 68)
- 步骤 7：清除 (p. 70)

第 1 步：创建 VPC 和子网

第一步是创建 VPC 和两个子网。此示例对 VPC 使用 IPv4 CIDR 块 10.0.0.0/16，但您可以选择其他 CIDR 块。有关更多信息，请参阅[VPC 和子网大小调整 \(p. 78\)](#)。

使用 AWS CLI 创建 VPC 和子网

1. 创建具有 10.0.0.0/16 CIDR 块的 VPC，并向此 VPC 关联 IPv6 CIDR 块。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
```

在返回的输出中，记录 VPC ID。

```
{  
    "vpc": {  
        "VpcId": "vpc-2f09a348",  
        ...  
    }  
}
```

2. 描述您的 VPC 以获取与 VPC 关联的 IPv6 CIDR 块。

```
aws ec2 describe-vpcs --vpc-id vpc-2f09a348
```

```
{  
    "vpcs": [  
        {  
            ...  
            "Ipv6CidrBlockAssociationSet": [  
                {  
                    ...  
                }  
            ]  
        }  
    ]  
}
```

```
        "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
        "AssociationId": "vpc-cidr-assoc-17a5407e",
        "Ipv6CidrBlockState": {
            "State": "ASSOCIATED"
        }
    ],
    ...
}
```

3. (从上一步中返回的范围) 创建具有 10.0.0.0/24 IPv4 CIDR 块和 2001:db8:1234:1a00::/64 IPv6 CIDR 块的子网。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24 --ipv6-cidr-block 2001:db8:1234:1a00::/64
```

4. 在 VPC 中创建第二个具有 10.0.1.0/24 IPv4 CIDR 块和 2001:db8:1234:1a01::/64 IPv6 CIDR 块的子网。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24 --ipv6-cidr-block 2001:db8:1234:1a01::/64
```

第 2 步：配置公有子网

在创建 VPC 和子网后，您可以将 Internet 网关连接到您的 VPC，创建自定义路由表，并为子网配置到 Internet 网关的路由，从而使其中一个子网成为公有子网。此示例创建一个将所有 IPv4 流量和 IPv6 流量路由到 Internet 网关的路由表。

使您的子网成为公有子网

1. 创建 Internet 网关。

```
aws ec2 create-internet-gateway
```

在返回的输出中，记录 Internet 网关 ID。

```
{
    "InternetGateway": {
        ...
        "InternetGatewayId": "igw-1ff7a07b",
        ...
    }
}
```

2. 使用上一步中的 ID 将 Internet 网关连接到您的 VPC。

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-id igw-1ff7a07b
```

3. 为您的 VPC 创建自定义路由表。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

在返回的输出中，记录路由表 ID。

```
{
```

```
"RouteTable": {  
    ...  
    "RouteTableId": "rtb-c1c8faa6",  
    ...  
}  
}
```

4. 在路由表中创建一个将所有 IPv6 流量 (::/0) 指向 Internet 网关的路由。

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-ipv6-cidr-block ::/0  
--gateway-id igw-1ff7a07b
```

Note

如果要将公有子网用于 IPv4 流量，则需要再添加一个用于指向 Internet 网关的 0.0.0.0/0 流量的路由。

5. 要确认您的路由已创建并且处于活动状态，您可以描述路由表并查看结果。

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{  
    "RouteTables": [  
        {  
            "Associations": [],  
            "RouteTableId": "rtb-c1c8faa6",  
            "VpcId": "vpc-2f09a348",  
            "PropagatingVgws": [],  
            "Tags": [],  
            "Routes": [  
                {  
                    "GatewayId": "local",  
                    "DestinationCidrBlock": "10.0.0.0/16",  
                    "State": "active",  
                    "Origin": "CreateRouteTable"  
                },  
                {  
                    "GatewayId": "local",  
                    "Origin": "CreateRouteTable",  
                    "State": "active",  
                    "DestinationIpv6CidrBlock": "2001:db8:1234:1a00::/56"  
                },  
                {  
                    "GatewayId": "igw-1ff7a07b",  
                    "Origin": "CreateRoute",  
                    "State": "active",  
                    "DestinationIpv6CidrBlock": "::/0"  
                }  
            ]  
        }  
    ]  
}
```

6. 路由表当前未与任何子网相关联。将它与您 VPC 中的子网进行关联，以便将来自该子网的流量路由到 Internet 网关。首先，描述您的子网，以便获得它们的 ID。您可以使用 --filter 选项仅返回新 VPC 的子网，使用 --query 选项仅返回子网 ID 及其 IPv4 和 IPv6 CIDR 块。

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query  
'Subnets[*].  
{ID:SubnetId,IPv4CIDR:CidrBlock,IPv6CIDR:Ipv6CidrBlockAssociationSet[*].Ipv6CidrBlock}'
```

```
[  
  {  
    "IPv6CIDR": [  
      "2001:db8:1234:1a00::/64"  
    ],  
    "ID": "subnet-b46032ec",  
    "IPv4CIDR": "10.0.0.0/24"  
  },  
  {  
    "IPv6CIDR": [  
      "2001:db8:1234:1a01::/64"  
    ],  
    "ID": "subnet-a46032fc",  
    "IPv4CIDR": "10.0.1.0/24"  
  }  
]
```

7. 您可以选择将哪个子网与自定义路由表进行关联，例如 subnet-b46032ec。此子网将是您的公有子网。

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-c1c8faa6
```

第 3 步：配置仅出口私有子网

您可以将 VPC 中的第二个子网配置为 IPv6 仅出口私有子网。在此子网中启动的实例能够通过仅出口 Internet 网关经由 IPv6 访问 Internet (如获取软件更新)，但 Internet 上的主机无法访问您的实例。

使子网成为仅出口私有子网

1. 为您的 VPC 创建仅出口 Internet 网关。在返回的输出中，记录网关 ID。

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-2f09a348
```

```
{  
  "EgressOnlyInternetGateway": {  
    "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",  
    "Attachments": [  
      {  
        "State": "attached",  
        "VpcId": "vpc-2f09a348"  
      }  
    ]  
  }  
}
```

2. 为您的 VPC 创建自定义路由表。在返回的输出中，记录路由表 ID。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

3. 在路由表中创建一个将所有 IPv6 流量 (::/0) 指向仅出口 Internet 网关的路由。

```
aws ec2 create-route --route-table-id rtb-abc123ab --destination-ipv6-cidr-block ::/0  
--egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

4. 将路由表与 VPC 中的第二个子网 (上一节描述的子网) 关联。此子网将成为具有仅出口 IPv6 Internet 访问权限的私有子网。

```
aws ec2 associate-route-table --subnet-id subnet-a46032fc --route-table-id rtb-abc123ab
```

第 4 步：修改子网的 IPv6 寻址行为

您可以修改子网的公有 IP 寻址行为，以便在子网中启动的实例能够自动接收 IPv6 地址。当您在子网中启动实例时，系统将子网范围中的一个 IPv6 地址分配给该实例的主网络接口 (eth0)。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --assign-ipv6-address-on-creation
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-a46032fc --assign-ipv6-address-on-creation
```

第 5 步：在公有子网中启动实例

要测试您的公有子网是公有子网并且其中的实例可通过 Internet 访问，请在您的公有子网中启动一个实例，然后连接到该实例。首先，您必须创建一个与您实例进行关联的安全组，以及在您连接到该实例时将使用的密钥对。有关安全组的更多信息，请参阅 [您的 VPC 的安全组 \(p. 119\)](#)。更多有关密钥对的信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 Amazon EC2 密钥对。

在您的公有子网中启动并连接到一个实例

1. 创建一个密钥对，使用 `--query` 选项和 `--output` 文本选项将您的私有密钥通过管道直接发送到扩展名为 .pem 的文件中。

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text > MyKeyPair.pem
```

在此示例中，启动 Amazon Linux 实例。如果您在 Linux 或 OS X 操作系统上使用 SSH 客户端连接到您的实例，请使用以下命令设置您的私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 MyKeyPair.pem
```

2. 为您的 VPC 创建一个安全组，然后添加一个允许从任意 IPv6 地址进行 SSH 访问的规则。

```
aws ec2 create-security-group --group-name SSHAcess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
    "GroupId": "sg-e1fb8c9a"  
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --ip-permissions '[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6": "::/0"}]}]
```

Note

如果使用 `::/0`，则可以允许所有 IPv6 地址使用 SSH 访问您的实例。对于这个简短的练习来说这是可接受的，但在生产中，仅授权特定 IP 地址或地址范围访问您的实例。

3. 使用您创建的安全组和密钥对在您的公有子网中启动一个实例。在输出中，记录您实例的实例 ID。

```
aws ec2 run-instances --image-id ami-0de53d8956e8dcf80 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-b46032ec
```

Note

在此示例中，AMI 是美国东部（弗吉尼亚北部）区域中的 Amazon Linux AMI。如果您在其他区域，则需要适合您区域的 AMI 的 AMI ID。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[查找 Linux AMI](#)。

4. 您的实例必须处于 running 状态才能连接到该实例。描述您的实例并确认其状态，然后记录其 IPv6 地址。

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{
    "Reservations": [
        {
            ...
            "Instances": [
                {
                    ...
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    ...
                    "NetworkInterfaces": [
                        {
                            "Ipv6Addresses": [
                                {
                                    "Ipv6Address": "2001:db8:1234:1a00::123"
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    }
}
```

5. 当您的实例处于运行状态时，您可以通过使用以下命令，在 Linux 或 OS X 计算机上使用 SSH 客户端连接到该实例。您的本地计算机必须已配置 IPv6 地址。

```
ssh -i "MyKeyPair.pem" ec2-user@2001:db8:1234:1a00::123
```

如果您从 Windows 计算机连接，请遵循以下说明：[使用 PuTTY 从 Windows 连接到您的 Linux 实例](#)。

第 6 步：在私有子网中启动实例

要测试仅出口私有子网中的实例能否访问 Internet，请在私有子网中启动一个实例，并使用公有子网中的堡垒实例连接该实例（可以使用在上节中启动的实例）。首先，您必须为此实例创建安全组。此安全组必须具有允许您的堡垒实例使用 SSH 进行连接的规则，以及允许使用 ping6 命令（ICMPv6 流量）来确保实例不能从 Internet 访问的规则。

1. 在 VPC 中创建一个安全组，并添加允许从公有子网中实例的 IPv6 地址进行入站 SSH 访问的规则以及允许所有 ICMPv6 流量的规则：

```
aws ec2 create-security-group --group-name SSHAccessRestricted --description "Security group for SSH access from bastion" --vpc-id vpc-2f09a348
```

```
{  
    "GroupId": "sg-aabb1122"  
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions '[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6": "2001:db8:1234:1a00::123/128"}]}'
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions '[{"IpProtocol": "58", "FromPort": -1, "ToPort": -1, "Ipv6Ranges": [{"CidrIpv6": "::/0"}]}'
```

2. 使用您创建的安全组和用于在公有子网中启动实例的密钥对在私有子网中启动一个实例。

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-aabb1122 --subnet-id subnet-a46032fc
```

使用 `describe-instances` 命令验证您的实例正在运行并获取其 IPv6 地址。

3. 在本地计算机上配置 SSH 代理转发，然后连接到公有子网中的实例。对于 Linux，请使用以下命令：

```
ssh-add MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

对于 OS X，请使用以下命令：

```
ssh-add -K MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

对于 Windows，请使用以下说明：[针对 Windows \(PuTTY\) 配置 SSH 代理转发 \(p. 205\)](#)。使用 IPv6 地址连接公有子网中的实例。

4. 从公有子网中的实例（堡垒实例），使用 IPv6 地址连接私有子网中的实例：

```
ssh ec2-user@2001:db8:1234:1a01::456
```

5. 从私有实例，通过对启用了 ICMP 的网站运行 `ping6` 命令来测试是否可以连接到 Internet，例如：

```
ping6 -n ietf.org
```

```
PING ietf.org(2001:1900:3001:11::2c) 56 data bytes  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=1 ttl=46 time=73.9 ms  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=2 ttl=46 time=73.8 ms  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=3 ttl=46 time=73.9 ms  
...
```

6. 要测试 Internet 上的主机能否访问私有子网中的实例，请在启用 IPv6 的计算机上使用 ping6 命令。您应收到超时响应。如果您获得有效响应，则可从 Internet 访问您的实例 — 检查与私有子网关联的路由表，并验证此表是否没有针对流入 Internet 网关的 IPv6 流量的路由。

```
ping6 2001:db8:1234:1a01::456
```

步骤 7：清除

在验证您可以连接到公有子网中的实例，并且私有子网中的实例能够访问 Internet 后，如果不再需要这些实例，可将其终止。要执行此操作，请使用 [terminate-instances](#) 命令。要删除您在此示例中创建的其他资源，请按列出的顺序使用以下命令：

1. 删除您的安全组：

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

```
aws ec2 delete-security-group --group-id sg-aabb1122
```

2. 删除您的子网：

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. 删除您的自定义路由表：

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

```
aws ec2 delete-route-table --route-table-id rtb-abc123ab
```

4. 将您的 Internet 网关与您的 VPC 分离：

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. 删除您的 Internet 网关：

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. 删除您的仅出口 Internet 网关：

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigo-015e0e244e24dfe8a
```

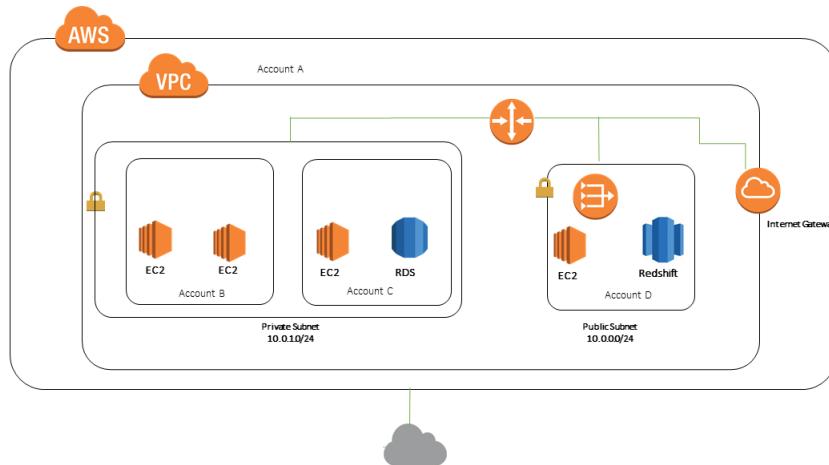
7. 删除您的 VPC：

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

示例：共享公有子网和私有子网

考虑这样一个方案：您想让一个账户负责基础设施，包括子网、路由表、网关和 CIDR 范围以及在同一个 AWS 组织中使用子网的其他账户。VPC 所有者（账户 A）创建路由基础设施，包括 VPC、子网、路由表、网关和网络 ACL。账户 D 想要创建面向公众的应用程序。账户 B 和账户 C 想要创建不需要连接到互联网且应该驻留在私有子网中的私有应用程序。账户 A 可以使用 AWS Resource Access Manager 为子网创建资源共享，然后共享子网。账户 A 与账户 D 共享公有子网，并与账户 B 和账户 C 共享私有子网。账户 B、账户 C 和账户 D 可以在子网中创建资源。每个账户只能看到与其共享的子网，例如，账户 D 只能看到公有子网。每个账户都可以控制其资源，包括实例和安全组。

账户 A 管理 IP 基础设施，包括公有子网和私有子网的路由表。共享子网不需要额外的配置，因此，其路由表与非共享子网路由表相同。



账户 A (账户 ID 111111111111) 与账户 D (444444444444) 共享私有子网。账户 D 看到下列子网，所有者列提供两个表明子网被共享的指标。

- 账户 ID 是 VPC 所有者 (111111111111)，因此不同于账户 D 的 ID (4444444444)。
- “共享”一词出现在所有者账户 ID 旁边。

Create subnet Actions									
Name		Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Route table	Default subnet	Owner
<input type="checkbox"/>	subnet-0bb1c79de301436ee	available	vpc-0ee975135d74bdce		10.0.2.0/24	251	rtb-0825a8caf09467ea8	No	111111111111 (\$)
<input type="checkbox"/>	subnet-0fe673ef5bd459924	available	vpc-0ee975135d74bdce		10.0.1.0/24	251	rtb-0825a8caf09467ea8	No	111111111111 (\$)

示例：使用 AWS PrivateLink 和 VPC 对等连接的服务

AWS PrivateLink 服务提供商配置在其 VPC 中运行服务的实例，并以网络负载均衡器为前端。将区域内 VPC 对等连接（VPC 在同一区域中）和区域间 VPC 对等连接（VPC 在不同的区域中）与 AWS PrivateLink 结合使用可允许对使用者进行私有访问。

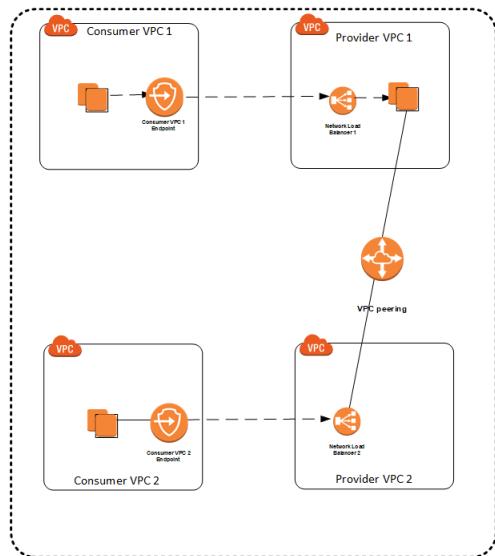
服务使用者或服务提供商可以完成配置。有关更多信息，请参阅以下示例。

示例

- [示例：服务提供商配置服务 \(p. 72\)](#)
- [示例：服务使用者配置访问 \(p. 72\)](#)
- [示例：服务提供商将服务配置为跨区域 \(p. 73\)](#)
- [示例：服务使用者配置跨区域访问 \(p. 74\)](#)

示例：服务提供商配置服务

考虑下面的例子，其中一个服务在提供商 VPC 1 中的实例上运行。使用者 VPC 1 中的资源可以通过使用者 VPC 1 中的 AWS PrivateLink VPC 终端节点进行访问。

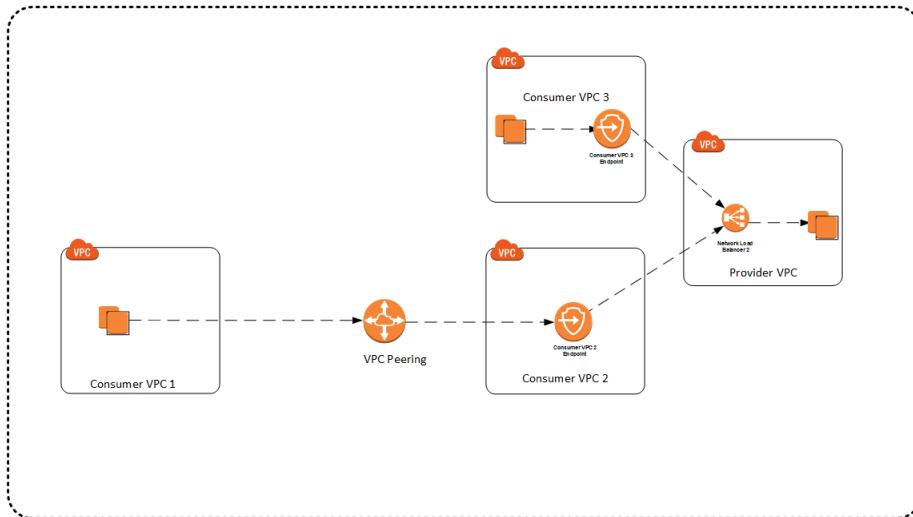


要允许使用者 VPC 2 中的资源私下访问该服务，服务提供商必须完成以下步骤：

1. 创建提供商 VPC 2。
2. 在提供商 VPC 1 和提供商 VPC 2 之间配置 VPC 对等，以便可以在两个 VPC 之间路由流量。
3. 在提供商 VPC 2 中创建网络负载平衡器 2。
4. 在网络负载平衡器 2 上配置目标组，指向 VPC 1 中服务实例的 IP 地址。
5. 调整与提供商 VPC 1 中的服务实例关联的安全组，使之允许来自网络负载平衡器 2 的流量。
6. 在提供商 VPC 2 中创建一个 VPC 终端节点服务配置，并将其与网络负载平衡器 2 关联。

示例：服务使用者配置访问

考虑下面的例子，其中一个服务在提供商 VPC 中的实例上运行。使用者 VPC 3 中的资源可以通过使用者 VPC 3 中的 AWS PrivateLink VPC 终端节点服务直接访问该服务。

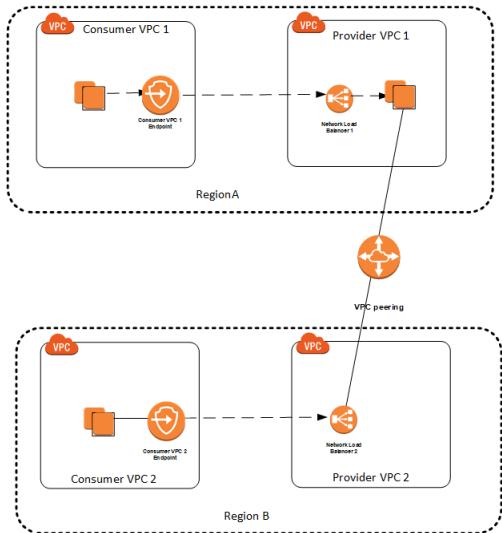


为了允许使用者 VPC 1 中的资源私有访问该服务，服务使用者必须完成以下步骤：

1. 创建使用者 VPC 2。
2. 创建跨越使用者 VPC 2 中一个或多个子网的 VPC 终端节点。
3. 调整与使用者 VPC 2 中的 VPC 终端节点服务关联的安全组，使之允许来自使用者 VPC 1 中实例的流量。调整与使用者 VPC 1 中的实例关联的安全组，使之允许流向使用者 VPC 2 中 VPC 终端节点服务的流量。
4. 在使用者 VPC 1 和使用者 VPC 2 之间配置 VPC 对等，以便在两个 VPC 之间路由流量。

示例：服务提供商将服务配置为跨区域

考虑下面的例子，其中一个服务在区域 A（例如 us-east-1 区域）提供商 VPC 1 中的实例上运行。在同一个区域的使用者 VPC 1 中的资源可以通过使用者 VPC 1 中的 AWS PrivateLink VPC 终端节点直接访问该服务。



为了允许区域 B（例如，eu-west-1 区域）中的使用者 VPC 2 中的资源私有访问该服务，服务提供商必须完成以下步骤：

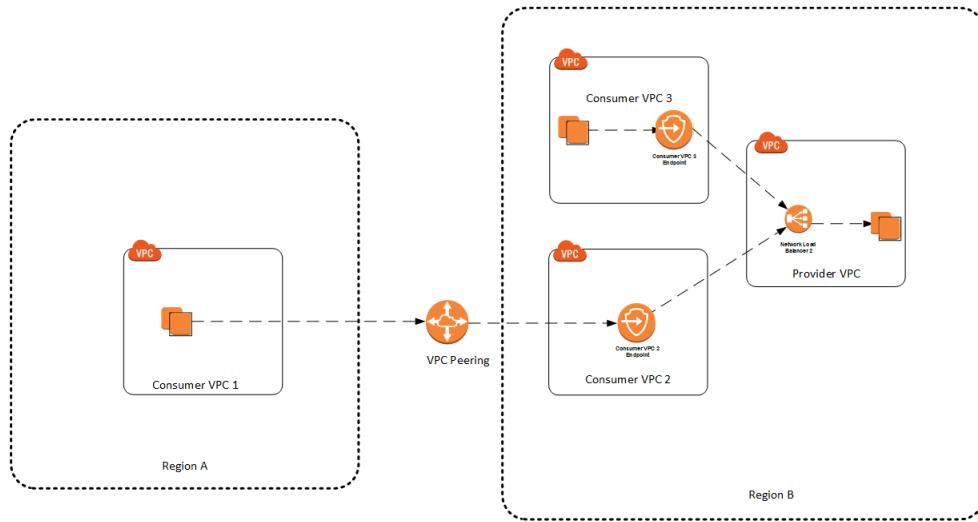
1. 在区域 B 中创建提供商 VPC 2。

2. 在提供商 VPC 1 和提供商 VPC 2 之间配置 VPC 区域间对等，以便可以在两个 VPC 之间路由流量。
3. 在提供商 VPC 2 中创建网络负载平衡器 2。
4. 在网络负载平衡器 2 上配置目标组，指向 VPC 1 中服务实例的 IP 地址。
5. 调整与提供商 VPC 1 中的服务实例关联的安全组，使之允许来自网络负载平衡器 2 的流量。
6. 在提供商 VPC 2 中创建一个 VPC 终端节点服务配置，并将其与网络负载平衡器 2 关联。

提供商 2 账户发生区域间对等数据传输费用、网络负载均衡器费用。提供商 1 账户发生服务实例费用。

示例：服务使用者配置跨区域访问

考虑下面的例子，其中一个服务在区域 A（例如 us-east-1 区域）提供商 VPC 中的实例上运行。使用者 VPC 3 中的资源可以通过使用者 VPC 3 中的 AWS PrivateLink VPC 终端节点服务直接访问该服务。



为了允许使用者 VPC 1 中的资源私有访问该服务，服务使用者必须完成以下步骤：

1. 在区域 B 中创建使用者 VPC 2。
2. 创建跨越使用者 VPC 2 中一个或多个子网的 VPC 终端节点点。
3. 调整与使用者 VPC 2 中的 VPC 终端节点服务关联的安全组，使之允许来自使用者 VPC 1 中实例的流量。调整与使用者 VPC 1 中的实例关联的安全组，使之允许流向使用者 VPC 2 中 VPC 终端节点服务的流量。
4. 在使用者 VPC 1 和使用者 VPC 2 之间配置 VPC 区域间对等，以便在两个 VPC 之间路由流量。

完成配置后，使用者 VPC 1 即可私有访问该服务。

使用者账户发生区域间对等数据传输费用、VPC 终端节点数据处理费用和 VPC 终端节点每小时费用。提供商账户发生网络负载均衡器费用和服务实例费用。

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 Amazon VPC 的一般概述 , 请参阅[什么是 Amazon VPC ? \(p. 1\)](#)。

内容

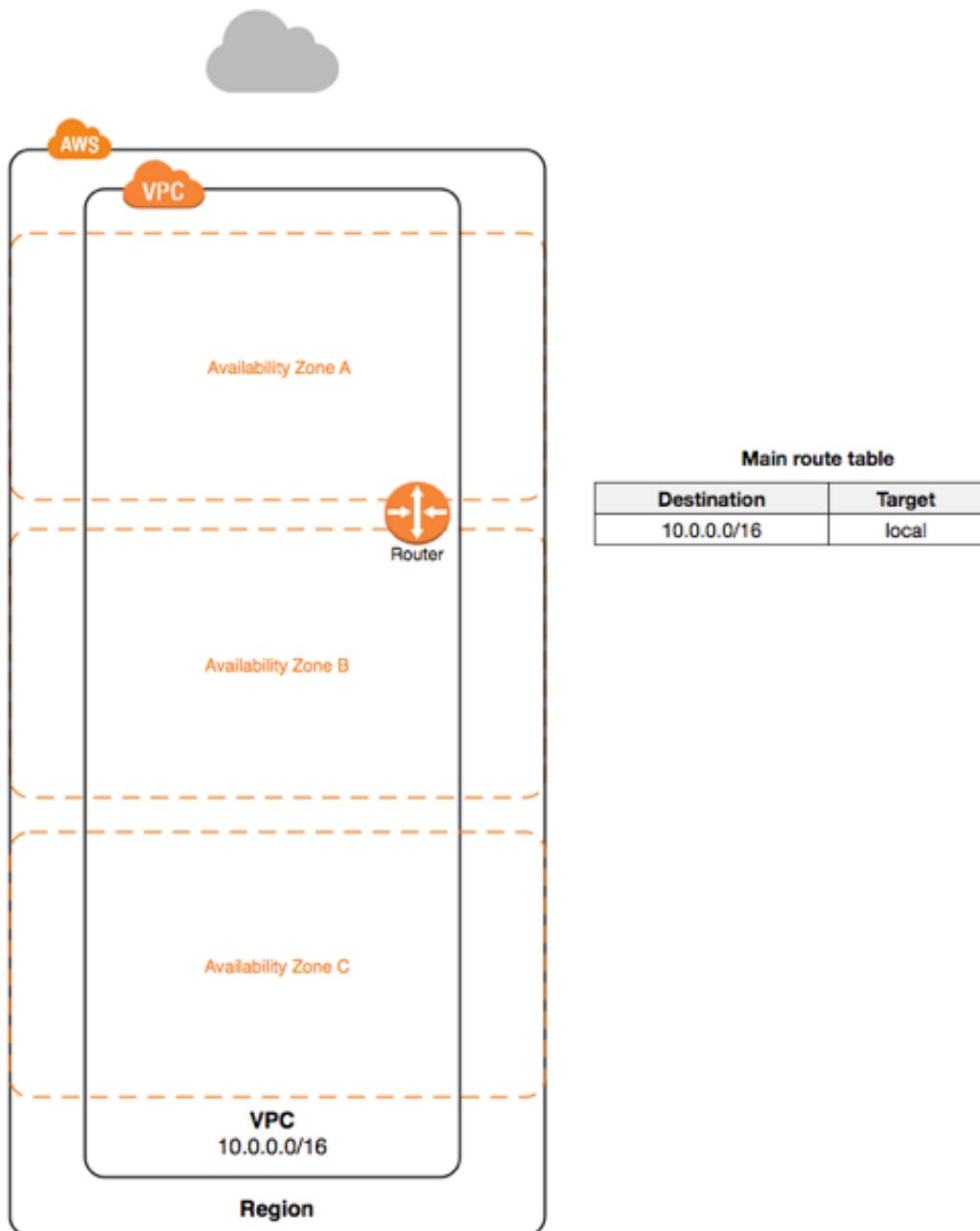
- [VPC 和子网基础知识 \(p. 75\)](#)
- [VPC 和子网大小调整 \(p. 78\)](#)
- [子网路由 \(p. 82\)](#)
- [子网安全性 \(p. 82\)](#)
- [与本地网络和其他 VPC 的连接 \(p. 83\)](#)
- [使用 VPC 和子网 \(p. 83\)](#)
- [使用共享 VPC \(p. 89\)](#)

VPC 和子网基础知识

Virtual Private Cloud (VPC) 是仅适用于您的 AWS 账户的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔绝。可在 VPC 中启动 AWS 资源 , 如 Amazon EC2 实例。

在创建 VPC 时 , 您必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围 ; 例如 , 10.0.0.0/16。这是您的 VPC 的主要 CIDR 块。有关 CIDR 表示法的更多信息 , 请参阅[RFC 4632](#)。

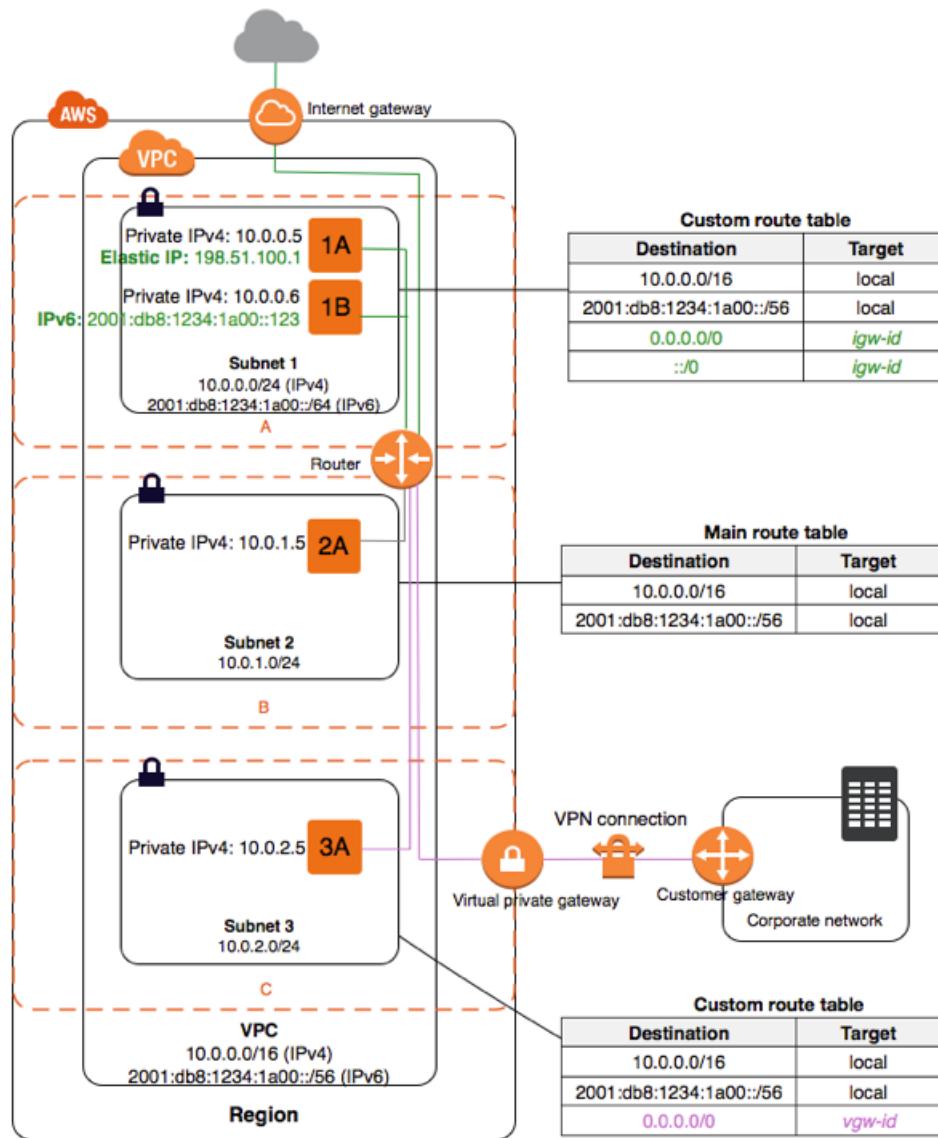
下图显示了具有 IPv4 CIDR 块的新 VPC 及主路由表。



VPC 跨越区域中的所有可用区。在创建 VPC 之后，您可以在每个可用区中添加一个或多个子网。在创建子网时，指定子网的 CIDR 块，它是 VPC CIDR 块的子集。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。可用区是被设计为可以隔离其他可用区的故障的不同位置。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。我们为每个子网指定一个唯一 ID。

您还可以选择为 VPC 及子网分配 IPv6 CIDR 块。

下图展示了一个在多个可用区内配置子网的 VPC。1A、1B、2A 和 3A 是 VPC 中的实例。此 VPC 以及子网 1 各自关联了一个 IPv6 CIDR 块。Internet 网关允许在 Internet 上通信，虚拟专用网络 (VPN) 连接可实现与您公司网络的通信。



如果一个子网的流量被路由到 Internet 网关，这个子网便是公有子网。在此图中，子网 1 是公有子网。如果您希望公有子网中的实例通过 IPv4 与 Internet 通信，则它必须具有公有 IPv4 地址或弹性 IP 地址 (IPv4)。有关公有 IPv4 地址的更多信息，请参阅[公有 IPv4 地址 \(p. 101\)](#)。如果您希望公有子网中的实例通过 IPv6 与 Internet 进行通信，则它必须具有 IPv6 地址。

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。在此图中，子网 2 是私有子网。

如果一个子网没有通向 Internet 网关的路由，但其流量会被路由到虚拟专用网关进行 Site-to-Site VPN 连接，这个子网便是仅限 VPN 子网。在此图中，子网 3 是仅限 VPN 的子网。目前，我们不支持通过 Site-to-Site VPN 连接的 IPv6 流量。

有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的[场景和示例 \(p. 23\)](#)、[Internet 网关 \(p. 192\)](#)以及[什么是 AWS Site-to-Site VPN ?](#)

Note

无论子网是哪种类型，子网的内部 IPv4 地址范围始终是私有的，我们不会将该地址块发布到 Internet。

您可以在自己的账户中创建的 VPC 和子网存在数量限制。有关更多信息，请参阅 [Amazon VPC 限制 \(p. 276\)](#)。

VPC 和子网大小调整

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

有关 IP 地址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

内容

- [针对 IPv4 的 VPC 和子网大小调整 \(p. 78\)](#)
- [向 VPC 中添加 IPv4 CIDR 块 \(p. 79\)](#)
- [针对 IPv6 的 VPC 和子网大小调整 \(p. 81\)](#)

针对 IPv4 的 VPC 和子网大小调整

当您创建 VPC 时，必须为这个 VPC 指定 IPv4 CIDR 块。允许的块大小介于 /16 网络掩码 (65,536 个 IP 地址) 和 /28 网络掩码 (16 个 IP 地址) 之间。在创建 VPC 后，您可以将辅助 CIDR 块与 VPC 关联。有关更多信息，请参阅 [向 VPC 中添加 IPv4 CIDR 块 \(p. 79\)](#)。

在创建 VPC 时，建议您指定来自私有 IPv4 地址范围 (如 /16 RFC 1918 所指定) 的 CIDR 块 (小于或等于)：

- 10.0.0.0 – 10.255.255.255 (10/8 前缀)
- 172.16.0.0 – 172.31.255.255 (172.16/12 前缀)
- 192.168.0.0 – 192.168.255.255 (192.168/16 前缀)

您可以创建一个具有公共可路由的 CIDR 块 (不在 RFC 1918 中指定的私有 IPv4 地址范围内) 的 VPC；但是，在本文档中，我们的私有 IP 地址指的是位于 VPC 的 CIDR 范围内的 IPv4 地址。

Note

如果您要创建用于其他 AWS 服务的 VPC，请参阅服务文档以验证对 IP 地址范围和联网组件是否有特定要求。

子网的 CIDR 块可以与 VPC 的 CIDR 块 (适用于 VPC 中的单一子网) 或 VPC 的 CIDR 块的子网 (适用于多个子网) 相同。允许的块大小在 /28 网络掩码与 /16 网络掩码之间。如果您在 VPC 中创建多个子网，子网的 CIDR 块不能重叠。

例如，如果创建其 CIDR 块为 10.0.0.0/24 的 VPC，则它支持 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 (对于地址 10.0.0.0 – 10.0.0.127)，另一个子网使用 CIDR 块 10.0.0.128/25 (对于地址 10.0.0.128 – 10.0.0.255)。

许多工具可帮助您计算子网 CIDR 块；例如，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。

每个子网 CIDR 块中的前四个 IP 地址和最后一个 IP 地址无法供您使用，而且无法分配到一个实例。例如，在具有 CIDR 块 10.0.0.0/24 的子网中，以下五个 IP 地址是保留的：

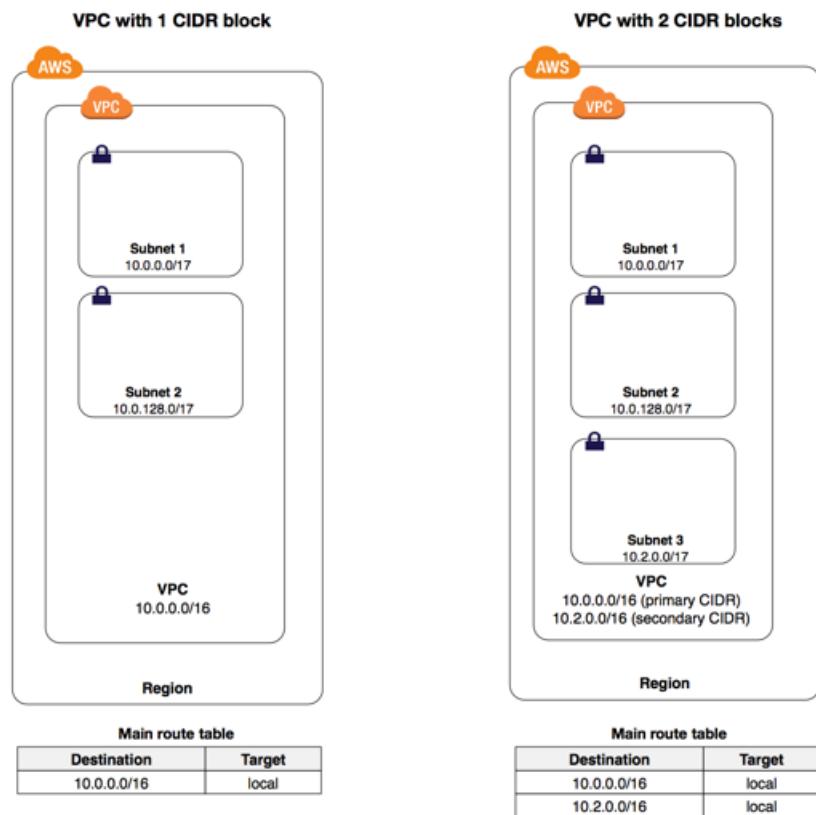
- 10.0.0.0：网络地址。
- 10.0.0.1：由 AWS 保留，用于 VPC 路由器。

- 10.0.0.2：由 AWS 保留。DNS 服务器的 IP 地址始终为 VPC 网络范围的基址 + 2；但是，我们也保留了每个子网范围基址 + 2 的 IP 地址。对于包含多个 CIDR 块的 VPC，DNS 服务器的 IP 地址位于主要 CIDR 中。有关更多信息，请参阅[Amazon DNS 服务器 \(p. 225\)](#)。
- 10.0.0.3：由 AWS 保留，供将来使用。
- 10.0.0.255：网络广播地址。我们在 VPC 中不支持广播，因此我们会保留此地址。

向 VPC 中添加 IPv4 CIDR 块

您可以将辅助 IPv4 CIDR 块与 VPC 关联。当您将 CIDR 块与 VPC 关联时，路由会自动添加到 VPC 路由表中，以便在 VPC 中启用路由（目的地是 CIDR 块，目标是 local。）

在以下示例中，左侧的 VPC 有一个 CIDR 块（10.0.0.0/16）和两个子网。在您添加第二个 CIDR 块（10.2.0.0/16）并从第二个 CIDR 的范围创建新的子网后，右侧的 VPC 表示同一 VPC 的架构。



要将 CIDR 块添加到 VPC，应遵循以下规则：

- 允许的块大小在 /28 网络掩码与 /16 网络掩码之间。
- 该 CIDR 块不得与 VPC 所关联的任何现有 CIDR 块重叠。
- 您可以使用的 IPv4 地址范围是有限制的。有关更多信息，请参阅[IPv4 CIDR 块关联限制 \(p. 80\)](#)。
- 您不能增加或减少现有 CIDR 块的大小。
- 可以与 VPC 关联的 CIDR 块数和可以添加到路由表的路由数是有限制的。如果这导致您超出限制，您就不能关联 CIDR 块。有关更多信息，请参阅[Amazon VPC 限制 \(p. 276\)](#)。
- CIDR 块不得与任何 VPC 路由表中的路由的 CIDR 范围相同或大于该范围。例如，如果您拥有一个通向虚拟专用网关、目的地为 10.0.0.0/24 的路由，则您不能关联相同范围或更大范围的 CIDR 块。但是，您可以关联 10.0.0.0/25 或更小的 CIDR 块。

- 如果您为 ClassicLink 启用了 VPC，则可以关联 10.0.0.0/16 和 10.1.0.0/16 范围中的 CIDR 块，但不能关联 10.0.0.0/8 范围中的任何其他 CIDR 块。
- 在向作为 VPC 对等连接的一部分的 VPC 中添加 IPv4 CIDR 块时，应遵循以下规则：
 - 如果 VPC 对等连接为 `active`，则可以向 VPC 中添加 CIDR 块，条件是这些块不与对等 VPC 的 CIDR 块重叠。
 - 如果 VPC 对等连接为 `pending-acceptance`，则请求方 VPC 的所有者不能向 VPC 中添加任何 CIDR 块，无论它是否与接受方 VPC 的 CIDR 块重叠。要么接受方 VPC 的所有者必须接受对等连接，要么请求方 VPC 的所有者必须删除 VPC 对等连接请求，添加 CIDR 块，然后请求新的 VPC 对等连接。
 - 如果 VPC 对等连接为 `pending-acceptance`，则接受方 VPC 的所有者可以向 VPC 中添加 CIDR 块。如果辅助 CIDR 块与请求方 VPC 的 CIDR 块重叠，则 VPC 对等连接请求将失败，无法被接受。
- 如果您使用 AWS Direct Connect 来通过 Direct Connect 网关连接到多个 VPC，则与 Direct Connect 网关关联的 VPC 不得具有重叠的 CIDR 块。如果您将 CIDR 块连接到其中一个与 Direct Connect 网关关联的 VPC，请确保新的 CIDR 块不会与任何其他关联 VPC 的现有 CIDR 块重叠。有关更多信息，请参阅 AWS Direct Connect 用户指南 中的 [Direct Connect 网关](#)。
- 在添加或删除 CIDR 块时，它会经历不同的状态：`associating | associated | disassociating | disassociated | failing | failed`。当 CIDR 块处于 `associated` 状态时，表示它已准备就绪，可供您使用。

下表提供了允许和受限的 CIDR 块关联的概述，是允许还是受限取决于 VPC 的主要 CIDR 块所在的 IPv4 地址范围。

IPv4 CIDR 块关联限制

主要 VPC CIDR 块所在的 IP 地址范围	受限的 CIDR 块关联	允许的 CIDR 块关联
10.0.0.0/8	其他 RFC 1918* 范围 (172.16.0.0/12 和 192.168.0.0/16) 中的 CIDR 块 如果您的主要 CIDR 位于 10.0.0.0/15 范围内，则不能添加 10.0.0.0/16 范围中的 CIDR 块。 198.19.0.0/16 范围中的 CIDR 块。	10.0.0.0/8 范围中任何其他不受限的 CIDR。 任何可公开路由的 IPv4 CIDR 块 (非 RFC 1918)，或 100.64.0.0/10 范围中的 CIDR 块。
172.16.0.0/12	其他 RFC 1918* 范围 (10.0.0.0/8 和 192.168.0.0/16) 中的 CIDR 块 172.31.0.0/16 范围中的 CIDR 块。 198.19.0.0/16 范围中的 CIDR 块。	172.16.0.0/12 范围中任何其他不受限的 CIDR。 任何可公开路由的 IPv4 CIDR 块 (非 RFC 1918)，或 100.64.0.0/10 范围中的 CIDR 块。
192.168.0.0/16	其他 RFC 1918* 范围 (172.16.0.0/12 和 10.0.0.0/8) 中的 CIDR 块 198.19.0.0/16 范围中的 CIDR 块。	192.168.0.0/16 范围中的任何其他 CIDR。 任何可公开路由的 IPv4 CIDR 块 (非 RFC 1918)，或 100.64.0.0/10 范围中的 CIDR 块。
198.19.0.0/16	RFC 1918* 范围中的 CIDR 块。	任何可公开路由的 IPv4 CIDR 块 (非 RFC 1918)，或 100.64.0.0/10 范围中的 CIDR 块。

主要 VPC CIDR 块所在的 IP 地址范围	受限的 CIDR 块关联	允许的 CIDR 块关联
可公开路由的 CIDR 块 (非 RFC 1918) , 或 100.64.0.0/10 范围中的 CIDR 块。	RFC 1918* 范围中的 CIDR 块。 198.19.0.0/16 范围中的 CIDR 块。	任何其他可公开路由的 IPv4 CIDR 块 (非 RFC 1918) , 或 100.64.0.0/10 范围中的 CIDR 块。

*RFC 1918 范围是在 [RFC 1918](#) 中指定的私有 IPv4 地址范围。

您可以取消与 VPC 相关联的 CIDR 块的关联，但无法取消最初用于创建 VPC 的 CIDR 块 (主要 CIDR 块) 的关联。要在 Amazon VPC 控制台中查看 VPC 的主要 CIDR，请选择您的 VPC，然后选择您的 VPC，并记下 CIDR 块下面的第一个条目。或者，您可以使用 [describe-vpcs](#) 命令：

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d
```

在返回的输出中，主要 CIDR 在顶层 CidrBlock 元素中返回 (下面的示例输出中的倒数第二个元素)。

```
{
    "Vpcs": [
        {
            "VpcId": "vpc-1a2b3c4d",
            "InstanceTenancy": "default",
            "Tags": [
                {
                    "Value": "MyVPC",
                    "Key": "Name"
                }
            ],
            "CidrBlockAssociations": [
                {
                    "AssociationId": "vpc-cidr-assoc-3781aa5e",
                    "CidrBlock": "10.0.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                },
                {
                    "AssociationId": "vpc-cidr-assoc-0280ab6b",
                    "CidrBlock": "10.2.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "State": "available",
            "DhcpOptionsId": "dopt-e0fe0e88",
            "CidrBlock": "10.0.0.0/16",
            "IsDefault": false
        }
    ]
}
```

针对 IPv6 的 VPC 和子网大小调整

您可以向自己账户中的现有 VPC 关联一个 IPv6 CIDR 块，或在创建新 VPC 时执行此操作。CIDR 块使用 /56 的固定前缀长度。您无法选择地址范围或 IPv6 CIDR 块大小；我们从 Amazon 的 IPv6 地址池将该块分配给您的 VPC。

如果您已向 VPC 关联 IPv6 CIDR 块，则可以将 IPv6 CIDR 块与 VPC 中的现有子网关联，或在创建新子网时执行此操作。子网的 IPv6 CIDR 块使用 /64 的固定前缀长度。

例如，您可以创建一个 VPC 并指定要向此 VPC 关联 IPv6 CIDR 块。Amazon 向您的 VPC 分配以下 IPv6 CIDR 块：2001:db8:1234:1a00::/56。您可以创建一个子网并从此范围分配 IPv6 CIDR 块；例如，2001:db8:1234:1a00::/64。

您可以取消 IPv6 CIDR 块与子网的关联，也可以取消 IPv6 CIDR 块与 VPC 的关联。在取消 IPv6 CIDR 块与 VPC 的关联后重新关联它们时，不一定会收到相同的 CIDR 块。

每个子网 CIDR 块中的前四个 IPv6 地址和最后一个 IPv6 地址无法供您使用，而且无法分配到一个实例。例如，在具有 CIDR 块 2001:db8:1234:1a00/64 的子网中，以下五个 IP 地址是保留的：

- 2001:db8:1234:1a00::
- 2001:db8:1234:1a00::1
- 2001:db8:1234:1a00::2
- 2001:db8:1234:1a00::3
- 2001:db8:1234:1a00:ffff:ffff:ffff:ffff

子网路由

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流量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，请参阅 [路由表 \(p. 181\)](#)。

在上图中，与子网 1 关联的路由表将所有 IPv4 流量 (0.0.0.0/0) 和 IPv6 流量 (::/0) 路由至 Internet 网关（例如 igw-1a2b3c4d）。实例 1A 具有 IPv4 弹性 IP 地址，实例 1B 具有 IPv6 地址，因此，可通过 Internet 分别经由 IPv4 和 IPv6 访问它们。

Note

(仅限 IPv4) 与您的实例关联的弹性 IPv4 地址或公有 IPv4 地址是通过 VPC 的 Internet 网关访问到的。经过 AWS Site-to-Site VPN 连接（在您的实例与其他网络之间）的流量经过虚拟专用网关，而不是 Internet 网关，因此不访问弹性 IPv4 地址或公有 IPv4 地址。

实例 2A 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) 网关或实例，允许 VPC 中的一个实例通过 IPv4 发起到 Internet 的出站连接，并阻止来自 Internet 的未经请求的入站连接。由于您可分配的弹性 IP 地址数量有限，因此，如果您有更多的实例需要静态的公有 IP 地址，我们建议您使用 NAT 设备。有关更多信息，请参阅 [NAT \(p. 200\)](#)。要通过 IPv6 发起到 Internet 的仅出站通信，您可以使用仅出口 Internet 网关。有关更多信息，请参阅 [仅出口 Internet 网关 \(p. 197\)](#)。

与子网 3 关联的路由表将所有 IPv4 流量 (0.0.0.0/0) 路由到虚拟专用网关（例如 vgw-1a2b3c4d）。实例 3A 可以通过 Site-to-Site VPN 连接访问企业网络内的计算机。

子网安全性

AWS 提供了可以用于在 VPC 中提高安全性的两个功能：安全组 和 网络 ACL。安全组可以控制您的实例的入站和出站数据流，网络 ACL 可以控制您的子网的入站和出站数据流。多数情况下，安全组即可满足您的需要；但是，如果您需要为您的 VPC 增添额外一层安全保护，您也可以使用网络 ACL。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

每个子网有意必须与一个网络 ACL 关联。您创建的每个子网均自动与 VPC 的默认网络 ACL 关联。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，请参阅 [网络 ACL \(p. 126\)](#)。

您可以在 VPC 或子网上创建流日志，以便捕获传入和传出您的 VPC 或子网中的网络接口的流量。您还可以在单独的网络接口上创建流日志。流日志会发布到 CloudWatch Logs。有关更多信息，请参阅[VPC 流日志 \(p. 165\)](#)。

与本地网络和其他 VPC 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 IPv4 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流量都将被丢弃。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
- 在该子网中运行的实例，其 IP 地址为 10.0.1.4 和 10.0.1.5
- 使用 CIDR 块 10.0.37.0/24 和 10.1.38.0/24 的本地主机网络

当 VPC 中的这些实例尝试与 10.0.37.0/24 地址空间中的主机通信时，由于 10.0.37.0/24 是分配给 VPC 的较大前缀 (10.0.0.0/16) 的一部分，因此丢弃这些流量。这些实例可与 10.1.38.0/24 空间中的主机通信，因为该块不是 10.0.0.0/16 的一部分。

您还可以在 VPC 之间创建 VPC 对等连接，或在 VPC 与其他 AWS 账户中的 VPC 之间创建连接。利用 VPC 对等连接，您可以在使用私有 IP 地址的 VPC 之间路由流量；但是，您无法在具有重叠 CIDR 块的 VPC 之间创建 VPC 对等连接。有关更多信息，请参阅[Amazon VPC Peering Guide](#)。

因此，我们建议您在创建 VPC 时使用足以满足未来预期增长需求的 CIDR 范围，并确保该范围不会与您公司或家庭网络中任何现有或未来预期的子网重叠，也不会与当前或未来的 VPC 重叠。

我们目前不支持通过 IPv6 的 AWS Site-to-Site VPN 连接。

使用 VPC 和子网

下列步骤用于手动创建 VPC 和子网。您还必须手动添加网关和路由表。或者，您可以使用 Amazon VPC 向导一步创建 VPC 及其子网、网关和路由表。有关更多信息，请参阅[场景和示例 \(p. 23\)](#)。

任务

- [创建 VPC \(p. 83\)](#)
- [在 VPC 中创建子网 \(p. 84\)](#)
- [将辅助 IPv4 CIDR 块与 VPC 关联 \(p. 85\)](#)
- [向 VPC 关联 IPv6 CIDR 块 \(p. 86\)](#)
- [向子网关联 IPv6 CIDR 块 \(p. 86\)](#)
- [在您的子网中启动一项实例 \(p. 86\)](#)
- [删除您的子网 \(p. 87\)](#)
- [取消 IPv4 CIDR 块与 VPC 的关联 \(p. 87\)](#)
- [取消 IPv6 CIDR 块与 VPC 或子网的关联 \(p. 88\)](#)
- [删除 VPC \(p. 89\)](#)

创建 VPC

您可以使用 Amazon VPC 控制台创建空 VPC。

使用控制台创建 VPC

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中，依次选择 Your VPCs、Create VPC。
3. 根据需要指定以下 VPC 详细信息，然后选择 Create VPC。
 - Name tag：可以选择为您的 VPC 提供名称。这样做可创建具有 Name 键以及您指定的值的标签。
 - IPv4 CIDR block：为 VPC 指定 IPv4 CIDR 块。我们建议您参照 [RFC 1918](#) 中指定的私有(非公有可路由)IP 地址范围，从中指定一个 CIDR 块，例如 10.0.0.0/16 或 192.168.0.0/16。

Note

您可以指定公共可路由 IPv4 地址的范围，但我们目前不支持从 VPC 中的公共可路由 CIDR 块直接访问 Internet。如果启动到范围从 224.0.0.0 到 255.255.255.255 (类 D 和类 E IP 地址范围) 的 VPC，Windows 实例将无法正常启动。

- IPv6 CIDR block：可通过选择 Amazon-provided IPv6 CIDR block 向您的 VPC 关联 IPv6 CIDR 块。
- 租赁：选择一个租赁选项。专用租赁可确保您的实例在单租户专用硬件上运行。有关更多信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [Dedicated Instances](#)。

或者，您也可以使用命令行工具。

使用命令行工具创建 VPC

- [create-vpc](#) (AWS CLI)
- [New-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行工具描述 VPC

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

有关 IP 地址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

创建 VPC 后，您可以创建子网。有关更多信息，请参阅 [在 VPC 中创建子网 \(p. 84\)](#)。

在 VPC 中创建子网

要向 VPC 中添加新的子网，必须为 VPC 范围中的子网指定 IPv4 CIDR 块。您可以指定要在其中放置子网的可用区。您可以在同一可用区内具有多个子网。

如果 VPC 已关联 IPv6 CIDR 块，则可以选择为子网指定 IPv6 CIDR 块。

使用控制台向 VPC 中添加子网

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中，选择 Subnets、Create Subnet。
3. 根据需要指定子网详细信息，然后选择 Create Subnet。
 - Name tag：可以选择为子网提供一个名称。这样做可创建具有 Name 键以及您指定的值的标签。
 - VPC：选择要为哪个 VPC 创建子网。
 - Availability Zone：可以选择将您的子网放置在哪个可用区中，或保留默认的 No Preference 让 AWS 为您选择可用区。
 - IPv4 CIDR block：为您的子网指定 IPv4 CIDR 块，如 10.0.1.0/24。有关更多信息，请参阅 [针对 IPv4 的 VPC 和子网大小调整 \(p. 78\)](#)。

- IPv6 CIDR block : (可选) 如果您的 VPC 已关联 IPv6 CIDR 块 , 请选择 Specify a custom IPv6 CIDR。指定子网的十六进制对值或保留默认值。
4. (可选) 如果需要 , 请重复上述步骤以在 VPC 中创建更多子网。

或者 , 您也可以使用命令行工具。

使用命令行工具添加子网

- [create-subnet](#) (AWS CLI)
- [New-EC2Subnet](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行工具描述子网

- [describe-subnets](#) (AWS CLI)
- [Get-EC2Subnet](#) (适用于 Windows PowerShell 的 AWS 工具)

创建子网后 , 您可以执行以下操作 :

- 配置您的路由。要将您的子网设为公有子网 , 必须将 Internet 网关连接到您的 VPC。有关更多信息 , 请参阅 [创建并附加 Internet 网关 \(p. 195\)](#)。然后您可以创建一个自定义路由表 , 并且添加到 Internet 网关的路由。有关更多信息 , 请参阅 [创建自定义路由表 \(p. 195\)](#)。有关其他路由选项 , 请参阅 [路由表 \(p. 181\)](#)。
- 修改子网设置 , 指定在该子网中启动的所有实例都接收公有 IPv4 地址和/或 IPv6 地址。有关更多信息 , 请参阅 [子网的 IP 寻址行为 \(p. 102\)](#)。
- 根据需要创建或修改您的安全组。有关更多信息 , 请参阅 [您的 VPC 的安全组 \(p. 119\)](#)。
- 根据需要创建或修改您的网络 ACL。有关更多信息 , 请参阅 [网络 ACL \(p. 126\)](#)。
- 与其他账户共享子网。有关更多信息 , 请参阅 [??? \(p. 90\)](#)。

将辅助 IPv4 CIDR 块与 VPC 关联

您可以向 VPC 中添加另一个 IPv4 CIDR 块。确保您已阅读适用的 [限制 \(p. 79\)](#)。

在关联 CIDR 块之后 , 状态转为 `associating`。当 CIDR 块处于 `associated` 状态时 , 表示它已准备就绪 , 可以使用。

使用控制台向 VPC 中添加 CIDR 块

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中 , 选择 Your VPCs。
3. 选择所需的 VPC , 然后选择 Actions、Edit CIDRs。
4. 选择 Add IPv4 CIDR , 然后输入要添加的 CIDR 块 , 例如 `10.2.0.0/16`。选择对勾图标。
5. 选择 Close (关闭)。

或者 , 您也可以使用命令行工具。

使用命令行工具添加 CIDR 块

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (适用于 Windows PowerShell 的 AWS 工具)

在添加所需的 IPv4 CIDR 块后，您可以创建子网。有关更多信息，请参阅 [在 VPC 中创建子网 \(p. 84\)](#)。

向 VPC 关联 IPv6 CIDR 块

您可以向任何现有的 VPC 关联 IPv6 CIDR 块。此 VPC 当前必须尚未关联任何 IPv6 CIDR 块。

使用控制台将 IPv6 CIDR 块与 VPC 关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions 和 Edit CIDRs。
4. 选择 Add IPv6 CIDR。添加 IPv6 CIDR 块后，选择 Close。

或者，您也可以使用命令行工具。

使用命令行工具将 IPv6 CIDR 块与 VPC 关联

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (适用于 Windows PowerShell 的 AWS 工具)

向子网关联 IPv6 CIDR 块

您可以向 VPC 中的现有子网关联 IPv6 CIDR 块。此子网当前必须尚未关联任何 IPv6 CIDR 块。

使用控制台将 IPv6 CIDR 块与子网关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，选择 Subnet Actions 和 Edit IPv6 CIDR。
4. 选择 Add IPv6 CIDR。为子网指定十六进制对 (例如，00) 并通过选择对勾图标来确认该条目。
5. 选择 Close (关闭)。

或者，您也可以使用命令行工具。

使用命令行工具将 IPv6 CIDR 块与子网关联

- [associate-subnet-cidr-block](#) (AWS CLI)
- [Register-EC2SubnetCidrBlock](#) (适用于 Windows PowerShell 的 AWS 工具)

在您的子网中启动一项实例

创建子网并配置路由后，您可以使用 Amazon EC2 控制台在您的子网中启动实例。

使用控制台将实例启动到子网中

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在控制面板上，选择 Launch Instance。
3. 按照向导中的指示操作。选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

如果您希望实例通过 IPv6 进行通信，则必须选择支持的实例类型。最新一代的所有实例类型都支持 IPv6 地址。

4. 在 Configure Instance Details 页上，确保已在 Network 列表中选择了所需的 VPC，然后选择要在其中启动实例的子网。将此页上的其他默认设置保留不变，然后选择 Next: Add Storage。
5. 在向导的后续页上，可为您的实例配置存储并添加标签。在 Configure Security Group (配置安全组) 页上，选择您所拥有的任何安全组，或根据向导的指示新建安全组。完成操作后，选择 Review and Launch。
6. 检查您的设置，然后选择 Launch。
7. 选择您所拥有的现有密钥对或者创建一个新的密钥对，然后在完成操作后选择 Launch Instances。

或者，您也可以使用命令行工具。

使用命令行工具将实例启动到子网中

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

删除您的子网

如果不再需要您的子网，可将其删除。您必须先终止子网中的任何实例。

使用控制台删除子网

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 终止子网中的所有实例。有关更多信息，请参阅 EC2 用户指南 中的[终止您的实例](#)。
3. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
4. 在导航窗格中，选择 Subnets。
5. 选择要删除的子网，然后依次选择 Subnet Actions (子网操作)、Delete Subnet (删除子网)。
6. 在 Delete Subnet 对话框中，选择 Yes, Delete。

或者，您也可以使用命令行工具。

使用命令行工具删除子网

- [delete-subnet](#) (AWS CLI)
- [Remove-EC2Subnet](#) (适用于 Windows PowerShell 的 AWS 工具)

取消 IPv4 CIDR 块与 VPC 的关联

如果您的 VPC 与多个 IPv4 CIDR 块关联，则可以取消 IPv4 CIDR 块与 VPC 的关联。您不能取消主要 IPv4 CIDR 块的关联。您只能取消整个 CIDR 块的关联；您无法取消 CIDR 块子集或 CIDR 块合并范围的关联。必须首先删除 CIDR 块中的所有子网。

使用控制台从 VPC 中删除 CIDR 块

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择所需的 VPC，然后选择 Actions、Edit CIDRs。

4. 在 VPC IPv4 CIDRs 下，选择要删除的 CIDR 块的删除按钮 (叉形记号)。
5. 选择 Close (关闭)。

或者，您也可以使用命令行工具。

使用命令行工具从 VPC 中删除 IPv4 CIDR 块

- [disassociate-vpc-cidr-block \(AWS CLI\)](#)
- [Unregister-EC2VpcCidrBlock \(适用于 Windows PowerShell 的 AWS 工具\)](#)

取消 IPv6 CIDR 块与 VPC 或子网的关联

如果不再需要 VPC 或子网支持 IPv6，但需要继续使用 VPC 或子网创建 IPv4 资源并与之通信，则可以取消 IPv6 CIDR 块关联。

要取消 IPv6 CIDR 块关联，必须先取消分配已分配给子网中任何实例的任何 IPv6 地址。有关更多信息，请参阅 [取消分配给实例的 IPv6 地址 \(p. 105\)](#)。

使用控制台取消 IPv6 CIDR 块与子网的关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，选择 Subnet Actions 和 Edit IPv6 CIDR。
4. 通过选择十字图标来删除子网的 IPv6 CIDR 块。
5. 选择 Close (关闭)。

使用控制台取消 IPv6 CIDR 块与 VPC 的关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions 和 Edit CIDRs。
4. 通过选择十字图标来删除 IPv6 CIDR 块。
5. 选择 Close (关闭)。

Note

取消 IPv6 CIDR 块关联不会自动删除您为 IPv6 网络配置的任何安全组规则、网络 ACL 规则或路由表路由。您必须手动修改或删除这些规则或路由。

或者，您也可以使用命令行工具。

使用命令行工具取消 IPv6 CIDR 块与子网的关联

- [disassociate-subnet-cidr-block \(AWS CLI\)](#)
- [Unregister-EC2SubnetCidrBlock \(适用于 Windows PowerShell 的 AWS 工具\)](#)

使用命令行工具取消 IPv6 CIDR 块与 VPC 的关联

- [disassociate-vpc-cidr-block \(AWS CLI\)](#)
- [Unregister-EC2VpcCidrBlock \(适用于 Windows PowerShell 的 AWS 工具\)](#)

删除 VPC

您可以随时删除您的 VPC。但是，必须先终止 VPC 中的所有实例。使用 VPC 控制台删除 VPC 时，将删除其所有组件，如子网、安全组、网络 ACL、路由表、Internet 网关、VPC 对等连接和 DHCP 选项。

如果您具有一个 AWS Site-to-Site VPN 连接，则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 Site-to-Site VPN 连接和网关。否则，您的网络管理员必须在您创建新的 Site-to-Site VPN 连接之后再次配置客户网关。

使用控制台删除 VPC

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 终止 VPC 中的所有实例。想要了解更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[终止您的实例](#)。
3. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
4. 在导航窗格中，选择 Your VPCs。
5. 选择要删除的 VPC，然后依次选择 Actions、Delete VPC。
6. 要删除 Site-to-Site VPN 连接，请选择相关选项；否则，保留不选。选择 Yes, Delete。

或者，您也可以使用命令行工具。使用命令行删除 VPC 时，必须首先终止所有实例，删除所有子网、自定义安全组和自定义路由表，并分离 VPC 中的任何 Internet 网关。

使用命令行工具删除 VPC

- [delete-vpc](#) (AWS CLI)
- [Remove-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

使用共享 VPC

VPC 共享允许多个 AWS 账户在共享的集中式管理的 Amazon Virtual Private Cloud (VPC) 中创建自己的应用程序资源，如 Amazon EC2 实例、Amazon Relational Database Service (RDS) 数据库、Amazon Redshift 群集和 AWS Lambda 函数。在此模型中，拥有 VPC 的账户（所有者）与属于 AWS Organizations 中同一组织的其他账户（参与者）共享一个或多个子网。共享子网之后，参与者可以查看、创建、修改和删除与他们共享的子网中的应用程序资源。参与者无法查看、修改或删除属于其他参与者或 VPC 拥有者的资源。

目录

- [共享 VPC 的先决条件 \(p. 89\)](#)
- [共享子网 \(p. 90\)](#)
- [将共享的子网取消共享 \(p. 90\)](#)
- [确定共享子网的拥有者 \(p. 90\)](#)
- [共享子网权限 \(p. 91\)](#)
- [拥有者和参与者的计费和计量 \(p. 91\)](#)
- [共享子网不支持的服务 \(p. 91\)](#)
- [限制 \(p. 91\)](#)

共享 VPC 的先决条件

您必须从组织的主账户启用资源共享。有关启用资源共享的信息，请参阅 AWS RAM 用户指南中的[通过 AWS Organizations 启用共享](#)。

共享子网

您可以与组织中的其他账户共享非默认子网。要共享子网，必须首先使用要共享的子网、AWS 账户、组织单位或要与之共享子网的整个组织创建一个资源共享。有关创建资源共享的信息，请参阅 AWS RAM 用户指南中的[创建资源共享](#)。

使用控制台共享子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，然后选择操作、共享子网。
4. 选择您的资源共享，然后选择共享子网。

使用 AWS CLI 共享子网

使用 `create-resource-share` 和 `associate-resource-share` 命令。

跨可用区映射子网

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的名称。例如，您的 AWS 账户的可用区 `us-east-1a` 可能与另一 AWS 账户的 `us-east-1a` 不在同一位置。

要跨账户协调可用区以便进行 VPC 共享，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，`use1-az1` 为 `us-east-1` 区域中的可用区之一。利用可用区 ID，您可以确定一个账户中的资源相对于另一个账户中的资源所在的位置。有关更多信息，请参阅 AWS RAM 用户指南中的[您的资源的 AZ ID](#)。

将共享的子网取消共享

拥有者随时可以将与参与者共享的子网取消共享。在拥有者将共享的子网取消共享后，将应用以下规则：

- 现有参与者资源将继续在已取消共享的子网中运行。
- 参与者在已取消共享的子网中无法再创建新资源。
- 参与者可以修改、描述和删除其位于子网中的资源。
- 如果参与者在已取消共享的子网中仍具有资源，则拥有者无法删除共享子网或共享子网 VPC。仅当参与者删除已取消共享的子网中的所有资源之后，拥有者才能删除子网或共享子网 VPC。

使用控制台取消共享子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，然后选择操作、共享子网。
4. 依次选择操作、停止共享。

使用 AWS CLI 取消共享子网

使用 `disassociate-resource-share` 命令。

确定共享子网的拥有者

参与者可以通过使用 Amazon VPC 控制台或命令行工具来查看已与其共享的子网。

确定子网拥有者（控制台）

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中，选择 Subnets。拥有者列显示子网拥有者。

使用 AWS CLI 确定子网拥有者

使用 `describe-subnets` 和 `describe-vpcs` 命令，这两条命令的输出中将包括拥有者的 ID。

共享子网权限

拥有者权限

VPC 拥有者负责创建、管理和删除所有 VPC 级别的资源（包括子网、路由表、网络 ACL、对等连接、VPC 终端节点、PrivateLink 终端节点、Internet 网关、NAT 网关、虚拟专用网关和中转网关连接）。

VPC 拥有者无法修改或删除参与者资源（包括参与者创建的安全组）。VPC 拥有者可以查看所有网络接口和连接到参与者资源的安全组的详细信息，以便于问题排查和审计。VPC 拥有者可以在 VPC、子网或 ENI 级别创建流日志订阅，以便监控流量或排查问题。

参与者权限

位于共享 VPC 中的参与者负责创建、管理和删除其资源（包括 Amazon EC2 实例、Amazon RDS 数据库和负载均衡器）。参与者无法查看或修改属于其他参与者账户的资源。参与者可以查看路由表和网络 ACL（连接到与其共享的子网）的详细信息。但是，他们无法修改 VPC 级别的资源（包括路由表、网络 ACL 或子网）。参与者可以使用安全组 ID 引用属于其他参与者或拥有者的安全组。参与者只能为他们拥有的接口创建流日志订阅。

拥有者和参与者的计费和计量

在共享 VPC 中，每个参与者为其应用程序资源（包括 Amazon EC2 实例、Amazon Relational Database Service 数据库、Amazon Redshift 集群和 AWS Lambda 函数）付费。参与者还支付与可用区间数据传输、跨 VPC 对等连接的数据传输和通过 AWS Direct Connect 网关的数据传输关联的数据传输费用。VPC 拥有者支付每小时费用（如果适用），跨 NAT 网关、虚拟专用网关、中转网关、PrivateLink 和 VPC 终端节点的数据处理和数据传输费用。在同一个可用区域（使用 AZ-ID 进行唯一标识）内数据传输是免费的，而不考虑通信资源的账户所有权。

共享子网不支持的服务

参与者不能将共享子网用于以下服务：

- AWS CloudHSM (Classic)
- AWS Glue
- Amazon EMR
- 网络负载均衡器

限制

以下限制适用于 VPC 共享的使用：

- 拥有者只能通过 AWS Organizations 与位于同一组织的其他账户或组织单位共享子网。
- 拥有者无法共享位于默认 VPC 中的子网。

- 参与者无法使用其他参与者或拥有者拥有的安全组启动资源。
- 参与者无法使用 VPC 的默认安全组启动资源，因为此安全组属于拥有者。
- 服务限制按独立账户应用。有关服务限制的更多信息，请参阅 Amazon Web Services 一般参考 中的 [AWS 服务限制](#)。
- 不会与参与者共享 VPC 标签。
- 当参与者在共享的子网中启动资源时，他们应确保将其安全组附加到资源，而不是依赖于默认安全组。参与者无法使用默认安全组，因为它属于 VPC 所有者。

默认 VPC 和默认子网

如果您的 AWS 账户是在 2013 年 12 月 4 日之后创建的，它仅支持 EC2-VPC。在这种情况下，您将在每个 AWS 区域拥有一个默认 VPC。默认 VPC 可供您使用，因此您不必创建和配置您自己的 VPC。您可以立即在默认 VPC 中启动 Amazon EC2 实例。您还可以在默认 VPC 中使用 Elastic Load Balancing、Amazon RDS 和 Amazon EMR 等服务。

默认 VPC 适用于快速入门和启动公共实例（如博客或简单的网站）。您可以按需修改您的默认 VPC 的组件。如果您更愿意创建符合您的特定要求的非默认 VPC（例如，使用您的首选 CIDR 块范围和子网大小），请参阅[示例方案 \(p. 23\)](#)。

内容

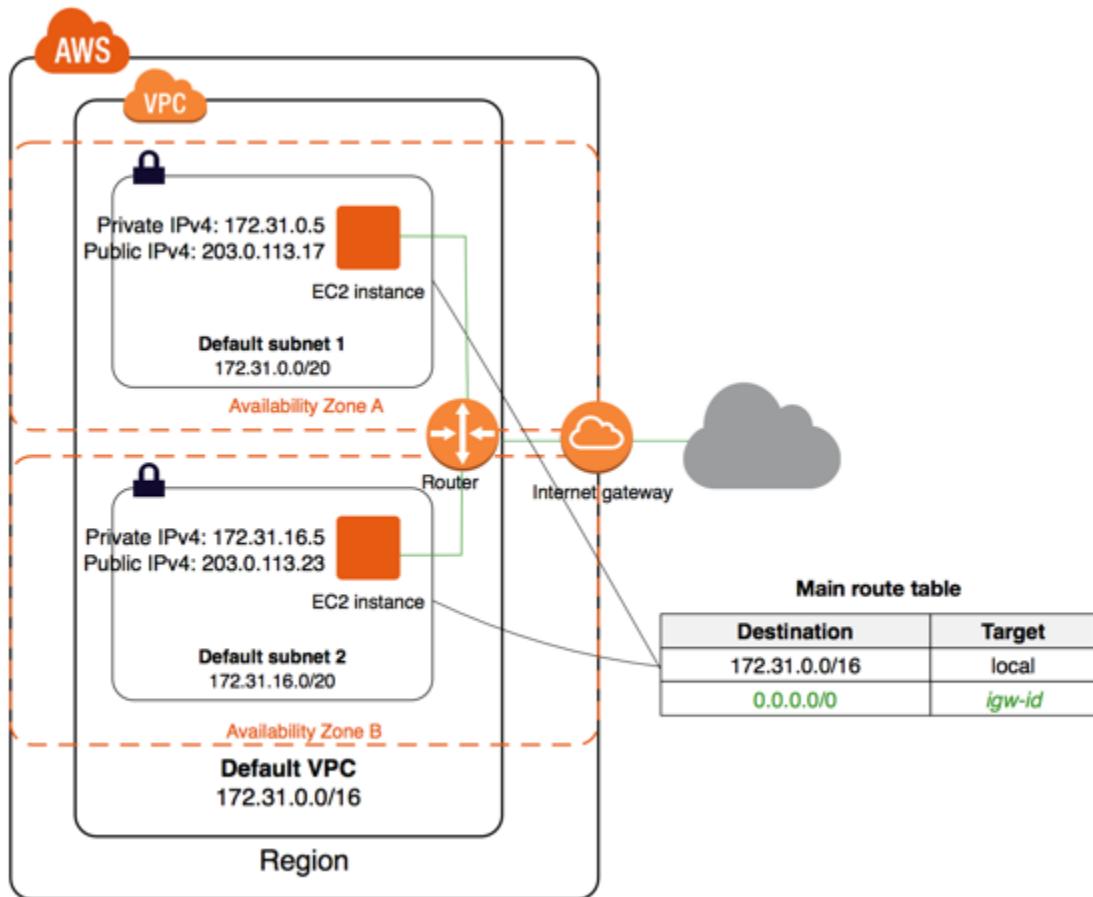
- [默认 VPC 组件 \(p. 93\)](#)
- [可用性和支持的平台 \(p. 95\)](#)
- [查看您的默认 VPC 和默认子网 \(p. 96\)](#)
- [在您的默认 VPC 内启动 EC2 实例。 \(p. 96\)](#)
- [删除您的默认子网和默认 VPC \(p. 97\)](#)
- [创建默认 VPC \(p. 97\)](#)
- [创建默认子网 \(p. 98\)](#)

默认 VPC 组件

当我们创建默认 VPC 时，我们会通过以下操作为您完成设置：

- 创建 IPv4 CIDR 块大小为 /16 的 VPC (172.31.0.0/16)。最多可提供 65536 个私有 IPv4 地址。
- 在每个可用区内创建大小为 /20 的默认子网。这将为每个子网提供多达 4,096 个地址，其中有一些被预留下来供我们使用。
- 创建 [internet 网关 \(p. 192\)](#)并将其连接到您的默认 VPC。
- 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。



您可以像使用任何其他 VPC 一样使用默认 VPC：

- 添加更多非默认子网。
- 修改主路由表。
- 添加更多路由表。
- 关联更多安全组。
- 更新默认安全组的规则。
- 添加 AWS Site-to-Site VPN 连接。
- 添加更多 IPv4 CIDR 块。

您可像使用任何其他子网一样使用默认子网；可添加自定义路由表和设置网络 ACL。您还可以在启动 EC2 实例时指定特定默认子网。

您可以选择将 IPv6 CIDR 块与默认 VPC 关联。有关更多信息，请参阅 [使用 VPC 和子网 \(p. 83\)](#)。

默认子网

默认情况下，默认子网为公有子网，因为主路由表会将指定发往 Internet 的子网流量发送到 Internet 网关。您可以从到 Internet 网关的目标 0.0.0.0/0 中删除路由，以使默认子网变为私有子网。但是，如果您执行此操作，则在该子网中运行的所有 EC2 实例都无法访问 Internet。

您在默认子网中启动的实例将同时接收公有 IPv4 地址和私有 IPv4 地址以及公有和私有 DNS 主机名。在默认 VPC 中的非默认子网内启动的实例不接收公有 IPv4 地址或 DNS 主机名。您可以更改您子网的默认公有 IP 寻址行为。有关更多信息，请参阅 [修改子网的公有 IPv4 寻址属性 \(p. 103\)](#)。

有时，AWS 可能会向某个区域添加新可用区。大多数情况下，我们会在几天内在此可用区中为您的默认 VPC 自动创建新的默认子网。但是，如果您对默认 VPC 进行过任何修改，那么我们不会添加新的默认子网。如果您希望对新的可用区使用默认子网，则可以自行创建一个。有关更多信息，请参阅 [创建默认子网 \(p. 98\)](#)。

可用性和支持的平台

如果您的 AWS 账户是在 2013 年 12 月 4 日之后创建的，它仅支持 EC2-VPC。在这种情况下，我们会为您在每个 AWS 区域内创建默认 VPC。因此，除非您创建一个非默认 VPC，并指定用它来启动实例，否则我们将在您的默认 VPC 中为您启动这个实例。

如果您的 AWS 账户是在 2013 年 3 月 18 日之前创建的，则它在您之前使用过的地区，支持 EC2-Classic 和 EC2-VPC；在您未曾使用过的地区仅支持 EC2-VPC。在此情况下，我们在每个您尚未创建任何 AWS 资源的区域中创建一个默认 VPC。除非您创建了一个非默认 VPC 并在新区域中启动实例时指定了它，否则我们将在该区域的默认 VPC 中启动实例。但是，如果您在之前使用过的区域启动实例，我们会在 EC2-Classic 中启动该实例。

如果您的 AWS 账户是在 2013-03-18 到 2013-12-04 这段时间内创建的，则它可能仅支持 EC2-VPC。或者，在您已使用的部分区域中，AWS 账户可能同时支持 EC2-Classic 和 EC2-VPC。有关检测您的 AWS 账户每个区域对平台的支持情况的信息，请参阅 [检测支持的平台以及您是否有默认 VPC \(p. 95\)](#)。想要了解有关每个区域何时启用默认 VPC 的信息，请参阅 Amazon VPC AWS 论坛中的[公告：启用默认 VPC 功能集的区域](#)。

如果一个 AWS 账户仅支持 EC2-VPC，则与该 AWS 账户关联的任何 IAM 账户也仅支持 EC2-VPC，并使用与该 AWS 账户相同的默认 VPC。

如果您的 AWS 账户同时支持 EC2-Classic 和 EC2-VPC，则可创建新的 AWS 账户或在您之前尚未使用的区域中启动实例。您可以执行此操作以获得使用 EC2-VPC 的好处，方便地在 EC2-Classic 内启动实例。如果您仍然更愿意将默认 VPC 添加到没有 VPC 并且支持 EC2-Classic 的区域，请参阅“我很想让我现有的 EC2 账户拥有默认 VPC。这是否可行的？”（在 [默认 VPC 常见问题](#) 中）。

有关 EC2-Classic 和 EC2-VPC 平台的更多信息，请参阅 [支持的平台](#)。

检测支持的平台以及您是否有默认 VPC

您可以使用 Amazon EC2 控制台或命令行确定您的 AWS 账户是否支持这两个平台，或者您是否具有默认 VPC。

使用 Amazon EC2 控制台检测平台支持

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航栏中，使用右上方的区域选择器选择您的区域。
3. 在 Amazon EC2 控制台控制面板上，从 Account Attributes (账户属性) 下找到 Supported Platforms (支持的平台)。如果有两个值 EC2 和 VPC，您可以将实例启动到两个中的任何一个平台中。如果有一个值 VPC，您只能将实例启动到 EC2-VPC 中。

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。

[Supported Platforms](#)

VPC

[Default VPC](#)

vpc-1a2b3c4d

如果您删除默认 VPC，Default VPC 将显示为 None。有关更多信息，请参阅[删除您的默认子网和默认 VPC \(p. 97\)](#)。

使用命令行检测平台支持

- [describe-account-attributes](#) (AWS CLI)
- [Get-EC2AccountAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

输出中的 `supported-platforms` 属性指示您可以在其中启动 EC2 实例的平台。

查看您的默认 VPC 和默认子网

您可以使用 Amazon VPC 控制台或命令行查看您的默认 VPC 和子网。

使用 Amazon VPC 控制台查看您的默认 VPC 和子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 在 Default VPC 列中，查找值 Yes。记下默认 VPC 的 ID。
4. 在导航窗格中，选择 Subnets。
5. 在搜索栏中，键入默认 VPC 的 ID。返回的子网是您的默认 VPC 中的子网。
6. 要验证哪些子网是默认子网，请在 Default Subnet 列中查找值 Yes。

使用命令行描述您的默认 VPC

- 使用 [describe-vpcs](#) (AWS CLI)
- 使用 [Get-EC2Vpc](#) (适用于 Windows PowerShell 的 AWS 工具)

将命令与 `isDefault` 筛选器结合使用并将筛选值设置为 `true`。

使用命令行描述您的默认子网

- 使用 [describe-subnets](#) (AWS CLI)
- 使用 [Get-EC2Subnet](#) (适用于 Windows PowerShell 的 AWS 工具)

将命令与 `vpc-id` 筛选器结合使用并将筛选值设置为默认 VPC 的 ID。在输出中，`DefaultForAz` 字段对默认子网设置为 `true`。

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，并在该可用区的相应子网内启动实例。或者，您可以通过在控制台中选择对应的默认子网、或在 AWS CLI 中指定子网或可用区，来为您的实例选择可用区。

使用控制台启动 EC2 实例

在您的默认 VPC 内启动 EC2 实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 从 EC2 控制面板中，选择 Launch Instance。
3. 按照向导中的指示操作。选择 AMI，然后选择实例类型。通过选择 Review and Launch，可接受向导其余部分的默认设置。这样将直接进入 Review Instance Launch (核查实例启动) 页。
4. 检视您的设置。在 Instance Details (实例详细信息) 部分中，Subnet (子网) 的默认值为 No preference (default subnet in any Availability Zone) (无首选项(任何可用区的默认子网))。这意味着这项实例会在我们选定的可用区的默认子网中启动。或者，可选择 Edit instance details，并为特定可用区选择默认子网。
5. 选择 Launch 以选择密钥对并启动实例。

使用命令行启动 EC2 实例

您可以使用以下命令之一启动 EC2 实例：

- `run-instances` (AWS CLI)
- `New-EC2Instance` (适用于 Windows PowerShell 的 AWS 工具)

要在您的默认 VPC 中启动 EC2 实例，请使用这些命令而不指定子网或可用区。

要在默认 VPC 中的特定默认子网中启动 EC2 实例，请指定子网 ID 或可用区。

删除您的默认子网和默认 VPC

您可以像删除其他任何子网或 VPC 一样删除默认子网或默认 VPC。但如果删除默认子网或默认 VPC，则您必须明确指定要在其中启动实例的另一个 VPC 中的子网，因为您无法在 EC2-Classic 内启动实例。如果您没有另一个 VPC，您必须创建非默认 VPC 与非默认子网。有关更多信息，请参阅 [创建 VPC \(p. 83\)](#)。

如果您删除了默认 VPC，则可以创建一个新的默认 VPC。有关更多信息，请参阅 [创建默认 VPC \(p. 97\)](#)。

如果您删除默认子网，则可以创建一个新的默认子网。有关更多信息，请参阅 [创建默认子网 \(p. 98\)](#)。或者，您也可以在您的默认 VPC 中创建一个非默认子网并与 AWS Support 联系以将该子网标记为默认子网。您必须提供以下详细信息：您的 AWS 账户 ID、区域和子网 ID。为了确保您的新默认子网按预期正常运行，请修改子网属性以将公有 IP 地址分配到在该子网中启动的实例。有关更多信息，请参阅 [修改子网的公有 IPv4 寻址属性 \(p. 103\)](#)。每个可用区只能有一个默认子网。不能在非默认 VPC 中创建默认子网。

创建默认 VPC

如果您删除了默认 VPC，则可以创建一个新的默认 VPC。您无法恢复之前删除的默认 VPC，并且无法将现有非默认 VPC 标记为默认 VPC。如果您的账户支持 EC2-Classic，您将无法利用这些步骤在支持 EC2-Classic 的区域中创建默认 VPC。

当您创建默认 VPC 时，将使用默认 VPC 的标准组件 ([p. 93](#)) 创建它 (包括每个可用区中的默认子网)。您无法指定您自己的组件。新的默认 VPC 的子网 CIDR 块可能不会与之前的默认 VPC 映射到同一可用区。例如，如果具有 CIDR 块的子网 172.31.0.0/20 是在之前的默认 VPC 的 us-east-2a 中创建的，则该子网可能在新的默认 VPC 的 us-east-2b 中创建。

如果您在该区域中已经有默认 VPC，则无法创建另一个默认 VPC。

使用 Amazon VPC 控制台创建默认 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 依次选择 Actions 和 Create Default VPC。
4. 选择 Create。关闭确认屏幕。

使用命令行创建默认 VPC

- 您可以使用 `create-default-vpc` AWS CLI 命令。此命令没有任何输入参数。

```
aws ec2 create-default-vpc
```

```
{  
    "Vpc": {  
        "VpcId": "vpc-3f139646",  
        "InstanceTenancy": "default",  
        "Tags": [],  
        "Ipv6CidrBlockAssociationSet": [],  
        "State": "pending",  
        "DhcpOptionsId": "dopt-61079b07",  
        "CidrBlock": "172.31.0.0/16",  
        "IsDefault": true  
    }  
}
```

此外，您还可以使用 `New-EC2DefaultVpc` Windows PowerShell 工具 命令或 `CreateDefaultVpc` Amazon EC2 API 操作。

创建默认子网

您可以在没有默认子网的可用区中创建一个默认子网。例如，如果您已删除默认子网，或者 AWS 已添加新的可用区但未在您的默认 VPC 中为该区域自动创建默认子网，则您可能需要创建一个默认子网。

创建默认子网时，将使用您的默认 VPC 中的下一个可用连续空间内的大小为 /20 的 IPv4 CIDR 块创建它。以下规则适用：

- 不能自行指定 CIDR 块。
- 不能恢复已删除的之前的默认子网。
- 每个可用区只能有一个默认子网。
- 不能在非默认 VPC 中创建默认子网。

如果您的默认 VPC 中没有用于创建大小为 /20 的 CIDR 块的足够地址空间，则请求会失败。如果您需要更多地址空间，则可以[将 IPv4 CIDR 块添加到您的 VPC \(p. 79\)](#)。

如果您已将 IPv6 CIDR 块与您的默认 VPC 关联，则新的默认子网不会自动接收 IPv6 CIDR 块。您可以改为在创建一个 IPv6 CIDR 块后将其与默认子网关联。有关更多信息，请参阅[向子网关联 IPv6 CIDR 块 \(p. 86\)](#)。

目前，您只能使用 AWS CLI、AWS 开发工具包或 Amazon EC2 API 创建默认子网。

使用命令行创建默认子网

- 使用 [create-default-subnet](#) AWS CLI 命令并指定要在其中创建子网的可用区。

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

或者，您也可以使用 [CreateDefaultSubnet](#) Amazon EC2 API 操作。

您的 VPC 中的 IP 地址

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

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

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

Note

要确保您的实例可以与 Internet 通信，您还必须将 Internet 网关附加到 VPC。有关更多信息，请参阅 [Internet 网关 \(p. 192\)](#)。

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

下表总结了 Amazon EC2 和 Amazon VPC 中 IPv4 与 IPv6 之间的差异。

IPv4 和 IPv6 特性与限制

IPv4	IPv6
格式为 32 位，4 组，每组最多 3 个数字。	格式为 128 位，8 组，每组 4 个十六进制数字。
所有 VPC 的默认项和必需值；无法删除。	可以选择启用。
VPC CIDR 块大小可以从 /16 到 /28。	VPC CIDR 块大小固定为 /56。
子网 CIDR 块大小可以从 /16 到 /28。	子网 CIDR 块大小固定为 /64。
您可以为您的 VPC 选择私有 IPv4 CIDR 块。	我们从 Amazon 的 IPv6 地址池中为您的 VPC 选择 IPv6 CIDR 块。您不能选择自己的范围。
存在私有 IP 地址和公有 IP 地址之分。要与 Internet 通信，需要通过网络地址转换 (NAT) 将公有 IPv4 地址映射为主要私有 IPv4 地址。	不区分公有 IP 地址和私有 IP 地址。IPv6 地址是公有的。
所有实例类型都支持。	受所有最新一代的实例类型以及 C3、R3 和 I2 上一代实例类型的支持。有关更多信息，请参阅 实例类型 。
受 EC2-Classic 和通过 ClassicLink 与 VPC 连接的 EC2-Classic 支持。	不受 EC2-Classic 和通过 ClassicLink 与 VPC 连接的 EC2-Classic 支持。
所有 AMI 都支持。	在针对 DHCPv6 进行了配置的 AMI 上自动受到支持。Amazon Linux 版本 2016.09.0 和更高版本以及 Windows Server 2008 R2 和更高版本进行了 DHCPv6 方面的配置。对于其他 AMI，您必须 手动配置实例 (p. 112) 以识别分配的任何 IPv6 地址。
实例会收到与其私有 IPv4 地址对应的 Amazon 提供的私有 DNS 主机名，如果适用，还会收到与其公有 IPv4 或弹性 IP 地址对应的公有 DNS 主机名。	不支持 Amazon 提供的 DNS 主机名。

IPv4	IPv6
支持弹性 IPv4 地址。	不支持弹性 IPv6 地址。
支持 AWS Site-to-Site VPN 连接和客户网关、NAT 设备及 VPC 终端节点。	不支持 AWS Site-to-Site VPN 连接和客户网关、NAT 设备及 VPC 终端节点。

我们支持通过虚拟专用网关到 AWS Direct Connect 连接的 IPv6 流量。有关更多信息，请参阅 [AWS Direct Connect 用户指南](#)。

私有 IPv4 地址

私有 IPv4 地址（也称作私有 IP 地址）无法通过 Internet 访问，但可用于 VPC 中实例之间的通信。当您在 VPC 中启动实例时，系统会将子网地址范围中的一个主要私有 IPv4 地址分配给该实例的默认网络接口（eth0）。另外，还为每个实例指定一个可解析为实例私有 IP 地址的私有（内部）DNS 主机名。如果您未指定主要私有 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 EC2 用户指南（适用于 Linux 实例）中的 [Elastic Network Interfaces](#)。

您可以为 VPC 中运行的实例分配其他私有 IP 地址，即所谓的辅助私有 IP 地址。与主要私有 IP 地址不同的是，您可以将一个网络接口的辅助私有 IP 地址重新分配给另一个网络接口。私有 IP 地址会在实例停止并重新启动时保持与网络接口的关联，并在实例终止时释放。有关主要和次要 IP 地址的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 [Multiple IP Addresses](#) 部分。

Note

我们所说的私有 IP 地址是 VPC 的 IPv4 CIDR 范围内的 IP 地址。大部分 VPC IP 地址范围均处于 RFC 1918 中指定的私有（非公有可路由）IP 地址范围内；但是，您可为您的 VPC 使用公有可路由的 CIDR 块。不管您的 VPC 使用何种 IP 地址范围，我们都支持从您的 VPC 的 CIDR 块（包括公共可路由的 CIDR 块）直接访问 Internet。您必须通过网关设置 Internet 访问，例如，通过 Internet 网关、虚拟专用网关、AWS Site-to-Site VPN 连接或 AWS Direct Connect。

公有 IPv4 地址

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

您可以通过执行以下操作，控制实例是否接收公有 IP 地址：

- 修改子网的公有 IP 寻址属性。有关更多信息，请参阅 [修改子网的公有 IPv4 寻址属性 \(p. 103\)](#)。
- 在实例启动过程中启用或禁用公有 IP 寻址功能，以覆盖子网的公有 IP 寻址属性。有关更多信息，请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)。

公有 IP 地址将从 Amazon 的公有 IP 地址池分配，它不与您的账户关联。在公有 IP 地址与您的实例取消关联后，该地址即释放回该池，并且不再可供您使用。您不能手动关联或取消关联公有 IP 地址。而是在某些情况下，我们从您的实例释放该公有 IP 地址，或向其分配新地址。有关详细信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 [公有 IP 地址](#)。

如果您需要向您的账户分配一个永久公有 IP 地址（您可根据需要将其分配给实例或将其实例中删除），请改为使用弹性 IP 地址。有关更多信息，请参阅 [弹性 IP 地址 \(p. 232\)](#)。

如果您的 VPC 启用了对 DNS 主机名的支持，则系统还会向收到公有 IP 地址或弹性 IP 地址的每个实例分配一个公有 DNS 主机名。我们会将公有 DNS 主机名解析为该实例在实例网络外的公有 IP 地址和在实例网络内的私有 IP 地址。有关更多信息，请参阅 [在您的 VPC 中使用 DNS \(p. 228\)](#)。

IPv6 地址

您可以选择向 VPC 和子网关联 IPv6 CIDR 块。有关更多信息，请参阅以下主题：

- 向 VPC 关联 IPv6 CIDR 块 (p. 86)
- 向子网关联 IPv6 CIDR 块 (p. 86)

如果您的 VPC 和子网关联了 IPv6 CIDR 块，并且满足以下条件之一，则 VPC 中的实例会收到 IPv6 地址：

- 您的子网配置为在启动期间向实例的主网络接口自动分配 IPv6 地址。
- 您在启动期间向实例手动分配 IPv6 地址。
- 您在启动后向实例分配 IPv6 地址。
- 您向同一子网中的某个网络接口分配 IPv6 地址，并在启动后将此网络接口附加到您的实例。

当实例在启动期间收到 IPv6 地址时，此地址将与实例的主网络接口 (eth0) 关联。您可以取消 IPv6 地址与主网络接口的关联。我们不支持为您的实例使用 IPv6 DNS 主机名。

IPv6 地址会在您停止和启动实例时保留下来，并在您终止实例时释放出来。您无法重新分配已分配给某个网络接口的 IPv6 地址；您必须先取消分配此—IPv6 地址。

通过将 IPv6 地址分配给附加到实例的网络接口，您可以为实例分配更多的 IPv6 地址。可以分配给网络接口的 IPv6 地址数量以及可以附加到实例的网络接口数量因实例类型而异。有关更多信息，请参阅 Amazon EC2 用户指南 中的 [每个实例类型的每个网络接口的 IP 地址](#)。

IPv6 地址具有全局唯一性，因此可通过 Internet 访问。您可以通过控制子网的路由或通过使用安全组和网络 ACL 规则来控制能否通过实例的 IPv6 地址对其进行访问。有关更多信息，请参阅 [安全性 \(p. 118\)](#)。

有关预留 IPv6 地址范围的更多信息，请参阅 [IANA IPv6 特殊用途地址注册表](#) 和 [RFC4291](#)。

子网的 IP 寻址行为

所有子网都有一个用于确定是否向在该子网中创建的网络接口分配公有 IPv4 地址和 IPv6 地址（如果适用）的可修改属性。这包括当您在该子网中启动实例时为实例创建的主网络接口 (eth0)。

不管子网属性如何，您仍然可以在启动时覆盖特定实例的此设置。有关更多信息，请参阅 [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#) 和 [在实例启动期间分配 IPv6 地址 \(p. 104\)](#)。

使用 IP 地址

您可以修改子网的 IP 寻址行为、在启动期间向实例分配公有 IPv4 地址并向您的实例分配/取消分配 IPv6 地址。

任务

- [修改子网的公有 IPv4 寻址属性 \(p. 103\)](#)
- [修改子网的 IPv6 寻址属性 \(p. 103\)](#)
- [在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)
- [在实例启动期间分配 IPv6 地址 \(p. 104\)](#)
- [向实例分配 IPv6 地址 \(p. 105\)](#)
- [取消分配给实例的 IPv6 地址 \(p. 105\)](#)
- [API 和命令概览 \(p. 105\)](#)

修改子网的公有 IPv4 寻址属性

默认情况下，非默认子网的 IPv4 公有寻址属性设置为 `false`，默认子网的此属性设置为 `true`。Amazon EC2 启动实例向导创建的非默认子网属于例外 — 该向导会将此属性设置为 `true`。您可以使用 Amazon VPC 控制台修改此属性。

修改子网的公有 IPv4 寻址行为

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，然后依次选择 Subnet Actions、Modify auto-assign IP settings。
4. 如果选中，则 Enable auto-assign public IPv4 address 复选框会为在所选子网中启动的所有实例请求公有 IPv4 地址。根据需要选中或清除该复选框，然后选择 Save。

修改子网的 IPv6 寻址属性

默认情况下，所有子网的 IPv6 寻址属性都设置为 `false`。您可以使用 Amazon VPC 控制台修改此属性。如果您为子网启用了 IPv6 寻址功能，则只有在您的网络接口或实例是使用 Amazon EC2 API 的 2016-11-15 版本或更高版本创建的情况下，您的网络接口或实例才会接收 IPv6 地址。在此子网中启动的实例会在主网络接口上收到一个 IPv6 地址。

您的子网必须具有关联的 IPv6 CIDR 块。

Note

如果您为子网启用了 IPv6 寻址功能，则只有在您的网络接口或实例是使用 Amazon EC2 API 的 2016-11-15 版本或更高版本创建的情况下，您的网络接口或实例才会接收 IPv6 地址。Amazon EC2 控制台使用最新的 API 版本。

修改子网的 IPv6 寻址行为

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，然后依次选择 Subnet Actions、Modify auto-assign IP settings。
4. 如果选中 Enable auto-assign IPv6 address 复选框，则会为在所选子网中创建的所有网络接口请求 IPv6 地址。根据需要选中或清除该复选框，然后选择 Save。

在实例启动期间分配公有 IPv4 地址

您可以控制是否在启动时为默认子网或非默认子网中的实例分配公有 IPv4 地址。

Important

启动后，即无法手动将该公有 IPv4 地址与您的实例取消关联。在某些情况下，它会自动释放，之后无法重新使用。如果需要可随意关联或取消关联的持久性公有 IP 地址，则在启动后将弹性 IP 地址与实例关联。有关更多信息，请参阅 [弹性 IP 地址 \(p. 232\)](#)。

在启动期间向实例分配公有 IPv4 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance (启动实例)。
3. 选择 AMI 及实例类型，然后选择 Next: Configure Instance Details。
4. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择一个 VPC。这将显示 Auto-assign Public IP 列表。选择 Enable (启用) 或 Disable (禁用) 可覆盖子网的默认设置。

Important

如果您指定多个网络接口，则不能分配公有 IPv4 地址。此外，如果您将某个现有的网络接口指定为 eth0，则无法使用自动分配公有 IPv4 功能覆盖子网设置。

5. 遵循向导中的剩余步骤来启动您的实例。
6. 在 Instances (实例) 屏幕上，选择您的实例。您可以在 Description 选项卡上的 IPv4 Public IP 字段中查看实例的公有 IP 地址。或者，您也可以在导航窗格中，选择 Network Interfaces，然后选择实例的 eth0 网络接口。您可在 IPv4 Public IP 字段中查看公有 IP 地址。

Note

公有 IPv4 地址在控制台中显示为网络接口的属性，但它通过 NAT 映射到主要私有 IPv4 地址。因此，如果您通过对 Windows 实例执行 ipconfig 或对 Linux 实例执行 ifconfig 等方式来检查实例上网络接口的属性，则不会显示公有 IP 地址。要从实例内确定实例的公有 IP 地址，您可以使用实例元数据。有关更多信息，请参阅[实例元数据和用户数据](#)。

此功能在启动时才可用。然而，无论您是否在启动时为实例分配公有 IPv4 地址，您都可以在启动后将弹性 IP 地址与实例相关联。有关更多信息，请参阅[弹性 IP 地址 \(p. 232\)](#)。

在实例启动期间分配 IPv6 地址

您可以在启动期间向实例自动分配 IPv6 地址。为此，您必须在具有[关联 IPv6 CIDR 块 \(p. 86\)](#)的 VPC 和子网中启动实例。IPv6 地址从子网范围分配到主网络接口 (eth0)。

在启动期间为实例自动分配 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance (启动实例)。
3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

选择支持 IPv6 地址的实例类型。

4. 在 Configure Instance Details 页上，从 Network 中选择 VPC，从 Subnet 中选择子网。对于 Auto-assign IPv6 IP，选择 Enable。
5. 遵循向导中的剩余步骤来启动您的实例。

或者，如果您希望在启动期间将子网范围内的特定 IPv6 地址分配给实例，则您可以将此地址分配到实例的主要网络接口。

在启动期间向实例分配特定的 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择 Launch Instance (启动实例)。
3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。

Note

选择支持 IPv6 地址的实例类型。

4. 在 Configure Instance Details 页上，从 Network 中选择 VPC，从 Subnet 中选择子网。
5. 转到 Network interfaces 部分。对于 eth0 网络接口，在 IPv6 IPs 下选择 Add IP。
6. 输入子网范围内的 IPv6 地址。
7. 遵循向导中的剩余步骤来启动您的实例。

有关在启动期间向实例分配多个 IPv6 地址的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[使用多个 IPv6 地址](#)。

向实例分配 IPv6 地址

如果您的实例位于具有[关联 IPv6 CIDR 块 \(p. 86\)](#)的 VPC 和子网中，您可以使用 Amazon EC2 控制台从子网范围向您的实例分配 IPv6 地址。

向实例关联 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 选择操作、联网和管理 IP 地址。
4. 在 IPv6 Addresses 下，选择 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择 Save (保存)。

或者，您也可以向网络接口分配 IPv6 地址。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中弹性网络接口主题中的[分配 IPv6 地址](#)。

取消分配给实例的 IPv6 地址

如果您的实例不再需要 IPv6 地址，则您可以使用 Amazon EC2 控制台取消其与实例的关联。

取消 IPv6 地址与实例的关联

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 选择操作、联网和管理 IP 地址。
4. 在 IPv6 Addresses 下方，为 IPv6 地址选择 Unassign。
5. 选择 Save (保存)。

或者，您也可以取消 IPv6 地址与网络接口的关联。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中弹性网络接口主题中的[取消分配 IPv6 地址](#)。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅[访问 Amazon VPC \(p. 7\)](#)。

在启动期间分配公有 IPv4 地址

- 将 `--associate-public-ip-address` 或 `--no-associate-public-ip-address` 选项与 `run-instances` 命令 (AWS CLI) 结合使用
- 将 `-AssociatePublicIp` 参数与 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用

在启动期间分配 IPv6 地址

- 将 `--ipv6-addresses` 选项与 `run-instances` 命令 (AWS CLI) 结合使用
- 将 `-Ipv6Addresses` 参数与 `New-EC2Instance` 命令 (适用于 Windows PowerShell 的 AWS 工具) 结合使用

修改子网的 IP 寻址行为

- [modify-subnet-attribute](#) (AWS CLI)
- [Edit-EC2SubnetAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

向网络接口分配 IPv6 地址

- [assign-ipv6-addresses](#) (AWS CLI)
- [Register-EC2Ipv6AddressList](#) (适用于 Windows PowerShell 的 AWS 工具)

取消分配已分配给网络接口的 IPv6 地址

- [unassign-ipv6-addresses](#) (AWS CLI)
- [Unregister-EC2Ipv6AddressList](#) (适用于 Windows PowerShell 的 AWS 工具)。

迁移到 IPv6

如果您的现有 VPC 仅支持 IPv4 并且您的子网中的资源配置为仅使用 IPv4，则可为您的 VPC 和资源启用 IPv6 支持。您的 VPC 可在双堆栈模式下运行 — 您的资源可通过 IPv4 和/或 IPv6 进行通信。IPv4 和 IPv6 通信彼此独立。

您不能为 VPC 和子网禁用 IPv4 支持；这是 Amazon VPC 和 Amazon EC2 的默认 IP 寻址系统。

Note

本信息假定，您的现有 VPC 具有公有和私有子网。有关设置新的 VPC 以用于 IPv6 的信息，请参阅[适用于 Amazon VPC 的 IPv6 入门 \(p. 16\)](#)。

下表概述了让您的 VPC 和子网使用 IPv6 的步骤。

步骤	备注
步骤 1：将 IPv6 CIDR 块与您的 VPC 和子网关联 (p. 109)	将 Amazon 提供的 IPv6 CIDR 块与您的 VPC 和您的子网关联。
步骤 2：更新路由表 (p. 110)	更新路由表以路由 IPv6 流量。对于公有子网，请创建一个将所有 IPv6 流量都从孩子网路由到 Internet 网关的路由。对于私有子网，请创建一个将所有发送到 Internet 的 IPv6 流量都从孩子网路由到仅出口 Internet 网关的路由。
步骤 3：更新安全组规则 (p. 110)	将安全组规则更新为包括 IPv6 地址规则。这样，使 IPv6 流量可以流入和流出您的实例。如果您已创建自定义网络 ACL 规则来控制出入子网的流量，则必须包括 IPv6 流量规则。
步骤 4：更改实例类型 (p. 111)	如果您的实例类型不支持 IPv6，则更改实例类型。
步骤 5：为实例分配 IPv6 地址 (p. 111)	将 IPv6 地址分配到您的子网的 IPv6 地址范围中的实例。
步骤 6：(可选) 在实例中配置 IPv6 (p. 112)	如果从未配置为使用 DHCPv6 的 AMI 中启动实例，则必须对实例进行手动配置，使其识别为实例分配的 IPv6 地址。

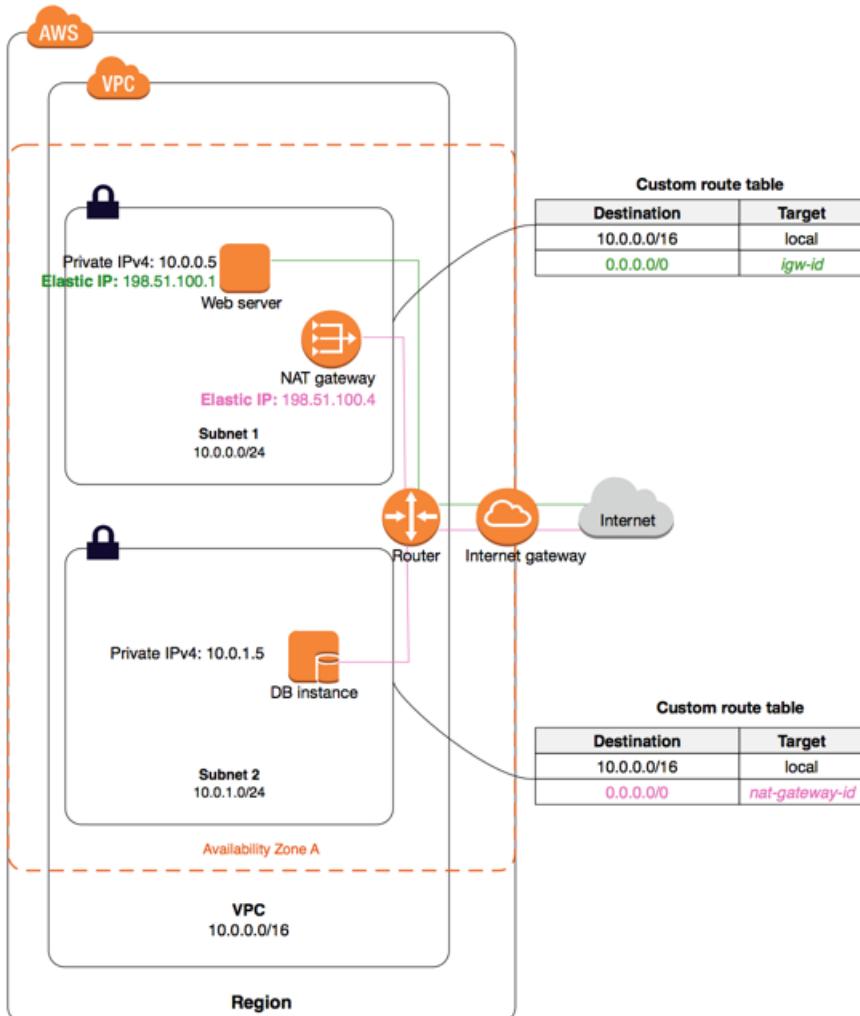
在迁移到使用 IPv6 之前，请确保您已了解 Amazon VPC 的 IPv6 寻址的功能：[IPv4 和 IPv6 特性与限制 \(p. 100\)](#)。

内容

- 示例：在具有公有和私有子网的 VPC 内启用 IPv6 (p. 107)
- 步骤 1：将 IPv6 CIDR 块与您的 VPC 和子网关联 (p. 109)
- 步骤 2：更新路由表 (p. 110)
- 步骤 3：更新安全组规则 (p. 110)
- 步骤 4：更改实例类型 (p. 111)
- 步骤 5：为实例分配 IPv6 地址 (p. 111)
- 步骤 6：(可选) 在实例中配置 IPv6 (p. 112)

示例：在具有公有和私有子网的 VPC 内启用 IPv6

在此示例中，您的 VPC 有公有和私有子网。私有子网中有一个数据库实例，该实例通过 VPC 中的 NAT 网关与 Internet 进行出站通信。公有子网中有一个面向公众的 Web 服务器，它通过 Internet 网关访问 Internet。下图表示您的 VPC 架构。



您的 Web 服务器的安全组 (`sg-11aa22bb`) 具有以下入站规则：

类型	协议	端口范围	源	评论
所有流量	全部	全部	sg-33cc44dd	允许与 33cc44dd 关联的实例 (数据库实例) 的所有流量进行入站访问。
HTTP	TCP	80	0.0.0.0/0	允许通过 HTTP 的 Internet 的入站流量。
HTTPS	TCP	443	0.0.0.0/0	允许通过 HTTPS 的 Internet 入站流量。
SSH	TCP	22	203.0.113.123/32	允许从您的本地计算机进行入站 SSH 访问；例如，在需要连接您的实例来执行管理任务时。

数据库实例的安全组 (sg-33cc44dd) 具有以下入站规则：

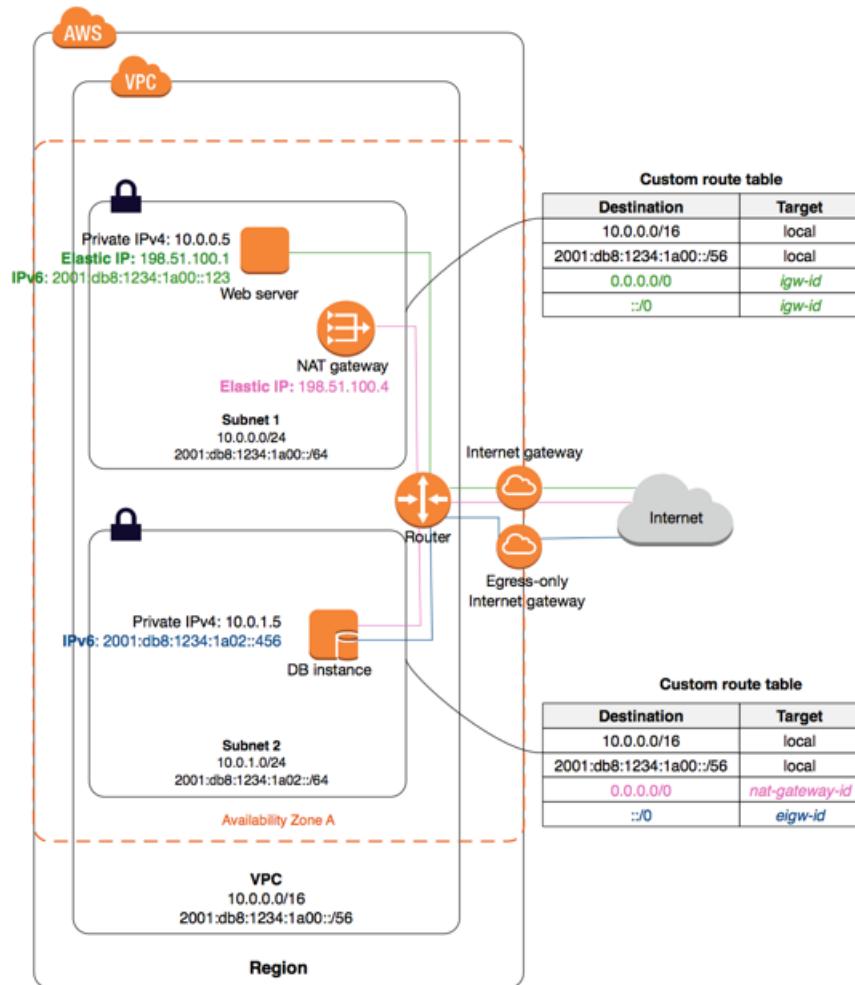
类型	协议	端口范围	源	评论
MySQL	TCP	3306	sg-11aa22bb	允许与 sg-11aa22bb 关联的实例 (Web 服务器实例) 的 MySQL 流量进行入站访问。

两个安全组都有允许所有出站 IPv4 流量的默认出站规则，没有其他出站规则。

您的 Web 服务器是 t2.medium 实例类型。您的数据库服务器是 m3.large。

您希望面向 IPv6 启用 VPC 和资源，需要它们在双堆栈模式下运行；换句话说，需要在 VPC 资源与 Internet 资源之间同时使用 IPv6 和 IPv4 寻址。

完成这些步骤之后，您的 VPC 将具有以下配置。



步骤 1：将 IPv6 CIDR 块与您的 VPC 和子网关联

您可将 IPv6 CIDR 块与 VPC 关联，然后将该范围内的一个 /64 CIDR 块与每个子网关联。

将 IPv6 CIDR 块与 VPC 关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择您的 VPC，然后选择 Actions 和 Edit CIDRs。
4. 选择 Add IPv6 CIDR。添加 IPv6 CIDR 块之后，选择 Close。

将 IPv6 CIDR 块与子网关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 选择您的子网，选择 Subnet Actions 和 Edit IPv6 CIDR。
4. 选择 Add IPv6 CIDR。为子网指定十六进制对 (例如，00) 并通过选择对勾图标来确认该条目。
5. 选择 Close (关闭)。对 VPC 中的其他子网重复上述步骤。

有关更多信息，请参阅针对 IPv6 的 VPC 和子网大小调整 (p. 81)。

步骤 2：更新路由表

对于公有子网，您必须更新自定义路由表，以使实例（例如 Web 服务器）能对 IPv6 流量使用 Internet 网关。

对于私有子网，您必须更新自定义路由表，以使实例（例如数据库实例）能对 IPv6 流量使用仅出口 Internet 网关。

为公有子网更新您的路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables 并选择与共有子网关联的路由表。
3. 在 Routes 选项卡上，选择 Edit。
4. 选择 Add another route。为目的地指定 `::/0`，为目标选择 Internet 网关 ID，然后选择保存。

为私有子网更新您的路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 如果您在私有子网中使用 NAT 设备，则它不支持 IPv6 流量。因此，请为您的私有子网创建一个仅出口 Internet 网关，以启用通过 IPv6 到 Internet 的出站通信并禁止入站通信。仅出口 Internet 网关仅支持 IPv6 流量。有关更多信息，请参阅[仅出口 Internet 网关 \(p. 197\)](#)。
3. 在导航窗格中，选择 Route Tables 并选择与私有子网关联的路由表。
4. 在 Routes 选项卡上，选择 Edit。
5. 选择 Add another route。对于 Destination (目的地)，指定 `::/0`。对于目标，选择仅出口 Internet 网关 ID，然后选择保存。

有关更多信息，请参阅[路由选项 \(p. 185\)](#)。

步骤 3：更新安全组规则

为了使您的实例能够通过 IPv6 发送和接收流量，您必须更新安全组规则以包含针对 IPv6 地址的规则。

例如，在上述示例中，您可以更新您 Web 服务器安全组 (`sg-11aa22bb`) 以添加允许来自 IPv6 地址的入站 HTTP、HTTPS 和 SSH 访问的规则。您不需要对数据库安全组的入站规则进行任何更改；默认情况下，允许来自 `sg-11aa22bb` 的所有通信的规则包括 IPv6 通信。

更新安全组规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，并选择您的 Web 服务器安全组。
3. 在 Inbound Rules 选项卡中，选择 Edit。
4. 对于每个规则，选择 Add another rule (再添加一条规则)，完成下面的操作后选择 Save (保存)：例如，要添加允许所有通过 IPv6 的 HTTP 流量的规则，对于 Type (类型)，选择 HTTP，对于 Source (源)，输入 `::/0`。

默认情况下，当您将 IPv6 CIDR 块与 VPC 关联时，会自动向安全组添加一条允许所有 IPv6 流量的出站规则。但是，如果您修改了安全组的原始出站规则，则不会自动添加此规则，您必须为 IPv6 流量添加等效的出站规则。有关更多信息，请参阅[您的 VPC 的安全组 \(p. 119\)](#)。

更新您的网络 ACL 规则

如果您将一个 IPv6 CIDR 块与您的 VPC 关联，则我们会自动向默认网络 ACL 添加规则以允许 IPv6 流量，前提是您未修改其默认规则。如果您修改了默认网络 ACL，或者使用可控制出入子网的流量的规则创建了自定义网络 ACL，则必须手动添加 IPv6 流量规则。有关更多信息，请参阅 [您的 VPC 的推荐网络 ACL 规则 \(p. 138\)](#)。

步骤 4：更改实例类型

当前一代的所有实例类型都支持 IPv6。有关更多信息，请参阅[实例类型](#)。

如果实例类型不支持 IPv6，您必须调整实例的大小以使其成为支持的实例类型。在上述示例中，数据库实例是 m3.large 实例类型，该实例类型不支持 IPv6。您必须将实例大小调整为受支持的实例类型，例如 m4.large。

要调整实例大小，请注意兼容性限制。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[调整实例大小的兼容性](#)。在此方案中，如果数据库实例从使用 HVM 虚拟化的 AMI 中启动，则可使用以下步骤将其大小调整为 m4.large 实例类型。

Important

要调整实例大小，您必须先停止该实例。停止并启动实例会更改该实例的公有 IPv4 地址（如果有）。如果实例存储卷中存储了任何数据，这些数据会被擦除。

调整实例大小

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances，然后选择数据库实例。
3. 依次选择 Actions、Instance State、Stop。
4. 在确认对话框中，选择 Yes, Stop。
5. 在实例处于选中状态时，依次选择 Actions、Instance Settings 和 Change Instance Type。
6. 对于 Instance Type（实例类型），选择新的实例类型，然后选择 Apply（应用）。
7. 要重启已停止的实例，请选择该实例，然后依次选择 Actions、Instance State 和 Start。在确认对话框中，选择 Yes, Start。

如果实例是由实例存储支持的 AMI，则无法使用前面的步骤调整实例大小。这种情况下，可从您的实例中创建一个实例存储支持的 AMI，然后使用新实例类型从您的 AMI 中启动新实例。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[创建实例存储支持的 Linux AMI](#) 和 Amazon EC2 用户指南（适用于 Windows 实例）中的[创建实例存储支持的 Windows AMI](#)。

如果有兼容性限制，您可能无法迁移到新实例类型。例如，如果从使用 PV 虚拟化的 AMI 中启动实例，只有 C3 既支持 PV 虚拟化又支持 IPv6。此实例类型可能不适合您的需要。这种情况下，您可能必须在基础 HVM AMI 上重新安装软件，然后启动新实例。

如果从新 AMI 中启动实例，可在启动过程中为实例分配 IPv6 地址。

步骤 5：为实例分配 IPv6 地址

在确认实例类型支持 IPv6 后，可使用 Amazon EC2 控制台为实例分配 IPv6 地址。该 IPv6 地址将分配给实例的主网络接口 (eth0)。

为实例分配 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。

2. 在导航窗格中，选择 Instances。
3. 选择您的实例，然后依次选择 Actions、Networking 和 Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择 Assign new IP。您可以输入子网范围内的特定 IPv6 地址，也可以保留默认的 Auto-Assign 值，让 Amazon 为您选择一个地址。
5. 选择是，请更新。

或者，如果启动了新实例（例如，如果无法调整实例大小，并且创建了一个新 AMI），则可在启动过程中分配 IPv6 地址。

在启动期间向实例分配 IPv6 地址

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 选择您的 AMI 和 IPv6 兼容实例类型，然后选择 Next: Configure Instance Details。
3. 在 Configure Instance Details 页面上，为 Network 选择一个 VPC，为 Subnet 选择一个子网。对于 Auto-assign IPv6 IP，选择 Enable。
4. 遵循向导中的剩余步骤来启动您的实例。

步骤 6：(可选) 在实例中配置 IPv6

如果使用 Amazon Linux 2016.09.0 或更高版本、Windows Server 2008 R2 或更高版本启动实例，则已经为 IPv6 配置实例，无需执行其他步骤。

如果从另一 AMI 中启动实例，则可能未针对 DHCPv6 进行配置，这意味着您为该实例分配的任何 IPv6 地址在主网络接口中均无法自动识别。要验证是否在您的网络接口上配置了 IPv6 地址，请在 Linux 上使用 ifconfig 命令，或在 Windows 上使用 ipconfig 命令。

可使用以下步骤配置您的实例。您需要使用公有 IPv4 地址连接到您的实例。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[连接到您的 Linux 实例](#)和 Amazon EC2 用户指南（适用于 Windows 实例）中的[连接到您的 Windows 实例](#)。

操作系统

- [Amazon Linux \(p. 112\)](#)
- [Ubuntu \(p. 113\)](#)
- [RHEL/CentOS \(p. 115\)](#)
- [Windows \(p. 116\)](#)

Amazon Linux

在 Amazon Linux 上配置 DHCPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 为您的实例获取最新软件包：

```
sudo yum update -y
```

3. 使用您所选的文本编辑器打开 /etc/sysconfig/network-scripts/ifcfg-eth0，找到下面这一行：

```
IPV6INIT=no
```

用以下内容替换此行：

```
IPV6INIT=yes
```

添加以下两行，保存更改：

```
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
```

4. 打开 /etc/sysconfig/network，删除下面这几行，保存更改：

```
NETWORKING_IPV6=no
IPV6INIT=no
IPV6_ROUTER=no
IPV6_AUTOCONF=no
IPV6_FORWARDING=no
IPV6TO4INIT=no
IPV6_CONTROL_RADVD=no
```

5. 打开 /etc/hosts，用下面的内容替换相关内容，保存更改：

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1          localhost6 localhost6.localdomain6
```

6. 重新启动您的实例。重新连接到您的实例，并使用 ifconfig 命令验证主网络接口是否可识别 IPv6 地址。

Ubuntu

您可以将 Ubuntu 实例配置为动态识别已分配给网络接口的任何 IPv6 地址。如果您的实例没有 IPv6 地址，则此配置可能会导致实例的启动时间延长多达 5 分钟。

必须作为根用户执行这些步骤。

Ubuntu Server 16

在正在运行的 Ubuntu Server 16 实例上配置 IPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 查看 /etc/network/interfaces.d/50-cloud-init.cfg 文件的内容：

```
cat /etc/network/interfaces.d/50-cloud-init.cfg
```

```
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

确认已配置回环网络设备 (lo)，记下网络接口的名称。在此示例中，网络接口名称为 eth0；根据实例类型，此名称可能不同。

3. 创建文件 `/etc/network/interfaces.d/60-default-with-ipv6.cfg` 并添加以下行。如果需要，将 `eth0` 替换为在上一步中检索到的网络接口的名称。

```
iface eth0 inet6 dhcp
```

4. 重启您的实例，或者通过运行以下命令重新启动网络接口。如果需要，将 `eth0` 替换为您的网络接口的名称。

```
sudo ifdown eth0 ; sudo ifup eth0
```

5. 重新连接到您的实例，并使用 `ifconfig` 命令验证网络接口上是否配置了 IPv6 地址。

使用用户数据配置 IPv6

- 您可以启动一个新的 Ubuntu 实例，并通过在启动期间指定以下用户数据来确保分配给该实例的任何 IPv6 地址在网络接口上自动进行配置。

```
#!/bin/bash
echo "iface eth0 inet6 dhcp" >> /etc/network/interfaces.d/60-default-with-ipv6.cfg
dhclient -6
```

在这种情况下，您无需连接到该实例来配置 IPv6 地址。

有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[启动时在 Linux 实例上运行命令](#)。

Ubuntu Server 14

如果您使用 Ubuntu Server 14，则必须提供针对在重启双堆栈网络接口时发生的[已知问题](#)的解决方法（重启导致超时延长，在此期间无法访问您的实例）。

必须作为根用户执行这些步骤。

在正在运行的 Ubuntu Server 14 实例上配置 IPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 编辑 `/etc/network/interfaces.d/eth0.cfg` 文件，使之包含以下内容：

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
    up dhclient -6 $IFACE
```

3. 重新启动您的实例：

```
sudo reboot
```

4. 重新连接到您的实例，并使用 `ifconfig` 命令验证网络接口上是否配置了 IPv6 地址。

启动 DHCPv6 客户端

或者，要在不执行任何额外配置的情况下立即为网络接口添加 IPv6 地址，您可以启动实例的 DHCPv6 客户端。但是，重启后，IPv6 地址不会持久保留在网络接口上。

在 Ubuntu 上启动 DHCPv6 客户端

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 启动 DHCPv6 客户端：

```
sudo dhclient -6
```

3. 使用 `ifconfig` 命令确认主网络接口是否可识别该 IPv6 地址。

RHEL/CentOS

RHEL 7.4 和 CentOS 7 和更高版本使用 `cloud-init` 配置您的网络接口并生成 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件。您可以创建自定义 `cloud-init` 配置文件来启用 DHCPv6，以便生成一个具有会在每次重启后启用 DHCPv6 的设置的 `ifcfg-eth0` 文件。

Note

由于某个已知问题，如果您使用的是具有最新版 `cloud-init-0.7.9` 的 RHEL/CentOS 7.4，这些步骤可能导致您在重启后丢失与实例的连接。作为解决方法，您可以手动编辑 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件。

在 RHEL 7.4 或 CentOS 7 上配置 DHCPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 使用您选择的文本编辑器创建自定义文件，例如：

```
/etc/cloud/cloud.cfg.d/99-custom-networking.cfg
```

3. 向您的文件中添加以下各行，并保存所做更改：

```
network:
  version: 1
  config:
    - type: physical
      name: eth0
      subnets:
        - type: dhcp
        - type: dhcp6
```

4. 重新启动您的实例。
5. 重新连接到您的实例，并使用 `ifconfig` 命令验证网络接口上是否配置了 IPv6 地址。

对于 RHEL 7.3 版和更早版本，您可以使用以下过程直接修改 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件。

在 RHEL 7.3 和更早版本上配置 DHCPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 使用您所选的文本编辑器打开 `/etc/sysconfig/network-scripts/ifcfg-eth0`，找到下面这一行：

```
IPV6INIT="no"
```

用以下内容替换此行：

```
IPV6INIT="yes"
```

添加以下两行，保存更改：

```
DHCPV6C=yes
NM_CONTROLLED=no
```

3. 打开 `/etc/sysconfig/network`，按如下所示添加或修改以下行，然后保存更改：

```
NETWORKING_IPV6=yes
```

4. 通过运行以下命令在您的实例上重启联网：

```
sudo service network restart
```

您可以使用 `ifconfig` 命令验证主网络接口是否可识别 IPv6 地址。

在 RHEL 6 或 CentOS 6 上配置 DHCPv6

1. 使用实例的公有 IPv4 地址连接到您的实例。
2. 按照上面过程中的步骤 2 - 4 操作以配置 RHEL 7/CentOS 7。
3. 如果您重启联网，并且收到指示无法获取 IPv6 地址的错误，则打开 `/etc/sysconfig/network-scripts/ifup-eth` 并找到以下行（默认情况下是行 327）：

```
if /sbin/dhclient "$DHCLIENTARGS"; then
```

删除 `$DHCLIENTARGS` 两侧的引号并保存更改。在您的实例上重启联网：

```
sudo service network restart
```

Windows

使用以下过程在 Windows Server 2003 和 Windows Server 2008 SP2 上配置 IPv6。

要确保 IPv6 优先于 IPv4，请从以下 Microsoft 支持页面下载一个名为 Prefer IPv6 over IPv4 in prefix policies 的修补程序：<https://support.microsoft.com/en-us/help/929852/how-to-disable-ipv6-or-its-components-in-windows>。

在 Windows Server 2003 上启用和配置 IPv6

1. 通过使用 `describe-instances` AWS CLI 命令或通过在 Amazon EC2 控制台中选中实例对应的 IPv6 IP 字段来获取实例的 IPv6 地址。
2. 使用实例的公有 IPv4 地址连接到您的实例。
3. 从您的实例中依次选择开始、控制面板、网络连接和本地连接。
4. 选择属性，然后选择安装。
5. 选择协议，然后选择添加。在网络协议列表中选择 Microsoft TCP/IP 版本 6，然后选择确定。
6. 打开命令提示符并打开 Network shell。

```
netsh
```

7. 切换到 interface IPv6 上下文。

```
interface ipv6
```

8. 使用以下命令，将 IPv6 地址添加至本地连接。使用您的实例的 IPv6 地址替换该 IPv6 地址的值。

```
add address "Local Area Connection" "ipv6-address"
```

例如：

```
add address "Local Area Connection" "2001:db8:1234:1a00:1a01:2b:12:d08b"
```

9. 退出 Network shell。

```
exit
```

10. 使用 ipconfig 命令确认本地连接是否可识别该 IPv6 地址。

在 Windows Server 2008 SP2 上启用和配置 IPv6

1. 通过使用 [describe-instances](#) AWS CLI 命令或通过在 Amazon EC2 控制台中选中实例对应的 IPv6 IP 字段来获取实例的 IPv6 地址。
2. 使用实例的公有 IPv4 地址连接到您的 Windows 实例。
3. 选择开始和控制面板。
4. 打开网络和共享中心，然后打开网络连接。
5. 右键单击局域网（对于网络接口）并选择属性。
6. 选中 Internet 协议版本 6 (TCP/IPv6) 复选框，然后选择确定。
7. 再次打开本地网络的属性对话框。依次选择 Internet 协议版本 6 (TCP/IPv6) 和属性。
8. 选择使用下列 IPv6 地址并执行以下操作：
 - 对于 IPv6 地址，输入您在步骤 1 中获取的 IPv6 地址。
 - 对于子网前缀长度，输入 64。
9. 选择确定，关闭属性对话框。
10. 打开命令提示符。使用 ipconfig 命令确认本地连接是否可识别该 IPv6 地址。

安全性

Amazon Virtual Private Cloud 提供三种功能，以供您用来提高和监控 Virtual Private Cloud (VPC) 的安全性：

- 安全组 — 用作关联 Amazon EC2 实例的防火墙，在实例级别同时控制入站和出站流量
- 网络访问控制列表 (ACL) — 用作关联的子网的防火墙，在子网级别同时控制入站和出站流量
- VPC 流日志 — 捕获有关在您的 VPC 中传入和传出网络接口的 IP 流量的信息。

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，请参阅[您的 VPC 的安全组 \(p. 119\)](#)。

您可以仅利用安全组来确保您的 VPC 实例安全，但您可以添加网络 ACL 以作为连接防御层。有关更多信息，请参阅[网络 ACL \(p. 126\)](#)。

您可以通过创建 VPC、子网或单独的网络接口的流日志来监控传入和传出实例的已接受的 IP 流量和已拒绝的 IP 流量。流日志数据将发布到 CloudWatch Logs，这可帮助您诊断过于严格或过于宽松的安全组和网络 ACL 规则。有关更多信息，请参阅[VPC 流日志 \(p. 165\)](#)。

您可以使用 AWS Identity and Access Management 来控制可以创建和管理安全组、网络 ACL 和流日志的组织成员。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，请参阅[控制访问 Amazon VPC 资源 \(p. 151\)](#)。

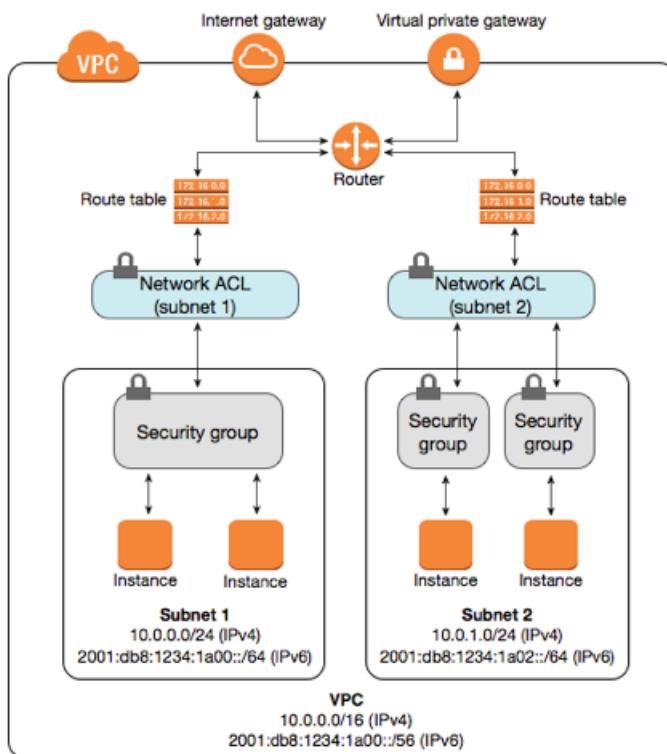
Amazon 安全组和网络 ACL 不筛选在链路本地地址 (169.254.0.0/16) 或 AWS 预留的 IPv4 地址间往返的流量；它们是子网的前四个 IPv4 地址（包括用于该 VPC 的 Amazon DNS 服务器地址）。同样，流日志不捕获在这些地址间往返的 IP 流量。这些地址支持以下服务：域名服务 (DNS)、动态主机配置协议 (DHCP)、Amazon EC2 实例元数据、密钥管理服务器 (KMS — 用于 Windows 实例的许可管理) 和子网中的路由。您可以在您的实例中实施额外的防火墙解决方案，以阻断与本地链接地址间的网络通信。

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
在实例级别运行	在子网级别运行
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
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	自动应用于与之关联的子网中的所有实例（因此，如果安全组规则过于宽松，则需要使用额外的防御层）

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 充当实例的虚拟防火墙以控制入站和出站流量。当您在 VPC 中启动实例时，您可以为该实例最多分配 5 个安全组。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到不同的安全组集合。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 VPC 的安全组及其规则的基本信息。

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，请参阅[安全组与网络 ACL 的比较 \(p. 118\)](#)。

目录

- [安全组基本信息 \(p. 119\)](#)
- [您的 VPC 的默认安全组 \(p. 120\)](#)
- [安全组规则 \(p. 121\)](#)
- [EC2-Classic 和 EC2-VPC 安全组之间的差异 \(p. 122\)](#)
- [使用安全组 \(p. 122\)](#)

安全组基本信息

以下是您的 VPC 安全组的基本特征：

- 系统对您为每个 VPC 创建的安全组数、向每个安全组添加的规则数以及与网络接口关联的安全组数设有限制。有关更多信息，请参阅[Amazon VPC 限制 \(p. 276\)](#)。

- 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。
- 当您创建一个安全组时，它没有入站规则。因此，在您向安全组添加入站规则之前，不允许来自另一台主机的入站流量传输到您的实例。
- 默认情况下，安全组包含允许所有出站流量的出站规则。您可以删除该规则并添加只允许特定出站流量的出站规则。如果您的安全组没有出站规则，则不允许来自您的实例的出站流量。
- 安全组是有状态的 — 如果您从实例发送一个请求，则无论入站安全组规则如何，都将允许该请求的响应流量流入。如果是为响应已允许的入站流量，则该响应可以出站，此时可忽略出站规则。

Note

系统对某些类型的流量使用了不同于其他流量的跟踪方式。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[连接跟踪](#)。

- 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）。
- 安全组与网络接口关联。在您启动实例之后，您可以更改与该实例关联的安全组，从而更改与主网络接口（eth0）关联的安全组。您还可以更改与任何其他网络接口关联的安全组。有关网络接口的更多信息，请参阅[弹性网络接口](#)。
- 创建安全组时，您必须为其提供名称和描述。以下规则适用：
 - 名称和描述的长度最多为 255 个字符。
 - 名称和描述只能使用以下字符：a-z、A-Z、0-9、空格和 _-:/()#,@[]+=&{}!\$*。
 - 安全组名称不能以 sg- 开头。
 - 安全组名称在 VPC 中必须是唯一的。

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没有指定其他安全组，我们会将默认安全组与您的实例相关联。

Note

如果您在 Amazon EC2 控制台中启动实例，则启动实例向导会自动定义“`launch-wizard-xx`”安全组，您可以将该安全组与实例关联，而非默认安全组。

下表介绍默认安全组的默认规则。

Inbound			
Source	Protocol	Port Range	Comments
安全组 ID (sg-xxxxxxxx)	全部	全部	允许从分配给同一安全组的实例发来的入站流量。
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	全部	全部	允许所有的出站 IPv4 流量。
::/0	全部	全部	允许所有的出站 IPv6 流量。如果您创建了具有 IPv6 CIDR 块的 VPC 或向现有的 VPC 关联了 IPv6 CIDR 块，则系统默认添加此规则。

您可以更改默认安全组的规则。

您无法删除默认安全组。如果您尝试删除默认安全组，会显示以下错误：Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user。

Note

如果您修改了安全组的出站规则，则当您向 VPC 关联 IPv6 块时，我们不会为 IPv6 流量自动添加出站规则。

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。您可以授予对某个特定 CIDR 范围或 VPC 或对等 VPC（需要 VPC 对等连接）中的其他安全组的访问权限。

以下是 VPC 中安全组规则的基本部分：

- （仅限入站规则）流量源和目标端口或端口范围。源可以是另一个安全组、IPv4 或 IPv6 CIDR 块或单个 IPv4 或 IPv6 地址。
- （仅限出站规则）流量目标和目标端口或端口范围。目标可以是另一个安全组、一个 IPv4 或 IPv6 CIDR 块、单个 IPv4 或 IPv6 地址，或前缀列表 ID（服务由前缀列表标识，即区域的服务的名称和 ID）。
- 任何有标准协议编号的协议（有关具体列表，请参阅[协议编号](#)）。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。
- 安全组规则的可选描述，可帮助您以后识别它。描述的长度最多为 255 个字符。允许的字符包括 a-z、A-Z、0-9、空格和 _-:/(#,@[]+=;!)\$*。

将 CIDR 块指定为规则的源时，将会允许从指定的协议和端口的特定地址进行通信。将安全组指定为规则的源时，将会允许从与指定协议和端口的源安全组关联的实例的弹性网络接口（ENI）进行通信。将安全组添加为源不会从源安全组添加规则。

如果指定单个 IPv4 地址，请使用 /32 前缀长度指定该地址。如果指定单个 IPv6 地址，请使用 /128 前缀长度指定该地址。

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。

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。

您添加的规则类型可能取决于该实例的用途。下表介绍 Web 服务器的安全组的示例规则。Web 服务器可接收来自所有 IPv4 和 IPv6 地址的 HTTP 及 HTTPS 流量，并将 SQL 或 MySQL 流量发送到数据库服务器。

Inbound			
Source	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	允许从所有 IPv4 地址进行入站 HTTP 访问
::/0	TCP	80	允许从所有 IPv6 地址进行入站 HTTP 访问
0.0.0.0/0	TCP	443	允许从所有 IPv4 地址进行入站 HTTPS 访问
::/0	TCP	443	允许从所有 IPv6 地址进行入站 HTTPS 访问
您网络的公有 IPv4 地址范围	TCP	22	允许从您的网络中的 IPv4 IP 地址对 Linux 实例进行入站 SSH 访问（通过 Internet 网关）

您网络的公有 IPv4 地址范围	TCP	3389	允许从您的网络中的 IPv4 IP 地址对 Windows 实例进行入站 RDP 访问 (通过 Internet 网关)
Outbound			
Destination	Protocol	Port Range	Comments
Microsoft SQL Server 数据库服务器的安全组的 ID	TCP	1433	允许 Microsoft SQL Server 出站访问指定安全组中的实例
MySQL 数据库服务器的安全组的 ID	TCP	3306	允许 MySQL 出站访问指定安全组中的实例

数据库服务器需要不同的规则集；例如，您可以添加一个规则以允许入站 MySQL 或 Microsoft SQL Server 访问（而不是入站 HTTP 和 HTTPS 流量）。有关 Web 服务器和数据库服务器的安全组规则示例，请参阅[安全性 \(p. 46\)](#)。

有关特定种类访问的安全组规则示例，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[安全组规则引用](#)。

过时的安全组规则

如果您的 VPC 具有与其他 VPC 的 VPC 对等连接，则安全组规则可引用对等 VPC 中的其他安全组。这使与已引用的安全组关联的实例能够和与正在引用的安全组关联的实例进行通信。

如果对等 VPC 的所有者删除引用的安全组，或者您或对等 VPC 的所有者删除 VPC 对等连接，则安全组规则将标记为 `stale`。与任何其他的安全组规则一样，您可以删除过时的安全组规则。

有关更多信息，请参阅 Amazon VPC Peering Guide 中的[使用过时的安全组](#)。

EC2-Classic 和 EC2-VPC 安全组之间的差异

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。有关用于 EC2-Classic 的安全组和用于 VPC 的安全组之间的区别的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[EC2-Classic 和 VPC 之间的区别](#)。

使用安全组

以下任务为您展示如何使用 Amazon VPC 控制台来处理安全组。

任务

- [修改默认安全组 \(p. 122\)](#)
- [创建安全组 \(p. 123\)](#)
- [添加、删除和更新规则 \(p. 123\)](#)
- [更改实例的安全组 \(p. 124\)](#)
- [删除安全组 \(p. 125\)](#)
- [删除“2009-07-15-default”安全组 \(p. 125\)](#)

修改默认安全组

您的 VPC 包括一个[默认安全组 \(p. 120\)](#)。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，请参阅[添加、删除和更新规则 \(p. 123\)](#)。

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。

使用控制台创建安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 输入安全组的名称（例如，`my-security-group`）并提供说明。从 VPC 菜单中选择您 VPC 的 ID，然后选择 Yes, Create。

使用命令行创建安全组

- `create-security-group` (AWS CLI)
- `New-EC2SecurityGroup` (适用于 Windows PowerShell 的 AWS 工具)

使用命令行描述一个或多个安全组

- `describe-security-groups` (AWS CLI)
- `Get-EC2SecurityGroup` (适用于 Windows PowerShell 的 AWS 工具)

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、删除和更新规则

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。

如果您有 VPC 对等连接，则可以从对等 VPC 中引用安全组作为您的安全组规则中的源或目标。有关更多信息，请参阅 Amazon VPC Peering Guide 中的[更新安全组以引用对等 VPC 安全组](#)。

使用控制台添加规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择需要更新的安全组。
4. 依次选择 Actions (操作)、Edit inbound rules (编辑入站规则)，或 Actions (操作)、Edit outbound rules (编辑出站规则)。
5. 对于 Type (类型)，选择流量类型，然后填写所需信息。例如，对于公有 Web 服务器，选择 HTTP 或 HTTPS，并将 Source 的值指定为 `0.0.0.0/0`。

Note

如果您使用 `0.0.0.0/0`，则允许所有 IPv4 地址使用 HTTP 或 HTTPS 访问您的实例。要限制访问，则输入特定 IP 地址或地址范围。

6. 还可允许在所有与此安全组关联的实例之间进行通信。使用以下选项创建入站规则：
 - Type (类型) : All Traffic (所有流量)
 - Source (来源) : 输入安全组的 ID。
7. 选择 Save rules (保存规则)。

使用控制台删除规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择需要更新的安全组。
4. 依次选择 Actions (操作)、Edit inbound rules (编辑入站规则)，或 Actions (操作)、Edit outbound rules (编辑出站规则)。
5. 选择您希望删除的规则右侧的删除按钮 (“x”)。
6. 选择 Save rules (保存规则)。

使用控制台修改现有安全组规则的协议、端口范围或者源或目标时，控制台会删除现有规则并为您添加新规则。

使用控制台更新规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择需要更新的安全组。
4. 依次选择 Actions (操作)、Edit inbound rules (编辑入站规则)，或 Actions (操作)、Edit outbound rules (编辑出站规则)。
5. 根据需要修改规则条目。
6. 选择 Save rules (保存规则)。

要使用 Amazon EC2 API 或命令行工具更新现有规则的协议、端口范围或者源或目标，您就无法修改规则；相反，您必须删除该现有规则并添加新规则。要仅更新规则描述，您可以使用 [update-security-group-rule-descriptions-ingress](#) 和 [update-security-group-rule-descriptions-egress](#) 命令。

使用命令行向安全组添加规则

- [authorize-security-group-ingress](#) 和 [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) 和 [Grant-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行从安全组中删除规则

- [revoke-security-group-ingress](#) 和 [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) 和 [Revoke-EC2SecurityGroupEgress](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行更新安全组规则的描述

- [update-security-group-rule-descriptions-ingress](#) 和 [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) 和 [Update-EC2SecurityGroupRuleEgressDescription](#) (适用于 Windows PowerShell 的 AWS 工具)

更改实例的安全组

在将实例启动到 VPC 中后，您可以更改与该实例关联的安全组。当实例处于 `running` 或 `stopped` 状态时，您可以更改实例的安全组。

Note

此过程会更改与实例的主网络接口 (eth0) 关联的安全组。要更改其他网络接口的安全组，请参阅[更改网络接口的安全组](#)。

使用控制台更改实例的安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 打开实例的上下文 (右键单击) 菜单，选择 Networking、Change Security Groups。
4. 在 Change Security Groups 对话框中，从该列表中选择一个或多个安全组，然后选择 Assign Security Groups。

使用命令行更改实例的安全组

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

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[更改实例的安全组 \(p. 124\)](#))。您无法删除默认安全组。

如果您使用控制台，则可以一次删除多个安全组。如果您使用命令行或 API，则一次只能删除一个安全组。

使用控制台删除安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups。
3. 选择一个或多个安全组，然后选择 Security Group Actions、Delete Security Group。
4. 在 Delete Security Group 对话框中，选择 Yes, Delete。

使用命令行删除安全组

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (适用于 Windows PowerShell 的 AWS 工具)

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. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
 - b. 在导航窗格中，选择 Network Interfaces。

- c. 从该列表中选择实例的网络接口，然后选择 Change Security Groups、Actions。
- d. 在 Change Security Groups 对话框中，从该列表中选择一个新的安全组，然后选择 Save。

Note

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
3. 在导航窗格中，选择 Security Groups。
4. 选择 2009-07-15-default 安全组，然后选择 Security Group Actions (安全组操作)、Delete Security Group (删除安全组)。
5. 在 Delete Security Group 对话框中，选择 Yes, Delete。

网络 ACL

网络访问控制列表 (ACL) 是 VPC 的一个可选安全层，可用作防火墙来控制进出一个或多个子网的流量。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，请参阅[安全组与网络 ACL 的比较 \(p. 118\)](#)。

目录

- [网络 ACL 基本信息 \(p. 126\)](#)
- [网络 ACL 规则 \(p. 127\)](#)
- [默认网络 ACL \(p. 127\)](#)
- [自定义网络 ACL \(p. 128\)](#)
- [临时端口 \(p. 131\)](#)
- [使用网络 ACL \(p. 131\)](#)
- [示例：控制对子网中实例的访问 \(p. 134\)](#)
- [API 和命令概览 \(p. 137\)](#)

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：

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

有关更多信息，请参阅 [Amazon VPC 限制 \(p. 276\)](#)。

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。只要有一条规则与流量匹配，即应用该规则，并忽略与之冲突的任意更高编号的规则。
- 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，请参阅[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。
- 针对特定流量选择 ALLOW 或 DENY。

默认网络 ACL

默认网络 ACL 配置为让所有流量流进和流出与其关联的子网。每个网络 ACL 还包含一个规则编号是星号的规则。此规则确保在数据包不匹配任何其他编号规则时拒绝该数据包。您可以修改或删除此规则。

下面是一个仅支持 IPv4 的示例默认网络 ACL。

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

如果您创建具有 IPv6 CIDR 块的 VPC 或将 IPv6 CIDR 块与您的现有 VPC 关联，我们会自动添加允许所有 IPv6 流量流入和流出您的子网的规则。我们还会添加规则编号为星号的规则，该规则可确保拒绝与任何其他编号规则不符的数据包。您不能修改或删除这些规则。下面是一个支持 IPv4 和 IPv6 的 VPC 的示例默认网络 ACL。

Note

如果您修改了您的默认网络 ACL 的入站规则，在您将 IPv6 块与您的 VPC 关联时，我们不会为入站 IPv6 流量自动添加 ALLOW 规则。同样，如果您修改了出站规则，我们不会为出站 IPv6 流量自动添加 ALLOW 规则。

入站					
规则 #	类型	协议	端口范围	源	允许/拒绝
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允许
101	所有 IPv6 流量	全部	全部	::/0	允许

*	所有流量	全部	全部	0.0.0.0/0	拒绝
*	所有 IPv6 流量	全部	全部	::/0	拒绝
出站					
规则 #	类型	协议	端口范围	目的地	允许/拒绝
100	所有流量	全部	全部	0.0.0.0/0	允许
101	所有 IPv6 流量	全部	全部	::/0	允许
*	所有流量	全部	全部	0.0.0.0/0	拒绝
*	所有 IPv6 流量	全部	全部	::/0	拒绝

自定义网络 ACL

下表显示了一个仅支持 IPv4 的 VPC 的自定义网络 ACL 示例。其中包括允许 HTTP 和 HTTPS 数据流进入的规则（入站规则 100 和 110）。存在相应的出站规则，以允许响应入站数据流（出站规则 120，适用于临时端口 32768-65535）。有关如何选择适当的临时端口的更多信息，请参阅[临时端口 \(p. 131\)](#)。

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 32768-65535）。

Note

每个网络 ACL 都包含一个默认规则，其规则编号是星号。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 #	类型	协议	端口范围	源	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTP 流量。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTPS 流量。
120	SSH	TCP	22	192.0.2.0/24	允许	允许来自您的家庭网络的公有 IPv4 地址范围的入站 SSH 流量（通过 Internet 网关）。
130	RDP	TCP	3389	192.0.2.0/24	允许	允许从您的家庭网络的公有 IPv4 地址范围到 Web 服务器的入站 RDP 流量（通过 Internet 网关）。
140	自定义 TCP	TCP	32768-65535	0.0.0.0/0	允许	允许来自 Internet 的入站返回 IPv4 流量（即源自子网的请求）。 此范围仅为示例。有关如何选择适当的临时

						端口的更多信息，请参阅 临时端口 (p. 131) 。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv4 流量。
出站						
规则 #	类型	协议	端口范围	目的地	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许出站 IPv4 HTTP 流量从子网流向 Internet。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许出站 IPv4 HTTPS 流量从子网流向 Internet。
120	自定义 TCP	TCP	32768-655350.0.0.0/0		允许	允许对 Internet 客户端的出站 IPv4 响应(例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参阅 临时端口 (p. 131) 。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv4 流量。

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)。当数据包目标为 SSL 端口(443)时，评估过程如下。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)，则它与任何规则均不匹配，而且“*”规则最终会拒绝这个数据包。

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。

Important

借助 Elastic Load Balancing，如果您的后端实例的子网有一个网络 ACL，并且您在其中针对源为 0.0.0.0/0 或子网的 CIDR 的所有流量添加了 DENY 规则，则您的负载均衡器将无法对这些实例执行运行状况检查。有关负载均衡器和后端实例的推荐网络 ACL 规则的更多信息，请参阅Classic Load Balancer 用户指南中的[VPC 中负载均衡器的网络 ACL](#)。

下表显示了关联有 IPv6 CIDR 块的 VPC 的自定义网络 ACL 的相同示例。此网络 ACL 包含适用于所有 IPv6 HTTP 和 HTTPS 流量的规则。在本例中，新规则插入在 IPv4 流量的现有规则之间；不过，您也可以在 IPv4 规则之后添加编号更高的规则。IPv4 和 IPv6 流量是独立的；因此，所有 IPv4 流量规则都不适用于 IPv6 流量。

入站						
规则 #	类型	协议	端口范围	源	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTP 流量。

105	HTTP	TCP	80	::/0	允许	允许来自任意 IPv6 地址的入站 HTTP 流量。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许来自任意 IPv4 地址的入站 HTTPS 流量。
115	HTTPS	TCP	443	::/0	允许	允许来自任意 IPv6 地址的入站 HTTPS 流量。
120	SSH	TCP	22	192.0.2.0/24	允许	允许来自您的家庭网络的公有 IPv4 地址范围的入站 SSH 流量 (通过 Internet 网关)。
130	RDP	TCP	3389	192.0.2.0/24	允许	允许从您的家庭网络的公有 IPv4 地址范围到 Web 服务器的入站 RDP 流量 (通过 Internet 网关)。
140	自定义 TCP	TCP	32768-65535	0.0.0.0/0	允许	允许来自 Internet 的入站返回 IPv4 流量 (即源自子网的请求)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参阅 临时端口 (p. 131) 。
145	自定义 TCP	TCP	32768-65535	::/0	允许	允许来自 Internet 的入站返回 IPv6 流量 (即源自子网的请求)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参阅 临时端口 (p. 131) 。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv4 流量。
*	所有流量	全部	全部	::/0	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
出站						
规则 #	类型	协议	端口范围	目的地	允许/拒绝	注释
100	HTTP	TCP	80	0.0.0.0/0	允许	允许出站 IPv4 HTTP 流量从子网流向 Internet。
105	HTTP	TCP	80	::/0	允许	允许出站 IPv6 HTTP 流量从子网流向 Internet。
110	HTTPS	TCP	443	0.0.0.0/0	允许	允许出站 IPv4 HTTPS 流量从子网流向 Internet。

115	HTTPS	TCP	443	::/0	允许	允许出站 IPv6 HTTPS 流量从子网流向 Internet。
120	自定义 TCP	TCP	32768-65535	0.0.0.0/0	允许	允许对 Internet 客户端的出站 IPv4 响应 (例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参阅 临时端口 (p. 131) 。
125	自定义 TCP	TCP	32768-65535	::/0	允许	允许对 Internet 客户端的出站 IPv6 响应 (例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关如何选择适当的临时端口的更多信息，请参阅 临时端口 (p. 131) 。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv4 流量。
*	所有流量	全部	全部	::/0	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

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 32768-65535。但是，您可能需要根据自己使用的或作为通信目标的客户端的类型为网络 ACL 使用不同的范围。

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 及更高版本使用端口 49152-65535。NAT 网关使用端口 1024 - 65535。例如，如果一个来自 Internet 上的 Windows XP 客户端的请求到达您的 VPC 中的 Web 服务器，则您的网络 ACL 必须有相应的出站规则，以支持目标为端口 1025-5000 的数据流。

如果您的 VPC 中的一个实例是发起请求的客户端，则您的网络 ACL 必须有入站规则来支持发送到实例类型（Amazon Linux、Windows Server 2008 等）特有的临时端口的数据流。

在实际中，为使不同客户端类型可以启动流量进入您 VPC 中的公有实例，您可以开放临时端口 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。请务必把 DENY 规则放在表的较前端，先于开放一系列临时端口的 ALLOW 规则。

使用网络 ACL

以下任务为您展示如何使用 Amazon VPC 控制台来处理网络 ACL。

任务

- [确定网络 ACL 关联 \(p. 132\)](#)

- 正在创建网络 ACL (p. 132)
- 正在添加和删除规则 (p. 132)
- 正在将子网与网络 ACL 关联 (p. 133)
- 解除网络 ACL 与子网的关联 (p. 133)
- 更改子网的网络 ACL (p. 134)
- 正在删除网络 ACL (p. 134)

确定网络 ACL 关联

您可以使用 Amazon VPC 控制台来确定与某个子网关联的网络 ACL。网络 ACL 可与多个子网关联，因此，您还可以确定与某个网络 ACL 关联的子网。

确定与某个子网关联的网络 ACL

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets，然后选择子网。

Network ACL (网络 ACL) 中已包含与子网相关联的网络 ACL 以及网络 ACL 的规则。

判断与网络 ACL 关联的特定子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Network ACLs。Associated With 列指示每个网络 ACL 的关联子网的数目。
3. 选择网络 ACL。
4. 在详细信息窗格中，选择 Subnet Associations 可显示与网络 ACL 关联的子网。

正在创建网络 ACL

您可以为 VPC 创建自定义网络 ACL。默认情况下，您创建的网络 ACL 将阻止所有入站和出站流量（直到您添加规则），且不与任何子网关联（直到您为其显式关联子网）。

创建网络网络 ACL

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Network ACLs。
3. 选择 Create Network ACL。
4. 在 Create Network ACL 对话框中，可以选择为您的网络 ACL 命名，从 VPC 列表中选择 VPC 的 ID，然后选择 Yes, Create。

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。

如果您使用的是 Amazon EC2 API 或命令行工具，则无法修改规则；您只能添加和删除规则。如果您使用的是 Amazon VPC 控制台，则可以修改现有规则的条目（该控制台删除该规则并为您添加新规则）。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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Network ACLs。
3. 在详细信息窗格中，根据需要添加的规则的类型，选择 Inbound Rules 或 Outbound Rules 选项卡，然后选择 Edit。
4. 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）。这会让添加新规则变得更加简单，无需对现有规则重新编号。

5. 从 Type 列表中选择规则。例如，要为 HTTP 添加规则，请选择 HTTP。如需添加规则以允许所有 TCP 流量，请选择 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，请选择 Custom Protocol Rule。
6. （可选）如果要创建自定义协议规则，请从 Protocol 列表中选择协议的编号和名称。有关更多信息，请参阅[IANA List of Protocol Numbers](#)。
7. （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）。
8. 在 Source 或 Destination 字段中（根据是入站规则还是出站规则），输入规则适用的 CIDR 范围。
9. 从 Allow/Deny（允许/拒绝）列表中，选择 ALLOW（允许）以允许指定数据流，或选择 DENY（拒绝）以拒绝指定数据流。
10. （可选）要添加其他规则，请选择 Add another rule，然后根据需要重复步骤 4 至 9。
11. 完成此操作后，选择 Save。

从网络 ACL 删除规则

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Network ACLs，然后选择网络 ACL。
3. 在详细信息窗格中，选择 Inbound Rules 或 Outbound Rules 选项卡，然后选择 Edit。为要删除的规则选择 Remove，然后选择 Save。

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Network ACLs，然后选择网络 ACL。
3. 在详细信息窗格中的 Subnet Associations 选项卡上，选择 Edit。选中要与网络 ACL 关联的子网的 Associate 复选框，然后选择 Save。

解除网络 ACL 与子网的关联

您可以解除自定义网络 ACL 与子网的关联 — 解除关联后，该子网将自动关联到默认网络 ACL。

解除子网与网络 ACL 的关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Network ACLs，然后选择网络 ACL。
3. 在详细信息窗格中，选择 Subnet Associations 选项卡。
4. 选择 Edit，然后取消选中子网的 Associate 复选框。选择 Save。

更改子网的网络 ACL

您可以更改与某个子网关联的网络 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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets，然后选择子网。
3. 选择 Network ACL 选项卡，然后选择 Edit。
4. 从 Change to 列表中选择要与子网关联的网络 ACL，然后选择 Save。

正在删除网络 ACL

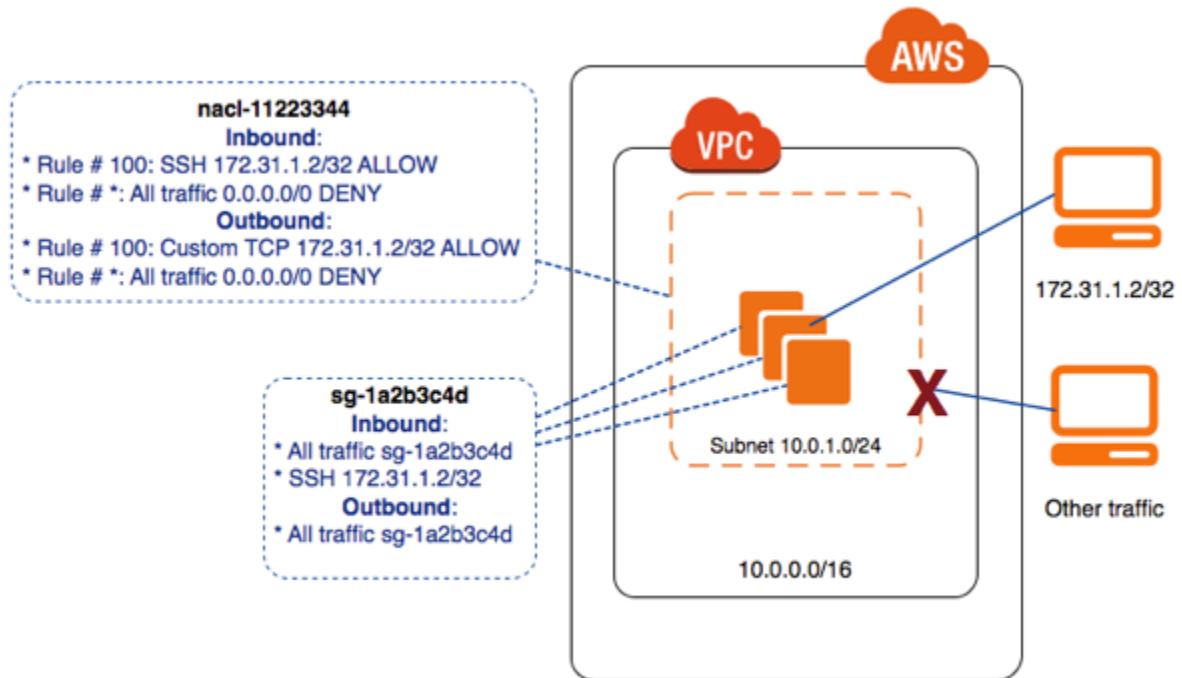
您只可以删除未与任何子网关联的网络 ACL。您无法删除默认网络 ACL。

删除网络 ACL

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Network ACLs。
3. 选择网络 ACL，然后选择 Delete。
4. 在确认对话框中，选择 Yes, Delete。

示例：控制对子网中实例的访问

在本示例中，子网中的任意两个实例可相互通信，并可从受信任的远程计算机访问它们。远程计算机可以是本地网络中的计算机、另一个子网中的实例或用于连接实例以执行管理任务的 VPC。安全组规则和网络 ACL 规则允许从远程计算机 (172.31.1.2/32) 的 IP 地址进行访问。来自 Internet 或其他网络的所有其他流量会被拒绝。



所有实例使用同一个安全组 (sg-1a2b3c4d)，均遵守以下规则。

入站规则

协议类型	协议	端口范围	源	注释
所有流量	全部	全部	sg-1a2b3c4d	允许关联到同一个安全组的实例相互通信。
SSH	TCP	22	172.31.1.2/32	允许远程计算机进行入站 SSH 访问。如果实例是 Windows 计算机，则该规则必须对端口 3389 改用 RDP 协议。

出站规则

协议类型	协议	端口范围	目的地	注释
所有流量	全部	全部	sg-1a2b3c4d	允许关联到同一个安全组的实例相互通信。

该子网关联到具有以下规则的网络 ACL。

入站规则

规则 #	类型	协议	端口范围	源	允许/拒绝	注释

100	SSH	TCP	22	172.31.1.2/32	允许	允许远程计算机的入站流量。如果实例是 Windows 计算机，则该规则必须对端口 3389 改用 RDP 协议。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝与前一条规则不符的所有其他入站流量。

出站规则

规则 #	类型	协议	端口范围	目的地	允许/拒绝	注释
100	自定义 TCP	TCP	1024-65535	172.31.1.2/32	允许	允许到远程计算机的出站响应。网络 ACL 是无状态的，因此需要该规则才能允许针对入站请求的响应流量。
*	所有流量	全部	全部	0.0.0.0/0	拒绝	拒绝不匹配前一条规则的所有其他出站流量。

该方案让您能够灵活地更改实例的安全组或安全组规则，并使用网络 ACL 作为备份防御层。该网络 ACL 规则应用到子网中的所有实例，因此，就算您不小心设置了过于宽松的安全组规则，网络 ACL 规则也会继续生效，只允许来自单一 IP 地址的访问。例如，以下规则比之前的规则更加宽松 — 它们允许来自任意 IP 地址的入站 SSH 访问。

入站规则

类型	协议	端口范围	源	注释
所有流量	全部	全部	sg-1a2b3c4d	允许关联到同一个安全组的实例相互通信。
SSH	TCP	22	0.0.0.0/0	允许来自任意 IP 地址的 SSH 访问。

出站规则

类型	协议	端口范围	目的地	注释

所有流量	全部	全部	0.0.0.0/0	允许所有出站流量。
------	----	----	-----------	-----------

但是，只有该子网中的其他实例和您的远程计算机能够访问该实例。网络 ACL 规则仍会阻止到该子网的所有入站流量，当然，您的远程计算机除外。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

为您的 VPC 创建网络 ACL

- [create-network-acl](#) (AWS CLI)
- [New-EC2NetworkAcl](#) (适用于 Windows PowerShell 的 AWS 工具)

说明您的一个或多个网络 ACL

- [describe-network-acls](#) (AWS CLI)
- [Get-EC2NetworkAcl](#) (适用于 Windows PowerShell 的 AWS 工具)

向网络 ACL 添加规则

- [create-network-acl-entry](#) (AWS CLI)
- [New-EC2NetworkAclEntry](#) (适用于 Windows PowerShell 的 AWS 工具)

从网络 ACL 中删除规则

- [delete-network-acl-entry](#) (AWS CLI)
- [Remove-EC2NetworkAclEntry](#) (适用于 Windows PowerShell 的 AWS 工具)

替换网络 ACL 中的现有规则

- [replace-network-acl-entry](#) (AWS CLI)
- [Set-EC2NetworkAclEntry](#) (适用于 Windows PowerShell 的 AWS 工具)

替换网络 ACL 关联

- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (适用于 Windows PowerShell 的 AWS 工具)

删除网络 ACL

- [delete-network-acl](#) (AWS CLI)
- [Remove-EC2NetworkAcl](#) (适用于 Windows PowerShell 的 AWS 工具)

您的 VPC 的推荐网络 ACL 规则

VPC 向导帮助您实现 Amazon VPC 的常见方案。如果按文档所述的那样实现这些方案，则将使用默认网络访问控制列表 (ACL) ，其中允许所有入站和出站流量。如果需要增加一层安全防护，则可创建网络 ACL 并添加规则。有关更多信息，请参阅[网络 ACL \(p. 126\)](#)。

我们建议对每个场景使用以下规则。

建议

- [场景 1 的推荐规则 \(p. 138\)](#)
- [场景 2 的推荐规则 \(p. 140\)](#)
- [场景 3 的推荐规则 \(p. 145\)](#)
- [场景 4 的推荐规则 \(p. 150\)](#)

注意事项

- 我们对 NAT 网关使用例如 32768-65535 或 1024-65535 的临时端口范围。您必须为您选择的配置适合的大小。有关更多信息，请参阅[临时端口 \(p. 131\)](#)。
- 如果您子网中主机间的最大传输单位 (MTU) 不同，您必须添加以下入站和出站网络 MTU 规则，以便确保路径 MTU 发现可正常工作并防止数据包丢失：选择自定义 ICMP 规则作为类型，并选择无法访问目标和需要分段，DF 标志已设置作为端口范围（类型 3，代码 4）。如果您使用 traceroute，还需添加以下规则：选择自定义 ICMP 规则作为类型，并选择超时和 TTL 中转过期作为端口范围（类型 11，代码 0）。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[EC2 实例的网络最大传输单位 \(MTU\)](#)。

场景 1 的推荐规则

场景 1 是一个子网，其中的实例可接收和发送 Internet 流量。有关更多信息，请参阅[场景 1：带单个公有子网的 VPC \(p. 23\)](#)。

下表显示我们推荐制定的规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许来自任意 IPv4 地址的入站 HTTP 流量。
110	0.0.0.0/0	TCP	443	允许	允许来自任意 IPv4 地址的入站 HTTPS 流量。
120	您的家庭网络的公有 IPv4 地址范围	TCP	22	允许	允许来自您的家庭网络的入站 SSH 流量（通过 Internet 网关）。
130	您的家庭网络的公有 IPv4 地址范围	TCP	3389	允许	允许来自您的家庭网络的入站 RDP 流量（通过 Internet 网关）。
140	0.0.0.0/0	TCP	32768-65535	允许	允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。

					此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
110	0.0.0.0/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
120	0.0.0.0/0	TCP	32768-65535	允许	允许对 Internet 客户端进行出站响应(例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv4 流量。

适用于 IPv6 的推荐规则

如果您实现了支持 IPv6 的场景 1 并创建了具有关联 IPv6 CIDR 块的 VPC 和子网，则必须向网络 ACL 添加单独的规则，以控制入站和出站 IPv6 流量。

以下是您的网络 ACL 的 IPv6 特定规则(除了上面列出的规则以外)。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允许	允许来自任意 IPv6 地址的入站 HTTP 流量。
160	::/0	TCP	443	允许	允许来自任意 IPv6 地址的入站 HTTPS 流量。
170	您的家庭网络的 IPv6 地址范围	TCP	22	允许	允许来自您的家庭网络的入站 SSH 流量(通过 Internet 网关)。
180	您的家庭网络的 IPv6 地址范围	TCP	3389	允许	允许来自您的家庭网络的入站 RDP 流量(通过 Internet 网关)。

190	::/0	TCP	32768-65535	允许	允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
140	::/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
150	::/0	TCP	32768-65535	允许	允许对 Internet 客户端进行出站响应(例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

场景 2 的推荐规则

场景 2 是一个公有子网，其中的实例可接收和发送 Internet 流量，以及一个私有子网，它无法直接从 Internet 收到流量。但是，它可以通过公有子网中的 NAT 网关或 NAT 实例启动发送到 Internet 的数据流(并接收响应)。有关更多信息，请参阅[场景 2：带有公有子网和私有子网\(NAT\)的 VPC \(p. 29\)](#)。

在这个场景中，您的公有子网有网络 ACL，私有子网有另一个单独的网络 ACL。下表显示我们推荐为每个 ACL 制定的规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。它们大多会在场景中模拟安全组规则。

公有子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许来自任意 IPv4 地址的入站 HTTP 流量。
110	0.0.0.0/0	TCP	443	允许	允许来自任意 IPv4 地址的入站 HTTPS 流量。

120	您家庭网络的公共 IP 地址范围	TCP	22	允许	允许来自您的家庭网络的入站 SSH 流量 (通过 Internet 网关)。
130	您家庭网络的公共 IP 地址范围	TCP	3389	允许	允许来自您的家庭网络的入站 RDP 流量 (通过 Internet 网关)。
140	0.0.0.0/0	TCP	1024-65535	允许	允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的入站 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
110	0.0.0.0/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。
140	0.0.0.0/0	TCP	32768-65535	允许	允许对 Internet 客户端进行出站响应 (例如，向访问子网中的 Web 服务器的人员提供网页)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
150	10.0.1.0/24	TCP	22	允许	允许对您的私有子网中的实例 (从 SSH 堡垒实例，如果有) 进行出站 SSH 访问。

*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站 IPv4 流量。
---	-----------	----	-----	----	----------------------------------

私有子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。
120	10.0.0.0/24	TCP	22	允许	允许来自公有子网的 SSH 堡垒实例的入站 SSH 流量 (如果有)。
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	0.0.0.0/0	TCP	1024-65535	允许	允许从公有子网中的 NAT 设备返回的入站流量，以处理源于私有子网的请求。 有关如何指定正确的临时端口的信息，请参阅本主题开始部分的重要说明。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的 IPv4 入站流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
110	0.0.0.0/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
120	10.0.0.0/24	TCP	32768-65535	允许	允许对公有子网的出站响应 (例如，响应与私有子网中的数据库服务器通信的公有子网中的 Web 服务器)。

					此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv4 流量。

适用于 IPv6 的推荐规则

如果您实现了支持 IPv6 的场景 2 并创建了具有关联 IPv6 CIDR 块的 VPC 和子网，则必须向网络 ACL 添加单独的规则，以控制入站和出站 IPv6 流量。

以下是您的网络 ACL 的 IPv6 特定规则(除了上面列出的规则以外)。

公有子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允许	允许来自任意 IPv6 地址的入站 HTTP 流量。
160	::/0	TCP	443	允许	允许来自任意 IPv6 地址的入站 HTTPS 流量。
170	您的家庭网络的 IPv6 地址范围	TCP	22	允许	允许来自您的家庭网络的通过 IPv6 的入站 SSH 流量(通过 Internet 网关)。
180	您的家庭网络的 IPv6 地址范围	TCP	3389	允许	允许来自您的家庭网络的通过 IPv6 的入站 RDP 流量(通过 Internet 网关)。
190	::/0	TCP	1024-65535	允许	允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。

Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
160	::/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
170	::/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet

180	2001:db8:1234: T601 ::/64	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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。
200	::/0	TCP	32768-65535	允许 允许对 Internet 客户端进行出站响应 (例如，向访问子网中的 Web 服务器的人员提供网页) 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
210	2001:db8:1234: T601 ::/64	22	允许	允许对您的私有子网中的实例 (从 SSH 堡垒实例，如果有) 进行出站 SSH 访问。
*	::/0	all	all	拒绝 拒绝所有未经前置规则 (不可修改) 处理的出站 IPv6 流量。

私有子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234: T600 ::/64	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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。	
170	2001:db8:1234: T600 ::/64	22	允许	允许来自公有子网的 SSH 堡垒实例的入站 SSH 流量 (如果适用)。	
180	2001:db8:1234: T600 ::/64	3389	允许	允许公有子网的 Microsoft Terminal Services 网关的入站 RDP 流量 (如果适用)。	

190	::/0	TCP	1024-65535	允许	允许从仅出口 Internet 网关返回的入站流量，以处理源于私有子网的请求。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
140	::/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
150	2001:db8:1234: 1600 ::/64		32768-65535	允许	允许对公有子网的出站响应(例如，响应与私有子网中的数据库服务器通信的公有子网中的 Web 服务器)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

场景 3 的推荐规则

场景 3 既是一个拥有可收发 Internet 流量的实例的公有子网，也是一个拥有仅能通过 AWS Site-to-Site VPN 连接与您的本地网络通信的实例的仅限 VPN 的子网。有关更多信息，请参阅[场景 3：具有公有和私有子网和 AWS Site-to-Site VPN 访问权限的 VPC \(p. 41\)](#)。

在这个场景中，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。下表显示我们推荐为每个 ACL 制定的规则。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

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许从任意 IPv4 地址到 Web 服务器的入站 HTTP 流量。

110	0.0.0.0/0	TCP	443	允许	允许从任意 IPv4 地址到 Web 服务器的入站 HTTPS 流量。
120	您的家庭网络的公有 IPv4 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 流量 (通过 Internet 网关)。
130	您的家庭网络的公有 IPv4 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 流量 (通过 Internet 网关)。
140	0.0.0.0/0	TCP	32768-65535	允许	<p>允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。</p> <p>此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅临时端口 (p. 131)。</p>
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的入站 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
110	0.0.0.0/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
120	10.0.1.0/24	TCP	1433	允许	<p>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。</p> <p>此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。</p>
140	0.0.0.0/0	TCP	32768-65535	允许	<p>允许对 Internet 客户端进行出站 IPv4 响应 (例如，向访问子网中的 Web 服务器的人员提供网页)。</p> <p>此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅临时端口 (p. 131)。</p>

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

仅限 VPN 的子网的 ACL 设置

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	10.0.0.0/24	TCP	1433	允许	<p>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。</p> <p>此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。</p>
120	您的家庭网络的私有 IPv4 地址范围	TCP	22	允许	允许来自家庭网络的入站 SSH 流量 (通过虚拟专用网关)。
130	您的家庭网络的私有 IPv4 地址范围	TCP	3389	允许	允许来自家庭网络的入站 RDP 流量 (通过虚拟专用网关)。
140	您的家庭网络的私有 IP 地址范围	TCP	32768-65535	允许	<p>允许本地网络中的客户端返回的入站流量 (通过虚拟专用网关)</p> <p>此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅临时端口 (p. 131)。</p>
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的入站数据流。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	您的家庭网络的私有 IP 地址范围	All	All	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)。该规则还包括规则 120；但是，可以通过使用特定协议类型及端口编号使此规则更为严格。如果您使此规则更为严格，则您的网络 ACL 中必须包括规则 120，以确保出站响应不会被阻止。

110	10.0.0.0/24	TCP	32768-65535	允许	允许对公有子网中 Web 服务器的出站响应。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
120	您的家庭网络的私有 IP 地址范围	TCP	32768-65535	允许	允许对本地网络中客户端的出站响应 (通过虚拟专用网关)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站数据流。

适用于 IPv6 的推荐规则

如果您实现了支持 IPv6 的场景 3 并创建了具有关联 IPv6 CIDR 块的 VPC 和子网，则必须向网络 ACL 添加单独的规则，以控制入站和出站 IPv6 流量。

以下是您的网络 ACL 的 IPv6 特定规则 (除了上面列出的规则以外)。

公有子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允许	允许来自任意 IPv6 地址的入站 HTTP 流量。
160	::/0	TCP	443	允许	允许来自任意 IPv6 地址的入站 HTTPS 流量。
170	您的家庭网络的 IPv6 地址范围	TCP	22	允许	允许来自您的家庭网络的通过 IPv6 的入站 SSH 流量 (通过 Internet 网关)。
180	您的家庭网络的 IPv6 地址范围	TCP	3389	允许	允许来自您的家庭网络的通过 IPv6 的入站 RDP 流量 (通过 Internet 网关)。
190	::/0	TCP	1024-65535	允许	允许来自 Internet 上的主机的入站返回流量，这些流量对应于源自子网的请求。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。

*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允许	允许出站 HTTP 流量从子网流向 Internet。
160	::/0	TCP	443	允许	允许出站 HTTPS 流量从子网流向 Internet。
170	2001:db8:1234: 1601 :/64		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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。
190	::/0	TCP	32768-65535	允许	允许对 Internet 客户端进行出站响应(例如，向访问子网中的 Web 服务器的人员提供网页) 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

仅限 VPN 的子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234: 1600 :/64		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。 此端口号仅为示例。其他示例包括用于访问 MySQL/Aurora 的 3306、用于访问 PostgreSQL 的 5432、用于访问 Amazon Redshift 的 5439 和用于访问 Oracle 的 1521。

*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	2001:db8:1234: 1600 ::/64		32768-65535	允许	允许对公有子网的出站响应(例如，响应与私有子网中的数据库服务器通信的公有子网中的 Web 服务器)。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

场景 4 的推荐规则

场景 4 是一个拥有只能通过 AWS Site-to-Site VPN 连接与您的本地网络通信的实例的子网。有关详细信息，请参阅[场景 4：仅具有一个私有子网以及 AWS Site-to-Site VPN 访问权限的 VPC \(p. 53\)](#)。

下表显示我们推荐制定的规则。除了已经明确要求的数据流之外，它们会阻塞所有数据流。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
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	32768-65535	允许	允许在子网中产生的请求返回的入站流量。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站数据流。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments

100	您的家庭网络的私有 IP 地址范围	All	All	允许	允许从子网到您的家庭网络的所有出站数据流。该规则还包括规则 120；但是，可以通过使用特定协议类型及端口编号使此规则更为严格。如果您使此规则更为严格，则您的网络 ACL 中必须包括规则 120，以确保出站响应不会被阻止。
120	您的家庭网络的私有 IP 地址范围	TCP	32768-65535	允许	允许对本地网络中客户端的出站响应。 此范围仅为示例。有关为您的配置选择正确的临时端口的信息，请参阅 临时端口 (p. 131) 。
*	0.0.0.0/0	全部	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站数据流。

适用于 IPv6 的推荐规则

如果您实现了支持 IPv6 的场景 4 并创建了具有关联 IPv6 CIDR 块的 VPC 和子网，则必须向网络 ACL 添加单独的规则，以控制入站和出站 IPv6 流量。

在这种情况下，无法通过使用 IPv6 的 VPN 连接访问数据库服务器，因此，不需要设置额外的网络 ACL 规则。以下是拒绝 IPv6 流量流入和流出子网的默认规则。

仅限 VPN 的子网的 ACL 规则

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的入站 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
*	::/0	all	all	拒绝	拒绝所有未经前置规则(不可修改)处理的出站 IPv6 流量。

控制访问 Amazon VPC 资源

要允许访问 Amazon VPC 资源而不共享安全凭证，您必须创建一个 IAM 策略，并将其附加到 IAM 用户或 IAM 用户所属的组。必须为 IAM 用户授予权限以使用所需的特定 Amazon VPC 资源和 Amazon EC2 API 操作。在将策略附加到一个或一组用户时，它允许或拒绝对指定资源执行指定任务。有些 API 操作支持资源级权限，这些权限使您可以控制用户可以创建或修改的特定资源。

Important

当前，不是所有 Amazon EC2 API 操作都支持资源级权限。如果 Amazon EC2 API 操作不支持资源级权限，那么，您可以向用户授予使用该操作的权限，但是必须为策略语句的资源元素指定 *。有关如何执行此操作的示例，请参阅以下示例策略：[1.管理 VPC \(p. 152\)](#)。我们以后会为其他 API 操作增加支持，并且为 Amazon EC2 资源添加 ARN。有关哪些 ARN 可以与哪些 Amazon EC2 API 操作一起使用以及每个 ARN 支持的条件密钥的信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 [Amazon EC2 API 操作支持的资源和条件](#)。

有关如何创建用于 Amazon EC2 的 IAM 策略、EC2 API 操作支持的资源以及 Amazon EC2 策略示例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[用于 Amazon EC2 的 IAM 策略](#)部分。

目录

- [针对 AWS CLI 或软件开发工具包的策略示例 \(p. 152\)](#)
- [控制台的策略示例 \(p. 158\)](#)

针对 AWS CLI 或软件开发工具包的策略示例

以下示例显示了您可用于控制 IAM 用户 Amazon VPC 权限的策略语句。这些示例面向使用 AWS CLI 或 AWS 开发工具包的用户。

示例

- [1.管理 VPC \(p. 152\)](#)
- [2. Amazon VPC 的只读策略 \(p. 153\)](#)
- [3. Amazon VPC 的自定义策略 \(p. 153\)](#)
- [4. 在特定子网中启动实例 \(p. 154\)](#)
- [5. 在特定 VPC 中启动实例 \(p. 154\)](#)
- [6. 在 VPC 中管理安全组 \(p. 155\)](#)
- [7. 创建和管理 VPC 对等连接 \(p. 155\)](#)
- [8. 创建和管理 VPC 终端节点 \(p. 158\)](#)

有关使用 ClassicLink 的策略示例，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[CLI 或 开发工具包策略示例](#)。

1.管理 VPC

以下策略允许用户创建和管理 VPC。可向一组网络管理员连接此策略。Action 元素指定与 VPC、子网、Internet 网关、客户网关、虚拟专用网关、Site-to-Site VPN 连接、路由表、弹性 IP 地址、安全组、网络 ACL 和 DHCP 选项组关联的 API 操作。策略还会允许组运行、停止、开始和终止示例。通过它，这组管理员还可列出 Amazon EC2 资源。

此策略使用通配符指定每种对象的所有操作（例如 *SecurityGroup*）。此外，还可显式地列出每项操作。如果使用通配符，则要注意，如果所添加的新操作在名称中包括策略中的任何通配符字符串，则策略将自动允许该组访问这些新操作。

Resource 元素使用通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。

```
{  
    "Version": "2012-10-17",  
    "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": "*"  
}
```

2. Amazon VPC 的只读策略

以下策略允许用户列出您的 VPC 及其组件。但用户无法创建、更新或删除它们。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["ec2:DescribeVpcs",  
                      "ec2:DescribeSubnets",  
                      "ec2:DescribeInternetGateways",  
                      "ec2:DescribeEgressOnlyInternetGateways",  
                      "ec2:DescribeVpcEndpoints",  
                      "ec2:DescribeNatGateways",  
                      "ec2:DescribeCustomerGateways",  
                      "ec2:DescribeVpnGateways",  
                      "ec2:DescribeVpnConnections",  
                      "ec2:DescribeRouteTables",  
                      "ec2:DescribeAddresses",  
                      "ec2:DescribeSecurityGroups",  
                      "ec2:DescribeNetworkAcls",  
                      "ec2:DescribeDhcpOptions",  
                      "ec2:DescribeTags",  
                      "ec2:DescribeInstances"],  
            "Resource": "*"  
        }  
    ]  
}
```

3. Amazon VPC 的自定义策略

以下策略允许用户启动实例、停止实例、开始实例、终止实例以及说明 Amazon EC2 和 Amazon VPC 的可用资源。

该策略中的第三个语句通过显式拒绝权限，防止任何其他策略可能允许用户访问更大范围的 API 操作。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": ["ec2:RunInstances",  
                "ec2:StopInstances"],  
      "Resource": "*"  
    }  
  ]  
}
```

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

4. 在特定子网中启动实例

以下策略允许用户在特定子网中启动实例，以及在请求中使用特定安全组。该策略通过为 subnet-1a2b3c4d 和 sg-123abc123 指定 ARN 实现上述目的。如果用户尝试在其他子网中启动实例或使用其他的安全组，请求将失败（除非其他策略或声明授予用户相应的权限）。

该策略还授予使用网络接口资源的权限。在子网中启动时，RunInstances 请求会默认创建一个主网络接口，因此，用户在启动实例时需要有创建此资源的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:subnet/subnet-1a2b3c4d",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/sg-123abc123"
            ]
        }
    ]
}
```

5. 在特定 VPC 中启动实例

以下策略允许用户在特定 VPC 中的任意子网中启动实例。此策略通过将条件密钥 (ec2:vpc) 应用于子网资源来实现上述目的。

该策略还授予用户仅使用具有标签“department=dev”的 AMI 启动实例的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:region:account:subnet/*",
            "Condition": {
                "StringEquals": {
                    "ec2:vpc": "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d"
                }
            }
        }
    ]
}
```

```
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:region::image/ami-*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

6. 在 VPC 中管理安全组

以下策略允许用户创建和删除特定 VPC 内任何安全组的入站和出站规则。此策略通过将条件密钥 (ec2:Vpc) 应用于 Authorize 和 Revoke 操作的安全组资源，来实现此目的。

第二条语句授予用户描述所有安全组的权限。这一授权是让用户能够使用 CLI 修改安全组的必要条件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress"
            ],
            "Resource": "arn:aws:ec2:region:account:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeSecurityGroups",
            "Resource": "*"
        }
    ]
}
```

7. 创建和管理 VPC 对等连接

以下是您可以用于管理 VPC 对等连接的创建和修改的策略示例。

a. 创建 VPC 对等连接

以下策略仅允许用户使用标记有 Purpose=Peering 的 VPC 来创建 VPC 对等连接请求。第一条语句对 VPC 资源应用条件键 (ec2:ResourceTag)。请注意，CreateVpcPeeringConnection 操作的 VPC 资源始终为请求者 VPC。

第二条语句向用户授予创建 VPC 对等连接资源的权限，因此使用 * 通配符代替特定资源 ID。

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:CreateVpcPeeringConnection",
        "Resource": "arn:aws:ec2:region:account:vpc/*",
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/Purpose": "Peering"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateVpcPeeringConnection",
        "Resource": "arn:aws:ec2:region:account:vpc-peering-connection/*"
    }
]
}
```

以下策略允许 AWS 账户 33333333333 中的用户使用 us-east-1 区域中的任何 VPC 创建 VPC 对等连接，但是仅当接受对等连接的 VPC 是特定账户 (777788889999) 中的特定 VPC (vpc-aaa111bb) 时。

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:CreateVpcPeeringConnection",
        "Resource": "arn:aws:ec2:us-east-1:33333333333:vpc/*"
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateVpcPeeringConnection",
        "Resource": "arn:aws:ec2:region:33333333333:vpc-peering-connection/*",
        "Condition": {
            "ArnEquals": {
                "ec2:AccepterVpc": "arn:aws:ec2:region:777788889999:vpc/vpc-aaa111bb"
            }
        }
    }
]
```

b. 接受 VPC 对等连接

以下策略仅允许用户接受来自 AWS 账户 44445555666 的 VPC 对等连接请求。这样有助于防止用户接受来自未知账户的 VPC 对等连接请求。第一条语句使用 ec2:RequesterVpc 条件键强制实施此策略。

该策略还向用户授予仅当 VPC 具有标签 Purpose=Peering 时才接受 VPC 对等请求的权限。

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:AcceptVpcPeeringConnection",
        "Resource": "arn:aws:ec2:region:account:vpc-peering-connection/*",
        "Condition": {
            "ArnEquals": {
                "ec2:RequesterVpc": "arn:aws:ec2:region:44445555666:vpc/vpc-aaa111bb"
            }
        }
    }
]
```

```

    "Condition": {
      "ArnEquals": {
        "ec2:RequesterVpc": "arn:aws:ec2:region:444455556666:vpc/*"
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}

```

c. 删除 VPC 对等连接

以下策略允许账户 444455556666 中的用户删除任何 VPC 对等连接，使用指定 VPC vpc-1a2b3c4d (处于相同账户中) 的连接除外。该策略同时指定 ec2:AcceptorVpc 和 ec2:RequesterVpc 条件密钥，因为 VPC 可能是原始 VPC 对等连接请求中的请求者 VPC 或对等方 VPC。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2>DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:444455556666:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AcceptorVpc": "arn:aws:ec2:region:444455556666:vpc/vpc-1a2b3c4d",
          "ec2:RequesterVpc": "arn:aws:ec2:region:444455556666:vpc/vpc-1a2b3c4d"
        }
      }
    }
  ]
}

```

d. 在特定账户中工作

以下策略允许用户完全在特定账户中处理 VPC 对等连接。用户可以查看、创建、接受、拒绝和删除 VPC 对等连接，前提是它们都处于 AWS 账户 333333333333 中。

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

第二条语句允许用户创建 VPC 对等连接，并允许访问账户 333333333333 中的所有 VPC 以便执行此操作。

第三条语句使用 * 通配符作为 Action 元素的一部分，以便允许执行所有 VPC 对等连接操作。条件密钥确保只能对与属于账户 333333333333 的 VPC 建立的 VPC 对等连接执行操作。例如，如果接受者或请求者 VPC 属于不同账户，则不允许用户删除 VPC 对等连接。用户无法与属于不同账户的 VPC 建立 VPC 对等连接。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",

```

```
"Resource": "*"
},
{
"Effect": "Allow",
"Action": ["ec2:CreateVpcPeeringConnection", "ec2:AcceptVpcPeeringConnection"],
"Resource": "arn:aws:ec2::33333333333:vpc/*"
},
{
"Effect": "Allow",
"Action": "ec2:*VpcPeeringConnection",
"Resource": "arn:aws:ec2::33333333333:vpc-peering-connection/*",
"Condition": {
"ArnEquals": {
"ec2:AccepterVpc": "arn:aws:ec2::33333333333:vpc/*",
"ec2:RequesterVpc": "arn:aws:ec2::33333333333:vpc/*"
}
}
}
]
```

8. 创建和管理 VPC 终端节点

以下策略授予用户创建、修改、查看和删除 VPC 终端节点、VPC 终端节点服务和 VPC 终端节点连接通知的权限。用户还可以接受和拒绝 VPC 终端节点连接请求。所有 `ec2:*VpcEndpoint*` 操作均不支持资源级权限，因此，您必须针对 `Resource` 元素使用 * 通配符，以允许用户使用所有资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*VpcEndpoint*",
            "Resource": "*"
        }
    ]
}
```

控制台的策略示例

您可以使用 IAM 策略向用户授予在 Amazon VPC 控制台中查看和使用特定资源的权限。您可以使用上一部分中的策略；但是，这些策略设计用于使用 AWS CLI 或 AWS 开发工具包发出的请求。控制台使用其他 API 操作实现其功能，因此这些策略可能不会按预期方式起作用。

此部分演示使用户可以使用 VPC 控制台的特定部分的策略。

示例

- [1. 使用 VPC 向导 \(p. 158\)](#)
- [2. 管理 VPC \(p. 162\)](#)
- [3. 管理安全组 \(p. 163\)](#)
- [4. 创建 VPC 对等连接 \(p. 164\)](#)

1. 使用 VPC 向导

您可以在 Amazon VPC 控制台中使用 VPC 向导创建、设置和配置 VPC，使它准备就绪可供使用。该向导根据您的要求提供不同的配置选项。想要了解更多有关使用 VPC 向导创建 VPC 的信息，请参阅 [场景和示例 \(p. 23\)](#)。

要使用户可以使用 VPC 向导，您必须向他们授予创建和修改组成所选配置的资源的权限。以下示例策略演示每个向导配置选项所需的操作。

Note

如果 VPC 向导在任何时候失败，则它会尝试断开并删除它创建的资源。如果您不向用户授予使用这些操作的权限，则这些资源保留在您的账户中。

选项 1：带单个公有子网的 VPC

第一个 VPC 向导配置选项创建带单个子网的 VPC。在 IAM 策略中，您必须向用户授予使用以下操作的权限，以便他们可以成功使用此向导选项：

- `ec2:CreateVpc`、`ec2:CreateSubnet`、`ec2:CreateRouteTable` 和 `ec2:CreateInternetGateway`：用于创建 VPC、子网、自定义路由表和 Internet 网关。
- `ec2:DescribeAvailabilityZones`：用于显示向导中的 Availability Zone (可用区) 列表和子网的 CIDR 块字段部分。即使用户要保留默认设置，他们也无法创建 VPC，除非显示这些选项。
- `ec2:DescribeVpcEndpointServices`：显示向导的 VPC 终端节点部分。
- `ec2:AttachInternetGateway`：用于将 Internet 网关连接到 VPC。
- `ec2:CreateRoute`：用于在自定义路由表中创建路由。路由将流量指向 Internet 网关。
- `ec2:AssociateRouteTable`：用于将自定义路由表关联到子网。
- `ec2:ModifyVpcAttribute`：用于修改 VPC 的属性以启用 DNS 主机名称，以便在此 VPC 中启动的每个实例都收到一个 DNS 主机名称。

此策略中没有 API 操作支持资源级权限，因此您无法控制用户可以使用的特定资源。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateVpc", "ec2:CreateSubnet", "ec2:DescribeAvailabilityZones",  
                "ec2:DescribeVpcEndpointServices",  
                "ec2:CreateRouteTable", "ec2:CreateRoute", "ec2:CreateInternetGateway",  
                "ec2:AttachInternetGateway", "ec2:AssociateRouteTable", "ec2:ModifyVpcAttribute"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

选项 2：带公有和私有子网的 VPC

第二个 VPC 向导配置选项用于创建具有公有和私有子网的 VPC 并提供用于启动 NAT 网关或 NAT 实例的选项。以下策略具有与前一个示例 (选项 1) 相同的操作，以及允许用户运行和配置 NAT 网关或 NAT 实例的操作。

无论您是要启动 NAT 实例还是 NAT 网关，都必须执行以下操作：

- `ec2:DescribeKeyPairs`：显示现有密钥对列表并加载向导的 NAT 部分。

要创建 NAT 网关，必须执行以下操作 (启动 NAT 实例时不必执行这些操作)：

- `ec2>CreateNatGateway`：创建 NAT 网关。
- `ec2:DescribeNatGateways`：检查 NAT 网关状态，直到它变为可用状态。

- `ec2:DescribeAddresses`：列出您的账户中可用于与 NAT 网关关联的弹性 IP 地址。

要启动 NAT 实例，必须执行以下操作（创建 NAT 网关时不必执行这些操作）：

- `ec2:DescribeImages`：用于查找已配置作为 NAT 实例运行的 AMI。
- `ec2:RunInstances`：用于启动 NAT 实例。
- `ec2:AllocateAddress` 和 `ec2:AssociateAddress`：用于向您的账户分配弹性 IP 地址，然后将它与 NAT 实例关联。
- `ec2:ModifyInstanceAttribute`：用于禁用 NAT 实例的源/目的地检查。
- `ec2:DescribeInstances`：用于检查实例的状态，直到它处于运行状态。
- `ec2:DescribeRouteTables`、`ec2:DescribeVpnGateways` 和 `ec2:DescribeVpcs`：用于收集有关必须添加到主路由表的路由的信息。

以下策略允许用户创建 NAT 实例或 NAT 网关。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateVpc", "ec2:CreateSubnet", "ec2:DescribeAvailabilityZones",  
                "ec2:DescribeVpcEndpointServices",  
                "ec2:CreateRouteTable", "ec2:CreateRoute", "ec2:CreateInternetGateway",  
                "ec2:CreateNatGateway",  
                "ec2:AttachInternetGateway", "ec2:AssociateRouteTable", "ec2:ModifyVpcAttribute",  
                "ec2:DescribeKeyPairs",  
                "ec2:DescribeImages", "ec2:RunInstances", "ec2:AllocateAddress",  
                "ec2:AssociateAddress",  
                "ec2:DescribeAddresses", "ec2:DescribeInstances", "ec2:ModifyInstanceStateAttribute",  
                "ec2:DescribeRouteTables",  
                "ec2:DescribeVpnGateways", "ec2:DescribeVpcs", "ec2:DescribeSubnets",  
                "ec2:DescribeNatGateways"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

可以对 `ec2:RunInstances` 操作使用资源级权限来控制用户启动实例的能力。例如，您可以指定一个启用了 NAT 的 AMI 的 ID，以便用户只能通过此 AMI 启动实例。要查明向导用于启动 NAT 实例的 AMI，请作为拥有完全权限的用户登录 Amazon VPC 控制台，然后执行 VPC 向导的第二个选项。切换到 Amazon EC2 控制台，选择 Instances (实例) 页面，选择 NAT 实例，并记下用于启动它的 AMI ID。

以下策略仅允许用户使用 `ami-1a2b3c4d` 启动实例。如果用户尝试使用任何其他 AMI 启动实例，则启动会失败。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:CreateVpc", "ec2:CreateSubnet", "ec2:DescribeAvailabilityZones",  
            "ec2:DescribeVpcEndpointServices",  
            "ec2:CreateRouteTable", "ec2:CreateRoute", "ec2:CreateInternetGateway",  
            "ec2:AttachInternetGateway", "ec2:AssociateRouteTable", "ec2:ModifyVpcAttribute",  
            "ec2:DescribeKeyPairs", "ec2:DescribeImages", "ec2:AllocateAddress",  
            "ec2:AssociateAddress",  
            "ec2:RunInstances"  
        ],  
        "Resource": "arn:aws:ec2:us-west-2:123456789012:ami-1a2b3c4d"  
    }]  
}
```

```

    "ec2:DescribeInstances", "ec2:ModifyInstanceAttribute", "ec2:DescribeRouteTables",
    "ec2:DescribeVpnGateways", "ec2:DescribeVpcs"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "ec2:RunInstances",
"Resource": [
    "arn:aws:ec2:region::image/ami-1a2b3c4d",
    "arn:aws:ec2:region:account:instance/*",
    "arn:aws:ec2:region:account:subnet/*",
    "arn:aws:ec2:region:account:network-interface/*",
    "arn:aws:ec2:region:account:volume/*",
    "arn:aws:ec2:region:account:key-pair/*",
    "arn:aws:ec2:region:account:security-group/*"
]
}
]
}
}

```

选项 3：具有公有和私有子网和 AWS Site-to-Site VPN 访问权限的 VPC

第三个 VPC 向导配置选项将创建具有公有和私有子网的 VPC，并在您的 VPC 与您自己的网络之间创建 AWS Site-to-Site VPN 连接。在您的 IAM 策略中，您必须授予用户使用与选项 1 相同的操作的权限。这样，他们可以创建一个 VPC 和两个子网，并为公有子网配置路由。要创建Site-to-Site VPN 连接，用户还必须具有使用以下操作的权限：

- `ec2:CreateCustomerGateway`：创建客户网关。
- `ec2>CreateVpnGateway` 和 `ec2:AttachVpnGateway`：创建虚拟专用网关并将其连接到 VPC。
- `ec2:EnableVgwRoutePropagation`：启用路由传播，以便自动将路由传播到您的路由表。
- `ec2:CreateVpnConnection`：创建Site-to-Site VPN 连接。
- `ec2:DescribeVpnConnections`、`ec2:DescribeVpnGateways` 和 `ec2:DescribeCustomerGateways`：显示向导的第二个配置页面上的选项。
- `ec2:DescribeVpcs` 和 `ec2:DescribeRouteTables`：收集有关必须添加到主路由表的路由的信息。

此策略中没有 API 操作支持资源级权限，因此您无法控制用户可以使用的特定资源。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpc", "ec2:CreateSubnet", "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcEndpointServices",
                "ec2:CreateRouteTable", "ec2:CreateRoute", "ec2:CreateInternetGateway",
                "ec2:AttachInternetGateway", "ec2:AssociateRouteTable", "ec2:ModifyVpcAttribute",
                "ec2:CreateCustomerGateway", "ec2:CreateVpnGateway", "ec2:AttachVpnGateway",
                "ec2:EnableVgwRoutePropagation", "ec2:CreateVpnConnection",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeCustomerGateways", "ec2:DescribeVpnConnections",
                "ec2:DescribeRouteTables",
                "ec2:DescribeNetworkAccls", "ec2:DescribeInternetGateways", "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}

```

选项 4：仅具有一个私有子网以及 AWS Site-to-Site VPN 访问权限的 VPC

第四个 VPC 配置选项将创建具有私有子网的 VPC，并在您的 VPC 与您自己的网络之间创建 Site-to-Site VPN 连接。与其他三个选项不同的是，用户无需权限即可创建 Internet 网关或将其连接到 VPC，而且他们无需权限即可创建路由表并将其与子网关联起来。若要建立 Site-to-Site VPN 连接，用户需要具有与前一示例（选项 3）中所列的相同的权限。

此策略中没有 API 操作支持资源级权限，因此您无法控制用户可以使用的特定资源。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
        "Action": [  
            "ec2:CreateVpc", "ec2>CreateSubnet", "ec2:DescribeAvailabilityZones",  
            "ec2:DescribeVpcEndpointServices",  
            "ec2:ModifyVpcAttribute", "ec2:CreateCustomerGateway", "ec2:CreateVpnGateway",  
            "ec2:AttachVpnGateway", "ec2:EnableVgwRoutePropagation", "ec2:CreateVpnConnection",  
            "ec2:DescribeVpnGateways", "ec2:DescribeCustomerGateways",  
            "ec2:DescribeVpnConnections",  
            "ec2:DescribeRouteTables", "ec2:DescribeNetworkAcls", "ec2:DescribeInternetGateways",  
            "ec2:DescribeVpcs"  
        ],  
        "Resource": "*"  
    ]  
}
```

2. 管理 VPC

在 VPC 控制台中的 Your VPCs (您的 VPC) 页面上，您可以创建或删除 VPC。要查看 VPC，用户必须拥有使用 `ec2:DescribeVPCs` 操作的权限。要使用 Create VPC (创建 VPC) 对话框创建 VPC，用户必须拥有使用 `ec2:CreateVpc` 操作的权限。

Note

默认情况下，VPC 控制台创建具有 Name 键和用户指定值的标签。如果用户没有使用 ec2:CreateTags 操作的权限，则他们在尝试创建 VPC 时，Create VPC (创建 VPC) 对话框中会显示错误。不过，VPC 可能已成功创建。

设置 VPC 时，您通常会创建一些独立对象，如子网和 Internet 网关。您无法删除 VPC，除非您取消关联并删除了这些独立对象。使用控制台删除 VPC 时，它会为您执行这些操作（终止实例除外；您必须自己执行此操作）。

以下示例允许用户在 Your VPCs (您的 VPC) 页面上查看和创建 VPC，以及删除使用 VPC 向导中的第一个选项创建的 VPC (带单个公有子网的 VPC)。此 VPC 具有一个与自定义路由表关联的子网以及一个连接到它的 Internet 网关。要使用控制台删除 VPC 及其组件，您必须向用户授予使用一些 `ec2:Describe*` 操作的权限，以便控制台可以检查是否有任何其他资源依赖于此 VPC。您还必须向用户授予取消路由表与子网的关联的权限、从 VPC 断开 Internet 网关的权限以及删除这两种资源的权限。

```
    "ec2:DescribeVpcPeeringConnections", "ec2:DescribeSecurityGroups",
    "ec2>CreateVpc", "ec2>DeleteVpc", "ec2:DetachInternetGateway",
"ec2>DeleteInternetGateway",
    "ec2:DisassociateRouteTable", "ec2:DeleteSubnet", "ec2:DeleteRouteTable"
],
"Resource": "*"
}
]
}
```

您无法将资源级权限应用于任何 ec2:Describe* API 操作，但是您可以将资源级权限应用于一些 ec2:Delete* 操作以控制用户可以删除的资源。

例如，以下策略仅允许用户删除具有标签 Purpose=Test 的路由表和 Internet 网关。用户无法删除没有此标签的各个路由表或 Internet 网关，同样，用户无法使用 VPC 控制台删除与不同路由表或 Internet 网关关联的 VPC。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs", "ec2:DescribeRouteTables", "ec2:DescribeVpnGateways",
"ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets", "ec2:DescribeDhcpOptions", "ec2:DescribeInstances",
"ec2:DescribeVpcAttribute",
                "ec2:DescribeNetworkAccls", "ec2:DescribeNetworkInterfaces",
"ec2:DescribeAddresses",
                "ec2:DescribeVpcPeeringConnections", "ec2:DescribeSecurityGroups",
                "ec2>CreateVpc", "ec2>DeleteVpc", "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable", "ec2:DeleteSubnet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2>DeleteInternetGateway",
            "Resource": "arn:aws:ec2:region:account:internet-gateway/*",
"Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2>DeleteRouteTable",
            "Resource": "arn:aws:ec2:region:account:route-table/*",
"Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

3. 管理安全组

要在 Amazon VPC 控制台中的 Security Groups (安全组) 页面上查看安全组，用户必须拥有使用 ec2:DescribeSecurityGroups 操作的权限。要使用 Create Security Group (创建安全组) 对话框创建安全组，用户必须拥有使用 ec2:DescribeVpcs 和 ec2:CreateSecurityGroup 操作的权限。如果用户没

有使用 `ec2:DescribeSecurityGroups` 操作的权限，他们仍可以使用该对话框创建安全组，只是可能出现错误消息，指示未能创建组。

在 Create Security Group (创建安全组) 对话框中，用户必须添加安全组名称和说明，但是他们无法为 Name tag (名称标签) 字段输入值，除非向他们授予了使用 `ec2:CreateTags` 操作的权限。但是，他们无需此操作即可成功创建安全组。

以下策略允许用户查看和创建安全组，以及对与 `vpc-1a2b3c4d` 关联的任何安全组添加和删除入站和出站规则。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeSecurityGroups", "ec2:DescribeVpcs", "ec2:CreateSecurityGroup"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DeleteSecurityGroup", "ec2:AuthorizeSecurityGroupIngress",  
            "ec2:AuthorizeSecurityGroupEgress",  
            "ec2:RevokeSecurityGroupIngress", "ec2:RevokeSecurityGroupEgress"  
        ],  
        "Resource": "arn:aws:ec2:::security-group/*",  
        "Condition": {  
            "ArnEquals": {  
                "ec2:Vpc": "arn:aws:ec2:::vpc/vpc-1a2b3c4d"  
            }  
        }  
    }  
]
```

4. 创建 VPC 对等连接

要在 Amazon VPC 控制台中查看 VPC 对等连接，用户必须拥有使用 `ec2:DescribePeeringConnections` 操作的权限。要使用 Create VPC Peering Connection (创建 VPC 对等连接) 对话框，用户必须拥有使用 `ec2:DescribeVpcs` 操作的权限。这样，他们不使用此操作也可查看和选择 VPC，该对话框无法加载。您可以将资源级权限应用于所有 `ec2:*PeeringConnection` 权限 (`ec2:DescribeVpcPeeringConnections` 除外)。

以下策略允许用户查看 VPC 对等连接，以及使用 Create VPC Peering Connection (创建 VPC 对等连接) 对话框创建仅使用特定请求者 VPC (`vpc-1a2b3c4d`) 的 VPC 对等连接。如果用户尝试创建使用不同请求者 VPC 的 VPC 对等连接，则请求会失败。

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2>CreateVpcPeeringConnection",  
        "Resource": [  
            "arn:aws:ec2:::vpc/vpc-1a2b3c4d"  
        ]  
    }  
]
```

```
    "arn:aws:ec2:*::*:vpc/vpc-1a2b3c4d",
    "arn:aws:ec2:*::*:vpc-peering-connection/*"
]
}
]
```

想要了解更多有关编写 IAM 策略以便使用 VPC 对等连接的示例，请参阅 [7. 创建和管理 VPC 对等连接 \(p. 155\)](#)。

VPC 流日志

利用 VPC 流日志这项功能，您可以捕获有关传入和传出您的 VPC 中网络接口的 IP 流量的信息。流日志数据可以发布到 Amazon CloudWatch Logs 和 Amazon S3。创建流日志后，您可以在选定目标中检索和查看其数据。

流日志可以帮助您完成大量任务；例如，排查流量未到达实例的原因，这反过来可帮助您诊断限制过于严格的安全组规则。您还可以使用流日志作为安全工具来监视到达您的实例的流量。

在使用流日志时会收取 CloudWatch Logs 费用，而无论您是将它们发送到 CloudWatch Logs 还是 Amazon S3。有关更多信息，请参阅 [Amazon CloudWatch 定价](#)。

目录

- [流日志基础知识 \(p. 165\)](#)
- [流日志记录 \(p. 166\)](#)
- [流日志限制 \(p. 168\)](#)
- [将流日志发布到 CloudWatch Logs \(p. 168\)](#)
- [将流日志发布到 Amazon S3 \(p. 171\)](#)
- [使用流日志 \(p. 175\)](#)
- [故障排除 \(p. 178\)](#)

流日志基础知识

您可以为 VPC、子网或网络接口创建流日志。如果您为子网或 VPC 创建流日志，则会监视 VPC 或子网中的每个网络接口。

受监控网络接口的流日志数据记录为流日志记录，这些是日志事件，由描述该流量的字段组成。有关更多信息，请参阅 [流日志记录 \(p. 166\)](#)。

要创建流日志，您必须指定要为其创建流日志的资源、要捕获的流量类型（接受的流量、拒绝的流量或所有流量），以及您要将流日志数据发布到的目标。如果已创建流日志，则需要几分钟来开始收集数据并将数据发布到选定目标。流日志不会为您的网络接口捕获实时日志流。有关更多信息，请参阅 [创建流日志 \(p. 176\)](#)。

如果在为子网或 VPC 创建了流日志之后，您在子网中启动了多个实例，则在该网络接口上记录到任何网络流量时，将立即为每个新网络接口创建一个新日志流（对于 CloudWatch Logs）或日志文件对象（对于 Amazon S3）。

您可以为其他 AWS 创建的网络接口创建流日志，例如 Elastic Load Balancing、Amazon RDS、Amazon ElastiCache、Amazon Redshift 和 Amazon WorkSpaces。但是，您不能使用这些服务控制台或 API 来创建流日志；您必须使用 Amazon EC2 控制台或 Amazon EC2 API。与此类似，您不能使用 CloudWatch Logs、Amazon S3 控制台或 API 为网络接口创建流日志。

如果您不再需要某个流日志，可将其删除。删除流日志将会禁用资源的流日志服务，不再创建新的流日志记录，也不会将这些记录发布到 CloudWatch Logs 或 Amazon S3。它不删除网络接口的任何现有流日志记录、日志流（对于 CloudWatch Logs）或日志文件对象（对于 Amazon S3）。要删除现有日志流，请使用 CloudWatch Logs 控制台。要删除现有日志文件对象，请使用 Amazon S3 控制台。在删除流日志之后，可能需要数分钟时间来停止收集数据。有关更多信息，请参阅[删除流日志 \(p. 177\)](#)。

流日志记录

流日志记录代表您的流日志中的网络流。每个记录捕获特定捕获窗口中的特定 5 元组的网络流。5 元组是一组 5 个不同的值，指定 Internet 协议 (IP) 流的源、目标和协议。捕获窗口是一段持续时间，在这段时间内流日志服务会聚合数据，然后再发布流日志记录。捕获窗口大约为 10 分钟，但最长可以为 15 分钟。

流日志记录语法

流日志记录是以空格分隔的字符串，采用以下格式：

```
<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol>
<packets> <bytes> <start> <end> <action> <log-status>
```

下表描述了流日志记录的各个字段。

字段	描述
version	VPC 流日志版本。
account-id	流日志的 AWS 账户 ID。
interface-id	为其记录流量的网络接口的 ID。
srcaddr	源 IPv4 或 IPv6 地址。网络接口的 IPv4 地址始终是其私有 IPv4 地址。
dstaddr	目标 IPv4 或 IPv6 地址。网络接口的 IPv4 地址始终是其私有 IPv4 地址。
srcport	流量的源端口。
dstport	流量的目标端口。
protocol	流量的 IANA 协议编号。有关更多信息，请参阅 分配的 Internet 协议编号 。
packets	捕获窗口中传输的数据包的数量。
bytes	捕获窗口中传输的字节数。
start	捕获窗口启动的时间，采用 Unix 秒的格式。
end	捕获窗口结束的时间，采用 Unix 秒的格式。
action	与流量关联的操作： <ul style="list-style-type: none">• ACCEPT：安全组或网络 ACL 允许记录的流量。• REJECT：安全组或网络 ACL 未允许记录的流量。
log-status	流日志的日志记录状态： <ul style="list-style-type: none">• OK：数据正常记录到选定目标。• NODATA：捕获窗口中没有传入或传出网络接口的网络流量。• SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。

Note

如果某个字段不适用于特定记录，则记录为该条目显示一个“-”符号。

流日志记录示例

已接受流量和已拒绝流量的流日志记录

下面是一个流日志记录的示例，其中允许指向账户 123456789010 中的网络接口 eni-abc123de 的 SSH 流量（目标端口 22，TCP 协议）：

```
2 123456789010 eni-abc123de 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010  
1418530070 ACCEPT OK
```

下面是一个流日志记录的示例，其中拒绝了指向账户 123456789010 中的网络接口 eni-abc123de 的 RDP 流量（目标端口 3389，TCP 协议）：

```
2 123456789010 eni-abc123de 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010  
1418530070 REJECT OK
```

无数据和跳过记录的流日志记录

以下示例的流日志记录在捕获窗口中未记录数据：

```
2 123456789010 eni-1a2b3c4d - - - - - 1431280876 1431280934 - NODATA
```

以下示例的流日志记录在捕获窗口中跳过了记录：

```
2 123456789010 eni-4b118871 - - - - - 1431280876 1431280934 - SKIPDATA
```

安全组和网络 ACL 规则

如果您正使用流日志来诊断过于严格或过于宽松的安全组规则或网络 ACL 规则，请注意这些资源的状态性。安全组是有状态的，这意味着对所允许流量的响应也会被允许，即使安全组中的规则不允许也是如此。相反，网络 ACL 是无状态的，因此对所允许流量的响应需要遵守网络 ACL 规则。

例如，您从家中的计算机（IP 地址为 203.0.113.12）对您的实例（网络接口的私有 IP 地址为 172.31.16.139）使用 ping 命令。您的安全组入站规则允许 ICMP 流量，出站规则不允许 ICMP 流量，但是，由于安全组是有状态的，因此允许从您的实例响应 ping。您的网络 ACL 允许入站 ICMP 流量，但不允许出站 ICMP 流量。由于网络 ACL 是无状态的，响应 Ping 将被丢弃，不会传输到您家中的计算机。在流日志中，它显示为 2 个流日志记录：

- 网络 ACL 和安全组都允许（因此可到达您的实例）的发起 ping 的 ACCEPT 记录。
- 网络 ACL 拒绝的响应 ping 的 REJECT 记录。

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142  
ACCEPT OK
```

```
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142  
REJECT OK
```

如果您的网络 ACL 允许出站 ICMP 流量，流日志会显示两个 ACCEPT 记录（一个针对发起 ping，一个针对响应 ping）。如果您的安全组拒绝入站 ICMP 流量，流日志会显示一个 REJECT 记录，因为流量无权到达您的实例。

IPv6 流量的流日志记录

下面是流日志记录的示例，其中允许账户 123456789010 中从 IPv6 地址 2001:db8:1234:a100:8d6e:3477:df66:f105 到网络接口 eni-f41c42bf 的 SSH 流量 (端口 22)。

```
2 123456789010 eni-f41c42bf 2001:db8:1234:a100:8d6e:3477:df66:f105
2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT OK
```

流日志限制

要使用流日志，您需要了解以下限制：

- 您无法为 EC2-Classic 平台中的网络接口启用流日志。这包含通过 ClassicLink 与 VPC 链接的 EC2-Classic 实例。
- 您不能为与您的 VPC 对等的 VPC 启用流日志，除非该对等 VPC 在您的账户中。
- 您不能标记流日志。
- 在创建流日志之后，您不能更改其配置；例如，您不能将不同的 IAM 角色与流日志关联。不过，您可以删除流日志并使用必需的配置创建新的流日志。
- 请注意，流日志 API 操作 (`ec2:*FlowLogs`) 支持资源级别的权限。要创建 IAM 策略来控制流日志 API 操作的使用，您必须在语句中为资源元素使用 * 通配符，以便授予用户使用该操作的所有资源的权限。有关更多信息，请参阅 [控制访问 Amazon VPC 资源 \(p. 151\)](#)。
- 如果网络接口有多个 IPv4 地址，并且流量发送到辅助私有 IPv4 地址，则流日志会在目的地 IP 地址字段中显示主要私有 IPv4 地址。
- 如果流量发送到某个 ENI 而目的地不是 ENI IP 地址中的任何一个，则流日志会在目的地 IP 地址字段中显示主要私有 IPv4 地址。
- 如果流量来自某个 ENI 而源不是 ENI IP 地址中的任何一个，则流日志会在源 IP 地址字段中显示主要私有 IPv4 地址。
- 如果流量发送到网络接口或由网络接口发送，则流日志始终在接口 IPv4 地址字段中显示主要私有 IPv4 地址，而不管数据包源或目标如何。

流日志不会捕获所有 IP 流量。以下类型的流量不予以记录：

- 实例与 Amazon DNS 服务器联系时生成的流量。如果您使用自己的 DNS 服务器，则将记录到该 DNS 服务器的所有流量。
- Windows 实例为 Amazon Windows 许可证激活而生成的流量。
- 实例元数据传入和传出 169.254.169.254 的流量。
- Amazon Time Sync Service 的传入和传出 169.254.169.123 的流量。
- DHCP 流量。
- 到默认 VPC 路由器的预留 IP 地址的流量。有关更多信息，请参阅 [VPC 和子网大小调整 \(p. 78\)](#)。
- 在终端节点网络接口和网络负载均衡器网络接口之间的流量。有关更多信息，请参阅 [VPC 终端节点服务 \(AWS PrivateLink\) \(p. 263\)](#)。

将流日志发布到 CloudWatch Logs

流日志可以将流日志数据直接发布到 Amazon CloudWatch。

在发布到 CloudWatch Logs 时，流日志数据将发布到日志组，并且每个网络接口在该日志组中有唯一的一条日志流。日志流包含流日志记录。您可以创建将数据发布到相同日志组的多个流日志。如果相同日志组中的一个或多个流日志存在相同网络接口，其中就会有一个组合日志流。如果您指定了一个流日志应该捕获已拒绝流

量，而另一个流日志应该捕获已接受流量，则组合日志流会捕获所有流量。有关更多信息，请参阅[流日志记录 \(p. 166\)](#)。

目录

- [用于将流日志发布到 CloudWatch Logs 的 IAM 角色 \(p. 169\)](#)
- [创建发布到 CloudWatch Logs 的流日志 \(p. 170\)](#)
- [处理 CloudWatch Logs 中的流日志记录 \(p. 171\)](#)

用于将流日志发布到 CloudWatch Logs 的 IAM 角色

与您的流日志关联的 IAM 角色必须具有足够的权限，以便将流日志发布到 CloudWatch Logs 中的指定日志组。附加到您的 IAM 角色的 IAM 策略必须至少包括以下权限：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "logs:CreateLogGroup",  
                "logs:CreateLogStream",  
                "logs:PutLogEvents",  
                "logs:DescribeLogGroups",  
                "logs:DescribeLogStreams"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

另请确保您的角色具有信任关系，以允许流日志服务代入该角色：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "vpc-flow-logs.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

用户还必须有权对与流日志关联的 IAM 角色使用 iam:PassRole 操作：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["iam:PassRole"],  
            "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"  
        }  
    ]  
}
```

您可以更新现有角色，或使用以下过程创建用于流日志的新角色。

创建流日志角色

为流日志创建 IAM 角色

1. 通过以下网址打开 IAM 控制台：[https://console.aws.amazon.com/iam/。](https://console.aws.amazon.com/iam/)
2. 在导航窗格中，选择 Roles 和 Create role。
3. 选择 EC2 作为服务以使用此角色。对于 Use case (使用案例)，选择 EC2。选择 Next: Permissions (下一步：权限)。
4. 在 Attach permissions policies (附加权限策略) 页上，选择 Next: Tags (下一步：标签)，还可以选择性地添加标签。选择 Next: Review (下一步：审核)。
5. 输入您的角色的名称（例如 Flow-Logs-Role），并且可以选择提供描述。选择 Create role。
6. 选择角色的名称。对于 Permissions (权限)，依次选择 Add inline policy (添加内联策略)、JSON。
7. 从 [用于将流日志发布到 CloudWatch Logs 的 IAM 角色 \(p. 169\)](#) 中复制第一个策略，并将其粘贴到窗口中。选择 View policy。
8. 为您的策略输入名称，然后选择 Create policy (创建策略)。
9. 选择角色的名称。对于 Trust relationships (信任关系)，选择 Edit trust relationship (编辑信任关系)。在现有策略文档中，将服务从 ec2.amazonaws.com 更改为 vpc-flow-logs.amazonaws.com。选择 Update Trust Policy。
10. 在 Summary 页面上，记录您的角色的 ARN。创建流日志时需要此 ARN。

创建发布到 CloudWatch Logs 的流日志

您可以为 VPC、子网或网络接口创建流日志。

创建网络接口的流日志

1. 打开 Amazon EC2 控制台 [https://console.aws.amazon.com/ec2/。](https://console.aws.amazon.com/ec2/)
2. 在导航窗格中，选择 Network Interfaces。
3. 选择一个或多个网络接口，然后选择操作、创建流日志。
4. 对于 Filter (筛选条件)，指定要记录的 IP 流量数据的类型。选择 All (全部) 将记录接受和拒绝的流量，选择 Rejected (已拒绝) 将仅记录被拒绝的流量，选择 Accepted (已接受) 将仅记录接受的流量。
5. 对于目的地，选择发送到 CloudWatch Logs。
6. 对于目标日志组，键入 CloudWatch Logs 中日志组的名称，流日志将发布到该日志组。如果您指定了不存在的日志组的名称，我们将尝试为您创建日志组。
7. 对于 IAM 角色，指定有权将日志发布到 CloudWatch Logs 的角色的名称。
8. 选择 Create。

为 VPC 或子网创建流日志

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中，选择 Your VPCs (您的 VPC) 或 Subnets (子网)。
3. 选择一个或多个 VPC 或子网，然后选择操作、创建流日志。
4. 对于 Filter (筛选条件)，指定要记录的 IP 流量数据的类型。选择 All (全部) 将记录接受和拒绝的流量，选择 Rejected (已拒绝) 将仅记录被拒绝的流量，选择 Accepted (已接受) 将仅记录接受的流量。
5. 对于目的地，选择发送到 CloudWatch Logs。
6. 对于目标日志组，键入 CloudWatch Logs 中日志组的名称，流日志将发布到该日志组。如果您指定了不存在的日志组的名称，我们将尝试为您创建日志组。
7. 对于 IAM 角色，指定有权将日志发布到 CloudWatch Logs 的 IAM 角色的名称。

8. 选择 Create。

处理 CloudWatch Logs 中的流日志记录

您可以像使用 CloudWatch Logs 收集的任意其他日志事件一样使用流日志记录。有关监视日志数据和指标筛选条件的更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [搜索和筛选日志数据](#)。

示例：为流日志创建 CloudWatch 指标筛选条件和警报

在此示例中，您有一个适用于 eni-1a2b3c4d 的流日志。您要创建一个警报，如果 1 小时内有 10 次或超过 10 次通过 TCP 端口 22 (SSH) 连接到您的实例的尝试遭到拒绝，该警报将向您发出提醒。首先，您必须创建一个指标筛选条件，该指标筛选条件与为其创建警报的流量的模式相匹配。然后，您可以为该指标筛选条件创建警报。

为已拒绝的 SSH 流量创建指标筛选条件并为该筛选条件创建警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Logs。
3. 为流日志的日志组选择相关联的 Metric Filters 值，然后选择 Add Metric Filter。
4. 对于 Filter Pattern (筛选模式)，输入以下内容：

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. 对于 Select Log Data to Test (选择要测试的日志数据)，选择您的网络接口对应的日志流。（可选）要查看与筛选条件模式匹配的日志数据行，请选择 Test Pattern (测试模式)。准备好之后，选择 Assign Metric。
6. 提供指标命名空间和名称，并确保将指标值设置为 1。完成后，选择 Create Filter。
7. 在导航窗格中，依次选择 Alarms 和 Create Alarm。
8. 在 Custom Metrics 部分中，为您创建的指标筛选条件选择命名空间。

Note

新指标可能需要几分钟才会在控制台中显示。

9. 选择您创建的指标名称，然后选择 Next (下一步)。
10. 输入警报的名称和说明。对于 is (为) 字段，选择 \geq 并输入 10。对于 for (期间) 字段，保留默认值 1 以指示连续期间。
11. 对于 Period (周期)，选择 1 Hour (1 小时)。对于 Statistic (统计数据)，选择 Sum (总计)。Sum 统计数据确保您捕获指定时间段内的数据点的总数。
12. 在操作部分中，您可以选择将通知发送到现有列表。或者，您可以创建新列表并输入在警报触发时应接收通知的电子邮件地址。完成后，选择 Create Alarm。

将流日志发布到 Amazon S3

流日志可以将流日志数据发布到 Amazon S3。

在发布到 Amazon S3 时，流日志数据将发布到您指定的现有 Amazon S3 存储桶。所有受监控网络接口的流日志记录将发布到存储桶中存储的一系列日志文件对象。如果流日志捕获 VPC 的数据，流日志将发布选定 VPC 中所有网络接口的流日志记录。有关更多信息，请参阅 [流日志记录 \(p. 166\)](#)。

要创建 Amazon S3 存储桶供流日志使用，请参阅 Amazon Simple Storage Service 入门指南 中的 [创建存储桶](#)。

目录

- [流日志文件 \(p. 172\)](#)
- [用于将流日志发布到 Amazon S3 的 IAM 角色 \(p. 172\)](#)
- [针对流日志的 Amazon S3 存储桶权限 \(p. 173\)](#)
- [与 SSE-KMS 存储桶结合使用时必需的 CMK 密钥策略 \(p. 174\)](#)
- [Amazon S3 日志文件权限 \(p. 174\)](#)
- [创建发布到 Amazon S3 的流日志 \(p. 174\)](#)
- [处理 Amazon S3 中的流日志记录 \(p. 175\)](#)

流日志文件

流日志收集流日志记录，将它们合并到日志文件，然后每隔五分钟将日志文件发布到 Amazon S3 存储桶。每个日志文件包含在上一个 5 分钟期间内记录的 IP 流量的流日志记录。

日志文件的最大文件大小为 75 MB。如果日志文件在 5 分钟期间内达到文件大小限制，流日志会停止向它添加流日志记录，将它发布到 Amazon S3 存储桶，然后创建一个新的日志文件。

日志文件将保存到指定的 Amazon S3 存储桶，并使用由流日志的 ID、区域及其创建日期决定的文件夹结构。存储桶文件夹结构使用以下格式：

```
bucket_ARN/optional_folder/AWSLogs/aws_account_id/  
vpcflowlogs/region/year/month/day/log_file_name.log.gz
```

同样，流日志的文件名由流日志的 ID、区域及其创建日期和时间决定。文件名使用以下格式：

```
aws_account_id_vpcflowlogs_region_flow_log_id_timestamp_hash.log.gz
```

Note

时间戳使用 YYYYMMDDTHHmNZ 格式。

例如，下面显示了一个流日志的日志文件的文件夹结构和文件名，该流日志是由 AWS 账户 123456789012 创建的，用于 us-east-1 区域中的资源，创建时间为 June 20, 2018 的 16:20 UTC，其中包含 16:15:00 到 16:19:59 的流日志记录：

```
arn:aws:s3:::my-flow-log-bucket/AWSLogs/123456789012/  
vpcflowlogs/us-east-1/2018/06/20/123456789012_vpcflowlogs_us-  
east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

用于将流日志发布到 Amazon S3 的 IAM 角色

IAM 委托人（例如，IAM 用户）必须具有足够的权限才能将流日志发布到 Amazon S3 存储桶。IAM 策略必须包含以下权限：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "logs:CreateLogDelivery",  
                "logs>DeleteLogDelivery"  
            ],  
            "Resource": "*"  
        }  
    ]
```

}

针对流日志的 Amazon S3 存储桶权限

默认情况下，Amazon S3 存储桶以及其中包含的对象都是私有的。只有存储桶拥有者才能访问存储桶和其中存储的对象。不过，存储桶拥有者可以通过编写访问策略来向其他资源和用户授予访问权限。

如果创建流日志的用户拥有存储桶，我们会自动向存储桶附加以下策略，以授予流日志将日志发布到存储桶的权限。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AWSLogDeliveryWrite",  
            "Effect": "Allow",  
            "Principal": {"Service": "delivery.logs.amazonaws.com"},  
            "Action": "s3:PutObject",  
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*",  
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}  
        },  
        {  
            "Sid": "AWSLogDeliveryAclCheck",  
            "Effect": "Allow",  
            "Principal": {"Service": "delivery.logs.amazonaws.com"},  
            "Action": "s3:GetBucketAcl",  
            "Resource": "arn:aws:s3:::bucket_name"  
        }  
    ]  
}
```

如果创建流日志的用户不拥有存储桶，也没有存储桶的 GetBucketPolicy 和 PutBucketPolicy 权限，流日志创建操作会失败。在这种情况下，存储桶拥有者必须手动将上述策略添加到存储桶，并指定流日志创建者的 AWS 账户 ID。有关更多信息，请参阅 Amazon Simple Storage Service 控制台用户指南中的[如何添加 S3 存储桶策略？](#)。如果存储桶从多个账户接收流日志，则将 Resource 元素条目添加到每个账户的 AWSLogDeliveryWrite 策略声明。例如，以下存储桶策略允许 AWS 账户 123123123123 和 456456456456 将流日志发布到名为 log-bucket 的存储桶中名为 flow-logs 的文件夹。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AWSLogDeliveryWrite",  
            "Effect": "Allow",  
            "Principal": {"Service": "delivery.logs.amazonaws.com"},  
            "Action": "s3:PutObject",  
            "Resource": [  
                "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",  
                "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"  
            ],  
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}  
        },  
        {  
            "Sid": "AWSLogDeliveryAclCheck",  
            "Effect": "Allow",  
            "Principal": {"Service": "delivery.logs.amazonaws.com"},  
            "Action": "s3:GetBucketAcl",  
            "Resource": "arn:aws:s3:::log-bucket"  
        }  
    ]  
}
```

Note

我们建议您向 AWSLogDeliveryAclCheck 和 AWSLogDeliveryWrite 权限授予日志传输 服务委托人，而不是单个 AWS 账户 ARN。

与 SSE-KMS 存储桶结合使用时必需的 CMK 密钥策略

如果使用具有客户托管的客户主密钥 (CMK) 的 AWS KMS 托管密钥 (SSE-KMS) 为 Amazon S3 存储桶启用了服务器端加密，则必须将以下内容添加到 CMK 的密钥策略中，以便流日志可以将日志文件写入存储桶。

```
{  
    "Sid": "Allow VPC Flow Logs to use the key",  
    "Effect": "Allow",  
    "Principal": {  
        "Service": [  
            "delivery.logs.amazonaws.com"  
        ]  
    },  
    "Action": [  
        "kms:Encrypt",  
        "kms:Decrypt",  
        "kms:ReEncrypt*",  
        "kms:GenerateDataKey*",  
        "kms:DescribeKey"  
    ],  
    "Resource": "*"  
}
```

Amazon S3 日志文件权限

除了必需的存储桶策略之外，Amazon S3 使用访问控制列表 (ACL) 管理对流日志创建的日志文件的访问。默认情况下，存储桶拥有者对每个日志文件具有 FULL_CONTROL 权限。如果日志传输拥有者与存储桶拥有者不同，则没有权限。日志传输账户具有 READ 和 WRITE 权限。有关更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的 [访问控制列表 \(ACL\) 概述](#)。

创建发布到 Amazon S3 的流日志

在您创建和配置 Amazon S3 存储桶后，您可以为 VPC、子网或网络接口创建流日志。

创建网络接口的流日志

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择一个或多个网络接口，然后选择操作、创建流日志。
4. 对于 Filter (筛选条件)，指定要记录的 IP 流量数据的类型。选择 All (全部) 将记录接受和拒绝的流量，选择 Rejected (已拒绝) 将仅记录被拒绝的流量，选择 Accepted (已接受) 将仅记录接受的流量。
5. 对于目的地，选择发送到 Amazon S3 存储桶。
6. 对于 S3 bucket ARN (S3 存储桶 ARN)，指定某个现有 Amazon S3 存储桶的 Amazon 资源名称 (ARN)。您可以在存储桶 ARN 中包括子文件夹。存储桶不能使用 AWSLogs 作为子文件夹名称，因为这是保留项。

例如，要指定名为 my-bucket 的存储桶中名为 my-logs 的子文件夹，请使用以下 ARN：

arn:aws:s3:::my-bucket/my-logs/

如果您拥有该存储桶，我们会自动创建资源策略并将它附加到该存储桶。有关更多信息，请参阅 [针对流日志的 Amazon S3 存储桶权限 \(p. 173\)](#)。

7. 选择 Create。

为 VPC 或子网创建流日志

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs (您的 VPC) 或 Subnets (子网)。
3. 选择一个或多个 VPC 或子网，然后选择操作、创建流日志。
4. 对于 Filter (筛选条件)，指定要记录的 IP 流量数据的类型。选择 All (全部) 将记录接受和拒绝的流量，选择 Rejected (已拒绝) 将仅记录被拒绝的流量，选择 Accepted (已接受) 将仅记录接受的流量。
5. 对于目的地，选择发送到 Amazon S3 存储桶。
6. 对于 S3 bucket ARN (S3 存储桶 ARN)，指定某个现有 Amazon S3 存储桶的 Amazon 资源名称 (ARN)。您可以在存储桶 ARN 中包括子文件夹。存储桶不能使用 AWSLogs 作为子文件夹名称，因为这是保留项。

例如，要指定名为 my-bucket 的存储桶中名为 my-logs 的子文件夹，请使用以下 ARN：

`arn:aws:s3:::my-bucket/my-logs/`

如果您拥有该存储桶，我们会自动创建资源策略并将它附加到该存储桶。有关更多信息，请参阅[针对流日志的 Amazon S3 存储桶权限 \(p. 173\)](#)。

7. 选择 Create。

处理 Amazon S3 中的流日志记录

日志文件是压缩文件。如果您使用 Amazon S3 控制台打开这些日志文件，则将对其进行解压缩，并且将显示流日志记录。如果您下载这些文件，则必须对其进行解压才能查看流日志记录。

您还可以使用 Amazon Athena 查询日志文件中的流日志记录。Amazon Athena 是一种交互式查询服务，让您能够使用标准 SQL 在 Amazon S3 中轻松分析数据。有关更多信息，请参阅 Amazon Athena 用户指南 中的[查询 Amazon VPC 流日志](#)。

使用流日志

您可以通过 Amazon EC2、Amazon VPC、CloudWatch 和 Amazon S3 控制台来使用流日志。

目录

- [控制流日志的使用 \(p. 175\)](#)
- [创建流日志 \(p. 176\)](#)
- [查看流日志 \(p. 176\)](#)
- [查看流日志记录 \(p. 176\)](#)
- [删除流日志 \(p. 177\)](#)
- [API 和 CLI 概述 \(p. 177\)](#)

控制流日志的使用

默认情况下，IAM 用户无权使用流日志。您可以创建一个 IAM 用户策略，该策略向用户授予创建、描述和删除流日志的权限。有关更多信息，请参阅 Amazon EC2 API Reference 中的[向 IAM 用户授予 Amazon EC2 资源必需的权限](#)。

下面是一个示例策略，该策略向用户授予创建、描述和删除流日志的完全权限。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteFlowLogs",
      "ec2>CreateFlowLogs",
      "ec2:DescribeFlowLogs"
    ],
    "Resource": "*"
  }
]
```

需要某些额外的 IAM 角色和权限配置，具体取决于您是发布到 CloudWatch Logs 还是 Amazon S3。有关更多信息，请参阅 [将流日志发布到 CloudWatch Logs \(p. 168\)](#) 和 [将流日志发布到 Amazon S3 \(p. 171\)](#)。

创建流日志

您可以为 VPC、子网或网络接口创建流日志。流日志可以将数据发布到 CloudWatch Logs 或 Amazon S3。

有关更多信息，请参阅 [创建发布到 CloudWatch Logs 的流日志 \(p. 170\)](#) 和 [创建发布到 Amazon S3 的流日志 \(p. 174\)](#)。

查看流日志

您可以在 Amazon EC2 和 Amazon VPC 控制台中，通过查看特定资源的 Flow Logs 选项卡来查看有关流日志的信息。当您选择资源时，将列出该资源的所有流日志。显示的信息包括流日志的 ID、流日志配置以及有关流日志的状态的信息。

查看您的网络接口的流日志的相关信息

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 选择网络接口，然后选择 Flow Logs (流日志)。此时有关流日志的信息将显示在选项卡上。Destination type (目标类型) 列指示要将流日志发布到的目标。

查看您的 VPC 或子网的流日志的相关信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs (您的 VPC) 或 Subnets (子网)。
3. 选择您的 VPC 或子网，然后选择 Flow Logs (流日志)。此时有关流日志的信息将显示在选项卡上。Destination type (目标类型) 列指示要将流日志发布到的目标。

查看流日志记录

您可以使用 CloudWatch Logs 控制台或 Amazon S3 控制台查看您的流日志记录，具体取决于所选的目标类型。在您创建流日志之后，可能需要几分钟才能显示在控制台中。

查看发布到 CloudWatch Logs 的流日志记录

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Logs (日志)，然后选择包含您的流日志的日志组。此时将显示每个网络接口的日志流的列表。
3. 选择包含要查看其流日志记录的网络接口 ID 的日志流。有关更多信息，请参阅 [流日志记录 \(p. 166\)](#)。

查看发布到 Amazon S3 的流日志记录

1. 通过以下网址打开 Amazon S3 控制台：[https://console.aws.amazon.com/s3/。](https://console.aws.amazon.com/s3/)
2. 对于 Bucket name (存储桶名称) , 选择流日志发布到的存储桶。
3. 对于 Name (名称) , 选中日志文件旁边的复选框。在对象概述面板上 , 选择 Download (下载)。

删除流日志

您可以使用 Amazon EC2 和 Amazon VPC 控制台删除流日志。

Note

使用这些过程可以禁用资源的流日志服务。删除流日志时 , 不会从 CloudWatch Logs 中删除现有日志流以及从 Amazon S3 中删除日志文件。必须使用相应服务的控制台来删除现有流日志数据。此外 , 删除发布到 Amazon S3 的流日志时 , 不会删除存储桶策略和日志文件访问控制列表 (ACL)。

删除网络接口的流日志

1. 打开 Amazon EC2 控制台 [https://console.aws.amazon.com/ec2/。](https://console.aws.amazon.com/ec2/)
2. 在导航窗格中 , 选择网络接口 , 然后选择网络接口。
3. 选择 Flow Logs (流日志) , 然后选择流日志的删除按钮 (叉号) 来删除该流日志。
4. 在确认对话框中 , 选择 Yes, Delete。

删除 VPC 或子网的流日志

1. 打开 Amazon VPC 控制台 [https://console.aws.amazon.com/vpc/。](https://console.aws.amazon.com/vpc/)
2. 在导航窗格中 , 选择 Your VPCs (您的 VPC) 或 Subnets (子网) , 然后选择资源。
3. 选择 Flow Logs (流日志) , 然后选择流日志的删除按钮 (叉号) 来删除该流日志。
4. 在确认对话框中 , 选择 Yes, Delete。

API 和 CLI 概述

您可以使用命令行或 API 执行此页面上介绍的任务。有关命令行界面的更多信息以及可用 API 操作的列表 , 请参阅[访问 Amazon VPC \(p. 7\)](#)。

创建流日志

- [create-flow-logs \(AWS CLI\)](#)
- [New-EC2FlowLog \(适用于 Windows PowerShell 的 AWS 工具\)](#)
- [CreateFlowLogs \(Amazon EC2 查询 API \)](#)

描述您的流日志

- [describe-flow-logs \(AWS CLI\)](#)
- [Get-EC2FlowLog \(适用于 Windows PowerShell 的 AWS 工具\)](#)
- [DescribeFlowLogs \(Amazon EC2 查询 API \)](#)

查看您的流日志记录 (日志事件)

- [get-log-events \(AWS CLI\)](#)
- [Get-CWLLogEvent \(适用于 Windows PowerShell 的 AWS 工具\)](#)

- [GetLogEvents](#) (CloudWatch API)

删除流日志

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DeleteFlowLogs](#) (Amazon EC2 查询 API)

故障排除

下面是您在使用流日志时可能遇到的问题。

问题

- [未完成的流日志记录 \(p. 178\)](#)
- [流日志处于活动状态，但没有流日志记录或日志组 \(p. 178\)](#)
- [错误 : LogDestinationNotFoundException \(p. 179\)](#)
- [超过 Amazon S3 存储桶策略限制 \(p. 179\)](#)

未完成的流日志记录

问题

您的流日志记录不完整，或者已不再发布。

原因

将流日志传送到 CloudWatch Logs 日志组时可能会出现问题。

解决方案

在 Amazon EC2 控制台或 Amazon VPC 控制台中，选择流日志选项卡以获取相关资源。有关更多信息，请参阅 [查看流日志 \(p. 176\)](#)。流日志表显示 Status 列中的所有错误。或者，使用 [describe-flow-logs](#) 命令，然后检查 DeliverLogsErrorMessage 字段中返回的值。可能会显示以下错误之一：

- [Rate limited](#)：如果应用了 CloudWatch 日志限制，则当某个网络接口的流日志记录数超过了可以在特定时间范围内发布的最大记录数时，会出现此错误。如果已达到您可创建的 CloudWatch Logs 日志组数量的上限，也可能出现此错误。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [CloudWatch 限制](#)。
- [Access error](#)：您的流日志的 IAM 角色没有足够的权限将流日志记录发布到 CloudWatch 日志组。有关更多信息，请参阅 [用于将流日志发布到 CloudWatch Logs 的 IAM 角色 \(p. 169\)](#)。
- [Unknown error](#)：流日志服务中出现内部错误。

流日志处于活动状态，但没有流日志记录或日志组

问题

您已创建了流日志，并且 Amazon VPC 或 Amazon EC2 控制台显示流日志为 Active。但是，您无法在 CloudWatch Logs 中看到任何日志流，也无法在 Amazon S3 存储桶中看到日志文件。

原因

原因可能是以下之一：

- 流日志仍处于创建过程中。在一些情况下，当您为要创建的日志组创建了流日志之后，有时会需要数分钟或更长时间才会显示数据。
- 还没有为您的网络接口记录任何流量。CloudWatch Logs 中的日志组仅在记录流量时创建。

解决方案

等待几分钟，以便系统创建日志组，或者记录流量。

错误：LogDestinationNotFoundException

问题

在您尝试创建流日志时收到了以下错误：LogDestinationNotFoundException

原因

在创建将数据发布到 Amazon S3 存储桶的流日志时，您可能会看到此错误。此错误指示无法找到指定的 S3 存储桶。

解决方案

请确保您指定了现有 S3 存储桶的 ARN，并且该 ARN 的格式正确。

超过 Amazon S3 存储桶策略限制

问题

在您尝试创建流日志时收到了以下错误：LogDestinationPermissionIssueException

原因

Amazon S3 存储桶策略的大小限制为 20 KB。

每次创建发布到 Amazon S3 存储桶的流日志时，我们都会自动将指定的存储桶 ARN（包括文件夹路径）添加到存储桶策略中的 Resource 元素。

创建发布到同一个存储桶的多个流日志可能会导致超出存储桶策略限制。

解决方案

请执行下列操作之一：

- 通过删除不再需要的流日志条目来清理存储桶的策略。
- 通过使用以下内容替换各个流日志条目，为整个存储桶授予权限：

```
arn:aws:s3:::bucket_name/*
```

如果您授予整个存储桶的权限，则新的流日志订阅不会向存储桶策略添加新权限。

VPC 联网组件

您可以使用以下组件配置您的 VPC 网络化：

联网组件

- 网络接口 (p. 180)
- 路由表 (p. 181)
- Internet 网关 (p. 192)
- 仅出口 Internet 网关 (p. 197)
- DHCP 选项集 (p. 224)
- DNS (p. 228)
- 弹性 IP 地址 (p. 232)
- VPC 终端节点 (p. 235)
- NAT (p. 200)
- VPC 对等 (p. 232)
- ClassicLink (p. 274)

弹性网络接口

弹性网络接口 (本文档称为网络接口) 是可包含以下属性的虚拟网络接口：

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

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

VPC 中的每个实例都有一个默认网络接口（主网络接口），系统会为该接口在 VPC 的 IPv4 地址范围内指定一个私有 IPv4 地址。您无法从实例断开主网络接口。您可以创建其他网络接口并将其挂载至您的 VPC 中的任何实例。您可以挂载的网络接口数因实例类型而有所差异。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[每个实例类型的每个网络接口的 IP 地址](#)。

当您想执行以下操作时，将多个网络接口附加到一个实例很有帮助：

- 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。

有关网络接口的更多信息以及在 Amazon EC2 控制台中使用网络接口的说明，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[弹性网络接口部分](#)。

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。一个子网一次只能与一个路由表关联，但您可以将多个子网与同一路由表关联。

内容

- [路由表基本信息 \(p. 181\)](#)
- [路由优先级 \(p. 184\)](#)
- [路由选项 \(p. 185\)](#)
- [使用路由表 \(p. 188\)](#)
- [API 和命令概览 \(p. 191\)](#)

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，则这个子网将与主路由表建立隐式关联。
- 您不能删除主路由表，但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）。
- 表中的每项路由都指定了一个目的 CIDR 和目标（例如，指向数据包被外部企业网络的 172.16.0.0/12 的数据将通向虚拟专用网关）。我们使用与流量匹配的最明确路由以判断数据流的路由方式。
 - IPv4 和 IPv6 的 CIDR 块是分开处理的。例如，目标 CIDR 为 0.0.0.0/0（所有 IPv4 地址）的路由不会自动包括所有 IPv6 地址。您必须为所有 IPv6 地址创建目标 CIDR 为 ::/0 的路由。
- 每个路由表都包含一个用于在 VPC 内部通过 IPv4 进行通信的本地路由。如果您的 VPC 有多个 IPv4 CIDR 块，则路由表为每个 IPv4 CIDR 块包含一个本地路由。如果您已将 IPv6 CIDR 块与 VPC 关联，则路由表为 IPv6 CIDR 块包含一个本地路由。您无法修改或删除这些路由。
- 在 VPC 中添加 Internet 网关、仅出口 Internet 网关、虚拟专用网关、NAT 设备、对等连接或 VPC 终端节点时，必须更新所有使用这些网关或连接的子网的路由表。
- 在每个 VPC 上创建的路由表和在每个路由表中添加的路由均存在数量限制。有关更多信息，请参阅[Amazon VPC 限制 \(p. 276\)](#)。

主路由表

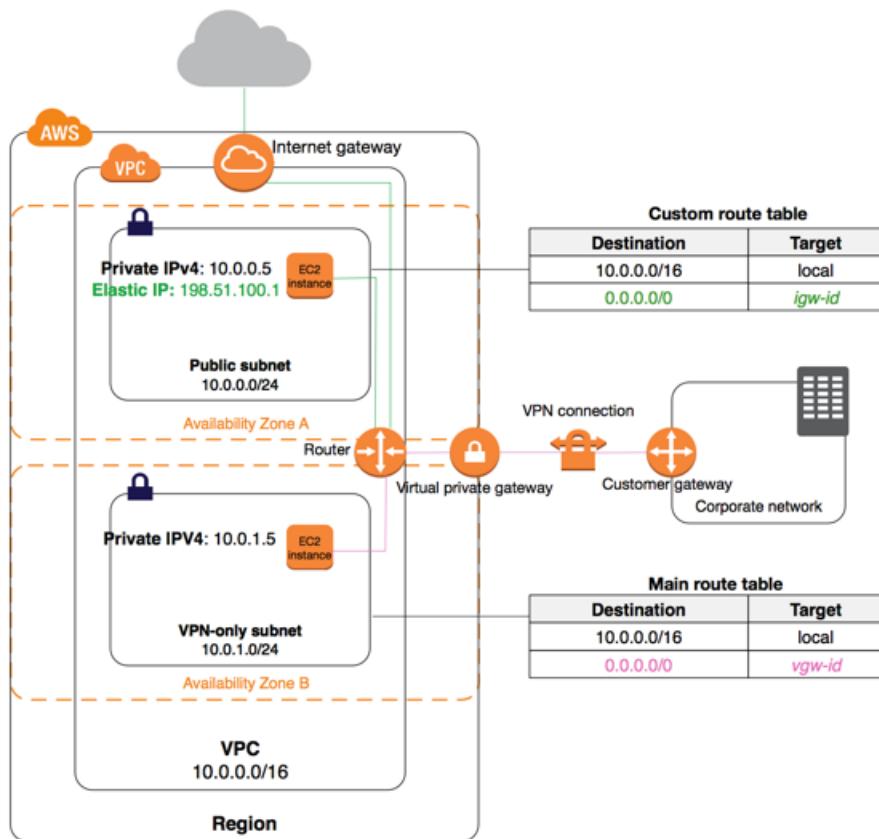
当您创建 VPC 时，它会自动生成主路由表。在 Amazon VPC 控制台中的 Route Tables 页面上，通过在 Main 列中查找 Yes 可以查看 VPC 的主路由表。主路由表控制未与任何其他路由表显式关联的所有子网的路由。您可以在主路由表中添加、删除和修改路由。

即使某个子网与主路由表已隐式关联，您也可以将它们显式关联。当您更改用作主路由表的表时，可以这样做。这会更改其他新子网或所有未与任何其他路由表显式关联的子网的默认设置。有关更多信息，请参阅[替换主路由表 \(p. 190\)](#)。

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显式控制每个子网的出站数据流的路由方式。

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



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），则新子网会自动生成通往 Internet 网关的路由。

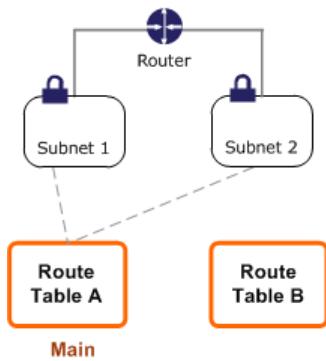
路由表关联

VPC 控制台显示与每个路由表显式关联的子网的数量，并提供与主路由表隐式关联的子网的信息。有关更多信息，请参阅 [判断与表显式关联的子网 \(p. 188\)](#)。

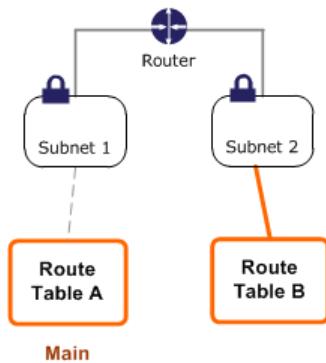
子网可以与主路由表建立显式或隐式关联。子网通常不会与主路由表建立显式关联，尽管当您替换主路由表时可能会临时生成显式关联。

您可能需要更改主路由表，但是为了避免数据流中断，您可以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。

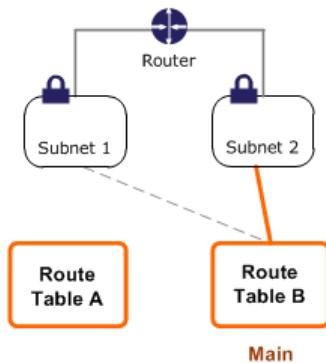
下图展示的是一个有两个子网的 VPC，并且这些子网都与主路由表（路由表 A）有隐式关联，自定义路由表（路由表 B）则未与任何子网相关。



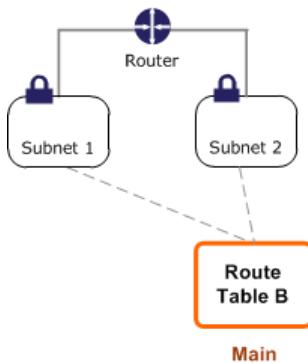
您可以在子网 2 和路由表 B 之间建立显式关联。



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。



路由优先级

我们使用路由表中与流量匹配的最具体的路由来判断数据流的路由方式 (最长前缀匹配)。

到 IPv4 和 IPv6 地址或 CIDR 块的路由是彼此独立的；我们使用与 IPv4 流量或 IPv6 流量匹配的最明确的路由来确定如何路由流量。

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

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

如果您已将一个虚拟专用网关连接到 VPC，并且已启用路由表上的路由传播，则代表Site-to-Site VPN 连接的路由会在您的路由表中自动显示为已传播路由。有关更多信息，请参阅[路由表和 VPN 路由优先级](#)。

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

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

路由选项

以下主题介绍了您的 VPC 中的特定网关或连接的路由。

选项

- [Internet 网关的路由表 \(p. 185\)](#)
- [NAT 设备的路由表 \(p. 185\)](#)
- [虚拟专用网关的路由表 \(p. 185\)](#)
- [VPC 对等连接的路由表 \(p. 185\)](#)
- [ClassicLink 路由表 \(p. 186\)](#)
- [VPC 终端节点的路由表 \(p. 187\)](#)
- [仅出口 Internet 网关的路由表 \(p. 187\)](#)
- [中转网关的路由表 \(p. 187\)](#)

Internet 网关的路由表

您可以通过向 Internet 网关添加路由来将一个子网设为公有子网。为此，请创建一个 Internet 网关并将其附加到您的 VPC，然后添加一个目的地为 `0.0.0.0/0` (对于 IPv4 流量) 或 `::/0` (对于 IPv6 流量) 且目标为 Internet 网关 ID (`igw-xxxxxxxx`) 的路由。有关更多信息，请参阅[Internet 网关 \(p. 192\)](#)。

NAT 设备的路由表

要使私有子网中的实例能够连接到 Internet，您可以在公有子网中创建一个 NAT 网关或启动 NAT 实例，然后为私有子网添加一个路由以将 IPv4 Internet 流量 (`0.0.0.0/0`) 路由到 NAT 设备。有关更多信息，请参阅[NAT 网关 \(p. 200\)](#) 和 [NAT 实例 \(p. 216\)](#)。NAT 设备不能用于 IPv6 流量。

虚拟专用网关的路由表

您可以使用 AWS Site-to-Site VPN 连接来支持 VPC 中的实例与您自己的网络进行通信。为此，请创建一个虚拟专用网关并将其附加到您的 VPC，然后添加一个目的地为您的网络且目标为虚拟专用网关 (`vgw-xxxxxxxx`) 的路由。您随后可以创建和配置 Site-to-Site VPN 连接。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的[什么是 AWS Site-to-Site VPN？](#)

我们目前不支持通过 AWS Site-to-Site VPN 连接的 IPv6 流量。但是，我们支持通过虚拟专用网关路由到 AWS Direct Connect 连接的 IPv6 流量。有关更多信息，请参阅[AWS Direct Connect 用户指南](#)。

VPC 对等连接的路由表

VPC 对等连接是两个 VPC 之间的网络连接，通过此连接，您可以使用私有 IPv4 地址在这两个 VPC 之间路由流量。任何一个 VPC 中的实例都可以彼此通信，就像它们属于同一网络中一样。

要在 VPC 对等连接中的 VPC 之间实现流量路由，必须将一个路由添加到 VPC 的一个或多个路由表，该路由指向 VPC 对等连接以访问对等连接中另一个 VPC 的全部或部分 CIDR 块。同样，另一个 VPC 的拥有者必须将一个路由添加到其 VPC 的路由表，以将流量路由回您的 VPC。

例如，您在具有以下信息的两个 VPC 之间具有 VPC 对等连接 (`pcx-1a2b1a2b`)：

- VPC A : `vpc-1111aaaa`，CIDR 块为 `10.0.0.0/16`
- VPC B : `vpc-2222bbbb`，CIDR 块为 `172.31.0.0/16`

要启用 VPC 之间的流量并允许访问任一 VPC 的整个 IPv4 CIDR 块，VPC A 的路由表的配置如下所示。

目的地	目标
10.0.0.0/16	本地
172.31.0.0/16	pcx-1a2b1a2b

VPC B 的路由表的配置如下所示。

目的地	目标
172.31.0.0/16	本地
10.0.0.0/16	pcx-1a2b1a2b

您的 VPC 对等连接也可以支持 VPC 中实例之间的 IPv6 通信，前提是已启用 VPC 和实例进行 IPv6 通信。有关更多信息，请参阅 [VPC 和子网 \(p. 75\)](#)。要在 VPC 之间启用 IPv6 流量路由，您必须向路由表中添加一条指向 VPC 对等连接的路由，以访问对等 VPC 的全部或部分 IPv6 CIDR 块。

例如，仍使用上面的 VPC 对等连接 (pcx-1a2b1a2b)，假设 VPC 具有以下信息：

- VPC A : IPv6 CIDR 块为 2001:db8:1234:1a00::/56
- VPC B : IPv6 CIDR 块为 2001:db8:5678:2b00::/56

要通过 VPC 对等连接启用 IPv6 通信，请将以下路由添加到 VPC A 的路由表中：

目的地	目标
10.0.0.0/16	本地
172.31.0.0/16	pcx-1a2b1a2b
2001:db8:5678:2b00::/56	pcx-1a2b1a2b

将以下路由添加到 VPC B 的路由表中：

目的地	目标
172.31.0.0/16	本地
10.0.0.0/16	pcx-1a2b1a2b
2001:db8:1234:1a00::/56	pcx-1a2b1a2b

有关 VPC 对等连接的更多信息，请参阅 [Amazon VPC Peering Guide](#)。

ClassicLink 路由表

ClassicLink 功能允许您将 EC2-Classic 实例链接到 VPC，从而允许 EC2-Classic 实例与 VPC 中使用私有 IPv4 地址的实例进行通信。有关 ClassicLink 的更多信息，请参阅 [ClassicLink \(p. 274\)](#)。

为 VPC 启用 ClassicLink 时，会向所有 VPC 的路由表添加一个路由，其目的地为 10.0.0.0/8，目标为 local。这允许 VPC 中的实例与后来链接到该 VPC 的任意 EC2-Classic 实例之间进行通信。如果您向启用

了 ClassicLink 的 VPC 另外添加一个路由表，该路由表会自动接收一个目的地为 10.0.0.0/8 并且目标为 local 的路由。如果禁用 VPC 的 ClassicLink，会从该 VPC 的所有路由表中自动删除此路由。

如果您的 VPC 的任意路由表具有地址范围在 10.0.0.0/8 CIDR 内的现有路由，则无法为该 VPC 启用 ClassicLink。这不包括 VPC 的 10.0.0.0/16 和 10.1.0.0/16 IP 地址范围的本地路由。

如果您已经为 VPC 启用了 ClassicLink，则无法再在路由表中添加 10.0.0.0/8 IP 地址范围的任何具体路由。

如果您修改 VPC 对等连接以允许 VPC 中的实例与已链接到对等 VPC 的 EC2-Classic 实例之间的通信，则静态路由将自动添加到您的路由表，其目的地为 10.0.0.0/8，目标为 local。如果您修改 VPC 对等连接以允许已链接到 VPC 的本地 EC2-Classic 实例与对等 VPC 中的实例之间的通信，则必须手动将路由添加到您的主路由表，其目的地为对等 VPC CIDR 块，目标为 VPC 对等连接。EC2-Classic 实例依赖主路由表来路由到对等 VPC。有关更多信息，请参阅 Amazon VPC Peering Guide 中的[使用 ClassicLink 进行配置](#)。

VPC 终端节点的路由表

使用 VPC 终端节点可以在您的 VPC 和其他 AWS 服务之间创建私有连接。创建终端节点时，您指定 VPC 中由该终端节点使用的路由表。路由会自动添加到每个路由表中，这些路由表的目的地指定服务的前缀列表 ID (p1-XXXXXX) ，目标具有相应终端节点 ID (vpce-XXXXXX)。您无法显式删除或修改终端节点路由，但可更改终端节点所使用的路由表。

有关终端节点路由的更多信息以及对到 AWS 服务的路由的影响，请参阅[网关终端节点路由 \(p. 250\)](#)。

仅出口 Internet 网关的路由表

您可以为 VPC 创建仅出口 Internet 网关，以允许私有子网中的实例发起到 Internet 的出站通信，但阻止 Internet 发起与这些实例的连接。仅出口 Internet 网关只适用于 IPv6 流量。要为仅出口 Internet 网关配置路由，请为将 IPv6 Internet 流量 (:/:0) 路由到仅出口 Internet 网关的私有子网添加路由。有关更多信息，请参阅[仅出口 Internet 网关 \(p. 197\)](#)。

中转网关的路由表

当您将 VPC 附加到 transit gateway 时，您需要添加流量的路由以便路由通过 transit gateway。

考虑以下场景：您有三个 VPC 附加到 transit gateway。在此场景中，所有附件都与 transit gateway 路由表关联且传播到 transit gateway 路由表。因此，所有附件都可以将数据包路由到彼此，而将 transit gateway 用作简单第 3 层 IP 集线器。

例如，您有两个 VPC，其中包含以下信息：

- VPC A : 10.1.0.0/16，附加 ID tgw-attach-1111111111111111
- VPC B : 10.2.0.0/16，附件 ID tgw-attach-2222222222222222

要启用 VPC 之间的流量并允许访问 transit gateway，VPC A 路由表的配置如下所示。

目的地	目标
10.1.0.0/16	本地
10.0.0.0/8	tgw-id

以下是 VPC 附件项的 transit gateway 路由表条目的示例。

目的地	目标
10.1.0.0/16	tgw-attach-1111111111111111

目的地	目标
10.2.0.0/16	tgw-attach-22222222222222222222

使用路由表

以下任务显示如何使用路由表。

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。

任务

- [判断与子网关联的具体路由表 \(p. 188\)](#)
- [判断与表显式关联的子网 \(p. 188\)](#)
- [创建自定义路由表 \(p. 189\)](#)
- [在路由表中添加和删除路由 \(p. 189\)](#)
- [启用和禁用路由传播 \(p. 189\)](#)
- [将子网与路由表关联 \(p. 190\)](#)
- [更改子网路由表 \(p. 190\)](#)
- [解除子网与路由表的关联 \(p. 190\)](#)
- [替换主路由表 \(p. 190\)](#)
- [删除路由表 \(p. 191\)](#)

判断与子网关联的具体路由表

可通过在 Amazon VPC 控制台中查看子网的详细信息，判断该子网与哪个路由表关联。

判断与子网关联的路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets。
3. 子网详细信息显示在 Summary (摘要) 选项卡中。选择 Route Table 选项卡可查看路由表 ID 及其路由。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，请参阅[判断与表显式关联的子网 \(p. 188\)](#)。

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，请参阅[替换主路由表 \(p. 190\)](#)）。

判断显式关联的子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables。
3. 查看 Explicitly Associated With 列以确定显式关联的子网数。
4. 选择所需的路由表。

- 在详细信息窗格中，选择 Subnet 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

您可以使用 Amazon VPC 控制台为 VPC 创建自定义路由表。

创建自定义路由表

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Route Tables。
- 选择 Create Route Table。
- 在 Create Route Table 对话框中，您可以选择为 Name tag 命名您的路由表。这样做可创建具有 Name 键以及指定值的标签。针对 VPC 选择您的 VPC，然后选择 Yes, Create。

在路由表中添加和删除路由

您可在路由表中添加、删除和修改路由。您只能修改已添加的路由。

修改路由或将路由添加到路由表

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Route Tables，然后选择路由表。
- 依次选择 Actions (操作)、Edit routes (编辑路由)。
- 要添加路由，请选择 Add route (添加路由)，为 Destination (目的地) 输入目的地 CIDR 块或单个 IP 地址，然后为 Target (目标) 选择一个目标。
- 要修改现有路由，请为 Destination 替换目的地 CIDR 块或单个 IP 地址，然后为 Target 选择一个目标。
- 完成后选择 Save routes (保存路由)。

从路由表中删除路由

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Route Tables，然后选择路由表。
- 依次选择 Actions (操作)、Edit routes (编辑路由)。
- 选择您希望删除的路由右侧的删除按钮（“x”）。
- 完成后选择 Save routes (保存路由)。

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，请参阅 Site-to-Site VPN 用户指南 中的 [Site-to-Site VPN 路由选项](#)。

启用路由传播

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Route Tables，然后选择路由表。
- 依次选择 Actions (操作) 和 Edit route propagation (编辑路由传播)。
- 选中虚拟专用网关旁边的 Propagate 复选框，然后选择 Save。

禁用路由传播

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables，然后选择路由表。
3. 依次选择 Actions (操作) 和 Edit route propagation (编辑路由传播)。
4. 取消选中 Propagate 复选框，然后选择 Save。

将子网与路由表关联

若要对特定子网应用路由表路由，您必须将路由表与子网关联。一个路由表可以与多个子网关联；但是一个子网一次只能与一个路由表关联。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。

关联路由表和子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables，然后选择路由表。
3. 在 Subnet Associations 选项卡上，选择 Edit。
4. 选中要与路由表关联的子网的 Associate 复选框，然后选择 Save。

更改子网路由表

您可以更改与子网关联的路由表。

更改子网路由表关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets，然后选择子网。
3. 在 Route Table 选项卡中，选择 Edit。
4. 从 Change to 列表中选择要与子网关联的新路由表，然后选择 Save。

解除子网与路由表的关联

您可以解除子网与路由表的关联。在将子网与其他路由表关联前，它与主路由表是隐式关联的。

解除子网与路由表的关联

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables，然后选择路由表。
3. 在 Subnet Associations 选项卡中，选择 Edit。
4. 取消选中子网的 Associate 复选框，然后选择 Save。

替换主路由表

您也可以更改作为 VPC 中主路由表的路由表。

替换主路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables。
3. 选择应为新的主路由表的路由表，然后选择 Set as Main Table。
4. 在确认对话框中，选择 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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables，然后选择路由表。
3. 在 Subnet Associations 选项卡中，选择 Edit。
4. 取消选中子网的 Associate 复选框，然后选择 Save。

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables。
3. 选择路由表，然后选择 Delete Route Table。
4. 在确认对话框中，选择 Yes, Delete。

API 和命令概览

您可以使用命令行或 API 执行此页面上介绍的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

创建自定义路由表

- [create-route-table](#) (AWS CLI)
- [New-EC2RouteTable](#) (适用于 Windows PowerShell 的 AWS 工具)

在路由表中添加路由

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (适用于 Windows PowerShell 的 AWS 工具)

将子网与路由表关联起来

- [associate-route-table](#) (AWS CLI)
- [Register-EC2RouteTable](#) (适用于 Windows PowerShell 的 AWS 工具)

说明一个或多个路由表

- [describe-route-tables](#) (AWS CLI)
- [Get-EC2RouteTable](#) (适用于 Windows PowerShell 的 AWS 工具)

从路由表中删除一条路由

- [delete-route](#) (AWS CLI)
- [Remove-EC2Route](#) (适用于 Windows PowerShell 的 AWS 工具)

替换路由表中的一条现有路由

- [replace-route](#) (AWS CLI)
- [Set-EC2Route](#) (适用于 Windows PowerShell 的 AWS 工具)

解除子网与路由表的关联

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (适用于 Windows PowerShell 的 AWS 工具)

更改与子网关联的路由表

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (适用于 Windows PowerShell 的 AWS 工具)

创建与 Site-to-Site VPN 连接关联的静态路由

- [create-vpn-connection-route](#) (AWS CLI)
- [New-EC2VpnConnectionRoute](#) (适用于 Windows PowerShell 的 AWS 工具)

删除与 Site-to-Site VPN 连接关联的静态路由

- [delete-vpn-connection-route](#) (AWS CLI)
- [Remove-EC2VpnConnectionRoute](#) (适用于 Windows PowerShell 的 AWS 工具)

启用虚拟专用网关 (VGW) 以将路由传播至 VPC 的路由表

- [enable-vgw-route-propagation](#) (AWS CLI)
- [Enable-EC2VgwRoutePropagation](#) (适用于 Windows PowerShell 的 AWS 工具)

禁止 VGW 传播路由至 VPC 的路由表

- [disable-vgw-route-propagation](#) (AWS CLI)
- [Disable-EC2VgwRoutePropagation](#) (适用于 Windows PowerShell 的 AWS 工具)

删除路由表

- [delete-route-table](#) (AWS CLI)
- [Remove-EC2RouteTable](#) (适用于 Windows PowerShell 的 AWS 工具)

Internet 网关

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

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

Internet 网关支持 IPv4 和 IPv6 流量。

启用 Internet 访问

要为 VPC 子网中的实例启用 Internet 访问，必须执行以下操作：

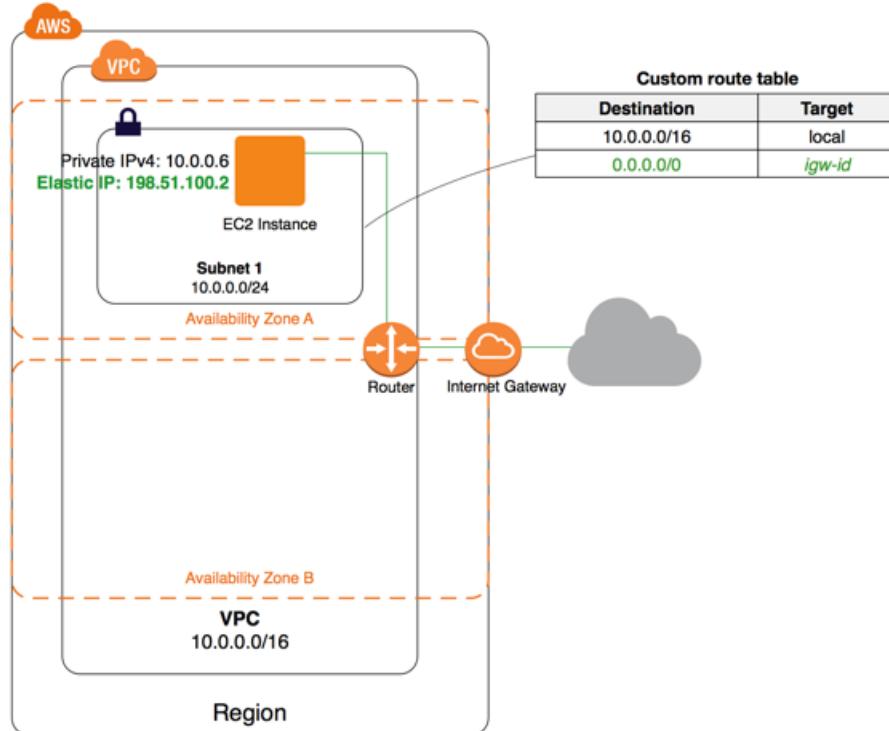
- 将 Internet 网关附加到 VPC。
- 确保子网的路由表指向 Internet 网关。
- 确保您的子网中的实例具有全局唯一 IP 地址（公有 IPv4 地址、弹性 IP 地址或 IPv6 地址）。
- 确保您的网络访问控制和安全组规则允许相关流量在您的实例中流入和流出。

要使用 Internet 网关，子网的路由表必须包含将 Internet 绑定流量定向到该 Internet 网关的路由。您可以将路由范围设定为路由表未知的所有目标（IPv4 为 $0.0.0.0/0$ ，IPv6 为 $::/0$ ），也可以将路由范围设定为一个较小的 IP 地址范围，例如，公司在 AWS 以外的公有终端节点的公有 IPv4 地址，或 VPC 以外的其他 Amazon EC2 实例的弹性 IP 地址。如果子网的关联路由表包含指向 Internet 网关的路由，则该子网称为公有子网。

要为 IPv4 启用 Internet 通信，实例必须具有与实例上的私有 IPv4 地址相关联的公有 IPv4 地址或弹性 IP 地址。实例只了解 VPC 和子网内定义的私有（内部）IP 地址空间。Internet 网关以逻辑方式代表实例提供一对一 NAT，这样一来，当流量离开 VPC 子网并流向 Internet 时，回复地址字段将设置为实例的公有 IPv4 地址或弹性 IP 地址，而不是私有 IP 地址。相反，指定发往实例的公有 IPv4 地址或弹性 IP 地址的流量会先将其目标地址转换为实例的私有 IPv4 地址，然后再传输到 VPC。

要为 IPv6 启用 Internet 通信，VPC 和子网必须具有关联的 IPv6 CIDR 块，并且必须为实例分配此子网范围内的 IPv6 地址。IPv6 地址是全球唯一的，因此默认为公有。

在下图中，VPC 中的子网 1 与自定义路由表相关联，该路由表将所有 Internet 绑定的 IPv4 流量指向一个 Internet 网关。实例具有弹性 IP 地址，可以与 Internet 通信。



对默认和非默认 VPC 的 Internet 访问

下表概述了 VPC 是否自动提供通过 IPv4 或 IPv6 进行 Internet 访问所需的组件。

组件	默认 VPC	非默认 VPC
Internet 网关	是	如果 VPC 是使用 VPC 向导中的第一个或第二个选项创建的，则是。否则，必须手动创建和连接 Internet 网关。
包含将 IPv4 流量路由到 Internet 网关的路由的路由表 (0.0.0.0/0)	是	如果 VPC 是使用 VPC 向导中的第一个或第二个选项创建的，则是。否则，您必须手动创建路由表并添加此路由。
包含将 IPv6 流量路由到 Internet 网关的路由的路由表 (::/0)	否	如果此 VPC 是使用 VPC 向导中的第一个或第二个选项创建的，并且您指定了将 IPv6 CIDR 块与此 VPC 关联的选项，则是。否则，您必须手动创建路由表并添加此路由。
公有 IPv4 地址自动分配到在子网中启动的实例	是 (默认子网)	否 (非默认子网)
IPv6 地址自动分配到在子网中启动的实例	否 (默认子网)	否 (非默认子网)

有关默认 VPC 的更多信息，请参阅[默认 VPC 和默认子网 \(p. 93\)](#)。有关使用 VPC 向导创建具有 Internet 网关的 VPC 的更多信息，请参阅[场景 1：带单个公有子网的 VPC \(p. 23\)](#)或[场景 2：带有公有子网和私有子网 \(NAT\) 的 VPC \(p. 29\)](#)。

有关您的 VPC 中的 IP 寻址以及控制如何为实例分配公有 IPv4 或 IPv6 地址的更多信息，请参阅[您的 VPC 中的 IP 地址 \(p. 100\)](#)。

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。

创建带有 Internet 网关的 VPC

下面介绍如何手动创建一个公有子网来支持 Internet 访问。

任务

- [创建子网 \(p. 194\)](#)
- [创建并附加 Internet 网关 \(p. 195\)](#)
- [创建自定义路由表 \(p. 195\)](#)
- [更新安全组规则 \(p. 195\)](#)
- [添加弹性 IP 地址 \(p. 196\)](#)
- [将 Internet 网关与您的 VPC 断开 \(p. 196\)](#)
- [删除 Internet 网关 \(p. 197\)](#)
- [API 和命令概览 \(p. 197\)](#)

创建子网

为您的 VPC 添加子网

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，选择 Subnets，然后选择 Create Subnet。
3. 在 Create Subnet 对话框中，选择 VPC，选择可用区，为子网指定 IPv4 CIDR 块。
4. (可选，仅限 IPv6) 对于 IPv6 CIDR block，选择 Specify a custom IPv6 CIDR。
5. 选择 Yes, Create。

有关子网的更多信息，请参阅[VPC 和子网 \(p. 75\)](#)。

创建并附加 Internet 网关

创建 Internet 网关并将其附加到 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Internet Gateways (Internet 网关)，然后选择 Create internet gateway (创建 Internet 网关)。
3. (可选) 为 Internet 网关命名，然后选择 Create (创建)
4. 选择刚刚创建的 Internet 网关，然后选择 Actions, Attach to VPC (操作，附加到 VPC)。
5. 从列表中选择 VPC，然后选择 Attach (附加)。

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。默认情况下，主路由表不包含至 Internet 网关的路由。以下过程创建一个自定义路由表 (其中一个路由将目标为 VPC 外的流量发送到 Internet 网关) 并将此路由表与子网相关联。

创建自定义路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables，然后选择 Create Route Table。
3. 在 Create Route Table 对话框中，可以选择命名您的路由表，选择您的 VPC，然后选择 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，依次选择 Edit、Add another route，然后根据需要添加以下路由。完成此操作后，选择 Save。
 - 对于 IPv4 流量，在 Destination (目的地) 框中指定 0.0.0.0/0，然后在 Target (目标) 列表中选择 Internet 网关 ID。
 - 对于 IPv6 流量，在 Destination (目的地) 框中指定 ::/0，然后在 Target (目标) 列表中选择 Internet 网关 ID。
6. 在 Subnet Associations 选项卡上，选择 Edit，选中子网的 Associate 复选框，然后选择 Save。

有关更多信息，请参阅[路由表 \(p. 181\)](#)。

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 的任何入站流量，但允许通往 Internet 的所有出站流量。因此，要使实例能够与 Internet 通信，请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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，然后选择 Create Security Group。

3. 在“Create Security Group”对话框中，为您的安全组指定名称和说明。从 VPC 列表中选择您的 VPC 的 ID，然后选择 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 Rules 选项卡上，选择 Edit。选择 Add Rule，然后填写所需信息。例如，从 Type 列表中选择 HTTP 或 HTTPS，然后在 Source 中输入 0.0.0.0/0 (对于 IPv4 流量) 或 ::/0 (对于 IPv6 流量)。完成此操作后，选择 Save。
6. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
7. 在导航窗格中，选择 Instances。
8. 依次选择实例、Actions、Networking 和 Change Security Groups。
9. 在 Change Security Groups (更改安全组) 对话框中，清除当前所选安全组的复选框，然后选中一个新的复选框。选择 Assign Security Groups。

有关更多信息，请参阅[您的 VPC 的安全组 \(p. 119\)](#)。

添加弹性 IP 地址

在子网中启动实例之后，如果希望它能够通过 IPv4 连接 Internet，则必须为其指定弹性 IP 地址。

Note

如果在启动过程中向实例分配了公有 IPv4 地址，则实例可从 Internet 进行访问，无需向它分配弹性 IP 地址。想要了解更多有关您实例的 IP 寻址的信息，请参阅[您的 VPC 中的 IP 地址 \(p. 100\)](#)。

使用控制台分配弹性 IP 地址并将其分配给一个实例

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate new address。
4. 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

5. 从列表中选择弹性 IP 地址，选择 Actions，然后选择 Associate address。
6. 选择 Instance 或 Network interface，然后选择实例 ID 或网络接口 ID。选择要与弹性 IP 地址关联的私有 IP 地址，然后选择 Associate。

有关更多信息，请参阅[弹性 IP 地址 \(p. 232\)](#)。

将 Internet 网关与您的 VPC 断开

如果不再需要通过 Internet 访问在非默认 VPC 中启动的实例，则可将 Internet 网关与 VPC 分离。如果 VPC 的某些资源具有关联的公有 IP 地址或弹性 IP 地址，则无法分离 Internet 网关。

分离 Internet 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs，然后选择弹性 IP 地址。
3. 选择 Actions、Disassociate address。选择 Disassociate address。
4. 在导航窗格中，选择 Internet Gateways。
5. 选择相应的 Internet 网关，然后选择 Actions, Detach from VPC (操作，与 VPC 分离)。
6. 在 Detach from VPC (与 VPC 分离) 对话框中，选择 Detach (分离)。

删除 Internet 网关

如果不再需要 Internet 网关，可将其删除。无法删除仍附加到 VPC 的 Internet 网关。

删除 Internet 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Internet Gateways。
3. 选择相应的 Internet 网关，然后依次选择 Actions (操作) 和 Delete internet gateway (删除 Internet 网关)。
4. 在 Delete internet gateway (删除 Internet 网关) 对话框中，选择 Delete (删除)。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅[访问 Amazon VPC \(p. 7\)](#)。

创建 Internet 网关

- [create-internet-gateway](#) (AWS CLI)
- [New-EC2InternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

将 Internet 网关附加到 VPC

- [attach-internet-gateway](#) (AWS CLI)
- [Add-EC2InternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

描述 Internet 网关

- [describe-internet-gateways](#) (AWS CLI)
- [Get-EC2InternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

将 Internet 网关与 VPC 分离

- [detach-internet-gateway](#) (AWS CLI)
- [Dismount-EC2InternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

删除 Internet 网关

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

仅出口 Internet 网关

仅出口 Internet 网关是一种横向扩展、支持冗余且高度可用的 VPC 组件，它能够实现从 VPC 中的实例经由 IPv6 到 Internet 的出站通信，并防止 Internet 发起与您的实例的 IPv6 连接。

Note

仅出口 Internet 网关只适用于 IPv6 流量。要通过 IPv4 实现仅出站 Internet 通信，请改用 NAT 网关。有关更多信息，请参阅[NAT 网关 \(p. 200\)](#)。

内容

- [仅出口 Internet 网关基本知识 \(p. 198\)](#)
- [使用仅出口 Internet 网关 \(p. 198\)](#)
- [API 和 CLI 概述 \(p. 200\)](#)

仅出口 Internet 网关基本知识

如果公有子网中的实例具有公有 IPv4 地址或 IPv6 地址，则其能够通过 Internet 网关连接到 Internet。同样，Internet 上的资源也可以使用其公有 IPv4 地址或 IPv6 地址发起与您的实例的连接，例如，当您使用本地计算机连接实例时。

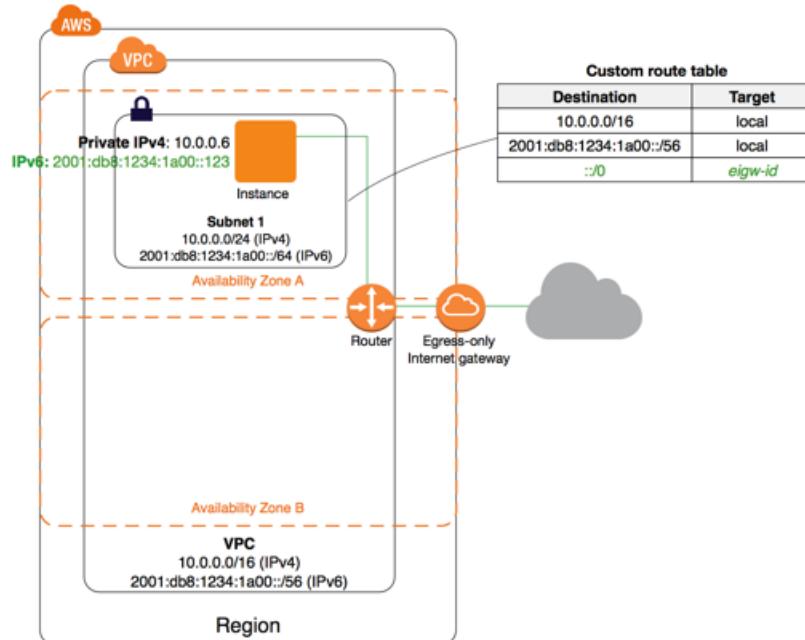
IPv6 地址是全球唯一的，因此默认为公有。如果您希望实例能够访问 Internet，但又想要阻止 Internet 上的资源发起与您的实例的通信，则您可以使用仅出口 Internet 网关。为此，请在 VPC 中创建一个仅出口 Internet 网关，然后向路由表中添加一条将所有 IPv6 流量 ($::/0$) 或特定的 IPv6 地址范围指向仅出口 Internet 网关的路由。子网中与路由表关联的 IPv6 流量会被路由到仅出口 Internet 网关。

仅出口 Internet 网关是有状态的：它将来自子网中实例的流量转发到 Internet 或其他 AWS 服务，然后将响应发回给实例。

仅出口 Internet 网关具有以下特性：

- 您无法将安全组与仅出口 Internet 网关关联。可以为私有子网中的实例使用安全组以便控制进出这些实例的流量。
- 您可以使用网络 ACL 控制仅出口 Internet 网关路由的进出子网的流量。

在下图中，VPC 具有一个 IPv6 CIDR 块，此 VPC 中的子网也具有一个 IPv6 CIDR 块。子网 1 关联了一个自定义路由表，它将所有 Internet 绑定的 IPv6 流量 ($::/0$) 指向 VPC 中的仅出口 Internet 网关。



使用仅出口 Internet 网关

以下部分介绍如何为私有子网创建仅出口 Internet 网关，以及如何为该子网配置路由。

创建仅出口 Internet 网关

您可以使用 Amazon VPC 控制台为您的 VPC 创建一个仅出口 Internet 网关。

创建仅出口 Internet 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Egress Only Internet Gateways。
3. 选择 Create Egress Only Internet Gateway。
4. 选择要在其中创建仅出口 Internet 网关的 VPC。选择 Create。

查看仅出口 Internet 网关

您可以在 Amazon VPC 控制台中查看有关仅出口 Internet 网关的信息。

查看有关仅出口 Internet 网关的信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Egress Only Internet Gateways。
3. 选择仅出口 Internet 网关以在详细信息窗格中查看其信息。

创建自定义路由表

要将发往 VPC 外部的流量发送到仅出口 Internet 网关，您必须创建一个自定义路由表并添加将流量发送到该网关的路由，然后将其与您的子网关联。

创建自定义路由表并添加到仅出口 Internet 网关的路由

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，依次选择 Route Tables、Create Route Table。
3. 在 Create Route Table 对话框中，可以选择命名您的路由表，选择您的 VPC，然后选择 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，选择 Edit，在 Destination 框中指定 ::/0，从 Target 列表中选择仅出口 Internet 网关 ID，然后选择 Save。
6. 在 Subnet Associations 选项卡上，选择 Edit，然后选中子网的 Associate 复选框。选择 Save (保存)。

或者，您也可以向与您的子网关联的现有路由表添加路由。选择您现有的路由表，然后按照上述步骤 5 和 6 为仅出口 Internet 网关添加路由。

有关路由表的更多信息，请参阅[路由表 \(p. 181\)](#)。

删除仅出口 Internet 网关

若您不再需要某一仅出口 Internet 网关，则可将其删除。路由表中指向已删除的仅出口 Internet 网关的任何路由都将保持 blackhole 状态，直到您手动删除或更新路由。

删除仅出口 Internet 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Egress Only Internet Gateways，然后选择仅出口 Internet 网关。

3. 选择 Delete。
4. 在确认对话框中选择 Delete Egress Only Internet Gateway。

API 和 CLI 概述

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅[访问 Amazon VPC \(p. 7\)](#)。

创建仅出口 Internet 网关

- [create-egress-only-internet-gateway](#) (AWS CLI)
- [New-EC2EgressOnlyInternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

描述仅出口 Internet 网关

- [describe-egress-only-internet-gateways](#) (AWS CLI)
- [Get-EC2EgressOnlyInternetGatewayList](#) (适用于 Windows PowerShell 的 AWS 工具)

删除仅出口 Internet 网关

- [delete-egress-only-internet-gateway](#) (AWS CLI)
- [Remove-EC2EgressOnlyInternetGateway](#) (适用于 Windows PowerShell 的 AWS 工具)

NAT

您可以使用 NAT 设备允许私有子网中的实例连接到 Internet（例如，为了进行软件更新）或其他 AWS 服务，但阻止 Internet 发起与实例的连接。NAT 设备将来自私有子网中实例的流量转发到 Internet 或其他 AWS 服务，然后将响应发回给实例。当流量流向 Internet 时，源 IPv4 地址替换为 NAT 设备的地址，同样，当响应流量流向这些实例时，NAT 设备将地址转换为这些实例的私有 IPv4 地址。

NAT 设备不支持 IPv6 流量，而是改用仅出口 Internet 网关。有关更多信息，请参阅[仅出口 Internet 网关 \(p. 197\)](#)。

Note

我们在本文中使用 NAT 是为了遵循通行的 IT 做法，而 NAT 设备的实际作用包括地址转换和端口地址转换 (PAT) 两方面。

AWS 提供了两种 NAT 设备：一种是 NAT 网关，一种是 NAT 实例。我们建议使用 NAT 网关，因为相较于 NAT 实例，它可以提供更高的可用性和更大的带宽。此外，NAT 网关服务也是一种托管服务，并不需要您进行管理。NAT 实例从 NAT AMI 启动。您可以选择将 NAT 实例用于特别的用途。

- [NAT 网关 \(p. 200\)](#)
- [NAT 实例 \(p. 216\)](#)
- [NAT 实例与 NAT 网关的比较 \(p. 223\)](#)

NAT 网关

您可以使用网络地址转换 (NAT) 网关允许私有子网中的实例连接到 Internet 或其他 AWS 服务，但阻止 Internet 发起与这些实例的连接。有关 NAT 的更多信息，请参阅[NAT \(p. 200\)](#)。

您在账户中创建和使用 NAT 网关会产生费用。NAT 网关小时使用费率和数据处理费率适用于此。Amazon EC2 数据传输费同样适用。有关更多信息，请参阅 [Amazon VPC 定价](#)。

NAT 网关不支持 IPv6 流量，而是改用仅出口 Internet 网关。有关更多信息，请参阅 [仅出口 Internet 网关 \(p. 197\)](#)。

目录

- [NAT 网关基本知识 \(p. 201\)](#)
- [使用 NAT 网关 \(p. 203\)](#)
- [控制 NAT 网关的使用 \(p. 206\)](#)
- [标记 NAT 网关 \(p. 206\)](#)
- [API 和 CLI 概述 \(p. 206\)](#)
- [使用 Amazon CloudWatch 监控 NAT 网关 \(p. 207\)](#)
- [NAT 网关问题排查 \(p. 211\)](#)

NAT 网关基本知识

要创建 NAT 网关，您必须指定 NAT 网关应处于哪个公有子网中。有关公有子网和私有子网的更多信息，请参阅 [子网路由 \(p. 82\)](#)。还必须在创建 NAT 网关时指定与该网关关联的 [弹性 IP 地址 \(p. 232\)](#)。一旦将弹性 IP 地址与 NAT 网关关联，便无法更改它。创建 NAT 网关之后，必须更新与您的一个或多个私有子网关联的路由表，以将 Internet 绑定流量指向该 NAT 网关。这使您的私有子网中的实例可以与 Internet 通信。

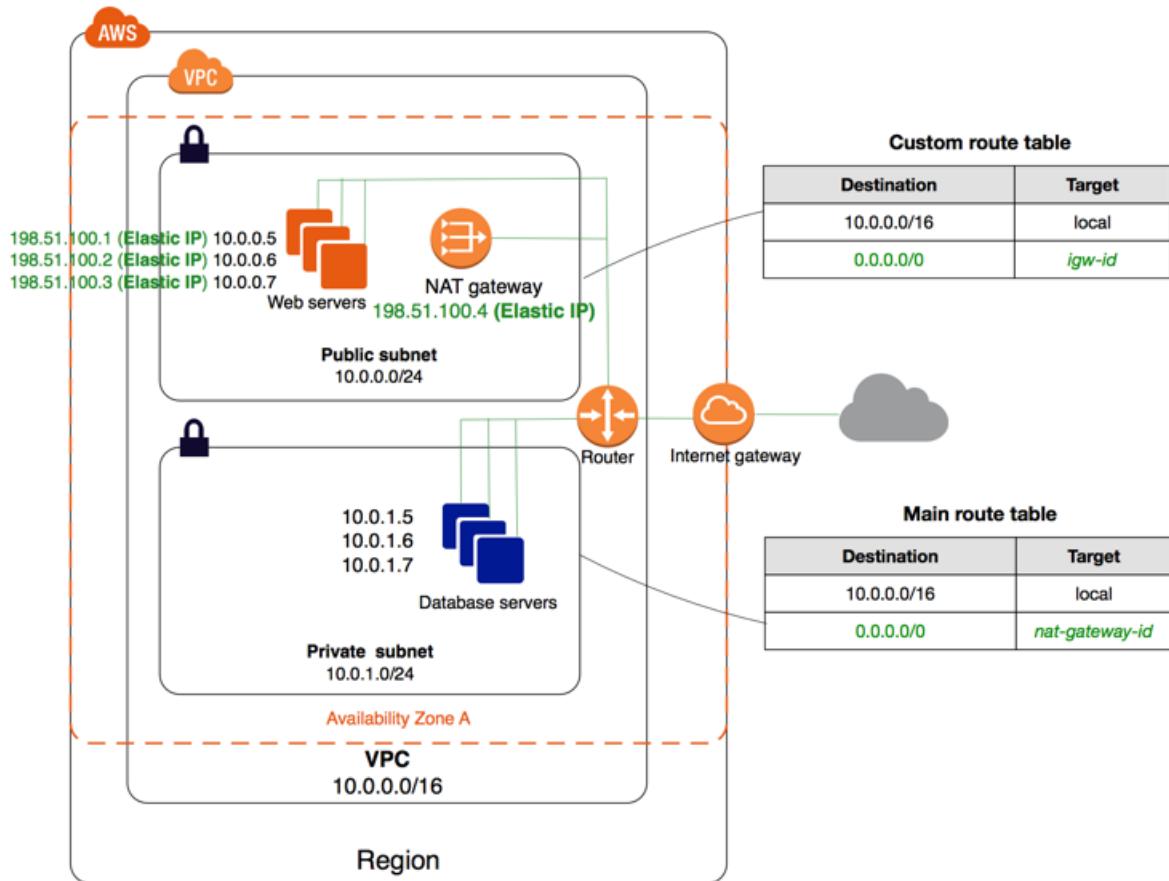
每个 NAT 网关都在特定可用区中创建，并在该可用区进行冗余实施。您可以在一个可用区中创建的 NAT 网关存在数量限制。有关更多信息，请参阅 [Amazon VPC 限制 \(p. 276\)](#)。

Note

如果您在多个可用区中拥有资源，并且它们共享一个 NAT 网关，则在该 NAT 网关的可用区不可用时，其他可用区中的资源将无法访问 Internet。要创建不依赖于可用区的架构，请在每个可用区中都创建一个 NAT 网关，并配置路由以确保这些资源使用自身可用区中的 NAT 网关。

您可以删除不再需要的 NAT 网关。删除 NAT 网关会解除其弹性 IP 地址关联，但不会从您的账户释放该地址。

下图演示了一个包含 NAT 网关的 VPC 架构。主路由表将 Internet 流量从私有子网中的实例发送到 NAT 网关。NAT 网关通过使用自身的弹性 IP 地址作为源 IP 地址，将流量发送到 Internet 网关。



NAT 网关规则和限制

NAT 网关具有以下特征和限制：

- NAT 网关支持 5 Gbps 带宽并会自动扩展到 45 Gbps。如果您需要更大的带宽，可以通过将资源拆分到多个子网中并在每个子网中都创建 NAT 网关来分配工作负载。
- 每个 NAT 网关只能关联一个弹性 IP 地址。创建弹性 IP 地址后，无法解除该地址与 NAT 网关的关联。如果您需要为 NAT 网关使用不同的弹性 IP 地址，则必须创建具有所需地址的新 NAT 网关，更新路由表，然后删除现有 NAT 网关（如果不再需要）。
- NAT 网关支持以下协议：TCP、UDP 和 ICMP。
- 不能为 NAT 网关关联安全组。可以为私有子网中的实例使用安全组以便控制进出这些实例的流量。
- 您可以使用网络 ACL 控制进出 NAT 网关所在子网的流量。网络 ACL 适用于 NAT 网关的流量。NAT 网关使用端口 1024–65535。有关更多信息，请参阅 [网络 ACL \(p. 126\)](#)。
- NAT 网关在创建时会收到一个网络接口，该网络接口从您的子网的 IP 地址范围自动分配有一个私有 IP 地址。可以在 Amazon EC2 控制台中查看 NAT 网关的网络接口。有关更多信息，请参阅 [查看有关网络接口的详细信息](#)。此网络接口的属性不可修改。
- 不能通过与 VPC 关联的 ClassicLink 连接来访问 NAT 网关。
- 对于每个唯一目的地，NAT 网关最多可以支持 55000 个并发连接。如果您每秒创建了大约 900 个与单个目的地的连接（大约每分钟 55,000 个连接），该限制也适用。如果目的地 IP 地址、目的地端口或协议（TCP/UDP/ICMP）发生更改，则可以再创建 55,000 个连接。若超过 55000 个连接，因接口分配错误导致连接错误的机会将提升。您可以通过查看您的 NAT 网关 ErrorPortAllocation CloudWatch 指标来监视这些错误。有关更多信息，请参阅 [使用 Amazon CloudWatch 监控 NAT 网关 \(p. 207\)](#)。

从 NAT 实例迁移

如果您已在使用 NAT 实例，可以将它替换为 NAT 网关。为此，可以在您的 NAT 实例所在的同一子网中创建一个 NAT 网关，然后将路由表中指向该 NAT 实例的现有路由替换为指向该 NAT 网关的路由。若要 NAT 网关使用 NAT 实例当前所用的弹性 IP 地址，您必须先解除该弹性 IP 地址与 NAT 实例的关联，并在创建 NAT 网关时将该地址与该网关关联。

Note

如果您将路由从 NAT 实例更改为 NAT 网关，或者，如果解除弹性 IP 地址与 NAT 实例的关联，则所有当前连接都会中断，必须重新建立。请确保您没有任何关键任务（或任何通过 NAT 实例操作的其他任务）正在运行。

将 NAT 网关用于 VPC 终端节点、AWS Site-to-Site VPN、AWS Direct Connect 或 VPC 对等连接

NAT 网关无法通过 VPC 终端节点、AWS Site-to-Site VPN 连接、AWS Direct Connect 或 VPC 对等连接发送流量。如果您在私有子网中的实例必须通过 VPC 终端节点、Site-to-Site VPN 连接或 AWS Direct Connect 访问资源，则使用私有子网的路由表将流量直接路由到这些设备。

例如，如果私有子网的路由表包含以下路由：Internet 绑定流量 (0.0.0.0/0) 路由到一个 NAT 网关，Amazon S3 流量 (pl-xxxxxxxxx；Amazon S3 的特定 IP 地址范围) 路由到一个 VPC 端点，而 10.25.0.0/16 流量路由到一个 VPC 对等连接。pl-xxxxxxxxx 和 10.25.0.0/16 IP 地址范围比 0.0.0.0/0 更加具体；当实例将流量发送到 Amazon S3 或对等 VPC 时，流量会发送到 VPC 端点或 VPC 对等连接。当实例将流量发送到 Internet（非 Amazon S3 IP 地址）时，流量会发送到 NAT 网关。

无法通过 VPC 对等连接、Site-to-Site VPN 连接或 AWS Direct Connect 将流量路由到 NAT 网关。这些连接另一端的资源不能使用 NAT 网关。

将流量发送到同一区域中的 Amazon S3 或 DynamoDB 时的最佳实践

为了避免在访问位于同一区域的 Amazon S3 和 DynamoDB 时产生 NAT 网关数据处理费用，请设置一个网关终端节点，并通过该网关终端节点而不是 NAT 网关路由流量。使用网关终端节点不会发生任何费用。有关更多信息，请参阅[网关 VPC 终端节点 \(p. 249\)](#)。

使用 NAT 网关

您可以使用 Amazon VPC 控制台创建、查看和删除 NAT 网关。也可以使用 Amazon VPC 向导创建具有公有子网、私有子网和 NAT 网关的 VPC。有关更多信息，请参阅[场景 2：带有公有子网和私有子网 \(NAT\) 的 VPC \(p. 29\)](#)。

任务

- [创建 NAT 网关 \(p. 203\)](#)
- [更新路由表 \(p. 204\)](#)
- [删除 NAT 网关 \(p. 204\)](#)
- [测试 NAT 网关 \(p. 204\)](#)

创建 NAT 网关

要创建 NAT 网关，必须指定子网和弹性 IP 地址。确保弹性 IP 地址当前未与实例或网络接口关联。若要从 NAT 实例迁移到 NAT 网关，并且希望重复使用 NAT 实例的弹性 IP 地址，则必须先解除该地址与 NAT 实例的关联。

创建 NAT 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格中，依次选择 NAT Gateways、Create NAT Gateway。
3. 指定要在其中创建 NAT 网关的子网，并选择要与该 NAT 网关关联的弹性 IP 地址的分配 ID。完成后，选择 Create a NAT Gateway。
4. NAT 网关会显示在控制台中。片刻之后，其状态会更改为 Available，此后它即准备好供您使用。

如果 NAT 网关变为 Failed 状态，则表示在创建过程中发生了错误。有关更多信息，请参阅 [NAT 网关变为 Failed 状态 \(p. 211\)](#)。

更新路由表

创建 NAT 网关之后，必须更新私有子网的路由表以将 Internet 流量指向该 NAT 网关。我们使用与流量匹配的最明确路由以判断数据流的路由方式（最长前缀匹配）。有关更多信息，请参阅 [路由优先级 \(p. 184\)](#)。

为 NAT 网关创建路由

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables。
3. 选择与私有子网关联的路由表，然后依次选择 Routes、Edit。
4. 选择 Add another route。对于 Destination，键入 0.0.0.0/0。对于 Target，选择 NAT 网关的 ID。

Note

若在从 NAT 实例进行迁移，则可以将指向该 NAT 实例的当前路由替换为指向 NAT 网关的路由。

5. 选择 Save (保存)。

为确保 NAT 网关可以访问 Internet，与 NAT 网关所在子网关联的路由表必须包含使 Internet 流量指向 Internet 网关的路由。有关更多信息，请参阅 [创建自定义路由表 \(p. 195\)](#)。如果删除 NAT 网关，则 NAT 网关路由会保留为 blackhole 状态，直到您删除或更新这些路由。有关更多信息，请参阅 [在路由表中添加和删除路由 \(p. 189\)](#)。

删除 NAT 网关

可以使用 Amazon VPC 控制台删除 NAT 网关。删除了 NAT 网关之后，其条目会在短时间内（通常为一小时）在 Amazon VPC 控制台中保持可见，在此之后自动删除。您无法自己删除此条目。

删除 NAT 网关

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 NAT Gateways。
3. 选择相应的 NAT 网关，然后依次选择 Actions (操作) 和 Delete NAT Gateway (删除 NAT 网关)。
4. 在确认对话框中，选择 Delete NAT Gateway。

测试 NAT 网关

创建 NAT 网关并更新路由表之后，可以从私有子网中的实例对 Internet 执行 ping 操作以测试它是否可以连接到 Internet。有关如何执行此操作的示例，请参阅 [测试 Internet 连接 \(p. 205\)](#)。

如果能够连接到 Internet，还可以执行以下测试以确定 Internet 流量是否在通过 NAT 网关进行路由：

- 您可以从私有子网中的实例跟踪流量的路由情况。为此，请从私有子网中的 Linux 实例运行 traceroute 命令。在输出中，应在一个跃点（通常是第一个跃点）中看到 NAT 网关的私有 IP 地址。

- 从私有子网中的实例连接第三方网站或工具时，查看该网站或工具显示的源 IP 地址。源 IP 地址应是您的 NAT 网关的弹性 IP 地址。可以在 Amazon VPC 控制台中的 NAT Gateways 页面上查看 NAT 网关的信息，以获得其弹性 IP 地址和私有 IP 地址。

如果上述测试失败，请参阅[NAT 网关问题排查 \(p. 211\)](#)。

测试 Internet 连接

以下示例演示如何测试私有子网中的实例是否可以连接到 Internet。

- 在公有子网中启动实例（您使用此实例作为堡垒主机）。有关更多信息，请参阅[在您的子网中启动一项实例 \(p. 86\)](#)。在启动向导中，确保选择一个 Amazon Linux AMI，并为实例分配公有 IP 地址。确保安全组规则允许来自本地网络的 IP 地址范围的入站 SSH 流量，以及发送到私有子网的 IP 地址范围的出站 SSH 流量（您也可以同时对入站和出站 SSH 流量使用 0.0.0.0/0 进行测试）。
- 在您的私有子网中启动实例。在启动向导中，确保选择一个 Amazon Linux AMI。请勿向实例分配公有 IP 地址。应确保安全组规则允许来自在公有子网中启动的实例的私有 IP 地址的入站 SSH 流量以及所有出站 ICMP 流量。必须选择用于在公有子网中启动实例的相同密钥对。
- 在本地计算机上配置 SSH 代理转发，并连接到公有子网中的堡垒主机。有关更多信息，请参阅[为 Linux 或 macOS 配置 SSH 代理转发 \(p. 205\)](#)或[针对 Windows \(PuTTY\) 配置 SSH 代理转发 \(p. 205\)](#)。
- 在堡垒主机中，连接到私有子网中的实例，然后从私有子网中的实例测试 Internet 连接。有关更多信息，请参阅[测试 Internet 连接 \(p. 205\)](#)。

为 Linux 或 macOS 配置 SSH 代理转发

- 在您的本地计算机上，将私有密钥添加到身份验证代理。

对于 Linux，请使用以下命令：

```
ssh-add -c mykeypair.pem
```

对于 macOS，请使用以下命令：

```
ssh-add -K mykeypair.pem
```

- 通过使用 -A 选项启用 SSH 代理转发来连接到公有子网中的实例，并使用该实例的公有地址；例如：

```
ssh -A ec2-user@54.0.0.123
```

针对 Windows (PuTTY) 配置 SSH 代理转发

- 如果尚未安装 Pageant，请从[PuTTY 下载页面](#)下载并安装 Pageant。
- 将您的私有密钥转换为 .ppk 格式。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[使用 PuTTYgen 转换您的私有密钥](#)。
- 启动 Pageant，右键单击任务栏上的 Pageant 图标（可能已隐藏），并选择 Add Key。选择您创建的 .ppk 文件，键入密码（如果需要），然后选择 Open。
- 启动 PuTTY 会话，并使用公有 IP 地址连接到公有子网中的实例。有关更多信息，请参阅[启动 PuTTY 会话](#)。在 Auth 类别中，确保选中了 Allow agent forwarding 选项，并将 Private key file for authentication 框留空。

测试 Internet 连接

- 从公有子网中的实例，使用私有 IP 地址连接到私有子网中的实例，例如：

```
ssh ec2-user@10.0.1.123
```

- 从私有实例，通过对启用了 ICMP 的网站运行 ping 命令来测试是否可以连接到 Internet，例如：

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms  
...
```

按键盘上的 Ctrl+C 以取消 ping 命令。如果 ping 命令失败，请参阅 [实例无法访问互联网 \(p. 213\)](#)。

- (可选) 如果您不再需要实例，请将其终止。想要了解更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[终止您的实例](#)。

控制 NAT 网关的使用

默认情况下，IAM 用户无权使用 NAT 网关。您可以创建一个 IAM 用户策略，以向用户授予创建、描述和删除 NAT 网关的权限。我们目前对所有 `ec2:*NatGateway*` API 操作都不支持资源级权限。有关用于 Amazon VPC 的 IAM 策略的更多信息，请参阅 [控制访问 Amazon VPC 资源 \(p. 151\)](#)。

标记 NAT 网关

您可以对 NAT 网关进行标记，以帮助您识别它或根据组织的需要对其进行分类。有关使用标签的信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[标记 Amazon EC2 资源](#)。

NAT 网关支持成本分配标签，因此您还可以使用标签来组织您的 AWS 账单和反映您自己的成本结构。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南中的[使用成本分配标签](#)。有关设置包含标签的成本分配报告的更多信息，请参阅 AWS Account Billing 简介中的[月度成本分配报告](#)。

API 和 CLI 概述

您可以使用命令行或 API 执行此页面上介绍的任务。有关命令行界面的更多信息以及可用 API 操作的列表，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

创建 NAT 网关

- [create-nat-gateway](#) (AWS CLI)
- [New-EC2NatGateway](#) (适用于 Windows PowerShell 的 AWS 工具)
- [CreateNatGateway](#) (Amazon EC2 查询 API)

标记 NAT 网关

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (适用于 Windows PowerShell 的 AWS 工具)
- [CreateTags](#) (Amazon EC2 查询 API)

描述 NAT 网关

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeNatGateways](#) (Amazon EC2 查询 API)

删除 NAT 网关

- [delete-nat-gateway \(AWS CLI\)](#)
- [Remove-EC2NatGateway \(适用于 Windows PowerShell 的 AWS 工具\)](#)
- [DeleteNatGateway \(Amazon EC2 查询 API \)](#)

使用 Amazon CloudWatch 监控 NAT 网关

您可以使用 CloudWatch 监控 NAT 网关，该工具可从 NAT 网关中收集信息并创建可读的、近乎实时的指标。您可以使用该信息监控 NAT 网关并进行问题排查。NAT 网关指标数据以每分钟一次的频率提供，统计数据的记录期限为 15 个月。

有关 Amazon CloudWatch 的更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。有关定价的更多信息，请参阅 [Amazon CloudWatch 定价](#)。

NAT 网关指标与维度

以下指标可用于 NAT 网关。

指标	描述
ActiveConnectionCount	通过 NAT 网关激活的并发 TCP 连接的总数。 零值表示未通过 NAT 网关激活任何连接。 单位：计数 Statistics：最有用的统计工具是 Max。
BytesInFromDestination	NAT 网关从目标接收的字节的数量。 如果 BytesOutToSource 的值小于 BytesInFromDestination 的值，则表示 NAT 网关处理期间可能存在数据丢失，或存在被 NAT 网关主动阻止的流量。 单位：字节 Statistics：最有用的统计工具是 Sum。
BytesInFromSource	NAT 网关从 VPC 中的客户端接收的字节的数量。 如果 BytesOutToDestination 的值小于 BytesInFromSource 的值，则 NAT 网关处理期间可能有数据丢失。 单位：字节 Statistics：最有用的统计工具是 Sum。
BytesOutToDestination	通过 NAT 网关发送到目标的字节的数量。 大于零的值指示有流量从 NAT 网关后面的客户端流向 Internet。如果 BytesOutToDestination 的值小于 BytesInFromSource 的值，则 NAT 网关处理期间可能有数据丢失。 单位：字节

指标	描述
	Statistics : 最有用的统计工具是 Sum。
BytesOutToSource	<p>通过 NAT 网关发送到 VPC 中客户端的字节的数量。</p> <p>大于零的值指示有流量从 Internet 流向 NAT 网关后面的客户端。如果 BytesOutToSource 的值小于 BytesInFromDestination 的值，则表示 NAT 网关处理期间可能存在数据丢失，或存在被 NAT 网关主动阻止的流量。</p> <p>单位：字节</p> <p>Statistics : 最有用的统计工具是 Sum。</p>
ConnectionAttemptCount	<p>通过 NAT 网关尝试的连接次数。</p> <p>如果 ConnectionEstablishedCount 的值小于 ConnectionAttemptCount 的值，则表示 NAT 网关后面的客户端已尝试为无响应的连接建立新连接。</p> <p>单位：计数</p> <p>Statistics : 最有用的统计工具是 Sum。</p>
ConnectionEstablishedCount	<p>通过 NAT 网关建立的连接的数量。</p> <p>如果 ConnectionEstablishedCount 的值小于 ConnectionAttemptCount 的值，则表示 NAT 网关后面的客户端已尝试为无响应的连接建立新连接。</p> <p>单位：计数</p> <p>Statistics : 最有用的统计工具是 Sum。</p>
ErrorPortAllocation	<p>NAT 网关无法分配源端口的次数。</p> <p>大于零的值表示通过 NAT 网关打开的并发连接太多。</p> <p>单位：计数</p> <p>Statistics : 最有用的统计工具是 Sum。</p>
IdleTimeoutCount	<p>从活动状态转换为空闲状态的连接的数量。如果活动连接未正常关闭并且前 350 秒内无活动，活动连接将转换为空闲状态。</p> <p>大于零的值指示存在已变为空闲状态的连接。如果 IdleTimeoutCount 的值增加，则可能指示 NAT 网关后面的客户端正在重复使用过期连接。</p> <p>单位：计数</p> <p>Statistics : 最有用的统计工具是 Sum。</p>

指标	描述
<code>PacketsDropCount</code>	<p>NAT 网关丢弃的数据包的数量。</p> <p>大于零的值可能指示 NAT 网关持续存在暂时性问题。如果此值较高，请参阅 AWS 服务运行状况控制面板。</p> <p>单位：计数</p> <p>Statistics：最有用的统计工具是 Sum。</p>
<code>PacketsInFromDestination</code>	<p>NAT 网关从目标接收的数据包的数量。</p> <p>如果 <code>PacketsOutToSource</code> 的值小于 <code>PacketsInFromDestination</code> 的值，则表示 NAT 网关处理期间可能存在数据丢失，或存在被 NAT 网关主动阻止的流量。</p> <p>单位：计数</p> <p>Statistics：最有用的统计工具是 Sum。</p>
<code>PacketsInFromSource</code>	<p>NAT 网关从 VPC 中的客户端接收的数据包的数量。</p> <p>如果 <code>PacketsOutToDestination</code> 的值小于 <code>PacketsInFromSource</code> 的值，则 NAT 网关处理期间可能有数据丢失。</p> <p>单位：计数</p> <p>Statistics：最有用的统计工具是 Sum。</p>
<code>PacketsOutToDestination</code>	<p>通过 NAT 网关发送到目标的数据包的数量。</p> <p>大于零的值指示有流量从 NAT 网关后面的客户端流向 Internet。如果 <code>PacketsOutToDestination</code> 的值小于 <code>PacketsInFromSource</code> 的值，则 NAT 网关处理期间可能有数据丢失。</p> <p>单位：计数</p> <p>Statistics：最有用的统计工具是 Sum。</p>
<code>PacketsOutToSource</code>	<p>通过 NAT 网关发送到 VPC 中客户端的数据包的数量。</p> <p>大于零的值指示有流量从 Internet 流向 NAT 网关后面的客户端。如果 <code>PacketsOutToSource</code> 的值小于 <code>PacketsInFromDestination</code> 的值，则表示 NAT 网关处理期间可能存在数据丢失，或存在被 NAT 网关主动阻止的流量。</p> <p>单位：计数</p> <p>Statistics：最有用的统计工具是 Sum。</p>

要筛选指标数据，请使用以下维度。

维度	描述
NatGatewayId	按 NAT 网关 ID 筛选指标数据。

查看 NAT 网关 CloudWatch 指标

NAT 网关指标按 1 分钟的时间间隔发送到 CloudWatch。您可以按照以下方法查看 NAT 网关的各项指标。

使用 CloudWatch 控制台查看指标

指标的分组首先依据服务命名空间，然后依据每个命名空间内的各种维度组合。

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，选择 Metrics。
3. 在 All metrics 下，选择 NAT gateway 指标命名空间。
4. 要查看指标，请选择指标维度。

使用 AWS CLI 查看指标

在命令提示窗口中，使用以下命令可列出可用于 NAT 网关服务的指标：

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

创建 CloudWatch 警报以监控 NAT 网关

您可以创建 CloudWatch 警报，用于在警报改变状态时发送 Amazon SNS 消息。警报会监控您指定的时间段内的某个指标。它将根据指标值在多个时间段内相对于给定阈值的情况向 Amazon SNS 主题发送通知。

例如，您可以创建警报来监控进入或离开 NAT 网关的流量。以下警报监控从您的 VPC 中的客户端通过 NAT 网关传到 Internet 的出站流量。如果在 15 分钟的时间段内字节数达到 500 万阈值，它将发送通知。

创建通过 NAT 网关的出站流量的警报

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格中，依次选择 Alarms 和 Create Alarm。
3. 选择 NAT gateway。
4. 选择所需的 NAT 网关和 BytesOutToDestination 指标，然后选择 Next。
5. 按如下所示配置警报，然后在完成后选择 Create Alarm：
 - 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 \geq 并输入 5000000。输入 1 作为连续周期数。
 - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
 - 在 Alarm Preview 下，选择 15 分钟的周期并指定 Sum 的统计数据。

您可以创建一个警报来监控 ErrorPortAllocation 指标并且在该值在三个连续 5 分钟的时间段内大于零(0)时发送通知。

创建警报以监控端口分配错误

1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。

2. 在导航窗格中，依次选择 Alarms 和 Create Alarm。
3. 选择 NAT Gateway。
4. 选择所需的 NAT 网关和 ErrorPortAllocation 指标，然后选择 Next。
5. 按如下所示配置警报，然后在完成后选择 Create Alarm：
 - 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 > 并输入 0。输入 3 作为连续周期数。
 - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
 - 在 Alarm Preview 下，选择 5 分钟的周期并指定 Maximum 的统计数据。

有关创建警报的更多示例，请参阅 Amazon CloudWatch 用户指南 中的[创建 Amazon CloudWatch 警报](#)。

NAT 网关问题排查

以下主题可帮助您排查在创建或使用 NAT 网关时可能遇到的常见问题。

问题

- [NAT 网关变为 Failed 状态 \(p. 211\)](#)
- [弹性 IP 地址和 NAT 网关限制 \(p. 212\)](#)
- [不支持可用区 \(p. 213\)](#)
- [NAT 网关不再可见 \(p. 213\)](#)
- [NAT 网关不响应 Ping 命令 \(p. 213\)](#)
- [实例无法访问互联网 \(p. 213\)](#)
- [到目标的 TCP 连接失败 \(p. 214\)](#)
- [追踪路由输出未显示 NAT 网关私有 IP 地址 \(p. 215\)](#)
- [Internet 连接在 350 秒后中断 \(p. 215\)](#)
- [无法建立 IPsec 连接 \(p. 216\)](#)
- [无法发起更多连接 \(p. 216\)](#)

NAT 网关变为 Failed 状态

问题

您创建了一个 NAT 网关，但它的状态为 Failed。

原因

创建 NAT 网关时出错。返回的错误消息提供了出现错误的原因。

解决方案

要查看错误消息，请前往 Amazon VPC 控制台，然后选择 NAT Gateways。选择您的 NAT 网关，然后在详细信息窗格的 Status 框中查看错误消息。

下表列出了 Amazon VPC 控制台中指示的可能的失败原因。执行所示任何纠正步骤之后，您可以再次尝试创建 NAT 网关。

Note

失败的 NAT 网关会在短时间（通常是大约一小时）之后自动删除。

显示的错误	原因	解决方案
子网没有足够的空闲地址来创建此 NAT 网关	指定的子网没有任何空闲的私有 IP 地址。NAT 网关需要从子网范围分配了私有 IP 地址的网络接口。	检查子网中可用的 IP 地址数，方法是在 Amazon VPC 控制台中前往 Subnets 页面。您可以在子网的详细信息窗格中查看 Available IP。要在子网中创建空闲的 IP 地址，可以删除未使用的网络接口，或终止不需要的实例。
网络 <code>vpc-xxxxxxxx</code> 未连接任何互联网网关	必须在具有 Internet 网关的 VPC 中创建 NAT 网关。	创建 Internet 网关，并将其连接到您的 VPC。有关更多信息，请参阅 创建并附加 Internet 网关 (p. 195) 。
弹性 IP 地址 <code>eipalloc-xxxxxxxx</code> 无法与此 NAT 网关相关联	指定的弹性 IP 地址不存在或无法找到。	检查弹性 IP 地址的分配 ID 以确保正确输入了它。确保指定的弹性 IP 地址与所创建的 NAT 网关在同一 AWS 区域中。
弹性 IP 地址 <code>eipalloc-xxxxxxxx</code> 已关联	指定的弹性 IP 地址已与其他资源关联，无法与 NAT 网关相关联。	检查哪个资源与弹性 IP 地址相关联。前往 Amazon VPC 控制台中的 Elastic IPs 页面，查看为实例 ID 或网络接口 ID 指定的值。如果该资源不需要该弹性 IP 地址，则可以解除两者的关联。或者，也可以向您的账户分配新的弹性 IP 地址。有关更多信息，请参阅 使用弹性 IP 地址 (p. 233) 。
此 NAT 网关在内部创建并使用的网络接口 <code>eni-xxxxxxxx</code> 处于无效状态。请重试。	为 NAT 网关创建或使用网络接口时出现问题。	您无法解决此错误。请再次尝试创建 NAT 网关。

弹性 IP 地址和 NAT 网关限制

问题

您在尝试分配弹性 IP 地址时收到以下错误：

The maximum number of addresses has been reached.

您在尝试创建 NAT 网关时收到以下错误：

Performing this operation would exceed the limit of 5 NAT gateways

原因

有 2 个可能的原因：

- 您已达到该区域账户的弹性 IP 地址数量的上限。
- 您已达到该可用区域账户的 NAT 网关数量的上限。

解决方案

如果您的弹性 IP 地址数已达到上限，则可以取消弹性 IP 地址与其他资源的关联，也可以使用 [Amazon VPC 限制表单](#) 请求提高上限。

如果您已达到 NAT 网关限制，则可以执行以下操作之一：

- 使用 [Amazon VPC Limits form](#) 请求提高限制。NAT 网关限制针对每个可用区执行。
- 检查 NAT 网关的状态。Pending、Available 或 Deleting 状态的网关就占用限额。如果您最近删除了 NAT 网关，请等待几分钟，以便状态从 Deleting 变为 Deleted。然后尝试新建一个 NAT 网关。
- 如果您在特定可用区中不需要 NAT 网关，请尝试在未达到限制的可用区中创建 NAT 网关。

有关更多信息，请参阅 [Amazon VPC 限制 \(p. 276\)](#)。

不支持可用区

问题

您在尝试创建 NAT 网关时收到以下错误：NotAvailableInZone

原因

您可能会尝试在受约束的可用区（即我们的扩展能力受约束的区域）中创建 NAT 网关。

解决方案

我们无法在这些可用区中支持 NAT 网关。您可以在其他可用区中创建 NAT 网关并将它用于受约束区域中的私有子网。您还可以将资源移动到不受约束的可用区，以便您的资源和 NAT 网关处于同一区中。

NAT 网关不再可见

问题

您创建了一个 NAT 网关，但它在 Amazon VPC 控制台中不可见。

原因

创建 NAT 网关时可能发生错误，该网关已失败。状态为 Failed 的 NAT 网关在短时间内（通常为一小时）在 Amazon VPC 控制台中可见，一个小时之后会被自动删除。

解决方案

查看 [NAT 网关变为 Failed 状态 \(p. 211\)](#) 中的信息，然后尝试创建新 NAT 网关。

NAT 网关不响应 Ping 命令

问题

如果您尝试从互联网（例如从家庭计算机）或从 VPC 中的任何实例对 NAT 网关的弹性 IP 地址或私有 IP 地址执行 ping 操作，则不会收到响应。

原因

NAT 网关仅从私有子网中的实例向 Internet 传输流量。

解决方案

要测试 NAT 网关是否正常运行，请参阅 [测试 NAT 网关 \(p. 204\)](#)。

实例无法访问互联网

问题

您创建了一个 NAT 网关并按照步骤进行了测试，但 ping 命令失败，或者您私有子网中的实例无法访问互联网。

原因

出现此问题的原因可能是以下原因之一：

- NAT 网关尚未准备好提供流量。
- 您的路由表未得到正确配置。
- 您的安全组或网络 ACL 阻止入站或出站流量。
- 您使用的是不受支持的协议。

解决方案

检查以下信息：

- 检查 NAT 网关是否处于 Available 状态。在 Amazon VPC 控制台中，转到 NAT Gateways 页面，然后在详细信息窗格中查看状态信息。如果 NAT 网关处于失败状态，则表示在创建它时可能发生了错误。有关更多信息，请参阅 [NAT 网关变为 Failed 状态 \(p. 211\)](#)。
- 检查您是否正确配置了路由表：
 - NAT 网关所处的公有子网必须具有将 Internet 流量路由到 Internet 网关的路由表。有关更多信息，请参阅 [创建自定义路由表 \(p. 195\)](#)。
 - 实例所处的私有子网必须具有将 Internet 流量路由到 NAT 网关的路由表。有关更多信息，请参阅 [更新路由表 \(p. 204\)](#)。
 - 检查是否有其他路由表条目将全部或部分 Internet 流量路由到其他设备而不是 NAT 网关。
- 确保私有实例的安全组规则允许出站 Internet 流量。要使 ping 命令正常运行，这些规则还必须允许出站 ICMP 流量。

Note

NAT 网关本身允许所有出站流量以及响应出站请求时收到的流量（因此它是有状态的）。

- 确保与私有子网和公有子网关联的网络 ACL 没有阻止入站或出站 Internet 流量的规则。要使 ping 命令正常运行，这些规则还必须允许入站和出站 ICMP 流量。

Note

可以启用流日志以帮助诊断由于网络 ACL 或安全组规则而中断的连接。有关更多信息，请参阅 [VPC 流日志 \(p. 165\)](#)。

- 如果使用 ping 命令，请确保在对启用了 ICMP 的网站执行 ping 操作。如果未启用 ICMP，您不会收到应答数据包。要对此进行测试，请从您自己计算机上的命令行终端执行相同的 ping 命令。
- 检查实例是否能够对其他资源成功执行 ping 操作，例如私有子网中的其他实例（假设安全组规则允许这样做）。
- 确保您的连接仅使用 TCP、UDP 或 ICMP 协议。

到目标的 TCP 连接失败

问题

在通过 NAT 网关从私有子网中的实例连接到特定目标时，有些 TCP 连接会成功，但也有些连接会失败或超时。

原因

出现此问题的原因可能是以下原因之一：

- 目标终端节点正在使用分段 TCP 数据包进行响应。NAT 网关当前不支持 TCP 或 ICMP 的 IP 分段。有关更多信息，请参阅 [NAT 实例与 NAT 网关的比较 \(p. 223\)](#)。
- 远程服务器上启用了 `tcp_tw_recycle` 选项，当 NAT 设备后有多个连接时，启用该选项会导致问题。

Solutions

通过执行以下操作，验证您尝试连接的终端节点是否正在使用分段 TCP 数据包进行响应：

1. 使用具有公共 IP 地址的公有子网中的实例来触发足够大的响应，以产生来自特定终端节点的分段。
2. 使用 `tcpdump` 实用工具验证终端节点是否将发送分段数据包。

Important

您必须使用公有子网中的实例来执行这些检查。您不能使用原始连接失败的实例，或者 NAT 网关或 NAT 实例后面的私有子网中的实例。

Note

发送或接收大型 ICMP 数据包的诊断工具将报告数据包丢失。例如，命令 `ping -s 10000 example.com` 将不会在 NAT 网关后面工作。

3. 如果终端节点发送分段 TCP 数据包，则可使用 NAT 实例代替 NAT 网关。

如果您有权访问远程服务器，则可以通过执行以下操作来验证是否已启用 `tcp_tw_recycle` 选项：

1. 在服务器上运行以下命令：

```
cat /proc/sys/net/ipv4/tcp_tw_recycle
```

如果输出为 1，则表明已启用 `tcp_tw_recycle` 选项。

2. 如果已启用 `tcp_tw_recycle` 选项，建议将其禁用。如果您需要重用连接，则 `tcp_tw_reuse` 是一个较为安全的选项。

如果您无权访问远程服务器，则可以通过临时禁用私有子网中的实例上的 `tcp_timestamps` 选项来进行测试。然后重新连接到远程服务器。如果连接成功，则上次连接失败的原因很可能是在远程服务器上启用了 `tcp_tw_recycle` 选项。如果可能，请与远程服务器的所有者联系，以验证是否已启用此选项，如已启用，则请求将其禁用。

追踪路由输出未显示 NAT 网关私有 IP 地址

问题

您的实例可以访问 Internet，但是当您执行 `traceroute` 命令时，输出未显示 NAT 网关的私有 IP 地址。

原因

您的实例在使用其他网关（例如互联网网关）访问互联网。

解决方案

在实例所处的子网的路由表中，检查以下信息：

- 确保存在将 Internet 流量发送到 NAT 网关的路由。
- 确保没有其他特定路由将 Internet 流量发送到其他设备（如虚拟专用网关或 Internet 网关）。

Internet 连接在 350 秒后中断

问题

您的实例可以访问互联网，但连接在 350 秒后断开。

原因

如果使用 NAT 网关的连接空闲 350 秒或更长时间，则连接会超时。

解决方案

要防止连接中断，您可以通过该连接发起更多流量。或者，您也可以在实例上启用值小于 350 秒的 TCP keepalive。

无法建立 IPsec 连接

问题

您无法与目标建立 IPsec 连接。

原因

NAT 网关当前不支持 IPsec 协议。

解决方案

您可以使用 NAT 遍历 (NAT-T) 将 IPsec 流量封装在 UDP (NAT 网关的支持协议) 中。请确保您已测试您的 NAT-T 和 IPsec 配置，以验证您没有丢弃 IPsec 流量。

无法发起更多连接

问题

您有通过 NAT 网关与目标建立的现有连接，但无法建立更多连接。

原因

您可能已达到单个 NAT 网关的并发连接数限制。有关更多信息，请参阅 [NAT 网关规则和限制 \(p. 202\)](#)。如果私有子网中的实例创建了大量连接，则您可能会达到该限制。

解决方案

请执行下列操作之一：

- 对每个可用区创建一个 NAT 网关，并在这些区域间分布客户端。
- 在公有子网中创建更多 NAT 网关并将客户端拆分到多个私有子网中（各自具有指向不同 NAT 网关的路由）。
- 限制客户端可对目的地创建的连接数。
- 关闭空闲连接以释放容量。

NAT 实例

通过使用您 VPC 中公有子网内的网络地址转换 (NAT) 实例，可让私有子网中的实例发起到 Internet 或其他 AWS 服务的出站 IPv4 流量，但阻止这些实例接收由 Internet 上的用户发起的入站流量。

有关公有子网和私有子网的更多信息，请参阅 [子网路由 \(p. 82\)](#)。有关 NAT 的更多信息，请参阅 [NAT \(p. 200\)](#)。

NAT 不支持 IPv6 流量，而是改用仅出口 Internet 网关。有关更多信息，请参阅 [仅出口 Internet 网关 \(p. 197\)](#)。

Note

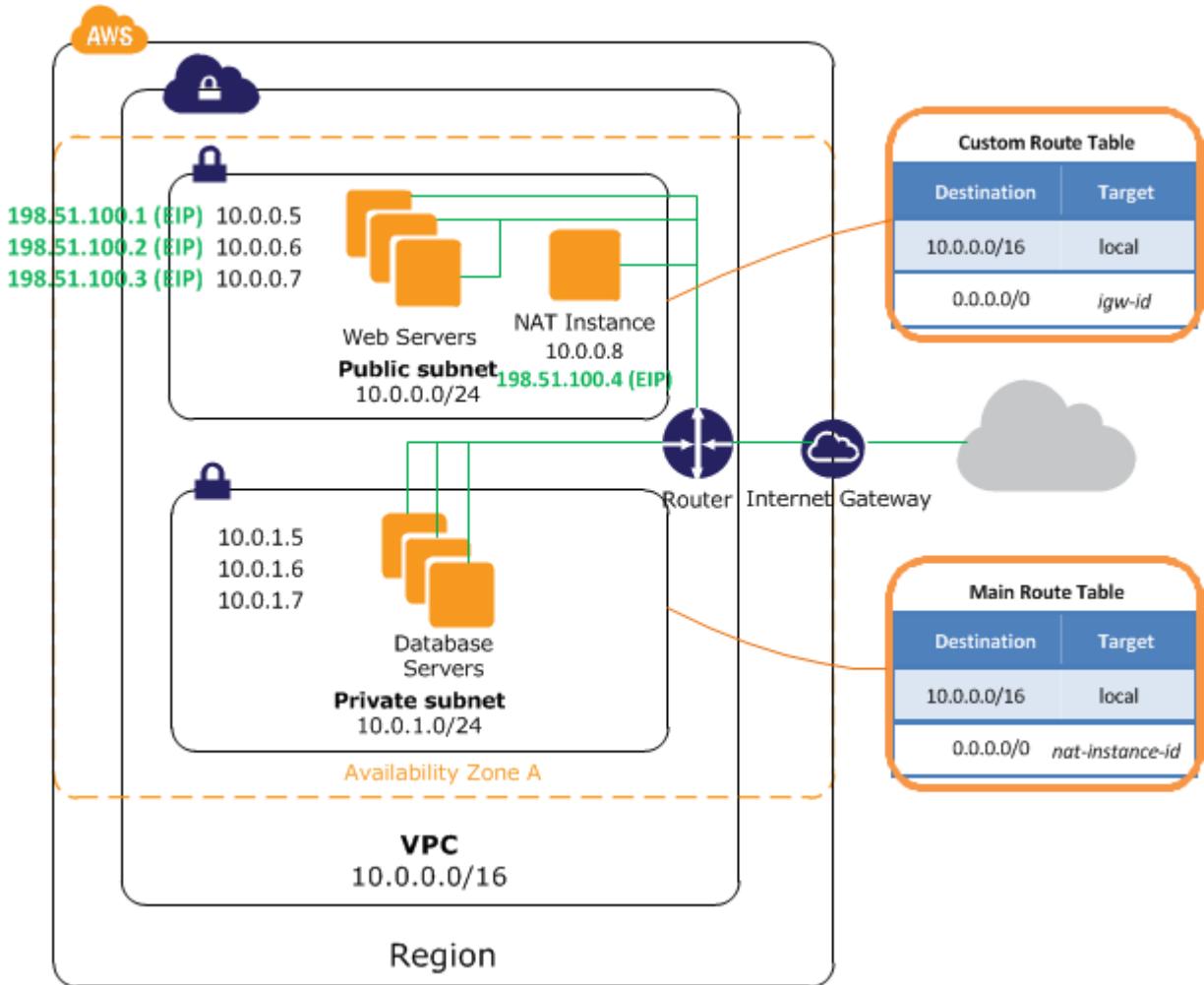
您也可以使用 NAT 网关，该网关是托管的 NAT 服务，可提供更高的可用性、更大的带宽，但所需的管理工作更少。对于常见使用案例，我们建议您使用 NAT 网关而不是 NAT 实例。有关更多信息，请参阅 [NAT 网关 \(p. 200\)](#) 和 [NAT 实例与 NAT 网关的比较 \(p. 223\)](#)。

内容

- NAT 实例基本信息 (p. 217)
- 设置 NAT 实例 (p. 218)
- 正在创建 NATSG 安全组 (p. 219)
- 正在禁用源/目标检查 (p. 220)
- 更新主路由表 (p. 221)
- 测试您的 NAT 实例配置 (p. 221)

NAT 实例基本信息

下图展示了 NAT 实例的基本信息。主路由表与私有子网关联，并将来自私有子网中实例的流量发送到公有子网中的 NAT 实例。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。



Amazon 提供 Amazon Linux AMI，并会将其配置作为 NAT 实例运行。这些 AMI 的名称包含字符串 amzn-ami-vpc-nat，因此可在 Amazon EC2 控制台中搜索它们。

当您从 NAT AMI 启动某个实例时，将对该实例进行以下配置：

- 在 `/etc/sysctl.d/10-nat-settings.conf` 中启用 IPv4 转发并禁用 ICMP 重定向

- 位于 `/usr/sbin/configure-pat.sh` 的脚本在启动时运行，并配置 iptables IP 伪装。

Note

我们建议您始终使用最新版本的 NAT AMI 来利用配置更新。

如果您在 VPC 上添加和删除辅助 IPv4 CIDR 块，请确保使用 AMI 版本 `amzn-ami-vpc-nat-hvm-2017.03.1.20170623-x86_64-ebs` 或更高版本。

您的 NAT 实例限制取决于所在区域的实例类型限制。有关更多信息，请参阅 [EC2 常见问题](#)。有关可用 NAT AMI 的列表，请参阅 [Amazon Linux AMI 矩阵](#)。

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，请参阅[场景 2：带有公有子网和私有子网 \(NAT\) 的 VPC \(p. 29\)](#)。向导可为您执行许多配置步骤，包括启动 NAT 实例和设置路由。不过，如果您愿意，您可以使用以下步骤手动创建和配置 VPC 和 NAT 实例。

1. 创建带有两个子网的 VPC。

Note

以下步骤用于手动创建和配置 VPC；而不是使用 VPC 向导创建 VPC。

- a. 创建 VPC (参见 [创建 VPC \(p. 83\)](#))
- b. 创建两个子网 (参见 [创建子网 \(p. 194\)](#))
- c. 将 Internet 网关附加到 VPC (请参阅[创建并附加 Internet 网关 \(p. 195\)](#))
- d. 创建一个用于将流向 VPC 外的流量发送到 Internet 网关的自定义路由表，然后将该路由表与一个子网关联，使其成为公有子网 (请参阅[创建自定义路由表 \(p. 195\)](#))
2. 创建 NATSG 安全组 (参见 [正在创建 NATSG 安全组 \(p. 219\)](#))。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 的名称包含字符串 `amzn-ami-vpc-nat`，因此可在 Amazon EC2 控制台中搜索它们。
 - a. 打开 Amazon EC2 控制台。
 - b. 在仪表板上，选择 Launch Instance 按钮，然后按如下所示完成向导：
 - i. 在 Choose an Amazon Machine Image (AMI) (选择一个 Amazon 系统映像 (AMI)) 页上，选择 Community AMIs (社区 AMI) 类别，然后搜索 `amzn-ami-vpc-nat`。在结果列表中，每个 AMI 的名称都包含版本，您可以选择最新 AMI，例如 `2013.09`。选择 Select。
 - ii. 在 Choose an Instance Type 页上，选择要启动的实例类型，然后选择 Next: Configure Instance Details。
 - iii. 在 Configure Instance Details (配置实例详细信息) 页上，从 Network (网络) 列表中选择您创建的 VPC，然后从 Subnet (子网) 列表中选择您的公有子网。
 - iv. (可选) 选中 Public IP (公有 IP) 复选框以要求您的 NAT 实例接收公有 IP 地址。如果决定现在不分配公有 IP 地址，则可分配弹性 IP 地址，并在启动您的实例后向其分配该地址。有关在启动时分配公有 IP 的更多信息，请参阅[在实例启动期间分配公有 IPv4 地址 \(p. 103\)](#)。选择 Next: Add Storage。
 - v. 可决定向您的实例添加存储，并可在下一页上添加标签。完成时选择 Next: Configure Security Group。
 - vi. 在 Configure Security Group (配置安全组) 页上，选择 Select an existing security group (选择一个现有的安全组) 选项，然后选择您创建的 NATSG 安全组。选择 Review and Launch。
 - vii. 检视您已经选择的设置。执行所需的任何更改，然后选择 Launch 以选择一个密钥对并启动您的实例。

4. (可选) 连接到 NAT 实例，根据需要进行修改，然后创建您自己的 AMI 并将其配置为作为 NAT 实例运行。您可以在下次您需要启动 NAT 实例时使用此 AMI。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[创建由 Amazon EBS 支持的 AMI](#)。
5. 禁用 NAT 实例的SrcDestCheck属性 (参见[正在禁用源/目标检查 \(p. 220\)](#))
6. 如果没有在启动期间向您的 NAT 实例分配公有 IP 地址（第 3 步），则需要将弹性 IP 地址与该实例关联。
 - a. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc>。
 - b. 在导航窗格中，选择 Elastic IPs，然后选择 Allocate new address。
 - c. 选择 Allocate。
 - d. 从列表中选择弹性 IP 地址，然后选择 Actions、Associate address。
 - e. 选择网络接口资源，然后选择 NAT 实例的网络接口。从 Private IP 列表中选择要与弹性 IP 地址关联的地址，然后选择 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 \(p. 221\)](#)。

使用命令行启动 NAT 实例

要在子网中启用 NAT 实例，请使用以下命令之一。有关更多信息，请参阅[访问 Amazon VPC \(p. 7\)](#)。

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

要获取配置为 NAT 实例运行的 AMI 的 ID，请使用命令描述映像，并使用筛选条件仅返回 Amazon 拥有以及名称包含 amzn-ami-vpc-nat 字符串的 AMI。以下示例使用 AWS CLI：

```
aws ec2 describe-images --filter Name="owner-alias",Values="amazon" --filter Name="name",Values="amzn-ami-vpc-nat*"
```

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

Inbound			
Source	Protocol	Port Range	Comments
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
您家庭网络的公共 IP 地址范围	TCP	22	允许从您的家庭网络到 NAT 实例的入站 SSH 访问 (通过 Internet 网关)

Outbound			
Destination	Protocol	Port Range	Comments
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 HTTPS 访问
-----------	-----	-----	---------------------------

创建 NATSG 安全组

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Security Groups，然后选择 Create Security Group。
3. 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，然后选择 Yes, Create。
4. 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。
5. 使用 Inbound Rules (入站规则) 选项卡添加入站流量规则，如下所示：
 - a. 选择 Edit。
 - b. 选择 Add another rule，然后从 Type 列表中选择 HTTP。在 Source (源) 字段中，指定私有子网的 IP 地址范围。
 - c. 选择 Add another rule，然后从 Type 列表中选择 HTTPS。在 Source (源) 字段中，指定私有子网的 IP 地址范围。
 - d. 选择 Add another rule，然后从 Type 列表中选择 SSH。在 Source (源) 字段中，指定网络的公有 IP 地址范围。
 - e. 选择 Save (保存)。
6. 使用 Outbound Rules (出站规则) 选项卡添加出站流量规则，如下所示：
 - a. 选择 Edit。
 - b. 选择 Add another rule，然后从 Type 列表中选择 HTTP。在 Destination (目标) 字段中，指定 0.0.0.0/0
 - c. 选择 Add another rule，然后从 Type 列表中选择 HTTPS。在 Destination (目标) 字段中，指定 0.0.0.0/0
 - d. 选择 Save (保存)。

有关更多信息，请参阅您的 VPC 的安全组 (p. 119)。

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。

您可以使用控制台或命令行，禁用正在运行或已停止运行的 NAT 实例 SrcDestCheck 属性。

使用控制台禁用源/目标检查

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 依次选择 NAT 实例、Actions (操作)、Networking (联网) 和 Change Source/Dest.Check。
4. 对于 NAT 实例，请确认已禁用此属性。否则，请选择 Yes, Disable。
5. 如果 NAT 实例具有辅助网络接口，请从 Description (目标) 选项卡上的 Network interfaces (网络接口) 中选择它，然后选择接口 ID 以转到网络接口页。依次选择 Actions (操作)、Change Source/Dest.Check (更改源/目标检查)，禁用设置，然后选择 Save (保存)。

使用命令行，禁用源/目标检查

您可以使用以下任一命令。有关更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

- [modify-instance-attribute \(AWS CLI\)](#)
- [Edit-EC2InstanceAttribute \(适用于 Windows PowerShell 的 AWS 工具\)](#)

更新主路由表

您 VPC 中的私有子网未与自定义路由表关联，因此它使用主路由表。默认情况下，主路由表使您的 VPC 中的实例能够互相通信。您必须添加一条路由，将所有其他子网流量发送到 NAT 实例。

更新主路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Route Tables。
3. 为 VPC 选择主路由表 (Main 列显示 Yes)。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。
4. 在 Routes 选项卡上选择 Edit，在 Destination 框中指定 0.0.0.0/0，从 Target 列表中选择 NAT 实例的实例 ID，然后选择 Save。
5. 在 Subnet Associations 选项卡上，选择 Edit，然后选中子网的 Associate 复选框。选择 Save (保存)。

有关更多信息，请参阅[路由表 \(p. 181\)](#)。

测试您的 NAT 实例配置

启动 NAT 实例并完成以上配置步骤之后，您可以执行简单的测试，以检查您的私有子网中的实例是否可以通过将 NAT 实例用作堡垒服务器来访问 Internet。为此，请更新您的 NAT 实例的安全组规则，以允许入站和出站 ICMP 流量以及出站 SSH 流量，将一个实例启动至您的私有子网中，配置 SSH 代理转发以访问您的私有子网中的实例，连接到您的实例，然后测试 Internet 连接。

更新您 NAT 实例的安全组

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Security Groups。
3. 找到与您的 NAT 实例关联的安全组，然后在 Inbound 选项卡中选择 Edit。
4. 选择添加规则，从类型列表中选择所有 ICMP - IPv4，然后从源列表中选择自定义。输入您私有子网的 IP 地址范围，例如 10.0.1.0/24。选择 Save (保存)。
5. 在 Outbound 选项卡中，选择 Edit。
6. 选择添加规则，从类型列表中选择 SSH，然后从目的地列表中选择自定义。输入您私有子网的 IP 地址范围，例如 10.0.1.0/24。选择 Save (保存)。
7. 选择添加规则，从类型列表中选择所有 ICMP - IPv4，然后从目的地列表中选择自定义。输入 0.0.0.0/0，然后选择 Save。

在您的私有子网中启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 在您的私有子网中启动实例。有关更多信息，请参阅[在您的子网中启动一项实例 \(p. 86\)](#)。确保您在启动向导中配置了以下选项，然后选择 Launch：
 - 在 Choose an Amazon Machine Image (AMI) (选择Amazon 系统映像(AMI)) 页面上，从 Quick Start (快速入门) 类别中选择 Amazon Linux AMI。
 - 在 Configure Instance Details (配置实例详细信息) 页面上，从 Subnet (子网) 列表中选择您的私有子网，并且不向您的实例分配公有 IP 地址。

- 在 Configure Security Group 页上，确保您的安全组包括入站规则，该规则允许从您的 NAT 实例的私有 IP 地址进行 SSH 访问，或者从公有子网的 IP 地址范围进行 SSH 访问；并且确保您具有允许出站 ICMP 流量的出站规则。
- 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，选择在启动 NAT 实例时所用的密钥对。

针对 Linux 或 OS X 配置 SSH 代理转发

- 在您的本地计算机上，将私有密钥添加到身份验证代理。

对于 Linux，请使用以下命令：

```
ssh-add -c mykeypair.pem
```

对于 OS X，请使用以下命令：

```
ssh-add -K mykeypair.pem
```

- 使用 -A 选项连接到您的 NAT 实例以启用 SSH 代理转发，例如：

```
ssh -A ec2-user@54.0.0.123
```

针对 Windows (PuTTY) 配置 SSH 代理转发

- 如果尚未安装 Pageant，请从 [PuTTY 下载页面](#) 下载并安装 Pageant。
- 将您的私有密钥转换为 .ppk 格式。有关更多信息，请参阅[使用 PuTTYgen 转换您的私有密钥](#)。
- 启动 Pageant，右键单击任务栏上的 Pageant 图标（可能已隐藏），并选择 Add Key。选择您创建的 .ppk 文件，输入密码（如果需要），然后选择 Open。
- 启动 PuTTY 会话以连接到您的 NAT 实例。在 Auth (身份验证) 类别中，确保选择了 Allow agent forwarding (允许代理转发) 选项，将 Private key file for authentication (用于身份验证的私有密钥文件) 字段留空。

测试 Internet 连接

- 通过对启用了 ICMP 的网站运行 ping 命令来测试您的 NAT 实例是否可以与 Internet 通信；例如：

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=48 time=74.9 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=48 time=75.1 ms  
...
```

按键盘上的 Ctrl+C 以取消 ping 命令。

- 从您的 NAT 实例，使用私有 IP 地址连接到您私有子网中的实例，例如：

```
ssh ec2-user@10.0.1.123
```

- 从您的私有实例，通过运行 ping 命令来测试您是否可以连接到 Internet：

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms  
...
```

按键盘上的 Ctrl+C 以取消 ping 命令。

如果 ping 命令失败，请检查以下信息：

- 检查您 NAT 实例的安全组规则是否允许来自您私有子网的入站 ICMP 流量。如果不允许，则您的 NAT 实例无法从您的私有实例接收 ping 命令。
 - 检查您是否正确配置了路由表。有关更多信息，请参阅 [更新主路由表 \(p. 221\)](#)。
 - 确保您对 NAT 实例禁用了源/目标检查。有关更多信息，请参阅 [正在禁用源/目标检查 \(p. 220\)](#)。
 - 确保您对启用了 ICMP 的网站发出 ping 命令。否则，您不会收到应答数据包。要对此进行测试，请从您自己计算机上的命令行终端执行相同的 ping 命令。
4. (可选) 如果不再需要，请终止您的私有实例。想要了解更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[终止您的实例](#)。

NAT 实例与 NAT 网关的比较

下面概括列出了 NAT 实例和 NAT 网关的区别。

属性	NAT 网关	NAT 实例
可用性	高度可用。每个可用区中的 NAT 网关都采用冗余实施。在每个可用区中创建一个 NAT 网关可确保架构不依赖于可用区。	使用脚本管理实例之间的故障转移。
带宽	可以扩展到 45 Gbps。	取决于实例类型的带宽。
维护	由 AWS 管理。您不需要进行任何维护。	由您管理，例如您需要对实例安装软件更新或操作系统补丁。
性能	软件经过优化以便处理 NAT 流量。	配置来执行 NAT 的通用 Amazon Linux AMI。
费用	费用取决于您使用的 NAT 网关的数量、使用时长以及您通过 NAT 网关发送的数据量。	费用取决于您使用的 NAT 实例的数量、使用时长以及实例类型和大小。
类型和大小	整合提供；您不需要选择类型或范围。	根据您的预测工作负载选择适当的实例类型和大小。
公有 IP 地址	在创建时选择弹性 IP 地址以与 NAT 网关关联。	为 NAT 实例使用弹性 IP 地址或公有 IP 地址。您随时可以通过将新的弹性 IP 地址与实例关联来更改公有 IP 地址。
私有 IP 地址	在您创建网关时自动从子网的 IP 地址范围中选择。	在您启动实例时，从子网的 IP 地址范围内分配特定的私有 IP 地址。
安全组	无法与 NAT 网关关联。您可以将安全组与 NAT 网关之后的资源关联，以控制入站和出站流量。	与您的 NAT 实例和 NAT 实例之后的资源关联，以控制入站和出站流量。
网络 ACL	使用网络 ACL 控制进出您的 NAT 网关所在子网的流量。	使用网络 ACL 控制进出您的 NAT 实例所在子网的流量。

属性	NAT 网关	NAT 实例
流日志	使用流日志捕获流量。	使用流日志捕获流量。
端口转发	不支持。	手动自定义配置以支持端口转发。
堡垒服务器	不支持。	用作堡垒服务器。
流量指标	查看 NAT 网关的 CloudWatch 指标 (p. 207) 。	查看实例的 CloudWatch 指标。
超时行为	如果连接超时，NAT 网关向 NAT 网关后方的任何资源返回 RST 数据包，尝试继续进行连接(它不发送 FIN 数据包)。	如果连接超时，NAT 实例向 NAT 实例后方的资源发送 FIN 数据包，以关闭连接。
IP 分段	支持转发 UDP 协议的 IP 分段数据包。 不支持 TCP 和 ICMP 协议的分段。将删除这些协议的分段数据包。	支持重组 UDP、TCP 和 ICMP 协议的 IP 分段数据包。

DHCP 选项集

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

您可以为虚拟私有云 (VPC) 配置 DHCP 选项集。

目录

- [DHCP 选项集概述 \(p. 224\)](#)
- [Amazon DNS 服务器 \(p. 225\)](#)
- [更改 DHCP 选项 \(p. 226\)](#)
- [使用 DHCP 选项集 \(p. 226\)](#)
- [API 和命令概览 \(p. 227\)](#)

DHCP 选项集概述

您在非默认 VPC 内启动的 Amazon EC2 实例默认属于私有实例；它们未分配公有 IPv4 地址，除非您在启动时特意为其分配一个，或是您修改子网的公有 IPv4 地址属性。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。

下表列出了针对 DHCP 选项集的所有支持的选项。您可在 DHCP 选项集中仅指定所需选项。有关这些选项的更多信息，请参阅 [RFC 2132](#)。

DHCP 选项名称	说明
domain-name-servers	最多四台域名服务器（即 AmazonProvidedDNS）的 IP 地址。默认 DHCP 选项集指定 AmazonProvidedDNS。如果指定的域名服务器不止一台，请使用逗号将它们隔开。尽管可以指定最多四个域名服务器，但请注意，某些操作系统可能会施加较低的限制。

DHCP 选项名称	说明
	如果要让实例接收 domain-name 中指定的自定义 DNS 主机名，则必须将 domain-name-servers 设置为自定义 DNS 服务器。
domain-name	如果您是在 us-east-1 中使用 AmazonProvidedDNS，请指定 ec2.internal。如果您是在其他区域中使用 AmazonProvidedDNS，请指定 region.compute.internal (例如 ap-northeast-1.compute.internal)。否则，请指定域名 (例如 example.com)。该值用于完成非限定的 DNS 主机名。有关 DNS 主机名和 VPC 中的 DNS 支持的更多信息，请参阅 在您的 VPC 中使用 DNS (p. 228) 。
	<p>Important</p> <p>某些 Linux 操作系统接受由空格分隔的多个域名。但是，Windows 以及其他 Linux 操作系统将该值视为单个域，因而会导致意外行为。如果您的 DHCP 选项集与有多个操作系统实例的 VPC 关联，请仅指定一个域名。</p>
ntp-servers	最多四个网络时间协议 (NTP) 服务器的 IP 地址。有关更多信息，请参阅 RFC 2132 的第 8.3 节。
netbios-name-servers	最多四个 NetBIOS 名称服务器的 IP 地址。
netbios-node-type	NetBIOS 节点类型 (1、2、4 或 8)。我们建议您指定 2 (点对点或 P 节点)。目前不支持广播和多播。有关这些节点类型的更多信息，请参阅 RFC 2132 的第 8.7 节，以及 RFC1001 的第 10 节。

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

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

您的 VPC 中的 Amazon DNS 服务器用于解析您在 Route 53 中的私有托管区域中指定的 DNS 域名。有关私有托管区域的更多信息，请参阅 Amazon Route 53 开发人员指南 中的 [使用私有托管区域](#)。

使用 Hadoop 框架的服务（如 Amazon EMR）要求实例解析自己的完全限定域名 (FQDN)。这种情况下，如果 domain-name-servers 选项设置为自定义值，则 DNS 解析可能会失败。要确保正确解析 DNS，请考虑在您的 DNS 服务器添加条件转发服务器，将针对域 *region-name*.compute.internal 的查询转发到 Amazon DNS 服务器。有关更多信息，请参阅 Amazon EMR 管理指南 中的 [设置 VPC 以托管集群](#)。

Note

您可以使用 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。如果您删除一个 VPC，与该 VPC 关联的 DHCP 选项集将与该 VPC 解除关联。

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。

使用 DHCP 选项集

此部分将为您展示如何使用 DHCP 选项集。

任务

- [正在创建 DHCP 选项集 \(p. 226\)](#)
- [更改 DHCP 选项集以供 VPC 使用 \(p. 227\)](#)
- [更改 VPC 以使用 NO DHCP 选项 \(p. 227\)](#)
- [正在删除 DHCP 选项集 \(p. 227\)](#)

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，请参阅[更改 DHCP 选项集以供 VPC 使用 \(p. 227\)](#)。

创建 DHCP 选项集

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 DHCP Options Sets，然后选择 Create DHCP options set。
3. 在该对话框中，输入要使用的选项值，然后选择 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 (域名服务器) 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。

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 选项集，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，请参阅[更改 VPC 以使用 NO DHCP 选项 \(p. 227\)](#)。

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，请参阅[正在创建 DHCP 选项集 \(p. 226\)](#)。

更改与 VPC 相关联的 DHCP 选项集。

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择 VPC，然后从 Actions (操作) 列表中选择 Edit DHCP Options Set (编辑 DHCP 选项集)。
4. 从 DHCP Options Set 列表中选择一组选项，然后选择 Save。

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 选择 VPC，然后从 Actions (操作) 列表中选择 Edit DHCP Options Set (编辑 DHCP 选项集)。
4. 从 DHCP Options Set 列表中选择 No DHCP Options Set，然后选择 Save。

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。

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 DHCP Options Sets。
3. 选择需要删除的 DHCP 选项集，然后选择 Delete。
4. 在确认对话框中，选择 Yes, Delete。

API 和命令概览

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅[访问 Amazon VPC \(p. 7\)](#)。

为您的 VPC 创建 DHCP 选项集

- [create-dhcp-options \(AWS CLI\)](#)
- [New-EC2DhcpOption \(适用于 Windows PowerShell 的 AWS 工具\)](#)

将 DHCP 选项集与指定 VPC 关联起来，或者不使用 DHCP 选项

- [associate-dhcp-options](#) (AWS CLI)
- [Register-EC2DhcpOption](#) (适用于 Windows PowerShell 的 AWS 工具)

说明一个或多个 DHCP 选项集

- [describe-dhcp-options](#) (AWS CLI)
- [Get-EC2DhcpOption](#) (适用于 Windows PowerShell 的 AWS 工具)

删除 DHCP 选项集

- [delete-dhcp-options](#) (AWS CLI)
- [Remove-EC2DhcpOption](#) (适用于 Windows PowerShell 的 AWS 工具)

在您的 VPC 中使用 DNS

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

公有 IPv4 地址可实现 Internet 间的通信，而私有 IPv4 地址可实现实例 (EC2-Classic 或 VPC) 网络内的通信。有关更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

我们提供 Amazon DNS 服务器。要使用您自己的 DNS 服务器，请为您的 VPC 创建一组新的 DHCP 选项。有关更多信息，请参阅 [DHCP 选项集 \(p. 224\)](#)。

目录

- [DNS 主机名 \(p. 228\)](#)
- [VPC 中的 DNS 支持 \(p. 229\)](#)
- [DNS 限制 \(p. 230\)](#)
- [查看您的 EC2 实例的 DNS 主机名称 \(p. 230\)](#)
- [更新您的 VPC 的 DNS 支持 \(p. 231\)](#)
- [使用私有托管区域 \(p. 231\)](#)

DNS 主机名

当您将实例启动到默认 VPC 中时，我们为实例提供与其公有 IPv4 和私有 IPv4 地址对应的公有和私有 DNS 主机名。当您在非默认 VPC 中启动实例时，我们会为实例提供私有 DNS 主机名，并根据您为 VPC 指定的 [DNS 属性 \(p. 229\)](#) 以及您的实例是否具有公有 IPv4 地址来决定是否提供公有 DNS 主机名。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[公有 IPv4 地址和外部 DNS 主机名](#)。

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

对于 us-east-1 区域，公有（外部）DNS 主机名采用 `ec2-public-ipv4-address.compute-1.amazonaws.com` 形式，对于其他区域，则采用 `ec2-public-ipv4-`

address.region.compute.amazonaws.com 形式。我们将公有 DNS 主机名解析为该实例在所在网络外的公有 IPv4 地址及其在所在网络内的私有 IPv4 地址。

我们不为 IPv6 地址提供 DNS 主机名。

VPC 中的 DNS 支持

您的 VPC 具有一些属性，可用于确定在 VPC 中启动的实例是否接收与其公有 IP 地址对应的公有 DNS 主机名，以及 VPC 是否支持通过 Amazon DNS 服务器进行的 DNS 解析。

属性	说明
<code>enableDnsHostnames</code>	指示具有公有 IP 地址的实例是否获得对应的公有 DNS 主机名。 如果此属性为 <code>true</code> ，VPC 中的实例将获取公有 DNS 主机名，但前提是 <code>enableDnsSupport</code> 属性也设置为 <code>true</code> 。
<code>enableDnsSupport</code>	指示是否支持 DNS 解析。 如果此属性为 <code>false</code> ，则不启用由 Amazon 提供的、将公有 DNS 主机名称解析为 IP 地址的 DNS 服务器。 如果此属性为 <code>true</code> ，则通过 169.254.169.253 IP 地址或是在 VPC IPv4 网络范围基础上“+2”的预留 IP 地址来查询 Amazon 提供的 DNS 服务器将会成功。有关更多信息，请参阅 Amazon DNS 服务器 (p. 225) 。

如果两个属性都设置为 `true`，则会发生以下情况：

- 具有公有 IP 地址的实例会收到对应的公有 DNS 主机名。
- Amazon 提供的 DNS 服务器可以解析 Amazon 提供的私有 DNS 主机名。

如果其中一个或两个属性设置为 `false`，则会发生以下情况：

- 具有公有 IP 地址的实例不会收到对应的公有 DNS 主机名。
- Amazon 提供的 DNS 服务器无法解析 Amazon 提供的私有 DNS 主机名。
- 如果 [DHCP 选项集 \(p. 224\)](#) 中存在自定义域名，则实例会收到自定义私有 DNS 主机名。如果您未使用 Amazon 提供的 DNS 服务器，您的自定义域名服务器必须正确解析主机名。

默认情况下，在默认 VPC 或 VPC 向导创建的 VPC 中，两个属性都设置为 `true`。默认情况下，在以任何其他方式创建的 VPC 中，仅 `enableDnsSupport` 属性设置为 `true`。

Important

如果您使用在 Amazon Route 53 中的私有托管区域中定义的自定义 DNS 域名，或者使用具有接口 VPC 终端节点的私有 DNS (AWS PrivateLink)，则必须将 `enableDnsHostnames` 和 `enableDnsSupport` 属性设置为 `true`。

Amazon DNS 服务器可以将私有 DNS 主机名解析为全部地址空间内的私有 IPv4 地址，包括您的 VPC 的 IPv4 地址范围不在 [RFC 1918](#) 指定的私有 IPv4 地址范围内的情况。

Important

如果您在 2016 年 10 月之前创建 VPC，并且您的 VPC 的 IPv4 地址范围不在 RFC 1918 所指定的私有 IPv4 地址范围内，则 Amazon DNS 服务器将无法解析私有 DNS 主机名。如果您希望 Amazon DNS 服务器能够对这些 IP 地址解析私有 DNS 主机名，请联系 [AWS Support](#)。

如果您在之前不支持 DNS 主机名和 DNS 支持的 VPC 中启用这两项内容，则您已经启动至该 VPC 中、具有公有 IPv4 地址或弹性 IP 地址的某个实例会获得一个公有 DNS 主机名。

DNS 限制

每个 Amazon EC2 实例可以向 Amazon 提供的 DNS 服务器发送的数据包数量限制为：每个网络接口每秒最多 1024 个数据包。不能提高此限制。由 Amazon 提供的 DNS 服务器支持的每秒 DNS 查询数量因查询类型、响应大小和所用协议而异。有关可扩展 DNS 架构的更多信息和建议，请参阅 [Amazon VPC 的混合云 DNS 解决方案白皮书](#)。

查看您的 EC2 实例的 DNS 主机名称

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

实例

使用控制台查看实例的 DNS 主机名称

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Instances。
3. 从列表中选择您的实例。
4. 在详细信息窗格中，Public DNS (IPv4) 和 Private DNS 字段显示 DNS 主机名 (如适用)。

使用命令行查看实例的 DNS 主机名

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (适用于 Windows PowerShell 的 AWS 工具)

网络接口

使用控制台查看网络接口的私有 DNS 主机名

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 从列表中选择网络接口。
4. 在详细信息窗格中，私有 DNS (IPv4) 字段显示私有 DNS 主机名。

使用命令行查看网络接口的 DNS 主机名

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

- [describe-network-interfaces](#) (AWS CLI)

- [Get-EC2NetworkInterface](#) (适用于 Windows PowerShell 的 AWS 工具)

更新您的 VPC 的 DNS 支持

您可以通过 Amazon VPC 控制台查看并更新您的 VPC 中的 DNS 支持属性。

使用控制台描述和更新 VPC 的 DNS 支持

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Your VPCs。
3. 从列表中选择 VPC。
4. 查看 Summary (摘要) 选项卡中的信息。在这个例子中，两项设置都已被启用。

DNS resolution Enabled
DNS hostnames Enabled

5. 要更新这些设置，请选择 Actions 并选择 Edit DNS Resolution 或 Edit DNS Hostnames。在打开的对话框中选择 Yes 或 No，然后选择 Save。

使用命令行说明 VPC 的 DNS 支持

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

- [describe-vpc-attribute](#) (AWS CLI)
- [Get-EC2VpcAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

使用命令行更新 VPC 的 DNS 支持

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

- [modify-vpc-attribute](#) (AWS CLI)
- [Edit-EC2VpcAttribute](#) (适用于 Windows PowerShell 的 AWS 工具)

使用私有托管区域

如果要使用自定义 DNS 域名 (如 example.com) 而不是使用私有 IPv4 地址或 AWS 提供的私有 DNS 主机名来访问您的 VPC 中的资源，可以在 Route 53 中创建一个私有托管区域。私有托管区域就是一个容器，其中包含的信息说明您希望如何在一个或多个 VPC 中为某个域及其子域路由流量而不将您的资源公开到 Internet。您可以创建 Route 53 资源记录集，用来确定 Route 53 将如何响应对您的域及其子域的查询。例如，如果您希望将对 example.com 的浏览器请求路由到您 VPC 中的某个 Web 服务器，可以在您的私有托管区域中创建一条 A 记录并指定该 Web 服务器的 IP 地址。有关创建私有托管区域的更多信息，请参阅 [Amazon Route 53 开发人员指南](#) 中的 [使用私有托管区域](#)。

要使用自定义 DNS 域名访问资源，必须连接到您的 VPC 中的实例。在您的实例中，您可通过使用 ping 命令来测试是否可从私有托管区域中的资源的自定义 DNS 名称访问该资源；例如，ping mywebserver.example.com。(您必须确保您的实例的安全组规则允许入站 ICMP 流量才能使 ping 命令正常运行。)

您可以从通过 ClassicLink 链接到您的 VPC 的 EC2-Classic 实例访问私有托管区域，前提是您为 VPC 启用了 ClassicLink DNS 支持。有关更多信息，请参阅 [Amazon EC2 用户指南 \(适用于 Linux 实例\)](#) 中的 [启用 ClassicLink DNS 支持](#)。否则，私有托管区域不支持 VPC 外的传递关系；例如，您不能使用资源的自定义私有 DNS 名称从 VPN 连接的另一端访问资源。

Important

如果您使用在 Amazon Route 53 中的私有托管区域中定义的自定义 DNS 域名，则必须将以下 `enableDnsHostnames` 和 `enableDnsSupport` 属性设置为 `true`。

VPC 对等

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

AWS 使用 VPC 的现有基础设施来创建 VPC 对等连接；该连接既非网关也非 AWS Site-to-Site VPN 连接，且不依赖某个单独的物理硬件。没有单点通信故障也没有带宽瓶颈。

有关使用 VPC 对等连接的更多信息以及可使用 VPC 对等连接的方案的示例，请参阅 [Amazon VPC Peering Guide](#)。

弹性 IP 地址

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

我们目前不支持对 IPv6 使用弹性 IP 地址。

目录

- [弹性 IP 地址基础信息 \(p. 232\)](#)
- [使用弹性 IP 地址 \(p. 233\)](#)
- [API 和 CLI 概述 \(p. 234\)](#)

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：

- 首先分配一个在 VPC 中使用的弹性 IP 地址，然后将其与 VPC 中的实例关联起来（每次只能将其分配给一个实例）。
- 弹性 IP 地址是网络接口的一项属性。您可以通过更新附加到实例的网络接口，将弹性 IP 地址与该实例关联起来。
- 如果将弹性 IP 地址与实例的 eth0 网络接口关联起来，系统会将其当前的公有 IPv4 地址（如果有）释放到 EC2-VPC 公有 IP 地址池中。如果取消关联弹性 IP 地址，系统将自动在几分钟内为 eth0 网络接口分配一个新的公有 IPv4 地址。如果再向您的实例附加一个网络接口，则不适用此情况。
- 在 VPC 中使用的弹性 IP 地址与在 EC2-Classic 中使用的弹性 IP 地址之间存在一些区别。有关更多信息，请参阅 [Amazon EC2 用户指南（适用于 Linux 实例）](#) 中的 [EC2-Classic 与 Amazon EC2-VPC 之间的弹性 IP 地址区别](#)。
- 您可以将弹性 IP 地址从一个实例移动到另一个实例。实例可以来自同一 VPC 或其他 VPC，但不可来自 EC2-Classic。
- 您的弹性 IP 地址会保持与您的 AWS 账户的关联，直到您明确释放这些地址为止。

- 为确保弹性 IP 地址的有效使用，当这些地址未与正在运行的实例关联或者关联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，对于与该实例关联的一个弹性 IP 地址，您无需承担相应费用，但对于与该实例关联的所有其他弹性 IP 地址，您需要承担相应费用。有关更多信息，请参阅 [Amazon EC2 定价](#)。
- 您仅可以拥有 5 个弹性 IP 地址；为了帮助保留这些弹性 IP 地址，您可以使用 NAT 设备（请参阅 [NAT \(p. 200\)](#)）。
- 弹性 IP 地址可通过 VPC 的 Internet 网关进行访问。如果您已经在 VPC 与网络之间设置了 AWS Site-to-Site VPN 连接，则 VPN 流量将通过虚拟专用网关而不是 Internet 网关，因此无法访问该弹性 IP 地址。
- 您可将已分配为在 EC2-Classic 平台中使用的弹性 IP 地址移至 VPC 平台。有关更多信息，请参阅 [Amazon EC2 用户指南 中的将弹性 IP 地址从 EC2-Classic 迁移到 EC2-VPC](#)。
- 您可以为已分配用于 VPC 的弹性 IP 地址添加标签；不过，不支持成本分配标签。如果您恢复弹性 IP 地址，标签不会恢复。

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

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Elastic IPs。
- 选择 Allocate new address。
- 选择 Allocate。

Note

如果您的账户支持 EC2-Classic，请首先选择 VPC。

查看您的弹性 IP 地址

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Elastic IPs。
- 要筛选显示列表，您可以在搜索框中输入为其分配该地址的实例的弹性 IP 地址或 ID 的一部分。

将弹性 IP 地址与运行的 VPC 实例相关联

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Elastic IPs。
- 选择分配用于 VPC (Scope 列的值为 vpc) 的弹性 IP 地址，选择 Actions，然后选择 Associate address。
- 选择 Instance 或 Network interface，然后选择实例 ID 或网络接口 ID。选择要与弹性 IP 地址关联的私有 IP 地址。选择 Associate。

Note

网络接口可能有几个属性，包括弹性 IP 地址。您可以创建网络接口，并在您的 VPC 中将它连接到实例或断开其与实例的连接。与直接将弹性 IP 地址与实例关联相比，使用弹性 IP 地址作为网络接口的属性的优势在于，只需要一步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。有关更多信息，请参阅 [弹性网络接口](#)。

如果 DNS 主机名称已启用，则在您将弹性 IP 地址与实例关联后，它将收到一个 DNS 主机名。有关更多信息，请参阅 [在您的 VPC 中使用 DNS \(p. 228\)](#)。

您可以对弹性 IP 地址应用标签，以帮助您识别它或根据组织的需要对其进行分类。

为弹性 IP 地址添加标签

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择弹性 IP 地址，然后选择标签。
4. 选择添加/编辑标签，根据需要输入标签键和值，然后选择保存。

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. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Disassociate address。
4. 系统提示时，选择 Disassociate address。

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）。对于被分配用于 VPC 但未与实例关联的所有弹性 IP 地址，您也需要承担相应费用。

解除弹性 IP 地址

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Release addresses。
4. 系统提示时，选择 Release。

如果您释放了您的弹性 IP 地址，则可能能够恢复它。如果弹性 IP 地址已分配给另一 AWS 账户，则无法恢复此地址，否则会导致您超出您的弹性 IP 地址限制。

当前，您只能使用 Amazon EC2 API 或命令行工具恢复弹性 IP 地址。

使用 AWS CLI 恢复弹性 IP 地址

- 使用 `allocate-address` 命令和 `--address` 参数指定 IP 地址。

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

API 和 CLI 概述

您可以使用命令行或 API 执行此页面上所说明的任务。有关命令行界面以及可用 API 列表的更多信息，请参阅 [访问 Amazon VPC \(p. 7\)](#)。

获取弹性 IP 地址

- `allocate-address` (AWS CLI)
- `New-EC2Address` (适用于 Windows PowerShell 的 AWS 工具)

将弹性 IP 地址与实例或网络接口关联起来

- [associate-address \(AWS CLI\)](#)
- [Register-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

说明一个或多个弹性 IP 地址

- [describe-addresses \(AWS CLI\)](#)
- [Get-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

为弹性 IP 地址添加标签

- [create-tags \(AWS CLI\)](#)
- [New-EC2Tag \(适用于 Windows PowerShell 的 AWS 工具\)](#)

解除弹性 IP 地址的关联

- [disassociate-address \(AWS CLI\)](#)
- [Unregister-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

释放弹性 IP 地址

- [release-address \(AWS CLI\)](#)
- [Remove-EC2Address \(适用于 Windows PowerShell 的 AWS 工具\)](#)

VPC 终端节点

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

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

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

接口终端节点（由 [AWS PrivateLink 提供支持](#)）

接口终端节点 (p. 237) 是一个弹性网络接口，具有来自子网 IP 地址范围的私有 IP 地址，用作发送到受支持的服务的通信的入口点。支持以下服务：

- [Amazon API Gateway](#)
- [App Mesh](#)
- [AWS CloudFormation](#)
- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon CloudWatch Events](#)
- [Amazon CloudWatch Logs](#)

- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- Amazon EC2 API
- Elastic Load Balancing
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Glue
- AWS Key Management Service
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon SageMaker 和 Amazon SageMaker 运行时
- Amazon SageMaker 笔记本实例
- AWS Secrets Manager
- AWS Security Token Service
- AWS Service Catalog
- Amazon SNS
- Amazon SQS
- AWS Systems Manager
- AWS Storage Gateway
- AWS Transfer for SFTP
- 其他 AWS 账户托管的终端节点服务 (p. 263)
- 支持的 AWS Marketplace 合作伙伴服务

网关终端节点

网关终端节点 (p. 249) 是一个网关，作为您在路由表中指定的路由的目标，用于发往受支持的 AWS 服务的流量。支持以下 AWS 服务：

- Amazon S3
- DynamoDB

控制 VPC 终端节点 的使用

默认情况下，IAM 用户无权使用终端节点。您可以创建一个 IAM 用户策略，向用户授予创建、修改、描述和删除终端节点的权限。对于所有 `ec2:*VpcEndpoint*` API 操作，或 `ec2:DescribePrefixLists` 操作，我们目前均不支持资源级权限。无法创建 IAM 策略，向用户授予使用特定终端节点或前缀列表的权限。以下是示例：

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:*VpcEndpoint*",  
            "Resource": "*"  
        }  
    ]  
}
```

}

接口 VPC 终端节点 (AWS PrivateLink)

利用接口 VPC 终端节点 (接口终端节点) , 您可连接到由 AWS PrivateLink 提供支持的服务。这些服务包括一些 AWS 服务 , 由其他 AWS 客户和合作伙伴在他们自己的 VPC 中托管的服务 (称为终端节点服务) , 以及受支持的 AWS Marketplace 合作伙伴服务。服务的所有者是服务提供商 , 您 (作为创建接口终端节点的委托人) 是服务使用者。

支持以下服务 :

- [Amazon API Gateway](#)
- [App Mesh](#)
- [AWS CloudFormation](#)
- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon CloudWatch Events](#)
- [Amazon CloudWatch Logs](#)
- [AWS CodeBuild](#)
- [AWS CodeCommit](#)
- [AWS CodePipeline](#)
- [AWS Config](#)
- [Amazon EC2 API](#)
- [Elastic Load Balancing](#)
- [Amazon Elastic Container Registry](#)
- [Amazon Elastic Container Service](#)
- [AWS Glue](#)
- [AWS Key Management Service](#)
- [Amazon Kinesis Data Firehose](#)
- [Amazon Kinesis Data Streams](#)
- [Amazon SageMaker 和 Amazon SageMaker 运行时](#)
- [Amazon SageMaker 笔记本实例](#)
- [AWS Secrets Manager](#)
- [AWS Security Token Service](#)
- [AWS Service Catalog](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [AWS Systems Manager](#)
- [AWS Storage Gateway](#)
- [AWS Transfer for SFTP](#)
- 其他 AWS 账户托管的 [终端节点服务 \(p. 263\)](#)
- 支持的 AWS Marketplace 合作伙伴服务

以下是设置接口终端节点的常规步骤 :

1. 选择要在其中创建接口终端节点的 VPC , 然后提供您要连接到的 AWS 服务、终端节点服务或 AWS Marketplace 服务的名称。

2. 在 VPC 中选择使用接口终端节点的子网。我们将在该子网中创建一个终端节点网络接口。您可以在不同的可用区内指定多个子网（在服务支持的情况下），以帮助确保您的接口终端节点能够在出现可用区故障时复原。在此情况下，我们将在您指定的每个子网中创建一个终端节点网络接口。

Note

终端节点网络接口是由请求者管理的网络接口。您可以在您的账户中查看它，但不能亲自管理。
有关更多信息，请参阅[弹性网络接口](#)。

3. 指定要与终端节点网络接口关联的安全组。安全组规则将控制从 VPC 中的资源发送到终端节点网络接口的通信。如果您未指定安全组，我们将关联 VPC 的默认安全组。
- 4.（可选；仅限 AWS 服务和 AWS Marketplace 合作伙伴服务）为终端节点启用[私有 DNS \(p. 238\)](#) 以便您能够使用服务的默认 DNS 主机名对服务发出请求。

Important

默认情况下，对于为 AWS 服务和 AWS Marketplace 合作伙伴服务创建的终端节点会启用私有 DNS。

5. 当服务提供商与使用者处于不同的账户中时，请参阅[the section called “接口终端节点可用区注意事项” \(p. 242\)](#)了解如何使用可用区 ID 识别接口终端节点可用区。
6. 已创建的接口终端节点在服务提供商接受后即可使用。服务提供商必须将服务配置为自动或手动接受请求。AWS 服务和 AWS Marketplace 服务一般会自动接受所有终端节点请求。有关终端节点生命周期的更多信息，请参阅[接口终端节点生命周期 \(p. 241\)](#)。

服务无法通过终端节点发起对您的 VPC 中的资源的请求。终端节点仅返回对从您的 VPC 中的资源启动的通信的响应。在集成服务和终端节点之前，请查看特定于服务的 VPC 终端节点文档，了解任何特定于服务的配置和限制。

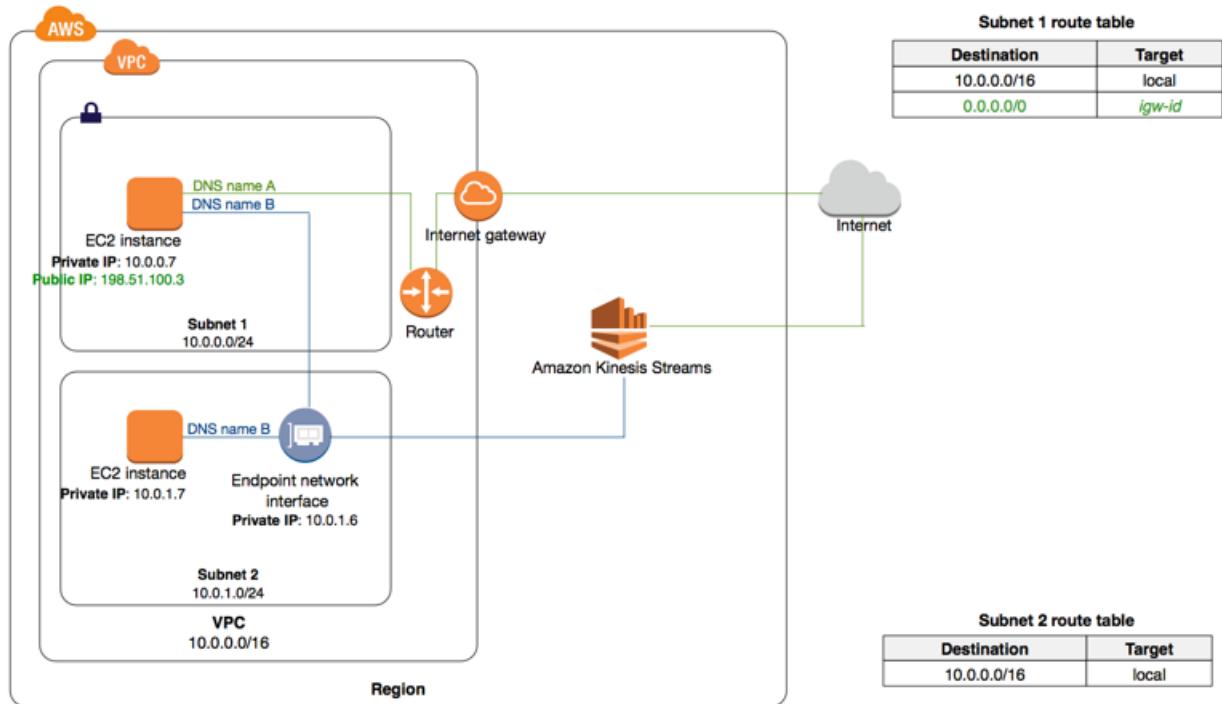
目录

- [私有 DNS \(p. 238\)](#)
- [接口终端节点属性和限制 \(p. 240\)](#)
- [接口终端节点生命周期 \(p. 241\)](#)
- [接口终端节点可用区注意事项 \(p. 242\)](#)
- [接口终端节点的定价 \(p. 242\)](#)
- [创建接口终端节点 \(p. 242\)](#)
- [查看您的接口终端节点 \(p. 245\)](#)
- [为接口终端节点创建和管理通知 \(p. 246\)](#)
- [通过接口终端节点访问服务 \(p. 247\)](#)
- [修改接口终端节点 \(p. 248\)](#)

私有 DNS

当您创建接口终端节点时，我们将生成您可用于与服务通信的终端节点特定 DNS 主机名。对于 AWS 服务和 AWS Marketplace 合作伙伴服务，私有 DNS（默认启用）会将私有托管区域与您的 VPC 相关联。托管区域包含服务的默认 DNS 名称（例如，`ec2.us-east-1.amazonaws.com`）的记录集，用于解析为您的 VPC 中的终端节点网络接口的私有 IP 地址。这使您能够使用服务的默认 DNS 主机名而不是终端节点特定 DNS 主机名向服务发出请求。例如，如果您的现有应用程序向 AWS 服务发出请求，则这些应用程序将继续通过接口终端节点发出请求，而无需任何配置更改。

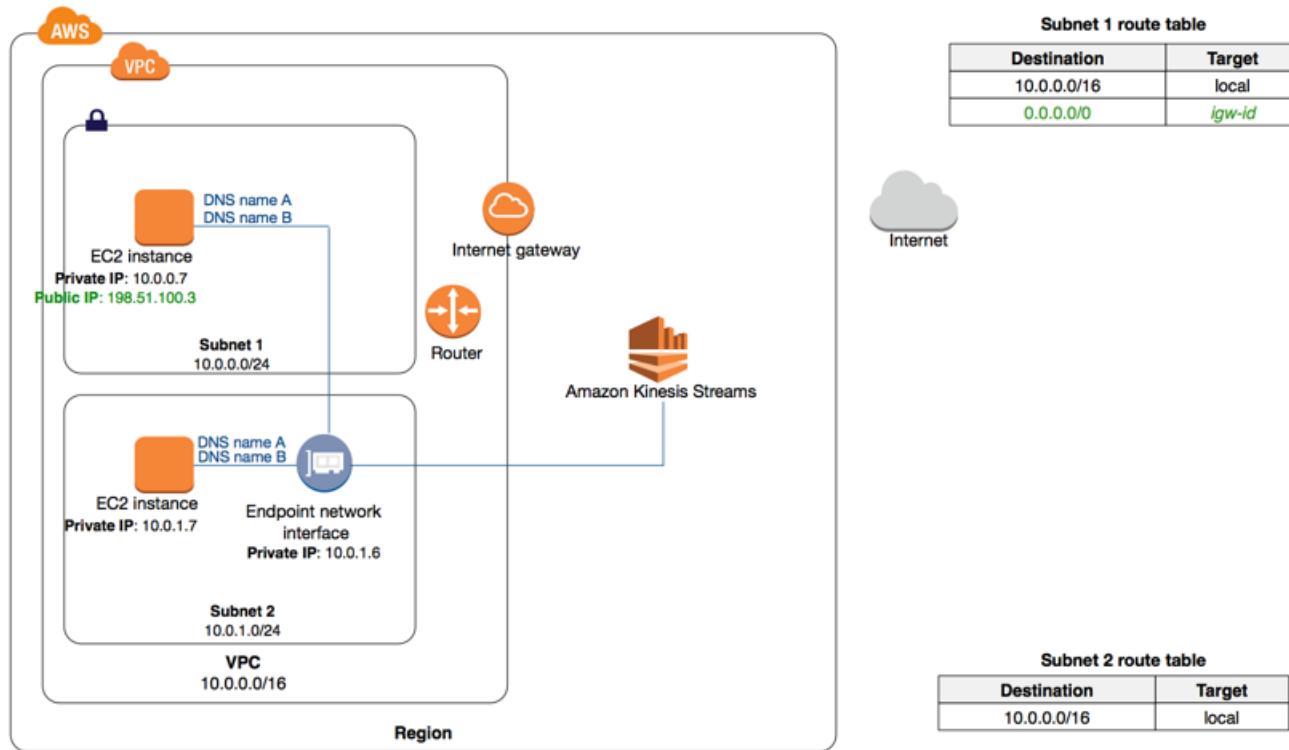
在下图中，您已为 Amazon Kinesis Data Streams 创建一个接口终端节点并在子网 2 中创建一个终端节点网络接口。您尚未为接口终端节点启用私有 DNS。任一子网中的实例都可通过接口终端节点使用终端节点特定 DNS 主机名（DNS 名称 B）与 Amazon Kinesis Data Streams 通信。子网 1 中的实例可通过 AWS 区域中的公有 IP 地址空间，使用服务的默认 DNS 名称（DNS 名称 A）与 Amazon Kinesis Data Streams 通信。



DNS name A: kinesis.us-east-1.amazonaws.com (default DNS hostname)

DNS name B: vpce-123-ab.kinesis.us-east-1.vpce.amazonaws.com (endpoint-specific hostname)

在下图中，您已为终端节点启用私有 DNS。任一子网中的实例都可通过接口终端节点使用终端节点特定 DNS 主机名 (DNS 名称 B) 或服务的默认 DNS 名称 (DNS 名称 A) 与 Amazon Kinesis Data Streams 通信。



DNS name A: kinesis.us-east-1.amazonaws.com (default DNS hostname)
DNS name B: vpce-123-ab.kinesis.us-east-1.vpce.amazonaws.com (endpoint-specific hostname)

Important

要使用私有 DNS，您必须将以下 VPC 属性设置为 `true : enableDnsHostnames` 和 `enableDnsSupport`。有关更多信息，请参阅[更新您的 VPC 的 DNS 支持 \(p. 231\)](#)。IAM 用户必须有权使用托管区域。有关更多信息，请参阅[Route 53 的身份验证和访问控制](#)。

接口终端节点属性和限制

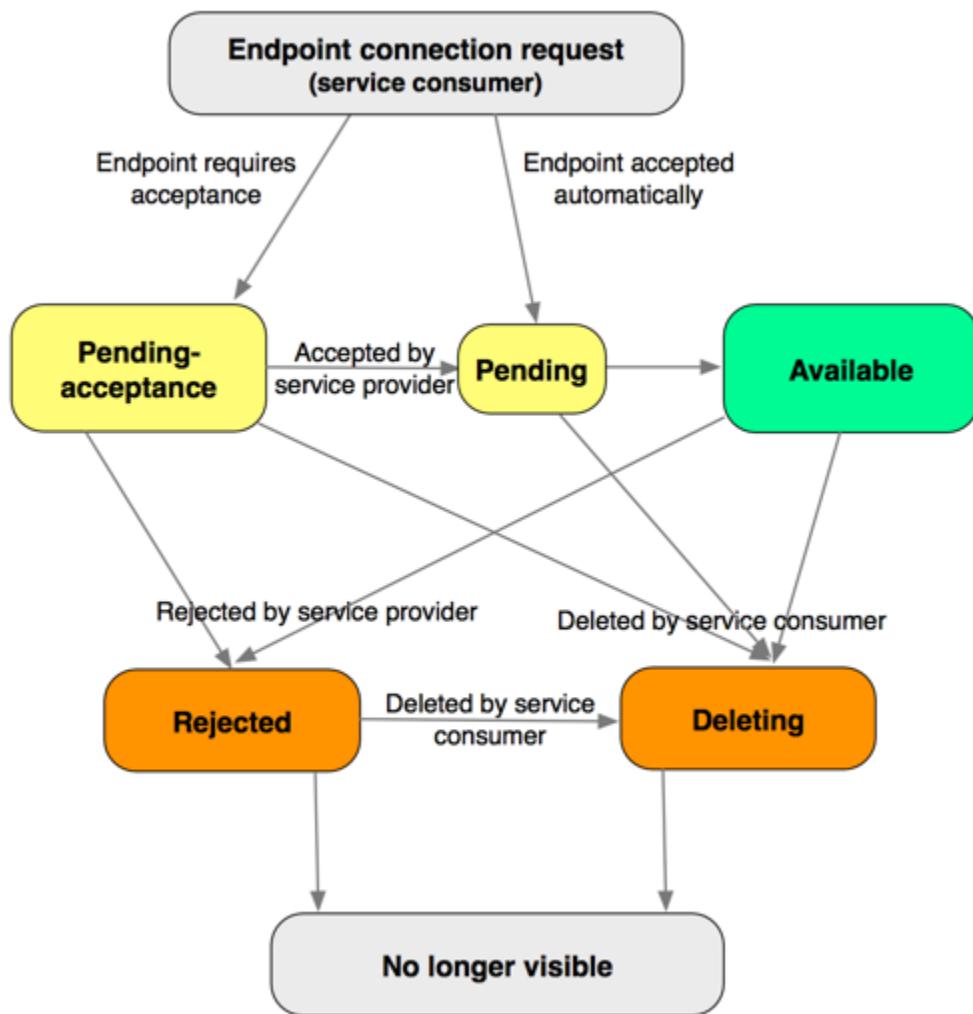
要使用接口终端节点，您需要了解它们的属性和当前限制：

- 对于每个接口终端节点，每个可用区您只能选择一个子网。
- 接口终端节点允许使用支持终端节点策略的服务的策略。有关支持策略的服务的信息，请参阅[the section called “使用 VPC 终端节点 控制对服务的访问” \(p. 262\)](#)。
- 可能无法在所有可用区中通过接口终端节点使用服务。要了解支持的可用区，请使用 `describe-vpc-endpoint-services` 命令或使用 Amazon VPC 控制台。有关更多信息，请参阅[创建接口终端节点 \(p. 242\)](#)。
- 创建接口终端节点时，将在映射至您的账户且独立于其他账户的可用区中创建此终端节点。当服务提供商与使用者处于不同的账户中时，请参阅[the section called “接口终端节点可用区注意事项” \(p. 242\)](#)了解如何使用可用区 ID 识别接口终端节点可用区。
- 默认情况下，每个可用区的每个接口终端节点可支持高达 10 Gbps 的带宽。可基于您的使用情况自动添加更多容量。
- 如果子网的网络 ACL 限制流量，您可能无法通过终端节点网络接口发送流量。请确保您增加了相应的规则，允许与子网的 CIDR 块之间的往返流量。
- 接口终端节点仅支持 TCP 流量。

- 仅在同一地区内支持终端节点。无法在 VPC 和其他区域内的服务之间创建终端节点。
- 无法标记终端节点。
- 终端节点仅支持 IPv4 流量。
- 无法将终端节点从一个 VPC 转移到另一个 VPC，也无法将终端节点从一项服务转移到另一项服务。
- 您可以为每个 VPC 创建的终端节点的数量有限制。有关更多信息，请参阅 [VPC 终端节点 \(p. 279\)](#)。

接口终端节点生命周期

从您创建接口终端节点 (终端节点连接请求) 时开始，接口终端节点将经历不同的阶段。在每个阶段，可能会有一些服务使用者和服务提供商可执行的操作。



以下规则适用：

- 服务提供商可以将其服务配置为自动或手动接受接口终端节点请求。AWS 服务和 AWS Marketplace 服务一般会自动接受所有终端节点请求。
- 服务提供商无法删除连接至其服务的接口终端节点。只有请求接口终端节点连接的服务使用者才可以删除接口终端节点。
- 服务提供商可以在接口终端节点已被接受 (手动或自动) 并处于 available 状态之后拒绝它。

接口终端节点可用区注意事项

创建接口终端节点时，将在映射至您的账户且独立于其他账户的可用区中创建此终端节点。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别接口终端节点可用区。例如，use1-az1 是 us-east-1 区域的 AZ ID，它映射至每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南 中的[您的资源的 AZ ID](#) 或使用 `describe-availability-zones`。

可能无法在所有可用区中通过接口终端节点使用服务。您可以使用以下操作中的任意一种，了解一项服务有哪些受支持的可用区：

- `describe-vpc-endpoint-services` (AWS CLI)
- `DescribeVpcEndpointServices` (API)
- 您创建接口终端结点时使用的 Amazon VPC 控制台。有关更多信息，请参阅[the section called “创建接口终端节点” \(p. 242\)](#)。

接口终端节点的定价

您在为某个服务创建和使用接口终端节点时需要付费。将按小时使用费率和数据处理费率收费。有关更多信息，请参阅 [AWS PrivateLink 定价](#)。

创建接口终端节点

要创建接口终端节点，您必须指定要在其中创建接口终端节点的 VPC 和要连接到的服务。

对于 AWS 服务或 AWS Marketplace 合作伙伴服务，您可以选择为终端节点启用[私有 DNS \(p. 238\)](#)，以便您可以使用默认的 DNS 主机名向服务发出请求。

Important

默认情况下，对于为 AWS 服务和 AWS Marketplace 合作伙伴服务创建的终端节点会启用私有 DNS。

有关 AWS 服务的特定信息，请参阅 [VPC 终端节点 \(p. 235\)](#)。

使用控制台创建连接到 AWS 服务的接口终端节点

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service category，请确保选中 AWS services。
4. 对于 Service Name，请选择要连接到的服务。对于 Type，请确保它指示 Interface。
5. 填写以下信息，然后选择 Create endpoint。
 - 对于 VPC，选择要在其中创建终端节点的 VPC。
 - 对于 Subnets，选择要在其中创建终端节点网络接口的子网 (可用区)。

Note

并非所有可用区都支持所有 AWS 服务。

- 要为接口终端节点启用私有 DNS，请选中启用私有 DNS 名称对应的复选框。

Note

默认情况下，此选项处于启用状态。要使用私有 DNS 选项，您的 VPC 的以下属性必须设置为 `true`：`enableDnsHostnames` 和 `enableDnsSupport`。有关更多信息，请参阅[更新您的 VPC 的 DNS 支持 \(p. 231\)](#)。

- 对于 Security group，选择要与终端节点网络接口关联的安全组。

要创建连接到终端节点服务的接口终端节点，您必须具有要连接到的服务的名称。服务提供商可为您提供此名称。

创建连接到终端节点服务的接口终端节点

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service category，选择 Find service by name。
4. 对于 Service Name，输入服务的名称（例如，com.amazonaws.us-east-1.vpce-svc-0e123abc123198abc）并选择 Verify。
5. 填写以下信息，然后选择 Create endpoint。
 - 对于 VPC，选择要在其中创建终端节点的 VPC。
 - 对于 Subnets，选择要在其中创建终端节点网络接口的子网（可用区）。

Note

并非所有可用区都支持此服务。

- 对于 Security group，选择要与终端节点网络接口关联的安全组。

创建连接到 AWS Marketplace 合作伙伴服务的接口终端节点

1. 转至 AWS Marketplace 上的 [PrivateLink](#) 页面并向软件即服务 (SaaS) 提供商订阅服务。支持接口终端节点的服务包括通过终端节点进行连接的选项。
2. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
3. 在导航窗格中，选择 Endpoints、Create Endpoint。
4. 对于 Service category，选择 Your AWS Marketplace services.
5. 选择您已订阅的 AWS Marketplace 服务。
6. 填写以下信息，然后选择 Create endpoint。
 - 对于 VPC，选择要在其中创建终端节点的 VPC。
 - 对于 Subnets，选择要在其中创建终端节点网络接口的子网（可用区）。

Note

并非所有可用区都支持此服务。

- 对于 Security group，选择要与终端节点网络接口关联的安全组。

使用 AWS CLI 创建接口终端节点

1. 使用 `describe-vpc-endpoint-services` 命令获取可用服务的列表。在返回的输出中，记录要连接到的服务的名称。ServiceType 字段指示是通过接口终端节点还是网关终端节点连接到服务。ServiceName 字段提供服务的名称。

```
aws ec2 describe-vpc-endpoint-services
```

```
{  
    "vpcEndpoints": [  
        {  
            "VpcEndpointId": "vpce-08a979e28f97a9f7c",  
            "VpcEndpointType": "Interface",  
            "VpcId": "vpc-06e4ab6c3b23ae3",  
            "ServiceName": "com.amazonaws.us-east-2.monitoring",  
            "State": "available",  
            "Status": "PENDING_ACCEPTANCE"  
        }  
    ]  
}
```

```

    "PolicyDocument": "{\n      \"Statement\": [\n        {\n          \"Action\": \"*\",\n          \"Resource\": \"*\n          \"/\n          \"Effect\": \"Allow\", \"Principal\": \"*\", \"\n          \"/\n          \"RouteTableIds\": [],\n          \"SubnetIds\": [\n            \"subnet-0931fc2fa5f1cbe44\"\n          ],\n          \"Groups\": [\n            {\n              \"GroupId\": \"sg-06e1d57ab87d8f182\",\n              \"GroupName\": \"default\"\n            }\n          ],\n          \"PrivateDnsEnabled\": false,\n          \"RequesterManaged\": false,\n          \"NetworkInterfaceIds\": [\n            \"eni-019b0bb3ede80ebfd\"\n          ],\n          \"DnsEntries\": [\n            {\n              \"DnsName\": \"vpce-08a979e28f97a9f7c-4r5zme9n.monitoring.us-\n              east-2.vpce.amazonaws.com\",\n              \"HostedZoneId\": \"ZC8PGOKIFKBRI\"\n            },\n            {\n              \"DnsName\": \"vpce-08a979e28f97a9f7c-4r5zme9n-us-\n              east-2c.monitoring.us-east-2.vpce.amazonaws.com\",\n              \"HostedZoneId\": \"ZC8PGOKIFKBRI\"\n            }\n          ],\n          \"CreationTimestamp\": \"2019-06-04T19:10:37.000Z\",\n          \"Tags\": [],\n          \"OwnerId\": \"123456789012\"\n        }\n      ]\n    }"
  ]
}

```

- 要创建接口终端节点，请使用 [create-vpc-endpoint](#) 命令并指定 VPC ID、VPC 终端节点（接口）的类型、服务名称、将使用终端节点的子网以及要与终端节点网络接口关联的安全组。

以下示例创建一个连接到 Elastic Load Balancing 服务的接口终端节点。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface --service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-abababab --security-group-id sg-1a2b3c4d
```

```
{
  "VpcEndpoint": {
    "PolicyDocument": "{\n      \"Statement\": [\n        {\n          \"Action\": \"*\",\n          \"Resource\": \"*\n          \"/\n          \"Effect\": \"Allow\", \"Principal\": \"*\", \"\n          \"/\n          \"VpcId\": \"vpc-ec43eb89\", \"\n          \"NetworkInterfaceIds\": [\n            \"eni-bf8aa46b\"\n          ],\n          \"SubnetIds\": [\n            \"subnet-abababab\"\n          ],\n          \"PrivateDnsEnabled\": true,\n          \"State\": \"pending\", \"\n          \"ServiceName\": \"com.amazonaws.us-east-1.elasticloadbalancing\", \"\n          \"RouteTableIds\": [],\n          \"Groups\": [\n            {\n              \"\n            }\n          ]\n        }\n      ]\n    }"
  }
}
```

```
        "GroupName": "default",
        "GroupId": "sg-1a2b3c4d"
    },
],
"VpcEndpointId": "vpce-088d25a4bbf4a7abc",
"VpcEndpointType": "Interface",
"CreationTimestamp": "2017-09-05T20:14:41.240Z",
"DnsEntries": [
{
    "HostedZoneId": "Z7HUB22UULQXV",
    "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7.elasticloadbalancing.us-
east-1.vpce.amazonaws.com"
},
{
    "HostedZoneId": "Z7HUB22UULQXV",
    "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
},
{
    "HostedZoneId": "Z1K56Z6FNPJRR",
    "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
}
]
}
```

或者，以下示例创建一个连接到另一 AWS 账户中的终端节点服务的接口终端节点（服务提供商将为您提供终端节点服务的名称）。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
--service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-
id subnet-abababab --security-group-id sg-1a2b3c4d
```

在返回的输出中，记录 DnsName 字段。您可以使用这些 DNS 名称访问 AWS 服务。

使用适用于 Windows PowerShell 的 AWS 工具或 API 描述可用服务

- [Get-EC2VpcEndpointService](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcEndpointServices](#) (Amazon EC2 查询 API)

使用适用于 Windows PowerShell 的 AWS 工具或 API 创建 VPC 终端节点

- [New-EC2VpcEndpoint](#) (适用于 Windows PowerShell 的 AWS 工具)
- [CreateVpcEndpoint](#) (Amazon EC2 查询 API)

查看您的接口终端节点

在创建接口终端节点之后，您可以查看有关它的信息。

使用控制台查看有关接口终端节点的信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的接口终端节点。
3. 要查看有关接口终端节点的信息，请选择 Details。DNS Names 字段将显示用于访问服务的 DNS 名称。
4. 要查看已创建接口终端节点的子网以及每个子网中的终端节点网络接口的 ID，请选择 Subnets。

5. 要查看与终端节点网络接口关联的安全组，请选择 Security Groups。

使用 AWS CLI 描述您的接口终端节点

- 您可使用 [describe-vpc-endpoints](#) 命令描述您的终端节点。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 描述您的 VPC 终端节点

- [Get-EC2VpcEndpoint](#) (适用于 Windows PowerShell 的 AWS 工具)
- [DescribeVpcEndpoints](#) (Amazon EC2 查询 API)

为接口终端节点创建和管理通知

您可以创建通知以接收针对您的接口终端节点上发生的特定事件的提醒。例如，您可在服务提供商接受接口终端节点时收到一封电子邮件。要创建通知，您必须将 [Amazon SNS 主题](#) 与通知关联。您可以订阅 SNS 主题以便在终端节点事件发生时收到电子邮件通知。

您用于通知的 Amazon SNS 主题必须具有允许 Amazon 的 VPC 终端节点服务代表您发布通知的主题策略。确保在您的主题策略中包含以下语句。有关更多信息，请参阅 [Amazon Simple Notification Service 开发人员指南](#) 中的[管理至 Amazon SNS 主题的访问](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

为接口终端节点创建通知

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoints 并选择您的接口终端节点。
- 选择 Actions、Create notification。
- 选择要与通知关联的 SNS 主题的 ARN。
- 对于 Events，选择要接收其通知的终端节点事件。
- 选择 Create Notification。

在创建通知后，您可以更改与通知关联的 SNS 主题，也可以为通知指定不同的终端节点事件。

为终端节点服务修改通知

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoints 并选择您的接口终端节点。

3. 选择 Actions、Modify Notification。
4. 指定 SNS 主题的 ARN 并根据要求更改终端节点事件。
5. 选择 Modify Notification。

如果您不再需要某通知，则可删除它。

删除通知

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的接口终端节点。
3. 选择 Actions、Delete notification。
4. 选择 Yes, Delete。

使用 AWS CLI 创建和管理通知

1. 要为接口终端节点创建通知，请使用 `create-vpc-endpoint-connection-notification` 命令并指定 SNS 主题的 ARN、要通知的事件以及终端节点的 ID；例如：

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
```

2. 要查看您的通知，请使用 `describe-vpc-endpoint-connection-notifications` 命令：

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

3. 要更改通知的 SNS 主题或终端节点事件，请使用 `modify-vpc-endpoint-connection-notification` 命令；例如：

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-arn arn:aws:sns:us-east-2:123456789012:mytopic
```

4. 要删除通知，请使用 `delete-vpc-endpoint-connection-notifications` 命令：

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-ids vpce-nfn-008776de7e03f5abc
```

通过接口终端节点访问服务

在创建接口终端节点之后，您可以通过终端节点 URL 将请求提交给支持的服务。您可以使用以下命令：

- 我们为接口终端节点生成的终端节点特定区域 DNS 主机名。主机名在其名称中包含一个唯一终端节点标识符、服务标识符、区域以及 `vpce.amazonaws.com`；例如，`vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com`。
- 我们为终端节点可用的每个可用区生成的终端节点特定区域 DNS 主机名。主机名在其名称中包含可用区；例如，`vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com`。如果架构隔离可用区（例如，为了故障遏制或降低区域数据传输费用），可使用此选项。

Note

对区域 DNS 主机名的请求将流至服务提供商账户中的相应可用区位置（可能没有与您的账户相同的可用区名称）。有关更多信息，请参阅[区域和可用区域概念](#)。

- 如果您为终端节点启用了私有 DNS（私有托管区域；仅适用于 AWS 服务和 AWS Marketplace 合作伙伴服务），则为区域的 AWS 服务的默认 DNS 主机名，例如 `ec2.us-east-1.amazonaws.com`。
- VPC 中的终端节点网络接口的私有 IP 地址。

例如，在您已具有连接到 Elastic Load Balancing 的接口终端节点且您尚未为其启用私有 DNS 选项的子网中，通过一个实例使用以下 AWS CLI 命令来描述您的负载均衡器。此命令将使用终端节点特定区域 DNS 主机名来使用接口终端节点发出请求：

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

如果您启用私有 DNS 选项，则不必在请求中指定终端节点 URL。AWS CLI 将使用区域 (`elasticloadbalancing.us-east-1.amazonaws.com`) 的 AWS 服务的默认终端节点。

修改接口终端节点

您可以通过更改接口终端节点所在的子网，更改与终端节点网络接口关联的安全组并修改标签，来修改接口终端节点。如果您删除接口终端节点的子网，则将删除子网中相应的终端节点网络接口。

更改接口终端节点的子网

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoints 并选择接口终端节点。
- 选择 Actions、Manage Subnets。
- 根据要求选择或取消选择子网，然后选择 Modify Subnets。

添加或删除与接口终端节点关联的安全组

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoints 并选择接口终端节点。
- 选择 Actions、Manage security groups。
- 根据要求选择或取消选择安全组，然后选择 保存。

添加或删除接口终端节点标签

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择终端节点。
- 选择接口终端节点，然后选择操作、添加/编辑标签。
- 添加或删除标签。

[添加标签] 选择创建标签，然后执行以下操作：

- 对于键，输入键名称。
- 对于值，输入键值。

[删除标签] 选择标签的键和值右侧的删除按钮 ("x")。

使用 AWS CLI 修改 VPC 终端节点

- 使用 `describe-vpc-endpoints` 命令获取您的接口终端节点的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 以下示例使用 [modify-vpc-endpoint](#) 命令将子网 subnet-aabb1122 添加到接口终端节点。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-id subnet-aabb1122
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 修改 VPC 终端节点

- [Edit-EC2VpcEndpoint](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ModifyVpcEndpoint](#) (Amazon EC2 查询 API)

使用 适用于 Windows PowerShell 的 AWS 工具 或 API 添加或删除 VPC 终端节点 标签

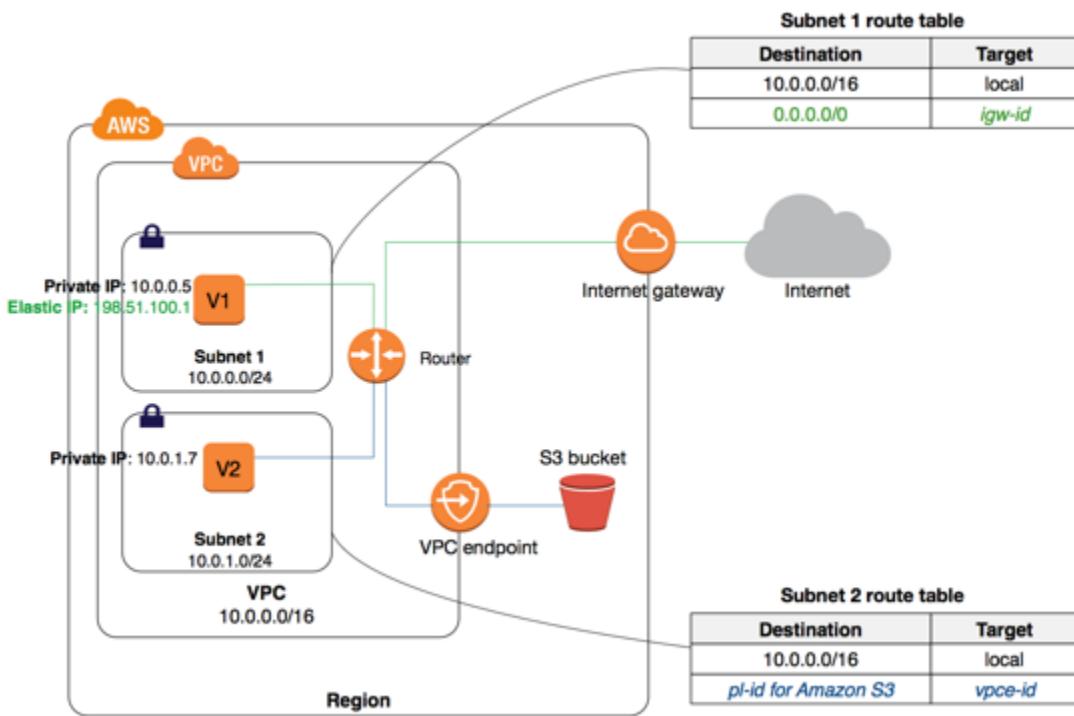
- [tag-resource](#) (AWS CLI)
- [TagResource](#) (适用于 Windows PowerShell 的 AWS 工具)
- [untag-resource](#) (AWS CLI)
- [TagResource](#) (适用于 Windows PowerShell 的 AWS 工具)

网关 VPC 终端节点

要创建和设置网关终端节点，请执行以下常规步骤：

1. 指定要在其中创建终端节点的 VPC 以及要连接到的服务。服务由前缀列表（即某个区域的服务的名称和 ID）标识。前缀列表 ID 使用 p1-xxxxxxx 格式，前缀列表名称使用“com.amazonaws.*region.service*”格式。使用前缀列表名称（服务名称）创建终端节点。
2. 向终端节点连接终端节点策略，该策略允许您对要连接的部分或所有服务进行访问。有关更多信息，请参阅[使用 VPC 终端节点策略 \(p. 262\)](#)。
3. 指定一个或多个路由表，在其中创建到服务的路由。路由表将控制 VPC 与其他服务之间的流量的路由。与其中任一路由表相关联的每个子网都可以访问终端节点，随后通过终端节点将来自这些子网实例的流量路由到服务。

在下图中，子网 2 中的实例可通过网关终端节点访问 Amazon S3。



您可以在单个 VPC 中创建多个终端节点 (例如，针对多项服务)。您还可以为单项服务创建多个终端节点，并使用不同的路由表通过同一服务的多个子网强制执行不同的访问策略。

创建终端节点后，您可以修改已连接到终端节点的终端节点策略，并添加或删除终端节点使用的路由表。

使用网关终端节点不会发生任何额外费用。采用标准的数据传输和资源使用计费方式。有关定价的更多信息，请参阅 [Amazon EC2 定价](#)。

目录

- [网关终端节点路由 \(p. 250\)](#)
- [网关终端节点限制 \(p. 252\)](#)
- [Amazon S3 的终端节点 \(p. 253\)](#)
- [Amazon DynamoDB 的终端节点 \(p. 257\)](#)
- [创建网关终端节点 \(p. 259\)](#)
- [修改您的安全组 \(p. 260\)](#)
- [修改网关终端节点 \(p. 261\)](#)
- [添加或删除网关终端节点标签 \(p. 261\)](#)

网关终端节点路由

在创建或修改终端节点时，您将指定用于通过终端节点访问服务的 VPC 路由表。路由会自动添加到每个路由表中，同时会添加一个指定服务的前缀列表 ID 的目的地 (pl-xxxxxxxx) 以及一个具有终端节点 ID 的目标 (vpce-xxxxxxxx)；例如：

目的地	目标
10.0.0.0/16	本地

目的地	目标
pl-1a2b3c4d	vpce-11bb22cc

前缀列表 ID 从逻辑上代表服务使用的公有 IP 地址的范围。与指定路由表关联的子网中的所有实例都会自动使用终端节点访问服务；未与指定路由表关联的子网不使用终端节点。这使您能够将其他子网中的资源与您的终端节点分离。

要查看服务的当前公有 IP 地址范围，您可以使用 [describe-prefix-lists](#) 命令 中的 [AWS IP 地址范围](#)。

Note

服务的公有 IP 地址的范围可能会不时更改。在根据服务的当前 IP 地址范围决定路由目标或做其他决策之前，请考虑产生的影响。

以下规则适用：

- 您可以在一个路由表中拥有针对不同服务的多个终端节点路由，也可以在不同的路由表中拥有针对同一服务的多个终端节点路由，但不能在一个路由表中拥有针对同一服务的多个终端节点路由。例如，如果您在 VPC 中创建了两个针对 Amazon S3 的终端节点，则您不能在同一路由表中同时为这两个终端节点创建终端节点路由。
- 您无法通过使用路由表 API 或 Amazon VPC 控制台中的“路由表”页面来在您的路由表中显式添加、修改或删除终端节点路由。您只能通过将路由表与终端节点关联来添加终端节点路由。要更改与终端节点关联的路由表，您可以[修改终端节点 \(p. 261\)](#)。
- 在您从终端节点删除路由表关联（通过修改终端节点）或删除终端节点时，将自动删除终端节点路由。

我们使用与流量匹配的最明确路由以判断数据流的路由方式（最长前缀匹配）。如果您的路由表中有针对指向 Internet 网关的所有 Internet 流量（`0.0.0.0/0`）的现有路由，则终端节点路由将优先于目标设定为服务的所有流量，因为服务的 IP 地址范围比 `0.0.0.0/0` 更具体。所有其他 Internet 流量（包括目标设定为其他区域内的服务的流量）将流向 Internet 网关。

但是，如果您有针对指向 Internet 网关或 NAT 设备的 IP 地址范围的现有、更具体的路由，则这些路由将优先。如果您有目标设定为与服务所使用的 IP 地址范围相同的 IP 地址范围的现有路由，则您的路由将优先。

示例：路由表中的终端节点路由

在此方案中，您的路由表中有一个针对指向 Internet 网关的所有 Internet 流量（`0.0.0.0/0`）的现有路由。来自子网的目标设定为其他 AWS 服务的任何流量将使用 Internet 网关。

目的地	目标
<code>10.0.0.0/16</code>	本地
<code>0.0.0.0/0</code>	<code>igw-1a2b3c4d</code>

创建指向支持的 AWS 服务的终端节点，并将您的路由表与该终端节点关联。将为路由表自动添加一个终端节点路由，其目的地为 `pl-1a2b3c4d`（假设这表示您已为其创建终端节点的服务）。现在，来自子网的目标设定为同一区域内的 AWS 服务的任何流量将流向该终端节点，而不是流向 Internet 网关。所有其他 Internet 流量（包括目标设定为其他服务的流量和目标设定为其他区域内的 AWS 服务的流量）将流向 Internet 网关。

目的地	目标
<code>10.0.0.0/16</code>	本地
<code>0.0.0.0/0</code>	<code>igw-1a2b3c4d</code>

目的地	目标
pl-1a2b3c4d	vpce-11bb22cc

示例：针对终端节点调整路由表

在此方案中，您已将路由表配置为允许子网中的实例通过 Internet 网关与 Amazon S3 存储桶进行通信。您已添加一个目的地为 54.123.165.0/24（假设这是 Amazon S3 中的当前 IP 地址范围）且目标为 Internet 网关的路由。然后创建一个终端节点，并将此路由表与该终端节点关联。这会自动将一个终端节点路由添加到路由表。然后使用 [describe-prefix-lists](#) 命令查看 Amazon S3 的 IP 地址范围。该范围为 54.123.160.0/19（它没有指向 Internet 网关的范围那么具体）。这意味着，目标设定为 54.123.165.0/24 IP 地址范围的任何流量将继续使用 Internet 网关，而不使用终端节点（前提是这仍是 Amazon S3 的公有 IP 地址范围）。

目的地	目标
10.0.0.0/16	本地
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

要确保通过终端节点来路由目标设定为相同区域内的 Amazon S3 的所有流量，您必须调整路由表中的路由。为此，您可以删除针对 Internet 网关的路由。现在，针对相同区域内的 Amazon S3 的所有流量将使用终端节点，并且与您的路由表关联的子网为私有子网。

目的地	目标
10.0.0.0/16	本地
pl-1a2b3c4d	vpce-11bb22cc

网关终端节点限制

要使用网关终端节点，您需要了解当前限制：

- 您无法在网络 ACL 的出站规则中使用前缀列表 ID 来允许或拒绝至终端节点中所指定服务的出站流量。如果您的网络 ACL 规则限制流量，则必须为服务指定 CIDR 块（IP 地址范围）。但是，您可在出站安全组规则中使用前缀列表 ID。有关更多信息，请参阅[安全组 \(p. 263\)](#)。
- 仅在同一地区内支持终端节点。无法在 VPC 和其他区域内的服务之间创建终端节点。
- 无法标记终端节点。
- 终端节点仅支持 IPv4 流量。
- 无法将终端节点从一个 VPC 转移到另一个 VPC，也无法将终端节点从一项服务转移到另一项服务。
- 您可以为每个 VPC 创建的终端节点的数量有限制。有关更多信息，请参阅[VPC 终端节点 \(p. 279\)](#)。
- 无法将终端节点连接扩展到 VPC 之外。VPC 中的 VPN 连接、VPC 对等连接、AWS Direct Connect 连接或 ClassicLink 连接的另一端的资源不能使用终端节点与终端节点服务中的资源进行通信。
- 您必须在您的 VPC 中启用 DNS 解析，或者，如果您使用自己的 DNS 服务器，请确保将针对所需服务（如 Amazon S3）的 DNS 请求正确解析为 AWS 维护的 IP 地址。有关更多信息，请参阅 Amazon Web Services 一般参考 中的 [在您的 VPC 中使用 DNS \(p. 228\)](#) 和 [AWS IP 地址范围](#)。

有关特定于 Amazon S3 的规则和限制的更多信息，请参阅 [Amazon S3 的终端节点 \(p. 253\)](#)。

有关特定于 DynamoDB 的规则和限制的更多信息，请参阅 [Amazon DynamoDB 的终端节点 \(p. 257\)](#)。

Amazon S3 的终端节点

如果您已设置从 VPC 访问 Amazon S3 资源的权限，则在您设置终端节点后可继续使用 Amazon S3 DNS 名称来访问这些资源。但请注意以下几点：

- 您的终端节点具有可控制使用终端节点访问 Amazon S3 资源的策略。默认策略允许 VPC 中的任何用户或服务使用来自任何 AWS 账户的凭证访问任何 Amazon S3 资源；包括与 VPC 关联的账户之外的其他 AWS 账户的 Amazon S3 资源。有关更多信息，请参阅[使用 VPC 终端节点 控制对服务的访问 \(p. 262\)](#)。
- Amazon S3 从受影响子网的实例收到的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。终端节点将切换网络路由，并断开打开的 TCP 连接。您的任务在转换期间将被中断，并且之前的任何使用公有 IPv4 地址的连接将不会恢复。建议您在创建或修改终端节点时不要运行任何重要任务；或进行测试以确保您的软件在连接中断后可自动重新连接到 Amazon S3。
- 您不能使用 IAM 策略或存储桶策略允许从 VPC IPv4 CIDR 范围（私有 IPv4 地址范围）进行访问。VPC CIDR 块可能重叠或相同，这可能会导致意外结果。因此，对于通过 VPC 终端节点向 Amazon S3 发出的请求，无法在 IAM 策略中使用 `aws:SourceIp` 条件。这适用于用户和角色的 IAM 策略以及任何存储桶策略。如果语句包含 `aws:SourceIp` 条件，则该值不与任何提供的 IP 地址或范围匹配。您可以改而执行以下操作：
 - 使用路由表来控制哪些实例可以通过终端节点访问 Amazon S3 中的资源。
 - 对于存储桶策略，您可以限制对特定终端节点或特定 VPC 的访问。有关更多信息，请参阅[使用 Amazon S3 存储桶策略 \(p. 256\)](#)。
- 终端节点当前不支持跨区域请求 — 确保在您的存储桶所在的区域内创建终端节点。您可以使用 Amazon S3 控制台或 `get-bucket-location` 命令来查找存储桶的位置。使用区域特定的 Amazon S3 终端节点访问存储桶；例如，`mybucket.s3-us-west-2.amazonaws.com`。有关 Amazon S3 的区域特定的终端节点的更多信息，请参阅 Amazon Web Services 一般参考 中的 [Amazon Simple Storage Service \(S3\)](#)。如果您使用 AWS CLI 向 Amazon S3 发起请求，请将默认区域设置为您的存储桶所在的区域，或在请求中使用 `--region` 参数。

Note

将 Amazon S3 的美国标准区域视为已映射到 `us-east-1` 区域。

- 终端节点目前只支持 IPv4 流量。

在对 Amazon S3 使用终端节点之前，确保您已阅读下面的一般限制：[网关终端节点限制 \(p. 252\)](#)。有关创建和查看 S3 存储桶的信息，请参阅 Amazon Simple Storage Service 控制台用户指南 中的 [如何创建 S3 存储桶](#) 和 [如何查看 S3 存储桶的属性](#)。

如果您在 VPC 中使用其他 AWS 服务，它们可能会对特定任务使用 S3 存储桶。确保终端节点策略允许对 Amazon S3 进行完全访问（默认策略），或允许对这些服务所使用的特定存储桶进行访问。或者，仅在未由这些服务中的任一服务使用的子网中创建终端节点，以允许这些服务继续使用公有 IP 地址访问 S3 存储桶。

下表列出了可能受终端节点影响的 AWS 服务，以及每项服务的任何具体信息。

AWS 服务	注意
Amazon AppStream 2.0	您的终端节点策略必须允许访问 AppStream 2.0 用于存储用户内容的特定存储桶。有关更多信息，请参阅 Amazon AppStream 2.0 管理指南 中的 主文件夹 和 VPC 终端节点 。
AWS CloudFormation	如果您的 VPC 中的资源必须响应等待条件或自定义资源请求，则您的终端节点策略必须至少允许对这些资源所使用的特定存储桶的访问。有关更多信

AWS 服务	注意
	息，请参阅 AWS CloudFormation 和 VPC 终端节点 。
CodeDeploy	您的终端节点策略必须允许对 Amazon S3 进行完全访问，或允许对您已为 CodeDeploy 部署创建的任何 S3 存储桶进行访问。
Elastic Beanstalk	您的终端节点策略必须至少允许对用于 Elastic Beanstalk 应用程序的任何 S3 存储桶进行访问。有关更多信息，请参阅 AWS Elastic Beanstalk 开发人员指南中的 将 Elastic Beanstalk 与 Amazon S3 配合使用 。
AWS OpsWorks	您的终端节点策略必须至少允许对 AWS OpsWorks 使用的特定存储桶进行访问。有关更多信息，请参阅 AWS OpsWorks 用户指南 中的 在 VPC 中运行堆栈 。
AWS Systems Manager	您的终端节点策略必须允许访问补丁管理器用于在您的 AWS 区域中执行补丁基准操作的 Amazon S3 存储桶。这些存储桶包含由补丁基准服务检索并在实例上运行的代码。有关更多信息，请参阅 AWS Systems Manager 用户指南 中的 为 Systems Manager 设置 VPC 终端节点 。 有关 SSM 代理执行操作所需的 S3 存储桶权限的列表，请参阅 AWS Systems Manager 用户指南 中的 SSM 代理的最低 S3 存储桶权限 。
Amazon Elastic Container Registry	您的终端节点策略必须允许访问 Amazon ECR 用于存储 Docker 镜像层的 Amazon S3 存储桶。有关更多信息，请参阅 Amazon Elastic Container Registry 用户指南 中的 接口 VPC 终端节点 (AWS PrivateLink) 。
Amazon WorkDocs	如果您在 Amazon WorkSpaces 或 EC2 实例中使用 Amazon WorkDocs 客户端，则您的终端节点策略必须允许对 Amazon S3 进行完全访问。
Amazon WorkSpaces	Amazon WorkSpaces 不直接取决于 Amazon S3。但如果您向 Amazon WorkSpaces 用户提供 Internet 访问权，则请记住，来自其他公司的网站、HTML 电子邮件和 Internet 服务可能取决于 Amazon S3。确保您的终端节点策略允许对 Amazon S3 进行完全访问，以便这些服务能够继续正常运行。

您的 VPC 和 S3 存储桶之间的流量不会脱离 Amazon 网络。

对 Amazon S3 使用终端节点策略

下面是访问 Amazon S3 的终端节点策略示例。有关更多信息，请参阅[使用 VPC 终端节点 策略 \(p. 262\)](#)。由用户决定满足业务需求的策略限制。例如，您可以指定区域（“`packages.us-west-1.amazonaws.com`”）避免 S3 存储桶名称混淆。

Important

所有类型的策略（包括 IAM 用户策略、终端节点策略、S3 存储桶策略和 Amazon S3 ACL 策略（如果有））都必须授予必要权限以便成功访问 Amazon S3。

Example 示例：限制对特定存储桶的访问

您可以创建一个策略来仅允许访问特定 S3 存储桶。如果您的 VPC 中有使用 S3 存储桶的其他 AWS 服务，这会非常有用。以下是仅允许访问 my_secure_bucket 的策略的示例。

```
{  
    "Statement": [  
        {  
            "Sid": "Access-to-specific-bucket-only",  
            "Principal": "*",  
            "Action": [  
                "s3:GetObject",  
                "s3:PutObject"  
            ],  
            "Effect": "Allow",  
            "Resource": ["arn:aws:s3:::my_secure_bucket",  
                        "arn:aws:s3:::my_secure_bucket/*"]  
        }  
    ]  
}
```

Example 示例：允许对 Amazon Linux AMI 存储库的访问

每个区域中的 Amazon Linux AMI 存储库都是 Amazon S3 存储桶。如果您希望 VPC 中的实例通过终端节点访问该存储库，请创建终端节点策略以允许对这些存储桶进行访问。

以下策略授予对 Amazon Linux 存储库的访问权限。

```
{  
    "Statement": [  
        {  
            "Sid": "AmazonLinuxAMIRepositoryAccess",  
            "Principal": "*",  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::packages.*.amazonaws.com/*",  
                "arn:aws:s3:::repo.*.amazonaws.com/*"  
            ]  
        }  
    ]  
}
```

以下策略授予对 Amazon Linux 2 存储库的访问权限。

```
{  
    "Statement": [  
        {  
            "Sid": "AmazonLinux2AMIRepositoryAccess",  
            "Principal": "*",  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::amazonlinux2-repos.*.amazonaws.com/*"  
            ]  
        }  
    ]  
}
```

```
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
}
```

使用 Amazon S3 存储桶策略

您可以使用存储桶策略来控制从特定终端节点或特定 VPC 对存储桶的访问。

对于通过 VPC 终端节点向 Amazon S3 发出的请求，无法在存储桶策略中使用 `aws:SourceIp` 条件。此条件未匹配任何指定的 IP 地址或 IP 地址范围，如果您向 Amazon S3 存储桶发出请求，可能不会有预期的效果。例如：

- 您的存储桶策略具有 `Deny` 效果和 `NotIpAddress` 条件，即仅从单个 IP 地址或有限 IP 地址范围获得访问权。对于通过终端节点向存储桶发出的请求，始终匹配 `NotIpAddress` 条件，并且语句的效果适用（假定策略中的其他限制匹配）。对存储桶的访问被拒绝。
- 您的存储桶策略具有 `Deny` 效果和 `IpAddress` 条件，即仅拒绝对单个 IP 地址或有限 IP 地址范围的访问。对于通过终端节点向存储桶发出的请求，条件不匹配，并且语句不适用。假定有其他语句允许在无 `IpAddress` 条件时访问，则允许对存储桶的访问。

请改为调整存储桶策略以限制对特定 VPC 或特定终端节点的访问。

有关 Amazon S3 的存储桶策略的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的[使用存储桶策略和用户策略](#)。

Example 示例：限制对特定终端节点的访问

下面是一个仅允许从终端节点 `vpce-1a2b3c4d` 访问特定存储桶 `my_secure_bucket` 的 S3 存储桶策略的示例。如果未使用指定的终端节点，则该策略拒绝对存储桶的所有访问。`aws:sourceVpce` 条件用于指定终端节点。`aws:sourceVpce` 条件不需要 VPC 终端节点资源的 ARN，而只需要终端节点 ID。

```
{
    "Version": "2012-10-17",
    "Id": "Policy1415115909152",
    "Statement": [
        {
            "Sid": "Access-to-specific-VPCE-only",
            "Principal": "*",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": ["arn:aws:s3:::my_secure_bucket",
                        "arn:aws:s3:::my_secure_bucket/*"],
            "Condition": {
                "StringNotEquals": {
                    "aws:sourceVpce": "vpce-1a2b3c4d"
                }
            }
        }
    ]
}
```

Example 示例：限制对特定 VPC 的访问

可以使用 `aws:sourceVpc` 条件来创建用于限制对特定 VPC 的访问的存储桶策略。如果您在同一 VPC 中配置了多个终端节点，并且您希望管理对所有终端节点的 S3 存储桶的访问，这会非常有用。下面是允许 VPC

vpc-111bbb22 访问 my_secure_bucket 及其对象的策略的示例。如果未使用指定的 VPC，则该策略拒绝对存储桶的所有访问。aws:sourceVpc 条件不需要 VPC 资源的 ARN，而只需要 VPC ID。

```
{  
    "Version": "2012-10-17",  
    "Id": "Policy1415115909152",  
    "Statement": [  
        {  
            "Sid": "Access-to-specific-VPC-only",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Effect": "Deny",  
            "Resource": ["arn:aws:s3:::my_secure_bucket",  
                        "arn:aws:s3:::my_secure_bucket/*"],  
            "Condition": {  
                "StringNotEquals": {  
                    "aws:sourceVpc": "vpc-111bbb22"  
                }  
            }  
        }  
    ]  
}
```

Amazon DynamoDB 的终端节点

如果您已设置从 VPC 访问 DynamoDB 表，则您可以继续访问这些表，如同您在设置终端节点后通常访问一样。但请注意以下几点：

- 您的终端节点具有可控制使用终端节点访问 DynamoDB 资源的策略。默认策略允许 VPC 内的任何用户或服务使用任何 AWS 账户中的凭证访问任何 DynamoDB 资源。有关更多信息，请参阅[使用 VPC 终端节点控制对服务的访问 \(p. 262\)](#)。
- DynamoDB 不支持基于资源的策略（例如，针对表）。对 DynamoDB 的访问权限通过各个 IAM 用户和角色的终端节点策略和 IAM 策略进行控制。
- 您无法通过 VPC 终端节点访问 Amazon DynamoDB Streams。
- 终端节点当前不支持跨区域请求 – 确保在您的 DynamoDB 表所在的区域内创建终端节点。
- 如果使用 AWS CloudTrail 记录 DynamoDB 操作，则日志文件包含 VPC 中的 EC2 实例的私有 IP 地址和通过终端节点执行的任何操作的终端节点 ID。
- 您的受影响子网中实例的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。终端节点将切换网络路由，并断开打开的 TCP 连接。您的任务在转换期间将被中断，并且之前的任何使用公有 IPv4 地址的连接将不会恢复。建议您在创建或修改终端节点时不要运行任何重要任务；或进行测试以确保您的软件在连接中断后可自动重新连接到 DynamoDB。

在对 DynamoDB 使用终端节点之前，确保您已阅读下面的一般限制：[网关终端节点限制 \(p. 252\)](#)。

对 DynamoDB 使用终端节点策略

下面是访问 DynamoDB 的终端节点策略示例。

Important

所有类型的策略（包括 IAM 用户策略和终端节点策略）都必须授予必要权限以便成功访问 DynamoDB。

Example 示例：只读访问权限

您可以创建通过 VPC 终端节点将操作限制为仅列出和描述 DynamoDB 表的策略。

```
{  
    "Statement": [  
        {  
            "Sid": "ReadOnly",  
            "Principal": "*",  
            "Action": [  
                "dynamodb:DescribeTable",  
                "dynamodb>ListTables"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

Example 示例：限制对特定表的访问权限

您可以创建限制对特定 DynamoDB 表的访问权限的策略。在此示例中，终端节点策略仅允许访问 StockTable。

```
{  
    "Statement": [  
        {  
            "Sid": "AccessToSpecificTable",  
            "Principal": "*",  
            "Action": [  
                "dynamodb:Batch*",  
                "dynamodb>Delete*",  
                "dynamodb:DescribeTable",  
                "dynamodb:GetItem",  
                "dynamodb:PutItem",  
                "dynamodb:Update*"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"  
        }  
    ]  
}
```

使用 IAM 策略控制对 DynamoDB 的访问权限

您可以为 IAM 用户、组或角色创建限制仅从特定 VPC 终端节点访问 DynamoDB 表的 IAM 策略。为此，您可以使用 IAM 策略中表资源的 `aws:sourceVpce` 条件键。

有关管理对 DynamoDB 的访问权限的更多信息，请参阅 Amazon DynamoDB 开发人员指南 中的 [Amazon DynamoDB 的身份验证和访问控制](#)。

Example 示例：限制从特定终端节点的访问

在此示例中，用户没有使用 DynamoDB 表的权限，除非通过终端节点 `vpce-11aa22bb` 进行访问。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AccessFromSpecificEndpoint",  
            "Action": "dynamodb:*",  
            "Effect": "Deny",  
            "Resource": "arn:aws:dynamodb:region:account-id:table/*",  
            "Condition": { "StringNotEquals" : { "aws:sourceVpce": "vpce-11aa22bb" } }  
        }  
    ]  
}
```

```
        ]  
    }
```

创建网关终端节点

要创建终端节点，您必须指定要在其中创建终端节点的 VPC 和要连接到的服务。

使用控制台创建网关终端节点

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service Name，请选择要连接到的服务。要创建连接到 DynamoDB 或 Amazon S3 的网关终端节点，请确保类型列指示网关。
4. 填写以下信息，然后选择 Create endpoint。
 - 对于 VPC，选择要在其中创建终端节点的 VPC。
 - 对于 Configure route tables，选择终端节点要使用的路由表。我们将自动向选定的路由表添加一个路由，以将目标设定为服务的流量指向终端节点。
 - 对于 Policy，选择策略的类型。您可以保留默认选项 Full Access 来允许对服务进行完全访问。或者，您可以选择 Custom，然后使用 AWS 策略生成器创建自定义策略，或在策略窗口中键入您自己的策略。

在创建终端节点之后，您可以查看有关它的信息。

使用控制台查看有关网关终端节点的信息

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 要查看有关终端节点的信息，请选择 Summary。您可以获取 Service 框中的服务的前缀列表名称。
4. 要查看有关终端节点所使用的路由表的信息，请选择 Route Tables。
5. 要查看连接到终端节点的 IAM 策略，请选择策略。

Note

Policy 选项卡仅显示终端节点策略。它不会为有权使用终端节点的 IAM 用户显示有关 IAM 策略的任何信息，也不会显示服务特定的策略；例如，S3 存储桶策略。

使用 AWS CLI 创建和查看终端节点

1. 使用 `describe-vpc-endpoint-services` 命令获取可用服务的列表。在返回的输出中，记录要连接到的服务的名称。serviceType 字段指示是通过接口终端节点还是网关终端节点连接到服务。

```
aws ec2 describe-vpc-endpoint-services
```

```
{  
    "serviceDetailSet": [  
        {  
            "serviceType": [  
                {  
                    "serviceType": "Gateway"  
                }  
            ...  
        }  
    ]  
}
```

- 要创建网关终端节点（例如，连接到 Amazon S3 的网关终端节点），请使用 `create-vpc-endpoint` 命令并指定 VPC ID、服务名称和将使用终端节点的路由表。(可选) 您可以使用 `--policy-document` 参数指定自定义策略来控制对服务的访问。如果未使用参数，我们将连接一个允许完全访问服务的默认策略。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-east-1.s3 --route-table-ids rtb-11aa22bb
```

- 使用 `describe-vpc-endpoints` 命令描述您的终端节点。

```
aws ec2 describe-vpc-endpoints
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 描述可用服务

- `Get-EC2VpcEndpointService` (适用于 Windows PowerShell 的 AWS 工具)
- `DescribeVpcEndpointServices` (Amazon EC2 查询 API)

使用适用于 Windows PowerShell 的 AWS 工具或 API 创建 VPC 终端节点

- `New-EC2VpcEndpoint` (适用于 Windows PowerShell 的 AWS 工具)
- `CreateVpcEndpoint` (Amazon EC2 查询 API)

使用适用于 Windows PowerShell 的 AWS 工具或 API 描述您的 VPC 终端节点

- `Get-EC2VpcEndpoint` (适用于 Windows PowerShell 的 AWS 工具)
- `DescribeVpcEndpoints` (Amazon EC2 查询 API)

修改您的安全组

如果与您的实例关联的 VPC 安全组限制出站流量，则您必须添加一条规则来允许目标设定为 AWS 服务的流量离开您的实例。

为网关终端节点添加出站规则

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Security Groups。
- 选择您的 VPC 安全组，选择 Outbound Rules 选项卡，然后选择 Edit。
- 从 Type 列表中选择流量类型，并输入端口范围 (如果需要)。例如，如果您使用实例从 Amazon S3 中检索对象，请从 Type 列表中选择 HTTPS。
- Destination 列表显示可用的 AWS 服务的前缀列表 ID 和名称。选择 AWS 服务的前缀列表 ID，或键入此 ID。
- 选择 Save。

有关安全组的更多信息，请参阅 [您的 VPC 的安全组 \(p. 119\)](#)。

使用命令行或 API 获取 AWS 服务的前缀列表名称、ID 和 IP 地址范围

- `describe-prefix-lists` (AWS CLI)
- `Get-EC2PrefixList` (适用于 Windows PowerShell 的 AWS 工具)
- `DescribePrefixLists` (Amazon EC2 查询 API)

修改网关终端节点

您可以通过更改或删除网关终端节点的策略并添加或删除终端节点所使用的路由表来修改网关终端节点。

更改与网关终端节点关联的策略

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择 Actions、Edit policy。
4. 您可以选择 Full Access 来允许完全访问。或者，选择 Custom，然后使用 AWS 策略生成器创建自定义策略，或在策略窗口中键入您自己的策略。完成此操作后，选择 Save。

Note

策略更改可能需要几分钟才能生效。

添加或删除网关终端节点所使用的路由表

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择 Actions、Manage route tables。
4. 选择或取消选择所需的路由表，然后选择 Modify Route Tables (修改路由表)。

使用 AWS CLI 修改网关终端节点

1. 使用 `describe-vpc-endpoints` 命令获取您的网关终端节点的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 以下示例使用 `modify-vpc-endpoint` 命令将路由表 `rtb-aaa222bb` 与网关终端节点关联，然后重置策略文档。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 修改 VPC 终端节点

- `Edit-EC2VpcEndpoint` (适用于 Windows PowerShell 的 AWS 工具)
- `ModifyVpcEndpoint` (Amazon EC2 查询 API)

添加或删除网关终端节点标签

标签提供一种标识网关终端节点的方法。您可以添加或删除标签。

添加或删除网关终端节点标签

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择终端节点。
3. 选择网关终端节点，然后选择操作、添加/编辑标签。
4. 添加或删除标签。

[添加标签] 选择创建标签，然后执行以下操作：

- 对于键，输入键名称。
- 对于值，输入键值。

[删除标签] 选择标签的键和值右侧的删除按钮 ("x")。

To add or remove a tag using the 适用于 Windows PowerShell 的 AWS 工具 or an API

- [create-tags](#) (AWS CLI)
- [CreateTags](#) (适用于 Windows PowerShell 的 AWS 工具)
- [delete-tags](#) (AWS CLI)
- [DeleteTags](#) (适用于 Windows PowerShell 的 AWS 工具)

使用 VPC 终端节点 控制对服务的访问

在创建终端节点时，您可为其连接终端节点策略来控制对连接到的服务的访问。终端节点策略必须采用 JSON 格式编写。

如果您使用针对 Amazon S3 的终端节点，则还可以使用 Amazon S3 存储桶策略来控制从特定终端节点或特定 VPC 对存储桶进行的访问。有关更多信息，请参阅 [使用 Amazon S3 存储桶策略 \(p. 256\)](#)。

目录

- [使用 VPC 终端节点 策略 \(p. 262\)](#)
- [安全组 \(p. 263\)](#)

使用 VPC 终端节点 策略

VPC 终端节点策略是一种 IAM 资源策略，您在创建或修改终端节点时可将它连接到终端节点。如果您在创建终端节点时不连接策略，我们将为您连接一个默认策略来允许对服务进行完全访问。终端节点策略不会覆盖或取代 IAM 用户策略或服务特定策略（如 S3 存储桶策略）。它是一个单独策略，用于控制从终端节点对指定服务进行的访问。

您不能将多个策略附加到一个终端节点；但您可以随时修改策略。请注意，如果您修改策略，则所做的更改可能需要几分钟才能生效。有关编写策略的更多信息，请参阅 IAM 用户指南 中的 [IAM 策略概述](#)。

您的终端节点策略可与任何 IAM 策略类似；但请注意以下几点：

- 仅与指定服务相关的策略部分将适用。不能使用终端节点策略来允许 VPC 中的资源执行其他操作；例如，如果您将 EC2 操作添加到针对 Amazon S3 的终端节点的终端节点策略，则这些操作将不会生效。
- 您的策略必须包含一个 [Principal](#) 元素。对于网关终端节点，如果您以格式 "AWS": "[AWS-account-ID](#)" 或 "AWS": "arn:aws:iam::[AWS-account-ID](#):root" 指定委托人，则只会向 AWS 账户根用户授予访问权限，而不是该账户的所有 IAM 用户和角色。
- 终端节点策略的大小不得超过 20480 个字符（包含空格）。

以下服务支持终端节点策略：

- [Amazon API Gateway](#)
- [Amazon CloudWatch](#)
- [Amazon CloudWatch Events](#)
- [Amazon CloudWatch Logs](#)
- [AWS CodeBuild](#)
- [AWS CodeCommit](#)

- Elastic Load Balancing
- Amazon Kinesis Data Firehose
- Amazon SageMaker 和 Amazon SageMaker 运行时
- Amazon SageMaker 笔记本实例
- AWS Secrets Manager
- AWS Security Token Service
- Amazon SNS
- Amazon SQS

有关 Amazon S3 和 DynamoDB 的示例终端节点策略，请参阅以下主题：

- 对 Amazon S3 使用终端节点策略 (p. 254)
- 对 DynamoDB 使用终端节点策略 (p. 257)

安全组

默认情况下，除非您明确限制出站访问，否则 Amazon VPC 安全组将允许所有出站流量。

创建接口终端节点时，您可以将安全组与在您的 VPC 中创建的终端节点网络接口关联。如果您未指定安全组，则您的 VPC 的默认安全组将自动与终端节点网络接口关联。您必须确保安全组的规则允许终端节点网络接口与您的 VPC 中与服务通信的资源进行通信。

对于网关终端节点，如果您的安全组的出站规则受到限制，则必须添加一条规则来允许从 VPC 到终端节点中指定的服务的出站流量。为此，您可以在出站规则中使用该服务的前缀列表 ID 作为目的地。有关更多信息，请参阅 [修改您的安全组 \(p. 260\)](#)。

删除集群VPC 终端节点

如果您不再需要某一终端节点，则可将其删除。删除网关终端节点也会删除终端节点所使用的路由表中的终端节点路由，但不会影响与终端节点所在的 VPC 关联的任何安全组。删除接口终端节点还将删除终端节点网络接口。

删除终端节点

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择 Actions、Delete Endpoint。
4. 在确认屏幕中，选择 Yes, Delete。

删除 VPC 终端节点

- [delete-vpc-endpoints \(AWS CLI\)](#)
- [Remove-EC2VpcEndpoint \(适用于 Windows PowerShell 的 AWS 工具\)](#)
- [DeleteVpcEndpoints \(Amazon EC2 查询 API\)](#)

VPC 终端节点服务 (AWS PrivateLink)

您可以在 VPC 中创建自己的应用程序并将其配置为 AWS PrivateLink 支持的服务（也称作终端节点服务）。其他 AWS 委托人可以使用[接口 VPC 终端节点 \(p. 237\)](#)，在他们的 VPC 和您的终端节点服务之间创建连接。您是服务提供商，而创建与您的服务之间的连接的 AWS 委托人是服务使用者。

目录

- [概述 \(p. 264\)](#)
- [终端节点服务可用区注意事项 \(p. 266\)](#)
- [终端节点服务限制 \(p. 266\)](#)
- [创建 VPC 终端节点服务配置 \(p. 267\)](#)
- [为您的终端节点服务添加和删除权限 \(p. 268\)](#)
- [更改网络负载均衡器和接受设置 \(p. 269\)](#)
- [接受和拒绝接口终端节点连接请求 \(p. 270\)](#)
- [为终端节点服务创建和管理通知 \(p. 271\)](#)
- [对连接信息使用代理协议 \(p. 272\)](#)
- [添加或删除 VPC 终端节点服务标签 \(p. 273\)](#)
- [删除终端节点服务配置 \(p. 273\)](#)

概述

以下是创建终端节点服务的一般步骤。

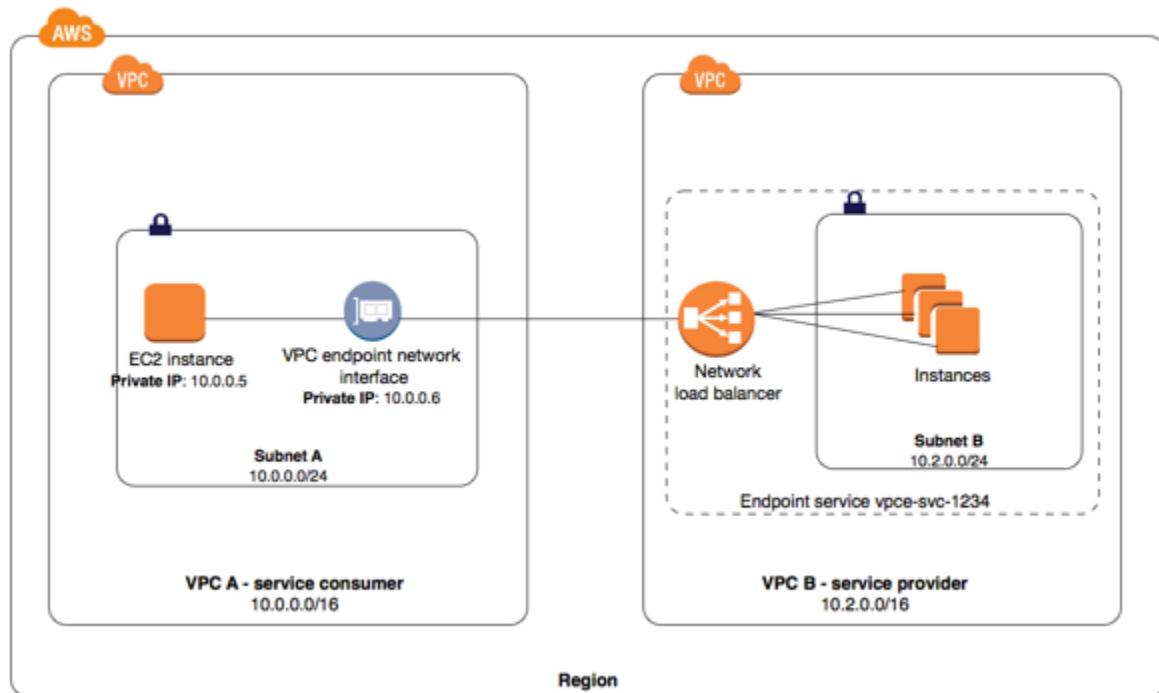
1. 在您的 VPC 中为应用程序创建一个网络负载均衡器，并针对提供服务的每个子网（可用区）对它进行配置。负载均衡器接收来自服务使用者的请求并将请求路由到您的服务。有关更多信息，请参阅 Network Load Balancer 用户指南 中的 [Network Load Balancer 入门](#)。我们建议您在区域内的所有可用区中配置您的服务。
2. 创建 VPC 终端节点服务配置并指定网络负载均衡器。

以下是一些常规步骤，通过这些步骤，服务使用者能够连接到您的服务。

1. 向特定服务用户（AWS 账户、IAM 用户和 IAM 角色）授予权限，允许他们创建与您的终端节点服务之间的连接。
2. 已被授予权限的服务使用者可创建与您的服务连接的接口终端节点（可选择在您已配置服务的每个可用区中创建）。
3. 要激活连接，请接受接口终端节点连接请求。默认情况下，必须手动接受连接请求。不过，您可以配置终端节点服务的接受设置，以便自动接受所有连接请求。

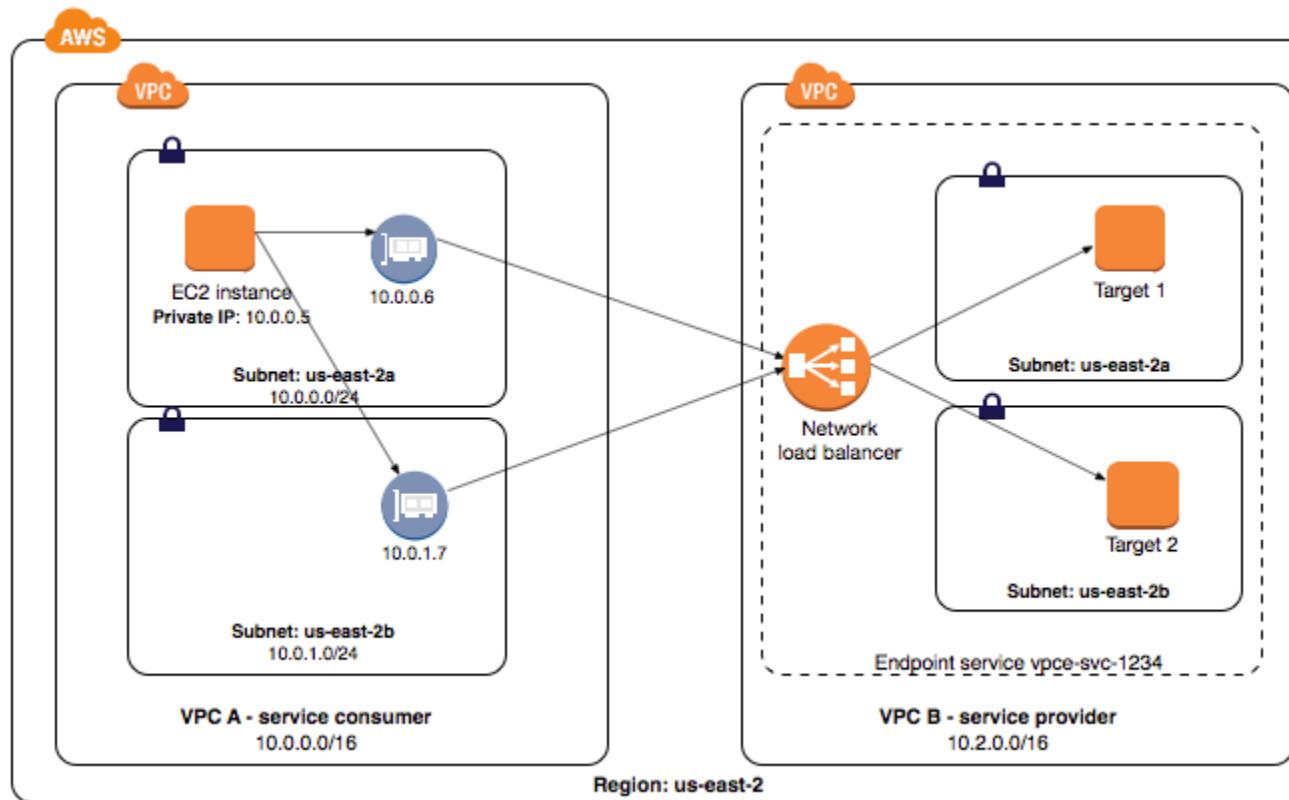
权限和接受设置的组合可帮助您控制哪些服务使用者（AWS 委托人）可以访问您的服务。例如，可以为您信任的选定委托人授予权限，并自动接受所有连接请求；您还可以为范围更广的委托人组授予权限，并手动接受您信任的特定连接请求。

在下图中，VPC B 的账户所有者是一个服务提供商并且有一项服务正在子网 B 的实例上运行。VPC B 的所有者具有一个服务终端节点 (vpce-svc-1234)，该节点已关联指向子网 B 中作为目标的实例的网络负载均衡器。VPC A 的子网 A 中的实例使用接口终端节点访问子网 B 中的服务。



为实现低延迟和容错能力，建议使用网络负载均衡器，其目标位于 AWS 区域的每个可用区中。要帮助使用[区域 DNS 主机名 \(p. 247\)](#)访问服务的服务使用者实现高可用性，可以启用跨区域负载均衡。借助跨区域负载均衡，负载均衡器将在所有启用可用区中的已注册目标之间分配流量。有关更多信息，请参阅[Network Load Balancer 用户指南 中的跨区域负载均衡](#)。启用跨区域负载均衡后，可能向账户收取区域数据传输费用。

在下图中，VPC B 的所有者是服务提供商并且已配置目标位于两个不同可用区中的 网络负载均衡器。服务使用者 (VPC A) 已在其 VPC 中相同的两个可用区中创建了接口终端节点。来自 VPC A 中实例对服务的请求可使用任一接口终端节点。



终端节点服务可用区注意事项

创建终端节点服务时，将在映射至您的账户且独立于其他账户的可用区中创建此服务。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别终端节点可用区。例如，use1-az1 是 us-east-1 区域的 AZ ID，它映射至每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南 中的 [您的资源的 AZ ID](#) 或使用 [escribe-availability-zones](#)。

终端节点服务限制

要使用终端节点服务，您需要了解当前规则和限制：

- 终端节点服务仅支持通过 TCP 的 IPv4 流量。
- 服务使用者必须使用特定于终端节点的 DNS 主机名才能访问终端节点服务。不支持私有 DNS。有关更多信息，请参阅 [通过接口终端节点访问服务 \(p. 247\)](#)。
- 如果终端节点服务与多个 网络负载均衡器 关联，那么对于某个特定的可用区，一个接口终端节点将仅建立一个与负载均衡器的连接。
- 对于终端节点服务，关联的网络负载均衡器可以支持针对每个唯一目标（IP 地址和端口）的 55000 个并发连接或每分钟约 55000 个连接。如果连接数超过该值，则会增大出现端口分配错误的几率。要修复端口分配错误，请将更多目标添加到目标组。有关网络负载均衡器目标组的信息，请参阅 Network Load Balancer 用户指南 中的 [网络负载均衡器的目标组](#) 和 [向您的目标组注册目标](#)。.
- 您账户中的可用区可能不会映射到与其他账户中的可用区相同的位置。例如，您的可用区 us-east-1a 与其他账户的可用区 us-east-1a 所表示的可能不是同一个位置。有关更多信息，请参阅 [区域和可用区域概念](#)。配置终端节点服务时，将在映射到您的账户的可用区中配置此服务。

创建 VPC 终端节点服务配置

您可使用 Amazon VPC 控制台或命令行创建终端节点服务配置。在开始前，请确保您已在 VPC 中为您的服务创建一个或多个网络负载均衡器。有关更多信息，请参阅 Network Load Balancer 用户指南 中的 [Network Load Balancer 入门](#)。

您可以在配置中选择指定，必须由您手动接受所有希望与您的服务连接的接口终端节点连接请求。您可以[创建通知 \(p. 271\)](#)，在有连接请求时接收提醒。如果您不接受连接，服务使用者将无法访问您的服务。

Note

无论接受设置如何，服务使用者还必须具有与您的服务建立连接的[权限 \(p. 268\)](#)。

使用控制台创建终端节点服务

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services、Create Endpoint Service。
3. 对于关联 Network Load Balancer，选择要与终端节点服务关联的 网络负载均衡器。
4. 对于 Require acceptance for endpoint，选中此复选框以手动接受针对您的服务的连接请求。如果未选中此选项，终端节点连接会被自动接受。
5. 选择 Create service。

在创建终端节点服务配置后，您必须添加权限以使服务使用者能够创建到您服务的接口终端节点。

使用 AWS CLI 创建终端节点服务

- 使用 `create-vpc-endpoint-service-configuration` 命令并为您的 网络负载均衡器 指定一个或多个 ARN。您可以选择指定是否需要接受针对您的服务的连接。

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
    arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
    vpce/e94221227f1ba532 --acceptance-required
```

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "NetworkLoadBalancerArns": [
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
            vpce/e94221227f1ba532"
        ],
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
        "ServiceState": "Available",
        "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
        "AcceptanceRequired": true,
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "BaseEndpointDnsNames": [
            "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
        ]
    }
}
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 创建终端节点服务

- [New-EC2VpcEndpointServiceConfiguration](#) (适用于 Windows PowerShell 的 AWS 工具)
- [CreateVpcEndpointServiceConfiguration](#) (Amazon EC2 查询 API)

为您的终端节点服务添加和删除权限

在创建终端节点服务配置后，您可以控制哪些服务使用者能够创建连接您服务的接口终端节点。服务使用者是 [IAM 委托人](#) — IAM 用户、IAM 角色和 AWS 账户。要为委托人添加或删除权限，您需要其 Amazon 资源名称 (ARN)。

- 对于 AWS 账户 (以及该账户中的所有委托人)，ARN 的格式为 `arn:aws:iam::aws-account-id:root`。
- 对于特定的 IAM 用户，ARN 的格式为 `arn:aws:iam::aws-account-id:user/user-name`。
- 对于特定的 IAM 角色，ARN 的格式为 `arn:aws:iam::aws-account-id:role/role-name`。

使用控制台添加或删除权限

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
3. 选择 Actions、Add principals to whitelist。
4. 指定要为其添加权限的委托人的 ARN。要添加更多委托人，请选择 Add principal。要删除委托人，请选择相应条目旁边的交叉图标。

Note

指定 * 可为所有委托人添加权限。这将使所有 AWS 账户中的所有委托人都能够创建到您终端节点服务的接口终端节点。

5. 选择 Add to Whitelisted principals。
6. 要删除委托人，请在列表中选择该委托人，然后选择 Delete。

使用 AWS CLI 添加和删除权限

1. 要为您的终端节点服务添加权限，请使用 [modify-vpc-endpoint-service-permissions](#) 命令并使用 `--add-allowed-principals` 参数为委托人添加一个或多个 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3  
--add-allowed-principals '[ "arn:aws:iam::123456789012:root" ]'
```

2. 要查看您已为终端节点服务添加的权限，请使用 [describe-vpc-endpoint-service-permissions](#) 命令。

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
```

```
{  
    "AllowedPrincipals": [  
        {  
            "PrincipalType": "Account",  
            "Principal": "arn:aws:iam::123456789012:root"  
        }  
    ]  
}
```

- 要为您的终端节点服务删除权限，请使用 [modify-vpc-endpoint-service-permissions](#) 命令并使用 `--remove-allowed-principals` 参数为委托人删除一个或多个 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3  
--remove-allowed-principals '[ "arn:aws:iam::123456789012:root" ]'
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 修改终端节点服务权限

- [Edit-EC2EndpointServicePermission](#) (适用于 Windows PowerShell 的 AWS 工具)
- [ModifyVpcEndpointServicePermissions](#) (Amazon EC2 查询 API)

更改网络负载均衡器和接受设置

您可以通过更改与终端节点服务关联的网络负载均衡器以及更改是否需要接受连接到您的终端节点服务的请求来修改终端节点服务配置。

如果已有接口终端节点连接到您的终端节点服务，则您无法取消关联负载均衡器。

使用控制台更改终端节点服务的网络负载均衡器

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
- 选择 Actions、Associate/Disassociate Network Load Balancers。
- 根据需要选择或取消选择负载均衡器，然后选择 Save。

使用控制台修改接受设置

- 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
- 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
- 选择 Actions、Modify endpoint acceptance setting。
- 选择或取消选择 Require acceptance for endpoint，然后选择 Modify。

使用 AWS CLI 修改负载均衡器和接受设置

- 要更改终端节点服务的负载均衡器，请使用 [modify-vpc-endpoint-service-configuration](#) 命令并使用 `--add-network-load-balancer-arn` 或 `--remove-network-load-balancer-arn` 参数；例如：

```
aws ec2 modify-vpc-endpoint-service-configuration --service-  
id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn  
arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-  
vpce/e94221227f1ba532
```

- 要更改是否需要接受，请使用 [modify-vpc-endpoint-service-configuration](#) 命令并指定 `--acceptance-required` 或 `--no-acceptance-required`；例如：

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-  
svc-09222513e6e77dc86 --no-acceptance-required
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 修改终端节点服务配置

- [Edit-EC2VpcEndpointServiceConfiguration](#) (适用于 Windows PowerShell 的 AWS 工具)

- [ModifyVpcEndpointServiceConfiguration](#) (Amazon EC2 查询 API)

接受和拒绝接口终端节点连接请求

在您创建终端节点服务后，已添加权限的服务使用者能够创建连接您服务的接口终端节点。有关创建接口终端节点的更多信息，请参阅[接口 VPC 终端节点 \(AWS PrivateLink\) \(p. 237\)](#)。

如果您已指定需要接受连接，则必须手动接受或拒绝对您的终端节点服务的接口终端节点连接请求。在接受接口终端节点后，它将变为 available 状态。

您可以在接口终端节点连接处于 available 状态之后拒绝该连接。

使用控制台接受或拒绝连接请求

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
3. Endpoint Connections 选项卡列出了目前有待您批准的终端节点连接。选择终端节点，选择 Actions，然后选择 Accept endpoint connection request 以接受连接或选择 Reject endpoint connection request 以拒绝连接。

使用 AWS CLI 接受或拒绝连接请求

1. 要查看待接受的终端节点连接，请使用 `describe-vpc-endpoint-connections` 命令并按 pendingAcceptance 状态筛选。

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-state,Values=pendingAcceptance
```

```
{  
    "VpcEndpointConnections": [  
        {  
            "VpcEndpointId": "vpce-0c1308d7312217abc",  
            "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",  
            "CreationTimestamp": "2017-11-30T10:00:24.350Z",  
            "VpcEndpointState": "pendingAcceptance",  
            "VpcEndpointOwner": "123456789012"  
        }  
    ]  
}
```

2. 要接受终端节点连接请求，请使用 `accept-vpc-endpoint-connections` 命令并指定终端节点 ID 和终端节点服务 ID。

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

3. 要拒绝终端节点连接请求，请使用 `reject-vpc-endpoint-connections` 命令。

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 接受和拒绝终端节点连接

- [Confirm-EC2EndpointConnection](#) 和 [Deny-EC2EndpointConnection](#) (适用于 Windows PowerShell 的 AWS 工具)

- [AcceptVpcEndpointConnections](#) 和 [RejectVpcEndpointConnections](#) (Amazon EC2 查询 API)

为终端节点服务创建和管理通知

您可以创建通知以针对在连接到您的终端节点服务的终端节点上发生的特定事件接收提醒。例如，您可以在接受或拒绝针对您的终端节点服务的终端节点请求时收到电子邮件。要创建通知，您必须将 Amazon SNS 主题与通知关联。您可以订阅 SNS 主题以在终端节点事件发生时收到电子邮件通知。有关更多信息，请参阅 [Amazon Simple Notification Service 开发人员指南](#)。

用于通知的 Amazon SNS 主题必须具有允许 Amazon VPC 终端节点服务代表您发布通知的主题策略。确保在您的主题策略中包含以下语句。有关更多信息，请参阅 [Amazon Simple Notification Service 开发人员指南](#) 中的 [管理至 Amazon SNS 主题的访问](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "vpce.amazonaws.com"  
            },  
            "Action": "SNS:Publish",  
            "Resource": "arn:aws:sns:region:account:topic-name"  
        }  
    ]  
}
```

为终端节点服务创建通知

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
3. 选择 Notifications、Create Notification。
4. 选择要与通知关联的 SNS 主题的 ARN。
5. 对于 Events，选择要接收其通知的终端节点事件。
6. 选择 Create Notification。

在创建通知后，您可以更改与通知关联的 SNS 主题，也可以为通知指定不同的终端节点事件。

为终端节点服务修改通知

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
3. 选择 Notifications、Actions、Modify Notification。
4. 指定 SNS 主题的 ARN 并根据需要选择或取消选择终端节点事件。
5. 选择 Modify Notification。

如果您不再需要某通知，则可删除它。

删除通知

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择您的终端节点服务。
3. 依次选择 Notifications、Actions、Delete Notification。
4. 选择 Yes, Delete。

使用 AWS CLI 创建和管理通知

- 要为终端节点服务创建通知，请使用 [create-vpc-endpoint-connection-notification](#) 命令并指定 SNS 主题的 ARN、要通知的事件以及终端节点服务的 ID；例如：

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

```
{  
    "ConnectionNotification": {  
        "ConnectionNotificationState": "Enabled",  
        "ConnectionNotificationType": "Topic",  
        "ServiceId": "vpce-svc-1237881c0d25a3abc",  
        "ConnectionEvents": [  
            "Reject",  
            "Accept",  
            "Delete",  
            "Connect"  
        ],  
        "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",  
        "ConnectionNotificationArn": "arn:aws:sns:us-east-2:123456789012:VpceNotification"  
    }  
}
```

- 要查看您的通知，请使用 [describe-vpc-endpoint-connection-notifications](#) 命令：

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

- 要更改通知的 SNS 主题或终端节点事件，请使用 [modify-vpc-endpoint-connection-notification](#) 命令；例如：

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-arn arn:aws:sns:us-east-2:123456789012:mytopic
```

- 要删除通知，请使用 [delete-vpc-endpoint-connection-notifications](#) 命令：

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-ids vpce-nfn-008776de7e03f5abc
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 创建和管理通知

- [New-EC2VpcEndpointConnectionNotification](#)、[Get-EC2EndpointConnectionNotification](#)、[Edit-EC2VpcEndpointConnectionNotification](#) 和 [Remove-EC2EndpointConnectionNotification](#) (适用于 Windows PowerShell 的 AWS 工具)
- [CreateVpcEndpointConnectionNotification](#)、[DescribeVpcEndpointConnectionNotifications](#)、[ModifyVpcEndpointConnectionNotifications](#) 和 [DeleteVpcEndpointConnectionNotifications](#) (Amazon EC2 查询 API)

对连接信息使用代理协议

网络负载均衡器向您的应用程序（您的服务）提供源 IP 地址。当服务使用者通过接口终端节点将流量发送至您的服务时，向您的应用程序提供的源 IP 地址是网络负载均衡器节点的私有 IP 地址而不是服务使用者的 IP 地址。

如果您需要服务使用者的 IP 地址及其对应的接口终端节点 ID，请在您的负载均衡器上启用代理协议并从代理协议标头中获取客户端 IP 地址。有关更多信息，请参阅 Network Load Balancer 用户指南 中的 [代理协议](#)。

添加或删除 VPC 终端节点服务标签

标签提供一种标识 VPC 终端节点服务的方法。您可以添加或删除标签。

添加或删除 VPC 终端节点服务标签

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择终端节点服务。
3. 选择 VPC 终端节点服务，然后选择操作、添加/编辑标签。
4. 添加或删除标签。

[添加标签] 选择创建标签，然后执行以下操作：

- 对于键，输入键名称。
- 对于值，输入键值。

[删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

To add or remove a tag using the 适用于 Windows PowerShell 的 AWS 工具 or an API

- [create-tags](#) (AWS CLI)
- [CreateTags](#) (适用于 Windows PowerShell 的 AWS 工具)
- [delete-tags](#) (AWS CLI)
- [DeleteTags](#) (适用于 Windows PowerShell 的 AWS 工具)

删除终端节点服务配置

您可以删除终端节点服务配置。删除该配置不会删除在您的 VPC 中托管的应用程序或关联的负载均衡器。

在删除终端节点服务配置之前，您必须拒绝已连接到该服务的任何 available 或 pending-acceptance VPC 终端节点。有关更多信息，请参阅 [接受和拒绝接口终端节点连接请求 \(p. 270\)](#)。

使用控制台删除终端节点服务配置

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Endpoint Services，然后选择该服务。
3. 依次选择 Actions 和 Delete。
4. 选择 Yes, Delete。

使用 AWS CLI 删除终端节点服务配置

- 使用 [delete-vpc-endpoint-service-configurations](#) 命令并指定该服务的 ID。

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpc-e-svc-03d5ebb7d9579a2b3
```

使用适用于 Windows PowerShell 的 AWS 工具或 API 删除终端节点服务配置

- [Remove-EC2EndpointServiceConfiguration](#) (适用于 Windows PowerShell 的 AWS 工具)

- [DeleteVpcEndpointServiceConfigurations](#) (Amazon EC2 查询 API)

ClassicLink

ClassicLink 允许您将 EC2-Classic 实例链接到账户中位于同一区域内的 VPC。这样，您可以将 VPC 安全组与 EC2-Classic 实例关联，以便允许 EC2-Classic 实例与 VPC 中的实例使用私有 IPv4 地址进行通信。通过 ClassicLink，无需使用公有 IPv4 地址或弹性 IP 地址即可在这些平台中的实例之间进行通信。有关私有和公有 IPv4 地址的更多信息，请参阅 [您的 VPC 中的 IP 地址 \(p. 100\)](#)。

ClassicLink 可用于账户支持 EC2-Classic 平台的所有用户，并且可以与任何 EC2-Classic 实例一起使用。

使用 ClassicLink 不收取任何额外费用。采用标准的数据传输和实例使用小时数计费方式。

有关 ClassicLink 及其使用方法的更多信息，请参阅 Amazon EC2 用户指南中的下列主题：

- [ClassicLink 基础知识](#)
- [ClassicLink 限制](#)
- [使用 ClassicLink](#)
- [ClassicLink API 和 CLI 概述](#)

VPN 连接

您可以使用下列 VPN 选项，连接 Amazon VPC 与远程网络和用户。

VPN 连接选项	描述
AWS Site-to-Site VPN	您可以在 VPC 和远程网络之间创建 IPsec VPN 连接。在 Site-to-Site VPN 连接的 AWS 一端，虚拟专用网关 提供两个 VPN 终端节点（隧道）来进行自动故障转移。您在 Site-to-Site VPN 连接的远程端配置 客户端网关。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 和 Amazon VPC 网络管理员指南 。
AWS 客户端 VPN	AWS 客户端 VPN 是一种基于客户端的托管 VPN 服务，让您能够安全地访问本地网络中的 AWS 资源。借助 AWS 客户端 VPN，您可以配置一个用户可以连接的终端节点，以建立安全的 TLS VPN 会话。这使客户端能够使用基于 OpenVPN 的 VPN 客户端从任何位置访问 AWS 或本地部署中的资源。有关更多信息，请参阅 AWS 客户端 VPN 用户指南 。
AWS VPN CloudHub	如果您拥有多个远程网络（例如，多个分公司），则可以通过虚拟专用网关创建多个 AWS Site-to-Site VPN 连接，来启用这些网络之间的通信。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的 使用 VPN CloudHub 在站点之间提供安全通信 。
第三方软件 VPN 设备	您可以通过在 VPC 中使用正在运行软件 VPN 设备的 Amazon EC2 实例来创建与远程网络的 VPN 连接。AWS 不提供或维护第三方软件 VPN 设备；但是，您可以选择合作伙伴和开源社区提供的一系列产品。在 AWS Marketplace 上查找第三方软件 VPN 设备。

您还可以使用 AWS Direct Connect 创建远程网络与 VPC 之间的专用私有连接。您可以将此连接与 AWS Site-to-Site VPN 结合来创建经 IPSec 加密的连接。有关更多信息，请参阅 AWS Direct Connect 用户指南 中的 [什么是 AWS Direct Connect？](#)。

Amazon VPC 限制

以下表格列出了您的 AWS 账户的每区域 Amazon VPC 资源限制。除非另外指明，否则您可使用 [Amazon VPC 限制表单](#) 申请提高这些限制。对于其中的一些限制，您可以使用 Amazon EC2 控制台的限制页面查看当前限制。

如果您请求对每个资源提升适用的限制，我们将提升该区域中所有资源的限制。例如，每个 VPC 的安全组的限制适用于该区域中的所有 VPC。

VPC 和子网

资源	默认限制	注释
每个区域的 VPC 数	5	每个区域的 Internet 网关数量限制与此直接相关。提高该限制会使每个区域的 Internet 网关数量限制提高同样的数量。 即使默认限制为每个区域 5 个 VPC，客户也可以根据需要在每个区域拥有 100 个 VPC。您可使用 Amazon VPC 限制表单 申请提高这些限制。
每个 VPC 的子网数量	200	-
每个 VPC 的 IPv4 CIDR 块数	5	该限制由主要 CIDR 块加上 4 个辅助 CIDR 块组成。
每个 VPC 的 IPv6 CIDR 块数	1	不能提高该限制。

DNS

有关更多信息，请参阅[DNS 限制 \(p. 230\)](#)。

弹性 IP 地址 (IPv4)

资源	默认限制	注释
每个区域的弹性 IP 地址数量	5	这是对 EC2-VPC 中使用的弹性 IP 地址数量的限制。对于在 EC2-Classic 中使用的弹性 IP 地址，请参阅 Amazon Web Services 一般参考中的 Amazon EC2 限制 。

网关

资源	默认限制	注释
每个区域的客户网关数	50	-
每个区域的仅出口 Internet 网关数	5	该限制与每个区域的 VPC 数量限制直接相关。要提高该限制，请提高每个区域的 VPC 数限制。您一次只能将一个仅出口 Internet 网关连接到 VPC。
每个区域的 Internet 网关数	5	该限制与每个区域的 VPC 数量限制直接相关。要提高该限制，请提高每个区域的 VPC 数限制。一次只有一个 Internet 网关可以连接到 VPC。
每个可用区的 NAT 网关	5	处于 pending、active 或 deleting 状态的 NAT 网关都占用限额。
每个区域的虚拟专用网关数	5	您一次只能将一个虚拟专用网关连接到 VPC。

网络 ACL

资源	默认限制	注释
每个 VPC 的网络 ACL 数	200	在 VPC 中，您可以将一个网络 ACL 关联到一个或多个子网。该限制与每个网络 ACL 的规则数不同。
每个网络 ACL 的规则数	20	这是单个网络 ACL 的单向限制，其中传入规则的限制为 20，传出规则的限制也为 20。该限制包括 IPv4 和 IPv6 规则，并包括默认拒绝规则（IPv4 的规则编号为 32767，IPv6 的规则编号为 32768，或在 Amazon VPC 控制台中使用星号 *）。 可将该限制提高至最大值 40；但是，由于处理额外规则需要增加工作负载，网络性能可能会受到影响。

网络接口

资源	默认限制	注释
每个实例的网络接口	-	该限制因实例类型而异。有关更多信息，请参阅 每个实例类型每个 ENI 的 IP 地址 。
每个区域的网络接口数	350	该限制大于默认限制 (350) 或您的按需实例限制值乘以 5。按需实例的默认限制为 20。如果您的按需实例限制低于 70，则应用默认限

资源	默认限制	注释
		制 350。要提高该限制，请提交申请或提高按需实例限制。

路由表

资源	默认限制	注释
每个 VPC 的路由表数	200	该限制包括主路由表。
每个路由表的路由 (非传播路由)	50	<p>可以将该限制提高至最大值 1000；但是，网络性能可能会受到影响。将单独为 IPv4 路由和 IPv6 路由实施该限制。</p> <p>如果您有 125 个以上的路由，我们建议您对调用进行分页以描述路由表，从而获得更好的性能。</p>
每个路由表的 BGP 通告路由 (传播路由)	100	不能提高该限制。如果您需要超过 100 个前缀，请通告默认路由。

安全组

资源	默认限制	注释
每个区域的安全组	2500	最大值为 10000。如果某个区域中有超过 5000 个安全组，我们建议您对调用进行分页以描述安全组，从而获得更好的性能。
每个安全组的入站或出站规则	60	<p>对于每个安全组，您可以设置 60 条入站规则和 60 条出站规则（入站规则和出站规则合起来总数为 120 条）。该限制对于 IPv4 规则和 IPv6 规则分开实施；例如，安全组可以有 60 条针对 IPv4 流量的入站规则和 60 条针对 IPv6 流量的入站规则。引用安全组或前缀列表 ID 的规则计为针对 IPv4 的一条规则及针对 IPv6 的一条规则。</p> <p>限制更改适用于入站和出站规则。该限制值与每个网络接口的安全组限制值的积不得超过 1000。例如，如果您希望将该限制增加到 100，我们会将每个网络接口的安全组数的限制减少为 10。</p>
每个网络接口的安全组数	5	要提高或降低该限制，请联系 AWS Support。最大值为 16。每个网络接口的安全组数限制与每个安全组的规则数限制的乘积不能超过 1000。例如，如果您将该限制提高到 10，我们会将每个安全组的规则数限制减至 100。

VPC 对等连接

资源	默认限制	注释
每个 VPC 的活动 VPC 对等连接	50	每个 VPC 的最大限制为 125 个对等连接。应相应地增加每个路由表的条目数；但是，网络性能可能会受到影响。
未完成的 VPC 对等连接请求	25	这是从您的账户请求的未完成 VPC 对等连接请求数的限制。
未接受的 VPC 对等连接请求的过期时间	1 周 (168 小时)	-

VPC 终端节点

资源	默认限制	注释
每个区域的网关 VPC 终端节点数	20	每个 VPC 不能有超过 255 个网关终端节点。
每个 VPC 的接口 VPC 终端节点	20	每个区域的接口端点的最大限制为该限制乘以该区域中的 VPC 数。

AWS Site-to-Site VPN 连接

资源	默认限制	注释
每个区域的Site-to-Site VPN 连接数	50	-
每个 VPC (每个虚拟专用网关) 的Site-to-Site VPN 连接数	10	-

VPC 共享

所有标准 VPC 限制均适用于共享的 VPC。

资源	默认限制	注释
可与 VPC 共享的不同账户的数量	100	这是可以与其共享 VPC 中的子网的不同参与者账户的数量限制。这是每个 VPC 的限制，并应用于 VPC 中共享的所有子网。在请求提高该限制之前，AWS 建议您对 <code>DescribeSecurityGroups</code> 和 <code>DescribeNetworkInterfaces</code> API 调用进行分页。要提高该限制，请联系 AWS Support。

资源	默认限制	注释
可以与账户共享的子网的数量	100	这是可以与 AWS 账户共享的最大子网数限制。在请求提高该限制之前，AWS 建议您对 <code>DescribeSecurityGroups</code> 和 <code>DescribeSubnets</code> API 调用进行分页。要提高该限制，请联系 AWS Support。

文档历史记录

下表描述了 Amazon VPC 用户指南、Amazon VPC Peering Guide 和 Amazon VPC 网络管理员指南 的每次发布中所做的重要更改。

功能	API 版本	描述	发行日期
AWS Site-to-Site VPN	2016-11-15	将 AWS Managed VPN (现在称为 AWS Site-to-Site VPN) 的内容移至 AWS Site-to-Site VPN 用户指南 。	2018 年 12 月 18 日
VPC 共享	2016-11-15	您可以与同一 AWS 组织中的多个账户共享位于同一 VPC 中的子网。	2018 年 11 月 27 日
区域间对等	2016-11-15	您可以在位于不同区域中的 VPC 之间创建 VPC 对等连接。有关更多信息，请参阅 Amazon VPC Peering Guide 。	2017 年 11 月 29 日
VPC 终端节点服务	2016-11-15	您可以在 VPC 中创建自己的 PrivateLink 服务并支持其他 AWS 账户和用户通过接口 VPC 终端节点连接到您的服务。有关更多信息，请参阅 VPC 终端节点服务 (AWS PrivateLink) (p. 263) 。	2017 年 11 月 28 日
创建默认子网	2016-11-15	您可以在没有默认子网的可用区中创建一个默认子网。有关更多信息，请参阅 创建默认子网 (p. 98) 。	2017 年 11 月 9 日
AWS 服务的接口 VPC 终端节点	2016-11-15	您可以创建接口终端节点以私密地连接到某些 AWS 服务。接口终端节点是具有私有 IP 地址的网络接口，可用作服务流量的入口点。有关更多信息，请参阅 VPC 终端节点 (p. 235) 。	2017 年 11 月 8 日
自定义 ASN	2016-11-15	创建虚拟专用网关时，可以为网关的 Amazon 端指定专用自治系统编号 (ASN)。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南 中的 虚拟专用网关 。	2017 年 10 月 10 日
VPN 隧道选项	2016-11-15	您可以为 VPN 隧道指定隧道内部 CIDR 块和自定义预共享密钥。有关更多信息，请参阅 Amazon VPC 网络管理员指南 中的 为您的 Site-to-Site VPN 连接配置 VPN 隧道 和 设置 Site-to-Site VPN 连接概述 。	2017 年 10 月 3 日
VPN 类别	2016-11-15	您可以查看 VPN 连接的类别。有关更多信息，请参阅 AWS Site-to-Site VPN 类别 。	2017 年 10 月 3 日
NAT 网关的标记支持	2016-11-15	您可以给自己的 NAT 网关加标签。有关更多信息，请参阅 标记 NAT 网关 (p. 206) 。	2017 年 9 月 7 日
NAT 网关的 Amazon CloudWatch 指标	2016-11-15	您可以查看 NAT 网关的 CloudWatch 指标。有关更多信息，请参阅 使用 Amazon CloudWatch 监控 NAT 网关 (p. 207) 。	2017 年 9 月 7 日
安全组规则说明	2016-11-15	您可以向安全组规则添加说明。有关更多信息，请参阅 安全组规则 (p. 121) 。	2017 年 8 月 31 日

功能	API 版本	描述	发行日期
VPC 的辅助 IPv4 CIDR 块	2016-11-15	您可以向 VPC 中添加多个 IPv4 CIDR 块。有关更多信息，请参阅 向 VPC 中添加 IPv4 CIDR 块 (p. 79) 。	2017 年 8 月 29 日
DynamoDB 的 VPC 端点	2016-11-15	您可使用 VPC 端点从您的 VPC 访问 Amazon DynamoDB。有关更多信息，请参阅 Amazon DynamoDB 的终端节点 (p. 257) 。	2017 年 8 月 16 日
恢复弹性 IP 地址	2016-11-15	如果您释放了一个弹性 IP 地址，则可能能够恢复它。有关更多信息，请参阅 使用弹性 IP 地址 (p. 233) 。	2017 年 8 月 11 日
创建默认 VPC	2016-11-15	如果您删除了现有默认 VPC，则可以创建一个新的默认 VPC。有关更多信息，请参阅 创建默认 VPC (p. 97) 。	2017 年 7 月 27 日
VPN 指标	2016-11-15	您可以查看 VPN 连接的 CloudWatch 指标。有关更多信息，请参阅 监控您的 Site-to-Site VPN 连接 。	2017 年 5 月 15 日
IPv6 支持	2016-11-15	您可以将一个 IPv6 CIDR 块与您的 VPC 关联并为您的 VPC 中的资源分配 IPv6 地址。有关更多信息，请参阅 您的 VPC 中的 IP 地址 (p. 100) 。	2016 年 12 月 1 日
对非 RFC 1918 IP 地址范围的 DNS 解析支持		Amazon DNS 服务器现在可以将私有 DNS 主机名解析为全部地址空间内的私有 IP 地址。有关更多信息，请参阅 在您的 VPC 中使用 DNS (p. 228) 。	2016 年 10 月 24 日
用于 VPC 对等的 DNS 解析支持	2016-04-01	您可以使本地 VPC 在通过对等 VPC 中的实例查询时将公有 DNS 主机名解析为私有 IP 地址。有关更多信息，请参阅 Amazon VPC Peering Guide 中的 修改 VPC 对等连接 。	2016 年 7 月 28 日
过时的安全组规则	2015-10-01	您可以了解自己的安全组是否被对等 VPC 中的安全组规则引用，找出过时的安全组规则。有关更多信息，请参阅 Amazon VPC Peering Guide 中的 使用过时的安全组 。	2016 年 12 月 5 日
在 VPC 对等连接上使用 ClassicLink	2015-10-01	您可以修改 VPC 对等连接，使本地链接的 EC2-Classic 实例能够与对等 VPC 中的实例进行通信，反之亦然。有关更多信息，请参阅 Amazon VPC Peering Guide 中的 使用 ClassicLink 进行配置 。	2016 年 4 月 26 日
NAT 网关	2015-10-01	您可在公有子网中创建 NAT 网关，并让私有子网中的实例向 Internet 或其他 AWS 服务发出出站流量。有关更多信息，请参阅 NAT 网关 (p. 200) 。	2015 年 12 月 17 日
VPN 增强功能	2015-04-15	现在，VPN 连接在连接的第 1 和第 2 阶段支持 AES 256 位加密功能、SHA-256 哈希函数、NAT 遍历及其他 Diffie-Hellman 组。此外，您现可为使用同一个客户网关设备的每个 VPN 连接使用相同的客户网关 IP 地址。	2015 年 10 月 28 日
VPC 流日志	2015-04-15	您可以创建流日志以捕获有关传入和传出您的 VPC 中的网络接口的 IP 流量的信息。有关更多信息，请参阅 VPC 流日志 (p. 165) 。	2015 年 6 月 10 日

功能	API 版本	描述	发行日期
VPC 终端节点	2015-03-01	使用终端节点可以在您的 VPC 和其他 AWS 服务之间创建私有连接，无需通过 Internet、VPN 连接、NAT 实例或 AWS Direct Connect 进行访问。有关更多信息，请参阅 VPC 终端节点 (p. 235) 。	2015 年 5 月 11 日
ClassicLink	2014-10-01	ClassicLink 允许将您的 EC2-Classic 实例链接到您账户中的 VPC。您可以将 VPC 安全组与 EC2-Classic 实例关联起来，从而允许 EC2-Classic 实例与 VPC 中使用私有 IP 地址的实例进行通信。有关更多信息，请参阅 ClassicLink (p. 274) 。	2015 年 1 月 7 日
使用私有托管区域	2014-09-01	您可以使用在 Route 53 中的私有托管区域中定义的自定义 DNS 域名访问您的 VPC 中的资源。有关更多信息，请参阅 使用私有托管区域 (p. 231) 。	2014 年 11 月 5 日
修改子网的公有 IP 寻址属性	2014-06-15	您可以修改子网的公有 IP 寻址属性以指示在该子网中启动的实例是否应接收公有 IP 地址。有关更多信息，请参阅 修改子网的公有 IPv4 寻址属性 (p. 103) 。	2014 年 6 月 21 日
VPC 对等	2014-02-01	您可以在两个 VPC 之间创建 VPC 对等连接，这样，任一 VPC 中的实例都可以使用私有 IP 地址相互通信（如同它们处于同一 VPC 中）。有关更多信息，请参阅 VPC 对等 (p. 232) 。	2014 年 3 月 24 日
新的 EC2 启动向导	2013-10-01	添加了有关重新设计的 EC2 启动向导的信息。有关更多信息，请参阅 步骤 3：将实例启动到 VPC 中 (p. 13) 。	2013 年 10 月 10 日
分配公有 IP 地址	2013-07-15	增加了有关在 VPC 中启动的实例的新公有 IP 地址功能的信息。有关更多信息，请参阅 在实例启动期间分配公有 IPv4 地址 (p. 103) 。	2013 年 8 月 20 日
启用 DNS 主机名称并禁用 DNS 解析	2013-02-01	<p>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。</p> <p>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。</p> <p>有关更多信息，请参阅在您的 VPC 中使用 DNS (p. 228)。</p>	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，您可以与不支持 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

功能	API 版本	描述	发行日期
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 3 日
专用实例	2011 年 2 月 28 日	专用实例是在您的 VPC 中启动、运行单个客户专用硬件的 Amazon EC2 实例。专用实例让您能充分利用 Amazon VPC 和 AWS 弹性预置的优势，比如仅为实际使用量付费与隔离的私有虚拟网络，所有这些优势让您的实例能在以硬件级别隔离的环境下运行。	2011 年 3 月 27 日