AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

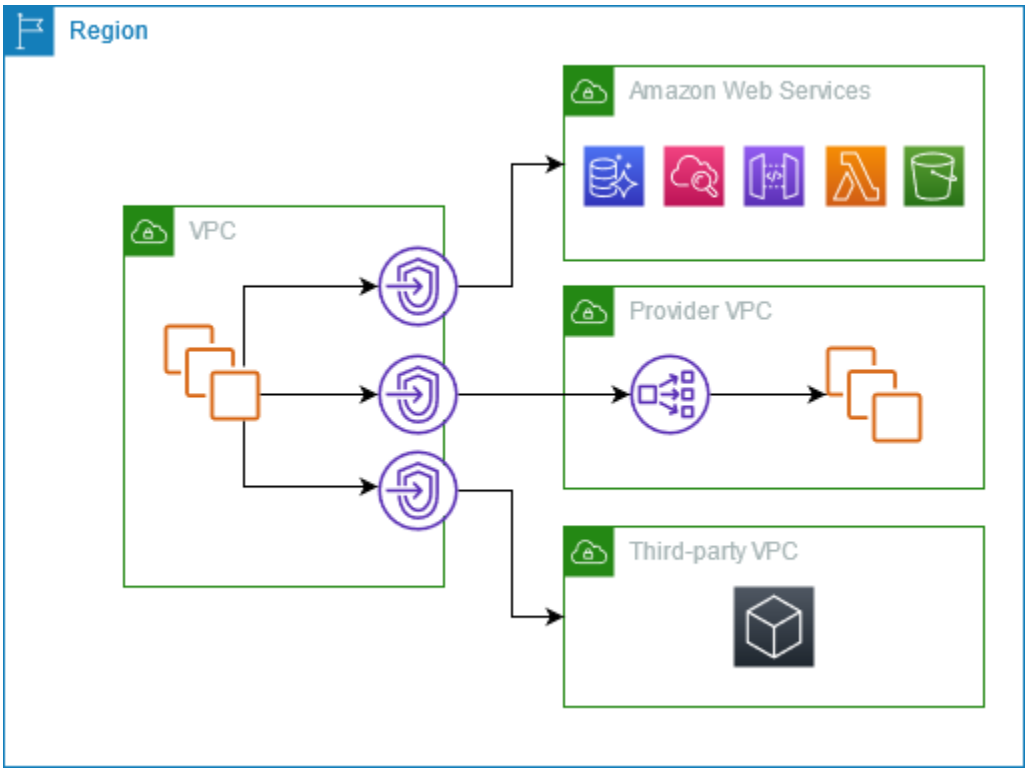
什么是 AWS PrivateLink？

AWS PrivateLink 是一种高度可用、可扩展的技术，您可以使用它来私下VPC连接到服务和资源，就像它们在您的服务中一样VPC。您无需使用 Internet 网关、NAT设备、公有 IP 地址、 AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接即可通过私有子网与服务或资源进行通信。因此，您可以控制可从您的访问的特定API端点、站点、服务和资源VPC。

使用案例

您可以创建VPC终端节点，将中的客户端连接到与之集成的服务和资源 AWS PrivateLink。VPC您可以创建自己的VPC终端节点服务并将其提供给其他 AWS 客户。有关更多信息，请参阅 the section called “概念”。

在下图中，左边的VPC私有子网中有几个 Amazon EC2 实例和五个VPC终端节点，即三个接口终端VPC节点、一个资源终VPC端节点和一个服务网络终VPC端节点。第一个接口VPC终端节点连接到 AWS 服务。第二个接口VPC终端节点连接到另一个 AWS 账户托管的服务（VPC终端节点服务）。第三个接口VPC端点连接到 AWS Marketplace 合作伙伴服务。资源VPC端点连接到数据库。服务网络VPC端点连接到服务网络。



了解更多

- the section called “概念”
- 访问权限 AWS 服务
- 访问 SaaS 产品
- 访问虚拟设备
- 共享您的服务

使用VPC端点

您可以使用以下任一方法创建、访问和管理VPC终端节点：

- AWS Management Console— 提供可用于访问 AWS PrivateLink 资源的 Web 界面。打开 Amazon VPC 控制台，然后选择终端节点或终端节点服务。
- AWS Command Line Interface (AWS CLI) — 为各种各样的命令提供命令 AWS 服务，包括 AWS PrivateLink。有关命令的更多信息 AWS PrivateLink，请参阅《AWS CLI 命令参考》中的 ec2。
- AWS CloudFormation – 创建用来描述 AWS 资源的模板。借助模板，您可以将这些资源作为一个单位进行预置和管理。有关更多信息，请参阅以下 AWS PrivateLink 资源：
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS:: ElasticLoadBalancing V2:: LoadBalancer
- AWS SDKs— 提供特定于语言APIs的内容。SDKs会处理许多连接细节，例如计算签名、处理请求重试次数和处理错误。有关更多信息，请参阅用于在 AWS上进行构建的工具。
- 查询 API-提供您使用HTTPS请求调用的低级API操作。使用查询API是访问 Amazon 的最直接方式 VPC。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 参考中的AWS PrivateLink 操作。

定价

有关VPC终端节点定价的信息，请参阅AWS PrivateLink 定价。

AWS PrivateLink 概念

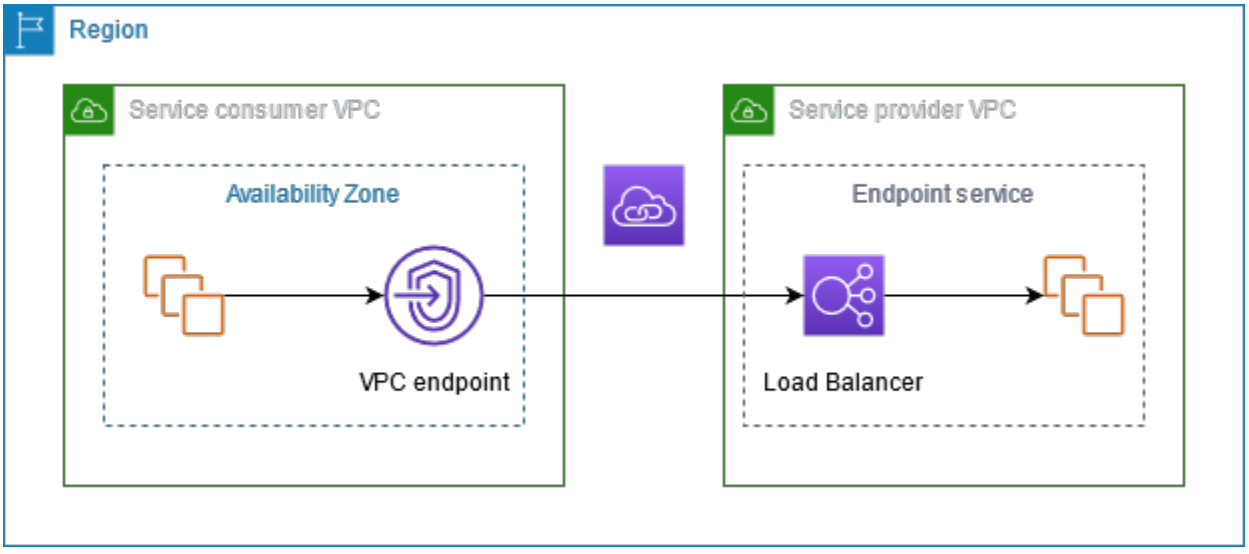
您可以使用 Amazon VPC 来定义虚拟私有云 (VPC)，这是一个逻辑上隔离的虚拟网络。您可以允许您的客户端连接到该VPC以外的目的地VPC。例如，向添加互联网网关VPC以允许访问互联网，或者添加VPN连接以允许访问您的本地网络。或者，使用 AWS PrivateLink 允许您的客户端VPCs使用私有 IP 地址VPC连接到其他服务器中的服务和资源，就好像这些服务和资源直接托管在您的中一样VPC。

以下是开始使用 AWS PrivateLink时需要理解的重要概念。

内容

架构图

下图简要概述了 AWS PrivateLink 工作原理。消费者创建VPC端点以连接到由提供商托管的终端节点服务和资源。



提供商

了解与提供商相关的概念。

服务提供商

服务的所有者为服务提供商。服务提供商包括 AWS、 AWS 合作伙伴和其他 AWS 账户。服务提供商可以使用 AWS 资源（例如EC2实例）或使用本地服务器托管其服务。

资源提供者

资源（例如数据库、节点集群或实例）的所有者是资源提供者。资源提供者包括 AWS 服务、 AWS 合作伙伴和其他 AWS 账户。资源提供者可以将其资源托管在本地VPCs或本地。

概念

- 端点服务
- 服务名称
- 服务状态
- 资源配置
- 资源网关

端点服务

服务提供商创建了端点服务，以使其服务在区域中可用。在创建端点服务时，服务提供商必须指定负载均衡器。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。

默认情况下，您的端点服务对服务使用者不可用。您必须添加允许特定 AWS 委托人连接到您的终端节点服务的权限。

服务名称

每个端点服务都由服务名称标识。服务使用者在创建VPC终端节点时必须指定服务的名称。服务使用者可以查询的服务名称 AWS 服务。服务提供商必须与服务使用者共享其服务名称。

服务状态

以下是端点服务可能具有的状态：

- `Pending` - 正在创建端点服务。
- `Available` - 端点服务可用。
- `Failed` - 无法创建端点服务。
- `Deleting` - 服务提供商删除了端点服务，删除正在进行中。

- `Deleted` - 端点服务已删除。

资源配置

资源提供者创建资源配置以共享资源。资源配置是一个逻辑对象，它表示单个资源（例如数据库）或一组资源（例如节点集群）。资源可以是 IP 地址、域名目标或 Amazon 数据库。RDS

与其他账户共享时，资源提供者必须通过资源共享共享共享 AWS RAM 资源以允许其他账户中的特定 AWS 委托人通过资源VPC端点连接到资源。

资源配置可以与委托人通过服务网络端点连接的服务网络VPC相关联。

资源网关

资源网关是进入共享资源的VPC起点。提供商创建资源网关以共享来自的资源VPC。

服务或资源使用者

服务或资源的用户是消费者。消费者可以从自己的本地VPCs或本地访问终端节点服务和资源。

概念

- VPC 端点
- 端点网络接口
- 端点策略
- 端点状态

VPC 端点

消费者创建VPC终端节点以将其VPC连接到终端节点服务或资源。在创建终端节点时，使用者必须指定终端VPC节点服务、资源或服务网络。有多种类型的VPC端点。您必须创建所需的终VPC端节点类型。

- `Interface`-创建要向终端服务发送TCP或UDP流量的接口终端节点。使用解析发往终端节点服务的流量DNS。
- `GatewayLoadBalancer` - 创建网关负载均衡器端点以将流量发送到使用私有 IP 地址的虚拟设备实例集。您可以使用路由表将流量从您的路由VPC到 Gateway Load Balancer 终端节点。网关负载均衡器将流量分配到虚拟设备，并且可以根据需求进行扩展。

- Resource-创建资源端点以访问与您共享并驻留在另一个资源中的资源VPC。资源终端节点允许您私密安全地访问资源，例如数据库、节点集群、实例、应用程序终端节点、域名目标或 IP 地址，这些地址可能位于另一个VPC或本地环境的私有子网中。资源端点不需要负载均衡器，可让您直接访问资源。
- Service network-创建服务网络端点以访问您创建或与您共享的服务网络。您可以使用单个服务网络端点私密安全地访问与服务网络关联的多个资源和服务。

还有另一种类型的VPC终端节点Gateway，它创建一个网关终端节点来向 Amazon S3 或 DynamoDB 发送流量。与其他类型的终端节点不同 AWS PrivateLink，网关VPC终端节点不使用。有关更多信息，请参阅 the section called “网关端点”。

端点网络接口

端点网络接口是请求者管理的网络接口，可作为发往终端节点服务、资源或服务网络的流量的入口点。对于您在创建VPC终端节点时指定的每个子网，我们都会在子网中创建一个终端节点网络接口。

如果VPC端点支持IPv4，则其端点网络接口具有IPv4地址。如果VPC端点支持IPv6，则其端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。使用地址描述端点网络接口时，请注意该IPv6地址已启denyAllIgwTraffic用。

端点策略

VPC终端节点策略是您附加到VPC终端节点的IAM资源策略。它决定哪些委托人可以使用VPC终端节点访问终端节点服务。默认VPC终端节点策略允许所有委托人对终VPC端节点上的所有资源执行所有操作。

端点状态

创建接口VPC终端节点时，终端节点服务会收到连接请求。服务提供商可以接受或拒绝请求。如果服务提供者接受请求，则服务使用者可以在VPC终端节点进入Available状态后使用该终端节点。

以下是VPC终端节点可能的状态：

- PendingAcceptance - 连接请求待处理。如果手动接受请求，则此为初始状态。
- Pending - 服务提供商接受了连接请求。如果自动接受请求，则此为初始状态。如果服务使用者修改VPC终端节点，则VPC终端节点将恢复到此状态。
- Available-终VPC端节点可供使用。
- Rejected - 服务提供商拒绝了连接请求。服务提供商也可以在连接可用后拒绝连接。

- `Expired` - 连接请求已过期。
- `Failed`-无法提供VPC终端节点。
- `Deleting`-服务使用者删除了VPC终端节点，并且正在进行删除。
- `Deleted`-终VPC端节点已删除。

AWS PrivateLink 连接

您的VPC流量通过终端节点与终端节点服务或资源之间的连接发送到VPC终端节点服务或资源。VPC终端节点与终端节点服务或资源之间的流量保留在 AWS 网络内，无需通过公共互联网。

服务提供商可添加权限，以便服务使用者可以访问端点服务。服务使用者可启动连接，而服务提供商可接受或拒绝连接请求。资源所有者或服务网络所有者通过与消费者共享资源配置或服务网络， AWS Resource Access Manager 以便使用者可以访问资源或服务网络。

使用接口VPC终端节点，使用IAM者可以使用终端节点策略来控制哪些委托人可以使用VPC终端节点访问终端节点服务或资源。

私有托管区

托管区域是用于DNS存放记录的容器，用于定义如何路由域或子域的流量。对于公有托管区，记录指定如何在互联网上路由流量。对于私有托管区域，记录会指定如何在您的中路由流量VPCs。

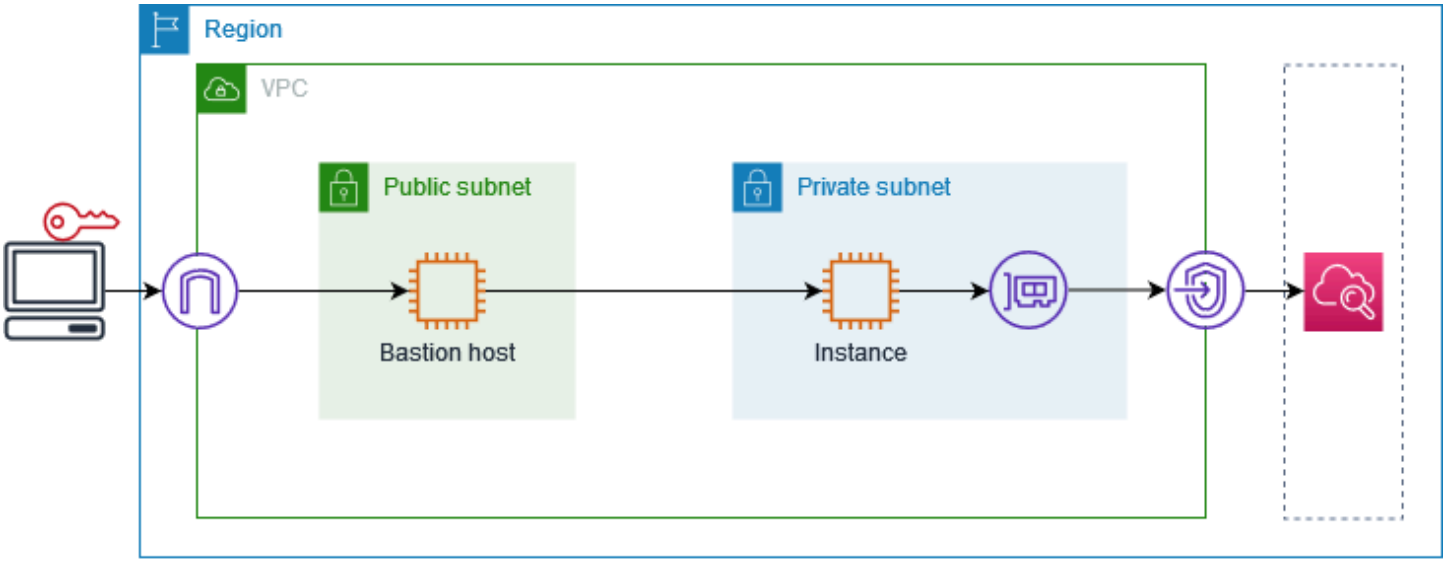
您可以将 Amazon Route 53 配置为将域流量路由到VPC终端节点。有关更多信息，请参阅使用您的域名将流量路由到VPC终端节点。

您可以使用 Route 53 来配置水平分割DNS，其中公共网站和由提供支持的终端节点服务使用相同的域名。 AWS PrivateLink DNS消费者对公共主机名的请求会VPC解析到端点网络接口的私有 IP 地址，但来自外部的请求会VPC继续解析到公共端点。有关更多信息，请参阅路由流量DNS机制和为 AWS PrivateLink 部署启用故障转移。

开始使用 AWS PrivateLink

本教程演示如何 CloudWatch 使用将请求从私有子网中的EC2实例发送到 Amazon AWS PrivateLink。

下图提供了此场景的概述。要从您的计算机连接到私有子网中的实例，您需要首先连接到公有子网中的堡垒主机。堡垒主机和实例必须使用相同的密钥对。由于私钥.pem文件位于您的计算机上，而不是堡垒主机上，因此您将使用SSH密钥转发。然后，您可以从堡垒主机连接到该实例，而无需在 ssh 命令中指定 .pem 文件。在为设置VPC终端节点后 CloudWatch，来自实例的流量将解析到终端节点网络接口，然后 CloudWatch 使用VPC终端节点发送到。 CloudWatch



出于测试目的，您可以使用单个可用区。在生产中，建议您使用至少两个可用区，来实现低延迟和高可用性。

任务

- 步骤 1：创建VPC带子网的
- 步骤 2：启动实例
- 步骤 3：测试 CloudWatch 访问权限
- 步骤 4：创建要访问的VPC终端节点 CloudWatch
- 步骤 5：测试VPC终端节点
- 步骤 6：清除

步骤 1：创建VPC带子网的

使用以下步骤创建VPC具有公有子网和私有子网的。

创建 VPC

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 选择创建VPC。
3. 要创建资源 VPC，请选择更多。
4. 在 “自动生成名称标签” 中，输入名称。VPC
5. 若要配置子网，请执行以下操作：
   a. 对于 Number of Availability Zones（可用区域数量），根据您的需求选择 1 或 2。
   b. 对于 Number of public subnets（公有子网数量），确保每个可用区有一个公有子网。
   c. 对于 Number of private subnets（私有子网数量），确保每个可用区有一个私有子网。
6. 选择创建VPC。

步骤 2：启动实例

使用您在上一步中创建的，在公有子网中启动堡垒主机，在私有子网中启动实例。VPC

先决条件

- 使用 .pem 格式创建密钥对。启动堡垒主机和实例时，必须选择此密钥对。
- 为堡垒主机创建一个安全组，允许来自该CIDR区块的入站SSH流量进入您的计算机。
- 为实例创建一个安全组，允许来自堡垒主机的安全组的入站SSH流量。
- 创建IAM实例配置文件并附加CloudWatchReadOnlyAccess策略。

启动堡垒主机

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 选择启动实例。
3. 对于 Name（名称），输入您的堡垒主机的名称。
4. 保留默认图像和实例类型。
5. 对于 Key pair（密钥对），选择您的密钥对。

6. 对于 Network settings（网络设置），执行以下操作：
   a. 对于 VPC，选择你的VPC。
   b. 对于 Subnet（子网），选择公有子网。
   c. 对于 Auto-assign public IP（自动分配公有 IP），选择 Enable（启用）。
   d. 对于 Firewall（防火墙），选择 Select existing security group（选择现有安全组），然后为堡垒主机选择安全组。
7. 选择启动实例。

启动实例

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 选择启动实例。
3. 对于 Name（名称），输入您的实例的名称。
4. 保留默认图像和实例类型。
5. 对于 Key pair（密钥对），选择您的密钥对。
6. 对于 Network settings（网络设置），执行以下操作：
   a. 对于 VPC，选择你的VPC。
   b. 对于 Subnet（子网），选择私有子网。
   c. 对于 Auto-assign public IP（自动分配公有 IP），选择 Disable（禁用）。
   d. 对于 Firewall（防火墙），选择 Select existing security group（选择现有安全组），然后为实例选择安全组。
7. 展开 Advanced details（高级详细信息）。IAM例如配置文件，请选择您的IAM实例配置文件。
8. 选择启动实例。

步骤 3：测试 CloudWatch 访问权限

使用以下步骤确认该实例无法访问 CloudWatch。您将使用只读 AWS CLI 命令来执行此操作 CloudWatch。

测试访问 CloudWatch 权限

1. 在您的计算机上，使用以下命令将密钥对添加到SSH代理，其中*key.pem*是您的.pem 文件的名称。

```
ssh-add ./key.pem
```

如果您收到一条错误消息，提示您的密钥对的权限过于开放，请运行以下命令，然后重试上一个命令。

```
chmod 400 ./key.pem
```

2. 从您的计算机连接到堡垒主机。您必须指定 -A 选项、实例用户名（例如 ec2-user）和堡垒主机的公有 IP 地址。

```
ssh -A ec2-user@bastion-public-ip-address
```

3. 从堡垒主机连接到实例。您必须指定实例用户名（例如 ec2-user）和实例的私有 IP 地址。

```
ssh ec2-user@instance-private-ip-address
```

4. 按如下方式在实例上运行 CloudWatch list-Metric s 命令。对于--region选项，请指定您创建的区域VPC。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

5. 几分钟后，命令会超时。这表明您无法使用当前VPC配置 CloudWatch 从实例进行访问。

```
Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
```

6. 保持与您的实例的连接。创建VPC终端节点后，您将再次尝试此list-metrics命令。

步骤 4：创建要访问的VPC终端节点 CloudWatch

使用以下步骤创建连接到的VPC端点 CloudWatch。

先决条件

为允许流量进入的VPC终端节点创建安全组 CloudWatch。例如，添加一条允许来自该VPCCIDR区块的HTTPS流量的规则。

为创建VPC终端节点 CloudWatch

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。

2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 对于 Name tag（名称标签），输入端点的名称。
5. 对于 Service category（服务类别），选择 AWS 服务。
6. 对于服务，请选择 com.amazonaws。 ***region***. 监控。
7. 对于 VPC，请选择您的VPC。
8. 对于 Subnets（子网），选择可用区，然后选择私有子网。
9. 对于安全组，选择终VPC端节点的安全组。
10. 对于策略，选择完全访问权限以允许所有委托人通过VPC端点对所有资源进行所有操作。
11. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
12. 选择创建端点。初始状态为 Pending（待处理）。在转到下一步之前，请等到状态变为 Available（可用）。这可能需要几分钟的时间。

步骤 5：测试VPC终端节点

验证VPC终端节点是否正在将请求从您的实例发送到 CloudWatch。

测试VPC端点

在您的实例上运行以下 命令。对于`--region`选项，请指定您创建VPC终端节点的区域。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

如果您收到响应，甚至是结果为空的响应，则表示您已连接到 CloudWatch 使用 AWS PrivateLink。

如果您遇到`Unauthorized0peration`错误，请确保该实例具有允许访问的IAM角色 CloudWatch。

如果请求超时，请验证以下内容：

- 终端节点的安全组允许流量进入 CloudWatch。
- 该`--region`选项指定您在其中创建VPC终端节点的区域。

步骤 6：清除

如果不再需要您为本教程创建的堡垒主机和实例，则可以将其删除。

终止实例

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择两个测试实例，然后依次选择 Instance state（实例状态）、Terminate instance（终止实例）。
4. 当系统提示您确认时，选择终止。

如果您不再需要该VPC终端节点，可以将其删除。

删除VPC终端节点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择VPC终端节点。
4. 选择操作，删除VPC端点。
5. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

AWS 服务 通过以下方式访问 AWS PrivateLink

您 AWS 服务 使用终端节点访问一个。默认服务端点是公共接口，因此您必须向您的服务端点添加互联网网关，VPC这样流量才能从传送VPC到 AWS 服务。如果此配置不符合您的网络安全要求，则无需使用 AWS PrivateLink Internet 网关VPC，即可像在您的网络安全要求中 AWS 服务 一样进行连接。VPC

您可以使用VPC终端节点私密访问与之 AWS 服务 集 AWS PrivateLink 成的内容。您无需使用互联网网关即可构建和管理应用程序堆栈的所有层。

定价

您需要按在每个可用区配置接口VPC终端节点的每小时计费。此外，您还需按照处理的数据 GB 付费。有关更多信息，请参阅AWS PrivateLink 定价。

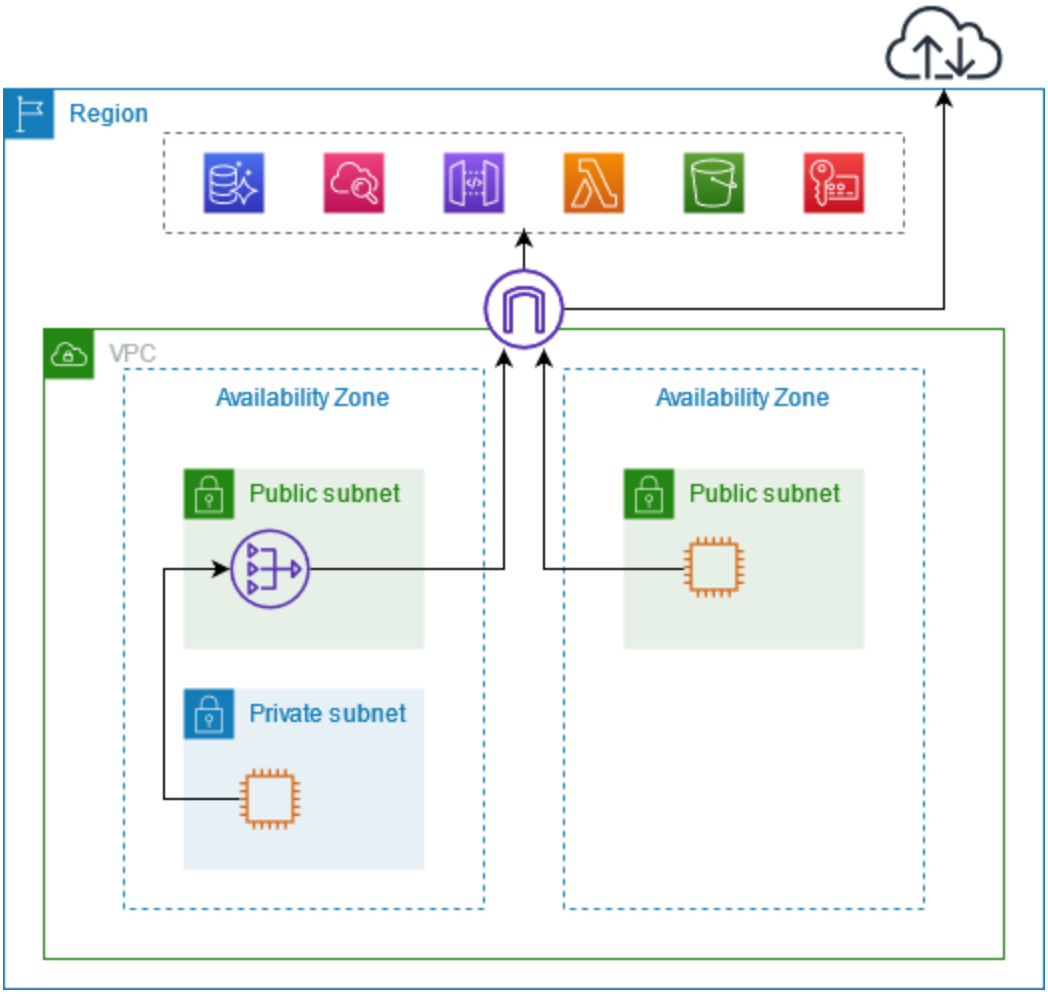
内容

概述

您可以 AWS 服务 通过他们的公共服务端点进行访问，也可以 AWS 服务 使用连接到支持的终端节点 AWS PrivateLink。本概述比较了这些方法。

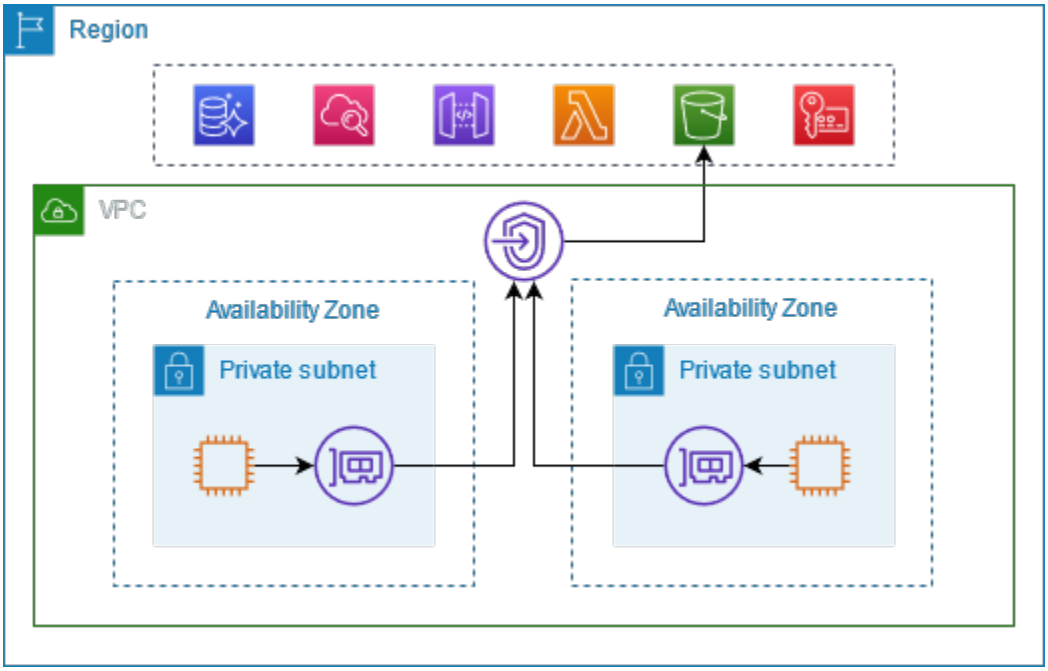
通过公有服务端点进行访问

下图显示了实例如何 AWS 服务 通过公共服务终端节点进行访问。 AWS 服务 从公有子网中的实例到的流量将路由到的 Internet 网关，VPC然后路由到 AWS 服务。 AWS 服务 从私有子网中的实例到的流量将路由到网NAT关，然后路由到的 Internet 网关VPC，然后再路由到。 AWS 服务当这些流量通过互联网网关时，它不会离开网络。 AWS



通过 Connect AWS PrivateLink

下图显示了实例是如何 AWS 服务 通过访问 AWS PrivateLink的。首先，创建接口VPC终端节点，用于在您的子网VPC和 AWS 服务 正在使用的网络接口之间建立连接。发往的 AWS 服务 流量使用解析到端点网络接口的私有 IP 地址DNS，然后使用终端节点与之间的连接发送到VPC终端节点网络接口的私有 IP 地址 AWS 服务。 AWS 服务



AWS 服务 自动接受连接请求。该服务无法通过VPC终端节点发起对资源的请求。

DNS主机名

大多数都 AWS 服务 提供公共区域终端节点，其语法如下。

```
protocol://service_code.region_code.amazonaws.com
```

例如，us-east-2 CloudWatch 中亚马逊的公共终端节点如下所示。

```
https://monitoring.us-east-2.amazonaws.com
```

使用 AWS PrivateLink，您可以使用私有终端节点向服务发送流量。当您创建接口VPC终端节点时，我们会创建区域和区域DNS名称，您可以使用这些名称与 AWS 服务 来自您的VPC进行通信。

您的接口VPC终端节点的区域DNS名称采用以下语法：

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

区域DNS名称的语法如下：

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

在为创建接口VPC终端节点时 AWS 服务，可以启用私有DNS。使用 privateDNS，您可以继续使用公有终端节点的DNS名称向服务发出请求，同时通过接口终VPC端节点利用私有连接。有关更多信息，请参阅 the section called “DNS分辨率”。

以下describe-vpc-endpoints命令显示接口终端节点的DNS条目。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

以下是启用私有DNS名称的 Amazon 接口终端节点 CloudWatch 的输出示例。第一个条目是私有区域端点。接下来的三个条目是私有分区端点。最后一个条目来自隐藏的私有托管区，该区域可将对公有端点的请求解析为端点网络接口的私有 IP 地址。

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

DNS分辨率

我们为您的接口VPC终端节点创建的DNS记录是公开的。因此，这些DNS名称是可以公开解析的。但是，来自外部的DNS请求VPC仍会返回终端节点网络接口的私有 IP 地址，因此，除非您有权访问终端节点服务，否则这些 IP 地址不能用于访问终端节点服务VPC。

私人 DNS

如果您DNS为接口VPC终端节点启用私有功能，并且同时启用VPC了DNS主机名和DNS解析，则我们会为您创建一个隐藏的 AWS托管私有托管区域。托管区域包含服务的默认DNS名称记录集，该记录集可将其解析为您的VPC终端节点网络接口的私有 IP 地址。因此，如果您的现有应用程序 AWS 服务 使用公共区域终端节点向发送请求，则这些请求现在会通过终端节点网络接口，而无需您对这些应用程序进行任何更改。

我们建议您为VPC终端节点启用私有DNS名称 AWS 服务。这样可以确保使用公共服务终端节点的请求（例如通过的请求）解析到您的VPC终端节点。 AWS SDK

Amazon 为您提供了一个名为 R oute 53 Resolver 的DNS服务器。VPCRoute 53 解析器会自动解析本地VPC域名并在私有托管区域中进行记录。但是，你不能从外部使用 Route 53 Resolver。VPC如果您想从本地网络访问VPC终端节点，可以使用 Route 53 解析器终端节点和解析器规则。有关更多信息，请参阅AWS Transit Gateway 与 AWS PrivateLink 和集成 Amazon Route 53 Resolver。

子网和可用区

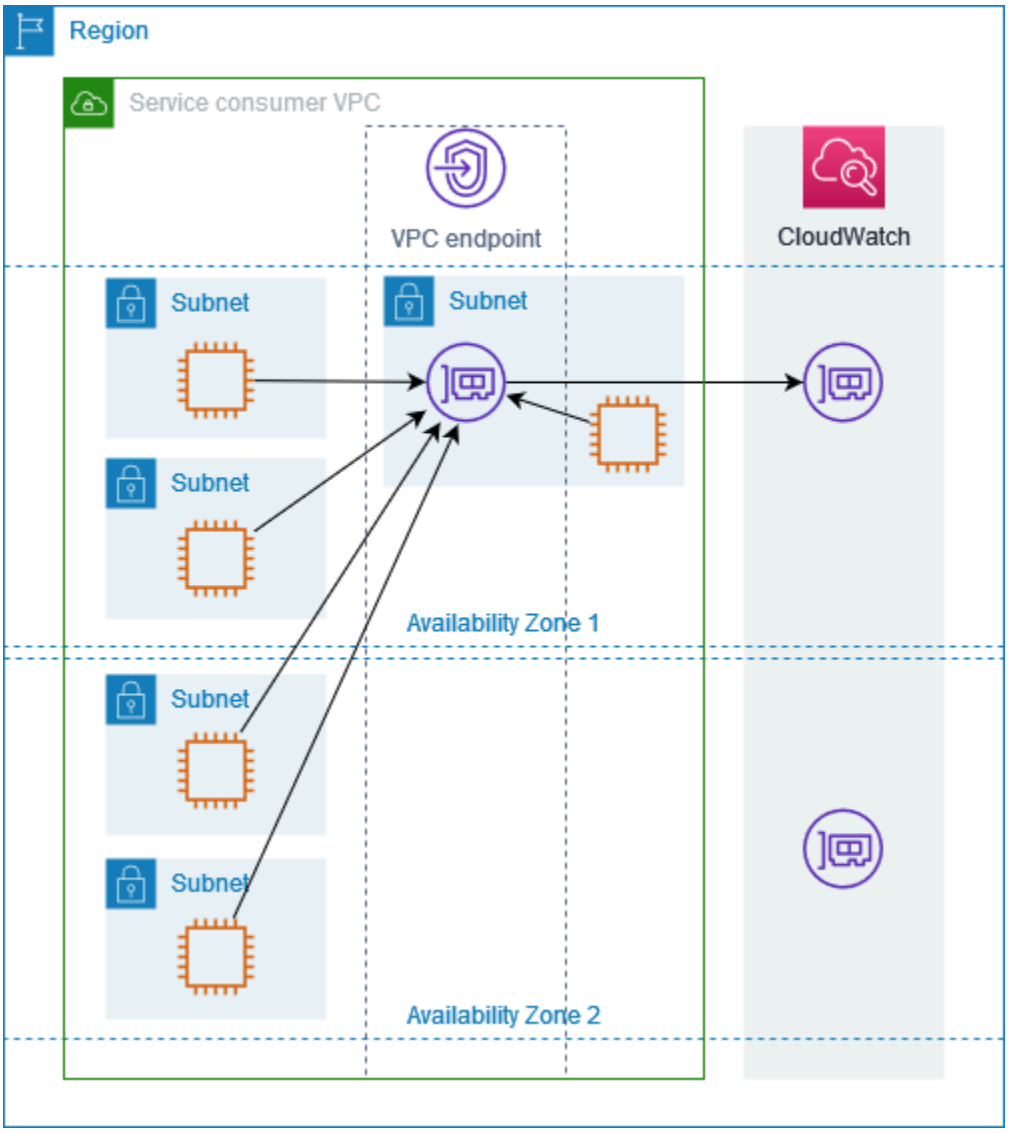
您可以为每个可用区配置一个子网的VPC终端节点。我们为您子网中的终端节点创建VPC终端节点网络接口。我们根据端点的 IP 地址类型为其子网中的每个VPC端点网络接口分配 IP 地址。端点网络接口的 IP 地址在其VPC终端节点的生命周期内不会更改。

在生产环境中，为提高可用性和弹性，我们建议采取以下措施：

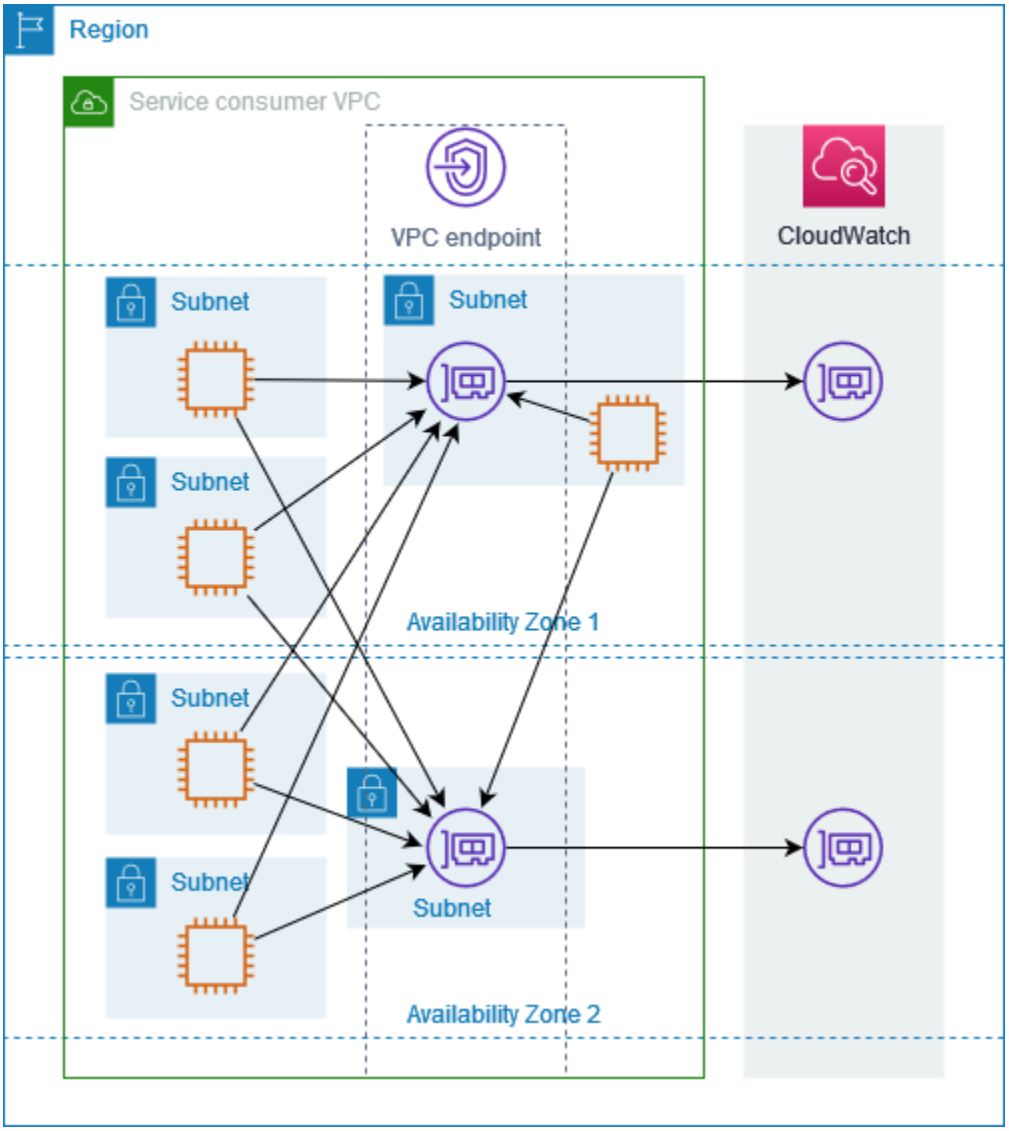
- 为每个VPC终端节点配置至少两个可用区，并在这些可用区 AWS 服务 中部署必须访问的 AWS 资源。
- 为VPC终端节点配置私有DNS名称。
- 使用 AWS 服务 其区域DNS名称（也称为公共终端节点）进行访问。

下图显示了在单个可用区中 CloudWatch 具有VPC终端节点网络接口的 Amazon 终端节点。当任何子网中的任何资源 CloudWatch使用其公有终端节点VPC访问 Amazon 时，我们会将流量解析到终端节点

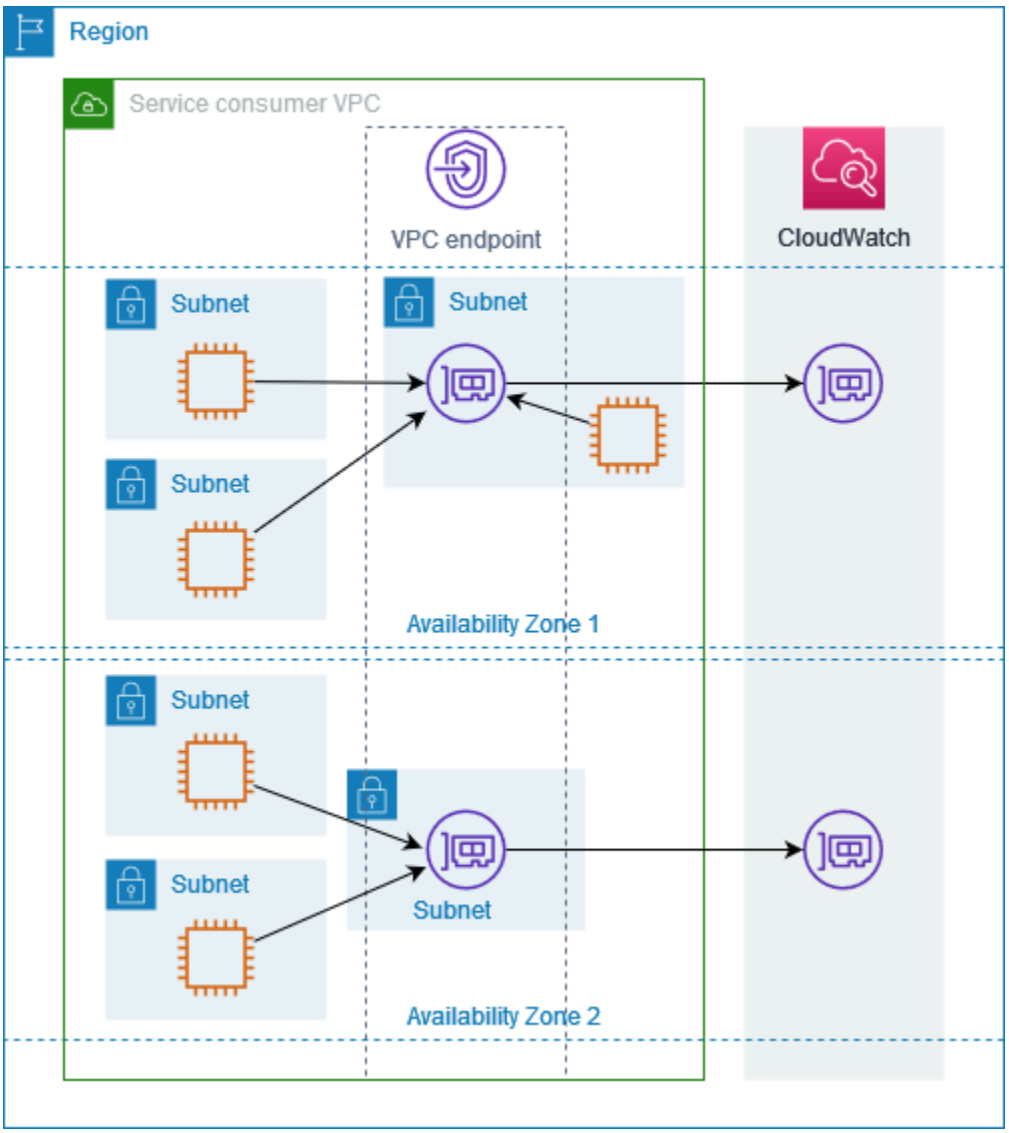
网络接口的 IP 地址。这包括来自其他可用区子网的流量。但是，如果可用区 1 受损，则可用区 2 中的资源将无法访问 Amazon CloudWatch。



下图显示了在两个可用区中 CloudWatch 具有VPC终端节点网络接口的 Amazon 终端节点。当任何子网中的任何资源使用其公共终端节点VPC访问 Amazon CloudWatch 时，我们会选择一个健康的终端节点网络接口，使用轮询算法在它们之间切换。然后，我们会将流量解析到选定端点网络接口的 IP 地址。



如果它更适合您的用例，则可以通过使用同一可用区中的端点网络接口，将流量从您的资源发送到 AWS 服务 。为此，请使用端点网络接口的私有区域端点或 IP 地址。



IP 地址类型

AWS 服务 即使他们不支持IPv6通过其公共端点，也可以IPv6通过其私有端点提供支持。支持的端点IPv6可以用AAAA记录响应DNS查询。

IPv6为接口终端节点启用的要求

- AWS 服务 必须使其服务端点可用IPv6。有关更多信息，请参阅 the section called “查看IPv6支持”。
- 接口端点的 IP 地址类型必须与接口端点的子网兼容，如下所述：
  - IPv4— 为您的端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围时，才支持此选项。

- IPv6— 为您的端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网时，IPv6才支持此选项。
- Dualstack — 将IPv4和IPv6地址分配给您的端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围时，才支持此选项。

如果接口VPC端点支持IPv4，则端点网络接口具有IPv4地址。如果接口VPC端点支持IPv6，则端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。如果您使用IPv6地址描述端点网络接口，请注意该接口已启`denyAllIgwTraffic`用。

AWS 服务 与之集成 AWS PrivateLink

以下内容与 AWS 服务 集成 AWS PrivateLink。您可以创建一个VPC终端节点来私下连接到这些服务，就像它们在您自己的服务中运行一样VPC。

选择AWS 服务列中的链接，查看与之集成的服务的文档 AWS PrivateLink。服务名称列包含您在创建接口VPC终端节点时指定的服务名称，或者它表示服务管理终端节点。

AWS 服务	服务名称
访问分析器	com.amazonaws。 *region*.access-analy
AWS Account Management	com.amazonaws。 *region*. 账户
亚马逊API网关	com.amazonaws。 *region*.execute-api
AWS AppConfig	com.amazonaws。 *region*.appconfig
	com.amazonaws。 *region*.appconfigdat
AWS App Mesh	com.amazonaws。 *region*.appmesh
	com.amazonaws。 *region*。 appmesh-envoy-management
AWS 应用程序运行器	com.amazonaws。 *region*.apprunner
AWS App Runner 服务	com.amazonaws。 *region*.apprunner.requests
Application Auto Scaling	com.amazonaws。 *region*. 应用程序自动缩放

AWS 服务	服务名称
AWS Application Discovery Service	com.amazonaws。*region*. 发现
	com.amazonaws。*region*.arsenal-disco
AWS 应用程序迁移服务	com.amazonaws。*region*.mgn
亚马逊 AppStream 2.0	com.amazonaws。*region*.appstream.api
	com.amazonaws。*region*.appstream.streamin
AWS AppSync	com.amazonaws。*region*.appsync-api
Amazon Athena	com.amazonaws。*region*.athena
AWS Audit Manager	com.amazonaws。*region*. 审计管理器
Amazon Aurora	com.amazonaws。*region*.rds
AWS Auto Scaling	com.amazonaws。*region*. 自动缩放计划
AWS B2B 数据交换	com.amazonaws。*region*.b2bi
AWS Backup	com.amazonaws。*region*. 备份
	com.amazonaws。*region*.backup-gatew
AWS Batch	com.amazonaws。*region*.batch
Amazon Bedrock	com.amazonaws。*region*. bedrock
	com.amazonaws。*region*.bedrock-agent
	com.amazonaws。*region*。 bedrock-agent-runtime
	com.amazonaws。*region*.bedrock 运行时
AWS Billing and Cost Management	com.amazonaws。*region*. 账单
	com.amazonaws。*region*. freetier

AWS 服务	服务名称
	com.amazonaws。 *region*. tax
AWS Billing Conductor	com.amazonaws。 *region*. billingcond
Amazon Braket	com.amazonaws。 *region*.braket
AWS Clean Rooms	com.amazonaws。 *region*. 洁净室
AWS Clean Rooms ML	com.amazonaws。 *region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws。 *region*.cloudcontro
	com.amazonaws。 *region*.cloudcontrolapi-fi
Amazon Cloud Directory	com.amazonaws。 *region*.cloud 目录
AWS CloudFormation	com.amazonaws。 *region*.cloudfor
AWS CloudHSM	com.amazonaws。 *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws。 *region*. 服务发现
	com.amazonaws。 *region*.servicediscovery-
	com.amazonaws。 *region*. 数据服务发现
	com.amazonaws。 *region*。 data-servicediscovery-fips
AWS CloudTrail	com.amazonaws。 *region*.cloudtra
Amazon CloudWatch	com.amazonaws。 *region*. 应用程序信号
	com.amazonaws。 *region*. 应用程序见解
	com.amazonaws。 *region*。显然
	com.amazonaws。 *region*. 显而易见的数据平面
	com.amazonaws。 *region*. 互联网监视器

AWS 服务	服务名称
	com.amazonaws。 *region*.internetmonitor-fies
	com.amazonaws。 *region*. 监控
	com.amazonaws。 *region*. 网络流量监视器
	com.amazonaws。 *region*. 网络流量监视器报告
	com.amazonaws。 *region*. 网络监视器
	com.amazonaws。 *region*.observability
	com.amazonaws。 *region*.rum
	com.amazonaws。 *region*.rum-dataplane
	com.amazonaws。 *region*. 合成物
	com.amazonaws。 *region*.sythetics-fips
Amazon CloudWatch 日志	com.amazonaws。 *region*.logs
AWS CodeArtifact	com.amazonaws。 *region*.codeartifact.api
	com.amazonaws。 *region*.codeartifact.存储库
AWS CodeBuild	com.amazonaws。 *region*.codebuild
	com.amazonaws。 *region*.codebuild-fips
AWS CodeCommit	com.amazonaws。 *region*.codemit
	com.amazonaws。 *region*.codemmit-fips
	com.amazonaws。 *region*.git-codecommi
	com.amazonaws。 *region*。 git-codecommit-fips
AWS CodeConnections	com.amazonaws。 *region*.codeconnections.api

AWS 服务	服务名称
	com.amazonaws。 *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws。 *region*.codeplo
	com.amazonaws。 *region*。 codedeploy-commands-secure
Amazon P CodeGuru rofiler	com.amazonaws。 *region*.codeguru-profiler
Amazon CodeGuru Reviewer	com.amazonaws。 *region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws。 *region*.codepilin
Amazon Comprehend	com.amazonaws。 *region*.comprehend
Amazon Comprehend Medical	com.amazonaws。 *region*.comprehendmedical
AWS Compute Optimizer	com.amazonaws。 *region*. 计算优化器
AWS Config	com.amazonaws。 *region*. 配置
Amazon Connect	com.amazonaws。 *region*.app 集成
	com.amazonaws。 *region*. 案例
	com.amazonaws。 *region*.connect-cam
	com.amazonaws。 *region*. 个人资料
	com.amazonaws。 *region*.voiceid
	com.amazonaws。 *region*. 智慧
AWS Connector Service	com.amazonaws。 *region*.aws连接器
AWS 控制目录	com.amazonaws。 *region*. 控制目录
AWS Cost Explorer	com.amazonaws。 *region*.ce
AWS 成本优化中心	com.amazonaws。 *region*。 cost-optimization-hub

AWS 服务	服务名称
AWS Data Exchange	com.amazonaws。*region*. 数据交换
AWS Data Exports	com.amazonaws。*region*。 bcm-data-exports
Amazon Data Firehose	com.amazonaws。*region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws。*region*.dms
	com.amazonaws。*region*.dms-fips
AWS DataSync	com.amazonaws。*region*.datasync
Amazon DataZone	com.amazonaws。*region*.datazone
AWS Deadline Cloud	com.amazonaws。*region*. 截止日期。管理
	com.amazonaws。*region*.deadline。日程安排
Amazon DevOps Guru	com.amazonaws。*region*.devops-guru
AWS Directory Service	com.amazonaws。*region*.ds
	com.amazonaws。*region*.ds-data
Amazon DocumentDB	com.amazonaws。*region*.rds
Amazon DynamoDB	com.amazonaws。*region*.dynamodb
	com.amazonaws。*region*.dynamodb-fips
亚马逊EBS直销 APIs	com.amazonaws。*region*.ebs
Amazon EC2	com.amazonaws。*region*.ec2
Amazon A EC2 uto Scaling	com.amazonaws。*region*. 自动缩放
EC2 映像生成器	com.amazonaws。*region*.imagebuilder
Amazon ECR	com.amazonaws。*region*.ecr.api

AWS 服务	服务名称
	com.amazonaws。*region*.ecr.dkr
Amazon ECS	com.amazonaws。*region*.ecs
	com.amazonaws。*region*.ecs-agent
	com.amazonaws。*region*.ecs-telemetry
Amazon EKS	com.amazonaws。*region*.eks
	com.amazonaws。*region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws。*region*.elasticbeanstalk
	com.amazonaws。*region*.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws。*region*.drs
Amazon Elastic File System	com.amazonaws。*region*.elastic 文件系统
	com.amazonaws。*region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws。*region*.elasticload bal
Amazon ElastiCache	com.amazonaws。*region*. elasticache
	com.amazonaws。*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws。*region*.mediaConnect
Amazon EMR	com.amazonaws。*region*.elasticmapreduc
Amazon EMR on EKS	com.amazonaws。*region*.emr-容器
Amazon EMR 无服务器	com.amazonaws。*region*.emr-serverless
	com.amazonaws。*region*。 emr-serverless-services.liv y
Amazon EMRWAL	com.amazonaws。*region*.emrwal.prod

AWS 服务	服务名称
AWS 最终用户消息社交	com.amazonaws。*region*. 社交消息
AWS Entity Resolution 数据匹配服务	com.amazonaws。*region*. 实体解决方案
Amazon EventBridge	com.amazonaws。*region*. 事件
	com.amazonaws。*region*.pipes
	com.amazonaws。*region*.pipes-data
	com.amazonaws。*region*.pipes-fips
	com.amazonaws。*region*.schemas
AWS Fault Injection Service	com.amazonaws。*region*.fis
Amazon FinSpace	com.amazonaws。*region*.finspace
	com.amazonaws。*region*.finspace api
Amazon Forecast	com.amazonaws。*region*. 预测
	com.amazonaws。*region*.forecastquer
	com.amazonaws。*region*.forecast-fips
	com.amazonaws。*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws。*region*. 欺诈探测器
Amazon FSx	com.amazonaws。*region*.fsx
	com.amazonaws。*region*.fsx-fips
AWS Glue	com.amazonaws。*region*. glue
	com.amazonaws。*region*.glue.dash
AWS Glue DataBrew	com.amazonaws。*region*.databrew

AWS 服务	服务名称
Amazon Managed Grafana	com.amazonaws。 *region*.grafana
	com.amazonaws。 *region*.grafana-工作区
AWS Ground Station	com.amazonaws。 *region*. 地面站
Amazon GuardDuty	com.amazonaws。 *region*.guardduty
	com.amazonaws。 *region*.guardduty-data
	com.amazonaws。 *region*。 guardduty-data-fips
	com.amazonaws。 *region*.guardduty-fips
AWS HealthImaging	com.amazonaws。 *region*。 dicom-medical-imaging
	com.amazonaws。 *region*. 医学影像
	com.amazonaws。 *region*。 runtime-medical-imaging
AWS HealthLake	com.amazonaws。 *region*.healthl
AWS HealthOmics	com.amazonaws。 *region*.analytics-omics
	com.amazonaws。 *region*。 control-storage-omics
	com.amazonaws。 *region*.storage-omics
	com.amazonaws。 *region*.tags-omics
	com.amazonaws。 *region*.workflows-omics
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAM身份中心	com.amazonaws。 *region*.identitystore
IAM Roles Anywhere	com.amazonaws。 *region*.rolesanwhere
Amazon Inspector	com.amazonaws。 *region*.inspector2

AWS 服务	服务名称
	com.amazonaws。 *region*.inspector-s
AWS IoT Core	com.amazonaws。 *region*.iot.data
	com.amazonaws。 *region*.iot.creditions
	com.amazonaws。 *region*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws。 *region*.deviceadvisor.iot
适用于 LoRaWAN 的 AWS IoT Core	com.amazonaws。 *region*.iotwireless.api
	com.amazonaws。 *region*.lorawan.cups
	com.amazonaws。 *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws。 *region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws。 *region*.greengrass
AWS IoT RoboRunner	com.amazonaws。 *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws。 *region*.iotsitewise.api
	com.amazonaws。 *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws。 *region*.iottwinmaker.api
	com.amazonaws。 *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws。 *region*.kendra
	aws.api。 *region*.kendra-ranking
AWS Key Management Service	com.amazonaws。 *region*.kms
	com.amazonaws。 *region*.kms-fips
Amazon Keyspaces (for Apache Cassandra)	com.amazonaws。 *region*. 卡桑德拉

AWS 服务	服务名称
	com.amazonaws。*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws。*region*.kinesis-streams
	com.amazonaws。*region*。 kinesis-streams-fips
AWS Lake Formation	com.amazonaws。*region*.lakefor
AWS Lambda	com.amazonaws。*region*.lambda
AWS Launch Wizard	com.amazonaws。*region*.launchWizard
Amazon Lex	com.amazonaws。*region*.models-v2-lex
	com.amazonaws。*region*.runtime-v2-lex
AWS License Manager	com.amazonaws。*region*. 许可证管理器
	com.amazonaws。*region*。 license-manager-fips
	com.amazonaws。*region*。 license-manager-linux-subscriptions
	com.amazonaws。*region*。 license-manager-linux-subscriptions-fips
	com.amazonaws。*region*。 license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws。*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws。*region*.lookoutmetric
Amazon Lookout for Vision	com.amazonaws。*region*.lookoutvision
Amazon Macie	com.amazonaws。*region*.macie2
AWS Mainframe Modernization	com.amazonaws。*region*.apptest

AWS 服务	服务名称
	com.amazonaws。*region*.m2
Amazon Managed Blockchain	com.amazonaws。*region*.managed区块链查询
	com.amazonaws。*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws。*region*.managedblockchain.bitcoin.testne
Amazon Managed Service for Prometheus	com.amazonaws。*region*.aps
	com.amazonaws。*region*.aps-workspaces
Amazon Managed Streaming for Apache Kafka	com.amazonaws。*region*.kafka
	com.amazonaws。*region*.kafka-fips
Amazon Managed Workflows for Apache Airflow	com.amazonaws。*region*.airflow.api
	com.amazonaws。*region*.airflow.api-fips
	com.amazonaws。*region*.airflow.env
	com.amazonaws。*region*.airflow.env-fips
	com.amazonaws。*region*.airflow.ops
AWS Management Console	com.amazonaws。*region*. 控制台
	com.amazonaws。*region*。登录
Amazon MemoryDB	com.amazonaws。*region*.memory-db
	com.amazonaws。*region*.memorydb-fips
AWS Migration Hub Orchestrator	com.amazonaws。*region*.migrationHub-Orchestrat
AWS Migration Hub Refactor Spaces	com.amazonaws。*region*.refactor-spaces

AWS 服务	服务名称
Migration Hub 策略建议	com.amazonaws。 *region*.migrationHub-strag
Amazon MQ	com.amazonaws。 *region*.mq
Amazon Neptune Analytics	com.amazonaws。 *region*.neptune-grap
	com.amazonaws。 *region*。 neptune-graph-data
	com.amazonaws。 *region*。 neptune-graph-fips
AWS Network Firewall	com.amazonaws。 *region*. 网络防火墙
	com.amazonaws。 *region*。 network-firewall-fips
亚马逊 OpenSearch 服务	这些端点由服务托管
AWS Organizations	com.amazonaws。 *region*. 组织
	com.amazonaws。 *region*.organs-fips
AWS Outposts	com.amazonaws。 *region*.outposts
AWS Panorama	com.amazonaws。 *region*. 全景
AWS 支付密码学	com.amazonaws。 *region*.payment-cryptograph
	com.amazonaws。 *region*.payment-cryptograph
AWS PCS	com.amazonaws。 *region*.pcs
	com.amazonaws。 *region*.pcs-fips
Amazon Personalize	com.amazonaws。 *region*. 个性化
	com.amazonaws。 *region*. 个性化活动
	com.amazonaws。 *region*.personalize 运行时
Amazon Pinpoint	com.amazonaws。 *region*。pinpoint

AWS 服务	服务名称
	com.amazonaws。 *region*。 pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws。 *region*.polly
AWS 价目表	com.amazonaws。 *region*.pricing.api
AWS 专用 5G	com.amazonaws。 *region*. 私有网络
AWS Private Certificate Authority	com.amazonaws。 *region*.acm-pca
	com.amazonaws。 *region*。 pca-connector-ad
	com.amazonaws。 *region*。 pca-connector-scep
AWS Proton	com.amazonaws。 *region*.proton
Amazon Q Business	aws.api。 *region*.qbusiness
Amazon Q 开发者版	com.amazonaws。 *region*.codewhisperer
	com.amazonaws。 *region*.q
	com.amazonaws。 *region*.qapps
Amazon Q 用户订阅	com.amazonaws。 *region*.service.user 订阅
Amazon QLDB	com.amazonaws。 *region*.qldb.session
Amazon QuickSight	com.amazonaws。 *region*.quicksight-网站
Amazon RDS	com.amazonaws。 *region*.rds
亚马逊RDS数据 API	com.amazonaws。 *region*.rds-data
Amazon Per RDS formance In	com.amazonaws。 *region*.pi
	com.amazonaws。 *region*.pi-fips
AWS re: Post 私密发布	com.amazonaws。 *region*.repostspace

AWS 服务	服务名称
回收站	com.amazonaws。 *region*.rbin
Amazon Redshift	com.amazonaws。 *region*.redshif
	com.amazonaws。 *region*.redshift-fips
	com.amazonaws。 *region*.redshift 无服务器
	com.amazonaws。 *region*。 redshift-serverless-fips
亚马逊 Redshift 数据 API	com.amazonaws。 *region*.redShift-data
	com.amazonaws。 *region*。 redshift-data-fips
Amazon Rekognition	com.amazonaws。 *region*. rekognition
	com.amazonaws。 *region*.rekognition-fips
	com.amazonaws。 *region*.streaming-rekognition
	com.amazonaws。 *region*。 streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws。 *region*.ram
AWS Resource Groups	com.amazonaws。 *region*. 资源组
	com.amazonaws。 *region*。 resource-groups-fips
AWS RoboMaker	com.amazonaws。 *region*.robomaker
Amazon S3	com.amazonaws。 *region*.s3
	com.amazonaws。 *region*.s3tables
Amazon S3 多区域访问点	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws。 *region*.s3-outposts
亚马逊 SageMaker AI	aws.sagemaker。 *region*. 实验

AWS 服务	服务名称
	aws.sagemaker。 *region*. 笔记本
	aws.sagemaker。 *region*.partner-app
	aws.sagemaker。 *region*. 工作室
	com.amazonaws。 *region*。 sagemaker-data-science-assistant
	com.amazonaws。 *region*.sagemaker.api
	com.amazonaws。 *region*.sagemaker.api-fips
	com.amazonaws。 *region*.sagemaker.featurestore-runtime
	com.amazonaws。 *region*.sagemaker.metrics
	com.amazonaws。 *region*.sagemaker.runtime
	com.amazonaws。 *region*.sagemaker.runtime-fips
节省计划	com.amazonaws。 *region*. 储蓄计划
AWS Secrets Manager	com.amazonaws。 *region*.secretsManag
AWS Security Hub	com.amazonaws。 *region*.securityh
AWS Security Token Service	com.amazonaws。 *region*.sts
AWS Serverless Application Repository	com.amazonaws。 *region*.serverless存储库
服务目录	com.amazonaws。 *region*.serviceCatalog
	com.amazonaws。 *region*.servicecatalog-appregistry
Amazon SES	com.amazonaws。 *region*.email-smtp

AWS 服务	服务名称
AWS SimSpace Weaver	com.amazonaws。*region*.simspaceweaver
AWS Snow Device Management	com.amazonaws。*region*。 snow-device-management
Amazon SNS	com.amazonaws。*region*.sns
Amazon SQS	com.amazonaws。*region*.sqs
Amazon SWF	com.amazonaws。*region*.swf
	com.amazonaws。*region*.swf-fips
AWS Step Functions	com.amazonaws。*region*. states
	com.amazonaws。*region*.sync-states
AWS Storage Gateway	com.amazonaws。*region*. storagegateway
AWS Supply Chain	com.amazonaws。*region*.scn
AWS Systems Manager	com.amazonaws。*region*.ec2messages
	com.amazonaws。*region*.ssm
	com.amazonaws。*region*.ssm-contacts
	com.amazonaws。*region*.ssm-事件
	com.amazonaws。*region*.ssm-quicksetup
	com.amazonaws。*region*.ssmmessages
AWS 电信网络生成器	com.amazonaws。*region*.tnb
Amazon Textract	com.amazonaws。*region*.extract
	com.amazonaws。*region*.textract-fips
Amazon Timestream	com.amazonaws。*region*.timestream.ingest-*cell*

AWS 服务	服务名称
	com.amazonaws。 *region*.timestream.query-*cell*
Amazon Timestream for InfluxDB	com.amazonaws。 *region*.timestream-influxdb
	com.amazonaws。 *region*。 timestream-influxdb-fips
Amazon Transcribe	com.amazonaws。 *region*. 转录
	com.amazonaws。 *region*.transcribe
Amazon Transcribe Medical	com.amazonaws。 *region*. 转录
	com.amazonaws。 *region*.transcribe
AWS Transfer for SFTP	com.amazonaws。 *region*. 转移
	com.amazonaws。 *region*.transfer.s
Amazon Translate	com.amazonaws。 *region*。翻译
AWS Trusted Advisor	com.amazonaws。 *region*. 值得信赖的顾问
Amazon Verified Permissions	com.amazonaws。 *region*. 已验证权限
Amazon VPC Lattice	com.amazonaws。 *region*.vpc-lattice
AWS Well-Architected Tool	com.amazonaws。 *region*.wellarchitected
Amazon WorkMail	com.amazonaws。 *region*.workmail
Amazon WorkSpaces	com.amazonaws。 *region*. 工作空间
Amazon 工作空间安全浏览器	com.amazonaws。 *region*.workspaces-Web
	com.amazonaws。 *region*。 workspaces-web-fips
Amazon WorkSpaces 瘦客户机	com.amazonaws。 *region*.thinclient.api
AWS X-Ray	com.amazonaws。 *region*.xray

查看可用的 AWS 服务 名字

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

以下示例显示了 AWS 服务 在指定区域中支持接口终端节点。该 --query 选项将输出限制为服务名称。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

下面是示例输出：

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

查看有关服务的信息

获得服务名称后，您可以使用describe-vpc-endpoint-services命令查看有关每个终端节点服务的详细信息。

以下示例显示有关指定区域中 Amazon CloudWatch 接口终端节点的信息。

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

下面是示例输出。VpcEndpointPolicySupported 表示是否支持端点策略。SupportedIpAddressTypes 表示支持哪些 IP 地址类型。

```
{
    "ServiceDetails": [
        {
```

```
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "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": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

查看端点策略支持

要验证服务是否支持终端节点策略，请调用describe-vpc-endpoint-services命令并检查的值VpcEndpointPolicySupported。可能的值为 true 和 false。

以下示例检查指定服务是否支持指定区域中的端点策略。--query 选项将输出限制为 VpcEndpointPolicySupported 的值。

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

下面是示例输出。

```
True
```

以下示例列出了 AWS 服务 在指定区域支持终端节点策略的。该 --query 选项将输出限制为服务名称。要使用 Windows 命令提示符运行此命令，请删除查询字符串周围的单引号，并将行连续字符从 \ 更改为 ^。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

下面是示例输出。

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

以下示例列出了 AWS 服务 在指定区域中不支持终端节点策略的。该 --query 选项将输出限制为服务名称。要使用 Windows 命令提示符运行此命令，请删除查询字符串周围的单引号，并将行连续字符从 \ 更改为 ^。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

下面是示例输出。

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
```

```
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

查看IPv6支持

您可以使用以下describe-vpc-endpoint-services命令查看 AWS 服务 在指定区域IPv6中可以访问的。该 `--query` 选项将输出限制为服务名称。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

下面是示例输出：

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
```

```
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
    "com.amazonaws.us-east-1.iotfleetwise",
    "com.amazonaws.us-east-1.kinesis-firehose",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.m2".
    "com.amazonaws.us-east-1.macie2".
    "com.amazonaws.us-east-1.networkflowmonitor".
    "com.amazonaws.us-east-1.networkflowmonitorreports".
    "com.amazonaws.us-east-1.pca-connector-scep",
    "com.amazonaws.us-east-1.pcs",
    "com.amazonaws.us-east-1.pcs-fips",
    "com.amazonaws.us-east-1.pi",
    "com.amazonaws.us-east-1.pi-fips",
    "com.amazonaws.us-east-1.polly",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.rbin",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.sagemaker.api",
    "com.amazonaws.us-east-1.securityhub",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.synthetics".
    "com.amazonaws.us-east-1.synthetics-fips".
    "com.amazonaws.us-east-1.textract",
    "com.amazonaws.us-east-1.textract-fips",
    "com.amazonaws.us-east-1.timestream-influxdb",
    "com.amazonaws.us-east-1.timestream-influxdb-fips",
    "com.amazonaws.us-east-1.trustedadvisor",
    "com.amazonaws.us-east-1.workmail",
    "com.amazonaws.us-east-1.xray"
```

```
]
```

AWS 服务 使用接口VPC终端节点访问一个

您可以创建接口VPC端点以连接到由其提供支持的服务 AWS PrivateLink，包括许多服务 AWS 服务。有关概述，请参阅 the section called “概念” 和 访问权限 AWS 服务。

对于您从中指定的每个子网VPC，我们在子网中创建一个终端节点网络接口，并为其分配一个子网地址范围内的私有 IP 地址。端点网络接口是由请求者管理的网络接口；您可以在您的 AWS 账户中查看，但无法自行管理。

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。

内容

- 前提条件
- 创建 VPC 终端节点
- 共享子网
- ICMP

前提条件

- 部署将访问您的 AWS 服务 中的的资源VPC。
- 要使用私有功能DNS，必须为自己VPC启用DNS主机名和DNS解析。有关更多信息，请参阅 Amazon VPC 用户指南中的查看和更新DNS属性。
- 要IPv6为接口终端节点启用， AWS 服务 必须支持通过访问IPv6。有关更多信息，请参阅 the section called “IP 地址类型”。
- 为终端节点网络接口创建一个安全组，允许来自您的资源的预期流量VPC。例如，为了确保 AWS CLI 可以向发送HTTPS请求 AWS 服务，安全组必须允许入站HTTPS流量。
- 如果您的资源位于带有网络的子网中ACL，请验证该网络是否ACL允许您的资源VPC和终端节点网络接口之间的流量。
- 您的 AWS PrivateLink 资源有配额。有关更多信息，请参阅 AWS PrivateLink 配额。

创建 VPC 终端节点

使用以下步骤创建连接到的接口VPC终端节点 AWS 服务。

为创建接口终端节点 AWS 服务

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 在 “类型” 中，选择AWS 服务。
5. 对于 Service name（服务名称），选择服务。有关更多信息，请参阅 the section called “与…集成的服务”。
6. 对于 VPC，请选择要VPC从中访问的 AWS 服务。
7. 如果您在步骤 5 中选择了 Amazon S3 的服务名称，并且要配置私有DNS支持，请选择其他设置，启用DNS名称。当您做出此选择时，它还会自动选择 “DNS仅为入站终端节点启用私有”。您只能为 Amazon S3 的接口终端节点配置DNS带有入站解析器终端节点的私有配置。如果您没有 Amazon S3 的网关终端节点，并且选择了DNS仅为入站终端节点启用私有，则在尝试此过程的最后一步时会收到错误消息。

   如果在步骤 5 中，您为除 Amazon S3 之外的任何服务选择了服务名称，则已选择其他设置，则已选择启用DNS名称。建议您保留默认值。这样可以确保使用公共服务终端节点的请求（例如通过的请求）解析到您的VPC终端节点。 AWS SDK
8. 对于子网，选择要在其中创建端点网络接口的子网。您可以为每个可用区选择一个子网。您无法从同一可用区中选择多个子网。有关更多信息，请参阅 the section called “子网和可用区”。

   默认情况下，我们选择子网 IP 地址范围中的 IP 地址，并将其分配给端点网络接口。要自己选择 IP 地址，请选择 “指定 IP 地址”。请注意，子网CIDR块中的前四个 IP 地址和最后一个 IP 地址保留供内部使用，因此您无法为终端节点网络接口指定它们。
9. 对于 IP address type（IP 地址类型），可从以下选项中进行选择：

   - IPv4— 为端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围并且服务接受IPv4请求时，才支持此选项。
   - IPv6— 为端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网并且服务接受IPv6IPv6请求时，才支持此选项。
   - Dualstack — 将IPv4和IPv6地址分配给端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围，并且服务同时接受IPv4和IPv6请求时，才支持此选项。
10. 对于 Security groups（安全组），选择要与端点网络接口关联的安全组。默认情况下，我们会为关联默认安全组VPC。

11. 对于策略，要允许所有委托人通过接口端点对所有资源进行所有操作，请选择完全访问权限。要限制访问权限，请选择自定义并输入策略。仅当服务支持VPC端点策略时，此选项才可用。有关更多信息，请参阅 端点策略。
12. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
13. 选择创建端点。

使用命令行创建接口端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

共享子网

您无法在与您共享的子网中创建、描述、修改或删除VPC终端节点。但是，您可以在与您共享的子网中使用VPC终端节点。

ICMP

接口端点不对 ping 请求做出响应。您可以使用 nc 或 nmap 命令来代替。

配置接口端点

创建接口VPC终端节点后，您可以更新其配置。

任务

- 添加或删除子网
- 关联安全组
- 编辑VPC终端节点策略
- 启用私有DNS名称
- 管理标签

添加或删除子网

您可以为接口端点的每个可用区选择一个子网。如果您要添加子网，我们会在您要添加的子网中创建端点网络接口，并为每个子网分配子网地址范围内的私有 IP 地址。如果您删除子网，我们会删除其端点网络接口。有关更多信息，请参阅 the section called “子网和可用区”。

使用控制台更改子网

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 依次选择 Actions（操作）、Manage subnets（管理子网）。
5. 根据需要选择或者取消选择可用区。对于每个可用区，选择一个子网。默认情况下，我们选择子网 IP 地址范围中的 IP 地址，并将其分配给端点网络接口。要为端点网络接口选择 IP 地址，请选择指定 IP 地址，然后输入子网IPv4地址范围中的一个地址。如果终端节点服务支持IPv6，您也可以输入子网IPv6地址范围中的地址。

   如果您为已有该终端节点的终端节点网络接口的子网指定 IP 地址，我们会用新的VPC终端节点网络接口替换该端点网络接口。此过程会暂时断开子网和VPC端点的连接。
6. 选择 Modify subnets（修改子网）。

使用命令行更改子网

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

关联安全组

您可以更改与您接口端点的网络接口相关联的安全组。安全组规则控制允许从您的资源进入终端节点网络接口的流量VPC。

使用控制台更改安全组

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 选择 Actions（操作）、Manage security groups（管理安全组）。
5. 根据需要选择或取消选择安全组。
6. 选择 Modify security groups（修改安全组）。

使用命令行更改安全组

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

编辑VPC终端节点策略

如果 AWS 服务 支持终端节点策略，则可以编辑终端节点的终端节点策略。在更新完端点策略后，您所做的更改可能需要几分钟才能生效。有关更多信息，请参阅 端点策略。

使用控制台更改端点策略

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 依次选择 Actions（操作）、Manage policy（管理策略）。
5. 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）并附加自定义策略。
6. 选择保存。

使用命令行更改端点策略

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

启用私有DNS名称

我们建议您为VPC终端节点启用私有DNS名称 AWS 服务。这样可以确保使用公共服务终端节点的请求（例如通过的请求）解析到您的VPC终端节点。 AWS SDK

要使用私有DNS名称，必须同时启用DNS主机名和DNS解析。VPC启用私有DNS名称后，私有 IP 地址可能需要几分钟才能变为可用。当您启用私有DNS名称时，我们创建的DNS记录是私有的。因此，私有DNS名称不可公开解析。

使用控制台更改私人DNS名称选项

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。

2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 选择操作，修改私人DNS名称。
5. 根据需要选择或清除 Enable for this endpoint（为此端点启用）。
6. 如果服务是 Amazon S3，则在上一步中为该终端节点选择 “启用” 也会选择 “DNS仅为入站终端节点启用私有”。如果您更喜欢标准私有DNS功能，请清除 “DNS仅为入站终端节点启用私有”。如果除了 Amazon S3 的接口终端节点之外，您没有用于 Amazon S3 的网关终端节点，并且您选择了DNS仅为入站终端节点启用私有功能，则在下一步中保存更改时会收到错误消息。有关更多信息，请参阅 the section called “私人 DNS”。
7. 选择 Save changes（保存更改）。

使用命令行更改私人DNS名称选项

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

管理标签

您可以对接口端点进行标记，以帮助您识别它或根据组织的需要对其进行分类。

使用控制台管理标签

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 依次选择 Actions（操作）、Manage tags（管理标签）。
5. 若要添加标签，请选择 Add new tag（添加新标签），然后输入标签的键和值。
6. 若要删除标签，请选择标签的键和值右侧的 Remove（删除）。
7. 选择 Save（保存）。

使用命令行管理标签

- create-tags 和 delete-tags (AWS CLI)
- New-EC2Tag和 Remove-EC2Tag（适用于 Windows 的工具 PowerShell）

接收接口端点事件的提醒

您可以创建通知以接收与接口端点相关的特定事件的提醒。例如，您可以在连接请求被接受或拒绝时收到电子邮件。

任务

- 创建SNS通知
- 添加访问策略
- 添加密钥策略

创建SNS通知

使用以下步骤为通知创建 Amazon SNS 主题并订阅该主题。

使用控制台为接口端点创建通知

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 在 Notifications（通知）选项卡上，选择 Create notofication（创建通知）。
5. 在 “通知” 中ARN，选择与您创建ARN的SNS主题对应的。
6. 要订阅事件，请从 Events（事件）中选择。
   - Connect（连接）– 服务使用者创建了接口端点。这会向服务提供商发送连接请求。
   - Accept（接受）– 服务提供商接受了连接请求。
   - Reject（拒绝）– 服务提供商拒绝了连接请求。
   - Delete（删除）– 服务使用者删除了接口端点。
7. 选择 Create notification（创建通知）。

使用命令行为接口端点创建通知

- create-vpc-endpoint-connection-通知 ()AWS CLI
- New-EC2VpcEndpointConnectionNotification（适用于 Windows 的工具 PowerShell）

添加访问策略

向 Amazon SNS 主题添加访问策略， AWS PrivateLink 允许您代表您发布通知，如下所示。有关更多信息，请参阅如何编辑我的 Amazon SNS 主题的访问策略？ 使用 `aws:SourceArn` 或 `aws:SourceAccount` 全局条件键来防止混淆代理人问题。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

添加密钥策略

如果您使用的是加密SNS主题，则KMS密钥的资源策略必须信任 AWS PrivateLink 才能调用 AWS KMS API操作。以下是示例密钥策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
```

```
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

删除接口端点

使用完VPC终端节点后，可以将其删除。删除接口端点还将删除其端点网络接口。

使用控制台删除接口端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

使用命令行删除接口端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

网关端点

网关VPC终端节点可提供与 Amazon S3 和 DynamoDB 的可靠连接，您无需互联网网关或设备 NAT。VPC与其他类型的终端节点不同 AWS PrivateLink，网关VPC终端节点不使用。

Amazon S3 和 DynamoDB 同时支持网关端点和接口端点。有关各选项的比较，请参阅以下内容：

- Amazon S3 的VPC终端节点类型
- 亚马逊 DynamoDB 的VPC终端节点类型

定价

使用网关端点不会发生任何额外费用。

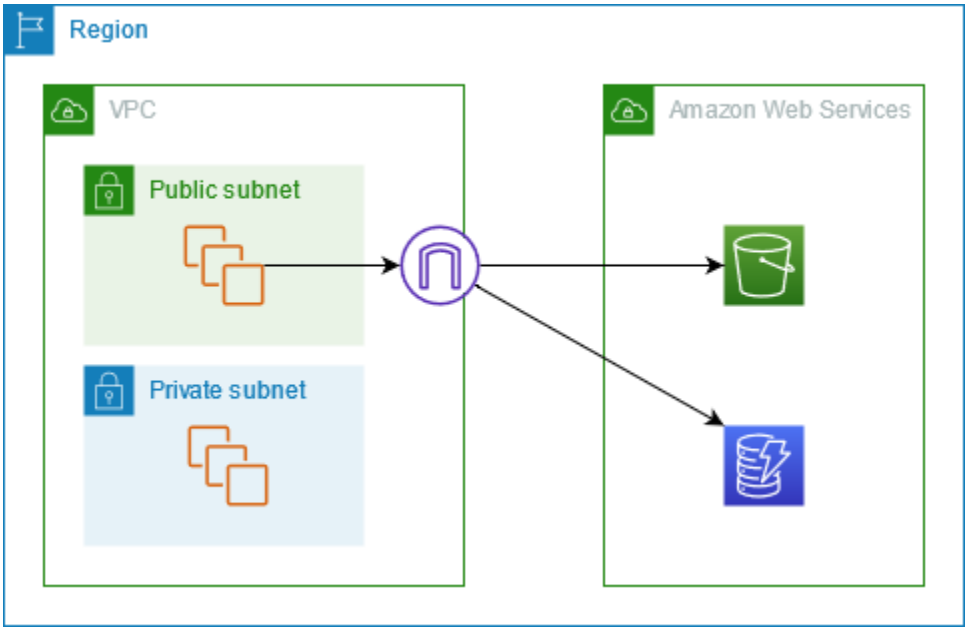
内容

概述

您可以通过 Amazon S3 和 DynamoDB 的公有服务端点或网关端点访问。本概述比较了这些方法。

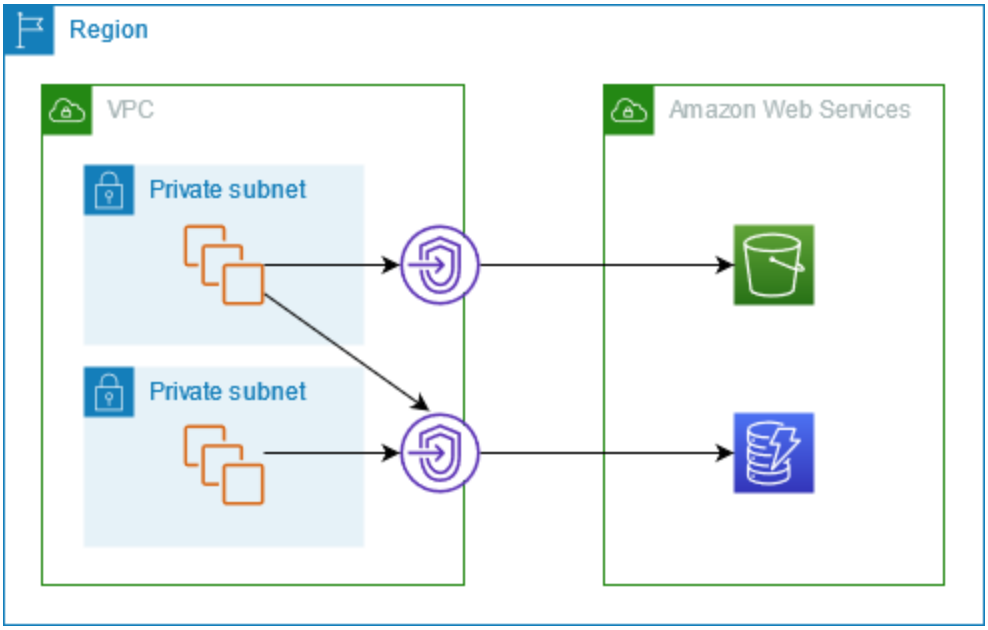
通过互联网网关访问

下图显示了实例如何通过其公有服务端点访问 Amazon S3 和 DynamoDB。从公有子网中的实例到 Amazon S3 或 DynamoDB 的流量将路由到该服务的互联网网关，然后再路由到VPC该服务。私有子网中的实例无法向 Amazon S3 或 DynamoDB 发送流量，因为根据定义，私有子网没有通往互联网网关的路由。要使私有子网中的实例能够向 Amazon S3 或 DynamoDB 发送流量，您需要向公有子网添加NAT一台设备，并将私有子网中的流量路由到该设备。NAT当流向 Amazon S3 或 DynamoDB 的流量通过互联网网关时，它不会离开网络。 AWS



通过网关端点进行访问

下图显示了实例如何通过网关端点访问 Amazon S3 和 DynamoDB。从您VPC到 Amazon S3 或 DynamoDB 的流量将路由到网关终端节点。每个子网路由表都必须有一条路由，该路由使用服务的前缀列表将以服务为目的地的流量发送到网关端点。有关更多信息，请参阅《Amazon VPC 用户指南》中的AWS托管前缀列表。



路由

创建网关终端节点时，您需要为启用的子网选择VPC路由表。以下路由将自动添加到您选择的各个路由表。目的地是所拥有服务的前缀列表 AWS ，目标是网关终端节点。

目标位置	目标
prefix_list_id	*gateway_endpoint_id*

注意事项

- 您可以查看我们添加到您的路由表中的端点路由，但不能修改或删除它们。要向路由表添加端点路由，请将其与网关端点关联。当您取消路由表与网关端点的关联或删除网关端点时，我们会删除端点路由。
- 与网关端点关联的路由表关联的子网中的所有实例会自动使用该网关端点来访问该服务。未与这些路由表关联的子网中的实例使用公有服务端点，而不是网关端点。
- 路由表既可以有通往 Amazon S3 的端点路由，也可以有通往 DynamoDB 的端点路由。您可以在多个路由表中拥有通往同一服务（Amazon S3 或 DynamoDB）的端点路由。您不能在一个路由表中拥有通往同一服务（Amazon S3 或 DynamoDB）的多个端点路由。
- 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)。对于带有端点路由的路由表，这意味着以下内容：
  - 如果存在一条向互联网网关发送所有互联网流量 (0.0.0.0/0) 的路由，端点路由优先于以当前区域中的服务（Amazon S3 或 DynamoDB）为目的地的流量。发往不同地点的流量 AWS 服务 使用互联网网关。
  - 以不同区域的服务（Amazon S3 或 DynamoDB）为目的地的流量会流向互联网网关，因为前缀列表特定于某个区域。
  - 如果在同一区域中存在为服务（Amazon S3 或 DynamoDB）指定确切 IP 地址范围的路由，则该路由优先于端点路由。

安全性

当您的实例通过网关端点访问 Amazon S3 或 DynamoDB 时，它们会使用其公有端点访问服务。这些实例的安全组必须允许进出服务的流量。以下是出站规则的示例。它引用服务的前缀列表的 ID。

目标位置	协议	端口范围
prefix_list_id	TCP	443

这些实例ACLs的子网网络还必须允许进出服务的流量。以下是出站规则的示例。您不能在网络ACL规则中引用前缀列表，但可以从其前缀列表中获取服务的 IP 地址范围。

目标位置	协议	端口范围
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

适用于 Amazon S3 的网关端点

您可以使用网关终端节点从自己的VPC网关VPC终端节点访问 Amazon S3。创建网关终端节点后，您可以将其添加为路由表中的目标，用于接收从您VPC到 Amazon S3 的流量。

使用网关端点不会发生任何额外费用。

Amazon S3 同时支持网关端点和接口端点。使用网关终端节点，您可以从您的访问Amazon S3VPC，无需互联网网关或NAT设备VPC，也无需支付额外费用。但是，网关终端节点不允许从本地网络、其他 AWS 区域的对VPCs等设备或通过传输网关进行访问。对于这些场景，您必须使用接口端点，后者需要额外付费。有关更多信息，请参阅 Amazon S3 用户指南中的 Amazon S 3 VPC 终端节点类型。

内容

注意事项

- 网关端点仅在您创建该端点所在的区域可用。请务必在您的 S3 存储桶所在的区域内创建网关端点。
- 如果您使用的是 Amazon DNS 服务器，则必须同时启用DNS主机名和DNS解析。VPC如果您使用的是自己的DNS服务器，请确保向 Amazon S3 发出的请求正确解析为由维护的 IP 地址 AWS。
- 对于通过网关端点访问 Amazon S3 的实例，安全组的出站规则必须允许进出 Amazon S3 的流量。您可以在安全组规则中引用 Amazon S3 的前缀列表的 ID。
- 通过网ACL关终端节点访问 Amazon S3 的实例的子网网络必须允许进出 Amazon S3 的流量。您不能在网络ACL规则中引用前缀列表，但可以从 Amazon S3 的前缀列表中获取 Amazon S3 的 IP 地址范围。
- 检查您使用的是否需要访问 S3 存储桶。 AWS 服务 例如，某项服务可能需要访问包含日志文件的存储桶，或者可能需要您将驱动程序或代理下载到您的EC2实例。如果是，请确保您的终端节点策略允许 AWS 服务 或资源使用`s3:GetObject`操作访问这些存储桶。
- 对于通过VPC终端节点向 Amazon S3 发出的请求，您不能在身份策略或存储桶策略中使用该`aws:SourceIp`条件。改为使用 `aws:VpcSourceIp` 条件。或者，您可以使用路由表来控制哪些EC2实例可以通过VPC终端节点访问 Amazon S3。
- 网关端点仅支持IPv4流量。
- Amazon S3 收到的来自受影响子网中实例的源IPv4地址从公有IPv4地址更改为您的VPC私有IPv4地址。端点交换网络路由，断开已打开的TCP连接。之前使用公共IPv4地址的连接不会恢复。建议您在创建或修改端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。
- 端点连接无法扩展到外部VPC。您的连接、对等VPN连接、VPC传输网关或 AWS Direct Connect 连接另一端的资源VPC不能使用网关终端节点与 Amazon S3 通信。
- 您的账户的默认配额为每个区域 20 个网关端点，该配额可调整。每个网关终端节点也限制为 255 个 VPC。

私人 DNS

在为 Amazon S3 创建网关终端节点和接口终端节点时，您可以配置私DNS有以优化成本。

Route 53 Resolver

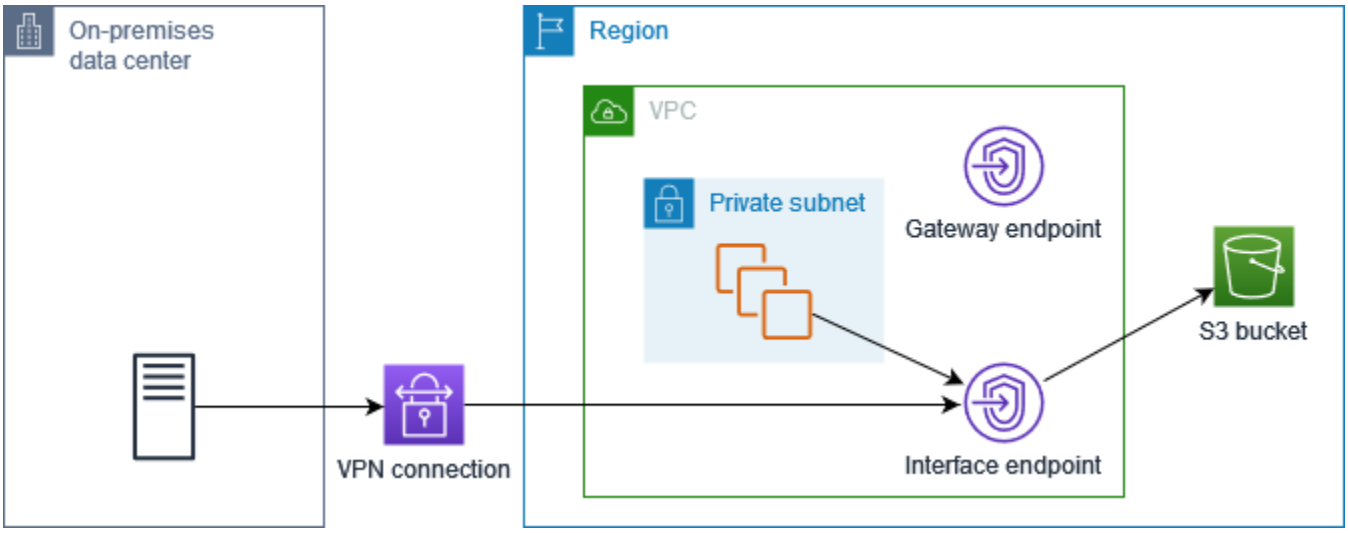
Amazon 为您提供了一个名为 R oute 53 Resolver VPC 的DNS服务器。Route 53 解析器会自动解析私有托管区域中的本地VPC域名和记录。但是，你不能从外部使用 Route 53 Resolver。VPCRoute 53 提供解析器端点和解析器规则，因此您可以从外部使用 Route 53 解析器。VPC入站解析器端点将来自本

地网络的DNS查询转发到 Route 53 解析器。出站解析器端点将来自 Route 53 解析器的DNS查询转发到本地网络。

当您将 Amazon S3 的接口终端节点配置为DNS仅对入站解析器终端节点使用私有时，我们会创建一个入站解析器终端节点。入站解析器终端节点将本地对 Amazon S3 的DNS查询解析到接口终端节点的私有 IP 地址。我们还将 ALIAS Route 53 解析器的记录添加到 Amazon S3 的公共托管区域，以便您的DNS查询解VPC析到 Amazon S3 公有 IP 地址，该地址将流量路由到网关终端节点。

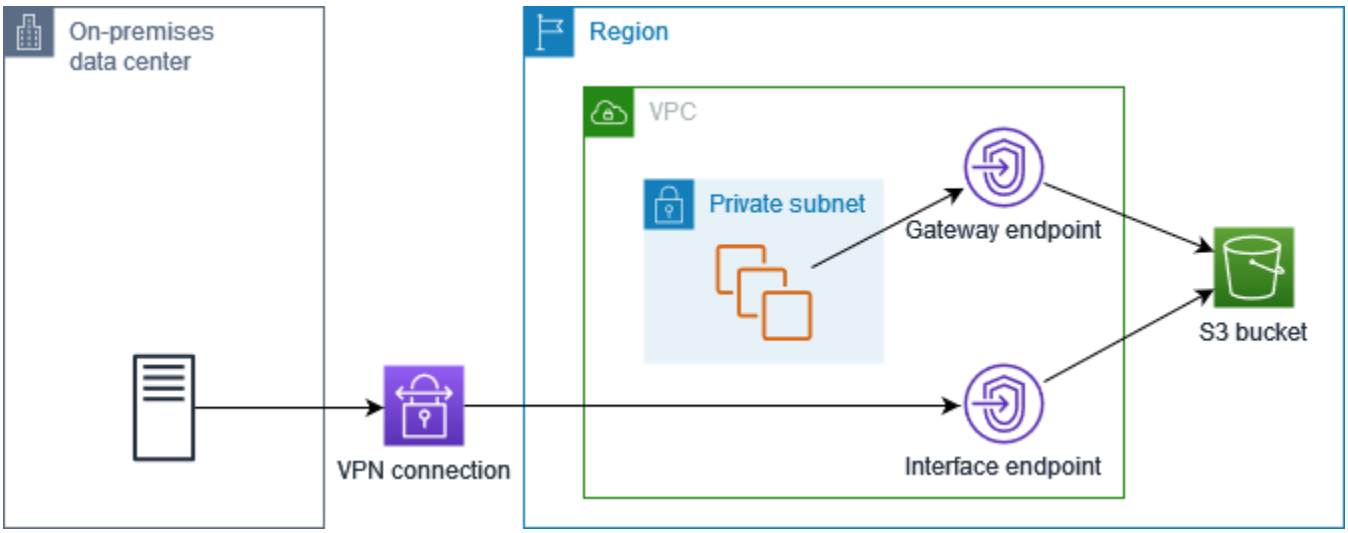
私人 DNS

如果您为 Amazon S3 DNS 的接口终端节点配置私有，但没有DNS仅为入站 Resolver 终端节点配置私有，则来自本地网络和您的本地网络的请求都将VPC使用该接口终端节点访问 Amazon S3。因此，您需要付费使用接口终端节点来处理来自的流量VPC，而不是使用网关终端节点，无需支付额外费用。



DNS仅限入站 Resolver 终端节点的私有

如果您DNS仅为入站 Resolver 终端节点配置私有，则来自本地网络的请求将使用接口终端节点访问 Amazon S3，而您的请求则VPC使用网关终端节点访问 Amazon S3。因此，您可以优化成本，因为您只需为无法使用网关端点的流量，付费使用接口端点。



配置私有 DNS

您可以在创建 Amazon S3 接口终端节点时或在创建接口终端节点之后为其配置私DNS有配置。有关更多信息，请参阅 the section called “创建 VPC 终端节点”（创建期间配置）或 the section called “启用私有DNS名称”（创建后配置）。

创建网关端点

使用以下过程创建连接到 Amazon S3 的网关端点。

使用控制台创建网关端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 对于 Service category（服务类别），选择 AWS 服务。
5. 对于服务，添加过滤器 “类型 = 网关”，然后选择 com. amazonaws。 *region*.s3。
6. 对于 VPC，选择要VPC在其中创建端点的。
7. 对于 Route tables（路由表），选择端点要使用的路由表。我们将自动添加一个路由，将以服务为目的地的流量指向端点网络接口。
8. 对于策略，选择完全访问权限以允许所有委托人通过VPC端点对所有资源进行所有操作。否则，请选择自定义以附加VPC终端节点策略，该策略控制委托人通过终VPC端节点对资源执行操作所拥有的权限。
9. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。

10. 选择创建端点。

使用命令行创建网关端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

使用存储桶策略控制访问

您可以使用存储桶策略来控制从特定终端节点、VPCs、IP 地址范围和 AWS 账户对存储桶的访问。这些示例假设还有一个允许您的使用案例所需访问权限的策略语句。

Example 示例：限制对特定端点的访问

您可以使用 aws: sourceVpce 条件密钥创建限制对特定终端节点的访问的存储桶策略。除非使用了指定的网关端点，否则以下策略会使用指定的操作拒绝对指定桶的访问。请注意，此策略通过 AWS Management Console使用指定的操作阻止对指定桶的访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example 示例：将访问权限限制为特定的 VPC

您可以使用 aws: sourceVpc condition 密钥创建限制访问特定VPCs存储桶策略。如果您在同一个端点中配置了多个端点，则此功能非常有用VPC。除非请求来自指定的，否则以下策略拒绝使用指定操作

访问指定存储桶VPC。请注意，此策略通过 AWS Management Console使用指定的操作阻止对指定桶的访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "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 条件密钥创建限制对特定 IP 地址范围的访问的策略。除非请求来自指定的 IP 地址，否则以下策略会使用指定的操作拒绝对指定桶的访问。请注意，此策略通过 AWS Management Console使用指定的操作阻止对指定桶的访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
```

```
    }
  ]
}
```

Example 示例：限制对特定存储桶的访问权限 AWS 账户

您可以使用 `s3:ResourceAccount` 条件键来创建策略，用于限制对特定 AWS 账户 中 S3 存储桶的访问。除非 S3 桶归指定的 AWS 账户所有，否则以下策略会使用指定的操作拒绝对这些桶的访问。

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

关联路由表

您可以更改与网关端点关联的路由表。当您关联路由表时，我们将自动添加一个路由，将以服务为目的地的流量指向端点网络接口。当您取消关联路由表时，我们会自动从路由表中删除端点路由。

使用控制台关联路由表

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择 Actions、Manage route tables。
5. 根据需要选择或取消选择路由表。
6. 选择 Modify route tables（修改路由表）。

使用命令行关联路由表

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

编辑VPC终端节点策略

您可以编辑网关终端节点的终端节点策略，该策略控制VPC通过终端节点访问 Amazon S3。默认策略允许完全访问。有关更多信息，请参阅 端点策略。

使用控制台更改端点策略

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 依次选择 Actions（操作）、Manage policy（管理策略）。
5. 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）并附加自定义策略。
6. 选择保存。

下面是访问 Amazon S3 的端点策略示例。

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。如果您的存储桶 AWS 服务 中有其他使用 S3 存储桶VPC，则此功能非常有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
```

```
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example 示例：限制对特定IAM角色的访问权限

您可以创建限制特定IAM角色访问权限的策略。必须使用 aws:PrincipalArn 向主体授予访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example 示例：限制对特定账户中用户的访问

您可以创建限制对特定账户的访问权限的策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

删除网关端点

用完网关端点后可以将其删除。当您删除网关端点时，我们会从子网路由表中删除端点路由。

如果启用了私DNS有网关终端节点，则无法删除网关终端节点。

使用控制台删除网关端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

使用命令行删除网关端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

适用于 Amazon DynamoDB 的网关端点

您可以使用网关终端节点访问亚马逊 DynamoDB。VPC VPC创建网关终端节点后，您可以将其添加为路由表中的目标，用于接收从您VPC到 DynamoDB 的流量。

使用网关端点不会发生任何额外费用。

DynamoDB 同时支持网关端点和接口端点。使用网关终端节点，您可以从VPC自己访问 DynamoDB，无需互联网网关NAT或设备，也无需VPC支付额外费用。但是，网关终端节点不允许从本地网络、其

他 AWS 区域的对VPCs等设备或通过传输网关进行访问。对于这些场景，您必须使用接口端点，后者需要额外付费。有关更多信息，请参阅亚马逊 DynamoD B VPC 开发者指南中的 DynamoDB 终端节点类型。

内容

注意事项

- 网关端点仅在您创建该端点所在的区域可用。确保在 DynamoDB 表所在的相同区域内创建网关端点。
- 如果您使用的是 Amazon DNS 服务器，则必须同时启用DNS主机名和DNS解析。VPC如果您使用的是自己的DNS服务器，请确保向 DynamoDB 发出的请求正确解析到由维护的 IP 地址。 AWS
- 对于通过网关端点访问 DynamoDB 的实例，安全组的规则必须允许进出 DynamoDB 的流量。您可以在安全组规则中引用 DynamoDB 的前缀列表的 ID。
- 通过网ACL关终端节点访问 DynamoDB 的实例的子网网络必须允许进出 DynamoDB 的流量。您不能在网络ACL规则中引用前缀列表，但可以从 DynamoDB 的前缀列表中获取 DynamoDB 的 IP 地址范围。
- 如果您使用 AWS CloudTrail 记录 DynamoDB 操作，则日志文件包含服务使用VPC者中实例的EC2私有 IP 地址以及通过终端节点执行的任何请求的网关终端节点的 ID。
- 网关端点仅支持IPv4流量。
- 来自受影响子网中实例的源IPv4地址从您的公有IPv4地址更改为私有IPv4地址。VPC端点切换网络路由并断开已打开的TCP连接。之前使用公共IPv4地址的连接不会恢复。建议您在创建或修改网关端点时不要运行任何重要任务。或者，进行测试以确保在连接中断时您的软件能够自动重新连接到DynamoDB。
- 端点连接无法扩展到外部VPC。您的连接、对等VPN连接、VPC传输网关或 AWS Direct Connect 连接另一端的资源VPC无法使用网关终端节点与 DynamoDB 通信。
- 您的账户的默认配额为每个区域 20 个网关端点，该配额可调整。每个网关终端节点也限制为 255 个VPC。

创建网关端点

使用以下过程创建连接到 DynamoDB 的网关端点。

使用控制台创建网关端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 对于 Service category（服务类别），选择 AWS 服务。
5. 对于服务，添加过滤器 “类型 = 网关”，然后选择 com. amazonaws。 *region*.dynamodb。
6. 对于 VPC，选择要VPC在其中创建端点的。
7. 对于 Route tables（路由表），选择端点要使用的路由表。我们将自动添加一个路由，将以服务为目的地的流量指向端点网络接口。
8. 对于策略，选择完全访问权限以允许所有委托人通过VPC端点对所有资源进行所有操作。否则，请选择自定义以附加VPC终端节点策略，该策略控制委托人通过终VPC端节点对资源执行操作所拥有的权限。
9. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
10. 选择创建端点。

使用命令行创建网关端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

使用IAM策略控制访问权限

您可以创建IAM策略来控制哪些IAM委托人可以使用特定终端节点访问 DynamoDB 表。VPC

Example 示例：限制对特定端点的访问

您可以使用 aws: sourceVpce 条件密钥创建限制对特定VPC终端节点的访问的策略。除非使用VPC指定的终端节点，否则以下策略将拒绝访问账户中的 DynamoDB 表。此示例假设还有一个允许您的使用案例所需访问权限的策略语句。

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example 示例：允许特定IAM角色进行访问

您可以创建允许使用特定IAM角色进行访问的策略。以下策略授予对指定IAM角色的访问权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
      }
   ]
}
```

Example 示例：允许来自特定账户的访问

您可以创建一个仅允许来自特定账户的访问的策略。以下策略向指定账户中的用户授予访问权限。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
       {
          "Sid": "Allow-access-from-account",
          "Effect": "Allow",
          "Principal": "*",
          "Action": "*",
          "Resource": "*",
          "Condition": {
             "StringEquals": {
                "aws:PrincipalAccount": "111122223333"
             }
          }
       }
    ]
}
```

关联路由表

您可以更改与网关端点关联的路由表。当您关联路由表时，我们将自动添加一个路由，将以服务为目的地的流量指向端点网络接口。当您取消关联路由表时，我们会自动从路由表中删除端点路由。

使用控制台关联路由表

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择 Actions、Manage route tables。
5. 根据需要选择或取消选择路由表。
6. 选择 Modify route tables（修改路由表）。

使用命令行关联路由表

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

编辑VPC终端节点策略

您可以编辑网关终端节点的终端节点策略，该策略控制通过终端节点对 DynamoDB VPC 的访问。默认策略允许完全访问。有关更多信息，请参阅 端点策略。

使用控制台更改端点策略

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 依次选择 Actions（操作）、Manage policy（管理策略）。
5. 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）并附加自定义策略。
6. 选择保存。

使用命令行修改网关端点

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

下面是访问 DynamoDB 的端点策略示例。

Example 示例：允许只读访问

您可以创建一个将访问限制为只读访问的策略。以下策略授予列出和描述 DynamoDB 表的权限。

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "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。以下策略允许对指定 DynamoDB 表的访问。

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

删除网关端点

用完网关端点后可以将其删除。当您删除网关端点时，我们会从子网路由表中删除端点路由。

使用控制台删除网关端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

使用命令行删除网关端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

通过以下方式访问 SaaS 产品 AWS PrivateLink

使用 AWS PrivateLink，您可以私下访问 SaaS 产品，就好像它们是自己运行一样VPC。

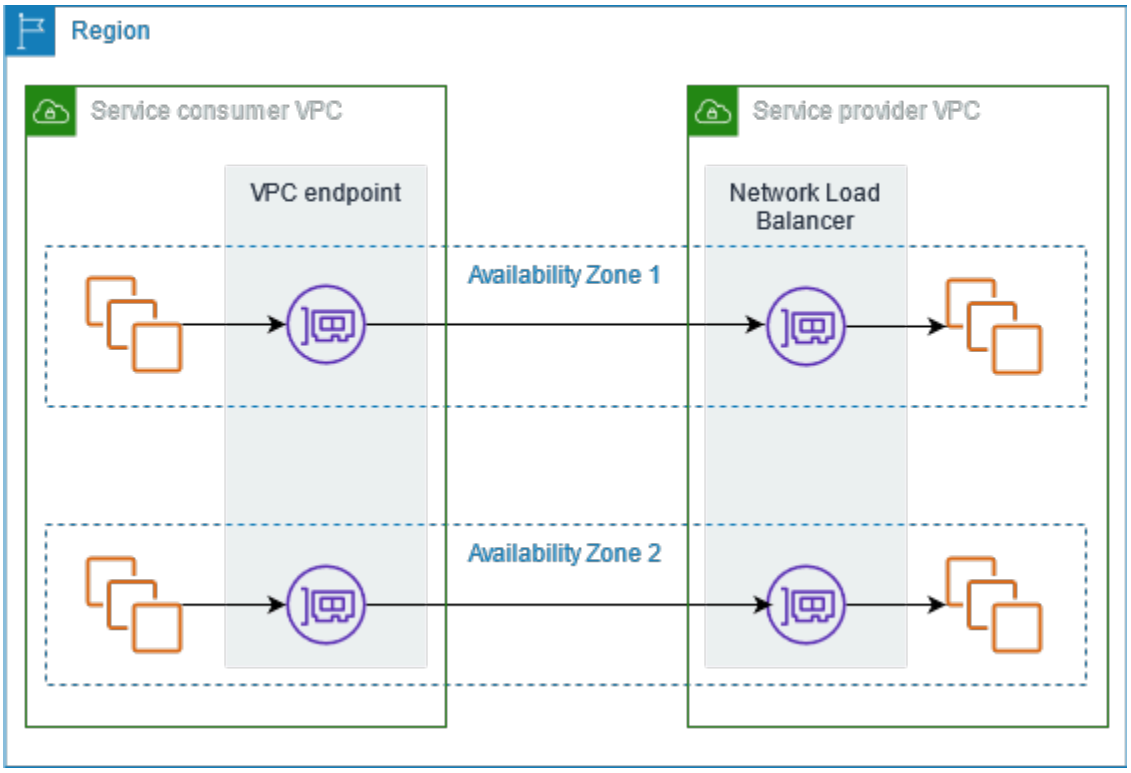
内容

概述

您可以发现、购买和配置由 AWS PrivateLink 直通提供支持的 SaaS 产品 AWS Marketplace。有关更多信息，请参阅使用安全私密地访问 SaaS 应用程序 AWS PrivateLink。

您还可以找到由 AWS PrivateLink AWS 合作伙伴提供支持的 SaaS 产品。有关更多信息，请参阅 AWS PrivateLink 合作伙伴。

下图显示了如何使用VPC端点连接到 SaaS 产品。服务提供商创建端点服务并向其客户授予端点服务的访问权限。作为服务使用者，您可以创建一个接口VPC终端节点，用于在您的VPC和终端节点服务中的一个或多个子网之间建立连接。



创建接口端点

使用以下步骤创建连接到 SaaS 产品的接口VPC终端节点。

要求

订阅服务。

创建连接到合作伙伴服务的接口端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 如果您是从购买服务的 AWS Marketplace，请执行以下操作：
    a. 在 “类型” 中，选择AWS Marketplace 服务。
    b. 选择服务。
5. 如果您订阅了标识为 “服务就绪” 的 AWS 服务，请执行以下操作：
    a. 在 “类型” 中，选择 “PrivateLink Ready 合作伙伴服务”。
    b. 输入服务的名称，然后选择验证服务。
6. 对于 VPC，请选择要VPC从中访问产品的。
7. 对于子网，选择要在其中创建端点网络接口的子网。
8. 对于 Security groups（安全组），选择要与端点网络接口关联的安全组。安全组规则必须允许端点网络接口中的资源VPC和端点网络接口之间的流量。
9. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
10. 选择创建端点。

配置接口端点

有关配置接口端点的信息，请参阅 the section called “配置接口端点”。

通过以下方式访问虚拟设备 AWS PrivateLink

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。您可以在创建VPC终端节点服务时指定 Gateway Load Balancer。其他 AWS 主体通过创建网关负载均衡器端点访问端点服务。

定价

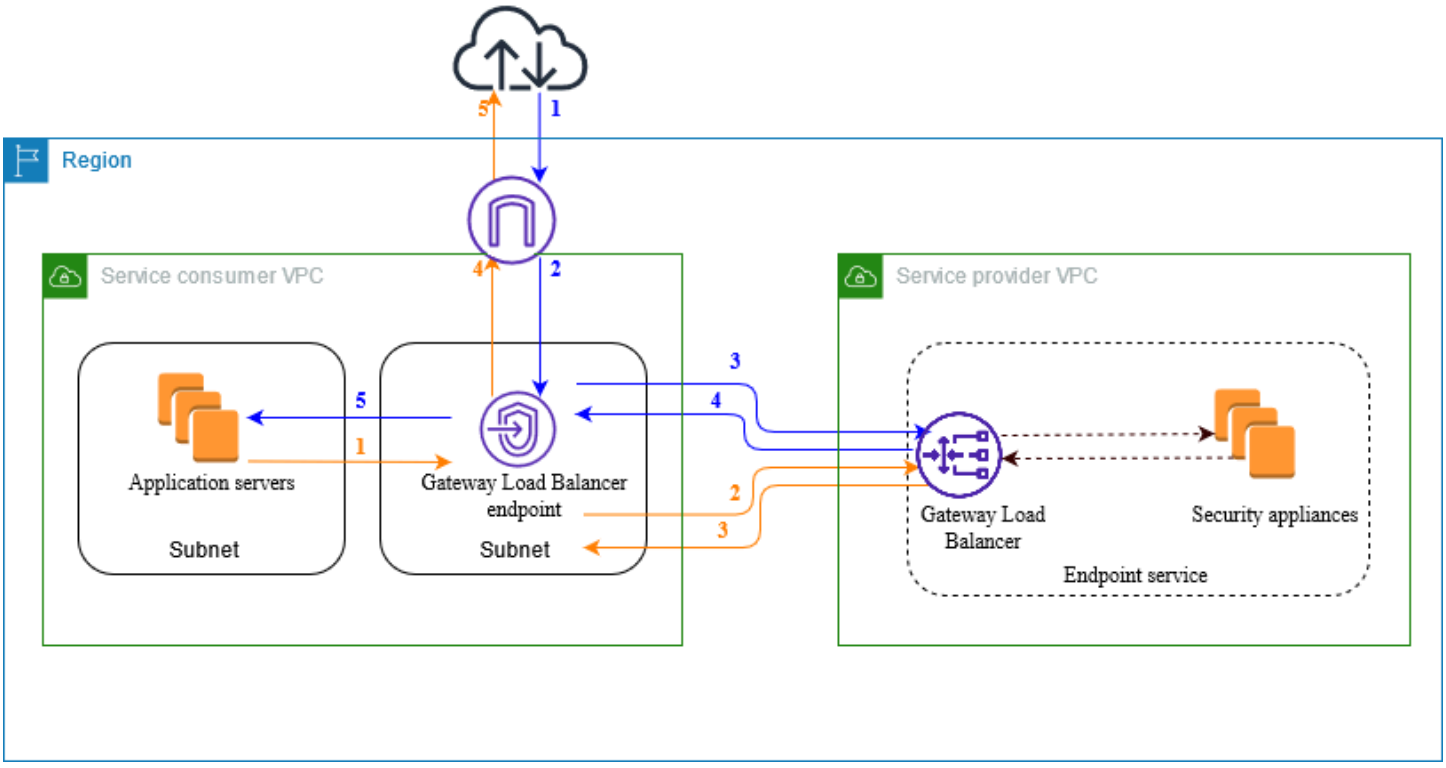
按照您的网关负载均衡器端点在每个可用区预置的每一小时向您收取费用。此外，您还需按照处理的数据 GB 付费。有关更多信息，请参阅AWS PrivateLink 定价。

内容

有关更多信息，请参阅网关负载均衡器。

概述

下图显示了应用程序服务器如何通过访问安全设备 AWS PrivateLink。应用程序服务器在服务使用者的子网中运行VPC。您在另一个子网中创建 Gateway Load Balancer 终端节点VPC。所有VPC通过 Internet 网关进入服务使用者的流量首先路由到 Gateway Load Balancer 端点进行检查，然后路由到目标子网。同样，离开应用程序服务器的所有流量会被路由到网关负载均衡器端点以进行检查，然后通过互联网网关被路由回应用程序服务器。



从互联网到应用程序服务器的流量（蓝色箭头）：

1. 流量VPC通过互联网网关进入服务消费者。
2. 根据路由表配置，将流量发送到网关负载均衡器端点。
3. 通过安全设备，将流量发送到网关负载均衡器以进行检查。
4. 检查完成后，将流量发送回网关负载均衡器端点。
5. 根据路由表配置，将流量发送到应用程序服务器。

从应用程序服务器到互联网的流量（橙色箭头）：

1. 根据路由表配置，将流量发送到网关负载均衡器端点。
2. 通过安全设备，将流量发送到网关负载均衡器以进行检查。
3. 检查完成后，将流量发送回网关负载均衡器端点。
4. 根据路由表配置，将流量发送到互联网网关。
5. 流量被路由回互联网。

IP 地址类型

服务提供商可以通过IPv4、IPv6或两IPv4者兼而有之地将其服务端点提供给服务使用者IPv6，即使他们的安全设备仅支持IPv4。如果您启用双栈支持，则现有消费者可以继续使用IPv4来访问您的服务，而新的消费者可以选择使用IPv6来访问您的服务。

如果 Gateway Load Balancer 端点支持IPv4，则端点网络接口具有IPv4地址。如果 Gateway Load Balancer 端点支持IPv6，则端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。如果您使用IPv6地址描述端点网络接口，请注意该接口已启`denyAllIgwTraffic`用。

IPv6为终端节点服务启用的要求

- 终端节点服务的VPC和子网必须有关联的IPv6CIDR块。
- 端点服务的所有网关负载均衡器必须使用双堆栈 IP 地址类型。安全设备不需要支持IPv6流量。

为 Gateway L IPv6 oad Balancer 终端节点启用的要求

- 终端节点服务的 IP 地址类型必须包含IPv6支持。
- 网关负载均衡器端点的 IP 地址类型必须与网关负载均衡器端点的子网兼容，如下所述：
  - IPv4— 为您的端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围时，才支持此选项。
  - IPv6— 为您的端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网时，IPv6才支持此选项。
  - Dualstack — 将IPv4和IPv6地址分配给您的端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围时，才支持此选项。
- 服务使用者中子网的路由表VPC必须路由IPv6流量，并且这些子网ACLs的网络必须允许IPv6流量。

路由

若要将流量路由到端点服务，请使用其 ID 将网关负载均衡器端点指定为路由表中的目标。在上图中，将路由添加到路由表，如下所示。请注意，双栈配置中包含IPv6路由。

互联网网关的路由表

此路由表必须具有将发往应用程序服务器的流量发送到网关负载均衡器端点的路由。

目标位置	目标
VPC IPv4 CIDR	本地
VPC IPv6 CIDR	本地
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

包含应用程序服务器的子网的路由表

此路由表必须具有将来自应用程序服务器的所有流量发送到网关负载均衡器端点的路由。

目标位置	目标
VPC IPv4 CIDR	本地
VPC IPv6 CIDR	本地
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

包含网关负载均衡器端点的子网的路由表

此路由表必须将从检查返回的流量发送到最终目标位置。如果流量来自互联网，本地路由会将流量发送到应用程序服务器。如果流量来自应用程序服务器，则添加将所有流量发送到互联网网关的路由。

目标位置	目标
VPC IPv4 CIDR	本地
VPC IPv6 CIDR	本地
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

创建检查系统作为网关负载均衡器端点服务

您可以创建自己的由提供支持的服务 AWS PrivateLink，称为终端节点服务。您是服务提供商，而与您的服务建立连接的 AWS 委托人是服务使用者。

端点服务需要网络负载均衡器或网关负载均衡器。在这种情况下，您将使用网关负载均衡器创建端点服务。有关使用网络负载均衡器创建端点服务的更多信息，请参阅 创建端点服务。

内容

注意事项

- 端点服务在您创建端点服务的区域可用。
- 当服务使用者检索有关端点服务的信息时，他们只能看到与服务提供商共有的可用区。当服务提供商与服务使用者处于不同的账户中时，`us-east-1a` 等可用区名称可能会映射到每个 AWS 账户中不同的实际可用区。您可以使用 AZ IDs 来始终如一地识别服务的可用区。有关更多信息，请参阅 Amazon EC2 用户指南IDs中的可用区。
- 您的 AWS PrivateLink 资源有配额。有关更多信息，请参阅 AWS PrivateLink 配额。

先决条件

- 创建一个服务VPC提供商，在可用区域中至少有两个子网，该服务应在其中可用。将一个子网用于安全设备实例，另一个用于网关负载均衡器。
- 在您的服务提供商中创建 Gateway Load Balancer VPC。如果您计划在终端节点服务上启用IPv6支持，则必须在 Gateway Load Balancer 上启用双堆栈支持。有关更多信息，请参阅网关负载均衡器入门。
- 在服务提供商中启动安全设备VPC，并将其注册到负载平衡器目标组。

创建端点服务

按照以下步骤，使用网关负载均衡器创建端点服务。

使用控制台创建端点服务

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 Create endpoint service（创建端点服务）。
4. 在 Load balancer type（负载均衡器类型）选项中选择 Gateway（网关）。
5. 对于 Available load balancers（可用负载均衡器），选择您的网关负载均衡器。
6. 在 Require acceptance for endpoint（需要接受以使用端点）选项中，选择 Acceptance required（需要接受）以要求手动接受对端点服务的连接请求。否则，将自动接受它们。
7. 对于 Supported IP address types（支持的 IP 地址类型），执行以下任一操作：
   - 选择 IPv4-启用终端节点服务以接受IPv4请求。
   - 选择 IPv6-启用终端节点服务以接受IPv6请求。
   - 选择IPv4和 IPv6-使终端节点服务能够同时接受IPv4和IPv6请求。
8. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
9. 选择 Create（创建）。

使用命令行创建端点服务

- create-vpc-endpoint-service-配置 ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

使您的端点服务可用

服务提供商必须执行以下操作才能向服务使用者提供服务。

- 添加权限以允许每个服务使用者连接到您的端点服务。有关更多信息，请参阅 the section called “管理权限”。
- 为服务使用者提供您的服务名称和支持的可用区，以便他们能够创建接口端点以连接到您的服务。有关更多信息，请参阅下面的过程。
- 接受服务使用者的端点连接请求。有关更多信息，请参阅the section called “接受或拒绝连接请求”。

AWS 委托人可以通过创建 Gateway Load Balancer 端点私密连接到您的终端节点服务。有关更多信息，请参阅 创建网关负载均衡器端点。

使用网关负载均衡器端点访问检查系统

您可以创建网关负载均衡器端点以连接到由 AWS PrivateLink支持的端点服务。

对于您从中指定的每个子网VPC，我们在子网中创建一个终端节点网络接口，并为其分配一个子网地址范围内的私有 IP 地址。终端节点网络接口是请求者管理的网络接口；您可以在自己的网络接口中查看 AWS 账户，但无法自己管理。

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。

内容

注意事项

- 您只能在服务使用者中选择一个可用区VPC。此后则无法更改此子网。若要在不同子网中使用网关负载均衡器端点，您必须创建新的网关负载均衡器端点。
- 您可以为每个服务的每个可用区创建单个网关负载均衡器端点，但必须选择网关负载均衡器支持的可用区。当服务提供商与服务使用者处于不同的账户中时，`us-east-1a` 等可用区名称可能会映射到每个 AWS 账户中不同的实际可用区。您可以使用 AZ IDs 来始终如一地识别服务的可用区。有关更多信息，请参阅 A mazon EC2 用户指南IDs中的可用区。
- 只有在服务提供商接受连接请求后，您才能使用端点服务。该服务无法VPC通过VPC终端节点向您的资源发起请求。终端节点仅返回对由您的资源发起的流量的响应VPC。
- 每个可用区的每个网关负载均衡器端点可支持高达 10 Gbps 的带宽并自动纵向扩展到高达 100 Gbps。
- 如果端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，网关负载均衡器端点将仅与每个可用区的一个负载均衡器的建立连接。
- 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端点。

- 当流量通过网关负载均衡器端点路由时，即使目标与网络负载均衡器位于同一VPC位置，也不支持网络负载均衡器客户端 IP 保留。
- 如果应用程序服务器和 Gateway Load Balancer 端点位于同一个子网中，则会针对从应用程序服务器到 Gateway Load Balancer 端点的流量评估NACL规则。
- 如果您将 Gateway Load Balancer 与仅限出口的 Internet 网关一起使用，则IPv6流量将被丢弃。相反，应使用互联网网关和入站防火墙规则。
- 您的 AWS PrivateLink 资源有配额。有关更多信息，请参阅 AWS PrivateLink 配额。

先决条件

- 创建一个服务VPC使用者，在可用区中至少有两个子网供您访问服务。将一个子网用于应用程序服务器，另一个用于网关负载均衡器端点。
- 要验证终端节点服务支持哪些可用区，请使用控制台或describe-vpc-endpoint-services命令描述终端节点服务。
- 如果您的资源位于带网络的子网中ACL，请验证该网络是否ACL允许终端节点网络接口与中的资源之间的流量VPC。

创建端点

按照以下步骤，创建可连接到检查系统端点服务的网关负载均衡器端点。

使用控制台创建网关负载均衡器端点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 对于类型，选择使用NLBs和的终端节点服务GWLBs。
5. 对于 Service name，输入服务的名称，然后选择 Verify service（验证服务）。
6. 对于 VPC，选择要VPC从中访问终端节点服务的。
7. 对于子网，请选择一个子网来创建端点网络接口。
8. 对于 IP address type（IP 地址类型），可从以下选项中进行选择：
    - IPv4— 为端点网络接口分配IPv4地址。仅当所选子网具有IPv4地址范围时，才支持此选项。
    - IPv6— 为端点网络接口分配IPv6地址。仅当所选子网是唯一子网时，IPv6才支持此选项。

- Dualstack — 将IPv4和IPv6地址分配给端点网络接口。仅当所选子网同时具有IPv4和IPv6地址范围时，才支持此选项。

9. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
10. 选择创建端点。初始状态为 `pending acceptance`。

使用命令行创建网关负载均衡器端点。

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

配置路由

使用以下步骤为服务使用者配置路由表VPC。这使安全设备能够对发往应用程序服务器的入站流量执行安全检查。有关更多信息，请参阅 the section called “路由”。

使用控制台配置路由

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Route Tables（路由表）。
3. 为互联网网关选择路由表，并执行以下操作：
   a. 依次选择 Actions（操作）、Edit routes（编辑路由）。
   b. 如果您支持IPv4，请选择添加路由。在目标中，输入应用程序服务器的子网IPv4CIDR块。对于目标，选择VPC终端节点。
   c. 如果您支持IPv6，请选择添加路由。在目标中，输入应用程序服务器的子网IPv6CIDR块。对于目标，选择VPC终端节点。
   d. 选择 Save changes（保存更改）。
4. 为包含应用程序服务器的子网选择路由表，并执行以下操作：
   a. 依次选择 Actions（操作）、Edit routes（编辑路由）。
   b. 如果您支持IPv4，请选择添加路由。在目标位置字段，输入 **`0.0.0.0/0`**。对于目标，选择VPC终端节点。
   c. 如果您支持IPv6，请选择添加路由。在目标位置字段，输入 **`::/0`**。对于目标，选择VPC终端节点。
   d. 选择 Save changes（保存更改）。

5. 为包含网关负载均衡器端点的子网选择路由表，并执行以下操作：

   a. 依次选择 Actions（操作）、Edit routes（编辑路由）。

   b. 如果您支持IPv4，请选择添加路由。在目标位置字段，输入 **0.0.0.0/0**。在 Target（目标）选项中，选择互联网网关。

   c. 如果您支持IPv6，请选择添加路由。在目标位置字段，输入 **::/0**。在 Target（目标）选项中，选择互联网网关。

   d. 选择 Save changes（保存更改）。

使用命令行配置路由

- create-route (AWS CLI)
- New-EC2Route（适用于 Windows 的工具 PowerShell）

管理标签

您可以对网关负载均衡器端点进行标记，以帮助您识别它或根据组织的需要对其进行分类。

使用控制台管理标签

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 依次选择 Actions（操作）、Manage tags（管理标签）。
5. 若要添加标签，请选择 Add new tag（添加新标签），然后输入标签的键和值。
6. 若要删除标签，请选择标签的键和值右侧的 Remove（删除）。
7. 选择 Save（保存）。

使用命令行管理标签

- create-tags 和 delete-tags (AWS CLI)
- New-EC2Tag和 Remove-EC2Tag（适用于 Windows 的工具 PowerShell）

删除网关负载均衡器端点

用完端点后，您可以将其删除。删除网关负载均衡器端点也会删除端点网络接口。如果路由表中存在指向端点的路由，则无法删除网关负载均衡器端点。

删除网关负载均衡器端点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（端点）并选择您的端点。
3. 依次选择 Actions（操作）、Delete Endpoint（删除端点）。
4. 在确认屏幕中，选择 Yes, Delete（是的，删除）。

删除网关负载均衡器端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

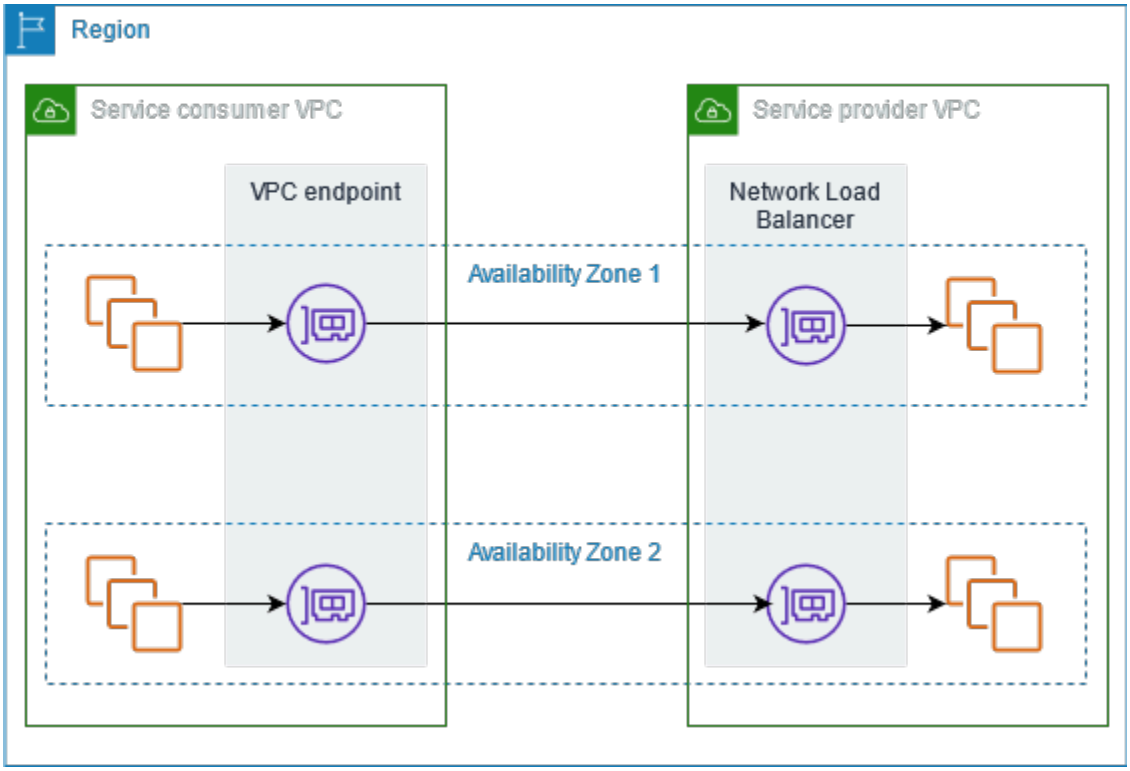
通过以下方式共享您的服务 AWS PrivateLink

您可以托管自己的 AWS PrivateLink 强化服务（称为端点服务），并与其他 AWS 客户共享。

内容

概述

下图显示了您如何 AWS 与其他 AWS 客户共享托管的服务，以及这些客户如何连接到您的服务。作为服务提供商，您可以在VPC作为服务前端的网络负载均衡器中创建 Network Load Balancer。然后，在创建VPC终端节点服务配置时选择此负载均衡器。您可向特定 AWS 主体授予权限，以便它们可以连接到您的服务。作为服务使用者，客户创建一个接口VPC终端节点，用于在他们从其VPC终端节点服务中选择的子网与您的终端节点服务之间建立连接。负载均衡器接收来自服务使用者的请求并将请求路由到托管您服务的目标。



为实现低延迟和高可用性，建议您在至少两个可用区中提供服务。

DNS主机名

服务提供商创建VPC终端节点服务时， AWS 会为该服务生成终端节点特定的DNS主机名。这些名称的语法如下：

```
endpoint_service_id.region.vpce.amazonaws.com
```

以下是 us-ea DNS st-2 区域中VPC终端节点服务的主机名示例：

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

当服务使用者创建接口VPC终端节点时，我们会创建区域和区域DNS名称，服务使用者可以使用这些名称与终端节点服务进行通信。区域名称的语法如下：

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

分区名称的语法如下：

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

私人 DNS

服务提供商还可以为其终端节点服务关联私有DNS名称，以便服务使用者可以使用其现有DNS名称继续访问该服务。如果服务提供商将私有DNS名称与其终端节点服务相关联，则服务使用者可以为其接口终端节点启用私有DNS名称。如果服务提供商未启用私有功能DNS，则服务使用者可能需要更新其应用程序以使用VPC终端节点服务的公共DNS名称。有关更多信息，请参阅 管理DNS姓名。

跨区域访问

服务提供商可以在一个区域托管服务，并在一组受支持的区域中提供该服务。服务使用者在创建终端节点时选择服务区域。

权限

- 默认情况下，IAM实体无权在多个区域提供终端节点服务或跨区域访问终端节点服务。要授予跨区域访问所需的权限，IAM管理员可以创建允许仅限`vpce:AllowMultiRegion`权限的操作的IAM策略。
- 要控制IAM实体在创建终端节点服务时可以指定为支持区域的区域，请使用`ec2:VpceSupportedRegion`条件键。
- 要控制IAM实体在创建VPC端点时可以指定为服务区域的区域，请使用`ec2:VpceServiceRegion`条件键。

注意事项

- 服务提供商必须先选择加入可选区域，然后才能将其添加为终端节点服务的支持区域。
- 您的终端节点服务必须可以从其托管区域进行访问。您无法将主机区域从支持的区域集中移除。为了实现冗余，您可以在多个区域部署终端节点服务，并为每个终端节点服务启用跨区域访问。
- 服务使用者必须先选择加入可选区域，然后才能将其选择为终端节点的服务区域。只要有可能，我们建议服务使用者使用区域内连接而不是跨区域连接来访问服务。区域内连接可提供更低的延迟和更低的成本。
- 如果服务提供商从支持的区域集中删除某个区域，则服务使用者在创建新终端节点时无法选择该区域作为服务区域。请注意，这不会影响使用此区域作为服务区域的现有终端节点访问终端节点服务。
- 为了获得高可用性，提供商和消费者都应使用至少两个可用区。请注意，跨区域访问不需要提供商和消费者使用相同的可用区。

- 通过跨区域访问，可以 AWS PrivateLink 管理可用区之间的故障转移。它不管理跨区域的故障转移。
- DNS名称友好的 AWS Marketplace 服务不支持跨区域访问。
- 为TCP空闲超时配置了自定义值的网络负载均衡器不支持跨区域访问。
- UDP分段不支持跨区域访问。

IP 地址类型

服务提供商可以通过IPv4、IPv6或两IPv4者兼而有之向服务消费者提供其服务端点IPv6，即使他们的后端服务器仅支持IPv4。如果您启用双栈支持，则现有消费者可以继续使用IPv4来访问您的服务，而新的消费者可以选择使用IPv6来访问您的服务。

如果接口VPC端点支持IPv4，则端点网络接口具有IPv4地址。如果接口VPC端点支持IPv6，则端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。如果您使用IPv6地址描述端点网络接口，请注意该接口已启`denyAllIgwTraffic`用。

IPv6为终端节点服务启用的要求

- 终端节点服务的VPC和子网必须有关联的IPv6CIDR块。
- 端点服务的所有网络负载均衡器必须使用双堆栈 IP 地址类型。目标不需要支持流IPv6量。如果服务处理代理协议版本 2 标头中的源 IP 地址，则必须处理IPv6地址。

IPv6为接口终端节点启用的要求

- 终端节点服务必须支持IPv6请求。
- 接口端点的 IP 地址类型必须与接口端点的子网兼容，如下所述：
  - IPv4— 为您的端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围时，才支持此选项。
  - IPv6— 为您的端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网时，IPv6才支持此选项。
  - Dualstack — 将IPv4和IPv6地址分配给您的端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围时，才支持此选项。

DNS记录接口端点的 IP 地址类型

接口端点支持的DNS记录 IP 地址类型决定了我们创建的DNS记录。接口端点的DNS记录 IP 地址类型必须与接口终端节点的 IP 地址类型兼容，如下所述：

- IPv4— 为私人、地区和地区DNS名称创建 A 记录。IP 地址类型必须是IPv4或 Dual stack。
- IPv6— 为私人、地区和地区DNS名称创建AAAA记录。IP 地址类型必须是IPv6或 Dual stack。
- Dualstack — 创建 A 并AAAA记录私有、区域和区域名称。DNSIP 地址类型必须为 Dualstack（双堆栈）。

创建由以下设备提供支持的服务 AWS PrivateLink

您可以创建自己的由提供支持的服务 AWS PrivateLink，称为终端节点服务。您是服务提供商，而创建与您的服务之间的连接的 AWS 主体是服务使用者。

端点服务需要网络负载均衡器或网关负载均衡器。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。在这种情况下，您将使用网络负载均衡器创建端点服务。有关使用网关负载均衡器创建端点服务的更多信息，请参阅 访问虚拟设备。

内容

注意事项

- 端点服务在您创建端点服务的区域可用。如果您启用跨区域访问或使用对等互VPC连或传输网关，则消费者可以从其他区域访问您的服务。
- 当服务使用者检索有关端点服务的信息时，他们只能看到与服务提供商共有的可用区。当服务提供商与服务使用者处于不同的账户中时，`us-east-1a` 等可用区名称可能会映射到每个 AWS 账户中不同的实际可用区。您可以使用 AZ IDs 来始终如一地识别服务的可用区。有关更多信息，请参阅 Amazon EC2 用户指南IDs中的可用区。
- 当服务使用者通过接口端点将流量发送至服务时，向应用程序提供的源 IP 地址是负载均衡器节点的私有 IP 地址而不是服务使用者的 IP 地址。如果您在负载均衡器上启用代理协议，则可以从代

理协议标头中获取服务使用者的地址和接口端点的地址。IDs有关更多信息，请参阅 Network Load Balancer 用户指南 中的代理协议。

- 一个网络负载均衡器只能与一个端点服务关联，但一个端点服务可与多个网络负载均衡器关联。
- 如果一个端点服务与多个网络负载均衡器相关联，则每个端点网络接口都与一个负载均衡器相关联。当来自端点网络接口的第一个连接启动时，我们会随机选择端点网络接口所在的同一可用区中的一个网络负载均衡器。来自此端点网络接口的所有后续连接请求都使用所选的负载均衡器。我们建议您为端点服务的所有负载均衡器使用相同的侦听器和目标组配置，这样无论选择哪个负载均衡器，使用者都可以成功使用端点服务。
- 您的 AWS PrivateLink 资源有配额。有关更多信息，请参阅 AWS PrivateLink 配额。

先决条件

- VPC为您的终端节点服务创建一个，该服务应在每个可用区中至少有一个子网。
- 要使服务使用者能够为您的VPC终端节点服务创建IPv6接口终端节点，VPC和子网必须具有关联的IPv6CIDR块。
- 在您的中创建一个 Network Load Balancer VPC。为每个可用区选择一个子网，在该子网中，服务应可供服务使用者使用。为实现低延迟和容错能力，建议您在该区域的至少两个可用区中提供服务。
- 如果您的网络负载均衡器有安全组，则它必须允许来自客户端 IP 地址的入站流量。或者，您可以关闭对通过流量的入站安全组规则的评估 AWS PrivateLink。有关更多信息，请参阅网络负载均衡器用户指南中的安全组。
- 要使您的终端节点服务能够接受IPv6请求，其网络负载均衡器必须使用双堆栈 IP 地址类型。目标不需要支持流IPv6量。有关更多信息，请参阅《网络负载均衡器用户指南》中的 IP 地址类型。

  如果您处理代理协议版本 2 标头中的源 IP 地址，请确认您可以处理IPv6地址。
- 在每个提供服务的可用区中启动实例，并将其注册到负载均衡器目标组。如果您没有在所有已启用的可用区域中启动实例，则可以启用跨区域负载均衡以支持使用区域DNS主机名访问服务的服务使用者。启用跨区域负载均衡后，可能收取区域数据传输费用。有关更多信息，请参阅网络负载均衡器用户指南中的跨区域负载均衡。

创建端点服务

按照以下步骤，使用网络负载均衡器创建端点服务。

使用控制台创建端点服务

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 Create endpoint service（创建端点服务）。
4. 对于 Load balancer type（负载均衡器类型），选择 Network（网络）。
5. 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。要查看为所选负载均衡器启用的可用区，请参阅所选负载均衡器的详细信息，包括的可用区。您的端点服务将在这些可用区中可用。
6. （可选）要使您的终端节点服务在托管区域以外的区域中可用，请从服务区域中选择区域。有关更多信息，请参阅 the section called “跨区域访问”。
7. 在 Require acceptance for endpoint（需要接受以使用端点）选项中，选择 Acceptance required（需要接受）以要求手动接受对端点服务的连接请求。否则将自动接受这些请求。
8. 对于 “启用私有DNS名称”，选择 “将私有DNS名称与服务关联” 以关联服务使用者可以用来访问您的服务的私有名称，然后输入私有DNS名称。DNS否则，服务使用者可以使用提供的终端节点专用DNS名称。 AWS在服务使用者可以使用私有DNS名称之前，服务提供商必须验证他们是否拥有该域名。有关更多信息，请参阅 管理DNS姓名。
9. 对于 Supported IP address types（支持的 IP 地址类型），执行以下任一操作：
   - 选择 IPv4-启用终端节点服务以接受IPv4请求。
   - 选择 IPv6-启用终端节点服务以接受IPv6请求。
   - 选择IPv4和 IPv6-使终端节点服务能够同时接受IPv4和IPv6请求。
10. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
11. 选择 Create（创建）。

使用命令行创建端点服务

- create-vpc-endpoint-service-配置 ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

使端点服务可供服务使用者使用

AWS 委托人可以通过创建接口终端节点私密连接到您的VPC终端节点服务。服务提供商必须执行以下操作才能向服务使用者提供服务。

- 添加权限以允许每个服务使用者连接到您的端点服务。有关更多信息，请参阅 the section called “管理权限”。
- 为服务使用者提供您的服务名称和支持的可用区，以便他们能够创建接口端点以连接到您的服务。有关更多信息，请参阅 the section called “作为服务使用者连接到端点服务”。
- 接受服务使用者的端点连接请求。有关更多信息，请参阅 the section called “接受或拒绝连接请求”。

作为服务使用者连接到端点服务

服务使用者可通过以下步骤创建接口端点以连接到端点服务。

使用控制台创建接口端点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 对于类型，选择使用NLBs和的终端节点服务GWLBs。
5. 在服务名称中，输入服务的名称（例如，`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`），然后选择验证服务。
6. （可选）要连接到终端节点区域以外的区域中可用的终端节点服务，请选择服务区域，启用跨区域终端节点，然后选择区域。有关更多信息，请参阅 the section called “跨区域访问”。
7. 对于 VPC，选择要VPC从中访问终端节点服务的。
8. 对于子网，选择要在其中创建端点网络接口的子网。
9. 对于 IP address type（IP 地址类型），可从以下选项中进行选择：
   - IPv4— 为端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围并且终端节点服务接受IPv4请求时，才支持此选项。
   - IPv6— 为端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网并且终端节点服务接受IPv6请求时，IPv6才支持此选项。
   - Dualstack — 将IPv4和IPv6地址分配给端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围并且终端节点服务同时接受IPv4和IPv6请求时，才支持此选项。
10. 对于DNS记录 IP 类型，请从以下选项中进行选择：
    - IPv4— 为私人、地区和地区DNS名称创建 A 记录。IP 地址类型必须是IPv4或 Dual stack。
    - IPv6— 为私人、地区和地区DNS名称创建AAAA记录。IP 地址类型必须是IPv6或 Dual stack。

- Dualstack — 创建 A 并AAAA记录私有、区域和区域名称。DNSIP 地址类型必须为 Dualstack（双堆栈）。
- 服务定义-为私人、区域和区域名称创建 A AAAA 记录，为区域和区域DNS名称创建 A DNS 记录。IP 地址类型必须为 Dualstack（双堆栈）。

11. 对于 Security group（安全组），选择要与端点网络接口关联的安全组。
12. 选择创建端点。

使用命令行创建接口端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

配置端点服务

创建端点服务后，您可以更新其配置。

任务

- 管理权限
- 接受或拒绝连接请求
- 管理负载均衡器
- 关联私有DNS名称
- 修改支持的区域
- 修改支持的 IP 地址类型
- 管理标签

管理权限

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）可以访问您的终端节点服务。例如，可以为您信任的特定主体授予权限，并自动接受所有连接请求；您还可以为范围更广的主体组授予权限，并手动接受您信任的特定连接请求。

默认情况下，您的端点服务对服务使用者不可用。您必须添加允许特定 AWS 委托人创建接口VPC终端节点以连接到您的终端节点服务的权限。要为 AWS 委托人添加权限，您需要其 Amazon 资源名称 (ARN)。以下列表包括支持的 AWS 委托ARNs人的示例。

ARNs对于 AWS 校长

AWS 账户 （包括账户中的所有委托人）

arn: aws: iam::: root *account_id*

角色

arn: aws: iam::: role/ *account_id role_name*

用户

arn: aws: iam::: user/ *account_id user_name*

所有校长合而为一 AWS 账户

*

注意事项

- 如果您授予所有人访问端点服务的权限，并将端点服务配置为接受所有请求，则即使您的负载均衡器没有公有 IP 地址，它也将是公有的。
- 如果您移除权限，则不会影响端点与服务之间先前已接受的现有连接。

使用控制台管理端点服务的权限

1. 打开 Amazon VPC 控制台，网址为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 Allow principals（允许主体）选项卡。
4. 要添加权限，请选择 Allow principals（允许主体）。对于要添加的委托人，请输入ARN委托人的。要添加另一个委托人，请选择 Add principal（添加委托人）。添加主体后，请选择 Allow principals（允许主体）。
5. 要删除权限，请选择该主体，然后依次选择 Actions（操作）、Delete（删除）。提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

使用命令行为端点服务添加权限

- modify-vpc-endpoint-service-权限 ()AWS CLI
- Edit-EC2EndpointServicePermission（适用于 Windows 的工具 PowerShell）

接受或拒绝连接请求

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）可以访问您的终端节点服务。例如，可以为您信任的特定主体授予权限，并自动接受所有连接请求；您还可以为范围更广的主体组授予权限，并手动接受您信任的特定连接请求。

您可以将端点服务配置为自动接受连接请求。否则，您必须手动接受或拒绝请求。如果您不接受连接请求，服务使用者将无法访问端点服务。

如果您授予所有人访问端点服务的权限，并将端点服务配置为接受所有请求，则即使您的负载均衡器没有公有 IP 地址，它也将是公有的。

当连接请求被接受或拒绝时，您会收到通知。有关更多信息，请参阅 the section called “接收端点服务事件的提醒”。

使用控制台修改接受设置

1. 打开 Amazon VPC 控制台，网址为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. 选择 Actions、Modify endpoint acceptance setting。
5. 选择或清除 Acceptance required（需要接受）。
6. 选择 Save changes（保存更改）

使用命令行修改接受设置

- modify-vpc-endpoint-service-配置 ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

使用控制台接受或拒绝连接请求

1. 打开 Amazon VPC 控制台，网址为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）选项卡中，选择端点连接。
5. 要接受连接请求，依次选择 Actions（操作）、Accept endpoint connection request（接受端点连接请求）。提示进行确认时，输入 **accept**，然后选择 Accept（接受）。

6. 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）。提示进行确认时，输入 **reject**，然后选择 Reject（拒绝）。

使用命令行接受或拒绝连接请求

- accept-vpc-endpoint-connections或 reject-vpc-endpoint-connections(AWS CLI)
- Approve-EC2EndpointConnection或 Deny-EC2EndpointConnection（适用于 Windows 的工具 PowerShell）

管理负载均衡器

您可以管理与端点服务相关联的负载均衡器。如果已有端点连接到端点服务，则您无法取消关联负载均衡器。

如果您为网络负载均衡器启用另一个可用区，则也可以为您的端点服务启用可用区。为终端节点服务启用可用区后，服务使用者可以将该可用区的子网添加到其接口VPC终端节点。

要使用控制台管理端点服务的负载均衡器

1. 打开 Amazon VPC 控制台，网址为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. 依次选择 Actions（操作）、Associate or disassociate load balancers（关联或取消关联负载均衡器）。
5. 根据需要更改端点服务配置。例如：
   - 选中负载均衡器的复选框，以便将其与端点服务关联。
   - 清除负载均衡器的复选框，以便将其与端点服务取消关联。您必须至少选择一个负载均衡器。
   - 如果您最近为负载均衡器启用了另一个可用区，则它会显示在 Included Availability Zones（包括的可用区）下。如果您在下一步中保存更改，则会为新的可用区启用端点服务。
6. 选择 Save changes（保存更改）

要使用命令行更改端点服务的负载均衡器

- modify-vpc-endpoint-service-配置 ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

要在最近为负载均衡器启用的可用区中启用端点服务，您只需使用端点服务的 ID 调用命令即可。

关联私有DNS名称

您可以将私有DNS名称与终端节点服务相关联。关联私有DNS名称后，您必须在DNS服务器上更新该域的条目。在服务使用者可以使用私有DNS名称之前，服务提供商必须验证他们是否拥有该域名。有关更多信息，请参阅 管理DNS姓名。

使用控制台修改终端节点服务的私有DNS名称

1. 打开 Amazon VPC 控制台，网址为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. 选择操作，修改私人DNS名称。
5. 选择 “将私有DNS名称与服务关联”，然后输入私有DNS名称。
   - 域名必须使用小写。
   - 您可以在域名中使用通配符（例如 **`*.myexampleservice.com`**)。
6. 选择 Save changes（保存更改）。
7. 验证状态后，私有DNS名称可供服务使用者使用。如果验证状态发生变化，新的连接请求将被拒绝，但现有连接不会受到影响。

使用命令行修改终端节点服务的私有DNS名称

- modify-vpc-endpoint-service-配置 ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

使用控制台启动域验证过程

1. 打开 Amazon VPC 控制台，网址为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. 选择操作，验证私有DNS名称的域名所有权。
5. 提示进行确认时，输入 **`verify`**，然后选择 Verify（验证）。

使用命令行启动域验证过程

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification（适用于 Windows 的工具 PowerShell）

修改支持的区域

您可以修改终端节点服务的支持区域集。在添加可选区域之前，必须先选择加入。您无法移除托管您的终端节点服务的区域。

删除区域后，服务使用者无法创建将其指定为服务区域的新终端节点。移除区域不会影响将其指定为服务区域的现有终端节点。当您移除某个区域时，我们建议您拒绝来自该区域的任何现有终端节点连接。

修改您的终端节点服务支持的区域

1. 打开 Amazon VPC 控制台，网址为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. 选择操作，修改支持的区域。
5. 根据需要选择和取消选择 “区域”。
6. 选择 Save changes（保存更改）。

修改支持的 IP 地址类型

您可以更改端点服务支持的 IP 地址类型。

考虑因素

要使您的终端节点服务能够接受IPv6请求，其网络负载均衡器必须使用双堆栈 IP 地址类型。目标不需要支持流IPv6量。有关更多信息，请参阅《网络负载均衡器用户指南》中的 IP 地址类型。

使用控制台修改支持的 IP 地址类型

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择终VPC端节点服务。
4. 依次选择 Actions（操作）、Modify supported IP address types（修改支持的 IP 地址类型）。

5. 对于 Supported IP address types（支持的 IP 地址类型），执行以下任一操作：
   - 选择 IPv4-启用终端节点服务以接受IPv4请求。
   - 选择 IPv6-启用终端节点服务以接受IPv6请求。
   - 选择IPv4和 IPv6-使终端节点服务能够同时接受IPv4和IPv6请求。
6. 选择 Save changes（保存更改）。

使用命令行修改支持的 IP 地址类型

- modify-vpc-endpoint-service-配置 ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

管理标签

您可以对资源进行标记，以帮助您识别资源或根据组织的需求进行分类。

使用控制台管理端点服务的标签

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择终VPC端节点服务。
4. 依次选择 Actions（操作）、Manage tags（管理标签）。
5. 对于每个要添加的标签，请选择 Add new tag（添加新标签），然后输入标签键和标签值。
6. 若要删除标签，请选择标签的键和值右侧的 Remove（删除）。
7. 选择 Save（保存）。

使用控制台管理端点连接的标签

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择终VPC端节点服务，然后选择端点连接选项卡。
4. 选择端点连接，然后依次选择 Actions（操作）、Manage tags（管理标签）。
5. 对于每个要添加的标签，请选择 Add new tag（添加新标签），然后输入标签键和标签值。
6. 若要删除标签，请选择标签的键和值右侧的 Remove（删除）。

7. 选择 Save（保存）。

使用控制台管理端点服务权限的标签

1. 打开 Amazon VPC 控制台，网址为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，然后选择允许委托人选项卡。
4. 选择主体，然后依次选择 Actions（操作）、Manage tags（管理标签）。
5. 对于每个要添加的标签，请选择 Add new tag（添加新标签），然后输入标签键和标签值。
6. 若要删除标签，请选择标签的键和值右侧的 Remove（删除）。
7. 选择 Save（保存）。

使用命令行添加和删除标签

- create-tags 和 delete-tags (AWS CLI)
- New-EC2Tag和 Remove-EC2Tag（适用于 Windows 的工具 PowerShell）

管理VPC终端节点服务的DNS名称

服务提供商可以为其终端节点服务配置私有DNS名称。假设服务提供商通过公共终端节点将其服务作为终端节点服务提供。如果服务提供商使用公共终端节点的DNS名称作为终端节点服务的私有DNS名称，则服务使用者可以使用相同的客户端应用程序访问公共终端节点或终端节点服务，而无需进行修改。如果请求来自服务使用者VPC，则私有DNS服务器会将DNS名称解析为端点网络接口的 IP 地址。否则，公共DNS服务器会将该DNS名称解析为公共端点。

在为终端节点服务配置私有DNS名称之前，必须通过执行域所有权验证检查来证明您拥有该域。

注意事项

- 一个终端节点服务只能有一个私有DNS名称。
- 当使用者创建接口终端节点以连接到您的服务时，我们会创建一个私有托管区域并将其与服务使用者关联VPC。我们在私有托管区域中创建了一CNAME条记录，该记录将终端节点服务的私有DNS名称映射到VPC终端节点的区域DNS名称。当使用者向服务的公共DNS名称发送请求时，私有DNS服务器会将请求解析到端点网络接口的 IP 地址。
- 要验证域名，您必须拥有公共主机名或公共提供DNS商。

- 您可以验证子域的域。例如，您可以验证 example.com，而不是 a.example.com。每个DNS标签最多可包含 63 个字符，整个域名的总长度不得超过 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。现在，您可以将 b.example.com 添加为私人名称。DNS在服务使用者可以使用该名称之前，您必须验证 example.com 或 b.example.com。
- Gateway Load Balancer 终端节点不支持私有DNS名称。

域所有权验证

您的域名与您通过DNS提供商管理的一组域名服务 (DNS) 记录相关联。TXTDNS记录是一种提供有关您的域名的额外信息的记录。其中包含一个名称和一个值。作为验证过程的一部分，您必须在DNS服务器上为您的公共领域添加一条TXT记录。

当我们在您的域名DNS设置中检测到TXT记录存在时，域名所有权验证即告完成。

添加记录后，您可以使用 Amazon VPC 控制台查看域名验证流程的状态。在导航窗格中，选择 Endpoint services（端点服务）。选择端点服务，并在 Details（详细信息）选项卡中检查 Domain verification status（域验证状态）的值。如果域验证正在等待处理，请等待几分钟，然后刷新屏幕。如果需要，您可以手动启动验证过程。选择操作，验证私有DNS名称的域名所有权。

验证状态后，私有DNS名称可供服务使用者使用。如果验证状态发生变化，新的连接请求将被拒绝，但现有连接不会受到影响。

如果验证状态为 failed（失败），请参阅 the section called “解决域验证问题”。

获取名称和值

我们为您提供您在TXT记录中使用的名称和值。例如，在 AWS Management Console中提供信息。选择端点服务，并在端点服务的 Details（详细信息）选项卡中查看 Domain verification name（域验证名称）和 Domain verification value（域验证值）。您还可以使用以下 describe-vpc-endpoint-service-configur ation AWS CLI s命令检索有关指定终端节点服务的私有DNS名称配置的信息。

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

下面是示例输出。当你创建TXT记录Name时，你将使用Value和。

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

例如，假设您的域名是 example.com，并且 `Value` 和 `Name` 如前面的示例输出所示。下表是TXT记录设置的示例。

Name	Type	值
_6e86v84tqgqubxbwii1m.example.com	TXT	vpce: l6p0 ERxlTt45jevFwOCp

建议您使用 `Name` 作为记录子域，因为基本域名可能已在使用中。但是，如果您的DNS提供商不允许DNS记录名称包含下划线，则可以省略 “_6e86v84tqqqubxbwii1m”，只需在记录中使用 “example.com” 即可。TXT

在我们验证“_6e86v84tqgqubxbwii1m.example.com”之后，服务使用者可使用“example.com”或子域（例如“service.example.com”或“my.service.example.com”）。

向你的域名的DNS服务器添加TXT一条记录

向域名DNS服务器添加TXT记录的过程取决于谁提供您的DNS服务。您的DNS提供商可能是 Amazon Route 53 或其他域名注册商。

Amazon Route 53

为公有托管区创建记录。使用以下值：

- 对于 “记录类型”，选择TXT。
- 在 TTL（秒）中，输入**1800**。
- 对于 Routing policy（路由策略），选择 Simple routing（简单路由）。
- 对于 Record name（记录名称），输入域或子域。
- 对于 Value/Route traffic to（值/流量路由至），输入域验证值。

有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用控制台创建记录。

一般过程

访问您的DNS提供商的网站并登录您的帐户。找到更新您的域名DNS记录的页面。添加一条包含我们提供的名称和值的TXT记录。DNS记录更新最多可能需要 48 小时才能生效，但生效时间通常要早得多。

有关更具体的说明，请查阅您的DNS提供商提供的文档。下表提供了几个常见提供DNS商的文档链接。此列表并不全面，也并非旨在推荐这些公司提供的产品或服务。

DNS/托管服务提供商	文档链接
GoDaddy	添加一条TXT记录
Dreamhost	添加自定义DNS记录
Cloudflare	管理DNS记录
HostGator	使用 HostGator /管理DNS记录 eNom
Namecheap	如何为我的域名添加TXT/SPF/DKIM/DMARC记录？
Names.co.uk	更改您的域名DNS设置
Wix	在您的 Wix TXT 账户中添加或更新记录

检查TXT记录是否已发布

您可以使用以下步骤验证您的私有域DNS名所有权验证TXT记录是否已正确发布到您的DNS服务器。您将运行 nslookup 命令，目前支持的平台有 Windows 和 Linux。

您将查询为您的域提供服务的DNS服务器，因为这些服务器包含的域 up-to-date信息最多。您的域名信息需要一段时间才能传播到其他DNS服务器。

验证您的TXT记录是否已发布到您的DNS服务器

1. 使用以下命令查找您的域的名称服务器。

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

此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. 使用以下命令验证TXT记录是否已正确发布，其中*name_server*是您在上一步中找到的名称服务器之一。

```
nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
```

3. 在上一步的输出中，验证后面的字符串是否与TXT值`text =`匹配。

   在我们的示例中，如果记录正确发布，则输出包括以下内容。

```
_6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
```

解决域验证问题

如果域验证过程失败，以下信息可以帮助您解决问题。

- 检查您的DNS提供商是否允许在TXT记录名称中使用下划线。如果您的DNS提供商不允许使用下划线，则可以省略记录中的域名验证名称（例如 “_6e86v84tqqqubxbwii1m”）。TXT
- 检查您的DNS提供商是否将域名附加到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。为避免域名重复，请在创建TXT记录时在域名的末尾添加一个句点。这会告诉您的DNS提供商，没有必要将域名附加到TXT记录中。
- 检查您的DNS提供商是否将DNS记录值修改为仅使用小写字母。只有当验证记录的属性值与我们提供的值完全匹配时，我们才会验证您的域。如果DNS提供商将您的TXT记录值更改为仅使用小写字母，请联系他们寻求帮助。
- 由于您支持多个区域或多个 AWS 账户，因而您可能需要多次验证您的域。如果您的DNS提供商不允许您拥有多个具有相同属性名称的TXT记录，请检查您的DNS提供商是否允许您为同一TXT记录分配多个属性值。例如，如果您由 Amazon Route 53 管理，则可以使用以下步骤。DNS

  1. 在 Route 53 控制台中，选择您在第一个区域验证域名时创建的TXT记录。
  2. 对于 Value（值），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。

  如果您的DNS提供商不允许您为同一TXT条记录分配多个值，则您可以使用TXT记录的属性名称中的值对域进行一次验证，另一次使用从属性名称中删除该值进行一次验证。但是，您只能对同一个域验证两次。

接收端点服务事件的提醒

您可以创建通知以接收与端点服务相关的特定事件的提醒。例如，您可以在连接请求被接受或拒绝时收到电子邮件。

任务

- 创建SNS通知
- 添加访问策略
- 添加密钥策略

创建SNS通知

使用以下步骤为通知创建 Amazon SNS 主题并订阅该主题。

使用控制台为端点服务创建通知

1. 打开 Amazon VPC 控制台，网址为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. 在 Notifications（通知）选项卡上，选择 Create notofication（创建通知）。
5. 在 “通知” 中ARN，选择与您创建ARN的SNS主题对应的。
6. 要订阅事件，请从 Events（事件）中选择。
   - Connect（连接）– 服务使用者创建了接口端点。这会向服务提供商发送连接请求。
   - Accept（接受）– 服务提供商接受了连接请求。
   - Reject（拒绝）– 服务提供商拒绝了连接请求。
   - Delete（删除）– 服务使用者删除了接口端点。
7. 选择 Create notification（创建通知）。

使用命令行为端点服务创建通知

- create-vpc-endpoint-connection-通知 ()AWS CLI
- New-EC2VpcEndpointConnectionNotification（适用于 Windows 的工具 PowerShell）

添加访问策略

向SNS主题添加访问策略， AWS PrivateLink 允许您代表您发布通知，如下所示。有关更多信息，请参阅如何编辑我的 Amazon SNS 主题的访问策略？ 使用 aws:SourceArn 或 aws:SourceAccount 全局条件键来防止混淆代理人问题。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint-service/service-
id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

添加密钥策略

如果您使用的是加密SNS主题，则KMS密钥的资源策略必须信任 AWS PrivateLink 才能调用 AWS KMS API操作。以下是示例密钥策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
```

```
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint-service/service-
id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

删除端点服务

完成端点服务后，您可以将其删除。如果有任何端点连接到处于 `available` 或 `pending-acceptance` 状态的端点服务，则您无法删除端点服务。

删除端点服务不会删除关联的负载均衡器，也不会影响向负载均衡器目标组注册的应用程序服务器。

使用控制台删除端点服务

1. 打开 Amazon VPC 控制台，网址为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. 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）。

使用命令行删除端点服务

- delete-vpc-endpoint-service-配置 ()AWS CLI
- Remove-EC2EndpointServiceConfiguration（适用于 Windows 的工具 PowerShell）

通过以下方式访问VPC资源 AWS PrivateLink

您可以使用资源VPC终端节点（VPC资源端点）私下访问其他VPC资源中的资源。资源终端节点允许您私密安全地访问VPC资源，例如数据库、节点集群、实例、应用程序终端节点、域名目标或 IP 地址，这些地址可能位于另一个VPC或本地环境的私有子网中。如果没有资源终端节点，则必须为自己添加互联网网关，VPC或者使用 AWS PrivateLink 接口终端节点和 Network Load Balancer 访问资源。资源端点不需要负载均衡器，因此您可以直接访问VPC资源。VPC资源由资源配置表示。资源配置与资源网关绑定。

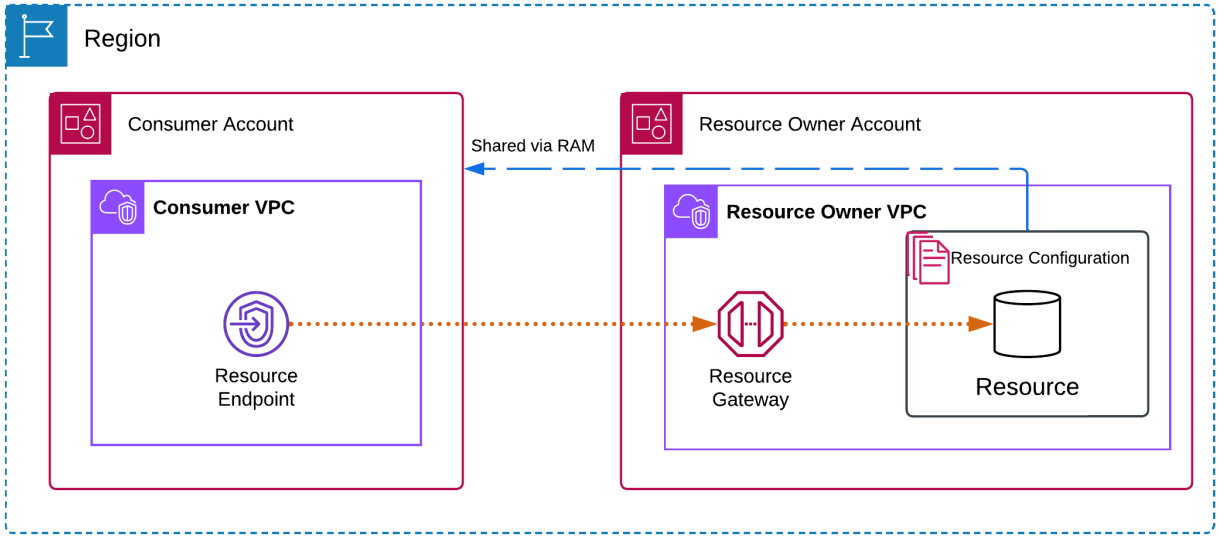
定价

当您使用资源终端节点访问资源时，您需要按配置资源VPC终端节点的每小时计费。您还需要按访问资源时处理的 GB 数据进行计费。有关更多信息，请参阅 AWS PrivateLink 定价。当您使用资源配置和资源网关启用对资源的访问时，您需要为资源网关处理的每 GB 数据付费。有关更多信息，请参阅 Amazon VPC Lattice 定价。

内容

概述

您可以访问自己账户中的资源或从其他账户与您共享的资源。要访问资源，您需要创建一个资源VPC终端节点，该终端节点使用网络接口在您的子网VPC和资源之间建立连接。发往资源的流量使用解析到资源端点网络接口的私有 IP 地址DNS，然后通过资源网关使用VPC端点与资源之间的连接发送到资源。



注意事项

- TCP支持流量。 UDP不支持流量。
- 网络连接必须从VPC包含资源端点的启动，而不是从拥有资源的端点启动。VPC资源VPC无法启动与终端节点的网络连接VPC。
- 唯一受支持的资源ARN是 Amazon RDS 资源。

DNS主机名

使用 AWS PrivateLink，您可以使用私有终端节点向资源发送流量。当您创建资源VPC终端节点时，我们会创建区域DNS名称（称为默认DNS名称），您可以使用这些名称从您的本地VPC和本地与资源进行通信。您的资源VPC端点的默认DNS名称采用以下语法：

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

在为使用的特定资源配置创建资源VPC终端节点时ARNs，可以启用私有DNS。使用 privateDNS，您可以使用 AWS 服务为资源配置的DNS名称继续向资源发出请求，同时通过资源VPC终端节点利用私有连接。有关更多信息，请参阅 the section called “DNS分辨率”。

以下describe-vpc-endpoint-associations命令显示资源端点的DNS条目。

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].DnsEntry'
```

以下是启用私有DNS名称的 Amazon RDS 数据库的资源终端节点的示例输出。第一个条目是默认DNS名称。第二个条目来自隐藏的私有托管区域，该区域将对公共端点的请求解析为端点网络接口的私有 IP 地址。

```
"DnsEntry": {
                "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
                "HostedZoneId": "ABCDEFGH123456789000"
            },
"PrivateDnsEntry": {
                "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
                "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
            }
```

DNS分辨率

我们为您的资源VPC终端节点创建的DNS记录是公开的。因此，这些DNS名称是可以公开解析的。但是，来自外部的DNS请求VPC仍会返回资源端点网络接口的私有 IP 地址。只要您可以通过VPN或 Direct Connect 访问资源端点所在的VPC，就可以使用这些DNS名称从本地访问资源。

私人 DNS

如果您DNS为资源VPC终端节点启用私有功能，并且同时启用VPC了DNS主机名和DNS解析，则我们会使用自定义DNS名称为资源配置创建隐藏的、 AWS托管的私有托管区域。托管区域包含资源默认DNS名称的记录集，该记录集可将其解析为您的VPC资源端点网络接口的私有 IP 地址。

Amazon 为您提供了一个名为 R oute 53 Resolver 的DNS服务器。VPCRoute 53 解析器会自动解析本地VPC域名并在私有托管区域中进行记录。但是，您不能从外部使用 Route 53 解析器。VPC如果您想从本地网络访问VPC终端节点，则可以使用默认DNS名称，也可以使用 Route 53 解析器终端节点和解析器规则。有关更多信息，请参阅AWS Transit Gateway 与 AWS PrivateLink 和集成 Amazon Route 53 Resolver。

子网和可用区

您可以为每个可用区配置一个子网的VPC终端节点。我们为您子网中的终端节点创建VPC终端节点网络接口。我们根据端点的 IP 地址类型为其子网中的每个VPC端点网络接口分配 IP 地址。在每个子网

中分配的 IP 地址数量取决于资源配置的数量。在生产环境中，为了获得高可用性和弹性，我们建议为每个VPC终端节点配置至少两个可用区。

IP 地址类型

资源端点可以支持IPv4IPv6、或双栈地址。支持的端点IPv6可以用AAAA记录响应DNS查询。资源终端节点的 IP 地址类型必须与资源终端节点的子网兼容，如下所述：

- IPv4— 为您的端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围时，才支持此选项。
- IPv6— 为您的端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网时，IPv6才支持此选项。
- Dualstack — 将IPv4和IPv6地址分配给您的端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围时，才支持此选项。

如果资源VPC端点支持IPv4，则端点网络接口具有IPv4地址。如果资源VPC端点支持IPv6，则端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。如果您使用IPv6地址描述端点网络接口，请注意该接口已启`denyAllIgwTraffic`用。

通过资源VPC端点访问资源

您可以使用VPC资源终端节点访问诸如域名、IP 地址或 Amazon RDS 数据库之类的资源。资源端点提供对资源的私有访问权限。创建资源终端节点时，可以指定单一、组或类型的资源配置ARN。一个资源端点只能与一个资源配置相关联。资源配置可以代表单个资源或一组资源。

先决条件

要创建资源终端节点，必须满足以下先决条件。

- 您必须拥有由您创建或通过其他账户与您共享的资源配置 AWS RAM。
- 如果从其他账户与您共享资源配置，则必须查看并接受包含该资源配置的资源共享。有关更多信息，请参阅《AWS RAM 用户指南》中的接受和拒绝邀请。

创建VPC资源端点

使用以下过程创建VPC资源端点。

创建VPC资源端点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 您可以指定一个名称，以便更轻松地查找和管理终端节点。
5. 在 “类型” 中，选择 “资源”。
6. 对于资源配置，请选择与您共享的资源配置。
7. 在 “网络设置” 中，选择要VPC从中访问资源的。
8. 如果要配置私人DNS支持，请选择 “其他设置”、“启用DNS名称”。要使用此功能，请确保启用启用DNS主机名和启用DNSVPC支持属性。
9. 选择创建端点。

使用命令行创建资源端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

管理资源端点

创建资源端点后，您可以更新其配置。

任务

- 删除 端点。
- 更新端点

删除 端点。

使用完VPC终端节点后，可以将其删除。

使用控制台删除终端节点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。

3. 选择端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

使用命令行删除端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

更新端点

您可以更新VPC终端节点。

使用控制台更新终端节点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择端点。
4. 选择操作和相应的选项。
5. 按照控制台步骤提交更新。

使用命令行更新端点

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

资源的VPC资源配置

资源配置表示您希望允许其他VPCs和账户中的客户访问的资源或一组资源。通过定义资源配置，您可以允许VPC从其他客户端VPCs和账户中的资源进行私有、安全、单向的网络连接。资源配置绑定到资源网关，通过该资源网关接收流量。

内容

- 资源配置的类型

- 资源网关
- 资源定义
- 协议
- 端口范围
- 访问 资源
- 与服务网络类型关联
- 服务网络的类型
- 通过共享资源配置 AWS RAM
- 监控
- 在莱迪VPC思中创建资源配置
- 管理VPC莱迪思资源配置的关联

资源配置的类型

资源配置可以有几种类型。不同的类型有助于代表不同类型的资源。错误类型包括：

- 单一资源配置：IP 地址或域名。它可以独立共享。
- 组资源配置：代表节点群集的子资源配置集合。它可以独立共享。
- 子资源配置：组资源配置的成员。它代表一个 IP 地址或域名。它不能独立共享；只能作为群组的一部分共享。它可以无缝地在群组中添加和删除。添加后，可以访问群组的用户可以自动访问该群组。
- ARN资源配置：表示由服务置备的支持的资源类型。 AWS 子资源配置由自动管理 AWS。

资源网关

资源配置与资源网关绑定。资源网关是一组资源网关ENIs，用作资源所在VPC的入口点。多个资源配置可以绑定到同一个资源网关。当其他VPCs或账户中的客户访问您的资源时VPC，该资源会看到来自该资源网关的本地流量VPC。

资源定义

在资源配置中，通过以下方式之一标识资源：

- 按 A mazon 资源名称 (ARN)：由服务配置的支持的资源类型可以通过 AWS 服务来识别。ARN例如，亚马逊RDS数据库。

- 按域名目标划分：任何可公开解析的域名。
- 按 IP 地址：对于IPv4和IPv6，仅IPs支持VPC中。

协议

创建资源配置时，可以定义该资源将支持的协议。当前，仅支持该TCP协议。

端口范围

创建资源配置时，您可以定义它将接受请求的端口。不允许客户端通过其他端口进行访问。

访问 资源

消费者可以使用VPC终端节点直接访问资源配置，也可以通过服务网络直接访问资源配置。VPC作为消费者，您可以允许从您VPC访问您账户中的资源配置或通过其他账户与您共享的资源配置 AWS RAM。

- 直接访问资源配置

  您可以在中创建类型为 r AWS PrivateLink VPC esource（资源终端节点）的终端节点，VPC以便从您的私下访问资源配置VPC。有关如何创建资源端点的更多信息，请参阅AWS PrivateLink用户指南中的访问VPC资源。
- 通过服务网络访问资源配置

  您可以将资源配置关联到服务网络，并将您的VPC资源配置连接到服务网络。您可以通过关联或使用服务网络VPC端点将您VPC连接到 AWS PrivateLink 服务网络。

  有关服务网络关联的更多信息，请参阅管理VPC莱迪思服务网络的关联。

  有关服务网络VPC端点的更多信息，请参阅AWS PrivateLink 用户指南中的访问服务网络。

与服务网络类型关联

当您与使用者账户（例如 Account-B）共享资源配置时，Account-B 可以通过资源VPC端点直接访问资源配置，也可以通过服务网络访问资源配置。 AWS RAM

要通过服务网络访问资源配置，Account-B 必须将资源配置与服务网络相关联。服务网络可在账户之间共享。因此，Account-B 可以与 Account-C 共享其服务网络（资源配置与之关联），从而使您的资源可以从 Account-C 访问。

为了防止此类传递共享，您可以指定不能将您的资源配置添加到可在账户之间共享的服务网络中。如果您指定此项，则 Account-B 将无法将您的资源配置添加到共享或将来可以与其他账户共享的服务网络中。

服务网络的类型

当您通过 AWS RAM与其他账户（例如 Account-B）共享资源配置时，Account-B 可以通过以下三种方式之一访问该资源：

- 使用资源类型的VPC端点（资源VPC端点）。
- 使用服务网络类型的VPC端点（服务网络VPC端点）。
- 使用服务网络VPC关联。

对于服务网络VPC端点和服务网络VPC关联，必须将资源配置放在 Account-B 中的服务网络中。 服务网络可在账户之间共享。因此，Account-B 可以与 Account-C 共享其服务网络（包含资源配置），从而可以从账户 C 访问您的资源。 为了防止此类传递共享，您可以禁止将您的资源配置添加到可在账户之间共享的服务网络中。如果您不允许这样做，那么 Account-B 将无法将您的资源配置添加到共享或可以与其他账户共享的服务网络中。

通过共享资源配置 AWS RAM

资源配置与集成 AWS Resource Access Manager。您可以通过与其他账户共享您的资源配置 AWS RAM。当您与账户共享资源配置时，该 AWS 账户中的客户可以私下访问该资源。您可以使用中的资源共享共享共享资源配置 AWS RAM。

使用 AWS RAM 控制台查看您已添加到的资源共享、您可以访问的共享资源以及与您共享资源的 AWS 账户。有关更多信息，请参阅《AWS RAM 用户指南》中与您共享的资源。

要从与资源配置相同账户VPC中的其他账户访问资源，您无需通过共享资源配置 AWS RAM。

监控

您可以对资源配置启用监控日志。您可以选择要将日志发送到的目的地。

在莱迪VPC思中创建资源配置

使用控制台创建资源配置。

使用控制台创建资源配置

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格的PrivateLink 和莱迪思下，选择资源配置。
3. 选择创建资源配置。
4. 输入一个在您的 AWS 账户中唯一的名称。创建资源配置后，您无法更改此名称。
5. 对于配置类型，为单个资源或子资源选择资源，为一组子资源选择资源组。
6. 选择您之前创建的资源网关或立即创建一个资源网关。
7. 选择您希望此资源配置所代表的资源的标识符。
8. 选择要共享资源的端口范围。
9. 在关联设置中，指定此资源配置是否可以与可共享的服务网络相关联。
10. 对于共享资源配置，请选择标识可以访问此资源的委托人的资源共享。
11. （可选）对于监控，如果您要监控资源配置的请求和响应，请启用资源访问日志和传送目标。
12. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
13. 选择创建资源配置。

要使用创建资源配置 AWS CLI

使用 create-resource-configuration 命令。

管理VPC莱迪思资源配置的关联

您与之共享资源配置的消费者账户以及您的账户中的客户端可以直接使用资源VPC终端节点或通过服务网络终端节点访问资源配置。因此，您的资源配置将具有端点关联和服务网络关联。

管理服务网络关联

创建或删除服务网络关联。

使用控制台管理服务网络关联

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格的PrivateLink 和莱迪思下，选择资源配置。
3. 选择资源配置的名称以打开其详细信息页面。
4. 选择服务网络关联选项卡。
5. 选择创建关联。

6. 从VPC莱迪思服务网络中选择一个服务网络。要创建服务网络，请选择创建VPC莱迪思网络。
7. （可选）要添加标签，请展开服务关联标签，选择添加新标签，然后输入标签键和标签值。
8. 选择 Save changes（保存更改）。
9. 要删除关联，请选中关联的复选框，然后选择操作，删除。提示进行确认时，输入 **`confirm`**，然后选择 Delete（删除）。

使用创建服务网络关联 AWS CLI

使用 create-service-network-resource-association 命令。

要删除服务网络关联，请使用 AWS CLI

使用 delete-service-network-resource-association 命令。

管理VPC端点关联

管理VPC端点关联。

使用控制台管理VPC端点关联

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格的PrivateLink 和莱迪思下，选择资源配置。
3. 选择资源配置的名称以打开其详细信息页面。
4. 选择 “端点关联” 选项卡。
5. 选择关联 ID 以打开其详细信息页面。在这里，您可以修改或删除关联。
6. 要创建新的端点关联，请转到左侧导航窗格中的PrivateLink 和莱迪思，然后选择终端节点。
7. 选择创建终端节点。
8. 选择要连接到您的资源配置VPC。
9. 选择VPC、子网和安全组。
10. （可选）要标记您的VPC终端节点，请选择添加新标签，然后输入标签密钥和标签值。
11. 选择创建端点。

要创建VPC端点关联，请使用 AWS CLI

使用 create-vpc-endpoint 命令。

要删除VPC端点关联，请使用 AWS CLI

使用 delete-vpc-endpoint 命令。

莱迪VPC思的资源网关

资源网关是进入资源所在地的VPC入口点。它跨越多个可用区。为了使您的资源可以从所有可用区域访问，您应该创建资源网关，使其跨越尽可能多的可用区。

如果您计划让其他VPCs或账户可以VPC访问其中的资源，则VPC必须拥有资源网关。您共享的每个资源都绑定到资源网关。当其他VPCs或账户中的客户访问您的资源时VPC，该资源会看到来自该资源网关的本地流量VPC。流量的源 IP 是资源网关的 IP。您可以为资源网关分配多个 IP 地址，以允许与该资源建立更多网络连接。中的多个资源VPC可以绑定到同一个资源网关。

资源网关不提供负载平衡功能。

内容

安全组

您可以将安全组附加到资源网关。资源网关的安全组规则控制从资源网关到资源的出站流量。

从资源网关流向数据库资源的流量推荐的出站规则

要使流量从资源网关流向资源，必须为资源接受的侦听器协议和端口范围创建出站规则。

目标位置	协议	端口范围	注释
CIDR range for resource	TCP	3306	允许从资源网关到数据库的流量。

IP 地址类型

资源网关可以有IPv4IPv6或双栈地址。资源网关的 IP 地址类型必须与资源网关的子网以及资源的 IP 地址类型兼容，如下所述：

- IPv4— 为您的网关网络接口分配IPv4地址。只有当所有选定的子网都有IPv4地址范围并且资源也有地址时，才支持此选项。IPv4
- IPv6— 为您的网关网络接口分配IPv6地址。仅当所有选定的子网仅为子网并且资源还有地址时，IPv6才支持此选项。IPv6
- Dualstack — 将IPv4和IPv6地址分配给您的网关网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围，并且资源具有IPv4或IPv6地址时，才支持此选项。

资源网关的 IP 地址类型与客户端的 IP 地址类型或访问资源的VPC终端节点无关。

在VPC莱迪思创建资源网关

使用控制台创建资源网关。

使用控制台创建资源网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的PrivateLink 和莱迪思下，选择资源网关。
3. 选择创建资源网关。
4. 输入一个在您的 AWS 账户中唯一的名称。
5. 选择资源网关的 IP 类型。
6. 选择资源所在VPC的。
7. 最多选择五个安全组来控制从服务网络VPC到的入站流量。
8. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入该标签的键和值。
9. 选择创建资源网关。

要使用创建资源网关 AWS CLI

使用 create-resource-gateway 命令。

在莱迪VPC思中删除资源网关

使用控制台删除资源网关。

使用控制台删除资源网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。

2. 在导航窗格中的PrivateLink 和莱迪思下，选择资源网关。
3. 选中要删除的资源网关的复选框，然后选择操作，删除。提示进行确认时，输入 **`confirm`**，然后选择 Delete（删除）。

要删除资源网关，请使用 AWS CLI

使用 delete-resource-gateway 命令。

通过以下方式访问服务网络 AWS PrivateLink

您可以使用服务网络VPC终端节点（服务网络终端节点）私密连接到服务网络。VPC服务网络终端节点允许您私密安全地访问与服务网络关联的资源和服务。这样，您就可以通过单个VPC端点私密访问多个资源和服务。

服务网络是资源配置和VPC莱迪思服务的逻辑集合。使用服务网络终端节点，您可以将服务网络连接到您的VPC，并从您VPC或从本地私下访问这些资源和服务。服务网络端点允许您连接到一个服务网络。要从您的连接到多个服务网络VPC，您可以创建多个服务网络终端节点，每个终端节点都指向不同的服务网络。

服务网络与 AWS Resource Access Manager (AWS RAM) 集成。您可以通过与其他帐户共享您的服务网络 AWS RAM。当您与其他 AWS 账户共享服务网络时，该账户可以创建服务网络终端节点来连接到服务网络。您可以使用中的资源共享共享服务网络 AWS RAM。

使用 AWS RAM 控制台查看您已添加到的资源共享、您可以访问的共享服务网络以及与您共享资源的 AWS 账户。有关更多信息，请参阅《AWS RAM 用户指南》中与您共享的资源。

定价

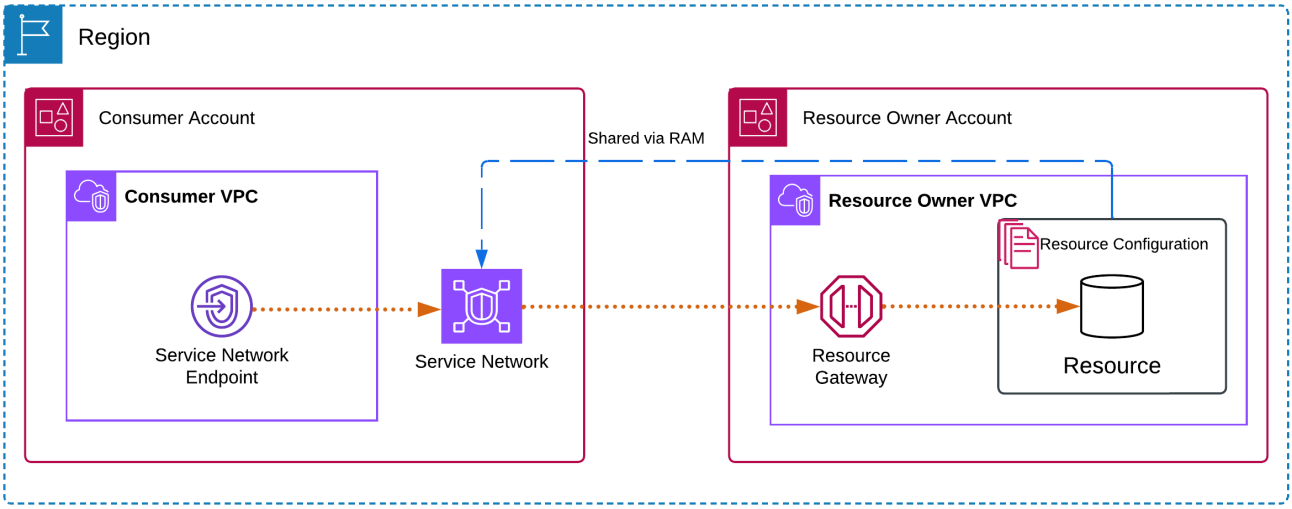
与您的服务网络关联的资源配置按小时计费。当您通过服务网络VPC终端节点访问资源时，还会按处理的 GB 数据计费。您无需为服务网络VPC终端节点本身按小时计费。有关更多信息，请参阅 Amazon VPC Lattice 定价。

内容

概述

您可以创建自己的服务网络，也可以通过其他账户与您共享服务网络。无论哪种方式，您都可以创建一个服务网络终端节点，以便从您的VPC服务网络终端节点连接到该终端节点。有关如何创建服务网络并将资源配置与其关联的更多信息，请参阅 Amazon VPC Lattice 用户指南。

下图显示了您的服务网络终端节点如何VPC访问服务网络。



只能从具有服务网络终端节点的启动到服务网络中的资源和服务的网络连接。VPCVPC拥有资源和服务的，无法启动与终端节点的网络连接VPC。

DNS主机名

使用 AWS PrivateLink，您可以使用私有终端节点将流量发送到服务网络。当您创建服务网络VPC终端节点时，我们会为每种资源和服务创建区域DNSDNS名称（称为默认名称），您可以使用这些资源和服务与本地资源和服务进行通信。VPC

服务网络中资源的默认DNS名称具有以下语法：

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

服务网络中莱迪思服务的默认DNS名称采用以下语法：

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

当您的服务网络具有可用的资源配置时ARNs，您可以启用私有DNS。使用 privateDNS，您可以使用服务为资源配置的DNS名称继续向资源发出请求，同时通过 AWS 服务网络VPC终端节点利用私有连接。有关更多信息，请参阅 the section called “DNS分辨率”。

DNS分辨率

当您创建服务网络端点时，我们会为每个资源配置以及与服务网络关联的莱迪思服务创建DNS名称。这些DNS记录是公开的。因此，这些DNS名称是可以公开解析的。但是，来自外部的DNS请求VPC仍会返回服务网络端点网络接口的私有 IP 地址。只要您可以通过VPN或 Direct Connect 访问服务网络端点所在的VPC，就可以使用这些DNS名称从本地访问资源和服务。

私人 DNS

如果您DNS为服务网络VPC终端节点启用私有化，并且同时启用VPC了DNS主机名和DNS解析，则我们会为具有自定义名称的资源配置创建隐藏的托 AWS管私有托管区域。DNS托管区域包含资源默认DNS名称的记录集，该记录集可将其解析为您的服务网络终端节点网络接口的私有 IP 地址。VPC

Amazon 为您提供了一个名为 R oute 53 Resolver 的DNS服务器。VPCRoute 53 解析器会自动解析本地VPC域名并在私有托管区域中进行记录。但是，您不能从外部使用 Route 53 解析器。VPC如果您想从本地网络访问VPC终端节点，则可以使用默认DNS名称，也可以使用 Route 53 解析器终端节点和解析器规则。有关更多信息，请参阅AWS Transit Gateway 与 AWS PrivateLink 和集成 Amazon Route 53 Resolver。

子网和可用区

您可以为每个可用区配置一个子网的VPC终端节点。我们为您子网中的终端节点创建VPC终端节点网络接口。我们根据端点的 IP 地址类型为其子网中的每个VPC端点网络接口分配 IP 地址。在生产环境中，为了获得高可用性和弹性，我们建议为每个VPC终端节点配置至少两个可用区。

IP 地址类型

服务网络端点可以支持IPv4IPv6、或双栈地址。支持的端点IPv6可以用AAAA记录响应DNS查询。服务网络终端节点的 IP 地址类型必须与资源终端节点的子网兼容，如下所述：

- IPv4— 为您的端点网络接口分配IPv4地址。仅当所有选定的子网都有IPv4地址范围时，才支持此选项。
- IPv6— 为您的端点网络接口分配IPv6地址。仅当所有选定的子网仅为子网时，IPv6才支持此选项。

- Dualstack — 将IPv4和IPv6地址分配给您的端点网络接口。仅当所有选定的子网同时具有IPv4和IPv6地址范围时，才支持此选项。

如果服务网络VPC端点支持IPv4，则端点网络接口具有IPv4地址。如果服务网络VPC端点支持IPv6，则端点网络接口具有IPv6地址。无法通过互联网访问端点网络接口IPv6的地址。如果您使用IPv6地址描述端点网络接口，请注意该接口已启`denyAllIgwTraffic`用。

通过服务网络端点访问服务网络

您可以使用服务网络终端节点访问服务网络。服务网络端点提供对服务网络中资源配置和服务的私有访问权限。

先决条件

要创建服务网络终端节点，必须满足以下先决条件。

- 您必须拥有一个由您创建或通过其他账户与您共享的服务网络 AWS RAM。
- 如果服务网络是从另一个账户与您共享的，则必须查看并接受包含该服务网络的资源共享。有关更多信息，请参阅《AWS RAM 用户指南》中的接受和拒绝邀请。

创建服务网络端点

创建服务网络终端节点以访问与您共享的服务网络。

创建服务网络终端节点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 您可以指定名称以便更轻松地查找和管理终端节点。
5. 对于类型，选择服务网络。
6. 对于服务网络，请选择与您共享的服务网络。
7. 在 “网络设置” 中，选择您要VPC从中访问服务网络的。
8. 如果要配置私人DNS支持，请选择 “其他设置”、“启用DNS名称”。要使用此功能，请确保启用启用DNS主机名和启用DNSVPC支持属性。
9. 选择创建端点。

使用命令行创建服务网络端点

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

管理服务网络端点

创建服务网络终端节点后，您可以更新其配置。

任务

- 删除 端点。
- 更新服务网络端点

删除 端点。

使用完VPC终端节点后，可以将其删除。

使用控制台删除终端节点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择服务网络端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

使用命令行删除端点

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (适用于 Windows 的工具 PowerShell)

更新服务网络端点

您可以更新VPC终端节点。

使用控制台更新终端节点

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择端点。
4. 选择操作和相应的选项。
5. 按照控制台步骤提交更新。

使用命令行更新端点

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

的身份和访问管理 AWS PrivateLink

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。 IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 AWS PrivateLink 资源。 IAM无需支付额外费用即可使用。 AWS 服务

内容

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你所做的工作 AWS PrivateLink。

服务用户-如果您使用 AWS PrivateLink 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 AWS PrivateLink 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。

服务管理员-如果您负责公司的 AWS PrivateLink 资源，则可能拥有完全访问权限 AWS PrivateLink。您的工作是确定您的服务用户应访问哪些 AWS PrivateLink 功能和资源。然后，您必须向 IAM 管理员提交请求，这样才能更改您的服务用户的权限。查看此页面的信息，了解 IAM 的基本概念。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写用于管理访问权限的策略 AWS PrivateLink。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户、IAM用户身份或通过担任IAM角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。在您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM用户指南》中的API请求AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的多因素身份验证和AWS IAM Identity Center 用户指南IAM中的AWS 多因素身份验证。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，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（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 Ident IAM ity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关IAM身份中心的信息，请参阅什么是IAM身份中心？ 在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

IAM用户是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组 是指定一个 IAM 用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并授予该群组管理IAM资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅用户指南中的IAMIAM用户用例。

IAM 角色

IAM角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但未与特定人员关联。要在中临时扮IAM演角色 AWS Management Console，可以从用户切换到IAM角色（控制台）。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建一个角色，并为该角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的为第三方身份提供商（联合）创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户存取 - 您可以使用 IAM 角色允许其他账户中的某个人（可信任主体）访问您账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

- 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。当你使用某些服务时，你可能会执行一个操作，然后在不同的服务中启动另一个操作。 FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。 FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两项操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。
- 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM用户指南》 AWS 服务中的创建角色以向委派权限。
- 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 AWS CLI 或 AWS API请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要为EC2实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅IAM用户指南中的使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以JSON文档的 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅《IAM用户指南》中的JSON策略概述。

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入这些角色。

IAM 策略定义操作的权限，无论您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的使用客户托管策略定义自定义IAM权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体（IAM用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。

- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。对成员账户中的实体（包括每个实体）的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 这些JSON策略可用于设置账户中资源的最大可用权限，而无需更新附加到您拥有的每项资源的IAM策略。这会RCP限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息RCPs，包括 AWS 服务 该支持的列表RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

AWS PrivateLink 如何使用 IAM

在使用管理IAM访问权限之前 AWS PrivateLink，请先了解哪些IAM功能可供使用 AWS PrivateLink。

IAM 功能	AWS PrivateLink 支持
基于身份的策略	是
基于资源的策略	Yes
策略操作	是
策略资源	Yes
策略条件键（特定于服务）	Yes
ACLs	不支持

IAM 功能	AWS PrivateLink 支持
ABAC（策略中的标签）	Yes
临时凭证	是
主体权限	Yes
服务角色	否
服务相关角色	否

要全面了解大多数IAM功能的使用方式 AWS PrivateLink 和其他 AWS 服务 功能，请参阅《IAM用户指南》IAM中与之配合使用的AWS 服务。

基于身份的策略 AWS PrivateLink

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的使用客户托管策略定义自定义IAM权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

基于身份的策略示例 AWS PrivateLink

要查看 AWS PrivateLink 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS PrivateLink

内部基于资源的政策 AWS PrivateLink

支持基于资源的策略：是

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的IAM管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM用户指南》IAM中的跨账户资源访问权限。

AWS PrivateLink 服务支持一种基于资源的策略，即终端节点策略。端点策略可控制哪些 AWS 主体可以使用端点访问端点服务。有关更多信息，请参阅 the section called “端点策略”。

的政策行动 AWS PrivateLink

支持策略操作：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON策略`Action`元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

ec2 命名空间中的操作

的某些操作 AWS PrivateLink 是 Amazon 的一部分EC2API。这些策略操作使用前`ec2`缀。有关更多信息，请参阅 Amazon EC2 API 参考中的AWS PrivateLink 操作。

vpce 命名空间中的操作

AWS PrivateLink 还提供仅`AllowMultiRegion`限权限的操作。此策略操作使用前`vpce`缀。

的政策资源 AWS PrivateLink

支持策略资源：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource`JSON策略元素指定要应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。最佳做法是，使用资源的 Amazon 资源名称 (ARN) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

的策略条件密钥 AWS PrivateLink

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，仅当 IAM 用户使用其 IAM 用户名进行标记时，您才可为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的AWS 全局条件上下文密钥。

以下条件键特定于 AWS PrivateLink：

- ec2:VpceMultiRegion
- ec2:VpceServiceName
- ec2:VpceServiceOwner
- ec2:VpceServicePrivateDnsName
- ec2:VpceServiceRegion
- ec2:VpceSupportedRegion

有关更多信息，请参阅 Amazon 的条件密钥EC2。

ACLs在 AWS PrivateLink

支持ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

ABAC与 AWS PrivateLink

支持ABAC（策略中的标签）：是

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在中 AWS，这些属性称为标签。您可以将标签附加到IAM实体（用户或角色）和许多 AWS 资源。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关更多信息ABAC，请参阅《IAM用户指南》中的使用ABAC授权定义权限。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的使用基于属性的访问控制 (ABAC)。

将临时证书与 AWS PrivateLink

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关其他信息，包括哪些 AWS 服务 适用于临时证书 AWS 服务 ，请参阅《IAM用户指南》IAM中的 “适用于临时证书”。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《用户指南》中的从IAM用户切换到IAM角色（控制台）。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅中的临时安全证书IAM。

的跨服务主体权限 AWS PrivateLink

支持转发访问会话 (FAS)：是

当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。当你使用某些服务时，你可能会执行一个操作，然后在不同的服务中启动另一个操作。 FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。 FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两项操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。

的服务角色 AWS PrivateLink

支持服务角色：否

服务角色是由一项服务代入、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM用户指南》 AWS 服务中的创建角色以向委派权限。

的服务相关角色 AWS PrivateLink

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

基于身份的策略示例 AWS PrivateLink

默认情况下，用户和角色没有创建或修改 AWS PrivateLink 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或来执行任务 AWS API。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的创建IAM策略（控制台）。

有关由 AWS PrivateLink定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》EC2中的 Amazon 操作、资源和条件密钥。ARNs

示例

控制VPC端点的使用

默认情况下，用户无权使用终端节点。您可以创建一个基于身份的策略，向用户授予创建、修改、描述和删除端点的权限。示例如下：

```
{
    "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 “端点策略”。

根据服务所有者控制VPC终端节点的创建

您可以使用ec2:VpceServiceOwner条件密钥根据谁拥有服务（amazonaws-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服务所有者创建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:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
```

```
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

控制可以为VPC终端节点服务指定的私有DNS名称

您可以使用ec2:VpceServicePrivateDnsName条件密钥根据与VPC终端节点服务关联的私有DNS名称来控制可以修改或创建哪些VPC终端节点服务。以下示例授予使用指定私有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:account-id:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
```

```
                }
            }
        }
    ]
}
```

控制可以为VPC终端节点服务指定的服务名称

您可以使用ec2:VpceServiceName条件密钥根据VPC终端节点服务名称来控制可以创建哪些VPC端点。以下示例授予使用指定服务名称创建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:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.s3"
                    ]
                }
            }
        }
    ]
}
```

使用VPC端点策略控制对端点的访问

终端节点策略是一种基于资源的策略，您可以将其附加到VPC终端节点，以控制哪些 AWS 委托人可以使用该终端节点访问终端节点。 AWS 服务

端点策略不会覆盖或取代基于身份的策略或基于资源的策略。例如，如果您使用接口终端节点连接到 Amazon S3，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VPCs终端节点访问存储桶。

内容

注意事项

- 端点策略是使用JSON策略语言的IAM策略文档。其中必须包含一个 Principal 元素。端点策略的大小不得超过 20480 个字符（包含空格）。
- 在为创建接口或网关终端节点时 AWS 服务，可以将单个终端节点策略附加到该终端节点。您可以随时更新端点策略。如果您不附加端点策略，我们将附加默认端点策略。
- 并非所有都 AWS 服务 支持端点策略。如果 AWS 服务 不支持终端节点策略，则我们允许对该服务的任何终端节点进行完全访问权限。有关更多信息，请参阅 the section called “查看端点策略支持”。
- 当您为除以外的VPC终端节点服务创建终端节点时 AWS 服务，我们允许对该终端节点进行完全访问权限。
- 对于引用系统生成的标识符的全局上下文键（例如，`aws:PrincipalAccount` 或 `aws:SourceVpc`），您不能使用通配符 (* or ?) 或数字条件运算符。
- 使用字符串条件运算符时，您必须在每个通配符之前或之后使用至少六个连续字符。
- 当您在资源或条件元素ARN中指定时，的账户部分ARN可以包含账户 ID 或通配符，但不能同时包含两者。

默认端点策略

默认端点策略授予对端点的完全访问权限。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

接口端点策略

有关终端节点策略的示例 AWS 服务，请参阅the section called “与…集成的服务”。表中的第一列包含每个 AWS PrivateLink 文档的链接 AWS 服务。如果 AWS 服务 支持端点策略，则其文档包括端点策略示例。

网关端点的主体

对于网关端点，必须将 `Principal` 元素设置为 `*`。要指定主体，请使用 `aws:PrincipalArn` 条件键。

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

如果您使用以下格式指定主体，则访问权限只会授予 AWS 账户根用户 ，而非该账户的所有用户和角色。

```
"AWS": "account_id"
```

有关网关端点的端点策略示例，请参阅以下内容：

- 适用于 Amazon S3 的端点

- 适用于 DynamoDB 的端点

更新VPC终端节点策略

按照以下步骤更新 AWS 服务的端点策略。在更新完端点策略后，您所做的更改可能需要几分钟才能生效。

使用控制台更新端点策略

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择VPC终端节点。
4. 依次选择 Actions（操作）、Manage policy（管理策略）。
5. 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）并附加自定义策略。
6. 选择保存。

使用命令行更新端点策略

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint（适用于 Windows 的工具 PowerShell）

AWS 的托管策略 AWS PrivateLink

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 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， AWS 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 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 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）。 AWS 当新服务启动或现有服务 AWS 服务 有新API操作可用时，最有可能更新 AWS 托管策略。

有关更多信息，请参阅 IAM IAM 用户指南中的 AWS 托管式策略。

AWS PrivateLinkAWS 托管策略的更新

查看 AWS PrivateLink 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “ AWS PrivateLink 文档历史记录” 页面上的订阅RSS源。

更改	描述	日期
AWS PrivateLink 开始跟踪更改	AWS PrivateLink 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 1 日

CloudWatch 的指标 AWS PrivateLink

AWS PrivateLink 将您的接口终端节点、Gateway Load Balancer 终端节点和终端节点服务的数据点发布到 Amazon CloudWatch 。 CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。每个数据点都有关联的时间戳和可选的测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控指定的指标，并在该指标超出您认为可接受的范围时启动操作（例如向电子邮件地址发送通知）。

将会发布所有接口端点、Gateway Load Balancer 端点和端点服务的指标。但不会发布网关端点的指标。默认情况下，每隔一分钟 AWS PrivateLink 向发送指标，无需支付额外费用。 CloudWatch

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

端点指标和维度

AWS/PrivateLinkEndpoints 命名空间包括有关接口端点和 Gateway Load Balancer 端点的下列指标。

指标	描述
ActiveConnections	并发活动连接的数量。这包括处于 SYN _ SENT 和ESTABLISHED状态的连接。 报告标准：端点在一分钟内收到了流量。 统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。 维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id

指标	描述
	• Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
BytesProcessed	在端点和端点服务之间交换的字节数，双向汇总。这是端点拥有者需要付费的字节数。账单将以 GB 为单位显示此值。 报告标准：端点在一分钟内收到了流量。 统计数据：最有用的统计数据是 Average、Sum、Maximum 和 Minimum。 维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
NewConnections	通过此端点建立的新连接数量。 报告标准：端点在一分钟内收到了流量。 统计数据：最有用的统计数据是 Average、Sum、Maximum 和 Minimum。 维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

指标	描述
PacketsDropped	此端点丢弃的数据包数量。此指标可能无法捕获所有丢包。值增加可能代表端点或端点服务运行不正常。 报告标准：端点在一分钟内收到了流量。 统计数据：最有用的统计工具是 Average、Sum 和 Maximum。 维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
RstPacketsReceived	端点收到RST的数据包数量。值增加可能代表端点服务运行不正常。 报告标准：端点在一分钟内收到了流量。 统计数据：最有用的统计工具是 Average、Sum 和 Maximum。 维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

要筛选这些指标，请使用以下维度。

维度	描述
Endpoint Type	按端点类型筛选指标数据（Interface | GatewayLoadBalancer）。
Service Name	按服务名称筛选指标数据。
Subnet Id	按子网筛选指标数据。
VPC Endpoint Id	按VPC端点筛选指标数据。

维度	描述
VPC Id	按VPC筛选指标数据。

端点服务指标和维度

AWS/PrivateLinkServices 命名空间包括有关端点服务的下列指标。

指标	描述
ActiveConnections	通过端点从客户端到目标的最大活动连接数量。值增加可能代表需要增加指向负载均衡器的目标。 报告标准：连接到端点服务的端点在一分钟内发送了流量。 统计数据：最有用的统计工具为 Average 和 Maximum。 维度 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
BytesProcessed	在端点服务和端点之间交换的字节数，双向汇总。 报告标准：连接到端点服务的端点在一分钟内发送了流量。 统计数据：最有用的统计工具是 Average、Sum 和 Maximum。 维度 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id

指标	描述
	• Service Id, VPC Endpoint Id
EndpointsCount	连接到端点服务的端点数量。 报告标准：在五分钟时间内有非零值。 统计数据：最有用的统计工具为 Average 和 Maximum。 维度 • Service Id
NewConnections	通过端点从客户端到目标建立的新连接数量。值增加可能代表需要增加指向负载均衡器的目标。 报告标准：连接到端点服务的端点在一分钟内发送了流量。 统计数据：最有用的统计工具是 Average、Sum 和 Maximum。 维度 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

指标	描述
RstPacketsSent	终端节点服务发送到端点RST的数据包数量。值增加可能代表存在运行不正常的目标。 报告标准：连接到端点服务的端点在一分钟内发送了流量。 统计数据：最有用的统计工具是 Average、Sum 和 Maximum。 维度 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

要筛选这些指标，请使用以下维度。

维度	描述
Az	按可用区筛选指标数据。
Load Balancer Arn	按负载均衡器筛选指标数据。
Service Id	按端点服务筛选指标数据。
VPC Endpoint Id	按VPC端点筛选指标数据。

查看 CloudWatch 指标

您可以使用 Amazon VPC 控制台、控制 CloudWatch 台或以下 AWS CLI 方式查看这些 CloudWatch 指标。

使用 Amazon VPC 控制台查看指标

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。选择您的端点，然后选择 Monitoring（监控）选项卡。
3. 在导航窗格中，选择 Endpoint services（端点服务）。选择您的端点服务，然后选择 Monitoring（监控）选项卡。

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，选择指标。
3. 选择 AWS/命PrivateLinkEndpoints名空间。
4. 选择 AWS/命PrivateLinkServices名空间。

要查看指标，请使用 AWS CLI

使用以下 list-metrics 命令列出接口端点和 Gateway Load Balancer 端点的可用指标：

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

使用以下 list-metrics 命令列出端点服务的可用指标：

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

使用内置的 Contributor Insights 规则

AWS PrivateLink 为您的终端节点服务提供内置的 “贡献者见解” 规则，以帮助您找出哪些端点是每个受支持指标的最大贡献者。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的 “贡献者见解”。

AWS PrivateLink 提供了以下规则：

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` – 按活动连接数进行端点排名。
- `VpcEndpointService-BytesByEndpointId-v1` – 按处理的字节数进行端点排名。
- `VpcEndpointService-NewConnectionsByEndpointId-v1` – 按新连接数进行端点排名。

- `VpcEndpointService-RstPacketsByEndpointId-v1`— 根据发送到端点RST的数据包数量对端点进行排名。

在使用内置规则之前，必须先启用规则。启用规则后，将开始收集贡献者数据。有关《投稿人见解》收费的信息，请参阅 Amazon CloudWatch 定价。

您必须具有以下权限才能使用 Contributor Insights：

- `cloudwatch:DeleteInsightRules` – 删除 Contributor Insights 规则。
- `cloudwatch:DisableInsightRules` – 禁用 Contributor Insights 规则。
- `cloudwatch:GetInsightRuleReport` – 获取数据。
- `cloudwatch:ListManagedInsightRules` – 列出可用的 Contributor Insights 规则。
- `cloudwatch:PutManagedInsightRules` – 启用 Contributor Insights 规则。

任务

- 启用 Contributor Insights 规则
- 禁用 Contributor Insights 规则
- 删除 Contributor Insights 规则

启用 Contributor Insights 规则

使用以下过程启用 AWS PrivateLink 使用 AWS Management Console 或的内置规则 AWS CLI。

启用 “投稿人见解” 规则以 AWS PrivateLink 使用控制台

1. 打开亚马逊VPC控制台，网址为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. 在 Contributor Insights 选项卡上，选择 Enable（启用）。
5. （可选）默认情况下，会启用所有规则。要仅启用特定规则，请选择无需启用的规则，然后依次选择 Actions（操作）、Disable rule（禁用规则）。当系统提示确认时，选择 Disable（禁用）。

启用 “投稿人见解” 规则以 AWS PrivateLink 使用 AWS CLI

1. 按如下方式使用list-managed-insight-rules命令枚举可用规则。对于--resource-arn选项，请指定您的终端节点服务的。ARN

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. 在 list-managed-insight-rules 命令的输出中，从 TemplateName 字段中复制模板名称。以下是该字段的示例。

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. 按如下方式使用put-managed-insight-rules命令启用规则。您必须指定模板名称和终ARN端节点服务的名称。

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

禁用 Contributor Insights 规则

您可以 AWS PrivateLink 随时禁用内置规则。禁用规则后，将停止收集贡献者数据，但现有的贡献者数据会保留 15 天。禁用规则后，您可以再次启用规则，以继续收集贡献者数据。

禁用 “投稿人见解” 规则以 AWS PrivateLink 使用控制台

1. 打开亚马逊VPC控制台，网址为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. 在 Contributor Insights 选项卡上，选择 Disable all（全部禁用），以禁用全部规则。或者，展开 Rules（规则）面板，选择要禁用的规则，然后依次选择 Actions（操作）、Disable rule（禁用规则）
5. 当系统提示确认时，选择 Disable（禁用）。

禁用 “投稿人见解” 规则以 AWS PrivateLink 使用 AWS CLI

使用disable-insight-rules命令禁用规则。

删除 Contributor Insights 规则

使用以下过程删除 AWS PrivateLink 使用 AWS Management Console 或的内置规则 AWS CLI。删除规则后，将停止收集贡献者数据，同时会删除现有的贡献者数据。

删除用于 AWS PrivateLink 使用控制台的 “投稿人见解” 规则

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择 Insights、Contributor Insights。
3. 展开 Rules（规则）面板，选择规则。
4. 然后依次选择 Actions（操作）、Delete rule（删除规则）。
5. 当系统提示进行确认时，选择 Delete（删除）。

删除投稿人见解的 AWS PrivateLink 使用规则 AWS CLI

使用delete-insight-rules命令删除规则。

AWS PrivateLink 配额

您的 AWS 账户对每项 AWS 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。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。

要请求提高限额，请参阅《服务限额用户指南》中的请求提高限额。

请求节流

的API操作 AWS PrivateLink 是 Amazon 的一部分EC2API。亚马逊在该EC2级别限制其API请求。AWS 账户 有关更多信息，请参阅《A mazon EC2 开发者指南》中的请求限制。此外，还会在组织级别限制API请求，以帮助提高绩效。 AWS PrivateLink如果您正在使用 AWS Organizations ，但仍处于账户级别API限制之内时收到RequestLimitExceeded错误代码，请参阅如何识别拨打大量电话的AWS API账户。如果您需要帮助，请联系您的客户团队或使用VPC服务和 “VPC终端节点” 类别提交技术支持案例。请务必附上 RequestLimitExceeded 错误代码的图片。

VPC端点配额

您的 AWS 账户具有以下与VPC终端节点相关的配额。

名称	默认值	可调整	注释
每个接口和网关 Load Balancer 终端节点 VPC	50	是	它是接口端点和网关负载均衡器端点的组合配额。
每个区域的网关VPC终端节点	20	是	每个网关终端节点最多可以创建 255 个 VPC
每个VPC端点的字符数策略	20,480	否	VPC终端节点策略的最大大小，包括空格

以下注意事项适用于通过VPC终端节点的流量：

- 默认情况下，每个VPC端点可以支持每个可用区高达 10 Gbps 的带宽，并且可以自动扩展到 100 Gbps。在所有可用区之间分配负载时，VPC终端节点的最大带宽是可用区域的数量乘以 100 Gbps。如果您的应用程序需要更高的吞吐量，请联系 AWS Support。

- 网络连接的最大传输单位 (MTU) 是可以通过VPC端点的最大允许数据包的大小（以字节为单位）。越大MTU，单个数据包中可以传递的数据就越多。VPC端点支持 8500 字节。MTU到达VPC端点的大小超过 8500 字节的数据包将被丢弃。
- 不支持路径MTU发现 (PMTUD)。VPC端点不会生成以下ICMP消息：`Destination Unreachable: Fragmentation needed and Don't Fragment was Set`（类型 3，代码 4）。
- VPC端点对所有数据包强制执行最大分段大小 (MSS) 限制。有关更多信息，请参阅RFC879。

的文档历史记录 AWS PrivateLink

下表描述了的版本 AWS PrivateLink。

变更	说明	日期
访问资源和服务网络	AWS PrivateLink 支持跨账户边界访问资源VPC和服务网络。	2024 年 12 月 1 日
跨区域访问	服务提供商可以在一个区域托管服务，并在一组 AWS 区域中提供该服务。服务使用者在创建终端节点时选择服务区域。	2024 年 11 月 26 日
指定的 IP 地址	在创建或修改终端节点时，您可以为终端节点网络接口指定 IP 地址。VPC	2023 年 8 月 17 日
IPv6 支持	您可以将 Gateway Load Balancer 终端节点服务和 Gateway Load Balancer 端点配置为同时IPv4支持IPv6IPv6地址或仅支持地址。	2022 年 12 月 12 日
Contributor Insights	您可以使用内置的 “贡献者见解” 规则来识别特定终端节点，这些端点是其 CloudWatch 指标的最大贡献者 AWS PrivateLink。	2022 年 8 月 18 日
IPv6 支持	服务提供商可以允许其终端节点服务接受IPv6请求，即使其后端服务仅支持也是如此IPv4。如果终端节点服务接受IPv6请求，则服务使用者可以启用对其接口终端节点的IPv6	2022 年 5 月 11 日

	支持，以便他们可以通过访问终端节点服务IPv6。	
CloudWatch 指标	AWS PrivateLink 发布您的接口终端节点、Gateway Load Balancer 终端节点和终端节点服务的 CloudWatch 指标。	2022 年 1 月 27 日
网关负载均衡器端点	您可以在中创建 Gateway Load Balancer VPC 终端节点，将流量路由VPC到您使用网关负载均衡器配置的终端节点服务。	2020 年 11 月 10 日
VPC端点策略	您可以将IAM策略附加到 AWS 服务的接口VPC终端节点，以控制对服务的访问。	2020 年 3 月 23 日
VPC终端节点和终端节点服务的条件密钥	您可以使用EC2条件键来控制对VPC端点和终端节点服务的访问。	2020 年 3 月 6 日
在创建时标记VPC终端节点和终端节点服务	您可以在创建VPC终端节点和终端节点服务时添加标签。	2020 年 2 月 5 日
私人DNS名字	您可以使用私人DNS名称从您的VPC内部访问 AWS PrivateLink 基于的服务。	2020 年 1 月 6 日
VPC端点服务	您可以创建自己的终端节点服务，并允许其他 AWS 账户 用户通过接口VPC终端节点连接到您的服务。您可以在 AWS Marketplace中将您的端点服务上架以开放订阅。	2017 年 11 月 28 日
的接口VPC端点 AWS 服务	AWS PrivateLink 无需使用 Internet 网关或NAT设备即可创建用于 AWS 服务 连接的接口终端节点。	2017 年 11 月 8 日

VPCDynamoDB 的终端节点	您可以创建网关VPC终端节点，以便在不使用互联网网关或设备的情况下从VPC您的设备访问 Amazon DynamoDB。NAT	2017 年 8 月 16 日
VPC亚马逊 S3 的终端节点	您可以创建网关VPC终端节点，以便在VPC不使用互联网网关或NAT设备的情况下从您的设备访问 Amazon S3。	2015 年 5 月 11 日

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。