aws

AWS Transit Gate

Amazon VPC

Amazon VPC: AWS Transit Gate

Table of Contents

什么是 Amazon VPC 公交网关？

Amazon Tr VPC ansit Gateways 是一个网络传输中心，用于互连虚拟私有云 (VPCs) 和本地网络。随着您的云基础设施在全球扩展，区域间对等互连使用 AWS 全球基础设施将中转网关连接在一起。 AWS 数据中心之间的所有网络流量都在物理层自动加密。Amazon Tr VPC ansit Gateways 是 Amazon Virtual Private Cloud(VPC) 的一项服务，可以在https://console.aws.amazon.com/vpc/家中通过亚马逊VPC控制台进行访问 #vpc/。

有关更多信息，请参阅 AWS Transit Gateway。

中转网关概念

以下是中转网关的关键概念：

- 挂载 — 您可以挂载以下各项：
  - 一个或多个 VPCs
  - Connect SD-WAN /第三方网络设备
  - 网 AWS Direct Connect 关
  - 与另一个中转网关的对等连接
  - 与传输网关的VPN连接
- T@@ ransit gateway 最大传输单位 (MTUMTU)-网络连接的最大传输单位 () 是可通过连接传递的最大允许数据包的大小（以字节为单位）。连接越MTU大，单个数据包中可以传递的数据就越多。传输网关支持VPCs、 AWS Direct Connect、Transi MTU t Gateway Connect 和对等连接附件（区域内、区域间和云WAN对等连接附件）之间的流量 8500 字节。通过VPN连接传输MTU的流量可以有 1500 字节。
- 中转网关路由表 — 中转网关具有默认的路由表，且可选具有其他路由表。路由表包含动态路由和静态路由，它们根据数据包的目标 IP 地址决定下一个跃点。这些路由的目标可以是任何中转网关挂载。默认情况下，Transit Gateway 挂载与默认的中转网关路由表关联。
- 关联 — 每个挂载都正好与一个路由表关联。每个路由表可以与零到多个附件关联。
- 路由传播-A VPC、VPN连接网关或 Direct Connect 网关可以将路由动态传播到公交网关路由表。默认情况下，使用 Connect 挂载，路由会传播到Transit Gateway路由表。使用时VPC，必须创建静态路由，才能将流量发送到传输网关。通过VPN连接，使用边界网关协议 (BGP) 将路由从传输网关传播到您的本地路由器。使用 Direct Connect 网关，允许的前缀源自您的本地路由器。BGP使用对等连接的连接时，您必须在中转网关路由表中创建静态路由以指向对等连接。

如何开始使用中转网关

使用以下资源帮助您创建和使用中转网关。

- 中转网关工作原理
- 开始使用公交网关
- 设计最佳实践

使用中转网关

可以使用以下任意接口创建、访问和管理中转网关：

- AWS Management Console — 提供您可用来访问中转网关的 Web 界面。
- AWS 命令行界面 (AWS CLI) — 为包括亚马逊在内的各种 AWS 服务提供命令，并在 Windows VPC、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。
- AWS SDKs— 提供特定于语言的API操作并处理许多连接细节，例如计算签名、处理请求重试和处理错误。有关更多信息，请参阅AWS SDKs。
- 查询 API-提供您使用HTTPS请求调用的低级API操作。使用查询API是访问 Amazon 的最直接方式 VPC，但它要求您的应用程序处理低级细节，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 参考文档。

定价

您需要按小时为中转网关上的每个挂载付费，并且需要为在中转网关上处理的流量付费。有关更多信息，请参阅 AWS Transit Gateway 定价。

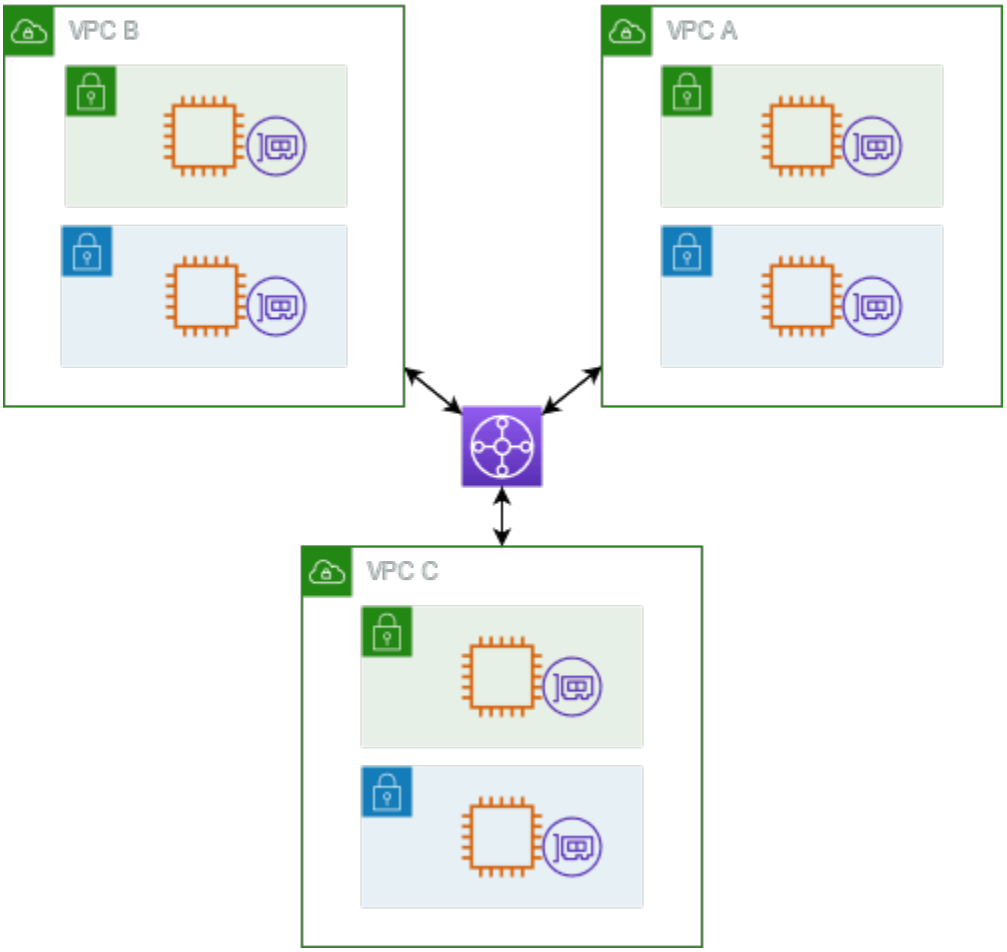
Amazon VPC 公交网关的工作原理

在 AWS Transit Gateway 中，传输网关充当区域虚拟路由器，用于在您的虚拟私有云 (VPCs) 和本地网络之间流动。中转网关根据网络流量的规模灵活地进行扩展。通过中转网关进行路由是在第 3 层运行的，其中，数据包根据其目的地 IP 地址发送到特定的下一个跃点挂载。

主题

架构图示例

下图显示了带有三个VPC附件的传输网关。其中每条路由的路由表都VPCs包括本地路由和将发往其他两条的流量发送VPCs到中转网关的路由。



以下是上图中所示挂载的原定设置中转网关路由表示例。每个CIDR区块都会VPC传播到路由表。从而让每个挂载都可以将数据包路由到另外两个挂载。

目标位置	目标	路由类型
VPC A CIDR	*Attachment for VPC A*	传播
VPC B CIDR	*Attachment for VPC B*	传播
VPC C CIDR	*Attachment for VPC C*	传播

资源连接

中转网关连接同时是数据包的源和目的地。您可以将以下资源附加到中转网关：

- 一个或多个VPCs。 AWS Transit Gateway 在VPC子网内部署弹性网络接口，然后由中转网关使用该接口来路由进出所选子网的流量。每个可用区必须至少有一个子网，以确保流量可以到达该可用区内每个子网中的资源。在创建挂载期间，只有在特定可用区内启用了某个子网时，才能确保同一可用区内的资源可到达该 Transit Gateway。如果子网路由表包含指向 Transit Gateway 的路由，则只有当 Transit Gateway 在同一可用区的子网中有挂载时，才会将流量转发到该 Transit Gateway。
- 一个或多个VPN连接
- 一个或多个 AWS Direct Connect 网关
- 一个或多个 Transit Gateway Connect 挂载
- 一个或多个中转网关对等连接
- 中转网关连接可同时是数据包的源和目的地。

等价多路径路由

AWS Transit Gateway 支持大多数附件的等价多路径 (ECMP) 路由。对于VPN附件，您可以在创建或修改传输网关时使用控制台启用或禁用ECMP支持。对于所有其他附件类型，适用以下ECMP限制：

- VPC-VPC 不支持，ECMP因为CIDR方块不能重叠。例如，您不能将VPC带有 CIDR 10.1.0.0/16 且秒钟VPC使用相同CIDR的 a 连接到传输网关，然后设置路由以对它们之间的流量进行负载平衡。
- VPN-禁用VPNECMP支持选项后，如果多条路径的前缀相等，公交网关将使用内部指标来确定首选路径。有关启用或禁用VPN附件ECMP的更多信息，请参阅the section called “中转网关”。
- AWS Transit Gateway Connec AWS Transit Gateway t-自动支持 Connect 附件ECMP。
- AWS Direct Connect 网 AWS Direct Connect 关-当网络前缀、前缀长度和 AS_ PATH 完全相同时，网关附件会自动支持ECMP多个 Direct Connect 网关附件。
- Transit gateway peering-不支持 Transit 网关对等，ECMP因为它既不支持动态路由，也无法针对两个不同的目标配置相同的静态路由。

> **Note**
>
> - BGP不支持 Multipath AS-Path Relax，因此您不能ECMP在不同的自治系统编号上使用 () ASNs。
> - ECMP不支持在不同的附件类型之间使用。例如，您无法在VPN和VPC附件ECMP之间启用。相反，将对中转网关路由进行评估，并根据评估的路径路由流量。有关更多信息，请参阅 the section called “路由评估顺序”。

- 单个 Direct Connect 网关支持ECMP跨多个传输虚拟接口。因此，我们建议您仅设置和使用单个 Direct Connect 网关，不要设置和使用多个网关来利用ECMP。有关 Direct Connect 网关和公共虚拟接口的更多信息，请参阅如何设置从公共虚拟接口 AWS 到的主动/主动或主动/被动 Direct Connect 连接？ 。

可用区

将连接到传输网关时，必须启用一个或多个可用区，供中转网关使用，将流量路由到VPC子网中的资源。VPC要启用每个可用区，您应指定确切一个子网。中转网关使用此子网中的一个 IP 地址将网络接口放入该子网中。启用可用区后，流量可以路由到中的所有子网VPC，而不仅仅是指定的子网或可用区。然而，只有驻留在拥有中转网关连接的可用区内的资源，才能到达中转网关。

如果流量来自目标附件不存在的可用区，则 Transit Gateway 将在内部将该流量路由到存在该附件的随机可用区。 AWS 对于这种类型的跨可用区流量，无需支付额外的中转网关费用。

我们建议您启用多个可用区以确保可用性。

使用设备模式支持

如果您计划在中配置有状态的网络设备VPC，则可以为设备所在的VPC附件启用设备模式支持。这可确保传输网关在源和目标之间的流量流的生命周期内对该VPC连接使用相同的可用区。它还允许传输网关向中的任何可用区发送流量VPC，前提是该区域中存在子网关联。有关更多信息，请参阅 示例：共享服务中的设备 VPC。

路由

您的中转网关使用传输网关路由表在附件之间路由IPv4和IPv6数据包。您可以将这些路由表配置为传播来自已连接网关VPCs、VPN连接网关和 Direct Connect 网关的路由表中的路由。您还可以将静态路由添加到中转网关路由表中。当数据包来自一个连接时，会使用与目的地 IP 地址相符的路由，将该数据包路由到另一个连接。

中转网关对等连接仅支持静态路由。

路由主题

- 路由表
- 路由表关联
- 路由传播

- 对等连接的路由
- 路由评估顺序

路由表

您的中转网关自动附带默认路由表。默认情况下，此路由表是默认的关联路由表和默认的传播路由表。或者，如果您禁用路由传播和路由表关联， AWS 不会为中转网关创建默认路由表。

您可以为中转网关创建其他路由表。这样，您就可以隔离连接的子网。每个连接可以与一个路由表相关联。一个挂载可以将其路由传播到一个或多个路由表。

您可以在中转网关路由表中创建丢弃与路由匹配的流量的黑洞路由。

将连接到传输网关时，必须VPC向子网路由表中添加路由，流量才能通过中转网关进行路由。有关更多信息，请参阅《亚马逊VPC用户指南》中的 Transit Gateway 路由。

路由表关联

您可以将中转网关连接与单个路由表相关联。每个路由表可以与零到多个连接关联，并可以将数据包转发到其他连接。

路由传播

每个挂载都附带可以安装到一个或多个中转网关路由表的路由。当挂载传播到中转网关路由表时，这些路由安装在路由表中。您无法根据通告的路由进行筛选。

对于VPC附件，的CIDR块VPC会传播到公交网关路由表。

当动态路由与VPN连接或 Direct Connect 网关连接一起使用时，您可以将从本地路由器获知的路由传播BGP到任何中转网关路由表。

当动态路由与VPN附件一起使用时，路由表中与该VPN连接关联的路由将通过BGP通告到客户网关。

对于 Connect 附件，路由表中与 Connect 附件关联的路由会通告给以VPC直BGP通方式运行的第三方虚拟WAN设备，例如 SD 设备。

对于 Direct Connect 网关连接，允许的前缀交互控制从哪些路由通告到客户网络。 AWS

当静态路由和传播路由具有相同的目标时，静态路由具有更高的优先级，因此传播路由不包含在路由表中。如果移除静态路由，则重叠的传播路由将包含在路由表中。

对等连接的路由

您可以将两个中转网关对等连接并在它们之间路由流量。为此，您可以在中转网关上创建对等挂载，并指定要与其创建对等连接的对等中转网关。然后，您可以在中转网关路由表中创建静态路由，以将流量路由到中转网关对等挂载。然后，路由到对等传输网关的流量可以路由到对等传输网关的VPC和VPN附件。

有关更多信息，请参阅 示例：对等中转网关。

路由评估顺序

中转网关路由是按以下顺序评估的：

- 目标地址的最具体路由。
- 对于具有相同CIDR但来自不同连接类型的路由，路由优先级如下所示：
  - 静态路由（例如，站点到站点的VPN静态路由）
  - 前缀列表引用的路由
  - VPC-传播路由
  - Direct Connect 网关传播路由
  - Transit Gateway 连接传播路由
  - 通过专用 Direct Connect 传播VPN的路由进行站点到站点
  - 站点到站点传播的路由 VPN
  - Transit Gateway 对等传播路由（云端）WAN

某些附件支持路径通告BGP。对于具有相同CIDR连接类型且来自相同连接类型的路由，路由优先级由BGP属性控制：

- 缩短 AS 路径长度
- 较低的MED值
- 如果附件支持 e ov BGP er i BGP 路由，则首选

> **Important**
>
> AWS 无法保证具有与上面列出的相同CIDR、附件类型和BGP属性的BGP路径的路径优先顺序一致。

AWS Transit Gateway 仅显示首选路线。只有当不再公布备用路由时，备用路由才会显示在 Transit Gateway 路由表中，例如，如果您通过 Direct Connect 网关和站点到站点VPN通告相同的路由。 AWS Transit Gateway 将仅显示从 Direct Connect 网关路由（首选路由）收到的路由。站点到站VPN点（即备用路由）仅在不再通告 Direct Connect 网关时才会显示。

VPC和公交网关路由表的区别

无论您使用的是路由表还是公交网关VPC路由表，路由表评估都会有所不同。

以下示例显示了VPC路由表。VPC本地路由的优先级最高，其次是最具体的路由。在静态路由和传播的路由具有相同的目标时，静态路由具有更高的优先级。

目的地	目标	优先级
10.0.0.0/16	本地	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345（静态）或 tgw-12345（静态）	2
172.31.0.0/16	vgw-12345（传播）	3
0.0.0.0/0	igw-12345	4

以下示例显示了公交网关路由表。如果您更喜欢 AWS Direct Connect 网关连接而不是VPN连接，请使用BGPVPN连接并在公交网关路由表中传播路由。

目标位置	连接（目标）	资源类型	路由类型	优先级
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	静态或传播	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	静态	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect 网关	传播	3

目标位置	连接（目标）	资源类型	路由类型	优先级
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	连接	传播	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	传播	5

公交网关场景示例

以下是中转网关的常见使用案例。您的中转网关并不仅限于这些使用案例。

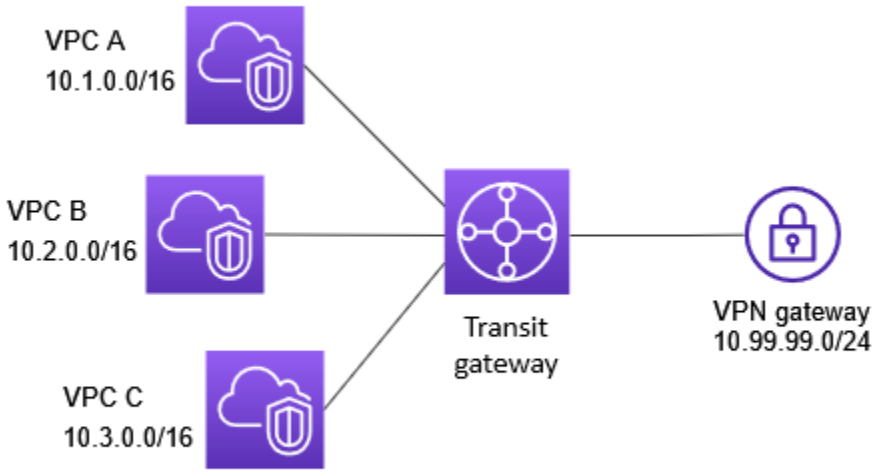
示例：集中式路由器

您可以将传输网关配置为连接所有VPCs AWS Direct Connect、和站点到站点VPN连接的集中式路由器。在该方案中，所有连接与中转网关默认路由表相关联，并传播到中转网关默认路由表。因此，所有挂载都可以将数据包路由到彼此，而将中转网关用作简单第 3 层 IP 路由器。

内容

概述

下表展示了此场景配置的主要组成部分。在这种情况下，传输网关有三个VPC附件和一个站点到站点VPN连接。来自 VPC A、VPC B 和 VPC C 中子网的数据包如果发往另一个子网中的子网VPC或VPN连接的第一个子网，则通过中转网关路由。



资源

为此场景创建以下资源：

- 三VPCs。有关创建的信息VPC，请参阅《Amazon VPC 用户指南》VPC中的创建。
- 中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
- 公交网关上有三个VPC附件。有关更多信息，请参阅 the section called “创建VPC附件”。
- 传输网关上的点对点VPN连接。每个CIDR区块都会VPC传播到公交网关路由表。VPN连接建立后，BGP会话即建立，站点到站点VPNCIDR传播到中转网关路由表，然后添加到客户网关表中。VPC CIDRs BGP有关更多信息，请参阅 the section called “创建与 a 的公交网关连接 VPN”。

  务必查看 AWS Site-to-Site VPN 用户指南中的客户网关设备的要求。

路由

每个都VPC有一个路由表，还有一个公交网关的路由表。

VPC路由表

每个都VPC有一个包含 2 个条目的路由表。第一个条目是中本地IPv4路由的默认条目VPC；此条目使该条目中的实例VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。下表显示了 VPC A 路由。

目标位置	目标
10.1.0.0/16	本地
0.0.0.0/0	tgw-id

中转网关路由表

下面是前一个图中显示的连接的默认路由表示例（启用了路由传播）。

目的地	目标	路由类型
10.1.0.0/16	*Attachment for VPC A*	传播
10.2.0.0/16	*Attachment for VPC B*	传播
10.3.0.0/16	*Attachment for VPC C*	传播
10.99.99.0/24	*Attachment for VPN connection*	传播

客户网关BGP表

客户网关BGP表包含以下内容VPCCIDRs。

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

示例：隔离 VPCs

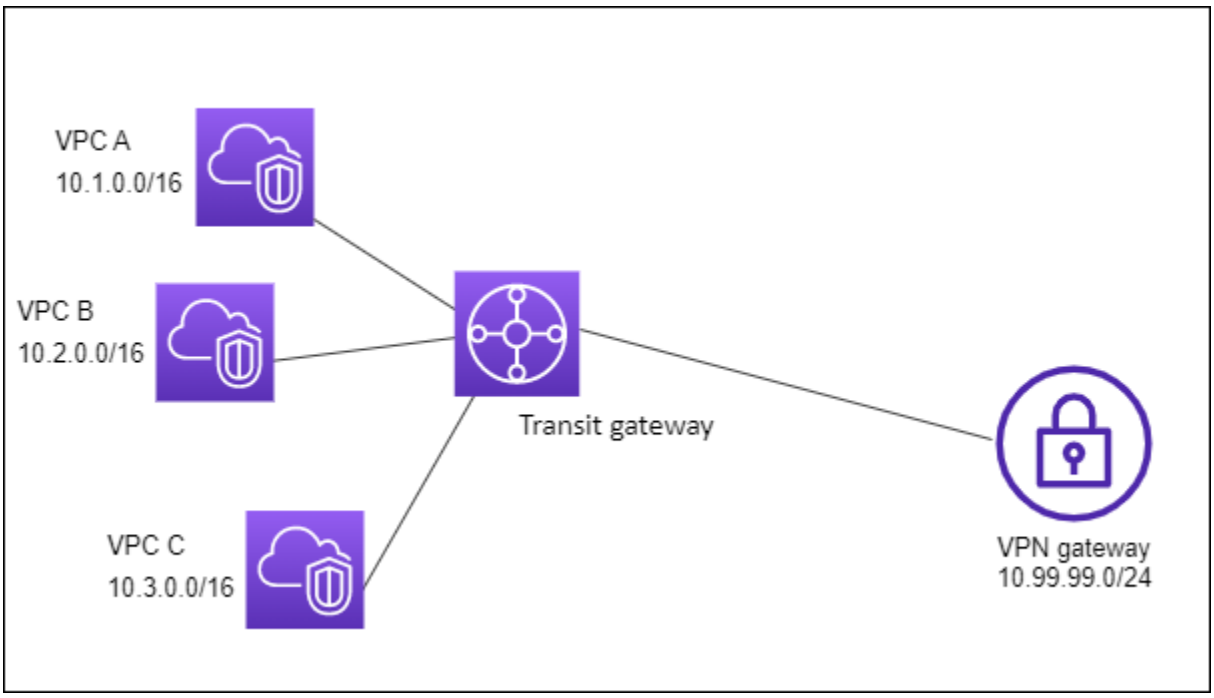
您可以将中转网关配置为多个隔离的路由器。这类似于使用多个中转网关，但在路由和挂载可能更改的情况下可提供更大的灵活性。在此方案中，每个隔离的路由器都有单个路由表。所有与隔离的路由器关

联的连接都传播其路由表并与这些路由表关联。与一个隔离的路由器关联的连接可以将数据包路由到彼此，但无法将数据包路由到另一个隔离路由器的连接或从中接收数据包。

内容

概述

下表展示了此场景配置的主要组成部分。来自 VPC A、VPC B 和 VPC C 的数据包会路由到传输网关。来自 VPC A、VPC B 和 VPC C 中以互联网为目的地的子网的数据包首先通过传输网关，然后路由到站点到站点VPN连接（如果目的地位于该网络内）。来自一个VPC的数据包如果目的地为另一个VPC子网（例如从 10.1.0.0 到 10.2.0.0），则会通过中转网关进行路由，但由于传输网关路由表中没有针对它们的路由，它们会被阻塞。



资源

为此场景创建以下资源：

- 三VPCs。有关创建的信息VPC，请参阅《Amazon VPC 用户指南》VPC中的创建。
- 中转网关。有关更多信息，请参阅 the section called “创建中转网关”。

- 三者的公交网关上有三个附件VPCs。有关更多信息，请参阅 the section called “创建VPC附件”。
- 传输网关上的点对点VPN连接。有关更多信息，请参阅 the section called “创建与 a 的公交网关连接VPN”。务必查看 AWS Site-to-Site VPN 用户指南中的客户网关设备的要求。

VPN连接启动后，BGP会话即建立，会话VPNCIDR传播到中转网关路由表，然后添加到客户网关BGP表中。VPC CIDRs

路由

每个都VPC有一个路由表，公交网关有两个路由表VPCs，一个用于连接。VPN

VPCA、VPC B 和 VPC C 路由表

每个都VPC有一个包含 2 个条目的路由表。第一个条目是中本地IPv4路由的默认条目VPC。此条目使该条目中的实例VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。下表显示了 VPC A 路由。

目标位置	目标
10.1.0.0/16	本地
0.0.0.0/0	tgw-id

中转网关路由表

此场景使用一个路由表作为连接，VPCs使用一个路由表作为VPN连接。

这些VPC附件与以下路由表相关联，该路由表具有该VPN连接的传播路由。

目标位置	目标	路由类型
10.99.99.0/24	*Attachment for VPN connection*	传播

该VPN附件与以下路由表相关联，该路由表包含每个VPC附件的传播路由。

目标位置	目标	路由类型
10.1.0.0/16	*Attachment for VPC A*	传播
10.2.0.0/16	*Attachment for VPC B*	传播
10.3.0.0/16	*Attachment for VPC C*	传播

有关在中转网关路由表中传播路由的更多信息，请参阅使用 Amazon Transit Gateways 启用传输到VPC公交网关路由表的路由。

客户网关BGP表

客户网关BGP表包含以下内容VPCCIDRs。

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

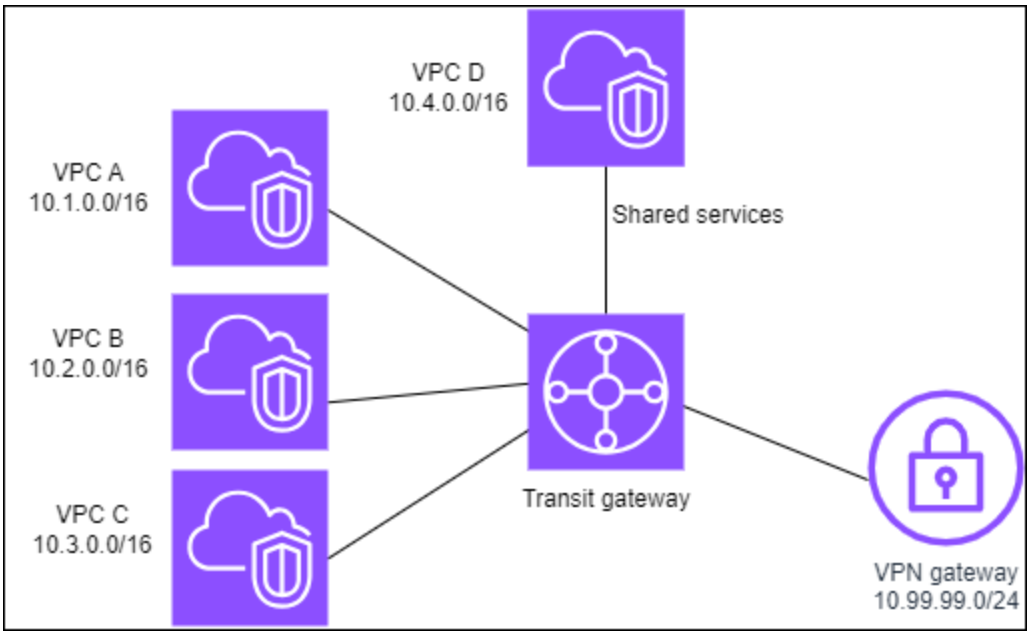
示例：VPCs使用共享服务隔离

您可以将中转网关配置为多个使用共享服务的隔离路由器。这类似于使用多个中转网关，但在路由和挂载可能更改的情况下可提供更大的灵活性。在此方案中，每个隔离的路由器都有单个路由表。所有与隔离的路由器关联的连接都传播其路由表并与这些路由表关联。与一个隔离的路由器关联的连接可以将数据包路由到彼此，但无法将数据包路由到另一个隔离路由器的连接或从中接收数据包。连接可以将数据包路由到共享服务，或从共享服务中接收数据包。如果您具有需要隔离的组，但这些组使用共享服务（例如生产系统），则可以使用该方案。

内容

概述

下表展示了此场景配置的主要组成部分。来自 VPC A、VPC B 和 VPC C 中以互联网为目的地的子网的数据包，首先通过传输网关进行路由，然后路由到客户网关进行站点VPN到站点。来自 VPC A、VPC B 或 VPC C 中子网且目的地为 VPC A、VPC B 或 VPC C 子网的数据包通过中转网关路由，由于传输网关路由表中没有针对它们的路由，它们会被阻塞。来自 VPC A、VPC B 和 VPC C 的数据包以 VPC D 作为目的路由，通过传输网关，然后到达 VPC D。



资源

为此场景创建以下资源：

- 四VPCs。有关创建的信息VPC，请参阅《Amazon VPC 用户指南》VPC中的创建。
- 中转网关。有关更多信息，请参阅创建中转网关。
- 公交网关上有四个附件，每个附件VPC。有关更多信息，请参阅 the section called “创建VPC附件”。
- 传输网关上的点对点VPN连接。有关更多信息，请参阅 the section called “创建与 a 的公交网关连接VPN”。

  务必查看 AWS Site-to-Site VPN 用户指南中的客户网关设备的要求。

VPN连接启动后，BGP会话即建立，会话VPNCIDR传播到中转网关路由表，然后添加到客户网关BGP表中。VPC CIDRs

- 每个隔离路由表VPC都与隔离路由表相关联并传播到共享路由表。
- 每个共享服务VPC都与共享路由表相关联并传播到两个路由表。

路由

每个都VPC有一个路由表，公交网关有两个路由表，一个用于VPN连接和共享服务。VPCs VPC

VPCA、VPC B、VPC C 和 VPC D 路由表

每个路由表VPC都有包含两个条目的路由表。第一个条目是中本地路由的默认条目VPC；此条目使该条目中的实例VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。

目标位置	目标
10.1.0.0/16	本地
0.0.0.0/0	*transit gateway ID*

中转网关路由表

此场景使用一个路由表作为连接，VPCs使用一个路由表作为VPN连接。

VPCA、B 和 C 附件与以下路由表相关联，该路由表包含VPN连接的传播路径和用于 D 的连接的传播路由。VPC

目标位置	目标	路由类型
10.99.99.0/24	*Attachment for VPN connection*	传播
10.4.0.0/16	*Attachment for VPC D*	传播

VPN附件和共享服务 VPC (VPCD) 附件与以下路由表相关联，其中包含指向每个VPC附件的条目。这允许通过VPN连接和共享服务与之通信VPC。VPCs

目标位置	目标	路由类型
10.1.0.0/16	*Attachment for VPC A*	传播

目标位置	目标	路由类型
10.2.0.0/16	*Attachment for VPC B*	传播
10.3.0.0/16	*Attachment for VPC C*	传播

有关更多信息，请参阅 使用 Amazon Transit Gateways 启用传输到VPC公交网关路由表的路由。

客户网关BGP表

客户网关BGP表包含所有四个网关CIDRs的VPCs。

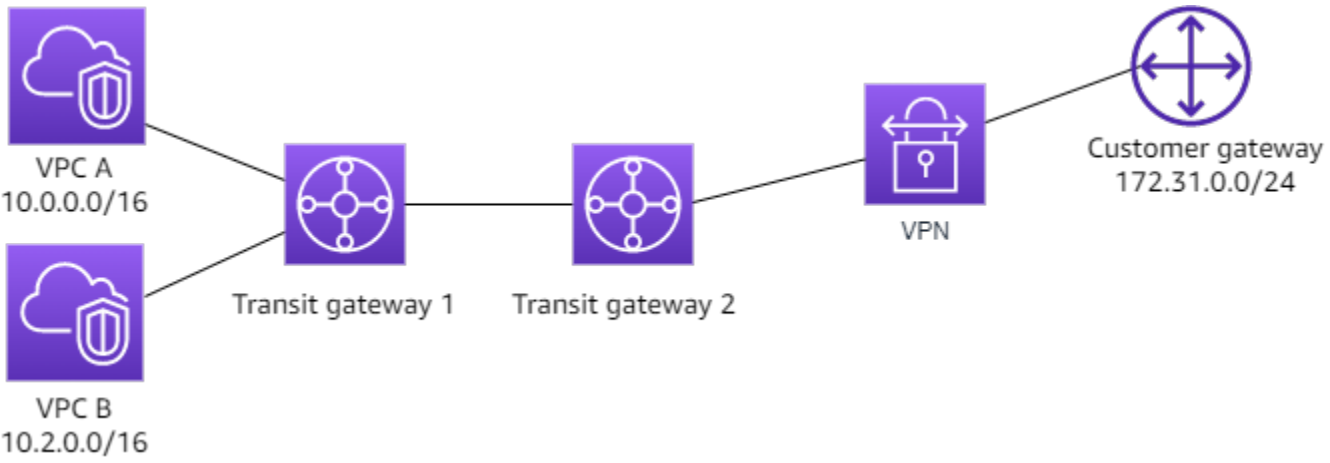
示例：对等中转网关

您可以在多个中转网关之间创建中转网关对等连接。然后，您可以在各个中转网关的连接之间路由流量。在这种情况下，VPN附件VPC与公交网关的默认路由表相关联，它们会传播到公交网关的默认路由表。每个中转网关路由表都有一个指向中转网关对等连接的静态路由。

内容

概述

下表展示了此场景配置的主要组成部分。传输网关 1 有两个VPC附件，中转网关 2 有一个站点到站点连接VPN。来自 VPC A 和 VPC B 中以 Internet 为目的地的子网的数据包首先通过传输网关 1 进行路由，然后通过传输网关 2 进行路由，然后路由到VPN连接。



资源

为此场景创建以下资源：

- 二VPCs。有关创建的信息VPC，请参阅《Amazon VPC 用户指南》VPC中的创建。
- 两个中转网关。它们可位于相同的区域或不同的区域中。有关更多信息，请参阅 the section called “创建中转网关”。
- 第一个公交网关上有两个VPC附件。有关更多信息，请参阅 the section called “创建VPC附件”。
- 第二个传输网关上的点对点VPN连接。有关更多信息，请参阅 the section called “创建与 a 的公交网关连接 VPN”。务必查看 AWS Site-to-Site VPN 用户指南中的客户网关设备的要求。
- 两个中转网关之间的中转网关对等挂载。有关更多信息，请参阅 Amazon 公交网关中的公VPC交网关对等连接附件。

创建附件时，每个VPC附件都会VPC传播到公交网关 1 的路由表。CIDRsVPN连接开启后，会发生以下操作：

- 会BGP话已建立
- 点对点VPNCIDR传播到中转网关 2 的路由表
- VPCCIDRs已添加到客户网关BGP表中

路由

每个网关都VPC有一个路由表，每个中转网关都有一个路由表。

VPCA 和 VPC B 路由表

每个都VPC有一个包含 2 个条目的路由表。第一个条目是中本地IPv4路由的默认条目VPC。此默认条目使该条目中的资源VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。下表显示了 VPC A 路由。

目标位置	目标
10.0.0.0/16	本地
0.0.0.0/0	tgw-1-id

中转网关路由表

以下是中转网关 1 的默认路由表示例，其中启用了路由传播。

目的地	目标	路由类型
10.0.0.0/16	*Attachment ID for VPC A*	传播
10.2.0.0/16	*Attachment ID for VPC B*	传播
0.0.0.0/0	*Attachment ID for peering connection*	静态

以下是中转网关 2 的默认路由表示例，其中启用了路由传播。

目的地	目标	路由类型
172.31.0.0/24	*Attachment ID for VPN connection*	传播
10.0.0.0/16	*Attachment ID for peering connection*	static
10.2.0.0/16	*Attachment ID for peering connection*	static

客户网关BGP表

客户网关BGP表包含以下内容VPCCIDRs。

- 10.0.0.0/16
- 10.2.0.0/16

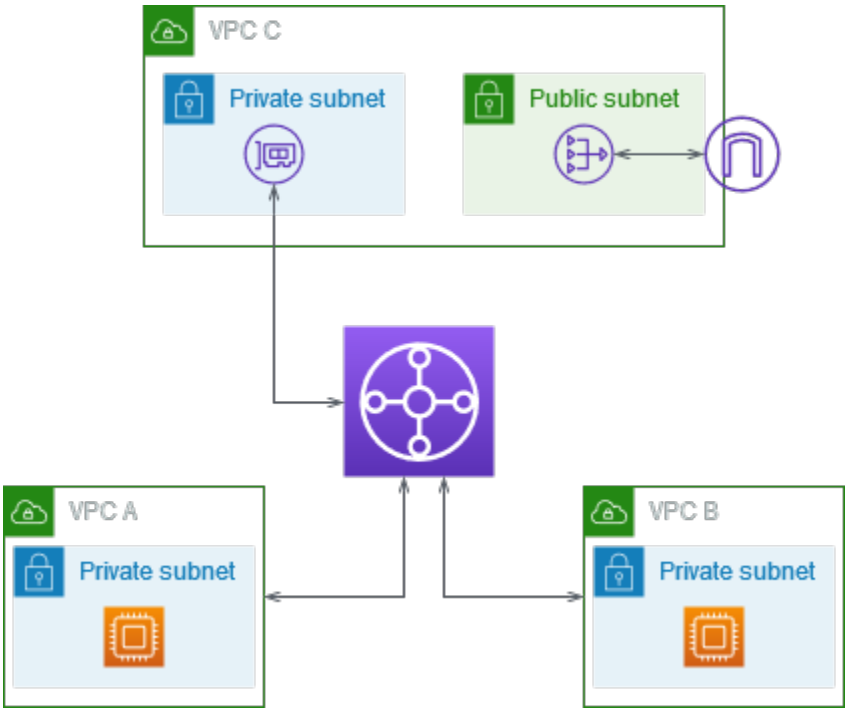
示例：到互联网的集中出站路由

您可以配置传输网关，将出站 Internet 流量从VPC没有 Internet 网关的VPC，路由到包含NAT网关和互联网网关的。

内容

概述

下表展示了此场景配置的主要组成部分。您在 VPC A 和 VPC B 中有只需要出站访问互联网的应用程序。您可以将 VPC C 配置为公用NAT网关和 Internet 网关，以及用于VPC连接的私有子网。将所有连接VPCs至公交网关。配置路由，使来自 VPC A 和 VPC B 的出站 Internet 流量通过传输网关到 VPC C。VPC C 中的NAT网关将流量路由到互联网网关。



资源

为此场景创建以下资源：

- 三VPCs个 IP 地址范围不重叠。有关更多信息，请参阅 Amazon VPC 用户指南VPC中的创建。

- VPCA 和 VPC B 各有带EC2实例的私有子网。
- VPCC 有以下几点：
  - 连接到. 的互联网网关VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的创建和连接互联网网关。
  - 带有网NAT关的公有子网。有关更多信息，请参阅 Amazon VPC 用户指南中的创建NAT网关。
  - 用于中转网关连接的私有子网。私有子网应与公有子网位于同一个可用区。
- 一个中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
- 公交网关上有三个VPC附件。每个CIDR区块都会VPC传播到公交网关路由表。有关更多信息，请参阅 the section called “创建VPC附件”。对于 VPC C，必须使用私有子网创建附件。如果您使用公有子网创建挂载，则实例流量会路由到互联网网关，但互联网网关会丢弃流量，因为实例没有公有 IP 地址。通过将连接置于私有子网中，流量将路由到NAT网关，网NAT关使用其弹性 IP 地址作为源 IP 地址将流量发送到互联网网关。

路由

每个都有路由表VPC，公交网关都有路由表。

路由表

- VPCA 的路由表
- VPCB 的路由表
- VPCC 的路由表
- 中转网关路由表

VPCA 的路由表

以下是一个示例路由表。第一个条目使中的VPC实例能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。

目标位置	目标
VPC A CIDR	本地
0.0.0.0/0	*transit-gateway-id*

VPCB 的路由表

以下是一个示例路由表。第一个条目使中的实例VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。

目标位置	目标
VPC B CIDR	本地
0.0.0.0/0	*transit-gateway-id*

VPCC 的路由表

通过向 Internet NAT 网关添加路由，将网关配置为公有子网。将另一个子网保留为私有子网。

以下是公有子网的示例路由表。第一个条目使中的VPC实例能够相互通信。第二个和第三个条目将 VPC A 和 VPC B 的流量路由到中转网关。其余条目将所有其他IPv4子网流量路由到互联网网关。

目标位置	目标
VPC C CIDR	本地
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

以下是私有子网的示例路由表。第一个条目使中的VPC实例能够相互通信。第二个条目将所有其他IPv4子网流量路由到NAT网关。

目标位置	目标
VPC C CIDR	本地
0.0.0.0/0	*nat-gateway-id*

中转网关路由表

以下是中转网关路由表的示例。每个CIDR区块都会VPC传播到公交网关路由表。静态路由向 VPC C 发送出站 Internet 流量。您可以选择通过为每个VPCCIDR路由添加黑洞路由来防止相互VPC通信。

CIDR	Attachment	路由类型
VPC A CIDR	*Attachment for VPC A*	传播
VPC B CIDR	*Attachment for VPC B*	传播
VPC C CIDR	*Attachment for VPC C*	传播
0.0.0.0/0	*Attachment for VPC C*	static

示例：共享服务中的设备 VPC

您可以在共享服务中配置设备（例如安全设备）VPC。设备首先在共享服务VPC中检查在公交网关附件之间路由的所有流量。启用设备模式后，传输网关会使用流哈希算法选择设备VPC中的单个网络接口，在流量生命周期内将流量发送到该接口。中转网关为返程流量使用相同的网络接口。这可确保双向流量以对称方式路由，即在流量生命周期内，双向流量通过连接中的同一个可用区进行路由。VPC如果您的架构中有多个中转网关，则每个中转网关都保持自己的会话关联性，并且每个中转网关可以选择不同的网络接口。

您必须将一个传输网关与设备连接起来，VPC以保证流量粘性。将多个传输网关连接到单个设备并VPC不能保证流量粘性，因为传输网关之间不共享流量状态信息。

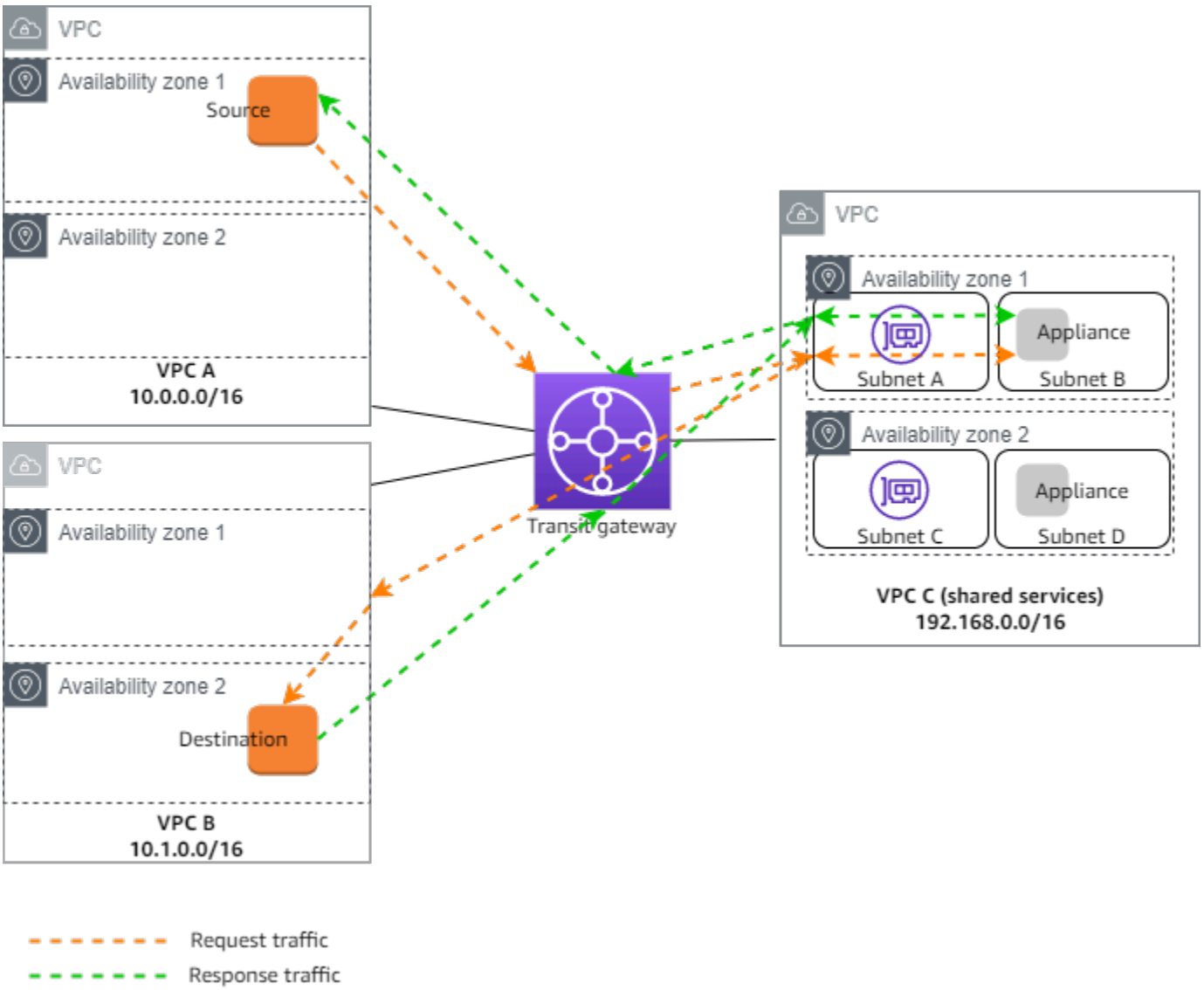
Important

- 只要源流量和目标流量从同一个传输网关连接进入集中VPC（检查VPC），设备模式下的流量就可以正确路由。如果源和目的地位于两个不同的公交网关连接上，则流量可能会下降。如果集中网络VPC接收来自其他网关（例如 Internet 网关）的流量，然后在检查后将该流量发送到传输网关附件，则流量可能会下降。
- 在现有连接上启用设备模式可能会影响该附件的当前路由，因为该连接可能会流经任何可用区。未启用设备模式时，流量将保持到原始可用区的流量。

内容

概述

下表展示了此场景配置的主要组成部分。公交网关有三个VPC附件。VPCC 是共享服务VPC。VPCA 和 VPC B 之间的流量被路由到传输网关，然后路由到 VPC C 中的安全设备进行检查，然后再路由到最终目的地。设备是一个有状态的设备，因此将同时检查请求和响应流量。为了实现高可用性，VPCC 语言的每个可用区中都有一个设备



您为此场景创建以下资源：

- 三VPCs。有关创建的信息VPC，请参阅《Amazon Virtual Private Cloud 用户指南》VPC中的创建。
- 中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
- 三个VPC附件-每个附件VPCs。有关更多信息，请参阅 the section called “创建VPC附件”。

  对于每个VPC附件，在每个可用区中指定一个子网。对于共享服务VPC，这些子网是流量VPC从中转网关路由到的子网。在前面的示例中，这些是子网 A 和 C。

  对于 VPC C 的VPC附件，启用设备模式支持，以便响应流量路由到 VPC C 中与源流量相同的可用区。

  Amazon VPC 控制台支持设备模式。您也可以使用 Amazon VPC API AWS SDK、an、启用设备模式或 AWS CloudFormation。 AWS CLI 例如，在-attachment或 create-transit-gateway-vpcmodify-transit-gateway-vpc-attachmen t命令中添加`--options ApplianceModeSupport=enable`。

> **Note**
>
> 只有源自检查的源流量和目标流量才能保证设备模式下的流量粘性。VPC

有状态设备和设备模式

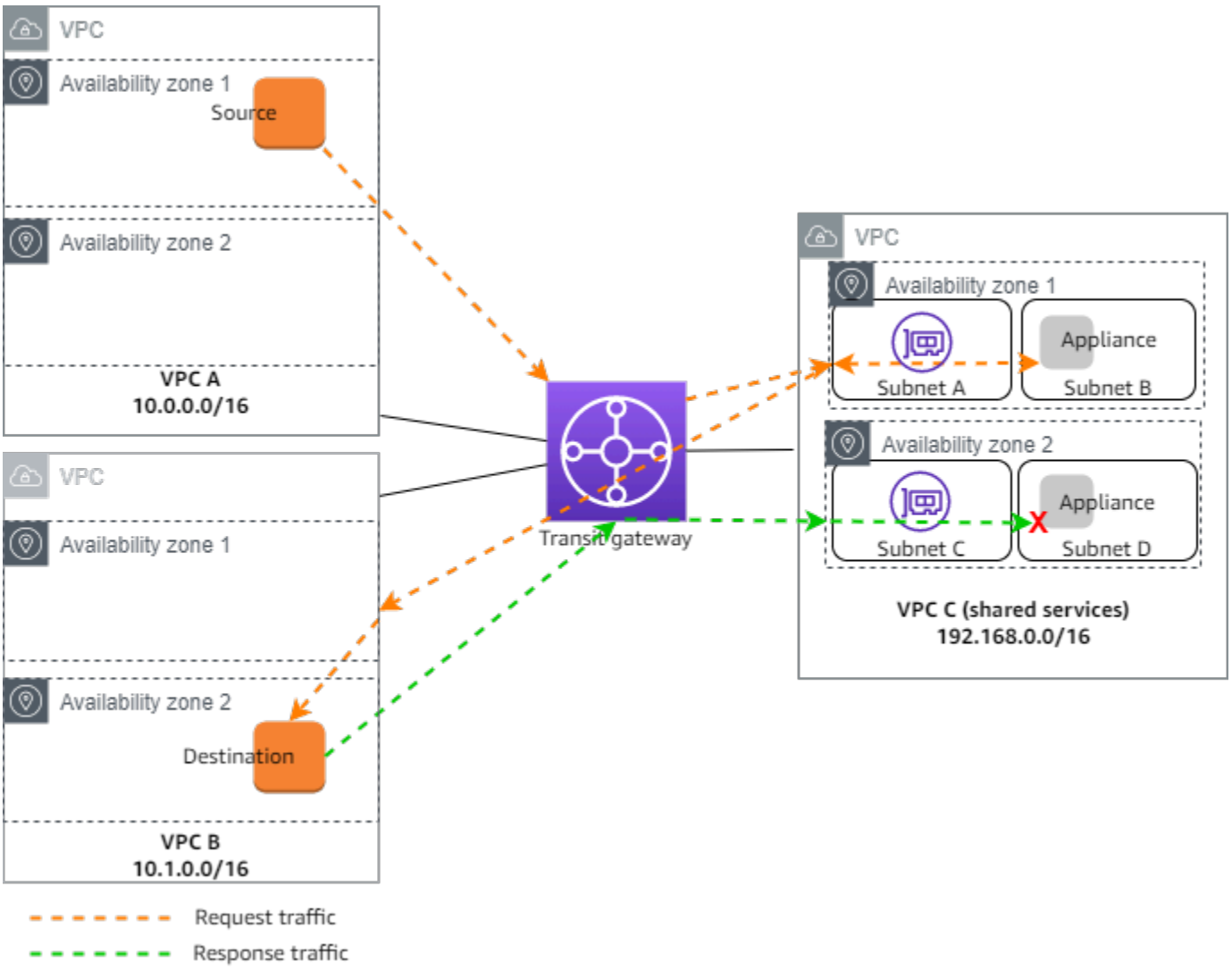
如果您的VPC附件跨越多个可用区，并且您要求源主机和目标主机之间的流量通过同一台设备进行状态检查，请为设备所在的VPC附件启用设备模式支持。

有关更多信息，请参阅 AWS 博客中的集中检查架构。

未启用设备模式时的行为

如果未启用设备模式，则传输网关会尝试保持流量在原始可用区的VPC附件之间路由，直到流量到达目的地。只有当可用区出现故障或该可用区中没有与附件关联的子网时，流量才会在VPC附件之间穿过可用区。

下图显示未启用设备模式支持时的流量。源自 VPC B 中可用区 2 的响应流量由传输网关路由到 VPC C 中的同一个可用区。因此，由于可用区 2 中的设备不知道来自 A 中来源的原始请求，因此流量会被丢弃。VPC



路由

每个路由表都VPC有一个或多个路由表，公交网关有两个路由表。

VPC路由表

VPCA 和 VPC B

VPCsA 和 B 的路由表有 2 个条目。第一个条目是中本地IPv4路由的默认条目VPC。此默认条目使该条目中的资源VPC能够相互通信。第二个条目将所有其他IPv4子网流量路由到传输网关。以下是 VPC A 的路由表。

目标位置	目标

目标位置	目标
10.0.0.0/16	本地
0.0.0.0/0	tgw-id

VPCC

共享服务 VPC (VPCC) 的每个子网都有不同的路由表。子网 A 由传输网关使用（您在创建VPC连接时指定此子网）。子网 A 的路由表将所有流量路由到子网 B 中的设备。

目的地	目标
192.168.0.0/16	本地
0.0.0.0/0	appliance-eni-id

子网 B（包含设备）的路由表将流量路由回中转网关。

目的地	目标
192.168.0.0/16	本地
0.0.0.0/0	tgw-id

中转网关路由表

此公交网关对 VPC A 和 VPC B 使用一个路由表，为共享服务 VPC (VPCC) 使用一个路由表。

VPCA 和 VPC B 附件与以下路由表相关联。路由表将所有流量路由到 VPC C。

目标位置	目标	路由类型
0.0.0.0/0	*Attachment ID for VPC C*	static

VPCC 连接与以下路由表关联。它将流量路由到 VPC A 和 VPC B。

目标位置	目标	路由类型
10.0.0.0/16	*Attachment ID for VPC A*	已传播
10.1.0.0/16	*Attachment ID for VPC B*	传播

开始使用 Amazon VPC 公交网关

以下任务可帮助您熟悉 Amazon Transit Gateways 中的中VPC转网关。此任务将引导您创建公交网关，然后VPCs使用该公交网关连接两个公交网关。

任务

先决条件

- 要演示使用公交网关的简单示例，请在同一个区域VPCs中创建两个。VPCs不能有重叠CIDRs。在每个EC2实例中启动一个 Amazon 实例VPC。有关更多信息，请参阅《亚马逊VPC用户指南》VPC 中的 “亚马逊入门”。
- 您不能让相同的路线指向两个不同的路由VPCs。如果公交网关路由表中CIDRs存在相同的路由，VPC则公交网关不会传播新连接的路由。
- 验证您拥有使用中转网关所需的权限。有关更多信息，请参阅 Amazon VPC 公交网关中的身份和访问管理 。
- 如果您没有向每个主机安全组添加ICMP规则，则无法在主机之间执行 ping 操作。有关更多信息，请参阅 Amazon VPC 用户指南中的使用安全组。

步骤 1：创建中转网关

当您创建中转网关时，我们创建一个默认的中转网关路由表，并将其用作默认的关联路由表和默认的传播路由表。

创建中转网关

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

2. 在区域选择器中，选择您在创建时使用的区域VPCs。
3. 在导航窗格中，选择 Transit Gateways（中转网关）。
4. 选择 Create Transit Gateway（创建中转网关）。
5. （可选）对于 Name tag (名称标签)，输入中转网关的名称。这会创建将“名称”作为键以及将您指定的名称作为值的标签。
6. （可选）对于 Description (描述)，输入中转网关的描述。
7. 在配置传输网关部分，执行以下操作：

   1. 对于 Amazon 端自治系统编号 (ASN)，请输入您的公交网关ASN的私有编号。这应该是ASN边界网关协议 (BGP) 会话 AWS 的一边。

      16 位的范围从 64512 到 65534 不等。ASNs

      32位的范围从42亿到4294967294不等。ASNs

      如果您采用多区域部署，我们建议您ASN为每个中转网关使用唯一的。
   2. （可选）选择是否启用以下任一选项：
      - DNS支持VPCs连接到此传输网关。
      - VPNECMP支持连接到传输网关的VPN连接。
      - 默认路由表关联，它会自动将公交网关附件与该公交网关的默认路由表相关联。
      - 默认路由表传播，它会自动将路由表附件传播到此公交网关的默认路由表。
      - 多播支持，允许您在此传输网关中创建多播域。
8. （可选）在 C onfigure-cross-account 共享选项部分，选择是否自动接受共享附件。如果启用，则会自动接受附件。否则，您必须接受或拒绝附件请求。
9. （可选）在 T ransit CIDR gateway 区块部分，为地址添加大小为 /24 或更大的CIDR区块，为IPv4地址添加 /64 或更大的CIDR区块。IPv6您可以关联任何公有或私有 IP 地址范围，169.254.0.0/16 范围内的地址以及与您的附件和本地网络的地址重叠的范围除外。VPC

   > **Note**
   >
   > 如果您正在配置 Connect (GRE) 附件或 PrivateIPVPNs，则使用传输网关CIDR块。Transit Gateway IPs 为该范围内的隧道终端节点 (GRE/PrivateIPVPN) 进行分配。

10. （可选）向此公交网关添加键值标签，以进一步帮助识别它。

    1. 选择 “添加新选项卡”。

2. 输入键名称和关联值。
3. 选择 Add new tag 以添加其他标签，或者跳到下一步。

11. 选择 Create Transit Gateway（创建中转网关）。创建网关时，中转网关的初始状态为 `pending`。

第 2 步：将您的VPCs连接到您的公交网关

等到您在上一部分中创建的中转网关显示为可用后，继续创建挂载。为每人创建一个附件VPC。

确认您已创建两个实例，VPCs并在每个EC2实例中启动了一个实例，如中所述先决条件 。

创建与的公交网关连接 VPC

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。
4. （可选）对于 Name tag（名称标签），输入挂载的名称。
5. 对于 Transit Gateway ID（中转网关 ID），选择要用于挂载的中转网关。
6. 对于 “附件类型”，选择VPC。
7. 选择是否启用DNS支持。在本练习中，请勿启用IPv6支持。
8. 对于 VPCID，请选择VPC要连接到传输网关的。
9. 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。
10. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。

每个连接都始终与正好一个路由表关联。路由表可以与零到多个连接关联。要确定要配置的路由，请决定中转网关的使用案例，然后配置路由。有关更多信息，请参阅 the section called “公交网关场景示例”。

步骤 3：在公交网关和您的公交网关之间添加路线 VPCs

路由表包括动态和静态路由，它们VPCs根据数据包的目的 IP 地址确定关联的下一跳。配置具有非本地路由目的地和中转网关挂载 ID 目标的路由。有关更多信息，请参阅 Amazon VPC 用户指南中的中转网关路由。

向路由表添加VPC路由

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Route Tables（路由表）。
3. 选择与您的关联的路由表VPC。
4. 选择 Routes（路由）选项卡，然后选择 Edit routes（编辑路由）。
5. 选择 Add route (添加路由)。
6. 在 Destination（目的地）列中，输入目的地 IP 地址范围。对于 Target（目标），选择 Transit Gateway（中转网关），然后选择中转网关 ID。
7. 选择 Save changes（保存更改）。

步骤 4：测试中转网关

您可以通过连接每个EC2VPC实例中的一个 Amazon 实例，然后在它们之间发送数据（例如 ping 命令）来确认传输网关已成功创建。有关更多信息，请参阅连接到您的 Linux 实例或连接到您的 Windows 实例。

步骤 5：删除中转网关

当您不再需要中转网关时，可以将其删除。

您不能删除具有资源挂载的中转网关。如果您尝试删除带有连接的中转网关，则系统会提示您先删除这些连接，然后才能删除中转网关。一旦中转网关被删除，您就停止对其产生费用。

删除中转网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。
3. 选择中转网关，然后依次选择 Actions（操作）、Delete transit gateway（删除中转网关）。
4. 输入 **`delete`**，然后选择删除。

   Transit gateways（中转网关）页面上中转网关的 State（状态）为 Deleting（正在删除）。删除后，将从页面中删除中转网关。

Amazon VPC 公交网关设计最佳实践

以下是您的中转网关设计的最佳实践：

- 为每个传输网关VPC连接使用单独的子网。例如，对于每个子网CIDR，请使用较小的子网/28，这样您就可以拥有更多的EC2资源地址。当您使用单独的子网时，您可以配置以下内容：
  - 保持与传输网关子网ACLs关联的入站和出站网络处于打开状态。
  - 根据您的流量，您可以将网络ACLs应用于工作负载子网。
- 创建一个网络ACL并将其与传输网关关联的所有子网关联。在入站和出站方向上都要保持网络ACL畅通。
- 将同一个VPC路由表与传输网关关联的所有子网相关联，除非您的网络设计需要多个VPC路由表（例如，通过多个NAT网关路由流量的中间框VPC）。
- 使用边界网关协议 (BGP) 点对点连接VPN。如果用于连接的客户网关设备或防火墙支持多路径，请启用该功能。
- 为 AWS Direct Connect 网关附件和BGP站点到站点VPN连接启用路由传播。
- 从对等互VPC连迁移到使用传输网关时。对VPC等互连和传输网关之间的MTU大小不匹配可能会导致某些数据包因非对称流量而丢失。VPCs同时更新两者，以避免由于大小不匹配而丢弃巨型数据包。
- 您不需要额外的中转网关即可实现高可用性，因为根据设计，中转网关具有高可用性。
- 限制中转网关路由表的数量，除非您的设计需要多个中转网关路由表。
- 为确保冗余，请在每个区域中使用单个中转网关进行灾难恢复。
- 对于具有多个中转网关的部署，我们建议您为每个中转网关使用唯一的自治系统编号 (ASN)。您还可以使用区域间对等功能。有关更多信息，请参阅使用 AWS Transit Gateway 区域间对等互连构建全球网络。

使用 Amazon 公交网关使用VPC公交网关

您可以使用 Amazon VPC 控制台或 AWS CLI。

主题

共享公交网关

您可以使用 Res AWS ource Access Manager (RAM) 在中跨账户或整个组织共享VPC附件的传输网关 AWS Organizations。RAM必须启用并与组织共享资源。有关更多信息，请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations共享资源。

注意事项

您可以使用 Res AWS ource Access Manager (RAM) 在中跨账户或整个组织共享VPC附件的传输网关 AWS Organizations。RAM必须启用并与组织共享资源。有关更多信息，请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations共享资源。

如果要共享中转网关，请考虑以下因素。

- 必须在拥有传输网关的同一个 AWS 账户中创建 AWS Site-to-Site VPN 附件。
- Direct Connect 网关的连接使用传输网关关联，可以与 Direct Connect 网关位于同一个 AWS 账户中，也可以与 Direct Connect 网关位于不同的账户中。

默认情况下，用户无权创建或修改 AWS RAM 资源。要允许用户创建或修改资源并执行任务，必须创建授予使用特定资源和API操作的权限的IAM策略。然后，您可以将这些策略附加到需要这些权限的IAM用户或群组。

仅资源拥有者能够执行以下操作：

- 创建资源共享。
- 更新资源共享。
- 查看资源共享。
- 查看您的账户在所有资源共享中共享的资源。
- 在所有资源共享中查看您与其共享资源的委托人。通过查看您与其共享资源的委托人，您可以确定谁有权访问您共享的资源。
- 删除资源共享。
- 运行所有公交网关、中转网关连接和中转网关路由表APIs。

您可以对与您共享的资源执行以下操作：

- 接受或拒绝资源共享邀请。
- 查看资源共享。
- 查看您可以访问的共享资源。
- 查看与您共享资源的所有委托人的列表。您可以查看他们与您共享的资源和资源共享。
- 可以运行 `DescribeTransitGatewaysAPI`.
- APIs运行创建和描述附件的`DescribeTransitGatewayVpcAttachments`，例如`CreateTransitGatewayVpcAttachment`和VPCs。
- 退出资源共享。

与您共享中转网关时，您无法创建、修改或删除其中转网关路由表或其中转网关路由表传播和关联。

在创建中转网关时，将在映射到您的账户并独立于其他账户的可用区中创建中转网关。如果中转网关和挂载实体位于不同的账户中，请使用可用区 ID 唯一且一致地标识可用区。例如，use1-az1 是 us-east-1 区域的可用区 ID，它映射到每个账户中的相同位置。 AWS

取消共享中转网关

当共享拥有者取消共享中转网关时，以下规则适用：

- Transit Gateway 挂载保持正常工作。
- 共享账户无法描述中转网关。
- 中转网关拥有者和共享拥有者可以删除 Transit Gateway 挂载。

当公交网关与另一个 AWS 账户取消共享时，或者如果与之共享公交网关的 AWS 账户已从组织中移除，则公交网关本身不会受到影响。

共享子网

VPC所有者可以将传输网关连接到共享子VPC网。参与者不能。根据所有者在共享VPC子网上设置的路由，来自参与VPC者资源的流量可以使用附件。

有关更多信息，请参阅 Amazon VPC 用户指南中的VPC与其他账户共享您的账户。

Amazon 公交网关中的VPC公交网关

传输网关允许您连接VPCs和VPN连接并在它们之间路由流量。公交网关跨平台运行 AWS 账户，您可以使用 AWS RAM 公交网关与其他账户共享您的公交网关。在您与其他人共享公交网关后 AWS 账户，账户所有者可以将其VPCs连接到您的公交网关。任一账户的用户都可以随时删除此挂载。

您可以在传输网关上启用多播，然后创建一个传输网关组播域，允许通过与该域关联的VPC附件将多播流量从您的多播源发送给组播组成员。

每个 o VPC r VPN 附件都与一个路由表相关联。该路由表决定来自该资源挂载的流量的下一个跃点。传输网关内部的路由表允许同时使用IPv4或IPv6CIDRs和目标。目标是VPCs和VPN连接。当您在公交网关上VPN连接VPC或创建连接时，该连接将与公交网关的默认路由表相关联。

您可以在公交网关内创建其他路由表，并更改VPC或与这些路由表的关VPN联。这使您可以对网络进行分段。例如，您可以将开发VPCs与一个路由表相关联，将生产VPCs与另一个路由表相关联。这使您能够在传输网关内创建隔离网络，类似于传统网络中的虚拟路由和转发 (VRFs)。

传输网关支持连接和VPN连接之间的动态VPCs和静态路由。您可以针对每个挂载启用或禁用路由传播。中转网关对等连接挂载仅支持静态路由。您可以将公交网关路由表中的路由指向对等连接附件，以便在对等传输网关之间路由流量。

您可以选择将一个IPv4或多个IPv6CIDR区块与您的公交网关相关联。当你为 Transit Gateway Connect 连接建立 Transit Gateway Connect 对等体时，你可以从CIDR区块中指定 IP 地址。您可以关联任何公有或私有 IP 地址范围，但该`169.254.0.0/16`范围中的地址以及与您的VPC附件和本地网络的地址重

叠的范围除外。有关IPv4和IPv6CIDR区块的更多信息，请参阅 Amazon VPC 用户指南中的VPCs和子网。

任务

- 使用 Amazon 公交网关创建VPC公交网关
- 使用 Amazon 公交网关查看VPC公交网关信息
- 使用 Amazon VPC 公交网关为公交网关添加或编辑标签
- 使用 Amazon 公交网关修改VPC公交网关
- 使用 Amazon VPC 公交网关接受资源共享
- 使用 Amazon 公VPC交网关接受共享附件
- 使用 Amazon 公交网关删除VPC公交网关

使用 Amazon 公交网关创建VPC公交网关

当您创建中转网关时，我们创建一个默认的中转网关路由表，并将其用作默认的关联路由表和默认的传播路由表。如果您选择不创建默认的中转网关路由表，则可以稍后创建一个。有关路由和路由表的更多信息，请参见 ???。

使用控制台创建中转网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。
3. 选择 Create Transit Gateway（创建中转网关）。
4. 对于 Name tag（名称标签），（可选）输入中转网关的名称。名称标签可让您更轻松地确定网关列表中的特定网关。当您添加 Name tag（名称标签）时，将使用 Name（名称）键和与您输入的值相等的值创建一个标签。
5. 对于 Description（描述），（可选）输入中转网关的描述。
6. 对于 Amazon 端自治系统编号 (ASN)，要么保留默认值以使用默认值，要ASN么输入公交网关ASN的私有值。这应该是ASN边界网关协议 (BGP) 会话 AWS 的一边。

   16 位的范围为 64512 到 65534。ASNs

   32位的区间为42亿至4294967294。ASNs

   如果您采用多区域部署，我们建议您ASN为每个中转网关使用唯一的。

7. 要获得DNS支持，如果您需要在从VPC连接VPC至传输网关的另一个实例中查询公用IPv4DNS主机名时将公用主机名解析为私有IPv4地址，请选择此选项。
8. 要获得VPNECMP支持，如果您需要VPN隧道间的等价多路径 (ECMP) 路由支持，请选择此选项。如果连接通告相同CIDRs，则流量将在它们之间平均分配。

   选择此选项时 BGPASN，广告的BGP属性以及诸如 AS-Path 之类的属性必须相同。

   > **Note**
   >
   > 要使用ECMP，必须创建使用动态路由的VPN连接。VPN不支持使用静态路由的连接ECMP。

9. 对于 Default route table association（默认路由表关联），选择此选项以自动将中转网关挂载与中转网关的默认路由表关联。
10. 对于 Default route table propagation（默认路由表传播），选择此选项以自动将中转网关挂载传播到中转网关的默认路由表。
11. （可选）要使用中转网关作为多播流量的路由器，请选择 Multicast support（多播支持）。
12. （可选）在 C onfigure-cross-account 共享选项部分，选择是否自动接受共享附件。如果启用，则会自动接受附件。否则，您必须接受或拒绝附件请求。

    对于 Auto accept shared attachments（自动接受共享的挂载），选择此选项以自动接受跨账户挂载。
13. （可选）对于 T ransit 网关CIDR区块，请为您的公交网关指定一个IPv4或多个IPv6CIDR区块。

    您可以为指定大小为 /24 或更大的CIDR方块（例如 /23 或 /22），也可以为IPv4指定大小 /64 或更大的CIDR方块（例如 /63 或 /62）。IPv6您可以关联任何公有或私有 IP 地址范围，169.254.0.0/16 范围内的地址以及与您的附件和本地网络的地址重叠的范围除外。VPC

    > **Note**
    >
    > 如果您正在配置 Connect (GRE) 附件或 PrivateIPVPNs，则使用传输网关CIDR块。Transit Gateway IPs 为该范围内的隧道终端节点 (GRE/PrivateIPVPN) 进行分配。

14. 选择 Create Transit Gateway(创建中转网关)。

要使用创建公交网关 AWS CLI

使用create-transit-gateway命令。

使用 Amazon 公交网关查看VPC公交网关信息

查看您的任何公交网关。

使用控制台查看公交网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格上，选择 T r ansit Gateways。该中转网关的详细信息显示在该页的网关列表下方。

要查看公交网关，请使用 AWS CLI

使用describe-transit-gateway命令。

使用 Amazon VPC 公交网关为公交网关添加或编辑标签

向资源添加标签以帮助整理和识别资源，例如，按用途、拥有者或环境。您可以向每个中转网关添加多个标签。每个中转网关的标签键必须是唯一的。如果您添加的标签中的键已经与中转网关关联，它将更新该标签的值。有关更多信息，请参阅标记您的 Amazon EC2 资源。

使用控制台向中转网关添加标签

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。
3. 选择要为其添加或编辑标签的公交网关。
4. 在页面的下面部分选择 Tags（标签）选项卡。
5. 选择 Manage tags（管理标签）。
6. 选择 Add new tag（添加新标签）。
7. 输入标签的键和值。
8. 选择Save（保存）。

使用 Amazon 公交网关修改VPC公交网关

您可以修改中转网关的配置选项。修改中转网关时，修改后的选项将仅应用于新的中转网关连接。不会修改您现有的中转网关连接，也不会出现任何服务中断的情况。

您无法修改他人与您共享的中转网关。

如果当前有任何 IP 地址用于 CIDR C onnect 对等体，则无法移除传输网关的屏蔽。

修改中转网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。
3. 选择要修改的中转网关。
4. 选择 Actions（操作）、Modify Transit Gateways（修改中转网关）。
5. 根据需要修改选项，然后选择 Modify Transit Gateway（修改中转网关）。

要修改您的中转网关，请使用 AWS CLI

使用modify-transit-gateway命令。

使用 Amazon VPC 公交网关接受资源共享

如果已将您添加到资源共享，您将收到加入资源共享的邀请。您必须接受资源共享，然后才能访问共享的资源。

接受资源共享

1. 打开 AWS RAM 控制台，网址为https://console.aws.amazon.com/ram/。
2. 在导航窗格中，依次选择 Shared with me（与我共享） 和 Resource shares（资源共享）。
3. 选择资源共享。
4. 选择 Accept resource share（接受资源共享）。
5. 要查看共享公交网关，请在 Amazon VPC 控制台中打开公交网关页面。

使用 Amazon 公VPC交网关接受共享附件

如果您在创建公交网关时未启用自动接受共享附件功能，则必须使用 Amazon VPC 控制台或 Amazon Console 手动接受跨账户（共享）附件。 AWS CLI

手动接受共享挂载

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。

3. 选择等待接受的中转网关连接。
4. 选择 Actions（操作）、Accept Transit Gateway attachment（接受中转网关挂载）。

要接受共享附件，请使用 AWS CLI

使用 accept-transit-gateway-vpc-attachment 命令。

使用 Amazon 公交网关删除VPC公交网关

您不能删除带有现有挂载的中转网关。您需要先删除所有挂载，然后才能删除中转网关。

使用控制台删除中转网关

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 选择要删除的中转网关。
3. 选择 Actions（操作）、Delete Transit Gateway（删除中转网关）。输入 **`delete`** 然后选择 Delete（删除） 以确认删除。

要使用删除公交网关 AWS CLI

使用delete-transit-gateway命令。

亚马逊VPC公交网关中的亚马逊VPC附件

将连接到传输网关时，必须从每个可用区指定一个子网，供中转网关用来路由流量。VPC从可用区中指定一个子网后，流量就可以到达该可用区的每个子网中的资源。

限制

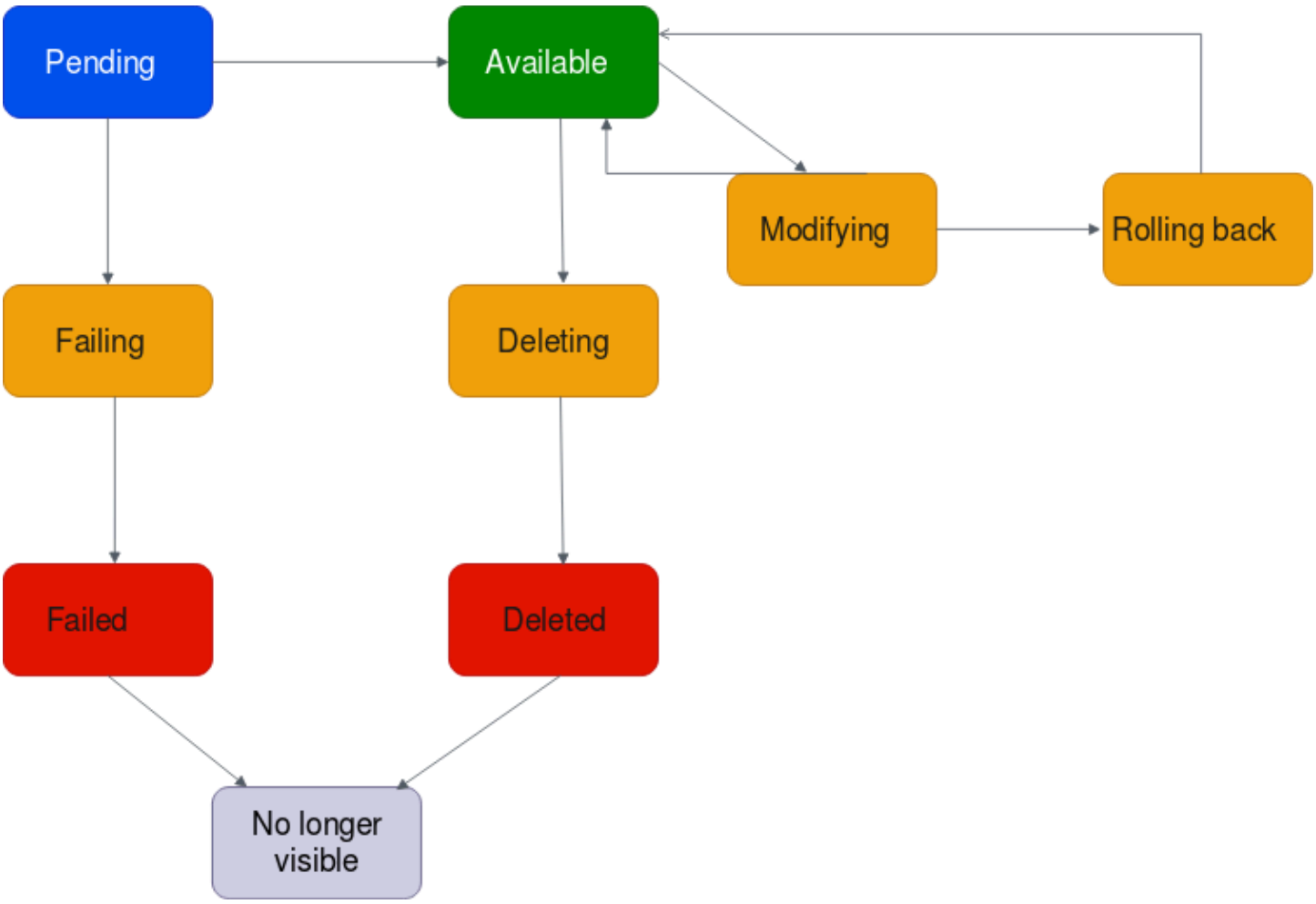
- 当您将连接到传输网关时，可用区中没有连接传输网关的任何资源都无法到达该传输网关。VPC如果子网路由表中有通往中转网关的路由，则只有当中转网关在同一可用区的子网中有挂载时，才会将流量转发到中转网关。
- VPC连接至公交网关的资源无法访问其他网关的安全组VPC，该安全组也连接到同一个传输网关。
- 公交网关不支持DNS解析使用 Amazon Route 53 中的私有托管区域VPCs设置的自定义连接DNS名称。要为所有VPCs连接到公交网关的私有托管区域配置名称解析，请参阅使用 Amazon Route 53 和 Tr AWS ansit Gateway 集中DNS管理混合云。

- 中转网关不支持相同网关之间的VPCs路由CIDRs。如果您将 a VPC 连接到公交网关，并且CIDR它与已连接到该公交网关CIDR的另一个VPC网关相同，则新连接的公交网关的路由VPC不会传播到公交网关路由表。
- 您无法为位于本地区域中的VPC子网创建附件。但可以将网络配置为允许本地区域中的子网通过父可用区连接到中转网关。有关更多信息，请参阅将 Local Zone 子网连接到中转网关。
- 您无法使用IPv6仅限子网创建传输网关附件。传输网关连接子网还必须支持IPv4地址。
- 在将公交网关添加到路由表之前，该中转网关必须至少有一个VPC附件。

VPC附件生命周期

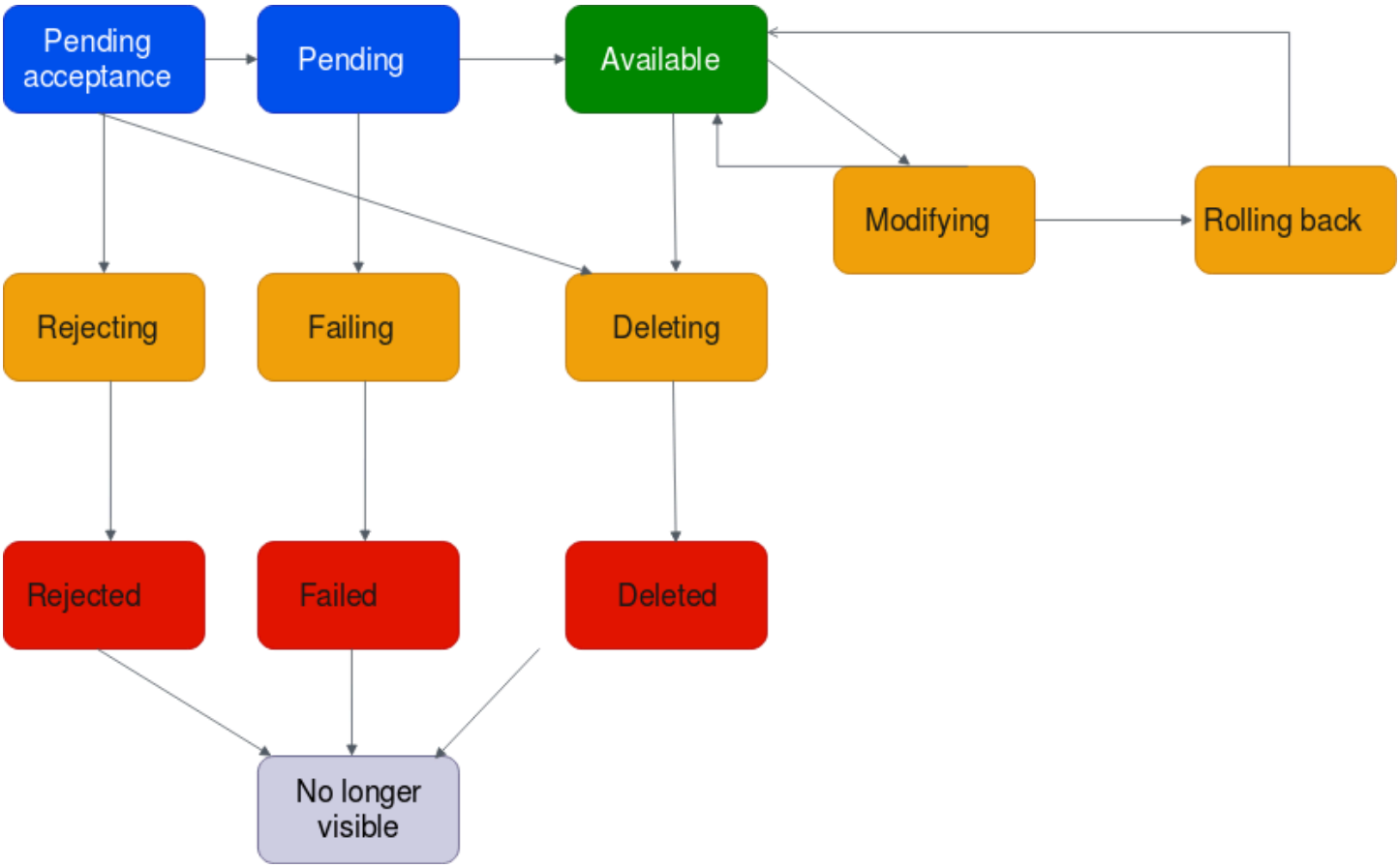
从请求启动时开始，VPC附件会经历不同的阶段。在每个阶段，您都可以采取一些操作，在附件的生命周期结束时，VPC附件会在一段时间内在 Amazon Virtual Private Cloud Console and in API 或命令行输出中保持可见。

下图显示了挂载在单个账户配置或打开了自动接受共享挂载选项的跨账户配置中会经历的状态。



- 待处理：已启动VPC附件请求并处于配置过程中。在此阶段，挂载可能会失败，也可能会变为 `available`。
- 失败：VPC附件请求失败。在这个阶段，VPC附件将转到`failed`。
- 失败：VPC附件请求失败。在此状态下，无法删除 VPC 挂载。失败的VPC附件会在 2 小时内保持可见状态，然后不再可见。
- 可用：VPC附件可用，流量可以在VPC和中转网关之间流动。在此阶段，挂载可以变为 `modifying`，也可以变为 `deleting`。
- 删除：正在删除的VPC附件。在此阶段，挂载可以变为 `deleted`。
- 已删除：`available`VPC附件已删除。处于这种状态时，无法修改VPC附件。该VPC附件会在 2 小时内保持可见，之后便不再可见。
- 正在修改：已请求修改VPC附件的属性。在此阶段，挂载可以变为 `available`，也可以变为 `rolling back`。
- 回滚：无法完成VPC附件修改请求，并且系统正在撤消所做的任何更改。在此阶段，挂载可以变为 `available`。

下图显示了挂载在自动接受共享挂载选项已关闭的跨账户配置中会经历的状态。



- 待接受：VPC附件请求正在等待接受。在此阶段，挂载可以变为 pending、rejecting 或 deleting。
- 拒绝：正在被拒绝的VPC附件。在此阶段，挂载可以变为 rejected。
- 已@@ 拒绝：pending acceptanceVPC附件已被拒绝。处于这种状态时，无法修改VPC附件。该VPC附件会在 2 小时内保持可见，之后便不再可见。
- 待处理：VPC附件已被接受，正在置备中。在此阶段，挂载可能会失败，也可能会变为 available。
- 失败：VPC附件请求失败。在这个阶段，VPC附件将转到failed。
- 失败：VPC附件请求失败。在此状态下，无法删除 VPC 挂载。失败的VPC附件会在 2 小时内保持可见状态，然后不再可见。
- 可用：VPC附件可用，流量可以在VPC和中转网关之间流动。在此阶段，挂载可以变为 modifying，也可以变为 deleting。
- 删除：正在删除的VPC附件。在此阶段，挂载可以变为 deleted。
- 已删除：available或pending acceptanceVPC附件已被删除。处于这种状态时，无法修改VPC附件。该VPC附件在 2 小时内保持可见状态，然后就不再可见了。
- 正在修改：已请求修改VPC附件的属性。在此阶段，挂载可以变为 available，也可以变为 rolling back。
- 回滚：无法完成VPC附件修改请求，并且系统正在撤消所做的任何更改。在此阶段，挂载可以变为 available。

任务

- 使用 Amazon VPC 公交网关创建VPC附件
- 使用 Amazon VPC 传输网关修改VPC附件
- 使用 Amazon VPC 公交网关修改VPC附件标签
- 使用 Amazon VPC 公交网关查看VPC附件
- 使用 Amazon VPC 传输网关删除VPC附件
- 对创建亚马逊VPC公交网关VPC附件进行故障排除

使用 Amazon VPC 公交网关创建VPC附件

使用控制台创建VPC附件

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

2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。
4. 对于 Name tag（名称标签），可选择是否输入中转网关挂载的名称。
5. 对于 Transit Gateway ID（中转网关 ID），选择要用于挂载的中转网关。您可以选择自己拥有的中转网关或与您共享的中转网关。
6. 对于“附件类型”，选择VPC。
7. 选择是否启用 Supp DNSort、S IPv6u pport 和设备模式支持。

   如果选择设备模式，则源和目标之间的流量将在该流的生命周期内对VPC连接使用相同的可用区。
8. 对于 VPCID，选择VPC要连接到传输网关的。

   它VPC必须至少有一个与之关联的子网。
9. 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。
10. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。

要使用创建VPC附件 AWS CLI

使用 create-transit-gateway-vpc-attachment 命令。

使用 Amazon VPC 传输网关修改VPC附件

使用控制台修改VPC附件

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择VPC附件，然后选择操作、修改公交网关附件。
4. 启用或禁用以下任一选项：

   - DNS支持
   - IPv6支持
   - 设备模式支持
5. 要在连接中添加或删除子网，请选择或清除要添加或删除的子网 ID 旁边的复选框。

> **Note**
>
> 当VPC附件处于修改状态时，添加或修改附件子网可能会影响数据流量。

6. 选择 Modify Transit Gateway attachment（修改中转网关挂载）。

要修改VPC附件，请使用 AWS CLI

使用 modify-transit-gateway-vpc-attachment 命令。

使用 Amazon VPC 公交网关修改VPC附件标签

使用控制台修改您的VPC附件标签

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择VPC附件，然后依次选择 “操作”、“管理标签”。
4. [添加标签]选择添加新标签，然后执行以下操作：
   - 对于 Key（键），输入键名称。
   - 对于 Value（值），输入键值。
5. [删除标签]在标签旁，选择 Remove（删除）。
6. 选择 Save (保存)。

   VPC只能使用控制台修改附件标签。

使用 Amazon VPC 公交网关查看VPC附件

使用控制台查看VPC附件

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 在资源类型列中，查找VPC。这些是附VPC件。
4. 选择挂载以查看其详细信息。

要使用查看您的VPC附件 AWS CLI

使用 describe-transit-gateway-vpc-attactions 命令。

使用 Amazon VPC 传输网关删除VPC附件

使用控制台删除VPC附件

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择VPC附件。
4. 选择 Actions（操作）、Delete Transit Gateway attachment（删除中转网关挂载）。
5. 当系统提示时，输入 **`delete`**，然后选择 Delete（删除）。

要使用删除VPC附件 AWS CLI

使用 delete-transit-gateway-vpc-attachment 命令。

对创建亚马逊VPC公交网关VPC附件进行故障排除

以下主题可以帮助您解决创建VPC附件时可能遇到的问题。

问题

VPC连接失败。

原因

原因可能是以下之一：

1. 创建VPC附件的用户没有创建服务相关角色的正确权限。
2. 由于IAM请求过多，例如您使用 AWS CloudFormation 创建权限和角色，因此存在限制问题。
3. 该账户具有服务相关角色，并且服务相关角色已被修改。
4. 中转网关未处于 `available` 状态。

解决方案

根据原因，可以尝试以下操作：

1. 验证用户是否具有创建服务相关角色的适当权限。有关更多信息，请参阅《IAM用户指南》中的服务相关角色权限。用户获得权限后，创建VPC附件。
2. 通过控制台手动创建VPC附件，或API。有关更多信息，请参阅 the section called “创建VPC附件”。
3. 验证服务相关角色是否具有适当权限。有关更多信息，请参阅 the section called “Transit Gateway”。
4. 验证中转网关是否处于 `available` 状态。有关更多信息，请参阅 the section called “查看公交网关”。

Ama VPC zon 公交网关VPN中的站点到站点附件

要将VPN连接连接到您的传输网关，则需要您指定客户网关。对VPN客户网关有特定的要求。有关客户网关设备要求的更多信息，包括网关配置文件示例，请参阅《AWS Site-to-Site VPN 用户指南》中的客户网关设备要求。

对于静态路由VPNs，您还需要将静态路由添加到公交网关路由表中。传输网关路由表中以VPN附件为目标的静态路由不会被 Site-to-Site 过滤，VPN因为在使用基于连接的路由时，这可能会允许意外的出站流量流动。BGP VPN有关向公交网关路由表添加静态路由的步骤，请参阅创建静态路由。

您可以使用 Amazon VPC 控制台或使用创建、查看或删除传输网关站点到站点VPN附件。 AWS CLI

任务

- VPN使用 Amazon Transit Gateways 创建VPC公交网关附件
- 使用 Amazon VPC 公交网关查看VPN附件
- 使用 Amazon VPC 传输网关删除VPN附件

VPN使用 Amazon Transit Gateways 创建VPC公交网关附件

使用控制台创建VPN附件

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。
4. 对于 Transit Gateway ID（中转网关 ID），选择要用于挂载的中转网关。您可以选择自己拥有的中转网关。
5. 对于 “附件类型”，选择VPN。

6. 对于客户网关，执行以下操作之一：
   - 要使用现有的客户网关，选择 Existing（现有），然后选择要使用的网关。

     如果您的客户网关位于启用NAT穿越功能 (NAT-TNAT) 的网络地址转换 () 设备之后，请使用设备的公有 IP 地址，并调整防火墙规则以解除对NAT端口 4500 的封锁UDP。
   - 要创建客户网关，请选择新建，然后在 IP 地址中键入静态公有 IP 地址和BGPASN。

     对于 Routing options（路由选项），选择是使用 Dynamic（动态）还是 Static（静态）。有关更多信息，请参阅《AWS Site-to-Site VPN 用户指南》中的站点到站点VPN路由选项。
7. 在隧道选项中，输入隧道的CIDR范围和预共享密钥。有关更多信息，请参阅站点到站点架构VPN。
8. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。

要使用创建VPN附件 AWS CLI

使用create-vpn-connection命令。

使用 Amazon VPC 公交网关查看VPN附件

使用控制台查看VPN附件

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 在资源类型列中，查找VPN。这些是附VPN件。
4. 选择挂载以查看其详细信息或添加标签。

要使用查看您的VPN附件 AWS CLI

使用describe-transit-gateway-attachments命令。

使用 Amazon VPC 传输网关删除VPN附件

使用控制台删除VPN附件

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择VPN附件。

4. 选择VPN连接的资源 ID 以导航到 “VPN连接” 页面。
5. 依次选择 Actions（操作）和 Delete（删除）。
6. 当系统提示进行确认时，选择 Delete（删除）。

要使用删除VPN附件 AWS CLI

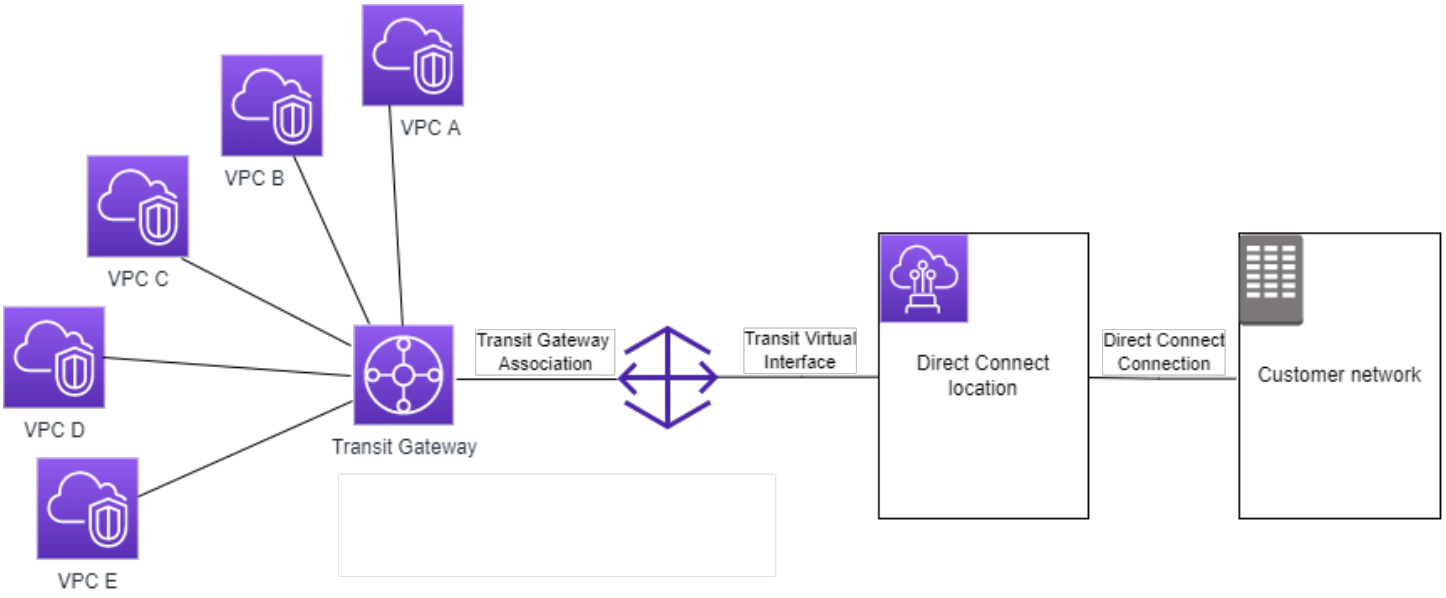
使用delete-vpn-connection命令。

连接到 Amazon 公交网关中的 Direct Connect 网关的VPC公交网关

使用中转虚拟接口将中转网关连接到 Direct Connect 网关。此配置提供以下好处。您可以：

- 管理多个VPCs或位于同一区域VPNs的单个连接。
- 将前缀从本地广告到本地 AWS 以及从本地广告到本地 AWS 。

下图说明了 Direct Connect 网关如何使您能够创建所有人VPCs都可以使用的指向 Direct Connect 连接的单个连接。



此解决方案包含以下组件：

- 中转网关。
- 一个 Direct Connect 网关。
- Direct Connect 网关与中转网关之间的关联。

- 连接到 Direct Connect 网关的中转虚拟接口。

有关使用中转网关配置 Direct Connect 网关的信息，请参阅 AWS Direct Connect 用户指南中的中转网关关联。

Amazon 公交网关中的公VPC交网关对等连接附件

您可以对域内和区域间中转网关进行对等，并在它们之间路由流量，包括IPv4和IPv6流量。为此，请在您的中转网关上创建对等挂载，然后指定中转网关。对等传输网关必须位于您的账户中。对等连接附件在可能与您共享的中转网关中不可用。

创建对等连接挂载请求后，对等中转网关（也称为接受方中转网关）的拥有者必须接受该请求。要在中转网关之间路由流量，请向中转网关路由表添加一个指向中转网关对等挂载的静态路由。

我们建议ASNs对每个对等公交网关使用 unique，以利用 future 的路径传播功能。

Transit Gateway 对等互连不支持使用其他区域中的将公用或私有IPv4DNS主机名解析为公用网关对等连接两VPCs侧 Amazon Route 53 Resolver 的私有IPv4地址。有关 Route 53 解析器的更多信息，请参阅《Amazon Route 53 开发人员指南》中的什么是 Route 53 解析器？。

区域间网关对等使用与对等互连相同的网络基础架构。VPC因此，当流量在区域之间传输时，将在虚拟网络层使用 AES -256 加密对其进行加密。当流量穿过物理控制之外的网络链路时，还会在物理层使用 AES -256 加密对其进行加密。 AWS因此，不受物理控制的网络链路上的流量会被双重加密 AWS。在同一区域内时，流量将仅在其经过超出 AWS物理控制范围的网络链路时进行物理层加密。

有关哪些区域支持公交网关对等连接的信息，请参阅AWS 公交网关FAQs。

选择加入 AWS 区域注意事项

您可以跨选择加入的区域边界对等连接中转网关。有关这些区域以及如何选择加入的信息，请参阅中的管理 AWS 区域Amazon Web Services 一般参考。在这些区域中使用中转网关对等连接时，请考虑以下事项：

- 只要接受对等连接挂载的账户已选择加入该区域，您就可以对等进入选择加入的区域。
- 无论区域选择加入状态如何，都将与接受对等互连附件的账户 AWS 共享以下账户数据：
  - AWS 账户 身份证
  - 中转网关 ID
  - 区域代码

- 删除中转网关挂载时，上述账户数据将被删除。
- 我们建议您在选择退出该区域之前删除中转网关对等连接挂载。如果不删除对等连接挂载，流量可能会继续通过挂载，并继续产生费用。如果您不删除挂载，则可以选择重新加入，然后删除挂载。
- 通常情况下，中转网关有发送人付款模式。通过跨选择加入边界使用中转网关对等连接挂载，您可能会在接受挂载的区域（包括您尚未选择加入的区域）中产生费用。有关更多信息，请参阅 AWS Transit Gateway 定价。

任务

- 使用 Amazon VPC 公交网关创建对等连接附件
- 使用 Amazon Tr VPC ansit Gateways 接受或拒绝对等连接请求
- 使用 Amazon Transit Gateways 向VPC公交网关路由表添加路由
- 使用 Amazon VPC 传输网关删除对等连接附件

使用 Amazon VPC 公交网关创建对等连接附件

在开始之前，请确保您获得了所要连接的中转网关的 ID。如果中转网关位于其他 AWS 账户网关中，请确保您拥有该传输网关所有者的 AWS 账户 ID。

创建对等挂载后，接受方中转网关的拥有者必须接受挂载请求。

使用控制台创建对等连接挂载

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。
4. 对于 Transit Gateway ID（中转网关 ID），选择要用于挂载的中转网关。您可以选择自己拥有的中转网关。与您共享的公交网关不可用于对等。
5. 对于 Attachment type (挂载类型)，选择 Peering Connection (对等连接)。
6. （可选）输入挂载的名称标签。
7. 对于 Account (账户)，执行以下操作之一：
   - 如果中转网关在您的账户中，请选择 My account (我的账户)。
   - 如果传输网关不同 AWS 账户，请选择其他账户。对于 Account ID (账户 ID)，输入 AWS 账户 ID。

8. 对于 Region (区域)，选择中转网关所在的区域。
9. 对于 Transit gateway ID (accepter) (中转网关 ID（接受方）)，输入您希望连接的中转网关的 ID。
10. 选择 Create Transit Gateway Attachment (创建中转网关挂载)。

要使用创建对等互连附件 AWS CLI

使用 create-transit-gateway-peering-attachment 命令。

使用 Amazon Tr VPC ansit Gateways 接受或拒绝对等连接请求

若要激活对等连接挂载，接受方中转网关的拥有者必须接受对等连接挂载请求。即使两个中转网关位于同一账户中，也必须执行此操作。对等连接挂载必须处于 pendingAcceptance 状态。接受来自接受方中转网关所在区域的对等连接挂载请求。

或者，您可以拒绝您收到的处于 pendingAcceptance 状态的任何对等连接请求。您必须拒绝来自接受方中转网关所在区域的请求。

使用控制台接受对等连接挂载请求

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments (中转网关挂载)。
3. 选择等待接受的中转网关对等挂载。
4. 选择 Actions (操作)、Accept transit gateway attachment (接受中转网关挂载)。
5. 将静态路由添加到中转网关路由表中。有关更多信息，请参阅 the section called “创建静态路由”。

使用控制台拒绝对等连接挂载请求

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments (中转网关挂载)。
3. 选择等待接受的中转网关对等挂载。
4. 选择 Actions (操作)、Reject transit gateway attachment (拒绝中转网关挂载)。

要接受或拒绝对等互连附件，请使用 AWS CLI

使用-attactach 和 accept-transit-gateway-peeringreject-transit-gateway-peering-at tachment 命令。

使用 Amazon Transit Gateways 向VPC公交网关路由表添加路由

要在对等中转网关之间路由流量，必须向中转网关路由表添加一个指向中转网关对等连接挂载的静态路由。接受方中转网关的拥有者还必须向其中转网关的路由表添加静态路由。

使用控制台创建静态路由

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要为其创建路由的路由表。
4. 选择 Actions（操作）、Create static route（创建静态路由）。
5. 在创建静态路由页面上，输入要为其创建路由的CIDR区块。例如，指定连接到对等传输网关的CIDR块。VPC
6. 选择路由的对等连接挂载。
7. 选择 Create static route (创建静态路由)。

要使用创建静态路由 AWS CLI

使用create-transit-gateway-route命令。

> **Important**
>
> 创建路由后，将中转网关路由表与中转网关对等挂载相关联。有关更多信息，请参阅 the section called “关联中转网关路由表”。

使用 Amazon VPC 传输网关删除对等连接附件

您可以删除中转网关对等挂载。任何一个中转网关的拥有者都可以删除挂载。

使用控制台删除对等连接挂载

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments (中转网关挂载)。
3. 选择中转网关对等挂载。
4. 选择 Actions (操作)、Delete transit gateway attachment (删除中转网关挂载)。

5. 输入 **delete**，然后选择 Delete (删除)。

要使用删除对等连接附件 AWS CLI

使用 delete-transit-gateway-peering-attachment 命令。

亚马逊公交网关中的 Transit Gateway Connect 附件和 Tr VPC ansit Gateway Connec

您可以创建 T ransit Gateway Connect 附件，以便在中转网关和中运行的第三方虚拟设备（例如 SD WAN 设备）之间建立连接VPC。Connect 附件支持通用路由封装 (GRE) 隧道协议以实现高性能，支持边界网关协议 (BGP) 以实现动态路由。创建 Connect 连接后，您可以在 Connect 连接上创建一条或多GRE条隧道（也称为 T ransit Gateway Connect 对等体），以连接传输网关和第三方设备。您通过GRE隧道建立两个BGP会话以交换路由信息。

> **Important**
>
> Transit Gat BGP eway Connect 对等体由两个在托管基础设施上终止的对 AWS等会话组成。两个对BGP等会话提供路由平面冗余，确保丢失一个对BGP等会话不会影响您的路由操作。从两个BGP会话中接收到的路由信息将累积给定的 Connect 对等体。这两个对BGP等会话还可以防止任何 AWS 基础设施操作，例如例行维护、修补、硬件升级和更换。如果您的 Connect 对等体在没有为冗余配置建议的双BGP对等会话的情况下运行，则在 AWS 基础设施运行期间，它可能会暂时失去连接。我们强烈建议您在 Connect 对等体上配置两个对等会话。BGP如果您已将多个 Connect 对等体配置为支持设备端的高可用性，我们建议您在每个 Connect 对BGP等体上配置两个对等会话。

Connect 附件使用现有VPC或 Direct Connect 附件作为底层传输机制。该挂载被称为运输挂载。传输网关将来自第三方设备的匹配GRE数据包识别为来自 Connect 附件的流量。它将任何其他数据包（包括源或目标信息不正确GRE的数据包）视为来自传输附件的流量。

> **Note**
>
> 要使用 Direct Connect 附件作为传输机制，你首先需要将 Direct Connect 与 T AWS ransit Gateway 集成。有关创建此集成的步骤，请参阅将 SD WAN 设备与 T AWS ransit Gateway 集成，以及 AWS Direct Connect。

Connect 对等节点

Connect 对等体（GRE隧道）由以下组件组成。

内部CIDR区块（BGP地址）

用于对等互BGP连的内部 IP 地址。您必须从的169.254.0.0/16范围中指定 /29 CIDR 区块。IPv4您可以选择从的fd00::/8范围中指定一个 /125 CIDR 块。IPv6以下CIDR区块是预留的，不能使用：

- 169.254.0.0/29
- 169.254.1.0/29
- 169.254.2.0/29
- 169.254.3.0/29
- 169.254.4.0/29
- 169.254.5.0/29
- 169.254.169.248/29

您必须将设备上该IPv4范围中的第一个地址配置为 BGP IP 地址。使用时IPv6，如果内部CIDR区块是 fd00:: /125，则必须在设备的隧道接口上配置此范围内的第一个地址 (fd00:: 1)。

在传输网关的所有隧道中，BGP地址必须是唯一的。

对等 IP 地址

Connect 对等体设备端的对等 IP 地址（GRE外部 IP 地址）。该地址可以是任何 IP 地址。IP 地址可以是IPv4或IPv6地址，但它的 IP 地址系列必须与传输网关地址相同。

Transit Gateway地址

Connect 对等体传输网关一侧的对等 IP 地址（GRE外部 IP 地址）。IP 地址必须从传输网关CIDR区块中指定，并且在传输网关上的 Connect 附件中必须是唯一的。如果您未指定 IP 地址，我们将使用传输网关CIDR区块中的第一个可用地址。

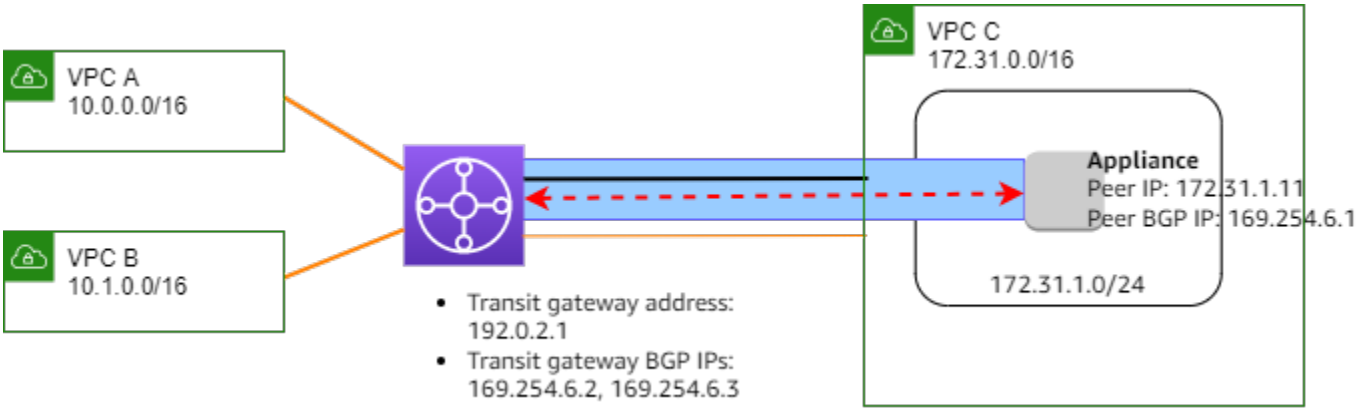
您可以在创建或修改公交网关时添加公交网关CIDR区块。

IP 地址可以是IPv4或IPv6地址，但它的 IP 地址系列必须与对等 IP 地址相同。

对等 IP 地址和传输网关地址用于唯一标识GRE隧道。您可以在多个隧道中重复使用任一地址，但不能在同一隧道中重复使用两个地址。

用于对BGP等互连的 Transit Gateway Connect 仅支持多协议 BGP (MP-BGP)，其中还需要IPv4单播寻址才能建立单播BGP会话。IPv6可以同时使用IPv4和IPv6地址作为GRE外部 IP 地址。

以下示例显示了中转网关和设备之间的 Connect 连接VPC。



图组件	描述
	VPC附件
	Connect 挂载
	GRE隧道（Connect 对等方）
	BGP对等会话

在前面的示例中，在现有附件（传输VPC附件）上创建了 Connect 附件。在 Connect 附件上创建一个 Connect 对等体，用于与中的设备建立连接VPC。中转网关地址为192.0.2.1，BGP地址范围为169.254.6.0/29。范围中的第一个 IP 地址 (169.254.6.1) 在设备上配置为对等 BGP IP 地址。

VPCC 的子网路由表中有一条路由，可将发往中转网关CIDR区块的流量指向中转网关。

目标位置	目标
172.31.0.0/16	本地
192.0.2.0/24	tgw-id

要求和注意事项

以下是 Connect 挂载的要求和注意事项。

- 有关哪些区域支持 Connect 附件的信息，请参阅公AWS 交网关FAQ。
- 必须将第三方设备配置为使用 Connect 附件通过GRE隧道发送和接收往返传输网关的流量。
- 必须将第三方设备配置为BGP用于动态路由更新和运行状况检查。
- 支持以下类型BGP的：
  - 外部 BGP (eBGP)：用于连接到与传输网关不同的自治系统中的路由器。如果使用 eBGP，则必须将 ebgp-multihop 配置为 time-to-live TTL 2。
  - 内部 BGP (iBGP)：用于连接到与传输网关处于同一自治系统的路由器。传输网关不会安装来自 i BGP peer（第三方设备）的路由，除非这些路由源自 e 对BGP等体，并且应该已经 next-hop-self 配置。第三方设备通过 i BGP peering 通告的路由必须有. ASN
  - MP-BGP（的多协议扩展BGP）：用于支持多种协议类型，例如IPv4和IPv6地址系列。
- 默认BGP保持连接超时为 10 秒，默认保持计时器为 30 秒。
- IPv6BGP不支持对等互连；仅支持IPv4基于BGP对等的对等。IPv6使用 MP-通过对IPv4BGP等交换前缀。BGP
- 不支持双向转发检测 (BFD)。
- BGP不支持优雅重启。
- 在创建中转网关对等体时，如果您未指定对等体ASN号码，我们会选择中转网关ASN号码。这意味着您的设备和公交网关将位于同一个自治系统中BGP。
- 当您有两个 Connect 对等体时，使用 AS-PATH 属性的Connect对等体是首选路由。BGP

  要在多个设备之间使用等价多路径 (ECMP) 路由，您必须将设备配置为使用相同 AS-属性的传输网关通告相同BGP的前缀。PATH要让公交网关选择所有可用ECMP路径，AS PATH 和自治系统编号 (ASN) 必须匹配。传输网关可以在 Connect 对等体ECMP之间用于相同的 Connect 连接，也可以在同一传输网关上的 Connect 附件之间使用。传输网关不能在单个对等体与之建立的两个冗余BGP对等体ECMP之间使用。
- 默认情况下，使用 Connect 挂载，路由会传播到Transit Gateway路由表。
- 不支持静态路由。
- 确保您的第三方设备外部接口（隧道源）最大传输单元 (MTU)
  - 与GRE隧道接口相匹配，或者 MTU
  - 应该大于GRE隧道接口的值。

任务

- 使用亚马逊VPC公交网关创建 Connect 附件
- 使用亚马逊VPC公交网关创建 Connect 对等体
- 使用亚马逊VPC公交网关查看 Connect 附件和 Connect 对等方
- 使用亚马逊VPC公交网关修改 Connect 附件和 Connect 对等标签
- 使用 Amazon VPC 公交网关删除 Connect 对等节点
- 使用亚马逊VPC公交网关删除 Connect 附件

使用亚马逊VPC公交网关创建 Connect 附件

要创建 Connect 挂载，您必须将现有挂载指定为传输挂载。您可以将VPC附件或 Direct Connect 附件指定为传输附件。

使用控制台创建 Connect 挂载

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择“中转网关挂载”。
3. 选择 Create Transit Gateway Attachment（创建中转网关挂载）。
4. （可选）对于 Name tag（名称标签），为挂载指定名称标签。
5. 对于Transit Gateway ID（中转网关 ID），选择要用于挂载的中转网关。
6. 对于 Attachment type（挂载类型），选择 Connect（连接）。
7. 对于 Transport Attachment ID（传输挂载 ID），选择现有挂载（传输挂载）的 ID。
8. 选择 Create Transit Gateway Attachment（创建中转网关连接）。

要使用创建 Connect 附件 AWS CLI

使用create-transit-gateway-connect命令。

使用亚马逊VPC公交网关创建 Connect 对等体

您可以为现有 Connect 附件创建 Connect 对等体（GRE隧道）。在开始之前，请确保已配置传输网关CIDR区块。您可以在创建或修改传输网关时配置公交网关CIDR区块。

创建 Connect 对等体时，必须在 Connect 对等体的设备端指定GRE外部 IP 地址。

要使用控制台创建 Connect 对等节点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择“中转网关挂载”。
3. 选择 Connect 挂载，然后选择 Actions（操作）、Create Connect peer（创建 Connect 对等节点）。
4. （可选）对于“名称标签”，为 Connect 对等节点指定名称标签。
5. （可选）在传输网关GRE地址中，指定传输网关的GRE外部 IP 地址。默认情况下，使用传输网关CIDR区块中的第一个可用地址。
6. 在 “对等GRE地址” 中，指定 Connect 对等体的设备端的GRE外部 IP 地址。
7. 对于 BGPInside CIDR 区块 IPv4，请指定用于对BGP等互连的内部IPv4地址范围。从该`169.254.0.0/16`范围中指定一个 /29 CIDR 方块。
8. （可选）对于BGP内部CIDR区块 IPv6，请指定用于对BGP等互连的内部IPv6地址范围。从该`fd00::/8`范围内指定一个 /125 CIDR 方块。
9. （可选）对于 Peer ASN，为设备指定边界网关协议 (BGPASN) 自治系统编号 ()。您可以使用ASN分配给您的网络的现有分配。如果你没有，你可以使用 64512—65534（16 位ASN）或4200000000—4294967294（32 位）范围ASN内的私有服务器。ASN

   默认值与中转网关ASN相同。如果将对等体配置ASN为与传输网关 ASN (eBGP) 不同，则必须将 ebgp-multihop 配置为 time-to-live (TTL) 值 2。
10. 选择 Create Connect peer（创建 Connect 对等节点）

要使用创建 Connect 对等体 AWS CLI

使用 create-transit-gateway-connect-peer 命令。

使用亚马逊VPC公交网关查看 Connect 附件和 Connect 对等方

查看您的 Connect 附件和 Connect 对等方。

要使用控制台查看 Connect 挂载和 Connect 对等节点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择“中转网关挂载”。
3. 选择 Connect 挂载。
4. 要查看 Connect 挂载对等节点，请选择 Connect Peers（Connect 对等节点）选项卡。

要查看您的 Connect 附件和 Connect 对等方，请使用 AWS CLI

使用describe-transit-gateway-connects和 describe-transit-gateway-connect-peers 命令。

使用亚马逊VPC公交网关修改 Connect 附件和 Connect 对等标签

您可以修改 Connect 挂载的标签。

要使用控制台修改 Connect 挂载标签

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Connect 挂载，然后选择 Actions（操作）、Manage tags（管理标签）。
4. 要添加标签，请选择 Add new tag（添加新标签）并指定键名称和键值。
5. 要删除标签，请选择移除。
6. 选择保存。

您可以修改 Connect 对等节点的标签。

要使用控制台修改 Connect 对等节点标签

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 选择 Connect 挂载，然后选择 Connect peers（Connect 对等节点）。
4. 选择 Connect 对等节点，然后选择“操作”、“管理标签”。
5. 要添加标签，请选择 Add new tag（添加新标签）并指定键名称和键值。
6. 要删除标签，请选择移除。
7. 选择保存。

要使用 AWS CLI修改 Connect 挂载和 Connect 对等节点标签

使用 create-tags 和 delete-tags 命令

使用 Amazon VPC 公交网关删除 Connect 对等节点

如果您不再需要某个 Connect 对等节点，可以将其删除。

要使用控制台删除 Connect 对等节点

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择“中转网关挂载”。
3. 选择 Connect 挂载。
4. 在“Connect 对等节点”选项卡中，选择 Connect 对等节点，然后选择“操作”、“删除 Connect 对等节点”。

要使用删除 Connect 对等体 AWS CLI

使用 delete-transit-gateway-connect-peer 命令。

使用亚马逊VPC公交网关删除 Connect 附件

如果您不再需要某个 Connect 挂载，则可以将其删除。您必须首先删除挂载的所有 Connect 对等节点。

要使用控制台删除 Connect 挂载

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择“中转网关挂载”。
3. 选择 Connect 挂载，然后选择 Actions（操作）、Delete Transit Gateway attachment（删除 Transit Gateway挂载）。
4. 输入 **`delete`**，然后选择 Delete（删除）。

要使用删除 Connect 附件 AWS CLI

使用delete-transit-gateway-connect命令。

Amazon 公交网关中的VPC公交网关路由表

使用中转网关路由表为中转网关挂载配置路由。

前缀列表引用

您可以在中转网关路由表中引用前缀列表。前缀列表是由您定义和管理的一个或多个CIDR区块条目组成的集合。您可以使用前缀列表来简化对资源中引用的 IP 地址的管理，以路由网络流量。例如，如果您经常在CIDRs多个公交网关路由表中指定相同的目的地，则可以在单个前缀列表CIDRs中管理这些目

的地，而不必在每个路由表CIDRs中重复引用相同的目的地。如果需要移除目标CIDR块，可以将其条目从前缀列表中删除，而不必从每个受影响的路由表中移除该路由。

在中转网关路由表中创建前缀列表引用时，前缀列表中的每个条目都将在中转网关路由表中表示为一个路由。

有关前缀列表的更多信息，请参阅 Amazon VPC 用户指南中的前缀列表。

任务

- 使用 Amazon 公交网关创建VPC公交网关路由表
- 使用 Amazon 公交网关查看VPC公交网关路由表
- 使用 Amazon 公交网关关联VPC公交网关路由表
- 使用 Amazon Transit Gateways 删除VPC公交网关路由表的关联
- 使用 Amazon Transit Gateways 启用传输到VPC公交网关路由表的路由
- 使用 Amazon VPC 公交网关禁用路由传播
- 使用 Amazon VPC 公交网关创建静态路由
- 使用 Amazon VPC 公交网关删除静态路由
- 使用 Amazon VPC 公交网关替换静态路由
- 使用亚马逊公VPC交网关将路由表导出到 Amazon S3
- 使用 Amazon 公交网关删除VPC公交网关路由表
- 使用 Amazon Tr VPC ansit Gateways 创建路由表前缀列表参考
- 使用 Amazon VPC 公交网关查看前缀列表参考
- 使用 Amazon VPC 公交网关修改前缀列表引用
- 使用 Amazon VPC 传输网关删除前缀列表引用

使用 Amazon 公交网关创建VPC公交网关路由表

使用控制台创建中转网关路由表

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择 Create Transit Gateway Route Table（创建中转网关路由表）。
4. （可选）对于 Name tag（名称标签），键入中转网关路由表的名称。这会创建标签键为“名称”的标签，其中，标签值是您指定的名称。

5. 对于 Transit Gateway ID（中转网关 ID），选择路由表的中转网关。
6. 选择 Create Transit Gateway Route Table（创建中转网关路由表）。

使用创建公交网关路由表 AWS CLI

使用 create-transit-gateway-route-table 命令。

使用 Amazon 公交网关查看VPC公交网关路由表

使用控制台查看中转网关路由表

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. （可选）要查找特定的路由表或一组路由表，请在筛选条件字段中输入全部或部分名称、关键词或属性。
4. 选中某个路由表对应的复选框或选择其 ID，以显示有关其关联、传播、路由和标签的信息。

要查看您的公交网关路由表，请使用 AWS CLI

使用 describe-transit-gateway-route-tables 命令。

要查看公交网关路由表的路由，请使用 AWS CLI

使用search-transit-gateway-routes命令。

要查看公交网关路由表的路径传播，请使用 AWS CLI

使用 get-transit-gateway-route-table-propagations 命令。

要查看公交网关路由表的关联，请使用 AWS CLI

使用 get-transit-gateway-route-table-associations 命令。

使用 Amazon 公交网关关联VPC公交网关路由表

您可以将中转网关路由表与 中转网关 挂载相关联。

使用控制台关联中转网关路由表

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

2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择路由表。
4. 在页面的下面部分，选择 Associations（关联）选项卡。
5. 选择 Create association（创建关联）。
6. 选择要关联的挂载，然后选择 Create association（创建关联）。

使用关联公交网关路由表 AWS CLI

使用 associate-transit-gateway-route-table 命令。

使用 Amazon Transit Gateways 删除VPC公交网关路由表的关联

您可以取消中转网关路由表与 中转网关 挂载的关联。

使用控制台取消中转网关路由表关联

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择路由表。
4. 在页面的下面部分，选择 Associations（关联）选项卡。
5. 选择要解除关联的挂载，然后选择 Delete association（删除关联）。
6. 当系统提示您确认时，选择 Delete association（删除关联）。

使用取消与公交网关路由表的关联 AWS CLI

使用 disassociate-transit-gateway-route-table 命令。

使用 Amazon Transit Gateways 启用传输到VPC公交网关路由表的路由

使用路由传播将挂载中的路由添加到路由表。

将路由传播到中转网关挂载路由表

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要为其创建传播的路由表。
4. 依次选择 Actions（操作）和 Create propagation（创建传播）。

5. 在 Create propagation（创建传播）页面上，选择挂载。
6. 选择 Create propagation（创建传播）。

要启用路由传播，请使用 AWS CLI

使用 enable-transit-gateway-route-table-propagation 命令。

使用 Amazon VPC 公交网关禁用路由传播

从路由表挂载删除传播的路由。

使用控制台禁用路由传播

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要从中删除传播的路由表。
4. 在页面的下面部分，选择 Propagations（传播）选项卡。
5. 选择挂载，然后选择 Delete propagation（删除传播）。
6. 当系统提示您确认时，选择 Delete propagation（删除传播）。

要禁用路由传播，请使用 AWS CLI

使用 disable-transit-gateway-route-table-propagation 命令。

使用 Amazon VPC 公交网关创建静态路由

为VPCVPN、或公交网关对等连接创建静态路由，也可以创建黑洞路由，丢弃与该路由匹配的流量。

传输网关路由表中以VPN附件为目标的静态路由不会被 “站点到站点VPN” 过滤。使用BGP基于 VPN based 时，这可能会允许意外的出站流量。

使用控制台创建静态路由

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要为其创建路由的路由表。
4. 选择 Actions（操作）、Create static route（创建静态路由）。
5. 在 “创建静态路由” 页面上，输入要为其创建路由的CIDR区块，然后选择 A ctive。

6. 为路由选择挂载。
7. 选择 Create static route（创建静态路由）。

使用控制台创建黑洞路由

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要为其创建路由的路由表。
4. 选择 Actions（操作）、Create static route（创建静态路由）。
5. 在创建静态路由页面上，输入要为其创建路由的CIDR区块，然后选择 Blackhol e。
6. 选择 Create static route（创建静态路由）。

要使用创建静态路由或黑洞路由 AWS CLI

使用create-transit-gateway-route命令。

使用 Amazon VPC 公交网关删除静态路由

从中转网关路由表中删除静态路由。

使用控制台删除静态路由

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择要删除其路由的路由表，然后选择 Routes（路由）。
4. 选择要删除的路由。
5. 选择 Delete static route（删除静态路由）。
6. 在确认框中，选择 Delete static route（删除静态路由）。

要使用删除静态路由 AWS CLI

使用delete-transit-gateway-route命令。

使用 Amazon VPC 公交网关替换静态路由

将公交网关路由表中的静态路由替换为其他静态路由。

使用控制台替换静态路由

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 在路由表中选择要替换的路由。
4. 在详细信息部分中，选择路径选项卡。
5. 选择操作、替换静态路由。
6. 对于类型，选择活动或黑洞。
7. 从选择附件下拉列表中，选择将取代路由表中当前连接的中转网关。
8. 选择替换静态路由。

要使用替换静态路由 AWS CLI

使用replace-transit-gateway-route命令。

使用亚马逊公VPC交网关将路由表导出到 Amazon S3

您可以将中转网关路由表中的路由导出到 Amazon S3 存储桶。这些路由将以JSON文件形式保存到指定的 Amazon S3 存储桶中。

使用控制台导出中转网关路由表

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择包含要导出的路由的路由表。
4. 依次选择 Actions（操作）和 Export routes（导出路由）。
5. 在 Export routes（导出路由）页上，对于 S3 bucket name（S3 存储桶名称），键入 S3 存储桶的名称。
6. 要筛选导出的路由，请在页面的 Filters（筛选条件）部分指定筛选参数。
7. 选择 Export routes（导出路由）。

要访问导出的路由，请在上打开 Amazon S3 控制台 https://console.aws.amazon.com/s3/，然后导航到您指定的存储桶。文件名包括 AWS 账户 ID、 AWS 区域、路由表 ID 和时间戳。选择文件并选择 Download（下载）。以下是一个JSON文件示例，其中包含有关两个传播的VPC附件路由的信息。

```
{
```

```
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

使用 Amazon 公交网关删除VPC公交网关路由表

使用控制台删除中转网关路由表

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。

3. 选择要删除的路由表。
4. 选择 Actions（操作）、Delete 中转网关 route table（删除中转网关路由表）。
5. 输入 **`delete`** 然后选择 Delete（删除） 以确认删除。

使用删除公交网关路由表 AWS CLI

使用 delete-transit-gateway-route-table 命令。

使用 Amazon Tr VPC ansit Gateways 创建路由表前缀列表参考

您可以在中转网关路由表中创建对前缀列表的引用。

使用控制台创建前缀列表引用

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择中转网关路由表。
4. 依次选择操作、创建前缀列表引用。
5. 对于前缀列表 ID，选择前缀列表的 ID。
6. 对于 Type（类型），选择是否应允许（Active（激活））或丢弃（Blackhole（黑洞））此前缀列表的流量。
7. 对于 Transit Gateway attachment ID（ Transit Gateway 挂载 ID），选择要将流量路由到的挂载的 ID。
8. 选择创建前缀列表引用。

要使用创建前缀列表引用 AWS CLI

使用 create-transit-gateway-prefix-list-referenc e 命令。

使用 Amazon VPC 公交网关查看前缀列表参考

查看公交网关路由表中的前缀列表引用。您也可以将前缀列表中的每个条目视为中转网关路由表中的单个路由。前缀列表路由的路由类型为 `propagated`。

使用控制台查看前缀列表引用

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

2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择中转网关路由表。
4. 在下方窗格中，选择前缀列表引用。此时页面上会列出前缀列表引用。
5. 选择路由。前缀列表中的每个条目都会作为路由表中的一个路由列出。

要查看前缀列表引用，请使用 AWS CLI

使用 get-transit-gateway-prefix-list-references 命令。

使用 Amazon VPC 公交网关修改前缀列表引用

您可以通过以下两种方式修改前缀列表引用：更改将流量路由到的挂载，或指示是否丢弃与路由匹配的流量。

无法在路由选项卡中修改前缀列表中的单个路由。要修改前缀列表中的条目，请使用托管前缀列表页面。有关更多信息，请参阅 Amazon VPC 用户指南中的修改前缀列表。

使用控制台修改前缀列表引用

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择中转网关路由表。
4. 在下方窗格中，选择前缀列表引用。
5. 选择前缀列表引用，然后选择 Modify references（修改引用）。
6. 对于 Type（类型），选择是否应允许（Active（激活））或丢弃（Blackhole（黑洞））此前缀列表的流量。
7. 对于 Transit Gateway attachment ID（ Transit Gateway 挂载 ID），选择要将流量路由到的挂载的 ID。
8. 选择修改前缀列表引用。

要修改前缀列表引用，请使用 AWS CLI

使用 modify-transit-gateway-prefix-list-referenc e 命令。

使用 Amazon VPC 传输网关删除前缀列表引用

如果您不再需要前缀列表引用，可以将其从中转网关路由表中删除。删除引用不会删除前缀列表。

使用控制台删除前缀列表引用

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway Route Tables（中转网关路由表）。
3. 选择中转网关路由表。
4. 选择前缀列表引用，然后选择 Delete references（删除引用）。
5. 选择 Delete references（删除引用）。

要修改前缀列表引用，请使用 AWS CLI

使用 delete-transit-gateway-prefix-list-referenc e 命令。

Amazon 公交网关中的VPC公交网关策略表

Transit Gateway 动态路由使用策略表为 AWS Cloud 路由网络流量WAN。该表包含用于按策略属性匹配网络流量的策略规则，然后将与规则匹配的流量映射到目标路由表。

您可以使用中转网关的动态路由，自动与对等中转网关类型交换路由和可达性信息。与静态路由不同，流量可以根据网络条件（如路径故障或拥塞）沿不同的路径路由。动态路由还增加了额外的安全层，在出现网络漏洞或入侵时，可以更轻松地重新路由流量。

> **Note**
>
> 目前，只有在创建公交网关对等连接WAN时，Cloud 才支持公交网关策略表。创建对等连接时，可以将该表与连接相关联。然后，该关联会自动使用策略规则填充表。
> 有关云端对等连接的更多信息WAN，请参阅《云用户指南》AWS 中的 Peerings。WAN

任务

- 使用 Amazon 公交网关创建VPC公交网关策略表
- 使用 Amazon 公交网关删除VPC公交网关策略表

使用 Amazon 公交网关创建VPC公交网关策略表

使用控制台创建中转网关策略表

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

2. 在导航窗格中，选择 Transit Gateway policy table（中转网关策略表）。
3. 选择 Create Transit Gateway policy table（创建中转网关策略表）。
4. （可选）对于 Name tag（名称标签），输入中转网关策略表的名称。这将创建一个标签，标签的值是您指定的名称。
5. 对于中转网关 ID，为策略表选择中转网关。
6. 选择 Create Transit Gateway policy table（创建中转网关策略表）。

使用创建传输网关策略表 AWS CLI

使用 create-transit-gateway-policy-table 命令。

使用 Amazon 公交网关删除VPC公交网关策略表

删除中转网关策略表。删除表后，该表中的所有策略规则都将被删除。

使用控制台删除中转网关策略表

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit Gateway policy tables（中转网关策略表）。
3. 选择要删除的中转网关策略表。
4. 选择 Actions（操作），然后选择 Delete policy table（删除策略表）。
5. 确认您要删除策略表。

使用删除传输网关策略表 AWS CLI

使用 delete-transit-gateway-policy-table 命令。

Amazon VPC 公交网关中的多播

多播是一种通信协议，用于同时向多台接收计算机传输单个数据流。Transit Gateway 支持在所连接的子网之间路由多播流量VPCs，它可以用作发送到多个接收实例的流量的实例的多播路由器。

主题

- 多播概念
- 注意事项

- 多播路由
- Amazon VPC 公交网关中的多播域
- Amazon 公VPC交网关中的共享多播域
- 使用 Amazon Tr VPC ansit Gateways 向组播组注册源
- 使用 Amazon Tr VPC ansit Gateways 向组播群组注册成员
- 使用 Ama VPC zon Transit Gateways 从多播组取消注册源
- 使用 Ama VPC zon Transit Gateways 从多播群组中注销成员
- 使用 Amazon VPC 公交网关查看多播组
- 在亚马逊VPC公交网关中为 Windows 服务器设置多播
- 示例：使用 Amazon VPC 公交网关管理IGMP配置
- 示例：使用 Amazon VPC 公交网关管理静态源配置
- 示例：在 Amazon VPC 公交网关中管理静态群组成员配置

多播概念

以下是多播的主要概念：

- 多播域 — 允许将一个多播网络分段成不同的域，并将中转网关用作多播路由器。您可以在子网级别定义多播域成员资格。
- 多播组 — 识别一组将发送和接收相同多播流量的主机。多播组由组 IP 地址标识。多播组成员资格由连接到EC2实例的各个弹性网络接口定义。
- Internet 组管理协议 (IGMP)-一种允许主机和路由器动态管理组播组成员资格的互联网协议。IGMP多播域包含使用该IGMP协议加入、离开和发送消息的主机。 AWS 支持IGMPv2协议IGMP和两者兼而有之，也支持静态（API基于）的组成员资格组播域。

- 多播源 — 与静态配置为发送多播流量的受支持EC2实例关联的 elastic network 接口。多播源仅适用于静态源配置。

  静态源组播域包含不使用该IGMP协议加入、离开和发送消息的主机。您可以使用 AWS CLI 来添加来源和组成员。静态添加的源发送多播流量，成员接收多播流量。
- 多播组成员 — 与接收多播流量的受支持EC2实例关联的 elastic network 接口。多播组具有多个组成员。在静态源组成员资格配置中，多播组成员只能接收流量。在IGMP群组配置中，成员可以发送和接收流量。

注意事项

- 有关支持的区域的信息，请参阅 T AWS ransit Gateway FAQs。
- 您必须创建一个新的中转网关才能支持多播。
- 使用或 AWS CLI、 Amazon Virtual Private Cloud Console 或管理多播组成员资格。IGMP
- 一个子网只能位于一个多播域中。
- 如果您使用非 Nitro 实例，则必须禁用 S ou rce/Dest 复选框。有关禁用检查的信息，请参阅《Amazon EC2 用户指南》中的更改源检查或目标检查。
- 非 Nitro 实例不能是多播发送方。
- 不支持通过 “站点到站点” AWS Direct Connect、“对等连接” 附件或传输网关 C VPN onnect 附件进行多播路由。
- 中转网关不支持多播数据包分段。分段多播数据包会被丢弃。有关更多信息，请参阅 最大传输单位 (MTU)。
- 启动时，IGMP主机发送多IGMPJOIN条消息以加入多播组（通常重试 2 到 3 次）。万一所有IGMPJOIN消息都丢失，主机将不会成为传输网关组播组的一部分。在这种情况下，您需要使用应用程序特定的方法重新触发来自主机的IGMPJOIN消息。
- 群组成员资格从传输网关收到IGMPv2JOIN消息开始，到收到IGMPv2LEAVE消息时结束。中转网关会跟踪成功加入多播组的主机。作为云多播路由器，传输网关每两分钟向所有成员IGMPv2QUERY发出一条消息。每个成员都会发送一条IGMPv2JOIN消息作为回应，这是成员续订会员资格的方式。如果成员未能回复连续三次查询，则中转网关将从其加入的所有组中删除此成员资格。但是，它会继续向该成员发送查询 12 个小时，然后将其从 to-be-queried 列表中永久删除。一条明确的IGMPv2LEAVE消息会立即永久地将主机从任何进一步的多播处理中移除。
- 中转网关会跟踪成功加入多播组的主机。如果中转网关出现故障，传输网关将在最后一条成功IGMPJOIN发送消息后的七分钟（420 秒）内继续向主机发送多播数据。Transit Gateway 会继续向主机发送成员资格查询长达 12 小时，或者直到它收到来自主机的IGMPLEAVE消息。
- 传输网关向所有成员发送IGMP成员资格查询数据包，以便它可以跟踪组播组成员资格。这些IGMP查询数据包的源 IP 是 0.0.0.0/32，目标 IP 是 224.0.0.1/32，协议是 2。您在IGMP主机（实例）上的安全组配置以及主机子网上的任何ACLs配置都必须允许这些IGMP协议消息。
- 当组播源和目标位于相同时VPC，您不能使用安全组引用将目标安全组设置为接受来自源安全组的流量。
- 对于静态组播组和源，Amazon T VPC ransit Gateways 会自动删除已不ENIs存在的静态组和源。这是通过定期担任 Tr ansit Gateway 服务相关角色在账户ENIs中描述来执行的。
- 仅支持IPv6静态多播。动态组播不是。

多播路由

在中转网关上启用多播时，它将充当多播路由器。当您将子网添加到某个多播域时，我们会将所有多播流量发送到与该多播域关联的中转网关。

网络 ACLs

网络ACL规则在子网级别运行。它们将应用于多播流量，因为中转网关位于子网外。有关更多信息，请参阅 Amazon VPC 用户指南ACLs中的网络。

对于 Internet 组管理协议 (IGMP) 多播流量，以下是最低入站规则。远程主机是发送多播流量的主机。

类型	协议	源	描述
自定义协议	IGMP(2)	0.0.0.0/32	IGMP查询
自定义UDP协议	UDP	远程主机 IP 地址	入站多播流量

以下是的最低出站规则IGMP。

类型	协议	目的地	描述
自定义协议	IGMP(2)	224.0.0.2/32	IGMP离开
自定义协议	IGMP(2)	多播组 IP 地址	IGMP加入
自定义UDP协议	UDP	多播组 IP 地址	出站多播流量

安全组

安全组规则在实例级别操作。它们可以应用于入站和出站多播流量。行为与单播流量相同。对于所有组成员实例，您必须允许来自组源的入站流量。有关更多信息，请参阅 Amazon VPC 用户指南中的安全组。

对于IGMP多播流量，您必须至少遵守以下入站规则。远程主机是发送多播流量的主机。您不能将安全组指定为UDP入站规则的来源。

类型	协议	源	描述
自定义协议	2	0.0.0.0/32	IGMP查询
自定义UDP协议	UDP	远程主机 IP 地址	入站多播流量

对于IGMP多播流量，您必须至少遵守以下出站规则。

类型	协议	目的地	描述
自定义协议	2	224.0.0.2/32	IGMP离开
自定义协议	2	多播组 IP 地址	IGMP加入
自定义UDP协议	UDP	多播组 IP 地址	出站多播流量

Amazon VPC 公交网关中的多播域

组播域允许将组播网络分割到不同的域中。要开始将多播与中转网关结合使用，请创建多播域，然后将子网与域关联。

多播域属性

下表详细介绍了多播域属性。您不能同时启用这两个属性。

属性	描述
`Igmpv2Support` (AWS CLI) IGMPv2支持（控制台）	此属性决定组成员如何加入或退出多播组。 当此属性处于禁用状态时，您必须将组成员手动添加到域中。 如果至少有一个成员使用该IGMP协议，则启用此属性。成员通过以下方式之一加入多播组： • 支持的成员IGMP使用`JOIN`和`LEAVE`消息。 • IGMP必须使用 Amazon VPC 控制台或，将不支持的成员添加到群组中或从群组中移除 AWS CLI。

属性	描述
	如果您注册多播组成员，则必须将其取消注册。传输网关会忽略手动添加的群组成员发送的IGMPLEAVE消息。
`StaticSourcesSupport` (AWS CLI) Static sources support（静态资源支持）（控制台）	此属性确定该组是否有静态多播源。 启用此属性后，必须使用 register-transit-gateway-multicast-group- sources 为多播域添加源。只有多播源才能发送多播流量。 禁用此属性时，则没有指定的多播源。位于与多播域关联的子网中的任何实例都可以发送多播流量，组成员将接收多播流量。

使用 Amazon VPC Transit Gateway 创建IGMP多播域

如果您尚未执行此操作，请查看可用的多播域属性。有关更多信息，请参阅 the section called “多播域”。

使用控制台创建IGMP多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择 Create transit gateway multicast domain（创建中转网关多播域）。
4. 对于 Name tag（名称标签），输入域的名称。
5. 对于 Transit Gateway ID（中转网关 ID），选择处理多播流量的中转网关。
6. 要获得IGMPv2支持，请选中该复选框。
7. 要获得静态源支持，请清除该复选框。
8. 要自动接受此多播域的跨账户子网关联，请选择 Auto accept shared associations（自动接受共享关联）。
9. 选择 Create transit gateway multicast domain（创建中转网关多播域）。

要使用创建IGMP多播域 AWS CLI

使用 create-transit-gateway-multicast-domain 命令。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

使用 Amazon Tr VPC ansit Gateways 创建静态源多播域

如果您尚未执行此操作，请查看可用的多播域属性。有关更多信息，请参阅 the section called “多播域”。

要使用控制台创建静态多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择 Create transit gateway multicast domain（创建中转网关多播域）。
4. 对于 Name tag（命名标签），输入用于标识域的名称。
5. 对于 Transit Gateway ID（中转网关 ID），选择处理多播流量的中转网关。
6. 要获得IGMPv2支持，请清除该复选框。
7. 要获得静态源支持，请选中该复选框。
8. 要自动接受此多播域的跨账户子网关联，请选择 Auto accept shared associations（自动接受共享关联）。
9. 选择 Create transit gateway multicast domain（创建中转网关多播域）。

要使用创建静态多播域 AWS CLI

使用 create-transit-gateway-multicast-domain 命令。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

使用 Amazon Transit Gateways 将VPC附件和子网与多播域相关联 VPC

使用以下步骤将VPC附件与多播域关联。创建关联时，您可以随后选择要包括在多播域中的子网。

在开始之前，您必须在公交网关上创建VPC附件。有关更多信息，请参阅 亚马逊VPC公交网关中的亚马逊VPC附件。

使用控制台将VPC附件与多播域关联

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域，然后依次选择 Actions（操作）、Create association（创建关联）。

4. 对于 Choose attachment to associate（选择要关联的挂载），选择中转网关挂载。
5. 对于 Choose subnets to associate（选择要关联的子网），选择要包括在多播域中的子网。
6. 选择 Create association（创建关联）。

要将VPC附件与多播域关联，请使用 AWS CLI

使用 associate-transit-gateway-multicast-domain 命令。

使用 Ama VPC zon Transit Gateways 取消子网与多播域的关联

使用以下过程取消子网与多播域的关联。

使用控制台取消子网的关联

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。
4. 选择 Associations (关联) 选项卡。
5. 选择子网，然后选择 Actions（操作）、Delete association（删除关联）。

要取消子网的关联，请使用 AWS CLI

使用 disassociate-transit-gateway-multicast-domain 命令。

使用 Amazon VPC 公交网关查看多播域关联

查看您的多播域以验证它们是否可用，以及它们是否包含相应的子网和附件。

要使用控制台查看多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。
4. 选择 Associations (关联) 选项卡。

要使用查看多播域 AWS CLI

使用 describe-transit-gateway-multicast-domains 命令。

使用 Amazon Tr VPC ansit Gateways 向多播域添加标签

向资源添加标签以帮助整理和识别资源，例如，按用途、拥有者或环境。您可以向每个多播域添加多个标签。每个多播域的标签键必须唯一。如果您添加的标签中的键已经与多播域关联，它将更新该标签的值。有关更多信息，请参阅标记您的 Amazon EC2 资源。

要使用控制台向多播域添加标签

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。
4. 依次选择 Actions（操作）、Manage tags（管理标签）。
5. 对于每个标签，选择 Add new tag（添加新标签），然后输入标签的 Key（键）和 Value（值）。
6. 选择保存。

要向多播域添加标签，请使用 AWS CLI

使用 create-tags 命令。

使用 Amazon VPC 传输网关删除多播域

使用以下过程删除中多播域。

要使用控制台删除多播域

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域，然后依次选择 Actions（操作）、Delete multicast domain（删除多播域）。
4. 提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

要删除多播域，请使用 AWS CLI

使用 delete-transit-gateway-multicast-domain 命令。

Amazon 公VPC交网关中的共享多播域

通过组播域共享，组播域所有者可以与其组织内或 AWS Organizations中的组织间的其他 AWS 账户共享该域。作为多播域拥有者，您可以集中创建和管理多播域。共享后，这些用户可以在共享的多播域上执行以下操作：

- 在多播域中注册和取消注册组成员或组源
- 将子网与多播域关联，并取消子网与多播域的关联

多播域拥有者可以与以下角色共享多播域：

- AWS 组织内部或组织中的跨组织账户 AWS Organizations
- 其组织内部的组织单位 AWS Organizations
- 它的整个组织都在 AWS Organizations
- AWS 之外的账户 AWS Organizations。

  要与组织外部的 AWS 帐户共享多播域，必须使用 AWS Resource Access Manager创建资源共享，然后在选择要与之共享多播域的委托人时选择 “允许与任何人共享”。有关创建资源共享的更多信息，请参阅 AWS RAM 用户指南中的在 AWS RAM中创建资源共享。

内容

共享多播域的先决条件

- 要共享多播域名，您必须在自己的 AWS 账户中拥有该域名。您无法共享已与您共享的多播域。

- 要与您的组织或中的组织单位共享多播域 AWS Organizations，必须启用与 AWS Organizations共享。有关更多信息，请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations 共享。

相关服务

多播域共享与 AWS Resource Access Manager (AWS RAM) 集成。 AWS RAM 是一项服务，可让您与任何 AWS 账户或通过任何账户共享 AWS 资源 AWS Organizations。利用 AWS RAM，您可通过创建 资源共享来共享您拥有的资源。资源共享指定要共享的资源以及与之共享的用户。消费者可以是个人 AWS 帐户、组织单位或整个组织 AWS Organizations。

有关的更多信息 AWS RAM，请参阅《AWS RAM 用户指南》。

共享的多播域权限

拥有者的权限

拥有者负责管理多播域以及他们注册或与该域关联的成员和挂载。拥有者可以随时更改或撤销共享访问权限。他们可以使用 AWS Organizations 来查看、修改和删除使用者在共享多播域上创建的资源。

使用者的权限

共享多播域的用户可以在共享多播域上执行以下操作，方法与他们创建的多播域相同：

- 在多播域中注册和取消注册组成员或组源
- 将子网与多播域关联，并取消子网与多播域的关联

使用者负责管理他们在共享多播域上创建的资源。

客户无法查看或修改其他使用者或多播域拥有者拥有的资源，也不能修改与他们共享的多播域。

计费和计量

对于拥有者或使用者的共享多播域，不会收取额外费用。

配额

共享多播域计入所有者和共享用户的组播域配额。

在 Amazon VPC 公交网关中跨可用区域共享资源

为了确保资源分布在某个地区的可用区中，Amazon T VPC ransit Gateways 会独立地将可用区映射到每个账户的名称。这可能会导致账户之间的可用区命名差异。例如，您 AWS 账户的可用区us-east-1a可能与其他 AWS 账户的可用区不同。us-east-1a

要确定您的多播域相对于账户的位置，您必须使用可用区 ID (AZ ID)。可用区 ID 是所有 AWS 账户中可用区的唯一且一致的标识符。例如，use1-az1是该us-east-1区域的可用区 ID，它在每个 AWS 账户中的位置都相同。

查看您账户IDs中可用区的可用区

1. 打开 AWS RAM 控制台，网址为 https://console.aws.amazon.com/ram。
2. 当前区域IDs的可用区显示在屏幕右侧的 “您的可用区 ID” 面板中。

使用 Amazon Tr VPC ansit Gateways 共享多播域

当所有者与您共享多播域时，您可以执行以下操作：

- 注册和取消注册组成员或组源
- 关联和取消关联子网

> **Note**
>
> 要共享多播域，必须将其添加到资源共享中。资源共享是一种 AWS RAM 允许您跨 AWS 账户共享资源的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用共享多播域时 Amazon Virtual Private Cloud Console，可以将其添加到现有资源共享中。要将多播域添加到新的资源共享中，必须首先使用 AWS RAM 控制台创建资源共享。
> 如果您是组织中的一员， AWS Organizations 并且启用了组织内部共享，则会自动授予组织中的消费者访问共享多播域的权限。否则，使用者将会收到加入资源共享的邀请，并在接受邀请后获得对共享多播域的访问权限。

您可以使用 Amazon Virtual Private Cloud 控制台、 AWS RAM 控制台或共享您拥有的多播域。 AWS CLI

要使用 *Amazon Virtual Private Cloud Console共享您拥有的多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Multicast Domains（多播域）。
3. 选择您的多播域，然后选择 Actions（操作）、Share multicast domain（共享多播域）。
4. 选择您的资源共享，然后选择 Share multicast domain（共享多播域）。

使用控制台共享您拥有的多播域 AWS RAM

请参阅《AWS RAM 用户指南》中的创建资源共享。

要共享您拥有的多播域，请使用 AWS CLI

使用create-resource-share命令。

使用 Ama VPC zon Transit Gateways 取消共享多播域

当共享的多播域被取消共享时，使用者多播域资源会发生以下情况：

- 使用者子网与多播域的关联被解除。子网仍保留在使用者账户中。
- 使用者组源和组成员将与多播域取消关联，然后从使用者账户中删除。

要取消共享多播域，必须将其从资源共享中删除。您可以通过 AWS RAM 控制台或 AWS CLI.

要取消共享您拥有的已共享多播域，必须从资源共享中将其删除。您可以使用 Amazon Virtual Private Cloud、 AWS RAM 控制台或 AWS CLI。

要使用 *Amazon Virtual Private Cloud Console取消共享您拥有的共享多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Multicast Domains（多播域）。
3. 选择您的多播域，然后依次选择 Actions（操作）、Stop sharing（停止共享）。

使用控制台取消共享您拥有的共享多播域 AWS RAM

请参阅《AWS RAM 用户指南》中的更新资源共享。

要取消共享您拥有的共享多播域，请使用 AWS CLI

使用disassociate-resource-share命令。

使用 Amazon Tr VPC ansit Gateways 识别共享的多播域

所有者和使用者可以使用和来识别共享的 Amazon Virtual Private Cloud 多播域 AWS CLI

要使用 *Amazon Virtual Private Cloud Console识别共享的多播域

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Multicast Domains（多播域）。
3. 选择您的多播域。
4. 在传输组播域详细信息页面上，查看所有者 ID 以识别组播域的 AWS 账户 ID。

要使用识别共享的多播域 AWS CLI

使用 describe-transit-gateway-multicast-domains 命令。该命令返回您拥有的多播域和与您共享的多播域。 `OwnerId`显示多播域所有者的 AWS 帐户 ID。

使用 Amazon Tr VPC ansit Gateways 向组播组注册源

> **Note**
>
> 仅当您将静态源支持属性设置为启用时，才需要执行此过程。

使用以下过程将源注册到多播组。源是发送多播流量的网络接口。

您需要以下信息才能添加源：

- 多播域的 ID
- 来源IDs的网络接口
- 多播组 IP 地址

使用控制台注册源

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。

3. 选择多播域，然后依次选择 Actions（操作）、Add group sources（添加组源）。
4. 在“组 IP 地址”中，输入要分配给多播域的IPv4CIDRIPv6CIDR块或块。
5. 在 Choose network interfaces (选择网络接口) 下，选择多播发送方的网络接口。
6. 选择 Add sources (添加源)。

要使用注册来源 AWS CLI

使用 register-transit-gateway-multicast-group-sources 命令。

使用 Amazon Tr VPC ansit Gateways 向组播群组注册成员

使用以下过程将组成员注册到多播组。

您需要以下信息才能添加成员：

- 多播域的 ID
- 小组IDs成员的网络接口
- 多播组 IP 地址

使用控制台注册成员

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域，然后依次选择 Actions（操作）、Add group members（添加组成员）。
4. 在“组 IP 地址”中，输入要分配给多播域的IPv4CIDRIPv6CIDR块或块。
5. 在 Choose network interfaces (选择网络接口) 下，选择多播接收方的网络接口。
6. 选择 Add members (添加成员)。

要使用注册会员 AWS CLI

使用 register-transit-gateway-multicast-group-members 命令。

使用 Ama VPC zon Transit Gateways 从多播组取消注册源

除非您手动将源添加到多播组，否则无需遵循此过程。

使用控制台删除源

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。
4. 选择组选项卡。
5. 选择源，然后选择 Remove source (删除源)。

要移除来源，请使用 AWS CLI

使用 deregister-transit-gateway-multicast-group-sources 命令。

使用 Ama VPC zon Transit Gateways 从多播群组中注销成员

除非您手动将成员添加到多播组，否则无需遵循此过程。

使用控制台取消注册成员

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。
4. 选择组选项卡。
5. 选择成员，然后选择 Remove member (删除成员)。

要取消注册会员，请使用 AWS CLI

使用 deregister-transit-gateway-multicast-group-members 命令。

使用 Amazon VPC 公交网关查看多播组

您可以查看有关您的组播组的信息，以验证是否使用该IGMPv2协议发现了成员。IGMP当 AWS 发现使用该协议的@@ 成员时，会显示成员类型MemberType（在控制台中 AWS CLI）或（在）。

使用控制台查看多播组

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择中转网关多播。
3. 选择多播域。

4. 选择组选项卡。

要查看组播组，请使用 AWS CLI

使用 search-transit-gateway-multicast-groups 命令。

以下示例显示IGMP协议发现了组播组成员。

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
        }
    ]
}
```

在亚马逊VPC公交网关中为 Windows 服务器设置多播

在 Windows Server 2019 或 2022 上设置多播以使用中转网关时，您需要执行其他步骤。要进行此设置 PowerShell，你需要使用并运行以下命令：

要为 Windows 服务器设置多播，请使用 PowerShell

1. 更改 Windows 服务器以IGMPv2代IGMPv3替 TCP /IP 堆栈：

```
PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
\Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
```

> **Note**
>
> New-ItemProperty是指定IGMP版本的属性索引。由于 IGMP v2 是多播支持的版本，因此该属性Value必须是。3您可以运行以下命令将IGMP版本设置为 2，而不是编辑 Windows 注册表。：

```
    Set-NetIPv4Protocol -IGMPVersion Version2
```

2. 默认情况下，Windows 防火墙会丢弃大多数UDP流量。您首先需要检查哪个连接配置文件用于多播：

```
PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

NetworkCategory
---------------
         Public
```

3. 更新上一步中的连接配置文件以允许访问所需UDP端口：

```
PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
```

4. 重启 EC2 实例。
5. 测试您的多播应用程序，确保流量按预期流动。

示例：使用 Amazon VPC 公交网关管理IGMP配置

此示例显示了至少一台使用该IGMP协议进行多播流量的主机。 AWS 当多播组收到来自实例的IGMPJOIN消息时，它会自动创建该组，然后将该实例添加为该组的成员。您也可以使用将非IGMP主机静态添加为群组的成员。 AWS CLI位于与多播域关联的子网中的任何实例都可以发送流量，组成员将接收多播流量。

使用以下步骤完成配置：

1. 创建一个VPC. 有关创建的更多信息VPCs，请参阅 Amazon VPC 用户指南VPC中的创建。
2. 在VPC中创建子网。有关创建子网的更多信息，请参阅 Amazon VPC 用户指南VPC中的在中创建子网。
3. 创建为多播流量配置的中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
4. 创建VPC附件。有关更多信息，请参阅 the section called “创建VPC附件”。
5. 创建为IGMP支持而配置的多播域。有关更多信息，请参阅 the section called “创建IGMP多播域”。

   使用以下设置：

   - 启用IGMPv2支持。
   - 禁用 Static sources support（静态源支持）。

6. 在传输网关VPC连接中的子网和组播域之间创建关联。有关更多信息，请参阅the section called “将VPC附件和子网与多播域相关联”。
7. 的默认IGMP版本EC2是IGMPv3。您需要更改所有IGMP群组成员的版本。您可以运行以下命令：

```
sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
```

8. 将不使用该IGMP协议的成员添加到组播组。有关更多信息，请参阅 the section called “将成员注册到多播组”。

示例：使用 Amazon VPC 公交网关管理静态源配置

此示例以静态方式将多播源添加到组中。主机不使用该IGMP协议加入或退出组播组。您需要静态添加接收多播流量的组成员。

使用以下步骤完成配置：

1. 创建一个VPC. 有关创建的更多信息VPCs，请参阅 Amazon VPC 用户指南VPC中的创建。
2. 在VPC中创建子网。有关创建子网的更多信息，请参阅 Amazon VPC 用户指南VPC中的在中创建子网。
3. 创建为多播流量配置的中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
4. 创建VPC附件。有关更多信息，请参阅 the section called “创建VPC附件”。
5. 创建配置为不IGMP支持且支持静态添加源的组播域。有关更多信息，请参阅 the section called “创建静态源组播域”。

   使用以下设置：

   - 禁用IGMPv2支持。
   - 要手动添加源，请启用 Static sources support（静态源支持）。

     当启用属性时，源是唯一可发送多播流量的资源。否则，位于与多播域关联的子网中的任何实例都可以发送多播流量，组成员将接收多播流量。
6. 在传输网关VPC连接中的子网和组播域之间创建关联。有关更多信息，请参阅the section called “将VPC附件和子网与多播域相关联”。
7. 如果您启用 Static sources support（静态源支持），请将源添加到多播组。有关更多信息，请参阅 the section called “将源注册到多播组”。
8. 将成员添加到多播组。有关更多信息，请参阅 the section called “将成员注册到多播组”。

示例：在 Amazon VPC 公交网关中管理静态群组成员配置

此示例显示了以静态方式向群组添加多播成员。主机不能使用该IGMP协议加入或退出组播组。位于与多播域关联的子网中的任何实例都可以发送多播流量，组成员将接收多播流量。

使用以下步骤完成配置：

1. 创建一个VPC. 有关创建的更多信息VPCs，请参阅 Amazon VPC 用户指南VPC中的创建。
2. 在VPC中创建子网。有关创建子网的更多信息，请参阅 Amazon VPC 用户指南VPC中的在中创建子网。
3. 创建为多播流量配置的中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
4. 创建VPC附件。有关更多信息，请参阅 the section called “创建VPC附件”。
5. 创建配置为不IGMP支持且支持静态添加源的组播域。有关更多信息，请参阅 the section called “创建静态源组播域”。

   使用以下设置：

   - 禁用IGMPv2支持。
   - 禁用 Static sources support（静态源支持）。
6. 在传输网关VPC连接中的子网和组播域之间创建关联。有关更多信息，请参阅the section called “将VPC附件和子网与多播域相关联”。
7. 将成员添加到多播组。有关更多信息，请参阅 the section called “将成员注册到多播组”。

Amazon VPC 公交网关流日志

Transit Gateway Flow Logs 是 Amazon Tr VPC ansit Gateway 的一项功能，它使您能够捕获有关进出中转网关的 IP 流量的信息。流日志数据可以发布到亚马逊 CloudWatch 日志、亚马逊 S3 或 Firehose。在创建流日志后，您可以在所选的目标中检索和查看其数据。流日志数据是在网络流量路径之外收集的，因此不会影响网络吞吐量或延迟。您可以创建或删除流日志，而不会对网络性能造成任何影响。Transit Gateway 流日志仅捕获与中转网关有关的信息，详见the section called “Transit Gateway 流日志记录”中所述。如果要捕获有关进出您的网络接口的 IP 流量的信息VPCs，请使用 VPC Flow Logs。有关更多信息，请参阅 Amazon VPC 用户指南中的使用VPC流日志记录 IP 流量。

> **Note**
>
> 要创建传输网关流日志，您必须是该传输网关的所有者。如果您不是所有者，则公交网关所有者必须授予您权限。

中转网关的流日志数据保存为流日志记录，即日志事件，由多个描述流量信息的字段组成。有关更多信息，请参阅 Transit Gateway 流日志记录。

要创建流日志，请指定：

- 要为其创建流日志的资源
- 指定您要将流日志数据发布到的目标

创建流日志后，需要几分钟来开始收集数据并将数据发布到选定目标。流日志不会为您的中转网关获取实时日志流。有关更多信息，请参阅 创建 Amazon VPC 公交网关流日志。

您可以将标签应用于流日志。每个标签都包含您定义的一个键和一个可选值。标签可以帮助您整理流日志，例如按目的或拥有者。

如果您不再需要某个流日志，可将其删除。删除流日志会禁用该资源的流日志服务，并且不会创建新的流日志记录或将其发布到 CloudWatch 日志或 Amazon S3。删除流日志不会删除传输网关的任何现有流日志记录或日志流（对于 CloudWatch 日志）或日志文件对象（对于 Amazon S3）。要删除现有的日志流，请使用 CloudWatch 日志控制台。要删除现有日志文件对象，请使用 Amazon S3 控制台。在删除流日志之后，可能需要数分钟时间来停止收集数据。有关更多信息，请参阅 删除 Amazon VPC 公交网关流日志记录。

限制

以下限制适用于 Transit Gateway 流日志：

- 不支持多播流量。
- 不支持 Connect 附件。所有 Connect 流日志都显示在传输附件下方，因此必须在传输网关或 Connect 传输附件上启用。

Transit Gateway 流日志记录

流日志记录代表您的中转网关中的网络流。每条记录都是一个字符串，字段用空格分隔。记录包含网络流的不同的结构信息，包括源、目标和协议。

当您创建流日志时，您可以为流日志记录使用默认格式，也可以指定自定义格式。

内容

默认格式

使用默认格式，流日志记录包括所有版本 2 到版本 6 字段，顺序如可用字段表中所示。您无法自定义或更改默认格式。要捕获其他字段或不同字段子集，请指定自定义格式。

自定义格式

使用自定义格式，您可以指定流日志记录中包含哪些字段以及采用哪种顺序。这使您可以根据具体需求创建流日志，并忽略无关的字段。使用自定义格式，还可减少从发布的流日志提取特定信息所需的单独流程。您可以指定任意数量的可用流日志字段，但必须至少指定一个。

可用字段

下表描述了中转网关流日志记录的所有可用字段。版本列表示在哪个版本中引入了该字段。

将流日志数据发布到 Amazon S3 时，字段的数据类型将取决于流日志格式。如果格式为纯文本，则所有字段的类型均为 STRING。如果格式为 Parquet，请参阅字段数据类型表。

如果某个字段不适用于或无法计算特定记录，则记录为该条目显示一个“-”符号。不直接来自数据包标头的元数据字段是最大努力的近似值，它们的值可能缺失或不准确。

字段	描述	版本
version	表示在哪个版本中引入了该字段。默认格式包括所有版本 2 字段，与它们在表格中出现的顺序相同。 实木复合地板数据类型：INT_32	2
resource-type	在其上创建订阅的资源的类型。对于 Transit Gateway 流日志，这将是TransitGateway。 实木复合地板数据类型：STRING	6
account-id	源传输网关所有者的 AWS 账户 ID。 实木复合地板数据类型：STRING	2
tgw-id	正在记录其流量的中转网关的 ID。 实木复合地板数据类型：STRING	6
tgw-attachment-id	正在记录其流量的中转网关连接的 ID。 实木复合地板数据类型：STRING	6
tgw-src-vpc-account-id	源VPC流量的 AWS 账户 ID。 实木复合地板数据类型：STRING	6
tgw-dst-vpc-account-id	目标VPC流量的 AWS 账户 ID。 实木复合地板数据类型：STRING	6
tgw-src-vpc-id	传输网关VPC的来源 ID 实木复合地板数据类型：STRING	6
tgw-dst-vpc-id	传输网关的VPC目的地 ID。 实木复合地板数据类型：STRING	6

字段	描述	版本
tgw-src-subnet-id	中转网关源流量的子网 ID。 实木复合地板数据类型：STRING	6
tgw-dst-subnet-id	中转网关目标流量的子网 ID。 实木复合地板数据类型：STRING	6
tgw-src-eni	流的源传输网关连接ENI的 ID。 实木复合地板数据类型：STRING	6
tgw-dst-eni	流的目标中转网关连接ENI的 ID。 实木复合地板数据类型：STRING	6
tgw-src-az-id	包含记录其流量的源中转网关的可用区的 ID。如果流量来自子位置，则记录会对此字段显示“-”符号。 实木复合地板数据类型：STRING	6
tgw-dst-az-id	包含记录其流量的目标中转网关的可用区的 ID。 实木复合地板数据类型：STRING	6
tgw-pair-attachment-id	根据流向的不同，这要么是流量的出口连接 ID，要么是入口连接 ID。 实木复合地板数据类型：STRING	6
srcaddr	传入流量的源地址。 实木复合地板数据类型：STRING	2
dstaddr	传出流量的目标地址。 实木复合地板数据类型：STRING	2

字段	描述	版本
srcport	流量的源端口。 实木复合地板数据类型：INT_32	2
dstport	流量的目标端口。 实木复合地板数据类型：INT_32	2
protocol	流量的IANA协议号。有关更多信息，请参阅分配的 Internet 协议编号。 实木复合地板数据类型：INT_64	2
packets	在流中传输的数据包的数量。 实木复合地板数据类型：INT_64	2
bytes	在流中传输的字节数。 实木复合地板数据类型：INT_64	2
start	在聚合时间间隔内，接收流的第一个数据包的时间（以 Unix 秒为单位）。在中转网关传输或收到数据包之后,最多 60 秒。 实木复合地板数据类型：INT_64	2
end	在聚合时间间隔内，接收流的最后一个数据包的时间（以 Unix 秒为单位）。在中转网关传输或收到数据包之后,最多 60 秒。 实木复合地板数据类型：INT_64	2

字段	描述	版本
log-status	流日志的状态： • OK — 数据正常记录到选定目标。 • NODATA— 在聚合间隔内，没有进出网络接口的网络流量。 • SKIPDATA— 在聚合间隔内，某些流日志记录被跳过。这可能是由于内部容量限制或内部错误。 实木复合地板数据类型：STRING	2
type	流量的类型。可能的值为 IPv4 | IPv6 | EFA。有关更多信息，请参阅 Amazon EC2 用户指南中的弹性结构适配器。 实木复合地板数据类型：STRING	3
packets-lost-no-route	由于未指定路由而丢失的数据包。 实木复合地板数据类型：INT_64	6
packets-lost-blackhole	数据包由于黑洞而丢失。 实木复合地板数据类型：INT_64	6
packets-lost-mtu-exceeded	由于大小超过，数据包丢失MTU。 实木复合地板数据类型：INT_64	6
packets-lost-ttl-expired	由于的过期，数据包丢失 time-to-live。 实木复合地板数据类型：INT_64	6

字段	描述	版本
tcp-flags	以下TCP标志的位掩码值： • FIN— 1 • SYN— 2 • RST— 4 • PSH— 8 • ACK— 16 • SYN-ACK — 18 • URG— 32 **Important** 当流日志条目仅包含ACK数据包时，标志值为 0 而不是 16。 有关TCP旗帜的一般信息（例如、和FIN、等标志的含义 ACK）SYN，请参阅维基百科上的TCP区段结构。 TCP在聚合间隔内，可以对标志进行 OR 运算。对于短连接，可以在流日志记录的同一行上设置标志，例如，19 代表 SYN-ACK 和 FIN，3 代表SYN和FIN。 实木复合地板数据类型：INT_32	3
region	包含记录其流量的中转网关的区域。 实木复合地板数据类型：STRING	4
flow-direction	相对于捕获流量的接口而言流的方向。可能的值包括：ingress | egress。 实木复合地板数据类型：STRING	5

字段	描述	版本
pkt-src-aws-service	srcaddr如果源 IP 地址用于 AWS 服务，则为 IP 地址范围子集的名称。可能的值包括：AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS。 实木复合地板数据类型：STRING	5
pkt-dst-aws-service	如果目标 IP 地址用于 AWS 服务，则为该dstaddr字段的 IP 地址范围子集的名称。有关可能的值的列表，请参阅 pkt-src-aws-service 字段。 实木复合地板数据类型：STRING	5

控制对流日志的使用

默认情况下，用户无权使用流日志。您可以创建一个用户策略，该策略向用户授予创建、描述和删除流日志的权限。有关更多信息，请参阅《亚马逊参EC2API考》中的 “向IAM用户授予亚马逊EC2资源所需的权限”。

下面是一个示例策略，该策略向用户授予创建、描述和删除流日志的完全权限。

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

```
  ]
}
```

需要进行一些额外的IAM角色和权限配置，具体取决于您是发布到 CloudWatch 日志还是 Amazon S3。有关更多信息，请参阅Transit Gateway 流量记录亚马逊 CloudWatch 日志中的记录 和 中转网关流日志 Amazon S3 中的记录 。

中转网关流日志定价

发布中转网关流日志时，将收取已出售日志的数据摄取和存储费用。有关发布销售日志时定价的更多信息，请打开 Amazon P CloudWatch ricing，然后在 “付费套餐” 下，选择 “日志” 并找到 Vended Logs。

为 Amazon Transi IAM t Gatew VPC ays 流日志创建或更新角色

您可以使用 AWS Identity and Access Management 控制台更新现有角色或使用以下过程创建用于流日志的新角色。

为流日志创建IAM角色

1. 打开IAM控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色）和 Create role（创建角色）。
3. 对于Select type of trusted entity（选择受信任实体的类型），选择 AWS service（服务）。对于“用例”，选择EC2。选择下一步。
4. 在 Add permissions（添加权限）页面，选择 Next: Tags（下一步: 标签），还可以选择性地添加标签。选择下一步。
5. 在命名、查看和创建页面上，输入您的角色名称并可选择性地提供描述。选择 Create role（创建角色）。
6. 选择角色的名称。对于 “添加权限”，选择 “创建内联策略”，然后选择JSON选项卡。
7. 从 IAM用于将流日志发布到 CloudWatch 日志的角色 中复制第一个策略，并将其粘贴到窗口中。选择Review policy（查看策略）。
8. 为您的策略输入名称，然后选择 Create policy（创建策略）。
9. 选择角色的名称。对于 Trust relationships（信任关系），选择 Edit trust relationship（编辑信任关系）。在现有策略文档中，将服务从 `ec2.amazonaws.com` 更改为 `vpc-flow-logs.amazonaws.com`。选择 Update Trust Policy（更新信任策略）。
10. 在 “摘要” 页面上，记下您的角色ARN对应的。创建流日志ARN时需要这个。

Transit Gateway 流量记录亚马逊 CloudWatch 日志中的记录

流日志可以将流日志数据直接发布到 Amazon CloudWatch。

发布到 Lo CloudWatch gs 后，流日志数据将发布到日志组，并且每个传输网关在日志组中都有唯一的日志流。日志流包含流日志记录。您可以创建将数据发布到相同日志组的多个流日志。如果同一中转网关存在于同一日志组中的一个或多个流日志中，则它具有一个组合日志流。如果您指定了一个流日志应该捕获已拒绝流量，而另一个流日志应该捕获已接受流量，则组合日志流会捕获所有流量。

当您将流日志发布到 Logs 时，会收取已售日志的数据摄取和存档费用。 CloudWatch 有关更多信息，请参阅 Amazon CloudWatch 定价。

在 CloudWatch 日志中，时间戳字段对应于流日志记录中捕获的开始时间。该ingestionTime字段提供日志收到流日志记录的日期和时间。 CloudWatch 此时间戳晚于在流日志记录中捕获的结束时间。

有关 CloudWatch 日志的更多信息，请参阅 Amazon Logs 用户指南中的发送到 CloudWatch CloudWatch 日志的日志。

内容

- IAM用于将流日志发布到 CloudWatch 日志的角色
- IAM用户传递角色的权限
- 创建发布到 Transit Gateways 流日志记录 Amazon CloudWatch Logs
- 在亚马逊上查看 Transit Gateway 流量日志记录 CloudWatch
- 处理 Amazon 日志中的 Transit Gateway 流量 CloudWatch 日志记录

IAM用于将流日志发布到 CloudWatch 日志的角色

与您的流日志关联的IAM角色必须具有足够的权限才能将流日志发布到日志中的指定 CloudWatch 日志组。该IAM角色必须属于你的 AWS 账户。

附加到您的IAM角色的IAM策略必须至少包含以下权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

另请确保您的角色具有信任关系，以允许流日志服务代入该角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

建议您使用 aws:SourceAccount 和 aws:SourceArn 条件键来防止出现混淆代理人问题。例如，您可以将以下条件块添加到以前的信任策略。源账户是流日志的所有者，源账户ARN是流日志ARN。如果您不知道流日志 ID，则可以将该部分替换为通配符 (*)，然后在创建流日志之后更新策略。ARN

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

IAM用户传递角色的权限

用户还必须有权使用与流日志关联的IAM角色的iam:PassRole操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

创建发布到 Transit Gateways 流日志记录 Amazon CloudWatch Logs

您可以为中转网关创建流日志。如果您以IAM用户身份执行这些步骤，请确保您拥有使用该`iam:PassRole`操作的权限。有关更多信息，请参阅 IAM用户传递角色的权限。

使用控制台创建中转网关流日志

1. 登录 AWS Management Console 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）。
3. 选中一个或多个中转网关的复选框，然后选择操作、创建流日志。
4. 对于目标，选择发送到 CloudWatch日志。
5. 对于 Destination log group（目的地日志组），选择当前的目的地日志组的名称。

   > **Note**
   >
   > 如果目的地日志组尚不存在，则在此字段中输入新名称将创建新的目标日志组。

6. 对于IAM角色，请指定有权将日志发布到 CloudWatch 日志的角色的名称。
7. 对于Log record format（日志记录格式），选定流日志记录的格式。
   - 要使用默认格式，请选择AWS default format（亚马逊云科技默认格式）。
   - 要使用自定义格式，请选择Custom format（自定义格式）然后从Log format（日志格式）选择字段。
8. （可选）选择Add new tag（添加新标签）以将标签应用于流日志。
9. 选择 Create flow log（创建流日志）。

使用命令行创建流日志

使用以下命令之一。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs（亚马逊EC2查询API）

以下 AWS CLI 示例创建了捕获中转网关信息的流日志。流日志使用角色传送到账户 123456789101 中名为“ CloudWatch my-flow-logs日志”的日志组。IAM publishFlowLogs

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

在亚马逊上查看 Transit Gateway 流量日志记录 CloudWatch

您可以使用日志控制台或 Amazon S3 控制台查看您的流 CloudWatch 日志记录，具体取决于所选的目标类型。在您创建流日志之后，可能需要几分钟才能显示在控制台中。

查看发布到日志的流 CloudWatch 日志记录

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，请选择 Logs（日志），然后选择包含您日志流的日志组。此时将显示每个中转网关的日志流的列表。
3. 选择包含您希望查看其流日志记录的中转网关 ID 的日志流。有关更多信息，请参阅 Transit Gateway 流日志记录。

处理 Amazon 日志中的 Transit Gateway 流量 CloudWatch 日志记录

您可以像处理日志收集的任何其他日志事件一样处理流 CloudWatch 日志记录。有关监控日志数据和指标筛选条件的更多信息，请参阅 Amazon CloudWatch 用户指南中的搜索和筛选日志数据。

示例：为流日志创建 CloudWatch 指标筛选器和警报

在此示例中，您有一个适用于 tgw-123abc456bca 的流日志。如果在 1 小时内有 10 次或更多通过 TCP端口 22 (SSH) 连接到您的实例的尝试被拒绝，则您想要创建一个警报，提醒您。首先，您必须创

建一个指标筛选条件，该指标筛选条件与为其创建警报的流量的模式相匹配。然后，您可以为该指标筛选条件创建警报。

为被拒绝的SSH流量创建指标筛选器并为过滤器创建警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择日志和日志组。
3. 选中日志组的复选框，然后选择操作、创建指标筛选器。
4. 对于Filter Pattern（筛选模式），输入以下内容：

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. 对于 Select log data to test（选择要测试的日志数据），选择您的中转网关对应的日志流。（可选）要查看与筛选条件模式匹配的日志数据行，请选择 Test pattern（测试模式）。准备就绪后，选择 Next（下一步）。
6. 输入筛选条件名称、指标命名空间和指标名称。将指标值设置为 **1**。完成后，选择 Next（下一步），然后选择 Create metric filter（创建指标筛选条件）。
7. 在导航窗格中，依次选择 Alarms（警报）和 All alarms（所有警报）。
8. 选择Create alarm（创建警报）。
9. 为您创建的指标筛选条件选择命名空间。

   新指标可能需要几分钟才会在控制台中显示。
10. 选择您创建的指标名称，然后选择 Select metric（选择指标）。
11. 按如下所示配置警报，然后选择 Next（下一步）：

    - 对于 Statistic（统计数据），选择 Sum（总计）。这可以确保您捕获指定时间段内的数据点的总数。
    - 对于 Period（周期），选择 1 hour（1 小时）。
    - 对于 Whenever（每当），选择 Greater/Equal（大于/等于，**>=**），然后输入 **10** 作为阈值。

- 对于 Additional configuration（其他配置），Datapoints to alarm（警报的数据点数），将默认值设为 **1**。

12. 在 “通知” 中，选择现有SNS主题，或选择 “创建新主题” 来创建新主题。选择 Next（下一步）。
13. 输入警报的名称和描述，然后选择 Next（下一步）。
14. 配置完警报后，选择 Create alarm（创建警报）。

中转网关流日志 Amazon S3 中的记录

流日志可以将流日志数据发布到 Amazon S3。

在发布到 Amazon S3 时，流日志数据将发布到您指定的现有 Amazon S3 存储桶。所有受监控的中转网关的流日志记录将发布到在存储桶中存储的一系列日志文件对象。

当您将流日志发布到 Amazon S3 时，将 Amazon CloudWatch 对出售的日志收取数据摄取和存档费用。有关销售日志 CloudWatch 定价的更多信息，请打开 Amazon Pric CloudWatch in g，选择日志，然后找到销售日志。

要创建用于流日志的 Amazon S3 存储桶，请参阅《Amazon Simple Storage Service 用户指南》中的Create a bucket（创建存储桶）。

有关多账户日志记录的更多信息，请参阅 AWS 解决方案库中的集中日志记录。

有关 CloudWatch 日志的更多信息，请参阅 Amazon 日志用户指南中的发送到 A mazon S3 的 CloudWatch 日志。

内容

流日志文件

VPCFlow Logs 是一项功能，可收集流日志记录，将其合并到日志文件中，然后每隔 5 分钟将日志文件发布到 Amazon S3 存储桶。每个日志文件包含在上一个 5 分钟期间内记录的 IP 流量的流日志记录。

日志文件的最大文件大小为 75 MB。如果日志文件在 5 分钟期间内达到文件大小限制，流日志会停止向它添加流日志记录。然后将它发布到 Amazon S3 存储桶，并创建一个新的日志文件。

在 Amazon S3 中，流日志文件的 Last modified（上次修改时间）字段表示文件上传到 Amazon S3 存储桶的日期和时间。此时间要晚于文件名中的时间戳，并且不同于将文件上传到 Amazon S3 存储桶所花费的时间。

日志文件格式

您可为日志文件指定下列格式之一。每个文件都被压缩为单个 Gzip 文件。

- Text – 纯文本。这是默认格式。
- Parquet – Apache Pparquet 是一种列式数据格式。与对纯文本数据的查询相比，对 Passic 格式的数据进行查询速度快 10 到 100 倍。使用 Gzip 压缩的 Parquet 格式的数据比 Gzip 压缩的纯文本格式的数据占用的存储空间少 20%。

日志文件选项

您也可以指定以下选项。

- Hive 兼容的 S3 前缀 – 启用 Hive兼容的前缀，而不是将分区导入 Hive 兼容工具中。请先使用 MSCK REPAIR TABLE 命令，然后再运行查询。
- 每小时分区 – 如果您有大量日志并且通常将查询定位到特定小时，则可以通过每小时对日志进行分区来获得更快的结果并节省查询成本。

日志文件 S3 存储桶结构

日志文件将保存到指定的 Amazon S3 存储桶，并使用由流日志的 ID、区域、创建日期及目标选项决定的文件夹结构。

默认情况下，文件传送到以下位置。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

如果启用 Hive 兼容的 S3 前缀，则文件将传送到以下位置。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/
```

如果启用每小时分区，则文件将传送到以下位置。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

如果启用 Hive 兼容的分区并每小时对流日志进行分区，则文件将传送到以下位置。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/hour=hour/
```

日志文件名称

日志文件的文件名基于流日志 ID、区域以及创建日期和时间。文件名使用以下格式。

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

下面显示了一个流日志的日志文件的示例，该流日志由 AWS 账户 123456789012 创建，用于 us-east-1 区域中的资源，创建时间为 June 20, 2018 16:20 UTC。该文件包含结束时间介于 16:20:00 和 16:24:59 之间的流日志记录。

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

IAM适用于向 Amazon IAM S3 发布流日志的委托人的政策

创建流日志的IAM委托人必须具有以下权限，这些权限是将流日志发布到目标 Amazon S3 存储桶所必需的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
```

```
      "Resource": "*"
    }
  ]
}
```

针对流日志的 Amazon S3 存储桶权限

默认情况下，Amazon S3 存储桶以及其中包含的对象都是私有的。只有存储桶拥有者才能访问存储桶和其中存储的对象。不过，存储桶拥有者可以通过编写访问策略来向其他资源和用户授予访问权限。

如果创建流日志的用户拥有存储桶并且对它具有 PutBucketPolicy 和 GetBucketPolicy 权限，则我们会自动将以下策略附加到存储桶。此策略将覆盖附加到存储桶的任何现有策略。

否则，存储桶拥有者必须将此策略添加到存储桶中，以指定流日志创建者的 AWS 账户 ID，否则流日志创建失败。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用存储桶策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl", "s3:ListBucket"],
            "Resource": "arn:aws:s3:::bucket_name",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

你ARN为之指定的 *my-s3-arn* 取决于您是否使用与 Hive 兼容的 S3 前缀。

- 默认前缀

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Hive 兼容的 S3 前缀

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

作为最佳实践，我们建议您将这些权限授予日志传输服务委托人而不是个人 AWS 账户 ARNs。此外，最好是使用 aws:SourceAccount 和 aws:SourceArn 条件键来防止出现混淆代理人问题。源账户是流日志的所有者，源账户ARN是日志服务的通配符 (*) ARN。

与 SSE-一起使用的必需密钥策略 KMS

您可以通过启用使用 Amazon S3 托管密钥的服务器端加密 (SSE-S3) 或使用密钥进行服务器端加密 (-) 来保护 Amazon S3 存储桶中的数据。KMS SSE KMS有关详情，请参阅《Amazon S3 用户指南》中的使用服务器端加密保护数据。

使用 SSE-KMS，您可以使用 AWS 托管密钥或客户托管密钥。使用 AWS 托管密钥，您就无法使用跨账户交付。流日志是从日志传输账户传输的，因此您必须授予跨账户传输的访问权限。要授予对您的 S3 存储桶的跨账户访问权限，请在启用存储桶加密时使用客户托管密钥并指定客户托管密钥的 Amazon 资源名称 (ARN)。有关详情，请参阅《Amazon S3 用户指南》中的使用 AWS KMS指定服务器端加密。

将 SSE-KMS 与客户托管密钥一起使用时，必须将以下内容添加到密钥的密钥策略（而不是您的 S3 存储桶的存储桶策略）中，这样 VPC Flow Logs 才能写入您的 S3 存储桶。

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Amazon S3 日志文件权限

除了所需的存储桶策略外，Amazon S3 还使用访问控制列表 (ACLs) 来管理对由流日志创建的日志文件的访问权限。默认情况下，存储桶拥有者对每个日志文件具有 FULL_CONTROL 权限。如果日志传输拥有者与存储桶拥有者不同，则没有权限。日志传输账户具有 READ 和 WRITE 权限。有关更多信息，请参阅 Amazon 简单存储服务用户指南中的访问控制列表 (ACL) 概述。

为 Amazon S3 创建 Transit Gateway Flow Logs 源账户角色

从源账户中，在 AWS Identity and Access Management 控制台中创建源角色。

创建源账户角色

1. 登录 AWS Management Console 并打开IAM控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 选择创建策略。
4. 在创建策略页面上，执行以下操作：

    1. 选择JSON。
    2. 将此窗口的内容替换为此部分开头的权限策略。
    3. 选择 Next: Tags（下一步：标签）和 Next: Review（下一步：审核）。

4. 输入您策略的名称和可选描述，然后选择 Create policy（创建策略）。
5. 在导航窗格中，选择角色。
6. 选择 Create role（创建角色）。
7. 对于 Trusted entity type（可信实体类型），选择 Custom trust policy（自定义信任策略）。对于 Custom trust policy（自定义信任策略），将 `"Principal": {},` 替换为以下内容，以指定日志传输服务。选择下一步。

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. 在 Add permissions（添加权限）页面上，选中您在此过程中先前创建的策略复选框，然后选择 Next（下一步）。
9. 输入您的角色的名称，并且可以选择提供描述。
10. 选择Create role（创建角色）。

创建发布到 Amazon S3 的 Transit Gateway 流日志记录

在您创建和配置 Amazon S3 存储桶后，您可以为中转网关创建流日志。

使用命令行工具创建发布到 Amazon S3 的中转网关流日志

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）或 Transit gateway attachments（中转网关连接）。
3. 选中一个或多个中转网关或中转网关连接复选框。
4. 选择 Actions（操作）、Create flow log（创建流日志）。
5. 配置流日志设置。有关更多信息，请参阅配置流日志设置。

使用控制台配置流日志设置

1. 对于 Destination（目的地），选择 Send to an S3 bucket（发送到 S3 存储桶）。
2. 对于 S3 存储桶 ARN，请指定现有 Amazon S3 存储桶的亚马逊资源名称 (ARN)。您可以选择包含子文件夹。例如，要在名为的存储桶`my-logs`中指定一个名为的子文件夹`my-bucket`，请使用以下命令：ARN

```
arn:aws::s3:::my-bucket/my-logs/
```

存储桶不能使用 AWSLogs 作为子文件夹名称，因为这是保留项。

如果您拥有该存储桶，我们会自动创建资源策略并将它附加到该存储桶。有关更多信息，请参阅针对流日志的 Amazon S3 存储桶权限。

3. 对于 Log record format（日志记录格式），选定流日志记录的格式。
   - 要使用默认流日志记录格式，请选择 AWS default format（亚马逊云科技默认格式）。
   - 要创建自定义格式，请选择Custom format（自定义格式）。对于Log format（日志行格式），选择要包括在流日志记录中的字段。
4. 对于 Log file format（日志文件格式），指定日志文件的格式。
   - Text – 纯文本。这是默认格式。
   - Parquet – Apache Pparquet 是一种列式数据格式。与对纯文本数据的查询相比，对 Passic 格式的数据进行查询速度快 10 到 100 倍。使用 Gzip 压缩的 Parquet 格式的数据比 Gzip 压缩的纯文本格式的数据占用的存储空间少 20%。
5. （可选）要使用 Hive 兼容的 S3 前缀，请选择 Hive-compatible S3 prefix（Hive 兼容的 S3 前缀）、Enable（启用）。
6. （可选）要每小时对流日志进行分区，请选择 Every 1 hour（60 mins）（每 1 小时（60 分钟））。
7. （可选）要向流日志添加标签，请选择 Add new tag（添加新标签）并指定标签键和值。
8. 选择 Create flow log（创建流日志）。

使用命令行工具创建发布到 Amazon S3 的流日志

使用以下命令之一。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs（亚马逊EC2查询API）

以下 AWS CLI 示例创建了一个流日志，用于捕获所有中转网关流量，VPCtgw-00112233344556677并将流日志传送到名为的 Amazon S3 存储桶flow-log-bucket。--log-format 参数指定流日志记录的自定义格式。

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

查看 Amazon S3 中的 Transit Gateway 流量日志记录

查看发布到 Amazon S3 的流日志记录

1. 在上打开 Amazon S3 控制台https://console.aws.amazon.com/s3/。
2. 对于 Bucket name（存储桶名称），选择流日志发布到的存储桶。
3. 在“名称”中，选中日志文件旁边的复选框。在对象概述面板上，选择 Download（下载）。

已处理 Amazon S3 中的流日志记录

日志文件是压缩文件。如果您使用 Amazon S3 控制台打开这些日志文件，则将对其进行解压缩，并且将显示流日志记录。如果您下载这些文件，则必须对其进行解压才能查看流日志记录。

Transit Gateway Flow 记录亚马逊数据 Firehose 中的记录

主题

- 用于跨账户传输的 IAM 角色
- 为 Amazon Data Firehose 创建 Transit Gateway Flow Logs 源账户角色
- 为 Amazon Data Firehose 创建 Transit Gateway Flow Logs 目标账户角色
- 创建发布到 Amazon Data Firehose 的 Transit Gateway 流日志记录

流日志可以将流日志数据直接发布到 Firehose。您可以选择将流日志发布到与资源监视器相同的帐户或不同的帐户。

先决条件

发布到 Firehose 时，流日志数据将以纯文本格式发布到 Firehose 传输流。您必须先创建一个 Firehose 传送流。有关创建传输流的步骤，请参阅《亚马逊数据 Firehose 开发者指南》中的创建亚马逊数据 Firehose 传输流。

定价

将收取标准摄取和传输费用。要了解更多信息，请打开 Amazon P CloudWatch ric ing，选择日志，然后找到销售日志。

用于跨账户传输的 IAM 角色

当您发布到 Kinesis Data Firehose 时，您可以选择与要监控的资源位于同一账户（源账户）或不同账户（目的地账户）中的传输流。要允许跨账号将流日志传输到 Firehose，您必须在源账户中创建一个IAM角色，在目标账户中创建一个IAM角色。

角色

- 源账户角色
- 目的地账户角色

源账户角色

在源账户中，创建授予以下权限的角色。在此示例中，角色的名称为 mySourceRole，但您也可以为该角色选择其他名称。最后一条语句允许目的地账户中的角色代入该角色。条件语句确保该角色仅传递给日志传输服务，并且仅在监控指定资源时传递。创建策略时，请使用条件键iam:AssociatedResourceARN指定要监控的网络接口或子网。VPCs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
              ]
          }
      }
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

确保该角色具有以下信任策略，允许日志传输服务代入该角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

目的地账户角色

在目标账户中，创建一个名称以开头的角色AWSLogDeliveryFirehoseCrossAccountRole。该角色必须授予以下权限。

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

```
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

确保该角色具有以下信任策略，允许您在源账户中创建的角色代入该角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

为 Amazon Data Firehose 创建 Transit Gateway Flow Logs 源账户角色

从源账户中，在 AWS Identity and Access Management 控制台中创建源角色。

创建源账户角色

1. 登录 AWS Management Console 并打开IAM控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 选择创建策略。
4. 在创建策略页面上，执行以下操作：
   1. 选择JSON。
   2. 将此窗口的内容替换为此部分开头的权限策略。
   3. 选择 Next: Tags（下一步：标签）和 Next: Review（下一步：审核）。

4. 输入您策略的名称和可选描述，然后选择 Create policy（创建策略）。

5. 在导航窗格中，选择角色。

6. 选择 Create role（创建角色）。

7. 对于 Trusted entity type（可信实体类型），选择 Custom trust policy（自定义信任策略）。对于 Custom trust policy（自定义信任策略），将 `"Principal": {},` 替换为以下内容，以指定日志传输服务。选择下一步。

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. 在 Add permissions（添加权限）页面上，选中您在此过程中先前创建的策略复选框，然后选择 Next（下一步）。

9. 输入您的角色的名称，并且可以选择提供描述。

10. 选择Create role（创建角色）。

为 Amazon Data Firehose 创建 Transit Gateway Flow Logs 目标账户角色

在目标账户中，在 AWS Identity and Access Management 控制台中创建目标角色。

创建目的地账户角色

1. 登录 AWS Management Console 并打开IAM控制台，网址为https://console.aws.amazon.com/iam/。

2. 在导航窗格中，选择策略。

3. 选择创建策略。

4. 在创建策略页面上，执行以下操作：

   1. 选择JSON。

   2. 将此窗口的内容替换为此部分开头的权限策略。

   3. 选择 Next: Tags（下一步：标签）和 Next: Review（下一步：审核）。

   4. 输入以开头的策略名称 AWSLogDeliveryFirehoseCrossAccountRole，然后选择创建策略。

5. 在导航窗格中，选择角色。

6. 选择 Create role（创建角色）。

7. 对于 Trusted entity type（可信实体类型），选择 Custom trust policy（自定义信任策略）。对于 Custom trust policy（自定义信任策略），将 `"Principal": {},` 替换为以下内容，以指定日志传输服务。选择下一步。

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. 在 Add permissions（添加权限）页面上，选中您在此过程中先前创建的策略复选框，然后选择 Next（下一步）。
9. 输入您的角色的名称，并且可以选择提供描述。
10. 选择Create role（创建角色）。

创建发布到 Amazon Data Firehose 的 Transit Gateway 流日志记录

使用控制台创建发布到 Firehose 的传输网关流日志

1. 打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）或 Transit gateway attachments（中转网关连接）。
3. 选中一个或多个中转网关或中转网关连接复选框。
4. 选择 Actions（操作）、Create flow log（创建流日志）。
5. 在 Destination（目的地）中，选择 Send to a Firehose Delivery System（发送到 Firehose 传输系统）。
6. 对于 Firehose Deliv ery ARN StreamARN，请选择您创建的要在其中发布流日志的。
7. 对于 Log record format（日志记录格式），选定流日志记录的格式。
   - 要使用默认流日志记录格式，请选择 AWS default format（亚马逊云科技默认格式）。
   - 要创建自定义格式，请选择Custom format（自定义格式）。对于Log format（日志行格式），选择要包括在流日志记录中的字段。
8. （可选）要向流日志添加标签，请选择 Add new tag（添加新标签）并指定标签键和值。
9. 选择 Create flow log（创建流日志）。

使用命令行工具创建发布到 Firehose 的流日志

使用以下命令之一：

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs（亚马逊EC2查询API）

以下 AWS CLI示例创建了一个流日志，用于捕获传输网关信息并将流日志传送到指定的 Firehose 传输流。

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

以下 AWS CLI示例创建了一个流日志，用于捕获公交网关信息，并将流日志传送到与源账户不同的Firehose传输流。

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
  --resource-ids gw-1a2b3c4d \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

创建 Amazon VPC 公交网关流日志

您可以为传输网关创建流日志，以便将数据发布到日 CloudWatch 志、Amazon S3 或 Amazon Data Firehose

有关更多信息，请参阅下列内容：

- 创建发布到 Transit Gateways 流日志记录 Amazon CloudWatch Logs
- 创建发布到 Amazon S3 的 Transit Gateway 流日志记录
- 创建发布到 Amazon Data Firehose 的 Transit Gateway 流日志记录

使用APIs或创建和管理 Amazon VPC Transit Gateways 流日志 CLI

您可以使用API或命令行执行本页上描述的任务。

使用CreateFlowLogsAPI或时有以下限制 create-flow-logsCLI：

- --resource-ids 最多可含有 25 个 TransitGateway 或 TransitGatewayAttachment 资源类型。
- --traffic-type 默认情况下不是必填字段。如果您在中转网关资源类型上使用此字段，会返回错误。此限制仅适用于中转网关资源类型。
- --max-aggregation-interval 具有默认值 60，这是中转网关资源类型的唯一可用值。如果您尝试传递任何其他值，则会返回错误。此限制仅适用于中转网关资源类型。
- --resource-type 支持两个新资源类型，TransitGateway 和 TransitGatewayAttachment。
- 如果您未设置要包含的字段，则 --log-format 会包含中转网关资源类型的所有日志字段。这仅适用于中转网关资源类型。

创建流日志

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowLogs（亚马逊EC2查询API）

描述您的流日志

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs（亚马逊EC2查询API）

查看您的流日志记录（日志事件）

- get-log-events (AWS CLI)
- 获取-CWLLogEvent (AWS Tools for Windows PowerShell)
- GetLogEvents (CloudWatch API)

删除流日志

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs（亚马逊EC2查询API）

查看 Amazon VPC 公交网关流日志记录

通过 Amazon 查看有关您的中转网关流量日志的信息VPC。选择资源时，会列出该资源的所有流日志。显示的信息包括流日志的 ID、流日志配置以及有关流日志的状态的信息。

查看中转网关流日志的相关信息

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）或 Transit gateway attachments（中转网关连接）。
3. 选择中转网关或中转网关连接，然后选择 Flow Logs（流日志）。此时有关流日志的信息将显示在选项卡上。Destination type（目标类型） 列指示要将流日志发布到的目标。

管理 Amazon VPC 公交网关流日志标签

您可以在 Amazon EC2 和 Amazon VPC 控制台中为流日志添加或删除标签。

为中转网关流日志添加或删除标签

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）或 Transit gateway attachments（中转网关连接）。
3. 选择中转网关或中转网关连接。
4. 对于所需的流日志选择 Manage tags（管理标签）。
5. 要添加新标签，请选择 Create Tag（创建标签）。要删除标签，请选择删除按钮（x）。
6. 选择 Save（保存）。

搜索 Amazon VPC 公交网关流量日志记录

您可以使用日志控制台搜索发布到 CloudWatch 日志的流 CloudWatch 日志记录。您可以使用度量筛选器筛选流日志记录。流日志记录用空格分隔。

使用日志控制台搜索流 CloudWatch 日志记录

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Logs（日志），然后选择 Log groups（日志组）。
3. 选择包含您的流日志的日志组。此时将显示每个中转网关的日志流的列表。
4. 如果您知道要搜索的中转网关，则选择单个日志流。或者，选择 Search Log Group（搜索日志组）以搜索整个日志组。如果日志组中有许多中转网关，则这可能需要一些时间，所需时间也取决于您选择的时间范围。
5. 对于 Filter events（筛选事件），请输入以下字符串。这假定流日志记录使用默认格式。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. 通过为字段指定值，根据需要修改筛选器。以下示例按特定的源 IP 地址进行筛选。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
```

```
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

以下示例将按中转网关 ID tgw-123abc456bca、目标端口和字节数进行筛选。

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

删除 Amazon VPC 公交网关流日志记录

您可以使用 Amazon VPC 控制台删除传输网关流日志。

使用这些过程可以禁用资源的流日志服务。删除流日志不会删除日志中的现有日志流，也不会删除 CloudWatch Amazon S3 中的日志文件。必须使用相应服务的控制台来删除现有流日志数据。此外，删除发布到 Amazon S3 的流日志不会删除存储桶策略和日志文件访问控制列表 (ACLs)。

删除中转网关流日志

1. 打开亚马逊VPC控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Transit gateways（中转网关）。
3. 选择一个 Transit gateway ID（中转网关 ID）。
4. 在流日志部分中，选择要删除的流日志。
5. 选择 Actions（操作），然后选择 Delete flow logs（删除流日志）。
6. 选择 Delete（删除）确认您要删除流日志。

使用 Amazon 公交网关监控VPC公交网关

您可以使用以下功能监控中转网关、分析流量模式以及排查中转网关的问题。

CloudWatch 指标

您可以使用 Amazon CloudWatch 以一组有序的时间序列数据（称为指标）的形式检索有关公交网关数据点的统计数据。您可使用这些指标来验证您的系统是否按预期运行。有关更多信息，请参阅 CloudWatch Amazon VPC 公交网关中的指标。

中转网关流日志

您可以使用中转网关流日志来获取中转网关上的网络流量的详细信息。有关更多信息，请参阅 中转网关流日志。

VPC 流日志

您可以使用 VPC Flow Logs 来捕获与您的中转网关VPCs相连的进出流量的详细信息。有关更多信息，请参阅 Amazon VPC 用户指南中的VPC流日志。

CloudTrail 日志

您可以使用捕获有关 AWS CloudTrail 向公交网关API发出的呼叫的详细信息，并将其作为日志文件存储在 Amazon S3 中。您可以使用这些 CloudTrail 日志来确定拨打了哪些呼叫、呼叫来自哪个源 IP 地址、谁拨打了电话、何时拨打了呼叫等。有关更多信息，请参阅 Amazon VPC 公交网关API呼吁 AWS CloudTrail。

CloudWatch 使用网络管理器的事件

您可以使用 AWS Network Manager 将事件转发到目标函数或流 CloudWatch，然后将这些事件路由到目标函数或流。网络管理器会生成拓扑更改、路由更新和状态更新的事件，所有这些事件都可用于提醒您注意中转网关的变化。有关更多信息，请参阅 T ransit Gateways AWS 全球网络用户指南中的使用 CloudWatch 事件监控您的全球网络。

CloudWatch Amazon VPC 公交网关中的指标

亚马逊将您的公交网关和公交网关附件的数据点VPC发布到亚马 CloudWatch 逊。 CloudWatch允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。每个数据点都有关联的时间戳和可选的测量单位。

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

Amazon 以 60 秒的 CloudWatch 间隔VPC测量并发送其指标。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

中转网关指标

AWS/TransitGateway 命名空间包括以下指标。

始终报告所有指标。它们的值取决于通过公交网关的流量。中转网关的指标维度有关支持的尺寸，请参阅。

指标	描述
BytesDropCountBlackhole	由于与 blackhole 路由匹配而被丢弃的字节数量。 统计数据：唯一有意义的统计数据是 Sum。
BytesDropCountNoRoute	由于与路由不匹配而被丢弃的字节数量。 统计数据：唯一有意义的统计数据是 Sum。
BytesIn	中转网关接收的字节数。 统计数据：唯一有意义的统计数据是 Sum。
BytesOut	从中转网关发送的字节数。 统计数据：唯一有意义的统计数据是 Sum。
PacketsIn	中转网关接收的数据包数。 统计数据：唯一有意义的统计数据是 Sum。
PacketsOut	中转网关发送的数据包数。 统计数据：唯一有意义的统计数据是 Sum。

指标	描述
PacketDropCountBlackhole	由于与 blackhole 路由匹配而被丢弃的数据包的数量。 统计数据：唯一有意义的统计数据是 Sum。
PacketDropCountNoRoute	由于与路由不匹配而被丢弃的数据包的数量。 统计数据：唯一有意义的统计数据是 Sum。

连接级指标

以下指标适用于中转网关连接。所有挂载指标都发布到中转网关拥有者的账户。单个连接指标也会发布到挂载所有者的账户。挂载所有者只能查看其自己挂载的指标。有关支持的附件类型的更多信息，请参阅 the section called “资源连接”。

始终报告所有指标。它们的值取决于进出公交网关附件的流量。中转网关的指标维度有关支持的尺寸，请参阅。

指标	描述
BytesDropCountBlackhole	由于与中转网关连接上的 blackhole 路由匹配而被丢弃的字节数量。 统计数据：唯一有意义的统计数据是 Sum。
BytesDropCountNoRoute	由于与中转网关连接上的路由不匹配而被丢弃的字节数量。 统计数据：唯一有意义的统计数据是 Sum。
BytesIn	中转网关从挂载接收的字节数。 统计数据：唯一有意义的统计数据是 Sum。
BytesOut	从中转网关发送到挂载的字节数。 统计数据：唯一有意义的统计数据是 Sum。
PacketsIn	中转网关从挂载接收的数据包数。

指标	描述
	统计数据：唯一有意义的统计数据是 Sum。
PacketsOut	中转网关向挂载发送的数据包数。 统计数据：唯一有意义的统计数据是 Sum。
PacketDropCountBlackhole	由于与中转网关连接上的 blackhole 路由匹配而被丢弃的数据包数。 统计数据：唯一有意义的统计数据是 Sum。
PacketDropCountNoRoute	由于与中转网关连接上的路由不匹配而被丢弃的数据包数。 统计数据：唯一有意义的统计数据是 Sum。

中转网关的指标维度

要筛选中转网关的指标，请使用以下维度。

维度	描述
TransitGateway	按中转网关筛选指标数据。
TransitGatewayAttachment	通过 中转网关 挂载筛选指标数据。

Amazon VPC 公交网关API呼吁 AWS CloudTrail

AWS CloudTrail 是一项提供用户、角色或服务所执行操作记录的 AWS 服务。 CloudTrail 将所有公交网关API呼叫捕获为事件。捕获的呼叫包括来自的调用 AWS Management Console 和对公交网关API操作的代码调用。如果您创建跟踪，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括传输网关的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向传输网关发出了什么请求API、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关公交网关的更多信息APIs，请参阅《亚马逊EC2API参考》中的 AWS Transit Gateway 操作。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

中的公交网关信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当活动通过公交网关发生时API，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括公交网关的事件API，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的以下内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为以下各项配置亚马逊SNS通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有对公交网关操作的呼叫都由记录 CloudTrail。例如，对`CreateTransitGateway`操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根凭证还是 AWS Identity and Access Management 用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅CloudTrail userIdentity 元素。

了解中转网关日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共API调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

日志文件包括您 AWS 账户的所有API呼叫的事件，而不仅仅是公交网关API呼叫。您可以API通过检查值为的eventSource元素来定位对公交网关的呼叫ec2.amazonaws.com。要查看特定操作（如 CreateTransitGateway）的记录，请检查是否有具有操作名称的 eventName 元素。

以下是使用控制台创建传输网关API的用户的公交网关 CloudTrail 日志记录示例。您可以使用 userAgent 元素标识控制台。您可以使用eventName元素识别请求的API呼叫。有关用户（Alice）的信息可在 userIdentity 元素中找到。

Example 示例： CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
```

```
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Amazon VPC 公交网关中的身份和访问管理

AWS 使用安全证书来识别您的身份并授予您访问 AWS 资源的权限。您可以使用 AWS Identity and Access Management (IAM) 的功能允许其他用户、服务和应用程序完全或以有限的方式使用您的 AWS 资源，而无需共享您的安全证书。

默认情况下，IAM用户无权创建、查看或修改 AWS 资源。要允许用户访问公交网关等资源并执行任务，您必须创建一个IAM策略，授予用户使用他们所需的特定资源和API操作的权限，然后将该策略附加到该用户所属的群组。在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。

要使用公交网关，以下 AWS 托管策略之一可能会满足您的需求：

- Amazon EC2FullAccess
- Amazon EC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

管理中转网关的策略示例

以下是使用中转网关的IAM策略示例。

创建具有所需标记的中转网关

以下示例允许用户创建中转网关。aws:RequestTag 条件键要求用户使用标签 stack=prod 标记中转网关。aws:TagKeys 条件键使用 ForAllValues 修饰符指示只允许在请求中使用键 stack（不能指定任何其他标签）。如果用户在创建中转网关时未传递此特定标签，或者不指定标签，请求将失败。

第二个语句使用 ec2:CreateAction 条件键使用户只能在 CreateTransitGateway 上下文中创建标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
```

```
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

使用中转网关路由表

以下示例允许用户仅为特定中转网关 (tgw-11223344556677889) 创建和删除中转网关路由表。用户还可以在任何中转网关路由表中创建和替换路由，但仅针对具有标签 network=new-york-office 的连接。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

在 Amazon Transit Gateways 中使用服务相关角色作为中VPC转

Amazon VPC 使用服务相关角色来获得代表您调用其他 AWS 服务所需的权限。有关更多信息，请参阅《IAM用户指南》中的使用服务相关角色。

中转网关服务相关角色

当您VPC使用公交网关时，Amazon 使用 AWS 服务相关角色来获得代表您调用其他服务所需的权限。

服务相关角色授予的权限

当您VPC使用公交网关时 AWSServiceRoleForVPCTransitGateway，Amazon 使用名为的服务相关角色代表您调用以下操作：

- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:ModifyNetworkInterfaceAttribute
- ec2:DeleteNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:AssignIpv6Addresses
- ec2:UnAssignIpv6Addresses

该AWSServiceRoleForVPCTransitGateway角色信任以下服务来代替该角色：

- transitgateway.amazonaws.com

AWSServiceRoleForVPCTransitGateway使用托管策略AWSVPCTransitGatewayServiceRolePolicy。

必须配置权限以允许实IAM体（例如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM用户指南》中的服务相关角色权限。

创建服务相关角色

您无需手动创建AWSServiceRoleForVPCTransitGateway角色。当您将账户VPC中的关联到公交网关时，Amazon 会为您VPC创建此角色。

VPC要让 Amazon 代表您创建服务相关角色，您必须拥有所需的权限。有关更多信息，请参阅《IAM用户指南》中的服务相关角色权限。

编辑服务相关角色

您可以编辑AWSServiceRoleForVPCTransitGateway使用的描述IAM。有关更多信息，请参阅《IAM用户指南》中的编辑服务相关角色。

删除服务相关角色

如果您不再需要使用中转网关，我们建议您将其删除AWSServiceRoleForVPCTransitGateway。

只有在删除 AWS 账户中的所有公交网关VPC附件后，才能删除此服务相关角色。这样可以确保您不会无意中删除访问附件的权限。VPC

您可以使用IAM控制台IAMCLI、或删除服务相关角色。IAM API有关更多信息，请参阅《IAM用户指南》中的删除服务相关角色。

删除后 AWSServiceRoleForVPCTransitGateway，如果您将账户VPC中的角色附加到公交网关，Amazon VPC 会再次创建该角色。

AWS Amazon VPC 公交网关中转网关的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户托管式策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 当新服务启动或现有服务 AWS 服务 有新API操作可用时，最有可能更新 AWS 托管策略。

有关更多信息，请参阅《IAM用户指南》中的AWS 托管策略。

要使用公交网关，以下 AWS 托管策略之一可能会满足您的需求：

- Amazon EC2FullAccess
- Amazon EC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS 托管策略： AWSVPCTransitGatewayServiceRolePolicy

该策略已附加到该角色AWSServiceRoleForVPCTransitGateway。这样VPC，Amazon 就可以为您的公交网关附件创建和管理资源。

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSVPCTransitGatewayServiceRolePolicy中的。

AWS 托管策略的公交网关更新

查看自 Amazon 于 2021 年 3 月VPC开始跟踪公交网关 AWS 托管政策变更以来这些更新的详细信息。

更改	描述	日期
亚马逊VPC开始追踪变更	亚马逊VPC开始跟踪其 AWS 托管政策的变更。	2021 年 3 月 1 日

Amazon 公交网关中的中VPC转网关网络 ACLs

网络访问控制列表 (NACL) 是可选的安全层。

网络访问控制列表 (NACL) 规则的应用方式不同，具体视情况而定：

- the section called “EC2实例和传输网关关联的子网相同”
- the section called “EC2实例和传输网关关联的子网不同”

EC2实例和传输网关关联的子网相同

考虑一个配置，其中EC2实例和传输网关关联位于同一个子网中。从实例到传输网关的流量以及从中转网关到EC2实例的流量都使用相同的网络ACL。

NACL对于从实例到传输网关的流量，规则如下所示：

- 出站规则使用目标 IP 地址进行评估。
- 入站规则使用源 IP 地址进行评估。

NACL规则适用于从传输网关到实例的流量，如下所示：

- 不评估出站规则。
- 不评估入站规则。

EC2实例和传输网关关联的子网不同

考虑一种配置，其中EC2实例位于一个子网中，传输网关关联位于不同的子网中，并且每个子网都与不同的网络关联ACL。

EC2实例子网的网络ACL规则如下所示：

- 出站规则使用目标 IP 地址来评估从实例指向中转网关的流量。

- 入站规则使用源 IP 地址来评估从中转网关指向实例的流量。

NACL中转网关子网的规则如下所示：

- 出站规则使用目标 IP 地址来评估从中转网关指向实例的流量。
- 出站规则不用来评估从实例指向中转网关的流量。
- 入站规则使用源 IP 地址来评估从实例指向中转网关的流量。
- 入站规则不用来评估从中转网关指向实例的流量。

最佳实践

为每个传输网关VPC连接使用单独的子网。对于每个子网，请使用较小的子网CIDR，例如 /28，这样您就可以拥有更多的EC2资源地址。当您使用单独的子网时，您可以配置以下内容：

- 保持与中转网关子网关联的入站和出站NACL处于打开状态。
- 根据您的流量，您可以应用NACLs于您的工作负载子网。

有关VPC附件工作原理的更多信息，请参阅the section called “资源连接”。

Amazon VPC 公交网关配额

您 AWS 账户 具有以下与中转网关相关的配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。

服务限额控制台提供有关您的账户限额的信息。您可以使用服务限额控制台查看默认限额，并对可调整的限额请求增加限额。有关更多信息，请参阅 Service Quotas 用户指南中的请求增加服务限额。

如果 Service Quotas 中尚未提供可调节的配额，则可以打开支持案例。

常规

名称	默认值	可调整
每个账户的中转网关	5	是
CIDR每个公交网关的区块数	5	否

该the section called “Connect 挂载和 Connect 对等节点”功能中使用了这些CIDR方块。

路由

名称	默认值	可调整
每个中转网关的中转网关路由表	20	是
单个中转网关在所有路由表中的组合路由（动态和静态）总数	10000	是
从虚拟路由器设备发布到 Connect 对等节点的动态路由	1000	是
从中转网关上的 Connect 对等节点发布到虚拟路由器设备的路由	5000	否
单个挂载的前缀的静态路由	1	否

发布的路由来自与 Connect 挂载关联的路由表。

中转网关挂载

一个中转网关不能有多个与同一个网关的VPC连接VPC。

名称	默认值	可调整
每个中转网关的挂载	5000	否
每个公交网关 VPC	5	否
每个中转网关的对等连接挂载	50	是
每个 中转网关 的待处理待对等连接数	10	是
在两个传输网关之间或一个传输网关与云WAN核心网络边缘之间建立对等连接 () CNE	1	否
每个 Connect 连接连接对等体（GRE隧道）	4	否

带宽

有许多因素会影响通过站点到站点VPN连接实现的带宽，包括但不限于：数据包大小、流量组合 (TCP/UDP)、中间网络上的整形或限制策略、互联网天气以及特定的应用程序要求。对于VPC附件、 AWS Direct Connect 网关或对等传输网关附件，我们将尝试提供超出默认值的额外带宽。

名称	默认值	可调整
每个可用区域的每个VPC附件的带宽	最高 100 Gbps	如需进一步帮助，请联系您的解决方案架构师 (SATAM) 或技术客户经理 ()。
每个可用区每个传输网关VPC连接的每秒数据包数	最高 7,500,000	如需进一步帮助，请联系您的解决方案架构师 (SATAM) 或技术客户经理 ()。

名称	默认值	可调整
该区域中每个可用区域的网 AWS Direct Connect 关或对等传输网关连接的带宽	最高 100 Gbps	如需进一步帮助，请联系您的解决方案架构师 (SATAM) 或技术客户经理 ()。
该地区每个可用可用区每个传输网关附件（AWS Direct Connect 和对等连接附件）的每秒数据包数	最高 7,500,000	如需进一步帮助，请联系您的解决方案架构师 (SATAM) 或技术客户经理 ()。
每VPN条隧道的最大带宽	最高 1.25 Gbps	否
每VPN条隧道每秒的最大数据包数	最高 14 万	否
每个 Connect 连接的每个 Connect 对等体（GRE隧道）的最大带宽	最高 5 Gbps	否
每个 Connect 对等连接每秒的最大数据包数量	最高 30 万	否

您可以使用等价多路径路由 (ECMP) 通过聚合多条隧道来获得更高的VPN带宽。VPN要使用ECMP，必须将VPN连接配置为动态路由。ECMP使用静态路由的VPN连接不支持。

只要底层传输（VPC或）附件支持所需的带宽，您最多可以为每个 Connect 连接创建 4 个 Connect 对等体（每个 Connect 连接的总带宽最高可达 20 Gbps AWS Direct Connect）。您可以使用横ECMP向扩展同一 Connect 连接的多个 Connect 对等体或同一传输网关上的多个 Connect 附件来获得更高的带宽。传输网关不能在同一 Connect 对BGP等体的对等体ECMP之间使用。

AWS Direct Connect 网关

名称	默认值	可调整
AWS Direct Connect 每个中转网关的网关	20	否
每个网关的中转 AWS Direct Connect 网关	6	否

最大传输单位 (MTU)

- 网络连接是指可通过该连接传递的最大允许数据包的大小（以字节为单位）。MTU连接越MTU大，单个数据包中可以传递的数据就越多。传输网关支持VPCs、 AWS Direct Connect、Transi MTU t Gateway Connect 和对等连接附件（区域内、区域间和云WAN对等连接附件）之间的流量 8500 字节。通过VPN连接传输MTU的流量可以有 1500 字节。
- 从对等互VPC连迁移到使用传输网关时，对VPC等网关和传输网关之间的MTU大小不匹配可能会导致一些非对称流量数据包丢失。VPCs同时更新两者，以避免由于大小不匹配而丢弃巨型数据包。
- 到达中转网关的大小超过 8500 字节的数据包将被丢弃。
- 传输网关不会为数据包生成 FRAG _，也不会NEEDED为ICMPv4数据包生成 Packet Too Big (PTB)。ICMPv6因此，不支持路径MTU发现 (PMTUD)。
- 传输网关对所有数据包强制执行最大分段大小 (MSS) 限制。有关更多信息，请参阅RFC879。
- 有关站点到站点VPN配额的详细信息MTU，请参阅《AWS Site-to-Site VPN 用户指南》中的最大传输单位 (MTU)。

多播

名称	默认值	可调整
每个中转网关的多播域	20	是
每个中转网关的多播网界面	10000	是
每个组播域关联 VPC	20	是
每个中转网关多播组的源数量	1	是
每个传输网关的静态和IGMPv2多播组成员和源	10000	否
每个传输网关IGMPv2组播组的静态和多播组成员	100	否
每个流的最大多播吞吐量	1Gbps	否
每个可用区的最大聚合多播吞吐量	20 Gbps	否

AWS 网络管理器

名称	默认值	可调整
每人全球网络 AWS 账户	5	是
每个全球网络的设备	200	是
每个全球网络的链接	200	是
每个全球网络的站点	200	是
每个全球网络的连接	500	否

其他配额资源

有关更多信息，请参阅下列内容：

- 《用户指南》AWS Site-to-Site VPN 中的@@ 站点到站点VPN配额
- 《亚马逊VPC用户指南》中的亚马逊VPC配额
- AWS Direct Connect 用户指南中的 AWS Direct Connect 配额

中转网关的文档历史记录

下表介绍中转网关的版本。

变更	说明	日期
AWS Transit Gatewa	增加了带宽限制。	2023 年 8 月 14 日
AWS Transit Gateway 流	中转网关现在支持流日志，允许您监控和记录中转网关之间的网络流量。	2022 年 7 月 14 日
中转网关策略表	使用策略表为中转网关设置动态路由，以便与对等类型的中转网关自动交换路由和可达性信息。	2022 年 7 月 13 日
Network Manager 用户指南	Network Manager 的指南已单独创建，不再包含在《AWS 中转网关 用户指南》中。	2021 年 12 月 2 日
对等挂载	您可以与同一区域内的中转网关创建对等连接。	2021 年 12 月 1 日
中转网关 Connect	您可以在中转网关和中运行的第三方虚拟设备之间建立连接VPC。	2020 年 12 月 10 日
设备模式	您可以在连接上启用设备模式，以确保该VPC连接的双向流量流经同一个可用区。	2020 年 10 月 29 日
前缀列表引用	您可以在中转网关路由表中引用前缀列表。	2020 年 8 月 24 日
修改中转网关	您可以修改中转网关的配置选项。	2020 年 8 月 24 日

CloudWatch 公交网关附件的指标	您可以查看单个公交网关附件的 CloudWatch 指标。	2020 年 7 月 6 日
Network Manager 路由分析器	您可以分析全球网络中的中转网关路由表中的路由。	2020 年 5 月 4 日
对等挂载	您可以与其他区域内的中转网关创建对等连接。	2019 年 12 月 3 日
多播支持	Transit Gateway 支持在所连接的子网之间路由多播流量，VPCs并可用作发送到多个接收实例的流量的实例的多播路由器。	2019 年 12 月 3 日
AWS 网络管理器	您可以可视化和监控围绕中转网关构建的全球网络。	2019 年 12 月 3 日
AWS Direct Connect 支持	您可以使用 AWS Direct Connect 网关通过中转虚拟接口将您的 AWS Direct Connect 连接连接到传输网关VPCs或VPNs连接到您的传输网关。	2019 年 3 月 27 日
初始版本	此版本引入了中转网关。	2018 年 11 月 26 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。