



AWS Transit Gateway

# Amazon VPC



# Amazon VPC: AWS Transit Gateway

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

---

# Table of Contents

Qu'est-ce qu'une passerelle de transit ? .....	1
Concepts de passerelle de transit .....	1
Comment démarrer avec les passerelles de transit .....	2
Utiliser des passerelles de transit .....	2
Tarification .....	3
Fonctionnement des passerelles de transit .....	4
Diagramme d'architecture .....	4
Attachements de ressources .....	6
Routage multivoies à coût égal .....	6
Zones de disponibilité .....	7
Routage .....	8
Tables de routage .....	9
Association de table de routage .....	9
Propagation du routage .....	9
Routes pour les attachements d'appairage .....	10
Ordre d'évaluation des routes .....	10
Mise en route .....	13
Prérequis .....	13
Étape 1 : Création de la passerelle de transit .....	14
Étape 2 : Raccorder vos VPC à votre passerelle de transit .....	14
Étape 3 : Ajouter des routes entre la passerelle de transit et vos VPC .....	15
Étape 4 : Tester la passerelle de transit .....	16
Étape 5 : Supprimer la passerelle de transit .....	16
Bonnes pratiques de conception .....	18
Exemples de cas d'utilisation .....	20
Routeur centralisé .....	20
Présentation .....	20
Ressources .....	21
Routage .....	22
VPC isolés .....	23
Présentation .....	23
Ressources .....	24
Routage .....	25
VPC isolés avec services partagés .....	26

Présentation .....	27
Ressources .....	27
Routage .....	28
Appairage .....	30
Présentation .....	30
Ressources .....	31
Routage .....	32
Routage sortant centralisé .....	33
Présentation .....	34
Ressources .....	34
Routage .....	35
VPC de l'appliance .....	38
Présentation .....	39
Appliances avec état et mode appliance .....	40
Routage .....	41
Utiliser des passerelles de transit .....	44
Passerelles de transit .....	44
Créer une passerelle de transit .....	45
Afficher vos passerelles de transit .....	47
Ajouter ou modifier les balises d'une passerelle de transit .....	48
Modifier une passerelle de transit .....	48
Partager une passerelle de transit .....	49
Accepter un partage de ressources .....	50
Accepter un attachement partagé .....	50
Supprimer une passerelle de transit .....	51
Attachements VPC .....	51
Cycle de vie des attachements VPC .....	52
Créer un attachement de passerelle de transit vers un VPC .....	55
Modifier l'attachement de votre VPC .....	56
Modifier les balises d'attachement de votre VPC .....	57
Afficher vos attachements de VPC .....	57
Supprimer un attachement de VPC .....	57
Résoudre les problèmes liés aux attachements VPC .....	58
Attachements VPN .....	59
Créer un attachement de passerelle de transit avec un VPN .....	59
Afficher vos attachements VPN .....	60

Attachements à une passerelle Direct Connect .....	60
Attachement d'appairage .....	61
Créer un attachement d'appairage .....	62
Accepter ou rejeter une demande d'attachement d'appairage .....	63
Ajouter un itinéraire à la table de routage de passerelle de transit .....	64
Afficher vos attachements de connexion d'appairage pour la passerelle de transit .....	65
Supprimer un attachement d'appairage .....	65
Considérations relatives à la Région AWS d'adhésion .....	66
Attachements Connect et pairs Connect .....	67
Connecter les pairs .....	68
Exigences et considérations .....	71
Création d'un attachement Connect .....	72
Créer un pair Connect (tunnel GRE) .....	73
Affichage de vos attachements Connect et de vos pairs Connect .....	74
Modifier votre attachement Connect et vos balises de pair Connect .....	74
Supprimer un pair Connect .....	75
Suppression d'un attachement Connect .....	76
Tables de routage de passerelle de transit .....	76
Créer une table de routage de passerelle de transit .....	76
Afficher les tables de routage de passerelle de transit .....	77
Associer une table de routage de passerelle de transit .....	77
Supprimer une association pour une table de routage de passerelle de transit .....	78
Propager une route vers une table de routage de passerelle de transit .....	78
Désactivation de la propagation du routage .....	79
Créer un itinéraire statique .....	79
Supprimer un routage statique .....	80
Remplacez une route statique .....	81
Exportation des tables de routage vers Amazon S3 .....	81
Supprimer une table de routage de passerelle de transit .....	83
Références des listes de préfixes .....	83
Tables de stratégie de passerelle de transit .....	86
Créer une table de stratégie de passerelle de transit .....	87
Supprimer une table de stratégie de passerelle de transit .....	88
Multicast sur les passerelles de transit .....	88
Concepts du multicast .....	1
Considérations .....	89

Multicast avec Windows Server .....	91
Routage multicast .....	92
Utilisation du multicast .....	93
Partager vos passerelles de transit .....	115
Annuler le partage d'une passerelle de transit .....	116
Sous-réseaux partagés .....	117
Transit Gateway Flow Logs .....	118
Limites .....	119
Enregistrements Transit Gateway Flow Logs .....	119
Format par défaut .....	120
Format personnalisé .....	120
Champs disponibles .....	120
Tarification Transit Gateway Flow Logs .....	126
Publier dans CloudWatch Logs .....	126
Rôles IAM pour publier des journaux de flux dans Logs CloudWatch .....	127
Autorisations pour les utilisateurs IAM pour transmettre un rôle .....	129
Créer un journal de flux qui publie dans CloudWatch Logs .....	130
Enregistrements du flux de processus dans CloudWatch Logs .....	131
Publier vers Amazon S3 .....	133
Fichiers journaux de flux .....	134
Politique IAM pour les principaux IAM qui publient des journaux de flux vers Amazon S3 ....	136
Autorisations du compartiment Amazon S3 pour les journaux de flux .....	136
Politique de clé obligatoire à utiliser avec SSE-KMS .....	138
Autorisations pour les fichiers journaux Amazon S3 .....	139
Créer un journal de flux qui publie vers Amazon S3 .....	139
Traiter des enregistrements de journal de flux dans Amazon S3 .....	141
Publier vers Kinesis Data Firehose .....	142
Rôles IAM pour la diffusion entre comptes .....	142
Créer un journal de flux qui publie sur Firehose .....	147
Utiliser des journaux de flux .....	148
Contrôler l'utilisation des journaux de flux .....	149
Créer un journal de flux .....	149
Afficher les journaux de flux .....	150
Ajouter ou supprimer des identifications pour les journaux de flux .....	150
Afficher les enregistrements de journaux de flux .....	151
Rechercher des enregistrements de journaux de flux .....	151

Supprimer un journal de flux .....	153
Présentation et limites de l'API et de la CLI .....	153
Surveiller vos passerelles de transit .....	156
Métriques CloudWatch .....	157
Métriques de passerelle de transit .....	157
Dimensions métriques pour les passerelles de transit .....	159
Journaux CloudTrail .....	159
Informations sur la passerelle de transit dans CloudTrail .....	160
Description des entrées des fichiers journaux d'une passerelle de transit .....	161
Gestion des identités et des accès .....	164
Exemples de stratégies pour gérer des passerelles de transit .....	164
Exemples de politiques pour gérer AWS Network Manager .....	167
Rôles liés à un service .....	167
Passerelle de transit .....	167
Politiques gérées par AWS .....	168
AWSVPCTransitGatewayServiceRolePolicy .....	169
Mises à jour des politiques .....	169
Listes ACL réseau .....	170
Même sous-réseau pour les instances EC2 et l'association de la passerelle de transit .....	170
Sous-réseaux différents pour les instances EC2 et l'association de la passerelle de transit ..	171
Bonnes pratiques .....	171
Quotas .....	173
Général .....	173
Routage .....	173
Attachements de passerelle de transit .....	174
Bande passante .....	175
AWS Direct Connect passerelles .....	177
Unité de transmission maximale (MTU) .....	177
Multicast .....	178
Gestionnaire de réseau .....	178
Ressources de quotas supplémentaires .....	179
Historique du document .....	180
.....	clxxxiii

# Qu'est-ce qu'une passerelle de transit ?

Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier vos VPC (Virtual Private Cloud) et vos réseaux sur site. À mesure que votre infrastructure cloud s'étend à l'échelle mondiale, l'appairage inter-région interconnecte des passerelles de transit à l'aide de l'Infrastructure mondiale AWS. Tout le trafic réseau entre les centres de données AWS est automatiquement chiffré au niveau de la couche physique.

Pour de plus amples informations, veuillez consulter [AWS Transit Gateway](#).

## Concepts de passerelle de transit

Voici les concepts clés pour les passerelles de transit :

- Attachements : Vous pouvez joindre les éléments suivants :
  - Un ou plusieurs VPC
  - Une appliance réseau Connect SD-WAN/tiers
  - Une passerelle AWS Direct Connect
  - Une connexion d'appairage avec une autre passerelle de transit
  - Une connexion VPN à une passerelle de transit
- Unité de transmission maximale (MTU) de passerelle de transit : L'unité de transmission maximale (MTU) d'une connexion réseau correspond à la taille, en octets, du paquet le plus volumineux susceptible d'être transmis via la connexion. Plus la MTU d'une connexion est élevée, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Une passerelle de transit prend en charge une MTU de 8 500 octets pour le trafic entre les VPC, AWS Direct Connect, Transit Gateway Connect et les attachements d'appairage. Le trafic sur les connexions VPN peut avoir une MTU de 1500 octets.
- Table de routage de passerelle de transit : Une passerelle de transit possède une table de routage par défaut et peut éventuellement avoir des tables de routage supplémentaires. Une table de routage comprend des routes dynamiques et statiques déterminant le prochain saut à partir de l'adresse IP de destination du paquet. La cible de ces routes pourrait être n'importe quel attachement de passerelle de transit. Par défaut, les réseaux de transit par passerelle sont associées à la table de routage de passerelle de transit par défaut.
- Associations : Chaque attachement est associé exactement à une seule table de routage. Chaque table de routage peut être associée à un ou plusieurs attachements (ou à aucun).

- Propagation de route : Un VPC, une connexion VPN ou une passerelle Direct Connect peut propager des routes de façon dynamique vers une table de routage de passerelle de transit. Avec un attachement Connect, les routes sont propagées à une table de routage de passerelle de transit par défaut. Avec un VPC, vous devez créer des routes statiques pour envoyer du trafic vers la passerelle de transit. Avec une connexion VPN, les routes sont propagées à partir de la passerelle de transit vers votre routeur sur site à l'aide du protocole BGP (Border Gateway Protocol). Avec une passerelle Direct Connect, les préfixes autorisés sont transmis à votre routeur sur site à l'aide du protocole BGP. Avec un attachement d'appairage, vous devez créer un itinéraire statique dans la table de routage de la passerelle de transit pour pointer vers l'attachement d'appairage.

## Comment démarrer avec les passerelles de transit

Aidez-vous des ressources suivantes pour créer et utiliser une passerelle de transit.

- [Fonctionnement des passerelles de transit](#)
- [Mise en route](#)
- [Bonnes pratiques de conception](#)

## Utiliser des passerelles de transit

Vous pouvez créer vos passerelles de transit, y accéder et les gérer à l'aide des interfaces suivantes :

- AWS Management Console — fournit une interface web que vous pouvez utiliser pour accéder à vos passerelles de transit.
- Interface de ligne de commande AWS (AWS CLI) : fournit des commandes pour un vaste éventail de services AWS, dont Amazon VPC ; compatibles avec Windows, macOS et Linux. Pour plus d'informations, consultez [AWS Command Line Interface](#).
- Kits SDK AWS : fournissent opérations d'API spécifiques d'un langage, et se chargent des nombreux détails de connexion, notamment le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour plus d'informations, consultez [AWSKits SDK](#).
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct pour accéder à Amazon VPC, mais elle nécessite que votre application gère les détails de bas niveau, tels que la génération d'un hachage

pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez la [Référence d'API Amazon EC2](#).

## Tarification

Vous êtes facturé par heure pour chaque attachement sur une passerelle de transit et pour le volume de trafic traité sur celle-ci. Pour plus d'informations, consultez [Tarification d'AWS Transit Gateway](#).

# Fonctionnement des passerelles de transit

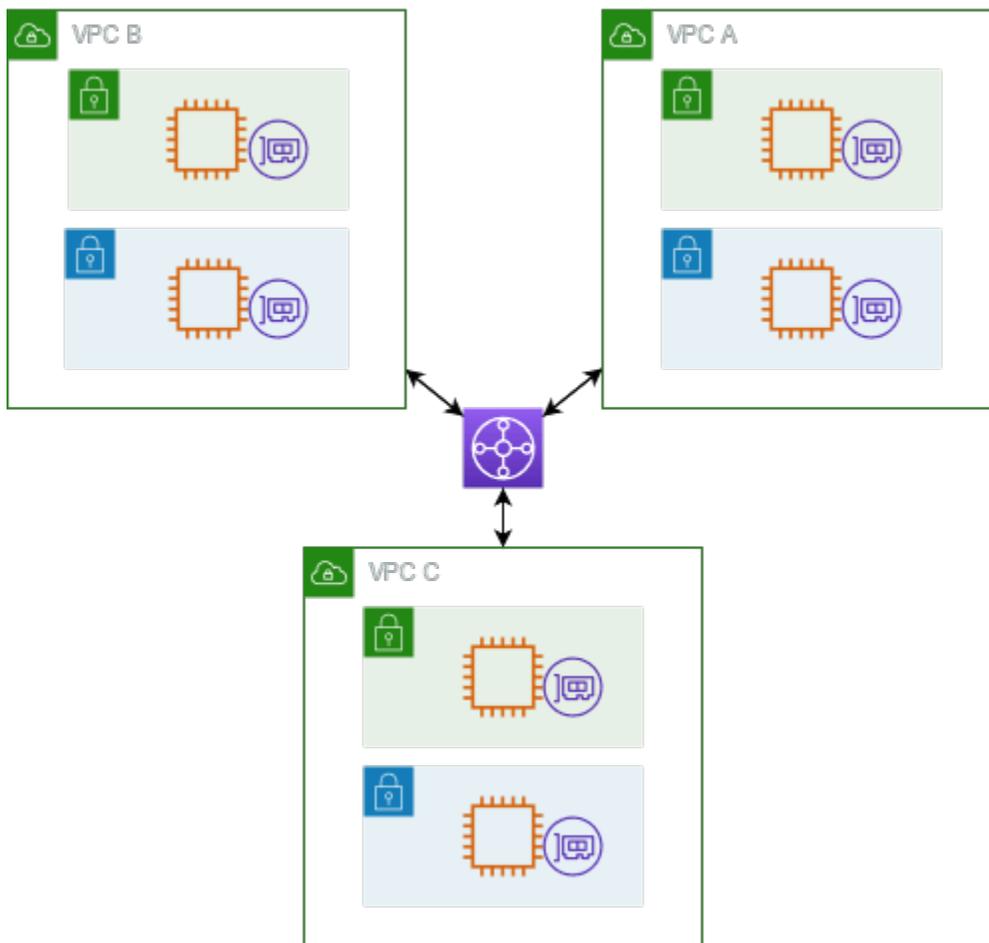
Une passerelle de transit agit en tant que routeur virtuel régional pour le trafic circulant entre vos Virtual Private Clouds (VPC) et connexions sur site. Une passerelle de transit dispose d'une scalabilité élastique en fonction du volume de trafic réseau. L'acheminement via une passerelle de transit fonctionne comme une couche 3, où les paquets sont envoyés vers un attachement next hop précis, en fonction de leurs adresses IP de destination.

## Table des matières

- [Diagramme d'architecture](#)
- [Attachements de ressources](#)
- [Routage multivoies à coût égal](#)
- [Zones de disponibilité](#)
- [Routage](#)

## Diagramme d'architecture

Le diagramme suivant montre une passerelle de transit avec des trois attachements VPC. La table de routage de chacun de ces VPC inclut l'acheminement local et ceux qui envoient le trafic destiné aux deux autres VPC vers la passerelle de transit.



Voici un exemple de table de routage de passerelle de transit par défaut pour les attachements présentés dans le diagramme précédent. Les blocs d'adresse CIDR de chaque VPC sont propagés vers la table de routage. Par conséquent, chaque attachement peut acheminer des paquets vers les deux autres attachements.

Destination	Target	Type de routage
<i>CIDR VPC A</i>	<i>Attachement pour le VPC A</i>	propagée
<i>CIDR VPC B</i>	<i>Attachement pour le VPC B</i>	propagée
<i>CIDR VPC C</i>	<i>Attachement pour le VPC C</i>	propagée

## Attachements de ressources

Un attachement de passerelle de transit est à la fois une source et une destination pour les paquets. Vous pouvez associer les ressources suivantes à votre passerelle de transit :

- Un ou plusieurs VPC. AWS Transit Gateway déploie une interface réseau élastique au sein des sous-réseaux VPC, qui est ensuite utilisée par la passerelle de transit pour acheminer le trafic vers et depuis les sous-réseaux choisis. Vous devez disposer d'au moins un sous-réseau pour chaque zone de disponibilité, ce qui permet au trafic d'atteindre les ressources de chaque sous-réseau de cette zone. Lors de la création d'une pièce jointe, les ressources d'une zone de disponibilité particulière peuvent atteindre une passerelle de transit uniquement si un sous-réseau est activé dans la même zone. Si une table de routage comprend une route vers la passerelle de transit, le trafic n'est transféré vers la passerelle de transit que lorsqu'elle possède un attachement dans un sous-réseau de la même zone de disponibilité.
- Une ou plusieurs connexions VPN
- Une ou plusieurs AWS Direct Connect passerelles
- Une ou plusieurs attachements Connect de passerelle de transit
- Une ou plusieurs connexions d'appairage pour les passerelle de transit
- Un attachement de la passerelle de transit peut être à la fois une source et une destination pour les paquets

## Routage multivoies à coût égal

AWS Transit Gateway prend en charge le routage ECMP (Equal Cost Multipath) pour la plupart des pièces jointes. Pour un attachement de VPN, vous pouvez activer ou désactiver le support ECMP à l'aide de la console lors de la création ou de la modification d'une passerelle de transit. Pour tous les autres types d'attachement, les restrictions ECMP suivantes s'appliquent :

- VPC : le VPC ne prend pas en charge ECMP car les blocs CIDR ne peuvent pas se chevaucher. Par exemple, vous ne pouvez pas associer un VPC avec un CIDR 10.1.0.0/16 à un second VPC utilisant le même CIDR à une passerelle de transit, puis configurer le routage pour équilibrer la charge du trafic entre eux.
- VPN : lorsque l'option de support ECMP du VPN est désactivée, une passerelle de transit utilise des indicateurs internes pour déterminer le chemin préféré en cas de présence de préfixes identiques sur plusieurs chemins. Pour plus d'informations sur l'activation ou la désactivation de l'ECMP pour un attachement VPN, consultez [the section called "Passerelles de transit"](#).

- AWS Transit Gateway Connect - Les pièces jointes AWS Transit Gateway Connect prennent automatiquement en charge l'ECMP.
- AWS Direct Connect Passerelle : les pièces jointes de AWS Direct Connect passerelle prennent automatiquement en charge le protocole ECMP sur plusieurs pièces jointes de passerelle Direct Connect lorsque le préfixe réseau, la longueur du préfixe et le code AS\_PATH sont exactement identiques.
- Appairage de passerelle de transit : l'appairage de passerelle de transit ne prend pas en charge ECMP car il ne prend pas en charge le routage dynamique et ne permet pas de configurer la même route statique pour deux cibles différentes.

#### Note

- BGP Multipath AS-Path Relax n'étant pas pris en charge, vous ne pouvez pas utiliser ECMP sur différents numéros de système autonome (ASN).
- ECMP n'est pas pris en charge entre les différents types d'attachement. Par exemple, vous ne pouvez pas activer ECMP entre un VPN et un attachement de VPC. Au lieu de cela, les routes de passerelle de transit sont évaluées et le trafic est acheminé en fonction de la route évaluée. Pour plus d'informations, consultez [the section called "Ordre d'évaluation des routes"](#).
- Une passerelle Direct Connect unique prend en charge ECMP sur plusieurs interfaces virtuelles de transit. Par conséquent, nous vous recommandons de configurer et d'utiliser une seule passerelle Direct Connect et de ne pas configurer et d'utiliser plusieurs passerelles pour tirer parti d'ECMP. Pour plus d'informations sur les passerelles Direct Connect et les interfaces virtuelles publiques, voir [Comment configurer une connexion AWS Direct Connect active/active ou active/passive depuis une interface virtuelle publique ?](#).

## Zones de disponibilité

Lorsque vous attachez un VPC à une passerelle de transit, vous devez permettre l'utilisation d'une ou plusieurs zones de disponibilité par cette passerelle de transit afin d'acheminer le trafic vers les ressources au sein des sous-réseaux du VPC. Pour activer chaque zone de disponibilité, vous devez spécifier exactement un sous-réseau. La passerelle de transit place une interface réseau dans ce sous-réseau à l'aide d'une adresse IP du sous-réseau. Après avoir activé une zone de disponibilité,

le trafic peut être acheminé vers tous ses sous-réseaux dans le VPC, pas uniquement le sous-réseau ou la zone de disponibilité spécifiés. Toutefois, seules les ressources qui résident dans les zones de disponibilité où il existe un attachement de passerelle de transit peuvent atteindre la passerelle de transit.

Si le trafic provient d'une zone de disponibilité dans laquelle la pièce jointe de destination n'est pas présente, AWS Transit Gateway achemine ce trafic en interne vers une zone de disponibilité aléatoire où la pièce jointe est présente. Il n'y a aucun frais de passerelle de transit supplémentaire pour ce type de trafic entre zones de disponibilité.

Nous vous recommandons d'activer plusieurs zones de disponibilité pour assurer une disponibilité.

### Utilisation du support du mode appliance

Si vous prévoyez de configurer une appliance réseau avec état dans votre VPC, vous pouvez activer le support du mode appliance pour cet attachement de VPC. Cela garantit que la passerelle de transit utilise la même zone de disponibilité pour cet attachement de VPC pendant la durée de vie d'un flux de trafic entre la source et la destination. Cela permet également à la passerelle de transit d'envoyer du trafic vers n'importe quelle zone de disponibilité du VPC, à condition qu'il existe une association de sous-réseau au sein de cette zone. Pour plus d'informations, consultez [Exemple : Appliance dans un VPC de services partagés](#).

## Routage

Votre passerelle de transit achemine les paquets IPv4 et IPv6 entre les attachements à l'aide des tables de routage de passerelle de transit. Vous pouvez configurer ces tables de routage pour propager des routes depuis les tables de routage pour les VPC attachés, les connexions VPN et les passerelles Direct Connect. Vous pouvez également ajouter des routes statiques aux tables de routage de passerelle de transit. Lorsqu'un paquet vient d'un attachement, il est acheminé vers un autre attachement en utilisant le routage correspondant à l'adresse IP de destination.

Pour les attachements d'appairage de passerelle de transit, seules les routes statiques sont prises en charge.

### Table des matières

- [Tables de routage](#)
- [Association de table de routage](#)
- [Propagation du routage](#)

- [Routes pour les attachements d'appairage](#)
- [Ordre d'évaluation des routes](#)

## Tables de routage

Votre passerelle de transit est automatiquement fournie avec une table de routage par défaut. Par défaut, cette table de routage est la table de routage d'association par défaut et la table de routage de propagation par défaut. Sinon, si vous désactivez la propagation du routage et l'association de la table de routage, AWS ne crée pas de table de routage par défaut pour la passerelle de transit.

Vous pouvez créer des tables de routage supplémentaires pour votre passerelle de transit. Cela vous permet d'isoler des sous-ensembles d'attachements. Chaque attachement peut être associé à une table de routage. Un attachement peut propager ses routes à une ou plusieurs autres tables de routage.

Vous pouvez créer une route blackhole dans votre table de routage de passerelle de transit, qui supprime le trafic correspondant à la route.

Lorsque vous attachez un VPC à une passerelle de transit, vous devez ajouter un itinéraire à votre table de routage de sous-réseau afin que le trafic passe par la passerelle de transit. Pour de plus amples informations, veuillez consulter [Routage pour une passerelle de transit](#) dans le Guide de l'utilisateur Amazon VPC.

## Association de table de routage

Vous pouvez associer un attachement de une passerelle de transit à une seule table de routage. Chaque table de routage peut être associée ou non, avec plusieurs attachements et peut transférer des paquets vers d'autres attachements.

## Propagation du routage

Chaque attachement est fourni avec des routes pouvant être installées dans une ou plusieurs tables de routage de passerelle de transit. Lorsqu'un attachement est propagé vers une table de routage de passerelle de transit, ces routes sont installées dans la table de routage. Vous ne pouvez pas filtrer les itinéraires annoncés.

Pour un attachement VPC, les blocs d'adresse CIDR du VPC sont propagés à la table de routage de la passerelle de transit.

Lorsque le routage dynamique est utilisé avec un attachement VPN ou un attachement de passerelle Direct Connect, vous pouvez propager les routes acquises auprès du routeur sur site via BGP vers n'importe quelle table de routage de passerelle de transit.

Lorsque le routage dynamique est utilisé avec un attachement VPN, les routes de la table de routage associée à l'attachement VPN sont publiées sur la passerelle client via BGP.

Pour une pièce jointe Connect, les routes de la table de routage associée à la pièce jointe Connect sont annoncés aux appliances virtuelles tierces, telles que les appliances SD-WAN, exécutées dans un VPC via BGP.

Pour une connexion à une passerelle Direct Connect, [les interactions avec les préfixes autorisés contrôlent les](#) itinéraires à partir desquels les itinéraires sont annoncés au réseau du client. AWS

Lorsqu'une route statique et un route propagée ont la même destination, la route statique a la priorité la plus élevée. La route propagée n'est donc pas incluse dans la table de routage. Si vous supprimez la route statique, la route propagée superposée est incluse dans la table de routage.

## Routes pour les attachements d'appairage

Vous pouvez appairer deux passerelles de transit, et acheminer le trafic entre elles. Pour ce faire, vous créez un attachement d'appairage sur votre passerelle de transit et spécifiez la passerelle de transit pair avec laquelle créer la connexion d'appairage. Vous créez ensuite une route statique dans votre table de routage de passerelle de transit pour acheminer le trafic vers l'attachement d'appairage de passerelle de transit. Le trafic acheminé vers la passerelle de transit pair peut ensuite être acheminé vers les attachements de VPC et réseaux VPN pour la passerelle de transit pair.

Pour plus d'informations, consultez [Exemple : passerelles de transit appairées](#).

## Ordre d'évaluation des routes

Les routes de passerelle de transit sont évaluées dans l'ordre suivant :

- Route la plus spécifique pour l'adresse de destination.
- Pour les itinéraires dotés du même CIDR, mais provenant de types d'attachement différents, la priorité de l'itinéraire est la suivante :
  - Routes statiques (par exemple, routes statiques Site-to-Site VPN)
  - Acheminements référencés dans la liste des préfixes

- Routes propagées VPC
- Routes propagées de passerelle Direct Connect
- Routes propagées de transit Gateway Connect
- Routes propagées Site-to-Site VPN
- Routes propagées d'appairage de Passerelle de transit (Cloud WAN)

Certaines pièces jointes prennent en charge la publicité d'itinéraires via BGP. Pour les routes ayant le même CIDR et le même type de pièce jointe, la priorité de la route est contrôlée par les attributs BGP :

- Longueur de chemin AS plus courte
- Valeur MED inférieure
- Les routes eBGP par rapport à iBGP sont préférées, si la pièce jointe les prend en charge

#### Important

AWS ne peut pas garantir un ordre de priorité d'itinéraire cohérent pour les routes BGP ayant le même CIDR, le même type de pièce jointe et les mêmes attributs BGP que ceux répertoriés ci-dessus.

AWS Transit Gateway affiche uniquement un itinéraire préféré. Un itinéraire de sauvegarde n'apparaîtra dans le tableau des itinéraires de Transit Gateway que s'il n'est plus annoncé, par exemple, si vous annoncez les mêmes itinéraires via la passerelle Direct Connect et via le VPN Site-to-Site. AWS Transit Gateway n'affichera que les itinéraires reçus de la passerelle Direct Connect, qui est l'itinéraire préféré. Le Site-to-Site VPN, qui est la route de sauvegarde, s'affiche uniquement lorsque la passerelle Direct Connect n'est plus annoncée.

## Différences entre les tables de routage du VPC et de la passerelle de transit

L'évaluation de la table de routage diffère selon que vous utilisiez une table de routage VPC ou une table de routage de passerelle de transit.

L'exemple suivant montre une table de routage VPC. La route locale de VPC dispose de la priorité la plus élevée, devant les routes les plus spécifiques. Lorsqu'une route statique et une route propagée ont une même destination, la route statique a la priorité.

Destination	Target	Priority
10.0.0.0/16	Locale	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (statique) ou tgw-12345 (statique)	2
172.31.0.0/16	vgw-12345 (propagée)	3
0.0.0.0/0	igw-12345	4

L'exemple suivant montre une table de routage de passerelle de transit. Si vous préférez utiliser l'attachement de passerelle AWS Direct Connect plutôt que le réseau VPN, vous pouvez utiliser une connexion VPN BGP et propager les routes dans la table de routage de passerelle de transit.

Destination	Attachement (Cible)	Type de ressource	Type de routage	Priority
10.0.0.0/16	tgw-attach-123   vpc-1234	VPC	Statique ou propagée	1
192.168.0.0/16	tgw-attach-789   vpn-5678	VPN	Statique	2
172.31.0.0/16	tgw-attach-456   dxgw_id	AWS Direct Connect passerelle	Propagée	3
172.31.0.0/16	tgw-attach-789   -123 tgw-conne ct-peer	Connexion	Propagé	4
172.31.0.0/16	tgw-attach-789   vpn-5678	VPN	Propagée	5

# Mise en route avec les passerelles de transit

Les tâches suivantes vous aideront à vous familiariser avec les passerelles de transit. Vous allez créer une passerelle de transit, puis connecter deux de vos VPC à l'aide de la passerelle de transit.

## Tâches

- [Prérequis](#)
- [Étape 1 : Création de la passerelle de transit](#)
- [Étape 2 : Raccorder vos VPC à votre passerelle de transit](#)
- [Étape 3 : Ajouter des routes entre la passerelle de transit et vos VPC](#)
- [Étape 4 : Tester la passerelle de transit](#)
- [Étape 5 : Supprimer la passerelle de transit](#)

## Prérequis

- Pour donner un exemple simple de l'utilisation d'une passerelle de transit, créez deux VPC dans la même région. Les CIDR des VPC ne peuvent pas se chevaucher. Démarrez une instance Amazon EC2 sur chaque VPC. Pour plus d'informations, consultez [Mise en route avec Amazon VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Vous ne pouvez pas avoir de routes identiques pointant vers deux VPC différents. Une passerelle de transit ne propage pas les CIDR d'un VPC nouvellement attaché si une route identique existe dans les tables de routage de passerelle de transit.
- Assurez-vous de disposer des autorisations nécessaires pour utiliser les passerelles de transit. Pour de plus amples informations, veuillez consulter [Identity and Access Management pour vos passerelles de transit](#).
- Vous ne pouvez pas effectuer un test ping entre les hôtes si vous n'avez pas ajouté une règle ICMP à chacun des groupes de sécurité des hôtes. Pour plus d'informations, consultez la section [Travailler avec les groupes de sécurité](#) dans le Guide de l'utilisateur Amazon VPC.

## Étape 1 : Création de la passerelle de transit

Lorsque vous créez une passerelle de transit, nous créons une table de routage de la passerelle de transit par défaut et nous l'utilisons comme table de routage d'association et table de routage de propagation par défaut.

Pour créer une passerelle de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le sélecteur de région, choisissez la région utilisée pour créer les VPC.
3. Dans le volet de navigation, choisissez Passerelles de transit.
4. Choisissez Create transit gateway (Créer une passerelle de transit).
5. (Facultatif) Pour Name tag (Balise nom), saisissez un nom pour la passerelle de transit. Une balise ayant la clé « Nom » et le nom spécifié comme valeur est alors créée.
6. (Facultatif) Dans le champ Description (Description), saisissez une description de la passerelle de transit.
7. Pour Amazon side Autonomous System Number (ASN), saisissez l'ASN privé de votre passerelle de transit. Ceci devrait être l'ASN pour le côté AWS d'une session Border Gateway Protocol (BGP) (protocole de passerelle frontière (BGP)).

La plage s'étend de 64512 à 65534 pour les ASN de 16 bits.

La plage s'étend de 4200000000 à 4294967294 pour les ASN de 32 bits.

Si vous avez un déploiement multi-régions, nous vous recommandons d'utiliser un seul ASN pour chacune de vos passerelles de transit.

8. (Facultatif) Vous pouvez modifier les paramètres par défaut si vous devez désactiver la prise en charge du DNS, ou bien si vous ne voulez pas de la table de routage d'association ou de la table de routage de propagation par défaut.
9. Choisissez Create transit gateway (Créer une passerelle de transit). Lorsque la passerelle est créée, l'état initial de la passerelle de transit est pending.

## Étape 2 : Raccorder vos VPC à votre passerelle de transit

Attendez que la passerelle de transit créée à l'étape précédente soit disponible avant de créer un attachement. Créez un attachement pour chaque VPC.

Confirmez que vous avez bien créé deux VPC et que vous avez lancé une instance EC2 pour chacun d'eux, comme décrit en [Prérequis](#).

Créer un attachement de passerelle de transit vers un VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de transit).
4. (Facultatif) Pour Name tag (Balise de nom), saisissez un nom pour l'attachement.
5. Pour Transit gateway ID (ID de passerelle de transit), choisissez la passerelle de transit à utiliser pour l'attachement.
6. Pour Attachment type (Type d'attachement), choisissez VPC.
7. Choisissez d'activer ou non la prise en charge du DNS. Pour cet exercice, n'activez pas la prise en charge d'IPv6.
8. Pour VPC ID (ID de VPC), choisissez le VPC à attacher à la passerelle de transit.
9. Pour Subnet IDs (ID de sous-réseau), sélectionnez un sous-réseau pour chaque zone de disponibilité utilisable par la passerelle de transit pour acheminer le trafic. Vous devez sélectionner au moins un sous-réseau. Vous pouvez sélectionner un seul sous-réseau par zone de disponibilité.
10. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de transit).

Chaque attachement est toujours associé avec une seule table de routage. Les tables de routage peuvent être associées à un ou plusieurs attachements (ou à aucun). Pour déterminer les routes à configurer, décidez du cas d'utilisation de votre passerelle de transit, puis configurez les routes. Pour plus d'informations, consultez [Exemples de cas d'utilisation](#).

## Étape 3 : Ajouter des routes entre la passerelle de transit et vos VPC

Une table de routage comprend des routes dynamiques et statiques déterminant le prochain saut pour les VPC associés à partir de l'adresse IP de destination du paquet. Configurez une route ayant une destination pour les routes non locales et la cible de l'ID de l'attachement de passerelle de transit. Pour de plus amples informations, veuillez consulter [Routage pour une passerelle de transit](#) dans le Guide de l'utilisateur Amazon VPC.

Pour ajouter une route vers une table de routage de VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage.
3. Choisissez la table de routage associée à votre VPC.
4. Choisissez l'onglet Routes, puis Modifier les routes.
5. Choisissez Ajouter une route.
6. Dans la colonne Destination, saisissez la plage d'adresse IP de destination. Pour Target (Cible), choisissez Transit Gateway (Passerelle de transit), puis choisissez l'ID de la passerelle de transit.
7. Sélectionnez Save Changes (Enregistrer les modifications).

## Étape 4 : Tester la passerelle de transit

Vous pouvez confirmer que la passerelle de transit est correctement créée en vous connectant à une instance Amazon EC2 dans chaque VPC, puis en échangeant des données entre eux, par exemple, à l'aide d'une commande ping. Pour de plus amples informations, veuillez consulter [Connexion à votre instance Linux](#) ou [Connexion à votre instance Windows](#).

## Étape 5 : Supprimer la passerelle de transit

Lorsque vous n'avez plus besoin d'une passerelle de transit, vous pouvez la supprimer.

Vous ne pouvez pas supprimer une passerelle de transit disposant d'attachements de ressources. Si vous essayez de supprimer une passerelle de transit contenant des attachements, vous serez invité à supprimer d'abord ces attachements avant de pouvoir supprimer la passerelle de transit. Dès que la passerelle de transit est supprimée, vous cessez de régler des frais pour elle.

Pour supprimer votre passerelle de transit

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Passerelles de transit.
3. Sélectionnez la passerelle de transit, puis choisissez Actions (Actions), Delete transit gateway (Supprimer la passerelle de transit).
4. Saisissez **delete** puis choisissez Delete (Supprimer).

L'État de la passerelle de transit sur la page des Passerelles de transit est Deleting (Suppression en cours). Une fois supprimée, la passerelle de transit est supprimée de la page.

# Bonnes pratiques pour la conception de passerelles de transit

Voici les meilleures pratiques pour la conception de votre passerelle de transit :

- Utilisez un sous-réseau distinct pour chaque attachement de VPC de passerelle de transit. Pour chaque sous-réseau, utilisez un petit CIDR, par exemple /28, afin d'avoir plus d'adresses pour les ressources EC2. Lorsque vous utilisez un sous-réseau distinct, vous pouvez configurer les éléments suivants :
  - Gardez ouvertes les ACL réseau entrante et sortante associées aux sous-réseaux de la passerelle de transit.
  - En fonction de votre flux de trafic, vous pouvez appliquer des ACL réseau à vos sous-réseaux de charge de travail.
- Créez une ACL réseau et combinez-la à tous les sous-réseaux associés à la passerelle de transit. Gardez la liste ACL réseau ouverte dans les directions entrantes et sortantes.
- Associez la même table de routage de VPC à tous les sous-réseaux attachés à la passerelle de transit, sauf si la conception de votre réseau nécessite plusieurs tables de routage de VPC (par exemple, un VPC middle-box qui achemine le trafic par le biais de plusieurs passerelles NAT).
- Utilisez les connexions Site-to-Site VPN BGP (Border Gateway Protocol). Si votre passerelle client ou votre pare-feu pour la connexion prend en charge plusieurs chemins, activez la fonction.
- Activez la propagation des itinéraires pour les pièces jointes à la AWS Direct Connect passerelle et les pièces jointes VPN BGP Site-to-Site.
- Lors de la migration depuis le peering VPC pour utiliser une passerelle de transit. Un décalage de taille MTU entre l'appairage de VPC et la passerelle de transit peut entraîner la chute de certains paquets pour le trafic asymétrique. Mettez à jour les deux VPC en même temps pour éviter la chute des paquets jumbo en raison d'un décalage de taille.
- Vous n'avez pas besoin d'autres passerelles de transit pour une haute disponibilité, car elle le sont déjà grâce à leur conception.
- Limitez le nombre de tables de routage de passerelle de transit, sauf si votre conception nécessite plusieurs tables de routage de passerelle de transit.
- Pour la redondance, utilisez une passerelle de transit unique dans chaque région pour la reprise après sinistre.

- Pour les déploiements avec plusieurs passerelles de transit, nous vous recommandons d'utiliser un numéro ASN (Autonomous System Number) unique pour chacune de vos passerelles de transit. Vous pouvez également utiliser l'appairage inter-région. Pour plus d'informations, voir [Création d'un réseau mondial à l'aide du AWS Transit Gateway peering interrégional](#).

# Voici des cas d'utilisation courants pour les passerelles de transit

Voici des cas d'utilisation courants pour les passerelles de transit. Vos passerelles de transit ne sont pas limitées à ces cas d'utilisation.

## Exemples

- [Exemple : routeur centralisé](#)
- [Exemple : VPC isolés](#)
- [Exemple : VPC isolés avec services partagés](#)
- [Exemple : passerelles de transit appairées](#)
- [Exemple : Routage sortant centralisé vers Internet](#)
- [Exemple : Appliance dans un VPC de services partagés](#)

## Exemple : routeur centralisé

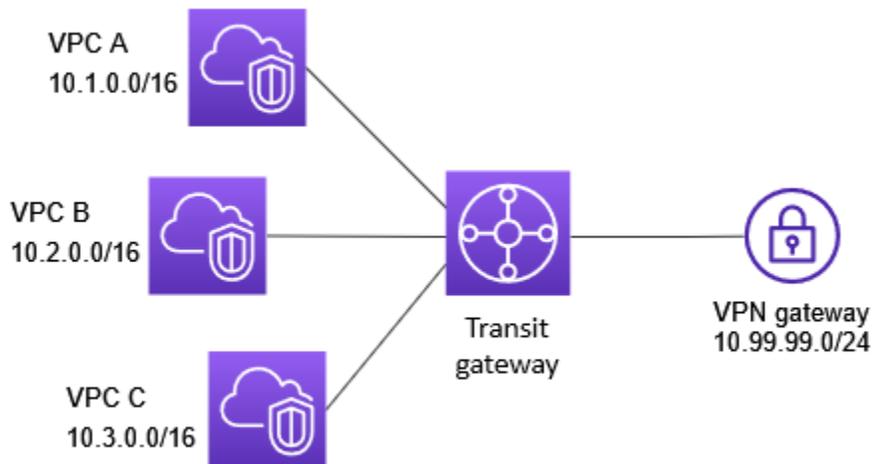
Vous pouvez configurer votre passerelle de transit en tant que routeur centralisé qui connecte toutes vos connexions VPC, AWS Direct Connect et Site-to-Site VPN. Dans ce scénario, tous les attachements sont associés à la table de routage par défaut de la passerelle de transit et propagés vers la table de routage par défaut de la passerelle de transit. Par conséquent, tous les attachements peuvent s'échanger des paquets, la passerelle de transit servant de simple routeur d'IP de couche 3.

## Table des matières

- [Présentation](#)
- [Ressources](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Dans ce scénario, il existe attachements de VPC et un attachement de Site-to-Site VPN à la passerelle de transit. Les paquets des sous-réseaux du VPC A, VPC B et VPC C qui sont destinés à un sous-réseau dans un autre VPC ou à la connexion VPN acheminent d'abord via la passerelle de transit.



## Ressources

Pour ce scénario, créez les ressources suivantes :

- Trois VPC. Pour en savoir plus sur la création d'un VPC, consultez la section [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Une passerelle de transit Pour de plus amples informations, veuillez consulter [the section called "Créer une passerelle de transit"](#).
- Trois attachements VPC sur la passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).
- Un attachement Site-to-Site VPN sur la passerelle de transit. Les blocs d'adresse CIDR de chaque VPC sont propagés vers la table de routage de la passerelle Transit Gateway. Lorsque la connexion VPN est opérationnelle, la session BGP est établie, le CIDR du Site-to-Site VPN se propage à la table de routage de passerelle de transit et les CIDR VPC sont ajoutés à la table BGP de la passerelle client. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit avec un VPN"](#).

Vérifiez que vous examinez la [configuration requise pour votre appareil de passerelle client](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN.

## Routage

Chaque VPC dispose d'une table de routage et il y a une table de routage pour la passerelle de transit.

### Tables de routage de VPC

Chaque VPC dispose d'une table de routage à deux entrées. La première entrée correspond à l'entrée par défaut pour le routage IPv4 local dans le VPC ; elle permet aux instances du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit. Le tableau suivant répertorie les routes du VPC A.

Destination	Cible
10.1.0.0/16	Locale
0.0.0.0/0	tgw-id

### Table de routage de passerelle de transit

Voici un exemple de table de routage par défaut pour les attachements présentés dans le diagramme précédent, la propagation du routage étant activée.

Destination	Target	Type de routage
10.1.0.0/16	<i>Attachement pour le VPC A</i>	propagée
10.2.0.0/16	<i>Attachement pour le VPC B</i>	propagée
10.3.0.0/16	<i>Attachement pour le VPC C</i>	propagée

Destination	Target	Type de routage
10.99.99.0/24	<i>Attachement pour la connexion VPN</i>	propagée

## Table BGP de passerelle client

La table BGP de la passerelle client contient les adresses CIDR VPC suivantes.

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

## Exemple : VPC isolés

Vous pouvez configurer votre passerelle de transit en tant que plusieurs routeurs isolés. Cela revient à utiliser plusieurs passerelles de transit, tout en offrant une plus grande flexibilité dans les cas où les routes et les attachements peuvent changer. Dans un tel scénario, chaque routeur isolé possède une seule table de routage. Tous les attachements associés à un routeur isolé se propagent et s'associent avec sa table de routage. Les attachements associés à un routeur isolé peuvent s'acheminer des paquets, mais ils ne peuvent pas acheminer ou recevoir des paquets venant d'attachements d'un autre routeur isolé.

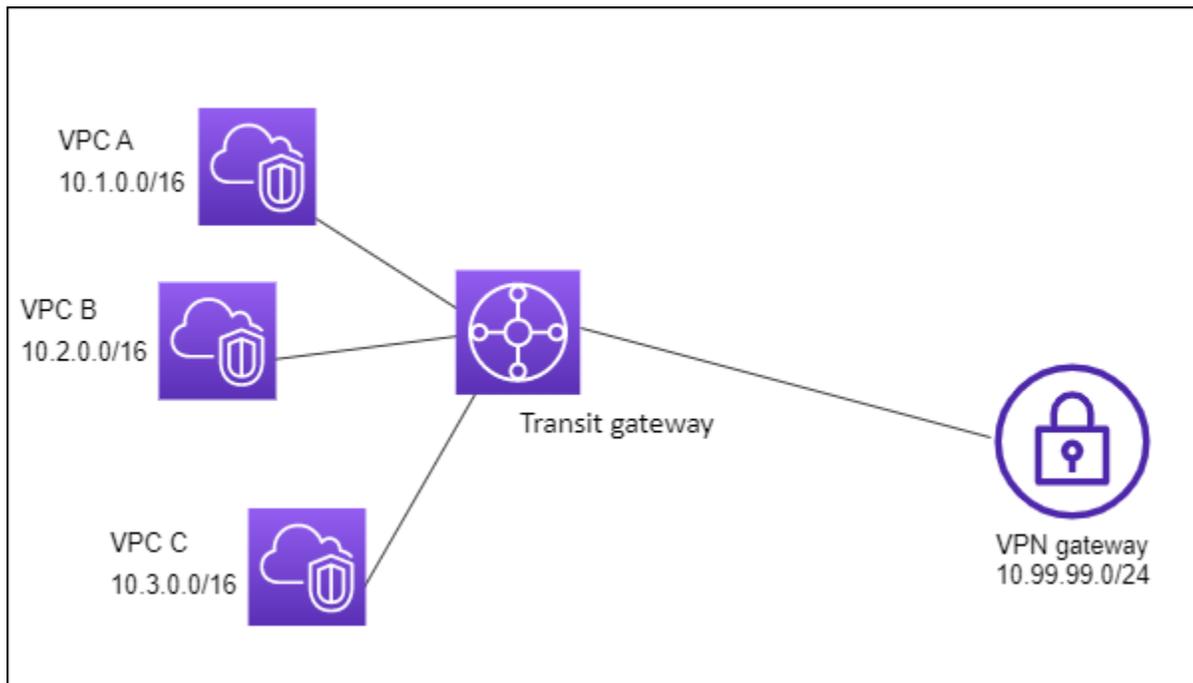
### Table des matières

- [Présentation](#)
- [Ressources](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Les paquets des VPC A, B et C sont acheminés vers la passerelle de transit. Les paquets provenant des sous-réseaux dans les VPC A, B et C qui ont Internet comme destination acheminent d'abord par le biais de la passerelle de transit, puis vers la connexion Site-to-Site VPN (si la destination se trouve dans ce réseau). Les paquets provenant d'un seul VPC et dont la destination est un sous-réseau

dans un autre VPC, par exemple compris entre 10.1.0.0 et 10.2.0.0, sont acheminés via la passerelle de transit, où ils sont bloqués car la table de routage de passerelle de transit ne contient pas de route pour eux.



## Ressources

Pour ce scénario, créez les ressources suivantes :

- Trois VPC. Pour en savoir plus sur la création d'un VPC, consultez la section [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Une passerelle de transit Pour de plus amples informations, veuillez consulter [the section called "Créer une passerelle de transit"](#).
- Trois attachements sur la passerelle de transit pour les trois VPC. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).
- Un attachement Site-to-Site VPN sur la passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit avec un VPN"](#). Vérifiez que vous examinez la [configuration requise pour votre appareil de passerelle client](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN.

Lorsque la connexion VPN est opérationnelle, la session BGP est établie, le CIDR du VPN se propage à la table de routage de la passerelle de transit et les CIDR VPC sont ajoutés à la table BGP de la passerelle client.

## Routage

Chaque VPC a une table de routage, et la passerelle de transit a deux tables de routage : une pour les VPC et une pour la connexion VPN.

### Tables de routage VPC A, VPC B et VPC C

Chaque VPC dispose d'une table de routage à deux entrées. La première entrée décrit l'entrée par défaut du routage IPv4 local du VPC. Cette entrée permet aux instances de ce VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit. Le tableau suivant répertorie les routes du VPC A.

Destination	Cible
10.1.0.0/16	Locale
0.0.0.0/0	tgw-id

### Tables de routage de passerelle de transit

Ce scénario utilise une table de routage pour les VPC et une table de routage pour la connexion VPN.

Les pièces jointes du VPC sont associées à la table de routage suivante, qui a une route propagée pour la pièce jointe du VPN.

Destination	Target	Type de routage
10.99.99.0/24	<i>Attachement pour la connexion VPN</i>	propagée

La pièce jointe VPN est associée à la table de routage suivante, qui a des routes propagées pour chacune des pièces jointes du VPC.

Destination	Target	Type de routage
10.1.0.0/16	<i>Attachement pour le VPC A</i>	propagée
10.2.0.0/16	<i>Attachement pour le VPC B</i>	propagée
10.3.0.0/16	<i>Attachement pour le VPC C</i>	propagée

Pour de plus amples informations sur la propagation de routes dans une table de routage de passerelle de transit, veuillez consulter [Propager une route vers une table de routage de passerelle de transit](#).

## Table BGP de passerelle client

La table BGP de la passerelle client contient les adresses CIDR VPC suivantes.

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

## Exemple : VPC isolés avec services partagés

Vous pouvez configurer votre passerelle de transit sous la forme de plusieurs routeurs isolés utilisant un service partagé. Cela revient à utiliser plusieurs passerelles de transit, tout en offrant une plus grande flexibilité dans les cas où les routes et les attachements peuvent changer. Dans un tel scénario, chaque routeur isolé possède une seule table de routage. Tous les attachements associés à un routeur isolé se propagent et s'associent avec sa table de routage. Les attachements associés à un routeur isolé peuvent s'acheminer des paquets, mais ils ne peuvent pas acheminer ou recevoir des paquets venant d'attachements d'un autre routeur isolé. Les attachements peuvent acheminer des paquets vers les services partagés, mais aussi recevoir des paquets provenant des services

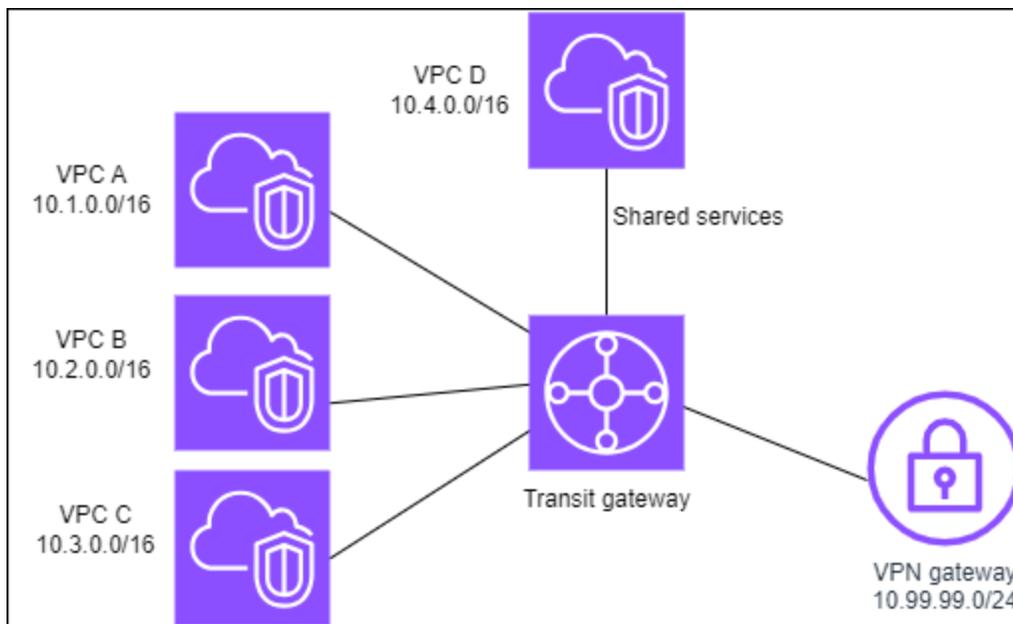
partagés. Vous pouvez utiliser ce scénario lorsque vous disposez de groupes nécessitant d'être isolés mais utilisant un service partagé, tel qu'un système de production.

## Table des matières

- [Présentation](#)
- [Ressources](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Les paquets provenant des sous-réseaux dans les VPC A, B et C qui ont Internet comme destination acheminent d'abord par le biais de la passerelle de transit, puis par le biais de la passerelle client vers la connexion Site-to-Site VPN. Les paquets provenant de sous-réseaux dans VPC A, VPC B ou VPC C qui ont une destination d'un sous-réseau dans VPC A, VPC B ou VPC C sont acheminés via la passerelle de transit, où ils sont bloqués car il n'y a pas de route pour eux dans la table de routage de passerelle de transit. Les paquets des VPC A, B et C ayant le VPC D comme destination sont acheminés via la passerelle de transit, puis vers le VPC D.



## Ressources

Pour ce scénario, créez les ressources suivantes :

- Quatre VPC. Pour en savoir plus sur la création d'un VPC, consultez la section [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Une passerelle de transit Pour de plus amples informations, veuillez consulter [Création d'une passerelle de transit](#).
- Quatre attachements VPC sur la passerelle de transit, un par VPC. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).
- Un attachement Site-to-Site VPN sur la passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit avec un VPN"](#).

Vérifiez que vous examinez la [configuration requise pour votre appareil de passerelle client](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN.

Lorsque la connexion VPN est opérationnelle, la session BGP est établie, le CIDR du VPN se propage à la table de routage de la passerelle de transit et les CIDR VPC sont ajoutés à la table BGP de la passerelle client.

- Chaque VPC isolé est associé à la table de routage isolée et propagé vers la table de routage partagée.
- Chaque VPC de services partagés est associé à la table de routage partagée et propagé aux deux tables de routage.

## Routage

Chaque VPC a une table de routage, et la passerelle de transit a deux tables de routage : une pour les VPC et une pour la connexion VPN et le VPC des services partagés.

### Tables de routage de VPC A, VPC B, VPC C et VPC D

Chaque VPC dispose d'une table de routage à deux entrées. La première entrée correspond à l'entrée par défaut pour le routage local dans le VPC ; elle permet aux instances du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit.

Destination	Cible
10.1.0.0/16	Locale
0.0.0.0/0	<i>ID de passerelle de transit</i>

## Tables de routage de passerelle de transit

Ce scénario utilise une table de routage pour les VPC et une table de routage pour la connexion VPN.

Les attachements A, B et C de VPC sont associés à la table de routage suivante, qui a une route propagée pour l'attachement VPN et une route propagée pour l'attachement du VPC D.

Destination	Target	Type de routage
10.99.99.0/24	<i>Attachement pour la connexion VPN</i>	propagée
10.4.0.0/16	<i>Attachement pour le VPC D</i>	propagée

L'attachement VPN et les attachements VPC de services partagés (VPC D) sont associés à la table de routage suivante, qui contient des entrées qui pointent vers chacune des attachements du VPC. Cela permet de communiquer avec les VPC à partir de la connexion VPN et du VPC de services partagés.

Destination	Target	Type de routage
10.1.0.0/16	<i>Attachement pour le VPC A</i>	propagée
10.2.0.0/16	<i>Attachement pour le VPC B</i>	propagée
10.3.0.0/16	<i>Attachement pour le VPC C</i>	propagée

Pour de plus amples informations, veuillez consulter [Propager une route vers une table de routage de passerelle de transit](#).

## Table BGP de passerelle client

La table BGP de la passerelle client contient les adresses CIDR pour les quatre VPC.

## Exemple : passerelles de transit appairées

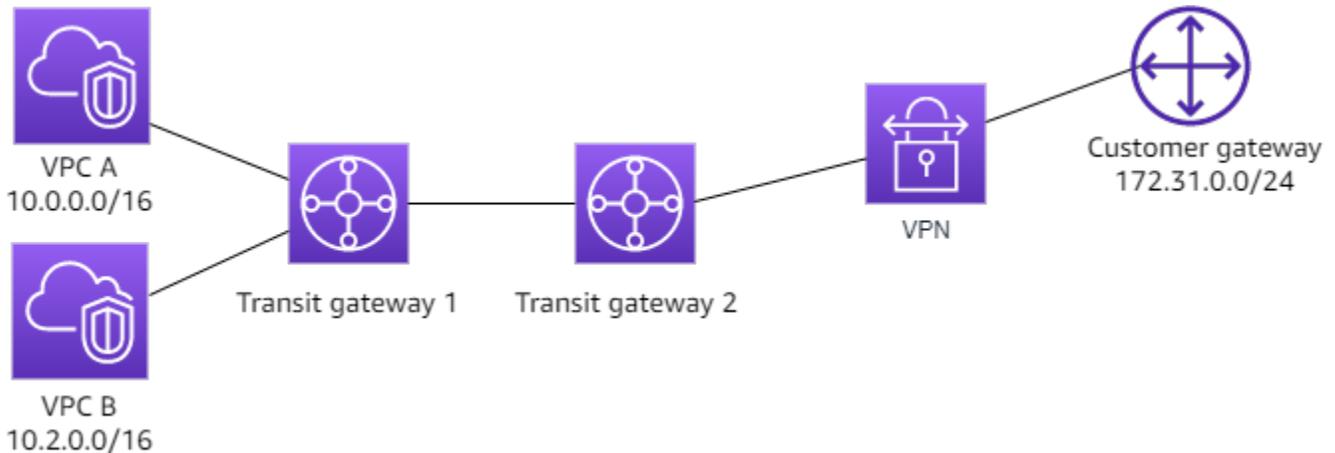
Vous pouvez créer une connexion d'appairage de passerelle de transit entre des passerelles de transit. Vous pouvez ensuite acheminer le trafic entre les attachements de chacune des passerelles de transit. Dans ce scénario, les attachements VPC et VPN sont associés aux tables de routage par défaut de la passerelle de transit et propagés vers les tables de routage par défaut de la passerelle de transit. Chaque table de routage de la passerelle de transit dispose d'un itinéraire statique pointant vers l'attachement de l'appairage de la passerelle de transit.

### Table des matières

- [Présentation](#)
- [Ressources](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. La passerelle de transit 1 comporte deux attachements VPC et la passerelle de transit 2, un attachement Site-to-Site VPN. Les paquets en provenance des sous-réseaux dans les VPC A et B ayant Internet comme destination sont d'abord acheminés via la passerelle 1, puis la 2, et enfin, vers la connexion VPN.



## Ressources

Pour ce scénario, créez les ressources suivantes :

- Deux VPC. Pour en savoir plus sur la création d'un VPC, consultez la section [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Deux passerelles de transit. Elles peuvent se trouver dans la même région ou dans des régions différentes. Pour de plus amples informations, veuillez consulter [the section called "Créer une passerelle de transit"](#).
- Deux attachements de VPC sur la première passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).
- Un attachement Site-to-Site VPN sur la seconde passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit avec un VPN"](#). Vérifiez que vous examinez la [configuration requise pour votre appareil de passerelle client](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN.
- Un attachement d'appairage de passerelle de transit entre les deux passerelles de transit. Pour de plus amples informations, veuillez consulter [Attachements d'appairage pour la passerelle de transit](#).

Lorsque vous créez les attachements VPC, les CIDR de chaque VPC sont propagés vers la table de routage la passerelle de transit 1. Lorsque la connexion VPN est en service, les actions suivantes se produisent :

- La session BGP est établie
- Le CIDR Site-to-Site VPN se propage à la table de routage pour la passerelle de transit 2

- Les CIDR des VPC sont ajoutés à la table BGP de la passerelle client

## Routage

Chaque VPC possède une table de routage et chaque passerelle de transit en a une également.

### Tables de routage VPC A et VPC B

Chaque VPC dispose d'une table de routage à deux entrées. La première entrée décrit l'entrée par défaut du routage IPv4 local du VPC. Cette entrée par défaut permet aux ressources du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit. Le tableau suivant répertorie les routes du VPC A.

Destination	Cible
10.0.0.0/16	locale
0.0.0.0/0	tgw-1-id

### Tables de routage de passerelle de transit

Voici un exemple de table de routage par défaut pour la passerelle de transit 1, avec la propagation de routage activée.

Destination	Target	Type de routage
10.0.0.0/16	<i>ID d'attachement du VPC A</i>	propagée
10.2.0.0/16	<i>ID d'attachement du VPC B</i>	propagée
0.0.0.0/0	<i>ID d'attachement de la connexion d'appairage</i>	statique

Voici un exemple de table de routage par défaut de la passerelle de transit 2, avec la propagation de routage activée.

Destination	Target	Type de routage
172.31.0.0/24	<i>ID d'attachement de la connexion VPN</i>	propagée
10.0.0.0/16	<i>ID d'attachement de la connexion d'appairage</i>	statique
10.2.0.0/16	<i>ID d'attachement de la connexion d'appairage</i>	statique

## Table BGP de passerelle client

La table BGP de la passerelle client contient les adresses CIDR VPC suivantes.

- 10.0.0.0/16
- 10.2.0.0/16

## Exemple : Routage sortant centralisé vers Internet

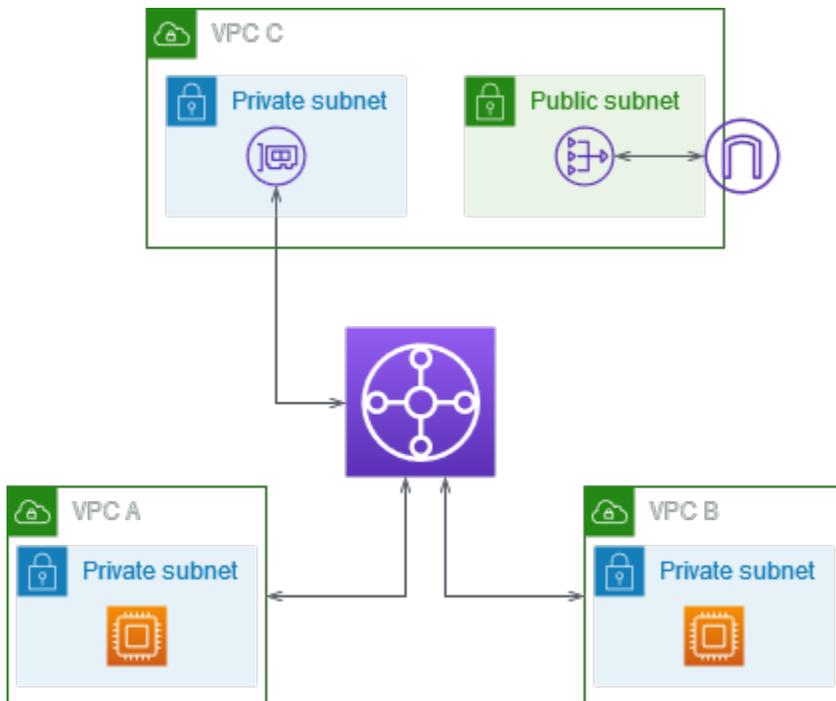
Vous pouvez configurer une passerelle de transit pour acheminer le trafic Internet sortant d'un VPC sans passerelle Internet vers un VPC qui contient une passerelle NAT et une passerelle Internet.

### Table des matières

- [Présentation](#)
- [Ressources](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Vous avez des applications dans VPC A et VPC B qui nécessitent un accès Internet sortant uniquement. Vous configurez le VPC C avec une passerelle NAT et une passerelle Internet, ainsi qu'un sous-réseau privé pour la connexion au VPC. Connectez tous les VPC à une passerelle Transit Gateway. Configurez le routage de sorte que le trafic Internet sortant provenant du VPC A et du VPC B traverse la passerelle Transit Gateway jusqu'au VPC C. La passerelle NAT du VPC C achemine le trafic vers la passerelle Internet.



## Ressources

Pour ce scénario, créez les ressources suivantes :

- Trois VPC avec des plages d'adresses IP qui ne se chevauchent pas. Pour plus d'informations, consultez [Créer un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Le VPC A et le VPC B disposent chacun de sous-réseaux privés avec des instances EC2.
- Le VPC C a les caractéristiques suivantes :
  - Une passerelle Internet associée au VPC. Pour plus d'informations, consultez la section [Création et attachement d'une passerelle Internet](#) dans le Guide de l'utilisateur Amazon VPC.
  - Sous-réseau public doté d'une passerelle NAT. Pour plus d'informations, consultez la section [Création et attachement d'une passerelle NAT](#) dans le Guide de l'utilisateur Amazon VPC.

- Un sous-réseau privé pour l'attachement de la passerelle de transit. Le sous-réseau privé doit se trouver dans la même zone de disponibilité que le sous-réseau public.
- Une passerelle de transit. Pour de plus amples informations, veuillez consulter [the section called “Créer une passerelle de transit”](#).
- Trois attachements VPC sur la passerelle de transit. Les blocs d'adresse CIDR de chaque VPC sont propagés vers la table de routage de la passerelle Transit Gateway. Pour de plus amples informations, veuillez consulter [the section called “Créer un attachement de passerelle de transit vers un VPC”](#). Pour le VPC C, vous devez créer l'attachement à l'aide du sous-réseau privé. Si vous créez l'attachement à l'aide du sous-réseau public, le trafic de l'instance est acheminé vers la passerelle Internet, mais la passerelle Internet interrompt le trafic car les instances ne possèdent pas d'adresse IP publique. En plaçant l'attachement dans le sous-réseau privé, le trafic est acheminé vers la passerelle NAT, et la passerelle NAT envoie le trafic vers la passerelle Internet en utilisant son adresse IP Elastic comme adresse IP source.

## Routage

Chaque VPC dispose de tables de routage et il y a une table de routage pour la passerelle Transit Gateway.

Tables de routage

- [Table de routage pour le VPC A](#)
- [Table de routage pour le VPC B](#)
- [Tables de routage du VPC C](#)
- [Table de routage de passerelle de transit](#)

### Table de routage pour le VPC A

Voici un exemple de table de routage. La première entrée permet aux instances du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit.

Destination	Target
<i>CIDR VPC A</i>	Locale

Destination	Target
0.0.0.0/0	<i>transit-gateway-id</i>

## Table de routage pour le VPC B

Voici un exemple de table de routage. Cette première entrée permet aux instances du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit.

Destination	Target
<i>CIDR VPC B</i>	Locale
0.0.0.0/0	<i>transit-gateway-id</i>

## Tables de routage du VPC C

Configurez le sous-réseau avec la passerelle NAT en tant que sous-réseau public en ajoutant un acheminement à la passerelle Internet. Laissez l'autre sous-réseau en tant que sous-réseau privé.

Voici un exemple de table de routage pour le sous-réseau public. La première entrée permet aux instances du VPC de communiquer entre elles. Les deuxième et troisième entrées acheminent le trafic pour le VPC A et le VPC B vers la passerelle Transit Gateway. La quatrième entrée achemine tout le reste du trafic IPv4 du sous-réseau vers la passerelle Internet.

Destination	Target
<i>CIDR VPC C</i>	Locale
<i>CIDR VPC A</i>	<i>transit-gateway-id</i>
<i>CIDR VPC B</i>	<i>transit-gateway-id</i>
0.0.0.0/0	<i>internet-gateway-id</i>

Voici un exemple de table de routage pour le sous-réseau privé. La première entrée permet aux instances du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle NAT.

Destination	Target
<i>CIDR VPC C</i>	Locale
0.0.0.0/0	<i>nat-gateway-id</i>

### Table de routage de passerelle de transit

Voici un exemple de table de routage de passerelle de transit. Les blocs d'adresse CIDR de chaque VPC sont propagés vers la table de routage de la passerelle Transit Gateway. L'acheminement statique envoie le trafic Internet sortant vers le VPC C. Vous pouvez éventuellement empêcher la communication entre les VPC en ajoutant un acheminement Blackhole pour chaque CIDR du VPC.

CIDR	Réseau de transit par passerelle	Type de routage
<i>CIDR VPC A</i>	<i>Attachement pour le VPC A</i>	propagée
<i>CIDR VPC B</i>	<i>Attachement pour le VPC B</i>	propagée
<i>CIDR VPC C</i>	<i>Attachement pour le VPC C</i>	propagée
0.0.0.0/0	<i>Attachement pour le VPC C</i>	statique

## Exemple : Appliance dans un VPC de services partagés

Vous pouvez configurer une appliance, telle qu'une appliance de sécurité, dans un VPC de services partagés. Tout le trafic qui est acheminé entre les réseaux de transit par passerelle est d'abord inspecté par l'appliance dans le VPC de services partagés. Lorsque le mode appliance est activé, une passerelle de transit sélectionne une seule interface réseau dans le VPC de l'appliance, à l'aide d'un algorithme de hachage de flux, vers laquelle envoyer du trafic pendant toute la durée de vie du flux. La passerelle de transit utilise la même interface réseau pour le trafic de retour. Cela garantit que le trafic est acheminé symétriquement dans les deux sens. Il est routé par le biais de la même zone de disponibilité dans l'attachement du VPC pendant toute la durée de vie du flux. Si vous avez plusieurs passerelles de transit dans votre architecture, chacune d'elles conserve sa propre affinité de session, et chaque passerelle de transit peut sélectionner une interface réseau différente.

Vous devez connecter exactement une passerelle Transit Gateway au VPC de l'appliance pour garantir la permanence du flux. La connexion de plusieurs passerelles de transit à un seul VPC d'appliance ne garantit pas la permanence du flux, car les passerelles de transit ne partagent pas les informations sur l'état du flux entre elles.

### Important

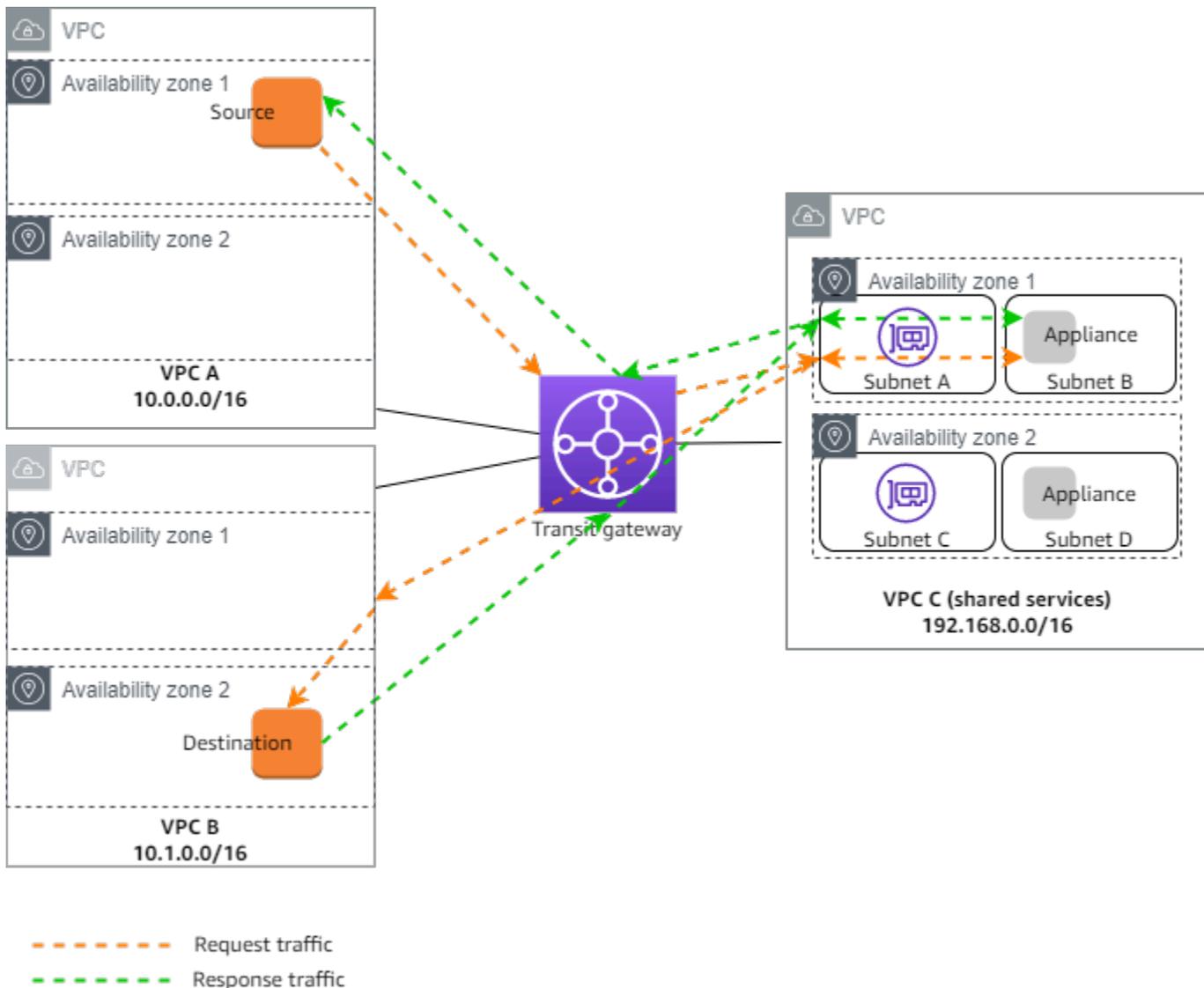
- Le trafic en mode appliance est acheminé correctement tant que le trafic source et de destination arrive vers un VPC centralisé (VPC d'inspection) à partir de la même pièce jointe de passerelle de transit. Le trafic peut chuter si la source et la destination entrent à partir de deux pièces jointes différentes de la passerelle de transit. Le mode Appliance ne s'applique pas au trafic entrant dans le réseau via un VPN.
- L'activation du mode appliance sur une pièce jointe existante peut affecter l'itinéraire actuel de cette pièce jointe, car la pièce jointe peut traverser n'importe quelle zone de disponibilité. Lorsque le mode appliance n'est pas activé, le trafic est maintenu dans la zone de disponibilité d'origine.

### Table des matières

- [Présentation](#)
- [Appliances avec état et mode appliance](#)
- [Routage](#)

## Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. La passerelle de transit comporte trois attachements de VPC. Le VPC C est un VPC de services partagés. Le trafic entre le VPC A et le VPC B est d'abord acheminé vers la passerelle de transit, puis ensuite vers une appliance de sécurité dans le VPC C pour inspection avant d'être dirigé vers sa destination finale. La solution matérielle-logicielle est une appliance avec état, par conséquent, le trafic de demande et de réponse sont inspectés tous les deux. Pour une haute disponibilité, il existe une appliance dans chaque zone de disponibilité du VPC C.



Pour ce scénario; vous créez les ressources suivantes :

- Trois VPC. Pour de plus amples informations sur la création d'un VPC, veuillez consulter [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon Virtual Private Cloud.
- Une passerelle de transit Pour plus d'informations, consultez [the section called “Créer une passerelle de transit”](#).
- Trois attachements de VPC : un pour chacun des VPC. Pour plus d'informations, consultez [the section called “Créer un attachement de passerelle de transit vers un VPC”](#).

Pour chaque attachement de VPC, spécifiez un sous-réseau dans chaque zone de disponibilité. Pour le VPC de services partagés, il s'agit des sous-réseaux où le trafic est acheminé vers le VPC à partir de la passerelle de transit. Dans l'exemple précédent, il s'agit des sous-réseaux A et C.

Pour l'attachement du VPC C, activez le support du mode de l'appliance afin que le trafic de réponse soit acheminé vers la même zone de disponibilité dans le VPC C que le trafic source.

La console Amazon VPC prend en charge le mode appliance. Vous pouvez aussi utiliser l'API Amazon VPC, un kit SDK AWS, la AWS CLI pour activer le mode appliance, ou AWS CloudFormation. Par exemple, ajoutez `--options ApplianceModeSupport=enable` à la commande [create-transit-gateway-vpc-attachment](#) ou [modify-transit-gateway-vpc-attachment](#).

#### Note

La stabilité du flux en mode appliance est garantie uniquement pour le trafic source et de destination qui provient du VPC d'inspection.

## Appliances avec état et mode appliance

Si vos attachements de VPC s'étendent sur plusieurs zones de disponibilité et que vous devez acheminer le trafic entre les hôtes de source et de destination par le biais de la même appliance pour une inspection avec état, activez le support du mode de l'appliance pour l'attachement du VPC dans lequel se trouve l'appliance.

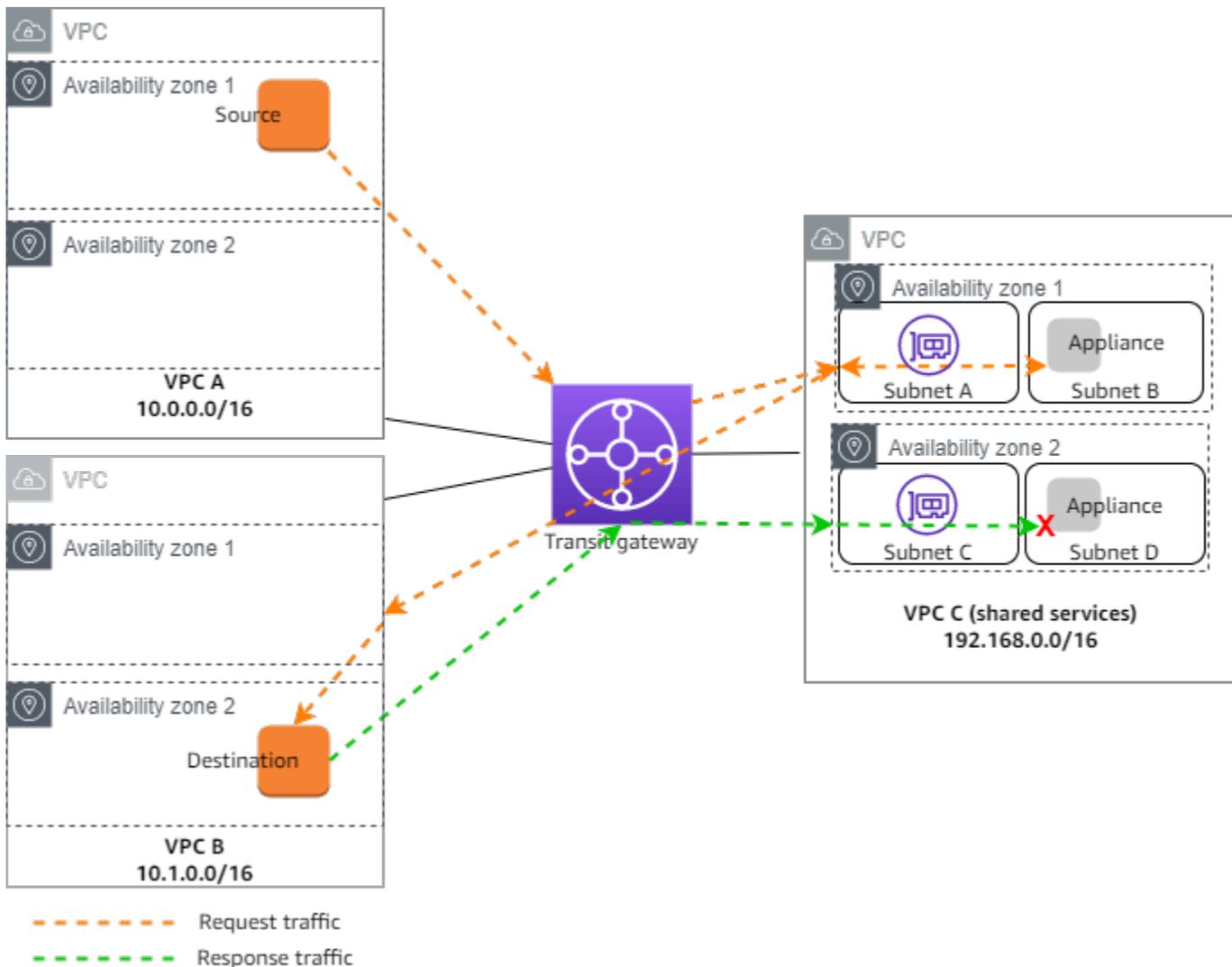
Pour plus d'informations, consultez [Architecture d'inspection centralisée](#) dans le blog AWS.

### Comportement lorsque le mode appliance n'est pas activé

Lorsque le mode appliance n'est pas activé, une passerelle de transit tente de maintenir le trafic acheminé entre les attachements du VPC dans la zone de disponibilité d'origine jusqu'à ce

qu'il atteigne sa destination. Le trafic traverse les zones de disponibilité entre les attachements uniquement en cas de défaillance de la zone de disponibilité ou si aucun sous-réseau n'est associé à un attachement de VPC dans cette zone de disponibilité.

Le diagramme suivant montre un flux de trafic lorsque le support du mode de l'appliance n'est pas activé. Le trafic de réponse provenant de la zone de disponibilité 2 du VPC B est acheminé par la passerelle de transit vers la même zone de disponibilité du VPC C. Le trafic est donc abandonné, car l'appliance dans la zone de disponibilité 2 n'a pas connaissance de la demande d'origine provenant de la source du VPC A.



## Routage

Chaque VPC dispose d'une ou de plusieurs tables de routage et la passerelle de transit comporte deux tables de routage.

## Tables de routage de VPC

### VPC A et VPC B

Les VPC A et B dispose de tables de routage avec 2 entrées. La première entrée décrit l'entrée par défaut du routage IPv4 local du VPC. Cette entrée par défaut permet aux ressources du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic du sous-réseau IPv4 vers la passerelle de transit. Voici la table de routage pour le VPC A :

Destination	Cible
10.0.0.0/16	locale
0.0.0.0/0	tgw-id

### VPC C

Le VPC de services partagés (VPC C) dispose de tables de routage différentes pour chaque sous-réseau. Le sous-réseau A est utilisé par la passerelle de transit (vous spécifiez ce sous-réseau lorsque vous créez l'attachement de VPC). La table de routage du sous-réseau A achemine tout le trafic vers l'appliance du sous-réseau B.

Destination	Target
192.168.0.0/16	Locale
0.0.0.0/0	appliance-eni-id

La table de routage du sous-réseau B, qui contient l'appliance, renvoie le trafic vers la passerelle de transit.

Destination	Target
192.168.0.0/16	Locale
0.0.0.0/0	tgw-id

## Tables de routage de passerelle de transit

Cette passerelle de transit utilise une table de routage pour le VPC A et le VPC B et une table de routage pour le VPC de services partagés (VPC C).

Les attachements des VPC A et B sont associées à la table de routage suivante. La table de routage achemine tout le trafic vers le VPC C.

Destination	Target	Type de routage
0.0.0.0/0	<i>ID d'attachement du VPC C</i>	statique

L'attachement du VPC C est associé à la table de routage suivante. Il achemine le trafic vers les VPC A et B.

Destination	Target	Type de routage
10.0.0.0/16	<i>ID d'attachement du VPC A</i>	propagée
10.1.0.0/16	<i>ID d'attachement du VPC B</i>	propagée

# Utiliser des passerelles de transit

Vous pouvez utiliser des passerelles de transit à l'aide de la console Amazon VPC ou de la AWS CLI.

## Table des matières

- [Passerelles de transit](#)
- [Attachements de passerelle de transit vers un VPC](#)
- [Attachements VPN de passerelle de transit](#)
- [Attachements d'une passerelle de transit à une passerelle Direct Connect](#)
- [Attachements d'appairage pour la passerelle de transit](#)
- [Attachements Transit Gateway Connect et pairs Transit Gateway Connect](#)
- [Tables de routage de passerelle de transit](#)
- [Tables de stratégie de passerelle de transit](#)
- [Multicast sur les passerelles de transit](#)

## Passerelles de transit

Une passerelle de transit vous permet d'attacher des VPC et des connexions VPN, et d'acheminer le trafic entre eux. Une passerelle de transit fonctionne de part Comptes AWS en part et vous pouvez l'utiliser AWS RAM pour partager votre passerelle de transit avec d'autres comptes. Une fois que vous avez partagé une passerelle de transit avec une autre Compte AWS, le propriétaire du compte peut associer ses VPC à votre passerelle de transit. Un utilisateur de l'un des comptes peut supprimer l'attachement à tout moment.

Vous pouvez activer la multicast sur une passerelle de transit, puis créer un domaine multicast de passerelle de transit qui autorise l'envoi du trafic multicast à partir de votre source multicast vers des membres de groupe multicast sur des attachements de VPC que vous associez au domaine.

Chaque VPC ou attachement VPN est associé à une seule table de routage. Cette table de routage commande le prochain saut pour le trafic venant de cet attachement de ressource. Une table de routage à l'intérieur de la passerelle de transit autorise les CIDR et les cibles IPv4 ou IPv6. Les cibles sont les VPC et les connexions VPN. Lorsque vous attachez un VPC ou créez une connexion VPN sur la passerelle de transit, l'attachement est associé à la table de routage par défaut de la passerelle de transit.

Vous pouvez créer d'autres tables de routage à l'intérieur de la passerelle de transit et modifier l'association de VPC ou de VPN avec ces tables de routage. Vous pouvez ainsi segmenter votre réseau. Par exemple, vous pouvez associer des VPC en développement avec une table de routage et des VPC de production avec une autre. Cela vous permettra de créer des réseaux isolés au sein d'une passerelle de transit similaires au routage et au transfert virtuels (VRF) des réseaux traditionnels.

Les passerelles de transit prennent en charge le routage dynamique et statique entre les VPC et les connexions VPN joints. Vous pouvez activer ou désactiver la propagation du routage pour chaque attachement. Les attachements d'appariement de passerelle de transit prennent uniquement en charge le routage statique. Toutefois, vous ne pouvez pas ajouter d'itinéraire statique pointant vers un peering entre deux passerelles de transit dans la même région.

Vous pouvez éventuellement associer un ou plusieurs blocs d'adresse CIDR IPv4 ou IPv6 à votre passerelle de transit. Spécifiez une adresse IP à partir du bloc d'adresse CIDR lorsque vous établissez un pair Transit Gateway Connect pour un [attachement Transit Gateway Connect](#). Vous pouvez associer n'importe quelle plage d'adresses IP publiques ou privées, sauf les adresses de la plage d'adresses 169.254.0.0/16, et des plages qui se chevauchent avec des adresses de vos attachements VPC et des réseaux sur site. Pour plus d'informations sur les blocs d'adresse CIDR IPv4 et IPv6, consultez [VPC et des sous-réseaux](#) dans le Guide de l'utilisateur Amazon VPC.

## Tâches

- [Créer une passerelle de transit](#)
- [Afficher vos passerelles de transit](#)
- [Ajouter ou modifier les balises d'une passerelle de transit](#)
- [Modifier une passerelle de transit](#)
- [Partager une passerelle de transit](#)
- [Accepter un partage de ressources](#)
- [Accepter un attachement partagé](#)
- [Supprimer une passerelle de transit](#)

## Créer une passerelle de transit

Lorsque vous créez une passerelle de transit, nous créons une table de routage de la passerelle de transit par défaut et nous l'utilisons comme table de routage d'association et table de routage de propagation par défaut. Si vous choisissez de ne pas créer la table de routage de la passerelle de

transit par défaut, vous pouvez en créer une ultérieurement. Pour plus d'informations sur les routes et les tables de routage, consultez [???](#).

Pour créer une passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Passerelles de transit.
3. Choisissez Create transit gateway (Créer une passerelle de transit).
4. Pour la Name tag (Balise nom), saisissez éventuellement un nom pour la passerelle de transit. Un nom permet d'identifier plus facilement une passerelle au sein d'une liste de passerelles. Lorsque vous ajoutez une Balise Nom, une balise est créée avec une clé de Nom et avec une valeur égale à la valeur saisie.
5. Pour Description, saisissez éventuellement une description pour la passerelle de transit .
6. Pour Amazon side Autonomous System Number (ASN), laissez la valeur par défaut pour utiliser l'ASN par défaut ou saisissez l'ASN privé de votre passerelle de transit. Il doit s'agir de l'ASN correspondant au AWS côté d'une session BGP (Border Gateway Protocol).

La plage va de 64512 à 65534 pour les ASN de 16 bits.

La plage va de 4200000000 à 4294967294 pour les ASN de 32 bits.

Si vous avez un déploiement multi-régions, nous vous recommandons d'utiliser un seul ASN pour chacune de vos passerelles de transit.

7. Pour DNS support (Support DNS), sélectionnez cette option si vous désirez que le VPC résolve les noms d'hôte de DNS IPv4 publiques vers des adresse IPv4 privées en cas d'interrogation de la part d'instances d'un autre VPC attaché à la passerelle de transit.
8. Pour VPN ECMP support (Prise en charge du protocole de VPN ECMP), sélectionnez cette option si vous avez besoin d'une prise en charge du routage ECMP (Equal Cost Multipath) entre des tunnels VPN. Si des connexions annoncent les mêmes CIDR, le trafic est distribué de façon égale.

Lorsque vous sélectionnez cette option, la version du moteur de cache annoncée, les attributs BGP tels que le AS-path et les communautés de préférence doivent être identiques.

**Note**

Pour utiliser l'ECMP, vous devez créer une connexion VPN qui utilise le routage dynamique. Les connexions VPN qui utilisent le routage statique ne prennent pas en charge l'ECMP.

9. Pour Default route table association (Association de table de routage par défaut), sélectionnez cette option pour associer automatiquement les réseaux de transit par passerelle avec la table de routage par défaut pour la passerelle de transit.
10. Pour Default route table propagation (Propagation de table de routage par défaut), sélectionnez cette option pour propager automatiquement les réseaux de transit par passerelle vers la table de routage par défaut pour la passerelle de transit.
11. (Facultatif) Pour utiliser la passerelle de transit comme routeur pour du trafic de multicast, sélectionnez Multicast support (Support multicast).
12. Pour Auto accept shared attachments (Accepter automatiquement les attachements partagés), sélectionnez cette option pour accepter automatiquement les attachements entre comptes.
13. (Facultatif) Pour Transit gateway CIDR blocks (Blocs d'adresses CIDR de passerelle de transit), spécifiez un ou plusieurs blocs d'adresse CIDR IPv4 ou IPv6 pour votre passerelle de transit.

Vous pouvez spécifier un bloc d'adresse CIDR de taille /24 ou plus grand (par exemple, /23 ou /22) pour IPv4, ou un bloc d'adresse CIDR de taille /64 ou plus (par exemple, /63 ou /62) pour IPv6. Vous pouvez associer n'importe quelle plage d'adresses IP publiques ou privées, sauf les adresses de la plage 169.254.0.0/16, et des plages qui se chevauchent avec les adresses de vos attachements VPC et des réseaux sur site.

14. Choisissez Create transit gateway (Créer une passerelle de transit).

Pour créer une passerelle de transit à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway](#).

## Afficher vos passerelles de transit

Pour afficher vos passerelles de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le volet de navigation, choisissez Passerelles de transit. Les informations de la passerelle de transit sont affichés sous la liste des passerelles sur la page.

Pour consulter vos passerelles de transport en commun à l'aide du AWS CLI

Utilisez la commande [describe-transit-gateways](#).

## Ajouter ou modifier les balises d'une passerelle de transit

Ajoutez des balises à vos ressources pour les organiser et les identifier, par exemple selon leur but, leur propriétaire ou leur environnement. Vous pouvez ajouter plusieurs balises à chaque passerelle de transit. Les clés de balise doivent être uniques pour chaque passerelle de transit. Si vous ajoutez une balise avec une clé qui est déjà associée à la passerelle de transit, la valeur de cette balise sera mise à jour. Pour de plus amples informations, veuillez consulter [Balisage de vos ressources Amazon EC2](#).

Ajouter des balises à une passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Passerelles de transit.
3. Sélectionnez la passerelle de transit pour laquelle vous souhaitez ajouter ou modifier des balises.
4. Choisissez l'onglet Tags (Balises) dans la partie inférieure de la page.
5. Choisissez Gérer les balises.
6. Choisissez Add new tag (Ajouter une nouvelle balise).
7. Saisissez une clé et une valeur pour la balise.
8. Choisissez Enregistrer.

## Modifier une passerelle de transit

Vous pouvez modifier les options de configuration de votre passerelle de transit. Lorsque vous modifiez une passerelle de transit, les options modifiées sont appliquées uniquement aux nouveaux attachements de passerelle de transit. Vos attachements de la passerelle de transit existants ne sont pas modifiés et ne voient pas d'interruption de service.

Vous ne pouvez pas modifier une passerelle de transit qui a été partagée avec vous.

Vous ne pouvez pas supprimer un bloc d'adresse CIDR pour la passerelle de transit si l'une des adresses IP est actuellement utilisée pour un [pair Connect](#).

### Modification d'une passerelle de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Passerelles de transit.
3. Choisissez la passerelle de transit à modifier.
4. Choisissez Actions, Modify transit gateway (Modifier la passerelle de transit).
5. Modifiez les options selon vos besoins, puis choisissez Modify transit gateway (Modifier la passerelle de transit).

Pour modifier votre passerelle de transit à l'aide du AWS CLI

Utilisez la commande [modify-transit-gateway](#).

## Partager une passerelle de transit

Vous pouvez l'utiliser AWS RAM pour [partager une passerelle de transit](#) entre différents comptes ou au sein de votre organisation dans AWS Organizations. Suivez la procédure suivante pour partager une passerelle de transit que vous possédez.

Vous devez activer le partage de ressources à partir du compte de gestion de votre organisation. Pour plus d'informations sur l'activation du partage des ressources, consultez la section [Activer le partage avec AWS les organisations](#) dans le guide de AWS RAM l'utilisateur.

### Partage d'une passerelle de transit

1. Ouvrez la AWS RAM console à l'adresse <https://console.aws.amazon.com/ram/>.
2. Sélectionnez Create a resource share (Créer un partage de ressources).
3. Sous Name (Nom), saisissez un nom descriptif pour le partage de ressources.
4. Pour Sélectionner le type de ressource, choisissez Passerelles de transit. Sélectionnez la passerelle de transit.
5. (Facultatif) Pour Mandataires, ajoutez les mandataires du partage de ressources. Pour chaque Compte AWS unité d'organisation ou organisation, spécifiez son ID et choisissez Ajouter.

Pour Autoriser les comptes externes, indiquez si vous souhaitez autoriser le partage de cette ressource avec Comptes AWS des comptes externes à votre organisation.

6. (Facultatif) Sous Tags (Balises), saisissez une clé et une paire de valeur de balise pour chaque balise. Ces balises sont appliquées au partage de ressource mais pas à la passerelle de transit.
7. Choisissez Créer une ressource.

## Accepter un partage de ressources

Si vous avez été ajouté à un partage de ressource, vous recevez une invitation à rejoindre le partage de ressource. Vous devez accepter le partage de ressource avant de pouvoir accéder aux ressources partagées.

Pour accepter un partage de ressources

1. Ouvrez la AWS RAM console à l'[adresse https://console.aws.amazon.com/ram/](https://console.aws.amazon.com/ram/).
2. Dans le panneau de navigation, choisissez Shared with me (Partagé avec moi), Resource shares (Partages de ressources).
3. Sélectionnez le partage de ressources.
4. Sélectionnez Accepter un partage de ressource.
5. Pour afficher la passerelle de transit partagée, ouvrez la page Transit Gateways (Passerelles de transit) dans la console Amazon VPC.

## Accepter un attachement partagé

Si vous n'avez pas activé la fonctionnalité Auto accept shared attachments (Accepter automatiquement les attachements partagés) lorsque vous avez créé votre passerelle de transit, vous devez accepter manuellement les attachements comptes multiples (partagés).

Pour accepter manuellement un attachement partagé

1. Ouvrez la console Amazon VPC à l'[adresse https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/).
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement de la passerelle de transit en attente d'acceptation.
4. Choisissez Actions, Accept transit gateway attachment (Accepter le réseau de transit par passerelle).

Pour accepter une pièce jointe partagée à l'aide du AWS CLI

Utilisez la commande [accept-transit-gateway-vpc-attachment](#).

## Supprimer une passerelle de transit

Vous ne pouvez pas supprimer une passerelle de transit avec des attachements existants. Vous devez d'abord supprimer tous les attachements avant de supprimer une passerelle de transit.

Pour supprimer une passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Choisissez la passerelle de transit à supprimer.
3. Choisissez Actions, Delete transit gateway (Supprimer la passerelle de transit). Saisissez **delete** et choisissez Delete (Supprimer) pour confirmer la suppression.

Pour supprimer une passerelle de transit à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway](#).

## Attachements de passerelle de transit vers un VPC

Lorsque vous attachez un VPC à une passerelle de transit, vous devez spécifier un sous-réseau depuis chaque zone de disponibilité que la passerelle de transit va utiliser pour acheminer le trafic. La spécification d'un sous-réseau depuis une zone de disponibilité permet au trafic d'atteindre les ressources de chaque sous-réseau au sein de cette zone de disponibilité.

### Limites

- Lorsque vous attachez un VPC à une passerelle de transit, les ressources des zones de disponibilité où il n'existe pas d'attachement de passerelle de transit ne peuvent pas atteindre celle-ci. S'il existe une route vers la passerelle de transit dans une table de routage de sous-réseau, le trafic n'est transféré vers la passerelle de transit que lorsqu'elle possède un attachement dans un sous-réseau de la même zone de disponibilité.
- Les ressources dans un VPC attaché à une passerelle de transit ne peuvent pas accéder aux groupes de sécurité d'un VPC différent également attaché à la même passerelle de transit.
- Une passerelle de transit n'est pas compatible avec la résolution DNS des noms DNS personnalisés lors de la configurations de VPC attachés à l'aide de zones hébergées privées dans Amazon Route 53. Pour configurer la résolution des noms pour les zones hébergées privées pour

tous les VPC connectés à une passerelle de transit, consultez la section [Gestion DNS centralisée du cloud hybride avec Amazon Route 53 et AWS Transit Gateway](#).

- Une passerelle de transit ne prend pas en charge le routage entre des VPC avec des CIDR identiques. Si vous attachez un VPC à une passerelle de transit et que son CIDR est identique au CIDR d'un autre VPC déjà attaché à la passerelle de transit, les acheminements du VPC nouvellement attaché ne sont pas propagés dans la table d'acheminement de la passerelle de transit.
- Vous ne pouvez pas créer de pièce jointe pour un sous-réseau de VPC résidant dans une zone locale. Toutefois, vous pouvez configurer votre réseau de sorte que les sous-réseaux de la zone locale puissent se connecter à une passerelle de transit via la zone de disponibilité parente. Pour plus d'informations, consultez [Connexion des sous-réseaux de la zone locale à une passerelle de transit](#).
- Vous ne pouvez pas créer un attachement de la passerelle de transit en utilisant des sous-réseaux uniquement IPv6. Les sous-réseaux d'attachement de la passerelle de transit doivent également prendre en charge les adresses IPv4.
- Une passerelle de transit doit avoir au moins un attachement VPC avant de pouvoir être ajoutée à une table de routage.

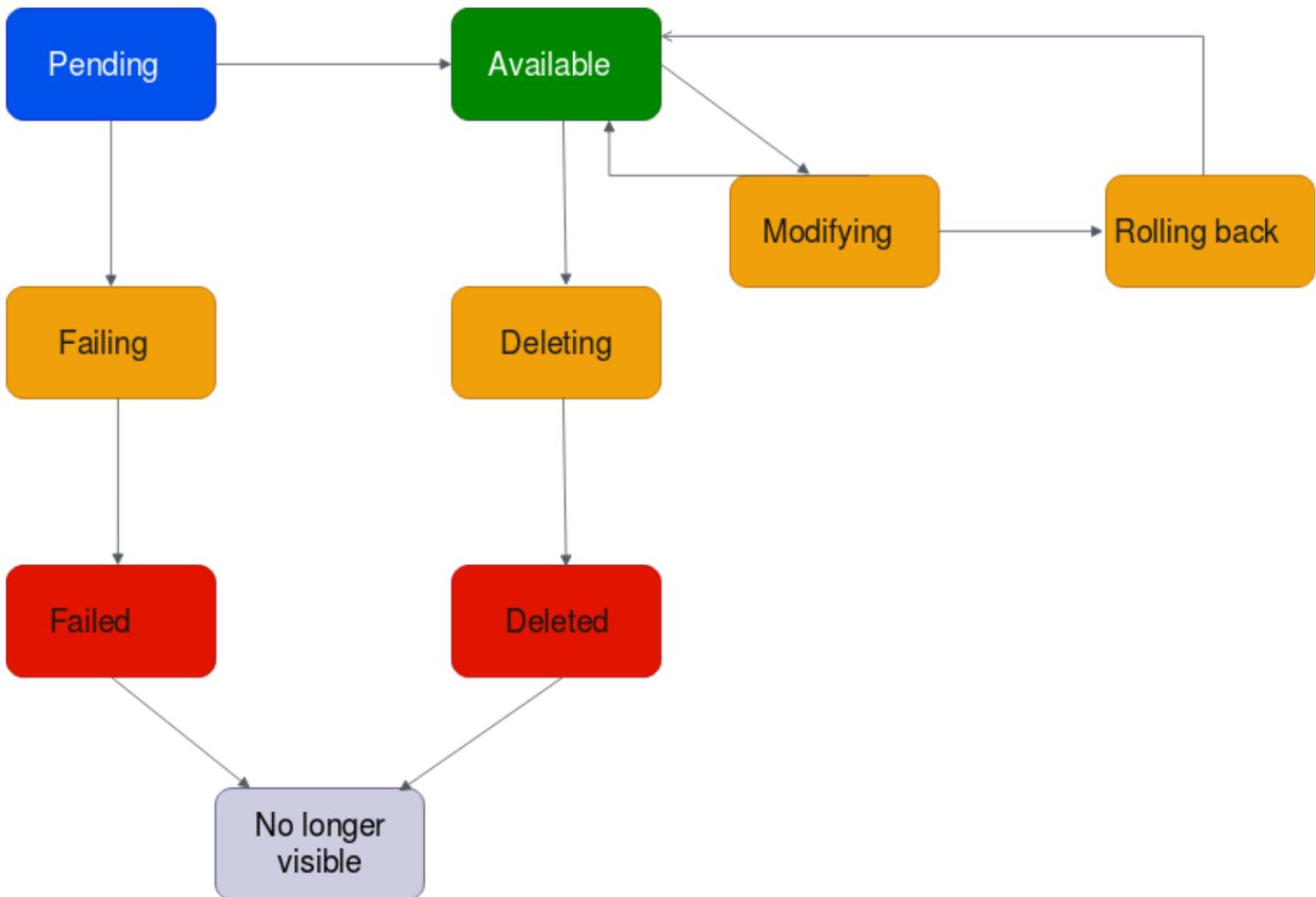
## Table des matières

- [Cycle de vie des attachements VPC](#)
- [Créer un attachement de passerelle de transit vers un VPC](#)
- [Modifier l'attachement de votre VPC](#)
- [Modifier les balises d'attachement de votre VPC](#)
- [Afficher vos attachements de VPC](#)
- [Supprimer un attachement de VPC](#)
- [Résolution des problèmes liés à la création d'attachements VPC](#)

## Cycle de vie des attachements VPC

Un attachement VPC passe par différentes étapes, à partir du lancement de la demande. Vous pouvez être amené à effectuer des actions à chaque étape. À la fin de son cycle de vie, l'attachement du VPC reste visible dans la Amazon Virtual Private Cloud Console et dans l'API ou la sortie de la ligne de commande, pendant une période déterminée.

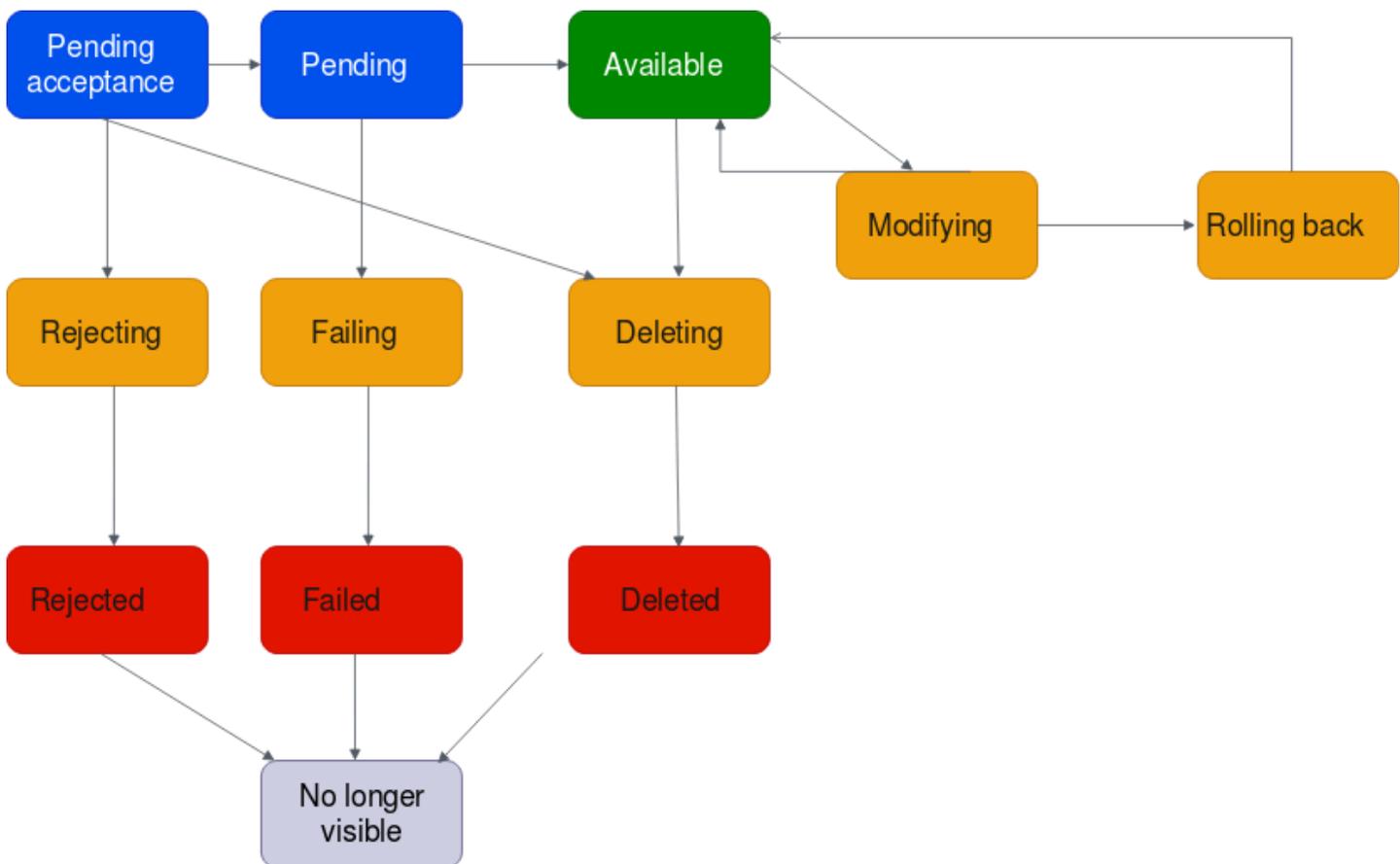
Le diagramme suivant montre les états par lesquels qu'un attachement peut passer dans une configuration de compte unique ou une configuration inter-comptes pour laquelle l'acceptation automatique des attachements partagés est activée.



- En attente : une demande d'attachement VPC a été lancée et est en processus de mise en service. À ce stade, l'attachement peut échouer, ou peut aller à available.
- Échec : une demande d'attachement VPC échoue. À ce stade, l'attachement VPC va à failed.
- Échec : la demande de l'attachement VPC a échoué. Dans cet état, il ne peut pas être supprimé. L'attachement VPC défaillant reste visible pendant 2 heures, puis n'est plus visible.
- Disponible : l'attachement VPC est disponible et le trafic peut circuler entre le VPC et la passerelle de transit. A ce stade, l'attachement peut aller à modifying, ou aller à deleting.
- Suppression : attachement VPC en cours de suppression. A ce stade, l'attachement peut aller à deleted.
- Supprimé : un attachement VPC available a été supprimé. Dans cet état, l'attachement VPC ne peut pas être modifié. L'attachement VPC reste visible pendant 2 heures, puis n'est plus visible.

- **Modification** : une demande a été faite pour modifier les propriétés de l'attachement VPC. A ce stade, l'attachement peut aller à `available`, ou aller à `rolling back`.
- **Retour arrière** : la demande de modification de l'attachement VPC ne peut pas être complétée et le système annule toutes les modifications qui ont été apportées. A ce stade, l'attachement peut aller à `available`.

Le diagramme suivant montre les états par lesquels qu'un attachement peut passer dans une configuration inter-comptes pour laquelle l'acceptation automatique des attachements partagés est désactivée.



- **Acceptation en attente** : La demande d'attachement VPC est en attente d'acceptation. À ce stade, l'attachement peut aller à `pending`, à `rejecting`, ou à `deleting`.
- **Rejet** : attachement VPC en train d'être rejeté. A ce stade, l'attachement peut aller à `rejected`.
- **Rejeté** : un attachement VPC `pending acceptance` a été rejeté. Dans cet état, l'attachement VPC ne peut pas être modifié. L'attachement VPC reste visible pendant 2 heures, puis n'est plus visible.

- En attente : la demande d'attachement VPC a été acceptée et est en processus de mise en service. À ce stade, l'attachement peut échouer, ou peut aller à `available`.
- Échec : une demande d'attachement VPC échoue. À ce stade, l'attachement VPC va à `failed`.
- Échec : la demande de l'attachement VPC a échoué. Dans cet état, il ne peut pas être supprimé. L'attachement VPC défaillant reste visible pendant 2 heures, puis n'est plus visible.
- Disponible : l'attachement VPC est disponible et le trafic peut circuler entre le VPC et la passerelle de transit. A ce stade, l'attachement peut aller à `modifying`, ou aller à `deleting`.
- Suppression : attachement VPC en cours de suppression. A ce stade, l'attachement peut aller à `deleted`.
- Supprimé : un attachement VPC `available` ou `pending acceptance` a été supprimé. Dans cet état, l'attachement VPC ne peut pas être modifié. L'attachement VPC reste visible 2 heures, puis n'est plus visible.
- Modification : une demande a été faite pour modifier les propriétés de l'attachement VPC. A ce stade, l'attachement peut aller à `available`, ou aller à `rolling back`.
- Retour arrière : la demande de modification de l'attachement VPC ne peut pas être complétée et le système annule toutes les modifications qui ont été apportées. A ce stade, l'attachement peut aller à `available`.

## Créer un attachement de passerelle de transit vers un VPC

Pour créer un attachement de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).
4. Pour Name tag (Balise nom), saisissez éventuellement un nom pour réseau de transit par passerelle.
5. Pour Transit gateway ID (ID de la passerelle de transit), choisissez la passerelle de transit pour l'attachement. Vous pouvez choisir une passerelle de transit que vous possédez ou une qui a été partagée avec vous.
6. Pour Attachment type (Type d'attachement), choisissez VPC.
7. Choisissez d'activer le support DNS, le support IPv6 et le support du mode appliance.

Si le mode appliance est choisi, le flux de trafic entre une source et une destination utilise la même zone de disponibilité pour l'attachement VPC pendant toute la durée de vie de ce flux.

8. Pour VPC ID (ID de VPC), choisissez le VPC à attacher à la passerelle de transit.

Ce VPC doit avoir au moins un sous-réseau associé.

9. Pour Subnet IDs (ID de sous-réseau), sélectionnez un sous-réseau pour chaque zone de disponibilité utilisable par la passerelle de transit pour acheminer le trafic. Vous devez sélectionner au moins un sous-réseau. Vous pouvez sélectionner un seul sous-réseau par zone de disponibilité.
10. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de transit).

Pour créer une pièce jointe VPC à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-vpc-attachment](#).

## Modifier l'attachement de votre VPC

Pour afficher vos attachements de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement VPC, puis choisissez Actions, Modify transit gateway attachment (Modifier le réseau de transit par passerelle).
4. Pour activer la prise en charge DNS, sélectionnez DNS support (Prise en charge DNS).
5. Pour ajouter un sous-réseau à l'attachement, puis au sous-réseau, activez la case à cocher.

L'ajout ou la modification d'un sous-réseau de pièces jointes VPC peut avoir un impact sur le trafic de données lorsque la pièce jointe est en état de modification.

6. Choisissez Modify transit gateway attachment (Modifier le réseau de transit par passerelle).

Pour modifier vos pièces jointes VPC à l'aide du AWS CLI

Utilisez la commande [modify-transit-gateway-vpc-attachment](#).

## Modifier les balises d'attachement de votre VPC

Pour afficher vos balises d'attachement de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement VPC, puis choisissez Actions, Manage tags (Gérer les balises).
4. [Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :
  - Pour Clé, saisissez le nom de la clé.
  - Pour Valeur, saisissez la valeur de la clé.
5. [Supprimer une balise] En regard de la balise, choisissez Remove (Supprimer).
6. Choisissez Enregistrer.

Les balises de pièce jointe VPC peuvent uniquement être modifiées à l'aide de la console.

## Afficher vos attachements de VPC

Pour afficher vos attachements de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Dans la colonne Resource type (Type de ressource), recherchez VPC. Il s'agit des attachements VPC.
4. Choisissez un attachement pour afficher ses détails.

Pour afficher vos pièces jointes VPC à l'aide du AWS CLI

Utilisez la commande [describe-transit-gateway-vpc-attachments](#).

## Supprimer un attachement de VPC

Pour supprimer un attachement de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.

3. Sélectionnez l'attachement de VPC.
4. Choisissez Actions, Delete transit gateway attachment (Supprimer le réseau de transit par passerelle).
5. Lorsque vous y êtes invité, tapez **delete**, puis choisissez Delete (Supprimer).

Pour supprimer une pièce jointe VPC à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway-vpc-attachment](#).

## Résolution des problèmes liés à la création d'attachements VPC

La rubrique suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer lorsque vous créez un attachement VPC.

### Problème

Sélectionnez l'attachement VPC.

### Cause

Ce problème peut être dû à l'une des raisons suivantes :

1. L'utilisateur qui crée l'attachement VPC ne dispose pas des autorisations correctes pour créer un rôle lié au service.
2. Un problème de limitation s'est produit, en raison d'un trop grand nombre de requêtes IAM. Par exemple, vous utilisez AWS CloudFormation pour créer des autorisations et des rôles.
3. Le compte a le rôle lié au service et le rôle lié au service a été modifié.
4. La passerelle de transit n'est pas dans l'état `available`.

### Solution

Selon la cause, essayez de procéder comme suit :

1. Vérifiez que l'utilisateur dispose des autorisations appropriées pour créer des rôles liés au service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM. Une fois que l'utilisateur dispose des autorisations, créez l'attachement VPC.
2. Créez manuellement l'attachement VPC via la console ou l'API. Pour plus d'informations, consultez [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).

3. Vérifiez que le rôle lié au service dispose des autorisations correctes. Pour plus d'informations, consultez [the section called "Passerelle de transit"](#).
4. Vérifiez que la passerelle de transit est dans l'état `available`. Pour plus d'informations, consultez [the section called "Afficher vos passerelles de transit"](#).

## Attachements VPN de passerelle de transit

Pour attacher une connexion VPN à votre passerelle de transit, vous devez indiquer la passerelle client. Pour de plus amples informations sur les exigences de votre passerelle client, consultez [Conditions requises pour votre passerelle client](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN .

Pour les VPN statiques, ajoutez les routes statiques à la table de routage de passerelle de transit.

## Créer un attachement de passerelle de transit avec un VPN

Pour créer un attachement VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).
4. Pour Transit gateway ID (ID de la passerelle de transit), choisissez la passerelle de transit pour l'attachement. Vous pouvez choisir une passerelle de transit que vous possédez.
5. Pour Attachment type (Type d'attachement), choisissez VPN.
6. Pour Customer Gateway (Passerelle client), effectuez l'une des actions suivantes :
  - Pour utiliser une passerelle client existante, choisissez Existante, puis sélectionnez la passerelle à utiliser.

Si votre passerelle client est située derrière un périphérique de traduction d'adresses réseau (NAT) qui est activé pour NAT Traversal (NAT-T), utilisez l'adresse IP publique de votre périphérique NAT et ajustez vos règles de pare-feu pour débloquer le port UDP 4500.

- Pour créer une passerelle client, choisissez Nouveau, puis pour Adresse IP, saisissez une adresse IP publique statique et la version du moteur de cache.

Pour Options de routage, sélectionnez Dynamique ou Statique. Pour de plus amples informations, veuillez consulter [Options de routage VPN site à site](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN .

7. Pour Tunnel Options (Options de tunnel), saisissez les plages CIDR et les clés pré-partagées pour votre tunnel. Pour plus d'informations, veuillez consulter les [Architectures Site-to-Site VPN](#).
8. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).

Pour créer une pièce jointe VPN à l'aide du AWS CLI

Utilisez la commande [create-vpn-connection](#).

## Afficher vos attachements VPN

Pour afficher vos attachements VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Dans la colonne Resource type (Type de ressource), recherchez VPN. Il s'agit des annexes VPN.
4. Choisissez un attachement pour afficher ses détails ou ajouter des balises.

Pour consulter les pièces jointes de votre VPN à l'aide du AWS CLI

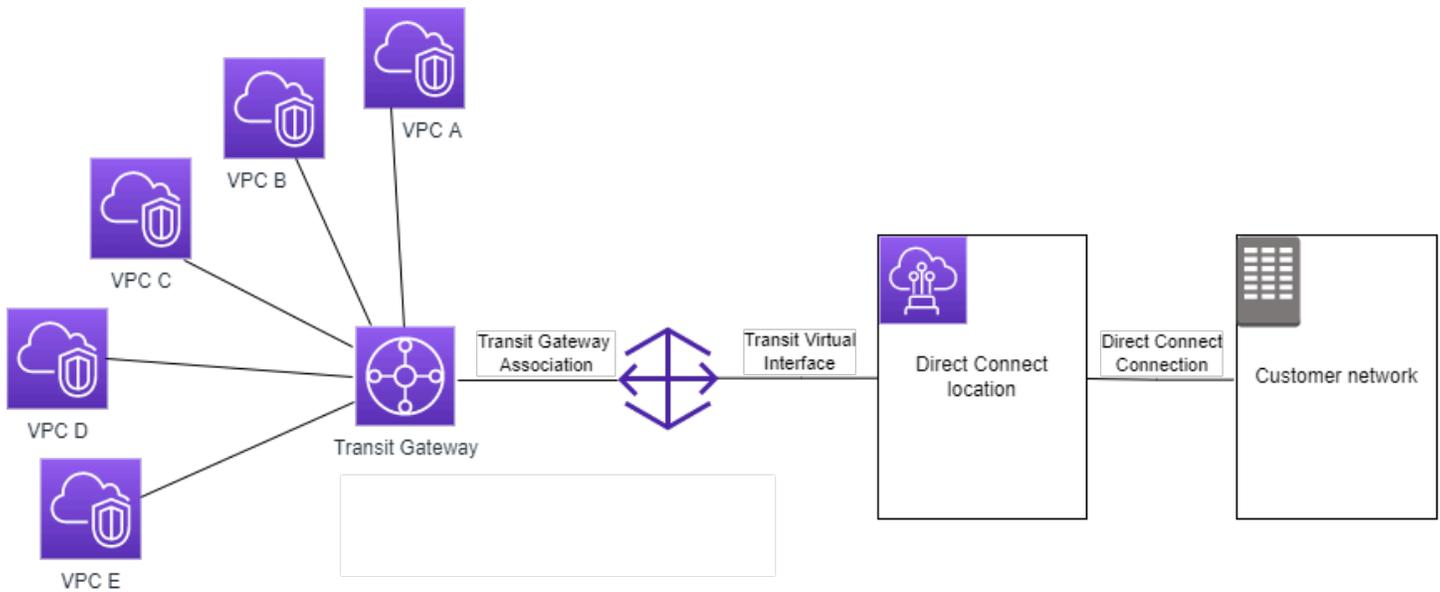
Utilisez la commande [describe-transit-gateway-attachments](#).

## Attachements d'une passerelle de transit à une passerelle Direct Connect

Attachez une passerelle de transit à une passerelle Direct Connect à l'aide d'une interface virtuelle de transit. Cette configuration offre les avantages suivants. Vous pouvez :

- Gérer une connexion unique pour plusieurs VPC ou VPN qui se trouvent dans la même région.
- Publier les préfixes des emplacements sur site sur AWS et les préfixes d'AWS sur les emplacements sur site.

Le schéma suivant illustre la façon dont la passerelle Direct Connect vous permet de créer une connexion unique à votre connexion Direct Connect que tous vos VPC peuvent utiliser.



La solution implique les éléments suivants :

- Une passerelle de transit
- Une passerelle Direct Connect.
- Une association entre la passerelle Direct Connect et la passerelle de transit.
- Une interface de transit virtuelle attachée à la passerelle Direct Connect.

Pour plus d'informations sur la configuration des passerelles Direct Connect avec les passerelles de transit, consultez la section [Associations de passerelles de transit](#) du Guide de l'utilisateur AWS Direct Connect.

## Attachements d'appairage pour la passerelle de transit

Vous pouvez appairer à la fois les passerelles de transit intrarégionales et inter-régionales et acheminer le trafic entre elles, ce qui inclut le trafic IPv4 et IPv6. Pour ce faire, créez un attachement d'appairage sur votre passerelle de transit et spécifiez une passerelle de transit. La passerelle de transit de pair peut se trouver dans votre compte ou dans un autre Compte AWS.

Après que vous avez créé une demande d'attachement d'appairage, le propriétaire de la passerelle de transit appairée (également appelée passerelle de transit acceptante) doit accepter la demande. Pour acheminer le trafic entre les passerelles de transit, vous devez ajouter une route statique à la table de routage de passerelle de transit qui pointe vers l'attachement d'appairage de passerelle de transit.

Nous vous recommandons d'utiliser des ASN uniques pour chaque passerelle de transit appairées afin de tirer parti des futures capacités de propagation de route.

L'appairage de Passerelle de transit ne prend pas en charge la résolution des noms d'hôte DNS IPv4 publics ou privés en adresses IPv4 privées sur les VPC de chaque côté de l'attachement d'appairage de Passerelle de transit à l'aide d'Amazon Route 53 Resolver dans une autre Région. Pour de plus amples informations sur le résolveur Route 53, veuillez consulter [Qu'est-ce qu'Amazon Route 53 Resolver ?](#) (langue française non garantie) dans le Guide du développeur Amazon Route 53.

L'appairage de passerelle de transit interrégional utilise la même infrastructure du réseau que l'appairage de VPC. Par conséquent, le trafic est chiffré à l'aide du chiffrement AES-256 au niveau de la couche réseau virtuel lors de son cheminement entre les régions. Le trafic est également chiffré à l'aide du chiffrement AES-256 sur la couche physique lorsqu'il traverse des liaisons réseau hors du contrôle physique de AWS. Par conséquent, le trafic est double chiffré sur les liaisons réseau en dehors du contrôle physique de AWS. Au sein de la même région, le trafic est chiffré au niveau de la couche physique uniquement lorsqu'il traverse des liaisons réseau hors du contrôle physique de AWS.

Pour plus d'informations sur les régions compatibles avec les attachements d'appairage de passerelles de transit, consultez [AWS FAQ sur Transit Gateways](#).

## Créer un attachement d'appairage

Avant de commencer, assurez-vous que vous avez l'ID de la passerelle de transit que vous souhaitez attacher. Si la passerelle de transit se trouve dans un autre Compte AWS, assurez-vous d'avoir l'ID de Compte AWS du propriétaire de la passerelle de transit.

Après la création de l'attachement d'appairage, le propriétaire de la passerelle de transit acceptante doit valider la demande d'attachement.

Pour créer un attachement d'appairage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).
4. Pour Transit gateway ID (ID de la passerelle de transit), choisissez la passerelle de transit pour l'attachement. Vous pouvez choisir une passerelle de transit que vous possédez ou une qui a été partagée avec vous.

5. Dans Attachment type (Type d'attachement), choisissez Peering Connexion (Connexion d'appairage).
6. Le cas échéant, saisissez une balise de nom pour l'attachement.
7. Pour Account (Compte), sélectionnez l'une des options suivantes :
  - Si la passerelle de transit se trouve dans votre compte, choisissez My account (Mon compte).
  - Si la passerelle de transit se trouve dans un autre Compte AWS, choisissez Autre compte. Dans Account ID (ID de compte), saisissez l'ID de Compte AWS.
8. Pour Région (Région), choisissez la région dans laquelle se trouve la passerelle de transit.
9. Pour Transit gateway (accepter) (Passerelle de transit acceptante), entrez l'ID de la passerelle de transit que vous souhaitez attacher.
10. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).

Pour créer un attachement d'appairage à l'aide de l'AWS CLI

Utilisez la commande [create-transit-gateway-peering-attachment](#).

## Accepter ou rejeter une demande d'attachement d'appairage

Pour activer l'attachement d'appairage, le propriétaire de la passerelle de transit acceptante doit accepter la demande d'attachement d'appairage. Cela est nécessaire même si les deux passerelles de transit sont dans le même compte. L'attachement d'appairage doit être dans l'état `pendingAcceptance`. Acceptez la demande d'attachement d'appairage de la région dans laquelle se trouve la passerelle de transit acceptante.

Vous pouvez rejeter toute demande de connexion d'appairage reçue qui se trouve dans l'état `pendingAcceptance`. Vous devez rejeter la demande de la région dans laquelle se trouve la passerelle de transit acceptante.

Pour accepter une demande d'attachement d'appairage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement d'appairage de passerelle de transit en attente d'acceptation.
4. Choisissez Actions, Accept transit gateway attachment (Accepter le réseau de transit par passerelle).

5. Ajoutez la route statique à la table de routage de passerelle de transit. Pour plus d'informations, consultez [the section called "Créer un itinéraire statique"](#).

Pour refuser une demande d'attachement d'appairage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement d'appairage de passerelle de transit en attente d'acceptation.
4. Choisissez Actions, Reject transit gateway attachment (Rejeter le réseau de transit par passerelle).

Pour accepter ou rejeter un attachement d'appairage à l'aide de l'AWS CLI

Utilisez les commandes [accept-transit-gateway-peering-attachment](#) et [reject-transit-gateway-peering-attachment](#).

## Ajouter un itinéraire à la table de routage de passerelle de transit

Pour acheminer le trafic entre les passerelles de transit appairées, vous devez ajouter un itinéraire statique à la table de routage de la passerelle de transit qui pointe vers l'attachement d'appairage de passerelle de transit. Le propriétaire de la passerelle acceptante doit également ajouter une route statique à la table de routage de sa passerelle de transit.

Pour créer un itinéraire statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage pour laquelle vous créez un itinéraire.
4. Choisissez Actions, Create static route (Créer un acheminement statique).
5. Sur la page Créer un acheminement statique, saisissez le bloc d'adresse CIDR pour lequel l'acheminement doit être créé. Spécifiez par exemple le bloc d'adresse CIDR d'un VPC attaché à la passerelle de transit homologue.
6. Choisissez l'attachement d'appairage pour l'itinéraire.
7. Choisissez Create static route (Créer un acheminement statique).

Pour créer un itinéraire statique à l'aide de l'AWS CLI

Utilisez la commande [create-transit-gateway-route](#).

 Important

Après avoir créé la route, associez la table de routage de passerelle de transit à l'attachement d'appairage de passerelle de transit. Pour plus d'informations, consultez [the section called “Associer une table de routage de passerelle de transit”](#).

## Afficher vos attachements de connexion d'appairage pour la passerelle de transit

Vous pouvez afficher les attachements d'appairage de votre passerelle de transit et les informations les concernant.

Pour afficher vos attachements d'appairage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Dans la colonne Resource type (Type de ressource), recherchez Peering (Appairage). Ce sont les attachements d'appairage.
4. Choisissez un attachement pour afficher ses détails.

Pour afficher les attachements d'appairage pour la passerelle de transit à l'aide de l'AWS CLI

Utilisez la commande [describe-transit-gateway-peering-attachments](#).

## Supprimer un attachement d'appairage

Vous pouvez supprimer un attachement d'appairage de passerelle de transit. Le propriétaire de l'une ou l'autre des passerelles de transit peut supprimer l'attachement.

Pour supprimer un attachement d'appairage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de passerelle de transit.
3. Sélectionnez l'attachement d'appairage de passerelle de transit.

4. Choisissez Actions, Delete transit gateway attachment (Supprimer le réseau de transit par passerelle).
5. Saisissez **delete**, puis choisissez Delete (Supprimer).

Pour supprimer un attachement d'appairage à l'aide de l'AWS CLI

Utilisez la commande [delete-transit-gateway-peering-attachment](#).

## Considérations relatives à la Région AWS d'adhésion

Vous pouvez appairer des passerelles de transit au-delà des frontières de la région d'adhésion. Pour en savoir plus sur ces régions et sur la façon d'y adhérer, consultez [Gestion des régions AWS](#) dans la Référence générale d'Amazon Web Services. Prenez en considération les éléments suivants lorsque vous utilisez l'appairage de passerelle de transit dans ces régions :

- Vous pouvez vous appairer à une région d'adhésion tant que le compte qui accepte l'attachement d'appairage a adhéré à cette région.
- Quel que soit le statut d'adhésion de la région, AWS partage les données de compte suivantes avec le compte qui accepte l'attachement d'appairage :
  - ID Compte AWS
  - ID de passerelle de transit
  - Code région
- Lorsque vous supprimez l'attachement de passerelle de transit, les données de compte ci-dessus sont supprimées.
- Nous vous recommandons de supprimer l'attachement d'appairage de passerelle de transit avant de vous désinscrire de la région. Si vous ne supprimez pas l'attachement d'appairage, le trafic peut continuer à passer par l'attachement et vous continuez à payer des frais. Si vous ne supprimez pas l'attachement, vous pouvez adhérer de nouveau, puis supprimer l'attachement.
- En général, la passerelle de transit a un modèle de paiement par l'expéditeur. En utilisant l'attachement d'appairage de passerelle de transit sur une limite d'adhésion, vous pouvez engendrer des frais dans une région qui accepterait l'attachement, y compris les régions auxquelles vous n'avez pas adhéré. Pour plus d'informations, consultez [Tarification AWS Transit Gateway](#).

# Attachements Transit Gateway Connect et pairs Transit Gateway Connect

Vous pouvez créer un attachement Transit Gateway Connect pour établir une connexion entre une passerelle de transit et des appliances virtuelles tierces (telles que les appliances SD-WAN) exécutées dans un VPC. Une attachement Connect prend en charge le protocole de tunnel GRE (Generic Routing Encapsulation) pour des performances élevées, et le protocole BGP (Border Gateway Protocol) pour le routage dynamique. Après avoir créé un attachement Connect, vous pouvez créer un ou plusieurs tunnels GRE (également appelés pairs Transit Gateway Connect) sur l'attachement Connect pour connecter la passerelle de transit et l'appliance tierce. Établissez deux sessions BGP sur le tunnel GRE pour échanger des informations de routage.

## Important

Un pair de passerelle de transit Connect se compose de deux sessions d'appairage BGP résiliées sur une infrastructure gérée par AWS. Les deux sessions d'appairage BGP fournissent une redondance du plan de routage, garantissant ainsi que la perte d'une session d'appairage BGP n'affecte pas votre opération de routage. Les informations de routage reçues par les deux sessions BGP sont cumulées pour le pair Connect donné. Les deux sessions d'appairage BGP protègent également contre toute opérations d'infrastructure AWS telle que la maintenance de routine, l'application de correctifs, les mises à niveau matérielles et les remplacements. Si votre pair Connect fonctionne sans la session d'appairage BGP double recommandée configurée pour la redondance, il peut subir une perte de connectivité momentanée pendant les opérations d'infrastructure AWS. Nous vous recommandons fortement de configurer les deux sessions d'appairage BGP sur votre pair Connect. Si vous avez configuré plusieurs pairs Connect pour prendre en charge la haute disponibilité côté appliance, nous vous recommandons de configurer les deux sessions d'appairage BGP sur chacun de vos pairs Connect.

Un attachement Connect utilise un VPC ou un attachement Direct Connect existant comme mécanisme de transport sous-jacent. C'est ce qu'on appelle un attachement de transport. La passerelle de transit identifie les paquets GRE correspondants provenant de l'appliance tierce en tant que trafic provenant de l'attachement Connect. Elle traite tous les autres paquets, y compris les paquets GRE avec des informations de source ou de destination incorrectes, comme du trafic provenant de l'attachement de transport.

**Note**

Pour utiliser un attachement Direct Connect comme mécanisme de transport, vous devez d'abord intégrer Direct Connect à AWS Transit Gateway. Pour connaître les étapes à suivre pour créer cette intégration, consultez [Intégrer des appareils SD-WAN à AWS Transit Gateway et AWS Direct Connect](#).

## Table des matières

- [Connecter les pairs](#)
- [Exigences et considérations](#)
- [Création d'un attachement Connect](#)
- [Créer un pair Connect \(tunnel GRE\)](#)
- [Affichage de vos attachements Connect et de vos pairs Connect](#)
- [Modifier votre attachement Connect et vos balises de pair Connect](#)
- [Supprimer un pair Connect](#)
- [Suppression d'un attachement Connect](#)

## Connecter les pairs

Un pair Connect (tunnel GRE) comprend les composants suivants.

### Blocs d'adresse CIDR à l'intérieur (adresses BGP)

Les adresses IP internes utilisées pour l'appairage BGP. Vous devez spécifier un bloc d'adresse CIDR /29 à partir de la plage 169.254.0.0/16 pour IPv4. Vous pouvez éventuellement spécifier un bloc d'adresse CIDR /125 à partir de la plage fd00:::/8 pour IPv6. Les blocs d'adresse CIDR suivants sont réservés et ne peuvent pas être utilisés :

- 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

Vous devez configurer la première adresse de la plage IPv4 de l'appliance en tant qu'adresse IP BGP. Lorsque vous utilisez IPv6, si votre bloc d'adresse CIDR intérieur est fd00::/125, vous devez configurer la première adresse de cette plage (fd00::1) sur l'interface tunnel de l'appliance.

Les adresses BGP doivent être uniques dans tous les tunnels d'une passerelle de transit.

### Adresses IP d'appairage

Adresse IP d'appairage (adresse IP externe GRE) du côté appliance du pair Connect. Il peut s'agir de n'importe quelle adresse IP. L'adresse IP peut être une adresse IPv4 ou IPv6, mais elle doit être de la même famille d'adresses IP que l'adresse de passerelle de transit.

### Adresse de passerelle de transit

Adresse IP d'appairage (adresse IP externe GRE) du côté passerelle de transit du pair Connect. L'adresse IP doit être spécifiée à partir du bloc d'adresse CIDR de la passerelle de transit et doit être unique sur les attachements Connect de la passerelle de transit. Si vous ne spécifiez pas d'adresse IP, nous utilisons la première adresse disponible dans le bloc d'adresse CIDR de la passerelle de transit.

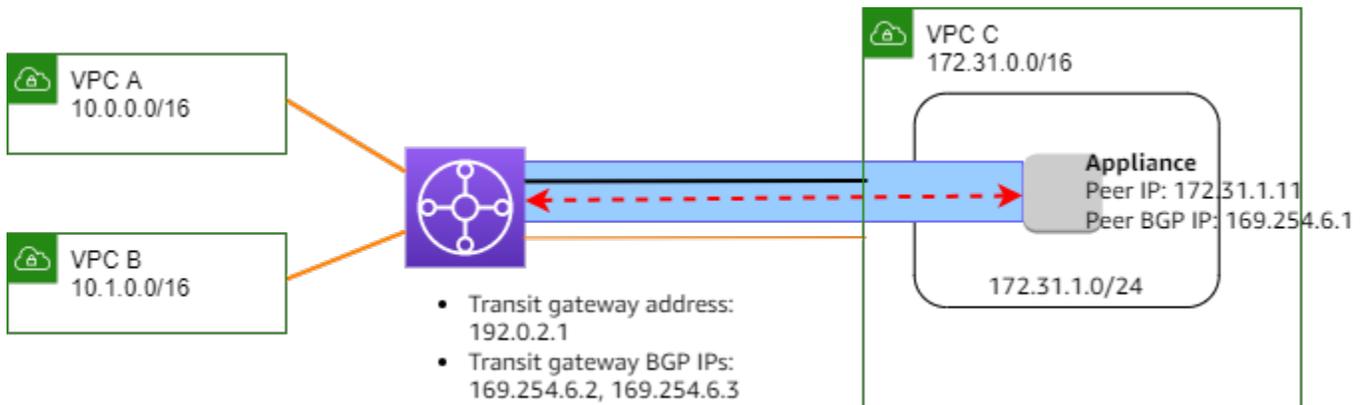
Vous pouvez ajouter un bloc d'adresse CIDR de passerelle de transit lorsque vous [créez](#) ou [modifiez](#) une passerelle de transit.

L'adresse IP peut être une adresse IPv4 ou IPv6, mais elle doit être de la même famille d'adresses IP que l'adresse IP d'appairage.

L'adresse IP d'appairage et l'adresse de passerelle de transit sont utilisées pour identifier de manière unique le tunnel GRE. Vous pouvez réutiliser l'une ou l'autre adresse sur plusieurs tunnels, mais pas les deux dans le même tunnel.

Transit Gateway Connect pour l'appairage BGP prend uniquement en charge le BGP multiprotocole (MP-BGP), où l'adressage IPv4 Unicast est également requis pour établir une session BGP pour IPv6 Unicast. Vous pouvez utiliser des adresses IPv4 et IPv6 pour les adresses IP GRE externes.

L'exemple suivant affiche un attachement Connect entre une passerelle de transit et une appliance dans un VPC.



Composant de schéma	Description
	Attachement VPC
	Connexion d'attachement
	Tunnel GRE (pair Connect)
	Session d'appairage BGP

Dans l'exemple précédent, un attachement Connect est créé sur un attachement VPC existant (l'attachement de transport). Un pair Connect est créé sur l'attachement Connect pour établir une connexion à une appliance dans le VPC. L'adresse de la passerelle de transit est 192.0.2.1, et la plage d'adresses BGP est 169.254.6.0/29. La première adresse IP de la plage (169.254.6.1) est configurée sur l'appliance en tant qu'adresse IP BGP appairée.

La table de routage de sous-réseau pour le VPC C a une route qui dirige le trafic destiné au bloc d'adresse CIDR de la passerelle de transit vers la passerelle de transit.

Destination	Cible
172.31.0.0/16	Locale
192.0.2.0/24	tgw-id

## Exigences et considérations

Voici les exigences et considérations relatives à l'attachement Connect :

- Pour plus d'informations sur les régions qui prennent en charge les attachements Connect, consultez les [FAQ sur AWS Transit Gateways](#).
- L'appliance tierce doit être configurée pour envoyer et recevoir du trafic via un tunnel GRE vers et en provenance de la passerelle de transit à l'aide de l'attachement Connect.
- L'appliance tierce doit être configurée pour utiliser BGP pour les mises à jour de routage dynamiques et les vérifications de l'état.
- Les types de BGP suivants sont pris en charge :
  - BGP extérieur (eBGP) : Utilisé pour la connexion à des routeurs se trouvant dans un système autonome différent de la passerelle de transit. Si vous utilisez eBGP, vous devez configurer `ebgp-multihop` avec une valeur TTL (time-to-live) de 2.
  - BGP intérieur (iBGP) : Utilisé pour la connexion à des routeurs se trouvant dans le même système autonome que la passerelle de transit. La passerelle de transit n'installera pas de routes provenant d'un pair iBGP (appliance tierce), sauf si les routes proviennent d'un pair eBGP et doivent avoir un next hop auto-configuré. Les routes annoncées par une appliance tierce via l'appairage iBGP doivent avoir un ASN.
  - MP-BGP (extensions multiprotocoles pour BGP) : Utilisé pour prendre en charge plusieurs types de protocole, tels que les familles d'adresses IPv4 et IPv6.
- Le délai d'attente des connexions actives BGP par défaut est de 10 secondes et le délai d'attente par défaut est de 30 secondes.
- L'appairage BGP IPv6 n'est pas pris en charge ; seul l'appairage BGP basé sur IPv4 est pris en charge. Les préfixes IPv6 sont échangés via l'appairage BGP IPv4 en utilisant MP-BGP.
- Le protocole BFD (Bidirectional Forwarding Detection) n'est pas pris en charge.
- Le redémarrage en douceur de BGP n'est pas pris en charge.
- Lorsque vous créez un pair de passerelle de transit, si vous ne spécifiez pas de numéro de pair ASN, nous choisissons le numéro ASN de la passerelle de transit. Cela signifie que votre appliance et votre passerelle de transit seront dans le même système autonome utilisant iBGP.
- Un pair Connect utilisant l'attribut BGP AS-PATH est la route préférée lorsque vous avez deux pairs Connect.

Pour utiliser le routage ECMP (equal-cost multi-path) entre plusieurs appliances, vous devez configurer l'appliance pour qu'elle annonce les mêmes préfixes sur la passerelle de transit avec le

même attribut BGP AS-PATH. Pour que la passerelle de transit choisisse tous les chemins ECMP disponibles, les numéros AS-PATH et ASN (Autonomous System Number) doivent correspondre. La passerelle de transit peut utiliser ECMP entre les pairs Connect pour le même attachement Connect ou entre des attachements Connect sur la même passerelle de transit. La passerelle de transit ne peut pas utiliser ECMP entre les appairages BGP redondants qu'un seul pair lui a établi.

- Avec un attachement Connect, les routes sont propagées à une table de routage de passerelle de transit par défaut.
- Les routes statiques ne sont pas prises en charge.
- Assurez-vous que l'unité de transmission maximale (MTU) de l'interface externe de votre appareil tiers (source tunnel)
  - corresponde à la MTU de l'interface du tunnel GRE, ou
  - soit supérieure à celle de l'interface du tunnel GRE.

## Création d'un attachement Connect

Pour créer un attachement Connect, vous devez spécifier un attachement existant en tant qu'attachement de transport. Vous pouvez spécifier un attachement VPC ou Direct Connect comme attachement de transport.

Pour créer un attachement Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit.
3. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de transport de la passerelle de transit).
4. (Facultatif) Pour Name tag (Balise de nom), spécifiez une balise de nom pour l'attachement.
5. Pour Transit gateway ID (ID de la passerelle de transit), choisissez la passerelle de transit pour l'attachement.
6. Pour Attachment type (Type d'attachement), choisissez Connect.
7. Pour Transport attachment ID (ID d'attachement de transport), choisissez l'ID d'un attachement existant (l'attachement de transport).
8. Choisissez Create transit gateway attachment (Créer un réseau de transit par passerelle).

Pour créer un attachement Connect à l'aide de la AWS CLI

Utilisez la commande [create-transit-gateway-connect](#).

## Créer un pair Connect (tunnel GRE)

Vous pouvez créer un pair Connect (tunnel GRE) pour un attachement Connect existant. Avant de commencer, vérifiez que vous avez configuré un bloc d'adresse CIDR de passerelle de transit. Vous pouvez configurer un bloc d'adresse CIDR de passerelle de transit lorsque vous [créez](#) ou [modifiez](#) une passerelle de transit.

Lorsque vous créez le pair Connect, vous devez spécifier l'adresse IP externe GRE côté appliance du pair Connect.

Pour créer un pair Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit.
3. Sélectionnez l'attachement Connect, puis choisissez Actions, Create connect peer (Créer un pair Connect).
4. (Facultatif) Pour Balise de nom, spécifiez une balise de nom pour le pair Connect.
5. (Facultatif) Pour Transit gateway GRE Address (Adresse GRE de passerelle de transit), spécifiez l'adresse IP externe GRE pour la passerelle de transit. Par défaut, la première adresse disponible dans le bloc d'adresse CIDR de la passerelle de transit sera utilisée.
6. Pour Adresse de pair GRE, spécifiez l'adresse IP externe GRE côté appliance du pair Connect.
7. Pour BGP Inside CIDR blocks IPv4 (blocs d'adresse CIDR IPv4 internes BGP), spécifiez la plage d'adresses IPv4 internes utilisées pour l'appariage BGP. Spécifiez un bloc d'adresse CIDR /29 dans la plage 169.254.0.0/16.
8. (Facultatif) Pour BGP Inside CIDR blocks IPv6 (blocs d'adresse CIDR IPv6 internes BGP), spécifiez la plage d'adresses IPv6 internes utilisées pour l'appariage BGP. Spécifiez un bloc d'adresse CIDR /125 dans la plage fd00::/8.
9. (Facultatif) Pour Peer ASN (Pair ASN), spécifiez le numéro d'ASN (Autonomous System Number) BGP (border Gateway Protocol) de l'appliance. Vous pouvez utiliser un ASN existant assigné à votre réseau. Si vous n'en n'avez pas, vous pouvez utiliser un ASN privé dans l'intervalle de 64512–65534 (ASN 16 bits) ou 4200000000–4294967294 (ASN 32 bits).

La valeur par défaut est le même ASN que la passerelle de transit. Si vous configurez le pair ASN pour être différent de l'ASN de passerelle de transit (eBGP), vous devez configurer ebgp-multihop avec une valeur time-to-live (TTL) de 2.

10. Choisissez Create connect peer (Créer un pair Connect).

Pour créer un pair Connect à l'aide de la AWS CLI

Utilisez la commande [create-transit-gateway-connect-peer](#) .

## Affichage de vos attachements Connect et de vos pairs Connect

Vous pouvez afficher vos attachements Connect et vos pairs Connect.

Pour afficher vos attachements Connect et vos pairs Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit.
3. Sélectionnez l'attachement Connect.
4. Pour afficher les pairs Connect pour l'attachement, choisissez l'onglet Connect Peers (Connecter les homologues) .

Pour afficher vos attachements Connect et vos pairs Connect à l'aide de la AWS CLI

Utilisez les commandes [describe-transit-gateway-connects](#) et [describe-transit-gateway-connect-peers](#).

## Modifier votre attachement Connect et vos balises de pair Connect

Vous pouvez modifier les balises de votre attachement Connect.

Pour afficher vos balises d'attachement Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Transit Gateway Attachments (Réseaux de transit par passerelle).
3. Sélectionnez l'attachement Connect, puis choisissez Actions, Manage tags (Gérer les balises).
4. Pour ajouter une balise, choisissez Add new tag (Ajouter une nouvelle balise) et spécifiez le nom et la valeur de la clé.
5. Pour supprimer une identification, choisissez Supprimer.

## 6. Choisissez Save (Enregistrer).

Vous pouvez modifier les balises de votre pair Connect.

Pour modifier vos balises de pairs Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Transit Gateway Attachments (Réseaux de transit par passerelle).
3. Sélectionnez l'attachement Connect, puis choisissez Connect peers (Pairs Connect).
4. Sélectionnez le pair Connect, puis choisissez Actions, Gérer les balises.
5. Pour ajouter une balise, choisissez Add new tag (Ajouter une nouvelle balise) et spécifiez le nom et la valeur de la clé.
6. Pour supprimer une identification, choisissez Supprimer.
7. Choisissez Save (Enregistrer).

Pour modifier votre attachement Connect et vos balises de pairs Connect à l'aide de la AWS CLI

Utilisez les commandes [create-tags](#) et [delete-tags](#).

## Supprimer un pair Connect

Si vous n'avez plus besoin d'un pair Connect, vous pouvez la supprimer.

Pour supprimer un pair Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit.
3. Sélectionnez l'attachement Connect.
4. Dans l'onglet Pairs Connect, sélectionnez le pair Connect et choisissez Actions, Supprimer le pair Connect.

Pour supprimer un pair Connect à l'aide de la AWS CLI

Utilisez la commande [delete-transit-gateway-connect-peer](#).

## Suppression d'un attachement Connect

Si vous n'avez plus besoin d'un attachement Connect, vous pouvez le supprimer. Vous devez d'abord supprimer tous les pairs Connect pour l'attachement.

Pour supprimer un attachement Connect à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit.
3. Sélectionnez l'attachement Connect, puis choisissez Actions, Delete transit gateway attachment (Supprimer le réseau de transit par passerelle).
4. Saisissez **delete**, puis choisissez Delete (Supprimer).

Pour supprimer un attachement Connect à l'aide de la AWS CLI

Utilisez la commande [delete-transit-gateway-connect](#).

## Tables de routage de passerelle de transit

Utilisez les tables de routage de passerelle de transit pour configurer l'acheminement de vos réseaux de transit par passerelle.

### Créer une table de routage de passerelle de transit

Pour créer une table de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Choisissez Create transit gateway route table (Créer une table de routage de passerelle de transit).
4. (Facultatif) Pour Balise Nom, saisissez un nom pour la table de routage de la passerelle de transit. Une balise est alors créée avec la clé de balise « Nom », où la valeur de la balise est le nom spécifié.
5. Pour Transit gateway ID (ID de passerelle de transit), choisissez la passerelle de transit pour la table de routage.
6. Choisissez Create transit gateway route table (Créer une table de routage de passerelle de transit).

Pour créer une table de routage de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-route-table](#).

## Afficher les tables de routage de passerelle de transit

Pour afficher vos tables de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. (Facultatif) Pour trouver une table de routage ou un ensemble de tables spécifique, saisissez une partie ou la totalité du nom, d'un mot clé ou d'un attribut dans le champ de filtre.
4. Activez la case à cocher d'une table de routage ou choisissez son ID pour afficher des informations sur ses associations, ses propagations, ses routes et ses balises.

Pour consulter les tables de routage de votre passerelle de transit à l'aide du AWS CLI

Utilisez la commande [describe-transit-gateway-route-tables](#).

Pour consulter le tableau des itinéraires d'une passerelle de transit à l'aide du AWS CLI

Utilisez la commande [search-transit-gateway-routes](#).

Pour afficher les propagations d'itinéraires d'une table de routage de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [get-transit-gateway-route-table-propagations](#).

Pour afficher les associations associées à une table de routage de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [get-transit-gateway-route-table-associations](#).

## Associer une table de routage de passerelle de transit

Vous pouvez associer une table de routage de passerelle de transit à un attachement de passerelle de transit.

Pour associer une table de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage.
4. Dans la partie inférieure de la page, sélectionnez l'onglet Associations.
5. Sélectionnez Créer une association.
6. Choisissez l'attachement à associer puis sélectionnez Créer une association.

Pour associer une table de routage de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [associate-transit-gateway-route-table](#).

## Supprimer une association pour une table de routage de passerelle de transit

Vous avez la possibilité de dissocier une table de routage de passerelle de transit d'un attachement de passerelle de transit.

Pour dissocier une table de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage.
4. Dans la partie inférieure de la page, sélectionnez l'onglet Associations.
5. Choisissez l'attachement à dissocier puis sélectionnez Supprimer une association.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer une association.

Pour dissocier une table de routage d'une passerelle de transit à l'aide du AWS CLI

Utilisez la commande [disassociate-transit-gateway-route-table](#).

## Propager une route vers une table de routage de passerelle de transit

Utilisez une propagation de route pour ajouter une route depuis un attachement vers une table de routage.

Pour propager une route vers une table de routage d'un attachement de passerelle de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage pour laquelle vous créez une propagation.
4. Sélectionnez Actions, puis Créer une propagation.
5. Sur la page Créer une propagation, choisissez l'attachement.
6. Sélectionnez Créer une propagation.

Pour activer la propagation des itinéraires à l'aide du AWS CLI

Utilisez la commande [enable-transit-gateway-route-table-propagation](#).

## Désactivation de la propagation du routage

Supprimez une route propagée à partir de l'attachement de table de routage.

Pour désactiver la propagation de route avec la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage à partir de laquelle la propagation doit être supprimée.
4. Dans la partie inférieure de la page, sélectionnez l'onglet Propagation.
5. Sélectionnez l'attachement puis choisissez Supprimer une propagation.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer la propagation.

Pour désactiver la propagation des itinéraires à l'aide du AWS CLI

Utilisez la commande [disable-transit-gateway-route-table-propagation](#).

## Créer un itinéraire statique

Vous pouvez créer un itinéraire statique pour un VPC, un VPN ou un attachement d'appairage de passerelle de transit, ou vous pouvez créer un itinéraire Blackhole qui supprime le trafic correspondant à l'itinéraire.

Les routes statiques d'une table de routage de passerelle de transit qui ciblent un attachement VPN ne sont pas filtrées par Site-to-Site VPN. Un flux de trafic sortant non intentionnel risque alors d'être autorisé dans le cas où un VPN basé sur BGP est utilisé.

Pour créer un itinéraire statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage pour laquelle vous créez un itinéraire.
4. Choisissez Actions, Create static route (Créer un acheminement statique).
5. Sur la page Create static route (Créer un acheminement statique), saisissez le bloc d'adresse CIDR pour lequel l'acheminement doit être créé, puis choisissez Active (Actif).
6. Choisissez l'attachement de l'itinéraire.
7. Choisissez Create static route (Créer un acheminement statique).

Pour créer un itinéraire Blackhole à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage pour laquelle vous créez un itinéraire.
4. Choisissez Actions, Create static route (Créer un acheminement statique).
5. Sur la page Create static route (Créer un acheminement statique), saisissez le bloc d'adresse CIDR pour lequel l'acheminement doit être créé, puis choisissez Blackhole.
6. Choisissez Create static route (Créer un acheminement statique).

Pour créer un itinéraire statique ou un itinéraire en trou noir à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-route](#).

## Supprimer un routage statique

Vous pouvez supprimer des routes statiques d'une table de routage de passerelle de transit.

Pour supprimer un itinéraire statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage pour laquelle l'itinéraire doit être supprimé, puis choisissez Routes (Itinéraires).

4. Choisissez l'itinéraire à supprimer.
5. Choisissez Delete static route (Supprimer l'acheminement statique).
6. Dans la boîte de dialogue de confirmation, choisissez Delete static route (Supprimer l'acheminement statique).

Pour supprimer un itinéraire statique à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway-route](#).

## Remplacez une route statique

Vous pouvez remplacer une route statique dans la table de routage d'une passerelle de transit par un itinéraire statique différent.

Pour remplacer une route statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Choisissez la route que vous souhaitez remplacer dans la table de routage.
4. Dans la section des détails, choisissez l'onglet Routes.
5. Choisissez Actions, Remplacer une route statique.
6. Pour le Type, choisissez Active ou Blackhole.
7. Dans la liste déroulante Choisir l'attachement, choisissez la passerelle de transit qui remplacera la passerelle actuelle dans la table de routage.
8. Choisissez Remplacer une route statique.

Pour remplacer un itinéraire statique à l'aide du AWS CLI

Utilisez la commande [replace-transit-gateway-route](#).

## Exportation des tables de routage vers Amazon S3

Vous pouvez exporter les routes dans vos tables de routage de passerelle de transit vers un compartiment Amazon S3. Les routes sont sauvegardées dans le compartiment Amazon S3 spécifié dans un fichier JSON.

Pour exporter des tables de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Choisissez la table de routage comprenant les routes à exporter.
4. Sélectionnez Actions, Exporter des routes.
5. Sur la page Exporter des routes, pour Nom du compartiment S3, saisissez le nom du compartiment S3.
6. Pour filtrer les routes exportées, spécifiez les paramètres de filtrage dans la section Filtres de la page.
7. Sélectionnez Exporter des routes.

Pour accéder aux routes exportées, ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/> et accédez au compartiment que vous avez spécifié. Le nom du fichier inclut l'ID de compte AWS, la région AWS, l'ID de table de routage et un horodatage. Sélectionnez le fichier et choisissez Télécharger. Voici un exemple de fichier JSON qui contient des informations sur deux routes propagées pour les attachements de VPC.

```
{
  "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"
  }
]
```

## Supprimer une table de routage de passerelle de transit

Pour supprimer une table de routage de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage de passerelle de transit.
3. Sélectionnez la table de routage à supprimer.
4. Choisissez Actions, Delete transit gateway route table (Supprimer la table de routage de la passerelle de transit).
5. Saisissez **delete** et choisissez Delete (Supprimer) pour confirmer la suppression.

Pour supprimer une table de routage d'une passerelle de transit à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway-route-table](#).

## Références des listes de préfixes

Vous pouvez référencer une liste de préfixes dans votre table de routage de passerelle de transit. Une liste de préfixes est un ensemble d'une ou plusieurs entrées de bloc d'adresse CIDR que vous définissez et gérez. Vous pouvez utiliser une liste de préfixes pour simplifier la gestion des adresses IP que vous référencez dans vos ressources pour acheminer le trafic réseau. Par exemple, si vous spécifiez fréquemment les mêmes CIDR de destination sur plusieurs tables de routage de passerelle

de transit, vous pouvez gérer ces CIDR dans une seule liste de préfixes, au lieu de référencer à plusieurs reprises les mêmes CIDR dans chaque table de routage. Si vous devez supprimer un bloc d'adresse CIDR de destination, vous pouvez supprimer son entrée de la liste des préfixes au lieu de supprimer la route de chaque table de routage affectée.

Lorsque vous créez une référence de liste de préfixes dans votre table de routage de passerelle de transit, chaque entrée de la liste de préfixes est représentée comme un itinéraire dans votre table de routage de passerelle de transit.

Pour de plus amples informations sur les listes de préfixes, veuillez consulter [Listes de préfixes](#) dans le Guide de l'utilisateur Amazon VPC.

## Créer une référence de liste de préfixes

Vous pouvez créer une référence à une liste de préfixes dans votre table de routage de passerelle de transit.

Pour créer une référence de liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Route Tables (Tables de routage de passerelle de transit).
3. Sélectionnez la table de routage de passerelle de transit.
4. Choisissez Actions, Create prefix list reference (Créer une référence de liste de préfixes).
5. Pour ID de liste de préfixes, choisissez l'ID de la liste de préfixes.
6. Pour Type, choisissez si le trafic vers cette liste de préfixes doit être autorisé (Actif) ou abandonné (Blackhole).
7. Pour Transit gateway attachment ID (ID de réseau de transit par passerelle), choisissez l'ID de l'attachement vers lequel acheminer le trafic.
8. Choisissez Create prefix list reference (Créer une référence de liste de préfixes).

Pour créer une référence de liste de préfixes à l'aide de la AWS CLI

Utilisez la commande [create-transit-gateway-prefix-list-reference](#).

## Afficher les références de la liste des préfixes

Vous pouvez afficher les références de liste de préfixes dans votre table de routage de passerelle de transit. Vous pouvez également afficher chaque entrée de la liste des préfixes sous la forme d'un itinéraire individuel dans votre table de routage de passerelle de transit. Le type d'itinéraire pour une route de liste de préfixes est propagated.

Pour afficher une référence de liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Route Tables (Tables de routage de passerelle de transit).
3. Sélectionnez la table de routage de passerelle de transit.
4. Dans le volet inférieur, choisissez Prefix list references (Références de liste de préfixes). Les références de la liste des préfixes sont répertoriées.
5. Choisissez Itinéraires. Chaque entrée de liste de préfixes est répertoriée en tant qu'itinéraire dans la table de routage.

Pour afficher une référence de liste de préfixes à l'aide de la AWS CLI

Utilisez la commande [get-transit-gateway-prefix-list-references](#).

## Modifier une référence de liste de préfixes

Vous pouvez modifier une référence de liste de préfixes en modifiant la pièce jointe vers laquelle le trafic est acheminé ou en indiquant s'il faut supprimer le trafic correspondant à l'itinéraire.

Vous ne pouvez pas modifier les itinéraires individuels d'une liste de préfixes dans l'onglet Routes. Pour modifier les entrées de la liste de préfixes, utilisez l'écran Managed Prefix Lists (Listes de préfixes gérées). Pour de plus amples d'informations, veuillez consulter [Modification d'une liste de préfixes](#) dans le Guide de l'utilisateur Amazon VPC.

Pour modifier une référence de liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Route Tables (Tables de routage de passerelle de transit).
3. Sélectionnez la table de routage de passerelle de transit.

4. Dans le volet inférieur, choisissez Prefix list references (Références de liste de préfixes).
5. Choisissez la référence de la liste de préfixes et choisissez Modify references (Modifier les références).
6. Pour Type, choisissez si le trafic vers cette liste de préfixes doit être autorisé (Actif) ou abandonné (Blackhole).
7. Pour Transit gateway attachment ID (ID de réseau de transit par passerelle), choisissez l'ID de l'attachement vers lequel acheminer le trafic.
8. Choisissez Modify prefix list reference (Modifier la référence de la liste des préfixes).

Pour modifier une référence de liste de préfixes à l'aide de la AWS CLI

Utilisez la commande [modify-transit-gateway-prefix-list-reference](#).

## Supprimer une référence de liste de préfixes

Si vous n'avez plus besoin d'une référence de liste de préfixes, vous pouvez la supprimer de votre table de routage de passerelle de transit. La suppression de la référence ne supprime pas la liste des préfixes.

Pour supprimer une référence de liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Route Tables (Tables de routage de passerelle de transit).
3. Sélectionnez la table de routage de passerelle de transit.
4. Choisissez la référence de la liste de préfixes et choisissez Delete references (Supprimer les références).
5. Choisissez Delete references (Supprimer la références).

Pour supprimer une référence de liste de préfixes à l'aide de la AWS CLI

Utilisez la commande [delete-transit-gateway-prefix-list-reference](#).

## Tables de stratégie de passerelle de transit

Le routage dynamique de passerelle de transit utilise des tables de stratégie afin d'acheminer le trafic réseau pour AWS Cloud WAN. La table contient des règles de stratégie permettant de faire

correspondre le trafic réseau par attributs de stratégie, puis mappe le trafic correspondant à la règle à une table de routage cible.

Vous pouvez utiliser des tables de stratégie afin de configurer un routage dynamique pour les passerelles de transit et d'échanger automatiquement des informations de routage et d'accessibilité avec des types de passerelles de transit appairés. Contrairement à une route statique, le trafic peut être acheminé sur un chemin différent en fonction des conditions du réseau, telles que les échecs de chemin ou la surcharge. Le routage dynamique ajoute également un niveau de sécurité dans la mesure où il est plus facile de réacheminer le trafic en cas de violation ou d'intrusion du réseau.

### Note

Les tables de politique de passerelle de transit ne sont actuellement prises en charge dans Cloud WAN que lors de la création d'une connexion appairage de passerelle de transit. Lorsque vous créez une connexion d'appairage, vous pouvez associer cette table à la connexion. L'association remplit ensuite automatiquement le tableau avec les règles de politique.

Pour plus d'informations sur les connexions d'appairage dans Cloud WAN, consultez [Peerings \(Appairage\)](#) dans le AWS Guide de l'utilisateur Cloud WAN.

## Créer une table de stratégie de passerelle de transit

Pour créer une table de stratégie de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateway policy table (Table de stratégie de passerelle de transit).
3. Choisissez Create transit gateway route table (Créer une table de stratégie de passerelle de transit).
4. (Facultatif) Pour Name tag (Balise nom), saisissez un nom pour la table de stratégie afin de créer une balise dont la valeur est le nom que vous spécifiez.
5. Pour Transit gateway ID (ID de passerelle de transit), choisissez la passerelle de transit pour la table de stratégie.
6. Choisissez Create transit gateway route table (Créer une table de stratégie de passerelle de transit).

Pour créer une table de politique de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-policy-table](#).

## Supprimer une table de stratégie de passerelle de transit

Supprimez une table de stratégie de passerelle de transit. Lorsqu'une table est supprimée, toutes les règles de stratégie de cette table sont supprimées.

Pour supprimer une table de stratégie de passerelle de transit à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateway policy tables (Tables de stratégie de passerelle de transit).
3. Choisissez la table de stratégie de passerelle de transit à supprimer.
4. Choisissez Actions, puis Delete policy table (Supprimer la table).
5. Confirmez que vous voulez supprimer la table.

Pour supprimer une table de politique de passerelle de transit à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway-policy-table](#).

## Multicast sur les passerelles de transit

Le multicast est un protocole de communication utilisé pour fournir un flux unique de données à plusieurs ordinateurs de réception simultanément. La passerelle de transit prend en charge le routage du trafic multicast entre les sous-réseaux des VPC attachés et sert de routeur multicast aux instances qui envoient le trafic destiné à plusieurs instances de réception.

### Concepts du multicast

Les principaux concepts de la multicast sont les suivants :

- **Domaine multicast** : permet la segmentation d'un réseau multicast en différents domaines et permet à la Passerelle de transit de se comporter comme plusieurs routeurs multicast. Vous définissez l'appartenance à un domaine de multicast au niveau du sous-réseau.
- **Groupe de multicast** : identifie un ensemble d'hôtes qui enverront et recevront le même trafic de multicast. Un groupe de multicast est identifié par une adresse IP de groupe. L'appartenance à

un groupe de multicast est définie par des interfaces réseau Elastic individuelles attachées à des instances EC2.

- Protocole de gestion de groupes Internet (IGMP) : protocole Internet qui permet aux hôtes et aux routeurs de gérer de façon dynamique l'appartenance à un groupe de multicast. Un domaine de multidiffusion IGMP contient des hôtes qui utilisent le protocole IGMP pour rejoindre, quitter et envoyer des messages. AWS prend en charge le protocole IGMPv2 et les domaines de multidiffusion IGMP et statiques (basés sur des API) à des groupes.
- Source multicast : une interface réseau Elastic associée à une instance EC2 prise en charge statiquement configurée pour envoyer du trafic multicast. Une source multicast s'applique uniquement aux configurations de source statique.

Un domaine multicast à source statique contient des hôtes qui n'utilisent pas le protocole IGMP pour rejoindre, quitter et envoyer des messages. Vous pouvez utiliser le AWS CLI pour ajouter une source et des membres du groupe. La source ajoutée statiquement envoie du trafic multicast et les membres reçoivent du trafic multicast.

- Membre du groupe multicast : Il s'agit d'une interface réseau Elastic associée à une instance EC2 compatible qui reçoit du trafic multicast. Un groupe multicast comporte plusieurs membres de groupe. Dans une configuration d'appartenance à un groupe à source statique, les membres du groupe multicast peuvent uniquement recevoir du trafic. Dans une configuration de groupe IGMP, les membres peuvent à la fois envoyer et recevoir du trafic.

## Considérations

- Pour plus d'informations sur les régions prises en charge, consultez [FAQ sur AWS Transit Gateway](#).
- Vous devez créer une nouvelle passerelle de transit pour prendre en charge le multicast.
- L'appartenance à un groupe de multidiffusion est gérée à l'aide du Amazon Virtual Private Cloud Console ou du AWS CLI IGMP.
- Un sous-réseau ne peut se trouver que dans un seul domaine multicast.
- Si vous utilisez une instance autre qu'une instance Nitro, vous devez désactiver la vérification de la Source/Dest (Source/Destination). Pour plus d'informations sur la désactivation de la vérification, consultez la section [Modification de la source ou de la destination](#) dans le guide de l'utilisateur Amazon EC2.
- Une instance autre qu'une instance Nitro ne peut pas être un expéditeur multicast.

- Le routage multicast n'est pas pris en charge sur le VPN de site à site AWS Direct Connect, les pièces jointes de peering ou les pièces jointes Connect de la passerelle de transit.
- Une Passerelle de transit n'est pas compatible avec la fragmentation des paquets multicast. Les paquets multicast fragmentés sont abandonnés. Pour plus d'informations, consultez [Unité de transmission maximale \(MTU\)](#).
- Au démarrage, un hôte IGMP envoie plusieurs messages IGMP JOIN pour rejoindre un groupe multicast (généralement 2 à 3 tentatives). Dans le cas peu probable où tous les messages IGMP JOIN se perdent, l'hôte ne fera pas partie du groupe multicast de la Passerelle de transit. Dans un tel scénario, vous devrez re-déclencher le message IGMP JOIN de l'hôte en utilisant des méthodes spécifiques à l'application.
- L'adhésion à un groupe commence à la réception du message IGMPv2 JOIN par la passerelle de transit et se termine à la réception du message IGMPv2 LEAVE. La passerelle de transit assure le suivi des hôtes qui ont réussi à rejoindre le groupe. En tant que routeur multicast dans le cloud, la Passerelle de transit émet un message IGMPv2 QUERY à tous les membres toutes les deux minutes. Chaque membre envoie un message IGMPv2 JOIN en réponse, c'est ainsi que les membres renouvellent leur adhésion. Si un membre ne répond pas à trois requêtes consécutives, la passerelle de transit supprime cette adhésion de tous les groupes joints. Cependant, il continue à envoyer des requêtes à ce membre pendant 12 heures avant de le supprimer définitivement de sa to-be-queried liste. Un message IGMPv2 LEAVE explicite supprime immédiatement et définitivement l'hôte de tout traitement multicast ultérieur.
- La passerelle de transit assure le suivi des hôtes qui ont réussi à rejoindre le groupe. En cas de panne de la passerelle de transit, celle-ci continue à envoyer des données multicast à l'hôte pendant sept minutes (420 secondes) après le dernier message IGMP JOIN réussi. La passerelle de transit continue d'envoyer des demandes d'adhésion à l'hôte pendant une période pouvant aller jusqu'à 12 heures ou jusqu'à ce qu'elle reçoive un message IGMP LEAVE de l'hôte.
- La Passerelle de transit envoie des paquets de demande d'adhésion à tous les membres IGMP afin de pouvoir suivre l'appartenance à un groupe multicast. L'adresse IP source de ces paquets de demande IGMP est 0.0.0.0/32, et l'adresse IP de destination est 224.0.0.1/32 et le protocole est 2. Votre configuration de groupe de sécurité sur les hôtes IGMP (instances) et toute configuration ACL sur les sous-réseaux hôtes doivent autoriser ces messages de protocole IGMP.
- Lorsque la source et la destination multicast sont dans le même VPC, vous ne pouvez pas utiliser le référencement de groupe de sécurité pour définir le groupe de sécurité de destination afin d'accepter le trafic provenant du groupe de sécurité de la source.
- Pour les groupes et les sources multicast statiques, les Passerelles de transit Amazon VPC suppriment automatiquement les groupes et les sources statiques pour les ENI qui n'existent plus.

Pour cela, le [rôle lié au service de Passerelle de transit](#) est régulièrement assumé afin de décrire les ENI du compte.

- Seule la multidiffusion statique prend en charge le protocole IPv6. La multidiffusion dynamique ne fonctionne pas.

## Multicast avec Windows Server

Vous devrez effectuer des actions supplémentaires lors de la configuration du multicast pour qu'il fonctionne avec des passerelles de transit sous Windows Server 2019 ou 2022. À l'aide de PowerShell, exécutez les commandes suivantes :

1. Effectuez les modifications nécessaires pour que Windows Server utilise IGMPv2 au lieu d'IGMPv3 pour la pile TCP/IP :

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

### Note

`New-ItemProperty` est un index de propriété qui indique la version de l'IGMP. Comme IGMP v2 est la version prise en charge pour la multidiffusion, la propriété `Value` doit être 3. Au lieu de modifier le registre Windows, vous pouvez exécuter la commande suivante pour définir la version IGMP sur 2. :

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

2. Le pare-feu Windows supprime la plupart du trafic UDP par défaut. Vous devez d'abord vérifier quel profil de connexion est utilisé pour le multicast :

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

```
NetworkCategory
```

```
-----
```

```
Public
```

3. Mettez à jour le profil de connexion de l'étape précédente pour autoriser l'accès au(x) port(s) UDP requis :

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

4. Redémarrez l'instance EC2.
5. Testez votre application multicast pour vous assurer que le trafic circule normalement.

## Routage multicast

Lorsque vous activez le multicast sur une passerelle de transit, celle-ci agit comme un routeur multicast. Lorsque vous ajoutez un sous-réseau à un domaine multicast, nous envoyons tout le trafic multicast à la passerelle de transit qui est associée à ce domaine multicast.

### Listes ACL réseau

Les règles ACL réseau fonctionnent au niveau du sous-réseau. Elles s'appliquent au trafic multicast, car les passerelles de transit résident à l'extérieur du sous-réseau. Pour plus d'informations, consultez [ACL réseau](#) dans le Guide de l'utilisateur Amazon VPC.

Pour le trafic multicast IGMP (Internet Group Management Protocol), les règles entrantes minimales sont énoncées ci-dessous. L'hôte distant est l'hôte qui envoie le trafic multicast.

Type	Protocole	Source	Description
Protocole personnalisé	IGMP (2)	0.0.0.0/32	Requête IGMP
Protocole UDP personnalisé	UDP	Adresse IP de l'hôte distant	Trafic multicast entrant

Les règles sortantes minimales pour IGMP sont énoncées ci-dessous.

Type	Protocole	Destination	Description
Protocole personnalisé	IGMP (2)	224.0.0.2/32	Quitter IGMP
Protocole personnalisé	IGMP (2)	Adresse IP du groupe multicast	Rejoindre IGMP
Protocole UDP personnalisé	UDP	Adresse IP du groupe multicast	Trafic multicast sortant

## Groupes de sécurité

Les règles de groupe de sécurité fonctionnent au niveau de l'instance. Elles peuvent être appliquées à la fois au trafic multicast entrant et sortant. La façon d'opérer est la même avec le trafic unicast. Pour toutes les instances membres du groupe, vous devez autoriser le trafic entrant à partir de la source du groupe. Pour de plus amples informations, veuillez consulter [Groupes de sécurité](#) dans le Guide de l'utilisateur Amazon VPC (français non garanti).

Pour le trafic multicast IGMP, vous devez disposer au minimum des règles entrantes suivantes. L'hôte distant est l'hôte qui envoie le trafic multicast. Vous ne pouvez pas spécifier un groupe de sécurité comme source de la règle UDP entrante.

Type	Protocole	Source	Description
Protocole personnalisé	2	0.0.0.0/32	Requête IGMP
Protocole UDP personnalisé	UDP	Adresse IP de l'hôte distant	Trafic multicast entrant

Pour le trafic multicast IGMP, vous devez disposer au minimum des règles sortantes suivantes.

Type	Protocole	Destination	Description
Protocole personnalisé	2	224.0.0.2/32	Quitter IGMP
Protocole personnalisé	2	Adresse IP du groupe multicast	Rejoindre IGMP
Protocole UDP personnalisé	UDP	Adresse IP du groupe multicast	Trafic multicast sortant

## Utilisation du multicast

Vous pouvez configurer le multicast sur les passerelles de transit à l'aide de la console Amazon VPC ou de la AWS CLI.

Avant de créer un domaine multicast, vous devez savoir si vos hôtes utilisent le protocole de gestion de groupes Internet (IGMP) pour le trafic multicast.

## Table des matières

- [Attributs de domaine multicast](#)
- [Gestion des configurations IGMP](#)
- [Gestion des configurations des sources statiques](#)
- [Gestion des configurations des membres de groupe statique](#)
- [Gestion des domaines multicast](#)
- [Gestion des groupes multicast](#)
- [Utilisation de domaines multicast partagés](#)

## Attributs de domaine multicast

Le tableau suivant détaille les attributs de domaine multicast. Vous ne pouvez pas activer les deux attributs en même temps.

Attribut	Description
Igmpv2Support (AWS CLI)	Cet attribut détermine la façon dont les membres du groupe rejoignent ou quittent un groupe multicast.
Prise en charge de IGMPv2 (console)	<p>Lorsque cet attribut est désactivé, vous devez ajouter les membres du groupe au domaine manuellement.</p> <p>Activez cet attribut si au moins un membre utilise le protocole IGMP. Les membres rejoignent le groupe multicast de l'une des manières suivantes :</p> <ul style="list-style-type: none"> <li>• Les membres qui prennent en charge IGMP utilisent les messages JOIN et LEAVE.</li> <li>• Les membres qui ne prennent pas en charge IGMP doivent être ajoutés ou supprimés du groupe à l'aide de la console Amazon VPC ou de la AWS CLI.</li> </ul> <p>Si vous enregistrez des membres de groupes multicast, vous devez également les désenregistrer. La passerelle de transit</p>

Attribut	Description
	ignore un message IGMP LEAVE envoyé par un membre du groupe ajouté manuellement.
<p data-bbox="110 338 500 422">StaticSourcesSupport (AWS CLI)</p> <p data-bbox="110 464 521 548">Prise en charge des sources statiques (console)</p>	<p data-bbox="587 338 1490 422">Cet attribut détermine s'il existe des sources multicast statiques pour le groupe.</p> <p data-bbox="587 464 1479 642">Lorsque cet attribut est activé, vous devez ajouter des sources pour un domaine de multidiffusion à l'aide de <a href="#">register-transit-gateway-multicast-group-sources</a>. Seules les sources multicast peuvent envoyer du trafic multicast.</p> <p data-bbox="587 684 1500 915">Lorsque cet attribut est désactivé, aucune source multicast n'est désignée. Toutes les instances qui se trouvent dans les sous-réseaux associés au domaine multicast peuvent envoyer du trafic multicast, et les membres du groupe reçoivent le trafic multicast.</p>

## Gestion des configurations IGMP

Lorsque vous avez au moins un hôte qui utilise le protocole IGMP pour le trafic multicast, AWS crée automatiquement le groupe multicast lorsqu'il reçoit un message IGMP JOIN d'une instance, puis ajoute cette dernière en tant que membre de ce groupe. Vous pouvez également ajouter de manière statique des hôtes non IGMP en tant que membres à un groupe à l'aide du. AWS CLI Toutes les instances qui se trouvent dans des sous-réseaux associés au domaine multicast peuvent envoyer du trafic et les membres du groupe reçoivent le trafic multicast.

Effectuez les étapes suivantes pour terminer cette configuration.

1. Créez un VPC. Pour en savoir plus sur la création de VPC, veuillez consulter la [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
2. Créez un sous-réseau dans le VPC. Pour en savoir plus sur la création de sous-réseaux, veuillez consulter la [Création d'un sous-réseau dans votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
3. Créez une passerelle de transit configurée pour le trafic multicast. Pour de plus amples informations, veuillez consulter [the section called "Créer une passerelle de transit"](#).

4. Créez un attachement VPC. Pour de plus amples informations, veuillez consulter [the section called “Créer un attachement de passerelle de transit vers un VPC”](#).
5. Créez un domaine multicast configuré pour prendre en charge IGMP. Pour de plus amples informations, veuillez consulter [the section called “Création d'un domaine multicast IGMP”](#).

Utilisez les paramètres suivants :

- Activer Prise en charge de IGMPv2.
  - Désactiver Prise en charge des sources statistiques.
6. Créez une association entre les sous-réseaux dans l'attachement VPC de passerelle de transit et le domaine multicast. Pour de plus amples informations, veuillez consulter [the section called “Associer des attachements et des sous-réseaux VPC à un domaine multicast”](#).
  7. La version IGMP par défaut pour EC2 est IGMPv3. Vous devez modifier la version de tous les membres du groupe IGMP. Vous pouvez exécuter la commande suivante :

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

8. Ajoutez les membres qui n'utilisent pas le protocole IGMP au groupe multicast. Pour de plus amples informations, veuillez consulter [the section called “Enregistrer des membres auprès d'un groupe multicast”](#).

## Gestion des configurations des sources statiques

Dans cette configuration, vous devez ajouter de façon statique des membres multicast à un groupe. Les hôtes n'utilisent pas le protocole IGMP pour rejoindre ou quitter des groupes multicast. Vous devez ajouter de façon statique les membres du groupe qui reçoivent le trafic multicast.

Effectuez les étapes suivantes pour terminer cette configuration.

1. Créez un VPC. Pour en savoir plus sur la création de VPC, veuillez consulter la [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.
2. Créez un sous-réseau dans le VPC. Pour en savoir plus sur la création de sous-réseaux, veuillez consulter la [Création d'un sous-réseau dans votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
3. Créez une passerelle de transit configurée pour le trafic multicast. Pour de plus amples informations, veuillez consulter [the section called “Créer une passerelle de transit”](#).

4. Créez un attachement VPC. Pour de plus amples informations, veuillez consulter [the section called “Créer un attachement de passerelle de transit vers un VPC”](#).
5. Créez un domaine multicast configuré sans prise en charge IGMP et pour prendre en charge l'ajout statique de sources. Pour de plus amples informations, veuillez consulter [the section called “Création d'un domaine multicast source statique”](#).

Utilisez les paramètres suivants :

- Désactiver Prise en charge de IGMPv2.
- Pour ajouter manuellement des sources, activez la prise en charge des sources statiques.

Les sources sont les seules ressources qui peuvent envoyer du trafic multicast lorsque l'attribut est activé. Dans le cas contraire, toutes les instances qui se trouvent dans les sous-réseaux associés au domaine multicast peuvent envoyer du trafic multicast et les membres du groupe reçoivent le trafic multicast.

6. Créez une association entre les sous-réseaux dans l'attachement VPC de passerelle de transit et le domaine multicast. Pour plus d'informations, consultez [the section called “Associer des attachements et des sous-réseaux VPC à un domaine multicast”](#).
7. Si vous activez Prise en charge des sources statiques, ajoutez la source au groupe multicast. Pour de plus amples informations, veuillez consulter [the section called “Enregistrement des sources auprès d'un groupe multicast”](#).
8. Ajoutez les membres au groupe multicast. Pour de plus amples informations, veuillez consulter [the section called “Enregistrer des membres auprès d'un groupe multicast”](#).

## Gestion des configurations des membres de groupe statique

Dans cette configuration, vous devez ajouter de façon statique des membres multicast à un groupe. Les hôtes ne peuvent pas utiliser le protocole IGMP pour rejoindre ou quitter des groupes multicast. Toutes les instances qui se trouvent dans des sous-réseaux associés au domaine multicast peuvent envoyer du trafic multicast et les membres du groupe reçoivent le trafic multicast.

Effectuez les étapes suivantes pour terminer cette configuration.

1. Créez un VPC. Pour en savoir plus sur la création de VPC, veuillez consulter la [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.

2. Créez un sous-réseau dans le VPC. Pour en savoir plus sur la création de sous-réseaux, veuillez consulter la [Création d'un sous-réseau dans votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
3. Créez une passerelle de transit configurée pour le trafic multicast. Pour de plus amples informations, veuillez consulter [the section called "Créer une passerelle de transit"](#).
4. Créez un attachement VPC. Pour de plus amples informations, veuillez consulter [the section called "Créer un attachement de passerelle de transit vers un VPC"](#).
5. Créez un domaine multicast configuré sans prise en charge IGMP et pour prendre en charge l'ajout statique de sources. Pour de plus amples informations, veuillez consulter [the section called "Création d'un domaine multicast source statique"](#).

Utilisez les paramètres suivants :

- Désactiver Prise en charge de IGMPv2.
  - Désactiver Prise en charge des sources statistiques.
6. Créez une association entre les sous-réseaux dans l'attachement VPC de passerelle de transit et le domaine multicast. Pour de plus amples informations, veuillez consulter [the section called "Associer des attachements et des sous-réseaux VPC à un domaine multicast"](#).
  7. Ajoutez les membres au groupe multicast. Pour de plus amples informations, veuillez consulter [the section called "Enregistrer des membres auprès d'un groupe multicast"](#).

## Gestion des domaines multicast

Pour commencer à utiliser le multicast avec une passerelle de transit, créez un domaine multicast, puis associez des sous-réseaux au domaine.

### Table des matières

- [Création d'un domaine multicast IGMP](#)
- [Création d'un domaine multicast source statique](#)
- [Associer des attachements et des sous-réseaux VPC à un domaine multicast](#)
- [Affichage de vos associations de domaines multicast](#)
- [Dissociation de sous-réseaux d'un domaine multicast](#)
- [Ajout de balises à un domaine multicast](#)
- [Suppression d'un domaine multicast](#)

## Création d'un domaine multicast IGMP

Si vous ne l'avez pas encore fait, vérifiez les attributs de domaine multicast disponibles. Pour de plus amples informations, veuillez consulter [the section called "Utilisation du multicast"](#).

### Console

Pour créer un domaine multicast IGMP à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Choisissez Create transit gateway multicast domain (Créer un domaine multicast pour la passerelle de transit).
4. Pour Name tag (Balise de nom), saisissez un nom pour le domaine.
5. Pour Transit gateway ID (ID de passerelle de transit), choisissez la passerelle de transit qui traite le trafic multicast.
6. Pour IGMPv2 support (prise en charge IGMPv2), activez la case à cocher.
7. Pour Static sources support (prise en charge des sources statiques), désactivez la case à cocher.
8. Pour accepter automatiquement les associations de sous-réseaux inter-comptes pour ce domaine multicast, sélectionnez Auto accept shared associations (Accepter automatiquement les associations partagées).
9. Choisissez Create transit gateway multicast domain (Créer un domaine multicast pour la passerelle de transit).

### Command line

Pour créer un domaine de multidiffusion IGMP à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-multicast-domain](#).

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

## Création d'un domaine multicast source statique

Si vous ne l'avez pas encore fait, vérifiez les attributs de domaine multicast disponibles. Pour de plus amples informations, veuillez consulter [the section called “Utilisation du multicast”](#).

### Console

Pour créer un domaine multicast statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Choisissez Create transit gateway multicast domain (Créer un domaine multicast pour la passerelle de transit).
4. Pour le Name tag (Nom de la balise), saisissez un nom pour identifier le domaine.
5. Pour Transit gateway ID (ID de passerelle de transit), choisissez la passerelle de transit qui traite le trafic multicast.
6. Pour IGMPv2 support (prise en charge IGMPv2), désactivez la case à cocher.
7. Pour Reject transit gateway attachment (Prise en charge des sources statiques), activez la case à cocher.
8. Pour accepter automatiquement les associations de sous-réseaux inter-comptes pour ce domaine multicast, sélectionnez Auto accept shared associations (Accepter automatiquement les associations partagées).
9. Choisissez Create transit gateway multicast domain (Créer un domaine multicast pour la passerelle de transit).

### Command line

Pour créer un domaine de multidiffusion statique à l'aide du AWS CLI

Utilisez la commande [create-transit-gateway-multicast-domain](#).

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

## Associer des attachements et des sous-réseaux VPC à un domaine multicast

Utilisez la procédure suivante pour associer un attachement de VPC à un domaine multicast. Lorsque vous créez une association, vous pouvez sélectionner les sous-réseaux à inclure dans le domaine multicast.

Avant de commencer, vous devez créer un attachement de VPC sur votre passerelle de transit. Pour de plus amples informations, veuillez consulter [Attachements de passerelle de transit vers un VPC](#).

### Console

Pour associer des attachements de VPC à un domaine multicast à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast, puis choisissez Actions, Create association (Créer une association).
4. Pour Choose attachment to associate (Choisir l'attachement à associer), sélectionnez réseau de transit par passerelle.
5. Dans Choose subnets to associate (Choisir les sous-réseaux à associer), sélectionnez les sous-réseaux à inclure dans le domaine multicast.
6. Sélectionnez Créer une association.

### Command line

Pour associer des pièces jointes VPC à un domaine de multidiffusion à l'aide du AWS CLI

Utilisez la commande [associate-transit-gateway-multicast-domain](#).

### Affichage de vos associations de domaines multicast

Vous pouvez afficher vos domaines multicast afin de vérifier qu'ils sont disponibles et qu'ils contiennent les sous-réseaux et les attachements appropriés.

## Console

Pour afficher un domaine multicast à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Cliquez sur l'onglet Associations .

## Command line

Pour afficher un domaine de multidiffusion à l'aide du AWS CLI

Utilisez la commande [describe-transit-gateway-multicast-domains](#).

## Dissociation de sous-réseaux d'un domaine multicast

Procédez comme suit pour dissocier les sous-réseaux d'un domaine multicast.

## Console

Pour dissocier les sous-réseaux à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Cliquez sur l'onglet Associations .
5. Sélectionnez le sous-réseau, puis choisissez Actions, Delete association (Supprimer l'association).

## Command line

Pour dissocier les sous-réseaux à l'aide du AWS CLI

Utilisez la commande [disassociate-transit-gateway-multicast-domain](#).

## Ajout de balises à un domaine multicast

Ajoutez des balises à vos ressources pour les organiser et les identifier, par exemple selon leur but, leur propriétaire ou leur environnement. Vous pouvez ajouter plusieurs balises à chaque domaine multicast. Les clés de balise doivent être uniques pour chaque domaine multicast. Si vous ajoutez une balise avec une clé qui est déjà associée au domaine multicast, la valeur de cette balise est mise à jour. Pour de plus amples informations, veuillez consulter [Balisage de vos ressources Amazon EC2](#).

### Console

Pour ajouter des balises à un domaine multicast à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Choisissez Actions, Manage tags (Gérer les balises).
5. Pour chaque balise, choisissez Add new tag (Ajouter une nouvelle balise) et saisissez une Clé et une Valeur pour la balise.
6. Choisissez Enregistrer.

### Command line

Pour ajouter des balises à un domaine de multidiffusion à l'aide du AWS CLI

Utilisez la commande [create-tags](#).

## Suppression d'un domaine multicast

Utilisez la procédure suivante pour supprimer un domaine multicast.

### Console

Pour supprimer un domaine multicast à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast, puis choisissez Actions, Delete multicast domain (Supprimer le domaine multicast).
4. Lorsque vous êtes invité à confirmer, entrez **delete**, puis choisissez Delete (Supprimer).

## Command line

Pour supprimer un domaine de multidiffusion à l'aide du AWS CLI

Utilisez la commande [delete-transit-gateway-multicast-domain](#).

## Gestion des groupes multicast

### Table des matières

- [Enregistrement des sources auprès d'un groupe multicast](#)
- [Enregistrer des membres auprès d'un groupe multicast](#)
- [Désenregistrement des sources d'un groupe multicast](#)
- [Désenregistrement des membres d'un groupe multicast](#)
- [Afficher vos groupes multicast](#)

### Enregistrement des sources auprès d'un groupe multicast

#### Note

Cette procédure n'est requise que lorsque vous avez défini l'attribut de Prise en charge des sources statiques sur activer.

Utilisez la procédure suivante pour enregistrer des sources avec un groupe multicast. La source est l'interface réseau qui envoie le trafic multicast.

Vous avez besoin des informations suivantes avant d'ajouter une source :

- L'ID du domaine multicast
- Les ID des interfaces réseau des sources

- Adresse IP du groupe multicast

## Console

Pour enregistrer les sources à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast, puis choisissez Actions, Add group sources (Ajouter des sources de groupe).
4. Pour Group IP address (Adresse IP du groupe), saisissez le bloc d'adresse CIDR IPv4 ou le bloc d'adresse CIDR IPv6 à affecter au domaine multicast.
5. Sous Choose network interfaces (Choisir des interfaces réseau), sélectionnez les interfaces réseau des utilisateurs multicast.
6. Choisissez Add sources (Ajouter des sources).

## Command line

Pour enregistrer des sources à l'aide du AWS CLI

Utilisez la commande [register-transit-gateway-multicast-group-sources](#).

## Enregistrer des membres auprès d'un groupe multicast

Utilisez la procédure suivante pour enregistrer les membres du groupe auprès d'un groupe multicast.

Vous avez besoin des informations suivantes avant d'ajouter des membres :

- L'ID du domaine multicast
- Les ID des interfaces réseau des membres du groupe
- Adresse IP du groupe multicast

## Console

Pour inscrire les membres à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast, puis choisissez Actions, Add group members (Ajouter des membres de groupe).
4. Pour Group IP address (Adresse IP du groupe), saisissez le bloc d'adresse CIDR IPv4 ou le bloc d'adresse CIDR IPv6 à affecter au domaine multicast.
5. Sous Choose network interfaces (Choisir des interfaces réseau), sélectionnez les interfaces réseau des récepteurs multicast.
6. Choisissez Add members (Ajouter des membres).

## Command line

Pour enregistrer des membres à l'aide du AWS CLI

Utilisez la commande [register-transit-gateway-multicast-group-members](#).

## Désenregistrement des sources d'un groupe multicast

Vous n'avez pas besoin de suivre cette procédure sauf si vous avez ajouté manuellement une source au groupe multicast.

## Console

Pour supprimer une source à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Cliquez sur l'onglet Groups (Groupes).
5. Sélectionnez les sources, puis choisissez Remove source (Supprimer la source).

## Command line

Pour supprimer une source à l'aide du AWS CLI

Utilisez la commande [deregister-transit-gateway-multicast-group-sources](#).

## Désenregistrement des membres d'un groupe multicast

Vous n'avez pas besoin de suivre cette procédure sauf si vous avez ajouté manuellement un membre au groupe multicast.

## Console

Pour annuler l'inscription de membres à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Cliquez sur l'onglet Groups (Groupes).
5. Sélectionnez les membres, puis choisissez Remove member (Supprimer le membre).

## Command line

Pour désenregistrer des membres à l'aide du AWS CLI

Utilisez la commande [deregister-transit-gateway-multicast-group-members](#).

## Afficher vos groupes multicast

Vous pouvez afficher des informations sur vos groupes multicast pour vérifier que les membres ont été découverts à l'aide du protocole IGMPv2. Le type de membre (dans la console) ou MemberType (dans le AWS CLI) affiche IGMP lorsque des membres du protocole sont AWS découverts.

## Console

Pour afficher les groupes multicast à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le panneau de navigation, choisissez Transit Gateway Multicast (Multicast pour la passerelle de transit).
3. Sélectionnez le domaine multicast.
4. Cliquez sur l'onglet Groups (Groupes).

## Command line

Pour afficher les groupes de multidiffusion à l'aide du AWS CLI

Utilisez la commande [search-transit-gateway-multicast-groups](#).

L'hôte distant est l'hôte qui envoie le trafic multicast.

```
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"
    }
  ]
}
```

## Utilisation de domaines multicast partagés

Avec le partage de domaines multicast, les propriétaires de domaines multicast peuvent partager le domaine avec d'autres comptes AWS au sein de leur organisation ou entre organisations dans AWS Organizations. En tant que propriétaire du domaine multicast, vous pouvez créer et gérer le domaine multicast de manière centralisée. Les consommateurs peuvent effectuer les opérations suivantes sur un domaine multicast partagé :

- Enregistrer et désenregistrer les membres du groupe ou des sources de groupe dans le domaine multicast

- Associer un sous-réseau au domaine multicast et dissocier les sous-réseaux du domaine multicast

Un propriétaire de domaine multicast peut partager un domaine multicast avec :

- Comptes AWS au sein de son organisation ou entre plusieurs organisations dans AWS Organizations
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- L'ensemble de son organisation dans AWS Organizations
- AWS comptes extérieurs à AWS Organizations.

Pour partager un domaine de multicast avec un AWS compte extérieur à votre organisation, vous devez créer un partage de ressources en à l'aide de AWS Resource Access Manager, puis choisir Autoriser le partage avec n'importe qui lorsque vous sélectionnez les entités principales avec lesquelles partager le domaine de multidiffusion. Pour plus d'informations sur la création d'un partage de ressources, veuillez consulter la section [Création d'un partage de ressources AWS RAM](#) dans le Guide de l'utilisateur AWS RAM

## Table des matières

- [Conditions préalables au partage d'un domaine multicast](#)
- [Services connexes](#)
- [Partage sur plusieurs zones de disponibilité](#)
- [Partage d'un domaine multicast](#)
- [Annulation du partage d'un domaine multicast partagé](#)
- [Identification d'un domaine multicast partagé](#)
- [Autorisations des domaines multicast partagés](#)
- [Facturation et mesures](#)
- [Quotas](#)

## Conditions préalables au partage d'un domaine multicast

- Pour partager un domaine multicast, vous devez le posséder dans votre compte AWS. Vous ne pouvez pas partager un domaine multicast qui a été partagé avec vous.
- Pour partager un domaine multicast avec votre organisation ou une unité d'organisation dans AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour plus d'informations,

veuillez consulter [Activation du partage avec AWS Organizations](#) dans le Guide de l'utilisateur AWS RAM.

## Services connexes

Le partage de domaine multicast s'intègre avec AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos ressources AWS avec n'importe quel compte AWS ou via AWS Organizations. Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être des comptes AWS individuels, des unités organisationnelles ou l'ensemble d'une organisation dans AWS Organizations.

Pour de plus amples informations sur AWS RAM, veuillez consulter le [Guide de l'utilisateur AWS RAM](#).

## Partage sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, la zone de disponibilité us-east-1a pour votre compte AWS peut avoir un emplacement autre que us-east-1a pour un autre compte AWS.

Pour identifier l'emplacement de votre domaine multicast par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité (AZ ID). L'ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité entre tous les comptes AWS. Par exemple, use1-az1 est l'ID de zone de disponibilité de la région us-east-1 et dont l'emplacement est identique dans chaque compte AWS.

Pour afficher les ID de zone de disponibilité pour votre compte

1. Ouvrez la console AWS RAM à l'adresse <https://console.aws.amazon.com/ram>.
2. Les ID de zone de disponibilité pour la région actuelle sont affichés dans le volet Your AZ ID (Votre ID de zone de disponibilité) dans la partie droite de l'écran.

## Partage d'un domaine multicast

Lorsqu'un propriétaire partage un domaine multicast avec un consommateur, le consommateur peut effectuer les opérations suivantes :

- Inscrire et annuler l'inscription des membres du groupe ou des sources de groupes
- Associer et dissocier des sous-réseaux

Pour partager un domaine multicast, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre des comptes AWS. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez un domaine multicast à l'aide de la Amazon Virtual Private Cloud Console, vous l'ajoutez à un partage de ressources existant. Pour ajouter le domaine multicast à un nouveau partage de ressources, vous devez d'abord créer le partage de ressources à l'aide de la [console AWS RAM](#).

Si vous faites partie d'une organisation et que le partage au sein de votre organisation est activé, les consommateurs de votre organisation ont automatiquement accès au domaine multicast partagé. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et l'accès au domaine multicast partagé leur est octroyé lorsqu'ils acceptent l'invitation.

Vous pouvez partager un domaine multicast que vous possédez à l'aide de la console \*Amazon Virtual Private Cloud Console, de la console AWS RAM ou de l'AWS CLI.

Pour partager un domaine multicast que vous possédez à l'aide de la \*Amazon Virtual Private Cloud Console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Multicast Domains (Domaines multicast).
3. Sélectionnez le domaine multicast, puis choisissez Actions, Share multicast domain (Partager le domaine multicast).
4. Sélectionnez votre partage de ressources, puis choisissez Share multicast domain (Partager le domaine multicast).

Pour partager un domaine multicast que vous possédez à l'aide de la console AWS RAM

Consultez [Création d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM.

Pour partager un domaine multicast que vous possédez à l'aide de la AWS CLI

Utilisez la commande [create-resource-share](#).

Annulation du partage d'un domaine multicast partagé

Lors de l'annulation du partage d'un domaine multicast partagé, les actions suivantes se produisent au niveau des ressources consommateur du domaine multicast :

- Les sous-réseaux des consommateurs sont dissociés du domaine multicast. Les sous-réseaux restent dans le compte consommateur.
- Les sources de groupes de consommateurs et les membres du groupe sont dissociés du domaine multicast, puis supprimés du compte consommateur.

Pour annuler le partage d'un domaine multicast, vous devez le supprimer du partage de ressources. Pour ce faire, vous pouvez utiliser soit la console AWS RAM, soit la AWS CLI.

Pour annuler le partage d'un domaine multicast partagé qui vous appartient, vous devez le supprimer du partage de ressources. Pour ce faire, vous pouvez utiliser la \*Amazon Virtual Private Cloud Console, la console AWS RAM ou la AWS CLI.

Pour annuler le partage d'un domaine multicast partagé que vous possédez à l'aide de la \*Amazon Virtual Private Cloud Console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Multicast Domains (Domaines multicast).
3. Sélectionnez votre domaine multicast, puis choisissez Actions, Stop sharing (Arrêter le partage).

Pour annuler le partage d'un domaine multicast partagé que vous possédez à l'aide de la consoleAWS RAM

Consultez [Mise à jour d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM.

Pour annuler le partage d'un domaine multicast partagé que vous possédez à l'aide de la AWS CLI

Utilisez la commande [disassociate-resource-share](#).

## Identification d'un domaine multicast partagé

Les propriétaires et les consommateurs peuvent identifier les domaines multicast partagés à l'aide de la \*Amazon Virtual Private Cloud Console et de la AWS CLI

Pour identifier un domaine multicast partagé à l'aide de la \*Amazon Virtual Private Cloud Console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Multicast Domains (Domaines multicast).
3. Sélectionnez votre domaine multicast.
4. Sur la page Détails du domaine multicast pour le transit, affichez ID du propriétaire pour identifier l'ID de compte AWS du domaine multicast.

Pour identifier un domaine multicast partagé à l'aide de la AWS CLI

Utilisez la commande [describe-transit-gateway-multicast-domains](#). La commande renvoie les domaines multicast que vous possédez et ceux qui sont partagés avec vous. OwnerId affiche l'ID de compte AWS du propriétaire du domaine multicast.

## Autorisations des domaines multicast partagés

### Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion du domaine multicast et des membres et attachements qu'ils enregistrent ou associent au domaine. Les propriétaires peuvent modifier ou révoquer l'accès partagé à tout moment. Ils peuvent utiliser AWS Organizations pour afficher, modifier et supprimer des ressources que les utilisateurs créent sur des domaines multicast partagés.

### Autorisations accordées aux consommateurs

Les consommateurs peuvent effectuer les opérations suivantes sur les domaines multicast partagés de la même manière qu'ils le feraient sur les domaines multicast qu'ils ont créés :

- Enregistrer et désenregistrer les membres du groupe ou des sources de groupe dans le domaine multicast
- Associer un sous-réseau au domaine multicast et dissocier les sous-réseaux du domaine multicast

Les consommateurs sont responsables de la gestion des ressources qu'ils créent sur le domaine multicast partagé.

Les clients ne peuvent pas afficher ou modifier les ressources appartenant à d'autres consommateurs ou au propriétaire du domaine multicast et ils ne peuvent pas modifier les domaines multicast qui sont partagés avec eux.

### Facturation et mesures

Il n'y a pas de frais supplémentaires pour le partage de domaines multicast pour le propriétaire ou les consommateurs.

### Quotas

Un domaine multicast partagé est pris en compte dans les quotas de domaine multicast du propriétaire et du consommateur.

# Considérations sur le partage de passerelle de transit

Vous pouvez utiliser AWS Resource Access Manager (RAM) pour partager une passerelle de transit pour les attachements de VPC entre plusieurs comptes ou au sein de votre organisation dans AWS Organizations. Le RAM doit être activé et les ressources doivent être partagées avec une organisation. Pour de plus amples informations, veuillez consulter [Activer le partage de ressources avec AWS Organizations](#) dans le Guide de l'utilisateur AWS RAM.

Lorsque vous souhaitez partager une passerelle de transit, prenez en compte les éléments suivants.

- Un attachement AWS Site-to-Site VPN doit être créé dans le compte AWS auquel appartient la passerelle de transit.
- Un attachement à une passerelle Direct Connect utilise une association de passerelles de transit et peut figurer dans le même compte AWS que la passerelle Direct Connect ou un compte différent de la passerelle Direct Connect.

Par défaut, les utilisateurs ne sont pas autorisés à créer ou modifier les ressources AWS RAM. Pour autoriser les utilisateurs à créer ou à modifier des ressources et à exécuter des tâches, vous devez créer des politiques IAM qui autorisent les utilisateurs à utiliser des actions d'API et des ressources spécifiques. Vous devez ensuite attacher ces stratégies aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Seul le propriétaire d'une ressource peut effectuer les opérations suivantes :

- Créer un partage de ressources.
- Mettre à jour un partage de ressources.
- Afficher un partage de ressources.
- Afficher les ressources partagées par votre compte sur tous les partages de ressources.
- Afficher les mandataires avec qui vous partagez vos ressources sur tous les partages de ressources. L'affichage des mandataires avec qui vous effectuez un partage vous permet de déterminer qui a accès à vos ressources partagées.
- Supprimer un partage de ressources.
- Exécutez toutes les API de passerelle de transit, d'attachement de passerelle de transit et de table de routage de passerelle de transit.

Vous pouvez effectuer les opérations suivantes sur les ressources partagées avec vous :

- Accepter ou refuser une invitation de partage de ressource.
- Afficher un partage de ressources.
- Afficher les ressources partagées auxquelles vous avez accès.
- Afficher une liste de tous les mandataires qui partagent des ressources avec vous. Vous pouvez voir les ressources et les partages de ressources qu'ils ont partagés avec vous.
- Vous pouvez exécuter l'API `DescribeTransitGateways`.
- Exécuter les API qui créent et décrivent les attachements, par exemple `CreateTransitGatewayVpcAttachment` et `DescribeTransitGatewayVpcAttachments`, dans leurs VPC.
- Quitter un partage de ressources.

Lorsqu'une passerelle de transit est partagée avec vous, vous ne pouvez pas créer, modifier ou supprimer ses tables de routage de passerelle de transit, ni ses propagations et associations de tables de routage de passerelle de transit.

Lorsque vous créez une passerelle de transit, elle est créée dans la zone de disponibilité mappée à votre compte et est indépendante des autres comptes. Lorsque la passerelle de transit et les entités d'attachement se trouvent dans des comptes différents, utilisez l'ID de zone de disponibilité pour identifier de façon unique et cohérente la zone de disponibilité. Par exemple, `use1-az1` est un ID de zone de disponibilité de la région `us-east-1` et est mappé au même emplacement dans chaque compte AWS.

## Annuler le partage d'une passerelle de transit

Lorsque le propriétaire du partage annule le partage de la passerelle de transit, les règles suivantes s'appliquent :

- L'attachement de la passerelle de transit reste fonctionnelle.
- Le compte partagé ne peut pas décrire la passerelle de transit.
- Le propriétaire de la passerelle de transit et le propriétaire du partage peuvent supprimer l'attachement de la passerelle de transit.

Lorsqu'une passerelle de transit n'est pas partagée avec un autre compte AWS, ou si le compte AWS avec lequel la passerelle de transit est partagée est supprimé de l'organisation, la passerelle de transit elle-même n'en sera pas affectée.

## Sous-réseaux partagés

Un propriétaire de VPC peut attacher une passerelle de transit à un sous-réseau VPC partagé. Les participants ne le peuvent pas. Le trafic provenant des ressources des participants peut utiliser les attachements en fonction des routes définies sur le sous-réseau VPC partagé par le propriétaire du VPC.

Pour plus d'informations, consultez [Partager votre VPC avec d'autres comptes](#) dans le Guide de l'utilisateur Amazon VPC.

# Journalisation du trafic réseau à l'aide de Transit Gateway Flow Logs

Transit Gateway Flow Logs est une fonction qui vous permet de capturer des informations sur le trafic IP circulant vers et depuis vos passerelles de transit. Les données du journal de flux peuvent être publiées sur Amazon CloudWatch Logs, Amazon S3 ou Firehose. Une fois que vous avez créé un journal de flux, vous pouvez extraire et afficher ses données dans la destination choisie. Les données du journal de flux sont collectées en dehors du chemin d'accès de votre trafic réseau et n'affectent donc pas le débit réseau ou la latence. Vous pouvez créer ou supprimer des journaux de flux sans risque d'impact sur les performances du réseau. Les Transit Gateway Flow Logs capturent les informations liées uniquement aux passerelles de transit, décrites dans [the section called “Enregistrements Transit Gateway Flow Logs”](#). Si vous souhaitez capturer les journaux de flux pour capturer des informations sur le trafic IP entrant et sortant sur les interfaces réseau dans votre VPC, utilisez les journaux de flux VPC. Pour de plus amples informations, consultez [Journalisation du trafic IP à l'aide des journaux de flux VPC](#) dans le Guide de l'utilisateur Amazon VPC.

## Note

Pour créer un journal de flux de passerelle de transit, vous devez être le propriétaire de la passerelle de transit. Si vous n'êtes pas le propriétaire, le propriétaire de la passerelle de transit doit vous donner l'autorisation.

Les données des journaux de flux pour une passerelle de transit surveillée sont enregistrées sous forme d'enregistrements de journaux de flux. Il s'agit d'événements de journaux, composés de champs qui décrivent le flux de trafic. Pour plus d'informations, consultez [Enregistrements Transit Gateway Flow Logs](#).

Pour créer un journal de flux, vous spécifiez :

- La ressource pour laquelle vous souhaitez créer le journal de flux.
- Les destinations où publier les données du journal de flux.

Une fois que vous avez créé un journal de flux, plusieurs minutes peuvent s'écouler avant qu'il ne commence à collecter et à publier des données dans les destinations choisies. Les journaux de

flux ne capturent pas de flux de journaux en temps réel pour vos passerelles de transit. Pour plus d'informations, consultez [Créer un journal de flux](#).

Vous pouvez appliquer des balises à vos journaux de flux. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises peuvent vous aider à organiser vos journaux de flux, par exemple par objectif ou par propriétaire.

Si vous n'avez plus besoin d'un journal de flux, vous pouvez le supprimer. La suppression d'un journal de flux désactive le service de journal de flux pour la ressource, et aucun nouvel enregistrement de journal de flux n'est créé ou publié sur CloudWatch Logs ou Amazon S3. La suppression du journal de flux ne supprime aucun enregistrement de journal de flux, aucun flux de journal (pour les CloudWatch journaux) ou aucun objet de fichier journal (pour Amazon S3) existant pour une passerelle de transit. Pour supprimer un flux de journal existant, utilisez la console CloudWatch Logs. Pour supprimer des objets de fichier journal existants, utilisez la console Amazon S3. Une fois que vous avez supprimé un journal de flux, plusieurs minutes peuvent s'écouler avant qu'il ne cesse de collecter des données. Pour de plus amples informations, consultez [Supprimer un journal de flux](#).

## Limites

Les restrictions suivantes s'appliquent aux journaux de flux de Transit Gateway :

- Le trafic de multidiffusion n'est pas pris en charge.
- Les pièces jointes Connect ne sont pas prises en charge. Tous les journaux de flux Connect apparaissent sous la pièce jointe de transport et doivent donc être activés sur la passerelle de transit ou sur la pièce jointe de transport Connect.

## Enregistrements Transit Gateway Flow Logs

Un enregistrement de journal de flux représente un flux de réseau dans votre passerelle de transit. Chaque enregistrement est une chaîne de caractères avec des champs séparés par des espaces. Un enregistrement inclut des valeurs pour les différents composants du flux de trafic, par exemple la source, la destination et le protocole.

Lorsque vous créez un journal de flux, vous pouvez utiliser le format par défaut pour l'enregistrement de journal de flux ou spécifier un format personnalisé.

### Table des matières

- [Format par défaut](#)
- [Format personnalisé](#)
- [Champs disponibles](#)

## Format par défaut

Avec le format par défaut, les enregistrements de journaux de flux incluent tous les champs version 2 à 6, dans l'ordre indiqué dans le tableau [Champs disponibles](#). Vous ne pouvez pas personnaliser ou modifier le format par défaut. Pour capturer les champs supplémentaires ou un sous-ensemble de champs différent, spécifiez plutôt un format personnalisé.

## Format personnalisé

Avec un format personnalisé, vous spécifiez quels champs sont inclus dans les enregistrements de journaux de flux et dans quel ordre. Cela vous permet de créer des journaux de flux qui correspondent spécifiquement à vos besoins et d'ignorer les champs qui ne sont pas pertinents. L'utilisation d'un format personnalisé peut également réduire la nécessité de faire appel à des processus distincts pour extraire des informations spécifiques des journaux de flux publiés. Vous pouvez spécifier n'importe quel nombre de champs de journal de flux disponibles, mais vous devez indiquer au moins un champ.

## Champs disponibles

Le tableau suivant décrit tous les champs disponibles pour un enregistrement de journal de flux de passerelle de transit. La colonne Version indique la version dans laquelle le champ a été introduit.

Lorsque vous publiez des données du journal de flux sur Amazon S3, le type de données des champs dépend du format du journal de flux. Si le format est en texte brut, tous les champs sont de type STRING. Si le format est Parquet, consultez le tableau des types de données de champ.

Si un champ ne s'applique pas à un enregistrement spécifique ou pourrait ne pas être calculé pour celui-ci, ce dernier affiche le symbole « - » pour cette entrée. Les champs de métadonnées qui ne proviennent pas directement de l'en-tête des paquets sont des approximations optimales, et leurs valeurs peuvent être manquantes ou inexactes.

Champ	Description	Version
version	Indique la version dans laquelle le champ a été introduit. Le format par défaut inclut tous les champs version 2, dans même ordre que dans le tableau.  Type de données Parquet : INT_32	2
resource-type	Type de ressource sur laquelle l'abonnement est créé. Pour les journaux de flux de Transit Gateway, ce sera le casTransitGateway. Type de données Parquet : CHAÎNE	6
account-id	Compte AWS ID du propriétaire de la passerelle de transit source.  Type de données Parquet : CHAÎNE	2
tgw-id	ID de la passerelle de transit pour laquelle le trafic est enregistré.  Type de données Parquet : CHAÎNE	6
tgw-attachment-id	ID de l'attachement de la passerelle de transit pour lequel le trafic est enregistré.  Type de données Parquet : CHAÎNE	6
tgw-src-vpc-account-id	L' Compte AWS ID du trafic VPC source.  Type de données Parquet : CHAÎNE	6
tgw-dst-vpc-account-id	L' Compte AWS ID du trafic VPC de destination.  Type de données Parquet : CHAÎNE	6
tgw-src-vpc-id	ID du VPC source pour la passerelle de transit  Type de données Parquet : CHAÎNE	6
tgw-dst-vpc-id	ID du VPC de destination pour la passerelle de transit.  Type de données Parquet : CHAÎNE	6
tgw-src-subnet-id	ID du sous-réseau pour le trafic source de la passerelle de transit.	6

Champ	Description	Version
	Type de données Parquet : CHAÎNE	
tgw-dst-subnet-id	ID du sous-réseau pour le trafic de destination de la passerelle de transit.  Type de données Parquet : CHAÎNE	6
tgw-src-eni	ID de l'ENI d'attachement de la passerelle de transit source pour le flux.  Type de données Parquet : CHAÎNE	6
tgw-dst-eni	ID du VPC d'attachement de la passerelle de transit de destination pour le flux.  Type de données Parquet : CHAÎNE	6
tgw-src-az-id	ID de la zone de disponibilité qui contient la passerelle de transit source pour laquelle le trafic est enregistré. Si le trafic provient d'un sous-emplacement, l'enregistrement affiche un symbole « - » pour ce champ.  Type de données Parquet : CHAÎNE	6
tgw-dst-az-id	ID de la zone de disponibilité qui contient la passerelle de transit de destination pour laquelle le trafic est enregistré.  Type de données Parquet : CHAÎNE	6
tgw-pair-attachment-id	Selon la direction du flux, il s'agit de l'identifiant d'attachement de sortie ou d'entrée du flux.  Type de données Parquet : CHAÎNE	6
srcaddr	Adresse source du trafic entrant.  Type de données Parquet : CHAÎNE	2

Champ	Description	Version
dstaddr	Adresse de destination du trafic sortant. Type de données Parquet : CHAÎNE	2
srcport	Port source du trafic Type de données Parquet : INT_32	2
dstport	Port de destination du trafic Type de données Parquet : INT_32	2
protocol	Numéro de protocole IANA du trafic (pour plus d'informations, consultez la page <a href="#">Assigned Internet Protocol Numbers</a> ). Type de données Parquet : INT_64	2
packets	Nombre de paquets transférés pendant le flux. Type de données Parquet : INT_64	2
bytes	Nombre d'octets transférés pendant le flux. Type de données Parquet : INT_64	2
start	Heure, en secondes Unix, à laquelle le premier paquet du flux a été reçu dans l'intervalle d'agrégation. Jusqu'à 60 secondes peuvent s'écouler après la transmission ou la réception du paquet sur la passerelle de transit. Type de données Parquet : INT_64	2
end	Heure, en secondes Unix, à laquelle le dernier paquet du flux a été reçu dans l'intervalle d'agrégation. Jusqu'à 60 secondes peuvent s'écouler après la transmission ou la réception du paquet sur la passerelle de transit. Type de données Parquet : INT_64	2

Champ	Description	Version
log-status	<p>Statut du journal de flux :</p> <ul style="list-style-type: none"> <li>• OK — Les données sont consignées normalement dans les destinations choisies.</li> <li>• PASDEDONNÉES — Il n'y a eu aucun trafic réseau depuis ou vers l'interface réseau pendant l'intervalle d'agrégation.</li> <li>• IGNORERLESDONNÉES — Certains enregistrements de journal de flux ont été ignorés pendant l'intervalle d'agrégation. Cela peut être dû à une contrainte de capacité interne ou à une erreur interne.</li> </ul> <p>Type de données Parquet : CHAÎNE</p>	2
type	<p>Type de trafic. Les valeurs possibles sont IPv4   IPv6   EFA. Pour plus d'informations, consultez <a href="#">Elastic Fabric Adapter</a> dans le guide de l'utilisateur Amazon EC2.</p> <p>Type de données Parquet : CHAÎNE</p>	3
packets-lost-no-route	<p>Paquets perdus en raison de l'absence de route spécifiée.</p> <p>Type de données Parquet : INT_64</p>	6
packets-lost-blackhole	<p>Paquets perdus en raison d'un trou noir.</p> <p>Type de données Parquet : INT_64</p>	6
packets-lost-mtu-exceeded	<p>Paquets perdus en raison d'une taille supérieure à la MTU.</p> <p>Type de données Parquet : INT_64</p>	6
packets-lost-ttl-expired	<p>Les paquets ont été perdus en raison de l'expiration de time-to-live.</p> <p>Type de données Parquet : INT_64</p>	6

Champ	Description	Version
tcp-flags	<p>Valeur de masque de bits pour les indicateurs TCP suivants :</p> <ul style="list-style-type: none"> <li>• FIN : 1</li> <li>• SYN : 2</li> <li>• RST : 4</li> <li>• PSH — 8</li> <li>• ACK — 16</li> <li>• SYN-ACK : 18</li> <li>• URG — 32</li> </ul> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> <b>Important</b></p> <p>Lorsqu'une entrée du journal de flux se compose uniquement de paquets ACK, la valeur de l'indicateur est 0, et non 16.</p> </div> <p>Pour des informations générales sur les indicateurs TCP (comme la signification des indicateurs tels que FIN, SYN et ACK), consultez <a href="#">Structure d'un segment TCP</a> sur Wikipédia.</p> <p>Les indicateurs TCP peuvent être interrogés pendant l'intervalle d'agrégation. Pour les connexions courtes, les indicateurs peuvent être définis sur la même ligne dans l'enregistrement de journal de flux, par exemple, 19 pour SYN-ACK et FIN, et 3 pour SYN et FIN.</p> <p>Type de données Parquet : INT_32</p>	3
region	<p>Région contenant la passerelle de transit où le trafic est enregistré.</p> <p>Type de données Parquet : CHAÎNE</p>	4

Champ	Description	Version
flow-direction	La direction du flux par rapport à l'interface où le trafic est capturé. Les valeurs possibles sont les suivantes : ingress   egress.  Type de données Parquet : CHAÎNE	5
pkt-src-aws-service	Le nom du sous-ensemble de <a href="#">plages d'adresses IP</a> indiquant srcaddr si l'adresse IP source est destinée à un AWS service. Les valeurs possibles sont les suivantes : AMAZON   AMAZON_AP PFLOW   AMAZON_CONNECT   API_GATEWAY   CHIME_MEE TINGS   CHIME_VOICECONNECTOR   CLOUD9   CLOUDFRON T   CODEBUILD   DYNAMODB   EBS   EC2   EC2_INSTA NCE_CONNECT   GLOBALACCELERATOR   KINESIS_V IDEO_STREAMS   ROUTE53   ROUTE53_HEALTHCHECKS   ROUTE53_HEALTHCHECKS_PUBLISHING   ROUTE53_R ESOLVER   S3   WORKSPACES_GATEWAYS.  Type de données Parquet : CHAÎNE	5
pkt-dst-aws-service	Le nom du sous-ensemble de plages d'adresses IP pour le dstaddr champ, si l'adresse IP de destination est celle d'un AWS service. Pour obtenir une liste des valeurs possibles, consultez le champ pkt-src-aws-service.  Type de données Parquet : CHAÎNE	5

## Tarification Transit Gateway Flow Logs

Les frais d'ingestion et de stockage de données pour les journaux payants s'appliquent lorsque vous publiez des journaux de flux Transit Gateway. Pour plus d'informations sur la tarification lors de la publication de journaux vendus, ouvrez [Amazon CloudWatch Pricing](#), puis sous Niveau payant, sélectionnez Logs et recherchez Vended Logs.

## Créez un journal de flux qui publie dans CloudWatch Logs

Les journaux de flux peuvent publier les données des journaux de flux directement sur Amazon CloudWatch.

Lorsqu'elles sont publiées dans CloudWatch Logs, les données du journal de flux sont publiées dans un groupe de journaux, et chaque passerelle de transit possède un flux de journal unique dans le groupe de journaux. Les flux de journaux contiennent des enregistrements de journaux de flux. Vous pouvez créer plusieurs journaux de flux qui publient des données dans le même groupe de journaux. Si la même passerelle de transit est présente dans un ou plusieurs journaux de flux d'un même groupe de journaux, elle dispose d'un flux de journaux combiné. Si vous avez indiqué qu'un journal de flux doit capturer le trafic refusé et que l'autre journal de flux doit capturer le trafic accepté, le flux de journaux combiné capture l'ensemble du trafic.

Les frais d'ingestion de données et d'archivage pour les journaux vendus s'appliquent lorsque vous publiez des journaux de flux dans Logs. CloudWatch Pour plus d'informations, consultez [Amazon CloudWatch Pricing](#).

Dans CloudWatch Logs, le champ d'horodatage correspond à l'heure de début enregistrée dans l'enregistrement du journal de flux. Le champ IngestionTime indique la date et l'heure auxquelles l'enregistrement du journal de flux a été reçu par Logs. CloudWatch L'horodatage est ultérieur à l'heure de fin capturée dans l'enregistrement du journal de flux.

Pour plus d'informations sur CloudWatch les journaux, consultez la section [Journaux envoyés à CloudWatch Logs](#) dans le guide de l'utilisateur Amazon CloudWatch Logs.

## Table des matières

- [Rôles IAM pour publier des journaux de flux dans Logs CloudWatch](#)
- [Autorisations pour les utilisateurs IAM pour transmettre un rôle](#)
- [Créez un journal de flux qui publie dans CloudWatch Logs](#)
- [Enregistrements du flux de processus dans CloudWatch Logs](#)

## Rôles IAM pour publier des journaux de flux dans Logs CloudWatch

Le rôle IAM associé à votre journal de flux doit disposer d'autorisations suffisantes pour publier des journaux de flux dans le groupe de journaux spécifié dans CloudWatch Logs. Le rôle IAM doit appartenir à votre Compte AWS.

La stratégie IAM associée à votre rôle IAM; doit au moins inclure les autorisations suivantes :

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

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource": "*"
  }
]
}

```

Assurez-vous également que votre rôle dispose d'une relation d'approbation qui permet au service de journaux de flux d'assumer le rôle.

```

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

```

Nous vous recommandons d'utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` pour vous protéger contre [le problème du député confus](#). Par exemple, vous pouvez ajouter le bloc de condition suivant à la stratégie d'approbation précédente. Le compte source est le propriétaire du journal de flux et l'ARN source est l'ARN du journal de flux. Si vous ne connaissez pas l'ID du journal de flux, vous pouvez remplacer cette partie de l'ARN par un caractère générique (\*), puis mettre à jour la stratégie après avoir créé le journal de flux.

```

"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },

```

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

## Création ou mise à jour d'un rôle IAM pour les journaux de flux

Vous pouvez mettre à jour un rôle existant ou utiliser la procédure suivante pour créer un nouveau rôle à utiliser avec les journaux de flux.

### Création d'un rôle IAM pour les journaux de flux

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle.
3. Pour Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez Service AWS . Pour Use case (Cas d'utilisation), choisissez EC2. Choisissez Suivant.
4. Dans la page Add permissions (Ajouter des autorisations), choisissez Next: Tags (Suivant : balises) et ajoutez des balises si vous le souhaitez. Choisissez Suivant.
5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un nom pour votre rôle et fournissez une Description, le cas échéant. Sélectionnez Créer un rôle.
6. Choisissez le nom de votre rôle. Pour Add permissions (Ajouter des autorisations), choisissez Create inline policy (Créer une politique en ligne), puis l'onglet JSON.
7. Copiez la première stratégie de [Rôles IAM pour publier des journaux de flux dans Logs CloudWatch](#) et collez-la dans la fenêtre. Choisissez Examiner une politique.
8. Entrez un nom pour votre stratégie, puis choisissez Créer une stratégie.
9. Sélectionnez le nom de votre rôle. Sous Relations d'approbation, choisissez Modifier la relation d'approbation. Dans le document de stratégie existant, modifiez le service de `ec2.amazonaws.com` à `vpc-flow-logs.amazonaws.com`. Choisissez Update Trust Policy.
10. Sur la page Summary (Récapitulatif), notez l'ARN de votre rôle. Vous en avez besoin lors de la création de votre journal de flux.

## Autorisations pour les utilisateurs IAM pour transmettre un rôle

Les utilisateurs doivent également disposer d'autorisations pour utiliser l'action `iam:PassRole` en ce qui concerne le rôle IAM associé au journal de flux.

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

## Créez un journal de flux qui publie dans CloudWatch Logs

Vous pouvez créer des journaux de flux pour les passerelles de transit. Si vous effectuez ces étapes en tant qu'utilisateur IAM, assurez-vous de disposer des autorisations nécessaires afin d'utiliser l'action `iam:PassRole`. Pour plus d'informations, consultez [Autorisations pour les utilisateurs IAM pour transmettre un rôle](#).

Pour créer un journal de flux de passerelle de transit à l'aide de la console

1. [Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/vpc/`](https://console.aws.amazon.com/vpc/).
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit).
3. Cochez les cases correspondant à une ou plusieurs passerelles de transit et sélectionnez Actions, puis Create flow log (Créer un journal de flux).
4. Pour Destination, choisissez Envoyer vers CloudWatch les journaux.
5. Pour Destination log group (Groupe de journaux de destination), choisissez le nom d'un groupe de journaux de destination actuel.

### Note

Si le groupe de journaux de destination n'existe pas encore, la saisie d'un nouveau nom dans ce champ créera un nouveau groupe de journaux de destination.

6. Pour le rôle IAM, spécifiez le nom du rôle autorisé à publier des journaux dans CloudWatch Logs.
7. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.

- Pour utiliser le format par défaut, choisissez AWS default format (Format par défaut).
  - Pour utiliser un format personnalisé, choisissez Custom format (Format personnalisé), puis sélectionnez des champs dans Log format (Format du journal).
8. (Facultatif) Sélectionnez Add new tag (Ajouter une nouvelle balise) pour appliquer des identifications au journal de flux.
  9. Choisissez Créer le journal de flux.

Pour créer un journal de flux à l'aide de la ligne de commande

Utilisez l'une des commandes suivantes.

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlowJournaux](#) (API de requête Amazon EC2)

L' AWS CLI exemple suivant crée un journal de flux qui capture les informations relatives aux passerelles de transit. Les journaux de flux sont transmis à un groupe de CloudWatch journaux dans Logs appelé my-flow-logs, dans le compte 123456789101, à l'aide du rôle IAM. publishFlowLogs

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

## Enregistrements du flux de processus dans CloudWatch Logs

Vous pouvez utiliser les enregistrements des journaux de flux comme vous le feriez avec tout autre événement de journal collecté par CloudWatch Logs. Pour plus d'informations sur la surveillance des données de journal et les filtres métriques, consultez la section [Recherche et filtrage des données de journal](#) dans le guide de CloudWatch l'utilisateur Amazon.

**Exemple : création d'un filtre CloudWatch métrique et d'une alarme pour un journal de flux**

Dans cet exemple, vous avez un journal de flux pour tgw-123abc456bca. Vous souhaitez créer une alarme qui vous alerte si au moins 10 tentatives de connexion à votre instance via le port TCP 22

(SSH) sont refusées dans un laps de temps d'une heure. Tout d'abord, vous devez créer un filtre de métrique qui correspond au modèle de trafic pour lequel créer l'alarme. Vous pouvez ensuite créer une alarme pour le filtre de métrique.

Pour créer un filtre de métrique pour le trafic SSH refusé et une alarme pour ce filtre :

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux).
3. Cochez la case en regard du groupe de journaux, puis choisissez Actions, Create metric filter (Créer un filtre de métrique).
4. Pour Modèle de filtre, fournissez les informations suivantes.

```
[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. Pour Select log data to test (Sélectionner les données de journal à tester), sélectionnez le flux de journal de votre passerelle de transit. (Facultatif) Pour afficher les lignes de données de journal qui correspondent au modèle de filtre, choisissez Test pattern (Tester le modèle). Lorsque vous avez terminé, choisissez Next (Suivant).
  6. Entrez un nom de filtre, un espace de noms de mesure et un nom de métrique. Définissez la valeur de métrique sur **1**. Lorsque vous avez terminé, choisissez Next (Suivant), puis Create metric filter (Créer un filtre de métrique).
  7. Dans le panneau de navigation, choisissez Alarms (Alarmes), All alarms (Toutes les alarmes).
  8. Choisissez Create alarm. (Créer une alarme).
  9. Choisissez l'espace de noms du filtre de métrique que vous avez créé.
- Il peut s'écouler quelques minutes avant qu'une nouvelle métrique ne s'affiche dans la console.
10. Sélectionnez le nom de la métrique que vous avez créée, puis choisissez Select metric (Sélectionner une métrique).
  11. Configurez l'alarme comme suit, puis choisissez Next (Suivant) :

- Pour Statistics (Statistique), choisissez Sum (Somme). Ainsi, vous capturez le nombre total de points de données pour la période spécifiée.
  - Pour Period (Période), choisissez 1 hour (1 heure).
  - Pour Chaque fois, choisissez Supérieur à/Égal à et saisissez **10** pour le seuil.
  - Sous Additional configuration (Configuration supplémentaire), conservez la valeur **1** pour Datapoints to alarm (Points de données à signaler).
12. Pour Notification, sélectionnez une rubrique SNS existante ou choisissez Create new topic (Créer une rubrique) pour en créer une nouvelle. Choisissez Next (Suivant).
  13. Saisissez le nom et la description de l'alarme, puis choisissez Next (Suivant).
  14. Lorsque vous avez terminé de configurer l'alarme, choisissez Create alarm (Créer une alarme).

## Créer un journal de flux qui publie vers Amazon S3

Les journaux de flux peuvent publier des données de journal de flux vers Amazon S3.

Lors de la publication vers Amazon S3, les données de journal de flux sont publiées dans un compartiment Amazon S3 existant que vous indiquez. Les enregistrements de journaux de flux pour toutes les passerelles de transit surveillées sont publiés dans une série d'objets de fichier journal qui sont stockés dans le compartiment.

Des frais d'ingestion de données et d'archivage sont appliqués aux journaux vendus lorsque vous publiez des journaux de flux sur Amazon S3. Amazon CloudWatch Pour plus d'informations sur la CloudWatch tarification des journaux vendus, ouvrez [Amazon CloudWatch Pricing](#), choisissez Logs, puis recherchez Vended Logs.

Pour créer un compartiment Amazon S3 à utiliser avec les journaux de flux, reportez-vous à [Créer un compartiment](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour plus d'informations sur la journalisation de plusieurs comptes, veuillez consulter [Journalisation centrale](#) dans la bibliothèque de solutions AWS .

Pour plus d'informations sur CloudWatch les journaux, consultez la section [Journaux envoyés à Amazon S3](#) dans le guide de l'utilisateur Amazon CloudWatch Logs.

### Table des matières

- [Fichiers journaux de flux](#)

- [Politique IAM pour les principaux IAM qui publient des journaux de flux vers Amazon S3](#)
- [Autorisations du compartiment Amazon S3 pour les journaux de flux](#)
- [Politique de clé obligatoire à utiliser avec SSE-KMS](#)
- [Autorisations pour les fichiers journaux Amazon S3](#)
- [Créer un journal de flux qui publie vers Amazon S3](#)
- [Traiter des enregistrements de journal de flux dans Amazon S3](#)

## Fichiers journaux de flux

VPC Flow Logs est une fonction qui collecte les enregistrements des journaux de flux, les consolide dans des fichiers journaux, puis publie les fichiers journaux dans le compartiment Amazon S3 à intervalles de 5 minutes. Chaque fichier journal contient des enregistrements de journaux de flux pour le trafic IP enregistré au cours des cinq dernières minutes.

La taille maximale d'un fichier journal est de 75 Mo. Si le fichier journal atteint la limite maximale de taille au cours de la période de 5 minutes, le journal de flux cesse de lui ajouter des enregistrements de journal de flux. Ensuite, il publie le journal de flux dans le compartiment Amazon S3, puis crée un fichier journal.

Dans Amazon S3, le champ Last modified (Dernière modification) du fichier de journal de flux indique la date et l'heure du téléchargement du fichier dans le compartiment Amazon S3. Cette date est postérieure à l'horodatage du nom du fichier et diffère par le temps nécessaire pour charger le fichier vers le compartiment Amazon S3.

### Format de fichier journal

Vous pouvez spécifier l'un des formats suivants pour les fichiers journaux. Chaque fichier est compressé dans un seul fichier Gzip.

- Text : texte brut. Il s'agit du format par défaut.
- Parquet : Apache Parquet est un format de données en colonnes. Les requêtes sur les données au format Parquet sont 10 à 100 fois plus rapides que les requêtes sur des données en texte brut. Les données au format Parquet avec compression Gzip occupent 20 % moins d'espace de stockage que le texte brut avec compression Gzip.

## Options de fichier journal

Le cas échéant, vous pouvez spécifier les options suivantes :

- Hive-compatible S3 prefixes (Préfixes S3 compatibles Hive) : activez les préfixes compatibles Hive au lieu d'importer des partitions dans vos outils compatibles Hive. Avant d'exécuter des requêtes, utilisez la commande `MSCK REPAIR TABLE`.
- Hourly partitions (Partitions horaires) : si vous disposez d'un grand volume de journaux et que vous ciblez généralement les requêtes à une heure spécifique, vous pouvez obtenir des résultats plus rapidement et économiser sur les coûts des requêtes en partitionnant les journaux toutes les heures.

## Structure du compartiment S3 du fichier journal

Les fichiers journaux sont enregistrés dans le compartiment Amazon S3 indiqué à l'aide d'une structure de dossiers qui est déterminée par l'ID du journal de flux, sa région, sa date de création et ses options de destination.

Par défaut, les fichiers sont distribués vers l'emplacement suivant.

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

Si vous activez les préfixes S3 compatibles Hive, les fichiers sont envoyés à l'emplacement suivant.

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

Si vous activez les partitions horaires, les fichiers sont envoyés à l'emplacement suivant.

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

Si vous activez les partitions compatibles Hive et que vous partitionnez le journal de flux par heure, les fichiers sont envoyés à l'emplacement suivant.

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

## Noms des fichiers journaux

Le nom de fichier d'un fichier journal est basé sur l'ID du journal de flux, la région et la date et l'heure de création. Les noms de fichier utilisent le format suivant.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Voici un exemple de fichier journal pour un journal de flux créé par le Compte AWS 123456789012, pour une ressource dans la région us-east-1, le June 20, 2018 à 16:20 UTC. Le fichier contient les enregistrements de journaux de flux avec une heure de fin comprise entre 16:20:00 et 16:24:59.

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

## Politique IAM pour les principaux IAM qui publient des journaux de flux vers Amazon S3

Le principal IAM qui crée le journal de flux doit avoir les autorisations suivantes, qui sont nécessaires pour publier les journaux de flux dans le compartiment Amazon S3 de destination.

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

## Autorisations du compartiment Amazon S3 pour les journaux de flux

Par défaut, les compartiments Amazon S3 et les objets qu'ils contiennent sont privés. Seul le propriétaire du compartiment peut accéder au compartiment et aux objets qui y sont stockés. Cependant, le propriétaire du compartiment peut accorder l'accès à d'autres ressources et à d'autres utilisateurs en créant une politique d'accès.

Si l'utilisateur qui crée le journal de flux est le propriétaire du compartiment et dispose des autorisations `PutBucketPolicy` et `GetBucketPolicy` pour le compartiment, nous attachons

automatiquement la stratégie suivante au compartiment. Cette politique remplace toute politique existante attachée au compartiment.

Sinon, le propriétaire du compartiment doit ajouter cette politique au compartiment en spécifiant l'ID du Compte AWS du créateur du journal de flux. Sinon, la création du journal de flux échoue. Pour plus d'informations, consultez [Utilisation de stratégies de compartiment](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

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

```
}
```

L'ARN que vous spécifiez pour *my-s3-arn* varie selon que vous utilisez des préfixes S3 compatibles avec Hive.

- Préfixes par défaut

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

- Préfixes S3 compatibles avec Hive

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

En tant que bonne pratique, nous vous recommandons d'accorder ces autorisations au principal du service de livraison des journaux plutôt qu'à des Compte AWS ARN individuels. Une autre bonne pratique consiste également à utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` afin de vous protéger contre [le problème du député confus](#). Le compte source est le propriétaire du journal de flux et l'ARN source est l'ARN à caractère générique (\*) du service de journaux.

## Politique de clé obligatoire à utiliser avec SSE-KMS

Vous pouvez protéger les données de votre compartiment Amazon S3 en activant soit le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3), soit le chiffrement côté serveur avec des clés KMS stockées (SSE-KMS). Pour plus d'informations, consultez la section [Protection des données à l'aide d'un chiffrement côté serveur](#) dans le Guide de l'utilisateur d'Amazon S3.

Avec SSE-KMS, vous pouvez utiliser une clé AWS gérée ou une clé gérée par le client. Avec une clé AWS gérée, vous ne pouvez pas utiliser la livraison entre comptes. Les journaux de flux sont diffusés à partir du compte de diffusion des journaux. Vous devez donc accorder l'accès pour la diffusion entre comptes. Pour accorder l'accès entre comptes à votre compartiment S3, utilisez une clé gérée par le client et spécifiez l'Amazon Resource Name (ARN) de la clé gérée par le client lorsque vous activez le chiffrement de compartiment. Pour plus d'informations, veuillez consulter la section [Spécification du chiffrement côté serveur avec AWS KMS](#) du Guide de l'utilisateur d'Amazon S3.

Lorsque vous utilisez SSE-KMS avec une clé gérée par le client, vous devez ajouter ce qui suit à la politique clé de votre clé (et non pas la politique de compartiment de votre compartiment S3), afin que les journaux de flux de VPC puissent écrire dans votre compartiment S3.

```
{
  "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": "*"
}
```

## Autorisations pour les fichiers journaux Amazon S3

Outre les stratégies de compartiment obligatoires, Amazon S3 utilise des listes de contrôle d'accès (ACL) afin de gérer l'accès aux fichiers journaux créés par un journal de flux. Par défaut, le propriétaire du compartiment dispose d'autorisations FULL\_CONTROL sur chaque fichier journal. Si le propriétaire de la diffusion des journaux n'est pas le propriétaire du compartiment, il ne dispose d'aucune autorisation. Le compte de diffusion des journaux possède les autorisations READ et WRITE. Pour de plus amples informations, veuillez consulter [Présentation des listes de contrôle d'accès \(ACL\)](#) dans le Guide du développeur Amazon Simple Storage Service.

## Créer un journal de flux qui publie vers Amazon S3

Une fois votre compartiment Amazon S3 créé et configuré, vous pouvez créer des journaux de flux pour les passerelles de transit.

Pour créer un journal de flux de passerelle de transit publié dans Amazon S3 à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit), Transit gateway attachment (Attachements de passerelle de transit).
3. Cochez les cases correspondant à une ou plusieurs passerelles de transit ou à un ou plusieurs attachements de passerelle de transit.
4. Choisissez Actions, Create flow log (Créer le journal de flux).
5. Configurez les paramètres du journal de flux. Pour de plus amples informations, veuillez consulter [Pour configurer les paramètres du journal de flux](#).

Pour configurer des paramètres de journaux de flux à l'aide de la console

1. Pour Destination, choisissez Send to an S3 bucket (Envoyer vers un compartiment S3).
2. Pour S3 bucket ARN (ARN de compartiment S3), indiquez l'Amazon Resource Name (ARN) d'un compartiment Amazon S3 existant. Vous pouvez éventuellement inclure un sous-dossier. Par exemple, pour spécifier le sous-dossier `my-logs` dans le compartiment `my-bucket`, utilisez l'ARN suivant :

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

Le compartiment ne peut pas utiliser `AWSLogs` comme nom de sous-dossier, car il s'agit d'un terme réservé.

Si vous êtes le propriétaire du compartiment, nous créons automatiquement une politique de ressource et l'attachons au compartiment. Pour de plus amples informations, veuillez consulter [Autorisations du compartiment Amazon S3 pour les journaux de flux](#).

3. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.
  - Pour utiliser le format de registre de journal de flux par défaut, sélectionnez AWS default format (Format par défaut).
  - Pour créer un format personnalisé, choisissez Custom format (Format personnalisé). Pour Log format (Format de journal), choisissez les champs à inclure dans l'enregistrement de journal de flux.
4. Pour Format du fichier journal, spécifiez le format du fichier journal.
  - Text : texte brut. Il s'agit du format par défaut.

- Parquet : Apache Parquet est un format de données en colonnes. Les requêtes sur les données au format Parquet sont 10 à 100 fois plus rapides que les requêtes sur des données en texte brut. Les données au format Parquet avec compression Gzip occupent 20 % moins d'espace de stockage que le texte brut avec compression Gzip.
5. (Facultatif) Pour utiliser des préfixes S3 compatibles avec Hive, choisissez Hive-compatible S3 prefix (Préfixe S3 compatible HIVE), Enable. (Activer).
  6. (Facultatif) Pour partitionner vos journaux de flux par heure, choisissez Every 1 hour (60 mins) (Toutes les 1 heure (60 minutes)).
  7. (Facultatif) Pour ajouter une identification au journal de flux, choisissez Add new tag (Ajouter une nouvelle identification) et spécifiez la clé et la valeur de l'identification.
  8. Choisissez Create flow log. (Créer le journal de flux).

Pour créer un journal de flux qui publie vers Amazon S3 à l'aide de l'outil de ligne de commande

Utilisez l'une des commandes suivantes.

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlowJournaux](#) (API de requête Amazon EC2)

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic de passerelle de transit pour VPC `tgw-00112233344556677` et fournit les journaux de flux à un compartiment Amazon S3 appelé. `flow-log-bucket` Le paramètre `--log-format` spécifie un format personnalisé pour les enregistrements de journal de flux.

```
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/
```

## Traiter des enregistrements de journal de flux dans Amazon S3

Les fichiers journaux sont compressés. Si vous ouvrez les fichiers journaux à l'aide de la console Amazon S3, ils sont décompressés et les enregistrements de journal de flux s'affichent. Si vous téléchargez les fichiers, vous devez les décompresser pour afficher les enregistrements de journaux de flux.

# Publier des journaux de flux sur Firehose

## Rubriques

- [Rôles IAM pour la diffusion entre comptes](#)
- [Créez un journal de flux qui publie sur Firehose](#)

Les journaux de flux peuvent publier les données des journaux de flux directement dans Firehose. Vous pouvez choisir de publier les journaux de flux sur le même compte que le moniteur de ressources ou sur un autre compte.

## Conditions préalables

Lors de la publication sur Firehose, les données du journal de flux sont publiées dans un flux de diffusion Firehose, au format texte brut. Vous devez d'abord avoir créé un flux de diffusion Firehose. Pour connaître les étapes de création d'un flux de diffusion, consultez la section [Création d'un flux de diffusion Amazon Data Firehose](#) dans le manuel du développeur Amazon Data Firehose.

## Tarifcation

Des frais d'ingestion et de diffusion standard s'appliquent. Pour plus d'informations, ouvrez [Amazon CloudWatch Pricing](#), sélectionnez Logs et recherchez Vended Logs.

## Rôles IAM pour la diffusion entre comptes

Lorsque vous publiez sur Kinesis Data Firehose, vous pouvez choisir un flux de diffusion qui se trouve dans le même compte que la ressource à surveiller (le compte source) ou dans un compte différent (le compte de destination). Pour permettre la transmission des journaux de flux entre comptes à Firehose, vous devez créer un rôle IAM dans le compte source et un rôle IAM dans le compte de destination.

## Rôles

- [Rôle du compte source](#)
- [Rôle du compte de destination](#)

## Rôle du compte source

Dans le compte source, créez un rôle qui accorde les autorisations suivantes. Dans cet exemple, le rôle a pour nom `mySourceRole`, mais vous pouvez choisir un nom différent. La dernière instruction

permet au rôle dans le compte de destination d'assumer ce rôle. Les instructions de condition garantissent que ce rôle est transmis uniquement au service de diffusion de journaux, et uniquement lors de la surveillance de la ressource spécifiée. Lorsque vous créez votre politique, spécifiez les VPC, les interfaces réseau ou les sous-réseaux que vous surveillez à l'aide de la clé de condition `iam:AssociatedResourceARN`.

```
{
  "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"
    }
  ]
}
```

```
}
```

Assurez-vous que ce rôle possède la politique de confiance suivante, qui permet au service de diffusion de journaux d'assumer ce rôle.

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

À partir du compte source, observez la procédure suivante afin de créer le rôle.

Pour créer le rôle du compte source

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Politiques.
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Create policy (Créer une stratégie), procédez comme suit :
  1. Choisissez JSON.
  2. Remplacez le contenu de cette fenêtre par la politique d'autorisations au début de cette section.
  3. Choisissez Next: Tags (Suivant : Balises), puis Next: Review (Suivant : Vérification).
  4. Saisissez un nom pour votre politique ainsi qu'une description facultative, puis choisissez Create policy (Créer une politique).
5. Dans le panneau de navigation, choisissez Roles (Rôles).
6. Sélectionnez Create role (Créer un rôle).
7. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée). Pour Custom trust policy (Politique de confiance personnalisée),

remplacez "Principal": {}, par ce qui suit, qui spécifie le service de diffusion de journaux. Choisissez Suivant.

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

8. Sur la page Add permissions (Ajouter des autorisations), cochez la case correspondant à la politique que vous avez créée plus tôt dans cette procédure, puis choisissez Next (Suivant).
9. Entrez un nom pour votre rôle et fournissez une description, le cas échéant.
10. Sélectionnez Créer un rôle.

## Rôle du compte de destination

Dans le compte de destination, créez un rôle dont le nom commence par AWSLogsDeliveryFirehoseCrossAccountRole. Ce rôle doit accorder les autorisations suivantes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Assurez-vous que ce rôle possède la politique de confiance suivante, qui permet au rôle que vous avez créé dans le compte source d'assumer ce rôle.

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

```
    "AWS": "arn:aws:iam::source-account:role/mySourceRole"
  },
  "Action": "sts:AssumeRole"
}
]
```

À partir du compte de destination, appliquez la procédure suivante afin de créer le rôle.

Pour créer le rôle du compte de destination

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Politiques.
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Create policy (Créer une stratégie), procédez comme suit :
  1. Choisissez JSON.
  2. Remplacez le contenu de cette fenêtre par la politique d'autorisations au début de cette section.
  3. Choisissez Next: Tags (Suivant : Balises), puis Next: Review (Suivant : Vérification).
  4. Entrez un nom pour votre politique commençant par AWSLogDeliveryFirehoseCrossAccountRole, puis choisissez Créer une politique.
5. Dans le panneau de navigation, choisissez Roles (Rôles).
6. Sélectionnez Create role (Créer un rôle).
7. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée). Pour Custom trust policy (Politique de confiance personnalisée), remplacez "Principal": {}, par ce qui suit, qui spécifie le service de diffusion de journaux. Choisissez Suivant.

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

8. Sur la page Add permissions (Ajouter des autorisations), cochez la case correspondant à la politique que vous avez créée plus tôt dans cette procédure, puis choisissez Next (Suivant).
9. Entrez un nom pour votre rôle et fournissez une description, le cas échéant.

## 10. Sélectionnez Créer un rôle.

### Créez un journal de flux qui publie sur Firehose

Pour créer un journal de flux de passerelle de transit publié sur Firehose à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit), Transit gateway attachment (Attachements de passerelle de transit).
3. Cochez les cases correspondant à une ou plusieurs passerelles de transit ou à un ou plusieurs attachements de passerelle de transit.
4. Choisissez Actions, Create flow log (Créer le journal de flux).
5. Pour Destination, choisissez Envoyer vers un système de distribution Firehose.
6. Pour Firehose Delivery Stream ARN (ARN du flux de distribution Firehose), choisissez l'ARN d'un flux de distribution que vous avez créé dans lequel le journal des flux doit être publié.
7. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.
  - Pour utiliser le format de registre de journal de flux par défaut, sélectionnez AWS default format (Format par défaut).
  - Pour créer un format personnalisé, choisissez Custom format (Format personnalisé). Pour Log format (Format de journal), choisissez les champs à inclure dans l'enregistrement de journal de flux.
8. (Facultatif) Pour ajouter une identification au journal de flux, choisissez Add new tag (Ajouter une nouvelle identification) et spécifiez la clé et la valeur de l'identification.
9. Choisissez Create flow log. (Créer le journal de flux).

Pour créer un journal de flux publié sur Firehose à l'aide de l'outil de ligne de commande

Utilisez l'une des commandes suivantes :

- [create-flow-logs](#) (CLI)AWS
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlowJournaux](#) (API de requête Amazon EC2)

L'exemple de AWS CLI suivant crée un journal de flux qui capture les informations relatives à la passerelle de transit et fournit le journal de flux au flux de diffusion Firehose spécifié.

```
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
```

L'exemple de AWS CLI suivant crée un journal de flux qui capture les informations relatives à la passerelle de transit et fournit le journal de flux à un flux de diffusion Firehose différent du compte source.

```
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
```

## Utiliser Transit Gateway Flow Logs

Vous pouvez utiliser les journaux de flux de Transit Gateway à l'aide des consoles Amazon EC2, Amazon VPC et CloudWatch Amazon S3.

### Tâches

- [Contrôler l'utilisation des journaux de flux](#)
- [Créer un journal de flux](#)
- [Afficher les journaux de flux](#)
- [Ajouter ou supprimer des identifications pour les journaux de flux](#)
- [Afficher les enregistrements de journaux de flux](#)
- [Rechercher des enregistrements de journaux de flux](#)
- [Supprimer un journal de flux](#)

- [Présentation et limites de l'API et de la CLI](#)

## Contrôler l'utilisation des journaux de flux

Par défaut, les utilisateurs ne sont pas autorisés à utiliser des journaux de flux. Vous pouvez créer une stratégie d'utilisateur qui autorise les utilisateurs à créer, décrire et supprimer des journaux de flux. Pour de plus amples informations, veuillez consulter [Attribution des autorisations nécessaires aux utilisateurs IAM pour les ressources Amazon EC2](#) dans la référence d'API Amazon EC2.

Voici un exemple de politique qui accorde aux utilisateurs les autorisations complètes pour créer, décrire et supprimer des journaux de flux.

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

Une configuration supplémentaire des rôles et des autorisations IAM est requise, selon que vous publiez sur CloudWatch Logs ou Amazon S3. Pour de plus amples informations, veuillez consulter [Créer un journal de flux qui publie dans CloudWatch Logs](#) et [Créer un journal de flux qui publie vers Amazon S3](#).

## Créer un journal de flux

Vous pouvez créer des journaux de flux pour vos passerelles de transit qui peuvent publier des données sur CloudWatch Logs, Amazon S3 ou Firehose.

Pour plus d'informations, consultez les ressources suivantes :

- [Créer un journal de flux qui publie dans CloudWatch Logs](#)

- [Créer un journal de flux qui publie vers Amazon S3](#)
- [Créez un journal de flux qui publie sur Firehose](#)

## Afficher les journaux de flux

Vous pouvez afficher les informations sur vos fichiers journaux dans la console Amazon VPC en accédant à l'onglet Flow Logs (Journaux de flux) pour une ressource spécifique. Lorsque vous sélectionnez la ressource, tous les journaux de flux de cette ressource sont répertoriés. Les informations affichées incluent l'ID du journal de flux, sa configuration et des informations sur son statut.

Pour afficher des informations sur les journaux de flux pour les passerelles de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit), Transit gateway attachment (Attachements de passerelle de transit).
3. Sélectionnez une passerelle de transit ou un attachement de passerelle de transit et choisissez Flow Logs (Journaux de flux). Les informations sur les fichiers journaux s'affichent dans l'onglet. La colonne Destination type (Type de destination) indique la destination où les journaux de flux sont publiés.

## Ajouter ou supprimer des identifications pour les journaux de flux

Vous pouvez ajouter ou supprimer les identifications d'un journal de flux dans les consoles Amazon EC2 et Amazon VPC.

Pour ajouter ou supprimer des balises pour un journal de flux de passerelle de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit), Transit gateway attachment (Attachements de passerelle de transit).
3. Sélectionnez une passerelle de transit ou un attachement de passerelle de transit.
4. Choisissez Manage tags (Gérer les identifications) pour le journal de flux requis.
5. Pour ajouter une nouvelle balise, choisissez Create Tag. (Créer une identification). Pour supprimer une identification, choisissez le bouton de suppression (x).
6. Choisissez Save (Enregistre).

## Afficher les enregistrements de journaux de flux

Vous pouvez consulter les enregistrements de vos CloudWatch journaux de flux à l'aide de la console Logs ou de la console Amazon S3, selon le type de destination choisi. Après la création du journal de flux, quelques minutes peuvent s'écouler avant qu'il ne s'affiche dans la console.

Pour afficher les enregistrements du journal de flux publiés dans CloudWatch Logs

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, choisissez Logs (Journaux), puis sélectionnez le groupe de journaux contenant votre journal de flux. Une liste de flux de journaux s'affiche pour chaque passerelle de transit.
3. Sélectionnez le flux de journaux contenant l'ID de la passerelle de transit pour laquelle vous souhaitez afficher les enregistrements du journal de flux. Pour plus d'informations, consultez [Enregistrements Transit Gateway Flow Logs](#).

Pour afficher des enregistrements de journal de flux publiés dans Amazon S3

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Pour Bucket name (Nom du compartiment), sélectionnez le compartiment dans lequel les journaux de flux sont publiés.
3. Pour Name (Nom), cochez la case en regard du fichier journal. Dans le panneau de présentation de l'objet, choisissez Download(Télécharger).

## Rechercher des enregistrements de journaux de flux

Vous pouvez rechercher les enregistrements de vos journaux de flux publiés dans CloudWatch Logs à l'aide de la console CloudWatch Logs. Vous pouvez utiliser des [filtres de métrique](#) pour filtrer les enregistrements de journal de flux. Les enregistrements de journaux de flux sont délimités par un espace.

Pour rechercher des enregistrements de journaux de flux à l'aide de la console CloudWatch Logs

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), puis Log groups (Groupes de journaux).

3. Sélectionnez le groupe de journaux contenant votre journal de flux. Une liste de flux de journaux s'affiche pour chaque passerelle de transit.
4. Sélectionnez le flux de journaux individuel si vous connaissez la passerelle de transit que vous recherchez. Vous pouvez également choisir Search Log Group (Rechercher dans le groupe de journaux) pour rechercher dans l'ensemble du groupe de journaux. Cela peut prendre un certain temps si votre groupe de journaux compte de nombreuses passerelles de transit, ou en fonction de la plage de temps que vous sélectionnez.
5. Pour Filter events (Événements de filtre), saisissez la chaîne suivante. Cela suppose que l'enregistrement de journaux de flux utilise le [format par défaut](#).

```
[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. Modifiez le filtre selon vos besoins en spécifiant des valeurs pour les champs. Dans les exemples suivants, le filtrage a lieu en fonction d'adresses IP source spécifiques.

```
[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]
```

L'exemple suivant filtre par ID de passerelle de transit tgw-123abc456bca, port de destination et nombre d'octets.

```
[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]
```

## Supprimer un journal de flux

Vous pouvez supprimer un journal de flux de passerelle de transit à l'aide de la console Amazon VPC.

Ces procédures désactivent le service de journaux de flux pour la ressource concernée. La suppression d'un journal de flux ne supprime pas les flux de journaux existants CloudWatch des journaux ou des fichiers journaux d'Amazon S3. Les données de journaux de flux existantes doivent être supprimées à l'aide de la console de service correspondante. En outre, l'effacement d'un journal de flux publié dans Amazon S3 ne supprime pas les politiques de compartiment et les listes de contrôle d'accès (ACL) de fichier journaux.

Pour supprimer un journal de flux de passerelle de transit

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit).
3. Choisissez un ID de passerelle de transit.
4. Dans la section Flow logs (Journaux de flux), choisissez les journaux de flux que vous souhaitez supprimer.
5. Choisissez Actions, puis Delete flow logs (Supprimer les journaux de flux).
6. Confirmez votre souhait de supprimer le flux en choisissant Delete (Supprimer).

## Présentation et limites de l'API et de la CLI

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou de l'API.

Les limites suivantes s'appliquent lorsque vous utilisez l'API [CreateFlowLogs](#) ou la CLI [create-flow-logs](#) :

- `--resource-ids` a une contrainte maximale de 25 types de ressource `TransitGateway` ou `TransitGatewayAttachment`.
- `--traffic-type` n'est pas un champ obligatoire par défaut. Une erreur est renvoyée si vous l'indiquez pour les types de ressource de passerelle de transit. Cette limite s'applique uniquement aux types de ressource de passerelle de transit.
- `--max-aggregation-interval` a pour valeur par défaut 60, qui est la seule valeur acceptée pour les types de ressource de passerelle de transit. Une erreur est renvoyée si vous essayez de transmettre une autre valeur. Cette limite s'applique uniquement aux types de ressource de passerelle de transit.
- `--resource-type` prend en charge deux types de ressource, `TransitGateway` et `TransitGatewayAttachment`.
- `--log-format` inclut tous les champs de journal pour les types de ressource de passerelle de transit si vous ne définissez pas les champs à inclure. Cette limite s'applique uniquement aux types de ressource de passerelle de transit.

Créer un journal de flux

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [CreateFlowJournaux](#) (API de requête Amazon EC2)

Décrire vos journaux de flux

- [describe-flow-logs](#) (AWS CLI)
- [Get-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DescribeFlowJournaux](#) (API de requête Amazon EC2)

Afficher vos enregistrements de journaux de flux (événements de journaux)

- [get-log-events](#) (AWS CLI)
- [Obtenez un appel \(\) LogEvent](#) (AWS Tools for Windows PowerShell)
- [GetLogÉvénements](#) (CloudWatchAPI)

## Supprimer un journal de flux

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DeleteFlowJournaux](#) (API de requête Amazon EC2)

# Surveiller vos passerelles de transit

Vous pouvez utiliser les fonctionnalités suivantes pour surveiller vos passerelles de transit, analyser les schémas de trafic et résoudre les problèmes relatifs à celles-ci.

## Métriques CloudWatch

Vous pouvez utiliser Amazon CloudWatch pour récupérer des statistiques sur les points de données de vos passerelles de transit sous la forme d'un ensemble ordonné de données de séries chronologiques appelées métriques. Vous pouvez utiliser ces métriques pour vérifier que le système fonctionne comme prévu. Pour de plus amples informations, veuillez consulter [Métriques CloudWatch pour vos passerelles de transit](#).

## Transit Gateway Flow Logs

Vous pouvez utiliser Transit Gateway Flow Logs pour capturer des informations détaillées sur le trafic réseau de vos passerelles de transit. Pour de plus amples informations, veuillez consulter [Transit Gateway Flow Logs](#).

## Journaux de flux VPC

Vous pouvez utiliser les journaux de flux VPC pour capturer des informations détaillées à propos du trafic entrant ou sortant des VPC attachés à vos passerelles de transit. Pour plus d'informations, consultez [Journaux de flux VPC](#) dans le Amazon VPC Guide de l'utilisateur.

## Journaux CloudTrail

Vous pouvez utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels effectués vers l'API de passerelle de transit et les stocker sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser ces journaux CloudTrail afin de déterminer les appels qui ont été effectués, l'adresse IP source d'où provient les appels, qui les a effectué, quand ils ont été effectués, et ainsi de suite. Pour de plus amples informations, veuillez consulter [Journalisation des appels d'API pour votre passerelle de transit avec AWS CloudTrail](#).

## Événements CloudWatch utilisant Network Manager

Vous pouvez l'utiliser AWS Network Manager pour transférer des événements vers CloudWatch, puis les acheminer vers des fonctions ou des flux cibles. Network Manager génère des événements pour les changements de topologie, les mises à jour de routage et les mises à jour de statut, qui peuvent tous être utilisés pour vous avertir des modifications apportées à vos passerelles de transit. Pour plus d'informations, consultez la section [Surveillance de votre réseau](#)

[mondial avec CloudWatch Events](#) du Guide de l'utilisateur des passerelles de transit pour les réseaux mondiaux AWS.

## Métriques CloudWatch pour vos passerelles de transit

Amazon VPC publie des points de données vers Amazon CloudWatch pour vos passerelles de transit et leurs attachements. CloudWatch vous permet de récupérer des statistiques relatives à ces points de données sous la forme d'un ensemble classé de données en séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une alarme CloudWatch pour surveiller une métrique spécifiée et initier une action (par exemple, l'envoi d'une notification à une adresse e-mail) si la métrique sort de ce que vous considérez comme une plage acceptable.

Amazon VPC mesure et envoie ses métriques à CloudWatch par intervalles de 60 secondes.

Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon CloudWatch](#).

### Table des matières

- [Métriques de passerelle de transit](#)
- [Dimensions métriques pour les passerelles de transit](#)

## Métriques de passerelle de transit

L'espace de noms AWS/TransitGateway inclut les métriques suivantes.

Métrique	Description
BytesDropCountBlackhole	Nombre d'octets abandonnés en raison de la correspondance avec une route blackhole .
BytesDropCountNoRoute	Nombre d'octets abandonnés en raison de la non-correspondance avec une route.

Métrique	Description
BytesIn	Nombre d'octets reçus par la passerelle de transit.
BytesOut	Nombre d'octets envoyés depuis la passerelle de transit.
PacketsIn	Nombre de paquets reçus par la passerelle de transit.
PacketsOut	Nombre de paquets envoyés par la passerelle de transit.
PacketDropCountBlackhole	Nombre de paquets abandonnés à cause d'une correspondance avec une route blackhole .
PacketDropCountNoRoute	Nombre de paquets abandonnés à cause d'une non-correspondance avec une route.

## Métriques au niveau des attachements

Les métriques suivantes sont disponibles pour les attachements de passerelle de transit. Toutes les métriques d'attachements sont publiées sur le compte du propriétaire de la passerelle de transit. Les métriques d'attachements individuelles sont publiées sur le compte du propriétaire de l'attachement. Le propriétaire de l'attachement ne peut afficher que les métriques de son propre attachement. Pour plus d'informations sur les types d'attachement pris en charge, consultez [the section called “Attachements de ressources”](#).

Métrique	Description
BytesDropCountBlackhole	Nombre d'octets abandonnés en raison de la correspondance avec une route blackhole sur l'attachement de la passerelle de transit.
BytesDropCountNoRoute	Nombre d'octets abandonnés en raison de la non-correspondance avec une route sur l'attachement de la passerelle de transit.
BytesIn	Nombre d'octets reçus par la passerelle de transit à partir de l'attachement.
BytesOut	Nombre d'octets envoyés de la passerelle de transit vers l'attachement.

Métrique	Description
PacketsIn	Nombre de paquets reçus par la passerelle de transit à partir de l'attachement.
PacketsOut	Nombre de paquets envoyés par la passerelle de transit vers l'attachement.
PacketDropCountBlackhole	Nombre de paquets abandonnés à cause d'une correspondance avec une route blackhole sur l'attachement de la passerelle de transit.
PacketDropCountNoRoute	Nombre de paquets abandonnés en raison de l'absence de correspondance avec une route sur l'attachement de la passerelle de transit.

## Dimensions métriques pour les passerelles de transit

Pour filtrer les métriques de vos passerelles de transit, utilisez les dimensions suivantes.

Dimension	Description
TransitGateway	Filtre les données de métriques par la passerelle de transit.
TransitGatewayAttachment	Filtre les données de métriques par l'attachement de la passerelle de transit.

## Journalisation des appels d'API pour votre passerelle de transit avec AWS CloudTrail

AWS CloudTrail est un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS. CloudTrail capture tous les appels d'API de passerelle de transit sous forme d'événements. Les appels capturés incluent les appels depuis la AWS Management Console et les appels de code vers les opérations d'API de passerelle de transit. Si vous créez un journal de suivi, vous pouvez diffuser en continu les événements CloudTrail vers un compartiment Amazon S3, et

notamment les événements pour les passerelles de transit. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à l'API de la passerelle de transit, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres informations.

Pour de plus amples informations sur les API de passerelle de transit, veuillez consulter [Actions de passerelle de transit AWS](#) dans la Référence d'API Amazon EC2.

Pour plus d'informations sur CloudTrail, consultez le [AWS CloudTrailGuide de l'utilisateur](#).

## Informations sur la passerelle de transit dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Lorsqu'une activité se produit par le biais de l'API de passerelle de transit, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de services AWS dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter [Affichage des événements avec l'historique des événements CloudTrail](#).

Pour un enregistrement continu des événements dans votre compte AWS, notamment les événements de l'API de passerelle de transit, créez un journal d'activité. Un journal de suivi permet à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- [Présentation de la création d'un journal d'activité](#)
- [Intégrations et services pris en charge par CloudTrail](#)
- [Configuration des Notifications de Amazon SNS pour CloudTrail](#)
- [Réception de fichiers journaux CloudTrail de plusieurs régions](#) et [Réception de fichiers journaux CloudTrail de plusieurs comptes](#)

Tous les appels vers les actions de passerelle de transit sont journalisés par CloudTrail. Par exemple, les appels vers l'action `CreateTransitGateway` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour de plus amples informations, consultez [l'élément `userIdentity` CloudTrail](#).

## Description des entrées des fichiers journaux d'une passerelle de transit

Un journal de suivi est une configuration qui permet la livraison d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Les fichiers journaux incluent les événements relatifs à tous les appels d'API pour votre compte AWS, pas uniquement aux appels d'API de passerelle de transit. Vous pouvez trouver les appels vers l'API de passerelle de transit en recherchant les éléments `eventSource` avec la valeur `ec2.amazonaws.com`. Pour afficher l'enregistrement d'une action spécifique, par exemple `CreateTransitGateway`, recherchez des éléments `eventName` avec le nom de l'action.

Voici des exemples d'enregistrements de journaux CloudTrail pour l'API de passerelle de transit en ce qui concerne un utilisateur qui a créé une passerelle de transit à l'aide de la console. Vous pouvez identifier la console à l'aide des éléments `userAgent`. Vous pouvez identifier l'appel d'API demandé à l'aide des éléments `eventName`. Il est possible de trouver des informations sur l'utilisateur (Alice) dans l'élément `userIdentity`.

Exemple Exemple : `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"
}
```

# Identity and Access Management pour vos passerelles de transit

AWS utilise les informations d'identification de sécurité pour identifier et vous accorder l'accès à vos ressources AWS. Vous pouvez utiliser les fonctions de AWS Identity and Access Management (IAM) pour permettre à d'autres utilisateurs, services et applications d'utiliser vos ressources AWS pleinement ou de façon limitée, sans partager vos autorisations de sécurité.

Par défaut, les utilisateurs IAM ne sont pas autorisés à créer, afficher ou modifier les ressources AWS. Pour permettre à un utilisateur d'accéder aux ressources, par exemple une passerelle de transit, et d'exécuter des tâches, vous devez créer une politique IAM qui accorde à l'utilisateur l'autorisation d'utiliser les ressources spécifiques et les actions d'API dont il a besoin, puis d'attacher la politique au groupe auquel cet utilisateur appartient. Quand vous attachez une stratégie à un utilisateur ou à un groupe d'utilisateurs, elle accorde ou refuse aux utilisateurs l'autorisation d'exécuter les tâches spécifiées sur les ressources spécifiées.

Pour travailler avec une passerelle de transit, l'une des stratégies gérées par AWS suivantes peut répondre à vos besoins :

- [AmazonEC2FullAccess](#)
- [AmazonEC2ReadOnlyAccess](#)
- [PowerUserAccess](#)
- [ReadOnlyAccess](#)

## Exemples de stratégies pour gérer des passerelles de transit

Voici des exemples de stratégies IAM pour l'utilisation des passerelles de transit.

Créer une passerelle de transit avec les balises requises

L'exemple suivant permet aux utilisateurs de créer une passerelle de transit. La clé de condition `aws:RequestTag` oblige les utilisateurs à baliser la passerelle de transit avec la balise `stack=prod`. La clé de condition `aws:TagKeys` utilise le modificateur `ForAllValues` pour indiquer que seule la clé `stack` est autorisée dans la demande. Aucune autre balise ne peut être spécifiée. Si les utilisateurs n'utilisent pas cette balise spécifique lorsqu'ils créent la passerelle de transit, ou s'ils ne spécifient aucune balise, la demande échoue.

La deuxième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le contexte de `CreateTransitGateway`.

```
{
  "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"
        }
      }
    }
  ]
}
```

## Utilisation des tables de routage de passerelle de transit

L'exemple suivant permet aux utilisateurs de créer et de supprimer des tables de routage de passerelle de transit pour une seule passerelle de transit uniquement (`tgw-11223344556677889`). Les utilisateurs peuvent également créer et remplacer des routes dans n'importe quelle table

de routage de passerelle de transit, mais uniquement pour les attachements qui ont la balise `network=new-york-office`.

```
{
  "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/*"
    }
  ]
}
```

## Exemples de politiques pour gérer AWS Network Manager

Pour des exemples de politiques, voir [Exemples de politiques pour gérer Network Manager](#) dans le Guide de l'utilisateur AWS Global Networks pour les passerelles de transit.

## Utilisation de rôles liés à un service pour vos passerelles de transit

Amazon VPC utilise des rôles liés à un service pour les autorisations requises pour appeler d'autres services AWS en votre nom. Pour de plus amples informations, veuillez consulter [Utilisation des rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

### Rôle lié à un service de passerelle de transit

Amazon VPC utilise des rôles liés à un service pour les autorisations nécessaires pour appeler d'autres services AWS en votre nom lorsque vous utilisez une passerelle de transit.

### Autorisations accordées par le rôle lié à un service

Amazon VPC utilise le rôle lié à un service nommé `AWSServiceRoleForVPCTransitGateway` pour appeler les actions suivantes en votre nom lorsque vous utilisez une passerelle de transit :

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

Le rôle `AWSServiceRoleForVPCTransitGateway` approuve les services suivants pour endosser le rôle :

- `transitgateway.amazonaws.com`

`AWSServiceRoleForVPCTransitGateway` utilise la politique gérée [AWSVPCTransitGatewayServiceRolePolicy](#).

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

## Création du rôle lié à un service

Vous n'avez pas besoin de créer manuellement le rôle `AWSServiceRoleForVPCTransitGateway`. Amazon VPC crée ce rôle pour vous lorsque vous associez un VPC dans votre compte à une passerelle de transit.

Pour qu' Amazon VPC crée un rôle lié à un service à votre place, vous devez avoir les autorisations nécessaires. Pour de plus amples informations, veuillez consulter [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

## Modification du rôle lié à un service

Vous pouvez modifier la description de `AWSServiceRoleForVPCTransitGateway` à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le IAM Guide de l'utilisateur.

## Suppression du rôle lié à un service

Si vous n'avez plus besoin d'utiliser des passerelles de transit, nous vous recommandons de supprimer `AWSServiceRoleForVPCTransitGateway`.

Vous pouvez supprimer ce rôle lié à un service après avoir supprimé tous les attachements de VPC de passerelle de transit de votre compte AWS. Ainsi, vous ne pouvez pas involontairement supprimer l'autorisation d'accéder à vos attachements de VPC.

Vous pouvez utiliser la console IAM, l'IAM CLI ou l'IAM API pour supprimer les rôles liés aux services. Pour de plus amples informations, veuillez consulter [Suppression d'un rôle lié à un service](#) dans le IAM Guide de l'utilisateur.

Après avoir supprimé `AWSServiceRoleForVPCTransitGateway`, Amazon VPC crée de nouveau le rôle si vous attachez un VPC de votre compte à une passerelle de transit.

## Politiques gérées par AWS pour les passerelles de transit

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas

d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

Pour travailler avec une passerelle de transit, l'une des stratégies gérées par AWS suivantes peut répondre à vos besoins :

- [AmazonEC2FullAccess](#)
- [AmazonEC2ReadOnlyAccess](#)
- [PowerUserAccess](#)
- [ReadOnlyAccess](#)

## Politique gérée par AWS : AWSVPCTransitGatewayServiceRolePolicy

Cette politique est attachée au rôle [AWSServiceRoleForVPCTransitGateway](#). Cela permet à Amazon VPC de créer et de gérer des ressources pour les attachements de votre passerelle de transit.

Pour afficher les autorisations de cette politique, consultez [AWSVPCTransitGatewayServiceRolePolicy](#) dans le Guide de référence des politiques gérées par AWS.

## Mises à jour des politiques gérées par AWS pour les passerelles de transit

Affiche des détails sur les mises à jour de politiques gérées par AWS pour les passerelles de transit depuis qu'Amazon VPC a commencé à suivre ces modifications en mars 2021.

Modification	Description	Date
Amazon VPC a commencé à assurer le suivi des modifications	Amazon VPC a commencé à suivre les modifications apportées à ses politiques gérées par AWS.	1er mars 2021

## Fonctionnement des ACL (listes de contrôle d'accès) réseau avec les passerelles de transit

Une liste de contrôle d'accès réseau (NACL) est une couche de sécurité facultative.

Les règles de liste de contrôle d'accès réseau (NACL) sont appliquées différemment, selon le scénario :

- [the section called “Même sous-réseau pour les instances EC2 et l'association de la passerelle de transit”](#)
- [the section called “Sous-réseaux différents pour les instances EC2 et l'association de la passerelle de transit”](#)

### Même sous-réseau pour les instances EC2 et l'association de la passerelle de transit

Imaginez une configuration dans laquelle vous disposez d'instances EC2 et d'une association de passerelle de transit dans le même sous-réseau. La même ACL réseau est utilisée pour le trafic des instances EC2 à la passerelle de transit et pour le trafic de la passerelle de transit aux instances.

Les règles NACL sont appliquées comme suit pour le trafic des instances à la passerelle de transit :

- Les règles sortantes utilisent l'adresse IP de destination pour l'évaluation.
- Les règles entrantes utilisent l'adresse IP source pour l'évaluation.

Les règles NACL sont appliquées de la manière suivante pour le trafic de la passerelle de transit aux instances :

- Les règles sortantes ne sont pas évaluées.

- Les règles entrantes ne sont pas évaluées.

## Sous-réseaux différents pour les instances EC2 et l'association de la passerelle de transit

Pensez à une configuration dans laquelle vous avez des instances EC2 dans un sous-réseau et une association de passerelle de transit dans un sous-réseau différent et chaque sous-réseau est associé à une ACL réseau différente.

Les règles ACL réseau sont appliquées comme suit pour le sous-réseau de l'instance EC2 :

- Les règles sortantes utilisent l'adresse IP de destination pour évaluer le trafic des instances à la passerelle de transit.
- Les règles entrantes utilisent l'adresse IP de destination pour évaluer le trafic de la passerelle de transit aux instances.

Les règles NACL sont appliquées comme suit pour le sous-réseau de la passerelle de transit :

- Les règles sortantes utilisent l'adresse IP de destination pour évaluer le trafic de la passerelle de transit aux instances.
- Les règles sortantes ne sont pas utilisées pour évaluer le trafic des instances à la passerelle de transit.
- Les règles entrantes utilisent l'adresse IP source pour évaluer le trafic des instances à la passerelle de transit.
- Les règles entrantes ne sont pas utilisées pour évaluer le trafic de la passerelle de transit aux instances.

## Bonnes pratiques

Utilisez un sous-réseau distinct pour chaque attachement de VPC de passerelle de transit. Pour chaque sous-réseau, utilisez un petit CIDR, par exemple /28, afin d'avoir plus d'adresses pour les ressources EC2. Lorsque vous utilisez un sous-réseau distinct, vous pouvez configurer les éléments suivants :

- Gardez ouverte l'ACL réseau entrante et sortante associée aux sous-réseaux de la passerelle de transit.

- En fonction de votre flux de trafic, vous pouvez appliquer des listes ACL réseau à vos sous-réseaux de charge de travail.

Pour plus d'informations sur la façon dont les pièces jointes de VPC fonctionnent, consultez [the section called “Attachements de ressources”](#).

# Quotas pour vos passerelles de transit

Vous Compte AWS disposez des quotas suivants (précédemment appelés limites) relatifs aux passerelles de transit. Sauf indication contraire, chaque quota est spécifique à la région.

La console Service Quotas fournit des informations sur les quotas de votre compte. Vous pouvez utiliser la console Service Quotas pour afficher les quotas par défaut et [demander des augmentations de quota](#) pour les quotas ajustables. Pour de plus amples informations, veuillez consulter [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Si un quota ajustable n'est pas encore disponible dans les Service Quotas, vous pouvez ouvrir une demande de support.

## Général

Nom	Par défaut	Ajustable
Passerelles Transit Gateway par compte	5	<a href="#">Oui</a>
Blocs d'adresses CIDR par passerelle Transit Gateway	5	Non

Les blocs d'adresse CIDR sont utilisés dans la fonction [the section called “Attachements Connect et pairs Connect”](#).

## Routage

Nom	Par défaut	Ajustable
Tables de routage Transit Gateway par passerelle Transit Gateway	20	<a href="#">Oui</a>
Nombre total d'acheminements combinés (dynamiques et statiques) sur toutes les tables de routage pour une passerelle de transit unique	10 000	<a href="#">Oui</a>

Nom	Par défaut	Ajustable
Routes dynamiques publiées depuis un dispositif de routeur virtuel vers un pair Connect	1 000	Oui
Routes publiées depuis un pair Connect sur une passerelle de transit vers un dispositif de routeur virtuel	5 000	Non
Acheminements statiques pour un préfixe à un seul attachement	1	Non

Les routes publiées proviennent de la table de routage associée à l'attachement Connect.

## Attachements de passerelle de transit

Une passerelle de transit ne peut pas avoir plus d'une pièce jointe de VPC au même VPC.

Nom	Par défaut	Ajustable
Attachements par passerelle Transit Gateway	5 000	Non
Passerelles Transit Gateway par VPC	5	Non
Attachements d'appairage par passerelle Transit Gateway	50	<a href="#">Oui</a>
Attachements d'appairage en attente par passerelle Transit Gateway	10	<a href="#">Oui</a>
Peering des pièces jointes entre deux passerelles de transit ou entre une passerelle de transit et un réseau central périphérique (CNE) Cloud WAN	1	Non
Pairs Connect (tunnels GRE) par attachement Connect	4	Non

## Bande passante

De nombreux facteurs peuvent affecter la bande passante réalisée via une connexion Site-to-Site VPN, y compris, sans s'y limiter, la taille des paquets, le mélange de trafic (TCP/UDP), les politiques de mise en forme ou de limitation sur les réseaux intermédiaires, la météo Internet et les exigences spécifiques des applications. Pour les attachements VPC, passerelles AWS Direct Connect ou attachements de la passerelle de transit paire, nous essaierons de fournir une bande passante supplémentaire au-delà de la valeur par défaut.

Nom	Par défaut	Ajustable
Bande passante par attachement VPC par zone de disponibilité	Jusqu'à 100 Gbit/s	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Paquets par seconde par passerelle de transit, attachement VPC par zone de disponibilité	Jusqu'à 7 500 000	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Bande passante pour la connexion à une AWS Direct Connect passerelle ou à une passerelle de transit pair par zone de disponibilité disponible dans la région	Jusqu'à 100 Gbit/s	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre

Nom	Par défaut	Ajustable
		responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Paquets par seconde par pièce jointe à une passerelle de transit (AWS Direct Connect et pièces jointes de peering) par zone de disponibilité disponible dans la région	Jusqu'à 7 500 000	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Bande passante maximale par tunnel VPN	Jusqu'à 1,25 Gbit/s	Non
Nombre maximal de paquets par seconde (PPS) par tunnel VPN	Jusqu'à 140 000	Non
Bande passante maximale par pair Connect (tunnel GRE) par attachement Connect	Jusqu'à 5 Gbit/s	Non
Nombre maximal de paquets par seconde par pair Connect	Jusqu'à 300 000	Non

Vous pouvez utiliser un routage ECMP (Equal Cost Multipath) pour obtenir une bande passante VPN plus importante en agrégeant plusieurs tunnels VPN. Pour utiliser l'ECMP, la connexion VPN doit être configurée pour le routage dynamique. L'ECMP n'est pas pris en charge sur les connexions VPN qui utilisent le routage statique.

Vous pouvez créer jusqu'à 4 homologues Connect par pièce jointe Connect (jusqu'à 20 Gbit/s de bande passante totale par pièce jointe Connect), à condition que l'attachement de transport sous-

jacent (VPC AWS Direct Connect ou) supporte la bande passante requise. Vous pouvez utiliser ECMP pour obtenir une bande passante plus importante en mettant à l'échelle horizontalement les divers pairs Connect d'un même attachement Connect ou les divers attachements Connect d'une même passerelle de transit. La passerelle de transit ne peut pas utiliser ECMP entre les pairs BGP d'un même pair Connect.

## AWS Direct Connect passerelles

Nom	Par défaut	Ajustable
AWS Direct Connect passerelles par passerelle de transit	20	Non
Passerelles de transit par AWS Direct Connect passerelle	6	Non

## Unité de transmission maximale (MTU)

- La MTU d'une connexion réseau est la taille, en octets, du plus gros paquet autorisé pouvant être transmis via la connexion. Plus la MTU d'une connexion est élevée, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Une passerelle de transit prend en charge une MTU de 8 500 octets pour le trafic entre les VPC, Transit AWS Direct Connect Gateway Connect et les pièces jointes de peering. Le trafic sur les connexions VPN peut avoir une MTU de 1 500 octets.
- Lors de la migration de l'appairage de VPC pour utiliser une passerelle de transit, un décalage de taille MTU entre l'appairage de VPC et la passerelle de transit peut entraîner la chute de certains paquets de trafic asymétriques. Mettez à jour les deux VPC en même temps pour éviter la chute des paquets jumbo en raison d'un décalage de taille.
- Les paquets d'une taille supérieure à 8 500 octets qui arrivent à la passerelle de transit sont abandonnés.
- La passerelle de transit ne génère pas le paquet FRAG\_NEEDED pour ICMPv4, ni le paquet Packet Too Big (PTB) pour ICMPv6. Par conséquent, la détection de la MTU du chemin (PMTUD) n'est pas prise en charge.
- La passerelle de transit applique la restriction MSS (Maximum Segment Size - taille maximum du segment) pour tous les paquets. Pour de plus amples informations, veuillez consulter [RFC879](#).

- Pour plus de détails sur les quotas Site-to-Site VPN pour l'unité de transmission maximale (MTU), veuillez consulter [Unité de transmission maximale \(MTU\)](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN (français non garanti).

## Multicast

Nom	Par défaut	Ajustable
Domaines multicast par passerelle de transit	20	<a href="#">Oui</a>
Interfaces de réseau de multicast par passerelle de Transit Gateway	10 000	<a href="#">Oui</a>
Associations de domaines multicast par VPC	20	<a href="#">Oui</a>
Sources par groupe multicast de passerelle de transit	1	<a href="#">Oui</a>
Membres et sources d'un groupe multicast statique et d'un groupe multicast IGMPv2 par passerelle de transit	10 000	Non
Membres d'un groupe multicast statique et d'un groupe multicast IGMPv2 par groupe multicast de passerelle de transit	100	Non
Débit multicast maximal par flux	1 Gbit/s	Non
Débit multicast cumulé maximal par zone de disponibilité	20 Gbit/s	Non

## AWS Directeur du réseau

Nom	Par défaut	Ajustable
Réseaux mondiaux par Compte AWS	5	Oui

Nom	Par défaut	Ajustable
Appareils par réseau mondial	200	Oui
Liens par réseau mondial	200	Oui
Sites par réseau mondial	200	Oui
Connexions par réseau mondial	500	Non

## Ressources de quotas supplémentaires

Pour de plus amples informations, consultez les ressources suivantes :

- [Quotas de Site-to-Site VPN](#) dans le Guide de l'utilisateur AWS Site-to-Site VPN
- [Quotas Amazon VPC](#) dans le Guide de l'utilisateur Amazon VPC
- [AWS Direct Connect quotas](#) dans le Guide de l'utilisateur AWS Direct Connect

# Historique du document pour les passerelles de transit

Le tableau suivant décrit les mises à jour des passerelles de transit.

Modification	Description	Date
<a href="#">Quotas de passerelle de transitAWS</a>	Des limites de bande passante ont été ajoutées.	14 août 2023
<a href="#">AWS Transit Gateway Flow Logs</a>	Les passerelles de transit prennent désormais en charge Transit Gateway Flow Logs, qui vous permet de surveiller et de journaliser le trafic réseau entre les passerelles.	14 juillet 2022
<a href="#">Tables de stratégie de passerelle de transit</a>	Utilisez des tables de stratégie afin de configurer un routage dynamique pour les passerelles de transit et d'échanger automatiquement des informations de routage et d'accessibilité avec des types de passerelles de transit appairés.	13 juillet 2022
<a href="#">Guide de l'utilisateur Network Manager</a>	Network Manager a été créé en tant que guide autonome et n'est plus inclus dans le AWSGuide de l'utilisateur Transit Gateway.	2 décembre 2021
<a href="#">Attachement d'appairage</a>	Vous pouvez créer une connexion d'appairage avec une passerelle de transit dans la même région.	1 décembre 2021

<a href="#">Transit Gateway Connect</a>	Vous pouvez établir une connexion entre une passerelle de transit et des appliances virtuelles tierces exécutées dans un VPC.	10 décembre 2020
<a href="#">Mode Appliance</a>	Vous pouvez activer le mode appliance sur une pièce jointe d'un VPC pour garantir que le trafic bidirectionnel circule dans la même zone de disponibilité pour la pièce jointe.	29 octobre 2020
<a href="#">Références des listes de préfixes</a>	Vous pouvez référencer une liste de préfixes dans votre table de routage de passerelle de transit.	24 août 2020
<a href="#">Modifier la passerelle de transit</a>	Vous pouvez modifier les options de configuration de votre passerelle de transit.	24 août 2020
<a href="#">Métriques CloudWatch pour les réseaux de transit par passerelle.</a>	Vous pouvez afficher les métriques CloudWatch pour les réseaux de transit par passerelle individuels.	6 juillet 2020
<a href="#">Analyseur de routes Network Manager</a>	Vous pouvez analyser les itinéraires de vos tables de routage de passerelle de transit dans votre réseau global.	4 mai 2020
<a href="#">Attachement d'appairage</a>	Vous pouvez créer une connexion d'appairage avec une passerelle de transit dans une autre région.	3 décembre 2019

---

<a href="#">Prise en charge de la multicast</a>	La passerelle de transit prend en charge le routage du trafic de multicast entre les sous-réseaux de VPC attachés et sert de routeur de multicast aux instances qui envoient le trafic destiné à plusieurs instances de réception.	3 décembre 2019
<a href="#">AWS Network Manager</a>	Vous pouvez visualiser et surveiller vos réseaux mondiaux construits autour des passerelles de transit.	3 décembre 2019
<a href="#">AWS Direct Connect Prise en charge de</a>	Vous pouvez utiliser une passerelle AWS Direct Connect pour connecter votre connexion AWS Direct Connect via une interface de transit virtuelle aux VPC ou VPN attachés à votre passerelle de transit.	27 mars 2019
<a href="#">Première version</a>	Cette version présente les passerelles de transit.	26 novembre 2018

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.