AWS Transit Gateway

Amazon VPC

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon VPC: AWS Transit Gateway

Copyright © 2025 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'Amazon VPC Transit Gateways ? ... 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
Exemple de schéma 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
Pièces jointes aux fonctions réseau ... 13
AWS Network Firewall intégration ... 13
Exemples de scénarios de passerelle de transit ... 14
Commencez avec les passerelles de transport en commun ... 38
Création d'une passerelle de transit à l'aide de la console ... 38
Prérequis ... 38
Étape 1 : Création de la passerelle de transit ... 39
Étape 2 : Attachez votre véhicule VPCs à votre passerelle de transport en commun ... 41
Étape 3 : Ajoutez des itinéraires entre la passerelle de transport en commun et votre VPCs ... 42
Étape 4 : Tester la passerelle de transit ... 42
Étape 5 : Supprimer la passerelle de transit ... 42
Création d'une passerelle de transit à l'aide de la ligne de commande ... 43
Prérequis ... 43
Étape 1 : Création de la passerelle de transit ... 44
Étape 2 : vérifier l'état de disponibilité de la passerelle de transit ... 45
Étape 3 : Attachez votre véhicule VPCs à votre passerelle de transport en commun ... 47
Étape 4 : Vérifiez que les pièces jointes de la passerelle de transit sont disponibles ... 48

Étape 5 : Ajoutez des itinéraires entre votre passerelle de transport en commun et VPCs 50
Étape 6 : Testez la passerelle de transit 51
Étape 7 : Supprimer les pièces jointes de la passerelle de transit et la passerelle de transit ... 51
Conclusion 54
Bonnes pratiques de conception 55
Utiliser des passerelles de transit 57
Passerelles de transport en commun partagées 57
Partager vos passerelles de transit 57
Annuler le partage d'une passerelle de transit 59
Sous-réseaux partagés 59
Passerelles de transit 60
Créer une passerelle de transit 61
Afficher une passerelle de transit 63
Ajouter ou modifier des balises de passerelle de transit 64
Modifier une passerelle de transit 64
Accepter un partage de ressources 65
Accepter un attachement partagé 66
Supprimer une passerelle de transit 66
Attachements VPC 67
Cycle de vie des attachements VPC 68
Mode Appliance 70
Référencement des groupes de sécurité 72
Création d'une pièce jointe VPC 73
Modifier une pièce jointe VPC 74
Modifier les balises de pièce jointe VPC 75
Afficher une pièce jointe VPC 76
Supprimer un attachement de VPC 76
Mettre à jour les règles entrantes des groupes de sécurité 77
Identifier les groupes de sécurité référencés 78
Supprimer les règles de groupe de sécurité obsolètes 78
Résoudre les problèmes liés aux attachements VPC 79
Accessoires pour fonctions réseau 80
Accepter ou rejeter une pièce jointe à une fonction réseau de passerelle de transit 80
Afficher les pièces jointes aux fonctions réseau 81
Acheminer le trafic via une passerelle de transit (fonction attachée) 82
Attachements VPN 84

Créer un attachement de passerelle de transit avec un VPN ... 85
Afficher une pièce jointe VPN ... 86
Supprimer un attachement VPN ... 86
Attachements d'une passerelle de transit à une passerelle Direct Connect ... 87
Attachement d'appairage ... 88
Considérations relatives à la AWS région d'inscription ... 89
Créer un attachement d'appairage ... 90
Accepter ou rejeter une demande de peering ... 91
Ajouter un itinéraire à une table de routage d'une passerelle de transit ... 92
Supprimer un attachement d'appairage ... 92
Attachements Connect et pairs Connect ... 93
Connecter les pairs ... 94
Exigences et considérations ... 97
Création d'un attachement Connect ... 98
Création d'un pair Connect ... 99
Afficher les pièces jointes Connect et Connect les pairs ... 100
Modifier la pièce jointe Connect et les balises Connect peer ... 101
Supprimer un pair Connect ... 102
Suppression d'un attachement Connect ... 102
Tables de routage de passerelle de transit ... 103
Créer une table de routage de passerelle de transit ... 104
Afficher les tables de routage de passerelle de transit ... 104
Associer une table de routage de passerelle de transit ... 105
Dissocier une table de routage d'une passerelle de transit ... 106
Activer la propagation des itinéraires ... 106
Désactivation de la propagation du routage ... 107
Créer un itinéraire statique ... 107
Supprimer un routage statique ... 108
Remplacez une route statique ... 109
Exportation des tables de routage vers Amazon S3 ... 109
Supprimer une table de routage de passerelle de transit ... 111
Créer une référence de liste de préfixes ... 111
Modifier une référence de liste de préfixes ... 112
Supprimer une référence de liste de préfixes ... 113
Tables de stratégie de passerelle de transit ... 114
Créer une table de stratégie de passerelle de transit ... 115

Supprimer une table de stratégie de passerelle de transit 115
Multicast sur les passerelles de transit 116
Concepts du multicast 1
Considérations 117
Routage multicast 119
Domaines de multidiffusion 121
Domaines de multidiffusion partagés 127
Enregistrer les sources avec un groupe de multidiffusion 133
Inscrire des membres auprès d'un groupe de multidiffusion 134
Annuler l'inscription des sources à un groupe de multidiffusion 134
Annuler l'inscription des membres à un groupe de multidiffusion 135
Afficher les groupes de multidiffusion 135
Configuration de la multidiffusion pour Windows Server 136
Exemple : gestion des configurations IGMP 137
Exemple : gestion des configurations de sources statiques 138
Exemple : gestion des configurations de membres de groupes statiques 140
Transit Gateway Flow Logs 141
Limites 142
Enregistrements Transit Gateway Flow Logs 142
Format par défaut 143
Format personnalisé 143
Champs disponibles 143
Contrôler l'utilisation des journaux de flux 149
Tarification Transit Gateway Flow Logs 150
Création ou mise à jour d'un rôle IAM dans le journal des flux 150
CloudWatch Journaux 151
Rôles IAM pour publier des journaux de flux dans Logs CloudWatch 152
Autorisations pour les utilisateurs IAM pour transmettre un rôle 153
Créez un journal de flux qui publie dans CloudWatch Logs 154
Afficher les enregistrements des journaux de flux 155
Enregistrements du journal des flux de processus 156
Amazon S3 157
Fichiers journaux de flux 158
Politique IAM pour les principaux IAM qui publient des journaux de flux vers Amazon S3 160
Autorisations du compartiment Amazon S3 pour les journaux de flux 161
Politique de clé obligatoire à utiliser avec SSE-KMS 163

Autorisations pour les fichiers journaux Amazon S3 164
Création du rôle du compte source 164
Créer un journal de flux qui publie vers Amazon S3 165
Afficher les enregistrements des journaux de flux 167
Enregistrements du journal de flux traités dans Amazon S3 167
Journaux de flux Amazon Data Firehose 168
Rôles IAM pour la diffusion entre comptes 168
Création du rôle du compte source 171
Création du rôle du compte de destination 172
Créez un journal de flux qui publie sur Firehose 173
Création et gestion des journaux de flux à l'aide de la CLI APIs or 175
Afficher les journaux de flux 176
Gérer les balises du journal de flux 176
Rechercher des enregistrements de journaux de flux 177
Supprimer un enregistrement du journal de flux 179
Métriques et événements 180
CloudWatch métriques 181
Métriques de passerelle de transit 181
Mesures relatives au niveau de la pièce jointe et à la zone de disponibilité 183
Dimensions métriques de la passerelle de transit 184
CloudTrail journaux 185
Événements de gestion 187
Exemples d'événements 187
Gestion des identités et des accès 190
Exemples de stratégies pour gérer des passerelles de transit 190
Rôles liés à un service 193
Passerelle de transit 193
AWS politiques gérées 194
AWSVPCTransitGatewayServiceRolePolicy 195
Mises à jour des politiques 195
Réseau ACLs 196
Même sous-réseau pour les EC2 instances et l'association des passerelles de transit 196
Différents sous-réseaux pour les EC2 instances et l'association des passerelles de transit .. 197
Bonnes pratiques 197
Quotas 199
Général 199

Routage 199
Attachements de passerelle de transit 200
Bande passante 201
AWS Direct Connect passerelles 203
Unité de transmission maximale (MTU) 203
Multicast 204
Gestionnaire de réseau 205
Ressources de quotas supplémentaires 205
Historique du document 206
..... ccx

Qu'est-ce qu'Amazon VPC Transit Gateways ?

Amazon VPC Transit Gateways est un hub de transit réseau utilisé pour interconnecter des clouds privés virtuels (VPCs) et des réseaux sur site. À mesure que votre infrastructure cloud s'étend à l'échelle mondiale, le peering interrégional connecte les passerelles de transport en commun à l'aide de l' AWS infrastructure mondiale. 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 VPCs
  - Une appliance réseau Connect SD-WAN/tiers
  - Une AWS Direct Connect passerelle
  - Une connexion d’appairage avec une autre passerelle de transit
  - Une connexion VPN à une passerelle de transit
  - Une pièce jointe à une fonction réseau. Pour de plus amples informations, veuillez consulter the section called “Pièces jointes aux fonctions réseau”.
- 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 VPCs Transit Gateway Connect et les pièces jointes de peering (pièces jointes intra-régionales, interrégionales et cloud WAN). AWS Direct Connect Le trafic sur les connexions VPN peut avoir une MTU de 1 500 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
- Commencez avec les passerelles de transport en commun
- 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.
- AWS Interface de ligne de commande (AWS CLI) : fournit des commandes pour un large éventail de AWS services, y compris Amazon VPC, et est prise en charge sous Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.
- AWS SDKs— Fournit des opérations d'API spécifiques au langage et prend en charge de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour de plus amples informations, veuillez consulter AWS SDKs.

- 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 le Amazon EC2 API Reference.

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.

Comment fonctionnent les passerelles Amazon VPC Transit

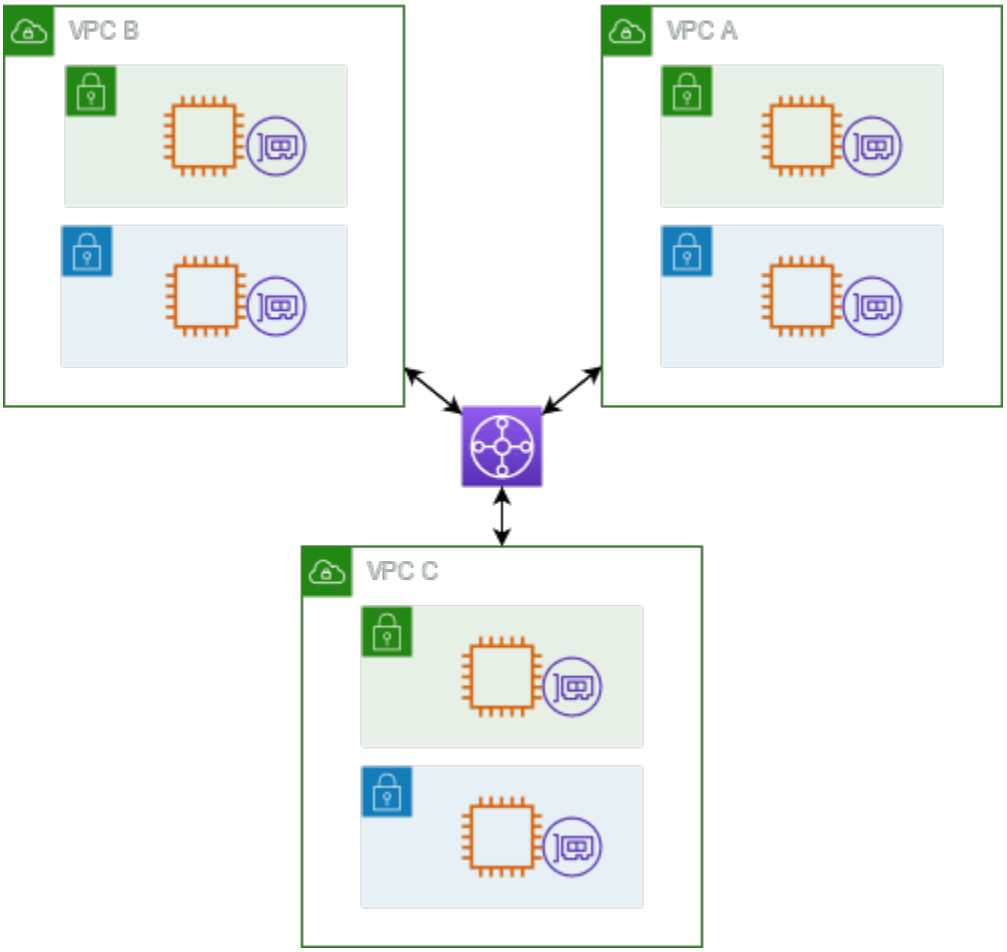
Dans AWS Transit Gateway, une passerelle de transit agit comme un routeur virtuel régional pour le trafic circulant entre vos clouds privés virtuels (VPCs) et les réseaux sur site. Une passerelle de transit dispose d'une scalabilité élastique en fonction du volume de trafic réseau. L'acheminement via 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.

Rubriques

- Exemple de schéma d'architecture
- Attachements de ressources
- Routage multivoies à coût égal
- Zones de disponibilité
- Routage
- Pièces jointes aux fonctions réseau
- Exemples de scénarios de passerelle de transit

Exemple de schéma d'architecture

Le diagramme suivant montre une passerelle de transit avec des trois attachements VPC. La table de routage pour chacune d'entre elles VPCs inclut l'itinéraire local et les itinéraires qui envoient le trafic destiné VPCs aux deux autres 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
VPC A CIDR	*Attachment for VPC A*	propagée
VPC B CIDR	*Attachment for VPC B*	propagée
VPC C CIDR	*Attachment for VPC C*	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 VPCs. 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 du'ne 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

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'est pas pris en charge. Vous ne pouvez donc pas utiliser l'ECMP sur différents numéros de système autonome (). ASNs
> - 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 de plus amples informations, veuillez consulter 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 Active/Active ou Active/Passive Direct Connect AWS 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 de plus amples informations, veuillez consulter Exemple : Appliance dans un VPC de services partagés.

Routage

Votre passerelle de transit achemine IPv4 et les IPv6 paquets entre les pièces jointes à l'aide des tables de routage de la passerelle de transit. Vous pouvez configurer ces tables de routage pour propager les itinéraires à partir des tables de routage pour les connexions VPN connectées et les passerelles Direct Connect. VPCs 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.

Rubriques relatives au routage

- 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. Si vous désactivez à la fois la propagation d'itinéraires et l'association de tables de routage, AWS cela ne crée pas de table de routage par défaut pour la passerelle de transit. Toutefois, si la propagation de routes ou l'association de tables de routage sont activées, AWS une table de routage par défaut est créée.

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 publiés 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 le réseau du client est annoncé. 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 toute 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 ayant le même CIDR, mais provenant de types de pièces jointes 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 par VPC

- Routes propagées par la passerelle Direct Connect
- Routes propagées par Transit Gateway Connect
- Site-to-Site VPN sur des routes privées propagées par Direct Connect
- Site-to-Site Routes propagées par VPN
- Routes propagées par le peering de Transit Gateway (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.
> - Pour les itinéraires annoncés vers une passerelle de transit sans MED, AWS Transit Gateway attribuera les valeurs par défaut suivantes :
>   - 0 pour les itinéraires entrants annoncés sur les pièces jointes Direct Connect.
>   - 100 pour les itinéraires entrants annoncés sur les pièces jointes VPN et Connect.

AWS Transit Gateway affiche uniquement un itinéraire préféré. Un itinéraire de sauvegarde n'apparaîtra dans le tableau des itinéraires de la passerelle de transit que si l'itinéraire précédemment actif n'est plus annoncé, par exemple, si vous annoncez les mêmes itinéraires via la passerelle Direct Connect et via Site-to-Site un VPN. 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, ne s'affiche que 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 à 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-connect-peer	Connexion	Propagé	4

Destination	Attachement (Cible)	Type de ressource	Type de routage	Priority
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagée	5

Pièces jointes aux fonctions réseau

Une pièce jointe à une fonction réseau est une ressource qui connecte une fonction de sécurité réseau, par exemple une AWS Network Firewall pièce jointe, directement à votre passerelle de transit. Il élimine le besoin de créer et de gérer manuellement l'inspection VPCs.

Avec un attachement à une fonction réseau :

- AWS crée et gère automatiquement l'infrastructure sous-jacente
- Le trafic peut être inspecté lorsqu'il passe par votre passerelle de transit
- Les politiques de sécurité sont appliquées de manière cohérente sur l'ensemble de votre réseau

- Vous pouvez diriger le trafic à travers le pare-feu à l'aide de règles de routage simples
- La pièce jointe fonctionne sur plusieurs zones de disponibilité pour une haute disponibilité

Cette intégration simplifie la sécurité du réseau en vous permettant d'associer des pare-feux directement à votre passerelle de transit plutôt que de créer des configurations de routage complexes et de gérer des points de terminaison distincts de manière séparée. VPCs

AWS Network Firewall intégration

AWS Network Firewall l'intégration vous permet de connecter un pare-feu sous la forme d'un groupe de points de terminaison Gateway Load Balancer, un par zone de disponibilité, dans un VPC tampon géré par des services. Une pièce jointe Network Firewall est créée avec le mode appliance automatiquement activé. Il n'est donc plus nécessaire de gérer explicitement l'inspection VPCs.

Grâce à l'intégration de Network Firewall, vous n'avez plus besoin de créer et de gérer l'inspection VPCs de vos déploiements de Network Firewall. Au lieu de sélectionner un VPC et des sous-réseaux lors de la création de votre pare-feu, vous sélectionnez directement le Transit Gateway, et vous approvisionnez et gérez AWS automatiquement toutes les ressources nécessaires en arrière-plan.

Vous verrez une nouvelle fonction réseau de passerelle de transit attachée au lieu d'un point de terminaison de pare-feu individuel.

Pour les scénarios entre comptes, le Transit Gateway peut être partagé en RAM entre le compte du propriétaire du Transit Gateway et le compte du propriétaire du Network Firewall, ce qui permet à l'un ou l'autre de ces comptes de gérer l'attachement au pare-feu. Une fois que votre pare-feu et votre pièce jointe sont prêts, vous pouvez simplement modifier vos tables de routage Transit Gateway pour envoyer le trafic vers la pièce jointe à des fins d'inspection.

> **Note**
>
> - Transit Gateway prend uniquement en charge le routage statique sur les pièces jointes du Network Firewall.
> - Les pare-feux tiers ne sont pas pris en charge.

Pour plus d'informations sur les pare-feux et les pièces jointes, consultez la section Pièces jointes aux fonctions réseau de la passerelle Transit.

Exemples de scénarios de passerelle 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.

Exemple : routeur centralisé

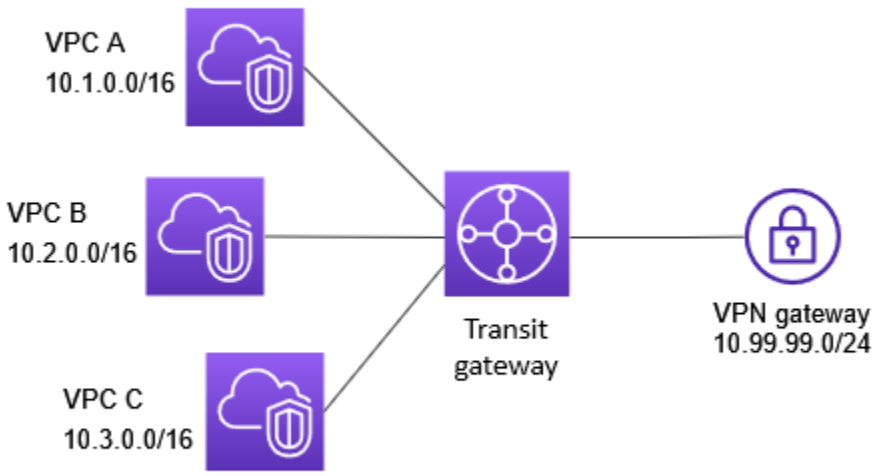
Vous pouvez configurer votre passerelle de transit en tant que routeur centralisé qui connecte toutes vos VPCs connexions et vos connexions Site-to-Site VPN. AWS Direct Connect Dans ce scénario, tous les attachements sont associés à la table de routage par défaut de la passerelle de transit et propagés 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 trois pièces jointes VPC et une pièce jointe 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 VPCs. Pour plus d'informations, consultez Créer 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 “Création d'une pièce jointe VPC”.
- Une pièce jointe 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 établie, la session BGP est établie et le CIDR Site-to-Site VPN se propage vers la table de routage de la passerelle de transit et les VPC CIDRs 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 est l'entrée par défaut pour le IPv4 routage local dans le VPC ; cette entrée permet aux instances de ce VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic de IPv4 sous-réseau 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	*Attachment for VPC A*	propagée
10.2.0.0/16	*Attachment for VPC B*	propagée
10.3.0.0/16	*Attachment for VPC C*	propagée

Destination	Target	Type de routage
10.99.99.0/24	*Attachment for VPN connection*	propagée

Table BGP de passerelle client

La table BGP de la passerelle client contient le VPC suivant. CIDRs

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

Exemple : isolé VPCs

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.

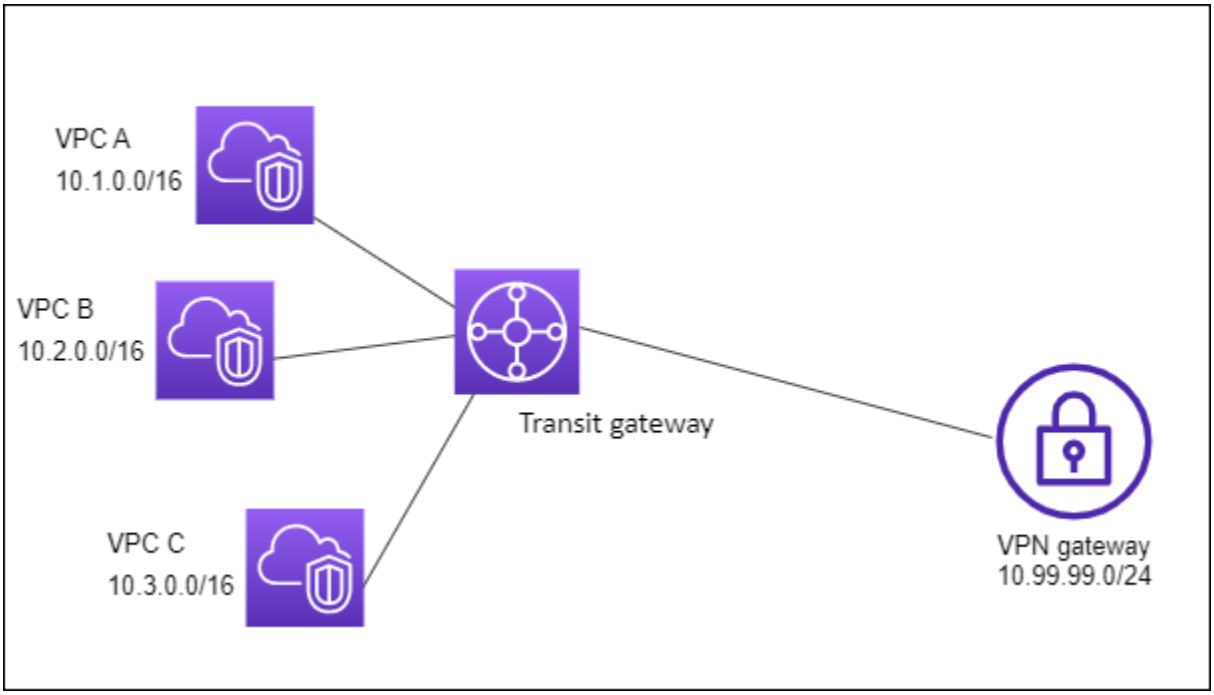
Table des matières

- 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 des VPC A, VPC B et VPC C dont la destination est Internet passent d'abord par la passerelle de transit, puis vers la connexion VPN (si Site-to-Site 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 VPCs. Pour plus d'informations, consultez Créer 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 pièces jointes sur la passerelle de transit pour les trois VPCs. Pour de plus amples informations, veuillez consulter the section called “Création d'une pièce jointe VPC”.
- Une pièce jointe 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 établie, la session BGP est établie et le CIDR VPN se propage vers la table de routage de la passerelle de transit et les VPC CIDRs sont ajoutés à la table BGP de la passerelle client.

Routage

Chaque VPC possède une table de routage et la passerelle de transit possède deux tables de routage, l'une pour la connexion VPN VPCs et l'autre 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 est l'entrée par défaut pour le IPv4 routage local dans le VPC. Cette entrée permet aux instances de ce VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic de IPv4 sous-réseau 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 la connexion VPN VPCs 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	*Attachment for VPN connection*	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

Destination	Target	Type de routage
10.1.0.0/16	*Attachment for VPC A*	propagée
10.2.0.0/16	*Attachment for VPC B*	propagée
10.3.0.0/16	*Attachment for VPC C*	propagée

Pour de plus amples informations sur la propagation de routes dans une table de routage de passerelle de transit, veuillez consulter Activez la propagation d'itinéraires vers une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways.

Table BGP de passerelle client

La table BGP de la passerelle client contient le VPC suivant. CIDRs

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

Exemple : isolé VPCs avec des 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.

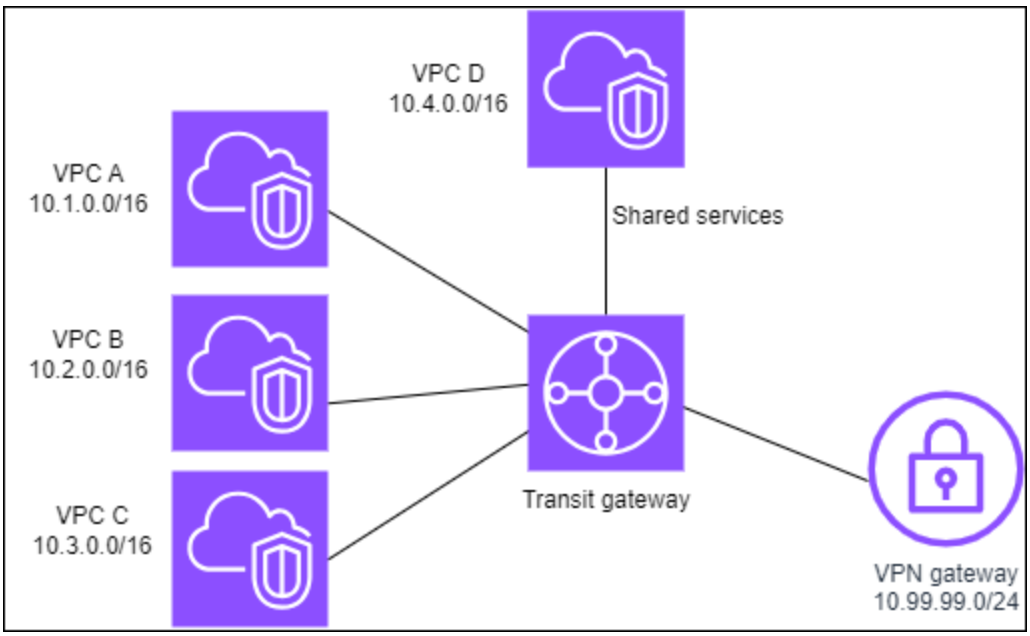
Table des matières

- Présentation
- Ressources

- Routage

Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Les paquets provenant des sous-réseaux des VPC A, VPC B et VPC C dont la destination est Internet passent d'abord par la passerelle de transit, puis vers la passerelle client pour le VPN. Site-to-Site 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 le 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 VPCs. Pour plus d'informations, consultez Créer 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 “Création d'une pièce jointe VPC”.

- Une pièce jointe 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 établie, la session BGP est établie et le CIDR VPN se propage vers la table de routage de la passerelle de transit et les VPC CIDRs 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 possède une table de routage, et la passerelle de transit possède deux tables de routage, l'une pour la connexion VPN VPCs et le VPC de 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 de IPv4 sous-réseau vers la passerelle de transit.

Destination	Cible
10.1.0.0/16	Locale
0.0.0.0/0	*transit gateway ID*

Tables de routage de passerelle de transit

Ce scénario utilise une table de routage pour la connexion VPN VPCs 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	*Attachment for VPN connection*	propagée
10.4.0.0/16	*Attachment for VPC D*	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 la communication VPCs entre la connexion VPN et le VPC de services partagés.

Destination	Target	Type de routage
10.1.0.0/16	*Attachment for VPC A*	propagée
10.2.0.0/16	*Attachment for VPC B*	propagée
10.3.0.0/16	*Attachment for VPC C*	propagée

Pour de plus amples informations, veuillez consulter Activez la propagation d'itinéraires vers une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways.

Table BGP de passerelle client

La table BGP de la passerelle client contient CIDRs les quatre VPCs.

Exemple : passerelles de transit appairées

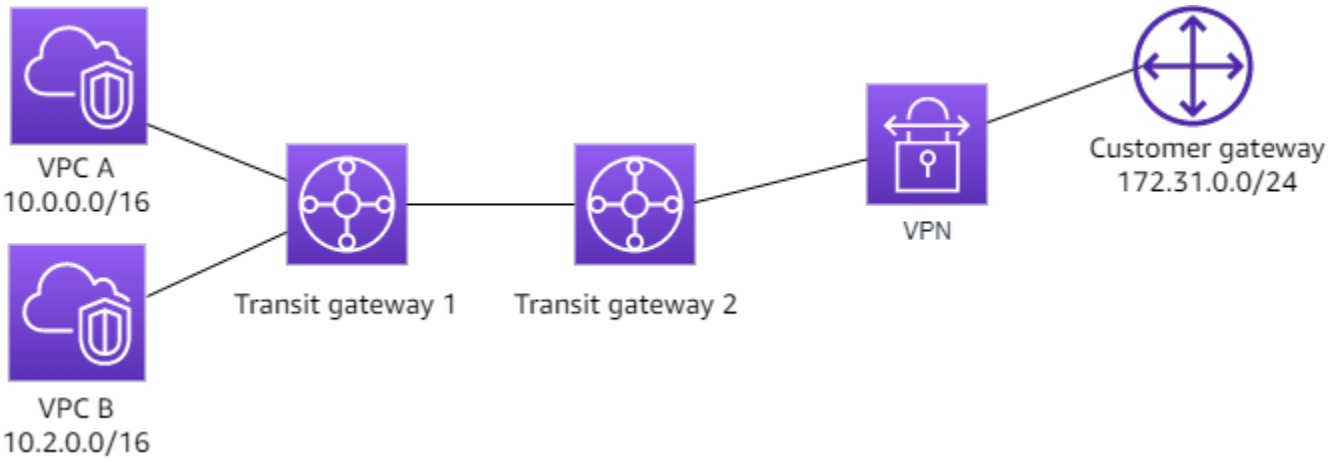
Vous pouvez créer une connexion d'appairage de passerelle de transit entre des passerelles de transit. Vous pouvez ensuite acheminer le trafic entre les attachements de chacune des passerelles de transit. Dans ce scénario, les attachements VPC et VPN sont associés aux tables de routage par défaut de 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 possède deux pièces jointes VPC et la passerelle de transit 2 possède une Site-to-Site connexion 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 VPCs. Pour plus d'informations, consultez Créer 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 “Création d'une pièce jointe VPC”.
- Une pièce jointe Site-to-Site VPN sur la deuxième 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 Pièces jointes de peering de passerelle de transit dans Amazon VPC Transit Gateways.

Lorsque vous créez les pièces jointes du VPC, celles de chaque VPC se propagent vers la CIDRs table de routage de 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 vers la table de routage de la passerelle de transit 2
- Les VPC CIDRs 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 est l'entrée par défaut pour le IPv4 routage local dans le VPC. Cette entrée par défaut permet aux ressources du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic de IPv4 sous-réseau 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	*Attachment ID for VPC A*	propagée
10.2.0.0/16	*Attachment ID for VPC B*	propagée
0.0.0.0/0	*Attachment ID for peering connection*	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	*Attachment ID for VPN connection*	propagée
10.0.0.0/16	*Attachment ID for peering connection*	statique
10.2.0.0/16	*Attachment ID for peering connection*	statique

Table BGP de passerelle client

La table BGP de la passerelle client contient le VPC suivant. CIDRs

- 10.0.0.0/16
- 10.2.0.0/16

Exemple : Routage sortant centralisé vers Internet

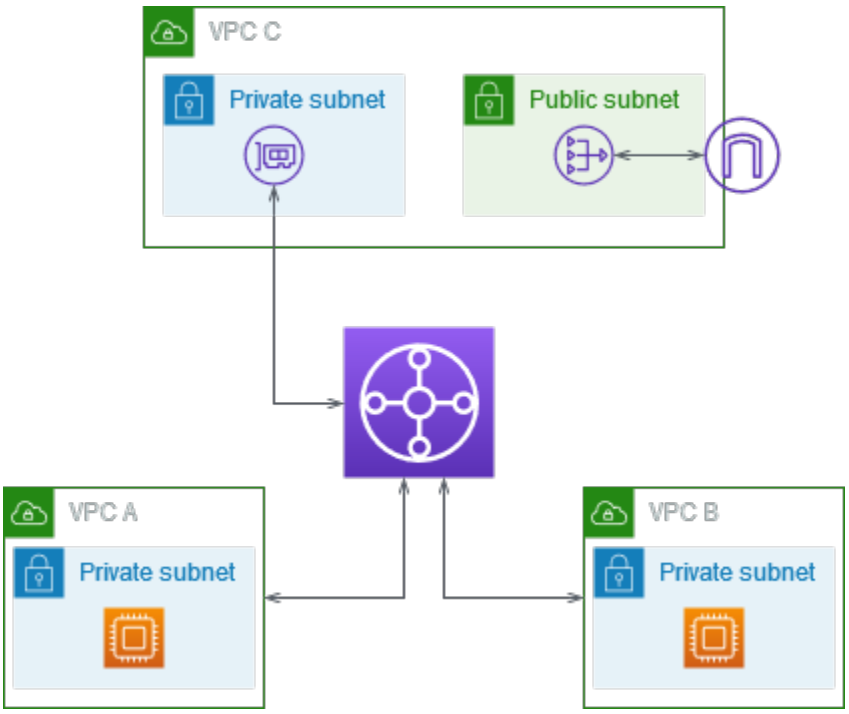
Vous pouvez configurer une passerelle de transit pour acheminer le trafic Internet sortant d'un VPC sans passerelle Internet vers un VPC qui contient une passerelle NAT et une passerelle Internet.

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 le tout VPCs à une passerelle de transport en commun. 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 VPCs avec des plages d'adresses IP qui ne sont ni identiques ni superposées. Pour plus d'informations, consultez Créer un VPC dans le Guide de l'utilisateur Amazon VPC.
- Le VPC A et le VPC B possèdent chacun des 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 "Création d'une pièce jointe 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 de IPv4 sous-réseau vers la passerelle de transit.

Destination	Target
VPC A CIDR	locale
0.0.0.0/0	*transit-gateway-id*

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 de IPv4 sous-réseau vers la passerelle de transit.

Destination	Target
VPC B CIDR	locale
0.0.0.0/0	*transit-gateway-id*

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. L'entrée restante achemine tout le reste du trafic de IPv4 sous-réseau vers la passerelle Internet.

Destination	Target
VPC C CIDR	locale
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

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 tous les autres trafics de IPv4 sous-réseau vers la passerelle NAT.

Destination	Target
VPC C CIDR	locale
0.0.0.0/0	*nat-gateway-id*

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
VPC A CIDR	*Attachment for VPC A*	propagée
VPC B CIDR	*Attachment for VPC B*	propagée
VPC C CIDR	*Attachment for VPC C*	propagée

CIDR	Réseau de transit par passerelle	Type de routage
0.0.0.0/0	*Attachment for VPC C*	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

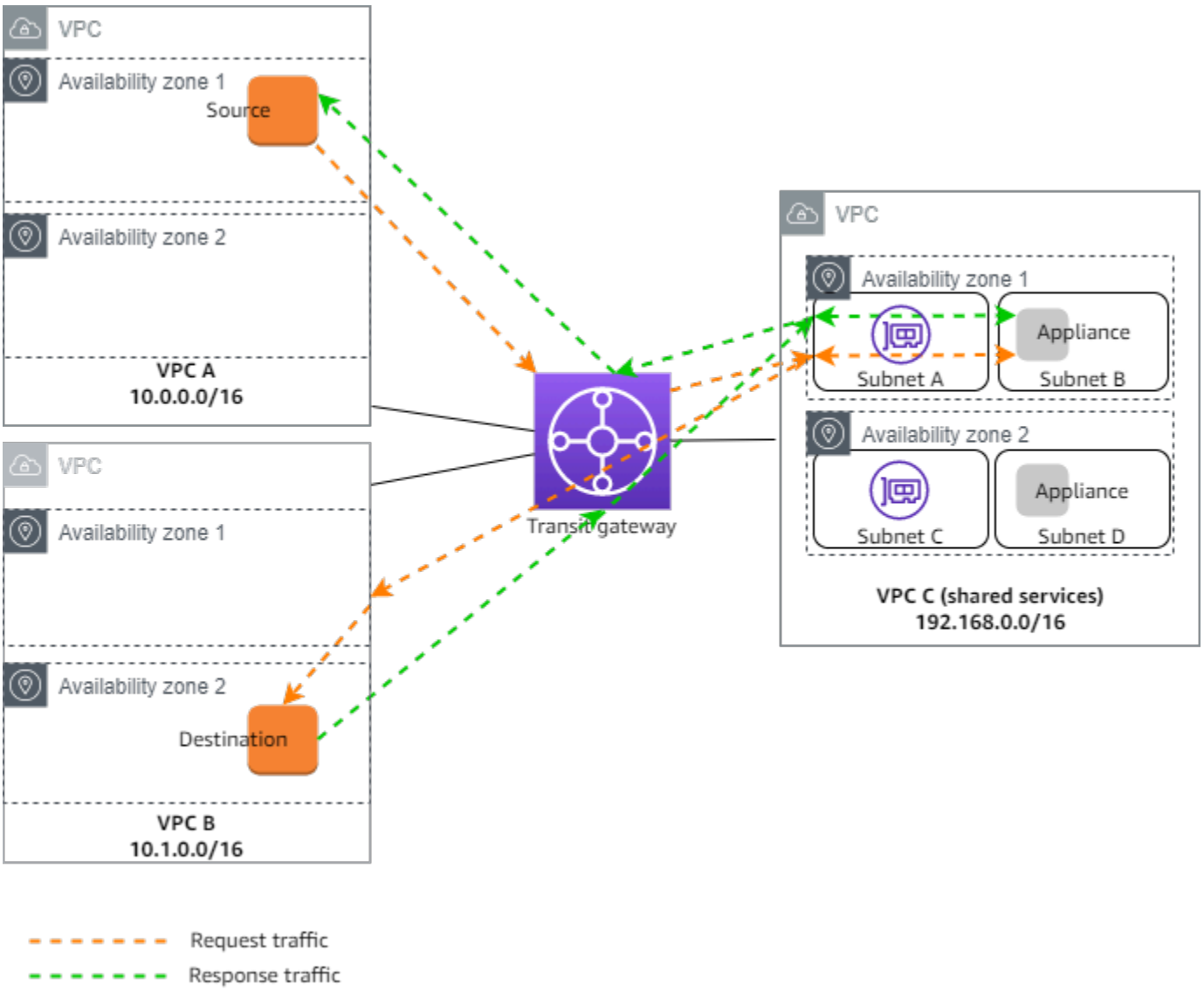
- Le trafic en mode appliance est acheminé correctement tant que le trafic source et de destination arrive vers un VPC centralisé (VPC d'inspection) à partir de la même pièce jointe de passerelle de transit. Le trafic peut chuter si la source et la destination se trouvent sur deux pièces jointes de passerelle de transit différentes. Le trafic peut chuter si le VPC centralisé reçoit le trafic d'une autre passerelle, par exemple une passerelle Internet, puis envoie ce trafic à la pièce jointe de la passerelle de transit après inspection.
- 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 VPCs. Pour plus d'informations, consultez Créer 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 accessoires en VPC, un pour chacun des. VPCs Pour de plus amples informations, veuillez consulter the section called “Création d'une pièce jointe 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 également utiliser l'API Amazon VPC, un AWS SDK, le 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

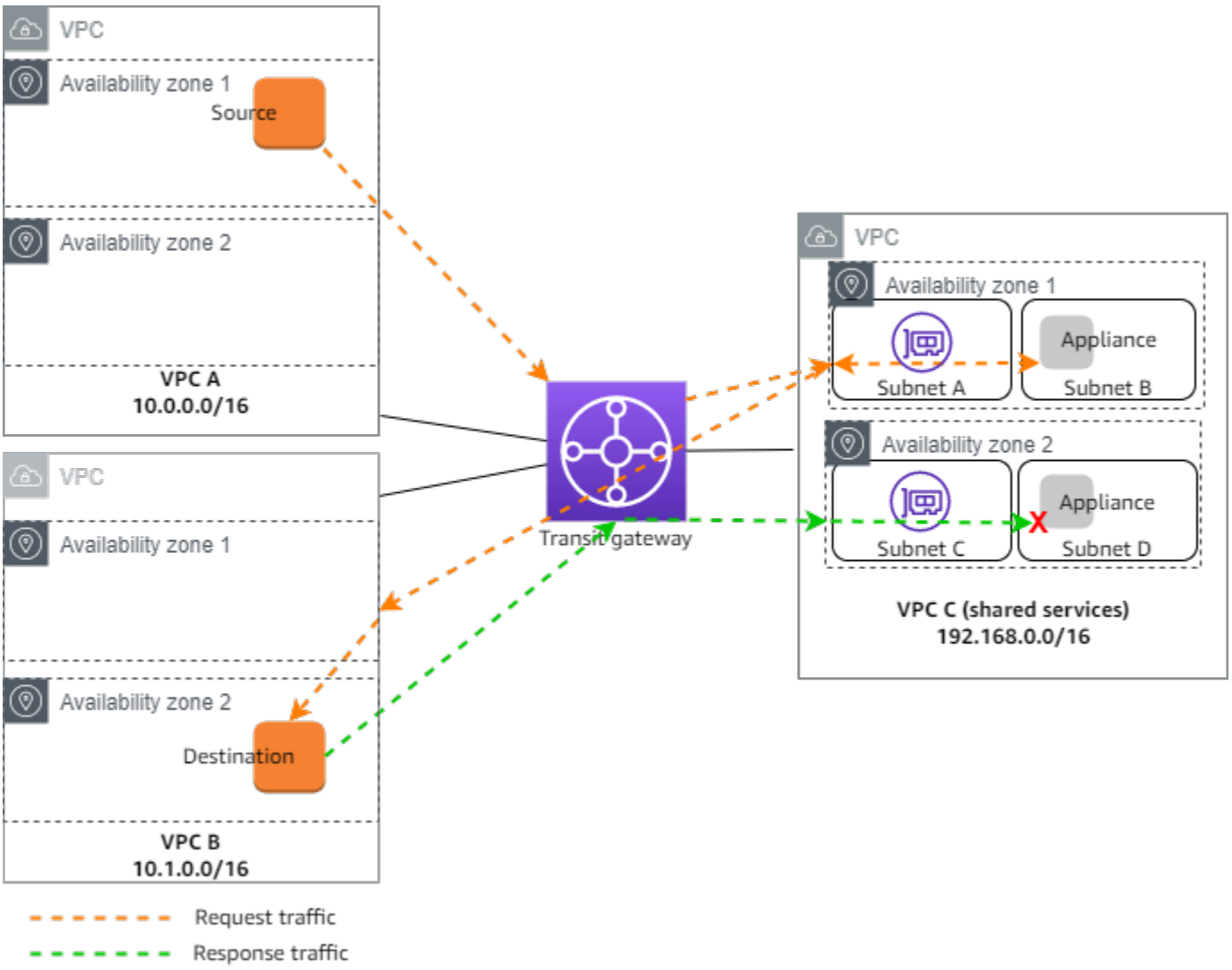
Si vos attachements de VPC s'étendent sur plusieurs zones de disponibilité et que vous devez acheminer le trafic entre les hôtes de source et de destination par le biais de la même appliance pour une inspection avec état, activez le support du mode de l'appliance pour l'attachement du VPC dans lequel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

Pour plus d'informations, consultez la section Architecture d'inspection centralisée dans le AWS blog.

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

VPCs A et B ont des tables de routage avec 2 entrées. La première entrée est l'entrée par défaut pour le IPv4 routage local dans le VPC. Cette entrée par défaut permet aux ressources du VPC de communiquer entre elles. La deuxième entrée achemine tout le reste du trafic de IPv4 sous-réseau 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	*Attachment ID for VPC C*	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	*Attachment ID for VPC A*	propagée
10.1.0.0/16	*Attachment ID for VPC B*	propagée

Tutoriels : Commencez à utiliser Amazon VPC Transit Gateways

Les didacticiels suivants vous aideront à vous familiariser avec les passerelles de transit dans Amazon VPC Transit Gateways. Les tâches décrites dans les didacticiels suivants vous guident dans la création d'une passerelle de transit, puis dans la connexion de deux d'entre vous VPCs à l'aide de cette passerelle de transit. Vous pouvez créer une passerelle de transit à l'aide de la console VPC Amaaozn ou du. AWS CLI

Tâches

- Tutoriel : Création d'une passerelle de AWS transit à l'aide de la console Amazon VPC
- Tutoriel : Création d'un AWS Transit Gateway à l'aide de la ligne de AWS commande

Tutoriel : Création d'une passerelle de AWS transit à l'aide de la console Amazon VPC

Dans ce didacticiel, vous allez apprendre à utiliser la console Amazon VPC pour créer une passerelle de transit et y VPCs connecter deux passerelles. Vous allez créer la passerelle de transit, associer les deux VPCs, puis configurer les itinéraires nécessaires pour permettre la communication entre la passerelle de transit et votre VPCs.

Prérequis

- Pour illustrer un exemple simple d'utilisation d'une passerelle de transit, créez-en deux VPCs dans la même région. Ils ne VPCs peuvent être ni identiques ni se chevaucher CIDRs. Lancez une EC2 instance Amazon dans chaque VPC. Pour plus d'informations, consultez Créer un VPC dans le guide de l'utilisateur Amazon VPC et Lancer une instance dans le guide de l'utilisateur Amazon. EC2
- Vous ne pouvez pas avoir des itinéraires identiques pointant vers deux itinéraires différents VPCs. Une passerelle de transit ne propage pas le CIDRs VPC nouvellement attaché si un itinéraire identique existe dans les tables de routage de la passerelle de transit.
- Assurez-vous de disposer des autorisations nécessaires pour utiliser les passerelles de transit. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans Amazon VPC Transit Gateways .

- 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 Configurer les règles des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Étapes

- Étape 1 : Création de la passerelle de transit
- Étape 2 : Attachez votre véhicule VPCs à votre passerelle de transport en commun
- Étape 3 : Ajoutez des itinéraires entre la passerelle de transport en commun et votre VPCs
- Étape 4 : Tester la passerelle de transit
- Étape 5 : Supprimer la passerelle de transit

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 que vous avez utilisée lorsque vous avez créé le VPCs.
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. Dans la section Configurer la passerelle de transit, procédez comme suit :

    1. Pour Amazon side Autonomous System Number (ASN), 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 est comprise entre 64512 et 65534 pour 16 bits. ASNs

La plage est comprise entre 4200000000 et 4294967294 pour 32 bits. ASNs

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

2. (Facultatif) Choisissez d'activer ou non l'une des options suivantes :
   - Support DNS pour les VPCs connexions à cette passerelle de transit.
   - Support VPN ECMP pour les connexions VPN connectées à la passerelle de transit.
   - Association de table de routage par défaut, qui associe automatiquement les pièces jointes de la passerelle de transit à la table de routage par défaut de cette passerelle de transit.
   - Propagation de la table de routage par défaut, qui propage automatiquement les pièces jointes de la table de routage vers la table de routage par défaut de cette passerelle de transit.
   - Support de multidiffusion, qui vous permet de créer des domaines de multidiffusion dans cette passerelle de transit.

8. (Facultatif) Dans la section Configure-cross-account des options de partage, choisissez d'accepter automatiquement les pièces jointes partagées. Si cette option est activée, les pièces jointes sont automatiquement acceptées. Dans le cas contraire, vous devez accepter ou rejeter les demandes de pièces jointes.
9. (Facultatif) Dans la section Blocs CIDR de la passerelle de transit, ajoutez un bloc CIDR de taille /24 ou plus pour les IPv4 adresses ou un bloc d'adresse CIDR /64 ou plus pour les adresses. 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.

   > **Note**
   >
   > Les blocs CIDR de passerelle de transit sont utilisés si vous configurez des pièces jointes Connect (GRE) ou VPNs PrivateIP. Transit Gateway attribue IPs aux points de terminaison du tunnel (GRE/PrivateIP VPN) de cette plage.

10. (Facultatif) Ajoutez des balises clé-valeur à cette passerelle de transit pour mieux l'identifier.
    1. Sélectionnez Ajouter une nouvelle balise.
    2. Saisissez le nom de la Clé et la Valeur associée.

3. Choisissez Ajouter un nouveau tag pour ajouter des tags supplémentaires, ou passez à l'étape suivante.

11. 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 : Attachez votre véhicule VPCs à votre passerelle de transport en commun

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

Vérifiez que vous en avez créé deux VPCs et lancé une EC2 instance dans chacune d'elles, comme décrit dansPrérequis.

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 le IPv6 support.
8. Pour VPC ID (ID de VPC), choisissez le VPC à attacher à la passerelle de transit.
9. Pour Sous-réseau IDs, sélectionnez un sous-réseau pour chaque zone de disponibilité à utiliser 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 de plus amples informations, veuillez consulter the section called “Exemples de scénarios de passerelle de transit”.

Étape 3 : Ajoutez des itinéraires entre la passerelle de transport en commun et votre VPCs

Une table de routage inclut des itinéraires dynamiques et statiques qui déterminent le saut suivant à associer VPCs en fonction 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 Enregistrer les modifications.

Étape 4 : Tester la passerelle de transit

Vous pouvez confirmer que la passerelle de transit a bien été créée en vous connectant à une EC2 instance Amazon dans chaque VPC, puis en envoyant des données entre eux, telles qu'une commande ping. Pour plus d'informations, consultez Connect to your EC2 instance dans le guide de EC2 l'utilisateur Amazon.

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 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, 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.

Tutoriel : Création d'un AWS Transit Gateway à l'aide de la ligne de AWS commande

Dans ce didacticiel, vous allez apprendre à utiliser le AWS CLI pour créer une passerelle de transit et y VPCs connecter deux passerelles. Vous allez créer la passerelle de transit, associer les deux VPCs, puis configurer les itinéraires nécessaires pour permettre la communication entre la passerelle de transit et votre VPCs.

Prérequis

Avant de commencer, assurez-vous d'avoir :

- AWS CLI installé et configuré avec les autorisations appropriées. Si vous ne l'avez pas AWS CLI installé, consultez la documentation de l'interface de ligne de AWS commande.
- Ils ne VPCs peuvent être ni identiques ni se chevaucher CIDRs. Pour plus d'informations, consultez Créer un VPC dans le Guide de l'utilisateur Amazon VPC.
- Une EC2 instance dans chaque VPC. Pour connaître les étapes de lancement d'une EC2 instance dans un VPC, consultez la section Lancer une instance dans le guide de EC2 l'utilisateur Amazon.
- Groupes de sécurité configurés pour autoriser le trafic ICMP entre les instances. Pour connaître les étapes à suivre pour contrôler le trafic à l'aide de groupes de sécurité, consultez la section Contrôler le trafic vers vos AWS ressources à l'aide de groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

- Autorisations IAM appropriées pour travailler avec les passerelles de transit. Pour vérifier les autorisations IAM des passerelles de transit, consultez la section Gestion des identités et des accès dans Amazon VPC Transit Gateways dans le guide.AWS Transit Gateway

Étapes

- Étape 1 : Création de la passerelle de transit
- Étape 2 : vérifier l'état de disponibilité de la passerelle de transit
- Étape 3 : Attachez votre véhicule VPCs à votre passerelle de transport en commun
- Étape 4 : Vérifiez que les pièces jointes de la passerelle de transit sont disponibles
- Étape 5 : Ajoutez des itinéraires entre votre passerelle de transport en commun et VPCs
- Étape 6 : Testez la passerelle de transit
- Étape 7 : Supprimer les pièces jointes de la passerelle de transit et la passerelle de transit
- Conclusion

Étape 1 : Création de la passerelle de transit

Lorsque vous créez une passerelle de transit, vous AWS créez une table de routage de passerelle de transit par défaut et l'utilisez comme table de routage d'association par défaut et comme table de routage de propagation par défaut. Voici un exemple de `create-transit-gateway` demande dans la `us-west-2` région. D'autres `options` ont été transmis dans la demande. Pour plus d'informations sur la `create-transit-gateway` commande, y compris une liste des options que vous pouvez transmettre dans la demande, consultez create-transit-gateway.

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

La réponse indique ensuite que la passerelle de transit a été créée. Dans la réponse, les valeurs `0ptions` renvoyées sont toutes des valeurs par défaut.

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
```

```
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> Cette commande renvoie des informations sur votre nouvelle passerelle de transit, notamment son identifiant. Prenez note de l'ID de passerelle de transit (`tgw-1234567890abcdef0`), car vous en aurez besoin lors des étapes suivantes.

Étape 2 : vérifier l'état de disponibilité de la passerelle de transit

Lorsque vous créez une passerelle de transit, elle est placée dans un `pending` état. L'état passera automatiquement de « en attente » à « disponible », mais tant que ce n'est pas le cas, vous ne pourrez pas en joindre VPCs tant que l'état ne changera pas. Pour vérifier l'état, exécutez la `describe-transit-gatweways` commande à l'aide de l'ID de passerelle de transit nouvellement créé et de l'option filtres. L'`filters`option utilise `Name=state` et `Values=available` associe. La commande recherche ensuite si l'état de votre passerelle de transit est disponible. Si c'est le cas, la réponse s'affiche`"State": "available"`. S'il se trouve dans un autre état, il n'est pas encore disponible pour utilisation. Patientez quelques minutes avant d'exécuter la commande.

Pour plus d'informations sur la commande `describe-transit-gateways`, consultez describe-transit-gateways.

```
aws ec2 describe-transit-gateways \
```

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

Attendez que l'état de la passerelle de transit passe de `pending` à `available` avant de continuer. Dans la réponse suivante, le `State` est devenu`available`.

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

Étape 3 : Attachez votre véhicule VPCs à votre passerelle de transport en commun

Une fois que votre passerelle de transit est disponible, créez une pièce jointe pour chaque VPC à l'aide du. `create-transit-gateway-vpc-attachment` Vous devrez inclure le `transit-gateway-id`vpc-id, le et le`subnet-ids`.

Pour plus d'informations sur la `create-transit-vpc attachment` commande, consultez create-transit-gateway-vpc-attachment.

Dans l'exemple suivant, la commande est exécutée deux fois, une fois pour chaque VPC.

Pour le premier VPC, exécutez ce qui suit en utilisant le premier `vpc_id` et : `subnet-ids`

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

La réponse indique que la pièce jointe a été correctement jointe. La pièce jointe est créée dans un `pending` état. Il n'est pas nécessaire de modifier cet état car il passe automatiquement à un `available` état. Cela peut prendre plusieurs minutes.

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

```
}
```

Pour le second VPC, exécutez la même commande que ci-dessus en utilisant le second `vpc_id` et : `subnet-ids`

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

La réponse à cette commande indique également une pièce jointe réussie, la pièce jointe étant actuellement dans un `pending` état.

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

Étape 4 : Vérifiez que les pièces jointes de la passerelle de transit sont disponibles

Les pièces jointes aux passerelles de transit sont créées dans un `pending` état initial. Vous ne pourrez pas utiliser ces pièces jointes dans vos itinéraires tant que l'état ne sera pas changé en`available`. Cela se fait automatiquement. Utilisez la `describe-transit-gateways`

commande, ainsi que le`transit-gateway-id`, pour vérifier le`State`. Pour plus d'informations sur la commande `describe-transit-gateways`, consultez describe-transit-gateways.

Exécutez la commande suivante pour vérifier l'état. Dans cet exemple, les champs facultatifs `Name` et `Values` les champs de filtres sont transmis dans la demande :

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

La réponse suivante montre que les deux pièces jointes sont dans un `available` même état :

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
```

```
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```

Étape 5 : Ajoutez des itinéraires entre votre passerelle de transport en commun et VPCs

Configurez les itinéraires dans la table de routage de chaque VPC pour diriger le trafic vers l'autre VPC via la passerelle de transit à l'aide de la `create-route` commande associée à la table de routage de `transit-gateway-id` chaque VPC. Dans l'exemple suivant, la commande est exécutée deux fois, une fois pour chaque table de routage. La demande inclut le`route-table-id`, le`destination-cidr-block`, et `transit-gateway-id` pour chaque route VPC que vous créez.

Pour plus d'informations sur `create-route` la commande, consultez create-route.

Pour la table de routage du premier VPC, exécutez la commande suivante :

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

Pour la table de routage du second VPC, exécutez la commande suivante. Cette route utilise un `route-table-id` et `destination-cidr-block` différent du premier VPC. Toutefois, comme vous n'utilisez qu'une seule passerelle de transit, c'est la même chose `transit-gateway-id` qui est utilisée.

```
aws ec2 create-route \
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

La réponse est renvoyée `true` pour chaque itinéraire, indiquant que les itinéraires ont été créés.

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

> **Note**
>
> Remplacez les blocs d'adresse CIDR de destination par les blocs d'adresse CIDR réels de votre. VPCs

Étape 6 : Testez la passerelle de transit

Vous pouvez vérifier que la passerelle de transit a bien été créée en vous connectant à une EC2 instance dans un VPC et en envoyant un ping à une instance dans l'autre VPC, puis en exécutant la commande. `ping`

1. Connectez-vous à votre EC2 instance dans le premier VPC à l'aide de SSH ou Instance Connect EC2
2. Envoyez un ping à l'adresse IP privée de l' EC2 instance dans le deuxième VPC :

   ```
   ping 10.2.0.50
   ```

   > **Note**
   >
   > `10.2.0.50`Remplacez-la par l'adresse IP privée réelle de votre EC2 instance dans le deuxième VPC.

Si le ping est réussi, votre passerelle de transit est correctement configurée et achemine le trafic entre vos VPCs.

Étape 7 : Supprimer les pièces jointes de la passerelle de transit et la passerelle de transit

Lorsque vous n'avez plus besoin de la passerelle de transit, vous pouvez la supprimer. Tout d'abord, vous devez supprimer toutes les pièces jointes. Exécutez la `delete-transit-gateway-vpc-attachment` commande en utilisant le `transit-gateway-attachment-id` pour chaque pièce

jointe. Après avoir exécuté la commande, utilisez-le `delete-transit-gateway` pour supprimer la passerelle de transit. Pour ce qui suit, supprimez les deux pièces jointes VPC et la passerelle de transit unique créées lors des étapes précédentes.

> **Important**
>
> Vous cesserez de payer des frais une fois que vous aurez supprimé toutes les pièces jointes de la passerelle de transit.

1. Supprimez les pièces jointes du VPC à l'aide de la `delete-transit-gateway-vpc-attachment` commande. Pour plus d'informations sur `delete-transit-gateway-vpc-attachment` la commande, consultez delete-transit-gateway-vpc-attachment.

   Pour la première pièce jointe, exécutez la commande suivante :

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

   La réponse de suppression pour le premier attachement VPC renvoie ce qui suit :

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

   Exécutez la `delete-transit-gateway-vpc-attachment` commande pour la deuxième pièce jointe :

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

   La réponse de suppression pour le deuxième attachement VPC renvoie ce qui suit :

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

2. Les pièces jointes sont conservées `deleting` jusqu'à ce qu'elles soient supprimées. Une fois supprimée, vous pouvez supprimer la passerelle de transit. Utilisez la `delete-transit-gateway` commande en même temps que le`transit-gateway-id`. Pour plus d'informations sur les `delete-transit-gateway` commandes, consultez delete-transit-gateway.

   L'exemple suivant supprime `My Transit Gateway` ce que vous avez créé à la première étape ci-dessus :

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

   Ce qui suit montre la réponse à la demande, qui inclut l'ID et le nom de la passerelle de transit supprimés, ainsi que les options d'origine définies pour la passerelle de transit lors de sa création.

   ```
   {
       "TransitGateway": {
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
   tgw-1234567890abcdef0",
           "State": "deleting",
           "OwnerId": "123456789012",
           "Description": "My Transit Gateway",
           "CreationTime": "2025-06-23T17:39:33+00:00",
           "Options": {
               "AmazonSideAsn": 64512,
               "AutoAcceptSharedAttachments": "disable",
               "DefaultRouteTableAssociation": "enable",
   ```

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

Conclusion

Vous avez créé avec succès une passerelle de transit, vous y avez VPCs attaché deux passerelles, configuré le routage entre elles et vérifié la connectivité. Cet exemple simple illustre les fonctionnalités de base d'Amazon VPC Transit Gateways. Pour des scénarios plus complexes, tels que la connexion à des réseaux sur site ou la mise en œuvre de configurations de routage plus avancées, consultez le guide de l'utilisateur d'Amazon VPC Transit Gateways.

Bonnes pratiques de conception d'Amazon VPC Transit Gateway

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 de disposer d'un plus grand nombre d'adresses pour EC2 les ressources. Lorsque vous utilisez un sous-réseau distinct, vous pouvez configurer les éléments suivants :
  - Gardez les réseaux entrants et sortants ACLs associés aux sous-réseaux de la passerelle de transit ouverts.
  - En fonction de votre flux de trafic, vous pouvez appliquer le réseau ACLs 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 des 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 de AWS Direct Connect passerelle et les pièces jointes Site-to-Site VPN BGP.
- 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 VPCs en même temps pour éviter que les paquets géants ne tombent en raison de différences 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.

Travaillez avec des passerelles de transit à l'aide d'Amazon VPC Transit Gateways

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

Rubriques

- Passerelles de transport en commun partagées
- Passerelles de transit dans Amazon VPC Transit Gateways
- Pièces jointes Amazon VPC dans Amazon VPC Transit Gateway
- AWS Pièces jointes aux fonctions réseau Transit Gateway
- AWS Site-to-Site VPN pièces jointes dans Amazon VPC Transit Gateways
- Pièces jointes d'une passerelle de transit à une passerelle Direct Connect dans Amazon VPC Transit Gateways
- Pièces jointes de peering de passerelle de transit dans Amazon VPC Transit Gateways
- Connectez les pièces jointes et connectez les pairs dans Amazon VPC Transit Gateways
- Tables de routage des passerelles de transit dans Amazon VPC Transit Gateways
- Tableaux des politiques relatives aux passerelles de transit dans Amazon VPC Transit Gateways
- Multidiffusion dans les passerelles de transit Amazon VPC

Passerelles de transport en commun partagées

Vous pouvez utiliser AWS Resource Access Manager (RAM) pour partager une passerelle de transit pour les pièces jointes VPC entre différents 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 .

Considérations

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

- Une AWS Site-to-Site VPN pièce jointe doit être créée dans le AWS compte propriétaire de la passerelle de transit.

- Une pièce jointe à une passerelle Direct Connect utilise une association de passerelle de transit et peut se trouver dans le même AWS compte que la passerelle Direct Connect ou dans un compte différent de celui de la passerelle Direct Connect.

Par défaut, les utilisateurs ne sont pas autorisés à créer ou à modifier AWS RAM des ressources. 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 tables de routage des passerelles de transit, des pièces jointes aux passerelles de transit et des passerelles de transit APIs.

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`.
- Exécutez le APIs qui crée et décrit les pièces jointes, par exemple `CreateTransitGatewayVpcAttachment` et`DescribeTransitGatewayVpcAttachments`, dans leur VPCs.

- 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 créé 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 identifiant AZ pour la région us-east-1 et correspond 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 plus partagée avec un autre AWS compte, ou si le AWS compte avec lequel la passerelle de transit est partagée est supprimé de l'organisation, la passerelle de transit elle-même n'est 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.

Passerelles de transit dans Amazon VPC Transit Gateways

Une passerelle de transit vous permet de connecter VPCs des connexions VPN et d'acheminer le trafic entre elles. Une passerelle de transit fonctionne de part en part Comptes AWS, 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 titulaire du compte peut l'associer VPCs 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 à la fois IPv6 CIDRs les cibles IPv4 ou. Les cibles sont VPCs 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 VPCs associer le développement à une table de routage et la production VPCs à une autre table de routage. Cela vous permet de créer des réseaux isolés au sein d'une passerelle de transit, de la même manière que le routage et le transfert virtuels (VRFs) dans les réseaux traditionnels.

Les passerelles de transit prennent en charge le routage dynamique et statique entre les connexions connectées VPCs et les connexions VPN. Vous pouvez activer ou désactiver la propagation du routage pour chaque attachement. Les attachements d'appairage de passerelle de transit prennent uniquement en charge le routage statique. Vous pouvez faire pointer les itinéraires des tables de routage des passerelles de transit vers l'attachement d'appairage pour acheminer le trafic entre les passerelles de transit homologues.

Vous pouvez éventuellement associer un IPv4 ou plusieurs blocs IPv6 CIDR 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 IPv6 CIDR IPv4 et les blocs CIDR, consultez la section Adressage IP dans le guide de l'utilisateur Amazon VPC.

Tâches

- Création d'une passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Afficher les informations relatives aux passerelles de transit à l'aide d'Amazon VPC Transit Gateways
- Ajouter ou modifier des balises pour une passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Modifier une passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Accepter un partage de ressources à l'aide d'Amazon VPC Transit Gateways
- Accepter une pièce jointe partagée à l'aide d'Amazon VPC Transit Gateways
- Supprimer une passerelle de transit à l'aide d'Amazon VPC Transit Gateways

Création d'une passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 ajouter 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 est comprise entre 64512 et 65534 pour 16 bits. ASNs

   La plage est comprise entre 4200000000 et 4294967294 pour 32 bits. ASNs

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

7. Pour le support DNS, sélectionnez cette option si vous avez besoin que le VPC transforme les noms d'hôtes IPv4 DNS publics en IPv4 adresses privées lorsqu'ils sont demandés par des instances d'un autre VPC connecté à la passerelle de transit.

8. Pour la prise en charge du référencement des groupes de sécurité, activez cette fonctionnalité pour référencer un groupe de sécurité VPCs attaché à une passerelle de transit. Pour plus d'informations sur le référencement des groupes de sécurité, consultezthe section called “Référencement des groupes de sécurité”.

9. 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 les connexions annoncent la même chose CIDRs, le trafic est réparti de manière égale entre elles.

   Lorsque vous sélectionnez cette option, l'ASN BGP annoncé, puis les attributs BGP tels que le chemin AS-Path, 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.

10. 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.

11. 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.

12. (Facultatif) Pour utiliser la passerelle de transit comme routeur pour du trafic de multicast, sélectionnez Multicast support (Support multicast).
13. (Facultatif) Dans la section Configure-cross-account des options de partage, choisissez d'accepter automatiquement les pièces jointes partagées. Si cette option est activée, les pièces jointes sont automatiquement acceptées. Dans le cas contraire, vous devez accepter ou rejeter les demandes de pièces jointes.

    Pour Auto accept shared attachments (Accepter automatiquement les attachements partagés), sélectionnez cette option pour accepter automatiquement les attachements entre comptes.
14. (Facultatif) Pour les blocs CIDR de passerelle de transit, spécifiez un IPv4 ou plusieurs blocs IPv6 CIDR pour votre passerelle de transit.

    Vous pouvez spécifier un bloc CIDR de taille /24 ou plus (par exemple, /23 ou /22) pour IPv4, ou un bloc 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.

    > **Note**
    >
    > Les blocs CIDR de passerelle de transit sont utilisés si vous configurez des pièces jointes Connect (GRE) ou VPNs PrivateIP. Transit Gateway attribue IPs aux points de terminaison du tunnel (GRE/PrivateIP VPN) de cette plage.
15. 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 les informations relatives aux passerelles de transit à l'aide d'Amazon VPC Transit Gateways

Consultez n'importe laquelle de vos passerelles de transport en commun.

Pour afficher 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. Les détails de la passerelle de transit sont affichés sous la liste des passerelles sur la page.

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

Utilisez la commande describe-transit-gateways.

Ajouter ou modifier des balises pour une passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 plus d'informations, consultez la section Marquage de vos EC2 ressources Amazon.

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. Choisissez 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 Save (Enregistrer).

Modifier une passerelle de transit à l'aide d'Amazon VPC Transit Gateways

Vous pouvez modifier les options de configuration d'une passerelle de transit. Lorsque vous modifiez une passerelle de transit, les pièces jointes de passerelle de transit existantes ne subissent aucune 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.

Accepter un partage de ressources à l'aide d'Amazon VPC Transit Gateways

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/.
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 une pièce jointe partagée à l'aide d'Amazon VPC Transit Gateways

Si vous n'avez pas activé la fonctionnalité d'acceptation automatique des pièces jointes partagées lorsque vous avez créé votre passerelle de transit, vous devez accepter manuellement les pièces jointes entre comptes (partagées) à l'aide de la console Amazon VPC ou de la AWS CLI.

Pour accepter manuellement un attachement partagé

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 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 à l'aide d'Amazon VPC Transit Gateways

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.

Pièces jointes Amazon VPC dans Amazon VPC Transit Gateway

Une pièce jointe Amazon Virtual Private Cloud (VPC) à une passerelle de transit vous permet d'acheminer le trafic vers et depuis un ou plusieurs sous-réseaux 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.

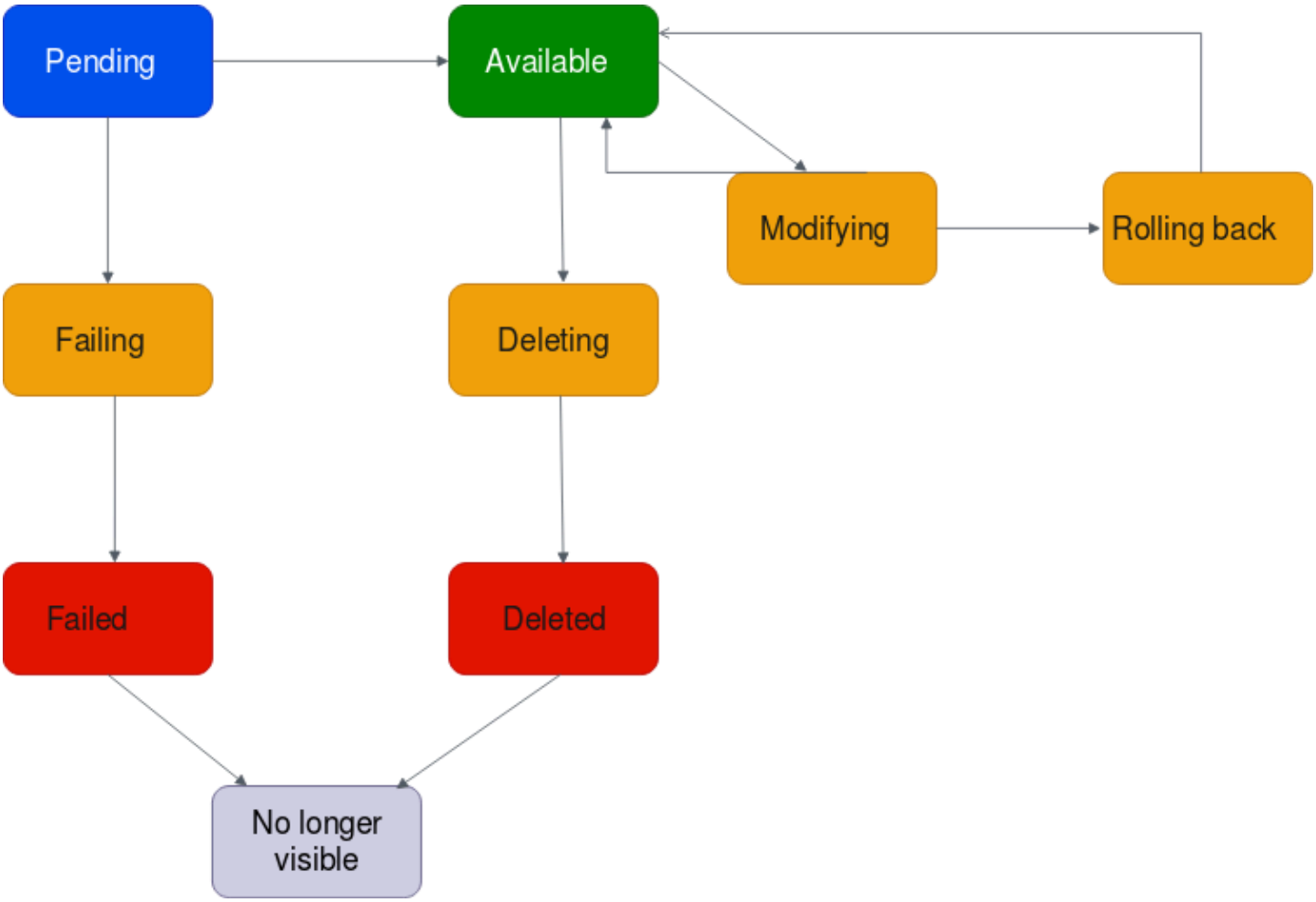
Limites

- 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.
- Une passerelle de transit ne prend pas en charge la résolution DNS pour les noms DNS personnalisés des configurations VPCs associées à l'aide de zones hébergées privées dans Amazon Route 53. Pour configurer la résolution des noms pour les zones hébergées privées pour toutes les personnes VPCs rattachées 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 deux VPCs adresses identiques CIDRs, ou si un CIDR d'une plage chevauche un CIDR d'un VPC rattaché. Si vous attachez un VPC à une passerelle de transit et que son CIDR est identique ou chevauche le CIDR d'un autre VPC déjà attaché à la passerelle de transit, les itinéraires du VPC nouvellement attaché ne sont pas propagés vers la table de routage 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 de pièce jointe à une passerelle de transit en utilisant IPv6 uniquement des sous-réseaux. Les sous-réseaux attachés aux passerelles de transit doivent également prendre en charge IPv4 les adresses.
- Une passerelle de transit doit avoir au moins un attachement VPC avant de pouvoir être ajoutée à une table de routage.

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.

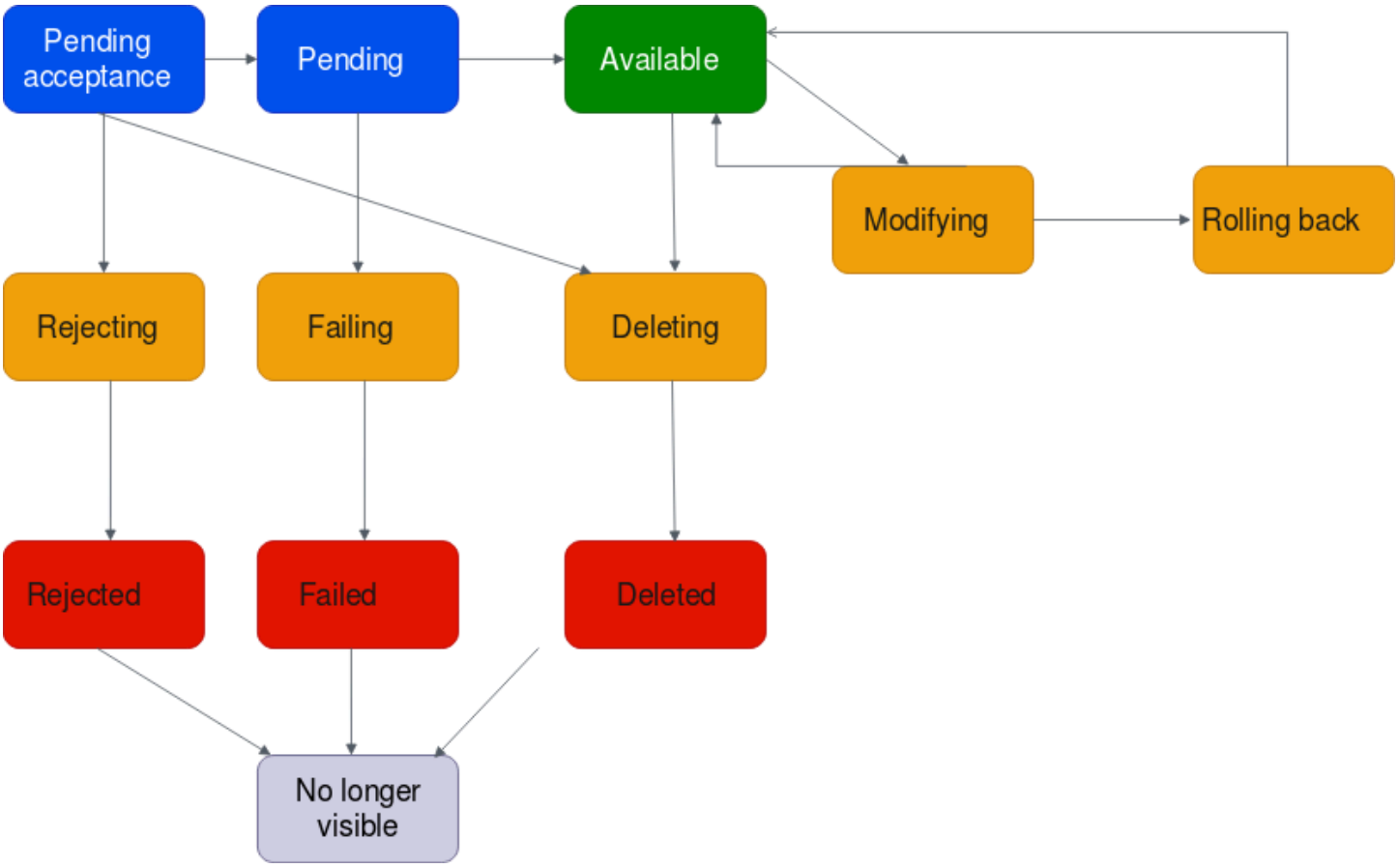
Le diagramme suivant montre les états par lesquels qu'un attachement peut passer dans une configuration de compte unique ou une configuration inter-comptes pour laquelle l' acceptation automatique des attachements partagés est activée.



- 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`.

Mode Appliance

Si vous envisagez de configurer une appliance réseau dynamique dans votre VPC, vous pouvez activer la prise en charge du mode appliance pour la pièce jointe VPC dans laquelle se trouve l'appliance lorsque vous créez une pièce jointe. Cela garantit que AWS Transit Gateway utilise la même zone de disponibilité pour cet attachement VPC pendant toute la durée de vie du flux de trafic entre une source et une destination. Cela permet également à une 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 dans cette zone. Bien que le mode appliance ne soit pris en charge que sur les pièces jointes VPC, le flux réseau peut provenir de tout autre type de connexion de passerelle de transit,

y compris les pièces jointes VPC, VPN et Connect. Le mode appliance fonctionne également pour les flux réseau dont les sources et les destinations sont différentes Régions AWS. Les flux réseau peuvent potentiellement être rééquilibrés entre différentes zones de disponibilité si vous n'activez pas initialement le mode appliance, mais que vous modifiez ultérieurement la configuration des pièces jointes pour l'activer. Vous pouvez activer ou désactiver le mode appliance à l'aide de la console, de la ligne de commande ou de l'API.

Le mode appliance dans AWS Transit Gateway optimise le routage du trafic en tenant compte des zones de disponibilité source et de destination lors de la détermination du chemin à travers un VPC en mode appliance. Cette approche améliore l'efficacité et réduit le temps de latence. Le comportement varie en fonction de la configuration spécifique et des modèles de trafic. Voici des exemples de scénarios.

Scénario 1 : routage du trafic dans une zone de disponibilité via le VPC de l'appliance

Lorsque le trafic circule de la zone de disponibilité source us-east-1a vers la zone de disponibilité de destination us-east-1a, avec des pièces jointes VPC en mode appliance à la fois dans us-east-1a et us-east-1b, Transit Gateway sélectionne une interface réseau parmi us-east-1a au sein du VPC de l'appliance. Cette zone de disponibilité est maintenue pendant toute la durée du flux de trafic entre la source et la destination.

Scénario 2 : routage du trafic des zones d'interdisponibilité via le VPC de l'appliance

Pour le trafic circulant de la zone de disponibilité source us-east-1a vers la zone de disponibilité de destination us-east-1b, avec des pièces jointes VPC en mode appliance dans us-east-1a et us-east-1b, Transit Gateway utilise un algorithme de hachage de flux pour sélectionner us-east-1a ou us-east-1b dans le VPC de l'appliance. La zone de disponibilité choisie est utilisée de manière cohérente pendant toute la durée de vie du flux.

Scénario 3 : routage du trafic via un VPC de l'appliance sans données de zone de disponibilité

Lorsque le trafic provient de la zone de disponibilité source us-east-1a vers une destination sans informations de zone de disponibilité (par exemple, le trafic lié à Internet), avec des pièces jointes VPC en mode appliance dans us-east-1a et us-east-1b, Transit Gateway sélectionne une interface réseau parmi us-east-1a au sein du VPC de l'appliance.

Scénario 4 : routage du trafic via un VPC d'appliance dans une zone de disponibilité distincte de la source ou de la destination

Lorsque le trafic circule de la zone de disponibilité source us-east-1a vers la zone de disponibilité de destination us-east-1b, avec des pièces jointes VPC en mode appliance dans différentes zones de disponibilité, par exemple us-east-1c et us-east-1d, Transit Gateway utilise un algorithme de hachage de flux pour sélectionner us-east-1c ou us-east-1d dans le VPC de l'appliance. La zone de disponibilité choisie est utilisée de manière cohérente pendant toute la durée de vie du flux.

> **Note**
>
> Le mode appliance n'est pris en charge que pour les pièces jointes VPC. Assurez-vous que la propagation de routage est activée pour une table de routage associée à une pièce jointe VPC de l'appliance.

Référencement des groupes de sécurité

Vous pouvez utiliser cette fonctionnalité pour simplifier la gestion des groupes de sécurité et le contrôle du instance-to-instance trafic entre VPCs eux qui sont attachés à la même passerelle de transit. Vous ne pouvez faire référence à des groupes de sécurité que dans les règles entrantes. Les règles de sécurité sortantes ne prennent pas en charge le référencement des groupes de sécurité. Aucun coût supplémentaire n'est associé à l'activation ou à l'utilisation du référencement des groupes de sécurité.

La prise en charge du référencement des groupes de sécurité peut être configurée à la fois pour les passerelles de transit et pour les pièces jointes VPC des passerelles de transit et ne fonctionnera que si elle a été activée à la fois pour une passerelle de transit et ses pièces jointes VPC.

Limites

Les limitations suivantes s'appliquent lors de l'utilisation du référencement de groupes de sécurité avec une pièce jointe VPC.

- Le référencement des groupes de sécurité n'est pas pris en charge sur les connexions d'appairage des passerelles de transit. Les deux VPCs doivent être rattachés à la même passerelle de transit.
- Le référencement des groupes de sécurité n'est pas pris en charge pour les pièces jointes VPC dans la zone de disponibilité use1-az3.

- Le référencement des groupes de sécurité n'est pas pris en charge pour les points de PrivateLink terminaison. Nous vous recommandons d'utiliser des règles de sécurité basées sur le CIDR IP comme alternative.
- Le référencement des groupes de sécurité fonctionne pour Elastic File System (EFS) tant qu'une règle de groupe de sécurité autorisant toutes les sorties est configurée pour les interfaces EFS du VPC.
- Pour la connectivité aux zones locales via une passerelle de transit, seules les zones locales suivantes sont prises en charge : us-east-1-atl-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a et us-west-2-phx-2a.
- Nous recommandons de désactiver cette fonctionnalité au niveau de l'attachement au VPC VPCs pour les sous-réseaux situés dans des zones Local AWS , Outposts et Wavelength Zones non pris en charge AWS , car cela pourrait entraîner une interruption de service.
- Si vous disposez d'un VPC d'inspection, le référencement des groupes de sécurité via la passerelle de transit ne fonctionne pas sur Gateway AWS Load Balancer ou sur un Network Firewall. AWS

Tâches

- Création d'une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways
- Modifier une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways
- Modifier les balises de pièce jointe d'un VPC à l'aide d'Amazon VPC Transit Gateways
- Afficher une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways
- Supprimer une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways
- Mettre à jour les règles entrantes des groupes de AWS Transit Gateway sécurité
- Identifier les groupes de sécurité AWS Transit Gateway référencés
- Supprimer les règles de groupe AWS Transit Gateway de sécurité obsolètes
- Résoudre les problèmes liés à la création de pièces jointes VPC Amazon VPC Transit Gateway

Création d'une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways

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 si vous souhaitez activer le support DNS, le IPv6support et le support en 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. Choisissez d'activer ou non la prise en charge du référencement des groupes de sécurité. Activez cette fonctionnalité pour référencer un groupe de sécurité VPCs attaché à une passerelle de transit. Pour plus d'informations sur le référencement des groupes de sécurité, consultezthe section called “Référencement des groupes de sécurité”.
9. Choisissez d'activer ou non IPv6le Support.
10. 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.
11. Pour Sous-réseau IDs, sélectionnez un sous-réseau pour chaque zone de disponibilité à utiliser 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.
12. 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 une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways

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. Activez ou désactivez l'une des options suivantes :
   - Prise en charge du DNS
   - IPv6 soutien
   - Prise en charge du mode appliance
5. Pour ajouter ou supprimer un sous-réseau de la pièce jointe, cochez ou décochez la case correspondant à l'ID de sous-réseau que vous souhaitez ajouter ou supprimer.

   > **Note**
   >
   > 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. Pour pouvoir référencer un groupe de sécurité VPCs attaché à une passerelle de transit, sélectionnez Support de référencement des groupes de sécurité. Pour plus d'informations sur le référencement des groupes de sécurité, consultezthe section called “Référencement des groupes de sécurité”.

   > **Note**
   >
   > Si vous désactivez le référencement de groupes de sécurité pour une passerelle de transit existante, il sera désactivé sur toutes les pièces jointes VPC.

7. 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 de pièce jointe d'un VPC à l'aide d'Amazon VPC Transit Gateways

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 Save (Enregistrer).

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

Afficher une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways

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 une pièce jointe VPC à l'aide d'Amazon VPC Transit Gateways

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.

Mettre à jour les règles entrantes des groupes de AWS Transit Gateway sécurité

Vous pouvez mettre à jour n'importe quelle règle de groupe de sécurité entrant associée à une passerelle de transit. Vous pouvez mettre à jour les règles du groupe de sécurité à l'aide de la console Amazon VPC ou à l'aide de la ligne de commande ou de l'API. Pour plus d'informations sur le référencement des groupes de sécurité, consultezthe section called “Référencement des groupes de sécurité”.

Pour mettre à jour les règles de votre groupe de sécurité 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 Groupes de sécurité.
3. Sélectionnez le groupe de sécurité, puis choisissez Actions, Modifier les règles entrantes pour modifier les règles entrantes.
4. Pour ajouter une règle, choisissez Ajouter une règle et spécifiez le type, le protocole et la plage de ports. Pour Source (règle entrante), entrez l'ID du groupe de sécurité dans le VPC connecté à la passerelle de transit.

   > **Note**
   >
   > Les groupes de sécurité d'un VPC connecté à la passerelle de transit ne sont pas automatiquement affichés.

5. Pour modifier une règle existante, modifiez ses valeurs (par exemple, la source ou la description).
6. Pour supprimer une règle, cliquez sur Supprimer à côté de la règle.
7. Sélectionnez Enregistrer les règles.

Pour mettre à jour les règles entrantes à l'aide de la ligne de commande

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

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

Identifier les groupes de sécurité AWS Transit Gateway référencés

Pour déterminer si votre groupe de sécurité est référencé dans les règles d'un groupe de sécurité d'un VPC rattaché à la même passerelle de transit, utilisez l'une des commandes suivantes.

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

Supprimer les règles de groupe AWS Transit Gateway de sécurité obsolètes

Une règle de groupe de sécurité périmée est une règle qui fait référence à un groupe de sécurité supprimé dans le même VPC ou dans un VPC rattaché à la même passerelle de transit. Lorsqu'une règle du groupe de sécurité devient obsolète, elle n'est pas automatiquement supprimée de votre groupe de sécurité et vous devez la supprimer manuellement.

Vous pouvez afficher et supprimer les règles du groupe de sécurité obsolètes pour un VPC à l'aide de la console Amazon VPC.

Pour afficher et supprimer des règles du groupe de sécurité obsolètes

1. Ouvrez la console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Security groups (Groupes de sécurité).
3. Choisissez Actions (Actions), Manage stale rules (Gestion les règles obsolètes).
4. PourVPC, choisissez le VPC dont les règles sont obsolètes.
5. Choisissez Modifier.
6. Choisissez le bouton Supprimer à la droite de la règle à supprimer. Choisissez Prévisualiser les modifications, Enregistrer les règles.

Pour décrire les règles de votre groupe de sécurité périmées à l'aide de la ligne de commande

- describe-stale-security-groups (AWS CLI)

- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Après avoir identifié les règles du groupe de sécurité obsolètes, vous pouvez les supprimer à l'aide des revoke-security-group-egresscommandes revoke-security-group-ingressor.

Résoudre les problèmes liés à la création de pièces jointes VPC Amazon VPC Transit Gateway

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 la pièce jointe VPC manuellement. Pour de plus amples informations, veuillez consulter the section called “Création d'une pièce jointe VPC”.
3. Vérifiez que le rôle lié au service dispose des autorisations correctes. Pour de plus amples informations, veuillez consulter the section called “Passerelle de transit”.

4. Vérifiez que la passerelle de transit est dans l'état `available`. Pour de plus amples informations, veuillez consulter the section called “Afficher une passerelle de transit”.

AWS Pièces jointes aux fonctions réseau Transit Gateway

Vous pouvez créer une pièce jointe à une fonction réseau à laquelle connecter directement votre passerelle de transit AWS Network Firewall. Il n'est donc plus nécessaire de créer et de gérer une inspection VPCs.

À l'aide d'un pare-feu, provisionne et gère AWS automatiquement toutes les ressources nécessaires en arrière-plan. Vous verrez une nouvelle pièce jointe à une passerelle de transit plutôt que des points de terminaison de pare-feu individuels. Cela simplifie le processus de mise en œuvre de l'inspection centralisée du trafic réseau.

Avant de pouvoir utiliser une pièce jointe de pare-feu, vous devez d'abord créer la pièce jointe dans AWS Network Firewall. Pour les étapes de création de la pièce jointe, voir Getting Started with AWS Network Firewall Management dans le guide du AWS Network Firewall développeur. Une fois le pare-feu créé, vous pouvez consulter la pièce jointe dans la console Transit Gateway dans la section Pièces jointes. La pièce jointe sera répertoriée avec un type de fonction réseau.

Rubriques

- Accepter ou rejeter une pièce jointe à une fonction réseau AWS Transit Gateway
- Afficher les pièces jointes aux fonctions réseau AWS Transit Gateway
- Acheminer le trafic via une fonction réseau AWS Transit Gateway en pièce jointe

Accepter ou rejeter une pièce jointe à une fonction réseau AWS Transit Gateway

Vous pouvez utiliser la console Amazon VPC, la AWS Network Firewall CLI ou l'API pour accepter ou rejeter un attachement à une fonction réseau de passerelle de transit, y compris les pièces jointes Network Firewall. Si vous êtes propriétaire d'une passerelle de transit et que quelqu'un a créé une pièce jointe pare-feu à votre passerelle de transit à partir d'un autre compte, vous devez accepter ou rejeter la demande de pièce jointe.

Pour accepter ou rejeter une attache à une fonction réseau à l'aide de la Network Firewall CLI, consultez le `AcceptNetworkFirewallTransitGatewayAttachment` ou

`RejectNetworkFirewallTransitGatewayAttachment` APIs dans la référence de l'AWS Network Firewall API.

Accepter ou rejeter une pièce jointe à une fonction réseau à l'aide de la console

Utilisez la console Amazon VPC pour accepter ou rejeter un attachement à une fonction réseau de passerelle de transit.

Pour accepter ou rejeter une pièce jointe à une fonction réseau 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 Gateways.
3. Choisissez les pièces jointes Transit Gateway.
4. Sélectionnez la pièce jointe dont l'état est En attente d'acceptation et le type de fonction réseau.
5. Choisissez Actions, puis choisissez Accepter la pièce jointe ou Rejeter la pièce jointe.
6. Dans la boîte de dialogue de confirmation, choisissez Accepter ou Rejeter.

Si vous acceptez la pièce jointe, elle devient active et le pare-feu peut inspecter le trafic. Si vous rejetez la pièce jointe, elle passe à l'état rejeté et sera finalement supprimée.

Afficher les pièces jointes aux fonctions réseau AWS Transit Gateway

Vous pouvez consulter les pièces jointes de vos fonctions réseau, y compris vos AWS Network Firewall pièces jointes, à l'aide de la console Amazon VPC ou de la console Network Manager pour obtenir une représentation visuelle de la topologie de votre réseau.

Afficher une pièce jointe à une fonction réseau à l'aide de la console Network Manager

Vous pouvez consulter les pièces jointes d'une fonction réseau à l'aide de la console Network Manager.

Pour afficher les pièces jointes du pare-feu dans Network Manager

1. Ouvrez la console Network Manager à la page d'https://console.aws.amazon.com/networkmanager/accueil/.
2. Créez un réseau mondial dans Network Manager si vous n'en avez pas déjà un.
3. Enregistrez votre passerelle de transit auprès de Network Manager.
4. Sous Réseaux mondiaux, choisissez le réseau mondial sur lequel se trouve la pièce jointe.

5. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit).
6. Choisissez la passerelle de transit pour laquelle vous souhaitez afficher les pièces jointes.
7. Choisissez la vue de l'arborescence topologique. Les pièces jointes du Network Firewall apparaissent avec une icône de fonction réseau.
8. Pour afficher les détails relatifs à un attachement de pare-feu spécifique, sélectionnez la passerelle de transit dans la vue topologique, puis sélectionnez l'onglet Fonction réseau.

La console Network Manager fournit des informations détaillées sur les pièces jointes de votre pare-feu, notamment leur statut, la passerelle de transit associée et les zones de disponibilité.

Afficher une pièce jointe à une fonction réseau à l'aide de la console Amazon VPC

Utilisez la console VPC pour consulter la liste des types de pièces jointes de votre passerelle de transit.

Pour afficher les types de pièces jointes d'une passerelle de transit à l'aide de la console VPC

- Consultez Afficher une pièce jointe VPC.

Acheminer le trafic via une fonction réseau AWS Transit Gateway en pièce jointe

Après avoir créé une pièce jointe à une fonction réseau, vous devez mettre à jour les tables de routage de votre passerelle de transit pour envoyer le trafic via le pare-feu à des fins d'inspection à l'aide de la console Amazon VPC ou de la CLI. Pour connaître les étapes de mise à jour d'une association de tables de routage d'une passerelle de transit, consultezAssocier une table de routage de passerelle de transit.

Acheminer le trafic via une pièce jointe au pare-feu à l'aide de la console

Utilisez la console Amazon VPC pour acheminer le trafic via une pièce jointe à une fonction réseau de passerelle de transit.

Pour acheminer le trafic via un attachement à une fonction réseau 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 Gateways.

3. Choisissez les tables de routage de Transit Gateway.
4. Sélectionnez la table de routage que vous souhaitez modifier.
5. Choisissez Actions, puis sélectionnez Créer un itinéraire statique.
6. Pour CIDR, entrez le bloc CIDR de destination pour l'itinéraire.
7. Pour Attachement, sélectionnez le rattachement de la fonction réseau. Par exemple, il peut s'agir d'une AWS Network Firewall pièce jointe.
8. Choisissez Create static route (Créer un acheminement statique).

> **Note**
>
> Seuls les itinéraires statiques sont pris en charge.

Le trafic correspondant au bloc CIDR de votre table de routage sera désormais envoyé à la pièce jointe du pare-feu pour inspection avant d'être redirigé vers sa destination finale.

Acheminer le trafic via un attachement à une fonction réseau à l'aide de la CLI ou de l'API

Utilisez la ligne de commande ou l'API pour acheminer une pièce jointe à une fonction réseau de passerelle de transit.

Pour acheminer le trafic via une fonction réseau attachée à l'aide de la ligne de commande ou de l'API

- Utilisez `create-transit-gateway-route`.

  Par exemple, la demande peut être destinée à acheminer une pièce jointe d'un pare-feu réseau :

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

  La sortie renvoie ensuite :

```
{
  "Route": {
```

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

Le trafic correspondant au bloc CIDR de votre table de routage sera désormais envoyé à la pièce jointe du pare-feu pour inspection avant d'être redirigé vers sa destination finale.

AWS Site-to-Site VPN pièces jointes dans Amazon VPC Transit Gateways

Vous pouvez connecter une pièce jointe Site-to-Site VPN à une passerelle de transit dans Amazon VPC Transit Gateways, ce qui vous permet de connecter vos réseaux VPCs et ceux sur site. Les itinéraires dynamiques et statiques sont pris en charge, de même que IPv4 et IPv6.

Prérequis

- Pour associer une connexion VPN à votre passerelle de transit, vous devez spécifier la passerelle client VPN, qui a des exigences spécifiques en matière d'appareils. Avant de créer une pièce jointe Site-to-Site VPN, passez en revue les exigences relatives à la passerelle client pour vous assurer que votre passerelle est correctement configurée. Pour plus d'informations sur ces exigences, y compris des exemples de fichiers de configuration de passerelle, consultez la section Exigences relatives à votre dispositif de passerelle client Site-to-Site VPN dans le guide de AWS Site-to-Site VPN l'utilisateur.
- Pour les itinéraires statiques VPNs, vous devez également d'abord ajouter les itinéraires statiques à la table des itinéraires de la passerelle de transit. Les itinéraires statiques d'une table de routage d'une passerelle de transit qui ciblent un rattachement VPN ne sont pas filtrés par le Site-to-Site VPN, car cela peut permettre un flux de trafic sortant involontaire lors de l'utilisation d'un VPN basé sur le BGP. Pour connaître les étapes permettant d'ajouter un itinéraire statique à une table de routage de passerelle de transit, consultezCréer un itinéraire statique.

Vous pouvez créer, afficher ou supprimer une pièce jointe Site-to-Site VPN de passerelle de transit à l'aide de la console Amazon VPC ou de la CLI AWS .

Tâches

- Création d'une passerelle de transit attachée à un VPN à l'aide d'Amazon VPC Transit Gateways
- Afficher une pièce jointe VPN à l'aide d'Amazon VPC Transit Gateway
- Supprimer une pièce jointe VPN à l'aide d'Amazon VPC Transit Gateways

Création d'une passerelle de transit attachée à un VPN à l'aide d'Amazon VPC Transit Gateways

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 publiques statique et la version du moteur de cache.

     Pour Options de routage, sélectionnez Dynamique ou Statique. Pour plus d'informations, consultez la section Options de routage Site-to-Site VPN dans le guide de AWS Site-to-Site VPN l'utilisateur.
7. Pour Tunnel Options (Options de tunnel), saisissez les plages CIDR et les clés pré-partagées pour votre tunnel. Pour plus d'informations, consultez Architectures Site-to-Site VPN.
8. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de transit).

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

Utilisez la commande create-vpn-connection.

Afficher une pièce jointe VPN à l'aide d'Amazon VPC Transit Gateway

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.

Supprimer une pièce jointe VPN à l'aide d'Amazon VPC Transit Gateways

Pour supprimer 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. Sélectionnez l'attachement VPN.
4. Choisissez l'ID de ressource de la connexion VPN pour accéder à la page Connexions VPN.
5. Choisissez Actions, Supprimer.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

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

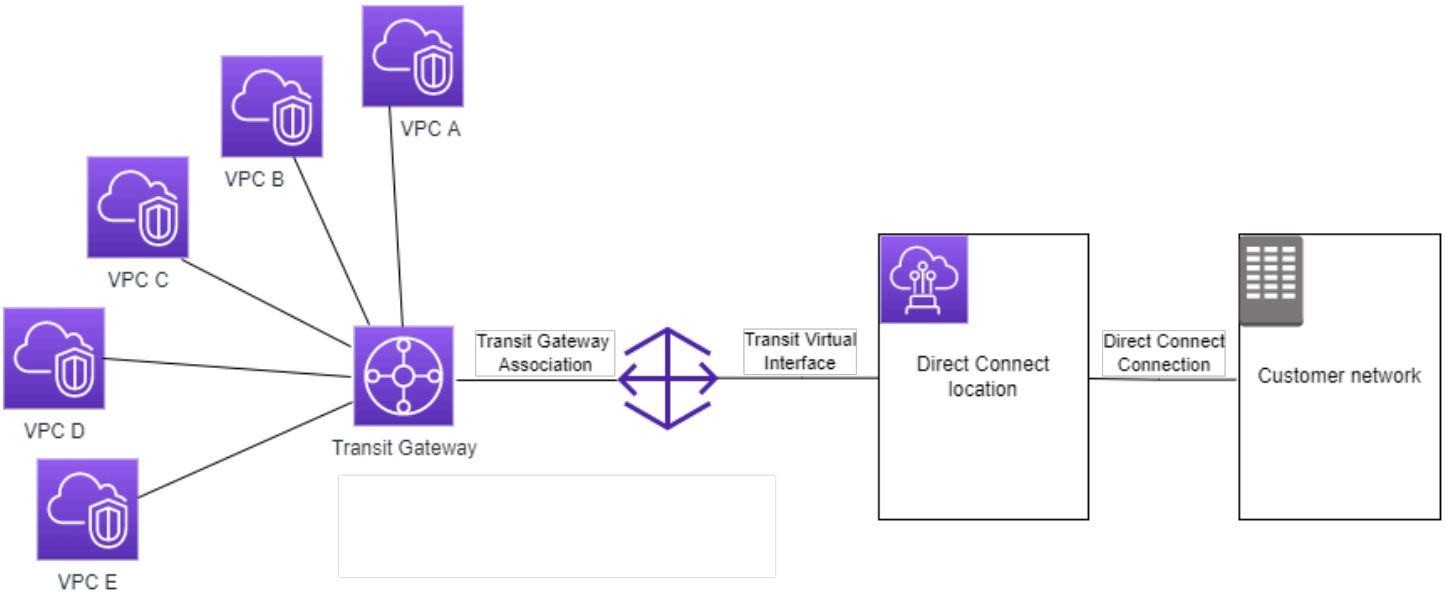
Utilisez la commande delete-vpn-connection.

Pièces jointes d'une passerelle de transit à une passerelle Direct Connect dans Amazon VPC Transit Gateways

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 :

- Gérez une seule connexion pour plusieurs VPCs ou pour celles VPNs qui se trouvent dans la même région.
- Faites de la publicité pour les préfixes depuis AWS AWS et vers le local.

Le schéma suivant montre comment la passerelle Direct Connect vous permet de créer une connexion unique à votre connexion Direct Connect que vous VPCs pouvez tous 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 .

Pièces jointes de peering de passerelle de transit dans Amazon VPC Transit Gateways

Vous pouvez associer les passerelles de transit intra-régionales et interrégionales et acheminer le trafic entre elles, y compris le trafic et. IPv4 IPv6 Pour ce faire, créez un attachement d'appairage sur votre passerelle de transit et spécifiez une passerelle de transit. La passerelle de transit homologue peut se trouver dans votre compte ou provenir d'un autre compte. Vous pouvez également demander une pièce jointe de peering depuis votre propre compte vers une passerelle de transit d'un autre compte.

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 un ASNs système unique pour chaque passerelle de transit pair afin de tirer parti des futures capacités de propagation des itinéraires.

Le peering de passerelle de transit ne prend pas en charge la résolution de noms d'hôtes IPv4 DNS publics ou privés en IPv4 adresses privées situées de VPCs part et d'autre de la pièce jointe d'appairage de la passerelle de transit en utilisant le 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 chiffré deux fois sur les liaisons réseau échappant au 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 qui prennent en charge les pièces jointes d'appairage des passerelles de transport en commun, consultez la section FAQsPasserelles de AWS transit.

Considérations relatives à la AWS région d'inscription

Vous pouvez appairer des passerelles de transit au-delà des frontières de la région d'adhésion. Pour plus d'informations sur ces régions et sur la manière de s'y inscrire, consultez la section Gestion des AWS régions. 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 la pièce jointe au peering :
  - Compte AWS ID
  - 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.

Tâches

- Création d'une pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways
- Accepter ou rejeter une demande de pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways
- Ajouter un itinéraire à une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Supprimer une pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways

Création d'une pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways

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 une autre Compte AWS, assurez-vous d'avoir l' Compte AWS identifiant 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. Les passerelles de transport partagées avec vous ne sont pas disponibles pour le peering.
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 est différente 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 une pièce jointe de peering à l'aide du AWS CLI

Utilisez la commande create-transit-gateway-peering-attachment.

Accepter ou rejeter une demande de pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways

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 une pièce jointe de peering à l'aide du AWS CLI

Utilisez les commandes accept-transit-gateway-peering-attachment et reject-transit-gateway-peering-attachment.

Ajouter un itinéraire à une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 du 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 de plus amples informations, veuillez consulter the section called “Associer une table de routage de passerelle de transit”.

Supprimer une pièce jointe de peering à l'aide d'Amazon VPC Transit Gateways

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 une pièce jointe de peering à l'aide du AWS CLI

Utilisez la commande delete-transit-gateway-peering-attachment.

Connectez les pièces jointes et connectez les pairs dans Amazon VPC Transit Gateways

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 Transit Gateway Connect consiste en deux sessions de peering BGP se terminant sur AWS une infrastructure gérée. 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 homologue Connect fonctionne sans la double session d'appairage BGP 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 une pièce jointe Direct Connect comme mécanisme de transport, vous devez d'abord intégrer Direct Connect à AWS Transit Gateway. Pour les étapes de création de cette intégration, voir Intégrer des appareils SD-WAN à AWS Transit Gateway et. AWS Direct 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 CIDR /29 dans la `169.254.0.0/16` plage pour. IPv4 Vous pouvez éventuellement spécifier un bloc CIDR /125 dans la `fd00::/8` plage 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 IPv4 plage de l'appliance en tant qu'adresse IP BGP. Lorsque vous utilisez IPv6, si votre bloc CIDR interne 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 IPv6 adresse IPv4 OR, mais elle doit appartenir à la même famille d'adresses IP que l'adresse de la 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.

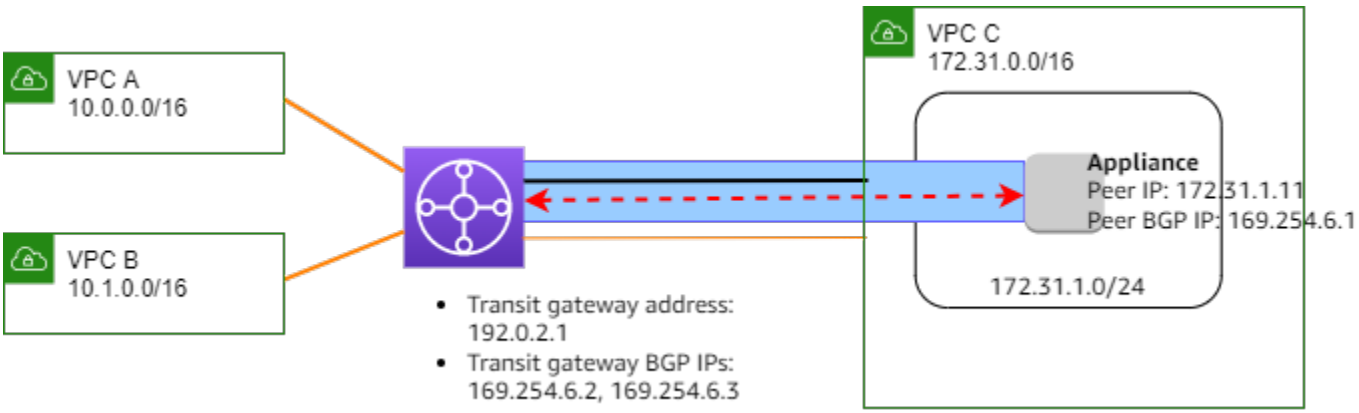
Vous pouvez ajouter un bloc d'adresse CIDR de passerelle de transit lorsque vous créez ou modifiez une passerelle de transit.

L'adresse IP peut être une IPv6 adresse IPv4 ou, mais elle doit appartenir à la même famille d'adresses IP que l'adresse IP du pair.

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 le peering BGP ne prend en charge que le protocole BGP multiprotocole (MP-BGP), où l'adressage Unicast est requis pour établir également une session BGP pour l' IPv4 Unicast. IPv6 Vous pouvez utiliser les deux IPv6 adresses IPv4 et pour les adresses IP externes GRE.

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 time-to-live (TTL) 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 homologue iBGP (appliance tierce), sauf si les routes proviennent d'un homologue eBGP et qu'elles auraient next-hop-self dû être configurées. 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 protocoles, tels que les familles d'adresses. IPv4 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.
- IPv6 Le peering BGP n'est pas pris en charge ; seul le peering BGP IPv4 basé est pris en charge. IPv6 les préfixes sont échangés via le peering IPv4 BGP à l'aide de 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.
- Configurez la MTU du tunnel GRE pour qu'elle soit inférieure à la MTU de l'interface externe en soustrayant la surcharge de l'en-tête GRE (8 octets) et de l'en-tête IP externe (20 octets). Par exemple, si le MTU de votre interface externe est de 1 500 octets, définissez le MTU du tunnel GRE sur 1 472 octets (1 500 - 8 - 20 = 1472) pour empêcher la fragmentation des paquets.

Tâches

- Création d'une pièce jointe Connect à l'aide d'Amazon VPC Transit Gateways
- Créez un pair Connect à l'aide d'Amazon VPC Transit Gateway
- Afficher les pièces jointes Connect et connecter les pairs à l'aide d'Amazon VPC Transit Gateway
- Modifiez la pièce jointe Connect et les balises d'homologue Connect à l'aide d'Amazon VPC Transit Gateways
- Supprimer un pair Connect à l'aide d'Amazon VPC Transit Gateways
- Supprimer une pièce jointe Connect à l'aide d'Amazon VPC Transit Gateways

Création d'une pièce jointe Connect à l'aide d'Amazon VPC Transit Gateways

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 attachement 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 attachement de la passerelle de transit).

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

Utilisez la commande create-transit-gateway-connect.

Créez un pair Connect à l'aide d'Amazon VPC Transit Gateway

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 les blocs CIDR BGP Inside IPv4, spécifiez la plage d' IPv4 adresses internes utilisées pour le peering BGP. Spécifiez un bloc d'adresse CIDR /29 dans la plage `169.254.0.0/16`.
8. (Facultatif) Pour les blocs BGP Inside CIDR IPv6, spécifiez la plage d' IPv6 adresses internes utilisées pour le peering 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 l'ASN homologue de manière à ce qu'il soit différent de l'ASN de la passerelle de transit (eBGP), vous devez configurer ebgp-multihop avec une time-to-live valeur (TTL) de 2.
10. Choisissez Create connect peer (Créer un pair Connect).

Pour créer un pair Connect à l'aide du AWS CLI

Utilisez la commande create-transit-gateway-connect-peer.

Afficher les pièces jointes Connect et connecter les pairs à l'aide d'Amazon VPC Transit Gateway

Consultez vos pièces jointes Connect et vos homologues 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 consulter vos pièces jointes Connect et vos homologues Connect à l'aide du AWS CLI

Utilisez les commandes describe-transit-gateway-connectsset describe-transit-gateway-connect-peers.

Modifiez la pièce jointe Connect et les balises d'homologue Connect à l'aide d'Amazon VPC Transit Gateways

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 (Attachements de la passerelle de transit).
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 à l'aide d'Amazon VPC Transit Gateways

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 du AWS CLI

Utilisez la commande delete-transit-gateway-connect-peer.

Supprimer une pièce jointe Connect à l'aide d'Amazon VPC Transit Gateways

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 une pièce jointe Connect à l'aide du AWS CLI

Utilisez la commande delete-transit-gateway-connect.

Tables de routage des passerelles de transit dans Amazon VPC Transit Gateways

Utilisez les tables de routage de passerelle de transit pour configurer l'acheminement de vos réseaux de transit par passerelle. Une table de routage est une table qui contient des règles qui régissent la manière dont le trafic réseau est acheminé entre votre VPCs et VPNs. Chaque itinéraire du tableau contient la plage d'adresses IP pour les destinations vers lesquelles vous souhaitez envoyer du trafic.

Les tables de routage de passerelle de transit vous permettent d'associer une table à une pièce jointe de passerelle de transit. Les pièces jointes VPC, VPN, Direct Connect, Peering et Connect sont toutes prises en charge. Lorsqu'ils sont associés, les itinéraires de ces pièces jointes sont propagés depuis la pièce jointe vers la table de routage de la passerelle de transit cible. Une pièce jointe peut être propagée à plusieurs tables de routage.

En outre, vous pouvez créer et gérer des itinéraires statiques à l'aide d'une table de routage. Par exemple, vous pouvez avoir un itinéraire statique utilisé comme itinéraire de secours en cas de perturbation du réseau affectant les itinéraires dynamiques.

Tâches

- Création d'une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Afficher les tables de routage des passerelles de transit à l'aide d'Amazon VPC Transit Gateways
- Associez une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Supprimer une association pour une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Activez la propagation d'itinéraires vers une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Désactiver la propagation d'itinéraires à l'aide d'Amazon VPC Transit Gateway
- Créez un itinéraire statique à l'aide d'Amazon VPC Transit Gateway
- Supprimer un itinéraire statique à l'aide d'Amazon VPC Transit Gateways
- Remplacer un itinéraire statique à l'aide des passerelles Amazon VPC Transit
- Exportez des tables de routage vers Amazon S3 à l'aide d'Amazon VPC Transit Gateway
- Supprimer une table de routage d'une passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Créez une référence de liste de préfixes de table de routage à l'aide d'Amazon VPC Transit Gateways

- Modifier une référence de liste de préfixes à l'aide d'Amazon VPC Transit Gateways
- Supprimer une référence de liste de préfixes à l'aide d'Amazon VPC Transit Gateways

Création d'une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 des passerelles de transit à l'aide d'Amazon VPC Transit Gateways

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 itinéraires 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.

Associez une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 à l'aide d'Amazon VPC Transit Gateways

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.

Activez la propagation d'itinéraires vers une table de routage de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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.

Désactiver la propagation d'itinéraires à l'aide d'Amazon VPC Transit Gateway

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.

Créez un itinéraire statique à l'aide d'Amazon VPC Transit Gateway

Créez un itinéraire statique pour une pièce jointe à un VPC, un VPN ou une passerelle de transit, ou vous pouvez créer un itinéraire en trou noir qui supprime le trafic correspondant à l'itinéraire.

Les itinéraires statiques d'une table de routage de passerelle de transit qui ciblent un rattachement VPN ne sont pas filtrés par le 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 itinéraire statique à l'aide d'Amazon VPC Transit Gateways

Supprimez les itinéraires statiques d'une table de routage d'une 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.

Remplacer un itinéraire statique à l'aide des passerelles Amazon VPC Transit

Remplacez un itinéraire statique dans une table de routage de 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.

Exportez des tables de routage vers Amazon S3 à l'aide d'Amazon VPC Transit Gateway

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 itinéraires exportés, ouvrez la console Amazon S3 à l'https://console.aws.amazon.com/s3/adresse et accédez au compartiment que vous avez spécifié. Le nom du fichier inclut l' Compte AWS ID, la AWS région, l'ID de la 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 d'une passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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.

Créez une référence de liste de préfixes de table de routage à l'aide d'Amazon VPC Transit Gateways

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 la même destination CIDRs sur plusieurs tables de routage de passerelles de transit, vous pouvez les gérer CIDRs dans une seule liste de préfixes, au lieu de les référencer à plusieurs reprises CIDRs 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.

Pour créer une référence de liste de préfixes 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 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 du AWS CLI

Utilisez la commande create-transit-gateway-prefix-list-reference.

Modifier une référence de liste de préfixes à l'aide d'Amazon VPC Transit Gateways

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 à l'adresse 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 du AWS CLI

Utilisez la commande modify-transit-gateway-prefix-list-reference.

Supprimer une référence de liste de préfixes à l'aide d'Amazon VPC Transit Gateways

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 à l'adresse 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 modifier une référence de liste de préfixes à l'aide du AWS CLI

Utilisez la commande delete-transit-gateway-prefix-list-reference.

Tableaux des politiques relatives aux passerelles de transit dans Amazon VPC Transit Gateways

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.

Tâches

- Création d'une table de politique de passerelle de transit à l'aide d'Amazon VPC Transit Gateways
- Supprimer une table de politique de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

Création d'une table de politique de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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 politique de passerelle de transit à l'aide d'Amazon VPC Transit Gateways

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.

Multidiffusion dans les passerelles de transit Amazon VPC

Le multicast est un protocole de communication utilisé pour fournir un flux unique de données à plusieurs ordinateurs de réception simultanément. Transit Gateway prend en charge le routage du trafic multicast entre les sous-réseaux connectés VPCs et sert de routeur multicast pour les instances envoyant du trafic destiné à plusieurs instances de réception.

Rubriques

- Concepts du multicast
- Considérations
- Routage multidiffusion
- Domaines de multidiffusion dans Amazon VPC Transit Gateway
- Domaines de multidiffusion partagés dans Amazon VPC Transit Gateway
- Enregistrez des sources auprès d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateways
- Enregistrez les membres d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateways
- Désenregistrer les sources d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateway
- Désenregistrer les membres d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateway
- Afficher les groupes de multidiffusion à l'aide des passerelles Amazon VPC Transit
- Configuration de la multidiffusion pour Windows Server dans Amazon VPC Transit Gateway
- Exemple : gestion des configurations IGMP à l'aide des passerelles Amazon VPC Transit
- Exemple : gestion des configurations de sources statiques à l'aide d'Amazon VPC Transit Gateways
- Exemple : gestion des configurations statiques des membres de groupes dans Amazon VPC Transit Gateways

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 multidiffusion est définie par des interfaces réseau élastiques individuelles associées aux EC2 instances.
- 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 joindre, quitter et envoyer des messages. AWS prend en charge le IGMPv2 protocole et les domaines de multidiffusion IGMP et statiques (basés sur des API) à des groupes.

- Source de multidiffusion : interface réseau élastique associée à une EC2 instance prise en charge configurée de manière statique pour envoyer du trafic de multidiffusion. 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 de multidiffusion : interface réseau élastique associée à une EC2 instance prise en charge qui reçoit du trafic de multidiffusion. 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

- La multidiffusion par passerelle de transit peut ne pas convenir aux transactions à haute fréquence ou aux applications sensibles aux performances. Nous vous recommandons vivement de consulter les quotas de multidiffusion pour connaître les limites. Contactez votre compte ou l'équipe d'architectes de solutions pour un examen détaillé de vos exigences de performance.
- Pour plus d'informations sur les régions prises en charge, consultez AWS Transit Gateway FAQs.
- 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 que Nitro, vous devez désactiver la case Source/Dest. 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 EC2 l'utilisateur Amazon.
- Une instance autre qu'une instance Nitro ne peut pas être un expéditeur multicast.
- Le routage multicast n'est pas pris en charge sur les pièces jointes Site-to-Site VPN 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 de plus amples informations, veuillez consulter Unité de transmission maximale (MTU).
- Au démarrage, un hôte IGMP envoie plusieurs IGMP JOIN messages pour rejoindre un groupe de multidiffusion (généralement 2 à 3 tentatives). Dans le cas peu probable où tous les IGMP JOIN les messages sont perdus, l'hôte ne fera pas partie du groupe de multidiffusion de la passerelle de transit. Dans un tel scénario, vous devrez redéclencher l'IGMP JOIN message de l'hôte utilisant des méthodes spécifiques à l'application.
- L'adhésion à un groupe commence par la réception de IGMPv2 JOIN message envoyé par la passerelle de transit et se termine par la réception du IGMPv2 LEAVE message. La passerelle de transit assure le suivi des hôtes qui ont réussi à rejoindre le groupe. En tant que routeur multidiffusion dans le cloud, la passerelle de transit émet un IGMPv2 QUERY message à tous les membres toutes les deux minutes. Chaque membre envoie un IGMPv2 JOIN message 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 explicite IGMPv2 LEAVE ce message supprime immédiatement et définitivement l'hôte de tout autre traitement de multidiffusion.
- 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, la passerelle de transit continue d'envoyer des données de multidiffusion à l'hôte pendant sept minutes (420 secondes) après le dernier IGMP réussi JOIN message. La passerelle de transit continue d'envoyer des demandes d'adhésion à l'hôte pendant 12 heures maximum ou jusqu'à ce qu'il reçoive un IGMP. LEAVE message 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. La configuration de votre groupe de sécurité sur les hôtes IGMP (instances) et toute ACLs configuration sur les sous-réseaux hôtes doivent autoriser ces messages du 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 de multidiffusion statiques, Amazon VPC Transit Gateway supprime automatiquement les groupes statiques et les sources ENIs qui n'existent plus. Cela se fait en assumant périodiquement le rôle lié au service Transit Gateway à décrire ENIs dans le compte.
- Seule la multidiffusion statique est prise en charge IPv6. La multidiffusion dynamique ne fonctionne pas.

Routage multidiffusion

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.

Réseau ACLs

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 la section Réseau ACLs 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

Type	Protocole	Destination	Description
Protocole UDP personnalisé	UDP	Adresse IP du groupe multicast	Trafic multicast sortant

Domaines de multidiffusion dans Amazon VPC Transit Gateway

Un domaine de multidiffusion permet de segmenter un réseau de multidiffusion en différents domaines. Pour commencer à utiliser le multicast avec une passerelle de transit, créez un domaine multicast, puis associez des sous-réseaux au domaine.

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) IGMPv2 support (console)	Cet attribut détermine la façon dont les membres du groupe rejoignent ou quittent un groupe multicast. Lorsque cet attribut est désactivé, vous devez ajouter les membres du groupe au domaine manuellement. Activez cet attribut si au moins un membre utilise le protocole IGMP. Les membres rejoignent le groupe multicast de l'une des manières suivantes : • Les membres qui prennent en charge IGMP utilisent les messages `JOIN` et `LEAVE`. • 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. Si vous enregistrez des membres de groupes multicast, vous devez également les désenregistrer. La passerelle de transit

Attribut	Description
	ignore un message IGMP LEAVE envoyé par un membre du groupe ajouté manuellement.
`StaticSourcesSupport` (AWS CLI) Prise en charge des sources statiques (console)	Cet attribut détermine s'il existe des sources multicast statiques pour le groupe. Lorsque cet attribut est activé, vous devez ajouter des sources pour un domaine de multidiffusion à l'aide de register-transit-gateway-multicast-group-sources. Seules les sources multicast peuvent envoyer du trafic multicast. 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.

Créez un domaine de multidiffusion IGMP à l'aide d'Amazon VPC Transit Gateway

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 “Domaines de multidiffusion”.

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 obtenir de l'IGMPv2 aide, cochez la case.
7. Pour la prise en charge des sources statiques, décochez la case.

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).

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 de multidiffusion source statique à l'aide d'Amazon VPC Transit Gateways

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 “Domaines de multidiffusion”.

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 obtenir de l'IGMPv2 aide, décochez la case.
7. Pour la prise en charge des sources statiques, cochez la case.
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).

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 pièces jointes et des sous-réseaux VPC à un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateways

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 Pièces jointes Amazon VPC dans Amazon VPC Transit Gateway.

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.

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.

Dissocier un sous-réseau d'un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateway

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

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).

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

Utilisez la commande disassociate-transit-gateway-multicast-domain.

Afficher les associations de domaines de multidiffusion à l'aide d'Amazon VPC Transit Gateway

Consultez vos domaines de multidiffusion pour vérifier qu'ils sont disponibles et qu'ils contiennent les sous-réseaux et les pièces jointes appropriés.

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 .

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

Utilisez la commande describe-transit-gateway-multicast-domains.

Ajouter des balises à un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateways

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 plus d'informations, consultez la section Marquage de vos EC2 ressources Amazon.

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 Save (Enregistrer).

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

Utilisez la commande create-tags.

Supprimer un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateways

Utilisez la procédure suivante pour supprimer un domaine multicast.

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).

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

Utilisez la commande delete-transit-gateway-multicast-domain.

Domaines de multidiffusion partagés dans Amazon VPC Transit Gateway

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. Une fois le partage effectué, ces utilisateurs peuvent effectuer les opérations suivantes sur un domaine de multidiffusion 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 :

- AWS comptes au sein de son organisation ou entre organisations dans AWS Organizations
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- Toute son organisation en AWS Organizations
- AWS comptes extérieurs à AWS Organizations.

  Pour partager un domaine de multidiffusion avec un AWS compte externe à votre organisation, vous devez créer un partage de ressources à l'aide de AWS Resource Access Manager, puis choisir Autoriser le partage avec n'importe qui lorsque vous sélectionnez les principaux avec lesquels 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
- Autorisations des domaines multicast partagés
- Facturation et mesures
- Quotas

- Partagez les ressources entre les zones de disponibilité dans Amazon VPC Transit Gateway
- Partagez un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateways
- Annuler le partage d'un domaine de multidiffusion partagé à l'aide d'Amazon VPC Transit Gateways
- Identifiez un domaine de multidiffusion partagé à l'aide d'Amazon VPC Transit Gateways

Conditions préalables au partage d'un domaine multicast

- Pour partager un domaine de multidiffusion, vous devez en être le propriétaire dans votre AWS compte. Vous ne pouvez pas partager un domaine multicast qui a été partagé avec vous.
- Pour partager un domaine de multidiffusion avec votre organisation ou une unité organisationnelle 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 à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte 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 indique les ressources à partager et les utilisateurs avec lesquels les partager. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou une organisation entière AWS Organizations.

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

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 les ressources créées par les consommateurs sur des domaines de multidiffusion partagés.

Autorisations accordées aux consommateurs

Les utilisateurs du domaine de multidiffusion partagé peuvent effectuer les opérations suivantes sur les domaines de multidiffusion partagés de la même manière que sur les domaines de multidiffusion 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 de multidiffusion partagé est pris en compte dans les quotas de domaine de multidiffusion du propriétaire et de l'utilisateur partagé.

Partagez les ressources entre les zones de disponibilité dans Amazon VPC Transit Gateway

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, Amazon VPC Transit Gateway associe 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, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

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'AZ ID est un identifiant unique et cohérent pour une zone de disponibilité pour tous les AWS comptes. Par exemple, `use1-az1` il s'agit d'un identifiant AZ pour la `us-east-1` région et il s'agit du même emplacement dans tous les AWS comptes.

Pour consulter l'AZ IDs des zones de disponibilité de votre compte

1. Ouvrez la AWS RAM console à la https://console.aws.amazon.com/ram/maison.
2. L'AZ IDs de la région actuelle s'affiche dans le panneau Your AZ ID sur le côté droit de l'écran.

Partagez un domaine de multidiffusion à l'aide d'Amazon VPC Transit Gateways

Lorsqu'un propriétaire partage un domaine de multidiffusion avec vous, vous pouvez effectuer les opérations suivantes :

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

> **Note**
>
> Pour partager un domaine multicast, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez un domaine de multidiffusion à l'aide du 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 AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès au domaine de multidiffusion 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 de multidiffusion dont vous êtes propriétaire à l'aide de la Amazon Virtual Private Cloud console, de AWS RAM la console ou du 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 à l'adresse 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 de multidiffusion dont vous êtes propriétaire 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 de multidiffusion dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Annuler le partage d'un domaine de multidiffusion partagé à l'aide d'Amazon VPC Transit Gateways

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. Vous pouvez le faire à partir de la AWS RAM console ou du AWS CLI.

Pour annuler le partage d'un domaine multicast partagé qui vous appartient, vous devez le supprimer du partage de ressources. Vous pouvez le faire à l'aide Amazon Virtual Private Cloud de AWS RAM la console ou du 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 à l'adresse 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 de multidiffusion partagé dont vous êtes propriétaire à l'aide de la console AWS 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 de multidiffusion partagé dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identifiez un domaine de multidiffusion partagé à l'aide d'Amazon VPC Transit Gateways

Les propriétaires et les consommateurs peuvent identifier les domaines de multidiffusion partagés à l'aide des Amazon Virtual Private Cloud AWS CLI

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

1. Ouvrez la console Amazon VPC à l'adresse 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 de multidiffusion en transit, consultez l'identifiant du propriétaire pour identifier l'identifiant de AWS compte du domaine de multidiffusion.

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

Utilisez la commande describe-transit-gateway-multicast-domains. La commande renvoie les domaines de multidiffusion que vous possédez et les domaines de multidiffusion partagés avec vous. `OwnerId`indique l'ID de AWS compte du propriétaire du domaine de multidiffusion.

Enregistrez des sources auprès d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateways

> **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 IDs interfaces réseau des sources
- Adresse IP du groupe multicast

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 l'adresse IP du groupe, entrez le bloc IPv4 CIDR ou le bloc IPv6 CIDR à attribuer au domaine de multidiffusion.
5. Sous Choose network interfaces (Choisir des interfaces réseau), sélectionnez les interfaces réseau des utilisateurs multicast.
6. Choisissez Add sources (Ajouter des sources).

Pour enregistrer des sources à l'aide du AWS CLI

Utilisez la commande register-transit-gateway-multicast-group-sources.

Enregistrez les membres d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateways

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 IDs interfaces réseau des membres du groupe
- Adresse IP du groupe multicast

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 l'adresse IP du groupe, entrez le bloc IPv4 CIDR ou le bloc IPv6 CIDR à attribuer au domaine de multidiffusion.
5. Sous Choose network interfaces (Choisir des interfaces réseau), sélectionnez les interfaces réseau des récepteurs multicast.
6. Choisissez Add members (Ajouter des membres).

Pour enregistrer des membres à l'aide du AWS CLI

Utilisez la commande register-transit-gateway-multicast-group-members.

Désenregistrer les sources d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateway

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

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).

Pour supprimer une source à l'aide du AWS CLI

Utilisez la commande deregister-transit-gateway-multicast-group-sources.

Désenregistrer les membres d'un groupe de multidiffusion à l'aide d'Amazon VPC Transit Gateway

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

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).

Pour désenregistrer des membres à l'aide du AWS CLI

Utilisez la commande deregister-transit-gateway-multicast-group-members.

Afficher les groupes de multidiffusion à l'aide des passerelles Amazon VPC Transit

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

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).

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"
        }
    ]
}
```

Configuration de la multidiffusion pour Windows Server dans Amazon VPC Transit Gateway

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. Pour configurer cela PowerShell, vous devez utiliser et exécuter les commandes suivantes :

Pour configurer la multidiffusion pour Windows Server à l'aide de PowerShell

1. Modifiez Windows Server à utiliser IGMPv2 plutôt que 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 d'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' EC2 instance.
5. Testez votre application multicast pour vous assurer que le trafic circule normalement.

Exemple : gestion des configurations IGMP à l'aide des passerelles Amazon VPC Transit

Cet exemple montre au moins un hôte qui utilise le protocole IGMP pour le trafic de multidiffusion. AWS crée automatiquement le groupe de multidiffusion lorsqu'il reçoit un `JOIN` message IGMP d'une instance, puis ajoute l'instance en tant que membre dans 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 plus d'informations, consultez Créer un VPC dans le Guide de l'utilisateur Amazon VPC.
2. Créez un sous-réseau dans le VPC. Pour plus d'informations, consultez la section Créer un sous-réseau 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 “Création d'une pièce jointe 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 de multidiffusion IGMP”.

   Utilisez les paramètres suivants :

   - Activez IGMPv2 le support.
   - 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 plus d'informations, voir 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 “Inscrire des membres auprès d'un groupe de multidiffusion”.

Exemple : gestion des configurations de sources statiques à l'aide d'Amazon VPC Transit Gateways

Cet exemple ajoute de manière statique des sources de multidiffusion 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 plus d'informations, consultez Créer un VPC dans le Guide de l'utilisateur Amazon VPC.
2. Créez un sous-réseau dans le VPC. Pour plus d'informations, consultez la section Créer un sous-réseau 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 “Création d'une pièce jointe 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 de multidiffusion source statique”.

   Utilisez les paramètres suivants :

   - Désactivez IGMPv2 le support.
   - 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 “Enregistrer les sources avec un groupe de multidiffusion”.
8. Ajoutez les membres au groupe multicast. Pour de plus amples informations, veuillez consulter the section called “Inscrire des membres auprès d'un groupe de multidiffusion”.

Exemple : gestion des configurations statiques des membres de groupes dans Amazon VPC Transit Gateways

Cet exemple montre l'ajout statique de membres de multidiffusion 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 plus d'informations, consultez Créer un VPC dans le Guide de l'utilisateur Amazon VPC.
2. Créez un sous-réseau dans le VPC. Pour plus d'informations, consultez la section Créer un sous-réseau 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 “Création d'une pièce jointe 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 de multidiffusion source statique”.

   Utilisez les paramètres suivants :

   - Désactivez IGMPv2 le support.
   - 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 “Inscrire des membres auprès d'un groupe de multidiffusion”.

Journaux de flux des passerelles Amazon VPC Transit

Transit Gateway Flow Logs est une fonctionnalité d'Amazon VPC Transit Gateways qui vous permet de capturer des informations sur le trafic IP à destination et en provenance de 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 des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre ordinateur VPCs, 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 de plus amples informations, veuillez consulter 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.

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, veuillez consulter Supprimer un enregistrement des journaux de flux Amazon VPC Transit Gateways.

Vous pouvez créer des journaux de flux pour vos passerelles de transit qui peuvent publier des données sur CloudWatch Logs, Amazon S3 ou Amazon Data Firehose. Pour plus d'informations, consultez les ressources suivantes :

- Créez 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

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 du texte brut, tous les champs sont de type STRING. Si le format est Parquet, consultez le tableau pour les types de données des champs.

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 TransitGateway. 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.	6

Champ	Description	Version
	Type de données Parquet : CHAÎNE	
tgw-src-subnet-id	ID du sous-réseau pour le trafic source de la passerelle de transit. Type de données Parquet : CHAÎNE	6
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

Champ	Description	Version
srcaddr	Adresse source du trafic entrant. Type de données Parquet : CHAÎNE	2
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 Assigned Internet Protocol Numbers). Type de données Parquet : INT_32	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

Champ	Description	Version
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
log-status	Statut du journal de flux : • OK — Les données sont consignées normalement dans les destinations choisies. • PASDEDONNÉES — Il n'y a eu aucun trafic réseau depuis ou vers l'interface réseau pendant l'intervalle d'agrégation. • 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. Type de données Parquet : CHAÎNE	2
type	Type de trafic. Les valeurs possibles sont IPv4 | IPv6 | EFA. Pour plus d'informations, consultez Elastic Fabric Adapter dans le guide de EC2 l'utilisateur Amazon. Type de données Parquet : CHAÎNE	3
packets-lost-no-route	Paquets perdus en raison de l'absence de route spécifiée. Type de données Parquet : INT_64	6
packets-lost-blackhole	Paquets perdus en raison d'un trou noir. Type de données Parquet : INT_64	6
packets-lost-mtu-exceeded	Paquets perdus en raison d'une taille supérieure à la MTU. Type de données Parquet : INT_64	6

Champ	Description	Version
packets-lost-ttl-expired	Les paquets ont été perdus en raison de l'expiration de time-to-live. Type de données Parquet : INT_64	6
tcp-flags	Valeur de masque de bits pour les indicateurs TCP suivants : • FIN : 1 • SYN : 2 • RST : 4 • PSH — 8 • ACK — 16 • SYN-ACK : 18 • URG — 32 **Important** Lorsqu'une entrée du journal de flux se compose uniquement de paquets ACK, la valeur de l'indicateur est 0, et non 16. Pour des informations générales sur les indicateurs TCP (comme la signification des indicateurs tels que FIN, SYN et ACK), consultez Structure d'un segment TCP sur Wikipédia. 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. Type de données Parquet : INT_32	3
region	Région contenant la passerelle de transit où le trafic est enregistré. Type de données Parquet : CHAÎNE	4

Champ	Description	Version
flow-direction	La direction du flux par rapport à l'interface où le trafic est capturé. Les valeurs possibles sont : ingress | egress. Type de données Parquet : CHAÎNE	5
pkt-src-aws-service	Le nom du sous-ensemble des plages d'adresses IP du srcaddr si l'adresse IP source est celle d'un AWS service. Les valeurs possibles sont : AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Type de données Parquet : CHAÎNE	5
pkt-dst-aws-service	Le nom du sous-ensemble des plages d'adresses IP du dstaddr champ, si l'adresse IP de destination est pour un AWS service. Pour obtenir une liste des valeurs possibles, consultez le champ pkt-src-aws-service . Type de données Parquet : CHAÎNE	5

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 plus d'informations, consultez la section Accorder aux utilisateurs IAM les autorisations requises pour Amazon EC2 Resources dans le manuel Amazon EC2 API Reference.

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 plus d'informations, consultez Enregistrements de Transit Gateway Flow Logs dans Amazon CloudWatch Logs et Enregistrements des journaux de flux des passerelles de transit dans Amazon S3 .

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.

Création ou mise à jour d'un rôle IAM pour les journaux de flux d'Amazon VPC Transit Gateway

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 à l'aide de la AWS Identity and Access Management console.

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 . Dans Cas d'utilisation, sélectionnez 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 Review policy (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.

Enregistrements de Transit Gateway Flow Logs dans Amazon 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 enregistrement Transit Gateways Flow Logs qui sera publié sur Amazon CloudWatch Logs
- Afficher les enregistrements des journaux de flux de Transit Gateway sur Amazon CloudWatch
- Traitez les enregistrements des journaux de flux de Transit Gateway dans Amazon 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"
    }
}
```

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 enregistrement Transit Gateways Flow Logs qui sera publié sur Amazon 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 de plus amples informations, veuillez consulter Autorisations pour les utilisateurs IAM pour transmettre un rôle.

Vous pouvez créer un journal de CloudWatch flux Amazon à l'aide de la console Amazon VPC ou de la CLI AWS .

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/
2. Dans le panneau de navigation, choisissez Transit gateways (Passerelles de transit).
3. Cochez les cases correspondant à une ou plusieurs passerelles de transit, puis choisissez Actions, 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-EC2FlowLog (AWS Tools for Windows PowerShell)

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
```

Afficher les enregistrements des journaux de flux de Transit Gateway sur Amazon CloudWatch

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/.
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 de plus amples informations, veuillez consulter Enregistrements Transit Gateway Flow Logs.

Traitez les enregistrements des journaux de flux de Transit Gateway dans Amazon 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 des journaux et des filtres de mesures, consultez la section Création de métriques à partir d'événements de journal à l'aide de filtres 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/.
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux).
3. Cochez la case correspondant au groupe de journaux, puis choisissez Actions, Créer un filtre 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 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).

Enregistrements des journaux de flux des passerelles de transit dans 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, consultez la section Créer un compartiment dans le guide de l'utilisateur Amazon S3.

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
- Création du rôle de compte source Transit Gateway Flow Logs pour Amazon S3
- Créez un enregistrement Transit Gateway Flow Logs qui sera publié sur Amazon S3
- Afficher les enregistrements des journaux de flux de Transit Gateway dans Amazon S3
- Enregistrements du journal de flux traités 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 nouvelle politique générée automatiquement est ajoutée à la politique d'origine.

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 les politiques relatives aux compartiments dans le guide de l'utilisateur d'Amazon Simple Storage Service.

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

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

L'ARN que vous spécifiez *my-s3-arn* dépend de l'utilisation de préfixes S3 compatibles avec Hive ou non.

- 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/*
```

Il est recommandé d'accorder ces autorisations au principal du service de livraison des journaux plutôt qu'à un individu Compte AWS ARNs. 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.

> **Note**
>
> L'utilisation de clés de compartiment S3 vous permet de réduire les coûts liés aux demandes AWS Key Management Service (AWS KMS) en réduisant vos AWS KMS demandes aux opérations de chiffrement et de déchiffrement grâce à l'utilisation d'une clé au niveau du compartiment. GenerateDataKey De par leur conception, les demandes ultérieures qui tirent parti de cette clé au niveau du compartiment n'entraînent pas de demandes d' AWS KMS API et ne valident pas l'accès par rapport à la politique de AWS KMS clé.

```
{
    "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 politiques de compartiment requises, Amazon S3 utilise des listes de contrôle d'accès (ACLs) pour 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 plus d'informations, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Création du rôle de compte source Transit Gateway Flow Logs pour Amazon S3

À partir du compte source, créez le rôle source dans la AWS Identity and Access Management console.

Pour créer le rôle du compte source

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet 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.

Créez un enregistrement Transit Gateway Flow Logs qui sera publié sur Amazon S3

Une fois votre compartiment Amazon S3 créé et configuré, vous pouvez créer des journaux de flux pour les passerelles de transit. Vous pouvez créer un journal de flux Amazon S3 à l'aide de la console Amazon VPC ou de la CLI AWS .

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 me 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-EC2FlowLog (AWS Tools for Windows PowerShell)

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic de passerelle de transit pour VPC `tgw-00112233344556677` et transmet 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/'
```

Afficher les enregistrements des journaux de flux de Transit Gateway dans Amazon S3

Pour afficher des enregistrements de journal de flux publiés dans Amazon S3

1. Ouvrez la console Amazon S3 à l'adresse 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 Nom, cochez la case à côté du fichier journal. Dans le panneau de présentation de l'objet, choisissez Download(Télécharger).

Enregistrements du journal de flux traités 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.

Les enregistrements de Transit Gateway Flow dans Amazon Data Firehose

Rubriques

- Rôles IAM pour la diffusion entre comptes
- Création du rôle de compte source Transit Gateway Flow Logs pour Amazon Data Firehose
- Créez le rôle de compte de destination Transit Gateway Flow Logs pour Amazon Data Firehose
- Créez un enregistrement Transit Gateway Flow Logs qui sera publié sur Amazon Data 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.

Tarification

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 VPCs interfaces réseau ou les sous-réseaux que vous surveillez à l'aide de la clé `iam:AssociatedResourceARN` de condition.

```
{
  "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"
    }
  ]
}
```

Rôle du compte de destination

Dans le compte de destination, créez un rôle dont le nom commence par AWSLogDeliveryFirehoseCrossAccountRole. 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"
    }
  ]
}
```

Création du rôle de compte source Transit Gateway Flow Logs pour Amazon Data Firehose

À partir du compte source, créez le rôle source dans la AWS Identity and Access Management console.

Pour créer le rôle du compte source

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet 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.

Créez le rôle de compte de destination Transit Gateway Flow Logs pour Amazon Data Firehose

À partir du compte de destination, créez le rôle de destination dans la AWS Identity and Access Management console.

Pour créer le rôle du compte de destination

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet 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 enregistrement Transit Gateway Flow Logs qui sera publié sur Amazon Data Firehose

Créez un journal de flux Transit Gateway qui sera publié sur Amazon Data Firehose. Avant de créer le journal de flux, assurez-vous d'avoir configuré les rôles de compte IAM source et de destination pour la diffusion entre comptes et que vous avez créé le flux de diffusion Firehose. Pour plus d'informations, consultez Journaux de flux Amazon Data Firehose. Vous pouvez créer un journal de flux Firehose à l'aide de la console Amazon VPC ou de la CLI. AWS

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-EC2FlowLog (AWS Tools for Windows PowerShell)

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
```

Créez et gérez les journaux de flux Amazon VPC Transit Gateway à l'aide APIs de la CLI

Vous pouvez effectuer les tâches décrites sur cette page à l'aide de la ligne de commande.

Les limites suivantes s'appliquent lors de l'utilisation de la create-flow-logscommande :

- `--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)

Décrire vos journaux de flux

- describe-flow-logs (AWS CLI)

- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Afficher vos enregistrements de journaux de flux (événements de journaux)

- get-log-events (AWS CLI)
- CWLLogÉvénement Get (AWS Tools for Windows PowerShell)

Supprimer un journal de flux

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

Afficher les enregistrements des journaux de flux Amazon VPC Transit Gateway

Consultez les informations relatives aux journaux de flux de votre passerelle de transit via Amazon VPC. Lorsque vous choisissez une ressource, tous les journaux de flux associés à 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.

Gérer les balises Flow Logs d'Amazon VPC Transit Gateway

Vous pouvez ajouter ou supprimer des balises pour 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 (Enregistrer).

Rechercher dans les enregistrements des journaux de flux Amazon VPC Transit Gateway

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/.
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 enregistrement des journaux de flux Amazon VPC Transit Gateways

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, la suppression d'un journal de flux publié sur Amazon S3 ne supprime pas les politiques de compartiment ni les listes de contrôle d'accès aux fichiers journaux (ACLs).

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).

Mesures et événements dans Amazon VPC Transit Gateways

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.

CloudWatch métriques

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 séries chronologiques, appelées métriques. Vous pouvez utiliser ces métriques pour vérifier que le système fonctionne comme prévu. Pour de plus amples informations, veuillez consulter CloudWatch métriques dans Amazon VPC Transit Gateways.

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 sur le trafic à destination et en provenance de ceux VPCs qui sont attachés à vos passerelles de transit. Pour plus d'informations, consultez la rubrique Journaux de flux VPC dans le Guide de l'utilisateur Amazon VPC.

CloudTrail journaux

Vous pouvez l'utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels passés à l'API de la passerelle de transit et les stocker sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser ces CloudTrail journaux pour déterminer quels appels ont été passés, l'adresse IP source d'où provient l'appel, qui a effectué l'appel, quand l'appel a été passé, etc. Pour de plus amples informations, veuillez consulter CloudTrail journaux.

CloudWatch Événements à l'aide de 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 à l'aide d' CloudWatch événements dans le guide de l'utilisateur des réseaux AWS mondiaux pour les passerelles de transit.

CloudWatch métriques dans Amazon VPC Transit Gateways

Amazon VPC publie des points de données sur Amazon CloudWatch pour vos passerelles de transit et les pièces jointes de vos passerelles de transit. CloudWatchvous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de 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 CloudWatch alarme pour surveiller une métrique spécifiée et lancer une action (telle que l'envoi d'une notification à une adresse e-mail) si la métrique dépasse ce que vous considérez comme une plage acceptable.

Amazon VPC mesure et envoie ses métriques à des intervalles de CloudWatch 60 secondes.

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

- Métriques de passerelle de transit
- Mesures relatives au niveau de la pièce jointe et à la zone de disponibilité
- Dimensions métriques de la passerelle de transit

Métriques de passerelle de transit

L'espace de noms `AWS/TransitGateway` inclut les métriques suivantes.

Toutes les mesures sont toujours rapportées. Leurs valeurs dépendent du trafic passant par la passerelle de transit. Voir Dimensions métriques de la passerelle de transit pour les dimensions prises en charge.

Métrique	Description
`BytesDropCountBlackhole`	Nombre d'octets abandonnés en raison de la correspondance avec une route `blackhole` . Statistiques : la seule statistique significative est `Sum`.
`BytesDropCountNoRoute`	Nombre d'octets abandonnés en raison de la non-correspondance avec une route. Statistiques : la seule statistique significative est `Sum`.
`BytesIn`	Nombre d'octets reçus par la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`BytesOut`	Nombre d'octets envoyés depuis la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`PacketsIn`	Nombre de paquets reçus par la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`PacketsOut`	Nombre de paquets envoyés par la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountBlackhole`	Nombre de paquets abandonnés à cause d'une correspondance avec une route `blackhole` . Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountNoRoute`	Nombre de paquets abandonnés à cause d'une non-correspondance avec une route. Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountTTLExpired`	Le nombre de paquets abandonnés en raison de l'expiration du TTL. Statistiques : la seule statistique significative est `Sum`.

Mesures relatives au niveau de la pièce jointe et à la zone de disponibilité

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”.

Les métriques de zone de disponibilité sont disponibles si elles sont activées pour les zones de disponibilité (AZs) sur les pièces jointes aux passerelles de transit. Seules les pièces jointes VPC prennent en charge les métriques Per-AZ. Toutes les mesures de niveau AZ sont publiées sur le compte du propriétaire de la passerelle de transit. Les statistiques AZ individuelles pour une pièce jointe sont également publiées sur le compte du propriétaire de la pièce jointe. Le propriétaire de la pièce jointe peut uniquement consulter les mesures par AZ pour sa propre pièce jointe.

Toutes les mesures sont toujours rapportées. Leurs valeurs dépendent du trafic entrant et/ou sortant de la pièce jointe de la passerelle de transit. Voir Dimensions métriques de la passerelle de transit pour les dimensions prises en charge.

Métrique	Description
`BytesDropCountBlackhole`	Nombre d'octets abandonnés en raison de la correspondance avec une route `blackhole` sur l'attachement de la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`BytesDropCountNoRoute`	Nombre d'octets abandonnés en raison de la non-correspondance avec une route sur l'attachement de la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`BytesIn`	Nombre d'octets reçus par la passerelle de transit à partir de l'attachement. Statistiques : la seule statistique significative est `Sum`.
`BytesOut`	Nombre d'octets envoyés de la passerelle de transit vers l'attachement.

Métrique	Description
	Statistiques : la seule statistique significative est `Sum`.
`PacketsIn`	Nombre de paquets reçus par la passerelle de transit à partir de l'attachement. Statistiques : la seule statistique significative est `Sum`.
`PacketsOut`	Nombre de paquets envoyés par la passerelle de transit vers l'attachement. Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountBlackhole`	Nombre de paquets abandonnés à cause d'une correspondance avec une route `blackhole` sur l'attachement de la passerelle de transit. Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountNoRoute`	Nombre de paquets abandonnés à cause d'une non-correspondance avec une route. Statistiques : la seule statistique significative est `Sum`.
`PacketDropCountTTLExpired`	Le nombre de paquets abandonnés en raison de l'expiration du TTL. Statistiques : la seule statistique significative est `Sum`.

Dimensions métriques de la passerelle de transit

Filtrez les données métriques des passerelles de transit à l'aide des dimensions suivantes :

Dimension	Description
`TransitGateway`	Filtre les données de métriques par la passerelle de transit.

Dimension	Description
`TransitGatewayAttachment`	Filtre les données de métriques par l'attachement de la passerelle de transit.
`TransitGateway , AvailabilityZone`	Filtre les données métriques par passerelle de transit et par zone de disponibilité.
`TransitGatewayAttachment , AvailabilityZone`	Filtre les données métriques par attachement à la passerelle de transit et par zone de disponibilité.

Enregistrez les appels d'API Amazon VPC Transit Gateways à l'aide de AWS CloudTrail

Amazon VPC Transit Gateways est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un. Service AWS CloudTrail capture tous les appels d'API pour Transit Gateway sous forme d'événements. Les appels capturés incluent des appels provenant de la console Transit Gateway et des appels de code vers les opérations de l'API Transit Gateway. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Transit Gateway, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l’identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d’identification d’utilisateur root ou d’utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- 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.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours à votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et

que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements de gestion de Transit Gateway

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Amazon VPC Transit Gateways enregistre toutes les opérations du plan de contrôle Transit Gateway en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de contrôle Amazon VPC Transit Gateways auxquelles Transit Gateway se connecte CloudTrail, consultez le manuel Amazon VPC Transit Gateways API Reference.

Exemples d'événements Transit Gateway

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les fichiers journaux incluent les événements relatifs à tous les appels d'API relatifs à votre AWS compte, et pas uniquement aux appels d'API de la 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 un exemple d'enregistrement de CloudTrail journal pour l'API de passerelle de transit pour 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`.

Example 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"
}
```

Gestion des identités et des accès dans Amazon VPC Transit Gateways

AWS utilise des identifiants de sécurité pour vous identifier et vous donner accès à vos AWS ressources. Vous pouvez utiliser les fonctionnalités de AWS Identity and Access Management (IAM) pour permettre à d'autres utilisateurs, services et applications d'utiliser vos AWS ressources dans leur intégralité ou de manière limitée, sans partager vos informations d'identification de sécurité.

Par défaut, les utilisateurs IAM ne sont pas autorisés à créer, afficher ou modifier AWS des ressources. 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 politique 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 utiliser une passerelle de transit, l'une des politiques AWS gérées 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/*"
        }
    ]
}
```

Utiliser des rôles liés à un service pour les passerelles de transit dans Amazon VPC Transit Gateways

Amazon VPC utilise des rôles liés à un service pour les autorisations requises pour appeler d'autres services AWS en votre nom. Pour plus d'informations, consultez la section 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 au service nommé AWSServiceRoleForVPCTransitGateway pour effectuer les actions suivantes en votre nom lorsque vous travaillez avec une passerelle de transit :

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

Le rôle AWSServiceRoleForVPCTransitGateway fait confiance aux services suivants pour assumer ce rôle :

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway utilise la politique géréeAWSVPCTransitGatewayServiceRolePolicy.

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

Il n'est pas nécessaire 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.

Modifier le rôle lié à un service

Vous pouvez modifier la description de AWSServiceRoleForVPCTransitGateway à l'aide d'IAM. Pour plus d'informations, voir Modifier la description d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer le rôle lié à un service

Si vous n'avez plus besoin d'utiliser les passerelles de transit, nous vous recommandons de supprimer AWSServiceRoleForVPCTransitGateway.

Vous ne pouvez supprimer ce rôle lié à un service qu'après avoir supprimé toutes les pièces jointes 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 plus d'informations, voir Supprimer un rôle lié à un service dans le Guide de l'utilisateur IAM.

Après avoir supprimé AWSServiceRoleForVPCTransitGateway, Amazon VPC crée à nouveau le rôle si vous associez un VPC de votre compte à une passerelle de transit.

AWS politiques gérées pour les passerelles de transit dans Amazon VPC Transit Gateways

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. 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 politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Pour utiliser une passerelle de transit, l'une des politiques AWS gérées suivantes peut répondre à vos besoins :

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS politique gérée : AWSVPCTransit GatewayServiceRolePolicy

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 voir les autorisations de cette stratégie, consultez AWSVPCTransitGatewayServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

Mises à jour des politiques AWS gérées par Transit Gateway

Consultez les détails des mises à jour des politiques AWS gérées 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 AWS gérées.	1er mars 2021

Réseau ACLs pour les passerelles de transit dans Amazon VPC Transit Gateways

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 EC2 instances et l'association des passerelles de transit”
- the section called “Différents sous-réseaux pour les EC2 instances et l'association des passerelles de transit”

Même sous-réseau pour les EC2 instances et l'association des passerelles de transit

Envisagez une configuration dans laquelle vous avez EC2 des instances et une association de passerelle de transit dans le même sous-réseau. La même ACL réseau est utilisée à la fois pour le trafic des EC2 instances vers la passerelle de transit et pour le trafic de la passerelle de transit vers les 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.

Différents sous-réseaux pour les EC2 instances et l'association des passerelles de transit

Imaginons une configuration dans laquelle vous avez des EC2 instances dans un sous-réseau et une association de passerelle de transit dans un sous-réseau différent, chaque sous-réseau étant associé à une ACL réseau différente.

Les règles ACL réseau sont appliquées comme suit pour le sous-réseau de l' EC2 instance :

- 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 l'appliquer NACLs 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 des passerelles de transit Amazon VPC

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	Oui
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	Oui
Nombre total d'acheminements combinés (dynamiques et statiques) sur toutes les tables de routage pour une passerelle de transit unique	10 000	Oui

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	Oui
Attachements d'appairage en attente par passerelle Transit Gateway	10	Oui
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 obtenue par le biais d'une connexion Site-to-Site VPN, notamment, mais sans s'y limiter : la taille des paquets, la composition du 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 passerell e 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) prenne en charge 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)

- 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 VPCs Transit Gateway Connect et les pièces jointes de peering (pièces jointes intra-régionales, interrégionales et cloud WAN). AWS Direct Connect 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 VPCs en même temps pour éviter que les paquets géants ne tombent en raison d'une incompatibilité de taille.
- 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 la MTU, consultez la section Unité de transmission maximale (MTU) dans le guide de l'AWS Site-to-Site VPN utilisateur.
- Les passerelles de transit prennent en charge Path MTU Discovery (PMTUD) pour le trafic entrant sur les pièces jointes VPC et Connect. La passerelle de transit génère les ICMPv4 paquets

`FRAG_NEEDED` pour et `Packet Too Big (PTB)` pour les ICMPv6 paquets. Les passerelles de transit ne prennent pas en charge le PMTUD sur les pièces Site-to-site jointes VPN, Direct Connect et Peering. Pour plus d'informations sur Path MTU Discovery, consultez Path MTU Discovery dans le guide de l'utilisateur Amazon VPC

Multicast

> **Note**
>
> La multidiffusion par passerelle de transit peut ne pas convenir aux transactions à haute fréquence ou aux applications sensibles aux performances. Nous vous recommandons vivement de vérifier les limites de multidiffusion suivantes. Contactez votre compte ou l'équipe d'architectes de solutions pour un examen détaillé de vos exigences de performance.

Nom	Par défaut	Ajustable
Domaines multicast par passerelle de transit	20	Oui
Interfaces de réseau de multicast par passerelle Transit Gateway	10 000	Oui
Associations de domaines multicast par VPC	20	Oui
Sources par groupe multicast de passerelle de transit	1	Oui
Membres et sources de groupes statiques et de IGMPv2 multidiffusion par passerelle de transit	10 000	Non
Membres de groupes statiques et de IGMPv2 multidiffusion par groupe de multidiffusion 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

Nom	Par défaut	Ajustable
Nombre maximal de paquets par seconde et par flux (moins de 10 récepteurs)	75 000	Non
Nombre maximal de paquets par seconde et par flux (plus de 10 récepteurs)	15 000	Non
Nombre maximal de paquets agrégés par seconde (moins de 10 récepteurs)	2 500 000	Non
Nombre maximal de paquets agrégés par seconde (plus de 10 récepteurs)	500 000	Non

AWS Directeur du réseau

Nom	Par défaut	Ajustable
Réseaux mondiaux par Compte AWS	5	Oui
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 en savoir plus, consultez les ressources suivantes :

- Site-to-Site Quotas VPN dans le guide de AWS Site-to-Site VPN l'utilisateur
- 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
Pièces jointes aux fonctions réseau	Créez une pièce jointe à une fonction réseau à laquelle connecter directement une passerelle de transit AWS Network Firewall.	16 juin 2025
Support pour le référencement des groupes de sécurité	Vous pouvez désormais référencer un groupe de sécurité VPCs attaché à une passerelle de transit.	25 septembre 2024
AWS Quotas de Transit Gateway	Des limites de bande passante ont été ajoutées.	14 août 2023
AWS Journaux de flux de Transit Gateway	Les passerelles de transit prennent désormais en charge Transit Gateway Flow Logs, qui vous permet de surveille r et de journaliser le trafic réseau entre les passerelles.	14 juillet 2022
Tables de stratégie de passerelle de transit	Utilisez des tables de stratégie afin de configurer un routage dynamique pour les passerell es de transit et d'échange r automatiquement des informations de routage et d'accessibilité avec des types de passerelles de transit appairés.	13 juillet 2022

Guide de l'utilisateur Network Manager	Network Manager a été créé en tant que guide autonome et n'est plus inclus dans le AWS Guide de l'utilisateur Transit Gateway.	2 décembre 2021
Attachement d'appairage	Vous pouvez créer une connexion d'appairage avec une passerelle de transit dans la même région.	1 décembre 2021
Transit Gateway Connect	Vous pouvez établir une connexion entre une passerelle de transit et des appliances virtuelles tierces exécutées dans un VPC.	10 décembre 2020
Mode Appliance	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
Références des listes de préfixes	Vous pouvez référencer une liste de préfixes dans votre table de routage de passerelle de transit.	24 août 2020
Modifier la passerelle de transit	Vous pouvez modifier les options de configuration de votre passerelle de transit.	24 août 2020

CloudWatch mesures relatives aux pièces jointes aux passerelles de transit	Vous pouvez consulter CloudWatch les statistiques relatives à chaque pièce jointe à une passerelle de transport en commun.	6 juillet 2020
Analyseur de routes Network Manager	Vous pouvez analyser les itinéraires de vos tables de routage de passerelle de transit dans votre réseau global.	4 mai 2020
Attachement d'appairage	Vous pouvez créer une connexion d'appairage avec une passerelle de transit dans une autre région.	3 décembre 2019
Prise en charge de la multicast	Transit Gateway prend en charge le routage du trafic multicast entre les sous-rése aux rattachés VPCs et sert de routeur multicast pour les instances envoyant du trafic destiné à plusieurs instances de réception.	3 décembre 2019
AWS Gestionnaire de réseau	Vous pouvez visualiser et surveiller vos réseaux mondiaux construits autour des passerelles de transit.	3 décembre 2019

AWS Direct Connect soutien	Vous pouvez utiliser une AWS Direct Connect passerelle pour connecter votre AWS Direct Connect connexion via une interface virtuelle de transit à la passerelle de transit VPCs ou VPNs attachée à celle-ci.	27 mars 2019
Première version	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.