AWS Transit Gate

Amazon VPC

Amazon VPC: AWS Transit Gate

Table of Contents

什么是 Amazon VPC Transit Gateway？

Amazon VPC Transit 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。

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
  - 与中转网关的 VPN 连接
  - 网络功能附件。有关更多信息，请参阅 the section called “网络功能附件”。
- 中转网关最大传输单位 (MTU) — 网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小（以字节为单位）。连接的 MTU 越大，可在单个数据包中传递的数据越多。传输网关支持 VPCs、 AWS Direct Connect、Transit Gateway Connect 和对等连接（区域内、区域间和云广域网对等连接附件）之间的 MTU 为 8500 字节。VPN 连接上的流量可以具有的 MTU 为 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 — VPC、VPN 连接或 Direct Connect 网关可以动态地将路由传播到中转网关路由表。默认情况下，使用 Connect 挂载，路由会传播到中转网关路由表。使用 VPC 时，您必须创建静态路由以将流量发送到中转网关。使用 VPN 连接时，路由使用边界网关协议 (BGP) 从中转网关传播到本地路由器。使用 Direct Connect 网关时，允许的前缀使用 BGP 溯源至本地路由器。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
- 中转网关入门
- 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 VPC 在内的各种 AWS 服务提供命令，并在 Windows、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 请求调用的低级别 API 操作。使用查询 API 是用于访问 Amazon VPC 的最直接方式，但需要您的应用程序处理低级别详细信息，例如生成哈希值以签署请求以及处理错误。有关更多信息，请参阅 Amazon EC2 API 参考。

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。

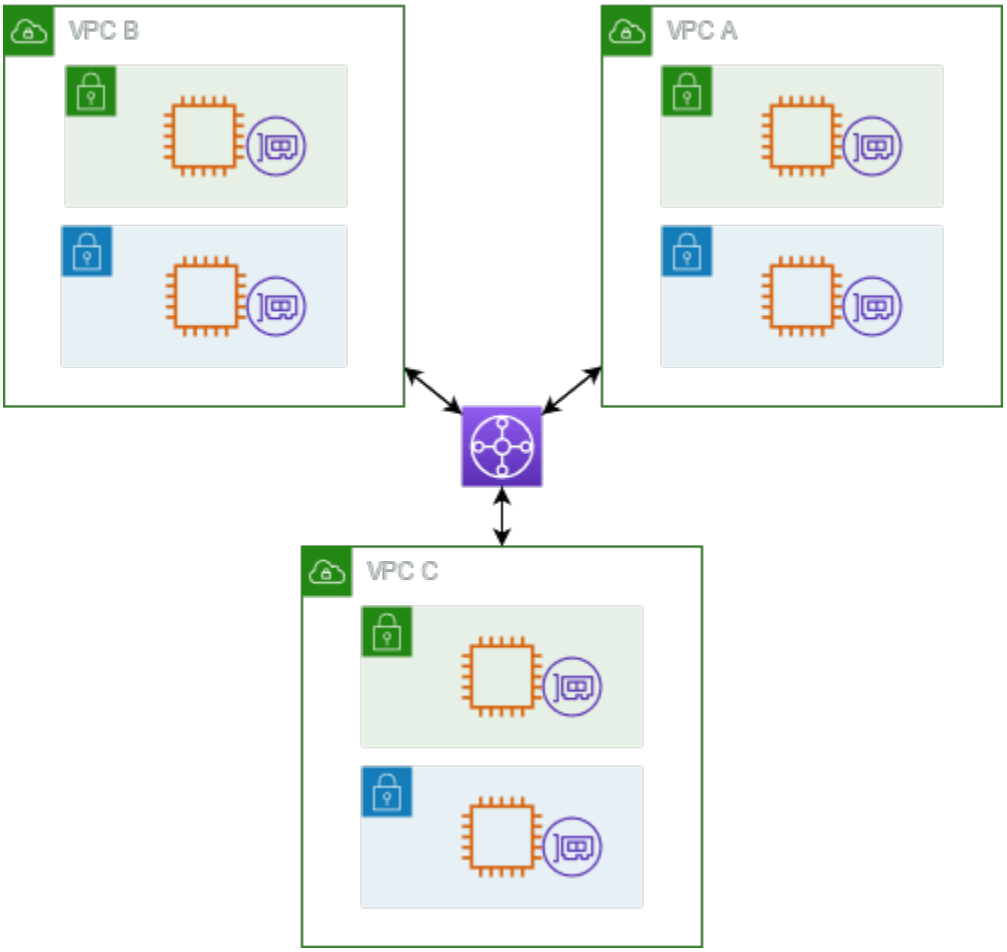
Amazon VPC Transit Gateways 的工作原理

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连接。

主题

示例架构图

下图显示了一个具有三个 VPC 连接的中转网关。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。



以下是上图中所示连接的原定设置中转网关路由表示例。每个 VPC 的 CIDR 块都将传播到该路由表。从而让每个连接都可以将数据包路由到另外两个连接。

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 子网中部署弹性网络接口，然后传输网关使用该接口来路由往返所选子网的流量。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。在创建连接期间，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连接时，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 连接
- 一个或多个中转网关对等连接

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 连接，您可以在创建或修改中转网关时使用控制台启用或禁用 ECMP 支持。对于所有其他连接类型，以下 ECMP 限制适用：

- VPC - VPC 不支持 ECMP，因为 CIDR 块不能重叠。例如，您不能将 CIDR 为 10.1.0.0/16 的 VPC 与使用相同 CIDR 的另一个 VPC 连接到中转网关，然后设置路由以对它们之间的流量进行负载均衡。
- VPN - 禁用 VPN ECMP support（VPN ECMP 支持）选项后，当多条路径的前缀相等时，中转网关会使用内部指标来确定首选路径。有关为 VPN 连接启用或禁用 ECMP 的更多信息，请参阅 the section called “中转网关”。
- AWS Transit Gateway Connec AWS Transit Gateway t-Connect 附件自动支持 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跨多个 Direct Connect 网关连接的 ECMP。
- 中转网关对等 - 中转网关对等不支持 ECMP，因为它既不支持动态路由，也不能针对两个不同的目标配置相同的静态路由。

> **Note**
>
> - 不支持 BGP Multipath as-Path Relax，因此您不能在不同的自治系统编号上使用 ECMP（ ）。ASNs
> - 不同连接类型之间不支持 ECMP。例如，您无法在 VPN 和 VPC 连接之间启用 ECMP。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 网关跨多个中转虚拟接口支持 ECMP。因此，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 AWS 从公共虚拟接口到的 Active/Active 或 Active/Passive Direct Connect 连接？ 。

可用区

当您将 VPC 连接到中转网关时，您必须启用要由中转网关使用的一个或多个可用区，以将流量路由到 VPC 子网中的资源。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。在启用可用区之后，流量可路由到 VPC 中的所有子网，而不只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 VPC 中配置有状态的网络设备，则可以为该设备所在的 VPC 连接启用设备模式支持。这可以确保在源和目标之间传输流量的生命周期内，中转网关为该 VPC 连接使用相同的可用区。它还允许中转网关将流量发送到 VPC 中的任何可用区，只要该区中存在子网关联。有关更多信息，请参阅示例：共享服务 VPC 中的设备。

路由

您的传输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。如果您同时禁用路由传播和路由表关联，则 AWS 不会为公交网关创建默认路由表。但是，如果启用了路由传播或路由表关联， AWS 则会创建默认路由表。

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。一个连接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 VPC 附加到中转网关时，您必须向子网路由表添加路由，以使流量通过中转网关进行路由。有关更多信息，请参阅《Amazon VPC 用户指南》中的 Transit Gateway 的路由。

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

每个连接都附带可以安装到一个或多个中转网关路由表的路由。当连接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 连接，VPC 的 CIDR 块将传播到中转网关路由表。

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

当动态路由与 VPN 连接一起使用时，路由表中与 VPN 连接关联的路由将通过 BGP 发布给客户网关。

对于 Connect 连接，与 Connect 连接关联的路由表中的路由会通过 BGP 向在 VPC 中运行的第三方虚拟设备（例如 SD-WAN 设备）公开。

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连接，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连接。路由到对等中转网关的流量随后可以路由到对等中转网关的 VPC 和 VPN 连接。

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。
- 如果路由的 CIDR 相同，但连接类型不同，则路由优先级如下所示：
  - 静态路由（例如， Site-to-SiteVPN 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 Connect 传播路由
  - Site-to-Site 通过私有直接连接传播的路由进行的 VPN
  - Site-to-Site VPN 传播的路由
  - 中转网关对等传播路由（Cloud WAN）

某些连接支持通过 BGP 的路由通告。如果路由的 CIDR 相同，连接类型也相同，则路由优先级受 BGP 属性控制：

- AS 路径长度更短
- MED 值更低
- 如果附件支持，则首选 eBGP 而不是 iBGP 路由

> **Important**
>
> - AWS 无法保证具有与上面列出的 CIDR、连接类型和 BGP 属性相同的 BGP 路由的路由优先顺序一致。
> - 对于通告到没有 MED 的公交网关的路由，T AWS ransit Gateway 将分配以下默认值：

- 0 表示在 Direct Connect 附件上通告的入站路由。
- 100 表示在 VPN 和 Connect 附件上通告的入站路由。

AWS Transit Gateway 仅显示首选路线。仅当不再通告之前的活动路由时，备用路由才会出现在中转网关路由表中，例如，如果您通过 Direct Connect 网关和 Site-to-Site 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。 Site-to-SiteVPN 作为备用路由，只有在不再通告 Direct Connect 网关时才会显示。

VPC 和中转网关路由表的差异

无论您使用的是 VPC 路由表还是中转网关路由表，路由表评估都会有所不同。

以下示例显示的是一张 VPC 路由表。VPC 本地路由具有最高的优先级，然后是最具体的路由。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

以下示例显示的是中转网关路由表。如果要选择 AWS Direct Connect 网关连接而不是 VPN 连接，则使用 BGP VPN 连接并传播中转网关路由表中的路由。

目的地	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

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

网络功能附件

网络功能附件是一种将网络安全功能（例如 AWS Network Firewall 附件）直接连接到您的传输网关的资源。它无需手动创建和管理检查 VPCs。

使用网络功能附件：

- AWS 自动创建和管理底层基础架构
- 当流量流经您的公交网关时，可以对其进行检查
- 在您的网络中始终如一地应用安全策略

- 您可以使用简单的路由规则引导流量通过防火墙
- 该附件可跨多个可用区使用，以实现高可用性

这种集成允许您将防火墙直接连接到传输网关，而不必创建复杂的路由配置并通过单独管理单独的终端节点，从而简化了网络安全。 VPCs

AWS Network Firewall 整合

AWS Network Firewall 集成允许您在服务管理的缓冲区 VPC 中以一组 Gateway Load Balancer 终端节点的形式连接防火墙，每个可用区一个。Network Firewall 连接是在自动启用设备模式的情况下创建的。这样就无需对检查进行明确管理 VPCs。

通过集成 Network Firewall，您不再需要 VPCs 为网络防火墙部署创建和管理检查。无需在创建防火墙时选择 VPC 和子网，而是直接选择 Transit Gateway，然后在幕后 AWS 自动配置和管理所有必要的资源。您将看到新的传输网关网络功能附件，而不是单个防火墙端点。

对于跨账户场景，Transit Gateway 可以从 Transit Gateway 所有者与 Network Firewall 所有者账户共享 RAM，从而允许任一账户管理防火墙附件。防火墙和附件准备就绪后，您只需修改 Transit Gateway 路由表，即可将流量发送到附件进行检查。

> **Note**
>
> - Transit Gateway 仅支持网络防火墙附件上的静态路由。
> - 不支持第三方防火墙。

有关防火墙和附件的更多信息，请参阅 T ransit 网关网络功能附件。

中转网关方案示例

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。

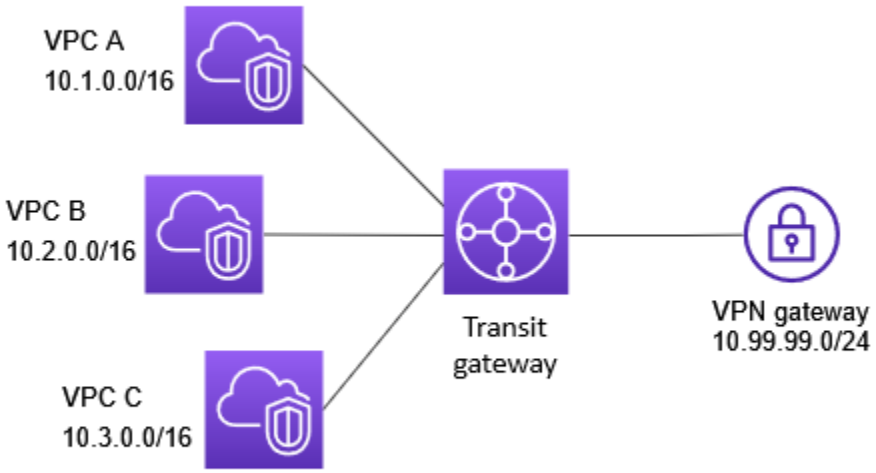
示例：集中式路由器

您可以将传输网关配置为连接所有 VPCs AWS Direct Connect、和 Site-to-Site 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，所有连接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

概览

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 连接和一个 Site-to-Site VPN 连接。来自 VPC A、VPC B 和 VPC C 并将其他 VPC 中的子网或 VPN 连接作为目的地的数据包，首先通过中转网关路由。



资源

为此场景创建以下资源：

- 三 VPCs。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 中转网关。有关更多信息，请参阅 the section called “创建中转网关”。
- 中转网关上有三个 VPC 连接。有关更多信息，请参阅 the section called “创建 VPC 连接”。
- 传输网关上的 Site-to-Site VPN 附件。每个 VPC 的 CIDR 块将传播到中转网关路由表。VPN 连接启动后，BGP 会话即建立， Site-to-SiteVPN CIDR 传播到传输网关路由表，VPC CIDRs 将添加到客户网关 BGP 表中。有关更多信息，请参阅 the section called “创建与 VPN 的中转网关连接”。

  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 VPC 具有一个路由表，并且中转网关具有一个路由表。

VPC 路由表

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

目的地	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 VPC CIDRs。

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

示例：隔离 VPCs

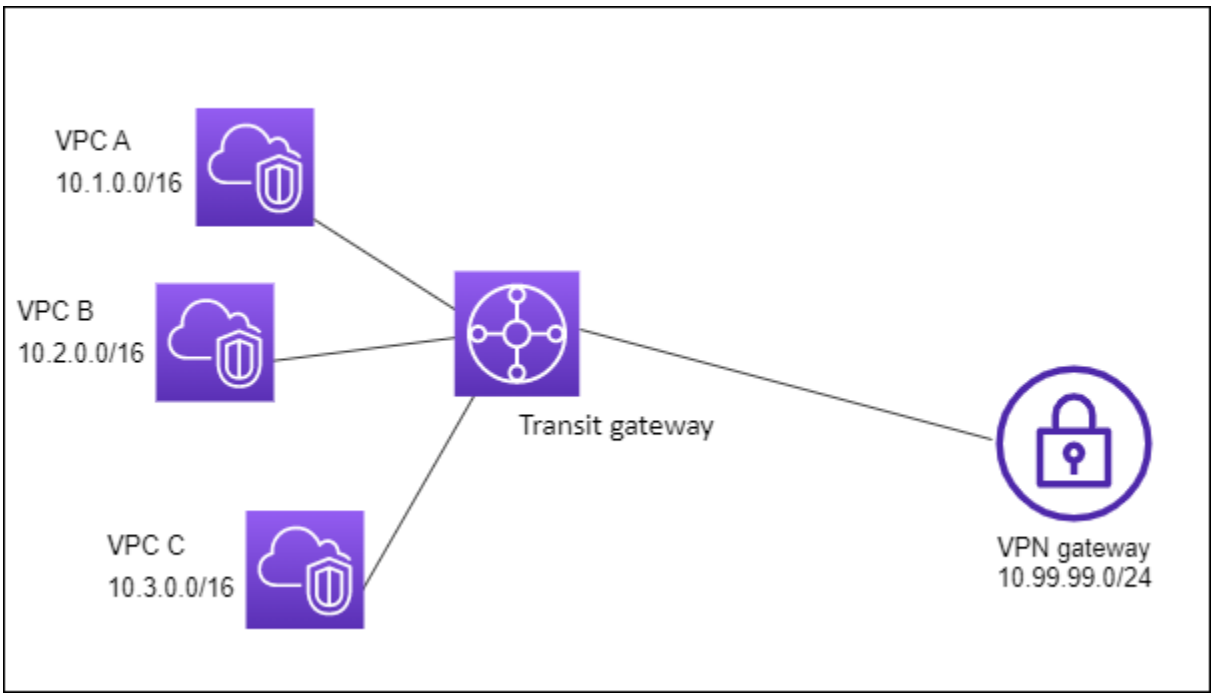
您可以将中转网关配置为多个隔离的路由器。这类似于使用多个中转网关，但在路由和连接可能更改的情况下可提供更大的灵活性。在此方案中，每个隔离的路由器都有单个路由表。所有与隔离的路由器关

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

概览

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 的数据包路由到中转网关。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进行路由，然后路由到 Site-to-Site VPN 连接（如果目标位于该网络内）。来自一个 VPC 并将另一个 VPC 中的子网作为目的地的数据包（例如从 10.1.0.0 到 10.2.0.0）通过中转网关进行路由，将在其中阻止这些数据包，因为在中转网关路由表中没有它们的路由。



资源

为此场景创建以下资源：

- 三 VPCs。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 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 连接”。
- 传输网关上的 Site-to-Site VPN 附件。有关更多信息，请参阅 the section called “创建与 VPN 的中转网关连接”。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，VPN CIDR 传播到传输网关路由表，VPC CIDRs 将添加到客户网关 BGP 表中。

路由

每个 VPC 都有一个路由表，传输网关有两个路由表，一个用于 VPN 连接。 VPCs

VPC A、VPC B 和 VPC C 路由表

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

目的地	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 VPN 连接 VPCs ，使用一个路由表进行 VPN 连接。

VPC 连接与以下路由表相关联，该路由表具有 VPN 连接的传播路由。

目的地	目标	路由类型
10.99.99.0/24	*Attachment for VPN connection*	传播

VPN 连接与以下路由表相关联，该路由表具有每个 VPC 连接的传播路由。

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

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 VPC 中转网关启用路由传播到中转网关路由表。

客户网关 BGP 表

客户网关 BGP 表包含以下 VPC CIDRs。

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

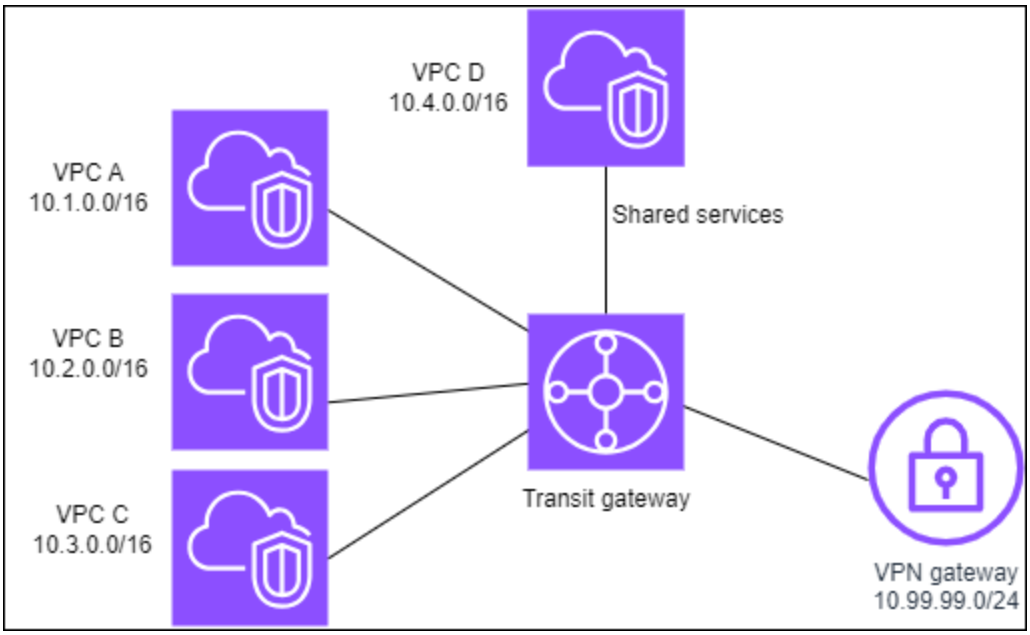
示例： VPCs 使用共享服务隔离

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，但在路由和连接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

概览

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 Site-to-Site VPN 的客户网关。如果数据包来自 VPC A、VPC B 或 VPC C 中的子网并以 VPC A、VPC B 或 VPC C 中的某个子网为目的地，则将通过中转网关进行路由，但由于中转网关路由表中没有这些子网的路由，因此将被阻止。来自 VPC A、VPC B 和 VPC C 并将 VPC D 作为目的地的数据包通过中转网关进行路由，然后路由到 VPC D。



资源

为此场景创建以下资源：

- 四 VPCs。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 中转网关。有关更多信息，请参阅创建中转网关。
- 中转网关上有四个连接，每个 VPC 一个。有关更多信息，请参阅 the section called “创建 VPC 连接”。
- 传输网关上的 Site-to-Site VPN 附件。有关更多信息，请参阅 the section called “创建与 VPN 的中转网关连接”。

  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，VPN CIDR 传播到传输网关路由表，VPC CIDRs 将添加到客户网关 BGP 表中。

- 每个隔离的 VPC 都与隔离路由表关联，并会传播到共享路由表。
- 每个共享的服务 VPC 都与共享路由表关联，并会传播到两个路由表。

路由

每个 VPC 都有一个路由表，传输网关有两个路由表，一个用于 VPN 连接 VPCs 和共享服务 VPC。

VPC A、VPC B、VPC C 和 VPC D 路由表

每个 VPC 都具有一个包含两个条目的路由表。第一个条目是 VPC 中本地路由的默认条目；这项条目允许该 VPC 中的实例在彼此之间进行通信。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 VPN 连接 VPCs ，使用一个路由表进行 VPN 连接。

VPC A、B 和 C 连接与以下路由表相关联，该路由表具有 VPN 连接的传播路由以及 VPC D 的连接的传播路由。

目的地	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 连接和共享服务 VPC（VPC D）连接与以下路由表相关联，该路由表具有指向各个 VPC 连接的条目。这允许 VPCs 从 VPN 连接和共享服务 VPC 与的通信。

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 VPC 中转网关启用路由传播到中转网关路由表。

客户网关 BGP 表

客户网关 BGP 表包含所有四个 VPCs网关 CIDRs 的。

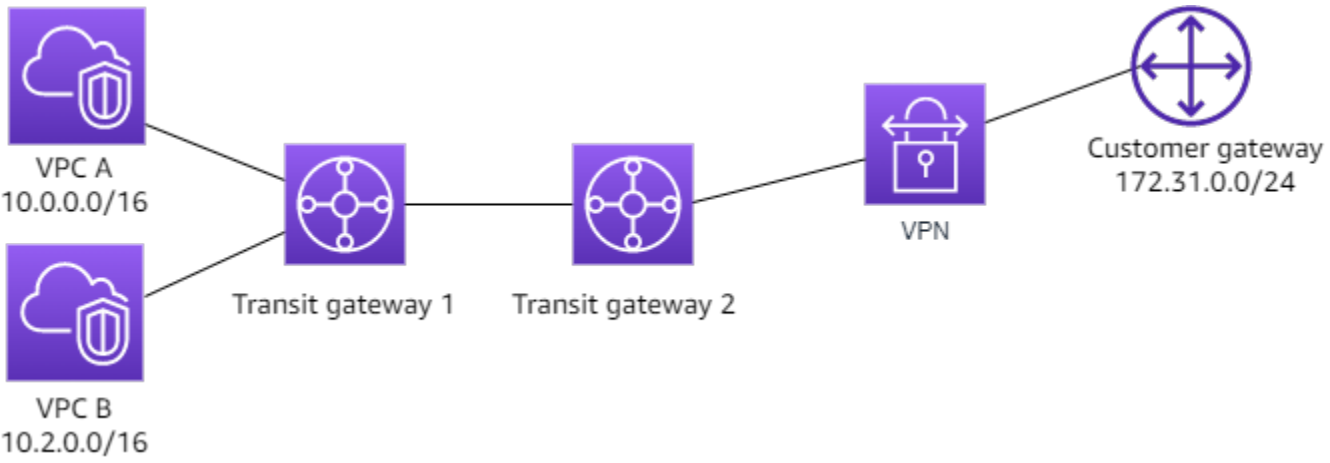
示例：对等中转网关

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。在该场景中，VPC 和 VPN 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。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

概览

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，传输网关 2 有一个 Site-to-Site VPN 连接。来自 VPC A 和 VPC B 中的子网并指向 Internet 的数据包通过中转网关 1 路由，然后通过中转网关 2，最后路由到 VPN 连接。



资源

为此场景创建以下资源：

- 二 VPCs。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 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”。
- 第一个中转网关上的两个 VPC 连接。有关更多信息，请参阅 the section called “创建 VPC 连接”。
- 第二个传输网关上的 Site-to-Site VPN 附件。有关更多信息，请参阅 the section called “创建与 VPN 的中转网关连接”。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连接。有关更多信息，请参阅 Amazon VPC Transit Gateways 中的中转网关对等节点连接。

创建 VPC 附件时，每个 VPC CIDRs 的都会传播到中转网关 1 的路由表。VPN 连接启动时，会发生以下操作：

- 建立了 BGP 会话
- Site-to-SiteVPN CIDR 传播到传输网关 2 的路由表
- VPC CIDRs 已添加到客户网关 BGP 表中

路由

每个 VPC 都有一个路由表，每个中转网关都有一个路由表。

VPC A 和 VPC B 路由表

每个 VPC 具有一个包含 2 个条目的路由表。第一个条目是 VPC 中本地 IPv4 路由的默认条目。此默认条目使该 VPC 中的资源能够相互通信。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。

目的地	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*	静态
10.2.0.0/16	*Attachment ID for peering connection*	静态

客户网关 BGP 表

客户网关 BGP 表包含以下 VPC CIDRs。

- 10.0.0.0/16
- 10.2.0.0/16

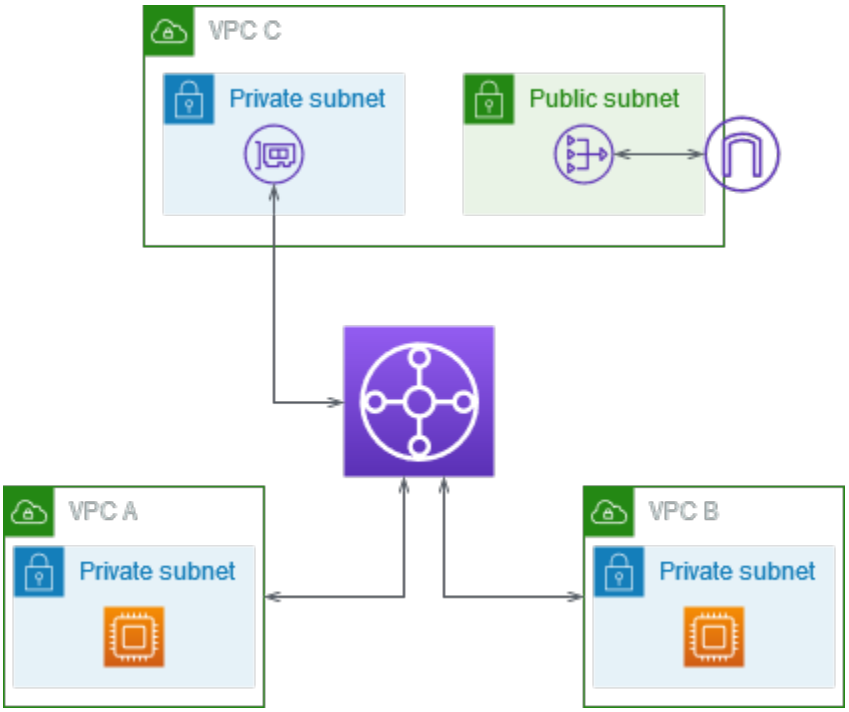
示例：到互联网的集中出站路由

您可以配置中转网关，将出站互联网流量从没有互联网网关的 VPC 路由到包含 NAT 网关和互联网网关的 VPC。

内容

概览

下表展示了此场景配置的主要组成部分。您的应用程序位于 VPC A 和 VPC B 中，这些应用程序只需要出站互联网访问。您可以为 VPC C 配置公有 NAT 网关和互联网网关，并为 VPC 连接配置私有子网。Connect 全部 VPCs 连接到公交网关。配置路由，以便来自 VPC A 和 VPC B 的出站互联网流量经过 VPC C 的中转网关。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 地址范围既不相同也不重叠。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。

- VPC A 和 VPC B 各有带 EC2 实例的私有子网。
- VPC C 具有以下内容：
  - 附加到 VPC 的互联网网关。有关更多信息，请参阅 Amazon VPC 用户指南中的创建并附加互联网网关。
  - 具有 NAT 网关的公有子网。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”。
- 中转网关上有三个 VPC 连接。每个 VPC 的 CIDR 块将传播到中转网关路由表。有关更多信息，请参阅 the section called “创建 VPC 连接”。对于 VPC C，您必须使用私有子网创建连接。如果您使用公有子网创建连接，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。通过将连接放在私有子网中，流量将路由到 NAT 网关，NAT 网关使用弹性 IP 地址作为源 IP 地址将流量发送到互联网网关。

路由

每个 VPC 都具有路由表，并且中转网关具有一个路由表。

路由表

- VPC A 的路由表
- VPC B 的路由表
- VPC C 的路由表
- 中转网关路由表

VPC A 的路由表

以下是一个示例路由表。第一个条目使 VPC 中的实例能够相互通信。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*

VPC B 的路由表

以下是一个示例路由表。第一个条目使该 VPC 中的实例能够相互通信。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 B CIDR	本地
0.0.0.0/0	*transit-gateway-id*

VPC C 的路由表

通过向互联网网关添加路由将具有 NAT 网关的子网配置为公有子网。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 VPC 中的实例能够相互通信。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 VPC 中的实例能够相互通信。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 VPC 的 CIDR 块将传播到中转网关路由表。静态路由将出站互联网流量发送到 VPC C。您可以选择通过为每个 VPC CIDR 添加黑洞路由来阻止内部 VPC 通信。

CIDR	附件	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*	静态

示例：共享服务 VPC 中的设备

您可以在共享服务 VPC 中配置设备（例如安全设备）。在 Transit Gateway 连接之间路由的所有流量首先由共享服务 VPC 中的设备进行检查。启用设备模式后，中转网关使用流哈希算法选择设备 VPC 中的单个网络接口，以便在流的生命周期内将流量发送到此。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，在流量的生命周期内，它将通过 VPC 连接中的同一可用区路由。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。

您必须将一个中转网关连接到设备 VPC，以保证流粘性。将多个中转网关连接到单个设备 VPC 并不能保证流粘性，因为中转网关不会彼此共享流状态信息。

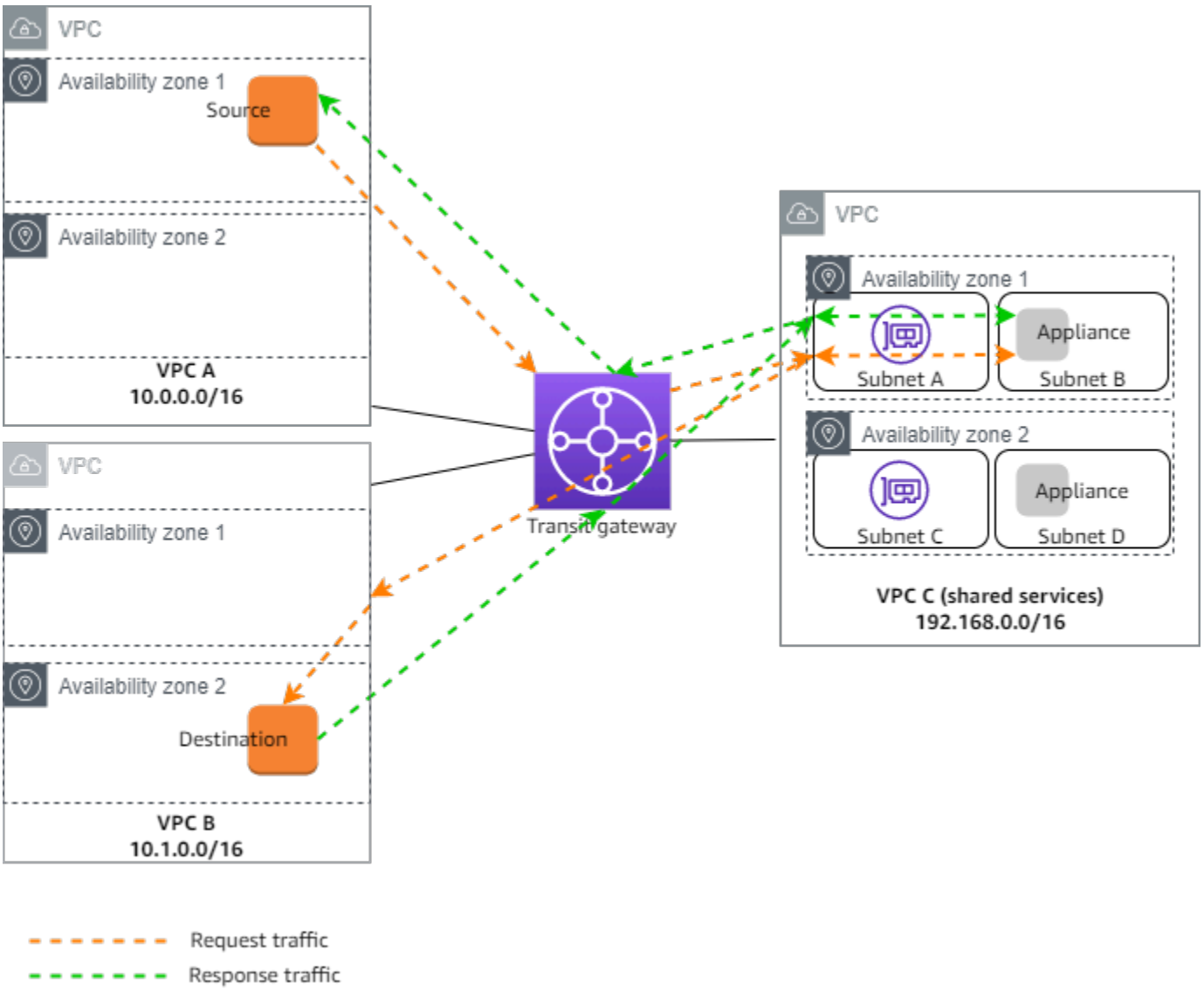
Important

- 只要源流量和目标流量指向来自同一个 Transit Gateway 连接的集中 VPC（检查 VPC），则设备模式下的流量就会正确路由。如果源和目标位于不同的中转网关连接上，则流量可能会丢失。如果集中式 VPC 接收来自另一个网关（如某个外部网关）的流量，然后在检查后再将这些流量发送到中转网关连接，则流量可能会丢失。
- 在现有连接上启用设备模式可能会影响该连接的当前路由，因为该连接可通过任何可用区流动。未启用设备模式时，流量会保留到来源可用区。

内容

概览

下表展示了此场景配置的主要组成部分。中转网关有三个 VPC 连接。VPC C 是共享服务 VPC。VPC A 和 VPC B 之间的流量将路由到中转网关，然后路由到 VPC C 中的安全设备进行检查，接着路由到最终目的地。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，VPC C 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。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 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 连接”。

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

  对于 VPC C 的 VPC 连接，启用设备模式支持，以便将响应流量路由到 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 软件开发工具包、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**
>
> 设备模式下的流粘性仅对源自检查 VPC 的源和目标流量有保证。

有状态设备和设备模式

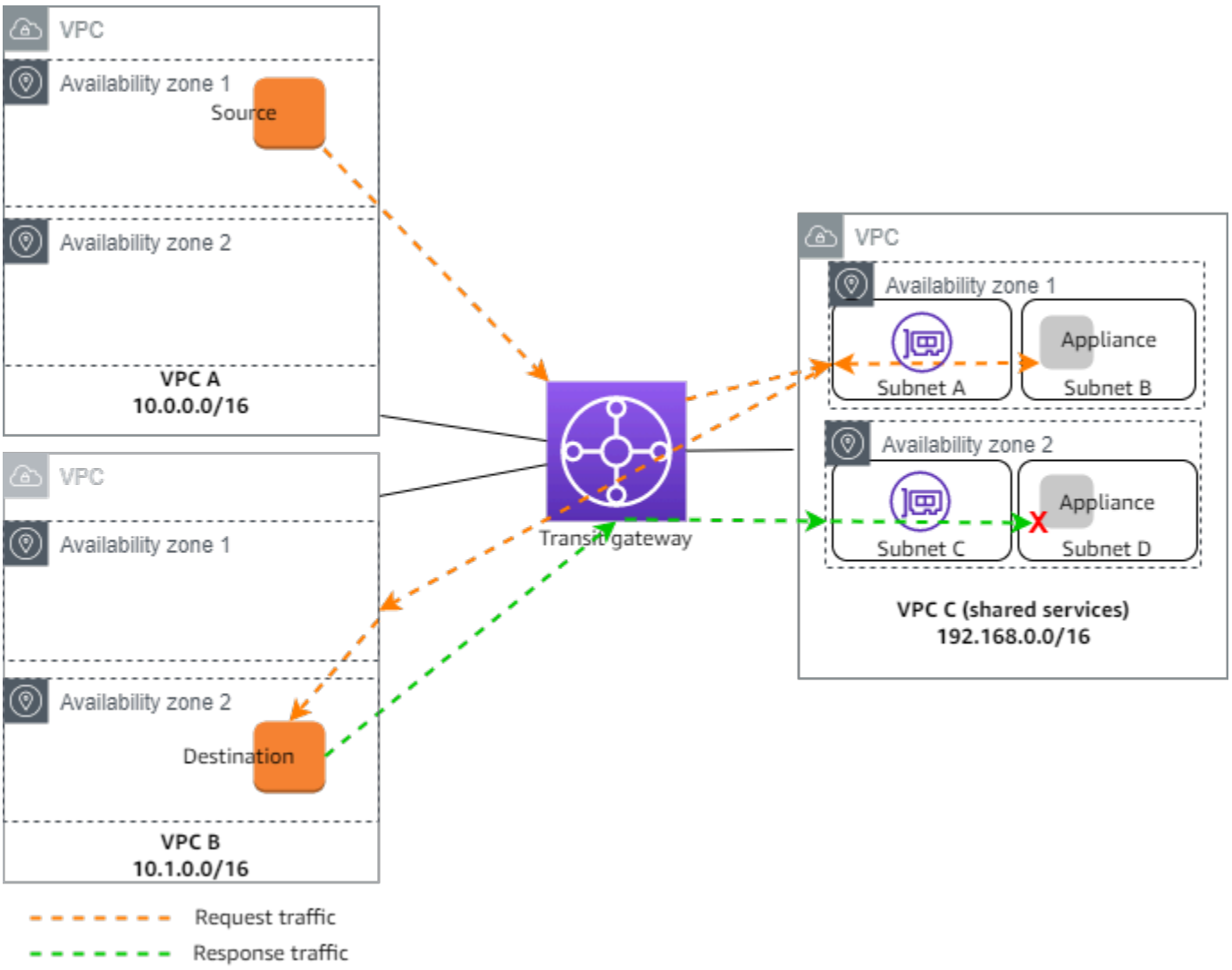
如果您的 VPC 连接跨越多个可用区，并且您需要通过同一设备路由源主机和目标主机之间的流量以进行状态检查，请为设备所在的 VPC 连接启用设备模式支持。

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

如果设备模式未启用，中转网关会尝试在源可用区内的 VPC 连接之间保持流量路由，直到流量到达目的地。只有在可用区出现故障或该可用区中没有与 VPC 连接关联的子网时，流量才会在挂接之间跨过可用区。

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 的响应流量由中转网关路由到 VPC C 中的同一可用区。因此，由于可用区 2 中的设备不知道来自 VPC A 中源的原始请求，流量被丢弃。



路由

每个 VPC 都有一个或多个路由表，中转网关有两个路由表。

VPC 路由表

VPC A 和 VPC B

VPCs A 和 B 的路由表有 2 个条目。第一个条目是 VPC 中本地 IPv4 路由的默认条目。此默认条目使该 VPC 中的资源能够相互通信。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。

目的地	目标

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	tgw-id

VPC C

共享服务 VPC (VPC C) 对于每个子网有不同的路由表。子网 A 由中转网关使用（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

此中转网关为 VPC A 和 VPC B 使用一个路由表，并为共享服务 VPC (VPC C) 使用一个路由表。

VPC A 和 VPC B 连接与以下路由表关联。路由表将所有流量路由到 VPC C。

目的地	目标	路由类型
0.0.0.0/0	*Attachment ID for VPC C*	静态

VPC C 连接与以下路由表相关联。它将流量路由到 VPC A 和 VPC B。

目的地	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

教程：开始使用 Amazon VPC 传输网关

以下教程可帮助您熟悉 Amazon VPC 传输网关中的传输网关。以下教程中的任务将指导您创建公交网关，然后 VPCs 使用该公交网关连接两个中转网关。您可以使用 Amaaozn VPC 控制台或使用创建传输网关。 AWS CLI

任务

- 教程：使用亚马逊 VPC 控制台创建 Tran AWS sit Gateway
- 教程：使用 AWS 命令行创建 T AWS ransit Gateway

教程：使用亚马逊 VPC 控制台创建 Tran AWS sit Gateway

在本教程中，您将学习如何使用 Amazon VPC 控制台创建传输网关并将两个网关 VPCs 连接到该网关。您将创建传输网关，连接两个网关 VPCs，然后配置必要的路由，以启用传输网关与您的之间的通信 VPCs。

先决条件

- 要演示使用公交网关的简单示例，请在同一区域创建两个 VPCs 。既 VPCs 不能相同也不能重叠 CIDRs。在每个 VPC 中启动一个 Amazon EC2 实例。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC 和亚马逊 EC2 用户指南中的启动实例。
- 你不能让相同的路线指向两个不同的路线 VPCs。如果公交网关路由表中 CIDRs 存在相同的路由，则传输网关不会传播新连接的 VPC 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 Transit Gateways 中的身份和访问管理 。
- 如果您尚未为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 用户指南中的配置安全组规则。

步数

- 步骤 1：创建中转网关
- 步骤 2：将您的 VPCs 连接到您的公交网关
- 步骤 3：在公交网关和您的公交网关之间添加路线 VPCs
- 步骤 4：测试中转网关
- 步骤 5：删除中转网关

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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. 在配置中转网关部分中执行以下操作：

   1. 对于 Amazon side Autonomous System Number (ASN)（Amazon 端自治系统编号 (ASN)），输入中转网关的私有 ASN。这应该是边界网关协议 (BGP) 会话一 AWS 侧的 ASN。

      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

      如果您有多区域部署，我们建议您为每个中转网关使用唯一的 ASN。

   2. （可选）选择是否启用以下任意操作之一：

      - 支持 VPCs 连接到此传输网关的 DNS。
      - 为连接到此中转网关的 VPN 连接提供 VPN ECMP 支持。
      - 默认路由表关联会自动将中转网关连接与此中转网关的默认路由表相关联。
      - 默认路由表传播会自动将路由表连接传播到此中转网关的默认路由表。
      - 组播支持允许在此中转网关中创建组播域。
8. （可选）在Configure-cross-account 共享选项部分，选择是否自动接受共享附件。如果已启用，则会自动接受连接。否则，必须接受或拒绝连接请求。
9. （可选）在传输网关 CIDR 块部分，为地址添加大小为 /24 或更大的 CIDR 块，为 IPv4 地址添加大小为 /64 或更大的 CIDR 块。 IPv6您可以关联任何公有或私有 IP 地址范围，但 169.254.0.0/16 范围以及与您的 VPC 连接和本地网络地址重叠的范围中的地址除外。

> **Note**
>
> 如果您正在配置 Connect (GRE) 附件或 Private VPNs IP，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/PrivateIP VPN）进行分配。

10. （可选）向此中转网关添加键值标签，以进一步识别它。
    1. 选择添加新标签。
    2. 输入键名称和关联值。
    3. 选择添加新标签以添加更多标签，或跳到下一步。
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`。

步骤 2：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，继续创建连接。为每个 VPC 创建连接。

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 VPC 的 Transit Gateway 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Create Transit Gateway Attachment（创建中转网关连接）。
4. （可选）对于 Name tag（名称标签），输入连接的名称。
5. 对于 Transit Gateway ID（中转网关 ID），选择要用于连接的中转网关。
6. 对于 Attachment type (连接类型)，选择 VPC。
7. 选择是否启用 DNS support (DNS 支持)。在本练习中，请勿启用IPv6 支持。
8. 对于 VPC ID，选择要附加到中转网关的 VPC。
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（创建中转网关连接）。

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 “中转网关方案示例”。

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连接 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的路由。

向 VPC 路由表中添加路由

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择路由表。
3. 选择与 VPC 关联的路由表。
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. 选择保存更改。

步骤 4：测试中转网关

您可以通过连接到每个 VPC 中的 Amazon EC2 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 Amazon EC2 用户指南中的 Connect 到您的 EC2 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连接的中转网关。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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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。

教程：使用 AWS 命令行创建 T AWS ransit Gateway

在本教程中，您将学习如何使用创建公交网关并将两个 VPCs 网关连接到该 AWS CLI 网关。您将创建传输网关，连接两个网关 VPCs，然后配置必要的路由，以启用传输网关与您的之间的通信 VPCs。

先决条件

在开始之前，请确保你有：

- AWS CLI 已安装并配置了适当的权限。如果您尚未 AWS CLI 安装，请参阅AWS 命令行界面文档。
- 既 VPCs 不能相同也不能重叠 CIDRs。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
- 每个 VPC 中有一个 EC2 实例。有关在 VPC 中启动 EC2 实例的步骤，请参阅 Amazon EC2 用户指南中的启动实例。
- 安全组配置为允许实例之间的 ICMP 流量。有关使用安全组控制流量的步骤，请参阅 Amazon VPC 用户指南中的使用安全组控制 AWS 资源流量。
- 使用公交网关的适当 IAM 权限。要查看公交网关 IAM 权限，请参阅AWS Transit Gateway 指南中的 Amazon VPC 传输网关中的身份和访问管理。

步数

- 步骤 1：创建中转网关
- 步骤 2：验证传输网关可用性状态
- 步骤 3：将您的 VPCs 连接到您的公交网关
- 步骤 4：验证传输网关附件是否可用
- 步骤 5：在您的公交网关和之间添加路线 VPCs
- 步骤 6：测试传输网关
- 步骤 7：删除传输网关附件和传输网关
- 结论

步骤 1：创建中转网关

创建传输网关时，AWS 会创建一个默认的公交网关路由表，并将其用作默认关联路由表和默认传播路由表。以下显示了该us-west-2区域的create-transit-gateway请求示例。请求中options还通过了其他内容。有关该create-transit-gateway命令的更多信息，包括可以在请求中传递的选项列表，请参阅create-transit-gateway。

```
aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --region us-west-2
```

然后，响应显示传输网关已创建。在响应中Options，返回的均为默认值。

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> 此命令返回有关您的新公交网关的信息，包括其 ID。记下公交网关 ID (tgw-1234567890abcdef0)，因为在后续步骤中将需要它。

步骤 2：验证传输网关可用性状态

创建公交网关时，它会处于pending状态。状态将自动从 “待处理” 更改为 “可用”，但在状态更改 VPCs 之前，您无法附加任何状态。要验证状态，请使用新创建的公交网关 ID 和 filters 选项运行describe-transit-gatweways命令。该filters选项使用Name=state并Values=available配对。然后，该命令会搜索以验证您的公交网关的状态是否处于可用状态。如果是，则显示响应"State": "available"。如果它处于任何其他状态，则它尚不可用。等待几分钟，然后再运行该命令。

有关 describe-transit-gateways 命令的更多信息，请参阅describe-transit-gateways。

```
aws ec2 describe-transit-gateways \
  --transit-gateway-ids tgw-1234567890abcdef0 \
  --filters Name=state,Values=available
```

等到中转网关状态从变pending为available后再继续。在以下响应中，State已更改为available。

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
            "State": "available",
            "OwnerId": "123456789012",
            "Description": "My Transit Gateway",
            "CreationTime": "2022-04-20T19:58:25+00:00",
            "Options": {
                "AmazonSideAsn": 64512,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "DefaultRouteTablePropagation": "enable",
```

```
                "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
                "MulticastSupport": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "example-transit-gateway"
                }
            ]
        }
    ]
}
```

步骤 3：将您的 VPCs 连接到您的公交网关

您的传输网关可用后，使用为每个 VPC 创建一个附件`create-transit-gateway-vpc-attachment`。你需要包括`transit-gateway-id`vpc-id、和`subnet-ids`。

有关该`create-transit-vpc attachment`命令的更多信息，请参见 create-transit-gateway-vpc-attactach。

在以下示例中，该命令运行两次，每个 VPC 运行一次。

对于第一个 VPC，使用第一个`vpc_id`和运行以下命令`subnet-ids`：

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0
```

响应显示成功附件。附件在某种`pending`状态下创建。无需更改此状态，因为它会自动变为`available`状态。这可能需要花几分钟的时间。

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-1234567890abcdef0",
```

```
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-1234567890abcdef0",
            "subnet-abcdef1234567890"
        ],
        "CreationTime": "2025-06-23T18:35:11+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

对于第二个 VPC，使用第二个 VPC 运行与上述相同的命令，vpc_id然后subnet-ids：

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-abcdef1234567890 \
  --subnet-ids subnet-abcdef01234567890
```

此命令的响应还显示连接成功，且附件当前处于pending状态。

```
{
    {
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-fedcba0987654321",
            "subnet-0987654321fedcba"
        ],
        "CreationTime": "2025-06-23T18:42:56+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
```

```
        }
    }
}
```

步骤 4：验证传输网关附件是否可用

公交网关附件是在初始pending状态下创建的。在状态更改为之前，您将无法在路径中使用这些附件available。这是自动发生的。使用describe-transit-gateways命令和transit-gateway-id来检查State。有关 describe-transit-gateways 命令的更多信息，请参阅describe-transit-gateways。

运行以下命令以检查状态。在此示例中，请求中传递了可选字段Name和Values过滤器字段：

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --filters Name=transit-gateway-id,Values=tgw-1234567890abcdef0
```

以下响应显示两个附件都处于available状态：

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
```

```
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```

步骤 5：在您的公交网关和之间添加路线 VPCs

在每个 VPC 的路由表中配置路由，使用命令和每个 VPC 路由表中的`create-route`命令将流量引导到另一个 VPC，通过中转网关将`transit-gateway-id`流量引导到另一个 VPC。在以下示例中，该命令运行两次，每个路由表运行一次。该请求包括您正在创建`transit-gateway-id`的每个 VPC 路由的`destination-cidr-block`、和。`route-table-id`

有关`create-route`命令的更多信息，请参阅 create- route。

对于第一个 VPC 的路由表，运行以下命令：

```
aws ec2 create-route \
  --route-table-id rtb-1234567890abcdef0 \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

对于第二个 VPC 的路由表，运行以下命令。此路由使用`route-table-id`与第一个 VPC `destination-cidr-block` 不同的和。但是，由于您只使用单个公交网关，因此使用`transit-gateway-id`的是相同的公交网关。

```
aws ec2 create-route \
```

```
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

每条路径`true`的响应都会返回，表示路径已创建。

```
{
    "Return": true
}
```

> **Note**
>
> 将目标 CIDR 块替换为您的实际 CIDR 块。 VPCs

步骤 6：测试传输网关

您可以通过连接到一个 VPC 中的实例并对另一个 VPC 中的 EC2 实例执行 ping 操作，然后运行`ping`命令来确认传输网关已成功创建。

1. 使用 SSH 或 Inst EC2 ance Connect 连接到第一个 VPC 中的 EC2 实例
2. Ping 第二个 VPC 中 EC2 实例的私有 IP 地址：

   ```
   ping 10.2.0.50
   ```

   > **Note**
   >
   > `10.2.0.50`替换为第二个 VPC 中 EC2 实例的实际私有 IP 地址。

如果 ping 成功，则表示您的传输网关配置正确，并且在您之间路由流量 VPCs。

步骤 7：删除传输网关附件和传输网关

当您不再需要传输网关时，可以将其删除。首先，必须删除所有附件。运行`delete-transit-gateway-vpc-attachment`命令，`transit-gateway-attachment-id`对每个附件使用。运行命令后，`delete-transit-gateway`使用删除传输网关。对于以下内容，删除在前面的步骤中创建的两个 VPC 附件和单个传输网关。

> **Important**
>
> 删除所有公交网关附件后，您将停止产生费用。

1. 使用`delete-transit-gateway-vpc-attachment`命令删除 VPC 附件。有关`delete-transit-gateway-vpc-attachment`命令的更多信息，请参见 delete-transit-gateway-vpc-attactach。

   对于第一个附件，请运行以下命令：

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-1234567890abcdef0
   ```

   第一个 VPC 附件的删除响应返回以下内容：

   ```
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "VpcId": "vpc-abcdef1234567890",
           "VpcOwnerId": "123456789012",
           "State": "deleting",
           "CreationTime": "2025-06-23T18:42:56+00:00"
       }
   }
   ```

   为第二个附件运行`delete-transit-gateway-vpc-attachment`命令：

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-abcdef1234567890
   ```

   第二个 VPC 附件的删除响应返回以下内容：

   ```
   The response returns:
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "VpcId": "vpc-abcdef1234567890",
   ```

```
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2. 附件在被删除之前一直处于deleting状态。删除后，您可以删除该传输网关。将该delete-transit-gateway命令与transit-gateway-id。有关delete-transit-gateway命令的更多信息，请参阅delete-transit-gateway。

   以下示例删除My Transit Gateway了您在上述第一步中创建的内容：

```
aws ec2 delete-transit-gateway \
  --transit-gateway-id tgw-1234567890abcdef0
```

   下图显示了对请求的响应，其中包括已删除的公交网关 ID 和名称，以及创建公交网关时为其设置的原始选项。

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "deleting",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        },
        "Tags": [
            {
                "Key": "Name",
```

```
                "Value": "example-transit-gateway"
            }
        ]
    }
}
```

结论

您已经成功创建了一个传输网关，连接了两个 VPCs 网关，在它们之间配置了路由，并验证了连通性。这个简单的示例演示了 Amazon VPC 传输网关的基本功能。对于更复杂的场景，例如连接到本地网络或实施更高级的路由配置，请参阅 Amazon VPC Transit Gateways 用户指南。

Amazon VPC 中转网关设计最佳实践

以下是您的中转网关设计的最佳实践：

- 为每个中转网关 VPC 附件使用单独的子网。例如，对于每个子网，使用较小的 CIDR/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 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 并将其与关联到中转网关的所有子网相关联。确保网络 ACL 在入站和出站方向打开。
- 将同一个 VPC 路由表与关联到中转网关的所有子网相关联，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盒 VPC）。
- 使用边界网关协议 (BGP) Site-to-Site VPN 连接。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 网关连接和 BGP Site-to-Site VPN 附件启用路由传播。
- 从 VPC 对等连接迁移出来，转而使用中转网关。如果 VPC 对等连接和 Transit Gateway 之间的 MTU 大小不匹配，则可能会因非对称流量而导致一些丢包。 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。
- 对于带多个中转网管的部署，我们建议您为每个中转网关使用唯一自治系统编号 (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 VPC Transit Gateways 利用中转网关

您可以通过 Amazon VPC 控制台或 AWS CLI使用中转网关。

主题

共享中转网关

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。必须启用 RAM，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

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和执行任务，您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，将这些策略附加到需要这些权限的 IAM 用户或组。

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 `DescribeTransitGateways` API。
- 运行用于创建和描述附件的，例如`CreateTransitGatewayVpcAttachment`和`DescribeTransitGatewayVpcAttachments`，在其中 VPCs。 APIs
- 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。如果中转网关和连接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 连接保持正常工作。

- 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 连接。

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

仅 VPC 所有者可以将中转网关附加到共享 VPC 子网。参与者不能。来自参与者资源的流量可以使用附件，具体取决于 VPC 所有者在共享 VPC 子网上设置的路由。

有关更多信息，请参阅《Amazon VPC 用户指南》中的 与其他账户共享 VPC。

Amazon VPC Transit Gateways 中的中转网关

传输网关使您能够连接 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。

您可以在中转网关上启用多播，然后创建一个中转网关多播域，允许通过与域关联的 VPC 挂载，将多播流量从多播源发送到多播组成员。

每个 VPC 或 VPN 挂载均与单个路由表关联。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 IPv6 CIDRs 和目标。目标是 VPCs和 VPN 连接。当在中转网关上挂载 VPC 或创建 VPN 连接时，挂载与中转网关的默认路由表关联。

您可以在中转网关内创建其他路由表，并更改 VPC 或 VPN 与这些路由表的关联。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。您可以将中转网关路由表中的路由指向对等节点连接，以便在对等传输网关之间路由流量。

您可以选择将一个或多个 IPv4 或 IPv6 CIDR 块与您的传输网关相关联。在为中转网关 Connect 挂载建立中转网关 Connect 对等节点时，您可以从 CIDR 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 `169.254.0.0/16` 范围以及与您的 VPC 挂载和本地网络地址重叠的范围中的地址除外。有关 IPv4 和 IPv6 CIDR 块的更多信息，请参阅 Amazon VPC 用户指南中的 IP 地址。

任务

- 使用 Amazon VPC 中转网关创建中转网关
- 使用 Amazon VPC Transit Gateways 查看中转网关信息
- 使用 Amazon VPC Transit Gateways 添加或编辑中转网关的标签
- 使用 Amazon VPC 中转网关修改中转网关
- 使用 Amazon VPC Transit Gateways 接受资源共享
- 使用 Amazon VPC Transit Gateways 接受共享连接
- 使用 Amazon VPC Transit Gateways 删除中转网关

使用 Amazon VPC 中转网关创建中转网关

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。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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 side Autonomous System Number (ASN)（Amazon 自治系统号 (ASN)），要么保留默认值以使用默认的 ASN，要么输入您中转网关的私有 ASN。这应该是边界网关协议 (BGP) 会话一 AWS 侧的 ASN。

   16 位的范围为 64512 到 65534。 ASNs

   32位的区间为42亿至4294967294。 ASNs

   如果您有多区域部署，我们建议您为每个中转网关使用唯一的 ASN。
7. 要获得 DNS 支持，如果您需要 VPC 在从连接到传输网关的其他 VPC 中的实例进行查询时将公有 IPv4 DNS 主机名解析为私有 IPv4 地址，请选择此选项。

8. 要获得安全组引用支持，请启用此功能以引用 VPCs 连接到传输网关的安全组。有关安全组引用的更多信息，请参阅 the section called “引用安全组”。
9. 对于 VPN ECMP support（VPN ECMP 支持），如果您在 VPN 隧道之间需要等价多路径（ECMP）路由支持，则选择此选项。如果连接通告相同 CIDRs，则流量将在它们之间平均分配。

   在选择该选项时，公布的 BGP ASN 和 BGP 属性（如 AS 路径）必须相同。

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

10. 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连接与中转网关的默认路由表关联。
11. 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连接传播到中转网关的默认路由表。
12. （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）。
13. （可选）在Configure-cross-account 共享选项部分，选择是否自动接受共享附件。如果已启用，则会自动接受连接。否则，必须接受或拒绝连接请求。

    对于 Auto accept shared attachments（自动接受共享的连接），选择此选项以自动接受跨账户连接。
14. （可选）对于公交网关 CIDR 块，请为您的传输网关指定一个 IPv4 或多个 IPv6 CIDR 块。

    您可以为指定大小为 /24 或更大的 CIDR 块（例如 /23 或 /22），也可以为 IPv4指定大小为 /64 或更大的 CIDR 块（例如 /63 或 /62）。 IPv6您可以关联任何公有或私有 IP 地址范围，但 169.254.0.0/16 范围以及与您的 VPC 连接和本地网络地址重叠的范围中的地址除外。

    > **Note**
    >
    > 如果您正在配置 Connect (GRE) 附件或 Private VPNs IP，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/PrivateIP VPN）进行分配。

15. 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 VPC Transit Gateways 查看中转网关信息

查看任一中转网关。

使用控制台查看中转网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。中转网关的详细信息显示在页面网关列表下方。

要查看公交网关，请使用 AWS CLI

使用 describe-transit-gateways 命令。

使用 Amazon VPC Transit Gateways 添加或编辑中转网关的标签

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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中转网关。
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 VPC 中转网关修改中转网关

您可以修改传输网关的配置选项。修改公交网关时，任何现有的公交网关附件都不会遇到任何服务中断。

您无法修改他人与您共享的中转网关。

如果任何 IP 地址当前用于 Connect 对等节点，您将无法删除中转网关的 CIDR 块。

修改中转网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Transit Gateways 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. 要查看共享的中转网关，请在 Amazon VPC 控制台中打开 Transit Gateways（中转网关） 页面。

使用 Amazon VPC Transit Gateways 接受共享连接

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 AWS CLI 手动接受跨账户（共享）附件。

手动接受共享连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择等待接受的中转网关连接。
4. 选择 Actions（操作）、Accept Transit Gateway attachment（接受中转网关连接）。

要接受共享附件，请使用 AWS CLI

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

使用 Amazon VPC Transit Gateways 删除中转网关

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

使用控制台删除中转网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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。

Amazon VPC Transit Gateways 中的 Amazon VPC 连接

通过与传输网关的 Amazon Virtual Private Cloud (VPC) 连接，您可以将流量路由进出一个或多个 VPC 子网。将 VPC 连接到中转网关时，必须从每个可用区中指定一个子网，供中转网关用于路由流量。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

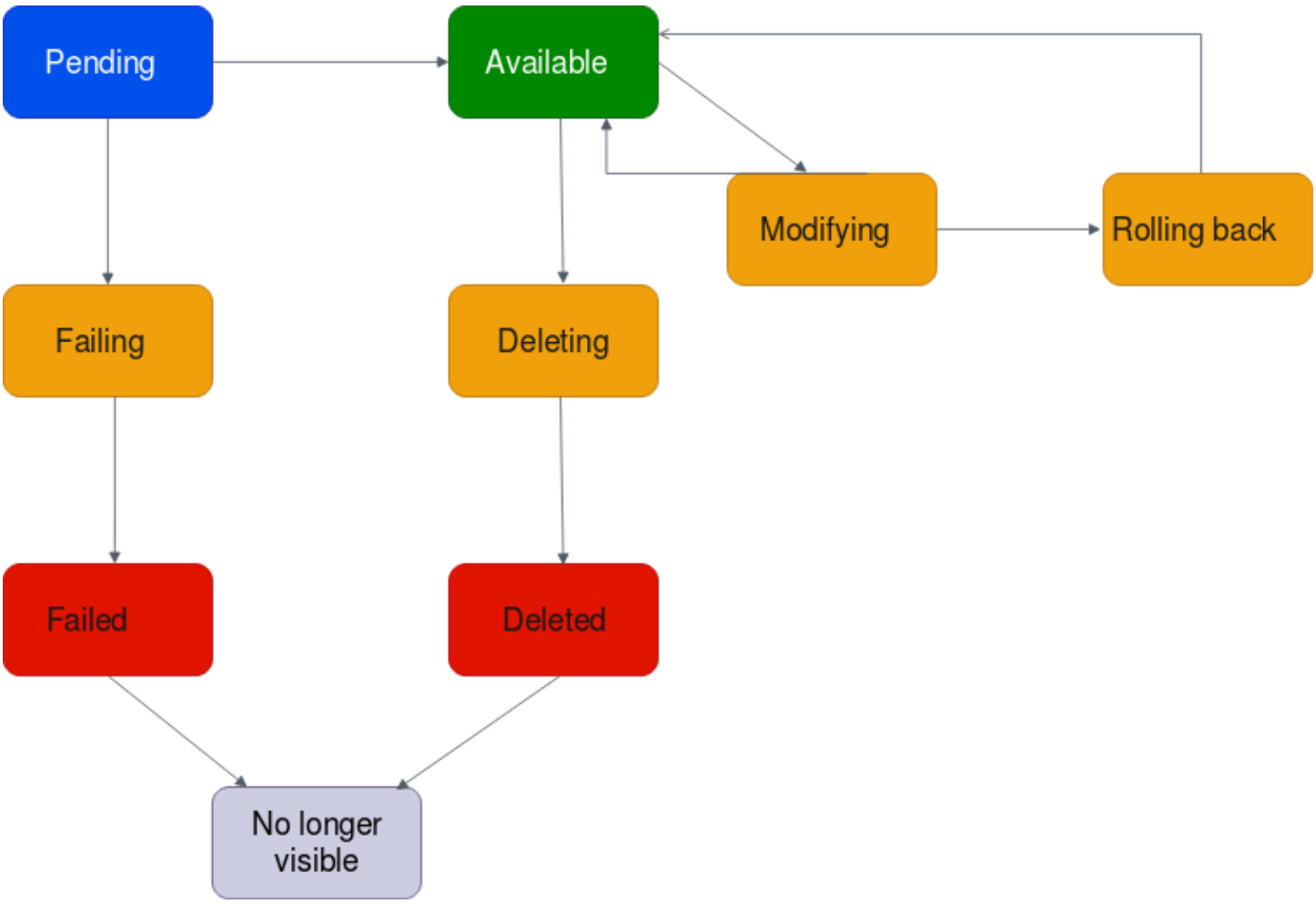
- 将 VPC 挂载到中转网关时，可用区中没有中转网关挂载的任何资源无法到达中转网关。如果子网路由表中有通往中转网关的路由，则只有当中转网关在同一可用区的子网中有挂载时，才会将流量转发到中转网关。
- 对于使用 Amazon Route 53 中的私有托管区域 VPCs设置的自定义 DNS 名称，传输网关不支持 DNS 解析。要为所有 VPCs 连接到传输网关的私有托管区域配置名称解析，请参阅使用 Amazon Route 53 和 Tr AWS ansit Gateway 对混合云进行集中化 DNS 管理。

- 如果某个范围内的 CIDR VPCs 与所连接的 VPC 中的 CIDR 重叠 CIDRs，则传输网关不支持在两者之间进行路由。如果您将 VPC 连接到传输网关，并且其 CIDR 与已连接到中转网关的另一个 VPC 的 CIDR 相同或重叠，则新连接的 VPC 的路由不会传播到中转网关路由表。
- 您不能为驻留在本地区域中的 VPC 子网创建连接。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。
- 在将中转网关添加到路由表之前，中转网关必须至少有一个 VPC 挂载。

VPC 挂载生命周期

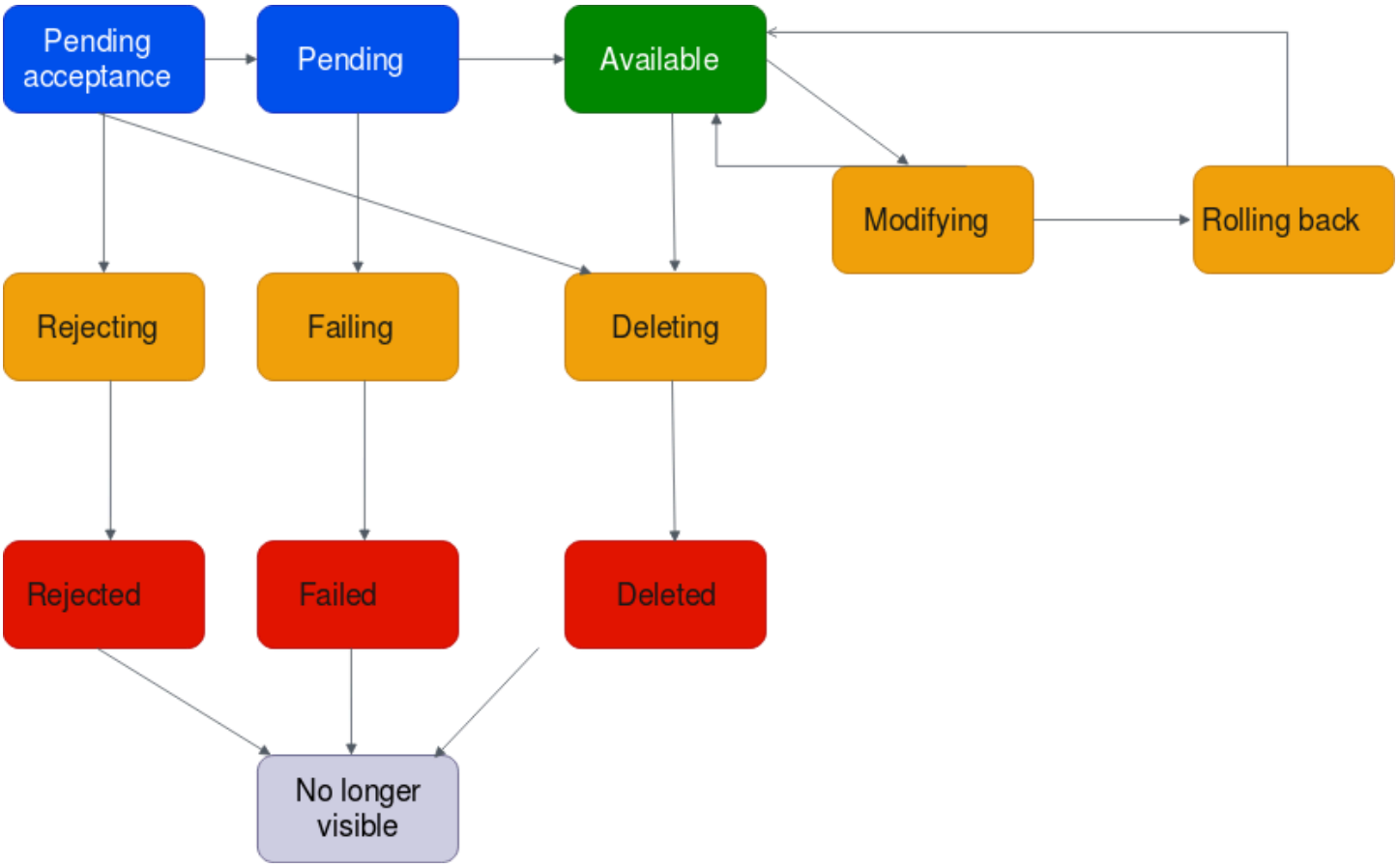
从请求发起开始，VPC 挂载会经历各个不同阶段。在每个阶段中，您都可以执行一些操作，在生命周期结束后，VPC 挂载仍会在 Amazon Virtual Private Cloud Console 和 API 或命令行输出中继续显示一段时间。

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：已发起了 VPC 挂载请求，正在进行配置。在此阶段，挂载可能会失败，也可能会变为 `available`。
- 即将失败：VPC 挂载请求将会失败。在此阶段，VPC 挂载会变为 `failed`。
- 失败：VPC 挂载请求失败。在此状态下，无法删除 VPC 挂载。失败的 VPC 挂载仍会继续显示 2 小时，之后不再显示。
- 可用：VPC 挂载可用，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`。
- 正在删除：正在删除 VPC 挂载。在此阶段，挂载可以变为 `deleted`。
- 已删除：已删除 `available` VPC 挂载。当 VPC 挂载处于此状态时，无法对其进行修改。VPC 挂载仍会继续显示 2 小时，之后不再显示。
- 正在修改：已请求修改 VPC 挂载的属性。在此阶段，挂载可以变为 `available`，也可以变为 `rolling back`。
- 正在回滚：无法完成 VPC 挂载修改请求，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。



- 等待接受：VPC 挂载请求正在等待接受。在此阶段，挂载可以变为 pending、rejecting 或 deleting。
- 正在拒绝：正在拒绝 VPC 挂载。在此阶段，挂载可以变为 rejected。
- 已拒绝：pending acceptance VPC 挂载已被拒绝。当 VPC 挂载处于此状态时，无法对其进行修改。VPC 挂载仍会继续显示 2 小时，之后不再显示。
- 待处理：已接受 VPC 挂载并正在进行配置。在此阶段，挂载可能会失败，也可能会变为 available。
- 即将失败：VPC 挂载请求将会失败。在此阶段，VPC 挂载会变为 failed。
- 失败：VPC 挂载请求失败。在此状态下，无法删除 VPC 挂载。失败的 VPC 挂载仍会继续显示 2 小时，之后不再显示。
- 可用：VPC 挂载可用，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。
- 正在删除：正在删除 VPC 挂载。在此阶段，挂载可以变为 deleted。
- 已删除：已删除 available 或 pending acceptance VPC 挂载。当 VPC 挂载处于此状态时，无法对其进行修改。VPC 挂载仍会继续显示 2 小时，之后不再显示。
- 正在修改：已请求修改 VPC 挂载的属性。在此阶段，挂载可以变为 available，也可以变为 rolling back。
- 正在回滚：无法完成 VPC 挂载修改请求，系统正在撤消所做的任何更改。在此阶段，挂载可以变为 available。

设备模式

如果您计划在 VPC 中配置有状态网络设备，则可以在创建连接时为设备所在的 VPC 连接启用设备模式支持。这可确保 T AWS ransit Gateway 在源和目标之间的流量流的生命周期内为该 VPC 连接使用相同的可用区。它还允许中转网关向 VPC 中的任何可用区发送流量，前提是该区域中存在子网关联。虽然设备模式仅支持 VPC 附件，但网络流可以来自任何其他传输网关连接类型，包括 VPC、VPN 和 Connect 附件。设备模式也适用于来源和目的地不同的网络流 AWS 区域。如果您最初没有启用设备模式，但后来编辑连接配置以启用该模式，则可能会在不同的可用区域之间重新平衡网络流。您可以使用控制台、命令行或 API 启用或禁用设备模式。

T AWS ransit Gateway 中的设备模式在确定通过设备模式 VPC 的路径时，会考虑源和目标可用区，从而优化流量路由。这种方法提高了效率并减少了延迟。行为因特定的配置和流量模式而异。以下是示例场景。

场景 1：通过设备 VPC 进行可用区内流量路由

当流量从源可用区 us-east-1a 流向目标可用区 us-east-1a，同时在 us-east-1a 和 us-east-1b 中都有设备模式 VPC 附件时，Transit Gateway 会在设备 VPC 内从 us-east-1a 中选择一个网络接口。此可用区将在源和目标之间的流量流的整个持续时间内进行维护。

场景 2：通过设备 VPC 进行可用区间流量路由

对于从源可用区 us-east-1a 流向目标可用区 us-east-1b 的流量，在 us-east-1a 和 us-east-1b 中均有设备模式 VPC 附件，Transit Gateway 使用流哈希算法在设备 VPC 中选择 us-east-1a 或 us-east-1b。所选可用区在流程的生命周期内始终如一地使用。

场景 3：通过没有可用区域数据的设备 VPC 路由流量

当流量从源可用区 us-east-1a 发往没有可用区信息的目的地（例如互联网流量），且在 us-east-1a 和 us-east-1b 中均有设备模式 VPC 附件时，Transit Gateway 会在设备 VPC 内从 us-east-1a 中选择一个网络接口。

场景 4：通过与源或目标不同的可用区中的设备 VPC 路由流量

当流量从源可用区 us-east-1a 流向目标可用区 us-east-1b，在不同的可用区中使用设备模式 VPC 附件，例如 us-east-1c 和 us-east-1d 时，Transit Gateway 使用流哈希算法在设备 VPC 中选择 us-east-1c 或 us-east-1d。所选可用区在流程的生命周期内始终如一地使用。

> **Note**
>
> 只有 VPC 附件支持设备模式。确保为与设备 VPC 连接关联的路由表启用路由传播。

引用安全组

您可以使用此功能来简化安全组管理和控制连接到同一传输网关的 instance-to-instance流量。 VPCs 您只能在入站规则中交叉引用安全组。出站安全规则不支持安全组引用。启用或使用安全组引用不会产生额外费用。

可以为中转网关和中转网关 VPC 附件配置安全组引用支持，并且只有在为传输网关及其 VPC 附件都启用安全组引用支持后才有效。

限制

将安全组引用与 VPC 附件一起使用时，存在以下限制。

- 不支持跨公交网关对等连接引用安全组。两者都 VPCs 必须连接到同一个传输网关。
- 可用区 use1-az3 中的 VPC 连接不支持引用安全组。
- PrivateLink 端点不支持引用安全组。我们建议使用基于 IP CIDR 的安全规则作为替代方案。
- 只要为 VPC 中的 EFS 接口配置了 “允许所有出口” 安全组规则，安全组引用就适用于弹性文件系统 (EFS)。
- 对于通过中转网关进行本地区域连接，仅支持以下本地区域：us-east-1-atl-2a、us-east-1-dfw-2a、us-east-1-iah-2a、us-west-2-lax-1a、us-west-2-lax-1b、us-east-1-mia-2a、us-east-1-chi-2a 和 us-west-2-phx-2a。
- 对于 VPCs 位于不支持的本地区域、Outposts 和 Wavelength Zones 中的子网，我们建议在 VPC 连接级别禁用此功能 AWS ，因为这 AWS 可能会导致服务中断。
- 如果您有检查 VPC，则通过传输网关引用的安全组不适用于跨网关 Load Balancer 或 AWS Net AWS work Firewall。

任务

- 使用 Amazon VPC 传输网关创建 VPC 连接
- 使用 Amazon VPC Transit Gateways 修改 VPC 连接
- 使用 Amazon VPC Transit Gateways 修改 VPC 连接标签
- 使用 Amazon VPC Transit Gateways 查看 VPC 连接
- 使用 Amazon VPC Transit Gateways 删除 VPC 连接
- 更新 AWS Transit Gateway 安全组入站规则
- 识别 AWS Transit Gateway 引用的安全组
- 移除陈旧 AWS Transit Gateway 的安全组规则
- 排查 Amazon VPC Transit Gateways VPC 连接创建问题

使用 Amazon VPC 传输网关创建 VPC 连接

使用控制台创建 VPC 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Create Transit Gateway Attachment（创建中转网关连接）。
4. 对于 Name tag（名称标签），可选择是否输入中转网关连接的名称。

5. 对于 Transit Gateway ID（中转网关 ID），选择要用于连接的中转网关。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 Attachment type（连接类型），选择 VPC。
7. 选择是否启用 DNS IPv6 支持、支持和设备模式支持。

   如果选择的是设备模式，源和目标之间的流量将在该流的生命周期内，为 VPC 连接使用相同的可用区。
8. 选择是否启用安全组引用支持。启用此功能可引用 VPCs 连接到传输网关的安全组。有关安全组引用的更多信息，请参阅 the section called “引用安全组”。
9. 选择是否启用 Supp IPv6ort。
10. 对于 VPC ID，选择要附加到中转网关的 VPC。

    此 VPC 必须至少有一个子网与其关联。
11. 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。
12. 选择 Create Transit Gateway Attachment（创建中转网关连接）。

使用创建 VPC 附件 AWS CLI

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

使用 Amazon VPC Transit Gateways 修改 VPC 连接

使用控制台修改 VPC 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 VPC 连接，然后依次选择 Actions（操作）和 Modify Transit Gateway attachment（修改中转网关连接）。
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. 要添加或删除连接中的子网，请选中或取消选中想要添加或删除的子网 ID 旁边的复选框。

> **Note**
>
> 当连接处于正在修改状态时，添加或修改 VPC 连接子网可能会影响数据流量。

6. 要能够引用 VPCs 连接到传输网关的安全组，请选择安全组引用支持。有关安全组引用的更多信息，请参阅 the section called “引用安全组”。

> **Note**
>
> 如果您为现有中转网关禁用安全组引用，则所有 VPC 连接都将禁用安全组引用。

7. 选择 Modify Transit Gateway attachment（修改中转网关连接）。

要修改您的 VPC 附件，请使用 AWS CLI

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

使用 Amazon VPC Transit Gateways 修改 VPC 连接标签

使用控制台修改 VPC 连接标签

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 VPC 连接，然后选择 Actions（操作）、Manage tags（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)。

仅可使用控制台修改 VPC 连接标签。

使用 Amazon VPC Transit Gateways 查看 VPC 连接

使用控制台查看 VPC 挂载

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 在 Resource type（资源类型）栏，寻找 VPC。这些是 VPC 挂载。
4. 选择挂载以查看其详细信息。

要查看您的 VPC 附件，请使用 AWS CLI

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

使用 Amazon VPC Transit Gateways 删除 VPC 连接

使用控制台删除 VPC 挂载

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

要删除 VPC 附件，请使用 AWS CLI

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

更新 AWS Transit Gateway 安全组入站规则

您可以更新与传输网关关联的任何入站安全组规则。您可以使用 Amazon VPC 控制台或使用命令行或 API 更新安全组规则。有关安全组引用的更多信息，请参阅 the section called “引用安全组”。

使用控制台更新安全组规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择安全组，选择操作、编辑入站规则，修改入站规则。

4. 要添加规则，请选择添加规则，然后指定类型、协议和端口范围。对于源（入站规则），输入与中转网关连接的 VPC 中安全组的 ID。

> **Note**
>
> 与中转网关连接的 VPC 中的安全组不会自动显示。

5. 要编辑现有的规则，请更改其值（例如，源或描述）。
6. 要删除规则，请选择该规则旁的删除。
7. 选择保存规则。

使用命令行更新入站规则

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

识别 AWS Transit Gateway 引用的安全组

要确定连接到同一传输网关的 VPC 中的安全组规则中是否引用了您的安全组，请使用以下命令之一。

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

移除陈旧 AWS Transit Gateway 的安全组规则

过时的安全组规则是指在同一 VPC 或连接到同一中转网关的 VPC 中引用已删除的安全组的规则。系统不会从您的安全组中自动移除过时的安全组规则，您必须手动删除它们。

您可以使用 Amazon VPC 控制台查看和删除某个 VPC 的过时安全组规则。

查看和删除过时安全组规则

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Security Groups（安全组）。

3. 选择 Actions (操作)、Manage stale rules (管理过时规则)。
4. 对于 VPC，请选择具有过时规则的 VPC。
5. 选择编辑。
6. 选择您希望删除的规则旁边的 Delete（删除）按钮。选择 Preview changes (预览更改)，然后选择 Save rules (保存规则)。

使用命令行描述您的过时的安全组规则

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

识别出陈旧的安全组规则后，您可以使用revoke-security-group-ingress或revoke-security-group-egress命令将其删除。

排查 Amazon VPC Transit Gateways VPC 连接创建问题

以下主题可帮助您排查在创建 VPC 挂载时可能遇到的问题。

问题

VPC 挂载失败。

原因

原因可能是以下之一：

1. 正在创建 VPC 挂载的用户没有创建服务相关角色的适当权限。
2. 由于 IAM 请求太多而存在限制问题，例如，您正在使用 AWS CloudFormation 创建权限和角色。
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。在用户获得权限后创建 VPC 挂载。
2. 手动创建 VPC 附件。有关更多信息，请参阅 the section called “创建 VPC 连接”。

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 “转换网关”。
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 “查看中转网关”。

AWS Transit Gateway 网络功能配件

您可以创建网络功能附件，将您的公交网关直接连接到 AWS Network Firewall。这样就无需创建和管理检查 VPCs。

使用防火墙附件，可在幕后 AWS 自动配置和管理所有必要的资源。您将看到新的传输网关附件，而不是单个防火墙端点。这简化了实施集中式网络流量检查的过程。

在使用防火墙附件之前，必须先在中创建附件 AWS Network Firewall。有关创建附件的步骤，请参阅《AWS Network Firewall 开发者指南》中的 “AWS Network Firewall 管理入门”。创建防火墙后，您可以在 Transit Gateway 控制台的 “附件” 部分下查看附件。该附件将以一种网络功能列出。

主题

- 接受或拒绝 Tr AWS ansit Gateway 网络功能附件
- 查看 AWS 公交 Gateway 网络功能附件
- 通过 Transi AWS t Gateway 网络功能附件路由流量

接受或拒绝 Tr AWS ansit Gateway 网络功能附件

您可以使用 Amazon VPC 控制台或 AWS Network Firewall CLI 或 API 来接受或拒绝传输网关网络功能附件，包括 Network Firewall 附件。如果您是传输网关的所有者，并且有人从另一个账户向您的传输网关创建了防火墙附件，则需要接受或拒绝连接请求。

要使用 Network Firewall CLI 接受或拒绝网络功能附件，请参阅 AWS Network Firewall API 参考*`RejectNetworkFirewallTransitGatewayAttachment`* APIs 中的`AcceptNetworkFirewallTransitGatewayAttachment`或。

使用控制台接受或拒绝网络功能附件

使用 Amazon VPC 控制台接受或拒绝传输网关网络功能附件。

使用控制台接受或拒绝网络功能附件

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

2. 在导航窗格中，选择传输网关。
3. 选择公交网关附件。
4. 选择状态为 “待接受” 且类型为 “网络” 功能的附件。
5. 选择 “操作”，然后选择 “接受附件” 或 “拒绝附件”。
6. 在确认对话框中，选择 “接受” 或 “拒绝”。

如果您接受附件，它就会变为活动状态，并且防火墙可以检查流量。如果您拒绝附件，则该附件将进入已拒绝状态，最终将被删除。

查看 AWS 公交 Gateway 网络功能附件

您可以使用 Amazon VPC 控制台或网络管理器控制台查看您的网络功能 AWS Network Firewall 附件，包括您的附件，以直观地呈现您的网络拓扑。

使用网络管理器控制台查看网络功能附件

您可以使用网络管理器控制台查看网络功能附件。

在网络管理器中查看防火墙附件

1. 在家中打开网络管理器控制台 https://console.aws.amazon.com/networkmanager//。
2. 如果您还没有全球网络，请在网络管理器中创建全球网络。
3. 向网络管理器注册您的传输网关。
4. 在 “全球网络” 下，选择连接所在的全球网络。
5. 在导航窗格中，选择 Transit gateways（中转网关）。
6. 选择要查看其附件的公交网关。
7. 选择拓扑树视图。Network Firewall 附件带有网络功能图标。
8. 要查看有关特定防火墙连接的详细信息，请在拓扑视图中选择传输网关，然后选择网络功能选项卡。

Network Manager 控制台提供有关您的防火墙附件的详细信息，包括其状态、关联的传输网关和可用区。

使用 Amazon VPC 控制台控制台查看网络功能附件

使用 VPC 控制台查看您的中转网关连接类型列表。

使用 VPC 控制台查看传输网关连接类型

- 请参阅查看 VPC 连接。

通过 Transi AWS t Gateway 网络功能附件路由流量

创建网络功能附件后，您需要更新您的传输网关路由表，以便使用 Amazon VPC 控制台或 CLI 通过防火墙发送流量进行检查。有关更新公交网关路由表关联的步骤，请参阅关联中转网关路由表。

使用控制台通过防火墙附件路由流量

使用 Amazon VPC 控制台通过传输网关网络功能附件路由流量。

使用控制台通过网络功能附件路由流量

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择传输网关。
3. 选择公交网关路由表。
4. 选择要修改的路由表。
5. 选择操作，然后选择创建静态路由。
6. 对于 CIDR，请输入路由的目标 CIDR 块。
7. 对于 “附件”，选择网络功能附件。例如，这可能是 AWS Network Firewall 附件。
8. 选择 Create static route（创建静态路由）。

> **Note**
>
> 仅支持静态路由。

现在，与您的路由表中 CIDR 块匹配的流量将被发送到防火墙附件进行检查，然后再转发到最终目的地。

使用 CLI 或 API 通过网络功能附件路由流量

使用命令行或 API 路由传输网关网络功能附件。

使用命令行或 API 通过网络功能附件路由流量

- 使用 `create-transit-gateway-route`。

例如，请求可能是路由网络防火墙附件：

```
aws ec2 create-transit-gateway-route \
  --transit-gateway-route-table-id tgw-rtb-0123456789abcdef0 \
  --destination-cidr-block 0.0.0.0/0 \
  --transit-gateway-attachment-id tgw-attach-0123456789abcdef0
```

然后输出返回：

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

现在，与您的路由表中 CIDR 块匹配的流量将被发送到防火墙附件进行检查，然后再转发到最终目的地。

AWS Site-to-Site VPN 亚马逊 VPC 传输网关中的附件

您可以将 Site-to-Site VPN 附件连接到 Amazon VPC 传输网关中的传输网关，从而连接您的网络 VPCs 和本地网络。既支持动态路由，也支持静态路由，还支持 IPv4 和 IPv6。

要求

- 将 VPN 连接连接到中转网关需要指定 VPN 客户网关，必须指定具有特定设备要求的 VPN 客户网关。在创建 Site-to-Site VPN 连接之前，请查看客户网关要求以确保您的网关设置正确。有关这些要求的更多信息（包括网关配置文件示例），请参阅《AWS Site-to-Site VPN 用户指南》中的 Site-to-Site VPN 客户网关设备的要求。

- 对于静态路由 VPNs，您还需要先将静态路由添加到公交网关路由表中。VPN 不会过滤传输网关路由表中以 VPN 连接为目标的静态路由，因为在使用基于 BGP 的 Site-to-Site VPN 时，这可能会允许意外的出站流量流动。请参阅 创建静态路由，了解将静态路由添加到中转网关路由表的步骤。

您可以使用 Amazon VPC 控制台或 AWS CLI 创建、查看或删除传输网关 VP Site-to-Site N 附件。

任务

- 使用 Amazon VPC 中转网关创建与 VPN 的中转网关连接
- 使用 Amazon VPC Transit Gateways 查看 VPN 连接
- 使用 Amazon VPC 中转网关删除 VPN 连接

使用 Amazon VPC 中转网关创建与 VPN 的中转网关连接

使用控制台创建 VPN 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Create Transit Gateway Attachment（创建中转网关连接）。
4. 对于 Transit Gateway ID（中转网关 ID），选择要用于连接的中转网关。您可以选择自己拥有的中转网关。
5. 对于 Attachment type（连接类型），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为 NAT 遍历（NAT-T）而启用的网络地址转换（NAT）设备后面，请使用您的 NAT 设备的公有 IP 地址，并调整防火墙规则以取消阻止 UDP 端口 4500。
   - 要创建客户网关，选择 New（新建），然后对于 IP 地址，键入静态 IP 地址和 BGP ASN。

     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 Site-to-Site VPN 路由选项。
7. 对于 Tunnel Options（隧道选项），请为隧道输入 CIDR 范围和预共享密钥。有关更多信息，请参阅 Site-to-Site VPN 架构。
8. 选择 Create Transit Gateway Attachment（创建中转网关连接）。

要创建 VPN 附件，请使用 AWS CLI

使用 create-vpn-connection 命令。

使用 Amazon VPC Transit Gateways 查看 VPN 连接

使用控制台查看 VPN 挂载

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关挂载）。
3. 在 Resource type（资源类型）栏，寻找 VPN。这些是 VPN 挂载。
4. 选择挂载以查看其详细信息或添加标签。

要查看您的 VPN 附件，请使用 AWS CLI

使用 describe-transit-gateway-attachments 命令。

使用 Amazon VPC 中转网关删除 VPN 连接

使用控制台删除 VPN 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 VPN 连接。
4. 选择 VPN 连接的资源 ID 以导航到 VPN 连接页。
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）。

要删除 VPN 附件，请使用 AWS CLI

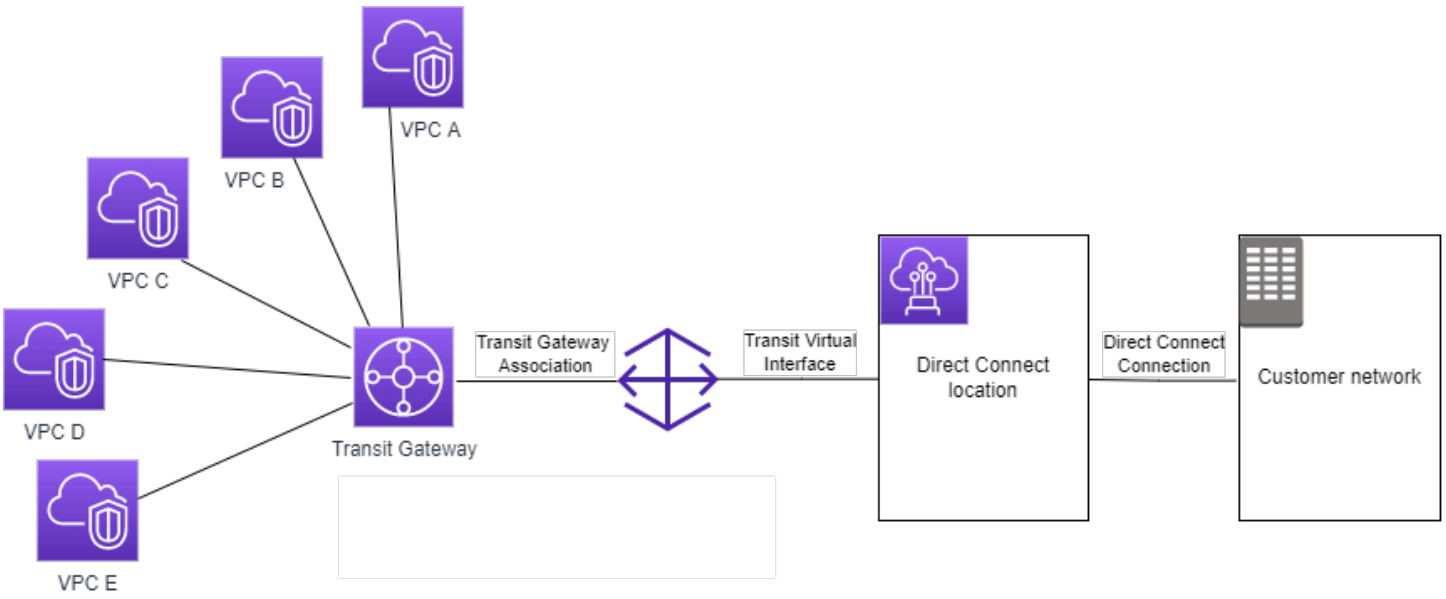
使用 delete-vpn-connection 命令。

Amazon VPC Transit Gateways 中与 Direct Connect 网关的中转网关连接

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 VPC Transit Gateways 中的中转网关对等节点连接

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连接，然后指定中转网关。对等传输网关可以在您的账户中，也可以来自其他账户。您也可以请求将对等连接从自己的账户发送到另一个账户的传输网关。

创建对等连接连接请求后，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连接的静态路由。

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有或私 IPv4 有 IPv4 DNS 主机名解析为 Amazon Route 53 Resolver 中转网关对等连接两 VPCs 侧的私有地址。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？。

区域间网关对等连接使用与 VPC 对等连接相同的网络基础设施。因此，当流量在区域之间传输时，在虚拟网络层将使用 AES-256 加密技术进行加密。在其经过超出 AWS物理控制范围的网络链路时，也会在物理层使用 AES-256 加密技术进行加密。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，请参阅管理 AWS 区域。在这些区域中使用中转网关对等连接时，请考虑以下事项：

- 只要接受对等连接连接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
- 删除中转网关连接时，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连接。如果不删除对等连接连接，流量可能会继续通过连接，并继续产生费用。如果您不删除连接，则可以选择重新加入，然后删除连接。
- 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连接，您可能会在接受连接的区域（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 Transit Gateways 创建对等节点连接
- 使用 Amazon VPC Transit Gateways 接受或拒绝对等节点连接请求
- 使用 Amazon VPC Transit Gateways 将路由添加到中转网关路由表
- 使用 Amazon VPC Transit Gateways 删除对等节点连接

使用 Amazon VPC Transit Gateways 创建对等节点连接

在开始之前，请确保您获得了所要连接的中转网关的 ID。如果传输网关位于另一个 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Create Transit Gateway Attachment（创建中转网关连接）。
4. 对于 Transit Gateway ID（中转网关 ID），选择要用于连接的中转网关。您可以选择自己拥有的中转网关。与您共享的中转风关不能用于对等节点。
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)。

要使用创建对等连接附件 AWS CLI

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

使用 Amazon VPC Transit Gateways 接受或拒绝对等节点连接请求

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 将路由添加到中转网关路由表

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Create static route (创建静态路由) 页面上，输入为其创建路由的 CIDR 块。例如，指定连接到对等中转网关的 VPC 的 CIDR 块。
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 Transit Gateways 删除对等节点连接

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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)。

要删除对等互连附件，请使用 AWS CLI

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

在 Amazon VPC 传输网关中连接附件和连接对等体

您可以创建中转网关 Connect 挂载，以便在 VPC 中运行的中转网关和第三方虚拟设备（例如 SD-WAN 设备）之间建立连接。Connect 挂载支持通用路由封装 (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 挂载后，您可以在 Connect 挂载上创建一个或多个 GRE 隧道（也称为 中转网关 Connect 对等节点）以连接中转网关和第三方设备。您可以通过 GRE 隧道建立两个 BGP 会话以交换路由信息。

> **Important**
>
> Transit Gateway Connect 对等体由两个 BGP 对等会话组成，这些会话在托管基础设施上 AWS终止。两个 BGP 对等会话提供路由层冗余，以确保丢失一个 BGP 对等会话不会影响您

的路由操作。从两个 BGP 会话接收到的路由信息将累积到给定的 Connect 对等节点。两个 BGP 对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，所导致的中断。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，则在基础设施运行期间 AWS ，它可能会暂时失去连接。我们强烈建议您在 Connect 对等节点上配置两个BGP 对等会话。如果您已配置多个 Connect 对等节点以支持设备端的高可用性，我们建议您在每个 Connect 对等节点上配置两个 BGP 对等会话。

Connect 挂载使用现有的 VPC 或 Direct Connect 挂载作为基础传输机制。该挂载被称为运输挂载。Transit Gateway将来自第三方设备的匹配 GRE 数据包标识为来自 Connect 挂载的流量。它将任何其他数据包（包括具有不正确源或目标信息的 GRE 数据包）视为传输挂载中的流量。

> **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 对等节点（GRE 隧道）由以下组件组成。

CIDR 块内部（BGP 地址）

用于 BGP 对等连接的内部 IP 地址。您必须从的`169.254.0.0/16`范围中指定 /29 CIDR 块。 IPv4 您可以选择从的`fd00::/8`范围中指定 /125 CIDR 块。 IPv6以下 CIDR 块由系统保留，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 块为 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Transit Gateway的所有隧道中，BGP 地址必须是唯一的。

对等 IP 地址

Connect 对等节点设备侧的对等 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 对等节点中转网关侧的对等 IP 地址（GRE 外部 IP 地址）。必须从Transit Gateway CIDR 块中指定 IP 地址，并且该地址在Transit Gateway的 Connect 挂载中必须是唯一的。如果您没有指定 IP 地址，我们将使用Transit Gateway CIDR 块中的第一个可用地址。

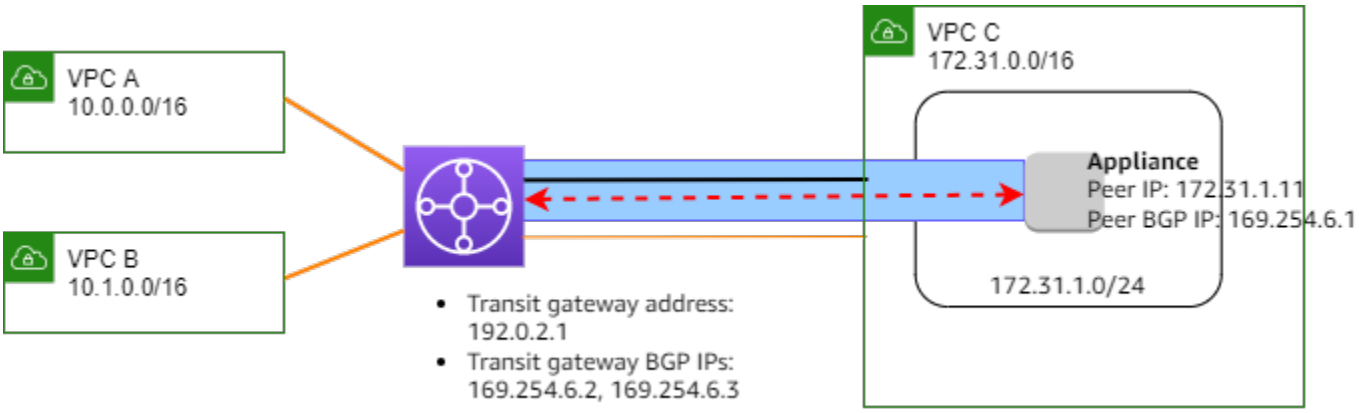
您可以在创建或修改Transit Gateway时添加Transit Gateway CIDR 块。

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Transit Gateway地址用于唯一地标识 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。

适用于 BGP 对等的 Transit Gateway Connect 仅支持多协议 BGP (MP-BGP)，在这种多协议 BGP (MP-BGP) 中，还需要 IPv4 单播寻址才能为单播建立 BGP 会话。 IPv6 您可以同时使用 IPv4 和 IPv6 地址作为 GRE 外部 IP 地址。

以下示例显示了Transit Gateway和 VPC 中的设备之间的 Connect 挂载。



图组件	描述
	VPC 挂载
	Connect 连接

图组件	描述
	GRE 隧道（Connect 对等节点）
	BGP 对等会话

在前面的示例中，在现有 VPC 挂载（传输挂载）上创建了一个 Connect 挂载。在 Connect 挂载上创建 Connect 对等节点，以建立与 VPC 中的设备的连接。Transit Gateway地址为 `192.0.2.1`，BGP 地址的范围为 `169.254.6.0/29`。范围中的第一个 IP 地址 (`169.254.6.1`) 在设备上被配置为对等 BGP IP 地址。

VPC C 的子网路由表有一个路由，该路由将发往Transit Gateway CIDR 块的流量指向Transit Gateway。

目的地	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 挂载的信息，请参阅 AWS Transit Gateway 常见问题解答。
- 必须将第三方设备配置为使用 Connect 挂载通过 GRE 隧道在Transit Gateway之间发送和接收流量。
- 必须将第三方设备配置为使用 BGP 进行动态路由更新和运行状况检查。
- 支持以下类型的 BGP：
  - 外部 BGP (eBGP)：用于连接到位于不同于Transit Gateway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 2。
  - 内部 BGP (iBGP)：用于连接到位于与 Transit Gateway 相同的自治系统的路由器。传输网关不会安装来自 iBGP 对等体（第三方设备）的路由，除非这些路由源自 eBGP 对等体并且应该已 next-hop-self配置。第三方设备通过 iBGP 对等连接发布的路由必须具有 ASN。

  - MP-BGP（BGP 的多协议扩展）：用于支持多种协议类型，例如和地址族。 IPv4 IPv6
- 默认 BGP 保持连接超时为 10 秒，默认的保持计时器为 30 秒。
- IPv6 不支持 BGP 对等互连；仅支持 IPv4基于 BGP 对等互连。 IPv6 使用 MP-BGP 通过 IPv4 BGP 对等互连交换前缀。
- 不支持双向转发检测 (BFD)。
- 不支持 BGP 平稳重启。
- 创建Transit Gateway对等节点时，如果您没有指定对等节点 ASN 编号，我们将选择Transit Gateway ASN 编号。这意味着您的设备和Transit Gateway将位于执行 iBGP 的同一个自治系统中。
- 当您有两个 Connect 对等节点时，使用 BGP AS-PATH 属性的 Connect 对等节点是首选路由。

  要在多个设备之间使用相同成本的多路径 (ECMP) 路由，您必须将设备配置为使用相同的 BGP AS-PATH 属性向Transit Gateway发布相同的前缀。要使Transit Gateway选择所有可用的 ECMP 路径，AS-PATH 和自治系统号 (ASN) 必须匹配。中转网关可以在同一 Connect 挂载的 Connect 对等节点之间使用 ECMP，也可以在同一中转网关上的 Connect 挂载之间使用 ECMP。Transit Gateway 不能在单个对等体建立的两个冗余 BGP 对等连接之间使用 ECMP。
- 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。
- 通过减去 GRE 标头（8 字节）和外部 IP 标头（20 字节）开销，将 GRE 隧道 MTU 配置为小于外部接口 MTU。例如，如果您的外部接口 MTU 为 1500 字节，请将 GRE 隧道 MTU 设置为 1472 字节（1500-8-20 = 1472），以防止数据包分段。

任务

- 使用 Amazon VPC Transit Gateways 创建 Connect 连接
- 使用 Amazon VPC Transit Gateways 创建 Connect 对等节点
- 使用 Amazon VPC 中转网关查看 Connect 连接和 Connect 对等节点
- 使用 Amazon VPC Transit Gateways 修改 Connect 连接和 Connect 对等节点
- 使用 Amazon VPC Transit Gateways 删除 Connect 对等节点
- 使用 Amazon VPC Transit Gateways 删除 Connect 连接

使用 Amazon VPC Transit Gateways 创建 Connect 连接

要创建 Connect 连接，您必须将现有连接指定为传输连接。您可以将 VPC 连接或 Direct Connect 连接指定为传输连接。

使用控制台创建 Connect 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择“中转网关连接”。
3. 选择 Create Transit Gateway Attachment（创建中转网关连接）。
4. （可选）对于 Name tag（名称标签），为连接指定名称标签。
5. 对于Transit Gateway ID（中转网关 ID），选择要用于连接的中转网关。
6. 对于 Attachment type（连接类型），选择 Connect（连接）。
7. 对于 Transport Attachment ID（传输连接 ID），选择现有连接（传输连接）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 Amazon VPC Transit Gateways 创建 Connect 对等节点

您可以为现有的 Connect 连接创建 Connect 对等节点（GRE 隧道）。在开始之前，请确保已配置中转网关 CIDR 块。您可以在创建或修改中转网关时配置中转网关 CIDR 块。

创建 Connect 对等节点时，必须在 Connect 对等节点的设备端指定 GRE 外部 IP 地址。

要使用控制台创建 Connect 对等节点

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择“中转网关连接”。
3. 选择 Connect 连接，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）对于 Transit Gateway GRE Address（中转网关 GRE 地址），为中转网关指定 GRE 外部 IP 地址。默认情况下，使用中转网关 CIDR 块中的第一个可用地址。
6. 对于“对等节点 GRE 地址”，为 Connect 对等节点的设备端指定 GRE 外部 IP 地址。
7. 对于 BGP 内部 CIDR 块 IPv4，请指定用于 BGP 对等的内部 IPv4 地址范围。从 `169.254.0.0/16` 范围中指定 /29 CIDR 块。
8. （可选）对于 BGP 内部 CIDR 块 IPv6，请指定用于 BGP 对等的内部 IPv6 地址范围。从 `fd00::/8` 范围中指定 /125 CIDR 块。

9. （可选）对于 Peer ASN（对等节点 ASN），为设备指定边界网关协议（BGP） 自治系统编号（ASN）。您可以使用指定给您的网络的现有 ASN。如果您没有 ASN，您可以使用 64512–65534（16 位 ASN）或 4200000000–4294967294（32 位 ASN）范围内的私有 ASN。

   默认值与Transit Gateway的 ASN 相同。如果将对等 ASN 配置为与传输网关 ASN (eBGP) 不同，则必须将 ebgp-multihop 配置为 2。 time-to-live
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 Amazon VPC 中转网关查看 Connect 连接和 Connect 对等节点

查看您的 Connect 连接和 Connect 对等节点。

要使用控制台查看 Connect 连接和 Connect 对等节点

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择“中转网关连接”。
3. 选择 Connect 连接。
4. 要查看 Connect 连接对等节点，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 Amazon VPC Transit Gateways 修改 Connect 连接和 Connect 对等节点

您可以修改 Connect 连接的标签。

要使用控制台修改 Connect 连接标签

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Connect 连接，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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateway Attachments（中转网关连接）。
3. 选择 Connect 连接，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 连接和 Connect 对等节点标签

使用 create-tags 和 delete-tags 命令

使用 Amazon VPC Transit Gateways 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择“中转网关连接”。
3. 选择 Connect 连接。
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 Amazon VPC Transit Gateways 删除 Connect 连接

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

要使用控制台删除 Connect 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择“中转网关连接”。
3. 选择 Connect 连接，然后选择 Actions（操作）、Delete Transit Gateway attachment（删除 Transit Gateway连接）。
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 VPC 中转网关中的中转网关路由表

使用中转网关路由表为中转网关连接配置路由。路由表是一个包含规则的表，这些规则用于指导您的 VPCs和 VPNs之间的网络流量路由方式。此表中的每个路由都包含您希望将流量发送到的目的地的 IP 地址范围。

中转网关路由表让您可以将表与中转网关连接关联。支持 VPC、VPN、Direct Connect 网关、对等连接和 Connect 连接。关联后，这些连接的路由会从连接传播到目标中转网关路由表。一个连接可以传播到多个路由表。

此外，您还可以使用路由表创建和管理静态路由。例如，可以让一个静态路由充当备份路由，以防发生影响任何动态路由的网络中断。

任务

- 使用 Amazon VPC Transit Gateways 创建中转网关路由表
- 使用 Amazon VPC 中转网关查看中转网关路由表
- 使用 Amazon VPC 中转网关关联中转网关路由表
- 使用 Amazon VPC Transit Gateways 删除中转网关路由表的关联
- 使用 Amazon VPC 中转网关启用路由传播到中转网关路由表
- 使用 Amazon VPC 中转网关禁用路由传播

- 使用 Amazon VPC 中转网关创建静态路由
- 使用 Amazon VPC Transit Gateways 删除静态路由
- 使用 Amazon VPC 中转网关替换静态路由
- 使用 Amazon VPC Transit Gateways 将路由表导出到 Amazon S3
- 使用 Amazon VPC 中转网关删除中转网关路由表
- 使用 Amazon VPC Transit Gateways 创建路由表前缀列表引用
- 使用 Amazon VPC 中转网关修改前缀列表引用
- 使用 Amazon VPC Transit Gateways 删除前缀列表引用

使用 Amazon VPC Transit Gateways 创建中转网关路由表

使用控制台创建中转网关路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC 中转网关查看中转网关路由表

使用控制台查看中转网关路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC 中转网关关联中转网关路由表

您可以将中转网关路由表与中转网关连接相关联。

使用控制台关联中转网关路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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. 选择要关联的连接，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 VPC Transit Gateways 删除中转网关路由表的关联

您可以取消中转网关路由表与中转网关连接的关联。

使用控制台取消中转网关路由表关联

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

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. 选择要解除关联的连接，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 VPC 中转网关启用路由传播到中转网关路由表

使用路由传播将连接中的路由添加到路由表。

将路由传播到中转网关连接路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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，选择连接。
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 中转网关禁用路由传播

从路由表连接删除传播的路由。

使用控制台禁用路由传播

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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. 选择连接，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 中转网关创建静态路由

为 VPC、VPN 或中转网关对等连接连接创建静态路由，也可以创建一个删除与该路由匹配的流量的黑洞路由。

VPN 不会过滤传输网关路由表中以 VPN 连接为目标的 Site-to-Site静态路由。当使用基于 BGP 的 VPN 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Create static route（创建静态路由）页面上，输入为其创建路由的 CIDR 块，然后选择 Active（激活）。
6. 为路由选择连接。
7. 选择 Create static route（创建静态路由）。

使用控制台创建黑洞路由

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Create static route（创建静态路由）页面上，输入为其创建路由的 CIDR 块，然后选择 Blackhole（黑洞）。
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 Transit Gateways 删除静态路由

删除中转网关路由表中的静态路由。

使用控制台删除静态路由

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 中转网关替换静态路由

将中转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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Amazon VPC Transit Gateways 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。路由将以 JSON 文件格式保存到指定的 Amazon S3 存储桶。

使用控制台导出中转网关路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 JSON 文件的示例，其中包含 VPC 附件的两个传播路由的相关信息。

```
{
  "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 VPC 中转网关删除中转网关路由表

使用控制台删除中转网关路由表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 创建路由表前缀列表引用

您可以在中转网关路由表中引用前缀列表。前缀列表是包含您定义和管理的一个或多个 CIDR 块条目的集合。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。如果需要删除目标 CIDR 块，则可以从前缀列表中删除其条目，而不是从每个受影响的路由表中删除路由。

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。

使用控制台创建前缀列表引用

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 连接 ID），选择要将流量路由到的连接的 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 中转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连接，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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

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 连接 ID），选择要将流量路由到的连接的 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 Transit Gateways 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 中的中转网关策略表

中转网关动态路由使用策略表来为 AWS 云广域网络路由网络流量。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**
>
> 在创建中转网关对等连接时，目前仅在云广域网络中支持中转网关策略表。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。
> 有关云广域网络中对等连接的更多信息，请参阅《AWS 云广域网络用户指南》中的对等连接。

任务

- 使用 Amazon VPC Transit Gateways 创建中转网关策略表
- 使用 Amazon VPC Transit Gateways 删除中转网关策略

使用 Amazon VPC Transit Gateways 创建中转网关策略表

使用控制台创建中转网关策略表

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 删除中转网关策略

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 中转网关中的组播

组播是一种通信协议，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

组播概念

以下是组播的主要概念：

- 组播域 — 允许将一个组播网络分段成不同的域，并将中转网关用作组播路由器。您可以在子网级别定义组播域成员资格。
- 组播组 — 识别一组将发送和接收相同组播流量的主机。组播组由组 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) — 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 IGMP 协议加入、离开和发送消息的主机。 AWS 支持 IGMPv2 协议以及 IGMP 和静态（基于 API）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。组播源仅适用于静态源配置。

  静态源组播域包含不使用 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。静态添加的源发送组播流量，成员接收组播流量。
- 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。组播组具有多个组成员。在静态源组成员资格配置中，组播组成员只能接收流量。在 IGMP 组配置中，成员既可以发送流量，也可以接收流量。

注意事项

- Transit Gateway 多播可能不适合高频交易或对性能敏感的应用程序。我们强烈建议您查看多播配额以了解限制。请联系您的客户或解决方案架构师团队，详细了解您的性能要求。
- 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组播。
- 组播组成员资格使用 Amazon Virtual Private Cloud Console 或或 IGMP AWS CLI进行管理。
- 一个子网只能位于一个组播域中。
- 如果您使用非 Nitro 实例，则必须禁用 Source/Dest (源/目标) 检查。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 实例不能是组播发送方。
- 不支持通过 Site-to-Site VPN AWS Direct Connect、对等连接或传输网关 Connect 附件进行多播路由。

- 中转网关不支持组播数据包分段。分段组播数据包会被丢弃。有关更多信息，请参阅 最大传输单元 (MTU)。
- 启动时，一台 IGMP 主机会发送多个 IGMP JOIN 加入多播组的消息（通常重试 2 到 3 次）。在不太可能的情况下，所有 IGMP JOIN 消息丢失，主机将不会成为传输网关组播组的一部分。在这种情况下，你需要重新触发 IGMP JOIN 使用特定于应用程序的方法从主机发送的消息。
- 群组成员资格始于收到 IGMPv2 JOIN 由中转网关发送的消息，并以收到消息结尾 IGMPv2 LEAVE 消息。中转网关会跟踪成功加入组播组的主机。作为云组播路由器，传输网关会发出 IGMPv2 QUERY 每两分钟向所有成员发送一次消息。每个成员发送一个 IGMPv2 JOIN 回复消息，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。一个明确的 IGMPv2 LEAVE message 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组播组的主机。如果中转网关出现故障，传输网关将在上次成功执行 IGMP 后的七分钟（420 秒）内继续向主机发送组播数据 JOIN 消息。传输网关会继续向主机发送成员资格查询长达 12 小时或直到它收到 IGMP LEAVE 来自主持人的消息。
- 中转网关将成员资格查询数据包发送给所有 IGMP 成员，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 为 0.0.0.0/32，目标 IP 为 224.0.0.1/32，协议为 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同一 VPC 中时，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 VPC Transit 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。动态组播不支持。

组播路由

在中转网关上启用组播时，它将充当组播路由器。当您将子网添加到某个组播域时，我们会将所有组播流量发送到与该组播域关联的中转网关。

网络 ACLs

网络 ACL 规则在子网级别运行。它们将应用于组播流量，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。

对于互联网组管理协议（IGMP）组播流量，您必须至少具有以下入站规则。远程主机是发送组播流量的主机。

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	入站组播流量

对于 IGMP，您必须至少具有以下出站规则。

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)	组播组 IP 地址	IGMP 加入
自定义 UDP 协议	UDP	组播组 IP 地址	出站组播流量

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组播流量。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 组播流量，您必须至少具有以下入站规则。远程主机是发送组播流量的主机。您不能将安全组指定为 UDP 入站规则的源。

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	入站组播流量

对于 IGMP 组播流量，您必须至少具有以下出站规则。

类型	协议	目的地	描述
自定义协议	2	224.0.0.2/32	IGMP 离开

类型	协议	目的地	描述
自定义协议	2	组播组 IP 地址	IGMP 加入
自定义 UDP 协议	UDP	组播组 IP 地址	出站组播流量

Amazon VPC Transit Gateways 中的组播域

组播域允许将一个组播网络分段分成不同域。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。 在至少有一个成员使用 IGMP 协议时启用此属性。成员通过以下方式之一加入多播组： • 支持 IGMP 的成员使用 `JOIN` 和 `LEAVE` 消息。 • 必须使用 Amazon VPC 控制台或 AWS CLI在组中添加或删除不支持 IGMP 的成员。 如果您注册多播组成员，则必须将其取消注册。中转网关将忽略手动添加的组成员发送的 IGMP `LEAVE` 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 传输网关创建 IGMP 组播域

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

要使用控制台创建 IGMP 组播域

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
3. 选择 Create transit gateway multicast domain（创建中转网关组播域）。
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），选择处理组播流量的中转网关。
6. 要获得IGMPv2 支持，请选中该复选框。
7. 对于静态源支持，请清除该复选框。
8. 要自动接受此组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（创建中转网关组播域）。

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 VPC 传输网关创建静态组播域

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

要使用控制台创建静态多播域

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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. 对于 Static sources support（静态源支持），请选择该复选框。
8. 要自动接受此组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（创建中转网关组播域）。

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 VPC 中转网关将 VPC 连接和子网与组播域关联

使用以下过程将 VPC 连接与组播域关联。创建关联时，您可以随后选择要包括在组播域中的子网。

开始之前，您必须先在中转网关上创建 VPC 连接。有关更多信息，请参阅 Amazon VPC Transit Gateways 中的 Amazon VPC 连接。

要使用控制台将 VPC 连接与组播域关联

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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（选择要关联的连接），选择中转网关连接。
5. 对于 Choose subnets to associate（选择要关联的子网），选择要包括在组播域中的子网。
6. 选择 Create association（创建关联）。

使用 VPC 附件与多播域关联 AWS CLI

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

使用 Amazon VPC Transit Gateways 取消关联组播域中的子网

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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）。

使用解除子网的关联 AWS CLI

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

使用 Amazon VPC 中转网关查看组播域关联

查看组播域以验证这些域可用，并且包含了相应的子网和连接。

要使用控制台查看组播域

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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 VPC Transit Gateways 向组播域添加标签

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。

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。

删除使用 Amazon VPC 中转网关的组播域

使用以下过程删除中组播域。

要使用控制台删除组播域

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
3. 选择多播域，然后依次选择 Actions（操作）、Delete multicast domain（删除组播域）。
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 VPC Transit Gateways 中的共享组播域

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，使用者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资源的用户。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

共享组播域的用户可以通过在他们创建的多播域上采用的操作方式，对共享的多播域执行以下操作：

- 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

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。

限额

共享的多播域计入共享用户和所有者的多播域配额。

在 Amazon VPC Transit Gateways 中跨可用区共享资源

为确保资源分配到区域的各可用区，Amazon VPC Transit Gateways 将可用区独立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. 在家中打开https://console.aws.amazon.com/ram/主 AWS RAM机。
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。

Amazon VPC Transit Gateways 共享组播域

当拥有者与您共享组播域时，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。当您使用共享多播域时 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Amazon VPC Transit Gateways 取消共享共享的组播域

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 识别共享的组播域

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 VPC Transit Gateways 将源注册到多播组

> **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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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 IPv6 CID IPv4 R 块或 CIDR 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)。

要注册来源，请使用 AWS CLI

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

使用 Amazon VPC Transit Gateways 取消注册组播组中的成员

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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 IPv6 CID IPv4 R 块或 CIDR 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 Amazon VPC Transit Gateways 取消注册组播组中的源

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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 Amazon VPC Transit Gateways 取消注册组播组中的成员

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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

2. 在导航窗格中，选择中转网关组播。
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 Transit Gateways 查看组播组

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。当 AWS 发现使用该协议的@@ 成员时，成员类型MemberType（在控制台中 AWS CLI）或（中）会显示 IGMP。

使用控制台查看多播组

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择中转网关组播。
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 协议发现了多播组成员。

```
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 Amazon VPC Transit Gateways 中为 Windows Server 设置组播

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 代替 TCP/IP 堆栈： IGMPv3

   ```
   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 是组播支持的版本，因此该属性 `Value` 必须为 3。您可运行以下命令将 IGMP 版本设置为 2，而无需编辑 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的 UDP 端口：

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

4. 重启实 EC2 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 Transit Gateways 管理 IGMP 配置

本示例显示至少有一台主机将 IGMP 协议用于多播流量时， AWS 会在收到来自实例的 IGMP JOIN 消息时自动创建多播组，然后将该实例添加为该组中的成员。您也可以使用将非 IGMP 主机作为成员静态添加至群组。 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 VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
2. 在 VPC 中创建子网。有关更多信息，请参阅 Amazon VPC 用户指南中的创建子网。
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 连接。有关更多信息，请参阅 the section called “创建 VPC 连接”。
5. 创建为 IGMP 支持配置的多播域。有关更多信息，请参阅 the section called “创建 IGMP 组播域”。

   使用以下设置：

   - 启用IGMPv2 支持。
   - 禁用 Static sources support（静态源支持）。
6. 在中转网关 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 连接和子网与组播域关联”。
7. 的默认 IGMP 版本 EC2 为 IGMPv3。您需要更改所有 IGMP 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 IGMP 协议的成员添加到多播组。有关更多信息，请参阅 the section called “将成员注册到多播组”。

示例：使用 Amazon VPC 传输网关管理静态源配置

此示例介绍如何将组播源静态添加到群组。主机不使用 IGMP 协议加入或退出组播组。您需要静态添加接收组播流量的组成员。

使用以下步骤完成配置：

1. 创建 VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。

2. 在 VPC 中创建子网。有关更多信息，请参阅 Amazon VPC 用户指南中的创建子网。
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 连接。有关更多信息，请参阅 the section called “创建 VPC 连接”。
5. 创建配置为不支持 IGMP 的多播域，并支持静态添加源。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，位于与组播域关联的子网中的任何实例都可以发送组播流量，组成员将接收组播流量。
6. 在中转网关 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 连接和子网与组播域关联”。
7. 如果您启用 Static sources support（静态源支持），请将源添加到组播组。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 Transit Gateways 中管理静态组成员配置

此示例显示静态地将多播成员添加到组中。主机不能使用 IGMP 协议加入或退出多播组。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 VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
2. 在 VPC 中创建子网。有关更多信息，请参阅 Amazon VPC 用户指南中的创建子网。
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 连接。有关更多信息，请参阅 the section called “创建 VPC 连接”。
5. 创建配置为不支持 IGMP 的多播域，并支持静态添加源。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. 在中转网关 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 连接和子网与组播域关联”。
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 中转网关流日志

利用 Amazon VPC 中转网关中的流日志功能，您可以获取传入和传出您的中转网关的 IP 流量信息。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 “中转网关流日志记录”中所述。如果您想捕获有关进出您的网络接口的 IP 流量的信息 VPCs，请使用 VPC 流日志。请参阅《Amazon VPC 用户指南》中的使用 VPC 流日志记录 IP 流量。

> **Note**
>
> 您必须是中转网关的所有者，才能创建中转网关流日志。如果您不是中转网关所有者，则该中转网关的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 中转网关流日志记录。

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。

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 Transit Gateways 流日志记录。

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：

- 创建发布到日志的流 CloudWatch 日志
- 创建发布到 Amazon S3 的流日志
- 创建发布到 Firehose 的流日志

限制

中转网关流日志存在以下限制：

- 不支持组播流量。
- 不支持 Connect 连接。所有 Connect 流日志都显示在传输连接下方，因此必须在中转网关或 Connect 传输连接上启用它。

中转网关流日志记录

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
- 自定义格式
- 可用字段

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，则所有字段均为类型 STRING。 如果格式为 Parquet，请参阅表格以了解字段数据类型。

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。 Parquet 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. Parquet 数据类型：STRING	6
account-id	源传输网关所有者的 AWS 账户 ID。 Parquet 数据类型：STRING	2
tgw-id	正在记录其流量的中转网关的 ID。 Parquet 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。 Parquet 数据类型：STRING	6
tgw-src-vpc-account-id	源 VPC 流量的 AWS 账户 ID。	6

字段	描述	版本
	Parquet 数据类型：STRING	
tgw-dst-vpc-account-id	目标 VPC 流量的 AWS 账户 ID。 Parquet 数据类型：STRING	6
tgw-src-vpc-id	中转网关的源 VPC 的 ID。 Parquet 数据类型：STRING	6
tgw-dst-vpc-id	中转网关的目标 VPC 的 ID。 Parquet 数据类型：STRING	6
tgw-src-subnet-id	中转网关源流量的子网 ID。 Parquet 数据类型：STRING	6
tgw-dst-subnet-id	中转网关目标流量的子网 ID。 Parquet 数据类型：STRING	6
tgw-src-eni	流的源中转网关连接 ENI 的 ID。 Parquet 数据类型：STRING	6
tgw-dst-eni	流的目标中转网关连接 ENI 的 ID。 Parquet 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。 Parquet 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。 Parquet 数据类型：STRING	6

字段	描述	版本
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。 Parquet 数据类型：STRING	6
srcaddr	传入流量的源地址。 Parquet 数据类型：STRING	2
dstaddr	传出流量的目标地址。 Parquet 数据类型：STRING	2
srcport	流量的源端口。 Parquet 数据类型：INT_32	2
dstport	流量的目标端口。 Parquet 数据类型：INT_32	2
protocol	流量的 IANA 协议编号。有关更多信息，请参阅分配的 Internet 协议编号。 Parquet 数据类型：INT_32	2
packets	在流中传输的数据包的数量。 Parquet 数据类型：INT_64	2
bytes	在流中传输的字节数。 Parquet 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。 Parquet 数据类型：INT_64	2

字段	描述	版本
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。 Parquet 数据类型：INT_64	2
log-status	流日志的状态： • OK — 数据正常记录到选定目标。 • NODATA — 聚合时间间隔内没有传入或传出网络接口的网络流量。 • SKIPDATA — 在聚合时间间隔内跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。 Parquet 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。 Parquet 数据类型：STRING	3
packets-lost-no-route	由于未指定路由而丢失的数据包。 Parquet 数据类型：INT_64	6
packets-lost-blackhole	数据包由于黑洞而丢失。 Parquet 数据类型：INT_64	6
packets-lost-mtu-exceeded	由于大小超过 MTU 而丢失的数据包。 Parquet 数据类型：INT_64	6
packets-lost-ttl-expired	由于的过期，数据包丢失 time-to-live。 Parquet 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，标记值为 0，而不是 16。 有关 TCP 标志的一般信息（例如 FIN、SYN 和 ACK 等标志的含义），请参阅 Wikipedia 上的 TCP 分段结构。 在聚合时间间隔内，TCP 标志可以是 OR-ed。对于短连接，标志必须在与流日志记录相同的行上设置，例如，对于 SYN-ACK 和 FIN 的 19，以及对于 SYN 和 FIN 的 3。 Parquet 数据类型：INT_32	3
region	包含记录其流量的中转网关的区域。 Parquet 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. Parquet 数据类型：STRING	5

字段	描述	版本
pkt-src-aws-service	如果源 IP 地址用于https://docs.aws.amazon.com/vpc/latest/userguide/aws-ip-ranges.html服务，则为 srcaddr 如果源 IP 地址用于 AWS 服务。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. Parquet 数据类型：STRING	5
pkt-dst-aws-service	如果源 IP 地址用于 服务，则为 dstaddr 字段，如果目标 IP 地址用于 AWS 服务。有关可能的值的列表，请查看 pkt-src-aws-service 字段中返回的子位置类型。 Parquet 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 Amazon EC2 API 参考中的授予 IAM 用户访问亚马逊 EC2 资源的必要权限。

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": "*"
```

```
    }
  ]
}
```

还需要一些额外的 IAM 角色和权限配置，具体取决于您发布到 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 Amazon S3 中的 Transit Gateways 流日志记录 。

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 VPC Transit Gateways 流日志创建或更新 IAM 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. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
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 Add permissions（添加权限），选择 Create inline policy（创建内联策略），然后选择 JSON 选项卡。
7. 从 用于将流日志发布到 CloudWatch 日志的 IAM 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 Summary（总结）页面上，记录您的角色的 ARN。创建流日志时需要此 ARN。

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 CloudWatch 日志后，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。

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。Ingesti onTime 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 CloudWatch 日志用户指南中的发送到 CloudWatch 日志的日志。

内容

- 用于将流日志发布到 CloudWatch 日志的 IAM 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

用于将流日志发布到 CloudWatch 日志的 IAM 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。IAM 角色必须属于您的 AWS 账户。

附加到您的 IAM 角色的 IAM policy 必须至少包括以下权限。

```
{
  "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。源帐户是流日志的所有者，并且源 ARN 是流日志 ARN。如果您不知道流日志 ID，则可以用通配符（*）替换 ARN 的该部分，然后在创建流日志后更新策略。

```
"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

用户还必须有权对与流日志关联的 IAM 角色使用 `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。如果以 IAM 用户身份执行这些步骤，请确保您具有使用 `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。

您可以使用 Amazon VPC 控制台或 AWS CLI 创建亚马逊 CloudWatch 流日志。

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. 选择一个或多个中转网关的复选框，然后选择 Actions（操作）、Creat flow log（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，请指定有权向 CloudWatch 日志发布日志的角色的名称。
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-EC2FlowLog (AWS Tools for Windows PowerShell)

以下 AWS CLI 示例创建了一个用于捕获传输网关信息的流日志。流日志将使用 IAM 角色传送到账户 123456789101 中名为 “ CloudWatch `my-flow-logs`日志” 的日志组。`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 中转网关流日志记录。

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 用户指南中的使用筛选条件根据日志事件创建指标。

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。您要创建一个警报，如果 1 小时内有 10 次或超过 10 次通过 TCP 端口 22（SSH）连接到您的实例的尝试遭到拒绝，该警报将向您发出提醒。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。

为已拒绝的 SSH 流量创建指标筛选条件并为该筛选条件创建警报

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. 选中日志组对应的复选框，然后选择 Actions（操作）、Create metric filter（创建指标筛选条件）。
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. 对于 Notification（通知），选择现有的 SNS 主题，或选择 Create new topic（新建主题）创建一个新主题。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）。

Amazon S3 中的 Transit Gateways 流日志记录

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 S3 用户指南》中的创建桶。

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

- 针对流日志的 Amazon S3 存储桶权限
- 与 SSE-KMS 结合使用时必需的密钥策略
- Amazon S3 日志文件权限
- 为 Amazon Data S3 创建 Transit Gateway 流日志源账户角色
- 创建发布到 Amazon S3 的 Transit Gateway 流日志记录
- 在 Amazon S3 中查看 Transit Gateway 流日志记录
- 已处理的 Amazon S3 中的流日志记录

流日志文件

VPC 流日志功能收集流日志记录，将它们合并到日志文件，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
```

将流日志发布到 Amazon S3 的 IAM 委托人的 IAM policy

创建流日志的 IAM 委托人必须具有以下权限，才能将流日志发布到目标 Amazon S3 存储桶。

```
{
```

```
  "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。这个新的自动生成的策略将附加到原始策略中。

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 简单存储服务用户指南中的存储桶策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
                }
            }
        },
```

```
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl"],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
                }
            }
        }
    ]
}
```

您指定的 ARN *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，并且源 ARN 是日志服务的通配符（*）ARN。

与 SSE-KMS 结合使用时必需的密钥策略

您可以通过启用 Amazon S3 托管式密钥的服务器端加密 (SSE-S3) 或 KMS 密钥的服务器端加密 (SSE-KMS) 来保护 Amazon S3 存储桶中的数据。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 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式密钥并指定客户托管式密钥的 Amazon Resource Name（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。

当您将 SSE-KMS 与客户托管式密钥结合使用时，必须将以下内容添加到密钥的密钥策略（不是 S3 存储桶的存储桶策略）中，以便 VPC 流日志可以写入 S3 存储桶。

> **Note**
>
> 使用 S3 存储桶密钥可通过使用存储桶级密钥将请求减少到 AWS KMS 加密 GenerateDataKey、和解密操作，从而节省 AWS Key Management Service (AWS KMS) 请求成本。根据设计，利用此存储桶级密钥的后续请求不会导致 AWS KMS API 请求或根据密钥策略验证访问权限。 AWS KMS

```
{
    "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 Simple Storage Service 用户指南》 中的访问控制列表（ACL）概述。

为 Amazon Data S3 创建 Transit Gateway 流日志源账户角色

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。您可以使用 Amazon VPC 控制台或 AWS CLI 创建 Amazon S3 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 bucket ARN（S3 存储桶 ARN），指定某个现有 Amazon S3 存储桶的 Amazon Resource Name（ARN）。您可以选择包含子文件夹。例如，要指定名为 `my-logs` 的存储桶中名为 `my-bucket` 的子文件夹，请使用以下 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-EC2FlowLog (AWS Tools for Windows PowerShell)

以下 AWS CLI 示例创建了一个流日志，用于捕获 VPC 的所有中转网关流量，`tgw-00112233344556677`并将流日志传输到名为的 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/'
```

在 Amazon S3 中查看 Transit Gateway 流日志记录

查看发布到 Amazon S3 的流日志记录

1. 打开 Amazon S3 控制台，网址为 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. 对于 Name（名称），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）。

已处理的 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。

Amazon Data Firehose 中的 Transit Gateway Flow 日志记录

主题

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

流日志数据发布到 Firehose 时，会以纯文本格式发布到 Firehose 传输流。您必须先创建 Firehose 传输流。有关创建传输流的步骤，请参阅 Amazon Data Firehose 开发人员指南中的创建 Amazon Data 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。要启用跨账户将流日志传输到 Firehose，您必须在源账户中创建 IAM 角色，并在目的地账户中创建 IAM 角色。

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 流日志源账户角色

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 流日志目的地账户角色

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

创建发布到 Amazon Data Firehose 的 Transit Gateway 流日志记录。确保已经为跨账户传输设置了源和目的地 IAM 账户，并且已创建 Firehose 传输流，然后才能创建流日志。请参阅将流日志发布到 Amazon Data Firehose了解更多信息。您可以使用亚马逊 VPC 控制台或 CLI AWS 创建 Firehose 流日志。

使用控制台创建发布到 Firehose 的中转网关流日志

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Delivery Stream ARN（Firehose 传输流 ARN），选择您创建的要在其中发布流日志的传输流的 ARN。
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 (CLI)AWS
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

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，并将流日志传送到源账户的其他 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
```

使用 APIs 或 CLI 创建和管理 Amazon VPC 传输网关流日志

您可以使用命令行执行此页面上介绍的任务。

使用该create-flow-logs命令时存在以下限制：

- `--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)

描述您的流日志

- describe-flow-logs (AWS CLI)

- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

查看您的流日志记录（日志事件）

- get-log-events (AWS CLI)
- 获取-CWLLog 事件 (AWS Tools for Windows PowerShell)

删除流日志

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

查看 Amazon VPC Transit Gateways 流日志记录

通过 Amazon VPC 查看关于您的中转网关流日志的信息。当您选择该资源时，将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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Transit Gateways 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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 Transit Gateways 流日志记录

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 Transit Gateways 流日志记录

可以使用 Amazon VPC 控制台删除中转网关流日志。

使用这些过程可以禁用资源的流日志服务。删除流日志不会从 CloudWatch 日志中删除现有日志流，也不会删除 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. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
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。

Amazon VPC 传输网关中的指标和事件

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 亚马逊 VPC 传输网关中的指标。

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。

Amazon VPC 流日志

您可以使用 VPC 流日志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 AWS CloudTrail 捕获有关对公交网关 API 的调用的详细信息，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 CloudTrail 日志。

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 亚马逊 VPC 传输网关中的指标

Amazon VPC 将您的中转网关和公交网关附件的数据点发布到亚马 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 VPC 以 60 秒的 CloudWatch 间隔测量并发送其指标。

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中转网关的流量。请参阅 公交网关指标维度 了解支持的维度。

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。

指标	描述
	统计数据：唯一有意义的统计数据是 Sum。
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。
PacketDropCountTTLExpired	由于 TTL 过期而丢弃的数据包数。 统计数据：唯一有意义的统计数据是 Sum。

附件级别和可用区域指标

以下指标适用于中转网关连接。所有连接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连接所有者的账户。连接所有者只能查看其自己连接的指标。有关支持的附件类型的更多信息，请参阅 the section called “资源连接”。

可用区指标可用于在公交网关附件上为可用区域 (AZs) 启用。只有 VPC 附件支持按可用区划分的指标。所有可用区级别的指标都将发布到公交网关所有者的账户。附件的各个可用区指标也会发布到附件所有者的账户。附件所有者只能查看自己附件的每个可用区的指标。

始终报告所有指标。它们的值取决于中转网关连接的入站和/或出站流量。请参阅 公交网关指标维度 了解支持的维度。

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。

指标	描述
BytesIn	中转网关从连接接收的字节数。 统计数据：唯一有意义的统计数据是 Sum。
BytesOut	从中转网关发送到连接的字节数。 统计数据：唯一有意义的统计数据是 Sum。
PacketsIn	中转网关从连接接收的数据包数。 统计数据：唯一有意义的统计数据是 Sum。
PacketsOut	中转网关向连接发送的数据包数。 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。
PacketDropCountTTLExpired	由于 TTL 过期而丢弃的数据包数。 统计数据：唯一有意义的统计数据是 Sum。

公交网关指标维度

使用以下维度筛选公交网关指标数据：

维度	描述
TransitGateway	按中转网关筛选指标数据。

维度	描述
TransitGatewayAttachment	通过中转网关连接筛选指标数据。
TransitGateway ，AvailabilityZone	按传输网关和可用区筛选指标数据。
TransitGatewayAttachment ，AvailabilityZone	按公交网关连接和可用区域筛选指标数据。

使用 AWS CloudTrail记录 Amazon VPC Transit Gateways API 调用

Amazon VPC Transit Gateways 与AWS CloudTrail一项服务集成，该服务提供用户、角色或角色所执行操作的记录 AWS 服务。 CloudTrail 将 Transit Gateway 的所有 API 调用捕获为事件。捕获的调用包括来自 Transit Gateways 控制台的调用和对 Transit Gateways API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向 Transit Gateway 发出的请求、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

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

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 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。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS Management Console 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 AWS CloudTrail Lake”。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

Transit Gateway 管理事件

管理事件提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

Amazon VPC Transit Gateways 将所有 Transit Gateway 控制面板操作记录为管理事件。有关 Transit Gateway 记录到的亚马逊 VPC 传输网关控制平面操作的列表 CloudTrail，请参阅亚马逊 VPC 中转网关 API 参考。

Transiat Gateway 事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 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，因此事件不会按任何特定顺序出现。

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 调用事件，而不仅仅是公交网关 API 调用。您可通过检查是否有包含值 `eventSource` 的 `ec2.amazonaws.com` 元素来查找对中转网关 API 的调用。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公交网关的用户的公交网关 API CloudTrail 日志记录示例。您可以使用 `userAgent` 元素标识控制台。可使用 `eventName` 元素标识请求的 API 调用。有关用户（`Alice`）的信息可在 `userIdentity` 元素中找到。

Example 例如： 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 Transit Gateways 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。要允许某个用户访问资源（如中转网关）和执行任务，您必须创建一个 IAM policy（该策略向该用户授予使用其所需的特定资源和 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：

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

管理中转网关的策略示例

以下是用于处理中转网关的示例 IAM 策略。

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 VPC Transit Gateways 中为中转网关使用服务相关角色

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

中转网关服务相关角色

Amazon VPC 使用服务链接角色获得在使用中转网关时代表您调用其他 AWS 服务所需的权限。

服务相关角色授予的权限

当您使用传输AWSServiceRoleForVPCTransit网关时，Amazon VPC 使用名为 Gatew ay 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

AWSServiceRoleForVPCTransitGateway 角色信任以下服务来代入该角色：

- transitgateway.amazonaws.com

AWSServiceRoleForVPCTransit网关使用托管策略AWSVPCTransitGatewayServiceRolePolicy。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。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。当您将账户中的 VPC 连接到中转网关时，Amazon VPC 会为您创建此角色。

编辑服务相关角色

您可以使用 IAM 编辑AWSServiceRoleForVPCTransit网关的描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色描述。

删除服务相关角色

如果您不再需要使用中转网关，我们建议您删除AWSServiceRoleForVPCTransit网关。

只有在删除 AWS 账户中的所有传输网关 VPC 附件后，才能删除此服务相关角色。这可确保您不会无意中删除访问您的 VPC 附件的权限。

您可以使用 IAM 控制台、IAM CLI 或 IAM API 删除服务相关角色。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AWSServiceRoleForVPCTransit网关后，如果您将账户中的 VPC 关联到传输网关，Amazon VPC 会再次创建该角色。

AWS Amazon VPC 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管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 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：

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS 托管策略： AWSVPCTransitGatewayServiceRolePolicy

此策略附加到角色AWSServiceRoleForVPCTransit网关。这允许 Amazon VPC 为您的中转网关连接创建和管理资源。

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

AWS 托管策略的公交网关更新

查看自 Amazon VPC 于 2021 年 3 月开始跟踪公交网关 AWS 托管策略更新以来，这些变更的详细信息。

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

Amazon VPC 传输网关中的中转网关网络 ACLs

网络访问控制列表 (NACL) 提供了一层可选的安全性。

根据场景，应用网络访问控制列表 (NACL) 规则的方式会有所不同：

- 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。从实例到中转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。

对于从实例指向中转网关的流量，按以下方式应用 NACL 规则：

- 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。

对于从中转网关指向实例的流量，按以下方式应用 NACL 规则：

- 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 ACL 关联。

网络 ACL 规则按以下方式应用于 EC2 实例子网：

- 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。

对于中转网关所在的子网，按以下方式应用网络 ACL 规则：

- 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

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

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

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

Amazon VPC Transit Gateways 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，每个配额是区域特定的。

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
每个中转网关的 CIDR 块	5	否

CIDR 块在 the section called “Connect 挂载和 Connect 对等节点” 功能中使用。

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
单个连接的前缀的静态路由	1	否

发布的路由来自与 Connect 连接关联的路由表。

中转网关连接

一个中转网关不能包含同一 VPC 的多个 VPC 连接。

名称	默认值	可调整
每个中转网关的连接	5000	否
每个 VPC 的中转网关	5	否
每个中转网关的对等连接连接	50	是
每个 中转网关 的待处理待对等连接数	10	是
两个中转网关之间，或者一个中转网关和一个云 WAN 核心网络边缘 (CNE) 之间的对等节点连接	1	否
每个 Connect 连接的 Connect 对等节点（GRE 隧道）数量	4	否

带宽

有许多因素会影响通过 Site-to-Site 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 连接，AWS Direct Connect 网关或对等中转网关连接，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
每个可用区每个 VPC 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 (SA) 或者技术客户经理 (TAM)。
每个可用区每个中转网关 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

名称	默认值	可调整
		构师 (SA) 或者技术客户经理 (TAM)。
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 (SA) 或者技术客户经理 (TAM)。
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 (SA) 或者技术客户经理 (TAM)。
每个 VPN 隧道的最大带宽	最高 1.25 Gbps	否
每个 VPN 隧道的每秒最大数据包数量	最高 14 万	否
每个 Connect 连接的每个 Connect 对等节点（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)，通过聚合多个 VPN 隧道来获得更高的 VPN 带宽。要使用 ECMP，必须配置 VPN 连接以进行动态路由。在使用静态路由的 VPN 连接上不支持 ECMP。

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 ECMP，通过在同一 Connect 连接的多个 Connect 对等节点之间或同一传输网关的多个 Connect 连接之间水平扩展以获得更高的带宽。中转网关不能在同一 Connect 对等节点的 BGP 对等连接之间使用 ECMP。

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

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

最大传输单元 (MTU)

- 网络连接的 MTU 是能够通过该连接传递的最大可允许数据包的大小（以字节为单位）。连接的 MTU 越大，可在单个数据包中传递的数据越多。传输网关支持 VPCs、 AWS Direct Connect、Transit Gateway Connect 和对等连接（区域内、区域间和云广域网对等连接附件）之间的 MTU 为 8500 字节。VPN 连接上的流量可以具有的 MTU 为 1500 字节。
- 从 VPC 对等连接迁移以使用 中转网关 时,如果 VPC 对等连接和 中转网关 之间的 MTU 大小不匹配，则可能会导致一些非对称流量丢包。 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。
- 中转网关会对所有数据包强制执行最大分段大小 (MSS) 固定。有关更多信息，请参阅 RFC879。
- 有关 MTU 的 Site-to-Site VPN 配额的详细信息，请参阅《AWS Site-to-Site VPN 用户指南》中的最大传输单位 (MTU)。
- 公交网关支持 Path MTU 发现 (PMTUD)，用于通过 VPC 和 Connect 附件传入流量。传输网关`FRAG_NEEDED`为 ICMPv4 数据包和`Packet Too Big (PTB)`数据包生成。 ICMPv6 公交网关不支持 VP Site-to-site N、Direct Connect 和对等连接上的 PMTUD。有关 Path MTU 发现的更多信息，请参阅 Amazon VPC 用户指南中的路径 MTU 发现

多播

> **Note**
>
> Transit Gateway 多播可能不适合高频交易或对性能敏感的应用程序。我们强烈建议您查看以下多播限制。请联系您的客户或解决方案架构师团队，详细了解您的性能要求。

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

名称	默认值	可调整
每个 VPC 的多播域关联数	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
每个流每秒的最大数据包数（少于 10 个接收器）	75000	否
每个流每秒的最大数据包数（大于 10 个接收器）	15000	否
每秒最大聚合数据包数（少于 10 个接收器）	250,000	否
每秒最大聚合数据包数（大于 10 个接收器）	500,000	否

AWS 网络管理器

名称	默认值	可调整
每个全球网络 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：

- Site-to-Site 《AWS Site-to-Site VPN 用户指南》中的 VPN 配额
- Amazon VPC 用户指南中的 Amazon 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
网络功能附件	创建网络功能附件，将公交网关直接连接到 AWS Network Firewall。	2025 年 6 月 16 日
安全组引用支持	现在，您可以引用 VPCs 连接到传输网关的安全组。	2024 年 9 月 25 日
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
对等连接	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 VPC 中运行的中转网关和第三方虚拟设备之间建立连接。	2020 年 12 月 10 日
设备模式	您可以在 VPC 连接上启用设备模式，以确保双向流量流过相同的可用区以进行连接。	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
对等连接	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。