AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

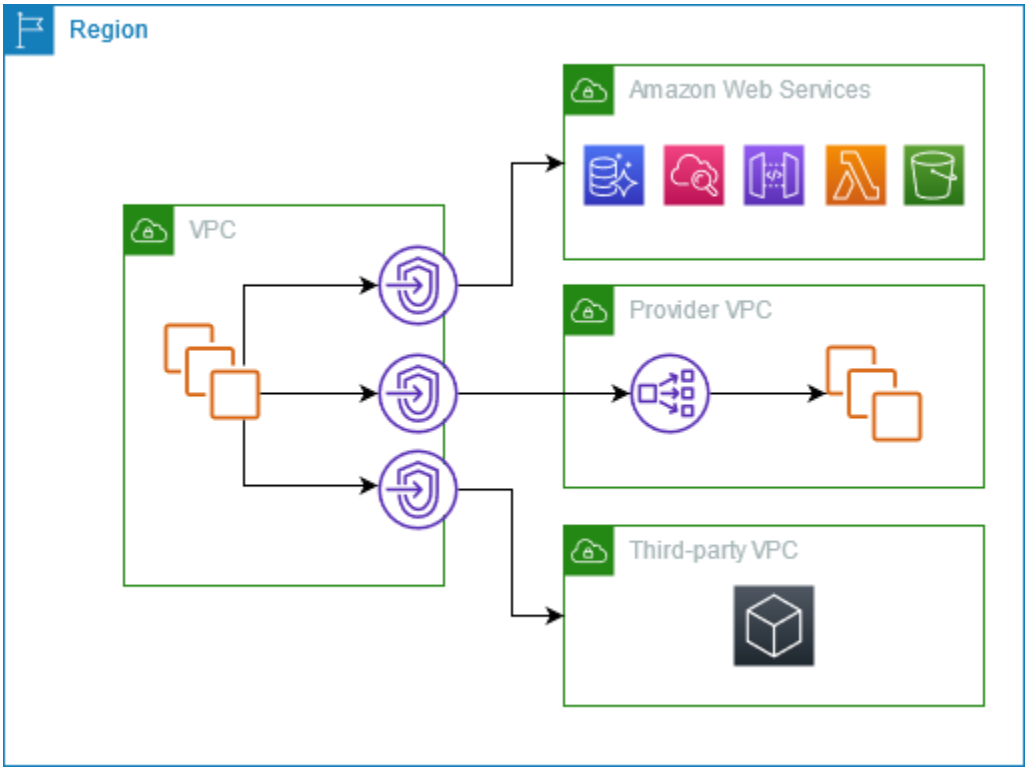
什么是 AWS PrivateLink？

AWS PrivateLink 是一种高度可用、可扩展的技术，您可以使用它以私密方式将您的 VPC 连接到服务，就像这些服务位于您的 VPC 中一样。您无需使用互联网网关、NAT 设备、公有 IP 地址、 AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接即可允许从您的私有子网与服务进行通信。因此，您可以控制可从 VPC 访问的特定 API 端点、站点和服务。

使用案例

您可以创建 VPC 终端节点，将 VPC 中的资源连接到与集成的服务 AWS PrivateLink。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”。

在下列示意图中，左侧的 VPC 拥有位于一个私有子网中的多个 EC2 实例和三个接口 VPC 端点。最顶端的 VPC 终端节点连接到。 AWS 服务中间 VPC 终端节点连接到另一个终端节点托管的服务 AWS 账户 （VPC 终端节点服务）。底部 VPC 终端节点连接到 AWS Marketplace 合作伙伴服务。



了解更多信息

- 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

与 VPC 端点结合使用

您可以使用以下任一方式创建、访问和管理 VPC 端点：

- 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:: EndpointConnection VPC 通知
  - AWS::EC2::VPCEndpointService
  - AWS:: EC2:: EndpointService VPC 权限
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS 软件开发工具包 — 提供特定语言的 API。 开发工具包关注许多连接详细信息，比如计算签名、处理请求重试和处理错误。有关更多信息，请参阅构建工具 AWS。
- 查询 API — 提供您使用 HTTPS 请求调用的低级别 API 操作。使用查询 API 是访问 Amazon VPC 的最直接方式。但是，它需要您的应用程序处理低级别的详细信息，例如生成哈希值以签署请求以及处理错误。有关更多信息，请参阅《Amazon EC2 API 参考》中的 AWS PrivateLink 操作。

定价

有关 VPC 端点定价的信息，请参阅 AWS PrivateLink 定价。

AWS PrivateLink 概念

您可以使用 Amazon VPC 定义虚拟私有云（VPC），这是一个逻辑隔离虚拟网络。您可以在 VPC 中启动 AWS 资源。您可以允许 VPC 中的资源连接到该 VPC 外部的资源。例如，向 VPC 添加互联网网

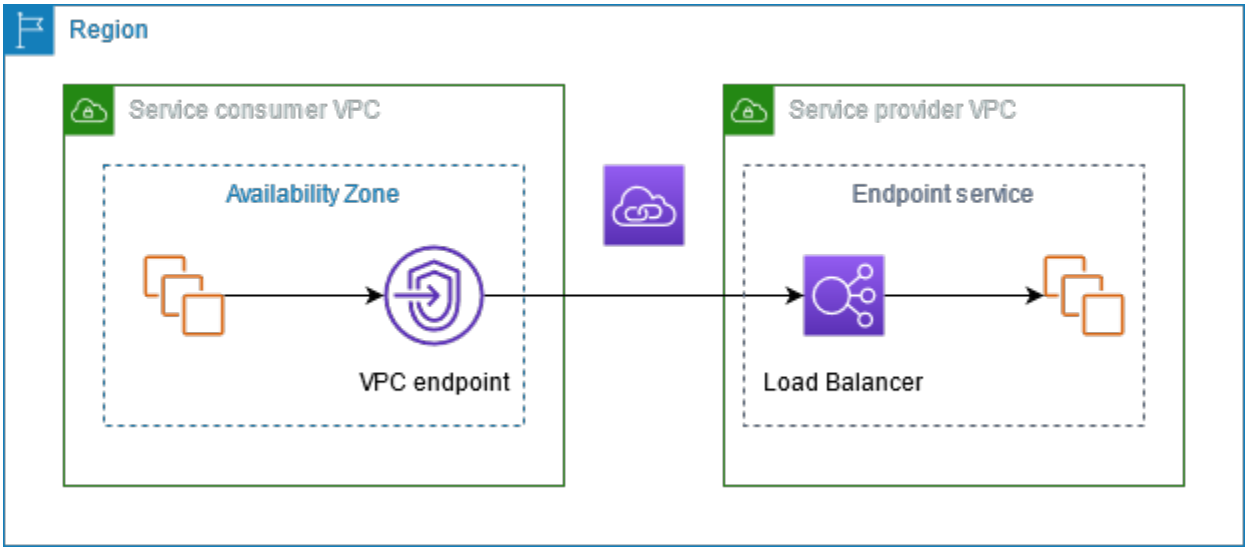
关以允许访问互联网，或添加 VPN 连接以允许访问您的本地网络。或者，使用 AWS PrivateLink 允许您的 VPC 中的资源使用私有 IP 地址连接到其他 VPC 中的服务，就像这些服务直接托管在您的 VPC 中一样。

以下是开始使用 AWS PrivateLink时需要理解的重要概念。

内容

架构示意图

下图简要概述了 AWS PrivateLink 工作原理。服务使用者创建接口 VPC 端点以连接到由服务提供商托管的端点服务。



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。

概念

- 端点服务

- 服务名称
- 服务状态

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。在创建 VPC 端点时，服务使用者必须指定服务名称。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。

服务使用者

服务的用户为服务使用者。服务使用者可以从 AWS 资源（例如 EC2 实例）或本地服务器访问终端节点服务。

概念

- VPC 端点
- 端点网络接口
- 端点策略
- 端点状态

VPC 端点

服务使用者可以创建 VPC 端点以将其 VPC 连接到端点服务。在创建 VPC 端点时，服务使用者必须指定端点服务的服务名称。VPC 端点有多种类型。您可以创建端点服务要求的 VPC 端点类型。

- `Interface` - 创建一个接口端点以将 TCP 流量发送到端点服务。发往端点服务的流量使用 DNS 进行解析。
- `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。您使用路由表将流量从您的 VPC 路由到网关负载均衡器端点。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。

还有另一种类型的 VPC 端点 `Gateway` ，它会创建一个网关端点来向 AmazonS3 或 DynamoDB 发送流量。与其他类型的 VPC 终端节点不同 AWS PrivateLink，网关终端节点不使用。有关更多信息，请参阅 the section called “网关端点”。

端点网络接口

端点网络接口是一个请求者管理的网络接口，其用作发往端点服务的流量的入口点。对于您在创建 VPC 端点时指定的每个子网，我们将在子网中创建一个端点网络接口。

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。无法从互联网访问端点网络接口的 IPv6 地址。当您使用 IPv6 地址描述端点网络接口时，请注意已启用 `denyAllIgwTraffic`。

端点网络接口的 IP 地址在其 VPC 端点的生命周期内不会变更。

端点策略

VPC 端点策略是一种 IAM 资源策略，您可以将其附加到接口端点。此策略确定哪些主体可以使用 VPC 端点访问端点服务。默认 VPC 端点策略允许所有主体通过 VPC 端点对所有资源执行所有操作。

端点状态

创建 VPC 端点时，端点服务会收到连接请求。服务提供商可以接受或拒绝请求。如果服务提供商接受请求，则服务使用者进入 `Available` 状态后即可使用 VPC 端点。

以下是 VPC 端点可能具有的状态：

- `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 端点，则 VPC 端点将返回此状态。
- `Available` - VPC 端点可供使用。
- `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` - VPC 端点不可用。
- `Deleting` - 服务提供商删除了 VPC 端点，删除正在进行中。
- `Deleted` - VPC 端点已删除。

AWS PrivateLink 连接

来自您的 VPC 的流量使用 VPC 端点和端点服务之间的连接发送到端点服务。VPC 终端节点和终端节点服务之间的流量保留在 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。

通过接口 VPC 端点，服务使用者可以使用端点策略来控制哪些 IAM 主体可以使用 VPC 端点访问端点服务。

私有托管区

托管区是 DNS 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，记录指定如何在 VPC 中路由流量。

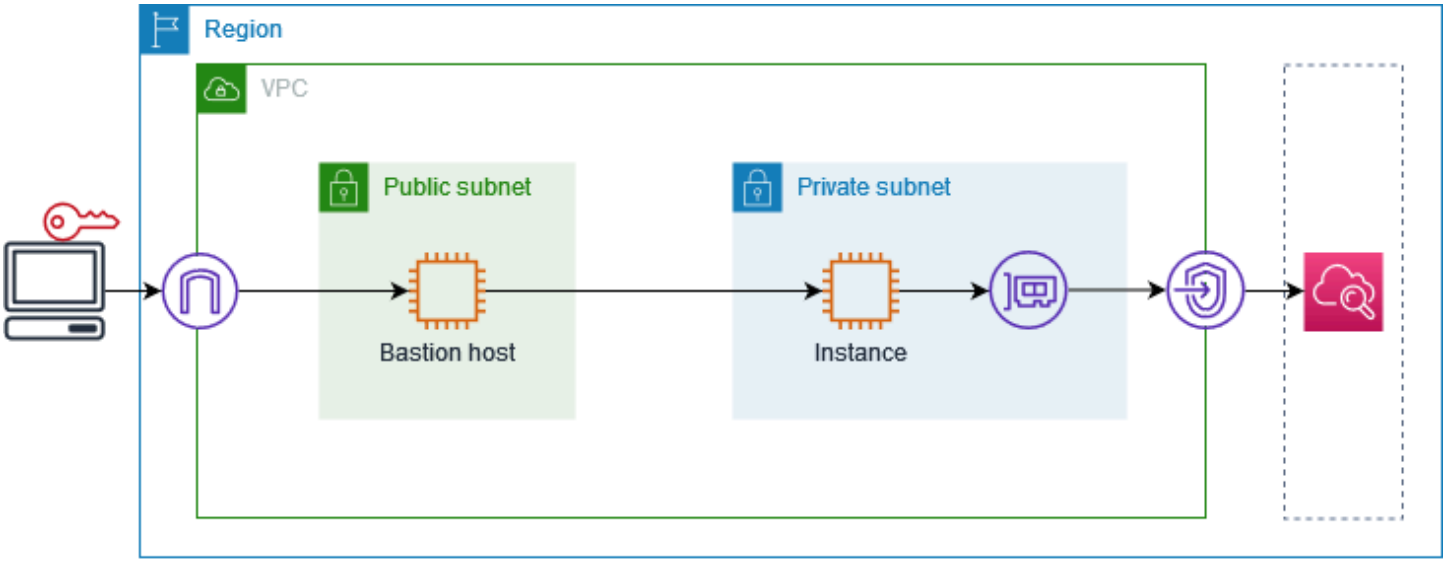
您可以配置 Amazon Route 53 以将域流量路由到 VPC 端点。有关更多信息，请参阅 Routing traffic to a VPC endpoint using your domain name（使用域名将流量路由到 VPC 端点）。

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来自使用者 VPC 的公有主机名 DNS 请求将解析到端点网络接口的私有 IP 地址，但来自 VPC 外部的请求会继续解析到公有端点。有关更多信息，请参阅用于路由流量和为 AWS PrivateLink 部署启用失效转移的 DNS 机制。

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。由于私钥的 .pem 文件位于您的计算机上，而不是在堡垒主机上，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。在为设置了 VPC 终端节点后 CloudWatch，来自该实例的流量将解析到终端节点网络接口，然后 CloudWatch 使用 VPC 终端节点发送到终端节点网络接口。 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：创建具有子网的 VPC
- 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 端点
- 步骤 6：清理

步骤 1：创建具有子网的 VPC

使用以下过程创建具有公有和私有子网的 VPC。

创建 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 选择创建 VPC。
3. 对于 Resources to create（要创建的资源），选择 VPC and more（VPC 等）。
4. 对于 Name tag auto-generation（名称标签自动生成），为 VPC 输入名称。
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 VPC，在公有子网中启动堡垒主机，并在私有子网中启动实例。

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，以允许来自计算机的 CIDR 块的入站 SSH 流量。
- 为实例创建一个安全组，以允许来自堡垒主机安全组的入站 SSH 流量。
- 创建 IAM 实例配置文件并附加CloudWatchReadOnly访问策略。

启动堡垒主机

1. 通过以下网址打开 Amazon EC2 控制台：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，选择您的 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. 通过以下网址打开 Amazon EC2 控制台：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，选择您的 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）。对于 IAM instance profile（IAM 实例配置文件），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。您将使用对的只读 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 .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，指定您在其中创建 VPC 的区域。

   ```
   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 CloudWatch 从具有当前 VPC 配置的实例进行访问。

   ```
   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 端点后，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 终端节点 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，添加允许来自 VPC CIDR 块的 HTTPS 流量的规则。

为创建 VPC 终端节点 CloudWatch

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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 Service（服务），选择 com.amazonaws.***region***.monitoring。
7. 对于 VPC，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 Security group（安全组），选择 VPC 端点的安全组。
10. 对于 Policy（策略），选择 Full access（完全访问权限）以允许所有主体通过 VPC 端点对所有资源执行所有操作。
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 端点

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，指定您在其中创建 VPC 端点的区域。

```
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。
- `--region` 选项指定了您在其中创建 VPC 端点的区域。

步骤 6：清理

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. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (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 VPC 端点，则可以将其删除。

删除 VPC 端点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 VPC 端点。
4. 选择 Actions（操作）、Delete VPC Endpoint（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。默认的服务端点是公有接口，因此您必须向 VPC 添加互联网网关，这样流量才能从 VPC 流向 AWS 服务。如果此配置不符合您的网络安全要求，则可以使用将您的 VPC 连接 AWS PrivateLink 到， AWS 服务 就像它们在您的 VPC 中一样，无需使用互联网网关。

您可以 AWS PrivateLink 使用 VPC 终端节点私密访问与之集成的内容。 AWS 服务 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。您还需要按处理的 GB 数据付费。有关更多信息，请参阅AWS PrivateLink 定价。

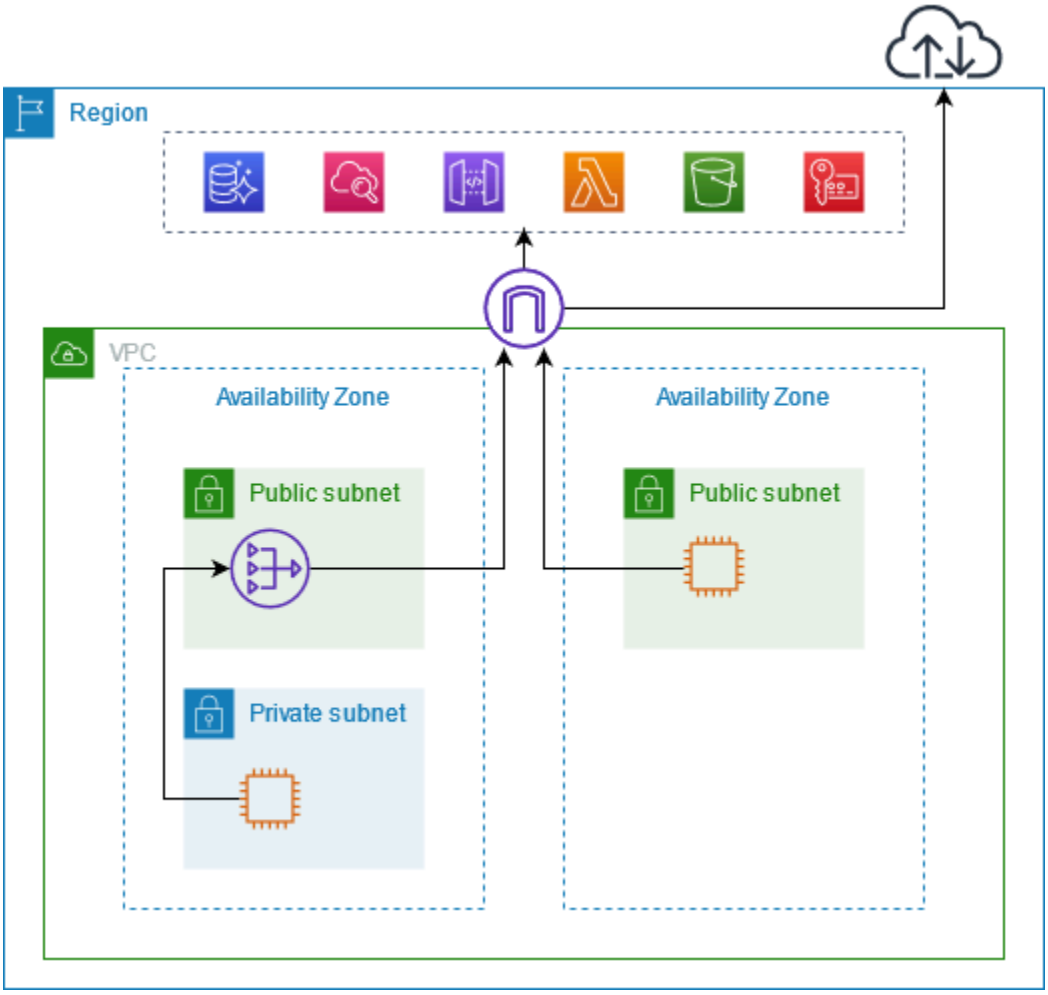
内容

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。

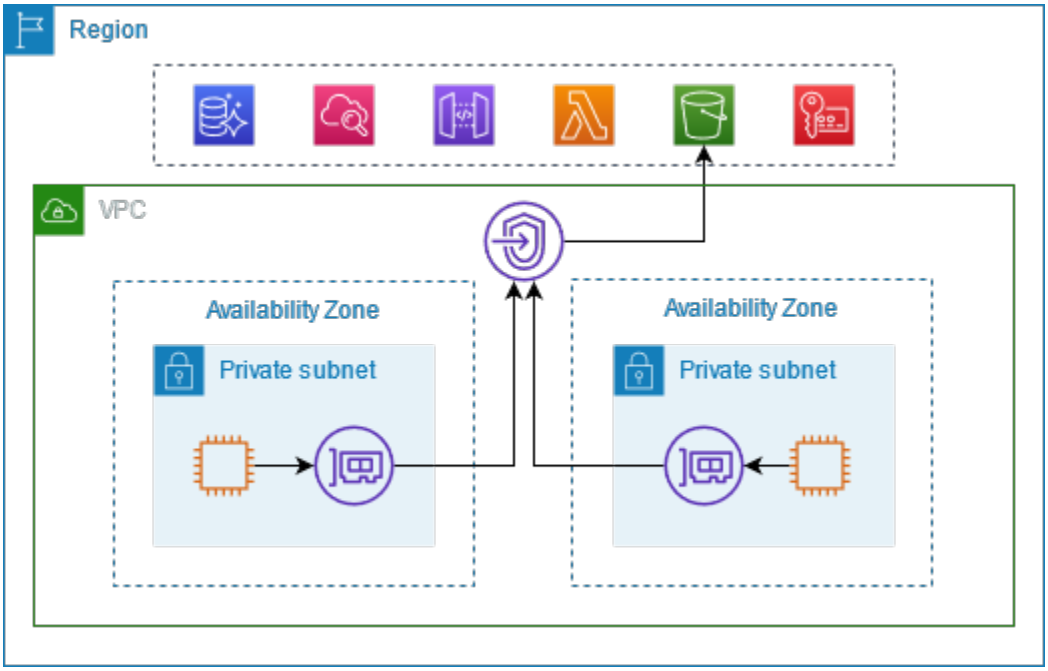
通过公有服务端点进行访问

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 VPC 的 Internet 网关，然后路由到 AWS 服务。从私有子网中的实例流向 AWS 服务的流量路由到 NAT 网关，然后路由到 VPC 的互联网网关，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 VPC 中的子网和 AWS 服务 正在使用的网络接口之间建立连接。发往的流量使用 DNS 解析到终端节点网络接口的私有 IP 地址，然后使用 VPC 终端节点与之间的连接发送到终端节点网络接口的私有 IP 地址 AWS 服务。 AWS 服务 AWS 服务



AWS 服务 自动接受连接请求。服务无法通过 VPC 端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 AWS 服务 从您的 VPC 与进行通信。

接口 VPC 端点的区域 DNS 名称的语法如下：

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

分区 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。借助私有 DNS，您可以继续使用其公共端点的 DNS 名称向服务发出请求，同时通过接口 VPC 端点利用私有连接。有关更多信息，请参阅 the section called “DNS 解析”。

以下 describe-vpc-endpoints 命令显示接口端点的 DNS 条目。

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

以下是启用私 CloudWatch 有 DNS 名称的 Amazon 接口终端节点的输出示例。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 解析

我们为您的接口 VPC 端点创建的 DNS 记录是公有的。因此，这些 DNS 名称是可公开解析的。但是，来自 VPC 外部的 DNS 请求仍会返回端点网络接口的私有 IP 地址，因此，除非您有权访问 VPC，否则这些 IP 地址不能用于访问端点服务。

私有 DNS

如果您为接口 VPC 终端节点启用私有 DNS，并且您的 VPC 同时启用了 DNS 主机名和 DNS 解析，我们将为您创建一个隐藏的 AWS托管私有托管区域。托管区包含服务的默认 DNS 名称的记录集，用于解析为您的 VPC 中的端点网络接口的私有 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。

我们建议您为的 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 AWS SDK 发出的请求）解析到您的 VPC 终端节点。

Amazon 为您的 VPC 提供 DNS 服务器，称为 Route 53 Resolver。Route 53 Resolver 自动解析私有托管区域中的本地 VPC 域名和记录。但是，您不能从 VPC 外部使用 Route 53 Resolver。如果要从本地网络访问您的 VPC 端点，则可以使用 Route 53 Resolver 端点和解析器规则。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

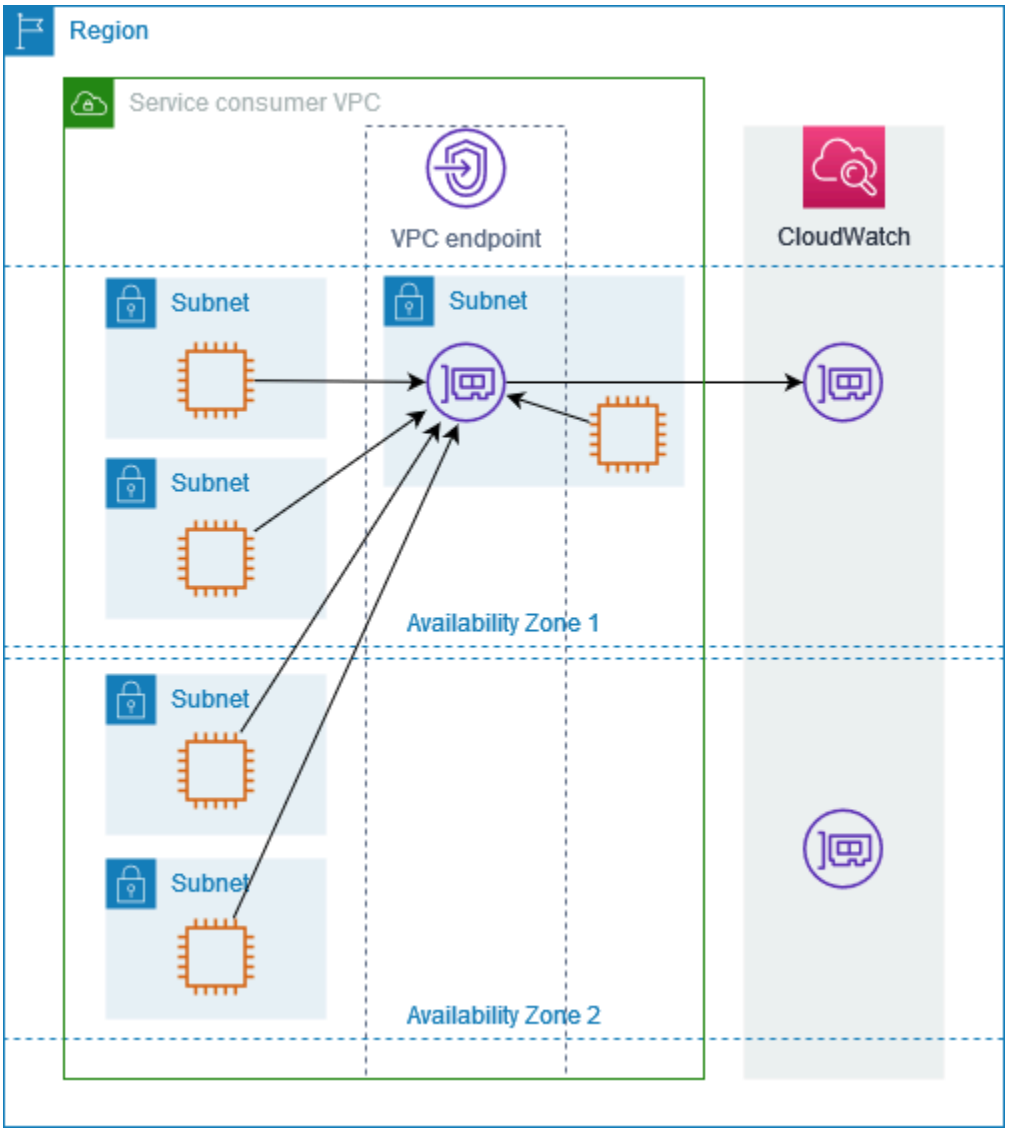
您可以配置 VPC 端点，每个可用区中有一个子网。我们将在您的子网中为 VPC 端点创建一个端点网络接口。我们将根据 VPC 端点的 IP 地址类型，为其子网中的每个端点网络接口分配 IP 地址。端点网络接口的 IP 地址在其 VPC 端点的生命周期内不会变更。

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：

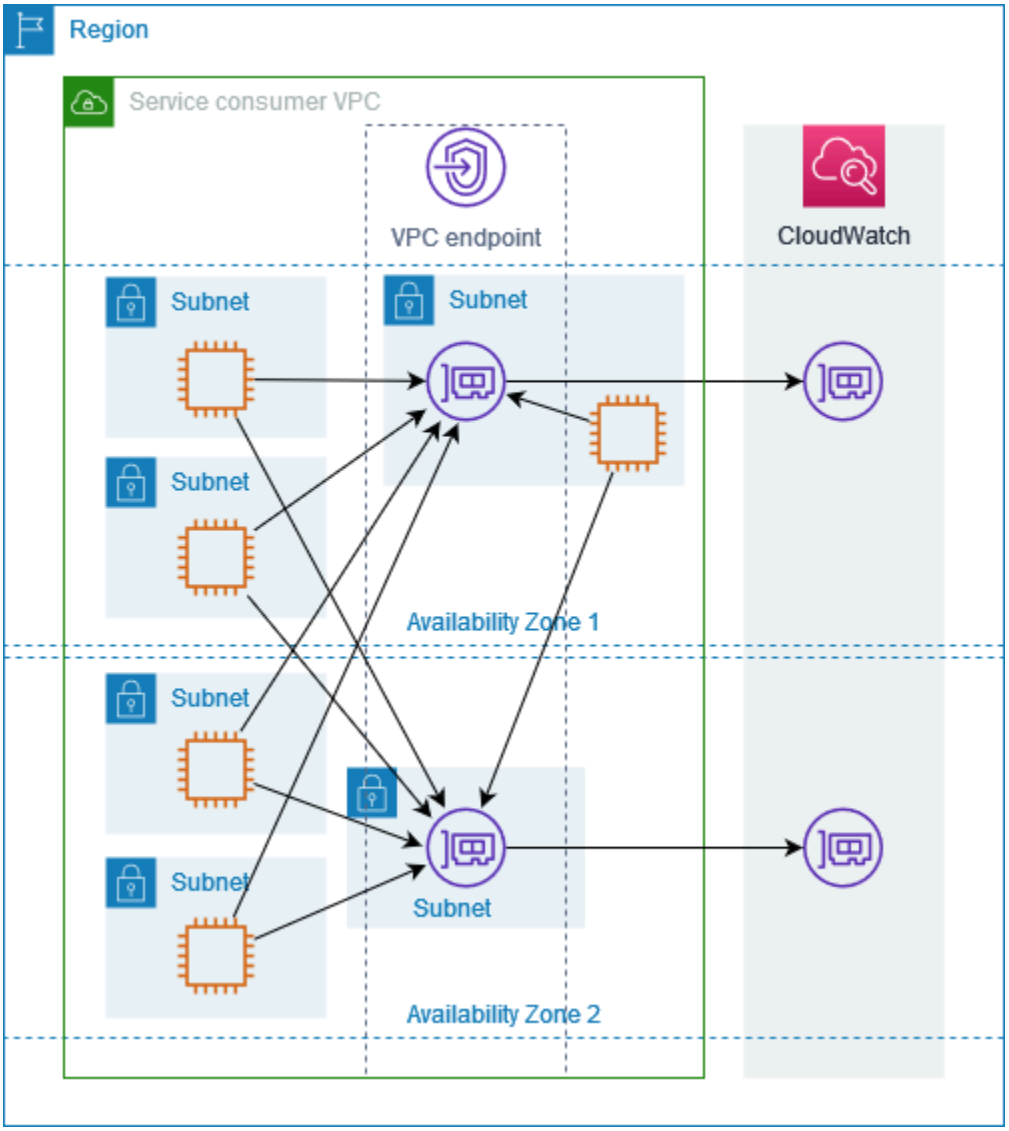
- 为每个 VPC 终端节点配置至少两个可用区，并在这些可用区 AWS 服务 中部署必须访问的 AWS 资源。
- 为 VPC 端点配置私有 DNS 名称。
- 使用 AWS 服务 其区域 DNS 名称（也称为公共终端节点）进行访问。

下图显示了 Amazon CloudWatch 的 VPC 终端节点，其终端节点网络接口位于单个可用区。当 VPC 中任何子网中的任何资源 CloudWatch使用其公有终端节点访问 Amazon 时，我们会将流量解析到终端

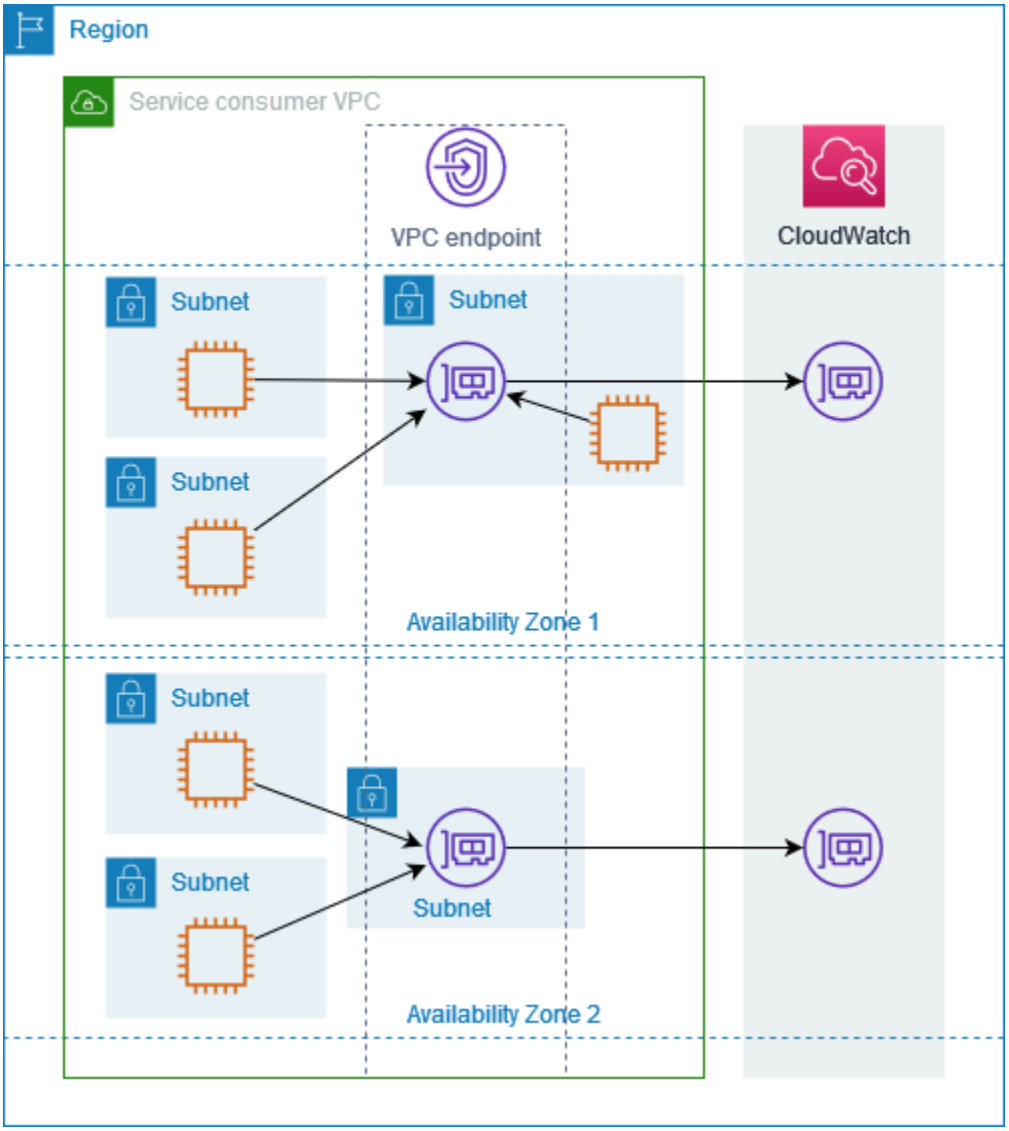
节点网络接口的 IP 地址。这包括来自其他可用区子网的流量。但是，如果可用区 1 受损，则可用区 2 中的资源将无法访问 Amazon CloudWatch。



下图显示了 Amazon 的 VPC 终端节点， CloudWatch 其终端节点网络接口位于两个可用区。当 VPC 中任何子网中的任何资源使用其公有终端节点访问 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 即使他们不通过其公共端点支持 IPv6，也可以通过其私有端点支持 IPv6。支持 IPv6 的端点可以使用 AAAA 记录响应 DNS 查询。

为接口端点启用 IPv6 的要求

- AWS 服务 必须使其服务端点通过 IPv6 可用。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 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围时，才支持此选项。

- IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网时，才支持此选项。
- Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 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。无法从互联网访问端点网络接口的 IPv6 地址。如果您使用 IPv6 地址描述端点网络接口，请注意已启用 `denyAllIgwTraffic`。

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 VPC 端点以私下连接到这些服务，如同这些服务就在您自己的 VPC 中运行。

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-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata
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*.application-autoscaling

AWS 服务	服务名称
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.streaming
AWS AppSync	com.amazonaws.*region*.appsync-api
Amazon Athena	com.amazonaws.*region*.athena
AWS Audit Manager	com.amazonaws.*region*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS B2B 数据交换	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*region*.bedrock
	com.amazonaws。 *## .bedro* ck-agent
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-runtime
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.braket
AWS Clean Rooms	com.amazonaws.*region*.cleanrooms
AWS 无尘室机器学习	com.amazonaws。 *## .cleanroo* ms-ml

AWS 服务	服务名称
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
AWS CloudHSM	com.amazonaws.*region*.cloudhsmv2
AWS Cloud Map	com.amazonaws.*region*.servicediscovery
	com.amazonaws.*region*.servicediscovery-fips
	com.amazonaws.*region*.data-servicediscovery
	com.amazonaws.*region*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*.cloudtrail
Amazon CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics
Amazon CloudWatch 日志	com.amazonaws.*region*.logs
Amazon CloudWatch 网络监视器	com.amazonaws。 regi@@ *on* .networ
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories

AWS 服务	服务名称
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws.*region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws。 *##.codeconnec* tions.api
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	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*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*region*.codewhisperer
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Config	com.amazonaws.*region*.config
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws.*region*.cases
	com.amazonaws.*region*.connect-campaigns

AWS 服务	服务名称
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
AWS 控制目录	com.amazonaws。 ####目录
AWS Data Exchange	com.amazonaws.*region*.dataexchange
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。 ##.##日期管理
	com.amazonaws。 ## .*dead* line.schedin
Amazon DevOps Guru	com.amazonaws.*region*.devops-guru
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws。 regi@@ *on* .dynamodb
Amazon EBS 直接 API	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
EC2 Image Builder	com.amazonaws.*region*.imagebuilder

AWS 服务	服务名称
Amazon ECR	com.amazonaws.*region*.ecr.api
	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*.elasticfilesystem
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR on EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless

AWS 服务	服务名称
亚马逊 EMR WAL	com.amazonaws。 regi@@ *on .emrwal* .prod
AWS Entity Resolution 数据匹配服务	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws。 *##* .pipes-data
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Amazon Managed Grafana	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
Amazon GuardDuty	com.amazonaws.*region*.guardduty-data

AWS 服务	服务名称
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws。 *## .dicom*-medical-imaging
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
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*.storage-omics
IAM Identity Center	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials
	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 服务	服务名称
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*.cassandra
	com.amazonaws.*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips

AWS 服务	服务名称
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB for Redis	com.amazonaws.*region*.memory-db
	com.amazonaws.*region*.memorydb-fips

AWS 服务	服务名称
AWS Migration Hub Orchestrator	com.amazonaws.*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws.*region*.refactor-spaces
Migration Hub 策略建议	com.amazonaws.*region*.migrationhub-strategy
Amazon Neptune Analytics	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
亚马逊 OpenSearch 服务	这些端点由服务托管
AWS Organizations	com.amazonaws。 *##*. 组织
	com.amazonaws。 regi@@ *on* .organtions-
AWS Outposts	com.amazonaws。 *##.ou* tposts
AWS Panorama	com.amazonaws.*region*.panorama
AWS 支付密码学	com.amazonaws.*region*.payment-cryptography.controlplane
	com.amazonaws.*region*.payment-cryptography.dataplane
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime
AWS Supply Chain	com.amazonaws。 *##* .scn
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly

AWS 服务	服务名称
AWS 专用 5G	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api。 *##* *.qbus* iness
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws。 region.@@ *quic* ksight
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS Data API	com.amazonaws.*region*.rds-data
AWS re: Post 私密发布	com.amazonaws。 *##* .repostspace
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
Amazon Redshift 数据 API	com.amazonaws.*region*.redshift-data
	com.amazonaws。 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 RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3

AWS 服务	服务名称
Amazon S3 多区域访问点	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts
服务目录	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry
Amazon SES	com.amazonaws.*region*.email-smtp
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

AWS 服务	服务名称
	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 Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS 电信网络生成器	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
适用于 InfluxDB 的亚马逊 Timestream	com.amazonaws。 *##.timestream* -influxdb
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer

AWS 服务	服务名称
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces 瘦客户机	com.amazonaws。 region.t@@ *hincli* ent.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 命令查看有关每个端点服务的详细信息。

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端点策略，请调用 describe-vpc-endpoint-services 命令并检查 VpcEndpointPolicySupported 的值。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",
    "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.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
```

```
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "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.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "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 desc ribe-vpc-endpoint-services 命令来查看在指定区域中 AWS 服务 可以通过 IPv6 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.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

AWS 服务 使用接口访问 VPC 终端节点

您可以创建接口 VPC 终端节点来连接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。

对于您在 VPC 中指定的每个子网，我们将在子网中创建一个端点网络接口，并为其分配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

- 先决条件
- 创建 VPC 端点
- 共享子网

先决条件

- 在您的 VPC AWS 服务 中部署用于访问的资源。
- 若要使用私有 DNS，您必须为 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。
- 要为接口终端节点启用 IPv6， AWS 服务 必须支持通过 IPv6 进行访问。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安全组，允许来自您的 VPC 中资源的预期流量。例如，为确保 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。

- 如果您的资源位于具有网络 ACL 的子网中，请验证网络 ACL 是否允许您的 VPC 中的资源与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 端点

使用以下过程创建连接到 AWS 服务的接口 VPC 端点。

为创建接口终端节点 AWS 服务

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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 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，选择您要从中访问 AWS 服务的 VPC。
7. 如果您在步骤 5 中选择了 Amazon S3 的服务名称，并且想要配置私有 DNS 支持，则请选择其他设置、启用 DNS 名称。当您做出此选择时，其还会自动选择仅对入站端点启用私有 DNS。您只能为 Amazon S3 的接口端点配置带有入站解析器端点的私有 DNS。如果您没有 Amazon S3 的网关端点，并且选择仅为入站端点启用私有 DNS，则在尝试执行此过程的最后一步时会收到错误消息。

   如果您在步骤 5 中为除 Amazon S3 之外的所有服务都选择了服务名称，则表明已选择了其他设置、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 AWS SDK 发出的请求）解析到您的 VPC 终端节点。
8. 在 Subnets（子网）选项中，为每个可用区选择一个您将从中访问 AWS 服务的子网。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”。

   我们将在您选择的每个子网中创建一个端点网络接口。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，然后输入子网地址范围中的 IPv4 地址。如果端点服务支持 IPv6，您也可以输入子网地址范围中的 IPv6 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 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围且服务接受 IPv4 请求时，才支持此选项。
- IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网且服务接受 IPv6 请求时，才支持此选项。
- Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 和 IPv6 地址范围且服务接受 IPv4 和 IPv6 请求时，才支持此选项。

10. 对于 Security groups（安全组），选择要与 VPC 端点的端点网络接口关联的安全组。默认情况下，我们会关联 VPC 的默认安全组。
11. 对于 Policy（策略），选择 Full access（完全访问权限）以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择 Custom（自定义）以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。该选项仅在服务支持 VPC 端点策略时可用。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 端点。但是，您可以在与您共享的子网中使用 VPC 端点。

配置接口端点

创建接口 VPC 端点后，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 端点策略
- 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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，然后输入子网地址范围中的 IPv4 地址。如果端点服务支持 IPv6，您也可以输入子网地址范围中的 IPv6 地址。

   如果您为已经有此 VPC 端点的端点网络接口的子网指定 IP 地址，我们会用新的端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。安全组规则将控制可以从 VPC 中的资源发送到端点网络接口的流量。

使用控制台更改安全组

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

2. 在导航窗格中，选择端点。
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 端点策略

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

我们建议您为的 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 AWS SDK 发出的请求）解析到您的 VPC 终端节点。

若要使用私有 DNS 名称，您必须为 VPC 启用 DNS 主机名和 DNS 解析。启用私有 DNS 名称时，私有 IP 地址可能需要几分钟才能变为可用。我们在您启用私有 DNS 名称时所创建的 DNS 记录为私有记录。因此，私有 DNS 名称不可公开解析。

使用控制台更改私有 DNS 名称选项

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 依次选择 Actions（操作）、Modify private DNS name（修改私有 DNS 名称）。
5. 根据需要选择或清除 Enable for this endpoint（为此端点启用）。
6. 如果服务为 Amazon S3，则在上一步中，选择为此端点启用会同时选择仅为入站端点启用私有 DNS。如果您偏好使用标准私有 DNS 功能，则请清除仅为入站端点启用私有 DNS。如果除了 Amazon S3 的接口端点之外，您没有 Amazon S3 的网关端点，并且选择仅为入站端点启用私有 DNS，则在下一步保存更改时，会收到错误消息。有关更多信息，请参阅 the section called “私有 DNS”。
7. 选择保存更改。

使用命令行更改私有 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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

使用以下过程为通知创建一个 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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. 对于 Notification ARN（通知 ARN），选择您创建的适用于 SNS 主题的 ARN。
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-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification（适用于 Windows 的工具 PowerShell）

添加访问策略

在 Amazon SNS 主题中添加 AWS PrivateLink 允许代表您发布通知的访问策略，如下所示。有关更多信息，请参阅如何编辑 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的 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

用完 VPC 端点后可以将其删除。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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择接口端点。
4. 选择 Actions（操作）、Delete VPC Endpoint（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 端点可提供与 Amazon S3 和 DynamoDB 的可靠连接，而无需为您的 VPC 提供互联网网关或 NAT 设备。与其他类型的 VPC 终端节点不同 AWS PrivateLink，网关终端节点不使用。

Amazon S3 和 DynamoDB 同时支持网关终端节点和接口终端节点。有关选项的比较，请参阅以下内容：

- 亚马逊 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。

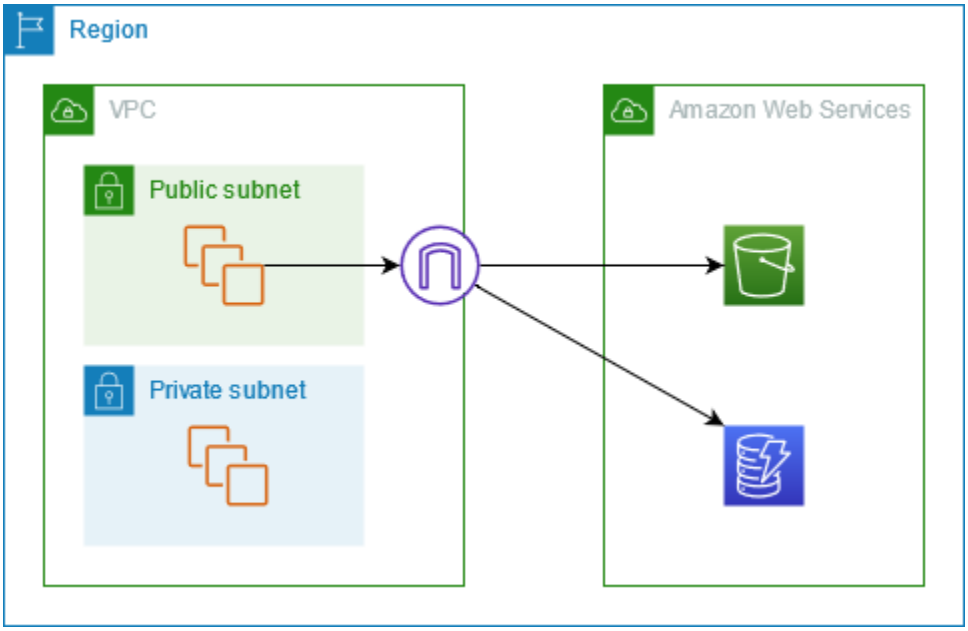
内容

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。

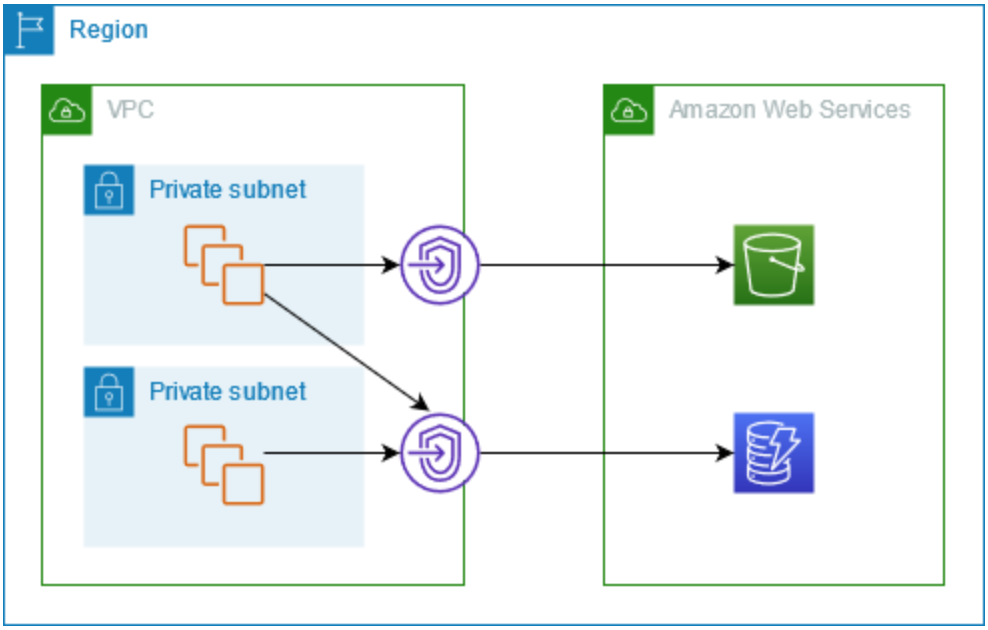
通过互联网网关访问

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流向 Amazon S3 或 DynamoDB 的流量路由到 VPC 的互联网网关，然后路由到服务。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。若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 设备并将私有子网中的流量路由到 NAT 设备。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。从您的 VPC 流向 Amazon S3 或 DynamoDB 的流量将路由到网关端点。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托管的前缀列表。



路由

创建网关端点时，选择您启用的子网的 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

这些实例的子网的网络 ACL 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 VPC 端点从 VPC 访问 Amazon S3。创建网关端点后，您可以将其添加为从您的 VPC 流向 Amazon S3 的流量的路由表中的目标。

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。借助网关端点，您可以从 VPC 访问 Amazon S3，而无需为 VPC 配备互联网网关或 NAT 设备，也无需任何额外费用。但是，网关终端节点不允许从本地网络、其他 AWS 区域的对等 VPC 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》中的适用于 Amazon S3 的 VPC 端点类型。

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，则必须为您的 VPC 同时启用 DNS 主机名和 DNS 解析。如果您使用自己的 DNS 服务器，请确保将针对 Amazon S3 的请求正确解析为 AWS维护的 IP 地址。
- 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。
- 对于通过网关端点访问 Amazon S3 的实例，子网的网络 ACL 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 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 端点向 Amazon S3 发出的请求，不能在身份策略或存储桶策略中使用 `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 端点访问 Amazon S3。
- 网关端点仅支持 IPv4 流量。
- Amazon S3 从受影响子网的实例收到的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。端点将切换网络路由，并断开打开的 TCP 连接。以前使用公有 IPv4 地址的连接不会恢复。建议您在创建或修改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。
- 无法将端点连接扩展到 VPC 之外。VPN 连接、VPC 对等连接、传输网关或您的 VPC 中 AWS Direct Connect 连接另一端的资源无法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 VPC 的网关端点限制为 255 个。

私有 DNS

在为 Amazon S3 创建网关端点和接口端点时，您可以配置私有 DNS 以优化成本。

Route 53 Resolver

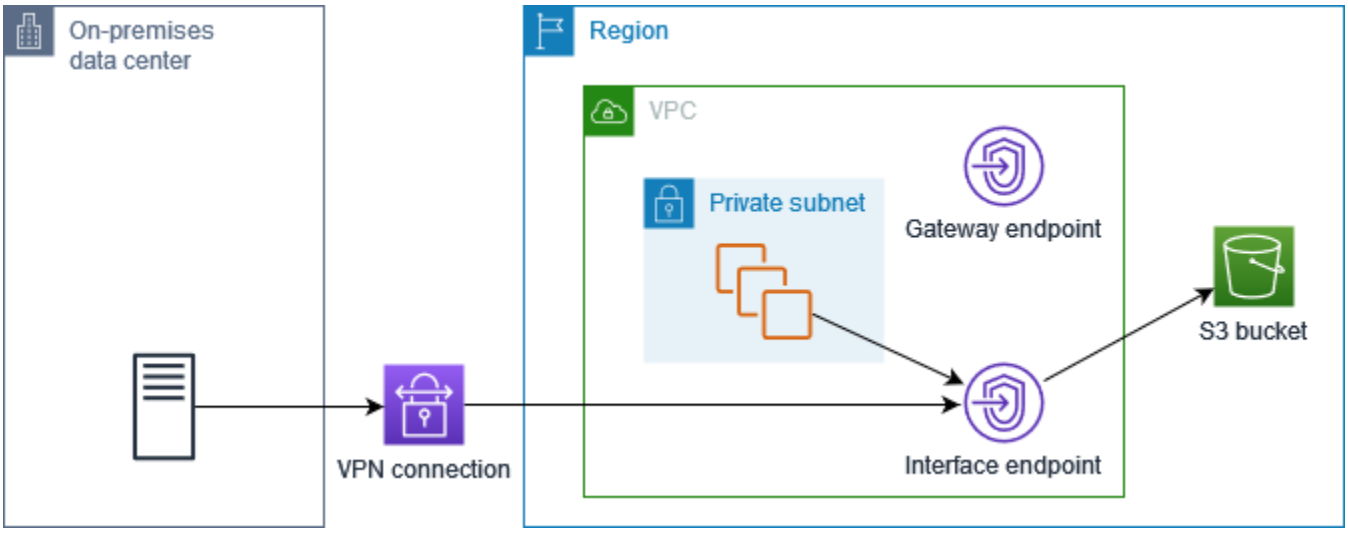
Amazon 为您的 VPC 提供 DNS 服务器，称为 Route 53 Resolver。Route 53 Resolver 自动解析私有托管区域中的本地 VPC 域名和记录。但是，您不能从 VPC 外部使用 Route 53 Resolver。Route 53 提供解析器端点和解析器规则，以便您可从 VPC 外部使用 Route 53 Resolver。入站解析器端点将

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

当您将 Amazon S3 的接口端点配置为仅对入站解析器端点使用私有 DNS 时，我们会创建入站解析器端点。对于 Amazon S3 的 DNS 查询，入站解析器端点会将其从本地解析到接口端点的私有 IP 地址。我们还将 Route 53 Resolver 的 ALIAS 记录添加到 Amazon S3 的公共托管区域，这样来自 VPC 的 DNS 查询便会解析到 Amazon S3 公有 IP 地址，从而将流量路由到网关端点。

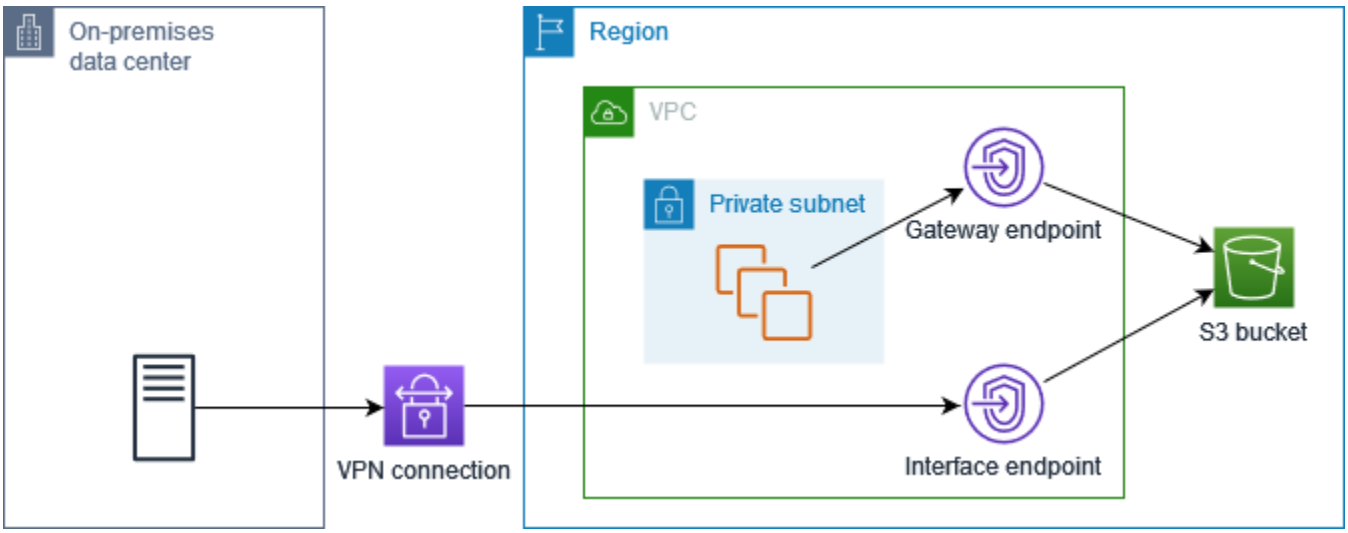
私有 DNS

如果您为 Amazon S3 的接口端点配置私有 DNS，但并非仅为入站解析器端点配置私有 DNS，则来自您的本地网络和 VPC 的请求都使用接口端点访问 Amazon S3。因此，您需要付费使用接口端点处理来自 VPC 的流量，而不是免费使用网关端点。



私有 DNS 仅适用于入站解析器端点

如果您仅为入站解析器端点配置私有 DNS，则来自您的本地网络的请求会使用接口端点访问 Amazon S3，而来自 VPC 的请求会使用网关端点访问 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 的接口端点时或在创建后，为其配置私有 DNS。有关更多信息，请参阅 the section called “创建 VPC 端点”（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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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。 ## .s3。
6. 在 VPC 选项中，选择要创建端点的 VPC。
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 Policy（策略），选择 Full access（完全访问权限）以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择 Custom（自定义）以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。
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特定终端节点、VPC、IP 地址范围和对存储桶的访问。 AWS 账户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 条件键来创建限制对特定端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：限制对特定 VPC 的访问

您可以使用 aws:sourceVpc 条件键来创建存储桶策略，用于限制对特定 VPC 的访问。如果您在同一 VPC 中配置了多个端点，这会非常有用。除非请求来自指定的 VPC，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",
      "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: VpcSource Ip 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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 端点策略

您可以为网关端点编辑端点策略，以此控制通过端点从 VPC 对 Amazon S3 进行的访问。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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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 VPC AWS 服务 中有其他使用 S3 存储桶，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

您可以创建限制对特定 IAM 角色的访问权限的策略。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。

如果私有 DNS 已启用，则无法删除网关端点。

使用控制台删除网关端点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择 Actions（操作）、Delete VPC Endpoint（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 VPC 端点从 VPC 访问 Amazon DynamoDB。创建网关端点后，您可以将其添加为路由表中的目标，用于从您的 VPC 流向 DynamoDB 的流量。

使用网关端点不会发生任何额外费用。

DynamoDB 同时支持网关终端节点和接口终端节点。使用网关终端节点，您可以从您的 VPC 访问 DynamoDB，无需为 VPC 使用互联网网关或 NAT 设备，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 区域的对等 VPC 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 DynamoDB 开发者指南中的 DynamoDB 的 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。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，则必须为您的 VPC 同时启用 DNS 主机名和 DNS 解析。如果您使用自己的 DNS 服务器，请确保将针对 DynamoDB 的请求正确解析为 AWS维护的 IP 地址。
- 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。
- 对于通过网关端点访问 DynamoDB 的实例，子网的网络 ACL 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者 VPC 中 EC2 实例的私有 IP 地址以及通过该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。
- 您的受影响子网中实例的源 IPv4 地址将从公有 IPv4 地址变为您的 VPC 中的私有 IPv4 地址。端点将切换网络路由，并断开打开的 TCP 连接。以前使用公有 IPv4 地址的连接不会恢复。建议您在创建或修改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。
- 无法将端点连接扩展到 VPC 之外。VPN 连接、VPC 对等连接、传输网关或您的 VPC 中 AWS Direct Connect 连接另一端的资源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 VPC 的网关端点限制为 255 个。

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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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。 regi@@ ***on*** .dynamodb。
6. 在 VPC 选项中，选择要创建端点的 VPC。
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 Policy（策略），选择 Full access（完全访问权限）以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择 Custom（自定义）以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。
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 policy 控制访问

您可以创建 IAM policy 来控制哪些 IAM 主体可以使用特定的 VPC 端点来访问 DynamoDB 表。

Example 示例：限制对特定端点的访问

您可以使用 aws:sourceVpce 条件键来创建用于限制对特定 VPC 端点的访问的策略。除非使用指定的 VPC 端点，否则以下策略将拒绝对账户中 DynamoDB 表的访问。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",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example 示例：允许来自特定 IAM 角色的访问

您可以创建策略，以允许使用特定 IAM 角色进行访问。以下策略将向指定 IAM 角色授予访问权限。

```
{
   "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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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 端点策略

您可以为网关端点编辑端点策略，以此控制通过端点从 VPC 对 DynamoDB 进行的访问。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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择网关端点。
4. 选择 Actions（操作）、Delete VPC Endpoint（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，就像它们在您自己的 VPC 中运行一样。

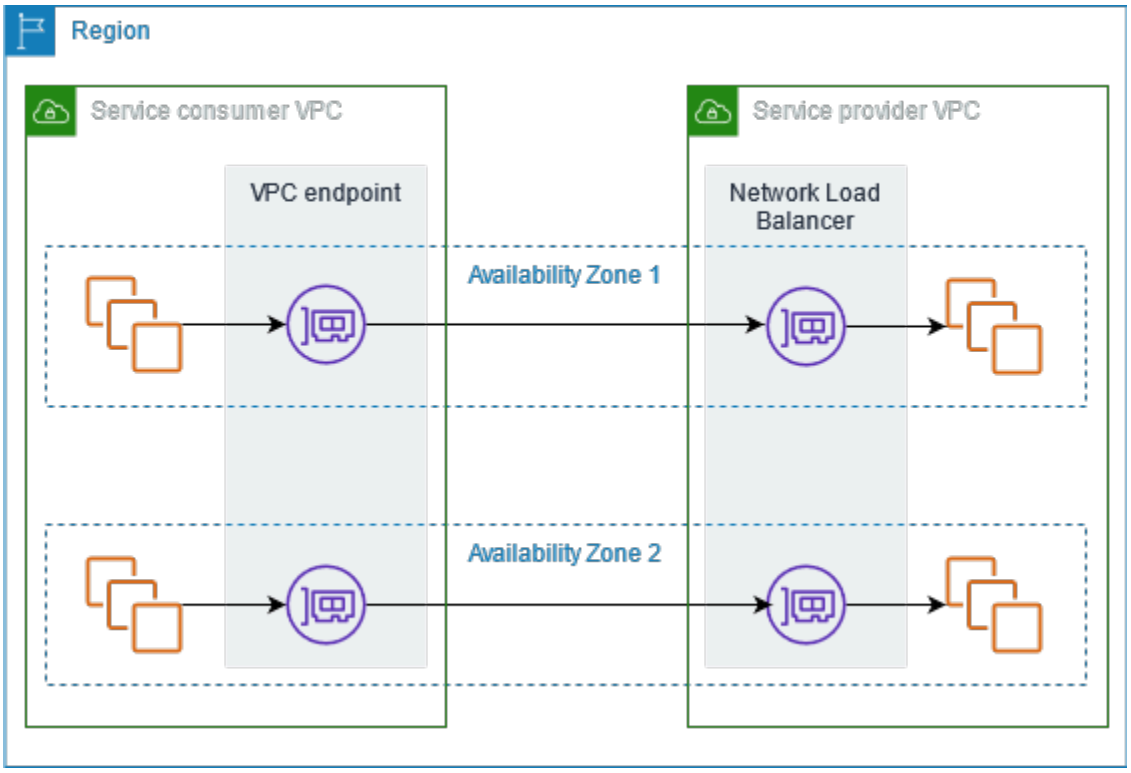
内容

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。欲了解更多信息，请参阅 AWS Marketplace：- 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，您可以创建接口 VPC 端点，该端点在您的 VPC 中的一个或多个子网与端点服务之间建立连接。



创建接口端点

使用以下过程创建连接到 SaaS 产品的接口 VPC 端点。

要求

订阅服务。

创建连接到合作伙伴服务的接口端点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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. 对于服务类别，选择 AWS Marketplace 服务。
   b. 输入服务的名称。
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. 对于 “服务” 类别，选择 PrivateLink Ready 合作伙伴服务。
   b. 输入服务的名称并选择 Verify service（验证服务）。
6. 对于 VPC，选择您要从中访问产品的 VPC。
7. 对于 Subnets（子网），为每个可用区选择一个您将从中访问产品的子网。
8. 对于 Security group（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 VPC 中的资源与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 端点服务时指定网关负载均衡器。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

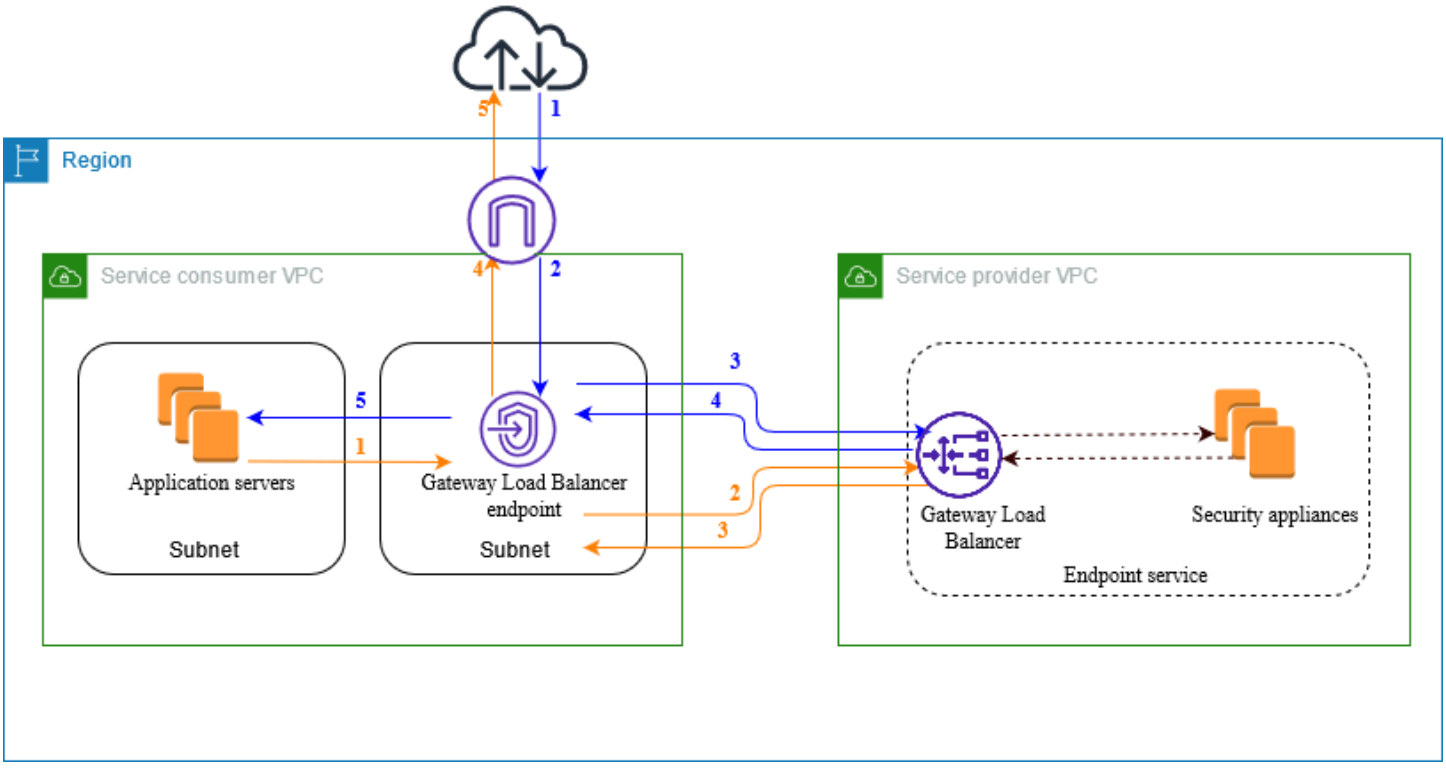
您需要按在每个可用区配置您的 Gateway Load Balancer 终端节点的每小时付费。您还需要按处理的 GB 数据付费。有关更多信息，请参阅AWS PrivateLink 定价。

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 VPC 的子网中运行。您在同一 VPC 的另一个子网中创建网关负载均衡器端点。通过互联网网关进入服务使用者 VPC 的所有流量首先会路由到网关负载均衡器端点，以便进行检查，然后再路由到目标子网。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. 流量通过互联网网关进入服务使用者 VPC。
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

服务提供商可通过 IPv4、IPv6 或 IPv4 和 IPv6 向服务使用者提供其服务端点，即使其安全设备仅支持 IPv4。如果您启用双堆栈支持，则现有使用者可继续使用 IPv4 访问您的服务，并且新的使用者可选择使用 IPv6 访问您的服务。

如果网关负载均衡器端点支持 IPv4，则端点网络接口具有 IPv4 地址。如果网关负载均衡器端点支持 IPv6，则端点网络接口具有 IPv6 地址。无法从互联网访问端点网络接口的 IPv6 地址。如果您使用 IPv6 地址描述端点网络接口，请注意已启用 `denyAllIgwTraffic`。

为端点服务启用 IPv6 的要求

- 端点服务的 VPC 和子网必须具有关联的 IPv6 CIDR 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。

为网关负载均衡器端点启用 IPv6 的要求

- 端点服务必须具有包含 IPv6 支持的 IP 地址类型。
- 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 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围时，才支持此选项。
  - IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网时，才支持此选项。
  - Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 和 IPv6 地址范围时，才支持此选项。
- 服务使用者 VPC 中子网的路由表必须路由 IPv6 流量，而这些子网的网络 ACL 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，双堆栈配置包含 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
###### IPv4 CIDR	*vpc-endpoint-id*
###### 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。您可以使用可用区 ID 一致地标识服务的可用区。有关更多信息，请参阅 A mazon EC2 用户指南中的可用区 ID。
- 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

- 在应提供服务的可用区中创建具有至少两个子网的服务提供商 VPC。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。
- 在服务提供商 VPC 中创建网关负载均衡器。如果您计划在端点服务上启用 IPv6 支持，则必须在网关负载均衡器上启用双堆栈支持。有关更多信息，请参阅网关负载均衡器入门。
- 在服务提供商 VPC 中启动安全设备，并将其注册到负载均衡器目标组。

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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 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 – 启用端点服务以接受 IPv4 请求。
   - 选择 IPv6 – 启用端点服务以接受 IPv6 请求。
   - 选择 IPv4 和 IPv6 – 启用端点服务以接受 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-configuration (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。

对于您在 VPC 中指定的每个子网，我们将在子网中创建一个端点网络接口，并为其分配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 VPC 中选择一个可用区。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。您可以使用可用区 ID 一致地标识服务的可用区。有关更多信息，请参阅 A mazon EC2 用户指南中的可用区 ID。
- 只有在服务提供商接受连接请求后，您才能使用端点服务。服务无法通过 VPC 端点发起对您的 VPC 中的资源的请求。端点仅返回对由您的 VPC 中的资源启动的流量的响应。
- 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进行路由时，不支持网络负载均衡器客户端 IP 保留，即使目标与网络负载均衡器位于同一 VPC 中亦是如此。
- 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

- 在您将从中访问服务的可用区中，创建一个包含至少两个子网的服务使用者 VPC。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。
- 若要验证端点服务支持哪些可用区，请使用控制台或 describe-vpc-endpoint-services 命令描述端点服务。
- 如果您的资源位于具有网络 ACL 的子网中，请验证网络 ACL 是否允许端点网络接口与 VPC 中的资源之间的流量。

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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（端点）。
3. 选择 Create endpoint（创建端点）。
4. 在 Service category（服务类别）选项中，选择 Other endpoint services（其他端点服务）。
5. 对于 Service name，输入服务的名称，然后选择 Verify service（验证服务）。
6. 在 VPC 选项中，选择要创建端点的 VPC。
7. 对于 Subnets（子网），选择要在其中创建端点的子网。
8. 对于 IP address type（IP 地址类型），可从以下选项中进行选择：
   - IPv4 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围时，才支持此选项。
   - IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网时，才支持此选项。
   - Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 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

按照以下过程为服务使用者 VPC 配置路由表。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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 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 Add route（添加路由）。对于 Destination（目标），输入应用程序服务器子网的 IPv4 CIDR 块。在 Target（目标）选项中，选择 VPC 端点。
   c. 如果您支持 IPv6，请选择 Add route（添加路由）。对于 Destination（目标），输入应用程序服务器子网的 IPv6 CIDR 块。在 Target（目标）选项中，选择 VPC 端点。
   d. 选择保存更改。
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 Add route（添加路由）。在 Destination（目标位置）字段，输入 **`0.0.0.0/0`**。在 Target（目标）选项中，选择 VPC 端点。
   c. 如果您支持 IPv6，请选择 Add route（添加路由）。在 Destination（目标位置）字段，输入 **`::/0`**。在 Target（目标）选项中，选择 VPC 端点。
   d. 选择保存更改。
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 Add route（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 Add route（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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
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. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
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)

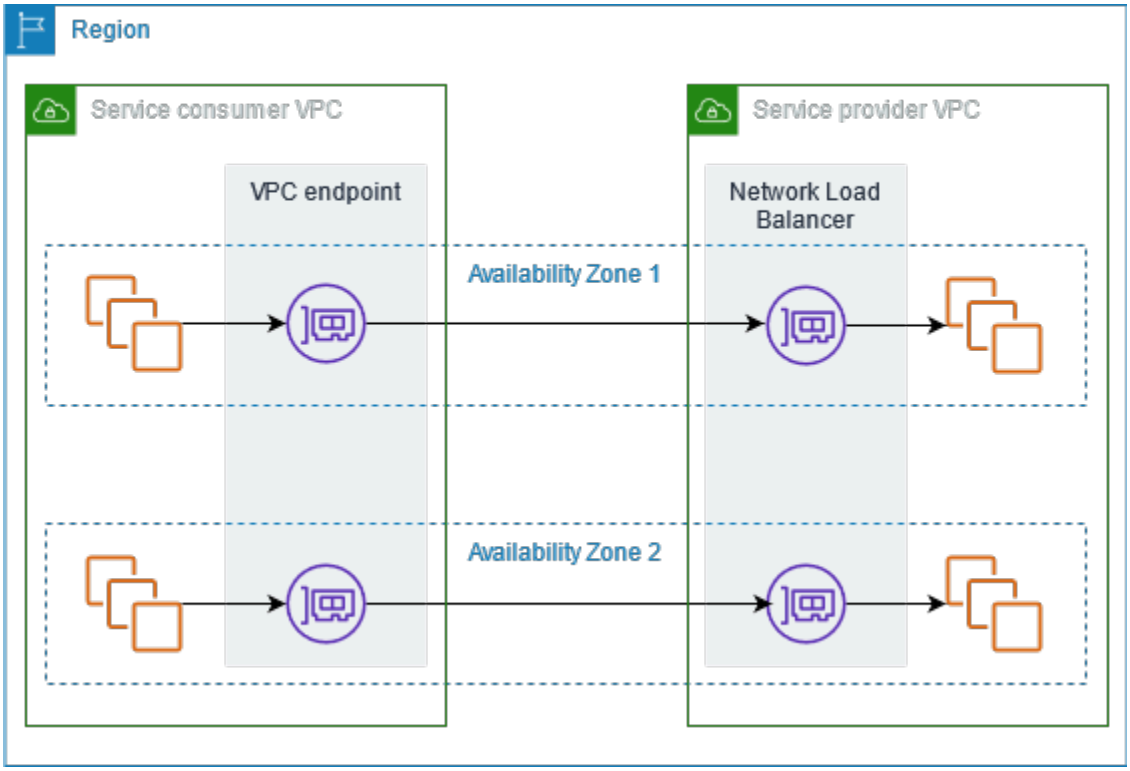
通过以下方式共享您的服务 AWS PrivateLink

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，您可在 VPC 中创建网络负载均衡器作为服务前端。然后，您可在创建 VPC 端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，客户可创建接口 VPC 端点，该端点会在他们从其 VPC 中选择的子网和您的端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

当服务提供商创建 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-east-2 区域中 VPC 端点服务的 DNS 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 端点时，我们会创建区域和分区 DNS 名称，供服务使用者用于与端点服务进行通信。区域名称的语法如下：

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

分区名称的语法如下：

```
endpoint_id-zone.endpoint_service_id.region.vpce.amazonaws.com
```

私有 DNS

服务提供商还可为其端点服务关联私有 DNS 名称，以便服务使用者继续使用其现有的 DNS 名称访问该服务。如果服务提供商将私有 DNS 名称与其端点服务相关联，则服务使用者可以为其接口端点启用私有 DNS 名称。如果服务提供商未启用私有 DNS，则服务使用者可能需要更新其应用程序，以使用 VPC 端点服务的公有 DNS 名称。有关更多信息，请参阅 管理 DNS 名称。

IP 地址类型

服务提供商可通过 IPv4、IPv6 或 IPv4 和 IPv6 向服务使用者提供其服务端点，即使其后端服务器仅支持 IPv4。如果您启用双堆栈支持，则现有使用者可继续使用 IPv4 访问您的服务，并且新的使用者可选择使用 IPv6 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。无法从互联网访问端点网络接口的 IPv6 地址。如果您使用 IPv6 地址描述端点网络接口，请注意已启用 `denyAllIgwTraffic`。

为端点服务启用 IPv6 的要求

- 端点服务的 VPC 和子网必须具有关联的 IPv6 CIDR 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。目标无需支持 IPv6 流量。如果该服务处理来自代理协议版本 2 标头的源 IP 地址，则它必须处理 IPv6 地址。

为接口端点启用 IPv6 的要求

- 端点服务必须支持 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 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围时，才支持此选项。
  - IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网时，才支持此选项。
  - Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 和 IPv6 地址范围时，才支持此选项。

接口端点的 DNS 记录 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端点的 IP 地址类型兼容，如下所述：

- IPv4 – 为私有、区域和分区 DNS 名称创建 A 记录。IP 地址类型必须为 IPv4 或 Dualstack（双堆栈）。
- IPv6 – 为私有、区域和分区 DNS 名称创建 AAAA 记录。IP 地址类型必须为 IPv6 或 Dualstack（双堆栈）。
- Dualstack（双堆栈）– 为私有、区域和分区 DNS 名称创建 A 和 AAAA 记录。IP 地址类型必须为 Dualstack（双堆栈）。

创建由其提供支持的服务 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。您可以使用 VPC 对等连接从其他区域访问端点服务。
- 端点服务仅支持通过 TCP 的流量。
- 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。您可以使用可用区 ID 一致地标识服务的可用区。有关更多信息，请参阅 A mazon EC2 用户指南中的可用区 ID。

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

- 在每个提供服务的可用区中，为端点服务创建具有至少一个子网的 VPC。
- 要使服务使用者能够为您的端点服务创建 IPv6 接口 VPC 端点，VPC 和子网必须具有关联的 IPv6 CIDR 块。
- 在 VPC 中创建网络负载均衡器。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 Network Load Balancer 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。
- 要使您的端点服务能够接受 IPv6 请求，其网络负载均衡器必须使用双堆栈 IP 地址类型。目标无需支持 IPv6 流量。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。

  如果您处理来自代理协议版本 2 标头的源 IP 地址，请验证您是否可以处理 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。如果您未在所有已启用的可用区中启动实例，则可启用跨区域负载均衡，以支持使用分区 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》中的跨区域负载平衡。

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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 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。包含的可用区列出了为所选网络负载均衡器启用的可用区。您的终端节点服务将在这些可用区域中可用。
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。否则将自动接受这些请求。
7. 对于 Enable private DNS name（启用私有 DNS 名称），选择 Associate a private DNS name with the service（将私有 DNS 名称与服务关联）以关联服务使用者可用于访问您服务的私有 DNS 名称，然后输入私有 DNS 名称。否则，服务使用者可以使用提供的终端节点专用的 DNS 名称。AWS服务提供商必须先验证服务使用者拥有该域，然后服务使用者才能使用私有 DNS 名称。有关更多信息，请参阅 管理 DNS 名称。
8. 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 – 启用端点服务以接受 IPv4 请求。
   - 选择 IPv6 – 启用端点服务以接受 IPv6 请求。
   - 选择 IPv4 和 IPv6 – 启用端点服务以接受 IPv4 和 IPv6 请求。
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 Create（创建）。

使用命令行创建端点服务

- create-vpc-endpoint-service-configuration (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 VPC 终端节点私密连接到您的终端节点服务。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，请参阅以下步骤。
- 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（端点）。
3. 选择 Create endpoint（创建端点）。
4. 在 Service category（服务类别）选项中，选择 Other endpoint services（其他端点服务）。
5. 对于 Service name（服务名称），请输入服务的名称（例如 `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`）然后选择 Verify service（验证服务）。
6. 对于 VPC，选择要在其中创建端点的 VPC。
7. 对于 Subnets（子网），选择您将从中访问端点服务的子网（可用区）。
8. 对于 IP address type（IP 地址类型），可从以下选项中进行选择：
   - IPv4 – 将 IPv4 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 地址范围且端点服务接受 IPv4 请求时，才支持此选项。
   - IPv6 – 将 IPv6 地址分配给端点网络接口。仅当所有选定子网均为仅限 IPv6 的子网且端点服务接受 IPv6 请求时，才支持此选项。
   - Dualstack（双堆栈）– 将 IPv4 和 IPv6 地址分配给端点网络接口。仅当所有选定子网都具有 IPv4 和 IPv6 地址范围且端点服务接受 IPv4 和 IPv6 请求时，才支持此选项。
9. 对于 DNS record IP type（DNS 记录 IP 类型），可从以下选项中进行选择：
   - IPv4 – 为私有、区域和分区 DNS 名称创建 A 记录。IP 地址类型必须为 IPv4 或 Dualstack（双堆栈）。
   - IPv6 – 为私有、区域和分区 DNS 名称创建 AAAA 记录。IP 地址类型必须为 IPv6 或 Dualstack（双堆栈）。

- Dualstack（双堆栈）– 为私有、区域和分区 DNS 名称创建 A 和 AAAA 记录。IP 地址类型必须为 Dualstack（双堆栈）。
- Service defined（已定义服务）– 为私有、区域和分区 DNS 名称创建 A 记录，为区域和分区 DNS 名称创建 AAAA 记录。IP 地址类型必须为 Dualstack（双堆栈）。

10. 对于 Security group（安全组），选择要与端点网络接口关联的安全组。
11. 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 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。您必须添加权限，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。要为 AWS 委托人添加权限，您需要其亚马逊资源名称 (ARN)。以下列表包括支持的 AWS 主体的 ARN 示例。

校长的 ARN AWS

AWS 账户 （包括账户中的所有委托人）

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

角色

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

用户

arn:aws:iam::*account_id*:user/*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，则不会影响之前接受的终端节点和服务之间的现有连接。

使用控制台管理端点服务的权限

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务，然后选择 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 Principals to add（要添加的主体），输入主体的 ARN。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-permissions (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。

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”。

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。
- 如果您拒绝已被接受的请求，则不会影响终端节点与服务之间的连接。

使用控制台修改接受设置

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

3. 选择端点服务。
4. 从 Endpoint connections（端点连接）选项卡中，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

您可以管理与您的终端节点服务关联的负载均衡器。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 Network Load Balancer 启用了另一个可用区，则也可以为终端节点服务启用该可用区。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。

使用控制台管理终端节点服务的负载均衡器

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务。
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. 根据需要更改终端节点服务配置。例如：
   - 选中负载均衡器的复选框以将其与终端节点服务关联。
   - 清除负载均衡器复选框以解除其与终端节点服务的关联。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，则该可用区将显示在 “已包含的可用区” 下。如果您在下一步中保存更改，则会为新的可用区启用终端节点服务。
6. 选择 Save changes（保存更改）

使用命令行管理终端节点服务的负载均衡器

- modify-vpc-endpoint-service-configuration (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终端节点服务，只需使用终端节点服务的 ID 调用命令即可。

关联私有 DNS 名称

您可以将私有 DNS 名称与端点服务相关联。关联私有 DNS 名称后，您必须更新 DNS 服务器上域的条目。服务提供商必须先验证服务使用者拥有该域，然后服务使用者才能使用私有 DNS 名称。有关更多信息，请参阅 管理 DNS 名称。

使用控制台修改端点服务私有 DNS 名称

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务。
4. 依次选择 Actions（操作）、Modify private DNS name（修改私有 DNS 名称）。
5. 选择 Associate a private DNS name with the service（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. 选择保存更改。
7. 如果验证状态为 verified（已验证），则私有 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。

使用命令行修改端点服务私有 DNS 名称

- modify-vpc-endpoint-service-configuration (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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务。
4. 依次选择 Actions（操作）、Verify domain ownership for private DNS name（验证私有 DNS 名称的域所有权）。
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 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

要使您的端点服务能够接受 IPv6 请求，其网络负载均衡器必须使用双堆栈 IP 地址类型。目标无需支持 IPv6 流量。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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 VPC 端点服务。
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 – 启用端点服务以接受 IPv4 请求。
   - 选择 IPv6 – 启用端点服务以接受 IPv6 请求。
   - 选择 IPv4 和 IPv6 – 启用端点服务以接受 IPv4 和 IPv6 请求。
6. 选择保存更改。

使用命令行修改支持的 IP 地址类型

- modify-vpc-endpoint-service-configuration (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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 VPC 端点服务。
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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 VPC 端点服务，然后选择 Endpoint connections（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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择 VPC 端点服务，然后选择 Allow principals（允许主体）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 端点服务的 DNS 名称

服务提供商可为其端点服务配置私有 DNS 名称。当服务提供商使用现有公有 DNS 名称作为其端点服务的私有 DNS 名称时，服务使用者无需更改任何使用现有公有 DNS 名称的应用程序。您必须先通过执行域所有权验证检查来证明您拥有该域，然后才能为端点服务配置私有 DNS 名称。

注意事项

- 端点服务只能有一个私有 DNS 名称。
- 不得为私有 DNS 名称创建 A 记录，以便只有服务使用者 VPC 中的服务器才能解析私有 DNS 名称。
- 网关负载均衡器端点不支持私有 DNS 名称。
- 要验证域，您必须拥有公有托管名称或公有 DNS 提供商。
- 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。您现在添加 b.example.com 作为私有 DNS 名称。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。

域所有权验证

您的域与一组域名服务（DNS）记录相关联，这些记录由您的 DNS 提供商管理。TXT 记录是一种 DNS 记录，可提供有关您的域的其他信息。其中包含一个名称和一个值。作为验证过程的一部分，您必须将 TXT 记录添加到公有域的 DNS 服务器。

当我们检测到域的 DNS 设置中存在 TXT 记录时，即完成域所有权验证。

添加记录后，您可以使用 Amazon VPC 控制台检查域验证过程的状态。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。依次选择 Actions（操作）、Verify domain ownership for private DNS name（验证私有 DNS 名称的域所有权）。

如果验证状态为 verified（已验证），则私有 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 desc ribe-vpc-endpoint-service-configurations AWS CLI 命令来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。创建 TXT 记录时，您需要使用 `Value` 和 `Name`。

```
[
    {
        "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。

名称	Type	值
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce: l6p0e 45jevfwoCP RxlTt

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，则可省略“_6e86v84tqgqubxbwii1m”，并且只需在 TXT 记录中使用“example.com”。

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”）。

将 TXT 记录添加到您的域的 DNS 服务器

将 TXT 记录添加到您的域的 DNS 服务器的过程取决于为您提供 DNS 服务的组织。您的 DNS 提供商可能是 Amazon Route 53 或其他域名注册商。

Amazon Route 53

为公有托管区创建记录。使用以下值：

- 对于 Record type（记录类型），选择 TXT。
- 对于 TTL (seconds) [TTL（秒）]，输入 **1800**。
- 对于 Routing policy（路由策略），选择 Simple routing（简单路由）。
- 对于 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

前往 DNS 提供商网站并登录您的账户。查找该页面以更新域的 DNS 记录。使用我们提供的名称和值来添加 TXT 记录。DNS 记录更新最长需要 48 小时生效，但通常情况下生效时间要早很多。

有关更具体的说明，请查阅 DNS 提供商提供的文档。下表提供了指向几个常用 DNS 提供商的文档链接。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/托管提供商	文档链接
GoDaddy	添加 TXT 记录
Dreamhost	添加自定义 DNS 记录
Cloudflare	管理 DNS 记录
HostGator	使用 HostGator /eNOM 管理 DNS 记录
Namecheap	如何为我的域添加 TXT/SPF/DKIM/DMARC 记录？
Names.co.uk	更改域的 DNS 设置
Wix	在您的 Wix 账户中添加或更新 TXT 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 DNS 名称域所有权验证 TXT 记录是否已正确发布到 DNS 服务器。你将运行该nslookup命令，该命令可用于 Windows 和 Linux。

您将查询为您的域名提供服务的 DNS 服务器，因为这些服务器包含的域 up-to-date 信息最多。您的域信息需要一定时间才会传播到其他 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 记录是否正确发布，其中 *name_server* 是您在上一步骤中找到的名称服务器之一。

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

3. 在上一步输出中，验证 `text =` 后面的字符串是否与 TXT 值匹配。

   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，则您可以从 TXT 记录中省略域验证名称（例如“_6e86v84tqgqubxbwii1m”）。
- 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 记录时在域名结尾添加句点。此步骤告知 DNS 提供商没有必要将域名附加到 TXT 记录。
- 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 TXT 记录值更改为仅使用小写字母，请联系他们获取帮助。
- 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 DNS 提供商不允许您拥有多条具有相同属性名称的 TXT 记录，请检查 DNS 提供商是否允许您将多个属性值分配给同一条 TXT 记录。例如，如果 DNS 由 Amazon Route 53 管理，则您可以按照以下步骤进行操作。

  1. 在 Route 53 控制台中，选择在验证第一个区域中的域时创建的 TXT 记录。
  2. 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 DNS 提供商不允许向同一条 TXT 记录分配多个值，则可以使用 TXT 记录的属性名称中的值来验证域一次，而另一次使用从属性名称中删除的值来验证域。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

使用以下过程为通知创建一个 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务。
4. 在 Notifications（通知）选项卡上，选择 Create notofication（创建通知）。
5. 对于 Notification ARN（通知 ARN），选择您创建的适用于 SNS 主题的 ARN。
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-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification（适用于 Windows 的工具 PowerShell）

添加访问策略

在 SNS 主题中添加 AWS PrivateLink 允许代表您发布通知的访问策略，如下所示。有关更多信息，请参阅如何编辑 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的 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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoint services（端点服务）。
3. 选择端点服务。
4. 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-configurations (AWS CLI)
- Remove-EC2EndpointServiceConfiguration（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 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS PrivateLink 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

内容

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 AWS PrivateLink。

服务用户-如果您使用该 AWS PrivateLink 服务完成工作，则您的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 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 AWS PrivateLink的访问权限的详细信息。

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 IAM 用户身份或通过担 AWS 账户根用户任 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 Identity Center）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。

当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 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您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《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

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。有关要求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 IAM Identity 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 Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定

的使用场景需要长期凭证以及 IAM 用户，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 组是一个指定一组 IAM 用户的身份。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，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 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，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

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，请创建角色并为角色定义权限。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创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。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 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。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）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 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，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 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。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务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 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 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》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 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 A@@ mazon EC2 上运行的应用程序 — 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。要向 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 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

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 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

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，用户可以代入角色。

IAM 策略定义操作的权限，无关乎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 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（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》中的创建 IAM 策略。

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。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。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中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 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 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》 中的访问控制列表（ACL）概览。

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 - 权限边界是一个高级功能，用于设置基于身份的策略可以为 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 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 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。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。

- 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。

如何 AWS PrivateLink 与 IAM 配合使用

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

您可以搭配使用的 IAM 功能 AWS PrivateLink

IAM 功能	AWS PrivateLink 支持
基于身份的策略	是
基于资源的策略	是
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
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 用户指南中的与 IAM 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附加到身份（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 用户指南中的创建 IAM 策略。

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。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

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

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。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》中的 IAM 角色与基于资源的策略有何不同。

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 策略的 `Action` 元素描述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。有一些例外情况，例如没有匹配 API 操作的仅限权限 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。

AWS PrivateLink 与亚马逊 EC2 共享其 API 命名空间。正在执行的策略操作在操作前 AWS PrivateLink 使用以下前缀：

```
ec2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "ec2:Describe*"
```

要查看 AWS PrivateLink 操作列表，请参阅 Amazon EC2 API 参考中的AWS PrivateLink 操作。有关更多信息，请参阅《服务授权参考》中的 Amazon EC2 定义的操作。

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 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）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，只有在使用 IAM 用户名标记 IAM 用户时，您才能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:VpceServiceName
- ec2:VpceServiceOwner
- ec2:VpcePrivateDnsName

要了解您可以对哪些操作和资源使用条件键，请参阅 Amazon EC2 定义的操作。

输入的 ACL AWS PrivateLink

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 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 with AWS PrivateLink

支持 ABAC（策略中的标签）	是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

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 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与 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。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

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《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。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 IAM 中的临时安全凭证。

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。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务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 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，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担任、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》中的创建向 AWS 服务委派权限的角色。

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与服务相关联的 AWS 服务服务角色。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 AWS API 执行任务。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，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

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

示例

- 控制 VPC 端点的使用
- 基于服务拥有者控制 VPC 端点创建
- 控制可为 VPC 端点服务指定的私有 DNS 名称
- 控制可为 VPC 端点服务指定的服务名称

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 端点控制对服务的访问的信息，请参阅 the section called “端点策略”。

基于服务拥有者控制 VPC 端点创建

您可以使用 ec2:VpceServiceOwner 条件键根据服务拥有者（amazon、aws-marketplace 或账户 ID）来控制可以创建的 VPC 端点。以下示例授予使用指定的服务拥有者创建 VPC 端点的权限。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"
                    ]
                }
            }
        }
    ]
}
```

控制可为 VPC 端点服务指定的私有 DNS 名称

您可以使用 ec2:VpceServicePrivateDnsName 条件键来控制可根据与 VPC 端点服务关联的私有 DNS 名称修改或创建哪些 VPC 端点服务。以下示例授予使用指定的私有 DNS 名称创建 VPC 端点服务的权限。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"
                    ]
                }
            }
        }
    ]
}
```

控制可为 VPC 端点服务指定的服务名称

您可以使用 ec2:VpceServiceName 条件键根据 VPC 端点服务名称来控制可以创建的 VPC 端点。以下示例授予使用指定的服务名称创建 VPC 端点的权限。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"
                    ]
                }
            }
        }
    ]
}
```

使用端点策略控制对 VPC 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。 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，如果您目前使用接口端点连接到 Amazon S3，则还可以使用 Amazon S3 存储桶策略来控制从特定端点或特定 VPC 对存储桶进行的访问。

内容

注意事项

- 端点策略是使用 IAM policy 语言的 JSON 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”。
- 当您为端点服务而非 AWS 服务创建 VPC 端点时，我们允许对该端点进行完全访问。

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

对于网关终端节点，必须将`Principal`元素设置为`*`。要指定委托人，请使用`aws:PrincipalArn`条件键。

```
"Condition": {
    "StringEquals": {
```

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

如果您按以下格式指定委托人，则 AWS 账户根用户 只能向该账户的用户和角色授予访问权限，而非所有用户和角色。

```
"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 端点策略

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. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择端点。
3. 选择 VPC 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。

使用命令行更新端点策略

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

AWS PrivateLink 的 CloudWatch 指标

AWS PrivateLink 会将有关接口端点、Gateway Load Balancer 端点和端点服务的数据点发布到 Amazon CloudWatch。利用 CloudWatch，您可以按一组有序的时间序列数据（称为指标）来检索关于这些数据点的统计数据。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，并在指标超出您的可接受范围时启动某个操作（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。预设情况下，AWS PrivateLink 会每隔一分钟向 CloudWatch 发送指标，并且不会产生额外的费用。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

目录

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。这包含处于 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。

指标	描述
	维度 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • 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	此端点收到的 RST 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。

维度	描述
VPC Endpoint Id	按 VPC 端点筛选指标数据。
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

指标	描述
	• Az, Load Balancer Arn, Service Id • 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	终端服务发送到端点的 RST 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

可使用 Amazon VPC 控制台、CloudWatch 控制台 或 AWS CLI 查看这些 CloudWatch 指标，具体如下。

使用 Amazon VPC 控制台查看指标

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints（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. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 AWS/PrivateLinkEndpoints 命名空间。
4. 选择 AWS/PrivateLinkServices 命名空间。

使用 AWS CLI 查看指标

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 为端点服务提供了内置的 Contributor Insights 规则，帮助您确定对各个受支持的指标而言贡献最大的端点。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的 Contributor Insights。

AWS PrivateLink 提供以下结果：

- `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` – 按发送到端点的 RST 数据包数进行端点排名。

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 Contributor Insights 费用的信息，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

按照以下过程，使用 AWS Management Console 或 AWS CLI 启用适用于 AWS PrivateLink 的内置规则。

使用控制台启用适用于 AWS PrivateLink 的 Contributor Insights 规则

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

使用 AWS CLI 启用适用于 AWS PrivateLink 的 Contributor Insights 规则

1. 使用以下 list-managed-insight-rules 命令枚举可用规则。对于 `--resource-arn` 选项，请指定端点服务的 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. 使用以下 put-managed-insight-rules 命令启用规则。您必须指定端点服务的模板名称和 ARN。

```
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

您可以随时禁用适用于 AWS PrivateLink 的内置规则。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。

使用控制台禁用适用于 AWS PrivateLink 的 Contributor Insights 规则

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

使用 AWS CLI 禁用适用于 AWS PrivateLink 的 Contributor Insights 规则

使用 disable-insight-rules 命令禁用规则。

删除 Contributor Insights 规则

按照以下过程，使用 AWS Management Console 或 AWS CLI 删除适用于 AWS PrivateLink 的内置规则。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。

使用控制台删除适用于 AWS PrivateLink 的 Contributor Insights 规则

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择 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）。

使用 AWS CLI 删除适用于 AWS PrivateLink 的 Contributor Insights 规则

使用 delete-insight-rules 命令删除规则。

AWS PrivateLink 配额

以下表格列出了您的账户的每区域 AWS PrivateLink 资源的配额（之前称为限制）。除非另有说明，否则您可以请求增加这些配额。有关更多信息，请参阅 Service Quotas User Guide（《服务限额用户指南》）中的 Requesting a quota increase（请求增加服务限额）。

如果您请求对每个资源提升适用的配额，我们将提升该区域中所有资源的配额。

名称	默认值	可调整	注释
每个 VPC 的接口和网关负载均衡器端点数	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 端点数	20	是	每个 VPC 最多可创建 255 个网关端点
每个 VPC 终端节点策略的字符数	20,480	不支持	VPC 端点策略的最大大小（包括空格）

以下注意事项适用于通过 VPC 端点传递的流量：

- 默认情况下，每个可用区的每个 VPC 端点可支持高达 10 Gbps 的带宽，并自动纵向扩展到高达 100 Gbps。在所有可用区之间分配负载时，VPC 端点的最大带宽等于可用区数量乘以 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) 是能够通过 VPC 端点传递的最大可允许数据包大小（以字节为单位）。MTU 越大，可在单个数据包中传递的数据越多。VPC 端点支持 8500 字节的 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 端点将对所有数据包强制执行最大分段大小 (MSS) 固定。有关更多信息，请参阅 RFC879。

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
指定的 IP 地址	在创建或修改 VPC 端点时，您可以为端点网络接口指定 IP 地址。	2023 年 8 月 17 日
IPv6 支持	您可以将网关负载均衡器端点服务和网关负载均衡器端点配置为同时支持 IPv4 和 IPv6 地址或仅支持 IPv6 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端点服务接受 IPv6 请求，即使他们的后端服务仅支持 IPv4。如果端点服务接受 IPv6 请求，则服务使用者可以为其接口端点启用 IPv6 支持，以便他们可以通过 IPv6 访问端点服务。	2022 年 5 月 11 日
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 VPC 中创建网关负载均衡器端点，将流量路由到	2020 年 11 月 10 日

	您使用网关负载均衡器配置的 VPC 端点服务。	
VPC 端点策略	您可以将某个 IAM policy 附加到某个 AWS 服务的接口 VPC 端点，以便控制对服务的访问。	2020 年 3 月 23 日
VPC 端点和端点服务的条件键	您可以使用 EC2 条件键来控制对 VPC 端点和端点服务的访问。	2020 年 3 月 6 日
在创建 VPC 端点和端点服务时添加标签	您可以在创建 VPC 端点和端点服务时添加标签。	2020 年 2 月 5 日
私有 DNS 名称	您可以使用私有 DNS 名称从您的 VPC 内访问 AWS PrivateLink 基于 VPC 的服务。	2020 年 1 月 6 日
VPC 端点服务	您可以创建自己的端点服务并允许其他 AWS 账户 账户和用户通过接口 VPC 端点连接到您的服务。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
接口 VPC 终端节点 AWS 服务	您 AWS PrivateLink 无需使用互联网网关或 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
适用于 DynamoDB 的 VPC 端点	您可以创建网关 VPC 端点以从您的 VPC 访问 Amazon DynamoDB，而无需使用互联网网关或 NAT 设备。	2017 年 8 月 16 日

Amazon S3 的 VPC 端点	您可以创建网关 VPC 端点以从您的 VPC 访问 Amazon S3，而无需使用互联网网关或 NAT 设备。	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。