亚马逊云科技

开发人员指南

Amazon Route 53

API 版本 2013-04-01

Amazon Route 53: 开发人员指南

Table of Contents

什么是 Amazon Route 53？

Amazon Route 53 是一种可用性高、可扩展性强的域名系统（DNS）Web 服务。您可以使用 Route 53 以任意组合执行三个主要功能：域注册、DNS 路由和运行状况检查。

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

如果您选择使用 Route 53 来执行所有这三种功能，请务必遵循以下顺序：

1. 注册域名

   您的网站需要一个名称，如 example.com。利用 Route 53 可以为您的网站或 Web 应用程序注册一个名称，称为域名。

   - 有关概述，请参阅域注册的工作原理。
   - 有关步骤，请参阅 注册新域。
   - 有关指导您注册域并在 Amazon S3 存储桶中创建简单网站的教程，请参阅 开始使用 Amazon Route 53。

2. 将 Internet 流量路由到您的域的资源

   当用户打开 Web 浏览器并在地址栏中输入您的域名 (example.com) 或子域名 (acme.example.com) 时，Route 53 会帮助将浏览器与您的网站或 Web 应用程序相连接。

   - 有关概述，请参阅如何将 Internet 流量路由到您的网站或 Web 应用程序。
   - 有关步骤，请参阅 将 Amazon Route 53 配置为 DNS 服务。
   - 有关如何将电子邮件发送到 Amazon 的程序 WorkMail，请参阅将流量路由到 Amazon WorkMail。

3. 检查资源的运行状况

   Route 53 会通过 Internet 将自动请求发送到资源（如 Web 服务器），以验证其是否可访问、可用且功能正常。您还可以选择在资源变得不可用时接收通知，并可选择将 Internet 流量从运行状况不佳的资源路由到别处。

   - 有关概述，请参阅Amazon Route 53 如何检查您的资源的运行状况。

- 有关步骤，请参阅 创建 Amazon Route 53 运行状况检查 。

Route 53 的其他功能

除了是一项域名系统 (DNS) Web 服务外，Route 53 还提供以下功能：

VPC 解析器

在 Amazon Outposts 机架中或任何其他本地网络 VPCs 中 Amazon Web Services 区域为你的 Amazon 获取递归 DNS。 VPCs 创建条件转发规则和 Route 53 端点，解析存储在 Route 53 私有托管区或本地 DNS 服务器中的自定义名称。

有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。

Outposts 上的 Amazon Route 53 Resolver

通过解析器终端节点将 Outpost 机架上的 VPC 解析器与本地数据中心的 DNS 服务器连接起来。这样就可以解析 Outposts 机架与其他本地资源之间的 DNS 查询。

有关更多信息，请参阅 什么是 Amazon Route 53 on Outposts？。

解析器 DNS 防火墙

在 VPC 解析器中保护您的递归 DNS 查询。创建域列表并构建防火墙规则，根据这些规则过滤出站的 DNS 流量。

有关更多信息，请参阅 使用 DNS Firewall 筛选出站 DNS 流量。

Traffic Flow

Easy-to-use 以及经济实惠的全球流量管理：根据地理位置、延迟、运行状况和其他考虑因素，将最终用户路由到最适合您应用程序的终端节点。

有关更多信息，请参阅 使用 Traffic Flow 来路由 DNS 流量。

Amazon Route 53 Profiles

使用 Route 53 配置文件，您可以跨多种 VPCs 不同方式 Amazon Web Services 账户应用和管理与 DNS 相关的 Route 53 配置。

有关更多信息，请参阅 Amazon Route 53 Profiles 是什么？。

主题

- 域注册的工作原理

- 如何将 Internet 流量路由到您的网站或 Web 应用程序
- Amazon Route 53 如何检查您的资源的运行状况
- Amazon Route 53 概念
- 如何开始使用 Amazon Route 53
- 访问 Amazon Route 53
- Amazon Identity and Access Management
- Amazon Route 53 定价和计费
- 将 Route 53 与 S Amazon DK 一起使用

域注册的工作原理

如果要创建网站或 Web 应用程序，请首先注册您的网站的名称，称为domain name。您的域名是用户在浏览器中输入以显示您的网站的名称 (如 example.com)。

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

以下是如何向 Amazon Route 53 注册域名的概述：

1. 选择一个域名并确认它是可用的，也就是说，没有人已经注册了您想要的域名。

   如果您想要的域名已经在使用，则您可以尝试其他名称，或尝试仅将顶级域 (例如 .com) 更改为另一个顶级域名，如 .ninja 或 .hockey。有关 Route 53 支持的顶级域的列表，请参阅 可向 Amazon Route 53 注册的域。 。
2. 向 Route 53 注册域名。注册域时，您可以提供域所有者和其他联系人的姓名和联系信息。

   当您向 Route 53 注册域时，相应服务将会通过执行以下操作自动将其自身设为域的 DNS 服务：
   - 创建与您的域具有相同名称的hosted zone。
   - 将一组由四个名称服务器构成的名称服务器组分配给托管区域。当有人使用浏览器访问您的网站（例如 www.example.com）时，这些名称服务器会告知浏览器在哪里查找您的资源，例如 Web 服务器或 Amazon S3 存储桶。（Amazon S3 是对象存储，用于从 Web 上的任意位置存储和检索任何数量的数据。存储桶是您存储在 S3 中的对象的容器。）

- 从托管区域获取名称服务器，并将其添加到域中。

有关更多信息，请参阅 如何将 Internet 流量路由到您的网站或 Web 应用程序。

3. 在注册过程结束时，我们会将您的信息发送给域注册商。domain registrar为 Amazon Registrar, Inc. 或我们的注册商合作者 Gandi。要确定您的域的注册商是谁，请参阅查找注册商。
4. 该注册商会将您的信息发送给域的注册机构。注册机构是销售一个或多个顶级域（如 .com）的域注册的公司。
5. 注册机构将有关您的域的信息存储在其自己的数据库中，并将一些信息存储在公共 WHOIS 数据库中。

有关如何注册域名的更多信息，请参阅注册新域。

如果您已经向另一个注册商注册了域名，则可以选择将该域注册转移到 Route 53。使用其它 Route 53 功能则不需要执行此操作。有关更多信息，请参阅 将域注册转移到 Amazon Route 53。

如何将 Internet 流量路由到您的网站或 Web 应用程序

Internet 上的所有计算机 (从您的智能手机或笔记本电脑连接到为海量零售网站提供内容的服务器)，均通过使用数字相互通信。称为 IP 地址的这些数字采用以下格式之一：

- 互联网协议版本 4 (IPv4) 格式，例如 192.0.2.44
- 互联网协议版本 6 (IPv6) 格式，例如 2001:0 db 8:85 a 3:0000:00:00:abcd: 0001:2345

当您打开浏览器访问某个网站时，您不需要记住并输入像这么长的一串字符。相反，您可以输入像 example.com 这样的域名，仍然可访问预期的网站。DNS 服务（例如 Amazon Route 53）有助于在域名和 IP 地址之间建立连接。

主题

- 有关对 Amazon Route 53 进行配置以路由域 Internet 流量的概述
- Amazon Route 53 如何为您的域路由流量

有关对 Amazon Route 53 进行配置以路由域 Internet 流量的概述

下面概述了如何使用 Amazon Route 53 控制台来注册域名，以及将 Route 53 配置为将 Internet 流量路由到您的网站或 Web 应用程序。

1. 您注册希望用户用于访问您的内容的域名。有关概述，请参阅域注册的工作原理。
2. 注册您的域名后，Route 53 会自动创建与该域的名称相同的公共托管区域。有关更多信息，请参阅使用公有托管区。
3. 要将流量路由到您的资源，请在您的托管区域中创建记录 (也称为资源记录集)。每个记录都包含有关如何要为您的域路由流量的信息，比如：

   Name

   记录的名称对应于您希望 Route 53 对其路由流量的域名 (example.com) 或子域名（www.example.com、retail.example.com）。

   托管区域中每个记录的名称必须以托管区域的名称结尾。例如，如果托管区域的名称为 example.com，则所有记录名称均必须以 example.com 结尾。Route 53 控制台会为您自动执行此操作。

   Type

   记录类型通常决定了您希望流量路由到的资源的类型。例如，要将流量路由到电子邮件服务器，请将 Type（类型）指定为 MX。要将流量路由到具有 IPv4 IP 地址的 Web 服务器，请将 “类型” 指定 A。

   值

   “Value”与“Type”密切相关。如果您将“Type”指定为“MX”，则对“Value”指定一个或多个电子邮件服务器的名称。如果将 “类型” 指定 A，则可以按 IPv4 格式指定 IP 地址，例如 192.0.2.136。

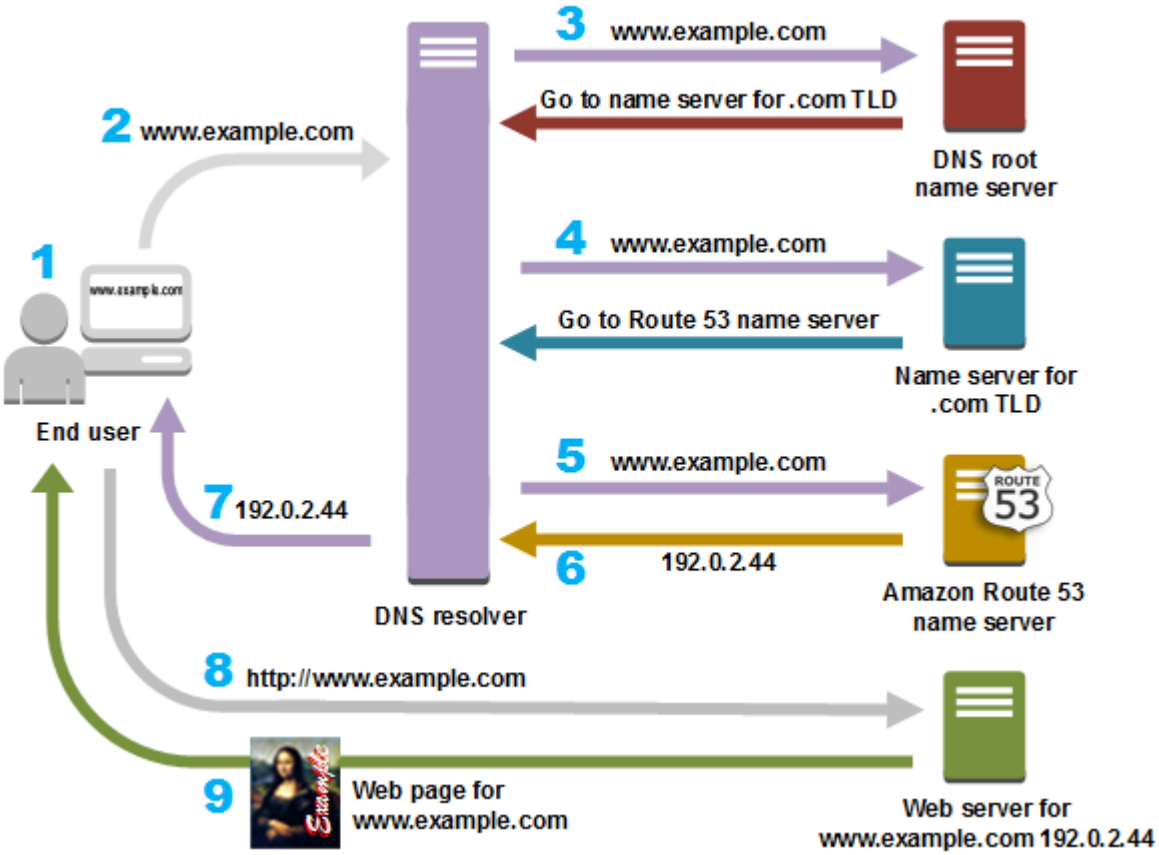
有关记录的更多信息，请参阅 使用记录。

您还可以创建特殊的 Route 53 记录（称为别名记录），用于将流量路由到 Amazon S3 存储桶、Amazon CloudFront 分配和其他 Amazon 资源。有关更多信息，请参阅在别名记录和非别名记录之间进行选择和将互联网流量路由到您的 Amazon 资源。

有关将 Internet 流量路由到您的资源的更多信息，请参阅将 Amazon Route 53 配置为 DNS 服务。

Amazon Route 53 如何为您的域路由流量

在您将 Amazon Route 53 配置为将 Internet 流量路由到您的资源（比如 Web 服务器或 Amazon S3 存储桶）之后，当有人请求 www.example.com 的内容时，将在短短几毫秒内发生以下情况：



1. 用户打开 Web 浏览器并在地址栏中输入 www.example.com，然后按 Enter。
2. 将对 www.example.com 的请求路由到 DNS 解析程序，该解析程序通常由用户的 Internet 服务提供商 (ISP) (比如有线 Internet 提供商、DSL 宽带提供商或企业网络) 进行管理。
3. ISP 的 DNS 解析程序将对 www.example.com 的请求转发到 DNS 根名称服务器。
4. DNS 解析程序将再次转发对 www.example.com 的请求，而这次会转发到 .com 域的其中一个 TLD 名称服务器。.com 域的名称服务器使用与 example.com 域关联的四个 Route 53 名称服务器的名称来响应该请求。

   DNS 解析程序会缓存（存储）四个 Route 53 名称服务器。下次有人浏览到 example.com 时，解析程序将跳过步骤 3 和 4，因为它已缓存了 example.com 的名称服务器。名称服务器通常缓存时长为两天。
5. DNS 解析程序选择一个 Route 53 名称服务器，并将对 www.example.com 的请求转发到该名称服务器。
6. Route 53 名称服务器在 example.com 托管区域中查找 www.example.com 记录、获取关联值（比如 Web 服务器的 IP 地址 192.0.2.44），并将该 IP 地址返回到 DNS 解析程序。
7. DNS 解析程序最终将获得用户所需的 IP 地址。解析程序将该值返回给 Web 浏览器。

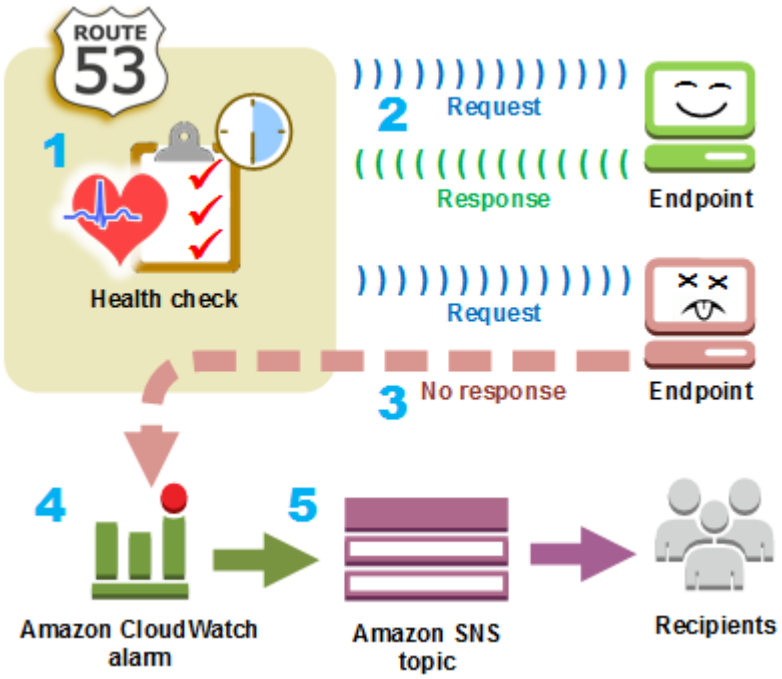
> **Note**
>
> DNS 解析程序还会将 example.com 的 IP 地址缓存您指定的一段时间，以便在下次有人浏览到 example.com 时，它可以更快地做出响应。有关更多信息，请参阅 time to live (TTL)。

8. Web 浏览器将对 www.example.com 的请求发送到它从 DNS 解析程序那里获得的 IP 地址。例如，您的内容是在 Amazon EC2 实例上运行的 Web 服务器或配置为网站终端节点的 Amazon S3 存储桶。
9. 192.0.2.44 上的 Web 服务器或其他资源将 www.example.com 的网页返回到 Web 浏览器，而 Web 浏览器会显示该页面。

Amazon Route 53 如何检查您的资源的运行状况

Amazon Route 53 运行状况检查可监控您的资源（如 Web 服务器和电子邮件服务器）的运行状况。您可以选择为运行状况检查配置 Amazon CloudWatch 警报，以便在资源不可用时收到通知。

如果您希望在资源变得不可用时收到通知，下面概述了运行状况检查的工作原理：



1. 您创建运行状况检查，并指定用于定义您希望运行状况检查如何工作的值，例如：
   - 您希望 Route 53 监控的终端节点（如 Web 服务器）的 IP 地址或域名。（您还可以监控其他运行状况检查的状态或 CloudWatch 警报的状态。）

- 您希望 Amazon Route 53 用于执行相应检查的协议：HTTP、HTTPS 或 TCP。
- 您希望 Route 53 向终端节点发送请求的频率，也就是请求时间间隔。
- 在 Route 53 认为终端节点运行状况不佳之前，终端节点必须尝试响应请求的连续次数，也就是失败阈值。
- （可选）当 Route 53 检测到终端节点运行状况不佳时，您希望接收通知的方式。配置通知时，Route 53 会自动设置 CloudWatch 警报。 CloudWatch 使用 Amazon SNS 通知用户终端节点运行状况不佳。

2. Route 53 开始以您在运行状况检查中指定的时间间隔向终端节点发送请求。

   如果终端节点响应请求，则 Route 53 会认为终端节点运行状况良好，因此不会采取任何措施。

3. 如果终端节点没有响应请求，则 Route 53 会开始计算终端节点未响应的连续请求的计数：
   - 如果计数达到为失败阈值指定的值，则 Route 53 会认为终端节点运行状况不佳。
   - 如果终端节点在计数达到故障阈值之前再次开始响应，则 Route 53 会将计数重置为 0，并且 CloudWatch 不会与您联系。
4. 如果 Route 53 认为终端节点运行状况不佳，并且您为运行状况检查配置了通知，则 Route 53 会发出通知 CloudWatch。

   如果您没有配置通知，则仍然可以在 Route 53 控制台中看到 Route 53 运行状况检查的状态。有关更多信息，请参阅 监控运行状况检查状态和获取通知。
5. 如果您为运行状况检查配置了通知，则 CloudWatch 会触发警报并使用 Amazon SNS 向指定的收件人发送通知。

除了检查指定终端节点的运行状况之外，您还可以将运行状况检查配置为检查一个或多个其他运行状况检查的运行状况，以便在指定数量的资源 (如五个 Web 服务器中的两个) 不可用时收到通知。您还可以配置运行状况检查来检查 CloudWatch 警报的状态，这样您就可以根据各种标准收到通知，而不仅仅是资源是否在响应请求。

如果您有执行相同功能的多个资源（例如 Web 服务器或数据库服务器），并且您希望 Route 53 仅将流量路由到运行状况良好的资源，则可以通过将运行状况检查与相应资源的每个记录相关联，来配置 DNS 故障转移。如果运行状况检查确定基础资源运行状况不佳，则 Route 53 会将流量从相关联的记录路由到别处。

有关使用 Route 53 监控资源运行状况的更多信息，请参阅 创建 Amazon Route 53 运行状况检查 。

Amazon Route 53 概念

下面概述了整个 Amazon Route 53 开发人员指南中所讨论的概念。

主题

域注册概念

下面概述了与域注册相关的概念。

- domain name
- domain registrar
- domain registry
- domain reseller
- top-level domain (TLD)

域名

用户在 Web 浏览器的地址栏中键入的名称 (比如 example.com)，用于访问某个网站或 Web 应用程序。要使您的网站或 Web 应用程序在 Internet 上可用，您首先要注册一个域名。有关更多信息，请参阅 域注册的工作原理。

域注册商

一家获得 ICANN（互联网名称与数字地址分配机构）认可，可以处理特定顶级域名的域名注册的公司（TLDs）。要找出域的注册商，请参阅 查找注册商。

域注册机构

有权销售具有一个特定顶级域的域的公司。例如，VeriSign是拥有出售带有.com TLD的域名的权利的注册机构。域注册机构可定义注册域的规则，比如地理 TLD 的住所要求。域注册机构还会维护具有相同 TLD 的所有域名的权威数据库。注册机构的数据库中包含一些信息，比如每个域的联系人信息和名称服务器等。

域经销商

出售注册商（比如 Amazon Registrar）的域名的公司。Amazon Route 53 是 Amazon Registrar 和我们的注册商合作者 Gandi 的域经销商。

顶级域 (TLD)

域名的最后一部分，比如 .com、.org 或 .ninja。有两种类型的顶级域：

通用顶级域

这些 TLDs 通常会让用户知道他们将在网站上找到什么。例如，具有 TLD .bike 的域名通常与摩托车或自行车企业或组织的网站有关。除了少数例外情况外，您可以使用任何您想要的通用 TLD，因此自行车俱乐部可将 .hockey TLD 用于其域名。

地理顶级域

TLDs 它们与诸如国家或城市之类的地理区域相关联。一些地理注册管理机构 TLDs 有居住地要求，而其他注册管理机构（例如）the section called ".io（英属印度洋领地）"则允许甚至鼓励将其用作通用 TLD。

有关向 Rou TLDs te 53 注册域名时可以使用的列表，请参阅可向 Amazon Route 53 注册的域。。

域名系统 (DNS) 概念

下面概述了与域名系统 (DNS) 相关的概念。

- alias record
- authoritative name server
- CIDR block
- DNS query
- DNS resolver
- Domain Name System (DNS)
- hosted zone
- IP address
- name servers
- private DNS

- recursive name server
- record (DNS record)
- reusable delegation set
- routing policy
- subdomain
- time to live (TTL)

别名记录

您可以使用 Amazon Route 53 创建的一种记录，用于将流量路由到诸如亚马逊 CloudFront 分配和 Amazon S3 存储桶之类的 Amazon 资源。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

权威名称服务器

一个名称服务器，该名称服务器具有关于域名系统 (DNS) 的一部分的明确信息，并通过返回适用的信息响应来自 DNS 解析程序的请求。例如，.com 顶级域 (TLD) 的权威名称服务器知道每个已注册 .com 域的名称服务器的名称。当 .com 权威名称服务器收到来自 example.com 的 DNS 解析程序的请求时，它会使用 example.com 域的 DNS 服务的名称服务器的名称进行响应。

Route 53 名称服务器是将 Route 53 用作 DNS 服务的每个域的权威名称服务器。这些名称服务器知道，您希望如何基于您在域的托管区域中创建的记录来路由您的域和子域的流量。（Route 53 名称服务器可存储将 Route 53 用作 DNS 服务的域的托管区域。）

例如，如果 Route 53 名称服务器收到对 www.example.com 的请求，它将找到该记录并返回记录中指定的 IP 地址（如 192.0.2.33）。

CIDR 块

CIDR 块是一种与基于 IP 的路由结合使用的 IP 范围。在 Route 53 中，你可以为 /0 到 /24 指定 /0 到 /48 之间的 IPv4 CIDR 块。 IPv6例如，一个 /24 IPv4 CIDR 块包含 256 个连续的 IP 地址。您可以将 CIDR 块（或 IP 范围）集组合到 CIDR 位置，然后反过来将其组合为可重用的 CIDR 集合。

DNS 查询

通常为由某个设备 (比如计算机或智能手机) 向与某域名关联的资源的域名系统 (DNS) 提交的请求。DNS 查询最常见的示例是，用户打开浏览器并在地址栏中键入域名。对 DNS 查询的响应通常是与诸如 Web 服务器之类的资源相关联的 IP 地址。发出请求的设备使用该 IP 地址与资源进行通信。例如，浏览器可以使用该 IP 地址从 Web 服务器中获取某个网页。

DNS 解析程序

通常由 Internet 服务提供商 (ISP) 管理的 DNS 服务器，充当用户请求与 DNS 名称服务器之间的中介。当您打开浏览器并在地址栏中输入域名时，您的查询将首先发送到 DNS 解析程序。该解析程序会与 DNS 名称服务器通信，以获取相应资源 (比如 Web 服务器) 的 IP 地址。DNS 解析程序也称为递归名称服务器，因为它会将请求发送到一系列权威 DNS 名称服务器，直到它获得返回到用户设备 (例如，笔记本电脑上的 Web 浏览器) 的响应 (通常为 IP 地址)。

域名系统 (DNS)

一个全球服务器网络，可帮助计算机、智能手机、平板电脑和其他已启用 IP 的设备之间相互通信。域名系统会将容易理解的名称 (例如 example.com) 转换为数字，这些数字称为 IP 地址，允许计算机在 Internet 上相互找到对方。

另请参阅IP address。

托管区域

一个记录容器，其中包含有关您希望如何路由域 (比如 example.com) 及其所有子域 (比如 www.example.com、retail.example.com 和 seattle.accounting.example.com) 的流量的信息。托管区域具有与相应域相同的名称。

例如，example.com 的托管区域可能包括如下两个记录：一个记录具有关于将 www.example.com 的流量路由到 IP 地址为 192.0.2.243 的 Web 服务器的信息；另一个记录具有关于将 example.com 的电子邮件路由到两个电子邮件服务器 (mail1.example.com 和 mail2.example.com) 的信息。每个电子邮件服务器还需要自己的记录。

另请参阅record (DNS record)。

IP 地址

分配给 Internet 上某个设备（例如笔记本电脑、智能手机或 Web 服务器）的一个数字，允许该设备与 Internet 上的其它设备进行通信。IP 地址采用以下格式之一：

- 互联网协议版本 4 (IPv4) 格式，例如 192.0.2.44
- 互联网协议版本 6 (IPv6) 格式，例如 2001:0 db 8:85 a 3:0000:00:00:abcd: 0001:2345

Route 53 同时支持 IPv4 和 IPv6 地址，用于以下目的：

- 对于地址，您可以创建类型为 A 的记录，或者为 IPv4 地址创建类型为 AAAA 的记录。 IPv6
- 您可以创建运行状况检查，将请求发送到地址 IPv4 或向 IPv6 地址发送请求。
- 如果 DNS 解析器位于 IPv6 网络上，则它可以使用 IPv4 或 IPv6 向 Route 53 提交请求。

名称服务器

域名系统 (DNS) 中的服务器，可帮助将域名转换为计算机用于彼此相互通信的 IP 地址。名称服务器为递归名称服务器（也称为 DNS resolver）或 authoritative name server。

有关 DNS 如何将流量路由到您的资源的概述（包括 Route 53 在此过程中的作用），请参阅 Amazon Route 53 如何为您的域路由流量。

私有 DNS

域名系统 (DNS) 的本地版本，允许您将域及其子域的流量路由到一个或多个亚马逊虚拟私有云中的亚马逊 EC2 实例 (VPCs)。有关更多信息，请参阅 使用私有托管区。

记录 (DNS 记录)

托管区域中的一个对象，用于定义您要如何路由域或子域的流量。例如，您可以为 example.com 和 www.example.com 创建记录，将流量路由到 IP 地址为 192.0.2.234 的 Web 服务器。

有关记录的更多信息（包括有关由特定于 Route 53 的记录所提供功能的信息），请参阅 将 Amazon Route 53 配置为 DNS 服务。

递归名称服务器

请参阅DNS resolver。

可重用的委派集

一组可用于多个托管区域的四个权威名称服务器。默认情况下，Route 53 会将随机选择的名称服务器分配给每个新的托管区域。为了更轻松地将大量域的 DNS 服务迁移到 Route 53，您可以创建可重用委派集，然后将可重用委派集与新的托管区域相关联。(您无法更改与现有托管区域相关联的名称服务器。)

创建一个可重用委派集，并以编程方式将其与托管区域相关联；不支持使用 Route 53 控制台。有关更多信息，请参阅亚马逊 Route 53 API 参考CreateReusableDelegationSet中的CreateHostedZone和。Amazon SDKs、和中也提供了同样的Amazon Command Line Interface功能Amazon Tools for Windows PowerShell。

路由策略

用于确定 Route 53 如何响应 DNS 查询的记录设置。Route 53 支持以下路由策略：

- 简单路由策略 - 用于将 Internet 流量路由到为您的域执行给定功能的单一资源（例如，为 example.com 网站提供内容的 Web 服务器）。

- 故障转移路由策略 - 如果您想要配置主动-被动故障转移，则可以使用该策略。
- 地理位置路由策略 - 用于根据用户的位置将 Internet 流量路由到您的资源。
- 地理位置临近度路由策略 - 用于根据资源的位置来路由流量，以及（可选）将流量从一个位置中的资源转移到另一个位置中的资源。
- 延迟路由策略 - 如果您的资源位于多个位置，并且您想要将流量路由到提供最佳延迟的资源，则可以使用该策略。
- 基于 IP 的路由策略 – 如果您希望根据用户的位置来路由流量，并且获得流量来源的 IP 地址，则可以使用该策略。
- 多值应答路由策略 - 如果您想要让 Route 53 用随机选择的正常记录（最多八条）响应 DNS 查询，则可以使用该策略。
- 加权路由策略 - 用于按照您指定的比例将流量路由到多个资源。

有关更多信息，请参阅 选择路由策略。

子域

一个域名，该域名拥有添加到已注册域名前面的一个或多个标签。例如，如果您注册了域名 example.com，则 www.example.com 为子域。如果您为 example.com 域创建了托管区域 accounting.example.com，则 seattle.accounting.example.com 为子域。

要为子域路由流量，请创建一个具有所需名称 (如 www.example.com) 的记录，并指定适用的值，例如 Web 服务器的 IP 地址。

生存时间 (TTL)

在向 Route 53 提交另一个请求以获取记录的当前值之前，您希望 DNS 解析程序缓存（存储）该记录的值的时间量（以秒为单位）。如果 DNS 解析程序在 TTL 到期之前收到对同一个域的另一个请求，则该解析程序将返回缓存的值。

较长的 TTL 会降低您的 Route 53 费用，这一点部分取决于 Route 53 响应的 DNS 查询的数量。在更改记录中的值 (例如通过更改 www.example.com 的 Web 服务器的 IP 地址) 后，较短的 TTL 会缩短 DNS 解析程序将流量路由到较旧资源的时间量。

控制和数据层面概念

以下是与 Amazon Route 53 如何将其功能划分为控制和数据层面相关的概念概述。像大多数 Amazon Web Services 服务一样，Route 53 服务包括一个控制层面，您可以通过该层面执行诸如创建、更新和

删除资源之类的管理操作；以及一个提供服务核心功能的数据层面。虽然两种功能均可靠，但控制层面已针对数据一致性进行优化，而数据层面也已针对可用性进行优化。数据层面的弹性设计使得即便是在罕见的中断事件过程中也能维持可用性，在中断事件过程中，控制层面可能不可用。为此，我们建议使用数据层面功能，其中，可用性非常重要。

对于 Route 53 的公共和私有 DNS 以及运行状况检查，控制平面位于 us- Amazon Web Services 区域 east-1 中，数据平面分布在全球各地。

Amazon Route 53 分为控制层面和数据层面，如下所示：

- 对于 Route 53 的公用和私有 DNS，控制平面由路由 53 组成 APIs，它允许您管理 DNS 条目，包括 Route 53 和流量流APIs。Route 53 控制台位于 us- Amazon Web Services 区域 east-1，但 Amazon 如果确定该区域存在损失，则 53 号公路控制台将由 us-west-2 提供服务。 Amazon Web Services 区域数据层面是权威 DNS 服务，它运行在 200 多个接入点 (POP) 位置，根据您的托管区域和运行状况检查数据应答 DNS 查询。
- 对于 Route 53 运行状况检查，控制平面由可用于创建、更新和删除运行状况检查的 Route 5 APIs 3 组成。Route 53 运行状况检查控制台位于 us- Amazon Web Services 区域 east-1，但 Amazon 如果确定该区域存在损害，则 Route 53 运行状况检查控制台将由 us-west-2 提供服务。 Amazon Web Services 区域数据层面是全球分布式服务，它可执行运行状况检查、汇总结果并将它们传送到 Route 53 公有和私有 DNS 以及 Amazon Global Accelerator 的数据层面。
- 对于 R oute 53 VPC 解析器，控制平面由 VPC 解析器组成 APIs ，允许您管理 Amazon VPC 设置、解析器规则、查询日志策略和 DNS 防火墙策略。数据层面是 DNS 解析器服务，用于应答 VPC 中的 DNS 查询、将查询转发给其他解析器的终端节点以及应用策略来筛选 DNS 查询的 DNS 防火墙数据层面。VPC Resolver 是一项区域服务，其控制平面和数据平面在每个 Amazon Web Services 区域服务中独立运行。
- Route 53 域注册仅在 us-east-1 Amazon Web Services 区域中的控制层面上进行管理。

有关数据平面、控制平面以及如何 Amazon 构建服务以满足高可用性目标的更多信息，请参阅 Amazon Builders 库中的 “使用可用区的静态稳定性” 论文。

运行状况检查概念

下面概述了与 Amazon Route 53 运行状况检查相关的概念。

- DNS failover
- endpoint
- health check

DNS 故障转移

将流量从运行状况不佳的资源路由到运行状况良好的资源的一种方法。当您有多个资源（例如，多个 Web 服务器或邮件服务器）执行同一功能时，可以将 Route 53 运行状况检查配置为检查您的资源的运行状况，并在您的托管区域中配置记录，以便仅将流量路由到运行状况良好的资源。

有关更多信息，请参阅 配置 DNS 故障转移。

endpoint

您将运行状况检查配置为监控其运行状况的资源 (比如 Web 服务器或电子邮件服务器)。你可以按 IPv4 地址 (192.0.2.243)、地址 (2001:0 db 8:85 a 3:0000:00:00:abcd: 0001:2345) 或 IPv6 域名 (example.com) 指定终端节点。

> **Note**
>
> 您还可以创建运行状况检查，以监控其他运行状况检查的状态或监控警报的 CloudWatch 警报状态。

运行状况检查

一个 Route 53 组件，让您可以执行以下操作：

- 监控指定终端节点 (比如 Web 服务器) 的运行状况是否良好
- (可选) 当某个终端节点运行状况不佳时收到通知
- (可选) 配置 DNS 故障转移，从而让您可以将 Internet 流量从运行状况不佳的资源重新路由到运行状况良好的资源

有关如何创建和使用运行状况检查的更多信息，请参阅创建 Amazon Route 53 运行状况检查 。

如何开始使用 Amazon Route 53

有关开始使用 Amazon Route 53 的信息，请参阅本指南中的以下主题：

- 设置 Amazon Route 53，其中说明了如何注册 Amazon、如何保护对 Amazon 账户的访问以及如何设置对 Route 53 的编程访问权限
- 开始使用 Amazon Route 53，其中阐述了如何注册域名、如何创建 Amazon S3 存储桶并将其配置为托管静态网站，以及如何将 Internet 流量路由到网站

访问 Amazon Route 53

您可以通过如下方法访问 Amazon Route 53：

- Amazon Web Services 管理控制台— 本指南中的过程解释了如何使用 Amazon Web Services 管理控制台 来执行任务。
- Amazon SDKs— 如果您使用的是 Amazon 为提供 SDK 的编程语言，则可以使用 SDK 访问 Route 53。 SDKs 简化身份验证，轻松与开发环境集成，并提供对 Route 53 命令的轻松访问。有关更多信息，请参阅用于 Amazon Web Services 的工具。
- Route 53 API - 如果要使用软件开发工具包不可用的编程语言，请参阅 Amazon Route 53 API 参考，以了解有关 API 操作及如何发出 API 请求的信息。
- Amazon Command Line Interface - 有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的开始设置 Amazon Command Line Interface。
- Amazon Tools for Windows PowerShell – 有关更多信息，请参阅 Amazon Tools for PowerShell 用户指南中的设置 Amazon Tools for Windows PowerShell。

Amazon Identity and Access Management

Amazon Route 53 与 Amazon Identity and Access Management (IAM) 集成，该服务允许您的组织执行以下操作：

- 在贵组织的 Amazon 账户下创建用户和群组
- 在 Amazon 账户中的用户之间轻松共享您的账户资源
- 为每个用户分配具有唯一性的安全凭证
- 精确地控制用户访问服务和资源的权限

例如，您可以将 IAM 与 Route 53 配合使用，以控制您 Amazon 账户中的哪些用户可以创建新的托管区域或更改记录。

有关 IAM 的一般信息，请参阅以下内容：

- Amazon Route 53 中的 Identity and Access Management
- Identity and Access Management (IAM)
- IAM 用户指南

Amazon Route 53 定价和计费

与其他 Amazon 产品一样，使用 Amazon Route 53 没有合同或最低承诺。您只需为您配置的托管区域和 Route 53 响应的 DNS 查询数量付费。有关更多信息，请参阅 Amazon Route 53 定价。

有关 Amazon 服务账单的信息，包括如何查看账单和管理账户和付款，请参阅Amazon Billing 用户指南。

将 Route 53 与 S Amazon DK 一起使用

Amazon 软件开发套件 (SDKs) 可用于许多流行的编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。

SDK 文档
Amazon CLI
适用于 Java 的 Amazon SDK
适用于 JavaScript 的 Amazon SDK
适用于 .NET 的 Amazon SDK
适用于 PHP 的 Amazon SDK
Amazon Tools for PowerShell
适用于 Python (Boto3) 的 Amazon SDK
适用于 Ruby 的 Amazon SDK
适用于 SAP ABAP 的 Amazon SDK

有关特定于 Route 53 的示例，请参阅 使用 Amazon SDK 的 Route 53 代码示例。

开始使用 Amazon Route 53

首先从基本操作开始，利用 Amazon Route 53 注册一个域并配置 Route 53 来响应解析到静态网站的 DNS 查询。第一个教程在打开的 Amazon S3 存储桶中托管一个静态网站，第二个教程使用 Amazon CloudFront 分发为该网站提供 SSL/TLS。

估算费用

- 注册域需要缴纳年费，金额从 9 USD 到数百美元不等，具体取决于是否为顶级域，例如 .com。有关更多信息，请参阅 Route 53 域注册定价。此费用不可退款。
- 当您注册域时，我们会自动创建一个与该域同名的托管区域。可使用该托管区域指定希望 Route 53 将域流量路由到哪里。
- 在本教程中，您将创建 Amazon S3 存储桶并上传示例网页。如果您是新 Amazon 客户，则可以免费开始使用 Amazon S3。如果您是现有 Amazon 客户，则费用取决于您存储的数据量、请求数据的次数以及传输的数据量。有关更多信息，请参阅 Amazon S3 定价。
- CloudFront 费用取决于您的数据请求数量、您使用的边缘站点数量以及传输的数据量。有关更多信息，请参阅CloudFront 定价。

主题

- 设置 Amazon Route 53
- 将您的域用于 Amazon S3 存储桶中的静态网站
- 使用 Amazon CloudFront 发行版为静态网站提供服务

设置 Amazon Route 53

本节中的概述和过程可帮助您入门 Amazon。

主题

- 注册获取 Amazon Web Services 账户
- 保护 IAM 用户
- 下载工具

注册获取 Amazon Web Services 账户

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

报名参加 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 Amazon Web Services 账户，就会创建Amazon Web Services 账户根用户一个。根用户有权访问该账户中的所有 Amazon Web Services 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看您当前的账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

下载工具

Amazon Web Services 管理控制台 包括适用于 Amazon Route 53 的控制台，但如果您想以编程方式访问服务，请参阅以下内容：

- API 指南记录了服务支持的操作，并提供了指向相关 SDK 和 CLI 文档的链接：
  - Amazon Route 53 API 参考

- 要调用 API 而不必处理诸如组装原始 HTTP 请求之类的低级细节，可以使用 S Amazon DK。它们 Amazon SDKs 提供了封装服务功能的函数和数据类型。 Amazon 要下载 S Amazon DK 并访问安装说明，请参阅相应页面：
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  有关完整列表 Amazon SDKs，请参阅亚马逊 Web Services 工具。
- 您可以使用 Amazon Command Line Interface (Amazon CLI) 通过命令行控制多个 Amazon 服务。您还可以使用脚本自动执行命令。有关更多信息，请参阅 Amazon Command Line Interface。
- Amazon Tools for Windows PowerShell 支持这些 Amazon 服务。有关更多信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考。

将您的域用于 Amazon S3 存储桶中的静态网站

本教程向您展示如何使用 Amazon Route 53 将域的 DNS 流量路由到托管静态网站的 Amazon Simple Storage Service 存储桶。您将创建将域指向 S3 网站端点的别名记录。

本教程是完整静态网站设置工作流程的一部分。有关将流量路由到任何 S3 存储桶的一般信息，请参阅将流量路由到在 Amazon S3 存储桶中托管的网站。

完成后，访客可以使用自定义域名访问您的静态网站。

> **Note**
>
> 您也可以将现有域转移到 Route 53，但与注册一个新域相比，这一过程更复杂且更耗时。有关更多信息，请参阅 将域注册转移到 Amazon Route 53。

先决条件

在开始之前，请完成如下步骤：

- 完成 设置 Amazon Route 53 中的步骤。
- 使用 Amazon Route 53 注册域名。有关更多信息，请参阅 注册新域。
- 为静态网站托管配置 Amazon Simple Storage Service 存储桶。有关完整说明，请参阅 Amazon Simple Storage Service 用户指南中的教程：使用注册到 Route 53 的自定义域配置静态网站。

完成 Amazon Simple Storage Service 教程后，您将获得：

- 为网站托管和重定向配置的 Amazon S3 存储桶（如果使用 www 子域）
- 网站内容已上传到您的存储桶
- 为您的网站存储桶配置公有访问权限

步骤 1：将您的域名的 DNS 流量路由到您的网站存储桶

现在，您已经为静态网站托管配置 Amazon Simple Storage Service 存储桶，请使用 Amazon Route 53 将您域的 DNS 流量路由到该存储桶。这样，访客就可以使用自定义域名访问您的网站。

将流量路由到您的网站

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。

> **Note**
>
> 当您注册域时，Amazon Route 53 将自动使用相同的名称创建一个托管区域。托管区域包含有关您希望 Route 53 如何路由域流量的信息。

3. 在托管区域列表中，选择您的域名。
4. 选择创建记录。
5. 指定以下值：

   记录名称

   留空以为根域创建记录。

   记录类型

   选择 A-将流量路由到一个 IPv4 地址和一些 Amazon 资源。

Alias

开启别名。

将流量路由到

选择 S3 网站端点的别名。

请选择在其中创建 S3 存储桶的区域。

选择 S3 存储桶。存储桶名称应与域名称相匹配。在列表中，存储桶名称将与创建存储桶所在区域的 Amazon S3 网站端点一起显示，例如 `s3-website-us-west-1.amazonaws.com (example.com)`。

如果您的存储桶未显示在列表中，请输入在其中创建存储桶的区域的 Amazon S3 网站端点，例如 **`s3-website-us-west-2.amazonaws.com`**。有关 Amazon S3 网站端点的完整列表，请参阅 Amazon S3 网站端点。

评估目标运行状况

接受默认值否。

6. 选择创建记录。

（可选）要为您的子域添加别名记录 (**`www.example.com`**)

如果您为子域创建了存储桶，请同时为其添加别名记录。

1. 选择创建记录。
2. 指定以下值：

记录名称

输入 **`www`**。

记录类型

选择 A-将流量路由到一个 IPv4 地址和一些 Amazon 资源。

Alias

开启别名。

将流量路由到

选择 S3 网站端点的别名。

请选择在其中创建 S3 存储桶的区域。

为子域选择 S3 存储桶，例如 `s3-website-us-west-2.amazonaws.com (www.example.com)`。

评估目标运行状况

接受默认值否。

3. 选择创建记录。

第 2 步：测试您的网站

要验证网站是否正常运行，请打开 Web 浏览器并浏览到以下内容 URLs：

- http://*your-domain-name*，例如，`example.com`— 显示*your-domain-name*存储桶中的索引文档
- http://www。 *your-domain-name*例如，`www.example.com`— 将您的请求重定向到存储桶 *your-domain-name*

在某些情况下，您可能需要清除缓存才能看到预期行为。

有关路由 Internet 流量的更多高级信息，请参阅 将 Amazon Route 53 配置为 DNS 服务。有关将互联网流量路由到 Amazon 资源的信息，请参阅将互联网流量路由到您的 Amazon 资源。

> **Note**
>
> Amazon S3 不支持对该网站进行 HTTPS 访问。如果您想使用 HTTPS，则可以使用亚马逊 CloudFront 为托管在 Amazon S3 上的静态网站提供服务。有关更多信息，请参阅 使用 Amazon CloudFront 发行版为静态网站提供服务。

使用 Amazon CloudFront 发行版为静态网站提供服务

本教程向您展示如何使用 Amazon Route 53 将您的域名的 DNS 流量路由到为静态网站提供服务的亚马逊 CloudFront 分配。您将创建别名记录，将您的域名和子域名指向 CloudFront 分配。

本教程是完整静态网站设置工作流程的一部分。有关将流量路由到任何 CloudFront 分布的一般信息，请参阅使用您的域名将流量路由到 Amazon CloudFront 分配。

完成后，访客可以使用您的自定义域名访问您的网站，该域名由提供 HTTPS 安全性 CloudFront。

先决条件

在开始之前，请完成如下步骤：

- 完成 设置 Amazon Route 53 中的步骤。
- 使用 Amazon Route 53 注册域名。有关更多信息，请参阅 注册新域。
- 使用亚马逊 CloudFront 和亚马逊简单存储服务创建安全的静态网站。有关完整说明，请参阅《Amazon CloudFront 开发者指南》中的安全静态网站入门。

完成 Amazon CloudFront 教程后，您将获得：

- 您的域名的 SSL/TLS 证书 Amazon Certificate Manager
- 为网站托管和重定向配置的 Amazon S3 存储桶
- CloudFront 您的根域名和子域名的发行版

步骤 1：将您的域名的 DNS 流量路由到您的 CloudFront 分配

现在，您的网站已经有了亚马逊 CloudFront 分配，请使用 Amazon Route 53 将您的域名的 DNS 流量路由到分配。这样，访客就可以使用自定义域名访问您的网站。

有关将流量路由到 CloudFront 分布的更多信息，请参阅使用您的域名将流量路由到 Amazon CloudFront 分配。

将流量路由到您的网站

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。

> **Note**
>
> 当您注册域时，Amazon Route 53 将自动使用相同的名称创建一个托管区域。托管区域包含有关您希望 Route 53 如何路由域流量的信息。

3. 在托管区域列表中，选择您的域名。
4. 选择创建记录。
5. 指定以下值：

   记录名称

   对于您的子域记录，请输入 **www**。

   记录类型

   选择 A-将流量路由到一个 IPv4 地址和一些 Amazon 资源。

   Alias

   开启别名。

   将流量路由到

   选择 “ CloudFront 分发别名”。

   选择 us-east-1 区域。

   选择您的 CloudFront 发行版。分发名称应与 CloudFront 控制台的 “域名” 列中显示的名称相匹配，例如`dddjjjkkk.cloudfront.net`。

   评估目标运行状况

   接受默认值否。
6. 选择创建记录。

为您的根域（**example.com**）添加别名记录

还要为根域添加别名记录，这样它就会指向将流量重定向到`www.example.com`的 CloudFront分发。

1. 选择创建记录。
2. 指定以下值：

   记录名称

   留空以为根域创建记录。

   记录类型

   选择 A-将流量路由到一个 IPv4 地址和一些 Amazon 资源。

Alias

开启别名。

将流量路由到

选择 “ CloudFront 分发别名”。

选择 us-east-1 区域。

选择您的根域 CloudFront 分布。

评估目标运行状况

接受默认值否。

3. 选择创建记录。

第 2 步：测试您的网站

要验证网站是否正常运行，请打开 Web 浏览器并浏览到以下内容 URLs：

- https://www。 *your-domain-name* ，例如，www.example.com— 显示*www.your-domain-name*存储桶中的索引文档
- https:// *your-domain-name* 例如，example.com— 将您的请求重定向到存储桶 *www.your-domain-name*

在某些情况下，您可能需要清除缓存才能看到预期行为。

有关路由 Internet 流量的更多高级信息，请参阅 将 Amazon Route 53 配置为 DNS 服务。有关将互联网流量路由到 Amazon 资源的信息，请参阅将互联网流量路由到您的 Amazon 资源。

与其他 服务集成

您可以将 Amazon Route 53 与其他 Amazon 服务集成，以记录发送到 Route 53 API 的请求，监控您的资源状态并为您的资源分配标签。此外，可以使用 Route 53 将互联网流量路由到您的 Amazon 资源。

主题

记录、监控和添加标签

Amazon CloudTrail

Amazon Route 53 与 Amazon CloudTrail一项服务集成，该服务可捕获有关您的 Amazon 账户发送到 Route 53 API 的每个请求的信息。您可以使用 CloudTrail 日志文件中的信息来确定向 Route 53 发出了哪些请求、发出每个请求的源 IP 地址、谁发出了请求、何时发出请求等。

有关更多信息，请参阅 使用记录亚马逊 Route 53 API 调用 Amazon CloudTrail。

Amazon CloudWatch

您可以使用 Amazon CloudWatch 来监控 Route 53 运行状况检查的状态（健康或不健康）。运行状况检查监控 Web 应用程序、Web 服务器以及其他资源的运行状况和性能。Route 53 按照您指定的固定间隔，通过互联网向您的应用程序、服务器或其它资源自动提交请求，以验证其是否可到达、是否可用及功能是否正常。

有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

标签编辑器

标签是您分配给 Amazon 资源的标签，包括 Route 53 域、托管区域和运行状况检查。每个标签都由键和值组成，这两个参数都由您定义。例如，您可以将一个键为“Customer”、值为“Example Corp.”的标签分配给域注册。您可以将标签用于多种用途；一种常见用途是对 Amazon 成本进行分类和跟踪。

有关更多信息，请参阅 给 Amazon Route 53 资源贴标签。

将流量路由到其他 Amazon 资源

您可以使用 Amazon Route 53 将流量路由到各种 Amazon 资源。

Amazon API Gateway

Amazon API Gateway 允许您在任何规模 APIs 上创建、发布、维护、监控和保护。您可以创建 APIs 该访问权限 Amazon 或其他 Web 服务，以及存储在 Amazon 云中的数据。

您可以使用 Route 53 将流量路由到 API Gateway API。有关更多信息，请参阅 使用域名将流量路由到 Amazon API Gateway API。

Amazon CloudFront

要加快网页内容的交付，您可以使用内容分发网络 (CDN) Amazon CloudFront。 Amazon CloudFront 可以使用全球边缘站点网络交付您的整个网站，包括动态、静态、流媒体和交互式内容。 CloudFront 将对您的内容的请求路由到边缘站点，从而为您的用户提供最低延迟。您可以使用 Route 53 将您的域的流量路由到您的 CloudFront 分配。有关更多信息，请参阅 使用您的域名将流量路由到 Amazon CloudFront 分配。

Amazon EC2

Amazon 在 Amazon 云端 EC2 提供可扩展的计算容量。您可以使用预配置的模板（Amazon 系统映像或 AMI）启动 EC2 虚拟计算环境（实例）。启动 EC2 实例时，EC2 会自动安装操作系统（Linux 或 Microsoft Windows）和 AMI 中包含的其他软件，例如 Web 服务器或数据库软件。

如果您在 EC2 实例上托管网站或运行 Web 应用程序，则可以使用 Route 53 将您的域（例如 example.com）的流量路由到您的服务器。有关更多信息，请参阅 将流量路由到 Amazon EC2 实例。

Amazon Elastic Beanstalk

如果您使用 Amazon Elastic Beanstalk 在 Amazon 云中部署和管理应用程序，则可以使用 Route 53 将您的域（例如 example.com）的 DNS 流量路由到 Elastic Beanstalk 环境。有关更多信息，请参阅 将流量路由到 Amazon Elastic Beanstalk 环境。

Elastic Load Balancing

如果您在多个 Amazon EC2 实例上托管网站，则可以使用 Elastic Load Balancing (ELB) 负载均衡器将流量分配到多个实例。当网站的流量随时间发生变化时，ELB 服务可自动缩放负载均衡器。负载均衡器还会监控其已注册实例的运行状况，并且只将域流量路由到运行状况良好的实例。

您可以使用 Route 53 将域的流量路由到传统、应用程序或网络负载均衡器。有关更多信息，请参阅 将流量路由到 ELB 负载均衡器。

Amazon Lightsail

Amazon Lightsail 提供在云中部署和管理网站、Web 应用程序和数据库所需的计算、存储及网络容量与功能，并按每月价格收费，费用优惠、可预测。

如果您使用 Lightsail，则可以使用 Route 53 将流量路由到您的 Lightsail 实例。有关更多信息，请参阅使用 Route 53 将域指向 Amazon Lightsail 实例。

Amazon S3

Amazon Simple Storage Service (Amazon S3) 提供安全、持久、高度可扩展的云存储。您可以配置 S3 存储桶，以托管能够包含网页和客户端脚本的静态网站。(S3 不支持服务器端脚本编写。) 您可以使用 Route 53 将流量路由到 Amazon S3 存储桶。有关更多信息，请参阅以下主题：

- 有关将流量路由到存储桶的信息，请参阅 将流量路由到在 Amazon S3 存储桶中托管的网站。
- 有关如何在 S3 存储桶中托管静态网站的更详细信息，请参阅 开始使用 Amazon Route 53。

Amazon Virtual Private Cloud (Amazon VPC)

接口终端节点允许您连接到由提供支持的服务 Amazon PrivateLink。这些服务包括一些 Amazon 服务、由其他 Amazon 客户和合作伙伴自行托管的服务 VPCs （称为端点服务）以及支持的 Amazon Web Services Marketplace 合作伙伴服务。

您可以使用 Route 53 将流量路由到接口端点。有关更多信息，请参阅 使用域名将流量路由到 Amazon Virtual Private Cloud 接口终端节点。

Amazon WorkMail

如果您使用亚马逊 WorkMail 发送企业电子邮件，并且使用 Route 53 作为 DNS 服务，则可以使用 Route 53 将流量路由到您的亚马逊 WorkMail 电子邮件域。有关更多信息，请参阅 将流量路由到 Amazon WorkMail。

有关更多信息，请参阅 将互联网流量路由到您的 Amazon 资源。

DNS 域名格式

域名 (包括域、托管区域和记录的名称) 由一系列以点分隔的标签组成。每个标签最长可为 63 个字节。域名的总长度不能超过 255 字节，包括点。Amazon Route 53 支持任何有效的域名。

命名要求取决于您是注册域名还是指定托管区域或记录的名称。请参阅适用的主题。

为域名注册设置域名格式

对于域名注册，域名只能包含字符 a-z、0-9 和 - (连字符) 。不能在标签开头或结尾指定连字符。

有关如何注册国际化域名 (IDN) 的信息，请参阅设置国际化域名的格式。

为托管区域和记录设置域名格式

对于托管区域和记录，域名可以包含以下任何可输出的 ASCII 字符 (不包括空格) :

- a-z
- 0-9
- - (连字符)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

Amazon Route 53 会将字母字符存储为小写字母 (a-z)，无论您指定将其存储为大写字母、小写字母还是转义码中的对应字母。

如果您的域名包含以下任意字符，则必须使用 \###### 格式的转义码指定字符 :

- 八进制字符 000 到 040 (十进制 0 到 32，十六进制 0x00 到 0x20)
- 八进制字符 177 到 377 (十进制 127 到 255，十六进制 0x7F 到 0xFF)
- . (句点) ，八进制字符 056 (十进制 46，十六进制 0x2E) ，当在域名中用作字符时。使用 . 作为标签之间的分隔符时，不需要使用转义码。

如果域名包含除 a 到 z、0-9、– (连字符) 或 _ (下划线) 之外的任意字符，Route 53 API 操作会将这些字符作为转义码返回。无论您在创建实体时将字符指定为字符还是转义码，都是如此。Route 53 控制台会将字符显示为字符，而不显示为转义码。

有关与八进制代码对应的 ASCII 字符的列表，请在 Internet 上搜索“ASCII 表”。

要指定国际化域名 (IDN)，请将其转换为域名代码。有关更多信息，请参阅 设置国际化域名的格式。

在托管区域和记录的名称中使用星号 (*)

您可以创建名称中包含 * 的托管区域和记录。

托管区域

- 域名最左侧的标签中不能包含 *。例如，不允许使用 *.example.com。
- 如果在其他位置包含 *，DNS 会将其视为 * 字符 (ASCII 42)，而不是通配符。

记录

DNS 会根据 * 字符出现在名称中的位置将它作为通配符或作为 * 字符 (ASCII 42) 来处理。请注意以下有关在记录的名称中使用 * 作为通配符的限制：

- * 必须替换域名中最左侧的标签，例如 *.example.com 或 *.acme.example.com。如果在任何其他位置包含 *（例如 prod.*.example.com），DNS 会将其视为 * 字符 (ASCII 42)，而不是通配符。
- * 必须替换整个标签。例如，您不能指定 *prod.example.com 或 prod*.example.com。
- 具体的域名优先。例如，如果您为 *.example.com 和 acme.example.com 创建记录，Route 53 始终使用 acme.example.com 记录中的值响应对 acme.example.com 的 DNS 查询。
- * 应用到针对包含星号的子域级别的 DNS 查询，以及该子域的所有子域。例如，如果您创建了名为 *.example.com 的记录，Route 53 使用该记录中的值来响应对 zenith.example.com、acme.zenith.example.com 和 pinnacle.acme.zenith.example.com（如果该托管区域没有任何类型的记录）的 DNS 查询。

  如果您创建名为 *.example.com 的记录并且没有 example.com 记录，Route 53 使用 `NXDOMAIN`（不存在域）响应对 example.com 的 DNS 查询。

> **Note**
>
> 如果您将 Route 53 与 Amazon Certificate Manager 结合使用，请注意，ACM 通配符证书仅保护一个子域级别。例如，*.example.com 的 ACM 证书可保护 login.example.com 和 test.example.com，但不保护 test.login.example.com。有关更多信息，请参阅 Amazon Certificate Manager 证书特征和限制。

- 您可以配置 Route 53，使其对针对相同级别的所有子域以及针对域名的 DNS 查询返回相同的响应。例如，您可以配置 Route 53 以使用 example.com 记录响应对 acme.example.com 和 zenith.example.com 等的 DNS 查询。执行以下步骤：

  1. 为域创建记录，如 example.com。
  2. 为子域创建别名记录，如 *.example.com。将您在步骤 1 中创建的记录指定作为别名记录的目标。

- 不能使用 * 作为类型为 NS 的记录的通配符。

设置国际化域名的格式

在注册新域名或创建托管区域和记录时，您可以指定除 a-z 以外的其它字符（例如，法语中的 ç）、其它字母表中的字符（例如西里尔字母或阿拉伯字母），也可以指定中文、日语或韩语中的字符。Amazon Route 53 在域名代码中存储这些国际化域名 (IDN)，域名代码将 Unicode 字符表示为 ASCII 字符串。

如果您正在注册域名，请注意以下事项：

- 只有当顶级域 (TLD) 支持 IDN 并支持要使用的语言时，才能使用 a-z、0-9 和 -（连字符）以外的字符。要确定 TLD 支持哪些语言，请参阅可向 Amazon Route 53 注册的域。。
- 如果名称仅包含字母 a-z，则可以使用不支持的语言指定名称。例如，如果 TLD 不支持法语，但您想要使用的名称仅包含没有变音符号的字符 a-z，您仍可以使用该名称。在此示例中，允许使用包含“c”的名称；不允许使用包含“ç”的名称。
- 如果 TLD 不支持 IDN 或不支持您希望用于域名的语言，则即使域名代码仅包含 a-z、0-9 和 -，您也无法在 域名代码中指定该名称。

以下示例显示了国际化域名“中国.asia”的域名代码表示形式：

```
xn--fiqs8s.asia
```

当您在新式浏览器的地址栏中输入 IDN 时，浏览器会将其转换为域名代码，然后再提交 DNS 查询或发出 HTTP 请求。

如何输入 IDN 取决于您要创建的内容（域名、托管区域或记录）以及创建方式 (API、软件开发工具包或 Route 53 控制台)：

- 如果您使用的是 Route 53 API 或 Amazon 开发工具包之一，则可以编程方式将 Unicode 值转换为域名代码。例如，如果您使用 Java，则可使用 java.net.IDN 库的 toASCII 方法将 Unicode 值转换为域名代码。
- 如果您使用 Route 53 控制台来注册域名，则可将名称（包括 Unicode 字符）粘贴到名称字段中，然后控制台会将该值转换为域名代码，再进行保存。
- 如果您使用 Route 53 控制台来创建托管区域或记录，则需在相应的 Name（名称）字段中输入名称之前先将域名转换为域名代码。有关在线转换器的信息，请在 Internet 上搜索“域名代码转换器”。

如果您要注册域名，请注意并非所有顶级域 (TLD) 都支持 IDN。有关 Route 53 支持的 TLD 列表，请参阅 可向 Amazon Route 53 注册的域。。已记录不支持 IDN 的 TLD。

使用 Amazon Route 53 注册和管理域

如果您要获取新域名，例如 URL http://example.com 的 example.com 部分，则可向 Amazon Route 53 注册该域名。也可以将现有域的注册从其它注册商转移到 Route 53 或将向 Route 53 进行的域注册转移到其它注册商。

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

本章中的过程介绍如何使用 Route 53 控制台注册和转移域，以及如何编辑域设置和查看域状态。如果您只想注册和管理几个域，则使用控制台是最简单的方法。

如果您需要注册和管理许多域，您可能更喜欢以编程方式进行更改。有关更多信息，请参阅 设置 Amazon Route 53。

> **Note**
>
> 如果您使用的是已存在 Amazon SDK 的语言，请使用 SDK，而不是尝试完成 APIs。 SDKs 使身份验证更简单，可轻松与开发环境集成，并提供对 Route 53 命令的轻松访问。

我们提供的域名注册服务遵循我们的域名注册协议。

主题

- 为域配置 DNSSEC
- 查找注册商以及有关域的其他信息
- Deleting a domain name registration（删除域名注册）
- 就域名注册问题联系 Su Amazon pport
- 下载域账单报告
- 可向 Amazon Route 53 注册的域。

注册新域

本节涵盖以下有关使用 Amazon Route 53 注册新域的主题：

1. 注册新域:
   - 了解使用 Route 53 控制台注册新域的 step-by-step程序。
   - 了解域名注册的注意事项和先决条件，例如就问题、定价、支持的顶级域名 (TLDs) 和自动创建托管区域等问题与 Support 联系 Amazon 。
2. 您在注册或转移域时指定的值:
   - 了解注册或转移域时需要提供的值，包括联系信息、隐私保护设置和自动续订选项。
   - 了解更改某些值（例如域所有者或注册人的电子邮件地址）的含义。
3. Amazon Route 53 在您注册域时返回的值:
   - 了解 Route 53 在成功注册域后返回的值，包括注册日期、到期日期、域状态代码、转移锁定状态和名称服务器。
4. Viewing the status of a domain registration（查看域注册的状态）:
   - 了解如何查看域注册的当前状态，包括 ICANN 状态代码以及需要采取的任何行动，例如验证注册人的电子邮件地址。

注册新域

注册新域或更新现有域的名称服务器

您可以将 Amazon Route 53 与您在 Route 53 注册的域以及您在其它 DNS 提供商处注册的域一起使用。根据您的 DNS 提供商，选择以下过程之一以在 Route 53 中注册并使用新域：

- 对于注册新域，请参阅 要使用 Route 53 注册域。
- 对于现有域，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

- 有关将域移到其它注册商的信息，请参阅当您想使用其它 DNS 服务更新名称服务器时。

域注册的注意事项

在开始之前，请注意以下事项：

联系 Su Amazon pport

如果您在注册域名时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

域注册定价

有关注册域的费用的信息，请参阅域注册的 Amazon Route 53 定价。

支持的域

有关支持的列表 TLDs，请参阅可向 Amazon Route 53 注册的域。 。

注册域后，您不能更改域名

如果您意外地注册了错误的域名，将无法进行更改。而是需要注册新的域名并指定正确的名称。您也无法获得意外注册域名的退款。

Amazon 积分

您不能使用 Amazon 积分来支付在 Route 53 上注册新域名的费用。

特殊或优惠的价格

TLD 注册表向一些域名分配了特殊或优惠的价格。您无法使用 Route 53 注册具有特殊或优惠价格的域。

托管区域的费用

您向 Route 53 注册某个域时，我们将为该域自动创建一个托管区域，且除了域注册的年费外，还将对该托管区域收取少量的月度费用。在此托管区域中，您可以存储有关如何将域的流量（例如路由到 Amazon EC2 实例或 CloudFront 分配）的信息。如果您不想立即使用域，则可删除该托管区域；如果在注册域后的 12 小时内删除托管区域，您的 Amazon 账单中将不会包含有关托管区域的任何费用。我们还会针对所收到的对域的 DNS 查询收取少量费用。有关更多信息，请参阅 Amazon Route 53 定价。

替换域的托管区域

如果您为域创建新托管区，则还必须更新域的名称服务器，以将这些名称服务器用作新的托管区。有关详细信息，请参阅 替换在 Route 53 注册的域的托管区域

要使用 Route 53 注册域

要使用 Route 53 注册域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择域，然后选择已注册的域。
3. 在已注册的域页面上，选择注册域。

   a. 在搜索域部分中，输入要注册的域名，选择搜索，了解该域名是否可用。

      如果要注册的域名包含 a-z、A-Z、0-9 和 -（连字符）以外的字符，请注意以下事项：

      - 您可以使用适当的字符输入名称。您不需要将名称转换为 Punycode。
      - 此时将显示语言列表。选择指定名称所用的语言。例如，如果您输入“příklad”（翻译成捷克语即“示例”），请选择捷克语 (CES) 或捷克语 (CZE)。

      > **Note**
      >
      > 对于具有多个代码的语言，您可能需要尝试下这些代码。尽管 CES 和 CZE 意思相同，但有些 TLD 注册表只支持其中一个。

      有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。

      如果您输入的域可用，则系统会显示；如果没有该域，则类似的域将显示为建议。

      最多可以选择注册五个域。您选择的域将出现在已选择的域列表中。

   b. 要注册多个域，请重复步骤 3a 到 3b。
4. 选择继续结账。
5. 在定价页面上，选择您想要注册域的年限，以及您是否希望我们在到期日期之前自动续订您的域注册。

> **Note**
>
> 域名注册和续订不可退款。如果您启用自动域续订，并且在我们续订注册之后决定不再需要该域名，您无法获得续订费用的退款。

选择下一步。

6. 在联系信息页面上，输入域注册人、管理员、技术和账单联系人的联系信息。您在此处输入的值将应用于您要注册的所有域。有关更多信息，请参阅 您在注册或转移域时指定的值。

> **Important**
>
> 根据 ICANN 转移策略，您在域注册期间列为注册人的联系人将拥有作为域名的注册名称持有者的某些权利。大多数域将在关闭 Amazon Web Services 账户 后被删除（有关更多信息，请参阅 我的 Amazon 账户已关闭或永久关闭，并且我的域已注册到 Route 53），但是，如果域保持在关闭的账户中，您列为注册人的联系人可以请求将域名转移给外部注册商。因此，重要的是，您列出的注册人联系人要么是您自己，要么是您信任的负责任的其他人。

请注意以下注意事项：

名字和姓

对于 First Name 和 Last Name，我们建议您指定官方 ID 上的名称。对于域设置的某些更改，有些域注册机构要求您提供身份证明。您的 ID 的姓名必须与该域的注册联系人的姓名匹配。

不同联系人

默认情况下，我们对全部三个联系人使用相同信息。如果要为一个或多个联系人输入不同的信息，请将与注册人相同切换开关的值更改为关闭位置。

> **Note**
>
> 对于 .it 域，注册者和管理联系人必须相同。

> **Note**
>
> 对于 .jp 域，技术和管理联系人必须相同。

多个域

如果您要注册多个域，我们将对所有域使用相同的联系人信息。

其他必要信息

对于某些顶级域名 (TLDs)，我们需要收集其他信息。对于这些 TLDs，请在邮政/邮政编码字段后输入适用的值。

Privacy protection（隐私保护）

选择是否要向 WHOIS 查询隐藏您的联系人信息。

> **Note**
>
> 必须为管理员、注册人、技术和账单联系人指定相同的隐私设置。

有关更多信息，请参阅以下主题：

- 启用或禁用域联系信息的隐私保护
- 可向 Amazon Route 53 注册的域。

> **Note**
>
> 要为 .uk、.co.uk、.me.uk 和 .org.uk 域启用隐私保护，您必须打开支持案例并请求隐私保护。

选择下一步。

7. 在预览页面上，检查您输入的信息，根据需要予以更正，阅读服务条款，并选中相应复选框，以确认您已阅读服务条款。

   选择提交。

8. 在导航窗格中，选择域，然后选择请求。

   在此页面上，您可以查看域的状态，也可以查看是否需要回复注册联系人的验证电子邮件。您也可以选择重新发送验证电子邮件。

   如果您为注册联系人指定了从未用于通过 Route 53 注册域的电子邮件地址，则某些 TLD 注册机构会要求您验证该地址是否有效。

   我们将从以下电子邮件地址之一发送验证电子邮件：

   - noreply@registrar.amazon — 适用于由亚马逊 TLDs 注册商注册。
   - noreply@domainnameverification.net 或 noreply@emailverification.info — 由我们的 TLDs 注册商助理 Gandi 注册。要确定您的 TLD 注册商是谁，请参阅查找注册商。

   > **Important**
   >
   > 注册联系人必须按照电子邮件中的说明来验证已收到电子邮件，否则我们必须按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

   a. 当您收到验证电子邮件时，请选择电子邮件中用于确认电子邮件地址是否有效的链接。如果您没有立即收到该电子邮件，请检查垃圾电子邮件文件夹。

   b. 返回请求页面。如果状态未自动更新为电子邮件地址已通过验证，请刷新浏览器。

9. 域注册完成后，下一步取决于您要使用 Route 53 还是其它 DNS 服务作为域的 DNS 服务：

   - Route 53 — 在您注册域时由 Route 53 创建的托管区域中，创建资源记录集以告知 Route 53 您希望如何为域和子域路由流量。

     例如，当有人在浏览器中输入您的域名并且该查询被转发到 Route 53 时，您希望 Route 53 用您数据中心中 Web 服务器的 IP 地址响应查询还是用 ELB 负载均衡器的名称响应查询？

     有关更多信息，请参阅 使用记录。

     > **Important**
     >
     > 如果您在 Route 53 自动创建的托管区域之外的托管区域中创建记录，则必须更新域的名称服务器，以将这些名称服务器用于新托管的区域。

- 其它 DNS 服务 — 配置您的新域，以将 DNS 查询路由到其它 DNS 服务。执行步骤更新名称服务器以使用其他注册商。

您在注册或转移域时指定的值

> **Note**
>
> 我们更新了 Route 53 的域控制台。在过渡期间，您可以继续使用旧控制台，也可以使用新控制台。对于两个控制台，Route 53 返回的大多数信息都是相同的。以下列表列出了差异。

在注册域或将域注册转移到 Amazon Route 53 时，需指定本主题中描述的值。

> **Note**
>
> 如果您要注册多个域，Route 53 将使用您为购物车中的所有域指定的值。

还可以更改当前已向 Route 53 注册的域的值。注意以下几点：

- 如果您更改域的联系人信息，我们会向注册联系人发送有关这一更改的电子邮件通知。这封电子邮件来自 noreply@registrar.amazon。对于大多数更改，注册联系人不需要响应。
- 如果联系人信息更改还构成所有权更改，我们将向注册联系人另外发送一封电子邮件。ICANN 要求注册联系人确认已收到电子邮件。有关更多信息，请参阅本节后面的 First Name, Last Name 和 Organization。

有关更改现有域设置的更多信息，请参阅更新域设置 。

您指定的值

- My Registrant, Administrative, and Technical contacts are all the same
- Contact Type
- First Name, Last Name
- Organization
- Email
- Phone

- Address 1
- Address 2
- Country
- State
- City
- Postal/Zip Code
- Fields for selected top-level domains
- Privacy Protection
- Auto-renew

与注册人联系人相同

指定是否要对域注册者、管理联系人和技术联系人使用相同的联系人信息。

联系人类型

此联系人的类别。注意以下几点：

- 如果您选择 Person 之外的选项，则必须输入组织名称。
- 对于某些人来说 TLDs，可用的隐私保护取决于您为 “联系人类型” 选择的值。有关 TLD 的隐私保护设置，请参阅可向 Amazon Route 53 注册的域。。
- 对于 .es 域，所有三个联系人的 Contact Type (联系人类型) 值均必须为 Person (个人)。

名字、姓氏

联系人的名字和姓氏。

> **Important**
>
> 对于 First Name 和 Last Name，我们建议您指定官方 ID 上的名称。要对域设置进行一些更改，您必须提供身份证明，并且 ID 的名称必须与域的注册联系人的名称匹配。

如果要将域转移到 Route 53 并且满足以下条件，则将更改域的所有者：

- 联系类型为个人。
- 您正在从当前设置中更改注册人联系人的名字 and/or 姓氏字段。

在这种情况下，ICANN 要求我们向注册联系人发送电子邮件以获得批准。我们将从以下电子邮件地址之一发送电子邮件：

TLDs	发出审批电子邮件的电子邮件地址
TLDs 由 Amazon 注册商注册	noreply@registrar.amazon
.fr	nic@nic.fr (该电子邮件将同时发送给当前注册联系人和新注册联系人。)
所有其他地址	noreply@domainnameverification.net 或 noreply@emailverification.info

要确定您的 TLD 注册商是谁，请参阅可向 Amazon Route 53 注册的域。。

> **Important**
>
> 注册联系人必须按照电子邮件中的说明来确认已收到电子邮件，否则我们必须按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

如果您更改注册联系人的电子邮件地址，我们会同时向注册联系人的新旧电子邮件地址发送此电子邮件。

某些 TLD 注册商会对更改域所有者收取费用。当您更改其中一个值时，Route 53 控制台会显示一条消息，告知您是否收费。

组织

与联系人关联的组织 (如果有)。对于注册和管理联系人，此组织通常为注册该域的组织。对于技术联系人，此组织可以是管理该域的组织。

当联系人类型为 Person 之外的任意值并且您更改了注册联系人的 Organization 字段时，便会更改域的所有者。ICANN 要求我们向注册联系人发送电子邮件以获得批准。我们将从以下电子邮件地址之一发送电子邮件：

TLDs	发出审批电子邮件的电子邮件地址
TLDs 由 Amazon 注册商注册	noreply@registrar.amazon
.fr	nic@nic.fr (该电子邮件将同时发送给当前注册联系人和新注册联系人。)
所有其他地址	noreply@domainnameverification.net 或 noreply@emailverification.info

要确定您的 TLD 注册商是谁，请参阅可向 Amazon Route 53 注册的域。。

如果您更改注册联系人的电子邮件地址，我们会同时向注册联系人的新旧电子邮件地址发送此电子邮件。

某些 TLD 注册商会对更改域所有者收取费用。当您更改组织的值时，Route 53 控制台会显示一条消息，告知您是否收费。

电子邮件

联系人的电子邮件地址。

如果您更改注册联系人的电子邮件地址，我们会同时向新旧电子邮件地址发送通知电子邮件。这封电子邮件来自 noreply@registrar.amazon。

电话

联系人的电话号码：

- 如果您输入美国或加拿大境内位置的电话号码，请在第一个字段中输入 1 并在第二个字段中输入 10 位的区号和电话号码。
- 如果要输入其他任何位置的电话号码，请在第一个字段中输入国家/地区代码，然后在第二个字段中输入电话号码的其余部分。有关国家/地区电话代码的列表，请参阅维基百科文章 List of country calling codes。

地址 1

联系人的街道地址。

地址 2

联系人的其他地址信息，例如公寓号或邮寄地址。

国家/地区

联系人的国家/地区。

州/省

联系人的州或省 (如果有)。

城市

联系人的城市。

邮政编码

联系人的邮政编码。

所选顶级域的字段

以下顶级域名 (TLDs) 要求您指定其他值：

- .com.au 和 .net.au
- .ca
- .es
- .fi
- .fr
- .it
- .ru
- .se
- .sg
- .co.uk、.me.uk、.org.uk 和 .uk

此外，许多都 TLDs 需要增值税识别号。

有关有效值的信息，请参阅《亚马逊 Route 53 API 参考》ExtraParam中的。

隐私保护

是否需要向 WHOIS 查询隐藏您的联系人信息。如果您选择开启隐私保护（新控制台）或隐藏联系人信息（旧控制台），WHOIS（“谁是”）查询将返回注册商的联系人信息或值“Protected by policy”。

> **Note**
>
> 必须为管理员、注册人、技术和账单联系人指定相同的隐私设置。

如果您选择 Don't hide contact information，您指定的电子邮件地址将收到更多垃圾邮件。

任何人都可以发送针对某个域的 WHOIS 查询并获取该域的所有联系人信息。WHOIS 命令在许多操作系统中都可用，并且在许多网站中还可作为 Web 应用程序提供。

> **Important**
>
> 尽管有合法用户希望获取与您的域关联的联系人信息，但最常见的用户是垃圾邮件发送者，他们的目标是向域联系人发送不需要的电子邮件和伪造优惠。一般而言，我们建议您为 Privacy Protection 选择 Hide contact information。

要为一些域启用或禁用隐私保护，您必须打开支持案例并请求隐私保护。

有关隐私保护的更多信息，请参阅以下主题：

- 启用或禁用域联系信息的隐私保护
- 可向 Amazon Route 53 注册的域。

自动续订（仅在编辑域设置时可用）

您是否希望 Route 53 在域到期之前自动续订该域。注册费将从您的 Amazon 账户中扣除。在旧控制台上，此设置仅在编辑域设置时可用。有关更多信息，请参阅 续订域注册。

> **Important**
>
> 如果您禁用自动续订，则到期日期过后将不续订域注册，您可能失去对域名的控制。

您可以续订域名的时间段因顶级域 (TLD) 而异。有关续订域的概览，请参阅续订域注册。有关将域注册延长指定年数的信息，请参阅延长域的注册期。

Amazon Route 53 在您注册域时返回的值

当您向 Amazon Route 53 注册域时，除了您指定的值之外，Route 53 还会返回以下值。

注册时间

最初向 Route 53 注册域的日期。

过期时间

当前注册期到期的日期和时间，采用格林威治标准时间 (GMT)。

尽管某些顶级域名的注册机构 (TLDs) 的注册期较长，但注册期通常为一年。有关您的 TLD 的注册和续订周期，请参阅可向 Amazon Route 53 注册的域。。

对于大多数人来说 TLDs，您最多可以将注册期延长十年。有关更多信息，请参阅 延长域的注册期。

域名状态代码

域的当前状态。

ICANN 是维护域名的中央数据库的组织，它开发了一组域名状态代码（也称为 EPP 状态代码），这些状态代码可指明对域名执行的各种操作的状态。例如，注册域名、将域名转移到其他注册商、续订域名注册等。所有注册商都使用这组状态代码。

有关域名状态代码的最新列表以及对每个代码含义的解释，请转到 ICANN 网站并搜索 epp status codes。(搜索 ICANN 网站；Web 搜索有时会返回旧版文档。)

转移锁定

是否锁定域以降低有人未经您许可而将您的域转移至其他注册商的概率。如果域被锁定，转移锁定的值将为开启。如果域未锁定，该值为关闭。

自动续订

Route 53 是否在临近到期日期时自动续订注册此域。

授权代码

将此域的注册转移到其他注册商时需要的代码。授权代码只根据请求生成。有关将域转移到其他注册商的信息，请参阅将域从 Amazon Route 53 转移到另一注册商。

名称服务器

响应此域的 DNS 查询的 Route 53 服务器。我们建议您不要删除 Route 53 名称服务器。

有关添加、更改或删除名称服务器的信息，请参阅为域添加或更改名称服务器和粘附记录。

Viewing the status of a domain registration（查看域注册的状态）

ICANN 是维护域名的中央数据库的组织，它开发了一组域名状态代码 (也称为 EPP 状态代码)，这些状态代码可指明对域名执行的各种操作 (例如，注册域名、将域名转移到其他注册商、续订域名注册等) 的状态。所有注册商都使用这组状态代码。

要查看您的域的状态代码，请执行以下过程。

查看域的 ICANN 代码状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，展开域，然后选择已注册的域。
3. 选择域的链接名称。
4. 如果您需要采取操作，例如向注册联系人重新发送验证电子邮件，则页面顶部的横幅将指示您需要采取的操作。
5. 要了解您的域的当前状态，请参阅域状态代码字段的值。

   有关域名状态代码的最新列表以及对每个代码含义的解释，请转到 ICANN 网站并搜索 epp status codes。(搜索 ICANN 网站；Web 搜索有时会返回旧版文档。)

您还可以在请求页面上查看注册状态。

查看注册状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，展开域，然后选择请求。
3. 在请求页面上，您可以查看注册状态，以及您对域名执行的任何其他操作的状态，例如删除域、锁定域转移、添加或删除 DNSSEC 密钥。

   还会列出您为完成某个过程可能需要采取的任何操作，例如验证您的电子邮件。

   - 要回应操作请求，请选择域名旁边的单选按钮，然后从操作下拉列表中选择操作。

更新域设置

本节提供以下有关在 Route 53 中管理域设置的主题的信息：

1. 更新域的联系信息和所有权:
   - 了解如何更新域的联系信息，包括管理员、技术人员、注册人和账单联系人。
   - 了解注册机构要求提供“域所有权变更表”时更改域所有者的过程。
2. 启用或禁用域联系信息的隐私保护:
   - 了解如何启用或禁用联系信息的隐私保护，该功能会在 WHOIS 查询中隐藏或泄露个人信息。
3. 启用或禁用域自动续订:
   - 了解如何启用或禁用域的自动续订，这决定了 Route 53 是否在到期前自动续订注册。
4. Locking a domain to prevent unauthorized transfer to another registrar（锁定域以防止未经授权转移到另一个注册商）:
   - 了解如何锁定域以防止域未经授权转移到其他注册商，以及如何在需要时禁用锁定功能。
5. 延长域的注册期:
   - 了解延长域注册期的流程，通常最长可延期十年（以一年为增量）。
6. 更新名称服务器以使用其他注册商 和 为域添加或更改名称服务器和粘附记录：
   - 了解如何更新名称服务器以使用其他 DNS 服务，或配置白标签（虚名）名称服务器。
   - 了解更改名称服务器和粘附记录时的注意事项和最佳实践。

更新域的联系信息和所有权

对于域的管理和技术联系人，您可以更改所有联系信息，无需授权更改。有关更多信息，请参阅 Updating contact information for a domain（更新域的联系信息）。

对于注册联系人，您可以更改大多数值，无需授权更改。但是，对于某些人来说 TLDs，更改域名的所有者需要获得授权。有关更多信息，请参阅相关主题。

主题

- 哪些因素会触发域所有权更改？
- TLDs 需要特殊处理才能更改所有者
- Updating contact information for a domain（更新域的联系信息）
- 在注册机构要求提供“域所有权变更表”的情况下更改域的所有者

哪些因素会触发域所有权更改？

> **Important**
>
> 根据 ICANN 转移策略，您列为注册人的联系人将拥有作为域名的注册名称持有者的某些权利。大多数域名将在您关闭后删除 Amazon Web Services 账户（有关更多信息，请参阅我的 Amazon 账户已关闭或永久关闭，并且我的域已注册到 Route 53），但是，如果某个域名仍处于已关闭的账户中，则您列为注册人的联系人可能可以请求将域名转让给外部注册商。因此，重要的是，您列出的注册人联系人要么是您自己，要么是您信任的负责任的其他人。

注册人联系信息的以下更改会触发域所有权更改流程：

对于人员联系人类型

更改名字或姓氏字段会触发所有权更改。

适用于非人员联系人类型（公司、协会、公共机构）

更改组织字段会触发所有权更改。

其他触发条件（所有联系人类型）

根据您域的 TLD 要求，其他联系人字段的更改也可能触发所有权更改流程，包括：

- 注册人电子邮件地址的更改
- 其他识别信息字段的更改

触发所有权更改的特定字段因 TLD 而异，并由域注册机构的政策决定。

> **Warning**
>
> 服务中断风险：触发所有权更改时，您将收到一封授权电子邮件。如果您未在 3-15 天内回复此电子邮件（视您的 TLD 而定），您的域注册将按照 ICANN 的要求被取消，这将中断您的网站和电子邮件服务。
> 在更改任何联系人之前，请务必确保您可以访问注册人的联系人电子邮件地址。

更改域的所有者时，请注意以下事项：

- 对于某些人来说 TLDs，更改域名所有者需要付费。要确定 TLD 对您的域是否收费，请参阅 Amazon Route 53 域注册定价中的“更改所有权价格”列。

  > **Note**
  >
  > 您不能使用 Amazon 积分来支付变更域名所有者的费用（如果有）。

- 对于某些人来说 TLDs，当您更改域名所有者时，我们会向注册人联系人的电子邮件地址发送一封授权电子邮件。注册联系人必须按照电子邮件中的说明授权更改。
- 对于某些人 TLDs，您需要填写域名所有权变更表并提供身份证明，以便 Amazon Route 53 支持工程师可以为您更新值。如果域的 TLD 要求填写“域所有权变更表”，控制台会显示一条消息，该消息链接到一个表单，用于开立支持案例。有关更多信息，请参阅 在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

TLDs 需要特殊处理才能更改所有者

当您更改域名的所有者时，某些域名的注册管理机构 TLDs 需要特殊处理。如果要更改以下任何域名的拥有者，请执行适用的过程。如果要更改任何其它域名的拥有者，则可以通过编程方式或使用 Route 53 控制台自行更改。请参阅Updating contact information for a domain（更新域的联系信息）。

以下内容 TLDs 需要特殊处理才能更改域名的所有者：

.be, .cl, .com.br, .es, .fi, .ru, .se, .sh

.be

您必须从注册局获取.be 域名的转移代码，然后向 Su Amazon pport 提起诉讼。

- 要获取转账码，请参阅 https://www.dnsbelgium。 be/en/manage-your-domain-name/change-holder #transfer，然后按照提示进行操作。
- 要提交案例，请参阅就域名注册问题联系 Su Amazon pport。

.cl

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.com.ar

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.com.br

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.es

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.fi

在 Route 53 控制台上启动所有者变更。启动变更后，您将收到来自 fi-domain-tech@traficom .fi 电子邮件地址的持有人转账密钥。收到密钥后，请向 Support 提交 Amazon 支持案例，然后与我们分享密钥代码。请参阅就域名注册问题联系 Su Amazon pport。

.qa

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.ru

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.se

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

.sh

您必须填写表单并将其提交给 Su Amazon pport。请参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者。

Updating contact information for a domain（更新域的联系信息）

要更新域的联系信息，请执行以下过程。

> **Warning**
>
> 服务中断风险：如果您的联系人更改触发所有者更改流程，您将收到一封授权电子邮件。如果您未在 3-15 天内回复此电子邮件（视您的 TLD 而定），您的域注册将按照 ICANN 的要求被取消，这将中断您的网站和电子邮件服务。

在进行任何联系人更改之前，请确保您可以访问注册人的联系人电子邮件地址。

更新域联系人之前

在更改域的注册人联系信息之前，请完成以下核对清单：

1. □ 验证电子邮件访问权限 - 确认您可以通过当前注册人的电子邮件地址接收电子邮件
2. □ 了解所有者更改触发条件 - 查看 the section called “哪些因素会触发域所有权更改？” 以了解哪些更改可能会触发所有者更改流程
3. □ 计划可能的停机时间 - 如果触发所有者更改，您有 3-15 天的时间回复授权电子邮件，否则您的域将被取消

更新域的联系信息

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择希望为其更新联系信息的域的名称。
4. 在联系信息选项卡中，选择编辑。
5. 如果您无法访问注册联系人的电子邮件地址，请执行以下步骤。如果您可以访问注册联系人的电子邮件地址，请跳至步骤 6。

   a. 仅 更改注册联系人的电子邮件地址。不更改任何域联系人的任何其他值。如果您想要更改其他值，请在流程中稍后部分更改。

      选择保存更改。

      为了验证新电子邮件地址，我们会向新地址（如果 TLD 需要）发送一封验证电子邮件。您必须选择电子邮件中的链接来验证新电子邮件地址的有效性。如果需要验证，而您未验证新电子邮件地址，Route 53 会根据 ICANN 的要求暂停域。

      如果您需要重新发送验证电子邮件，请导航至已注册的域页面，选择您更新的域名旁边的单选按钮，然后选择要更新的域的名称。在验证您的电子邮件以避免域被暂停提醒上，选择再次发送电子邮件。

   b. 如果要更改域的注册人、管理员、技术或账单联系人的其他值，请返回步骤 1，并重复此过程。

6. 更新适用的值。您也可以选择复制注册联系人，以自动填写您为注册联系人输入的相同信息。有关更多信息，请参阅 您在注册或转移域时指定的值。

   根据域的 TLD 以及要更改的值，控制台可能会显示以下消息：

   “To change the registrant name or organization, open a case.”

   如果您看到该消息，请跳过此过程的剩余部分，并参阅在注册机构要求提供“域所有权变更表”的情况下更改域的所有者了解更多信息。
7. 选择保存。
8. 如果您更改了域所有者（如哪些因素会触发域所有权更改？中所述），我们会向域的注册联系人发送电子邮件。电子邮件会要求有关所有者更改的授权。

   如果我们未在 3 至 15 天内收到更改授权（具体时间取决于顶级域），我们必须按照 ICANN 的要求取消请求。

   电子邮件来自以下电子邮件地址之一。

TLDs	发出授权电子邮件的电子邮件地址
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
所有其他地址	以下电子邮件地址之一： • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

9. 如果您在更新联系信息时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

有关可用于更新联系人信息的 API 的信息，请参阅UpdateDomainContact。

在注册机构要求提供“域所有权变更表”的情况下更改域的所有者

如果您的域名注册机构要求您完成域名所有权变更并将表格提交给 Supp Amazon ort，请执行以下步骤。若要确定是否需要执行此过程，请参阅以下主题：

- 要确定您要更改的值是否被视为更改所有者，请参阅哪些因素会触发域所有权更改？。
- 若要确定您的域是否需要域所有权变更表单，请参阅TLDs 需要特殊处理才能更改所有者。

在注册机构要求提供“域所有权变更表”时更改域的所有者

1. 请参阅本主题的介绍，确定您的域的注册机构是否需要特殊处理来更改域的拥有者。如果是这种情况，并且如果需要填写“域所有权变更”表，请继续此过程。

   如果无需填写“域所有权变更”表，请改为执行适用主题中的过程。
2. 下载域所有权变更表。该文件被压缩为 .zip 文件。
3. 填写表单。
4. 对于域的以前所有者和 新所有者的注册联系人，获取已签名身份证明（身份证、驾驶证、护照或其他合法的身份证明）的副本。

   此外，如果将法律实体列为注册组织，请收集域的以前所有者和 新所有者的以下信息：

   - 证明域的注册组织存在。
   - 证明以前所有者和新所有者的代表有权代表组织操作。此文档必须是经过认证的法律文档，签名人员位置同时包含组织的名称和代表的姓名（如 CEO、总裁或执行总监）。
5. 扫描“域所有权变更表”和所需证明。将扫描的文档保存为常见格式 (如 .pdf 文件或 .png 文件)。
6. 使用域名当前注册的 Amazon 账户登录 Support C enter。Amazon

> **Important**
>
> 您必须使用根账户，或者使用通过以下一种或多种方式被授予 IAM 权限的用户登录：
>
> - 已为用户分配AdministratorAccess托管策略。
> - 为用户分配了 AmazonRoute53 DomainsFullAccess 托管策略。
> - 为用户分配了 AmazonRoute53 FullAccess 托管策略。

如果您没有使用根账户或者具有所需权限的用户登录，则我们将无法更新域拥有者。此项要求可防止未经授权的用户更改域的所有者。

7. 指定以下值：

关于

接受 Account and billing 的默认值。

服务

接受 Domains 的默认值。

类别

接受 Change of Ownership 的默认值。

严重性

接受 General question 的默认值。

选择下一步：其他信息

主题

指定 Change the owner of a domain (更改域所有者)。

说明

提供以下信息：

- 希望更改其所有者的域
- 注册域名的@@ Amazon 账户的 12 位数账户 ID

添加附件

上传第 5 步中扫描的文档。

联系方式

指定联系方式并输入适用的值。

8. 选择提交。

S Amazon upport 工程师会审查您提供的信息并更新设置。工程师将在更新完成后与您联系，或者随时联系您以了解更多信息。

启用或禁用域联系信息的隐私保护

当您向 Amazon Route 53 注册域或向 Route 53 转移域时，我们默认为域的所有联系人启用隐私保护。这通常会在 WHOIS (即“Who is”) 查询中隐藏大多数联系信息，并减少收到的垃圾邮件数量。启用隐私保护后，您的联系信息将被替换为注册商的联系信息或者短语“REDACTED FOR PRIVACY”或“On behalf of <domain name> owner”（代表 <域名> 所有者）。

如果您选择禁用隐私保护，则必须为域的所有联系人都禁用。如果您确实禁用了隐私保护，则任何人都可以发送域名的 WHOIS 查询，对于大多数顶级域名 (TLDs)，则可能能够获得您在注册或转让域名时提供的所有联系信息，包括姓名、地址、电话号码和电子邮件地址。WHOIS 命令的使用很广泛，许多操作系统中都包含该命令，并且还以 Web 应用程序的形式存在于许多网站上。

如果您要将域名转让给其他注册商，并且已为域名联系人启用隐私保护，则验证转移的电子邮件将从在亚马逊注册商处注册 TLDs 的 identity-protect.org 地址发送。要确定您的 TLD 注册商是谁，请参阅查找注册商。

可以在 WHOIS 查询中隐藏的信息主要取决于两个因素：

顶级域的注册机构

大多数 TLD 注册机构会自动隐藏所有联系信息，有些则允许您选择隐藏所有联系信息，另外一些仅允许隐藏某些信息，还有一些不允许隐藏任何信息。某些 TLD 注册机构故意抑制隐私保护，以遵守当地法规或注册机构政策。

启用域隐私保护后，您的联系信息将被替换为隐私保护服务的联系信息或短语“REDACTED FOR PRIVACY”。隐私保护服务应用垃圾邮件防护功能（地址轮换和SPF/DKIM/spam分析），并且在大多数情况下，会自动转发通过这些过滤器的电子邮件。但是，不建议将重要电子邮件发送到受隐私保护的电子邮件地址，因为垃圾邮件机制可能会阻止它们被转发。

此外，选择哪个隐私保护机制用于域是不可配置的，并且由系统自动选择。我们的隐私保护服务的联系详细信息无法手动更新。

> **Note**
>
> 要为一些域启用或禁用隐私保护，您必须打开支持案例并请求隐私保护。有关更多信息，请参阅可向 Amazon Route 53 注册的域。中的适用部分：
>
> - .co.uk（英国）
> - .me.uk（英国）
> - .org.uk（英国）

- .link

注册商

当您向 Route 53 注册域或者将域转移到 Route 53 时，域的注册商为 Amazon Registrar 或我们的注册商合作者 Gandi。Amazon Registrar 和 Gandi 默认隐藏不同的信息：

- Amazon Registrar — 默认隐藏所有联系信息。但是，TLD 注册机构的规定优先。
- Gandi — 默认隐藏除组织名称（如果有）以外的所有联系信息。但是，TLD 注册机构的规定优先。

  对于不允许隐私保护的地理位置 TLDs，您的个人信息将在 Gandi 网站的 Whois 目录搜索页面上标记为 “已删除”。但是，您的个人信息可能会出现在域注册机构或第三方 WHOIS 网站上。

要确定域的 TLD 隐藏了哪些信息，请参阅可向 Amazon Route 53 注册的域。。

如果希望为使用 Route 53 注册的域启用或禁用隐私保护，请执行以下过程。

Important

隐私保护的可用性：并非所有人都能获得隐私保护 TLDs。不支持隐私保护 TLDs 的常见内容包括.de、.us、.com.au、.es 和其他几个。
如果您在编辑域的联系人信息时看不到“隐私保护”部分，则表示您域的 TLD 不支持隐私保护。有关不支持隐私保护 TLDs 的完整列表，请参阅TLDs 不支持隐私保护的。有关任何 TLD 的隐私保护支持的详细信息，请参阅 可向 Amazon Route 53 注册的域。。

为域的联系信息启用或禁用隐私保护

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择希望为其启用或禁用隐私保护的域的名称。
4. 在联系信息部分中，选择编辑。
5. 在隐私保护部分中，选择是否要隐藏联系信息。您必须为下面的四个联系人都指定相同的隐私设置：管理员、注册人、技术和账单联系人。

> **Note**
>
> 如果未显示隐私保护部分，则表示您域的 TLD 不支持隐私保护。您的联系人信息将在不支持隐私保护的域的 WHOIS 查询中公开显示。

6. 选择保存更改。
7. 如果您在启用或禁用隐私保护时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

TLDs 不支持隐私保护的

以下内容 TLDs 不支持隐私保护。如果您的域名使用其中之一 TLDs，则您的联系信息将在 WHOIS 查询中公开显示：

通用 TLDs

.audio、.ceo、.diet、.flowers、.guitars、.hosting、.juegos、.property、.sexy

地理 TLDs

.cl（智利）、.com.ar（阿根廷）、.com.au（澳大利亚）、.com.br（巴西）、.com.sg（新加坡）、.de（德国）、.es（西班牙）、.in（印度）、.net.au（澳大利亚）、.qa（卡塔尔）、.ru（俄罗斯）、.sg（新加坡）、.sus（美国）、.vg（英属维尔京群岛）

> **Note**
>
> 此列表包括最常见 TLDs 的不支持隐私保护的内容。有关特定 TLD 隐私保护支持的完整 up-to-date信息以及相关信息，请参阅中的各个 TLD 页面。可向 Amazon Route 53 注册的域。

隐私保护问题疑难排解

隐私保护选项在控制台中不可用

这表明您域的 TLD 不支持隐私保护。您的联系人信息将在 WHOIS 查询中公开显示。 TLDs 由于注册政策或当地法规，这肯定是正常行为。

要验证您的 TLD 是否支持隐私保护，请查看 可向 Amazon Route 53 注册的域。 中的各个 TLD 页面或参阅 TLDs 不支持隐私保护的。

启用隐私保护后，联系人信息仍然可见

一些注册机构维护自己的 WHOIS 数据库，即使在 Route 53 中启用隐私保护，也可能继续显示联系人信息。此功能由 TLD 注册机构而非 Route 53 控制。

此外，一些 TLD 注册机构故意为其域提供有限的隐私保护或编辑服务。

启用或禁用域自动续订

如果您想更改 Amazon Route 53 是否在域注册到期日期之前自动为域续订注册，或者想查看当前自动续订设置，请执行以下过程。

请注意，您不能使用 Amazon 积分来支付续订域名的费用。

> **Note**
>
> 如果您打算取消 Amazon 账户，请务必关闭自动续订。否则，您将继续收到来自的续订通知 Amazon。但是，除非您重新激活账户，否则您的域不会续订。

为域启用或禁用自动续订

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择要更新的域的名称。
4. 在详细信息部分的操作下拉列表中，选择开启自动续订

   在是否为 <domain name> 开启自动续订功能？中，同意支付年费，然后选择开启。

   > **Note**
   >
   > 所列价格适用于当前注册期，并且可能会发生变化。有关更多信息，请参阅 Amazon Route 53 域注册定价。

5. 要关闭自动续订，请在操作下拉列表中选择关闭自动续订。
6. 如果您在启用或禁用自动续订时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

Locking a domain to prevent unauthorized transfer to another registrar（锁定域以防止未经授权转移到另一个注册商）

所有通用域名 TLDs 和许多地理域名的域名注册机构 TLDs 允许您锁定域名，以防止有人在未经您许可的情况下将域名转让给其他注册商。要确定是否域的注册机构是否允许您锁定域，请参阅可向 Amazon Route 53 注册的域。。如果支持锁定并且您想要锁定域，请执行以下步骤。如果希望将域转移到另一个注册商，也可以使用该过程禁用锁定。

锁定域以防止未经授权转移到另一个注册商

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered Domains。
3. 选择要更新的域的名称。
4. 在详细信息部分的操作下拉列表中，选择开启转移锁定或关闭转移锁定，具体取决于您要开启还是关闭转移锁定。

   您可以导航到请求页面以查看请求的进度。
5. 如果您在锁定域名时遇到问题，可以免费联系 S Amazon upport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

在 WHOIS 搜索中，此状态显示为：`clientTransferProhibited`。有些人TLDs 可能还具有以下状态：

- `clientUpdateProhibited`
- `clientDeleteProhibited`

延长域的注册期

当您向 Amazon Route 53 注册域或将域注册转移到 Route 53 时，我们会将域配置为自动续订。尽管某些顶级域名的注册机构 (TLDs) 的续订期限较长，但自动续订期限通常为一年。

注意以下几点：

最大续订周期

所有通用代码 TLDs 和许多国家/地区代码都 TLDs 允许您将域名注册延长更长的期限，通常以一年为增量延长至十年。要确定是否可以延长域的注册期，请参阅可向 Amazon Route 53 注册的域。。如果允许更长的注册期，请执行以下过程。

针对您可以续订或延长域注册期的限制

有些 TLD 注册机构对于何时可以续订或延长域注册期有所限制，例如域过期之前至少两个月。即使注册机构允许延长域的注册期，他们也可能不允许在域过期之前的当前天数延期。

> **Note**
>
> 例如，如果您拥有的域名的最长允许续订期限为 5 年，则您可以随时添加年度续订，直至达到 5 年的限制。 TLDs 更具体地说，如果您域的当前有效期为 2.5 年，则最多只能再续订 2 年。

Amazon 积分

您不能使用 Amazon 积分来支付延长域名注册期限的费用。

延长域的注册期

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered Domains。
3. 选择您希望为其延长注册期的域的名称。
4. 在详细信息部分的操作下拉列表中，选择续订域注册。
5. 在续订域注册对话框的续订期下拉列表中，选择要延长注册的年限。

   该列表基于当前到期日期以及此域的注册机构允许的最长注册期显示所有当前选项。持续期下方列出了适用该年限的到期日期。
6. 选择续订域注册。

   当我们收到注册机构已更新您的到期日期的确认信息时，我们会向您发送一封电子邮件，确认我们已更改到期日期。
7. 如果您在延长域名注册期限时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅就域名注册问题联系 Su Amazon pport。

更新名称服务器以使用其他注册商

如果要将 DNS 管理移至其他注册商，则需要更新要指向的名称服务器

在您要使用其他 DNS 服务时更新域的名称服务器

1. 使用 DNS 服务提供的过程获取域的名称服务器。
2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Registered domains。
4. 选择您要配置为使用其他 DNS 服务的域的名称。
5. 在详细信息部分的操作下拉列表下，选择编辑名称服务器。
6. 删除现有的名称服务器，然后将名称服务器的名称更改为您在步骤 1 中从 DNS 服务获取的名称服务器。
7. 选择保存更改。
8. （可选）删除 Route 53 在您注册域时自动创建的托管区域。这可以防止您因为未使用的托管区域被收取费用。

    a. 在导航窗格中，选择托管区。
    b. 选择与您的域同名的托管区域对应的单选按钮。
    c. 选择 Delete Hosted Zone。
    d. 选择 Confirm 以确认您要删除该托管区域。

为域添加或更改名称服务器和粘附记录

在您向 Route 53 注册域时，我们会自动为该域创建托管区域，将四个名称服务器分配给托管区域，然后更新域注册以使用这些名称服务器。您通常不需要更改这些设置，除非您想使用其他 DNS 服务，或者您想使用白标签名称服务器。

Route 53 中每个域的名称服务器的最大数量为 6。

> **Warning**
>
> 如果您将名称服务器更改为错误的值，在粘附记录中指定错误的 IP 地址，或者删除一个或多个名称服务器而未指定新的名称服务器，则您的网站或应用程序可能在 Internet 上多达两天变得不可用。

主题

更改名称服务器和粘附记录的注意事项

请考虑以下问题，然后再更改您的配置。

主题

您想要让 Route 53 成为您域的 DNS 服务

如果您当前正在使用其它 DNS 服务，并且想让 Route 53 成为您域的 DNS 服务，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务 以获得有关如何将 DNS 服务迁移到 Route 53 的详细说明。

> **Important**
>
> 如果您未严格遵守迁移过程，则您的域可能多达两天在 Internet 上变得不可用。

您想使用其它 DNS 服务

如果您想为您的域使用 Route 53 以外的 DNS 服务，请使用以下过程将域注册的名称服务器更改为其它 DNS 服务提供的名称服务器。

> **Note**
>
> 如果您更改名称服务器后 Route 53 返回以下错误消息，则 TLD 的注册机构没有将您指定的名称服务器识别为有效的名称服务器：
>
> ```
> "We're sorry to report that the operation failed after we
> forwarded your request to our registrar associate. This is
> ```

```
because: One or more of the specified name servers are not known
to the domain registry."
```

TLD 注册管理机构通常支持公有 DNS 服务提供的域名服务器，但不支持私有 DNS 服务器，例如您在亚马逊 EC2 实例上配置的 DNS 服务器，除非注册机构有这些域名服务器的 IP 地址。Route 53 不支持使用 TLD 注册机构无法识别的名称服务器。如果您遇到此错误，必须更改为 Route 53 或其它公有 DNS 服务的名称服务器。

您想使用白标签名称服务器

如果您希望名称服务器的名称成为域名的子域，可以创建白标签名称服务器。（白标签名称服务器也称为虚名称服务器或私有名称服务器。）例如，您可以为域 example.com 创建名称服务器 ns1.example.com 至 ns4.example.com。要使用白标签名称服务器，请使用以下过程来指定名称服务器的 IP 地址，而不是名称。这些 IP 地址称为粘附记录。

有关配置白标签名称服务器的更多信息，请参阅配置白标签名称服务器。

您要更改 .it 域的名称服务器

IName 您的 IT 域的服务器必须通过 DNS 检查。我们建议您在 https://dns-check.nic.it/ 检查名称服务器，然后再提交变更请求。该注册表继续使用您进行更改之前的名称服务器响应 DNS 查询。如果以前的名称服务器不再可用，您的域在 Internet 上将不可用。

> **Important**
>
> 任何时候当您更改域的名称服务器时，在取消旧 DNS 服务之前或者删除使用旧名称服务器的 Route 53 托管区域之前，请确认新 DNS 可以响应查询。

有关通过.it 域名注册表获取帮助 Amazon 以更正域名服务器名称的信息，请参阅就域名注册问题联系 Su Amazon pport。

添加或更改名称服务器或粘附记录

要添加或更改名称服务器或粘附记录，请执行以下过程。

> **Note**
>
> 默认情况下，DNS 解析程序通常会将名称服务器的名称缓存两天。因此，您的更改可能需要两天才能生效。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

为域添加或更改名称服务器或粘附记录

1. 查看更改名称服务器和粘附记录的注意事项并解决适用的问题（如果有）。
2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Registered domains。
4. 选择您希望为其编辑设置的域的名称。
5. 在详细信息部分的操作下拉列表中，选择编辑名称服务器。
6. 在编辑名称服务器对话框中，您可以执行以下操作：

   - 通过执行以下操作之一来更改域的 DNS 服务：
     - 使用 Route 53 托管区域的名称服务器替换其它 DNS 服务的名称服务器
     - 使用其它 DNS 服务的名称服务器替换 Route 53 托管区域的名称服务器
     - 使用不同 Route 53 托管区域的名称服务器替换某个 Route 53 托管区域的名称服务器

     有关更改域的 DNS 服务的信息，请参阅将 Amazon Route 53 作为现有域的 DNS 服务。对于要用于域 DNS 服务的 Route 53 托管区域的名称服务器的更多信息，请参阅 获取公有托管区域的名称服务器。
   - 添加一个或多个名称服务器。
   - 替换现有名称服务器的名称。
   - 如果您指定白标签名称服务器，请在粘附记录中添加或更改 IP 地址。您可以按 IPv4 或 IPv6格式输入地址。如果名称服务器有多个 IP 地址，请在单独的行中输入每个地址。

     白标签名称服务器在名称服务器的名称（如 ns1.example.com）中包括您的域名（如 example.com）。如果您指定白标签名称服务器时，Route 53 提示您为名称服务器指定一个或多个 IP 地址。IP 地址称为粘附记录。有关更多信息，请参阅 配置白标签名称服务器。
   - 删除名称服务器。选择该名称服务器的字段右侧的 x 图标。

> **Warning**
>
> 如果您将名称服务器更改为错误的值，在粘附记录中指定错误的 IP 地址，或者删除一个或多个名称服务器而未指定新的名称服务器，则您的网站或应用程序可能在 Internet 上多达两天变得不可用。

7. 选择更新。
8. 如果您在添加或更改域名服务器或粘贴记录时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

续订域注册

当您向 Amazon Route 53 注册域或将域注册转移到 Route 53 时，我们会将域配置为自动续订。尽管某些顶级域名的注册机构 (TLDs) 的续订期限较长，但自动续订期限通常为一年。有关您的 TLD 的注册和续订周期，请参阅可向 Amazon Route 53 注册的域。。

> **Note**
>
> 您不能使用 Amazon 积分来支付续订域名的费用。

对于大多数顶级域名 (TLDs)，您可以更改域名的到期日期。有关更多信息，请参阅 延长域的注册期。

> **Important**
>
> 如果要关闭自动续订，请注意会对域产生的以下影响：
>
> - 如果您续订得不够早，有些 TLD 注册机构会在到期日期之前删除域。如果您要保留某个域名，强烈建议您将自动续订保持启用状态。
> - 此外，我们还强烈建议您不要计划在域到期后重新注册域。某些注册商在域到期后立即允许其他人注册这些域，因此您可能无法在其他人获得域之前重新注册该域。
> - 某些注册机构会对恢复到期域收取大量额外费用。
> - 在到达或临近到期日期时，域将无法在 Internet 上使用。

要确定是否已为您的域启用自动续订，请参阅启用或禁用域自动续订。

如果已启用自动续订，将发生以下情况：

到期前 45 天

我们会向注册联系人发送电子邮件，告知您当前已启用自动续订功能并说明如何禁用该功能。使您的注册联系人电子邮件地址保持最新，以免错过此电子邮件。

到期前 35 天或 30 天

对于除.com.ar 和.com.br 域名之外的所有域名，我们会在域名到期日前 35 天续订域名注册，因此我们有时间在域名到期之前解决您的续订问题。

.com.ar 和 .com.br 域名的注册机构要求我们在域名到期前 30 天内续费。我们将在到期前的第 30 天收到来自注册商合作者 Gandi 的续订电子邮件，如果启用自动续订则需在同一天续订域。

> **Note**
>
> 当我们续订您的域时，会向您发送一封电子邮件，告知您我们已对其进行续订。如果续订失败，我们会向您发送一封电子邮件，解释失败原因。

如果已禁用自动续订，则在域名的到期日期临近时将出现以下情况：

到期前 45 天

我们会向域的注册联系人发送电子邮件，告知您当前已禁用自动续订功能并说明如何启用该功能。使您的注册联系人电子邮件地址保持最新，以免错过此电子邮件。

到期前 30 天和 7 天

如果已为域禁用自动续订，则域注册管理机构 ICANN 要求注册商向您发送一封电子邮件。电子邮件来自以下电子邮件地址之一：

- noreply@registrar.amazon — 用于注册商为 Amazon Registrar 的域。
- noreply@domainnameverification.net 或 noreply@emailverification.info — 对于注册商是我们的注册商助理的域名，Gandi。

要确定您的 TLD 注册商是谁，请参阅可向 Amazon Route 53 注册的域。。

如果您在到期前 30 天内启用自动续订并且未通过域续订期，我们会在 24 小时内续订域。

> **Important**
>
> 部分 TLD 注册机构对您可以续订域的时间设置了限制。有关域的详细信息，请参阅 可向 Amazon Route 53 注册的域。。此外，处理续订最多需要一天时间。如果您在启用自动续订前拖延太久，可能还未来得及处理续订，域就已经到期，您可能会因此失去该域。如果到期日期临近，建议您手动延长域的到期日期。有关更多信息，请参阅 延长域的注册期。

有关续订期的更多信息，请参阅 可向 Amazon Route 53 注册的域。 中有关您的 TLD 的“续订和恢复域的截止日期”部分。

到期日期之后

对于大多数域，注册商都会在域到期之后的短时间内予以保留，这样您便可以在到期日期之后续订已到期域；但如果您要保留域，我们强烈建议您使自动续订功能保持启用状态。有关在到期日期之后尝试续订域的信息，请参阅Restoring an expired or deleted domain（恢复已到期或已删除的域）。

如果您的域过期，但允许延迟续订，您可以按标准续订价格续订域。要确定某个域是否仍在延期续订期内，请执行延长域的注册期一节中的过程。如果仍列出了该域，则说明它仍在延期续订期内。

有关续订期的更多信息，请参阅 可向 Amazon Route 53 注册的域。 中有关您的 TLD 的“续订和恢复域的截止日期”部分。

Restoring an expired or deleted domain（恢复已到期或已删除的域）

如果您没有在延迟续期结束之前续订域名，或者您不小心删除了该域名，则对于某些顶级域名注册机构 (TLDs)，您可以在域名可供其他注册机构注册之前将其恢复。

如果某个域被删除，或其延迟续订期已过，则它不会再出现在 Amazon Route 53 控制台中。

> **Important**
>
> 恢复域的价格通常较高一些，有时远远超过注册或续订域的价格。有关恢复域的当前价格信息，请参阅 Amazon Route 53 域注册定价中的“恢复价格”一列。

您不能使用 Amazon 积分来支付恢复过期域名的费用。

在域被删除或延迟续订期到期后尝试恢复域注册

1. 确定域的 TLD 注册表是否支持恢复域，如果支持，确定允许恢复的期限。

   a. 转到 可向 Amazon Route 53 注册的域。 。

   > **Important**
   >
   > 对于在注册后的前 5 天内删除的通用 TLD 域，标准的 30 天兑换期（要查看实际的兑换期天数，请参阅 可向 Amazon Route 53 注册的域。 ）不适用。取而代之的是，这些域可以立即用于新注册。

   b. 查找您的域的 TLD，并查看“续订和恢复域的截止日期”部分中的值。

   > **Important**
   >
   > 我们会将恢复请求转发给 Gandi，Gandi 将在星期一到星期五的工作时间处理这些请求。Gandi 的总部设在巴黎，那里的时间为 UTC/GMT +1 小时。因此，在极少数情况下，可能需要一周甚至更长时间才能处理完请求，具体取决于您提交请求的时间。

2. 审核恢复域的价格，该价格通常较高一些，有时远远超过注册或续订域的价格。在 Amazon Route 53 域注册定价中，找到您的域的 TLD（如 .com），并查看“恢复价格”列中的价格。如果您仍要恢复域，请记下价格；您在随后步骤中将需要它。
3. 使用注册域名的 Amazon 账户登录 Support C enter。Amazon
4. 指定以下值：

   关于

   接受 Account and billing 的默认值。

   服务

   接受 Domains 的默认值。

   类别

   接受 Restoration 的默认值。

   严重性

   接受 General question 的默认值。

选择下一步：其他信息

主题

输入 Restore an expired domain (恢复已到期域) 或 Restore a deleted domain (恢复已删除域)。

说明

提供以下信息：

- 要恢复的域
- 注册域名的Amazon 账户的 12 位数账户 ID
- 确认您同意恢复域的价格。使用以下文本：

  “我同意恢复域的价格为 ____ 美元。”

  将空白处替换为您在步骤 2 中找到的价格。

联系方式

指定联系方式并输入适用的值。

5. 选择提交。
6. 当我们得知我们能否恢复您的域名时，Suppor Amazon t 代表将与您联系。此外，如果我们能够恢复您的域，控制台中将重新显示该域。到期日期取决于域是已到期还是被意外删除：

   域已到期

   新的到期日期通常是旧的到期日之后的一年或两年（具体取决于 TLD）。

   > **Note**
   >
   > 新的到期日期不是从还原该域的日期开始计算。

   域被意外删除

   过期日期通常不会更改。

替换在 Route 53 注册的域的托管区域

如果您删除域的托管区域，当您让该域随时在 Internet 上可用时，需要创建另一个托管区域。请执行以下过程。

替换域的托管区域

1. 创建公有托管区域。有关更多信息，请参阅 创建公有托管区域。
2. 在托管区域中创建记录。记录定义您要如何路由域 (example.com) 及子域（acme.example.com 和 zenith.example.com）的流量。有关更多信息，请参阅 使用记录。
3. 更新域配置以使用新托管区域的名称服务器。有关更多信息，请参阅 为域添加或更改名称服务器和粘附记录。

   > **Important**
   >
   > 当您创建托管区域时，Route 53 将为托管区域分配一组四个名称服务器。如果您删除某个托管区，然后再创建一个托管区，Route 53 将分配另一组四个名称服务器。通常，新托管区域的任何名称服务器与前一个托管区域的任何名称服务器都不相符。如果您不更新域配置以使用新托管区域的名称服务器，域将在 Internet 上保持不可用。

4. 如果您在替换域名的托管区域时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

转移域

您可以将域注册从另一个注册商转移到 Amazon Route 53，从一个 Amazon 账户转移到另一个账户，或从 Route 53 转移到另一个注册商。将域从一个 Amazon 账户转移到另一个账户不收费。

本节涵盖以下有关域转移的主题：

1. 选择转移类型
   - 了解将域注册转移到 Route 53 与仅将 Route 53 用于 DNS 托管的区别。
   - 根据您的域管理和 DNS 托管目标，了解哪个选项最适合您的需求。
2. 转移前核对清单
   - 在将域转移到 Route 53 之前，请完成必要的准备步骤，以避免常见的转移失败。
   - 验证域资格，获取授权代码，并且准备您的 DNS 设置，以便顺利完成转移流程。

3. 将域注册转移到 Amazon Route 53
   - 了解将域从其他注册商转移到 Route 53 的分步过程，包括先决条件、授权代码和更新 DNS 设置。
   - 了解域的转移如何影响到期日期以及不同顶级域 (TLD) 的注意事项。
4. 常见转移问题
   - 通过了解域要求、授权流程和时间注意事项，防止常见的转移问题。
   - 了解如何解决转移问题，以及在转移延迟或被拒绝时应该采取的行动。
5. 将域从 Amazon Route 53 转移到另一注册商
   - 了解将域从 Route 53 转移到其他注册商的流程，包括获取授权代码、更新 DNS 设置和回复确认电子邮件。
   - 请留意将 DNS 服务转移到其他提供商时的注意事项，以及对别名记录和路由策略等 Route 53 专属功能的潜在影响。
6. 将域转移到其它 Amazon 账户
   - 了解如何将域从一个 Amazon 账户转移到另一个账户，包括发起和接受转移所需的角色和权限。
   - 了解域转移后将托管区迁移到新账户的可选步骤。
7. 转移状态
   - 了解如何查看域转移请求的状态以及转移过程中不同状态代码的含义。
8. 将域转移到 Amazon Route 53 对域注册的到期日期有何影响
   - 了解将域转移到 Route 53 对域到期日期的影响。

通过遵循上面列示主题中提供的信息，就可以有效地将域转入和转出 Route 53，管理转移流程，确保平稳过渡，同时保持正确的 DNS 配置和路由。

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

选择您的 Route 53 转移类型

当您想要将 Amazon Route 53 用于自己的域时，有两种选择。了解其中的差异将有助于您根据自己的需求选择正确的方法：

将域注册转移到 Route 53

使用此选项，Route 53 将成为您的域注册商。这意味着您将通过 Route 53 管理自己的域续订、联系人信息和 DNS 设置。

如果您想要执行以下操作，请选择此选项：

- 在统一位置进行域管理和 DNS 托管
- 利用 Route 53 域管理功能
- 通过在 Amazon 账单上进行域续订来简化账单

预期发生的情况：

- 完成时间：5-7 天
- 先决条件：来自当前注册商的授权代码，解锁域，验证注册者电子邮件
- 续订费用支付方：Route 53

下一步：完成 域转移的转移前核对清单 以准备转移。

仅将 Route 53 用于 DNS 托管

使用此选项，您可以保留其当前的域注册商，但使用 Route 53 作为您的 DNS 服务。

如果您想要执行以下操作，请选择此选项：

- 保持您现有的注册商关系
- 无需更改注册商即可使用 Route 53 高级 DNS 功能
- 以最少的先决条件快速入门

预期发生的情况：

- 完成时间：最长 2 天（取决于 DNS 传播情况）
- 先决条件：无
- 续订费用支付方：您当前的注册商

下一步：转到 将 Amazon Route 53 配置为 DNS 服务 以设置 DNS 托管。

> **Important**
>
> 您无需转移域注册即可使用 Route 53 作为您的 DNS 服务。您可以保留现有的注册商，仅将 Route 53 用于 DNS 托管。

域转移的转移前核对清单

在开始将域注册转移到 Amazon Route 53 之前，请完成以下检查，以避免常见的转移失败并确保流程顺利。

决定要转移的内容

选择最符合您需求的选项：

将域注册转移到 Route 53

您的注册商变为 Amazon Route 53。您需要向 Route 53 支付域续订费用，并通过 Route 53 控制台管理域设置。

下一步：继续完成此核对清单，然后遵循 将域注册转移到 Amazon Route 53。

仅将 Route 53 用于 DNS 托管

保留您当前的注册商，但使用 Route 53 名称服务器进行 DNS 解析。您继续向当前的注册商支付续订费用。

下一步：跳过此核对清单并遵循 将 Amazon Route 53 配置为 DNS 服务。

先决条件核对清单

在开始域转移之前，请完成以下所有操作。

转移前核对清单（完成所有项目）

1. □ 验证注册商的电子邮件访问权限

   确认您可以通过注册商的电子邮件地址接收电子邮件，因为它将收到域转移授权电子邮件。

> **Important**
>
> 如果您无法访问当前注册商的电子邮件地址，请将注册商联系人的电子邮件地址更新到当前的注册商，并等待 60 天后再进行转移。

2. □ 解锁域

   访问您当前的注册商域设置并禁用“域锁定”或“转移锁定”保护（如果已启用）。

   > **Note**
   >
   > 禁用锁定后，更改需几分钟才能生效，之后才开始转移。

3. □ 获取授权码

   向当前的注册商请求授权代码（授权码），并对其进行保密处理。您将在稍后的转移过程中在 Route 53 控制台中输入此代码。

4. □ 验证域年龄和资格

   确认您的域符合 ICANN 的转移要求：

   - 自最初注册以来，该域必须已有至少 60 天的历史。
   - 如果域注册已到期，并且已还原，则必须已在至少 60 天前还原。

   > **Tip**
   >
   > 如果最近更新注册商的联系方式（例如，更改您的姓名或电子邮件），ICANN 规则可能会暂时阻止转移。有些注册商允许您选择退出此保留 — 如果您不确定，请咨询当前的注册商。

5. □ 准备付款方式

   确保您的 Amazon 账户使用有效的付款方式。当您将域转移到 Route 53 时，我们向您的 Amazon 账户收取的转移费用会根据顶级域而改变。

   有关当前定价，请参阅 Route 53 定价。

> **Note**
>
> 您不能使用 Amazon 积分来支付域转移费用。Route 53 在开始流程之前收取转移费用，如果转移失败，则立即退款。

6. □ 禁用 DNSSEC（如果已启用）

   如果您当前的注册商当前已启用 DNSSEC，请在开始转移之前暂时将其禁用。这样可以确保在不出现 DNS 验证问题的情况下完成转移。

   这点为何如此重要：

   转移域时，存储在当前注册商处的 DNSSEC 密钥（KSK/ZSK）和 DS 记录不会自动转移到 Route 53。如果您重新启用 DNSSEC 且没有在 Route 53 中重新配置这些密钥，则您的域可能无法通过 DNS 验证。

   安全方法（建议）：

   1. 在初始化转移之前，请在您当前的注册商处禁用 DNSSEC。
   2. 完成域转移并创建您的 Route 53 托管区（如果尚未创建）。
   3. 验证是否在没有启用 DNSSEC 的情况下已正确解析所有 DNSEC 记录。
   4. 使用托管区的新 KSK/ZSK 值在 Route 53 中配置 DNSSEC。
   5. 通过向您的 TLD 注册商（现为 Route 53）发布新的 DS 记录来重新启用 DNSSEC。

   > **Tip**
   >
   > 如果您要转移域，同时在 Route 53 中创建新的托管区，请在转移之前禁用 DNSSEC，然后等到托管区设置通过验证且 DNS 解析正常运行后再重新启用 DNSSEC。确认后，您可以从 Route 53 的控制台再次安全地启用 DNSSEC。在重新启用 DNSSEC 之前，请务必在 Route 53 中验证您的 DNS 配置。有关 Route 53 的 DNSSEC 的更多信息，请参阅 为域配置 DNSSEC。

可选：首先转移 DNS 服务

在转移域注册之前，请考虑将您的 DNS 服务转移到 Route 53。此方法提供以下优势：

- 降低转移期间网站或电子邮件停机的风险
- 允许您在提交完全转移之前测试 Route 53 的 DNS 功能
- 提供域转移遇到问题时的回退选项

要首先转移 DNS 服务，请参阅 将 Amazon Route 53 配置为 DNS 服务。

后续步骤

完成此核对清单后：

1. 遵循 将域注册转移到 Amazon Route 53 中的分步转移流程。
2. 在转移过程中，监控您的电子邮件中是否有授权消息。

将域注册转移到 Amazon Route 53

> **Important**
>
> 在将任何国家/地区代码顶级域名 (ccTLDs) 转移到 Route 53（.cc 和.tv 除外）的过程中，所有者联系人的更新都将被忽略，并使用注册机构中的所有者联系人数据。转移完成后，您可以更新所有者联系信息。有关更多信息，请参阅 更新域的联系信息和所有权。

要将域注册转移到 Amazon Route 53，请按照本主题中的步骤操作。

转移过程概述

域转移涉及以下关键步骤：

1. 填写转移前核对清单

   验证先决条件以避免转移失败。请参阅 域转移的转移前核对清单。
2. 在 Route 53 控制台中请求转移

   输入域名和授权代码。请参阅步骤 5：请求转移。
3. 通过电子邮件授权（需要客户操作）

   单击在 5 天内发送到注册人电子邮件的授权链接。请参阅步骤 6：单击确认和授权电子邮件中的链接。

4. 等待完成

   除非当前的注册商拒绝，否则转移将自动完成。在控制台中监控状态。

最常见的故障点

以下是常见问题的解决方案：

- 未收到电子邮件：验证注册人的电子邮件是否可以访问并检查垃圾邮件文件夹
- 域已锁定：开始转移之前，在当前的注册商处解锁
- 授权码无效：向当前注册商请求新的授权代码
- 60 天规则违规：60 天的 ICANN 规则（资格时间段）。在首次注册或注册人联系人更改后 60 天内阻止转移。有些注册商允许在更改之前选择退出 — 如果适用，请询问您当前的注册商。

> **Important**
>
> 如果您跳过某个步骤，您的域可能在互联网上不可用。

注意以下几点：

联系 Su Amazon pport

如果您在转移域时遇到问题，则可以免费联系 Amazon Support。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

到期日期

有关转移域如何影响当前到期日期的信息，请参阅将域转移到 Amazon Route 53 对域注册的到期日期有何影响。

转移费用

当您将域名转移到 Route 53 时，我们对您的 Amazon 账户收取的转移费用取决于顶级域名，例如.com 或.org。有关更多信息，请参阅 Route 53 定价。

您不能使用 Amazon 积分来支付将域名转移到 Route 53 的费用（如果有）。

> **Note**
>
> 在开始转移流程之前，Route 53 会收取您的域的转移费用。如果转移由于某种原因而失败，我们会立即将您的费用记入您的账户中。

特殊和高级域名

TLD 注册表向一些域名分配了特殊或优惠的价格。如果域具有特殊或优惠的价格，您无法将该域转移到 Route 53。

域配额

每个 Amazon 账户的默认最大域名数为 20。您可以请求提高配额。有关更多信息，请参阅 域的配额。

名称服务器限制

Route 53 中每个域的名称服务器的最大数量为 6。

主题

顶级域的转移要求

大多数域注册商对将域转移到其他注册商施加了要求。这些要求的主要目的是为了防止欺诈性域的拥有者反复在不同注册商之间转移域。各注册商要求不尽相同，但以下为典型要求：

- 您必须至少在 60 天前向当前注册商注册域或将域注册转移到当前注册商。
- 如果域名注册已到期，并且必须恢复，则必须已在至少 60 天前恢复。

- 域不能具有以下任何域名状态代码：
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - serverTransferProhibited
- 某些顶级域的注册机构不允许在更改 (例如对域所有者的更改) 完成之前转移。

有关域名状态代码的当前列表以及对每个代码含义的解释，请转到 ICANN 的网站，然后搜索“EPP status codes”。(搜索 ICANN 网站；Web 搜索有时会返回旧版文档。)

> **Note**
>
> ICANN 是制定用于管理域名注册和转移的政策的组织机构。

您还可以在 Whois 网站查看域名的状态代码和其它信息。

步骤 1：确认 Amazon Route 53 支持顶级域

请参阅可向 Amazon Route 53 注册的域。。如果您要转移的域的顶级域在列表中，您可以将该域转移到 Amazon Route 53。

如果 TLD 未在列表中，则目前不能将域注册转移到 Route 53。我们偶尔会 TLDs 向列表中添加更多内容，因此请回来查看我们是否为你的域名添加了支持。

步骤 2（可选）：将您的 DNS 服务转移到 Amazon Route 53 或其它 DNS 服务提供商

为何先转移 DNS？

某些注册商提供免费 DNS 服务，当他们收到 Route 53 转移域注册的请求时，可能会立即禁用该 DNS 服务。如果您希望 Route 53 为您的域提供 DNS 服务，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

步骤 3：通过当前注册商更改设置

使用当前注册商提供的方法，对要转移的每个域执行以下各项操作。

- Confirm that the email for the registrant contact for your domain is up to date
- Unlock the domain so it can be transferred
- Confirm that the domain status allows you to transfer the domain
- Disable DNSSEC for the domain
- Get an authorization code
- Renew your domain registration before you transfer the domain (selected geographic TLDs)

确认您的域的注册联系人的电子邮件是最新的

我们将向该电子邮件地址发送电子邮件，以请求转移授权。您需要单击电子邮件中的链接，以对转移进行授权。如果您不单击该链接，则我们必须取消转移。

> **Important**
>
> 根据 ICANN 转移策略，您列为注册人的联系人将拥有作为域名的注册名称持有者的某些权利。大多数域名将在您关闭后删除 Amazon Web Services 账户（有关更多信息，请参阅我的 Amazon 账户已关闭或永久关闭，并且我的域已注册到 Route 53），但是，如果某个域名仍处于已关闭的账户中，则您列为注册人的联系人可能可以请求将域名转让给外部注册商。因此，重要的是，您列出的注册人联系人要么是您自己，要么是您信任的负责任的其他人。

解锁域以使其可转移

ICANN（注册管理机构）要求您在转移域之前先解锁域。

确认域状态允许您转移域

有关更多信息，请参阅 顶级域的转移要求。

禁用域的 DNSSEC

如果您在域中使用 DNSSEC，并将域注册转移到了 Route 53，则必须先在以前的注册商处禁用 DNSSEC。然后，转移域注册后，采取步骤在 Route 53 中为域设置 DNSSEC。Route 53 支持将 DNSSEC 用于域注册，并支持 DNSSEC 签名。有关更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

> **Important**
>
> 如果您在配置了 DNSSEC 的情况下将域注册转移到 Route 53，则 DNSSEC 公有密钥也会转移。如果您将 DNS 服务转移到不支持 DNSSEC 的提供商，则 DNS 解析会间歇性失败，直至您从域中删除 DNSSEC 密钥。有关更多信息，请参阅 删除域的公有密钥。

获取授权代码

来自当前注册商的授权代码会授权我们请求将域注册转移到 Route 53。您将在稍后的过程中在 Route 53 控制台中输入此代码。

某些顶级域有额外的要求：

.co.za 域

您无需获取授权代码即可将 .co.za 域名转移到 Route 53。

.uk、.co.uk、.me.uk 和 .org.uk 域

如果要将 .uk、.co.uk、.me.uk 或 .org.uk 域转移到 Route 53，则无需获取授权代码。相反，请使用当前域注册商提供的方法将域的 IPS 标签的值更新为 GANDI (全部大写)。(.uk 域名的注册机构 Nominet 需要一个 IPS 标签。) 如果您的注册商未提供更改 IPS 标签值的方法，请联系 Nominet。

更改 IPS 标签时，请注意以下事项：

您必须在五天内请求转移

如果在更改 IPS 标签后五天内未请求传输，则标签将更改回先前的值。您必须再次更改 IPS 标签的值，否则传输请求将失败。

在 WHOIS 查询中查看 IPS 标签

在完成转移到 Route 53 之前，对 IPS 标签的更改不会出现在 WHOIS 查询中。

来自 Gandi 的电子邮件

您可能会从我们的注册服务商 Gandi 收到一封有关转移过程的电子邮件。如果您从 Gandi (transfer-auth@gandi.net) 收到一封有关转移您的域的电子邮件，请忽略该电子邮件中的说明，因为它们与 .uk、.co.uk、.me.uk、或 .org.u 域无关。请改为按照本主题中的说明操作。

在转移域名之前，请续订域名注册（选定的地理位置 TLDs）

对于大多数人来说 TLDs，当您转移域名时，注册会自动延长一年。但是，对于某些地理区域 TLDs，当您转移域名时，注册不会延长。如果您要将包含其中一个域名的域名转移到 Route 53 TLDs，我们建议您在转移域名之前续订域名注册，尤其是在到期日临近的情况下。

> **Important**
>
> 如果您未在转移之前续订域，注册可能会在转移完成之前过期。如果出现这种情况，该域在 Internet 上不可用，并且可能会允许其他人购买该域名。

将以下域转移到其他注册商时，不会自动延长注册：

- .ch（瑞士）
- .cl（智利）
- .co.uk（英国）
- .co.za（南非）
- .com.au（澳大利亚）
- .cz（捷克共和国）
- .es（西班牙）
- .fi（芬兰）
- .im（英国属地曼岛）
- .jp（日本）
- .me.uk（英国）
- .net.au（澳大利亚）
- .org.uk（英国）
- .se（瑞典）
- .uk（英国）

步骤 4：获取您的名称服务器的名称

如果您使用 Amazon Route 53 作为 DNS 服务，或者您要继续使用现有的 DNS 服务，则我们将在稍后的过程中自动为您获取名称服务器的名称。跳至步骤 5：请求转移。

如果要在将域转移到 Route 53 的同时将 DNS 服务更改为 Route 53 以外的提供商，请使用由 DNS 服务提供商提供的步骤来获取要转移的每个域的名称服务器的名称。

> **Important**
>
> 如果您的域的注册商也是域的 DNS 服务提供商，请在继续进行域注册转移过程之前，先将您的 DNS 服务转移到 Route 53 或其它 DNS 服务提供商。
> 如果您在转移域注册的同时转移 DNS 服务，则您的网站、电子邮件以及与域相关联的 Web 应用程序可能会变得不可用。有关更多信息，请参阅 步骤 2（可选）：将您的 DNS 服务转移到 Amazon Route 53 或其它 DNS 服务提供商。

步骤 5：请求转移

要将域注册从当前注册商转移到 Amazon Route 53，请使用 Route 53 控制台请求转移。Route 53 会处理与域的当前注册商的通信。

最多可以使用控制台转移五个域。

所使用的步骤取决于您是要转移单个域还是多达五个域：

- 将单个域的域注册转移到 Route 53
- 将最多五个域的域注册转移到 Route 53

使用将域转移到您的账户过程将单个域名转移到您的账户。

将单个域的域注册转移到 Route 53

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 在已注册的域页面上，从转移至下拉列表中选择单个域。
4. 在将域转移到您的账户页面的检查域的可转移性部分，输入要将注册转移到 Route 53 的域的名称，然后选择检查。
5. 如果域注册可供转移，请确认您已完成顶级域的转移要求，然后选择下一步。

   如果域注册不可以转移，则 Route 53 控制台会列出原因。有关如何解决阻止您转移注册的问题的信息，请联系您的注册商。

6. 在 DNS 服务页面上，查看有关名称服务器的信息，然后选择下一步。
7. 如果系统提示，请输入您在 步骤 3：通过当前注册商更改设置 中获得的来自当前注册商的授权代码或 IPS 标签。

   > **Note**
   >
   > 您无需输入授权代码即可将 .co.za、.uk、.co.uk、.me.uk 或 .org.uk 域转移到 Route 53。

   选择下一步。
8. 在域定价选项页面上，选择您想要注册域的年限，以及您是否希望我们在到期日期之前自动续订您的域注册。

   > **Note**
   >
   > 域名注册和续订不可退款。如果您启用自动域续订，并且在我们续订注册之后决定不再需要该域名，您无法获得续订费用的退款。

   选择下一步。
9. 在联系信息页面上，输入域注册人、管理、技术和帐单联系人的联系信息。您在此处输入的值将应用于您要注册的所有域。有关更多信息，请参阅 您在注册或转移域时指定的值。

   请注意以下注意事项：

   名字和姓

   对于 First Name 和 Last Name，我们建议您指定官方 ID 上的名称。对于域设置的某些更改，有些域注册机构要求您提供身份证明。您的 ID 的姓名必须与该域的注册联系人的姓名匹配。

   不同联系人

   默认情况下，我们对全部三个联系人使用相同信息。如果要为一个或多个联系人输入不同的信息，请将与注册人相同切换开关的值更改为关闭位置。

   > **Note**
   >
   > 对于 .it 域，注册者和管理联系人必须相同。

其他必要信息

对于某些顶级域名 (TLDs)，我们需要收集其他信息。对于这些 TLDs，请在邮政/邮政编码字段后输入适用的值。

Privacy protection（隐私保护）

选择是否要向 WHOIS 查询隐藏您的联系人信息。

> **Note**
>
> 必须为管理员、注册者和技术联系人指定相同的隐私设置。

有关更多信息，请参阅以下主题：

- 启用或禁用域联系信息的隐私保护
- 可向 Amazon Route 53 注册的域。

> **Note**
>
> 要为 .uk、.co.uk、.me.uk 和 .org.uk 域启用隐私保护，您必须打开支持案例并请求隐私保护。

选择下一步。

10. 在检查页面上，检查您输入的信息，也可以选择更正这些信息。阅读服务条款，并选中相应复选框，以确认您已阅读服务条款。

    选择 Submit request (提交请求)。

11. 在导航窗格中，选择域，然后选择请求。

    在此页面上，您可以查看域的状态，也可以查看是否需要回复注册联系人的验证电子邮件。您也可以选择重新发送验证电子邮件。

    如果您为注册联系人指定了从未用于通过 Route 53 注册域的电子邮件地址，则某些 TLD 注册机构会要求您验证该地址是否有效。

    我们将从以下电子邮件地址之一发送验证电子邮件：

- noreply@registrar.amazon — 适用于由亚马逊 TLDs注册商注册。
- noreply@domainnameverification.net 或 noreply@emailverification.info — 由我们的 TLDs 注册商助理 Gandi 注册。要确定您的 TLD 注册商是谁，请参阅查找注册商。

> **Important**
>
> 注册联系人必须按照电子邮件中的说明来验证已收到电子邮件，否则我们必须按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

a. 当您收到验证电子邮件时，请选择电子邮件中用于确认电子邮件地址是否有效的链接。如果您没有立即收到该电子邮件，请检查垃圾电子邮件文件夹。

b. 返回请求页面。如果状态不自动更新为 email-address is verified，请选择 Refresh status。

12. 域转移完成后，下一步取决于您要使用 Route 53 还是其它 DNS 服务作为域的 DNS 服务：

- Route 53 — 在您注册域时由 Route 53 创建的托管区域中，创建资源记录集以告知 Route 53 您希望如何为域和子域路由流量。

  例如，当有人在浏览器中输入您的域名并且该查询被转发到 Route 53 时，您希望 Route 53 用您数据中心中 Web 服务器的 IP 地址响应查询还是用 Elastic Load Balancing 的负载均衡器的名称响应查询？

  有关更多信息，请参阅 使用记录。

  > **Important**
  >
  > 如果您在 Route 53 自动创建的托管区域之外的托管区域中创建记录，则必须更新域的名称服务器，以将这些名称服务器用于新托管的区域。

- 其它 DNS 服务 — 配置您的新域，以将 DNS 查询路由到其它 DNS 服务。执行步骤更新名称服务器以使用其他注册商。

使用以下步骤可将最多五个域转移到您的账户。

将最多五个域的域注册转移到 Route 53

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 在导航窗格中，选择 Registered domains。
3. 在已注册的域页面上，从转移至下拉列表中选择多个域。
4. 在将多个域转移到您的账户页面上，输入最多五个您要转移的域，以及每行域的授权码（如果需要），然后选择检查。
5. 如果域注册可供转移，则该域将在域可用性列表中列为可用。选中要转移注册的每个域旁边的复选框，确认您已完成顶级域的转移要求，然后选择下一步。

   如果域注册不可以转移，则 Route 53 控制台会列出原因。有关如何解决阻止您转移注册的问题的信息，请联系您的注册商。
6. 在 DNS 服务页面上，查看有关名称服务器的信息，然后选择下一步。

> **Note**
>
> 域名注册和续订不可退款。如果您启用自动域续订，并且在我们续订注册之后决定不再需要该域名，您无法获得续订费用的退款。

7. 在联系信息页面上，输入域注册者、管理员和技术联系人的联系信息。您在此处输入的值将应用于您要转移的所有域。

> **Important**
>
> 我们建议您为注册人联系人（域拥有者）指定以下值：
>
> - 名和姓：我们建议您指定您的官方 ID 上显示的姓名。对于域设置的某些更改，有些域注册机构要求您提供身份证明。您的 ID 的姓名必须与该域的注册联系人的姓名匹配。
> - 联系详细信息：在域转移过程中，我们建议您指定的值与在当前注册商处指定的值相同。当您更改注册人联系人的联系详细信息时，您会更改域拥有者，但某些 TLD 注册商不允许您在域转移期间更改域拥有者。如果您更改注册人联系人的联系详细信息，则转移过程可能会失败。在您转移域后，您可以更改注册人联系人的详细联系信息。

默认情况下，我们对全部三个联系人使用相同信息。如果要为一个或多个联系人输入不同的信息，请将与注册人相同的值设置为关闭位置。

> **Note**
>
> 对于 .it 域，注册者和管理联系人必须相同。

有关更多信息，请参阅 您在注册或转移域时指定的值。

8. 对于某些人来说 TLDs，我们需要收集其他信息。对于这些TLDs，请在邮政/邮政编码字段后输入适用的值。
9. 如果 Contact Type 的值为 Person，请选择是否要在 WHOIS 查询中隐藏您的联系信息。有关更多信息，请参阅 启用或禁用域联系信息的隐私保护。
10. 选择提交。
11. 检查您输入的信息，阅读服务条款，并选中相应复选框，以确认您已阅读服务条款。
12. 选择 Submit request (提交请求)。

    我们确认域符合转移条件，并向域的注册联系人发出一封电子邮件，以请求转移域的授权。
13. 在导航窗格中，选择域，然后选择请求。

    在此页面上，您可以查看域的状态，也可以查看是否需要回复注册联系人的验证电子邮件。您也可以选择重新发送验证电子邮件。

    如果您为注册联系人指定了从未用于通过 Route 53 注册域的电子邮件地址，则某些 TLD 注册机构会要求您验证该地址是否有效。

    我们将从以下电子邮件地址之一发送验证电子邮件：

    - noreply@registrar.amazon — 适用于由亚马逊 TLDs注册商注册。
    - noreply@domainnameverification.net 或 noreply@emailverification.info — 由我们的 TLDs 注册商助理 Gandi 注册。要确定您的 TLD 注册商是谁，请参阅查找注册商。

    > **Important**
    >
    > 注册联系人必须按照电子邮件中的说明来验证已收到电子邮件，否则我们必须按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

    a. 当您收到验证电子邮件时，请选择电子邮件中用于确认电子邮件地址是否有效的链接。如果您没有立即收到该电子邮件，请检查垃圾电子邮件文件夹。
    b. 返回请求页面。如果状态不自动更新为 email-address is verified，请选择 Refresh status。
14. 域转移完成后，下一步取决于您要使用 Route 53 还是其它 DNS 服务作为域的 DNS 服务：

- Route 53 — 在您注册域时由 Route 53 创建的托管区域中，创建资源记录集以告知 Route 53 您希望如何为域和子域路由流量。

  例如，当有人在浏览器中输入您的域名并且该查询被转发到 Route 53 时，您希望 Route 53 用您数据中心中 Web 服务器的 IP 地址响应查询还是用 ELB 负载均衡器的名称响应查询？

  有关更多信息，请参阅 使用记录。

  > **Important**
  >
  > 如果您在 Route 53 自动创建的托管区域之外的托管区域中创建记录，则必须更新域的名称服务器，以将这些名称服务器用于新托管的区域。

- 其它 DNS 服务 — 配置您的新域，以将 DNS 查询路由到其它 DNS 服务。执行步骤更新名称服务器以使用其他注册商。

步骤 6：单击确认和授权电子邮件中的链接

在您请求转移后不久，我们会向该域的注册联系人发送一封或多封电子邮件：

确认注册联系人可联系上的电子邮件

如果您从未向 Route 53 注册域或向 Route 53 转移域，我们会向您发送一封电子邮件，要求您确认电子邮件地址是有效的。我们保留此信息，因此我们不必再次发送此确认电子邮件。

获取转移域的授权的电子邮件

对于某些人来说 TLDs，您需要回复电子邮件才能授权域名转移。

泛型， TLDs 例如.com、.net 和.org

具有通用 TLD（如 .com、.net 或 .org）的域无需授权。

地理位置， TLDs 例如.co.uk 和.jp

对于具有地理 TLD 的域，我们需要获取您的授权来转移域。如果您转移 10 个域，我们必须向您发送 10 封电子邮件，您必须单击每封电子邮件中的授权链接。

电子邮件将全部送至域的注册联系人：

- 如果您是域注册联系人，请按照该电子邮件中的说明授权转移。

- 如果其他人是注册联系人，请要求此人按照电子邮件中的说明授权转移。

> **Important**
>
> 如果您要转移具有地理 TLD 的域，我们将最多等待 5 天时间以便注册联系人授权转移。如果注册联系人在五天内未做出响应，我们将取消转移操作，并向注册联系人发送一封电子邮件，以告知取消事宜。

主题

新所有者或电子邮件地址的授权电子邮件

如果更改了以下值，我们会向您单独发送一封电子邮件，要求提供授权：

域所有者

如果您更改域的所有者 (如哪些因素会触发域所有权更改？中所述)，我们会向域的注册联系人发送电子邮件。

注册人联系人的电子邮件地址（仅适用于某些 TLDs人）

对于某些人 TLDs，如果您更改注册人联系人的电子邮件地址，我们会向注册人联系人的旧电子邮件地址和新电子邮件地址发送一封电子邮件。收到电子邮件的注册联系人必须按照电子邮件中的说明授权更改。

对于对域所有者或注册联系人电子邮件地址的更改，如果我们在 3-15 天内未收到更改授权（具体时间取决于顶级域），我们必须按照 ICANN 的要求取消请求。

发出授权电子邮件的电子邮件地址

所有电子邮件均来自以下电子邮件地址之一。

TLDs	发出授权电子邮件的电子邮件地址
.com.au 和 .net.au	no-reply@ispapi.net 该电子邮件包含指向 http://transfers.ispapi.net 的链接。
.fr	nic@nic.fr (如果您在转移域的同时要更改 .fr 域名的注册联系人)。(会将该电子邮件同时发送给当前注册联系人和新注册联系人。)
所有其他地址	以下电子邮件地址之一： • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

要确定您的 TLD 注册商是谁，请参阅可向 Amazon Route 53 注册的域。。

当前注册商的批准

如果注册联系人授权转移，我们将开始与您当前的注册商合作转移您的域。此步骤最多可能需要十天时间，具体取决于您的域的 TLD：

- 通用顶级域 — 最多需要七天时间
- 地理顶级域（也称为国家/地区代码顶级域）— 最多需要十天时间

如果您当前的注册商没有回复我们的转移请求 (此情况在注册商中很常见)，将自动进行转移。如果您当前的注册商拒绝转移请求，我们会向当前注册联系人发送一封电子邮件通知。注册者需要联系当前的注册商，并解决转移问题。

接下来会发生什么

当您的域转移获得批准后，我们会向注册联系人发送另一封电子邮件。有关此过程的更多信息，请参阅查看域转移的状态。

域名转移完成后，我们会立即向您的 Amazon 账户收取域名转移费用。有关按 TLD 收费的列表，请参阅 Amazon Route 53 域注册定价。

> **Note**
>
> 这是一次性费用，所以该费用不会显示在您的 CloudWatch 账单指标中。有关 CloudWatch 指标的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch指标。

步骤 7：更新域配置

转移完成后，您可以选择更改如下设置：

转移锁定

要将域转移到 Route 53，您必须禁用转移锁定。如果要重新启用锁定以防止未经授权的转移，请参阅Locking a domain to prevent unauthorized transfer to another registrar（锁定域以防止未经授权转移到另一个注册商）。

Automatic renewal（自动续订）

我们将转移的域配置为在到期日期临近时自动续订。有关如何更改此设置的信息，请参阅启用或禁用域自动续订。

延长注册期

预设情况下，Route 53 每年都会续订域。如果要将域注册更长的时间，请参阅延长域的注册期。

DNSSEC

有关配置域的 DNSSEC 的信息，请参阅为域配置 DNSSEC。

防止 Route 53 的常见转移问题

如果您在域转移过程中遇到问题，以下是最常见的问题以及解决方法：

> **Note**
>
> 如果您的转移已经失败，请参阅 将我的域转移到 Amazon Route 53 失败 了解故障后的疑难排解。

您没有收到授权电子邮件

如果您没有收到来自 Route 53 的授权电子邮件，以下是最常见的原因和解决方案：

- 检查您的垃圾邮件文件夹 - 授权电子邮件有时会被电子邮件提供商过滤。
- 验证您的电子邮件地址 - 确认您域的联系人信息中的注册商电子邮件地址是最新且可以访问。
- 更新您的联系人信息 - 如果电子邮件地址已过期，请在开始转移之前向当前的注册商进行更新。
- 重新发送授权电子邮件 - 在 Route 53 控制台中，针对处于转移状态的域单击“重新发送授权电子邮件”。

您收到“授权代码无效”错误

如果您收到“授权码无效” 错误，请尝试以下解决方案：

- 仔细检查代码 - 授权代码区分大小写。直接从注册商的界面复制并粘贴代码，以免出现键入错误。
- 检查代码是否已过期 - 授权代码可能在 5-30 天之间过期，具体取决于您当前的注册商。如果您的验证代码已过期，请申请新的代码。
- 移除多余的空格 - 确保在输入代码时没有前导或尾随空格。
- 获取新的授权代码 - 如果代码仍然失败，请向当前的注册商申请新的授权代码。

您的域已在当前注册商处锁定

当您的当前注册商启用转移锁定（也称为“域锁定”或“禁止客户转移”）时，域转移可能会失败。这是一种常见的安全设置，可防止未经授权的转移。

要解决此问题，请执行以下操作：

- 解锁您的域 - 登录当前注册商的控制面板并禁用域转移锁定。
- 验证是否已移除锁定 - 您可以使用任何公有 WHOIS 查询工具确认域状态显示为“OK”，而不是“clientTransferProhibited”。
- 向注册商寻求帮助 - 如果您看不到解锁域的选项，请联系当前注册商的支持团队。他们可以帮助您移除锁定。

您的域不符合转移资格

如果您的域转移由于资格问题而被拒绝，请检查以下内容：

- 验证域年龄 - 自注册或上次转移以来，您的域必须已存在至少 60 天。
- 检查 TLD 支持 - 确认 Route 53 支持您域的顶级域（TLD）。有关支持的 TLD，请参阅 可向 Amazon Route 53 注册的域。。
- 审查域状态 - 带有特定状态码（例如“pendingTransfer”或“redemptionPeriod”）的域无法转移。

- 检查过期日期 - 已过期或过期后 15 天内的域可能无法转移。
- 解决账单问题 - 确保您当前注册商的所有未付费用均已支付。

您的转移时间超出预期

如果您的转移似乎出现延迟，您应该了解以下内容：

- 正常时间范围 - 大多数转移在 5-7 天内完成，但最长可能需要 10 天。
- 监控转移状态 - 在 Route 53 控制台中查看您的转移进度。有关更多信息，请参阅 查看域转移的状态。
- 快速回复电子邮件 - 两家注册商都可能发送确认电子邮件，要求您回复此电子邮件才能继续。
- 联系您当前的注册商 - 如果转移延迟，请联系您当前的注册商，确保他们没有阻止转移。

何时联系 Amazon Support

如果您尝试上述解决方案，但问题仍然存在，或者遇到以下问题，请联系 Amazon Support：

- 多次尝试输入正确信息后转移失败
- 转移过程中的账单或付款问题
- Route 53 控制台中的技术错误使您无法开始转移
- 处于“待处理”状态超过 10 天的转移

联系支持人员时，请提供您的域名、转移请求 ID（如果有）以及有关您遇到的特定错误或问题的详细信息。

将域从 Amazon Route 53 转移到另一注册商

当您将域从 Amazon Route 53 转移到另一个注册商时，您会从 Route 53 中获取一些信息，并将其提供给新的注册商。新注册商将执行剩余的工作。

> **Important**
>
> 如果您目前正在使用 Route 53 作为您的 DNS 服务提供商，并且还要将 DNS 服务转移到另一个提供商，请注意，以下 Route 53 功能与其它 DNS 服务提供商提供的功能并没有直接并行的关系。您需要与新的 DNS 服务提供商一起合作，来确定如何实现类似的功能：
>
> - 别名记录。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。
> - 简单路由策略以外的路由策略。有关更多信息，请参阅 选择路由策略。
> - 与记录关联的运行状况检查。有关更多信息，请参阅 配置 DNS 故障转移。

大多数域注册商对将域转移到其他注册商施加了要求。这些要求的主要目的是为了防止欺诈性域的拥有者反复在不同注册商之间转移域。各注册商要求不尽相同，但以下为典型要求：

- 您必须至少在 14 天前向当前注册商注册域或将域注册转移到当前注册商。
- 域不能具有以下任何域名状态代码：
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - serverTransferProhibited

有关域名状态代码的最新列表以及对每个代码含义的解释，请转到 ICANN 网站并搜索 epp status codes。(搜索 ICANN 网站；Web 搜索有时会返回旧版文档。)

> **Note**
>
> 如果您想将域名转移到其他域名注册商，但注册域名的 Amazon 账户已关闭、暂停或终止，则可以联系 Su Amazon pport 寻求帮助。域名不能在注册后的前 14 天内转移。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

> **Note**
>
> 如果新的注册商需要 REG-ID 码，您可以联系 Support 寻求 Amazon 帮助。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

要将域从 Route 53 转移到其它注册商

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择您要转移到其他注册商的域的名称。
4. 在域名页面上，检查域名状态代码的值。如果它是如下值之一，则当前无法转移域：
   - pendingDelete

- pendingTransfer
- redemptionPeriod
- clientTransferProhibited
- serverTransferProhibited

有关域名状态代码的最新列表以及对每个代码含义的解释，请转到 ICANN 网站并搜索 epp status codes。(搜索 ICANN 网站；Web 搜索有时会返回旧版文档。)

如果域名状态码的值为 serverTransferProhibited，则可以免费联系 Su Amazon pport，了解为转移域名必须做什么。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

5. 如果转移锁定的值为开，请从操作下拉列表中选择关闭转移锁定。
6. 除 .be、.co.za、.ru、.uk、.co.uk、.me.uk 和 .org.uk 域之外的所有域 — 在域名页面上，从转出下拉列表中选择转移到其他注册商。

   在转移到其他注册商对话框中，选择复制以复制域名转移的授权码。您将在此过程的后续步骤中向您的注册商提供此值。

   > **Note**
   >
   > 对于.eu 域，您还可以在以下注册机构处使用“my.eu”面板生成授权代码：https://my.eurid.eu/。

   .be、.co.za、.es、.ru、.uk、.co.uk、.me.uk 和 . org.uk 域 — 执行以下操作：

   .be 域

   从 DNS 比利时网站的注册机构处获得 .ru 域的授权代码。

   .co.za 域

   您无需获取授权代码即可将 .co.za 域名转移到其他注册商。

   .ru 域

   从.ru 域名的注册局获取授权码，网址为 https://www.nic。 ru/en/auth/recovery/:

   a. 选择按域名恢复凭证的选项。

   b. 输入您的域名，然后选择继续。

c. 按照屏幕上的提示进行操作，以进入 RU-CENTER 管理页面。

d. 在 Manage your account (管理您的账户) 部分中，选择 Domain transfer (域转移)。

e. 与 REGRU-RU 确认转移。

.uk、.co.uk、.me.uk 和 .org.uk 域

将 IPS 标签更改为新注册商的值：

a. 转到 Nominet 网站的 Find a Registrar 页面，然后查找新注册商的 IPS 标签。(Nominet 是 .uk、.co.uk、.me.uk 和 .org.uk 域的注册机构。)

b. 在已注册域 >域名页面上，选择转出下拉列表，然后选择更新 IPS 标签，并指定您在步骤 6a 中获得的值。

c. 选择更新。

> **Note**
>
> 您也可以在 Nominet 控制台上更新 IPS 标签。有关说明，请参阅切换注册商。

7. 如果您目前没有使用 Route 53 作为域的 DNS 服务提供商，请跳至步骤 10。

   如果您当前正在使用 Route 53 作为域的 DNS 服务提供商，请执行以下步骤：

   a. 请选择 Hosted Zones (托管区域)。

   b. 选择您的域的托管区域的名称。域和托管区域具有相同的名称。

   c. 如果您希望继续使用 Route 53 作为域的 DNS 服务提供商：获取 Route 53 分配到您的托管区域的四个名称服务器的名称。有关更多信息，请参阅 获取公有托管区域的名称服务器。

      如果不想继续使用 Route 53 作为域的 DNS 服务提供商：请记下您的所有记录（除 NS 和 SOA 记录之外）的设置。对于特定于 Route 53 的功能（比如别名记录），您需要与您的新 DNS 服务提供商一起合作，以确定如何实现类似的功能。

8. 如果您要将 DNS 服务转移到另一个提供商，请使用新 DNS 服务提供的方法执行以下任务：

   - 创建一个托管区域
   - 创建可重现 Route 53 记录的功能的记录
   - 获取新 DNS 服务分配到您的托管区域的名称服务器

9. 使用由新注册商提供的过程来请求转移域。

除 .co.za、.uk、.co.uk、.me.uk 和 .org.uk 域之外的所有域 — 系统将提示您输入在此过程的步骤 6 中从 Route 53 控制台获得的授权代码。

10. 如果您仍然希望使用 Route 53 作为 DNS 服务提供商，请使用由新注册商提供的过程来指定您在步骤 7 中获得的 Route 53 名称服务器的名称。如果要使用其他 DNS 服务提供商，则在步骤 8 中创建新的托管区时，请指定新提供商为您提供的名称服务器的名称。
11. 回复确认电子邮件：

    除 .jp 域之外的所有域

    Route 53 会向该域的注册联系人的电子邮件地址发送确认电子邮件：

    - 如果您未回复此电子邮件，则转移会在指定日期自动执行。
    - 如果您希望尽快执行转移或希望取消转移，请选择电子邮件中的链接来转到 Route 53 网站，然后选择适用的选项。
    - 根据顶级域名的不同，确认电子邮件可能包含一个链接，指向 https://approvemove.com您可以批准或拒绝转移。为域名联系人启用隐私保护后，电子邮件将从在亚马逊注册商处注册 TLDs 的 identity-protect.org 地址发送。要确定您的 TLD 注册商是谁，请参阅查找注册商。

    .jp 域

    Route 53 向域名注册人联系人的电子邮件地址发送一封确认电子邮件，地址为 noreply@domainnameverification.net 或 noreply@emailverification.info，其中包含确认转移的链接：

    - 如果您未回复此电子邮件，则转移会在指定日期取消。
    - 如果您希望尽快执行转移或希望取消转移，请选择电子邮件中的链接来转到 Route 53 网站，然后选择适用的选项。您需要提供在步骤 7 中提供域的授权码。

    此外，您可能会收到来自 WIXI.jp 的电子邮件。您可以忽略此邮件。
12. 如果您要将域转移到的域注册商报告转移失败，请联系该注册商以了解更多信息。当您将域转移到其它注册商时，所有状态更新将转到新的注册商，因此 Route 53 没有有关转移失败原因的信息。

    如果新注册商因为您从 Route 53 收到的授权代码无效而报告转移失败，请向 Amazon Support 开设一个案例。（您不需要支持合同，且没有费用。）有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

> **Note**
>
> Gandi 生成的授权代码有效期约为 5 天。如果您在此时间段之后尝试转移，则可能会因为代码过期而失败。

13. 如果您将 DNS 服务转移到了另一个 DNS 服务提供商，则可以在 DNS 解析程序停止响应包含 Route 53 名称服务器的名称的 DNS 查询之后删除托管区域中的记录并删除托管区域。此过程通常需要两天时间，这是 DNS 解析程序缓存域的名称服务器的名称通常消耗的时间量。

    > **Important**
    >
    > 如果您在 DNS 解析程序仍在响应包含 Route 53 名称服务器的名称的 DNS 查询的同时删除托管区域，则您的域将在互联网上不可用。

    在删除一个托管区域后，Route 53 将停止计算该托管区域的月费。有关更多信息，请参阅以下文档：

    - 删除记录
    - 删除公有托管区域
    - Route 53 定价

将域转移到其它 Amazon 账户

如果您使用某个 Amazon 账户注册了域，并且想要将该域转移到另一个 Amazon 账户，则可以使用新控制台或使用 Amazon CLI 或其他编程方法方便地转移。

主题

步骤 1：将域转移到其它 Amazon 账户

域名不能在注册后的前 14 天内转移。

启动域转移后，您必须使用根账户，或者使用通过以下一种或多种方式被授予 IAM 权限的用户登录：

- 为用户分配了 AdministratorAccess 托管策略。
- 为用户分配了 AmazonRoute53DomainsFullAccess 托管策略。
- 为用户分配了 AmazonRoute53FullAccess 托管策略。
- 为用户分配了 PowerUserAccess 托管策略。
- 用户有权执行以下所有操作：`TransferDomains`、`DisableDomainTransferLock` 和 `RetrieveDomainAuthCode`。

如果您没有使用根账户或者具有所需权限的用户登录，则我们将无法执行转移。此要求可防止未经授权的用户将域转移到其它 Amazon Web Services 账户。

转移过程分为两个步骤。首先，原始账户拥有者启动转移：在启动向另一个 Amazon Web Services 账户 转移程序中，目标账户拥有者在接受从另一个 Amazon Web Services 账户 转移步骤中接受转移。

将域转移到其它 Amazon 账户

1. 使用域当前注册到的 Amazon Web Services 账户 登录 Amazon。
2. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Registered domains。
4. 选择您要转移到另一个 Amazon Web Services 账户 的域的名称。
5. 在详细信息部分上方的转移出下拉列表中，选择转移到另一个 Amazon Web Services 账户。
6. 在转移到另一个 Amazon Web Services 账户 对话框中，输入目标账户 ID。您可以从目标 Amazon Web Services 账户 拥有者获得此 ID。
7. 选择确认。
8. 在生成密码对话框中，复制密码，并将其转发给接收 Amazon Web Services 账户 拥有者。

   在请求页面上，域的状态将显示正在进行中，类型将显示内部传出。

接受来自其他 Amazon 账户的域转移

1. 使用接收域的 Amazon Web Services 账户 登录 Amazon。
2. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择请求。
4. 在请求页面上，选择要从另一个 Amazon Web Services 账户 转移的域名旁边的单选按钮。如果域已准备好转移，则状态为需要执行操作，类型为内部转移域。

您有三天的时间来接受请求。如果在三天内未接受转移，则转移请求将取消。

5. 在操作下拉列表中，选择接受。

   您也可以选择拒绝来取消转移过程。

6. 如果您接受，请在将域转移到您的账户页面的密码部分，输入您从原始账户拥有者收到的密码。

   阅读条款和条件，然后选择下一步。

7. 导航至请求页面，以监控转移状态和其他需要完成的步骤。

8. 转移完成后，您可以更新联系信息。有关更多信息，请参阅 更新域的联系信息和所有权。

以编程方式转移域

您可以使用 Amazon CLI、Amazon SDK 之一或 Route 53 API 以编程方式转移域。有关更多信息，请参阅以下文档：

- 有关转移过程的概览和有关使用 Route 53 域注册 API 转移域的 API 操作的文档，请参阅 Amazon Route 53 API 参考中的 TransferDomainToAnotherAwsAccount。
- 有关以编程方式转移域的其它选项的文档，请参阅“Amazon 文档”页面的指南和 API 参考部分中的“软件开发工具包和工具包”。
- 接收账户有三天时间使用 transfer-domain-to-another-aws-account API 接受来自原始账户的转移。如果在三天内未接受转移，则转移请求将取消。

> **Important**
>
> 当您将域转移到其它 Amazon 账户时，不会转移域的托管区。如果您还想转移托管区域，请等到域转移完成，然后查看步骤 2（可选）：将托管区域迁移到其它 Amazon 账户。

步骤 2（可选）：将托管区域迁移到其它 Amazon 账户

如果您使用 Route 53 作为域的 DNS 服务，则在您将域转移到其它 Amazon 账户时，Route 53 不会转移托管区域。如果域注册与一个账户相关联，且相应的托管区域与另一个账户相关联，则域注册和 DNS 功能都不受影响。唯一的影响是，您需要使用一个账户登录 Route 53 控制台查看域，并使用另一个账户登录以查看托管区域。

如果您拥有从中传输域的账户以及将域传输到的账户，您可以选择将域的托管区域迁移到不同账户，但这不是必需的。Route 53 将继续使用现有托管区域中的记录来路由域的流量。

> **Important**
>
> 如果您未拥有从中传输域的账户以及将域传输到的账户，则必须将现有托管区域迁移到您将域传输到的 Amazon 账户，或者在您拥有的 Amazon 账户中创建新的托管区域。如果您未拥有创建了用于路由域流量的托管区域的账户，则无法控制如何路由流量。

要将现有托管区域迁移到新账户，请参阅将托管区迁移到其它 Amazon 账户。

要创建新的托管区域，请参阅将 Amazon Route 53 作为现有域的 DNS 服务。此主题通常在从其它注册商向 Route 53 传输域时使用，但当您将域从一个 Amazon 账户传输到另一个时，过程是相同的。

> **Important**
>
> 白标签名称服务器：如果您的域使用白标签名称服务器（类似于 ns1.example.com 的自定义名称服务器主机名），则需要执行其他步骤：
>
> - 转移域注册时：转移完成后，向新的注册商更新粘附记录
> - 迁移托管区时：在区域迁移后，请向域注册商更新粘附记录，因为即使主机名保持不变，IP 地址也会更改
>
> 有关详细说明，请参阅the section called “步骤 7：创建粘附记录和更改注册商的名称服务器”。

查看域转移的状态

在您启动从其它域注册商到 Amazon Route 53 的域转移之后，可以在请求页面（新控制台）或 Route 53 控制台的待处理请求（旧控制台）页面上跟踪其状态。Status 列中包含当前步骤的简要描述。以下列表中包含了控制台中的文字，以及对每个步骤更加详细的描述。

> **Note**
>
> 当您提交转移请求时，初始状态为 Domain transfer request submitted，该状态表明我们已经收到您的请求。

确定域是否满足转移要求 (步骤 1/14)

我们要确定您的域状态是否符合转移资格。必须解锁您的域，并且在您提交转移请求时，该域不能包含以下任何状态代码：

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

仅限地理 TLD — 验证 WHOIS 信息（步骤 2/14）

如果您要转移具有地理 TLD 的域，我们将对您的域发送 WHOIS 查询，以确定您是否已禁用域的隐私保护。如果当前的注册商仍然在启用隐私保护，我们将无法访问转移域所需的信息。

> **Note**
>
> 具有通用 TLD（如 .com、.net 或 .org）的域无需授权。

仅限地理 TLD — 向注册联系人发送电子邮件以获取转移授权（步骤 3/14）

如果您要转移具有地理 TLD 的域，我们将向该域的注册联系人发送电子邮件。此电子邮件的目的是确认转移由域的授权联系人所请求。

> **Note**
>
> 具有通用 TLD（如 .com、.net 或 .org）的域无需授权。

向当前注册商验证转移 (步骤 4/14)

我们已经向域的当前注册商发送请求，以启动转移。

仅限地理 TLD — 等待来自注册联系人的授权（步骤 5/14）

我们已向域的注册联系人发送电子邮件 (请参阅步骤 3/14)，正在等待注册联系人单击电子邮件中的链接来授权转移。如果您要转移具有地理 TLD 的域，并且您出于某种原因而没有收到电子邮件，请参阅重新发送授权和确认电子邮件。

已联系当前的注册商以请求转移 (步骤 6/14)

我们要与当前的域注册商合作以最终确定转移。

等待当前的注册商完成转移 (步骤 7/14)

您当前的注册商要确认您的域是否符合转移要求。此步骤最多可能需要十天时间，具体取决于您的域的 TLD：

- 通用顶级域 — 最多需要七天时间
- 地理顶级域（也称为国家/地区代码顶级域）— 最多需要十天时间

> **Note**
>
> 如果您在转移 .JP 域时已批准从 Route 53 发送的确认电子邮件，但在步骤 7 中它已停止数天，请联系 Amazon Support 中心寻求帮助。

对于大多数注册商，该过程是完全自动化的，不能加速。有些注册商会向您发送电子邮件，请求您批准转移；如果您的注册商发送此确认电子邮件，则转移过程可能会比七到十天快得多。

有关注册商可能拒绝转移的原因的信息，请参阅顶级域的转移要求。

向注册联系人确认该联系人是否已启动转移 (步骤 8/14)

某些 TLD 注册机构会向注册联系人发送另一封电子邮件，以确认授权用户是否已请求域转移。

将名称服务器与注册机构同步 (步骤 9/14)

只有当您作为转移请求的一部分而提供的名称服务器与当前注册商列出的名称服务器不同时，才会执行此步骤。我们会尝试将您的名称服务器更新为您所提供的新名称服务器。

将设置与注册机构同步 (步骤 10/14)

我们要验证转移是否已成功完成，并将您的域相关数据与我们的注册商合作者进行同步。

向注册机构发送更新的联系信息 (步骤 11/14)

如果您在请求转移时更改了域的所有权，则我们将尝试进行此更改。不过，大多数注册机构不允许在转移域的过程中转移所有权。

最终确定向 Route 53 转移 (步骤 12/14)

我们确认转移过程已成功。

最终确定转移 (步骤 13/14)

我们将在 Route 53 中设置您的域。

转移完成 (步骤 14/14)

您的转移已成功完成。

将域转移到 Amazon Route 53 对域注册的到期日期有何影响

当您在注册商之间转移域时，某些 TLD 注册机构允许您让域的到期日期保持不变，某些注册机构会向到期日期添加一年，而某些注册机构会将到期日期更改为转移日期之后一年。

> **Note**
>
> 对于大多数 TLD，您可以在将域转移到 Amazon Route 53 之后将域的注册期延长达十年之久。有关更多信息，请参阅 延长域的注册期。

通用 TLD

当您将具有通用 TLD (例如 .com) 的域转移到 Route 53 时，域的新到期日期为在您之前的注册商规定的到期日期的基础上再加一年。

地理 TLD

当您将具有地理 TLD (例如 .co.uk) 的域转移到 Route 53 时，域的新到期日期取决于该 TLD。在下表中找到您的 TLD，以确定转移您的域对到期日期有何影响。

洲	地理 TLD 和转移域对到期日期的影响
非洲	.co.za — 到期日期保持不变。
美洲	.cl、.com.ar、.com.br — 到期日期保持不变。 .ca、.co、.mx、.us — 在旧的到期日期的基础上增加一年。
亚洲/大洋洲	.com.au、.com.sg、.jp、.net.au、.sg – 到期日期保持不变。 .co.nz、.in、.net.nz、.org.nz - 在原来到期日期的基础上再增加一年。
欧洲	.ch、.co.uk、.es、.fi、.me.uk、.org.uk、.se — 到期日期保持不变。 .berlin、.eu、.io、.me、.ruhr、.wien — 在旧的到期日期的基础上增加一年。

洲	地理 TLD 和转移域对到期日期的影响
	.be、.de、.fr、.it、.nl — 新的到期日期为转移日期之后一年。

重新发送授权和确认电子邮件

对于与域注册相关的几个操作，ICANN 要求我们从域的注册联系人获取授权，或确认注册联系人的电子邮件地址有效。为了获取授权或确认，我们会发送一封电子邮件，邮件中包含一个链接。您有 3 到 15 天的时间来单击该链接，具体时间取决于执行的操作和顶级域。在这之后，该链接将失效。

如果您未在分配的时间内单击电子邮件中的链接，ICANN 通常会要求我们暂停域或取消操作，具体取决于您尝试执行的操作：

注册域

我们暂停了域，因此不能在 Internet 上访问它。要重新发送确认电子邮件，请参阅为域注册重新发送确认电子邮件。

TLDs 仅限地理位置 — 将域名转移到 Amazon Route 53

如果您要转移具有地理 TLD 的域，我们将取消此转移。要重新发送授权电子邮件，请参阅为域转移重新发送授权电子邮件。

> **Note**
>
> 具有通用 TLD（如 .com、.net 或 .org）的域无需授权。

更改域的注册联系人 (所有者) 的姓名或电子邮件地址

我们取消了更改。要重新发送授权电子邮件，请参阅重新发送授权电子邮件以更新注册联系人或删除域。

删除域

我们取消了删除请求。要重新发送授权电子邮件，请参阅重新发送授权电子邮件以更新注册联系人或删除域。

TLDs 仅限地理位置-将域名从 Route 53 转移到其他注册商

如果您要转移具有地理 TLD 的域，新注册商将取消此转移。

> **Note**
>
> 具有通用 TLD（如 .com、.net 或 .org）的域无需授权。

主题

更新电子邮件地址

我们始终会向域的注册联系人的电子邮件地址发送确认和授权电子邮件。对于某些人 TLDs，在以下情况下，我们需要向注册人联系人的旧电子邮件地址和新电子邮件地址发送电子邮件：

- 您正在更改已向 Amazon Route 53 注册的域的电子邮件地址
- 您正在更改转移到 Route 53 的域的电子邮件地址

重新发送电子邮件

请遵循适用的过程重新发送确认或授权电子邮件。

- 为域注册重新发送确认电子邮件
- 为域转移重新发送授权电子邮件
- 重新发送授权电子邮件以更新注册联系人或删除域

为域注册重新发送确认电子邮件

1. 检查注册联系人的电子邮件地址，必要时更新。有关更多信息，请参阅 更新域的联系信息和所有权。
2. 检查电子邮件应用程序的垃圾邮件文件夹中是否存在来自以下电子邮件地址之一的电子邮件。

   如果时间太久，该链接将会失效，但我们会再向您发送一封电子邮件，告知您如何查找确认电子邮件。

TLDs	发送批准或确认电子邮件的电子邮件地址

TLDs	发送批准或确认电子邮件的电子邮件地址
.fr	nic@nic.fr
所有其他地址	以下电子邮件地址之一： • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> 这些电子邮件可能包含指向 www.verify-whois.com 的链接。此链接可以安全使用。

3. 使用 Amazon Route 53 控制台重新发送确认电子邮件：

   a. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   b. 在导航窗格中，选择 Registered domains。

   c. 选择希望为其重新发送电子邮件的域的名称。

   d. 在标题为“Your domain might be suspended”的警告框中，选择 Send email again。

   > **Note**
   >
   > 如果没有警告框，则表示您已确认注册联系人的电子邮件地址有效。

4. 如果您在重新发送确认电子邮件时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

为域转移重新发送授权电子邮件

此方法不适用于 .jp 域转出请求。

1. 使用当前域注册商提供的方法，确认域的隐私保护是否处于禁用状态。如果没有，请将其禁用。

   我们会向当前注册商保存在 WHOIS 数据库中的电子邮件地址发送授权电子邮件。启用隐私保护后，该电子邮件地址通常会被屏蔽。当前注册商可能不会将 Amazon Route 53 发送到 WHOIS 数据库中的电子邮件地址的电子邮件发送到您的实际电子邮件地址。

   > **Note**
   >
   > 如果域的当前注册商不让您关闭隐私保护，而您在步骤 5：请求转移中指定了有效的授权代码，则我们仍可以转移域。

2. 检查注册联系人的电子邮件地址，必要时更新。请使用域的当前注册商提供的方法。
3. 检查电子邮件应用程序的垃圾邮件文件夹中是否存在来自以下电子邮件地址之一的电子邮件。

   如果时间太久，该链接将会失效，但我们会再向您发送一封电子邮件，告知您如何查找授权电子邮件。

TLDs	发送批准或确认电子邮件的电子邮件地址
.com.au 和 .net.au	no-reply@ispapi.net 该电子邮件包含指向的链接https://approve.domainadmin.com。
.fr	nic@nic.fr
所有其他地址	以下电子邮件地址之一： • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> 这些电子邮件可能包含指向 www.verify-whois.com 的链接。此链接可以安全使用。

4. 如果转移已停止 (例如我们因为时间太长而取消了转移)，请再次请求转移，我们会向您发送另一封授权电子邮件。

> **Note**
>
> 在请求转移后的前 15 天内，您可以通过检查 Route 53 控制台的 Dashboard（控制面板）页面上的 Notifications（通知）表格确定转移的状态。15 天后， Amazon CLI 使用获取状态。有关更多信息，请参阅 Amazon CLI 命令引用中的 route53domains。

   如果转移仍在进行，请执行以下步骤重新发送授权电子邮件。

   a. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
   b. 在 Notifications（通知）表中，找到希望转移的域。
   c. 在该域的 Status 列中，选择 Resend email。

5. 如果您在重新发送域名转移授权电子邮件时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

重新发送授权电子邮件以更新注册联系人或删除域

1. 检查注册联系人的电子邮件地址，必要时更新。有关更多信息，请参阅 更新域的联系信息和所有权。
2. 检查电子邮件应用程序的垃圾邮件文件夹中是否存在来自以下电子邮件地址之一的电子邮件。

   如果时间太久，该链接将会失效，但我们会再向您发送一封电子邮件，告知您如何查找授权电子邮件。

TLDs	发送授权电子邮件的电子邮件地址
.fr	nic@nic.fr

TLDs	发送授权电子邮件的电子邮件地址
所有其他地址	以下电子邮件地址之一： • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> 这些电子邮件可能包含指向 www.verify-whois.com 的链接。此链接可以安全使用。

3. 取消更改或删除。你有两个选择：

   - 您可以等待 3 至 15 天，此后我们将自动取消请求的操作。
   - 或者，您可以联系 S Amazon upport，要求他们取消操作。

> **Important**
>
> 转移类型和取消方式：取消方法取决于转移类型：
>
> - Route 53 的外部注册商：按照本主题中的步骤操作（等待自动取消或联系 Su Amazon pport）
> - Amazon 账户之间：使用 `CancelDomainTransferToAnotherAwsAccount` API 或联系 Suppor Amazon t
>
> 请勿联系您当前的外部注册商取消向 Route 53 的转移，因为他们无法取消使用 Amazon 已经在进行的转移。

4. 取消更改或删除后，您可以再次更改联系信息或删除域，我们会向您发送另一封授权电子邮件。

5. 如果您在重新发送授权电子邮件时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

为域配置 DNSSEC

攻击者有时会通过拦截 DNS 查询并向 DNS 解析程序返回自己的 IP 地址而不是 Internet 端点的实际 IP 地址来劫持发往这些端点的流量。然后，系统会将用户路由到攻击者在虚假响应中提供的 IP 地址，例如虚假网站。

可以通过配置用于确保 DNS 流量安全的协议 – 域名系统安全扩展 (DNSSEC) 来保护您的域免受此类攻击，即 DNS 欺骗或中间人攻击。

> **Important**
>
> Amazon Route 53 支持将 DNSSEC 签名和 DNSSEC 用于域注册。如果要为使用 Route 53 注册的域配置 DNSSEC 签名，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

主题

DNSSEC 如何保护域的概览

当您为域配置 DNSSEC 时，DNS 解析程序将为来自中间解析程序的响应建立信任链。该信任链从域 (您的域的父区域) 的 TLD 注册机构开始，至 DNS 服务提供商的授权名称服务器结束。并非所有 DNS 解析程序都支持 DNSSEC。仅支持 DNSSEC 的解析程序将执行任何签名或真实性验证。

为清晰起见，下面简要介绍如何为向 Amazon Route 53 注册的域配置 DNSSEC，以保护您的互联网主机免遭 DNS 欺骗：

1. 使用 DNS 服务提供商提供的方法通过非对称密钥对中的私有密钥 来签署 托管区域内的记录。

> **Important**
>
> Route 53 支持将 DNSSEC 签名和 DNSSEC 用于域注册。要了解更多信息，请参阅在 Amazon Route 53 中配置 DNSSEC 签名。

2. 向域注册商提供密钥对中的公有密钥，并指定用于生成密钥对的算法。域注册商会将公有密钥和算法转发给顶级域 (TLD) 的注册机构。

   有关如何为向 Route 53 注册的域执行此步骤的信息，请参阅 为域添加公有密钥。

在配置 DNSSEC 后，下面介绍如何保护您的域免受 DNS 欺骗：

1. 提交 DNS 查询，例如通过浏览网站或发送电子邮件消息。
2. 将请求路由到 DNS 解析程序。解析程序负责根据请求向客户端返回相应的值，例如，运行 Web 服务器或电子邮件服务器的主机的 IP 地址。
3. 如果该 IP 地址已在 DNS 解析程序中缓存（因为其他人已提交过相同的 DNS 查询且解析程序已获得该值），解析程序会将该 IP 地址返回给提交请求的客户端。然后，客户端将使用该 IP 地址来访问主机。

   如果该 IP 地址未在 DNS 解析程序中进行缓存，解析程序将向您的域的父区域发送请求，在 TLD 注册机构该操作会返回两个值：

   - Delegation Signer (DS) 记录，这是与用于签署记录的私有密钥对应的公有密钥。
   - 域的授权名称服务器的 IP 地址。
4. DNS 解析程序将原始请求发送至另一个 DNS 解析程序。如果该解析程序没有此 IP 地址，它将重复该过程，直至解析程序将请求发送到位于您的 DNS 服务提供商的名称服务器。该名称服务器将返回两个值：
   - 域的记录，如 example.com。其中通常包含主机的 IP 地址。
   - 您在配置 DNSSEC 时创建的记录的签名。
5. DNS 解析程序将使用您向域注册商提供的公有密钥（注册商又将其转发给 TLD 注册机构）来执行以下两项操作：
   - 建立信任链。
   - 确认来自 DNS 服务提供商的签名响应合法，并且未被来自攻击者的错误响应替换。
6. 如果响应是真实的，解析程序会将该值返回给提交请求的客户端。

   如果无法对响应进行验证，解析程序将向用户返回错误。

如果域的 TLD 注册机构没有用于域的公有密钥，解析程序将使用它从 DNS 服务提供商处获得的响应来响应 DNS 查询。

为域配置 DNSSEC 的先决条件和最大数量

要为域配置 DNSSEC，您的域和 DNS 服务提供商必须满足以下先决条件：

- TLD 的注册机构必须支持 DNSSEC。要确定 TLD 注册机构是否支持 DNSSEC，请参阅可向 Amazon Route 53 注册的域。。
- 域的 DNS 服务提供商必须支持 DNSSEC。

> **Important**
>
> Route 53 支持将 DNSSEC 签名和 DNSSEC 用于域注册。要了解更多信息，请参阅在 Amazon Route 53 中配置 DNSSEC 签名。

- 您必须使用域的 DNS 服务提供商配置 DNSSEC，然后才能将域的公有密钥添加至 Route 53。
- 可以添加到域的公有密钥的数量取决于该域的 TLD：
  - .com 和 .net 域 — 最多 13 个密钥
  - 所有其它域 — 最多 4 个密钥

为域添加公有密钥

您在轮换密钥或为域启用 DNSSEC 时，请在用域的 DNS 服务提供商配置 DNSSEC 之后执行以下步骤。

为域添加公有密钥

1. 如果您尚未用 DNS 服务提供商配置 DNSSEC，请使用服务提供商提供的方法来配置 DNSSEC。
2. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Registered domains。
4. 选择要为其添加密钥的域的名称。
5. 在 DNSSEC 密钥选项卡中，选择添加密钥。
6. 指定以下值：

密钥类型

选择您要上传密钥签名密钥 (KSK) 还是区域签名密钥 (ZSK)。

算法

选择您用来为托管区域签署记录的算法。

公有密钥

指定您在使用 DNS 服务提供商配置 DNSSEC 时所使用的非对称密钥对中的公有密钥。

请注意以下几点：

- 指定公有密钥，而不是摘要。
- 您必须以 base64 格式指定密钥。

7. 选择添加。

> **Note**
>
> 一次只能添加一个公有密钥。如果您需要添加更多密钥，请等待，直至收到来自 Route 53 的确认电子邮件。

8. 当 Route 53 收到来自注册机构的响应时，我们会向域的注册联系人发送电子邮件。该电子邮件将确认已将公有密钥添加到注册结构的域或解释无法添加密钥的原因。

删除域的公有密钥

您在轮换密钥或为域禁用 DNSSEC 时，请使用以下步骤删除公有密钥，然后再用 DNS 服务提供商禁用 DNSSEC。请注意以下几点：

- 如果您要轮换公有密钥，我们建议您在添加新公有密钥之后最多等待 3 天，再删除旧私有密钥。
- 如果您要禁用 DNSSEC，请先删除域的公有密钥。我们建议您最多等待 3 天，再用域的 DNS 服务禁用 DNSSEC。

> **Important**
>
> 如果已为域启用 DNSSEC 并用 DNS 服务禁用 DNSSEC，则支持 DNSSEC 的 DNS 解析程序将向客户端返回 `SERVFAIL` 错误，客户端将无法访问与该域关联的端点。

删除域的公有密钥

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择要从中删除密钥的域的名称。
4. 在 DNSSEC 密钥选项卡中，选择您要删除的密钥旁边的单选按钮，然后选择删除密钥。
5. 在删除 DNSSEC 密钥对话框中，在文本框中输入 delete 以确认要删除密钥，然后选择删除。

> **Note**
>
> 一次只能删除一个公有密钥。如果您需要删除更多密钥，请等待，直至收到来自 Amazon Route 53 的确认电子邮件。

6. 当 Route 53 收到来自注册机构的响应时，我们会向域的注册联系人发送电子邮件。该电子邮件将确认已将公有密钥从注册结构的域中删除或解释无法删除密钥的原因。

查找注册商以及有关域的其他信息

要使用 GetDomainDetailAPI 查看域名信息，您可以使用任何 SDKs 或 Amazon CLI。有关更多信息，请参阅 get-domain-detail。

使用 **`get-domain-detail`** CLI 查看有关域的信息

- 使用以下 CLI：

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> 此命令仅在 us-east- Amazon Web Services 区域 1 中运行。

输出中将列出有关域的所有信息，包括注册商、注册日期、隐私设置等。

查看有关在 Route 53 注册的域的信息

> **Note**
>
> 自 2025 年 1 月 28 日起，某些域注册机构可能会从 WHOIS 过渡到用于域注册数据查询的注册数据访问协议（RDAP）。如果您通过 WHOIS 直接从注册机构访问域注册信息，则在相关注册机构停止支持 WHOIS 时，您可能需要更新应用程序以使用 RDAP 端点。
> Route 53 域的服务功能保持不变。本声明仅适用于在 Route 53 服务之外进行的直接注册机构 WHOIS 查询。

您可以查看使用 Route 53 注册的域的相关信息。此信息包括一些详细信息，例如域最初注册的时间以及域所有者以及技术人员、管理员和账单联系人的联系信息。

WHOIS

WHOIS 是一个可公开访问的免费名录，其中包含有关域注册商和注册管理机构赞助的域信息。它既作为在端口 43 上接受查询的服务，又作为网站提供，每个网站均可通过 IPv4和进行访问 IPv6。WHOIS 是一种分布式分层查询。有关更多信息，请参阅关于 WHOIS。

向层次结构的不同级别发出 WHOIS 请求可以提供不同的信息：

- 向根 WHOIS（whois.iana.org）发出的请求提供有关注册管理机构的信息。
- 向注册机构 WHOIS 发出的请求会提供有关注册商的信息以及有关该域的一些公开信息。
- 向注册商 WHOIS 发出的请求将提供有关该域的所有公开信息。

由于 WHOIS 有多个级别，包括由 TLD 注册管理机构和域注册商运营的 WHOIS 查询，因此在 Route 53 控制台上关闭隐私保护只能在注册商提供的 WHOIS 上将其关闭。无论您是否在 Route 53 中关闭了 WHOIS 查询服务，某些注册管理机构都会着意为其 WHOIS 查询服务维护隐私保护或编辑服务。要获取有关您的域的完整信息，我们建议您使用注册商提供的 WHOIS。

注意以下几点：

在启用隐私保护的情况下向域联系人发送电子邮件

如果为域启用了隐私保护，则注册人、技术和管理联系人的联系信息将替换为 Amazon Registrar 隐私服务的联系信息。例如，如果 example.com 域已在 Amazon Registrar 注册，并且启用了隐私保护，则对 WHOIS 查询的响应中的注册人电子邮件的值将类似于 owner1234@example.com.identity-protect.org。

要在启用隐私保护的情况下联系一个或多个域联系人，请向相应的电子邮件地址发送电子邮件。我们会自动将您的电子邮件转发给相应的联系人。

报告滥用行为

要举报任何非法活动或违反可接受使用政策的行为，包括不当内容、网络钓鱼、恶意软件或垃圾邮件，请发送电子邮件至 trustandsafety@support.aws.com。

查看有关在 Route 53 注册的域的信息

1. 在 Web 浏览器中，转到以下某个网站：
   - 亚马逊注册商 WHOIS: https://registrar.amazon.com /whoi s
   - 亚马逊注册商 RDAP: https://registrar.amazon.com /rdap
   - Gandi WHOIS：https://whois.gandi.net
2. 输入要查看其信息的域的名称，然后选择搜索。

Deleting a domain name registration（删除域名注册）

对于大多数顶级域名 (TLDs)，如果您不再需要注册，则可以将其删除。如果注册机构允许您删除注册，请执行本主题中的过程。

注意以下几点：

注册费用不可退款

如果在注册的计划到期时间之前删除域名注册， Amazon 将不退还注册费。

TLDs 允许您删除域名注册

要确定是否可以删除域注册，请参阅可向 Amazon Route 53 注册的域。。如果您的 TLD 的部分不包含“删除域注册”子部分，您可以删除该域。在删除域之前，请务必禁用域锁定。有关禁用域锁的更多信息，请参阅DisableDomainTransferLock。

如果您无法删除某个域注册该怎么办？

如果您的域的注册机构不允许您删除域名注册，您必须等待该域到期。要确保该域不被自动续订，请为该域禁用自动续订。当到期时间日期已过时，Route 53 将自动删除域的注册。有关如何更改自动续订设置的信息，请参阅启用或禁用域自动续订。

域被删除并再次可供注册之前的延迟

几乎所有注册机构都会阻止任何用户立即注册刚到期的域名。典型延迟是一至三个月，具体取决于 TLD。有关更多信息，请参阅可向 Amazon Route 53 注册的域。中有关您的 TLD 的“续订和恢复域名的截止日期”部分。

> **Important**
>
> 如果您只想在 Amazon 账户之间转移域名或将域名转移给其他注册商，请不要删除域名并期望重新注册该域名。请改为参阅合适的文档：
>
> - 将域转移到其它 Amazon 账户
> - 将域从 Amazon Route 53 转移到另一注册商

删除域名注册

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Registered domains。
3. 选择域的名称。

   如果要删除 .co.uk、.me.uk、.org.uk 或 .uk 域，请参阅 删除 .co.uk、.me.uk、.org.uk 和 .uk 域名注册。
4. 如果 TLD 的注册机构允许删除域名注册，请选择删除域。

   某些域可能要求我们向域注册者发送电子邮件，以确认该注册人是否想要删除域。如果您收到一封电子邮件，则将来自以下电子邮件地址之一：

   - noreply@registrar.amazon — 适用于由亚马逊 TLDs 注册商注册。
   - noreply@domainnameverification.net 或 noreply@emailverification.info — 由我们的 TLDs 注册商助理 Gandi 注册。

要确定您的 TLD 注册商是谁，请参阅可向 Amazon Route 53 注册的域。。

5. 如果您收到验证电子邮件，请选择电子邮件中的链接，并批准或拒绝删除域的请求。

> **Important**
>
> 注册联系人必须立即按照电子邮件中的说明操作，否则我们必须根据 ICANN 的要求，在一天后尽快取消删除请求。

当您的域被删除后，您将收到另一封电子邮件。要确定您的请求的最新状态，请参阅 Viewing the status of a domain registration（查看域注册的状态）。

6. 在托管区域中删除已删除域的记录，然后删除托管区域。在删除一个托管区域后，Route 53 会停止计算该托管区域的月费。有关更多信息，请参阅以下文档：

   - 删除记录
   - 删除公有托管区域
   - Route 53 定价

7. 如果您在删除域名注册时遇到问题，可以免费联系 Su Amazon pport。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

删除 .co.uk、.me.uk、.org.uk 和 .uk 域名注册

如果要删除 .co.uk、.me.uk、.org.uk 或 .uk 域，请在 .uk 域的注册机构 Nominet 上创建一个账户。有关更多信息，请参阅 Nominet 网站上的“Cancelling your domain name”(取消您的域名)，网址为 https://www.nominet.uk/domain-support/。

> **Important**
>
> 如果您删除（取消）.uk 域名，该域名将在几天内前删除，可供任何人注册。如果您只想转移域名，请不要删除它。

过程概览：

1. 在 Nominet 网站上，如果您是第一次登录，按照说明进行操作。请参阅https://secure.nominet.org.uk/auth/login.html。Nominet 会向您发送一封电子邮件，其中包含创建密码的说明。
2. 按照您从 Nominet 收到的电子邮件中的说明操作。
3. 登录 Nominet 网站，并按照说明取消（删除）域名。

就域名注册问题联系 Su Amazon pport

Amazon 为所有 Amazon 客户免费提供基本支持计划。该计划包含针对以下域注册相关问题的协助：

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

- 将域移入移出或 Amazon Route 53
- 在 Amazon 账户之间转移域名
- 提升对 Route 53 实体的配额，例如您可以注册的域的数量（请参阅 配额）。
- 更改域的所有者
- 更新域所有者的联系信息
- 重新发送确认和授权电子邮件
- 续订域
- 还原已到期的域
- 获取有关 Route 53 账单的信息
- 为 .uk 域提供身份证明
- 关闭 Amazon 账户后删除域名或禁用自动续费

要就这些问题以及与域名注册相关的其他问题与 Su Amazon pport 联系 Support，请执行适用的程序。

主题

在可以登录 Amazon 账户时联系 Amazon Support

要在能够登录 Amazon 账户后联系 Amazon Support，请执行以下步骤：

1. 使用域名当前注册的 Amazon 账户登录 Suppor Amazon t。

   > **Important**
   >
   > 必须使用域当前注册到的根账户登录。此项要求可防止未经授权的用户劫持您的账户。

2. 选择账户和账单
3. 指定以下值：

   关于

   接受 Account and Billing Support 的默认值。

   服务

   接受 Domains 的默认值。

   类别

   接受 Registration Issue 的默认值。

   严重性

   选择适用的严重性。

   主题

   输入问题的简短摘要。

   说明

   更详细地描述您遇到的问题，并附上任何相关文档或屏幕截图。

   联系方式

   选择联系方式 Web。我们将使用与您的 Amazon 账户关联的电子邮件地址与您联系。
4. 选择提交。

当你无法登录 Amazon 账户时联系 Amazon Support

要在无法登录 Amazon 账户时联系 Amazon Support，请执行以下步骤：

1. 前往 “我是 Amazon 客户，我正在寻找账单或账户支持” 页面。
2. 填写表单。
3. 选择提交。

下载域账单报告

如果您管理多个域并且要按域查看指定时间段内的费用，则可下载域账单报告。此报告包括适用于域注册的所有费用，如下所示：

- 注册域
- 续订域注册
- 将域转移到 Amazon Route 53
- 更改域名的所有者（对于某些人来说 TLDs，此操作是免费的）

有时，您的账单报告能够显示未来的账单周期。发生这种情况是因为域自动续订过程在域过期前一个月开始。因此，例如，在八月报告中，您可能会看到一个账单周期，从九月开始一直持续到次年九月。

在使用控制台运行报告时，您可以选择以下选项：

- 过去 12 个月：报告中包括从您运行报告之前的一年到当天的费用。例如，如果您在 6 月 3 日运行该报告，其中包括从上一年 6 月 3 日到当天的费用。
- 上一年的个别月份：报告中包括指定月份的费用。

如果您以编程方式运行报告，则可以获取从 2014 年 7 月 31 日开始的任何日期范围内的费用。这是 Route 53 开始支持域注册的日期。例如，请参阅 Amazon CLI 命令参考中的查看账单。

账单报告采用 CSV 格式，其内容由 ViewBillingAPI 描述。

下载域账单报告

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 在导航窗格中，选择 Registered Domains。
3. 选择 Domain billing report。
4. 选择报告的日期范围，然后选择 Download domain report。
5. 按照提示打开报告或保存报告。
6. 如果您在下载域名账单报告时遇到问题，可以免费联系 S Amazon upport。有关更多信息，请参阅就域名注册问题联系 Su Amazon pport。

可向 Amazon Route 53 注册的域。

> **Important**
>
> 以下顶级域限制仅适用于域注册。使用 Route 53 DNS 服务时，您可以使用所选的任何顶级域以及任何域注册商。此页面上的信息仅涉及您可以利用 Route 53 注册的域。有关将 Route 53 用作 DNS 服务的更多信息，请参阅 如何将 Internet 流量路由到您的网站或 Web 应用程序。

以下通用域名和地理顶级域名列表显示了可用于向 Amazon Route 53 注册域名的顶级域名 (TLDs)。

向 Route 53 注册域

TLD 注册表向一些域名分配了特殊或优惠的价格。您无法使用 Route 53 注册具有特殊或优惠价格的域。您可以 TLDs在 Route 53 上注册的包含在以下列表中。如果不包含 TLD，则无法向 Route 53 注册域。

将域转移到 Route 53

如果下表中包含 TLD，您可向 Route 53 转移域。如果不包含 TLD，则无法向 Route 53 转移域。

大多数情况下 TLDs，您需要从当前注册商那里获得授权码才能转移域名。要确定您是否需要授权代码，请参阅您的 TLD 的“转移所需的授权代码”部分。

域注册和转移的定价

有关注册域或将域转移到 Route 53 的费用，请参阅域注册的 Amazon Route 53 定价。

使用 Route 53 作为您的 DNS 服务

可将 Route 53 用作任何域的 DNS 服务，即便下表中不包含该域的 TLD 也不影响。有关将 Route 53 用作 DNS 服务的更多信息，请参阅 如何将 Internet 流量路由到您的网站或 Web 应用程序。有

关如何将用于您的域的 DNS 服务转移到 Route 53 的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

国际化域名

并非所有域名都 TLDs 支持国际化域名 (IDNs)，即包含 ASCII 字符 a-z、0-9 和-（连字符）以外的字符的域名。每个 TLD 的列表表明该顶级域名是否支持。 IDNs有关国际化域名的更多信息，请参阅 DNS 域名格式。

向注册地理域 TLDs

地理注册规则因国家 TLDs 而异。某些国家/地区不受限制，这意味着世界各地的任何人都可以注册，而其他国家/地区则有特定限制，如居住地。每个地理 TLD 的列示内容都指明了是否存在任何限制。

对支持的顶级域的索引

主题

- 通用顶级域
- 地理顶级域

通用顶级域

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B，

.band, .bargains, .beer,.bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .bot, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .christmas, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .free, .fun, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .hot, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .moi, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja, .now

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub. .pw（帕劳）

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, reviews。, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .spot, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team, .tech,.technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zone

地理顶级域

非洲

.ac（阿森松岛）, .co.za（南非）, .sh（圣赫勒拿岛）

美洲

.ai（安圭拉）, .ca（加拿大）, .cl（智利）, .co（哥伦比亚）, .com.ar（阿根廷）, .com.br（巴西）, .com.mx（墨西哥）, .mx（墨西哥）, .us（美国）, .vc（圣文森特和格林纳丁斯）, .vg（英属维尔京群岛）

亚洲/大洋洲

.au（澳大利亚）, .cc（科科斯（基林）群岛）, .co.nz（新西兰）, .com.au（澳大利亚）, .com.sg（新加坡共和国）, .fm（密克罗尼西亚联邦）, .in（印度）, .jp（日本）, .io（英属印度洋领地）, .net.au（澳大利亚）, .net.nz（新西兰）, .nz（新西兰）, .org.nz（新西兰）, .pw（帕劳）, .qa（卡塔尔）, .ru（俄罗斯联邦）, .sg（新加坡共和国）

欧洲

.be（比利时）, .berlin（德国的城市柏林）, .ch（瑞士）, .co.uk（英国）, .cz（捷克共和国）, .de（德国）, .es（西班牙）, .eu（欧盟）, .fi（芬兰）, .fr（法国）, .gg（格恩西）, .im（英国属地曼岛）, .it（意大利）, .me（黑山共和国）, .me.uk（英国）, .nl（荷兰）, .org.uk（英国）, .ruhr（鲁尔区，德国西部）, .se（瑞典）, .uk（英国）, .wien（奥地利的城市维也纳）

通用顶级域

通用顶级域名 (gTLDs) 是在全球范围内使用和识别的全球扩展名，例如.com、.net 和.org。通用顶级域还包括专业域，如 .bike、.condos 和 .marketing。

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B，

.band, .bargains, .beer, .bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .bot, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, .christmas, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .free, .fun, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .hot, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .moi, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja, .now

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, reviews。, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .spot, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team,.tech, .technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zone

.ac

请参阅.ac（阿森松岛）。

Return to index

.academy

供学校和大学等教育机构使用。此外，教育机构附属的招聘人员、顾问、广告商、学生、教师和管理人员也使用该域名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.accountants

供会计行业附属的企业、集团和个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.actor

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.adult

供仅托管成人内容的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.agency

供标识为代理机构的任何企业或集团使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天

- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.airforce

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.apartments

供房地产代理、房东和租户使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.associates

供名称中包含“associates”一词的企业和公司使用。还可供要指明其组织专业性质的任何集团或代理机构使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.auction

用于与拍卖相关的活动和基于拍卖的购买和销售。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、西班牙语和拉丁语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.audio

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .audio 域或将 .audio 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .audio 域。

供视听行业以及对广播、声音设备、音频制作和音频流感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .audio 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.band

用于共享有关乐队和乐队活动的信息。还供音乐人与他们的粉丝互动以及销售与乐队相关的商品。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、西班牙语和拉丁语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bargains

用于提供有关销售和促销的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天

- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.beer

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bet

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bid

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bike

供为自行车爱好者提供服务的企业或集团使用，如自行车店、摩托车专卖店和修理店。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bingo

供在线游戏网站使用或用于共享有关 bingo 游戏的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天

- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bio

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.biz

用于商业用途。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持简体中文、繁体中文、丹麦语、芬兰语、德语、匈牙利语、日语、韩语、拉脱维亚语、立陶宛语、挪威语、波兰语、葡萄牙语、西班牙语和瑞典语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.black

供那些喜欢黑色或要将黑色与其企业或品牌关联的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.blue

供那些喜欢蓝色或要将蓝色与其企业或品牌关联的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.bot

用于聊天机器人和 AI 相关的产品和服务。此域名扩展有助于传达人工智能中自动化系统、对话界面和新兴技术的本质。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.boutique

用于提供有关精品店和小型专卖店的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.builders

供附属于建筑行业的公司和个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.business

供任何类型的企业使用。可用于替代 .biz 扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.buzz

用于提供有关最新新闻和事件的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cab

供附属于出租车行业的公司和个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cafe

供咖啡企业以及对咖啡文化感兴趣的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.camera

供摄影爱好者和任何希望分享照片的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.camp

供公园和娱乐部门、夏令营、作家工作室、健身训练营和露营爱好者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.capital

用作常规类别，用于描述任何类型的资本，如金融资本或城市资本。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cards

供专门制作卡片 (如电子贺卡、印制贺卡、名片和扑克牌) 的企业使用。还适用于那些想要讨论卡片游戏的规则和策略的玩家。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.care

供护理领域的企业或代理机构使用。此外，还适用于慈善组织。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.careers

用于提供有关求职招聘的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cash

供从事资金相关活动的任何组织、集团或个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.casino

供赌博行业或想分享赌博和赌场游戏信息的玩家使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.catering

供餐饮企业或想分享食品相关活动信息的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cc

请参阅.cc（科科斯（基林）群岛）。

Return to index

.center

从研究组织到社区中心均将其用作通用扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ceo

用于获取有关 CEOs 及其等值的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持德语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.chat

供任何类型的在线聊天网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cheap

供推广和销售低价产品的电子商务网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.christmas

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 43 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 86 天之间
- 从注册表中删除域：到期后 86 天

.church

供任意规模和教派的教堂与其会众联系及发布教堂相关事件和活动的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.city

用于提供有关特定城市的信息，如兴趣点、当地热门观光景点或社区活动。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.claims

供负责处理保险索赔或提供法律服务的公司使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cleaning

供提供清洁服务的企业或个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.click

供要将单击操作与其网站关联 (例如，在网站上单击产品即可购买) 的企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.clinic

供医疗保健行业和医疗专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.clothing

供时装行业的企业或人员使用，包括零售商、百货商店、设计师、裁缝和折扣店。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.cloud

用作通用扩展名，是提供云计算技术和服务的公司的理想选择。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.club

供任何类型的俱乐部或组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西班牙语和日语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.coach

供对培训感兴趣的任何人使用，如体育专业人士、生活方式教练或企业培训师。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.codes

用作各种代码的通用扩展名，如执行代码、生成代码或编程代码。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.coffee

供咖啡行业从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.college

供学校和大学等教育机构使用。此外，教育机构附属的招聘人员、顾问、广告商、学生、教师和管理人员也使用该域名。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、简体和繁体中文、西里尔语、希腊语、希伯来语、日语和泰国语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.com

用于商业网站。这是 Internet 上最受欢迎的扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.community

供任何类型的社区、俱乐部、组织或专门兴趣小组使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.company

用作各种企业的通用扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.computer

用作通用扩展名，可提供有关计算机的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.condos

供与公寓关联的个人和企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.construction

供建筑行业从业者使用，如建设者和承包商。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.consulting

供顾问和其他附属于咨询行业的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、中文、法语、西里尔语、梵文、德语、希腊语、希伯来语、日语、韩语、拉丁语、西班牙语、泰米尔语和泰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.contact

供任意规模和教派的教堂与其会众联系及发布教堂相关事件和活动的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.contractors

供承包商使用，如建筑行业的承包商。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cool

供希望将其品牌与最新趋势关联的组织和集团使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.coupons

供提供在线优惠券和优惠码的零售商和制造商使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.credit

供信贷行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.creditcard

供发放信用卡的公司或银行使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.cruises

供航海业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.dance

供舞蹈家、舞蹈老师和舞蹈学校使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.dating

供交友网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.deal

用于提供优惠、折扣和特别优惠的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.deals

用于提供有关在线交易和销售的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.degree

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.delivery

供提供各种商品或服务的公司使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.democrat

用于提供有关民主党的信息。还可供掌管选举办公室的官员、选举出来的官员、热衷于政治的人士和顾问使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.dental

供牙科专业人员和牙科供应商使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.design

供任意规模和教派的教堂与其会众联系及发布教堂相关事件和活动的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.diamonds

供钻石爱好者以及从事钻石行业的人 (包括销售商、经销商和商家) 使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.diet

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .diet 域或将 .diet 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .diet 域。

供保健和健身专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .diet 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.digital

可用于一切与数字相关的对象，但最适合技术企业。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.direct

用作通用扩展名，但最适合直接通过电子商务网站向客户销售产品的人员。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.directory

供媒体部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.discount

用于大幅度降价的折扣网站和企业。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.dog

供爱犬人士以及提供犬只服务和产品的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.domains

用于提供有关域名的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.education

用于提供有关教育的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.email

用于提供有关促销电子邮件的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.energy

用作通用扩展名，但更适用于能源或节能领域的企业或个人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.engineering

供工程公司和专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.enterprises

用于提供有关企业和业务的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.equipment

用于提供有关设备、设备零售商或制造商以及租赁店的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.estate

用于提供有关房地产和房地产领域的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.events

用于提供有关各种事件的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.exchange

用于任何类型的交换：股票交易、商品交换甚至简单的信息交换。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.expert

供在各个领域具有专业知识的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.exposed

用作各种主题的通用扩展名，包括摄影、小报和调查报导。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.express

用作通用扩展名，但更适合注重迅速交付商品或服务的企业或个人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.fail

供任何犯了错误的人使用，但更适用于发布幽默的、“失败的”错误和挫折。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.fan

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.farm

供农业生产从业者使用，如农场主和农业工程师。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.finance

供财务部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.financial

供财务部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.fish

用作通用扩展名，但更适用于与鱼类和渔业相关的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.fitness

用于宣传健身和健身服务。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.flights

供旅行社代理、航空公司及附属于旅游行业的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.florist

供花商使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.flowers

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .flowers 域或将 .flowers 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .flowers 域。

用于提供与花卉有关的任何内容，如在线花卉销售或提供有关花卉种植与栽培的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .flowers 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.fm

请参阅.fm（密克罗尼西亚联邦）。

Return to index

.football

供足球运动涉及的相关从业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.forsale

用于销售商品和服务。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.foundation

供非营利性组织、慈善机构和其他类型的基金会使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.free

用于提供免费产品、服务或内容的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.fun

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.fund

用作与基金相关的任何内容的通用扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.furniture

供家具制造商、销售商以及附属于家具行业的所有从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.futbol

用于提供有关足球的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.fyi

用作通用扩展名，但更适用于共享各种信息。“FYI”是“for your information”(供参考) 的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gallery

供美术馆所有者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.games

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gift

供出售礼品或提供礼品相关服务的企业或组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gifts

供出售礼品或提供礼品相关服务的企业或组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gives

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.glass

供玻璃行业从业者使用，如玻璃切割工人或窗户安装工人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.global

供具有国际市场或愿景的企业或集团使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、白俄罗斯语、波斯尼亚语、保加利亚语、中文 (简体)、中文 (繁体)、丹麦语、德语、印地语、匈牙利语、冰岛语、韩语、拉脱维亚语、立陶宛语、马其顿语、黑山语、波兰语、俄罗斯语、塞尔维亚语、西班牙语、瑞典语和乌克兰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.gmbh

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gold

用作通用扩展名，但更适用于购买或出售黄金或黄金相关产品的公司。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.golf

供高尔夫游戏专用网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.graphics

供图形行业从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.gratis

供提供免费产品 (如促销品、下载或优惠券) 的网站使用。“Gratis”是一个西班牙语单词，表示“免费”。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.green

供专门讨论节能、生态学、环境和绿色生活方式的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.gripe

用于共享投诉和批评。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.group

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.guide

用作通用扩展名，但更适用于关注旅游目的地、服务和产品的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.guitars

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .guitars 域或将 .guitars 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .guitars 域。

供吉他爱好者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .guitars 域转移到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.guru

供希望分享各种主题知识的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.haus

供房地产和建筑行业使用。“Haus”是一个德语单词，表示“房屋”。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.healthcare

供医疗保健部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.help

用作通用扩展名，但更适用于提供在线帮助和信息的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.hiv

供专门抗击 HIV 的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.hockey

供曲棍球游戏专用网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.holdings

供金融顾问、股票经纪人和从事投资的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.holiday

供旅游行业从业人员以及从事聚会策划和特殊场合策划的个人及企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.host

供提供 Web 托管平台和服务的公司使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、简体中文、繁体中文、希腊语、希伯来语、韩语和泰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.hosting

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .hosting 域或将 .hosting 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .hosting 域。

用于托管网站或供托管行业从业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .hosting 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.hot

用于以热门话题、热门内容或时间敏感型优惠为特色的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.house

供房地产代理以及房屋的买家和卖家使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.im

请参阅.im（英国属地曼岛）。

Return to index

.immo

供房地产部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.immobilien

用于提供有关房地产的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.industries

供希望标识为工业的任何公司或商业企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.info

用于传播信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ink

供纹身爱好者或与墨水相关的任何行业 (如出版和印刷行业) 使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语和拉丁语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.institute

供任何组织或集团使用，尤其是研究和教育组织。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.insure

供保险公司和保险经纪人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.international

供具有国际连锁的企业、进行国际旅游的个人或具有国际影响的慈善组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.investments

用作通用扩展名，但更适用于宣传投资机会。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.io

请参阅.io（英属印度洋领地）。

Return to index

.irish

用于宣传爱尔兰文化和组织。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、简体中文、繁体中文、法语、德语、希腊语、希伯来语、日语、韩语、西班牙语、泰米尔语和泰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.jewelry

供珠宝卖家和买家使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.juegos

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .juegos 域或将 .juegos 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .juegos 域。

供各种游戏网站使用。“Juegos”是一个西班牙语单词，表示“游戏”。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .juegos 域转移到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.kaufen

用于提供有关电子商务的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.kim

供名字或姓氏为 Kim 的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.kitchen

供厨房零售商、厨师、美食博主和食品行业的任何从业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.kiwi

供希望支持新西兰猕猴桃文化的公司和个人使用。它还可用作提供慈善救助的平台，以帮助重建在 2010 年和 2011 年地震中损坏的基督城。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持毛利语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.land

供农民、房地产代理、商业地产开发商和对地产感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.law

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.lease

供房地产经纪人、房东和租户使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.legal

供法律专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.lgbt

供女同性恋、男同性恋、双性恋和变性人群体使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.life

用作通用扩展名，适合多种企业、集团和个人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.lighting

供摄影师、设计师、架构师、工程师和其他对照明感兴趣的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.limited

用作通用扩展名，适合多种企业、集团和个人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.limo

供司机、豪华轿车公司和汽车租赁机构使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.link

提供有关创建在线快捷链接的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

UniRegistry 是 .LINK 域的注册机构。根据 UniRegistry 政策，注册机构级别 WHOIS 显示为“REDACTED FOR PRIVACY”。关闭我们的隐私保护功能只会影响显示在注册商级别 Amazon Registrar WHOIS 上的信息。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.live

用作通用扩展名，适合多种企业、集团和个人。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.llc

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.loan

供贷方、借方和贷款专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持丹麦语、德语、挪威语和瑞典语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.loans

供贷方、借方和贷款专业人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.lol

用于幽默和喜剧网站。“LOL”是“laugh out loud”(大笑) 的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.ltd

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.maison

供房地产部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.management

用于提供有关商界和公司管理的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.marketing

供营销部门用于各种用途。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.mba

供提供工商管理硕士 (MBA) 信息的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.media

供媒体和娱乐部门使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.memorial

供专门承办活动的纪念组织和人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.mobi

供希望其网站可通过手机访问的公司和个人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.moda

用于提供有关时尚的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.moi

法语意为 “我”。用于向讲法语的最终用户发送法语内容的信号。适用于法语版的个人博客 CVs、作品集、爱好或兴趣网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.money

供专注于资金和资金相关活动的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.mortgage

供抵押贷款行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.movie

供提供有关影片和影片制作信息的网站使用。适合专业人员和粉丝。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.name

供希望创建个性化 Web 展示的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

威瑞信是.name 的注册机构 TLDs，允许您注册二级域名（名称.n ame）和三级域名（名字）。 姓氏.nam e)。Route 53 仅支持二级域，既可用于注册域，又可用于向 Route 53 转移现有域。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.net

用于所有类型的网站。.net 扩展名是网络的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.network

供从事网络行业或要通过联网建立连接的从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.news

用于分发任何有报道价值的信息，例如，与新闻传播有关的最新事件或信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ninja

供希望自己与忍者能力关联的个人和企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天

- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.now

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.onl

.onl 扩展名是“online (在线)”的缩写，在西班牙语中是非盈利性组织的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.online

.onl 扩展名是“online (在线)”的缩写，在西班牙语中是非盈利性组织的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.org

供各类组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.partners

供律师事务所、投资方和各种公司使用。还可供旨在建立关系的社交网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.parts

用作通用扩展名，但更适用于零件制造商、销售商和买家。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.photo

供摄影师和对照片感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.photography

供摄影师和对照片感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.photos

供摄影师和对照片感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.pics

供摄影师和对照片感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.pictures

供对摄影、艺术和媒体感兴趣的任何人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.pink

供那些喜欢粉色或要将粉色与其企业或品牌关联的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.pizza

供披萨餐馆和披萨爱好者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.place

用作通用扩展名，但更适用于家庭和旅游部门。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.plumbing

供水暖行业的从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.plus

用作通用扩展名，但更适合大号服装、附加软件或可提供“额外”功能或尺寸的任何产品。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.poker

供扑克玩家和游戏网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.porn

仅供成人网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.press

仅供成人网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.pro

供获得许可并具有资质的专业人员和专业组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.productions

供制作广告、广播广告和音乐视频的工作室和制作公司使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.properties

用于提供有关任何类型资产 (包括房地产或知识产权) 的信息。还可供有房屋、建筑或土地要出售、租赁或出租的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.property

用于提供有关任何类型资产 (包括房地产或知识产权) 的信息。还可供有房屋、建筑或土地要出售、租赁或出租的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .property 域转移到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.pub

供出版、广告或酿造行业的从业者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.qpon

用于优惠券和促销代码。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.recipes

供有菜谱要分享的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.red

供那些喜欢红色或要将红色与其企业或品牌关联的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.reise

供与旅游或旅行相关的网站使用。“Reise”是一个德语单词，表示“上升”、“升起”或“踏上旅程。”

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.reisen

供与旅游或旅行相关的网站使用。“Reisen”是德语单词，表示“旅行”。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.rentals

用于所有类型的出租业务。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.repair

供维修服务或想教其他人如何维修各种物品的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.report

用作通用扩展名，但更适用于提供有关业务报告、社区出版物、书籍报告或新闻报告的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.republican

用于提供有关共和党的信息。还可供掌管选举办公室的官员、选举出来的官员、热衷于政治的人士和顾问使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.restaurant

供餐饮行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

reviews。

供那些希望发表观点并阅读他人评论的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.rip

供专门介绍死亡和纪念的网站使用。“RIP”是“rest in peace”(安息) 的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.rocks

用作通用扩展名，但更适用于“硬石、摇滚”人士：音乐家、地质学家、珠宝师、登山者等。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.run

用作通用扩展名，但更适用于健身和运动行业。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.sale

供电子商务网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.sarl

供通常位于法国的有限责任公司使用。“SARL”是“Société à Responsabilité Limité”的缩写。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.school

用于提供有关教育、教育机构和学校相关活动的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.schule

用于提供有关基于德语的教育、教育机构和学校相关活动的信息。“Schule”是一个德语单词，表示“学校”。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天

- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.services

供专注于多种服务的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.sex

仅用于提供成人内容。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.sexy

用于色情内容。还用于描述最受欢迎和令人兴奋的品牌、产品、信息和网站。

Return to index

Important

您不能再使用 Route 53 注册新的 .sexy 域或将 .sexy 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .sexy 域。

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

不支持。不再支持将 .sexy 域转移到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.shiksha

供教育机构使用。“Shiksha”是印度语中的学校。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.shoes

供鞋零售商、设计师、制造商或时尚博主使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.shop

用于在线和 brick-and-mortar零售企业以及服务提供商。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.shopping

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.show

用作通用扩展名，但更适用于娱乐行业。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.singles

供交友服务、度假村及为希望建立联系的人员提供服务的其他企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.site

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ski

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.soccer

供足球游戏专用网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.social

用于提供有关社交媒体、论坛和在线对话的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.solar

用于提供有关太阳系或太阳能的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.solutions

供各种顾问、 do-it-yourself服务和顾问使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.software

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.space

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.spot

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.store

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.stream

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.studio

用作通用扩展名，但更适用于房地产、艺术或娱乐行业的从业者。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.style

用作通用扩展名，但更适用于专注于最新趋势 (如时尚、设计、建筑和艺术) 的网站。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.sucks

用作通用扩展名，但更适合那些想要分享负面体验或向其他人提醒诈骗、欺诈行为或问题产品的人。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.supplies

供在线销售商品的企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.supply

供在线销售商品的企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.support

供可提供各种支持 (包括客户、产品或系统支持或情感、财务或精神支持) 的企业、集团或慈善机构使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.surgery

用于提供有关手术、药品和医疗保健的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.systems

主要供技术行业和提供技术服务的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.tattoo

供纹身爱好者和纹身行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西里尔语 (主要是俄语)、法语、德语、意大利语、葡萄牙语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tax

用于提供有关税务、税务申报和税法的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.taxi

供出租车、司机和班车公司使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.team

供希望标识为团队的任何企业或组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tech

供技术爱好者和专注于公司、服务和制造商中的技术的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.technology

供技术爱好者和专注于公司、服务和制造商中的技术的人员使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.tennis

用于提供与网球游戏有关的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.theater

供专门关注剧院、戏剧集和音乐剧的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tienda

供要与讲西班牙语的消费者联系的零售企业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tips

供那些想要分享有关几乎任何主题的知识和建议的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tires

供轮胎的制造商、分销商或买家使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.today

用于提供有关当前活动、新闻、天气、娱乐等的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.tools

用于提供有关任何类型工具的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tours

用作通用扩展名，但更适用于旅游公司。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.town

用于宣传城市的场所、文化和社区。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.toys

供玩具行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.trade

用作通用扩展名，但更适用于商务网站或贸易服务。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持丹麦语、德语、挪威语和瑞典语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.training

供培训师、教练和教育工作者使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天

- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.tv

用于提供有关电视和媒体的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

无。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.university

供大学和其他教育组织使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.uno

用于提供有关西班牙、葡萄牙和意大利社区或社团的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.vacations

供旅行和旅游行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.vegas

用于宣传拉斯维加斯市和拉斯维加斯生活方式。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ventures

供企业家、初创公司、风险投资家、投资银行和金融家使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.vg

请参阅.vg（英属维尔京群岛）。

Return to index

.viajes

供旅游机构、旅行社、旅行博客、旅游公司、租赁服务、旅游博主和旅游零售商使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.video

供媒体和视频行业使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语、拉丁语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间

- 从注册表中删除域名：到期后 75 天

.villas

供要出售、出租或租赁别墅的房地产代理和业主使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.vision

用作通用扩展名，但更适合验光师和眼科医生等眼科专家。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.vote

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.voyage

供旅游机构、旅行社、旅行博客、旅游公司、租赁服务、旅游博主和旅游零售商使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.watch

用于获取有关流媒体网站、网页 TVs、视频或手表的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.website

用于提供有关网站开发、促销、改进和体验的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、简体中文、繁体中文、希腊语、希伯来语、日语、韩语和泰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.wedding

Return to index

注册和续订的租赁期

1 到 10 年。

限制

无。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持中文、法语、德语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.wiki

有关提供有关在线文档的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语和拉丁语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.wine

Return to index

注册和续订的租赁期

1 到 10 年。

Privacy protection（隐私保护）

支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.work

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.works

供企业、组织和个人来交流有关工作、职业和雇佣服务的信息。此扩展名可用来替代 .com、.net 或 .org 扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天

- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.world

供要提供有关全球主题信息的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.wtf

供任何要用常见 (但粗俗) 缩略语“WTF”标识的人使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.XXX

供仅托管成人内容的网站使用。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.xyz

用作任何用途的通用扩展名。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

.xyz 域的注册机构 Generation XYZ 将一些域名视为高级域名。您不能向 Route 53 注册高级 .xyz 域或向其转移此类域。有关更多信息，请参阅 Generation XYZ 网站。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.zone

用于提供有关任何区域类型 (包括时区、气候区域和运动区域) 的信息。

Return to index

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持法语和西班牙语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

地理顶级域

以下域名后缀按地理位置分组，包括特定国家/地区的官方域名，即国家/地区代码顶级域名 (ccTLDs)。示例包括 .be (比利时)、.in (印度) 和 .mx (墨西哥)。cc 的注册规则因国家/地区TLDs 而异。某些国家/地区不受限制，这意味着世界各地的任何人都可以注册，而其他国家/地区则有特定限制，如居住地。每个 ccTLD 的列示内容都指明了是否存在任何限制。

> **Important**
>
> 在将任何 cc 转移TLDs 到 Route 53 的过程中，除了.cc 和.tv 之外，所有者联系人的更新都将被忽略，并使用注册表中的所有者联系人数据。转移完成后，您可以更新所有者联系信息。有关更多信息，请参阅 更新域的联系信息和所有权。

Return to index

非洲

.ac（阿森松岛）, .co.za（南非）, .sh（圣赫勒拿岛）

美洲

.ai（安圭拉）, .ca（加拿大）, .cl（智利）, .co（哥伦比亚）, .com.ar（阿根廷）, .com.br（巴西）, .com.mx（墨西哥）, .mx（墨西哥）, .us（美国）, .vc（圣文森特和格林纳丁斯）, .vg（英属维尔京群岛）

亚洲/大洋洲

.au（澳大利亚）, .cc（科科斯（基林）群岛）, .co.nz（新西兰）, .com.au（澳大利亚）, .com.sg（新加坡共和国）, .fm（密克罗尼西亚联邦）, .in（印度）, .jp（日本）, .io（英属印度洋领地）, .net.au（澳大利亚）, .net.nz（新西兰）, .nz（新西兰）, .org.nz（新西兰）, .pw（帕劳）, .qa（卡塔尔）, .ru（俄罗斯联邦）, .sg（新加坡共和国）

欧洲

.be（比利时）, .berlin（德国的城市柏林）, .ch（瑞士）, .co.uk（英国）, .cz（捷克共和国）, .de（德国）, .es（西班牙）, .eu（欧盟）, .fi（芬兰）, .fr（法国）, .gg（格恩西）, .im（英国属地曼岛）, .it（意大利）, .me（黑山共和国）, .me.uk（英国）, .nl（荷兰）, .org.uk（英国）, .ruhr（鲁尔区，德国西部）, .se（瑞典）, .uk（英国）, .wien（奥地利的城市维也纳）

非洲

您可以使用以下非洲顶级域名 (TLDs) 在 Amazon Route 53 上注册域名。

, ,

Return to index

.ac（阿森松岛）

Return to index

也用作在学术界广受欢迎的通用 TLD。

注册和续订的租赁期

一年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 80 天

.co.za（南非）

Return to index

注册和续订的租赁期

一年。

限制

只有二级域可用于 .za 扩展名。Route 53 支持二级域 .co.za。

对公众开放，但有一些限制：

- 注册对可确定身份的法律实体 (个人和法人) 开放。
- 域名必须在注册过程中通过区域检查。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

否

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日前一天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前一天
- 可以使用注册表进行恢复：到期后 1 天到 9 天之间
- 从注册表中删除域名：到期后 9 天

.sh（圣赫勒拿岛）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 80 天

美洲

您可以使用以下美洲顶级域名 (TLDs) 在 Amazon Route 53 上注册域名。

, , , , , , , , , , ,

Return to index

.ai（安圭拉）

Return to index

注册和续订的租赁期

注册：两到十年。续约：两到九年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 53 号公路可以延迟续约：到期后 45 天内
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.ca（加拿大）

Return to index

带有 (à) 或不带 (a) 重音符的域名变体会自动保留给注册人，并成为管理捆绑包的一部分。要激活捆绑包中的域，注册人必须为该域提出注册申请。捆绑包中的所有域都必须由同一个注册人在同一个注册商处注册。注册人还需要为捆绑包中的所有域提交转移申请才能完成转移。

来自 TLD 注册机构的确认电子邮件

当您注册 .ca 域时，您将收到一封包含链接的电子邮件，该链接指向注册协议的接受步骤。您必须在七天内完成该过程，否则您的域将无法注册。

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 注册对加拿大相关个人或组织开放，如“加拿大注册人要求”中所述。
- 注册联系人：您必须提供域所有者的完整、准确的法律名称。
- 管理和技术联系人：您必须指定 Person 作为联系人类型，并提供居住在加拿大的个人的联系信息。
- 在注册过程中，必须从下面的法律类型中选择一种：
  - ABO：加拿大原住民（个人或团体）

- ASS：加拿大非法人协会
- CCO：加拿大公司或加拿大省或地区
- CCT：加拿大公民
- EDU：加拿大教育机构
- GOV：加拿大政府或政府实体
- HOP：加拿大医院
- INB：加拿大《印第安人法案》认可的印第安乐队
- LAM：加拿大图书馆、档案馆或博物馆
- LGR：加拿大公民或永久居民的法定代表
- MAJ： Her/His 女王陛下/国王
- OMK：在加拿大注册的官方商标
- PLT：加拿大政党
- PRT：在加拿大注册的合伙企业
- RES：加拿大永久居民
- TDM：在加拿大注册的商标（非加拿大所有者类型）
- TRD：加拿大工会
- TRS：在加拿大成立的信托基金

Privacy protection（隐私保护）

- 人员 - 对于所有联系人，联系人姓名、地址、电话号码、传真号码和电子邮件地址均将隐藏，因为 CIRA 会自动将其隐私保护应用于个人。该隐私保护选项仅适用于注册商 Whois。
- 公司、协会或公共机构 — 注册表级不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：情况不尽相同。请联系 Amazon Support。

删除域注册

.ca 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.cl（智利）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .cl 域或将 .cl 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .cl 域。

Return to index

续订期限

两年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

转移所需的授权代码

不支持。不再支持将 .cl 域转移到 Route 53。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：请联系 Amazon Support。
- 可以对 Route 53 进行延期续订：请联系 Amazon Support。
- 从 Route 53 中删除域名：请联系 Amazon Support。
- 可以使用注册表进行恢复：请联系 Amazon Support。
- 从注册表中删除域名：联请系 Amazon Support。

.co（哥伦比亚）

Return to index

注册和续订的租赁期

1 到 5 年。

限制

对公众开放，没有任何限制。

隐私保护（适用于：个人）

所有信息均会隐藏。

如果联系人类型不是个人，则由 WHOIS 显示公司名称和国家或地区。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 45 天之间
- 从注册表中删除域名：到期后 50 天

.com.ar（阿根廷）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .com.ar 域或将 .com.ar 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .com.ar 域。

Return to index

续订期限

一年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。为防止未经授权的转移，请限制对注册人电子邮件地址和可能允许所有权变更 APIs 的 Route 53 的访问权限。UpdateDomainContact有关更多信息，请参阅服务授权参考和 域记录所有者的权限示例 中的 Route 53 域的操作、资源和条件键。

转移所需的授权代码

不支持。不再支持将 .com.ar 域传输到 Route 53。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：请联系 Amazon Support。

- 可以对 Route 53 进行延期续订：请联系 Amazon Support。
- 从 Route 53 中删除域名：请联系 Amazon Support。
- 可以使用注册表进行恢复：请联系 Amazon Support。
- 从注册表中删除域名：联请系 Amazon Support。

.com.br（巴西）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .br 域或将 .br 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .br 域。

Return to index

续订期限

一年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

转移所需的授权代码

不支持。不再支持将 .com.br 域转移到 Route 53。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：到期前 30 天直至到期日
- 可以对 Route 53 进行延期续订：直到过期后 119 天
- 从 Route 53 中删除域名：过期后 119 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 119 天

.com.mx（墨西哥）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.mx（墨西哥）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.us（美国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

.us 域的注册机构不允许域名中包含 Federal Communications Commission v. Pacifica Foundation No. 77-528。

对公众开放，但有一项限制：

- .us 扩展名用于位于美国的网站或活动。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 65 天

.vc（圣文森特和格林纳丁斯）

风险资本融资、大专院校等还通常将其用作通用 TLD。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 80 天

.vg（英属维尔京群岛）

视频游戏所涉及的组织也通常将其用作通用 TLD。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直至到期日后 44 天
- 可以对 Route 53 进行延期续订：是
- 从 Route 53 中删除域名：过期后 45 天
- 从注册表中删除域名：到期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 74 天之间
- 域再次公开可用：到期后 80 天

亚洲/大洋洲

您可以使用以下亚洲和大洋洲顶级域名 (TLDs) 在 Amazon Route 53 上注册域名。

, , , , , , , , , , , , , , ,

Return to index

.au（澳大利亚）

Return to index

来自 TLD 注册机构的确认电子邮件

我们的注册商助理 Gandi 通过以下方式转售.au 域名。DomainDirectors当您将域名转移到 Route 53 时，DomainDirectors 会向该域的注册人联系人发送一封电子邮件以验证联系人信息或授权转移请求。

注册和续订的租赁期

1 到 5 年。

限制

对公众开放，但有一些限制：

- .au 域向以下对象开放：在澳大利亚注册的法人、贸易、合作关系或专营商；经许可能在澳大利亚进行贸易的外国公司；以及澳大利亚注册商标的所有者或申请人。个人无法注册 .au 域名。注册人联系人必须是公司。
- 在注册过程中，您必须指明以下内容：
  - 您的注册类型：ABN (澳大利亚企业号码)、ACN (澳洲公司注册号) 或 TM (商标，如果域名与商标对应)。
  - 您的 ID 号，可以是澳大利亚企业号码（ABN）、澳大利亚公司注册号（ACN）或 TM（商标）。
  - 您的注册商名称，即注册域的法人实体的名称。此值必须与提供的 ABN（澳大利亚企业号码）、ACN（澳洲公司注册号）或 TM（商标）上的名称完全匹配。
  - 您的资格类型，即注册域名的法人实体的类型。
  - 允许您注册此域名的原因（策略原因）：
    - 域名与注册商的公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写相匹配。（策略原因 1）
    - 域名符合分配规则，但不是注册商公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写。（策略原因 2）。要查看 .au 的分配规则，请参阅 .au 注册表中的附表 A。
- 不正确或不匹配的联系信息（包括姓名、ABN 或商标 (TM) 号）将导致注册、交易和续订失败。可能需要变更所有权才能更正现有域的信息。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

不支持。

转移所需的授权代码

可以。除了 Route 53 控制台之外，您还可以从 .au 注册表中获取转移代码。

DNSSEC

支持域注册。设置密钥时，您必须选择 DNS 安全算法 2 (DH)。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期前 60 天直至到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 29 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 30 天

删除域注册

.au 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

变更所有权

使用 Route 53 控制台更改拥有者。请参阅Updating contact information for a domain（更新域的联系信息）。然后完成以下过程以完成所有权变更：

1. 新老注册者都必须点击他们在 transfers@1api.net 的电子邮件中收到的链接到他们列出的电子邮件地址。您必须在 14 天内完成此过程，否则必须重新开始。

2. 确认回复后，将在短时间内处理注册表中的拥有者变更，而无需进一步确认。

.cc（科科斯（基林）群岛）

Return to index

此外，名称中带有“cc”的组织 (如咨询公司、云计算公司或自行车俱乐部) 还通常将其用作通用 TLD。该扩展名是“.com”的一个常用替代名称。

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

- 隐藏 — 地址、电话号码、传真号码和电子邮件地址
- 不隐藏 — 联系人姓名和组织名称

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 65 天

.co.nz（新西兰）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 个人需年满 18 岁。
- 组织必须已注册。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 134 天之间
- 从注册表中删除域：到期后 134 天

.com.au（澳大利亚）

Return to index

来自 TLD 注册机构的确认电子邮件

我们的注册商助理 Gandi 通过以下方式转售.com.au域名。DomainDirectors当您将域名转移到 Route 53 时，DomainDirectors 会向该域的注册人联系人发送一封电子邮件以验证联系人信息或授权转移请求。

注册和续订的租赁期

1 到 5 年。

限制

对公众开放，但有一些限制：

- .com.au 和 .net.au 域向以下对象开放：在澳大利亚注册的合作关系或专营商；经许可能在澳大利亚进行交易的外国公司；以及澳大利亚注册商标的所有者或申请人。个人无法注册 .com.au/.net.au 域名。注册人联系人必须是公司。
- 您的域名必须与名称 (已向澳大利亚相关机构注册) 或商标 (商标的缩写或缩略词) 相同。
- 域名应指明您的活动。例如，它应指明您销售的产品或提供的服务。
- 在注册过程中，您必须提供以下信息：
  - 您的注册类型：ABN (澳大利亚企业号码)、ACN (澳洲公司注册号) 或 TM (商标，如果域名与商标对应)。
  - 您的 ID 号，可以是澳大利亚企业号码 (ABN)、澳大利亚公司注册号 (ACN) 或商标 (TM)（如果域名与商标对应）。
  - 您的注册商名称，即注册该域的法人实体的名称。此值必须所提供的名称完全匹配。
  - 您的资格类型，即注册此域名的法人实体的类型。
  - 允许您注册此域名的原因（策略原因）：
    - 域名与注册商的公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写相匹配。（策略原因 1）
    - 域名符合分配规则，但不是注册商公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写。（策略原因 2）。要查看 .com.au 的分配规则，请参阅 .com.au 注册表中的附表 C。
- 不正确或不匹配的联系信息（包括姓名、ABN 或商标 (TM) 号）将导致注册、交易和续订失败。可能需要变更所有权才能更正现有域的信息。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。设置密钥时，您必须选择 DNS 安全算法 2 (DH)。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期前 60 天直至到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 29 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 30 天

删除域注册

.com.au 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

变更所有权

以编程方式或使用 Route 53 控制台更改拥有者。请参阅Updating contact information for a domain（更新域的联系信息）。然后完成以下过程以完成所有权变更：

1. 新老注册者都必须点击他们在 transfers@1api.net 的电子邮件中收到的链接到他们列出的电子邮件地址。您必须在 14 天内完成此过程，否则必须重新开始。

2. 确认回复后，将在短时间内处理注册表中的拥有者变更，而无需进一步确认。

.com.sg（新加坡共和国）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .com.sg 域或将 .com.sg 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .sg 域。

Return to index

续订期限

一两年。

删除域注册

.com.sg 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

转移所需的授权代码

不支持。不再支持将 .com.sg 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 60 天

.fm（密克罗尼西亚联邦）

在线媒体和广播所涉及的组织也通常将其用作通用 TLD。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 79 天之间
- 从注册表中删除域名：到期后 84 天

.in（印度）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 65 天

.jp（日本）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，但有一项限制：

- 只有在日本的个人或公司可以注册 .jp 域名。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持日语。

转移所需的授权代码

可以。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续约：到期日前 16 天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前 6 天
- 可以使用注册表进行恢复：请联系 Amazon Support。
- 从注册表中删除域名：联请系 Amazon Support。

> **Note**
>
> 目前 non-general-purpose无法注册.jp 和.or.jp 等日本域名。

.io（英属印度洋领地）

此外，与计算机相关的组织 (如在线服务、基于浏览器的游戏和初创公司) 通常将其用作通用 TLD。

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

除国家/地区外，所有信息 state/province 均被隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

.io 域的注册机构也将授权代码用作某些操作的一次性密码，如启用或禁用隐私保护。如果要执行多个需要密码的操作，则必须为每个操作生成另一个授权代码。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域：到期后 90 天

.net.au（澳大利亚）

Return to index

来自 TLD 注册机构的确认电子邮件

我们的注册商助理 Gandi 通过以下方式转售.net.au 域名。DomainDirectors当您将域名转移到 Route 53 时，DomainDirectors 会向该域的注册人联系人发送一封电子邮件以验证联系人信息或授权转移请求。

注册和续订的租赁期

1 到 5 年。

限制

对公众开放，但有一些限制：

- .com.au 和 .net.au 域向以下对象开放：在澳大利亚注册的法人、贸易、合作关系或专营商；经许可能在澳大利亚进行交易的外国公司；以及澳大利亚注册商标的所有者或申请人。
- 您的域名必须与名称 (已向澳大利亚相关机构注册) 或商标 (缩写或缩略词) 相同。

- 域名应指明您的活动。例如，它应指明您销售的产品或提供的服务。
- 在注册过程中，您必须指明以下内容：
  - 您的注册类型：ABN (澳大利亚企业号码)、ACN (澳洲公司注册号) 或 TM (商标，如果域名与商标对应)。
  - 您的 ID 号，可以是澳大利亚企业号码 (ABN)、澳大利亚公司注册号 (ACN) 或商标 (TM)（如果域名与商标对应）。
  - 您的注册商名称，即注册该域的法人实体的名称。此值必须所提供的名称完全匹配。
  - 您的资格类型，即注册此域名的法人实体的类型。
  - 允许您注册此域名的原因（策略原因）：
    - 域名与注册商的公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写相匹配。（策略原因 1）
    - 域名符合分配规则，但不是注册商公司或商业名称、组织或协会名称或商标的首字母缩略词或缩写。（策略原因 2）。要查看 .net.au 的分配规则，请参阅 net.au 注册表中的附表 E。
- 不正确或不匹配的联系信息（包括姓名、ABN 或商标 (TM) 号）将导致注册、交易和续订失败。可能需要变更所有权才能更正现有域的信息。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。设置密钥时，您必须选择 DNS 安全算法 2 (DH)。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期前 60 天直至到期日

- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 29 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 30 天

删除域注册

.net.au 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

变更所有权

以编程方式或使用 Route 53 控制台更改拥有者。请参阅Updating contact information for a domain（更新域的联系信息）。然后完成以下过程以完成所有权变更：

1. 新老注册者都必须点击他们在 transfers@1api.net 的电子邮件中收到的链接到他们列出的电子邮件地址。您必须在 14 天内完成此过程，否则必须重新开始。

2. 确认回复后，将在短时间内处理注册表中的拥有者变更，而无需进一步确认。

.net.nz（新西兰）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 个人需年满 18 岁。
- 组织必须已注册。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编

程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 134 天之间
- 从注册表中删除域：到期后 134 天

.nz（新西兰）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 个人需年满 18 岁。
- 组织必须已注册。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编

程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 134 天之间
- 从注册表中删除域：到期后 134 天

.org.nz（新西兰）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 个人需年满 18 岁。
- 组织必须已注册。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编

程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 44 天
- 可以使用注册表进行恢复：到期后 44 天到 134 天之间
- 从注册表中删除域：到期后 134 天

.pw（帕劳）

Return to index

.pw 最初是为帕劳居民保留的，帕劳是西太平洋中大洋洲密克罗尼西亚子区域的一个岛国，但是，现在该域通常用于代表“专业网站”，且可供所有人使用。

注册和续订的租赁期

1 到 10 年。

隐私保护（适用于所有联系人类型：个人、公司、协会和公共机构）

组织名称之外的所有信息都处于隐藏状态。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 75 天

.qa（卡塔尔）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .qa 域或将 .qa 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .qa 域。

Return to index

续订期限

1 到 5 年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

转移所需的授权代码

不支持。不再支持将 .qa 域转移到 Route 53。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 31 天

.ru（俄罗斯联邦）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .ru 域或将 .ru 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .ru 域。

Return to index

注册和续订的租赁期

一年。

> **Note**
>
> .ru 域的注册机构将在域到期的当天更新域的到期日期。在到达该日期之前，WHOIS 查询将显示该域名的旧到期日期，无论您何时使用 Route 53 续订域名都是如此。

限制

对公众开放，但有一些限制：

- 个人可能需要提供护照号码或政府签发的 ID 号。
- 外国公司可能需要提供公司 ID 或公司注册。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

不支持。

转移所需的授权代码

不支持。不再支持将 .ru 域传输到 Route 53。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日前 2 天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前 2 天
- 可以使用注册表进行恢复：到期后 2 天到 28 天之间
- 从注册表中删除域名：到期后 28 天

删除域注册

.ru 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.sg（新加坡共和国）

> **Important**
>
> 您不再能够使用 Route 53 注册新的 .sg 域或将 .sg 域转移到 Route 53。我们将继续支持已经使用 Route 53 注册的 .sg 域。

Return to index

续订期限

一两年。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

转移所需的授权代码

不支持。不再支持将 .sg 域传输到 Route 53。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 60 天

删除域注册

.sg 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

欧洲

您可以使用以下欧洲顶级域名 (TLDs) 在 Amazon Route 53 上注册域名。

, , , , , , , , , , , , , , , , , , , ,

Return to index

.be（比利时）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

可以。您可以从 DNS 比利时网站获取转移代码。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：于到期日期
- 可以使用注册表进行恢复：直到到期后 40 天
- 从注册表中删除域名：到期后 40 天

.berlin（德国的城市柏林）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 所有者、管理或技术联系人必须提供位于柏林的地址，负责管理的联系人必须为个人。
- 您必须在注册后的 12 个月内激活并使用 .berlin 域 (适用于网站、重新导向或电子邮件地址)。
- 如果在 .berlin 域下发布网站或您的 .berlin 域重新导向至其它网站，则该网站内容必须与柏林相关。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持拉丁语和西里尔语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 80 天

.ch（瑞士）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 9 天
- 从 Route 53 中删除域名：过期后 9 天
- 可以使用注册表进行恢复：到期后 9 天到 49 天之间
- 从注册表中删除域名：到期后 49 天

.co.uk（英国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持

国际化域名

不支持。

转移所需的授权代码

如果要将 .co.uk 域转移到 Route 53，则无需获取授权代码。相反，请使用当前域注册商提供的方法将域的 IPS 标签的值更新为 GANDI (全部大写)。(.uk 域名的注册机构 Nominet 需要一个 IPS 标签。) 如果您的注册商不会更改 IPS 标签的值，请联系 Nominet。

> **Note**
>
> 当您注册 .co.uk 域时，Route 53 会自动将该域的 IPS 标签设置为 GANDI。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期日前 180 天到到期后 30 天之间
- 可以对 Route 53 进行延期续订：过期后 30 天到 90 天之间
- 从 Route 53 中删除域名：过期后 90 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 92 天

删除域注册

.co.uk 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.cz（捷克共和国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持，但会为所有联系人隐藏电子邮件地址和电话号码。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

如果您当前的注册商没有提供授权码，请转到 `https://www.nic.cz/whois/send-password/` 以申请授权码，使 CZ 域名注册机构将其发送到注册人的电子邮件地址。

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 58 天
- 从 Route 53 中删除域名：过期后 59 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 60 天

.de（德国）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，但有一些限制：

- 您必须居住在德国，或者您的管理联系人 (自然人) 居住在德国并且具有除了邮政信箱之外的地址。
- 在注册过程中，必须对域名的 DNS (A、MX 和 CNAME) 进行正确配置，以使其可以通过注册机构的区域检查。需要属于两种不同 C 类的三台服务器。
- 如果您使用的 DNS 服务不是 Route 53，则域的名称服务器必须通过检查，以确保其配置正确。要确定您的域名的域名服务器能否通过检查，请参阅 https://www.denic。 de/en/service/tools/nast/。
- 您必须提供符合注册表验证要求的联系信息。联系人详细信息无效或格式不正确可能会导致域续订失败。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：于到期日期
- 可以使用注册表进行恢复：请联系 Amazon Support。
- 从注册表中删除域名：联请系 Amazon Support。

.es（西班牙）

Return to index

Domain purchase or transfer

> **Important**
>
> 您现在可以购买新的 .es 域名或将 .es 域转移至 Route 53。注册人联系人的联系人类型不存在限制。管理员/技术人员/账单联系人类型必须是人。

注册和续订的租赁期

1 到 5 年。

限制

向对西班牙语感兴趣或与之有关系的公众开放。

自 2016 年起，.ES 域名注册者必须提供注册者联系电子邮件。如果您尚未提供此信息，则需要在将域名转移到 Route 53 之前在当前的注册商处提供。

您将需要以下信息：

- ESNIC 标识符类似于。*AAAA0-ESNIC-F0*
- 如果您不知道 ESNIC 标识符，则可以从当前注册商处获取。可以在以下网址查找您的注册商：https://www.dominios.es/en。

根据您是否记得注册商处的密码，您可以按照以下程序之一更新自己的注册者电子邮件：

- 如果你记得自己的密码，请通过 https://www.nic 登录。 es/sgnd/login.action 使用你的 ESNIC 标识符和密码。

  登录后，您可以通过选择注册页面上的编辑选项卡来编辑注册者的电子邮件联系方式。
- 如果你忘记了密码，请浏览至 https://www.nic。 es/sgnd/peticion/editCorreo.action？request_locale=en。

  在表单中填入您的 ESNIC 标识符、新的有效注册者电子邮件联系方式。然后，通过选择不使用 eID/Certificate 处理来验证表单，并且上传请求的身份证件。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持

国际化域名

支持。

转移所需的授权代码

是

.es 注册表使用管理授权码 time-to-live，授权码可能会过期。如果您的域名存在转移锁 (clientTransferProhibited) 状态，则可以通过将其从域中移除来刷新授权码。如果域没有转移锁定，则可以先将其开启，然后再关闭，从而刷新授权码。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日前 6 天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前 6 天
- 可以使用注册表进行恢复：到期前 6 天到到期后 4 天之间
- 从注册表中删除域名：到期后 4 天

.eu（欧盟）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一项限制：

- 您必须提供来自欧洲经济区 (EEA) 30 国之一的有效邮政地址，或者，如果您是欧盟 (EU) 27 个成员国之一的公民，则必须指定您的欧盟公民身份。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

您还可以在以下注册机构处使用“My.eu”面板生成授权代码：https://my.eurid.eu/。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：于到期日期
- 可以使用注册表进行恢复：直到到期后 40 天
- 从注册表中删除域名：到期后 40 天

WHOIS 搜索

有关现有 .eu 域的信息，请参阅 https://whois.eurid.eu/en/。

.fi（芬兰）

Return to index

注册和续订的租赁期

1 到 5 年。

限制

对公众开放，但有一些限制：

- .fi 可用于在芬兰有永久居住地并且具有芬兰身份证号的个人以及在芬兰注册的法人或私营企业主。
- 如果注册者的联系地址在芬兰，则个人注册者需要芬兰身份号码，公司注册者则需要芬兰公司号码，并且注册期间您必须提供以下信息：
  - 联系人基于芬兰的自然人还是法人。
  - 如果基于法人的名字，则需提供记录该名称的注册机构的标识符。
  - 如果基于法人的名字，则需提供记录该名称的注册机构中的记录编号。
  - 法人在芬兰的识别号。
  - 自然人在芬兰的识别号。
  - 如果注册人为非芬兰公司，则必须提供公司编号作为增值税号。
- 如果注册者地址不在芬兰，则无需芬兰身份号码或公司号码。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：不可以

删除域注册

有关删除域的信息，请参阅 Deleting a domain name registration（删除域名注册）。

.fr（法国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 个人必须年满18岁，并且必须提供date-of-birth。
- 组织必须位于欧洲经济区或瑞士。
- 组织应填写所有公司标识字段 (增值税号、SIREN、WALDEC、DUNS 等)，以便于 AFNIC 日后执行任何验证。
- 相同的资格条件也适用于管理联系人。
- 名称和条款需经 AFNIC 事先审查 (命名规章第 2.4 款) 并满足以下附加条件：
  - 将之前被保留或禁止的域名向有合法权利并且出于善意行事的申请人开放。
  - 以 ville、mairie、agglo、cc、cg 和 cr 开头的名称需符合 AFNIC 命名约定。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 27 天
- 从 Route 53 中删除域名：过期后 28 天
- 可以使用注册表进行还原：到期后 28 天到 58 天之间
- 从注册表中删除域名：到期后 58 天

.gg（格恩西）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天

- 可以使用注册表进行还原：到期后 30 天到 35 天之间
- 从注册表中删除域名：到期后 35 天

.im（英国属地曼岛）

此外，即时消息服务或要开发“I am”品牌的个人也将其用作通用 TLD。

Return to index

注册和续订的租赁期

一两年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 30 天

.it（意大利）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，但有一些限制：

- 个人或组织必须拥有位于欧盟的注册地址。
- 如果原产国为意大利，则必须输入财务代码。如果原产国在欧盟内，则必须输入标识文档号 (ID 号)。
- 域的名称服务器必须通过 DNS 检查。我们建议您在 https://dns-check.nic.it/ 检查名称服务器，然后再提交变更请求。如果域名不符合技术要求（例如，其并未与操作名称服务器关联），而您在 30 天内未进行更正，注册机构将会删除您的域名。由于被删除的域不满足技术要求，因此我们不会为这些域发放退款。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持。

转移所需的授权代码

是

DNSSEC

不支持。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 13 天
- 从注册表中删除域名：到期后 49 天
- 可以使用注册表进行恢复：到期后 14 天到 44 天之间
- 从注册表中删除域名：联请系 Amazon Support。

.me（黑山共和国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

.me 域的注册机构 Domain.me 将两个字母的域名和一些更长的域名视为高级域名。不能向 Route 53 注册高级 .me 域或将此类域转移到 Route 53。有关高级 .me 域名的更多信息，请参阅 domain.me 网站。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持阿拉伯语、白俄罗斯语、波斯尼亚语、保加利亚语、简体中文、繁体中文、克罗地亚语、丹麦语、法语、德语、印地语、匈牙利语、冰岛语、意大利语、韩语、拉脱维亚语、立陶宛语、蒙古语、黑山语、波兰语、葡萄牙语、俄语、塞尔维亚语、西班牙语、瑞典语、土耳其语和乌克兰语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日

- 可以对 Route 53 进行延期续订：直到过期后 29 天
- 从 Route 53 中删除域名：过期后 30 天
- 可以使用注册表进行恢复：到期后 30 天到 60 天之间
- 从注册表中删除域名：到期后 65 天

.me.uk（英国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持

国际化域名

不支持。

转移所需的授权代码

如果要将 .me.uk 域转移到 Route 53，则无需获取授权代码。相反，请使用当前域注册商提供的方法将域的 IPS 标签的值更新为 GANDI (全部大写)。(.uk 域名的注册机构 Nominet 需要一个 IPS 标签。) 如果您的注册商不会更改 IPS 标签的值，请联系 Nominet。

> **Note**
>
> 当您注册 .me.uk 域时，Route 53 会自动将该域的 IPS 标签设置为 GANDI。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期日前 180 天到到期后 30 天之间
- 可以对 Route 53 进行延期续订：过期后 30 天到 90 天之间
- 从 Route 53 中删除域名：过期后 90 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 92 天

删除域注册

.me.uk 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.nl（荷兰）

Return to index

注册和续订的租赁期

一年。

限制

对公众开放，但有一些限制：

- 所有者或管理联系人必须提供位于荷兰的有效地址。必须在当地有业务。
- 如果您没有位于荷兰的有效地址，注册机构 SIDN 将根据居所地址步骤为您提供居所地址。
- 域名必须为 3-63 个字符，不包括 .nl。

Privacy protection（隐私保护）

由注册机构确定。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

不支持。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日前 1 天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前一天
- 可以使用注册表进行恢复：到期前 1 天到到期后 39 天之间
- 从注册表中删除域名：到期后 39 天

.org.uk（英国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持

国际化域名

不支持。

转移所需的授权代码

如果要将 .org.uk 域转移到 Route 53，则无需获取授权代码。相反，请使用当前域注册商提供的方法将域的 IPS 标签的值更新为 GANDI (全部大写)。(.uk 域名的注册机构 Nominet 需要一个 IPS 标签。) 如果您的注册商不会更改 IPS 标签的值，请联系 Nominet。

> **Note**
>
> 当您注册 .org.uk 域时，Route 53 会自动将该域的 IPS 标签设置为 GANDI。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期日前 180 天到到期后 30 天之间
- 可以对 Route 53 进行延期续订：过期后 30 天到 90 天之间
- 从 Route 53 中删除域名：过期后 90 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 92 天

删除域注册

.org.uk 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.ruhr（鲁尔区，德国西部）

Return to index

.ruhr 扩展名用于鲁尔区域 (德国西部)。

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一项限制：

- 管理联系人必须是拥有德国地址的个人。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持 (ä、ö、ü、ß)。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：联请系 Amazon Support。

.se（瑞典）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 如果您在瑞典，则必须提供有效的瑞典 ID 号。ID 编号的格式为 YYMMDD-NNNN。
- 如果您在瑞典之外，则必须输入有效的 ID 号，例如税务 ID 号。

其他验证要求

自 2025 年 10 月 1 日起，.se 域注册需要额外的身份验证，以符合注册表新的 NIS 2.0 要求。当您注册 .se 域时，我们会与您联系以请求验证文档。在您提供所需文档并完成验证之前，您的域注册将一直处于待处理状态。要提交您的文档，请联系 Supp Amazon ort。

.se 注册表还会对现有域进行定期审计，并可能请求对最近注册的域或您对域名进行某些更改（例如更新域所有者或联系人信息）时进行额外验证。如果您的域处于 `serverHold` 状态，则意味着注册表需要先进行验证，然后才能完全激活您的域。

您需要提供的文档：

- 对于个人：政府签发的身份证件（例如身份证或护照）和 3 个月以内的地址证明。
- 对于公司或组织：公司或组织的注册证书，以及地址证明（如果与注册证书不同）。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

不支持。我们建议您通过限制 RetrieveDomainAuthCodeAPI 操作的访问权限来防止未经授权的传输。（当您限制对此 Route 53 API 的访问权限时，还会限制谁可以使用 Route 53 控制台和其他编程方法生成授权码。）Amazon SDKs 有关更多信息，请参阅 Amazon Route 53 中的 Identity and Access Management。

国际化域名

支持拉丁语、瑞典语和意第绪语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日前 1 天
- 可以对 Route 53 进行延期续订：否
- 从 Route 53 中删除域名：过期前一天
- 可以使用注册表进行恢复：到期前 1 天到到期后 59 天之间
- 从注册表中删除域名：到期后 64 天

.uk（英国）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，没有任何限制。

Privacy protection（隐私保护）

所有信息均会隐藏。

域锁定，用于防止未经授权的传输

支持

国际化域名

不支持。

转移所需的授权代码

如果要将 uk 域转移到 Route 53，则无需获取授权代码。相反，请使用当前域注册商提供的方法将域的 IPS 标签的值更新为 GANDI (全部大写)。(.uk 域名的注册机构 Nominet 需要一个 IPS 标签。) 如果您的注册商不会更改 IPS 标签的值，请联系 Nominet。

> **Note**
>
> 当您注册 .uk 域时，Route 53 会自动将该域的 IPS 标签设置为 GANDI。

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：到期日前 180 天到到期后 30 天之间
- 可以对 Route 53 进行延期续订：过期后 30 天到 90 天之间
- 从 Route 53 中删除域名：过期后 90 天
- 可以使用注册表进行恢复：否
- 从注册表中删除域名：到期后 92 天

删除域注册

.uk 域的注册机构不允许删除域注册。相反，您必须禁用自动续订并等待域到期。有关更多信息，请参阅 Deleting a domain name registration（删除域名注册）。

.wien（奥地利的城市维也纳）

Return to index

注册和续订的租赁期

1 到 10 年。

限制

对公众开放，但有一些限制：

- 您必须展示奥地利城市维也纳的经济、文化、旅游、历史、社会或其他吸引力。
- 在整个注册期限内，必须将 .wien 域名与上述条件结合使用。

Privacy protection（隐私保护）

不支持。

域锁定，用于防止未经授权的传输

支持。

国际化域名

支持拉丁语。

转移所需的授权代码

是

DNSSEC

支持域注册。有关更多信息，请参阅 为域配置 DNSSEC。

续订和恢复域名的截止日期

- 可以续订：直到到期日
- 可以对 Route 53 进行延期续订：直到过期后 44 天
- 从 Route 53 中删除域名：过期后 45 天
- 可以使用注册表进行恢复：到期后 45 天到 75 天之间
- 从注册表中删除域名：到期后 80 天

将 Amazon Route 53 配置为 DNS 服务

可将 Amazon Route 53 用作域 (如 example.com) 的 DNS 服务。当 Route 53 用作您的 DNS 服务时，它会通过将友好域名 (例如 www.example.com) 转换为数字 IP 地址 (例如 192.0.2.1，计算机可利用这些地址互相连接) 来将互联网流量路由到您的网站。当有人在浏览器中输入您的域名或向您发送电子邮件时，会向 Route 53 转发一个 DNS 查询，后者会用相应的值来响应。例如，Route 53 可能使用 example.com 的 Web 服务器的 IP 地址作出响应。

> **⚠ DNS 托管与域注册**
>
> 本章介绍如何仅使用 Route 53 进行 DNS 托管。这意味着您的域注册将保留在当前的注册商处，并且您将继续向他们支付域续订费用。Route 53 仅会管理您的 DNS 设置和处理域的 DNS 查询。
>
> 如果您还想将域注册转移到 Route 53（将 Route 53 同时作为注册商和 DNS 服务），请参阅域转移的转移前核对清单 和 将域注册转移到 Amazon Route 53。

在本章中，我们说明了如何配置 Route 53 以将互联网流量路由到正确位置。另外，我们会说明在您当前正在使用其它 DNS 服务的情况下，如何将 DNS 服务迁移到 Route 53，以及如何使用 Route 53 作为新域的 DNS 服务。

主题

将 Amazon Route 53 作为现有域的 DNS 服务

如果您要将一个或多个域注册传输到 Route 53，并且您当前正在使用的域注册商不提供付费 DNS 服务，则在迁移域之前需要迁移 DNS 服务。否则，在您传输域的过程中注册商将停止提供 DNS 服务，且关联的网站和 Web 应用程序将在 Internet 上不可用。(您也可以将 DNS 服务从当前注册商迁移到另一个 DNS 服务提供商。对于在 Route 53 注册的域，我们不要求您使用 Route 53 作为 DNS 服务提供商。)

此过程取决于您目前是否在使用该域：

- 如果该域目前正在获取流量（例如，如果您的用户正在使用该域名浏览网站或访问 Web 应用程序），请参阅 将 Route 53 作为正在使用的域的 DNS 服务。
- 如果该域没有获取任何流量 (或正在获取非常少的流量)，请参阅将 Route 53 作为非活动域的 DNS 服务。

对于这两个选项，您的域都应在整个迁移过程中保持可用。但在极少的情况下，如果出现问题，第一个选项可让您快速回滚迁移。如果使用第二个选项，您的域可能在几天内不可用。

如果您想与 Amazon 的专家联系，请访问销售支持。

将 Route 53 作为正在使用的域的 DNS 服务

如果要为目前正在获取流量（例如，如果您的用户正在使用该域名浏览网站或访问 Web 应用程序）的域将 DNS 服务迁移至 Amazon Route 53，请执行此部分中的过程。

主题

- 步骤 11：重新启用 DNSSEC 签名（如果需要）

步骤 1：从当前 DNS 服务提供商获取当前 DNS 配置（可选但推荐）

当您将 DNS 服务从另一个提供商迁移至 Route 53 时，您将在 Route 53 中重现当前 DNS 配置。在 Route 53 中，您创建一个与您的域同名的托管区域，并且您在该托管区域中创建记录。每条记录均指示您希望如何针对指定域名或子域名路由流量。例如，有人在 Web 浏览器中输入您的域名时，您是希望将流量路由到您数据中心中的 Web 服务器、Amazon EC2 实例、CloudFront 分配，还是其它某个位置？

您使用的过程取决于当前 DNS 配置的复杂性：

- 在当前 DNS 配置简单的情况下 — 如果您只是将几个子域的互联网流量路由到少数资源（例如，Web 服务器或 Amazon S3 存储桶），则可以在 Route 53 控制台中手动创建几条记录。
- 在当前 DNS 配置更复杂且您只希望重现当前配置的情况下 — 如果您可以从当前 DNS 服务提供商处获取区域文件并将该区域文件导入 Route 53 中，则可简化迁移过程。(并非所有 DNS 服务提供商都提供区域文件。) 在导入区域文件时，Route 53 将通过在您的托管区域中创建相应记录来自动重现现有配置。

  请询问您目前的 DNS 服务提供商的客户支持，请教如何获取区域文件 或记录列表。有关所需区域文件格式的信息，请参阅通过导入区域文件来创建记录。
- 在当前 DNS 配置更复杂且您对 Route 53 路由功能感兴趣的情况下 — 查看以下文档以了解您是否需要使用其它 DNS 服务提供商未提供的 Route 53 功能。如果是这样，您可以手动创建记录，也可以导入区域文件，并稍后创建或更新记录：
  - 在别名记录和非别名记录之间进行选择 介绍了 Route 53 别名记录的优势，这些记录可免费将流量路由到一些 Amazon 资源，例如 CloudFront 分配和 Amazon S3 存储桶。
  - 选择路由策略 介绍了 Route 53 路由选项，例如，基于用户位置的路由、基于用户和资源之间延迟的路由、基于资源是否正常运行的路由以及基于指定权重传输到相应资源的路由。

> **Note**
>
> 您也可以导入区域文件，并在稍后更改配置以利用别名记录和复杂的路由策略。

如果您无法获取区域文件，或者如果您要在 Route 53 中手动创建记录，则您可能要迁移的记录包括：

- A（地址）记录 — 将域名或子域名与相应资源的 IPv4 地址（例如，192.0.2.3）关联

- AAAA（地址）记录 — 将域名或子域名与相应资源的 IPv6 地址（例如，2001:0db8:85a3:0000:0000:abcd:0001:2345）关联
- 邮件服务器 (MX) 记录 — 将流量路由到邮件服务器
- 别名记录 — 将一个域名 (example.net) 的流量重新路由到另一个域名 (example.com)
- 其它支持的 DNS 记录类型的记录 — 有关支持的记录类型的列表，请参阅 支持的 DNS 记录类型。

步骤 2：创建托管区域

为了告知 Amazon Route 53 您希望如何路由您的域的流量，您创建一个与您的域同名的托管区域，然后在该托管区域中创建记录。

> **Important**
>
> 您只能为您有权管理的域创建托管区域。通常，这意味着您拥有该域，但您还可以为域的注册商开发应用程序。

创建托管区域时，Route 53 会自动为此区域创建名称服务器 (NS) 记录和授权起始点 (SOA) 记录。该 NS 记录标识通过 Route 53 与您的托管区域关联的四个名称服务器。要使 Route 53 成为您的域的 DNS 服务，您需要更新该域的注册以使用这四个名称服务器。

> **Important**
>
> 请不要创建其他名称服务器 (NS) 或授权起始点 (SOA) 记录，并且不要删除现有的 NS 和 SOA 记录。

创建托管区域

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 如果您对 Route 53 不熟悉，请选择 DNS management（DNS 管理）项下的 Get started（入门），然后选择 Create hosted zones（创建托管区域）。

   如果您已经在使用 Route 53，请在导航窗格中选择 Hosted zones（托管区域），然后选择 Create hosted zones（创建托管区域）。

3. 在 Create hosted zone（创建托管区域）窗格中，输入域名，还可以选择输入注释。有关设置的详细信息，请选择打开右侧的帮助面板。

   有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。
4. 对于 Type（类别），接受 Public hosted zone（公有托管区域）的默认值。
5. 选择 Create Hosted Zone（创建托管区域）。

步骤 3：创建记录

创建一个托管区域后，您可在该托管区域中创建记录，这些记录定义您要将域 (example.com) 或子域 (www.example.com) 的流量路由到的位置。例如，如果您希望将 example.com 和 www.example.com 的流量路由到 Amazon EC2 实例上的 Web 服务器，则可创建两条记录，一条记录名为 example.com，另一条记录名为 www.example.com。在每条记录中，指定您的 EC2 实例的 IP 地址。

您可通过多种方式创建记录：

导入区域文件

如果您已在 步骤 1：从当前 DNS 服务提供商获取当前 DNS 配置（可选但推荐） 中从当前 DNS 服务获取区域文件，这将是最轻松的方式。Amazon Route 53 无法预测何时创建别名记录或使用特殊路由类型 (例如，加权或故障转移)。因此，如果您导入区域文件，Route 53 会使用简单路由策略创建标准 DNS 记录。

有关更多信息，请参阅 通过导入区域文件来创建记录。

在控制台中单独创建记录

如果您没有获取区域文件，并且您只想创建几条具有 Simple 路由策略的记录来开始操作，则可在 Route 53 控制台中创建记录。您可以同时创建别名记录和非别名记录。

有关更多信息，请参阅以下主题：

- 选择路由策略
- 在别名记录和非别名记录之间进行选择
- 通过使用 Amazon Route 53 控制台创建记录

以编程方式创建记录

您可以使用某个 Amazon 软件开发工具包、Amazon CLI 或 Amazon Tools for Windows PowerShell 创建记录。有关更多信息，请参阅 Amazon 文档。

如果您正在使用 Amazon 未提供软件开发工具包的编程语言，您也可以使用 Route 53 API。有关更多信息，请参阅 Amazon Route 53 API 参考。

步骤 4：减小 TTL 设置

记录的 TTL（生存时间）设置指定您希望 DNS 解析程序缓存记录和使用缓存信息的时间。当 TTL 过期时，解析程序会向域的 DNS 服务提供商发送另一个查询以获取最新信息。

NS 记录的典型 TTL 设置为 172800 秒或两天。NS 记录列出了域名系统 (DNS) 可用来获取有关如何路由域流量的信息的名称服务器。通过为当前 DNS 服务提供商和 Amazon Route 53 减小 NS 记录的 TTL，可在您将 DNS 迁移至 Route 53 的过程中发现问题时缩短域的停机时间。如果您不减小 TTL，则您的域可能会在出现问题时最多两天内在 Internet 上不可用。

> **Note**
>
> 一些完整解析程序可能会缓存父权威服务器的 NS 记录的 TTL，因此还必须减少在父权威 DNS 服务器上注册的 NS 记录的 TTL。

我们建议您针对以下 NS 记录更改 TTL：

- 当前 DNS 服务提供商的托管区域中的 NS 记录。(您的当前提供商可能使用不同的术语。)
- 您在步骤 2：创建托管区域中创建的托管区域中的 NS 记录。

为当前 DNS 服务提供商减小 NS 记录的 TTL 设置

- 使用域的当前 DNS 服务提供商提供的方法来更改域的托管区域中的 NS 记录的 TTL。

减小 Route 53 托管区域中的 NS 记录的 TTL 设置

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中选择 Hosted Zones。
3. 选择托管区域的名称。
4. 选择 NS 记录，然后选择 Edit（编辑）。
5. 更改 TTL (Seconds) 的值。我们建议您指定一个介于 60 秒和 900 秒 (15 分钟) 之间的值。

6. 选择保存更改。

步骤 5：（如果您已配置 DNSSEC）从父区域中删除 DS 记录

如果已为域配置 DNSSEC，请在将域迁移到 Route 53 之前从父区域中删除 Delegation Signer (DS) 记录。

如果父区域通过 Route 53 或其他注册商托管，请联系他们以删除 DS 记录。

由于目前无法在两个提供程序之间启用 DNSSEC 签名，因此必须删除任何 DS 或 DNSKEY 才能停用 DNSSEC。这会临时向 DNS 解析程序发出信号，以禁用 DNSSEC 验证。在步骤 11 中，您可以在完成向 Route 53 的过渡后重新启用 DNSSEC 验证（如果需要）。

有关更多信息，请参阅 删除域的公有密钥。

步骤 6：等待旧 TTL 过期

如果您的域正在使用中（例如，如果用户正在使用该域名浏览网站或访问 Web 应用程序），则 DNS 解析程序已缓存当前 DNS 服务提供商所提供的名称服务器的名称。已在几分钟前缓存该信息的 DNS 解析程序会将其保存近两天。

为了确保一次性完成 DNS 服务到 Route 53 的迁移，请在减小 TTL 后等待两天。为期两天的 TTL 过期且解析程序请求您的域的名称服务器后，解析程序将获取当前名称服务器，并且还将获取您在步骤 4：减小 TTL 设置中指定的新 TTL。

步骤 7：更新 NS 记录以使用 Route 53 名称服务器

要开始将 Amazon Route 53 用作域的 DNS 服务，请使用注册商提供的方法，或使用父区域，以将 NS 记录中的当前名称服务器替换为 Route 53 名称服务器。

> **Note**
>
> 当您使用当前 DNS 服务提供商更新 NS 记录以使用 Route 53 名称服务器时，您正在更新域的 DNS 配置。（这相当于更新域的某个 Route 53 托管区域中的 NS 记录，只不过您更新设置时使用的是您从中迁出的 DNS 服务。）

在注册机构或父区域更新 NS 记录以使用 Route 53 名称服务器

1. 在 Route 53 控制台中，获取您的托管区域的名称服务器：

a. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

b. 在导航窗格中，选择 Hosted zones（托管区域）。

c. 在 Hosted zones（托管区域）页面上，选择适用的托管区域的名称。

d. 记下 Hosted zone details（托管区域详细信息）部分为 Name servers（名称服务器）列出的四个名称。

2. 使用域的当前 DNS 服务所提供的方法来更新托管区域的 NS 记录。如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录。此过程取决于当前 DNS 服务是否允许您删除名称服务器：

   如果您可以删除名称服务器

   - 记下托管区域的 NS 记录中的当前名称服务器的名称。如果您需要还原到当前 DNS 配置，则这些是您要指定的服务器。
   - 从 NS 记录删除当前名称服务器。
   - 使用您在此过程的步骤 1 中获取的所有四个 Route 53 名称服务器的名称更新 NS 记录。

   > **Note**
   >
   > 完成后，NS 记录中的名称服务器将只有这四个 Route 53 名称服务器。

   如果您无法删除名称服务器

   - 选择使用自定义名称服务器的选项。
   - 添加您在此过程的步骤 1 中获取的所有四个 Route 53 名称服务器。

步骤 8：监控域的流量

监控域的流量，包括网站或应用程序流量，以及电子邮件：

- 在流量慢或停止的情况下 — 请使用上一个 DNS 服务提供的方法，将相应域对应的名称服务器改回之前的名称服务器。这些是您在在注册机构或父区域更新 NS 记录以使用 Route 53 名称服务器的步骤 7 中记下的名称服务器。然后，确定出错的位置。
- 在流量未受影响的情况下 — 继续至 步骤 9：将 NS 记录的 TTL 重新改为更高的值。

步骤 9：将 NS 记录的 TTL 重新改为更高的值

在域的 Amazon Route 53 托管区域中，将 NS 记录对应的 TTL 更改为更典型的值，例如，172800 秒 (两天)。这减少用户的延迟，因为他们不必像 DNS 解析程序一样通常需要等待为您的域的名称服务器发送查询。

更改 Route 53 托管区域中的 NS 记录的 TTL

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中选择 Hosted Zones。
3. 选择托管区域的名称。
4. 在托管区域的记录列表中，选择 NS 记录。
5. 选择编辑。
6. 将 TTL (Seconds) 更改为您希望 DNS 解析程序缓存您的域的名称服务器的名称的秒数。我们建议的值为 172800 秒。
7. 选择保存更改。

步骤 10：将域注册转移到 Amazon Route 53

现在您已将域的 DNS 服务转移到 Amazon Route 53，您可以选择将域的注册转移到 Route 53。有关更多信息，请参阅 将域注册转移到 Amazon Route 53。

步骤 11：重新启用 DNSSEC 签名（如果需要）

现在您已将域的 DNS 服务转移到 Amazon Route 53，您可以重新启用 DNSSEC 签名。

启用 DNSSEC 签名有两个步骤：

- 步骤 1：为 Route 53 启用 DNSSEC 签名，并请求 Route 53 根据客户托管密钥在 Amazon Key Management Service (Amazon KMS) 中创建密钥签名密钥 (KSK)。
- 步骤 2：通过向父区域添加 Delegation Signer (DS) 记录，为托管区域创建信任链，以便使用受信任的加密签名对 DNS 响应进行身份验证。

  有关说明，请参阅启用 DNSSEC 签名并建立信任链。。

将 Route 53 作为非活动域的 DNS 服务

如果要为不获取任何流量 (或正在获取非常少的流量) 的域将 DNS 服务迁移到 Amazon Route 53，请执行本部分中的过程。

主题

步骤 1：从当前 DNS 服务提供商（非活动域）获取当前 DNS 配置

当您将 DNS 服务从另一个提供商迁移至 Route 53 时，您将在 Route 53 中重现当前 DNS 配置。在 Route 53 中，您创建一个与您的域同名的托管区域，并且您在该托管区域中创建记录。每条记录均指示您希望如何针对指定域名或子域名路由流量。例如，有人在 Web 浏览器中输入您的域名时，您是希望将流量路由到您数据中心中的 Web 服务器、Amazon EC2 实例、CloudFront 分配，还是其它某个位置？

您使用的过程取决于当前 DNS 配置的复杂性：

- 在当前 DNS 配置简单的情况下 — 如果您只是将几个子域的互联网流量路由到少数资源（例如，Web 服务器或 Amazon S3 存储桶），则可以在 Route 53 控制台中手动创建几条记录。
- 在当前 DNS 配置更复杂且您只希望重现当前配置的情况下 — 如果您可以从当前 DNS 服务提供商处获取区域文件并将该区域文件导入 Route 53 中，则可简化迁移过程。(并非所有 DNS 服务提供商都提供区域文件。) 在导入区域文件时，Route 53 将通过在您的托管区域中创建相应记录来自动重现现有配置。

  请询问您目前的 DNS 服务提供商的客户支持，请教如何获取区域文件 或记录列表。有关所需区域文件格式的信息，请参阅通过导入区域文件来创建记录。
- 在当前 DNS 配置更复杂且您对 Route 53 路由功能感兴趣的情况下 — 查看以下文档以了解您是否需要使用其它 DNS 服务提供商未提供的 Route 53 功能。如果是这样，您可以手动创建记录，也可以导入区域文件，并稍后创建或更新记录：
  - 在别名记录和非别名记录之间进行选择 介绍了 Route 53 别名记录的优势，这些记录可免费将流量路由到一些 Amazon 资源，例如 CloudFront 分配和 Amazon S3 存储桶。

- 选择路由策略 介绍了 Route 53 路由选项，例如，基于用户位置的路由、基于用户和资源之间延迟的路由、基于资源是否正常运行的路由以及基于指定权重传输到相应资源的路由。

> **Note**
>
> 您也可以导入区域文件，并在稍后更改配置以利用别名记录和复杂的路由策略。

如果您无法获取区域文件，或者如果您要在 Route 53 中手动创建记录，则您可能要迁移的记录包括：

- A（地址）记录 — 将域名或子域名与相应资源的 IPv4 地址（例如，192.0.2.3）关联
- AAAA（地址）记录 — 将域名或子域名与相应资源的 IPv6 地址（例如，2001:0db8:85a3:0000:0000:abcd:0001:2345）关联
- 邮件服务器 (MX) 记录 — 将流量路由到邮件服务器
- 别名记录 — 将一个域名 (example.net) 的流量重新路由到另一个域名 (example.com)
- 其它支持的 DNS 记录类型的记录 — 有关支持的记录类型的列表，请参阅 支持的 DNS 记录类型。

步骤 2：创建托管区域（非活动域）

为了告知 Amazon Route 53 您希望如何路由您的域的流量，您创建一个与您的域同名的托管区域，然后在该托管区域中创建记录。

> **Important**
>
> 您只能为您有权管理的域创建托管区域。通常，这意味着您拥有该域，但您还可以为域的注册商开发应用程序。

创建托管区域时，Route 53 会自动为此区域创建名称服务器 (NS) 记录和授权起始点 (SOA) 记录。该 NS 记录标识通过 Route 53 与您的托管区域关联的四个名称服务器。要使 Route 53 成为您的域的 DNS 服务，您需要更新该域的注册以使用这四个名称服务器。

> **Important**
>
> 请不要创建其他名称服务器 (NS) 或授权起始点 (SOA) 记录，并且不要删除现有的 NS 和 SOA 记录。

创建托管区域

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 如果您不熟悉 Route 53，请选择入门。

   如果您已经在使用 Route 53，请在导航窗格中选择 Hosted zones（托管区域）。
3. 选择 Create Hosted Zone（创建托管区域）。
4. 在 Create hosted zone（创建托管区域）窗格中，输入域名，还可以选择输入注释。要了解有关某项设置的更多信息，请将鼠标指针暂停在其标签上方以查看其工具提示。

   有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS域名格式。
5. 对于 Record Type（记录类型），接受 Public hosted zone（公有托管区域）的默认值。
6. 选择 Create Hosted Zone（创建托管区域）。

步骤 3：创建记录（非活动域）

创建一个托管区域后，您可在该托管区域中创建记录，这些记录定义您要将域 (example.com) 或子域 (www.example.com) 的流量路由到的位置。例如，如果您希望将 example.com 和 www.example.com 的流量路由到 Amazon EC2 实例上的 Web 服务器，则可创建两条记录，一条记录名为 example.com，另一条记录名为 www.example.com。在每条记录中，指定您的 EC2 实例的 IP 地址。

您可通过多种方式创建记录：

导入区域文件

如果您已在 步骤 1：从当前 DNS 服务提供商（非活动域）获取当前 DNS 配置 中从当前 DNS 服务获取区域文件，这将是最轻松的方式。Amazon Route 53 无法预测何时创建别名记录或使用特殊路由类型 (例如，加权或故障转移)。因此，如果您导入区域文件，Route 53 会使用简单路由策略创建标准 DNS 记录。

有关更多信息，请参阅 通过导入区域文件来创建记录。

在控制台中单独创建记录

如果您没有获取区域文件，并且您只想创建几条具有 Simple 路由策略的记录来开始操作，则可在 Route 53 控制台中创建记录。您可以同时创建别名记录和非别名记录。

有关更多信息，请参阅以下主题：

- 选择路由策略
- 在别名记录和非别名记录之间进行选择
- 通过使用 Amazon Route 53 控制台创建记录

以编程方式创建记录

您可以使用某个 Amazon 软件开发工具包、Amazon CLI 或 Amazon Tools for Windows PowerShell 创建记录。有关更多信息，请参阅 Amazon 文档。

如果您正在使用 Amazon 未提供软件开发工具包的编程语言，您也可以使用 Route 53 API。有关更多信息，请参阅 Amazon Route 53 API 参考。

步骤 4：更新域注册以使用 Amazon Route 53 名称服务器（非活动域）

创建完域的记录后，您可以将您的域的 DNS 服务更改为 Amazon Route 53。执行以下过程可更新域注册商的设置。

更新域的名称服务器

1. 在 Route 53 控制台中，获取您的 Route 53 托管区域的名称服务器：
   a. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
   b. 在导航窗格中，选择 Hosted zones（托管区域）。
   c. 在 Hosted zones（托管区域）页面上，选择托管区域的单选按钮（不是名称），然后选择 View details（查看详细信息）。
   d. 在托管区域的详细信息页面上，选择 Hosted zone details（托管区域详细信息）。
   e. 记下针对 Name servers（名称服务器）列出的四个名称。
2. 使用域注册商提供的方法，将域的名称服务器更改为使用您在此过程的步骤 2 中获取的四个 Route 53 名称服务器。

   如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录。

为新域配置 DNS 路由

您从 Route 53 购买的新域

在 Route 53 中注册域时，我们会自动将 Route 53 设置为该域的 DNS 服务。Route 53 会创建一个与该域同名的托管区，将四个名称服务器分配给托管区，并更新该域以使用这些名称服务器。

您从其他注册商处购买的新域

例如，当您从其他注册商处购买域时，由于 Route 53 不提供顶级域（TLD），因此您有两种选择：

- 仅使用 Route 53 进行 DNS 托管：保留您当前的注册商，但将 DNS 管理委托给 Route 53。按照以下步骤创建托管区并更新注册商的名称服务器。
- 将域注册转移到 Route 53：将 Route 53 作为您的注册商和 DNS 服务。请参阅 域转移的转移前核对清单 了解先决条件，参阅 将域注册转移到 Amazon Route 53 了解转移过程。

有关 Route 53 支持的 TLD 的更多信息，请参阅 可向 Amazon Route 53 注册的域。。

按照以下说明创建公共托管区，然后使用注册商创建的名称服务器：

为 Route 53 域创建托管区

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区，然后选择创建托管区。
3. 在名称中，输入要为其创建托管区的域的名称，例如 `example.com`，然后输入可选描述，接下来选择公共托管区，然后选择创建托管区。
4. 创建托管区后，请注意创建的四个名称服务器（NS）记录。每个记录都将以“ns-”开头。

   在您的域注册商处，从上方输入名称服务器，将域管理委托给您的 Route 53 托管区。

路由 DNS 流量

要指定希望 Route 53 如何路由该域的互联网流量，可在该托管区域中创建记录。例如，如果您希望将对 example.com 的请求路由到 Amazon EC2 实例上运行的某个 Web 服务器，可以在 example.com 托管区中创建一条记录并指定该 EC2 实例的弹性 IP 地址。有关更多信息，请参阅以下主题：

- 有关如何在托管区中创建记录的信息，请参阅 使用记录。
- 有关如何将流量路由到所选 Amazon 资源的信息，请参阅 将互联网流量路由到您的 Amazon 资源。
- 有关 DNS 如何工作的信息，请参阅如何将 Internet 流量路由到您的网站或 Web 应用程序。
- 要检查 DNS 响应，请参阅 检查来自 Route 53 的 DNS 响应。

将流量路由到您的资源

当用户请求您的网站或 Web 应用程序（例如，通过在 Web 浏览器中输入您的域名）时，Amazon Route 53 可帮助将用户路由到您的资源，如 Amazon S3 存储桶或数据中心的 Web 服务器。要配置 Route 53 将流量路由到您的资源，请执行以下操作：

1. 创建一个托管区域。您可以创建公有或私有托管区域：

   公有托管区域

   例如，如果您想将互联网流量路由到您的资源，请创建一个公共托管区域，以便您的客户可以查看您在 EC2 实例上托管的公司网站。有关更多信息，请参阅 使用公有托管区。

   私有托管区域

   如果您要在 Amazon VPC 内路由流量，则创建私有托管区域。有关更多信息，请参阅 使用私有托管区。

2. 在托管区域中创建记录。记录定义您希望针对每个域名或子域名将流量路由到何处。例如，要将 www.example.com 的流量路由到数据中心的 Web 服务器，您通常会在 example.com 托管区域中创建 www.example.com 记录。

   有关更多信息，请参阅以下主题：

   - 使用记录
   - 路由子域的流量
   - 将互联网流量路由到您的 Amazon 资源

路由子域的流量

当您希望将子域（如 acme.example.com 或 zenith.example.com）的流量路由至您的资源时，您有两个选项：

在域的托管区域中创建记录

通常情况下，要路由子域的流量，应在托管区域中创建一条与域同名的记录。例如，要将 acme.example.com 的 Internet 流量路由到数据中心的 Web 服务器，应在 example.com 托管区域中创建一条名为 acme.example.com 的记录。有关更多信息，请参阅主题使用记录及其子主题。

为子域创建一个托管区域，并在新的托管区域中创建记录

您还可以为子域创建托管区域。使用单独的托管区域将 Internet 流量路由至子域的做法，有时称为“将子域的责任委托给托管区域”或“将子域委托给其他名称服务器”或类似用语的组合。下面概览了使用方式：

1. 您可以创建一个托管区域，其名称与要路由流量的子域相同，例如 acme.example.com。
2. 在新的托管区域中创建记录，以定义您要如何路由子域 (acme.example.com) 及其子域（如 backend.acme.example.com）的流量。
3. 您可以获取在创建新托管区域时 Route 53 分配给新托管区域的名称服务器。
4. 您在托管区域中为该域创建了一条新的 NS 记录 (example.com)。NS 记录名称必须是子域名 (acme.example.com)，并且您可以指定在步骤 3 中获得的四个域名服务器作为记录值。

使用单独的托管区域为子域路由流量时，您可以使用 IAM 权限来限制对子域的托管区域的访问权限。如果您有多个由不同组管理的子域，则为每个子域创建托管区域，可以显著减少必须对域的托管区域中的记录具有访问权限的人数。

要实施此委派流程，您需要以下 IAM 权限。有关 Route 53 IAM 策略的更多信息，请参阅Amazon Route 53 中的 Identity and Access Management：

家长账户（拥有 example.com）

用户或角色需要权限才能修改父域托管区域中的记录：

儿童账户（创建 acme.example.com）

用户或角色需要权限才能创建和管理子域托管区域：

为子域使用单独的托管区域还允许您为域和子域使用不同的 DNS 服务。有关更多信息，请参阅 使用 Amazon Route 53 作为子域的 DNS 服务，但不迁移父域。

对于每个 DNS 解析程序中第一个 DNS 查询，这种配置对性能会有小的影响。解析程序必须先从根域的托管区域获取信息，然后从子域的托管区域获取信息。在子域的第一个 DNS 查询后，解析程序会缓存信息，且不需要再次获取此信息，直到 TTL 到期和其他客户端从该解析程序请求该子域为止。有关更多信息，请参阅在您创建或编辑 Amazon Route 53 记录时指定的值部分中的 TTL（秒）。

主题

- 创建另一个托管区域来路由子域的流量
- 为其他级别的子域路由流量

创建另一个托管区域来路由子域的流量

一种路由子域流量的方法是为子域创建一个托管区域，然后在新的托管区域中为子域创建记录。(更常用的选项是在域的托管区域中为子域创建记录。)

> **Note**
>
> 此过程说明如何将子域委托给 Route 53。您也可以将子域委托给其他 DNS 服务，方法是创建指向这些服务的域名服务器的 NS 记录。

过程概览：

1. 为子域创建托管区域。有关更多信息，请参阅 为子域创建新的托管区域。
2. 将记录添加到子域的托管区域。如果域的托管区域包含属于子域的托管区域中的任何记录，则在托管区域中为子域复制这些记录。有关更多信息，请参阅 在子域的托管区域中创建记录
3. 在域的托管区域中为子域创建 NS 记录，这会将子域的责任委托给新托管区域中的名称服务器。如果域的托管区域包含属于子域的托管区域中的任何记录，则从域的托管区域中删除记录。（第 2 步中您在托管区域中为子域创建的副本。）有关更多信息，请参阅 更新域的托管区域。

为子域创建新的托管区域

要使用 Route 53 控制台为子域创建托管区域，请执行以下步骤。

为子域创建托管区域 (控制台)

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 如果您不熟悉 Route 53，请选择入门。

   如果您已经在使用 Route 53，请在导航窗格中选择 Hosted zones（托管区域）。
3. 选择 Create Hosted Zone（创建托管区域）。
4. 在右侧窗格中，输入子域的名称，如 acme.example.com。您也可以根据需要输入注释。

   有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS域名格式。
5. 对于 Type（类型），接受 Public hosted zone（公有托管区域）的默认值。
6. 在右窗格的底部，选择 Create hosted zone（创建托管区域）。

在子域的托管区域中创建记录

要定义您希望 Route 53 如何路由子域 (acme.example.com) 及其子域（如 backend.acme.example.com）的流量，请在子域的托管区域中创建记录。

对于在托管区域中为子域创建记录，请注意以下事项：

- 请勿在子域的托管区域中创建其他名称服务器 (NS) 或授权起始点 (SOA) 记录，且请勿删除现有的 NS 和 SOA 记录。
- 在子域的托管区域中创建子域的所有记录。例如，如果您有 example.com 和 acme.example.com 域的托管区域，请在 acme.example.com 托管区域中创建 acme.example.com 子域的所有记录。这包括 backend.acme.example.com 和 beta.backend.acme.example.com 等记录。
- 如果域 (example.com) 的托管区域已包含属于子域 (acme.example.com) 的托管区域中的任何记录，则在托管区域中为子域复制这些记录。在流程的最后一步中，您稍后删除域的托管区域中的重复记录。

> **Important**
>
> 如果您有一些子域的记录同时处于域的托管区域以及子域的托管区域中，则 DNS 行为将不一致。其行为将取决于 DNS 解析程序缓存了哪些名称服务器、域托管区域 (example.com) 的名称服务器或子域托管区域 (acme.example.com) 的名称服务器。在某些情况下，当记录存在但不在 DNS 解析程序将查询提交到的托管区域中时，Route 53 会返回 NXDOMAIN（不存在的域）。

有关更多信息，请参阅 使用记录。

更新域的托管区域

当您创建托管区域时，Route 53 会自动为该区域分配四个名称服务器。托管区域的 NS 记录标识响应域或子域的 DNS 查询的名称服务器。要开始使用子域的托管区域中的记录路由 Internet 流量，您应在域 (example.com) 的托管区域中创建新的 NS 记录，用子域 (acme.example.com) 名称为其命名。对于 NS 记录的值，您应从子域的托管区域指定名称服务器的名称。

下面介绍当 Route 53 从子域 acme.example.com 或其子域之一的 DNS 解析程序中收到 DNS 查询时将发生的情况。

1. Route 53 在域 (example.com) 的托管区域中进行查找，并找到子域 (acme.example.com) 的 NS 记录。

2. Route 53 从域 (example.com) 的托管区域中的 acme.example.com NS 记录获取名称服务器，并将这些名称服务器返回到 DNS 解析程序。
3. 解析程序向 acme.example.com 托管区域的名称服务器重新提交针对 acme.example.com 的查询。
4. Route 53 使用 acme.example.com 托管区域中的记录响应此查询。

要配置 Route 53 使用子域的托管区域路由子域的流量并从域的托管区域中删除所有重复记录，请执行以下过程：

配置 Route 53 使用子域的托管区域（控制台）

1. 在 Route 53 控制台中，获取子域的托管区域的名称服务器：
   a. 在导航窗格中，选择 Hosted zones（托管区域）。
   b. 在 Hosted zones（托管区域）页面上，选择子域的托管区域的名称。
   c. 在右侧窗格中，复制 Hosted zones details（托管区域详细信息）部分中 Name servers（名称服务器）下所列的四个服务器的名称。
2. 选择域 (example.com，而非子域) 的托管区域的名称。
3. 选择创建记录。
4. 选择 Simple routing（简单路由），然后选择 Next（下一步）。
5. 请选择定义简单记录。
6. 指定以下值：

   Name

   输入子域的名称（例如，`acme.example.com`）。这必须与您创建的子域托管区域的名称完全匹配。

   值/流量路由至

   选择 IP address or another value depending on the record type（IP 地址或取决于记录类型的其它值），然后粘贴您在步骤 1 中复制的名称服务器的名称。

   记录类型

   选择 NS – Name servers for a hosted zone（NS — 用于托管区域的名称服务器）。

   TTL (秒)

   更改为更常用的 NS 记录值，如 172800 秒。

7. 选择 Define simple record（定义简单记录），然后选择 Create records（创建记录）。
8. 如果域的托管区域包含您在子域的托管区域中重新创建的任何记录，则从域的托管区域中删除这些记录。有关更多信息，请参阅 删除记录。

   完成后，子域的所有记录应在子域的托管区域中。

为其他级别的子域路由流量

您可以将流量路由到子域的子域 (如 backend.acme.example.com)，采用的方式与您将流量路由到子域 (如 acme.example.com) 相同。要么在域的托管区域中创建记录；要么为更低级别的子域创建托管区域，然后在该新的托管区域中创建记录。

如果您选择为低一级子域创建单独的托管区域，请在与域名更近一级的子域的托管区域中为低一级的子域创建 NS 记录。这有助于确保将流量正确路由到您的资源。例如，假设您需要路由以下各子域的流量：

- subdomain1.example.com
- subdomain2.subdomain1.example.com

要使用另一个托管区域来路由 subdomain2.subdomain1.example.com 的流量，您需要执行以下操作：

1. 创建名为 subdomain2.subdomain1.example.com 的托管区域。
2. 在 subdomain2.subdomain1.example.com 的托管区域中创建记录。有关更多信息，请参阅 在子域的托管区域中创建记录。
3. 复制 subdomain2.subdomain1.example.com 托管区域的名称服务器的名称。
4. 在 subdomain1.example.com 托管区域中，创建一个名为 subdomain2.subdomain1.example.com 的 NS 记录，并粘贴 subdomain2.subdomain1.example.com 托管区域的名称服务器的名称。

   此外，删除 subdomain1.example.com 中的任何重复记录。有关更多信息，请参阅 更新域的托管区域。

   创建此 NS 记录后，Route 53 开始使用 subdomain2.subdomain1.example.com 托管区域来路由 subdomain2.subdomain1.example.com 子域的流量。

使用托管区域

托管区是一个记录容器，记录中包含的信息说明您希望如何路由特定域（如 example.com）及其子域（acme.example.com、zenith.example.com）的流量。托管区与相应域具有相同的名称。有两种类型的托管区：

- 公有托管区 包含指定了如何路由 Internet 流量的记录。有关更多信息，请参阅 使用公有托管区。
- 私有托管区 包含指定了如何在 Amazon VPC 中路由流量的记录。有关更多信息，请参阅 使用私有托管区。

使用公有托管区

公有托管区域是一个容器，其中包含的信息说明您希望如何路由特定域（如 example.com）及其子域（acme.example.com 和 zenith.example.com）的 Internet 流量。您可以通过两种方式获取公有托管区域：

- 在 Route 53 中注册域时，我们会自动为您创建一个托管区域。
- 在将一个现有域的 DNS 服务转移到 Route 53 时，您会首先为该域创建托管区域。有关更多信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

在这两种情况下，之后都要在托管区域中创建记录，以指定希望如何路由该域及其子域的流量。例如，您可以创建一条记录，将 www.example.com 的流量路由到 CloudFront 分配或数据中心内的 Web 服务器。有关记录的更多信息，请参阅 使用记录。

本主题介绍了如何使用 Amazon Route 53 控制台创建、列出和删除公有托管区域。

> **Note**
>
> 您还可以使用 Route 53 私有托管区域在您通过 Amazon VPC 服务创建的一个或多个 VPCs 内路由流量。有关更多信息，请参阅 使用私有托管区。

主题

- 使用公有托管区域的注意事项
- 创建公有托管区域
- 获取公有托管区域的名称服务器

- 列出公有托管区域
- 查看公有托管区域的 DNS 查询指标
- 删除公有托管区域
- 检查来自 Route 53 的 DNS 响应
- 配置白标签名称服务器
- Amazon Route 53 为公有托管区域创建的 NS 和 SOA 记录
- 为管理公有 DNS 记录启用加速恢复

使用公有托管区域的注意事项

使用公有托管区域时，请注意以下注意事项：

NS 和 SOA 记录

创建托管区域时，Amazon Route 53 会自动为此区域创建名称服务器 (NS) 记录和授权起始点 (SOA) 记录。NS 记录会识别您提供给注册商或 DNS 服务的四个名称服务器，以便系统将 DNS 查询路由到 Route 53 名称服务器。有关 NS 和 SOA 记录的更多信息，请参阅 Amazon Route 53 为公有托管区域创建的 NS 和 SOA 记录。

拥有相同名称的多个托管区域

您可以创建具有相同名称的多个托管区域，然后为每个托管区域添加不同的记录。Route 53 会为每个托管区域分配四个名称服务器，而且每个托管区域的名称服务器各不相同。在更新注册商的名称服务器记录时，请务必为正确的托管区域 (其中包含您希望 Route 53 在响应域的查询时所使用的记录) 使用 Route 53 名称服务器。对于名称相同的其它托管区域中的记录，Route 53 从不会返回其值。

可重用的委派集

默认情况下，Route 53 会为您创建的每个托管区域分配一组唯一的四个名称服务器（统称为委托集）。如果您要创建大量的托管区域，可以通过编程方式创建可重用的委托集。(可重用的委托集在 Route 53 控制台中不可用。) 然后，可以通过编程方式创建托管区域，并为每个托管区域分配同一个可重用委托集，即相同的四个名称服务器。

可重用委托集会简化将 DNS 服务迁移到 Route 53 的过程，因为您可以指示域名注册商为所有您希望使用 Route 53 作为其 DNS 服务的域使用相同的四个名称服务器。有关更多信息，请参阅CreateReusableDelegationSet《亚马逊 Route 53 API 参考》。

创建公有托管区域

公有托管区域是一个容器，其中包含的信息说明您希望如何路由特定域（如 example.com）及其子域（acme.example.com 和 zenith.example.com）的 Internet 流量。创建托管区域后，创建记录以指定希望如何路由该域及其子域的流量。

⚠ 限制

请注意使用 Route 53 创建托管区的以下限制。

- 您只能为您有权管理的域创建托管区域。通常，这意味着您拥有该域，但您还可以为域的注册商开发应用程序。
- 您只能为域和子域创建托管区。Route 53 不支持托管顶级域（TLD），例如 `.com`。

使用 Route 53 控制台创建公有托管区域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 如果您不熟悉 Route 53，请在 DNS Management（DNS 管理）下选择 Get started（入门）。

   如果您已经在使用 Route 53，请在导航窗格中选择 Hosted zones（托管区域）。
3. 选择 Create Hosted Zone（创建托管区域）。
4. 在创建托管区域窗格中，输入希望为其路由流量的域的名称。您也可以根据需要输入注释。

   有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。
5. 对于 Type，接受 Public Hosted Zone 的默认值。
6. 选择创建。
7. 创建记录，指定您希望如何路由该域及其子域的流量。有关更多信息，请参阅 使用记录。
8. 要使用新托管区域中的记录路由域的流量，请参阅适用的主题：

   - 如果您要让 Route 53 成为向另一个域注册商注册的域的 DNS 服务，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。
   - 如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录。

获取公有托管区域的名称服务器

如果要更改用于域注册的 DNS 服务，您可以获取公有托管区域的名称服务器。有关如何更改 DNS 服务的信息，请参阅将 Amazon Route 53 作为现有域的 DNS 服务。

> **Note**
>
> 某些注册商仅允许使用 IP 地址指定名称服务器；不允许您指定完全限定的域名。如果注册商要求您使用 IP 地址，则您可以使用 dig 实用工具 (适用于 Mac、Unix 或 Linux) 或 nslookup 实用工具 (适用于 Windows) 来获取名称服务器的 IP 地址。我们很少更改名称服务器的 IP 地址；如果需要更改 IP 地址，我们会提前通知您。

使用 Route 53 控制台获取托管区域的名称服务器

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 在 Hosted zones（托管区域）页面上，选择托管区域的单选按钮（不是名称），然后选择 View details（查看详细信息）。
4. 在托管区域的详细信息页面上，选择 Hosted zone details（托管区域详细信息）。
5. 记下针对 Name servers（名称服务器）列出的四个名称。

列出公有托管区域

您可以使用 Amazon Route 53 控制台列出您使用当前 Amazon 账户创建的所有托管区域。有关如何使用 Route 53 API 列出托管区域的信息，请参阅亚马逊 Route 53 API 参考ListHostedZones中的。

使用 Route 53 控制台列出与 Amazon 账户关联的公共托管区域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。该页面显示与您当前登录的 Amazon 账户关联的托管区域列表。
3. 要筛选托管区域，请使用表顶部的搜索栏。

   搜索行为取决于托管区域是最多包含 2000 个记录，还是包含 2000 个以上记录：

最多 2,000 个托管区域

- 要显示具有特定值的记录，请单击搜索栏，在下拉列表中选择一个属性，然后输入一个值。您也可以直接在搜索栏中输入一个值，然后按 Enter 键。例如，要显示名称以 **abc** 开头的托管区域，请在搜索栏中输入该值，然后按 Enter 键。
- 要仅显示具有相同托管区域类型的托管区域，请在下拉列表中选择该类型，然后输入类型。

2,000 个以上托管区域

- 您可以根据确切的域名、所有属性和类型搜索属性。
- 使用确切的域名进行搜索，以获得更快的搜索结果。

查看公有托管区域的 DNS 查询指标

您可以查看 Route 53 对指定的公有托管区域或公有托管区域组合所响应的 DNS 查询总数。指标显示在中 CloudWatch，允许您查看图表，选择要查看的时间段，并以其他各种方式自定义指标。您还可以创建告警和配置通知，以便在指定时间段内 DNS 查询数量超过或低于指定级别时收到通知。

> **Note**
>
> Route 53 会自动向发送所有公共托管区域的 DNS 查询数量，因此您无需进行任何配置即可查看查询指标。 CloudWatch DNS 查询指标不收费。

哪些 DNS 查询计算在内？

指标仅包括 DNS 解析器转发到 Route 53 的查询。如果 DNS 解析程序已缓存对查询 (如 example.com 的负载均衡器的 IP 地址) 的响应，则解析程序将继续返回缓存的响应而不将查询转发到 Route 53，直到相应记录的 TTL 到期为止。

根据为域名 (example.com) 或子域名称 (www.example.com) 提交的 DNS 查询的数量、用户正在使用的解析程序以及记录的 TTL，DNS 查询指标可能只包含提交到 DNS 解析程序的数千个查询中的一个查询的信息。有关 DNS 的工作方式的更多信息，请参阅Amazon Route 53 如何为您的域路由流量。

托管区域的查询指标何时开始显示在 CloudWatch 中？

在您创建托管区域后，托管区域最长可能需要经过几个小时，才会显示在 CloudWatch 中。此外，您必须为托管区域中的记录提交 DNS 查询来显示数据。

指标仅适用于美国东部（弗吉尼亚北部）

要获取控制台指标，您必须将区域指定为美国东部（弗吉尼亚北部）。要使用 Amazon CLI 获取指标，您必须不指定该 Amazon 区域，或者指定`us-east-1`为区域。如果您选择任何其它区域，则 Route 53 指标将不可用。

CloudWatch DNS 查询的指标和维度

有关 DNS 查询的 CloudWatch 指标和维度的信息，请参阅使用 Amazon 监控托管区域 CloudWatch。有关 CloudWatch 指标的信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 指标。

获取有关 DNS 查询的更详细数据

要获取有关 Route 53 响应的每个 DNS 查询的更多详细信息，包括以下值，可以配置查询日志记录：

- 请求的域名或子域名
- 请求的日期和时间
- DNS 记录类型（例如 A 或 AAAA）
- 响应 DNS 查询的 53 号路边缘站点
- DNS 响应代码，例如 `NoError` 或 `ServFail`

有关更多信息，请参阅 公有 DNS 查询日志记录。

如何获取 DNS 查询指标

在您创建托管区域后不久，Amazon Route 53 开始每分钟向发送一次指标和维度 CloudWatch。您可以使用以下过程在 CloudWatch 控制台上查看指标或使用 Amazon Command Line Interface (Amazon CLI) 查看这些指标。

主题

- 在 CloudWatch 控制台中查看公共托管区域的 DNS 查询指标
- 使用获取 DNS 查询指标 Amazon CLI

在 CloudWatch 控制台中查看公共托管区域的 DNS 查询指标

要在 CloudWatch 控制台中查看公共托管区域的 DNS 查询指标，请执行以下步骤。

在 CloudWatch 控制台上查看公共托管区域的 DNS 查询指标

1. 登录 Amazon Web Services 管理控制台 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 在控制台右上角的 Amazon 区域列表中，选择美国东部（弗吉尼亚北部）。如果您选择任何其他 Amazon 区域，则 Route 53 指标不可用。
4. 在 All metrics (所有指标) 选项卡上，选择 Route 53。
5. 选择 Hosted Zone Metrics (托管区域指标)。
6. 选中一个或多个具有指标名称的托管区域的复选框DNSQueries。
7. 在 Graphed metrics (图形化指标) 选项卡上，更改适用的值以查看所需格式的指标。

   对于统计数据，选择求和或 SampleCount；这两个统计数据都显示相同的值。

使用获取 DNS 查询指标 Amazon CLI

要使用获取 DNS 查询指标 Amazon CLI，请使用get-metric-data命令。注意以下几点：

- 您可以在单独的 JSON 文件中为命令指定大多数值。有关更多信息，请参阅 get-metric-data。
- 该命令为您在 JSON 文件中为 `Period` 指定的每个间隔返回一个值。`Period` 以秒为单位，因此，如果指定五分钟的时间段并为 `Period` 指定 `60`，则会得到五个值。如果您指定一个五分钟的时间段，并为 `Period` 指定 `300`，则会得到一个值。
- 在 JSON 文件中，您可以为 `Id` 指定任何值。
- 要么不指定 Amazon 区域，要么指定`us-east-1`为区域。如果您选择任何其它区域，则 Route 53 指标将不可用。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的配置 Amazon CLI。

以下是你用来获取 2019 年 5 月 1 日 4:01 到 4:07 之间五分钟时间段的 DNS 查询指标的 Amazon CLI 命令。`metric-data-queries` 参数引用命令后面的示例 JSON 文件。

```
aws cloudwatch get-metric-data --metric-data-queries file://./metric.json --start-time
 2019-05-01T04:01:00Z --end-time 2019-05-01T04:07:00Z
```

下面是示例 JSON 文件：

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

下面是此命令的输出。注意以下几点：

- 命令中的开始时间和结束时间涵盖了七分钟的时间段，从 2019-05-01T04:01:00Z 到 2019-05-01T04:07:00Z。
- 只有 6 个返回值。2019-05-01T04:05:00Z 没有值，因为该分钟内没有任何 DNS 查询。
- JSON 文件中指定的 Period 值为 60（秒），因此以一分钟为间隔报告值。

```
{
    "MetricDataResults": [
        {
            "Id": "my_dns_queries_id",
            "StatusCode": "Complete",
            "Label": "DNSQueries",
            "Values": [
                101.0,
                115.0,
                103.0,
                127.0,
```

```
                111.0,
                120.0
            ],
            "Timestamps": [
                "2019-05-01T04:07:00Z",
                "2019-05-01T04:06:00Z",
                "2019-05-01T04:04:00Z",
                "2019-05-01T04:03:00Z",
                "2019-05-01T04:02:00Z",
                "2019-05-01T04:01:00Z"
            ]
        }
    ]
}
```

删除公有托管区域

本节介绍了如何使用 Amazon Route 53 控制台删除公有托管区域。

只有在没有任何记录 (默认 SOA 和 NS 记录除外) 时，您才可以删除托管区域。如果您的托管区域包含其他记录，则必须先将其删除，然后才能删除托管区域。这样可以防止您意外删除仍包含记录的托管区域。

主题

- 防止流量路由到您的域
- 删除由其他服务创建的公有托管区域
- 使用 Route 53 控制台删除公有托管区域

防止流量路由到您的域

如果您希望保留域注册但又希望停止路由指向您网站或 Web 应用程序的 Internet 流量，我们建议您删除托管区域中的记录 而不是删除托管区域。

> **Important**
>
> 如果您删除托管区域，则无法取消删除它。您必须创建新的托管区域并更新域注册的名称服务器，这最多需要 48 个小时生效。此外，如果您删除托管区域，其他人可以劫持域并使用您的域名将流量路由到他们自己的资源。
> 如果您将子域的责任委托给托管区域，并且要删除子托管区域，则还必须通过删除与子托管区域同名的 NS 记录来更新父托管区域。例如，如果要删除托管区域 acme.example.com，则还

必须删除 example.com 托管区域中的 NS 记录 acme.example.com。我们建议您先删除 NS 记录，并等待 NS 记录上的 TTL 持续时间，然后再删除子托管区域。这可确保在 DNS 解析程序仍然缓存子托管区域的名称服务器期间，某人不能劫持子托管区域。

如果您要避免托管区域的每月费用，可以将域的 DNS 服务转移到免费 DNS 服务。在转移 DNS 服务时，您需要更新域注册的名称服务器。如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录，了解有关如何将 Route 53 名称服务器替换为新 DNS 服务的名称服务器的信息。如果此域已向其他注册商注册，请使用注册商提供的方法更新此域注册的名称服务器。有关更多信息，请在 Internet 上搜索“免费 DNS 服务”。

删除由其他服务创建的公有托管区域

如果其它服务创建了一个托管区域，您无法使用 Route 53 控制台删除它。相反，您需要使用针对其他服务的合适过程：

- Amazon Cloud Map— 要删除在创建公有 DNS 命名空间时 Amazon Cloud Map 创建的托管区域，请删除该命名空间。 Amazon Cloud Map 自动删除托管区域。有关更多信息，请参阅 Amazon Cloud Map 开发人员指南中的删除命名空间。
- Amazon Elastic Container Service (Amazon ECS) 服务发现 — 要删除 Amazon ECS 在您使用服务发现创建服务时创建的公有托管区域，请删除使用该命名空间的 Amazon ECS 服务，并删除该命名空间。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的删除服务。

使用 Route 53 控制台删除公有托管区域

要使用 Route 53 控制台删除公有托管区域，请执行以下过程。

要使用 Route 53 控制台删除公有托管区域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择要删除的托管区域的突出显示的链接。
3. 确认您要删除的托管区域仅包含 NS 和 SOA 记录。如果它包含其它记录，请将其删除。此外，您还需要禁用 DNSSEC 签名：

> **Note**
>
> 如果您在未完成以下要求的情况下尝试删除托管区，Route 53 将返回错误：
>
> - 如果启用 DNSSEC 签名：指定的托管区包含 DNSSEC 密钥签名密钥，因此无法删除
> - 如果存在其他资源记录集（默认 SOA 和 NS 记录除外）：指定的托管区包含非必需的资源记录集，因此无法删除

- 在托管区域详细信息页面的 Records（记录）列表中，如果记录列表内任何记录对应的 Type（类型）列值不是 NS 或 SOA，请选择此行，然后选择 Delete（删除）。

  要选择多个连续的记录，请选择第一行，按住 Shift 键，然后选择最后一行。要选择多个不连续的记录，请选择第一行，按住 Ctrl 键，然后选择其余各行。

  > **Note**
  >
  > 如果您为子域的托管区域创建了任何 NS 记录，请也删除此类记录。

4. 返回到 Hosted Zones（托管区域）页面，然后选择您要删除的托管区域所对应的那一行。
5. 选择删除。
6. 键入确认密钥，然后选择 Delete（删除）。
7. 如果您想要使域在互联网上不可用，我们建议您将 DNS 服务转移到免费的 DNS 服务，然后删除 Route 53 托管区域。这可防止以后的 DNS 查询可能被错误路由。

   如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录，了解有关如何将 Route 53 名称服务器替换为新 DNS 服务的名称服务器的信息。如果此域已向其他注册商注册，请使用注册商提供的方法更改此域的名称服务器。

   > **Note**
   >
   > 如果您要删除子域 (acme.example.com) 的托管区域，则不需要更改域 (example.com) 的名称服务器。

检查来自 Route 53 的 DNS 响应

如果您为域创建了 Amazon Route 53 托管区域，则可以使用控制台中的 DNS 检查工具，查看在您配置域以将 Route 53 用作 DNS 服务时 Route 53 会如何响应 DNS 查询。对于地理位置、地理位置和延迟记录，您还可以模拟来自特定 DNS 解析器 and/or 客户端 IP 地址的查询，以了解 Route 53 将返回什么响应。

> **Important**
>
> 该工具不会向域名系统提交查询，只会根据托管区域中的记录中的设置做出响应。无论托管区当前是否用于路由域的流量，该工具都会返回相同的信息。

DNS 检查工具仅适用于公有托管区域。

> **Note**
>
> DNS 检查工具返回的信息与您期望从 `dig` 命令的答案部分得到的信息类似。因此，如果您查询子域中指向父名称服务器的名称服务器，则不会返回这些名称服务器。

主题

使用检查工具查看 Amazon Route 53 如何响应 DNS 查询

您可以使用此工具查看 Amazon Route 53 为响应记录的 DNS 查询而返回的响应。

使用此检查工具查看 Route 53 如何响应 DNS 查询

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区。
3. 在 Hosted Zones 页面上，选择托管区域的名称。控制台会显示此托管区域的记录列表。
4. 要直接转到 Check response from Route 53（查看来自 Route 53 的响应）页面，请选择 Test record（测试记录）。
5. 指定以下值：

- 记录的名称，其中不包括托管区域的名称。例如，要检查 www.example.com，请输入 www。要检查 example.com，请将记录名称字段留空。
- 要检查的记录的类型，例如 A 或 CNAME（别名记录）。

6. 选择 Get Response。
7. Response returned by Route 53 部分包括以下值：

   DNS 响应代码

   此类代码表示查询是否有效。最常见的响应代码是 NOERROR，表示查询有效。如果响应无效，则 Route 53 会返回响应代码，该代码可解释无效的原因。有关可能的响应代码列表，请查看 IANA 网站上的 DNS RCODES。

   协议

   Amazon Route 53 使用此类协议 (UDP 或 TCP) 来响应查询。

   Route 53 返回的响应

   Route 53 会将此类值返回给 Web 应用程序。此类值可以是以下任一项：

   - 对于非别名记录，响应会包含此类值或记录中的值。
   - 对于具有相同名称和类型 (包括加权、延迟、地理位置和故障转移) 的多个记录，响应会根据请求包含相应记录的值。
   - 对于引用其他记录以外的 Amazon 资源的别名记录，响应包含 Amazon 资源的 IP 地址或域名，具体取决于资源的类型。
   - 对于引用其他记录的别名记录，响应会包含此类值或引用的记录的值。

使用检查工具模拟来自特定 IP 地址的查询（仅限于地理位置和延迟记录）

如果您创建了延迟或地理位置记录，则可以使用检查工具模拟来自 DNS 解析程序和客户端 IP 地址的查询。

使用检查工具模拟来自指定 IP 地址的查询

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区。
3. 在 Hosted Zones 页面上，选择托管区域的名称。控制台会显示此托管区域的记录列表。
4. 要直接转到 Check response from Route 53 页面，请选择 Test record set。

要转到特定记录的 Check response from Route 53 (检查来自 Route 53 的响应) 页面，请选中此记录对应的复选框，然后选择 Test record set (测试记录集)。

5. 如果您选择测试记录集而不先选择记录，请指定以下值：

   - 记录的名称，其中不包括托管区域的名称。例如，要检查 www.example.com，请输入 www。要检查 example.com，请将记录名称字段留空。
   - 要检查的记录的类型，例如 A 或 CNAME（别名记录）。

6. 指定适用的值：

   解析程序 IP 地址

   指定 IPv4 或 IPv6 地址以模拟客户端用于发出请求的 DNS 解析器的位置。这对于测试延迟和地理位置记录非常有用。如果省略此值，则该工具将使用 Amazon 美国东部（弗吉尼亚北部）区域 (us-east-1) 中 DNS 解析器的 IP 地址。

   EDNS0 客户端子网 IP

   如果解析器支持 EDNS0，请输入适用地理位置中 IP 地址对应的客户端子网 IP，例如，192.0.2.0 或 2001:db8:85a3::8a2e:370:7334。

   子网掩码

   如果您指定 EDNS0 client subnet IP 的 IP 地址，则可以选择指定您希望检查工具纳入 DNS 查询的 IP 地址的位数。例如，如果您分别为 EDNS0 client subnet IP（EDNS0 客户端子网 IP）和 Subnet mask（子网掩码）指定了 192.0.2.44 与 24，则检查工具会模拟来自 192.0.2.0/24 的查询。地址的默认值为 24 位， IPv4 地址的默认值为 IPv6 64 位。

7. 选择 Get Response。

8. Response returned by Route 53 部分包括以下值：

   发送到 Route 53 的 DNS 查询

   此类查询采用 BIND 格式，由检查工具将其发送到 Route 53。这种格式与 Web 应用程序在发送查询时所用的格式相同。通常，三个值分别表示记录的名称、IN (即 Internet) 和记录的类型。

   DNS 响应代码

   此类代码表示查询是否有效。最常见的响应代码是 NOERROR，表示查询有效。如果响应无效，则 Route 53 会返回响应代码，该代码可解释无效的原因。有关可能的响应代码列表，请查看 IANA 网站上的 DNS RCODES。

协议

Amazon Route 53 使用此类协议 (UDP 或 TCP) 来响应查询。

Route 53 返回的响应

Route 53 会将此类值返回给 Web 应用程序。此类值可以是以下任一项：

- 对于非别名记录，响应会包含此类值或记录中的值。
- 对于具有相同名称和类型 (包括加权、延迟、地理位置和故障转移) 的多个记录，响应会根据请求包含相应记录的值。
- 对于引用其他记录以外的 Amazon 资源的别名记录，响应包含 Amazon 资源的 IP 地址或域名，具体取决于资源的类型。
- 对于引用其他记录的别名记录，响应会包含此类值或引用的记录的值。

配置白标签名称服务器

每个 Amazon Route 53 托管区域都与四个名称服务器 (统称为委托集) 关联。默认情况下，名称服务器具有如 ns-2048.awsdns-64.com 的名称。如果您希望名称服务器的域名与托管区域的域名相同（例如 ns1.example.com），则可以配置白标签名称服务器，也称为虚名称服务器或私有名称服务器。

以下步骤说明了如何配置一组四个白标签名称服务器，供您为多个域重用。例如，假设您拥有 example.com、example.org 和 example.net 这三个域。通过以下步骤，您可以为 example.com 配置白标签名称服务器，然后为 example.org 和 example.net 重用此类服务器。

主题

步骤 1：创建 Route 53 可重用委托集

白标签名称服务器与 Route 53 可重用的委派集相关联。只有托管区域和可重复使用的委托集是由同一个 Amazon 账户创建的，您才能为托管区域使用白标域名服务器。

要创建可重复使用的委托集，您可以使用 Route 53 AP Amazon I、CLI 或其中一个 Amazon SDKs。有关更多信息，请参阅以下文档：

- Route 53 API — 参见CreateReusableDelegationSet亚马逊 Route 53 API 参考
- Amazon CLI — 参见create-reusable-delegation-set《Amazon CLI 命令参考》
- Amazon SDKs请参阅 “文档” 页面上相应的 SDK Amazon 文档

步骤 2：创建或重新创建 Amazon Route 53 托管区域并更改 NS 和 SOA 记录的 TTL

创建或重新创建 Amazon Route 53 托管区域：

- 如果您当前未将 Route 53 用作您要使用白标签名称服务器的域的 DNS 服务 — 请创建托管区域，并指定您在上一步为每个托管区域创建的可重用委托集。有关更多信息，请参阅CreateHostedZone《亚马逊 Route 53 API 参考》。
- 如果您将 Route 53 用作您要使用白标签名称服务器的域的 DNS 服务 — 则必须重新创建您要使用白标签名称服务器的托管区域，并指定您在上一步为每个托管区域创建的可重用委托集。

> **Important**
>
> 您无法更改与现有托管区域关联的名称服务器。您只能在创建托管区域时，才可将一个可重用委托集与托管区域相关联。

在您创建托管区域时，并在尝试访问对应域的资源之前，更改每个托管区域的以下 TTL 值：

- 将托管区域的 NS 记录对应的 TTL 值更改为 60 秒或更低。
- 将托管区域的 SOA 记录对应的 TTL 下限值更改为 60 秒或更低。这是 SOA 记录中的最后一个值。

如果您不小心向注册商提供了白标签名称服务器的错误 IP 地址，则您的网站将变得无法访问，并且在您更正这个问题之后的 TTL 持续时间内仍然无法访问。通过设置较低的 TTL，您可以缩短网站不可用的持续时间。

有关创建托管区域以及为托管区域的名称服务器指定可重复使用的委托集的更多信息，请参阅 Amazon Route 53 API 参考CreateHostedZone中的。

步骤 3：重新创建托管区域的记录

在您于步骤 2 中创建的托管区域中创建记录：

- 如果您要将域的 DNS 服务迁移到 Amazon Route 53 – 则可通过导入现有记录的相关信息，创建记录。有关更多信息，请参阅 通过导入区域文件来创建记录。
- 如果您要替换现有托管区域以便使用白标签名称服务器 — 请在新的托管区域中，重新创建当前托管区域中显示的记录。Route 53 不提供从托管区域导出记录的方法，但一些第三方供应商提供。然后，您可以使用 Route 53 导入功能，导入路由策略为“简便”的非别名记录。您无法导出然后重新导入路由策略不为“简便”的别名记录或记录。

  有关使用 Route 53 API 创建记录的信息，请参阅亚马逊 Route 53 API 参考CreateHostedZone中的。有关使用 Route 53 控制台创建记录的信息，请参阅 使用记录。

步骤 4：获取 IP 地址

获取可重复使用的委托集中域名服务器的 IPv4 和 IPv6 地址，然后填写下表。

可重用委托集中名称服务器的名称（示例：Ns-2048.awsdns-64.com）	IPv4 和 IPv6 地址	您要分配给白标签名称服务器的名称（示例：ns1.example.com）
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

例如，假设可重用委托集的四个名称服务器为：

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

下方显示的是 Linux 和 Windows 命令 (您可通过运行此类命令获取四个名称服务器中第一个服务器的 IP 地址)：

适用于 Linux 的 dig 命令

```
% dig A ns-2048.awsdns-64.com +short
192.0.2.117
```

```
% dig AAAA ns-2048.awsdns-64.com +short
2001:db8:85a3::8a2e:370:7334
```

适用于 Windows 的 nslookup 命令

```
c:\> nslookup ns-2048.awsdns-64.com
Non-authoritative answer:
Name:    ns-2048.awsdns-64.com
Addresses:  2001:db8:85a3::8a2e:370:7334
          192.0.2.117
```

步骤 5：为白标签名称服务器创建记录

在域名（如 example.com）与白标签名称服务器（如 ns1.example.com）的域名相同的托管区域中，创建八个记录：

- 每个白标签名称服务器一个 A 记录
- 每个白标签名称服务器一个 AAAA 记录

> **Important**
>
> 如果您为两个或更多托管区域使用相同的白标签名称服务器，请勿针对其他托管区域执行此步操作。

为每个记录指定以下值。请根据您在上一步所填写的表格，指定相应值：

路由策略

指定 Simple routing（简单路由）。

记录名称

您要分配给其中一个白标签名称服务器的名称，例如，ns1.example.com。对于前缀 (即本示例中的 ns1)，您可以使用域名中有效的任何值。

值/流量路由至

您的可重复使用的委托集中其中一个 Route 53 域名服务器的 IPv4 或 IPv6 地址。

> **Important**
>
> 如果您在为白标签名称服务器创建记录时指定了错误的 IP 地址，则当您执行后续步骤时，将无法通过 Internet 访问网站或 Web 应用程序。即使您立即更正 IP 地址，您的网站或 Web 应用程序在 TTL 持续时间内也仍然无法访问。

记录类型

在为IPv4 地址创建记录时指定 A。

在创建IPv6 地址记录时指定 AAAA。

TTL (秒)

此值表示 DNS 解析程序在将其它 DNS 查询转发给 Route 53 之前缓存此记录中信息所用的时间量。我们建议您指定 60 秒或更短的初始值，这样，当您不小心在此类记录中指定了错误值时，可以快速恢复。

步骤 6：更新 NS 和 SOA 记录

在您要使用白标签名称服务器的托管区域中更新 SOA 和 NS 记录。每次针对一个托管区域和对应的域执行步骤 6 到步骤 8，然后对另一个托管区域和域重复这些步骤。

> **Important**
>
> 先从域名（如 example.com）与白标签名称服务器（如 ns1.example.com）的域名相同的 Amazon Route 53 托管区域开始。

1. 将 Route 53 名称服务器的名称替换为其中一个白标签名称服务器的名称，以更新 SOA 记录

   示例

   将 Route 53 名称服务器的名称替换为：

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   替换为其中一个白标签名称服务器的名称：

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > 您在步骤 2：创建或重新创建 Amazon Route 53 托管区域并更改 NS 和 SOA 记录的 TTL 中更改了最后一个值，即存续时间 (TTL)。

   有关使用 Route 53 控制台更新记录的信息，请参阅 编辑记录。
2. 在 NS 记录中，记下域对应的当前名称服务器的名称，以便在必要时恢复为此类名称服务器。
3. 更新 NS 记录。将 Route 53 名称服务器的名称替换为四个白标签名称服务器的名称，例如 `ns1.example.com`、`ns2.example.com`、`ns3.example.com` 和 `ns4.example.com`。

步骤 7：创建粘附记录和更改注册商的名称服务器

使用注册商提供的方法来创建粘附记录并更改注册商的名称服务器：

1. 添加粘附记录：

- 如果您要更新域名与白标签名称服务器的域名相同的域 — 请创建名称和 IP 地址与您在步骤 4 获取的值一致的四个粘附记录。在相应的粘合记录中同时包含白标域名服务器的IPv4 和 IPv6 地址，例如：

  ns1.example.com — IP 地址 = 192.0.2.117 和 2001:db8:85a3::8a2e:370:7334

  注册商会对粘附记录使用各种不同的术语。您可能还会看到有些地方将其称为注册新名称服务器或类似内容。

- 如果您要更新其他域 – 如果 Route 53 是您的 DNS 服务，则必须先完成上一个项目符号中的步骤，然后创建与域名匹配的粘附记录。然后，跳到本过程的步骤 2。

2. 将域对应的名称服务器更改为白标签名称服务器的名称。

如果您要将 Amazon Route 53 用作 DNS 服务，请参阅 为域添加或更改名称服务器和粘附记录。

步骤 8：监控网站或应用程序的流量

监控您在步骤 7 中创建粘附记录和更改名称服务器的网站或应用程序的流量：

- 如果流量停止 — 请使用注册商提供的方法，将相应域对应的名称服务器改回之前的 Route 53 名称服务器。这些是您在步骤 6b 中记下的名称服务器。然后，确定出错的位置。
- 如果流量未受影响 — 请针对您要使用相同白标签名称服务器的其余托管区域，重复执行步骤 6 到步骤 8 操作。

第 9 步：更改 TTLs 回其原始值

对于当前使用白标签名称服务器的所有托管区域，更改以下值：

- 将托管区域的 NS 记录对应的 TTL 值更改为较典型的 NS 记录值，例如，172800 秒 (即两天)。
- 将托管区域的 SOA 记录对应的 TTL 下限值更改为较典型的 SOA 记录值，例如，900 秒。这是 SOA 记录中的最后一个值。

步骤 10：（可选）联系递归 DNS 服务

可选如果您使用的是 Amazon Route 53 地理定位路由，请联系支持 EDNS0 edns-client-subnet 扩展的递归 DNS 服务，并向他们提供您的白标域名服务器的名称。这样可确保这些 DNS 服务会根据查询的大致来源地理位置，继续将 DNS 查询路由到最佳 Route 53 位置。

Amazon Route 53 为公有托管区域创建的 NS 和 SOA 记录

Amazon Route 53 会自动为您创建的每个公有托管区域创建名称服务器 (NS) 记录和授权起始点 (SOA) 记录。您很少需要更改这些记录。

主题

名称服务器 (NS) 记录

Amazon Route 53 会自动创建名称与托管区域名称相同的名称服务器 (NS) 记录。它列出的四个名称服务器是托管区域的权威名称服务器。除了极少数情况外，我们建议您不要在此记录中添加、更改或删除名称服务器。

下面的示例展示了 Route 53 名称服务器的名称格式（这些仅为示例；请勿在您更新注册商的名称服务器记录时使用）：

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

要获取托管区域的名称服务器列表，请执行以下操作：

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 在 Hosted zones（托管区域）页面上，选择托管区域的单选按钮（不是名称），然后选择 View details（查看详细信息）。
4. 在托管区域的详细信息页面上，选择 Hosted zone details（托管区域详细信息）。
5. 记下针对 Name servers（名称服务器）列出的四个名称。

有关将 DNS 服务从另一个 DNS 服务提供商迁移到 Route 53 的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

授权起始点 (SOA) 记录

授权起始点 (SOA) 记录可识别有关域的基本 DNS 信息，例如：

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

SOA 记录包含以下元素：

- 创建了 SOA 记录的 Route 53 名称服务器，例如，`ns-2048.awsdns-64.net`。
- 管理员的电子邮件地址。将 @ 符号替换为句点，例如，`hostmaster.example.com`。默认值是不受监控的 amazon.com 电子邮件地址。
- 一个序列号，您可以选择在更新托管区域中的记录时递增它。Route 53 不会自动递增序列号。（序列号由支持辅助 DNS 的 DNS 服务使用。）在示例中，此值为 1。
- 辅助 DNS 服务器在查询主 DNS 服务器的 SOA 记录以检查更改之前等待的刷新时间（以秒为单位）。在示例中，此值为 `7200`。
- 辅助服务器在重试失败区域转移之前等待的重试时间间隔（以秒为单位）。通常，重试时间小于刷新时间。在示例中，此值为 `900`（15 分钟）。
- 以秒为单位的时间，在此之前，辅助服务器会一直尝试完成区域转移。如果在成功转移区域之前此时间结束，辅助服务器将停止响应查询，因为它认为其数据过于陈旧，不可靠。在示例中，此值为 `1209600`（两周）。
- 最短存续时间 (TTL)。此值有助于定义递归解析器应缓存来自 Route 53: 的以下响应的时间长度：

  NXDOMAIN

  > 没有任何类型的记录具有在 DNS 查询中指定的名称，例如 example.com。也没有任何记录是在 DNS 查询中指定的名称的子级，例如 zenith.example.com。

  NODATA

  > 至少有一条记录具有在 DNS 查询中指定的名称，但这些记录均不具有在 DNS 查询中指定的类型（例如 A）。

  当 DNS 解析程序缓存 NXDOMAIN 或 NODATA 响应时，这称为逆向缓存。

  逆向缓存的持续时间是以下值中的较小值：

  - 此值 — SOA 记录中的最短 TTL。在示例中，此值为 `86400`（一天）。
  - SOA 记录的 TTL 的值。默认值为 900 秒。有关更改此值的信息，请参阅编辑记录。

当 Route 53 使用 NXDOMAIN 或 NODATA 响应（负面响应）响应 DNS 查询时，将向您收取标准查询的费用。（请参阅 Amazon Route 53 定价中的“查询”）如果您担心负面响应的成本，一种选择是更改 SOA 记录的 TTL、SOA 记录中的最小 TTL（此值），或同时更改两者。请注意，增加这些 TTLs值（适用于整个托管区域的负面响应）可能会产生正面和负面影响：

- 互联网上的 DNS 解析器会将记录的不存在状态缓存更长时间，从而减少了转发到 Route 53 的查询的数量。这可以减少 DNS 查询的 Route 53 费用。
- 但是，如果您错误地删除了有效的记录，然后重新创建该记录，DNS 解析器将缓存负面响应（此记录不存在）达更长时间。这会延长您的客户或用户无法访问相应资源的时间，例如 acme.example.com 的 Web 服务器。

在 Route 53 中查找 SOA 记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要查看其记录的域的链接名称。
4. 在 Records（记录）部分，您可以看到列出的所有记录，还可以筛选记录以查找您的 SOA 值。

为管理公有 DNS 记录启用加速恢复

Route 53 用于管理公有 DNS 记录的加速恢复旨在在美国东部（弗吉尼亚北部）地区出现服务不可用时实现 60 分钟的恢复时间目标 (RTO)。在 Route 53 公共托管区域上启用后，在 Amazon 检测到美国东部（弗吉尼亚北部）区域的运营受损后，您将能够在大约 60 分钟内恢复对公共托管区域中的 DNS 记录进行更改。

> **Important**
>
> 加速恢复仅适用于公共托管区域。不支持私有托管区域。

> **Note**
>
> 在区域服务受损期间，来自 Route 53 数据平面的 DNS 查询解析继续正常工作。有关数据平面与控制平面操作的理解，请参阅 Route 53 中的弹性。

主题

加速恢复公共 DNS 记录的工作原理

启用加速恢复后，Route 53 将在美国西部（俄勒冈）地区维护您的公共托管区域的副本。如果美国东部（弗吉尼亚北部）地区的服务长时间不可用，Route 53 将在 60 分钟内执行故障转移，自动将支持加速恢复的公共托管区域的控制平面操作重定向到美国西部（俄勒冈）区域。然后，您可以继续通过 CLI、SDK 和 API 以编程方式更改 DNS。请注意，故障转移期间将提供有限的 API 方法。有关更多详细信息，请参阅 “其他注意事项” 部分。当该区域恢复时，Route 53 将执行故障恢复程序，自动将控制飞机操作定向回美国东部（弗吉尼亚北部）区域。

> **Note**
>
> 在美国东部（弗吉尼亚北部）区域受到任何损害之前，您必须先启用加速恢复，以管理公共托管区域上的公有 DNS 记录。这可以通过控制台、CLI、SDK 或 API 来完成（参见下方本页标题为 “如何为管理公共 DNS 记录启用加速恢复” 的部分）。故障转移发生后，您无法启用加速恢复来管理公有 DNS 记录。

故障转移后重新提交 DNS 更改

在正常情况下，美国东部（弗吉尼亚北部）地区将接受对启用加速恢复的公共托管区域所做的更改，然后成功复制到美国西部（俄勒冈）区域。但是，当美国东部（弗吉尼亚北部）地区发生服务中断时，美国东部（弗吉尼亚北部）地区可能会接受某些更改，但可能不会复制到美国西部（俄勒冈）区域。这些飞行中的变更被称为 “搁浅变更”。故障转移完成后，Route 53 建议您在恢复 DNS 工作流程之前重新提交搁置的更改。您可以通过使用 API 或使用来实现此目的 Amazon CloudFormation，如下所述。

使用 API 跟踪和提交 DNS 更改

如果您使用 Route 53 AP Amazon I、CLI 或 Amazon SDKs 来管理 DNS 记录，则需要分别使用 ChangeResourceRecordSets API 和 GetChange API 来提交和跟踪 DNS 更改。

当您使用 ChangeResourceRecordSets API 更改 DNS 时，Route 53 会返回您所做更改的标识符 (ID)（ChangeInfo有关更改响应对象的详细信息，请参阅）。您可以在随后向 GetChange API 发出的请求中提供此 ID，并观察变更的状态。状态为 INSYNC 的 DNS 更改已复制到美国西部（俄勒冈）区域，并传播到所有 Route 53 DNS 服务器。在故障转移之前或之后，您无需对这些更改采取进一步的操作。但是，在美国东部（弗吉尼亚北部）地区减值期间， GetChange 可能会返回 “待定”，这表明您的更改可能尚未复制到美国西部（俄勒冈）地区。如果是这样的话，当故障转移完成时， GetChange 将返回 NoSuchChange，表示 Route 53 无法复制此 DNS 更改。因此，在故障转移之后，您可以放心地忽略这些搁浅的 DNS 更改，然后将其作为新的 DNS 更改重新提交。当 Route 53 向 Healt Amazon h Dashboard 发布消息时，您将知道故障转移过程已完成。

Amazon CloudFormation 用于跟踪和提交更改

Amazon CloudFormation 使用 GetChange API 自动跟踪 DNS 更改的复制状态，并且只有在 DNS 更改被确认为不同步后才完成更新。如果您使用 CloudFormation 管理 DNS 记录，但美国东部（弗吉尼亚北部）区域不可用，则在不可用期间，您使用的操作 CloudFormation 将无法成功完成。但是，在 Route 53 故障转移过程完成后，您只需重试相同的操作即可重新提交 DNS 更改。 CloudFormation

故障恢复到美国东部（弗吉尼亚北部）区域

区域恢复后，Route 53 会将您的公共托管区域的控制飞机运营恢复到美国东部（弗吉尼亚北部）区域。在故障恢复期间，您无需重新提交 DNS 更改，因为在此过程中不会引入任何搁置的更改。

其他注意事项

还有一些与加速恢复功能相关的注意事项需要注意：

1. 在故障转移期间，您将无法创建新的托管区域、删除现有托管区域、启用 DNSSEC 签名或禁用 DNSSEC 签名。
2. Amazon PrivateLink 故障转移后连接将无法正常工作，但在故障恢复到美国东部（弗吉尼亚北部）地区后连接将再次正常工作。
3. CloudFront 目前不支持@@ 统一费率计划。
4. 无法删除启用了加速恢复功能的托管区域。在尝试删除托管区域之前，必须禁用加速恢复。
5. 在故障转移期间，启用了加速恢复的公共托管区域将继续支持以下 API 方法。但是，在故障恢复发生之前，所有其他 Route 53 API 方法都无法运行。
   - `ChangeResourceRecordSets`
   - `GetChange`
   - `GetGeoLocation`
   - `GetHostedZone`

- GetHostedZoneCount
- GetHostedZoneLimit
- GetReusableDelegationSet
- GetReusableDelegationSetLimit
- ListGeoLocations
- ListHostedZones
- ListHostedZonesByName
- ListResourceRecordSets
- ListReusableDelegationSets

如何为管理公有 DNS 记录启用加速恢复

您可以使用 Route 53 控制台、API、CLI 或 SDK 启用加速恢复以管理公有 DNS 记录。启用加速恢复所需的时间将取决于您的公共托管区域的大小和其他因素。您应该计划启用加速恢复的过程最多需要几个小时。您可以在公共托管区域的加速恢复选项卡中或通过 GetHostedZone API 查看启用过程的状态。流程最终确定后，将有一段短暂的时间不接受 DNS 更改，最长持续几分钟。完成后，DNS 更改可以照常进行。

使用 Route 53 控制台启用和禁用加速恢复

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要为其启用加速恢复功能的公共托管区域。
4. 在 “加速恢复” 选项卡中，选择 “启用”。
5. 选择保存更改。
6. 监控托管区域的状态。状态显示在安装过程中启用加速恢复，完成后更改为 “启用”。

您可以使用上述相同步骤禁用加速恢复，但可以选择 “禁用”。

要启用的 CLI 示例

```
aws route53 update-hosted-zone-features --enable-accelerated-recovery --hosted-zone-id
 Z123456789
```

要禁用的 CLI 示例

```
aws route53 update-hosted-zone-features --no-enable-accelerated-recovery --hosted-zone-
id Z123456789
```

使用私有托管区

私有托管区域是一个容器，其中包含有关您希望 Amazon Route 53 如何响应您使用 Amazon VPC 服务创建的一个或多个 VPCs 域中的域及其子域的 DNS 查询的信息。下面是私有托管区域的工作原理：

1. 先创建私有托管区（例如 example.com），并指定要与该托管区关联的 VPC。创建托管区域后，您可以 VPCs 与其关联更多内容。
2. 您在托管区域中创建记录，以确定 Route 53 如何响应您的域名以及您内部和之间的子域名的 DNS 查询。 VPCs例如，假设您的数据库服务器在 VPC 中与您的私有托管区域关联的 EC2 实例上运行。您创建 A 或 AAAA 记录（如 db.example.com），并指定数据库服务器的 IP 地址。

   有关记录的更多信息，请参阅 使用记录。有关使用私有托管区域的 Amazon VPC 要求的信息，请参阅 Amazon VPC 用户指南中的使用私有托管区域。
3. 当应用程序提交 db.example.com 的 DNS 查询时，Route 53 会返回相应的 IP 地址。要从私有托管区域获得答案，您还必须在其中一个关联的托管区域中运行EC2 实例 VPCs （或者拥有来自混合设置的入站终端节点）。如果您尝试从外部 VPCs 或混合设置中查询私有托管区域，则查询将在互联网上以递归方式解析。
4. 应用程序使用从 Route 53 获得的 IP 地址与数据库服务器建立连接。

创建私有托管区时，将使用以下名称服务器：

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

使用这些名称服务器是因为 DNS 协议要求每个托管区都必须具有 NS 记录集。这些名称服务器属于保留的服务器，Route 53 公有托管区不得使用。在已与托管区域关联的 VPC 中，您只能使用连接到私有托管区域中 VPCs 指定区域的入站终端节点，通过 VPC 解析器查询这些区域。

虽然域名服务器在互联网上可见，但 VPC Resolver 无法连接到域名服务器地址。此外，如果您通过互联网直接查询名称服务器，不会返回私有托管区信息。相反，VPC 解析器检测到查询位于基于 VPC 与托管区域关联的私有命名空间内，并使用直接的私有连接来访问私有 DNS 服务器。

> **Note**
>
> 如果需要，您可以更改私有托管区中的 NS 记录集，私有 DNS 解析仍然有效。我们不建议这种做法，但如果您选择这样做，则应使用公有 DNS 服务器不使用的预留域名。

如果希望路由您的域的互联网流量，可使用 Route 53 公有托管区域。有关更多信息，请参阅 使用公有托管区。

主题

使用私有托管区域的注意事项

使用私有托管区域时请注意以下事项：

- Amazon VPC settings
- Route 53 health checks
- Supported routing policies for records in a private hosted zone
- Split-view DNS
- Public and private hosted zones that have overlapping namespaces
- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 VPC Resolver rules
- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Amazon VPC 设置

要使用私有托管区域，您必须将以下 Amazon VPC 设置设为 `true`：

- `enableDnsHostnames`
- `enableDnsSupport`

有关更多信息，请参阅 Amazon VPC 用户指南中的查看和更新 VPC 的 DNS 属性。

Route 53 运行状况检查

在私有托管区中，只能将 Route 53 运行状况检查与失效转移、多值应答、加权、延迟、地理位置和地理位置临近度记录相关联。有关将运行状况检查与故障转移记录关联的信息，请参阅在私有托管区域中配置故障转移。

私有托管区域中的记录支持的路由策略

在私有托管区域中创建记录时，可以使用以下路由策略：

- 路由简单
- 故障转移路由
- 多值应答路由
- 加权路由
- 基于延迟的路由
- 地理位置路由
- 地理位置临近度路由

不支持使用其他路由策略在私有托管区域中创建记录。

拆分视图 DNS

可以使用 Route 53 来配置分割视图 DNS，又称作水平分割 DNS。在拆分视图 DNS 中，内部使用的域名 (accounting.example.com) 和外部使用的域名（例如，公共网站 (www.example.com)）相同 (example.com)。您可能还希望在内部和外部使用相同的子域名，但是为内部和外部用户提供不同的内容或要求不同的身份验证。

要配置拆分视图 DNS，请执行以下步骤：

1. 创建具有相同名称的公共和私有托管区域。（如果您在公共托管区域中使用其他 DNS 服务，则拆分视图 DNS 仍然可以使用。）
2. 将一个或多个 Amazon VPCs 与私有托管区域关联。Route 53 VPC 解析器使用私有托管区域在指定 VPCs区域中路由 DNS 查询。

3. 在每个托管区域中创建记录。公共托管区域中的记录控制互联网流量的路由方式，私有托管区域中的记录控制流量在您的 Amazon 中的路由方式。 VPCs

如果您需要对 VPC 和本地工作负载执行名称解析，则可以使用 Route 53 VPC 解析器。有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。

具有重叠命名空间的公有和私有托管区域

如果您的私有和公有托管区域具有重叠的命名空间，例如 example.com 和 accounting.example.com，VPC Resolver 会根据最具体的匹配项来路由流量。当用户登录到您与私有托管区域关联的 Amazon VPC 中的 EC2 实例时，以下是 Route 53 VPC 解析器处理 DNS 查询的方式：

1. VPC 解析器评估私有托管区域的名称是否与请求中的域名匹配，例如 accounting.example.com。以下任一形式均可定义为匹配：
   - 相同匹配
   - 私有托管区域的名称是请求中域名的父级。例如，假设请求中的域名如下：

     seattle.accounting.example.com

     以下托管区域匹配，因为它们是 seattle.accounting.example.com 的父级：
     - accounting.example.com
     - example.com

   如果没有匹配的私有托管区域，VPC Resolver 会将请求转发给公有 DNS 解析器，您的请求将作为常规 DNS 查询进行解析。
2. 如果存在与请求中的域名匹配的私有托管区域名称，则会在该托管区域中搜索与请求中的域名和 DNS 类型匹配的记录，如 accounting.example.com 的 A 记录。

> **Note**
>
> 如果有匹配的私有托管区域，但没有与请求中的域名和类型相匹配的记录，则 VPC 解析器不会将请求转发给公有 DNS 解析器。而是将 NXDOMAIN (不存在的域) 返回给客户端。

具有重叠命名空间的私有托管区域

如果您有两个或更多具有重叠命名空间的私有托管区域，例如 example.com 和 accounting.example.com，VPC Resolver 会根据最具体的匹配项来路由流量。

> **Note**
>
> 如果您有一个私有托管区域 (example.com) 和 Route 53 VPC 解析器规则，用于将流量路由到您的网络，则优先使用 VPC 解析器规则。请参阅Private hosted zones and Route 53 VPC Resolver rules。

当用户登录到您已与所有私有托管区域关联的 Amazon VPC 中的 EC2 实例时，以下是 VPC 解析器处理 DNS 查询的方式：

1. VPC 解析器会评估请求中的域名（例如 accounting.example.com）是否与其中一个私有托管区域的名称匹配。
2. 如果没有与请求中的域名完全匹配的托管区域，VPC Resolver 会检查是否存在名称为请求中域名的父域名的托管区域。例如，假设请求中的域名如下：

   `seattle.accounting.example.com`

   以下托管区域匹配，因为它们是 `seattle.accounting.example.com` 的父项：

   - `accounting.example.com`
   - `example.com`

   VPC 解析器`accounting.example.com`之所以选择，是因为它比`example.com`它更具体。
3. VPC Resolver 在`accounting.example.com`托管区域中搜索与请求中的域名和 DNS 类型相匹配的记录，例如 A 记录。`seattle.accounting.example.com`

   如果没有与请求中的域名和类型相匹配的记录，VPC 解析器会将 NXDOMAIN（不存在的域）返回给客户端。

私有托管区域和 Route 53 VPC 解析器规则

如果您有一个私有托管区域 (example.com) 和一个 VPC 解析器规则，用于将流量路由到您的网络，则优先使用 VPC 解析器规则。

例如，假设您有以下配置：

- 您有一个名为 example.com 的私有托管区域，并将其与 VPC 关联。
- 您创建了一条 Route 53 VPC 解析器规则，该规则将 example.com 的流量转发到您的网络，然后将该规则与同一 VPC 相关联。

在此配置中，VPC 解析器规则优先于私有托管区域。DNS 查询将转发到您的网络，而不是根据私有托管区域中的记录进行解析。

委派子域的责任

您现在可在私有托管区中创建 NS 记录来委托子域的责任。有关更多信息，请参阅 解析程序委托规则教程。

自定义 DNS 服务器

如果您在 VPC 中的亚马逊 EC2 实例上配置了自定义 DNS 服务器，则必须将这些 DNS 服务器配置为将您的私有 DNS 查询路由到亚马逊为您的 VPC 提供的 DNS 服务器的 IP 地址。此 IP 地址是 VPC 网络范围的基础上“+2”。例如，如果您的 VPC 的 CIDR 范围为 10.0.0.0/16，则 DNS 服务器的 IP 地址为 10.0.0.2。

如果您想在 VPCs 和您的网络之间路由 DNS 查询，可以使用 VPC 解析器。有关更多信息，请参阅什么是 Route 53 VPC 解析器？。

所需的 IAM 权限

要创建私有托管区域，除了授予 Route 53 EC2 操作的权限外，您还需要授予 Amazon 操作的 IAM 权限。有关更多信息，请参阅《服务授权参考》中的 Route 53 的操作、资源和条件键。

创建私有托管区域

私有托管区域是您托管在一个或多个 Amazon 虚拟私有云 (VPCs) 中的域的记录容器。您为某个域（例如 example.com）创建托管区域，然后创建记录来告诉 Amazon Route 53 您希望如何将流量路由到您的域内和之间。 VPCs

> **Important**
>
> 当您创建私有托管区域时，必须将一个 VPC 与该托管区域关联，并且您指定的 VPC 与该托管区域必须是使用相同账户创建的。创建托管区域后，您可以 VPCs 与其关联其他区域 VPCs ，包括您使用其他 Amazon 账户创建的托管区域。
>
> 要 VPCs 将您使用一个账户创建的账户与使用其他账户创建的私有托管区域相关联，您必须授权该关联，然后以编程方式建立关联。有关更多信息，请参阅 将您使用不同 Amazon 账户创建的 Amazon VPC 和私有托管区域相关联。

有关使用 Route 53 API 创建私有托管区域的信息，请参阅 Amazon Route 53 API 参考。

使用 Route 53 控制台创建私有托管区域

1. 对于要与 Route 53 托管区域关联的每个 VPC，请将以下 VPC 设置更改为 `true`：

- `enableDnsHostnames`
- `enableDnsSupport`

有关更多信息，请参阅 Amazon VPC 用户指南中的更新 VPC 的 DNS 支持。

2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 如果您不熟悉 Route 53，请选择入门。

   如果您已经在使用 Route 53，请在导航窗格中选择 Hosted zones（托管区域）。
4. 选择 Create Hosted Zone（创建托管区域）。
5. 在 Create Private Hosted Zone（创建私有托管区域）窗格中输入域名，还可以选择输入备注。

   有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。
6. 在 Type（类型）列表中，选择 Private hosted zone（私有托管区域）。
7. 在 VPC ID 列表中，选择要与托管区域关联的 VPC。

   > **Note**
   >
   > 如果控制台显示以下消息，则表明您尝试关联的托管区域与同一 VPC 中的另一个托管区域的命名空间相同：
   > “A conflicting domain is already associated with the given VPC or Delegation Set.”（存在冲突的域已与给定 VPC 或委派集关联。）
   > 例如，如果托管区域 A 和托管区域 B 具有相同的域名（如 `example.com`），则无法将两个托管区域与同一 VPC 关联。
8. 选择 Create Hosted Zone（创建托管区域）。

列出私有托管区域

您可以使用 Amazon Route 53 控制台列出您使用当前 Amazon 账户创建的所有托管区域。有关如何使用 Route 53 API 列出托管区域的信息，请参阅亚马逊 Route 53 API 参考ListHostedZones中的。

列出与 Amazon 账户关联的托管区域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。

   托管区域页面会自动显示使用当前 Amazon 账户创建的所有托管区域的列表。Type 列会指明托管区域是私有还是公有。选择列标题，可将所有私有托管区域和所有公有托管区域分组。

将更多内容 VPCs 与私有托管区域关联

如果您使用同一个 Amazon 账户创建了托管区域，则可以使用 Amazon Route 53 控制台 VPCs 与私有托管区域进行更多关联。VPCs

> **Important**
>
> 如果要将 VPCs 使用一个账户创建的私有托管区域与使用其他账户创建的私有托管区域相关联，则必须先授权该关联。此外，您不能使用 Amazon 控制台授权关联或将其 VPCs 与托管区域关联。有关更多信息，请参阅 将您使用不同 Amazon 账户创建的 Amazon VPC 和私有托管区域相关联。

有关如何使用 Route 53 API VPCs 与私有托管区域进行更多关联的信息，请参阅《Amazon Route 53 API 参考》VPCWithHostedZone中的 “关联”。

使用 Route 53 控制台将其它 VPCs 与私有托管区域关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要 VPCs 与之关联的私有托管区域的单选按钮。
4. 选择编辑。
5. 选择 Add VPC（添加 VPC）。
6. 选择区域以及要与托管区域关联的 VPC 的 ID。
7. 要将更多内容 VPCs 与该托管区域关联，请重复步骤 5 和 6。
8. 选择保存更改。

将您使用不同 Amazon 账户创建的 Amazon VPC 和私有托管区域相关联

如果您想将使用一个账户创建的 VPC 与使用其他 Amazon 账户创建的私有托管区域相关联，请执行以下步骤：

将您使用不同 Amazon 账户创建的 Amazon VPC 和私有托管区域关联

1. 使用创建托管区域的账户，通过以下方法之一授权将 VPC 与私有托管区域关联：

   - Amazon CLI— 参见create-vpc-association-authorization《Amazon CLI 命令参考》
   - Amazon SDK 或 Amazon Tools for Windows PowerShell— 参见 “文档” 页面上的相应Amazon 文档
   - 亚马逊 Route 53 API — 参见亚马逊 Route 53 API 参考中的创建VPCAssociation授权

   注意以下几点：

   - 如果您想将通过一个账户创建 VPCs 的多个托管区域与使用其他账户创建的托管区域相关联，则必须为每个 VPC 提交一份授权请求。
   - 在授权关联时，您必须指定托管区域 ID，因此私有托管区域必须已存在。
   - 您不能使用 Route 53 控制台来授权将 VPC 与私有托管区域关联，或直接进行关联。
2. 使用创建 VPC 的账户将 VPC 与托管区域关联。与授权关联一样，你可以使用 Amazon SDK、适用于 Windows 的工具 PowerShell Amazon CLI、或 Route 53 API。如果您使用的是 API，请使用 “关联 VPCWith HostedZone” 操作。
3. 推荐 — 删除将 VPC 与托管区域关联的授权。删除授权不会影响关联，只是禁止您以后将 VPC 与该托管区域重新关联。如果要将 VPC 与托管区域重新关联，您需要重复执行此过程的步骤 1 和 2。

> **Important**
>
> `ListHostedZonesByVPC`返回给定 VPC 的托管区域，`GetHostedZone`API 返回与托管区域 VPCs 关联的区域。这些 APIs 仅考虑由 `AssociateVPCWithHostedZone` API 创建或创建私有托管区域时创建的托管区域与 VPC 的关联。如果您想要托管区域与 VPC 关联的完整列表，也可以致电ListProfileResourceAssociations。

> **Note**
>
> 有关可创建的最大授权数，请参阅实体的配额。

取消与私 VPCs 有托管区域的关联

您可以使用 Amazon Route 53 控制台取消与私 VPCs 有托管区域的关联。这将导致 Route 53 停止使用托管区域中的记录对在 VPC 中发起的 DNS 查询进行路由通信。例如，如果 example.com 托管区域与 VPC 关联，并且您取消了托管区域与该 VPC 的关联，则 Route 53 会停止解析针对 example.com 或 example.com 托管区域中任何其它记录的 DNS 查询。

> **Note**
>
> 您无法取消最后一个 VPC 与私有托管区域的关联。如果要取消该 VPC 的关联，必须先将另一个 VPC 与托管区域关联。

取消与私 VPCs 有托管区域的关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要取消与一个或多个托管区域关联的私有托管区域 VPCs 的单选按钮。
4. 选择编辑。
5. 在要与此托管区域解除关联的 VPC 旁边选择 Remove VPC（删除 VPC）。
6. 选择保存更改。

删除私有托管区域

本节介绍了如何使用 Amazon Route 53 控制台删除私有托管区域。

只有在没有任何记录 (默认 SOA 和 NS 记录除外) 时，您才可以删除私有托管区域。如果您的托管区域包含其他记录，则必须先将其删除，然后才能删除托管区域。这样可以防止您意外删除仍包含记录的托管区域。

主题

删除由其他服务创建的私有托管区域

如果其它服务创建了一个私有托管区域，您将无法使用 Route 53 控制台删除它。相反，您需要使用针对其他服务的合适过程：

- Amazon Cloud Map— 要删除在创建私有 DNS 命名空间时 Amazon Cloud Map 创建的托管区域，请删除该命名空间。 Amazon Cloud Map 自动删除托管区域。有关更多信息，请参阅 Amazon Cloud Map 开发人员指南中的删除命名空间。
- Amazon Elastic Container Service (Amazon ECS) 服务发现 — 要删除 Amazon ECS 在您使用服务发现创建服务时创建的私有托管区域，请删除使用该命名空间的 Amazon ECS 服务，并删除该命名空间。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的删除服务。

使用 Route 53 控制台删除私有托管区域

要使用 Route 53 控制台删除私有托管区域，请执行以下过程。

要使用 Route 53 控制台删除私有托管区域

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 确认您要删除的托管区域仅包含 NS 和 SOA 记录。如果它包含其他记录，请将其删除：
   a. 选择要删除的托管区域的名称。
   b. 在 Record（记录）页面，如果记录列表内任何记录对应的 Type（类型）列值不是 NS 或 SOA，请选择此行，然后选择 Delete（删除）。

      要选择多个连续的记录，请选择第一行，按住 Shift 键，然后选择最后一行。要选择多个不连续的记录，请选择第一行，按住 Ctrl 键，然后选择其余各行。
3. 在“Hosted Zones”页面上，选择您要删除的托管区域所对应的那一行。
4. 选择删除。
5. 键入确认密钥，然后选择 Delete（删除）。

VPC 权限

VPC 权限使用身份和访问管理 (IAM) 策略条件，允许您在使用 “关联”、“取消VPCFromHostedZone关联”、“创建VPCAssociation授权” VPCWith HostedZone、“删除VPCAssociation授权” 和 “VPCListHostedZonesBy” VPCs 时设置精细权限。CreateHostedZone APIs

通过 IAM 策略条件`route53:VPCs`，您可以向其他 Amazon 用户授予精细的管理权限。这允许您向某个人授予将托管区关联至以下对象、取消其与托管区的关联、为其创建 VPC 关联授权、删除其 VPC 关联授权、创建托管区或列出其托管区的权限：

- 单个 VPC。
- 同一区域 VPCs 内的任何一个。
- 多个 VPCs。

有关 VPC 权限的更多信息，请参阅 使用 IAM 策略条件进行精细访问控制。

要了解如何对 Amazon 用户进行身份验证，请参阅使用身份进行身份验证；要了解如何控制对 Route 53 资源的访问权限，请参阅访问控制。

将托管区迁移到其它 Amazon 账户

在将托管区迁移到其他 Amazon Web Services 账户 时，请执行以下建议的步骤。

这些步骤最适合记录更改频率较低的托管区。对于记录频繁更新的托管区，请考虑以下事项：

- 迁移期间不要更新任何资源记录。
- 转移委托后，在旧托管区和新托管区中发布资源记录更改。

先决条件

安装或升级 Amazon CLI：

有关下载、安装和配置 Amazon CLI 的信息，请参阅 Amazon Command Line Interface 用户指南。

> **Note**
>
> 配置 CLI，以便您能在同时使用创建了托管区域的账户和要将托管区域迁移到的账户时使用它。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的配置 。

如果您已在使用 Amazon CLI，建议您升级到最新版本的 CLI，以便 CLI 命令能够支持最新的 Route 53 功能。

主题

步骤 1：准备迁移

准备步骤可帮助您最大限度地降低与迁移托管区相关的风险。

1. 监控区域可用性

您可以监控区域以了解域名的可用性。这可以帮助您解决可能导致回滚迁移的任何问题。您可以使用 CloudWatch 或查询日志记录来监控流量最多的域名。有关设置查询日志记录的更多信息，请参阅 监控 Amazon Route 53。

可以通过 Shell 脚本或第三方服务来完成监控。但是，其不应作为确定是否需要回滚的唯一信号，因为由于域不可用，您也可能会从客户处获得反馈。

2. 降低 TTL 设置值

记录的 TTL（生存时间）设置指定您希望 DNS 解析程序缓存记录和使用缓存信息的时间。当 TTL 过期时，解析程序会向域的 DNS 服务提供商发送另一个查询以获取最新信息。

NS 记录的典型 TTL 设置为 172800 秒或两天。NS 记录列出了域名系统 (DNS) 可用来获取有关如何路由域流量的信息的名称服务器。通过为当前 DNS 服务提供商和 Route 53 减小 NS 记录的 TTL，可在您将 DNS 迁移至 Route 53 的过程中发现问题时缩短域的停机时间。如果您不减小 TTL，则您的域可能会在出现问题时最多两天内在 Internet 上不可用。

降低 TTL

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中选择托管区。
3. 选择托管区域的名称。
4. 选择 NS 记录，然后在记录详细信息窗格中选择编辑记录。
5. 更改 TTL（秒）的值。我们建议您指定一个介于 60 秒和 900 秒 (15 分钟) 之间的值。
6. 选择保存。

3. 从父区域中移除 DS 记录（如果您已配置 DNSSEC）

如果已为域配置 DNSSEC，请在将域迁移到 Route 53 之前从父区域中删除 Delegation Signer (DS) 记录。

如果父区域通过 Route 53 进行托管，请参阅 删除域的公有密钥 以获取更多信息。如果父区域在另一个注册商处进行托管，请联系他们移除 DS 记录。

Route 53 目前不支持迁移 DNSSEC 设置。因此，您需要通过从父区域中移除 DS 记录来禁用在迁移之前对您的域执行的 DNSSEC 验证。迁移完成后，您可以通过在新托管区上配置 DNSSEC 并将相应 DS 记录添加到父区域来重新启用 DNSSEC 验证。

4. 确保没有其他依赖迁移托管区的持续操作

某些操作将依赖于迁移托管区中的 DNS 解析，例如，TLS/SSL 证书续订过程可能需要更改 DNS 记录，而提供商会尝试将 DNS 记录解析为验证方法。在迁移之前，应确保没有其他操作发生，以避免托管区迁移造成意外影响。

步骤 2：创建新的托管区

在要将托管区迁移到的目标账户中创建新的托管区。

选择相应选项卡，查看 Amazon CLI 或控制台的说明。

- CLI
- 控制台

CLI

输入以下命令：

```
aws route53 create-hosted-zone \
            --name $hosted_zone_name \
            --caller-reference $unique_string
```

有关更多信息，请参阅 create-hosted-zone。

Console

使用其他账户创建新的托管区域

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

   使用要将托管区域迁移到的账户的账户凭证登录。
2. 创建一个托管区域。有关更多信息，请参阅 创建公有托管区域。
3. 记下托管区域 ID。在某些情况下，您在此过程的后面需要使用此信息。
4. 从 Route 53 控制台注销。

在新区域中也要降低 NS TTL，类似于准备“步骤 1：降低 TTL 设置值”中的“降低 TTL”设置。

步骤 3：（可选）迁移运行状况检查

您可以将新账户中的 DNS 记录与要从中迁移的账户中的 Route 53 运行状况检查相关联。要迁移 Route 53 运行状况检查，您需要使用与现有账户相同的配置，在新账户中创建新的运行状况检查。有关更多信息，请参阅 创建 Amazon Route 53 运行状况检查 。

步骤 4：将记录从旧托管区迁移到新的托管区

您可以使用控制台或 Amazon CLI，将记录从 Amazon Web Services 账户 迁移到另一个。

Console

如果您的区域仅包含几条记录，则可以考虑使用 Route 53 控制台列出旧区域中的记录，记下这些记录，然后在新区域中创建这些记录。如果您已在 步骤 3：（可选）迁移运行状况检查 中迁移运行

状况检查，则在新的托管区中创建记录时，应指定新的运行状况检查 ID。有关更多信息，请参阅以下主题：

- 列出记录
- 通过使用 Amazon Route 53 控制台创建记录
- 配置 DNS 故障转移

您还应该降低新区域中的 NS TTL，类似于步骤 1 中的降低 TTL 设置。

CLI

如果您的区域包含大量记录，则可以导出要迁移到文件的记录，编辑此文件，然后使用编辑后的文件在新的托管区中创建记录。以下过程使用 Amazon CLI 命令，但也有第三方工具可用于此目的。

1. 运行以下命令：

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
   ```

   请注意以下几点：

   - 对于 *hosted-zone-id*，请指定包含要迁移记录的旧托管区的 ID。
   - 对于 *path-to-output-file*，指定要在其中保存输出的目录路径和文件名。
   - > 字符将输出发送到指定文件。
   - Amazon CLI 将自动处理包含 100 条以上记录的托管区域的分页。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的使用 Amazon 命令行界面的分页选项。

     如果您使用其它编程方法（如某个 Amazon 软件开发工具包）列出记录，对于每个结果页，您最多可以获取 100 条记录。如果托管区域包含 100 条以上的记录，您必须提交多个请求才能列出所有记录。

   创建此输出的副本。在新的托管区域中创建记录后，建议您在新的托管区域上运行 Amazon CLI `list-resource-record-sets` 命令并比较两个输出以确保已创建所有记录。

2. 编辑要迁移的记录

   编辑导出的文件，然后才能将其与 `change-resource-record-sets` 命令结合使用。您可以使用文本编辑器中的“搜索并替换”功能来进行这些更改。

> **Note**
>
> 以下步骤描述使用文本编辑器进行手动编辑。高级用户可以使用 jq、Python 或其他脚本语言等编程工具自动执行这些转换。

打开您在本过程步骤 1 中创建的包含要迁移记录的文件副本，然后进行以下更改：

- 将文件顶部的 ResourceRecordSets 元素替换为 `Changes` 元素。
- 可选 — 添加 `Comment` 元素。
- 删除与托管区名称的 NS 和 SOA 记录相关的行。新的托管区域已具有这些记录。
- 为每条记录添加 `Action` 和 `ResourceRecordSets` 元素，根据需要添加左方括号和右方括号（`{` `}`）以使 JSON 代码有效。

  > **Note**
  >
  > 您可以使用 JSON 验证程序来验证所有大括号和方括号是否位于正确的位置。要查找在线 JSON 验证器，请在浏览器中搜索“JSON 验证器”。

- 如果托管区域包含任何引用同一托管区域中的其他记录的别名，请进行以下更改：
  - 将托管区域 ID 更改为新托管区域的 ID。

    > **Important**
    >
    > 如果别名记录指向另一个资源（例如负载均衡器），请勿将托管区 ID 更改为域的托管区 ID。如果意外更改了托管区 ID，需将托管区 ID 回滚为资源本身的托管区 ID，而不是域的托管区 ID。该资源托管区 ID 可以在创建资源的 Amazon 控制台中找到。

  - 将别名记录移至文件的底部。Route 53 必须先创建别名记录引用的记录，然后才能创建别名记录。

    > **Important**
    >
    > 如果一条或多条别名记录引用其他别名记录，则作为别名目标的记录在文件中必须位于引用别名记录之前。例如，如果 `alias.example.com` 为

alias.alias.example.com 的别名目标，则 alias.example.com 必须在文件中出现在后者之前。

- 删除将流量路由到流量策略实例的任何别名记录。记下这些记录，以便您稍后能重新创建它们。

- 如果您已在 步骤 3：（可选）迁移运行状况检查 中迁移运行状况检查，请更改记录以与新创建的运行状况检查 ID 相关联。

以下示例显示了 example.com 托管区域的记录被编辑后的版本。红色的斜体文本是新版本：

```
{
    "Comment": "string",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "ResourceRecords": [
                    {
                        "Value": "192.0.2.4"
                    },
                    {
                        "Value": "192.0.2.5"
                    },
                    {
                        "Value": "192.0.2.6"
                    }
                ],
                "Type": "A",
                "Name": "route53documentation.com.",
                "TTL": 300
            }
        },
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "AliasTarget": {
                    "HostedZoneId": "Z3BJ6K6RIION7M",
                    "EvaluateTargetHealth": false,
                    "DNSName": "s3-website-us-west-2.amazonaws.com."
                },
                "Type": "A",
```

```
                "Name": "www.route53documentation.com."
            }
        }
    ]
}
```

3. 将大文件拆分成多个小文件

   如果您有大量记录或者您的记录包含大量值 (例如，大量 IP 地址)，您可能需要将文件拆分为多个小文件。最大值为：

   - 每个文件最多可包含 1000 条记录。
   - 所有 `Value` 元素中的值的最大组合长度为 32000 个字节。

4. 在新托管区中创建记录

   输入以下 CLI：

   ```
   aws route53 change-resource-record-sets \
               --hosted-zone-id new-hosted-zone-id \
               --change-batch file://path-to-file-that-contains-records
   ```

   指定以下值：

   - 对于 *new-hosted-zone-id*，指定新托管区的 ID。
   - 对于 *path-to-file-that-contains-records*，请指定您在前面步骤中编辑的目录路径和文件名。

   如果您已删除将流量路由到流量策略实例的任何别名记录，请使用 Route 53 控制台重新创建它们。有关更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

步骤 5：比较新托管区域和旧托管区域中的记录

要确认您已在新托管区中成功创建所有记录，请输入如下 CLI 命令以列出新托管区中的记录，并将输出与旧托管区中的记录列表进行比较。

```
aws route53 list-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
            --output json > path-to-output-file
```

指定以下值：

- 对于 *new-hosted-zone-id*，指定新托管区的 ID。
- 对于 *path-to-output-file*，指定要在其中保存输出的目录路径和文件名。使用与您在步骤 4 中使用的不同文件名。

  > 字符将输出发送到指定文件。

将此输出与来自步骤 4 的输出进行比较。除了 NS 和 SOA 记录的值以及您在步骤 4 中所做的任何更改 (如不同的托管区 ID 或域名)，两个输出应相同。

如果新托管区中的记录与旧托管区中的记录不匹配，执行下列操作之一：

- 使用 Route 53 控制台进行少量纠正。有关更多信息，请参阅 编辑记录。
- 从新托管区中删除 NS 和 SOA 记录之外的所有记录，然后重复步骤 4 中的过程。

步骤 6：将域注册更新为使用新托管区域的名称服务器

完成将记录迁移到新托管区之后，将域注册的名称服务器更改为使用新托管区的名称服务器。有关更多信息，请参阅将 Amazon Route 53 作为现有域的 DNS 服务。

如果您的托管区正在使用中（例如，如果您的用户正在使用该域名浏览网站或访问 Web 应用程序），则应继续监控托管区的流量和可用性，包括网站或应用程序流量、电子邮件等。

- 如果流量慢或停止 - 请将域注册的名称服务改回旧托管区中的名称服务器。然后，确定出错的位置。
- 如果流量未受影响 - 继续至下一步。

步骤 7：将 NS 记录的 TTL 重新改为更高的值

在新托管区中，将 NS 记录对应的 TTL 更改为更典型的值，例如，172800 秒 (两天)。这减少用户的延迟，因为他们不必像 DNS 解析程序一样通常需要等待为您的域的名称服务器发送查询。

更改 TTL

1. 请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中选择托管区。
3. 选择托管区域的名称。

4. 选择 NS 记录，然后在记录详细信息窗格中选择编辑记录。
5. 将 TTL（秒）的值更改为您希望 DNS 解析程序缓存您的域的名称服务器的名称的秒数。我们建议的值为 172800 秒。
6. 选择保存。

步骤 8：重新启用 DNSSEC 签名并建立信任链（如果需要）

您可以通过两个步骤重新启用 DNSSEC 签名：

1. 为 Route 53 启用 DNSSEC 签名，并请求 Route 53 根据客户托管密钥在 Amazon Key Management Service 中创建密钥签名密钥（KSK）。
2. 通过向父区域添加 Delegation Signer（DS）记录，为托管区创建信任链，以便使用受信任的加密签名对 DNS 响应进行身份验证。

有关说明，请参阅启用 DNSSEC 签名并建立信任链。。

步骤 9：（可选）删除旧托管区域

如果您确信您不再需要旧托管区域，则可选择将其删除。有关说明，请参阅删除公有托管区域。

> **Important**
>
> 在将域注册更新为使用新托管区域的名称服务器后的至少 48 小时内，不要删除旧托管区域或该托管区域中的任何记录。如果在 DNS 解析程序停止使用旧托管区域中的记录之前删除该托管区域，则在解析程序开始使用新托管区域之前，您的域在 Internet 上不可用。

使用记录

为您的域创建托管区域 (例如 example.com) 之后，您需要创建记录以告知域名系统 (DNS) 您希望如何路由该域的流量。

例如，您可以创建记录来使 DNS 执行以下操作：

- 将 example.com 的 Internet 流量路由到您数据中心中某个主机的 IP 地址。
- 将该域的电子邮件 (ichiro@example.com) 路由到邮件服务器 (mail.example.com)。
- 将名为 operations.tokyo.example.com 的子域的流量路由到另一台主机的 IP 地址。

每个记录都包括域或子域的名称、记录类型 (例如，具有 MX 路由电子邮件类型的记录) 以及适用于该记录类型的其他信息 (对于 MX 记录，其他信息可能包括一个或多个邮件服务器的主机名、每个服务器的优先级等)。有关不同记录类型的信息，请参阅支持的 DNS 记录类型。

托管区域中每个记录的名称必须以托管区域的名称结尾。例如，example.com 托管区域可以包含 www.example.com 和 accounting.tokyo.example.com 子域的记录，但不能包含 www.example.ca 子域的记录。

> **Note**
>
> 要为复杂的路由配置创建记录，您也可以使用 Traffic Flow 可视化编辑器，并将配置保存为流量策略。然后，您可以将流量策略关联至同一托管区域或多个托管区域中的一个或多个域名 (例如 example.com) 或子域名 (例如 www.example.com)。此外，如果新配置无法正常工作，您还可以回滚更新。有关更多信息，请参阅 使用 Traffic Flow 来路由 DNS 流量。

对于您添加到托管区域的记录，Amazon Route 53 不收取费用。有关可在托管区域中创建的最大记录数的信息，请参阅 配额。

主题

选择路由策略

要创建记录，需要先选择一个路由策略，它决定了 Amazon Route 53 响应查询的方式：

- 简单路由策略 - 对于为您的域执行给定功能的单一资源（例如为 example.com 网站提供内容的 Web 服务器），可以使用该策略。在私有托管区域中，可以使用简单的路由创建记录。
- 故障转移路由策略 - 如果您想要配置主动-被动故障转移，则可以使用该策略。在私有托管区域中，可以使用失效转移路由创建记录。
- 地理位置路由策略 - 如果您想要根据用户的位置来路由流量，则可以使用该策略。在私有托管区域中，可以使用地理位置路由创建记录。
- 地理位置临近度路由策略 - 用于根据资源的位置来路由流量，以及（可选）将流量从一个位置中的资源转移到另一个位置中的资源。在私有托管区中，可以使用地理位置临近度路由创建记录。
- 延迟路由策略-当您有多个资源 Amazon Web Services 区域 并且想要将流量路由到延迟最佳的区域时使用。在私有托管区域中，可以使用延迟路由创建记录。
- 基于 IP 的路由策略 – 如果您希望根据用户的位置来路由流量，并且获得流量来源的 IP 地址，则可以使用该策略。
- 多值应答路由策略 - 如果您想要让 Route 53 用随机选择的正常记录（最多八条）响应 DNS 查询，则可以使用该策略。在私有托管区域中，可以使用多值应答路由创建记录。
- 加权路由策略 - 用于按照您指定的比例将流量路由到多个资源。在私有托管区域中，可以使用加权路由创建记录。

主题

路由简单

简单路由让您可以配置标准 DNS 记录，无需特殊 Route 53 路由，例如加权或延迟。使用简单路由，您通常将流量路由到单个资源，例如，路由到您网站的 Web 服务器。

可以对私有托管区中的记录使用简单路由策略。

如果您在 Route 53 控制台中选择简单路由策略，就无法创建具有相同名称和类型的多个记录，但您可在相同记录中指定多个值，例如多个 IP 地址。（如果您为别名记录选择简单路由策略，则只能在当前托管区域中指定一个 Amazon 资源或一条记录。）如果您在记录中指定多个值，则 Route 53 将所有值以随机顺序返回到递归解析程序，解析程序将值返回到提交 DNS 查询的客户端（例如，Web 浏览器）。然后，客户端选择值并重新提交查询。使用简单路由策略时，您可以指定多个 IP 地址，但这些 IP 地址不会进行运行状况检查。

有关您在使用简单路由策略创建记录时所指定值的信息，请参阅以下主题：

- 简单记录的特定值
- 简单别名记录的特定值
- 所有路由策略的通用值
- 所有路由策略的别名记录的通用值

故障转移路由

故障转移路由允许您将流量路由到某个资源 (如果该资源正常) 或路由到其他资源 (如果第一个资源不正常)。主和辅助记录可以将流量路由到从配置为网站的 Amazon S3 存储桶到复杂记录树的任何目的地。有关更多信息，请参阅 主动/被动故障转移。

可以对私有托管区中的记录使用失效转移路由策略。

有关您在使用故障转移路由策略创建记录时所指定值的信息，请参阅以下主题：

- 故障转移记录的特定值
- 故障转移别名记录的特定值
- 所有路由策略的通用值
- 所有路由策略的别名记录的通用值

地理位置路由

地理位置路由允许您根据用户的地理位置 (即 DNS 查询的来源位置) 选择提供流量的资源。例如，您可能想要将来自欧洲的所有查询全部路由到位于法兰克福区域的 Elastic Load Balancing 负载均衡器。

使用地理位置路由时，您可以对您的内容进行本地化，以用户使用的语言显示您网站的部分或全部。您还可以使用地理位置路由，以便仅向您拥有分配权限的位置分配内容。另一种可能的用途是以可预测easy-to-manage的方式在端点之间平衡负载，以便每个用户位置始终如一地路由到同一个端点。

您可以按大陆、按国家/地区或者按美国各州指定地理位置。如果您为重叠的地理区域创建了单独的记录（例如，北美一个记录，加拿大一个记录），则最小的地理区域具有更高的优先级。这允许您将某个大陆的部分查询路由到一个资源，并将该大陆上选定国家/地区的查询路由到另一个资源。(有关每个大陆上的国家/地区的列表，请参阅位置。)

地理位置路由的工作原理是将 IP 地址映射到位置。但是，有些 IP 地址无法映射到地理位置，因此即使您创建了覆盖全部七大洲的地理位置记录，Amazon Route 53 仍会收到一些来自其无法识别的位置的 DNS 查询。您可以创建一条默认记录，用以处理来自未映射到任何位置的 IP 地址的查询，以及来自您未创建地理位置记录的位置的查询。如果您不创建默认记录，则对于来自上述位置的查询，Route 53 将返回“无应答”响应。

可以对共有和私有托管区中的记录使用地理位置路由。

有关更多信息，请参阅 Amazon Route 53 如何使用 EDNS0 估计用户的位置。

有关您在使用地理定位路由策略创建记录时所指定值的信息，请参阅以下主题：

- 地理位置记录的特定值
- 地理位置别名记录的特定值
- 所有路由策略的通用值
- 所有路由策略的别名记录的通用值

私有托管区中的地理位置路由

对于私有托管区域，Route 53 会根据查询来源的 VPC 响应 DNS 查询。 Amazon Web Services 区域有关列表 Amazon Web Services 区域，请参阅 Amazon EC2 用户指南中的区域和区域。

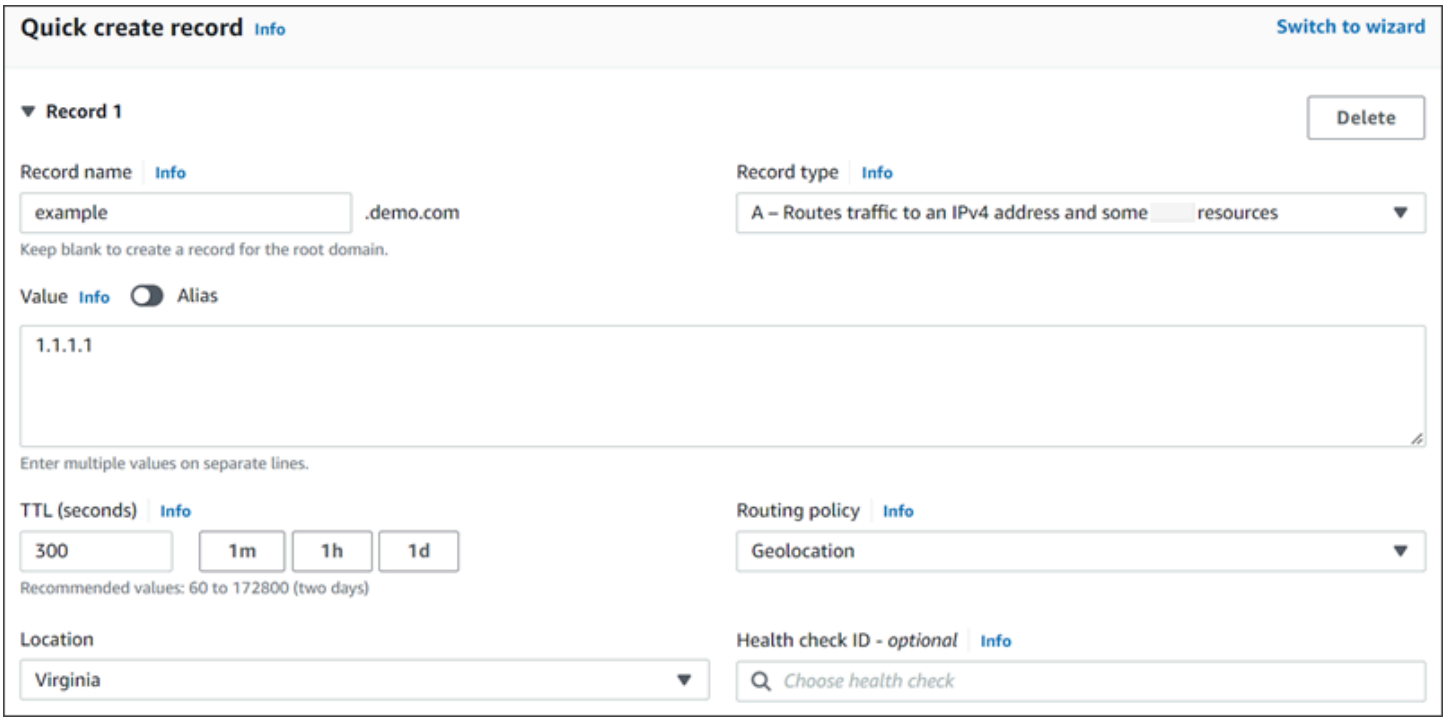
如果 DNS 查询源自混合网络的本地部分，则将被视为源自 VPC 所在的 Amazon Web Services 区域 。

如果包括运行状况检查，您可以为以下项创建默认记录：

- 未映射到地理位置的 IP 地址。
- 来自您尚未为其创建地理位置记录的位置的 DNS 查询。

如果 DNS 查询所在区域的地理位置记录运行不正常，则将返回默认记录（如果它运行正常）。

在下图的示例配置中，来自 us- Amazon Web Services 区域 east-1（弗吉尼亚州）的 DNS 查询将路由到 1.1.1.1 终端节点。



地理位置临近度路由

地理位置临近度路由能让 Amazon Route 53 根据您的用户和资源的地理位置将流量路由到您的资源。它将流量路由到位置最近的可用资源。（可选）您也可以通过指定一个值来增加或减少路由到指定资源的流量，该值称为偏差。偏差可以增加或减少路由到某个资源的流量所来自的地理区域的大小。

为您的资源创建地理位置临近度规则并为每个规则指定以下值之一：

- 如果您使用的是 Amazon 资源，请指定您在其中创建资源的 Amazon Web Services 区域 或本地区域组。
- 如果您使用的是非Amazon 资源，请指定资源的纬度和经度。

要使用 L Amazon ocal Zones，必须先启用它们。有关更多信息，请参阅《Amazon Local Zones 用户指南》中的 Local Zones 入门。

要了解 Amazon Web Services 区域 和 Local Zones 之间的区别，请参阅亚马逊 EC2 用户指南中的区域和区域。

（可选）要更改 Route 53 路由到某个资源的流量所来自的地理区域的大小，请为该偏差指定一个适用值：

- 要扩大 Route 53 从中将流量路由到资源的地理区域的大小，请为该偏差指定一个介于 1 和 99 之间的正整数。Route 53 将缩小相邻区域的大小。
- 要缩小 Route 53 从中将流量路由到资源的地理区域的大小，请指定一个介于 -1 和 -99 之间的负偏差。Route 53 将扩大相邻区域的大小。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

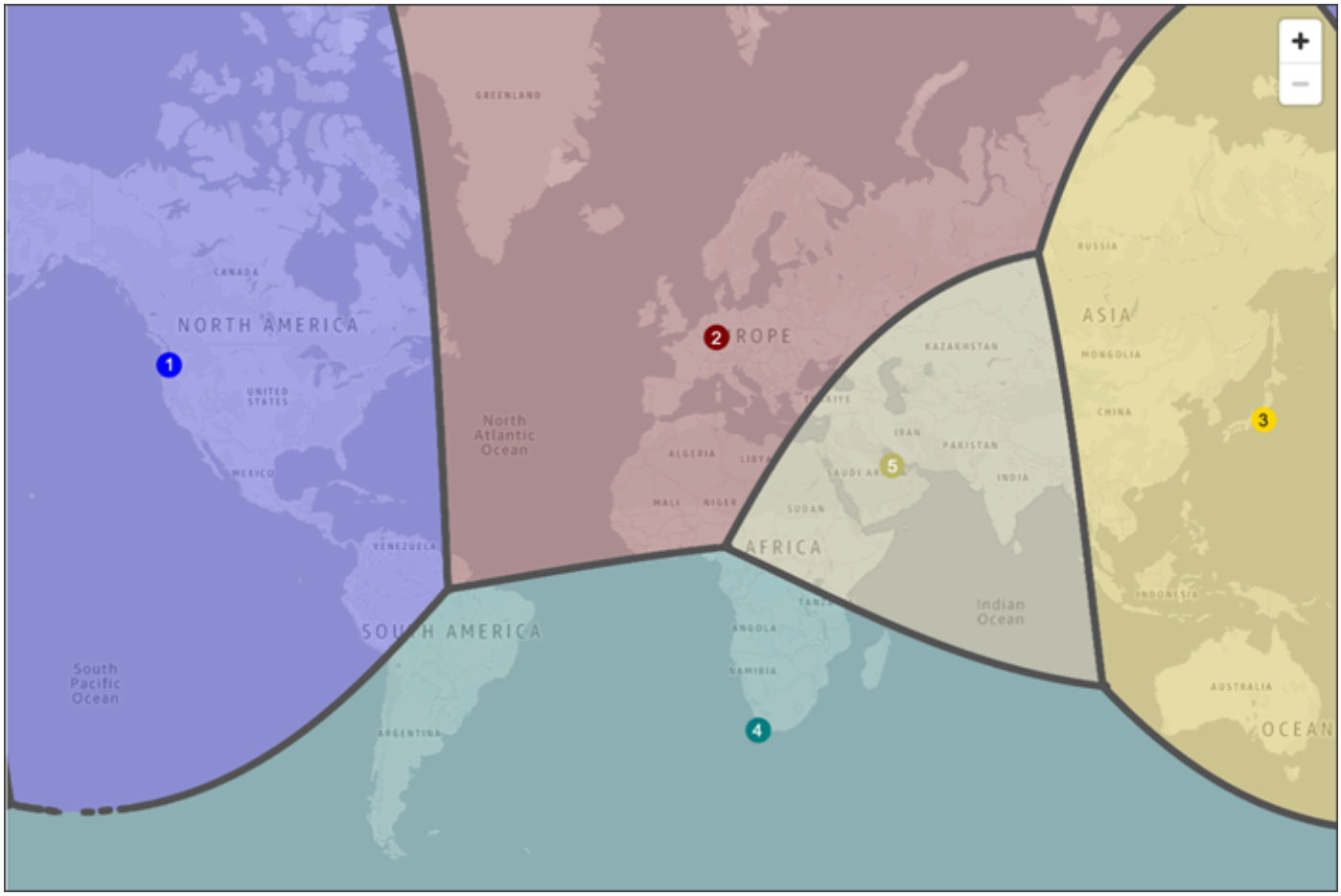
- 新控制台
- 旧控制台

New console

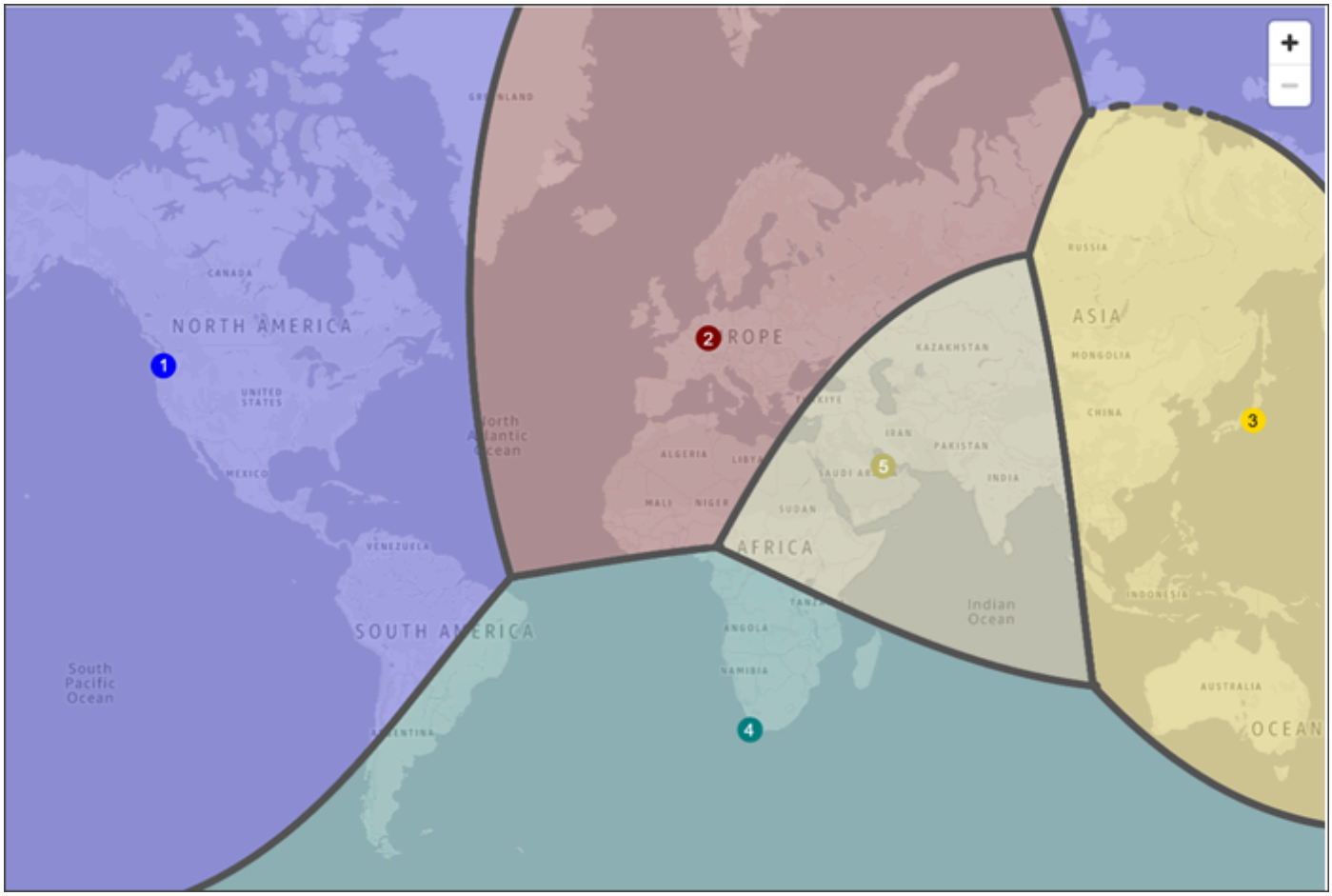
下图显示了四张 Amazon Web Services 区域（编号为 1 到 5）：

1. 美国西部（俄勒冈州）
2. 欧洲地区（法兰克福）
3. 亚太地区（东京）
4. 非洲（开普敦）
5. 中东（巴林）

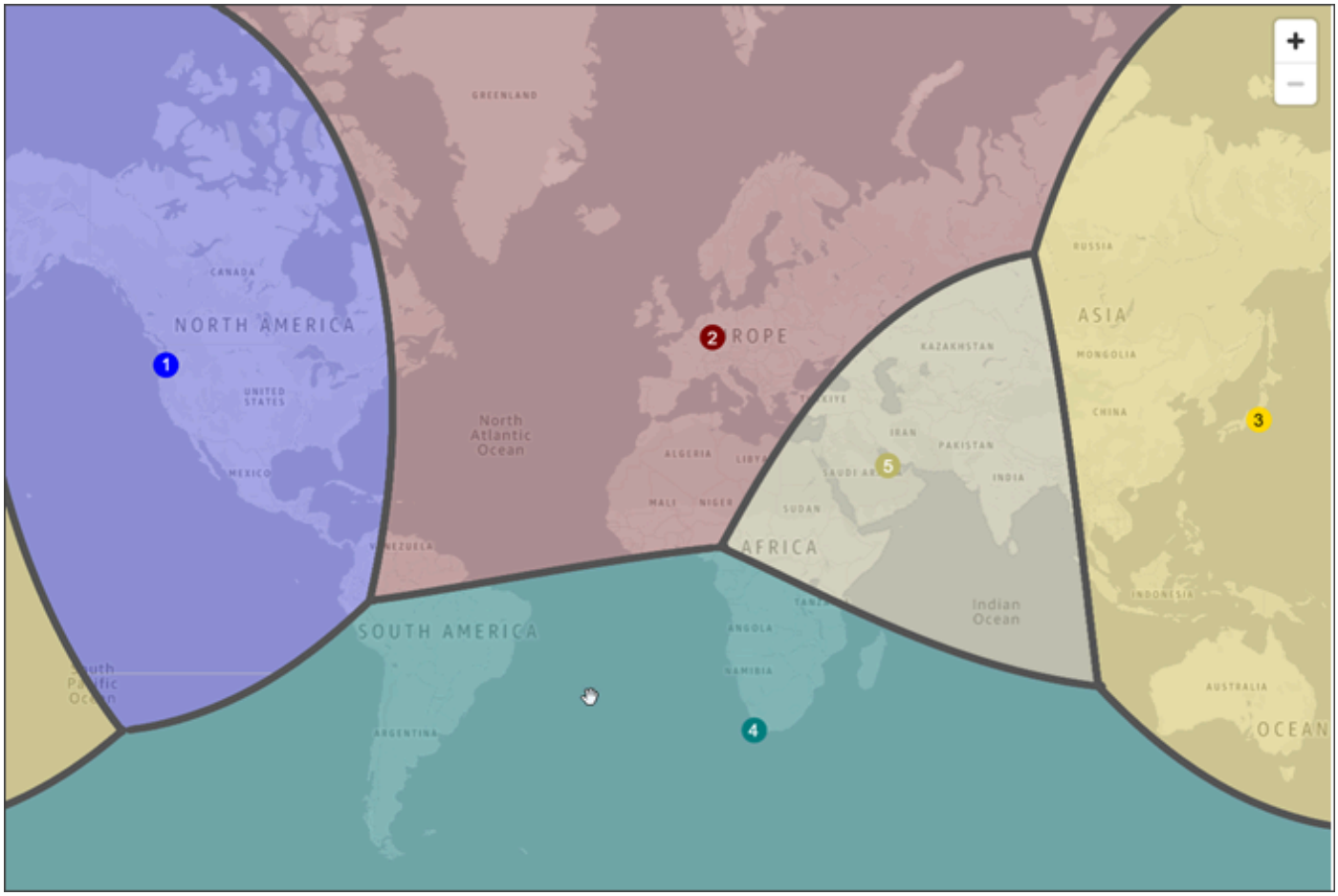
> **Note**
>
> 这些地图仅适用于 Traffic Flow。



以下地图显示如果您为美国西部（俄勒冈州）区域（地图上的编号为 1）添加了偏差值 +25 时，将发生的情况。相比从前，来自更大面积的北美区域以及所有南美区域的流量将路由到该区域中的资源。



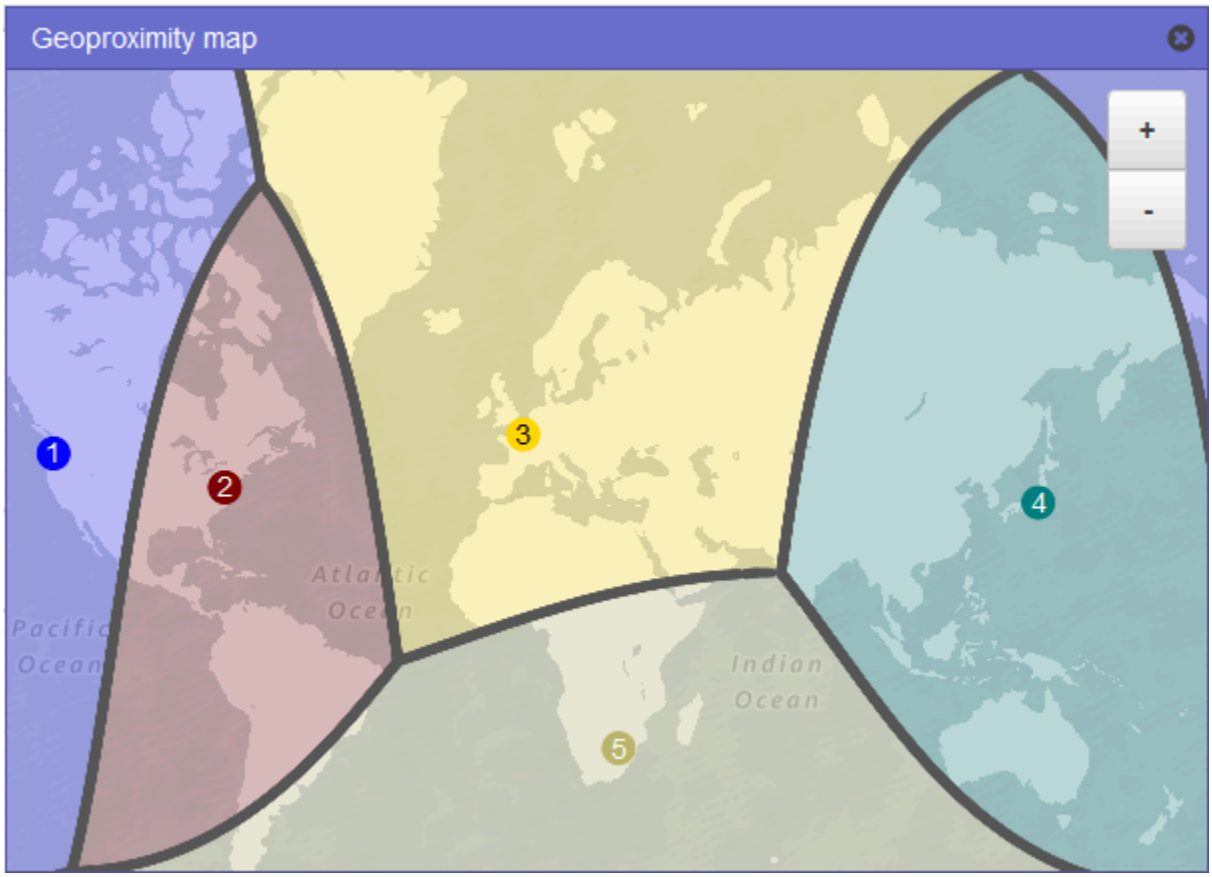
以下地图显示如果您将美国西部（俄勒冈州）区域的偏差值改为 -25 时，将发生的情况。流量从北美和南美的较小部分路由到该区域的资源，而更多流量路由到邻近区域 2、3 和 4 的资源。



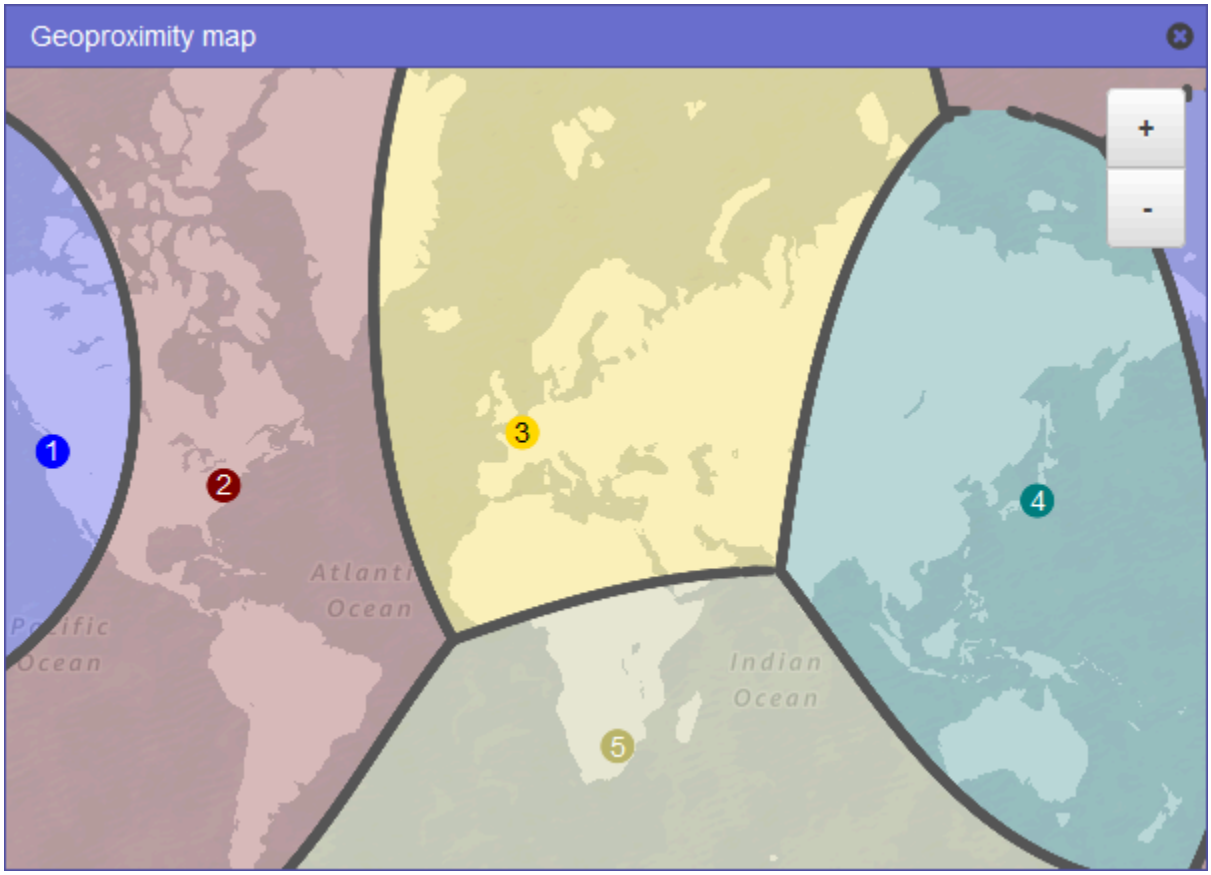
Old console

下图显示了四个 Amazon Web Services 区域（编号为 1 到 4）以及南非约翰内斯堡的一个由纬度和经度 (5) 指定的位置。

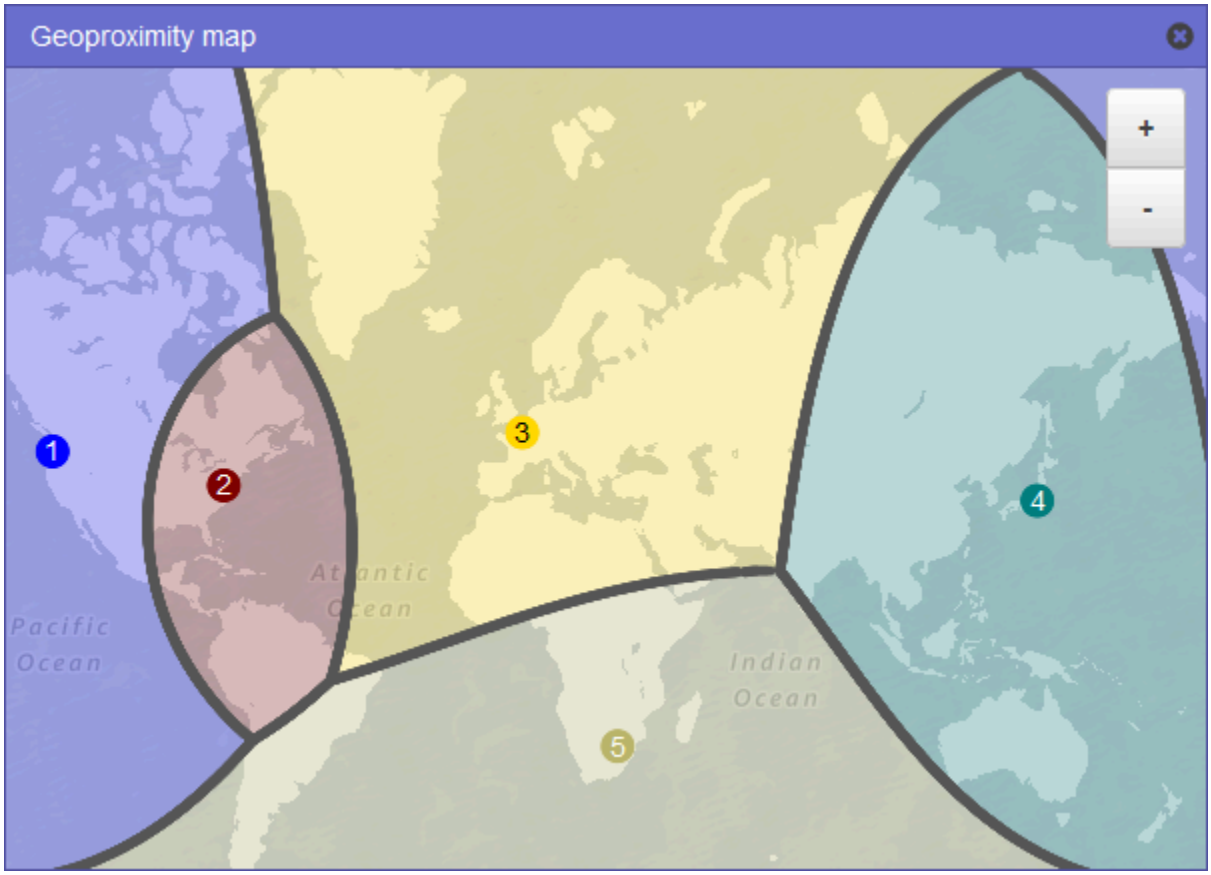
> **Note**
>
> 这些地图仅适用于 Traffic Flow。



以下地图显示如果您为美国东部（弗吉尼亚州北部）区域（地图上的编号为 2）添加了偏差值 +25 时，将发生的情况。相比从前，来自更大面积的北美区域以及所有南美区域的流量将路由到该区域中的资源。



以下地图显示如果您将美国东部（弗吉尼亚州北部）区域的偏差值改为 -25 时，将发生的情况。相比从前，来自较小面积的北美和南美区域的流量路由到该区域中的资源，更多流量路由到临近区域 1、3 和 5 中的资源。



更改资源的偏移会造成的影响取决于多种因素，包括：

- 您具有的资源的数量。
- 资源彼此之间的距离。
- 您在地理区域之间的边界区域附近拥有的用户数。例如，假设您在 Amazon Web Services 区域 美国东部（弗吉尼亚北部）和美国西部（俄勒冈）拥有资源，并且在美国德克萨斯州的达拉斯、奥斯汀和圣安东尼奥市有大量用户。这些城市之间的资源距离大致相等，因此偏见的微小变化可能会导致流量从一个资源 Amazon Web Services 区域 向另一个资源的大幅波动。

我们建议您以较小的增量来更改偏差，以防止由于流量的意外摆动而导致您的资源被耗尽。

有关更多信息，请参阅 Amazon Route 53 如何使用 EDNS0 估计用户的位置。

Amazon Route 53 如何使用偏差来路由流量

以下是 Amazon Route 53 用于确定如何路由流量的公式：

偏差

```
Biased distance = actual distance * [1 - (bias/100)]
```

当偏差值为正值时，Route 53 会将 DNS 查询的源和您在地理位置邻近记录中指定的资源（例如中的 EC2 实例 Amazon Web Services 区域）视为它们比实际距离更近。例如，假设您具有以下地理位置临近度记录：

- Web 服务器 A 的记录，它具有正偏差 50
- Web 服务器 B 的记录，它没有偏差

当某个地理位置临近度记录具有正偏差 50 时，Route 53 会将查询的源与该记录的资源之间的距离减半。之后，Route 53 将计算哪一资源更接近查询的源。假设 Web 服务器 A 与查询的源相距 150 千米，而 Web 服务器 B 与查询的源相距 100 千米。如果这两个记录都没有偏差，Route 53 会将查询路由到 Web 服务器 B，因为它更近。但是，由于 Web 服务器 A 的记录具有正偏差 50，Route 53 将认为 Web 服务器 A 与查询的源相距 75 千米。因此，Route 53 会将查询路由到 Web 服务器 A。

下面是针对正偏差 50 的计算：

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

基于延迟的路由

如果您的应用程序以多个方式托管 Amazon Web Services 区域，则可以从提供最低延迟的请求中处理他们的请求 Amazon Web Services 区域 ，从而提高用户的性能。

> **Note**
>
> 有关用户与您的资源之间延迟的数据完全基于用户与 Amazon 数据中心之间的流量。如果您未在中使用资源 Amazon Web Services 区域，则您的用户和资源之间的实际延迟可能与 Amazon 延迟数据有很大差异。即使您的资源与 Amazon Web Services 区域位于同一城市，也是如此。

要使用基于延迟的路由，您可以为多个 Amazon Web Services 区域中的资源创建延迟记录。当 Route 53 收到您的域或子域（example.com 或 apex.example.com）的 DNS 查询时，它确定您为哪些 Amazon Web Services 区域 创建了延迟记录、哪个区域能够为用户提供最低的延迟，然后选择该区域的延迟记录。Route 53 使用所选记录的值（例如 Web 服务器的 IP 地址）进行响应。

例如，假设您在美国西部（俄勒冈州）区域和亚太地区（新加坡）区域都有 Elastic Load Balancing 负载均衡器。您为每个负载均衡器创建了延迟记录。当位于伦敦的用户在浏览器中输入您的域名时，将出现以下情况：

1. DNS 将查询路由到 Route 53 名称服务器。
2. Route 53 查询其有关伦敦与新加坡区域以及伦敦与俄勒冈州区域之间延迟的数据。
3. 如果伦敦与俄勒冈州区域之间的延迟较低，则 Route 53 使用位于俄勒冈州的负载均衡器的 IP 地址响应查询。如果伦敦与新加坡区域之间的延迟较低，则 Route 53 使用位于新加坡的负载均衡器的 IP 地址响应查询。

由于网络连接和路由的变化，Internet 上主机之间的延迟不会一成不变。基于延迟的路由所依据的是在一段时间内执行的延迟测量，这些测量会反映上述变化。这周路由到俄勒冈区域的请求下周可能会被路由到新加坡区域。

> **Note**
>
> 当浏览器或其他查看器使用支持 EDNS0 edns-client-subnet 扩展的 DNS 解析器时，DNS 解析器会向 Route 53 发送用户 IP 地址的截断版本。如果您配置了基于延迟的路由，Route 53 在将流量路由到您的资源时会考虑该值。有关更多信息，请参阅 Amazon Route 53 如何使用 EDNS0 估计用户的位置。

可以对私有托管区中的记录使用延迟路由策略。

有关您在使用延迟路由策略创建记录时所指定值的信息，请参阅以下主题：

- 延迟记录的特定值
- 延迟别名记录的特定值
- 所有路由策略的通用值
- 所有路由策略的别名记录的通用值

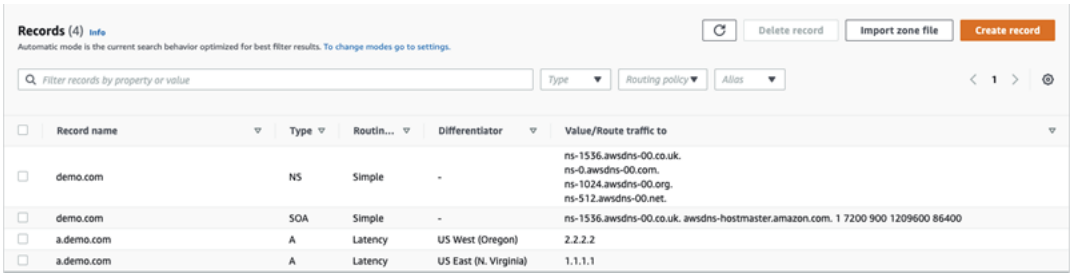
私有托管区中基于延迟的路由

对于私有托管区域，Route 53 使用与查询来源的 VPC 相同 Amazon Web Services 区域或距离最近的终端节点来回答 DNS 查询。 Amazon Web Services 区域

> **Note**
>
> 如果您将出站端点转发到入站端点，则记录将根据入站端点的位置而不是出站端点的位置进行解析。

如果包括运行状况检查，并且查询源延迟时间最短的记录运行状况不佳，则会返回延迟次低的运行状况良好的端点。

在下图的示例配置中，来自 us- Amazon Web Services 区域 east-1 或最接近它的 DNS 查询将路由到 1.1.1.1 终端节点。来自 us-west-2 或最接近它的 DNS 查询将被路由到 2.2.2.2 端点。



基于 IP 的路由

借助 Amazon Route 53 中基于 IP 的路由，您可以利用对网络、应用程序和客户端的了解来微调 DNS 路由，从而为最终用户做出最佳 DNS 路由决策。基于 IP 的路由通过以映射的形式将数据上传到 Route 53，使您可以精细控制以优化性能或降低网络成本。 user-IP-to-endpoint

地理位置和基于延迟的路由以 Route 53 收集并保持更新的数据为基础。这种方法适用于大多数客户，但基于 IP 的路由为您提供了额外的能力，可以根据您客户群的特定知识来优化路由。例如，全球视频内容提供商可能希望从特定互联网服务提供商（ISP）路由最终用户。

以下是基于 IP 的路由的一些常见使用案例：

- 您希望将最终用户从某些终端节点路由 ISPs 到特定的终端节点，以便优化网络传输成本或性能。
- 您希望根据对客户实际位置的了解，为现有 Route 53 路由类型添加覆盖，例如地理位置路由。

管理 IP 范围并将其与资源记录集关联 () RRSet

对于 IPv4，您可以使用长度介于 1 到 24 位（含）之间的 CIDR 块，而对于IPv6长度介于 1 到 48 位（含）之间的 CIDR 块。要定义零位 CIDR 块（0.0.0.0/0 或:: /0），请使用默认（“*”）位置。

对于 CIDR 长于 CIDR 集合中指定长度的 DNS 查询，Route 53 会将其与较短的 CIDR 进行匹配。例如，如果您在 CIDR 集合中指定 2001:0DB8:: /32 作为 CIDR 块，并且查询源自 2001:0:0000: DB8 1234:: /48，则该查询将匹配。另一方面，如果您在 CIDR 集合中指定 2001:0DB8: 0000:1234:: /48，并且查询源自 2001:0:: /32，则这将不匹配，Route 53 将使用默认（“DB8*”）位置的记录进行回答。

您可以将 CIDR 块（或 IP 范围）集组合到 CIDR 位置中，然后将这些区块组合为名为 CIDR 集合的可重用实体：

CIDR 块

采用 CIDR 表示法的 IP 范围，例如 192.0.2.0/24 或 2001:: /32。DB8

CIDR 位置

已命名的 CIDR 块列表。例如， example-isp-seattle= [192.0.2.0/24、203.0.113.0/22、198.51.100.0/24、2001:: /32]。DB8CIDR 位置列表中的块不必相邻或处于相同的范围内。

单个位置可以同时包含 IPv4 和 IPv6 块，并且此位置可以分别与 A 和 AAAA 记录集相关联。

例如，位置名称通常是一个位置，但也可以是任何字符串，例如，公司-A。

CIDR 集合

已命名的位置集合。例如，我的收藏 = [example-isp-seattle， example-isp-tokyo]。

基于 IP 的路由资源记录集会引用集合中的位置，并且具有相同记录集名称和类型的所有资源记录集必须引用同一个集合。例如，如果您在两个区域创建网站，并希望根据原始 IP 地址将 DNS 查询从两个不同的 CIDR 位置定向到特定网站，那么这两个位置都必须列在同一个 CIDR 集合中。

不能对私有托管区中的记录使用基于 IP 的路由策略。

有关您在使用基于 IP 的路由策略创建记录时所指定值的信息，请参阅以下主题：

- 针对基于 IP 的记录的特定值
- 基于 IP 的别名记录的特定值
- 所有路由策略的通用值

- 所有路由策略的别名记录的通用值

主题

- 使用 CIDR 位置和 CIDR 块创建 CIDR 集合
- 使用 CIDR 位置和 CIDR 块
- 删除 CIDR 集合
- 将地理位置移动到基于 IP 的路由

使用 CIDR 位置和 CIDR 块创建 CIDR 集合

要开始使用，请创建 CIDR 集合并向其添加 CIDR 块和位置。

使用 Route 53 控制台创建 CIDR 集合

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 IP-based routing（基于 IP 的路由），然后选择 CIDR collections（CIDR 集合）。
3. 选择 Create CIDR collection（创建 CIDR 集合）。
4. 在 Create CIDR collection（创建 CIDR 集合）窗格中，在 Details（详细信息）下方，输入集合的名称。
5. 选择 Create collection（创建集合）以创建空集合。

   –或者–

   在 创建 CIDR 位置部分中，于 CIDR 位置框中输入 CIDR 位置的名称。例如，位置名称可以是任何标识字符串，例如，**company 1** 或者 **Seattle**。它不必是实际的地理位置。

   > **Important**
   >
   > CIDR 位置名称的最大长度为 16 个字符。

   在 CIDR 块框中每行输入一个 CIDR 块。这些地址可以是 o IPv4 r IPv6 地址，范围为 /0 到 /24，对于 IPv4 /0 到 /48。 IPv6

6. 在输入 CIDR 块以后，选择 Create CIDR collection（创建 CIDR 集合）或 Add another location（添加其他位置），以继续输入位置和 CIDR 块。您可以在每个集合中输入多个 CIDR 位置。
7. 在输入 CIDR 位置后，选择 Create CIDR collection（创建 CIDR 集合）。

使用 CIDR 位置和 CIDR 块

通过 Route 53 控制台使用 CIDR 位置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择基于 IP 的路由），再选择 CIDR 集合，然后在 CIDR 集合部分，在集合名称列表中点击 CIDR 集合的链接。

   在 CIDR locations（CIDR 位置）页面中，您可以创建、删除 CIDR 位置，或者编辑位置及其 CIDR 块。

   - 要创建位置，请选择 Create CIDR location（创建 CIDR 位置）。
   - 在 Create CIDR location（创建 CIDR 位置）窗格中，输入位置的名称、与该位置关联的 CIDR 块，然后选择 Create（创建）。
   - 要查看 CIDR 位置和其中的 CIDR 块，请选择位置旁边的单选按钮，以在 CIDR 位置窗格中显示其名称和 CIDR 块。

     在此窗格中，您也可以选择编辑以更新位置或其 CIDR 块的名称。完成编辑后，选择 Save（保存）。
   - 要删除 CIDR 位置和其中的 CIDR 块，请选择您要删除的位置旁边的单选按钮，然后选择 Delete（删除）。要确认删除操作，请在文本输入字段中输入位置名称，然后选择 Delete（删除）。

   > **Important**
   >
   > 删除 CIDR 位置的操作无法撤消。如果您有与该位置关联的任何 DNS 记录，您的域可能会因此无法访问。

删除 CIDR 集合

要删除 CIDR 集合及其位置和块，需使用 Route 53 控制台

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 IP-based routing（基于 IP 的路由），然后选择 CIDR collections（CIDR 集合）。
3. 在 CIDR collections（CIDR 集合）部分，点击您要删除的集合的带有链接的名称。
4. 在 CIDR locations（CIDR 位置）页面中，每次选择一个位置，然后选择 Delete（删除），并在对话框中输入其名称，然后选择 Delete（删除）。您必须先删除与 CIDR 集合关联的所有位置，然后才能删除该集合。
5. 删完所有 CIDR 位置后，在 CIDR locations（CIDR 位置）页面中，选择您要删除的集合旁边的单选按钮，然后选择 Delete（删除）。

将地理位置移动到基于 IP 的路由

如果您使用的是地理位置或地理位置临近度路由策略，并且始终发现特定客户端路由目的地不是基于物理位置或网络拓扑的最佳端点，则可以使用基于 IP 的路由来更好地定向这些客户端的公有 IP 范围。

下表包含现有地理位置路由的示例地理位置配置，我们将针对加利福尼亚州 IP 范围进行微调。

记录集名称	路由策略和起源	应用程序端点的 IP 地址
example.com	地理位置路由（美国）	198.51.100.1
example.com	地理位置路由（欧洲）	198.51.100.2

要覆盖从加利福尼亚州到新的应用程序端点的 IP 范围，请首先使用新的记录集名称重新创建地理位置路由。

记录集名称	路由策略和起源	应用程序端点的 IP 地址
geo.example.com	地理位置路由（美国）	198.51.100.1
geo.example.com	地理位置路由（欧洲）	198.51.100.2

然后，创建基于 IP 的路由记录和指向您最近重新创建的地理位置路由记录集的默认记录。

记录集名称	路由策略和起源	应用程序端点的 IP 地址
example.com	基于 IP 的路由（默认）	您希望设置为默认值的 geo.example.com 应用程序端点的别名记录。例如 `198.51.100.1` 。
example.com	基于 IP 的路由（加利福尼亚州 IP 范围）	`198.51.100.3`

多值应答路由

多值应答路由允许您将 Amazon Route 53 配置为返回多个值（如您的 Web 服务器的 IP 地址）来响应 DNS 查询。您可以为几乎任意记录指定多个值，但多值应答路由也允许您检查每个资源的运行状况，以便 Route 53 只返回正常资源的值。虽然它不能替代负载均衡器，但由于其具备返回多个可进行运行状况检查的 IP 地址的能力，您可以将它与 DNS 配合使用，以提高可用性和负载均衡性。

要将流量以近乎随机的方式路由到多个资源（如 Web 服务器），请为每个资源创建一条多值应答记录，并（可选）将 Route 53 运行状况检查与每条记录关联。Route 53 通过最多八条正常记录响应 DNS 查询，并向不同的 DNS 解析程序提供不同的应答。如果 Web 服务器在解析程序缓存响应后变得不可用，则客户端软件可以尝试响应中提供的其他 IP 地址。

注意以下几点：

- 如果为多值应答记录关联了运行状况检查，则 Route 53 仅当运行状况检查正常时才使用相应的 IP 地址响应 DNS 查询。
- 如果您没有为多值应答记录关联运行状况检查，则 Route 53 始终认为记录正常。
- 如果您有不超过 8 条正常的记录，Route 53 将使用所有正常记录响应所有 DNS 查询。
- 如果所有记录都不正常，Route 53 会向 DNS 查询提供最多 8 条不正常的记录。

可以对私有托管区中的记录使用多值应答路由策略。

有关您在使用多值应答路由策略创建记录时所指定值的信息，请参阅 多值应答记录的特定值 和 所有路由策略的通用值。

加权路由

加权路由允许您将多个资源关联至单个域名 (example.com) 或子域名 (acme.example.com)，并选择向每个资源路由多少流量。这可用于多种用途，例如负载均衡、测试软件新版本等。

要配置加权路由，您可以创建与每个资源同名、同类型的记录，然后根据要发送到每个资源的流量的规模为每条记录分配相对权重。Amazon Route 53 将根据您分配给记录的权重（占该组中所有记录总权重的比例）向资源发送流量：

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

例如，如果您想要将极少的一部分流量发送到一个资源，并将其余流量发送到另一个资源，则可以指定权重 1 和 255。权重为 1 的资源将获得 1/256 (1/(1+255)) 的流量，另一个资源将获得 255/256 (255/(1+255)) 的流量。您可以通过更改权重来逐渐改变平衡。如果要停止向某个资源发送流量，您可以将该记录的权重更改为 0。

有关您在使加权路由策略创建记录时所指定值的信息，请参阅以下主题：

- 加权记录的特定值
- 加权别名记录的特定值
- 所有路由策略的通用值
- 所有路由策略的别名记录的通用值

可以对私有托管区中的记录使用加权路由策略。

运行状况检查和加权路由

如果为一组加权记录中的所有记录添加运行状况检查，但为部分记录指定非零权重并为其他记录指定零权重，那么运行状况检查会按照所有记录均具有非零权重的情况进行，但下列情况除外：

- Route 53 最初仅考虑非零加权记录（如果有）。
- 如果权重大于 0 的所有记录的运行状况都不良，Route 53 会考虑零权重的记录。

下表详细说明了 0 加权记录包含运行状况检查时的行为：

	记录 1	记录 2	记录 3
重量	1	1	0

	记录 1	记录 2	记录 3
包括运行状况检查？	支持	是	是
运行状态检查状态	运行状况不佳	运行状况不佳	正常
DNS 查询已回答？	否	否	是
运行状态检查状态	运行状况不佳	运行状况不佳	运行状况不佳
DNS 查询已回答？	支持	是	否
运行状态检查状态	运行状况不佳	正常	运行状况不佳
DNS 查询已回答？	否	是	否
运行状态检查状态	正常	正常	运行状况不佳
DNS 查询已回答？	支持	是	否
运行状态检查状态	正常	正常	正常
DNS 查询已回答？	支持	是	否

下表详细说明了 0 加权记录不包含运行状况检查时的行为：

	记录 1	记录 2	记录 3

	记录 1	记录 2	记录 3
重量	1	1	0
包括运行状况检查？	支持	是	否
运行状态检查状态	正常	正常	不适用
DNS 查询已回答？	支持	是	否
运行状态检查状态	运行状况不佳	运行状况不佳	不适用
DNS 查询已回答？	否	否	是
运行状态检查状态	运行状况不佳	正常	不适用
DNS 查询已回答？	否	是	否

Amazon Route 53 如何使用 EDNS0 估计用户的位置

为了提高地理定位、地理位置、基于 IP 的路由和延迟路由的准确性，Amazon Route 53 支持 EDNS0 的 edns-client-subnet扩展。（EDNS0 向 DNS 协议添加了几个可选扩展。）Route 53 edns-client-subnet 只能在 DNS 解析器支持的情况下使用：

- 当浏览器或其他查看器使用不支持的 DNS 解析器时 edns-client-subnet，Route 53 会使用 DNS 解析器的源 IP 地址来估计用户的位置，并使用解析器位置的 DNS 记录来响应地理位置查询。
- 当浏览器或其他查看器使用支持 edns-client-subnet的 DNS 解析器时，DNS 解析器会向 Route 53 发送用户 IP 地址的截断版本。Route 53 根据该截断的 IP 地址而不是 DNS 解析程序的源 IP 地址来确定用户的位置；这通常能够更准确地估计用户的位置。然后，Route 53 使用用户位置的 DNS 记录响应地理位置查询。
- EDNS0 不适用于私有托管区域。对于私有托管区域，Route 53 使用来自私有托管区域所在的 VPC 解析器的数据来做出地理位置和延迟路由决策。 Amazon Web Services 区域

有关更多信息 edns-client-subnet，请参阅 DNS 请求中的 EDNS 客户端子网 RFC，客户端子网。

在别名记录和非别名记录之间进行选择

Amazon Route 53 别名记录为 DNS 功能提供特定于 Route 53 的扩展。别名记录允许您将流量路由到选定 Amazon 资源，包括但不限于 CloudFront 分配和 Amazon S3 存储桶。它们还允许您将流量从托管区域中的一个记录路由到另一个记录。

与 CNAME 记录不同，您可以在 DNS 命名空间的顶端节点（又称为顶级域名）上创建别名记录。例如，如果您注册了 DNS 名称 example.com，则顶级域名为 example.com。您不能为 example.com 创建 CNAME 记录，但可以为 example.com 创建一条会将流量路由到 www.example.com 的别名记录（前提是 www.example.com 的记录类型不是 CNAME 类型）。

Route 53 收到针对别名记录的 DNS 查询时，Route 53 使用该资源的适用值响应：

- Amazon API Gateway 自定义区域 API 或边缘优化 API - Route 53 使用您的 API 的一个或多个 IP 地址响应。
- Amazon VPC 接口终端节点 - Route 53 使用您的接口终端节点的一个或多个 IP 地址响应。
- CloudFront 分发 — Route 53 使用一个或多个 IP 地址作为响应，这些服务器可以提供您的内容的 CloudFront 边缘服务器。
- App Runner 服务 - Route 53 使用一个或多个 IP 地址来响应。
- Elastic Beanstalk 环境 - Route 53 使用环境的一个或多个 IP 地址来响应。
- Elastic Load Balancing 负载均衡器 - Route 53 使用负载均衡器的一个或多个 IP 地址来响应。这包括应用程序负载均衡器、经典负载均衡器和网络负载均衡器。
- Amazon Global Accelerator 加速器 — Route 53 使用加速器的 IP 地址进行响应。
- OpenSearch 服务 — Rout e 53 使用 OpenSearch 服务自定义域的一个或多个 IP 地址进行响应。
- 配置为静态网站的 Amazon S3 存储桶 - Route 53 使用 Amazon S3 存储桶的一个 IP 地址来响应。
- 同一托管区中同类型的其他 Route 53 记录 – Route 53 会如同查询针对由别名记录所引用的记录一样做出响应（请参阅 别名记录和 CNAME 记录的比较）。
- Amazon AppSync 域名 — Route 53 使用您的接口终端节点的一个或多个 IP 地址进行响应。

有关更多信息，请参阅 将互联网流量路由到您的 Amazon 资源。

当您使用别名记录将流量路由到 Amazon 资源时，Route 53 会自动识别资源中的更改。例如，假设 example.com 的一个别名记录指向位于 lb1-1234.us-east-2.elb.amazonaws.com 上的一个 Elastic

Load Balancing 负载均衡器。如果负载均衡器的 IP 地址更改，Route 53 将使用新 IP 地址自动开始响应 DNS 查询。

如果别名记录指向 Amazon 资源，则无法设置生存时间 (TTL)；Route 53 使用该资源的默认 TTL。如果某个别名记录指向同一托管区域中的另一个记录，则 Route 53 将使用该别名记录指向的记录的 TTL。有关 Elastic Load Balancing 当前 TL 值的更多信息，请转到 Elastic Load Balancing 用户指南中的请求路由选择并搜索“ttl”。

有关使用 Route 53 控制台创建记录的更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。有关为别名记录指定的值的信息，请参阅在您创建或编辑 Amazon Route 53 记录时指定的值中的相关主题：

- 简单别名记录的特定值
- 加权别名记录的特定值
- 延迟别名记录的特定值
- 故障转移别名记录的特定值
- 地理位置别名记录的特定值
- 地理位置临近度别名记录的特定值
- 所有路由策略的别名记录的通用值

别名记录和 CNAME 记录的比较

别名记录与 CNAME 记录类似，但有一些重要的区别。以下列表比较别名记录和 CNAME 记录。

您可以将查询重定向到的资源

别名记录

别名记录只能将查询重定向到选定 Amazon 资源，包括但不限于以下资源：

- Amazon S3 存储桶
- CloudFront 分布
- 同一 Route 53 托管区域中的其它记录

例如，您可以创建一个名为 acme.example.com 的别名记录，该记录将查询重定向到 Amazon S3 存储桶（也称为 acme.example.com）。您还可以创建一个 acme.example.com 别名记录，该记录将查询重定向到 example.com 托管区域中名为 zenith.example.com 的记录。

CNAME 记录

CNAME 记录可以将 DNS 查询重定向到任何 DNS 记录。例如，您可以创建一条 CNAME 记录，该记录将查询从 acme.example.com 重定向到 zenith.example.com 或 acme.example.org。您不需要使用 Route 53 作为您要将查询重定向到的域的 DNS 服务。

创建与域同名的记录（顶级域名处的记录）

别名记录

在大多数配置中，您可以创建一个与托管区域（区域 APEX）同名的别名记录。一个例外情况是，当您要将来自区域 APEX（如 example.com）的查询重定向到具有类型 CNAME（如 zenith.example.com）的同一托管区域中的记录时。别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为顶级域名创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

CNAME 记录

您不能创建与托管区域（区域 APEX）同名的 CNAME 记录。对于域名 (example.com) 的托管区域和子域 (zenith.example.com) 的托管区域都是如此。

DNS 查询的定价

别名记录

Route 53 不对 Amazon 资源的别名查询收费。有关更多信息，请参阅 Amazon Route 53 定价。

CNAME 记录

Route 53 收取 CNAME 查询费用。

> **Note**
>
> 如果您创建一条 CNAME 记录，此记录重定向到 Route 53 托管区域（同一托管区域或另一托管区域）中另一条记录的名称，则每个 DNS 查询作为两个查询收费：
>
> - Route 53 以要重定向到的记录的名称响应第一个 DNS 查询。
> - 然后，DNS 解析程序必须对于第一个响应中的记录提交另一个查询，以获取有关将流量定向到何处的信息，例如 Web 服务器的 IP 地址。
>
> 如果 CNAME 记录重定向到由另一个 DNS 服务托管的记录的名称，则 Route 53 对一个查询收取费用。另一个 DNS 服务可能会对第二个查询收取费用。

在 DNS 查询中指定的记录类型

别名记录

仅当别名记录的名称（如 acme.example.com）和别名记录的类型（如 A 或 AAAA）与 DNS 查询中的名称和类型匹配时，Route 53 才响应 DNS 查询。

CNAME 记录

无论在 DNS 查询中指定的记录类型是什么（如 A 或 AAAA），CNAME 记录都会重定向对记录名称的 DNS 查询。

记录在 dig 或 nslookup 查询中如何列出

别名记录

在对 dig 或 nslookup 查询的响应中，别名记录以您在创建记录时指定的记录类型列出，例如 A 或 AAAA。（您为别名记录指定的记录类型取决于您要将流量路由到的资源。例如，要将流量路由到 S3 存储桶，请指定 A 作为类型。）别名属性仅在 Route 53 控制台或对编程请求（例如 Amazon CLI `list-resource-record-sets` 命令）的响应中可见。

CNAME 记录

CNAME 记录在响应 dig 或 nslookup 查询时作为 CNAME 记录列出。

支持的 DNS 记录类型

Amazon Route 53 支持本节中列出的 DNS 记录类型。每个记录类型还包括当您使用 API 访问 Route 53 时如何设置 `Value` 元素格式的示例。

> **Note**
>
> 对于包含域名的记录类型，请输入一个完全限定域名，例如 www.example.com。结尾圆点是可选的；Route 53 会假定该域名是完全限定的。这意味着，Route 53 会将 www.example.com（不包含结尾圆点）和 www.example.com.（包含结尾圆点）视为相同。

Route 53 为 DNS 功能提供了一个名为别名记录的扩展。与 CNAME 记录类似，别名记录允许您将流量路由到所选 Amazon 资源，如 CloudFront 分配和 Amazon S3 存储桶。有关更多信息，包括别名记录和 CNAME 记录的比较，请参阅在别名记录和非别名记录之间进行选择。

主题

A 记录类型

使用 A 记录将流量路由到资源（如 Web 服务器），并使用圆点分隔的十进制格式表示的 IPv4 地址。

Amazon Route 53 控制台示例

```
192.0.2.1
```

Route 53 API 示例

```
<Value>192.0.2.1</Value>
```

AAAA 记录类型

使用 AAAA 记录将流量路由到资源（如 Web 服务器），并使用圆点分隔的十六进制格式表示的 IPv6 地址。

Amazon Route 53 控制台示例

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Route 53 API 示例

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA 记录类型

CAA 记录指定允许哪些证书颁发机构 (CA) 为域或子域颁发证书。创建 CAA 记录有助于防止错误的 CA 为您的域颁发证书。CAA 记录不能替代由您的证书颁发机构指定的安全要求，例如验证您是域所有者的要求。

您可以使用 CAA 记录指定以下内容：

- 哪些证书颁发机构 (CA) 可以签发 SSL/TLS 证书 (如果有)
- CA 为域或子域签发证书时要联系的电子邮件地址或 URL

当您将 CAA 记录添加到托管区域时，您可以指定由空格分隔的三个设置：

```
flags tag "value"
```

请注意有关 CAA 记录的格式的以下事项：

- `tag` 的值只能包含字符 A-Z、a-z 和 0-9。
- 始终用引号 ("") 将 `value` 引起来。
- 一些 CA 允许或需要 `value`。以名称-值对的形式指定其他值，并以分号 (;) 分隔，例如：

  ```
  0 issue "ca.example.net; account=123456"
  ```
- 如果某个 CA 接收了对某个子域 (如 www.example.com) 的证书的请求并且该子域没有 CAA 记录，则该 CA 将提交对父域 (如 example.com) 的 CAA 记录的 DNS 查询。如果父域的记录存在，并且证书请求有效，则 CA 会为子域颁发证书。
- 我们建议您咨询您的 CA 来确定要为 CAA 记录指定的值。
- 您不能创建名称相同的 CAA 记录和 CNAME 记录，因为 DNS 不允许 CNAME 记录和任何其他类型的记录使用相同的名称。

主题

授权 CA 为域或子域颁发证书

要授权 CA 为域或子域颁发证书，请创建一条与域或子域同名的记录，并指定以下设置：

- 标签 - `0`
- 标签 - `issue`
- 值 - 您授权为域或子域颁发证书的 CA 的代码

例如，假设您要授权 ca.example.net 为 example.com 颁发证书。您为 example.com 创建了一条具有以下设置的 CAA 记录：

```
0 issue "ca.example.net"
```

有关如何授权 Amazon Certificate Manager 颁发证书的信息，请参阅 Amazon Certificate Manager 用户指南中的配置 CAA 记录。

授权 CA 为域或子域颁发通配符证书

要授权 CA 为域或子域颁发通配符证书，请创建一条与域或子域同名的记录，并指定以下设置。通配符证书适用于该域或子域及其所有子域。

- 标签 - `0`
- 标签 - `issuewild`
- 值 - 您授权为域或子域以及它们的子域颁发证书的 CA 的代码

例如，假设您要授权 ca.example.net 为 example.com 颁发通配符证书 (适用于 example.com 及其所有子域)。您为 example.com 创建了一条具有以下设置的 CAA 记录：

```
0 issuewild "ca.example.net"
```

当您要授权 CA 为域或子域颁发通配符证书时，请创建一条与域或子域同名的记录，并指定以下设置。通配符证书适用于该域或子域及其所有子域。

阻止任何 CA 为域或子域颁发证书

要阻止任何 CA 为域或子域颁发通配符证书，请创建一条与域或子域同名的记录，并指定以下设置：

- 标签 - `0`
- 标签 - `issue`
- 值 – `";"`

例如，假设您不希望任何 CA 为 example.com 颁发证书。您为 example.com 创建了一条具有以下设置的 CAA 记录：

```
0 issue ";"
```

如果您不希望任何 CA 为 example.com 或其子域颁发证书，则可以为 example.com 创建一条具有以下设置的 CAA 记录：

```
0 issuewild ";"
```

> **Note**
>
> 如果您为 example.com 创建了 CAA 记录并指定了以下两个值，使用值 ca.example.net 的 CA 可以为 example.com 颁发证书：
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

请求任何 CA 在收到无效的证书请求时联系您

如果您希望收到对证书的无效请求的任何 CA 联系您，请指定以下设置：

- 标签 - `0`
- 标签 - `iodef`

- 值 - 您希望 CA 在收到无效的证书请求时通知的 URL 或电子邮件地址。使用适用的格式：

  "mailto:*email-address*"

  "http://*URL*"

  "https://*URL*"

例如，如果您希望收到对证书的无效请求的任何 CA 向 admin@example.com 发送电子邮件，则可以创建一条具有以下设置的 CAA 记录：

```
0 iodef "mailto:admin@example.com"
```

使用 CA 支持的另一个设置

如果您的 CA 支持未在 CAA 记录的 RFC 中定义的功能，请指定以下设置：

- 标记 - 128（如果 CA 不支持指定的功能，此值会阻止 CA 颁发证书。）
- 标签 - 您授权 CA 使用的标签
- 值 - 与标签的值对应的值

例如，假设您的 CA 在收到无效的证书请求时支持发送文本消息。(我们不了解支持此选项的任何 CA。) 记录的设置可能如下所示：

```
128 exampletag "15555551212"
```

示例

Route 53 控制台示例

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Route 53 API 示例

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
```

```
</ResourceRecord>
```

CNAME 记录类型

别名记录将当前记录的名称（例如 acme.example.com）的 DNS 查询映射到另一个域（example.com 或 example.net）或子域（acme.example.com 或 zenith.example.org）。

> **Important**
>
> DNS 协议不允许您为 DNS 命名空间的顶端节点（也称为区域顶点）创建别名记录 (CNAME)。例如，如果您注册了 DNS 名称 example.com，则顶级域名为 example.com。您不能为 example.com 创建 CNAME 记录，但可以为 www.example.com、newproduct.example.com 等创建 CNAME 记录。
> 此外，如果您为某个子域创建 CNAME 记录，则不能为该子域创建任何其他记录。例如，如果您为 www.example.com 创建别名记录，则不能创建其 Name (名称) 字段的值为 www.example.com 的任何其他记录。

Amazon Route 53 还支持别名记录，这使得您可以将查询路由到所选 Amazon 资源，例如 CloudFront 分配和 Amazon S3 存储桶。别名在某些方面与 CNAME 记录类型类似；不过，您可以为顶级域名创建一个别名。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

Route 53 控制台示例

```
hostname.example.com
```

Route 53 API 示例

```
<Value>hostname.example.com</Value>
```

DS 记录类型

委派签名者 (DS) 记录引用委派子域区域的区域密钥。如果您在配置 DNSSEC 签名时建立信任链，您可能会创建 DS 记录。有关在 Route 53 中配置 DNSSEC 的更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

前三个值是表示密钥标签、算法和摘要类型的十进制数。第四个值是区域密钥的摘要。有关 DS 记录格式的更多信息，请参阅 RFC 4034。

Route 53 控制台示例

```
123 4 5 1234567890abcdef1234567890absdef
```

Route 53 API 示例

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

HTTPS 记录类型

HTTPS 资源记录是服务绑定（SVCB）DNS 记录的一种形式，它提供扩展的配置信息，使客户端能够通过 HTTP 协议轻松安全地连接到服务。配置信息以参数形式提供，这些参数允许在一个 DNS 查询中进行连接，而不必进行多个 DNS 查询。

HTTPS 资源记录的格式为：

```
SvcPriority TargetName SvcParams(optional)
```

RFC 9460 第 9.1 节中描述了以下参数。

SvcPriority

表示优先级的整数。0 优先级表示别名模式，通常用于在顶级域中设置别名。对于 Route 53，此值是整数 0-32767，其中 1-32767 是服务模式记录。优先级越低，首选项越高。

TargetName

别名目标（用于别名模式）或备用端点（用于服务模式）的域名。

SvcParams（可选）

以空格分隔的列表，每个参数都由键值对或独立键组成。如果有多个值，则以逗号分隔的列表显示这些值。以下是定义的 SvcParams：

- `1:alpn` – 应用程序层协议协商协议 ID 默认为 HTTP/1.1，h2 是 TLS 上的 HTTP/2，h3 是 HTTP/3（QUIC 协议上的 HTTP）。
- `2:no-default-alpn` – 不支持默认值，您必须提供 `alpn` 参数。
- `3:port` – 替代端点或可以到达服务的端口。
- `4:ipv4hint` – IPv4 地址提示。
- `5:ech` – 加密的客户端 Hello。
- `6:ipv6hint` – IPv6 地址提示。

- 7:dohpath – HTTPS 上的 DNS 模板
- 8:ohttp – 该服务运作 Oblivious HTTP 目标

适用于别名模式的 Amazon Route 53 控制台示例

```
0 example.com
```

适用于服务模式的 Amazon Route 53 控制台示例

```
16 example.com alpn="h2,h3" port=808
```

适用于别名模式的 Amazon Route 53 API 示例

```
<Value>0 example.com</Value>
```

适用于服务模式的 Route 53 API 示例

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

有关更多信息，请参阅 RFC 9460，通过 DNS 的服务绑定和参数规范（SVCB 和 HTTPS 资源记录）。

> **Note**
>
> Route 53 不支持任意的未知密钥表示格式 keyNNNNN

MX 记录类型

MX 记录指定邮件服务器的名称，如果您有两个或多个邮件服务器，则指定优先级顺序。MX 记录的每个值都包含两个值，即优先级和域名。

优先级

表示电子邮件服务器优先级的一个整数。如果只指定一个服务器，则优先级可以是 0 到 65535 之间的任意整数。如果指定多个服务器，则为优先级指定的值指示您要将邮件路由到第一个、第二个等电子邮件服务器中的哪一个。优先级值最低的服务器优先。例如，如果您有两个电子邮件服务器，

并且为优先级指定值 10 和 20，则电子邮件始终会路由到优先级为 10 的服务器 (除非该服务器不可用)。如果您指定值为 10 和 10，则电子邮件会大致同等地路由到两个服务器。

域名

电子邮件服务器的域名。指定 A 或 AAAA 记录的名称 (如 mail.example.com)。在 RFC 2181, Clarifications to the DNS Specification 中，10.3 小节禁止为域名值指定 CNAME 记录的名称。（当 RFC 提到“别名”时，指的是 CNAME 记录，而不是 Route 53 别名记录。）

Amazon Route 53 控制台示例

```
10 mail.example.com
```

Route 53 API 示例

```
<Value>10 mail.example.com</Value>
```

NAPTR 记录类型

名称权威指针 (NAPTR) 是动态授权发现系统 (DDDS) 应用程序用于将一个值转换为另一个值或将一个值替换为另一个值的一种记录类型。例如，一个常见的用途是将电话号码转换为 SIP URI。

NAPTR 记录的 `Value` 元素包含六个以空格分隔的值：

订单

当您指定多个记录时，您希望 DDDS 应用程序评估记录的顺序。有效值：0 - 65535。

Preference

当您指定具有相同 Order 的两个或更多记录时，您评估这些记录的顺序首选项。例如，如果两个记录的 Order 为 1，则 DDDS 应用程序首先会评估具有较低 Preference 的记录。有效值：0 - 65535。

Flags

特定于 DDDS 应用程序的一个设置。RFC 3404 中当前定义的值为大写字母和小写字母 "A"、"P"、"S" 和 "U"，以及空字符串 ""。将 Flags 用引号引起来。

服务

特定于 DDDS 应用程序的一个设置。将 Service 用引号引起来。

有关更多信息，请参阅适用的 RFC：

- URI DDDS 应用程序 - https://tools.ietf.org/html/rfc3404#section-4.4
- S-NAPTR DDDS 应用程序 - https://tools.ietf.org/html/rfc3958#section-6.5
- U-NAPTR DDDS 应用程序 - https://tools.ietf.org/html/rfc4848#section-4.5

Regexp

DDDS 应用程序用于将输入值转换为输出值的一个正则表达式。例如，IP 电话系统可使用一个正则表达式将用户输入的电话号码转换为 SIP URI。将 Regexp 用引号引起来。为 Regexp 指定一个值，或者为 Replacement 指定一个值，但不要同时为这两者指定值。

该正则表达式可包含以下任何可打印 ASCII 字符：

- a-z
- 0-9
- - (连字符)
- (space)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (引号)。要在字符串中包含引号字符，请在它前面加上 \ 字符：\"。
- \ (反斜杠)。要在字符串中包含反斜杠，请在它前面加上 \ 字符：\\。

以八进制格式指定所有其他值，例如国际化域名。

有关 Regexp 的语法，请参阅 RFC 3402 的第 3.2 节“Substitution Expression Syntax”

Replacement

您希望 DDDS 应用程序对其提交 DNS 查询的下一个域名的完全限定域名 (FQDN)。DDDS 应用程序会用您为 Replacement 指定的值 (如果有) 来替换输入值。为 Regexp 指定一个值，或者为 Replacement 指定一个值，但不要同时为这两者指定值。如果您为 Regexp 指定了一个值，请为替换指定一个圆点 (.)。

域名可以包含 a-z、0-9 和 - (连字符)。

有关 DDDS 应用程序和 NAPTR 记录的更多信息，请参阅以下 RFC：

- RFC 3401
- RFC 3402
- RFC 3403

- RFC 3404

Amazon Route 53 控制台示例

```
100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Route 53 API 示例

```
<ResourceRecord>
   <Value>100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .</Value>
   <Value>100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .</
Value>
   <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

NS 记录类型

NS 记录会标识托管区域的名称服务器。请注意以下几点：

- NS 记录的最常见用途是控制域的 Internet 流量路由方式。要使用托管区域中的记录路由域的流量，请更新域注册设置以使用默认 NS 记录中的四个名称服务器。（这是与托管区域同名的 NS 记录。）
- 您可以为子域 (acme.example.com) 创建单独的托管区域，并使用该托管区域为子域及其子域 (subdomain.acme.example.com) 路由 Internet 流量。您可以通过在根域的托管区域 (example.com) 中创建另一个 NS 记录来设置此配置，称为 "将子域的责任委托给托管区域"。有关更多信息，请参阅路由子域的流量。
- 您还可以使用 NS 记录配置白标名称服务器。有关更多信息，请参阅 配置白标签名称服务器。
- NS 记录的另一个用途是私有托管区，当您创建委托规则将子域的授权委托给本地解析器时，即可使用 NS 记录。在创建委托规则之前，必须创建此 NS 记录。有关更多信息，请参阅 解析器端点如何将您的 DNS 查询转发 VPCs 到您的网络。

有关 NS 记录的更多信息，请参阅 Amazon Route 53 为公有托管区域创建的 NS 和 SOA 记录。

Amazon Route 53 控制台示例

```
ns-1.example.com
```

Route 53 API 示例

```
<Value>ns-1.example.com</Value>
```

PTR 记录类型

PTR 记录将 IP 地址映射到相应的域名。

Amazon Route 53 控制台示例

```
hostname.example.com
```

Route 53 API 示例

```
<Value>hostname.example.com</Value>
```

SOA 记录类型

授权起始点 (SOA) 记录会提供有关域和相应 Amazon Route 53 托管区域的信息。有关 SOA 记录中的字段的信息，请参阅 Amazon Route 53 为公有托管区域创建的 NS 和 SOA 记录。

Route 53 控制台示例

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Route 53 API 示例

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF 记录类型

SPF 记录以前用于验证电子邮件发件人的身份。但是，不再建议您创建记录类型为 SPF 的记录。RFC 7208 中的 Sender Policy Framework（SPF）for Authorizing Use of Domains in Email, Version 1（在电子邮件中授权使用域的发件人策略框架（SPF），版本 1）已更新为：“...[I]ts existence and mechanism defined in [RFC4408] have led to some interoperability issues。Accordingly, its use is no longer appropriate for SPF version 1; implementations are not to use it.“（...在 [RFC4408] 中定义的其存在和机制已导致一些互操作性问题。因此，它已不再适合 SPF 版本 1；实施方案中不应再使用它。）在 RFC 7208 中，请参阅第 14.1 节 SPF DNS 记录类型。

建议您创建一个包含适用值的 TXT 记录，而不是 SPF 记录。有关有效值的更多信息，请参阅维基百科文章发件人策略框架。

Amazon Route 53 控制台示例

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API 示例

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV 记录类型

SRV 记录 `Value` 元素包含四个以空格分隔的值。前三个值为分别是表示优先级、权重和端口的十进制数。第四个值为一个域名。SRV 记录用于访问服务，例如电子邮件或通信服务。有关 SRV 记录格式的信息，请参阅要连接到的服务的文档。

Amazon Route 53 控制台示例

```
10 5 80 hostname.example.com
```

Route 53 API 示例

```
<Value>10 5 80 hostname.example.com</Value>
```

SSHFP 记录类型

安全 Shell 指纹记录（SSHFP）可识别与域名关联的 SSH 密钥。为建立信任链，必须使用 DNSSEC 保护 SSHFP 记录。有关 DNSSEC 的更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

SSHFP 资源记录的格式为：

```
[Key Algorithm] [Hash Type] Fingerprint
```

以下参数在 RFC 4255 中定义。

密钥算法

算法类型：

- 0 – 已保留且未使用。
- 1： RSA – Rivest–Shamir–Adleman 算法是最早的公有密钥密码系统之一，至今仍用于安全的数据传输。
- 2： DSA – 数字签名算法是用于数字签名的联邦信息处理标准。DSA 基于模幂和离散对数数学模型。
- 3： ECDSA – 椭圆曲线数字签名算法是使用椭圆曲线密码学的 DSA 变体。
- 4： Ed25519 – Ed25519 算法是使用 SHA-512（SHA-2）和 Curve25519 的 EdDSA 签名方案。
- 6： Ed448 – Ed448 是使用 SHAKE256 和 Curve448 的 EdDSA 签名方案。

哈希类型

用于创建公有密钥哈希的算法：

- 0 –已保留且未使用。
- 1： SHA-1
- 2： SHA-256

指纹

哈希的十六进制表示。

Amazon Route 53 控制台示例

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Route 53 API 示例

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

有关更多信息，请参阅 RFC 4255：使用 DNS 安全发布 Secure Shell（SSH）密钥指纹。

SVCB 记录类型

您可以使用 SVCB 记录来传送访问服务端点的配置信息。SVCB 是一种通用 DNS 记录，可用于协商各种应用协议的参数。

SVCB 资源记录的格式为：

```
SvcPriority TargetName SvcParams(optional)
```

RFC 9460 第 2.3 节中描述了以下参数。

SvcPriority

表示优先级的整数。0 优先级表示别名模式，通常用于在顶级域中设置别名。优先级越低，首选项越高。

TargetName

别名目标（用于别名模式）或备用端点（用于服务模式）的域名。

SvcParams（可选）

以空格分隔的列表，每个参数都由键值对或独立键组成。如果有多个值，则以逗号分隔的列表显示这些值。对于 Route 53，此值是整数 0-32767，其中 1-32767 是服务模式记录。以下是定义的 SvcParams：

- `1:alpn` – 应用程序层协议协商协议 ID 默认为 HTTP/1.1，h2 是 TLS 上的 HTTP/2，h3 是 HTTP/3（QUIC 协议上的 HTTP）。
- `2:no-default-alpn` – 不支持默认值，您必须提供 `alpn` 参数。
- `3:port` – 可以访问服务的替代端点的端口。
- `4:ipv4hint` – IPv4 地址提示。
- `5:ech` – 加密的客户端 Hello。
- `6:ipv6hint` – IPv6 地址提示。
- `7:dohpath` – HTTPS 上的 DNS 模板
- `8:ohttp` – 该服务运作 Oblivious HTTP 目标

适用于别名模式的 Amazon Route 53 控制台示例

```
0 example.com
```

适用于服务模式的 Amazon Route 53 控制台示例

```
16 example.com alpn="h2,h3" port=808
```

适用于别名模式的 Amazon Route 53 API 示例

```
<Value>0 example.com</Value>
```

适用于服务模式的 Route 53 API 示例

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

有关更多信息，请参阅 RFC 9460，通过 DNS 的服务绑定和参数规范（SVCB 和 HTTPS 资源记录）。

> **Note**
>
> Route 53 不支持任意的未知密钥表示格式 `keyNNNNN`

TLSA 记录类型

您可以借助 TLSA 记录来使用基于 DNS 的命名实体身份验证（DANE）。TLSA 记录将证书/公有密钥与传输层安全性协议（TLS）端点相关联，客户端可以使用以 DNSSEC 签名的 TLSA 记录来验证证书/公有密钥。

只有在您的域上启用 DNSSEC 后，才可信任 TLSA 记录。有关 DNSSEC 的更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

TLSA 资源记录的格式为：

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

以下参数在 RFC 6698 的第 3 节中指定。

证书用量

指定提供的关联，该关联将用于与 TLS 握手中展示的证书相匹配：

- 0：CA 约束 – 必须在服务器在 TLS 中提供的端点实体证书的任意公有密钥基础设施（PKIX）认证路径中找到证书或公有密钥。此约束限制哪些 CA 可用于为指定的服务颁发证书。
- 1：服务证书约束 – 指定端点实体证书（或公有密钥），该证书必须与服务器在 TLS 中提供的端点实体证书相匹配。此认证限制主机上的指定服务可以使用的端点实体证书。
- 2：信任锚断言 – 指定在验证服务器在 TLS 中提供的端点实体证书时必须用作“信任锚”的证书（或公有密钥）。允许域管理员指定信任锚。
- 3：域颁发的证书 – 指定必须与服务器在 TLS 中提供的端点实体证书相匹配的证书（或公有密钥）。该认证允许域管理员在不涉及第三方 CA 的情况下为域颁发证书。此证书不需要通过 PKIX 验证。

选择器

指定服务器在握手中所提供证书的哪一部分与关联值相匹配：

- 0：必须匹配整个证书。
- 1：必须匹配主题公有密钥或 DER 编码的二进制结构。

匹配类型

指定证书匹配项的显示方式（由“选择器”字段确定）：

- 0：内容完全匹配。
- 1：SHA-256 哈希。
- 2：SHA-512 哈希。

证书关联数据

要根据其他字段的设置进行匹配的数据。

Amazon Route 53 控制台示例

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Route 53 API 示例

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

有关更多信息，请参阅 RFC 6698，基于 DNS 的命名实体身份验证（DANE）传输层安全性协议（TLS）协议：TLSA。

TXT 记录类型

TXT 记录包含一个或多个用双引号 ('') 引起的字符串。当您使用简单路由策略时，请将域 (example.com) 或子域 (www.example.com) 的所有值包含在同一 TXT 记录中。

主题

- 输入 TXT 记录值
- TXT 记录值中的特殊字符
- TXT 记录值中的大写字符和小写字符

- 示例

输入 TXT 记录值

单个字符串最多可包含 255 个字符，包括以下内容：

- a-z
- A-Z
- 0-9
- 空格
- - (连字符)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

如果您需要输入长度大于 255 个字符的值，请将该值分解为包含 255 个字符或更少字符的字符串，并将每个字符串用双引号 (") 括起来。在控制台中的同一行上，列出所有字符串：

```
"String 1" "String 2" "String 3"
```

对于 API，在同一 Value 元素中包含所有字符串：

```
<Value>"String 1" "String 2" "String 3"</Value>
```

TXT 记录中的值的最大长度为 4000 个字符。

要输入多个 TXT 值，请每行输入一个值。

TXT 记录值中的特殊字符

如果您的 TXT 记录包含以下任意字符，则必须使用 \###格式的转义码指定字符：

- 八进制字符 000 到 040 (十进制 0 到 32，十六进制 0x00 到 0x20)
- 八进制字符 177 到 377 (十进制 127 到 255，十六进制 0x7F 到 0xFF)

例如，如果您的 TXT 记录的值为 "exämple.com"，则应指定 "ex\344mple.com"。

有关 ASCII 字符和八进制代码之间的映射，请在 Internet 上搜索“ASCII 八进制代码”。一个有用的参考是 ASCII 代码 – 扩展 ASCII 表。

要将引号 (") 包含在字符串中，请在引号前面放置反斜杠 (\) 字符：\"。

TXT 记录值中的大写字符和小写字符

大小写将被保留，因此 "Ab" 和 "aB" 是不同的值。

示例

Amazon Route 53 控制台示例

在单独的行中放置每个值：

```
"This string includes \"quotation marks\"."
"The last character in this string is an accented e specified in octal format: \351"
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API 示例

在单独的 Value 元素中放置每个值：

```
<Value>"This string includes \"quotation marks\"."</Value>
<Value>"The last character in this string is an accented e specified in octal format:
 \351"</Value>
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

通过使用 Amazon Route 53 控制台创建记录

以下步骤介绍如何使用 Amazon Route 53 控制台创建记录。有关如何使用 Route 53 API 创建记录的信息，请参阅亚马逊 Route 53 API 参考ChangeResourceRecordSets中的。

> **Note**
>
> 要为复杂的路由配置创建记录，您也可以使用 Traffic Flow 可视化编辑器，并将配置保存为流量策略。然后，您可以将流量策略关联至同一托管区域或多个托管区域中的一个或多个域名 (例如 example.com) 或子域名 (例如 www.example.com)。此外，如果新配置无法正常工作，您还可以回滚更新。有关更多信息，请参阅 使用 Traffic Flow 来路由 DNS 流量。

使用 Route 53 控制台创建记录

1. 如果您不打算创建别名记录，请转至步骤 2。

如果您要创建别名记录，将 DNS 流量路由到 Elastic Load Balancing 负载均衡器或其他 Route 53 记录以外的 Amazon 资源，则还要转到步骤 2。

如果您打算创建别名记录以将流量路由到 Elastic Load Balancing 负载均衡器，并且已使用不同账户创建了托管区和负载均衡器，则执行过程 获取 Elastic Load Balancing 负载均衡器的 DNS 名称 以获取负载均衡器的 DNS 名称。

2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 如果您的域已有托管区域，则跳至步骤 5。如果没有，请执行相关步骤以创建托管区域：

   - 要将互联网流量路由到您的资源，例如 Amazon S3 存储桶或 Amazon EC2 实例，请参阅创建公有托管区域。
   - 要路由 VPC 中的流量，请参阅创建私有托管区域。
5. 在 Hosted Zones（托管区域）页面上，选择您要在其中创建记录的托管区域的名称。
6. 选择创建记录。
7. 选择并定义适用的路由策略和值。有关更多信息，请参阅关于您要创建的记录类别的主题：

   - 所有路由策略的通用值
   - 所有路由策略的别名记录的通用值
   - 简单记录的特定值
   - 简单别名记录的特定值
   - 故障转移记录的特定值
   - 故障转移别名记录的特定值
   - 地理位置记录的特定值
   - 地理位置别名记录的特定值
   - 地理位置临近度记录的特定值
   - 地理位置临近度别名记录的特定值
   - 延迟记录的特定值
   - 延迟别名记录的特定值
   - 针对基于 IP 的记录的特定值
   - 基于 IP 的别名记录的特定值
   - 多值应答记录的特定值

- 加权记录的特定值
- 加权别名记录的特定值

8. 选择创建记录。

> **Note**
>
> 您的新记录需要一定时间才会传播到 Route 53 DNS 服务器。目前，验证更改是否已传播的唯一方法是使用 GetChangeAPI 操作。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

9. 如果您要创建多个记录，则重复步骤 7 至 8。

获取 Elastic Load Balancing 负载均衡器的 DNS 名称

1. Amazon Web Services 管理控制台 使用用于创建您想要为其创建别名记录的 Classic、Application 或 Network Load Balancer 的 Amazon 账户登录。
2. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择负载均衡器。
4. 在负载均衡器列表中，选择您要为其创建别名记录的负载均衡器。
5. 在 Description 选项卡上，获得 DNS name 的值。
6. 如果要为其他 Elastic Load Balancing 负载均衡器创建别名记录，则重复步骤 4 和 5。
7. 退出 Amazon Web Services 管理控制台.
8. 使用您用于创建 Route 53 托管区域的 Amazon 帐户 Amazon Web Services 管理控制台 再次登录。
9. 返回到过程 通过使用 Amazon Route 53 控制台创建记录 的步骤 3。

资源记录集权限

资源记录集权限使用身份和访问管理 (IAM) 策略条件来允许您为 Route 53 控制台上的操作或使用 ChangeResourceRecordSetsAPI 设置精细权限。

资源记录集定义为具有相同名称和类型（和类，但对于大多数用途，类始终为 IN 或 internet）的多个资源记录，但它们包含不同的数据。例如，如果您选择地理位置路由，则可以让多条 A 或 AAAA 记录指向同一个域的不同端点。所有这些 A 或 AAAA 记录组合构成资源记录集。有关 DNS 术语的更多信息，请参阅 RFC 7719。

通过 IAM 策略条件、`route53:ChangeResourceRecordSetsNormalizedRecordNames`和`route53:ChangeResourceRe`，您可以向任何其他 Amazon 账户中的其他 Amazon 用户授予精细的管理权限。这样便可授予某人以下权限：

- 单个资源记录集。
- 特定 DNS 记录类型的所有资源记录集。
- 名称包含特定字符串的资源记录集。
- 使用 ChangeResourceRecordSetsAPI 或 Route 53 控制台时，执行任何或全部`CREATE | UPSERT | DELETE`操作。

您还可以创建结合任何 Route 53 策略条件的访问权限。例如，您可以授予某人修改 marketing-example.com 的 A 记录数据的权限，但不允许该用户删除任何记录。

有关资源记录集权限的更多信息，以及如何使用这些权限的示例，请参阅 使用 IAM 策略条件进行精细访问控制。

要了解如何对 Amazon 用户进行身份验证，请参阅使用身份进行身份验证并了解如何控制对 Route 53 资源的访问权限，请参阅访问控制。

在您创建或编辑 Amazon Route 53 记录时指定的值

使用 Amazon Route 53 控制台创建记录时，您指定的值取决于您要使用的路由策略以及您是否在创建将流量路由到 Amazon 资源的别名记录。

别名记录将流量路由到您为其指定目标 Amazon 资源的某些资源（例如 Elastic Load Balancing、CloudFront 分配、Amazon S3 存储桶）。您也可以选择关联运行状况检查，并配置目标运行状况评估。以下主题提供了每种路由策略和记录类型所需值的详细信息，可帮助您有效地配置 Route 53 记录。

主题

- 地理位置记录的特定值
- 地理位置别名记录的特定值
- 地理位置临近度记录的特定值
- 地理位置临近度别名记录的特定值
- 延迟记录的特定值
- 延迟别名记录的特定值
- 针对基于 IP 的记录的特定值
- 基于 IP 的别名记录的特定值
- 多值应答记录的特定值
- 加权记录的特定值
- 加权别名记录的特定值

所有路由策略的通用值

以下是您在创建或编辑 Amazon Route 53 记录时可以指定的通用值。所有路由策略都使用这些值。

主题

- 记录名称
- 值/流量路由至
- TTL（秒）

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

CNAME 记录

如果您要创建 Record type（记录类型）值为 CNAME 的记录，则该记录的名称不能与托管区域的名称相同。

特殊字符

有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。

通配符

您可以在名称中使用星号 (*) 字符。DNS 会根据 * 字符出现在名称中的位置将它作为通配符或作为 * 字符 (ASCII 42) 来处理。有关更多信息，请参阅 在托管区域和记录的名称中使用星号 (*)。

> **Important**
>
> 对于类型为 NS 的资源记录集，不能使用 * 通配符。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

A - IPv4 地址

IPv4 格式的 IP 地址，例如 192.0.2.235。

AAAA - IPv6 地址

IPv6 格式的 IP 地址，例如 2001:0db8:85a3:0:0:8a2e:0370:7334。

CAA - 证书颁发机构授权

3 个以空格分隔的值，可控制允许哪些证书颁发机构为由 Record name（记录名称）指定的域或子域签发证书或通配符证书。您可以使用 CAA 记录指定以下内容：

- 哪些证书颁发机构 (CA) 可以签发 SSL/TLS 证书 (如果有)
- CA 为域或子域签发证书时要联系的电子邮件地址或 URL

CNAME - 规范名称

您希望 Route 53 在响应此记录的 DNS 查询时返回的完全限定域名（例如，www.example.com）。结尾的点是可选的；Route 53 会假定该域名是完全限定的。这意味着，Route 53 会将 www.example.com（不包含结尾圆点）和 www.example.com.（包含结尾圆点）视为相同。

MX - 邮件交换

一个优先级和一个指定邮件服务器的域名，例如 10 mailserver.example.com。结尾圆点被视为可选。

NAPTR - 名称权威指针

六个以空格分隔的设置，由动态授权发现系统 (DDDS) 应用程序用来将一个值转换为另一个值或将一个值替换为另一个值。有关更多信息，请参阅 NAPTR 记录类型。

PTR - 指针

您希望 Route 53 返回的域名。

NS - 名称服务器

名称服务器的域名，例如 ns1.example.com。

> **Note**
>
> 您只能使用简单的路由策略来指定 NS 记录。

SPF - 发件人策略框架

包括在引号中的 SPF 记录，例如 "v=spf1 ip4:192.168.0.1/16-all"。建议不要使用 SPF 记录。有关更多信息，请参阅 支持的 DNS 记录类型。

SRV - 服务定位器

SRV 记录。SRV 记录用于访问服务，例如电子邮件或通信服务。有关 SRV 记录格式的信息，请参阅要连接到的服务的文档。结尾圆点将视为可选。

SRV 记录的格式为：

[优先级] [权重] [端口] [服务器主机名]

例如：

1 10 5269 xmpp-server.example.com.

TXT - 文本

文本记录。包含在引号内的文本，例如 "Sample text entry"。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

所有路由策略的别名记录的通用值

以下是您在创建或编辑 Amazon Route 53 记录时可以指定的通用别名值。所有路由策略都使用这些值。

主题

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

CNAME 记录

如果您要创建 Type (类型) 值为 CNAME 的记录，则该记录的名称不能与托管区域的名称相同。

CloudFront 分配和 Amazon S3 存储桶的别名

您指定的值部分取决于您要将流量路由到的 Amazon 资源：

- CloudFront 分配 - 您的分配必须包含与记录名称匹配的备用域名。例如，如果记录的名称是 acme.example.com，您的 CloudFront 分配必须包含 acme.example.com，以作为备用域名之一。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的使用备用域名 (CNAME)。
- Amazon S3 存储桶 - 记录的名称必须与您的 Amazon S3 存储桶的名称匹配。例如，如果您的存储桶的名称是 acme.example.com，则此记录的名称也必须是 acme.example.com。

  此外，您还必须配置该存储桶以用于网站托管。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的为网站托管配置存储桶。

特殊字符

有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。

通配符

您可以在名称中使用星号 (*) 字符。DNS 会根据 * 字符出现在名称中的位置将它作为通配符或作为 * 字符 (ASCII 42) 来处理。有关更多信息，请参阅 在托管区域和记录的名称中使用星号 (*)。

值/流量路由至

从列表中选择的值或在字段中键入的值取决于将流量路由到的 Amazon 资源。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅 将互联网流量路由到您的 Amazon 资源。

Important

如果您使用相同的 Amazon 账户创建托管区域以及将流量路由到的资源，并且您的资源未出现在 Endpoint（终端节点）列表中，请检查以下内容：

- 确认您为 Record type（记录类型）选择支持的值。支持的值特定于您要将流量路由到的资源。例如，要将流量路由到 S3 存储桶，您必须选择 A — IPv4 address（A - IPv4 地址）作为 Record type（记录类型）。
- 确认该账户具有列出适用资源所需的 IAM 权限。例如，要使 CloudFront 分配出现在 Endpoint（终端节点）列表中，该账户必须具有执行以下操作的权限：`cloudfront:ListDistributions`。

  有关 IAM policy 示例，请参阅 使用 Amazon Route 53 控制台所需的权限。

如果您使用其它 Amazon 账户创建托管区域和资源，则 Endpoint（终端节点）列表不会显示您的资源。请参阅以下有关您的资源类型的文档，确定要在 Endpoint（终端节点）中键入的值。

API Gateway 自定义区域 API 和边缘优化 API

对于 API Gateway 自定义区域 API 和边缘优化 API，请执行以下操作之一：

- 如果您使用相同账户来创建您的 Route 53 托管区域和 API - 选择 Endpoint（终端节点），然后从列表中选择一个 API。如果您有很多 API，则可输入 API 终端节点的前几个字符，以筛选该列表。

> **Note**
>
> 此记录的名称必须与 API 的自定义域名匹配，例如 api.example.com。

- 如果您使用了不同的账户来创建您的 Route 53 托管区域和 API - 输入 API 的 API 终端节点，如 api.example.com。

  如果您使用了一个 Amazon 账户来创建当前托管区域，并使用另一个账户来创建 API，则 API 不会显示在 API Gateway APIs 下的 Endpoints（终端节点）列表中。

  如果您使用了一个账户来创建当前托管区域，并使用一个或多个不同账户来创建您的所有 API，则 Endpoints（终端节点）列表在 API Gateway APIs 下显示 No targets available（无可用目标）。有关更多信息，请参阅 使用域名将流量路由到 Amazon API Gateway API。

CloudFront 分配

对于 CloudFront 分配，请执行以下操作之一：

- 如果您使用了相同账户来创建您的 Route 53 托管区域和 CloudFront 分配 - 选择 Endpoint（终端节点），然后从列表中选择一种分配。如果您有很多分配，则可以输入分配域名的前几个字符，以便筛选该列表。

  如果分配未显示在列表中，请注意：

  - 此记录的名称必须与分配中的备用域名匹配。
  - 如果您刚刚在分配中添加备用域名，则可能需要 15 分钟才能使更改传播到所有 CloudFront 边缘站点。更改传播完成之前，Route 53 无法获知新的备用域名。
- 如果您使用了不同账户来创建您的 Route 53 托管区域和分配 - 输入分配的 CloudFront 域名，如 d111111abcdef8.cloudfront.net。

  如果您使用了一个 Amazon 账户来创建当前托管区域，并使用另一个账户来创建分配，则分配不会显示在 Endpoints（终端节点）列表中。

  如果您使用了一个账户来创建当前托管区域，并使用一个或多个不同账户来创建您的所有分配，则 Endpoints（终端节点）列表在 CloudFront distributions（CloudFront 分配）下显示 No targets available（无可用目标）。

> **Important**
>
> 请勿将查询路由到尚未传播到所有边缘站点的 CloudFront 分配，否则您的用户将无法访问相应的内容。

您的 CloudFront 分配必须包含与记录名称匹配的备用域名。例如，如果记录的名称是 acme.example.com，您的 CloudFront 分配必须包含 acme.example.com，以作为备用域名之一。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的使用备用域名 (CNAME)。

如果为分配启用 IPv6，请创建两个记录，一个记录的 Record type（记录类型）值为 A — IPv4 address（A - IPv4 地址），而另一个记录的值为 AAAA — IPv6 address（AAAA - IPv6 地址）。有关更多信息，请参阅 使用您的域名将流量路由到 Amazon CloudFront 分配。

App Runner 服务

对于 App Runner 服务，执行下列操作之一：

- 如果您使用相同账户来创建自己的 Route 53 托管区和 App Runner 服务 - 选择 Amazon Web Services 区域，然后从列表中选择您要将流量路由到其中的环境的域名。
- 如果您使用不同账户来创建您自己的 Route 53 托管区和 App Runner - 输入自定义域名。有关更多信息，请参阅 Managing custom domain names for App Runner（管理 App Runner 服务的自定义域名）。

  如果您使用了一个 Amazon 账户来创建当前托管区，并使用另一个账户来创建 App Runner，则 App Runner 不会显示在端点列表中。

有关更多信息，请参阅 配置 Amazon Route 53 以将流量路由到 App Runner 服务。

具有区域化子域的 Elastic Beanstalk 环境

如果 Elastic Beanstalk 环境的域名包括您在其中部署环境的区域，则您可以创建一个将流量路由到该环境的别名记录。例如，域名 `my-environment.us-west-2.elasticbeanstalk.com` 是区域化域名。

> **Important**
>
> 对于在 2016 年年初之前创建的环境，域名不包括该区域。要将流量路由到这些环境，您必须创建 CNAME 记录，而不是别名记录。请注意，不能为根域名创建 CNAME 记录。例如，如果您的域名为 example.com，则可创建一个能将 acme.example.com 的流量路

由到 Elastic Beanstalk 环境的记录，但不能创建可将 example.com 的流量路由到 Elastic Beanstalk 环境的记录。

对于具有区域化子域的 Elastic Beanstalk 环境，请执行以下操作之一：

- 如果您使用相同账户来创建您的 Route 53 托管区域和 Elastic Beanstalk 环境 - 选择 Endpoint（终端节点），然后从列表中选择一个环境。如果您有很多环境，则可以输入环境的 CNAME 属性的前几个字符，以便筛选该列表。
- 如果您使用了不同账户来创建您的 Route 53 托管区域和 Elastic Beanstalk 环境 - 输入 Elastic Beanstalk 环境的 CNAME 属性。

有关更多信息，请参阅 将流量路由到 Amazon Elastic Beanstalk 环境。

ELB 负载均衡器

对于 ELB 负载均衡器，请执行以下操作之一：

- 如果您使用了相同账户来创建您的 Route 53 托管区域和负载均衡器 - 选择 Endpoint（终端节点），然后从列表中选择一个负载均衡器。如果您有很多负载均衡器，您可输入 DNS 名称的前几个字符，以筛选该列表。
- 如果您使用了不同账户来创建您的 Route 53 托管区域和负载均衡器 - 输入您在过程 获取 Elastic Load Balancing 负载均衡器的 DNS 名称 中获得的值。

  如果您使用了一个 Amazon 账户来创建当前托管区域，并使用另一个账户来创建负载均衡器，则该负载均衡器不会显示在 Endpoints（终端节点）列表中。

  如果您使用了一个账户来创建当前托管区域，并使用一个或多个不同账户来创建您的所有负载均衡器，则 Endpoints（终端节点）列表在 Elastic Load Balancers 下显示 No targets available（无可用目标）。

控制台将为来自不同账户的 Application Load Balancer 和经典负载均衡器添加 dualstack. 前缀。当一个客户端（例如 Web 浏览器）请求与您的域名 (example.com) 或子域名 (www.example.com) 对应的 IP 地址时，该客户端可以请求 IPv4 地址（A 记录）、IPv6 地址（AAAA 记录），或同时请求 IPv4 和 IPv6 地址（此时需用不同的请求来实现）。dualstack. 标识让 Route 53 能够基于客户端所请求的 IP 地址格式使用您的负载均衡器的相应 IP 地址进行响应。

有关更多信息，请参阅 将流量路由到 ELB 负载均衡器。

Amazon Global Accelerator 加速器

对于 Amazon Global Accelerator 加速器，输入加速器的 DNS 名称。您可以为使用当前 Amazon 账户或使用另一 Amazon 账户创建的加速器输入 DNS 名称。

Amazon S3 存储桶

对于配置为网站终端节点的 Amazon S3 存储桶，请执行以下操作之一：

- 如果您使用相同账户来创建您的 Route 53 托管区域和 Amazon S3 存储桶 - 选择 Endpoint（终端节点），然后从列表中选择一个存储桶。如果您有很多存储桶，则可输入 DNS 名称的前几个字符，以筛选该列表。

  Endpoint（终端节点）的值变为存储桶的 Amazon S3 网站终端节点。
- 如果您使用了不同账户来创建您的 Route 53 托管区域和 Amazon S3 存储桶 - 输入您在其中创建了 S3 存储桶的区域的名称。使用《Amazon Web Services 一般参考》中 Amazon S3 网站端点表中网站端点列显示的值。

  如果您使用当前账户之外的其它 Amazon 账户来创建您的 Amazon S3 存储桶，则该存储桶不会显示在 Endpoints（终端节点）列表中。

您必须配置该存储桶以用于网站托管。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的为网站托管配置存储桶。

记录的名称必须与您的 Amazon S3 存储桶的名称匹配。例如，如果您的 Amazon S3 存储桶的名称是 acme.example.com，则此记录的名称也必须是 acme.example.com。

在加权别名、延迟别名、故障转移别名或地理位置别名记录组中，您可以仅创建一个将查询路由到 Amazon S3 存储桶的记录，因为该记录的名称必须与存储桶名称匹配且存储桶名称必须全局唯一。

Amazon OpenSearch Service

对于 OpenSearch Service，请执行下列操作之一：

- OpenSearch Service 自定义域：记录的名称必须与自定义域匹配。例如，如果您的自定义域名称是 test.example.com，则此记录的名称也必须是 test.example.com。
- 如果您使用相同账户来创建自己的 Route 53 托管区和 OpenSearch Service 域 – 选择 Amazon Web Services 区域，然后选择域名。
- 如果您使用不同账户来创建自己的 Route 53 托管区和 OpenSearch Service 域 - 输入自定义域名。有关更多信息，请参阅创建自定义端点。

  如果您使用了一个 Amazon 账户来创建当前托管区，并使用另一个账户来创建 OpenSearch Service 域，则该域不会显示在端点列表中。

如果您使用了一个账户来创建当前托管区，并使用一个或多个不同账户来创建您的所有 OpenSearch Service 域，则端点列表在 OpenSearch Service 下显示无可用目标。

有关更多信息，请参阅 将 Amazon Route 53 配置为将流量路由到亚马逊 OpenSearch 服务域终端节点。

Amazon VPC 接口终端节点

对于 Amazon VPC 接口终端节点，请执行以下操作之一：

- 如果您使用了相同账户来创建您的 Route 53 托管区域和接口终端节点 - 选择 Endpoint（终端节点），然后从列表中选择一个接口终端节点。如果您有很多接口终端节点，则可输入 DNS 主机名的前几个字符，以筛选该列表。
- 如果您使用了不同账户来创建您的 Route 53 托管区域和接口终端节点 - 输入接口终端节点的 DNS 主机名，如 vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com。

  如果您使用了一个 Amazon 账户来创建当前托管区域，并使用另一个账户来创建接口终端节点，则接口终端节点不会显示在 VPC endpoints（VPC 终端节点）下的 Endpoints（终端节点）列表中。

  如果您使用了一个账户来创建当前托管区域，并使用一个或多个不同账户来创建您的所有接口终端节点，则 Endpoints（终端节点）列表在 VPC endpoints（VPC 终端节点）下显示 No targets available（无可用目标）。

  有关更多信息，请参阅 使用域名将流量路由到 Amazon Virtual Private Cloud 接口终端节点。

此托管区域中的记录

对于此托管区域中的记录，选择 Endpoint（终端节点），然后选择适用的记录。如果您有很多记录，则可输入名称的前几个字符，以筛选该列表。

如果托管区域仅包含默认 NS 和 SOA 记录，则 Endpoints（终端节点）列表显示 No Targets Available（无可用目标）。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法选择 Record type（记录类型）值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

简单记录的特定值

创建简单记录时，请指定以下值。

主题

路由策略

选择 Simple routing（简单路由）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

有关记录名称的更多信息，请参阅 记录名称。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称

- MX - 邮件交换
- NAPTR - 名称权威指针
- NS – 名称服务器

  名称服务器的域名，例如 ns1.example.com。

  > **Note**
  >
  > 您只能使用简单的路由策略来指定 NS 记录。

- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

基于您希望 Route 53 响应 DNS 查询的方式选择 Record type（记录类型）的值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

简单别名记录的特定值

在创建别名记录时，请指定以下值。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

> **Note**
>
> 如果您在 Amazon GovCloud (US) Region 中使用 Route 53，则此功能有一些限制。有关更多信息，请参阅 Amazon GovCloud (US)用户指南中的 Amazon Route 53 页面。

主题

- 路由策略
- 记录名称
- 值/流量路由至
- 记录类型
- Evaluate Target Health

路由策略

选择 Simple routing（简单路由）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

有关记录名称的更多信息，请参阅 记录名称。

值/流量路由至

从列表中选择的值或在字段中键入的值取决于将流量路由到的 Amazon 资源。

有关您可以作为目标的 Amazon 资源的信息，请参阅“值/流量路由至”的别名记录的通用值。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅 将互联网流量路由到您的 Amazon 资源。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

基于您要将流量路由到的 Amazon 资源选择合适的值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 address（A - IPv4 地址）。

Amazon VPC 接口终端节点

选择 A — IPv4 address（A - IPv4 地址）。

CloudFront 分配

选择 A — IPv4 address（A - IPv4 地址）。

如果为分配启用 IPv6，请创建两个记录，一个记录的 Type（类型）值为 A — IPv4 address（A - IPv4 地址），而另一个记录的值为 AAAA — IPv6 address（AAAA - IPv6 地址）。

App Runner 服务

选择 A — IPv4 address（A - IPv4 地址）

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 address（A - IPv4 地址）

ELB 负载均衡器

选择 A — IPv4 address（A - IPv4 地址）或 AAAA — IPv6 address（AAAA - IPv6 地址）

Amazon S3 存储桶

选择 A — IPv4 address（A - IPv4 地址）

OpenSearch Service

选择 A — IPv4 address（A - IPv4 地址）或 AAAA — IPv6 address（AAAA - IPv6 地址）

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

Evaluate Target Health

当路由策略的值为简单时，您可以选择否或默认的是，因为评估目标运行状况对简单路由没有影响。如果您只有一个具有给定名称和类型的记录，Route 53 将使用该记录中的值响应 DNS 查询，无论资源运行状况是否良好。

对于其他路由策略，评估目标运行状况可确定 Route 53 是否检查别名记录所指资源的运行状况：

- 评估目标运行状况可带来运营优势的服务：对于负载均衡器（ELB）和带有负载均衡器的 Amazon Elastic Beanstalk 环境，将评估目标运行状况设置为是可让 Route 53 将流量路由出运行状况不佳的资源。
- 高可用性服务：对于诸如 Amazon S3 存储桶、VPC 接口端点、Amazon API Gateway、Amazon Global Accelerator、Amazon OpenSearch Service 和 Amazon VPC Lattice 之类的服务，评估目标运行状况不会带来任何运营优势，因为这些服务专为高可用性而设计。对于这些服务的失效转移场景，请改用 Route 53 运行状况检查。

有关评估目标运行状况如何与不同 Amazon 服务配合使用的详细信息，请参阅 API 参考中的 EvaluateTargetHealth 文档。

故障转移记录的特定值

在创建故障转移记录时，请指定以下值。

> **Note**
>
> 有关在私有托管区域中创建故障转移记录的更多信息，请参阅在私有托管区域中配置故障转移。

主题

- 路由策略
- 记录名称
- 记录类型
- TTL（秒）
- 值/流量路由至
- 故障转移记录类型
- 运行状况检查
- 记录 ID

路由策略

选择 Failover（故障转移）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为故障转移记录组中的两个记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

为主辅故障转移记录选择相同的值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器

- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

故障转移记录类型

为此记录选择适用的值。为正常进行故障转移，您必须创建一主一辅的故障转移记录。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与故障转移记录相同的非故障转移记录。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain Name (域名) 的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain Name (域名) 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

记录 ID

输入唯一标识主和辅助记录的值。

故障转移别名记录的特定值

在创建故障转移别名记录时，请指定以下值。

有关更多信息，请参阅以下主题：

- 有关在私有托管区域中创建故障转移记录的更多信息，请参阅在私有托管区域中配置故障转移。
- 有关别名记录的更多信息，请参阅在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- 故障转移记录类型
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择 Failover（故障转移）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为故障转移记录组中的两个记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值。为主辅故障转移记录选择相同的值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具

有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以定位哪些 Amazon 资源的信息，请参阅流向的 value/route 流量别名记录的常用值。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

> **Note**
>
> 创建主和辅助故障转移记录时，您可以选择创建一个故障转移和一个故障转移别名记录，它们具有相同的 Name（名称）和 Record type（记录类型）值。如果您混合使用故障转移和故障转移别名记录，则其中任意一个记录集都可以作为主记录。

故障转移记录类型

为此记录选择适用的值。为正常进行故障转移，您必须创建一主一辅的故障转移记录。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与故障转移记录相同的非故障转移记录。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain Name (域名) 的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain Name (域名) 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果

环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将“评估目标运行状况”设置为“是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将“评估目标运行状况”设置为“是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：
  - 为使应用程序负载均衡器或网络负载均衡器被认为是正常运行的，包含目标的目标组必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
  - 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入唯一标识主和辅助记录的值。

地理位置记录的特定值

在创建地理位置记录时，请指定以下值。

主题

路由策略

选择 Geolocation（地理位置）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

为地理位置记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

为地理位置记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

位置

在您配置 Route 53 根据查询发起位置响应 DNS 查询时，请选择您希望 Route 53 使用此记录中的设置来响应的大洲或国家/地区。如果您希望 Route 53 响应美国各个州的 DNS 查询，请从 Location（位置）列表中选择 United States（美国），然后选择 Sublocation（子位置）下的州。

对于私有托管区域，请选择距离您的资源所在的 Amazon Web Services 区域 最近的大洲、国家/地区或区域。例如，如果您的资源位于 us-east-1，则可以指定北美洲、美国或弗吉尼亚州。

> **Important**
>
> 建议您创建一个 Location（位置）值为 Default（默认）的地理位置记录。这涵盖您尚未创建记录的地理位置以及 Route 53 无法确定其位置的 IP 地址。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与地理位置记录相同的非地理位置记录。

有关更多信息，请参阅 地理位置路由。

以下是 Amazon Route 53 将与每个大陆关联的国家/地区。国家/地区代码来自 ISO 3166。有关更多信息，请参阅 Wikipedia 文章 ISO 3166-1 alpha-2：

非洲 (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南极洲 (AN)

AQ、GS、TF

亚洲 (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

欧洲 (EU)

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

> **Note**
>
> 一些提供商认为TR在亚洲，IP地址将反映出这一点。

北美洲 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

大洋洲 (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南美洲 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 不支持创建以下国家/地区的地理位置记录：布韦岛 (BV)，圣诞岛 (CX)、西撒哈拉 (EH)、赫德岛和麦克唐纳群岛 (HM)。没有关于这些国家/地区的 IP 地址的数据。

美国各州

当您将 Route 53 配置为根据作为查询发起地的美国州来响应 DNS 查询时，请从 U.S. states（美国各州）列表中选择该州。美国领地（例如波多黎各）作为 Location (位置) 列表中的国家/地区列出。

> **Important**
>
> 一些 IP 地址与美国关联，但是不属于单独的州。如果您为美国的所有州创建记录，我们建议您也为美国创建一个记录，以为这些无关联的 IP 地址路由查询。如果不为美国创建记录，Route 53 将使用默认地理位置记录（如果您创建了默认记录）的设置来响应来自无关联美国 IP 地址的 DNS 查询，或者提供“无应答”响应。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain Name (域名) 的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain Name (域名) 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

对于地理位置记录，如果某个终端节点的运行状况不佳，Route 53 将在记录中查找更大的关联地理区域。例如，假设您对于美国某个州、美国、北美和所有位置（Location (位置) 为 Default (默认)）都有对应的记录。如果该州记录的终端节点运行状况不佳，Route 53 将依次检查美国、北美和所有位置的记录，直到它找到具有正常终端节点的记录。如果所有适用的记录均不正常（包括所有位置的记录），则 Route 53 将使用最小地理区域的记录的值响应 DNS 查询。

记录 ID

输入在地理位置记录组中唯一标识此记录的值。

地理位置别名记录的特定值

在创建地理位置别名记录时，请指定以下值。

有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- 位置
- 美国各州
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择 Geolocation（地理位置）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为地理位置记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值。为地理位置记录组中的所有记录选择相同值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以瞄准哪些 Amazon 资源的信息，请参阅值/流量路由至。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

位置

在您配置 Route 53 根据查询发起位置响应 DNS 查询时，请选择您希望 Route 53 使用此记录中的设置来响应的大洲或国家/地区。如果您希望 Route 53 响应美国各个州的 DNS 查询，请从 Location（位置）列表中选择 United States（美国），然后从 Sublocation（子位置）列表中选择州。

对于私有托管区域，请选择最接近您的资源所在的大洲、国家或分区。 Amazon Web Services 区域 例如，如果您的资源位于 us-east-1，则可以指定北美洲、美国或弗吉尼亚州。

> **Important**
>
> 建议您创建一个 Location（位置）值为 Default（默认）的地理位置记录。这涵盖您尚未创建记录的地理位置以及 Route 53 无法确定其位置的 IP 地址。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与地理位置记录相同的非地理位置记录。

有关更多信息，请参阅 地理位置路由。

以下是 Amazon Route 53 将与每个大陆关联的国家/地区。国家/地区代码来自 ISO 3166。有关更多信息，请参阅 Wikipedia 文章 ISO 3166-1 alpha-2：

非洲 (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南极洲 (AN)

AQ、GS、TF

亚洲 (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

欧洲（EU）

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

> **Note**
>
> 一些提供商认为 TR 在亚洲，IP 地址将反映出这一点。

北美洲 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

大洋洲 (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南美洲 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 不支持为以下国家/地区创建地理位置记录：布维岛 (BV)、圣诞岛 (CX)、西撒哈拉 (EH) 和赫德岛和群岛 (HM)。 McDonald 没有关于这些国家/地区的 IP 地址的数据。

美国各州

当您将 Route 53 配置为根据作为查询发起地的美国州来响应 DNS 查询时，请从 U.S. states（美国各州）列表中选择该州。美国领地（例如波多黎各）作为 Location (位置) 列表中的国家/地区列出。

> **Important**
>
> 一些 IP 地址与美国关联，但是不属于单独的州。如果您为美国的所有州创建记录，我们建议您也为美国创建一个记录，以为这些无关联的 IP 地址路由查询。如果不为美国创建记录，Route 53 将使用默认地理位置记录（如果您创建了默认记录）的设置来响应来自无关联美国 IP 地址的 DNS 查询，或者提供“无应答”响应。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

对于地理位置记录，如果某个终端节点的运行状况不佳，Route 53 将在记录中查找更大的关联地理区域。例如，假设您对于美国某个州、美国、北美和所有位置（Location (位置) 为 Default (默认)）都有对应的记录。如果该州记录的终端节点运行状况不佳，Route 53 将依次检查美国、北美和所有位置的

记录，直到它找到具有正常终端节点的记录。如果所有适用的记录均不正常（包括所有位置的记录），则 Route 53 将使用最小地理区域的记录的值响应 DNS 查询。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将 “评估目标运行状况” 设置为 “是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将 “评估目标运行状况” 设置为 “是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：

- 为使 Application Load Balancer 或 Network Load Balancer 被认为是正常运行的，包含目标的每个目标组都必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
- 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入在地理位置记录组中唯一标识此记录的值。

地理位置临近度记录的特定值

在创建地理位置临近度记录时，请指定以下值。

主题

- 路由策略
- 记录名称
- 记录类型
- TTL（秒）
- 值/流量路由至
- 终端节点位置
- 偏差
- 运行状况检查
- 记录 ID

路由策略

选择地理位置临近度。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

为地理位置临近度记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

为地理位置临近度记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

终端节点位置

您可以使用以下方法之一指定资源端点位置：

自定义坐标

指定某个地理区域的经度和纬度。

Amazon Web Services 区域

从位置列表中选择可用区域。

有关区域的更多信息，请参见 Amazon 全球基础设施。

Amazon Local Zone 组

从位置列表中选择一个可用的 Local Zone 组。

有关 Local Zones 的更多信息，请参阅《Amazon Local Zones 用户指南》中的可用 Local Zones。Local Zone 组通常是指没有结尾字符的 Local Zone 区域。例如，如果 Local Zone 为 `us-east-1-bue-1a`，则 Local Zone 组为 `us-east-1-bue-1`。

您还可以使用 describe-availability-zones CLI 命令识别特定 Local Zone 的 Local Zones 组：

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

此命令返回：`"GroupName": "us-west-2-den-1"`，指定 Local Zone `us-west-2-den-1a` 属于 Local Zone 组 `us-west-2-den-1`。

您不能创建记录名称和记录类型的值与地理位置临近度记录相同的非地理位置临近度记录。

您也不能创建两个为相同记录名称和记录类型指定相同位置的地理位置临近度资源记录集。

偏差

偏差可以增大或减小 Route 53 路由到某个资源的流量所来自的地理区域。正偏差会扩大区域，负偏差会缩小区域。有关更多信息，请参阅 Amazon Route 53 如何使用偏差来路由流量。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、地理位置临近度别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在评估目标运行状况下选择是。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain Name (域名) 的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain Name (域名) 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

对于地理位置临近度记录，如果某个端点的运行状况不佳，Route 53 会查找运行状况仍然良好的最近端点。

记录 ID

输入在地理位置临近度记录组中唯一标识此记录的值。

地理位置临近度别名记录的特定值

在创建地理位置临近度别名记录时，请指定以下值。

有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- 终端节点位置
- 偏差
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择地理位置临近度。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为地理位置临近度记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值。为地理位置临近度记录组中的所有记录选择相同值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以瞄准哪些 Amazon 资源的信息，请参阅值/流量路由至。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

终端节点位置

您可以使用以下方法之一指定资源端点位置：

自定义坐标

指定某个地理区域的经度和纬度。

Amazon Web Services 区域

从位置列表中选择可用区域。

有关区域的更多信息，请参见 Amazon 全球基础设施。

Amazon 本地区域组

从位置列表中选择一个可用的 Local Zone 区域。

有关 Local Zones 的更多信息，请参阅《Amazon Local Zones 用户指南》中的可用 Local Zones。Local Zone 组通常是指没有结尾字符的 Local Zone 区域。例如，如果 Local Zone 为 `us-east-1-bue-1a`，则 Local Zone 组为 `us-east-1-bue-1`。

您还可以使用 describe-availability-zonesCLI 命令识别特定本地区域的 Local Zones 组：

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

此命令返回：`"GroupName": "us-west-2-den-1"`，指定 Local Zone `us-west-2-den-1a` 属于 Local Zone 组 `us-west-2-den-1`。

您不能创建记录名称和记录类型的值与地理位置临近度记录相同的非地理位置临近度记录。

您也不能创建两个为相同记录名称和记录类型指定相同位置的地理位置临近度资源记录集。

有关更多信息，请参阅 available-local-zones .html

偏差

偏差可以增大或减小 Route 53 路由到某个资源的流量所来自的地理区域。正偏差会扩大区域，负偏差会缩小区域。有关更多信息，请参阅 Amazon Route 53 如何使用偏差来路由流量。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、地理位置临近度别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在评估目标运行状况下选择是。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

对于地理位置临近度记录，如果某个端点的运行状况不佳，Route 53 会查找运行状况仍然良好的最近端点。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将 “评估目标运行状况” 设置为 “是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将 “评估目标运行状况” 设置为 “是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：

- 为使 Application Load Balancer 或 Network Load Balancer 被认为是正常运行的，包含目标的每个目标组都必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
- 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入在地理位置临近度记录组中唯一标识此记录的值。

延迟记录的特定值

在创建延迟记录时，请指定以下值。

主题

路由策略

选择 Latency（延迟）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为延迟记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

基于您希望 Route 53 响应 DNS 查询的方式选择 Type（类型）的值。

为延迟记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度（以秒为单位）。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析器为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

区域

您在此记录中指定的资源所在的 Amazon EC2 区域。Route 53 会根据您指定的其他值来提供 Amazon EC2 区域建议。这也适用于私有托管区域。我们建议您不要更改此值。

请注意以下几点：

- 您只能为每个 Amazon EC2 区域创建一个延迟记录。
- 您不必为所有 Amazon EC2 区域创建延迟记录。Route 53 会从您为其创建延迟记录的区域中选择延迟性能最佳的区域。
- 您不能创建 Record name（记录名称）和 Record type（记录类型）的值与延迟记录相同的非延迟记录。
- 如果您创建标记有区域 cn-north-1 的记录，则无论延迟如何，Route 53 始终都会使用此记录响应来自中国的查询。

有关使用延迟记录的更多信息，请参阅基于延迟的路由。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

记录 ID

输入在延迟记录组中唯一标识此记录的值。

延迟别名记录的特定值

在创建延迟别名记录时，请指定以下值。

有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- Region
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择 Latency（延迟）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为延迟记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

为延迟记录组中的所有记录选择相同值。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以定位哪些 Amazon 资源的信息，请参阅流向的 value/route 流量别名记录的常用值。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

Region

您在此记录中指定的资源所在的 Amazon EC2 区域。Route 53 根据您指定的其他值推荐亚马逊 EC2 区域。这也适用于私有托管区。我们建议您不要更改此值。

注意以下几点：

- 您只能为每个 Amazon EC2 地区创建一条延迟记录。
- 您无需为所有 Amazon EC2 区域创建延迟记录。Route 53 会从您为其创建延迟记录的区域中选择延迟性能最佳的区域。
- 您不能创建 Record name（记录名称）和 Record type（记录类型）的值与延迟记录相同的非延迟记录。
- 如果您创建标记有区域 cn-north-1 的记录，则无论延迟如何，Route 53 始终都会使用此记录响应来自中国的查询。

有关使用延迟记录的更多信息，请参阅基于延迟的路由。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain Name (域名) 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果

环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将“评估目标运行状况”设置为“是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将“评估目标运行状况”设置为“是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：
  - 为使 Application Load Balancer 或 Network Load Balancer 被认为是正常运行的，包含目标的每个目标组都必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
  - 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入在延迟记录组中唯一标识此记录的值。

针对基于 IP 的记录的特定值

在创建基于 IP 的记录时，请指定以下值。

> **Note**
>
> 虽然允许在私有托管区域中创建基于 IP 的记录，但不支持这样做。

主题

- 路由策略
- 记录名称
- 记录类型
- TTL（秒）
- 值/流量路由至
- 位置
- 运行状况检查
- 记录 ID

路由策略

选择 IP-based（基于 IP）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为基于 IP 的记录组中的所有记录输入相同名称。

CNAME 记录

如果您要创建 Record type（记录类型）值为 CNAME 的记录，则该记录的名称不能与托管区域的名称相同。

特殊字符

有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。

通配符

您可以在名称中使用星号 (*) 字符。DNS 会根据 * 字符出现在名称中的位置将它作为通配符或作为 * 字符 (ASCII 42) 来处理。有关更多信息，请参阅 在托管区域和记录的名称中使用星号 (*)。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

基于您希望 Route 53 响应 DNS 查询的方式选择 Type（类型）的值。

为基于 IP 的记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅 值/流量路由至“值/流量路由至”的通用值。

位置

您在此记录中指定的资源所在的 CIDR 位置的名称，由 CIDR 位置内的 CIDR 块值指定。

有关使用基于 IP 的记录的更多信息，请参阅 基于 IP 的路由。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。

- 对于失效转移别名、地理位置别名、基于 IP 的别名、延迟别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

记录 ID

输入在基于 IP 的记录组中唯一标识此记录的值。

基于 IP 的别名记录的特定值

在创建基于 IP 的别名记录时，请指定以下值。

> **Note**
>
> 虽然允许在私有托管区域创建基于 IP 的别名记录，但不支持这样做。

有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- 位置
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择 IP-based（基于 IP）。

> **Note**
>
> 虽然允许在私有托管区域创建基于 IP 的别名记录，但不支持这样做。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为基于 IP 的记录组中的所有记录输入相同名称。

CNAME 记录

如果您要创建 Record type（记录类型）值为 CNAME 的记录，则该记录的名称不能与托管区域的名称相同。

CloudFront 分配和 Amazon S3 存储桶的别名

您指定的值在一定程度上取决于您要将流量路由到的 Amazon 资源：

- CloudFront 分发-您的分配必须包含与记录名称相匹配的备用域名。例如，如果记录的名称为 acme.example.com，您的 CloudFront 分配必须包含 acme.example.com，以作为备用域名之一。有关更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的使用备用域名 (CNAMEs)。
- Amazon S3 存储桶 - 记录的名称必须与您的 Amazon S3 存储桶的名称匹配。例如，如果您的存储桶的名称是 acme.example.com，则此记录的名称也必须是 acme.example.com。

  此外，您还必须配置该存储桶以用于网站托管。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的为网站托管配置存储桶。

特殊字符

有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅DNS 域名格式。

通配符

您可以在名称中使用星号 (*) 字符。DNS 会根据 * 字符出现在名称中的位置将它作为通配符或作为 * 字符 (ASCII 42) 来处理。有关更多信息，请参阅 在托管区域和记录的名称中使用星号 (*)。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值。为基于 IP 的记录组中的所有记录选择相同值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以定位哪些 Amazon 资源的信息，请参阅流向的 value/route 流量别名记录的常用值。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

位置

在您配置 Route 53 根据查询发起位置响应 DNS 查询时，请选择您希望 Route 53 使用此记录中的设置来响应的 CIDR 位置。

> **Important**
>
> 建议您创建一个 Location（位置）值为 Default（默认）的基于 IP 的记录。此纪录涵盖您尚未创建记录的位置以及 Route 53 无法确定其位置的 IP 地址。

您不能创建与基于 IP 的 non-IP-based记录具有相同的 “记录名称” 和 “记录类型” 值的记录。

有关更多信息，请参阅 基于 IP 的路由。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。

- 对于失效转移别名、地理位置别名、基于 IP 的路由别名、延迟别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

对于基于 IP 的别名记录，如果某个端点的运行状况不佳，Route 53 将在更大的关联位置中查找记录。例如，假设您对于美国某个州、美国、北美和所有位置（Location (位置) 为 Default (默认)）都有对应的记录。如果该州记录的终端节点运行状况不佳，Route 53 将依次检查美国、北美和所有位置的记录，直到它找到具有正常终端节点的记录。如果所有适用的记录均不正常（包括所有位置的记录），则 Route 53 将使用最小地理区域的记录的值响应 DNS 查询。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将 “评估目标运行状况” 设置为 “是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将 “评估目标运行状况” 设置为 “是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：
  - 为使 Application Load Balancer 或 Network Load Balancer 被认为是正常运行的，包含目标的每个目标组都必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
  - 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入在基于 IP 的记录组中唯一标识此记录的值。

多值应答记录的特定值

在创建多值应答记录时，请指定以下值。

> **Note**
>
> 不支持创建多值应答别名记录。

主题

- 路由策略
- 记录名称
- 记录类型
- TTL（秒）
- 值/流量路由至
- 运行状况检查
- 记录 ID

路由策略

选择 Multivalue answer（多值应答）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为多值记录组中的所有记录输入相同的名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

选择 NS 和 CNAME 之外的任何值。

为多值应答记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

> **Note**
>
> 如果您创建两个或更多具有相同名称和类型的多值应答记录，您正在使用控制台，并且您为 TTL 指定了不同的值，则 Route 53 会将所有记录的 TTL 值更改为您上次指定的值。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。如果输入多个值，请将每个值放在单独的行中。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- MX - 邮件交换
- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架

- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。
- 对于故障转移别名、地理位置别名、延迟别名或加权别名记录组中的一个或多个别名记录，为 Evaluate target health（评估目标运行状况）选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

记录 ID

输入在多值应答记录组中唯一标识此记录的值。

加权记录的特定值

在创建加权记录时，请指定以下值。

主题

路由策略

选择 Weighted (加权)。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Record name（记录名称）字段中输入值（例如 @ 符号）。

为加权记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称。

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

为加权记录组中的所有记录选择相同值。

TTL（秒）

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即 2 天），则可以减少 DNS 递归解析程序为获取此记录中的最新信息而必须对 Route 53 发出的调用数。这可以缩短延迟并减少您的 Route 53 服务账单费用。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

但是，如果您为 TTL 指定了较长的值，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序在向 Route 53 请求最新信息之前，会在更长时间内使用其缓存中的值。如果您更改了已在使用的域或子域的设置，我们建议您在一开始指定较短的值，例如 300 秒，在确认新设置正确后再增加该值。

如果您将此记录与运行状况检查关联，我们建议您指定 60 秒或更短的 TTL，以便让客户端快速响应运行状况的变化。

您必须为此加权记录组中的所有记录指定相同的 TTL 值。

> **Note**
>
> 如果您创建两个或更多具有相同名称和类型的加权记录，并且您为 TTL 指定不同的值，则 Route 53 会将所有记录的 TTL 值更改为您上次指定的值。

如果一组加权记录包含将流量路由至一个 ELB 负载均衡器的一个或多个加权别名记录，建议您为具有相同名称和类型的所有非别名加权记录指定 60 秒的 TTL。将 TTL 设置为 60 秒（负载均衡器的 TTL）之外的值将改变您为 Weight (权重) 指定的值的效果。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。为 Record type（记录类型）输入合适的值。对于除 CNAME 之外的所有类型，都可输入多个值。在单独的行中输入每个值。

您可以将流量路由到或指定以下值：

- A - IPv4 地址
- AAAA - IPv6 地址
- CAA - 证书颁发机构授权
- CNAME - 规范名称
- MX - 邮件交换

- NAPTR - 名称权威指针
- PTR - 指针
- SPF - 发件人策略框架
- SRV - 服务定位器
- TXT - 文本

有关上述值的更多信息，请参阅“值/流量路由至”的通用值。

权重

确定 Route 53 使用当前记录响应的 DNS 查询的比例。Route 53 会计算具有相同 DNS 名称和类型组合的记录的权重之和。然后 Route 53 会基于一个资源的权重占总额的比率来响应查询。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与加权记录相同的非加权记录。

输入 0 到 255 之间的整数。要禁止路由到某个资源，请将 Weight (权重) 设置为 0。如果将组中所有记录的 Weight (权重) 都设置为 0，则流量以相同的概率路由到所有资源。这将确保您不会无意中对一组加权记录禁用路由。

当您将运行状况检查与加权记录关联时，将 Weight (权重) 设置为 0 的效果是不同的。有关更多信息，请参阅 Amazon Route 53 在已配置运行状况检查时如何选择记录。

运行状况检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您将检查一组具有相同的名称、类型和路由策略（例如故障转移或加权记录）的记录中所有记录的运行状况，并指定所有记录的运行状况检查 ID。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。

- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

记录 ID

输入在加权记录组中唯一标识此记录的值。

加权别名记录的特定值

在创建加权别名记录时，请指定以下值。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

主题

- 路由策略
- 记录名称
- 记录类型
- 值/流量路由至
- 重量
- 健康检查
- 评估目标运行状况
- 记录 ID

路由策略

选择 Weighted（加权）。

记录名称

输入您希望为其路由流量的域或子域的名称。默认值为托管区的名称。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

为加权记录组中的所有记录输入相同名称。

有关记录名称的更多信息，请参阅 记录名称

记录类型

DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

根据您要将流量路由到的 Amazon 资源选择适用的值：

API Gateway 自定义区域 API 或边缘优化 API

选择 A — IPv4 地址。

Amazon VPC 接口终端节点

选择 A — IPv4 地址。

CloudFront 分布

选择 A — IPv4 地址。

如果已 IPv6 为分配启用，则创建两条记录，一条的值为 A（ IPv4 地址表示类型），另一条的值为 AAAA — IPv6 地址。

App Runner 服务

选择 A — IPv4 地址

具有区域化子域的 Elastic Beanstalk 环境

选择 A — IPv4 地址

ELB 负载均衡器

选择 A — IPv4 地址或 AAAA — IPv6 地址

亚马逊 S3 存储桶

选择 A — IPv4 地址

OpenSearch 服务

选择 A — IPv4 地址或 AAAA — IPv6 地址

此托管区域中的其他记录

选择您要为其创建别名的记录的类型。除 NS 和 SOA 之外的所有类型都受支持。

> **Note**
>
> 如果您要创建与托管区域（称为顶级域名）同名的别名记录，则无法将流量路由到 Type (类型) 值为 CNAME 的记录。这是因为，别名记录必须与您要将流量路由到的目标记录具有相同的类型，而为 Zone Apex（机构根网域）创建 CNAME 记录的做法不受支持，即使对于别名记录也是如此。

为加权记录组中的所有记录选择相同值。

值/流量路由至

您从列表中选择的值或在字段中键入的值取决于您要将流量路由到的 Amazon 资源。

有关您可以定位哪些 Amazon 资源的信息，请参阅流向的 value/route 流量别名记录的常用值。

有关如何配置 Route 53 以将流量路由到特定 Amazon 资源的更多信息，请参阅将互联网流量路由到您的 Amazon 资源。

重量

确定 Route 53 使用当前记录响应的 DNS 查询的比例。Route 53 会计算具有相同 DNS 名称和类型组合的记录的权重之和。然后，Route 53 根据资源权重与总重量的比率来响应查询。

您不能创建 Record name（记录名称）和 Record type（记录类型）的值与加权记录相同的非加权记录。

输入 0 到 255 之间的整数。要禁止路由到某个资源，请将 Weight (权重) 设置为 0。如果将组中所有记录的 Weight (权重) 都设置为 0，则流量以相同的概率路由到所有资源。这将确保您不会无意中对一组加权记录禁用路由。

当您将运行状况检查与加权记录关联时，将 Weight (权重) 设置为 0 的效果是不同的。有关更多信息，请参阅 Amazon Route 53 在已配置运行状况检查时如何选择记录。

健康检查

如果您希望 Route 53 检查指定终端节点的运行状况，并仅当该终端节点正常运行的情况下才使用此记录响应 DNS 查询，请选择运行状况检查。

Route 53 不会检查记录中指定的终端节点的运行状况，如由 Value（值）字段中的 IP 地址指定的终端节点。为记录选择运行状况检查时，Route 53 会检查您在运行状况检查中指定的终端节点的运行状况。有关 Route 53 如何确定终端节点是否正常运行的信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

仅当 Route 53 在两个或更多记录之间选择响应 DNS 查询的记录，而且您希望 Route 53 在一定程度上基于运行状况检查的状态来进行此选择时，将运行状况检查与记录关联才有用。仅在以下配置中使用运行状况检查：

- 您正在检查一组具有相同名称、类型和路由策略的记录（例如故障转移或加权记录）中所有记录的运行状况，然后 IDs 为所有记录指定运行状况检查。如果记录的运行状况检查指出某个终端节点运行状况不佳，则 Route 53 将停止使用该记录的值来响应查询。

- 对于失效转移别名、地理位置别名、延迟别名、基于 IP 的别名或加权别名记录组中的一个或多个别名记录，在 Evaluate Target Health（评估目标运行状况）下选择 Yes（是）。如果这些别名记录引用相同托管区域中的非别名记录，则还必须为所引用的记录指定运行状况检查。如果您将运行状况检查与别名记录关联，并在 Evaluate Target Health（评估目标运行状况）下选择了 Yes（是），则两者都必须评估为 true。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。

如果您的运行状况检查仅以域名来指定端点，则建议您为每个端点创建一个单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。对于 Domain name（域名）的值，指定服务器的域名（例如 us-east-2-www.example.com），而不是记录的名称 (example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

评估目标运行状况

如果您希望 Route 53 通过检查 Endpoint（终端节点）指定的资源的运行状况来确定是否使用此记录响应 DNS 查询，请选择 Yes（是）。

注意以下几点：

API Gateway 自定义 APIs 区域和边缘优化 APIs

当终端节点为 API Gateway 自定义区域 API 或边缘优化 API 时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

CloudFront 分布

当终端节点是 CloudFront 分布时，您无法将 “评估目标生命值” 设置为 “是”。

具有区域化子域的 Elastic Beanstalk 环境

如果您在 Endpoint 中指定了 Elastic Beanstalk 环境，并且该环境包含 ELB 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的 EC2 亚马逊实例。（如果环境包含多个 Amazon EC2 实例，则该环境会自动包含一个 ELB 负载均衡器。）如果您将 “评估目标运行状况” 设置为 “是”，并且没有一个 Amazon EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他运行状况良好的可用资源（如果有）。

如果环境包含单个 Amazon EC2 实例，则没有特殊要求。

ELB 负载均衡器

运行状况检查行为取决于负载均衡器的类型：

- 经典负载均衡器 — 如果您在 Endpoin t 中指定 ELB Classic 负载均衡器，则 Elastic Load Balancing 仅将查询路由到在负载均衡器中注册的运行状况良好的亚马逊 EC2 实例。如果您将 Evalu ate Target Health 设置为 “是”，并且没有 EC2 实例运行状况良好，或者负载均衡器本身运行状况不佳，则 Route 53 会将查询路由到其他资源。
- Application Load Balancer 和 Network Load Balancers - 如果您指定 ELB Application Load Balancer 或 Network Load Balancers，并且将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是），Route 53 会根据与负载均衡器关联的目标组的运行状况将查询路由到负载均衡器：
  - 为使 Application Load Balancer 或 Network Load Balancer 被认为是正常运行的，包含目标的每个目标组都必须至少包含一个正常运行的目标。如果任何目标组只包含运行状况不佳的目标，则负载均衡器被认为是不正常的，并且 Route 53 会将查询路由到其他资源。
  - 没有注册目标的目标组被认为是运行状况不佳。

> **Note**
>
> 当您创建负载均衡器时，您需配置 Elastic Load Balancing 运行状况检查设置；这并不是 Route 53 运行状况检查，但是会执行类似的功能。请勿为您在 ELB 负载均衡器中注册的 EC2 实例创建 Route 53 运行状况检查。

S3 桶

当终端节点为 S3 存储桶时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

Amazon VPC 接口终端节点

当终端节点为 Amazon VPC 接口终端节点时，将 Evaluate target health（评估目标运行状况）设置为 Yes（是）没有任何特殊要求。

同一托管区中的其他记录

如果您在 Endpo int 中指定的 Amazon 资源是一条记录或一组记录（例如，一组加权记录），但不是其他别名记录，我们建议您将运行状况检查与终端节点中的所有记录关联起来。有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？。

记录 ID

输入在加权记录组中唯一标识此记录的值。

通过导入区域文件来创建记录

如果您要从另一个 DNS 服务提供商迁移，并且您的当前 DNS 服务提供商允许您将当前 DNS 设置导出到区域文件，则您可以通过导入区域文件来快速为 Amazon Route 53 托管区域创建所有记录。

> **Note**
>
> 区域文件使用称为 BIND 的标准格式来以文本格式表示记录。有关区域文件格式的信息，请参阅 Wikipedia 条目 Zone file。有关其他信息，请参阅 RFC 1034, Domain Names—Concepts and Facilities 第 3.6.1 节，以及 RFC 1035, Domain Names—Implementation and Specification 第 5 节。

如果要通过导入区域文件来创建记录，请注意以下事项：

- 区域文件必须采用符合 RFC 标准的格式。
- 区域文件中记录的域名必须与托管区域的名称相匹配。
- Route 53 支持 `$ORIGIN` 和 `$TTL` 关键字。如果区域文件包含 `$GENERATE` 或 `$INCLUDE` 关键字，导入将失败，Route 53 将返回错误。
- 当导入区域文件时，Route 53 会忽略区域文件中的 SOA 记录。Route 53 还会忽略与托管区域同名的任何 NS 记录。
- 您可以导入最多 1000 条记录。
- 如果托管区域已包含显示在区域文件中的记录，则导入过程将失败，并且不会创建任何记录。
- 对于包含反斜杠字符的 TXT 记录，区域文件导入过程会将某些反斜杠序列解释为控制字符。要在 TXT 记录值中包含字面反斜杠字符：
  - 在区域文件中使用双反斜杠（`\\`）来表示最终 TXT 记录中的单个字面反斜杠。
  - 例如，如果您的 TXT 记录应包含 `\\jYTDWqH...`（带有字面反斜杠和 j），请在区域文件中指定 `\\\\jYTDWqH...`。

  这对于 ACME 质询记录和其他包含字面反斜杠字符的 TXT 记录尤其重要。
- 对于长 TXT 记录（例如 DKIM 记录），区域文件导入过程支持将内容拆分为多个字符串。要创建包含多个字符串的 TXT 记录：

- 在区域文件中使用具有相同记录名称和类型的单独行。

  Example

  ```
  example.com. 300 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC"
  example.com. 300 IN TXT
   "7fCC6C13dM9tXuJmUBH7D4Vw8y1ByJ8z9QX2fvLm3pN4sR5tU6vW7xY8zA9bC0dE1f"
  example.com. 300 IN TXT
   "G2hI3jK4lM5nO6pQ7rS8tU9vW0xY1zA2bC3dE4fG5hI6jK7lM8nO9pQ0rS1tU2vW3x"
  ```

  导入过程会自动将它们合并到包含多个字符串的单个 TXT 记录中。每个字符串最多可以包含 65,535 个字符。不要将长字符串连接成单引号值。

- 我们建议您查看区域文件的内容，以确认记录名称根据需要包含或排除尾随点：
  - 当区域文件中的记录的名称包含结尾圆点 (`example.com.`) 时，导入过程将该名称解释为完全限定域名，并使用该名称创建 Route 53 记录。
  - 当区域文件中的记录的名称不包含结尾圆点 (`www`) 时，导入过程将该名称与区域文件中的域名 (`example.com`) 连接起来，并使用连接起来的名称 (`www.example.com`) 创建 Route 53 记录。

  如果导出过程未向记录的完全限定域名添加结尾圆点，则 Route 53 导入过程会将域名添加到记录名称中。例如，假设您要将记录导入到托管区域 `example.com`，而区域文件中的 MX 记录的名称是 `mail.example.com`，不带尾部圆点。Route 53 导入过程会创建一个名为 `mail.example.com.example.com` 的 MX 记录。

  > **Important**
  >
  > 对于 CNAME、MX、PTR 和 SRV 记录，此行为也适用于包含在 RDATA 值中的域名。例如，假设您有 `example.com` 的一个区域文件。如果区域文件中的 CNAME 记录（`support`，不包含结尾圆点）具有 RDATA 值 `www.example.com`（也不包含结尾圆点），则导入过程会创建名为 `support.example.com` 的 Route 53 记录来将流量路由到 `www.example.com.example.com`。在导入区域文件之前，请查看 RDATA 值并进行更新(如适用)。对于包含反斜杠字符的 TXT 记录，请在区域文件中使用双反斜杠（`\\\\`）来表示字面反斜杠。

Route 53 不支持将记录导出到区域文件。

> **Note**
>
> 如果您创建与托管区域同名的记录，则不要在 Name (名称) 字段中输入值（例如 @ 符号）。

通过导入区域文件来创建记录

1. 从当前为域提供服务的 DNS 服务提供商那里获取区域文件。此过程和相关术语因服务提供商而异。有关将记录导出或保存到区域文件或 BIND 文件的信息，请参阅提供商的界面和文档。

   如果找不到有关此过程的信息，则试着询问您当前的 DNS 提供商的客户支持，以获取您的记录列表或区域文件信息。

2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 在 Hosted Zones（托管区域）页面上，创建一个新的托管区域：

   a. 选择 Create hosted zone（创建托管区域）。

   b. 输入您的域名，并可选择输入注释。

   c. 选择创建。

5. 选择 Import zone file（导入区域文件）。
6. 在 Import zone file（导入区域文件）窗格中，将区域文件的内容粘贴到 Zone file（区域文件）文本框中。
7. 选择导入。

   > **Note**
   >
   > 根据您的区域文件中记录的数量，您可能需要等待几分钟，记录才能创建完毕。

8. 如果您使用域的另一个 DNS 服务（这很常见，如果您向另一个注册商注册了该域的话），则将 DNS 服务迁移到 Route 53。在完成该步骤后，您的注册商会开始将 Route 53 识别为您的 DNS 服务，以响应对您的域的 DNS 查询，而这些查询将开始被发送到 Route 53 DNS 服务器。（通常，在 DNS 查询开始被路由到 Route 53 之前，会有一两天的延迟，因为有关您以前的 DNS 服务的信息将在 DNS 解析程序中缓存这么长时间。）有关更多信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

编辑记录

以下步骤介绍如何使用 Amazon Route 53 控制台编辑记录。有关如何使用 Route 53 API 编辑记录的信息，请参阅亚马逊 Route 53 API 参考ChangeResourceRecordSets中的。

> **Note**
>
> 您对记录的更改需要一定时间才会传播到 Route 53 DNS 服务器。目前，验证更改是否已传播的唯一方法是使用 GetChangeAPI 操作。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

使用 Route 53 控制台编辑记录

1. 如果您不打算编辑别名记录，请转至步骤 2。

   如果您打算编辑别名记录以将流量路由到 Elastic Load Balancing 经典负载均衡器、应用程序负载均衡器或网络负载均衡器，并且已使用不同账户创建了 Route 53 托管区和负载均衡器，请执行过程 获取 Elastic Load Balancing 负载均衡器的 DNS 名称 以获取负载均衡器的 DNS 名称。

   如果您正在编辑任何其他 Amazon 资源的别名记录，请跳至步骤 2。
2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 在 Hosted Zones (托管区域) 页面上，选择包含您要编辑的记录的托管区域对应的行。
5. 选择要编辑的记录的行，然后在 Edit record（编辑记录）窗格中输入您的更改。
6. 输入适用的值。有关更多信息，请参阅 在您创建或编辑 Amazon Route 53 记录时指定的值。
7. 选择保存更改。
8. 如果您要编辑多个记录，则重复步骤 5 至 7。

删除记录

以下步骤介绍如何使用 Route 53 控制台删除记录。有关如何使用 Route 53 API 删除记录的信息，请参阅亚马逊 Route 53 API 参考ChangeResourceRecordSets中的。

> **Note**
>
> 您对记录的更改需要一定时间才会传播到 Route 53 DNS 服务器。目前，验证更改是否已传播的唯一方法是使用 GetChangeAPI 操作。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

删除记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在“Hosted Zones (托管区域)”页面上，选择包含您要删除的记录的托管区域所对应的那一行。
3. 在记录列表中，选择您要删除的记录。

   要选择多个连续的记录，请选择第一行，按住 Shift 键，然后选择最后一行。要选择多个不连续的记录，请选择第一行，按住 Ctrl 键，再选择其他行。

   不能删除类型值为 NS或 SOA 的记录。
4. 选择删除。
5. 选择 Delete（删除）以关闭对话框。

列出记录

以下步骤介绍如何使用 Amazon Route 53 控制台列出一个托管区域中的记录。有关如何使用 Route 53 API 列出记录的信息，请参阅亚马逊 Route 53 API 参考ListResourceRecordSets中的。

列出记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 在 Hosted Zones 页面上，选择托管区域的名称。
4. 若要更改搜索模式，请选择记录表右上角的齿轮图标。选择如下选项之一：

   - 自动

在此模式下，服务使用基于多条记录的筛选条件。“完整”模式适用于不到 2000 条记录，而“快速”模式适用于超过 2000 条记录。

- 完整

  在此模式下，所有搜索筛选条件均可用，但搜索性能可能会较慢。

- 快速

  在此模式下，某些高级功能不可用，但搜索性能会更较快。

要仅显示选定的记录，请在记录列表上方输入适用的搜索条件。在自动模式中，搜索行为取决于托管区域是最多包含 2000 条记录，还是包含 2000 条以上的记录：

最多 2,000 条记录和完整模式

- 要显示具有特定值的记录，请在搜索栏中输入一个值，然后按 Enter。例如，要显示 IP 地址以 192.0 开头的记录，请在搜索字段中输入该值，然后按 Enter。
- 要只显示具有相同 DNS 记录类型的记录，请在下拉列表中选择 Record type（记录类型），然后输入记录类型。
- 要仅显示别名记录，请在下拉列表中选择 Aliase（别名），然后输入 **`Yes`**。
- 要仅显示加权记录，请在下拉列表中选择 Routing policy（路由策略），然后输入 **`WEIGHTED`**。

超过 2,000 条记录和快速模式

- 您可以仅按记录名称，而不是按记录值进行搜索。另外，不能根据记录类型、别名或加权记录筛选。

  为此，请将光标置于筛选器文本框中，选择属性，然后选择记录名称。

- 对于有三个标签（三个部分由点分隔）的记录，在搜索字段中输入一个值并按 Enter 时，Route 53 控制台自动从记录名称右侧数起的第三个标签开始执行通配符搜索。例如，假设托管区域 example.com 包含名称为 record1.example.com 到 record100.example.com 的 100 个记录。(Record1 就是从右侧数起的第三个标签。) 看一下您搜索下列值时的结果：
  - record1 - Route 53 控制台搜索 record1*.example.com，会返回 record1.example.com、record10.example.com 到 record19.example.com，还有 record100.example.com。
  - record1.example.com - 在上一个例子中，控制台搜索 record1*.example.com 并返回相同的记录。
  - 1 - 控制台搜索 1*.example.com 且没有返回记录。

- example - 控制台搜索 example*.example.com 且没有返回记录。
- example.com - 在本示例中，控制台不执行通配符搜索。它返回托管区域中的所有记录。
- 自动搜索模式 - 使用此搜索模式时，必须先提供属性（例如记录名称）才能进行搜索。

> **Note**
>
> 如果右边的第三个标签包含一个或多个连字符（例如 `third-label.example.com`），并且在连字符之前搜索第三个标签的一部分（在本例中为 `third`），则 Route 53 不会返回任何记录。相反，要么包含连字符（搜索 `third-`），要么在连字符之前省略字符（搜索 `third`）。

- 对于具有四个或多个标签的记录，必须指定确切的记录名称。不支持通配符搜索。例如，如果托管区域包含一个名为 label4.record1.example.com 的记录，那么只有在搜索字段中指定 label4.record1.example.com 才能找到该记录。

在 Amazon Route 53 中配置 DNSSEC 签名

域名系统安全扩展 (DNSSEC) 签名允许 DNS 解析程序验证来自 Amazon Route 53 且未被篡改的 DNS 响应。使用 DNSSEC 签名时，托管区域的每个响应都使用公有密钥加密技术进行签名。有关 DNSSEC 的概述，请参阅 Amazon re:Invent 2021 - Amazon Route 53：年度回顾中的 DNSSEC 部分。

在本章中，我们将说明如何为 Route 53 启用 DNSSEC 签名、如何使用密钥签名密钥 (KSKs) 以及如何解决问题。您可以使用 DNSSEC 登录 Amazon Web Services 管理控制台 或以编程方式使用 API。有关使用 CLI 或使用 Rou SDKs te 53 的更多信息，请参阅设置 Amazon Route 53。

在启用 DNSSEC 签名之前，请注意以下事项：

- 为了帮助防止区域中断并避免域变得不可用的问题，您必须快速解决和处理 DNSSEC 错误。我们强烈建议您设置 CloudWatch 警报，在检测到`DNSSECInternalFailure`或`DNSSECKeySigningKeysNeedingAction`错误时提醒您。有关更多信息，请参阅 使用 Amazon 监控托管区域 CloudWatch。
- DNSSEC 中有两种密钥：密钥签名密钥 (KSK) 和区域签名密钥 (ZSK)。在 Route 53 DNSSEC 签名中，每个 KSK 都基于您拥有的 Amazon KMS 中的非对称客户托管密钥。您负责 KSK 管理，其中包括根据需要进行轮换。ZSK 管理由 Route 53 执行。

- 当您为托管区域启用 DNSSEC 签名时，Route 53 将 TTL 限制为一周。如果您为托管区域中的记录设置了一周以上的 TTL，则不会出现错误。但是，Route 53 对记录强制执行一周的 TTL。TTL 少于一周的记录和其它托管区域中未启用 DNSSEC 签名的记录不受影响。
- 当您使用 DNSSEC 签名时，不支持多供应商配置。如果您配置了白标域名称服务器（也称为虚名称服务器或私有名称服务器），请确保这些名称服务器由单一 DNS 提供商提供。
- 某些 DNS 提供商在其权威 DNS 中不支持委派签名者（DS）记录。如果您的父区域由不支持 DS 查询（未在 DS 查询响应中设置 AA 标志）的 DNS 提供商托管，则当您在其子区域中启用 DNSSEC 时，子区域将变得无法解析。确保您的 DNS 提供商支持 DS 记录。
- 设置 IAM 权限以允许除区域拥有者之外的其他用户添加或删除区域中的记录非常有用。例如，区域拥有可以添加 KSK 并启用签名，还可能负责密钥转动。但是，其他人可能负责使用托管区域的其它记录。有关 IAM policy 示例，请参阅 域记录所有者的权限示例。
- 要查看该顶级域是否支持 DNSSEC，请参阅 可向 Amazon Route 53 注册的域。 。

主题

启用 DNSSEC 签名并建立信任链。

递增步骤适用于托管区域拥有者和父区域维护者。这二者可以是同一个人，但如果不是，区域拥有者应该通知父区域维护者并与其合作。

我们建议按照本文中的步骤对区域进行签名并将其纳入信任链中。以下步骤将最大限度地降低启用 DNSSEC 所存在的风险。

> **Note**
>
> 在 在 Amazon Route 53 中配置 DNSSEC 签名 中开始之前，请务必阅读先决条件。

启用 DNSSEC 签名需要执行三个步骤，如以下几节所述。

主题

步骤 1：准备启用 DNSSEC 签名

准备步骤可通过监控区域可用性并减少启用签名与插入委派签名者 (DS) 记录之间的等待时间，帮助您最大限度地降低启用 DNSSEC 所存在的风险。

准备启用 DNSSEC 签名

1. 监控区域可用性。

   您可以监控区域以了解域名的可用性。这可以帮助您在启用 DNSSEC 签名后解决可能需要回滚的任何问题。您可以使用查询日志记录来监控流量最多的域名。有关设置查询日志记录的更多信息，请参阅 监控 Amazon Route 53。

   可以通过 Shell 脚本或第三方服务来完成监控。但是，其不应作为确定是否需要回滚的唯一信号。由于域名不可用，您也可能会从客户处获得反馈。

2. 降低区域的最大 TTL。

   区域的最大 TTL 是该区域中最长的 TTL 记录。在以下示例区域中，区域的最大 TTL 为 1 天（86400 秒）。

Name	TTL	记录类	记录类型	记录数据
example.com。	900	IN	SOA	ns1.example.com. hostmaster.example.com。2002022401 10800 15 604800 300

Name	TTL	记录类	记录类型	记录数据
example.com。	900	IN	NS	ns1.example.com。
route53.example.com。	86400	IN	TXT	**some txt record**

降低区域的最大 TTL 将有助于缩短启用签名与插入委派签名者 (DS) 记录之间的等待时间。我们建议将区域的最大 TTL 降低到 1 小时（3600 秒）。如果任何解析程序在缓存已签名记录时遇到问题，您可以在一个小时后回滚。

回滚：撤消 TTL 更改。

3. 降低 SOA TTL 和 SOA 最小字段。

SOA 最小字段是 SOA 记录数据中的最后一个字段。在以下 SOA 记录示例中，最小字段的值为 5 分钟（300 秒）。

Name	TTL	记录类	记录类型	记录数据
example.com。	900	IN	SOA	ns1.example.com. hostmaster.example.com。2002022401 10800 15 604800 300

SOA TTL 和 SOA 最小字段决定了解析程序记住否定回答的时长。启用签名后，Route 53 名称服务器开始返回否定回答的 NSEC 记录。NSEC 包含解析程序可能用来综合否定回答的信息。如果由于 NSEC 信息导致解析程序对姓名假定否定回答而必须回滚，那么您只需等待 SOA TTL 和 SOA 最小字段的最大值，解析程序就会停止假定。

回滚：撤消 SOA 更改。

4. 确保 TTL 和 SOA 最小字段更改有效。

   用于确保您GetChange到目前为止所做的更改已传播到所有 Route 53 DNS 服务器。

步骤 2：启用 DNSSEC 签名并创建 KSK

您可以在 Route 53 控制台上使用 Amazon CLI 或启用 DNSSEC 签名并创建密钥签名密钥 (KSK)。

- CLI
- 控制台

当您提供或创建 KMS 密钥时，应遵循以下几个要求。有关更多信息，请参阅 使用适用于 DNSSEC 的客户托管密钥。

CLI

您可以使用已有密钥，或通过使用自己的 `hostedzone_id`、`cmk_arn`、`ksk_name` 和 `unique_string` 值运行如下 Amazon CLI 命令来创建密钥（以确保请求是唯一的）：

```
aws --region us-east-1 route53 create-key-signing-key \
   --hosted-zone-id $hostedzone_id \
   --key-management-service-arn $cmk_arn --name $ksk_name \
   --status ACTIVE \
   --caller-reference $unique_string
```

有关客户托管式密钥的更多信息，请参阅 使用适用于 DNSSEC 的客户托管密钥。另请参阅CreateKeySigningKey。

要启用 DNSSEC 签名，请使用您自己的值运行如下 Amazon CLI 命令：`hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

有关更多信息，请参阅enable-hosted-zone-dnssec和 EnableHostedZoneDNSSEC。

Console

要启用 DNSSEC 签名并创建 KSK

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择您要为其启用 DNSSEC 签名的托管区域。
3. 在 DNSSEC signing（DNSSEC 签名）选项卡上，选择 Enable DNSSEC signing（启用 DNSSEC 签名）。

> **Note**
>
> 如果本部分中的选项为 Disable DNSSEC signing（禁用 DNSSEC 签名），则表示您已完成启用 DNSSEC 签名的第一步。请确保您为 DNSSEC 的托管区域建立了信任链，或者此区域已经存在信任链，然后您便完成了操作。有关更多信息，请参阅 步骤 3：建立信任链。

4. 在 Key-signing key (KSK) creation（密钥签名密钥 (KSK) 创建）部分，选择 Create new KSK（创建新的 KSK），并在 Provide KSK name（提供 KSK 名称）下输入 Route 53 将为您创建的 KSK 名称。名称只能包含字母、数字和下划线 (_)。此名称必须唯一。
5. 在 Customer managed CMK（客户托管 CMK）中，选择 Route 53 在为您创建 KSK 时要使用的客户管理密钥。您可以使用适用于 DNSSEC 签名的现有客户托管密钥，也可以创建新的客户托管密钥。

   当您提供或创建客户托管密钥时，有几个要求。有关更多信息，请参阅 使用适用于 DNSSEC 的客户托管密钥。
6. 输入现有客户托管密钥的别名。如果要使用新的客户托管式密钥，请输入客户托管密钥的别名，Route 53 将为您创建密钥。

> **Note**
>
> 如果您选择让 Route 53 创建客户托管密钥，请注意，每个客户托管密钥都会单独收取费用。有关更多信息，请参阅 Amazon 密钥管理服务定价。

7. 选择 Enable DNSSEC signing（启用 DNSSEC 签名）。

启用区域签名后，请完成以下步骤（无论是使用控制台还是 CLI）：

1. 确保区域签名有效。

   如果你使用了 Amazon CLI，你可以使用`EnableHostedZoneDNSSEC()`调用输出中的操作 ID 来运行 get-change 或GetChange确保所有 Route 53 DNS 服务器都在签署响应（status =`INSYNC`）。

2. 至少等待前一个区域的最大 TTL 的时长。

   等待解析程序清除其缓存中的所有未签名记录。为此，等待时长至少应为前一个区域的最大 TTL。在上面的 `example.com` 区域，等待时间为 1 天。

3. 监控客户问题报告。

   启用区域签名后，客户可能会开始看到与网络设备和解析程序相关的问题。建议的监控周期为 2 周。

   下面是可能会看到的问题示例：

   - 某些网络设备可以将 DNS 响应大小限制在 512 字节以下，这对于某些签名响应来说太小。应重新配置这些网络设备，以便允许更大的 DNS 响应。
   - 一些网络设备对 DNS 响应进行深入检查并删除其无法理解的某些记录，如用于 DNSSEC 的记录。应该重新配置这些设备。
   - 一些客户的解析程序称可以接受比其网络支持的响应大小更大的 UDP 响应。您可以测试网络功能并适当配置解析程序。有关更多信息，请参阅 DNS 回复大小测试服务器。

回滚：调用 DisableHostedZoneDNSSEC，然后回滚中的步骤。步骤 1：准备启用 DNSSEC 签名

步骤 3：建立信任链

在 Route 53 中为托管区域启用 DNSSEC 签名后，请为托管区域建立信任链，以完成 DNSSEC 签名设置。您可以通过在父托管区域创建 Delegation Signer (DS) 记录，并使用 Route 53 提供的信息，以完成此操作。根据域注册的位置，您可以将记录添加到 Route 53 中的父托管区域或其它域注册商。

要建立 DNSSEC 签名信任链。

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择要为其建立 DNSSEC 信任链的托管区域。您必须首先启用 DNSSEC 签名。
3. 在 DNSSEC signing（DNSSEC 签名）选项卡，在 DNSSEC signing（DNSSEC 签名）中，选择 View information to create DS record（查看信息以创建 DS 记录）。

   > **Note**
   >
   > 如果您没有在本部分中看到 View information to create DS record（查看信息以创建 DS 记录），那么在建立信任链之前，必须启用 DNSSEC 签名。选择 Enable DNSSEC

signing（启用 DNSSEC 签名）并完成 步骤 2：启用 DNSSEC 签名并创建 KSK 中的所述步骤，然后回到这些步骤建立信任链。

4. 在 Establish a chain of trust（建立信任链）中，选择 Route 53 registrar（Route 53 注册商）或者 Another domain registrar（另一域注册商），具体取决于您的域注册位置。
5. 使用步骤 3 提供的值以在 Route 53 中为父托管区域创建 DS 记录。如果您的域未托管在 Route 53，请使用提供的值在域注册商网站上创建 DS 记录。

   要建立父区域的信任链：

   - 如果通过 Route 53 管理您的域，请执行以下步骤：

     确保配置正确的签名算法（ECDSAP256SHA256 以及类型 13）和摘要算法（SHA-256 和类型 2）。

     如果 Route 53 是您的注册商，请在 Route 53 控制台中执行以下操作：

     1. 请注意 Key type（密钥类型）、Signing algorithm（签名算法）和 Public key（公有密钥）的值。在导航窗格中，选择 Registered domains。
     2. 选择一个域，然后在 DNSSEC 密钥选项卡中选择添加密钥。
     3. 在管理 DNSSEC 密钥对话框中，从下拉菜单中为 Route 53 注册商选择适当的密钥类型和算法。
     4. 为 Route 53 注册商复制 Public key（公有密钥）。在 Manage DNSSEC keys（管理 DNSSEC 密钥）对话框中，将值粘贴到 Public key（公有密钥）框中。
     5. 选择添加。

        Route 53 会将 DS 记录从公有密钥添加到父区域。例如，如果您的域是 `example.com`，则 DS 记录会添加到 .com DNS 区域。

   - 如果您的域托管在其他注册机构处，请按照其他域名注册商部分中的说明进行操作。

     为确保以下步骤顺利进行，请将低 DS TTL 引入父区域。如果您需要回滚更改，我们建议将 DS TTL 设置为 5 分钟（300 秒）以加快恢复速度。

     - 要建立子区域的信任链：

       如果您的父区域由其他注册表管理，请联系注册商以引入区域的 DS 记录。通常无法调整 DS 记录的 TTL。

     - 如果您的父区域托管在 Route 53 上，请联系父区域拥有者以引入区域的 DS 记录。

将 $ds_record_value 提供给父区域拥有者。您可以通过单击 “查看信息” 在控制台中创建 DS 记录并复制 D S 记录字段，或者调用 getDNSSec API 并检索 “” 字段的值来获取它：DSRecord

```
aws --region us-east-1 route53 get-dnssec
            --hosted-zone-id $hostedzone_id
```

父区域拥有者可以通过 Route 53 控制台或 CLI 插入记录。

- 要使用插入 DS 记录 Amazon CLI，父区域所有者创建并命名了一个类似于以下示例的 JSON 文件。父区域拥有者可能会将文件命名为 inserting_ds.json。

```
{
    "HostedZoneId": "$parent_zone_id",
    "ChangeBatch": {
        "Comment": "Inserting DS for zone $zone_name",
        "Changes": [
            {
                "Action": "UPSERT",
                "ResourceRecordSet": {
                    "Name": "$zone_name",
                    "Type": "DS",
                    "TTL": 300,
                    "ResourceRecords": [
                        {
                            "Value": "$ds_record_value"
                        }
                    ]
                }
            }
        ]
    }
}
```

然后运行以下命令：

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- 要使用控制台插入 DS 记录，

打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

在导航窗格中，选择 Hosted zones（托管区域）、托管区域的名称，然后选择 Create record（创建记录）按钮。确保为 Routing policy（路由策略）选择简单路由。

在记录名称字段中输入与 `$zone_name` 相同的名称，从记录类型下拉菜单中选择 DS，并在值字段中输入 `$ds_record_value` 的值，然后选择创建记录。

回滚：从父区域中删除 DS，等待 DS TTL，然后回滚建立信任的步骤。如果父区域托管在 Route 53 上，父区域拥有者可以将 JSON 文件中的 `Action` 从 `UPSERT` 更改为 `DELETE`，然后重新运行上面的示例 CLI。

6. 等待更新传播，具体基于域记录的 TTL。

   如果父区域使用的是 Route 53 DNS 服务，则父区域所有者可以通过 GetChangeAPI 确认完全传播。

   否则，您可以定期检查 DS 记录的父区域，然后再等 10 分钟，以提高完整传播 DS 记录插入的可能性。请注意，一些注册商计划了 DS 插入，例如，每天一次。

在父区域中引入委派签名者 (DS) 记录时，已获取 DS 的经验证的解析程序将开始验证来自该区域的响应。

为了确保建立信任的步骤顺利进行，请完成以下操作：

1. 找到最大 NS TTL。

   有 2 组 NS 记录与您的区域相关：

   - 委托 NS 记录 — 这是由父区域持有的您的区域的 NS 记录。您可以通过运行如下 Unix 命令找到此记录（如果区域为 example.com，则父区域为 com）：

     ```
     dig -t NS com
     ```

     选择一个 NS 记录，然后运行以下命令：

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     例如：

```
dig @b.gtld-servers.net. -t NS example.com
```

- 区内 NS 记录 — 这是您的区域中的 NS 记录。您可以通过运行以下 Unix 命令找到此记录：

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  例如：

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  请注意两个区域的最大 TTL。

2. 等待最大 NS TTL。

   在 DS 插入之前，解析程序获得签名响应，但未验证签名。插入 DS 记录后，在区域的 NS 记录到期之前，解析程序无法看到该记录。当解析程序重新获取 NS 记录时，也将会返回 DS 记录。

   如果您的客户在时钟不同步的主机上运行解析程序，请确保时钟与正确时间相差 1 小时以内。

   完成此步骤后，所有 DNSSEC 感知解析程序将会验证您的区域。

3. 注意名称解析。

   应注意解析程序验证您的区域时没有出现问题。确保同时考虑到客户向您报告问题所需的时间。

   我们建议监控最长 2 周时间。

4. （可选）加长 DS 和 N TTLs S 的长度。

   如果对设置满意，可以保存所做的 TTL 和 SOA 更改。请注意，Route 53 将已签名区域的 TTL 限制为 1 周。有关更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

   如果您可以更改 DS TTL，建议将其设置为 1 小时。

禁用 DNSSEC 签名

在 Route 53 中禁用 DNSSEC 签名的步骤有所不同，具体取决于托管区域所属的信任链。

例如，您的托管区域可能具有包含 Delegation Signer (DS) 记录的父区域，作为信任链的一部分。托管区域本身也可能是启用 DNSSEC 签名的子区域的父区域，这是信任链的另一部分。在执行禁用 DNSSEC 签名的步骤之前，请调查并确定托管区域的完整信任链。

在禁用签名时，必须仔细撤消托管区域启用 DNSSEC 签名的信任链。要从信任链中删除托管区域，请删除包含此托管区域的信任链的所有 DS 记录。这意味着您必须按顺序执行以下操作：

1. 删除此托管区域对于属于信任链一部分的子区域具有的所有 DS 记录。
2. 从父区域删除 DS 记录。如果您具有信任岛（父区域中没有 DS 记录，此区域中的子区域没有 DS 记录），则可以跳过此步骤。
3. 如果无法删除 DS 记录，为了从信任链中删除该区域，请从父区域中删除 NS 记录。有关更多信息，请参阅 为域添加或更改名称服务器和粘附记录。

通过以下递增步骤，您可以监控各个步骤的有效性，以避免区域中的 DNS 可用性问题。

禁用 DNSSEC 签名

1. 监控区域可用性。

   您可以监控区域以了解域名的可用性。这可以帮助您在启用 DNSSEC 签名后解决可能需要回滚的任何问题。您可以使用查询日志记录来监控流量最多的域名。有关设置查询日志记录的更多信息，请参阅 监控 Amazon Route 53。

   可以通过 Shell 脚本或付费服务完成监控。但是，其不应作为确定是否需要回滚的唯一信号。由于域名不可用，您也可能会从客户处获得反馈。
2. 查找当前 DS TTL。

   您可以通过运行以下 Unix 命令找到 DS TTL：

   ```
   dig -t DS example.com example.com
   ```
3. 找到最大 NS TTL。

   有 2 组 NS 记录与您的区域相关：

   - 委托 NS 记录 — 这是由父区域持有的您的区域的 NS 记录。您可以通过运行以下 Unix 命令找到此记录：

     首先找到父区域的 NS（如果您的区域为 example.com，则父区域为 com）：

     ```
     dig -t NS com
     ```

     选择一个 NS 记录，然后运行以下命令：

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

例如：

```
dig @b.gtld-servers.net. -t NS example.com
```

- 区内 NS 记录 — 这是您的区域中的 NS 记录。您可以通过运行以下 Unix 命令找到此记录：

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  例如：

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  请注意两个区域的最大 TTL。

4. 从父区域删除 DS 记录。

   请与父区域拥有者联系以删除 DS 记录。

   回滚：重新插入 DS 记录，确认 DS 插入有效，并等待最大 NS（而不是 DS TTL），然后所有解析程序将再次开始验证。

5. 确认删除 DS 是否有效。

   如果父区域使用的是 Route 53 DNS 服务，则父区域所有者可以通过 GetChangeAPI 确认完全传播。

   否则，您可以定期检查 DS 记录的父区域，然后再等 10 分钟，以提高完整传播 DS 记录删除的可能性。请注意，一些注册商计划了 DS 删除，例如，每天一次。

6. 等待 DS TTL。

   等待直到所有解析程序缓存中的 DS 记录过期。

7. 禁用 DNSSEC 签名并停用密钥签名密钥 (KSK)。

   - CLI
   - 控制台

   CLI

   致电 DisableHostedZoneDNSSEC 然后。DeactivateKeySigningKey APIs

   例如：

```
aws --region us-east-1 route53 disable-hosted-zone-dnssec \
            --hosted-zone-id $hostedzone_id

aws --region us-east-1 route53 deactivate-key-signing-key \
            --hosted-zone-id $hostedzone_id --name $ksk_name
```

Console

禁用 DNSSEC 签名

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择您要为其禁用 DNSSEC 签名的托管区域。
3. 在 DNSSEC signing（DNSSEC 签名）选项卡上，选择 Disable DNSSEC signing（禁用 DNSSEC 签名）。
4. 在 Disable DNSSEC signing（禁用 DNSSEC 签名）的页面上，根据您要禁用 DNSSEC 签名的区域，选择以下任一选项。
   - 仅限父区域 — 此区域具有带有 DS 记录的父区域。在这种情况下，您必须删除父区域的 DS 记录。
   - 仅限子区域 — 此区域具有包含一个或多个子区域的信任链的 DS 记录。在这种情况下，您必须删除区域的 DS 记录。
   - 父区域和子区域 — 此区域包含一个或多个子区域的信任链的 DS 记录以及具有 DS 记录的父区域。对于此场景，请执行以下操作：

     a. 删除区域的 DS 记录。

     b. 删除父区域的 DS 记录。

     如果您具有信任岛，可跳过本步骤。
5. 确定您在步骤 4 中删除的每个 DS 记录的 TTL，请确保最长的 TTL 时间已过期。
6. 选中复选框以确认您已按顺序执行步骤。
7. 在字段中键入 disable，如图所示，然后选择 Disable（禁用）。

停用密钥签名密钥 (KSK) 的步骤

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择您要为其停用密钥签名密钥的托管区域。
3. 在 “密钥签名密钥” (KSKs) 部分，选择要停用的 KSK，然后在 “操作” 下，选择 “编辑 KSK”，将 KSK 状态设置为 “非活动”，然后选择 “保存 KSK”。

回滚：呼叫ActivateKeySigningKey和 EnableHostedZoneDN APIs SSEC。

例如：

```
aws --region us-east-1 route53 activate-key-signing-key \
            --hosted-zone-id $hostedzone_id --name $ksk_name

aws --region us-east-1 route53 enable-hosted-zone-dnssec \
            --hosted-zone-id $hostedzone_id
```

8. 确认禁用区域签名是否有效。

   使用EnableHostedZoneDNSSEC()呼叫中的 ID 进行运行 GetChange，确保所有 Route 53 DNS 服务器都已停止对响应进行签名（状态 =INSYNC）。

9. 注意名称解析。

   应注意解析程序验证您的区域时没有导致问题。还要考虑 1-2 周客户向您报告问题所需的时间。

10. （可选）清除。

    如果您不想重新启用签名，则可以清 KSKs 理DeleteKeySigningKey并删除相应的客户托管密钥以节省成本。

使用适用于 DNSSEC 的客户托管密钥

当您在 Amazon Route 53 中启用 DNSSEC 签名时，Route 53 会为您创建密钥签名密钥 (KSK)。要创建 KSK，Route 53 必须使用支持 DNSSEC Amazon Key Management Service 的客户托管密钥。本节介绍了有关客户管理密钥的详细信息和要求，在您使用 DNSSEC 时能够有所帮助。

在使用适用于 DNSSEC 的客户托管密钥时，请牢记以下几点：

- 与 DNSSEC 签名一起使用的客户托管密钥必须位于美国东部（弗吉尼亚北部）区域。
- 客户托管密钥必须是采用 ECC_NIST_P256 密钥规格的非对称客户托管密钥。这些客户托管密钥仅用于签名和验证。有关创建非对称客户托管密钥的帮助，请参阅 Amazon Key Management Service 开发人员指南中的创建非对称客户托管密钥。要帮助查找现有客户托管密钥的加密配置，请参阅 Amazon Key Management Service 开发人员指南中的查看客户托管密钥的加密配置。
- 如果您在 Route 53 中自行创建客户托管密钥以与 DNSSEC 一起使用，则必须包含特定的密钥策略语句，以便为 Route 53 提供所需的权限。Route 53 必须能够访问您的客户托管密钥，以便它可以为您创建 KSK。有关更多信息，请参阅 DNSSEC 签名所需的 Route 53 客户托管密钥权限。
- Route 53 可以创建客户托管密钥供您使用 DNSSEC 签名，无需额外 Amazon KMS 权限。 Amazon KMS 但是，如果要在创建密钥后对其进行编辑，则必须具有特定的权限。您必须具有以下特定权限：`kms:UpdateKeyDescription`、`kms:UpdateAlias` 和 `kms:PutKeyPolicy`。
- 请注意，无论您是创建客户托管密钥还是让 Route 53 为您创建密钥，您拥有的每个客户托管密钥都会单独收取费用。有关更多信息，请参阅Amazon Key Management Service 定价。

使用密钥签名密钥 () KSKs

启用 DNSSEC 签名时，Route 53 会为您创建密钥签名密钥 (KSK)。在 Route 53 中， KSKs 每个托管区域最多可以有两个。启用 DNSSEC 签名后，您可以添加、删除或编辑您的。 KSKs

使用您的设备时，请注意以下几点 KSKs：

- 在删除 KSK 之前，您必须编辑 KSK 以将其状态设置为 Inactive（非活动）。
- 当为托管区域启用 DNSSEC 签名时，Route 53 会将 TTL 限制为一周。如果将托管区域中记录的 TTL 设置为超过一周，则不会出现错误，但 Route 53 会强制执行一周的 TTL。
- 为了帮助防止区域中断并避免域变得不可用的问题，您必须快速解决和处理 DNSSEC 错误。我们强烈建议您设置 CloudWatch 警报，在检测到`DNSSECInternalFailure`或`DNSSECKeySigningKeysNeedingAction`错误时提醒您。有关更多信息，请参阅 使用 Amazon 监控托管区域 CloudWatch。
- 本节中描述的 KSK 操作允许您轮换区域。 KSKs有关更多信息和 step-by-step示例，请参阅博客文章使用 Amazon Route 53 配置 DNSSEC 签名和验证中的 DNSSEC 密钥轮换。

要 KSKs 在中使用 Amazon Web Services 管理控制台，请按照以下各节中的指导进行操作。

添加密钥签名密钥 (KSK)

启用 DNSSEC 签名时，Route 53 会为您创建密钥签名密钥 (KSK)。您也可以 KSKs 单独添加。在 Route 53 中， KSKs 每个托管区域最多可以有两个。

创建 KSK 时，您必须提供或请求 Route 53 以创建用于 KSK 的客户托管密钥。当您提供或创建客户托管密钥时，有几个要求。有关更多信息，请参阅 使用适用于 DNSSEC 的客户托管密钥。

请按照以下步骤在 Amazon Web Services 管理控制台中添加 KSK。

要添加 KSK

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择一个托管区域。
3. 在 DNSSEC 签名选项卡的密钥签名密钥 (KSKs) 下，选择切换到高级视图，然后在操作下选择添加 KSK。
4. 在 KSK 项下，输入 Route 53 将为您创建的 KSK 的名称。名称只能包含字母、数字和下划线 (_)。此名称必须唯一。
5. 输入适用于 DNSSEC 签名的客户托管密钥，或输入 Route 53 将为您创建的新客户托管密钥的别名。

   > **Note**
   >
   > 如果您选择让 Route 53 创建客户托管密钥，请注意，每个客户托管密钥都会单独收取费用。有关更多信息，请参阅Amazon Key Management Service 定价。

6. 选择 Create KSK（创建 KSK）。

编辑密钥签名密钥 (KSK)

您可以将 KSK 的状态编辑为 Active（活动）或者 Inactive（非活动）。当 KSK 处于活动状态时，Route 53 将使用该 KSK 进行 DNSSEC 签名。在删除 KSK 之前，您必须编辑 KSK 以将其状态设置为 Inactive（非活动）。

按照以下步骤在 Amazon Web Services 管理控制台中编辑 KSK。

要编辑 KSK

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择一个托管区域。
3. 在 DNSSEC 签名选项卡的密钥签名密钥 (KSKs) 下，选择切换到高级视图，然后在操作下选择编辑 KSK。
4. 对 KSK 进行所需的更新，然后选择 Save（保存）。

删除密钥签名密钥 (KSK)

在删除 KSK 之前，您必须编辑 KSK 以将其状态设置为 Inactive（非活动）。

您可能删除 KSK 的原因之一是例行密钥转动的一部分。定期转动加密密钥是最佳实践。您的组织可能有关于转动密钥频率的标准指导。

请按照以下步骤在 Amazon Web Services 管理控制台中删除 KSK。

要删除 KSK

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域），然后选择一个托管区域。
3. 在 DNSSEC 签名选项卡的密钥签名密钥 (KSKs) 下，选择切换到高级视图，然后在操作下选择删除 KSK。
4. 按照指导确认删除 KSK。

Route 53 中的 KMS 密钥和 ZSK 管理

本节介绍 Route 53 用于启用 DNSSEC 签名的区域的当前做法。

> **Note**
>
> Route 53 将使用以下规则（可能更改）。未来的任何更改都不会降低您的区域或 Route 53 的安保状况。

Route 53 如何使用与你的 KSK Amazon KMS 关联的

在 DNSSEC 中，KSK 用于为 DNSKEY 资源记录集生成资源记录签名（RRSIG)。所有这些ACTIVE KSKs 都用在 RRSIG 生成中。Route 53 通过在关联的 KMS 密钥上调用 Sign Amazon KMS API 来生成 RRSIG。有关更多信息，请参阅 Amazon KMS API 参考指南中的签名。这些RRSIGs不计入区域的资源记录集限制。

RRSIG 拥有过期期限。为防止过期，每隔一 RRSIGs 到 RRSIGs 七天对其进行一次再生，从而定期刷新。

每次您拨打 RRSIGs 以下任一电话时，也会刷新： APIs

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

每次 Route 53 执行刷新时，我们都会生成 15 个刷新 RRSIGs 以覆盖接下来的几天，以防关联的 KMS 密钥无法访问。对于 KMS 密钥成本估算，您可以假设每天定期刷新一次。无意中对 KMS 密钥策略进行更改可能导致无法访问 KMS 密钥。无法访问的 KMS 密钥会将关联的 KSK 状态设置为 ACTION_NEEDED。我们强烈建议您在检测到DNSSECKeySigningKeysNeedingAction错误时通过设置 CloudWatch 警报来监控这种情况，因为验证解析器将在最后一个 RRSIG 到期后开始失败查找。有关更多信息，请参阅 使用 Amazon 监控托管区域 CloudWatch。

Route 53 如何管理区域的 ZSK

每个启用 DNSSEC 签名的新托管区域都将有一个 ACTIVE 区域签名密钥（ZSK)。ZSK 是为每个托管区域单独生成的，为 Route 53 所有。当前的密钥算法是 ECDSAP256SHA256。

我们将在签名开启后的 7—30 天内开始在该区域进行定期 ZSK 转动。目前，Route 53 使用“发布前密钥滚动”方法。有关更多信息，请参阅发布前区域签名密钥滚动。这种方法将向该区域引入另一个 ZSK。转动将每 7-30 天重复一次。

如果该区域的任何一个 KSK ACTION_NEEDED 处于状态，Route 53 将暂停 ZSK 轮换，因为 Route 53 将无法重新生成 for DNSKEY 资源记录集以应对该区域 ZSK 的变化。 RRSIGs 清除条件后，ZSK 转动将自动恢复。

Route 53 中的 DNSSEC 不存在证明

> **Note**
>
> Route 53 将使用以下规则（可能更改）。未来的任何更改都不会降低您的区域或 Route 53 的安保状况。

DNSSEC 中有三种不存在证明：

- 与查询名称匹配的记录的不存在证明。
- 与查询类型匹配的类型的不存在证明。
- 用于生成回应记录的通配符记录的存在证明。

Route 53 使用 BL 方法执行了与查询名称匹配的记录的不存在证明。有关更多信息，请参阅 BL。这是一种能够生成证明的紧凑表示法并防止区域步行的方式。

如果有记录与查询名称匹配但与查询类型不匹配（例如查询 web.example）。 com/AAAA but there is only web.example.com/Apresent），我们返回一个包含所有支持的资源记录类型的最小 NSEC（下一个安全）记录。

当 Route 53 从通配符记录中合成答案时，响应将不会附带通配符的下一条安全记录或 NSEC 记录。在某些实施过程（通常是执行离线签名）中会使用此类 NSEC 记录，以防止响应中的资源记录签名（RRRSIG）被重新使用来欺骗不同的响应。Route 53 对非 DNSKey 记录使用在线签名来生成 RRSIGs特定于该响应的响应，这些响应不能重复用于不同的响应。

DNSSEC 签名的问题排查

本节中的信息可以帮助您解决 DNSSEC 签名问题，包括启用、禁用和密钥签名密钥 ()。KSKs

启用 DNSSEC

在开始启用 DNSSEC 签名之前，请确保已阅读 在 Amazon Route 53 中配置 DNSSEC 签名 中的先决条件。

禁用 DNSSEC

为了安全地禁用 DNSSEC，Route 53 将检查目标区域是否在信任链中。它检查目标区域的父区域是否有目标区域的任何 NS 记录和 DS 记录。如果目标区域无法公开解析，例如，在查询 NS 和 DS

时获得 SERVFAIL 响应，则 Route 53 无法确定禁用 DNSSEC 是否安全。您可以联系父区域来解决这些问题，并稍后重试禁用 DNSSEC。

KSK 状态为 Action needed（需要操作）

当 Route 53 DNSSEC 无法访问相应的（由于权限更改或ACTION_NEEDED删除）时，KSK 可以将其KeySigningKey状态更改为 “需要操作” Amazon KMS key （或 Amazon KMS key 处于状态）。

如果 KSK 的状态是 Action needed（需要操作），这意味着最终会对使用 DNSSEC 验证解析程序的客户端造成区域中断，并且您必须迅速采取行动，防止生产区域变得无法解析。

要纠正此问题，请确保您的 KSK 所基于的客户托管式密钥已启用且具有正确的权限。有关所需权限的更多信息，请参阅 DNSSEC 签名所需的 Route 53 客户托管密钥权限。

修复 KSK 后，使用控制台或（如所述）再次将其激活。 Amazon CLI步骤 2：启用 DNSSEC 签名并创建 KSK

为了防止将来出现此问题，请考虑按照中的建议添加一个 Amazon CloudWatch 指标来跟踪 KSK 的状态。在 Amazon Route 53 中配置 DNSSEC 签名

KSK 状态为 Internal failure（内部故障）

当 KSK 的状态为内部故障（或处于KeySigningKey状态）时，INTERNAL_FAILURE在问题得到解决之前，您无法使用任何其他 DNSSEC 实体。在使用 DNSSEC 签名（包括使用此 KSK 或其它 KSK）之前，您必须采取措施。

要更正问题，请重试激活或停用 KSK。

要在使用时更正问题 APIs，请尝试启用签名 (EnableHostedZoneDNSSEC) 或禁用签名 (DisableHostedZoneD NSSEC)。

重要的是要及时纠正 Internal failure（内部故障）这一问题。在解决问题之前，您无法对托管区域进行任何其它更改，除了为修复 Internal failure（内部故障）所进行的操作。

使用 Amazon Cloud Map 创建记录和运行状况检查

如果您要将互联网流量或 Amazon VPC 内的流量路由到应用程序组件或微服务，则可以使用 Amazon Cloud Map 自动创建记录和（可选）运行状况检查。有关更多信息，请参见Amazon Cloud Map 开发人员指南。

DNS 约束和行为

DNS 消息传递受若干因素约束，这些因素会影响您创建和使用托管区域及记录的方式。本节将对这些因素加以说明。

最大响应大小

为了符合 DNS 标准，通过 UDP 发送的响应大小不超过 512 字节。超过 512 字节的响应将被截断，解析程序必须通过 TCP 重新发出请求。如果解析程序支持 RFC 2671 中定义的 EDNS0 并向 Amazon Route 53 公布了 EDNS0 选项，Route 53 将允许通过 UDP 发送的响应达到 4096 字节，而且不会截断。

“授权”部分的处理

为使查询成功，Route 53 会将相关托管区域的名称服务器 (NS) 记录附加到 DNS 响应的“授权”部分。对于找不到的名称（NXDOMAIN 响应），Route 53 会将相关托管区域的授权起始点 (SOA) 记录（如 RFC 1035 中定义）附加到 DNS 响应的“授权”部分。

“其他”部分的处理

Route 53 会将记录附加到“其它”部分。如果记录已知且合适，服务将为“应答”部分中引述的 MX、CNAME、NS 或 SRV 记录的任何目标附加 A 或 AAAA 记录。有关 DNS 记录类型的更多信息，请参阅支持的 DNS 记录类型。

相关主题

有关开始将域注册（而非仅 DNS 托管）转移到 Route 53 的更多信息，请参阅以下主题：

- 域转移的转移前核对清单 – 在转移域注册之前请完成此核对清单，以避免常见的转移失败。
- 将域注册转移到 Amazon Route 53 – 将域注册从其他注册商转移到 Route 53 的分步流程。
- 转移域 – 概述所有域转移选项，包括在 Amazon 账户之间的转移。

使用 Traffic Flow 来路由 DNS 流量

Traffic Flow 大大简化了在大型复杂配置中创建和维护记录的过程。

在以下情况下，管理托管区域中的相关记录可能具有挑战性：

- 您有很多执行相同操作的资源，例如为同一个域提供流量的 Web 服务器。
- 您希望使用别名记录和组合使用 Route 53 路由策略（如延迟、故障转移和加权）来创建复杂的记录树。

Traffic Flow 优势

为了更轻松地跟踪记录及其关系，Traffic Flow 通过以下功能简化了 DNS 记录的创建：

可视化编辑器

通过 Traffic Flow 可视化编辑器，您可以创建复杂的记录树并查看记录之间的关系。例如，您可以创建一个配置，其中延迟别名记录引用加权记录，而加权记录引用多个 Amazon Web Services 区域中的资源。每个配置称为流量策略。您可以免费创建任意数量的流量策略。

版本控制

您可以创建流量策略的多个版本，这样，在配置发生变化时不必从头开始。旧版本将继续存在，直到您删除它们；每个流量策略的默认限制为 1000 个版本。您可以选择为每个版本提供描述。

自动创建和更新记录

流量策略可以表示数十条甚至数百条记录。通过 Traffic Flow，您可以通过创建流量策略记录来自动创建所有这些记录。您可以在树的根中指定托管区域和记录的名称，例如 example.com 或 www.example.com，Route 53 会自动创建树中的所有其他记录。根记录（流量策略记录）将显示在托管区域的记录列表中；所有其它记录都将隐藏。

创建流量策略的新版本时，您可以选择性地更新使用先前流量策略版本创建的流量策略记录。更新流量策略记录时，Route 53 会自动更新树中的所有其它记录。您还可以通过再次更新流量策略记录以使用以前版本的流量策略，从而快速回滚更改。

> **Note**
>
> 您只能使用 Traffic Flow 为公有托管区创建记录。

地理位置临近度路由策略

使用 Traffic Flow 时，可以使用 Traffic Flow 视觉编辑器上的地理位置临近度地图，更直观地了解流量是如何路由到每个全球端点。有关更多信息，请参阅 地理位置临近度路由。

在不同托管区域中重用多个记录

您可以使用流量策略在多个公有托管区域中自动创建记录。例如，如果您对多个域名使用相同的 Web 服务器，则可以使用相同的流量策略在 example.com、example.org 和 example.net 的托管区域中创建流量策略记录。

当客户端提交对根记录名称（例如 example.com 或 www.example.com）的查询时，Route 53 会根据您用于创建相应流量策略记录的流量策略中的配置响应查询。

对于每个流量策略记录，每月都会产生费用。有关更多信息，请参阅 Amazon Route 53 定价的“流量”部分。

要尽量减少这些费用，您可以在托管区域中创建一个或多个别名记录，以引用该托管区域中的流量策略记录。例如，您可以为 example.com 创建一条流量策略记录，然后为 www.example.com 创建一条引用此流量策略记录的别名记录。

创建和管理流量策略

主题

- 创建流量策略
- 创建流量策略时指定的值
- 查看显示地理位置临近度设置效果的地图
- 创建流量策略的其他版本
- 通过使用 JSON 文档来创建流量策略
- 查看流量策略版本和关联的策略记录
- 删除流量策略版本和流量策略

创建流量策略

要创建流量策略，请执行以下过程。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

创建流量策略

1. 设计您的配置。有关复杂 DNS 路由配置的工作原理的信息，请参阅创建 Amazon Route 53 运行状况检查 中的配置 DNS 故障转移。
2. 基于您的配置设计，创建要用于终端节点的运行状况检查。
3. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
4. 在导航窗格中，选择 Traffic policies。
5. 选择 Create traffic policy。
6. 输入名称和可选描述，然后选择下一步。
7. 在编辑器上，在属性窗格中选择 DNS 资源记录类型。此类型将分配给您为此流量策略创建的所有资源记录。

   选择确认。有关更多信息，请参阅 创建流量策略时指定的值。
8. 在编辑器页面中，选择连接到，然后选择新路由规则、新端点、现有路由规则或现有端点之一。如果您选择新路由规则，请在属性窗格中选择该路由规则并选择确认。然后，在属性窗格中输入相应的值。重复此过程，直到您的策略完成。有关适用于每种连接类型值的更多信息，请参阅 创建流量策略时指定的值。

   您可以通过以下方式删除流量策略的规则、终端节点和分支：

   - 要删除规则或端点，请在编辑器中选择规则或端点，然后在属性窗格中选择删除。

> **Important**
>
> 如果您删除的规则具有子规则和终端节点，则 Amazon Route 53 也会删除所有子项。

- 如果将两个规则连接到同一个子规则或端点，并且要删除其中一个连接，请选择要删除的连接，然后在该连接的属性窗格中选择删除。

9. 选择创建策略。
10. 可选：在创建策略记录页面上，使用新的流量策略在一个托管区中创建一个或多个策略记录。有关更多信息，请参阅 创建或更新策略记录时指定的值。您也可以稍后在同一托管区域或其他托管区域中创建策略记录。

    如果您不想立即创建策略记录，请选择取消，控制台将显示您使用当前 Amazon 账户创建的流量策略和策略记录的列表。
11. 如果您在之前的步骤中指定了策略记录的设置，请选择创建策略记录。

Old console

创建流量策略

1. 设计您的配置。有关复杂 DNS 路由配置的工作原理的信息，请参阅创建 Amazon Route 53 运行状况检查 中的配置 DNS 故障转移。
2. 基于您的配置设计，创建要用于终端节点的运行状况检查。
3. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
4. 在导航窗格中，选择 Traffic policies。
5. 选择 Create traffic policy。
6. 在 Name policy 页面上，指定适用的值。有关更多信息，请参阅 创建流量策略时指定的值。
7. 选择下一步。
8. 在 Create traffic policy (创建流量策略) 策略名称 v1 页面上，指定适用的值。有关更多信息，请参阅 创建流量策略时指定的值。

   您可以通过以下方式删除流量策略的规则、终端节点和分支：

   - 要删除规则或终端节点，请单击框右上角的 x。

> **Important**
>
> 如果您删除的规则具有子规则和终端节点，则 Amazon Route 53 也会删除所有子项。

- 如果将两个规则连接到同一个子规则或终端节点，并且要删除其中一个连接，请将光标停留在要删除的连接上，然后单击该连接对应的 x。

9. 选择 Create traffic policy。
10. 可选：在 Create policy records with traffic policy (使用流量策略创建策略记录) 页面上，使用新的流量策略在一个托管区域中创建一个或多个策略记录。有关更多信息，请参阅 创建或更新策略记录时指定的值。您也可以稍后在同一托管区域或其他托管区域中创建策略记录。

    如果您不想立即创建策略记录，请选择跳过此步骤，控制台将显示您使用当前 Amazon 账户创建的流量策略和策略记录的列表。
11. 如果您在之前的步骤中指定了策略记录的设置，请选择 Create policy record。

创建流量策略时指定的值

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。除非另有说明，否则以下列表适用于两种控制台。

当您创建流量策略时，可指定以下值。

-
-
-
-
-
-
-
-

策略名称

输入描述流量策略的名称。此值会显示在控制台的流量策略列表中。流量策略的名称在创建后不可更改。

版本

当您创建流量策略或现有策略的新版本时，此值由 Amazon Route 53 自动分配。

版本说明

输入适用于此版流量策略的描述。此值会显示在控制台的流量策略版本列表中。

DNS 类型

使用此流量策略版本创建策略记录时，选择您希望 Amazon Route 53 分配给所有记录的 DNS 类型。有关受支持类型的列表，请参阅支持的 DNS 记录类型。

> **Important**
>
> 如果您正在创建现有流量策略的新版本，则可以更改 DNS 类型。但是，您无法编辑策略记录，并选择具有与用于创建该策略记录的流量策略版本不同的 DNS 类型的流量策略版本。例如，如果您使用具有 DNS type 为 A 的流量策略版本创建了策略记录，则无法编辑该策略记录，并选择具有任何其他 DNS type 值的流量策略版本。

如果要将流量路由到以下 Amazon 资源，请选择适用的值：

- CloudFront 分发-选择 A: IPv4 格式中的 IP 地址或格式为 AAAA: IP 地址。 IPv6

> **Note**
>
> CloudFront 别名端点不支持评估运行状况检查。但是，您可以创建运行状况检查来监控 CloudFront 终端节点。有关更多信息，请参阅 创建和更新运行状况检查。

- ELB 应用程序负载均衡器-选择 A: 格式为 IP 地址或 IPv4 格式为 AAAA: IP 地址。 IPv6
- ELB Classic 负载均衡器-选择 A: IPv4 格式中的 IP 地址或格式为 AAAA: IP 地址。 IPv6
- ELB 网络负载均衡器-选择 A: IPv4 格式中的 IP 地址或格式为 AAAA: IP 地址。 IPv6
- Elastic Beanst alk 环境：选择 A: 格式中的 IP 地址。 IPv4

- 配置为网站终端节点的 Amazon S3 存储桶：选择 IPv4 格式为 A: IP 地址。

连接到

基于您的配置设计选择适用的规则或终端节点。

故障转移规则

当您要配置主动–被动故障转移时，请选择此选项，在此情况下，一个资源会在可用时接受所有流量，而另一个资源会在第一个资源不可用时接受所有流量。

有关更多信息，请参阅 主动/被动故障转移。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

地理位置规则

当您希望 Amazon Route 53 基于用户的位置来响应 DNS 查询时，请选择此选项。

有关更多信息，请参阅 地理位置路由。

当您选择 Geolocation rule 时，还会选择发起请求的国家/地区或美国州。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

延迟规则

当您在多个 Amazon EC2 数据中心中有执行相同功能的资源，并且您希望 Route 53 使用延迟最佳的资源响应 DNS 查询时，请选择此选项。

当您选择延迟规则时，还应选择一个 Amazon Web Services 区域。

有关更多信息，请参阅 基于延迟的路由。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

地理位置临近度规则

当您希望 Route 53 根据资源的位置和（可选）您指定的偏差响应 DNS 查询时，请选择此选项。偏差能让您将更多流量发送到资源，或者从资源中发出更多流量。

当您选择 Geoproximity rule 时，请输入以下值：

终端节点位置

选择适用的值：

- 自定义（输入坐标）-如果您的终端节点不是 Amazon 资源，请选择自定义（输入坐标）。
- 答 Amazon Web Services 区域 — 如果您的终端节点是 Amazon 资源，请选择您在其中创建资源的。 Amazon Web Services 区域
- Amazon 本地区域-如果您的终端节点是一种 Amazon 资源，请选择您在其中创建资源的 Amazon 本地区域。

如果您使用 L Amazon ocal Zones，则必须先将其启用。有关更多信息，请参阅《Amazon Local Zones 用户指南》中的 Local Zones 入门。

有关可用的 Local Zones，请参阅 Amazon Local Zones 位置。

要了解 Amazon Web Services 区域 和 Local Zones 之间的区别，请参阅亚马逊 EC2 用户指南中的区域和区域。

> **Important**
>
> 单个地理位置邻近路由策略不能包含两个或多个地理上位于同一大都市区内的位置。

此外，一些区域 Amazon Web Services 区域 和 Local Zones，例如美国西部（俄勒冈州）和美国波特兰，彼此距离太近，无法在相同的地理邻近路由策略中使用。如果您需要将流量路由到同一大都市区内的多个位置，请改为定义地理位置邻近路由策略，为该区域的两个不同端点生成 50/50 加权路由规则（WRR），从而在这些端点之间均匀分配流量。

Coordinates

如果您为 Endpoint location（终端节点位置）选择了 Custom (enter coordinates)（自定义 [输入坐标]），请输入资源位置的纬度和经度。注意以下几点：

- 纬度代表赤道以南 (负) 或以北 (正) 的位置。有效值为 -90 度到 90 度。
- 经度代表主子午线以西 (负) 或以东 (正) 的位置。有效值为 -180 度到 180 度。
- 您可以从一些联机映射应用程序中获得纬度和经度。例如，在 Google 地图中，位置的 URL 指定了纬度和经度：

  https://www.google.com/maps/@ 47.6086111，-122.3409953,20z
- 您最多可以输入两位精度小数，例如 47.63。如果指定具有更高精度的值，Route 53 会将该值截断到小数点后的两个数位。对于赤道处的纬度和经度，0.01 度大约是 0.69 英里。

偏差

（可选）要更改 Route 53 路由到某个资源的流量所来自的地理区域的大小，请为 Bias（偏差）指定一个适用值：

- 要扩大 Route 53 从中将流量路由到资源的地理区域的大小，请为该偏差指定一个介于 1 和 99 之间的正整数。Route 53 将缩小相邻区域的大小。
- 要缩小 Route 53 从中将流量路由到资源的地理区域的大小，请指定一个介于 -1 和 -99 之间的负偏差。Route 53 将扩大相邻区域的大小。

> **Important**
>
> 偏差值的更改效果是相对的（基于其他资源的位置），而不是绝对的（基于距离）。因此，更改的影响是难以预测的。例如，根据您的资源所在的位置，将偏差从 10 更改为 15 可能意味着在纽约市大都会地区增加或减去大量流量之间的差异。我们建议您以较小的增量更改偏差并对结果进行评估，然后进行其他更改 (如果适用)。

有关更多信息，请参阅 地理位置临近度路由。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

多值应答规则

当您希望 Route 53 用随机选择的最多大约八条正常应答响应 DNS 查询时，请选择此选项。

有关更多信息，请参阅 多值应答路由。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

加权规则

当您具有执行相同功能的多个资源（例如，服务于相同网站的 Web 服务器），并希望 Route 53 按照您指定的比例（例如，1/3 路由到一台服务器，2/3 路由到另一台服务器）将流量路由到这些资源时，请选择此选项。

当您选择加权规则时，请输入要应用于此规则的权重。

有关更多信息，请参阅 加权路由。

> **Note**
>
> 默认情况下，评估目标运行状况处于选中状态，它将评估流量通过别名记录路由到的目标端点的运行状况。如果端点未通过别名记录接收 DNS 流量，则取消选中此项，如果您想监控端点的运行状况，请创建运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

端点

选择此选项可指定要将 DNS 查询路由到的资源，例如 CloudFront 分配或 Elastic Load Balancing 负载均衡器。

现有规则

当您要将 DNS 查询路由到此流量策略中的现有规则时，请选择此选项。例如，您可以创建两个或更多地理位置规则，这些规则会将不同国家/地区的查询路由到同一个故障转移规则。然后，该失效转移规则可能会将查询路由到两个 Elastic Load Balancing 负载均衡器。

如果流量策略不包含任何规则，则此选项不可用。

现有终端节点

当您要将 DNS 查询路由到现有终端节点时，请选择此选项。例如，如果您有两个失效转移规则，则您可能要将两个 On failover（辅助）选项的 DNS 查询路由到同一 Elastic Load Balancing 负载均衡器。

如果流量策略不包含任何终端节点，则此选项不可用。

值类型

选择适用的选项：

CloudFront 分布

如果要将流量路由到 CloudFront 分配，请选择此选项。只有在 DNS 类型中选择 A: IP 地址格式为 A: IP 地址或为 DNS 类型选择 IPv4格式为 AAAA: IP 地址时，该选项才可用。 IPv6

> **Note**
>
> CloudFront 别名端点不支持评估运行状况检查。但是，您可以创建运行状况检查来监控 CloudFront 终端节点。有关更多信息，请参阅 创建和更新运行状况检查。

ELB 应用程序负载均衡器

如果要将流量路由到 Elastic Load Balancing 应用程序负载均衡器，请选择此选项。只有在 DNS 类型中选择 A: IP 地址 IPv4 格式或格式为 AAAA: IP 地址时，该选项才可用。 IPv6

ELB 经典负载均衡器

如果要将流量路由到 Elastic Load Balancing 经典负载均衡器，请选择此选项。只有在 DNS 类型中选择 A: IP 地址IPv4 格式或格式为 AAAA: IP 地址时，该选项才可用。 IPv6

ELB 网络负载均衡器

如果要将流量路由到 Elastic Load Balancing 网络负载均衡器，请选择此选项。只有在 DNS 类型中选择 A: IP 地址IPv4 格式或格式为 AAAA: IP 地址时，该选项才可用。 IPv6

Elastic Beanstalk 环境

如果要将流量路由到 Elastic Beanstalk 环境，请选择此选项。只有在 DNS 类型中选择 A: IP 地址 IPv4 格式时，该选项才可用。

S3 网站终端节点

如果要将流量路由到配置为网站终端节点的 Amazon S3 存储桶，请选择此选项。只有在 DNS 类型中选择 A: IP 地址 IPv4 格式时，该选项才可用。

DNS type 类型的值

如果您希望 Route 53 使用 Value（值）字段中的值来响应 DNS 查询，请选择此选项。例如，如果您在创建此流量策略时针对 DNS type（DNS 类型）的值选择了 A，则 Value type（值类型）列表中的此选项将为 Type A value（类型 A 值）。这要求您在 “值” 字段中输入 IPv4 格式化的 IP 地址。Route 53 将利用 Value（值）字段中的 IP 地址来响应路由到此终端节点的 DNS 查询。

值

基于您针对值类型选择的选项，选择或输入一个值：

CloudFront 分布

从与当前 Amazon 账户关联的分配列表中选择一个 CloudFront 分配。

ELB 应用程序负载均衡器

从与当前 Amazon 账户关联的负载均衡器列表中选择一个 Elastic Load Balancing 应用程序负载均衡器。

ELB 经典负载均衡器

从与当前 Amazon 账户关联的负载均衡器列表中选择一个 Elastic Load Balancing Classic 负载均衡器。

ELB 网络负载均衡器

从与当前 Amazon 账户关联的负载均衡器列表中选择一个 Elastic Load Balancing 网络负载均衡器。

Elastic Beanstalk 环境

从与当前 Amazon Web Services 账户关联的环境列表中选择一个 Elastic Beanstalk 环境。

S3 网站终端节点

从配置为网站终端节点并与当前 Amazon 账户关联的 Amazon S3 存储桶列表中选择一个 Amazon S3 存储桶。

> **Important**
>
> 当您基于此流量策略创建策略记录时，您在此处选择的存储桶必须与您在策略记录为Policy record DNS name指定的域名 (如 www.example.com) 匹配。如果 Value（值）与 Policy record DNS name（策略记录 DNS 名称）不匹配，则 Amazon S3 不会响应该域名的 DNS 查询。

DNS type 类型的值

输入一个值，该值与当您启动此流量策略时为 DNS type 指定的值对应。例如，如果您针对 DNS type (DNS 类型) 选择了 MX，请输入两个值：您希望分配到邮件服务器的优先级，以及该邮件服务器的域名，例如 `10 sydney.mail.example.com`。

有关支持的 DNS 类型的更多信息，请参阅支持的 DNS 记录类型。

键（仅限新控制台）

输入路由规则或键端点的友好名称。此值在编辑器中显示为节点的名称。

查看显示地理位置临近度设置效果的地图

地理邻近性规则允许您指定资源的位置，包括在 Amazon Web Services 区域、或 Local Zones 中，以及使用纬度和经度在非Amazon 位置中的位置。在您创建地理位置临近度规则时，默认情况下，Route 53 会将互联网流量路由到与您用户最接近的资源。您还可以选择通过指定偏差将更多流量或更少流量路由到给定的资源，该偏差值可扩大或缩小路由到资源的流量所来自的地理区域的大小。有关地理位置临近度路由的更多信息，请参阅地理位置临近度路由。

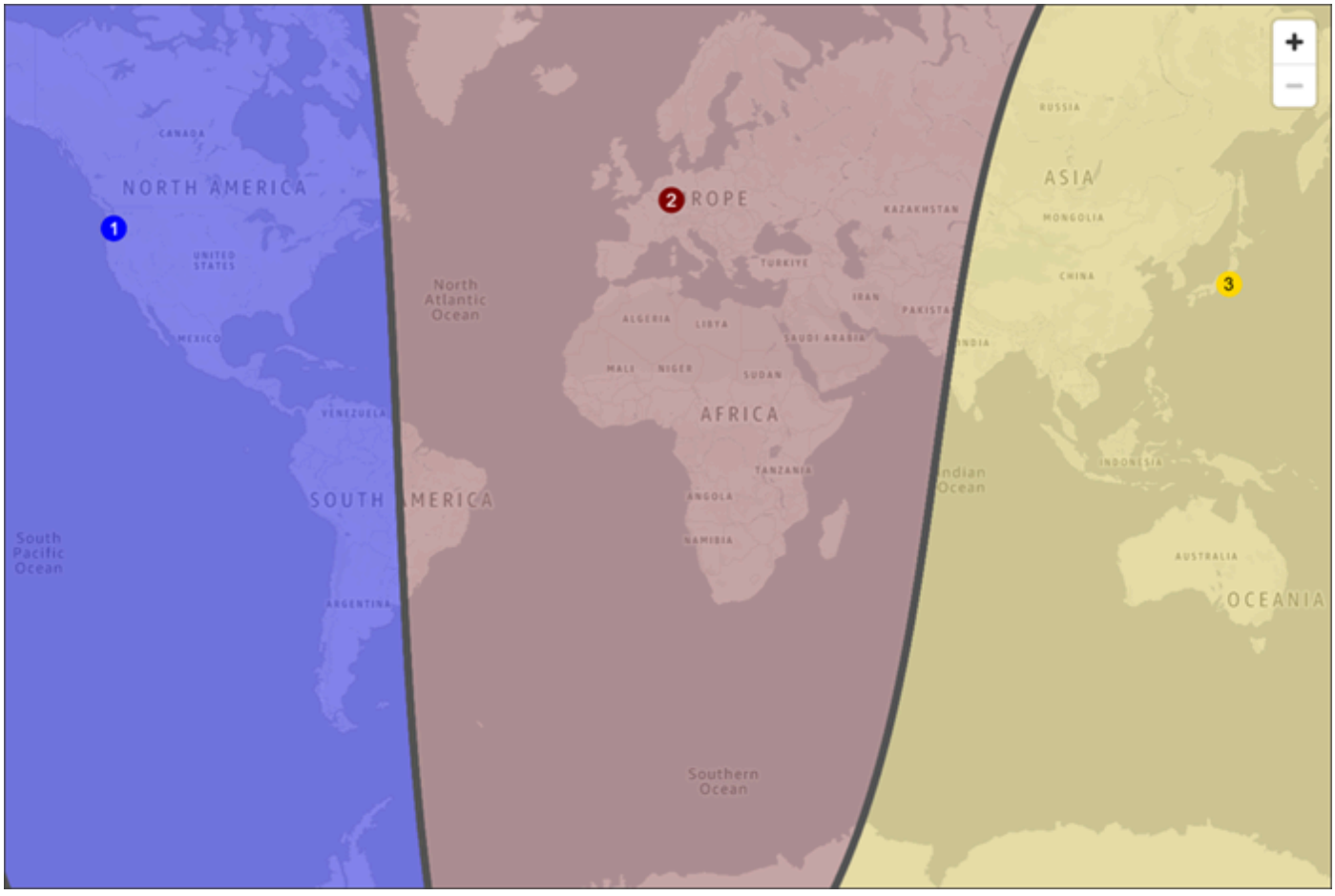
> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

您可以显示一个地图，其中展示您的地理位置临近度设置的效果。例如，如果您有资源位于美国西部（俄勒冈州）、欧洲地区（法兰克福）和亚太地区（东京）区域，并且您未指定偏差，则地图如下所示。



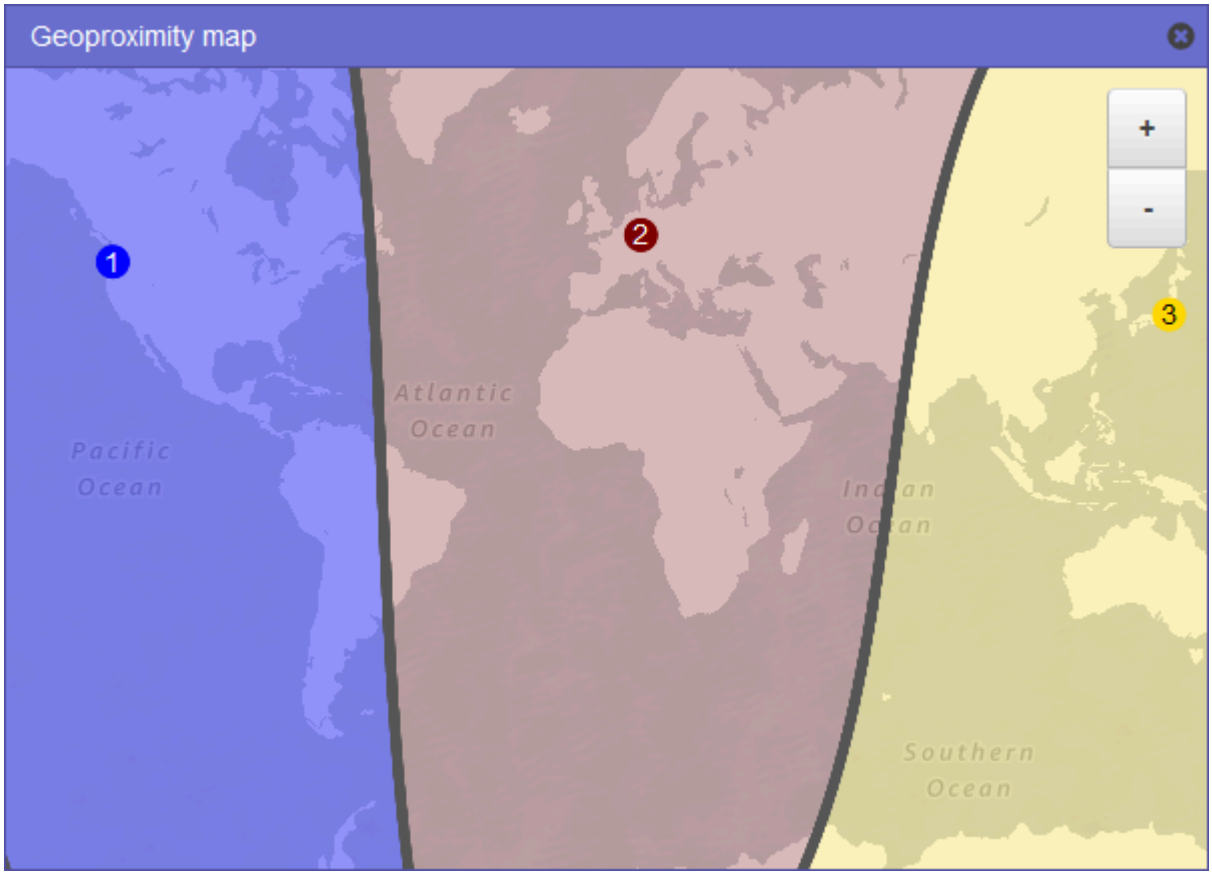
地理位置临近度规则地图会自动显示在属性中，并在您添加或删除区域时更新。

注意以下几点：

- 该地图精确到大约 10 英里（16 公里）范围内。
- 在您添加、编辑或删除区域时，或者在更改某个区域的偏差设置时，该地图会自动调整。
- 各个规则定义中的区域编号和颜色对应于地图上的编号和颜色。
- 您可以放大和缩小以查看更多或更少细节。使用地图上的 + 和 - 按钮、触摸板或者鼠标上的滚轮来更改缩放级别。如果您看不到区域或区域编号，则可以放大属性窗格，这些信息就会出现。
- 您可在地图窗口内部移动地图，以查看特定区域。使用触摸板，或者使用鼠标点击并拖动地图。您还可在浏览器窗口中移动地图窗口。
- 如果您在某个策略中有多个地理位置临近度规则，则在地图上一次只能查看一个规则。

Old console

您可以显示一个地图，其中展示您的地理位置临近度设置的效果。例如，如果您有资源位于美国西部（俄勒冈州）、欧洲地区（法兰克福）和亚太地区（东京）区域，并且您未指定偏差，则地图如下所示。



要显示地理位置临近度规则地图，请选择 Show geoproximity map (显示地理位置临近度地图) 旁边的图形图标。（此图标显示在规则的顶部。）要隐藏地图，请再次选择该图标，或者选择地图右上角的 x。

注意以下几点：

- 该地图精确到大约 10 英里（16 公里）范围内。
- 在您添加、编辑或删除区域时，或者在更改某个区域的偏差设置时，该地图会自动调整。
- 各个规则定义中的区域编号和颜色对应于地图上的编号和颜色。
- 您可以放大和缩小以查看更多或更少细节。使用地图上的 + 和 - 按钮、触摸板或者鼠标上的滚轮来更改缩放级别。
- 您可在地图窗口内部移动地图，以查看特定区域。使用触摸板，或者使用鼠标点击并拖动地图。您还可在浏览器窗口中移动地图窗口。
- 如果您在某个策略中有多个地理位置临近度规则，则在地图上一次只能查看一个规则。

创建流量策略的其他版本

当您编辑流量策略时，Amazon Route 53 会自动创建该流量策略的另一个版本，并保留以前的版本，除非您选择删除这些版本。新版本与您正在编辑的流量策略具有相同的名称；它与原始版本的区别在于 Route 53 自动递增的版本号。您可以在具有相同名称的流量策略的任何现有版本的基础上创建流量策略的新版本。

Route 53 不会重用给定流量策略的新版本的版本号。例如，如果您创建的三个版本 MyTrafficPolicy，删除最后两个版本，然后创建另一个版本，则新版本为版本 4。通过保留以前的版本，Route 53 可确保当新配置不按您希望的方式来路由流量时，您可以回滚到以前的配置。

要创建新的流量策略版本，请执行以下过程。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

创建流量策略的另一个版本

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择您要创建其新版本的流量策略的名称。
4. 在页面顶部的 Traffic policy versions 表中，选中您要用作新流量策略版本的基础的流量策略版本对应的复选框。
5. 选择 Edit policy as new version。
6. 在描述对话框中，输入新流量策略版本的描述。建议您指定可将该版本与相同流量策略的其他版本区分开来的描述。创建新的策略记录时，您指定的值将显示在此流量策略的可用版本列表中。
7. 选择下一步。
8. 更新配置 (如果适用)。有关更多信息，请参阅 创建流量策略时指定的值。

   您可以通过以下方式删除流量策略的规则、终端节点和分支：

   - 要删除规则或端点，请在编辑器中选择该规则或端点，然后在属性窗格中选择删除。

     > **Important**
     >
     > 如果您删除的规则具有子规则和终端节点，则 Route 53 也会删除所有子项。

   - 如果将两个规则连接到同一个子规则或端点，并且要删除其中一个连接，请选择要删除的连接，然后在属性窗格中选择删除。
9. 完成编辑后，请选择 Save as new version。
10. 可选：指定相应设置，以通过使用新的流量策略版本在一个托管区域中创建一个或多个策略记录。有关更多信息，请参阅 创建或更新策略记录时指定的值。您也可以稍后在同一托管区域或其他托管区域中创建策略记录。

    如果您不想立即创建策略记录，请选择取消，控制台将显示您使用当前 Amazon 账户创建的流量策略和策略记录的列表。
11. 如果您在之前的步骤中指定了策略记录的设置，请选择 Create policy record。

Old console

创建流量策略的另一个版本

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择您要创建其新版本的流量策略的名称。
4. 在页面顶部的 Traffic policy versions 表中，选中您要用作新流量策略版本的基础的流量策略版本对应的复选框。
5. 选择 Edit policy as new version。
6. 在更新描述页面上，输入新流量策略版本的描述。建议您指定可将该版本与相同流量策略的其他版本区分开来的描述。创建新的策略记录时，您指定的值将显示在此流量策略的可用版本列表中。
7. 选择下一步。
8. 更新配置 (如果适用)。有关更多信息，请参阅 创建流量策略时指定的值。

   您可以通过以下方式删除流量策略的规则、终端节点和分支：

   - 要删除规则或终端节点，请单击框右上角的 x。

     > **Important**
     >
     > 如果您删除的规则具有子规则和终端节点，则 Route 53 也会删除所有子项。

   - 如果将两个规则连接到同一个子规则或终端节点，并且要删除其中一个连接，请将光标停留在要删除的连接上，然后单击该连接对应的 x。
9. 完成编辑后，请选择 Save as new version。
10. 可选：指定相应设置，以通过使用新的流量策略版本在一个托管区域中创建一个或多个策略记录。有关更多信息，请参阅 创建或更新策略记录时指定的值。您也可以稍后在同一托管区域或其他托管区域中创建策略记录。

    如果您不想立即创建策略记录，请选择跳过此步骤，控制台将显示您使用当前 Amazon 账户创建的流量策略和策略记录的列表。
11. 如果您在之前的步骤中指定了策略记录的设置，请选择 Create policy record。

通过使用 JSON 文档来创建流量策略

您可以通过导入 JSON 格式的文档来创建新的流量策略或现有流量策略的新版本，该文档描述了要包含在流量策略中的所有终端节点和规则。有关 JSON 文档格式以及您可以复制和修改的几个示例的信息，请参阅 Amazon Route 53 API 参考中的流量策略文档格式。

要获取现有流量策略版本的 JSON 格式文档，最简单的方法是在 CLI Amazon 中使用该`get-traffic-policy`命令。有关更多信息，请参阅《Amazon CLI Command Reference》中的 get-traffic-policy。

`get-traffic-policy` 命令创建的 JSON 文件包含反斜杠 (\ ) 作为转义字符。在导入 JSON 文件之前，请将所有反斜杠替换为空字符。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

通过导入 JSON 文档来创建流量策略

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 要通过导入 JSON 文档来创建新的流量策略，请执行以下步骤：
   a. 在导航窗格中，选择 Traffic policies。
   b. 选择 Create traffic policy。
   c. 在 Name policy 页面上，指定适用的值。有关更多信息，请参阅 创建流量策略时指定的值。
   d. 跳至步骤 4。
3. 要通过导入 JSON 文档来创建现有流量策略的新版本，请执行以下步骤：

a. 在导航窗格中，选择 Traffic policies。
b. 选择您希望用作新版本的基础的流量策略的名称。
c. 在 Traffic policy versions 表中，选中您要作为创建新版本的基础的版本对应的复选框。
d. 选择 Edit policy as new version。
e. 在更新描述页面上，输入新版本的描述。
f. 跳至步骤 4。

4. 选择下一步。
5. 在编辑器页面上，选择编辑器右上角的 json 编辑器

   （  ）

   图标。
6. 输入新的流量策略，粘贴示例流量策略，或粘贴现有流量策略。

   有关策略示例，请参阅 Traffic Flow 策略 JSON 示例。
7. 选择更新。

Old console

通过导入 JSON 文档来创建流量策略

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 要通过导入 JSON 文档来创建新的流量策略，请执行以下步骤：

   a. 在导航窗格中，选择 Traffic policies。
   b. 选择 Create traffic policy。
   c. 在 Name policy 页面上，指定适用的值。有关更多信息，请参阅 创建流量策略时指定的值。
   d. 跳至步骤 4。
3. 要通过导入 JSON 文档来创建现有流量策略的新版本，请执行以下步骤：

   a. 在导航窗格中，选择 Traffic policies。
   b. 选择您希望用作新版本的基础的流量策略的名称。
   c. 在 Traffic policy versions 表中，选中您要作为创建新版本的基础的版本对应的复选框。

d. 选择 Edit policy as new version。

e. 在更新描述页面上，输入新版本的描述。

f. 跳至步骤 4。

4. 选择下一步。
5. 选择 Import traffic policy。
6. 输入新的流量策略，粘贴示例流量策略，或粘贴现有流量策略。

   有关策略示例，请参阅 Traffic Flow 策略 JSON 示例

7. 选择 Import traffic policy。

查看流量策略版本和关联的策略记录

您可以查看为流量策略创建的所有版本，以及通过使用该流量策略的每个版本创建的所有策略记录。

> **Note**
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

查看流量策略版本和关联的策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择流量策略的链接名称。
4. 顶部表列出了您创建的流量策略的所有版本。该表包含以下信息：

版本号

您所创建的流量策略的每个版本的号码。如果您选择相应的版本号，则控制台将显示该版本的配置。

策略记录数

通过使用此流量策略版本所创建的策略记录数。

DNS 类型

创建流量策略版本时指定的 DNS 类型。

版本说明

创建流量策略版本时指定的描述。

5. 底部表列出了通过使用顶部表中的流量策略版本所创建的所有策略记录。该表包含以下信息：

DNS 名称

您已将流量策略与之关联的 DNS 名称。

Status

可能的值包括：

已申请

Route 53 已完成策略记录和相应记录的创建或更新。

Creating

Route 53 正在创建新策略记录的记录。

Updating

您已更新策略记录，并且 Route 53 正在创建一组新的记录，以替代指定 DNS 名称的一组现有记录。

Deleting

Route 53 正在删除策略记录和关联的记录。

失败

Route 53 无法创建或更新策略记录和关联的记录。

DNS 类型

Route 53 为此策略记录创建的所有记录的 DNS 类型。当您编辑策略记录时，必须指定具有与要编辑的策略记录的 DNS 类型相同的 DNS 类型的流量策略版本。

版本

指示用于创建策略记录的流量策略的版本。

TTL (以秒为单位)

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即两天），则您为 Route 53 服务支付的费用较少，因为递归解析程序不经常向 Route 53 发送请求。但是，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序会在更长时间内使用其缓存中的值，而不是要求 Route 53 提供最新信息。

Old console

查看流量策略版本和关联的策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择流量策略的名称。
4. 顶部表列出了您创建的流量策略的所有版本。该表包含以下信息：

   版本号

   您所创建的流量策略的每个版本的号码。如果您选择相应的版本号，则控制台将显示该版本的配置。

   策略记录数

   通过使用此流量策略版本所创建的策略记录数。

   DNS 类型

   创建流量策略版本时指定的 DNS 类型。

   版本说明

   创建流量策略版本时指定的描述。

5. 底部表列出了通过使用顶部表中的流量策略版本所创建的所有策略记录。该表包含以下信息：

策略记录 DNS 名称

您已将流量策略与之关联的 DNS 名称。

Status

可能的值包括：

已申请

Route 53 已完成策略记录和相应记录的创建或更新。

Creating

Route 53 正在创建新策略记录的记录。

Updating

您已更新策略记录，并且 Route 53 正在创建一组新的记录，以替代指定 DNS 名称的一组现有记录。

Deleting

Route 53 正在删除策略记录和关联的记录。

失败

Route 53 无法创建或更新策略记录和关联的记录。

已使用版本

指示用于创建策略记录的流量策略的版本。

DNS 类型

Route 53 为此策略记录创建的所有记录的 DNS 类型。当您编辑策略记录时，必须指定具有与要编辑的策略记录的 DNS 类型相同的 DNS 类型的流量策略版本。

TTL (以秒为单位)

您希望 DNS 递归解析器缓存有关此记录的信息的时间长度 (以秒为单位)。如果您指定较长的值（例如，172800 秒，即两天），则您为 Route 53 服务支付的费用较少，因为递归解析程序不经常向 Route 53 发送请求。但是，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序会在更长时间内使用其缓存中的值，而不是要求 Route 53 提供最新信息。

删除流量策略版本和流量策略

要删除流量策略，您必须删除为该流量策略创建的所有版本 (包括原始版本)。此外，要删除流量策略版本，您必须删除通过使用该流量策略版本创建的所有策略记录。

> **Important**
>
> 如果您删除 Amazon Route 53 用于响应 DNS 查询的策略记录，则 Route 53 将停止响应相应 DNS 名称的查询。例如，如果 Route 53 使用 www.example.com 的策略记录来响应 www.example.com 的 DNS 查询，并且您删除该策略记录，则您的用户将无法通过使用域名 www.example.com 来访问您的网站或 Web 应用程序。

要删除流量策略版本以及 (可选) 流量策略，请执行以下过程：

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

删除流量策略版本和流量策略

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择要针对其删除流量策略版本且 (可选) 要完全删除的流量策略的链接名称。
4. 如果要在顶部表中删除的流量策略版本显示在策略记录表的版本列中，请选中底部表中相应策略记录的复选框。

   例如，如果要删除流量策略的版本 3，但是通过使用版本 3 创建了底部表中的策略记录之一，请选中该策略记录的复选框。

5. 选择删除策略记录，然后在删除策略记录对话框中，选择确认。
6. 刷新页面，直到您删除的策略记录不再出现在表中。
7. 在顶部表中，选中要删除的流量策略版本的复选框。
8. 选择删除。
9. 如果删除了之前步骤中的所有流量策略版本，并且还要删除流量策略，请刷新页面显示，直到该表为空。
10. 在导航窗格中，选择 Traffic policies。
11. 在流量策略列表中，选中要删除的流量策略的复选框。
12. 选择 Delete traffic policy。

Old console

删除流量策略版本和流量策略

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Traffic policies。
3. 选择要针对其删除流量策略版本且 (可选) 要完全删除的流量策略的名称。
4. 如果要在顶部表中删除的流量策略版本显示在底部表的 Version used 列中，请选中底部表中相应策略记录的复选框。

   例如，如果要删除流量策略的版本 3，但是通过使用版本 3 创建了底部表中的策略记录之一，请选中该策略记录的复选框。
5. 选择 Delete policy records。
6. 选择底部表的刷新按钮来刷新显示，直到删除的策略记录不再出现在表中。
7. 在顶部表中，选中要删除的流量策略版本的复选框。
8. 选择 Delete version。
9. 如果删除了之前步骤中的所有流量策略版本，并且还要删除流量策略，请选择顶部表的刷新按钮来刷新显示，直到该表为空。
10. 在导航窗格中，选择 Traffic policies。
11. 在流量策略列表中，选中要删除的流量策略的复选框。
12. 选择 Delete traffic policy。

创建和管理策略记录

要将 Internet 流量路由到您在创建流量策略时指定的资源，您可以创建一个或多个策略记录。每个策略记录标识您希望在其中创建策略记录的托管区，以及要路由流量的域名或子域名。例如，如果您希望为 www.example.com 路由流量，则为 example.com 托管区域指定托管区域 ID，为 Policy record DNS name (策略记录 DNS 名称) 指定 www.example.com。

如果您想要为多个域名或子域名使用相同的流量策略来路由流量，有两个选项可供使用：

- 您可以为每个域名或子域名创建一个策略记录。
- 您可以创建一个策略记录，然后创建引用该策略记录的 CNAME（即别名记录）。

例如，如果您想要为 example.com、example.net 和 example.org 使用相同的流量策略，则可以执行以下任一操作：

- 为每个这些域名创建一个策略记录。
- 为其中一个域名创建一个策略记录，然后在托管区域中为另外两个域名创建 CNAME 记录。在两个 CNAME 记录中，您指定为其创建策略记录的记录名称。

如果您想要为某个域及其子域使用相同的流量策略，例如 example.com 和 www.example.com，则为一个名称创建策略记录，然后为其余名称创建别名记录。例如，您可以为 example.com 创建一条策略记录，然后为 www.example.com 记录创建将 example.com 作为别名目标的别名记录。

> **Note**
>
> 您创建的每个策略记录，每月都会产生费用。如果您希望为多个域名或子域名使用同一个流量策略，可以使用 CNAME（即别名记录）来减少费用：
>
> - 如果您创建一个策略记录以及引用该策略记录的一个或多个 CNAME 记录，您只需为该策略记录以及 CNAME 记录的 DNS 查询支付费用。
> - 如果您在相同托管区域中创建一个策略记录以及引用该策略记录的一个或多个别名记录，您只需为该策略记录以及别名记录的 DNS 查询支付费用。

主题

- 更新策略记录
- 删除策略记录

创建策略记录

要创建策略记录，请执行以下过程。

> **Important**
>
> 对于您创建的每个策略记录，每月都会产生费用。如果您稍后删除策略记录，则费用会按比例收取。有关更多信息，请参阅 Amazon Route 53 定价页面的“Traffic Flow”部分。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

创建策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在 Policy records 页面上，选择 Create policy records。
4. 在 Create policy records 页面上，指定适用的值。有关更多信息，请参阅 创建或更新策略记录时指定的值。
5. 要向同一个托管区添加其他记录，请选择添加策略记录。
6. 选择 Create policy records。

   创建的策略记录的状态可能需要几分钟才会显示为已应用。

7. 如果要在其他托管区域中创建策略记录，请重复步骤 3 到 5。

> **Note**
>
> 如果策略记录状态为失败，请选择状态旁边的信息按钮以获取有关失败的更多信息。如果您需要更多帮助并想联系 Amazon 支持人员，请参阅如何获得技术支持 Amazon？

Old console

创建策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在 Policy records 页面上，选择 Create policy records。
4. 在 Create policy records 页面上，指定适用的值。有关更多信息，请参阅 创建或更新策略记录时指定的值。
5. 选择 Create policy records。

   创建的策略记录的状态可能需要几分钟才会显示为已应用。
6. 如果要在其他托管区域中创建策略记录，请重复步骤 3 到 5。

> **Note**
>
> 如果策略记录状态为失败，请选择状态旁边的信息按钮以获取有关失败的更多信息。如果您需要更多帮助并想联系 Amazon 支持人员，请参阅如何获得技术支持 Amazon？

创建或更新策略记录时指定的值

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。除非另有说明，否则以下列表适用于两种控制台。

当您创建或更新策略记录时，可指定以下值

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

流量策略

选择要将其配置用于此策略记录的流量策略。

版本

选择要将其配置用于此策略记录的流量策略的版本。

如果要更新现有的策略记录，则必须选择 DNS 类型与策略记录的当前 DNS 类型相匹配的版本。例如，如果策略记录的 DNS 类型为 A，则必须选择 DNS 类型为 A 的版本。

托管区域

选择相应的托管区域，您要在该托管区域中使用指定的流量策略和版本创建策略记录。创建策略记录后，将无法再更改 Hosted zone 的值。

DNS 名称（新控制台）、策略记录 DNS 名称（旧控制台）

当您创建策略记录时，请使用指定流量策略和版本中的配置输入您希望 Route 53 响应 DNS 查询的域名或子域名。

要在指定的托管区中为多个域名或子域名使用相同的配置，请选择添加策略记录（新控制台）或添加另一个策略记录（旧控制台），并输入适用的域名或子域名和 TTL。

创建策略记录后，将无法再更改 Policy record DNS name 的值。

TTL (以秒为单位)

输入您希望 DNS 递归解析器缓存有关此记录的信息的时间长度（以秒为单位）。如果您指定较长的值（例如，172800 秒，即两天），则您为 Route 53 服务支付的费用较少，因为递归解析程序不经常向 Route 53 发送请求。但是，对记录所做的更改（例如，新的 IP 地址）需要更长时间才能生效，因为递归解析程序会在更长时间内使用其缓存中的值，而不是要求 Route 53 提供最新信息。

更新策略记录

要更新策略记录中的设置，请执行以下过程。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

更新策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在策略记录页面上，选中要更新的策略记录的复选框，然后选择编辑。
4. 在编辑策略记录页面上，指定适用的值。有关更多信息，请参阅 创建或更新策略记录时指定的值。
5. 选择编辑策略记录。

   创建的策略记录的状态可能需要几分钟才会显示为已应用。
6. 要更新其他策略记录，请重复步骤 3 到 5。

> **Note**
>
> 如果策略记录状态为失败，请选择状态旁边的信息按钮以获取有关失败的更多信息。如果您需要更多帮助并想联系 Amazon 支持人员，请参阅如何获得技术支持 Amazon？

Old console

更新策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在 Policy records 页面上，选中要更新的策略记录的复选框，然后选择 Edit policy record。
4. 在编辑策略记录页面上，指定适用的值。有关更多信息，请参阅 创建或更新策略记录时指定的值。
5. 选择编辑策略记录。

   创建的策略记录的状态可能需要几分钟才会显示为已应用。
6. 要更新其他策略记录，请重复步骤 3 到 5。

> **Note**
>
> 如果策略记录状态为失败，请选择状态旁边的信息按钮以获取有关失败的更多信息。如果您需要更多帮助并想联系 Amazon 支持人员，请参阅如何获得技术支持 Amazon？

删除策略记录

要删除策略记录，请执行以下过程。

> **Important**
>
> 如果您删除 Amazon Route 53 用于响应 DNS 查询的策略记录，则 Route 53 将停止响应相应 DNS 名称的查询。例如，如果 Route 53 使用 www.example.com 的策略记录来响应 www.example.com 的 DNS 查询，并且您删除该策略记录，则您的用户将无法通过使用域名 www.example.com 来访问您的网站或 Web 应用程序。

> **Note**
>
> 我们正在更新 Route 53 的 Traffic Flow 控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

删除策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在策略记录页面上，选中要删除的策略记录的复选框，然后选择删除。
4. 在删除策略记录对话框中，选择确认。

   等待几分钟并刷新页面，确保策略记录从列表中消失。

Old console

删除策略记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择策略记录。
3. 在 Policy records 页面上，选中要删除的策略记录的复选框，然后选择 Delete policy record。

   等待几分钟并刷新页面，确保策略记录从列表中消失。

什么是 Route 53 VPC 解析器？

Route 53 VPC 解析器以递归方式响应来自公共记录 Amazon 资源、亚马逊 VPC 特定的 DNS 名称和 Amazon Route 53 私有托管区域的 DNS 查询，默认情况下全部可用。 VPCs

> **Note**
>
> Route 53 VPC 解析器以前被称为 Route 53 Resolver，但在引入 Route 53 全球解析器时被重命名。

亚马逊 VPC 通过 VPC+2 IP 地址连接到 VPC 解析器。此 VPC+2 地址连接到可用区内的 VPC 解析器。

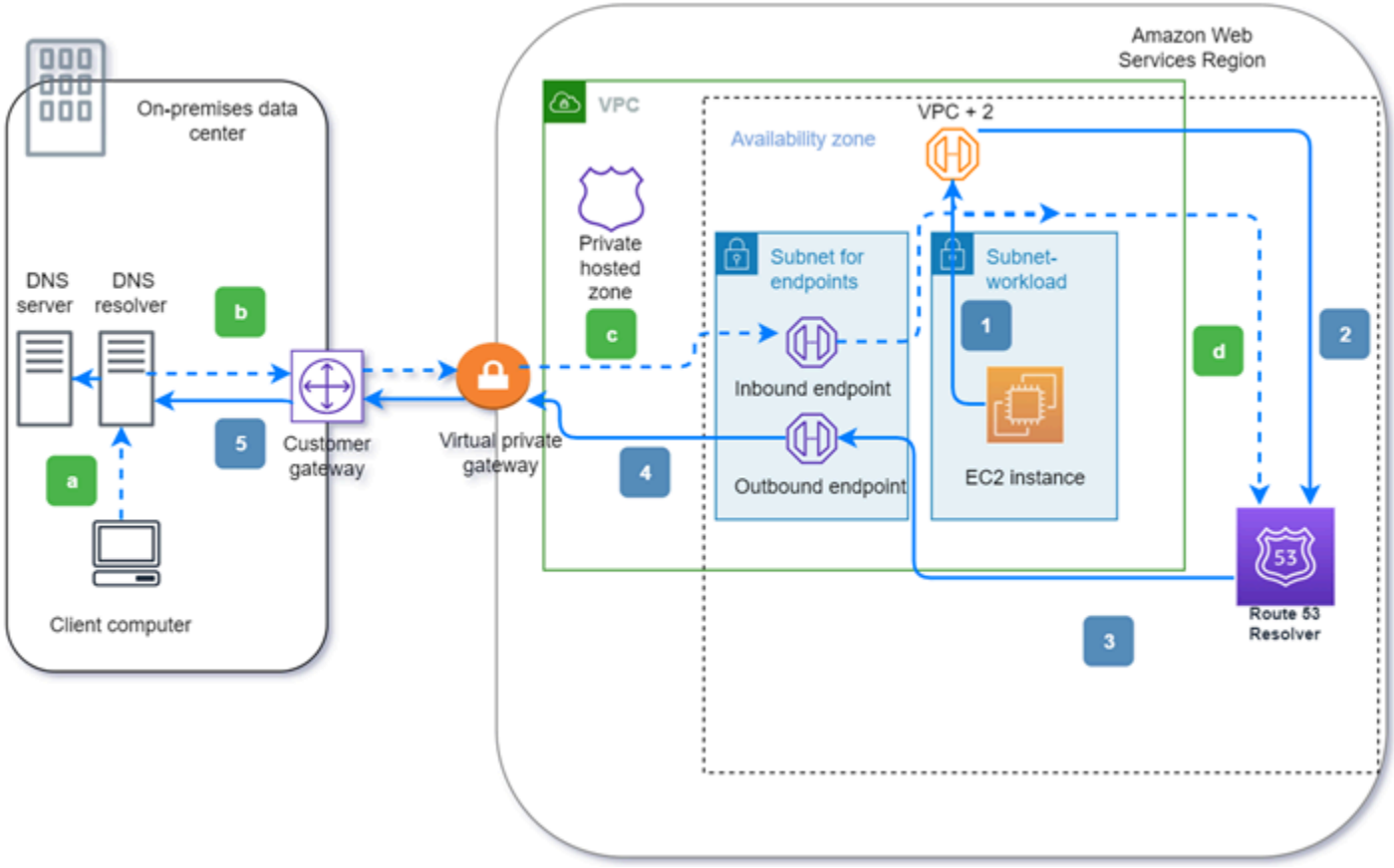
VPC 解析器会自动回答以下问题的 DNS 查询：

- EC2 实例的本地 VPC 域名（例如 ec2-192-0-2-44.compute-1.amazonaws.com）。
- 私有托管区（例如 acme.example.com）中的记录。
- 对于公共域名，VPC Resolver 会对互联网上的公共域名服务器执行递归查找。

如果您的工作负载同时利用本地资源 VPCs 和本地资源，则还需要解析本地托管的 DNS 记录。同样，这些本地资源可能需要解析托管在上的名称 Amazon。通过解析器端点和条件转发规则，您可以解析本地资源之间的 DNS 查询，并 VPCs 通过 VPN 或 Direct Connect (DX) 创建混合云设置。具体来说：

- 入站解析程序端点允许从您的本地网络或其他 VPC 对您的 VPC 进行 DNS 查询。
- 出站解析程序端点允许从您的 VPC 对您的本地网络或另一个 VPC 执行 DNS 查询。
- 解析程序规则允许您为每个域名创建一条转发规则，并指定要将 DNS 查询从 VPC 转发到本地 DNS 解析程序和从本地转发到 VPC 的域名。规则将直接应用于您的 VPC，可以在多个账户之间共享。

下图显示了使用解析程序端点的混合 DNS 解析原理。请注意，该图已简化为仅显示一个可用区。



下图说明了以下步骤：

出站（实心箭头 1–5）：

1. 亚马逊 EC2 实例需要将域名的 DNS 查询解析为域名 internal.example.com。权威 DNS 服务器位于本地数据中心。此 DNS 查询将发送到连接到 VPC 解析器的 VPC 中的 VPC+2。
2. VPC 解析器转发规则配置为将查询转发到本地数据中心的 internal.example.com。
3. 查询将被转发到出站端点。
4. 出站终端节点通过与数据中心之间的 Amazon 私有连接将查询转发给本地 DNS 解析器。连接可以是 Amazon Direct Connect 或 Amazon Site-to-Site VPN，描述为虚拟专用网关。
5. 本地 DNS 解析器解析 internal.example.com 的 DNS 查询，并通过相同的路径反向将答案返回给亚马逊 EC2 实例。

入站（虚线箭头 a–d）：

a. 本地数据中心的客户端需要将 DNS 查询解析为域 dev.example.com 的 Amazon 资源。它会将查询发送到本地 DNS 解析程序。

b. 本地 DNS 解析程序有一条转发规则，可将对 dev.example.com 的查询指向入站端点。

c. 查询通过私有连接（例如 Amazon Direct Connect 或）到达入站终端节点 Amazon Site-to-Site VPN，该连接被描述为虚拟网关。

d. 入站终端节点将查询发送到 VPC 解析器，VPC 解析器解析 dev.example.com 的 DNS 查询，并通过相同的路径反向将答案返回给客户端。

主题

解决与您的网络VPCs 之间的 DNS 查询

VPC 解析器包含您配置的终端节点，用于回复本地环境的 DNS 查询。

> **Note**
>
> 不支持将私有 DNS 查询从本地或其他 VPC DNS 服务器转发到任何 VPC CIDR + 2 地址，这可能会导致结果不稳定。我们建议您改用 Resolver 入站端点。

您还可以通过配置转发规则，在网络上的 VPC 解析器和 DNS 解析器之间集成 DNS 解析器。您的网络可以包含可从 VPC 访问的任何网络，如下所示：

- VPC 本身
- 另一个对等 VPC
- 与 VPN 或网络地址转 Amazon 换 (NAT) 网关连接的本地网络 Amazon Direct Connect

在开始转发查询之前，您需要在连接的 VPC 中创建 Resolver 入 and/or 站出站终端节点。这些端点为入站或出站查询提供路径：

入站终端节点：您网络上的 DNS 解析器可以通过此终端节点将 DNS 查询转发给 Route 53 VPC 解析器

有两种类型的入站终端节点，一种是转发到 IP 地址的默认入站终端节点，另一种是委托入站终端节点，它将托管在 Route 53 私有托管区域中的子域的权限委托给 Route 53 VPC 解析器。入站终端节点允许您的 DNS 解析器轻松解析 Amazon 资源（例如 Route 53 私有托管区域中的 EC2 实例或记录）的域名。有关更多信息，请参阅 [您网络上的 DNS 解析器如何将 DNS 查询转发到解析器端点]。

出站终端节点：VPC 解析器有条件地通过此终端节点将查询转发给您网络上的解析器

要转发选定的查询，您可以创建 Resolver 规则，指定要转发的 DNS 查询的域名（例如 example.com），以及希望将查询转发到您网络上的 DNS 解析程序的 IP 地址。如果查询与多个规则匹配（example.com、acme.example.com），VPC 解析程序会选择匹配最具体的规则（acme.example.com）并将查询转发到该规则中指定的 IP 地址。有三种类型的规则：转发、系统和委托。有关更多信息，请参阅 [解析器端点如何将您的 DNS 查询转发 VPCs 到您的网络]。

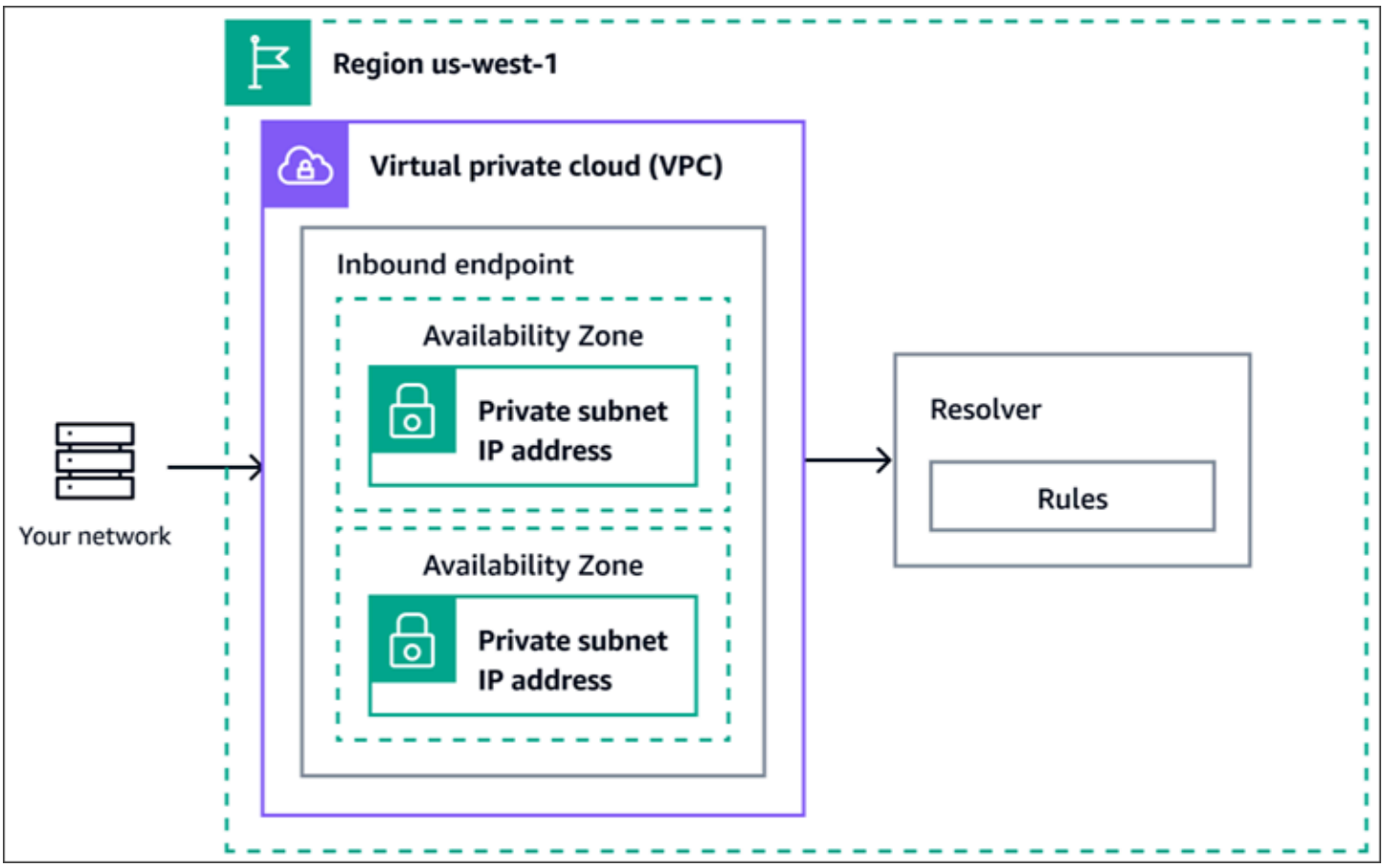
与 Amazon VPC 一样，VPC 解析器也是区域性的。在您所在的每个区域中 VPCs，您可以选择是将查询从您的网络转发 VPCs到您的网络（出站查询），还是将查询从您的网络转发到您的网络 VPCs（入站查询），或者两者兼而有之。

不能在不属于自己的 VPC 中创建解析程序端点。只有 VPC 拥有者才能创建诸如入站终端节点等 VPC 级资源。

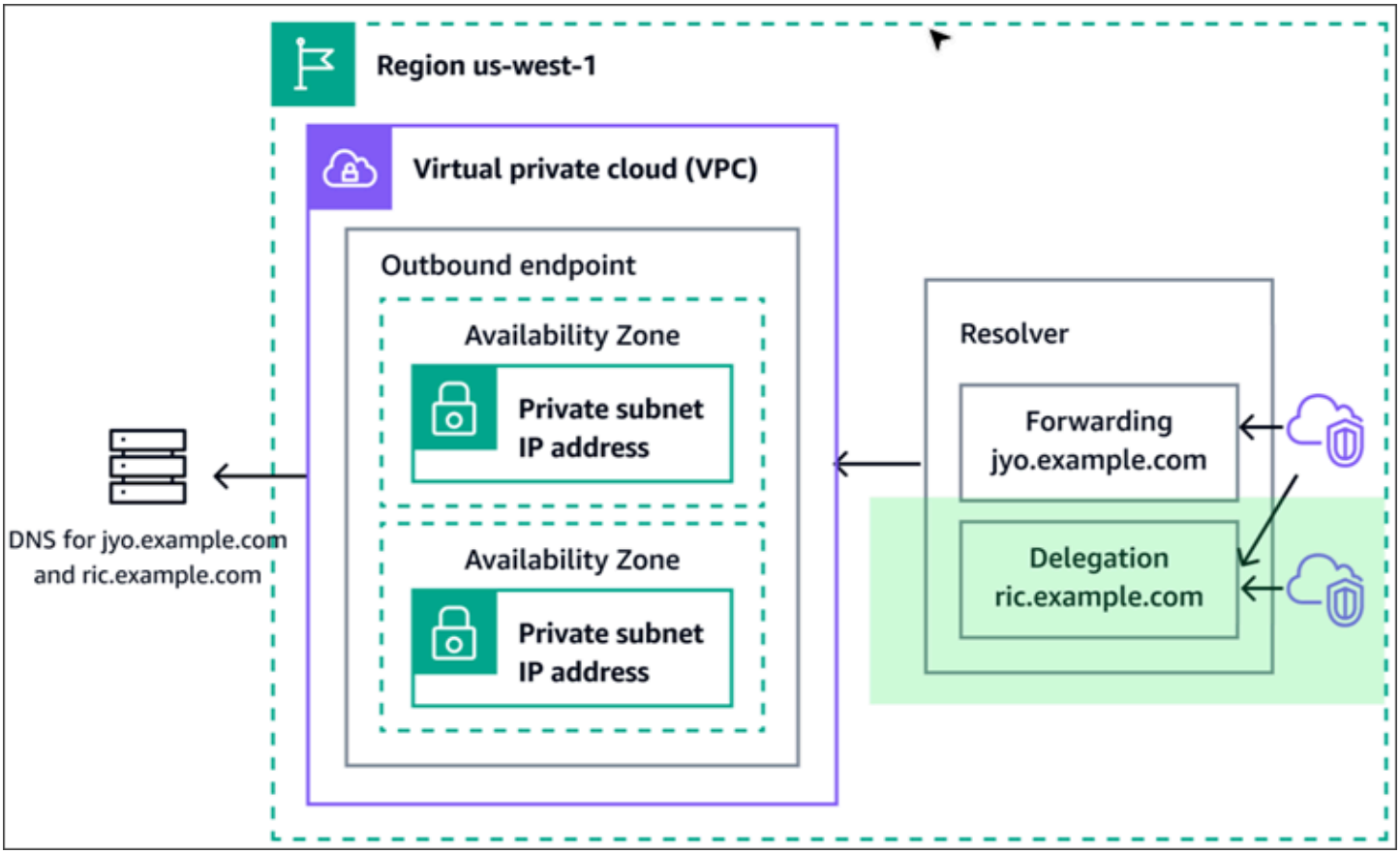
> **Note**
>
> 当您创建 Resolver 端点时，无法指定将实例租赁属性设置为 `dedicated` 的 VPC。有关更多信息，请参阅 。

要使用入站或出站转发，您在 VPC 中创建一个 Resolver 端点。作为端点的定义的一部分，您指定希望将入站 DNS 查询转发到的 IP 地址或 DNS 委托，或者您希望出站查询源自的 IP 地址。对于您指定的每个 IP 地址和委托，VPC 解析器都会自动创建一个 VPC 弹性网络接口。

下图显示了从网络上的 DNS 解析程序到 Route 53 Resolver 端点的 DNS 查询的路径。



下图显示了从您的一个 EC2 实例 VPCs到网络上的 DNS 解析器的 DNS 查询路径。jyo.example.com 域使用转发规则，而 ric.example.com 子域已将转发权限委托给 VPC 解析器。



有关 VPC 网络接口的概览，请参阅 Amazon VPC 用户指南中的弹性网络接口。

主题

- 您网络上的 DNS 解析器如何将 DNS 查询转发到解析器端点
- 解析器端点如何将您的 DNS 查询转发 VPCs 到您的网络
- 创建入站和出站端点的注意事项

您网络上的 DNS 解析器如何将 DNS 查询转发到解析器端点

要将 DNS 查询从您的网络转发到 Route 53 VPC 解析器，您需要在 Amazon 区域中创建入站终端节点。入站端点分为两类：默认和委托。

创建默认入站端点的步骤

1. 您可以在 VPC 中创建默认的 Resolver 入站终端节点，并指定网络上的解析器将 DNS 查询转发到的 IP 地址，以及包含允许通过端口 53 访问 TCP 和 UDP 的入站规则的 VPC 安全组。有关说明，请参阅 配置入站转发。

对于您为入站终端节点指定的每个 IP 地址，VPC Resolver 会在您创建入站终端节点的 VPC 中创建一个 VPC 弹性网络接口。

2. 您可配置网络上的解析程序，将针对相应域名的 DNS 查询转发到您在入站端点中指定的 IP 地址。有关更多信息，请参阅 创建入站和出站端点的注意事项。

以下是 VPC 解析器如何通过默认入站终端节点解析来自您的网络的 DNS 查询：

1. 网络上的网络浏览器或其他应用程序会针对您转发到 VPC 解析器的域名提交 DNS 查询。
2. 您网络上的解析程序将查询转发到入站端点内的 IP 地址。
3. 入站终端节点将查询转发给 VPC 解析器。
4. VPC Resolver 在 DNS 查询中获取域名的适用值，可以在内部获取，也可以通过对公共域名服务器执行递归查找。
5. VPC 解析器将值返回到入站终端节点。
6. 入站端点将值返回到您网络上的解析程序。
7. 您网络上的解析程序将值返回到应用程序。
8. 应用程序使用 VPC Resolver 返回的值提交请求，例如对 Amazon S3 存储桶中的对象的请求。

创建委托入站端点的步骤

1. 您可以在 VPC 中创建委托解析器入站终端节点。有关说明，请参阅 配置入站转发。

   对于您为入站终端节点指定的每个 IP 地址，VPC Resolver 会在您创建入站终端节点的 VPC 中创建一个 VPC 弹性网络接口。

2. 您可以在网络上配置解析器，将适用域名的 DNS 查询委托给 VPC 解析器。对于粘附记录，您必须输入入站端点的 IP 地址。有关更多信息，请参阅 创建入站和出站端点的注意事项。

以下是 VPC 解析器如何通过委托入站终端节点解析来自您的网络的 DNS 查询：

1. 作为先决条件，您必须从本地委托在私有托管区中托管的子域。由于您是通过入站委托端点委托子域，因此使用入站端点 IP 地址作为正在委托的子域的粘附记录。

> **Note**
>
> 您可能还需要包含粘附记录以确保 DNS 查询可解析。如果您将子域委托给与父域位于同一区域的名称服务器，则需要使用粘附记录。

2. 网络上的 Web 浏览器或其他应用程序针对您委托给 VPC 解析器的域名提交 DNS 查询。
3. 您网络上的解析程序将查询转发到入站端点内的 IP 地址。
4. 入站终端节点将查询委托给 VPC 解析器。
5. VPC Resolver 将 Amazon 资源地址从私有托管区域返回到入站终端节点。
6. 入站端点将值返回到您网络上的解析程序。
7. 您网络上的解析程序将值返回到应用程序。
8. 应用程序使用 VPC Resolver 返回的值提交请求，例如对 Amazon S3 存储桶中的对象的请求。

创建入站终端节点不会改变 VPC 解析器的行为，它只是提供从 Amazon 网络外部位置到 VPC 解析器的路径。

解析器端点如何将您的 DNS 查询转发 VPCs 到您的网络

当您要将 DNS 查询从一个 Amazon 区域中一个或多个 EC2 VPCs 实例转发到您的网络时，请执行以下步骤。

1. 您在 VPC 中创建一个 Resolver 出站终端节点，并指定几个值：
   - 希望 DNS 查询在到达您网络上解析程序之前经过的 VPC。
   - 一个 VPC 安全组，其中包含允许通过端口 53（或您在网络上进行 DNS 查询所使用的端口）上进行 TCP 和 UDP 访问的出站规则

   对于您为出站终端节点指定的每个 IP 地址，VPC 解析器都会在您指定的 VPC 中创建一个 Amazon VPC 弹性网络接口。有关更多信息，请参阅 创建入站和出站端点的注意事项。
2. 您可以创建一个或多个规则，这些规则指定您要委托给 VPC 解析器进行转发的 DNS 查询的域名，或者希望 VPC 解析器转发给您网络上的解析器。对于转发规则，您还要指定解析程序的 IP 地址。有关更多信息，请参阅 使用规则控制将哪些查询转发到您的网络。
3. 您可以将每条规则与要将 VPCs DNS 查询转发到您的网络的规则相关联。

使用规则控制将哪些查询转发到您的网络

规则控制哪些 DNS 查询解析器终端节点转发给您网络上的 DNS 解析器，以及哪些查询 VPC 解析器自己应答。

您可以通过多种方法分类规则。一种方法是按照规则的创建者分类：

- 自动定义规则 — VPC Resolver 会自动创建自动定义的规则，并将这些规则与您的规则相关联。VPCs这些规则大多适用于 VPC Amazon Resolver 回答查询的特定域名。有关更多信息，请参阅 VPC 解析器为其创建自动定义的系统规则的域名。
- 自定义规则-您可以创建自定义规则并将这些规则与关联 VPCs。目前，您可以创建两种类型的自定义规则，即条件转发规则（也称为转发规则）和委托规则。转发规则会让 VPC 解析器将您的 DNS 查询转发 VPCs 到您网络上的 DNS 解析器的 IP 地址。

  如果您为与自动定义规则相同的域创建转发规则，VPC Resolver 会根据转发规则中的设置将对该域名的查询转发给您网络上的 DNS 解析器。

  委托规则将 DNS 查询连同委托规则中与 NS 记录匹配的委托记录一起转发到网络上的解析程序。

另一种方法是按照规则执行的操作来分类：

- 条件转发规则 — 希望将对指定域名的 DNS 查询转发到您网络上的 DNS 解析程序时，可创建条件转发规则（也称为转发规则）。
- 系统规则 — 系统规则会让 VPC Resolver 有选择地覆盖转发规则中定义的行为。创建系统规则时，VPC 解析器会解析指定子域名的 DNS 查询，否则这些查询将由您网络上的 DNS 解析器解析。

  默认情况下，转发规则会应用到一个域名及其所有子域。如果您希望将对某个域的查询转发到您网络上的解析程序，但不想为某些子域转发查询，则为这些子域创建系统规则。例如，如果您为 example.com 创建一个转发规则，但不希望转发针对 acme.example.com 的查询，则可以创建系统规则，为域名指定 acme.example.com。
- 递归规则 — VPC 解析器会自动创建名为 Internet Resolver 的递归规则。此规则会让 Route 53 VPC Resolver 充当您未为其创建自定义规则以及 VPC 解析器未为其创建自动定义规则的任何域名的递归解析器。有关如何覆盖此行为的更多信息，请参阅本主题下文中的“将所有查询转发到您的网络”。

您可以创建适用于特定域名（您的或大多数 Amazon 域名）、公共 Amazon 域名或所有域名的自定义规则。

将对特定域名的查询转发到您的网络

要将对特定域名（例如 example.com）的查询转发到您的网络，您可以创建规则并指定该域名。对于转发规则，您还必须指定网络上要将查询转发到其中的 DNS 解析程序的 IP 地址；或者，对于委托规则，创建要将授权委托给本地解析程序的委托记录。然后，将每条规则与您要将 VPCs DNS 查询转发到您的网络的规则相关联。例如，您可以为 example.com、example.org 和 example.net 创建单独的规则。然后，您可以将规则与 Amazon 区域 VPCs 中的任意组合相关联。

将对 amazonaws.com 的查询转发到您的网络

域名 amazonaws.com 是 EC2实例和 S3 存储桶等 Amazon 资源的公共域名。如果要将对 amazonaws.com 的查询转发到您的网络，请创建规则，为域名指定 amazonaws.com，然后根据要使用的方法为规则类型指定转发或委托。

> **Note**
>
> 即使您为 amazonaws.com 创建了转发规则，VPC 解析器也不会自动转发某些 amazonaws.com 子域的 DNS 查询。有关更多信息，请参阅 VPC 解析器为其创建自动定义的系统规则的域名。有关如何覆盖此行为的更多信息，请参阅下文中的“将所有查询转发到您的网络”。

将所有查询转发到您的网络

如果要将所有查询转发到您的网络，请创建一个规则，指定“。”（dot）表示域名，并将该规则与您要将所有 DNS 查询转发到您的网络的规则相关联。 VPCs VPC 解析器仍无法将所有 DNS 查询转发到您的网络，因为在网络之外使用 DNS 解析器 Amazon 会破坏某些功能。例如，某些内部 Amazon 域名的内部 IP 地址范围无法从外部访问 Amazon。有关当您创建“.”规则时对其查询不会转发到您网络的域名列表，请参阅VPC 解析器为其创建自动定义的系统规则的域名。

但是，可以禁用反向 DNS 的自动定义系统规则，从而允许“.”规则将所有反向 DNS 查询转发到您的网络。有关如何关闭自动定义规则的更多信息，请参阅 VPC 解析器中反向 DNS 查询的转发规则。

如果您要尝试将对所有域名的 DNS 查询转发到网络，包括默认情况下会从转发中排除的域名，您可以创建“.”规则并执行以下操作之一：

- 将 VPC 的 `enableDnsHostnames` 标记设置为 `false`
- 为VPC 解析器为其创建自动定义的系统规则的域名中列出的域名创建规则

> **Important**
>
> 如果您将所有域名转发到您的网络，包括 VPC Resolver 在创建 “.” 规则时排除的域名，则某些功能可能会停止运行。

VPC 解析器如何确定查询中的域名是否与任何规则匹配

Route 53 VPC Resolver 将 DNS 查询中的域名与查询来源的 VPC 关联的规则中的域名进行比较。在以下情况下，VPC 解析器会认为域名匹配：

- 域名完全匹配
- 查询中的域名是规则中域名的子域

例如，如果规则中的域名是 acme.example.com，则 VPC 解析器会认为 DNS 查询中的以下域名是匹配的：

- acme.example.com
- zenith.acme.example.com

以下域名不匹配：

- example.com
- nadir.example.com

如果查询中的域名与多个规则（例如 example.com 和 www.example.com）中的域名匹配，则 VPC 解析器使用包含最具体域名的规则 (www.example.com) 路由出站 DNS 查询。

VPC 解析器如何确定将 DNS 查询转发到何处

在 VPC 中的 EC2 实例上运行的应用程序提交 DNS 查询时，Route 53 VPC 解析器会执行以下步骤：

1. 解析程序检查规则中的域名。

   如果查询中的域名与默认转发规则中的域名匹配，VPC Resolver 会将查询转发到您在创建出站终端节点时指定的 IP 地址。出站端点随后将查询转发到您网络上解析程序的 IP 地址，您在创建规则时指定该地址。

如果响应中的委托记录与委托规则匹配，则 Resolver 通过与委托规则关联的出站端点将授权委托给本地解析程序。

有关更多信息，请参阅 VPC 解析器如何确定查询中的域名是否与任何规则匹配。

2. Resolver 端点根据“.”规则中的设置来转发 DNS 查询。

   如果查询中的域名与任何其他规则中的域名不匹配，VPC Resolver 将根据自动定义的 “” 中的设置转发查询。（点）规则。点阵规则适用于所有域名，但私有托管区域中的某些 Amazon 内部域名和记录名称除外。如果查询中的域名与您的自定义转发规则中的任何名称都不匹配，则此规则会让 VPC 解析器将 DNS 查询转发到公共名称服务器。如果要将所有查询转发到您网络上的 DNS 解析程序，您可以创建自定义转发规则，为域名指定“.”，为类型指定转发，并指定这些解析程序的 IP 地址。

3. VPC 解析器将响应返回给提交查询的应用程序。

在多个区域中使用规则

Route 53 VPC Resolver 是一项区域服务，因此您在一个 Amazon 区域中创建的对象仅在该区域可用。要在多个区域中使用同一个规则，您必须在各个区域中创建该规则。

创建规则的 Amazon 账户可以与其他 Amazon 账户共享该规则。有关更多信息，请参阅 与其他 Amazon 账户共享解析器规则并使用共享规则。

VPC 解析器为其创建自动定义的系统规则的域名

解析器自动创建自动定义的系统规则，这些规则定义默认情况下如何解析所选域的查询：

- 对于私有托管区域和亚马逊 EC2特定域名（例如 compute.amazonaws.com 和 compute.internal），如果您为不太具体的域名（例如 “”）创建条件转发规则，则自动定义的规则可确保您的私有托管区域和 EC2 实例继续解析。 (dot) 或 “com”。
- 对于公开预留的域名（例如 localhost 和 10.in-addr.arpa），DNS 最佳实践建议在本地应答查询，而不是转发到公有名称服务器。请参阅 RFC 6303，本地服务的 DNS 区域。

> **Note**
>
> 如果为 "."（点）或 "com" 创建条件转发规则，我们建议您还为 amazonaws.com 创建系统规则。（系统规则会让 VPC 解析器在本地解析特定域和子域名的 DNS 查询。）创建此系统规则可以提高性能，减少转发到您的网络的查询数量，并降低 VPC 解析器费用。

如果要覆盖自动定义的规则，可以为相同的域名创建条件转发规则。

您还可以禁用某些自动定义的规则。有关更多信息，请参阅 VPC 解析器中反向 DNS 查询的转发规则。

VPC 解析器创建以下自动定义的规则。

私有托管区域的规则

对于您与 VPC 关联的每个私有托管区域，VPC Resolver 都会创建一个规则并将其与 VPC 关联。如果您将私有托管区域与多个托管区域相关联 VPCs，VPC Resolver 会将该规则与同一个 VPCs区域相关联。

规则的类型为 Forward (转发)。

各种 Amazon 内部域名的规则

此部分中内部域名的所有规则类型均为 Forward（转发）。VPC 解析器将这些域名的 DNS 查询转发给 VPC 的权威域名服务器。

> **Note**
>
> 当你将 VPC 的`enableDnsHostnames`标志设置为时，VPC 解析器会创建其`true`中的大部分规则。即使您没有使用解析器终端节点，VPC 解析器也会创建规则。

VPC 解析器会创建以下自动定义的规则，并在您将 VPC 的`enableDnsHostnames`标志设置为：`true`

- *Region-name*.compute.internal，例如 eu-west-1.compute.internal。us-east-1 区域不使用此域名。
- *Region-name*.compute。 *amazon-domain-name*，例如 eu-west-1.compute.amazonaws.com 或 cn-north-1.compute.amazonaws.com.cn。us-east-1 区域不使用此域名。
- ec2.internal。只有 us-east-1 区域使用此域名。
- compute-1.internal。只有 us-east-1 区域使用此域名。
- compute-1.amazonaws.com。只有 us-east-1 区域使用此域名。

以下自动定义规则用于对规则进行反向 DNS 查找，这些规则是 VPC 解析器在您将 VPC 的`enableDnsHostnames`标志设置为时创建的。`true`

- 10.in-addr.arpa
- 16.172.in-addr.arpa 到 31.172.in-addr.arpa

- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- 每个 VPC 的 CIDR 范围的规则。例如，如果 VPC 的 CIDR 范围为 10.0.0.0/23，VPC 解析器会创建以下规则：
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

当您将 VPC 的 `enableDnsHostnames` 标记设置为 `true` 时，对于与 localhost 相关的域，还会创建以下自动定义的规则并与 VPC 关联：

- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa

当您通过传输网关或 VPC 对等互连将 VPC 与其他 VPC 连接并启用 DNS 支持时，VPC 解析器会创建以下自动定义的规则，并将其与您的 VPC 关联起来：

- 对等 VPC 的 IP 地址范围的反向 DNS 查找，例如 0.192.in-addr.arpa

  如果您向 VPC 添加 IPv4 CIDR 块，VPC 解析器会为新 IP 地址范围添加自动定义的规则。
- 如果另一个 VPC 处于其他区域，则为以下域名：
  - *Region-name*.compute.internal。us-east-1 区域不使用此域名。
  - *Region-name*.compute。 *amazon-domain-name*。us-east-1 区域不使用此域名。
  - ec2.internal。只有 us-east-1 区域使用此域名。
  - compute-1.amazonaws.com。只有 us-east-1 区域使用此域名。

所有其他域的规则

VPC 解析器创建一个“.”（点）规则，适用于本主题前面未指定的所有域名。“.” 规则具有递归类型，这意味着该规则会让 VPC 解析器充当递归解析器。

创建入站和出站端点的注意事项

在 Amazon 区域中创建入站和出站 Resolver 终端节点之前，请考虑以下问题。

主题

- 每个 区域中的入站和出站端点的数量
- 对入站和出站端点使用相同的 VPC
- 入站端点和私有托管区域
- VPC 对等连接
- 共享子网中的 IP 地址
- 您的网络与您在其中创建端点的网络之间的连接 VPCs
- 在共享规则时，您还会共享出站端点
- 选择用于端点的协议
- 使用配置为专用实例租用 VPCs 的 VPC 解析器

每个 区域中的入站和出站端点的数量

当你想将某个 Amazon 区域的 DNS 与网络的 DNS 集成时，通常需要一个 Resolver 入站终端节点（用于你要转发到自己的 DNS 查询 VPCs）和一个出站终端节点（用于从你的网络转发 VPCs 到你的网络的查询）。 VPCs 您可以创建多个入站端点和多个出站端点，但一个端点足以处理各方向的 DNS 查询。注意以下几点：

- 对于每个 Resolver 端点，您可以在不同的可用区中指定两个或更多 IP 地址。端点中的每个 IP 地址每秒可处理大量 DNS 查询。（有关针对端点中每个 IP 地址当前每秒处理的最大查询数，请参阅Route 53 VPC 解析器的配额）。如果您需要 VPC Resolver 来处理更多查询，则可以向现有终端节点添加更多 IP 地址，而不必添加其他终端节点。
- VPC Resolver 的定价基于终端节点中的 IP 地址数量以及终端节点处理的 DNS 查询数量。每个端点包含至少两个 IP 地址。有关 VPC 解析器定价的更多信息，请参阅 Amazon Route 53 定价。
- 每个规则指定了 DNS 查询转发自的出站端点。如果您在 Amazon 区域中创建了多个出站端点，并且您希望将部分或全部 Resolver 规则与每个 VPC 关联，则需要创建这些规则的多个副本。

对入站和出站端点使用相同的 VPC

您可以在同一 VPC 中创建入站和出站终端节点，也可以在同一区域的不同 VPCs VPC 中创建入站和出站终端节点。

有关更多信息，请参阅 Amazon Route 53 的最佳实践。

入站端点和私有托管区域

如果您希望 VPC Resolver 使用私有托管区域中的记录解析入站 DNS 查询，请将私有托管区域与您在其中创建入站终端节点的 VPC 相关联。有关将私有托管区域与关联的信息 VPCs，请参阅使用私有托管区。

VPC 对等连接

无论您选择的 VPC 是否与其他 VPCs VPC 对等，您都可以将 Amazon 区域中的任何 VPC 用于入站或出站终端节点。有关更多信息，请参阅 Amazon Virtual Private Cloud VPC 对等互联。

共享子网中的 IP 地址

创建入站或出站端点时，只有在当前账户创建了 VPC 时，才能在共享子网中指定 IP 地址。如果另一个账户创建 VPC 并与您的账户共享 VPC 中的子网，则您无法在该子网中指定 IP 地址。有关共享子网的更多信息，请参阅 Amazon VPC 用户指南 VPCs中的使用共享子网。

您的网络与您在其中创建端点的网络之间的连接 VPCs

您的网络与您在其中创建终端节点的 VPCs 网络之间必须有以下连接之一：

- 入站端点 — 在您的网络与为其创建入站端点的各个 VPC 之间，您必须设置 Amazon Direct Connect 连接或 VPN 连接。
- 出站端点 — 在您的网络与您为其创建出站端点的各个 VPC 之间，您必须设置 Amazon Direct Connect 连接、VPN 连接或网络地址转换 (NAT) 网关。

在共享规则时，您还会共享出站端点

创建规则时，您可以指定希望 VPC 解析器用于将 DNS 查询转发到您的网络的出站终端节点。如果您与其他 Amazon 账户共享该规则，则还会间接共享您在规则中指定的出站终端节点。如果您 VPCs 在一个 Amazon 地区使用多个 Amazon 账户进行创建，则可以执行以下操作：

- 在该区域中创建一个出站端点。
- 使用一个 Amazon 账户创建规则。
- 与在该地区创建 VPCs 的所有 Amazon 账户共享规则。

这允许您使用一个区域中的一个出站终端节点将多个 DNS 查询转发到您的网络， VPCs 即使这些查询 VPCs 是使用不同的 Amazon 账户创建的。

选择用于端点的协议

端点协议决定如何将数据传输到入站端点和从出站端点传输数据。不需要加密 VPC 流量的 DNS 查询，因为网络上的每个数据包流都要根据规则单独授权，以便在传输和传送其之前验证正确的源和目标。未经传输实体和接收实体特别授权，信息基本上不可能在实体之间任意传递。如果将数据包路由到目标，但没有与之匹配的规则，则该数据包将被丢弃。有关更多信息，请参阅 VPC 功能。

可用的协议包括：

- Do53：端口 53 上的 DNS。使用 VPC 解析器中继数据，无需额外加密。虽然外部各方无法读取数据，但可以在 Amazon 网络内查看。使用 UDP 或 TCP 发送数据包。Do53 主要用于亚马逊内部和亚马逊 VPCs之间的流量。目前，这是唯一可用于委托入站端点的协议。
- DoH：通过加密的 HTTPS 会话传输数据。DoH 可提升安全性，其中未经授权的用户无法解密数据，并且除预期接收方外，任何人都无法读取数据。不适用于委托入站端点。
- DoH-FIPS：通过符合 FIPS 140-2 加密标准的加密 HTTPS 会话传输数据。仅入站端点支持 有关更多信息，请参阅 FIPS PUB 140-2。不适用于委托入站端点。

对于转发类型的入站端点，可以按以下方式应用协议：

- 结合使用 Do53 和 DoH。
- 结合使用 Do53 和 DoH-FIPS。
- 单独使用 Do53。
- 单独使用 DoH。
- 单独使用 DoH-FIPS。
- 无，即视为 Do53。

对于出站端点，可以按以下方式应用协议：

- 结合使用 Do53 和 DoH。
- 单独使用 Do53。
- 单独使用 DoH。
- 无，即视为 Do53。

另请参阅 创建或编辑入站端点时指定的值 和 创建或编辑出站端点时指定的值。

使用配置为专用实例租用 VPCs 的 VPC 解析器

当您创建 Resolver 端点时，无法指定将实例租赁属性设置为 `dedicated` 的 VPC。VPC 解析器不能在单租户硬件上运行。

您仍然可以使用 VPC 解析器来解析源自 VPC 的 DNS 查询。创建至少一个将实例租赁属性设置为 `default` 的 VPC，并在您创建入站和出站端点时指定该 VPC。

当您创建转发规则时，可以将其与任何 VPC 关联，不论实例租约属性的设置如何。

Route 53 VPC 解析器的可用性和可扩展性

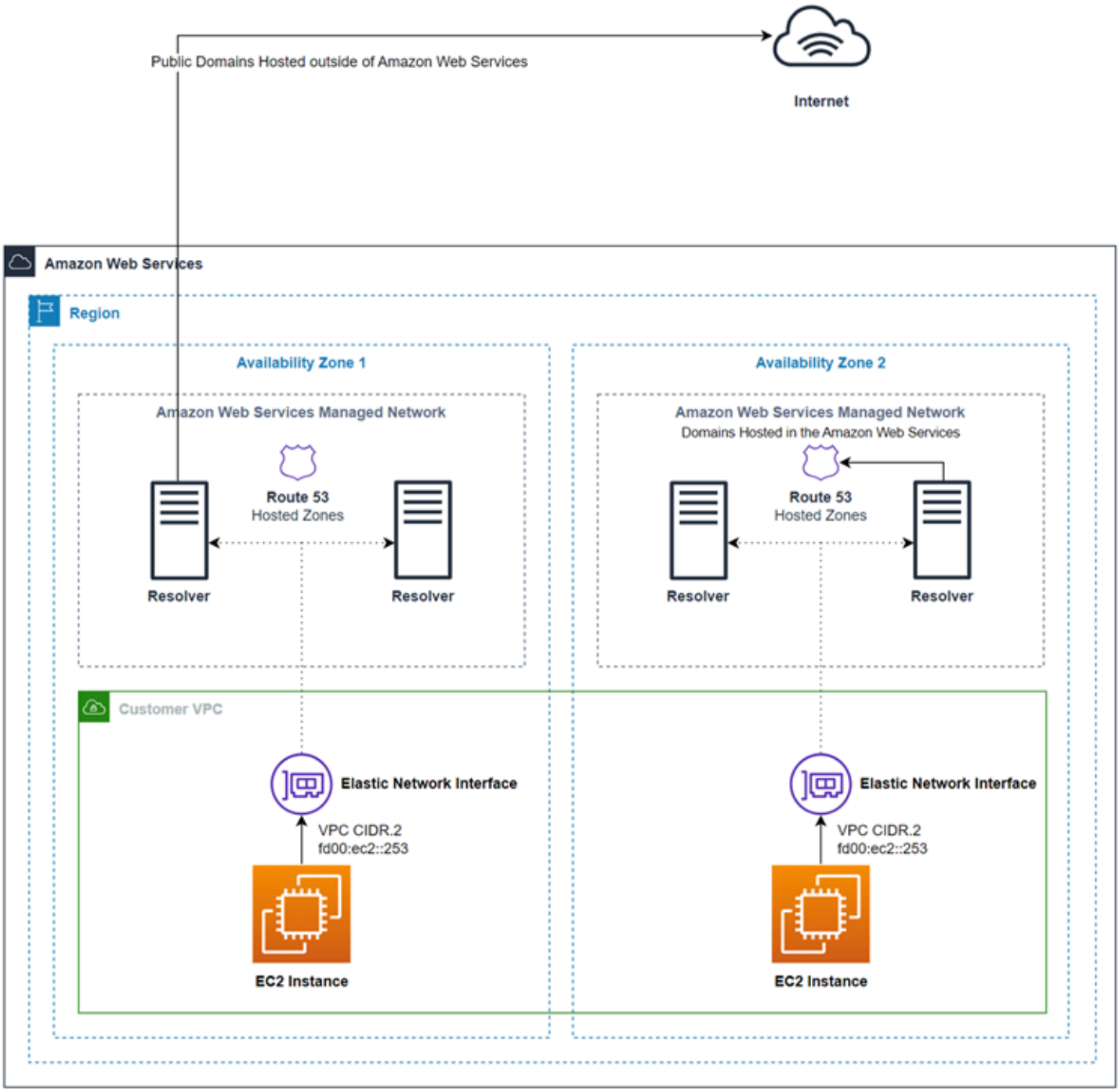
在 Amazon VPC CIDR + 2 地址和 fd00: ec2:: 253 上运行的 Route 53 VPC 解析器默认全部可用，它以递归方式响应公共记录 VPCs、亚马逊 VPC 特定的 DNS 名称和 Route 53 私有托管区域的 DNS 查询。Route 53 VPC 解析器由两个对用户透明的高可用性组件组成：Nitro Resolver 服务和区域解析器队列。Nitro Resolver 服务是一项服务，在 Nitro 实例上在 Nitro 卡中运行，在老一代实例中在 Dom0 中运行，并在主机服务器上使用发往本地的 Route 53 VPC 解析器的数据包。有关更多信息，请参阅 Amazon Nitro 系统的安全设计。

Nitro Resolver 服务带有本地缓存，这有助于通过响应实例在短时间内发出的重复查询来减小延迟。当 Nitro Resolver 服务收到一个没有缓存答案的查询时，它会将查询转发给 Zonal Resolver 实例集，这是一个高度可用的解析程序实例集，通常与此实例位于同一个可用区。当路径中的上游名称服务器或其他组件在处理查询时出现故障时，Nitro Resolver 服务通常可以透明地处理这些故障，而不会影响实例上运行的工作负载。此外，如果解析器遇到来自域名服务器的查询超时、连接被拒绝或 SERVFAILS，它可能会使用超出 Time-To-Live (TTL) 值的缓存答案进行响应，以提高可用性。Nitro Resolver 服务和 Zonal Resolver 实例集之间的查询仅限于客户 VPC 之外的严格控制网络，客户无法访问该网络，并且网络受到严格的安全控制。通过在 VPC 外部处理 Nitro Resolver 服务与 Zonal Resolver 实例集之间的查询，可以防止客户拦截其 VPC 内部的 DNS 查询。发往外部域名服务器的查询 Amazon 将通过公共互联网，源自属于区域解析器队列的公有 IP 地址。我们目前不支持 edns0-Client 子网属性，这意味着发往公有 DNS 名称服务器的所有查询都不包含有关源客户 IP 地址的信息。

Nitro Resolver 服务是实例上的链接本地服务的一部分。Link-Local 服务包括 Route 53 VPC 解析器、亚马逊时间服务 (NTP)、实例元数据服务 (IMDS) 和 Windows 许可服务（适用于 Windows 实例）。这些服务随着您在 VPC 中创建的每个弹性网络接口而扩展，每个网络接口允许每秒发送 1024 个数据包 (PPS) 到链接本地服务。超过此限制的数据包将被拒收。您可以根据 ethtool 返回的 `linklocal_allowance_exceeded` 值确定是否已超过此限制。有关 ethtool 的更多信息，请参阅亚马逊 EC2 用户指南中的监控您的亚马逊 EC2 实例的网络性能。 CloudWatch代理也可以将此 CloudWatch 指标报告给指标。由于 Route 53 VPC 解析器是按网络接口实现的，因此当您在更多可用区域中添加更多实例时，它会扩展并变得更加可靠。对每个 VPC 的查询数量没有汇总限制，因此

Route 53 VPC 解析器可以在 VPC 的范围内进行扩展，这本质上取决于网络地址使用情况 (NAU)。有关更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的您的 VPC 的网络地址使用情况。

下图概述了 Route 53 VPC 解析器如何解析可用区内的 DNS 查询。



开始使用 Route 53 VPC 解析程序

Route 53 VPC 解析器控制台包含一个向导，可指导您完成以下步骤以开始使用 VPC 解析器：

- 创建端点：入站和/或出站。
- 对于出站端点，请创建一个或多个转发规则，指定希望将 DNS 查询路由到您的网络的域名。
- 如果创建出站端点，请选择您希望与规则关联的 VPC。

使用向导配置 Route 53 VPC 解析器

1. 登录 Amazon Web Services 管理控制台 并打开 VPC 解析器控制台，网址为https://console.aws.amazon.com/route53resolver/。
2. 在 “欢迎使用 Route 53 VPC 解析器” 页面上，选择配置终端节点。
3. 在导航栏上，选择您要在其中创建解析程序端点的区域。
4. 在 Basic configuration (基本配置) 下，选择您转发 DNS 查询的方向：
   - 入站和出站：该向导将引导您完成设置，使您既可以将网络上的解析器的 DNS 查询转发到 VPC 中的 VPC 解析器，也可以将 VPC 中的指定查询（例如 example.com 或 example.net）转发给网络上的解析器。
   - 仅限入站：该向导将引导您完成设置，允许您将来自网络解析器的 DNS 查询转发到 VPC 中的 VPC 解析器。
   - Outbound only (仅限出站)：向导将引导您完成设置，将来自 VPC 的指定查询转发到您网络上的解析程序。
5. 选择下一步。
6. 如果您选择 Inbound and outbound (入站或出站) 或者 Inbound only (仅限入站)，则输入适用的值来配置入站端点。然后继续执行第 7 步。有关更多信息，请参阅 创建或编辑入站端点时指定的值。

   如果选择 Outbound only (仅限出站)，则跳至步骤 7。
7. 输入适用的值来配置出站端点。有关更多信息，请参阅 创建或编辑出站端点时指定的值。
8. 如果您选择 Inbound and outbound (入站或出站) 或者 Outbound only (仅限出站)，则输入适用的值来创建规则。有关更多信息，请参阅 创建或编辑规则时指定的值。
9. 在 Review and create (审核和创建) 页面上，确认上一页上指定的设置是否正确。如有必要，针对适用部分选择 Edit (编辑)，并更新设置。如果对设置满意，请选择 Submit (提交)。

> **Note**
>
> 创建出站端点仅需一两分钟。在第一个出站端点创建完成之前，您无法创建另一个出站端点。

10. 如果您要创建多个规则，请参阅管理转发规则。
11. 如果您创建入站端点，请配置网络上的 DNS 解析程序，将相应的 DNS 查询转发到您入站端点的 IP 地址。有关更多信息，请参阅您 DNS 应用程序的文档。

将入站 DNS 查询转发给您的 VPCs

要将您的网络中的 DNS 查询转发到 VPC 解析器，您需要创建一个入站终端节点。入站端点指定您希望网络上的 DNS 解析程序将 DNS 查询转发到的 IP 地址（在您的 VPC 可用的 IP 地址范围中）。这些 IP 地址不是公有 IP 地址，因此对于每个入站终端节点，您需要使用连接或 VPN Amazon Direct Connect 连接将 VPC 连接到您的网络。

在实施入站委托时，您需要将本地 DNS 基础设施中的子域的 DNS 权限委托给 VPC 解析器。要正确配置此委托，您必须使用入站端点的 IP 地址作为正在委托的子域的本地名称服务器上的粘附记录（NS 记录）。例如，如果您通过 IP 地址为 10.0.1.100 和 10.0.1.101 的入站委派终端节点将子域 “aws.example.com” 委托给 VPC 解析器，则您将在本地 DNS 服务器上创建 NS 记录，将 “aws.example.com” 指向这些 IP 地址。这样可以确保委托子域的 DNS 查询通过入站终端节点正确路由到 VPC 解析器，从而允许 VPC 解析器使用关联的私有托管区域的记录进行响应。

配置入站转发

要创建入站端点，请执行以下步骤。

创建入站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Inbound endpoints (入站端点)。
3. 在导航栏上，选择您要在其中创建入站端点的区域。
4. 选择 Create inbound endpoint (创建入站端点)。
5. 输入适用的值。有关更多信息，请参阅 创建或编辑入站端点时指定的值。
6. 选择创建。

7. 配置您网络上的 DNS 解析程序，将相应的 DNS 查询转发到您入站端点的 IP 地址。有关更多信息，请参阅您 DNS 应用程序的文档。

创建或编辑入站端点时指定的值

创建或编辑入站端点时，您指定以下值：

前哨基地 ID

如果您要在 VPC 上为 VPC 解析器创建终端节点，则这是 Amazon Outposts ID。 Amazon Outposts

端点名称

可在控制面板上轻松找到入站端点的友好名称。

端点类别

选择默认或委托。当类别为默认时，您网络上的解析程序会将 DNS 请求转发到入站端点的 IP 地址。当类别为委托时，域的权限将委托给 VPC 解析器。

region-name 区域中的 VPC

来自您的网络的所有入站 DNS 查询都会在发往 VPC 解析器的途中通过此 VPC。

此端点的安全组

您希望用于控制对此 VPC 的访问的一个或多个安全组的 ID。所指定的安全组必须包含一个或多个入站规则。入站规则必须允许端口 53 上的 TCP 和 UDP 访问。如果您使用的是 DoH 协议，则还必须允许安全组中的端口 443。创建端点后，您无法更改此值。

某些安全组规则会导致连接受到跟踪，对于入站端点来说，每个 IP 地址在每秒内的最大查询总数可能低至 1500。为避免安全组导致的连接跟踪，请参阅未跟踪的连接。

> **Note**
>
> 要添加多个安全组，请使用 Amazon CLI 命令`create-resolver-endpoint`。有关更多信息，请参阅 create-resolver-endpoint。

有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

端点类型

端点类型可以是 IPv4 IPv6、或双栈 IP 地址。对于双栈终端节点，该终端节点将同时包含 IPv4 和 IPv6 地址，您的网络上的 DNS 解析器可以将 DNS 查询转发到该地址。

> **Note**
>
> 出于安全考虑，我们拒绝所有双栈和 IPv6 IP 地址从公共互联网直接访问 IPv6 流量。

IP 地址

您希望网络上的 DNS 解析程序将 DNS 查询转发到的 IP 地址。您必须至少指定两个 IP 地址，以实现冗余配置。如果您创建了委托入站终端节点，请使用这些 IP 地址作为要将权限委托给 VPC Resolver 的子域的粘合 NS 记录。注意以下几点：

多个可用区域

我们建议您在至少两个可用区中指定 IP 地址。您可以选择在这些可用区或其他可用区中指定其他 IP 地址。

IP 地址和 Amazon VPC 弹性网络接口

对于您指定的可用区、子网和 IP 地址的每种组合，VPC 解析器都会创建一个 Amazon VPC 弹性网络接口。有关针对端点中每个 IP 地址当前每秒处理的最大 DNS 查询数，请参阅Route 53 VPC 解析器的配额。有关每个弹性网络接口定价的信息，请参阅 Amazon Route 53 定价页面上的“Amazon Route 53”。

> **Note**
>
> Resolver 端点具有私有 IP 地址。这些 IP 地址在端点的生命周期内不会发生变化。

对于每个 IP 地址，指定以下值。每个 IP 地址必须位于在 VPC in the region-name Region (<区域名称> 区域中的 VPC) 所指定 VPC 的可用区中。

可用区

希望 DNS 查询在到达您的 VPC 之前经过的可用区。您指定的可用区必须配置有子网。

子网

包含您要分配给解析器端点 ENIs的 IP 地址的子网。这些是您要发送 DNS 查询的地址。子网必须具有一个可用 IP 地址。

子网 IP 地址必须与端点类型相匹配。

IP 地址

您要分配到入站端点的 IP 地址。

选择是希望 VPC 解析器从指定子网中的可用 IP 地址中为您选择 IP 地址，还是要自己指定 IP 地址。

如果您选择自己指定 IP 地址，请输入或 IPv6 地址， IPv4 或同时输入两者。

协议

端点协议确定如何将数据传输到入站端点。根据所需的安全级别选择一个或多个协议。

- Do53：（默认）使用 Route 53 VPC 解析器中继数据，无需额外加密。虽然外部各方无法读取数据，但可以在 Amazon 网络内查看。这是目前唯一可用于委托入站端点类别的协议。
- DoH：通过加密的 HTTPS 会话传输数据。DoH 可提升安全性，其中未经授权的用户无法解密数据，并且除预期接收方外，任何人都无法读取数据。
- DoH-FIPS：通过符合 FIPS 140-2 加密标准的加密 HTTPS 会话传输数据。仅入站端点支持 有关更多信息，请参阅 FIPS PUB 140-2。

> **Note**
>
> 对于 DOH/DOH-FIPS 入站终端节点，存在已知问题，即在 VPC 解析器查询日志中发布的源 IP 不正确。

对于入站端点，可以按以下方式应用协议：

- 结合使用 Do53 和 DoH。
- 结合使用 Do53 和 DoH-FIPS。
- 单独使用 Do53。
- 单独使用 DoH。
- 单独使用 DoH-FIPS。
- 无，即视为 Do53。

> **Important**
>
> 不能将入站端点的协议直接从仅使用 Do53 更改为仅使用 DoH 或 DoH-FIPS。这是为了防止依赖于 Do53 的传入流量突然中断。要将协议从 Do53 更改为 DoH 或 DoH-FIPS，必须

先启用 Do53 和 DoH，或者启用 Do53 和 DoH-FIPS，以确保使用 DoH 协议或 DoH-FIPS 传输所有传入流量，然后移除 Do53。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

管理入站端点

要管理入站端点，请执行相关步骤。

主题

- 查看和编辑入站端点
- 查看入站端点的状态
- 删除入站端点

查看和编辑入站端点

要查看和编辑入站端点的设置，请执行以下步骤。

查看和编辑入站端点的设置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Inbound endpoints (入站端点)。
3. 在导航栏上，选择您在其中创建了入站端点的区域。
4. 选择您要查看或编辑设置的端点的选项。
5. 选择 View details (查看详细信息) 或 Edit (编辑)。

   有关入站端点的值的信息，请参阅创建或编辑入站端点时指定的值。
6. 如果选择 Edit (编辑)，请输入适用的值，然后选择 Save (保存)。

查看入站端点的状态

要查看入站端点的状态，请执行以下过程。

查看入站端点的状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Inbound endpoints (入站端点)。
3. 在导航栏上，选择您在其中创建了入站端点的区域。Status (状态) 列包含以下值之一：

   Creating

   VPC 解析器正在为该终端节点创建和配置一个或多个 Amazon VPC 网络接口。

   正常运行

   此终端节点的 Amazon VPC 网络接口配置正确，能够在您的网络和 VPC 解析器之间传递入站或出站 DNS 查询。

   Updating

   VPC 解析器正在将一个或多个网络接口与此终端节点关联或取消关联。

   自动恢复

   VPC Resolver 正在尝试恢复与此终端节点关联的一个或多个网络接口。在恢复过程中，端点可以工作但容量受限，因为每个 IP 地址（每个网络接口）的 DNS 查询数有限制。有关当前限制，请参阅Route 53 VPC 解析器的配额。

   需要操作

   此终端节点运行状况不佳，VPC 解析器无法自动将其恢复。要解决该问题，我们建议您检查与此端点关联的每个 IP 地址。对于每个不可用的 IP 地址，请添加另一个 IP 地址，然后删除该不可用 IP 地址。（端点必须始终包含至少两个 IP 地址。）状态 Action needed (需要操作) 可能有各种原因。以下是两个常见原因：

   - 已使用 Amazon VPC 删除与端点关联的一个或多个网络接口。
   - 出于超出 VPC 解析程序控制的某种原因，无法创建网络接口。

   Deleting

   VPC 解析器正在删除此端点和相关的网络接口。

删除入站端点

要删除入站端点，请执行以下步骤。

> **Important**
>
> 如果您删除入站终端节点，则来自您的网络的 DNS 查询将不再转发到您在终端节点中指定的 VPC 中的 VPC 解析器。

删除入站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Inbound endpoints (入站端点)。
3. 在导航栏上，选择您在其中创建了入站端点的区域。
4. 选中您要删除的端点对应的选项。
5. 选择删除。
6. 要确认您要删除该端点，请输入端点的名称并选择 Submit (提交)。

将出站 DNS 查询转发到您的网络

要将来自一个或多个 Amazon EC2 实例的 DNS 查询转发 VPCs 到您的网络，您需要创建一个出站终端节点和一条或多条规则：

出站端点

要将您的 DNS 查询转发 VPCs 到您的网络，您需要创建一个出站终端节点。出站端点指定发起查询的 IP 地址。您从 VPC 可用的 IP 地址范围中选择的这些 IP 地址不是公有 IP 地址。这意味着，对于每个出站端点，您需要使用 Amazon Direct Connect 连接、VPN 连接或网络地址转换 (NAT) 网关来将 VPC 连接到网络。请注意，您可以为同一地区的多个 VPCs 出站终端节点使用相同的出站终端节点，也可以创建多个出站终端节点。如果您希望使用您的出站终端节点 DNS64，则可以 DNS64 使用 Amazon Virtual Private Cloud 启用。有关更多信息，请参阅 Amazon VPC 用户指南NAT64中的DNS64 和。

VPC 解析器规则中的目标 IP 由 VPC 解析器随机选择，并且不优先选择特定的目标 IP 而不是另一个。如果目标 IP 未响应转发的 DNS 请求，VPC 解析器将重试目标中的随机 IP 地址。 IPs

确保所有目标 IP 地址都可以从解析程序端点访问。如果 VPC 解析器无法将出站 DNS 查询转发到任何目标 IP，则可能会导致 DNS 解析时间延长。

Rules

要为希望转发到您的网络上的 DNS 解析程序的查询指定域名，您可以创建一个或多个规则。每个转发规则指定一个域名。然后，您可以将规则与要向您的网络转发查询的规则相关联。 VPCs

出站委托规则遵循与标准转发规则不同的特定委托原则。创建委托规则时，VPC Resolver 会根据 DNS 响应中的 NS 记录评估规则中的委托记录，以确定是否应进行委托。只有当委托规则配置与 DNS 响应中返回的实际 NS 记录相匹配时，VPC 解析器才会将权限委托给您的本地解析器。与基于域名匹配重定向查询的转发规则不同，委托规则遵守 DNS 委托链，只有在响应中的权威名称服务器与委托配置匹配时才会激活。

有关更多信息，请参阅以下主题：

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 VPC Resolver rules

配置出站转发

要配置 VPC 解析器以将源自您的 VPC 的 DNS 查询转发到您的网络，请执行以下步骤。

> **Important**
>
> 创建出站终端节点后，必须创建一个或多个规则并将其与一个或多个规则相关联 VPCs。规则指定要转发到您的网络的 DNS 查询的域名。

创建出站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Outbound endpoints (出站端点)。
3. 在导航栏上，选择您要在其中创建出站端点的区域。
4. 选择 Create outbound endpoint (创建出站端点)。
5. 输入适用的值。有关更多信息，请参阅 创建或编辑出站端点时指定的值。
6. 选择创建。

> **Note**
>
> 创建出站端点仅需一两分钟。在第一个出站端点创建完成之前，您无法创建另一个出站端点。

7. 创建一个或多个规则，指定要转发到您网络的 DNS 查询的域名。有关该过程的更多信息，请参阅接下来的步骤。

要创建一个或多个转发规则，请执行以下步骤。

创建转发规则并将这些规则与一个或多个规则关联 VPCs

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您想要在其中创建规则的区域。
4. 选择 Create rule（创建规则）。
5. 输入适用的值。有关更多信息，请参阅 创建或编辑规则时指定的值。
6. 选择 Save。
7. 要添加其它规则，请重复步骤 4 到 6。

创建或编辑出站端点时指定的值

创建或编辑出站端点时，您指定以下值：

前哨基地 ID

如果您要在 VPC 上为 VPC 解析器创建终端节点，则这是 Amazon Outposts ID。 Amazon Outposts

端点名称

可在控制面板上轻松找到出站端点的友好名称。

region-name 区域中的 VPC

所有出站 DNS 查询将在到达您的网络之前流经此 VPC。

此端点的安全组

您希望用于控制对此 VPC 的访问的一个或多个安全组的 ID。所指定的安全组必须包含一个或多个出站规则。对于在您网络上用于 DNS 查询的端口，出站规则必须允许该端口上的 TCP 和 UDP 访问。创建端点后，您无法再更改此值。

某些安全组规则会导致连接受到跟踪，并可能影响每秒内从出站端点到目标名称服务器发出的最大查询次数。为避免安全组导致的连接跟踪，请参阅未跟踪的连接。

有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

端点类型

端点类型可以是 IPv4 IPv6、或双栈 IP 地址。对于双栈终端节点，该终端节点将同时包含 IPv4 和 IPv6 地址，您的网络上的 DNS 解析器可以将 DNS 查询转发到该地址。

> **Note**
>
> 出于安全考虑，我们拒绝所有双栈和 IPv6 IP 地址的直接 IPv6 流量访问公共互联网。

IP 地址

您希望 VPC 解析器在网络解析器途中将 DNS 查询转发到您的 VPC 中的 IP 地址。这些不是网络上 DNS 解析器的 IP 地址；您在创建与一个或多个关联的规则时指定解析器 IP 地址。 VPCs您必须至少指定两个 IP 地址，以实现冗余配置。

> **Note**
>
> Resolver 端点具有私有 IP 地址。这些 IP 地址在端点的生命周期内不会发生变化。

注意以下几点：

多个可用区域

我们建议您在至少两个可用区中指定 IP 地址。您可以选择在这些可用区或其他可用区中指定其他 IP 地址。

IP 地址和 Amazon VPC 弹性网络接口

对于您指定的可用区、子网和 IP 地址的每种组合，VPC 解析器都会创建一个 Amazon VPC 弹性网络接口。有关针对端点中每个 IP 地址当前每秒处理的最大 DNS 查询数，请参阅Route 53

VPC 解析器的配额。有关每个弹性网络接口定价的信息，请参阅 Amazon Route 53 定价页面上的“Amazon Route 53”。

IP 地址的顺序

您可以按任意顺序指定 IP 地址。转发 DNS 查询时，VPC 解析器不会根据 IP 地址的列出顺序选择 IP 地址。

对于每个 IP 地址，指定以下值。每个 IP 地址必须位于在 VPC in the region-name Region (<区域名称> 区域中的 VPC) 所指定 VPC 的可用区中。

可用区

希望 DNS 查询在到达您的网络之前经过的可用区。您指定的可用区必须配置有子网。

子网

其中包含希望 DNS 查询在到达您的网络之前源自的 IP 地址的子网。子网必须具有一个可用 IP 地址。

子网 IP 地址必须与端点类型相匹配。

IP 地址

希望 DNS 查询在到达您的网络之前源自的 IP 地址。

选择是希望 VPC 解析器从指定子网中的可用 IP 地址中为您选择 IP 地址，还是要自己指定 IP 地址。

如果您选择自己指定 IP 地址，请输入 IPv4 或 IPv6 地址，或同时输入两者。

协议

端点协议决定如何从出站端点传输数据。根据所需的安全级别选择一个或多个协议。

- Do53：（默认）使用 Route 53 VPC 解析器中继数据，无需额外加密。虽然外部各方无法读取数据，但可以在 Amazon 网络内查看该数据。
- DoH：通过加密的 HTTPS 会话传输数据。DoH 可提升安全性，其中未经授权的用户无法解密数据，并且除预期接收方外，任何人都无法读取数据。

对于出站端点，可以按以下方式应用协议：

- 结合使用 Do53 和 DoH。
- 单独使用 Do53。

- 单独使用 DoH。
- 无，即视为 Do53。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

创建或编辑规则时指定的值

创建或编辑转发规则时，您指定以下值：

规则名称

通过友好名称可在控制面板上轻松找到规则。

规则类型

选择适用的值：

- 转发 – 当您希望将指定域名的 DNS 查询转发到您网络上的 DNS 解析程序时，请选择此选项。
- 委托 — 如果您要将托管在私有托管区域中的子域的权限委托给您的本地解析器（或其他 VPC 上的 VPC 解析器），请选择此选项。
- 系统 — 如果您希望 VPC Resolver 有选择地覆盖转发规则中定义的行为，请选择此选项。创建系统规则时，VPC 解析器会解析指定子域名的 DNS 查询，否则这些查询将由您网络上的 DNS 解析器解析。

默认情况下，转发规则会应用到一个域名及其所有子域。如果您希望将对某个域的查询转发到您网络上的解析程序，但不想为某些子域转发查询，则为这些子域创建系统规则。例如，如果您为 example.com 创建一个转发规则，但不希望转发针对 acme.example.com 的查询，则可以创建系统规则，为域名指定 acme.example.com。

委托记录 - 仅适用于委托规则

与此域匹配的 DNS 查询会转发给您网络上的解析程序。

> **Note**
>
> 作为委托规则的先决条件，当使用私有托管区进行出站委托时，您必须在私有托管区中创建 NS 记录。记录是：NS - 名称服务器通过带有委托规则的 Resolver 出站端点进行委托。有关更多信息，请参阅 NS 记录类型。

VPCs 那些使用这条规则的人

使用 VPCs 此规则转发对指定域名或名称的 DNS 查询的。您可以根据需要将规则应用于 VPCs 任意数量。

域名 - 仅适用于转发规则

此域名的 DNS 查询将转发到您在 Target IP addresses (目标 IP 地址) 中指定的 IP 地址。例如，您可以指定特定域（example.com）、顶级域（com）或点（.）来转发所有 DNS 查询。有关更多信息，请参阅 VPC 解析器如何确定查询中的域名是否与任何规则匹配。

出站端点

VPC 解析器通过您在此处指定的出站终端节点将 DNS 查询转发到您在目标 IP 地址中指定的 IP 地址。

目标 IP 地址

如果 DNS 查询与您在 Domain name (域名) 中指定的名称匹配，出站端点会将查询转发到您在此处指定的 IP 地址。这些通常是您网络上 DNS 解析程序的 IP 地址。

Target IP addresses (目标 IP 地址) 仅在 Rule type (规则类型) 的值为 Forward (转发) 时可用。

指定 IPv4 要用于终端节点 IPv6 的地址、协议和 ServerNameIndication 协议。ServerNameIndication 仅当所选协议为 DoH 时才适用。

不支持通过出站端点解析网络上 DoH 解析程序的 FQDN 的目标 IP 地址。出站端点需要有网络上 DoH 解析程序的目标 IP 地址才能转发 DoH 查询。如果您网络上的 DoH 解析器需要在 TLS SNI 和 HTTP 主机标头中提供 FQDN，ServerNameIndication 则必须提供。

ServerNameIndication

想要转发查询的目标 DoH 服务器的服务器名称指示。此选项仅用于协议为 DoH 的情况。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签。有关对成本分配使用标签的更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

管理出站端点

要管理出站端点，请执行相关步骤。

主题

查看和编辑出站端点

要查看和编辑出站端点的设置，请执行以下步骤。

查看和编辑出站端点的设置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Outbound endpoints (出站端点)。
3. 在导航栏上，选择您在其中创建了出站端点的区域。
4. 选择您要查看或编辑设置的端点的选项。
5. 选择 View details (查看详细信息) 或 Edit (编辑)。

   有关出站端点的值的信息，请参阅创建或编辑出站端点时指定的值。
6. 如果选择 Edit (编辑)，请输入适用的值，然后选择 Save (保存)。

查看出站端点的状态

要查看出站端点的状态，请执行以下过程。

查看出站端点的状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Outbound endpoints (出站端点)。
3. 在导航栏上，选择您在其中创建了出站端点的区域。Status (状态) 列包含以下值之一：

   Creating

   VPC 解析器正在为该终端节点创建和配置一个或多个 Amazon VPC 网络接口。

正常运行

此终端节点的 Amazon VPC 网络接口配置正确，能够在您的网络和 VPC 解析器之间传递入站或出站 DNS 查询。

Updating

VPC 解析器正在将一个或多个网络接口与此终端节点关联或取消关联。

自动恢复

VPC Resolver 正在尝试恢复与此终端节点关联的一个或多个网络接口。在恢复过程中，端点可以工作但容量受限，因为每个 IP 地址（每个网络接口）的 DNS 查询数有限制。有关当前限制，请参阅Route 53 VPC 解析器的配额。

需要操作

此终端节点运行状况不佳，VPC 解析器无法自动将其恢复。要解决该问题，我们建议您检查与此端点关联的每个 IP 地址。对于每个不可用的 IP 地址，请添加另一个 IP 地址，然后删除该不可用 IP 地址。（端点必须始终包含至少两个 IP 地址。）状态 Action needed (需要操作) 可能有各种原因。以下是两个常见原因：

- 已使用 Amazon VPC 删除与端点关联的一个或多个网络接口。
- 出于超出 VPC 解析程序控制的某种原因，无法创建网络接口。

Deleting

VPC 解析器正在删除此端点和相关的网络接口。

删除出站端点

在删除端点之前，必须先删除与 VPC 关联的所有规则。

要删除出站端点，请执行以下步骤。

> **Important**
>
> 如果您删除出站终端节点，VPC 解析器将停止将 DNS 查询从您的 VPC 转发到您的网络，以获取指定已删除出站终端节点的规则。

删除出站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Outbound endpoints (出站端点)。
3. 在导航栏上，选择您在其中创建了出站端点的区域。
4. 选中您要删除的端点对应的选项。
5. 选择删除。
6. 要确认您要删除该端点，请输入端点的名称，然后选择 Submit (提交)。

管理转发规则

如果您希望 VPC Resolver 将对指定域名的查询转发到您的网络，则可以为每个域名创建一个转发规则，并指定要转发查询的域的名称。

主题

- 查看和编辑转发规则
- 创建转发规则
- 添加反向查找规则
- 将转发规则与 VPC 关联
- 解除转发规则与 VPC 的关联
- 与其他 Amazon 账户共享解析器规则并使用共享规则
- 删除转发规则
- VPC 解析器中反向 DNS 查询的转发规则

查看和编辑转发规则

要查看和编辑转发规则的设置，请执行以下步骤。

查看和编辑转发规则的设置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。

3. 在导航栏上，选择您在其中创建了规则的区域。
4. 选择您要查看或编辑设置的规则的选项。
5. 选择 View details (查看详细信息) 或 Edit (编辑)。

   有关转发规则的值的信息，请参阅创建或编辑规则时指定的值。
6. 如果选择 Edit (编辑)，请输入适用的值，然后选择 Save (保存)。

创建转发规则

要创建一个或多个转发规则，请执行以下步骤。

创建转发规则并将这些规则与一个或多个规则关联 VPCs

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您想要在其中创建规则的区域。
4. 选择 Create rule（创建规则）。
5. 输入适用的值。有关更多信息，请参阅 创建或编辑规则时指定的值。
6. 选择 Save。
7. 要添加其它规则，请重复步骤 4 到 6。

添加反向查找规则

如果您需要控制 VPC 中的反向查找，可以向出站解析程序端点添加规则。

要创建反向查找规则

1. 按照上一步中的步骤操作，直到步骤 5。
2. 指定规则时，为您想要反向查找转发规则的一个或多个 IP 地址输入 PTR 记录。

   例如，如果需要转发对 10.0.0.0/23 范围内地址的查找，请输入两个规则：

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

这些子网中的任何 IP 地址都将引用为这些 PTR 记录的子域，例如，10.0.1.161 的反向查找地址将为 161.1.0.10.in-addr.arpa，该地址是 1.0.10.in-addra.arpa 的子域。

3. 指定要将这些查找转发到的服务器。
4. 将这些规则添加到您的出站解析程序端点。

请注意，为 VPC 开启 enableDNSHostNames 将自动添加 PTR 记录。请参阅什么是 Route 53 VPC 解析器？。仅当您希望为给定的 IP 范围显式指定解析程序时（例如，将查询转发到 Active Directory 服务器时），才需要执行上一步骤。

将转发规则与 VPC 关联

创建转发规则后，必须将该规则与一条或多条转发规则关联 VPCs。这些规则只有在与 VPC 关联后才会生效。当您将规则与 VPC 关联时，VPC 解析器开始将规则中指定的域名的 DNS 查询转发给您在规则中指定的 DNS 解析器。查询经过您在创建规则时指定的出站端点。

将转发规则与一个或多个转发规则关联 VPCs

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您在其中创建了规则的区域。
4. 选择要与一个或多个规则关联的规则的名称 VPCs。
5. 选择 Associate VPC (关联 VPC)。
6. 在 “使用VPCs 此规则” 下 VPCs ，选择要与该规则关联的。
7. 选择添加。

解除转发规则与 VPC 的关联

在下列情况下，您可以从 VPC 解除关联的转发规则：

- 对于源自此 VPC 的 DNS 查询，您希望 VPC 解析器停止将对规则中指定的域名的查询转发到您的网络。
- 您希望删除转发规则。如果某条规则当前与一个或多个规则关联 VPCs，则必须先取消该规则与所有规则的关联， VPCs 然后才能将其删除。

如果要取消转发规则与一个或多个转发规则的关联 VPCs，请执行以下步骤。

解除转发规则与 VPC 的关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您在其中创建了规则的区域。
4. 选择要取消与一条或多 VPCs条规则关联的规则的名称。
5. 选择要与之解除规则关联的 VPC 所对应的选项。
6. 选择取消关联。
7. 键入 disassociate (取消关联) 以确认。
8. 选择提交。

与其他 Amazon 账户共享解析器规则并使用共享规则

您可以与其他账户共享您使用一个 Amazon 账户创建的 Resolver 规则。 Amazon 为了共享规则，Route 53 VPC Resolver 控制台与 Amazon 资源访问管理器集成。有关 Resource Access Manager 的更多信息，请参阅 Resource Access Manager 用户指南。

注意以下几点：

将共享规则与关联 VPCs

如果另一个 Amazon 账户与您的账户共享了一个或多个规则，则您可以将这些规则与您的 VPCs 账户关联起来，就像将创建的规则与您的账户关联一样 VPCs。有关更多信息，请参阅 将转发规则与 VPC 关联。

删除或取消共享规则

如果您与其他账户共享一条规则，然后删除该规则或停止共享该规则，并且该规则与一个或多个 VPCs账户相关联，则 Route 53 VPC Resolver 将开始 VPCs根据其余规则处理这些规则的 DNS 查询。该行为与您从 VPC 上解除关联规则的行为相同。

如果将规则共享给组织单位（OU）并将该 OU 中的账户移至其他 OU，则该共享规则与该账户中任何 VPC 的所有关联都将删除。但是，如果 VPC 解析器规则已与目标 OU 共享，则 VPC 关联将保持不变且不会解除关联。

规则和关联的最大数量

当一个账户创建规则并与一个或多个其他账户共享规则时，每个 Amazon 区域的最大规则数将适用于创建该规则的账户。

当与之共享规则的账户将该规则与一个或多个关联时 VPCs，规则之间和 VPCs 每个区域的最大关联数将应用于与之共享该规则的账户。

有关当前 VPC 解析器配额，请参阅Route 53 VPC 解析器的配额。

Permissions

要与其他 Amazon 账户共享规则，您必须拥有使用该PutResolverRulePolicy操作的权限。

对与之共享规则的 Amazon 账户的限制

与其共享了规则的账户无法更改或删除该规则。

标签

只有创建规则的账户可以添加、删除或查看规则上的标签。

要查看规则当前的共享状态（包括共享规则的账户或与其共享了规则的账户），以及将规则与其他账户共享，请执行以下步骤。

查看共享状态并与其他 Amazon 账户共享规则

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您在其中创建了规则的区域。

   Sharing status (共享状态) 列显示当前账户所创建规则或者与当前账户所共享规则的当前共享状态。

   - 未共享：当前 Amazon 账户创建了规则，但该规则未与任何其他账户共享。
   - Shared by me (由我共享)：当前账户创建的规则并且已与一个或多个账户共享。
   - Shared With me (与我共享)：其他账户创建的规则并且已与当前账户共享。
4. 选择您要显示共享信息或者您要与其他账户共享的规则的名称。

在 “规则:*rule name*” 页面上，“所有者” 下的值显示创建规则的账户的 ID。除非 Sharing status (共享状态) 的值为 Shared with me (与我共享)，否则这是当前账户。如果是共享的规则，则 Owner (所有者) 是创建该规则并与当前账户进行共享的账户。

5. 选择 Share (共享) 以查看更多信息或与其他账户共享规则。Resource Access Manager 控制台根据 Sharing status (共享状态) 的值显示一个页面：

   - Not shared (未共享)：显示 Create resource share (创建资源共享) 页面。有关如何与其他账户、OU 或组织共享规则的信息，请跳到步骤 6。
   - Shared by me (由我共享)：Shared resources (共享的资源) 页面显示由当前账户拥有并与其他账户共享的规则和其他资源。
   - Shared with me (与我共享)：Shared resources (共享的资源) 页面显示由其他账户拥有并与当前账户共享的规则和其他资源。

6. 要与其他 Amazon 账户、组织单位或组织共享规则，请指定以下值。

   > **Note**
   >
   > 您无法更新共享设置。如果想要更改任何以下设置，您必须使用新设置重新共享规则，然后删除旧的共享设置。

   说明

   输入可以帮助您记住为什么共享规则的简短说明。

   资源

   选中与您要共享的规则对应的复选框。

   主体

   输入 Amazon 账号、OU 名称或组织名称。

   标签

   指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

   这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签；您也可以将标签用于其他目的。有关对成本分配使用标签的更多信息，请参阅 Amazon Billing 用户指南中的使用成本分配标签。

删除转发规则

要删除转发规则，请执行以下步骤。

注意以下几点：

- 如果转发规则与任何规则关联 VPCs，则必须先取消该规则与的关联， VPCs然后才能删除该规则。有关更多信息，请参阅 解除转发规则与 VPC 的关联。
- 您无法删除默认的 Internet Resolver (Internet 解析程序) 规则，该规则的值为 Recursive (递归) (针对 Type (类型)) 。此规则会让 Route 53 VPC Resolver 充当您未为其创建自定义规则以及 VPC 解析器未为其创建自动定义规则的任何域名的递归解析器。有关如何为规则分类的更多信息，请参阅使用规则控制将哪些查询转发到您的网络。

删除转发规则

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择规则。
3. 在导航栏上，选择您在其中创建了规则的区域。
4. 选中您要删除的规则对应的选项。
5. 选择删除。
6. 要确认删除该规则，请输入规则的名称，然后选择 Submit (提交)。

VPC 解析器中反向 DNS 查询的转发规则

当 Amazon VPC 中的虚拟私`enableDnsSupport`有云 (VPC) 的`enableDnsHostnames`和设置`true`为时，VPC 解析器会自动为反向 DNS 查询创建自动定义的系统规则。有关这些设置的更多信息，请参阅 Amazon VPC 开发人员指南中的 VPC 中的 DNS 属性。

反向 DNS 查询的转发规则对于 SSH 或 Active Directory 等服务特别有用，这些服务可以选择通过对客户尝试从中连接到资源的 IP 地址执行反向 DNS 查找来验证用户身份。有关自动定义系统规则的更多信息，请参阅 VPC 解析器为其创建自动定义的系统规则的域名。

您可以关闭这些规则并修改所有反向 DNS 查询，以便将它们转发到本地名称服务器进行解析。

关闭自动规则后，请创建规则以根据需要将查询转发到本地资源。有关如何管理转发规则的详细信息，请参阅 管理转发规则。

关闭自动定义的规则

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格的 VPC 解析器下，选择 VPCs，然后选择一个 VPC ID。
3. 在 Autodefined rules for reverse DNS resolution（反向 DNS 解析的自动定义规则）下，取消选中复选框。如果已取消选中该复选框，则可以选中该复选框以启用自动定义的反向 DNS 解析。

有关相关信息 APIs，请参阅 VPC 解析器配置 APIs。

解析程序委托规则教程

委托规则允许 VPC 解析器通过指定的出站终端节点访问托管委派区域的域名服务器。虽然转发规则通知 VPC 解析器通过出站终端节点将 DNS 查询转发到与指定域名匹配的域名服务器，但委派规则通知 VPC 解析器通过返回委托的 NS 记录时指定的出站终端节点访问委派域名服务器。当 DNS 响应中的 NS 记录与委派记录中指定的域名匹配时，VPC 解析器会向委派域名服务器发送查询。

使用 Resolver 端点出站委托的步骤

1. 在 VPC 中创建一个解析器出站终端节点，您希望通过该终端节点向网络上的解析器发出 DNS 查询。

   您可以使用以下 API 或 CLI 命令：

   - CreateResolverEndpoint API
   - create-resolver-endpoint CLI
2. 创建一个或多个委托规则，这些规则指定应通过指定的出站端点将查询委托到您的网络的域名。

   使用 CLI 创建委托规则的示例：

   ```
   aws route53resolver create-resolver-rule \
   --region REGION \
   --creator-request-id delegateruletest \
   --delegation-record example.com \
   --name delegateruletest \
   --rule-type DELEGATE \
   --resolver-endpoint-id outbound endpoint ID
   ```
3. 将委托规则与您想要委托查询的委托规则相关联。 VPCs

您可以使用以下 API 或 CLI 命令：

- AssociateResolverRuleAPI。
- associate-resolver-rulesCLI 命令。

Resolver 出站端点支持的委托类型

VPC 解析器支持两种类型的出站委派：

- 路由 53 私有托管区域到 VPC 解析器出站委派：

  使用出站委托，将私有托管区中的子域委托给本地 DNS 服务器或 Internet 上的公有托管区。此出站委托允许您在私有托管区和委托区域之间分配 DNS 记录的管理。根据您的 DNS 设置，可以在私有托管区中使用或不使用粘附记录进行委托。有关更多信息，请参阅 私有托管区到出站。
- VPC 解析器出站到出站委托：

  使用出站到出站委托，将子域从您的本地 DNS 服务器委托给位于相同或不同位置的另一个本地服务器。这类似于从私有托管区委托给出站端点，您可以在其中委托给本地名称服务器上托管的区域。有关更多信息，请参阅 出站到出站。

通往 VPC Resolver 的 Route 53 私有托管区域出站委派示例配置

假设有一个 DNS 设置，其中父托管区托管在 Amazon VPC 的 Route 53 私有托管区中，子域委托给在欧洲、亚洲和北美洲托管的名称服务器。所有 DNS 查询都通过 VPC 解析器传递。

按照示例步骤配置您的私有托管区域和 VPC 解析器。

配置出站委托的私有托管区

1. 对于私有托管区设置：

   父托管区：`hr.example.com`

```
$TTL    86400 ; 24 hours
$ORIGIN hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
```

```
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of Zone Delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue Record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue Record
```

2. 对于欧洲本地区域中的本地名称服务器：

   - 托管区：eu.hr.example.com NS IP：10.0.0.30

```
$TTL    86400 ; 24 hours
$ORIGIN eu.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. 对于亚洲本地区域中的本地名称服务器：

   托管区：apac.hr.example.com、10.0.0.40

   APAC 名称服务器可以将子域委托给其他名称服务器。

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

   托管区：engineering.apac.hr.example.com、10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. 对于北美洲本地区域中的本地名称服务器：

托管区：na.hr.example.net NS IP：10.0.0.50

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

VPC 解析器设置

- 对于 VPC 解析器，您需要设置一条转发规则和两条委托规则：

  转发规则

  1. 用于转发 out-of-zone委派记录，因此 Route 53 VPC 解析器知道委托的 NS 的 IP 以转发初始请求。

     domain-name：hr.example.net target-ips：10.0.0.50

  委托规则

  1. 区域内委托的委托规则：

     委托记录：hr.example.com
  2. 区域外委托的委托规则：

     委托记录：hr.example.net

出站到出站委托示例配置

不是将父托管区置于 Amazon VPC 中，而是假设有一个 DNS 设置，其中父托管区位于本地中心位置，而子域被委托给在欧洲、亚洲和北美洲托管的名称服务器。所有 DNS 查询都通过 VPC 解析器传递。

按照示例步骤配置您的本地 DNS 和 VPC 解析器。

配置本地 DNS

1. 对于本地中心区域中的本地名称服务器：

   - 父托管区：hr.example.com

     托管区 hr.example.com，NS IP：10.0.0.20

```
$TTL    86400 ; 24 hours
$ORIGIN hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of zone delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue record
```

2. 对于欧洲本地区域中的本地名称服务器（欧洲、亚洲和北美洲名称服务器的配置与私有托管区的出站委托配置相同）：

   - 托管区：eu.hr.example.com NS IP：10.0.0.30

```
$TTL    86400 ; 24 hours
$ORIGIN eu.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. 对于亚洲本地区域中的本地名称服务器：

   托管区：apac.hr.example.com、10.0.0.40

   APAC 名称服务器可以将子域委托给其他名称服务器。

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
```

```
test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

托管区：engineering.apac.hr.example.com、10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. 对于北美洲本地区域中的本地名称服务器：

   托管区：na.hr.example.net NS IP：10.0.0.50

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

VPC 解析器设置

- 对于 VPC 解析器，您需要设置转发规则和委托规则：

  转发规则

  1. 对于转发初始请求，以便将查询转发到位于中心位置的父托管区 hr.example.com：

     domain-name：hr.example.com target-ips：10.0.0.20

  2. 为了转发 out-of-zone委派记录，让 VPC 解析器知道委托域名服务器的 IP 地址来转发初始请求：

     domain-name：hr.example.net target-ips：10.0.0.50

委托规则

1. 区域内委托的委托规则：

   委托记录：`hr.example.com`
2. 区域外委托的委托规则：

   委托记录：`hr.example.net`

在 Amazon Route 53 中启用 DNSSEC 验证

当您在 Amazon Route 53 中为 Virtual Private Cloud (VPC) 启用 DNSSEC 验证时，会对 DNSSEC 签名进行加密检查，以确保响应未被篡改。您可以在 VPC 详细信息页面上启用 DNSSEC 验证。

VPC 解析器在执行递归 DNS 解析时将 DNSSEC 验证应用于公共签名名称。

但是，如果 VPC 解析器转发到其他 DNS 解析器，则该解析器正在执行递归 DNS 解析，因此还必须应用 DNSSEC 验证。

> **Important**
>
> 启用 DNSSEC 验证可能会影响 VPC 中 Amazon 资源的公有 DNS 记录的 DNS 解析，这可能导致中断。注意，启用或禁用 DNSSEC 验证可能耗时数分钟。

> **Note**
>
> 目前，您的 VPC（又名 AmazonProvided DNS）中的 Route 53 VPC 解析器会忽略 DNS 查询中的 DO（DNSSEC OK）EDNS 标头位和 CD（检查已禁用）位。如果您已配置 DNSSEC，则这意味着虽然 VPC 解析器确实执行 DNSSEC 验证，但它不会返回 DNSSEC 记录，也不会在响应中设置 AD 位。因此，VPC 解析器目前不支持您自己执行 DNSSEC 验证。如果需要进行自己的 DNSSEC 验证，您必须执行自己的递归 DNS 解析。

要为 VPC 启用 DNSSEC 验证

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 在导航窗格中的 VPC 解析器下，选择VPCs。
3. 在 DNSSEC 验证下，选中复选框。如果已选中该复选框，则可以清除该复选框以禁用 DNSSEC 验证。

   注意，启用或禁用 DNSSEC 验证可能耗时数分钟。

将互联网流量路由到您的 Amazon 资源

您可以使用 Amazon Route 53 将流量路由到各种 Amazon 资源。

- 使用域名将流量路由到 Amazon API Gateway API
- 使用您的域名将流量路由到 Amazon CloudFront 分配
- 将流量路由到 Amazon EC2 实例
- 将流量路由到 Amazon App Runner 服务
- 将流量路由到 Amazon Global Accelerator
- 将流量路由到 Amazon Elastic Beanstalk 环境
- 将流量路由到 ELB 负载均衡器
- 将流量路由到在 Amazon S3 存储桶中托管的网站
- 使用域名将流量路由到 Amazon Virtual Private Cloud 接口终端节点
- 将流量路由到 Amazon WorkMail
- 将流量路由到亚马逊 OpenSearch 服务域终端节点
- 将流量路由到 Amazon VPC Lattice 服务域端点
- 将流量路由到其他 Amazon 资源
- 使用创建 Amazon Route 53 和 Route 53 VPC 解析器资源 Amazon CloudFormation

使用域名将流量路由到 Amazon API Gateway API

您可以使用 Amazon API Gateway 来创建、发布、维护、监控和保护 APIs。除了存储在 Amazon 云中的数据外APIs ，您还可以创建访问 Amazon 服务或其他 Web 服务。

用于将域流量路由到 API Gateway API 的方法取决于您创建的是区域 API Gateway 终端节点，还是边缘优化的 API Gateway 终端节点。如果您创建私有 API Gateway 端点，则过程略有不同。

- 区域 API 端点：您创建将流量路由到区域 API 端点的 Route 53 别名记录。
- 边缘优化的 API 端点：您创建将流量路由到边缘优化 API 的 Route 53 别名记录。这会导致流量被路由到与边缘优化 API 关联的 CloudFront 分发。
- 私有 API 端点：您创建一个 Route 53 别名记录，该记录使用私有托管区中 API Gateway 的接口 VPC 端点将流量路由到您的私有 API 端点。

别名记录是对 DNS 的 Route 53 扩展，类似于 CNAME 记录。有关别名记录和 CNAME 记录的比较，请参阅在别名记录和非别名记录之间进行选择。

> **Note**
>
> Route 53 不对对 API Gateway APIs 或其他 Amazon 资源的别名查询收费。

主题

先决条件

要开始使用，您需要满足以下条件：

- 具有自定义域名的 API Gateway API（如 api.example.com），此域名与您要创建的 Route 53 记录的名称匹配。

  有关更多信息，请参阅以下主题：

  - APIs在《亚马逊 API Gateway 开发者指南》中@@ 为 HTTP 设置自定义域名。
  - 在 Amazon API Gateway 开发者指南 APIs中@@ 为 REST 设置自定义域名。
  - 在 Amazon API Gateway 开发者指南 WebSocket APIs中@@ 设置自定义域名。
  - 亚马逊 API Gateway 开发者指南 APIs 中的 API Gatewa y 中私有域名的自定义域名。
- 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其他注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

配置 Route 53 以将流量路由到 API Gateway 终端节点

要配置 Route 53 以将流量路由到 API Gateway 终端节点，请执行以下过程。

Custom domain names for public APIs

以下过程介绍如何将流量路由到 API Gateway 终端节点，以获取公共自定义域名 APIs。

将流量路由到 API Gateway 端点

1. 如果您使用相同账户创建了 Route 53 托管区和端点，请跳到步骤 2。

   如果您使用不同账户创建了托管区和端点，请获取您要使用的自定义域名的目标域名：

   a. 登录 Amazon Web Services 管理控制台 并打开 API Gateway 控制台，网址为https://console.aws.amazon.com/apigateway/。
   b. 在导航窗格中，选择自定义域名。
   c. 选择您希望使用的自定义域名，并获取 API Gateway 域名的值。
2. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 选择具有要用于将流量路由到 API 的域名的托管区域的名称。
5. 选择创建记录。
6. 指定以下值：

   > **Important**
   > 建议开启别名。对于未使用 Route 53 别名记录的域名，如果您使用的 VPC 启用了私有 DNS 来调用私有 API，则可能会遇到问题。私有 DNS 会覆盖 VPC 中的默认 DNS 解析行为，这可能会导致与外部 DNS 记录发生冲突。

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

   记录名称

   输入要用于将流量路由到 API 的域名。

   您要将流量路由到的 API 必须包含自定义域名（如 api.example.com），此域名与您要创建的 Route 53 记录的名称匹配。

Alias

如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

值/流量路由至

选择 Alias to API Gateway API（API Gateway API 的别名），然后选择终端节点所在的区域。

如何指定 E ndpoint 的值取决于您是使用相同的 Amazon 账户还是不同的账户创建托管区域和 API：

- 相同账户-目标域名列表仅 APIs 包括自定义域名与您为记录名称指定的值相匹配的域名。选择适用的值。
- 不同账户 - 输入您在此过程的步骤 1 中获得的值。

记录类型

选择 A — IPv4 地址。

评估目标运行状况

要控制 DNS 故障转移，请配置自定义运行状况检查。有关示例，请参阅 API Gateway user guide（《API Gateway 用户指南》）中的 Configure custom health checks for DNS failover（为 DNS 故障转移配置自定义运行状况检查）。

7. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到 API。

Custom domain names for private APIs

以下过程介绍如何将流量路由到私有自定义域名的 API Gateway 终端节点 APIs。

将流量路由到 API Gateway 端点

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择具有要用于将流量路由到 API 的域名的私有托管区的名称。
4. 选择创建记录。
5. 指定以下值：

路由策略

选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

记录名称

输入要用于将流量路由到 API 的域名。

您要将流量路由到的 API 必须包含自定义域名（如 api.example.com），此域名与您要创建的 Route 53 记录的名称匹配。

Alias

开启别名。

值/流量路由至

选择 VPC 端点的别名。选择端点所在的区域，然后选择 VPC 端点。

记录类型

如果您使用 IPv6 您的 VPC 终端节点，请创建 AAAA 记录类型。如果您为 VPC 端点使用双堆栈，请创建 AAAA 和 A 记录类型。

评估目标运行状况

要控制 DNS 故障转移，请配置自定义运行状况检查。有关示例，请参阅 API Gateway user guide（《API Gateway 用户指南》）中的 Configure custom health checks for DNS failover（为 DNS 故障转移配置自定义运行状况检查）。

6. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到 API。

使用您的域名将流量路由到 Amazon CloudFront 分配

本主题提供了将 DNS 流量路由到任何 Amazon CloudFront 分发的全面程序。如果您要使用 Amazon CloudFront 和 Amazon 简单存储服务设置静态网站，请查看使用 Amazon CloudFront 发行版为静态网站提供服务完整教程。

您可以使用 Amazon CloudFront（ Amazon 内容分发网络 (CDN)）作为加快网络内容交付速度的一种方式。 CloudFront 可以使用全球边缘站点网络交付您的整个网站，包括动态、静态、流媒体和交互式内容。请求内容的用户将自动路由到可为用户提供最低延迟的边缘站点。

> **Note**
>
> 您只能将流量路由到公共托管区域的 CloudFront 分配。

CloudFront 要用于分发您的网站内容，请创建一个分配并为其指定设置。例如，指定 CloudFront要从中获取内容的 Amazon S3 存储桶或 HTTP 服务器，是否只允许选定的用户访问您的内容，以及是否希望用户使用 HTTPS。

创建分配时， CloudFront 会为该分配分配分配分配一个域名，例如d111111abcdef8.cloudfront.net。您可以在中为您的内容使用此域名，例如：URLs

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

或者，您可以在中使用自己的域名 URLs，例如：

```
http://example.com/logo.jpg
```

按照《Amazon CloudFront 开发者指南》中的步骤，在分配的文件 URLs 中使用您自己的域名，而不是 CloudFront 分配给您的 CloudFront 分配的域名。有关在 CloudFront分配中使用自己的域名的更多信息，请参阅 URLs 通过添加备用域名使用自定义 (CNAMEs)。

当您在 CloudFront 分配中使用 Route 53 域名时，请使用 Amazon Route 53 创建指向您的 CloudFront 分配的别名记录。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，但您既可以为根域 (如 example.com) 又可以为子域 (如 www.example.com) 创建别名记录。(只能为子域创建 CNAME 记录。) 当 Route 53 收到与别名记录的名称和类型均匹配的 DNS 查询时，Route 53 将用与您的分配关联的域名来响应。

> **Note**
>
> Route 53 不对 CloudFront 分配或其他 Amazon 资源的别名查询收费。

先决条件

要开始使用，您需要满足以下条件：

1. 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其他注册商。
2. Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

   有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。
3. CloudFront 分发租户或分 CloudFront 销租户。分配必须包含一个备用域名，该域名必须与您要用于您的分配的域名相匹配， URLs 而不是与 CloudFront 分配给您的分配的域名相匹配。对于 CloudFront 分发租户，它必须包含您要用于的域名 URLs。

   例如，如果您希望内容包含域名 e xample.com，则分配的 “备用域名” 字段必须包含 example.com。 URLs

   有关更多信息，请参阅《Amazon CloudFront 开发者指南》中的以下文档：

   - 创建分配的任务列表
   - 使用 CloudFront控制台创建或更新分配

   > **Note**
   >
   > 如果您要创建静态网站，请参阅《亚马逊 CloudFront 开发者指南》中的安全静态网站入门，了解完整的设置说明。
4. （可选）申请公共证书，以便亚马逊 CloudFront 分配需要 HTTPS。有关更多信息，请参阅 Amazon Certificate Manager 用户指南中的 Amazon Certificate Manager中的 DNS 验证。

将 Amazon Route 53 配置为将流量路由到分 CloudFront 配

要将 Amazon Route 53 配置为将流量路由到 CloudFront 分配，请按照以下步骤操作。有关在 CloudFront分配中使用自己的域名的更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的 URLs 通过添加备用域名使用自定义域名 (CNAMEs)。

> **Note**
>
> 更改通常在 60 秒内传播到所有 Route 53 服务器。当更改传播时，您将能够使用在此过程中创建的别名记录的名称将流量路由到您的 CloudFront 分配。

将流量路由到分CloudFront 配

1. 获取 CloudFront 分配给您的分配的域名并确定 IPv6 是否已启用：

   a. 登录 Amazon Web Services 管理控制台 并打开 CloudFront 控制台，网址为https://console.amazonaws.cn/cloudfront/v4/home。

   b. 在 ID 列中，选择要向其路由流量的分配的关联名称（而不是复选框）。

   c. 在 General（常规）选项卡上，获取 Distribution Domain name（分配域名）字段的值。

   d. 在 “常规” 选项卡的 “设置” 部分，选择 “编辑”，然后滚动查看该IPv6字段以查看该分配 IPv6 是否已启用。如果 IPv6 启用，则需要为分配创建两个别名记录，一个用于将 IPv4流量路由到分配，另一个用于路由 IPv6 流量。选择取消。

      有关更多信息，请参阅《亚马逊 CloudFront 开发者指南》 IPv6中您在创建或更新分配时指定的值主题中的启用。

2. 对于分 CloudFront 销租户，

   a. 在左侧导航栏中选择 SaaS，然后选择分配租户，接下来选择带有您要将流量路由到其中的域名的分配租户

   b. 在常规详细信息部分中，复制端点的值。

3. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

4. 在导航窗格中，选择 Hosted zones（托管区域）。

5. 为要用于将流量路由到 CloudFront 分配的域名选择托管区域的链接名称。

6. 选择创建记录。

7. 指定以下值：

   记录名称

   输入您要用于将流量路由到您的 CloudFront 分配的域名。默认值为托管区的名称。

   例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的分配，请输入 acme。

   记录类型

   选择 A — IPv4 地址。

   如果已 IPv6 为分发启用并且您正在创建第二条记录，请选择 AAAA — IPv6 地址。

Alias

开启别名。

> **Important**
>
> 您必须创建别名记录才能使 CloudFront 分配生效。

将流量路由到

选择 “ CloudFront 分发别名”。选择在创建 CloudFront 分配时分配给分配的域名。这是您在第 1 步中获得的值。

对于 CloudFront 分发租户，请从步骤 2 中选择终端节点。

评估目标运行状况

接受默认值否。

路由策略

选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

8. 选择创建记录。
9. 如果已 IPv6 为分发启用，请重复步骤 5 到 7。对除记录类型字段外的其余字段指定相同设置，如步骤 6 中所述。

将流量路由到 Amazon EC2 实例

Amazon 在 Amazon 云端 EC2 提供可扩展的计算容量。您可以使用预配置的模板（Amazon 系统映像或 AMI）启动 EC2 虚拟计算环境（实例）。启动 EC2 实例时， EC2 会自动安装操作系统（Linux 或 Microsoft Windows）和 AMI 中包含的其他软件，例如 Web 服务器或数据库软件。

如果您在实例上托管网站或运行 Web 应用程序，则可以使用 Amazon Route 53 将域名（例如 example.com）的流量路由到您的服务器。 EC2

先决条件

要开始使用，您需要满足以下条件：

- 一个亚马逊 EC2 实例。有关启动 EC2 实例的信息，请参阅以下文档：

- Linux — 请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 Linux 实例入门
- 微软 Windows — 参见亚马逊 EC2 用户指南中的亚马逊 EC2 Windows 实例入门

> **Important**
>
> 我们建议您同时创建弹性 IP 地址并将其与您的 EC2实例关联。弹性 IP 地址可确保您的 Amazon EC2 实例的 IP 地址永远不会更改。有关定价的信息，请参阅弹性 IP 地址定价。

- 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其他注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

将 Amazon Route 53 配置为将流量路由到亚马逊 EC2 实例

要将 Amazon Route 53 配置为将流量路由到 EC2 实例，请执行以下步骤。

将流量路由到 Amazon EC2 实例

1. 获取 Amazon EC2 实例的 IP 地址：
   a. 登录 Amazon Web Services 管理控制台 并打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
   b. 在控制台右上角的“区域”列表中，选择您启动实例所在的区域。
   c. 在导航窗格中，选择 Instances (实例)。
   d. 在表中，选择要向其路由流量的实例。
   e. 在底部窗格的描述选项卡上，获取 Elastic 的值 IPs。

      如果您没有将弹性 IP 与实例关联，则获取 IPv4 Public IP 的值。
2. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 选择与您要路由其流量的域的名称相符的托管区域的名称。
5. 选择创建记录。
6. 指定以下值：

路由策略

选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

记录名称

输入您要用于将流量路由到您的 EC2 实例的域名。默认值为托管区的名称。

例如，如果托管区域的名称为 example.com，并且您想使用 acme.example.com 将流量路由到您的实例，请输入 acme。 EC2

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值）。输入您在第 1 步中获得的 IP 地址。

记录类型

选择 A — IPv4 地址。

TTL (秒)

接受默认值 300。

7. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此过程中创建的记录的名称将流量路由到您的 EC2 实例。

> **Important**
>
> 如果您释放弹性 IP，请确保同时删除指向它的 DNS 记录。如果不这样做，则会有一条悬挂 DNS 记录可以被未经授权的用户接管。

将流量路由到 Amazon App Runner 服务

Amazon App Runner 是一项完全托管的服务，可让开发人员轻松大规模部署容器化 Web 应用程序，APIs 无需事先具备基础架构经验。从源代码或容器镜像开始。App Runner 会自动构建和部署 Web 应用程序，通过加密实现流量负载平衡，扩展以满足您的流量需求，并使您的服务可以轻松地与在私有 Amazon VPC 中运行的其他 Amazon 服务和应用程序进行通信。使用 App Runner 时，您无需考虑服

务器或扩展，而是有更多时间专注于应用程序。有关更多信息，请参阅《Amazon App Runner 开发人员指南》中的什么是 Amazon App Runner。

> **Important**
>
> 亚马逊 Route 53 目前支持 2022 年 8 月 1 日之后创建的 Amazon App Runner 服务的别名记录。

要将域流量路由至 App Runner 服务，请使用 Amazon Route 53 创建一个指向 App Runner 服务的别名记录。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，除了您既可以为根域（如 example.com）又可以为子域（如 www.example.com（http://www.example.com/））创建别名记录。只能为子域创建 CNAME 记录。

> **Note**
>
> 对于针对 App Runner 服务或其他 Amazon 资源的别名查询，Route 53 不收费。

先决条件

要开始使用，您需要满足以下条件：

- App Runner 服务。有关创建 App Runner 服务的信息，请参阅 App Runner 入门。
- 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其它注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。
- 将自定义域关联到 App Runner 服务。有关更多信息，请参阅 Managing custom domain names for App Runner（管理 App Runner 服务的自定义域名）。
- 配置 App Runner 返回给 Route 53 托管区的证书验证记录以启动域验证过程。有关更多信息，请参阅 Amazon Certificate Manager 用户指南中的 Amazon Certificate Manager中的 DNS 验证。

配置 Amazon Route 53 以将流量路由到 App Runner 服务

要配置 Amazon Route 53 以将流量路由到 App Runner 服务，请执行以下过程。

将流量路由到 App Runner 服务

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择与您要路由其流量的域的名称相符的托管区域的名称。
4. 选择创建记录。
5. 指定以下值：

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

   记录名称

   输入要用于将流量路由到 App Runner 服务的域名。默认值为托管区的名称。

   例如，如果托管区的名称为 example.com，并且您要使用 acme.example.com 将流量路由到 App Runner 服务，请输入 acme。

   值/流量路由至

   选择 Alias to App Runner Service（App Runner 服务的别名），然后选择 Amazon Web Services 区域。选择要向其路由流量的环境的域名。

   记录类型

   接受默认值 A — IPv4 地址。

   评估目标运行状况

   选择否。 有关评估目标运行状况的信息，请参阅 Evaluate Target Health。
6. 选择创建记录。

   更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到 App Runner 服务。

将流量路由到 Amazon Global Accelerator

Amazon Global Accelerator 是一项服务，您可以在其中创建加速器以提高本地和全球用户的应用程序性能。该服务会立即对运行状况或配置的变化做出反应，以确保来自客户端的互联网流量始终引导至运行状况良好的端点。Global Accelerator 包括容错架构 Amazon Shield Standard，并集成了容错架构，用于自动在线缓解 DDo S 攻击。有关更多信息，请参阅《 Amazon Global Accelerator 开发者指南》中的什么是全球加速。

默认情况下，Global Accelerator 为您提供与加速器关联的静态 IP 地址。静态 IP 地址是来自 Amazon 边缘网络的任意广播。加速器包括默认 DNS 名称，但在大多数情景中，您都可以将 DNS 配置为在加速器中使用您的自定义域（例如 www.example.com），而非所分配的静态 IP 地址或默认 DNS 名称。

> **Note**
>
> 对于针对 Global Accelerator 或其他 Amazon 资源的别名查询，Route 53 不收费。

先决条件

要开始使用，您需要满足以下条件：

- 加速器。您可以创建标准加速器，也可以创建自定义路由加速器。有关更多信息，请参阅创建标准加速器和创建自定义路由加速器。
- 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其它注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

配置 Amazon Route 53 以将流量路由到加速器

要配置 Amazon Route 53 以将流量路由到加速器，请执行以下过程。

将流量路由到加速器

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择与您要路由其流量的域的名称相符的托管区域的名称。
4. 选择创建记录。
5. 指定以下值：

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

   记录名称

   输入要用于将流量路由到加速器的域名。默认值为托管区的名称。

   例如，如果托管区的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的 Global Accelerator，请输入 acme。

   值/流量路由至

   选择 Global Accelerator 的别名，然后选择 Amazon Web Services 区域。选择加速器的 DNS 名称。

   您可以为使用当前 Amazon Web Services 账户 或使用另一个 Amazon Web Services 账户创建的加速器输入 DNS 名称。

   记录类型

   接受默认值 A — IPv4 地址。

   评估目标运行状况

   接受默认值 Yes（是）。
6. 选择创建记录。

   更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到加速器。

将流量路由到 Amazon Elastic Beanstalk 环境

如果您使用 Amazon Elastic Beanstalk 在 Amazon 云中部署和管理应用程序，则可以使用 Amazon Route 53 将您的域（例如 example.com）的 DNS 流量路由到新的或现有的 Elastic Beanstalk 环境。

要将 DNS 流量路由到 Elastic Beanstalk 环境，请参阅以下主题中的步骤。

> **Note**
>
> 这些步骤假定您已经使用 Route 53 作为您的域的 DNS 服务。如果您正在使用其它 DNS 服务，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务，以了解有关将 Route 53 用作域的 DNS 服务提供商的信息。

主题

将应用程序部署到 Elastic Beanstalk 环境

如果您已有要将流量路由到的 Elastic Beanstalk 环境，请跳到 获取 Elastic Beanstalk 环境的域名。

创建应用程序并将其部署到 Elastic Beanstalk 环境中

- 有关创建应用程序并将其部署到 Elastic Beanstalk 环境的信息，请参阅 Amazon Elastic Beanstalk 开发人员指南中的开始使用 Elastic Beanstalk。

获取 Elastic Beanstalk 环境的域名

如果您已经了解 Elastic Beanstalk 环境的域名，请跳到创建将流量路由到 Elastic Beanstalk 环境的 Amazon Route 53 记录。

获取 Elastic Beanstalk 环境的域名

1. 登录 Amazon Web Services 管理控制台 并打开 Elastic Beanstalk 控制台，网址为。https://console.aws.amazon.com/elasticbeanstalk/
2. 在应用程序列表中，找到要向其路由流量的应用程序，并获取 URL 的值。如果您未看到应用程序列表，请在导航窗格中选择 Applications（应用程序）。

   有关 URL 的更多信息，请参阅 Elastic Beanstalk 开发人员指南中的 Elastic Beanstalk 环境的域名。

创建将流量路由到 Elastic Beanstalk 环境的 Amazon Route 53 记录

Amazon Route 53 记录包含用于控制如何将流量路由到 Elastic Beanstalk 环境的设置。您可以创建 CNAME 记录或别名记录，具体取决于环境的域名是否包含部署环境所在的区域，例如，us-east-2。新环境在域名中包含区域；2016 年年初之前创建的环境则不包含。有关 CNAME 与别名记录的比较，请参阅在别名记录和非别名记录之间进行选择。

如果域名不包括区域

您必须创建 CNAME 记录。但是，由于 DNS 施加的限制，您只能为子域（而不是根域名称）创建别名记录 (CNAME)。例如，如果您的域名为 example.com，则可创建一个能将 acme.example.com 的流量路由到 Elastic Beanstalk 环境的记录，但不能创建可将 example.com 的流量路由到 Elastic Beanstalk 环境的记录。

请参阅创建 CNAME 记录以将流量路由到 Elastic Beanstalk 环境 过程。

如果域名包括区域

您可以创建别名记录。别名记录特定于 Route 53，与 CNAME 记录相比有两个重要优势：

- 您可以为根域名或子域创建别名记录。例如，如果域名为 example.com，则可创建能够将对 example.com 或 acme.example.com 的请求路由到 Elastic Beanstalk 环境的记录。
- Route 53 不对使用别名记录来路由流量的请求收费。

请参阅创建 Amazon Route 53 别名记录以将流量路由到 Elastic Beanstalk 环境 过程。

创建 CNAME 记录以将流量路由到 Elastic Beanstalk 环境

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要用于将流量路由到 Elastic Beanstalk 环境的托管区域的名称。
4. 选择创建记录。
5. 选择切换以快速创建
6. 指定以下值：

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

记录名称

输入要用于将流量路由到 Elastic Beanstalk 环境的域名。默认值为托管区的名称。

例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的环境，请输入 acme。

> **Important**
> 您不能创建与托管区域同名的 CNAME 记录。

Alias

如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

值/流量路由至

选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值），然后输入您在主题 获取 Elastic Beanstalk 环境的域名 中执行过程时获取的值。如果您使用了不同账户来创建您的 Route 53 托管区域和 Elastic Beanstalk 环境，请输入 Elastic Beanstalk 环境的 CNAME 属性。

记录类型

选择 CNAME。

TTL（秒）

接受默认值 300。

7. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。

创建 Amazon Route 53 别名记录以将流量路由到 Elastic Beanstalk 环境

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要用于将流量路由到 Elastic Beanstalk 环境的托管区域的名称。
4. 选择创建记录。

5. 指定以下值：

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

   记录名称

   输入要用于将流量路由到 Elastic Beanstalk 环境的域名。默认值为托管区的名称。

   例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的环境，请输入 acme。

   值/流量路由至

   选择 Alias to Elastic Beanstalk environment（Elastic Beanstalk 环境的别名），然后选择终端节点所在的区域。选择要向其路由流量的环境的域名。这是您在执行主题获取 Elastic Beanstalk 环境的域名中的过程时获取的值。

   如果您使用了不同账户来创建您的 Route 53 托管区域和 Elastic Beanstalk 环境，请输入 Elastic Beanstalk 环境的 CNAME 属性。

   记录类型

   接受默认的 A — IPv4 地址。

   评估目标运行状况

   接受默认值 Yes（是）。

6. 选择创建记录。

   更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到 Elastic Beanstalk 环境。

将流量路由到 ELB 负载均衡器

如果您在多个 Amazon EC2 实例上托管网站，则可以使用 Elastic Load Balancing (ELB) 负载均衡器将流量分配到多个实例。当网站的流量随时间发生变化时，ELB 服务可自动缩放负载均衡器。负载均衡器还会监控其已注册实例的运行状况，并且只将域流量路由到运行状况良好的实例。

要将域流量路由至 ELB 负载均衡器，请使用 Amazon Route 53 创建一个指向负载均衡器的别名记录。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，但您既可以为根域 (如

example.com) 又可以为子域 (如 www.example.com) 创建别名记录。(只能为子域创建 CNAME 记录。)

> **Note**
>
> 对于针对 ELB 负载均衡器或其它 Amazon 资源的别名查询，Route 53 不收费。

先决条件

要开始使用，您需要满足以下条件：

- 一个 ELB 负载均衡器。您可以使用 ELB 经典负载均衡器、Application Load Balancer 或 Network Load Balancer。有关创建负载均衡器的信息，请参阅 Elastic Load Balancing 用户指南中的 Elastic Load Balancing 入门。

  为负载均衡器命名，以便将来能够想起它的用途。您在创建负载均衡器时指定的名称是您在 Route 53 控制台中创建别名记录时将选择的名称。
- 注册的域名。您可以使用 Route 53 作为您的域注册商，也可以使用其它注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

配置 Amazon Route 53 以将流量路由到 ELB 负载均衡器

要配置 Amazon Route 53 以将流量路由到 ELB 负载均衡器，请执行以下过程。

将流量路由到 ELB 负载均衡器

1. 如果您使用相同账户创建 Route 53 托管区域和 ELB 负载均衡器，请跳到步骤 2。

   如果您使用不同的账户创建托管区域和 ELB 负载均衡器，请执行获取 Elastic Load Balancing 负载均衡器的 DNS 名称中的步骤，以获取负载均衡器的 DNS 名称。
2. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。

4. 选择具有要用于将流量路由到负载均衡器的域名的托管区域的名称。
5. 选择创建记录。
6. 指定以下值：

路由策略

选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

记录名称

输入要用于将流量路由到 ELB 负载均衡器的域名或子域名。默认值为托管区的名称。

例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到负载均衡器，请输入 acme。

Alias

如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

值/流量路由至

选择 Alias to Application and 经典负载均衡器 （Application Load Balancer 和经典负载均衡器的别名）或 Alias to Network Load Balancer（网络负载均衡器的别名），然后选择终端节点所在的区域。

如果您使用相同的 Amazon 账户创建了托管区域和 ELB 负载均衡器，请选择您在创建负载均衡器时为其分配的 DNS 名称。

如果您使用不同账户创建托管区域和 ELB 负载均衡器，请输入您在此过程的步骤 1 中获取的值。

> **Note**
>
> 控制台在双栈前面加上双重堆栈。 仅限于来自同一个 Amazon 账户的应用程序和 Classic Load Balancer 的 DNS 名称。当客户端（例如网络浏览器）请求您的域名 (example.com) 或子域名 (www.example.com) 的 IP 地址时，客户端可以请求地址（A 记录）、 IPv4 地址（AAAA 记录）或两者兼而有之， IPv4 并 IPv6 请求 IPv6地址（在单独的请求中，先请求一个）。 IPv4 dualstack. 标识让 Route 53 能够基于客户端所请求的 IP 地址格式使用您的负载均衡器的相应 IP 地址进行响应。您需要为来自不同账户的 Application Load Balancer 和经典负载均衡器添加 dualstack. 前缀。

记录类型

选择 A — IPv4 地址。

评估目标运行状况

如果您希望 Route 53 根据资源的运行状况路由流量，请选择 Yes（是）。有关检查资源运行状况的更多信息，请参阅创建 Amazon Route 53 运行状况检查 。

7. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到负载均衡器。

将流量路由到在 Amazon S3 存储桶中托管的网站

本主题提供将 DNS 流量路由到为静态网站托管配置的任何 Amazon Simple Storage Service 存储桶的全面过程。如果您要使用 Amazon Simple Storage Service 来设置静态网站，请参阅 将您的域用于 Amazon S3 存储桶中的静态网站 以获取完整的教程。

Amazon Simple Storage Service (Amazon S3) 提供安全、持久、高度可扩展的云存储。您可以配置 S3 桶，以托管能够包含网页和客户端脚本的静态网站。(S3 不支持服务器端脚本编写。)

要将域流量路由至 S3 存储桶，请使用 Amazon Route 53 创建一个指向存储桶的别名记录。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，除了您既可以为根域 (如 example.com) 又可以为子域 (如 www.example.com) 创建别名记录。只能为子域创建 CNAME 记录。

> **Note**
>
> 对于针对 S3 存储桶或其它 Amazon 资源的别名查询，Route 53 不收费。

先决条件

要开始使用，您需要满足以下条件：

- 配置用于托管静态网站的 S3 存储桶。

  有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的教程：使用注册到 Route 53 的自定义域配置静态网站。

> **Important**
>
> 该存储桶必须与您的域或子域同名。例如，如果您要使用子域 acme.example.com，存储桶的名称必须为 acme.example.com。

您可以将某个域及其子域 (例如 example.com 和 www.example.com) 的流量路由到单个存储桶。为域和每个子域创建一个存储桶，并将除了其中一个存储桶之外的所有存储桶配置为将流量重定向到剩余的存储桶。

> **Note**
>
> 配置为网站终端节点的 S3 存储桶不支持 SSL/TLS，因此您需要将流量路由到 CloudFront 分配并使用 S3 存储桶作为分配的来源。
> 有关如何创建 CloudFront 分配的说明，请参阅使用您的域名将流量路由到 Amazon CloudFront 分配。

- 注册的域名。您可以使用 Route 53 作为您的域注册商，也可以使用其它注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

配置 Amazon Route 53 以将流量路由到 S3 存储桶

要配置 Amazon Route 53 以将流量路由到配置为托管静态网站的 S3 存储桶，请执行以下过程。

将流量路由到 S3 存储桶

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择具有要用于将流量路由到 S3 存储桶的域名的托管区域的名称。
4. 选择创建记录。
5. 指定以下值：

记录名称

输入要用于将流量路由到 S3 存储桶的域名。默认值为托管区的名称。

例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的存储桶，请输入 acme。

记录类型

选择 A — IPv4 地址。

Alias

开启别名。

将流量路由到

选择 Alias to S3 website endpoint（S3 网站终端节点的别名），然后选择终端节点所在的区域。

选择与您为 Record name（记录名称）指定的名称相同的存储桶。

仅在存储桶符合以下要求时，该列表才包含存储桶：

- 存储桶名称与您正在创建的记录的名称相同。
- 存储桶配置为网站终端节点。
- 当前 Amazon 账户创建的存储桶。

  如果您使用了不同的 Amazon 账户创建存储桶，输入您在其中创建 S3 存储桶的区域的名称。有关区域名称的正确格式，请参阅《Amazon Web Services 一般参考》中 Amazon S3 网站端点表的网站端点列。

评估目标运行状况

选择否。 有关评估目标运行状况的信息，请参阅 Evaluate Target Health。

路由策略

选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

6. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此步骤中创建的别名记录的名称将流量路由到 S3 存储桶。

使用域名将流量路由到 Amazon Virtual Private Cloud 接口终端节点

您可以使用 Amazon PrivateLink 通过亚马逊虚拟私有云 (Amazon VPC) 接口终端节点访问所选服务。这些服务包括一些 Amazon 服务、由其他 Amazon 客户和合作伙伴自己 VPCs托管的服务以及支持的 Amazon Web Services Marketplace 合作伙伴服务。

要将域流量路由到接口终端节点，请使用 Amazon Route 53 创建别名记录。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，但您既可以为根域 (如 example.com) 又可以为子域 (如 www.example.com) 创建别名记录。只能为子域创建 CNAME 记录。

> **Note**
>
> Route 53 不对接口终端节点或其他 Amazon 资源的别名查询收费。

主题

先决条件

要开始使用，您需要满足以下条件：

- 一个 Amazon VPC 接口终端节点。有关更多信息，请参阅《Amazon VPC 用户指南》中的接口 VPC 端点 (Amazon PrivateLink)。
- 注册的域名。您可以使用 Amazon Route 53 作为您的域注册商，也可以使用其它注册商。
- Route 53 用作域的 DNS 服务。如果您使用 Route 53 注册域名，我们会自动将 Route 53 配置为该域的 DNS 服务。

  有关将 Route 53 用作域的 DNS 服务提供商的信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。

配置 Amazon Route 53 以将流量路由到 Amazon VPC 接口终端节点

要配置 Amazon Route 53 以将流量路由到 Amazon VPC 接口终端节点，请执行以下过程。

将流量路由到 Amazon VPC 接口终端节点

1. 如果您使用相同账户创建了 Route 53 托管区域和 Amazon VPC 终端节点，请跳到步骤 2。

   如果您使用不同的账户创建了托管区域和接口终端节点，请获取接口终端节点的服务名称：

   a. 登录 Amazon Web Services 管理控制台 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
   b. 在导航窗格中，选择端点。
   c. 在右窗格中，选择要向其路由 Internet 流量的终端节点。
   d. 在底部窗格中，获取 DNS 名称的值，例如，vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com。
2. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Hosted zones（托管区域）。
4. 选择具有要用于将流量路由到接口终端节点的域名的托管区域的名称。
5. 选择创建记录。
6. 指定以下值：

   路由策略

   选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

   记录名称

   输入要用于将流量路由到 Amazon VPC 接口终端节点的域名。

   Alias

   如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

   值/流量路由至

   选择 Alias to VPC endpoint（VPC 终端节点的别名），然后选择终端节点所在的区域。

   如何指定 Endpoints 的值取决于您是使用相同的 Amazon 账户还是不同的账户创建托管区域和接口终端节点：

   - 相同账户 - 选择列表，并找到类别 Amazon VPC endpoints（Amazon VPC 终端节点）。然后，选择您要将 Internet 流量路由到的接口终端节点的 DNS 名称。
   - 不同账户 - 输入您在此过程的步骤 1 中获得的值。

记录类型

选择 A — IPv4 地址。

评估目标运行状况

选择否。 有关评估目标运行状况的信息，请参阅 Evaluate Target Health。

7. 选择创建记录。

更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您将能够使用在此过程中创建的别名记录的名称将流量路由到接口终端节点。

将流量路由到 Amazon WorkMail

您可以使用 Route 53 将流量路由到您的 Amazon WorkMail 电子邮件域。您的 Route 53 托管区域（例如 example.com）的名称必须与亚马逊 WorkMail 域名的名称相匹配。

> **Note**
>
> 您只能将流量路由到公共托管区域的 Amazon WorkMail 域。

要将流量路由到 Amazon WorkMail，请执行以下四个步骤。

将 Amazon Route 53 配置为你的 DNS 服务并添加亚马逊 WorkMail 组织和电子邮件域

1. 如果您尚未注册要在电子邮件地址 (如 john@example.com) 中使用的域名，请立即注册域，以便知道域是否可用。有关更多信息，请参阅 注册新域。

   如果 Amazon Route 53 不是您添加到亚马逊的电子邮件域的 DNS 服务 WorkMail，请将该域的 DNS 服务迁移到 Route 53。有关更多信息，请参阅 将 Amazon Route 53 作为现有域的 DNS 服务。
2. 添加 Amazon WorkMail 组织和电子邮件域。有关更多信息，请参阅 Amazon WorkMail 管理员指南中的新用户入门。

为亚马逊创建 Route 53 TXT 记录 WorkMail

1. 在 Amazon WorkMail 控制台的导航窗格中，选择域名。
2. 选择要用于将流量路由到亚马逊的电子邮件域名，例如 example.com。 WorkMail

3. 打开另一个浏览器选项卡，然后打开 Route 53 控制台。
4. 在 Route 53 控制台中，执行以下操作：
   a. 在导航窗格中，选择 Hosted zones（托管区域）。
   b. 选择您要用于 Amazon WorkMail 电子邮件域的托管区域的名称。
5. 在 Amazon WorkMail 控制台的 “步骤 1：验证域名所有权” 部分中，转到 “主机名” 列，然后复制电子邮件域名前面的值部分。

   例如，如果您的亚马逊 WorkMail 电子邮件域名为 example.com，主机名的值为 _amazonses.example.com，请复制 _amazonses。
6. 在 Route 53 控制台中，执行以下操作：
   a. 选择 Create record（创建记录），然后选择 Simple routing（简单路由）。
   b. 对于 Record name（记录名称），请粘贴您在步骤 5 中复制的值。
   c. 对于 Record type（记录类型），选择 TXT – Text（TXT - 文本）。
7. 在 Amazon WorkMail 控制台中，对于 TXT 记录，复制值列的值，包括引号。
8. 在 Route 53 控制台中，执行以下操作：
   a. 对于 Value/Route traffic to（值/流量路由至），选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值），然后粘贴您在步骤 7 中复制的值。

      请勿更改任何其他设置。
   b. 选择创建。

为亚马逊创建 Route 53 MX 记录 WorkMail

1. 在 Amazon WorkMail 控制台的 “步骤 2：完成域名设置” 部分中，转到 “记录” 类型为 MX 的行，然后复制 “值” 列的值。
2. 在 Route 53 控制台中，执行以下操作：
   a. 选择创建记录。
   b. 对于 Value/Route traffic to（值/流量路由至），选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值），然后粘贴您在步骤 1 中复制的值。
   c. 对于 Record type（记录类型），请选择 MX – Mail Exchange（MX - 邮件交换）。

请勿更改任何其他设置。

d. 选择创建记录。

为亚马逊创建四条 Route 53 别名记录记录 WorkMail

1. 在 Amazon WorkMail 控制台的 “步骤 2：完成域名设置” 部分中，转到记录类型为 CNAME 的第一行。在 Hostname 列中，复制您的电子邮件域名前面的值。

   例如，如果您的亚马逊 WorkMail 电子邮件域名为 e xample.com，主机名的值为 autodisco ver.example.com，请复制自动发现。
2. 在 Route 53 控制台中，执行以下操作：

   a. 选择创建记录。

   b. 对于 Record name（记录名称），请粘贴您在步骤 1 中复制的值。

   c. 对于 Record type（记录类型），选择 CNAME - Canonical Name（CNAME - 规范名称）。
3. 在 Amazon WorkMail 控制台中，在记录类型为 CNAME 的第一行中，复制 “值” 列的值。
4. 在 Route 53 控制台中，执行以下操作：

   a. 对于 Value/Route traffic to（值/流量路由至），选择 IP address or another value depending on the record type（根据记录类型选择 IP 地址或其它值），然后粘贴您在步骤 3 中复制的值。

   请勿更改任何其他设置。

   b. 选择创建记录。
5. 对 Amazon WorkMail 控制台中列出的其余别名记录重复步骤 1 到 4。

将流量路由到亚马逊 OpenSearch 服务域终端节点

Amazon OpenSearch Service 是一项托管服务，可以轻松地在中部署、操作和扩展OpenSearch 集群 Amazon Web Services 云。 OpenSearch 服务服务域与OpenSearch 服务集群同义。域是包含您指定的设置、实例类型、实例计数和存储资源的集群。有关更多信息，请参阅《亚马逊 OpenSearch 服务开发者指南》中的什么是亚马逊 OpenSearch 服务。

先决条件

要开始使用，您需要满足以下条件：

具有自定义域名的 OpenSearch 服务域，例如 example.com，该域名与您要创建的 Route 53 记录的名称相匹配。

有关更多信息，请参阅以下主题：

- 在《亚马逊 OpenSearch 服务开发者指南》中@@ 入门。
- 在《亚马逊 OpenSearch 服务开发者指南》中@@ 创建自定义终端节点。

将 Amazon Route 53 配置为将流量路由到亚马逊 OpenSearch 服务域终端节点

要使用 Route 53 将流量路由到 OpenSearch 服务，您首先需要获得 OpenSearch 服务提供的域终端节点。只有在具有双堆栈网络模式的 OpenSearch 服务域上启用自定义终端节点时，才会提供此双堆栈端点。有关更多信息，请参阅《亚马逊 OpenSearch 服务开发者指南》中的创建自定义终端节点。

将流量路由到 OpenSearch 服务端点

1. 前往https://aws.amazon.com并选择 “登录到控制台”。
2. 在 “分析” 下，选择 “亚马逊 OpenSearch 服务”。
3. 在托管集群下，选择域。
4. 在域页面上，选择要向其路由流量的域名。
5. 在域详细信息页面上，复制域端点 v2（双堆栈）的值。
6. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
7. 在导航窗格中，选择 Hosted zones（托管区域）。
8. 为要用于将流量路由到 OpenSearch 服务终端节点的域名选择托管区域的链接名称。域名必须与 S OpenSearch ervice 中定义的自定义终端节点相匹配。
9. 选择创建记录。

   可以使用该向导来创建记录，也可以选择 Switch to quick create（切换到快速创建）。
10. 指定以下值：

    路由策略

    选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

    记录名称

    输入您要用于将流量路由到 OpenSearch 服务域终端节点的域名。默认值为托管区的名称。

例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的分配，请输入 acme。

Alias

如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

值/流量路由至

选择 OpenSearch 服务域终端节点的别名。选择创建OpenSearch 服务域的区域，然后选择您在步骤 5 中获得的值。

记录类型

为双栈选择 A — IPv4 地址、AAAA — IPv6 地址或两者兼而有之。

评估目标运行状况

选择否。 有关评估目标运行状况的信息，请参阅 Evaluate Target Health。

11. 选择创建记录。

将流量路由到 Amazon VPC Lattice 服务域端点

Amazon VPC Lattice 是一项完全托管的应用程序网络服务，用于连接、保护和监控应用程序的服务和资源。您可以将 VPC Lattice 与单个虚拟私有云 (VPC) 配合使用，也可以将 VPCs 来自一个或多个账户的多个虚拟私有云 (VPC) 结合使用。有关更多信息，请参阅 Amazon VPC Lattice 用户指南中的什么是 Amazon VPC Lattice。

先决条件

要开始使用，您需要满足以下条件：

具有自定义域名（例如 example.com）的 VPC Lattice 服务域，此域名与您要创建的 Route 53 记录的名称匹配。

有关更多信息，请参阅 Amazon VPC Lattice 用户指南中的将自定义域名与服务关联。

配置 Amazon Route 53 以将流量路由到 VPC Lattice 服务域端点

要使用 Route 53 将流量路由到 Amazon VPC Lattice 服务域，您需要先获取 VPC Lattice 提供的域服务端点。有关更多信息，请参阅 Amazon VPC Lattice 用户指南中的将自定义域名与服务关联。

将流量路由到 VPC Lattice 服务域端点

1. 前往https://aws.amazon.com并选择 “登录到控制台”。
2. 在网络和内容传输下，选择 VPC。
3. 在 Un PrivateLink der 和 Lattice 中选择莱迪思服务。
4. 创建 VPC Lattice 服务或选择现有的 VPC Lattice 服务。

> **Note**
>
> 创建 VPC Lattice 服务时，必须指定自定义域配置并提供自定义域名。如果您选择现有服务，则该服务还必须具有自定义域。

5. 在域配置下，复制自定义域名的值。
6. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
7. 在导航窗格中，选择 Hosted zones（托管区域）。
8. 对于域，选择要用于将流量路由到 VPC Lattice 服务的托管区关联名称。域名必须与 VPC Lattice 中定义的自定义域端点匹配。
9. 选择创建记录。

   可以使用该向导来创建记录，也可以选择 Switch to quick create（切换到快速创建）。
10. 指定以下值：

    路由策略

    选择适用的路由策略。有关更多信息，请参阅 选择路由策略。

    记录名称

    输入要用于将流量路由到 Amazon VPC 服务域端点的域名。默认值为托管区的名称。

    例如，如果托管区域的名称为 example.com，并且您要使用 acme.example.com 将流量路由到您的分配，请输入 acme。

    Alias

    如果您使用 Quick create（快速创建）记录创建方法，请启用 Alias（别名）。

值/流量路由至

选择 VPC Lattice 服务的别名。选择在其中创建 VPC Lattice 服务域的区域，然后选择您在步骤 5 中获得的值。

记录类型

为双栈选择 A — IPv4 地址、AAAA — IPv6 地址，或两者兼而有之。

评估目标运行状况

选择否。 有关评估目标运行状况的信息，请参阅 Evaluate Target Health。

11. 选择创建记录。

将流量路由到其他 Amazon 资源

以下是其他指南中有关如何使用 Route 53 将流量路由到这些服务的主题列表。

- Amazon Cloud Map 用户指南中的使用 Amazon Cloud Map。
- 在《 Amazon App Runner 开发者指南》中@@ 管理自定义域名。
- 《Amazon Transfer Family 用户指南》中的使用 Route 53 作为 DNS 提供商。
- 使用 Route 53 将域指向 Amazon Lightsail 实例。

创建 Amazon Route 53 运行状况检查

Amazon Route 53 运行状况检查监控 Web 应用程序、Web 服务器以及其它资源的运行状况和性能。您创建的每种运行状况检查都可以监控以下任一内容：

- 指定资源（如 Web 服务器）的运行状况。
- 其它运行状况检查的状态。
- Amazon CloudWatch 告警的状态。
- 此外，借助 Amazon 应用程序恢复控制器 (ARC)，您可以使用 DNS 故障转移记录设置路由控制运行状况检查，以管理应用程序的流量故障转移。要了解更多信息，请参阅 Amazon 应用程序恢复控制器 (ARC) 开发人员指南。

有关运行状况检查类型的概览，请参阅 Amazon Route 53 运行状况检查类型。有关创建运行状况检查的信息，请参阅创建和更新运行状况检查。

在创建运行状况检查后，您可以获取运行状况检查的状态、在状态更改时获取通知，还可以配置 DNS 故障转移：

获取运行状况检查状态和通知

可在 Route 53 控制台中查看运行状况检查的当前和最近状态。还可以通过以下项之一以编程方式进行运行状况检查：AAmazon 软件开发工具包、Amazon Command Line Interface、Amazon Tools for Windows PowerShell 或 Route 53 API。

如果您要在运行状况检查的状态更改时接收通知，可为每个运行状况检查配置 Amazon CloudWatch 告警。

有关查看运行状况检查状态和接收通知的信息，请参阅监控运行状况检查状态和获取通知。

配置 DNS 故障转移

如果您有多个执行相同功能的资源，则可配置 DNS 故障转移，以使 Route 53 将流量从运行状况不佳的资源路由到运行状况良好的资源。例如，如果您有两台 Web 服务器，其中一台 Web 服务器运行状况不佳，则 Route 53 可将流量路由到另一台 Web 服务器。有关更多信息，请参阅 配置 DNS 故障转移。

主题

- Amazon Route 53 运行状况检查类型

- Amazon Route 53 如何确定运行状况检查是否正常
- 创建、更新和删除运行状况检查
- 配置 DNS 故障转移
- 为运行状况检查命名和添加标签
- 将运行状况检查程序与早于 2012-12-12 的 Amazon Route 53 API 版本结合使用

Amazon Route 53 运行状况检查类型

您可以创建以下类型的 Amazon Route 53 运行状况检查：

监控端点的运行状况检查

您可以配置运行状况检查来监控通过 IP 地址或域名指定的端点。Route 53 按照您指定的固定间隔，通过互联网向您的应用程序、服务器或其它资源自动提交请求，以验证其是否可到达、是否可用及功能是否正常。您也可以通过配置运行状况检查来发出与用户发出的请求类似的请求，如从特定 URL 请求网页。

监控其他运行状况检查的运行状况检查 (已计算的运行状况检查)

您可以创建运行状况检查，以监控 Route 53 是将其它运行状况检查视为运行状况良好还是不佳。在下面的情况下，这种运行状况检查可能很有用：您有多个执行相同功能的资源 (如多台 Web 服务器)，您主要关注的是运行状况良好的资源数是否达到最少数目。您可以为每个资源创建运行状况检查，而不为这些运行状况检查配置通知。然后，您可以创建一个运行状况检查，来监控其他运行状况检查的状态，并且仅在可用的 Web 资源数低于指定阈值时通知您。

监控 CloudWatch 告警的运行状况检查

您可以创建用于监控 CloudWatch 指标状态的 CloudWatch 告警，这些指标包括 Amazon DynamoDB 数据库的受限读取事件数或被认为运行状况良好的 Elastic Load Balancing 主机数。在创建告警后，可以创建运行状况检查，使其监控与 CloudWatch 针对告警监控的数据流相同的数据流。

为了提高复原能力和可用性，Route 53 不等待 CloudWatch 告警进入 ALARM 状态。运行状况检查的状态会根据数据流以及 CloudWatch 告警中的条件从运行状况良好更改为运行状况不佳。

Route 53 支持 CloudWatch 告警的以下功能：

- 标准精度指标。不支持高精度指标。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的高分辨率指标。

- 统计数据：Average、Minimum、Maximum、Sum 和 SampleCount。不支持扩展统计数据。
- Route 53 不支持“M (N)”告警。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的评估告警。
- 运行状况检查只能监控与运行状况检查同处一个 Amazon 账户的 CloudWatch 告警。
- Route 53 不支持使用指标数学查询多个 CloudWatch 指标的告警。

Amazon 应用程序恢复控制器（ARC）中的路由控制

ARC 中的运行状况检查与路由控制关联，路由控制是简单的开关切换。您可以使用故障转移 DNS 记录配置每个路由控制运行状况检查。然后，您只需在 ARC 中更新路由控制，即可重新路由流量和故障转移应用程序，例如跨可用区或 Amazon 区域。有关更多信息，请参阅《ARC 开发人员指南》中的 ARC 中的路由控制。

Amazon Route 53 如何确定运行状况检查是否正常

Amazon Route 53 用来确定运行状况检查是否正常的方法取决于运行状况检查的类型。

Route 53 如何确定监控端点的运行状况检查的状态

Route 53 在世界各地都具有运行状况检查程序。当您创建监控端点的运行状况检查时，运行状况检查程序将开始向您指定的端点发送请求，以确定该端点是否运行良好。您可以选择 Route 53 要使用的位置，也可以指定检查之间的时间间隔：每 10 秒或每 30 秒。请注意，不同数据中心的 Route 53 运行状况检查程序不会彼此协作，因此无论您选择多久的时间间隔，都会遇到有时每秒收到多个请求、然后接下来的几秒根本没有任何运行状况检查请求的情况。

每个运行状况检查程序基于以下两个值评估端点的运行状况：

- 响应时间。资源可能出于各种原因而响应缓慢或无法响应运行状况检查请求。例如，资源被关闭以进行维护，它处于分布式拒绝服务 (DDoS) 攻击下，或者网络被关闭。
- 端点是否响应您指定的一系列连续运行状况检查 (失败阈值)

Route 53 将聚合运行状况检查程序中的数据并确定端点是否运行正常：

- 如果超过 18% 的运行状况检查程序报告端点运行状况良好，则 Route 53 将认为它运行状况良好。
- 如果 18% 或更少的运行状况检查程序报告端点运行状况良好，则 Route 53 将认为它运行状况不佳。

选择 18% 的值是为了确保位于多个区域的运行状况检查程序认为端点运行状况良好。这可以防止端点仅因为网络条件问题导致与部分运行状况检查位置隔离而被视为运行状况不佳。在未来的版本中，这个值可能会更改。

单个运行状况检查程序用于确定端点运行状况是否正常的响应时间取决于运行状况检查的类型：

- HTTP 和 HTTPS 运行状况检查 — Route 53 必须能够在四秒内与端点建立 TCP 连接。此外，该端点必须在连接后的两秒内用 2xx 或 3xx 的 HTTP 状态代码来响应。

  > **Note**
  >
  > HTTPS 运行状况检查不验证 SSL/TLS 证书，因此，如果证书无效或过期，检查不会失败。

- TCP 运行状况检查 — Route 53 必须能够在十秒内与端点建立 TCP 连接。
- 使用字符串匹配的 HTTP 和 HTTPS 运行状况检查 — 与 HTTP 和 HTTPS 运行状况检查一样，Route 53 必须能够在四秒内与端点建立 TCP 连接，并且端点必须在连接后的两秒内使用 HTTP 状态代码 2xx 或 3xx 来响应。

  Route 53 运行状况检查程序在收到 HTTP 状态代码之后，它必须在接下来的两秒内收到来自端点的响应正文。Route 53 将在响应正文中搜索您指定的字符串。该字符串必须完全显示在响应正文的前 5120 个字节中，否则端点将无法通过运行状况检查。如果您使用的是 Route 53 控制台，则需在 Search String（搜索字符串）字段中指定字符串。如果您使用的是 Route 53 API，则需在创建运行状况检查时在 `SearchString` 元素中指定字符串。

对于监控端点的运行状况检查 (TCP 运行状况检查除外)，如果来自端点的响应包含任何标头，则标头的格式必须为 RFC7230 规范《超文本传输协议 (HTTP/1.1)：消息语法和路由》第 3.2 节“标头字段”中定义的格式。

Route 53 在没有足够的数据来确定实际状态、运行正常或不正常时，将新的运行状况检查视为正常。如果您选择了反转运行状况检查状态的选项，则 Route 53 在有足够的数据之前将运行状况检查视为不正常。

Route 53 如何确定监控其它运行状况检查的运行状况检查的状态

运行状况检查可以监控其他运行状况检查的状态；此类型的运行状况检查称为已计算的运行状况检查。进行监控的运行状况检查是父运行状况检查，受监控的运行状况检查是子运行状况检查。一个父运行状况检查可以监控最多 255 个子运行状况检查的运行状况。以下是监控的工作原理：

- Route 53 将视为运行状况良好的子运行状况检查的数量相加。

- Route 53 将该数字与运行状况必须正常、否则即认为父运行状况检查的状态不良的子运行状况检查数量进行比较。

有关更多信息，请参阅[您在创建或更新运行状况检查时指定的值]中的[监控其他运行状况检查（已计算的运行状况检查）]。

Route 53 在没有足够的数据来确定实际状态、运行正常或不正常时，将新的运行状况检查视为正常。如果您选择了反转运行状况检查状态的选项，则 Route 53 在有足够的数据之前将运行状况检查视为不正常。

Route 53 如何确定监控 CloudWatch 告警的运行状况检查的状态

当您创建基于 CloudWatch 告警的运行状况检查时，Route 53 监控对应告警的数据流而不是监控告警状态。如果数据流指示告警的状态为 OK (正常)，则认为该运行状况检查正常。如果数据流指示状态为 Alarm (告警)，则认为该运行状况检查不正常。如果数据流未提供足够的信息来确定告警的状态，则运行状况检查状态将取决于 Health check status (运行状况检查状态) 的设置：运行状况良好、运行状况不佳或上一个已知状态。（在 Route 53 API 中，此设置为 `InsufficientDataHealthStatus`。）

Route 53 不支持跨账户 CloudWatch 警报。

> **Note**
>
> 由于 Route 53 运行状况检查监控 CloudWatch 数据流而非 CloudWatch 告警的状态，您无法使用 CloudWatch SetAlarmState API 操作强行更改运行状况检查的状态。

Route 53 在没有足够的数据来确定实际状态、运行正常或不正常时，将新的运行状况检查视为正常。如果您选择了反转运行状况检查状态的选项，则 Route 53 在有足够的数据之前将运行状况检查视为不正常。

创建、更新和删除运行状况检查

> **Important**
>
> 如果您要更新或删除与记录关联的运行状况检查，请先查看[在配置了 DNS 故障转移的情况下更新或删除运行状况检查]中的任务，然后再继续。

本节涵盖以下有关管理 Route 53 运行状况检查的主题：

1. 创建和更新运行状况检查：
   - 了解如何使用 Route 53 控制台创建和更新运行状况检查。
   - 了解创建或更新运行状况检查时需要指定的值，例如端点监控、协议、IP 地址、域名和高级配置选项。
2. 创建运行状况检查时的显示值：
   - 根据您在创建运行状况检查时输入的内容，了解 Route 53 控制台显示的值，例如完整的 URL 或 IP 地址和端口。
3. 更新 CloudWatch 告警变更的运行状况检查：
   - 了解在更改关联 CloudWatch 告警的设置时如何更新运行状况检查。
4. 删除运行状况检查：
   - 按照步骤使用 Route 53 控制台删除运行状况检查。
5. 在配置了 DNS 故障转移的情况下更新或删除运行状况检查：
   - 了解更新或删除与 DNS 记录关联的运行状况检查时需要执行的建议任务，以确保路由和故障转移配置正确。
6. 配置路由器和防火墙规则：
   - 了解如何配置路由器和防火墙规则以允许来自 Route 53 运行状况检查程序的入站流量，从而确保运行状况检查取得成功。

通过遵循本节提供的信息，就可以有效地创建、更新和删除 Route 53 运行状况检查，管理运行状况检查配置，并确保恰当集成 DNS 故障转移和路由策略。

主题

- 为 Amazon Route 53 运行状况检查配置路由器和防火墙规则

创建和更新运行状况检查

以下过程介绍如何使用 Route 53 控制台创建和更新运行状况检查。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

创建或更新运行状况检查

1. 如果要更新已经与记录关联的运行状况检查，请执行在配置了 DNS 故障转移的情况下更新或删除运行状况检查中推荐的任务。
2. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Health Checks (运行状况检查)。
4. 如果要更新现有的运行状况检查，请选择该运行状况检查的链接 ID，然后选择编辑。

   如果要创建运行状况检查，请选择创建运行状况检查。
5. 输入适用的值。请注意，有些值在创建运行状况检查后无法更改。有关更多信息，请参阅 您在创建或更新运行状况检查时指定的值。
6. 选择创建运行状况检查。

> **Note**
>
> Route 53 在没有足够的数据来确定实际状态、运行正常或不正常时，将新的运行状况检查视为正常。

7. 将运行状况检查与一个或多个 Route 53 记录关联。有关创建和更新记录的信息，请参阅使用记录。

Old console

创建或更新运行状况检查

1. 如果要更新已经与记录关联的运行状况检查，请执行在配置了 DNS 故障转移的情况下更新或删除运行状况检查中推荐的任务。
2. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Health Checks (运行状况检查)。
4. 如果要更新现有的运行状况检查，请选择该运行状况检查，然后选择 Edit Health Check。

   如果要创建运行状况检查，请选择 Create Health Check。有关每种设置的更多信息，请将鼠标指针移到标签上以查看其工具提示。
5. 输入适用的值。请注意，有些值在创建运行状况检查后无法更改。有关更多信息，请参阅 您在创建或更新运行状况检查时指定的值。
6. 选择 Create Health Check。

   > **Note**
   >
   > Route 53 在没有足够的数据来确定实际状态、运行正常或不正常时，将新的运行状况检查视为正常。如果您选择了反转运行状况检查状态的选项，则 Route 53 在有足够的数据之前将运行状况检查视为不正常。
7. 将运行状况检查与一个或多个 Route 53 记录关联。有关创建和更新记录的信息，请参阅使用记录。

您在创建或更新运行状况检查时指定的值

在创建或更新运行状况检查时，您会指定适用的值。请注意，有些值在创建运行状况检查后无法更改。

主题

- 监控端点
- 监控其他运行状况检查（已计算的运行状况检查）

- 监控 CloudWatch 告警
- 高级配置（仅限“监控端点”）
- 在运行状况检查失败时收到通知

名称

可选，但建议设置：要为运行状况检查分配的名称。如果您为 Name（名称）指定值，Route 53 将为运行状况检查添加标签、将值 Name（名称）分配给该标签键，并将您指定的值分配给标签值。Name（名称）标签的值将显示在 Route 53 控制台的运行状况检查列表中，以便于您轻松区分各个运行状况检查。

有关为运行状况检查添加标签的更多信息，请参阅为运行状况检查命名和添加标签。

What to monitor

您希望此运行状况检查监控端点还是监控其它运行状况检查的状态：

- Endpoint（端点）— Route 53 监控您指定的端点的运行状况。可通过提供域名或 IP 地址和端口来指定端点。

  > **Note**
  >
  > 如果您指定了非 Amazon 端点，则会产生附加费用。有关更多信息，包括 Amazon 端点的定义，请参阅 Route 53 定价页上的“运行状况检查”。

- Status of other health checks (calculated health check)（其它运行状况检查（已计算的运行状况检查）的状态）— Route 53 根据您指定的其它运行状况检查的状态来确定此运行状况检查是否运行良好。您还可以指定需要有多少个运行状况检查运行良好，才会将此运行状况检查视为运行良好。
- State of CloudWatch alarm data stream（CloudWatch 告警数据流的状态）– Route 53 通过监控 CloudWatch 告警的数据流确定此运行状况检查是否运行良好。

监控端点

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

如果您希望此运行状况检查来监控端点，请指定以下值：

- 使用以下指定端点
- IP 地址
- 域名

Specify endpoint by

您要使用 IP 地址还是使用域名来指定端点。

创建运行状况检查后，您将无法更改 Specify endpoint by 的值。

IP address (仅限于“Specify endpoint by IP address”)

在下拉列表中选择协议，在文本框中输入 IP 地址、端口和路径。

- 协议可以是以下之一：

  HTTP — Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTP 请求并等待 2xx 或 3xx 的 HTTP 状态代码。

- HTTPS — Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTPS 请求并等待 2xx 或 3xx 的 HTTP 状态代码。

  > **Important**
  >
  > 如果您选择 HTTPS，则端点必须支持 TLS v1.0、v1.1 或 v1.2。

  如果您选择 HTTPS 作为 Protocol 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。

- TCP — Route 53 尝试建立 TCP 连接。

有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

创建运行状况检查后，您将无法更改 Protocol 的值。

对于 IP 地址，如果您选择使用 IP 地址指定端点，则可以输入需要 Route 53 对其执行运行状况检查的端点的 IPv4 或 IPv6 地址。

Route 53 不能检查 IP 地址为本地、私有、不可路由或多播范围的端点的运行状况。有关无法为其创建运行状况检查的 IP 地址的更多信息，请参阅以下文档：

- RFC 5735, Special Use IPv4 Addresses（RFC 5735，特殊使用 IPv4 地址
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space.（RFC 6598，适用于共享地址空间的 IANA 保留 IPv4 前缀）
- RFC 5156, Special-Use IPv6 Addresses（RFC 5156，特殊使用 IPv6 地址

如果端点为 Amazon EC2 实例，我们建议您创建一个弹性 IP 地址，将其与您的 EC2 实例关联，并指定该弹性 IP 地址。这样可以确保您的实例的 IP 地址绝不会发生变化。有关更多信息，请参阅《Amazon EC2 用户指南》中的弹性 IP 地址 (EIP)。

如果您删除 Amazon EC2 实例，请确保同时删除与 EIP 关联的运行状况检查。有关更多信息，请参阅 Amazon Route 53 运行状况检查的最佳实践。

> **Note**
>
> 如果您指定了非 Amazon 端点，则会产生附加费用。有关更多信息，包括 Amazon 端点的定义，请参阅 Route 53 定价页上的“运行状况检查”。

对于端口，请输入需要 Route 53 执行运行状况检查的端点上的端口。

对于路径（仅限 HTTP 和 HTTPS 协议），请输入您希望 Route 53 在执行运行状况检查时请求的路径。该路径可以是端点在运行正常时为其返回 HTTP 状态代码 2xx 或 3xx 的任何值，例如文件 /docs/route53-health-check.html。您还可以包含查询字符串参数，例如 /welcome.html?language=jp&login=y。如果您未包含前导斜杠 (/) 字符，Route 53 会自动添加一个。

Domain name (仅限于“Specify endpoint by domain name”，所有协议)

如果您已选择 Specify endpoint by domain name（通过域名指定端点），则此值为您希望 Route 53 对其执行运行状况检查的端点的域名 (example.com) 或子域名 (backend.example.com)。

如果您选择通过域名指定端点，Route 53 将按您在 Request interval（请求间隔）中指定的时间间隔发送 DNS 查询，以解析您在 Domain name（域名）中指定的域名。然后，Route 53 将使用 DNS 返回的 IP 地址来检查端点的运行状况。

> **Note**
>
> 如果您通过域名指定端点，Route 53 将只使用 IPv4 向该端点发送运行状况检查。如果没有用于您为 Domain name 指定的名称的 A 类记录，运行状况检查将失败，并显示“DNS resolution failed”错误。

如果要检查故障转移、地理位置、地理位置临近度、延迟、多值或加权记录的运行状况，并且您选择的是通过域名指定端点，那么我们建议您为每个端点创建单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。为 Domain name 值指定服务器的域名 (such as us-east-2-www.example.com)，而不是记录的名称 (www.example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

此外，如果协议的值为 HTTP 或 HTTPS，则 Route 53 将传递 `Host` 标头中的域名值，如本列表中前面的主机名称中所述。如果 Protocol（协议）的值为 TCP，Route 53 将不传递 `Host` 标头。

> **Note**
>
> 如果您指定了非 Amazon 端点，则会产生附加费用。有关更多信息，包括 Amazon 端点的定义，请参阅 Route 53 定价页上的“运行状况检查”。

Old console

如果您希望此运行状况检查来监控端点，请指定以下值：

- Specify endpoint by
- 协议
- IP 地址
- Host name
- 端口

- 域名
- 路径

Specify endpoint by

您要使用 IP 地址还是使用域名来指定端点。

创建运行状况检查后，您将无法更改 Specify endpoint by 的值。

协议

您希望 Route 53 用于检查端点运行状况的方法：

- HTTP — Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTP 请求并等待 2xx 或 3xx 的 HTTP 状态代码。
- HTTPS — Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTPS 请求并等待 2xx 或 3xx 的 HTTP 状态代码。

  > **Important**
  >
  > 如果您选择 HTTPS，则端点必须支持 TLS v1.0、v1.1 或 v1.2。

  如果您选择 HTTPS 作为 Protocol 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。
- TCP — Route 53 尝试建立 TCP 连接。

有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

创建运行状况检查后，您将无法更改 Protocol 的值。

IP address (仅限于“Specify endpoint by IP address”)

如果您已选择 Specify endpoint by IP address（使用 IP 地址指定端点），则此值为您希望 Route 53 对其执行运行状况检查的端点的 IPv4 或 IPv6 地址。

Route 53 不能检查 IP 地址为本地、私有、不可路由或多播范围的端点的运行状况。有关无法为其创建运行状况检查的 IP 地址的更多信息，请参阅以下文档：

- RFC 5735, Special Use IPv4 Addresses（RFC 5735，特殊使用 IPv4 地址
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space.（RFC 6598，适用于共享地址空间的 IANA 保留 IPv4 前缀）

- RFC 5156, Special-Use IPv6 Addresses（RFC 5156，特殊使用 IPv6 地址

如果端点为 Amazon EC2 实例，我们建议您创建一个弹性 IP 地址，将其与您的 EC2 实例关联，并指定该弹性 IP 地址。这样可以确保您的实例的 IP 地址绝不会发生变化。有关更多信息，请参阅《Amazon EC2 用户指南》中的弹性 IP 地址 (EIP)。

如果您删除 Amazon EC2 实例，请确保同时删除与 EIP 关联的运行状况检查。有关更多信息，请参阅 Amazon Route 53 运行状况检查的最佳实践。

> **Note**
>
> 如果您指定了非 Amazon 端点，则会产生附加费用。有关更多信息，包括 Amazon 端点的定义，请参阅 Route 53 定价页上的“运行状况检查”。

Host name (仅限于“Specify endpoint by IP address”，仅限于 HTTP 和 HTTPS 协议)

您希望 Route 53 在 HTTP 和 HTTPS 运行状况检查的 `Host` 标头中传递的值。通常是您希望 Route 53 对其执行运行状况检查的网站的完全限定 DNS 名称。以下是 Route 53 在检查端点的运行状况时构造 `Host` 标头的方式：

- 如果您为 Port（端口）指定值 **`80`**，为 Protocol（协议）指定 HTTP，则 Route 53 将向端点传递一个包含 Host name（主机名称）的值的 `Host` 标头。
- 如果您为 Port（端口）指定值 **`443`**，为 Protocol（协议）指定 HTTPS，则 Route 53 将向端点传递一个包含 Host name（主机名称）的值的 `Host` 标头。
- 如果您为 Port（端口）指定其它值，为 Protocol（协议）指定 HTTP 或 HTTPS，则 Route 53 将向端点传递一个包含值 *`Host name`*（主机名称）：*`Port`*（端口）的 `Host` 标头。

如果您选择通过 IP 地址指定端点，并且未指定 Host name（主机名称）的值，Route 53 将替代上述每种情况中 `Host` 标头中的 IP address（IP 地址）值。

端口

您需要 Route 53 对其执行运行状况检查的端点上的端口。

Domain name (仅限于“Specify endpoint by domain name”，所有协议)

如果您已选择 Specify endpoint by domain name（通过域名指定端点），则此值为您希望 Route 53 对其执行运行状况检查的端点的域名 (example.com) 或子域名 (backend.example.com)。

如果您选择通过域名指定端点，Route 53 将按您在 Request interval（请求间隔）中指定的时间间隔发送 DNS 查询，以解析您在 Domain name（域名）中指定的域名。然后，Route 53 将使用 DNS 返回的 IP 地址来检查端点的运行状况。

> **Note**
>
> 如果您通过域名指定端点，Route 53 将只使用 IPv4 向该端点发送运行状况检查。如果没有用于您为 Domain name 指定的名称的 A 类记录，运行状况检查将失败，并显示“DNS resolution failed”错误。

如果要检查故障转移、地理位置、地理位置临近度、延迟、多值或加权记录的运行状况，并且您选择的是通过域名指定端点，那么我们建议您为每个端点创建单独的运行状况检查。例如，为向 www.example.com 提供内容的每台 HTTP 服务器创建运行状况检查。为 Domain name 值指定服务器的域名 (such as us-east-2-www.example.com)，而不是记录的名称 (www.example.com)。

> **Important**
>
> 在此配置中，如果创建 Domain name 的值与记录名称匹配的运行状况检查，然后将该运行状况检查与记录关联，那么运行状况检查结果将无法预测。

此外，如果协议的值为 HTTP 或 HTTPS，则 Route 53 将传递 `Host` 标头中的域名值，如本列表中前面的主机名称中所述。如果 Protocol（协议）的值为 TCP，Route 53 将不传递 `Host` 标头。

> **Note**
>
> 如果您指定了非 Amazon 端点，则会产生附加费用。有关更多信息，包括 Amazon 端点的定义，请参阅 Route 53 定价页上的“运行状况检查”。

Path (仅限于 HTTP 和 HTTPS 协议)

您希望 Route 53 在执行运行状况检查时请求的路径。该路径可以是在端点运行正常时可为其返回 HTTP 状态代码 `2xx` 或 `3xx` 的任意值，如文件 `/docs/route53-health-check.html`。您也可以包括查询字符串参数，例如，`/welcome.html?language=jp&login=y`。如果您未包含前导斜杠 (/) 字符，Route 53 会自动添加一个。

监控其他运行状况检查（已计算的运行状况检查）

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

如果您希望此运行状况检查可监控其他运行状况检查的状态，请指定以下值：

- Health checks to monitor
- Report healthy when

Health checks to monitor

您希望 Route 53 监控的运行状况检查，用于确定此运行状况检查的运行状况。

最多可向 Health checks to monitor 中添加 256 个运行状况检查。要从列表中删除运行状况检查，请选择位于该运行状况检查的突出显示部分右侧的 x。

> **Note**
>
> 您无法配置已计算的运行状况检查来监控其他已计算的运行状况检查的运行状况。

如果您禁用已计算的运行状况检查正在监控的某个运行状况检查，Route 53 会将此已禁用的运行状况检查视为正常，因为它计算的是已计算的运行状况检查是否正常。如果您希望将禁用的运行状况检查视为运行状况不佳，请选中 Invert health check status (反转运行状况检查状态) 复选框。

Report healthy when

您希望 Route 53 执行的、用于确定此运行状况检查是否运行良好的计算：

- Report healthy when at least x of y selected health checks are healthy（当 y 个特定的运行状况检查中的 x 个报告正常时）— 当您添加到 Health checks to monitor（待监控的运行状况检查）的指定数量的运行状况检查运行良好时，则 Route 53 认为此运行状况检查运行良好。请注意以下几点：
  - 如果您指定的数字大于 Health checks to monitor（待监控的运行状况检查）中的运行状况检查数，则 Route 53 始终认为此运行状况检查的运行状况不佳。
  - 如果您指定 0，则 Route 53 始终认为此运行状况检查运行良好。
- Report healthy when all health checks are healthy (AND)（所有运行状况检查均正常时才报告正常 (AND)）— 仅当您添加到 Health checks to monitor（待监控的运行状况检查）的所有运行状况检查都运行良好时，Route 53 才认为此运行状况检查运行良好。
- Report healthy when one or more health checks are healthy (OR)（一个或多个运行状况检查正常时报告正常 (OR)）— 当您添加到 Health checks to monitor（待监控的运行状况检查）的运行状况检查中至少有一项运行良好时，Route 53 将认为此运行状况检查运行良好。

Old console

如果您希望此运行状况检查可监控其他运行状况检查的状态，请指定以下值：

- Health checks to monitor
- Report healthy when
- Invert health check status
- 已禁用

Health checks to monitor

您希望 Route 53 监控的运行状况检查，用于确定此运行状况检查的运行状况。

最多可向 Health checks to monitor 中添加 256 个运行状况检查。要从列表中删除运行状况检查，请选择位于该运行状况检查的突出显示部分右侧的 x。

> **Note**
>
> 您无法配置已计算的运行状况检查来监控其他已计算的运行状况检查的运行状况。

如果您禁用已计算的运行状况检查正在监控的某个运行状况检查，Route 53 会将此已禁用的运行状况检查视为正常，因为它计算的是已计算的运行状况检查是否正常。如果您希望将禁用的运

行状况检查视为运行状况不佳，请选中 Invert health check status (反转运行状况检查状态) 复选框。

Report healthy when

您希望 Route 53 执行的、用于确定此运行状况检查是否运行良好的计算：

- Report healthy when at least x of y selected health checks are healthy（当 y 个特定的运行状况检查中的 x 个报告正常时）— 当您添加到 Health checks to monitor（待监控的运行状况检查）的指定数量的运行状况检查运行良好时，则 Route 53 认为此运行状况检查运行良好。请注意以下几点：
  - 如果您指定的数字大于 Health checks to monitor（待监控的运行状况检查）中的运行状况检查数，则 Route 53 始终认为此运行状况检查的运行状况不佳。
  - 如果您指定 0，则 Route 53 始终认为此运行状况检查运行良好。
- Report healthy when all health checks are healthy (AND)（所有运行状况检查均正常时才报告正常 (AND)）— 仅当您添加到 Health checks to monitor（待监控的运行状况检查）的所有运行状况检查都运行良好时，Route 53 才认为此运行状况检查运行良好。
- Report healthy when one or more health checks are healthy (OR)（一个或多个运行状况检查正常时报告正常 (OR)）— 当您添加到 Health checks to monitor（待监控的运行状况检查）的运行状况检查中至少有一项运行良好时，Route 53 将认为此运行状况检查运行良好。

反转运行状况检查状态（仅限旧控制台）

要在新控制台上反转运行状况检查，请参阅 反转运行状况检查。

选择是否让 Route 53 反转运行状况检查的状态。如果您选择此选项，则 Route 53 会将状态良好的运行状况检查视为状况不佳，反之亦然。

已禁用（仅限旧控制台）

要在新控制台上禁用运行状况检查，请参阅 禁用或启用运行状况检查。

停止 Route 53 执行运行状况检查。在您禁用运行状况检查时，Route 53 停止聚合所引用运行状况检查的状态。

在您禁用运行状况检查之后，Route 53 将运行状况检查的状态始终视为正常。如果您配置了 DNS 故障转移，Route 53 会继续将流量路由到对应的资源。如果您要停止将流量路由到某个资源，请反转运行状况检查。

> **Note**
>
> 在禁用了运行状况检查时，仍会收取运行状况检查费用。

监控 CloudWatch 告警

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

如果您希望此运行状况检查监控 CloudWatch 告警的告警状态，请指定以下值：

- CloudWatch 告警
- 运行状态检查状态

CloudWatch 告警

选择您希望 Route 53 用来确定此运行状况检查是否运行良好的 CloudWatch 告警。CloudWatch 告警必须与运行状况检查同处一个 Amazon Web Services 账户。

> **Note**
>
> Route 53 支持 CloudWatch 告警的以下功能：
>
> - 标准精度指标。不支持高精度指标。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的高分辨率指标。
> - 统计数据：`Average`、`Minimum`、`Maximum`、`Sum` 和 `SampleCount`。不支持扩展统计数据。

- Route 53 不支持“M (N)”告警。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的评估告警。

Route 53 不支持使用指标数学查询多个 CloudWatch 指标的告警。

如果要创建告警，请执行以下步骤：

1. 选择 create（创建）。CloudWatch 控制台将出现在新的浏览器选项卡中。
2. 输入适用的值。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的创建或编辑 CloudWatch 告警。
3. 返回到显示 Route 53 控制台的浏览器选项卡。
4. 选择 CloudWatch alarm 列表旁边的刷新按钮。
5. 从列表中选择新告警。

Important

如果您在创建运行状况检查后更改 CloudWatch 告警的设置，则必须更新该运行状况检查。有关更多信息，请参阅 在您更改 CloudWatch 告警告警设置时更新运行状况检查（仅限于监控 CloudWatch 告警的运行状况检查）。

运行状态检查状态

当 CloudWatch 没有足够的数据来判断您为 CloudWatch alarm（CloudWatch 告警）所选的告警的状态时，请选择运行状况检查的状态（正常、不正常或上一个已知状态）。如果您选择使用上一个已知状态，Route 53 使用上次 CloudWatch 有足够数据来确定告警状态时运行状况检查的状态。对于没有上一个已知状态的新运行状况检查，运行状况检查的默认状态为运行良好。

Health check status（运行状态检查状态）的值提供 CloudWatch 指标的数据流短暂不可用时的临时状态。（Route 53 监控 CloudWatch 指标的数据流，而不是相应告警的状态。）如果指标频繁不可用或长时间（超过几小时）不可用，建议您不要使用上一个已知状态。

Old console

如果您希望此运行状况检查监控 CloudWatch 告警的告警状态，请指定以下值：

- CloudWatch 告警

- 运行状态检查状态
- Invert health check status
- 已禁用

CloudWatch 告警

选择您希望 Route 53 用来确定此运行状况检查是否运行良好的 CloudWatch 告警。CloudWatch 告警必须与运行状况检查同处一个 Amazon Web Services 账户。

> **Note**
>
> Route 53 支持 CloudWatch 告警的以下功能：
>
> - 标准精度指标。不支持高精度指标。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的高分辨率指标。
> - 统计数据：`Average`、`Minimum`、`Maximum`、`Sum` 和 `SampleCount`。不支持扩展统计数据。
> - Route 53 不支持“M (N)”告警。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的评估告警。
>
> Route 53 不支持使用指标数学查询多个 CloudWatch 指标的告警。

如果要创建告警，请执行以下步骤：

1. 选择 create（创建）。CloudWatch 控制台将出现在新的浏览器选项卡中。
2. 输入适用的值。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的创建或编辑 CloudWatch 告警。
3. 返回到显示 Route 53 控制台的浏览器选项卡。
4. 选择 CloudWatch alarm 列表旁边的刷新按钮。
5. 从列表中选择新告警。

> **Important**
>
> 如果您在创建运行状况检查后更改 CloudWatch 告警的设置，则必须更新该运行状况检查。有关更多信息，请参阅 在您更改 CloudWatch 告警告警设置时更新运行状况检查（仅限于监控 CloudWatch 告警的运行状况检查）。

运行状态检查状态

当 CloudWatch 没有足够的数据来判断您为 CloudWatch alarm（CloudWatch 告警）所选的告警的状态时，请选择运行状况检查的状态（正常、不正常或上一个已知状态）。如果您选择使用上一个已知状态，Route 53 使用上次 CloudWatch 有足够数据来确定告警状态时运行状况检查的状态。对于没有上一个已知状态的新运行状况检查，运行状况检查的默认状态为运行良好。

Health check status（运行状态检查状态）的值提供 CloudWatch 指标的数据流短暂不可用时的临时状态。（Route 53 监控 CloudWatch 指标的数据流，而不是相应告警的状态。）如果指标频繁不可用或长时间（超过几小时）不可用，建议您不要使用上一个已知状态。

反转运行状况检查状态（仅限旧控制台）

要在新控制台上反转运行状况检查，请参阅 反转运行状况检查。

选择是否让 Route 53 反转运行状况检查的状态。如果您选择此选项，则 Route 53 会将状态良好的运行状况检查视为状况不佳，反之亦然。

已禁用（仅限旧控制台）

要在新控制台上禁用运行状况检查，请参阅 禁用或启用运行状况检查。

停止 Route 53 执行运行状况检查。当您禁用运行状况检查时，Route 53 停止监控对应的 CloudWatch 指标。

在您禁用运行状况检查之后，Route 53 将运行状况检查的状态始终视为正常。如果您配置了 DNS 故障转移，Route 53 会继续将流量路由到对应的资源。如果您要停止将流量路由到某个资源，请反转运行状况检查。

> **Note**
>
> 在禁用了运行状况检查时，仍会收取运行状况检查费用。

高级配置（仅限“监控端点”）

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

- 新控制台

- 旧控制台

New console

- 请求间隔
- Failure threshold
- 字符串匹配
- 搜索字符串
- Latency graphs
- 启用 SNI
- Host name

请求间隔

每个 Route 53 运行状况检查程序获得来自端点的响应的时间与它发送下一个运行状况检查请求的时间之间的秒数。如果您选择的时间间隔为 30 秒，则全球数据中心的每个 Route 53 运行状况检查程序均会每隔 30 秒向您的端点发送一次运行状况检查请求。平均来说，您的端点每隔两秒会收到一次运行状况检查请求。如果选择的时间间隔为 10 秒，则端点每秒接收超过一次请求。

请注意，不同数据中心的 Route 53 运行状况检查程序不会彼此协作，因此无论您选择多久的时间间隔，都会遇到有时每秒收到多个请求、然后接下来的几秒根本没有任何运行状况检查请求的情况。

创建运行状况检查后，您将无法更改 Request interval 的值。

> **Note**
>
> 如果您选择 Fast (10 seconds) 作为 Request interval 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。

Failure threshold

为了 Route 53 将端点的当前状态在运行良好和运行不佳之间切换，该端点必须通过或未通过的连续运行状况检查数量。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

String matching (HTTP 和 HTTPS)

您是否希望 Route 53 通过向端点提交 HTTP 或 HTTPS 请求并搜索指定字符串的响应正文来确定端点的运行状况。如果响应正文包含您在 Search string（搜索字符串）中指定的值，Route 53 将认为端点运行良好。如果不包含或者端点无响应，Route 53 将认为端点运行状况不佳。搜索字符串必须完全出现在响应正文的前 5120 个字节中。

创建运行状况检查后，您将无法更改 String matching 的值。

> **Note**
>
> 如果您选择 Yes 作为 String matching 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。

运行状况检查程序如何处理压缩响应

如果端点是返回压缩响应的 Web 服务器，则仅当 Web 服务器使用运行状况检查程序支持的压缩算法压缩响应时，Route 53 运行状况检查程序才会在检查指定的搜索字符串之前解压缩响应。运行状况检查程序支持以下压缩算法：

- Gzip
- Deflate

如果使用其它算法压缩响应，则运行状况检查程序无法在搜索字符串之前解压缩响应。在这种情况下，搜索几乎总是会失败，而 Route 53 会认为端点运行状况不佳

Search string (仅在启用“String matching”时)

您希望 Route 53 在来自端点的响应正文中搜索的字符串。最大长度为 255 个字符。

Route 53 在响应正文中搜索 Search string（搜索字符串）时会考虑大小写。

Latency graphs

选择您是否需要 Route 53 在多个 Amazon 区域和端点测量运行状况检查程序之间的延迟。如果您选择该选项，在 Route 53 控制台的 Health checks（运行状况检查）页面上的 Latency（延迟）选项卡中会显示 CloudWatch 延迟图表。如果 Route 53 运行状况检查程序无法连接到端点，Route 53 将无法显示该端点的延迟图表。

创建运行状况检查后，您将无法更改 Latency measurements 的值。

> **Note**
>
> 如果将 Route 53 配置为测量运行状况检查程序与端点之间的延迟，则会产生额外费用。有关更多信息，请参阅 Route 53 定价。

Enable SNI (仅限于 HTTPS)

指定您是否希望 Route 53 在 TLS 协商期间通过 `client_hello` 消息将主机名称发送到端点。这使得端点能够使用适用的 SSL/TLS 证书响应 HTTPS 请求。

某些端点要求 HTTPS 请求在 client_hello 消息中包含主机名。如果不启用 SNI，则运行状况检查状态可能会显示失败。错误消息将取决于服务器为响应不包含 SNI 信息的请求而进行的配置。运行状况检查也可能因为其他原因而存在故障状态。如果已启用 SNI 并且仍收到错误，请检查端点上的 SSL/TLS 配置并确认您的证书是否有效。

请注意以下要求：

- 端点必须支持 SNI。
- 您的端点上的 SSL/TLS 证书在 `Common Name` 字段中包含一个域名，在 `Subject Alternative Names` 字段中可能包含多个域名。证书中的其中一个域名必须与您为 Host name 指定的值匹配。

Health checker regions

选择您希望 Route 53 通过在建议的区域使用运行状况检查程序还是通过在您指定的区域使用运行状况检查程序来检查端点的运行状况。

如果您更新运行状况检查以删除已在执行运行状况检查的区域，Route 53 将继续从该区域执行检查长达一小时。这将确保某些健康检查程序始终检查端点（例如，如果您将三个区域替换为四个不同的区域）。

如果您选择 Customize，请选择区域对应的 x 以将其删除。单击列表底部的空白可将区域添加回列表中。您必须至少指定三个区域。

Host name (仅限于“Specify endpoint by IP address”，仅限于 HTTP 和 HTTPS 协议)

您希望 Route 53 在 HTTP 和 HTTPS 运行状况检查的 `Host` 标头中传递的值。通常是您希望 Route 53 对其执行运行状况检查的网站的完全限定 DNS 名称。以下是 Route 53 在检查端点的运行状况时构造 `Host` 标头的方式：

- 如果您为 Port（端口）指定值 **`80`**，为 Protocol（协议）指定 HTTP，则 Route 53 将向端点传递一个包含 Host name（主机名称）的值的 `Host` 标头。

- 如果您为端口指定值 **443**，为协议指定 HTTPS，则 Route 53 将向端点传递一个包含主机名称的值的 `Host` 标头。
- 如果您为 Port（端口）指定其它值，为 Protocol（协议）指定 HTTP 或 HTTPS，则 Route 53 将向端点传递一个包含值 *`Host name`*（主机名称）：*`Port`*（端口）的 `Host` 标头。

如果您选择通过 IP 地址指定端点，并且未指定 Host name（主机名称）的值，Route 53 将替代上述每种情况中 `Host` 标头中的 IP address（IP 地址）值。

Old console

如果您选择监控端点的选项，还可以指定以下设置：

- 请求间隔
- Failure threshold
- 字符串匹配
- 搜索字符串
- 延迟图
- 启用 SNI
- 运行状况检查程序区域
- Invert health check status
- 已禁用

请求间隔

每个 Route 53 运行状况检查程序获得来自端点的响应的时间与它发送下一个运行状况检查请求的时间之间的秒数。如果您选择的时间间隔为 30 秒，则全球数据中心的每个 Route 53 运行状况检查程序均会每隔 30 秒向您的端点发送一次运行状况检查请求。平均来说，您的端点每隔两秒会收到一次运行状况检查请求。如果选择的时间间隔为 10 秒，则端点每秒接收超过一次请求。

请注意，不同数据中心的 Route 53 运行状况检查程序不会彼此协作，因此无论您选择多久的时间间隔，都会遇到有时每秒收到多个请求、然后接下来的几秒根本没有任何运行状况检查请求的情况。

创建运行状况检查后，您将无法更改 Request interval 的值。

> **Note**
>
> 如果您选择 Fast (10 seconds) 作为 Request interval 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。

Failure threshold

为了 Route 53 将端点的当前状态在运行良好和运行不佳之间切换，该端点必须通过或未通过的连续运行状况检查数量。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

String matching (HTTP 和 HTTPS)

您是否希望 Route 53 通过向端点提交 HTTP 或 HTTPS 请求并搜索指定字符串的响应正文来确定端点的运行状况。如果响应正文包含您在 Search string（搜索字符串）中指定的值，Route 53 将认为端点运行良好。如果不包含或者端点无响应，Route 53 将认为端点运行状况不佳。搜索字符串必须完全出现在响应正文的前 5120 个字节中。

创建运行状况检查后，您将无法更改 String matching 的值。

> **Note**
>
> 如果您选择 Yes 作为 String matching 的值，将产生额外费用。有关更多信息，请参阅 Route 53 定价。

运行状况检查程序如何处理压缩响应

如果端点是返回压缩响应的 Web 服务器，则仅当 Web 服务器使用运行状况检查程序支持的压缩算法压缩响应时，Route 53 运行状况检查程序才会在检查指定的搜索字符串之前解压缩响应。运行状况检查程序支持以下压缩算法：

- Gzip
- Deflate

如果使用其它算法压缩响应，则运行状况检查程序无法在搜索字符串之前解压缩响应。在这种情况下，搜索几乎总是会失败，而 Route 53 会认为端点运行状况不佳

Search string (仅在启用“String matching”时)

您希望 Route 53 在来自端点的响应正文中搜索的字符串。最大长度为 255 个字符。

Route 53 在响应正文中搜索 Search string（搜索字符串）时会考虑大小写。

Latency graphs

选择您是否需要 Route 53 在多个 Amazon 区域和端点测量运行状况检查程序之间的延迟。如果您选择该选项，在 Route 53 控制台的 Health checks（运行状况检查）页面上的 Latency（延迟）选项卡中会显示 CloudWatch 延迟图表。如果 Route 53 运行状况检查程序无法连接到端点，Route 53 将无法显示该端点的延迟图表。

创建运行状况检查后，您将无法更改 Latency measurements 的值。

> **Note**
>
> 如果将 Route 53 配置为测量运行状况检查程序与端点之间的延迟，则会产生额外费用。有关更多信息，请参阅 Route 53 定价。

Enable SNI (仅限于 HTTPS)

指定您是否希望 Route 53 在 TLS 协商期间通过 `client_hello` 消息将主机名称发送到端点。这使得端点能够使用适用的 SSL/TLS 证书响应 HTTPS 请求。

某些端点要求 HTTPS 请求在 `client_hello` 消息中包含主机名。如果不启用 SNI，则运行状况检查状态可能会显示失败。错误消息取决于服务器为响应不包含 SNI 信息的请求而进行的配置。运行状况检查也可能因为其他原因而存在故障状态。如果已启用 SNI 并且仍收到错误，请检查端点上的 SSL/TLS 配置并确认您的证书是否有效。

请注意以下要求：

- 端点必须支持 SNI。
- 您的端点上的 SSL/TLS 证书在 `Common Name` 字段中包含一个域名，在 `Subject Alternative Names` 字段中可能包含多个域名。证书中的其中一个域名必须与您为 Host name 指定的值匹配。

Health checker regions

选择您希望 Route 53 通过在建议的区域使用运行状况检查程序还是通过在您指定的区域使用运行状况检查程序来检查端点的运行状况。

如果您更新运行状况检查以删除已在执行运行状况检查的区域，Route 53 将继续从该区域执行检查长达一小时。这将确保某些健康检查程序始终检查端点（例如，如果您将三个区域替换为四个不同的区域）。

如果您选择 Customize，请选择区域对应的 x 以将其删除。单击列表底部的空白可将区域添加回列表中。您必须至少指定三个区域。

反转运行状况检查状态（仅限旧控制台）

要在新控制台上反转运行状况检查，请参阅 反转运行状况检查。

选择是否让 Route 53 反转运行状况检查的状态。如果您选择此选项，则 Route 53 会将状态良好的运行状况检查视为状况不佳，反之亦然。例如，您可能希望在配置了字符串匹配且端点返回指定值时，Route 53 将运行状况检查判断为不正常。

已禁用（仅限旧控制台）

要在新控制台上禁用运行状况检查，请参阅 禁用或启用运行状况检查。

停止 Route 53 执行运行状况检查。当您禁用运行状况检查时，Route 53 停止尝试与端点建立 TCP 连接。

在您禁用运行状况检查之后，Route 53 将运行状况检查的状态始终视为正常。如果您配置了 DNS 故障转移，Route 53 会继续将流量路由到对应的资源。如果您要停止将流量路由到某个资源，请反转运行状况检查。

> **Note**
>
> 在禁用了运行状况检查时，仍会收取运行状况检查费用。

在运行状况检查失败时收到通知

使用以下选项配置运行状况检查失败时的电子邮件通知：

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Create alarm (仅在创建运行状况检查时)

指定是否要创建默认 CloudWatch 告警。如果选择 Yes（是），CloudWatch 将在此端点的状态变为不正常且 Route 53 认为端点运行状况不佳的时间达到一分钟时，向您发送 Amazon SNS 通知。

> **Note**
>
> 如果您希望 CloudWatch 在状态恢复正常时向您发送另一个 Amazon SNS 通知，可以在创建运行状况检查后创建另一个告警。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的创建 Amazon CloudWatch 告警。

如果要为现有的运行状况检查创建告警，或者要在 Route 53 认为端点运行状况不佳的时间多于或少于一分钟（默认值）时收到通知，请选择 No（否）并在创建运行状况检查后添加告警。有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

Send notification to (仅在创建告警时)

指定您希望 CloudWatch 向现有 Amazon SNS 主题还是向新主题发送通知：

- Existing SNS topic（现有 SNS 主题）— 从列表中选择主题的名称。主题必须位于美国东部（弗吉尼亚北部）区域。
- New SNS topic（新建 SNS 主题）— 在 Topic name（主题名称）中输入主题名称，并在 Recipients（收件人）中输入要将通知发送到的电子邮件地址。可以使用逗号 (,)、分号 (;) 或空格分隔多个地址。

  Route 53 将在美国东部（弗吉尼亚北部）区域创建主题。

Topic name (仅在创建新 SNS 主题时)

如果指定 New SNS Topic，请输入新主题的名称。

Recipient email addresses (仅在创建新 SNS 主题时)

如果您指定了 New SNS topic，请输入要将通知发送到的电子邮件地址。可用逗号 (,)、分号 (;) 或空格分隔多个名称。

创建运行状况检查时 Amazon Route 53 显示的值

Create Health Check (创建运行状况检查) 页面将根据您输入的值显示以下值：

URL

Route 53 在执行运行状况检查时要将请求发送到的完整 URL（适用于 HTTP 或 HTTPS 运行状况检查）或 IP 地址和端口（适用于 TCP 运行状况检查）。

运行状况检查类型

根据您为此运行状况检查指定的设置，此值为 Basic 或 Basic + additional options。有关其它选项的定价信息，请参阅 Route 53 定价。

在您更改 CloudWatch 告警告警设置时更新运行状况检查（仅限于监控 CloudWatch 告警的运行状况检查）

如果您创建 Route 53 运行状况检查来监控 CloudWatch 告警的数据流，然后更新 CloudWatch 告警中的设置，Route 53 将不会自动更新运行状况检查中的告警设置。如果希望运行状况检查开始使用新告警设置，则需要更新运行状况检查。

> **Note**
>
> 要以编程方式更新运行状况检查，可以使用 `UpdateHealthCheck` API。只需指定 `AlarmIdentifier` 和 `Region` 的当前值，Route 53 将从 CloudWatch 获取最新设置。有关此操作的更多信息，请参见 Amazon Route 53 API 参考的 UpdateHealthCheck。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

用新的 CloudWatch 告警设置更新运行状况检查

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选中要更新的运行状况检查的链接 ID。

4. 选择编辑。

   注意事项说明用于运行状况检查的 CloudWatch 告警已更改。Details 字段中将显示新的告警设置。

5. 选择保存。

Old console

用新的 CloudWatch 告警设置更新运行状况检查（控制台）

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选中您要更新的运行状况检查对应的复选框。
4. 选择 Edit health check。

   注意事项说明用于运行状况检查的 CloudWatch 告警已更改。Details 字段中将显示新的告警设置。

5. 选择保存。

禁用或启用运行状况检查

禁用运行状况检查会阻止 Route 53 执行运行状况检查。在您禁用运行状况检查时，Route 53 停止聚合所引用运行状况检查的状态。在您禁用运行状况检查之后，Route 53 将运行状况检查的状态始终视为正常。如果您配置了 DNS 故障转移，Route 53 会继续将流量路由到对应的资源。如果您要停止将流量路由到某个资源，请更改倒置的值。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

创建或编辑运行状况检查时，可以在旧控制台上禁用或启用运行状况检查。有关更多信息，请参阅 您在创建或更新运行状况检查时指定的值。

要在新控制台上禁用运行状况检查，请执行以下步骤。

禁用或启用运行状况检查（仅限新控制台）

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 在操作列中选择三个点，然后选择禁用或启用。

   或者，选择要禁用或启用的运行状况检查的链接 ID。
4. 在配置表中，状态字段指定是启用还是禁用运行状况检查。
5. 要禁用或启用运行状况检查，请选择禁用或启用。

反转运行状况检查

如果反转运行状况检查，则 Route 53 会将状态良好的运行状况检查视为状况不佳，反之亦然。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

创建或编辑运行状况检查时，可以在旧控制台上反转运行状况检查。有关更多信息，请参阅 您在创建或更新运行状况检查时指定的值。

要在新控制台上反转运行状况检查，请执行以下步骤。

反转运行状况检查（仅限新控制台）

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 在操作列中选择三个点，然后选择反转。

   或者选择要反转的运行状况检查的链接 ID。
4. 在配置表中，反转字段指定运行状况检查反转（是）或不反转（否）。
5. 选择反转，以反转运行状况检查。

   如果要撤消反转状态，且已反转字段为是，请再次选择反转。

删除运行状况检查

要禁用运行状况检查，请执行以下过程。

> **Note**
>
> 如果您正在使用 Amazon Cloud Map，并且已配置 Amazon Cloud Map 以在注册实例时创建 Route 53 运行状况检查，则无法使用 Route 53 控制台删除运行状况检查。当您注销实例时，会自动删除运行状况检查。当运行状况检查不再显示在 Route 53 控制台中之前，可能会有几小时的延迟。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

删除运行状况检查

1. 如果要删除与记录关联的运行状况检查，请执行在配置了 DNS 故障转移的情况下更新或删除运行状况检查中推荐的任务。
2. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择运行状况检查。
4. 选择要删除的运行状况检查的链接 ID。
5. 选择删除。
6. 在文本框中输入 **`confirm`**，然后选择删除。

Old console

删除运行状况检查 (控制台)

1. 如果要删除与记录关联的运行状况检查，请执行在配置了 DNS 故障转移的情况下更新或删除运行状况检查中推荐的任务。
2. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
3. 在导航窗格中，选择 Health Checks (运行状况检查)。
4. 在右窗格中，选择要删除的运行状况检查。
5. 选择 Delete Health Check。
6. 选择 Yes, Delete 以确认。

在配置了 DNS 故障转移的情况下更新或删除运行状况检查

当您要更新或删除与记录关联的运行状况检查或者要更改具有关联的运行状况检查的记录时，必须考虑您的更改对 DNS 查询或 DNS 故障转移配置有何影响。

> **Important**
>
> 即使运行状况检查与一个或多个记录关联，Route 53 也不会禁止您删除该运行状况检查。如果您删除运行状况检查，并且未更新关联的记录，则运行状况检查的未来状态将无法预测，且可能发生变化。这会影响 DNS 故障转移配置的 DNS 查询的路由。

要更新或删除已与记录关联的运行状况检查，建议您执行以下任务：

1. 标识与运行状况检查关联的记录。要标识与运行状况检查关联的记录，您必须执行以下操作之一：
   - 使用 Route 53 控制台查看每个托管区域中的记录。有关更多信息，请参阅 列出记录。
   - 对每个托管区域运行 `ListResourceRecordSets` API 操作并查看响应。有关更多信息，请参阅 Amazon Route 53 API 参考中的 ListResourceRecordSets。
2. 评估因更新或删除运行状况检查或因更新记录产生的行为更改。根据该评估确定进行哪些更改。

   有关更多信息，请参阅 忽略运行状况检查时，会出现什么情况？
3. 相应更改运行状况检查和记录。有关更多信息，请参阅以下主题：

- 创建和更新运行状况检查
- 编辑记录

4. 删除您不再使用的运行状况检查 (如果有)。有关更多信息，请参阅 删除运行状况检查。

为 Amazon Route 53 运行状况检查配置路由器和防火墙规则

Route 53 在检查端点的运行状况时会向您在创建运行状况检查时指定的 IP 地址和端口发送 HTTP、HTTPS 或 TCP 请求。为使运行状况检查成功，您的路由器和防火墙规则必须允许来自 Route 53 运行状况检查程序所使用 IP 地址的入站流量。

有关用于 Route 53 运行状况检查程序、用于 Route 53 名称服务器和其它 Amazon 服务的 IP 地址的当前列表，请参阅 Amazon Route 53 服务器的 IP 地址范围。

在 Amazon EC2 中，安全组充当防火墙。有关详细信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 安全组。要将您的安全组配置为允许 Route 53 运行状况检查，您可以允许来自每个 IP 地址范围的入站流量，也可以使用 Amazon 托管的前缀列表。

要使用 Amazon 托管的前缀列表，请修改您的安全组，以允许来自 `com.amazonaws.<region>.route53-healthchecks` 的入站流量，其中 `<region>` 是您的 Amazon EC2 实例或资源的 Amazon Web Services 区域。如果您使用 Route 53 运行状况检查来检查 IPv6 端点，则还应允许来自 `com.amazonaws.<region>.ipv6.route53-healthchecks` 的入站流量。

有关 Amazon 托管的前缀列表的更多信息，请参阅《Amazon VPC 用户指南》中的使用 Amazon 托管的前缀列表。

> **Important**
>
> 当您将 IP 地址添加到允许的 IP 地址列表中时，为创建运行状况检查时您指定的每个 Amazon 区域添加 CIDR 范围内的所有 IP 地址，以及全局 CIDR 范围。您可能会看到运行状况检查请求仅来自某个区域中的一个 IP 地址。但是，该 IP 地址随时可能更改为该区域的另一个 IP 地址。如果要确保同时包含当前和较旧的运行状况检查程序 IP 地址，请将 ALL /26 和 /18 IP 地址范围添加到允许列表中。有关完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon IP 地址范围。
>
> 当您将 Amazon 托管的前缀列表添加到入站安全组时，它会自动添加所有必要的范围。

配置 DNS 故障转移

当您有多个执行同一功能的资源（例如，多台 HTTP 服务器或邮件服务器）时，可以配置 Amazon Route 53，以便检查您的资源的运行状况并仅使用正常资源来响应 DNS 查询。例如，假设您的网站 example.com 托管在 6 台服务器上，这些服务器位于全球三个数据中心，每个数据中心两台。您可以对 Route 53 进行配置，以检查这些服务器的运行状况，并且只使用当前运行状况良好的服务器来响应对 example.com 的 DNS 查询。

Route 53 可以检查您的资源在简单和复杂配置中的运行状况：

- 在简单配置中，可创建一组具有相同名称和类型的记录，例如，用于 example.com 的一组加权记录，其类型为 A。然后，可对 Route 53 进行配置以检查相应资源的运行状况。Route 53 将根据资源的运行状况来响应 DNS 查询。有关更多信息，请参阅 简单 Amazon Route 53 配置中的运行状况检查的工作原理。
- 在更复杂的配置中，将创建根据多个标准路由流量的一个记录树。例如，如果用户的延迟是您最重要的标准，则您可能会使用延迟别名记录，以便将流量路由至可提供最短延迟的区域。延迟别名记录可能会将每个区域中的加权记录作为别名目标。加权记录可能会根据实例类型将流量路由到 EC2 实例。和简单配置一样，可以将 Route 53 配置为根据资源的运行状况路由流量。有关更多信息，请参阅 复杂 Amazon Route 53 配置中的运行状况检查的工作原理。

主题

配置 DNS 故障转移的任务列表

要使用 Route 53 配置 DNS 故障转移，请执行以下任务：

1. 绘制配置的完整树形图，并指明您要为每个节点创建哪种记录 (加权别名、故障转移、延迟等)。在树顶端放入域名 (例如 example.com) 的记录，您的用户将使用它访问您的网站或 Web 应用程序。

   树形图中显示的记录类型取决于配置的复杂程度：

   - 在简单的配置中，您的图表不会包含任何别名记录，或者别名记录会将流量直接路由到 ELB 负载均衡器等资源，而不是路由到另一 Route 53 记录。有关更多信息，请参阅 简单 Amazon Route 53 配置中的运行状况检查的工作原理。
   - 在复杂配置中，您的图表将在多级树中包含别名记录 (如加权别名和故障转移别名) 和非别名记录的组合，如复杂 Amazon Route 53 配置中的运行状况检查的工作原理主题中的示例。

   > **Note**
   >
   > 要快速轻松地为复杂路由配置创建记录并将这些记录与运行状况检查关联，可以使用 Traffic Flow 可视化编辑器并将该配置保存为流量策略。然后，您可以将流量策略关联至同一托管区域或多个托管区域中的一个或多个域名 (例如 example.com) 或子域名 (例如 www.example.com)。此外，如果新配置无法正常工作，您还可以回滚更新。有关更多信息，请参阅 使用 Traffic Flow 来路由 DNS 流量。

   有关更多信息，请参阅以下文档：

   - 选择路由策略
   - 在别名记录和非别名记录之间进行选择

2. 对于不能为其创建别名记录的资源，如 Amazon EC2 服务器和数据中心中运行的电子邮件服务器，为其创建运行状况检查。您会将这些运行状况检查与您的非别名记录相关联。

   有关更多信息，请参阅 创建、更新和删除运行状况检查。

3. 必要时配置路由器和防火墙规则，以使 Route 53 可向您在运行状况检查中指定的端点发送常规请求。有关更多信息，请参阅 为 Amazon Route 53 运行状况检查配置路由器和防火墙规则。

4. 在您的图表中创建所有非别名记录，并将您在第 2 步中创建的运行状况检查与相应的记录关联。

   如果您要在不包含任何别名记录的配置中配置 DNS 故障转移，请跳过其余的任务。

5. 创建将流量路由到 Amazon 资源（如 ELB 负载均衡器和 CloudFront 分配）的别名记录。如果您希望 Route 53 在某一资源运行状况不佳时尝试该树的其它分支，请将每个别名记录的 Evaluate

Target Health（评估目标运行状况）值均设置为 Yes（是）。（Evaluate Target Health（评估目标运行状况）不支持某些 Amazon 资源。）

6. 从您在第 1 步中创建的树形图的底部开始，创建别名记录，将流量路由至在第 4 步和第 5 步中创建的记录。如果您希望 Route 53 在树的某一分支中所有非别名记录均运行状况不良时尝试该树的其它分支，请将每个别名记录的 Evaluate Target Health（评估目标运行状况）值均设置为 Yes（是）。

   请记住，在创建对应的另一记录以前，不能创建将流量路由到这一记录的别名记录。

简单 Amazon Route 53 配置中的运行状况检查的工作原理

当有两个或更多资源执行相同功能 (例如用于 example.com 的两个或更多 Web 服务器) 时，可使用下列运行状况检查功能，将流量仅路由到运行状况良好的资源：

检查 EC2 实例和其他资源的运行状况 (非别名记录)

如果要将流量路由到无法为其创建别名记录的资源 (如 EC2 实例)，可为每个资源创建记录和运行状况检查。然后，将每个运行状况检查与适用的记录关联。运行状况检查会定期检查对应资源的运行状况，而且 Route 53 仅将流量路由到运行状况检查报告为运行状况良好的资源。

评估 Amazon 资源的运行状况（别名记录）

如果使用别名记录将流量路由到所选 Amazon 资源（如 ELB 负载均衡器），可以将 Route 53 配置为评估资源运行状况并仅将流量路由到运行状况良好的资源。在配置别名记录以评估一个资源的运行状况时，不需要为该资源创建运行状况检查。

下面将简单介绍一下，在简单配置中如何配置 Route 53 来检查资源的运行状况：

1. 确定希望 Route 53 监控其运行状况的资源。例如，您可能要监控所有响应对 example.com 的请求的 HTTP 服务器。
2. 对于不能为其创建别名记录的资源，如 EC2 实例或您自己的数据中心中运行的服务器，为其创建运行状况检查。您指定如何将运行状况检查请求发送到资源：使用哪种协议 (TCP、HTTPS 或 HTTP)、使用哪个 IP 地址和端口，对于 HTTP/HTTPS 运行状况检查，还需指定域名和路径。

> **Note**
>
> 如果您正在使用的任何资源是可以为其创建别名记录的资源，如 ELB 负载均衡器，不要为这些资源创建运行状况检查。

常见配置是为每个资源创建一个运行状况检查，并对该运行状况检查端点使用与资源相同的 IP 地址。运行状况检查将请求发送到指定的 IP 地址。

> **Note**
>
> Route 53 不能检查 IP 地址为本地、私有、不可路由或多播范围的资源的运行状况。有关不能为其创建运行状况检查的 IP 地址的更多信息，请参阅 RFC 5735, Special Use IPv4 Addresses 和 RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space。

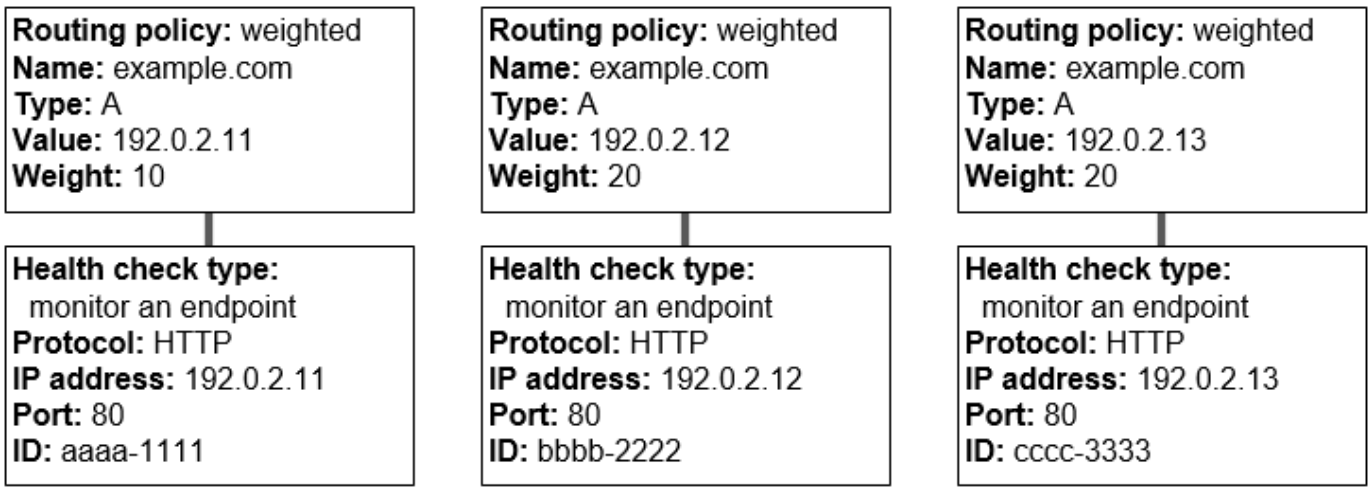
有关创建运行状况检查的更多信息，请参阅创建、更新和删除运行状况检查。

3. 您可能需要配置路由器和防火墙规则，以使 Route 53 可向您在运行状况检查中指定的端点发送常规请求。有关更多信息，请参阅 为 Amazon Route 53 运行状况检查配置路由器和防火墙规则。
4. 您可以为资源创建一组记录，例如一组加权记录。您可以组合使用别名和非别名记录，但它们都必须具有相同的 Name (名称)、Type (类型) 和 Routing Policy (路由策略)。

   您如何配置 Route 53 来检查资源的运行状况取决于您是要创建别名记录还是非别名记录：

   - 别名记录 — 为 Evaluate Target Health（评估目标运行状况）指定 — Yes（是）。
   - 非别名记录 — 将您在第 2 步中创建的运行状况检查与对应记录关联。

   完成后，您的配置将类似于以下图表，其中仅包含非别名记录：



有关使用 Route 53 控制台创建记录的更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

5. 如果您创建了运行状况检查，Route 53 会定期向端点发送运行状况检查请求；它在接收 DNS 查询时不执行运行状况检查。Route 53 会根据响应确定端点是否运行良好，并使用该信息来确定如何响应查询。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

   Route 53 不会检查记录中所指定资源的运行状况，如在 example.com 的 A 记录中指定的 IP 地址。当您将运行状况检查与记录关联时，Route 53 将开始检查您在运行状况检查中所指定端点的运行状况。您还可以配置 Route 53 以监控其它运行状况检查的运行状况或监控 CloudWatch 告警的数据流。有关更多信息，请参阅 Amazon Route 53 运行状况检查类型。

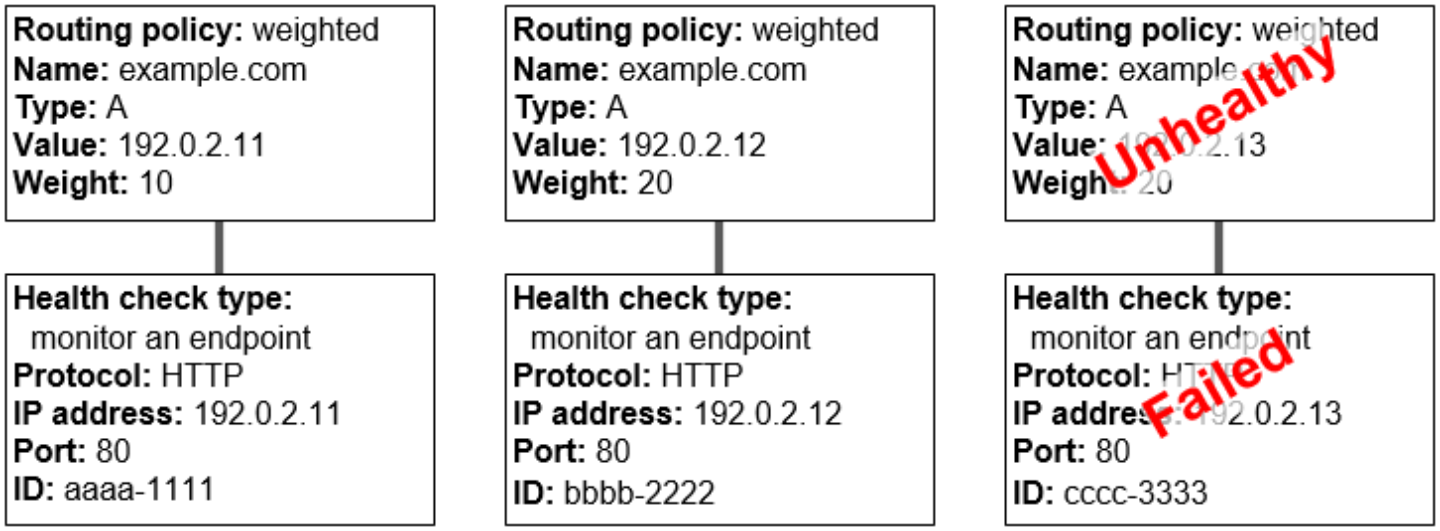
当 Route 53 收到对 example.com 的查询时，将发生以下情况：

1. Route 53 根据路由策略选择记录。在这种情况下，它会根据权重来选择记录。
2. 它通过检查选定记录的运行状况检查的状态来确定该记录的当前运行状况。
3. 如果所选记录运行状况不佳，则 Route 53 会选择不同的记录。此时，将不考虑运行状况不佳的记录。

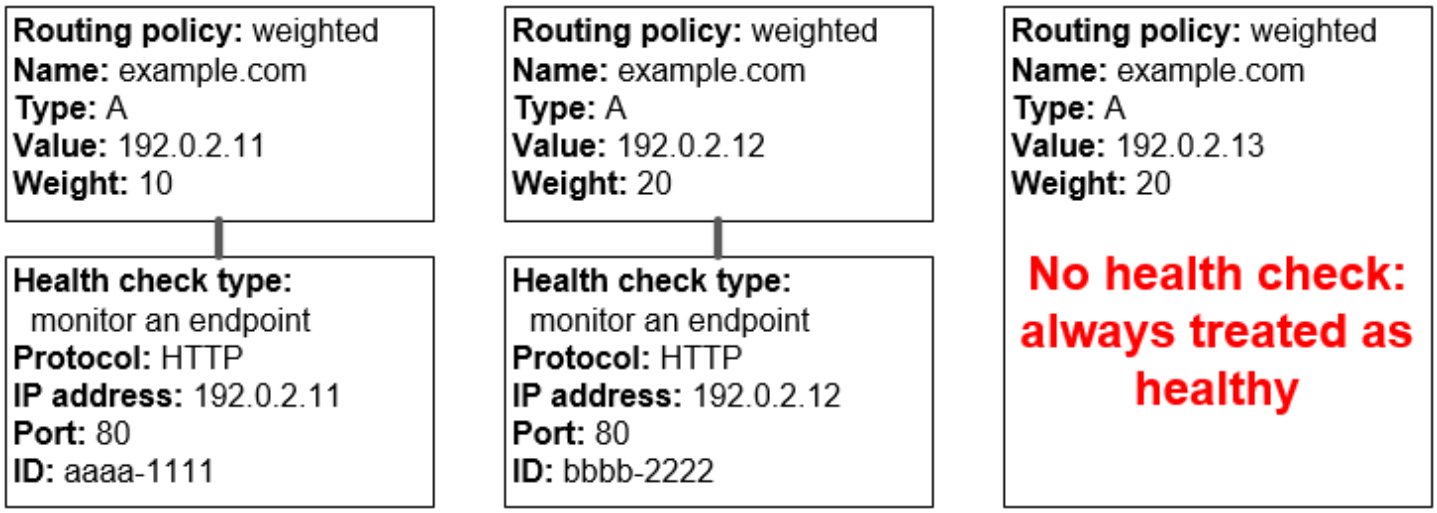
   有关更多信息，请参阅 Amazon Route 53 在已配置运行状况检查时如何选择记录。
4. 当 Route 53 发现运行状况良好的记录时，它会使用适用值 (如 A 记录中的 IP 地址) 来响应查询。

以下示例显示了一组加权记录，其中第三个记录的运行状况不佳。最初，Route 53 会根据所有三个记录的权重选择一个记录。如果第一次碰巧选择了运行状况不佳的记录，Route 53 会选择另一个记录，但这次将在计算中忽略第三个记录的权重：

- 当 Route 53 最初从全部三个记录中进行选择时，在大约 20% 的时间内 (10/(10+20+20))，它会使用第一个记录来响应请求。
- 当 Route 53 确定第三个记录运行状况不佳时，在大约 33% 的时间内 (10/(10+20))，它将使用第一个记录来响应请求。



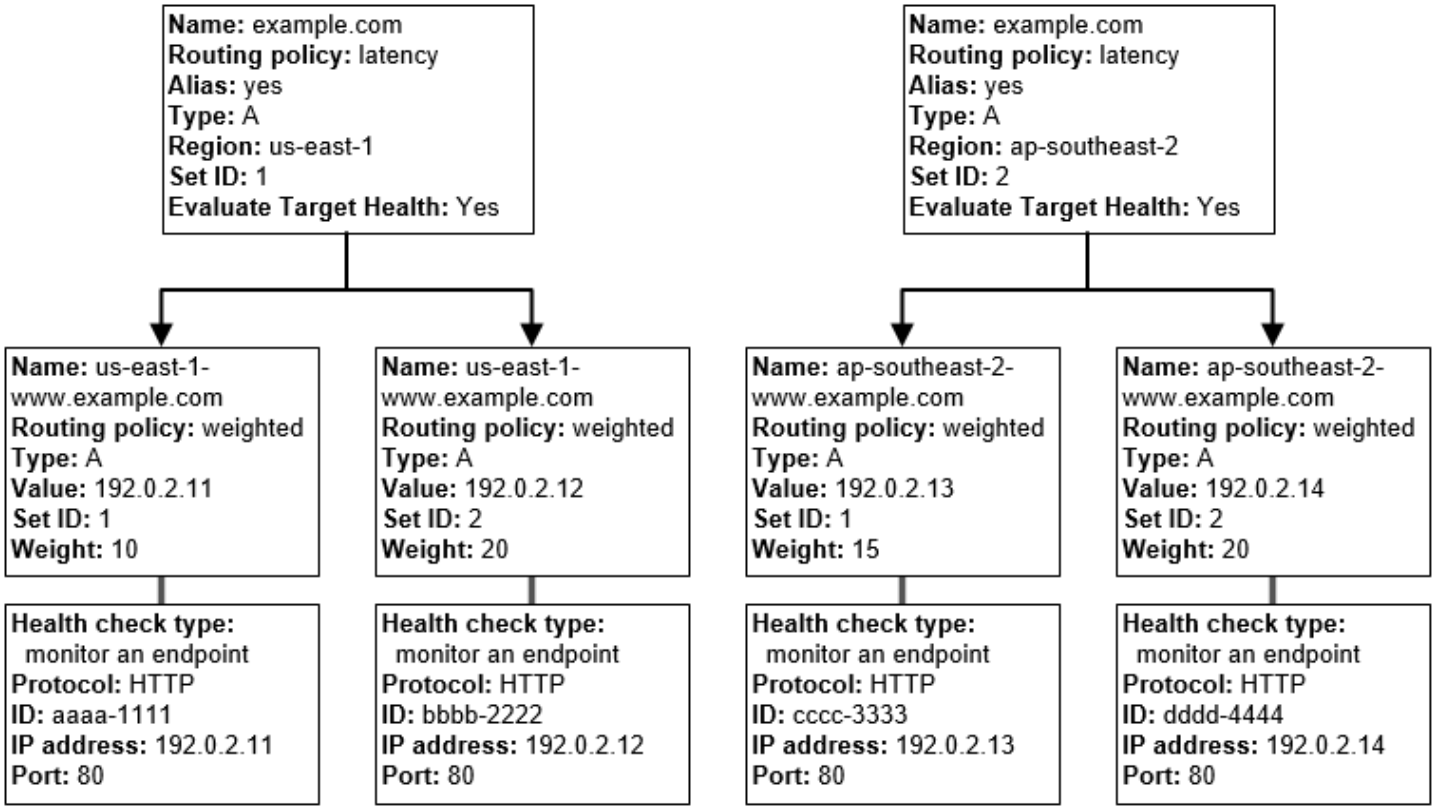
如果您在一组记录的一个或多个记录中省略运行状况检查，则 Route 53 无法确定对应资源的运行状况。Route 53 将这些记录视为运行良好。



复杂 Amazon Route 53 配置中的运行状况检查的工作原理

在复杂配置中检查资源运行状况的工作原理与简单配置中大致相同。但在复杂配置中，可以使用别名记录（如加权别名和故障转移别名）和非别名记录的组合来构建决策树，以使您能够更好地控制 Route 53 响应请求的方式。

例如，您可以使用延迟别名记录选择一个靠近用户的区域，并对每个区域内的两个或多个资源使用加权记录，以针对单个端点或可用区域的故障提供保护。下图演示了此配置。



以下是如何配置 Amazon EC2 和 Route 53 的方式。让我们从树底部开始，因为这是您即将创建记录的顺序：

- 您在 us-east-1 和 ap-southeast-2 这两个区域中分别有两个 EC2 实例。您希望 Route 53 根据 EC2 实例的运行状况决定是否将流量路由到其中，所以为每个实例创建运行状况检查。您可以配置为每个运行状况检查都会向对应实例的弹性 IP 地址发送运行状况检查请求。

  Route 53 是一项全球服务，您无需指定要为其创建运行状况检查的区域。

- 您希望根据实例类型将流量路由到每个区域中的两个实例，所以可为每个实例创建加权记录，并为每个记录指定权重。(您可以稍后更改权重，来更改路由到某个实例的流量。) 然后，将适用的运行状况检查与每个实例关联。

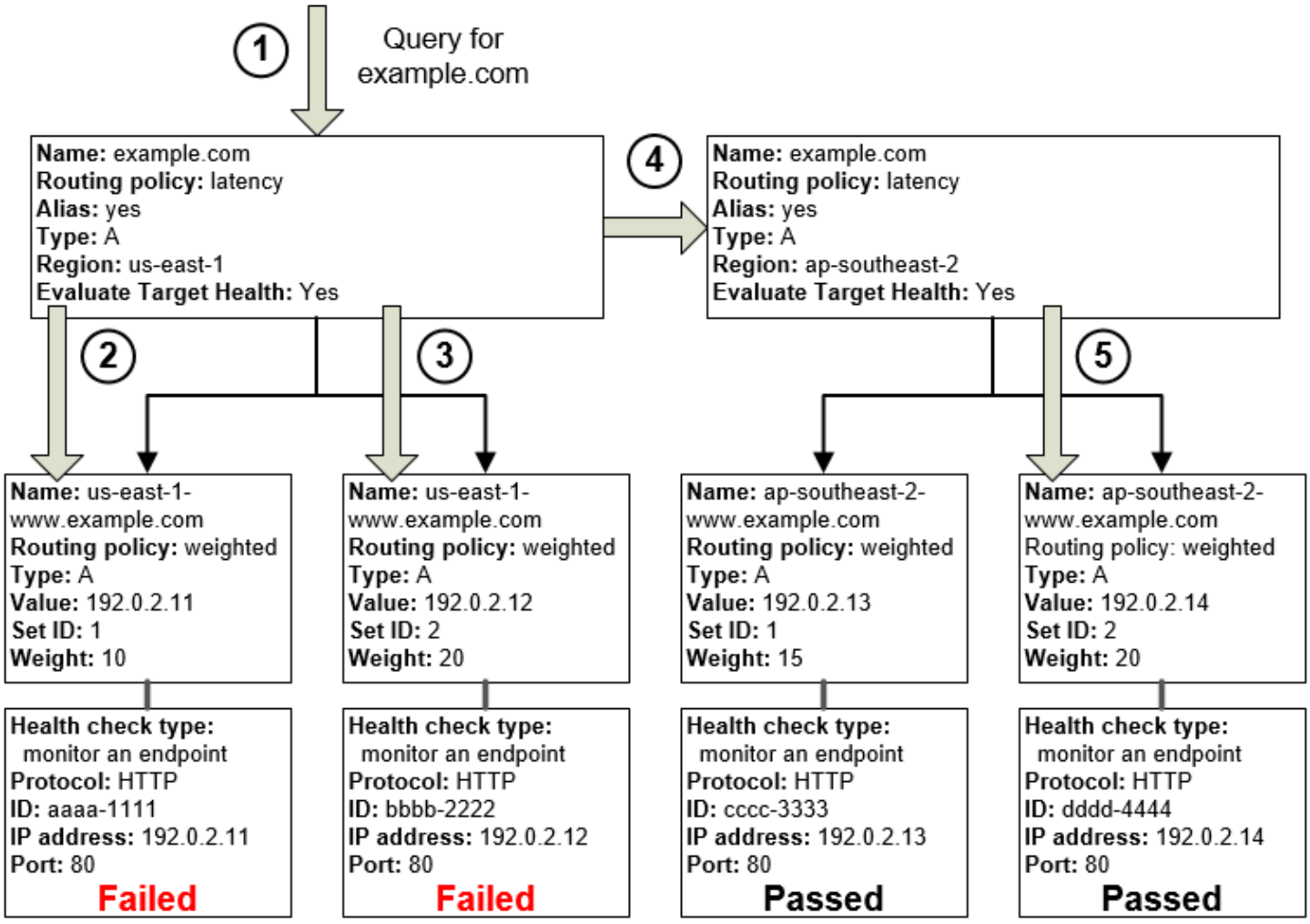
  在创建记录时，可以使用 us-east-1-www.example.com 和 ap-southeast-2-www.example.com 这样的名称。只有等到了树顶端，您才可以为记录指定用户将用于访问网站或 Web 应用程序的名称 (例如 example.com)。

- 您希望将流量路由到可为用户提供最低延迟的区域，因此为树顶端的记录选择延迟路由策略。

  您希望将流量路由到每个区域中的记录，而不是直接路由到每个区域中的资源 (加权记录已执行该功能)。因此，创建延迟别名记录。

在创建别名记录时，为它们指定用户将用于访问网站或 Web 应用程序的名称 (例如 example.com)。别名记录将 example.com 的流量路由到 us-east-1-www.example.com 和 ap-southeast-2-www.example.com 记录。

对于两个延迟别名记录，将 Evaluate Target Health 的值设置为 Yes。这会让 Route 53 去确定一个区域中是否存在任何运行状况良好的资源，然后再尝试将流量路由到对应区域。如果没有，Route 53 会选择其它区域中正常运行的资源。



前面的图表说明了以下事件序列：

1. Route 53 收到针对 example.com 的查询。根据用户提出请求的延迟，Route 53 为 us-east-1 区域选择延迟别名记录。
2. Route 53 根据权重选择加权记录。延迟别名记录的 Evaluate Target Health（评估目标运行状况）为 Yes（是），因此 Route 53 将检查选定的加权记录的运行状况。

3. 运行状况检查失败，因此 Route 53 根据权重选择其它加权记录并检查其运行状况。该记录的运行状况也不佳。
4. Route 53 退出该树的分支，查找其延迟仅次于最佳的延迟别名记录，并为 ap-southeast-2 选择该记录。
5. Route 53 根据权重再次选择记录，然后检查所选资源的运行状况。假定该资源运行状况良好，则 Route 53 在对查询的响应中返回适用的值。

主题

在将运行状况检查与别名记录关联时会发生什么？

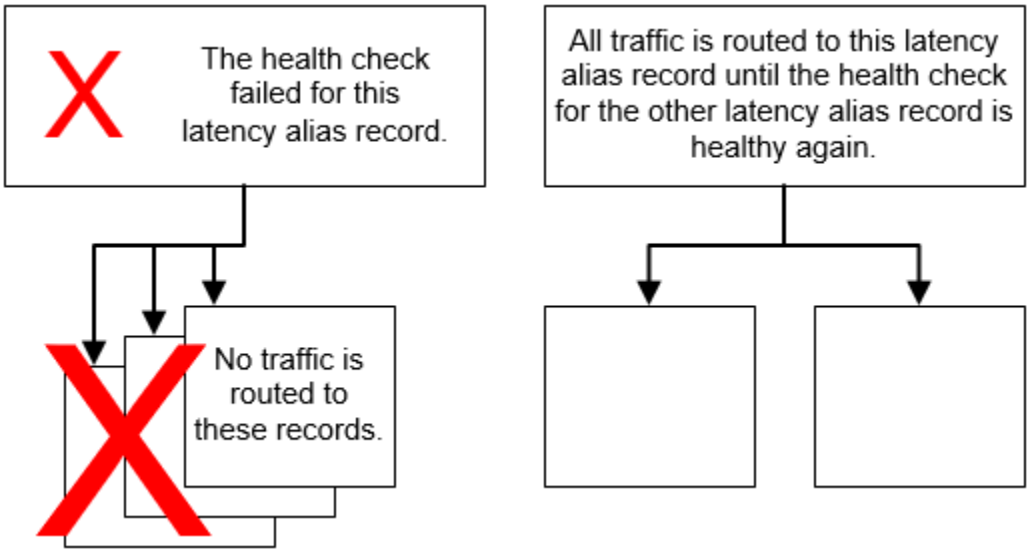
您可以将运行状况检查与别名记录相关联，以作为将 Evaluate Target Health 的值设置为 Yes 的替代或补充。但是，如果 Route 53 根据基础资源 (HTTP 服务器、数据库服务器和您的别名记录引用的其它资源) 的运行状况来响应查询，这样关联通常更有用。例如，假设以下配置：

- 将运行状况检查分配给其别名目标为一组加权记录的延迟别名记录。
- 将延迟别名记录的 Evaluate Target Health 值设置为 Yes。

在此配置中，必须同时满足以下两个条件，Route 53 才会为加权记录返回适用值：

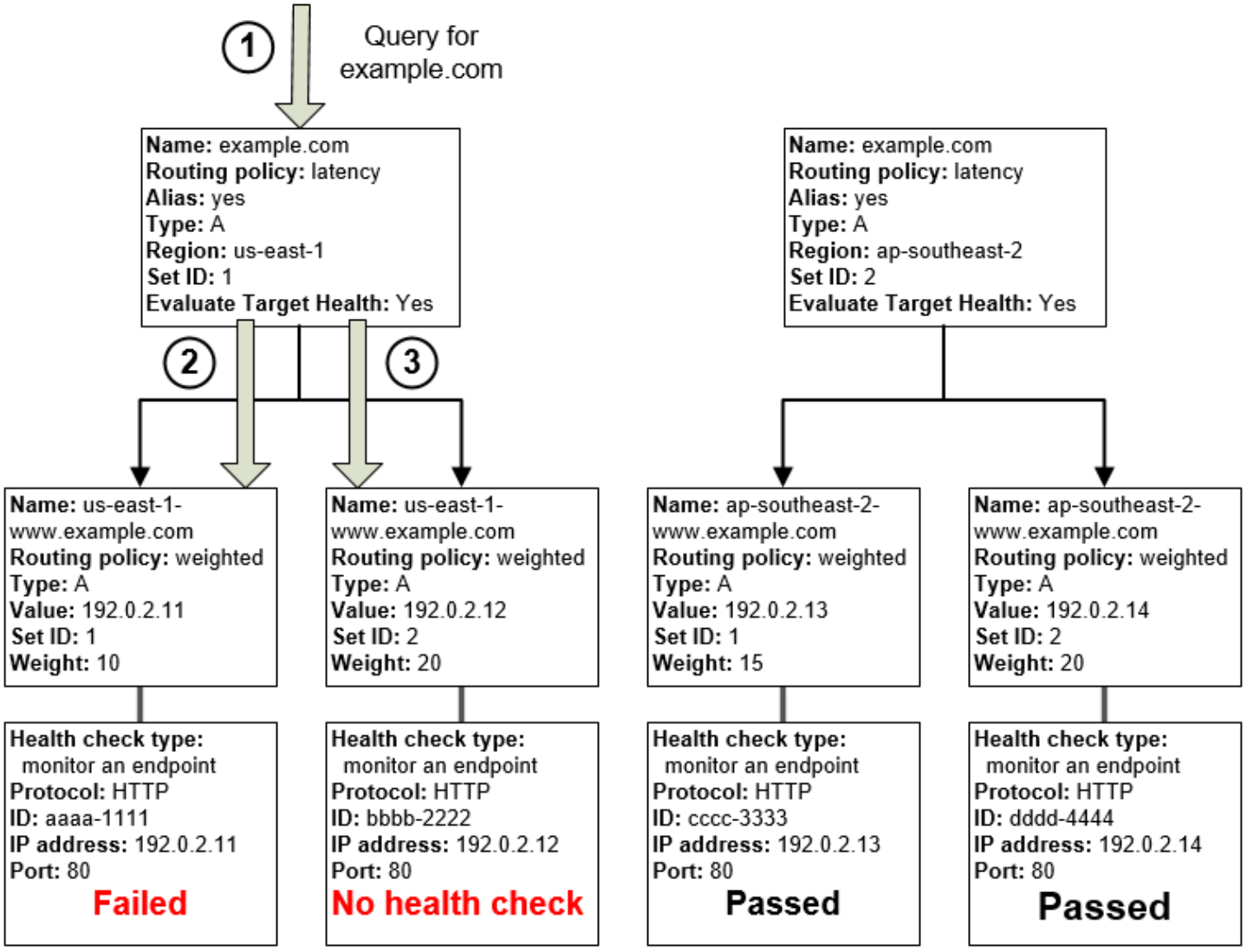
- 必须通过与延迟别名记录关联的运行状况检查。
- 必须至少有一个加权记录因为与已通过的运行状况检查关联或因为不与运行状况检查相关联而被视为运行状况良好。在后一种情况下，Route 53 始终认为加权记录运行状况良好。

在下图中，左上角的延迟别名记录的运行状况检查失败。因此，Route 53 停止响应那些使用该延迟别名记录所引用的任何加权记录的查询，即使这些记录的运行状况良好也同样如此。仅在延迟别名记录恢复良好的运行状况时，Route 53 才会再次开始考虑这些加权记录。(有关例外情况，请参阅Amazon Route 53 在已配置运行状况检查时如何选择记录。)



忽略运行状况检查时，会出现什么情况？

在复杂配置中，应将运行状况检查与所有非别名记录关联，这一点非常重要。在下面的示例中，us-east-1 区域的一个加权记录中缺少运行状况检查。



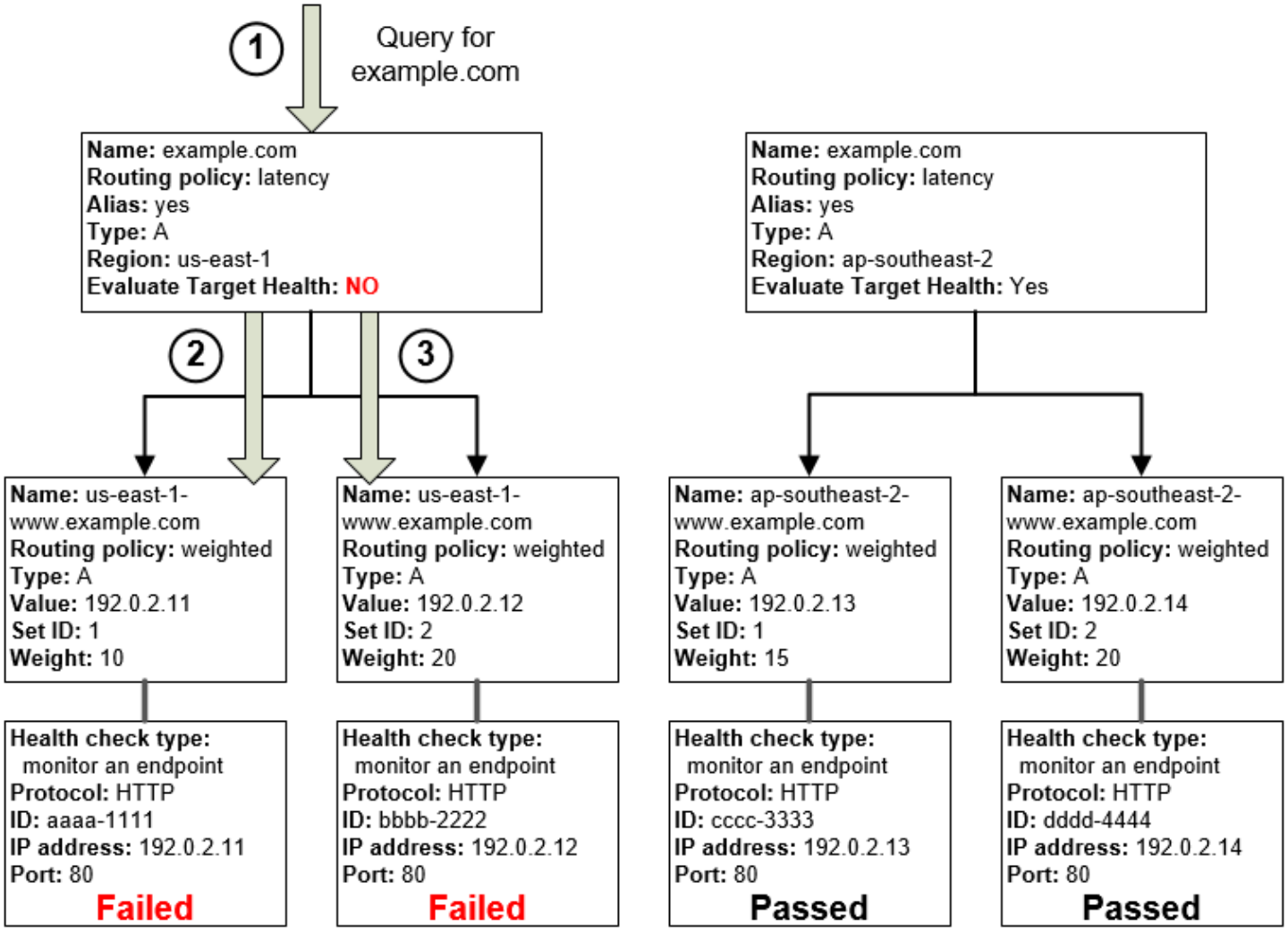
在此配置中，当您忽略对非别名记录的运行状况检查时，将发生以下情况：

1. Route 53 收到针对 example.com 的查询。根据用户提出请求的延迟，Route 53 为 us-east-1 区域选择延迟别名记录。
2. Route 53 为延迟别名记录查找别名目标，并检查相应运行状况检查的状态。一个加权记录的运行状况检查失败，因此不考虑该记录。
3. 用于 us-east-1 区域的别名目标中的其他加权记录没有运行状况检查。相应的资源可能运行状况良好或运行状况不佳，但没有运行状况检查，Route 53 无法了解真实情况。Route 53 假定该资源运行状况良好，并在对查询的响应中返回相应的值。

当您将“Evaluate Target Health”设置为“No”时，会出现什么情况？

通常，应该为树中所有别名记录将 Evaluate Target Health (评估目标运行状况) 设置为 Yes (是)。如果将 Evaluate Target Health（评估目标运行状况）设置为 No（否），Route 53 会继续将流量路由到别名记录引用的记录，即使这些记录未通过运行状况检查。

在以下示例中，所有加权记录都有关联的运行状况检查，但对于 us-east-1 区域的延迟别名记录，则将 Evaluate Target Health (评估目标运行状况) 设置为 No (否)：



在此配置中，当您将别名记录的 Evaluate Target Health 设置为 No 时，将出现以下情况：

1. Route 53 收到针对 example.com 的查询。根据用户提出请求的延迟，Route 53 为 us-east-1 区域选择延迟别名记录。
2. Route 53 确定用于延迟别名记录的别名目标，并检查相应运行状况检查。两项检查都失败。

3. 由于用于 us-east-1 区域中的延迟别名记录的 Evaluate Target Health（评估目标运行状况）值为 No（否），Route 53 必须在此分支中选择一个记录，而不是忽略该分支并在 ap-southeast-2 区域中查找运行状况良好的记录。

Amazon Route 53 在已配置运行状况检查时如何选择记录

如果您配置了为具有相同名称、相同类型 (A 或 AAAA) 和相同路由策略 (如加权或故障转移) 的一组记录中的所有记录进行运行状况检查，则 Route 53 会选择运行良好的记录并返回该记录中的适用值，以响应 DNS 查询。

例如，假设您创建三个加权 A 记录，并且为所有三个记录分配运行状况检查。如果其中一个记录的运行状况检查结果是运行状况不良，则 Route 53 会使用另外两个记录之一中的 IP 地址响应 DNS 查询。

Route 53 使用以下方法来选择运行状况良好的记录：

1. Route 53 最初根据路由策略和您为每个记录指定的值来选择记录。例如，对于加权记录，Route 53 会根据您为每个记录指定的权重选择记录。
2. Route 53 会确定记录是否运行状况良好：
   - 关联运行状况检查的非别名记录 — 如果将运行状况检查与非别名记录关联，Route 53 会检查运行状况检查的当前状态。

     Route 53 会定期检查在运行状况检查中指定的端点的运行状况；当 DNS 查询到达时，它不会执行运行状况检查。

     您可以将运行状况检查与别名记录关联，但我们建议您仅将运行状况检查与非别名记录关联。有关更多信息，请参阅 在将运行状况检查与别名记录关联时会发生什么？。
   - “评估目标运行状况”设置为“是”的别名记录 — Route 53 会检查别名记录所引用资源（例如，ELB 负载均衡器或同一托管区域中的另一记录）的运行状况。
3. 如果记录的运行状况良好，Route 53 将使用适用值（如 IP 地址）响应查询。

   如果记录运行状况不良，则 Route 53 会使用相同标准选择另一记录并重复上述流程，直到找到一个运行状况良好的记录。

Route 53 将使用以下标准选择记录：

不带运行状况检查的记录始终是运行状况良好的记录

如果具有相同名称和类型的一组记录中的某个记录没有关联的运行状况检查，Route 53 将始终认为其运行状况良好，并始终将其包含在可用的响应查询中。

如果没有运行状况良好的记录，则认为所有记录均为运行状况良好

如果一组记录中所有记录的运行状况均不良，而 Route 53 需要返回一些内容以响应 DNS 查询，但它没有了选择记录的标准。在这种情况下，Route 53 将认为该组中所有记录的运行状况都良好，并根据路由策略和为每个记录指定的值选择记录。

权重为 0 的加权记录

如果为一组加权记录中的所有记录添加运行状况检查，但为部分记录指定非零权重并为其他记录指定零权重，那么运行状况检查会按照所有记录均具有非零权重的情况进行，但下列情况除外：

- Route 53 最初仅考虑非零加权记录（如果有）。
- 如果权重大于 0 的所有记录的运行状况都不良，Route 53 会考虑零权重的记录。

由于 Route 53 在某些情况下会考虑零加权记录，因此务必确保零加权目标对 DNS 查询也有可行的答案。

有关加权记录的更多信息，请参阅 运行状况检查和加权路由。

别名记录

还可以为每个别名记录将 Evaluate Target Health (评估目标运行状况) 设置为 Yes (是)，为别名记录配置运行状况检查。此时，Route 53 会评估记录将流量路由到其中的资源 (例如，ELB 负载均衡器或同一托管区域中的另一记录) 的运行状况。

例如，假设别名记录的别名目标是一组全部具有非零权重的加权记录：

- 只要至少有一个加权记录的运行状况良好，Route 53 便认为该别名记录运行状况良好。
- 如果所有加权记录的运行状况都不良，Route 53 将认为该别名记录运行状况不良。
- Route 53 将不再考虑该树分支中的记录，直到至少有一个加权记录再次变为正常状态。

有关更多信息，请参阅 复杂 Amazon Route 53 配置中的运行状况检查的工作原理。

故障转移记录

故障转移记录的工作方式通常和其他路由类型相同。您可以创建运行状况检查并将其与非别名记录关联，然后将别名记录的 Evaluate Target Health (评估目标运行状况) 设置为 Yes (是)。请注意以下几点：

- 主记录和辅助记录都可以是非别名记录或者别名记录。

- 如果您将运行状况检查与主和辅助故障转移记录关联，下面是 Route 53 响应请求的方式：
  - 如果 Route 53 认为主记录运行状况良好（如果运行状况检查端点的运行状况良好），Route 53 将只返回主记录来响应 DNS 查询。
  - 如果 Route 53 认为主记录运行状况不佳，辅助记录运行状况良好，Route 53 将改为返回辅助记录。
  - 如果 Route 53 认为主和辅助记录的运行状况都不佳，Route 53 将返回主记录。
- 在配置辅助记录时，可添加运行状况检查，也可不添加。如果您省略用于辅助记录的运行状况检查，并且主记录的运行状况检查端点运行状况不佳，则 Route 53 始终使用辅助记录来响应 DNS 查询。即使辅助记录运行状况不良时也是如此。

有关更多信息，请参阅以下主题：

- 使用一个主资源和一个辅助资源配置主动/被动故障转移
- 使用多个主资源和多个辅助资源配置主动/被动故障转移

主动/主动和主动/被动故障转移

可以使用 Route 53 运行状况检查来配置双活和主动/被动的故障转移配置。您可以使用故障转移以外的任何路由策略 (或路由策略组合) 配置主动/被动故障转移，并使用故障转移路由策略配置主动/被动故障转移。

主题

- 主动/主动故障转移
- 主动/被动故障转移

主动/主动故障转移

如果您希望所有资源在大部分时间内都可用，可使用此故障转移配置。当某个资源不可用时，Route 53 可以检测到它运行状况不佳并且停止在响应查询时包含该资源。

在双活故障转移中，具有相同名称、相同类型（例如 A 或 AAAA）和相同路由策略（如加权或延迟）的所有记录处于活动状态，除非 Route 53 认为它们运行状况不良。Route 53 可以使用任何运行状况良好的记录响应 DNS 查询。

主动/被动故障转移

如果您希望主资源或资源组在大部分时间内可用，同时希望辅助资源或资源组处于备用状态以防所有主资源均不可用，可使用主动/被动故障转移配置。响应查询时，Route 53 将只包含运行状况良好的主资

源。如果所有主资源的运行状况都不佳，Route 53 将只在 DNS 查询的响应中包含运行状况良好的辅助资源。

主题

使用一个主资源和一个辅助资源配置主动/被动故障转移

要使用一个主记录和一个辅助记录创建主动/被动故障转移配置，只需创建相应记录并指定 Failover (故障转移) 作为路由策略。当主资源运行状况良好时，Route 53 使用主记录响应 DNS 查询。当主资源运行状况不良时，Route 53 使用辅助记录响应 DNS 查询。

使用多个主资源和多个辅助资源配置主动/被动故障转移

您还可以将多个资源与主记录和/或辅助记录关联。在使用该配置时，只要有至少一个关联资源的运行状况良好，Route 53 便认为主故障转移记录的运行状况良好。有关更多信息，请参阅 Amazon Route 53 在已配置运行状况检查时如何选择记录。

要使用多个资源为主记录或辅助记录配置主动/被动故障转移，请执行以下任务。

1. 为要将流量路由到其中的每个资源 (例如 EC2 实例或您数据中心中的 Web 服务器) 创建运行状况检查。

   > **Note**
   >
   > 如果您要将流量路由到可以为其创建别名记录的任何 Amazon 资源，不要为这些资源创建运行状况检查。在创建别名记录时，改为将 Evaluate Target Health (评估目标运行状况) 设置为 Yes (是)。

   有关更多信息，请参阅 创建和更新运行状况检查。
2. 为主资源创建记录，并指定以下值：
   - 为每个记录指定相同的名称、类型和路由策略。例如，您可以创建三个都名为 failover-primary.example.com 的 A 加权记录。
   - 如果您要使用可以为其创建别名记录的 Amazon 资源，请将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是）。

如果您要使用不能为其创建别名记录的资源，请将第 1 步中的适用运行状况检查与每个记录关联。

有关更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

3. 如果适合，则为辅助资源创建记录，并指定以下值：
   - 为每个记录指定相同的名称、类型和路由策略。例如，您可以创建三个都名为 failover-secondary.example.com 的 A 加权记录。
   - 如果您要使用可以为其创建别名记录的 Amazon 资源，请将 Evaluate Target Health（评估目标运行状况）设置为 Yes（是）。

     如果您要使用不能为其创建别名记录的资源，请将第 1 步中的适用运行状况检查与每个记录关联。

   > **Note**
   >
   > 有些客户使用 Web 服务器作为其主资源，并将配置为网站端点的 Amazon S3 存储桶作为辅助资源。S3 存储桶包含简单的“暂时不可用”消息。如果您使用该配置，可以跳过此步骤，只需为第 4 步中的辅助资源创建一个故障转移别名记录。

4. 创建一主一辅的两个故障转移别名记录，并指定以下值：

   主记录
   - 名称 — 指定希望 Route 53 用于路由流量的域名 (example.com) 或子域名 (www.example.com)。
   - 别名 — 指定 Yes（是）。
   - 别名目标 — 指定您在第 2 步中创建的记录的名称。
   - 路由策略 — 指定 Failover（故障转移）。
   - 故障转移记录类型 — 指定 Primary（主副本）。
   - 评估目标运行状况 — 指定 Yes（是）。
   - 与运行状况检查关联 — 指定 No（否）。

   辅助记录
   - 名称 — 指定为主记录指定的相同名称。
   - 别名 — 指定 Yes（是）。
   - 别名目标 — 如果为您在第 3 步中创建的辅助资源创建了记录，请指定对应记录的名称。如果您使用 Amazon S3 存储桶作为辅助资源，请指定网站端点的 DNS 名称。

- 路由策略 — 指定 Failover（故障转移）。
- 故障转移记录类型 — 指定 Secondary（辅助）。
- 评估目标运行状况 — 指定 Yes（是）。
- 与运行状况检查关联 — 指定 No（否）。

使用加权记录配置主动/被动故障转移

您还可以使用加权记录实现主动/被动故障转移，但需注意以下事项。如果为部分记录指定非零权重，为其它记录指定零权重，则 Route 53 仅使用具有非零权重且运行状况良好的记录响应 DNS 查询。如果权重大于 0 的所有记录的运行状况都不良，则 Route 53 将使用零权重记录响应查询。

> **Note**
>
> 具有非零权重的所有记录都必须处于运行状况不良的状态，然后 Route 53 才能开始使用零权重的记录响应 DNS 查询。在所有其他资源不可用，且最后一个运行状况良好的资源 (如 Web 服务器) 无法处理所有流量时，会导致您的 Web 应用程序或网站不可靠。

在私有托管区域中配置故障转移

如果要在私有托管区域中创建故障转移记录，请注意以下几点：

- Route 53 运行状况检查程序在 VPC 外部。要通过 IP 地址检查 VPC 中端点的运行状况，您必须为 VPC 中的实例分配公有 IP 地址。
- 您可以创建 CloudWatch 指标、将告警与该指标关联，然后创建基于告警数据流的运行状况检查。例如，您可以创建用于检查 EC2 `StatusCheckFailed` 指标状态的 CloudWatch 指标，向该指标添加告警，然后为该告警创建基于数据流的运行状况检查，以检查 Virtual Private Cloud (VPC) 中仅有私有 IP 地址的实例。有关使用 CloudWatch 控制台创建 CloudWatch 指标和告警的信息，请参阅 Amazon CloudWatch 用户指南。

有关更多信息，请参阅使用私有托管区和使用 CloudWatch 监控运行状况检查。

Amazon Route 53 如何避免故障转移问题

Route 53 实施的故障转移算法不仅用于将流量路由到正常运行的端点，还用于避免使灾难情况因错误配置的运行状况检查和应用程序、端点超载和分区故障而变得更严重。

主题

Amazon Route 53 如何避免级联故障

作为抵御级联故障的第一道防线，每个请求路由算法 (如加权和故障转移) 都有在万不得已的情况下采用的模式。在此特殊模式下，当所有记录都被视为运行状况不佳时，Route 53 算法将重新认为所有记录均运行良好。

例如，如果某个应用程序在多个主机上的所有实例都拒绝运行状况检查请求，Route 53 DNS 服务器无论如何都会选择一个回复，而不是不返回任何 DNS 回复或返回 NXDOMAIN（不存在的域）响应。应用程序可以响应用户，但仍无法通过运行状况检查，因此这可针对配置错误提供一些保护。

同样，如果应用程序超载并且三个端点中的一个未能通过运行状况检查，使其无法进行 Route 53 DNS 响应，Route 53 将会在其余两个端点之间分配响应。如果其余的端点无法处理额外负载并且失败，Route 53 将恢复为向全部三个端点分发请求。

Amazon Route 53 如何处理互联网分区

尽管并不常见，但有时确实存在重要的 Internet 分区，这意味着大型地理区域之间无法通过 Internet 进行通信。在这些分区中，Route 53 位置可能会就端点的运行状况状态得出不同的结论，并且可能与向 CloudWatch 报告的状态不同。每个 Amazon 区域中的 Route 53 运行状况检查程序会不断向所有 Route 53 位置发送运行状况检查状态。在互联网分区中，每个 Route 53 位置可能只能访问其中的部分状态，通常来自与其距离最近的区域。

例如，在会影响与南美洲之间双向连接的互联网分区中，Route 53 南美洲（圣保罗）位置中的 Route 53 DNS 服务器可能能够正常访问南美洲（圣保罗）Amazon 区域中的运行状况检查端点，但却无法访问其它端点。同时，美国东部（俄亥俄）中的 Route 53 可能无法访问南美洲（圣保罗）区域中的运行状况检查端点，并得出相应的记录运行状况不佳的结论。

对于此类分区，Route 53 位置更容易根据端点的本地可见性得出有关端点运行状况的不同结论。因此，当只有一部分可访问的运行状况检查程序认为端点运行正常时，每个 Route 53 位置都认为该端点运行正常。

为运行状况检查命名和添加标签

您可以向 Amazon Route 53 运行状况检查中添加标签，这些标签可为每个运行状况检查提供一个比运行状况检查 ID 更容易理解的名称。这些标签与 Amazon 账单与成本管理 提供的、用于整理 Amazon

账单的标签相同。有关将标签用于成本分配的更多信息，请参阅 Amazon Billing 用户指南中的将成本分配标签用于自定义账单报告。

每个标签都包含您定义的键 (标签的名称) 和值。为运行状况检查添加标签时，建议您添加的标签应包含键和值的下列值：

- 键 — Name（名称）
- 值 — 要为运行状况检查指定的名称

Name（名称）标签的值将显示在 Route 53 控制台的运行状况检查列表中，以便于您轻松区分各个运行状况检查。要查看一个运行状况检查的其他标签，您可以选择该运行状况检查，然后选择 Tags (标签) 选项卡。

有关标签的更多信息，请参阅以下主题：

- 要在 Route 53 控制台中添加或编辑运行状况检查时添加、编辑或删除 Name（名称）标签，请参阅创建和更新运行状况检查。
- 有关为 Route 53 资源添加标签概览，请参阅 给 Amazon Route 53 资源贴标签。

标签限制

下面是适用于标签的基本限制：

- 每个资源的最大标签数 — 新控制台上为 50 个，旧控制台上为 10 个。
- 最大 Key（键）长度 - 128 个 Unicode 字符
- 最大 Value（值）长度 - 256 个 Unicode 字符
- Key（键）和 Value（值）的有效值 — UTF-8 字符集中的大写和小写字母、数字、空格及以下字符：_ . : / = + - and @
- 标签键和值区分大小写
- 请不要对键或值使用 `aws:` 前缀；它保留供 Amazon 使用

添加、编辑和删除运行状况检查的标签

以下过程演示如何在 Route 53 控制台上对运行状况检查使用标签。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

向运行状况检查中添加标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选择要为其添加标签的运行状况检查的链接 ID。
4. 在底部页面中，选择标签选项卡，然后选择管理，再选择添加新标签。
5. 在键字段中输入标签的名称，然后在值字段中输入值。
6. 选择保存。

编辑运行状况检查的标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选择运行状况检查的链接 ID。
4. 在底部窗格中，选择标签选项卡，然后选择管理。
5. 您现在可以编辑和添加更多标签。
6. 选择保存。

删除运行状况检查的标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选择运行状况检查的链接 ID。
4. 在底部窗格中，选择标签选项卡，然后选择管理。
5. 在要删除的标签的旁边，选择删除。
6. 选择保存。

Old console

向运行状况检查中添加标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选择一个运行状况检查，或选择多个运行状况检查 (如果要向多个运行状况检查中添加相同的标签)。
4. 在底部窗格中，选择 Tags 选项卡，然后选择 Add/Edit Tags。
5. 在 Add/Edit Tags 对话框的 Key 字段中输入标签的名称，在 Value 字段中输入值。
6. 选择 Apply changes。

编辑运行状况检查的标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选择一个运行状况检查。

   如果您选择共享同一标签的多个运行状况检查，则无法同时编辑所有标签的值。但请注意，如果您选择了拥有某一标签的多个运行状况检查并且其中至少有一个运行状况检查没有该标签，则可编辑出现在这些运行状况检查中的标签的值。

例如，假设您选择多个有成本中心标签的运行状况检查和一个没有该标签的运行状况检查。您选择添加标签的选项，并指定成本中心作为键，指定 777 作为值。对于已有 Cost Center（成本中心）标签的选定运行状况检查，Route 53 将值更改为 777。对于没有 Cost Center（成本中心）标签的这个运行状况检查，Route 53 会添加一个标签并将其值设置为 777。

4. 在底部窗格中，选择 Tags 选项卡，然后选择 Add/Edit Tags。
5. 在 Add/Edit Tags 对话框中，编辑值。
6. 选择保存。

删除运行状况检查的标签

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选择一个运行状况检查，或选择多个运行状况检查 (如果要从多个运行状况检查中删除相同的标签)。
4. 在底部窗格中，选择 Tags 选项卡，然后选择 Add/Edit Tags。
5. 在 Add/Edit Tags 对话框中，选择要删除的标签旁边的 *X*。
6. 选择保存。

将运行状况检查程序与早于 2012-12-12 的 Amazon Route 53 API 版本结合使用

自 2012-12-12 版本的 Amazon Route 53 API 起，开始支持运行状况检查。如果某个托管区域包含已配置运行状况检查的记录，建议您仅使用 2012-12-12 API 或更高版本。在将运行状况检查用于早期 API 版本时，请注意以下限制。

- `ChangeResourceRecordSets` 操作无法创建或删除包括 `EvaluateTargetHealth`、`Failover` 或 `HealthCheckId` 元素的记录。
- `ListResourceRecordSets` 操作可以列出包括这些元素的记录，但这些元素不包括在输出中。响应的 `Value` 元素中包含一条消息，指出该记录包括不受支持的属性。

监控运行状况检查状态和获取通知

可在 Amazon Route 53 控制台中监控运行状况检查的状态。还可以设置 CloudWatch 告警并在运行状况检查的状态更改时自动获取通知。

主题

查看运行状况检查状态以及运行状况检查失败的原因

在 Route 53 控制台中，您可以查看 Route 53 运行状况检查程序报告的运行状况检查状态（“正常”或“不正常”）。对于除已计算的运行状况检查之外的所有运行状况检查，您还可以查看上一次运行状况检查失败”的原因，例如，运行状况检查程序无法与端点建立连接。

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

查看运行状况检查的状态和上次失败原因

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 有关所有运行状况检查的状态概览（运行状况良好或不佳），请查看 Status （状态）列。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

4. 对于除已计算的运行状况检查之外的所有运行状况检查，您可以查看正在检查指定端点的运行状况的 Route 53 运行状况检查程序的状态。
5. 选择要查看其详细信息的运行状况检查的链接 ID。
6. 在底部窗格中，选择运行状况检查程序 选项卡。

> **Note**
>
> 新的运行状况检查必须传播到 Route 53 运行状况检查程序，运行状况检查状态和上次失败原因才会出现在 Status（状态）列中。直至传播完成，该列中的消息才会对无可用状态进行说明。

7. 此表中包括以下值：

   运行状况检查程序 IP

   执行运行状况检查的 Route 53 运行状况检查程序的 IP 地址。

   上次检查

   运行状况检查的日期和时间，或上次失败的日期和时间。

   状态

   运行状况检查的当前状态或上次运行状况检查失败的原因。

Old console

查看运行状况检查的状态和上次失败原因

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 有关所有运行状况检查的状态概览（运行状况良好或不佳），请查看 Status （状态）列。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。
4. 对于除已计算的运行状况检查之外的所有运行状况检查，您可以查看正在检查指定端点的运行状况的 Route 53 运行状况检查程序的状态。选择运行状况检查。
5. 在底部窗格中，选择 Health Checkers (运行状况检查程序) 选项卡。

> **Note**
>
> 新的运行状况检查必须传播到 Route 53 运行状况检查程序，运行状况检查状态和上次失败原因才会出现在 Status（状态）列中。直至传播完成，该列中的消息才会对无可用状态进行说明。

6. 选择您要查看运行状况检查的当前状态，还是要查看上次失败的日期和时间以及失败原因。Status (状态) 选项卡上的表包含以下值：

   运行状况检查程序 IP

   执行运行状况检查的 Route 53 运行状况检查程序的 IP 地址。

   上次检查

   运行状况检查的日期和时间或上次失败的日期和时间，具体取决于您在 Status (状态) 选项卡顶部选择的选项。

   状态

   运行状况检查的当前状态或上次运行状况检查失败的原因，具体取决于您在 Status (状态) 选项卡顶部选择的选项。

监控运行状况检查程序与端点之间的延迟

如果您在创建运行状况检查时选择监控端点的状态（而不是其它运行状况检查的状态），并且您选择了 Latency graphs（延迟图表）选项，则可在 Route 53 控制台上的 CloudWatch 图表中查看以下值：

- Route 53 运行状况检查程序与端点建立 TCP 连接所用的平均时间（毫秒）
- Route 53 运行状况检查程序接收响应 HTTP 或 HTTPS 请求的第一个字节所用的平均时间（毫秒）
- Route 53 运行状况检查程序完成 SSL/TLS 握手所用的平均时间（毫秒）。

> **Note**
>
> 您不能为现有的运行状况检查启用延迟监控。

Important

状况检查程序在 16 个冗余可用区域上运行。有时，由于部署、更新、维护等原因，可用区域可能不可用。运行状况检查系统旨在解决这一问题，而避免对客户产生任何影响。

Note

我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

查看 Route 53 运行状况检查程序与端点之间的延迟

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选择要查看其指标的运行状况检查的链接 ID。您只能查看用于监控端点状态并且已启用 Latency graphs (延迟图表) 选项的运行状况检查的延迟数据。
4. 在底部窗格中，选择指标选项卡。
5. 选择要为其显示延迟图表的时间范围和地理区域。

   这些图表会显示指定时间范围的状态：

   TCP 连接时间 (仅限于 HTTP 和 TCP)

   选定地理区域中的 Route 53 运行状况检查程序与端点建立 TCP 连接所用的平均时间（毫秒）。

   到达第一个字节的时间 (仅限于 HTTP 和 HTTPS)

   选定地理区域中的 Route 53 运行状况检查程序接收响应 HTTP 或 HTTPS 请求的第一个字节所用的平均时间（毫秒）。

完成 SSL 交换的时间(仅限于 HTTPS)

选定地理区域中的 Route 53 运行状况检查程序完成 SSL/TLS 握手所用的平均时间（毫秒）。

6. 要查看大图并指定不同的设置，请选择该图右上角的三个点。您可以更改以下设置：

Statistic

更改 CloudWatch 对数据执行的计算。

时间范围：

显示不同时间段内的运行状况检查的状态，例如，隔夜或上周。

周期

更改图表中的数据点之间的间隔。

请注意以下几点：

- 如果您刚刚创建运行状况检查，可能需要等待几分钟时间，数据才会显示在图表上，运行状况检查指标才会显示在可用指标列表中。
- 该图表不会自动自行刷新。要更新显示，请选择刷新 () 图标。
- 如果出于某种原因未能通过运行状况检查（例如连接超时），Route 53 将无法测量延迟，受影响时间段的图表中将缺少延迟数据。

Old console

查看 Route 53 运行状况检查程序与端点之间的延迟

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选择相应运行状况检查对应的行。您只能查看用于监控端点状态并且已启用 Latency graphs (延迟图表) 选项的运行状况检查的延迟数据。
4. 在底部窗格中，选择 Latency (延迟) 选项卡。

5. 选择要为其显示延迟图表的时间范围和地理区域。

   这些图表会显示指定时间范围的状态：

   TCP 连接时间 (仅限于 HTTP 和 TCP)

   选定地理区域中的 Route 53 运行状况检查程序与端点建立 TCP 连接所用的平均时间（毫秒）。

   到达第一个字节的时间 (仅限于 HTTP 和 HTTPS)

   选定地理区域中的 Route 53 运行状况检查程序接收响应 HTTP 或 HTTPS 请求的第一个字节所用的平均时间（毫秒）。

   完成 SSL 交换的时间(仅限于 HTTPS)

   选定地理区域中的 Route 53 运行状况检查程序完成 SSL/TLS 握手所用的平均时间（毫秒）。

   > **Note**
   >
   > 如果您选择了多个运行状况检查，图表将为每个运行状况检查显示具有不同颜色的行。

6. 要查看更大的图表并指定不同设置，请单击图表。您可以更改以下设置：

   Statistic

   更改 CloudWatch 对数据执行的计算。

   时间范围：

   显示不同时间段内的运行状况检查的状态，例如，隔夜或上周。

   周期

   更改图表中的数据点之间的间隔。

   请注意以下几点：

   - 如果您刚刚创建运行状况检查，可能需要等待几分钟时间，数据才会显示在图表上，运行状况检查指标才会显示在可用指标列表中。

- 该图表不会自动自行刷新。要更新显示，请选择刷新
  ()
  图标。
- 如果出于某种原因未能通过运行状况检查（例如连接超时），Route 53 将无法测量延迟，受影响时间段的图表中将缺少延迟数据。

使用 CloudWatch 监控运行状况检查

Route 53 运行状况检查与 CloudWatch 指标集成，以便于您执行以下操作：

- 验证是否已正确配置运行状况检查。
- 查看运行状况检查在指定时间段内的状态。
- 将 CloudWatch 配置为在运行状况检查的状态为不正常时发送 Amazon SNS 提示。请注意，可能会在运行状况检查失败的几分钟后才会收到关联的 SNS 通知。

有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

主题

检查运行状况检查状态

> **Note**
>
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

查看运行状况检查的状态

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查。
3. 选择要查看其指标的运行状况检查的链接 ID。
4. 在底部窗格中，选择指标选项卡。

   这两个图表以一分钟间隔显示了上一小时的状态：

   运行状态检查状态

   该图表显示端点运行状况的 Route 53 评估。1 表示运行状况正常，0 表示运行状况不正常。

   报告端点正常的运行状态检查程序 (%)

   对于仅监控端点的运行状况检查，该图表显示了认为所选端点运行状况良好的 Route 53 运行状况检查程序的百分比。

   当运行状况检查已禁用，此指标不可用。

   正常子运行状况检查数

   仅适用于已计算的运行状况检查，该图表显示运行状况良好的子运行状况检查的数量。
5. 要查看大图并指定不同的设置，请选择右上角的三个点，然后选择放大。您可以更改以下设置：

   Statistic

   更改 CloudWatch 对数据执行的计算。

   时间范围：

   显示不同时间段内的运行状况检查的状态，例如，隔夜或上周。

   周期

   更改图表中的数据点之间的间隔。

   请注意以下几点：

- 如果您刚刚创建运行状况检查，可能需要等待几分钟时间，数据才会显示在图表上，运行状况检查指标才会显示在可用指标列表中。
- 该图表不会自动自行刷新。要更新显示，请选择刷新
  ()
  图标。

Old console

查看运行状况检查的状态 (新控制台)

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Health Checks (运行状况检查)。
3. 选择相应运行状况检查对应的行。
4. 在底部窗格中，选择 Monitoring (监控) 选项卡。

   这两个图表以一分钟间隔显示了上一小时的状态：

   运行状态检查状态

   该图表显示端点运行状况的 Route 53 评估。1 表示运行状况正常，0 表示运行状况不正常。

   报告端点正常的运行状态检查程序 (%)

   对于仅监控端点的运行状况检查，该图表显示了认为所选端点运行状况良好的 Route 53 运行状况检查程序的百分比。

   当运行状况检查已禁用，此指标不可用。

   正常子运行状况检查数

   仅适用于已计算的运行状况检查，该图表显示运行状况良好的子运行状况检查的数量。

   > **Note**
   >
   > 如果您选择了多个运行状况检查，图表将为每个运行状况检查显示具有不同颜色的行。

5. 要查看更大的图表并指定不同设置，请单击图表。您可以更改以下设置：

Statistic

更改 CloudWatch 对数据执行的计算。

时间范围：

显示不同时间段内的运行状况检查的状态，例如，隔夜或上周。

周期

更改图表中的数据点之间的间隔。

请注意以下几点：

- 如果您刚刚创建运行状况检查，可能需要等待几分钟时间，数据才会显示在图表上，运行状况检查指标才会显示在可用指标列表中。
- 该图表不会自动自行刷新。要更新显示，请选择刷新 () 图标。

查看运行状况检查告警

> **Note**
> 我们正在更新 Route 53 的运行状况检查控制台。在过渡期间，您可以继续使用旧控制台。

选择您正在使用的控制台的选项卡。

- 新控制台
- 旧控制台

New console

查看 CloudWatch 告警状态和编辑 Amazon Route 53 的告警

1. 在 Route 53 控制台的导航窗格中，选择运行状况检查。
2. 选择要查看其告警的运行状况检查的链接 ID。

3. 在详细信息页面的底部，选择告警选项卡。

   告警列表中包含已为所选运行状况检查创建的所有 Route 53 告警。

   State (状态) 列显示每个告警的当前状态：

   正常

   CloudWatch 已从 Route 53 运行状况检查中积累了足够的统计数据，确定端点不满足告警阈值。

   数据不足

   CloudWatch 未积累足够的统计数据来确定端点是否满足告警阈值。这是新告警的初始状态。如果 CloudWatch 指标不可用，或者您删除运行状况检查而不删除关联的告警，则告警状态也将更改为 INSUFFICIENT DATA。

   告警

   CloudWatch 已从 Route 53 运行状况检查中积累了足够的统计数据，确定端点满足告警阈值并向指定的电子邮件地址发送通知。

4. 要在 CloudWatch 控制台中查看告警，请选择告警的链接名称，控制台会提供有关告警的更多详细信息，例如，告警更新和状态更改的历史记录。您还可以在 CloudWatch 控制台上编辑告警。

5. 要在 CloudWatch 控制台上创建新的 CloudWatch 告警，请选择创建 CloudWatch 告警。有关更多信息，请参阅《CloudWatch 用户指南》中的查找和创建建议告警。

Old console

查看 CloudWatch 告警状态和编辑 Amazon Route 53 的告警

1. 在 Route 53 控制台的导航窗格中，选择 Health Checks（运行状况检查）。
2. 选择任意运行状况检查对应的行。
3. 在详细信息窗格中（在 x 运行状况检查已选定之后），选择右边三角
   ( )
   图标。

   CloudWatch 告警列表中包含已使用当前 Amazon 账户创建的所有 Route 53 告警。

   State (状态) 列显示每个告警的当前状态：

正常

CloudWatch 已从 Route 53 运行状况检查中积累了足够的统计数据，确定端点不满足告警阈值。

数据不足

CloudWatch 未积累足够的统计数据来确定端点是否满足告警阈值。这是新告警的初始状态。如果 CloudWatch 指标不可用，或者您删除运行状况检查而不删除关联的告警，则告警状态也将更改为 INSUFFICIENT DATA。

告警

CloudWatch 已从 Route 53 运行状况检查中积累了足够的统计数据，确定端点满足告警阈值并向指定的电子邮件地址发送通知。

4. 要查看或编辑告警设置，请选择告警的名称。
5. 要在 CloudWatch 控制台中查看告警，请在该告警对应的 More Options（更多选项）列中选择 View（视图），控制台会提供有关告警的更多详细信息，例如，告警更新和状态更改的历史记录。
6. 要查看您已使用当前 Amazon 账户创建的所有 CloudWatch 告警，包括用于其它 Amazon 服务的告警，请选择 View All CloudWatch Alarms（查看全部的 CloudWatch 告警）。
7. 要查看所有可用的 CloudWatch 指标（包括当前 Amazon 账户目前未使用的指标），请选择 View All CloudWatch Metrics（查看全部 CloudWatch 指标）。

在 CloudWatch 控制台上查看运行状况检查指标

要使用 CloudWatch 控制台查看 Route 53 指标

1. 登录 Amazon Web Services 管理控制台并打开 CloudWatch 控制台（https://console.aws.amazon.com/cloudwatch/）。
2. 将当前区域更改为美国东部（弗吉尼亚北部）。如果您选择其它任何区域作为当前区域，Route 53 指标将不可用。
3. 在导航窗格中，选择 Metrics (指标)。
4. 在 All metrics (所有指标) 选项卡上，选择 Route 53。
5. 选择 Health Check Metrics (运行状况检查指标)。
6. 您还可以在 CloudWatch 控制台上设置 SNS 通知。有关更多信息，请参阅《CloudWatch 用户指南》中的创建建议告警。

使用 SNS 通知创建告警

> **Note**
>
> 以下步骤仅适用于旧控制台。新控制台会将您引导至 CloudWatch 控制台创建告警。有关更多信息，请参阅《CloudWatch 用户指南》中的查找和创建建议告警。

在运行状况检查状态为运行不佳时接收 Amazon SNS 通知（旧控制台）

1. 在 Route 53 控制台的导航窗格中，选择 Health Checks（运行状况检查）。
2. 选择相应运行状况检查对应的行。
3. 在底部窗格中，选择 Alarms (告警) 选项卡。

   该表列出了已为此运行状况检查创建的告警。
4. 选择 Create Alarm (创建告警)。
5. 指定以下值：

   告警名称

   输入您希望 Route 53 在 Alarms（告警）选项卡上的 Name（名称）列中显示的名称。

   告警说明

   （可选）输入告警的描述。此值显示在 CloudWatch 控制台上。

   发送通知

   选择当此运行状况检查的状态触发告警时是否希望 Route 53 向您发送通知。

   通知目标(仅当“发送目标”为“Yes”时)

   如果您希望 CloudWatch 向现有 SNS 主题发送通知，请从列表中选择该主题。

   如果您希望 CloudWatch 发送通知，但不是向现有 SNS 主题发送，请执行以下操作之一：

   - 如果您希望 CloudWatch 发送电子邮件通知 — 选择 New SNS topic（新建 SNS 主题）并继续此过程。
   - 如果您希望 CloudWatch 通过其它方法发送通知 — 打开新的浏览器选项卡，转到 Amazon SNS 控制台，然后创建新主题。然后，返回到 Route 53 控制台，从 Notification target（通知目标）列表中选择新主题的名称，并继续执行此过程。

Topic name（仅在您选择创建新 Amazon SNS 主题时适用）

输入新 Amazon SNS 主题的名称。

Recipient email addresses（仅在您选择创建新 Amazon SNS 主题时适用）

输入在运行状况检查触发告警时希望 Route 53 将 SNS 通知发送到的电子邮件地址。

告警目标

选择您希望 Route 53 为此运行状况检查评估的值：

- Health check status（运行状况检查状态）— Route 53 运行状况检查程序报告运行状况检查为正常或不正常
- 报告端点运行正常的运行状况检查程序(%)—（仅监控端点的运行状况检查） 报告运行状况检查状态为正常的 Route 53 运行状况检查程序的百分比
- Number of healthy child health checks（正常的子运行状况检查的数量）（仅限于已计算的运行状况检查）— 已计算的运行状况检查中将运行状况检查的状态报告为正常的子运行状况检查的数量
- TCP connection time（TCP 连接时间）（仅限于 HTTP 和 TCP 运行状况检查）— Route 53 运行状况检查程序与端点建立 TCP 连接所用的时间（毫秒）
- Time to complete SSL handshake（完成 SSL 握手的时间）—（仅限于 HTTPS 运行状况检查）Route 53 运行状况检查程序完成 SSL/TLS 握手所需的时间（毫秒）
- Time to first type（第一个字节的时间）（仅限于 HTTP 和 HTTPS 运行状况检查）— Route 53 运行状况检查程序接收响应 HTTP 或 HTTPS 请求的第一个字节所用的时间（毫秒）

告警目标

对基于延迟的告警目标（TCP connection time、Time to complete SSL handshake、Time to first byte），选择您希望 CloudWatch 为特定区域还是所有区域 (Global) 中的 Route 53 运行状况检查程序计算延迟。

请注意，如果您选择一个区域，Route 53 每分钟仅测量两次延迟，样本数将比选择所有区域时小。因此，更有可能出现离群值。为防止出现虚假告警通知，建议您指定更多的连续时间段，只有这些时间段内的运行状况检查都失败，CloudWatch 才会向您发送通知。

满足条件

使用以下设置可确定 CloudWatch 应在何时触发告警。

告警目标	建议的条件	描述
运行状态检查状态	最小值 < 1	当端点运行状况不佳时，Route 53 运行状况检查程序将会报告。
报告端点正常的运行状态检查程序 (%)	平均值 < 预期百分比	仅监控端点的运行状况检查 — 当报告状态为正常的运行状况检查程序少于 18% 时，Route 53 将认为运行状况检查的状态为不正常。请勿选择此指标的 Sample Count（样本数），因为样本数的范围可能随 Route 53 添加更多运行状况检查区域而发生变化。平均值 将始终准确表示报告运行状况检查状态的检查程序的百分比。
正常子运行状况检查数	最小值 < 预期的正常子运行状况检查数	最小值 统计数据将返回最保守的值，并表示最糟糕的情况。
TCP 连接时间	平均值 > 所需时间 (毫秒)	平均值的值比其他统计数据更为一致。
完成 SSL 交换的时间	平均值 > 所需时间 (毫秒)	平均值的值比其他统计数据更为一致。
到达第一个字节的时间	平均值 > 所需时间 (毫秒)	平均值的值比其他统计数据更为一致。

连续周期至少 ***y*** 分/小时/天 ***x*** 一次

指定在多少个连续时间段内指定的值均满足标准，Route 53 才会发送通知。然后指定时间段的长度。

6. 当您选择 Create（创建）时，Amazon SNS 会向您发送一封电子邮件，其中包含有关新 SNS 主题的信息。
7. 在电子邮件中，选择 Confirm subscription（确认订阅)。您必须确认订阅，才能开始接收 CloudWatch 通知。

使用 DNS Firewall 筛选出站 DNS 流量

使用 Resolver DNS 防火墙，您可以筛选和监管虚拟私有云 (VPC) 的出站 DNS 流量。为此，您需要在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，将规则组关联到您的 VPC，然后监控 DNS Firewall 日志和指标中的活动。根据活动，您可以相应地调整 DNS Firewall 的行为。

DNS 防火墙为来自您的出站 DNS 请求提供保护 VPCs。这些请求通过 VPC 解析器进行域名解析。DNS Firewall 保护的主要用途是帮助防止数据的 DNS 泄露。当错误的参与者损害 VPC 中的应用程序实例，然后使用 DNS 查找数据并将数据从 VPC 发送到他们控制的域时，就可能会发生 DNS 泄露。使用 DNS Firewall，您可以监控和控制应用程序可以查询的域。您可以拒绝对已知不良域的访问，并允许所有其它查询通过。或者，您可以拒绝对除明确信任的域之外的所有域的访问。

您还可以使用 DNS Firewall 阻止在私有托管区域（共享或本地）中对资源（包括 VPC 终端节点名称）的解析请求。它还可以阻止对公共或私有 Amazon EC2 实例名称的请求。

DNS 防火墙是 Route 53 VPC 解析器的一项功能，不需要设置任何额外的 VPC 解析器即可使用。

Amazon Firewall Manager 支持 DNS 防火墙

您可以使用 Firewall Manager 集中配置和管理中 VPCs 各个账户的 DNS 防火墙规则组关联 Amazon Organizations。Firewall Manager 会自动添加 VPCs 属于防火墙管理器 DNS 防火墙策略范围的关联。有关更多信息，请参阅Amazon WAF Amazon Firewall Manager、和 Amazon Shield Advanced 开发者指南Amazon Firewall Manager中的。

DNS 防火墙的工作原理 Amazon Network Firewall

DNS Firewall 和 Network Firewall 都提供域名筛选，但适用于不同类型的流量。将 DNS Firewall 和 Network Firewall 相结合，您便可以通过两个不同的网络路径为应用程序层流量配置基于域的筛选。

- DNS 防火墙可筛选来自您 VPCs内部应用程序通过 Route 53 VPC 解析器的出站 DNS 查询。您还可以将 DNS Firewall 配置为向阻止的域名发送查询的自定义响应。
- Network Firewall 为网络层和应用层流量提供过滤功能，但无法查看 Route 53 VPC 解析器发出的查询。

有关 Network Firewall 的更多信息，请参阅 Network Firewall 开发人员指南。

解析器 DNS 防火墙的工作原理

Resolver DNS 防火墙允许您控制对网站的访问，并阻止通过 Route 53 VPC 解析器从您的 VPC 发出的 DNS 级威胁。使用 DNS Firewall，您可以在与您的防火墙关联的规则组中定义域名过滤规则 VPCs。您可以指定要允许或阻止的域名列表，也可以指定解析器 DNS Firewall 高级规则，以抵御基于 DNS 隧道和域生成算法 (DGA) 的威胁。您可以自定义对所阻止 DNS 查询的响应。对于包含域列表的规则，您还可以微调该规则以允许某些查询类型（例如 MX-Records）通过。

DNS Firewall 仅筛选域名。它不会将该名称解析为要阻止的 IP 地址。此外，DNS Firewall 筛选 DNS 流量，但不筛选其它应用层协议，如 HTTPS、SSH、TLS、FTP 等。

解析器 DNS 防火墙组件和设置

您可以使用以下中央组件和设置管理 DNS Firewall。

DNS Firewall 规则组

DNS Firewall 规则组是用于筛选 DNS 查询的 DNS Firewall 规则的已命名、可重复使用的集合。使用过滤规则填充规则组，然后将该规则组与一个或多个 VPCs规则组相关联。当您关联规则组与 VPC 时，您可以为 VPC 启用 DNS Firewall 过滤。然后，当 VPC 解析器收到与之关联的规则组的 VPC 的 DNS 查询时，VPC 解析器会将该查询传递给 DNS 防火墙进行筛选。

如果您将多个规则组与单个 VPC 关联，则通过每个关联中的优先级设置来指明它们的处理顺序。DNS Firewall 从最低数值优先级设置向上处理 VPC 的规则组。

有关更多信息，请参阅 DNS Firewall 规则组和规则。

DNS Firewall 规则

为 DNS Firewall 规则组中的 DNS 查询定义筛选规则。每个规则都指定一个域列表或 DNS Firewall 保护，以及对域与规则中的域规范匹配的 DNS 查询执行的操作。您可以允许（仅限带域列表的规则）、阻止匹配查询或针对其发出提醒。在包含域列表的规则中，您还可以为列表中的域指定查询类型，例如，您可以阻止或允许特定域的 MX 查询类型。您还可以为阻止的查询定义自定义响应。

对于 DNS Firewall 规则，您只能阻止匹配查询或针对其发出提醒。

规则组中的每个规则都有一个在规则组中唯一的优先级设置。DNS Firewall 将从最低设置开始，按优先级顺序处理规则组中的规则。

DNS Firewall 规则仅存在于定义这些规则的规则组上下文中。您不能独立于规则组重复使用或引用规则。

有关更多信息，请参阅 DNS Firewall 规则组和规则。

域名清单

定义用于 DNS 筛选的已命名、可重复使用的域规范集合。规则组中的每个规则都需要单一的域列表。您可以选择指定要允许访问的域、要拒绝访问的域或两者的组合。您可以创建自己的域名列表，也可以使用为您 Amazon 管理的域名列表。

有关更多信息，请参阅 解析器 DNS 防火墙域列表。

域重定向设置（仅限域列表）

通过域重定向设置，您可以配置 DNS Firewall 规则来检查 DNS 重定向链中的所有域（默认），例如 CNAME、DNAME 等，或者只检查第一个域并信任其余域。如果选择检查整个 DNS 重定向链，则必须将后续域添加到规则中设置为“ALLOW ”的域列表中。如果选择检查整个 DNS 重定向链，则必须将后续域添加到域列表中，并将其设置为需要规则采取的行动，即 ALLOW、BLOCK 或 ALERT。

有关更多信息，请参阅 DNS Firewall 中的规则设置。

查询类型（仅限域列表）

通过查询类型设置，您可以配置 DNS Firewall 规则来筛选特定的 DNS 查询类型。如果未选择查询类型，则该规则应用于所有 DNS 查询类型。例如，您可能想要阻止特定域的所有查询类型，但允许 MX 记录。

有关更多信息，请参阅 DNS Firewall 中的规则设置。

DNS Firewall Advanced 保护

根据 DNS 查询中的已知威胁签名检测可疑 DNS 查询。规则组中的每个规则都需要单一的 DNS Firewall Advanced 保护设置。您可以选择如下方面的保护：

- 域生成算法 (DGAs)

  DGAs 被攻击者用来生成大量域来发起恶意软件攻击。

- DNS 隧道

  DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

- DGA 字典

  攻击 DGAs 者使用字典通过字典单词生成域名，以逃避恶意软件 command-and-control通信中的检测。

在 DNS Firewall Advanced 规则中，您可以选择阻止与威胁匹配的查询或针对其发出提醒。威胁防护算法由管理和更新 Amazon。

有关更多信息，请参阅 解析器 DNS 防火墙高级。

置信度阈值（仅限 DNS Firewall Advanced 保护）

DNS 威胁防护的置信度阈值。创建 DNS Firewall Advanced 规则时必须提供此值。置信度值代表：

- 高 – 仅检测证实度最高的威胁，误报率低。
- 中 – 在检测威胁和误报之间保持平衡。
- 低 – 提供最高威胁检测率，但也会增加误报。

有关更多信息，请参阅 DNS Firewall 中的规则设置。

DNS Firewall 规则组与 VPC 之间的关联

使用 DNS 防火墙规则组为 VPC 定义保护，并为该 VPC 启用 VPC 解析器 DNS 防火墙配置。

如果您将多个规则组与单个 VPC 关联，则可通过关联中的优先级设置来指明它们的处理顺序。DNS Firewall 从最低数值优先级设置向上处理 VPC 的规则组。

有关更多信息，请参阅 为您的 VPC 启用解析器 DNS 防火墙保护。

VPC 的 DNS 防火墙配置

指定 VPC 解析器应如何处理 VPC 级别的 DNS 防火墙保护。只要您至少有一个与 VPC 关联的 DNS Firewall 规则组，此配置就会生效。

此配置指定了 DNS 防火墙无法过滤查询时 Route 53 VPC 解析器如何处理查询。默认情况下，如果 VPC Resolver 没有收到来自 DNS 防火墙的查询响应，则它将失败关闭并阻止查询。

有关更多信息，请参阅 DNS Firewall VPC 配置。

监控 DNS Firewall 操作

您可以使用 Amazon CloudWatch 来监控由 DNS 防火墙规则组筛选的 DNS 查询数量。CloudWatch 收集原始数据并将其处理为可读的、近乎实时的指标。

有关更多信息，请参阅 使用 Amazon 监控解析器 DNS 防火墙规则组 CloudWatch。

您可以使用 Amazon EventBridge（一种使用事件将应用程序组件连接在一起的无服务器服务）来构建可扩展的事件驱动应用程序。

有关更多信息，请参阅 使用管理解析器 DNS 防火墙事件 Amazon EventBridge。

解析器 DNS 防火墙如何过滤 DNS 查询

当 DNS 防火墙规则组与您的 VPC 的 Route 53 VPC 解析器关联时，防火墙会过滤以下流量：

- 源于该 VPC 内并通过 VPC DNS 传递的 DNS 查询。
- 通过 Resolver 端点从本地部署资源传递到具有与其解析程序关联的 DNS Firewall 的同一 VPC 的 DNS 查询。

当 DNS Firewall 收到 DNS 查询时，它会使用您配置的规则组、规则和其他设置筛选查询，并将结果发送回 VPC 解析器：

- DNS Firewall 使用与 VPC 关联的规则组评估 DNS 查询，直到找到匹配项或用尽所有规则组。DNS Firewall 按照您在关联中设置的优先级顺序评估规则组，从最低的数字设置开始。有关更多信息，请参阅DNS Firewall 规则组和规则和为您的 VPC 启用解析器 DNS 防火墙保护。
- 在每个规则组中，DNS Firewall 根据每个规则的域列表或 DNS Firewall Advanced 保护评估 DNS 查询，直到找到匹配规则或用尽所有规则。DNS Firewall 从最低数值设置开始，按优先级顺序评估规则。有关更多信息，请参阅 DNS Firewall 规则组和规则。
- 当 DNS 防火墙发现与规则的域列表匹配或 DNS 防火墙高级规则保护所识别的异常时，它会终止查询评估并向 VPC 解析器提供结果。如果操作是`alert`，则 DNS 防火墙还会向配置的 VPC 解析器日志发送警报。有关更多信息，请参阅 DNS Firewall 中的规则操作、解析器 DNS 防火墙域列表 和 解析器 DNS 防火墙高级。
- 如果 DNS Firewall 在没有找到匹配项的情况下评估所有规则组，它会照常响应查询。

VPC 解析器根据来自 DNS 防火墙的响应来路由查询。万一 DNS 防火墙无法响应，VPC 解析器会应用 VPC 配置的 DNS 防火墙故障模式。有关更多信息，请参阅 DNS Firewall VPC 配置。

使用解析器 DNS 防火墙的高级步骤

要在您的 Amazon Virtual Private Cloud VPC 中实施 Resolver DNS 防火墙筛选，请执行以下高级步骤。

- 定义您的筛选方法、域列表或 DNS Firewall 保护 — 确定要如何筛选查询，确定需要的域规范，并定义用于评估查询的逻辑。例如，您可能希望允许除已知坏域列表中的查询之外的所有查询。或者您可能想要做相反的事情，即阻止所有出批准域列表以外的域，也就是所谓的围墙花园法。您可以创

建和管理自己的已批准或屏蔽域名规范列表，也可以使用为您 Amazon 管理的域名列表。对于 DNS 防火墙保护，您可以通过屏蔽所有查询来筛选查询，也可以提醒可能包含与威胁相关的异常的域名（DGA、DNS 隧道、字典 DGA）的任何可疑查询流量，以测试您的 DNS 防火墙设置。有关更多信息，请参阅解析器 DNS 防火墙域列表和解析器 DNS 防火墙高级。

- 创建防火墙规则组 — 在 DNS Firewall 中，创建一个规则组来筛选 VPC 的 DNS 查询。您必须在要使用规则组的每个区域中创建规则组。您可能还想将过滤行为分成多个规则组，以便在不同的 VPCs 过滤场景中重复使用。有关规则组的信息，请参阅DNS Firewall 规则组和规则。
- 添加和配置规则 — 为您希望规则组提供的每个域列表和筛选行为添加规则到规则组。设置规则的优先级设置，以便它们在规则组中以正确的顺序进行处理，请为要首先评估的规则赋予最低的优先级。有关规则的信息，请参阅 DNS Firewall 规则组和规则。
- 将规则组关联到您的 VPC — 要开始使用您的 DNS Firewall 规则组，请将其与您的 VPC 关联。如果您要为 VPC 使用多个规则组，请设置每个关联的优先级，以便按正确的顺序处理规则组，请为您要首先评估的规则组提供最低的优先级。有关更多信息，请参阅 管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联。
- （可选）更改 VPC 的防火墙配置 — 如果您希望 Route 53 VPC 解析器在 DNS 防火墙无法为查询发送回响应时阻止查询，请在 VPC 解析器中更改 VPC 的 DNS 防火墙配置。有关更多信息，请参阅 DNS Firewall VPC 配置。

在多个区域使用解析器 DNS 防火墙规则组

Resolver DNS Firewall 是一项区域服务，因此您在一个 Amazon 区域中创建的对象仅在该区域可用。要在多个区域中使用同一个规则，您必须在各个区域中创建该规则。

创建规则组的 Amazon 账户可以与其他 Amazon 账户共享该规则组。有关更多信息，请参阅 在账户之间 Amazon 共享解析器 DNS 防火墙规则组。

解析器 DNS 防火墙的区域可用性

DNS 防火墙有以下几种版本 Amazon Web Services 区域：

- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（马来西亚）

- 亚太地区（墨尔本）
- 亚太地区（孟买）
- 亚太地区（大阪）区域
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（泰国）
- 亚太地区（东京）
- 加拿大（中部）区域
- 加拿大西部（卡尔加里）
- 欧洲地区（法兰克福）区域
- 欧洲地区（爱尔兰）区域
- 欧洲地区（伦敦）区域
- 欧洲地区（米兰）
- 欧洲地区（巴黎）区域
- 欧洲地区（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 墨西哥（中部）
- 中东（巴林）
- 中东（阿联酋）
- 南美洲（圣保罗）
- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈州）
- 中国（北京）
- 中国（宁夏）

- Amazon GovCloud (US)

解析器 DNS 防火墙入门

DNS Firewall 控制台提供有向导，引导您完成开始使用 DNS Firewall 的以下步骤：

- 为要使用的每组规则创建规则组。
- 对于每个规则，填充要检查的域列表。您可以创建自己的域名列表，也可以使用 Amazon 托管域名列表。
- 将您的规则组与您想要使用它们 VPCs 的地方相关联。

解析器 DNS 防火墙围墙花园示例

在本教程中，您将创建一个规则组，该规则组会阻止除您信任的选定域组以外的所有域。这就是所谓的封闭平台，或称围墙花园法。

要使用控制台向导配置 DNS Firewall 规则组

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 3。

   - 或者 -

   登录 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。
4. 在 Rule groups（规则组）页面上，选择 Add rule group（添加规则组）。
5. 对于规则组名称，输入 **`WalledGardenExample`**。

   在标签部分，可以选择输入标签的键-值对。标签可帮助您组织和管理 Amazon 资源。有关更多信息，请参阅 给 Amazon Route 53 资源贴标签。
6. 选择添加规则组。

7. 在WalledGardenExample详细信息页面上，选择规则选项卡，然后选择添加规则。
8. 在规则详细信息窗格中，输入规则名称 **BlockAll**。
9. 在 Domain list（域列表）窗格上，选择 Add my own domain list（添加我自己的域列表）。
10. 在 Choose or create a new domain list（选择或创建新的域列表）中选择 Create new domain（创建新域列表）。
11. 输入域名列表名称**AllDomains**，然后在每行输入一个域名文本框中，输入星号:*****。
12. 对于域重定向设置，可接受默认设置，并将“查询类型-可选”留空。
13. 对于操作，请选择阻止，然后将响应保留在原定设置 NODATA 状态下等待发送。
14. 选择添加规则。您的规则显示在WalledGardenExample页面BlockAll的 “规则” 选项卡中。
15. 在WalledGardenExample页面上，选择添加规则以向您的规则组添加第二条规则。
16. 在规则详细信息窗格中，输入规则名称 **AllowSelectDomains**。
17. 在 Domain list（域列表）窗格上，选择 Add my own domain list（添加我自己的域列表）。
18. 在 Choose or create a new domain list（选择或创建新的域列表）项下，选择 Create new domain list（创建新域列表）。
19. 输入域列表名称 **ExampleDomains**。
20. 在每行输入一个域文本框的第一行中，输入 **example.com**，然后在第二行输入 **example.org**。

    > **Note**
    >
    > 如果希望此规则也应用于子域，则需要将这些域添加到列表中。例如，要添加示例 .com 的所有子域，请将 ***.example.com** 添加到列表中。

21. 对于域重定向设置，可接受默认设置，并将“查询类型-可选”留空。
22. 对于操作，请选择允许。
23. 选择添加规则。您的规则都显示在WalledGardenExample页面的 “规则” 选项卡中。
24. 在该WalledGardenExample页面的 “规则” 选项卡中，您可以通过选择 “优先级” 列中列出的数字并键入新数字来调整规则组中规则的评估顺序。DNS Firewall 从最低优先级设置开始评估规则，因此优先级最低的规则将第一个评估。在此示例中，我们希望 DNS Firewall 首先识别并允许对选定的域列表进行 DNS 查询，然后阻止任何剩余的查询。

    调整规则优先级，使其AllowSelectDomains具有较低的优先级。

现在，您有了一个只允许通过特定域查询的规则组。要开始使用它，请将其与要使用筛选行为 VPCs 的地点相关联。有关更多信息，请参阅 管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联。

解析器 DNS 防火墙屏蔽列表示例

在本教程中，您将创建一个规则组，用于阻止已知为恶意域。您还将为阻止列表中的域添加一个允许的 DNS 查询类型。规则组允许通过 VPC 解析器发出所有其他出站 DNS 请求。

要使用控制台向导配置 DNS Firewall 阻止列表

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 3。

   - 或者 -

   登录 Amazon Web Services 管理控制台 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。
4. 在 Rule groups（规则组）页面上，选择 Add rule group（添加规则组）。
5. 对于规则组名称，输入 **`BlockListExample`**。

   在标签部分，可以选择输入标签的键-值对。标签可帮助您组织和管理 Amazon 资源。有关更多信息，请参阅 给 Amazon Route 53 资源贴标签。
6. 在BlockListExample详细信息页面上，选择规则选项卡，然后选择添加规则。
7. 在规则详细信息窗格中，输入规则名称 **`BlockList`**。
8. 在 Domain list（域列表）窗格上，选择 Add my own domain list（添加我自己的域列表）。
9. 在 Choose or create a new domain list（选择或创建新的域列表）项下，选择 Create new domain list（创建新域列表）。
10. 输入域名列表名称 **`MaliciousDomains`**，然后在文本框中输入要阻止的域。例如 **`example.org`**。每行输入一个域。

    > **Note**
    >
    > 如果希望此规则也应用于子域，则必须将这些域添加到列表中。例如，要添加示例 .org 的所有子域，请将 **`*.example.org`** 添加到列表中。

11. 对于域重定向设置，可接受默认设置，并将“查询类型-可选”留空。
12. 对于操作，请选择 BLOCK（阻止），然后将响应保留在原定设置 NODATA 状态下等待发送。
13. 选择添加规则。您的规则显示在BlockListExample页面的 “规则” 选项卡中
14. 在该BlockedListExample页面的规则选项卡中，您可以通过选择 “优先级” 列中列出的数字并键入新数字来调整规则组中规则的评估顺序。DNS Firewall 从最低优先级设置开始评估规则，因此优先级最低的规则将第一个评估。

    选择并调整规则优先级，以便BlockList在您可能拥有的任何其他规则之前或之后对其进行评估。大多数情况下，应首先阻止已知的恶意域。也就是说，与它们关联的规则应具有最低的优先级编号。
15. 要添加允许 BlockList 域名的 MX 记录的规则，请在规则选项卡的BlockedListExample详细信息页面上，选择添加规则。
16. 在规则详细信息窗格中，输入规则名称 **`BlockList-allowMX`**。
17. 在 Domain list（域列表）窗格上，选择 Add my own domain list（添加我自己的域列表）。
18. 在选择或创建新的域列表项下，选择 **`MaliciousDomains`**。
19. 对于域重定向设置，可接受默认设置。
20. 在 DNS 查询类型列表中，选择 MX：指定邮件服务器。
21. 对于操作，请选择 ALLOW（允许）。
22. 选择添加规则。
23. 在该BlockedListExample页面的规则选项卡中，您可以通过选择 “优先级” 列中列出的数字并键入新数字来调整规则组中规则的评估顺序。DNS Firewall 从最低优先级设置开始评估规则，因此优先级最低的规则将第一个评估。

    选择并调整规则优先级，以便在您可能拥有的任何其他规则之前或之后评估 BlockList-allowMX。由于要允许 MX 查询，因此请确保 BlockList-allowMx 规则的优先级低于。BlockList

您现在拥有一个阻止特定恶意域查询，但允许特定 DNS 查询类型的规则组。要开始使用它，请将其与要使用筛选行为 VPCs的地点相关联。有关更多信息，请参阅 管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联。

DNS Firewall 规则组和规则

本节介绍您可以为 DNS 防火墙规则组和规则配置的设置，以定义您的 DNS 防火墙行为 VPCs。它还介绍了如何管理规则组和规则的设置。

按照需要的方式配置规则组后，您可以直接使用它们，并且您可以在 Amazon Organizations的各个账户和组织之间共享和管理这些规则组。

- 您可以将一个规则组与多个规则组相关联 VPCs，以便在整个组织中提供一致的行为。有关信息，请参阅管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联。
- 您可以在账户之间共享规则组，从而在整个组织中实现一致的 DNS 查询管理。有关信息，请参阅在账户之间 Amazon 共享解析器 DNS 防火墙规则组。
- 您可以通过在 Amazon Firewall Manager 策略中管理规则组 Amazon Organizations 来在整个组织中使用规则组。有关 Firewall Manager 的信息，请参阅Amazon WAF Amazon Firewall Manager、和 Amazon Shield Advanced 开发者指南Amazon Firewall Manager中的。

DNS Firewall 中的规则组设置

创建或编辑 DNS Firewall 规则组时，您指定以下值：

Name

通过唯一名称可在控制面板上轻松找到规则组。

（可选）描述

为规则组提供更多上下文的简短描述。

Region

您在创建规则组时选择的 Amazon 区域。您在一个区域中创建的规则组仅在该区域中可用。要在多个区域中使用同一个规则，您必须在各个区域中创建该规则。

Rules

规则组筛选行为包含在其规则中。有关信息，请参阅以下部分。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签。有关对成本分配使用标签的更多信息，请参阅 Amazon Billing 用户指南中的使用成本分配标签。

DNS Firewall 中的规则设置

创建或编辑 DNS Firewall 规则组时，您指定以下值：

Name

用于规则组中规则的唯一标识符。

（可选）描述

提供有关规则的更多信息的简短描述。

域名清单

规则检查的域列表。您可以创建和管理自己的域列表，也可以订阅 Amazon 为您管理的域列表。有关更多信息，请参阅 解析器 DNS 防火墙域列表。

规则可以包含域列表或 DNS Firewall Advanced 保护，但不能同时包含两者。

域重定向设置（仅限域列表）

您可以选择让 DNS Firewall 规则仅检查 DNS 重定向链中的第一个域或所有（默认）域，比如 CNAME、DNAME 等。如果选择检查所有域，则必须将 DNS 重定向链中的后续域添加到域列表中，并将其设置为需要规则采取的行动，即 ALLOW、BLOCK 或 ALERT。有关更多信息，请参阅 解析器 DNS 防火墙组件和设置。

查询类型（仅限域列表）

此规则检查的 DNS 查询类型列表。有效值如下所示：

- 答：返回 IPv4 地址。
- AAAA：返回 IPv6 地址。
- CAA： CAs 可以为域名创建 SSL/TLS 认证的限制。
- CNAME：返回另一个域名。
- DS：标识委派区域 DNSSEC 签名密钥的记录。
- MX：指定邮件服务器。
- NAPTR： Regular-expression-based重写域名。
- NS：权威名称服务器。
- PTR：将 IP 地址映射到域名。
- SOA：此区的授权起始点记录。
- SPF：列出有权从某个域发送电子邮件的服务器。

- SRV：用于标识服务器的特定应用程序值。
- TXT：验证电子邮件发件人和特定应用程序的值。
- 您使用 DNS 类型 ID 定义的查询类型，例如 AAAA 的类型为 28。这些值必须定义为 TYPE *NUMBER*，其中*NUMBER*可以是 1-65334，例如，。 TYPE28有关更多信息，请参阅 DNS 记录类型列表。

  您可以为每条规则创建一个查询类型。

  > **Note**
  >
  > 如果您设置的防火墙阻止规则的操作为 NXDOMAIN 查询类型等于 AAAA，则此操作将不会应用于启用时生成的合成 IPv6 地址。 DNS64

DNS Firewall Advanced 保护

根据 DNS 查询中的已知威胁签名检测可疑 DNS 查询。您可以选择如下方面的保护：

- 域生成算法 (DGAs)

  DGAs 被攻击者用来生成大量域来发起恶意软件攻击。

- DNS 隧道

  DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

- DGA 字典

  攻击 DGAs 者使用字典通过字典单词生成域名，以逃避恶意软件command-and-control 通信中的检测。

在 DNS Firewall Advanced 规则中，您可以选择阻止与威胁匹配的查询或针对其发出提醒。

有关更多信息，请参阅 解析器 DNS 防火墙高级。

规则可以包含 DNS Firewall Advanced 保护或域列表，但不能同时包含两者。

置信度阈值（仅限 DNS Firewall Advanced）

DNS Firewall Advanced 的置信度阈值。创建 DNS Firewall Advanced 规则时必须提供此值。置信度值代表：

- 高 – 仅检测证实度最高的威胁，误报率低。
- 中 – 在检测威胁和误报之间保持平衡。

- 低 – 提供最高威胁检测率，但也会增加误报。

有关更多信息，请参阅 DNS Firewall 中的规则设置。

Action

您希望 DNS Firewall 如何处理域名与规则域列表中的规范匹配的 DNS 查询。有关更多信息，请参阅 DNS Firewall 中的规则操作。

优先级

规则组中唯一确定处理顺序的正整数设置。DNS Firewall 根据规则组中的规则检查 DNS 查询，从最低数值优先级设置开始并向上检查。您可以随时更改规则的优先级，例如更改处理顺序或为其它规则留出空间。

DNS Firewall 中的规则操作

当 DNS Firewall 在规则中找到 DNS 查询与域规范之间的匹配时，它会将规则中指定的操作应用于查询。

您需要在创建的每条规则中指定下列选项之一：

- Allow— 停止检查查询并允许其通过。不适用于 DNS Firewall Advanced。
- Alert— 停止检查查询，允许其通过，并在 Route 53 VPC 解析器日志中记录查询警报。
- Block— 停止检查查询，阻止其前往其预期目的地，并将该查询的阻止操作记录在 Route 53 VPC 解析器日志中。

  回复已配置的阻止响应，具体如下：

  - NODATA— 响应表示查询成功，但没有可用的响应。
  - NXDOMAIN— 响应表示查询的域名不存在。
  - OVERRIDE— 在响应中提供自定义替换。此选项需要以下额外设置：
    - Record value— 为响应查询而发送回的自定义 DNS 记录。
    - Record type— DNS 记录的类型。这决定了记录值的格式。必须是 CNAME。
    - Time to live in seconds— DNS 解析器或 Web 浏览器缓存覆盖记录并使用它来响应此查询的建议时间（如果再次收到该查询）。预设情况下，此值为零，并且记录不会被缓存。

有关查询日志配置和内容的更多信息，请参阅 Resolver 查询日志记录 和 VPC 解析器查询日志中显示的值。

使用 Alert 测试阻止规则

首次创建阻止规则时，可以通过将操作设置为 Alert 以进行测试。然后，您可以查看规则提示的查询数，以查看如果将操作设置为 Block，将会阻止多少查询。

管理 DNS Firewall 中的规则组和规则

要在控制台中管理规则组和规则，请按照本节中的指导操作。

当您对 DNS Firewall 实体（如规则和域列表）进行更改时，DNS Firewall 会在存储和使用实体的任何位置传播更改。您的更改将在几秒钟内应用，但是当更改到达某些位置但没有到达其它剩余位置时，可能会短暂地出现不一致的情况。因此，如果您将域添加到阻止规则引用的域列表中，则新域可能会在 VPC 的一个区域中暂时被阻止，而在另一个区域中仍然被允许。当您首次配置规则组和 VPC 关联并更改现有设置时，可能会出现这种临时不一致的情况。通常而言，这种类型的任何不一致情况都只会持续几秒钟。

创建规则组和规则

要创建规则组并向其添加规则，请按照此过程中的步骤操作。

要创建规则组及其规则

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 3。

   - 或者 -

   登录到 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。
4. 选择 Add rule group（添加规则组），然后按照向导指导来指定您的规则组和规则设置。

   有关规则组的值的信息，请参阅 DNS Firewall 中的规则组设置。

   有关规则的值的信息，请参阅 DNS Firewall 中的规则设置。

查看和更新规则组和规则

使用以下过程查看规则组以及分配给规则组的规则。您也可以更新规则组和规则设置。

要查看和更新规则组

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 3。

   - 或者 -

   登录到 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。
4. 选择要查看或编辑的规则组，然后选择 View details（查看详细信息）。
5. 在规则组的页面中，您可以查看和编辑设置。

   有关规则组的值的信息，请参阅 DNS Firewall 中的规则组设置。

   有关规则的值的信息，请参阅 DNS Firewall 中的规则设置。

删除规则组

要删除规则组，请执行以下步骤。

> **Important**
>
> 如果您删除与 VPC 关联的规则组，DNS Firewall 将删除该关联并停止该规则组向 VPC 提供的保护。

删除 DNS Firewall 实体

当您删除可以在 DNS Firewall 中使用的实体（例如规则组中可能正在使用的域列表或可能与 VPC 关联的规则组）时，DNS Firewall 将检查该实体当前是否正在使用。如果发现它正在使用，DNS Firewall

会警告您。DNS Firewall 几乎每次都能确定实体是否正在使用中。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在 DNS Firewall 配置中进行检查。如果实体是引用的域列表，请检查是否有规则组正在使用它。如果实体是规则组，请检查它是否与任何规则组关联 VPCs。

删除规则组

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 3。

   - 或者 -

   登录到 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。
4. 选择要删除的规则组，然后选择删除，并确认删除。

解析器 DNS 防火墙域列表

域列表是您在规则组内的 DNS Firewall 规则中使用的一组可重复使用的域规范。当您关联规则组与 VPC 时，DNS Firewall 会将您的 DNS 查询与规则中使用的域列表进行比较。如果找到匹配项，则会根据匹配规则的操作处理 DNS 查询。有关规则组和规则的更多信息，请参阅 DNS Firewall 规则组和规则。

域列表允许您将显式域规范与要对其执行的操作分开。您可以在多个规则中使用单个域列表，对域列表执行的任何更新都会自动影响使用该列表的所有规则。

域列表分为两大类：

- 托管域名列表， Amazon 可为您创建和维护。
- 您自己的域列表，将由您自己创建和维护列表。

本部分介绍可供您使用的托管域列表的类型，并提供有关创建和管理自己的域列表（如果您选择这样做）的指导。

托管域列表

托管域列表包含与恶意活动或其他潜在威胁相关的域名。 Amazon 维护这些列表是为了让 Route 53 VPC 解析器客户在使用 DNS 防火墙时能够免费检查出站 DNS 查询。

随时了解不断变化的威胁情形会非常耗时且成本高昂。当您实施和使用 DNS 防火墙时，托管域列表可以为您节省时间。 Amazon 当出现新的漏洞和威胁时，会自动更新列表。 Amazon 通常会在公开披露之前收到有关新漏洞的通知，因此 DNS Firewall 可以经常在新威胁广为人知之前为您部署缓解措施。

托管域列表旨在帮助保护您免受常见的 Web 威胁，并为您的应用程序添加另一层安全保护。 Amazon 托管域列表的数据既来自内部 Amazon 来源，也来自内部来源 RecordedFuture，并且会不断更新。但是， Amazon 托管域列表并不是用来替代其他安全控制措施，例如 Amazon GuardDuty，这些控制由您选择的 Amazon 资源决定。

最佳实践是在生产环境中使用托管域列表之前，请在非生产环境中对其进行测试，并将规则操作设置为 `Alert`。使用 Amazon CloudWatch 指标以及解析器 DNS 防火墙采样请求或 DNS 防火墙日志来评估规则。如果您对规则执行操作的情况感到满意，请根据需要更改操作设置。

可用的 Amazon 托管域名列表

本部分介绍当前可用的 托管域列表。当您位于支持这些列表的区域时，在您管理域列表以及为规则指定域列表时，便可以在控制台上看到这些域列表。在日志中，域列表记录在 `firewall_domain_list_id field` 中。

Amazon 为所有使用 Resolver DNS Firewall 的用户提供以下托管域列表（按可用区域划分）。

- `AWSManagedDomainsMalwareDomainList`— — 与发送恶意软件、托管恶意软件或分发恶意软件关联的域。
- `AWSManagedDomainsBotnetCommandandControl` — 与控制感染垃圾邮件恶意软件的计算机网络相关联的域。
- `AWSManagedDomainsAggregateThreatList`— 与多个 DNS 威胁类别（包括恶意软件、勒索软件、僵尸网络、间谍软件和 DNS 隧道）关联的域名，可帮助阻止多种类型的威胁。`AWSManagedDomainsAggregateThreatList`包括此处列出的其他 Amazon 托管域列表中的所有域。
- `AWSManagedDomainsAmazonGuardDutyThreatList`— 与 Amazon GuardDuty DNS 安全调查结果相关的域名。这些域名仅来自 GuardDuty的威胁情报系统，不包含来自外部第三

方来源的域名。更具体地说，目前此列表将仅屏蔽内部生成并用于以下检测的域：影响：/。声誉、影响：/。声誉、影响：EC2/AbusedDomainRequest。声誉、影响 GuardDuty：/.声誉、影响：.Repution、Impact：EC2BitcoinDomainRequest.Repution、Impact：EC2MaliciousDomainRequest.Repution。Runtime/AbusedDomainRequest.Reputation, Impact:Runtime/BitcoinDomainRequest.Reputation, and Impact:Runtime/MaliciousDomainRequest

有关更多信息，请参阅 Amazon GuardDuty 用户指南中的查找类型。

Amazon 无法下载或浏览托管域名列表。为了保护知识产权，您无法查看或编辑 Amazon 托管域列表中的各个域名规范。此限制还有助于避免恶意用户设计专门避开已发布列表的威胁。

测试托管域列表

我们提供以下一组域用于测试托管域名列表：

AWSManagedDomainsBotnetCommandandControl

- controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsMalwareDomainList

- controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsAggregateThreatList 和 AWSManaged DomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

如果这些域未被屏蔽，它们将解析为 1.2.3.4。如果您在 VPC 中使用托管域列表，则查询这些域将返回规则中的屏蔽操作设置为（例如 NODATA）的响应。

有关托管域列表的更多信息，请联系 Amazon Web Services 支持 中心。

下表列出了 Amazon 托管域列表的区域可用性。

托管域列表区域可用性

Region	托管域列表是否可用？
非洲（开普敦）	是
亚太地区（香港）	是
亚太地区（海得拉巴）	是
亚太地区（雅加达）	是
亚太地区（马来西亚）	是
亚太地区（墨尔本）	是
亚太地区（孟买）	是
亚太地区（大阪）区域	是
亚太地区（首尔）	是
亚太地区（新加坡）	是
亚太地区（悉尼）	是
亚太地区（泰国）	是
亚太地区（东京）	是
加拿大（中部）区域	是

Region	托管域列表是否可用？
加拿大西部（卡尔加里）	是
欧洲地区（法兰克福）区域	是
欧洲地区（爱尔兰）区域	是
欧洲地区（伦敦）区域	是
欧洲地区（米兰）	是
欧洲地区（巴黎）区域	是
欧洲地区（西班牙）	是
欧洲地区（斯德哥尔摩）	是
欧洲（苏黎世）	是
以色列（特拉维夫）	是
中东（巴林）	是
中东（阿联酋）	是
南美洲（圣保罗）	是
美国东部（弗吉尼亚州北部）	是
美国东部（俄亥俄州）	是

Region	托管域列表是否可用？
美国西部（北加利福尼亚）	是
美国西部（俄勒冈州）	是
中国（北京）	是
中国（宁夏）	支持
Amazon GovCloud (US)	是

其它安全注意事项

Amazon 托管域列表旨在帮助保护您免受常见网络威胁的侵害。应根据文档使用这些列表，它为您的应用程序添加另一层安全性。但是，托管域列表并非用于取代其他安全控制措施，这些控制措施由您所选择的 Amazon 资源决定。为确保您的资源 Amazon 得到适当保护，请参阅责任共担模型中的指南。

减少误报情况

如果您在使用 托管域列表阻止查询的规则中遇到误报情况，请执行以下步骤：

1. 在 VPC Resolver 日志中，确定导致误报的规则组和托管域列表。您可以通过查找 DNS Firewall 阻止但您希望允许通过的查询日志来执行此操作。日志记录列出了规则组、规则操作和托管列表。有关日志的更多信息，请参阅 VPC 解析器查询日志中显示的值。
2. 在规则组中创建一个新规则，明确允许被阻止的查询通过。创建规则时，您可以使用您希望允许的域规范定义自己的域列表。要遵循有关规则组和规则管理的指导，请访问 创建规则组和规则。
3. 确定规则组内新规则的优先级，使其在使用托管列表的规则之前运行。若要执行此操作，请为新规则提供较低的数字优先级设置。

更新了规则组后，新规则将在阻止规则运行之前明确允许您希望允许使用的域名。

管理您自己的域列表

您可以创建自己的域列表，以指定托管域列表产品中没有找到或您希望自行处理的域类别。

除了本节所述的步骤外，在创建或更新规则时，还可以在控制台中在 Resolver DNS Firewall 规则管理环境中创建域列表。

域列表中的每个域规范必须满足以下要求：

- 它可以选择从 *（星号）开始。
- 除了可选的起始星号和句点作为标签之间的分隔符外，它只能包含以下字符：、A-Z、a-z0-9、-（连字符）。
- 它的长度必须介于 1 到 255 个字符之间。

当您对 DNS Firewall 实体（如规则和域列表）进行更改时，DNS Firewall 会在存储和使用实体的任何位置传播更改。您的更改将在几秒钟内应用，但是当更改到达某些位置但没有到达其它剩余位置时，可能会短暂地出现不一致的情况。因此，如果您将域添加到阻止规则引用的域列表中，则新域可能会在 VPC 的一个区域中暂时被阻止，而在另一个区域中仍然被允许。当您首次配置规则组和 VPC 关联并更改现有设置时，可能会出现这种临时不一致的情况。通常而言，这种类型的任何不一致情况都只会持续几秒钟。

在生产环境中使用域列表之前对其进行测试

最佳实践是在生产环境中使用域列表之前，请在非生产环境中对其进行测试，并将规则操作设置为 Alert。使用 Amazon CloudWatch 指标和 VPC 解析器日志评估规则。日志为所有提示和阻止操作提供域列表名称。如果您对域列表与您的 DNS 查询的匹配情况感到满意，请根据需要更改规则操作设置。有关 CloudWatch 指标和查询日志的信息，请参阅使用 Amazon 监控解析器 DNS 防火墙规则组 CloudWatchVPC 解析器查询日志中显示的值、和管理 Resolver 查询日志记录配置。

要添加域列表

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。继续执行步骤 2。

   - 或者 -

   登录到 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在导航窗格中的 DNS 防火墙下，选择域列表。在 Domain list（域列表）页上，您可以选择并编辑现有域列表，也可以添加自己的域列表。
3. 要添加域列表，请选择 Add domain list（添加域列表）。
4. 为您的域列表提供一个名称，然后在文本框中输入域规范，每行一个。

   如果您将 Switch to bulk upload（切换到批量上载）切换为 on（开启），输入您创建域列表所在的 Amazon S3 存储桶 URI。此域列表每行应有一个域名。

   > **Note**
   >
   > 重复的域名会导致批量导入失败。

5. 选择 Add domain list（添加域列表）。Domain lists（域列表）页面会列出您的新域列表。

创建域列表后，您可以从 DNS Firewall 规则中按名称引用域列表。

删除 DNS Firewall 实体

当您删除可以在 DNS Firewall 中使用的实体（例如规则组中可能正在使用的域列表或可能与 VPC 关联的规则组）时，DNS Firewall 将检查该实体当前是否正在使用。如果发现它正在使用，DNS Firewall 会警告您。DNS Firewall 几乎每次都能确定实体是否正在使用中。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在 DNS Firewall 配置中进行检查。如果实体是引用的域列表，请检查是否有规则组正在使用它。如果实体是规则组，请检查它是否与任何规则组关联 VPCs。

要删除域列表

1. 在导航窗格中，选择 Domain lists（域列表）。
2. 在导航栏中，选择域列表的区域。
3. 选择要删除的域名列表，然后选择删除，并确认删除。

解析器 DNS 防火墙高级

DNS Firewall Advanced 根据 DNS 查询中的已知威胁签名检测可疑 DNS 查询。您可以指定规则中的威胁类型，在规则组内的 DNS Firewall 规则中使用该类型。当您关联规则组与 VPC 时，DNS Firewall 会将您的 DNS 查询与规则中标记的域进行比较。如果找到匹配项，则会根据匹配规则的操作处理 DNS 查询。

DNS Firewall Advanced 的工作原理是通过检查 DNS 有效载荷中的一系列关键标识符来识别可疑的 DNS 威胁特征，包括请求的时间戳、请求和响应的频率、DNS 查询字符串以及出站和入站 DNS 查询的长度、类型或大小。根据威胁签名的类型，您可以配置要阻止的策略，或者直接对查询进行记录和提醒。通过使用一组扩展的威胁标识符，您可以防范来自域来源的 DNS 威胁，这些域来源可能尚未被更广泛的安全社区维护的威胁情报源分类。

目前，DNS Firewall Advanced 提供以下保护：

- 域生成算法 (DGAs)

  DGAs 被攻击者用来生成大量域来发起恶意软件攻击。

- DNS 隧道

  DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

- DGA 字典

  攻击 DGAs 者使用字典通过字典单词生成域名，以逃避恶意软件 command-and-control通信中的检测。

要了解如何创建规则，请参阅 创建规则组和规则 和 DNS Firewall 中的规则设置。

减少误报情况

如果您在使用 DNS Firewall Advanced 保护阻止查询的规则中遇到误报情况，请执行以下步骤：

1. 在 VPC 解析器日志中，确定导致误报的规则组和 DNS 防火墙高级保护。您可以通过查找 DNS Firewall 阻止但您希望允许通过的查询日志来执行此操作。日志记录列出了规则组、规则操作和 DNS Firewall Advanced 保护。有关日志的更多信息，请参阅 VPC 解析器查询日志中显示的值。
2. 在规则组中创建一个新规则，明确允许被阻止的查询通过。创建规则时，您可以使用您希望允许的域规范定义自己的域列表。要遵循有关规则组和规则管理的指导，请访问 创建规则组和规则。
3. 确定规则组内新规则的优先级，使其在使用托管列表的规则之前运行。若要执行此操作，请为新规则提供较低的数字优先级设置。

更新了规则组后，新规则将在阻止规则运行之前明确允许您希望允许使用的域名。

为 DNS Firewall 配置日志记录

您可以使用 Amazon CloudWatch 指标和解析器查询日志来评估您的 DNS 防火墙规则。日志为所有提示和阻止操作提供域列表名称。有关 Amazon 的更多信息 CloudWatch，请参阅使用 Amazon 监控解析器 DNS 防火墙规则组 CloudWatch。

启用 DNS Firewall 后，将其关联到 VPC，并且您已启用日志记录，`firewall_rule_group_id`、`firewall_rule_action` 和 `firewall_domain_list_id`是日志中提供的 DNS Firewall 特定字段。

> **Note**
>
> 查询日志将仅显示 DNS 防火墙规则阻止的查询的其他 DNS 防火墙字段。

要开始记录源自您的 DNS 防火墙规则筛选的 DNS 查询 VPCs，请在 Amazon Route 53 控制台中执行以下任务：

要为 DNS Firewall 配置 Resolver 查询日志记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 展开 Route 53 控制台菜单。在控制台的左上角，选择三个水平条（ ☰ ）图标。
3. 在 Resolver 菜单中，选择 Query logging（查询日志记录）。
4. 在区域选择器中，选择要在其中创建查询日志配置的 Amazon 区域。

   该区域必须与您创建的、与 DNS 防火墙关联且要记录查询的区域相同。 VPCs 如果您有 VPCs 多个区域，则必须为每个区域创建至少一个查询日志配置。
5. 选择 Configure query logging（配置查询日志记录）。
6. 指定以下值：

   查询日志记录配置名称

   为查询日志记录配置输入名称。名称会显示在控制台的查询日志配置列表中。输入名称将有助于以后查找此配置。

查询日志的目标保存位置

选择您希望 VPC 解析器向其发送查询日志的 Amazon 资源类型。有关如何在选项（CloudWatch 日志组、S3 存储桶和 Firehose 传输流）中进行选择的信息，请参阅。Amazon 您可以向其发送 VPC 解析器查询日志的资源

选择资源类型后，您可以创建该类型的另一个资源，也可以选择由当前 Amazon 账户创建的现有资源。

> **Note**
>
> 您只能选择在步骤 4 选择的 Amazon 区域中创建的资源，也即您创建查询日志记录配置的区域。如果您选择创建新资源，则该资源将在同一区域创建。

VPCs 记录以下各项的查询

此查询日志配置将记录源自您选择的 DNS 查询。 VPCs 选中当前区域中您希望 VPC 解析器记录查询的每个 VPC 的复选框，然后选择选择。

> **Note**
>
> 对于特定目标类型，VPC 日志传输只能启用一次。日志无法传输到同一类型的多个目标。例如，无法将 VPC 日志传输到两个 Amazon S3 目标。

7. 选择 Configure query logging（配置查询日志记录）。

> **Note**
>
> 您应在成功创建查询日志配置后数分钟内开始在日志中看到 VPC 中的资源执行的 DNS 查询。

在账户之间 Amazon 共享解析器 DNS 防火墙规则组

您可以在 Amazon 账户之间共享 DNS 防火墙规则组。要共享规则组，请使用 Amazon Resource Access Manager (Amazon RAM)。DNS 防火墙控制台与 Amazon RAM 控制台集成。有关的更多信息 Amazon RAM，请参阅 Resource A ccess Manager 用户指南。

注意以下几点：

将共享规则组与关联 VPCs

如果其他 Amazon 账户与您的账户共享了规则组，则您可以像关联已创建 VPCs 的规则组一样将其与您的账户相关联。有关更多信息，请参阅 管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联。

删除或取消共享规则组

如果您与其他账户共享规则组，然后删除该规则组或停止共享，则 DNS Firewall 会删除其他账户在该规则组与其之间创建的所有关联 VPCs。

规则组和关联的最大设置

共享规则组及其关联将包含 VPCs 在与之共享规则组的账户的计数中。

有关当前的 DNS Firewall 配额，请参阅 解析器 DNS 防火墙的配额。

Permissions

要与其他 Amazon 账户共享规则组，您必须拥有使用该PutFirewallRuleGroupPolicy操作的权限。

对与之共享规则组的 Amazon 账户的限制

与其共享了规则组的账户无法更改或删除该规则组。

标签

只有创建规则组的账户可以添加、删除或查看规则组上的标签。

要查看规则当前的共享状态（包括共享规则组的账户或与其共享了规则组的账户），以及将规则组与其它账户共享，请执行以下步骤。

查看共享状态并与其他 Amazon 账户共享规则组

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 规则组。
3. 在导航栏上，选择您在其中创建了规则组的区域。

   Sharing status（共享状态）列显示当前账户所创建规则组或者与当前账户所共享规则组的当前共享状态：

   - 未共享：当前 Amazon 账户创建了规则组，但该规则组未与任何其他账户共享。

- Shared by me（由我共享）：当前账户创建了规则组并且已与一个或多个账户共享。
- Shared With me（与我共享）：其它账户创建了规则组并且已与当前账户共享。

4. 选择您要显示共享信息或者您要与其它账户共享的规则组名称。

   在规则组：***rule group name***页面上，所有者下的值显示了创建规则组的账户的 ID。除非 Sharing status (共享状态) 的值为 Shared with me (与我共享)，否则这是当前账户。在这种情况下，所有者是创建规则组并与当前账户共享该规则组的账户。

5. 选择 Share（共享）以查看更多信息或与其它账户共享规则组。 Amazon RAM 控制台中会显示一个页面，具体取决于共享状态的值：

   - Not shared (未共享)：显示 Create resource share (创建资源共享) 页面。有关如何与其它账户、组织单位 (OU) 或组织共享规则组的信息，请转到此步骤后的步骤。
   - Shared by me（由我共享）：Shared resources（共享的资源）页面显示由当前账户拥有并与其它账户共享的规则组和其它资源。
   - Shared with me（与我共享）：Shared resources（共享的资源）页面显示由其它账户拥有并与当前账户共享的规则组和其它资源。

6. 要与其他 Amazon 账户、组织单位或组织共享规则组，请指定以下值。

   > **Note**
   >
   > 您无法更新共享设置。要更改任何以下设置，您必须使用新设置重新共享规则组，然后删除旧的共享设置。

   说明

   输入可以帮助您记住为什么共享规则组的简短说明。

   资源

   选中与您要共享的规则组对应的复选框。

   主体

   输入 Amazon 账号、OU 名称或组织名称。

   标签

   指定一个或多个键及对应的值。例如，您可以为 Key 指定成本中心，为值指定 456。

这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签；您也可以将标签用于其他目的。有关对成本分配使用标签的更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

为您的 VPC 启用解析器 DNS 防火墙保护

通过将一个或多个规则组与 VPC 关联，您可以为 VPC 启用 DNS Firewall 保护。每当 VPC 与 DNS 防火墙规则组关联时，Route 53 VPC 解析器都会提供以下 DNS 防火墙保护：

- VPC 解析器通过 DNS 防火墙路由 VPC 的出站 DNS 查询，DNS 防火墙使用关联的规则组筛选查询。
- VPC 解析器会强制执行 VPC 的 DNS 防火墙配置中的设置。

要为 VPC 提供 DNS Firewall 保护，您可以执行以下操作：

- 创建和管理 DNS Firewall 规则组和 VPC 之间的关联。有关规则组的信息，请参阅DNS Firewall 规则组和规则。
- 配置您希望 VPC 解析器在故障期间如何处理 VPC 的 DNS 查询，例如，如果 DNS 防火墙不为 DNS 查询提供响应。

管理您的 VPC 和解析器 DNS 防火墙规则组之间的关联

要查看规则组的 VPC 关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

   在导航窗格中选择 DNS 防火墙，以在 Amazon VPC 控制台上打开 DNS 防火墙规则组页面。

   - 或者 -

   登录到 Amazon Web Services 管理控制台 并打开

   下方的亚马逊 VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的 DNS 防火墙下，选择规则组。
3. 在导航栏中，选择规则组的区域。

4. 选择要关联的规则组。
5. 请选择查看详细信息。此时将显示规则组页面。
6. 在底部，您可以看到一个选项卡式详细信息区域，其中包含规则和相关 VPCs规则。选择 “关联” 选项卡VPCs。

将规则组与 VPC 关联

1. 按照前述程序要查看规则组的 VPC 关联中的知识找到规则组的 VPC 关联。
2. 在 VPCs “关联” 选项卡中，选择 “关联 VPC”。
3. 在下拉列表中找到要与规则组关联的 VPC。选择该 VPC，然后选择 Associate（关联）。

在规则组页面中，您的 VPC 列在 VPCs “关联” 选项卡中。起初，该关联的 Status（状态）报告为 Updating（正在更新）。在关联完成后，状态将更改为 Complete（完成）。

要删除规则组与 VPC 之间的关联

1. 按照前述程序要查看规则组的 VPC 关联中的知识找到规则组的 VPC 关联。
2. 选择要从列表中移除的 VPC，然后选择取消关联。验证，然后确认操作。

在规则组页面上，您的 VPC 将列在 “已关联 VPCs” 选项卡中，状态为 “取消关联”。操作完成后，DNS Firewall 将更新列表以删除 VPC。

DNS Firewall VPC 配置

您的 VPC 的 DNS 防火墙配置决定了 Route 53 VPC 解析器是否允许查询或在出现故障时阻止查询，例如，当 DNS 防火墙受损、无响应或在区域中不可用时。只要您有一个或多个 DNS 防火墙规则组与 VPC 关联，VPC 解析器就会强制执行 VPC 的防火墙配置。

您可以将 VPC 配置为失效打开或失效关闭。

- 默认情况下，故障模式处于关闭状态，这意味着 VPC Resolver 会阻止任何未收到来自 DNS 防火墙的回复的查询，并发送 D SERVFAIL NS 响应。这种方法有利于提升安全性，但会降低可用性。
- 如果您启用失效打开，VPC 解析器将在未收到 DNS 防火墙的回复时允许通过查询。这种方法有利于提升可用性，但会降低安全性。

要更改 VPC（控制台）的 DNS Firewall 配置

1. 登录 Amazon Web Services 管理控制台 并打开 VPC 解析器控制台，网址为https://console.aws.amazon.com/route53resolver/。
2. 在导航窗格的 “解析器” 下，选择VPCs。
3. 在该VPCs页面中，找到并编辑 VPC。根据需要将 DNS Firewall 配置更改为失败打开或失败关闭。

要更改 VPC (API) 的 DNS Firewall 行为

- 通过调用UpdateFirewallConfig、启用或禁用来更新 VPC 防火墙配置 `FirewallFailOpen`。

您可以通过调用，通过 API 检索您的 VPC 防火墙配置列表ListFirewallConfigs。

Amazon Route 53 Profiles 是什么？

使用 Route 53 配置文件，您可以跨多种 VPCs不同方式 Amazon Web Services 账户应用和管理与 DNS 相关的 Route 53 配置。配置文件使管理许多人的 DNS 设置与管理单个 VPC 的 DNS 设置 VPCs 一样简单，当您更新配置文件时，其设置会传播到所有 VPCs 与该配置文件关联的人。您也可以使用 Amazon Web Services 账户 在同一地区与之共享个人资料 Amazon RAM。以下是您可以关联到某个配置文件的 Route 53 当前支持的资源：

- 私有托管区及其中指定的设置。有关使用私有托管区的更多信息，请参阅 使用私有托管区。
- 解析器规则，包括转发规则和系统规则。有关 Resolver 规则的更多信息，请参阅 管理转发规则。
- DNS Firewall 规则组。有关 DNS 防火墙规则组的更多信息，请参阅 DNS Firewall 规则组和规则。
- 接口 VPC 端点 有关接口 VPC 端点的更多信息，请参阅 Amazon VPC 用户指南中的接口 VPC 端点。
- VPC 解析器查询日志配置。有关 VPC 解析器查询日志记录的更多信息，请参阅Resolver 查询日志记录。

某些 VPC 配置直接在配置文件中进行管理。这些配置为：

- Resolver 规则的反向 DNS 查找配置。
- DNS Firewall 故障模式配置。
- DNSSEC 验证配置。

例如，您可以为与配置文件关联的所有内容启用 DNS 防火墙故障模式配置，但保留 VPC 现有的 DNSSEC 验证配置。 VPCs

> **Important**
>
> 为上述配置启用配置文件设置并将配置文件关联到 VPC 后，配置文件设置立即生效。

您还可以使用 Amazon CloudFormation 为新配置的 DNS 设置一致的 DNS 设置。 VPCs

每个 VPC 可关联一个配置文件，每个配置文件可关联的资源数量各不相同。有关更多信息，请参阅 Route 53 配置文件中的配额 。

如何确定 Route 53 配置文件设置的优先级

可以为配置文件设置本地 DNS 设置和关联，以用于迁移或其他测试目的。当 DNS 查询同时与 VPC 直接关联的私有托管区的 Resolver 规则和配置文件关联的私有托管区的 Resolver 规则匹配时，优先采用本地 DNS 设置。当对冲突的域名进行 DNS 查询时，最具体的域名将会胜出。下表列出了评估顺序的示例：

DNS 查询	配置文件规则	VPC 规则	评估的规则
example.com	example.com	example.com	本地 VPC
test.example.com	test.example.com	example.com	配置文件
marketing.example.com	无	marketing.example.com	本地 VPC

Route 53 配置文件区域可用性

要查看区域可用性和端点，请参阅 Amazon 一般参考指南中的 Route 53 的服务端点。

使用 Route 53 配置文件的概括步骤

要在您的亚马逊虚拟私有云中实现 Amazon Route 53 配置文件 VPCs，请执行以下高级步骤。

1. 创建空配置文件 - 第一步是创建一个可以关联到 DNS 资源的空配置文件。有关更多信息，请参阅创建 Route 53 配置文件。
2. 将 DNS 资源与配置文件关联 — 您当前可以与配置文件关联的资源包括私有托管区域、解析器规则（包括转发和系统）、DNS 防火墙规则组、VPC 解析器查询日志配置以及接口 VPC 终端节点。有关更多信息，请参阅 将 DNS Firewall 规则组与 Route 53 配置文件关联、将私有托管区与 Route 53 配置文件相关联、将 Resolver 规则与 Route 53 配置文件相关联、将 VPC 解析器查询日志配置关联到 Route 53 配置文件和将接口 VPC 端点与 Route 53 配置文件关联。
3. 为配置文件配置一些 VPC 设置 — 某些 DNS 设置（例如与配置文件关联的托管区域）会 VPCs 立即应用于。对于 DNSSEC 验证、Resolver 反向 DNS 查找和 DNS Firewall 故障模式配置，可以选择以下选项之一：

- 对于 DNSSEC 验证，您可以选择使用本地 VPC 配置（默认）、启用验证或禁用所有与配置文件 VPCs 关联的验证。
- 对于 Resolver 反向 DNS 查找配置，可以将其启用、禁用或在本地使用为 VPC 定义的自动定义规则（默认）。
- 对于 DNS Firewall 故障模式配置，可以将其启用、禁用或在本地使用为 VPC 定义的故障模式配置（默认）。

有关更多信息，请参阅 编辑 Route 53 配置文件的配置。

4. 将@@ 配置文件关联到一个或多个配置文件 VPCs — 要开始使用您的个人资料，请将其与一个或多个配置文件相关联 VPCs。有关更多信息，请参阅 将 Route 53 配置文件关联到 VPCs。

创建 Route 53 配置文件

要创建 Route 53 配置文件，请按照本主题中的指导操作。选择一个选项卡，使用 Route 53 控制台创建 Route 53 配置文件，或者 Amazon CLI。

- 控制台
- CLI

Console

创建 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 在导航栏上，选择您想要在其中创建配置文件的区域。
4. 输入配置文件的名称，可以选择添加标签，然后选择创建配置文件。

   这将创建一个采用默认配置的空配置文件，您可以为其关联资源。将资源与配置文件关联后，您可以将其与多个配置文件相关联， VPCs 并编辑某些解析器配置如何应用于。 VPCs

CLI

您可以通过运行如下 Amazon CLI 命令并使用自己的值来创建配置文件name。

```
aws route53profiles create-profile --name test
```

以下是运行此命令后的示例输出。

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```

要将配置文件与不同的资源关联并编辑配置文件的 VPC 配置，请参阅以下步骤：

主题

- 将 DNS Firewall 规则组与 Route 53 配置文件关联
- 将私有托管区与 Route 53 配置文件相关联
- 将 Resolver 规则与 Route 53 配置文件相关联
- 将接口 VPC 端点与 Route 53 配置文件关联
- 将 VPC 解析器查询日志配置关联到 Route 53 配置文件
- 编辑 Route 53 配置文件的配置
- 将 Route 53 配置文件关联到 VPCs

将 DNS Firewall 规则组与 Route 53 配置文件关联

有关创建规则组的说明，请参阅 创建规则组和规则，然后选择一个选项卡，使用 Route 53 控制台或 Amazon CLI将 DNS Firewall 规则组与 Route 53 配置文件关联。

- 控制台
- CLI

Console

关联 DNS Firewall 规则组

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在导航窗格中，选择配置文件，然后在配置文件表中，选择要使用的配置文件的链接名称。
4. 在该 <配置文件名称> 页面上，选择 DNS Firewall 规则组选项卡，然后选择关联。
5. 在 DNS Firewall 规则组部分，最多可以选择 10 个之前创建的规则组。如果要关联 10 个以上的规则组，请使用 APIs。有关更多信息，请参阅 AssociateResourceToProfile。

   要创建新的规则组，请参阅 创建规则组和规则。
6. 选择下一步。
7. 在指定优先级页面上，可以通过单击预分配优先级序号并键入新的序号来设置规则组的处理顺序。优先级的许可值介于 100 到 9900 之间。

   规则组评估从数字最小的优先级设置开始，并逐渐增大。您可以随时更改规则组的优先级，例如更改处理顺序或为其它规则组留出空间。

   选择提交。
8. 关联进度显示在 DNS Firewall 规则组对话框的状态列中。

CLI

通过运行如下 Amazon CLI 命令并使用您自己的`nameprofile-id`、`resource-arn`和值，可以将规则组与配置文件相关联`priority`：

```
aws route53profiles associate-resource-to-profile --name test-
resource-association --profile-id rp-4987774726example --resource-arn
arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/
rslvr-frg-cfe7f72example --resource-properties "{\"priority\": 102}"
```

以下是运行此命令后的示例输出。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
```

```
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```


将私有托管区与 Route 53 配置文件相关联

有关如何创建私有托管区的说明，请参阅 创建私有托管区域，然后按照此过程中的步骤将私有托管区与配置文件关联。

关联私有托管区

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在导航窗格中，选择配置文件，然后在配置文件表中，选择要使用的配置文件的链接名称。
4. 在 <配置文件名称> 页面上，选择私有托管区选项卡，然后选择关联。
5. 在关联私有托管区页面上，最多可以选择 10 个之前创建的私有托管区。如果您想关联 10 个以上的私有托管区域，请使用 APIs。有关更多信息，请参阅 AssociateResourceToProfile。

   要创建私有托管区，请参阅 创建私有托管区域：
6. 选择关联
7. 关联进度显示在私有托管区选项卡的状态列中。

将 Resolver 规则与 Route 53 配置文件相关联

有关如何创建 Resolver 规则的说明，请参阅 创建转发规则，然后按照此程序中的步骤将 Resolver 规则与配置文件关联。

关联 VPC 解析器规则

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在 <配置文件名称> 页面上，选择 Resolver 规则选项卡，然后选择关联。
4. 在关联 Resolver 规则页面的 Resolver 规则表中，最多可以选择 10 条之前创建的 Resolver 规则。如果要关联 10 个以上的解析器规则，请使用。 APIs有关更多信息，请参阅 AssociateResourceToProfile。

   要创建 Resolver 规则，请参阅 创建转发规则。
5. 选择关联
6. 关联进度显示在 Resolver 规则页面的状态列中。

将接口 VPC 端点与 Route 53 配置文件关联

有关如何创建接口 VPC 端点的说明，请参阅 VPC 用户指南中的创建 VPC 端点，然后按照本程序中的步骤，将 VPC 端点与配置文件关联。

关联 VPC 端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在 <配置文件名称> 页面上，选择 VPC 端点选项卡，然后选择关联。
4. 在关联 VPC 端点页面的 VPC 端点表中，最多可以选择 10 个之前创建的端点。如果要关联 10 个以上的终端节点，请使用 APIs。有关更多信息，请参阅 AssociateResourceToProfile。

   要创建 Resolver 规则，请参阅 创建转发规则。
5. 选择关联
6. 关联进度显示在 VPC 端点选项卡的状态列中。

将 VPC 解析器查询日志配置关联到 Route 53 配置文件

有关如何创建 VPC 解析器查询日志配置的说明，请参阅，然后选择一个选项卡配置（VPC 解析器查询日志），使用 Route 53 控制台将 VPC 解析器配置与 Route 53 配置文件关联，或者。 Amazon CLI

- 控制台
- CLI

Console

关联查询日志配置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在配置文件名称页面上，选择解析器查询日志配置选项卡，然后选择关联。
4. 在 “关联查询日志配置” 页面的 Resolver 查询日志配置表中，您最多可以选择先前创建的三个配置。如果要关联三个以上的查询日志配置，请使用 API。有关更多信息，请参阅AssociateResourceToProfile。
5. 要创建新的 VPC 解析器查询日志配置，请参阅配置（VPC 解析器查询日志）。
6. 选择关联
7. 关联进度显示在 R esolver 查询日志配置选项卡的状态列中。

CLI

通过运行如下 Amazon CLI 命令并使用自己的和值，可以将查询日志配置与配置文件相关联resource-arn。name profile-id

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-config/rqlc-cfe7f72example
```

以下是运行此命令后的示例输出。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851226.613,
        "Id": "rpr-001913120b8example",
        "ModificationTime": 1710851226.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
```

```
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:resolver-
query-log-config/rqlc-cfe7f72example",
        "ResourceType": "RESOLVER_QUERY_LOG_CONFIG",
        "Status": "CREATING",
        "StatusMessage": "Creating rp-4987774726example to rqlc-cfe7f72example
 association"
    }
}
```

编辑 Route 53 配置文件的配置

将资源与配置文件关联后，您可以编辑默认 VPC 配置以决定如何将其应用于 VPCs。

编辑配置文件的配置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在导航窗格中，选择配置文件，然后在配置文件表中，选择要使用的配置文件的链接名称。
4. 在 <配置文件名称> 页面上，选择配置选项卡，然后选择编辑。
5. 在编辑配置页面上，为 VPC DNSSEC 配置、Resolver 反向 DNS 查找配置和 DNS Firewall 故障模式配置选择其中一个值。

   有关这些值的更多信息，请参阅 Route 53 配置文件的配置设置。
6. 选择更新。

Route 53 配置文件的配置设置

编辑 Route 53 配置文件的配置时，请指定以下值：

DNSSEC 配置

选择以下任一值：

- 使用本地 VPC DNSSEC 配置 - 默认

  选择此选项可使所有与此配置文件 VPCs 关联的用户保留其本地 DNSSEC 验证配置。
- 启用 DNSSEC 验证

选择此选项可在与该配置文件VPCs 关联的所有内容中启用 DNSSEC 验证。

- 禁用 DNSSEC 验证

  选择此选项可禁用所有与此配置文件关联VPCs 的 DNSSEC 验证。

Resolver 反向 DNS 查找配置

选择以下任一值：

- 启用

  选择此选项可创建自动定义的规则，以便在所有关联的 DNS 中进行反向 DNS 查找 VPCs。

- 未启用

  选择此选项可不为所有关联的 DNS 反向查找创建自动定义的规则 VPCs。

- 使用本地自动定义的规则 - 默认

  选择此选项可使用本地 VPC 设置对关联人进行反向 DNS 查找 VPCs。

DNS Firewall 故障模式配置

选择以下任一值：

- 禁用

  选择此选项可关闭关联的 DNS 防火墙故障模式 VPCs。使用此选项，DNS Firewall 将阻止它无法正确评估的所有查询。

- Enabled (已启用)

  选择此选项可为所有关联用户保持 DNS 防火墙故障模式处于打开状态 VPCs。使用此选项，如果 DNS Firewall 无法正确评估查询，它将允许查询继续。

- 使用本地故障模式设置 - 默认

  选择此选项可以使用本地 VPC DNS Firewall 故障模式设置。

有关配置的更多信息，请参阅

- 在 Amazon Route 53 中启用 DNSSEC 验证
- VPC 解析器中反向 DNS 查询的转发规则
- DNS Firewall VPC 配置

将 Route 53 配置文件关联到 VPCs

要将 Route 53 配置文件与 VPC 关联，请按照本主题中的指导操作。选择一个选项卡，使用 Route 53 控制台将 Route 53 配置文件关联到 VPC，或者 Amazon CLI。

- 控制台
- CLI

Console

要关联 VPCs

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航栏上，选择您在其中创建了配置文件的区域。
3. 在<Profile name>页面上，选择VPCs选项卡，然后选择关联。
4. 在 “关联 VPCs” 页面上，您最多可以选择之前创建的 10 个 VPCs 。如果要关联超过 10 个 VPCs，请使用 APIs。有关更多信息，请参阅 AssociateProfile。
5. 选择关联
6. 关联进度显示在VPCs页面的状态列中。

CLI

您可以通过运行如下 Amazon CLI 命令并使用您自己的`name`、`profile-id`和值来列出配置文件`resource-id`：

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

以下是运行此命令后的示例输出。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
```

```
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

查看和更新 Amazon Route 53 Profiles

选择控制台选项卡，查看和编辑 Route 53 配置文件。选择 CLI 选项卡 Amazon CLI ，用于列出您拥有的、由您共享或与您共享的个人资料。

- 控制台
- CLI

Console

查看和更新 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 选择要查看或编辑的配置文件名称旁边的按钮。
4. 在 <配置文件名称> 页面上，可以查看当前关联的 DNS 资源、关联新的资源以及编辑标签和 VPC 配置。

CLI

您可以通过运行如下 Amazon CLI 命令来列出配置文件：

```
aws route53profiles list-profiles
```

以下是运行此命令后的示例输出。

```
{
```

```
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

您可以运行如下 Amazon CLI 命令并对 `profile-association-id` 使用自己的值，从而获取与此配置文件关联的特定 VPC 的信息：

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

以下是运行此命令后的示例输出。

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

删除 Amazon Route 53 配置文件

选择一个选项卡，使用 Route 53 控制台删除 Route 53 配置文件，或者 Amazon CLI。

- 控制台
- CLI

Console

删除 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 选择要删除的配置文件旁边的单选按钮，然后选择删除。

> **Important**
>
> 如果个人资料与关联，则无法将其删除 VPCs。此外，如果将配置文件共享给其他人 Amazon Web Services 账户，则与 VPCs 该配置文件配置关联的任何配置都将丢失这些配置。

4. 在 删除 <配置文件名称> 对话框中，键入 **confirm**，然后选择删除。

CLI

> **Important**
>
> 如果个人资料与关联，则无法将其删除 VPCs。此外，如果将配置文件共享给其他人 Amazon Web Services 账户，则与 VPCs 该配置文件配置关联的任何配置都将丢失这些配置。

您可以通过运行如下 Amazon CLI 命令并使用自己的值来删除配置文件profile-id：

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

以下是运行此命令后的示例输出。

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
```

```
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "DELETED",
        "StatusMessage": "Deleted Profile"
    }
}
```

查看和更新与 Amazon Route 53 配置文件关联的 Route 53 资源

选择控制台选项卡查看 Route 53 配置文件资源关联，也可以选择编辑 DNS Firewall 规则组的优先级。选择 CLI 选项卡 Amazon CLI ，用于列出资源关联并查看 DNS 防火墙规则组优先级的更新示例。

- 控制台
- CLI

Console

查看和更新与配置文件关联的资源

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 在导航栏上，选择您在其中创建了配置文件的区域。
4. 选择要查看或编辑资源关联的配置文件名称旁边的按钮。
5. 在 <配置文件名称> 页面上，选择要查看或编辑的资源的选项卡，即 DNS Firewall 规则组、私有托管区、Resolver 规则或 VPC 端点。
6. 在资源的选项卡页上，可以查看关联资源的名称、ARN 和状态。您还可以选择齿轮图标来调整资源表中的显示内容。

   在 DNS Firewall 规则组选项卡页上，您还可以选择规则组的优先级条目，并将其编辑为更小或更大的数字。规则组按照从最低优先级序号到最高优先级序号的顺序进行评估。

CLI

您可以通过运行如下 Amazon CLI 命令并使用自己的值来列出与配置文件关联的资源`profile-id`：

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

以下是运行此命令后的示例输出。

```
{
    "ProfileResourceAssociations": [
        {
            "CreationTime": 1710851216.613,
            "Id": "rpr-001913120a7example",
            "ModificationTime": 1710851216.613,
            "Name": "test-resource-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
            "ResourceProperties": "{\"priority\":102}",
            "ResourceType": "FIREWALL_RULE_GROUP",
            "Status": "COMPLETE",
            "StatusMessage": "Completed creation of Profile to DNS Firewall rule
 group association"
        }
    ]
}
```

您可以更新与配置文件关联的 DNS 防火墙规则组的优先级，方法是运行如下 Amazon CLI 命令，为和使用自己的值，profile-resource-association-id并使用自己的值--resource-properties：

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

以下是运行此命令后的示例输出。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
```

```
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

取消资源与 Amazon Route 53 配置文件的关联

在删除个人资料之前，必须解除所有资源与该配置文件的关联。

取消与 Route 53 配置文件关联的资源的关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 在导航栏上，选择要取消资源关联的配置文件的创建区域。
4. 选择要取消资源关联的配置文件名称旁边的按钮。
5. 在配置文件名称页面上，选择要删除的资源的选项卡，即 DNS 防火墙规则组、私有托管区域、解析器查询日志、解析器规则或 VP C 终端节点。
6. 在资源的选项卡页上，选择要取消关联的资源，然后选择取消关联。
7. 在取消资源关联对话框中，键入 **`confirm`**，然后选择取消关联。

查看 VPCs 与 Amazon Route 53 个人资料相关的内容

选择控制台选项卡，查看和编辑 Route 53 配置文件与 VPC 的关联。选择 CLI 选项卡， Amazon CLI 用于列出配置文件与 VPC 的关联，或者获取有关特定关联的信息

- 控制台
- CLI

Console

查看 VPCs 与配置文件关联的内容

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 在导航栏上，选择您在其中创建了配置文件的区域。
4. 选择要查看其关联的配置文件名称旁边的按钮 VPCs。
5. 在<Profile name>页面上选择VPCs选项卡。
6. 在的选项卡页上， VPCs 您可以查看关联人员的姓名、ARN 和状态。 VPCs

CLI

你可以通过运行如下 Amazon CLI 命令来列出与之关联的配置文件： VPCs

```
aws route53profiles list-profile-associations
```

以下是运行此命令后的示例输出。

```
{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
            "ModificationTime": 1709338974.772,
```

```
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

您可以运行如下 Amazon CLI 命令并对 `profile-association-id` 使用自己的值，从而获取与此配置文件关联的特定 VPC 的信息：

`aws route53profiles get-profile-association --profile-association-id` **`rpassoc-489ce212fexample`**

以下是运行此命令后的示例输出。

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

取消 VPC 与 Amazon Route 53 配置文件的关联

选择一个选项卡，使用 Route 53 控制台将 Route 53 配置文件与 VPC 断开关联，或者。 Amazon CLI

- 控制台
- CLI

Console

取消与 Route 53 配置文件关联的 VPC 的关联

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 在导航栏上，选择要取消 VPC 关联的配置文件的创建区域。
4. 选择要取消 VPC 关联的配置文件名称旁边的按钮。
5. 在<Profile name>页面上选择VPCs选项卡。
6. 在资源的 VPCs 选项卡页上，选择要取消关联的 VPC，然后选择取消关联。
7. 在取消资源关联对话框中，键入 **confirm**，然后选择取消关联。

CLI

您可以通过运行如下 Amazon CLI 命令并使用自己的值来解除配置文件与 VPC 的`profile-id`关联：`--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

以下是运行此命令后的示例输出。

```
"ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851401.362,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "DELETING",
        "StatusMessage": "Deleting Profile Association"
    }
```

使用共享的 Route 53 配置文件

可以通过以下方式与其他账户共享配置文件：

- 授予只读权限，这意味着其他账户可以将个人资料与其关联起来 VPCs。在这种情况下，所有 DNS 资源和配置都将在关联的 DNS 上生效 VPCs。
- 授予管理员权限。在这种情况下，拥有共享个人资料的账户可以修改个人资料，然后将其与其关联起来 VPCs。所有者还可以创建客户托管权限，用于指定可以由使用者账户执行的操作。有关更多信息，请参阅《Amazon RAM 用户指南》中的客户托管权限。

Amazon Route 53 配置文件与 Amazon Resource Access Manager (Amazon RAM) 集成以实现资源共享。 Amazon RAM 是一项服务，可让您与其他人 Amazon Web Services 账户 或通过共享某些 Route 53 资源 Amazon Organizations。使用 Amazon RAM，您可以通过创建资源共享来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用者可包括：

- 具体 Amazon Web Services 账户
- 其组织内部的组织单位 Amazon Organizations
- 它的整个组织都在 Amazon Organizations

有关的更多信息 Amazon RAM，请参阅《Amazon RAM 用户指南》。

本主题说明如何共享您拥有的资源以及如何使用共享给您的资源。

内容

授予共享 Route 53 配置文件的权限

IAM 主体需要一组最低权限才能共享配置文件。我们建议使用 `AmazonRoute53ProfilesFullAccess` 托管 IAM 策略，确保 IAM 主体拥有共享和使用所共享配置文件的必需权限。

如果使用自定义 IAM 策略，则需要进行 `route53profiles:GetProfilePolicy` 和 `route53profiles:PutProfilePolicy` 操作。这些是仅限权限的 IAM 操作。如果 IAM 委托人未获得这些权限，则在尝试使用该 Amazon RAM 服务共享个人资料时会出错。

共享 Route 53 配置文件的先决条件

- 要共享 Route 53 个人资料，您必须在自己的账户中拥有该档案 Amazon Web Services 账户。这意味着资源必须分配或预调配到您的账户。您无法共享已与您共享的 Route 53 配置文件。
- 要与您的企业或 Amazon Organizations内的企业部门共享 Route 53 配置文件，您必须允许与 Amazon Organizations共享。有关更多信息，请参阅Amazon RAM 《用户指南》中的允许与 Amazon Organizations 共享。

共享 Route 53 配置文件

当您与他人共享您拥有的个人资料时 Amazon Web Services 账户，您可以让他们将该个人资料中与 DNS 相关的设置应用于他们 VPCs。这样可以更轻松地在成千上万个服务器上应用统一的 DNS 配置，VPCs 同时将管理开销降至最低。

要共享 Route 53 配置文件，您必须将它添加到资源共享。资源共享是一项 Amazon RAM 资源，可让您跨 Amazon Web Services 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。在使用 Route 53 控制台共享 Route 53 配置文件时，必须将它添加到现有资源共享。要将 Route 53 配置文件添加到新的资源共享，您必须首先使用 Amazon RAM 控制台创建资源共享。

如果您是组织中的一员， Amazon Organizations 并且启用了组织内部共享，则组织中的用户将自动获得访问共享的 Route 53 个人资料的权限。否则，使用者将会收到加入资源共享的邀请，并在接受邀请后获得对共享 Route 53 配置文件的访问权限。

您可以开始在 Route 53 控制台上共享您拥有的 Route 53 配置文件，然后继续在控制 Amazon RAM 台上继续共享。

使用 Route 53 控制台共享所拥有的 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 选择要共享的配置文件，然后在配置文件详细信息页面上，选择共享配置文件。
4. 您将进入 Amazon RAM 控制台，在那里您可以按照以下步骤操作：在Amazon RAM 用户指南中创建资源共享。

5. 如果与您共享某个配置文件，则配置文件表中会包含“与我共享”文本。

   共享配置文件后，此配置文件将在配置文件表中列示为已共享。

使用 Amazon RAM 控制台共享您拥有的 Route 53 配置文件

请参阅《Amazon RAM 用户指南》中的创建资源共享。

要共享您拥有的 Route 53 配置文件，请使用 Amazon CLI

使用 create-resource-share 命令。

取消共享 Route 53 配置文件

当您取消共享配置文件时，如果 VPCs 该配置文件与其配置文件相关联，则这些配置文件将丢失，并默认为特定于 VPC 的配置。

要取消共享您拥有的已共享 Route 53 配置文件，必须从资源共享中将其删除。您可以使用 Route 53 控制台、 Amazon RAM 控制台或 Amazon CLI完成此操作。

使用 Route 53 控制台取消共享您拥有的共享 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 选择要取消共享的配置文件的链接名称，然后在 <配置文件名称> 页面上选择管理共享。
4. 您将进入 Amazon RAM 控制台，在那里您可以按照以下步骤操作：更新Amazon RAM 用户指南中的资源共享。

使用控制台取消共享您拥有的共享 Route 53 配置文件 Amazon RAM

请参阅《Amazon RAM 用户指南》中的更新资源共享。

要取消共享您拥有的共享 Route 53 配置文件，请使用 Amazon CLI

使用 disassociate-resource-share 命令。

识别共享的 Route 53 配置文件

拥有者和使用者可以使用 Route 53 控制台和 Amazon CLI标识共享的 Route 53 配置文件。

使用 Route 53 控制台识别共享的 Route 53 配置文件

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择配置文件。
3. 如果与您共享某个配置文件，则配置文件表中会包含“与我共享”文本。

   共享配置文件后，此配置文件将在配置文件表中列示为已共享。

要识别共享的 Route 53 配置文件，请使用 Amazon CLI

使用 get-profile 或 list-profile 命令。这些命令返回有关您所拥有的 Route 53 配置文件以及 Route 53 配置文件共享状态的信息。

对共享 Route 53 配置文件的责任和权限

拥有者的权限

配置文件所有者可以查看、管理和删除配置文件资源关联，包括由使用者账户建立的资源关联。所有者可以查看和删除其所拥有的 VPC 关联。此外，只有配置文件所有者才能删除其所拥有的配置文件，这也会自动删除此配置文件的所有资源关联。

> **Note**
>
> 您必须创建自定义管理权限，该权限除了默认操作外，还应包含将配置文件共享到的账户中的任何资源关联起来的 `route53profiles:AssociateResourceToProfile` 操作，因为默认策略 `AWSRAMPermissionRoute53ProfileAllowAssociation` 不包含此操作。

使用者的权限

共享配置文件使用者的默认权限为只读权限。凭借只读权限，他们可以查看关联的资源并将其与之关联 VPCs，但无法管理资源关联。

所有者还可以在 Amazon RAM 控制台上创建客户托管权限。有关更多信息，请参阅《Amazon RAM 用户指南》中的创建和使用客户托管权限。

计费和计量

Route 53 配置文件按照 VPC 关联的数量计费。配置文件所有者负责支付使用者的 VPC 关联账单。

实例限额

配置文件的所有者和使用者具有相同的限额，但每个账户在某个区域中使用的 Route 53 配置文件数量除外。有关更多信息，请参阅 Route 53 配置文件中的配额 。

什么是 Amazon Route 53 on Outposts？

Amazon Outposts 是一项完全托管的服务，可将 Amazon 基础架构 APIs、服务和工具扩展到客户驻地。这允许客户使用与中相同的编程接口，在本地工作负载下运行 Amazon 服务 Amazon Web Services 区域。有关更多信息，请参阅什么是 Amazon Outposts？ 在《Amazon Outposts 用户指南》中。

Route 53 on Outposts 提供两种功能：

- 一个 VPC 解析器，用于缓存来自的所有 DNS 查询。 Amazon Outposts
- 在部署入站和出站端点时，可以在 Outpost 和本地 DNS 解析程序之间设置混合连接。

有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。

此外，Route 53 on Outposts 允许在 Outpost 内解析查询，而不是往返最近的 Amazon Web Services 区域，从而减少了网络延迟。

- 一个 VPC 解析器，用于缓存来自的所有 DNS 查询。 Amazon Outposts
- 在部署入站和出站端点时，可以在 Outpost 和本地 DNS 解析程序之间设置混合连接。

有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。

此外，Route 53 on Outposts 允许在 Outpost 内解析查询，而不是往返最近的 Amazon Web Services 区域，从而减少了网络延迟。

> **Note**
>
> 如果你的 Amazon Outposts 机架版本与 Outposts 上的 Route 53 不兼容， Amazon 客户团队会收到通知，他们将与你联系以帮助你升级。 Amazon Outposts

架构概述

Outposts 上的 Route 53 实现了分布式 DNS 架构：

- DNS 记录和托管区域仍 Amazon 在该地区的 Amazon Route 53 中进行管理

- 解析器功能扩展到您的 Amazon Outposts 机架，用于本地查询处理

这种设计优化了查询性能和可用性，同时保持集中的 DNS 记录管理。DNS 记录继续存储 Amazon 在该区域中，而不是本地存储在 Amazon Outposts 机架上。

Amazon Route 53 on Outposts 功能

下表描述了 Route 53 on Outposts 功能与 Amazon Route 53 功能的对比。

Route 53 on Outposts 与 Route 53 对比

功能	在 Route 53 on Outposts 上的可用性
VPC 解析器	可以。VPC Resolver 为托管在 Outpost 机架上的应用程序、中的对等 VPC 以及任何可公开访问 Amazon Web Services 区域的主机名维护本地记录缓存。
运行状况检查	否，运行状况检查从 Amazon Web Services 区域中计算和报告。如果 Outpost 与云断开连接，端点将无法打开，且无法故障转移到备份。
解析程序端点	可以。Outpost 机架上的解析程序端点允许从本地 DNS 服务器转发和接收 DNS 查询。 只有 IPv4 终端节点类型可用于终端节点。
解析器 DNS 防火墙	不可用。
流量流	不可用。

VPC 解析器与 V Amazon Outposts PC 断开连接时的行为

如果与 Amazon Outposts 断开连接 Amazon Web Services 区域，则前哨站上的解析器的行为如下：

- 控制面板更改不可用。
- 运行状况检查和 DNS 故障转移功能不可用。
- 针对本地托管在 Outposts 上的资源的 DNS 查询已得到解析；但在某些情况下，如果在 Outpost 处于断开连接状态时更新了资源的 IP 地址，则响应可能会失效。

- 针对区域内 VPC 上托管的资源的 DNS 查询可以解析。但是，在 Outpost 与 Amazon Web Services 区域 的连接恢复之前，资源将无法访问。
- 如果公有 DNS 资源的 DNS 查询在 Outpost 的 VPC 解析器缓存中可用，则可以解决这些查询。

开启 VPC 解析器入门 Amazon Outposts

在你订购了 Amazon Outposts 机架并已交付后，如下所述：在Amazon Outposts 指南中创建，你可以 Amazon Outposts在 Outpost 上设置 Resolver。

> **Important**
>
> Outpost 上的解析器只能由拥有机架的 Amazon 账户创建。 Amazon Outposts 如果与其他账户共享 Amazon Outposts 机架，则这些账户无法在共享机架上的 Outpost 上创建 Resolver。

你也可以使用 APIs 来管理 Outposts 上的 53 号公路。有关详细信息，请参阅 Resolver on Outpost actions。

> **Important**
>
> 在上创建 VPC 解析器缓存最多可能需要 30-150 分钟。 Amazon Outposts

交付 Amazon Outposts 机架后，你可以在 Outposts 上选择加入 Route 53。

配置 Resolver on Outpost

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 在 Outpost 上的解析器页面上，选择创建 VPC 解析器。
5. 在创建 VPC 解析器页面上：
   - 在下方，Amazon Outposts选择 Amazon Outposts 要在其上创建 VPC 解析器的。
   - 在 VPC 解析器名称文本框中输入 VPC 解析器的名称。
   - 在 VPC 解析器的推荐实例类型填充了 Amazon EC2 实例后，选择一个实例。

有关实例类型的更多信息，请参阅 Resolver on Outpost 上的限额。

- 对于实例数量，选择 VPC VPC 解析器的弹性接口实例数量。默认值为 4。

  如果您的实例类型 Amazon Outposts 不支持 VPC 解析器，则无法创建 VPC 解析器。

6. 选择创建 VPC 解析器。

   您可以在 O utpost 上的解析器页面上监控 VPC 解析器的创建情况。

创建入站端点

在创建 Resolver on Outpost 后，您可以添加入站和出站端点，以解析与本地网络之间的 DNS 查询。

为 Resolver on Outpost 配置入站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 在入站端点表中，选择创建入站端点。
6. 在创建入站端点页面上，输入适用的值。有关更多信息，请参阅 在 Outpost 上创建或编辑入站端点时指定的值。
7. 选择创建端点。

在 Outpost 上创建或编辑入站端点时指定的值

创建或编辑入站端点时，您指定以下值：

前哨基地 ID

如果您要在 VPC 上为 VPC 解析器创建终端节点，则这是 Amazon Outposts ID。 Amazon Outposts

端点名称

可在控制面板上轻松找到入站端点的友好名称。

region-name 区域中的 VPC

来自您的网络的所有入站 DNS 查询都会在发往 VPC 解析器的途中通过此 VPC。

此端点的安全组

您希望用于控制对此入站端点的访问的一个或多个安全组的 ID。所指定的安全组必须包含一个或多个入站规则。入站规则必须允许端口 53 上的 TCP 和 UDP 访问。创建端点后，您无法更改此值。

有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

IP 地址

您要分配到入站端点的 IP 地址。您必须至少指定两个 IP 地址，以实现冗余配置。注意以下几点：

IP 地址和 Amazon VPC 弹性网络接口

对于您指定的可用区、子网和 IP 地址的每种组合，VPC 解析器都会创建一个 Amazon VPC 弹性网络接口。有关针对端点中每个 IP 地址当前每秒处理的最大 DNS 查询数，请参阅Route 53 VPC 解析器的配额。有关每个弹性网络接口定价的信息，请参阅 Amazon Route 53 定价页面上的“Amazon Route 53”。

> **Note**
>
> Resolver 端点具有私有 IP 地址。这些 IP 地址在端点的生命周期内不会发生变化。

对于每个 IP 地址，指定以下值。每个 IP 地址必须位于在 VPC in the region-name Region (<区域名称> 区域中的 VPC) 所指定 VPC 的可用区中。

可用区

希望 DNS 查询在到达您的 VPC 之前经过的可用区。您指定的可用区必须配置有子网。

子网

包含您要将 DNS 转发到的 IP 地址的子网。子网必须具有一个可用 IP 地址。

为 IPv4 地址指定子网。 IPv6 不支持。

IP 地址

您要将 DNS 查询转发到的 IP 地址。

选择是希望 VPC 解析器从指定子网中的可用 IP 地址中为您选择 IP 地址，还是要自己指定 IP 地址。

如果您选择自己指定 IP 地址，请输入 IPv4 地址。 IPv6 不支持。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签；您也可以将标签用于其他目的。有关对成本分配使用标签的更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

创建出站端点

选择并配置 VPC 解析器后，您还可以添加入站和出站终端节点，以解析本地网络的 DNS 查询。

> **Note**
>
> 当您配置出站终端节点时，VPC Resolver 会缓存 DNS 响应，以便在您的 Outpost 与该区域断开连接时仍可以解析查询。维护此缓存可能会增加对本地解析程序的 DNS 请求。

为 Resolver on Outpost 配置出站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选标记，然后选择查看详情。
5. 在出站端点表中，选择创建出站端点。
6. 在创建出站端点页面上，输入适用的值。有关更多信息，请参阅 在 Amazon Outposts上创建或编辑出站端点时指定的值。
7. 选择创建端点。

在 Amazon Outposts上创建或编辑出站端点时指定的值

创建或编辑出站端点时，您指定以下值：

前哨基地 ID

如果您要在 VPC 上为 VPC 解析器创建终端节点，则这是 Amazon Outposts ID。 Amazon Outposts

端点名称

可在控制面板上轻松找到出站端点的友好名称。

region-name 区域中的 VPC

来自您 VPC 的所有入站 DNS 查询经过此 VPC 流向您的网络。

此端点的安全组

您希望用于控制对此 VPC 的访问的一个或多个安全组的 ID。所指定的安全组必须包含一个或多个出站规则。对于在您网络上用于 DNS 查询的端口，出站规则必须允许该端口上的 TCP 和 UDP 访问。创建端点后，您无法更改此值。

有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

IP 地址

您要分配到出站端点的 IP 地址。您必须至少指定两个 IP 地址，以实现冗余配置。注意以下几点：

IP 地址和 Amazon VPC 弹性网络接口

对于您指定的可用区、子网和 IP 地址的每种组合，VPC 解析器都会创建一个 Amazon VPC 弹性网络接口。有关针对端点中每个 IP 地址当前每秒处理的最大 DNS 查询数，请参阅Route 53 VPC 解析器的配额。有关每个弹性网络接口定价的信息，请参阅 Amazon Route 53 定价页面上的“Amazon Route 53”。

> **Note**
>
> Resolver 端点具有私有 IP 地址。这些 IP 地址在端点的生命周期内不会发生变化。

对于每个 IP 地址，指定以下值。每个 IP 地址必须位于在 VPC in the region-name Region (<区域名称> 区域中的 VPC) 所指定 VPC 的可用区中。

可用区

您希望 DNS 查询从 VPC 发出时所经过的可用区。您指定的可用区必须配置有子网。

子网

包含您要从中转发 DNS 查询的 IP 地址的子网。子网必须具有一个可用 IP 地址。

为 IPv4 地址指定子网。 IPv6 不支持。

IP 地址

您要分配到出站端点的 IP 地址。

选择是希望 VPC 解析器从指定子网中的可用 IP 地址中为您选择 IP 地址，还是要自己指定 IP 地址。

如果您选择自己指定 IP 地址，请输入 IPv4 地址。 IPv6 不支持。

标签

指定一个或多个键及对应的值。例如，您可以为 Key（密钥）指定 Cost center（成本中心），并为 Value（值）指定 456。

这些是 Amazon 账单与成本管理 用于整理 Amazon 账单的标签；您也可以将标签用于其他目的。有关对成本分配使用标签的更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

为出站端点创建转发规则

您还可以为出站端点创建转发规则。有关更多信息，请参阅 创建转发规则并将这些规则与一个或多个规则关联 VPCs。

管理 Resolver on Outpost

要管理 Resolver on Outpost，请执行相关步骤。

主题

- 编辑 Resolver on Outpost
- 查看 Resolver on Outpost 状态
- 删除 Resolver on Outpost

编辑 Resolver on Outpost

要编辑 Resolver on Outpost，请执行以下步骤。

编辑 Resolver on Outpost

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选标记，然后选择编辑。
5. 您可以编辑以下信息：
   - VPC 解析器名称
   - 实例类型
   - 实例数
6. 完成编辑后，选择保存更改。

查看 Resolver on Outpost 状态

要查看 Resolver on Outpost 的状态，请执行以下步骤。

查看入站端点的状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选标记，然后选择查看详情。
5. Resolver on Outpost 页面的状态列包含以下值之一：

   Creating

   Resolver on Outpost 正在创建中。

   正常运行

   Resolver on Outpost 配置正确。

   Updating

   Resolver on Outpost 正在更新实例类型。

需要操作

此 VPC 解析器运行状况不佳，无法自动恢复。要解决此问题，我们建议您确保该实例 Amazon Outposts 可以在 Outpost 上支持 Resolver。

Deleting

Resolver on Outpost 正在删除中。

创建失败

Resolver on Outpost 创建失败。

删除失败

Resolver on Outpost 删除失败。要修正此问题，请在几分钟后重试。

删除 Resolver on Outpost

> **Note**
>
> 在删除 Resolver on Outpost 之前，必须先删除与其关联的所有端点。

要删除 Resolver on Outpost，请执行以下步骤。

删除 Resolver on Outpost

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选框，然后选择删除。
5. 在删除 VPC 解析器对话框中，**delete**在文本框中输入，然后选择删除。

管理 Resolver on Outpost 上的入站端点

要管理 Resolver on Outpost 上的入站端点，请执行相关步骤。

主题

查看和编辑入站端点

要查看和编辑入站端点的设置，请执行以下步骤。

查看和编辑入站端点的设置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于运行状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 在入站端点列表中，选择您要查看或编辑设置的端点对应的选项。
6. 选择 View details (查看详细信息) 或 Edit (编辑)。

   有关入站端点的值的信息，请参阅在 Amazon Outposts上创建或编辑出站端点时指定的值。
7. 如果选择 Edit (编辑)，请输入适用的值，然后选择 Save (保存)。

查看入站端点的状态

要查看入站端点的状态，请执行以下过程。

查看入站端点的状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于操作状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 入站端点列表的状态列包含以下值之一：

Creating

VPC 解析器正在为该终端节点创建和配置一个或多个 Amazon VPC 网络接口。

正常运行

此终端节点的 Amazon VPC 网络接口配置正确，能够在您的网络和 VPC 解析器之间传递入站或出站 DNS 查询。

Updating

解析程序正在将一个或多个网络接口与此端点关联或解除其关联。

自动恢复

VPC Resolver 正在尝试恢复与此终端节点关联的一个或多个网络接口。在恢复过程中，端点可以工作但容量受限，因为每个 IP 地址（每个网络接口）的 DNS 查询数有限制。有关当前限制，请参阅Route 53 VPC 解析器的配额。

需要操作

此终端节点运行状况不佳，VPC 解析器无法自动将其恢复。要解决该问题，我们建议您检查与此端点关联的每个 IP 地址。对于每个不可用的 IP 地址，请添加另一个 IP 地址，然后删除该不可用 IP 地址。端点必须始终包含至少两个 IP 地址。状态 Action needed (需要操作) 可能有各种原因。以下是两个常见原因：

- 已使用 Amazon VPC 删除与端点关联的一个或多个网络接口。
- 出于某种不在 VPC Resolver 控制范围内的原因，无法创建网络接口。

Deleting

解析程序正在删除此端点和关联的网络接口。

删除入站端点

要删除入站端点，请执行以下步骤。

> **Important**
> 如果您删除入站终端节点，则来自您的网络的 DNS 查询将不再转发到您在终端节点中指定的 VPC 中的 VPC 解析器。

删除入站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于操作状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 选中想要删除的端点旁边的复选框。
6. 选择删除。
7. 要确认您要删除该端点，请输入端点的名称并选择 Submit (提交)。

管理 Resolver on Outpost 上的出站端点

要管理 Resolver on Outpost 上的出站端点，请执行相关步骤。

主题

查看和编辑出站端点

要查看和编辑出站端点的设置，请执行以下步骤。

查看和编辑出站端点的设置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于操作状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 在出站端点列表中，选择您要查看或编辑设置的端点旁的复选框。
6. 选择 View details (查看详细信息) 或 Edit (编辑)。

   有关出站端点的值的信息，请参阅在 Amazon Outposts上创建或编辑出站端点时指定的值。

7. 如果选择 Edit (编辑)，请输入适用的值，然后选择 Save (保存)。

查看出站端点的状态

要查看出站端点的状态，请执行以下过程。

查看出站端点的状态

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 在导航栏上，选择您 Amazon Outposts 所在的地区。
4. 选中处于操作状态的 VPC 解析器旁边的复选框，然后选择查看详情。
5. 出站端点列表的状态列包含以下值之一：

   Creating

   VPC 解析器正在为该终端节点创建和配置一个或多个 Amazon VPC 网络接口。

   正常运行

   此终端节点的 Amazon VPC 网络接口配置正确，能够在您的网络和 VPC 解析器之间传递入站或出站 DNS 查询。

   Updating

   解析程序正在将一个或多个网络接口与此端点关联或解除其关联。

   自动恢复

   VPC Resolver 正在尝试恢复与此终端节点关联的一个或多个网络接口。在恢复过程中，端点可以工作但容量受限，因为每个 IP 地址（每个网络接口）的 DNS 查询数有限制。有关当前限制，请参阅Route 53 VPC 解析器的配额。

   需要操作

   此终端节点运行状况不佳，VPC 解析器无法自动将其恢复。要解决该问题，我们建议您检查与此端点关联的每个 IP 地址。对于每个不可用的 IP 地址，请添加另一个 IP 地址，然后删除该不可用 IP 地址。（端点必须始终包含至少两个 IP 地址。）状态 Action needed (需要操作) 可能有各种原因。以下是两个常见原因：

   - 已使用 Amazon VPC 删除与端点关联的一个或多个网络接口。

- 出于某种不在 VPC Resolver 控制范围内的原因，无法创建网络接口。

Deleting

解析程序正在删除此端点和关联的网络接口。

删除出站端点

在删除端点之前，必须先删除与 VPC 关联的所有规则。

要删除出站端点，请执行以下步骤。

> **Important**
>
> 如果您删除出站终端节点，VPC 解析器将停止将 DNS 查询从您的 VPC 转发到您的网络，以获取指定已删除出站终端节点的规则。

删除出站端点

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，展开解析程序，然后导航到 Outposts。
3. 选中处于操作状态的 VPC 解析器旁边的复选框，然后选择查看详情。
4. 在出站端点列表中，选择您要删除的端点对应的选项。
5. 选择删除。
6. 要确认您要删除该端点，请输入端点的名称，然后选择 Submit (提交)。

什么是 Route 53 全球解析器？

Route 53 Global Resolver 是一款可访问互联网的 DNS 解析器，可为组织中的远程位置、分支机构和本地环境中的授权客户提供简单、安全和可靠的 DNS 解析。您可以解析托管在 Amazon Route 53 私有托管区域上的域名或互联网上的公共域名的查询，同时通过全球 anycast 架构保持高可用性。Route 53 Global Resolver 通过筛选对潜在恶意域的查询，帮助您保护客户免受基于 DNS 的数据泄露攻击。

Route 53 Global Resolver 使用任播 IP 地址，自动将 DNS 查询路由到离您的源查询位置最近的 Amazon 区域，以实现最佳延迟和可用性。您可以选择您的全球解析器应从中为您的授权客户端提供 DNS 解析的地区，为客户机配置不同的私有域和公共域名解析视图，过滤恶意域名以及监控组织内的 DNS 活动。

主题

为什么选择 Route 53 全球解析器？

Route 53 Global Resolver 为跨多个位置的远程和混合客户端以及工作负载提供集中式 DNS 安全和筛选。无论您的工作负载、应用程序或用户位于何处，Route 53 Global Resolver 都能确保一致的 DNS 保护，而无需复杂的本地基础架构。

远程和混合环境的主要好处：

- 简化管理-使用单一解决方案配置私有域和公共域解析，而不是管理多个本地 DNS 服务器
- 统一 DNS 安全-在所有远程客户端和混合工作负载上应用一致的筛选策略
- 可扩展的保护-自动扩展以处理来自不断增长的远程员工和云工作负载的 DNS 查询
- 减少基础架构-最大限度地减少每个远程位置对 DNS 安全设备的需求

要开始使用，请参阅：

- the section called “概念和术语”-DNS 安全部署的核心概念
- the section called “工作原理”-Route 53 全球解析器如何保护远程和混合环境
- the section called “教程：创建你的第一个 Route 53 全球解析器”-首次设置 DNS 过滤的教程

Route 53 全球解析器的关键概念和组件

Route 53 Global Resolver 使用多个关键组件协同工作，为您的组织提供分流的 DNS 解析、通过全球任播架构实现的高可用性以及全面的 DNS 安全。了解这些 Route 53 Global Resolver 概念有助于您设计和部署解决方案，以实现对私有和公共资源的无缝访问，确保跨多个区域的服务连续性，并防范基于 DNS 的威胁。

适用于本地和远程位置客户端的 DNS 解析器

要为分布式工作负载、客户地点和用户部署 Route 53 Global Resolver，请配置以下关键组件：

全局解析器

主服务实例，可为您的组织提供跨多个 Amazon 区域的 DNS 解析和筛选。您的全球解析器使用 anycast 技术将 DNS 查询自动路由到最近的可用区域，从而确保所有客户都能快速响应，无论其位置如何。

任播 IP 地址

分配给您的全局解析器的两个唯一 IPv6 地址 IPv4 或您在客户端设备和网络设备上配置的地址。这些任播 IP 地址在全球范围内是相同的，这简化了所有位置的 DNS 配置。Anycast IP 寻址支持将 DNS 请求自动路由到最近的全球解析器，从而优化响应时间并提高服务可靠性。

DNS 视图

配置模板允许您将不同的 DNS 策略应用于网络中的不同客户端组。使用 DNS 视图实现水平分割 DNS，例如，对远程位置应用严格的筛选和令牌身份验证，同时对分支机构使用基于 IP 的访问和不同的安全策略。

DNS 客户端身份验证

选择最适合您的部署的身份验证方法：

基于令牌的身份验证

使用 (DoH) 和 DNS-over-HTTPS DNS-over-TLS (DoT) 的加密令牌保护 DNS 连接。您可以为单个客户端或设备组生成唯一的访问令牌，设置到期期限，并根据需要撤消令牌。

基于访问源的身份验证

使用 IP 地址和 CIDR 范围许可列表控制访问权限。您可以配置分支机构的公有 IP 地址或网络范围，然后根据您的安全要求指定每个地点可以使用哪些 DNS 协议（DNS-over-Port-53、DoT 或 DoH）。

DNS 协议选择

根据您的安全性和兼容性需求选择适当的 DNS 协议：

- DNS-over-Port-53 (Do53)-用于最大限度地提高与现有网络基础设施的兼容性
- DNS-over-TLS (DoT)-需要使用带有专用端口隔离的加密 DNS 进行网络监控时使用
- DNS-over-HTTPS (DoH)-需要绕过网络限制时使用，因为流量显示为常规 HTTPS

分流量 DNS 解析

Route 53 Global Resolver 使组织能够从任何位置无缝解析私有域和公共域，无需复杂的 VPN 配置或特定于区域的 DNS 设置。

混合 DNS 解析

混合 DNS 解析允许 Route 53 Global Resolver 同时解析来自本地用户和应用程序到私有应用程序的 Amazon查询。

全球私有区域访问权限

全球私有区域访问将 Amazon Route 53 私有托管区域的覆盖范围扩展到了 VPC 边界之外。Internet 上任何地方的授权客户都可以解析私有域名，从而使分散的团队无需传统的网络连接要求即可访问内部资源。

无缝故障转移

无缝故障转移可确保即使个别 Amazon 区域不可用，也能持续访问私有和公共资源。anycast 架构可自动将查询路由到健康区域，同时保持一致的解析行为。

高可用性和全球影响力

Route 53 Global Resolver 通过分布式架构和自动故障转移功能提供企业级可用性。

多区域部署

多区域部署将 Route 53 Global Resolver 实例分布到至少 2 个 Amazon 区域，以确保高可用性并允许在服务中断期间进行故障转移。您可以根据地理要求和合规性需求选择特定的区域。

自动地理优化

自动地理优化会根据网络拓扑和延迟将 DNS 查询路由到最近的可用 Amazon 区域。这缩短了响应时间，改善了分布在全球的组织的用户体验。

内置冗余

内置冗余功能可在主区域不可用时自动故障转移到备用区域，从而确保服务的连续性。当流量被透明地重新路由时，客户端继续使用相同的任播 IP 地址。

DNS 解析和转发

私有托管区域解析

私有托管区域解析使 Route 53 全球解析器能够跨 Amazon 区域解析对 Route 53 私有托管区域的 DNS 查询。这样，授权的客户端就可以从互联网上的任何地方解析由 Route 53 托管的应用程序和资源的域名。

地平线分割 DNS

Split-Horizon DN S 根据进行查询的客户端提供不同的 DNS 响应。Route 53 Global Resolver 可以解析互联网上的公共域，同时解析私有域，从而提供对公共和私有资源的无缝访问。

DNSSEC 验证

DNSSEC 验证验证来自公共域名服务器的 DNSSEC 签名域的 DNS 响应的真实性和完整性。此验证可确保 DNS 响应在传输过程中不会被篡改，从而防范 DNS 欺骗和缓存中毒攻击。

EDNS 客户端子网 (ECS)

EDNS 客户端子网是一项可选功能，可将 DNS 查询中的客户端子网信息转发给权威域名服务器。这可以实现更准确的基于地理位置的 DNS 响应，通过将客户端定向到更近的内容交付网络或服务器，从而有可能减少延迟。对于 DNS-over-TLS (DoT) 和 DNS-over-HTTPS (DoH) 连接，您可以使用 EDNS0 传递客户端 IP 地址信息。在全局解析器上启用 ECS 后，如果查询中未提供客户端 IP，则该服务会自动注入客户端 IP。

DNS 过滤和域名列表

Route 53 Global Resolver 使用管理的域列表提供基于域的筛选 Amazon ，以屏蔽或允许特定域。

DNS 过滤规则

DNS 过滤规则定义了 Route 53 全球解析器如何根据域匹配标准处理 DNS 查询。规则按优先级顺序进行评估，可以为对特定域或域类别的查询指定操作（允许、阻止或警报）。

域名列表

域列表是过滤规则中使用的域的集合。它们可以是：

- 自定义域名列表-您创建和维护的域名集合
- Amazon 托管域列表-预先配置的威胁列表和由其维护的内容类别 Amazon ，它们利用威胁情报来识别恶意域。可用的威胁列表包括：
  - 恶意软件域-已知托管或分发恶意软件的域名
  - 僵尸网络命令和控制-僵尸网络用于命令和控制通信的域
  - 垃圾邮件-与垃圾邮件和有害电子邮件活动相关的域名
  - 网络钓鱼-网络钓鱼攻击中用于窃取凭据和个人信息的域名
  - Amazon GuardDuty 威胁列表-由 GuardDuty 威胁情报识别的域名

可用内容类别包括社交媒体、赌博和其他帮助组织控制对特定类型内容的访问权限的类别。

为了保护知识产权和保持安全有效性，无法查看或编辑托管列表中的各个域名规范。

高级 DNS 威胁检测

Route 53 Global Resolver 使用动态算法分析来检测高级 DNS 威胁，例如 DNS 隧道和域生成算法。与匹配已知不良域名的域列表不同，算法检测会实时分析 DNS 查询模式以识别可疑行为。

DNS 隧道检测

DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

域生成算法 (DGA) 检测

攻击者使用域生成算法 (DGAs) 为其 command-and-control服务器创建大量域名。

置信度阈值

每种检测算法都会输出一个确定规则触发的置信度分数。更高的置信阈值可以减少误报，但可能会错过复杂的攻击。较低的阈值会提高检测灵敏度，但需要额外的警报分析才能过滤误报。

操作限制

高级威胁防护规则仅支持`ALERT`和`BLOCK`操作。不支持该`ALLOW`操作，因为算法检测无法对良性流量进行明确分类，只能识别潜在的恶意模式。

监控和日志记录

查询 日志

查询日志提供有关 Route 53 Global Resolver 处理的 DNS 查询的详细信息，包括源 IP、查询的域、响应代码、采取的策略操作和时间戳。日志可以传送到亚马逊 CloudWatch、Amazon Data Firehose 或亚马逊简单存储服务，用于分析和合规报告。

OCSF 格式

开放网络安全架构框架 (OCSF) 格式是 Route 53 Global Resolver 用于 DNS 查询日志的标准化日志格式。这种格式提供一致的结构化数据，可轻松与安全信息和事件管理 (SIEM) 系统和其他安全工具集成。

日志目的地

日志目标决定了 DNS 查询日志的传送位置，每个日志都有不同的特征：

- Amazon 简单存储服务-经济实惠的长期存储，非常适合合规和批量分析。与亚马逊 Athena 和亚马逊 EMR 等分析工具集成。
- Ama CloudWatch zon Logs-与亚马逊警报和控制面板集成的实时监控和 CloudWatch 警报。支持临时查询的日志见解。
- Amazon Data Firehose-具有内置数据转换功能的实时流式传输到外部系统。支持自动缩放和缓冲。

可观测性区域

可观察性区域决定 DNS 查询日志的传送位置。

Route 53 全球解析器的工作原理

Route 53 Global Resolver 支持在公有域和私有域之间进行分流的 DNS 解析，通过 Amazon Web Services 区域 您选择的两个或更多域名提供高可用性，并通过拦截请求和应用 DNS 过滤策略来保护 DNS 查询。了解此过程有助于您解决问题并优化部署以提高性能、可用性和安全性。

当客户端进行 DNS 查询时会发生什么

当你所在地有人尝试查询域名时，Route 53 Global Resolver 会通过多个安全层处理他们的 DNS 请求。

DNS 查询处理包括以下顺序步骤：

1. 查询接收-客户端设备向 Route 53 全球解析器任播 IP 地址发送 DNS 查询。anycast 路由会自动将查询定向到最近的 Amazon 区域。
2. 身份验证-Route 53 Global Resolver 使用配置的身份验证方法（所有协议均基于令牌 DoH/DoT 或 IP 访问源）对客户端进行身份验证。
3. 策略评估-该服务根据配置的安全策略和域列表评估 DNS 查询，以确定适当的操作（允许、阻止或警报）。对于针对私有托管区域的查询，Route 53 Global Resolver 会在继续解析之前，根据管理员管理的 DNS 视图规则，检查客户端是否有权访问私有域。
4. 解@@ 析-对于允许的查询，Route 53 Global Resolver 会根据需要使用公共 DNS 解析器或私有托管区域解析来执行 DNS 解析。
5. 响应传送-该服务将 DNS 响应返回给客户端，并记录查询详细信息以供监控和分析。

全球任播架构

Route 53 Global Resolver 使用任播 IP 地址提供全球可用性和自动地理路由。

Route 53 全球解析器使用任播 IP 地址提供：

- 自动地理路由-DNS 查询会自动路由到最近的 Amazon 区域，以获得最佳性能。
- 内置冗余-如果某个区域不可用，流量会自动故障转移到下一个最近的区域。
- 一致的 IP 地址-无论位于何处，客户端都使用相同的任播 IP 地址，从而简化了配置。

DNS 过滤和安全

Route 53 Global Resolver 通过多层提供全面的 DNS 过滤和安全。DNS 过滤和安全架构图说明了如何通过身份验证、策略评估和解析层处理查询。

Route 53 全球解析器通过以下方式提供全面的 DNS 安全：

- 基于域的筛选-使用自定义或 Amazon 托管域列表阻止或允许基于域名的查询。
- 威胁情报集成-利用 Amazon 托管威胁情报自动阻止已知的恶意域名。
- 高级威胁检测-检测和阻止 DNS 隧道尝试和域生成算法 (DGA) 模式。
- 实时监控-生成有关安全事件和违反策略的警报和日志。

Route 53 全球解析器的 DNS 安全和水平分割用例

Route 53 全球解析器解决了组织面临的三个主要的 DNS 难题：

在公有 DNS 和私有 DNS 解析之间启用分流量

允许从任何位置全局访问 Amazon Route 53 上的私有托管区域 (PHZs)，同时解析互联网上的公共域。允许远程位置和分支机构解析内部应用程序名称，而无需复杂的 VPN 配置或特定于区域的转发。实施水平分割 DNS 以根据进行查询的客户端提供不同的 DNS 响应，从而帮助远程客户端解析私有域和公共域的查询。

保护 DNS 流量免受 DNS 泄露攻击

通过筛选对恶意域的查询，保护远程位置和分支机构免受基于 DNS 的数据泄露攻击。使用 DNS-over-HTTPS (DoH) 和 DNS-over-TLS (DoT) 对传输中的 DNS 流量进行加密，确保只有经过授权的客户端才能访问您的 DNS 服务，从而提高隐私。应用安全策略来阻止 DNS 隧道和域生成算法

（ ）DGAs等威胁。使用 DNSSEC 签名域的 DNSSEC（域名系统安全扩展）验证 DNS 响应的真实性，以防范 DNS 欺骗和缓存中毒攻击。

高可用性和全球影响力

通过全球部署实现高可用性，并通过单一管理界面在全球范围内保持一致的 DNS 配置。Route 53 Global Resolver 在 Amazon Web Services 区域 您选择的范围内运行，使用任播 IP 地址自动将查询路由到最近的可用区域，以实现最佳性能和可靠性。全球企业可以集中配置和管理 DNS 策略，同时为客户提供一组 IP 地址，这些地址可在全球范围内自动进行地理优化。内置冗余功能可确保即使个别区域不可用，也能保持服务连续性。

其他功能支持以下主要用例：

实施 DNS 筛选和内容策略

通过创建自定义域名列表或使用 Amazon 托管域名列表来管理多个位置的互联网访问。为了帮助您根据需要实施筛选和内容策略，托管域列表包括涵盖多个域的多类 DNS 威胁。使用 IP 许可名单或访问令牌配置访问源，并为不同的办公地点或客户群组设置不同的筛选策略。

针对不同部署场景的灵活身份验证

选择最适合您的部署的身份验证方法：基于令牌的身份验证或使用源 CIDR 范围许可名单的基于 IP 的身份验证。

保持可见性和合规性

通过向亚马逊 CloudWatch、Firehose 或亚马逊简单存储服务传输日志，监控整个组织的 DNS 活动。为集中日志存储选择一个目标区域，以支持安全审计、合规性要求和威胁调查。

Amazon 与 Route 53 全球解析器集成的服务可增强 DNS 安全性

Route 53 Global Resolver 与其他 Amazon 服务无缝集成，提供全面的 DNS 安全和管理功能。这些集成增强了 Route 53 Global Resolver 的核心功能，并支持高级用例：

Amazon Route 53

Route 53 Global Resolver 与 Amazon Route 53 集成，在全球范围内解析私有托管区域。有关更多信息，请参阅 Amazon Route 53 开发人员指南。

亚马逊 CloudWatch

Route 53 Global Resolver 可以将查询日志传送到亚马逊 CloudWatch 进行监控和分析。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

Amazon Simple Storage Service

Route 53 Global Resolver 可以将查询日志存储在亚马逊简单存储服务存储桶中，以便长期存储和分析。有关更多信息，请参阅 Amazon S3 用户指南。

Amazon Data Firehose

Route 53 Global Resolver 可以将查询日志流式传输到 Amazon Data Firehose 进行实时处理。有关更多信息，请参阅《Amazon Data Firehose 开发人员指南》。

Route 53 Resolver DNS Firewall

Route 53 全球解析器通过提供全局 DNS 过滤功能来补充 Route 53 解析器 DNS 防火墙。有关更多信息，请参阅 R oute 53 解析器 DNS 防火墙文档。

Amazon Global Accelerator

Route 53 全球解析器可与 Amazon Global Accelerator Route 53 配合使用，为 DNS 解析提供优化的全球网络性能。有关更多信息，请参见Amazon Global Accelerator 开发人员指南。

如何通过 Amazon 接口访问和管理 Route 53 全球解析器

Route 53 Global Resolver 提供了多种访问方法，以适应不同的管理偏好和自动化要求。您可以通过以下接口管理 Route 53 全局解析器：

Amazon Web Services 管理控制台

为 Route 53 全球解析器 Amazon Web Services 管理控制台 提供了一个基于 Web 的界面。您可以使用控制台配置 DNS 过滤策略、管理身份验证设置和监控查询日志。

Amazon Command Line Interface (Amazon CLI)

Amazon CLI 提供对 Route 53 全球解析器 API 操作的直接访问。您可以使用自动执行 Route 53 Global Resolver 任务，并将其集成到您的脚本和工作流程中。 Amazon CLI

Amazon SDKs

Amazon SDKs 提供了多种编程语言。您可以使用将 Cloud Resolver 功能集成 SDKs 到您的应用程序中。

REST API

Route 53 Global Resolver 提供了一个 REST API，你可以用它来以编程方式管理 DNS 解析和过滤策略。

支持 Amazon Web Services 区域

Route 53 Global Resolver 有以下 Amazon Web Services 区域版本：

- US East (N. Virginia) Region
- 美国东部（俄亥俄州）区域
- 美国西部（北加利福尼亚）区域
- 美国西部（俄勒冈州）区域
- 欧洲地区（法兰克福）区域
- 欧洲地区（爱尔兰）区域
- 欧洲地区（伦敦）区域
- 亚太地区（孟买）区域
- 亚太地区（新加坡）区域
- 亚太地区（东京）区域
- 亚太地区（悉尼）区域

为 Route 53 Global Resolver 设置账户访问权限

在开始使用 Route 53 Global Resolver 之前，您需要一个 Amazon 账户和相应的权限才能访问 Route 53 全球解析器资源。这包括创建具有必要权限的 IAM 用户和角色。

本节将指导您完成配置用户和角色以访问 Route 53 Global Resolver 所需的步骤。

主题

注册获取 Amazon Web Services 账户

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

要注册 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 Amazon Web Services 账户，就会创建Amazon Web Services 账户根用户一个。根用户有权访问该账户中的所有 Amazon Web Services 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看当前账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

创建策略和角色

配置 Amazon 身份和访问管理 (IAM) 权限，以便您的团队可以部署和管理 Route 53 全球解析器资源。您可以使用管理权限获得完全访问权限，也可以使用只读权限来监视和查看配置。

所有 Route 53 全球解析器 API 操作都需要适当的 IAM 权限。如果您没有所需的权限，API 调用将返回 `AccessDeniedException` (401) 或 `UnauthorizedException` (401) 错误。

管理权限

如果您是首次设置 Route 53 Global Resolver 或管理服务的各个方面，则需要管理权限。您可以使用以下 Amazon 托管策略：

- AmazonRoute53GlobalResolverFullAccess-提供对 Route 53 全球解析器资源的完全访问权限，包括创建、更新和删除全局解析器、DNS 视图、防火墙规则和域列表
- AmazonRoute53FullAccess-如果您计划使用私有托管区域转发，则为必填项
- CloudWatchLogsFullAccess-如果您计划向 Amazon 发送日志，则为必填项 CloudWatch
- AmazonS3FullAccess-如果您计划从 Amazon S3 导入防火墙域列表或向 Amazon S3 发送日志，则为必填项

只读权限

如果您只需要查看 Route 53 Global Resolver 的配置和日志，则可以使用以下 Amazon 托管策略：

- AmazonRoute53GlobalResolverReadOnlyAccess-提供对 Route 53 全球解析器资源的只读访问权限，包括查看全局解析器、DNS 视图、防火墙规则、域列表和访问源
- AmazonRoute53ReadOnlyAccess-需要查看私有托管区域关联
- CloudWatchReadOnlyAccess-需要在 Amazon 中查看日志 CloudWatch
- AmazonS3ReadOnlyAccess-需要查看存储在 Amazon S3 中的防火墙域列表文件

网络注意事项

在实施 Route 53 全球解析器之前，请考虑以下网络要求：

客户端 IP 范围

只有在使用基于访问源的身份验证时才需要这样做。确定将使用 Route 53 全球解析器的所有客户端的 IP 地址范围（CIDR 块）。您需要这些来配置访问来源的规则。

DNS 协议

确定您的客户端将使用哪些 DNS 协议：

- Do53- 端口 53 上的标准 DNS (UDP/TCP)
- DoH- DNS-over-HTTPS 用于加密查询
- DoT- DNS-over-TLS 用于加密查询

防火墙和安全组

确保您的网络防火墙和安全组允许在相应的端口（Do53 为 53，DoH 为 443，DoH 为 443，交通部为 853，交通部为 853）上的 Route 53 Global Resolver anycast IP 地址的出站流量。

教程：创建你的第一个 Route 53 全球解析器

本入门指南演示了 Route 53 Global Resolver 的基本组件，并可选择创建简单的 DNS 过滤设置。本教程涵盖了核心概念，但不包括客户机配置、日志记录或私有域解析等生产要求。

完成后，您将获得基本的 Route 53 全局解析器设置，该设置可以过滤 DNS 查询并阻止恶意域。

以下各节介绍如何使用 Route 53 全球解析器快速开始使用 DNS 安全和筛选。

先决条件

在使用 Route 53 Global Resolver 之前，您需要一个 Amazon 帐户和相应的权限才能访问、查看和编辑 Route 53 全球解析器组件。您的系统管理员必须完成中的步骤the section called “设置账户访问权限”，然后返回本教程。

步骤 1：创建全局解析器

首先，创建一个全球解析器实例，然后选择它将运行的 Amazon 区域。

1. 打开 Route 53 全球解析器控制台，网址为https://console.aws.amazon.com/route53globalresolver/。
2. 选择 “创建全局解析器”。
3. 在 “名称” 中，输入全球解析器的描述性名称。
4. 在描述中，可以选择输入描述。
5. 对于区域，选择两个或更多要 Amazon Web Services 区域 在其中实例化全局解析器。选择离客户端最近的区域，以获得最佳性能。
6. （可选）添加标签以帮助组织和管理您的资源。
7. 选择 “创建全局解析器”。

您将立即收到任播 IPv4 地址，您的客户可以使用这些地址来联系解析器。全局解析器创建过程需要几分钟才能完成，地址才会起作用。

步骤 2：创建 DNS 视图并配置身份验证

创建 DNS 视图以组织您的客户端，并使用 IP 访问源配置身份验证。本教程使用基于 IP 的身份验证。您也可以将访问令牌用于卫生部/交通部协议。

1. 在 Route 53 全球解析器控制台中，选择您的全局解析器。
2. 选择创建 DNS 视图。
3. 在名称中，输入您的 DNS 视图的描述性名称。
4. 在描述中，可以选择输入描述。
5. 选择创建 DNS 视图。
6. 创建 DNS 视图后，选择访问源，然后选择创建访问源。
7. 对于 CIDR 阻止，请输入您的客户机的 IP 地址范围（例如，`203.0.113.0/24`）。
8. 对于协议，请选择 Do53（端口 53 上的 DNS）进行基本设置。
9. 选择 “创建访问源规则”。

步骤 3：配置 DNS 过滤规则（可选）

设置基本的 DNS 过滤规则以阻止对恶意域的访问。

1. 在 DNS 视图中，选择防火墙规则，然后选择创建防火墙规则。
2. 在名称中，输入规则的描述性名称。
3. 对于 “优先级”，输入`100`（数字越小优先级越高）。
4. 在 “操作” 中，选择 “屏蔽”。
5. 对于域列表类型，请选择Amazon 托管域列表。
6. 在托管域列表中，选择恶意软件AmazonGuardDutyThreatList和僵尸网络命令与控制以阻止已知的恶意域（您可以添加其他托管列表或稍后创建自定义列表）。
7. 选择创建防火墙规则。

第 4 步：测试您的配置

测试您的 Route 53 全局解析器配置是否正常运行。

1. 在您配置的 CIDR 范围内的客户端计算机上，使用全局解析器提供的任播 IP 地址测试 DNS 解析：

```
nslookup example.com <anycast-ip-address>
```

2. 验证合法域名是否能正确解析。
3. 测试被屏蔽的域名是否被正确过滤。您可以使用测试域创建自定义域名列表，以验证您的防火墙规则是否正常运行。有关托管域列表的更多信息，请参阅托管域列表。
4. 查看 Route 53 全球解析器控制台，了解查询日志和筛选活动。

有关全面的测试程序和故障排除，请参阅 Route 53 全球解析器故障排除。

步骤 5：监控 DNS 活动

为您的 DNS 活动配置日志记录。

1. 选择可观测性区域。
2. 选择查询日志的目的地。

有关全面的测试程序和故障排除，请参阅 R oute 53 Global Resolver 的测试和故障排除。

步骤 6：清理（可选）

如果您创建此配置是出于测试目的，并且不想继续使用 Route 53 Global Resolver，请清理资源以避免持续收费。

1. 在 Route 53 全球解析器控制台中，删除您创建的所有防火墙规则。
2. 删除您创建的所有访问源规则。
3. 删除 DNS 视图。
4. 删除全局解析器。

> **Important**
>
> 删除这些资源将停止任何配置为使用这些资源的客户机的 DNS 解析。在删除解析器或移除访问规则之前，请更新您的客户端配置。

后续步骤

现在您已经有了基本的 Route 53 全局解析器配置，您可以探索其他功能：

- 将客户端设备配置为使用您的解析器（生产时需要）。更新您的客户端 DNS 设置，以使用全局解析程序提供的任播 IP 地址。
- 设置日志记录以进行监控和满足合规性（建议用于生产）。配置到亚马逊 CloudWatch、亚马逊 S3 或 Amazon Data Firehose 的日志以进行监控和分析。有关更多信息，请参阅 使用 Route 53 全球解析器监控 DNS 活动和性能。
- 为内部域配置私有托管区域转发（如果您有私有 Amazon 资源，则为必填项）。有关更多信息，请参阅使用私有托管区域。
- 使用 DNS-over-HTTPS (DoH) 或 DNS-over-TLS (DoT) 设置加密的 DNS 连接。有关更多信息，请参阅配置加密 DNS。
- 创建自定义域列表和高级筛选规则。有关更多信息，请参阅 DNS 筛选。

使用 Route 53 全球解析器管理 DNS 视图

您可以管理正在进行的 Route 53 全球解析器操作，包括更新 DNS 视图以控制哪些客户端设备组可以解析为内部资源以及要过滤哪些域。

管理 DNS 视图

创建 DNS 视图后，您可以更新其配置、启用或禁用它们以及管理其生命周期。

为客户端设备组创建 DNS 视图

DNS 视图是一个逻辑分组，为一组客户端设备（例如远程员工、分支机构设备或本地设备）定义安全策略。每个视图都有自己的身份验证要求、筛选规则和私有托管区域关联。

创建 DNS 视图

1. 打开控制台，网址为https://console.aws.amazon.com/route53globalresolver/。
2. 从列表中选择您的全球解析器。
3. 选择 DNS 视图选项卡。
4. 选择创建 DNS 视图。
5. 在 DNS 查看详细信息部分：

a. 在 DNS 视图名称中，输入 DNS 视图的描述性名称（最多 128 个字符）。

b. （可选）在“描述”中，输入 DNS 视图的描述（最多 255 个字符）。

6. 在 DNS 查询处理部分，配置以下设置：

- DNSSEC 验证 -选择“启用”或“禁用”。DNSSEC 验证使全球解析器能够验证 DNS 响应的真实性。
- 防火墙规则失败打开行为-选择“启用”允许在 DNS 防火墙无法评估查询时继续查询，或者选择“禁用”以阻止此类查询。
- EDNS0 客户端子网-选择“启用”可提高客户端定位精度，以便将流量路由到附近资源并提高缓存效率，或者选择“禁用”以关闭此功能。

7. 选择创建 DNS 视图。

创建 DNS 视图后，您可以配置访问控制、防火墙规则和私有托管区域关联。

编辑 DNS 视图

创建后，您可以修改 DNS 视图设置，包括 DNS 查询处理选项和相关资源。

编辑 DNS 视图

1. 在控制台中，导航到您的全局解析器。
2. 选择 DNS 视图选项卡。
3. 选择要编辑的 DNS 视图，然后选择编辑。
4. 根据需要修改 DNS 视图设置，然后选择保存更改。

启用和禁用 DNS 视图

您可以暂时禁用 DNS 视图而不将其删除。禁用后，全局解析器将停止为与该 DNS 视图关联的客户端设备提供请求。

> **Warning**
>
> 禁用 DNS 视图会立即停止与该视图关联的所有客户端设备的 DNS 解析。确保为受影响的客户端设备配置了备用 DNS 解析。

删除 DNS 视图

在删除 DNS 视图之前，必须先删除所有关联的资源，包括访问源规则、访问令牌、防火墙规则和私有托管区域关联。

> **Warning**
> 删除 DNS 视图是不可逆的，并且会立即停止与该视图关联的所有客户端设备的 DNS 解析。

管理私有托管区域关联

您可以根据需要查看、更新和删除私有托管区域关联，以控制哪些客户端设备组有权访问内部资源。

查看关联

要在 DNS 视图中查看所有私有托管区域关联，请导航到您的 DNS 视图并查看私有托管区域部分以查看所有关联区域及其状态和关联详细信息。

更新关联

您可以通过选择关联、选择编辑、更新关联名称并保存更改来更新私有托管区域关联的名称。

移除关联

删除私有托管区域关联后，Route 53 Global Resolver 将停止使用该区域来解析关联的 DNS 视图的 DNS 查询。

> **Warning**
> 删除私有托管区域关联会立即影响 DNS 解析。对已取消关联区域中的域的查询将使用公有 DNS 而不是私有区域记录进行解析。

在 Route 53 全球解析器中配置 DNS 视图设置

Route 53 Global Resolver 允许您根据不同的客户端设备组的安全要求和访问需求为其配置不同的 DNS 策略和访问控制。根据不同的客户端设备组的安全要求和访问需求，在 Route 53 Global Resolver 中为其设置 DNS 策略和访问控制。

为客户端组配置 DNS 设置

每个 DNS 视图都有多个设置，用于控制如何处理和解析不同客户端设备组的 DNS 查询。

DNSSEC 验证

DNSSEC 验证有助于确保公共域名的 DNS 响应是真实的，并且没有被篡改。启用 DNSSEC 验证后，Route 53 Global Resolver 会检查 DNSSEC 签名，并针对签名无效的域返回 SERVFAIL。

在以下情况下，可以考虑启用 DNSSEC 验证：

- 您的组织需要对 DNS 响应进行加密验证
- 你需要防御 DNS 欺骗和缓存中毒攻击
- 您的合规性要求需要 DNSSEC 验证

> **Note**
>
> DNSSEC 验证仅适用于公共域。私有托管区域使用自己的身份验证机制。

EDNS 客户端子网 (ECS)

EDNS 客户端子网在发送到权威服务器的 DNS 查询中包含有关客户端网络位置的信息。这使内容交付网络和地理分布的服务能够提供适合位置的响应。

ECS 可以帮助您：

- 从地理分布的服务中获得更好的性能
- 提高内容分发网络路由的准确性
- 更好地遵守区域内容限制

隐私注意事项：

- ECS 向权威服务器显示部分客户端 IP 信息（最大值为 /24，最大值为 IPv4 /48） IPv6
- 在启用之前，请考虑贵组织的隐私要求

防火墙无法打开

防火墙失效打开设置决定了由于服务受损或配置问题而无法评估 DNS 防火墙规则时会发生什么。

已禁用（默认）

如果无法评估防火墙规则，则会阻止 DNS 查询。这为您提供了最大的安全性，但可能会在服务出现问题期间影响可用性。

已启用

如果无法评估防火墙规则，则允许 DNS 查询。在出现服务问题期间，这会优先考虑可用性而不是安全性。

组织客户端设备组的最佳实践

在为不同的客户端设备组设计 DNS 视图时，请遵循以下最佳实践：

查看组织策略

- 按安全要求分开-为具有不同安全许可或访问级别的客户端设备创建不同的视图
- 按位置整理-对不同的地理位置或网段使用不同的视图
- 按设备类型分组-为服务器、工作站、移动设备或物联网设备创建专用视图
- 使用描述性名称-选择能清楚表明视图目的和目标客户机设备的名称

安全注意事项

- 最低权限原则-为每个视图配置其客户端设备所需的最低访问权限
- 默认拒绝-从限制性防火墙规则开始，然后根据需要添加例外情况
- 定期审查-定期检查和更新 DNS 视图配置
- 监控使用情况-使用 DNS 查询日志监控和分析 DNS 视图使用模式

在 Route 53 Global Resolver 中使用访问源和令牌管理访问控制

Route 53 Global Resolver 提供了两种控制客户端设备访问的主要方法：基于 IP 的身份验证的访问源和基于令牌的身份验证的访问令牌。本章涵盖了这两种方法，可帮助您为自己的环境选择正确的身份验证方法并实施全面的访问控制。

主题

- 了解 Route 53 全局解析器中的访问控制方法

- 配置访问源和访问源规则
- 管理加密身份验证的访问令牌
- 访问控制最佳实践和安全注意事项

了解 Route 53 全局解析器中的访问控制方法

Route 53 Global Resolver 提供了两种不同的身份验证方法来控制客户端对您的 DNS 基础设施的访问。每种方法都适用于不同的用例和环境。

基于 IP 的访问源

> 您可以配置访问源规则，允许或拒绝基于客户端 IP 地址的 DNS 查询。此方法非常适合 IP 范围可预测的环境，例如分支机构或 VPN 连接。访问源支持所有 DNS 协议（Do53、DoT 和 DoH），并为网络管理员提供了直接的配置。

基于令牌的身份验证

> 访问令牌使用加密的、有时间限制的凭据为 DoH 和 DoT 协议提供安全的身份验证。此方法适用于移动客户端和 IP 地址频繁变化的环境。您可以在令牌到期之前续订令牌，它们通过加密提供增强的安全性。

选择身份验证方法时，请考虑以下因素：

选择正确的身份验证方法

因素	访问来源	访问令牌
适用于	固定 IP 范围、办公网络、VPN 用户	移动设备、动态员工 IPs、远程工作人员
安全级别	基于网络，依赖 IP 信任	加密凭证，有时间限制
管理复杂性	简单的 IP 范围管理	代币生命周期和分发
协议支持	Do53、DoT、DoH	美国交通部，仅限卫生部

您可以同时使用这两种方法来创建分层安全。例如，将访问源用于办公网络，将令牌用于远程工作者。

配置访问源和访问源规则

访问源根据 IP 地址控制客户端的访问权限。您可以创建访问源规则，指定哪些 IP 范围可以查询您的 DNS 基础架构以及它们可以使用哪些协议。

创建访问源规则

按照以下步骤创建访问源规则，允许特定 IP 范围查询您的 DNS 基础架构。

1. 打开 Route 53 全球解析器控制台并导航到您的 DNS 视图。
2. 在访问源部分中，选择创建访问源规则。
3. 在 “名称” 中，输入标识此规则用途的描述性名称，例如`office-network`或`vpn-users`。
4. 对于 IP 地址范围，请指定应具有访问权限的 IP 地址。您可以对 IP 范围使用 CIDR 表示法：`192.168.1.0/24`或单个 IP 地址：`203.0.113.5/32`。
5. 在 “协议” 中，选择此规则适用于的 DNS 协议：
   - Do53- 标准 DNS 上线 UDP/TCP （端口 53）
   - D@@ o T-TLS 上的 DNS（端口 853）
   - 卫生部-通过 HTTPS 进行 DNS（端口 443）
6. 选择 “创建访问源规则”。

来自指定 IP 范围的客户端设备现在可以使用所选协议查询您的 DNS 基础架构。

了解规则评估和优先级

Route 53 Global Resolver 在识别要使用的正确视图时会评估访问源规则。

- 规则按从最具体的 IP 范围到最不具体的 IP 范围进行处理，其中最具体的匹配规则优先。
- 如果没有匹配的规则，则默认情况下请求将被拒绝。

通过从不同的 IP 地址查询来测试您的访问源配置，以确保规则按预期运行。

管理加密身份验证的访问令牌

访问令牌为 DoH 和 DoT 协议提供加密身份验证。与基于 IP 的访问源不同，令牌无论客户位于何处都能正常工作，并通过加密和过期控制提供更高的安全性。

创建访问令牌

按照以下步骤创建访问令牌，以对使用 DoH 或 DoT 协议的客户端设备进行身份验证。

1. 打开 Route 53 全球解析器控制台并导航到您的 DNS 视图。
2. 在访问源部分中，选择创建访问令牌。
3. 在名称中，输入标识令牌用途的描述性名称，例如`mobile-devices`或`remote-workers-q4`。
4. 对于到期，设置令牌的到期时间。出于安全考虑，我们建议 90 天或更短时间。在设置到期期限时，请考虑您的代币分配和续订能力。
5. 选择创建访问令牌。
6. 使用贵组织的安全通信渠道将令牌安全地分发到您的客户端设备。

使用访问令牌配置客户端设备

将客户端设备配置为使用访问令牌对 Route 53 全球解析器基础架构进行身份验证。

卫生部配置

要使用访问令牌配置 DoH，您需要全局解析器的 DNS 名称或 IP 地址：

1. 使用 GetGlobalResolver API 检索解析器的连接详情。
2. 请注意（例如，3.3.3、3.3.4）和`ipv4Addresses`（例如 a1bc234567890a.route53globalresolver.globalresolver.glob dnsName al.on.aws）。
3. 使用 DNS 名称将令牌作为 URL 参数包含在 DoH 端点中：

```
https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<token-value>
```

`<token-value>`用您生成的实际令牌替换。

交通部配置

对于使用访问令牌的 DoT 查询，请将该令牌包含在 EDNS0 选项中，规格如下：

- 选项代码：`0xffa0`
- 选项数据：字符串格式的访问令牌

具体实现取决于您的 DoT 客户端软件及其处理 EDNS0 选项的方式。

代币生命周期管理

管理令牌到期和续订，以维护您的客户端设备的安全访问。

- 监控到期日期-提前跟踪代币到期日期和计划续订。
- 到期前续费-在旧令牌到期之前创建新令牌，以避免服务中断。
- 定期轮换令牌-即使在令牌到期之前也要定期更换令牌，以增强安全性。
- 撤销已被盗的代币-如果您怀疑令牌已被盗用，请立即将其删除。

考虑为大型部署实施自动令牌续订流程，以减少管理开销。

平台配置示例

使用这些特定于平台的示例，使用您的 Route 53 Global Resolver 访问令牌和连接详细信息配置客户端设备。

Windows 配置

按照以下步骤使用 netsh 命令将 Windows 客户端配置为使用带有访问令牌的 DoH。

1. 以管理员身份打开命令提示符。
2. 启用全局 DoH 设置：

```
netsh dns add global doh=yes
```

3. 使用访问令牌注册 DoH 服务器。将示例值替换为实际的解析器详细信息：

```
netsh dns add encryption server=3.3.3.3 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
netsh dns add encryption server=3.3.3.4 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
```

4. 刷新 DNS 缓存：

```
ipconfig /flushdns
```

5. 验证配置：

```
netsh dns show global
```

macOS 配置

按照以下步骤使用带有访问令牌的 DoH 移动配置文件配置 macOS 客户端。

使用以下结构创建移动设备配置文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>DNSSettings</key>
      <dict>
        <key>DNSProtocol</key>
        <string>HTTPS</string>
        <key>ServerAddresses</key>
        <array>
          <string>3.3.3.3</string>
          <string>3.3.3.4</string>
        </array>
        <key>ServerURL</key>
        <string>https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?
token=<your-token></string>
      </dict>
      <key>PayloadType</key>
      <string>com.apple.dnsSettings.managed</string>
    </dict>
  </array>
</dict>
</plist>
```

通过 “系统设置” > “设备管理” 安装配置文件。

访问控制最佳实践和安全注意事项

遵循这些最佳实践，为您的 Route 53 Global Resolver 基础设施维护安全有效的访问控制。

安全最佳实践

实施以下安全措施来保护您的 DNS 基础架构：

- 使用分层身份验证-将可信网络的访问源与移动用户的令牌相结合。这种方法提供了深度防御并适应不同的客户场景。
- 实施最低权限访问权限-仅授予对客户端实际需要的 IP 范围和协议的访问权限。避免过于宽泛的访问源规则，因为这可能会使您的基础架构遭到未经授权的使用。
- 定期轮换令牌-定期更换访问令牌，甚至在访问令牌到期之前。这种做法限制了被盗令牌的影响，并保持了安全卫生。
- 监控访问模式-查看 DNS 查询日志，找出异常的访问模式或潜在的安全问题。为来自意外 IP 范围的查询或使用过期令牌的查询设置警报。

运营最佳实践

请遵循以下操作惯例来维护可靠的访问控制：

- 记录您的访问控制策略-清晰地记录哪些访问源和令牌为哪些客户群提供服务。
- 定期测试访问控制-验证您的访问源规则和令牌在不同的客户端位置和场景中是否正常运行。
- 为令牌续订制定计划-建立在旧代币到期之前分发新代币的流程，以避免服务中断。
- 定期查看访问控制-删除未使用的访问源规则和过期的令牌，以保持干净的配置。

使用 Route 53 全球解析器保护客户端的 DNS

以下各节介绍如何创建规则来保护您的客户端进行的 DNS 查询。

主题

配置和管理 DNS 防火墙规则

创建和查看防火墙规则

防火墙规则定义了 Route 53 Global Resolver 如何根据域列表、托管域列表、内容类别或高级威胁防护处理 DNS 查询。每条规则都指定了优先级、目标域和要采取的操作。

规则优先级的最佳实践：

- 将优先级 100-999 用于高优先级允许规则（可信域）
- 使用优先级 1000-4999 设置屏蔽规则（已知威胁）
- 对警报规则（监控和分析）使用优先级 5000-9999
- 在优先级之间留出空白，以便将来可以插入 future 规则

创建 DNS 防火墙规则

1. 在 Route 53 全球解析器控制台中，导航到您的 DNS 视图。
2. 选择 “防火墙规则” 选项卡。
3. 选择创建防火墙规则。
4. 在 “规则详情” 部分：
   a. 在规则名称中，输入规则的描述性名称（最多 128 个字符）。
   b. （可选）在规则描述中，输入规则的描述（最多 255 个字符）。
5. 在规则配置部分，选择规则配置类型：
   - 客户管理的域名列表-使用您创建和管理的域名列表
   - Amazon 托管域名列表-使用 Amazon 提供的可供您使用的域名列表
   - DNS 防火墙高级保护-从一系列托管保护中进行选择并指定置信阈值
6. 在 “规则操作” 中，选择规则匹配时要采取的操作：
   - 允许-DNS 查询已解决
   - 警报-允许 DNS 查询但会创建警报
   - 屏蔽-DNS 查询已被阻止
7. 选择创建防火墙规则。

使用以下步骤查看分配给他们的规则。您也可以更新规则和规则设置。

查看和更新规则

1. 在 Route 53 全球解析器控制台中，导航到您的 DNS 视图。
2. 选择 DNS 防火墙规则选项卡。
3. 选择要查看或编辑的规则，然后选择编辑。
4. 在 “规则” 页面中，您可以查看和编辑设置。

有关规则的值的信息，请参阅 the section called “DNS Firewall 中的规则设置”。

删除规则

1. 在 Route 53 全球解析器控制台中，导航到您的 DNS 视图。
2. 选择 DNS 防火墙规则选项卡。
3. 选择要删除的规则，然后选择删除，然后确认删除。

DNS Firewall 中的规则设置

在 DNS 视图中创建或编辑 DNS 防火墙规则时，需要指定以下值：

Name

DNS 视图中规则的唯一标识符。

（可选）描述

提供有关规则的更多信息的简短描述。

域名清单

规则检查的域列表。您可以创建和管理自己的域名列表，也可以订阅为您 Amazon 管理的域名列表。

规则可以包含域列表或 DNS Firewall Advanced 保护，但不能同时包含两者。

查询类型（仅限域列表）

此规则检查的 DNS 查询类型列表。有效值如下所示：

- 答：返回 IPv4 地址。
- AAAA：返回 IPv6 地址。
- CAA： CAs 可以为域名创建 SSL/TLS 认证的限制。
- CNAME：返回另一个域名。

- DS：标识委派区域 DNSSEC 签名密钥的记录。
- MX：指定邮件服务器。
- NAPTR： Regular-expression-based重写域名。
- NS：权威名称服务器。
- PTR：将 IP 地址映射到域名。
- SOA：此区的授权起始点记录。
- SPF：列出有权从某个域发送电子邮件的服务器。
- SRV：用于标识服务器的特定应用程序值。
- TXT：验证电子邮件发件人和特定应用程序的值。

您使用 DNS 类型 ID 定义的查询类型，例如 AAAA 的类型为 28。这些值必须定义为 TYPENUMBER，其中NUMBER可以是 1-65334，例如，。 TYPE28有关更多信息，请参阅 DNS 记录类型列表。

您可以为每条规则创建一个查询类型。

DNS Firewall Advanced 保护

根据 DNS 查询中的已知威胁签名检测可疑 DNS 查询。您可以选择如下方面的保护：

- 域生成算法 (DGAs)

  DGAs 被攻击者用来生成大量域来发起恶意软件攻击。

- DNS 隧道

  DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

在 DNS Firewall Advanced 规则中，您可以选择阻止与威胁匹配的查询或针对其发出提醒。

有关更多信息，请参阅 DNS 防火墙高级保护。

规则可以包含 DNS Firewall Advanced 保护或域列表，但不能同时包含两者。

置信度阈值（仅限 DNS Firewall Advanced）

DNS Firewall Advanced 的置信度阈值。创建 DNS Firewall Advanced 规则时必须提供此值。置信度值代表：

- 高 – 仅检测证实度最高的威胁，误报率低。
- 中 – 在检测威胁和误报之间保持平衡。
- 低 – 提供最高威胁检测率，但也会增加误报。

有关更多信息，请参阅 DNS 防火墙中的规则设置。

Action

您希望 DNS Firewall 如何处理域名与规则域列表中的规范匹配的 DNS 查询。有关更多信息，请参阅 the section called “DNS Firewall 中的规则操作”。

优先级

用于确定处理顺序的 DNS 视图中规则的唯一正整数设置。DNS Firewall 根据 DNS 视图中的规则检查 DNS 查询，从最低的数字优先级设置开始，然后向上移动。您可以随时更改规则的优先级，例如更改处理顺序或为其它规则留出空间。

DNS Firewall 中的规则操作

当 DNS Firewall 在规则中找到 DNS 查询与域规范之间的匹配时，它会将规则中指定的操作应用于查询。

您需要在创建的每条规则中指定下列选项之一：

- 允许-停止检查查询并允许其通过。不适用于 DNS Firewall Advanced。
- 警报 — 停止检查查询，允许其通过，并在 Route 53 Resolver 日志中记录查询警报。
- 阻止 — 停止检查查询，阻止其前往其预期目的地，并将该查询的阻止操作记录在 Route 53 Resolver 日志中。

  回复已配置的阻止响应，具体如下：
  - NODAT A — 响应表示查询成功，但没有可用的响应。
  - NXDOMAI N — 响应表示查询的域名不存在。
  - 覆盖-在响应中提供自定义覆盖。此选项需要以下额外设置：
    - 记录值-为响应查询而发送回的自定义 DNS 记录。
    - 记录类型-DNS 记录的类型。这决定了记录值的格式。必须是 CNAME。
    - 存@@ 活时间（以秒为单位）— DNS 解析器或 Web 浏览器缓存覆盖记录并使用它来响应此查询的建议时间（如果再次收到该查询）。预设情况下，此值为零，并且记录不会被缓存。

Route 53 全球解析器的托管域列表

托管域列表包含与恶意活动或其他潜在威胁相关的域名。 Amazon 维护这些列表是为了让 Route 53 Global Resolver 客户在使用 DNS 防火墙时能够针对他们检查互联网绑定的 DNS 查询。

随时了解不断变化的威胁情形会非常耗时且成本高昂。在全局解析器上实施和使用 DNS 防火墙时，托管域列表可以为您节省时间。 Amazon 当出现新的漏洞和威胁时，会自动更新列表。

托管域列表分为威胁和内容类别，旨在帮助保护您免受常见网络威胁的侵害，还可以阻止对非域名的查询解析 safe-for-work。

最佳实践是在生产环境中使用托管域列表之前，请在非生产环境中对其进行测试，并将规则操作设置为 `Alert`。使用 Amazon CloudWatch 指标和 DNS 防火墙采样请求或全球解析器日志来评估规则。如果您对规则执行操作的情况感到满意，请根据需要更改操作设置。

可用的 Amazon 托管域名列表

本节介绍全球解析器当前可用的托管域名列表。 Amazon 为 Global Resolver 的所有用户提供以下按威胁或内容类型分类的托管域列表。

威胁类别

恶意软件
僵尸网络/命令与控制
聚合威胁列表
Amazon GuardDuty 威胁清单
网络钓鱼
垃圾电子邮件

内容类别

暴力和仇恨言论
适合孩子
在线广告
科学
家庭与育儿

Pets
求职和求职
宗教
Lifestyle
家居与花园
犯罪和非法活动
体育和娱乐
车辆
金融服务
房地产
爱好和兴趣
出行中
食物和餐饮
政府和法律
教育
时尚
健康
购物
成人和成人内容
科技与互联网
商业与经济

新闻

搜索引擎和门户

艺术与文化

娱乐

军事

社交网络

避开代理

重定向

电子邮件

翻译

虐待儿童

堕胎

赌博

黑客攻击

大麻

Cryptocurrency

约会

人工智能和 Machine Learning

停放的域名

私有 IP 地址

无法下载或浏览托管域列表。为了保护知识产权，您无法查看或编辑托管域列表中的各个域名规范。此限制还有助于避免恶意用户设计专门避开已发布列表的威胁。

建立要屏蔽或允许的域名列表

您可以创建自己的域列表，以指定托管域列表产品中没有找到或您希望自行处理的域类别。

除了本节所述的步骤外，在创建或更新规则时，您还可以在控制台中在 DNS 防火墙规则管理环境中创建域列表。

域列表中的每个域规范必须满足以下要求：

- 它可以选择从 *（星号）开始。
- 除了可选的起始星号和句点（作为标签之间）的分隔符之外，它必须只包含以下字符：A-Z、a-z、0-9、-（连字符）。
- 它的长度必须介于 1 到 255 个字符之间。

创建域名列表

1. 在 Route 53 全球解析器控制台中，导航到您的全球解析器。
2. 选择 “域名列表” 选项卡。
3. 选择创建域名列表。
4. 为您的域名列表提供名称和可选描述以及任何标签，然后选择创建域名列表。
5. 创建域名并投入运行后，您可以通过选择添加域名开始向域名列表中添加域名。
6. 如果您选择从 Amazon S3 存储桶上传域名列表，请输入您在其中创建域列表的 Amazon S3 存储桶的 URI。此域列表每行应有一个域名。
7. 否则，请在文本框中输入您的域名规范，每行一个。
8. 选择添加域名。

删除域名列表

1. 在 Route 53 全球解析器控制台中，导航到您的全球解析器。
2. 选择 “域名列表” 选项卡。
3. 选择要删除的域列表，然后选择 Delete（删除），并确认删除。

DNS 防火墙高级保护

DNS Firewall Advanced 根据 DNS 查询中的已知威胁签名检测可疑 DNS 查询。您可以在与 DNS 视图关联的 DNS 防火墙规则中使用的规则中指定威胁类型。

DNS Firewall Advanced 的工作原理是通过检查 DNS 有效载荷中的一系列关键标识符来识别可疑的 DNS 威胁特征，包括请求的时间戳、请求和响应的频率、DNS 查询字符串以及出站和入站 DNS 查询的长度、类型或大小。根据威胁签名的类型，您可以配置要阻止的策略，或者直接对查询进行记录和提醒。通过使用一组扩展的威胁标识符，您可以防范来自域来源的 DNS 威胁，这些域来源可能尚未被更广泛的安全社区维护的威胁情报源分类。

目前，DNS Firewall Advanced 提供以下保护：

- 域生成算法 (DGAs)

  DGAs 被攻击者用来生成大量域来发起恶意软件攻击。
- DNS 隧道

  DNS 隧道技术是指攻击者利用 DNS 隧道从客户端窃取数据，而无需与客户端建立网络连接。

要了解如何创建规则，请参阅the section called “配置和管理 DNS 防火墙规则”。

减少误报情况

如果您在使用 DNS Firewall Advanced 保护阻止查询的规则中遇到误报情况，请执行以下步骤：

1. 在全局解析器日志中，确定导致误报的规则和 DNS 防火墙高级保护。您可以通过查找 DNS Firewall 阻止但您希望允许通过的查询日志来执行此操作。日志记录列出了 DNS 视图、规则、规则操作和 DNS 防火墙高级保护。
2. 在 DNS 视图中创建一条新规则，明确允许被屏蔽的查询通过。创建规则时，您可以使用您希望允许的域规范定义自己的域列表。请遵循规则管理指南，网址为the section called “配置和管理 DNS 防火墙规则”。
3. 在规则中优先考虑新规则，使其在使用托管列表的规则之前运行。若要执行此操作，请为新规则提供较低的数字优先级设置。

更新规则后，新规则将在屏蔽规则运行之前明确允许您想要允许的域名。

在 Route 53 全球解析器中管理 DNS 安全策略

管理全局解析器

创建全局解析器后，您可以从 “全局解析器” 页面查看其详细信息、编辑其配置和管理相关资源。

查看解析器详情

Global Resolvers 页面显示所有解析器的列表，其中包含关键信息，包括解析器名称、部署区域、关联的 DNS 视图、可观察性区域和操作状态。

编辑全局解析器

创建解析器后，您可以修改解析器的名称和描述。创建全球解析器后，您无法修改部署的区域。

管理防火墙规则

创建防火墙规则后，您可以根据需要修改其优先级、更新其配置或将其删除。

规则优先级和评估顺序

防火墙规则按优先级顺序进行评估，优先处理较低的数字。当一个查询匹配多个规则时，仅应用第一个匹配规则的操作。

更新防火墙规则

创建防火墙规则后，您可以更新防火墙规则的大部分内容，包括其优先级、操作和目标域。

使用 Route 53 全球解析器配置私有托管区域关联

Route 53 Global Resolver 允许您从授权客户端解析与 Route 53 私有托管区域相关的记录。您可以将 Route 53 私有托管区域与允许获得 DNS 视图授权的客户端解析的 DNS 视图相关联。

主题

- 使用 Route 53 全球解析器管理私有托管区域关联

使用 Route 53 全球解析器管理私有托管区域关联

为内部应用程序创建私有托管区域

在将私有托管区域与 DNS 视图关联之前，必须先使用 Amazon Route 53 控制台或 API 创建该区域。

创建私有托管区域

1. 打开 Amazon Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择创建托管区域。
4. 在 “域名” 中，输入您的私有区域的域名（例如，`internal.example.com`）。
5. 对于 Type（类型），选择 Private hosted zone（私有托管区域）。
6. VPCs 要与托管区域关联，请选择 VPCs 要与托管区域关联的。或者，您可以使用 `CreateHostedZone` API 操作跳过输入值，因为您将改为将该区域与 Route 53 全球解析器相关联。
7. 选择创建托管区域。

创建私有托管区域后，添加内部服务所需的 DNS 记录。

将私有托管区域与 DNS 视图相关联

要使 Route 53 全球解析器能够解析私有托管区域的查询，您必须将该区域与一个或多个 DNS 视图相关联。

将私有托管区域与 DNS 视图相关联

1. 在 Route 53 全球解析器控制台中，导航到您的全局解析器。
2. 选择要关联私有托管区域的 DNS 视图。
3. 在私有托管区域部分，选择关联托管区域。
4. 对于托管区域，选择要关联的私有托管区域。
5. 在协会名称中，输入该关联的描述性名称。
6. 选择关联托管区域。

关联过程通常需要几分钟才能完成。完成后，Route 53 Global Resolver 将使用私有托管区域中的记录来回答来自与 DNS 视图关联的客户端设备的 DNS 查询。

使用 Route 53 全球解析器监控 DNS 活动和性能

Route 53 Global Resolver 可全面了解组织内的 DNS 活动，使您能够识别安全威胁、分析客户端设备行为并保持合规性。本章介绍可用的监控工具，以及设置 DNS 监控、配置日志记录目标以及分析 DNS 数据以调查威胁和优化性能的详细过程。

Amazon 提供以下监控工具来帮助您维护安全、可靠的 DNS 服务：

- Amazon 实时 CloudWatch跟踪 DNS 查询量、响应时间和安全事件。创建仪表板以监控各个位置的 DNS 性能，并设置警报，以便在查询量激增或响应时间增加时通知您。对于 Route 53 Global Resolver，您可以监控查询量、响应时间和筛选活动。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon Lo CloudWatch gs 使您能够监控、存储和访问来自亚马逊 EC2 实例和其他来源的日志文件。 CloudTrailRoute 53 Global Resolver 可以将 DNS 查询日志直接传送到 CloudWatch 日志，以进行实时监控和分析。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- Amazon EventBridge 可用于实现 Amazon 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 Amazon 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- Amazon CloudTrail捕获由您的账户或代表您的 Amazon 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 Amazon、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 Amazon CloudTrail 《用户指南》。

主题

使用 Route 53 全球解析器了解 DNS 活动

Route 53 Global Resolver 提供全面的 DNS 查询记录功能，用于监控客户端设备活动并识别安全威胁。在 Route 53 Global Resolver 中启用 DNS 查询日志，以查看客户端设备访问了哪些网站，识别潜在的安全威胁并分析 DNS 解析模式。日志会捕获有关每个查询的全面信息，包括应用了哪些安全策略。

DNS 日志中捕获了哪些信息

每个 DNS 查询日志条目都提供有关客户端设备活动和安全策略实施的详细信息：

- 查询信息-使用的域名、查询类型、查询类别和协议
- 客户端设备信息-源 IP 地址、DNS 视图和身份验证方法
- 响应信息-响应码、答案记录和响应时间

- 安全操作-防火墙规则匹配项、威胁检测结果和采取的措施
- 元数据-时间戳、全球解析器 ID、区域和跟踪信息

用于安全集成的 OCSF 格式

DNS 查询日志使用开放网络安全架构框架 (OCSF)，该框架为安全事件数据提供了标准化格式。这种格式允许：

- 标准化分析-跨不同安全工具的架构一致
- 提高了互操作性-可轻松与 SIEM 和分析平台集成
- 增强关联性-能够将 DNS 事件与其他安全数据关联
- 未来兼容性-Support 支持不断变化的安全分析需求

OCSF 日志格式示例

Route 53 Global Resolver DNS 查询日志遵循 OCSF 架构结构，提供有关每个 DNS 查询、响应和安全操作的详细信息。以下示例显示了允许和拒绝的查询的日志格式。

Route 53 全球解析器 DNS 日志——允许访问示例

此示例显示了允许通过防火墙规则进行的 DNS 查询。该日志包括查询详情、响应信息以及带有 Route 53 全球解析器专用标识符的丰富数据。


```
{
    "action_id": 1,
    "action_name": "Allowed",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-east-1",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
```

```
        "direction": "Inbound",
        "direction_id": 1,
        "protocol_name": "udp",
        "protocol_num": 17,
        "protocol_ver": "",
        "uid": "db21d1739ddb423a"
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [{
        "rdata": "3.3.3.3",
        "type": "A",
        "class": "IN",
        "ttl": 300
    },
    {
        "rdata": "3.3.3.4",
        "type": "A",
        "class": "IN",
        "ttl": 300
    }],
    "src_endpoint": {
        "ip": "3.3.3.1",
        "port": 56576
    },
    "enrichments": [{
        "name": "global-resolver",
        "value": "gr-a1b2c3d4fexample",
        "data": {
            "dns_view_id": "dnsv-a1b2c3d4fexample",
            "firewall_rule_id": "fr-a1b2c3d4fexample",
            "token_id": "t-a1b2c3d4fexample",
            "token_name": "device-123456",
            "token_expiration": "1789419206",
        }
    }],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
```

```
            }
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "NOERROR",
    "rcode_id": 0,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "start_time": 1761358379995,
    "status": "Success",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```

Route 53 全球解析器 DNS 日志——访问被拒绝示例

此示例显示了被防火墙规则阻止的 DNS 查询。该日志包括拒绝操作、空答案数组和表示查询未处理的拒绝响应代码。

```
{
    "action_id": 2,
    "action_name": "Denied",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
```

```
        "provider": "AWS",
        "region": "us-west-2",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
        "direction": "Inbound",
        "direction_id": 1,
        "protocol_name": "tcp",
        "protocol_num": 6,
        "protocol_ver_id": 4,
        "uid": "9fdc6fbc09794d5e"
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [],
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "enrichments": [
        {
            "name": "global-resolver",
            "value": "gr-a1b2c3d4fexample",
            "data": {
                "dns_view_id": "dnsv-a1b2c3d4fexample",
                "firewall_rule_id": "fr-a1b2c3d4fexample",
                "token_id": "t-a1b2c3d4fexample",
                "token_name": "device-123456",
                "token_expiration": "1789419206",
            }
        }
    ],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
            }
        }
```

```
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "REFUSED",
    "rcode_id": 5,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "start_time": 1761358379995,
    "status": "Failure",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```

使用 Route 53 全局解析器配置 DNS 监控和日志记录

在 Route 53 全局解析器中配置 DNS 监控，以捕获有关 DNS 查询、响应和安全操作的详细信息。本节介绍设置日志记录目标和配置监控工具的步骤。

设置可观测性区域

在配置 DNS 日志记录之前，您必须设置一个用于存储日志和指标的可观测区域。该区域决定了您的监控数据的处理和存储位置。

1. 打开 Route 53 全球解析器控制台，网址为https://console.aws.amazon.com/route53globalresolver/。
2. 在导航窗格中，选择设置。
3. 在可观测性区域部分中，选择设置区域。
4. 选择要存储监控数据的 Amazon 区域，然后选择设置区域。

设置可观察性区域后，您可以在该区域配置日志传输目标。

使用 Route 53 全球解析器解决 DNS 问题

Route 53 Global Resolver 提供全面的 DNS 解析功能，但有时您可能需要对连接、性能或配置问题进行故障排除。使用 DNS 日志、监控数据和诊断技术，通过 Route 53 全球解析器识别和解决影响客户端设备 DNS 解析的问题。本章提供了解决常见 DNS 问题和优化性能的系统方法。

主题

使用 Route 53 全球解析器诊断 DNS 连接问题

Route 53 Global Resolver 提供可靠的 DNS 解析，但由于配置、身份验证或网络问题，偶尔会出现连接问题。当客户端设备无法使用 Route 53 全球解析器解析域名时，请使用这些系统的方法来识别和解决连接问题。

客户端设备无法解析域

请按照以下步骤诊断解析故障：

1. 验证查询是否到达全局解析器
   - 查看 DNS 查询日志，了解来自受影响客户端设备 IP 地址的查询
   - 确认客户端设备配置了正确的任播 IP 地址
   - 测试从客户端设备到 anycast 的网络连接 IPs
2. 检查客户端设备身份验证
   - 验证客户端设备是否已通过身份验证以获得正确的 DNS 视图
   - 查看客户端设备的 IP 地址或 CIDR 块的访问源规则
   - 确认访问令牌有效且未过期（用于基于令牌的身份验证）
3. 查看防火墙规则
   - 检查防火墙规则是否阻止了查询
   - 查看规则优先级并确保允许规则的优先级高于屏蔽规则
   - 验证防火墙失效打开行为设置

4. 确认 DNS 视图关联

- 验证内部域的私有托管区域关联
- 检查关联的私有托管区域中是否存在 DNS 记录
- 确保查询中的域名与区域名称完全匹配

间歇性解析失败

对于零星的 DNS 解析问题，请调查以下潜在原因：

身份验证问题

- 检查访问令牌的到期时间和续订模式
- 查看身份验证日志，查看失败的身份验证尝试
- 验证客户端设备的时钟同步以进行令牌验证

网络连接

- 监控网络路径变化或路由问题
- 检查防火墙或 NAT 设备配置是否有更改
- 验证到最近区域的任播路由是否一致

服务运行状况

- 在 S Amazon ervice Health Dashboard 中查看 Route 53 全球解决程序问题
- 查看错误率峰值的 CloudWatch 指标
- 监控私有托管区域关联状态

意想不到的公开决议

当查询解析到公有 DNS 而不是私有托管区域时：

1. 验证私有托管区域配置

- 确认私有托管区域包含预期的 DNS 记录
- 检查记录名称是否与查询的域名完全匹配
- 验证记录类型是否与查询类型（A、AAAA、CNAME 等）相匹配

2. 检查 DNS 视图关联

- 验证私有托管区域是否与正确的 DNS 视图相关联

- 确认客户端设备已通过 DNS 视图的身份验证
- 在控制台中查看关联状态

3. 查看防火墙规则
   - 检查是否存在可能阻止私有区域查询的防火墙规则
   - 验证规则评估顺序和优先级
   - 查看 DNS 查询日志以了解防火墙操作

使用 Route 53 全球解析器解决 DNS 性能问题

Route 53 Global Resolver 旨在通过全局任播架构实现最佳性能，但各种因素都会影响 DNS 解析速度。使用 Route 53 全球解析器解决 DNS 解析速度缓慢的问题，优化查询响应时间，以提高客户端设备性能。

DNS 解析速度慢

要诊断和解决 DNS 响应时间慢的问题，请执行以下操作：

1. 分析查询响应时间
   - 使用 DNS 查询日志来识别响应时间较长的查询
   - 比较不同域名和查询类型的响应时间
   - 监控一段时间内的响应时间趋势
2. 检查查询量是否很高
   - 监控查询 CloudWatch 量峰值的指标
   - 识别生成过多查询的客户端设备或 DNS 视图
   - 寻找可能表明配置错误的查询模式
3. 查看缓存性能
   - 分析经常查询的域名的缓存命中率
   - 查看 DNS 记录的 TTL 设置
   - 考虑根据查询模式调整 TTL 值
4. 验证最佳区域选择
   - 确保全球解析器区域靠近客户端设备位置
   - 监控任播路由，以确认查询到达最近的区域
   - 如果客户端设备的地理位置较远，可以考虑添加区域

性能优化策略

使用以下策略优化 DNS 性能：

缓存优化

- 根据查询模式和更改频率调整 TTL 值
- TTLs 对于稳定的记录，使用更长的时间， TTLs 对于经常变化的记录，使用较短的时间
- 监控缓存命中率并进行 TTLs 相应调整

区域优化

- 在最接近客户端设备集中的区域部署全局解析器
- 按地区监控查询路由模式和响应时间
- 考虑添加区域以获得更好的地理覆盖范围

协议优化

- 根据安全和性能要求选择适当的 DNS 协议
- 考虑 DNS-over-HTTPS (DoH) 使用具有缓存优势的加密连接
- 使用 DNS-over-TLS (DoT) 进行开销较低的加密连接

规则优化

- 审查和优化防火墙规则的优先级和复杂性
- 将经常匹配的规则按优先级顺序排列得更高
- 尽可能简化复杂的规则条件

对 Route 53 全局解析器中的配置问题进行故障排除

Route 53 Global Resolver 为 DNS 视图、身份验证和防火墙规则提供了广泛的配置选项，这有时会导致配置冲突或不匹配。识别并解决影响 DNS 解析的常见 Route 53 全局解析器配置问题。

身份验证问题

常见的身份验证问题和解决方案：

访问源规则不匹配

- 验证客户端设备的 IP 地址与配置的 CIDR 块相匹配
- 检查更改源 IP 地址的 NAT 或代理设备
- 确保访问源规则涵盖所有预期的客户端设备 IP 范围

令牌身份验证失败

- 验证客户端设备上的令牌配置是否正确
- 查看代币到期日期和续订流程
- 确保客户端设备时钟同步以进行令牌验证

协议不匹配

- 验证客户端设备是否使用访问源规则允许的协议
- 检查 DoH 和 DoT 的配置是否与令牌协议匹配
- 确保防火墙规则不会阻止所需的协议

DNS 视图配置问题

常见的 DNS 视图配置问题：

DNS 视图关联不正确

- 验证客户端设备是否已通过身份验证到预期的 DNS 视图
- 检查私有托管区域是否与正确的 DNS 视图相关联
- 查看应用于每个 DNS 视图的防火墙规则

DNS 设置冲突

- 查看 DNSSEC 验证设置是否与客户端设备兼容
- 检查 EDNS 客户端子网设置，确保隐私和性能平衡
- 验证防火墙失效打开行为是否符合安全要求

防火墙规则问题

常见的防火墙规则配置问题：

规则优先级冲突

- 查看规则评估顺序并确保优先级分配正确
- 检查是否存在优先级高于预期允许规则的屏蔽规则
- 在生产部署之前，在受控环境中测试规则更改

域名列表不匹配

- 验证自定义域名列表中的域名规范

- 检查通配符模式的语法和覆盖范围是否正确
- 确保域名列表已更新和同步

内部资源访问疑难解答

管理内部资源访问时的常见问题和解决方案：

客户端设备无法解析到私有区域记录

- 验证私有托管区域是否与正确的 DNS 视图相关联
- 检查客户端设备是否已通过身份验证以获得正确的 DNS 视图
- 确保查询中的域名与区域名称完全匹配
- 验证私有托管区域中是否存在 DNS 记录

间歇性解析失败

- 在控制台中检查关联状态
- 查看 DNS 查询日志以了解错误模式
- 验证 Route 53 全球解析器与亚马逊 Route 53 之间的网络连接

意想不到的公开决议

- 确认私有托管区域包含预期记录
- 检查可能阻止查询的防火墙规则
- 验证查询来自与 DNS 视图关联的客户端设备

Route 53 全球解析器的配额

您的 Amazon 账户对每项 Amazon 服务都有默认配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Route 53 全球解析器的配额，请打开 Serv ice Quotas 控制台。在导航窗格中，选择Amazon 服务，然后选择 Route 53 Global Resolver。

要请求提高配额，请参阅《Service Quotas 用户指南》中的请求提高配额。如果限额在服务限额中尚不可用，请使用提高限制表格。

您的 Amazon 账户具有以下与 Route 53 全球解析器相关的配额。

软限额

下表描述了 Route 53 Global Resolver 中可以增加的配额。有关更改配额的信息，请参阅 Servic e Quotas 用户指南中的请求增加配额。

对于某些客户，您的账户配额可能低于这些发布的配额。如果您认为自己不应该遇到 Resource limit exceeded (超出资源限制) 错误，请使用 Service Quotas 控制台请求增加配额。

资源	默认配额	可调整
每个账户的全球解析人员	2	可以
每个全局解析器的 DNS 浏览量	5	是
每个账户的 DNS 浏览量	50	可以
每个账户的域列表	1000	是
每个域名列表中的域名	100000	是
文件中从 S3 导入的域	10000	是
所有防火墙规则中的域数量	1000000	是
每个 DNS 视图的防火墙规则	100	是
每个全局解析器的访问令牌	5000	是
每个全局解析器访问源	1000	是
每个全局解析器的访问源 CIDR 大小	65000	否
每个 DNS 视图的私有托管区域	1000	是

硬限额

下表描述了 Route 53 Global Resolver 中无法增加的配额。

资源或操作	配额
每个（全球解析器、目标类型、区域）的日志传输配置	1

使用创建 Amazon Route 53 和 Route 53 VPC 解析器资源 Amazon CloudFormation

Amazon Route 53 和 Route 53 VPC Resolver 与 Amazon CloudFormation一项服务集成，该服务可帮助您对 Amazon 资源进行建模和设置，从而减少创建和管理资源和基础设施所花费的时间。您可以创建一个描述所需所有 Amazon 资源的模板，并为您预 Amazon CloudFormation 置和配置这些资源。

使用时 Amazon CloudFormation，您可以重复使用您的模板来一致且重复地设置 Route 53 和 VPC 解析器资源。只需描述一次您的资源，然后在多个 Amazon Web Services 账户 区域中一遍又一遍地配置相同的资源。

Route 53、VPC 解析器和模板 Amazon CloudFormation

要为 Route 53、VPC 解析器和相关服务配置和配置资源，您必须了解Amazon CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 Amazon CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D Amazon CloudFormation esigner 来帮助你开始使用 Amazon CloudFormation 模板。有关更多信息，请参阅什么是 Amazon CloudFormation 设计器？ 在《Amazon CloudFormation 用户指南》中。

Route 53 支持在中创建以下资源类型 Amazon CloudFormation：

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

有关更多信息（包括 Route 53 资源的 JSON 和 YAML 模板示例），请参阅 Amazon CloudFormation 用户指南中的 Amazon Route 53 资源类型参考。

VPC 解析器支持在中 Amazon CloudFormation创建以下资源类型：

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallDomainList`

- AWS::Route53Resolver::FirewallRuleGroupAssociation
- AWS::Route53Resolver::ResolverDNSSECConfig
- AWS::Route53Resolver::ResolverEndpoint
- AWS::Route53Resolver::ResolverQueryLoggingConfig
- AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation
- AWS::Route53Resolver::ResolverRule
- AWS::Route53Resolver::ResolverRuleAssociation

有关更多信息，包括 VPC 解析器资源的 JSON 和 YAML 模板示例，请参阅用户指南中的 R oute 53 VPC 解析器资源类型参考。Amazon CloudFormation

Route 53 和 Amazon CloudFormation的最佳实践

使用 Amazon CloudFormation 管理 Route 53 资源时，请遵循以下最佳实践，以避免常见问题并确保部署可靠。

了解最终一致性

Route 53 使用最终一致的模型进行 DNS 更改。这可能会影响 Amazon CloudFormation 操作，尤其是在回滚和快速连续更改期间。

> **Important**
>
> Amazon CloudFormation 尝试回滚 DNS 记录更改时，由于 Route 53 的最终一致性模型，回滚可能会失败。如果 Amazon CloudFormation 尝试重新创建最近删除但由于最终一致性而似乎仍然存在的记录，则可能会遇到InvalidChangeBatch错误，使您的 DNS 处于损坏状态。

为最大限度地减少与最终一致性有关的问题：

- 谨慎计划更改 - 避免对相同的 DNS 记录进行快速连续更改
- 首先在非生产环境中测试 - 在将其应用于生产环境之前，请务必在开发环境中测试 DNS 更改
- 监控部署-在 DNS 相关部署期间密切关注 Amazon CloudFormation 堆栈事件。有关监控指南，请参阅 监控 Amazon Route 53。
- 妥善准备回滚程序 - 准备手动恢复程序，以防自动回滚失败

DNS 记录的顺序和逻辑 IDs

在中创建多个 DNS 记录时 Amazon CloudFormation，请注意记录排序和逻辑 ID 分配。

> **Warning**
>
> 如果您在 Amazon CloudFormation 模板中的数组或列表中定义 DNS 记录，则在列表中间插入新记录可能会导致 Amazon CloudFormation 将逻辑重新分配 IDs 给现有记录。这会触发记录替换，从而导致服务中断和回滚失败。

DNS 记录管理的最佳实践：

- 使用显式逻辑 IDs-始终为 DNS 记录分配显式、有意义的逻辑 IDs ，而不是依赖数组索引。有关 Amazon CloudFormation 逻辑的更多信息 IDs，请参阅《Amazon CloudFormation 用户指南》中的“资源” 部分结构
- 附加新记录 - 向现有列表添加新的 DNS 记录时，请将其附加到列表末尾，而不是将其插入列表中间
- 分组相关记录 - 考虑使用 `AWS::Route53::RecordSetGroup` 将相关记录放在一起进行管理。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的AWS::Route53::RecordSet群组。
- 审核更改集 - 请务必在部署之前审核 Amazon CloudFormation 更改集，以识别意外的记录替换。有关更多信息，请参阅 Amazon CloudFormation 用户指南中的使用更改集更新堆栈。

处理回滚失败

如果由于 DNS 相关问题导致 Amazon CloudFormation 回滚失败，则可能需要执行手动恢复。

从失败的 DNS 回滚中执行手动恢复

1. 通过查看 Amazon CloudFormation 堆栈事件和 Route 53 托管区域记录来识别失败的 DNS 记录
2. 通过 Route 53 控制台或 API 手动创建或更新缺少的 CLI 记录。有关创建记录的信息，请参阅 使用记录。
3. 恢复 DNS 后，更新您的 Amazon CloudFormation 模板以匹配当前状态
4. 部署更正后的模板以 Amazon CloudFormation 恢复与实际资源的同步

要防止回滚失败：

- 避免在高流量期间进行可能触发 DNS 记录替换的更改

- 实施运行状况检查和监控以快速检测 DNS 问题。有关运行状况检查的信息，请参阅 创建和更新运行状况检查。
- 考虑对关键 DNS 更改使用蓝绿部署策略。有关部署最佳实践的更多信息，请参阅 Amazon Route 53 的最佳实践。
- 记录手动 DNS 恢复的紧急程序

了解更多关于 Amazon CloudFormation

要了解更多信息 Amazon CloudFormation，请参阅以下资源：

- Amazon CloudFormation
- Amazon CloudFormation 用户指南
- Amazon CloudFormation API 引用
- Amazon CloudFormation 命令行界面用户指南

使用 Amazon SDK 的 Route 53 代码示例

以下代码示例显示如何将 Route 53 与 Amazon 软件开发工具包（SDK）一起使用。

有关 Amazon SDK 开发人员指南和代码示例的完整列表，请参阅 将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- 使用 Route 53 的代码示例 Amazon SDKs
  - 使用 Route 53 的基本示例 Amazon SDKs
    - 使用 Route 53 执行的操作 Amazon SDKs
      - 将 ChangeResourceRecordSets 与 CLI 配合使用
      - 将 CreateHostedZone 与 CLI 配合使用
      - 将 DeleteHostedZone 与 CLI 配合使用
      - 将 GetHostedZone 与 CLI 配合使用
      - ListHostedZones与 Amazon SDK 或 CLI 配合使用
      - 将 ListHostedZonesByName 与 CLI 配合使用
      - 将 ListQueryLoggingConfigs 与 CLI 配合使用
- 使用 Route 53 注册域名的代码示例 Amazon SDKs
  - 使用 Route 53 注册域名的基本示例 Amazon SDKs
    - 开始使用 Route 53 域注册
    - 学习使用 Amazon SDK 注册 Route 53 域名的基础知识
    - 使用 Route 53 注册域名的操作 Amazon SDKs
      - CheckDomainAvailability与 Amazon SDK 或 CLI 配合使用
      - CheckDomainTransferability与 Amazon SDK 或 CLI 配合使用
      - GetDomainDetail与 Amazon SDK 或 CLI 配合使用
      - GetDomainSuggestions与 Amazon SDK 或 CLI 配合使用
      - GetOperationDetail与 Amazon SDK 或 CLI 配合使用
      - ListDomains与 Amazon SDK 或 CLI 配合使用
      - ListOperations与 Amazon SDK 或 CLI 配合使用
      - 与 Amazon SDK ListPrices 配合使用
      - RegisterDomain与 Amazon SDK 或 CLI 配合使用

- ViewBilling与 Amazon SDK 或 CLI 配合使用

使用 Route 53 的代码示例 Amazon SDKs

以下代码示例展示了如何将 Route 53 与 Amazon 软件开发套件 (SDK) 一起使用。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景的上下文查看操作。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- 使用 Route 53 的基本示例 Amazon SDKs
  - 使用 Route 53 执行的操作 Amazon SDKs
    - 将 ChangeResourceRecordSets 与 CLI 配合使用
    - 将 CreateHostedZone 与 CLI 配合使用
    - 将 DeleteHostedZone 与 CLI 配合使用
    - 将 GetHostedZone 与 CLI 配合使用
    - ListHostedZones与 Amazon SDK 或 CLI 配合使用
    - 将 ListHostedZonesByName 与 CLI 配合使用
    - 将 ListQueryLoggingConfigs 与 CLI 配合使用

使用 Route 53 的基本示例 Amazon SDKs

以下代码示例展示了如何使用 Amazon Route 53 的基础知识 Amazon SDKs。

示例

- 使用 Route 53 执行的操作 Amazon SDKs
  - 将 ChangeResourceRecordSets 与 CLI 配合使用
  - 将 CreateHostedZone 与 CLI 配合使用
  - 将 DeleteHostedZone 与 CLI 配合使用
  - 将 GetHostedZone 与 CLI 配合使用
  - ListHostedZones与 Amazon SDK 或 CLI 配合使用

- 将 ListHostedZonesByName 与 CLI 配合使用
- 将 ListQueryLoggingConfigs 与 CLI 配合使用

使用 Route 53 执行的操作 Amazon SDKs

以下代码示例演示了如何使用执行各个 Route 53 操作 Amazon SDKs。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 Amazon Route 53 API 参考。

示例

- 将 ChangeResourceRecordSets 与 CLI 配合使用
- 将 CreateHostedZone 与 CLI 配合使用
- 将 DeleteHostedZone 与 CLI 配合使用
- 将 GetHostedZone 与 CLI 配合使用
- ListHostedZones与 Amazon SDK 或 CLI 配合使用
- 将 ListHostedZonesByName 与 CLI 配合使用
- 将 ListQueryLoggingConfigs 与 CLI 配合使用

将 **ChangeResourceRecordSets** 与 CLI 配合使用

以下代码示例演示如何使用 ChangeResourceRecordSets。

CLI

Amazon CLI

创建、更新或删除资源记录集

以下 change-resource-record-sets 命令使用 hosted-zone-id Z1R8UBAEXAMPLE 以及 C:\awscli\route53\change-resource-record-sets.json 文件中的 JSON 格式配置创建资源记录集：

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

有关更多信息，请参阅《亚马逊 Route 53 API 参考》 ChangeResourceRecordSets 中的 POST。

JSON 文件中的配置取决于要创建的资源记录集的类型：

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover 别名

基本语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

加权语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
```

```
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

别名语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

加权别名语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
```

```
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

延迟语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
```

```
    {...}
  ]
}
```

延迟别名语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

失效转移语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
```

```
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

失效转移别名语法：

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[ChangeResourceRecordSets](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例为 www.example.com 创建 A 记录，并将 test.example.com 的 A 记录从 192.0.2.3 更改为 192.0.2.1。请注意，TXT 类型记录的更改值必须采用双引号。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}
```

```
Edit-R53ResourceRecordSet @params
```

示例 2：此示例说明如何创建别名资源记录集。'Z222222222'是您要在其中创建别名资源记录集的 Amazon Route 53 托管区的 ID。'example.com' 是您要为其创建别名的 Zone Apex（机构根网域），而 'www.example.com' 是您也想为其创建别名的子域。'Z1111111111111'是负载均衡器的托管区域ID的示例，'-1111111111.us-east example-load-balancer -1.elb.amazonaws.com'是负载均衡器域名的示例，亚马逊53号路由使用该域名回应example.com和www.example.com的查询。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}
```

```
Edit-R53ResourceRecordSet @params
```

示例 3：此示例为 www.example.com 创建了两条 A 记录。在四分之一的时间 (1/(1+3))，Amazon Route 53 使用第一个资源记录集的两个值（192.0.2.9 和 192.0.2.10）来响应 www.example.com 的查询。在四分之三的时间 (3/(1+3))，Amazon Route 53 使用第二个资源记录集的两个值（192.0.2.11 和 192.0.2.12）来响应 www.example.com 的查询。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

示例 4：此示例说明如何创建加权别名资源记录集，假设 example.com 是要为其创建加权别名资源记录集的域。 SetIdentifier 将两个加权别名资源记录集彼此区分开来。此元素

是必需的，因为两个资源记录集的“名称”和“类型”元素具有相同的值。Z1111111111111 和 Z3333333333333 是 ELB 负载均衡器的托管区域的示例，值 IDs 为指定。 DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com 和- example-load-balancer 44444444444.us-east-1.elb.amazonaws.com 是亚马逊 Route 53 回复 example.com 查询的 Elastic Load Balancing 域名的示例。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}
```

```
Edit-R53ResourceRecordSet @params
```

示例 5：此示例创建两个延迟别名资源记录集，一个用于美国西部（俄勒冈州）地区 (us-west-2) 的 ELB 负载均衡器，另一个用于亚太地区（新加坡）(ap-southeast-1) 的负载均衡器。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}
```

```
Edit-R53ResourceRecordSet @params
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) ChangeResourceRecordSets中的。

适用于 PowerShell V5 的工具

示例 1：此示例为 www.example.com 创建 A 记录，并将 test.example.com 的 A 记录从 192.0.2.3 更改为 192.0.2.1。请注意，TXT 类型记录的更改值必须采用双引号。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords = @()
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
```

```
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

示例 2：此示例说明如何创建别名资源记录集。'Z222222222'是您要在其中创建别名资源记录集的 Amazon Route 53 托管区的 ID。'example.com' 是您要为其创建别名的 Zone Apex（机构根网域），而 'www.example.com' 是您也想为其创建别名的子域。'Z1111111111111'是负载均衡器的托管区域ID的示例，'-1111111111.us-east example-load-balancer -1.elb.amazonaws.com'是负载均衡器域名的示例，亚马逊53号路由使用该域名回应example.com和www.example.com的查询。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
```

```
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

示例 3：此示例为 www.example.com 创建了两条 A 记录。在四分之一的时间 (1/(1+3))，Amazon Route 53 使用第一个资源记录集的两个值（192.0.2.9 和 192.0.2.10）来响应 www.example.com 的查询。在四分之三的时间 (3/(1+3))，Amazon Route 53 使用第二个资源记录集的两个值（192.0.2.11 和 192.0.2.12）来响应 www.example.com 的查询。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}
```

```
Edit-R53ResourceRecordSet @params
```

示例 4：此示例说明如何创建加权别名资源记录集，假设 example.com 是要为其创建加权别名资源记录集的域。 SetIdentifier 将两个加权别名资源记录集彼此区分开来。此元素是必需的，因为两个资源记录集的“名称”和“类型”元素具有相同的值。Z1111111111111 和 Z3333333333333 是 ELB 负载均衡器的托管区域的示例，值 IDs 为指定。 DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com 和- example-load-balancer 44444444444.us-east-1.elb.amazonaws.com 是亚马逊 Route 53 回复 example.com 查询的 Elastic Load Balancing 域名的示例。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
```

```
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

示例 5：此示例创建两个延迟别名资源记录，一个用于美国西部（俄勒冈州）地区 (us-west-2) 的 ELB 负载均衡器，另一个用于亚太地区（新加坡）(ap-southeast-1) 的负载均衡器。有关更多详细信息，请参阅 Amazon Route 53 文档。您可以使用 Get-R53Change cmdlet 进行轮询以确定更改何时完成。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
```

```
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) ChangeResourceRecordSets中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **CreateHostedZone** 与 CLI 配合使用

以下代码示例演示如何使用 CreateHostedZone。

CLI

Amazon CLI

创建托管区

以下 create-hosted-zone 命令使用调用方参考 2014-04-01-18:47 添加名为 example.com 的托管区。可选注释中包含一个空格，因此必须用引号括起来：

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的“使用托管区”。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateHostedZone中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：创建名为“example.com”的新托管区，并与可重复使用的委托集相关联。请注意，您必须为 CallerReference 参数提供一个值，这样在必要时需要重试的请求就不会有执行两次操作的风险。由于托管区域是在 VPC 中创建的，因此它自动为私有区域，因此您不应设置-HostedZoneConfig _ PrivateZone 参数。

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) CreateHostedZone中的。

适用于 PowerShell V5 的工具

示例 1：创建名为“example.com”的新托管区，并与可重复使用的委托集相关联。请注意，您必须为 CallerReference 参数提供一个值，这样在必要时需要重试的请求就不会有执行两次操作的风险。由于托管区域是在 VPC 中创建的，因此它自动为私有区域，因此您不应设置-HostedZoneConfig _ PrivateZone 参数。

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) CreateHostedZone中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DeleteHostedZone** 与 CLI 配合使用

以下代码示例演示如何使用 DeleteHostedZone。

CLI

Amazon CLI

删除托管区

以下 delete-hosted-zone 命令将删除 id 为 Z36KTIQEXAMPLE 的托管区：

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DeleteHostedZone中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：删除具有指定 ID 的托管区。在命令继续之前，您将收到进行确认的提示，除非您添加了 -Force 开关参数。

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DeleteHostedZone中的。

适用于 PowerShell V5 的工具

示例 1：删除具有指定 ID 的托管区。在命令继续之前，您将收到进行确认的提示，除非您添加了 -Force 开关参数。

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DeleteHostedZone中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **GetHostedZone** 与 CLI 配合使用

以下代码示例演示如何使用 GetHostedZone。

CLI

Amazon CLI

获取有关托管区的信息

以下 get-hosted-zone 命令获取 id 为 Z1R8UBAEXAMPLE 的托管区的相关信息：

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetHostedZone中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回 ID 为 Z1D633 的托管区域的详细信息PJN98FT9。

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetHostedZone中的。

适用于 PowerShell V5 的工具

示例 1：返回 ID 为 Z1D633 的托管区域的详细信息PJN98FT9。

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetHostedZone中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

ListHostedZones与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 ListHostedZones。

CLI

Amazon CLI

列出与当前 Amazon 账户关联的托管区域

以下`list-hosted-zones`命令列出了与当前 Amazon 账户关联的前 100 个托管区域的摘要信息。：

```
aws route53 list-hosted-zones
```

如果您有超过 100 个托管区，或者想要将它们按小于 100 的数量分组列出，请包含 `--max-items` 参数。例如，要一次列出一个托管区，请使用以下命令：

```
aws route53 list-hosted-zones --max-items 1
```

要查看有关下一个托管区的信息，请从上一个命令的响应中获取 `NextToken` 的值，并将其包含在 `--starting-token` 参数中，例如：

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListHostedZones中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：输出所有公有和私有托管区。

```
Get-R53HostedZoneList
```

示例 2：输出与 ID 为 NZ8 X2CISAMPLE 的可重复使用的委托集关联的所有托管区域

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) ListHostedZones中的。

适用于 PowerShell V5 的工具

示例 1：输出所有公有和私有托管区。

```
Get-R53HostedZoneList
```

示例 2：输出与 ID 为 NZ8 X2CISAMPLE 的可重复使用的委托集关联的所有托管区域

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) ListHostedZones中的。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
 aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!("  ID :   {}", zone_id);
        println!("  Name : {}", zone_name);
        println!();
    }
```

```
    Ok(())
}
```

- 有关 API 的详细信息，请参阅适用ListHostedZones于 Rust 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **ListHostedZonesByName** 与 CLI 配合使用

以下代码示例演示如何使用 ListHostedZonesByName。

CLI

Amazon CLI

以下命令列出最多 100 个按域名排序的托管区：

```
aws route53 list-hosted-zones-by-name
```

输出：

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-2",
          "Config": {
              "Comment": "test2",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z119WBBTVP5WFX",
          "Name": "2.example.com."
      },
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-1",
          "Config": {
              "Comment": "test",
```

```
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "IsTruncated": false,
    "MaxItems": "100"
}
```

以下命令列出按名称排序的托管区，开头为 www.example.com：

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

输出：

```
{
    "HostedZones": [
        {
            "ResourceRecordSetCount": 2,
            "CallerReference": "mwunderl20150527-1",
            "Config": {
                "Comment": "test",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "DNSName": "www.example.com",
    "IsTruncated": false,
    "MaxItems": "100"
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListHostedZonesByName中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：按照域名以 ASCII 顺序返回所有公有和私有托管区。

```
Get-R53HostedZonesByName
```

示例 2：按照域名以 ASCII 顺序返回公有和私有托管区，开头为指定的 DNS 名称。

```
Get-R53HostedZonesByName -DnsName example2.com
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) ListHostedZonesByName中的。

适用于 PowerShell V5 的工具

示例 1：按照域名以 ASCII 顺序返回所有公有和私有托管区。

```
Get-R53HostedZonesByName
```

示例 2：按照域名以 ASCII 顺序返回公有和私有托管区，开头为指定的 DNS 名称。

```
Get-R53HostedZonesByName -DnsName example2.com
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) ListHostedZonesByName中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **ListQueryLoggingConfigs** 与 CLI 配合使用

以下代码示例演示如何使用 ListQueryLoggingConfigs。

CLI

Amazon CLI

列出查询日志记录配置

以下list-query-logging-configs示例列出了有关您 Amazon 账户中托管区域前 100 个查询日志配置的信息Z1OX3WQEXAMPLE。

```
aws route53 list-query-logging-configs \
```

```
    --hosted-zone-id Z1OX3WQEXAMPLE
```

输出：

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的记录 DNS 查询。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListQueryLoggingConfigs中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回与当前 Amazon Web Services 账户关联的 DNS 查询日志记录的所有配置。

```
Get-R53QueryLoggingConfigList
```

输出：

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) ListQueryLoggingConfigs中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回与当前 Amazon Web Services 账户关联的 DNS 查询日志记录的所有配置。

```
Get-R53QueryLoggingConfigList
```

输出：

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) ListQueryLoggingConfigs中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

使用 Route 53 注册域名的代码示例 Amazon SDKs

以下代码示例展示了如何通过 Amazon 软件开发套件 (SDK) 使用 Route 53 域名注册。

基本功能是向您展示如何在服务中执行基本操作的代码示例。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景的上下文查看操作。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- 使用 Route 53 注册域名的基本示例 Amazon SDKs
  - 开始使用 Route 53 域注册

- 学习使用 Amazon SDK 注册 Route 53 域名的基础知识
- 使用 Route 53 注册域名的操作 Amazon SDKs
  - CheckDomainAvailability与 Amazon SDK 或 CLI 配合使用
  - CheckDomainTransferability与 Amazon SDK 或 CLI 配合使用
  - GetDomainDetail与 Amazon SDK 或 CLI 配合使用
  - GetDomainSuggestions与 Amazon SDK 或 CLI 配合使用
  - GetOperationDetail与 Amazon SDK 或 CLI 配合使用
  - ListDomains与 Amazon SDK 或 CLI 配合使用
  - ListOperations与 Amazon SDK 或 CLI 配合使用
  - 与 Amazon SDK ListPrices 配合使用
  - RegisterDomain与 Amazon SDK 或 CLI 配合使用
  - ViewBilling与 Amazon SDK 或 CLI 配合使用

使用 Route 53 注册域名的基本示例 Amazon SDKs

以下代码示例说明如何使用 with 的基础 Amazon Route 53 domain registration 知识 Amazon SDKs。

示例

- 开始使用 Route 53 域注册
- 学习使用 Amazon SDK 注册 Route 53 域名的基础知识
- 使用 Route 53 注册域名的操作 Amazon SDKs
  - CheckDomainAvailability与 Amazon SDK 或 CLI 配合使用
  - CheckDomainTransferability与 Amazon SDK 或 CLI 配合使用
  - GetDomainDetail与 Amazon SDK 或 CLI 配合使用
  - GetDomainSuggestions与 Amazon SDK 或 CLI 配合使用
  - GetOperationDetail与 Amazon SDK 或 CLI 配合使用
  - ListDomains与 Amazon SDK 或 CLI 配合使用
  - ListOperations与 Amazon SDK 或 CLI 配合使用
  - 与 Amazon SDK ListPrices 配合使用
  - RegisterDomain与 Amazon SDK 或 CLI 配合使用
  - ViewBilling与 Amazon SDK 或 CLI 配合使用

开始使用 Route 53 域注册

以下代码示例显示如何开始使用 Route 53 域注册。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
```

```
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ListPrices中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
 *
 */
```

```
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
 String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
 route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
```

```
                        "Registration: " + pr.registrationPrice().price() + " " +
 pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
 + pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
 pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考ListPrices中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.
```

```
 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
```

```
    }
}
```

- 有关 API 的详细信息，请参阅适用ListPrices于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

学习使用 Amazon SDK 注册 Route 53 域名的基础知识

以下代码示例演示了如何：

- 列出当前域，并列出过去一年的操作。
- 查看过去一年的账单，并查看域类型的价格。
- 获取域建议。
- 检查域可用性和可转移性。
- （可选）申请域注册。
- 获取操作详细信息。
- （可选）获取域详细信息。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

在命令提示符中运行交互式场景。

```
public static class Route53DomainScenario
{
    /*
```

```
   Before running this .NET code example, set up your development environment,
including your credentials.

   This .NET example performs the following tasks:
       1. List current domains.
       2. List operations in the past year.
       3. View billing for the account in the past year.
       4. View prices for domain types.
       5. Get domain suggestions.
       6. Check domain availability.
       7. Check domain transferability.
       8. Optionally, request a domain registration.
       9. Get an operation detail.
      10. Optionally, get a domain detail.
  */

   private static Route53Wrapper _route53Wrapper = null!;
   private static IConfiguration _configuration = null!;

   static async Task Main(string[] args)
   {
       // Set up dependency injection for the Amazon service.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
                   .ConfigureServices((_, services) =>
           services.AddAWSService<IAmazonRoute53Domains>()
               .AddTransient<Route53Wrapper>()
           )
           .Build();

       _configuration = new ConfigurationBuilder()
           .SetBasePath(Directory.GetCurrentDirectory())
           .AddJsonFile("settings.json") // Load settings from .json file.
           .AddJsonFile("settings.local.json",
               true) // Optionally, load local settings.
           .Build();

       var logger = LoggerFactory.Create(builder =>
       {
```

```
            builder.AddConsole();
        }).CreateLogger(typeof(Route53DomainScenario));

        _route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            await ListDomains();
            await ListOperations();
            await ListBillingRecords();
            await ListPrices();
            await ListDomainSuggestions();
            await CheckDomainAvailability();
            await CheckDomainTransferability();
            var operationId = await RequestDomainRegistration();
            await GetOperationalDetail(operationId);
            await GetDomainDetails();
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List account registered domains.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomains()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"1. List account domains.");
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
```

```
        {
            Console.WriteLine($"\t{i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {
            Console.WriteLine("\tNo domains found in this account.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain operations in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListOperations()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"2. List account domain operations in the past
year.");
        var operations = await _route53Wrapper.ListOperations(
            DateTime.Today.AddYears(-1));
        for (int i = 0; i < operations.Count; i++)
        {
            Console.WriteLine($"\tOperation Id: {operations[i].OperationId}");
            Console.WriteLine($"\tStatus: {operations[i].Status}");
            Console.WriteLine($"\tDate: {operations[i].SubmittedDate}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List billing in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListBillingRecords()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"3. View billing for the account in the past year.");
        var billingRecords = await _route53Wrapper.ViewBilling(
            DateTime.Today.AddYears(-1),
            DateTime.Today);
        for (int i = 0; i < billingRecords.Count; i++)
```

```
        {
            Console.WriteLine($"\tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
            Console.WriteLine($"\tOperation: {billingRecords[i].Operation}");
            Console.WriteLine($"\tPrice: {billingRecords[i].Price}");
        }
        if (!billingRecords.Any())
        {
            Console.WriteLine("\tNo billing records found in this account for the
past year.");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List prices for a few domain types.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListPrices()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. View prices for domain types.");
        var domainTypes = new List<string> { "net", "com", "org", "co" };

        var prices = await _route53Wrapper.ListPrices(domainTypes);
        foreach (var pr in prices)
        {
            Console.WriteLine($"\tName: {pr.Name}");
            Console.WriteLine($"\tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
            Console.WriteLine($"\tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
            Console.WriteLine($"\tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
            Console.WriteLine($"\tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
            Console.WriteLine();
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
```

```
    /// List domain suggestions for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomainSuggestions()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"5. Get domain suggestions.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to get available domain
suggestions.");
            domainName = Console.ReadLine();
        }

        var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName,
true, 5);
        foreach (var suggestion in suggestions)
        {
            Console.WriteLine($"\tSuggestion Name: {suggestion.DomainName}");
            Console.WriteLine($"\tAvailability: {suggestion.Availability}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check availability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainAvailability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Check domain availability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
availability.");
            domainName = Console.ReadLine();
        }

        var availability = await
_route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\tAvailability: {availability}");
```

```
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
 transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
 _route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\tNote: This example uses domain request settings in
 settings.json.");
        Console.WriteLine($"\tTo change the domain registration settings, set the
 values in that file.");
        Console.WriteLine($"\tRemember, registering an actual domain will incur
 an account billing cost.");
        Console.WriteLine($"\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
```

```
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();
            contact.CountryCode =
CountryCode.FindValue(_configuration["Contact:CountryCode"]);
            contact.ContactType =
ContactType.FindValue(_configuration["Contact:ContactType"]);

            _configuration.GetSection("Contact").Bind(contact);

            var operationId = await _route53Wrapper.RegisterDomain(
                domainName,
                Convert.ToBoolean(_configuration["AutoRenew"]),
                Convert.ToInt32(_configuration["DurationInYears"]),
                contact);
            if (operationId != null)
            {
                Console.WriteLine(
                    $"\tRegistration requested. Operation Id: {operationId}");
            }

            return operationId;
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }

    /// <summary>
    /// Get details for an operation.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task GetOperationalDetail(string? operationId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Get an operation detail.");

        var operationDetails =
            await _route53Wrapper.GetOperationDetail(operationId);

        Console.WriteLine(operationDetails);
```

```
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Optionally, get details for a registered domain.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\tNote: you must have a registered domain to get
 details.");
        Console.WriteLine($"\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }

            var domainDetails = await
 _route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}
```

场景用于 Route 53 域注册操作的包装程序方法。

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
```

```
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }


    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }


    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Availability.Value;
    }
```

```
    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }


    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }


    /// <summary>
    /// Get details for a domain action operation.
```

```
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
 {operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }


    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
```

```
    {
        // This example uses the same contact information for admin, registrant,
and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }


    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
```

```
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }


    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }


    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
```

```
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }


    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
 {result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}
```

- 有关 API 详细信息，请参阅《适用于 .NET 的 Amazon SDK API Reference》中的以下主题。
  - CheckDomainAvailability

- CheckDomainTransferability
- GetDomainDetail
- GetDomainSuggestions
- GetOperationDetail
- ListDomains
- ListOperations
- ListPrices
- RegisterDomain
- ViewBilling

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库 中查找完整示例，了解如何进行设置和运行。

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
 *
 * This Java code example performs the following operations:
```

```
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
 * 4. View prices for domain types.
 * 5. Get domain suggestions.
 * 6. Check domain availability.
 * 7. Check domain transferability.
 * 8. Request a domain registration.
 * 9. Get operation details.
 * 10. Optionally, get domain details.
 */

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <domainType> <phoneNumber> <email> <domainSuggestion>
 <firstName> <lastName> <city>

                Where:
                    domainType - The domain type (for example, com).\s
                    phoneNumber - The phone number to use (for example,
 +91.9966564xxx)      email - The email address to use.      domainSuggestion -
 The domain suggestion (for example, findmy.accountants).\s
                    firstName - The first name to use to register a domain.\s
                    lastName -  The last name to use to register a domain.\s
                    city - the city to use to register a domain.\s
                    """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
```

```
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. List current domains.");
        listDomains(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. List operations in the past year.");
        listOperations(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. View billing for the account in the past year.");
        listBillingRecords(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. View prices for domain types.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Get domain suggestions.");
        listDomainSuggestions(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
```

```
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
domainSuggestion, phoneNumber, email, firstName,
                lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxx not found in xxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }

    public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
            System.out.println("The contact first name is " +
response.registrantContact().firstName());
            System.out.println("The contact last name is " +
response.registrantContact().lastName());
            System.out.println("The contact org name is " +
response.registrantContact().organizationName());

        } catch (Route53Exception e) {
```

```
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
        try {
            GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                    .operationId(operationId)
                    .build();

            GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
            System.out.println("Operation detail message is " +
response.message());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
            String domainSuggestion,
            String phoneNumber,
            String email,
            String firstName,
            String lastName,
            String city) {

        try {
            ContactDetail contactDetail = ContactDetail.builder()
                    .contactType(ContactType.COMPANY)
                    .state("LA")
                    .countryCode(CountryCode.IN)
                    .email(email)
                    .firstName(firstName)
                    .lastName(lastName)
                    .city(city)
                    .phoneNumber(phoneNumber)
                    .organizationName("My Org")
```

```
                    .addressLine1("My Address")
                    .zipCode("123 123")
                    .build();

            RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                    .adminContact(contactDetail)
                    .registrantContact(contactDetail)
                    .techContact(contactDetail)
                    .domainName(domainSuggestion)
                    .autoRenew(true)
                    .durationInYears(1)
                    .build();

            RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
            System.out.println("Registration requested. Operation Id: " +
response.operationId());
            return response.operationId();

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }

    public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainTransferabilityResponse response = route53DomainsClient
                    .checkDomainTransferability(transferabilityRequest);
            System.out.println("Transferability: " +
response.transferability().transferable().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

```
   public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainAvailabilityResponse response = route53DomainsClient
                   .checkDomainAvailability(availabilityRequest);
           System.out.println(domainSuggestion + " is " +
response.availability().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                   .domainName(domainSuggestion)
                   .suggestionCount(5)
                   .onlyAvailable(true)
                   .build();

           GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
           List<DomainSuggestion> suggestions = response.suggestionsList();
           for (DomainSuggestion suggestion : suggestions) {
               System.out.println("Suggestion Name: " +
suggestion.domainName());
               System.out.println("Availability: " + suggestion.availability());
               System.out.println(" ");
           }

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
```

```
   }

   public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
       try {
           ListPricesRequest pricesRequest = ListPricesRequest.builder()
                   .tld(domainType)
                   .build();

           ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
           listRes.stream()
                   .flatMap(r -> r.prices().stream())
                   .forEach(content -> System.out.println(" Name: " +
content.name() +
                           " Registration: " +
content.registrationPrice().price() + " "
                           + content.registrationPrice().currency() +
                           " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();
```

```
            ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
            listRes.stream()
                    .flatMap(r -> r.billingRecords().stream())
                    .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                            " Operation: " + content.operationAsString() +
                            " Price: " + content.price()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
            Instant myTime = localDateTime.toInstant(zoneOffset);

            ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- 有关 API 详细信息，请参阅《Amazon SDK for Java 2.x API Reference》中的以下主题。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
 */

val DASHES: String = String(CharArray(80)).replace("\u0000", "-")

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
 <lastName> <city>
        Where:
           domainType - The domain type (for example, com).
```

```
            phoneNumber - The phone number to use (for example, +1.2065550100)

            email - The email address to use.
            domainSuggestion - The domain suggestion (for example,
findmy.example).
            firstName - The first name to use to register a domain.
            lastName -  The last name to use to register a domain.
            city - The city to use to register a domain.
    """

    if (args.size != 7) {
        println(usage)
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
    listOperations()
    println(DASHES)

    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
```

```
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("7. Check domain transferability.")
    checkDomainTransferability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("8. Request a domain registration.")
    val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
 firstName, lastName, city)
    println(DASHES)

    println(DASHES)
    println("9. Get operation details.")
    getOperationalDetail(opId)
    println(DASHES)

    println(DASHES)
    println("10. Get domain details.")
    println("Note: You must have a registered domain to get details.")
    println("Otherwise an exception is thrown that states ")
    println("Domain xxxxxxx not found in xxxxxxx account.")
    getDomainDetails(domainSuggestion)
    println(DASHES)
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
```

```
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
```

```
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
```

```
    }
}

suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
```

```
}

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }
```

```
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}

suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- 有关 API 详细信息，请参阅《Amazon SDK for Kotlin API Reference》中的以下主题。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

使用 Route 53 注册域名的操作 Amazon SDKs

以下代码示例演示如何使用执行各个 Route 53 域名注册操作 Amazon SDKs。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 Amazon Route 53 domain registration API 参考。

示例

- CheckDomainAvailability与 Amazon SDK 或 CLI 配合使用
- CheckDomainTransferability与 Amazon SDK 或 CLI 配合使用
- GetDomainDetail与 Amazon SDK 或 CLI 配合使用
- GetDomainSuggestions与 Amazon SDK 或 CLI 配合使用
- GetOperationDetail与 Amazon SDK 或 CLI 配合使用
- ListDomains与 Amazon SDK 或 CLI 配合使用
- ListOperations与 Amazon SDK 或 CLI 配合使用
- 与 Amazon SDK ListPrices 配合使用
- RegisterDomain与 Amazon SDK 或 CLI 配合使用
- ViewBilling与 Amazon SDK 或 CLI 配合使用

CheckDomainAvailability与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `CheckDomainAvailability`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考CheckDomainAvailability中的。

CLI

Amazon CLI

确定是否可以在 Route 53 上注册域名

以下 `check-domain-availability` 命令返回有关域名 `example.com` 是否可以使用 Route 53 进行注册的信息。

此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

输出：

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 支持大量顶级域 (TLDs)，例如.com和.jp，但我们不支持所有可用的域名 TLDs。如果您查看某个域是否可用，而 Route 53 不支持该顶级域，check-domain-availability 会返回以下消息。

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

有关在 Route 53 注册域名时可以 TLDs 使用的列表，请参阅《亚马逊 Route 53 开发者指南》中的 “您可以在亚马逊 Route 53 上注册的域名”。有关使用 Amazon Route 53 注册域的更多信息，请参阅《Amazon Route 53 开发人员指南》中的注册新域。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CheckDomainAvailability中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
```

```
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
 CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                    .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
 response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考CheckDomainAvailability中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
```

```
    }
}
```

- 有关 API 的详细信息，请参阅适用CheckDomainAvailability于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`CheckDomainTransferability`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `CheckDomainTransferability`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
```

```
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考CheckDomainTransferability中的。

CLI

Amazon CLI

确定域是否可以传输到 Route 53

以下 `check-domain-transferability` 命令返回有关是否可以将域名 `example.com` 传输到 Route 53 的信息。

此命令仅在 `us-east-1` 区域中运行。如果您的默认区域设置为 `us-east-1`，则可以省略 `region` 参数。

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

输出：

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的将域注册转移到 Amazon Route 53。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CheckDomainTransferability中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
           System.out.println("Transferability: " +
response.transferability().transferable().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考CheckDomainTransferability中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- 有关 API 的详细信息，请参阅适用CheckDomainTransferability于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`GetDomainDetail`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `GetDomainDetail`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
{result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考GetDomainDetail中的。

CLI

Amazon CLI

获取有关指定域的详细信息

以下 get-domain-detail 命令显示有关指定域的详细信息。

此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

输出：

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
```

```
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon",
    "RegistrarUrl": "http://registrar.amazon.com",
    "AbuseContactEmail": "abuse@registrar.amazon.com",
```

```
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetDomainDetail中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考GetDomainDetail中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}
```

- 有关 API 的详细信息，请参阅适用GetDomainDetail于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`GetDomainSuggestions`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `GetDomainSuggestions`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考GetDomainSuggestions中的。

CLI

Amazon CLI

获取建议的域名列表

以下 get-domain-suggestions 命令根据域名 example.com 显示建议域名列表。响应仅包含可用域名。此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

输出：

```
{
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
```

```
        },
        {
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetDomainSuggestions中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();
```

```
            GetDomainSuggestionsResponse response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
 suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考GetDomainSuggestions中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
```

```
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}
```

- 有关 API 的详细信息，请参阅适用GetDomainSuggestions于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`GetOperationDetail`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `GetOperationDetail`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
```

```
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考GetOperationDetail中的。

CLI

Amazon CLI

获取操作的当前状态

某些域注册操作是异步运行的，并在完成之前返回响应。这些操作会返回一个操作 ID，您可以使用它来获取当前状态。以下 `get-operation-detail` 命令返回指定操作的状态。

此命令仅在 `us-east-1` 区域中运行。如果您的默认区域设置为 `us-east-1`，则可以省略 `region` 参数。

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

输出：

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetOperationDetail中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考GetOperationDetail中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- 有关 API 的详细信息，请参阅适用GetOperationDetail于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`ListDomains`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `ListDomains`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
        results.Add(domain);
    }
    return results;
}
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ListDomains中的。

CLI

Amazon CLI

列出使用当前 Amazon 账户注册的域名

以下`list-domains`命令列出了有关在当前 Amazon 账户中注册的域名的摘要信息。

此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains list-domains
    --region us-east-1
```

输出：

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListDomains中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考ListDomains中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- 有关 API 的详细信息，请参阅适用ListDomains于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

ListOperations与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 ListOperations。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   /// <summary>
   /// List operations for the account that are submitted after a specified
date.
   /// </summary>
   /// <returns>A collection of operation summary records.</returns>
   public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
   {
       var results = new List<OperationSummary>();
       var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
           new ListOperationsRequest()
           {
               SubmittedSince = submittedSince
           });

       // Get the entire list using the paginator.
```

```
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ListOperations中的。

CLI

Amazon CLI

列出返回操作 ID 的操作的状态

某些域注册操作是异步运行的，并在完成之前返回响应。这些操作会返回一个操作 ID，您可以使用它来获取当前状态。以下 `list-operations` 命令列出了有关当前域注册操作的状态等摘要信息。

此命令仅在 `us-east-1` 区域中运行。如果您的默认区域设置为 `us-east-1`，则可以省略 `region` 参数。

```
aws route53domains list-operations
    --region us-east-1
```

输出：

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
```

```
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

输出包括所有返回操作 ID 的操作，以及您在使用当前 Amazon 账户注册的所有域名上执行的操作。如果只想获取在指定日期之后提交的操作，可以包含 `submitted-since` 参数并以 Unix 格式和协调世界时（UTC）指定日期。以下命令可获取在协调世界时间 2020 年 1 月 1 日凌晨 12:00 之后提交的所有操作的状态。

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListOperations中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
```

```
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
            Instant myTime = localDateTime.toInstant(zoneOffset);

            ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考ListOperations中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun listOperations() {
    val currentDate = Date()
```

```
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}
```

- 有关 API 的详细信息，请参阅适用ListOperations于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

与 Amazon SDK **`ListPrices`** 配合使用

以下代码示例演示如何使用 `ListPrices`。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ListPrices中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
       try {
           ListPricesRequest pricesRequest = ListPricesRequest.builder()
                   .tld(domainType)
                   .build();

           ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
           listRes.stream()
                   .flatMap(r -> r.prices().stream())
                   .forEach(content -> System.out.println(" Name: " +
content.name() +
                           " Registration: " +
content.registrationPrice().price() + " "
                           + content.registrationPrice().currency() +
                           " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考ListPrices中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
```

```
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}
```

- 有关 API 的详细信息，请参阅适用ListPrices于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

RegisterDomain与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 RegisterDomain。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
```

```
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
 {domainName}");
            return null;
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考RegisterDomain中的。

CLI

Amazon CLI

注册域

以下 register-domain 命令注册一个域，并从 JSON 格式的文件中检索所有参数值。

此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

register-domain.json 的内容：

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
```

```
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

输出：

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

要确认操作成功，可以运行 `get-operation-detail`。有关更多信息，请参阅 get-operation-detail。

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的注册新域。

有关哪些顶级域名 (TLDs) 需要值`ExtraParams`以及有效值的信息，请参阅ExtraParam《Amazon Route 53 API 参考》。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考RegisterDomain中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
            String domainSuggestion,
            String phoneNumber,
            String email,
            String firstName,
            String lastName,
            String city) {

        try {
            ContactDetail contactDetail = ContactDetail.builder()
                    .contactType(ContactType.COMPANY)
                    .state("LA")
                    .countryCode(CountryCode.IN)
                    .email(email)
                    .firstName(firstName)
                    .lastName(lastName)
                    .city(city)
                    .phoneNumber(phoneNumber)
                    .organizationName("My Org")
                    .addressLine1("My Address")
                    .zipCode("123 123")
```

```
                .build();

        RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                .adminContact(contactDetail)
                .registrantContact(contactDetail)
                .techContact(contactDetail)
                .domainName(domainSuggestion)
                .autoRenew(true)
                .durationInYears(1)
                .build();

        RegisterDomainResponse response =
 route53DomainsClient.registerDomain(domainRequest);
        System.out.println("Registration requested. Operation Id: " +
 response.operationId());
        return response.operationId();

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
  }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考RegisterDomain中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
```

```
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- 有关 API 的详细信息，请参阅适用RegisterDomain于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

ViewBilling与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 ViewBilling。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
```

```
        return results;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ViewBilling中的。

CLI

Amazon CLI

获取当前 Amazon 账户域名注册费用的账单信息

以下 view-billing 命令返回当前账户自 2018 年 1 月 1 日（Unix 时间为 1514764800）至 2019 年 12 月 31 日午夜（Unix 时间为 1577836800）期间的所有与域相关的账单记录。

此命令仅在 us-east-1 区域中运行。如果您的默认区域设置为 us-east-1，则可以省略 region 参数。

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

输出：

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
```

```
}
```

有关更多信息，请参阅ViewBilling《亚马逊 Route 53 API 参考》。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ViewBilling中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();

           ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
           listRes.stream()
                   .flatMap(r -> r.billingRecords().stream())
                   .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                           " Operation: " + content.operationAsString() +
                           " Price: " + content.price()));

       } catch (Route53Exception e) {
```

```
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考ViewBilling中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
```

```
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}
```

- 有关 API 的详细信息，请参阅适用ViewBilling于 K otlin 的Amazon SDK API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅将 Route 53 与 S Amazon DK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

Amazon Route 53 中的安全性

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 Amazon 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础架构。 Amazon 还为您提供可以安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Route 53 的合规性计划，请参阅合规性计划范围内的Amazon 服务。
- 云端安全-您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Route 53 时应用责任共担模型。以下主题说明如何配置 Route 53 以实现您的安全性和合规性目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 Route 53 资源。

主题

Route 53 中的数据保护

责任 Amazon 分适用于 Amazon Route 53 中的数据保护。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 Amazon 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 Amazon 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://www.amazonaws.cn/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或 Amazon Web Services 服务 使用 Route 53 或其他方式时 Amazon SDKs。 Amazon CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

防止 Route 53 中悬挂委派记录

使用 Route 53，客户可以创建托管区（比如 `example.com`）来托管其 DNS 记录。每个托管区均附带一个“委托集”，此集内含有四个名称服务器，客户可以借此服务器在父域中配置 NS 记录。这些 NS 记录可称为“委托 NS 记录”或“委托记录”。

为了使 `example.com` Route 53 托管区成为权威区域，`example.com` 域的合法所有者需要通过域注册商在其“.com”父域中配置委托记录。如果客户无法访问在父域中配置的四个名称服务器，例如由于关联的托管区被删除，则可能会带来攻击者可利用的风险。这称为“悬挂委托记录”风险。

在托管区遭到删除的情况下，Route 53 可防止出现悬挂委托记录的风险。删除后，如果使用相同的域名创建新的托管区，Route 53 会查看指向已删除托管区的委托记录是否仍存在于父域中。如果存在，Route 53 会阻止分配任何重叠的名称服务器。这是以下示例中的场景 1。

但是，还存在 Route 53 无法防范的其他悬挂委托记录风险，如以下示例中的场景 2 和 3 所述。为了保护自己免受这些更广泛的风险，请确保父 NS 记录与为 Route 53 托管区的委托集相匹配。您可以通过

Route 53 控制台或者，找到托管区域的委托集 Amazon CLI。有关更多信息，请参阅 列出记录或 get-hosted-zone。

此外，为 Route 53 托管区启用 DNSSEC 签名可以在上述最佳实践之外提供另一层保护。DNSSEC 会验证 DNS 答案是否来自权威来源，从而有效防止此种风险。有关更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

示例

在以下示例中，我们假设您拥有一个域 example.com 及其子域 child.example.com。我们将解释在各种情况下如何创建悬挂委托记录、Route 53 如何保护域免遭滥用，以及如何有效降低与悬挂委托记录相关的风险。

方案 1:

> 您可以使用四个名称服务器 <ns1>、<ns2>、<ns3> 和 <ns4> 创建一个托管区 child.example.com。您在托管区 example.com 中正确设置了委托，并使用四个名称服务器 <ns1>、<ns2>、<ns3> 和 <ns4> 为 child.example.com 创建委托 NS 记录。当删除 child.example.com 托管区而未移除 example.com 中的委托 NS 记录时，Route 53 会阻止将 <ns1>、<ns2>、<ns3> 和 <ns4> 分配给具有相同域名的新创建托管区，从而防止 child.example.com 出现悬挂委托记录的风险。

方案 2:

> 与场景 1 类似，但这次删除了子托管区和托管区 example.com 中的委托 NS 记录。但是，您可以重新添加委托 NS 记录 <ns1>、<ns2>、<ns3> 和 <ns4> 而不创建子托管区。在这里，<ns1>、<ns2>、<ns3> 和 <ns4> 是悬挂委托记录，因为 Route 53 移除了阻止分配 <ns1>、<ns2>、<ns3> 和 <ns4> 的法定保留，现在允许新创建的托管区使用上述名称服务器。为了降低风险，请从委托记录中删除 <ns1>、<ns2>、<ns3> 和 <ns4>，并且仅在创建了子托管区后才将其重新添加。

场景 3：

> 在此场景中，您将创建一个 Route 53 可重复使用的委托集，其中含有 <ns1>、<ns2>、<ns3> 和 <ns4> 名称服务器。然后，将域 example.com 委托给父域 .com 中的这些名称服务器。但是，您尚未在可重用的委托集中为 example.com 创建托管区。此处的 <ns1>、<ns2>、<ns3> 和 <ns4> 为悬挂委托记录。为了降低风险，请使用带有 <ns1>、<ns2>、<ns3> 和 <ns4> 名称服务器的可重复使用委托集创建托管区。

Amazon Route 53 中的 Identity and Access Management

要对 Amazon Route 53 资源执行任何操作，例如注册域名或更新记录， Amazon Identity and Access Management (IAM) 要求您验证自己是经批准的 Amazon 用户。如果您使用的是 Route 53 控制台，可通过提供您的 Amazon 用户名和密码来验证您的身份。

在您对身份进行身份验证后，IAM 会 Amazon 通过验证您是否有权执行操作和访问资源来控制您的访问权限。如果您是账户管理员，则可使用 IAM 控制其他用户对与您的账户关联的资源的访问。

本章说明如何使用 IAM 和 Route 53 帮助保护您的资源。

主题

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 Amazon Web Services 账户根用户，或者通过担任 IAM 角色进行身份验证。

对于编程访问， Amazon 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的Amazon 签名版本 4。

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先会有一个名为 Amazon Web Services 账户 root 用户的登录身份，该身份可以完全访问所有资源 Amazon Web Services 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 Amazon Web Services 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Amazon Directory Service ，或者 Amazon Web Services 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 Amazon 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 Amazon CLI 或 Amazon API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。 EC2有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

访问控制

要创建、更新、删除或列出 Amazon Route 53 资源，您需要有权执行该操作，并且您需要有权访问相应资源。

下面几节介绍如何管理 Route 53 的权限。我们建议您先阅读概述。

管理 Amazon Route 53 资源的访问权限的概览

每个 Amazon 资源都归一个 Amazon 账户所有，创建或访问资源的权限受权限策略的约束。

> **Note**
>
> 账户管理员 (或管理员用户) 是具有管理员权限的用户。有关管理员的更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

在您授予权限时，您将决定谁可以获得权限，获得对哪些资源的权限，以及他们有权执行的操作。

如果用户想在 Amazon 外部进行交互，则需要编程访问权限 Amazon Web Services 管理控制台。Amazon APIs 和 Amazon Command Line Interface 需要访问密钥。可能的话，创建临时凭证，该凭证由一个访问密钥 ID、一个秘密访问密钥和一个指示凭证何时到期的安全令牌组成。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
IAM	使用短期证书签署对 Amazon CLI 或的编程请求 Amazon APIs（直接或使用 Amazon SDKs）。	按照 IAM 用户指南中的将临时证书与 Amazon 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期证书签署对 Amazon CLI 或的编程请求 Amazon APIs（直接或使用 Amazon SDKs）。	按照《IAM 用户指南》中管理 IAM 用户的访问密钥中的说明进行操作。

主题

- ARNs 适用于 Amazon Route 53 资源
- 了解资源所有权
- 管理对 资源的访问
- 指定策略元素：资源、操作、效果和委托方
- 在策略中指定条件

ARNs 适用于 Amazon Route 53 资源

Amazon Route 53 支持用于 DNS、运行状况检查和域注册的多种资源类型。在策略中，您可以通过将 * 用于 ARN 来授予或拒绝授予对以下资源的访问权限：

- 运行状况检查
- 托管区域

- 可重用的委派集
- 资源记录集变更批处理的状态 (仅限 API)
- 流量策略 (流量)
- 流量策略实例 (流量)

并非所有 Route 53 资源都支持权限。您不能授予或拒绝对以下资源的访问权限：

- Domains
- 单个记录
- 域的标签
- 运行状况检查的标签
- 托管区域的标签

Route 53 提供 API 操作来处理其中每个类型的资源。有关更多信息，请参阅 Amazon Route 53 API 参考。有关您为授予或拒绝使用每项操作的权限而指定的操作和 ARN 的列表，请参阅Amazon Route 53 API 权限：操作、资源和条件参考。

了解资源所有权

一个 Amazon 账户拥有在该账户中创建的资源，不管这些资源是谁创建的。具体而言，资源所有者是对 Amazon 资源创建请求进行身份验证的委托人实体（即根账户或 IAM 角色）的账户。

以下示例说明了它的工作原理：

- 如果您使用账户的根账户凭证创建托管区域，则您的 Amazon 账户就是该资源的所有者。 Amazon
- 如果您在 Amazon 账户中创建用户并向该用户授予创建托管区域的权限，则该用户可以创建托管区域。但是，您的 Amazon 账户（即该用户所属的账户）将拥有该托管区域资源。
- 如果您在 Amazon 账户中创建具有创建托管区域权限的 IAM 角色，则任何能够担任该角色的人都可以创建托管区域。该角色所属的 Amazon 账户拥有托管区域资源。

管理对 资源的访问

权限策略 指定谁可以访问哪些内容。此部分介绍用于为 Amazon Route 53 创建权限策略的选项。有关 IAM policy 语法和说明的信息，请参阅《IAM 用户指南》中的 Amazon IAM policy 参考。

附加到 IAM 身份的策略称作基于身份的策略（IAM 策略），而附加到资源的策略称作基于资源的策略。Route 53 只支持基于身份的策略（IAM 策略）。

主题

- 基于身份的策略（IAM 策略）
- 基于资源的策略

基于身份的策略（IAM 策略）

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

- 向您账户中的用户或组附加权限策略 - 账户管理员可以使用与特定用户关联的权限策略为该用户授予创建 Amazon Route 53 资源的权限。
- 将@@ 权限策略附加到角色（授予跨账户权限）-您可以向由其他 Amazon 账户创建的用户授予执行 Route 53 操作的权限。为实现这一点，您可以将权限策略附加到一个 IAM 角色，然后允许其他账户中的用户代入此角色。以下示例说明如何对两个 Amazon 账户（账户 A 和账户 B）实施该操作：
  1. 账户 A 管理员创建一个 IAM 角色，向该角色附加一个权限策略来授予创建或访问属于账户 A 的资源的权限。
  2. 账户 A 管理员将信任策略附加到角色。信任策略将账户 B 标识为可担任该角色的委托人。
  3. 随后，账户 B 管理员可以将代入角色的权限委派给账户 B 中的用户或组。这将允许账户 B 中的用户创建或访问账户 A 中的资源。

  有关如何向其他 Amazon 账户中的用户委派权限的更多信息，请参阅 IAM 用户指南中的访问管理。

以下示例策略允许用户执行 `CreateHostedZone` 操作，以便为任何 Amazon 账户创建公有托管区域：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
```

```
            "Resource":"*"
        }
    ]
}
```

如果您希望该策略也适用于私有托管区域，则需要授予使用 Route 53 `AssociateVPCWithHostedZone` 操作和两个 Amazon EC2 操作的权限`DescribeRegion`，`DescribeVpcs`以及，如以下示例所示：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

有关将策略附加到 Route 53 的身份的更多信息，请参阅 将基于身份的策略（IAM 策略）用于 Amazon Route 53。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

基于资源的策略

其它服务（例如 Amazon S3）也支持将权限策略附加到资源。例如，您可以将策略附加到 S3 存储桶以管理对该存储桶的访问权限。Amazon Route 53 不支持将策略附加到资源。

指定策略元素：资源、操作、效果和委托方

Amazon Route 53 包括可以在每个 Route 53 资源（请参阅 ARNs 适用于 Amazon Route 53 资源）上使用的 API 操作（请参阅 Amazon Route 53 API 参考）。您可以向用户或联合身份用户授予执行这些操作中的任一操作或所有操作的权限。请注意，有些 API 操作 (如注册域) 需要具有执行多个操作的权限。

以下是基本的策略元素：

- 资源 – 您使用 Amazon 资源名称（ARN）来标识策略应用到的资源。有关更多信息，请参阅 ARNs 适用于 Amazon Route 53 资源。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，根据指定的 `Effect`，`route53:CreateHostedZone` 权限会允许或拒绝用户执行 Route 53 `CreateHostedZone` 操作。
- 效果 – 您指定当用户尝试对指定资源执行操作时的效果（允许或拒绝）。如果您没有明确授予对操作的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体：在基于身份的策略（IAM 策略）中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。Route 53 不支持基于资源的策略。

有关 IAM policy 语法和说明的信息，请参阅《IAM 用户指南》中的 Amazon IAM policy 参考。

有关显示所有 Route 53 API 操作及其适用于的资源的列表，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

在策略中指定条件

当您授予权限时，可使用 IAM policy 语言来指定策略何时生效。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：条件。

要表示条件，您可以使用预定义的条件键。没有特定于 Route 53 的条件键。但是，您可以根据需要使用 Amazon 多种条件键。有关 Amazon 宽密钥的完整列表，请参阅 IAM 用户指南中的条件可用密钥。

将基于身份的策略（IAM 策略）用于 Amazon Route 53

本主题提供了基于身份的策略的示例，这些示例展示了账户管理员如何将权限策略附加到 IAM 身份，从而授予对 Amazon Route 53 资源执行操作的权限。

Important

我们建议您首先阅读一下介绍性主题，这些主题说明了管理对 Route 53 资源的访问的基本概念和选项。有关更多信息，请参阅 管理 Amazon Route 53 资源的访问权限的概览。

Note

授予访问权限时，托管区域和 Amazon VPC 必须属于相同分区。分区是一组 Amazon Web Services 区域。每个分区的作用域 Amazon Web Services 账户 仅限于一个分区。
以下是支持的分区：

- `aws` - Amazon Web Services 区域
- `aws-cn` – 中国区域
- `aws-us-gov` - Amazon GovCloud (US) Region

有关更多信息，请参阅《Amazon 一般参考》中的访问管理和 Amazon Route 53 端点和限额。

主题

下面显示了一个示例权限策略。`Sid` 或语句 ID 是可选的：

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid" : "AllowPublicHostedZonePermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:UpdateHostedZoneComment",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:DeleteHostedZone",
                "route53:ChangeResourceRecordSets",
                "route53:ListResourceRecordSets",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZonesByName"
            ],
            "Resource": "*"
        },
        {
         "Sid" : "AllowHealthCheckPermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHealthCheck",
                "route53:UpdateHealthCheck",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:DeleteHealthCheck",
                "route53:GetCheckerIpRanges",
                "route53:GetHealthCheckCount",
                "route53:GetHealthCheckStatus",
                "route53:GetHealthCheckLastFailureReason"
            ],
            "Resource": "*"
        }
    ]
}
```

该策略包含两条语句：

- 第一条语句授予创建和管理公有托管区域及其记录所需的操作的权限。Amazon 资源名称 (ARN) 中的通配符 (*) 允许访问当前账户拥有的所有托管区域。 Amazon
- 第二条语句授予创建和管理运行状况检查所需的全部操作的权限。

有关您为授予或拒绝使用每项操作的权限而指定的操作和 ARN 的列表，请参阅Amazon Route 53 API 权限：操作、资源和条件参考。

使用 Amazon Route 53 控制台所需的权限

要授予对 Amazon Route 53 控制台的完全访问权，您可以在以下权限策略中授予权限：

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:*",
                "route53domains:*",
                "tag:*",
                "ssm:GetParametersByPath",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "sns:CreateTopic",
                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:Sign",
```

```
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

下面是需要权限的原因：

`route53:*`

您可以执行除以下操作之外的所有 Route 53 操作：

- 创建和更新 Alias Targe t 的值为 CloudFront 分配、Elastic Load Balancing 负载均衡器、Elastic Beanstalk 环境或 Amazon S3 存储桶的别名记录。(通过这些权限，您可以创建其别名目标值为同一托管区域中的另一个记录的别名记录。)
- 使用私有托管区域。
- 使用域。
- 创建、删除和查看 CloudWatch 警报。
- 在 Route 53 控制台中呈现 CloudWatch 指标。

`route53domains:*`

允许您使用域。

> **Important**
>
> 如果您单独列出 `route53` 操作，则必须包含 `route53:CreateHostedZone` 才能使用域。注册域时，会同时创建一个托管区域，因此包括注册域权限的策略还需要创建托管区域的权限。

对于域注册，Route 53 不支持向单个资源授予或拒绝权限。

route53resolver:*

允许您使用 Route 53 VPC 解析器。

ssm:GetParametersByPath

允许您在创建新的别名记录、私有托管区和运行状况检查时获取公开可用的区域。

cloudfront:ListDistributions

允许您创建和更新以 Alias Targe t 的值为 CloudFront 分布的别名记录。

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的分配的列表。

elasticloadbalancing:DescribeLoadBalancers

您可以创建和更新别名目标值为 ELB 负载均衡器的别名记录。

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的负载均衡器的列表。

elasticbeanstalk:DescribeEnvironments

可让您创建和更新 Alias Target（别名目标）值为 Elastic Beanstalk 环境的别名记录。

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的环境的列表。

s3:ListAllMyBuckets、**s3:GetBucketLocation** 和 **s3:GetBucketWebsite**

可让您创建和更新 Alias Target（别名目标）值为 Amazon S3 存储桶的别名记录。（只有将存储桶配置为网站终端节点时，才可以创建 Amazon S3 存储桶的别名；`s3:GetBucketWebsite` 用于获取所需的配置信息。）

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的存储桶的列表。

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

允许您使用私有托管区域。

所有列出的 **ec2** 权限

让你使用 Route 53 VPC 解析器。

sns:ListTopics, **sns:ListSubscriptionsByTopic**, **sns:CreateTopic**, **cloudwatch:DescribeAlarms**, **cloudwatch:PutMetricAlarm**, **cloudwatch:DeleteAlarms**

允许您创建、删除和查看 CloudWatch 警报。

cloudwatch:GetMetricStatistics

允许您创建 CloudWatch 指标运行状况检查。

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的统计数据。

apigateway:GET

可让您创建和更新 Alias Target（别名目标）值为 Amazon API Gateway API 的别名记录。

如果您未使用 Route 53 控制台，则不需要此权限。Route 53 仅使用它来获取 APIs 要在控制台中显示的列表。

kms:*

允许您使用 Amazon KMS 来启用 DNSSEC 签名。

域记录所有者的权限示例

使用资源记录集权限，您可以设置精细的权限，以限制 Amazon 用户可以更新或修改的内容。有关更多信息，请参阅 使用 IAM 策略条件进行精细访问控制。

在某些情况下，托管区域所有者可能负责托管区域的整体管理，而组织中的另一个人负责这些任务的子集。例如，启用 DNSSEC 签名的托管区域所有者可能想要创建一个 IAM 策略，其中包括允许其他人在托管区域中添加和删除资源集记录 (RRs) 以及其他任务。托管区域所有者选择为记录所有者或其他人员启用的特定权限将取决于其组织的策略。

以下是一个允许记录所有者修改流量策略和运行状况检查的 IAM 策略示例。 RRs不允许使用此策略的记录所有者执行区域级操作，例如创建或删除区域、启用或禁用查询日志记录、创建或删除可重用的委派集或更改 DNSSEC 设置。

```
{
      "Sid": "Do not allow zone-level modification ",
      "Effect": "Allow",
      "Action": [
        "route53:ChangeResourceRecordSets",
        "route53:CreateTrafficPolicy",
```

```
        "route53:DeleteTrafficPolicy",
        "route53:CreateTrafficPolicyInstance",
        "route53:CreateTrafficPolicyVersion",
        "route53:UpdateTrafficPolicyInstance",
        "route53:UpdateTrafficPolicyComment",
        "route53:DeleteTrafficPolicyInstance",
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:List*",
        "route53:Get*"
      ],
      "Resource": [
        "*"
      ]
}
```

DNSSEC 签名所需的 Route 53 客户托管密钥权限

当您为 Route 53 启用 DNSSEC 签名时，Route 53 会根据 () 中的客户托管密钥创建密钥签名密钥 (KSK)。 Amazon Key Management Service Amazon KMS您可以使用支持 DNSSEC 签名的现有客户托管密钥或创建一个新密钥。Route 53 必须具有访问您的客户托管密钥的权限，以便它能够为您创建 KSK。

要使 Route 53 能够访问您的客户托管密钥，请确保您的客户托管密钥策略包含以下语句：

```
{
            "Sid": "Allow Route 53 DNSSEC Service",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
            "Action": ["kms:DescribeKey",
                       "kms:GetPublicKey",
                       "kms:Sign"],
            "Resource": "*"
        },
        {
            "Sid": "Allow Route 53 DNSSEC to CreateGrant",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
```

```
            "Action": ["kms:CreateGrant"],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
```

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。为了保护您 Amazon KMS 免受其侵害，您可以选择通过提供aws:SourceAccount和aws:SourceArn条件的组合（两个或一个）来限制服务对基于资源的策略中的资源的权限。 aws:SourceAccount是托管区域所有者的 Amazon 账户 ID。aws:SourceArn是托管区域的 ARN。

以下是可添加的两个权限示例：

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- 或者 -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
```

```
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

有关更多信息，请参阅《IAM 用户指南》中的混淆代理人问题。

客户管理型策略示例

您可以创建自己的自定义 IAM 策略，以授予执行 Route 53 操作的相关权限。您可以将这些自定义策略附加到需要指定权限的 IAM 组。这些策略在您使用 Route 53 API Amazon SDKs、或 Amazon CLI 时起作用。以下示例显示了几个常见使用情形的权限。有关为用户授予 Route 53 的完全访问权限的策略，请参阅 使用 Amazon Route 53 控制台所需的权限。

示例

- 示例 1：允许对所有托管区域进行读取访问
- 示例 2：允许创建和删除托管区域
- 示例 3：允许完全访问所有域（仅限于公有托管区域）
- 示例 4：允许创建入站和出站 Route 53 VPC 解析器终端节点

示例 1：允许对所有托管区域进行读取访问

以下权限策略向用户授予列出所有托管区域并查看某一托管区域中的所有记录的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
```

```
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

示例 2：允许创建和删除托管区域

以下权限策略允许用户创建和删除托管区域并跟踪更改进度。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

示例 3：允许完全访问所有域（仅限于公有托管区域）

以下权限策略允许用户执行与域注册有关的所有操作，包括注册域和创建托管区域的权限。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

注册域时，会同时创建一个托管区域，因此包括注册域权限的策略还需要创建托管区域的权限。（对于域注册，Route 53 不支持向单个资源授予权限。）

有关使用私有托管区域所需权限的信息，请参阅使用 Amazon Route 53 控制台所需的权限。

示例 4：允许创建入站和出站 Route 53 VPC 解析器终端节点

以下权限策略允许用户使用 Route 53 控制台创建 Resolver 入站和出站终端节点。

其中一些权限仅当在控制台中创建终端节点时才需要。如果您希望仅授予以编程方式创建入站和出站终端节点的权限，则可以省略上面这些权限：

- `route53resolver:ListResolverEndpoints` 允许用户查看入站或出站终端节点列表，以便他们验证终端节点是否已创建。
- 显示可用区列表时需要 `DescribeAvailabilityZones`。
- `DescribeVpcs`是显示列表所必需的VPCs。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
```

```
                "route53resolver:CreateResolverEndpoint",
                "route53resolver:ListResolverEndpoints",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

对 Amazon Route 53 Resolver使用服务相关角色

Route 53 VPC 解析器使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 VPC 解析器。服务相关角色由 VPC Resolver 预定义，包括该服务代表您调用其他 Amazon 服务所需的所有权限。

服务相关角色使设置 VPC Resolver 变得更加容易，因为您不必手动添加必要的权限。VPC 解析器定义其服务相关角色的权限，除非另有定义，否则只有 VPC 解析器可以担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。

只有在先删除相关资源后，才能删除服务相关角色。这可以保护您的 VPC 解析器资源，因为您不会无意中移除访问这些资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅与 IAM 配合使用的Amazon 服务，并查找 Service-linked Role（服务相关角色）列中为 Yes（是）的服务。选择是和链接，查看该服务的服务关联角色文档。

主题

- VPC 解析器的服务相关角色权限
- 为 VPC 解析器创建服务相关角色
- 编辑 VPC 解析器的服务相关角色
- 删除 VPC 解析器的服务相关角色
- VPC 解析器服务相关角色支持的区域

VPC 解析器的服务相关角色权限

VPC Resolver 使用**AWSServiceRoleForRoute53Resolver**服务相关角色代表您传送查询日志。

角色权限策略允许 VPC Resolver 对您的资源完成以下操作：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务关联角色权限。

为 VPC 解析器创建服务相关角色

您无需手动创建服务关联角色。当您在 Amazon Route 53 控制台、或 Amazon API 中创建解析器查询日志配置关联时，VPC 解析器会为您创建服务相关角色。 Amazon CLI

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务关联角色可以出现在您的账户中。此外，如果您在 2020 年 8 月 12 日开始支持服务相关角色之前使用 VPC 解析器服

务，那么 VPC Resolver 会在您的账户中创建该AWSServiceRoleForRoute53Resolver角色。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您创建一个新的 Resolver 查询日志配置关联时，将再次为您创建 AWSServiceRoleForRoute53Resolver 服务相关角色。

编辑 VPC 解析器的服务相关角色

VPC 解析器不允许您编辑AWSServiceRoleForRoute53Resolver服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 VPC 解析器的服务相关角色

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 VPC 解析器服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除使用的 VPC 解析器资源 **AWSServiceRoleForRoute53Resolver**

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 展开 Route 53 控制台菜单。在控制台的左上角，选择三个水平条（ ☰ ）图标。
3. 在 Resolver 菜单中，选择 Query logging（查询日志记录）。
4. 选择查询日志记录配置名称旁边的复选框，然后选择 Delete（删除）。
5. 在 Delete query logging configuration（删除查询日志记录配置）文本框中，选择 Stop logging queries（停止日志记录查询）。

这将解除配置与 VPC 的关联。您还可以通过编程方式解除查询日志记录配置的关联。有关更多信息，请参阅 disassociate-resolver-query-log-config。

6. 日志记录查询停止后，您可以选择在字段中键入 **delete**，然后选择 Delete（删除）以删除查询日志记录配置。但是，这对于删除 AWSServiceRoleForRoute53Resolver 使用的资源并非必需。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 Amazon CLI、或 Amazon API 删除AWSServiceRoleForRoute53Resolver服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

VPC 解析器服务相关角色支持的区域

VPC Resolver 不支持在提供服务的每个区域中使用服务相关角色。您可以在以下区域中使用 AWSServiceRoleForRoute53Resolver 角色。

区域名称	区域标识	VPC 解析器中的 Support
美国东部（弗吉尼亚州北部）	us-east-1	是
美国东部（俄亥俄州）	us-east-2	是
美国西部（北加利福尼亚）	us-west-1	是
美国西部（俄勒冈州）	us-west-2	是
亚太地区（孟买）	ap-south-1	是
亚太地区（大阪）	ap-northeast-3	是
Asia Pacific (Seoul)	ap-northeast-2	是
亚太地区（新加坡）	ap-southeast-1	是
亚太地区（悉尼）	ap-southeast-2	是
亚太地区（东京）	ap-northeast-1	是
加拿大（中部）	ca-central-1	是

区域名称	区域标识	VPC 解析器中的 Support
欧洲地区（法兰克福）	eu-central-1	是
欧洲地区（爱尔兰）	eu-west-1	是
欧洲地区（伦敦）	eu-west-2	是
欧洲（巴黎）	eu-west-3	是
南美洲（圣保罗）	sa-east-1	是
中国（北京）	cn-north-1	是
中国（宁夏）	cn-northwest-1	是
Amazon GovCloud (US)	us-gov-east-1	是
Amazon GovCloud (US)	us-gov-west-1	是

Amazon 亚马逊 Route 53 的托管策略

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon 托管策略： AmazonRoute53 FullAccess

您可以将 `AmazonRoute53FullAccess` 策略附加到 IAM 身份。

此策略授予对 Route 53 资源的完全访问权限，包括域名注册和运行状况检查，但不包括 VPC 解析器。

权限详细信息

该策略包含以下权限。

- route53:* - 您可以执行除以下操作之外的所有 Route 53 操作：
  - 创建和更新 Alias Targe t 的值为 CloudFront 分配、Elastic Load Balancing 负载均衡器、Elastic Beanstalk 环境或 Amazon S3 存储桶的别名记录。(通过这些权限，您可以创建其别名目标值为同一托管区域中的另一个记录的别名记录。)
  - 使用私有托管区域。
  - 使用域。
  - 创建、删除和查看 CloudWatch 警报。
  - 在 Route 53 控制台中呈现 CloudWatch 指标。
- route53domains:* - 可让您使用域。
- cloudfront:ListDistributions— 允许您创建和更新以 Alias Targe t 的值为 CloudFront分布的别名记录。

  如果您未使用 Route 53 控制台，则不需要此权限。Route 53 仅用它来获取要在控制台中显示的分配的列表。
- cloudfront:GetDistributionTenantByDomain— 用于获取 CloudFront 多租户分配，允许您创建和更新 Alias Targe t 的值为 CloudFront 分配租户的别名记录。
- cloudfront:GetConnectionGroup— 用于获取 CloudFront 多租户分配，允许您创建和更新 Alias Targe t 的值为 CloudFront 分配租户的别名记录。
- cloudwatch:DescribeAlarms— 与sns:ListTopics和sns:ListSubscriptionsByTopic一起允许您创建、删除和查看 CloudWatch 警报。
- cloudwatch:GetMetricStatistics— 允许您创建 CloudWatch指标运行状况检查。

  如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的统计数据。
- cloudwatch:GetMetricData— 允许您显示 CloudWatch 运行状况检查指标的状态。
- ec2:DescribeVpcs— 允许您显示列表 VPCs。
- ec2:DescribeVpcEndpoints - 可让您显示 VPC 终端节点列表。
- ec2:DescribeRegions - 可让您显示可用区列表。
- elasticloadbalancing:DescribeLoadBalancers - 可让您创建和更新 Alias Target（别名目标）值为 Elastic Load Balancing 负载均衡器的别名记录。

如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的负载均衡器的列表。

- `elasticbeanstalk:DescribeEnvironments` - 可让您创建和更新 Alias Target（别名目标）值为 Elastic Beanstalk 环境的别名记录。

  如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用它来获取要在控制台中显示的环境的列表。

- `es:ListDomainNames`— 允许您显示当前用户在活跃地区拥有的所有 Amazon Ser OpenSearch vice 域名的名称。
- `es:DescribeDomains`— 允许您获取指定 Amazon OpenSearch 服务域的域配置。
- `lightsail:GetContainerServices`— 允许你使用 Lightsail 容器服务来创建和更新 Alias Target 的值为 Lightsail 域的别名记录。
- `s3:ListBucket`、`s3:GetBucketLocation` 和 `s3:GetBucketWebsite` - 可让您创建和更新 Alias Target（别名目标）值为 Amazon S3 存储桶的别名记录。（只有将存储桶配置为网站终端节点时，才可以创建 Amazon S3 存储桶的别名；`s3:GetBucketWebsite` 用于获取所需的配置信息。）

  如果您未使用 Route 53 控制台，则不需要这些权限。Route 53 仅用这些权限来获取要在控制台中显示的存储桶的列表。

- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — 允许您创建、删除和查看 CloudWatch 警报。
- `tag:GetResources` - 可让您在资源中显示标签。例如，您的运行状况检查的名称。
- `apigateway:GET` - 可让您创建和更新 Alias Target（别名目标）值为 Amazon API Gateway API 的别名记录。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
```

```
    "route53:*",
    "route53domains:*",
    "cloudfront:ListDistributions",
    "cloudfront:GetDistributionTenantByDomain",
    "cloudfront:GetConnectionGroup",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricData",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRegions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticbeanstalk:DescribeEnvironments",
    "es:ListDomainNames",
    "es:DescribeDomains",
    "lightsail:GetContainerServices",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "apigateway:GET",
   "Resource": "arn:aws:apigateway:*::/domainnames"
  }
 ]
}
```

Amazon 托管策略： AmazonRoute53 ReadOnlyAccess

您可以将 AmazonRoute53ReadOnlyAccess 策略附加到 IAM 身份。

此策略授予对 Route 53 资源的只读访问权限，包括域注册和运行状况检查，但不包括 VPC 解析器。

权限详细信息

该策略包含以下权限。

- `route53:Get*` - 获取 Route 53 资源。
- `route53:List*` – 列出 Route 53 资源。
- `route53:TestDNSAnswer` - 获取 Route 53 为响应 DNS 请求而返回的值。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略： AmazonRoute53 DomainsFullAccess

您可以将 `AmazonRoute53DomainsFullAccess` 策略附加到 IAM 身份。

此策略授予对 Route 53 域注册资源的完全访问权限。

权限详细信息

该策略包含以下权限。

- `route53:CreateHostedZone` - 可让您创建 Route 53 托管区域。
- `route53domains:*` - 可让您注册域名并执行相关操作。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略： AmazonRoute53 DomainsReadOnlyAccess

您可以将 `AmazonRoute53DomainsReadOnlyAccess` 策略附加到 IAM 身份。

此策略授予对 Route 53 域注册资源的只读访问权限。

权限详细信息

该策略包含以下权限。

- `route53domains:Get*` - 可让您从 Route 53 中检索域列表。
- `route53domains:List*` - 可让您显示 Route 53 域的列表。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略： AmazonRoute53 ResolverFullAccess

您可以将 AmazonRoute53ResolverFullAccess 策略附加到 IAM 身份。

此策略授予对 Route 53 VPC 解析器资源的完全访问权限。

权限详细信息

该策略包含以下权限。

- route53resolver:*— 允许您在 Route 53 控制台上创建和管理 VPC 解析器资源。
- ec2:DescribeSubnets - 可让您列出 Amazon VPC 子网。
- ec2:CreateNetworkInterface、ec2:DeleteNetworkInterface 和 ec2:ModifyNetworkInterfaceAttribute - 可让您创建、修改和删除网络接口。
- ec2:DescribeNetworkInterfaces - 可让您显示网络接口列表。
- ec2:DescribeSecurityGroups - 可让您显示所有安全组的列表。
- ec2:DescribeVpcs— 允许您显示列表 VPCs。
- ec2:DescribeAvailabilityZones - 可让您列出可供您使用的区域。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AmazonRoute53ResolverFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略： AmazonRoute53 ResolverReadOnlyAccess

您可以将 AmazonRoute53ResolverReadOnlyAccess 策略附加到 IAM 身份。

此策略授予对 Route 53 VPC 解析器资源的只读访问权限。

权限详细信息

该策略包含以下权限。

- route53resolver:Get*— 获取 VPC 解析器资源。
- route53resolver:List*— 允许您显示 VPC 解析器资源列表。
- ec2:DescribeNetworkInterfaces - 可让您显示网络接口列表。
- ec2:DescribeSecurityGroups - 可让您显示所有安全组的列表。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略：Route53 ResolverServiceRolePolicy

您不能将 Route53ResolverServiceRolePolicy 附加到自己的 IAM 实体。此策略附加到服务相关角色，允许 Route 53 VPC 解析器访问由 VPC 解析器使用或管理的 Amazon 服务和资源。有关更多信息，请参阅 对 Amazon Route 53 Resolver使用服务相关角色。

Amazon 托管策略： AmazonRoute53 ProfilesFullAccess

您可以将 AmazonRoute53ProfilesReadOnlyAccess 策略附加到 IAM 身份。

此策略授予对 Amazon Route 53 配置文件资源的完全访问权限。

权限详细信息

该策略包含以下权限。

- route53profiles - 可让您在 Route 53 控制台上创建和管理配置文件资源。
- ec2— 允许校长获取有关 VPCs信息。

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:PutProfilePolicy",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
```

```
}
```

Amazon 托管策略： AmazonRoute53 ProfilesReadOnlyAccess

您可以将 `AmazonRoute53ProfilesReadOnlyAccess` 策略附加到 IAM 身份。

此策略授予对 Amazon Route 53 配置文件资源的只读访问权限。

权限详细信息

有关权限的更多信息，请参阅 Amazon Route 53 API 权限：操作、资源和条件参考。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon 托管策略的 Route 53 更新

查看自该服务开始跟踪这些更改以来 Route 53 Amazon 托管策略更新的详细信息。有关此页面更改的自动提醒，请订阅 Route 53 文档历史记录页面上的 RSS 源。

更改	描述	日期
AmazonRoute53 FullAccess — 更新了政策	添加了 `cloudwatch:GetMetricData` 、`tag:GetResources` 、`es:ListDomainNames` 、`es:DescribeDomains` 、`cloudfront:GetDistributionTenantByDomain` 、`cloudfront:GetConnectionGroup` 和 `lightsail:GetContainerServices` 的权限。这些权限使您能够获取最多 500 个运行 CloudWatch 状况检查指标、最多 100 个运行状况检查名称、获取指定亚马逊 OpenSearch 服务域的域配置、列出当前用户在活动区域中拥有的所有亚马逊 OpenSearch 服务域的名称、获取 CloudFront 多租户分配并获取 Lightsail 容器服务。	2025 年 6 月 1 日
AmazonRoute53 ProfilesFullAccess — 更新了政策	添加了 `GetProfilePolicy` 和 `PutProfilePolicy` 权限。这些是仅限权限的 IAM 操作。如果 IAM 委托人未获得这些权限，则在尝试使用该	2024 年 8 月 27 日

更改	描述	日期
	Amazon RAM 服务共享个人资料时会出错。	
AmazonRoute53 ProfilesReadOnlyAccess — 更新了政策	添加了 `GetProfilePolicy` 权限。这是仅限权限的 IAM 操作。如果 IAM 委托人未获得此权限，则尝试使用该 Amazon RAM 服务访问配置文件的策略时将发生错误。	2024 年 8 月 27 日
AmazonRoute53 ResolverFullAccess — 更新了政策	添加了语句 ID (Sid)，以唯一地标识策略。	2024 年 8 月 5 日
AmazonRoute53 ResolverReadOnlyAccess — 更新了政策	添加了语句 ID (Sid)，以唯一地标识策略。	2024 年 8 月 5 日
AmazonRoute53 ProfilesFullAccess — 新政策	Amazon Route 53 添加了一项新策略，允许完全访问 Amazon Route 53 配置文件资源。	2024 年 4 月 22 日
AmazonRoute53 ProfilesReadOnlyAccess — 新政策	Amazon Route 53 添加了一项新策略，允许以只读形式访问 Amazon Route 53 配置文件资源。	2024 年 4 月 22 日
53 号公路 ResolverServiceRolePolicy — 新政策	Amazon Route 53 添加了一项附加到服务相关角色的新策略，允许 VPC 解析器访问由解析器使用或管理的 Amazon 服务和资源。	2021 年 7 月 14 日
AmazonRoute53 ResolverReadOnlyAccess — 新政策	Amazon Route 53 添加了一项新政策，允许对 VPC 解析器资源进行只读访问。	2021 年 7 月 14 日

更改	描述	日期
AmazonRoute53 ResolverFullAccess — 新政策	Amazon Route 53 添加了一项新政策，允许完全访问 VPC 解析器资源。	2021 年 7 月 14 日
AmazonRoute53 DomainsReadOnlyAccess — 新政策	Amazon Route 53 添加了一项新策略，允许以只读形式访问 Route 53 域资源。	2021 年 7 月 14 日
AmazonRoute53 DomainsFullAccess — 新政策	Amazon Route 53 添加了一项新策略，允许完全访问 Route 53 域资源。	2021 年 7 月 14 日
AmazonRoute53 ReadOnlyAccess — 新政策	Amazon Route 53 添加了一项新策略，允许以只读形式访问 Route 53 资源。	2021 年 7 月 14 日
AmazonRoute53 FullAccess — 新政策	Amazon Route 53 添加了一项新策略，允许完全访问 Route 53 资源。	2021 年 7 月 14 日
Route 53 已开启跟踪更改	Route 53 开始跟踪其 Amazon 托管策略的更改。	2021 年 7 月 14 日

使用 IAM 策略条件进行精细访问控制

在 Route 53 中，使用 IAM policy 授予权限时，您可以指定条件（请参阅 访问控制）。例如，您可以：

- 授予权限以允许访问单个资源记录集。
- 授予权限以允许用户访问托管区域中特定 DNS 记录类型的所有资源记录集，例如 A 和 AAAA 记录。
- 授予权限以允许用户访问其名称包含特定字符串的资源记录集。
- 授予权限以允许用户仅在 Route 53 控制台上或使用 ChangeResourceRecordSetsAPI 时执行部分`CREATE | UPSERT | DELETE`操作。
- 授予允许用户将私有托管区与特定 VPC 关联或取消关联的权限。

- 授予允许用户将关联至特定 VPC 的托管区列示出来的权限。
- 授予允许用户创建新的私有托管区并将其关联至特定 VPC 的权限。
- 授予允许用户创建或删除 VPC 关联授权的权限。

您还可以创建组合任意精细权限的权限。

标准化 Route 53 条件键值

您为策略条件输入的值必须格式化或标准化，如下所示：

对于 **`route53:ChangeResourceRecordSetsNormalizedRecordNames`**：

- 所有字母必须为小写形式。
- DNS 名称不得带有结尾圆点。
- 除 a-z、0-9、-（连字符）、_（下划线）和 .（句点，作为标签之间的分隔符）以外的字符必须使用 \三位八进制代码格式的转义码。例如，`\052` 是字符 * 的八进制代码。

对于 **`route53:ChangeResourceRecordSetsActions`**，该值可为以下任意值，且必须为大写：

- CREATE
- UPSERT
- DELETE

对于 **`route53:ChangeResourceRecordSetsRecordTypes`**：

- 该值必须为大写，并且可以是 Route 53 支持的任何一种 DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。

对于 **`route53:VPCs`**：

- 该值必须采用 `VPCId=<vpc-id>,VPCRegion=<region>` 格式。
- `<vpc-id>` 和 `<region>` 的值必须为小写，比如 `VPCId=vpc-123abc` 和 `VPCRegion=us-east-1`。
- 上下文键和值区分大小写。

> **Important**
>
> 要获得按预期允许或限制操作的权限，您必须遵循以下约定。此条件键仅接受`VPCId`且`VPCRegion`元素，不支持任何其他 Amazon 资源 Amazon Web Services 账户，例如。

您可以使用《IAM 用户指南》中的 Access Analyzer 或 Policy Simulator 验证策略是否按预期授予或限制权限。您还可以通过将 IAM policy 应用于执行 Route 53 操作的测试用户或角色来验证权限。

指定条件：使用条件键

Amazon 为所有支持 IAM 进行访问控制的 Amazon 服务提供了一组预定义的条件键（Amazon范围内的条件键）。例如，您可以先使用 `aws:SourceIp` 条件键检查请求者的 IP 地址，然后再允许执行操作。有关更多信息和 Amazon范围条件键的列表，请参阅 IAM 用户指南中的可用条件键。

> **Note**
>
> Route 53 不支持基于标签的条件键。

下表显示了适用于 Route 53 的 Route 53 服务专属条件键。

Route 53 条件键	API 操作	值类型	说明
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	多值	表示请求中的 DNS 记录名称列表ChangeResourceRecordSets。要获得预期的行为，IAM policy 中的 DNS 名称必须标准化，如下所示： • 所有字母必须为小写形式。 • DNS 名称不得带有结尾圆点。 • 除 a 到 z、0 到 9、-（连字符）、_（下划线）和 .（句点，作为标签之间的分隔符）以

Route 53 条件键	API 操作	值类型	说明
			外的字符必须使用 \三位八进制代码格式的转义码。
route53:ChangeResourceRecordSetsRecordTypes	ChangeResourceRecordSets	多值	表示 ChangeResourceRecordSets 请求中的 DNS 记录类型列表。 ChangeResourceRecordSetsRecordTypes 可以是 Route 53 支持的任何 DNS 记录类型。有关更多信息，请参阅 支持的 DNS 记录类型。在策略中，所有内容必须以大写形式输入。
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets	多值	表示 ChangeResourceRecordSets 请求中的操作列表。 ChangeResourceRecordSetsActions 可为以下任意值（必须为大写）： • CREATE • UPSERT • DELETE

Route 53 条件键	API 操作	值类型	说明
route53:VPCs	助理VPCWithHostedZone 取消关联VPCFromHostedZone ListHostedZonesByVPC CreateHostedZone 创建VPCAssociation授权 删除VPCAssociation授权	多值	表示请求 VPCs 中AssociateVPCWithHostedZone 、、、DisassociateVPCFromHostedZone ListHostedZonesByVPC CreateHostedZone CreateVPCAssociationAuthorization 、和的列表DeleteVPCAssociationAuthorization ，格式为 “VPCId=<vpc-id>，VPCRegion= <region>

策略示例：使用条件实现精细访问

此部分中的每个示例均将 Effect 子句设置为 Allow，并且仅指定允许的操作、资源和参数。只允许访问 IAM policy 中明确列出的项目。

在某些情况下，可以重新编写这些策略以使其成为基于拒绝的策略（即将 Effect 子句设置为 Deny 并反转策略中的所有逻辑）。然而，我们建议您避免使用基于拒绝的策略，因为与基于允许的策略相比，它们难以编写正确。由于需要进行文本标准化，因此对于 Route 53 来说尤其如此。

授予权限以限制访问具有特定名称的 DNS 记录

以下权限策略授予允许对 example.com 和 marketing.example.com 的托管区 Z12345 执行 ChangeResourceRecordSets 操作的权限。它使用 route53:ChangeResourceRecordSetsNormalizedRecordNames 条件键，以限制用户仅对与指定名称匹配的记录执行操作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com", "marketing.example.com"]
                }
            }
          }
        ]
}
```

ForAllValues:StringEquals 是一个适用于多值键的 IAM 条件运算符。仅当 ChangeResourceRecordSets 中所有更改的 DNS 名称均为 example.com 时，上述策略中的条件才允许该操作。有关更多信息，请参阅《IAM 用户指南》中的 IAM 条件运算符和具有多个键或值的 IAM 条件。

要实现与具有特定后缀的名称相匹配的权限，可以在策略中使用 IAM 通配符（*）及条件运算符 StringLike 或 StringNotLike。当 ChangeResourceRecordSets 操作中所有更改的 DNS 名称均以“-beta.example.com”结尾时，以下策略将允许该操作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringLike":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["*-beta.example.com"]
                }
            }
          }
        ]
}
```

> **Note**
>
> IAM 通配符与域名通配符不同。请参阅以下示例，了解如何将通配符与域名一起使用。

授予权限，限制访问与包含通配符的域名相匹配的 DNS 记录

以下权限策略授予允许对 example.com 的托管区 Z12345 执行 ChangeResourceRecordSets 操作的权限。它使用 route53:ChangeResourceRecordSetsNormalizedRecordNames 条件键，以限制用户仅对与 *.example.com 匹配的记录执行操作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["\
\052.example.com"]
                }
            }
          }
        ]
```

```
}
```

\052 是 DNS 名称中字符 * 的八进制代码，且 \052 中的 \ 转义为 \\ 以遵循 JSON 语法。

授予权限以限制访问特定 DNS 记录

以下权限策略授予允许对 example.com 的托管区 Z12345 执行 ChangeResourceRecordSets 操作的权限。它使用三个条件键的组合来限制用户操作，只允许创建或编辑具有特定 DNS 名称和类型的 DNS 记录。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com"],
                     "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],
                     "route53:ChangeResourceRecordSetsActions": ["CREATE",
 "UPSERT"]
                }
            }
          }
        ]
}
```

授予限制访问的权限，以仅创建和编辑指定类型的 DNS 记录

以下权限策略授予允许对 example.com 的托管区 Z12345 执行 ChangeResourceRecordSets 操作的权限。它使用 route53:ChangeResourceRecordSetsRecordTypes 条件键，以限制用户仅对与指定类型匹配的记录执行操作（A 和 AAAA）。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

授予指定 IAM 主体可以在其中操作的 VPC 的权限

以下权限策略授予在 vpc-id 指定的 VPC 上允许 `AssociateVPCWithHostedZone`、`DisassociateVPCFromHostedZone`、`ListHostedZonesByVPC`、和 `DeleteVPCAssociationAuthorization` 操作的权限。

> **Important**
>
> 必须采用 `VPCId=<vpc-id>,VPCRegion=<region>` 格式提供条件值。如果在条件值中指定了 VPC ARN，则条件键不会生效。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
```

```
                "route53:*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "route53:VPCs": [
                        "VPCId=<vpc-id>,VPCRegion=<region>"
                    ]
                }
            }
        },
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcs",
            "Resource": "*"
        }
    ]
}
```

Amazon Route 53 API 权限：操作、资源和条件参考

在设置访问控制和编写可附加到 IAM 身份的权限策略（基于身份的策略）时，您可以使用 Route 53 的操作、资源和条件密钥列表、Route 53 域的操作、资源和条件密钥、 VPC 解析器的操作、资源和条件密钥以及 Amazon Route 53 配置文件允许与共享 DNS 设置的操作、资源和条件密钥列表，以及服务授权参考 VPCs中允许与共享 DNS 设置的 Amazon Route 53 配置文件的操作、资源和条件密钥列表。这些页面包括每个 Amazon Route 53 API 操作、您必须授予访问权限的操作以及必须授予访问权限的 Amazon 资源。您可以在策略的 `Action` 字段中指定这些操作，并在策略的 `Resource` 字段中指定资源值。

您可以在 Amazon Route 53 策略中使用范围的条件键来表达条件。有关 Amazon范围密钥的完整列表，请参阅 IAM 用户指南中的可用密钥。

> **Note**
>
> 授予访问权限时，托管区域和 Amazon VPC 必须属于相同分区。分区是一组 Amazon Web Services 区域。每个分区的作用域 Amazon Web Services 账户 仅限于一个分区。
> 以下是支持的分区：

- aws - Amazon Web Services 区域
- aws-cn – 中国区域
- aws-us-gov - Amazon GovCloud (US) Region

有关更多信息，请参阅《Amazon 一般参考》中的访问权限管理。

> **Note**
>
> 要指定操作，请在 API 操作名称之前使用相应前缀（route53、route53domains 或 route53resolver），例如：
>
> - route53:CreateHostedZone
> - route53domains:RegisterDomain
> - route53resolver:CreateResolverEndpoint

Amazon Route 53 中的日志记录和监控

Amazon Route 53 提供了 DNS 查询日志记录以及使用运行状况检查监控您的资源的功能。此外，Route 53 还与其他 Amazon 服务集成，以提供额外的日志记录和监控：

记录 DNS 查询

您可以配置 Route 53 以记录有关 Route 53 收到的查询的信息，例如请求的域或子域、请求的日期和时间以及 DNS 记录类型（如 A 或 AAAA）。

有关更多信息，请参阅 公有 DNS 查询日志记录。

Amazon CloudTrail 用于记录控制台和编程操作

CloudTrail 提供了用户、角色或 Amazon 服务采取的 Route 53 操作的记录。使用收集的信息 CloudTrail，您可以跟踪发出的请求、请求来源的 IP 地址、发出请求的人、发出请求的时间以及其他详细信息。有关更多信息，请参阅 使用记录亚马逊 Route 53 API 调用 Amazon CloudTrail。

监控域注册

Route 53 控制面板提供了有关您的域注册的状态的详细信息，如域转移的状态和接近到期日期的域。

有关更多信息，请参阅 监控域注册。

使用 Route 53 运行状况检查和 Amazon CloudWatch 来监控您的资源

您可以通过创建 Route 53 运行状况检查 CloudWatch 来监控您的资源，该检查用于收集原始数据并将其处理为可读的近乎实时的指标。

有关更多信息，请参阅 使用 Amazon Route 53 运行状况检查和亚马逊监控您的资源 CloudWatch。

使用亚马逊监控 Rou CloudWatch te 53 VPC 解析器终端节点

您可以使用监控 CloudWatch 解析器终端节点转发的 DNS 查询数量。

有关更多信息，请参阅 使用亚马逊监控 Route 53 VPC 解析器终端节点 CloudWatch。

使用 Amazon Trusted Advisor

Trusted Advisor 借鉴了从服务 Amazon 客户中学到的最佳实践。 Trusted Advisor 检查您的 Amazon 环境，然后在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。所有 Amazon 客户均可使用五张 Trusted Advisor 支票。拥有商业或企业支持计划的客户可以查看所有 Trusted Advisor 支票。

有关更多信息，请参阅 Trusted Advisor。

Amazon Route 53 的合规性验证

作为多项合规计划的一部分，第三方审计师对 Amazon Route 53 的安全与 Amazon 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规计划范围内的 Amazon 服务列表，请参阅按合规计划划分的范围内的Amazon 服务。有关一般信息，请参阅 Amazon 合规性计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅在 Artifac t 中 Amazon 下载报告。

您在使用 Route 53 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。如果您使用 53 号公路需要遵守 HIPAA、PCI 或 FedRAMP 等标准，请提供资源来帮助： Amazon

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 Amazon
- 设计符合 HIPAA 安全性和合规性要求的架构白皮书 — 此白皮书介绍公司如何使用 Amazon 创建符合 HIPAA 标准的应用程序。

- Amazon 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地。
- Amazon Config— 该 Amazon 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。
- Amazon Security Hub CSPM— 此 Amazon 服务可全面了解您的安全状态 Amazon ，帮助您检查是否符合安全行业标准和最佳实践。

Amazon Route 53 中的恢复功能

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

Route 53 将其功能划分为控制面板和数据面板。像大多数 Amazon 服务一样，Route 53 服务包括控制面板和数据面板；控制面板可以辅助您执行诸如创建、更新和删除资源之类的管理操作，而数据面板提供该服务核心功能。有关 Route 53 控制面板和数据面板的更多信息，请参阅 控制和数据层面概念。

Route 53 主要是一项全球服务，但以下功能支持 Amazon 区域：

- 如果您使用 Route 53 VPC 解析器设置混合配置，则可以在您选择的 Amazon 区域中创建终端节点，并在多个可用区域中指定 IP 地址。对于出站终端节点，请在您创建终端节点的同一区域中创建规则。有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。
- 您可以配置 Route 53 运行状况检查以检查您在特定区域创建的资源的运行状况，例如亚马逊 EC2 实例和 Elastic Load Balancing 负载均衡器。
- 创建用于监控终端节点的运行状况检查时，您可以选择性地指定您希望 Route 53 从中执行运行状况检查的区域。

有关 Amazon 区域和可用区的更多信息，请参阅Amazon 全球基础设施。

Amazon Route 53 中的基础设施安全性

作为一项托管服务，Amazon Route 53 受到 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及如何 Amazon 保护基础设施的信息，请参阅Amazon 云安全。要使用基础设施安全的最佳实践来设计您的 Amazon 环境，请参阅 S Amazon ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 Amazon 已发布的 API 调用通过网络访问 Route 53。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

将结果从 Resolver DNS 防火墙发送到 Security Hub CSPM

Amazon Security Hub CSPM为您提供安全状态的全面视图， Amazon 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub CSPM 从 Amazon Web Services 账户 Amazon Web Services 服务、和支持的第三方合作伙伴产品中收集安全数据，并帮助您分析安全趋势并识别优先级最高的安全问题。

通过将 Resolver DNS 防火墙与 Security Hub CSPM 集成，你可以将发现结果从 DNS 防火墙发送到 Security Hub CSPM。然后，Security Hub CSPM 将这些发现纳入其对您的安全态势的分析中。

目录

Security Hub CSPM 中的发现是如何运作的

在 Security Hub CSPM 中，调查发现是安全检查或安全相关检测的可观测记录。有些发现来自其他合作伙伴 Amazon Web Services 服务 或第三方合作伙伴发现的问题。Security Hub CSPM 也有自己的安全控制措施，用于检测安全问题并生成调查结果。

Security Hub CSPM 提供了用于管理来自所有这些来源的调查发现的工具。您可以查看和筛选调查发现列表，并查看调查发现的详细信息。有关信息，请参阅《Amazon Security Hub 用户指南》中的 “在 Sec urity Hub CSPM 中查看查找结果详情和查找历史记录”。您还可以自动更新调查发现或将其发送到自定义操作。有关更多信息，请参阅《Amazon Security Hub 用户指南》中的自动修改 Security Hub CSPM 发现结果并对其采取措施。

Security Hub CSPM 中的所有发现都使用一种称为 Amazon 安全调查结果格式 (ASFF) 的标准 JSON 格式。ASFF 包含有关安全问题根源、受影响资源以及调查发现当前状态的详细信息。有关更多信息，请参阅 Amazon Security Hub 用户指南中的 Amazon Security Finding 格式 (ASFF)。

DNS 防火墙是向 Securit Amazon Web Services 服务 y Hub CSPM 发送发现结果的防火墙之一。

DNS Firewall 发送的调查发现类型

DNS Firewall 具有以下集成：

- 托管域列表：与托 Amazon 管域列表关联的域名被阻止或提醒的查询相关的安全发现。
- 自定义域列表：对于与客户域列表关联的域，与阻止或发出提醒的查询相关的安全调查发现。
- DNS Firewall Advanced：与由 DNS Firewall Advanced 阻止或发出提醒的查询相关的安全调查发现。

Security Hub CSPM 以安全调查结果格式 (ASFF) 提取来自 DNS 防火墙的Amazon 调查结果。在 ASFF 中，Types 字段提供结果类型。来自 DNS Firewall 的调查发现可能具有 Types 的以下值。

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

在 Security Hub CSPM 不可用时重试

如果 Security Hub CSPM 不可用，DNS Firewall 会重试发送发现结果，直到收到结果。

更新 Security Hub CSPM 中的现有调查发现

如果再次观察到相同的调查发现，DNS Firewall 将更新现有调查发现。

来自 DNS Firewall 的典型调查发现

Security Hub CSPM 以安全调查结果格式 (ASFF) 提Amazon 取 DNS 防火墙调查结果。

下面是来自 DNS Firewall 的典型调查发现（采用 ASFF 格式）示例。

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "00000000-0000-0000-0000-example1",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-
resolver-dns-firewall-aws-list",
            "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
            "CompanyName": "Amazon",
            "Region": "us-east-1",
            "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-
rule-group/rslvr-frg-example1",
            "AwsAccountId": "000000000000",
            "Types": [
```

```
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ],
            "FirstObservedAt": "2024-12-06T19:58:49.000Z",
            "LastObservedAt": "2024-12-06T19:58:49.000Z",
            "CreatedAt": "2024-12-06T19:58:49.000Z",
            "UpdatedAt": "2024-12-06T19:58:49.000Z",
            "Severity": {
                "Label": "HIGH",
                "Normalized": 70
            },
            "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC
 vpc-example1",
            "Description": "DNS Firewall ALERT",
            "ProductFields": {
                "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
                "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-
example1",
                "aws/route53resolver/dnsfirewall/queryType": "A",
                "aws/route53resolver/dnsfirewall/queryClass": "IN",
                "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-
example1",
                "aws/route53resolver/dnsfirewall/transport": "UDP",
                "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
                "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
 List",
                "aws/securityhub/CompanyName": "Amazon"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "rslvr-in-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "ResourceType": "ResolverEndpoint",
                            "EndpointId": "rslvr-in-example1"
                        }
                    }
                },
                {
                    "Type": "Other",
```

```
                "Id": "rni-example1",
                "Partition": "aws",
                "Region": "us-east-1",
                "Details": {
                    "Other": {
                        "NetworkInterfaceId": "rni-example1",
                        "ResourceType": "ResolverNetworkInterface"
                    }
                }
            }
        ],
        "WorkflowState": "NEW",
        "Workflow": {
            "Status": "NEW"
        },
        "RecordState": "ACTIVE",
        "FindingProviderFields": {
            "Severity": {
                "Label": "HIGH"
            },
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ]
        },
        "ProcessedAt": "2024-12-11T19:33:35.494Z"
    }
```

启用和配置集成

要将 DNS 防火墙与 Security Hub CSPM 集成，必须先启用 Security Hub CSPM。有关启用 Security Hub CSPM 的信息，请参阅用户指南中的启用 Security Hub CSPM。Amazon Security Hub

停止向 Security Hub CSPM 传送调查结果

要停止向 Security Hub CSPM 发送 DNS 防火墙调查结果，你可以使用 Security Hub CSPM 控制台或 Security Hub CSPM API。

有关说明，请参阅 Amazon Security Hub 用户指南中的禁用集成调查发现流。

监控 Amazon Route 53

监控是维护 Amazon 解决方案可靠性、可用性和性能的重要组成部分。您应该从 Amazon 解决方案的所有部分收集监控数据，以便在出现多点故障时可以更轻松地对其进行调试。不过，在开始监控之前，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

主题

公有 DNS 查询日志记录

您可以配置 Amazon Route 53 以记录有关 Route 53 接收公有 DNS 查询的信息，如下所示：

- 请求的域名或子域名
- 请求的日期和时间
- DNS 记录类型（例如 A 或 AAAA）

- 响应 DNS 查询的 53 号路边缘站点
- DNS 响应代码，例如 NoError 或 ServFail

配置查询日志记录后，Route 53 会将日志发送到 CloudWatch 日志。您可以使用 “ CloudWatch 日志” 工具访问查询日志。

查询日志仅包含 DNS 解析程序发送到 Route 53 的查询。如果 DNS 解析程序已缓存对查询 (如 example.com 的负载均衡器的 IP 地址) 的响应，则解析程序将继续返回缓存的响应而不将查询发送到 Route 53，直到相应记录的 TTL 到期为止。

根据为域名 (example.com) 或子域名称 (www.example.com) 提交的 DNS 查询的数量、用户正在使用的解析程序以及记录的 TTL，查询日志可能只包含提交到 DNS 解析程序的数千个查询中的一个查询的信息。有关 DNS 的工作方式的更多信息，请参阅如何将 Internet 流量路由到您的网站或 Web 应用程序。

如果您不需要详细的日志信息，则可以使用 Amazon CloudWatch 指标来查看 Route 53 响应的托管区域的 DNS 查询总数。有关更多信息，请参阅 查看公有托管区域的 DNS 查询指标。

主题

为 DNS 查询配置日志记录

要开始记录指定托管区域的 DNS 查询，您需要在 Amazon Route 53 控制台中执行以下任务：

- 选择您希望 Route 53 向其发布日志的日志组，或者创建一个新的日志组。 CloudWatch

> **Note**
>
> 日志组必须位于美国东部（弗吉尼亚北部）区域。

- 选择 Create 以完成。

> **Note**
>
> 如果用户正在提交对您的域的 DNS 查询，则您会在创建查询日志配置后几分钟内开始看到日志中的查询。

为 DNS 查询配置日志记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 选择要为其配置查询日志记录的托管区域。
4. 在 Hosted zone details 窗格中，选择 Configure query logging。
5. 选择现有日志组或创建新的日志组。
6. 如果您收到有关权限的提示（如果您之前未使用新控制台配置查询日志记录，则会发生这种情况），请执行以下操作之一：
   - 如果您已经有 10 个资源策略，则无法再创建新策略。选择任何资源策略，然后选择 Edit（编辑）。编辑将授予 Route 53 向您的日志组写入日志的权限。选择保存。提示会消失，您可以继续下一步。
   - 如果您以前从未配置过查询日志记录（或者您尚未创建 10 个资源策略），则需要向 Route 53 授予将日志写入 CloudWatch 日志组的权限。选择 Grant permissions（授予权限）。提示会消失，您可以继续下一步。
7. 选择 P ermissions-可选查看一个表，该表显示资源策略是否与 CloudWatch 日志组匹配，以及 Route 53 是否有权向其发布日志 CloudWatch。
8. 选择创建。

使用 Amazon CloudWatch 访问 DNS 查询日志

Amazon Route 53 将查询 CloudWatch 日志直接发送到日志；这些日志永远无法通过 Route 53 访问。相反，您可以使用 CloudWatch 日志近乎实时地查看日志、搜索和筛选数据，以及将日志导出到 Amazon S3。

Route 53 为每个 Route 53 边缘站点创建一个 CloudWatch 日志流，用于响应指定托管区域的 DNS 查询并将查询日志发送到适用的日志流。例如，每个日志流名称的格式均为*hosted-zone-id*/*edge-location-ID*Z1D633PJN98FT9/DFW3。

例如，每个边缘位置都由三个字母的代码和一个任意分配的数字来标识。 DFW3三个字母代码通常对应邻近节点位置的机场的国际航空协会机场代码。（这些缩写将来可能会更改。）有关边缘站点的列表，请参阅 Route 53 产品详细信息页上的“Route 53 全球网络”。

> **Note**
>
> 您可能会看到一些不符合上述惯例的前缀或后缀。这些编码属性仅供内部使用。

有关更多信息，请参阅相应文档：

- Amazon CloudWatch 日志用户指南
- 亚马逊 CloudWatch 日志 API 参考
- CloudWatch 《Amazon CLI 命令参考》的“日志”部分
- 显示在 DNS 查询日志中的值

更改日志的保留周期并将日志导出到 Amazon S3

默认情况下， CloudWatch Logs 无限期存储查询日志。您可以选择指定保留期，以便 CloudWatch Logs 删除早于保留期的日志。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的“CloudWatch 日志”中的更改日志数据保留期。

如果您想保留日志数据，但不需要使用 CloudWatch 日志工具来查看和分析数据，则可以将日志导出到 Amazon S3，这样可以降低存储成本。有关更多信息，请参阅将日志数据导出至 Amazon S3。

有关定价的信息，请参阅适用的定价页：

- CloudWatch 定价页面上的“Amazon CloudWatch 日志”
- Amazon S3 定价

> **Note**
>
> 当您配置 Route 53 以记录 DNS 查询时，不会产生任何 Route 53 费用。

停止查询日志记录

如果您希望 Amazon Route 53 停止向 CloudWatch 日志发送查询日志，请执行以下步骤删除查询日志配置。

删除查询日志记录配置

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 为您要删除其查询日志记录配置的托管区域选择名称。
4. 在 Hosted zone details（托管区域详细信息）窗格中，选择 Delete query logging configuration（删除查询日志记录配置）。
5. 选择删除以确认。

显示在 DNS 查询日志中的值

每个日志文件都为 Amazon Route 53 从相应边缘站点中的 DNS 解析程序接收的每个 DNS 查询包含一个日志条目。每个日志条目都包含以下值：

日志格式版本

此查询日志的版本号。如果向日志添加字段或更改现有字段的格式，我们将增大此值。

查询时间戳

Route 53 对请求做出响应的日期和时间，采用 ISO 8601 格式和协调世界时 (UTC)，例如，`2017-03-16T19:20:25.177Z`。

有关 ISO 8601 格式的信息，请参阅维基百科文章 ISO 8601。有关 UTC 的信息，请参阅维基百科文章协调世界时。

托管区域 ID

与此日志中的所有 DNS 查询关联的托管区域的 ID。

查询名称

在请求中指定的域或子域

查询类型

在请求中指定的 DNS 记录类型，或 ANY。有关 Route 53 支持的类型的信息，请参阅 支持的 DNS 记录类型。

响应代码

Route 53 在对 DNS 查询做出的响应中返回的 DNS 响应代码。

第 4 层协议

用于提交查询的协议，即 TCP 或 UDP。

Route 53 边缘站点

对查询做出响应的 Route 53 边缘站点。例如，每个边缘位置都由三个字母的代码和一个任意数字标识。 DFW3三个字母代码通常对应邻近节点位置的机场的国际航空协会机场代码。（这些缩写将来可能会更改。）

有关边缘站点的列表，请参阅 Route 53 产品详细信息页上的“Route 53 全球网络”。

解析程序 IP 地址

向 Route 53 提交请求的 DNS 解析程序的 IP 地址。

EDNS 客户端子网

发起请求的客户端的部分 IP 地址 (如果可从 DNS 解析程序获得)。

有关更多信息，请参阅 IETF 草案 Client Subnet in DNS Requests。

查询日志示例

以下是示例查询日志（Region 是占位符）：

```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP Region 192.168.1.1
 -
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP Region
 192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP Region
 2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP Region
 192.168.3.1 192.168.111.0/24
```

```
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP Region
 192.168.1.2 -
```

Resolver 查询日志记录

您可以记录以下 DNS 查询：

- 源自您指定的 Amazon Virtual Pri VPCs vate Cloud 的查询，以及对这些 DNS 查询的响应。
- 来自使用入站 Resolver 端点的本地部署资源的查询。
- 使用出站 Resolver 端点进行递归 DNS 解析的查询。
- 使用 Resolver DNS 防火墙规则阻止、允许或监控域列表的查询。

VPC 解析器查询日志包含以下值：

- 创建 VPC 的 Amazon 区域
- 查询源自的 VPC 的 ID
- 查询源自的实例的 IP 地址
- 查询源自的资源的实例 ID
- 首次进行查询的日期和时间
- 请求的 DNS 名称（例如 prod.example.com）
- DNS 记录类型 (如 A 或 AAAA)
- DNS 响应代码，如 `NoError` 或 `ServFail`
- DNS 响应数据，如在对 DNS 查询做出的响应中返回的 IP 地址
- 对 DNS Firewall 规则操作的响应

有关记录的所有值的详细列表以及示例，请参阅 VPC 解析器查询日志中显示的值。

> **Note**
>
> 按照 DNS 解析器的标准配置，解析器将 DNS 查询缓存一段时间长度由解析器的 time-to-live (TTL) 决定。Route 53 VPC 解析器会缓存来自您的查询 VPCs，并尽可能从缓存中做出响应以加快响应速度。VPC Resolver 查询日志仅记录唯一查询，而不记录 VPC 解析器能够从缓存中响应的查询。
>
> 例如，假设其中一个 EC2 实例提交了对 accounting VPCs .example.com 的请求，该实例的查询日志配置正在记录查询。VPC Resolver 会缓存对该查询的响应，并记录查询。如果同一实

例的弹性网络接口在 VPC 解析器缓存的 TTL 内查询 accounting.example.com，则 VPC 解析器会响应来自缓存的查询。未记录第二个查询。

您可以将日志发送到以下 Amazon 资源之一：

- Amazon CloudWatch 日CloudWatch 志（日志）日志组
- Amazon S3 (S3) 存储桶
- Firehose 传输流

有关更多信息，请参阅 Amazon 您可以向其发送 VPC 解析器查询日志的资源。

主题

Amazon 您可以向其发送 VPC 解析器查询日志的资源

> **Note**
>
> 如果您希望记录具有较高每秒查询 (QPS) 的工作负载的查询，则应使用 Amazon S3 确保您的查询日志在写入目标时不会受到节流限制。如果您使用 Amazon CloudWatch，则可以提高该`PutLogEvents`操作的每秒请求次数上限。要了解有关提高 CloudWatch 限制的更多信息，请参阅 Amazon CloudWatch 用户指南中的CloudWatch 日志配额。

您可以将 VPC 解析器查询日志发送到以下 Amazon 资源：

亚马逊 CloudWatch 日志（亚马逊 CloudWatch 日志）日志组

您可以使用 Logs Insights 来分析日志并创建指标与告警。

有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。

Amazon S3 (S3) 存储桶

S3 存储桶对于长期日志归档来说非常经济。延迟通常较高。

支持所有 S3 服务器端加密选项。有关更多信息，请参阅《Amazon S3 用户指南》中的使用服务器端加密保护数据。

如果您选择使用 Amazon KMS 密钥进行服务器端加密 (SSE-KMS)，则必须更新客户托管密钥的密钥策略，以便日志传输账户可以写入您的 Amazon S3 存储桶。有关与 SSE-KMS 一起使用的所需密钥策略的更多信息，请参阅亚马逊用户指南中的 Amazon S3 存储桶服务器端加密。 CloudWatch

如果 S3 存储桶位于您拥有的账户中，则所需的权限会自动添加到您的存储桶策略中。如果要将日志发送到不属于您的账户中的 S3 存储桶，则 S3 存储桶的拥有者必须在其存储桶策略中为您的账户添加权限。例如：

JSON

```
{
    "Version":"2012-10-17",
    "Id": "CrossAccountAccess",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your_bucket_name/
AWSLogs/your_caller_account/*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
```

```
}
```

> **Note**
>
> 如果要将日志存储在组织的中央 S3 存储桶中，我们建议您从集中账户（具有写入中央存储桶的必要权限）设置查询日志记录配置，并使用 RAM 以跨账户共享配置。

有关更多信息，请参阅 Amazon Simple Storage Service 用户指南。

Firehose 传输流

您可以将日志实时流式传输到亚马逊 OpenSearch 服务、Amazon Redshift 或其他应用程序。

有关更多信息，请参阅《Amazon Data Firehose 开发人员指南》。

有关 Resolver 查询日志的定价信息，请参阅 Amazon CloudWatch 定价。

CloudWatch 使用 VPC 解析器日志时，即使日志直接发布到 Amazon S3，也会收取销售日志费用。有关更多信息，请参阅按照 Amazon 定价的日志 CloudWatch 定价。

管理 Resolver 查询日志记录配置

配置（VPC 解析器查询日志）

您可以通过两种方式配置 VPC 解析器查询日志：

- 直接 VPC 关联- VPCs 直接关联到查询日志配置。
- 配置@@ 文件关联-将查询日志配置关联到 Route 53 配置文件，这会将日志记录应用于与该配置文件 VPCs关联的所有配置。有关更多信息，请参阅 将 VPC 解析器查询日志配置关联到 Route 53 配置文件。

要开始记录源自您的 DNS 查询 VPCs，请在 Amazon Route 53 控制台中执行以下任务：

要配置 Resolver 查询日志记录

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

2. 展开 Route 53 控制台菜单。在控制台的左上角，选择三个水平条

   （ ☰ ）

   图标。

3. 在 Resolver 菜单中，选择 Query logging（查询日志记录）。

4. 在区域选择器中，选择要在其中创建查询日志配置的 Amazon 区域。该区域必须与您创建要记录 DNS 查询的区域相同。 VPCs 如果您有 VPCs 多个区域，则必须为每个区域创建至少一个查询日志配置。

5. 选择 Configure query logging（配置查询日志记录）。

6. 指定以下值：

   查询日志记录配置名称

   为查询日志记录配置输入名称。名称会显示在控制台的查询日志配置列表中。输入名称将有助于以后查找此配置。

   查询日志的目标保存位置

   选择您希望 VPC 解析器向其发送查询日志的 Amazon 资源类型。有关如何在选项（CloudWatch 日志组、S3 存储桶和 Firehose 传输流）中进行选择的信息，请参阅。Amazon 您可以向其发送 VPC 解析器查询日志的资源

   选择资源类型后，您可以创建该类型的另一个资源，也可以选择由当前 Amazon 账户创建的现有资源。

   > **Note**
   >
   > 您只能选择在步骤 4 选择的 Amazon 区域中创建的资源，也即您创建查询日志记录配置的区域。如果您选择创建新资源，则该资源将在同一区域创建。

   VPCs 记录以下各项的查询

   此查询日志配置将记录源自您选择的 DNS 查询。 VPCs 选中当前区域中您希望 VPC 解析器记录查询的每个 VPC 的复选框，然后选择选择。

   备选方案：您可以将此查询日志配置关联到 Route 53 配置文件，这样可以将日志记录应用于与该配置文件 VPCs关联的所有配置，而不是 VPCs 直接关联。有关更多信息，请参阅 将 VPC 解析器查询日志配置关联到 Route 53 配置文件。

> **Note**
>
> 对于特定目标类型，VPC 日志传输只能启用一次。日志无法传送到同一类型的多个目标，例如，VPC 日志无法传送到 2 个 Amazon S3 目标。

7. 选择 Configure query logging（配置查询日志记录）。

> **Note**
>
> 您应在成功创建查询日志配置后数分钟内开始在日志中看到 VPC 中的资源执行的 DNS 查询。

VPC 解析器查询日志中显示的值

每个日志文件都为 Amazon Route 53 从相应边缘站点中的 DNS 解析程序接收的每个 DNS 查询包含一个日志条目。每个日志条目都包含以下值：

版本

此查询日志格式的版本号。当前版本为 `1.1`。

版本值包含 **`major_version.minor_version`** 格式的主要版本和次要版本。例如，您可以具有为 `1.7` 的 `version` 值，其中，`1` 是主要版本，`7` 是次要版本。

如果 Route 53 对不向后兼容的日志结构进行更改，则主要版本将递增。这包括删除已存在的 JSON 字段，或更改字段内容的表示方式（例如，日期格式）。

如果更改将新字段添加到日志文件中，则 Route 53 会增加次要版本。如果新信息可用于 VPC 中的部分或所有现有 DNS 查询，则可能会发生这种情况。

account_id

创建 VPC 的 Amazon 账户的 ID。

region

您创建 VPC 的 Amazon 区域。

vpc_id

查询源自的 VPC 的 ID。

query_timestamp

提交查询的日期和时间，采用 ISO 8601 格式和协调世界时 (UTC)，例如，2017-03-16T19:20:17Z。

有关 ISO 8601 格式的信息，请参阅维基百科文章 ISO 8601。有关 UTC 的信息，请参阅维基百科文章协调世界时。

query_name

查询中指定的域名 (example.com) 或子域名 (www.example.com)。

query_type

在请求中指定的 DNS 记录类型，或 ANY。有关 Route 53 支持的类型的信息，请参阅 支持的 DNS 记录类型。

query_class

查询的类。

rcode

VPC 解析器在响应 DNS 查询时返回的 DNS 响应代码。此响应代码表示查询是否有效。最常见的响应代码是 NOERROR，表示查询有效。如果响应无效，则 Resolver 会返回响应代码，该代码可解释无效的原因。有关可能的响应代码列表，请参阅 IANA RCODEs 网站上的 DNS。

answer_type

VPC 解析器为响应查询而返回的值的 DNS 记录类型（例如 A、MX 或 CNAME）。有关 Route 53 支持的类型的信息，请参阅 支持的 DNS 记录类型。

rdata

VPC 解析器在响应查询时返回的值。例如，对于 A 记录，这是 IPv4 格式化的 IP 地址。对于别名记录，这是别名记录中的域名。

answer_class

VPC 解析器对查询的响应的类别。

srcaddr

查询源自的主机的 IP 地址。

srcport

查询源自的实例上的端口。

transport

用于提交 DNS 查询的协议。

srcids

IDs `instance`、`resolver_endpoint`、和 DNS 查询源自或通过的。`resolver_network_interface`

实例

查询源自的实例的 ID。

> **Note**
>
> 如果您在 Route 53 VPC 解析器查询日志中看到的实例 ID 在您的账户中不可见，则可能是因为 DNS 查询来自您使用的 Amazon EKS 或 Fargate 控制台。 Amazon CloudShell Amazon Lambda

resolver_endpoint

将 DNS 查询传递到本地部署 DNS 服务器的解析程序端点的 ID。

> **Note**
>
> 如果您的 CNAME 记录通过不同的解析程序端点跨越不同的转发规则进行链接，则查询日志仅显示链中使用的最后一个解析程序端点的 ID。要通过多个端点跟踪完整的解析路径，您可以关联不同查询日志记录配置中的日志。

firewall_rule_group_id

查询中与域名匹配的 DNS Firewall 规则组 ID。仅当 DNS Firewall 找到与操作设置为提示或阻止的规则匹配时，才会填充此选项。

有关防火墙规则组更多信息，请参阅 DNS Firewall 规则组和规则。

firewall_rule_action

查询中与域名匹配的规则指定的操作。仅当 DNS Firewall 找到与操作设置为提示或阻止的规则匹配时，才会填充此选项。

firewall_domain_list_id

查询中与域名匹配的规则使用的域列表。仅当 DNS Firewall 找到与操作设置为提示或阻止的规则匹配时，才会填充此选项。

additional_properties

日志传送事件的其他信息。is_delayed：日志的传送是否出现延迟。

Route 53 VPC 解析器查询日志示例

以下是一个解析程序查询日志示例：

```
    {
      "srcaddr": "4.5.64.102",
      "vpc_id": "vpc-7example",
      "answers": [
          {
              "Rdata": "203.0.113.9",
              "Type": "PTR",
              "Class": "IN"
          }
      ],
      "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
      "firewall_rule_action": "BLOCK",
      "query_name": "15.3.4.32.in-addr.arpa.",
      "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
      "query_class": "IN",
      "srcids": {
          "instance": "i-0d15cd0d3example"
      },
      "rcode": "NOERROR",
      "query_type": "PTR",
      "transport": "UDP",
      "version": "1.100000",
      "account_id": "111122223333",
      "srcport": "56067",
      "query_timestamp": "2021-02-04T17:51:55Z",
      "region": "us-east-1"
  }
```

与其他 Amazon 账户共享 Resolver 查询日志配置

您可以与其他账户共享您使用一个 Amazon 账户创建的查询日志配置。 Amazon 为了共享配置，Route 53 VPC Resolver 控制台与 Amazon 资源访问管理器集成。有关 Resource Access Manager 的更多信息，请参阅 Resource Access Manager 用户指南。

注意以下几点：

VPCs 与共享查询日志配置关联

如果另一个 Amazon 账户与您的账户共享了一个或多个配置，则您可以像 VPCs 关联您创建的配置一样 VPCs 与该配置关联。

删除或取消共享配置

如果您与其他账户共享配置，然后删除该配置或停止共享该配置，并且如果有一个或多个账户与该配置相关联，则 Route 53 VPC Resolver 将停止记录源自 VPCs 这些账户的 DNS 查询。 VPCs

可以与配置关联的查询日志配置的最大数量 VPCs

当一个账户创建配置并与一个或多个其他账户共享配置时，每个账户将应用可与该配置关联的最大数量。 VPCs 例如，如果您的组织中有 10,000 个帐户，则可以在中央账户中创建查询日志配置并通过共享该配置将其共享 Amazon RAM 给组织帐户。然后，组织账户会将该配置与其账户的查询日志配置 VPC 关联进行 VPCs 计数，每个 Amazon Web Services 区域 限制为 100。但是，如果所有账户 VPCs 都在一个账户中，则可能需要提高该账户的服务限制。

有关当前 VPC 解析器配额，请参阅Route 53 VPC 解析器的配额。

Permissions

要与其他 Amazon 账户共享规则，您必须拥有使用该PutResolverQueryLogConfigPolicy操作的权限。

对与之共享规则的 Amazon 账户的限制

与其共享了规则的账户无法更改或删除该规则。

标签

只有创建规则的账户可以添加、删除或查看规则上的标签。

要查看规则当前的共享状态（包括共享规则的账户或与其共享了规则的账户），以及将规则与其他账户共享，请执行以下步骤。

要查看共享状态并将查询日志记录配置与其它 Amazon 账户共享

1. 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Query Logging（查询日志记录）。
3. 在导航栏上，选择您在其中创建了规则的区域。

   Sharing status (共享状态) 列显示当前账户所创建规则或者与当前账户所共享规则的当前共享状态。

   - 未共享：当前 Amazon 账户创建了规则，但该规则未与任何其他账户共享。
   - Shared by me (由我共享)：当前账户创建的规则并且已与一个或多个账户共享。
   - Shared With me (与我共享)：其他账户创建的规则并且已与当前账户共享。
4. 选择您要显示共享信息或者您要与其他账户共享的规则的名称。

   在 “规则:*rule name*” 页面上，“所有者” 下的值显示创建规则的账户的 ID。除非 Sharing status (共享状态) 的值为 Shared with me (与我共享)，否则这是当前账户。如果是共享的规则，则 Owner (所有者) 是创建该规则并与当前账户进行共享的账户。

   还会显示共享状态。
5. 选择共享配置以打开 Amazon RAM 控制台
6. 要创建资源共享，请按照《Amazon RAM 用户指南》中的在 Amazon RAM中创建资源共享的步骤操作。

> **Note**
>
> 您无法更新共享设置。如果想要更改任何以下设置，您必须使用新设置重新共享规则，然后删除旧的共享设置。

监控域注册

Amazon Route 53 控制面板提供有关域注册状态的详细信息，包括：

- 新域注册的状态
- 向 Route 53 进行域转移的状态
- 临近到期日期的域的列表

建议您定期检查 Route 53 控制台中的控制面板（尤其是在注册新域或向 Route 53 转移域之后），以确认没有需要处理的问题。

我们还建议您确认域的联系人信息是最新的。当域到期日期临近时，我们会向域的注册联系人发送电子邮件，其中包含有关域到期时间和续订方法的信息。

使用 Amazon Route 53 运行状况检查和亚马逊监控您的资源 CloudWatch

您可以通过创建 Amazon Route 53 运行状况检查 CloudWatch 来监控您的资源，该检查用于收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存两周，以便您访问历史信息并更好地了解资源的运行情况。默认情况下，Route 53 运行状况检查的指标数据每隔 CloudWatch 一分钟自动发送到。

有关 Route 53 运行状况检查的详细信息，请参阅 使用 CloudWatch 监控运行状况检查。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。

Route 53 运行状况检查的指标和维度

当您创建运行状况检查时，Amazon Route 53 开始每 CloudWatch 分钟向您指定的资源发送一次指标和维度。通过 Route 53 控制台可以查看运行状况检查的状态。您也可以使用以下过程在 CloudWatch 控制台中查看指标或使用 Amazon Command Line Interface (Amazon CLI) 查看这些指标。

使用 CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Metrics (指标)。
3. 在 All Metrics 选项卡上，选择 Route 53。
4. 选择 Health Check Metrics (运行状况检查指标)。

要查看指标，请使用 Amazon CLI

- 在命令提示符处输入下面的命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

主题

CloudWatch Route 53 运行状况检查的指标

AWS/Route53 命名空间包括 Route 53 运行状况检查的以下指标。

ChildHealthCheckHealthyCount

对于计算的运行状况检查，状况良好的运行状况检查的数量。

有效统计数据：Average（推荐）、Minimum、Maximum

单位：计数

ConnectionTime

Route 53 运行状况检查程序与端点建立 TCP 连接所用的平均时间（毫秒）。您可以跨所有区域或针对一个选定地理区域查看 ConnectionTime 的运行状况检查。

有效统计数据：Average（推荐）、Minimum、Maximum

单位：毫秒

HealthCheckPercentageHealthy

将所选端点视为运行状况良好的 Route 53 运行状况检查程序的百分比。

有效统计数据：Average、Minimum、Maximum

单位：百分比

HealthCheckStatus

正在检查的运行状况检查端点 CloudWatch 的状态。 1 表示健康，0 表示不健康。

有效统计数据：Minimum、Average 和 Maximum

单位：无

SSLHandshake时间

Route 53 运行状况检查程序完成 SSL 握手所用的平均时间（毫秒）。您可以跨所有区域或针对一个选定地理区域查看 SSLHandshakeTime 的运行状况检查。

有效统计数据：Average（推荐）、Minimum、Maximum

单位：毫秒

TimeToFirstByte

Route 53 运行状况检查程序接收响应 HTTP 或 HTTPS 请求的第一个字节所用的平均时间（毫秒）。您可以跨所有区域或针对一个选定地理区域查看 TimeToFirstByte 的运行状况检查。

有效统计数据：Average（推荐）、Minimum、Maximum

单位：毫秒

Route 53 运行状况检查指标的维度

Route 53 运行状况检查指标使用 AWS/Route53 命名空间并提供了 HealthCheckId 的指标。在检索指标时，您必须提供 HealthCheckId 维度。

此外，对于 ConnectionTime、SSLHandshakeTime 和 TimeToFirstByte，您可以选择指定 Region。如果省略Region，则 CloudWatch 返回所有地区的指标。如果包含Region，则仅 CloudWatch 返回指定区域的指标。

有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

使用 Amazon 监控托管区域 CloudWatch

您可以使用 Amazon 收集原始数据并将其处理 CloudWatch 为可读的近乎实时的指标，从而监控您的公共托管区域。在 Route 53 收到指标所依据的 DNS 查询后不久即可获得指标。 CloudWatch Route 53 托管区域的指标数据的粒度为一分钟。

有关更多信息，请参阅以下文档

- 有关如何在 Amazon CloudWatch 控制台中查看指标以及如何使用 Amazon Command Line Interface (Amazon CLI) 检索指标的概述和信息，请参阅 查看公有托管区域的 DNS 查询指标
- 有关指标保留期限的信息，请参阅 Amazon CloudWatch API 参考GetMetricStatistics中的。
- 有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。
- 有关 CloudWatch 指标的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 指标。

主题

CloudWatch Route 53 公共托管区域的指标

AWS/Route53 命名空间包含 Route 53 托管区的以下指标：

DNSQueries

对于托管区，Route 53 在指定时间段内响应的 DNS 查询数。

有效统计数据：总和， SampleCount

单位：计数

区域：Route 53 是一项全球性服务。要获取托管区域指标，您必须为区域指定美国东部（弗吉尼亚北部）。

DNSSECInternal失败

如果托管区域中的任何对象处于 INTERNAL_FAILURE 状态，则值为 1。否则，值为 0。

有效统计数据：Sum

单位：计数

卷：每个托管区每 4 小时 1 个

区域：Route 53 是一项全球性服务。要获取托管区域指标，您必须为区域指定美国东部（弗吉尼亚北部）。

DNSSECKeySigningKeysNeedingAction

处于 ACTION_NEEDED 状态的密钥签名密钥 (KSKs) 的数量（由于 KMS 故障）。

有效统计数据：总和， SampleCount

单位：计数

卷：每个托管区每 4 小时 1 个

区域：Route 53 是一项全球性服务。要获取托管区域指标，您必须为区域指定美国东部（弗吉尼亚北部）。

DNSSECKeySigningKeyMaxNeedingActionAge

密钥签名密钥 (KSK) 设置为 ACTION_NEEDED 状态后已过去的时间。

有效统计数据：Maximum

单位：秒

卷：每个托管区每 4 小时 1 个

区域：Route 53 是一项全球性服务。要获取托管区域指标，您必须为区域指定美国东部（弗吉尼亚北部）。

DNSSECKeySigningKeyAge

自创建密钥签名密钥 (KSK) 以来（而非自激活以来）所经过的时间。

有效统计数据：Maximum

单位：秒

卷：每个托管区每 4 小时 1 个

区域：Route 53 是一项全球性服务。要获取托管区域指标，您必须为区域指定美国东部（弗吉尼亚北部）。

CloudWatch Route 53 公共托管区域指标的维度

托管区域的 Route 53 指标使用 `AWS/Route53` 命名空间并提供了 `HostedZoneId` 的指标。要获取 DNS 查询数量，您必须在 `HostedZoneId` 维度中指定托管区域的 ID。

使用亚马逊监控 Route 53 VPC 解析器终端节点 CloudWatch

您可以使用 Amazon CloudWatch 来监控由 Route 53 VPC 解析器终端节点转发的 DNS 查询数量。Amazon CloudWatch 收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存两周，以便您访问历史信息并更好地了解资源的运行情况。默认情况下，Resolver 端点的指标数据每隔五分钟自动发送 CloudWatch一次。五分钟间隔也是可以发送指标数据的最小间隔。

有关 VPC 解析器的更多信息，请参阅什么是 Route 53 VPC 解析器？。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。

Route 53 VPC 解析器的指标和维度

当您配置 VPC Resolver 以将 DNS 查询转发到您的网络，反之亦然时，VPC 解析器开始每五分钟发送一次指标和维度， CloudWatch 大约与转发的查询数量相同。您可以使用以下过程在 CloudWatch 控制台中查看指标或使用 Amazon Command Line Interface (Amazon CLI) 查看这些指标。

使用控制台查看 VPC 解析器 CloudWatch 指标

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航栏上，选择您在其中创建了端点的区域。
3. 在导航窗格中，选择指标。
4. 在全部指标选项卡上，选择 Route 53 Resolver (Route 53 解析程序)。
5. 选择 By Endpoint (按端点) 以查看指定端点的查询计数。然后，选择您想要查看其查询数的端点。

   选择 “跨所有终端节点” 可查看当前 Amazon 账户创建的所有入站终端节点或所有出站终端节点的查询计数。然后选择InboundQueryVolume或OutboundQueryVolume查看所需的计数。

要查看指标，请使用 Amazon CLI

- 在命令提示符处输入下面的命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

主题

- CloudWatch Route 53 VPC 解析器的基本指标
- CloudWatch Route 53 VPC 解析器的详细指标
- Route 53 VPC 解析器指标的维度

CloudWatch Route 53 VPC 解析器的基本指标

`AWS/Route53Resolver`命名空间包括免费的 Route 53 VPC 解析器终端节点和 IP 地址的基本指标。

主题

Route 53 VPC 解析器终端节点的指标

AWS/Route53Resolver命名空间包括 Route 53 VPC 解析器终端节点的以下指标。

EndpointHealthyENICount

处于 OPERATIONAL 状态的弹性网络接口数。这表示此端点（由 EndpointId 指定）的 Amazon VPC 网络接口配置正确，并能够在您的网络和 Resolver 之间传递入站和出站 DNS 查询。

有效统计数据：最小值、最大值、平均值

单位：计数

EndpointUnhealthyENICount

处于 AUTO_RECOVERING 状态的弹性网络接口数。

这意味着解析程序正在尝试恢复一个或多个与端点关联的 Amazon VPC 网络接口（由 EndpointId 指定）。在恢复过程中，端点会工作但容量受限，并且在完全恢复之前无法处理 DNS 查询。

有效统计数据：最小值、最大值、平均值

单位：计数

InboundQueryVolume

对于入站终端节点，指 VPCs 通过指定的终端节点从您的网络转发到您的网络的 DNS 查询数量EndpointId。

有效统计数据：Sum

单位：计数

OutboundQueryVolume

对于出站终端节点，指通过指定的终端节点从您转发 VPCs 到您的网络的 DNS 查询数量EndpointId。

有效统计数据：Sum

单位：计数

OutboundQueryAggregateVolume

对于出站终端节点，指从 Amazon 转发 VPCs 到您的网络的 DNS 查询总数，包括以下内容：

- 通过由指定的终端节点从您的网络转发 VPCs 到您的网络的 DNS 查询数量`EndpointId`。
- 当当前账户与其他账户共享 Resolver 规则时 VPCs ，由其他账户创建的查询将通过`EndpointId`指定的终端节点转发到您的网络。

有效统计数据：Sum

单位：计数

ResolverEndpointCapacityStatus

Resolver 端点的容量状态。该指标表示当前的容量利用率状态，其中：0 = 正常（正常运行容量），1 = 警告（至少有一个弹性网络接口的容量利用率超过 50%），2 = 严重（至少有一个弹性网络接口的容量利用率超过 75%）。

容量状态由多个因素决定，包括查询量、查询延迟、DNS 协议、DNS 数据包大小和连接跟踪状态。

有效统计数据：Maximum

单位：无

VPC 解析器终端节点容量管理的最佳实践

为解决容量问题，我们通常建议您增加 Resolver 端点的弹性网络接口数量。但是，以下是针对特定端点类型的重要注意事项：

对于入站端点，流量负载平衡取决于客户。因此，容量警告或严重提醒可能表示存在一个“热点”，其中一部分弹性网络接口的利用率不成比例。

- 要确定潜在的负载平衡问题，请分别检查每个 elastic network interface 的InboundQueryVolume指标。

对于出站端点，流量将在弹性网络接口之间自动平衡。容量问题可能是由于目标名称服务器出现问题，也可能是由于高延迟的超时查询使 Resolver 网络接口不堪重负。

- 在这些情况下，仅仅增加弹性网络接口数量可能没有效果，此时我们建议修复目标名称服务器。

Route 53 VPC 解析器 IP 地址的指标

AWS/Route53Resolver 命名空间包括与 Resolver 入站或出站端点关联的每个 IP 地址的以下指标。（当您指定终端节点时，VPC 解析器会创建一个 Amazon VPC 弹性网络接口。）

InboundQueryVolume

对于入站端点的每个 IP 地址，从您的网络转发到指定 IP 地址的 DNS 查询数。每个 IP 地址都由 IP 地址 ID 标识。您可以使用 Route 53 控制台获取此值。在适用端点的页面上，在“IP 地址”部分中参阅 IP address ID (IP 地址 ID) 列。您也可以使用ListResolverEndpointIpAddresses以编程方式获取值。

有效统计数据：Sum

单位：计数

OutboundQueryAggregateVolume

对于您的出站终端节点的每个 IP 地址，从亚马逊转发 VPCs 到您的网络的 DNS 查询总数，包括以下内容：

- 使用指定 IP 地址从您的网络转发 VPCs 到您的网络的 DNS 查询数量。
- 当当前账户与其他账户共享 Resolver 规则时 VPCs ，来自这些规则的查询由其他账户创建，然后使用指定的 IP 地址转发到您的网络。

每个 IP 地址都由 IP 地址 ID 标识。您可以使用 Route 53 控制台获取此值。在适用端点的页面上，在“IP 地址”部分中参阅 IP address ID (IP 地址 ID) 列。您也可以使用ListResolverEndpointIpAddresses以编程方式获取值。

有效统计数据：Sum

单位：计数

CloudWatch Route 53 VPC 解析器的详细指标

Route 53 VPC Resolver 提供 RNI 增强版和目标名称服务器指标作为终端节点的选择加入功能。这些指标每隔 1 分钟发送 CloudWatch 一次。

> **Note**
>
> - 默认情况下，详细指标未启用，但可以在终端节点级别启用。这些指标可以在使用 RniEnhancedMetricsEnabled 和 TargetNameServerMetricsEnabled

标志创建或更新端点时以编程方式启用。有关更多信息，请参阅CreateResolverEndpoint和UpdateResolverEndpoint。

- 使用 Route 53 Resolver 终端节点详细指标需支付标准 CloudWatch 定价和费用。有关更多信息，请参阅 Amazon CloudWatch 定价。

主题

RNI 增强指标

Route 53 Resolver 向亚马逊发布了 RNI 增强指标， CloudWatch 用于监控解析器终端节点和解析器 IP 地址的性能和运行状况。`AWS/Route53Resolver`命名空间包括以下 Route 53 Resolver 入站和出站终端节点的 RNI 增强指标`EndpointId`，`RniId`维度：

P90 ResponseTime

与解析器终端节点 (`RniId`) 关联的解析器 IP () 收到的 DNS 查询的响应延迟百分位数 () `EndpointId`

有效统计数据：Maximum

单位：微秒

ServFailQueries

发送到与解析器终端节点关联的解析器 IP (`RniId`) 的 DNS 查询的 SERVFAIL 响应数 () `EndpointId`

有效统计数据：Sum

单位：计数

NxDomainQueries

发送到与解析器终端节点关联的解析器 IP (`RniId`) 的 DNS 查询的 NXDOMAIN 响应数量 () `EndpointId`

有效统计数据：Sum

单位：计数

RefusedQueries

发送到与解析器终端节点关联的解析器 IP (RniId) 的 DNS 查询的拒绝响应数 () EndpointId

有效统计数据：Sum

单位：计数

FormErrorQueries

发送到与解析器终端节点关联的解析器 IP (RniId) 的 DNS 查询的 FORMERR 响应数 () EndpointId

有效统计数据：Sum

单位：计数

TimeoutQueries

发送到与解析器终端节点关联的解析器 IP (RniId) 的 DNS 查询的超时次数 () EndpointId

有效统计数据：Sum

单位：计数

目标名称服务器指标

Route 53 Resolver 向 Amazon 发布目标名称服务器指标， CloudWatch 用于监控与解析器终端节点关联的目标名称服务器的性能和可用性。AWS/Route53Resolver命名空间包含 Route 53 Resolver 出站终端节点的以下详细指标EndpointID，TargetNameServerIP维度：

P90 ResponseTime

通过解析器端点发送的 DNS 查询的目标域名服务器 IP (TargetNameServerIP) 的响应延迟 () 的第 90 个百分位数 () EndpointID

有效统计数据：Maximum

单位：微秒

RequestQueries

通过解析器端点 () 发送到目标名称服务器 IP (TargetNameServerIP) 的 DNS 查询数。EndpointID

有效统计数据：Sum

单位：计数

TimeoutQueries

通过解析器端点 (EndpointID) 发送的、在目标名称服务器 IP (TargetNameServerIP) 处超时的 DNS 查询数。

有效统计数据：Sum

单位：计数

> **Note**
>
> 在某些情况下，可能会在 VPC 解析器指标 (ResolverEndpointCapacityStatus) 和 RNI 增强型指标中观察到差距。当您的网络接口连续进行定期维护或更新时，可能会出现这些差距。将网络接口返回服务后，我们的服务至少需要 1 分钟才能收集运营数据并发布这些指标。这些差距并不表示您的 VPC 解析器终端节点出现故障。如果您要为这些指标配置 CloudWatch 警报，我们建议您采取以下措施：
>
> - 将警报设置为 “将丢失的数据视为忽略”，或者
> - 将报警阈值的评估期配置为超过五分钟。
>
> 这些设置将有助于减少正常维护活动期间的错误警报。

Route 53 VPC 解析器指标的维度

入站和出站终端节点的 Route 53 VPC 解析器指标使用AWS/Route53Resolver命名空间并提供以下维度的指标：

- EndpointId：如果您为EndpointId维度指定值，则 CloudWatch 返回指定终端节点的 DNS 查询次数。如果您未指定EndpointId，则 CloudWatch 返回当前 Amazon 账户为所有终端节点创建的 DNS 查询次数。
- RniIdOutboundQueryAggregateVolume和InboundQueryVolume指标支持维度。
- EndpointId、、、P90ResponseTimeServFailQueriesNxDomainQueriesRefusedQueriesFormE和与解析器端点关联TimeoutQueries的解析器 IP 地址支持RniId维度。
- EndpointIDP90ResponseTimeRequestQueries、和与解析器端点关联TimeoutQueries的目标名称服务器支持TargetNameServerIP维度。

使用 Amazon 监控解析器 DNS 防火墙规则组 CloudWatch

您可以使用 Amazon CloudWatch 来监控由解析器 DNS 防火墙规则组筛选的 DNS 查询数量。Amazon CloudWatch 收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存两周，以便您访问历史信息并更好地了解资源的运行情况。默认情况下，DNS 防火墙规则组的指标数据每隔五分钟自动发送 CloudWatch 一次。

有关 DNS Firewall 的更多信息，请参阅 使用 DNS Firewall 筛选出站 DNS 流量。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。

解析器 DNS 防火墙的指标和维度

当您将解析器 DNS 防火墙规则组与 VPC 关联以过滤 DNS 查询时，DNS 防火墙开始每 5 分钟向 CloudWatch 其筛选的查询发送一次指标和维度。有关 DNS Firewall 的指标和维度的信息，请参阅 CloudWatch 解析器 DNS 防火墙的指标。

您可以使用以下过程在 CloudWatch 控制台中查看指标或使用 Amazon Command Line Interface (Amazon CLI) 查看这些指标。

使用 CloudWatch 控制台查看 DNS 防火墙指标

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航栏上，选择要查看的区域。
3. 在导航窗格中，选择指标。
4. 在所有指标选项卡上，选择 Route 53 VPC 解析器。
5. 选择您感兴趣的指标。

要查看指标，请使用 Amazon CLI

- 在命令提示符处输入下面的命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

主题

- CloudWatch 解析器 DNS 防火墙的指标

CloudWatch 解析器 DNS 防火墙的指标

AWS/Route53Resolver命名空间包括解析器 DNS 防火墙规则组的指标。

主题

解析器 DNS 防火墙规则组的指标

FirewallRuleGroupQueryVolume

与防火墙规则组（由 FirewallRuleGroupId 指定）匹配的 DNS Firewall 查询数。

维度：FirewallRuleGroupId

有效统计数据：Sum

单位：计数

的指标 VPCs

VpcFirewallQueryVolume

来自 VPC（由 VpcId 指定）的 DNS Firewall 查询数。

维度：VpcId

有效统计数据：Sum

单位：计数

防火墙规则组和 VPC 关联的指标

FirewallRuleGroupVpcQueryVolume

与防火墙规则组（由 FirewallRuleGroupId 指定）匹配且来自 VPC（由 VpcId 指定）的 DNS Firewall 查询数。

维度：FirewallRuleGroupId, VpcId

有效统计数据：Sum

单位：计数

防火墙规则组中域列表的指标

FirewallRuleQueryVolume

与防火墙规则组（由 FirewallRuleGroupId 指定）中的防火墙域列表（（由 FirewallDomainListId 指定））匹配的 DNS 防火墙查询数。

维度：FirewallRuleGroupId, FirewallDomainListId

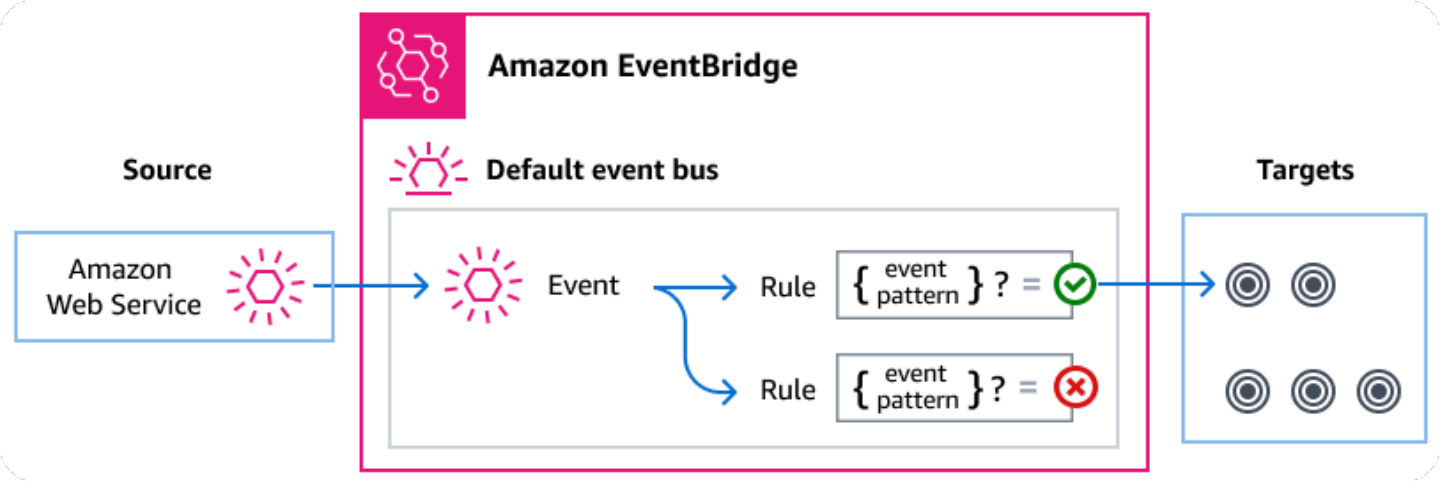
有效统计数据：Sum

单位：计数

使用管理解析器 DNS 防火墙事件 Amazon EventBridge

Amazon EventBridge 是一项无服务器服务，它使用事件将应用程序组件连接在一起，使您可以更轻松地构建可扩展的事件驱动应用程序。事件驱动型架构是一种构建松耦合软件系统的风格，这些系统通过发出和响应事件 来协同工作。事件代表资源或环境中的变化。

与许多 Amazon 服务一样，DNS Firewall 生成事件并将其发送到 EventBridge 默认事件总线。（默认事件总线会在每个 Amazon 账户中自动预置。）事件总线是接收事件并将其传送到零个或多个目的地或目标的路由器。为事件总线指定的规则会在事件到达时进行评估。每条规则都会检查事件是否与规则的事件模式相匹配。如果事件确实匹配，事件总线会将事件发送到指定的目标。



主题

解析器 DNS 防火墙事件

VPC 解析器会自动将 DNS 防火墙事件发送到默认 EventBridge 事件总线。可以在事件总线上创建规则；每个规则都包括一个事件模式以及一个或多个目标。与规则的事件模式相匹配的事件会尽力传送给指定的目标。事件可能不按顺序传送。

以下事件由 DNS Firewall 生成。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 EventBridge。

事件详细信息类型	说明
DNS Firewall 阻止	对域执行的任何阻止操作。
DNS Firewall 警报	对域执行的任何警报操作。

使用 EventBridge 规则发送解析器 DNS 防火墙事件

要让 EventBridge 默认事件总线向目标发送 DNS 防火墙事件，必须创建一个规则，其中包含与所需 DNS 防火墙事件中的数据匹配的事件模式。

创建规则包含以下一般步骤：

1. 为指定的规则创建事件模式：
   - VPC 解析器是规则评估的事件来源。
   - （可选）：要匹配的任何其他事件数据。

   有关更多信息，请参阅 ???。
2. （可选）：创建输入转换器，在将信息 EventBridge 传递给规则目标之前，对事件中的数据进行自定义。

有关更多信息，请参阅《EventBridge 用户指南》中的输入转换。

3. 指定要 EventBridge 向其发送与事件模式匹配的事件的目标。

   目标可以是其他 Amazon 服务、 software-as-a-service (SaaS) 应用程序、API 目标或其他自定义终端节点。有关更多信息，请参阅 EventBridge 用户指南中的目标。

有关创建事件总线规则的全面说明，请参阅《EventBridge 用户指南》中的创建对事件作出反应的规则。

为解析器 DNS 防火墙事件创建事件模式

当 DNS Firewall 将事件传送到默认事件总线时，会 EventBridge 使用为每条规则定义的事件模式来确定是否应将事件传送到规则的目标。事件模式与所需 DNS Firewall 事件中的数据相匹配。每个事件模式是一个 JSON 对象，其中包含：

- 标识发送事件的服务的 `source` 属性。对于 DNS Firewall 事件，其源为 `aws.route53resolver`。
- （可选）：包含要匹配的事件类型数组的 `detail-type` 属性。
- （可选）：包含要匹配的其他事件数据的 `detail` 属性。

例如，以下事件模式与来自 DNS Firewall 的警报和阻止事件相匹配：

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

虽然以下事件模式与 BLOCK 操作相匹配：

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS Firewall 在 6 小时内仅为同一个域发送一次相同的事件。例如：

1. 实例 i-123 在 T1 时间发送了 exampledomain.com 的 DNS 查询。DNS Firewall 在首次发生时发送了警报或阻止事件。

2. 实例 i-123 在 T1+30 分钟内发送了一 DNSquery 个 exampledomain.com。DNS Firewall 未发送警报或阻止事件，因为这是在 6 小时内重复发生的。
3. 实例 i-123 在 T1+7 小时的时间发送了 exampledomain.com 的 DNS 查询。DNS Firewall 发送了警报或阻止事件，因为这是在 6 小时之外发生的。

有关写入事件模式的更多信息，请参阅《EventBridge 用户指南》中的事件模式。

正在测试 DNS 防火墙事件的事件模式 EventBridge

您可以使用 EventBridge 沙盒快速定义和测试事件模式，而不必完成创建或编辑规则的更大过程。使用沙盒，您可以定义事件模式，并使用示例事件来确认该模式与所需事件相匹配。 EventBridge 您可以选择直接从沙箱中使用该事件模式创建新规则。

有关更多信息，请参阅EventBridge 用户指南中的使用 EventBridge 沙盒测试事件模式。

为 DNS 防火墙创建 EventBridge 规则和目标

以下过程向您展示如何创建允许 EventBridge 为所有 DNS 防火墙警报和阻止操作发送事件的规则，以及如何添加 Amazon Lambda 功能作为规则的目标。

1. Amazon CLI 用于创建 EventBridge 规则：

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. 附加 Lambda 函数作为规则的目标：

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. 要添加调用目标所需的权限，请运行以下 Lambda Amazon CLI 命令：

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge 权限

DNS Firewall 不需要任何其他权限即可向 Amazon EventBridge传输事件。

您指定的目标可能需要特定的权限或配置。有关为目标使用特定服务的更多详细信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 目标。

其他 EventBridge 资源

有关如何使用 EventBridge 来处理和管理事件的更多信息，请参阅《Amazon EventBridge 用户指南》中的以下主题。

- 有关事件总线工作原理的详细信息，请参阅 Amazon EventBridge 事件总线。
- 有关事件结构的信息，请参阅事件。
- 有关构造事件模式 EventBridge 以便在将事件与规则进行匹配时使用的信息，请参阅事件模式。
- 有关创建规则以指定 EventBridge 所处理事件的信息，请参阅规则。
- 有关指定向哪些服务或其他目标 EventBridge 发送匹配事件的信息，请参阅 Targets。

解析器 DNS 防火墙事件详细信息参考

来自 Amazon 服务的所有事件都有一组公共字段，其中包含有关事件的元数据，例如作为事件来源的 Amazon 服务、事件的生成时间、事件发生的账户和区域等。有关这些常规字段的定义，请参阅《Amazon EventBridge 用户指南》中的事件结构参考。

此外，每个事件都有一个 `detail` 字段，其中包该特定事件专有的数据。下面的参考定义了各种 DNS Firewall 事件的详细信息字段。

使用 EventBridge 选择和管理 DNS 防火墙事件时，请记住以下几点：

- 来自 DNS Firewall 的所有事件的 `source` 字段都设置为 `aws.route53resolver`。
- `detail-type` 字段指定事件类型。

  例如，`DNS Firewall Block` 或 `DNS Firewall Alert`。
- `detail` 字段包含该特定事件专有的数据。

有关如何构造使规则能够匹配 DNS Firewall 事件的事件模式的信息，请参阅《Amazon EventBridge 用户指南》中的事件模式。

有关事件及其 EventBridge 处理方式的更多信息，请参阅《Amazon EventBridge 用户指南》中的Amazon EventBridge 事件。

主题

DNS Firewall 警报事件详细信息

以下是警报状态事件的详细信息字段。

之所以包含 `source` 和 `detail-type` 字段，是因为其包含 Route 53 事件的特定值。

```
{...,
 "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

标识事件的类型。

对于这一事件，此值为 DNS Firewall Alert。

source

标识生成事件的服务。对于 DNS Firewall 事件，此值为 aws.route53resolver。

detail

包含关于事件信息的 JSON 对象。生成事件的服务决定该字段的内容。

对于此事件，此数据包括：

account-id

创建 VPC 的 ID。 Amazon Web Services 账户

last-observed-at

在 VPC 中进行 Alert/Block 查询的时间戳。

query-name

查询中指定的域名 (example.com) 或子域名 (www.example.com)。

query-type

在请求中指定的 DNS 记录类型，或 ANY。有关 Route 53 支持的类型的信息，请参阅 支持的 DNS 记录类型。

query-class

查询的类。

transport

用于提交 DNS 查询的协议。

firewall-rule-action

查询中与域名匹配的规则指定的操作。ALERT 或 BLOCK。

firewall-rule-group-id

查询中与域名匹配的 DNS Firewall 规则组 ID。有关防火墙规则组更多信息，请参阅 DNS Firewall DNS Firewall 规则组和规则。

firewall-domain-list-id

查询中与域名匹配的规则使用的域列表。

`firewall-protection`

DNS 防火墙高级保护：DGA、DICTIONARY_DGA 或 DNS_TUNNELING。有关更多信息，请参阅 DNS Firewall 解析器 DNS 防火墙高级。

`resourcese`

包含资源类型以及与其有关的其他详细信息。

`resource-type`

指定资源类型，例如解析程序端点或 VPC 实例。

`resource-type``-detail`

有关该资源的其他详细信息。

Example DNS Firewall 警报事件

以下是示例警报事件。

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DGA",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
```

```
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```

DNS Firewall 阻止事件详细信息

以下是的详细信息字段*event name*。

之所以包含 source 和 detail-type 字段，是因为其包含 Route 53 事件的特定值。

```
{...,
 "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
```

```
    {
        "resource-type": "string",
        "resolver-endpoint-details": {
        "id": "string"
      }
    }
]
```

`detail-type`

标识事件的类型。

对于这一事件，此值为 `DNS Firewall Alert`。

`source`

标识生成事件的服务。对于 DNS Firewall 事件，此值为 `aws.route53resolver`。

`detail`

包含关于事件信息的 JSON 对象。生成事件的服务决定该字段的内容。

对于此事件，此数据包括：

`account-id`

创建 VPC 的 ID。 Amazon Web Services 账户

`last-observed-at`

在 VPC 中进行 Alert/Block 查询的时间戳。

`query-name`

查询中指定的域名 (example.com) 或子域名 (www.example.com)。

`query-type`

在请求中指定的 DNS 记录类型，或 ANY。有关 Route 53 支持的类型的信息，请参阅 支持的 DNS 记录类型。

`query-class`

查询的类。

`transport`

用于提交 DNS 查询的协议。

`firewall-rule-action`

查询中与域名匹配的规则指定的操作。ALERT 或 BLOCK。

`firewall-rule-group-id`

查询中与域名匹配的 DNS Firewall 规则组 ID。有关防火墙规则组更多信息，请参阅 DNS Firewall DNS Firewall 规则组和规则。

`firewall-domain-list-id`

查询中与域名匹配的规则使用的域列表。

`firewall-protection`

DNS 防火墙高级保护：DGA、DICTIONARY_DGA 或 DNS_TUNNELING。有关更多信息，请参阅 DNS Firewall 解析器 DNS 防火墙高级。

`resourcese`

包含资源类型以及与其有关的其他详细信息。

`resource-type`

指定资源类型，例如解析程序端点或 VPC 实例。

`resource-type``-detail`

有关该资源的其他详细信息。

Example 事件示例

以下是示例阻止事件。

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
```

```
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DNS_TUNNELING",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```


使用记录亚马逊 Route 53 API 调用 Amazon CloudTrail

Route 53 与 Amazon CloudTrail一项服务集成，该服务提供用户、角色或 Amazon 服务在 Route 53 中采取的操作的记录。 CloudTrail 将 Route 53 的所有 API 调用捕获为事件，包括来自 Route 53 控制台的调用和对 Route 53 的代码调用 APIs。如果您创建了跟踪，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Route 53 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Route 53 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

主题

- 53 号公路的信息在 CloudTrail
- 在事件历史记录中查看 Route 53 事件

- 了解 Route 53 日志文件条目

53 号公路的信息在 CloudTrail

CloudTrail 在您创建 Amazon 账户时已在您的账户上启用。当 Route 53 中发生活动时，该活动会与其他 Amazon 服务CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 Amazon 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录您的 Amazon 账户中的事件，包括 Route 53 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有区域。跟踪记录 Amazon 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅:

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 Route 53 操作均由《亚马逊 Route 53 API 参考》记录 CloudTrail 并记录在案。例如，对`CreateHostedZone`、`CreateHealthCheck`、和`RegisterDomain`操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

在事件历史记录中查看 Route 53 事件

CloudTrail 允许您在事件历史记录中查看最近的事件。要查看 Route 53 API 请求的事件，您必须在控制台顶部的区域选择器中选择美国东部（弗吉尼亚北部）。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 CloudTrail 事件历史查看事件。

了解 Route 53 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

`eventName` 元素可标识发生的操作。（在 CloudTrail 日志中，域名注册操作的第一个字母是小写的，尽管操作名称中的首字母是大写的。 例如，`UpdateDomainContact`如日志`updateDomainContact`中所示）。 CloudTrail 支持所有 Route 53 API 操作。以下示例显示了一个演示以下操作的 CloudTrail 日志条目：

- 列出与 Amazon 账户关联的托管区域
- 创建运行状况检查
- 创建两个记录
- 删除托管区域
- 为已注册的域更新信息
- 创建 Route 53 VPC 解析器出站终端节点


```
{
    "Records": [
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
            "eventName": "ListHostedZones",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2015-01-16T00:41:48Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": null,
            "responseElements": null,
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
```

```
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
            "eventName": "CreateHealthCheck",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:57Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "callerReference": "2014-05-06 64832",
                "healthCheckConfig": {
                    "iPAddress": "192.0.2.249",
                    "port": 80,
                    "type": "TCP"
                }
            },
            "responseElements": {
                "healthCheck": {
                    "callerReference": "2014-05-06 64847",
                    "healthCheckConfig": {
                        "failureThreshold": 3,
                        "iPAddress": "192.0.2.249",
                        "port": 80,
                        "requestInterval": 30,
                        "type": "TCP"
                    },
                    "healthCheckVersion": 1,
                    "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
                },
                "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
```

```
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "accountId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "type": "IAMUser",
            "userName": "smithj"
        }
    },
    {
        "additionalEventData": {
            "Note": "Do not use to reconstruct hosted zone"
        },
        "apiVersion": "2013-04-01",
        "awsRegion": "us-east-1",
        "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
        "eventName": "ChangeResourceRecordSets",
        "eventSource": "route53.amazonaws.com",
        "eventTime": "2018-01-16T00:41:43Z",
        "eventType": "AwsApiCall",
        "eventVersion": "1.02",
        "recipientAccountId": "444455556666",
        "requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
        "requestParameters": {
            "changeBatch": {
                "changes": [
                    {
                        "action": "CREATE",
                        "resourceRecordSet": {
                            "name": "prod.example.com.",
                            "resourceRecords": [
                                {
                                    "value": "192.0.1.1"
                                },
                                {
                                    "value": "192.0.1.2"
                                },
                                {
                                    "value": "192.0.1.3"
                                },
                                {
                                    "value": "192.0.1.4"
                                }
                            ],
                            "tTL": 300,
```

```
                            "type": "A"
                        }
                    },
                    {
                        "action": "CREATE",
                        "resourceRecordSet": {
                            "name": "test.example.com.",
                            "resourceRecords": [
                                {
                                    "value": "192.0.1.1"
                                },
                                {
                                    "value": "192.0.1.2"
                                },
                                {
                                    "value": "192.0.1.3"
                                },
                                {
                                    "value": "192.0.1.4"
                                }
                            ],
                            "tTL": 300,
                            "type": "A"
                        }
                    }
                ],
                "comment": "Adding subdomains"
            },
            "hostedZoneId": "Z1PA6795UKMFR9"
        },
        "responseElements": {
            "changeInfo": {
                "comment": "Adding subdomains",
                "id": "/change/C156SRE0X2ZB10",
                "status": "PENDING",
                "submittedAt": "Jan 16, 2018 12:41:43 AM"
            }
        },
        "sourceIPAddress": "192.0.2.92",
        "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
        "userIdentity": {
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "accountId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/smithj",
```

```
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "type": "IAMUser",
            "userName": "smithj"
        }
    },
    {
        "apiVersion": "2013-04-01",
        "awsRegion": "us-east-1",
        "eventID": "0cb87544-ebee-40a9-9812-e9dda1962cb2",
        "eventName": "DeleteHostedZone",
        "eventSource": "route53.amazonaws.com",
        "eventTime": "2018-01-16T00:41:37Z",
        "eventType": "AwsApiCall",
        "eventVersion": "1.02",
        "recipientAccountId": "444455556666",
        "requestID": "6d5d149f-9d18-11e4-b752-f9c6311f3510",
        "requestParameters": {
            "id": "Z1PA6795UKMFR9"
        },
        "responseElements": {
            "changeInfo": {
                "id": "/change/C1SIJYUYIKVJWP",
                "status": "PENDING",
                "submittedAt": "Jan 16, 2018 12:41:36 AM"
            }
        },
        "sourceIPAddress": "192.0.2.92",
        "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
        "userIdentity": {
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "accountId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "type": "IAMUser",
            "userName": "smithj"
        }
    },
    {
        "eventVersion": "1.05",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
```

```
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "userName": "smithj",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2018-11-01T19:43:59Z"
                    }
                },
                "invokedBy": "test"
            },
            "eventTime": "2018-11-01T19:49:36Z",
            "eventSource": "route53domains.amazonaws.com",
            "eventName": "updateDomainContact",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "domainName": {
                    "name": "example.com"
                }
            },
            "responseElements": {
                "requestId": "034e222b-a3d5-4bec-8ff9-35877ff02187"
            },
            "additionalEventData": "Personally-identifying contact information is not
logged in the request",
            "requestID": "015b7313-bf3d-11e7-af12-cf75409087f6",
            "eventID": "f34f3338-aaf4-446f-bf0e-f72323bac94d",
            "eventType": "AwsApiCall",
            "recipientAccountId": "444455556666"
        },
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2018-11-01T14:33:09Z"
```

```
                    },
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "AROAIUZEZLWWZOEXAMPLE",
                        "arn": "arn:aws:iam::123456789012:role/Admin",
                        "accountId": "123456789012",
                        "userName": "Admin"
                    }
                }
            },
            "eventTime": "2018-11-01T14:37:19Z",
            "eventSource": "route53resolver.amazonaws.com",
            "eventName": "CreateResolverEndpoint",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.176",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
 Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "creatorRequestId": "123456789012",
                "name": "OutboundEndpointDemo",
                "securityGroupIds": [
                    "sg-05618b249example"
                ],
                "direction": "OUTBOUND",
                "ipAddresses": [
                    {
                        "subnetId": "subnet-01cb0c4676example"
                    },
                    {
                        "subnetId": "subnet-0534819b32example"
                    }
                ],
                "tags": []
            },
            "responseElements": {
                "resolverEndpoint": {
                    "id": "rslvr-out-1f4031f1f5example",
                    "creatorRequestId": "123456789012",
                    "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
                    "name": "OutboundEndpointDemo",
                    "securityGroupIds": [
                        "sg-05618b249example"
                    ],
```

```
                    "direction": "OUTBOUND",
                    "ipAddressCount": 2,
                    "hostVPCId": "vpc-0de29124example",
                    "status": "CREATING",
                    "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
 Creating the Resolver Endpoint",
                    "creationTime": "2018-11-01T14:37:19.045Z",
                    "modificationTime": "2018-11-01T14:37:19.045Z"
                }
            },
            "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",
            "eventID": "cb05b4f9-9411-4507-813b-33cb0example",
            "eventType": "AwsApiCall",
            "recipientAccountId": "123456789012"
        }
    ]
}
```

Amazon Route 53 故障排除

本页将介绍有关 Amazon Route 53 的下列故障排除主题：

> **Important**
>
> 请注意，您不能使用 Amazon Route 53 在中国区域注册或转移域。但是，您可以在其中一个中国区域中创建托管区域，并将该托管区域的名称服务器与您使用全局账户注册的域或向其它域注册商注册的域相关联。

1. 域不可用：
   - 了解域可能无法在互联网上使用的常见原因，比如未对注册人电子邮件进行确认、DNS 服务转移问题、名称服务器设置不正确或托管区遭到删除。
2. 域暂停：
   - 了解域暂停（ClientHold 状态）的原因以及如何取消域暂停，包括域过期、注册人电子邮件变更未得到确认以及付款处理问题。
3. 域操作失败：
   - 解决因联系人信息无效而导致的域操作失败，包括注册、转移、续订和联系人更新问题。
4. 域转移失败：
   - 了解域无法转移到 Route 53 的常见原因，例如转移未获授权、授权代码无效或国际化域名问题。
5. DNS 设置未生效：
   - 排查 DNS 设置更改尚未生效的情况，包括 DNS 解析程序缓存、名称服务器更新不正确以及存在多个同名托管区。
6. “未找到服务器” 错误：
   - 从浏览器中查找“未找到服务器”错误的解决方案，例如缺少记录、记录值不正确或资源不可用。
7. 将流量路由到 S3 存储桶：
   - 解决尝试将流量路由到为网站托管配置的 Amazon S3 存储桶时出现的问题。
8. 账单问题：
   - 了解常见的计费方案，包括同一个托管区收费两次、为域开具多张发票，以及关闭或永久关闭 Amazon Web Services 账户时出现的域注册问题。

主题

我的域在 Internet 上不可用

您的域在 Internet 上不可用，有以下几个最常见的可能原因。

主题

您注册了新域，但没有单击确认电子邮件中的链接

当您注册一个新域时，ICANN 会要求我们确认注册联系人的电子邮件地址是否有效。为进行确认，我们会发送一封电子邮件，其中包含一个链接。(如果您没有响应这第一封电子邮件，我们会向您再次发送同样的电子邮件，但最多再发送两次。) 您有 3 到 15 天的时间来单击该链接，具体时间取决于顶级域。在这之后，该链接将失效。

如果您没有在规定的时间内单击电子邮件中的链接，ICANN 会要求我们暂停该域。有关如何向注册联系人重新发送确认电子邮件的信息，请参阅重新发送授权和确认电子邮件。

您将域注册转移到了 Amazon Route 53，但没有转移 DNS 服务

如果您以前的注册商随域注册提供免费的 DNS 服务，则该注册商可能在您将域注册转移到 Route 53 时即停止提供 DNS 服务。执行以下步骤，确定是否为此原因，如果是，请予以解决。

恢复 DNS 服务 - 如果您以前的注册商在您将域注册转移到 Route 53 后取消了 DNS 服务，

1. 请联系您以前的注册商，确认他们是否取消了您的域的 DNS 服务。如果是，则执行下面三个最快速的方法 (按必要性排序)，来恢复域的 DNS 服务：

   - 如果以前的注册商提供付费 DNS 服务，则请他们使用您的域的旧 DNS 记录和名称服务器恢复 DNS 服务。
   - 如果以前的注册商规定不进行域注册就不提供付费 DNS 服务，则询问他们您是否可以将域注册转移回来，然后使用您的域的旧 DNS 记录和名称服务器恢复 DNS 服务。
   - 如果您可以将域注册重新转移回以前的注册商，但他们没有保留您的 DNS 记录，则询问他们您是否可以将域注册重新转移到他们那里，并获得以前分配给您的域的相同名称服务器集。如果不可以，您将不得不自己重新创建旧的 DNS 记录。但一旦您完成此操作，您的域将再次变得可用。

   如果您以前的注册商无法帮助您完成以上任一选项，请继续执行步骤 2。

   > **Important**
   >
   > 如果您无法使用在将域转移到 Route 53 时所指定的名称服务器恢复 DNS 服务，则在您完成本过程中其余步骤的至多两天后，您的域在 Internet 上会变得再次可用。DNS 解析程序通常会将域名服务器的名称缓存 24 到 48 个小时，在此之后所有 DNS 解析程序才能获得新名称服务器的名称。

2. 选择一个新的 DNS 服务，例如 Route 53。
3. 使用新的 DNS 服务提供的方法来创建托管区域和记录：

   a. 创建一个与您的域 (如 example.com) 同名的托管区域。

   b. 使用以前的注册商提供的区域文件创建记录。

   如果您选择 Route 53 作为您的新 DNS 服务，则可以通过导入区域文件来创建记录。有关更多信息，请参阅 通过导入区域文件来创建记录。

4. 获得新托管区域的名称服务器。如果您选择 Route 53 作为 DNS 服务，请参阅 获取公有托管区域的名称服务器。
5. 将您的域名服务器更改为在步骤 4 中获得的名称服务器。有关更多信息，请参阅 为域添加或更改名称服务器和粘附记录。

您转移了域注册并在域设置中指定了错误的名称服务器

当您将域注册转移到 Amazon Route 53 时，您为域指定的设置之一是将响应域的 DNS 查询的一组名称服务器。这些名称服务器来自于和域同名的托管区域。托管区域包含有关您如何路由域流量的信息，如 www.example.com 的 Web 服务器的 IP 地址。

您可能无意中为错误的托管区域指定了名称服务器，如果您有多个和域同名的托管区域，尤其容易发生这种错误。要确认域是否使用着正确的托管区域的名称服务器，并在必要时更新域的名称服务器，请执行以下过程。

> **Important**
>
> 如果在将域转移到 Route 53 时指定了错误的名称服务器记录，则在纠正名称服务器后，可能需要长达两天时间 DNS 服务才能完全恢复。这是因为分布在 Internet 上的 DNS 解析程序通常每两天请求一次名称服务器，并缓存应答。

获取托管区域的名称服务器

1. 如果您对域使用另一个 DNS 服务，则使用该 DNS 服务提供的方法获取托管区域的名称服务器。然后跳到下一个步骤。

   如果您使用 Route 53 作为域的 DNS 服务，请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区。
3. 在 Hosted Zones 页面上，选择托管区域的单选按钮 (不是名称)。

   > **Important**
   >
   > 如果多个托管区域具有相同名称，请确保选择正确托管区域的名称服务器。
4. 在右窗格中，记下 Name Servers 下所列的四个服务器。

确认域使用正确的名称服务器

1. 如果您对域使用另一个 DNS 服务，请登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

   如果您使用 Route 53，则跳到下一步。
2. 在导航窗格中，选择 Registered Domains。
3. 选择您希望为其编辑设置的域的名称。
4. 选择 Add or Edit Name Servers。
5. 比较在上一过程中获得的名称服务器列表与 Edit Name Servers for domain name 对话框中的名称服务器列表。
6. 如果此处所列的名称服务器和在上一过程中获得的名称服务器不匹配，则更改此处的名称服务器，然后选择 Update。

您首先转移了 DNS 服务，但没有等待足够长时间就转移了域注册

当您将 DNS 服务转移到 Amazon Route 53 或另一个 DNS 服务时，您向域注册商更新了域配置，以使用新 DNS 服务的名称服务器。

响应您的域请求的 DNS 解析程序通常会将名称服务器的名称缓存 24 到 48 小时。如果您更改某个域的 DNS 服务，将一个 DNS 服务的名称服务器替换为另一个 DNS 服务的名称服务器，则最多 48 个小时后，DNS 解析程序才开始使用新名称服务器，并进而使用新的 DNS 服务。

下面解释了在转移 DNS 服务后太早转移域会导致域在 Internet 上不可用的原因：

1. 您转移了域的 DNS 服务。
2. 您将域转移到 Route 53 时 DNS 解析程序还没有开始使用您的新 DNS 服务的名称服务器。
3. 当您将域转移到 Route 53 后，您以前的注册商随即取消了您的域的 DNS 服务。
4. DNS 解析程序还在将查询路由到您的旧 DNS 服务，但不再有任何记录告诉它们如何路由您的流量。

当旧 DNS 服务的名称服务器的缓存到期时，DNS 将开始使用新的 DNS 服务。遗憾的是，没有办法来加快这一过程。

您删除了 Route 53 用于路由域的 Internet 流量的托管区域

如果 Route 53 是您的域的 DNS 服务，则当您删除了用于路由域的 Internet 流量的托管区域后，该域在 Internet 上会变得不可用。不管是否向 Route 53 注册了该域，都是如此。

> **Important**
>
> 还原域的 Internet 服务可能需要长达 48 小时。

在您删除了 Route 53 用于路由域的 Internet 流量的托管区域后还原 Internet 服务

1. 创建另一个与域同名的托管区域。有关更多信息，请参阅 创建公有托管区域。
2. 重新创建您删除的托管区域中的记录。有关更多信息，请参阅 使用记录。
3. 获取 Route 53 分配给新托管区域的名称服务器的名称。有关更多信息，请参阅 获取公有托管区域的名称服务器。
4. 更新域注册以使用您在步骤 3 中获取的名称服务器：
   - 如果此域已向 Route 53 注册，请参阅 为域添加或更改名称服务器和粘附记录。
   - 如果此域已向其他域注册商注册，请使用注册商提供的方法更新域注册以使用新名称服务器。
5. 为缓存了已删除托管区域的名称服务器的名称的递归解析程序等待名称服务器的 TTL 过去。在 TTL 过去后，当浏览器或应用程序提交域或其子域之一的 DNS 查询时，递归解析程序会将此查询转发到新托管区域的 Route 53 名称服务器。有关更多信息，请参阅 Amazon Route 53 如何为您的域路由流量。

   名称服务器的 TTL 可能长达 48 小时，具体取决于域的 TLD。

您的域已被暂停

因为我们不得不暂停您的域，这将导致您的域在 Internet 上不可用。有关更多信息，请参阅 我的域暂停 (状态为 ClientHold)。

我的域暂停 (状态为 ClientHold)

如果 Amazon Route 53 暂停您的域，则该域在 Internet 上会变得不可用。您可以使用以下任一方法来确定一个域是否已暂停：

- 在 Route 53 控制台中，在 Registered domains（已注册的域）页面底部的 Alerts（提醒）表中查找该域名。如果 Status 列的值为 clientHold，则该域已暂停。
- 针对该域发送 WHOIS 查询。如果 Domain Status 的值为 clientHold，则该域已暂停。WHOIS 命令在许多操作系统中都可用，并且在许多网站中还可作为 Web 应用程序提供。

此外，当我们暂停一个域时，通常会向该域的注册联系人的电子邮件地址发送一封电子邮件。但是，如果暂停该域是基于法院判决，则法院可能不允许我们通知注册联系人。

要使一个域在 Internet 上再次可用，必须解除暂停。以下是域被暂停的原因以及解除暂停的方法。

> **Note**
>
> 如果您需要帮助以取消域暂停，可以免费联系 Amazon Support。有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

主题

您注册了新域，但没有单击确认电子邮件中的链接

当您首次向 Amazon 注册一个域时，ICANN 会要求我们确认注册联系人的电子邮件地址是否有效。为进行确认，我们会发送一封电子邮件，其中包含一个链接。您有 3 到 15 天的时间来单击该链接，具体时间取决于顶级域。在这之后，该链接将失效。

> **Note**
>
> 如果您已向 Amazon Route 53 注册了一个或多个域，并使用了相同的注册联系人电子邮件地址，则我们不会发送确认电子邮件。

如果您没有在规定的时间内单击电子邮件中的链接，ICANN 会要求我们暂停该域。有关如何向注册联系人重新发送确认电子邮件的信息，请参阅重新发送授权和确认电子邮件。当您确认电子邮件地址有效后，我们会自动对域解除暂停。

您禁用了自动续订域，因此您的域到期

如果为域启用了自动续订 (新域或转移域的默认值)，我们会在到期日期之前不久自动续订域注册。如果您禁用自动续订，我们会向注册联系人的电子邮件地址发送三封提醒电子邮件，以提醒您域注册即将到期。在域到期之日的前 45 天，我们就开始发送这些电子邮件。

如果您禁用自动续订域，而且没有手动延长域注册期，我们通常会在到期之日暂停域。请注意，有些域的注册机构甚至会在到期日之前删除域。

有关如何续订到期域的信息，请参阅 续订域注册。

您更改了注册联系人的电子邮件地址，但您未验证新电子邮件地址的有效性

如果您将注册联系人的电子邮件地址更改为以前未验证的地址，ICANN 会要求我们确认注册联系人的电子邮件地址有效。为进行确认，我们会发送一封电子邮件，其中包含一个链接。您有 3 到 15 天的时间来单击该链接，具体时间取决于顶级域。在这之后，该链接将失效。

如果您没有 TLD 注册机构允许的时间内单击电子邮件中的链接，ICANN 会要求我们暂停该域。有关如何向注册联系人重新发送确认电子邮件的信息，请参阅重新发送授权和确认电子邮件。当您确认电子邮件地址有效后，我们会自动对域解除暂停。

我们无法处理您的自动续订域付款，因此您的域到期

如果对域启用了自动续订，但我们无法处理您的付款 (例如，因为您的信用卡到期)，我们会向域注册联系人的电子邮件地址发送多封电子邮件。如果我们没有收到付款，我们通常会在到期之日暂停该域。请注意，有些域的注册机构甚至会在到期日之前删除域。

有关如何续订到期域的信息，请参阅 续订域注册。

用户违反了 Amazon 可接受使用策略，因此我们暂停了域

如果因为用户违反 Amazon 可接受使用策略而导致我们暂停了域，我们会向域的注册联系人发送一封电子邮件。（如果 Amazon 账户因涉及欺诈而被暂停，我们不会发送通知电子邮件。）

如果对暂停有异议，请发送电子邮件至 trustandsafety@support.aws.com。

由于法院判决而暂停域

如果暂停域是出于法院判决结果，则我们无法对域解除暂停，直到法院撤销判决。如果对法院判决的有效性有异议，请发送电子邮件至 trustandsafety@support.aws.com 并附加适用的文档。

我的域操作失败

如果您的域名操作失败，以下是一些故障排除提示。操作可以是注册、转移、续订或联系人更新。

域操作由于联系人信息无效而失败

如果域操作因联系人信息无效错误而失败，则说明您提供的联系人详细信息不符合注册机构的验证要求。

要解决此问题，请确认所有联系人详细信息的格式正确：

- 姓名 - 确保姓名仅包含有效字符且格式正确。
- 地址 - 确认地址格式符合该国家/地区的邮政标准。
- 电话号码 - 使用该国家/地区的正确国际格式。
- 标识字段 - 对于需要标识号的域，请确保指定国家/地区的格式正确。

更正联系人信息后，请再次尝试域操作。有关不同顶级域的具体要求，请参阅 可向 Amazon Route 53 注册的域。。

将我的域转移到 Amazon Route 53 失败

如果您的域转移已经失败或被拒绝，请使用此部分来诊断和解决故障。

> **Note**
>
> 要防止在活跃转移期间出现问题，请参阅 防止 Route 53 的常见转移问题。

主题

- 没有单击授权电子邮件中的链接
- 您从当前注册商获取的授权代码无效

- 尝试将 .es 域转移到 Amazon Route 53 时出现“Parameters in request are not valid（请求中的参数无效）”错误
- 域名代码中是否列出了您要转移到 Amazon Route 53 的国际化域名？
- 常见转移错误消息

没有单击授权电子邮件中的链接

当您将域注册转移到 Amazon Route 53 时，按照 ICANN（域注册管理机构）的要求，域的注册联系人必须向我们提供转移授权。为获得授权，我们会向您发送一封电子邮件，其中包含一个链接。您有 5 到 15 天的时间来单击该链接，具体时间取决于顶级域。在这之后，该链接将失效。

如果您没有在规定的时间内单击电子邮件中的链接，ICANN 会要求我们取消该转移。有关如何向注册联系人重新发送授权电子邮件的信息，请参阅重新发送授权和确认电子邮件。

您从当前注册商获取的授权代码无效

如果您请求将域转移到 Amazon Route 53，但没有收到授权电子邮件，请检查 Route 53 控制台中的状态页面。如果状态页面显示您从注册商处获得的转移授权代码无效，请执行以下步骤：

1. 联系域的当前注册商，请求新的授权代码。请确认以下内容：
   - 新的授权代码保持有效状态的时间。必须在该代码到期之前请求域转移。
   - 新的授权代码不同于无效的代码。如果仍是一样的，请要求当前注册商刷新授权代码。
2. 提交另一个请求以转移域。有关更多信息，请参阅 步骤 5：请求转移主题中的 将域注册转移到 Amazon Route 53。

尝试将 .es 域转移到 Amazon Route 53 时出现“Parameters in request are not valid（请求中的参数无效）”错误

当您尝试将 .es 域转移到 Route 53 而注册联系人的联系人类型是 Company（公司）时，Amazon Route 53 将返回“Parameters in request are not valid（请求中的参数无效）”错误。要完成转移，请将注册者的联系类型更改为 Person（人员），然后重新提交。

域名代码中是否列出了您要转移到 Amazon Route 53 的国际化域名？

在注册新域名或创建托管区域和记录时，您可以指定除 a-z 以外的其它字符（例如，法语中的 ç）、其它字母表中的字符（例如西里尔字母或阿拉伯字母），也可以指定中文、日语或韩语中的字

符。Amazon Route 53 在域名代码中存储这些国际化域名 (IDN)，域名代码将 Unicode 字符表示为 ASCII 字符串。

如果在将 IDN 转移到 Route 53 时出错，请使用域名代码来表示该错误，然后重试。有关更多信息，请参阅 设置国际化域名的格式。

常见转移错误消息

当域转移失败时，您通常会在 Route 53 控制台中或通过电子邮件收到错误消息。以下是最常见的错误消息以及如何解决这些错误：

“转移被注册机构拒绝”

当域注册机构出于以下几种原因之一阻止转移时，就会发生此错误。最常见的原因是：

- 该域不符合 ICANN 的 60 天规则。ICANN 要求在首次注册或注册人联系人更改后的 60 天内阻止转移。
- 该域已在您当前的注册商处启用转移锁定。
- 域处于阻止转移的状态，例如 `clientTransferProhibited`、`serverTransferProhibited`、`pendingDelete`、`pendingTransf` 或 `redemptionPeriod`。

要解决此问题，请向当前注册商检查以下内容：

- 确认该域自注册之日起已超过 60 天。如果您最近更改注册人的联系人信息，则可能需要在更改后等待 60 天。有些注册商允许您选择退出此限制，因此请询问您当前的注册商是否提供此选项。
- 通过禁用任何转移锁定或域锁定来解锁域。
- 检查您的域状态是否允许转移。您可以使用 WHOIS 查询或联系您当前的注册商来验证名状态。

“授权代码无效”或“授权码不正确”

此错误意味着您输入的授权代码（也称为 EPP 代码或转移代码）无效。如果代码已过期、输入错误或不是从您当前的注册商处获得，则可能会发生这种情况。

要解决此问题，请执行以下操作：

- 联系当前注册商，请求新的授权代码。请务必询问代码将保持有效状态多长时间，这样您就可以在其过期之前完成转移。

- 收到新代码后，请确认它与之前的代码不同。如果相同，请要求您的注册商刷新或重新生成授权代码。
- 仔细检查您输入的代码是否与提供的代码完全一致，包括任何大写或小写字母、数字和特殊字符。

“未收到转移授权电子邮件”或“授权超时”

如果您未在要求的时间范围内（通常为 5 天）单击转移确认电子邮件中的授权链接，就会发生此错误。ICANN 要求所有域转移都必须执行此授权步骤。

如果您没有收到授权电子邮件或错过截止日期，请检查以下内容：

- 检查您的垃圾电子邮件文件夹。转移授权电子邮件有时会被电子邮件提供商过滤。
- 确认您的邮箱未满且没有可能阻止电子邮件传送的存储限制。
- 检查您的电子邮件提供商是否有过滤来自未知发件人的传入邮件的策略。
- 确认您可以访问注册人的电子邮件账户，并且该电子邮件地址仍处于活跃状态。

如有必要，请在请求另一次转移之前向当前的注册商更新您的联系人信息。有关重新发送授权电子邮件的信息，请参阅 重新发送授权和确认电子邮件。

“域已锁定”或“禁止转移”

此错误表示您的域启用锁定，这会阻止转移。大多数注册商默认启用域锁定，将其作为一项安全措施，以防止未经授权的转移。

要解决此问题，请登录当前域注册商的账户，并禁用域锁定或转移锁定设置。具体步骤因注册商而异，但您通常可以在域管理或安全设置中找到这些设置。如果您在查找这些设置时需要帮助，请联系当前的注册商寻求帮助。

“需要验证联系人信息”

当您最近更改域的联系人信息时，就会发生此错误。ICANN 规则要求在联系人更改后等待 60 天才能转移域，以防止欺诈性转移。

您有两个选项来解决此问题：

- 在更改联系人之日起等待 60 天，然后再尝试转移。
- 联系当前的注册商以验证您当前的联系人信息。如果您可以验证自己的身份，某些注册商可能会允许您选择退出 60 天的限制。

> **Note**
>
> 如果您收到的错误消息未在此处列出，请联系 Amazon Support 并附上确切的错误文本。我们的支持团队可以根据您的具体情况帮助您诊断和解决转移问题。

我更改了 DNS 设置，但没有生效

如果您更改了 DNS 设置而更改没有生效，以下是一些常见原因。

主题

您在最近 48 小时将 DNS 服务转移到了 Amazon Route 53，所以 DNS 仍在使用您之前的 DNS 服务

当您将 DNS 服务转移到 Amazon Route 53 时，您使用了域注册商提供的方法将以前 DNS 服务的名称服务器替换为 Route 53 的四个名称服务器。

> **Note**
>
> 如果您不确定是否做了这一部分工作，请参阅 您最近将 DNS 服务转移到 Amazon Route 53，但没有向域注册商更新名称服务器。

域注册商通常对名称服务器使用 24 到 48 个小时的 TTL (生存时间)。这意味着当某个 DNS 解析程序在获取您的域名服务器时，会在长达 48 小时的时间内使用该信息，之后才会提交对于域的最新名称服务器的另一个请求。如果您在最近 48 小时内将 DNS 服务转移到 Route 53，然后更改了 DNS 设置，则有些 DNS 解析程序仍在使用您的旧 DNS 服务来路由域流量。

您最近将 DNS 服务转移到 Amazon Route 53，但没有向域注册商更新名称服务器

您的域的注册商拥有域的各种信息，包括域的 DNS 服务的名称服务器。域注册商通常也是您的 DNS 服务，因此与您的域关联的名称服务器属于注册商。这些名称服务器告知 DNS 从何处获取有关您希望如何路由域流量的信息，例如，路由到您的域的 Web 服务器 IP 地址。

当您将 DNS 服务转移到 Amazon Route 53 时，需要使用域注册商提供的方法来更改与域关联的名称服务器。通常，您需要将注册商提供的名称服务器替换为四个 Route 53 名称服务器，它们与您为域创建的托管区域相关联。

如果您为域创建了一个新的托管区域和记录，并指定了与上一 DNS 服务不同的设置，但 DNS 仍在将流量路由到旧资源，则有可能您没有向域注册商更新名称服务器。要确定注册商是否在使用您的 Route 53 托管区域的名称服务器，并在必要时更新域的名称服务器，请执行以下过程：

获取您的托管区域的名称服务器，并向域注册商更新名称服务器设置

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区。
3. 在 Hosted Zones（托管区域）页面上，选择托管区域的单选按钮（不是名称）。

   > **Important**
   >
   > 如果多个托管区域具有相同名称，请确保选择正确托管区域的名称服务器。

4. 在 Record name（记录名称）列表中，记下 Name Servers（名称服务器）下所列的四个服务器。
5. 使用域注册商提供的方法显示域名服务器的列表。
6. 如果域名服务器和您在步骤 4 中获得的名称服务器匹配，则表明域配置正确。

   如果域的名称服务器和您在步骤 4 中获得的名称服务器不匹配，更新域以使用 Route 53 名称服务器。
7.

> **Important**
>
> 如果您将域的名称服务器更改为来自 Route 53 托管区域的名称服务器，可能需要多达两天时间更改才会生效，Route 53 才能成为您的 DNS 服务。这是因为分布在 Internet 上的 DNS 解析程序通常每两天请求一次名称服务器，并缓存应答。

DNS 解析程序仍在使用记录的旧设置

如果您更改了记录中的设置，但您的流量仍被路由到旧资源 (如您的网站的 Web 服务器)，一个可能的原因是 DNS 仍缓存有以前的设置。每个记录都有一个 TTL (生存时间) 值，用来指定您希望 DNS 解析程序缓存记录中的信息 (如 Web 服务器的 IP 地址) 的时间 (以秒为单位)。直到经过 TTL 所指定的时间后，DNS 解析程序才继续返回旧值以响应 DNS 查询。如果您想知道记录的 TTL 值，请执行以下过程。

> **Note**
>
> 对于别名记录，TTL 由记录将流量路由到的 Amazon 资源决定。有关更多信息，请参阅 在别名记录和非别名记录之间进行选择。

查看记录的 TTL

1. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在托管区域页面上，选择包含该记录的托管区域的名称。
3. 在记录列表中，找到要了解其 TTL 值的记录，查看 TTL 列的值。

> **Note**
>
> 现在更改 TTL 不会使更改更快生效。DNS 解析程序已将此值缓存，因此，在经过旧设置所指定的时间之前，它们不会得到新的设置。

您有多个同名的托管区域，并且更新了未与该域关联的一个托管区域

您可以使用同一账户或使用多个账户创建具有相同名称的多个托管区域。要指定 Route 53 用于路由域的 Internet 流量的托管区域，您可以获取该托管区域的四个 Route 53 名称服务器，然后更新域注册以使用这些名称服务器。

如果您在一个托管区域中添加、更改或删除记录，但您的域注册使用的是另一个托管区域的名称服务器，则 Route 53 对 DNS 查询的响应将不会反映您的更改。要确定您的域注册是否正在对您已更新其中记录的托管区域使用名称服务器，请执行以下任务：

1. 确定哪些名称服务器与您的域注册相关联。请参阅添加或更改名称服务器或粘附记录。
2. 将您在步骤 1 中获得的名称服务器与 Route 53 分配给您更新其中记录的托管区域的名称服务器进行比较。请参阅获取公有托管区域的名称服务器。

如果域注册的名称服务器与您更新其中记录的托管区域的名称服务器不匹配，则有两个选项：

更改当前与域关联的托管区域中的记录（推荐）

记下您在当前未与域注册关联的托管区域中所做的更改。然后转到与域注册相关联的托管区域，并进行相同的更改。这是首选方法，因为更改几乎立即生效。有关更多信息，请参阅 编辑记录。

更新您的域名注册以使用不同的名称服务器

更改域注册以使用您更新的托管区域中的名称服务器。

> **Important**
>
> 如果您更改与您的域名注册相关联的域名服务器，您的域名将在 Internet 上长达 2 天不可用。这是因为 DNS 解析程序通常会将名称服务器的名称缓存 2 天。有关 DNS 工作原理的概述，包括有关解析程序缓存的信息，请参阅Amazon Route 53 如何为您的域路由流量。

通过更改与域注册关联的名称服务器，您实质上是在更改域的 DNS 服务。您有两个选项，具体取决于域当前是否正在使用中：

- 如果域正在使用中，请参阅将 Route 53 作为正在使用的域的 DNS 服务。
- 如果域当前处于非活动状态，请执行以下任务：
  1. 获取要用于将流量路由到域的托管区域的名称服务器。请参阅获取公有托管区域的名称服务器。

2. 在您在步骤 1 中获得名称服务器的托管区域中，确认 NS 记录使用相同的四个名称服务器。否则，请更新 NS 记录。请参阅编辑记录。
3. 更新域注册以使用您在步骤 1 中获取的名称服务器。请参阅添加或更改名称服务器或粘附记录。

我的浏览器显示“找不到服务器”错误

当您尝试浏览域 (example.com) 或子域 (www.example.com) 时，如果您的浏览器显示“找不到服务器”错误，则下面是一些常见的原因解释。

主题

您没有为域或子域名创建记录

如果您没有为域或子域创建记录，那么如果有人在浏览器中输入该名称，DNS 就不知道该将流量路由到哪里。有关更多信息，请参阅 使用记录。

您虽然创建了记录但指定了错误的值

当您创建记录时，很容易指定错误的值（如 Web 服务器的 IP 地址或 CloudFront 指派给您的 Web 分配的域名）。如果记录存在但您仍收到“找不到服务器”错误，我们建议您确认值是否正确。

您将流量路由到的资源不可用

如果记录指定的资源 (如 Web 服务器) 不可用，则浏览器将返回“找不到服务器”错误。我们建议您检查要将流量路由到的资源的状态。

无法将流量路由到为托管网站而配置的 Amazon S3 存储桶

当您为网站托管配置 Amazon S3 存储桶时，您为该存储桶指定的名称必须与您用来将流量路由到存储桶的记录名称相同。例如，如果您要将 example.com 的流量路由到为网站托管而配置的某个 S3 存储桶，则该存储桶的名称必须为 example.com。

如果您要将流量路由到为网站托管而配置的某个 S3 存储桶，但该存储桶的名称未出现在 Amazon Route 53 控制台的 Alias Target（别名目标）列表中；或者您尝试以编程方式创建一个别名记录，但从 Route 53 API、Amazon 软件开发工具包之一、Amazon CLI 或 Amazon Tools for Windows PowerShell 收到 InvalidInput 错误，请检查以下事项：

- 存储桶名称与记录名称完全匹配，如 example.com 或 www.example.com。
- S3 存储桶已正确配置，以用于网站托管。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的在 Amazon S3 上托管静态网站。

同一个托管区域被收费两次

如果您在创建一个托管区域后的 12 小时内删除了它，我们不会向您收费。12 小时后，我们会立即针对托管区域收取标准月费。对于不是整月的情况，托管区域的月费不会按比例减少。(这一费用同样适用于您注册域时我们自动创建的托管区域。)

如果您在某月的最后一天 (例如 1 月 31 日) 创建了一个托管区域，则 1 月的费用可能随 2 月的费用一起出现在 2 月的发票上。请注意，Amazon Route 53 使用协调世界时 (UTC) 作为时区来确定托管区域的创建时间。

我的域被收取多张发票的费用

当注册订阅、支付注册费、转移费用或包含预付费用的续订费时，将生成一张唯一的发票。即使付款交易失败，该发票仍保留在账单控制台上。在账单控制台上，在按服务分列的账单详情选项卡的注册商-全球子部分下，相关账单行项目显示为 [x] 数量。

要查看免收费用的发票，请完成以下步骤：

在账单控制台上查看免收费用的发票

1. 登录 Amazon Web Services 管理控制台，然后通过以下网址打开 Amazon 账单与成本管理 控制台：https://console.aws.amazon.com/costmanagement/。
2. 在导航窗格上，选择账单。
3. 选择发票详细了解任何免收费用的发票。

要在账单控制台上查看成功的付款和退款，请完成以下步骤：

确认已成功处理的付款或退款

1. 在导航窗格中，选择 Payments（付款）。
2. 选择交易选项卡查看交易表，了解所有已完成的 Amazon 交易。

我的 Amazon 账户已关闭或永久关闭，并且我的域已注册到 Route 53

如果您关闭了 Amazon 账户，或者您的账户已关闭或永久关闭，则您的域将按程序删除：

1. 我们会每天通知您的账户已关闭，您的域将在接下来的 5 天内被暂停。
2. 您的域被暂停后，将发生以下情况：
   - 如果您的注册商是 Amazon Registrar，我们会通知您，我们将在 30 天内删除您的域。有关更多信息，请参阅 查找注册商以及有关域的其他信息。
   - 如果您的注册商是 Gandi，我们会通知您，我们将在您的账户永久关闭时将您的域释放给 Gandi。
3. 等待 30 天后，我们将删除账户中所有在 Amazon Registrar 注册的域，并向您发送更新信息。
4. 当您的账户永久关闭后，我们会将账户中所有在 Gandi 注册的域释放给 Gandi。

如果您在可以恢复域的期限内重新打开账户，我们将取消暂停您的域，或者通知您的域已被删除，但这些域或许能够被恢复。有关更多信息，请参阅 可向 Amazon Route 53 注册的域。。

> **Note**
>
> 关闭账户后 90 天后，您将无法再重新打开账户。有关更多信息，请参阅《Amazon 账户管理指南》中的关闭账户。

有关更多信息，请参阅 就域名注册问题联系 Su Amazon pport。

Amazon Route 53 服务器的 IP 地址范围

Amazon Web Services (Amazon) 以 JSON 格式发布其当前的 IP 地址范围。如果防火墙或安全组基于源 IP 地址限制传入流量，请确认您的配置允许来自适用的 IP 地址范围的流量。

要查看 Route 53 的当前 IP 地址范围，请下载 ip-ranges.json，并在文件中搜索以下值：

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

有关用于 Amazon 资源的 IP 地址范围的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon IP 地址范围。

Route 53 服务器的 IP 地址范围

`"service": "ROUTE53"` – 这些 IP 地址范围由 Route 53 名称服务器使用。如果要将 Route 53 用作一个或多个域的 DNS 服务，并且希望能够使用 `dig` 或 `nslookup` 命令来查询 Route 53 名称服务器，请将这些范围添加到允许的 IP 地址范围列表中。

> **Note**
>
> Route 53 名称服务器的 IP 地址是静态的。

Route 53 运行状况检查的 IP 地址范围

`"service": "ROUTE53_HEALTHCHECKS"` – 这些 IP 地址范围由 Route 53 运行状况检查程序使用。如果您使用 Route 53 运行状况检查来检查网络上资源的运行状况，请将这些范围添加到允许的 IP 地址范围列表中。

> **Note**
>
> 我们很少更改运行状况检查器的 IP 地址范围。监控 ip-ranges.json 文件中是否有对这些范围的任何更新。

有关用于运行状况检查的 IP 地址的更多信息，请参阅为 Amazon Route 53 运行状况检查配置路由器和防火墙规则。

引用前缀列表

前缀列表是一组可用于配置安全组的一个或多个 CIDR 块条目。用于 Amazon EC2 实例的规则的路由器和防火墙必须允许来自 Route 53 运行状况检查程序所使用 IP 地址的入站流量。引用前缀列表可以帮助您简化规则中 CIDR 块的管理。如果您经常在多个规则中使用相同的 CIDR，则可以在单个前缀列表中管理这些 CIDR，而不是在每个规则中反复引用相同的 CIDR。如果需要删除 CIDR 块，则可以从前缀列表中删除其条目，而不是从每个受影响的规则中删除 CIDR。有关前缀列表的一般更多信息，请参阅《Amazon VPC 用户指南》中的使用托管的前缀列表对 CIDR 块进行分组。

Amazon 托管的前缀列表是 Amazon 服务的 IP 地址范围集。Amazon 托管的前缀列表由 Amazon 创建和维护，并且可供拥有 Amazon 账户的任何人使用。您无法创建、修改、共享或删除Amazon托管的前缀列表。

有关 Amazon 托管的前缀列表的更多信息，请参阅《Amazon VPC 用户指南》中的使用 Amazon 托管的前缀列表。

Route 53 运行状况检查的内部 IP 地址范围

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"` – Route 53 仅在内部使用这些 IP 地址范围。您不需要将这些范围添加到允许的范围列表中。

给 Amazon Route 53 资源贴标签

标签是您分配给 Amazon 资源的标签。每个标签都由键和值组成，这两个参数都由您定义。例如，密钥可能是 “域”，值可能是 “example.com”。您可以将标签用于各种用途；一个常见的用途是对您的 Amazon Route 53 成本进行分类和跟踪。当您对 Route 53 托管区域、域和运行状况检查应用标签时， Amazon 会生成以逗号分隔值 (CSV) 文件形式的成本分配报告，其中包含按标签汇总的使用量和成本。您可以设置代表业务类别（例如成本中心、应用程序名称或所有者）的标签，以便整理多种服务的成本。有关对成本分配使用标签的更多信息，请参阅《Amazon Billing 用户指南》https://docs.amazonaws.cn/awsaccountbilling/latest/aboutv2/中的使用成本分配标签。

为了便于使用并获得最佳效果，请使用中的标签编辑器 Amazon Web Services 管理控制台，它提供了一种集中、统一的方式来创建和管理标签。有关更多信息，请参阅 Amazon Web Services 管理控制台入门中的使用标签编辑器。您还可以使用 Route 53 控制台对某些资源应用标签：

- 运行状况检查 - 有关更多信息，请参阅 为运行状况检查命名和添加标签。
- Route 53 VPC 解析器入站终端节点 — 有关更多信息，请参阅创建或编辑入站端点时指定的值。
- Resolver 出站终端节点 - 有关更多信息，请参阅 创建或编辑出站端点时指定的值。
- Resolver 规则 - 有关更多信息，请参阅 创建或编辑规则时指定的值。
- 托管区 – 有关更多信息，请参阅 使用托管区域。

> **Note**
>
> 解析器终端节点的费用按照 VPC 解析器网络接口分配。由于目前无法标记 VPC Resolver 网络接口，因此解析器终端节点目前不支持基于标签的成本分配。有关 VPC Resolver 定价的信息，请参阅 Amazon Route 53 定价。

您也可以通过使用 Route 53 API 将标签应用于资源。有关更多信息，请参阅 Amazon Route 53 API 参考中的按功能划分的 Route 53 API 操作主题中与标签有关的操作。

教程

本节涵盖以下教程：

Route 53 用作子域的 DNS 服务

了解如何使用 Route 53 作为新子域或现有子域的 DNS 服务，并仍然对父域使用其它 DNS 服务。

转换到基于延迟的路由

了解如何在 Route 53 中逐步从标准路由迁移到基于延迟的路由，并将用户定向到延迟最低的可用 Amazon 端点。

将加权记录和延迟记录结合起来，实现平稳、低风险的转换，并具有完全的控制和回滚功能。

将另一个区域添加到基于延迟的路由

通过添加新的 Amazon 区域并逐步将流量转移到新区域，扩展基于延迟的路由设置。

将流量路由到一个区域中的多个 Amazon EC2 实例

使用延迟记录和加权记录的组合，将流量路由到一个特定 Amazon Web Services 区域中的多个 Amazon EC2 实例。

管理超过 100 个加权记录

学习如何通过创建加权别名记录和加权记录树，将流量定向到 100 多个端点。

对容错多记录应答进行加权

了解如何对包含多条记录的 DNS 响应进行加权，从而在多个端点之间提供容错和负载均衡。

这些教程涵盖了各种使用案例和场景，它们有助于您有效地利用 Route 53 的路由策略、加权记录和基于延迟的路由来优化 DNS 管理和流量路由。

主题

使用 Amazon Route 53 作为子域的 DNS 服务，但不迁移父域

Amazon Route 53 可以灵活管理子域的 DNS，您无需迁移整个父域即可利用其功能。

您可以创建新的子域或将现有子域迁移到 Route 53，同时使父域继续托管在其他 DNS 服务提供商处。

使用 Route 53 创建新的子域：

1. 为新子域创建托管区。
2. 将子域所需的 DNS 记录（例如 A、CNAME、MX）添加到托管区。
3. 获取分配给托管区的 Route 53 名称服务器。
4. 添加指向 Route 53 名称服务器的子域的 NS（名称服务器）记录，更新父域的 DNS 配置。

将现有子域迁移到 Route 53：

1. 为子域创建托管区域。
2. 从现有 DNS 服务提供商处获取子域的当前 DNS 配置。
3. 将相应的 DNS 记录添加到托管区。
4. 获取分配给托管区的 Route 53 名称服务器。
5. 添加指向 Route 53 名称服务器的子域的 NS 记录，更新父域的 DNS 配置。

通过执行这些步骤，就可以为子域利用运行状况检查、路由策略和流量管理等 Route 53 高级功能，同时维持父域在现有提供商处的 DNS 配置。

主题

创建使用 Amazon Route 53 作为 DNS 服务的子域，但不迁移父域

您可以创建一个使用 Amazon Route 53 作为 DNS 服务的子域而无需从另一个 DNS 服务迁移父域。

此过程有以下基本步骤：

1. 弄清您是否应使用此过程。
2. 为子域创建 Route 53 托管区域。

3. 将新子域的记录添加到您的 Route 53 托管区域。
4. 仅 API：确认您的更改已传播到所有 Route 53 DNS 服务器。

> **Note**
>
> 目前，验证更改是否已传播的唯一方式是使用 GetChange API 操作。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

5. 添加子域的名称服务器记录，从而更新父域的 DNS 服务。

确定使用哪些过程来创建子域

本主题中的过程说明如何执行不常见的操作。如果您已经在使用 Route 53 作为域的 DNS 服务，并且仅希望将某个子域（例如 www.example.com）的流量路由到您的资源（例如，运行在 EC2 实例上的 Web 服务器），请参阅 路由子域的流量。

仅当您在在某个域（如 example.com）使用其它 DNS 服务，并且您希望开始为该域的新子域使用 Route 53 作为 DNS 服务（例如 www.example.com）时才使用此过程。

为新的子域创建托管区域

如果您想使用 Amazon Route 53 作为新子域的 DNS 服务但不想迁移父域时，必须先为子域创建一个托管区域。Route 53 将有关您的子域的信息存储到托管区域中。

有关如何使用 Route 53 控制台创建托管区域的信息，请参阅 创建公有托管区域。

创建记录

您可以使用 Amazon Route 53 控制台或 Route 53 API 创建记录。在您向 Route 53 委派子域责任后，在 Route 53 中创建的记录将成为 DNS 所使用的记录，具体解释见本过程稍后的 用子域的名称服务器记录更新 DNS 服务。

> **Important**
>
> 请勿在 Route 53 托管区域中创建其它名称服务器 (NS) 或授权起始点 (SOA) 记录，且请勿删除现有的 NS 和 SOA 记录。

要使用 Route 53 控制台创建记录，请参阅 使用记录。要使用 Route 53 API 创建记录，请使用 ChangeResourceRecordSets。有关更多信息，请参阅 Amazon Route 53 API 参考中的 ChangeResourceRecordSets。

检查更改状态（仅限 API）

创建新的托管区域和更改记录需要一定时间才能传播到 Route 53 DNS 服务器。如果您使用 ChangeResourceRecordSets 创建记录，则可以使用 GetChange 操作确定更改是否已传播。（(ChangeResourceRecordSets 返回 ChangeId 的值，您可将该值包含在后续的 GetChange 请求中。如果您使用控制台创建记录，则 ChangeId 不可用。）有关更多信息，请参阅 Amazon Route 53 API 参考中的 GET GetChange。

> **Note**
>
> 更改通常在 60 秒内传播到所有 Route 53 名称服务器。

用子域的名称服务器记录更新 DNS 服务

对 Amazon Route 53 记录的更改传播后（请参阅 检查更改状态（仅限 API）），请添加子域的 NS 记录来更新父域的 DNS 服务。这称为向 Route 53 委派子域的责任。例如，如果父域 example.com 通过另一个 DNS 服务托管，并且您在 Route 53 中创建了子域 test.example.com，则必须使用 test.example.com 的新 NS 记录更新 example.com 的 DNS 服务。

请执行以下过程。

1. 使用您的 DNS 服务提供的方法备份父域的区域文件。
2. 在 Route 53 控制台中，获取您的 Route 53 托管区域的名称服务器：
   a. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
   b. 在导航窗格中，选择 Hosted zones（托管区域）。
   c. 在 Hosted zones（托管区域）页面上，选择托管区域的单选按钮（不是名称），然后选择 View details（查看详细信息）。
   d. 在托管区域的详细信息页面上，选择 Hosted zone details（托管区域详细信息）。
   e. 记下为 Name servers（名称服务器）列出的四台服务器。

此外，也可以使用 GetHostedZone 操作。有关更多信息，请参阅 Amazon Route 53 API 参考中的 GetHostedZone。

3. 使用父域的 DNS 服务提供的方法，将子域的 NS 记录添加到父域的区域文件。在这些 NS 记录中，指定四个与您在步骤 1 中创建的托管区域关联的 Route 53 名称服务器。

> **Important**
>
> 不要将授权起始点 (SOA) 记录添加到父域的区域文件中。因为子域将使用 Route 53，父域的 DNS 服务对子域不具权限。
> 如果您的 DNS 服务为子域自动添加了一个 SOA 记录，请删除子域的该记录。但是，不要删除父域的该 SOA 记录。

将子域的 DNS 服务迁移到 Amazon Route 53，但不迁移父域

您可以迁移一个子域以便使用 Amazon Route 53 作为 DNS 服务，而无需从另一个 DNS 服务迁移父域。

此过程有以下基本步骤：

1. 弄清您是否应使用此过程。
2. 为子域创建 Route 53 托管区域。
3. 从父域的当前 DNS 服务提供商那里获取当前 DNS 配置。
4. 将子域的记录添加到您的 Route 53 托管区域。
5. 仅 API：确认您的更改已传播到所有 Route 53 DNS 服务器。

> **Note**
>
> 目前，验证更改是否已传播的唯一方式是使用 GetChange API 操作。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

6. 添加子域的名称服务器记录，更新父域的 DNS 服务提供商的 DNS 配置。

确定使用哪些过程来创建子域

本主题中的过程说明如何执行不常见的操作。如果您已经在使用 Route 53 作为域的 DNS 服务，并且仅希望将某个子域（例如 www.example.com）的流量路由到您的资源（例如，运行在 EC2 实例上的 Web 服务器），请参阅 路由子域的流量。

仅当您在在某个域（如 example.com）使用其它 DNS 服务，并且您希望开始为该域的现有子域使用 Route 53 作为 DNS 服务（例如 www.example.com）时才使用此过程。

为子域创建托管区域

如果您想将子域从另一个 DNS 服务迁移到 Amazon Route 53，但不想迁移父域，则可以首先为子域创建一个托管区域。Route 53 将有关您的子域的信息存储到托管区域中。

有关如何使用 Route 53 控制台创建托管区域的信息，请参阅 创建公有托管区域。

从 DNS 服务提供商那里获取当前的 DNS 配置

为了简化将现有子域迁移到 Route 53 的过程，请从当前为域提供服务的 DNS 服务提供商那里获取域的当前 DNS 配置。您可以根据此信息将 Route 53 配置为子域的 DNS 服务。

您要求的内容和格式取决于您目前正在使用哪家公司作为您的 DNS 服务提供商。理想情况下，它们将为您提供一个区域文件，其中包含有关当前配置中所有记录的信息。（记录会告知 DNS 您希望如何针对您的域和子域路由流量。例如，有人在 Web 浏览器中输入您的域名时，您是希望将流量路由到您数据中心中的 Web 服务器、Amazon EC2 实例、CloudFront 分配，还是其它某个位置？）如果您可以从当前 DNS 服务提供商那里获取区域文件，可以编辑区域文件，删除您不想迁移到 Amazon Route 53 的记录。然后，将其余的记录导入您的 Route 53 托管区域，从而大大简化该过程。尝试询问您的当前 DNS 服务提供商的客户支持，如何获取区域文件或记录列表。

创建记录

以您从当前 DNS 服务提供商那里获取的记录作为起点，在为子域创建的 Amazon Route 53 托管区域中创建相应的记录。在您向 Route 53 委派子域责任后，在 Route 53 中创建的记录将成为 DNS 所使用的记录，具体解释见本过程稍后的 用子域的名称服务器记录更新 DNS 服务。

> **Important**
>
> 请勿在 Route 53 托管区域中创建其它名称服务器 (NS) 或授权起始点 (SOA) 记录，且请勿删除现有的 NS 和 SOA 记录。

要使用 Route 53 控制台创建记录，请参阅 使用记录。要使用 Route 53 API 创建记录，请使用 ChangeResourceRecordSets。有关更多信息，请参阅 Amazon Route 53 API 参考中的 ChangeResourceRecordSets。

检查更改状态（仅限 API）

创建新的托管区域和更改记录需要一定时间才能传播到 Route 53 DNS 服务器。如果您使用 ChangeResourceRecordSets 创建记录，则可以使用 GetChange 操作确定更改是否已传播。（ChangeResourceRecordSets 返回 ChangeId 的值，您可将该值包含在后续的 GetChange 请求中。如果您使用控制台创建记录，则 ChangeId 不可用。）有关更多信息，请参阅 Amazon Route 53 API 参考中的 GET GetChange。

> **Note**
>
> 更改通常在 60 秒内传播到所有 Route 53 名称服务器。

用子域的名称服务器记录更新 DNS 服务

对 Amazon Route 53 记录的更改传播后（请参阅 检查更改状态（仅限 API）），请添加子域的 NS 记录来更新父域的 DNS 服务。这称为向 Route 53 委派子域的责任。例如，假设父域 example.com 通过另一个 DNS 服务托管，而您要将子域 test.example.com 迁移到 Route 53。您必须为 test.example.com 创建一个托管区域，并使用 Route 53 分配给 test.example.com 的新托管区域的 NS 记录更新 example.com 的 DNS 服务。

请执行以下过程。

1. 使用您的 DNS 服务提供的方法备份父域的区域文件。
2. 如果域以前的 DNS 服务提供商有办法为其名称服务器更改 TTL 设置，则我们建议您将设置改为 900 秒。这样会限制客户端请求尝试使用过时的名称服务器来解析域名的时间。如果当前 TTL 是 172800 秒 (两天，这是常见的默认设置)，则您仍需要等待两天，解析程序和客户端才能停止使用以前的 TTL 缓存 DNS 记录。TTL 设置到期后，您可以安全地删除存储于先前的提供商的记录，并仅对 Route 53 进行更改。
3. 在 Route 53 控制台中，获取您的 Route 53 托管区域的名称服务器：
   a. 登录 Amazon Web Services 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
   b. 在导航窗格中，选择 Hosted zones（托管区域）。

c. 在 Hosted zones（托管区域）页面上，选择托管区域的单选按钮（不是名称），然后选择 View details（查看详细信息）。

d. 在托管区域的详细信息页面上，选择 Hosted zone details（托管区域详细信息）。

e. 记下为 Name servers（名称服务器）列出的四台服务器。

此外，也可以使用 `GetHostedZone` 操作。有关更多信息，请参阅 Amazon Route 53 API 参考中的 GetHostedZone。

4. 使用父域的 DNS 服务提供的方法，将子域的 NS 记录添加到父域的区域文件。为 NS 记录指定与子域相同的名称。对于 NS 记录中的值，指定四个与您在步骤 2 中创建的托管区域关联的 Route 53 名称服务器。请注意，不同的 DNS 服务使用不同的术语。您可能需要联系您的 DNS 服务技术支持来了解如何执行此步骤。

> **Important**
>
> 不要将授权起始点 (SOA) 记录添加到父域的区域文件中。因为子域将使用 Route 53，父域的 DNS 服务对子域不具权限。
> 如果您的 DNS 服务为子域自动添加了一个 SOA 记录，请删除子域的该记录。但是，不要删除父域的该 SOA 记录。

根据父域的名称服务器的 TTL 设置的不同，传播对 DNS 解析程序的更改可能需要 48 小时或更长的时间。在此期间，DNS 解析程序可能仍使用父域 DNS 服务的名称服务器应答请求。此外，客户端计算机的缓存中可能还是子域以前的名称服务器。

5. 在域注册商的 TTL 设置到期后 (请参阅步骤 2)，从父域的区域文件中删除以下记录：

- 您添加到 Route 53 中的记录，如 创建记录 中所述。
- 您的 DNS 服务的 NS 记录。当您完成删除以上 NS 记录后，区域文件中仅有的 NS 记录将是您在步骤 4 中创建的 NS 记录。

在 Amazon Route 53 中转换到基于延迟的路由

利用基于延迟的路由，Amazon Route 53 可以将您的用户定向到延迟最低的可用 Amazon 终端节点。例如，您可能将 `www.example.com` 这样的 DNS 名称与在美国东部（俄亥俄）和欧洲（爱尔兰）区域中托管的 ELB 经典负载均衡器、Application Load Balancer 或网络负载均衡器、Amazon EC2 实例或弹性 IP 地址关联。Route 53 DNS 服务器根据过去几周的网络条件判断，哪些区域中的哪些

实例应服务于特定用户。一个在伦敦的用户很可能被定向到欧洲（爱尔兰）实例，而一个在芝加哥的用户很可能被定向到美国东部（俄亥俄）实例，依此类推。Route 53 支持将基于延迟的路由用于 A、AAAA、TXT 和 CNAME 记录，也支持将别名用于 A 和 AAAA 记录。

> **Note**
>
> 有关用户与您的资源之间延迟的数据完全基于用户与 Amazon 数据中心之间的流量。如果您未使用 Amazon 区域中的资源，则用户与资源之间的实际延迟可能与 Amazon 延迟数据有很大差异。即使您的资源与 Amazon 区域位于同一城市，也是如此。

为实现顺利、低风险的过渡，您可以组合加权与延迟记录，逐渐从标准路由迁移到在每个阶段都具有完全控制和回滚能力的基于延迟的路由。让我们来考虑一个示例，其中 www.example.com 目前托管在美国东部（俄亥俄）区域中的一个 Amazon EC2 实例上。该实例具有弹性 IP 地址 W.W.W.W。假设您要继续将流量路由到美国东部（俄亥俄）区域（如果适用），同时也开始将用户定向到美国西部（加利福尼亚北部）区域（弹性 IP X.X.X.X）和欧洲（爱尔兰）区域（弹性 IP Y.Y.Y.Y）中的其它 Amazon EC2 实例。example.com 的 Route 53 托管区域已经有 www.example.com 的一个记录，其 Type（类型）为 A，Value（值）（IP 地址）为 W.W.W.W。

完成下面的示例后，您将拥有两个加权别名记录：

- 将 www.example.com 的现有记录转换为加权别名记录，以继续将大部分流量定向到美国东部（俄亥俄）区域中的现有 Amazon EC2 实例。
- 您创建另一个加权别名记录，该记录最初只将一小部分流量定向到延迟记录，后者再将流量路由到所有三个区域。

通过更新这些加权别名记录中的权重，您可以逐渐从将流量仅路由到美国东部（俄亥俄）区域，转变为将流量路由到具有 Amazon EC2 实例的所有三个区域。

转换到基于延迟的路由

1. 制作 www.example.com 记录的副本，但使用新的域名，例如，copy-www.example.com。为新记录指定与 的记录相同的 Type (A) 和 ValueW.W.W.W (www.example.com)。
2. 更新 www.example.com 的现有 A 记录，使其成为一个加权别名记录：
   - 对于 Value/Route traffic to（值/流量路由至），选择 Alias to another record in this hosted zone（此托管区域中另一条记录的别名），然后指定 copy-www.example.com。
   - 对于 Weight（权重），请指定 100。

完成更新后，Route 53 会继续使用此记录将所有流量路由到 IP 地址为 W.W.W.W 的资源。

3. 为每个 Amazon EC2 实例创建延迟记录，例如：

   - 美国东部（俄亥俄），弹性 IP 地址 W.W.W.W
   - 美国西部（加利福尼亚北部），弹性 IP 地址 X.X.X.X
   - 欧洲（爱尔兰），弹性 IP 地址 Y.Y.Y.Y

   为所有延迟记录指定相同的域名 (如 www-lbr.example.com) 和相同的类型 A。

   延迟记录创建完毕后，Route 53 会继续使用您在步骤 2 中更新的记录路由流量。

   您可以使用 www-lbr.example.com 来执行诸如验证测试等工作，以确保每个终端节点可以接受请求。

4. 现在，我们来将 www-lbr.example.com 延迟记录添加到 www.example.com 加权记录，并开始将有限的流量路由到相应的 Amazon EC2 实例。这意味着美国东部（俄亥俄）区域中的 Amazon EC2 实例将从两个加权记录获得流量。

   为 www.example.com 创建另一个加权别名记录：

   - 对于 Value/Route traffic to（值/流量路由至），选择 Alias to another record in this hosted zone（此托管区域中另一条记录的别名），然后指定 www-lbr.example.com.
   - 对于 Weight（权重），请指定 1。

   当您完成以上工作并且您的更改同步到 Route 53 服务器后，Route 53 开始将极少一部分流量 (1/101) 路由到您在步骤 3 中为其创建了延迟记录的 Amazon EC2 实例。

5. 当您确信您的终端节点为传入流量进行了适当的扩展时，应相应地调整权重。例如，如果您希望 10% 的请求以基于延迟的路由为基础，则将权重分别改为 90 和 10。

有关创建延迟记录的更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

在 Amazon Route 53 中将另一个区域添加到基于延迟的路由

如果您在使用基于延迟的路由，并且希望在新区域中添加实例，可以将流量逐渐转移到新区域，采用的方式与 在 Amazon Route 53 中转换到基于延迟的路由 中介绍的将流量逐渐转移到基于延迟的路由方式相同。

例如，假设您使用基于延迟的路由来路由 www.example.com 的流量，并且希望将亚太地区（东京）中的 Amazon EC2 实例添加到美国东部（俄亥俄）、美国西部（加利福尼亚北部）和欧洲（爱尔兰）中的实例。以下示例过程介绍了一种在另一个区域中添加实例的方法。

对于本例，example.com 的 Amazon Route 53 托管区域已经拥有 www.example.com 的一个加权别名记录，可将流量路由到 www-lbr.example.com 的基于延迟的记录：

- 美国东部（俄亥俄），弹性 IP 地址 W.W.W.W
- 美国西部（加利福尼亚北部），弹性 IP 地址 X.X.X.X
- 欧洲（爱尔兰），弹性 IP 地址 Y.Y.Y.Y

该加权别名记录的权重为 100。当您过渡到基于延迟的路由后，假定您删除了用于过渡的其他加权记录。

在 Route 53 中将另一个区域添加到基于延迟的路由

1. 创建四个新的基于延迟的记录，其中三个为原始区域，以及一个您要开始向其中路由流量的新区域。

   - 美国东部（俄亥俄），弹性 IP 地址 W.W.W.W
   - 美国西部（加利福尼亚北部），弹性 IP 地址 X.X.X.X
   - 欧洲（爱尔兰），弹性 IP 地址 Y.Y.Y.Y
   - 亚太地区（东京），弹性 IP 地址 Z.Z.Z.Z

   为所有延迟记录指定相同的新域名 (如 www-lbr-2012-04-30.example.com) 和相同的类型 A。

   延迟记录创建完毕后，Route 53 会继续使用原始加权别名记录 (www.example.com) 和延迟记录 (www-lbr.example.com) 路由流量。

   您可以使用 www-lbr-2012-04-30.example.com 记录来执行诸如验证测试等工作，以确保每个终端节点都可以接受请求。
2. 为新的延迟记录创建加权别名记录：

   - 对于域名，指定现有加权别名记录 www.example.com 的名称。

- 对于 Value/Route traffic to（值/流量路由至），选择 Alias to another record in this hosted zone（此托管区域中另一条记录的别名），然后指定 `www-lbr-2012-04-30.example.com`。
- 对于 Weight（权重），请指定 1。

完成以上工作后，Route 53 开始将极少一部分流量 (1/101) 路由到您在步骤 1 中为其创建了 `www-lbr-2012-04-30.example.com` 延迟记录的 Amazon EC2 实例。剩下的流量将继续路由到 `www-lbr.example.com` 延迟记录，其中不包括亚太地区（东京）区域中的 Amazon EC2 实例。

3. 当您确信您的终端节点为传入流量进行了适当的扩展时，应相应地调整权重。例如，如果您希望有 10% 的请求路由到包括东京区域的延迟记录，则将 `www-lbr.example.com` 的权重从 100 改为 90，将 `www-lbr-2012-04-30.example.com` 的权重从 1 改为 10。

有关创建记录的更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

在 Amazon Route 53 中使用延迟和加权记录将流量路由到一个区域中的多个 Amazon EC2 实例

如果您的应用程序在两个或更多 Amazon EC2 区域的 Amazon EC2 实例上运行，并且您在一个或多个区域有多个 Amazon EC2 实例，则可以使用基于延迟的路由将流量路由到正确的区域，然后使用加权记录并基于您指定的加权将流量路由到区域内的实例中。

例如，假设您在美国东部（俄亥俄）区域有三个具有弹性 IP 地址的 Amazon EC2 实例，并且您希望针对用户（美国东部 [俄亥俄] 是其适当区域）在所有三个 IP 之间均匀分配请求。在其它区域一个 Amazon EC2 实例就足够，但其实您可以同时对多个区域应用相同的方法。

在 Amazon Route 53 中使用延迟和加权记录将流量路由到一个区域中的多个 Amazon EC2 实例

1. 为区域中的 Amazon EC2 实例创建一组加权记录。请注意以下几点：

   - 为每个加权记录指定相同的 Record name（记录名称）值（如 `us-east.example.com`）和 Record type（记录类型）。
   - 对于 Value/Route traffic to（值/流量路由至），选择 IP address or another value depending on the record type（根据记录类型的 IP 地址或其它值），然后指定弹性 IP 地址之一的值。
   - 如果您希望平等地对 Amazon EC2 实例进行加权，则为 Weight（权重）指定相同的值。
   - 对于集 ID，为每个记录指定唯一值。

有关加权记录值的更多信息，请参阅 加权路由。

2. 如果您在其它区域有多个 Amazon EC2 实例，则对其它区域重复步骤 1。在每个区域中，指定不同的 Name 值。
3. 如果您在某个区域中拥有多个 Amazon EC2 实例（如美国东部 [俄亥俄]），请创建一个延迟别名记录。对于值/流量路由至，选择此托管区域中另一个记录的别名，然后指定您分配给该区域中加权记录的记录名称字段中的值（例如，`us-east.example.com`）。
4. 如果您在某个区域中拥有一个 Amazon EC2 实例，请创建一个延迟记录。对于 Record name（记录名称），指定与您在步骤 3 中创建的延迟别名记录相同的值。对于 Value/Route traffic to（值/流量路由至），选择 IP address or another value depending on the record type（根据记录类型的 IP 地址或其它值），然后指定该区域中 Amazon EC2 实例的弹性 IP 地址。

   有关向 Amazon EC2 实例添加别名记录的更多信息，请参阅 将流量路由到 Amazon EC2 实例

有关创建记录的更多信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。

在 Amazon Route 53 中管理超过 100 个加权记录

Amazon Route 53 允许您配置加权记录。对于给定名称和类型 (如 `www.example.com`，类型 A)，您可以配置多达 100 个替代响应，且每个响应都有自己的权重。在响应对 `www.example.com` 的查询时，Route 53 DNS 服务器会选择一个加权随机响应来返回给 DNS 解析程序。将返回权重为 2 的加权记录的值，而且平均来讲，其返回频率是权重为 1 的加权记录的值的两倍。

如果您需要将流量定向到超过 100 个终端节点，则实现此目标的一种方式是使用加权别名记录和加权记录树。例如，树的第一个“级别”最多可以包含 100 个加权别名记录，而每个加权别名记录又可以指向最多 100 个加权记录。Route 53 允许最多三级递归，因此您可以管理多达 100 万个唯一加权终端节点。

一个简单的二级树可能看起来像下面这样：

加权别名记录

- `www.example.com` 的 `www-a.example.com` 别名，权重为 1
- `www.example.com` 的 `www-b.example.com` 别名，权重为 1

加权记录

- www-a.example.com，类型 A，值 192.0.2.1，权重 1
- www-a.example.com，类型 A，值 192.0.2.2，权重 1

- www-b.example.com，类型 A，值 192.0.2.3，权重 1
- www-b.example.com，类型 A，值 192.0.2.4，权重 1

有关创建记录的更多信息，请参阅 使用记录。

在 Amazon Route 53 中对容错多记录应答进行加权

> **Note**
>
> 使用多值应答路由策略的记录的行为方式与本教程中记录的配置的行为方式非常相似。主要区别在于，教程中的配置允许您指定权重，这在您的终端节点具有不同容量时很有用。有关更多信息，请参阅 多值应答路由。

一个 Amazon Route 53 加权记录只能与一个记录关联，即一个名称（如 example.com）与一个记录类型（如 A）的组合。但是，通常需要对包含多个记录的 DNS 响应进行加权。

例如，对于一个服务，您可能有八个 Amazon EC2 实例或弹性 IP 终端节点。如果该服务的客户端支持连接重试 (就像所有常见的浏览器一样)，则在 DNS 响应中提供多个 IP 地址会在任何特定终端节点发生故障时为这些客户端提供可选的终端节点。如果将响应配置为包含两个或多个可用区中托管的 IP 的组合，您甚至可以防范可用区故障。

当大量客户端 (如移动 Web 应用程序) 共享一小组 DNS 缓存时，多记录应答也十分有用。在这种情况下，多记录应答允许客户端将请求定向到多个终端节点，即使客户端从共享缓存收到通用 DNS 响应。

通过使用记录与加权别名记录的组合，可以实现这些类型的加权多记录应答。您可以将八个终端节点分为两组不同的记录集，每组包含四个 IP 地址：

endpoint-a.example.com，类型 A，具有下列值：

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

endpoint-b.example.com，类型 A，具有下列值：

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

然后，您可以创建指向每个组的加权别名记录：

- www.example.com 的 endpoint-a.example.com 别名，类型 A，权重为 1
- www.example.com 的 endpoint-b.example.com 别名，类型 A，权重为 1

有关创建记录的更多信息，请参阅 使用记录。

Amazon Route 53 的最佳实践

本节提供了 Amazon Route 53 各个组件的最佳实践，包括：

1. DNS 最佳实践：
   - 了解生存时间 (TTL) 值和响应能力与可靠性之间的权衡取舍。
   - 尽可能使用别名记录代替 CNAME 记录，以提高性能并节省成本。
   - 配置默认路由策略，确保所有客户端都能收到响应。
   - 利用基于延迟的路由来最大限度地减少应用程序延迟，利用 geolocation/geoproximity 路由来实现稳定性和可预测性。
   - 使用面向自动化工作流程的 GetChange API 验证更改的传播。
   - 委托来自父区域的子域以实现一致的路由。
   - 使用多值应答路由，避免大量的单一响应。
2. Resolver 最佳实践：
   - 通过避免同一 VPC 同时与 Resolver 规则及其入站端点相关联来防止路由循环。
   - 实施安全组规则以减少连接跟踪开销，并最大程度地提高查询吞吐量。
   - 配置入站端点，采用多个可用区中的 IP 地址以实现冗余。
   - 请注意潜在的 DNS 区域行走攻击，如果您的终端遇到限制，请联系 Su Amazon pport。
3. 运行状况检查最佳实践：
   - 遵循有关优化 Amazon Route 53 运行状况检查的建议，确保可靠监控资源

通过遵循这些最佳实践，就可以优化 DNS 基础设施的性能、可靠性和安全性，确保将流量高效地路由到应用程序和服务

主题

Amazon Route 53 DNS 的最佳实践

使用 Amazon Route 53 DNS 服务时，请遵循以下最佳实践来获得最佳结果。

使用数据层面功能进行 DNS 故障转移和应用恢复

Route 53 的数据层面（包括运行状况检查和 Amazon 应用程序恢复控制器 (ARC) 路由控制在全球范围内分布，旨在于存在严重事件时依然能够实现 100% 的可用性和功能性。它们彼此集成，不依赖于控制面板的功能。虽然这些服务（包括其控制台）的控制面板通常非常可靠，但它们的设计方式更集中，且会优先考虑持久性和一致性，而不是高可用性。对于灾难恢复期间的失效转移等方案，我们建议您使用 Route 53 运行状况检查和 ARC 路由控制之类的功能，这些功能将依赖数据面板功能来更新 DNS。有关更多信息，请参阅控制和数据层面概念和博客：使用 Amazon Route 53 创建灾难恢复机制。

为 DNS 记录选择 TTL 值

DNS TTL 是数字值（以秒为单位），DNS 解析器用于决定在不对 Route 53 进行另一次查询的情况下，记录可以缓存的时长。必须为所有 DNS 记录指定 TTL。TTL 值的推荐范围为 60 到 172,800 秒。

选择 TTL 就是在延迟和可靠性以及对变化的响应能力之间进行权衡。由于记录时间较短 TTLs ，DNS 解析器会更快地注意到记录的更新，因为他们必须更频繁地进行查询。这会增加查询量（和成本）。随着 TTL 不断延长，DNS 解析器会更频繁地应答缓存中的查询，这样的操作通常更快、更便宜，且在某些情况下更可靠，因为它避免了在互联网上开展的查询。没有所谓正确的选择，但您可以考虑是响应性还是可靠性对您而言更重要。

设置 TTL 值时要考虑的事项包括：

- 将 DNS 记录设置 TTLs 为您可以承受的等待更改生效的时间长度。对于委派（NS 记录集）或其他很少更改的记录（例如 MX 记录）而言，情况尤其如此。对于这些记录，建议使用 TTLs 更长的时间。1 小时（3600 秒）和 1 天（86,400 秒）之间的值是较为常见的选择。
- 对于需要作为快速故障转移机制的一部分进行更改的记录（尤其是经过健康检查的记录），较低的值 TTLs是合适的。在这种情况下，通常选择将 TTL 设置为 60 秒或 120 秒。
- 当您要更改关键 DNS 条目时，我们建议您暂时缩短 TTLs。如果需要，您随后可以快速进行更改、观察和回滚。在更改完成并按预期工作后，您可以增加 TTL。

有关更多信息，请参阅 TTL（秒）。

CNAME 记录

DNS CNAME 记录是一种将一个域名指向另一个域名的方法。如果 DNS 解析器解析了 domain-1.example.com 并找到指向 domain-2.example.com 的别名记录，则 DNS 解析器必须继续解析 domain-2.example.com，然后才能响应。这些记录适用于许多情况，例如当网站拥有多个域名时确保一致性。

但是，DNS 解析器必须进行更多查询才能回答 CNAMEs，这会增加延迟和成本。在可能的情况下，使用 Route 53 别名记录是一种速度更快、价格更低的替代方案。别名记录允许 Route 53 对 Amazon 资源（例如负载均衡器）和同一托管区域内的其他域直接做出响应。

有关更多信息，请参阅 将互联网流量路由到您的 Amazon 资源。

高级 DNS 路由

- 使用地理位置、地理邻近或基于延迟的路由时，请始终设置默认值，除非您希望某些客户端接收没有应答的响应。
- 为了尽量减少应用程序延迟，请使用基于延迟的路由。这种类型的路由数据可能会经常更改。
- 要确保路由稳定性和可预测性，请使用地理位置或地理邻近路由。

有关更多信息，请参阅 地理位置路由、地理位置临近度路由 和 基于延迟的路由。

DNS 更改传播

当您使用 Route 53 控制台或 API 创建或更新记录或托管区域时，更改需要一段时间才能在互联网上反映出来。这被称为更改传播。尽管在全球范围内的传播通常不到一分钟，但偶尔会出现延迟，例如由于同步到一个位置的问题，或者在极少数情况下由于中央控制面板内出现问题。如果您正在构建自动配置工作流程，并且必须等待变更传播完成后再继续下一个工作流程步骤，请使用 GetChangeAPI 验证您的 DNS 更改是否已生效（`Status =INSYNC`）。

DNS 委派

当您在 DNS 中委派多个级别的子域时，始终从父区域委派非常重要。例如，如果您正在委派 www.dept.example.com，则应该从 dept.example.com 区域执行，而不是从 example.com 区域执行。从祖父区域到子区域的委派可能根本无法正常工作，也可能仅以不一致的方式工作。有关更多信息，请参阅 路由子域的流量。

DNS 响应的大小

避免创建大型单个响应。如果响应大于 512 字节，则许多 DNS 解析器必须通过 TCP 而不是 UDP 重试，这会降低可靠性并导致响应速度变慢。我们建议使用多值应答路由，它将选择 8 个运行正常的随机 IP 来将响应保持在 512 字节边界内。

有关更多信息，请参阅 多值应答路由 和 DNS 回包大小测试服务器。

VPC 解析器的最佳实践

本节提供优化 Amazon Route 53 VPC 解析器的最佳实践，涵盖以下主题：

1. 避免使用 Resolver 端点循环配置：
   - 确保同一 VPC 不会同时与 Resolver 规则及其入站端点相关联，从而防止路由循环。
   - 利用 Amazon RAM 它在账户 VPCs 之间共享，同时保持正确的路由配置。

   有关更多信息，请参阅 避免使用 Resolver 端点循环配置。
2. Resolver 端点扩展：
   - 实施根据连接状态允许通信的安全组规则，以减少连接跟踪开销
   - 遵循针对入站和出站 Resolver 端点的推荐安全组规则，最大程度地提高查询吞吐量。
   - 监控生成 DNS 流量的唯一 IP 地址和端口组合，避免出现容量限制。

   有关更多信息，请参阅 Resolver 端点扩展。
3. Resolver 端点的高可用性：
   - 创建入站端点，采用至少两个可用区中的 IP 地址以实现冗余。
   - 配置额外的网络接口，以确保维护或流量激增期间的可用性

   有关更多信息，请参阅 解析程序端点的高可用性 。
4. 防止 DNS 区域步行攻击：
   - 注意潜在的 DNS 区域步行攻击，攻击者会试图从 DNSSEC 签名的 DNS 区域检索所有内容。
   - 如果您的终端由于怀疑区域行走而出现限流，请联系 Support Amazon 寻求帮助。

   有关更多信息，请参阅 DNS 区域步行 。

通过遵循这些最佳实践，您可以优化 VPC Resolver 部署的性能、可扩展性和安全性，从而确保您的应用程序和资源可靠、高效地解析 DNS。

避免使用 Resolver 端点循环配置

不要将同一 VPC 与 Resolver 规则及其入站端点关联（无论它是端点的直接目标，还是通过本地部署 DNS 服务器）。当 Resolver 规则中的出站端点指向与规则共享 VPC 的入站端点时，可能会导致一个循环，其中查询在入站和出站端点之间持续传递。

仍然可以使用 Amazon Resource Access Manager (Amazon RAM) 将转发规则与其他 VPCs 账户共享的转发规则相关联。与中心关联的私有托管区域（或中央 VPC）仍将从查询解析到入站端点，因为转发解析程序规则不会更改此分辨率。

Resolver 端点扩展

Resolver 端点安全组使用连接跟踪来收集有关进出端点的流量信息。每个端点接口都具有可跟踪的最大连接数，并且大量 DNS 查询可能会超过连接，从而导致节流和查询丢失。连接跟踪 Amazon是监控流经安全组的流量状态的默认行为（SGs）。在中使用连接跟踪 SGs 会降低流量的吞吐量，但是，您可以实现未跟踪的连接以减少开销并提高性能。有关更多信息，请参阅未跟踪的连接。

如果使用限制性安全组规则强制执行连接跟踪，或者通过网络负载均衡器路由查询（请参阅自动跟踪的连接），则对于一个端点来说，每个 IP 地址每秒处理的最大查询总数可能低至 1500。

入站 Resolver 端点的入口和出口安全组规则建议

入口规则		
协议类型	端口号	源 IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0
出口规则		
协议类型	端口号	目的地 IP
TCP	全部	0.0.0.0/0
UDP	全部	0.0.0.0/0

出站 Resolver 端点的入口和出口安全组规则建议

入口规则		
协议类型	端口号	源 IP
TCP	全部	0.0.0.0/0
UDP	全部	0.0.0.0/0
出口规则		

协议类型	端口号	目的地 IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

> **Note**
>
> 安全组端口要求：
>
> - 入站端点需要入口规则，这些规则允许端口 53 上的 TCP 和 UDP 接收来自您网络的 DNS 查询。出口规则可以允许所有端口，因为端点可能需要响应来自不同源端口的查询。
> - 出站端点需要出口规则，这些规则允许 TCP 和 UDP 访问您网络上用于 DNS 查询的端口。上面的示例中显示端口 53，因为它是最常见的 DNS 端口，但您的网络可能使用不同的端口。入口规则可以允许所有端口容纳来自 DNS 服务器的响应。

入站 Resolver 端点

对于使用入站解析程序端点的客户端，如果您拥有超过 40,000 个唯一 IP 地址和端口组合来生成 DNS 流量，弹性网络接口的容量将受到影响。

解析程序端点的高可用性

在创建 VPC 解析器入站终端节点时，Route 53 要求您创建至少两个 IP 地址，网络上的 DNS 解析器会将查询转发到这两个 IP 地址。您还应在至少两个可用区中指定 IP 地址以实现冗余。

如果您要求任何时候都可用多个弹性网络接口端点，我们建议您在自身需求的基础上至少再多创建一个的网络接口，以确保您有额外的容量可用于处理可能的流量激增。额外的网络接口还可确保维护或升级等服务操作期间的可用性。

有关更多信息，请参阅这篇详细的博客文章：如何使用解析器端点实现 DNS 的高可用性以及创建或编辑入站端点时指定的值。

DNS 区域步行

DNS 区域步行攻击试图从 DNSSEC 签名的 DNS 区域获取所有内容。如果 VPC Resolver 团队检测到的流量模式与在您的终端节点上行走 DNS 区域时生成的流量模式相匹配，则服务团队将限制您的终端节点上的流量。因此，您可能会发现 DNS 查询超时的百分比很高。

如果您观察到终端节点的容量减少并且认为终端节点受到了错误限制，请前往 h https://console.aws.amazon.com/support/ ome#/ 创建支持案例。

Amazon Route 53 运行状况检查的最佳实践

有效的运行状况检查配置对于维持高可用性和弹性基础设施至关重要。以下是设置和管理 Amazon Route 53 运行状况检查时要考虑的一些最佳实践：

1. 对运行状况检查端点使用弹性 IP 地址：
   - 对运行状况检查端点使用弹性 IP 地址以确保监控的一致性。
   - 如果您不再使用 Amazon EC2 实例，请记得删除所有相关的运行状况检查，以避免潜在的安全风险或数据泄露。

   有关更多信息，请参阅 您在创建或更新运行状况检查时指定的值。
2. 配置适当的运行状况检查间隔：
   - 根据应用程序的要求和所监控资源的重要性设置运行状况检查的间隔。
   - 间隔越短，故障检测速度就越快，但可能会增加 Route 53 的成本和资源负荷。
   - 较长的间隔可以降低成本和资源负荷，但可能会导致故障检测产生延迟。

   有关更多信息，请参阅 高级配置（仅限“监控端点”）。
3. 实现告警通知：
   - 将 Amazon 配置 CloudWatchalarms 为在运行状况检查失败或恢复时接收通知。
   - 根据应用程序要求和资源的预期行为设置适当的告警阈值。
   - 将通知集成在监控和事件响应流程中。

   有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。
4. 策略性地利用运行状况检查区域：
   - 根据用户和资源的地理分布选择运行状况检查区域。
   - 考虑对关键资源使用多个运行状况检查区域，以提高可靠性并降低区域中断的影响。
5. 监控运行状况检查日志和指标：
   - 定期查看 Route 53 运行状况检查日志和 CloudWatch 指标，以确定潜在问题或性能瓶颈
   - 分析运行状况检查失败的原因，并采取适当措施来解决潜在的问题。
6. 实施失效转移和失效自动恢复策略：
   - 利用 Route 53 的失效转移路由策略，在出现故障时自动将流量路由到运行状况良好的资源。

- 规划并测试失效转移和失效自动恢复流程，以确保中断和恢复期间实现无缝过渡。

有关更多信息，请参阅 配置 DNS 故障转移。

7. 定期查看和更新运行状况检查：
   - 根据需要更新运行状况检查端点、间隔和告警阈值，以保持最佳的监控和性能。

通过遵循这些最佳实践，就可以有效地利用 Amazon Route 53 运行状况检查来监控资源的运行状况和可用性，从而确保应用程序和服务拥有可靠和高性能的基础设施。

配额

Amazon Route 53 API 请求和实体的数量受以下配额（以前称为“限制”）的约束。

主题

使用 Service Quotas 来查看和管理配额

您可以使用 Service Quotas 服务来查看许多 Amazon 服务的配额，并请求增加配额。有关更多信息，请参阅 Service Quotas 用户指南。（您目前可以使用服务配额来查看和管理域、Route 53 和 Route 53 VPC 解析器配额。）

> **Note**
>
> 要查看配额并请求提高 Route 53 的配额，您必须将区域更改为美国东部（弗吉尼亚北部）。要查看 VPC Resolver 的配额并申请更高的配额，请切换到适用的区域。

实体的配额

Amazon Route 53 实体受以下配额的约束。

有关获取当前配额（以前称为“限制”）的信息，请参阅以下 Route 53 操作：

- GetAccountLimit— 获取运行状况检查、托管区域、可重复使用的委托集、流量策略和流量策略记录的配额
- GetHostedZoneLimit— 获取托管区域和 Amazon 上可与私 VPCs 有托管区域关联的记录配额
- GetReusableDelegationSetLimit— 获取可以与可重复使用的委托集关联的托管区域数量的配额

主题

- 记录的配额
- Route 53 VPC 解析器的配额
- 运行状况检查的配额
- 查询日志配置的配额
- Traffic Flow 策略和策略记录的配额
- 可重复使用的委派集的配额
- Route 53 配置文件中的配额

域的配额

实体	配额
Domains	每个 Amazon 账户 20* 请求更高的配额。

*截至 2021 年 3 月，新客户的数量限制为 20。

如果您有一个现有账户，并且您的默认限制现在为 50，则该限制将保持在 50。

托管区域的配额

实体	配额
托管区域	每个 Amazon 账户的初始配额为 500，但您可以根据需要申请更高的配额。 请求更高的配额。
可以使用相同可重用委派集的托管区域	100 请求更高的配额。
	300

实体	配额
Amazon VPCs ，您可以将其与每个托管区域的私有托管区域相关联	如果想要 300 个以上的关联，我们建议使用 Route 53 配置文件。有关更多信息，请参阅 Amazon Route 53 Profiles 是什么？。
可以与 VPC 相关联的私有托管区域	没有配额 *
您可以创建的授权，以便您可以将一个账户创建的授权与另一个账户创建的托管区域相关联 VPCs	1000
每个托管区域可以创建的密钥签名密钥 (KSK) 数量	2

* 您可以将 VPC 与您通过 Amazon 账户控制的任何或全部私有托管区域相关联。例如，假设您有三个 Amazon 账户，并且所有三个账户的默认配额均为 500 个托管区域。如果您为所有这三个账户都创建 500 个私有托管区域，则可以将 VPC 与所有 1,500 私有托管区域相关联。

记录的配额

实体	配额
记录	每个托管区域 10,000 个 请求更高的配额。 托管区域中大于 10,000 个记录的配额将产生额外费用。有关详细信息，请参阅 Amazon Route 53 定价。
记录集中的记录	每个记录集 400 个
地理位置、延迟、多值应答、加权和基于 IP 的记录	具有相同名称和类型的 100 个记录

实体	配额
地理位置临近度记录	具有相同名称和类型的 30 个记录
CIDR 集合	每人 5 Amazon Web Services 账户个 请求更高的配额。
CIDR 块	每个 CIDR 集合 1000 个。 请求更高的配额。

Route 53 VPC 解析器的配额

本部分包含所有 Route 53 VPC 解析器配额

Route 53 VPC 解析器的配额

使用以下步骤增加 Route 53 VPC 解析器的配额。

要增加 Resolver 配额

1. 在 https://console.amazonaws.cn/servicequotas/home/services/route53resolver/quotas 打开 Service Quotas 控制台。
2. 转到要提高限制的区域。
3. 选择要增加的 Route 53 VPC 解析器配额名称。
4. 选择 Request quota increase（请求增加配额），输入配额值，然后选择 Request（请求）。

Route 53 VPC 解析器终端节点的配额

实体	配额
每个 Amazon 区域的终端节点	每个 Amazon 账户 4 个 请求更高的配额。
每个端点的 IP 地址	6

实体	配额
	请求更高的配额。
每条规则的 IP 地址	6
每个 Amazon 区域的规则	每个 Amazon 账户 1000 请求更高的配额。
规则与 VPCs 每个 Amazon 区域之间的关联	每个 Amazon 账户 2000 请求更高的配额。
一个端点中每个 IP 地址的每秒 UDP 查询数	10,000*

* 端点中的每个 IP 地址每秒最多可以处理 10,000 个 UDP DNS 查询 (QPS)。DNS QPS 数量因查询类型、响应大小、目标名称服务器运行状况、查询响应时间、往返延迟,和正在使用的协议而有所不同。例如，对目标名称服务器的查询响应速度较慢可能会显著降低网络接口的容量。此外，为了确保高可用性，Route 53 Resolver 为其收到的每个 DNS 请求生成冗余出站查询。因此，每个出站网络接口的 QPS 将与发送到 Route 53 VPC 解析器的 QPS 不匹配。使用 CloudWatch 指标来衡量向每个网络接口发送了多少查询。有关更多信息，请参阅 Route 53 VPC 解析器 IP 地址的指标。如果您的最大查询速率超过端点中任何网络接口容量的 50%，则可以添加更多网络接口以增加端点容量。

即使安全组配置不需要跟踪，也会自动跟踪通过 Network Load Balancer 和 Amazon Lambda （有关完整列表，请参阅自动跟踪的连接）等应用程序建立的连接。

如果使用限制性安全组规则强制执行连接跟踪，或者通过网络负载均衡器路由查询，则对于入站端点来说，每个 IP 地址每秒处理的最大查询总数可能低至 1500。

Route 53 VPC 解析器查询日志的配额

实体	配额

实体	配额
按 Amazon 区域查询日志配置	20 请求更高的配额。
每个 Amazon 区域的查询日志配置 VPC 关联	100 * 请求更高的配额。
查询配置共享到的账户的日志配置每个 Amazon 区域每个账户的 VPC 关联（包括使用 RAM 共享的查询长配置）。	100 请求更高的配额。

* 这是一个区域限制，可累积应用于单个区域内的所有 VPC Resolver 查询日志配置。在同一区域内创建其他查询日志配置不会提供额外的 VPC 关联容量。

解析器 DNS 防火墙的配额

实体	配额
每个 Amazon 区域单个账户与 VPC 关联的规则组数	5
每个 Amazon 区域的单个账户在单个 Amazon S3 文件中包含的 DNS 防火墙域数量	250,000 请求更高的配额。
每个 Amazon 区域单个账户的 DNS 防火墙规则组数量	1000 请求更高的配额。
每个 Amazon 区域单个账户的规则组中的规则数量	100 请求更高的配额。

实体	配额
每个 Amazon 地区的单个账户的域名列表数量	1000 请求更高的配额。
可以在每个 Amazon 区域单个账户的所有域列表中指定的最大域数。	100000 请求更高的配额。

Resolver on Outpost 上的限额

实体	配额
Resolver on Outpost 实例限制	6 个（至少需要 4 个）

Resolver on Outpost 实例类型以及每种实例类型每秒可容纳的 DNS 查询次数：

实例类型	每秒查询数
c5.large	最多 7,000
c5.xlarge	最多 12,000
c5.2xlarge	最多 24,000
c5.4xlarge	最多 56,000
c5d.large	最多 7,000
c5d.xlarge	最多 12,000
c5d.2xlarge	最多 24,000

实例类型	每秒查询数
c5d.4xlarge	最多 56,000
m5.large	最多 7,000
m5.xlarge	最多 12,000
m5.2xlarge	最多 24,000
m5.4xlarge	最多 56,000
m5d.large	最多 7,000
m5d.xlarge	最多 12,000
m5d.2xlarge	最多 24,000
m5d.4xlarge	最多 56,000
r5.large	最多 7,000
r5.xlarge	最多 12,000
r5.2xlarge	最多 24,000
r5.4xlarge	最多 56,000
r5d.large	最多 7,000
r5d.xlarge	最多 12,000

实例类型	每秒查询数
r5d.2xlarge	最多 24,000
r5d.4xlarge	最多 56,000

Resolver on Outpost 端点实例类型以及每种实例类型每秒可容纳的 DNS 查询次数：

实例类型	每秒查询数
c5.large	最多 5,000
c5.xlarge	最高 10,000
c5.2xlarge	最多 18,000
c5.4xlarge	最多 30,000
c5d.large	最多 5,000
c5d.xlarge	最高 10,000
c5d.2xlarge	最多 18,000
c5d.4xlarge	最多 30,000
m5.large	最多 5,000
m5.xlarge	最高 10,000
m5.2xlarge	最多 18,000

实例类型	每秒查询数
m5.4xlarge	最多 30,000
m5d.large	最多 5,000
m5d.xlarge	最高 10,000
m5d.2xlarge	最多 18,000
m5d.4xlarge	最多 30,000
r5.large	最多 5,000
r5.xlarge	最高 10,000
r5.2xlarge	最多 18,000
r5.4xlarge	最多 30,000
r5d.large	最多 5,000
r5d.xlarge	最高 10,000
r5d.2xlarge	最多 18,000
r5d.4xlarge	最多 30,000

运行状况检查的配额

实体	配额

实体	配额
运行状况检查	每个 Amazon 账户 200 次有效的运行状况检查 请求更高的配额。
已计算的运行状况检查可监控的子运行状况检查	255
响应运行状况检查请求的标头的最大总长度	16384 字节 (16K)

查询日志配置的配额

实体	配额
查询日志配置	每个托管区域 1 个

Traffic Flow 策略和策略记录的配额

实体	配额
流量策略 有关 Route 53 流量的更多信息，请参阅 使用 Traffic Flow 来路由 DNS 流量。	每个 Amazon 账户 50 个 请求更高的配额。
流量策略版本	每个流量策略 1000 个
流量策略记录（在 Route 53 API 中称为 “策略实例” Amazon SDKs、Amazon Command Line Interface	每个 Amazon 账户 5 个 请求更高的配额。

实体	配额
、和 Amazon Tools for Windows PowerShell ）	

可重复使用的委派集的配额

实体	配额
可重用的委派集	每个 Amazon 账户 100 个 请求更高的配额。

Route 53 配置文件中的配额

实体	配额
一个区域中每个配置的 Amazon Web Services 账户 Route 53 配置文件数量	5 请求更高的配额。
VPCs 可以与个人资料关联的数量	1000 请求更高的配额。
每个配置文件的 DNS Firewall 规则组数量	5
每个配置文件的 Resolver 规则数量	1000 请求更高的配额。
每个配置文件的私有托管区数量	1000

实体	配额
	请求更高的配额。
每个配置文件的 VPC 解析器查询日志配置数量	2

API 请求的最大数量

Amazon Route 53 API 请求受以下最大数量的约束。

主题

- ChangeResourceRecordSets 请求中元素和字符的数量
- Amazon Route 53 API 请求的频率
- Route 53 VPC 解析器 API 请求的频率

`ChangeResourceRecordSets` 请求中元素和字符的数量

`ResourceRecord` 元素

一个请求不能包含超过 1000 个 `ResourceRecord` 元素（包括别名记录）。当 `Action` 元素的值为 `UPSERT` 时，每个 `ResourceRecord` 元素会统计两次。

最大字符数

一个请求的所有 `Value` 元素中的字符总数 (包括空格) 不得超过 32,000 个字符。当 `Action` 元素的值为 `UPSERT` 时，`Value` 元素中的每个字符会统计两次。

Amazon Route 53 API 请求的频率

所有 Amazon Route 53 API 请求

对于 Amazon Route 53，每个 Amazon 账户每秒 APIs五次请求。如果您每秒提交的请求超过五个，则 Amazon Route 53 会返回 HTTP 400 错误 (`Bad request`)。响应标头还包括一个其值为 `Throttling` 的 `Code` 元素，以及一个值为 `Rate exceeded` 的 `Message` 元素。

> **Note**
>
> 如果您的应用程序超过了此限制，我们建议您为重试实施指数退避。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon中的错误重试和指数回退。

`ChangeResourceRecordSets` 请求

如果 Route 53 在下一个请求到达之前无法处理某个请求，则它将拒绝同一个托管区域的后续请求，并返回 HTTP 400 错误 (`Bad request`)。响应标头还包括一个值为 `PriorRequestNotComplete` 的 `Code` 元素，以及一个值为 `The request was rejected because Route 53 was still processing a prior request.` 的 `Message` 元素。

`CreateHealthCheck` 请求

您可以每隔 2 秒提交一个`CreateHealthCheck`请求 Amazon Web Services 账户。

Route 53 VPC 解析器 API 请求的频率

所有请求

每个区域每个 Amazon 账户每秒五次请求。如果您在一个区域中每秒提交的请求超过五个，VPC 解析器将返回 HTTP 400 错误 (`Bad request`)。响应标头还包括一个其值为 `Throttling` 的 `Code` 元素，以及一个值为 `Rate exceeded` 的 `Message` 元素。

> **Note**
>
> 如果您的应用程序超过了此限制，我们建议您为重试实施指数退避。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon中的错误重试和指数回退。

相关信息

下列相关资源在您使用此服务的过程中会有所帮助。

主题

Amazon 资源

Amazon Web Services 中提供一些有用的指南、论坛和其它资源。

- Amazon Route 53 API 参考 - 参考指南提供了架构位置；完整说明了 API 操作、参数和数据类型；并提供了该服务返回的错误列表。
- Amazon CloudFormation 用户指南 中的 AWS::Route53::RecordSet 类型 - 将 Amazon Route 53 与 Amazon CloudFormation 一起使用以创建 Amazon CloudFormation 堆栈自定义 DNS 名称的一种属性。
- 开发论坛 - 基于社区的论坛，供开发人员讨论与 Route 53 有关的技术问题。
- Amazon 支持中心 - 此站点汇集了有关您近期的支持案例的信息，以及来自 Amazon Trusted Advisor 和运行状况检查的结果，并提供了指向开发论坛、技术常见问题解答、服务运行状况控制面板以及有关 Amazon 支持计划的信息的链接。
- Amazon Premium Support 信息 – 提供有关 Amazon Premium Support 信息的主要网页，该服务是一种一对一的快速响应支持渠道，可帮助您在 Amazon 基础设施服务上构建和运行应用程序。
- 联系我们 – 用于咨询有关您的账单或账户的问题的链接。如有技术问题，请使用上述开发论坛或支持连接。
- Route 53 产品信息 - 提供 Route 53 相关信息（包括功能、定价等信息）的主要网页。

- 入门资源中心 – 了解如何设置 Amazon Web Services 账户、加入 Amazon 社区和启动您的第一个应用程序。
- Amazon Web Services 支持 中心 – 用于创建和管理 Amazon Web Services 支持 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及Amazon Trusted Advisor。
- Amazon Web Services 支持 – 提供有关 Amazon Web Services 支持 的信息的主要网页，这是一个一对一的快速响应支持渠道，可以帮助您在云中构建和运行应用程序。

- 联系我们 – 用于查询有关 Amazon 账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon 网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

第三方工具和库

除了 Amazon 资源外，您还可以找到适用于 Amazon Route 53 的各种第三方工具和库。

- AmazonRoute53AppsScript (通过 webos-goodies)

  Amazon Route 53 的 Google 电子表格管理。
- 用于 .NET 的 Amazon 组件（通过 SprightlySoft）

  用于 Amazon Web Services 的 SprightlySoft .NET 组件，支持 REST 操作和 Route 53。
- Boto API 下载 (通过 github)

  用于访问 Amazon Web Services 的 Boto Python 接口。
- cli53 (通过 github)

  用于 Route 53 的命令行界面。
- Dasein Cloud API

  基于 Java 的 API。
- R53.py (通过 github)

  保留受源代码控制的 DNS 配置的规范版本，并计算更改配置所需的最小变更集。
- route53d

  DNS 前端到 Route 53 API（支持增量区域转移 (IXFR)）。
- Route53Manager (通过 github)

  基于 Web 的接口。
- Ruby Fog (通过 github)

  Ruby 云服务库。
- WebService::Amazon::Route53 (通过 CPAN)

  Amazon Route 53 API 的 Perl 界面。

图形用户界面

以下第三方工具提供用于使用 Amazon Route 53 的图形用户界面 (GUI)：

- R53 Fox
- Ylastic

文档历史记录

以下条目描述了每个 Route 53 文档版本中的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

主题

2025 年版本

2025年12月15日

添加了 Route 53 解析器终端节点的详细 CloudWatch 指标。新指标增强了解析器网络接口和目标名称服务器级别的监控功能，包括 DNS 查询的 P90 响应延迟、对 SERVFAIL、NXDOMAIN、REFECTED 和 FORMERR 响应状态的跟踪，以及对出站解析器端点的目标名称服务器的可用性监控。有关更多信息，请参阅 CloudWatch Route 53 VPC 解析器的详细指标。

2025 年 6 月 26 日

向 AWS/Route53Resolver 命名空间添加了 ResolverEndpointCapacityStatus。有关更多信息，请参阅 Route 53 VPC 解析器终端节点的指标。

2025 年 6 月 25 日

Amazon Route 53 现在支持 VPC Lattice 服务自定义域端点的别名记录。有关更多信息，请参阅 将流量路由到 Amazon VPC Lattice 服务域端点。

2025 年 6 月 24 日

现在，您可以在 VPC 解析器中使用入站和出站委托。有关更多信息，请参阅 您网络上的 DNS 解析器如何将 DNS 查询转发到解析器端点。

2025 年 6 月 1 日

添加了 cloudwatch:GetMetricData、tag:GetResources、es:ListDomainNames、es:DescribeDoma 和 lightsail:GetContainerServices 的权限。这些权限使您能够获取最多 500 个运行 CloudWatch 状况检查指标、最多 100 个运行状况检查名称、获取指定亚马逊 OpenSearch 服务域的域配置、列出当前用户在活动区域中拥有的所有亚马逊 OpenSearch 服务域的名称、获取 CloudFront 多租户分配并获取 Lightsail 容器服务。有关更多信息，请参阅 Amazon 托管策略：AmazonRoute53 FullAccess。

2025 年 4 月 28 日

您现在可以将接口 VPC 端点关联到 Route 53 配置文件。有关更多信息，请参阅 将接口 VPC 端点与 Route 53 配置文件关联。

2025 年 4 月 28 日

现在，您可以向 CloudFront 分发租户添加别名记录。有关更多信息，请参阅 使用您的域名将流量路由到 Amazon CloudFront 分配。

2025 年 2 月 27 日

更新了 Route 53 指南，提供了 Traffic Flow 的全新控制台体验。有关更多信息，请参阅创建和管理流量策略和创建和管理策略记录。

2025 年 1 月 14 日

Amazon Route 53 现在支持 OpenSearch 服务自定义域终端节点的别名记录。有关更多信息，请参阅 将流量路由到亚马逊 OpenSearch 服务域终端节点。

2025 年 1 月 13 日

在 Security Hub CSPM 中添加了解析器 DNS 防火墙调查结果。有关更多信息，请参阅 将结果从 Resolver DNS 防火墙发送到 Security Hub CSPM。

2024 年版

2024 年 11 月 15 日

添加了 Resolver DNS Firewall Advanced，这是解析器 DNS 防火墙上的一组新功能，允许您识别和阻止与高级 DNS 威胁（例如 DNS 隧道、域生成算法 (DGA) 和基于字典 DGA 的威胁）相关的 DNS 流量。有关更多信息，请参阅 解析器 DNS 防火墙高级。

2024 年 10 月 29 日

添加了对 HTTPS、SSHFP、SVCB 和 TLSA DNS 记录类型的支持。有关更多信息，请参阅 支持的 DNS 记录类型。

2024 年 10 月 3 日

为 DoH 出站 Resolver 端点添加了服务名称指示 (SNI) 的支持。有关更多信息，请参阅 创建或编辑规则时指定的值。

2024 年 9 月 3 日

现在，您可以使用`route53:VPCs`策略条件向其授予管理托管区域关联的精细访问权限。 VPCs有关更多信息，请参阅 使用 IAM 策略条件进行精细访问控制。

2024 年 8 月 27 日

`AmazonRoute53ProfilesFullAccess` 添加了 `GetProfilePolicy` 和 `PutProfilePolicy` 权限。这些是仅限权限的 IAM 操作。如果 IAM 委托人未获得这些权限，则在尝试使用该 Amazon RAM 服务共享个人资料时会出错。有关更多信息，请参阅 Amazon 托管策略： AmazonRoute53 ProfilesFullAccess。

2024 年 8 月 27 日

`AmazonRoute53ProfilesReadOnlyAccess` 添加了 `GetProfilePolicy` 权限。这是仅限权限的 IAM 操作。如果 IAM 委托人未获得此权限，则在尝试使用该 Amazon RAM 服务访问配置文件的策略时将发生错误。有关更多信息，请参阅 Amazon 托管策略： AmazonRoute53 ProfilesReadOnlyAccess。

2024 年 8 月 5 日

添加了语句 ID (Sid)，以唯一地标识托管策略 AmazonRoute53ResolverFullAccess。有关更多信息，请参阅 Amazon 托管策略： AmazonRoute53 ResolverFullAccess。

2024 年 8 月 5 日

添加了语句 ID (Sid)，以唯一地标识托管策略 AmazonRoute53ResolverReadOnlyAccess。有关更多信息，请参阅 Amazon 托管策略： AmazonRoute53 ResolverReadOnlyAccess。

2024 年 7 月 18 日

更新了整个 Route 53 指南，为运行状况检查提供全新的控制台体验。有关更多信息，请参阅 创建、更新和删除运行状况检查。

2024 年 4 月 30 日

您现在可以决定 DNS Firewall 规则是检查（默认）还是信任 DNS 重定向链。有关更多信息，请参阅解析器 DNS 防火墙组件和设置和DNS Firewall 中的规则设置。

2024 年 4 月 22 日

现在，您可以使用 Route 53 配置文件与许多人共享特定于 DNS 的配置， VPCs 并与 Amazon 帐户共享。有关更多信息，请参阅 Amazon Route 53 Profiles 是什么？。

2024 年 4 月 22 日

添加了托管策略 AmazonRoute53ProfilesReadOnlyAccess 和 AmazonRoute53ProfilesFullAccess，以授予对 Amazon Route 53 Profiles 的只读和完全访问权限。有关更多信息，请参阅 Amazon 亚马逊 Route 53 的托管策略。

2024 年 2 月 5 日

现在，您可以通过 DNS 防火墙使用 Amazon EventBridge 发送实时警报。有关更多信息，请参阅使用管理解析器 DNS 防火墙事件 Amazon EventBridge。

2024 年 1 月 9 日

您现在可以将 DNS 查询类型用作 DNS Firewall 规则的可选值，以区分该规则对特定 DNS 查询类型的响应。有关更多信息，请参阅解析器 DNS 防火墙组件和设置和DNS Firewall 中的规则设置。

2024 年 1 月 9 日

您现在可以使用“快速创建记录”或“创建记录”向导来创建地理位置临近度路由记录。有关更多信息，请参阅 地理位置临近度路由、地理位置临近度记录的特定值 和 地理位置临近度别名记录的特定值。

2023 年发行版

2023 年 12 月 20 日

现在，您可以通过 HTTPS 将 DNS 与解析器端点一起使用。有关更多信息，请参阅 选择用于端点的协议。

2023 年 7 月 20 日

Outposts 上的亚马逊 Route 53 现已在机架上 Amazon Outposts 线。它包括一个 VPC 解析器，用于缓存来自的所有 DNS 查询。 Amazon Outposts在部署入站和出站端点时，您还可以在 Outpost 和本地 DNS 解析程序之间设置混合连接。有关更多信息，请参阅 什么是 Amazon Route 53 on Outposts？。

2023 年 7 月 19 日

启用本地区域后，您现在可以将它们与地理位置临近度路由（仅限流量流）一起使用。有关更多信息，请参阅 地理位置临近度路由 和流量策略文档格式。

2023 年 3 月 22 日

更新了整个 Route 53 指南，为您提供全新的域控制台体验。您还可以使用全新的主机体验将域名从一个域名转移 Amazon Web Services 账户 到另一个域名 Amazon Web Services 账户。有关更多信息，请参阅注册新域和转移域。

2023 年 3 月 10 日

现在，您可以通过 Route 53 VPC 解析器使用 IPv4 IPv6、或双堆栈终端节点连接到您的资源。有关更多信息，请参阅创建或编辑入站端点时指定的值和创建或编辑出站端点时指定的值。

2022 版本

2022 年 9 月 21 日

现在，您可以使用策略条件为用户提供在 Amazon Route 53 中更新资源记录集的精细访问权限。有关更多信息，请参阅 使用 IAM 策略条件进行精细访问控制。

2022 年 8 月 30 日

亚马逊 Route 53 现在支持 2022 年 8 月 1 日之后创建的 Amazon App Runner 服务的别名记录。有关更多信息，请参阅 将流量路由到 Amazon App Runner 服务。

2022 年 6 月 1 日

Amazon Route 53 现在已经可以使用基于 IP 的路由选项。有关更多信息，请参阅 基于 IP 的路由。

2022 年 3 月 16 日

Amazon Route 53 中的私有托管区域现在支持地理位置和基于延迟的路由选项。有关更多信息，请参阅 使用私有托管区域的注意事项。

2022 年 1 月 25 日

变更.com.au和.net.au所有权的流程 TLDs 已简化，包括回复两封电子邮件（由新旧注册人发出），并且不包括填写表格。有关更多信息，请参阅.com.au（澳大利亚）和.net.au（澳大利亚）。

2021 版本

2021 年 10 月 26 日

添加了对使用 Amazon Route 53 禁用默认反向 DNS 规则的支持 现在，您可以禁用创建这些规则，改为根据需要将反向 DNS 命名空间的查询转发到外部服务器。有关更多信息，请参阅 VPC 解析器中反向 DNS 查询的转发规则。

2021 年 9 月 1 日

添加了一个新的入门主题，该主题将引导您完成为静态网站创建 Amazon CloudFront 发行版的过程。有关更多信息，请参阅 使用 Amazon CloudFront 发行版为静态网站提供服务。

2021 年 7 月 14 日

已开始追踪 Amazon Route 53 的 Amazon 托管政策。有关更多信息，请参阅 Amazon 亚马逊 Route 53 的托管策略。

2021 年 3 月 31 日

添加了解析器 DNS 防火墙。使用 DNS 防火墙，您可以为来自您的出站 DNS 请求提供保护 VPCs。有关更多信息，请参阅 使用 DNS Firewall 筛选出站 DNS 流量。

2020 版本

2020 年 12 月 17 日

为 Route 53 VPC 解析器添加了对 DNSSEC 签名的支持。有关更多信息，请参阅 在 Amazon Route 53 中配置 DNSSEC 签名。

为 Route 53 VPC 解析器添加了对 DNSSEC 验证的支持。有关更多信息，请参阅 在 Amazon Route 53 中启用 DNSSEC 验证。

2020 年 9 月 23 日

更新了 Route 53 指南，提供了全新控制台体验。有关更多信息，请参阅 什么是 Amazon Route 53？。

2020 年 9 月 1 日

添加了对 Resolver 查询日志的支持。有关更多信息，请参阅 Resolver 查询日志记录。

2018 版本

2018 年 12 月 20 日

您可以创建 Route 53 别名记录，将流量路由到 API Gateway APIs 或 Amazon VPC 接口终端节点。有关更多信息，请参阅 值/流量路由至。

2018 年 11 月 28 日

Route 53 自动命名（也称为服务发现）现在是一项单独的服务 Amazon Cloud Map。有关更多信息，请参见Amazon Cloud Map 开发人员指南。

2018 年 11 月 19 日

您可以使用 Route 53 解析程序通过 Direct Connect 或 VPN 连接配置 VPC 和您网络之间的 DNS 解析。（解析程序是递归 DNS 服务的新名称，此服务预设情况下提供给 Amazon Virtual Private Cloud (Amazon VPC) 中的所有客户。）这样，您就可以将来自您网络上解析程序的 DNS 查询转发到 Route 53 Resolver。解析程序还可让您将对于所选域名 (example.com) 和子域名 (api.example.com) 的查询从 VPC 转发到您网络上的解析程序。有关更多信息，请参阅 什么是 Route 53 VPC 解析器？。

2018 年 11 月 7 日

当您使用 Route 53 Traffic Flow 和地理位置临近度路由时，您可以使用交互式地图直观显示您的最终用户如何路由到您遍布全球的端点。有关更多信息，请参阅 查看显示地理位置临近度设置效果的地图。

2018 年 10 月 18 日

您可以使用 Route 53 控制台和 API 来临时禁用 Route 53 运行状况检查。这可让您轻松地暂停监控端点（如 Web 服务器），以便您可以对其执行维护，而不会触发告警或生成不必要的日志或状态消息。有关更多信息，请参阅您在创建或更新运行状况检查时指定的值中的“已禁用”。该功能适用于所有三种类型的 Route 53 运行状况检查：监控终端节点的运行状况检查、监控其他运行状况检查的运行状况检查和监控 CloudWatch 警报的运行状况检查。

2018 年 3 月 13 日

如果您使用自动命名，您现在可以使用第三方运行状况检查程序来评估资源的运行状况。当资源在 Internet 上不可用时，例如由于实例位于 Amazon VPC 中，此功能会非常有用。有关更多信息，请参阅HealthCheckCustomConfig《亚马逊 Route 53 API 参考》。

2018 年 3 月 9 日

IAM 现在包括适用于自动命名的托管策略。有关更多信息，请参阅 Amazon 亚马逊 Route 53 的托管策略。

2018 年 2 月 6 日

现在，您可以配置自动命名来创建别名记录，用于将流量路由到 ELB 负载均衡器或者创建 CNAME 记录。有关更多信息，请参阅 Amazon Route 53 RegisterInstanceAPI 参考中 API 文档中的属性。

2017 版本

2017 年 12 月 5 日

您现在可以使用 Route 53 自动命名 API 来针对微服务预置实例。自动命名可让您自动创建 DNS 记录并选择基于您定义的模板进行运行状况检查。有关更多信息，请参阅什么是 Amazon Cloud Map？ 在《Amazon Cloud Map 开发人员指南》中。

2017 年 11 月 16 日

现在，您可以通过编程方式同时获取对 Route 53 资源（例如托管区域和运行状况检查）的当前配额，以及您目前使用的每个资源的数量。有关更多信息 GetAccountLimit，请参阅《亚马逊 Route 53 API 参考》GetReusableDelegationSetLimit中的GetHostedZoneLimit、和。

2017 年 10 月 3 日

Route 53 现已成为符合 HIPAA 要求的一项服务。有关更多信息，请参阅 Amazon Route 53 的合规性验证。

2017 年 9 月 29 日

现在，您可以通过编程方式检查域是否可以传输到 Route 53。有关更多信息，请参阅CheckDomainTransferability《亚马逊 Route 53 API 参考》。

2017 年 9 月 11 日

现在，您可以创建 Route 53 别名记录，以将互联网流量路由到 Elastic Load Balancing 网络负载均衡器。有关别名记录的更多信息，请参阅在别名记录和非别名记录之间进行选择。

2017 年 9 月 7 日

如果您使用 Route 53 作为您的公有、授权 DNS 服务，则您现在可以记录 Route 53 接收的 DNS 查询。有关更多信息，请参阅 公有 DNS 查询日志记录。

2017 年 9 月 1 日

如果您使用 Route 53 Traffic Flow，您现在可以使用地理位置临近度路由，基于您的用户和资源之间的实际距离路由流量。您也可以通过指定正偏差或负偏差，将更多或更少的流量路由到每个资源。有关更多信息，请参阅 地理位置临近度路由。

2017 年 8 月 21 日

您现在可以使用 Route 53 创建认证机构授权 (CAA) 记录，该记录可让您指定可为您的域和子域颁发证书的证书颁发机构。有关更多信息，请参阅 CAA 记录类型。

2017 年 8 月 18 日

现在，您可以使用 Route 53 控制台将大量域传输到 Route 53。有关更多信息，请参阅 将域注册转移到 Amazon Route 53。

2017 年 8 月 4 日

注册域名时，某些顶级域名的注册机构 (TLDs) 要求您验证您为注册人联系人指定的电子邮件地址是否有效。现在，您可以发送验证电子邮件并确认您已在域注册流程中成功验证电子邮件地址。有关更多信息，请参阅 注册新域。

2017 年 6 月 21 日

如果您要将流量以近乎随机的方式路由到多个资源 (例如 Web 服务器)，您现在可以为每个资源创建一条多值应答记录，并可选择将 Route 53 运行状况检查关联至每条记录。Route 53 通过最多八

条对应于每条 DNS 查询的正常记录响应 DNS 查询，并向不同的 DNS 解析程序提供不同的应答。有关更多信息，请参阅 多值应答路由。

2017 年 4 月 10 日

当您使用 Route 53 控制台将域注册转移到 Route 53 时，现在可以选择下列选项之一来将域的 DNS 服务的名称服务器与被转移的域注册关联：

- 将名称服务器用于您选择的 Route 53 托管区域
- 将名称服务器用于域的当前 DNS 服务
- 使用您指定的名称服务器

Route 53 会自动将这些名称服务器与被转移的域注册相关联。

2016 版本

2016 年 11 月 21 日

现在，您可以创建使用 IPv6 地址检查终端节点运行状况的运行状况检查。有关更多信息，请参阅 创建和更新运行状况检查。

2016 年 11 月 15 日

现在，您可以使用 Route 53 API 操作将您用一个账户创建的 Amazon VPC 与用另一个账户创建的私有托管区域相关联。有关更多信息，请参阅 将您使用不同 Amazon 账户创建的 Amazon VPC 和私有托管区域相关联。

2016 年 8 月 30 日

在此版本中，Route 53 添加了以下新功能：

- 名称权威指针 (NAPTR) 记录 — 现在，您可以创建 NAPTR 记录，动态授权发现系统 (DDDS) 应用程序会使用该记录将一个值转换为另一个值，或将一个值替换为另一个值。例如，一种常见的用途是将电话号码转换为 SIP URIs。有关更多信息，请参阅 NAPTR 记录类型。
- DNS 查询测试工具 — 您现在可以模拟对记录的 DNS 查询，并查看 Route 53 返回的值。对于地理位置和延迟记录，您还可以模拟来自特定 DNS 解析器 and/or 客户端 IP 地址的请求，以了解 Route 53 会向使用该解析器 and/or IP 地址的客户端返回什么响应。有关更多信息，请参阅 检查来自 Route 53 的 DNS 响应。

2016 年 8 月 11 日

使用此版本，您可以创建能够将流量路由到 ELB 应用程序负载均衡器的别名记录。该过程与适用于 Classic 负载均衡器的过程相同。有关更多信息，请参阅 值/流量路由至。

2016 年 8 月 9 日

在此版本中，Route 53 增加了对用于域注册的 DNSSEC 的支持。DNSSEC 允许您保护您的域名免受 DNS 欺骗攻击（也称为攻击）。 man-in-the-middle有关更多信息，请参阅 为域配置 DNSSEC。

2016 年 7 月 7 日

现在，您可以手动延长域注册，用长于注册机构所指定的最短注册期的初始注册期来注册域。有关更多信息，请参阅 延长域的注册期。

2016 年 7 月 6 日

如果您是联系地址在印度的 AISPL 客户，现在可以使用 Route 53 来注册域。有关更多信息，请参阅在印度管理账户。

2016 年 26 月 5 日

在此版本中，Route 53 添加了以下新功能：

- 域账单报告 — 现在，您可以下载按域列出所有域注册费用的报告（指定时间段内）。该报告包括所有需要付费的域名注册操作，包括注册域名、将域名转移到 Route 53、续订域名注册以及（对于某些人 TLDs）更改域名所有者。有关更多信息，请参阅以下文档：
  - Route 53 控制台 — 请参阅 下载域账单报告
  - Route 53 API — 参见ViewBilling《亚马逊 Route 53 API 参考》。
- 新增 TLDs — 您现在可以注册具有以下内容的域名 TLDs：.college、.consulting、.host、.name、.online、.republic、.rocks、.sucks、.trade、.website 和.uk。有关更多信息，请参阅 可向 Amazon Route 53 注册的域。。
- 域名注册新增 APIs 功能-对于需要确认注册人联系人电子邮件地址有效的操作，例如注册新域名，您现在可以通过编程方式确定注册人联系人是否点击了确认电子邮件中的链接，如果没有，则该链接是否仍然有效。您还可以通过编程方式请求我们再发送一封确认电子邮件。有关更多信息，请参阅 Amazon Route 53 API 参考：
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

2016 年 4 月 5 日

在此版本中，Route 53 添加了以下新功能：

- 基于 CloudWatch 指标的健康检查-您现在可以根据任何 CloudWatch 指标的警报状态创建运行状况检查。对于标准 Route 53 运行状况检查无法访问的端点（如 Amazon Virtual Private Cloud

(VPC) 中只有私有 IP 地址的实例），这种运行状况检查方法很有用。有关更多信息，请参阅以下文档：

- Route 53 控制台 — 请参阅“您在创建或更新运行状况检查时指定的值”主题中的 监控 CloudWatch 告警。
- Route 53 API — 参见亚马逊 Route 53 API 参考UpdateHealthCheck中的CreateHealthCheck和。

- 可配置的运行状况检查位置 — 现在，您可以选择用于检查资源运行状况的 Route 53 运行状况检查区域，从而减轻端点运行状况检查的负担。如果您的客户集中在一个或几个地理区域，此功能很有用。有关更多信息，请参阅以下文档：
  - Route 53 控制台 — 请参阅“您在创建或更新运行状况检查时指定的值”主题中的 高级配置（仅限“监控端点”）。
  - Route 53 API — 参见《亚马逊 Route 53 API 参考》UpdateHealthCheck中的CreateHealthCheck和`Regions`元素。
- 私有托管区域中的故障转移 — 现在，您可以在私有托管区域中创建故障转移和故障转移别名记录。如果将此功能与基于指标的运行状况检查相结合，您甚至可以为只有私有 IP 地址且使用标准 Route 53 运行状况检查无法访问的端点配置 DNS 故障转移。有关更多信息，请参阅以下文档：
  - Route 53 控制台 — 请参阅 在私有托管区域中配置故障转移。
  - Route 53 API — 参见ChangeResourceRecordSets《亚马逊 Route 53 API 参考》。
- 私有托管区域中的别名记录 — 过去，您可以创建别名记录，只将 DNS 查询路由到同一托管区域中的其它 Route 53 记录。在此版本中，您还可以创建别名记录，将 DNS 查询路由到具有区域化子域、Elastic Load Balancing 负载均衡器和 Amazon S3 存储桶的 Elastic Beanstalk 环境。（您仍然无法创建将 DNS 查询路由到 CloudFront 分配的别名记录。）有关更多信息，请参阅以下文档：
  - Route 53 控制台 — 请参阅 在别名记录和非别名记录之间进行选择。
  - Route 53 API — 参见ChangeResourceRecordSets《亚马逊 Route 53 API 参考》。

2016 年 2 月 23 日

您在创建或更新 HTTPS 运行状况检查时，现在可以配置 Route 53，以便在 TLS 协商期间将主机名发送到端点。这允许端点使用适用的 SSL/TLS 证书响应 HTTPS 请求。有关更多信息，请参阅“您在创建或更新运行状况检查时指定的值”主题中对 高级配置（仅限“监控端点”）字段中的 SNI 的描述。有关在使用 API 创建或更新运行状况检查时如何启用 SNI 的信息，请参阅 Amazon Route 53 API 参考UpdateHealthCheck中的CreateHealthCheck和。

2016 年 1 月 27 日

现在，您可以为其他 100 多个顶级域名 (TLDs) 注册域名，例如.accounts、.band 和.city。有关支持的完整列表 TLDs，请参阅可向 Amazon Route 53 注册的域。。

2016 年 1 月 19 日

现在，您可以创建能将流量路由到 Elastic Beanstalk 环境的别名记录。有关使用 Route 53 控制台创建记录的信息，请参阅 通过使用 Amazon Route 53 控制台创建记录。有关使用 API 创建记录的信息，请参阅《亚马逊 Route 53 API 参考》ChangeResourceRecordSets中的。

2015 版本

2015 年 12 月 3 日

Route 53 控制台现在包含一个可视化编辑器，可让您快速创建结合使用 Route 53 加权、延迟、故障转移和地理位置路由策略的复杂路由配置。然后，您可以将该配置与同一托管区域或多个托管区域中的一个或多个域名 (例如 example.com) 或子域名 (例如 www.example.com) 关联。此外，如果新配置无法正常工作，您还可以回滚更新。使用 Route 53 API、、和 Amazon CLI， Amazon SDKs也可以使用相同的功能 Amazon Tools for Windows PowerShell。有关使用可视化编辑器的信息，请参阅使用 Traffic Flow 来路由 DNS 流量。有关使用 API 创建流量控制配置的信息，请参阅 Amazon Route 53 API 参考。

2015 年 10 月 19 日

在此版本中，Route 53 添加了以下新功能：

- 亚马逊@@ 注册商公司注册.com 和.net 域名 — 亚马逊现在是TLDs通过 Amazon Registrator, Inc. 注册的.com 和.net 顶级域名 () 的 ICANN 认证注册商。当您使用 Route 53 注册.com 或.net 域名时，亚马逊注册商将成为记录在案的注册商，并将在您的 Whois 查询结果中列为 “赞助注册商”。有关使用 Route 53 注册域的信息，请参阅 使用 Amazon Route 53 注册和管理域。
- .com 和 .net 域的隐私保护 — 现在，当您使用 Route 53 注册 .com 或 .net 域时，所有个人信息（包括名字和姓氏）都会被隐藏。使用 Route 53 注册其它域时，不会隐藏名字和姓氏。有关隐私保护的更多信息，请参阅启用或禁用域联系信息的隐私保护。

2015 年 9 月 15 日

在此版本中，Route 53 添加了以下新功能：

- 已计算的运行状况检查 — 现在，您可以创建运行状况检查，其状态由其它运行状况检查的运行状况来确定。有关更多信息，请参阅 创建和更新运行状况检查。此外，请参阅CreateHealthCheck《亚马逊 Route 53 API 参考》。

- 用于运行状况检查的延迟测量 — 现在，您可以配置 Route 53，以测量运行状况检查程序与端点之间的延迟。延迟数据显示在 Route 53 控制台的 Amazon CloudWatch 图表中。要为新运行状况检查启用延迟测量，请参阅主题 您在创建或更新运行状况检查时指定的值 中 高级配置（仅限“监控端点”） 下的 Latency measurements（延迟测量）设置。(您不能为现有的运行状况检查启用延迟测量。) 此外，请参阅MeasureLatency《亚马逊 Route 53 API 参考》CreateHealthCheck中的主题。
- Route 53 控制台中运行状况检查仪表板的更新 — 用于监控运行状况检查的仪表板已通过多种方式进行了改进，包括用于监控 Route 53 运行状况检查器与您的终端节点之间延迟的 CloudWatch 图表。有关更多信息，请参阅 监控运行状况检查状态和获取通知。

2015 年 3 月 3 日

现在，Amazon Route 53 开发人员指南说明了如何为 Route 53 托管区域配置白标签名称服务器。有关更多信息，请参阅 配置白标签名称服务器。

2015 年 2 月 26 日

现在，您可以使用 Route 53 API 按名称的字母顺序列出与 Amazon 账户关联的托管区域。还可以获取与某个账户关联的托管区域的计数。有关更多信息，请参阅亚马逊 Route 53 API 参考GetHostedZoneCount中的ListHostedZonesByName和。

2015 年 2 月 11 日

在此版本中，Route 53 添加了以下新功能：

- 运行状况检查状态 — 现在，Route 53 控制台中的运行状况检查页面包括一个 Status（状态）列，通过该列可查看所有运行状况检查的总体状态。有关更多信息，请参阅 查看运行状况检查状态以及运行状况检查失败的原因。
- 与集成 Amazon CloudTrail — Route 53 现在可以与 Route 53 配合使用， CloudTrail 以捕获有关您的 Amazon 账户向 Route 53 API 发送的每个请求的信息。集成 Route 53， CloudTrail 允许您确定向 Route 53 API 发出了哪些请求、发出每个请求的源 IP 地址、谁发出了请求、何时发出请求等等。有关更多信息，请参阅 使用记录亚马逊 Route 53 API 调用 Amazon CloudTrail。
- 运行状况检查快速警报 — 使用 Route 53 控制台创建运行状况检查时，您现在可以同时为运行状况检查创建 Amazon CloudWatch 警报，并指定在 Route 53 认为终端节点运行状况不佳一分钟内应通知谁。有关更多信息，请参阅 创建和更新运行状况检查。
- 用于托管区域和域的标记 — 现在，您可以将通常用于成本分配的标记分配给 Route 53 托管区域和域。有关更多信息，请参阅 给 Amazon Route 53 资源贴标签。

2015 年 2 月 5 日

现在，您可以使用 Route 53 控制台来更新域的联系人信息。有关更多信息，请参阅 您在注册或转移域时指定的值。

2015 年 1 月 22 日

现在，您可以在利用 Route 53 注册新域名时指定国际化域名。（Route 53 已支持将国际化域名用于托管区域和记录。）有关更多信息，请参阅 DNS 域名格式。

2014 版本

2014 年 11 月 25 日

在此版本中，您现在可以编辑在创建托管区域时为其指定的备注。在控制台中，只需单击 Comment 字段旁的铅笔图标，然后输入新值。有关使用 Route 53 API 更改评论的更多信息，请参阅亚马逊 Route 53 API 参考UpdateHostedZoneComment中的。

2014 年 11 月 5 日

在此版本中，Route 53 添加了以下新功能：

- 使用 Amazon Virtual Private Cloud 服务 VPCs 创建的私有 D NS — 您现在可以使用 Route 53 管理您的内部域名， VPCs 而无需将 DNS 数据暴露给公共互联网。有关更多信息，请参阅 使用私有托管区。
- 运行状况检查失败原因 —现在，您可以查看所选运行状况检查的当前状态，以及有关每个 Route 53 运行状况检查程序报告的运行状况检查上次失败原因的详细信息。状态包含 HTTP 状态代码和失败原因，失败原因包括多种故障类型的信息，如字符串匹配失败和响应超时。有关更多信息，请参阅 查看运行状况检查状态以及运行状况检查失败的原因。
- 可重用的委派集 — 现在您可以将同一组四个权威名称服务器（合称为委派集）应用于与不同域名对应的多个托管区域。这可以大大简化将 DNS 服务迁移到 Route 53 和管理大量托管区域的过程。目前，使用可重用的委派集需要您使用 Route 53 API 或 Amazon 软件开发工具包。有关更多信息，请参阅 Amazon Route 53 API 参考。
- 改进了地理定位路由 — 通过添加对 EDNS0 edns-client-subnet 扩展的支持，我们进一步提高了地理定位路由的准确性。有关更多信息，请参阅 地理位置路由。
- 对签名 v4 的支持 — 现在，您可以使用签名版本 4 签署所有 Route 53 API 请求。有关更多信息，请参阅 Amazon Route 53 API 参考中的签署 Route 53 API 请求。

2014 年 7 月 31 日

在此版本中，您现在可以执行以下操作：

- 使用 Route 53 注册域名。有关更多信息，请参阅 使用 Amazon Route 53 注册和管理域。
- 配置 Route 53，根据生成 DNS 查询的地理位置来响应查询。有关更多信息，请参阅 地理位置路由。

2014 年 7 月 2 日

在此版本中，您现在可以执行以下操作：

- 编辑运行状况检查中的大多数值。有关更多信息，请参阅 创建、更新和删除运行状况检查。
- 使用 Route 53 API 获取 Route 53 运行状况检查程序用于检查资源运行状况的 IP 范围列表。可以使用这些 IP 地址来配置您的路由器和防火墙规则，以允许运行状况检查程序检查您资源的运行状况。有关更多信息，请参阅GetCheckerIpRanges《亚马逊 Route 53 API 参考》。
- 为运行状况检查指定成本分配标签，还允许您为运行状况检查指定名称。有关更多信息，请参阅为运行状况检查命名和添加标签。
- 使用 Route 53 API 获取与您的 Amazon 账户关联的运行状况检查的数量。有关更多信息，请参阅GetHealthCheckCount《亚马逊 Route 53 API 参考》。

2014 年 30 月 4 日

在此版本中，您现在可以创建运行状况检查，并使用域名而不是 IP 地址来指定端点。当终端节点的 IP 地址不是固定的，或者由多个实例（例如 Amazon EC2 或 Amazon RDS 实例）提供服务时 IPs，这很有用。有关更多信息，请参阅 创建和更新运行状况检查。

此外，Amazon Route 53 开发人员指南中以前包含的、有关使用 Route 53 API 的一些信息已移动。现在，所有 API 文档都会显示在 Amazon Route 53 API 参考中。

2014 年 4 月 18 日

在此版本中，当运行状况检查 Port（端口）值为 443 且 Protocol（协议）值为 HTTPS 时，Route 53 会在 `Host` 标头中传递不同的值。现在，在运行状况检查期间，Route 53 会向端点传递一个包含 Host Name（托管区域）字段值的 `Host` 标头。如果您是使用 `CreateHealthCheck` API 操作创建的运行状况检查，则为 `FullyQualifiedDomainName` 元素的值。

有关更多信息，请参阅 创建、更新和删除运行状况检查。

2014 年 9 月 4 日

在此版本中，您现在可以查看当前报告某一端点运行良好的 Route 53 运行状况检查程序的百分比。

此外，Amazon 中的 Health Check Status 指标 CloudWatch 现在仅显示零（如果您的终端节点在给定时间段内运行状况不佳）或一（如果终端节点在该时间段内运行正常）。该指标不再显示介于 0 和 1 之间的值，来反映 Route 53 运行状况检查报告端点运行状况良好的部分。

有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

2014 年 2 月 18 日

在此版本中，Route 53 添加了以下功能：

- 运行状况检查故障转移阈值：您现在可以指定端点的运行状况检查必须连续失败多少次（介于 1 次和 10 次连续检查之间），Route 53 才会认为端点运行状况不佳。运行状况不佳的端点必须通过相同数量的检查，才被视为运行状况良好。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。
- 运行状况检查请求时间间隔：您现在可以指定 Route 53 为了确定端点的运行状况是否良好而向端点发送请求的频率。有效设置为 10 秒和 30 秒。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

2014 年 1 月 30 日

在此版本中，Route 53 添加了以下功能：

- HTTP 和 HTTPS 字符串匹配运行状况检查：Route 53 现在支持运行状况检查根据响应正文中是否出现指定字符串来确定端点的运行状况。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。
- HTTPS 运行状况检查：Route 53 现在支持将运行状况检查应用于仅限 SSL 的安全网站。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。
- **`ChangeResourceRecordSets`** API 操作的 **`UPSERT`**：在使用 `ChangeResourceRecordSets` API 操作创建或更改记录时，现在可以使用 UPSERT 操作在给定名称和类型的记录不存在时创建新记录，或更新现有记录。有关更多信息，请参阅ChangeResourceRecordSets《亚马逊 Route 53 API 参考》。

2014 年 1 月 7 日

在此版本中，Route 53 支持根据指定字符串是否出现在响应正文中来确定端点运行状况的运行状况检查。有关更多信息，请参阅 Amazon Route 53 如何确定运行状况检查是否正常。

2013 版本

2013 年 8 月 14 日

在此版本中，Route 53 支持通过导入 BIND 格式的区域文件来创建记录。有关更多信息，请参阅通过导入区域文件来创建记录。

此外，Route 53 运行状况检查的 CloudWatch 指标已集成到 Route 53 控制台中并进行了简化。有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

2013 年 1 月 26 日

在此版本中，Route 53 增加了对将运行状况检查与 CloudWatch 指标集成的支持，因此您可以执行以下操作：

- 验证是否已正确配置运行状况检查。
- 查看运行状况检查端点在指定时间段内的运行状况。
- 配置 CloudWatch 为在所有 Route 53 运行状况检查器认为您的指定终端节点运行状况不佳时发送亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 警报。

有关更多信息，请参阅 使用 CloudWatch 监控运行状况检查。

2013 年 6 月 11 日

在此版本中，Route 53 增加了对创建别名记录的支持，这些别名记录将 DNS 查询路由到亚马逊 CloudFront 分配的备用域名。可将此功能用于顶级域名的替代域名 (example.com) 和子域的替代域名 (www.example.com)。有关更多信息，请参阅 使用您的域名将流量路由到 Amazon CloudFront 分配。

2013 年 5 月 30 日

在此版本中，Route 53 增加了对评估 ELB 负载均衡器和关联的 Ama EC2 zon 实例运行状况的支持。有关更多信息，请参阅 创建 Amazon Route 53 运行状况检查 。

2013 年 3 月 28 日

重新编写了有关运行状况检查和故障转移的文档，以提高可用性。有关更多信息，请参阅 创建 Amazon Route 53 运行状况检查 。

2013 年 2 月 11 日

在此版本中，Route 53 支持故障转移和运行状况检查。有关更多信息，请参阅 创建 Amazon Route 53 运行状况检查 。

2012 版本

2012 年 3 月 21 日

在此版本中，Route 53 允许您创建延迟记录。有关更多信息，请参阅 基于延迟的路由。

2011 版本

2011 年 12 月 21 日

在此版本中，中的 Route 53 控制台 Amazon Web Services 管理控制台 允许您通过从列表中选择 Elastic Load Balancer 来创建别名记录，而不必手动输入负载均衡器的托管区域 ID 和 DNS 名称。新功能记载在 Amazon Route 53 开发人员指南中。

2011 年 11 月 16 日

在此版本中，您可以使用中的 Route 53 控制台 Amazon Web Services 管理控制台 来创建和删除托管区域，以及创建、更改和删除记录。整个 Amazon Route 53 开发人员指南中都相应地记载了新功能。

2011 年 10 月 18 日

Amazon Route 53 入门指南已合并到 Amazon Route 53 开发人员指南，而开发人员指南已重新整理以增强可用性。

2011 年 5 月 24 日

此版本的 Amazon Route 53 推出了别名记录，从而允许您创建 Zone Apex（机构根网域）别名、加权记录、新 API (2011-05-05) 以及服务等级协议。此外，在经过六个月的 Beta 测试后，Route 53 现已全面推出。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的 Amazon Route 53 产品页和 在别名记录和非别名记录之间进行选择。

2010 版本

2010 年 12 月 5 日

本指南是 Amazon Route 53 开发人员指南的第一个版本。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。