Amazon Virtual Private Cloud

AWS PrivateLink

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

AWS PrivateLink 和 VPC 终端节点

AWS PrivateLink 是一项具有高可用性的可扩展技术，支持您将您的 VPC 私密地连接到支持的 AWS 服务、由其他 AWS 账户托管的服务（VPC 终端节点服务）以及支持的 AWS Marketplace 合作伙伴服务。您无需使用互联网网关、NAT 设备、公有 IP 地址、AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接，就能与该服务通信。因此，您的 VPC 不会对公有 Internet 公开。

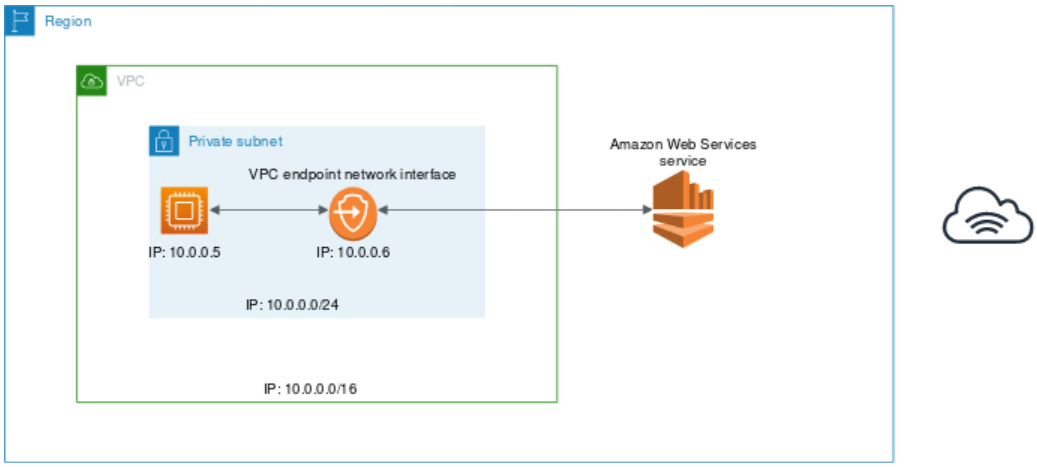
您可以创建自己的 VPC 终端节点服务（由 AWS PrivateLink 提供支持），并支持其他 AWS 客户访问您的服务。

VPC 终端节点概念

以下是 VPC 终端节点的主要概念：

- VPC 终端节点 — VPC 中可让您私下连接到服务的入口点。以下是不同类型的 VPC 终端节点。您可以创建受支持的服务所需要的 VPC 终端节点类型。
  - 网关终端节点 (p. 18)
  - 接口终端节点 (p. 3)
  - 网关负载均衡器终端节点 (p. 15)
- 终端节点服务 — 您 VPC 中自己的应用程序或服务。其他 AWS 委托人可以创建从其 VPC 到您的终端节点服务的终端节点。

要使用 AWS PrivateLink ，请在您的 VPC 中为服务创建 VPC 终端节点。您可以创建受支持的服务所需要的 VPC 终端节点类型。此操作将在您的子网中创建一个带有私有 IP 地址的弹性网络接口，用作发送到服务的流量的入口点。下图显示的基本架构用于将您的 VPC 安全连接到支持 AWS PrivateLink 的 AWS 服务。



与 VPC 终端节点结合使用

您可以使用以下任一方式创建、访问和管理 VPC 终端节点：

- AWS Management Console – 提供您可用来访问 VPC 终端节点的 Web 界面。
- AWS Command Line Interface (AWS CLI) – 为众多 AWS 服务（包括 Amazon VPC）提供命令。AWS CLI 在 Windows、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。

- AWS 开发工具包 – 提供特定于语言的 API。开发工具包关注许多连接详细信息，比如计算签名、处理请求重试和处理错误。有关更多信息，请参阅 AWS 开发工具包。
- 查询 API — 提供您使用 HTTPS 请求调用的低级别 API 操作。使用查询 API 是访问 Amazon VPC 的最直接方式。但是，它需要您的应用程序处理低级别的详细信息，例如生成哈希值以签署请求以及处理错误。有关更多信息，请参阅 Amazon EC2 API 参考。

终端节点配置示例

有关 AWS PrivateLink 和 VPC 对等连接示例的信息，请参阅 Amazon VPC 用户指南中的示例：使用 AWS PrivateLink 和 VPC 对等连接的服务。

终端节点的定价

有关终端节点定价的信息，请参阅 AWS PrivateLink 定价。

VPC 终端节点

VPC 终端节点使您能够在 Virtual Private Cloud (VPC) 与支持的服务和之间建立连接，而无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。因此，您的 VPC 不会对公有 Internet 公开。

VPC 终端节点是虚拟设备。它们是水平扩展、冗余和高度可用的 VPC 组件。以下是不同类型的 VPC 终端节点。您可以创建受支持的服务所需要的 VPC 终端节点类型。

接口终端节点

接口终端节点 (p. 3)是一个弹性网络接口，具有来自子网 IP 地址范围的私有 IP 地址。它可作为发往由 AWS 或者 AWS 客户或合作伙伴拥有的服务的流量入口点。有关与 AWS PrivateLink 集成的 AWS 服务列表，请参阅 支持 AWS PrivateLink 的服务 (p. 61)。

您需要根据每小时使用量付费并支付数据处理费用。有关更多信息，请参阅接口端点定价。

网关负载均衡器终端节点

Gateway Load Balancer 端点 (p. 15)是一个弹性网络接口，具有来自子网 IP 地址范围的私有 IP 地址。它可作为拦截流量并将流量路由到您使用 Gateway Load Balancer 配置的网络或安全服务的入口点。您可以将网关负载均衡器终端节点指定为路由表中路由的目标。仅针对使用 Gateway Load Balancer 配置的端点服务支持 Gateway Load Balancer 端点。

您需要根据每小时使用量付费并支付数据处理费用。有关更多信息，请参阅 Gateway Load Balancer 端点定价。

网关终端节点

网关端点 (p. 18)是一个网关，它是路由表中路由的目标，用于发往 Amazon S3 或 DynamoDB 的流量。

使用网关端点不会产生任何费用。

Amazon S3 同时支持网关端点和接口端点。有关两个选项的对比，请参阅 Amazon S3 用户指南中的适用于 Amazon S3 的 VPC 终端节点类型。

接口 VPC 终端节点（AWS PrivateLink）

利用接口 VPC 终端节点（接口终端节点），您可连接到由 AWS PrivateLink 提供支持的服务。这些服务包括一些 AWS 服务，由其他 AWS 客户和合作伙伴在他们自己的 VPC 中托管的服务（称为终端节点服务），以及受支持的 AWS Marketplace 合作伙伴服务。服务的所有者是服务提供商，您 (作为创建接口终端节点的委托人) 是服务使用者。

以下是设置接口终端节点的常规步骤：

1. 选择要在其中创建接口终端节点的 VPC，然后提供您要连接到的 AWS 服务、终端节点服务或 AWS Marketplace 服务的名称。
2. 在 VPC 中选择使用接口终端节点的子网。我们将在该子网中创建一个终端节点网络接口。终端节点网络接口从您的子网 IP 地址范围分配一个私有 IP 地址，并保留此 IP 地址，直到该接口终端节点被删除为止。您可以在不同的可用区中指定多个子网 (在服务支持的情况下)，以帮助确保您的接口终端节点能够在出现可用区故障时复原。在此情况下，我们将在您指定的每个子网中创建一个终端节点网络接口。

   Note

   终端节点网络接口是由请求者管理的网络接口。您可以在您的账户中查看它，但不能亲自管理。有关更多信息，请参阅请求者托管的网络接口。
3. 指定要与终端节点网络接口关联的安全组。安全组规则将控制从 VPC 中的资源发送到终端节点网络接口的通信。如果您未指定安全组，我们将关联 VPC 的默认安全组。

4. （可选；仅限 AWS 服务和 AWS Marketplace 合作伙伴服务）为终端节点启用私有 DNS (p. 4)，以便您可以使用服务的默认 DNS 主机名对服务发出请求。

   Important

   默认情况下，面向 AWS 服务和 AWS Marketplace 合作伙伴服务创建的终端节点已启用私有 DNS。
   私有 DNS 在其他子网中启用，该子网位于同一 VPC 和可用区或本地扩展区。
5. 当服务提供商与使用者处于不同的账户中时，请参阅 the section called “接口终端节点可用区注意事项” (p. 7) 了解如何使用可用区 ID 识别接口端点可用区。
6. 已创建的接口终端节点在服务提供商接受后即可使用。服务提供商必须将服务配置为自动或手动接受请求。AWS 服务和 AWS Marketplace 服务一般会自动接受所有终端节点请求。有关终端节点生命周期的更多信息，请参阅 接口终端节点生命周期 (p. 6)。

服务无法通过终端节点发起对您的 VPC 中的资源的请求。终端节点仅返回对从您的 VPC 中的资源启动的通信的响应。在集成服务和终端节点之前，请查看特定于服务的 VPC 终端节点文档，了解任何特定于服务的配置和限制。

目录

用于接口终端节点的私有 DNS

Important

Amazon S3 接口终端节点不支持私有 DNS。

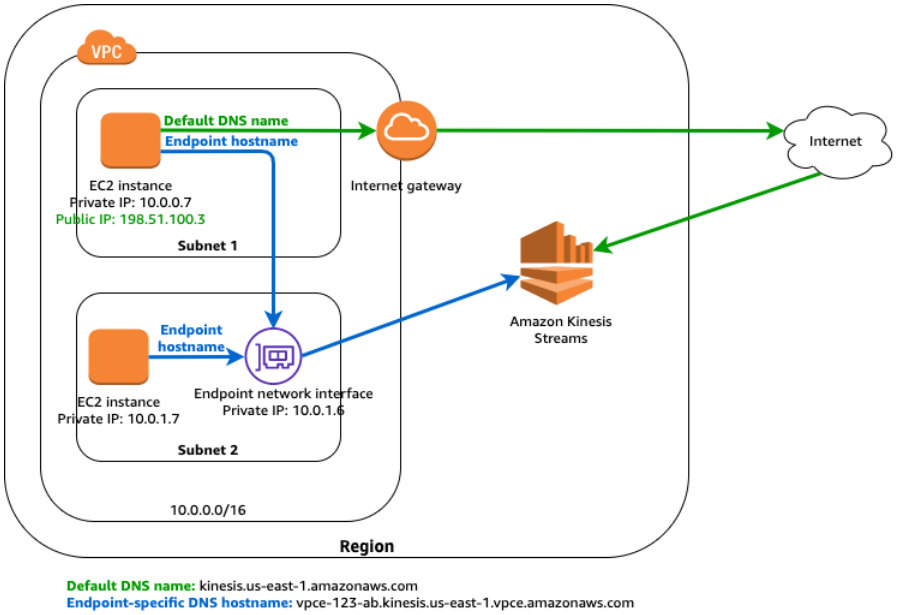
当您创建接口终端节点时，我们将生成您可用于与服务通信的终端节点特定 DNS 主机名。对于 AWS 服务和 AWS Marketplace 合作伙伴服务，私有 DNS 选项（默认开启）会将私有托管区域与您的 VPC 相关联。托管区域包含服务的默认 DNS 名称（例如，`ec2.us-east-1.amazonaws.com`）的记录集，用于解析为您的 VPC 中的终端节点网络接口的私有 IP 地址。这使您能够使用服务的默认 DNS 主机名而不是终端节点特定 DNS 主机名向服务发出请求。例如，如果您的现有应用程序向 AWS 服务发出请求，则这些应用程序将继续通过接口终端节点发出请求，而无需任何配置更改。

在下图显示的示例中，子网 2 中有 Amazon Kinesis Data Streams 的一个接口终端节点和一个终端节点网络接口。您尚未为接口终端节点启用私有 DNS。子网的路由表具有以下路由。

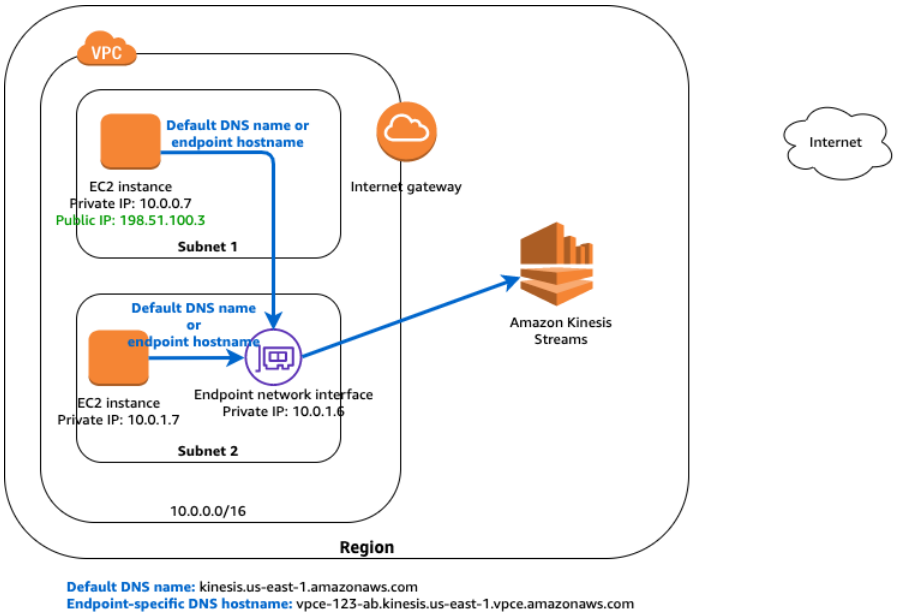
子网 1	
目标	目标
10.0.0.0/16	本地

0.0.0.0/0	internet-gateway-id
子网 2	
目标	目标
10.0.0.0/16	本地

任一子网中的实例都可以使用特定于终端节点的 DNS 主机名通过接口终端节点向 Amazon Kinesis Data Streams 发送请求。子网 1 中的实例可以使用其默认 DNS 名称，通过 AWS 区域中的公有 IP 地址空间与 Amazon Kinesis Data Streams 通信。



在下图中，终端节点的私有 DNS 已启用。任一子网中的实例都可以使用默认的 DSN 主机名或特定于终端节点的 DNS 主机名，通过接口终端节点向 Amazon Kinesis Data Streams 发送请求。



Important

要使用私有 DNS，您必须将以下 VPC 属性设置为 `true`：`enableDnsHostnames` 和 `enableDnsSupport`。有关详细信息，请参阅查看和更新您的 VPC 的 DNS 支持。IAM 用户必须有权使用托管区域。有关更多信息，请参阅 Route 53 的身份验证和访问控制。

接口终端节点属性和限制

要使用接口终端节点，您需要了解它们的属性和当前限制：

- 对于每个接口终端节点，每个可用区您只能选择一个子网。
- 可能无法在所有可用区中通过接口终端节点使用服务。要了解支持的可用区，请使用 describe-vpc-endpoint-services 命令或使用 Amazon VPC 控制台。有关更多信息，请参阅 创建接口终端节点 (p. 8)。
- 创建接口终端节点时，将在映射至您的账户且独立于其他账户的可用区中创建此终端节点。当服务提供商与使用者处于不同的账户中时，请参阅 the section called “接口终端节点可用区注意事项” (p. 7) 了解如何使用可用区 ID 识别接口端点可用区。
- 当服务提供商和使用者具有不同的账户并使用多个可用区，并且使用者查看 VPC 终端节点服务信息时，响应仅包括公共可用区。例如，当服务提供商账户使用 `us-east-1a` 和 `us-east-1c` 而使用者使用 `us-east-1a` 和 `us-east-1b` 时，响应包括公共可用区 `us-east-1a` 中的 VPC 终端节点服务。
- 默认情况下，每个可用区的每个接口终端节点可支持高达 10 Gbps 的带宽，以及高达 40Gbps 的突增。如果您的应用程序需要更高的突增或持续的吞吐量，请联系 AWS Support。
- 如果子网的网络 ACL 限制流量，您可能无法通过终端节点网络接口发送流量。请确保您增加了相应的规则，允许与子网的 CIDR 块之间的往返流量。
- 确保与终端网络接口关联的安全组允许终端网络接口与 VPC 中与此服务通信的资源之间进行通信。为确保命令行工具（例如 AWS CLI）可以通过 HTTPS 从 VPC 中的资源向 AWS 服务发出请求，安全组必须允许入站 HTTPS（端口 443）流量。
- 接口终端节点仅支持 TCP 流量。
- 在创建终端节点时，您可为其连接终端节点策略来控制对连接到的服务的访问。有关更多信息，请参阅策略最佳实践和the section called “控制对服务的访问权限” (p. 33)。
- 查看终端节点服务的服务特定的限制。
- 参与者无法在其未拥有的 VPC 中创建 Amazon Route53 解析程序终端节点。只有 VPC 拥有者才能创建诸如入站终端节点等 VPC 级资源。
- 仅在同一区域内支持终端节点。无法在 VPC 和其他区域内的服务之间创建终端节点。
- 终端节点仅支持 IPv4 流量。
- 无法将终端节点从一个 VPC 转移到另一个 VPC，也无法将终端节点从一项服务转移到另一项服务。
- 您可以为每个 VPC 创建的终端节点的数量有配额。有关更多信息，请参阅 AWS PrivateLink 配额 (p. 67)。

连接到本地数据中心

您可以使用以下类型的连接进行接口终端节点与本地数据中心之间的连接：

- AWS Direct Connect
- AWS Site-to-Site VPN

接口终端节点生命周期

从您创建接口终端节点 (终端节点连接请求) 时开始，接口终端节点将经历不同的阶段。在每个阶段，可能会有一些服务使用者和服务提供商可执行的操作。

以下规则适用：

- 服务提供商可以将其服务配置为自动或手动接受接口终端节点请求。AWS 服务和 AWS Marketplace 服务一般会自动接受所有终端节点请求。
- 服务提供商无法删除连接至其服务的接口终端节点。只有请求接口终端节点连接的服务使用者才可以删除接口终端节点。
- 服务提供商可以在接口终端节点已被接受 (手动或自动) 并处于 `available` 状态之后拒绝它。

接口终端节点可用区注意事项

创建接口终端节点时，将在映射至您的账户且独立于其他账户的可用区中创建此终端节点。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别接口终端节点可用区。例如，`use1-az1` 是 `us-east-1` 区域的可用区 ID，并映射到每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南中您的资源的 AZ ID 或使用 describe-availability-zones。

可能无法在所有可用区中通过接口终端节点使用服务。您可以使用以下操作中的任意一种，了解一项服务有哪些受支持的可用区：

- describe-vpc-endpoint-services (AWS CLI)
- DescribeVpcEndpointServices (API)
- 您创建接口终端结点时使用的 Amazon VPC 控制台。有关更多信息，请参阅 the section called “创建接口终端节点” (p. 8)。

查看可用的 AWS 服务名称

使用 Amazon VPC 控制台创建终端节点时，可以获得可用 AWS 服务名称的列表。

使用 AWS CLI 创建终端节点时，可以先使用 describe-vpc-endpoint-services 命令查看服务名称，然后再使用 create-vpc-endpoint 命令创建终端节点。

Console

使用控制台查看可用的 AWS 服务

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. Service Name (服务名称) 部分将列出可用的服务。

Command line

使用 AWS CLI 查看可用的 AWS 服务

- 使用 describe-vpc-endpoint-services 命令获取您可以连接的可用服务的列表。`ServiceType` 字段指示是通过接口终端节点还是网关终端节点连接到服务。`ServiceName` 字段提供服务的名称。以下示例列出了所有接口端点的名称和拥有者。

```
aws ec2 describe-vpc-endpoint-services --filter "Name=service-
type,Values=Interface" --query "ServiceDetails[*].[ServiceName, Owner]" --output
 table
```

```
-------------------------------------------------------------------
|                    DescribeVpcEndpointServices                  |
+-----------------------------------------------------+----------+
|  aws.sagemaker.us-west-2.notebook                   |  amazon  |
|  aws.sagemaker.us-west-2.studio                     |  amazon  |
|  com.amazonaws.us-west-2.access-analyzer            |  amazon  |
|  com.amazonaws.us-west-2.acm-pca                    |  amazon  |
...
```

使用 AWS Tools for Windows PowerShell 查看可用的 AWS 服务

- Get-EC2VpcEndpointService

使用 API 查看可用的 AWS 服务

- DescribeVpcEndpointServices

创建接口终端节点

要创建接口终端节点，您必须指定要在其中创建接口终端节点的 VPC 和要连接到的服务。

对于 AWS 服务或 AWS Marketplace 合作伙伴服务，您可以选择为终端节点启用私有 DNS (p. 4)，以便您可以使用服务的默认 DNS 主机名向服务发出请求。

> **Important**
>
> 默认情况下，面向 AWS 服务和 AWS Marketplace 合作伙伴服务创建的终端节点已启用私有 DNS。

Console

使用控制台创建连接到 AWS 服务的接口终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service category (服务类别)，请确保选中 AWS services (Amazon 服务)。
4. 对于 Service Name，请选择要连接到的服务。对于 Type，请确保它指示 Interface。
5. 填写以下信息，然后选择 Create endpoint。
   - 对于 VPC，选择要在其中创建端点的 VPC。
   - 对于 Subnets，选择要在其中创建终端节点网络接口的子网 (可用区)。

     并非所有可用区都支持所有 AWS 服务。
   - 要为接口终端节点启用私有 DNS，请选中启用 DNS 名称对应的复选框。

     > **Important**
     >
     > Amazon S3 接口终端节点不支持私有 DNS。

     默认情况下，此选项处于启用状态。要使用私有 DNS 选项，您的 VPC 的以下属性必须设置为 `true`：`enableDnsHostnames` 和 `enableDnsSupport`。有关详细信息，请参阅查看和更新您的 VPC 的 DNS 支持。
   - 对于 Security group，选择要与终端节点网络接口关联的安全组。

- （可选）添加或删除标签。

  [添加标签] 选择 Add tag（添加标签），然后执行以下操作：
  - 对于 Key（键），输入键名称。
  - 对于 Value（值），输入键值。

  [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

要创建连接到终端节点服务的接口终端节点，您必须具有要连接到的服务的名称。服务提供商可为您提供此名称。

创建连接到终端节点服务的接口终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service category，选择 Find service by name。
4. 对于 Service Name，输入服务的名称 (例如，`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) 并选择 Verify。
5. 填写以下信息，然后选择 Create endpoint。
   - 对于 VPC，选择要在其中创建端点的 VPC。
   - 对于 Subnets（子网），选择要在其中创建端点网络接口的子网（可用区）。

     并非所有可用区都支持此服务。
   - 对于 Security group（安全组），选择要与端点网络接口关联的安全组。
   - （可选）添加或删除标签。

     [添加标签] 选择 Add tag（添加标签），然后执行以下操作：
     - 对于 Key（键），输入键名称。
     - 对于 Value（值），输入键值。

     [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

创建连接到 AWS Marketplace 合作伙伴服务的接口终端节点

1. 转至 AWS Marketplace 中的 PrivateLink 页面并向软件即服务 (SaaS) 提供商订阅服务。支持接口终端节点的服务包括通过终端节点进行连接的选项。
2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 在导航窗格中，选择 Endpoints、Create Endpoint。
4. 对于 Service category (服务类别)，选择 Your AWS Marketplace services (您的 Amazon Marketplace 服务)。
5. 选择您已订阅的 AWS Marketplace 服务。
6. 填写以下信息，然后选择 Create endpoint。
   - 对于 VPC，选择要在其中创建终端节点的 VPC。
   - 对于 Subnets，选择要在其中创建终端节点网络接口的子网 (可用区)。

     并非所有可用区都支持此服务。
   - 对于 Security group，选择要与终端节点网络接口关联的安全组。
   - （可选）添加或删除标签。

     [添加标签] 选择 Add tag（添加标签），然后执行以下操作：

- 对于 Key（键），输入键名称。
- 对于 Value (值)，输入键值。

[删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

Command line

使用 AWS CLI 创建接口终端节点

1. 使用 describe-vpc-endpoint-services 命令获取可用服务的列表。在返回的输出中，记录要连接到的服务的名称。`ServiceType` 字段指示是通过接口终端节点还是网关终端节点连接到服务。`ServiceName` 字段提供服务的名称。
2. 要创建接口终端节点，请使用 create-vpc-endpoint 命令并指定 VPC ID、VPC 终端节点（接口）的类型、服务名称、将使用终端节点的子网以及要与终端节点网络接口关联的安全组。

   以下示例创建连接到 Elastic Load Balancing 服务的接口终端节点。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-
abababab --security-group-id sg-1a2b3c4d
```

```
{
    "VpcEndpoint": {
        "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\",
 \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\":
 \"*\"\n    }\n  ]\n}",
        "VpcId": "vpc-ec43eb89",
        "NetworkInterfaceIds": [
            "eni-bf8aa46b"
        ],
        "SubnetIds": [
            "subnet-abababab"
        ],
        "PrivateDnsEnabled": true,
        "State": "pending",
        "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
        "RouteTableIds": [],
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "VpcEndpointId": "vpce-088d25a4bbf4a7abc",
        "VpcEndpointType": "Interface",
        "CreationTimestamp": "2017-09-05T20:14:41.240Z",
        "DnsEntries": [
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-
ks83awe7.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z1K56Z6FNPJRR",
                "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
            }
```

```
        ]
    }
}
```

或者，以下示例创建一个连接到另一账户中的终端节点服务的接口终端节点 (服务提供商将为您提供终端节点服务的名称)。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-
id subnet-abababab --security-group-id sg-1a2b3c4d
```

在返回的输出中，记录 `privateDnsNames` 字段。您可以使用这些 DNS 名称访问 AWS 服务。

描述可用的服务并使用 AWS Tools for Windows PowerShell 创建 VPC 终端节点

- Get-EC2VpcEndpointService
- New-EC2VpcEndpoint

描述可用的服务并使用 API 创建 VPC 终端节点

- DescribeVpcEndpointServices
- CreateVpcEndpoint

查看您的接口终端节点

在创建接口终端节点之后，您可以查看有关它的信息。

Console

使用控制台查看有关接口终端节点的信息

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择您的接口终端节点。
3. 要查看有关接口终端节点的信息，请选择 Details。DNS Names 字段将显示用于访问服务的 DNS 名称。
4. 要查看已创建接口终端节点的子网以及每个子网中的终端节点网络接口的 ID，请选择 Subnets。
5. 要查看与终端节点网络接口关联的安全组，请选择 Security Groups。

Command line

使用 AWS CLI 描述您的接口终端节点

- 您可使用 describe-vpc-endpoints 命令描述您的终端节点。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

使用 AWS Tools for PowerShell 或 API 描述您的 VPC 终端节点

- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints (Amazon EC2 查询 API)

为接口终端节点创建和管理通知

您可以创建通知以接收针对您的接口终端节点上发生的特定事件的提醒。例如，您可在服务提供商接受接口终端节点时收到一封电子邮件。要创建通知，您必须将 Amazon SNS 主题与通知关联。您可以订阅 SNS 主题以在终端节点事件发生时收到电子邮件通知。

您用于通知的 Amazon SNS 主题必须具有允许 Amazon 的 VPC 终端节点服务代表您发布通知的主题策略。确保在您的主题策略中包含以下语句。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南 中的 Amazon SNS 中的 Identity and Access Management。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Command line

使用 AWS CLI 创建和管理通知

1. 要为接口终端节点创建通知，请使用 create-vpc-endpoint-connection-notification 命令。指定 SNS 主题的 ARN、要通知的事件以及终端节点的 ID，如以下示例所示。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events
 Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
```

2. 要查看您的通知，请使用 describe-vpc-endpoint-connection-notifications 命令。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

3. 要更改通知的 SNS 主题或终端节点事件，请使用 modify-vpc-endpoint-connection-notification 命令。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-
id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

4. 要删除通知，请使用 delete-vpc-endpoint-connection-notifications 命令。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

通过接口终端节点访问服务

在创建接口终端节点之后，您可以通过终端节点 URL 将请求提交给支持的服务。您可以使用以下命令：

- 如果您为终端节点启用了私有 DNS（私有托管区域；仅适用于 AWS 服务和 AWS Marketplace 合作伙伴服务），则为该区域的 AWS 服务的默认 DNS 主机名。例如：`ec2.us-east-1.amazonaws.com`。

Important

Amazon S3 接口终端节点不支持私有 DNS。

- 我们为接口终端节点生成的终端节点特定的区域 DNS 主机名。主机名在其名称中包含一个唯一终端节点标识符、服务标识符、区域以及 vpce.amazonaws.com。例如：vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com。
- 我们为终端节点可用的每个可用区生成的终端节点特定区域 DNS 主机名。主机名在其名称中包含可用区。例如：vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com。如果架构隔离可用区（例如，为了故障遏制或降低区域数据传输费用），可使用此选项。

  对区域 DNS 主机名的请求将流至服务提供商账户中的相应可用区位置 (可能没有与您的账户相同的可用区名称)。有关更多信息，请参阅区域和可用区域概念。
- VPC 中的终端节点网络接口的私有 IP 地址。

要获取区域和分区 DNS 名称，请参阅查看您的接口终端节点 (p. 11)。

例如，如果您在某个子网中已具有连接到 Elastic Load Balancing 的接口终端节点且您尚未为其启用私有 DNS 选项，则在该子网中通过一个实例使用以下 AWS CLI 命令来描述您的负载均衡器。此命令将使用终端节点特定的区域 DNS 主机名来使用接口终端节点发出请求。

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

如果您启用私有 DNS 选项，则不必在请求中指定终端节点 URL。AWS CLI 将使用区域 (AWS) 的 elasticloadbalancing.us-east-1.amazonaws.com 服务的默认终端节点。

修改接口终端节点

您可以修改接口终端节点的以下属性：

- 接口终端节点所在的子网
- 与终端网络接口关联的安全组
- 标签
- 私有 DNS 选项

Note

启用私有 DNS 时，私有 IP 地址可能需要几分钟才能变为可用。

- 终端节点策略（如果服务支持）

如果您删除接口终端节点的子网，则将删除子网中相应的终端节点网络接口。

Console

更改接口终端节点的子网

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择接口终端节点。
3. 选择 Actions、Manage Subnets。
4. 根据要求选择或取消选择子网，然后选择 Modify Subnets。

添加或删除与接口终端节点关联的安全组

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择接口终端节点。
3. 选择 Actions、Manage security groups。
4. 根据要求选择或取消选择安全组，然后选择 保存。

添加或删除接口终端节点标签

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点。
3. 选择接口终端节点，然后选择操作、添加/编辑标签。
4. 添加或删除标签。

   [添加标签] 选择创建标签，然后执行以下操作：

   - 对于 Key (键)，输入键名称。
   - 对于 Value（值），输入键值。

   [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

修改私有 DNS 选项

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择接口终端节点。
3. 选择 Actions (操作)，Modify Private DNS names (修改私有 DNS 名称)。
4. 根据需要设置该选项，然后选择 Modify Private DNS names (修改私有 DNS 名称)。

更新终端节点策略

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择接口终端节点。
3. 选择 Actions、Edit policy。
4. 选择 Full Access (完全访问) 以允许对服务进行完全访问，或者选择 Custom (自定义) 并指定自定义策略。选择 Save（保存）。

Command line

使用 AWS CLI 修改 VPC 终端节点

1. 使用 describe-vpc-endpoints 命令获取您的接口终端节点的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 以下示例使用 modify-vpc-endpoint 命令将子网 `subnet-aabb1122` 添加到接口终端节点。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-
id subnet-aabb1122
```

使用 AWS Tools for Windows PowerShell 或 API 修改 VPC 终端节点

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (Amazon EC2 查询 API)

使用 AWS Tools for Windows PowerShell 或 API 添加或删除 VPC 终端节点标签

- tag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)
- untag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)

网关负载均衡器终端节点 (AWS PrivateLink)

网关负载均衡器终端节点使您能够拦截流量并将流量路由到您使用网关负载均衡器配置用于安全检查等的服务。服务的拥有者是服务提供商，您 (作为创建网关负载均衡器终端节点的委托人) 是服务使用者。

以下是设置网关负载均衡器终端节点的常规步骤：

1. 确保已配置网关负载均衡器终端节点服务。有关更多信息，请参阅 网关负载均衡器端点的 VPC 终端节点服务 (p. 38)。
2. 选择要在其中创建网关负载均衡器终端节点的 VPC，然后提供服务的名称。
3. 在 VPC 中选择使用网关负载均衡器终端节点的子网。我们将在该子网中创建一个终端节点网络接口。终端节点网络接口从您的子网 IP 地址范围分配一个私有 IP 地址，并保留此 IP 地址，直到该网关负载均衡器终端节点被删除为止。

   Note

   终端节点网络接口是由请求者管理的网络接口。您可以在您的账户中查看它，但不能亲自管理。有关更多信息，请参阅请求者托管的网络接口。
4. 已创建的网关负载均衡器终端节点在服务提供商接受后即可使用。服务提供商可以将服务配置为自动或手动接受请求。
5. 配置子网路由表和网关路由表以将流量指向网关负载均衡器终端节点。有关更多信息，请参阅 Amazon VPC 用户指南中的路由到网关负载均衡器终端节点。

目录

网关负载均衡器终端节点属性和限制

要使用网关负载均衡器终端节点，请注意以下事项：

- 对于每个网关负载均衡器终端节点，您只能在 VPC 中选择一个可用区 (子网)。以后您不能更改子网。要在不同子网中使用网关负载均衡器终端节点，请在该子网中创建新的网关负载均衡器终端节点。您可以针对服务为每个可用区创建单个 Gateway Load Balancer 端点，但仅能够针对 Gateway Load Balancer 支持的可用区创建。

- 每个网关负载均衡器终端节点最高支持 40Gbps 的带宽。
- 如果子网的网络 ACL 限制流量，您可能无法通过网关负载均衡器终端节点发送流量。请确保您增加了相应的规则，允许与子网的 CIDR 块之间的往返流量。
- 不支持安全组。
- 不支持终端节点策略。
- 可能无法在所有可用区中通过网关负载均衡器终端节点使用服务。要了解支持的可用区，请使用 describe-vpc-endpoint-services 命令或使用 Amazon VPC 控制台。有关更多信息，请参阅 创建网关负载均衡器终端节点 (p. 16)。
- 创建网关负载均衡器终端节点时，将在映射至您的账户且独立于其他账户的可用区中创建此终端节点。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别终端节点可用区。例如，`use1-az1` 是 `us-east-1` 区域的可用区 ID，并映射到每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南中您的资源的 AZ ID 或使用 describe-availability-zones。
- 要将流量保持在同一可用区内，我们建议您在将向其发送流量的每个可用区中创建网关负载均衡器终端节点。
- 仅在同一区域内支持终端节点。无法在 VPC 和其他区域内的服务之间创建终端节点。
- 终端节点仅支持 IPv4 流量。
- 无法将终端节点从一个 VPC 转移到另一个 VPC，也无法将终端节点从一项服务转移到另一项服务。
- 您可以为每个 VPC 创建的终端节点的数量有配额。有关更多信息，请参阅 AWS PrivateLink 配额 (p. 67)。

网关负载均衡器终端节点生命周期

从您创建网关负载均衡器终端节点（终端节点连接请求）时开始，网关负载均衡器终端节点将经历不同的阶段。在每个阶段，可能会有一些服务使用者和服务提供商可执行的操作。

以下规则适用：

- 服务提供商可将其服务配置为自动或手动接受网关负载均衡器终端节点请求。
- 服务提供商无法删除连接至其服务的网关负载均衡器终端节点。只有请求连接的服务使用者才可以删除网关负载均衡器终端节点。
- 服务提供商可以在网关负载均衡器终端节点被接受并处于 `available` 状态后拒绝该终端节点。

网关负载均衡器终端节点的定价

您在为某个服务创建和使用网关负载均衡器终端节点时需要付费。将按小时使用费率和数据处理费率收费。有关更多信息，请参阅 AWS PrivateLink 定价。您可以使用 Amazon VPC 控制台或 AWS CLI 查看网关负载均衡器终端节点的总数。

创建网关负载均衡器终端节点

要创建网关负载均衡器终端节点，您必须指定要在其中创建该终端节点的 VPC 和要连接到的服务。

Console

要创建网关负载均衡器终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service category，选择 Find service by name。
4. 对于 Service Name（服务名称），输入服务的名称并选择 Verify（验证）。

5. 填写以下信息，然后选择 Create endpoint。
   - 对于 VPC，选择要在其中创建终端节点的 VPC。
   - 对于 Subnets（子网），选择要在其中创建网关负载均衡器终端节点网络接口的子网（可用区）。
   - （可选）要添加标签，选择 Add tag（添加标签），然后为标签指定键和值。

Command line

使用 AWS CLI 创建网关负载均衡器终端节点。

使用 create-vpc-endpoint 命令，并指定 VPC ID、VPC 终端节点（网关负载均衡器）的类型、服务名称以及在其中创建网关负载均衡器终端节点的子网。

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --vpc-id vpc-id --
subnet-ids subnet-id --service-name gateway-load-balancer-service-name
```

使用 AWS Tools for Windows PowerShell 或 API 创建 VPC 终端节点

- New-EC2VpcEndpoint
- CreateVpcEndpoint

查看网关负载均衡器终端节点

在创建网关负载均衡器终端节点之后，您可以查看有关它的信息。

Console

要使用控制台查看有关网关负载均衡器终端节点的信息

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中选择 Endpoints（终端节点）并选择您的网关负载均衡器终端节点。
3. 选择 Details。
4. 要查看已创建网关负载均衡器终端节点的子网以及终端节点网络接口的 ID，请选择 Subnets（子网）。

Command line

要使用命令行工具或 API 描述网关负载均衡器终端节点

- describe-vpc-endpoints (AWS CLI)
- Get-EC2VpcEndpoint（适用于 Windows PowerShell 的 AWS 工具）
- DescribeVpcEndpoints（Amazon EC2 查询 API）

为网关负载均衡器终端节点添加或删除标签

您可以添加或删除网关负载均衡器终端节点的标签。

Console

要添加或删除标签

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。

2. 在导航窗格中，选择终端节点。
3. 选择网关负载均衡器终端节点，选择 Actions（操作）、Add/Edit Tags（添加/编辑标签）。
4. 添加或删除标签。

   [添加标签] 选择创建标签，然后执行以下操作：
   - 对于 Key (键)，输入键名称。
   - 对于 Value (值)，输入键值。

   [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

Command line

要使用命令行工具或 API 添加或删除标签

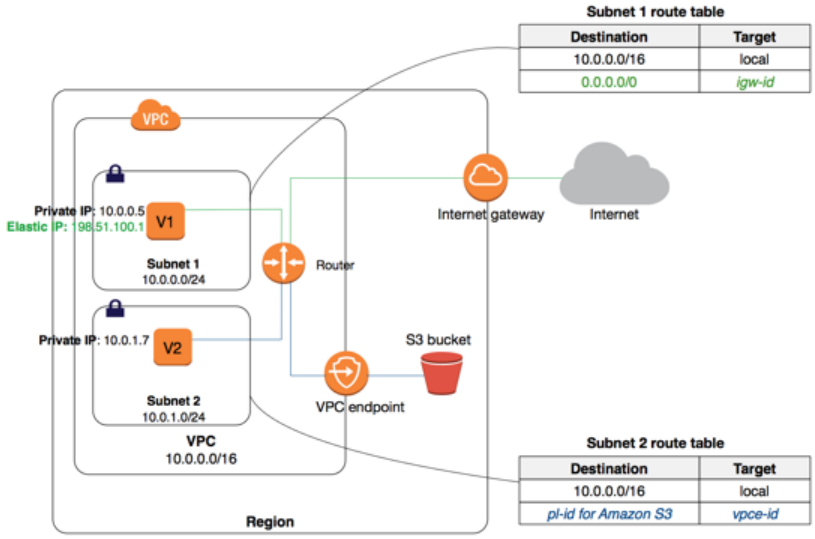
- 使用 create-tags 和 delete-tags。(AWS CLI)
- 使用 New-EC2Tag 和 Remove-EC2Tag (AWS Tools for Windows PowerShell)
- 使用 CreateTags 和 DeleteTags。（Amazon EC2 查询 API）

网关 VPC 终端节点

要创建和设置网关终端节点，请执行以下常规步骤：

1. 指定要在其中创建终端节点的 VPC 以及要连接到的服务。服务由 AWS 托管的前缀列表（即某个区域的服务的名称和 ID）标识。AWS 前缀列表 ID 使用 `pl-xxxxxxx` 格式，AWS 前缀列表名称使用“com.amazonaws.*region*.*service*”格式。使用 AWS 前缀列表名称（服务名称）创建终端节点。
2. 向终端节点连接终端节点策略，该策略允许您对要连接的部分或所有服务进行访问。有关更多信息，请参阅 使用 VPC 终端节点策略 (p. 33)。
3. 指定一个或多个路由表，在其中创建到服务的路由。路由表将控制 VPC 与其他服务之间的流量的路由。与其中任一路由表相关联的每个子网都可以访问终端节点，随后通过终端节点将来自这些子网实例的流量路由到服务。

在下图中，子网 2 中的实例可通过网关终端节点访问 Amazon S3。



您可以在单个 VPC 中创建多个终端节点 (例如，针对多项服务)。您还可以为单项服务创建多个终端节点，并使用不同的路由表通过同一服务的多个子网强制执行不同的访问策略。

创建终端节点后，您可以修改已连接到终端节点的终端节点策略，并添加或删除终端节点使用的路由表。

目录

网关终端节点的定价

使用网关终端节点不会发生任何额外费用。采用标准的数据传输和资源使用计费方式。有关定价的更多信息，请参阅 Amazon EC2 定价。

网关终端节点路由

在创建或修改终端节点时，您将指定用于通过终端节点访问服务的 VPC 路由表。路由会自动添加到每个路由表中，同时会添加一个指定服务 (`pl-xxxxxxxx`) 的AWS前缀列表 ID 的目的地，以及一个具有终端节点 ID (`vpce-xxxxxxxx`) 的目标；例如：

目的地	目标
10.0.0.0/16	本地
pl-1a2b3c4d	vpce-11bb22cc

前缀列表 ID 从逻辑上代表服务使用的公有 IP 地址的范围。与指定路由表关联的子网中的所有实例会自动使用该终端节点来访问服务。未与指定路由表关联的子网不使用终端节点。这使您能够将其他子网中的资源与您的终端节点分离。

要查看服务的当前公有 IP 地址范围，您可以使用 describe-prefix-lists 命令发布的当前 IP 地址范围的列表。中的AWS IP 地址范围。

> **Note**
>
> 服务的公有 IP 地址的范围可能会不时更改。在根据服务的当前 IP 地址范围决定路由目标或做其他决策之前，请考虑产生的影响。

以下规则适用：

- 您可以在一个路由表中拥有针对不同服务的多个终端节点路由，并且可以在不同的路由表中拥有针对同一服务的多个终端节点路由。但不能在一个路由表中拥有针对同一服务的多个终端节点路由。例如，如果您在 VPC 中创建了两个针对 Amazon S3 的终端节点，则您不能在同一路由表中同时为这两个终端节点创建终端节点路由。

- 您无法通过使用路由表 API 或 Amazon VPC 控制台中的“路由表”页面来在您的路由表中显式添加、修改或删除终端节点路由。您只能通过将路由表与终端节点关联来添加终端节点路由。要更改与终端节点关联的路由表，您可以修改终端节点 (p. 32)。
- 在您从终端节点删除路由表关联 (通过修改终端节点) 或删除终端节点时，将自动删除终端节点路由。

我们使用与流量匹配的最明确路由以判断数据流的路由方式 (最长前缀匹配)。如果您的路由表中有针对指向互联网网关的所有 Internet 流量 (`0.0.0.0/0`) 的现有路由，则终端节点路由将优先于目标设定为服务的所有流量，因为服务的 IP 地址范围比 `0.0.0.0/0` 更具体。所有其他 Internet 流量（包括目标设定为其他区域内的服务的流量）将流向互联网网关。

但是，如果您有针对指向互联网网关或 NAT 设备的 IP 地址范围的现有、更具体的路由，则这些路由将优先。如果您有目标设定为与服务所使用的 IP 地址范围相同的 IP 地址范围的现有路由，则您的路由将优先。

示例：路由表中的终端节点路由

在此方案中，您的路由表中有一个针对指向互联网网关的所有 Internet 流量 (`0.0.0.0/0`) 的现有路由。来自子网的目标设定为其他 AWS 服务的任何流量将使用互联网网关。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-1a2b3c4d

创建指向支持的 AWS 服务的终端节点，并将您的路由表与该终端节点关联。将为路由表自动添加一个终端节点路由，其目的地为 `pl-1a2b3c4d`（假设这表示您已为其创建终端节点的服务）。现在，来自子网的目标设定为同一区域内的 AWS 服务的任何流量将流向该终端节点，而不是流向互联网网关。所有其他 Internet 流量（包括目标设定为其他服务的流量和目标设定为其他区域内的 AWS 服务的流量）将流向互联网网关。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

示例：针对终端节点调整路由表

在此方案中，`54.123.165.0/24` 在 Amazon S3 的 IP 地址范围内，您将路由表配置为允许子网中的实例通过互联网网关与 Amazon S3 存储桶进行通信。您已添加一个以 `54.123.165.0/24` 为目的地并指向互联网网关的路由。然后创建一个终端节点，并将此路由表与该终端节点关联。这会自动将一个终端节点路由添加到路由表。然后使用 describe-prefix-lists 命令查看 Amazon S3 的 IP 地址范围。该范围为 `54.123.160.0/19` (它没有指向互联网网关的范围那么具体)。这意味着，目标设定为 `54.123.165.0/24` IP 地址范围的任何流量将继续使用互联网网关，而不使用终端节点（前提是这仍是 Amazon S3 的公有 IP 地址范围）。

目的地	目标
10.0.0.0/16	本地
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

要确保通过终端节点来路由目标设定为相同区域内的 Amazon S3 的所有流量，您必须调整路由表中的路由。为此，您可以删除针对互联网网关的路由。现在，针对相同区域内的 Amazon S3 的所有流量将使用终端节点，并且与您的路由表关联的子网为私有子网。

目的地	目标
10.0.0.0/16	本地
pl-1a2b3c4d	vpce-11bb22cc

网关终端节点限制

要使用网关终端节点，您需要了解当前限制：

- 您无法在网络 ACL 的出站规则中使用 AWS 前缀列表 ID 来允许或拒绝至终端节点中所指定服务的出站流量。如果您的网络 ACL 规则限制流量，则必须为服务指定 CIDR 块 (IP 地址范围)。但是，您可在出站安全组规则中使用 AWS 前缀列表 ID。有关更多信息，请参阅 安全组 (p. 34)。
- 仅在同一区域内支持终端节点。无法在 VPC 和其他区域内的服务之间创建终端节点。
- 终端节点仅支持 IPv4 流量。
- 无法将终端节点从一个 VPC 转移到另一个 VPC，也无法将终端节点从一项服务转移到另一项服务。
- 您可以为每个 VPC 创建的终端节点的数量有配额。有关更多信息，请参阅 AWS PrivateLink 配额 (p. 67)。
- 无法将终端节点连接扩展到 VPC 之外。VPC 中的 VPN 连接、VPC 对等连接、中转网关、AWS Direct Connect 连接或 ClassicLink 连接的另一端的资源，不能使用终端节点来与终端节点服务中的资源通信。
- 您必须在您的 VPC 中启用 DNS 解析，或者，如果您使用自己的 DNS 服务器，请确保将针对所需服务（如 Amazon S3）的 DNS 请求正确解析为维护的 IP 地址AWS 有关更多信息，请参阅 Amazon VPC 用户指南中的在您的 VPC 中使用 DNS 和 Amazon Web Services 一般参考中的 AWS IP 地址范围。
- 查看终端节点服务的服务特定的限制。

有关特定于 Amazon S3 的规则和限制的更多信息，请参阅 Amazon S3 的终端节点 (p. 21)。

有关特定于 DynamoDB 的规则和限制的更多信息，请参阅 适用于 Amazon DynamoDB 的终端节点 (p. 27)。

Amazon S3 的终端节点

如果您已设置从 VPC 访问 Amazon S3 资源的权限，则在您设置终端节点后可继续使用 Amazon S3 DNS 名称来访问这些资源。但请注意以下几点：

- 您的终端节点具有可控制使用终端节点访问 Amazon S3 资源的策略。默认策略允许 VPC 中的任何用户或服务使用来自任何 AWS 账户 的凭证访问任何 Amazon S3 资源；包括与 VPC 关联的账户之外的 AWS 账户 的 Amazon S3 资源。有关更多信息，请参阅 使用 VPC 终端节点控制对服务的访问权限 (p. 33)。
- Amazon S3 从受影响子网的实例收到的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。终端节点将切换网络路由，并断开打开的 TCP 连接。以前使用公有 IPv4 地址的连接不会恢复。建议您在创建或修改终端节点时不要运行任何重要任务；或进行测试以确保您的软件在连接中断后可自动重新连接到 Amazon S3。
- 您不能使用 IAM 策略或存储桶策略允许从 VPC IPv4 CIDR 范围（私有 IPv4 地址范围）进行访问。VPC CIDR 块可能重叠或相同，这可能会导致意外结果。因此，对于通过 VPC 终端节点向 Amazon S3 发出的请求，无法在 IAM 策略中使用 `aws:SourceIp` 条件。这适用于用户和角色的 IAM 策略以及任何存储桶策略。如果语句包含 `aws:SourceIp` 条件，则该值不与任何提供的 IP 地址或范围匹配。您可以改而执行以下操作：
  - 使用路由表来控制哪些实例可以通过终端节点访问 Amazon S3 中的资源。

  - 对于存储桶策略，您可以限制对特定终端节点或特定 VPC 的访问。有关更多信息，请参阅 Amazon S3 存储桶策略 (p. 25)。
- 终端节点当前不支持跨区域请求 — 确保在您的存储桶所在的区域内创建终端节点。您可以使用 Amazon S3 控制台或 get-bucket-location 命令来查找存储桶的位置。使用区域特定的 Amazon S3 终端节点访问存储桶；例如，`mybucket.s3.us-west-2.amazonaws.com`。有关 Amazon S3 的特定于区域的终端节点的更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Simple Storage Service (S3)。如果您使用 AWS CLI 向 Amazon S3 发起请求，请将默认区域设置为您的存储桶所在的相同区域，或在请求中使用 `--region` 参数。

    Note

    将 Amazon S3 的美国标准区域视为映射到该 `us-east-1` 区域。
- 终端节点目前只支持 IPv4 流量。

在对 Amazon S3 使用终端节点之前，确保您已阅读下面的一般限制：网关终端节点限制 (p. 21)。有关创建和查看 S3 存储桶的信息，请参阅 Amazon Simple Storage Service 用户指南中的如何创建 S3 存储桶和如何查看 S3 存储桶的属性。

如果您在 VPC 中使用其他 AWS 服务，它们可能会对特定任务使用 S3 存储桶。确保终端节点策略允许对 Amazon S3 进行完全访问（默认策略），或允许对这些服务所使用的特定存储桶进行访问。或者，仅在未由这些服务中的任一服务使用的子网中创建终端节点，以允许这些服务继续使用公有 IP 地址访问 S3 存储桶。

下表列出了可能受终端节点影响的 AWS 服务，以及每项服务的任何具体信息。

AWS服务	注意
Amazon AppStream 2.0	您的终端节点策略必须允许访问 AppStream 2.0 用于存储用户内容的特定存储桶。有关更多信息，请参阅 Amazon AppStream 2.0 管理指南 中的将 Amazon S3 VPC 终端节点用于主文件夹和应用程序设置持久性。
AWS CloudFormation	如果您的 VPC 中的资源必须响应等待条件或自定义资源请求，则您的终端节点策略必须至少允许对这些资源所使用的特定存储桶的访问。有关更多信息，请参阅为 AWS CloudFormation 设置 VPC 终端节点。
CodeDeploy	您的终端节点策略必须允许对 Amazon S3 进行完全访问，或允许对您已为 CodeDeploy 部署创建的任何 S3 存储桶进行访问。
Elastic Beanstalk	您的终端节点策略必须至少允许对用于 Elastic Beanstalk 应用程序的任何 S3 存储桶进行访问。有关更多信息，请参阅 AWS Elastic Beanstalk 开发人员指南中的将 Elastic Beanstalk 与 Amazon S3 配合使用。
Amazon EMR	您的终端节点策略必须允许访问 Amazon Linux 存储库和由 Amazon EMR 使用的其他存储桶。有关更多信息，请参阅 Amazon EMR 管理指南 中的私有子网的最低 Amazon S3 策略。
AWS OpsWorks	您的终端节点策略必须至少允许对 使用的特定存储桶进行访问AWS OpsWorks 有关更多信息，请参阅 AWS OpsWorks 用户指南中的在 VPC 中运行堆栈。

AWS服务	注意
AWS Systems Manager	您的终端节点策略必须允许访问补丁管理器在您的 AWS 区域用于补丁基准操作的 Amazon S3 存储桶。这些存储桶包含由补丁基准服务检索并在实例上运行的代码。有关更多信息，请参阅 AWS Systems Manager 用户指南中的创建 Virtual Private Cloud 终端节点。 有关 SSM Agent 执行操作所需的 S3 存储桶权限的列表，请参阅 AWS Systems Manager 用户指南中的 SSM 代理的最低 S3 存储桶权限。
Amazon Elastic Container Registry	您的终端节点策略必须允许访问 Amazon ECR 用于存储 Docker 镜像层的 Amazon S3 存储桶。有关更多信息，请参阅 Amazon Elastic Container Registry 用户指南 中的适用于 Amazon ECR 的最低 Amazon S3 存储桶权限。
Amazon WorkDocs	如果您在 WorkSpaces 或 EC2 实例中使用 Amazon WorkDocs 客户端，则终端节点策略必须允许对 Amazon S3 的完全访问权限。
WorkSpaces	WorkSpaces 不直接依赖于 Amazon S3。但如果您向 WorkSpaces 用户提供 Internet 访问权限，则请记住，来自其他公司的网站、HTML 电子邮件和 Internet 服务可能取决于 Amazon S3。确保您的终端节点策略允许对 Amazon S3 进行完全访问，以便这些服务能够继续正常运行。

您的 VPC 和 S3 存储桶之间的流量不会脱离 Amazon 网络。

Amazon S3 终端节点策略

下面是访问 Amazon S3 的终端节点策略示例。有关更多信息，请参阅 使用 VPC 终端节点策略 (p. 33)。由用户决定满足其业务需求的策略限制。

> **Important**
>
> 所有类型的策略 — IAM 用户策略、终端节点策略、S3 存储桶策略和 Amazon S3 ACL 策略（如果有）— 都必须授予必要权限以便成功访问 Amazon S3。
> AWS建议您在将终端节点的使用限制为特定调用者时，在 VPC 终端节点策略中使用 IAM 条件而不是 IAM `Principal` 元素。这些条件的示例有 `aws:PrincipalArn`、`aws:PrincipalAccount`、`aws:PrincipalOrgId`、和 `aws:PrincipalOrgPaths`。有关条件上下文键的更多信息，请参阅 AWS Identity and Access Management 用户指南中的 AWS 全局条件上下文键。

Example 示例：限制对特定存储桶的访问

您可以创建一个策略来仅允许访问特定 S3 存储桶。如果您的 VPC 中有使用 S3 存储桶的其他 AWS 服务，这会非常有用。以下是仅允许访问指定存储桶的策略的示例。

```
{
  "Effect": "Allow",
  "Action": [
     "s3:ListBucket",
     "s3:GetObject",
```

```
      "s3:PutObject"
   ],
   "Resource": [
      "arn:aws:s3:::example-bucket",
      "arn:aws:s3:::example-bucket/*"
   ]
}
```

Example 示例：将此 VPC 终端节点的使用限制为账户中的特定 IAM 角色

您可以创建将 VPC 终端节点的使用限制为特定 IAM 角色的策略。以下是仅允许访问指定账户中指定角色的示例。

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 示例：将此 VPC 终端节点的使用限制为特定账户中的用户

您可以创建将 VPC 终端节点的使用限制为特定账户的策略。以下是仅允许访问指定账户中用户的示例。

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

Example 示例：允许对 Amazon Linux AMI 存储库的访问

每个区域中的 Amazon Linux AMI 存储库都是 Amazon S3 存储桶。如果您希望 VPC 中的实例通过终端节点访问该存储库，请创建终端节点策略以允许对这些存储桶进行访问。

以下策略授予对 Amazon Linux 存储库的访问权限。

您需要将 `region` 替换为您的 AWS 区域，例如 us-east-1。

```
{
  "Statement": [
    {
      "Sid": "AmazonLinuxAMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
```

```
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*"
      ]
    }
  ]
}
```

以下策略授予对 Amazon Linux 2 存储库的访问权限。

您需要将 `region` 替换为您的 AWS 区域，例如 us-east-1。

```
{
  "Statement": [
    {
      "Sid": "AmazonLinux2AMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*"
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
}
```

Amazon S3 存储桶策略

您可以使用存储桶策略来控制从特定终端节点、VPC、IP 地址或 AWS 账户 对存储桶的访问。

对于通过 VPC 终端节点向 Amazon S3 发出的请求，无法在存储桶策略中使用 `aws:SourceIp` 条件。此条件未匹配任何指定的 IP 地址或 IP 地址范围，如果您向 Amazon S3 存储桶发出请求，可能不会有预期的效果。例如：

- 您的存储桶策略具有 `Deny` 效果和 `NotIpAddress` 条件，即仅从单个 IP 地址或有限 IP 地址范围获得访问权。对于通过终端节点向存储桶发出的请求，始终匹配 `NotIpAddress` 条件，并且语句的效果适用 (假定策略中的其他限制匹配)。对存储桶的访问被拒绝。
- 您的存储桶策略具有 `Deny` 效果和 `IpAddress` 条件，即仅拒绝对单个 IP 地址或有限 IP 地址范围的访问。对于通过终端节点向存储桶发出的请求，条件不匹配，并且语句不适用。假定有其他语句允许在无 `IpAddress` 条件时访问，则允许对存储桶的访问。

反之，请使用 `aws:VpcSourceIp` 控制从特定 IP 地址范围的访问。

要使 IAM 用户能够使用存储桶策略，您必须向他们授予使用 `s3:GetBucketPolicy` 和 `s3:PutBucketPolicy` 操作的权限。

有关 Amazon S3 的存储桶策略的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用存储桶策略和用户策略。

Example 示例：限制对特定终端节点的访问

您可以使用 `aws:sourceVpce` 条件来创建用于限制对特定终端节点的访问的存储桶策略。下面是一个 S3 存储桶策略示例，该存储桶仅允许从端点 `vpce-1a2b3c4d` 访问存储桶 `example_bucket`。如果未使用指

定的终端节点，则该策略拒绝对存储桶的所有访问。aws:sourceVpce 条件不需要 VPC 终端节点资源的 ARN，而只需要终端节点 ID。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example 示例：限制对特定 VPC 的访问

您可以使用 aws:sourceVpc 条件来创建存储桶策略，用于限制对特定 VPC 的访问。如果您在同一 VPC 中配置了多个终端节点，并且您希望管理对所有终端节点的 S3 存储桶的访问，这会非常有用。下面是允许 VPC vpc-111bbb22 访问 example_bucket 及其对象的策略的示例。如果未使用指定的 VPC，则该策略拒绝对存储桶的所有访问。aws:sourceVpc 条件不需要 VPC 资源的 ARN，而只需要 VPC ID。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

Example 示例：限制对特定 IP 地址范围的访问

您可以使用 aws:VpcSourceIp 条件来创建策略，用于限制对特定 IP 地址范围的访问。下面是允许 172.31.0.0/16 访问 example_bucket 及其对象的策略的示例。该策略拒绝从其他 IP 地址范围访问存储桶。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-CIDR-only",
```

```
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example 示例：限制对特定 AWS 账户 中存储桶的访问

您可以使用 `s3:ResourceAccount` 条件来创建策略，用于限制对特定 AWS 账户 中 S3 存储桶的访问。如果您希望限制 VPC 内的客户端访问您不拥有的存储桶，这将非常有用。以下是一个策略示例，该策略限制对单个 AWS 账户 （账户 ID 为 `111122223333`）所拥有的资源的访问。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

适用于 Amazon DynamoDB 的终端节点

如果您已设置从 VPC 访问 DynamoDB 表，则您可以继续访问这些表，如同您在设置网关终端节点后通常访问一样。但请注意以下几点：

- 您的终端节点具有可控制使用终端节点访问 DynamoDB 资源的策略。默认策略允许 VPC 内的任何用户或服务使用任何AWS账户中的凭证访问任何 DynamoDB 资源。有关更多信息，请参阅 使用 VPC 终端节点控制对服务的访问权限 (p. 33)。
- DynamoDB 不支持基于资源的策略（例如，针对表）。对 DynamoDB 的访问权限通过各个 IAM 用户和角色的终端节点策略和 IAM 策略进行控制。
- 终端节点当前不支持跨区域请求 — 确保在您的 DynamoDB 表所在的区域内创建终端节点。
- 如果您使用 AWS CloudTrail 记录 DynamoDB 操作，则日志文件包含 VPC 中 EC2 实例的私有 IP 地址和通过终端节点执行的任何操作的终端节点 ID。
- 您的受影响子网中实例的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。终端节点将切换网络路由，并断开打开的 TCP 连接。以前使用公有 IPv4 地址的连接不会恢复。建议您在创建或修改终端节点时不要运行任何重要任务；或进行测试以确保您的软件在连接中断后可自动重新连接到 DynamoDB。

在对 DynamoDB 使用终端节点之前，确保您已阅读下面的一般限制：网关终端节点限制 (p. 21)。

有关创建网关 VPC 终端节点的更多信息，请参阅网关 VPC 终端节点 (p. 18)。

DynamoDB 终端节点策略

终端节点策略是 IAM 策略，您可以将其附加到终端节点以允许访问您要连接的部分或所有服务。下面是访问 DynamoDB 的终端节点策略示例。

> **Important**
>
> 所有类型的策略（IAM 用户策略和终端节点策略）都必须授予必要权限以便成功访问 DynamoDB。

Example 示例：只读访问权限

您可以创建通过 VPC 终端节点将操作限制为仅列出和描述 DynamoDB 表的策略。

```
{
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Example 示例：限制对特定表的访问权限

您可以创建限制对特定 DynamoDB 表的访问权限的策略。在此示例中，终端节点策略仅允许访问 `StockTable`。

```
{
  "Statement": [
    {
      "Sid": "AccessToSpecificTable",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"
    }
  ]
}
```

使用 IAM 策略控制对 DynamoDB 的访问权限

您可以为 IAM 用户、组或角色创建限制仅从特定 VPC 终端节点访问 DynamoDB 表的 IAM 策略。为此，您可以在 IAM 策略中使用表资源的 `aws:sourceVpce` 条件键。

有关管理对 DynamoDB 访问权限的更多信息，请参阅 Amazon DynamoDB 开发人员指南 中的 Amazon DynamoDB 的身份验证和访问控制。

Example 示例：限制从特定终端节点的访问

在此示例中，用户没有使用 DynamoDB 表的权限，除非通过终端节点 `vpce-11aa22bb` 进行访问。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AccessFromSpecificEndpoint",
         "Action": "dynamodb:*",
         "Effect": "Deny",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": { "StringNotEquals" : { "aws:sourceVpce": "vpce-11aa22bb" } }
      }
   ]
}
```

Example 示例：将此 VPC 终端节点的使用限制为账户中的特定 IAM 角色

您可以创建将 VPC 终端节点的使用限制为特定 IAM 角色的策略。以下是限制 `SomeRole` 账户中 `111122223333` 访问权限的示例。

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 示例：将此 VPC 终端节点的使用限制为特定账户中的用户

您可以创建将 VPC 终端节点的使用限制为特定账户的策略。以下是限制 `111122223333` 账户中用户访问权限的示例。

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

创建网关终端节点

要创建终端节点，您必须指定要在其中创建终端节点的 VPC 和要连接到的服务。

使用控制台创建网关终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints、Create Endpoint。
3. 对于 Service Name，请选择要连接到的服务。要创建连接到 DynamoDB 或 Amazon S3 的网关终端节点，请确保类型列指示网关。
4. 填写以下信息，然后选择 Create endpoint。

   - 对于 VPC，选择要在其中创建终端节点的 VPC。
   - 对于 Configure route tables，选择终端节点要使用的路由表。我们将自动向选定的路由表添加一个路由，以将目标设定为服务的流量指向终端节点。
   - 对于 Policy，选择策略的类型。您可以保留默认选项 Full Access 来允许对服务进行完全访问。或者，您可以选择 Custom (自定义)，然后使用 AWS 策略生成器创建自定义策略，或在策略窗口中输入您自己的策略。
   - （可选）添加或删除标签。

     [添加标签] 选择 Add tag（添加标签），然后执行以下操作：

     - 对于 Key（键），输入键名称。
     - 对于 Value（值），输入键值。

     [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

在创建终端节点之后，您可以查看有关它的信息。

使用控制台查看有关网关终端节点的信息

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 要查看有关终端节点的信息，请选择 Summary。您可以在 Service (服务) 框中获取服务的 AWS 前缀列表名称。
4. 要查看有关终端节点所使用的路由表的信息，请选择 Route Tables。
5. 要查看附加到终端节点的 IAM 策略，请选择策略。

   Note

   Policy 选项卡仅显示终端节点策略。它不会为有权使用终端节点的 IAM 用户显示有关 IAM 策略的任何信息。也不会显示服务特定的策略；例如，S3 存储桶策略。

使用 AWS CLI 创建和查看终端节点

1. 使用 describe-vpc-endpoint-services 命令获取可用服务的列表。在返回的输出中，记录要连接到的服务的名称。`serviceType` 字段指示是通过接口终端节点还是网关终端节点连接到服务。

```
aws ec2 describe-vpc-endpoint-services
```

```
{
    "serviceDetailSet": [
        {
            "serviceType": [
                {
                    "serviceType": "Gateway"
                }
            ...
```

2. 要创建网关终端节点（例如，连接到 Amazon S3 的网关终端节点），请使用 create-vpc-endpoint 命令并指定 VPC ID、服务名称和将使用终端节点的路由表。(可选) 您可以使用 `--policy-document` 参数指定自定义策略来控制对服务的访问。如果未使用参数，我们将连接一个允许完全访问服务的默认策略。

   对于 Amazon S3，您必须将 `--vpc-endpoint-type` 参数设置为 `Gateway`。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-east-1.s3 --route-table-ids rtb-11aa22bb --vpc-endpoint-type Gateway
```

3. 使用 describe-vpc-endpoints 命令描述您的终端节点。

```
aws ec2 describe-vpc-endpoints
```

使用AWS Tools for Windows PowerShell或 API 描述可用服务

- Get-EC2VpcEndpointService (AWS Tools for Windows PowerShell)
- DescribeVpcEndpointServices（Amazon EC2 查询 API）

使用 AWS Tools for Windows PowerShell 或 API 创建 VPC 终端节点

- New-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- CreateVpcEndpoint（Amazon EC2 查询 API）

使用 AWS Tools for Windows PowerShell 或 API 描述您的 VPC 终端节点

- Get-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- DescribeVpcEndpoints（Amazon EC2 查询 API）

修改安全组

如果与您的实例关联的 VPC 安全组限制出站流量，则您必须添加一条规则来允许目标设定为 AWS 服务的流量离开您的实例。

为网关终端节点添加出站规则

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Security Groups。
3. 选择您的 VPC 安全组，选择出站规则选项卡，然后选择编辑出站规则。
4. 从 Type 列表中选择流量类型，并输入端口范围 (如果需要)。例如，如果您使用实例从 Amazon S3 中检索对象，请从 Type (类型) 列表中选择 HTTPS。
5. 对于 Destination (目的地)，首先输入 `pl-` 以显示可用 AWS 服务的前缀列表 ID 和名称。选择 AWS 服务的前缀列表 ID，或输入此 ID。
6. 选择 Save（保存）。

使用命令行或 API 获取 AWS 服务的前缀列表名称、ID 和 IP 地址范围

- describe-prefix-lists (AWS CLI)
- Get-EC2PrefixList (AWS Tools for Windows PowerShell)
- DescribePrefixLists（Amazon EC2 查询 API）

修改网关终端节点

您可以通过更改或删除网关终端节点的策略并添加或删除终端节点所使用的路由表来修改网关终端节点。

如果要将现有 Amazon S3 网关终端节点迁移到接口终端节点，请在创建 Amazon S3 接口终端节点后删除 Amazon S3 网关终端节点。有关更多信息，请参阅 the section called “创建接口终端节点” (p. 8) 和 the section called “删除 VPC 终端节点” (p. 34)。

更改与网关终端节点关联的策略

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择 Actions、Edit policy。
4. 您可以选择 Full Access 来允许完全访问。或者，选择 Custom (自定义)，然后使用 AWS 策略生成器创建自定义策略，或在策略窗口中输入您自己的策略。完成此操作后，选择 Save。

   Note

   策略更改可能需要几分钟才能生效。

添加或删除网关终端节点所使用的路由表

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择操作和管理路由表。
4. 选择或取消选择所需的路由表，然后选择 Modify Route Tables (修改路由表)。

使用 AWS CLI 修改网关终端节点

1. 使用 describe-vpc-endpoints 命令获取您的网关终端节点的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 以下示例使用 modify-vpc-endpoint 命令将路由表 `rtb-aaa222bb` 与网关终端节点关联，然后重置策略文档。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

使用 AWS Tools for Windows PowerShell 或 API 修改 VPC 终端节点

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (Amazon EC2 查询 API)

添加或删除网关终端节点标签

标签提供一种标识网关终端节点的方法。您可以添加或删除标签。

添加或删除网关终端节点标签

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点。

3. 选择网关终端节点，然后选择操作、添加/编辑标签。
4. 添加或删除标签。

   [添加标签] 选择 Create tag（创建标签），然后执行以下操作：
   - 对于 Key（键），输入键名称。
   - 对于 Value（值），输入键值。

   [删除标签] 选择标签的键和值右侧的删除按钮 (“x”)。

使用 AWS Tools for Windows PowerShell 或 API 添加或删除标签

- create-tags（AWS CLI）
- CreateTags (AWS Tools for Windows PowerShell)
- delete-tags (AWS CLI)
- DeleteTags (AWS Tools for Windows PowerShell)

使用 VPC 终端节点控制对服务的访问权限

在创建接口或网关终端节点时，您可为其附加终端节点策略来控制对连接到的服务的访问。终端节点策略必须采用 JSON 格式编写。并非所有服务都支持终端节点策略。

如果您使用针对 Amazon S3 的终端节点，则还可以使用 Amazon S3 存储桶策略来控制从特定终端节点或特定 VPC 对存储桶进行的访问。有关更多信息，请参阅 Amazon S3 存储桶策略 (p. 25)。

目录

使用 VPC 终端节点策略

VPC 终端节点策略是一种 IAM 资源策略，您在创建或修改终端节点时可将它附加到终端节点。如果您在创建终端节点时不连接策略，我们将为您连接一个默认策略来允许对服务进行完全访问。如果服务不支持终端节点策略，则终端节点允许对服务进行完全访问。终端节点策略不会覆盖或取代 IAM 用户策略或服务特定策略（如 S3 存储桶策略）。它是一个单独策略，用于控制从终端节点对指定服务进行的访问。

您不能将多个策略附加到一个终端节点。但是，您可以随时修改策略。如果您修改策略，则所做的更改可能需要几分钟才能生效。有关编写策略的更多信息，请参阅 IAM 用户指南 中的 IAM 策略概述。

您的终端节点策略可与任何 IAM 策略类似；但请注意以下几点：

- 您的策略必须包含一个 Principal 元素。有关网关终端节点的其他信息，请参阅 网关终端节点的终端节点策略 (p. 33)。
- 终端节点策略的大小不得超过 20480 个字符（包含空格）。

有关支持终端节点策略的服务的信息，请参阅 支持 AWS PrivateLink 的服务 (p. 61)。

网关终端节点的终端节点策略

对于应用于网关终端节点的终端节点策略，如果您以格式 `Principal` 或 `"AWS":"account-ID"` 指定 `"AWS":"arn:aws:iam::account-ID:root"`，则只会向账户根用户授予访问权限，而不是该账户的所有 IAM 用户和角色。

如果您为 `Principal` 元素指定 Amazon Resource Name (ARN)，则保存策略时 ARN 将转换为唯一的委托人 ID。

有关 Amazon S3 和 DynamoDB 的终端节点策略示例，请参阅以下主题：

- Amazon S3 终端节点策略 (p. 23)
- DynamoDB 终端节点策略 (p. 28)

安全组

创建接口终端节点时，您可以将安全组与在您的 VPC 中创建的终端节点网络接口关联。如果您未指定安全组，则您的 VPC 的默认安全组将自动与终端节点网络接口关联。您必须确保安全组的规则允许终端节点网络接口与您的 VPC 中与服务通信的资源进行通信。

对于网关终端节点，如果您的安全组的出站规则受到限制，则必须添加一条规则来允许从 VPC 到终端节点中指定的服务的出站流量。为此，您可以在出站规则中使用该服务的 AWS 前缀列表 ID 作为目的地。有关更多信息，请参阅 修改安全组 (p. 31)。

安全组不适用于网关负载均衡器终端节点。

删除 VPC 终端节点

如果您不再需要某一终端节点，则可将其删除。删除网关终端节点也会删除终端节点所使用的路由表中的终端节点路由，但不会影响与终端节点所在的 VPC 关联的任何安全组。删除接口终端节点或网关负载均衡器终端节点也会删除终端节点网络接口。

如果路由表中存在指向终端节点的路由，则无法删除网关负载均衡器终端节点。

删除终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints 并选择您的终端节点。
3. 选择 Actions、Delete Endpoint。
4. 在确认屏幕中，选择 Yes, Delete。

删除 VPC 终端节点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- DeleteVpcEndpoints (Amazon EC2 查询 API)

VPC 终端节点服务（AWS PrivateLink）

您可以在 VPC 中创建自己的应用程序并将其配置由 AWS PrivateLink 提供支持的服务（也称作端点服务）。其他 AWS 委托人可以使用接口 VPC 终端节点 (p. 3)或 Gateway Load Balancer 端点 (p. 15)（具体取决于服务类型），在他们的 VPC 和您的端点服务之间创建连接。您是服务提供商，而创建与您的服务之间的连接的 AWS 委托人是服务使用者。

目录

接口终端节点的 VPC 终端节点服务

以下是为接口终端节点创建终端节点服务的一般步骤。

1. 在您的 VPC 中为应用程序创建一个 Network Load Balancer，并针对提供服务的每个子网（可用区）对它进行配置。负载均衡器接收来自服务使用者的请求并将请求路由到您的服务。或者，您可以将 Application Load Balancer 配置为 Network Load Balancer 的目标，然后 Application Load Balancer 可以将请求路由到您的服务。有关更多信息，请参阅 Network Load Balancer 用户指南。

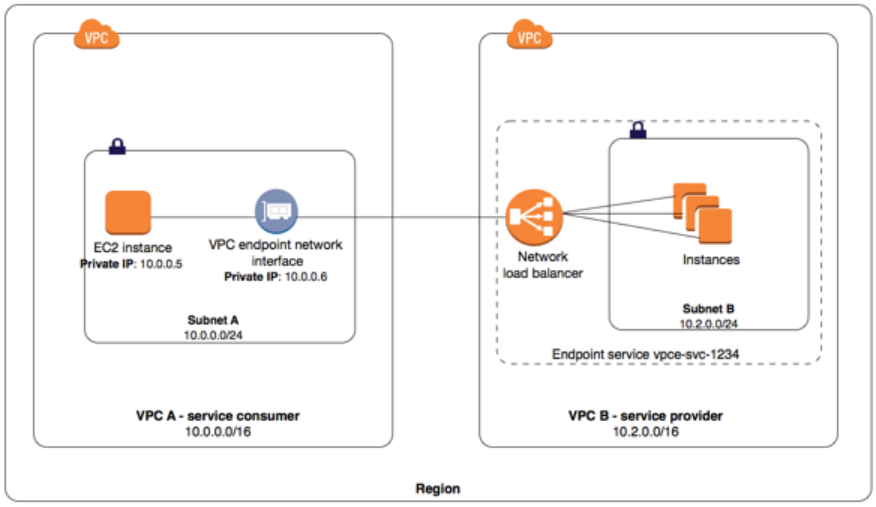
   我们建议您在区域内的所有可用区中配置您的服务。
2. 创建 VPC 终端节点服务配置并指定 Network Load Balancer。

以下是一些常规步骤，通过这些步骤，服务使用者能够连接到您的服务。

1. 向特定服务使用者（AWS 账户、IAM 用户和 IAM 角色）授予权限，允许他们创建与您的端点服务之间的连接。
2. 已被授予权限的服务使用者可创建与您的服务连接的接口终端节点（可选择在您已配置服务的每个可用区中创建）。
3. 要激活连接，请接受接口终端节点连接请求。默认情况下，必须手动接受连接请求。不过，您可以配置终端节点服务的接受设置，以便自动接受所有连接请求。

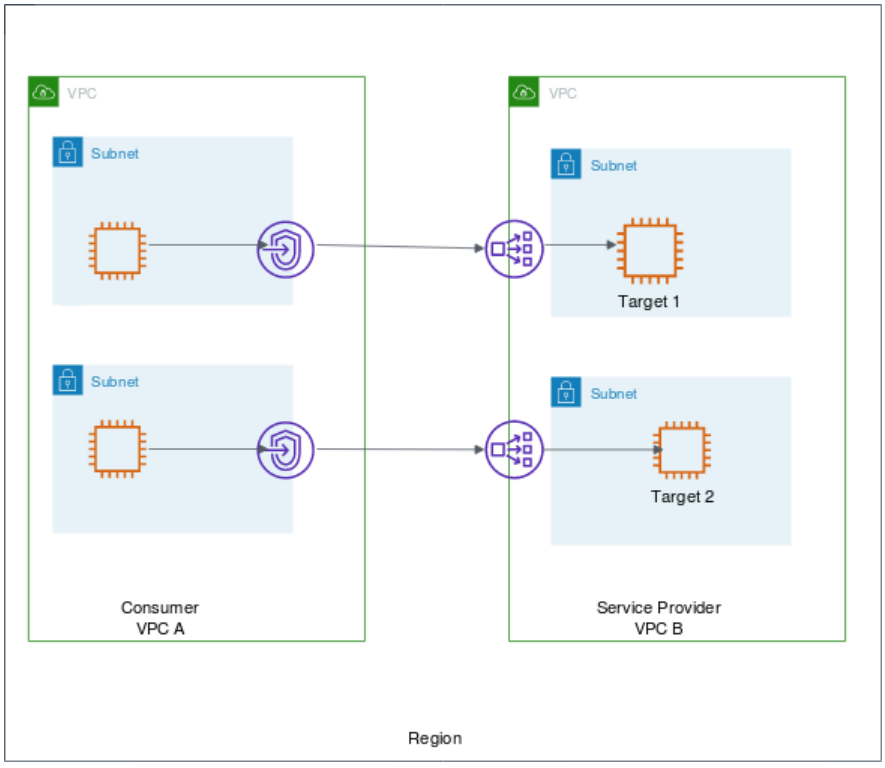
权限和接受设置的组合可帮助您控制哪些服务使用者（AWS 委托人）可以访问您的服务。例如，可以为您信任的选定委托人授予权限，并自动接受所有连接请求；您还可以为范围更广的委托人组授予权限，并手动接受您信任的特定连接请求。

在下图中，VPC B 的账户拥有者是一个服务提供商并且有一项服务正在子网 B 的实例上运行。VPC B 的拥有者具有一个服务终端节点 (vpce-svc-1234)，该节点已关联指向子网 B 中作为目标的实例的 Network Load Balancer。VPC A 的子网 A 中的实例使用接口终端节点访问子网 B 中的服务。



为实现低延迟和容错能力，建议使用网络负载均衡器，其目标位于 AWS 区域的每个可用区中。要帮助使用区域 DNS 主机名 (p. 12)访问服务的服务使用者实现高可用性，您可以启用跨区域负载均衡。借助跨区域负载均衡，负载均衡器将在所有启用可用区中的已注册目标之间分配流量。有关更多信息，请参阅 Network Load Balancer 用户指南 中的跨区域负载均衡。启用跨区域负载均衡后，可能向账户收取区域数据传输费用。

在下图中，VPC B 的拥有者是服务提供商并且已配置目标位于两个不同可用区中的 Network Load Balancer。服务使用者 (VPC A) 已在其 VPC 中相同的两个可用区中创建了接口终端节点。来自 VPC A 中实例对服务的请求可使用任一接口终端节点。



有关配置服务和支持服务使用者通过 VPC 对等连接访问服务的示例，请参阅 Amazon VPC 用户指南中的示例：使用 AWS PrivateLink 和 VPC 对等连接的服务。

终端节点服务可用区注意事项

创建终端节点服务时，将在映射至您的账户且独立于其他账户的可用区中创建此服务。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别终端节点可用区。例如，`use1-az1` 是 `us-east-1` 区域的 AZ ID，映射至每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南中的您的资源的 AZ ID 或使用 describe-availability-zones。

当服务提供商和使用者具有不同的账户并使用多个可用区，并且使用者查看 VPC 终端节点服务信息时，响应仅包括公共可用区。例如，当服务提供商账户使用 `us-east-1a` 和 `us-east-1c` 而使用者使用 `us-east-1a` 和 `us-east-1b` 时，响应包括公共可用区 `us-east-1a` 中的 VPC 终端节点服务。

终端节点服务 DNS 名称

当您创建 VPC 终端节点服务时，AWS 将生成您可用于与服务通信的端点特定的 DNS 主机名。这些名称包括 VPC 终端节点 ID、可用区名称和区域名称。例如，vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com。默认情况下，您的使用者使用该 DNS 名称访问服务，通常需要修改应用程序配置。

如果端点服务适用于 AWS 服务或 AWS Marketplace 中可用的服务，则存在默认 DNS 名称。对于其他服务，服务提供商可以配置私有 DNS 名称，以便使用者可以使用现有 DNS 名称访问服务，而无需更改其应用程序。有关更多信息，请参阅 私有 DNS 名称 (p. 53)。

服务提供商可以在 IAM 策略语句中使用 ec2:VpceServicePrivateDnsName 条件上下文密钥来控制可以创建哪些私有 DNS 名称。有关更多信息，请参阅 IAM 用户指南中的 Amazon EC2 定义的操作。

私有 DNS 名称要求

服务提供商可以为新的终端节点服务或现有终端节点服务指定私有 DNS 名称。要使用私有 DNS 名称，请启用该功能，然后指定私有 DNS 名称。在使用者可以使用私有 DNS 名称之前，您必须验证您是否拥有对域/子域的控制权。您可以使用 Amazon VPC 控制台或 API 启动域所有权验证。域所有权验证完成后，使用者通过使用私有 DNS 名称访问终端节点。

连接到本地数据中心

您可以使用以下类型的连接进行接口终端节点与本地数据中心之间的连接：

- AWS Direct Connect
- AWS Site-to-Site VPN

通过 VPC 对等连接访问服务

您可以将 VPC 对等连接与 VPC 终端节点结合使用，以允许跨 VPC 对等连接对使用者进行私有访问。有关更多信息，请参阅 Amazon VPC 用户指南中的示例：使用 AWS PrivateLink 和 VPC 对等连接的服务。

对连接信息使用代理协议

Network Load Balancer 向您的应用程序（您的服务）提供源 IP 地址。当服务使用者通过接口终端节点将流量发送至您的服务时，向您的应用程序提供的源 IP 地址是 Network Load Balancer 节点的私有 IP 地址而不是服务使用者的 IP 地址。

如果您需要服务使用者的 IP 地址及其对应的接口终端节点 ID，请在您的负载均衡器上启用代理协议并从代理协议标头中获取客户端 IP 地址。有关更多信息，请参阅 Network Load Balancer 用户指南 中的代理协议。

规则和限制

要使用终端节点服务，您需要了解当前规则和限制：

- 终端节点服务仅支持通过 TCP 的 IPv4 流量。
- 服务使用者可以使用特定于终端节点的 DNS 主机名访问终端节点服务或私有 DNS 名称。
- 如果终端节点服务与多个 Network Load Balancer 关联，那么对于某个特定的可用区，一个接口终端节点将仅建立一个与负载均衡器的连接。
- 对于终端节点服务，关联的网络负载均衡器可以支持针对每个唯一目标（IP 地址和端口）的 55000 个并发连接或每分钟约 55000 个连接。如果连接数超过该值，则会增大出现端口分配错误的几率。要修复端口分配错误，请将更多目标添加到目标组。有关 Network Load Balancer 目标组的信息，请参阅 Network Load Balancer 用户指南中的 Network Load Balancer 的目标组和向您的目标组注册目标。
- 您账户中的可用区可能不会映射到与其他账户中的可用区相同的位置。例如，您的可用区 `us-east-1a` 与其他账户的可用区 `us-east-1a` 可能不是同一个位置。有关更多信息，请参阅区域和可用区。配置终端节点服务时，将在映射到您的账户的可用区中配置此服务。
- 终端节点服务仅在您创建终端节点服务的区域可用。
- 查看终端节点服务的服务特定的限制。
- 查看终端节点服务的安全最佳实践和示例。有关更多信息，请参阅策略最佳实践和 the section called “控制对服务的访问权限” (p. 33)。

网关负载均衡器端点的 VPC 终端节点服务

您可以使用网关负载均衡器将流量分配到网络虚拟设备队列。这些设备可用于安全检查、合规性、策略控制和其他网络服务。然后，您可以将 Gateway Load Balancer 配置为 VPC 终端节点服务，以便其他 AWS 委托人能够通过 Gateway Load Balancer 端点访问该服务。

以下是为网关负载均衡器终端节点创建终端节点服务的一般步骤。

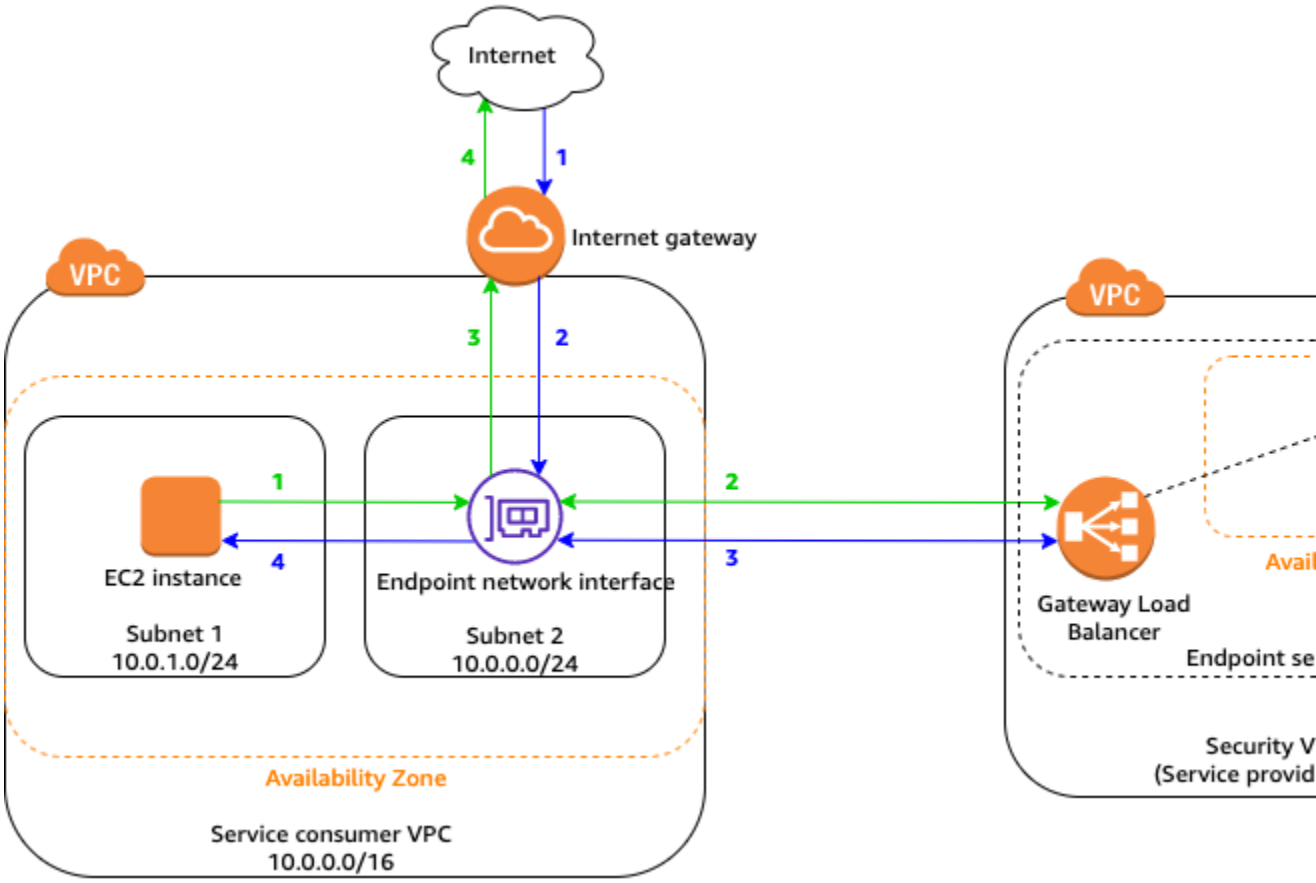
1. 为虚拟设备创建网关负载均衡器。有关更多信息，请参阅 Gateway Load Balancer 入门。

   我们建议您在区域内的所有可用区中配置您的服务。
2. 创建 VPC 终端节点服务配置并指定网关负载均衡器。

以下是一些常规步骤，通过这些步骤，服务使用者能够连接到您的服务。

1. 向特定服务使用者（AWS 账户、IAM 用户和 IAM 角色）授予权限，允许他们创建与您的端点服务之间的连接。
2. 已获得权限的服务使用者会向您的服务创建 Gateway Load Balancer 端点 (p. 15)。
3. 要激活连接，请接受终端节点连接请求。默认情况下，必须手动接受连接请求。不过，您可以配置终端节点服务的接受设置，以便自动接受所有连接请求。

在以下示例中，安全设备队列配置在安全 VPC 中的网关负载均衡器之后。已为网关负载均衡器配置终端节点服务。服务使用者 VPC 的拥有者在其 VPC 的子网 2 中创建一个网关负载均衡器终端节点（通过终端节点网络接口表示）。通过互联网网关进入 VPC 的所有流量首先会路由到网关负载均衡器终端节点，以便在安全 VPC 中进行检查，然后再路由到目标子网。同样，离开子网 1 中的 EC2 实例的所有流量首先会路由到网关负载均衡器终端节点，以便在安全 VPC 中进行检查，然后再路由到互联网。



有关此方案的路由配置的更多信息，请参阅 Amazon VPC 用户指南 中的路由到 Gateway Load Balancer 端点。

可用区注意事项

创建终端节点服务时，将在映射至您的账户且独立于其他账户的可用区中创建此服务。当服务提供商与使用者处于不同的账户中时，请使用可用区 ID 唯一且一致地识别终端节点可用区。例如，`use1-az1` 是 `us-east-1` 区域的 AZ ID，映射至每个 AWS 账户中的相同位置。有关可用区 ID 的信息，请参阅 AWS RAM 用户指南中的您的资源的 AZ ID 或使用 describe-availability-zones。

当服务提供商和使用者具有不同的账户并使用多个可用区，并且使用者查看 VPC 终端节点服务信息时，响应仅包括公共可用区。例如，当服务提供商账户使用 `us-east-1a` 和 `us-east-1c` 而使用者使用 `us-east-1a` 和 `us-east-1b` 时，响应包括公共可用区 `us-east-1a` 中的 VPC 终端节点服务。

规则和限制

要将终端节点服务用于网关负载均衡器终端节点，请注意当前的规则和限制：

- 如果终端节点服务与多个网关负载均衡器关联，那么对于某个特定的可用区，一个网关负载均衡器终端节点将仅建立一个与负载均衡器的连接。
- 不支持私有 DNS 名称。
- 您账户中的可用区可能不会映射到与其他账户中的可用区相同的位置。例如，您的可用区 `us-east-1a` 与其他账户的可用区 `us-east-1a` 可能不是同一个位置。有关更多信息，请参阅区域和可用区。配置终端节点服务时，将在映射到您的账户的可用区中配置此服务。

为接口终端节点创建 VPC 终端节点服务配置

您可使用 Amazon VPC 控制台或命令行创建终端节点服务配置。有关 VPC 终端节点限制的更多信息，请参阅 Amazon VPC 用户指南中的限制。

在开始前，请确保您已在 VPC 中为您的服务创建一个或多个 Network Load Balancer。有关更多信息，请参阅 Network Load Balancer 用户指南中的 Network Load Balancer 入门。

您可以在配置中选择指定，必须由您手动接受所有希望与您的服务连接的接口终端节点连接请求。您可以创建通知 (p. 46)，在有连接请求时接收提示。如果您不接受连接，服务使用者将无法访问您的服务。

Note

无论接受设置如何，服务使用者还必须具有与您的服务建立连接的权限 (p. 42)。

在创建终端节点服务配置后，您必须添加权限以使服务使用者能够创建到您服务的接口终端节点。

Console

创建端点服务

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）、Create endpoint service（创建端点服务）。
3. 对于 Load balancer type（负载均衡器类型），请选择 Network（网络）。
4. 对于 Available load balancers（可用负载均衡器），选择要与端点服务关联的 Network Load Balancer。
5. 对于 Require acceptance for endpoint（需要接受以使用端点），选中此复选框以手动接受针对您的服务的连接请求。否则，会自动接受端点连接。
6. 对于 Enable private DNS name（启用私有 DNS 名称），选中此复选框以将私有 DNS 名称与服务关联，然后输入私有 DNS 名称。
7. （可选）要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
8. 选择 Create（创建）。

AWS CLI

创建端点服务

使用 create-vpc-endpoint-service-configuration 命令并为您的 Network Load Balancer 指定一个或多个 ARN。您可以选择指定是否需要接受针对您的服务的连接以及服务是否具有私有 DNS 名称。

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532 --acceptance-required --privateDnsName exampleservice.com
```

下面是示例输出。

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "NetworkLoadBalancerArns": [
```

```
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532"
        ],
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
        "ServiceState": "Available",
        "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
        "PrivateDnsName": "exampleService.com",
        "AcceptanceRequired": true,
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "BaseEndpointDnsNames": [
            "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
        ]
    }
}
```

Tools for Windows PowerShell

创建端点服务

使用 New-EC2VpcEndpointServiceConfiguration。

API

创建端点服务

使用 CreateVpcEndpointServiceConfiguration。

为网关负载均衡器终端节点创建 VPC 终端节点服务配置

您可使用 Amazon VPC 控制台或命令行创建终端节点服务配置。在开始前，请确保您已在 VPC 中为您的服务创建一个或多个网关负载均衡器。有关更多信息，请参阅 Gateway Load Balancer 入门。

您可以在配置中选择指定，必须由您手动接受所有希望与您的服务连接的网关负载均衡器终端节点连接请求。您可以创建通知 (p. 46)，在有连接请求时接收提示。如果您不接受连接，服务使用者将无法访问您的服务。

在创建端点服务配置后，您必须添加权限 (p. 42)以使服务使用者能够创建到您服务的 Gateway Load Balancer 端点。

Console

创建端点服务

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）、Create endpoint service（创建端点服务）。
3. 对于 Load balancer type（负载均衡器类型），请选择 Gateway（网关）。
4. 对于 Available load balancers（可用负载均衡器），选择要与端点服务关联的 Gateway Load Balancer。
5. 对于 Require acceptance for endpoint（需要接受以使用端点），选中此复选框以手动接受针对您的服务的连接请求。否则，会自动接受端点连接。
6. （可选）要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
7. 选择 Create（创建）。

AWS CLI

创建端点服务

使用 create-vpc-endpoint-service-configuration 命令并为您的网关负载均衡器指定一个或多个 ARN。您可以选择指定是否需要接受针对您的服务的连接。

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-arns gateway-load-balancer-arn --no-acceptance-required
```

Tools for Windows PowerShell

创建端点服务

使用 New-EC2VpcEndpointServiceConfiguration。

API

创建端点服务

使用 CreateVpcEndpointServiceConfiguration。

为您的终端节点服务添加和删除权限

在创建终端节点服务配置后，您可以控制哪些服务使用者能够创建连接您服务的接口终端节点或网关负载均衡器终端节点。服务使用者是 IAM 委托人 – IAM 用户、IAM 角色和AWS账户。要为委托人添加或删除权限，您需要其 Amazon Resource Name (ARN)。

- 对于 AWS 账户（以及该账户中的所有委托人），ARN 的格式为 `arn:aws:iam::aws-account-id:root`。
- 对于特定的 IAM 用户，ARN 的格式为 `arn:aws:iam::aws-account-id:user/user-name`。
- 对于特定的 IAM 角色，ARN 的格式为 `arn:aws:iam::aws-account-id:role/role-name`。

> **Note**
>
> 如果您将权限设置为“任何人都可以访问”，并将接受模型设置为“接受所有请求”，则您刚已将负载均衡器公开。由于获取 AWS 账户很容易，因此，即使您的负载均衡器没有公有 IP 地址，对于谁可以访问该账户也没有实际限制。

Console

为您的端点服务添加和删除权限

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择端点服务然后选择 Actions（操作）、Allow principals（允许委托人）。
4. 指定要为其添加权限的委托人的 ARN。要添加另一个委托人，请选择 Add principal（添加委托人）。要删除委托人，请选择相应条目旁边的 Remove（删除）。

   指定 * 可为所有委托人添加权限。这支持所有 AWS 账户中的所有委托人创建指向您的端点服务的端点。
5. 选择 Allow principals（允许委托人）。

AWS CLI

为您的端点服务添加权限

使用 modify-vpc-endpoint-service-permissions 命令。指定 `--add-allowed-principals` 参数，为委托人添加一个或多个 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

查看为端点服务添加的权限

使用 describe-vpc-endpoint-service-permissions 命令。

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3
```

下面是示例输出。

```
{
    "AllowedPrincipals": [
        {
            "PrincipalType": "Account",
            "Principal": "arn:aws:iam::123456789012:root"
        }
    ]
}
```

为您的端点服务删除权限

使用 modify-vpc-endpoint-service-permissions 命令。指定 `--remove-allowed-principals` 参数，为委托人删除一个或多个 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --remove-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Tools for Windows PowerShell

为您的端点服务添加和删除权限

使用 Edit-EC2EndpointServicePermission。

API

为您的端点服务添加和删除权限

使用 ModifyVpcEndpointServicePermissions。

更改端点服务配置

您可以通过更改与终端节点服务关联的负载均衡器以及更改是否需要接受连接到您的终端节点服务的请求来修改终端节点服务配置。

如果已有终端节点连接到您的终端节点服务，则您无法取消关联负载均衡器。

Console

更改端点服务的负载均衡器

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。

3. 选择端点服务然后选择 Actions（操作）、Associate or disassociate load balancers（关联或取消关联负载均衡器）。
4. 根据需要选择或取消选择负载均衡器，然后选择 Save changes（保存更改）。

修改接受设置

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择端点服务然后选择 Actions（操作）、Modify endpoint acceptance setting（修改端点接受设置）。
4. 选择或取消选中 Acceptance required（需要接受），然后选择 Save changes（保存更改）。

AWS CLI

更改端点服务的负载均衡器

使用 modify-vpc-endpoint-service-configuration 命令。以下示例使用 `--remove-network-load-balancer-arn` 参数删除 Network Load Balancer。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-
id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532
```

更改是否需要接受

使用 modify-vpc-endpoint-service-configuration 命令并指定 `--acceptance-required` 或 `--no-acceptance-required`。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-
svc-09222513e6e77dc86 --no-acceptance-required
```

Tools for Windows PowerShell

更改端点服务配置

使用 Edit-EC2VpcEndpointServiceConfiguration。

API

更改端点服务配置

使用 ModifyVpcEndpointServiceConfiguration。

接受并拒绝终端节点连接请求

在您创建终端节点服务后，已添加权限的服务使用者能够创建连接您服务的接口终端节点或网关负载均衡器终端节点。有关更多信息，请参阅 接口 VPC 终端节点（AWS PrivateLink）(p. 3) 和 网关负载均衡器终端节点（AWS PrivateLink）(p. 15)。

如果您已指定需要接受连接请求，则必须手动接受或拒绝对您的终端节点服务的终端节点连接请求。在接受端点后，它将变为 `available` 状态。请注意，可能需要花费一些时间才能使验证状态完成更改以及使状态变为 `available`。

您可以在端点连接处于 `available` 状态之后拒绝该连接。

Console

接受或拒绝连接请求

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择端点服务。
4. 从 Endpoint connections（端点连接）选项卡上，选择终端节点。要接受连接请求，请选择 Actions（操作）、Accept endpoint connection request（接受端点连接请求）。要拒绝连接请求，请选择 Actions（操作）、Reject endpoint connection request（拒绝端点连接请求）。

AWS CLI

查看待接受的端点连接

使用 describe-vpc-endpoint-connections 命令并依据 `pendingAcceptance` 状态进行筛选。

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-
state,Values=pendingAcceptance
```

下面是示例输出。

```
{
    "VpcEndpointConnections": [
        {
            "VpcEndpointId": "vpce-0c1308d7312217abc",
            "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
            "CreationTimestamp": "2017-11-30T10:00:24.350Z",
            "VpcEndpointState": "pendingAcceptance",
            "VpcEndpointOwner": "123456789012"
        }
    ]
}
```

接受端点连接请求

使用 accept-vpc-endpoint-connections 命令并指定端点 ID 和端点服务 ID。

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-
endpoint-ids vpce-0c1308d7312217abc
```

拒绝端点连接请求

使用 reject-vpc-endpoint-connections 命令。

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-
endpoint-ids vpce-0c1308d7312217abc
```

Tools for Windows PowerShell

接受或拒绝连接请求

使用 Confirm-EC2EndpointConnection 和 Deny-EC2EndpointConnection。

API

接受或拒绝连接请求

使用 AcceptVpcEndpointConnections 和 RejectVpcEndpointConnections。

为终端节点服务创建和管理通知

您可以创建通知以针对在连接到您的终端节点服务的终端节点上发生的特定事件接收提醒。例如，您可以在接受或拒绝针对您的终端节点服务的终端节点请求时收到电子邮件。要创建通知，您必须将 Amazon SNS 主题与通知关联。您可以订阅 SNS 主题以在终端节点事件发生时收到电子邮件通知。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

用于通知的 Amazon SNS 主题必须具有允许 Amazon VPC 终端节点服务代表您发布通知的主题策略。确保在您的主题策略中包含以下语句。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的管理对 Amazon SNS 主题的访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Console

为终端节点服务创建通知

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择端点服务然后选择 Notifications（通知）选项卡。
4. 选择 Create notification（创建通知）。
5. 对于 Notification ARN（通知 ARN），选择要与通知关联的 SNS 主题的 ARN。
6. 对于 Events（事件），选择要接收其通知的端点事件。
7. 选择 Create notification（创建通知）。

创建通知后，您可以修改其设置。

为终端节点服务修改通知

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择端点服务然后选择 Notifications（通知）选项卡。
4. 选择通知，然后依次选择 Actions（操作）、Modify notification（修改通知）。
5. 根据要求更改 SNS 主题和端点事件。
6. 选择保存更改。

如果您不再需要某通知，则可删除它。

删除通知

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。

2. 在导航窗格中，选择终端节点服务。
3. 选择端点服务然后选择 Notifications（通知）选项卡。
4. 选择通知，然后依次选择 Actions（操作）、Delete notification（删除通知）。
5. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

AWS CLI

为终端节点服务创建通知

使用 create-vpc-endpoint-connection-notification 命令。指定 SNS 主题的 ARN、要通知的事件以及端点服务的 ID。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect
 Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

下面是示例输出。

```
{
    "ConnectionNotification": {
        "ConnectionNotificationState": "Enabled",
        "ConnectionNotificationType": "Topic",
        "ServiceId": "vpce-svc-1237881c0d25a3abc",
        "ConnectionEvents": [
            "Reject",
            "Accept",
            "Delete",
            "Connect"
        ],
        "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
        "ConnectionNotificationArn": "arn:aws:sns:us-
east-2:123456789012:VpceNotification"
    }
}
```

查看通知

使用 describe-vpc-endpoint-connection-notifications 命令。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

更改通知的 SNS 主题或端点事件

使用 modify-vpc-endpoint-connection-notification 命令。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-
nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

删除通知

使用 delete-vpc-endpoint-connection-notifications 命令。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

Tools for Windows PowerShell

创建和管理通知

使用以下命令：

- New-EC2VpcEndpointConnectionNotification
- Get-EC2EndpointConnectionNotification
- Edit-EC2VpcEndpointConnectionNotification
- Remove-EC2EndpointConnectionNotification

API

创建和管理通知

使用以下命令：

- CreateVpcEndpointConnectionNotification
- DescribeVpcEndpointConnectionNotifications
- ModifyVpcEndpointConnectionNotification
- DeleteVpcEndpointConnectionNotifications

添加或删除 VPC 终端节点服务标签

标签提供一种标识 VPC 终端节点服务的方法。您可以添加或删除标签。

Console

添加或删除 VPC 终端节点服务标签

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services（端点服务）。
3. 选择 VPC 终端节点服务，然后选择 Actions（操作）、Manage tags（管理标签）。
4. 添加或删除标签。

   [添加标签] 选择 Add new tag（添加新标签），然后输入标签键和标签值。

   [删除标签] 选择标签键和值右侧的 Remove（删除）。

AWS CLI

使用 create-tags 和 delete-tags。

API

使用 CreateTags 和 DeleteTags。

删除终端节点服务配置

您可以删除终端节点服务配置。删除该配置不会删除在您的 VPC 中托管的应用程序或关联的负载均衡器。

在删除端点服务配置之前，您必须拒绝已附加到该服务的任何 `available` 或 `pending-acceptance` VPC 终端节点。有关更多信息，请参阅 接受并拒绝终端节点连接请求 (p. 44)。

Console

删除端点服务配置

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点服务。
3. 选择终端节点服务。
4. 选择 Actions（操作）、Delete endpoint services（删除端点服务）。
5. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

AWS CLI

删除端点服务配置

使用 delete-vpc-endpoint-service-configurations 命令。指定服务 ID。

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-
svc-03d5ebb7d9579a2b3
```

Tools for Windows PowerShell

删除端点服务配置

使用 Remove-EC2EndpointServiceConfiguration。

API

删除端点服务配置

使用 DeleteVpcEndpointServiceConfigurations。

VPC 终端节点和 VPC 终端节点服务的身份和访问管理

使用 IAM 管理对 VPC 终端节点和 VPC 终端节点服务的访问。

控制 VPC 终端节点的使用

默认情况下，IAM 用户无权使用终端节点。您可以创建一个 IAM 用户策略，向用户授予创建、修改、描述和删除终端节点的权限。以下是示例。

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

有关使用 VPC 终端节点控制对服务的访问的信息，请参阅the section called “控制对服务的访问权限” (p. 33)。

基于服务拥有者控制 VPC 终端节点创建

您可以使用 `ec2:VpceServiceOwner` 条件键根据服务拥有者（`amazon`、`aws-marketplace` 或账户 ID）来控制可以创建的 VPC 终端节点。以下示例授予使用指定的服务拥有者创建 VPC 终端节点的权限。要使用此示例，请替换区域、账户 ID 和服务拥有者。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc/*",
                "arn:aws:ec2:region:accountId:security-group/*",
                "arn:aws:ec2:region:accountId:subnet/*",
                "arn:aws:ec2:region:accountId:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
```

```
        }
    ]
}
```

控制可为 VPC 终端节点服务指定的私有 DNS 名称

您可以使用 ec2:VpceServicePrivateDnsName 条件键来控制可根据与 VPC 终端节点服务关联的私有 DNS 名称修改或创建哪些 VPC 终端节点服务。以下示例授予使用指定的私有 DNS 名称创建 VPC 终端节点服务的权限。要使用此示例，请替换区域、账户 ID 和私有 DNS 名称。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

控制可为 VPC 终端节点服务指定的服务名称

您可以使用 ec2:VpceServiceName 条件键基于 VPC 终端节点服务名称来控制可以创建的 VPC 终端节点。以下示例授予使用指定的服务名称创建 VPC 终端节点的权限。要使用此示例，请替换区域、账户 ID 和服务名称。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc/*",
                "arn:aws:ec2:region:accountId:security-group/*",
                "arn:aws:ec2:region:accountId:subnet/*",
                "arn:aws:ec2:region:accountId:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.s3"
                    ]
```

```
                }
            }
        }
    ]
}
```

终端节点服务的私有 DNS 名称

当您创建 VPC 终端节点服务时，我们将生成您可用于与服务通信的终端节点特定的 DNS 主机名。这些名称包括 VPC 终端节点 ID、可用区名称以及区域名称，例如，vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com。默认情况下，您的使用者使用该 DNS 名称访问服务，通常需要修改应用程序配置。

如果终端节点服务适用于 AWS 服务或 AWS Marketplace 中可用的服务，则存在默认 DNS 名称。对于其他服务，服务提供商可以配置私有 DNS 名称，以便使用者可以使用现有 DNS 名称访问服务，而无需更改其应用程序。有关更多信息，请参阅 VPC 终端节点服务 (p. 35)。

服务提供商可以为新的终端节点服务或现有终端节点服务指定私有 DNS 名称。要使用私有 DNS 名称，请启用该功能，然后指定私有 DNS 名称。在使用者可以使用私有 DNS 名称之前，您必须验证您是否拥有对域/子域的控制权。您可以使用 Amazon VPC 控制台或 API 启动域所有权验证。域所有权验证完成后，使用者通过使用私有 DNS 名称访问终端节点。

要验证域，您必须拥有公有托管名称或公有 DNS 提供商。

为网关负载均衡器终端节点创建的终端节点服务不支持私有 DNS 名称。

概括过程如下：

1. 添加私有 DNS 名称。有关更多信息，请参阅 the section called “为接口终端节点创建 VPC 终端节点服务配置” (p. 40) 或 the section called “修改现有终端节点服务私有 DNS 名称” (p. 55)。
2. 请注意 DNS 服务器记录所需的 Domain verification value (域验证值) 和 Domain verification name (域验证名称)。有关更多信息，请参阅 the section called “查看终端节点服务私有 DNS 名称配置” (p. 56)。
3. 向 DNS 服务器添加记录。有关更多信息，请参阅 the section called “VPC 终端节点服务私有 DNS 名称验证” (p. 54)。
4. 验证私有 DNS 名称。有关更多信息，请参阅 the section called “手动启动终端节点服务私有 DNS 名称域验证” (p. 56)。

您可以使用 Amazon VPC 控制台或 Amazon VPC API 管理验证过程。

- the section called “VPC 终端节点服务私有 DNS 名称验证” (p. 54)
- the section called “修改现有终端节点服务私有 DNS 名称” (p. 55)
- the section called “删除终端节点服务私有 DNS 名称” (p. 57)
- the section called “查看终端节点服务私有 DNS 名称配置” (p. 56)
- Amazon VPC 私有 DNS 域名验证 TXT 记录 (p. 57)

域名验证注意事项

注意有关域所有权验证的以下要点：

- 仅当验证状态为 verified (已验证) 时，使用者才能使用私有 DNS 名称访问终端节点服务。
- 如果验证状态从 verified (已验证) 更改为 pendingVerification (待验证) 或 failed (失败)，则现有的使用者连接保留，但任何新的连接请求都将被拒绝。

  Important

  对于担心与不再处于已验证状态的终端节点服务的连接的服务提供商，我们建议您使用 Describevpcendpoints 以定期检查验证状态。我们建议您每天至少执行一次此检查。

- 终端节点服务只能有一个私有 DNS 名称。
- 您可以为新的终端节点服务或现有终端节点服务指定私有 DNS 名称。
- 您只能使用公有域名服务器。
- 您可以在域名中使用通配符，例如“*.myexampleservice.com”。
- 您必须对每个终端节点服务执行单独的域所有权验证检查。
- 您可以验证子域的域。例如，您可以验证 example.com，而不是 a.example.com。按照 RFC 1034 中的规定，每个 DNS 标签最多可包含 63 个字符，域名总长度不得超过 255 个字符。

  如果添加其他子域，则必须验证子域或域。例如，假设您有 .example.com 并验证了 example.com。您现在添加 b.example.com 作为私有 DNS 名称。在使用者可以使用该名称之前，您必须验证 example.com 或 b.example.com。
- 域名必须小写。

VPC 终端节点服务私有 DNS 名称验证

您的域与一组域名系统 (DNS) 记录相关联，这些记录由您的 DNS 提供商管理。TXT 记录是一种 DNS 记录，可提供有关您的域的其他信息。每个 TXT 记录均包含一个名称和一个值。

启动域所有权验证时，我们向您提供 TXT 记录所使用的名称和值。例如，如果域是 myexampleservice.com，则我们生成的 TXT 记录设置如下例所示：

终端节点私有 DNS 名称 TXT 记录

域验证名称	类型	域验证值
_vpce:aksldja21i1	TXT	vpce:asjdakjshd78126eu21

使用指定的 Domain verification name (域验证名称) 和 Domain verification value (域验证值) 向域的 DNS 服务器添加 TXT 记录。当我们检测到域的 DNS 设置中存在 TXT 记录时，即完成域所有权验证。

如果您的 DNS 提供商不允许 DNS 记录名称包含下划线，则可以从 Domain verification name (域验证名称) 中省略 _aksldja21i1 。在这种情况下，对于前面的示例，TXT 记录名称将是 myexampleservice.com，而不是 _aksldja21i1.myexampleservice.com。

将 TXT 记录添加到您的域的 DNS 服务器

将 TXT 记录添加到您的域的 DNS 服务器的过程取决于为您提供 DNS 服务的组织。您的 DNS 提供商可能是 Amazon Route 53 或其他域名注册商。此部分介绍将 TXT 记录添加到 Route 53 的过程，以及适用于其他 DNS 提供商的通用过程。

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 选择 Endpoint Services (终端节点服务)。
3. 选择终端节点服务。
4. 在 Details (详细信息) 选项卡上，记下 Domain verification value (域验证值) 和 Domain verification name (域验证名称) 旁边显示的值。
5. 如果 Route 53 为您要验证的域提供 DNS 服务，而且您已使用用于 Route 53 的相同账户登录 AWS Management Console，我们会提供相应选项，允许您从 Amazon VPC 控制台立即更新 DNS 服务器。

   如果您使用其他 DNS 提供商，则更新 DNS 记录的过程因您使用的 DNS 或 Web 托管提供商而异。下表列出了指向几个常用提供商的文档的链接。此列表并不详尽，并且其中包含的内容不是对任何公司的产品或服务的认可或推荐。如果表中未列出您的提供商，则也许可以将域用于终端节点。

DNS/托管提供商	文档链接
GoDaddy	添加 TXT 记录（外部链接）
Dreamhost	如何添加自定义 DNS 记录？（外部链接）
Cloudflare	在 CloudFlare 中管理 DNS 记录（外部链接）
HostGator	通过 HostGator/eNom 管理 DNS 记录（外部链接）
Namecheap	如何为我的域添加 TXT/SPF/DKIM/DMARC 记录？（外部链接）
Names.co.uk	更改您的域的 DNS 设置（外部链接）
Wix	在您的 Wix 账户中添加或更新 TXT 记录（外部链接）

当验证完成后，Amazon VPC 控制台中域的状态会从待验证更改为已验证。

6. 您现在可以将私有域名用于 VPC 终端节点服务。

如果 DNS 设置未正确更新，域状态在 Details (详细信息) 选项卡上显示 failed (失败) 状态。如果发生这种情况，请完成位于the section called “排查常见的域验证问题” (p. 59)的故障排除页面上的步骤。在验证是否已正确创建您的 TXT 记录后，请重试该操作。

修改现有终端节点服务私有 DNS 名称

您可以为新的或现有的终端节点服务修改终端节点服务私有 DNS 名称。

更新名称后，更新 DNS 服务器上域的条目。我们会自动轮询 DNS 服务器以验证该记录是否存在于服务器上。DNS 记录更新最长需要 48 小时生效，通常情况下生效时间要早很多。有关更多信息，请参阅 the section called “私有 DNS 域名验证 TXT 记录” (p. 57) 和 the section called “VPC 终端节点服务私有 DNS 名称验证” (p. 54)。

Console

修改端点服务私有 DNS 名称

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点服务。
3. 选择终端节点服务，然后依次选择 Actions (操作) 和 Modify private DNS name (修改私有 DNS 名称)。
4. 选择 Associate a private DNS name with the serivce（将私有 DNS 名称与服务关联），然后输入私有 DNS 名称。
5. 选择保存更改。

AWS CLI

修改端点服务私有 DNS 名称

使用 modify-vpc-endpoint-service-configuration。

API

修改端点服务私有 DNS 名称

使用 ModifyVpcEndpointServiceConfiguration。

查看终端节点服务私有 DNS 名称配置

您可以查看终端节点服务的终端节点服务私有 DNS 名称。

Console

查看端点服务私有 DNS 名称配置

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint Services (终端节点服务)，然后选择终端节点服务。
3. Details (详细信息) 选项卡显示私有 DNS 域所有权检查的以下信息：
   - Domain verification status (域验证状态)：验证状态。
   - Domain verification type (域验证类型)：验证类型。
   - Domain verification value (域验证值)：DNS 值。
   - Domain verification name (域验证名称)：记录子域的名称。

AWS CLI

查看端点服务私有 DNS 名称配置

使用 describe-vpc-endpoint-service-configurations。

API

查看端点服务私有 DNS 名称配置

使用 DescribeVpcEndpointServiceConfigurations。

手动启动终端节点服务私有 DNS 名称域验证

服务提供商必须证明他们拥有私有 DNS 名称域，然后使用者才能使用私有 DNS 名称。

Console

启动私有 DNS 名称域的验证过程

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点服务。
3. 选择端点服务，然后依次选择 Actions（操作）、Verify domain owernship for Private DNS Name（验证私有 DNS 名称的域所有权）。
4. 提示进行确认时，输入 **`verify`**，然后选择 Verify（验证）。

   如果 DNS 设置未正确更新，域验证状态为 failed（失败）。如果发生这种情况，请完成位于the section called “排查常见的域验证问题” (p. 59)的故障排除页面上的步骤。

AWS CLI

启动私有 DNS 名称域的验证过程

使用 start-vpc-endpoint-service-private-dns-verification。

API

启动私有 DNS 名称域的验证过程

使用 StartVpcEndpointServicePrivateDnsVerification。

删除终端节点服务私有 DNS 名称

只有在没有到服务的连接后，才能删除终端节点服务私有 DNS 名称。

Console

删除端点服务私有 DNS 名称

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点服务。
3. 选择终端节点服务，然后依次选择 Actions (操作) 和 Modify private DNS name (修改私有 DNS 名称)。
4. 清除 Associate a private DNS name with the service （将私有 DNS 名称与服务关联）。
5. 选择保存更改。

AWS CLI

删除端点服务私有 DNS 名称

使用 modify-vpc-endpoint-service-configuration。

API

删除端点服务私有 DNS 名称

使用 ModifyVpcEndpointServiceConfiguration。

Amazon VPC 私有 DNS 域名验证 TXT 记录

您的域与一组域名系统 (DNS) 记录相关联，这些记录由您的 DNS 提供商管理。TXT 记录是一种 DNS 记录，可提供有关您的域的其他信息。每个 TXT 记录均包含一个名称和一个值。

使用 Amazon VPC 控制台或 API 启动域所有权验证时，我们向您提供 TXT 记录所使用的名称和值。例如，如果域是 myexampleservice.com，则 Amazon VPC 生成的 TXT 记录设置如下例所示：

终端节点私有 DNS 名称 TXT 记录

域验证名称	类型	域验证值
_vpce:aksldja21i1.myexampleservice.com	TXT	vpce:asjdakjshd78126eu21

使用指定的 Domain verification name (域验证名称) 和 Domain verification value (域验证值) 向域的 DNS 服务器添加 TXT 记录。当 Amazon VPC 检测到域的 DNS 设置中存在 TXT 记录时，即完成 Amazon VPC 域所有权验证。

如果您的 DNS 提供商不允许 DNS 记录名称包含下划线，则可以对 Domain verification name (域验证名称) 使用域名。在这种情况下，对于前面的示例，TXT 记录名称将是 myexampleservice.com。

您可以在排查常见的私有 DNS 域验证问题 (p. 59)中找到有关如何检查域所有权验证设置的故障排除信息和说明。

Amazon Route 53

将 TXT 记录添加到您的域的 DNS 服务器的过程取决于为您提供 DNS 服务的组织。您的 DNS 提供商可能是 Amazon Route 53 或其他域名注册商。此部分介绍将 TXT 记录添加到 Route 53 的过程，以及适用于其他 DNS 提供商的通用过程。

将 TXT 记录添加到 Route 53 托管域的 DNS 记录

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 选择 Endpoint Services (终端节点服务)。
3. 选择终端节点服务。
4. 在 Details (详细信息) 选项卡上，记下 Domain verification value (域验证值) 和 Domain verification name (域验证名称) 旁边显示的值。
5. 在 Amazon Route 53 控制台中，为托管区域创建记录。有关如何创建记录的信息，请参阅 Amazon Route 53 开发人员指南中的使用 Amazon Route 53 控制台创建记录。使用以下值：
   - 对于 Record type（记录类型），选择 TXT。
   - 对于 TTL (Seconds) (TTL (秒))，输入 **1800**。
   - 对于 Routing policy（路由策略），选择 Simple routing（简单路由）。
   - 对于 Value/Route traffic to（值/路由流量到），从 Amazon VPC 控制台输入 Domain verification value（域验证值）。
6. 在 Amazon VPC 控制台的终端节点服务页面的详细信息选项卡上，检查终端节点旁边的域验证状态列中的值。如果状态为“pending verification (等待验证)”，请等待几分钟，然后选择 refresh (刷新)。重复此过程，直至状态列中的值为“verified (已验证)”。您可以手动启动验证过程。有关更多信息，请参阅 the section called “手动启动终端节点服务私有 DNS 名称域验证” (p. 56)。

Generic procedures for other DNS providers

将 TXT 记录添加到 DNS 配置的过程因服务提供商而有所不同。有关特定步骤，请参阅您的 DNS 提供商文档。本部分中的过程提供将 TXT 记录添加到域的 DNS 配置的基本概述。

将 TXT 记录添加到您的域的 DNS 服务器 (一般步骤)

1. 转到您的 DNS 提供商的网站。如果您不确定您的域使用的 DNS 提供商，可以使用免费的 Whois 服务进行查找。
2. 在提供商网站上，登录到您的账户。
3. 查找用于更新您的域的 DNS 记录的页面。此页面的名称通常为“DNS Records (DNS 记录)”、“DNS Zone File (DNS 区文件)”或“Advanced DNS (高级 DNS)”。如果您不确定，请参阅提供商的文档。
4. 使用提供的名称和值添加一条 TXT 记录AWS

   Important

   某些 DNS 提供商会自动将域名附加到 DNS 记录的末尾。添加已包含域名（如 _pmBGN/7Mjnf.example.com）的记录可能会导致域名重复（如 _pmBGN/7Mjnfexample.com.example.com）。要避免域名重复，请在 DNS 记录中的域名结尾添加句点。这将向您的 DNS 提供商指出，记录名称完全符合条件（即，不再相对于该域名），并将防止 DNS 提供商附加其他域名。
5. 保存您的更改。DNS 记录更新最长需要 48 小时生效，通常情况下生效时间要早很多。

排查常见的私有 DNS 域验证问题

要使用 Amazon VPC 验证终端节点服务私有 DNS 域名，请使用 Amazon VPC 控制台或 API 启动该过程。本节包含有可帮助解决验证过程问题的信息。

常见的域验证问题

如果您尝试验证域但遇到问题，请查看下面的可能原因和解决方法。

- 您正在尝试验证您不拥有的域。除非您拥有域，否则您无法验证域。
- 您的 DNS 提供商不允许在 TXT 记录名称中使用下划线。某些 DNS 提供商不允许在域的 DNS 记录名称中包含下划线字符。如果提供商有此要求，可以省略 TXT 记录名称中的 _amazovpc。
- 您的 DNS 提供商已将域名附加到 TXT 记录的末尾。某些 DNS 提供商会自动将您的域名附加到 TXT 记录的属性名称中。例如，如果您创建一个属性名称为 _amazonvpc.example.com 的记录，提供商可能会附加域名，最终的属性名称将为 _amazonvpc.example.com.example.com。要避免域名重复，您可以在创建 TXT 记录时在域名结尾添加句点。此步骤告知 DNS 提供商没有必要将域名附加到 TXT 记录。
- 您的 DNS 提供商修改了 DNS 记录值。某些提供商会自动修改 DNS 记录值以仅使用小写字母。我们仅在您的域检测到其属性值与您启动域所有权验证流程时提供的值完全匹配的验证记录时才验证您的域。如果域的 DNS 提供商将 TXT 记录值更改为仅使用小写字母，请与 DNS 提供商联系获取更多帮助。
- 您需要多次验证同一个域。您可能需要从不同区域发送或使用同一个域从多个 AWS 账户发送，因而需要多次验证您的域。如果 DNS 提供商不允许您拥有多条具有相同属性名称的 TXT 记录，您仍可以验证两个域。如果 DNS 提供商允许，可以将多个属性值分配到同一条 TXT 记录。例如，如果 DNS 由 Amazon Route 53 管理，可以按照以下步骤为同一条 TXT 记录设置多个值：

  1. 在 Route 53 控制台中，选择在验证第一个区域中的域时创建的 TXT 记录。
  2. 在 Value (值) 框中，转到现有属性值的末尾，然后按 Enter。
  3. 添加附加区域的属性值，然后保存记录集。

  如果 DNS 提供商不允许向同一条 TXT 记录分配多个值，则可以使用 TXT 记录的属性名称中的值来验证域一次，而另一次使用从属性名称中删除的值来验证域。例如，您使用“_asnbcdasd”进行验证，然后使用“asnbcdasd”进行验证。此解决方案的缺点是只能对同一个域验证两次。

如何检查域验证设置

您可以使用以下过程验证您的私有 DNS 名称域所有权验证 TXT 记录是否正确发布到您的 DNS 服务器。此过程使用 nslookup 工具，目前支持的平台有 Windows 和 Linux。在 Linux 上，您也可以使用 dig。

这些说明中的命令在 Windows 7 中执行，我们使用的示例域为 example.com。

在此过程中，您首先要查找适用于您的域的 DNS 服务器，然后查询这些服务器以查看 TXT 记录。您查询适用于您的域的 DNS 服务器，因为这些服务器包含适用于您的域的最新信息，这可能需要一定时间才会传播到其他 DNS 服务器。

验证您的域所有权验证 TXT 记录已发布到您的 DNS 服务器

1. 通过采取以下步骤查找您的域的名称服务器。

   a. 进入命令行。要进入 Windows 7 中的命令行，请选择开始，然后输入 cmd。在基于 Linux 的操作系统中，打开终端窗口。

   b. 在命令提示符处，输入以下命令，其中 <domain> 是您的域。

   ```
   nslookup -type=NS <domain>
   ```

   例如，如果您的域是 example.com，则命令如下所示。

```
nslookup -type=NS example.com
```

命令的输出将列出可用于您的域的名称服务器。您将在下一步骤中查询这些服务器之一。

2. 通过采取以下步骤，验证 TXT 记录已正确发布。

   a. 在命令提示符处，输入以下命令，其中 <domain> 是您的域，<name server> 是您在步骤 1 中找到的某个名称服务器。

   ```
   nslookup -type=TXT  _aksldja21i1.<domain> <name server>
   ```

   在 _aksldja21i1.example.com 示例中，如果我们在步骤 1 中找到的名称服务器名为 ns1.name-server.net，则输入以下内容。

   ```
   nslookup -type=TXT  _aksldja21i1.example.com ns1.name-server.net
   ```

   b. 在命令的输出中，请验证 `text =` 后的字符串与在 Amazon VPC 控制台的身份列表中选择域时看到的 TXT 值匹配。

   在本示例中，我们正在 _aksldja21i1.example.com 下寻找值为 `asjdakjshd78126eu21` 的 TXT 记录。如果记录已正确发布，我们希望命令具有以下输出。

   ```
   _aksldja21i1.example.com text = "asjdakjshd78126eu21"
   ```

与 AWS PrivateLink 集成的 AWS 服务

以下服务与 AWS PrivateLink 集成。您可以创建接口终端节点 (p. 3)以连接到这些服务。

当服务与 AWS PrivateLink 集成但不支持 VPC 终端节点策略时，VPC 终端节点策略列会显示“否”。选择“是”链接以查看支持 VPC 终端节点策略的服务的文档。

AWS服务	VPC 终端节点策略
Amazon API Gateway	是
Amazon AppStream 2.0	否
AWS App Mesh	否
Application Auto Scaling	是
Amazon Athena	是
AWS Audit Manager	是
Amazon Aurora	是
AWS Auto Scaling	是
Amazon Braket	是
AWS Certificate Manager Private Certificate Authority	是
Amazon Cloud Directory	是
AWS CloudFormation	否
AWS CloudHSM	是
AWS CloudTrail	否
Amazon CloudWatch	是
Amazon CloudWatch Events	是
Amazon CloudWatch Logs	是
AWS CodeArtifact	是
AWS CodeBuild	是
AWS CodeCommit	是

AWS服务	VPC 终端节点策略
AWS CodeDeploy	是
Amazon CodeGuru Profiler	否
Amazon CodeGuru Reviewer	否
AWS CodePipeline	否
AWS CodeStar 连接	是
Amazon Comprehend	是
Amazon Comprehend Medical	是
AWS Config	是
Amazon Connect Customer Profiles	是
AWS Database Migration Service	是
AWS Data Exchange	是
AWS DataSync	否
AWS Device Farm	否
Amazon DevOps Guru	是
Amazon EBS 直接 API	否
Amazon EC2	是
EC2 Image Builder	是
Amazon EC2 Auto Scaling	是
AWS Elastic Beanstalk	是
Amazon Elastic File System	是
Elastic Load Balancing	是
Amazon Elastic Container Registry	是
Amazon Elastic Container Service	是
Amazon EMR	是
Amazon EventBridge	是
AWS Fault Injection Simulator	是

AWS服务	VPC 终端节点策略
Amazon FinSpace	✓ 是
Amazon Fraud Detector	✓ 是
AWS Glue	✓ 是
AWS Identity and Access Management Access Analyzer	✓ 是
Amazon HealthLake	✓ 是
AWS IoT Core	✗ 否
AWS IoT Core for LoRaWAN	✗ 否
AWS IoT Greengrass	✓ 是
AWS IoT SiteWise	✗ 否
Amazon Kendra	✓ 是
AWS Key Management Service	✓ 是
Amazon Keyspaces（针对 Apache Cassandra）	✓ 是
Amazon Kinesis Data Firehose	✓ 是
Amazon Kinesis Data Streams	✓ 是
AWS Lake Formation	✓ 是
AWS Lambda	✓ 是
AWS License Manager	✓ 是
Amazon Lookout for Equipment	✓ 是
Amazon Lookout for Vision	✓ 是
Amazon Managed Blockchain	✗ 否
Amazon Managed Workflows for Apache Airflow	✓ 是
Amazon Nimble Studio	✓ 是
AWS Proton	✓ 是
Amazon QLDB	✓ 是
Amazon RDS	✓ 是
Amazon RDS Data API	✓ 是

AWS服务	VPC 终端节点策略
Amazon Redshift	✓ 是
Amazon Rekognition	✓ 是
Amazon S3	✓ 是
Amazon S3 多区域访问点	✓ 是
Amazon SageMaker 和 Amazon SageMaker Runtime	✓ 是
Amazon SageMaker Notebook	✓ 是
AWS Secrets Manager	✓ 是
AWS Security Token Service	✓ 是
AWS Server Migration Service	✗ 否
AWS Service Catalog	✗ 否
Amazon SES	✗ 否
Amazon SNS	✓ 是
Amazon SQS	✓ 是
AWS Step Functions	✓ 是
AWS Systems Manager	✓ 是
AWS Storage Gateway	✗ 否
Amazon Textract	✓ 是
Amazon Transcribe	✓ 是
Amazon Transcribe Medical	✓ 是
AWS Transfer for SFTP	✗ 否
Amazon WorkSpaces	✓ 是
AWS X-Ray	✓ 是
其他 AWS 账户托管的终端节点服务 (p. 35)	✗ 否
支持的 AWS Marketplace 合作伙伴服务	✗ 否

查看可用的 AWS 服务名称

您可以使用 describe-vpc-endpoint-services 命令查看支持 VPC 终端节点的服务名称。

您可以运行以下命令以获取网关或接口终端节点的服务名称列表。`service-type` 筛选条件的可能值为 `Interface` 和 `Gateway`。该 `--query` 选项将输出限制为服务名称。

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=service-type --
query ServiceNames
```

以下示例显示了支持接口终端节点的服务。

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=Interface --query
 ServiceNames
```

下面是示例输出：

```
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.acm-pca",
    "com.amazonaws.us-east-1.airflow.api",
    "com.amazonaws.us-east-1.airflow.env",
    "com.amazonaws.us-east-1.airflow.ops",
    "com.amazonaws.us-east-1.application-autoscaling",
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.athena",
...
```

获得服务名称后，可以通过使用以下命令查看详细信息。

```
aws ec2 describe-vpc-endpoint-services --service-name service-name
```

以下示例显示有关 `us-east-1` 区域中 Amazon S3 接口终端节点的信息。`service-type` 筛选条件将 Amazon S3 网关终端节点从输出中排除。

```
aws ec2 describe-vpc-endpoint-services --service-name "com.amazonaws.us-east-1.s3" --filter
 Name=service-type,Values=Interface --region us-east-1
```

下面是示例输出：

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.s3",
            "ServiceId": "vpce-svc-081d84efcdc7bac15",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
```

```
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "s3.us-east-1.vpce.amazonaws.com"
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": []
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.s3"
    ]
}
```

AWS PrivateLink 配额

以下表格列出了您的账户的每区域 AWS PrivateLink 资源的配额（之前称为限制）。除非另有说明，否则您可以请求增加这些配额。有关更多信息，请参阅 Service Quotas 用户指南中的请求增加配额。

如果您请求对每个资源提升适用的配额，我们将提升该区域中所有资源的配额。

名称	默认值	可调整	注释
每个区域的网关 VPC 终端节点数	20	是	每个 VPC 的网关终端节点限制为 255 个
每个 VPC 的接口和网关负载均衡器终端节点	50	是	它是一个 VPC 中接口终端节点和网关负载均衡器终端节点的组合配额。
VPC 终端节点策略大小	20480 个字符	否	VPC 终端节点策略的大小包括空格

以下选项适用于通过 VPC 终端节点传递的流量。

- 默认情况下，每个可用区的每个接口终端节点可支持高达 10 Gbps 的带宽，以及高达 40Gbps 的突增。如果您的应用程序需要更高的突增或持续的吞吐量，请联系 AWS Support。
- 网络连接的最大传输单位 (MTU) 是能够通过 VPC 终端节点传递的最大可允许数据包的大小（以字节为单位）。MTU 越大，可在单个数据包中传递的数据越多。VPC 终端节点支持 8500 字节的 MTU。到达 VPC 终端节点的大小超过 8500 字节的数据包将被丢弃。
- VPC 终端节点不会生成 FRAG_NEEDEDICMP 数据包，因此不支持路径 MTU 发现 (PMTUD)。
- VPC 终端节点会对所有数据包强制执行最大分段大小 (MSS) 固定。有关更多信息，请参阅 RFC879。