Guide de l’utilisateur

AWS Direct Connect

AWS Direct Connect: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Direct Connect ?

AWS Direct Connect relie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Une extrémité du câble est raccordée à votre routeur et l'autre à un routeur AWS Direct Connect . Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les AWS services publics (par exemple, vers Amazon S3) ou vers Amazon VPC, en contournant les fournisseurs de services Internet sur votre chemin réseau. Un AWS Direct Connect emplacement permet d'accéder AWS à la région à laquelle il est associé. Vous pouvez utiliser une seule connexion dans une région publique ou AWS GovCloud (US) pour accéder aux AWS services publics dans toutes les autres régions publiques.

Le schéma suivant présente une vue d'ensemble détaillée de la manière dont AWS Direct Connect les interfaces sont établies avec votre réseau.

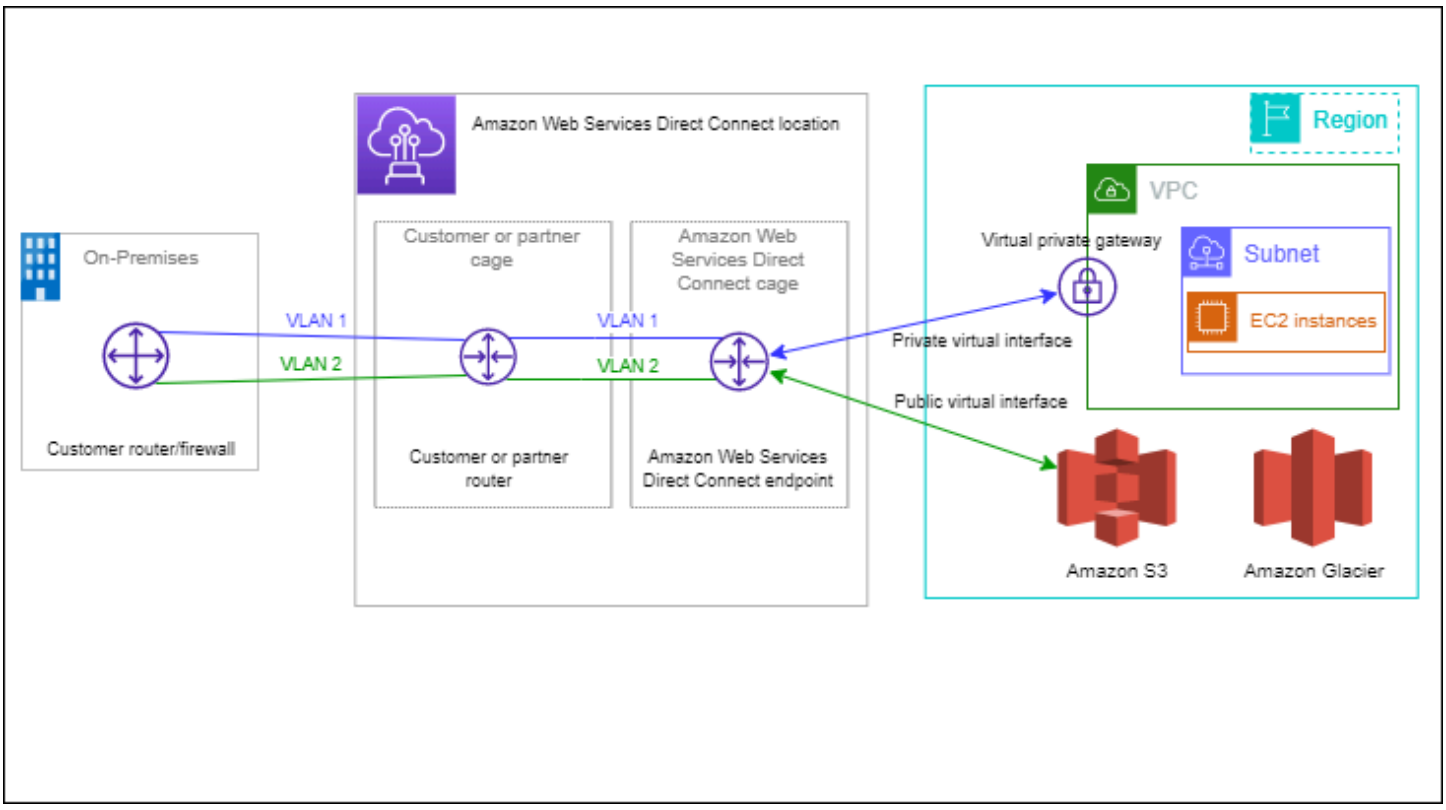


Table des matières

- Accès à une région AWS à distance
- Stratégies de routage et communautés BGP (Border Gateway Protocol)

AWS Direct Connect composants

Voici les principaux composants que vous utilisez pour AWS Direct Connect :

Connexions

Créez une connexion dans un AWS Direct Connect lieu pour établir une connexion réseau entre vos locaux et une AWS région. Pour plus d'informations, consultez AWS Direct Connect connexions.

Interfaces virtuelles

Créez une interface virtuelle pour permettre l'accès aux AWS services. Une interface virtuelle publique permet d'accéder à des services publics, comme Amazon S3. Une interface virtuelle privée permet d'accéder à votre VPC. Pour plus d'informations, consultez AWS Direct Connect interfaces virtuelles et Conditions préalables pour les interfaces virtuelles.

Exigences réseau

Pour être utilisé AWS Direct Connect dans un AWS Direct Connect lieu, votre réseau doit répondre à l'une des conditions suivantes :

- Votre réseau est colocalisé avec un emplacement existant AWS Direct Connect . Pour plus d'informations sur les AWS Direct Connect emplacements disponibles, consultez les détails du produit AWS Direct Connect.
- Vous travaillez avec un AWS Direct Connect partenaire membre du réseau de AWS partenaires (APN). Pour de plus amples informations, veuillez consulter Partenaires APN prenant en charge AWS Direct Connect.
- Vous travaillez avec un fournisseur de services indépendant pour vous connecter à AWS Direct Connect.

Votre réseau doit également répondre aux conditions suivantes :

- Votre réseau doit utiliser une fibre optique monomode avec un émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, un émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits ou un émetteur-récepteur 100GBASE-LR4 pour 100 gigabit Ethernet.
- La négociation automatique d'un port doit être désactivée pour une connexion dont la vitesse de port est supérieure à 1 Gb/s. Toutefois, selon le point de terminaison AWS Direct Connect qui dessert votre connexion, il peut être nécessaire d'activer ou de désactiver la négociation automatique pour les connexions à 1 Gbit/s. Si votre interface virtuelle reste inactive, consultez Dépannage de problèmes (de liaison de données) de niveau 2.
- L'encapsulation VLAN 802.1Q doit être prise en charge sur l'ensemble de la connexion, y compris les périphériques intermédiaires.
- Votre périphérique doit prendre en charge l'authentification protocole de passerelle frontière (BGP) et BGP MD5.
- (Facultatif) Vous pouvez configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau. Le BFD asynchrone est automatiquement activé pour chaque AWS Direct Connect interface virtuelle. Elle est automatiquement activée pour les interfaces virtuelles Direct Connect, mais ne prend effet que lorsque vous la configurez sur votre routeur. Pour plus d'informations, consultez Activer la BFD pour une connexion Direct Connect.

AWS Direct Connect prend en charge les protocoles de communication IPv4 et IPv6. Les adresses IPv6 fournies par les AWS services publics sont accessibles via AWS Direct Connect des interfaces virtuelles publiques.

AWS Direct Connect prend en charge une taille de trame Ethernet de 1522 ou 9023 octets (en-tête Ethernet de 14 octets + balise VLAN de 4 octets + octets pour le datagramme IP + FCS de 4 octets) au niveau de la couche du lien. Vous pouvez définir la MTU de vos interfaces virtuelles privées. Pour plus d'informations, consultez Définir la MTU du réseau pour les interfaces virtuelles privées ou les interfaces de transit virtuelles.

Tarification pour AWS Direct Connect

AWS Direct Connect comporte deux éléments de facturation : les heures de port et le transfert de données sortants. La tarification en heures-port se base sur la capacité et le type de connexion (dédiée ou hébergée).

Les frais de transfert de données sortants pour les interfaces privées et les interfaces virtuelles de transit sont alloués au AWS compte responsable du transfert de données. Il n'y a pas de frais supplémentaires pour l'utilisation d'une passerelle AWS Direct Connect pour plusieurs comptes.

Pour les AWS ressources adressables publiquement (par exemple, les compartiments Amazon S3, les instances EC2 classiques ou le trafic EC2 passant par une passerelle Internet), si le trafic sortant est destiné à des préfixes publics détenus par le même compte AWS payeur et faisant l'objet d'une publicité active AWS via une interface virtuelle AWS Direct Connect publique, l'utilisation des transferts de données sortants (DTO) est mesurée en fonction du propriétaire de la ressource au taux de transfert de données. AWS Direct Connect

Pour plus d'informations, consultez Tarification AWS Direct Connect.

AWS Direct Connect entretien

AWS Direct Connect est un service entièrement géré dans le cadre duquel Direct Connect effectue régulièrement des activités de maintenance sur un parc matériel prenant en charge le service. Les connexions Direct Connect sont fournies sur des appareils matériels autonomes qui vous permettent de créer des connexions réseau hautement résilientes entre Amazon Virtual Private Cloud et votre infrastructure sur site. Cette fonctionnalité vous permet d'accéder à vos AWS ressources de manière fiable, évolutive et rentable. Pour plus d'informations, consultez Recommandations relatives à la résilience AWS Direct Connect.

Il existe deux types de maintenance Direct Connect : maintenance planifiée et maintenance d'urgence :

- Maintenance planifiée. La maintenance planifiée est planifiée à l'avance afin d'améliorer la disponibilité et de proposer de nouvelles fonctionnalités. Ce type de maintenance est planifié pendant une période de maintenance au cours de laquelle nous envoyons trois notifications : 14 jours calendaires, 7 jours calendaires et 1 jour calendaire.

  > **Note**
  >
  > Les jours civils incluent les jours non ouvrables et les jours fériés locaux.

- Maintenance d'urgence. La maintenance d'urgence est lancée sur une base critique en raison d'une panne impactant le service qui nécessite une action immédiate de la part d' AWS pour rétablir les services. Ce type de maintenance n'est pas planifié à l'avance. Les clients concernés sont informés de la maintenance d'urgence jusqu'à 60 minutes avant la maintenance.

Nous vous recommandons de suivre les recommandations de résilience AWS Direct Connect afin de pouvoir transférer le trafic de manière souple et proactive vers votre connexion Direct Connect redondante pendant la maintenance. Nous vous recommandons également de tester régulièrement de manière proactive la résilience de vos connexions redondantes afin de vérifier que le basculement fonctionne comme prévu. Grâce à cette the section called "AWS Direct Connect Test de basculement" fonctionnalité, vous pouvez vérifier que votre trafic passe par l'une de vos interfaces virtuelles redondantes.

Pour obtenir des conseils sur les critères d'éligibilité pour lancer une demande d'annulation de maintenance planifiée, consultez Comment annuler un événement de maintenance Direct Connect ?.

> **Note**
>
> Les demandes de maintenance d'urgence ne peuvent pas être annulées car AWS elles doivent être prises immédiatement pour rétablir le service.

Pour plus d'informations sur les événements de maintenance, consultez la section Événements de maintenance dans les AWS Direct Connect FAQ.

Accès à une région AWS à distance

Les emplacements AWS Direct Connect se trouvant dans des régions publiques ou AWS GovCloud (US) peuvent accéder aux services publics de toutes les autres régions publiques (à l'exception de la Chine (Beijing et Ningxia)). En outre, les connexions AWS Direct Connect des régions publiques ou AWS GovCloud (US) peuvent être configurées pour accéder à un VPC de votre compte dans toute autre région publique (à l'exception de la Chine (Beijing et Ningxia)). Par conséquent, vous pouvez utiliser une même connexion AWS Direct Connect pour créer des services sur plusieurs régions. L'ensemble du trafic réseau reste sur l'épine dorsale du réseau AWS mondial, même si vous accédez à des services AWS publics ou à un VPC dans une autre région.

Tout transfert de données à partir d'une région à distance est facturé au tarif de transfert de données de la région à distance. Pour plus d'informations sur la tarification du transfert de données, consultez la section Tarification sur la page d'informations d'AWS Direct Connect.

Pour plus d'informations sur les stratégies de routage et les communautés BGP prises en charge par une connexion AWS Direct Connect, consultez Stratégies de routage et communautés BGP (Border Gateway Protocol).

Accès aux services publics d'une région à distance

Pour accéder aux ressources publiques dans une région à distance, vous devez configurer une interface virtuelle publique et établir une session BGP (Border Gateway Protocol). Pour de plus amples informations, veuillez consulter AWS Direct Connect interfaces virtuelles.

Une fois que vous avez créé une interface virtuelle publique et établi une session BGP, votre routeur a accès aux routes des autres régions AWS publiques. Pour en savoir plus sur les préfixes publiés par AWS, consultez la section Plages d'adresses IP AWS du Référence générale d'Amazon Web Services.

Accès aux VPC d'une région à distance

Vous pouvez créer une Passerelle Direct Connect dans toutes les régions publiques. Utilisez-la pour associer votre connexion AWS Direct Connect, via une interface virtuelle privée, aux VPC de votre compte situés dans d'autres régions ou à une passerelle de transit. Pour de plus amples informations, veuillez consulter Utilisation des passerelles Direct Connect.

Vous pouvez également créer une interface virtuelle publique pour votre connexion AWS Direct Connect et établir une connexion VPN à votre VPC dans la région à distance. Pour en savoir plus sur la configuration de la connectivité VPN vers un VPC, consultez Scénarios d'utilisation du cloud privé virtuel Amazon dans le Guide de l'utilisateur d'Amazon VPC.

Options de connectivité réseau vers VPC Amazon

La configuration suivante peut être utilisée pour connecter des réseaux distants à votre environnement Amazon VPC. Ces options sont utiles pour intégrer les ressources AWS à vos services sur site existants :

- Amazon Virtual Private Cloud Connectivity Options

Stratégies de routage et communautés BGP (Border Gateway Protocol)

AWS Direct Connect applique des politiques de routage entrant (depuis votre centre de données sur site) et sortant (depuis votre AWS région) pour une connexion publique. AWS Direct Connect Vous pouvez également utiliser les balises de la communauté protocole de passerelle frontière (BGP) sur

des routes publiées par Amazon et appliquer des balises de la communauté BGP sur les routes que vous publiez sur Amazon.

Stratégies de routage d'interface virtuelle publique

Si vous avez l'habitude AWS Direct Connect d'accéder à AWS des services publics, vous devez spécifier les préfixes IPv4 ou IPv6 publics pour faire de la publicité sur BGP.

Les stratégies de routage de trafic entrant suivantes s'appliquent :

- Vous devez être propriétaire des préfixes publics, qui doivent être enregistrés en tant que tels dans le registre Internet régional approprié.
- Le trafic doit être destiné à des préfixes publics Amazon. Le routage transitif entre les connexions n'est pas pris en charge.
- AWS Direct Connect effectue un filtrage des paquets entrants pour vérifier que la source du trafic provient du préfixe que vous avez annoncé.

Les stratégies de routage de trafic sortant suivantes s'appliquent :

- AS_PATH et Longest Prefix Match sont utilisés pour déterminer le chemin de routage. AWS recommande d'annoncer des itinéraires plus spécifiques AWS Direct Connect si le même préfixe est annoncé à la fois sur Internet et sur une interface virtuelle publique.
- AWS Direct Connect annonce tous les préfixes des AWS régions locales et éloignées lorsqu'ils sont disponibles et inclut les préfixes sur le réseau provenant d'autres points de présence (PoP) AWS non régionaux lorsqu'ils sont disponibles, par exemple, et Route 53. CloudFront

  > **Note**
  >
  > - Les préfixes répertoriés dans le fichier JSON des plages d'adresses AWS IP, ip-ranges.json, pour les régions AWS chinoises ne sont annoncés que dans les régions chinoises. AWS
  > - Les préfixes répertoriés dans le fichier JSON des plages d'adresses AWS IP, ip-ranges.json, pour les régions AWS commerciales ne sont annoncés que dans les régions commerciales. AWS
  >
  > Pour plus d'informations sur le fichier ip-ranges.json, consultez la section Plages d'adresses IP AWS dans Références générales AWS.

- AWS Direct Connect annonce des préfixes avec une longueur de chemin minimale de 3.

- AWS Direct Connect annonce tous les préfixes publics auprès de la célèbre communauté NO_EXPORT BGP.
- Si vous publiez les mêmes préfixes provenant de deux régions différentes à l'aide de deux interfaces virtuelles publiques différentes, et que les deux ont les mêmes attributs BGP et la plus longue longueur de préfixe, la priorité AWS sera donnée à la région d'origine pour le trafic sortant.
- Si vous avez plusieurs AWS Direct Connect connexions, vous pouvez ajuster le partage de charge du trafic entrant en publiant des préfixes ayant les mêmes attributs de chemin.
- Les préfixes annoncés par ne AWS Direct Connect doivent pas être annoncés au-delà des limites du réseau de votre connexion. Par exemple, ces préfixes ne doivent pas être inclus dans les tables de routage Internet public.
- AWS Direct Connect conserve les préfixes annoncés par les clients au sein du réseau Amazon. Nous ne publions pas à nouveau les préfixes clients tirés d'un VIF public sous les formes suivantes :
  - Autres AWS Direct Connect clients
  - Des réseaux homologues au réseau AWS mondial
  - Des fournisseurs de transit d'Amazon

Communautés BGP d'interface virtuelle publique

AWS Direct Connect prend en charge les balises communautaires BGP scope pour aider à contrôler la portée (régionale ou mondiale) et les préférences d'itinéraire du trafic sur les interfaces virtuelles publiques. AWS traite toutes les routes reçues d'un VIF public comme si elles étaient étiquetées avec la balise communautaire BGP NO_EXPORT, ce qui signifie que seul le AWS réseau utilisera ces informations de routage.

Portée des communautés BGP

Vous pouvez appliquer des balises de la communauté BGP aux préfixes publics que vous publiez sur Amazon pour indiquer dans quelle mesure propager vos préfixes sur le réseau Amazon : pour la région AWS locale uniquement, pour toutes les régions d'un continent ou pour toutes les régions publiques.

Région AWS communautés

Pour les politiques de routage entrant, vous pouvez utiliser les communautés BGP suivantes pour vos préfixes :

- `7224:9100`—Local Régions AWS
- `7224:9200`—Tout Régions AWS pour un continent :
  - À l'échelle de l'Amérique du Nord
  - Asie-Pacifique
  - Europe, Moyen-Orient et Afrique
- `7224:9300`—Global (toutes les AWS régions publiques)

> **Note**
>
> Si vous n'appliquez aucun tag communautaire, les préfixes sont annoncés par défaut dans toutes les AWS régions publiques (mondiales).
> Les préfixes marqués des mêmes communautés et ayant des attributs AS_PATH identiques peuvent prendre en charge des chemins d'accès multiples.

Les communautés `7224:1` – `7224:65535` sont réservées par AWS Direct Connect.

Pour les politiques de routage sortant, AWS Direct Connect applique les communautés BGP suivantes aux itinéraires annoncés :

- `7224:8100`—Routes provenant de la même AWS région à laquelle le AWS Direct Connect point de présence est associé.
- `7224:8200`—Routes en provenance du même continent auquel le AWS Direct Connect point de présence est associé.
- Aucune étiquette : routes en provenance d'autres continents.

> **Note**
>
> Pour recevoir tous les préfixes AWS publics, n'appliquez aucun filtre.

Les communautés qui ne sont pas prises en charge pour une connexion AWS Direct Connect publique sont supprimées.

Communauté BGP `NO_EXPORT`

Pour les politiques de routage sortant, la balise de communauté BGP `NO_EXPORT` est prise en charge pour les interfaces virtuelles publiques.

AWS Direct Connect fournit également des tags communautaires BGP sur les itinéraires Amazon annoncés. Si vous avez l' AWS Direct Connect habitude d'accéder à AWS des services publics, vous pouvez créer des filtres basés sur ces tags communautaires.

Pour les interfaces virtuelles publiques, toutes les routes destinées AWS Direct Connect aux clients sont étiquetées avec le tag communautaire NO_EXPORT.

Stratégies de routage d'interface virtuelle privée et d'interface virtuelle de transit

Si vous utilisez AWS Direct Connect pour accéder à vos AWS ressources privées, vous devez spécifier les préfixes IPv4 ou IPv6 pour faire de la publicité sur BGP. Ces préfixes peuvent être publics ou privés.

Les règles de routage sortant suivantes s'appliquent en fonction des préfixes annoncés :

- AWS évalue d'abord la longueur du préfixe le plus long. AWS recommande de publier des itinéraires plus spécifiques à l'aide de plusieurs interfaces virtuelles Direct Connect si les chemins de routage souhaités sont destinés à des connexions actives/passives. Voir Influencer le trafic sur les réseaux hybrides à l'aide de la correspondance de préfixe la plus longue pour plus d'informations.
- La préférence locale est l'attribut BGP qu'il est recommandé d'utiliser lorsque les chemins de routage souhaités sont destinés à des connexions actives/passives et que les longueurs de préfixes annoncées sont les mêmes. Cette valeur est définie par région pour préférer les AWS Direct Connect emplacements associés aux mêmes emplacements Région AWS en utilisant la valeur communautaire de préférence locale `7224:7200` —Medium. Lorsque la région locale n'est pas associée à l'emplacement Direct Connect, elle est définie sur une valeur inférieure. Cela s'applique uniquement si aucune balise communautaire de préférence locale n'est attribuée.
- La longueur AS_PATH peut être utilisée pour déterminer le chemin de routage lorsque la longueur du préfixe et les préférences locales sont identiques.
- Le discriminateur à sorties multiples (MED) peut être utilisé pour déterminer le chemin de routage lorsque la longueur du préfixe, les préférences locales et AS_PATH sont identiques. AWS ne recommande pas d'utiliser les valeurs MED étant donné leur faible priorité lors de l'évaluation.

- AWS partagera la charge entre plusieurs interfaces virtuelles de transit ou privées lorsque les préfixes ont la même longueur et les mêmes attributs BGP.

Communautés BGP d'interface virtuelle privée et Interface virtuelle de transit

Lorsqu'un site Région AWS achemine le trafic vers des sites sur site via des interfaces virtuelles privées ou de transit Direct Connect, l'emplacement Direct Connect associé Région AWS influence la capacité à utiliser le routage multichemin à coût égal (ECMP). Régions AWS préférez les emplacements Direct Connect associés Région AWS par défaut. Consultez la section AWS Direct Connect Emplacements pour identifier l'emplacement associé à Région AWS n'importe quel emplacement Direct Connect.

Lorsqu'aucune balise communautaire de préférence locale n'est appliquée, Direct Connect prend en charge l'ECMP sur des interfaces virtuelles privées ou de transit pour les préfixes de même longueur, de même longueur AS_PATH et de même valeur MED sur deux chemins ou plus dans les scénarios suivants :

- Le trafic Région AWS d'envoi possède au moins deux chemins d'interface virtuelle à partir d'emplacements situés dans les mêmes installations associées Région AWS, que ce soit dans les mêmes installations de colocation ou dans des installations de colocation différentes.
- Le trafic Région AWS d'envoi possède au moins deux chemins d'interface virtuelle provenant d'emplacements ne se trouvant pas dans la même région.

Pour plus d'informations, voir Comment configurer une connexion Direct Connect active/active ou active/passive AWS à partir d'une interface virtuelle privée ou de transit ?

> **Note**
>
> Cela n'a aucun effet sur l'ECMP à destination et en Région AWS provenance des sites sur site.

Pour contrôler les préférences d'itinéraire, Direct Connect prend en charge les balises communautaires BGP de préférence locale pour les interfaces virtuelles privées et les interfaces virtuelles de transit.

Communautés BGP de préférence locale

Vous pouvez utiliser les balises de la communauté BGP de préférence locale pour équilibrer la charge et définir les préférences de routage du trafic entrant vers votre réseau. Pour chaque préfixe que vous publiez sur une session BGP, vous pouvez appliquer une balise de communauté afin d'indiquer la priorité du chemin associé pour le trafic en retour.

Les balises de communauté BGP de préférence locale suivantes sont prises en charge :

- `7224:7100` – Préférence faible
- `7224:7200` – Préférence moyenne
- `7224:7300` – Préférence élevée

Les balises de communauté BGP de préférence locale sont mutuellement exclusives. Pour équilibrer la charge du trafic entre plusieurs AWS Direct Connect connexions (actives/actives) reliées à la même région ou à des AWS régions différentes, appliquez le même tag de communauté ; par exemple, `7224:7200` (préférence moyenne) sur les préfixes des connexions. Si l'une des connexions échoue, le trafic sera alors équilibré à l'aide d'ECMP sur les connexions actives restantes, quelles que soient leurs associations de région d'origine. Pour permettre le basculement sur plusieurs connexions AWS Direct Connect (actives/passives), appliquez une balise de communauté avec une préférence plus élevée pour les préfixes de l'interface virtuelle principale ou active et une préférence inférieure pour les préfixes de l'interface virtuelle de sauvegarde ou passive. Par exemple, définissez les balises de communauté BGP pour vos interfaces virtuelles principales ou actives sur `7224:7300` (préférence élevée) et `7224:7100` (préférence faible) pour vos interfaces virtuelles passives.

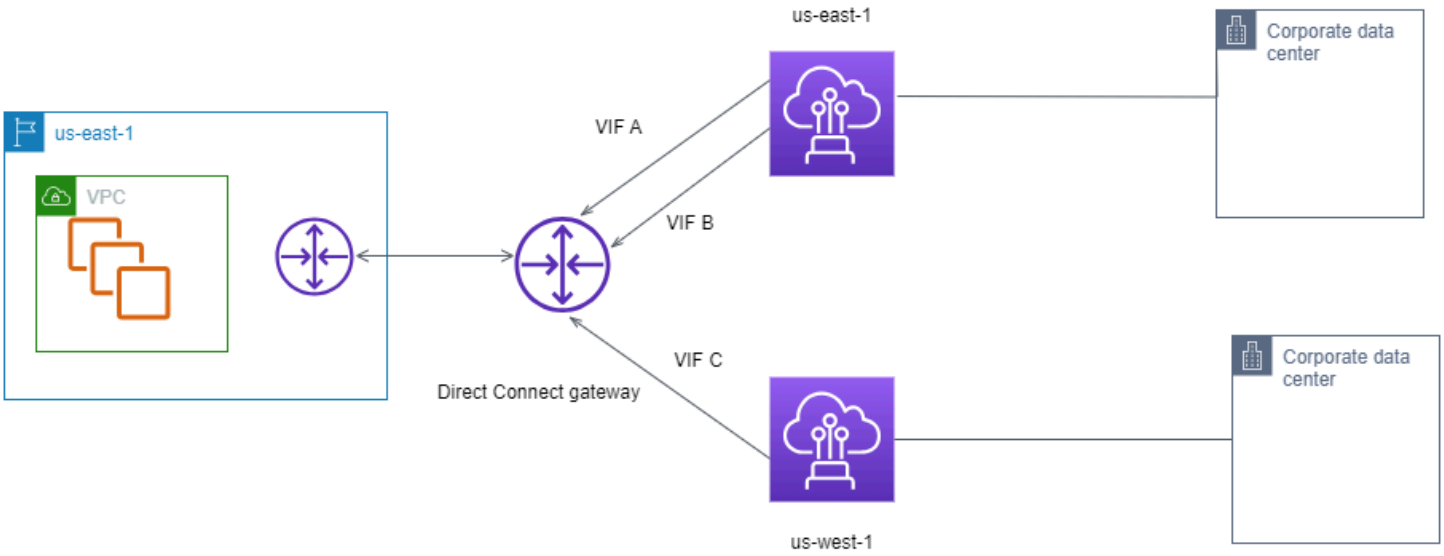
Les balises de communauté BGP de préférence locale sont évaluées avant tout attribut AS_PATH, et de la plus faible à la plus haute préférence (la plus haute préférence correspond à la préférée).

Exemple de routage d'une interface virtuelle privée

Considérez la configuration dans laquelle la région d'origine de l' AWS Direct Connect emplacement 1 est identique à la région d'origine du VPC. Il existe un AWS Direct Connect emplacement redondant dans une région différente. Deux VIF privés (VIF A et VIF B) relient l' AWS Direct Connect emplacement 1 (us-east-1) à la passerelle Direct Connect. Un VIF privé (VIF C) relie l' AWS Direct Connect emplacement (us-west-1) à la passerelle Direct Connect. Pour que le trafic AWS passe par le VIF B avant le VIF A, définissez l'attribut AS_PATH du VIF B pour qu'il soit plus court que l'attribut AS_PATH du VIF A.

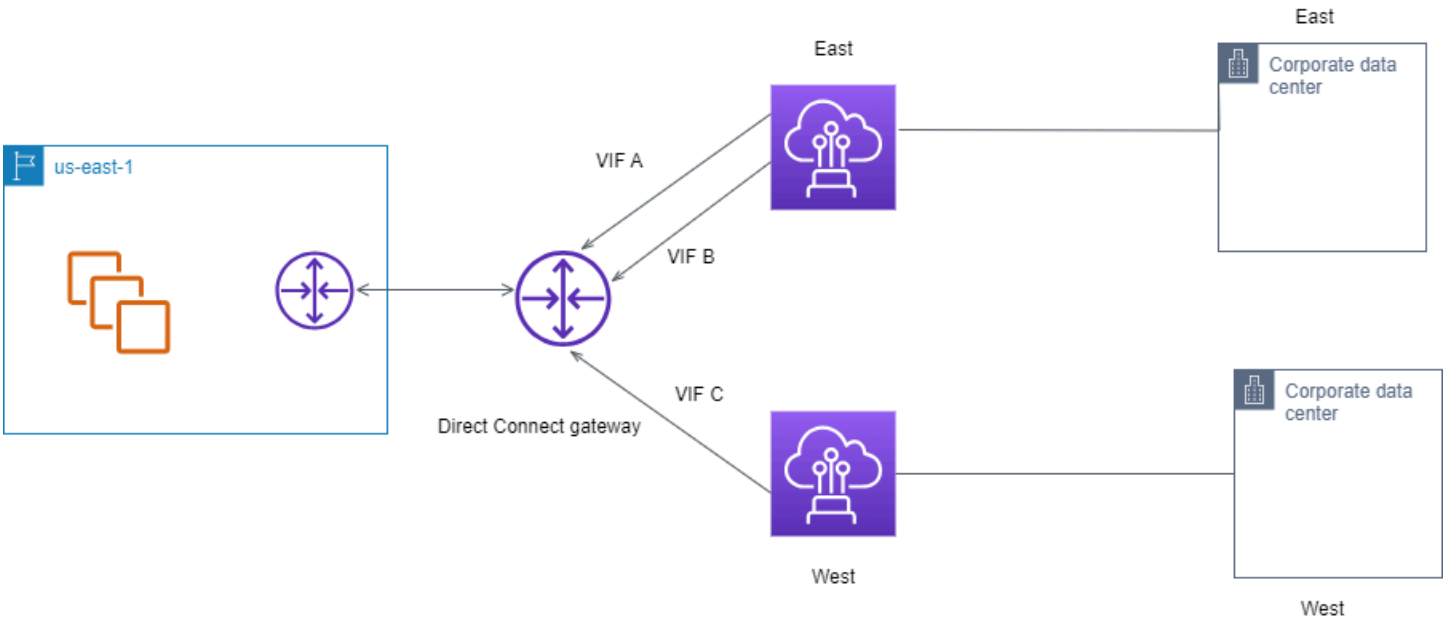
Les VIF ont les configurations suivantes :

- VIF A (dans us-east-1) publie 172.16.0.0/16 et possède un attribut AS_PATH de 65001, 65001, 65001
- VIF B (dans us-east-1) publie 172.16.0.0/16 et possède un attribut AS_PATH de 65001, 65001
- VIF C (dans us-west-1) publie 172.16.0.0/16 et possède un attribut AS_PATH de 65001



Si vous modifiez la configuration de la plage CIDR du VIF C, les routes comprises dans la plage d'adresses CIDR du VIF C utilisent le VIF C car le préfixe est le plus long.

- VIF C (dans us-west-1) publie 172.16.0.0/24 et possède un attribut AS_PATH de 65001


East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

Utiliser le AWS Direct Connect Resiliency Toolkit pour démarrer

AWS permet aux clients d'établir des connexions réseau hautement résilientes entre Amazon Virtual Private Cloud (Amazon VPC) et leur infrastructure sur site. Le AWS Direct Connect Resiliency Toolkit fournit un assistant de connexion avec plusieurs modèles de résilience. Ces modèles vous aident à déterminer, puis à passer une commande pour le nombre de connexions dédiées afin d'atteindre votre objectif en matière de SLA (contrat de niveau de service). Vous sélectionnez un modèle de résilience, puis le AWS Direct Connect Resiliency Toolkit vous guide tout au long du processus de commande de connexion dédié. Les modèles de résilience sont conçus pour vous assurer de disposer du nombre approprié de connexions dédiées dans plusieurs emplacements.

Le AWS Direct Connect Resiliency Toolkit présente les avantages suivants :

- Il fournit des conseils pour vous aider à déterminer, puis commander les connexions dédiées AWS Direct Connect redondantes appropriées.
- Il garantit que les connexions dédiées redondantes ont la même vitesse.
- Il configure automatiquement les noms des connexions dédiées.
- Approuve automatiquement vos connexions dédiées lorsque vous avez un AWS compte existant et que vous sélectionnez un AWS Direct Connect partenaire connu. La lettre d'autorisation (LOA) peut être téléchargée immédiatement.
- Crée automatiquement un ticket d'assistance pour l'approbation de la connexion dédiée lorsque vous êtes un nouveau AWS client ou que vous sélectionnez un (autre) partenaire inconnu.
- Il fournit un récapitulatif des commandes de vos connexions dédiées, avec le SLA réalisable et le coût port-heure pour les connexions dédiées commandées.
- Il crée des groupes d'agrégation de liaisons (LAG) et ajoute le nombre approprié de connexions dédiées aux LAG lorsque vous sélectionnez une vitesse différente de 1 Gb/s, 10 Gb/s ou 100 Gb/s.
- Il fournit un récapitulatif des LAG avec le SLA de connexions dédiées réalisable, ainsi que le coût port-heure total pour chaque connexion dédiée commandées dans le cadre du LAG.
- Il vous empêche de terminer les connexions dédiées sur le même appareil AWS Direct Connect .
- Fournit un moyen de tester votre configuration pour la résilience. Vous utilisez AWS pour réduire la session d'appairage BGP afin de vérifier que le trafic est acheminé vers l'une de vos interfaces virtuelles redondantes. Pour plus d'informations, consultez the section called "AWS Direct Connect Test de basculement".

- Fournit des CloudWatch métriques Amazon pour les connexions et les interfaces virtuelles. Pour plus d'informations, consultez Surveillance.

Les modèles de résilience suivants sont disponibles dans le AWS Direct Connect Resiliency Toolkit :

- Maximum Resiliency (Résilience maximale) : Ce modèle vous permet de commander des connexions dédiées pour atteindre un SLA de 99,99 %. Pour cela, vous devez répondre à toutes les exigences pour atteindre le SLA, qui sont spécifiées dans le Contrat de niveau de service AWS Direct Connect.
- High Resiliency (Haute résilience) : Ce modèle vous permet de commander des connexions dédiées pour atteindre un SLA de 99,9 %. Pour cela, vous devez répondre à toutes les exigences pour atteindre le SLA, qui sont spécifiées dans le Contrat de niveau de service AWS Direct Connect.
- Développement et test : Ce modèle vous permet d'obtenir une résilience de développement et de test pour les charges de travail non critiques, en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans un seul emplacement.
- Classic (Classique). Ce modèle est conçu pour les utilisateurs disposant de connexions existantes et désireuses d'ajouter des connexions supplémentaires. Ce modèle ne fournit pas de SLA.

La meilleure pratique consiste à utiliser l'assistant de connexion du AWS Direct Connect Resiliency Toolkit pour commander les connexions dédiées afin d'atteindre votre objectif de SLA.

Après avoir sélectionné le modèle de résilience, le AWS Direct Connect Resiliency Toolkit vous guide à travers les procédures suivantes :

- Sélection du nombre de connexions dédiées
- Sélection de la capacité de connexion et de l'emplacement des connexion dédiées
- Commande des connexions dédiées
- Vérification que les connexions dédiées sont prêtes à être utilisées
- Téléchargement de votre lettre d'autorisation (LOA-CFA) pour chaque connexion dédiée
- Vérification du respect de vos exigences de résilience pour votre configuration

Prérequis

AWS Direct Connect prend en charge les vitesses de port suivantes sur fibre monomode : émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits ou 100GBASE-LR4 pour 100 gigabit Ethernet.

Vous pouvez configurer une AWS Direct Connect connexion de l'une des manières suivantes :

Modèle	Bande passante	Méthode
Connexion dédiée	1 Gb/s, 10 Gb/s et 100 Gb/s	Travaillez avec un AWS Direct Connect partenaire ou un fournisseur de réseau pour connecter un routeur de votre centre de données, de votre bureau ou de votre environnement de colocation à un AWS Direct Connect emplacement. Le fournisseur de réseau n'a pas besoin d'être un Partnaire AWS Direct Connect pour vous connecter à une connexion dédiée. Les connexions dédiées AWS Direct Connect prennent en charge ces vitesses de port sur fibre optique monomode : 1 Gb/s : 1000BASE-LX (1310 nm), 10 Gb/s : 10GBASE-LR (1310 nm) et 100 Gb/s : 100GBASE-LR4.
Connexion hébergée	50 Mo/s, 100 Mo/s, 200 Mo/s, 300 Mo/s, 400 Mo/s, 500 Mo/s, 1 Gbit/s, 2 Gbits/s, 5 Gbits/s et 10 Gbits/s	Travaillez avec un AWS Direct Connect partenaire du programme de partenariat pour connecter un routeur de votre centre de données,

Modèle	Bande passante	Méthode
		de votre bureau ou de votre environnement de colocation à un AWS Direct Connect emplacement. Seuls certains partenaires offrent des connexions de capacité plus élevée.

Pour les connexions AWS Direct Connect avec des bandes passantes de 1 Gbit/s ou plus, assurez-vous que votre réseau répond aux exigences suivantes :

- Votre réseau doit utiliser une fibre optique monomode avec un émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, un émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits ou un émetteur-récepteur 100GBASE-LR4 pour 100 gigabit Ethernet.
- La négociation automatique d'un port doit être désactivée pour une connexion dont la vitesse de port est supérieure à 1 Gb/s. Toutefois, selon le point de terminaison AWS Direct Connect qui dessert votre connexion, il peut être nécessaire d'activer ou de désactiver la négociation automatique pour les connexions à 1 Gbit/s. Si votre interface virtuelle reste inactive, consultez Dépannage de problèmes (de liaison de données) de niveau 2.
- L'encapsulation VLAN 802.1Q doit être prise en charge sur l'ensemble de la connexion, y compris les périphériques intermédiaires.
- Votre périphérique doit prendre en charge l'authentification protocole de passerelle frontière (BGP) et BGP MD5.
- (Facultatif) Vous pouvez configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau. Le BFD asynchrone est automatiquement activé pour chaque AWS Direct Connect interface virtuelle. Elle est automatiquement activée pour les interfaces virtuelles Direct Connect, mais ne prend effet que lorsque vous la configurez sur votre routeur. Pour plus d'informations, consultez Activer la BFD pour une connexion Direct Connect.

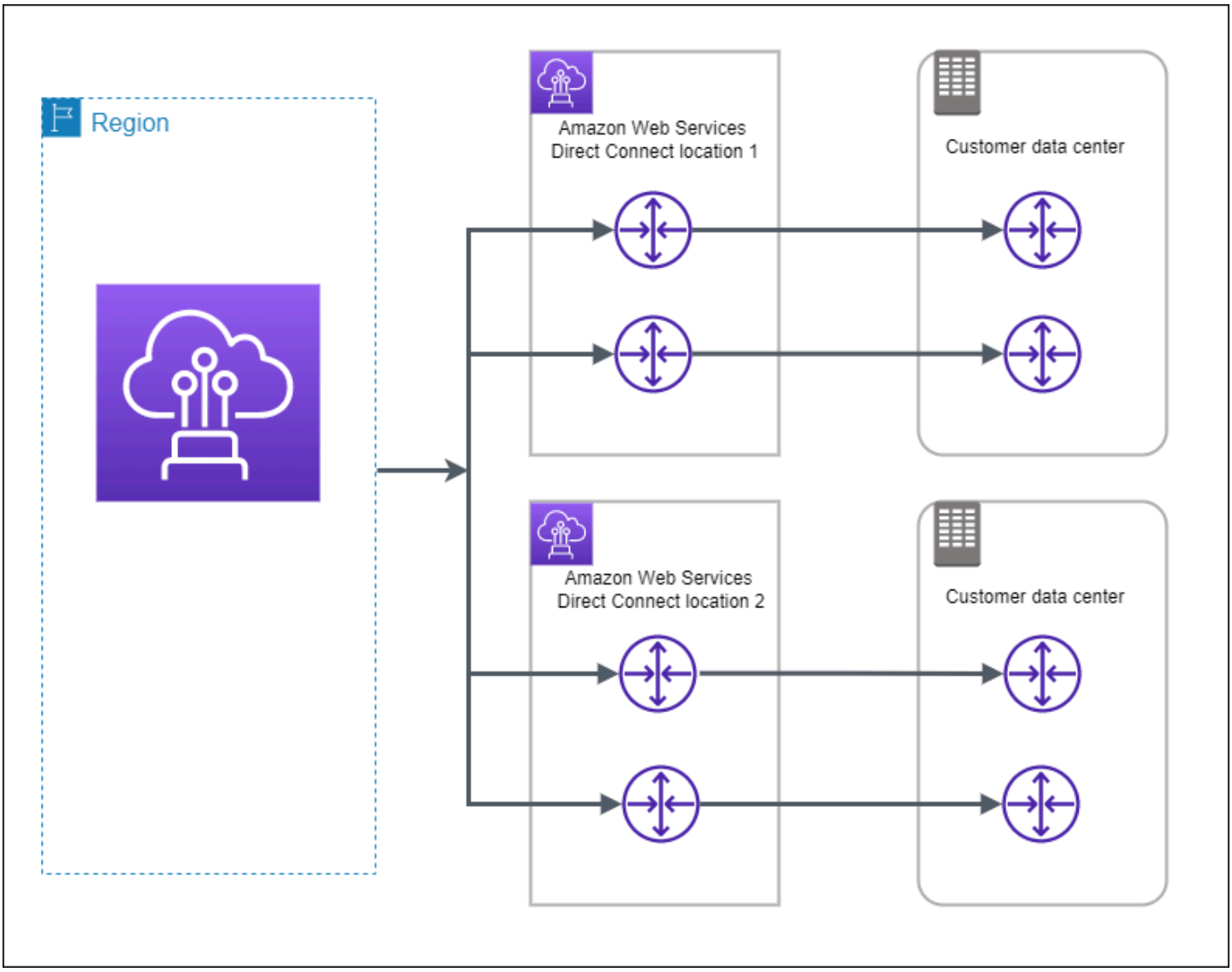
Veillez à disposer des informations suivantes avant de commencer votre configuration :

- Le modèle de résilience que vous souhaitez utiliser.
- La vitesse, l'emplacement et le partenaire pour toutes vos connexions.

Vous n'avez besoin de la vitesse que pour une seule connexion.

Résilience maximale

Vous pouvez obtenir une résilience maximale pour les charges de travail critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans plusieurs emplacements (comme illustré dans la figure suivante). Ce modèle offre une résilience contre les défaillances de l'appareil, de la connectivité et de l'emplacement complet. La figure suivante montre les deux connexions de chaque centre de données client vers les mêmes AWS Direct Connect emplacements. Vous pouvez éventuellement faire en sorte que chaque connexion d'un centre de données client soit dirigée vers différents emplacements.



Les procédures suivantes montrent comment utiliser le AWS Direct Connect Resiliency Toolkit pour configurer un modèle de résilience maximale.

Rubriques

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser AWS Direct Connect, vous avez besoin d'un AWS compte si vous n'en avez pas déjà un.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 : Configurer le modèle de résilience

Pour configurer un modèle de résilience maximale

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connexions, puis Créer une connexion.
3. Sous Connection ordering type (Type de commande de connexion), choisissez Connection wizard (Assistant de connexion).
4. Sous Resiliency level (Niveau de résilience), choisissez Maximum Resiliency, (Résilience maximale), puis Next (Suivant).
5. Dans le volet Configure connections (Configurer les connexions), sous Connection settings (Paramètres de connexion), procédez comme suit :

   a. Pour Bandwidth (Bande passante), choisissez la bande passante pour les connexions dédiées.

      Cette bande passante s'applique à toutes les connexions créées.

   b. Pour le premier fournisseur de services de localisation, sélectionnez l' AWS Direct Connect emplacement approprié pour la connexion dédiée.

   c. Le cas échéant, pour First Sub location (Premier sous-emplacement), choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) sur plusieurs étages du bâtiment.

d. Si vous avez sélectionné Other (Autre) pour First location service provider (Fournisseur de services du premier emplacement), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

e. Pour le fournisseur de services de deuxième localisation, sélectionnez l' AWS Direct Connect emplacement approprié.

f. Le cas échéant, pour Second Sub location (Deuxième sous-emplacement), choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) sur plusieurs étages du bâtiment.

g. Si vous avez sélectionné Other (Autre) pour Second location service provider (Fournisseur de services du deuxième emplacement), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

h. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

6. Choisissez Suivant.
7. Vérifiez vos connexions, puis choisissez Continue (Continuer).

   Si vos lettres d'autorisation (LOA) sont prêtes, vous pouvez choisir Download LOA (Télécharger la lettre d'autorisation), puis cliquer sur Continue (Continuer).

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures. Durant cette période de temps, vous pouvez recevoir un e-mail de demande d'informations supplémentaires sur votre cas d'utilisation ou sur l'emplacement spécifié. L'e-mail est envoyé à l'adresse e-mail que vous avez utilisée lors de votre inscription AWS. Vous devrez y répondre sous 7 jours, ou la connexion sera supprimée.

Étape 3 : Créer vos interfaces virtuelles

Vous pouvez créer une interface virtuelle privée pour vous connecter à votre VPC. Vous pouvez également créer une interface virtuelle publique pour vous connecter à des AWS services publics qui ne figurent pas dans un VPC. Lorsque vous créez une interface virtuelle privée vers un VPC,

vous avez besoin d'une interface virtuelle privée pour chaque VPC auquel vous vous connectez. Par exemple, vous avez besoin de trois interfaces virtuelles privées pour vous connecter à trois VPC.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.
Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool

Ressource	Informations obligatoires

	Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.10` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)
	
	Note
	Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies.

Ressource	Informations obligatoires
	• (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ou ASN appartiennent à un ISP ou un opérateur réseau, nous vous demandons des informations supplémentaires. Il peut s'agir d'un document présentant l'en-tête d'une

entreprise officielle ou d'un e-mail envoyé par le nom de domaine de l'entreprise attestant que vous pouvez utiliser le préfixe réseau/l'ASN.

Lorsque vous créez une interface virtuelle publique, l'examen et l'approbation de votre demande peuvent prendre jusqu' AWS à 72 heures.

Pour mettre en service une interface virtuelle publique pour des services non VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   d. Pour BGP ASN (Version du moteur de cache), saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Paramètres supplémentaires, procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour fournir votre propre clé BGP, saisissez votre clé MD5 BGP.

   Si vous ne saisissez aucune valeur, nous générons une clé BGP.

c. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Pour mettre en service une interface virtuelle privée sur un VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, pour Type, choisissez Privé.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour le Type de passerelle, choisissez Passerelle privée virtuelle ou passerelle Direct Connect.

   d. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis entrez le AWS compte.

e. Pour Passerelle privée virtuelle, sélectionnez la passerelle privée virtuelle à utiliser pour cette interface.

f. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

g. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

   Les valeurs valides sont 1 à 2147483647.

6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      > **Important**
      >
      > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même.
      >
      > - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
      > - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

      [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

   b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Étape 4 : Vérifier la configuration de résilience de votre interface virtuelle

Après avoir établi des interfaces virtuelles vers le AWS cloud ou vers Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour plus d'informations, consultez the section called "AWS Direct Connect Test de basculement".

Étape 5 : Vérifier la connectivité de vos interfaces virtuelles

Après avoir établi des interfaces virtuelles avec le AWS Cloud ou Amazon VPC, vous pouvez vérifier votre AWS Direct Connect connexion à l'aide des procédures suivantes.

Pour vérifier la connexion de votre interface virtuelle au AWS Cloud

- Exécutez `traceroute` et vérifiez que l' AWS Direct Connect identifiant figure dans la trace réseau.

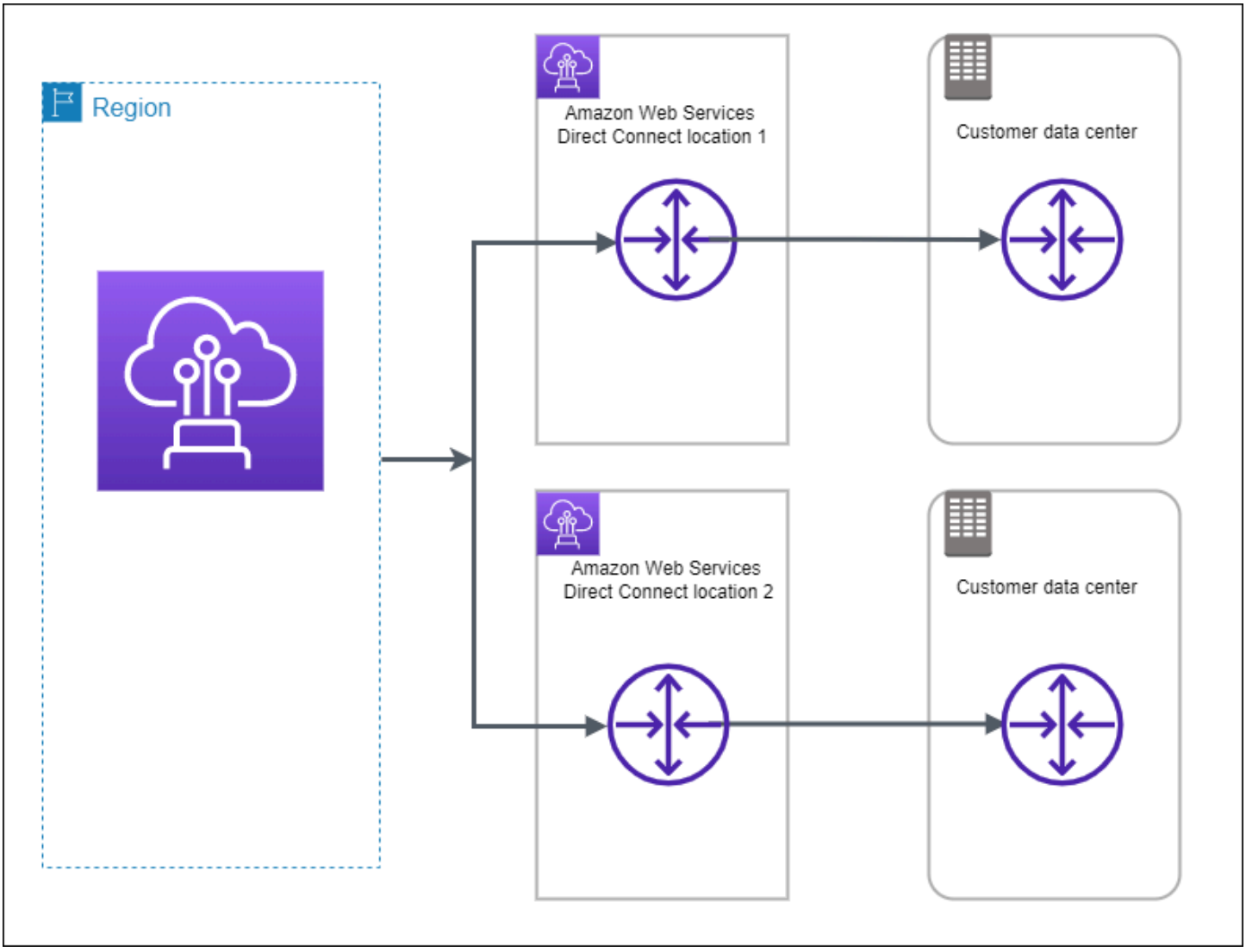
Pour vérifier la connexion de votre interface virtuelle à Amazon VPC

1. A l'aide d'une AMI pouvant être interrogée par une commande Ping, comme une AMI Amazon Linux, lancez une instance EC2 dans le VPC attaché à votre passerelle privée virtuelle. Les AMI Amazon Linux sont disponibles dans l'onglet Démarrage rapide lorsque vous utilisez l'assistant de lancement d'instance dans la console Amazon EC2. Pour plus d'informations, consultez la section Lancer une instance dans le guide de l'utilisateur Amazon EC2. Vérifiez que le groupe de sécurité associé à l'instance inclut une règle autorisant le trafic ICMP entrant (pour la requête ping).

2. Après l'exécution de l'instance, récupérez son adresse IPv4 privée (par exemple, 10.0.0.4). La console Amazon EC2 affiche l'adresse dans le cadre des détails de l'instance.
3. Interrogez l'adresse IPv4 privée par une commande Ping et obtenez une réponse.

Haute résilience

Vous pouvez obtenir une haute résilience pour les charges de travail critiques en utilisant deux connexions simples à plusieurs emplacements (comme illustré dans la figure suivante). Ce modèle offre une résilience contre les défaillances de connectivité provoquées par une coupure de fibre ou une défaillance d'appareil. Cela permet également d'éviter une défaillance complète de l'emplacement.



Les procédures suivantes montrent comment utiliser le AWS Direct Connect Resiliency Toolkit pour configurer un modèle à haute résilience.

Rubriques

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser AWS Direct Connect, vous avez besoin d'un AWS compte si vous n'en avez pas déjà un.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 : Configurer le modèle de résilience

Pour configurer un modèle de haute résilience

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connexions, puis Créer une connexion.
3. Sous Connection ordering type (Type de commande de connexion), choisissez Connection wizard (Assistant de connexion).
4. Sous Resiliency level (Niveau de résilience), choisissez High Resiliency, (Haute résilience), puis Next (Suivant).
5. Dans le volet Configure connections (Configurer les connexions), sous Connection settings (Paramètres de connexion), procédez comme suit :

   a. Pour Bandwidth (Bande passante), choisissez la bande passante pour les connexions.

      Cette bande passante s'applique à toutes les connexions créées.

   b. Pour le premier fournisseur de services de localisation, sélectionnez l' AWS Direct Connect emplacement approprié.

   c. Le cas échéant, pour First Sub location (Premier sous-emplacement), choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) sur plusieurs étages du bâtiment.

d. Si vous avez sélectionné Other (Autre) pour First location service provider (Fournisseur de services du premier emplacement), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

e. Pour le fournisseur de services de deuxième localisation, sélectionnez l' AWS Direct Connect emplacement approprié.

f. Le cas échéant, pour Second Sub location (Deuxième sous-emplacement), choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) sur plusieurs étages du bâtiment.

g. Si vous avez sélectionné Other (Autre) pour Second location service provider (Fournisseur de services du deuxième emplacement), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

h. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

6. Choisissez Suivant.
7. Vérifiez vos connexions, puis choisissez Continue (Continuer).

   Si vos lettres d'autorisation (LOA) sont prêtes, vous pouvez choisir Download LOA (Télécharger la lettre d'autorisation), puis cliquer sur Continue (Continuer).

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures. Durant cette période de temps, vous pouvez recevoir un e-mail de demande d'informations supplémentaires sur votre cas d'utilisation ou sur l'emplacement spécifié. L'e-mail est envoyé à l'adresse e-mail que vous avez utilisée lors de votre inscription AWS. Vous devrez y répondre sous 7 jours, ou la connexion sera supprimée.

Étape 3 : Créer vos interfaces virtuelles

Vous pouvez créer une interface virtuelle privée pour vous connecter à votre VPC. Vous pouvez également créer une interface virtuelle publique pour vous connecter à des AWS services publics qui ne figurent pas dans un VPC. Lorsque vous créez une interface virtuelle privée vers un VPC,

vous avez besoin d'une interface virtuelle privée pour chaque VPC auquel vous vous connectez. Par exemple, vous avez besoin de trois interfaces virtuelles privées pour vous connecter à trois VPC.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.
Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool

Ressource	Informations obligatoires

	Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.10` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)
	
	Note
	Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies.

Ressource	Informations obligatoires
	• (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ou ASN appartiennent à un fournisseur de services Internet ou à un opérateur réseau, vous AWS demande des informations supplémentaires. Il peut s'agir d'un document

présentant l'en-tête d'une entreprise officielle ou d'un e-mail envoyé par le nom de domaine de l'entreprise attestant que vous pouvez utiliser le préfixe réseau/l'ASN.

Lorsque vous créez une interface virtuelle publique, l'examen et l'approbation de votre demande peuvent prendre jusqu' AWS à 72 heures.

Pour mettre en service une interface virtuelle publique pour des services non VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   d. Pour BGP ASN (Version du moteur de cache), saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Paramètres supplémentaires, procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour fournir votre propre clé BGP, saisissez votre clé MD5 BGP.

   Si vous ne saisissez aucune valeur, nous générons une clé BGP.

c. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Pour mettre en service une interface virtuelle privée sur un VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, pour Type, choisissez Privé.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour le Type de passerelle, choisissez Passerelle privée virtuelle ou passerelle Direct Connect.

   d. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis entrez le AWS compte.

e. Pour Passerelle privée virtuelle, sélectionnez la passerelle privée virtuelle à utiliser pour cette interface.

f. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

g. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

   Les valeurs valides sont 1 à 2147483647.

6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      > **Important**
      >
      > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même.
      >
      > - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
      > - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

      [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

   b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Étape 4 : Vérifier la configuration de résilience de votre interface virtuelle

Après avoir établi des interfaces virtuelles vers le AWS cloud ou vers Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour plus d'informations, consultez the section called "AWS Direct Connect Test de basculement".

Étape 5 : Vérifier la connectivité de vos interfaces virtuelles

Après avoir établi des interfaces virtuelles avec le AWS Cloud ou Amazon VPC, vous pouvez vérifier votre AWS Direct Connect connexion à l'aide des procédures suivantes.

Pour vérifier la connexion de votre interface virtuelle au AWS Cloud

- Exécutez `traceroute` et vérifiez que l' AWS Direct Connect identifiant figure dans la trace réseau.

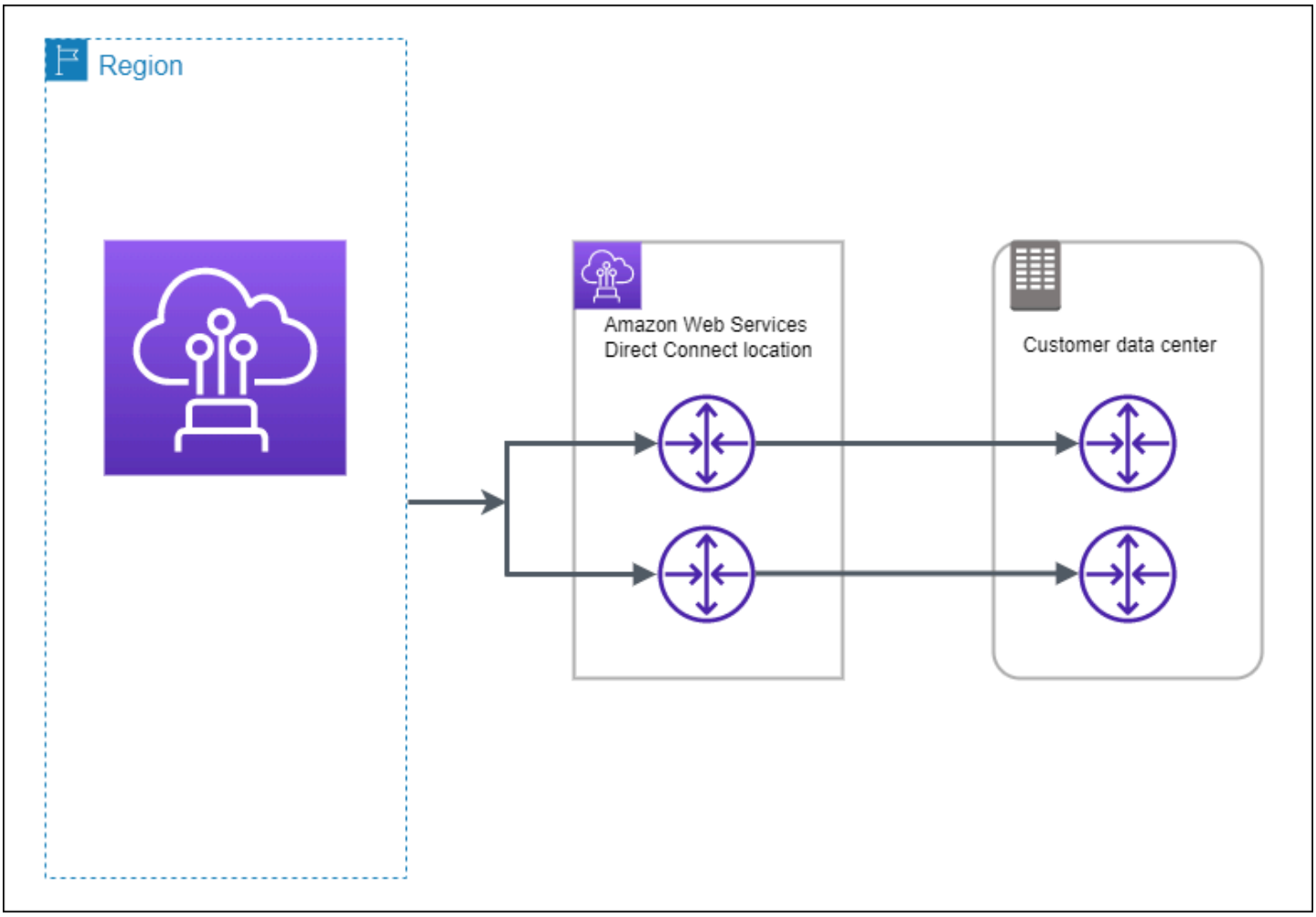
Pour vérifier la connexion de votre interface virtuelle à Amazon VPC

1. A l'aide d'une AMI pouvant être interrogée par une commande Ping, comme une AMI Amazon Linux, lancez une instance EC2 dans le VPC attaché à votre passerelle privée virtuelle. Les AMI Amazon Linux sont disponibles dans l'onglet Démarrage rapide lorsque vous utilisez l'assistant de lancement d'instance dans la console Amazon EC2. Pour plus d'informations, consultez la section Lancer une instance dans le guide de l'utilisateur Amazon EC2. Vérifiez que le groupe de sécurité associé à l'instance inclut une règle autorisant le trafic ICMP entrant (pour la requête ping).

2. Après l'exécution de l'instance, récupérez son adresse IPv4 privée (par exemple, 10.0.0.4). La console Amazon EC2 affiche l'adresse dans le cadre des détails de l'instance.
3. Interrogez l'adresse IPv4 privée par une commande Ping et obtenez une réponse.

Développement et test

Vous pouvez obtenir une résilience de développement et de test pour les charges de travail non critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans un seul emplacement (comme illustré dans la figure suivante). Ce modèle offre une résilience contre les défaillances de l'appareil, mais n'assure pas la résilience contre les défaillances de l'emplacement.



Les procédures suivantes montrent comment utiliser le AWS Direct Connect Resiliency Toolkit pour configurer un modèle de développement et de test de résilience.

Rubriques

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser AWS Direct Connect, vous avez besoin d'un AWS compte si vous n'en avez pas déjà un.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 : Configurer le modèle de résilience

Pour configurer le modèle de résilience

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connexions, puis Créer une connexion.
3. Sous Connection ordering type (Type de commande de connexion), choisissez Connection wizard (Assistant de connexion).
4. Sous Resiliency level (Niveau de résilience), choisissez Development and test, (Développement et test), puis Next (Suivant).
5. Dans le volet Configure connections (Configurer les connexions), sous Connection settings (Paramètres de connexion), procédez comme suit :

   a. Pour Bandwidth (Bande passante), choisissez la bande passante pour les connexions.

      Cette bande passante s'applique à toutes les connexions créées.

   b. Pour le premier fournisseur de services de localisation, sélectionnez l' AWS Direct Connect emplacement approprié.

   c. Le cas échéant, pour First Sub location (Premier sous-emplacement), choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) sur plusieurs étages du bâtiment.

   d. Si vous avez sélectionné Other (Autre) pour First location service provider (Fournisseur de services du premier emplacement), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

   e. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

6. Choisissez Suivant.
7. Vérifiez vos connexions, puis choisissez Continue (Continuer).

   Si vos lettres d'autorisation (LOA) sont prêtes, vous pouvez choisir Download LOA (Télécharger la lettre d'autorisation), puis cliquer sur Continue (Continuer).

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures. Durant cette période de temps, vous pouvez recevoir un e-mail de demande d'informations supplémentaires sur votre cas d'utilisation ou sur l'emplacement spécifié. L'e-mail est envoyé à l'adresse e-mail que vous avez utilisée lors de votre inscription AWS. Vous devrez y répondre sous 7 jours, ou la connexion sera supprimée.

Étape 3 : Créer une interface virtuelle

Pour commencer à utiliser votre AWS Direct Connect connexion, vous devez créer une interface virtuelle. Vous pouvez créer une interface virtuelle privée pour vous connecter à votre VPC. Vous pouvez également créer une interface virtuelle publique pour vous connecter à des AWS services publics qui ne figurent pas dans un VPC. Lorsque vous créez une interface virtuelle privée vers un VPC, vous avez besoin d'une interface virtuelle privée pour chaque VPC auquel vous vous connectez. Par exemple, vous avez besoin de trois interfaces virtuelles privées pour vous connecter à trois VPC.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.

Ressource	Informations obligatoires
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.

Ressource	Informations obligatoires

Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.10` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)

Ressource	Informations obligatoires
	Note Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ou ASN appartiennent à un ISP ou un opérateur réseau, nous vous demandons des informations supplémentaires. Il peut s'agir d'un document présentant l'en-tête d'une

entreprise officielle ou d'un e-mail envoyé par le nom de domaine de l'entreprise attestant que vous pouvez utiliser le préfixe réseau/l'ASN.

Lorsque vous créez une interface virtuelle publique, AWS peut prendre jusqu'à 72 heures pour vérifier ou approuver votre demande.

Pour mettre en service une interface virtuelle publique pour des services non VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   d. Pour BGP ASN (Version du moteur de cache), saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Paramètres supplémentaires, procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour fournir votre propre clé BGP, saisissez votre clé MD5 BGP.

   Si vous ne saisissez aucune valeur, nous générons une clé BGP.

c. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Pour mettre en service une interface virtuelle privée sur un VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, pour Type, choisissez Privé.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour le Type de passerelle, choisissez Passerelle privée virtuelle ou passerelle Direct Connect.

   d. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis entrez le AWS compte.

e. Pour Passerelle privée virtuelle, sélectionnez la passerelle privée virtuelle à utiliser pour cette interface.

f. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

g. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

   Les valeurs valides sont 1 à 2147483647.

6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      > **Important**
      >
      > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même.
      >
      > - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
      > - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

      [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

   b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Étape 4 : Vérifier la configuration de résilience de votre interface virtuelle

Après avoir établi des interfaces virtuelles vers le AWS cloud ou vers Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour plus d'informations, consultez the section called "AWS Direct Connect Test de basculement".

Étape 5 : Vérifier votre interface virtuelle

Après avoir établi des interfaces virtuelles avec le AWS Cloud ou Amazon VPC, vous pouvez vérifier votre AWS Direct Connect connexion à l'aide des procédures suivantes.

Pour vérifier la connexion de votre interface virtuelle au AWS Cloud

- Exécutez `traceroute` et vérifiez que l' AWS Direct Connect identifiant figure dans la trace réseau.

Pour vérifier la connexion de votre interface virtuelle à Amazon VPC

1. A l'aide d'une AMI pouvant être interrogée par une commande Ping, comme une AMI Amazon Linux, lancez une instance EC2 dans le VPC attaché à votre passerelle privée virtuelle. Les AMI Amazon Linux sont disponibles dans l'onglet Démarrage rapide lorsque vous utilisez l'assistant de lancement d'instance dans la console Amazon EC2. Pour plus d'informations, consultez la section Lancer une instance dans le guide de l'utilisateur Amazon EC2. Vérifiez que le groupe de sécurité associé à l'instance inclut une règle autorisant le trafic ICMP entrant (pour la requête ping).

2. Après l'exécution de l'instance, récupérez son adresse IPv4 privée (par exemple, 10.0.0.4). La console Amazon EC2 affiche l'adresse dans le cadre des détails de l'instance.
3. Interrogez l'adresse IPv4 privée par une commande Ping et obtenez une réponse.

Classique

Sélectionnez Classique lorsque vous disposez de connexions existantes.

Les procédures suivantes illustrent les scénarios courants de configuration de connexion AWS Direct Connect .

Table des matières

Prérequis

Pour les connexions AWS Direct Connect dont les vitesses de port sont supérieures ou égales à 1 Gbit/s, assurez-vous que votre réseau répond aux exigences suivantes :

- Votre réseau doit utiliser une fibre optique monomode avec un émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, un émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits ou un émetteur-récepteur 100GBASE-LR4 pour 100 gigabit Ethernet.
- La négociation automatique d'un port doit être désactivée pour une connexion dont la vitesse de port est supérieure à 1 Gb/s. Toutefois, selon le point de terminaison AWS Direct Connect qui dessert votre connexion, il peut être nécessaire d'activer ou de désactiver la négociation automatique pour les connexions à 1 Gbit/s. Si votre interface virtuelle reste inactive, consultez Dépannage de problèmes (de liaison de données) de niveau 2.

- L'encapsulation VLAN 802.1Q doit être prise en charge sur l'ensemble de la connexion, y compris les périphériques intermédiaires.
- Votre périphérique doit prendre en charge l'authentification protocole de passerelle frontière (BGP) et BGP MD5.
- (Facultatif) Vous pouvez configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau. Le BFD asynchrone est automatiquement activé pour chaque AWS Direct Connect interface virtuelle. Elle est automatiquement activée pour les interfaces virtuelles Direct Connect, mais ne prend effet que lorsque vous la configurez sur votre routeur. Pour plus d'informations, consultez Activer la BFD pour une connexion Direct Connect.

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser AWS Direct Connect, vous avez besoin d'un compte si vous n'en avez pas déjà un.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 : demander une connexion AWS Direct Connect dédiée

Pour les connexions dédiées, vous pouvez soumettre une demande de connexion à l'aide de la AWS Direct Connect console. Pour les connexions hébergées, contactez un AWS Direct Connect partenaire pour demander une connexion hébergée. Assurez-vous de disposer des informations suivantes :

- La vitesse du port requise. Vous ne pouvez pas modifier la vitesse de port une fois que vous avez créé la demande de connexion.
- AWS Direct Connect Emplacement auquel la connexion doit être interrompue.

> **Note**
>
> Vous ne pouvez pas utiliser la AWS Direct Connect console pour demander une connexion hébergée. Contactez plutôt un AWS Direct Connect partenaire, qui peut créer une connexion hébergée pour vous, que vous acceptez ensuite. Ignorer la procédure suivante et passez à Accepter votre connexion hébergée.

Pour créer une nouvelle AWS Direct Connect connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connexions, puis Créer une connexion.

3. Choisissez Classique.
4. Dans le volet Créer une connexion, sous Paramètres de connexion, procédez comme suit :

   a. Dans Nom, indiquez le nom de la connexion.

   b. Dans Emplacement, sélectionnez l'emplacement AWS Direct Connect approprié.

   c. Le cas échéant, pour Sous-emplacement, choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) à plusieurs étages du bâtiment.

   d. Pour Vitesse du port, choisissez la bande passante de connexion.

   e. Pour les applications sur site, sélectionnez Se connecter via un AWS Direct Connect partenaire lorsque vous utilisez cette connexion pour vous connecter à votre centre de données.

   f. Pour le fournisseur de services, sélectionnez le AWS Direct Connect partenaire. Si vous utilisez un partenaire qui ne figure pas dans la liste, sélectionnez Other (Autre).

   g. Si vous avez sélectionné Other (Autre) pour Service provider (Fournisseur de services), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.

   h. (Facultatif) Ajoutez ou supprimez une balise.

      [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

      - Pour Key (Clé), saisissez le nom de la clé.
      - Pour Valeur, saisissez la valeur de clé.

      [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

5. Choisissez Create Connection (Créer une connexion).

L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures. Durant cette période de temps, vous pouvez recevoir un e-mail de demande d'informations supplémentaires sur votre cas d'utilisation ou sur l'emplacement spécifié. L'e-mail est envoyé à l'adresse e-mail que vous avez utilisée lors de votre inscription AWS. Vous devrez y répondre sous 7 jours, ou la connexion sera supprimée.

Pour plus d'informations, consultez AWS Direct Connect connexions.

Accepter votre connexion hébergée

Vous devez accepter la connexion hébergée dans la AWS Direct Connect console avant de pouvoir créer une interface virtuelle. Cette étape s'applique uniquement aux connexions hébergées.

Pour accepter une interface virtuelle hébergée

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez la connexion hébergée, puis choisissez Accepter.

   Choisissez Accepter.

(Connexion dédiée) Étape 3 : Télécharger la LOA-CFA

Après votre demande de connexion, nous mettons à votre disposition une Lettre d'autorisation et l'Affectation d'installation de connexion (LOA-CFA) que vous pouvez télécharger, ou nous vous envoyons par e-mail une demande d'informations supplémentaires. La LOA-CFA est l'autorisation de connexion à AWS, et elle est requise par le fournisseur de colocation ou votre fournisseur de réseau pour établir la connexion interréseau (interconnexion).

Pour télécharger la LOA-CFA

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez la connexion et choisissez View details (Afficher les détails).
4. Choisissez Télécharger LOA-CFA.

   La LOA-CFA est téléchargée sur votre ordinateur au format PDF.

   > **Note**
   >
   > Si le lien n'est pas activé, cela signifie que la LOA-CFA n'est pas encore disponible pour téléchargement. Vérifiez que vous n'avez pas reçu d'e-mail vous demandant des

informations supplémentaires. Si elle n'est toujours pas disponible et que vous n'avez pas reçu d'e-mail après 72 heures, contactez le support AWS.

5. Après avoir téléchargé la LOA-CFA, procédez comme suit :

   - Si vous travaillez avec un AWS Direct Connect partenaire ou un fournisseur de réseau, envoyez-lui le LOA-CFA afin qu'il puisse commander une interconnexion pour vous sur place. AWS Direct Connect S'il ne peut pas commander la connexion transversale pour vous, vous pouvez contacter le fournisseur de colocalisation directement.
   - Si vous avez du matériel sur AWS Direct Connect place, contactez le fournisseur de colocation pour demander une connexion interréseau. Vous devez être client du fournisseur de colocalisation. Vous devez également leur présenter le LOA-CFA qui autorise la connexion au AWS routeur, ainsi que les informations nécessaires pour se connecter à votre réseau.

AWS Direct Connect les sites répertoriés comme plusieurs sites (par exemple, Equinix DC1-DC6 et DC10-DC11) sont configurés en tant que campus. Si votre équipement ou l'équipement de votre fournisseur de réseau est situé dans l'un de ces sites, vous pouvez demander une connexion transversale vers votre port attribué, même s'il se trouve dans un autre bâtiment sur le campus.

> **Important**
>
> Un campus est traité comme un AWS Direct Connect lieu unique. Pour bénéficier de la haute disponibilité, configurez des connexions vers différents emplacements AWS Direct Connect .

Si vous ou votre fournisseur de réseau rencontrez des problèmes pour établir une connexion physique, consultez Dépannage de problèmes (physiques) de niveau 1.

Étape 4 : Créer une interface virtuelle

Pour commencer à utiliser votre AWS Direct Connect connexion, vous devez créer une interface virtuelle. Vous pouvez créer une interface virtuelle privée pour vous connecter à votre VPC. Vous pouvez également créer une interface virtuelle publique pour vous connecter à des AWS services publics qui ne figurent pas dans un VPC. Lorsque vous créez une interface virtuelle privée vers un VPC, vous avez besoin d'une interface virtuelle privée pour chaque VPC auquel vous souhaitez vous connecter. Par exemple, vous avez besoin de trois interfaces virtuelles privées pour vous connecter à trois VPC.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.
Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même

Ressource	Informations obligatoires

	interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.0` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)
	
	Note
	Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies.
	  • (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour

Ressource	Informations obligatoires
	l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Nous vous demandons des informations supplémentaires si vos préfixes publics ou ASN appartiennent à un ISP ou un opérateur réseau. Il peut s'agir d'un document présentant l'en-tête

d'une entreprise officielle ou d'un e-mail envoyé par le nom de domaine de l'entreprise attestant que vous pouvez utiliser le préfixe réseau/l'ASN.

Pour les interfaces virtuelles privées et les interfaces virtuelles publiques, l'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus grand paquet admissible qui peut être transmis sur la connexion. La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 9001 (trames jumbo). La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 8500 (trames jumbo). Vous pouvez spécifier la MTU lorsque vous créez l'interface ou la mettre à jour après l'avoir créée. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Pour vérifier si une connexion ou une interface virtuelle prend en charge les images jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez Jumbo Frame Capable dans l'onglet Résumé.

Lorsque vous créez une interface virtuelle publique, l'examen et l'approbation de votre demande peuvent prendre jusqu' AWS à 72 heures.

Pour mettre en service une interface virtuelle publique pour des services non VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.
   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.
   c. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).
   d. Pour BGP ASN, entrez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Paramètres supplémentaires, procédez comme suit :

a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

   [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

   - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
   - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

   [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour fournir votre propre clé BGP, saisissez votre clé MD5 BGP.

   Si vous ne saisissez aucune valeur, nous générons une clé BGP.

c. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Pour mettre en service une interface virtuelle privée sur un VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, pour Type, choisissez Privé.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :

a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

c. Pour le Type de passerelle, choisissez Passerelle privée virtuelle ou passerelle Direct Connect.

d. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis entrez le AWS compte.

e. Pour Passerelle privée virtuelle, sélectionnez la passerelle privée virtuelle à utiliser pour cette interface.

f. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

g. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

   Les valeurs valides sont 1 à 2147483647.

6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      > **Important**
      >
      > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même.
      >
      > - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.

- Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.
8. Vous devez utiliser votre périphérique BGP pour publier le réseau que vous utilisez pour la connexion VIF publique.

Étape 5 : Télécharger la configuration de routeur

Après avoir créé une interface virtuelle pour votre AWS Direct Connect connexion, vous pouvez télécharger le fichier de configuration du routeur. Le fichier contient les commandes nécessaires pour configurer votre routeur afin qu'il soit utilisé avec votre interface virtuelle publique ou privée.

Pour télécharger la configuration du routeur

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez la connexion et choisissez View details (Afficher les détails).
4. Choisissez Télécharger la configuration de routeur.
5. Pour Télécharger la configuration de routeur, procédez comme suit :

a. Pour Fournisseur, sélectionnez le fabricant de votre routeur.

b. Pour Plateforme, sélectionnez le modèle de votre routeur.

c. Pour Logiciels, sélectionnez la version du logiciel de votre routeur.

6. Choisissez Télécharger, puis utilisez la configuration appropriée pour votre routeur afin de vous assurer de pouvoir vous connecter à AWS Direct Connect:

Pour accéder à des exemples de fichiers de configuration, consultez Exemples de fichiers de configuration du routeur.

Une fois que vous avez configuré votre routeur, le statut de l'interface virtuelle devient UP. Si l'interface virtuelle reste inactive et que vous ne pouvez pas envoyer de ping à l'adresse IP homologue de l' AWS Direct Connect appareil, consultezDépannage de problèmes (de liaison de données) de niveau 2. Si vous pouvez pinger l'adresse IP d'appairage, consultez Dépannage des problèmes (de réseau/transport) de niveau 3/4. Si la session d'appairage BGP est établie, mais que vous ne parvenez pas à acheminer le trafic, consultez Dépannage des problèmes de routage.

Étape 6 : Vérifier votre interface virtuelle

Après avoir établi des interfaces virtuelles avec le AWS Cloud ou Amazon VPC, vous pouvez vérifier votre AWS Direct Connect connexion à l'aide des procédures suivantes.

Pour vérifier la connexion de votre interface virtuelle au AWS Cloud

- Exécutez `traceroute` et vérifiez que l' AWS Direct Connect identifiant figure dans le traçage réseau.

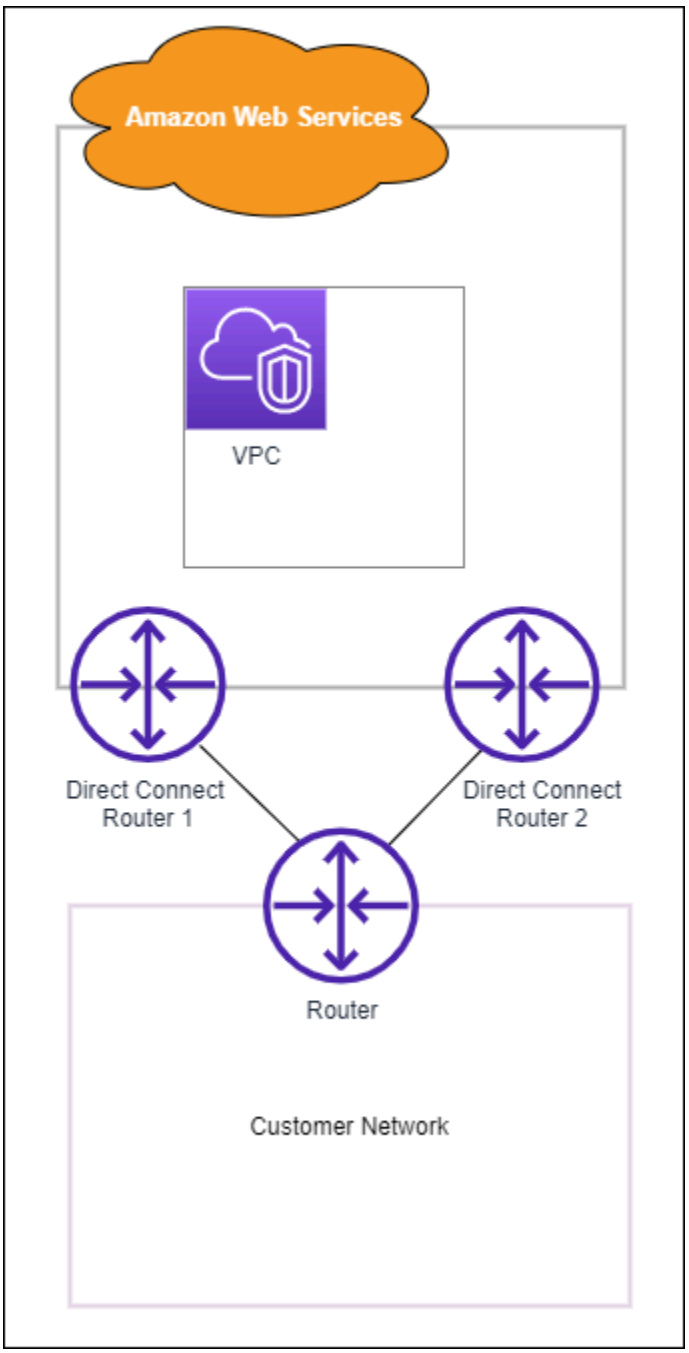
Pour vérifier la connexion de votre interface virtuelle à Amazon VPC

1. A l'aide d'une AMI pouvant être interrogée par une commande Ping, comme une AMI Amazon Linux, lancez une instance EC2 dans le VPC attaché à votre passerelle privée virtuelle. Les AMI Amazon Linux sont disponibles dans l'onglet Démarrage rapide lorsque vous utilisez l'assistant de lancement d'instance dans la console Amazon EC2. Pour plus d'informations, consultez la section Lancer une instance dans le guide de l'utilisateur Amazon EC2. Vérifiez que le groupe de sécurité associé à l'instance inclut une règle autorisant le trafic ICMP entrant (pour la requête ping).

2. Après l'exécution de l'instance, récupérez son adresse IPv4 privée (par exemple, 10.0.0.4). La console Amazon EC2 affiche l'adresse dans le cadre des détails de l'instance.
3. Interrogez l'adresse IPv4 privée par une commande Ping et obtenez une réponse.

(Recommandé) Étape 7 : Configurer les connexions redondantes

Pour permettre le basculement, nous vous recommandons de demander et de configurer deux connexions dédiées à AWS, comme illustré dans la figure suivante. Ces connexions peuvent se terminer sur un ou deux routeurs de votre réseau.



Différentes configurations s'offrent à vous lorsque vous mettez en service deux connexions dédiées :

- Actif/Actif (plusieurs chemins BGP). Il s'agit de la configuration par défaut, dans laquelle les deux connexions sont actives. AWS Direct Connect prend en charge le multiacheminement vers plusieurs interfaces virtuelles au même endroit, et le trafic est partagé entre les interfaces en fonction du flux. Si une connexion devient indisponible, l'ensemble du trafic est acheminé via l'autre connexion.

- Actif/Passif (basculement). Une connexion gère le trafic tandis que l'autre est en veille. Si la connexion active devient indisponible, l'ensemble du trafic est acheminé via la connexion passive. Vous devez ajouter le préfixe AS_PATH aux routes sur l'un de vos liens pour qu'il devienne le lien passif.

La façon dont vous configurez les connexions n'a pas d'incidence sur la redondance, mais elle a une incidence sur les stratégies qui déterminent la façon dont vos données sont acheminées via les deux connexions. Nous vous recommandons de configurer les deux connexions comme étant actives.

Si vous utilisez une connexion VPN pour la redondance, veillez à mettre en place un mécanisme de vérification de l'état et de basculement. Si vous utilisez l'une des configurations suivantes, vous devez vérifier le routage de la table de routage pour acheminer vers la nouvelle interface réseau.

- Vous utilisez vos propres instances pour le routage. Par exemple, l'instance est le pare-feu.
- Vous utilisez votre propre instance qui met fin à une connexion VPN.

Pour atteindre une haute disponibilité, nous vous recommandons vivement de configurer des connexions vers différents AWS Direct Connect sites.

Pour plus d'informations sur AWS Direct Connect la résilience, consultez les recommandations en matière de AWS Direct Connect résilience.

AWS Direct Connect Test de basculement

Les modèles de résilience Boîte à outils de résilience AWS Direct Connect sont conçus pour vous assurer que vous disposez du nombre approprié de connexions d'interfaces virtuelles dans plusieurs emplacements. Une fois l'exécution de l'assistant terminée, utilisez le test de basculement Boîte à outils de résilienc AWS Direct Connect pour réduire la session d'appairage BGP afin de vérifier que le trafic est acheminé vers l'une de vos interfaces virtuelles redondantes et répond à vos exigences de résilience.

Utilisez le test pour vous assurer que le trafic est acheminé sur des interfaces virtuelles redondantes lorsqu'une interface virtuelle est hors service. Vous démarrez le test en sélectionnant une interface virtuelle, une session d'appairage BGP et la durée d'exécution du test. AWS place la session d'appairage BGP de l'interface virtuelle sélectionnée sur l'état down. Lorsque l'interface est définie sur cet état, le trafic doit passer par une interface virtuelle redondante. Si votre configuration ne contient pas les connexions redondantes appropriées, la session d'appairage BGP échoue et le trafic n'est

pas acheminé. Lorsque le test est terminé ou que vous arrêtez manuellement le test, AWS restaure la session BGP. Une fois le test terminé, vous pouvez utiliser la Boîte à outils de résilience AWS Direct Connect pour ajuster votre configuration.

> **Note**
>
> N'utilisez pas cette fonctionnalité pendant une période de maintenance de Direct Connect car la session BGP peut être restaurée prématurément pendant ou après la maintenance.

Historique des tests

AWS supprime l'historique des tests après 365 jours. L'historique des tests inclut l'état des tests exécutés sur tous les appairages BGP. L'historique inclut les sessions d'appairage BGP testées, les heures de début et de fin et l'état du test, qui peut être l'une des valeurs suivantes :

- En cours : le test est en cours d'exécution.
- Terminé : le test a été exécuté pendant la durée spécifiée.
- Annulé : le test a été annulé avant l'heure spécifiée.
- Échec : le test n'a pas été exécuté pendant la durée spécifiée. Ceci peut se produire lorsqu'il y a un problème avec le routeur.

Pour plus d'informations, consultez the section called "Affichage de l'historique des tests de basculement de l'interface virtuelle".

Autorisations de validation

Le seul compte qui a l'autorisation d'exécuter le test de basculement est le compte qui possède l'interface virtuelle. Le propriétaire du compte reçoit une indication via AWS CloudTrail qu'un test a été exécuté sur une interface virtuelle.

Démarrage du test de basculement de l'interface virtuelle

Vous pouvez démarrer le test de basculement de l'interface virtuelle à l'aide de la console AWS Direct Connect ou de l'outil AWS CLI.

Pour démarrer le test de basculement de l'interface virtuelle à partir de la console AWS Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Choisissez Interfaces virtuelles.
3. Sélectionnez les interfaces virtuelles, puis choisissez Actions, Réduire le BGP.

   Vous pouvez exécuter le test sur une interface virtuelle publique, privée ou de transit.
4. Dans la boîte de dialogue Démarrer le test d'échec, procédez comme suit :

   a. Pour Appairages à réduire pour test, choisissez les sessions d'appairage à tester, par exemple IPv4.
   b. Pour Durée maximale du test, saisissez la durée du test en minutes.

      La valeur maximale est de 4.320 minutes (72 heures).

      La valeur par défaut est de 180 minutes (3 heures).
   c. Pour Pour confirmer le test, saisissez Confirmer.
   d. Choisissez Confirmer.

   La session d'appairage BGP est placée sur l'état DOWN. Vous pouvez envoyer du trafic pour vérifier qu'il n'y a pas de pannes. Si nécessaire, vous pouvez arrêter le test immédiatement.

Pour démarrer le test de basculement de l'interface virtuelle à l'aide de l'outil AWS CLI

Utilise StartBgpFailoverTest.

Affichage de l'historique des tests de basculement de l'interface virtuelle

Vous pouvez afficher l'historique des tests de basculement de l'interface virtuelle à l'aide de la console AWS Direct Connect ou de l'outil AWS CLI.

Pour afficher l'historique des tests de basculement de l'interface virtuelle à partir de la console AWS Direct Connecte

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.

2. Choisissez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).
4. Choisissez Historique des tests.

   La console affiche les tests d'interface virtuelle que vous avez effectués pour l'interface virtuelle.
5. Pour afficher les détails d'un test spécifique, sélectionnez l'identifiant du test.

Pour afficher l'historique des tests de basculement de l'interface virtuelle à l'aide de l'outil AWS CLI

Utilise ListVirtualInterfaceTestHistory.

Arrêt du test de basculement de l'interface virtuelle

Vous pouvez arrêter le test de basculement de l'interface virtuelle à l'aide de la console AWS Direct Connect ou de l'outil AWS CLI.

Pour arrêter le test de basculement de l'interface virtuelle à partir de la console AWS Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Choisissez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle, puis choisissez Actions, Annuler le test.
4. Choisissez Confirmer.

AWS restaure la session d'appairage BGP. L'historique des tests affiche « annulé » pour le test.

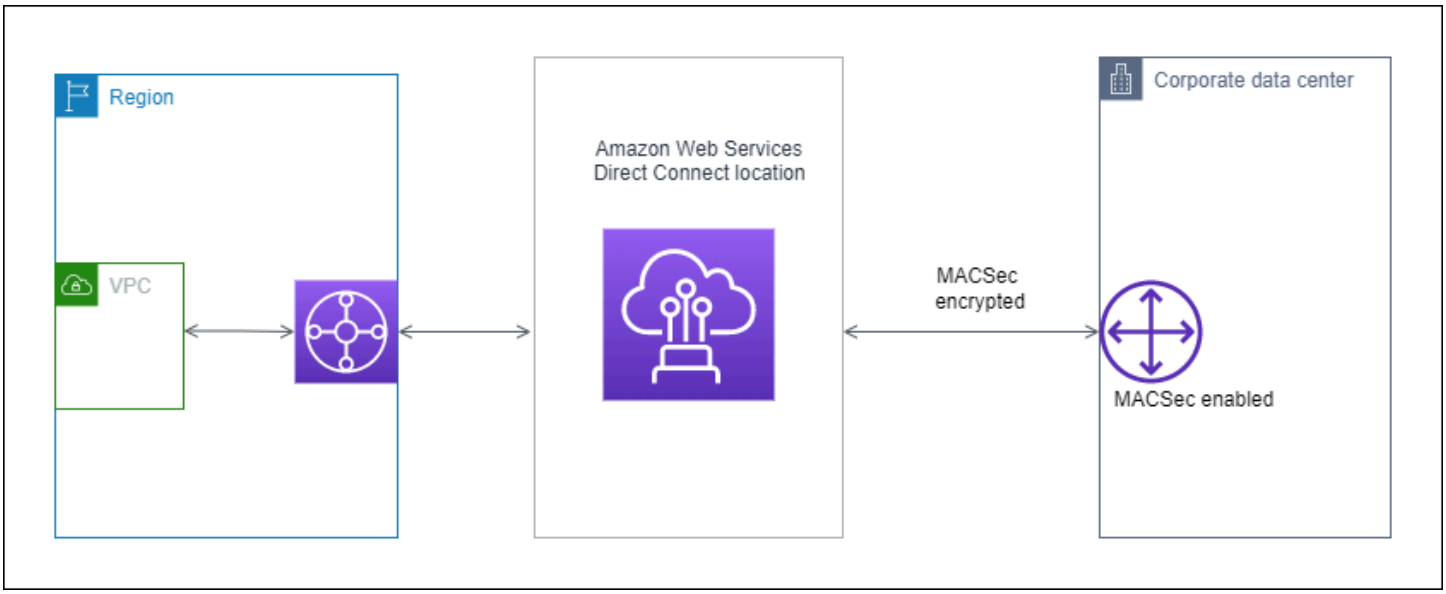
Pour arrêter le test de basculement de l'interface virtuelle à l'aide de l'outil AWS CLI

Utilise StopBgpFailoverTest.

Sécurité MAC

MAC Security (MACsec) est une norme IEEE qui garantit la confidentialité, l'intégrité des données et l'authenticité de l'origine des données. MacSec fournit un point-to-point chiffrement de couche 2 via la connexion croisée à. AWS MacSec fonctionne au niveau de la couche 2 entre deux routeurs de couche 3 et fournit le chiffrement sur le domaine de couche 2. Toutes les données circulant sur le réseau AWS mondial interconnecté aux centres de données et aux régions sont automatiquement cryptées au niveau de la couche physique avant de quitter le centre de données.

Dans le diagramme suivant, la connexion dédiée et vos ressources sur site doivent prendre en charge MACsec. Le trafic de couche 2 qui transite via la connexion dédiée vers ou depuis le centre de données est chiffré.



Concepts de MACsec

Les principaux concepts de MACsec sont les suivants :

- La sécurité MAC (MACsec) : une norme IEEE 802.1 de couche 2 qui garantit la confidentialité, l'intégrité et l'authenticité de l'origine des données. Pour plus d'informations sur le protocole, consultez 802.1AE : sécurité MAC (MACsec).
- Clé secrète MACsec : clé pré-partagée qui établit la connectivité MACsec entre le routeur local du client et le port de connexion sur le site. AWS Direct Connect La clé est générée par les appareils situés aux extrémités de la connexion à l'aide de la paire CKN/CAK que vous avez fournie à votre appareil AWS et que vous avez également configurée sur celui-ci.

- Le Nom de la clé de connexion (CKN) et la Clé d'association de connectivité (CAK) : les valeurs de cette paire sont utilisées pour générer la clé secrète MACsec. Vous générez les valeurs de paire, vous les associez à une AWS Direct Connect connexion et vous les configurez sur votre appareil Edge à la fin de la AWS Direct Connect connexion.

Connexions prises en charge

MACsec est disponible sur les connexions dédiées. Pour plus d'informations sur la façon de commander des connexions compatibles MACsec, consultez AWS Direct Connect.

Commencee à utiliser MACsec sur des connexions dédiées

Les tâches suivantes vous aideront à vous familiariser avec MacSec sur des connexions AWS Direct Connect dédiées. L'utilisation de MacSec est gratuite.

Avant de configurer MacSec sur une connexion dédiée, notez ce qui suit :

- MACsec est prise en charge sur les connexions Direct Connect dédiées de 10 Gb/s et 100 Gb/s aux points de présence sélectionnés. Pour ces connexions, les suites de chiffrement MacSec suivantes sont prises en charge :
  - Pour les connexions 10 Gbit/s, GCM-AES-256 et GCM-AES-XPN-256.
  - Pour les connexions 100 Gbit/s, GCM-AES-XPN-256.

- Seules les clés MacSec 256 bits sont prises en charge.
- La numérotation étendue des paquets (XPN) est requise pour les connexions 100 Gbit/s. Pour les connexions 10 Gbit/s, Direct Connect prend en charge le GCM-AES-256 et le GCM-AES-XPN-256. Les connexions haut débit, telles que les connexions dédiées à 100 Gbit/s, peuvent rapidement épuiser l'espace de numérotation des paquets 32 bits d'origine de MacSec, ce qui vous obligerait à faire pivoter vos clés de chiffrement toutes les quelques minutes pour établir une nouvelle association de connectivité. Pour éviter cette situation, la modification de la norme IEEE 802.1aeBW-2013 a introduit la numérotation étendue des paquets, augmentant l'espace de numérotation à 64 bits, allégeant ainsi les exigences de rapidité pour la rotation des clés.
- L'identifiant de canal sécurisé (SCI) est requis et doit être activé. Ce paramètre ne peut pas être ajusté.
- La balise IEEE 802.1Q (Dot1q/VLAN) offset/dot1 n'q-in-clear est pas prise en charge pour déplacer une balise VLAN en dehors d'une charge utile chiffrée.

Pour plus d'informations sur Direct Connect et MacSec, consultez la section MacSec des AWS Direct Connect FAQ.

Rubriques

Conditions préalables requises pour MACsec

Exécutez les tâches suivantes avant de configurer MACsec sur une connexion dédiée.

- Créez une paire CKN/CAK pour la clé secrète MACsec.

  Vous pouvez créer la paire à l'aide d'un outil standard ouvert. La paire doit répondre aux exigences décrites dans the section called “Étape 4 : configurer votre routeur sur site”.
- Assurez-vous de disposer d'un appareil compatible avec MACsec à votre extrémité de la connexion.
- Le Secure Channel Identifier (SCI) doit être activé.
- Seules les clés MACsec 256 bits sont prises en charge, offrant ainsi la toute dernière protection avancée des données.

Rôles liés à un service

AWS Direct Connect utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Direct Connect Les rôles liés au service sont prédéfinis par AWS Direct Connect et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. Un rôle lié à un service facilite la configuration AWS Direct Connect car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Direct Connect définit les autorisations associées à ses rôles liés aux services

et, sauf indication contraire, seul AWS Direct Connect peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM. Pour plus d'informations, consultez the section called "Rôles liés à un service".

Considérations clés sur le protocole CKN/CAK pré-partagé par MACsec

AWS Direct Connect utilise des CMK AWS gérées pour les clés pré-partagées que vous associez à des connexions ou à des LAG. Secrets Manager stocke vos paires CKN et CAK pré-partagées sous forme de secret chiffré par la clé racine du Secrets Manager. Pour en savoir plus, veuillez consulter la rubrique CMK gérées par AWS dans le Guide du développeur AWS Key Management Service .

La clé stockée est par nature en lecture seule, mais vous pouvez planifier une suppression de sept à trente jours à l'aide de la console ou de l'API AWS Secrets Manager. Lorsque vous planifiez une suppression, le CKN ne peut pas être lu, ce qui peut affecter votre connectivité réseau. Dans ce cas, nous appliquons les règles suivantes :

- Si la connexion est en attente, nous dissocions le CKN de la connexion.
- Si la connexion est disponible, nous en informons le propriétaire par e-mail. Si vous ne prenez aucune mesure dans les 30 jours, nous dissocierons le CKN de votre connexion.

Lorsque nous dissocions le dernier CKN de votre connexion et que le mode de chiffrement de la connexion est défini sur « doit chiffrer », nous définissons le mode sur « should_encrypt » pour éviter toute perte soudaine de paquets.

Étape 1 : Créer une connexion

Pour commencer à utiliser MACsec, vous devez activer cette fonctionnalité lorsque vous créez une connexion dédiée. Pour plus d'informations, consultez the section called "Créer une connexion à l'aide de l'assistant de connexion".

(Facultatif) Étape 2 : créer un groupe d'agrégation de liaisons (LAG)

Si vous utilisez plusieurs connexions à des fins de redondance, vous pouvez créer un LAG compatible avec MACsec. Pour plus d'informations, consultez the section called "Considérations sur la MACsec" et the section called "Créer un LAG".

Étape 3 : associer le CKN/CAK à la connexion ou au LAG

Après avoir créé la connexion ou le LAG compatible avec MACsec, vous devez associer un CKN/CAK à la connexion. Pour plus d'informations, consultez les étapes suivantes :

- the section called “Associer une MACsec CKN/CAK à une connexion”
- the section called “Associer une MACsec CKN/CAK à un LAG”

Étape 4 : configurer votre routeur sur site

Mettez à jour votre routeur sur site avec la clé secrète MACsec. La clé secrète MacSec du routeur local et celle de l' AWS Direct Connect emplacement doivent correspondre. Pour plus d'informations, consultez the section called “Télécharger le fichier de configuration du routeur”.

Étape 5 : (Facultatif) supprimer l'association entre le CKN/CAK et la connexion ou le LAG

Si vous devez supprimer l'association entre la clé MACsec et la connexion ou le LAG, consultez l'une des manières suivantes :

- the section called “Supprimer l'association entre une connexion et une clé secrète MACsec”
- the section called “Supprimer l'association entre un LAG et une clé secrète MACsec”

AWS Direct Connect connexions

AWS Direct Connect vous permet d'établir une connexion réseau dédiée entre votre réseau et l'un des AWS Direct Connect sites.

Il existe deux types de connexions :

- Connexion dédiée : une connexion Ethernet physique associée à un seul client. Les clients peuvent demander une connexion dédiée via la AWS Direct Connect console, la CLI ou l'API. Pour plus d'informations, consultez the section called "Connexions dédiées".
- Connexion hébergée : connexion Ethernet physique qu'un AWS Direct Connect partenaire fournit pour le compte d'un client. Pour demander une connexion hébergée, les clients doivent contacter un partenaire du programme de partenariat AWS Direct Connect , lequel alloue la connexion. Pour plus d'informations, consultez the section called "Connexions hébergées".

Connexions dédiées

Pour créer une connexion dédiée AWS Direct Connect , vous avez besoin des informations suivantes :

AWS Direct Connect location

Travaillez avec un partenaire dans le cadre du programme de AWS Direct Connect partenariat pour vous aider à établir des circuits réseau entre un AWS Direct Connect site et votre centre de données, votre bureau ou votre environnement de colocation. Il peut également contribuer à fournir un espace de colocalisation au sein de la même installation que l'emplacement. Pour plus d'informations, consultez Partenaires APN prenant en charge AWS Direct Connect.

Vitesse du port

Les valeurs possibles sont 1 Gb/s, 10 Gb/s et 100 Gb/s.

Vous ne pouvez pas modifier la vitesse de port une fois que vous avez créé la demande de connexion. Pour modifier la vitesse du port, vous devez créer et configurer une nouvelle connexion.

Vous pouvez créer une connexion à l'aide de l'assistant de connexion ou créer une connexion classique. À l'aide de l'assistant de connexion, vous pouvez configurer des connexions à l'aide

des recommandations relatives à la résilience. L'assistant est recommandé si vous configurez des connexions pour la première fois. Si vous préférez, vous pouvez utiliser la version classique pour créer des connexions one-at-a-time. La version classique est recommandée si vous avez déjà une configuration existante à laquelle vous souhaitez ajouter des connexions. Vous pouvez créer une connexion autonome ou une connexion à associer à un LAG dans votre compte. Si vous associez une connexion à un LAG, elle est créée avec les mêmes vitesse du port et emplacement que ceux spécifiés dans le LAG.

Après votre demande de connexion, nous mettons à votre disposition une Lettre d'autorisation - Affectation d'installation de connexion (LOA-CFA) que vous pouvez télécharger, ou vous envoie par e-mail une demande d'informations supplémentaires. Si vous recevez une demande d'informations supplémentaires, vous devez y répondre sous 7 jours, sinon la connexion sera supprimée. Le LOA-CFA est l'autorisation de connexion à AWS, et est exigé par votre fournisseur de réseau pour commander une connexion croisée pour vous. Si vous n'avez pas d'équipement sur AWS Direct Connect place, vous ne pouvez pas commander de connexion croisée pour vous-même sur place.

Les opérations suivantes sont disponibles pour les connexions dédiées :

- the section called “Créer une connexion à l'aide de l'assistant de connexion”
- the section called “Créer une connexion classique”
- the section called “Afficher les détails de votre connexion”
- the section called “Mise à jour d'une connexion”
- the section called “Associer une MACsec CKN/CAK à une connexion”
- the section called “Supprimer l'association entre une connexion et une clé secrète MACsec”
- the section called “Supprimer les connexions”

Vous pouvez ajouter une connexion dédiée à un groupe d'agrégation de liaisons (LAG), ce qui vous permet de traiter plusieurs connexions comme une seule. Pour plus d’informations, veuillez consulter Associer une connexion à un LAG.

Après avoir créé une connexion, créez une interface virtuelle pour vous connecter à des ressources AWS publiques et privées. Pour plus d’informations, consultez AWS Direct Connect interfaces virtuelles.

Si vous ne disposez d'aucun équipement sur un AWS Direct Connect site, contactez d'abord un AWS Direct Connect partenaire dans le cadre du programme de AWS Direct Connect partenariat. Pour plus d'informations, consultez Partenaires APN prenant en charge AWS Direct Connect.

Si vous souhaitez créer une connexion qui utilise la sécurité MAC (MACsec), passez en revue les conditions préalables requises avant de créer la connexion. Pour plus d'informations, consultez the section called "Conditions préalables requises pour MACsec ".

Créer une connexion à l'aide de l'assistant de connexion

Cette section décrit la création d'une connexion à l'aide de l'assistant de connexion. Si vous préférez créer une connexion classique, consultez les étapes indiquées sur the section called "Étape 2 : demander une connexion AWS Direct Connect dédiée".

Pour créer une connexion à l'aide de l'assistant de connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connexions, puis Créer une connexion.
3. Sur la page Créer une connexion, sous Type de commande de connexion, choisissez Assistant de connexion.
4. Choisissez un Niveau de résilience pour vos connexions réseau. Un niveau de résilience peut être l'un des suivants :

   - Résilience maximale
   - Haute résilience
   - Développement et test

   Pour obtenir des descriptions et des informations plus détaillées sur ces niveaux de résilience, consultez Utiliser le AWS Direct Connect Resiliency Toolkit pour démarrer.
5. Choisissez Suivant.
6. Sur la page Configurer les connexions, fournissez les informations suivantes.

   a. Dans la liste déroulante Bande passante, choisissez la bande passante requise pour votre connexion. Cela peut aller de 1 Gb/s à 100 Gb/s.

   b. Pour Emplacement, choisissez l' AWS Direct Connect emplacement approprié, puis choisissez le premier fournisseur de services de localisation, sélectionnez le fournisseur de services fournissant la connectivité pour la connexion à cet emplacement.

   c. Pour Deuxième emplacement, choisissez le lieu approprié AWS Direct Connect au deuxième emplacement, puis choisissez le fournisseur de services du deuxième emplacement,

sélectionnez le fournisseur de services fournissant la connectivité pour la connexion à ce deuxième emplacement.

d. (Facultatif) Configurez la sécurité MAC (MACsec) pour la connexion. Sous Paramètres supplémentaires, sélectionnez Demander un port compatible MACsec.

   MACsec est disponible uniquement sur les connexions dédiées.

e. (Facultatif) Choisissez Ajouter une balise pour ajouter des paires clé/valeur afin de mieux identifier cette connexion.

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise existante, choisissez-la, puis choisissez Supprimer la balise. Vous ne pouvez pas avoir de balises vides.

7. Choisissez Suivant.
8. Sur la page Vérifier et créer, vérifiez la connexion. Cette page affiche également les coûts estimés pour l'utilisation du port et les frais supplémentaires de transfert de données.
9. Choisissez Créer.
10. Téléchargez votre Lettre d'autorisation et votre Affectation d'installation de connexion (LOA-CFA). Pour plus d'informations, consultez the section called “Télécharger la LOA-CFA”.

Utilisez l'une des commandes suivantes.

- create-connection (AWS CLI)
- CreateConnection(AWS Direct Connect API)

Créer une connexion classique

Pour les connexions dédiées, vous pouvez soumettre une demande de connexion à l'aide de la AWS Direct Connect console. Pour les connexions hébergées, contactez un AWS Direct Connect partenaire pour demander une connexion hébergée. Assurez-vous de disposer des informations suivantes :

- La vitesse du port requise. Pour les connexions dédiées, vous ne pouvez pas modifier la vitesse de port une fois que vous avez créé la demande de connexion. Pour les connexions hébergées, votre partenaire AWS Direct Connect peut modifier la vitesse.

- AWS Direct Connect Emplacement auquel la connexion doit être interrompue.

> **Note**
>
> Vous ne pouvez pas utiliser la AWS Direct Connect console pour demander une connexion hébergée. Contactez plutôt un AWS Direct Connect partenaire, qui peut créer une connexion hébergée pour vous, que vous acceptez ensuite. Ignorer la procédure suivante et passez à Accepter votre connexion hébergée.

Pour créer une nouvelle AWS Direct Connect connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Sur l'écran AWS Direct Connect, sous Mise en route, choisissez Création d'une connexion.
3. Choisissez Classique.
4. Dans Nom, indiquez le nom de la connexion.
5. Dans Emplacement, sélectionnez l'emplacement AWS Direct Connect approprié.
6. Le cas échéant, pour Sous-emplacement, choisissez l'étage le plus proche de vous ou de votre fournisseur de réseau. Cette option n'est disponible que si l'emplacement comprend des salles d'interconnexion (MMR) à plusieurs étages du bâtiment.
7. Pour Vitesse du port, choisissez la bande passante de connexion.
8. Pour Sur site), sélectionnez Se connecter via un partenaire AWS Direct Connect lorsque vous utilisez cette connexion pour vous connecter à votre centre de données.
9. Pour le fournisseur de services, sélectionnez le AWS Direct Connect partenaire. Si vous utilisez un partenaire qui ne figure pas dans la liste, sélectionnez Other (Autre).
10. Si vous avez sélectionné Other (Autre) pour Service provider (Fournisseur de services), pour Name of other provider (Nom de l'autre fournisseur), saisissez le nom du partenaire que vous utilisez.
11. (Facultatif) Choisissez Ajouter une balise pour ajouter des paires clé/valeur afin de mieux identifier cette connexion.
    - Pour Clé, saisissez le nom de la clé.
    - Pour Valeur, saisissez la valeur de clé.

Pour supprimer une balise existante, choisissez-la, puis choisissez Supprimer la balise. Vous ne pouvez pas avoir de balises vides.

12. Choisissez Create Connection (Créer une connexion).

L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures. Durant cette période de temps, vous pouvez recevoir un e-mail de demande d'informations supplémentaires sur votre cas d'utilisation ou sur l'emplacement spécifié. L'e-mail est envoyé à l'adresse e-mail que vous avez utilisée lors de votre inscription AWS. Vous devrez y répondre sous 7 jours, ou la connexion sera supprimée.

Pour plus d'informations, consultez AWS Direct Connect connexions.

Télécharger la LOA-CFA

Après avoir traité votre demande de connexion, vous pouvez télécharger la LOA-CFA. Si le lien n'est pas activé, cela signifie que la LOA-CFA n'est pas encore disponible pour téléchargement. Vérifiez si vous avez reçu un e-mail vous demandant des informations.

La facturation commence automatiquement lorsque le port est actif ou 90 jours après l'émission de la LOA, selon la première éventualité. Vous pouvez éviter les frais de facturation en supprimant le port avant l'activation ou dans les 90 jours suivant l'émission de la LOA.

Si votre connexion n'est pas opérationnelle au bout de 90 jours et que la LOA-CFA n'a pas été émise, nous vous enverrons un e-mail vous avertissant que le port sera supprimé dans 10 jours. Si vous n'activez pas le port dans les 10 jours supplémentaires, le port sera automatiquement supprimé et vous devrez recommencer le processus de création du port.

> **Note**
>
> Pour plus d'informations sur la tarification, consultez Tarification d'AWS Direct Connect. Si vous n'avez plus besoin de la connexion une fois que vous avez réédité la LOA-CFA, vous devez supprimer vous-même la connexion. Pour plus d'informations, consultez Supprimer les connexions.

Console

Pour télécharger la LOA-CFA

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez la connexion et puis choisissez Afficher les détails.
4. Choisissez Télécharger LOA-CFA.

> **Note**
>
> Si le lien n'est pas activé, cela signifie que la LOA-CFA n'est pas encore disponible pour téléchargement. Un cas de support sera créé pour demander des informations supplémentaires. Une fois que vous aurez répondu à la demande et que celle-ci aura été traitée, le LOA-CFA sera disponible au téléchargement. S'il n'est toujours pas disponible, contactez le Support AWS.

5. Envoyez la LOA-CFA à votre fournisseur de réseau ou de colocalisation pour qu'ils puissent vous commander une connexion transversale. Le processus de contact peut varier pour chaque fournisseur de colocalisation. Pour plus d'informations, consultez Demande de connexions croisées sur AWS Direct Connect des sites.

Command line

Pour télécharger la LOA-CFA à l'aide de la ligne de commande ou de l'API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

Mise à jour d'une connexion

Vous pouvez mettre à jour les attributs de connexion suivants :

- Nom de la connexion.
- Le mode de chiffrement MACsec de la connexion.

> **Note**
>
> MACsec est disponible uniquement sur les connexions dédiées.

Les valeurs valides sont :

- `should_encrypt`
- `must_encrypt`

  Lorsque vous définissez le mode de chiffrement sur cette valeur, la connexion est interrompue lorsque le chiffrement est interrompu.
- `no_encrypt`

Console

Pour mettre à jour une connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez la connexion et puis choisissez Modifier.
4. Modifiez la connexion :

   [Modifier le nom] Pour Nom, saisissez un nouveau nom pour la connexion.

   [Add a tag] Choisissez Add tag (Ajouter une balise) et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.
5. Choisissez Modifier la connexion.

Command line

Pour ajouter et supprimer une balise à l'aide de la ligne de commande

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Pour mettre à jour une connexion à l'aide de la ligne de commande ou de l'API

- update-connection (mise à jour de la connexion) (AWS CLI)
- UpdateConnection(AWS Direct Connect API)

Associer une MACsec CKN/CAK à une connexion

Après avoir créé la connexion compatible avec MACsec, vous pouvez associer un CKN/CAK à la connexion.

> **Note**
>
> Vous ne pouvez pas modifier une clé secrète MACsec après l'avoir associée à une connexion. Si vous devez modifier la clé, dissociez-la de la connexion, puis associez une nouvelle clé à la connexion. Pour plus d'informations sur la suppression d'une association, veuillez consulter the section called “Supprimer l'association entre une connexion et une clé secrète MACsec”.

Console

Pour associer une clé MACsec à une connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, choisissez Connexions.
3. Sélectionnez une connexion et puis choisissez Afficher les détails.
4. Choisissez Associer une clé.
5. Saisissez la clé MACsec.

[Utiliser la paire CAK/CKN] Choisissez Paire de clés, puis procédez comme suit :

- Pour la Clé d'association de connectivité (CAK), saisissez la CAK.
- Pour le Nom de la clé d'association de connectivité (CKN), saisissez le CKN.

[Utiliser le secret] Choisissez le secret Existing Secret Manager, puis pour Secret, sélectionnez la clé secrète MACsec.

6. Choisissez Associer une clé.

Command line

Pour associer une clé MACsec à une connexion

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

Supprimer l'association entre une connexion et une clé secrète MACsec

Vous pouvez supprimer l'association entre la connexion et la clé MACsec.

Console

Pour supprimer une association entre une connexion et une clé MACsec

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2.
3. Dans le volet de gauche, choisissez Connexions.
4. Sélectionnez une connexion et puis choisissez Afficher les détails.
5. Sélectionnez le secret MACsec à supprimer, puis choisissez Dissocier la clé.
6. Dans la boîte de dialogue de confirmation, saisissez dissocier, puis choisissez Dissocier.

Command line

Pour supprimer une association entre une connexion et une clé MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

Connexions hébergées

Pour créer une connexion AWS Direct Connect hébergée, vous avez besoin des informations suivantes :

AWS Direct Connect location

Travaillez avec un AWS Direct Connect partenaire dans le cadre du programme de AWS Direct Connect partenariat pour vous aider à établir des circuits réseau entre un AWS Direct Connect site et votre centre de données, votre bureau ou votre environnement de colocation. Il peut également contribuer à fournir un espace de colocalisation au sein de la même installation que l'emplacement. Pour plus d'informations, consultez Partenaires de livraison AWS Direct Connect.

> **Note**
>
> Vous ne pouvez pas demander une connexion hébergée via la AWS Direct Connect console. Toutefois, un AWS Direct Connect partenaire peut créer et configurer une connexion hébergée pour vous. Une fois configurée, la connexion s'affiche dans le volet Connexions de la console.
> Vous devez accepter la connexion hébergée avant de pouvoir l'utiliser. Pour plus d'informations, consultez the section called "Accepter une connexion hébergée".

Vitesse du port

Pour les connexions hébergées, les valeurs possibles sont 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s et 25 Gbit/s. Notez que seuls les AWS Direct Connect partenaires répondant à des exigences spécifiques peuvent créer une connexion hébergée de 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s ou 25 Gbit/s. Les connexions 25 Gbit/s ne sont disponibles que dans les emplacements Direct Connect où des vitesses de port de 100 Gbit/s sont disponibles.

Notez ce qui suit :

- Les vitesses des ports de connexion ne peuvent être modifiées que par votre AWS Direct Connect partenaire. Vous n'êtes plus obligé de supprimer puis de recréer une connexion afin de mettre à niveau ou de réduire la bande passante d'une connexion hébergée existante. Pour modifier la vitesse de votre port, veuillez contacter le AWS Direct Connect partenaire qui gère votre connexion hébergée.
- AWS utilise la régulation du trafic sur les connexions hébergées, ce qui signifie que lorsque le débit de trafic atteint le débit maximal configuré, le trafic excédentaire est supprimé. Cela peut entraîner le fait qu'un trafic « en rafales » présente un débit inférieur à celui d'un trafic non « en rafales ».
- Les trames Jumbo peuvent être activées sur les connexions uniquement si elles sont initialement activées sur la connexion parent hébergée AWS Direct Connect . Si les trames Jumbo ne sont pas activées sur cette connexion parent, elles ne peuvent être activées sur aucune connexion.

Les opérations de console suivantes sont disponibles une fois que vous avez demandé une connexion hébergée et que vous l'avez acceptée :

- the section called "Afficher les détails de votre connexion"
- the section called "Mise à jour d'une connexion"
- the section called "Supprimer les connexions"

Après avoir accepté une connexion, créez une interface virtuelle pour vous connecter à des ressources AWS publiques et privées. Pour plus d'informations, consultez AWS Direct Connect interfaces virtuelles.

Accepter une connexion hébergée

Si vous souhaitez acheter une connexion hébergée, vous devez contacter un AWS Direct Connect AWS Direct Connect partenaire du programme de partenariat. Le partenaire mettra la connexion en service. Une fois que la connexion est configurée, elle s'affiche dans le volet Connexions de la console AWS Direct Connect .

Avant de pouvoir commencer à utiliser une connexion hébergée, vous devez accepter la connexion.

Console

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez la connexion et choisissez Afficher les détails.
4. Cochez la case de confirmation et choisissez Accepter.

Command line

Pour créer une connexion à l'aide de la ligne de commande ou de l'API

- confirm-connection (AWS CLI)
- ConfirmConnection(AWS Direct Connect API)

Afficher les détails de votre connexion

Vous pouvez afficher l'état actuel de votre connexion. Vous pouvez également afficher votre ID de connexion (par exemple, `dxcon-12nikabc`) et vérifier qu'il correspond à celui figurant sur la LOA-CFA que vous avez reçue ou téléchargée.

Pour plus d'informations sur la surveillance des connexions, consultez Surveillance.

Console

Pour afficher les informations sur une connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, choisissez Connexions.
3. Sélectionnez une connexion et puis choisissez Afficher les détails.

Command line

Pour créer une connexion à l'aide de la ligne de commande ou de l'API

- describe-connections (AWS CLI)

- DescribeConnections(AWS Direct Connect API)

Supprimer les connexions

Vous pouvez supprimer une connexion tant qu'aucune interface virtuelle n'y est attachée. La suppression de votre connexion met fin à tous les frais d'heure de port associés à cette connexion, mais des frais de connexion croisée ou de circuit réseau peuvent tout de même vous être facturés (voir ci-dessous). AWS Direct Connect les frais de transfert de données sont associés aux interfaces virtuelles. Pour plus d'informations sur la suppression d'une interface virtuelle, consultez la page Supprimer les interfaces virtuelles.

Avant de supprimer une connexion, téléchargez le LOA correspondant à la connexion contenant les informations entre comptes afin de disposer des informations pertinentes sur les circuits déconnectés. Pour connaître les étapes à suivre pour télécharger la LOA de connexion, consultez the section called “Télécharger la LOA-CFA”.

Lorsque vous supprimez une connexion, AWS demandez au fournisseur de colocation de déconnecter votre périphérique réseau du routeur Direct Connect en retirant le câble de raccordement à fibre optique du panneau de brassage approprié. AWS Cependant, votre fournisseur de colocation ou de circuit peut toujours vous facturer des frais de connexion croisée ou de circuit réseau, car le câble de connexion croisée est peut-être toujours connecté à votre périphérique réseau. Ces frais de connexion sont indépendants de Direct Connect et doivent être annulés auprès du fournisseur de colocation ou du circuit en utilisant les informations de la LOA.

Si la connexion fait partie du groupe d'agrégation de liaisons (LAG), il est impossible de la supprimer sans que le LAG devienne inférieur au nombre minimum de connexions opérationnelles configuré.

Console

Pour supprimer une connexion

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez les connexions, puis choisissez Supprimer.
4. Dans la boîte de dialogue de confirmation Supprimer, sélectionnez Supprimer.

Command line

Pour supprimer une connexion à l'aide de la ligne de commande ou de l'API

- delete-connection (AWS CLI)
- DeleteConnection(AWS Direct Connect API)

Demande de connexions croisées sur AWS Direct Connect des sites

Lorsque vous avez téléchargé votre Lettre d'autorisation - Affectation d'installation de connexion (LOA-CFA), vous devez finaliser votre connexion inter-réseau, également appelée connexion transversale. Si votre équipement se trouve déjà sur un AWS Direct Connect site, contactez le fournisseur approprié pour effectuer le raccordement croisé. Pour obtenir des informations spécifiques pour chaque fournisseur, consultez le tableau ci-dessous. Contactez votre fournisseur pour connaître la tarification d'une connexion transversale. Lorsque la connexion transversale est établie, vous pouvez créer les interfaces virtuelles à l'aide de la console AWS Direct Connect .

Certains lieux sont configurés sous forme de campus. Pour plus d'informations, y compris les vitesses disponibles dans chaque emplacement, consultez la section Emplacements AWS Direct Connect.

Si vous ne possédez pas encore d'équipement sur un AWS Direct Connect site, vous pouvez travailler avec l'un des partenaires du réseau de AWS partenaires (APN). Il vous aidera à vous connecter à un emplacement AWS Direct Connect . Pour plus d'informations, consultez la section Support des partenaires APN. AWS Direct Connect Vous devez communiquer la LOA-CFA au fournisseur que vous avez sélectionné afin de simplifier votre demande de connexion transversale.

Une AWS Direct Connect connexion peut donner accès à des ressources dans d'autres régions. Pour de plus amples informations, veuillez consulter Accès à une région AWS à distance.

> **Note**
>
> Si la connexion transversale n'est pas terminée dans un délai de 90 jours, l'autorisation accordée par la LOA-CFA expire. Pour renouveler une LOA-CFA expirée, vous pouvez la télécharger à nouveau à partir de la console AWS Direct Connect . Pour de plus amples informations, veuillez consulter Télécharger la LOA-CFA.

Colocalisations

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)

- USA Ouest (Oregon)
- Afrique (Le Cap)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Chine (Beijing)
- Chine (Ningxia)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Milan)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Zurich)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)
- Amérique du Sud (São Paulo)
- AWS GovCloud (USA Est)
- AWS GovCloud (US-Ouest)

USA Est (Ohio)

Emplacement	Comment demander une connexion
Cologix COL2, Columbus	Contactez Cologix à l'adresse sales@cologix.com.

Emplacement	Comment demander une connexion
Cologix MIN3, Minneapolis	Contactez Cologix à l'adresse sales@cologix.com.
CyrusOne West III, Houston	Envoyez une demande à l'aide du portail client.
Equinix CH2, Chicago	Contactez Equinix à l'adresse awsdealreg@equinix.com.
QTS, Chicago	Contactez QTS à l'adresse AConnect@qtsdatacenters.com.
Centres de données Netrality, 1102 Grand, Kansas City	Contactez les Centres de données Netrality à l'adresse support@netrality.com.

USA Est (Virginie du Nord)

Emplacement	Comment demander une connexion
165 Halsey Street, Newark	Contactez operations@165halsey.com.
CoreSite 32 km, New York	Passez une commande via le portail CoreSite client. Une fois que vous avez rempli le formulaire, vérifiez que la commande est correcte et validez-la sur le site web.
CoreSite VA1-VA2, Reston	Passez une commande sur le portail CoreSite client. Une fois que vous avez rempli le formulaire, vérifiez que la commande est correcte et validez-la sur le site web.
Immobilier numérique ATL1 et ATL2, Atlanta	Contactez Digital Realty à l'adresse amazon.orders@digitalrealty.com.
Immobilier numérique IAD38, Ashburn	Contactez Digital Realty à l'adresse amazon.orders@digitalrealty.com.
Equinix DC1-DC6 et DC10-D12, Ashburn	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix DAA1-DC3 et DC6, Dallas	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
Equinix MI1, Miami	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Contactez Equinix à l'adresse awsdealreg@equinix.com.
KIO Networks QRO1, Querétaro, Mexique	Contactez KIO Networks ».
Markley, One Summer Street, Boston	Pour les clients actuels, créez une demande via le portail client. Pour les nouvelles demandes, contactez sales@markleygroup.com.
Neutrality Data Centers, MMR, 2e étage, Philadelphie	Contactez les Centres de données Netrality à l'adresse support@netrality.com.
QTS ATL 1, Atlanta	Contactez QTS à l'adresse AConnect@qtsdatacenters.com.

USA Ouest (Californie du Nord)

Emplacement	Comment demander une connexion
CoreSite, LA1, Los Angeles	Passez une commande via le portail CoreSite client. Une fois que vous avez rempli le formulaire, vérifiez que la commande est correcte et validez-la sur le site web.
CoreSite SV2, Milpitas	Passez une commande via le portail CoreSite client. Une fois que vous avez rempli le formulaire, vérifiez que la commande est correcte et validez-la sur le site web.
CoreSite SV4, Santa Clara	Passez une commande via le portail CoreSite client. Après avoir rempli le formulaire, vérifiez l'exactitude de la commande, puis approuvez-la MyCoreSite sur le site Web.
EdgeConneX, Phénix	Passez une commande à l'aide du portail client EdgeOS. Après avoir soumis le formulaire, EdgeConne X fournira un formulaire de commande de service pour approbation. Vous

Emplacement	Comment demander une connexion
	pouvez envoyer vos questions à l'adresse cloudaccess@edgeconnex.com.
Equinix LA3, El Segundo	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix SV1 et SV5, San José	Contactez Equinix à l'adresse awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Contactez phoenixNAP Provisioning à l'adresse provisioning@phoenixnap.com.

USA Ouest (Oregon)

Emplacement	Comment demander une connexion
CoreSite DE1, Denver	Passez une commande via le portail CoreSite client. Une fois que vous avez rempli le formulaire, vérifiez que la commande est correcte et validez-la sur le site web.
Digital Realty SEA10, bâtiment Westin, Seattle	Contactez Digital Realty à l'adresse amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Passez une commande à l'aide du portail client EdgeOS. Après avoir soumis le formulaire, EdgeConne X fournira un formulaire de commande de service pour approbation. Vous pouvez envoyer vos questions à l'adresse cloudaccess@edgeconnex.com.
Equinix SE2, Seattle	Contactez Equinix à l'adresse support@equinix.com.
Pittock Block, Portland	Envoyez les demandes par e-mail à l'adresse crossconnect@pittock.com ou par téléphone au +1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Contactez Switch SUPERNAP à l'adresse orders@supernap.com.
TierPoint Seattle	Contactez-nous TierPoint à l'adresse sales@tierpoint.com.

Afrique (Le Cap)

Emplacement	Comment demander une connexion
Cape Town Internet Exchange/Centres de données Teraco	Contactez Teraco à l'adresse support@teraco.co.za pour les clients Teraco existants ou connect@teraco.co.za pour les nouveaux clients.
Teraco JB1, Johannesburg, Afrique du Sud	Contactez Teraco à l'adresse support@teraco.co.za pour les clients Teraco existants ou connect@teraco.co.za pour les nouveaux clients.

Asie-Pacifique (Jakarta)

Emplacement	Comment demander une connexion
DCI JK3, Jakarta	Contactez DCI Indonesia à l'adresse jessie.w@dci-indonesia.com.com.
Centre de données NTT 2, Jakarta	Contactez NTT à l'adresse tps.cms.presales@global.ntt.

Asie-Pacifique (Mumbai)

Emplacement	Comment demander une connexion
Equinix, Bombay	Contactez Equinix à l'adresse awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Contactez le NetMagic service des ventes et du marketing au numéro gratuit 18001033130 ou à marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Contactez Sify à l'adresse aws.directconnect@sifycorp.com.
STT Delhi DC2, Delhi	Contactez STT sur demande. AWSDX@sttelemediagdc .in.

Emplacement	Comment demander une connexion
STT GDC Pvt. Ltd. VSB, Chennai	Contactez STT sur demande. AWSDX@sttelemediagdc .in.
STT Hyderabad DC1, Hyderabad	Contactez STT sur demande. AWSDX@sttelemediagdc .in.

Asie-Pacifique (Séoul)

Emplacement	Comment demander une connexion
Digital Realty ICN1, Séoul	Contactez Digital Realty à l'adresse amazon.orders@digitalrealty.com.
Centre de données KINX Gasan, Séoul	Contactez KINX à l'adresse sales@kinx.net.
LG U+ Pyeong-Chon Mega Center, Séoul	Envoyez le document LOA à kidcadmin@lguplus.co.kr et center8@kidc.net.

Asie-Pacifique (Singapour)

Emplacement	Comment demander une connexion
Equinix HK1, Tsuen Wan N.T., RAS de Hong Kong	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix SG2, Singapour	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Global Switch, Singapour	Contactez Global Switch à l'adresse salessingapore@globalswitch.com.
GPX, Mumbai	Contactez GPX (Equinix) à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
iAdvantage Mega-i, Hong Kong	Contactez iAdvantage à l'adresse cs@iadvantage.net ou passez une commande via le formulaire électronique de commande de câblage iAdvantage.
Menara AIMS, Kuala Lumpur	Les clients AIMS existants peuvent commander une connexion transversale via le portail du service client, en remplissant le formulaire de demande d'intervention (Engineering Work Order Request Form). Ils peuvent contacter service.delivery@aims.com.my en cas de problème pour soumettre la demande.
Centre de données TCC, Bangkok	Contactez TCC Technology Co., Ltd à l'adresse gateway.ne@tcc-technology.com.

Asie-Pacifique (Sydney)

Emplacement	Comment demander une connexion
CDC Hume 2, Canberra	Connectez-vous au portail client sur le portail client du CDC.
Datacom DH6, Auckland	Contactez Datacom chez Datacom Orbit —Auckland.
Equinix ME2, Melbourne	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix SY3, Sydney	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Global Switch, Sydney	Contactez Global Switch à l'adresse salessydney@globalswitch.com.
NEXTDC C1, Canberra	Contactez NEXTDC à l'adresse nxtops@nextdc.com.
NEXTDC M1, Melbourne	Contactez NEXTDC à l'adresse nxtops@nextdc.com.
NEXTDC P1, Perth	Contactez NEXTDC à l'adresse nxtops@nextdc.com.
NEXTDC S2, Sydney	Contactez NEXTDC à l'adresse nxtops@nextdc.com.

Asie-Pacifique (Tokyo)

Emplacement	Comment demander une connexion
Centre de données AT Tokyo Chuo, Tokyo	Contactez AT TOKYO à l'adresseat-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Contactez Chief Telecom à l'adresse vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Contactez CHT Taipei IDC NOC à l'adresse taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix TY2, Tokyo	Contactez Equinix à l'adresse awsdealreg@equinix.com.
NEC Inzai, Inzaï	Contactez NEC Inzai à l'adresse connection_support@ices.jp.nec.com.

Canada (Centre)

Emplacement	Comment demander une connexion
Allied 250 Front St W, Toronto	Contactez driches@alliedreit.com.
Cologix MTL3, Montréal	Contactez Cologix à l'adresse sales@cologix.com.
Cologix VAN2, Vancouver	Contactez Cologix à l'adresse sales@cologix.com.
eStruxture, Montreal	Contactez eStruxture à l'adresse directconnect@estruxture.com.

Chine (Beijing)

Emplacement	Comment demander une connexion
CIDS Jiachuang IDC, Beijing	Contactez dx-order@sinnet.com.cn.

Emplacement	Comment demander une connexion
Sinnet Jiuxianqiao IDC, Beijing	Contactez dx-order@sinnet.com.cn.
GDS No. 3 Data Center, Shanghai	Contactez dx@nwcdcloud.cn.
GDS No. 3 Data Center, Shenzhen	Contactez dx@nwcdcloud.cn.

Chine (Ningxia)

Emplacement	Comment demander une connexion
Industrial Park IDC, Ningxia	Contactez dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Contactez dx@nwcdcloud.cn.

Europe (Francfort)

Emplacement	Comment demander une connexion
CE Colo, Prague, République tchèque	Contactez CE Colo à l'adresse info@cecolo.com.
DigiPlex Ulven, Oslo, Norvège	Contactez-nous DigiPlex à l'adresse helpme@digiplex.com.
Equinix AM3, Amsterdam, Pays-Bas	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix FR5, Francfort	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix HE6, Helsinki	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix MU1, Munich	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix WA1, Varsovie	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
Interxion AMS7, Amsterdam	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion CPH2, Copenhagen	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion FRA6, Francfort	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion MAD2, Madrid	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion VIE2, Vienne	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion ZUR1, Zurich	Contactez Interxion à l'adresse customer.services@interxion.com.
IPB, Berlin	Contactez IPB à l'adresse kontakt@ipb.de.
Equinix ITConic MD2, Madrid	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Europe (Irlande)

Emplacement	Comment demander une connexion
Digital Realty (Royaume-Uni), Docklands	Contactez Digital Realty (Royaume-Uni) à l'adresse amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Contactez Eircom à l'adresse awsorders@eircom.ie.
Equinix DX1, Dublin	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix LD5, Londres (Slough)	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
Interxion DUB2, Dublin	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion MRS1, Marseille	Contactez Interxion à l'adresse customer.services@interxion.com.

Europe (Milan)

Emplacement	Comment demander une connexion
CDLAN srl Via Caldera 21, Milan	Contactez CDLAN à l'adresse sales@cdlan.it.
Equinix, ML2, Milan, Italie	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Europe (Londres)

Emplacement	Comment demander une connexion
Digital Realty (Royaume-Uni), Docklands	Contactez Digital Realty (Royaume-Uni) à l'adresse amazon.orders@digitalrealty.com.
Equinix LD5, Londres (Slough)	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix MA3, Manchester	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Telehouse West, Londres	Contactez Telehouse UK à l'adresse sales.support@uk.telehouse.net.

Europe (Paris)

Emplacement	Comment demander une connexion
Equinix PA3, Paris	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Interxion PAR7, Paris	Contactez Interxion à l'adresse customer.services@interxion.com.
Telehouse Voltaire, Paris	Contactez Telehouse Paris Voltaire via la page Contactez-nous.

Europe (Stockholm)

Emplacement	Comment demander une connexion
Interxion STO1, Stockholm	Contactez Interxion à l'adresse customer.services@interxion.com.

Europe (Zurich)

Emplacement	Comment demander une connexion
Equinix ZRH51, Oberengstringen, Suisse	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Israël (Tel Aviv)

Emplacement	Comment demander une connexion
MedOne, Haïfa	Contactez-nous MedOne à l'adresse support@Medone.co.il
EdgeConnex, Herzliya	Contactez-nous EdgeConnect à l'adresse info@edgeconnecx.com

Moyen-Orient (Bahreïn)

Emplacement	Comment demander une connexion
AWS Bahreïn DC53, Manama	Pour finaliser la connexion, vous pouvez collaborer avec l'un de nos partenaires fournisseurs de réseau dans l'emplace ment afin d'établir la connectivité. Vous fournirez ensuite une lettre d'autorisation (LOA) du fournisseur de réseau AWS au AWS Support Center. AWS effectue la connexion croisée à cet emplacement.
AWS Bahreïn DC52, Manama	Pour finaliser la connexion, vous pouvez collaborer avec l'un de nos partenaires fournisseurs de réseau dans l'emplace ment afin d'établir la connectivité. Vous fournirez ensuite une lettre d'autorisation (LOA) du fournisseur de réseau AWS au AWS Support Center. AWS effectue la connexion croisée à cet emplacement.

Moyen-Orient (EAU)

Emplacement	Comment demander une connexion
Equinix DX1, Dubai, Émirats Arabes Unis	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Centre de SmartHub données Etisalat, Fujairah, Émirats arabes unis	Contactez le centre de SmartHub données Etisalat à l'adresse IntlSales-C& WS@etisalat.ae.

Amérique du Sud (São Paulo)

Emplacement	Comment demander une connexion
Equinix RJ2, Rio de Janeiro	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
Equinix SP4, São Paulo	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Tivit	Contactez Tivit à l'adresse aws@tivit.com.br.

AWS GovCloud (USA Est)

Vous ne pouvez pas commander de connexions dans cette région.

AWS GovCloud (US-Ouest)

Emplacement	Comment demander une connexion
Equinix SV5, San Jose	Contactez Equinix à l'adresse awsdealreg@equinix.com.

AWS Direct Connect interfaces virtuelles

Vous devez créer l'une des interfaces virtuelles (VIF) suivantes pour commencer à utiliser votre AWS Direct Connect connexion.

- Interface virtuelle privée : une interface virtuelle privée permet d'accéder à une instance Amazon VPC avec des adresses IP privées.
- Interface virtuelle publique : une interface virtuelle publique peut accéder à tous les services AWS publics à l'aide d'adresses IP publiques.
- Interface de transit virtuelle : une interface de transit virtuelle doit être utilisée pour accéder à une ou plusieurs passerelles de transit Amazon VPC associées à des passerelles Direct Connect. Vous pouvez utiliser les interfaces virtuelles de transport en commun avec n'importe quelle connexion AWS Direct Connect dédiée ou hébergée, quelle que soit la vitesse. Pour plus d'informations sur les configurations de passerelle Direct Connect, veuillez consulter the section called “Passerelles Direct Connect”.

Pour vous connecter à d'autres AWS services à l'aide d'adresses IPv6, consultez la documentation du service pour vérifier que l'adressage IPv6 est pris en charge.

Règles publicitaires de préfixe d'interface virtuelle publique

Nous vous communiquons les préfixes Amazon appropriés afin que vous puissiez accéder à vos VPC ou à d'autres AWS services. Vous pouvez accéder à tous les AWS préfixes via cette connexion, par exemple Amazon EC2, Amazon S3 et Amazon.com. Vous n'avez pas accès aux préfixes autres qu'Amazon. Pour obtenir la liste actuelle des préfixes annoncés par AWS, voir Plages d'adresses AWS IP dans le. Référence générale d'Amazon Web Services AWS ne publie pas à nouveau les préfixes clients reçus via les interfaces virtuelles publiques de Direct AWS Connect à d'autres clients. Pour plus d'informations sur les interfaces virtuelles publiques et les stratégies de routage, consultezthe section called “Stratégies de routage d'interface virtuelle publique”.

> **Note**
>
> Nous vous recommandons d'utiliser un filtre de pare-feu (basé sur l'adresse source/de destination des paquets) pour contrôler le trafic vers et depuis certains préfixes. Si vous utilisez un filtre de préfixe (commande route-map), assurez-vous qu'il accepte les préfixes

ayant une correspondance exacte ou plus longs. Les préfixes annoncés AWS Direct Connect peuvent être agrégés et peuvent différer des préfixes définis dans votre filtre de préfixes.

Interfaces virtuelles hébergées

Pour utiliser votre AWS Direct Connect connexion avec un autre compte, vous pouvez créer une interface virtuelle hébergée pour ce compte. Le propriétaire de l'autre compte doit accepter l'interface virtuelle hébergée pour commencer à l'utiliser. Une interface virtuelle hébergée fonctionne comme une interface virtuelle standard et peut se connecter à des ressources publiques ou à un VPC.

Vous pouvez utiliser des interfaces virtuelles de transport en commun avec des connexions dédiées ou hébergées Direct Connect, quelle que soit leur vitesse. Les connexions hébergées ne prennent en charge qu'une seule interface virtuelle.

Pour créer une interface virtuelle, les informations suivantes sont requises :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.

Ressource	Informations obligatoires
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.

Ressource	Informations obligatoires

Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.10` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)

Ressource	Informations obligatoires
	Note Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

SiteLink

Si vous créez une interface virtuelle privée ou de transit, vous pouvez utiliser SiteLink.

SiteLink est une fonctionnalité Direct Connect optionnelle pour les interfaces privées virtuelles qui permet la connectivité entre deux points de présence Direct Connect (PoPs) de la même AWS partition en utilisant le chemin le plus court disponible sur le AWS réseau. Cela vous permet de connecter votre réseau sur site via le réseau mondial AWS sans avoir à acheminer votre trafic via une région. Pour plus d'informations sur la SiteLink section Présentation AWS Direct Connect SiteLink.

> **Note**
>
> SiteLink n'est pas disponible dans AWS GovCloud (US) et dans les régions de Chine.

Il existe des frais de tarification distincts pour l'utilisation SiteLink. Pour plus d'informations, consultez Tarification AWS Direct Connect.

SiteLink ne prend pas en charge tous les types d'interfaces virtuelles. Le tableau suivant indique le type d'interface et s'il est pris en charge.

Type de l'interface virtuelle	Prise en charge/Non prise en charge
Interface virtuelle de transit	Pris en charge
Une interface privée virtuelle attachée à une passerell e Direct Connect avec une passerelle virtuelle	Pris en charge
Une interface privée virtuelle attachée à une passerelle Direct Connect non associée à une passerelle virtuelle ou à une passerelle de transit	Pris en charge
Une interface privée virtuelle attachée à une passerelle virtuelle	Non pris en charge
Interface virtuelle publique	Non pris en charge

Le comportement de routage du trafic en provenance Régions AWS (passerelles virtuelles ou de transit) vers des sites locaux via une interface virtuelle SiteLink activée varie légèrement par rapport au comportement par défaut de l'interface virtuelle Direct Connect avec un AWS chemin prédéfini. Lorsque cette option SiteLink est activée, les interfaces virtuelles d'un emplacement Direct Connect Région AWS préfèrent un chemin BGP avec une longueur de chemin AS inférieure, quelle que soit la région associée. Par exemple, une région associée est annoncée pour chaque emplacement Direct Connect. Si cette option SiteLink est désactivée, le trafic provenant d'une passerelle virtuelle ou de transit préfère par défaut un emplacement Direct Connect qui lui est associé Région AWS, même si le routeur des emplacements Direct Connect associés à différentes régions annonce un chemin avec une longueur de chemin AS plus courte. La passerelle virtuelle ou de transit préfère toujours le chemin depuis les emplacements Direct Connect locaux vers le chemin associé Région AWS.

SiteLink prend en charge une taille MTU maximale de trame jumbo de 8500 ou 9001, selon le type d'interface virtuelle. Pour plus d'informations, consultez the section called "Définir la MTU du réseau pour les interfaces virtuelles privées ou les interfaces de transit virtuelles".

Conditions préalables pour les interfaces virtuelles

Avant de créer une interface virtuelle, procédez comme suit :

- Créez une connexion. Pour plus d'informations, consultez the section called "Créer une connexion à l'aide de l'assistant de connexion".
- Créez un groupe d'agrégation de liaisons (LAG) lorsque vous avez plusieurs connexions que vous souhaitez traiter comme une seule. Pour plus d'informations, veuillez consulter Associer une connexion à un LAG.

Pour créer une interface virtuelle, les informations suivantes sont requises :

Ressource	Informations obligatoires
Connection	La AWS Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interface virtuelle	Un nom pour l'interface virtuelle.

Ressource	Informations obligatoires
Propriétaire de l'interface virtuelle	Si vous créez l'interface virtuelle pour un autre compte, vous avez besoin de l'identifiant de AWS compte de cet autre compte.
(Interface virtuelle privée uniquement) Connexion	Pour vous connecter à un VPC dans la même AWS région, vous avez besoin de la passerelle privée virtuelle de votre VPC. L'ASN correspondant au côté Amazon de la session BGP est hérité de la passerelle privée virtuelle . Lorsque vous créez une passerelle privée virtuelle, vous pouvez spécifier votre propre ASN privé. Sinon, Amazon fournit un ASN par défaut. Pour plus d'informations, consultez Création d'une passerelle privée virtuelle dans le Guide de l'utilisateur Amazon VPC. Pour vous connecter à un VPC par le biais d'une passerelle Direct Connect, vous avez besoin de cette dernière. Pour plus d'informations, consultez Passerelles Direct Connect.
VLAN	Une balise de réseau local virtuel (VLAN) unique qui n'est pas déjà utilisée sur votre connexion. La valeur doit être comprise entre 1 et 4094 et doit être conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion AWS Direct Connect . Si vous disposez d'une connexion hébergée, votre AWS Direct Connect partenaire fournit cette valeur. Vous ne pouvez pas modifier la valeur après avoir créé l'interface virtuelle.

Ressource	Informations obligatoires

Adresses IP d'appairage	Une interface virtuelle peut prendre en charge une session d'appairage BGP pour IPv4, IPv6 ou une de chaque (double pile). N'utilisez pas les adresses IP élastiques (EIP) ou Bring your own IP addresses (BYOIP) depuis le pool Amazon pour créer une interface virtuelle publique. Vous ne pouvez pas créer plusieurs sessions BGP pour la même famille d'adressage IP sur la même interface virtuelle. Les plages d'adresses IP sont attribuées à chaque fin de l'interface virtuelle pour la session d'appairage BGP.
	
	• Caractéristiques et restrictions IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les adresses IPv4 publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR IPv4 appartenant au client
	
	Il peut s'agir de n'importe quelle adresse IP publique (appartenant au client ou fournie par AWS), mais le même masque de sous-rése au doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/31` plage, telle que`203.0.113.0/31` , vous pouvez l'utiliser `203.0.113.0` pour votre adresse IP homologue et `203.0.113.1` pour l'adresse IP AWS homologue. Ou, si vous allouez une `/24` plage, par exemple`198.51.100.0/24` , vous pouvez l'utiliser `198.51.100.0` pour votre adresse IP homologue et `198.51.100.20` pour l'adresse IP AWS homologue.
	  • Une plage d'adresses IP appartenant à votre AWS Direct Connect partenaire ou fournisseur de services Internet, ainsi qu'une autorisation LOA-CFA
	  • Un AWS CIDR /31 fourni. Contactez Support AWS pour demander un bloc CIDR IPv4 public (et fournissez un cas d'utilisation dans votre requête)

Ressource	Informations obligatoires
	> **Note** > Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' AWS adresses IPv4 publiques fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des adresses IPv4 privées pour vous. Si vous spécifiez le vôtre, assurez-v ous de spécifier des CIDR privés pour l'interface de votre routeur et pour l'interface AWS Direct Connect uniquement. Par exemple, ne spécifiez pas d'autres adresses IP provenant de votre réseau local. Comme pour une interface virtuelle publique, le même masque de sous-réseau doit être utilisé à la fois pour votre adresse IP homologue et pour l'adresse IP homologue du AWS routeur. Par exemple, si vous allouez une `/30` plage, telle que`192.168.0.0/30` , vous pouvez l'utiliser `192.168.0.1` pour votre adresse IP homologue et `192.168.0.2` pour l'adresse IP AWS homologue. • IPv6 : Amazon vous alloue automatiquement un bloc CIDR IPv6 /125. Vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6.
Famille d'adresses	Si la session d'appairage BGP se déroulera sur IPv4 ou IPv6.
Informations BGP	• Un Protocole de passerelle frontière (BGP) Numéro de système autonome (ASN) public ou privé pour votre côté de la session BGP. Si vous utilisez un ASN public, vous devez en être propriétaire. Si vous utilisez un ASN privé, vous pouvez définir une valeur ASN personnalisée. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 1 et 2147483647. L'ajout d'un préfixe AS (Autonomous System) ne fonctionne pas si vous utilisez un ASN privé pour une interface virtuelle publique. • AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option. • Une clé d'authentification MD5 BGP. Vous pouvez fournir la vôtre ou laisser Amazon en générer une pour vous.

Ressource	Informations obligatoires

(Interface virtuelle publique uniquement) Préfixes que vous voulez publier	Routes IPv4 publiques ou routes IPv6 à publier via le protocole BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4 : Le CIDR IPv4 peut se chevaucher avec un autre CIDR IPv4 public annoncé AWS Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Les CIDR proviennent de différentes AWS régions. Assurez-vous d'appliquer les balises communautaires BGP sur les préfixes publics.
	  • Vous utilisez AS_PATH lorsque vous avez un ASN public dans une configuration active/passive.
	  Pour plus d'informations, consultez les Stratégies de routage et communautés BGP.
	• IPv6 : Indiquez un préfixe de longueur /64 ou inférieure.
	• Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.
	• Vous pouvez spécifier n'importe quelle longueur de préfixe sur une interface virtuelle publique Direct Connect. IPv4 doit prendre en charge tout ce qui est compris entre /1 et /32, et IPv6 doit prendre en charge tout ce qui est compris entre /1 et /64.

Ressource	Informations obligatoires
(Interface virtuelle privée uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 9001 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les cadres Jumbo s'appliqu ent uniquement aux itinéraires propagés à partir de. AWS Direct Connect Si vous ajoutez des routes statiques à une table de routage qui pointe vers votre passerelle privée virtuelle, le trafic acheminé via les routes statiques est envoyé via une MTU de 1500. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.
(Interfac e virtuelle de transit uniquement) Trames Jumbo	Unité de transmission maximale (MTU) de paquets dépassés AWS Direct Connect. La valeur par défaut est 1500. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Les trames Jumbo sont prises en charge jusqu'à 8500 MTU pour Direct Connect. Les routes statiques et les routes propagées configurées dans la table de routage de passerelle de transit prendront en charge les trames Jumbo, y compris depuis les instances EC2 avec des entrées de table de routage statique VPC jusqu'à l'attachement de la passerelle de transit. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Lorsque vous créez une interface virtuelle, vous pouvez spécifier le compte propriétaire de l'interface virtuelle. Lorsque vous choisissez un AWS compte qui n'est pas le vôtre, les règles suivantes s'appliquent :

- Pour les VIF privés et les VIF de transit, le compte s'applique à l'interface virtuelle et à la destination de la passerelle privée virtuelle/Direct Connect.
- Pour les VIF publics, le compte est utilisé pour la facturation de l'interface virtuelle. L'utilisation du transfert de données sortant (DTO) est mesurée en fonction du propriétaire de la ressource au taux de transfert de AWS Direct Connect données.

> **Note**
>
> Les préfixes 31 bits sont pris en charge sur tous les types d'interfaces virtuelles Direct Connect. Consultez RFC 3021 : Utilisation de préfixes 31 bits sur les liaisons point à point IPv4 pour plus d'informations.

Créer une interface virtuelle

Vous pouvez créer une interface virtuelle pour vous connecter à une passerelle de transit, une interface virtuelle publique pour vous connecter à des ressources publiques (services non VPC) ou une interface virtuelle privée pour vous connecter à un VPC.

Pour créer une interface virtuelle pour les comptes qui vous AWS Organizations appartiennent ou AWS Organizations qui sont différents du vôtre, créez une interface virtuelle hébergée. Pour plus d'informations, consultez the section called "Créer une interface virtuelle hébergée".

Prérequis

Avant de commencer, veillez à lire les informations suivantes Conditions préalables pour les interfaces virtuelles.

Créer une interface virtuelle publique

Lorsque vous créez une interface virtuelle publique, la verification et l'approbation de votre demande peuvent prendre jusqu'à 72 heures.

Pour mettre en service une interface virtuelle publique

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.

3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   d. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Paramètres supplémentaires, procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

   b. Pour fournir votre propre clé BGP, saisissez votre clé MD5 BGP.

      Si vous ne saisissez aucune valeur, nous générons une clé BGP. Si vous avez fourni votre propre clé, ou si nous l'avons générée pour vous, cette valeur s'affiche dans la colonne Clé d'authentification BGP sur la page de détails de l'interface virtuelle d'Interfaces virtuelles.

   c. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.

> **Important**
>
> Vous pouvez ajouter des préfixes supplémentaires à un VIF public existant et les publier en contactant le support AWS. Dans votre dossier d'assistance, fournissez une liste des préfixes CIDR supplémentaires que vous souhaitez ajouter au VIF public et publier.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.
8. Téléchargez la configuration de routeur pour votre périphérique. Pour plus d'informations, consultez Télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle publique à l'aide de la ligne de commande ou de l'API

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface(AWS Direct Connect API)

Créer une interface virtuelle privée

Vous pouvez fournir une interface virtuelle privée à une passerelle privée virtuelle dans la même région que votre AWS Direct Connect connexion. Pour plus d'informations sur le provisionnement d'une interface virtuelle privée sur une AWS Direct Connect passerelle, consultezUtilisation des passerelles Direct Connect.

Si vous utilisez l'assistant VPC pour créer un VPC, la propagation du routage est automatiquement activée pour vous. Avec la propagation du routage, les routes sont remplies automatiquement pour les tables de routage de votre VPC. Vous pouvez activer ou désactiver la propagation du routage. Pour plus d'informations, consultez Autorisation de la propagation du routage dans votre table de routage dans le Guide de l'utilisateur Amazon VPC.

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. La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 9001 (trames jumbo). La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 8500 (trames jumbo). Vous pouvez spécifier la MTU lorsque vous créez l'interface ou la mettre à jour après l'avoir créée. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la console AWS Direct Connect et recherchez Jumbo Frame Capable (Capacité de trame Jumbo) sous l'onglet Summary.

Pour mettre en service une interface virtuelle privée sur un VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, choisissez Privée.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :
   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.
   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.
   c. Pour Propriétaire de l'interface virtuelle, choisissez Mon AWS compte si l'interface virtuelle est destinée à votre AWS compte.
   d. Pour Passerelle Direct Connect, sélectionnez la passerelle Direct Connect.
   e. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).
   f. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1 à 2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :
   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

[IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

- Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
- Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

> **Important**
>
> Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage (autre que la RFC 1918) et spécifier l'adresse vous-même.
>
> - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
> - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.
8. Téléchargez la configuration de routeur pour votre périphérique. Pour plus d'informations, consultez Télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle privée à l'aide de la ligne de commande ou de l'API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Créer une interface de transit virtuelle vers la passerelle Direct Connect

Pour connecter votre AWS Direct Connect connexion à la passerelle de transit, vous devez créer une interface de transit pour votre connexion. Spécifiez la passerelle Direct Connect à laquelle vous souhaitez vous connecter.

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. La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 9001 (trames jumbo). La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 8500 (trames jumbo). Vous pouvez spécifier la MTU lorsque vous créez l'interface ou la mettre à jour après l'avoir créée. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Pour vérifier si une connexion ou une interface virtuelle prend en charge les trames jumbo, sélectionnez-la dans la console AWS Direct Connect et recherchez Jumbo Frame Capable (Capacité de trame Jumbo) sous l'onglet Summary.

> **Important**
>
> Si vous associez votre passerelle de transit à une ou plusieurs passerelles Direct Connect, le numéro de système autonome (ASN) utilisé par la passerelle de transit et la passerelle Direct Connect doivent être différents. Par exemple, si vous utilisez l'ASN 64512 par défaut pour la passerelle de transit et la passerelle Direct Connect, la demande d'association échoue.

Pour mettre en service une interface de transit virtuelle vers une passerelle Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Private (Privée).
5. Sous Transit virtual interface settings (Paramètres de l'interface virtuelle de transit), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour Propriétaire de l'interface virtuelle, choisissez Mon AWS compte si l'interface virtuelle est destinée à votre AWS compte.

   d. Pour Passerelle Direct Connect, sélectionnez la passerelle Direct Connect.

   e. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   f. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1 à 2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

      > **Important**
      >
      > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927

pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage (autre que la RFC 1918) et spécifier l'adresse vous-même.

- Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
- Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 8500 (trames jumbo), sélectionnez Jumbo MTU (MTU size 8500) [MTU Jumbo (taille MTU 8500)].

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Une fois l'interface virtuelle créée, vous pouvez télécharger la configuration du routeur pour votre appareil. Pour plus d'informations, consultez Télécharger le fichier de configuration du routeur.

Pour créer une interface de transit virtuelle à l'aide de la ligne de commande ou de l'API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Pour afficher la liste des interfaces virtuelles attachées à une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayPièces jointes (AWS Direct Connect API)

Télécharger le fichier de configuration du routeur

Une fois que vous avez créé l'interface virtuelle et que celle-ci est à l'état actif, vous pouvez télécharger le fichier de configuration de routeur pour votre routeur.

Si vous utilisez l'un des routeurs suivants pour les interfaces virtuelles sur lesquelles MACsec est activé, nous créons automatiquement le fichier de configuration de votre routeur :

- Commutateurs Cisco Nexus série 9K+ exécutant le logiciel NX-OS 9.3 ou version ultérieure
- Routeurs Juniper Networks série M/MX exécutant le logiciel JunOS 9.5 ou une version plus récente

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).
4. Choisissez Télécharger la configuration de routeur.
5. Pour Télécharger la configuration de routeur, procédez comme suit :
    a. Pour Fournisseur, sélectionnez le fabricant de votre routeur.
    b. Pour Plateforme, sélectionnez le modèle de votre routeur.
    c. Pour Logiciels, sélectionnez la version du logiciel de votre routeur.
6. Choisissez Télécharger, puis utilisez la configuration appropriée pour votre routeur afin de vous assurer de pouvoir vous connecter à AWS Direct Connect:

Considérations sur la MACsec

Si vous devez configurer manuellement votre routeur pour MACsec, utilisez le tableau suivant à titre indicatif.

Paramètre	Description
Longueur de CKN	Il s'agit d'une chaîne de 64 caractères hexadécimaux (0—9, A—E). Utilisez toute la longueur pour optimiser la compatibilité multiplateforme.
Longueur de CAK	Il s'agit d'une chaîne de 64 caractères hexadécimaux (0—9, A—E). Utilisez toute la longueur pour optimiser la compatibilité multiplateforme.
Algorithme de chiffrement	AES_256_CMAC
Suite de chiffrement SAK	• Pour les connexions 100 Gb/s : GCM_AES_XPN_256 • Pour les connexions 10 Gb/s : GCM_AES_XPN_256 ou GCM_AES _256
Suite de chiffrement à clé	16
Compensation de confidentialité	0
Indicateur ICV	Non
Heure du changement de clé SAK	Substitution de PN>

Afficher les détails de l'interface virtuelle

Vous pouvez afficher l'état actuel de votre interface virtuelle. Les détails sont les suivants :

- État de connexion
- Nom
- Emplacement
- VLAN

- Détails du BGP
- Adresses IP d'appairage

Pour afficher les informations relatives à une interface virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).

Pour décrire des interfaces virtuelles à l'aide de la ligne de commande ou de l'API

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces (AWS Direct Connect API)

Ajouter ou supprimer un homologue BGP

Ajouter ou supprimer une session d'appairage BGP IPv4 ou IPv6 à votre interface virtuelle.

Une interface virtuelle ne peut prendre en charge qu'une session d'appairage BGP IPv4 et une session d'appairage BGP IPv6.

Dans le cas d'une session d'appairage BGP IPv6, vous ne pouvez pas spécifier vos propres adresses d'appairage IPv6. Amazon vous alloue automatiquement un bloc CIDR IPv6 /125.

BGP multi-protocole n'est pas pris en charge. IPv4 et IPv6 fonctionnent en mode double pile pour l'interface virtuelle.

AWS active MD5 par défaut. Vous ne pouvez pas modifier cette option.

Ajouter un appairage BGP

Utilisez la procédure suivante pour ajouter un appairage BGP.

Pour ajouter un appairage BGP

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.

2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).
4. Choisissez Ajouter un appairage.
5. (Interface virtuelle privée) Pour ajouter des appairages BGP IPv4, procédez comme suit :
   - Choisissez IPv4.
   - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic. Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.
6. (Interface virtuelle publique) Pour ajouter des appairages BGP IPv4, procédez comme suit :
   - Pour IP du pair de votre routeur, entrez l'adresse de destination CIDR IPv4 où le trafic doit être envoyé.
   - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

   > **Important**
   >
   > Si vous autorisez l' AWS attribution automatique des adresses IP, un CIDR /29 sera attribué à partir de 169.254.0.0/16. AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et destination du trafic. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même. Pour plus d'informations sur la RFC 1918, consultez Allocation d'adresses pour les réseaux Internet privés.
7. (Interface virtuelle privée ou publique) Pour ajouter des pairs BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement assignées à partir du pool d'adresses IPv6 d'Amazon ; vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.
8. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

   Pour une interface virtuelle publique, l'ASN doit être privé ou déjà enregistré sur la liste verte de l'interface virtuelle.

   Les valeurs valides sont 1-2147483647.

   Notez que si vous n'entrez pas de valeur, nous en attribuons une automatiquement.

9. Pour fournir votre propre clé BGP, pour Clé d'authentification BGP, saisissez votre clé MD5 BGP.
10. Choisissez Ajouter un appairage.

Pour créer un appairage BGP à l'aide de la ligne de commande ou de l'API

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (API AWS Direct Connect)

Supprimer un appairage BGP

Si votre interface virtuelle comporte à la fois une session d'appairage BGP IPv4 et une IPv6, vous pouvez supprimer une des sessions d'appairage BGP (mais pas les deux).

Pour supprimer un appairage BGP

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).
4. Sous Peerings (Appairages), sélectionnez l'appairage que vous souhaitez supprimer, puis choisissez Supprimer.
5. Dans la boîte de dialogue Remove peering from virtual interface (Supprimer un appairage de l'interface virtuelle), sélectionnez Supprimer.

Pour supprimer un appairage BGP à l'aide de la ligne de commande ou de l'API

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (API)AWS Direct Connect

Définir la MTU du réseau pour les interfaces virtuelles privées ou les interfaces de transit virtuelles

AWS Direct Connect prend en charge une taille de trame Ethernet de 1522 ou 9023 octets (14 octets d'en-tête Ethernet + 4 octets de balise VLAN + octets pour le datagramme IP + 4 octets FCS) au niveau de la couche de liaison.

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. La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 9001 (trames jumbo). La MTU d'une interface privée virtuelle peut être soit de 1500, soit de 8500 (trames jumbo). Vous pouvez spécifier la MTU lorsque vous créez l'interface ou la mettre à jour après l'avoir créée. Définir la MTU d'une interface virtuelle sur 8500 (trames jumbo) peut entraîner une mise à jour de la connexion physique sous-jacente si elle n'a pas été mise à jour pour prendre en charge les trames jumbo. La mise à jour de la connexion interrompt la connectivité réseau pour toutes les interfaces virtuelles associées à la connexion pendant un maximum de 30 secondes. Pour vérifier si une connexion ou une interface virtuelle prend en charge les images jumbo, sélectionnez-la dans la AWS Direct Connect console et recherchez Jumbo Frame Capable dans l'onglet Résumé.

Une fois que vous avez activé les trames jumbo pour votre interface virtuelle privée ou votre interface virtuelle de transit, vous pouvez uniquement l'associer à une connexion ou à un LAG doté d'une capacité de trame Jumbo. Les trames jumbo sont prises en charge sur une interface virtuelle privée attachée à une passerelle virtuelle privée ou à une passerelle Direct Connect, ou sur une interface virtuelle de transit attachée à une passerelle Direct Connect. Si vous avez deux interfaces virtuelles privées qui annoncent la même route mais utilisent des valeurs MTU différentes ou si vous disposez d'un VPN site à site qui annonce la même route, la MTU 1500 est utilisée.

Important

Les cadres Jumbo s'appliqueront uniquement aux itinéraires propagés AWS Direct Connect et aux itinéraires statiques via des passerelles de transit. Les trames jumbo sur les passerelles de transit ne prennent en charge que 8500 octets.
Si une instance EC2 ne prend pas en charge les trames jumbo, elle supprime les trames jumbo de Direct Connect. Tous les types d'instances EC2 prennent en charge les trames jumbo, à l'exception de C1, CC1, T1 et M1. Pour plus d'informations, consultez la section Unité de transmission maximale (MTU) du réseau pour votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

Pour les connexions hébergées, les trames Jumbo peuvent être activées uniquement si elles sont initialement activées sur la connexion parent hébergée Direct Connect. Si les trames Jumbo ne sont pas activées sur cette connexion parent, elles ne peuvent être activées sur aucune connexion.

Pour définir la MTU d'une interface virtuelle privée

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez Modifier.
4. Sous Jumbo (taille MTU 9001 MTU) ou jumbo (MTU de taille MTU 8500), sélectionnez Enabled.
5. Sous Accepter, sélectionnez Je comprends que la ou les connexion(s) sélectionnée(s) sera(ont) interrompue(s) pendant une brève période. L'état de l'interface virtuelle est `pending` jusqu'à ce que la mise à jour soit terminée.

Pour définir la MTU d'une interface virtuelle privée à l'aide de la ligne de commande ou de l'API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct Connect API)

Ajouter ou supprimer des balises de l'interface virtuelle

Les balises permettent d'identifier l'interface virtuelle. Vous pouvez ajouter ou supprimer une balise si vous êtes le propriétaire du compte pour l'interface virtuelle.

Pour ajouter ou supprimer une balise de l'interface virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez Modifier.
4. Ajoutez ou supprimez une balise.

   [Add a tag] Choisissez Add tag (Ajouter une balise) et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

5. Choisissez Edit virtual interface (Modifier l'interface virtuelle).

Pour ajouter et supprimer une balise à l'aide de la ligne de commande

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Supprimer les interfaces virtuelles

Supprimez un ou plusieurs interfaces virtuelles. Avant de pouvoir supprimer une connexion, vous devez supprimer son interface virtuelle. La suppression d'une interface virtuelle arrête AWS Direct Connect les frais de transfert de données associés à l'interface virtuelle.

Pour supprimer une interface virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, sélectionnez Interfaces virtuelles.
3. Sélectionnez les interfaces virtuelles, puis choisissez Supprimer.
4. Dans la boîte de dialogue de confirmation Supprimer, sélectionnez Supprimer.

Pour supprimer une interface virtuelle à l'aide de la ligne de commande ou de l'API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface (AWS Direct Connect API)

Créer une interface virtuelle hébergée

Vous pouvez créer une interface virtuelle hébergée publique, de transit ou privée. Avant de commencer, veillez à lire les informations suivantes Conditions préalables pour les interfaces virtuelles.

Créer une interface virtuelle privée hébergée

Pour créer une interface virtuelle privée hébergée

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, pour Type, choisissez Privé.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour le Propriétaire de l'interface virtuelle, choisissez Un autre compte AWS , puis pour le Propriétaire de l'interface virtuelle, entrez l'ID du compte auquel appartient cette interface virtuelle.

   d. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   e. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

> **Important**
>
> Si vous autorisez l' AWS attribution automatique des adresses IP, un CIDR /29 sera attribué à partir de 169.254.0.0/16. AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et destination du trafic. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage (autre que la RFC 1918) et spécifier l'adresse vous-même. Pour plus d'informations sur la RFC 1918, consultez Allocation d'adresses pour les réseaux Internet privés.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Une fois que l'interface virtuelle hébergée est acceptée par le propriétaire de l'autre compte AWS , vous pouvez télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle privée hébergée à l'aide de la ligne de commande ou de l'API

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(AWS Direct Connect API)

Créer une interface virtuelle publique hébergée

Pour créer une interface virtuelle publique hébergée

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.

2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Public (Publique).
5. Sous Public virtual interface settings (Paramètres de l'interface virtuelle publique), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis pour Propriétaire de l'interface virtuelle, entrez l'ID du compte auquel appartient cette interface virtuelle.

   d. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   e. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1-2147483647.
6. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

   [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

   - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
   - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

   > **Important**
   >
   > Si vous autorisez l' AWS attribution automatique des adresses IP, un CIDR /29 sera attribué à partir de 169.254.0.0/16. AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et destination du trafic. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même. Pour plus d'informations sur la RFC 1918, consultez Allocation d'adresses pour les réseaux Internet privés.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

7. Pour publier des préfixes vers Amazon, pour Préfixes que vous voulez publier, saisissez les adresses de destination CIDR IPv4 (séparées par des virgules) vers lesquelles le trafic doit être acheminé via l'interface virtuelle.
8. Pour fournir votre propre clé pour authentifier la session BGP, sous Additional Settings (Paramètres supplémentaires), saisissez la clé sous BGP authentication key (Clé d'authentification BGP).

   Si vous ne saisissez aucune valeur, nous générons une clé BGP.
9. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.
10. Choisissez Créer une interface virtuelle.
11. Une fois que l'interface virtuelle hébergée est acceptée par le propriétaire de l'autre compte AWS , vous pouvez télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle publique hébergée à l'aide de la ligne de commande ou de l'API

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct Connect API)

Créer une interface de transit virtuelle hébergée

Pour créer une interface de transit virtuelle hébergée

> **Important**
>
> Si vous associez votre passerelle de transit à une ou plusieurs passerelles Direct Connect, le numéro de système autonome (ASN) utilisé par la passerelle de transit et la passerelle Direct

Connect doivent être différents. Par exemple, si vous utilisez l'ASN 64512 par défaut pour la passerelle de transit et la passerelle Direct Connect, la demande d'association échoue.

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Private (Privée).
5. Sous Transit virtual interface settings (Paramètres de l'interface virtuelle de transit), procédez comme suit :

   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.

   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.

   c. Pour Propriétaire de l'interface virtuelle, choisissez Un autre AWS compte, puis pour Propriétaire de l'interface virtuelle, entrez l'ID du compte auquel appartient cette interface virtuelle.

   d. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).

   e. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1-2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
      - Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

> **Important**
>
> Si vous autorisez l' AWS attribution automatique des adresses IP, un CIDR /29 sera attribué à partir de 169.254.0.0/16. AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et destination du trafic. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage, et spécifier l'adresse vous-même. Pour plus d'informations sur la RFC 1918, consultez Allocation d'adresses pour les réseaux Internet privés.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 8500 (trames jumbo), sélectionnez Jumbo MTU (MTU size 8500) [MTU Jumbo (taille MTU 8500)].

c. [Facultatif] Ajoutez une balise. Procédez comme suit :

[Add a tag] Choisissez Add tag (Ajouter une balise) et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.
8. Une fois que l'interface virtuelle hébergée est acceptée par le propriétaire de l'autre compte AWS , vous pouvez télécharger le fichier de configuration du routeur.

Pour créer une interface de transit virtuelle hébergée à l'aide de la ligne de commande ou de l'API

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct Connect API)

Accepter une interface virtuelle hébergée

Avant de pouvoir commencer à utiliser une interface virtuelle hébergée, vous devez accepter l'interface virtuelle. Pour une interface privée virtuelle, vous devez également disposer d'une

passerelle privée virtuelle ou d'une passerelle Direct Connect. Pour une interface virtuelle, vous devez disposer d'une passerelle de transit existante ou d'une passerelle Direct Connect.

Pour accepter une interface virtuelle hébergée

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle et choisissez View details (Afficher les détails).
4. Choisissez Accepter.
5. Cela s'applique aux interfaces virtuelles privées et aux interfaces virtuelles de transit.

   (Interface virtuelle de transit) Dans la boîte de dialogue Accept virtual interface (Accepter l'interface virtuelle), sélectionnez une passerelle Direct Connect, puis choisissez Accept virtual interface (Accepter l'interface virtuelle).

   (Interface virtuelle privée) Dans la boîte de dialogue Accept virtual interface (Accepter l'interface virtuelle), sélectionnez une passerelle privée virtuelle ou une passerelle Direct Connect, puis choisissez Accept virtual interface (Accepter l'interface virtuelle).
6. Après avoir accepté l'interface virtuelle hébergée, le propriétaire de la connexion AWS Direct Connect peut télécharger le fichier de configuration du routeur. L'option Télécharger la configuration de routeur n'est pas disponible pour le compte qui accepte l'interface virtuelle hébergée.

Pour accepter une interface virtuelle privée hébergée à l'aide de la ligne de commande ou de l'API

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct Connect API)

Pour accepter une interface virtuelle publique hébergée à l'aide de la ligne de commande ou de l'API

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct Connect API)

Pour accepter une interface de transit virtuelle hébergée à l'aide de la ligne de commande ou de l'API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct Connect API)

Migrer une interface virtuelle

Utilisez cette procédure lorsque vous souhaitez effectuer l'une des opérations de migration d'interface virtuelle suivantes :

- Migrer une interface virtuelle existante associée à une connexion vers un autre LAG.
- Migrer une interface virtuelle existante associée à un LAG existant vers un nouveau LAG.
- Migrer une interface virtuelle existante associée à une connexion vers une autre connexion.

Note

- Vous pouvez migrer une interface virtuelle vers une nouvelle connexion au sein de la même région, mais vous ne pouvez pas la migrer d'une région à l'autre. Lorsque vous migrez ou associez une interface virtuelle existante à une nouvelle connexion, les paramètres de configuration associés aux interfaces virtuelles sont les mêmes. Pour résoudre ce problème, vous pouvez préparer la configuration sur la connexion, puis mettre à jour la configuration BGP.
- Vous ne pouvez pas migrer une VIF d'une connexion hébergée vers une autre connexion hébergée. Les identifiants de VLAN sont uniques ; par conséquent, migrer une VIF de cette manière signifierait que les VLAN ne correspondent pas. Vous devez supprimer la connexion ou la VIF, puis la recréer à l'aide d'un VLAN identique pour la connexion et la VIF.

Important

L'interface virtuelle s'arrête pendant une courte période. Nous vous recommandons d'effectuer cette procédure pendant une fenêtre de maintenance.

Pour migrer une interface virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Sélectionnez l'interface virtuelle, puis choisissez Edit (Modifier).
4. Pour Connection (Connexion), sélectionnez le LAG ou la connexion.
5. Choisissez Edit virtual interface (Modifier l'interface virtuelle).

Pour migrer une interface virtuelle à l'aide de la ligne de commande ou de l'API

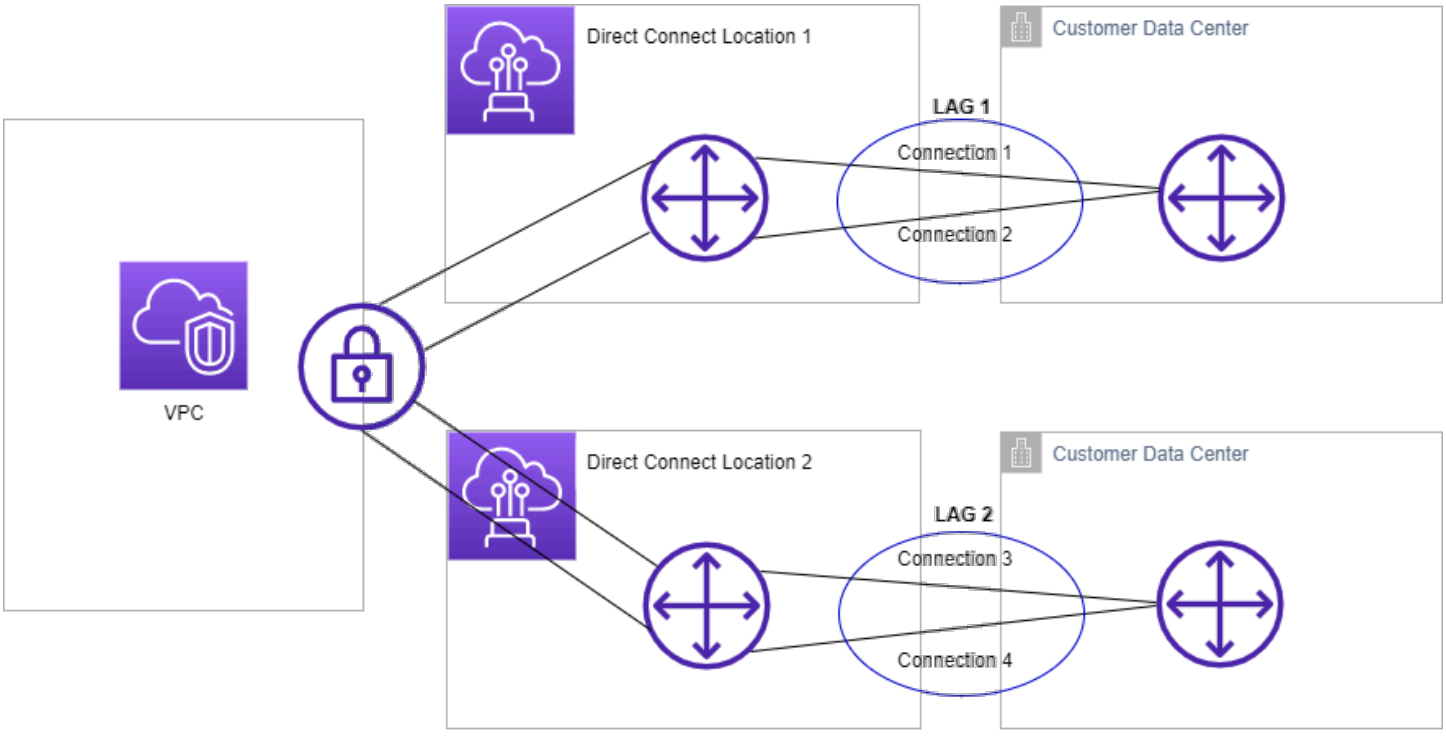
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (AWS Direct Connect API)

Groupes d'agrégation de liaisons (LAG)

Vous pouvez utiliser plusieurs connexions pour augmenter la bande passante disponible. Un groupe d'agrégation de liaisons (LAG) est une interface logique qui utilise le Link Aggregation Control Protocol (LACP) pour regrouper plusieurs connexions à un point de terminaison AWS Direct Connect unique, ce qui vous permet de les traiter comme une connexion gérée unique. Les LAG simplifient la configuration car la configuration LAG s'applique à toutes les connexions du groupe.

> **Note**
>
> Le LAG multi-châssis (MLAG) n'est pas pris en charge par AWS.

Dans le schéma suivant, vous avez quatre connexions, avec deux connexions à chaque emplacement. Vous pouvez créer un LAG pour les connexions qui se terminent sur le même AWS appareil et au même endroit, puis utiliser les deux LAG au lieu des quatre connexions pour la configuration et la gestion.



Vous pouvez créer un LAG à partir des connexions existantes, ou vous pouvez mettre en service de nouvelles connexions. Après avoir créé le LAG, vous pouvez lui associer des connexions existantes (qu'elles soient autonomes ou fassent partie d'un autre LAG).

Les règles suivantes s'appliquent :

- Toutes les connexions doivent être des connexions dédiées et avoir une vitesse de port de 1 Gb/s, 10 Gb/s ou 100 Gb/s.
- Toutes les connexions du LAG doivent utiliser la même bande passante.
- Vous pouvez avoir un maximum de deux connexions 100G ou quatre connexions avec une vitesse de port inférieure à 100G dans un LAG. Chaque connexion du LAG est comptabilisée dans la limite de connexion globale pour la région.
- Toutes les connexions du LAG doivent être résiliées au même point de terminaison AWS Direct Connect.
- Les LAG sont pris en charge pour tous les types d'interfaces virtuelles (publiques, privées et de transit).

Lorsque vous créez un LAG, vous pouvez télécharger la Lettre d'autorisation - Affectation d'installation de connexion (LOA-CFA) pour chaque nouvelle connexion physique individuellement à partir de la console AWS Direct Connect. Pour plus d'informations, consultez Télécharger la LOA-CFA.

Tous les LAG possèdent un attribut qui détermine le nombre minimum de connexions opérationnelles dans le LAG pour que ce dernier soit opérationnel. Par défaut, l'attribut des nouveaux LAG est défini sur 0. Vous pouvez mettre à jour votre LAG pour spécifier une valeur différentece (qui signifie que votre LAG entier n'est plus opérationnel si le nombre de connexions opérationnelles est inférieur à ce seuil). Cet attribut peut être utilisé pour prévenir l'utilisation excessive des connexions restantes.

Toutes les connexions d'un LAG fonctionnent en mode Actif/Actif.

> **Note**
>
> Lorsque vous créez un LAG ou associez plus de connexions au LAG, vous n'êtes pas en mesure de garantir suffisamment de ports disponibles sur un point de terminaison AWS Direct Connect donné.

Considérations sur la MACsec

Prenez en considération les points suivants lorsque vous souhaitez configurer MACsec sur des LAG :

- Lorsque vous créez un LAG à partir de connexions existantes, nous dissocions toutes les clés MACsec des connexions. Ensuite, nous ajoutons les connexions au LAG et associons la clé LAG MACsec aux connexions.
- Lorsque vous associez une connexion existante à un LAG, les clés MACsec actuellement associées au LAG sont associées à la connexion. Par conséquent, nous dissocions les clés MACsec de la connexion, ajoutons la connexion au LAG, puis associons la clé LAG MACsec à la connexion.

Créer un LAG

Vous pouvez créer un LAG en mettant en service de nouvelles connexions ou en regroupant des connexions existantes.

Vous ne pouvez pas créer de LAG avec de nouvelles connexions si cela vous fait dépasser la limite de connexion globale pour la région.

Pour créer un LAG à partir de connexions existantes, ces dernières doivent être sur le même appareil AWS (être résiliées au même point de terminaison AWS Direct Connect). Elles doivent également utiliser la même bande passante. Vous ne pouvez pas migrer une connexion à partir d'un LAG existant si la suppression de la connexion fait passer le nombre minimum de connexions opérationnelles du LAG en dessous de la valeur configurée.

> **Important**
>
> Pour les connexions existantes, la connectivité à AWS est interrompue pendant la création du LAG.

Create a LAG with new connections using the console

Pour créer un LAG avec de nouvelles connexions

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez Créer LAG.
4. Sous Lag creation type (Type de création de LAG), choisissez Demander de nouvelles connexions et fournissez les informations suivantes :

- Nom de LAG : nom pour le LAG.
- Emplacement : emplacement pour le LAG.
- Vitesse du port : vitesse du port pour les connexions.
- Nombre de nouvelles connexions : le nombre de nouvelles connexions à créer. Vous pouvez avoir un maximum de quatre connexions lorsque la vitesse du port est de 1G ou 10G, ou deux lorsque la vitesse du port est de 100G.
- (Facultatif) Configurez la sécurité MAC (MACsec) pour la connexion. Sous Paramètres supplémentaires, sélectionnez Demander un port compatible MACsec.

  MACsec est disponible uniquement sur les connexions dédiées.
- (Facultatif) Ajoutez ou supprimez une balise.

  [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

  - Pour Key (Clé), saisissez le nom de la clé.
  - Pour Valeur, saisissez la valeur de clé.

  [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

5. Sélectionnez Créer LAG.

Create a LAG with existing connections using the console

Pour créer un LAG à partir des connexions existantes

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez Créer LAG.
4. Sous Lag creation type (Type de création de LAG), choisissez Utiliser les connexions existantes et fournissez les informations suivantes :

   - Nom de LAG : nom pour le LAG.
   - Connexions existantes : la connexion Direct Connect à utiliser pour le LAG.
   - (Facultatif) Nombre de nouvelles connexions : le nombre de nouvelles connexions à créer. Vous pouvez avoir un maximum de quatre connexions lorsque la vitesse du port est de 1G ou 10G, ou deux lorsque la vitesse du port est de 100G.

- Liens minimum : le nombre minimum de connexions opérationnelles pour que le LAG soit opérationnel. Si vous ne spécifiez aucune valeur, nous attribuons une valeur par défaut de 0.

5. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

6. Sélectionnez Créer LAG.

Command line

Pour créer un LAG à l'aide de la ligne de commande ou de l'API

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

Pour décrire vos LAG à l'aide de la ligne de commande ou de l'API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Pour télécharger la LOA-CFA à l'aide de la ligne de commande ou de l'API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

Après que vous créez un LAG, vous pouvez y associer des connexions ou les dissocier. Pour plus d'informations, consultez Associer une connexion à un LAG et Dissocier une connexion d'un LAG.

Afficher les détails de votre LAG

Après que vous créez un LAG, vous pouvez afficher ses détails.

Console

Pour afficher des informations sur votre LAG :

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Vous pouvez consulter les informations liées au LAG, notamment son ID et le point de terminaison AWS Direct Connect sur lequel les connexions s'arrêtent.

Command line

Pour obtenir des informations sur votre LAG à l'aide de la ligne de commande ou de l'API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Mettre à jour un LAG

Vous pouvez mettre à jour les attributs de groupe d'agrégation de liaisons (LAG) suivants :

- Le nom du LAG.
- La valeur du nombre minimum de connexions opérationnelles pour que le LAG soit opérationnel.
- Le mode de chiffrement MACsec du LAG.

  MACsec est disponible uniquement sur les connexions dédiées.

  AWS attribue cette valeur à chaque connexion faisant partie du LAG.

  Les valeurs valides sont :

  - `should_encrypt`
  - `must_encrypt`

    Lorsque vous définissez le mode de chiffrement sur cette valeur, les connexions sont interrompues lorsque le chiffrement est interrompu.
  - `no_encrypt`

- Les balises.

> **Note**
>
> Si vous ajustez la valeur seuil du nombre minimum de connexions opérationnelles, veillez à ce que la nouvelle valeur n'entraîne pas la chute du LAG sous le seuil sinon il n'est plus opérationnel.

Console

Pour mettre à jour un LAG

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez le LAG, puis choisissez Modifier.
4. Modification du LAG

   [Modifier le nom] Pour Nom du LAG, saisissez un nouveau nom de LAG.

   [Ajuster le nombre minimum de connexions] Pour Liens minimum, saisissez le nombre minimum de connexions opérationnelles.

   [Add a tag] Choisissez Add tag (Ajouter une balise) et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.
5. Choisissez Modifier le LAG.

Command line

Pour mettre à jour un LAG à l'aide de la ligne de commande ou de l'API

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

Pour ajouter et supprimer une balise à l'aide de la ligne de commande

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Associer une connexion à un LAG

Vous pouvez associer une connexion existante à un LAG. La connexion peut être autonome ou faire partie d'un autre LAG. La connexion doit se trouver sur le même appareil AWS et doit utiliser la même bande passante que le LAG. Si la connexion est déjà associée à un autre LAG, vous ne pouvez pas la réassocier si la suppression de la connexion fait passer le nombre minimum de connexions opérationnelles du LAG en dessous de la valeur configurée.

L'association d'une connexion à un LAG réassocie automatiquement ses interfaces virtuelles au LAG.

> **Important**
>
> La connectivité à AWS via la connexion est temporairement interrompue pendant l'association.

Console

Pour associer une connexion à un LAG

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez le LAG, puis choisissez Afficher les détails.
4. Sous Connexions, choisissez Associer une connexion.
5. Pour Connexion, choisissez la connexion Direct Connect à utiliser pour le LAG.
6. Choisissez Associer une connexion.

Command line

Pour associer une connexion à l'aide de la ligne de commande ou de l'API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

Dissocier une connexion d'un LAG

Convertissez une connexion en autonome en la dissociant d'un LAG. Vous ne pouvez pas dissocier une connexion sans que le LAG devienne inférieur au nombre minimum de connexions opérationnelles configuré.

La dissociation d'une connexion d'un LAG ne dissocie pas automatiquement les interfaces virtuelles.

> **Important**
>
> Votre connexion à AWS est interrompue pendant la dissociation.

Console

Pour dissocier une connexion d'un LAG

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, choisissez LAG.
3. Sélectionnez le LAG, puis choisissez Afficher les détails.
4. Sous Connexions, sélectionnez la connexion dans la liste des connexions disponibles et choisissez Dissocier.
5. Dans la boîte de dialogue de confirmation, choisissez Disassociate (Dissocier).

Command line

Pour dissocier une connexion à l'aide de la ligne de commande ou de l'API

- disassociate-connection-from-lag (AWS CLI)

- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

Associer une MACsec CKN/CAK à un LAG

Après avoir créé le LAG compatible avec MACsec, vous pouvez associer un CKN/CAK à la connexion.

> **Note**
>
> Vous ne pouvez pas modifier une clé secrète MACsec après l'avoir associée à un LAG. Si vous devez modifier la clé, dissociez-la de la connexion, puis associez une nouvelle clé à la connexion. Pour plus d'informations sur la suppression d'une association, veuillez consulter the section called “Supprimer l'association entre un LAG et une clé secrète MACsec”.

Console

Pour associer une clé MACsec à un LAG

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Choisissez Associer une clé.
5. Saisissez la clé MACsec.

   [Utiliser la paire CAK/CKN] Choisissez Paire de clés, puis procédez comme suit :

   - Pour la Clé d'association de connectivité (CAK), saisissez la CAK.
   - Pour le Nom de la clé d'association de connectivité (CKN), saisissez le CKN.

   [Utiliser le secret] Choisissez le secret Existing Secret Manager, puis pour Secret, sélectionnez la clé secrète MACsec.
6. Choisissez Associer une clé.

Command line

Pour associer une clé MACsec à un LAG

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct ConnectAPI)

Supprimer l'association entre un LAG et une clé secrète MACsec

Vous pouvez supprimer l'association entre le LAG et la clé MACsec.

Console

Pour supprimer une association entre un LAG et une clé MACsec

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Sélectionnez le secret MACsec à supprimer, puis choisissez Dissocier la clé.
5. Dans la boîte de dialogue de confirmation, saisissez dissocier, puis choisissez Dissocier.

Command line

Pour supprimer une association entre un LAG et une clé MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

Supprimer les LAG

Si vous n'avez plus besoin de certains LAG, vous pouvez les supprimer. Vous ne pouvez pas supprimer un LAG si des interfaces virtuelles y sont associées. Vous devez d'abord supprimer les interfaces virtuelles ou les associer à un autre LAG ou à une autre connexion. La suppression d'un LAG ne supprime pas les connexions du LAG ; vous devez les supprimer vous-même. Pour plus d'informations, consultez Supprimer les connexions.

Console

Pour supprimer un LAG

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez LAG.
3. Sélectionnez les LAG, puis choisissez Supprimer.
4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

Command line

Pour supprimer un LAG à l'aide de la ligne de commande ou de l'API

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

Utilisation des passerelles Direct Connect

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

Table des matières

Passerelles Direct Connect

Utilisez AWS Direct Connect une passerelle pour connecter vos VPC. Vous associez une passerelle AWS Direct Connect à l'une des passerelles suivantes :

- Un passerelle de transit quand vous avez plusieurs VPC dans la même région
- Passerelle privée virtuelle

Vous pouvez également utiliser une passerelle privée virtuelle pour étendre votre zone locale. Cette configuration permet au VPC associé à la zone locale de se connecter à une passerelle Direct Connect. La passerelle Direct Connect se connecte à un emplacement Direct Connect dans une région. Le centre de données sur site dispose d'une connexion Direct Connect vers l'emplacement Direct Connect. Pour plus d'informations, consultez la section Accès aux zones locales à l'aide d'une passerelle Direct Connect dans le Guide de l'utilisateur Amazon VPC.

Une passerelle Direct Connect est une ressource accessible partout dans le monde. Vous pouvez vous connecter à n'importe quelle région globalement à l'aide d'une passerelle Direct Connect. Cela inclut AWS GovCloud (US) mais n'inclut pas les régions de AWS Chine.

Les clients utilisant Direct Connect avec des VPC qui contournent actuellement une zone de disponibilité parent ne pourront pas migrer leurs connexions Direct Connect ou leurs interfaces virtuelles.

Les ci-après décrivent les scénarios dans lesquels vous pouvez utiliser une passerelle Direct Connect.

Une passerelle Direct Connect n'autorise pas les associations de passerelles se trouvant sur la même passerelle Direct Connect à échanger du trafic entre elles (par exemple, une passerelle privée virtuelle vers une autre passerelle privée virtuelle). Une exception à cette règle, mise en œuvre en novembre 2021, est lorsqu'un superréseau est publié sur deux VPC ou plus, dont les passerelles privées virtuelles (VGW) attachées sont associées à la même passerelle Direct Connect et sur la même interface virtuelle. Dans ce cas, les VPC peuvent communiquer les uns avec les autres via le point de terminaison Direct Connect. Par exemple, si vous publiez un superréseau (par exemple, 10.0.0.0/8 ou 0.0.0.0/0) qui chevauche les VPC connectés à une passerelle Direct Connect (par exemple, 10.0.0.0/24 et 10.0.1.0/24) et sur la même interface virtuelle, les VPC peuvent communiquer entre eux à partir de votre réseau sur site.

Si vous souhaitez bloquer les communications VPC à VPC au sein d'une passerelle Direct Connect, procédez comme suit :

1. Configurez des groupes de sécurité sur les instances et les autres ressources du VPC pour bloquer le trafic entre les VPC, en les utilisant également dans le cadre du groupe de sécurité par défaut du VPC.
2. Évitez de publier un superréseau depuis votre réseau sur site qui chevauche vos VPC. Au lieu de cela, vous pouvez annoncer des acheminements plus spécifiques à partir de votre réseau sur site qui ne chevauchent pas avec vos VPC.
3. Allouez une seule passerelle Direct Connect pour chaque VPC que vous souhaitez connecter à votre réseau sur site au lieu d'utiliser la même passerelle Direct Connect pour plusieurs VPC. Par exemple, au lieu d'utiliser une seule passerelle Direct Connect pour vos VPC de développement et de production, utilisez des passerelles Direct Connect distinctes pour chacun de ces VPC.

Une passerelle Direct Connect n'empêche pas l'envoi du trafic depuis une association de passerelles vers l'association de passerelles elle-même (par exemple lorsque vous disposez d'une route supernet sur site qui contient les préfixes de l'association de passerelles). Si vous avez une configuration avec plusieurs VPC connectés à des passerelles de transit associées à la même passerelle Direct Connect, les VPC peuvent communiquer. Pour empêcher les VPC de communiquer, associez une table de routage aux pièces jointes VPC pour lesquelles l'option Blackhole est définie.

Les ci-après décrivent les scénarios dans lesquels vous pouvez utiliser une passerelle Direct Connect.

Scénarios

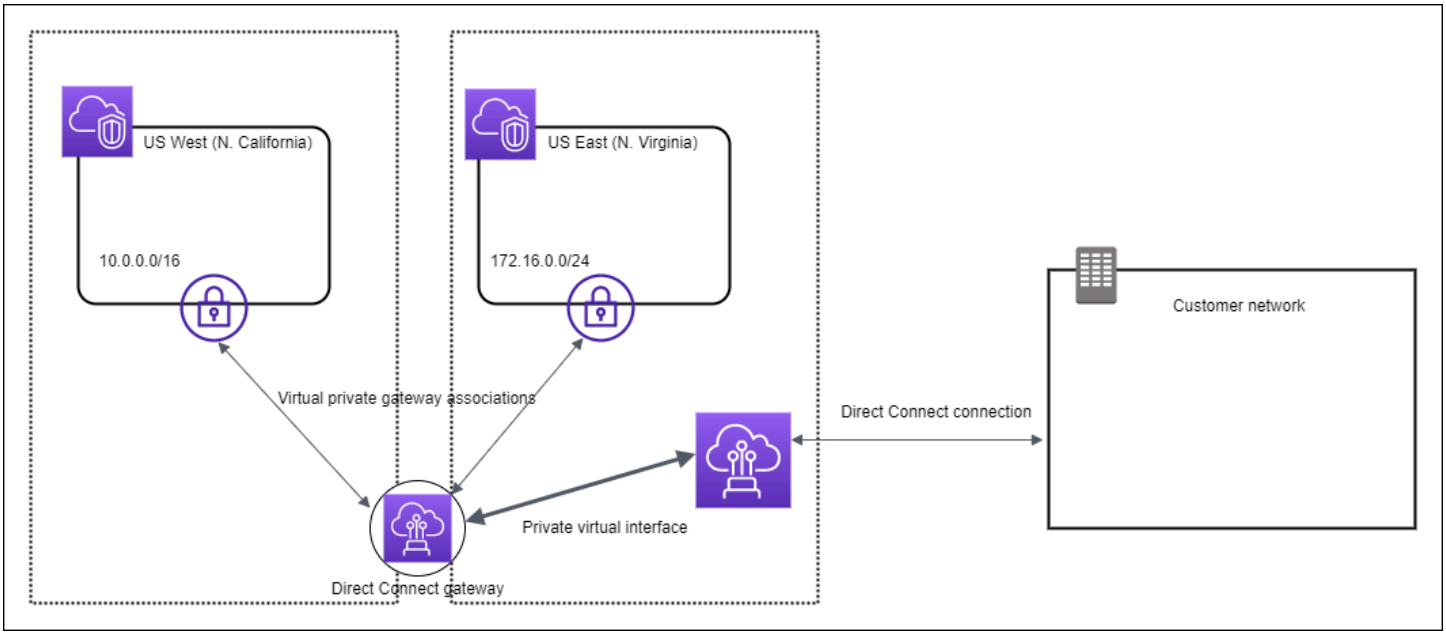
- Associations de la passerelle privée virtuelle

- Associations de passerelles privées virtuelles entre comptes
- Associations de la passerelle de transit
- Associations de passerelles de transit entre comptes
- Création d'une passerelle Direct Connect
- Suppression de passerelles Direct Connect
- Migration d'une passerelle privée virtuelle vers une passerelle Direct Connect

Associations de la passerelle privée virtuelle

Dans le diagramme suivant, la passerelle Direct Connect vous permet d'utiliser votre connexion AWS Direct Connect dans la région USA Est (Virginie du Nord) pour accéder aux VPC de votre compte dans les régions USA Est (Virginie du Nord) et USA Ouest (Californie du Nord).

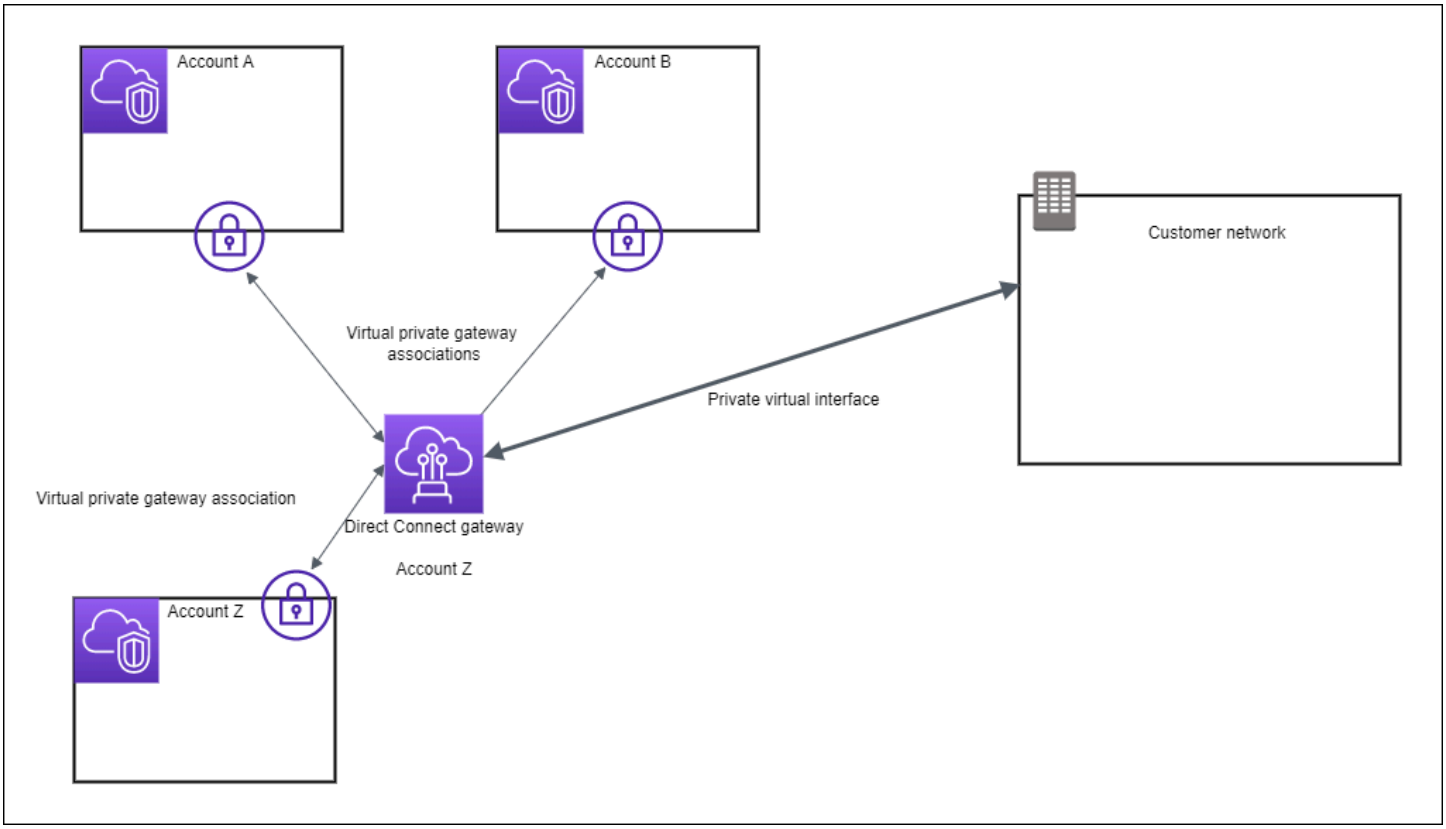
Chaque VPC possède une passerelle privée virtuelle qui se connecte à la passerelle Direct Connect à l'aide d'une association de passerelle privée virtuelle. La passerelle Direct Connect utilise une interface virtuelle privée pour la connexion à l' AWS Direct Connect emplacement. Il existe une connexion AWS Direct Connect entre l'emplacement et le centre de données du client.



Associations de passerelles privées virtuelles entre comptes

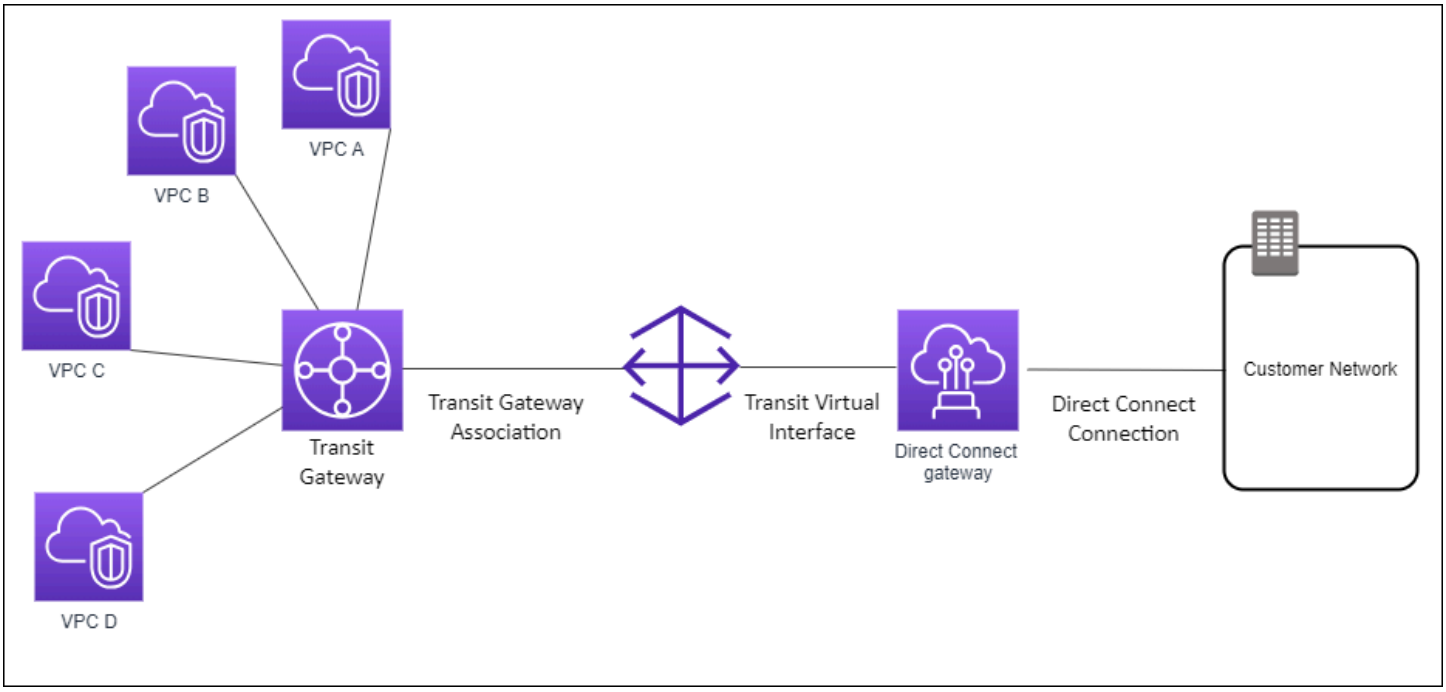
Imaginez ce scénario d'un propriétaire de passerelle Direct Connect (compte Z) qui possède la passerelle Direct Connect. Le compte A et le compte B souhaitent utiliser la passerelle Direct

Connect. Le compte A et le compte B envoient chacun une proposition d'association au compte Z. Le compte Z accepte les propositions d'associations et peut éventuellement mettre à jour les préfixes qui sont autorisés à partir de la passerelle privée virtuelle du compte A ou de la passerelle privée virtuelle du compte B. Une fois que le compte Z a accepté les propositions, le compte A et le compte B peuvent acheminer le trafic depuis leur passerelle privée virtuelle vers la passerelle Direct Connect. Le compte Z est également propriétaire du routage vers les clients étant donné qu'il est propriétaire de la passerelle.



Associations de la passerelle de transit

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



La solution implique les éléments suivants :

- Une passerelle de transit disposant d'attachements VPC.
- 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.

Cette configuration offre les avantages suivants. Vous pouvez :

- Gérer une connexion unique pour plusieurs VPC ou VPN qui se trouvent dans la même région.
- Annoncez les préfixes depuis AWS AWS et vers le local.

Pour plus d'informations sur la configuration des passerelles de transit, consultez Utilisation des passerelles de transit dans le Guide des passerelles de transit Amazon VPC.

Associations de passerelles de transit entre comptes

Imaginez ce scénario d'un propriétaire de passerelle Direct Connect (compte Z) qui possède la passerelle Direct Connect. Compte A détient la passerelle de transit et souhaite utiliser la passerelle Direct Connect. Compte Z accepte les propositions d'association et peut éventuellement mettre à jour les préfixes autorisés à partir de la passerelle de transit du compte A. Une fois que le compte

Z a accepté les propositions, les VPC attachés à la passerelle de transit peuvent acheminer le trafic depuis la passerelle de transit vers la passerelle Direct Connect. Le compte Z est également propriétaire du routage vers les clients étant donné qu'il est propriétaire de la passerelle.

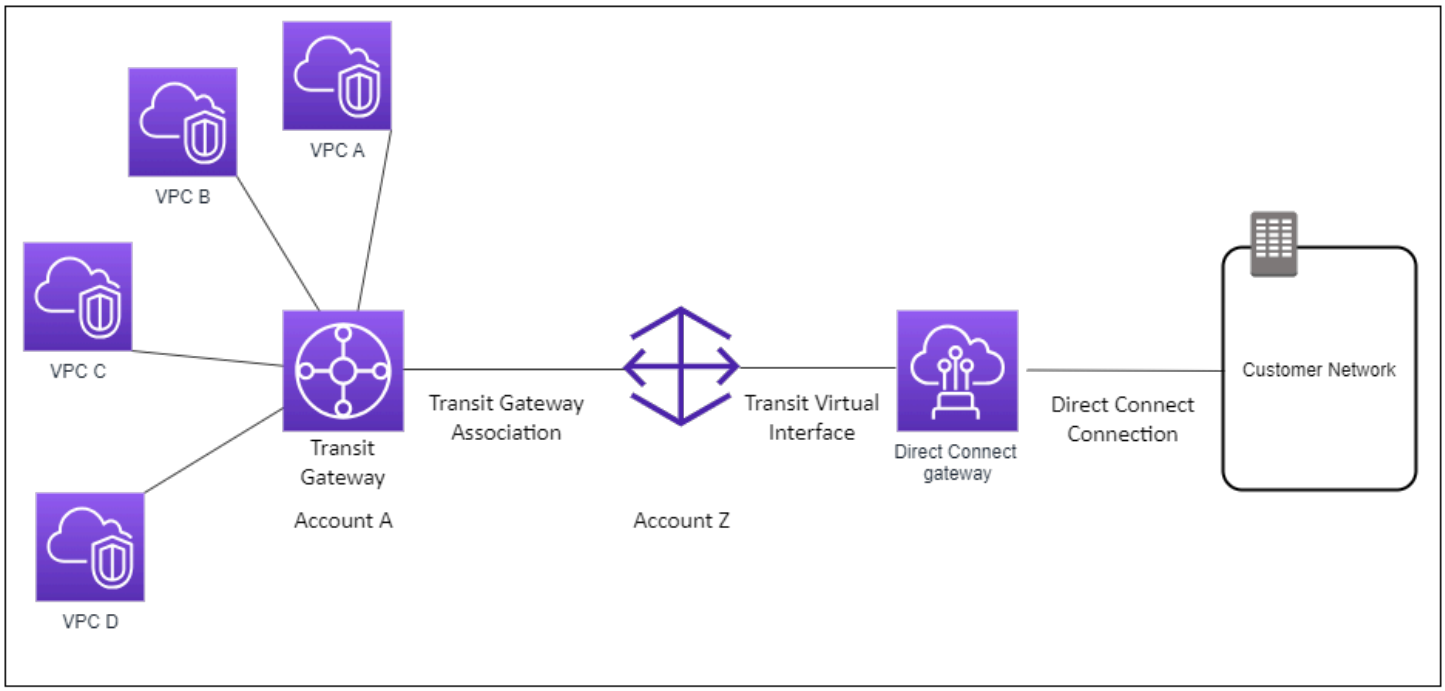


Table des matières

Création d'une passerelle Direct Connect

Vous pouvez créer une passerelle Direct Connect dans toutes les régions prises en charge.

Pour créer une passerelle Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Choisissez Créer une passerelle Direct Connect.
4. Spécifiez les informations suivantes, puis choisissez Créer une passerelle Direct Connect.
   - Nom : indiquez un nom vous permettant d'identifier la passerelle Direct Connect.

- ASN côté Amazon : spécifiez l'ASN relatif au côté Amazon de la session BGP. L'ASN doit être compris entre 64 512 et 65 534 ou entre 4 200 000 000 et 4 294 967 294.
- Passerelle privée virtuelle : pour associer une passerelle privée virtuelle, choisissez la passerelle privée virtuelle.

Pour créer une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Suppression de passerelles Direct Connect

Si vous n'avez plus besoin d'une passerelle Direct Connect, vous pouvez la supprimer. Vous devez d'abord dissocier toutes les passerelles privées virtuelles et supprimer l'interface virtuelle privée attachée.

Pour supprimer une passerelle Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Sélectionnez les passerelles, puis choisissez Supprimer.

Pour supprimer une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

Migration d'une passerelle privée virtuelle vers une passerelle Direct Connect

Si vous aviez une passerelle privée virtuelle attachée à une interface virtuelle et que vous souhaitez migrer vers une passerelle Direct Connect, effectuez les opérations suivantes :

Pour migrer vers une passerelle Direct Connect

1. Créez une passerelle Direct Connect. Pour plus d'informations, consultez the section called "Création d'une passerelle Direct Connect".
2. Créez une interface virtuelle pour la passerelle Direct Connect. Pour plus d'informations, consultez the section called "Créer une interface virtuelle".
3. Associez la passerelle privée virtuelle à la passerelle Direct Connect. Pour plus d'informations, consultez the section called "Association et dissociation de passerelles privées virtuelles".
4. Supprimez l'interface virtuelle associée à la passerelle privée virtuelle. Pour plus d'informations, consultez the section called "Supprimer les interfaces virtuelles".

Associations de la passerelle privée virtuelle

Vous pouvez faire appel à une passerelle AWS Direct Connect pour associer votre connexion AWS Direct Connect , via une interface virtuelle privée, à un ou plusieurs VPC de n'importe quel compte situés dans la même région ou dans d'autres régions. Vous ne pouvez pas associer une passerelle Direct Connect à la passerelle privée virtuelle du VPC. Ensuite, vous créez une interface virtuelle privée pour votre AWS Direct Connect connexion à la passerelle Direct Connect. Il est possible d'attacher plusieurs interfaces virtuelles privées à votre passerelle Direct Connect.

Les règles suivantes s'appliquent aux associations de passerelles privées virtuelles :

- N'activez la propagation d'itinéraires qu'après avoir associé une passerelle virtuelle à une passerelle Direct Connect. Si vous activez la propagation des itinéraires avant d'associer les passerelles, les itinéraires risquent d'être propagés de manière incorrecte.
- Il existe des restrictions concernant la création et l'utilisation des passerelles Direct Connect. Pour plus d'informations, consultez Quotas.
- Vous ne pouvez pas attacher une passerelle Direct Connect à une passerelle privée virtuelle lorsque la passerelle Direct Connect est déjà associée à une passerelle de transit.
- Les VPC auxquels vous vous connectez via une passerelle Direct Connect ne peuvent pas avoir des blocs d'adresse CIDR qui se chevauchent. Si vous ajoutez un bloc CIDR IPv4 à un VPC qui est associé à une passerelle Direct Connect, assurez-vous que ce nouveau bloc ne chevauche pas un bloc CIDR existant d'un autre VPC associé. Pour de plus amples informations, veuillez consulter Ajout de blocs d'adresse CIDR IPv4 à un VPC dans le Guide de l'utilisateur Amazon VPC.
- Il n'est pas possible de créer une interface virtuelle publique vers une passerelle Direct Connect.

- Une passerelle Direct Connect prend uniquement en charge la communication entre les interfaces virtuelles privées attachées et les passerelles privées virtuelles associées et peut activer une passerelle privée virtuelle vers une autre passerelle privée. Les flux de trafic suivants ne sont pas pris en charge :
  - Communication directe entre les VPC qui sont associés à une passerelle Direct Connect unique. Cela inclut le trafic d'un VPC à un autre à l'aide d'un branchement en épingle à cheveux via un réseau sur site par le biais d'une passerelle Direct Connect unique.
  - Communication directe entre les interfaces virtuelles qui sont attachées à une passerelle Direct Connect unique.
  - Communication directe entre les interfaces virtuelles attachées à une passerelle Direct Connect unique et une connexion VPN sur une passerelle privée virtuelle qui est associée à la même passerelle Direct Connect.
- Vous ne pouvez pas associer une passerelle réseau privé virtuel à plusieurs passerelles Direct Connect, ni attacher une interface réseau privé virtuel à plusieurs passerelles Direct Connect.
- Une passerelle réseau privé virtuel que vous associez à une passerelle Direct Connect doit être attachée à un VPC.
- Une proposition d'association de passerelle privée virtuelle expire 7 jours après sa création.
- Une proposition d'association de passerelle privée virtuelle acceptée ou supprimée reste visible pendant 3 jours.
- Une passerelle privée virtuelle peut être associée à une passerelle Direct Connect et également attachée à une interface virtuelle.
- Le détachement d'une passerelle privée virtuelle d'un VPC dissocie également la passerelle privée virtuelle d'une passerelle Direct Connect.

Pour connecter votre AWS Direct Connect connexion à un VPC de la même région uniquement, vous pouvez créer une passerelle Direct Connect. Vous pouvez également créer une interface virtuelle privée et l'attacher à la passerelle privée virtuelle du VPC. Pour plus d'informations, consultez Créer une interface virtuelle privée et VPN CloudHub.

Pour utiliser votre AWS Direct Connect connexion avec un VPC dans un autre compte, vous pouvez créer une interface virtuelle privée hébergée pour ce compte. Lorsque le propriétaire de l'autre compte accepte l'interface virtuelle hébergée, il peut choisir de l'attacher à une passerelle réseau privé virtuel ou à une passerelle Direct Connect dans son compte. Pour plus d'informations, consultez AWS Direct Connect interfaces virtuelles.

Table des matières

Créer une passerelle privée virtuelle

La passerelle réseau privé virtuel doit être attachée au VPC auquel vous souhaitez vous connecter.

> **Note**
>
> Si vous envisagez d'utiliser la passerelle privée virtuelle pour une passerelle Direct Connect et une connexion VPN dynamique, définissez l'ASN de la passerelle privée virtuelle avec la valeur dont vous avez besoin pour la connexion VPN. Sinon, l'ASN sur la passerelle privée virtuelle peut être défini sur n'importe quelle valeur autorisée. La passerelle Direct Connect publie tous les VPC connectés sur l'ASN qui lui est affecté.

Après avoir créé une passerelle réseau privé virtuel, vous devez l'attacher à votre VPC.

Pour créer une passerelle réseau privé virtuel et l'attacher à votre VPC

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles privées virtuelles, puis Créer une passerelle privée virtuelle.
3. (Facultatif) Entrez un nom pour votre passerelle réseau privé virtuel. Cette étape crée une balise avec une clé de `Name` et la valeur que vous spécifiez.
4. Pour ASN, conservez la sélection par défaut pour utiliser le numéro d'ASN Amazon par défaut. Sinon, choisissez ASN personnalisé et entrez une valeur. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 4200000000 et 4294967294.
5. Cliquez sur Créer une passerelle réseau privé virtuel.
6. Sélectionnez la passerelle réseau privé virtuel que vous avez créée, puis choisissez Actions, Attacher au VPC.

7. Sélectionnez le VPC dans la liste et choisissez Oui, attacher.

Pour créer une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- CreateVpnGateway(API de requête Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Pour attacher une passerelle réseau privé virtuel à un VPC à l'aide de la ligne de commande ou de l'API

- AttachVpnGateway(API de requête Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Association et dissociation de passerelles privées virtuelles

Vous pouvez associer ou dissocier une passerelle privée virtuelle et une passerelle Direct Connect. Le propriétaire du compte de la passerelle privée virtuelle effectue ces opérations.

Pour associer une passerelle privée virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect, puis sélectionnez la passerelle Direct Connect.
3. Sélectionnez Afficher les détails.
4. Choisissez Associations de passerelles, puis choisissez Associer la passerelle.
5. Pour Gateways (Passerelles), choisissez les passerelles privées virtuelles à associer, puis choisissez Associate gateway (Associer la passerelle).

Vous pouvez afficher toutes les passerelles privées virtuelles qui sont associées à la passerelle Direct Connect en cliquant sur Gateway associations (Associations de passerelles).

Pour dissocier une passerelle privée virtuelle

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect, puis sélectionnez la passerelle Direct Connect.
3. Sélectionnez Afficher les détails.
4. Choisissez Associations de passerelle, puis sélectionnez la passerelle privée virtuelle.
5. Choisissez Dissocier.

Pour associer une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- create-direct-connect-gateway-association ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Pour afficher la liste des passerelles privées virtuelles associées à une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-associations ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Pour dissocier une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-association ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Création d'une interface virtuelle privée vers la passerelle Direct Connect

Pour connecter votre AWS Direct Connect connexion au VPC distant, vous devez créer une interface virtuelle privée pour votre connexion. Spécifiez la passerelle Direct Connect à laquelle vous souhaitez vous connecter.

> **Note**
>
> Si vous acceptez une interface virtuelle privée hébergée, vous pouvez l'associer à une passerelle Direct Connect dans votre compte. Pour plus d'informations, consultez Accepter une interface virtuelle hébergée.

Pour mettre en service une interface virtuelle privée vers une passerelle Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Type d'interface virtuelle, choisissez Privée.
5. Sous Paramètres de l'interface virtuelle privée, procédez comme suit :
   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.
   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.
   c. Pour Propriétaire de l'interface virtuelle, choisissez Mon AWS compte si l'interface virtuelle est destinée à votre AWS compte.
   d. Pour Passerelle Direct Connect, sélectionnez la passerelle Direct Connect.
   e. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).
   f. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1 à 2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :
   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.

- Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

  > **Important**
  >
  > Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage (autre que la RFC 1918) et spécifier l'adresse vous-même.
  >
  > - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
  > - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

  [IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 9001 (trames jumbo), sélectionnez MTU Jumbo (taille MTU 9001).

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

   - Pour Key (Clé), saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   [Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Une fois l'interface virtuelle créée, vous pouvez télécharger la configuration du routeur pour votre appareil. Pour plus d'informations, consultez Télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle privée à l'aide de la ligne de commande ou de l'API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Pour afficher la liste des interfaces virtuelles attachées à une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-pièces jointes ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Association d'une passerelle privée virtuelle entre comptes

Vous pouvez associer une passerelle Direct Connect à une passerelle privée virtuelle appartenant à n'importe quel AWS compte. La passerelle Direct Connect peut être une passerelle existante ou vous pouvez créer une nouvelle passerelle. Le propriétaire de la passerelle privée virtuelle crée une proposition d'association et le propriétaire de la passerelle Direct Connect doit accepter la proposition d'association.

Une proposition d'association peut contenir des préfixes qui seront autorisés à partir de la passerelle privée virtuelle. Le propriétaire de la passerelle Direct Connect peut éventuellement remplacer les préfixes demandés dans la proposition d'association.

Préfixes autorisés

Lorsque vous associez une passerelle privée virtuelle à une passerelle Direct Connect, vous spécifiez une liste des préfixes Amazon VPC à publier dans la passerelle Direct Connect. La liste de préfixes agit comme un filtre qui permet de publier les même CIDR, ou des CIDR plus petits, dans la passerelle Direct Connect. Vous devez définir les préfixes autorisés dans une plage identique ou plus large à celle des CIDR VPC, étant donné que nous allouons l'ensemble des CIDR VPC à la passerelle privée virtuelle.

Examinez le cas où le CIDR VPC est 10.0.0.0/16. Vous pouvez définir les Préfixes autorisés sur 10.0.0.0/16 (valeur du CIDR VPC) ou 10.0.0.0/15 (valeur plus large que le CIDR VPC).

Toute interface virtuelle à l'intérieur des préfixes réseau annoncés via Direct Connect est uniquement propagée aux passerelles de transit entre les régions, et non au sein d'une même région. Pour

plus d'informations sur la façon dont les préfixes autorisés interagissent avec les passerelles privées virtuelles et les passerelles de transit, consultez the section called "Interactions des préfixes autorisés".

Tâches

- Création d'une proposition d'association
- Acceptation ou refus d'une proposition d'association
- Mise à jour des préfixes autorisés pour une association
- Suppression d'une proposition d'association

Création d'une proposition d'association

Si vous possédez la passerelle privée virtuelle, vous devez créer une proposition d'association. La passerelle privée virtuelle doit être attachée à un VPC de votre AWS compte. Le propriétaire de la passerelle Direct Connect doit partager l'identifiant de la passerelle Direct Connect et l'identifiant de son AWS compte. Après avoir créé la proposition, le propriétaire de la passerelle Direct Connect doit l'accepter pour que vous puissiez obtenir l'accès au réseau sur site via AWS Direct Connect.

Pour créer une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Virtual private gateways (Passerelles privées virtuelles) et sélectionnez la passerelle privée virtuelle.
3. Sélectionnez Afficher les détails.
4. Choisissez Direct Connect gateway associations (Associations de la passerelle Direct Connect) et choisissez Associate Direct Connect gateway (Associer la passerelle Direct Connect).
5. Sous Association account type (Type de compte d'association), pour Account owner (Propriétaire du compte), choisissez Another account (Un autre compte).
6. Pour le Propriétaire de la passerelle Direct Connect, saisissez l'ID du compte AWS qui possède la passerelle Direct Connect.
7. Sous Association settings (Paramètres de l'association), effectuez les opérations suivantes :

   a. Pour Direct Connect gateway ID (ID de la passerelle Direct Connect), saisissez l'ID de la passerelle Direct Connect.

b. Pour le propriétaire de la passerelle Direct Connect, entrez l'ID du AWS compte propriétaire de la passerelle Direct Connect pour l'association.

c. (Facultatif) Pour spécifier une liste des préfixes à autoriser à partir de la passerelle privée virtuelle, ajoutez les préfixes dans Préfixes autorisés, en les séparant par des virgules ou en les entrant sur des lignes séparées..

8. Choisissez Associate Direct Connect gateway (Associer la passerelle Direct Connect).

Pour créer une proposition d'association à l'aide de la ligne de commande ou de l'API

- create-direct-connect-gateway-proposition d'association ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Acceptation ou refus d'une proposition d'association

Si vous possédez la passerelle Direct Connect, vous devez accepter la proposition d'association afin de créer l'association. Dans le cas contraire, vous pouvez rejeter la proposition d'association.

Pour accepter une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Sélectionnez la passerelle Direct Connect avec les propositions en attente, puis choisissez Afficher les détails.
4. Dans l'onglet Propositions en attente, sélectionnez la proposition, puis choisissez Accepter la proposition.
5. (Facultatif) Pour spécifier une liste des préfixes à autoriser à partir de la passerelle privée virtuelle, ajoutez les préfixes dans Préfixes autorisés, en les séparant par des virgules ou en les entrant sur des lignes séparées.
6. Choisissez Accepter la proposition.

Pour rejeter une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.

2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Sélectionnez la passerelle Direct Connect avec les propositions en attente, puis choisissez Afficher les détails.
4. Dans l'onglet Propositions en attente, sélectionnez la passerelle privée virtuelle et choisissez Rejeter la proposition.
5. Dans la boîte de dialogue Rejeter la proposition, entrez Supprimer et choisissez Rejeter la proposition.

Pour afficher les propositions d'associations à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-propositions d'association ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

Pour accepter une proposition d'association à l'aide de la ligne de commande ou de l'API

- accept-direct-connect-gateway-proposition d'association ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Pour rejeter une proposition d'association à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-proposition d'association ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Mise à jour des préfixes autorisés pour une association

Vous pouvez mettre à jour les préfixes qui sont autorisés à partir de la passerelle privée virtuelle sur la passerelle Direct Connect.

Si vous êtes le propriétaire de la passerelle privée virtuelle, créez une nouvelle proposition d'association pour la même passerelle Direct Connect et la passerelle privée virtuelle, en précisant les préfixes à autoriser.

Si vous êtes le propriétaire de la passerelle Direct Connect, mettez à jour les préfixes autorisés lorsque vous acceptez la proposition d'association ou mettez à jour les préfixes autorisés pour une association existante comme suit.

Pour mettre à jour les préfixes autorisés pour une association existante à l'aide de la ligne de commande ou de l'API

- update-direct-connect-gateway-association ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Suppression d'une proposition d'association

Le propriétaire de la passerelle privée virtuelle peut supprimer la proposition d'association de la passerelle Direct Connect si celle-ci reste en attente d'acceptation. Une fois qu'une proposition d'association a été acceptée, vous ne pouvez pas la supprimer. Mais vous pouvez dissocier la passerelle privée virtuelle de la passerelle Direct Connect. Pour plus d'informations, consultez the section called "Association et dissociation de passerelles privées virtuelles".

Pour supprimer une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Virtual private gateways (Passerelles privées virtuelles) et sélectionnez la passerelle privée virtuelle.
3. Sélectionnez Afficher les détails.
4. Choisissez Pending Direct Connect gateway associations (Associations en attente de la passerelle Direct Connect), sélectionnez l'association et choisissez Delete association (Supprimer l'association).
5. Dans la boîte de dialogue Supprimer la proposition d'association, entrez Supprimer et choisissez Supprimer.

Pour supprimer une proposition d'association en attente à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-proposition d'association ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Associations de la passerelle de transit

Vous pouvez utiliser une passerelle AWS Direct Connect pour connecter votre connexion AWS Direct Connect via une interface de transit virtuelle aux VPC ou VPN qui sont attachés à votre

passerelle de transit. Vous associez une passerelle Direct Connect à la passerelle de transit. Créez ensuite une interface virtuelle de transit pour votre AWS Direct Connect connexion à la passerelle Direct Connect.

Les règles suivantes s'appliquent aux associations des passerelles de transit :

- Vous ne pouvez pas attacher une passerelle Direct Connect à une passerelle de transit lorsque la passerelle Direct Connect est déjà associée à une passerelle privée virtuelle ou attachée à une interface virtuelle privée.
- Il existe des restrictions concernant la création et l'utilisation des passerelles Direct Connect. Pour plus d'informations, consultez Quotas.
- Une passerelle Direct Connect prend en charge la communication entre les interfaces virtuelles de transport rattachées et les passerelles de transport associées.
- Si vous vous connectez à plusieurs passerelles de transit qui se trouvent dans des régions différentes, utilisez des ASN uniques pour chaque passerelle de transit.
- Toute interface virtuelle à l'intérieur des préfixes réseau annoncés via Direct Connect est uniquement propagée aux passerelles de transit d'une région à l'autre, mais pas au sein d'une même région

Association et dissociation de passerelles de transit

Pour associer une passerelle de transit

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect, puis sélectionnez la passerelle Direct Connect.
3. Sélectionnez Afficher les détails.
4. Choisissez Gateways associations (Associations de passerelles) et choisissez Associate gateway (Associer la passerelle).
5. Pour Passerelles, choisissez la passerelle de transit à associer.
6. Dans Préfixes autorisés, saisissez les préfixes (séparés par une virgule ou sur une nouvelle ligne) que la passerelle Direct Connect annonce au centre de données sur site. Pour en savoir plus sur les préfixes autorisés, consultez the section called "Interactions des préfixes autorisés".
7. Choisissez Associer passerelle

Vous pouvez afficher toutes les passerelles qui sont associées à la passerelle Direct Connect en cliquant sur Gateway associations (Associations de passerelles).

Pour dissocier une passerelle de transit

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect, puis sélectionnez la passerelle Direct Connect.
3. Sélectionnez Afficher les détails.
4. Choisissez Associations de passerelle, puis sélectionnez la passerelle de transit.
5. Choisissez Dissocier.

Pour mettre à jour les préfixes autorisés pour une passerelle de transit

Vous pouvez ajouter ou supprimer des préfixes autorisés sur la passerelle de transit.

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez les passerelles Direct Connect, puis la passerelle Direct Connect pour laquelle vous souhaitez ajouter ou supprimer des préfixes autorisés.
3. Choisissez l'onglet Associations de passerelles.
4. Choisissez la passerelle que vous voulez modifier, puis choisissez Modifier.
5. Dans Préfixes autorisés, saisissez les préfixes que la passerelle Direct Connect annonce au centre de données sur site. Pour les préfixes multiples, séparez chaque préfixe par une virgule ou placez chaque préfixe sur une nouvelle ligne. Les préfixes que vous ajoutez doivent correspondre aux CIDR Amazon VPC pour toutes les passerelles privées virtuelles. Pour en savoir plus sur les préfixes autorisés, consultez the section called “Interactions des préfixes autorisés”.
6. Sélectionnez Edit association.

   Dans la section Association de passerelles, l'état affiche la mise à jour. Lorsque vous avez terminé, l'état devient associé.
7. Choisissez Dissocier.
8. Choisissez à nouveau Dissocier pour confirmer que vous souhaitez dissocier la passerelle.

Dans la section Association de passerelles, l'état affiche la dissociation. Lorsque vous avez terminé, un message de confirmation s'affiche et la passerelle est supprimée de la section. Cela peut prendre plusieurs minutes ou plus.

Pour associer une passerelle de transit à l'aide de la ligne de commande ou de l'API

- create-direct-connect-gateway-association ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Pour afficher les passerelles de transit associées à une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-associations ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Pour dissocier une passerelle de transit à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-association ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Pour mettre à jour des préfixes autorisés pour une passerelle de transit à l'aide de la ligne de commande ou de l'API

- update-direct-connect-gateway-association ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Création d'une interface de transit virtuelle vers la passerelle Direct Connect

Pour connecter votre AWS Direct Connect connexion à la passerelle de transit, vous devez créer une interface de transit pour votre connexion. Spécifiez la passerelle Direct Connect à laquelle vous souhaitez vous connecter.

> **Important**
>
> Si vous associez votre passerelle de transit à une ou plusieurs passerelles Direct Connect, le numéro de système autonome (ASN) utilisé par la passerelle de transit et la passerelle Direct Connect doivent être différents. Par exemple, si vous utilisez l'ASN 64512 par défaut pour la passerelle de transit et la passerelle Direct Connect, la demande d'association échoue.

Pour mettre en service une interface de transit virtuelle vers une passerelle Direct Connect

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.
3. Choisissez Créer une interface virtuelle.
4. Sous Virtual interface type (Type d'interface virtuelle), pour Type, choisissez Private (Privée).
5. Sous Transit virtual interface settings (Paramètres de l'interface virtuelle de transit), procédez comme suit :
   a. Pour Nom de l'interface virtuelle, saisissez le nom de l'interface virtuelle.
   b. Pour Connexion, choisissez la connexion Direct Connect que vous souhaitez utiliser pour cette interface.
   c. Pour Propriétaire de l'interface virtuelle, choisissez Mon AWS compte si l'interface virtuelle est destinée à votre AWS compte.
   d. Pour Passerelle Direct Connect, sélectionnez la passerelle Direct Connect.
   e. Pour VLAN, saisissez le numéro d'identification de votre réseau local virtuel (VLAN).
   f. Pour BGP ASN, saisissez le numéro ASN du protocole BGP de votre routeur homologue local pour la nouvelle interface virtuelle.

      Les valeurs valides sont 1 à 2147483647.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :
   a. Pour configurer un appairage BGP IPv4 ou IPv6, procédez comme suit :

      [IPv4] Pour configurer un appairage BGP IPv4, choisissez IPv4 et effectuez l'une des opérations suivantes :

- Pour spécifier vous-même ces adresses IP, pour IP du pair de votre routeur, saisissez l'adresse de destination CIDR IPv4 à laquelle Amazon doit envoyer le trafic.
- Pour IP du pair du routeur Amazon, entrez l'adresse CIDR IPv4 à utiliser pour envoyer le trafic vers AWS.

> **Important**
>
> Si vous autorisez l' AWS attribution automatique d'adresses IPv4, un CIDR /29 sera attribué à partir de 169.254.0.0/16 IPv4 Link-Local conformément à la RFC 3927 pour la connectivité. point-to-point AWS ne recommande pas cette option si vous avez l'intention d'utiliser l'adresse IP homologue du routeur client comme source et/ou destination pour le trafic VPC. Vous devez plutôt utiliser la RFC 1918 ou un autre adressage (autre que la RFC 1918) et spécifier l'adresse vous-même.
>
> - Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.
> - Pour plus d'informations sur la RFC 3927, consultez Configuration dynamique des adresses lien-local IPv4.

[IPv6] Pour configurer un appairage BGP IPv6, choisissez IPv6. Les adresses d'appairage IPv6 sont automatiquement attribuées à partir du pool d'adresses IPv6 d'Amazon. Vous ne pouvez pas spécifier d'adresses IPv6 personnalisées.

b. Pour remplacer l'unité de transmission maximale (MTU) de 1500 (valeur par défaut) par 8500 (trames jumbo), sélectionnez Jumbo MTU (MTU size 8500) [MTU Jumbo (taille MTU 8500)].

c. (Facultatif) Sous Activer SiteLink, choisissez Activé pour activer la connectivité directe entre les points de présence Direct Connect.

d. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

- Pour Key (Clé), saisissez le nom de la clé.
- Pour Valeur, saisissez la valeur de clé.

[Supprimer une balise] En regard de la balise, choisissez Supprimer la balise.

7. Choisissez Créer une interface virtuelle.

Une fois l'interface virtuelle créée, vous pouvez télécharger la configuration du routeur pour votre appareil. Pour plus d'informations, consultez Télécharger le fichier de configuration du routeur.

Pour créer une interface de transit virtuelle à l'aide de la ligne de commande ou de l'API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Pour afficher la liste des interfaces virtuelles attachées à une passerelle Direct Connect à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-pièces jointes ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Association d'une passerelle de transit entre comptes

Vous pouvez associer une passerelle Direct Connect existante ou une nouvelle passerelle Direct Connect à une passerelle de transit appartenant à n'importe quel AWS compte. Le propriétaire de la passerelle de transit crée une proposition d'association et le propriétaire de la passerelle Direct Connect doit accepter la proposition d'association.

Une proposition d'association peut contenir les préfixes qui seront autorisés à partir de la passerelle de transit. Le propriétaire de la passerelle Direct Connect peut éventuellement remplacer les préfixes demandés dans la proposition d'association.

Préfixes autorisés

Pour une association de passerelles de transit, vous mettez en service la liste des préfixes autorisés sur la passerelle Direct Connect. La liste est utilisée pour acheminer le trafic depuis les locaux AWS vers la passerelle de transit, même si aucun CIDR n'est attribué aux VPC attachés à la passerelle de transit. Les préfixes de la liste des préfixes autorisés de la passerelle Direct Connect proviennent de la passerelle Direct Connect et sont publiés sur le réseau sur site. Pour plus d'informations sur la façon dont les préfixes autorisés interagissent avec les passerelles de transit et les passerelles privées virtuelles, consultez the section called “Interactions des préfixes autorisés”.

Tâches

- Création d'une proposition d'association de la passerelle de transit

- Acceptation ou rejet d'une proposition d'association de la passerelle de transit
- Mise à jour des préfixes autorisés pour une association de passerelle de transit
- Suppression d'une proposition d'association de passerelle de transit

Création d'une proposition d'association de la passerelle de transit

Si vous possédez la passerelle de transit, vous devez créer la proposition d'association. La passerelle de transit doit être attachée à un VPC ou à un VPN dans votre AWS compte. Le propriétaire de la passerelle Direct Connect doit partager l'ID de la passerelle Direct Connect et l'ID de son compte AWS . Après avoir créé la proposition, le propriétaire de la passerelle Direct Connect doit l'accepter pour que vous puissiez obtenir l'accès au réseau sur site via AWS Direct Connect.

Pour créer une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, choisissez Passerelles de transit, puis sélectionnez la passerelle de transit.
3. Sélectionnez Afficher les détails.
4. Choisissez Direct Connect gateway associations (Associations de la passerelle Direct Connect) et choisissez Associate Direct Connect gateway (Associer la passerelle Direct Connect).
5. Sous Association account type (Type de compte d'association), pour Account owner (Propriétaire du compte), choisissez Another account (Un autre compte).
6. Pour le Propriétaire de la passerelle Direct Connect, saisissez l'ID du compte qui possède la passerelle Direct Connect.
7. Sous Association settings (Paramètres de l'association), effectuez les opérations suivantes :
   a. Pour Direct Connect gateway ID (ID de la passerelle Direct Connect), saisissez l'ID de la passerelle Direct Connect.
   b. Pour le Propriétaire de l'interface virtuelle, saisissez l'ID du compte qui possède l'interface virtuelle pour l'association.
   c. (Facultatif) Pour spécifier une liste des préfixes à autoriser à partir de la passerelle de transit, ajoutez les préfixes dans Préfixes autorisés, en les séparant par des virgules ou en les saisissant sur des lignes séparées.
8. Choisissez Associate Direct Connect gateway (Associer la passerelle Direct Connect).

Pour créer une proposition d'association à l'aide de la ligne de commande ou de l'API

- create-direct-connect-gateway-proposition d'association ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Acceptation ou rejet d'une proposition d'association de la passerelle de transit

Si vous possédez la passerelle Direct Connect, vous devez accepter la proposition d'association afin de créer l'association. Vous avez également la possibilité de rejeter la proposition d'association.

Pour accepter une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Sélectionnez la passerelle Direct Connect avec les propositions en attente, puis choisissez Afficher les détails.
4. Dans l'onglet Propositions en attente, sélectionnez la proposition, puis choisissez Accepter la proposition.
5. ((Facultatif) Pour spécifier une liste des préfixes à autoriser à partir de la passerelle de transit, ajoutez les préfixes dans Préfixes autorisés, en les séparant par des virgules ou en les saisissant sur des lignes séparées.
6. Choisissez Accepter la proposition.

Pour rejeter une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Passerelles Direct Connect.
3. Sélectionnez la passerelle Direct Connect avec les propositions en attente, puis choisissez Afficher les détails.
4. Sur l'onglet Propositions en attente, sélectionnez la passerelle de transit, puis choisissez Rejeter la proposition.
5. Dans la boîte de dialogue Rejeter la proposition, entrez Supprimer et choisissez Rejeter la proposition.

Pour afficher les propositions d'associations à l'aide de la ligne de commande ou de l'API

- describe-direct-connect-gateway-propositions d'association ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

Pour accepter une proposition d'association à l'aide de la ligne de commande ou de l'API

- accept-direct-connect-gateway-proposition d'association ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Pour rejeter une proposition d'association à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-proposition d'association ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Mise à jour des préfixes autorisés pour une association de passerelle de transit

Vous pouvez mettre à jour les préfixes autorisés à partir de la passerelle de transit via la passerelle Direct Connect.

Si vous êtes le propriétaire de la passerelle de transit, créez une nouvelle proposition d'association pour la même passerelle Direct Connect et la passerelle privée virtuelle, en précisant les préfixes à autoriser.

Si vous êtes le propriétaire de la passerelle Direct Connect, mettez à jour les préfixes autorisés lorsque vous acceptez la proposition d'association ou mettez à jour les préfixes autorisés pour une association existante comme suit.

Pour mettre à jour les préfixes autorisés pour une association existante à l'aide de la ligne de commande ou de l'API

- update-direct-connect-gateway-association ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Suppression d'une proposition d'association de passerelle de transit

Le propriétaire de la passerelle de transit peut supprimer la proposition d'association de la passerelle Direct Connect si celle-ci reste en attente d'acceptation. Une fois qu'une proposition d'association a

été acceptée, vous ne pouvez pas la supprimer. Mais vous pouvez dissocier la passerelle de transit de la passerelle Direct Connect. Pour plus d'informations, consultez the section called "Création d'une proposition d'association de la passerelle de transit".

Pour supprimer une proposition d'association

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, choisissez Passerelles de transit, puis sélectionnez la passerelle de transit.
3. Sélectionnez Afficher les détails.
4. Choisissez Pending Direct Connect gateway associations (Associations en attente de la passerelle Direct Connect), sélectionnez l'association et choisissez Delete association (Supprimer l'association).
5. Dans la boîte de dialogue Supprimer la proposition d'association, entrez Supprimer et choisissez Supprimer.

Pour supprimer une proposition d'association en attente à l'aide de la ligne de commande ou de l'API

- delete-direct-connect-gateway-proposition d'association ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Interactions des préfixes autorisés

Découvrez la façon dont les préfixes autorisés interagissent avec les passerelles de transit et les passerelle privées virtuelles. Pour plus d'informations, consultez the section called "Stratégies de routage et communautés BGP (Border Gateway Protocol)".

Associations de la passerelle privée virtuelle

La liste de préfixes (IPv4 et IPv6) agit comme un filtre qui permet de publier les même CIDR, ou une plage plus petite de CIDR, dans la passerelle Direct Connect. Vous devez définir les préfixes sur une plage identique ou plus large que le bloc CIDR du VPC.

> **Note**
>
> La liste autorisée fonctionne uniquement comme un filtre, et seul le CIDR VPC associé sera publié sur la passerelle client.

Considérons le scénario où vous avez un VPC avec CIDR 10.0.0.0/16 attaché à une passerelle privée virtuelle.

- Lorsque la liste des préfixes autorisés est définie sur 22.0.0.0/24, vous ne recevez pas de route, car 22.0.0.0/24 est à la fois différent et supérieur à 10.0.0.0/16.
- Lorsque la liste des préfixes autorisés est définie sur 10.0.0.0/24, vous ne recevez pas d'itinéraire, car 10.0.0.0/24 est différent de 10.0.0.0/16.
- Lorsque la liste des préfixes autorisés est définie sur 10.0.0.0/15, vous ne recevez 10.0.0.0/16, parce que l'adresse IP est plus large que 10.0.0.0/16.

Lorsque vous supprimez ou ajoutez un préfixe autorisé, le trafic qui n'utilise pas ce préfixe n'est pas impacté. Pendant les mises à jour, l'état passe de `associated` à `updating`. La modification d'un préfixe existant ne peut retarder que le trafic qui utilise ce préfixe.

Associations de la passerelle de transit

Pour une association de passerelles de transit, vous mettez en service la liste des préfixes autorisés sur la passerelle Direct Connect. La liste achemine le trafic sur site vers ou depuis une passerelle Direct Connect vers la passerelle de transit, même si aucun CIDR n'est attribué aux VPC attachés à la passerelle de transit. Les préfixes autorisés fonctionnent différemment selon le type de passerelle :

- Pour les associations de passerelles de transit, seuls les préfixes autorisés saisis seront publiés sur site. Ils apparaîtront comme provenant de l'ASN de la passerelle Direct Connect.
- Pour les passerelles privées virtuelles, les préfixes autorisés saisis agissent comme un filtre pour autoriser des CIDR identiques ou plus petits.

Considérons le scénario où vous avez un VPC avec CIDR 10.0.0.0/16 attaché à une passerelle de transit.

- Lorsque la liste des préfixes autorisés est définie sur 22.0.0.0/24, vous recevez 22.0.0.0/24 via BGP sur votre interface de transit virtuelle. Vous ne recevez pas 10.0.0.0/16, car nous provisionnons directement les préfixes qui sont dans la liste des préfixes autorisés.
- Lorsque la liste des préfixes autorisés est définie sur 10.0.0.0/24, vous recevez 10.0.0.0/24 via BGP sur votre interface de transit virtuelle. Vous ne recevez pas 10.0.0.0/16, car nous provisionnons directement les préfixes qui sont dans la liste des préfixes autorisés.
- Lorsque la liste des préfixes autorisés est définie sur 10.0.0.0/8, vous recevez 10.0.0.0/8 via BGP sur votre interface de transit virtuelle.

Les chevauchements de préfixes autorisés ne sont pas autorisés lorsque plusieurs passerelles de transit sont associées à une passerelle Direct Connect. Par exemple, si vous avez une passerelle de transit avec une liste de préfixes autorisés qui inclut 10.1.0.0/16 et une deuxième passerelle de transit avec une liste de préfixes autorisés qui inclut 10.2.0.0/16 et 0.0.0.0/0, vous ne pouvez pas définir les associations de la deuxième passerelle de transit sur 0.0.0.0/0. Comme 0.0.0.0/0 inclut tous les réseaux IPv4, vous ne pouvez pas configurer 0.0.0.0/0 si plusieurs passerelles de transit sont associées à une passerelle Direct Connect. Une erreur est renvoyée, indiquant que les routes autorisées chevauchent une ou plusieurs routes autorisées existantes sur la passerelle Direct Connect.

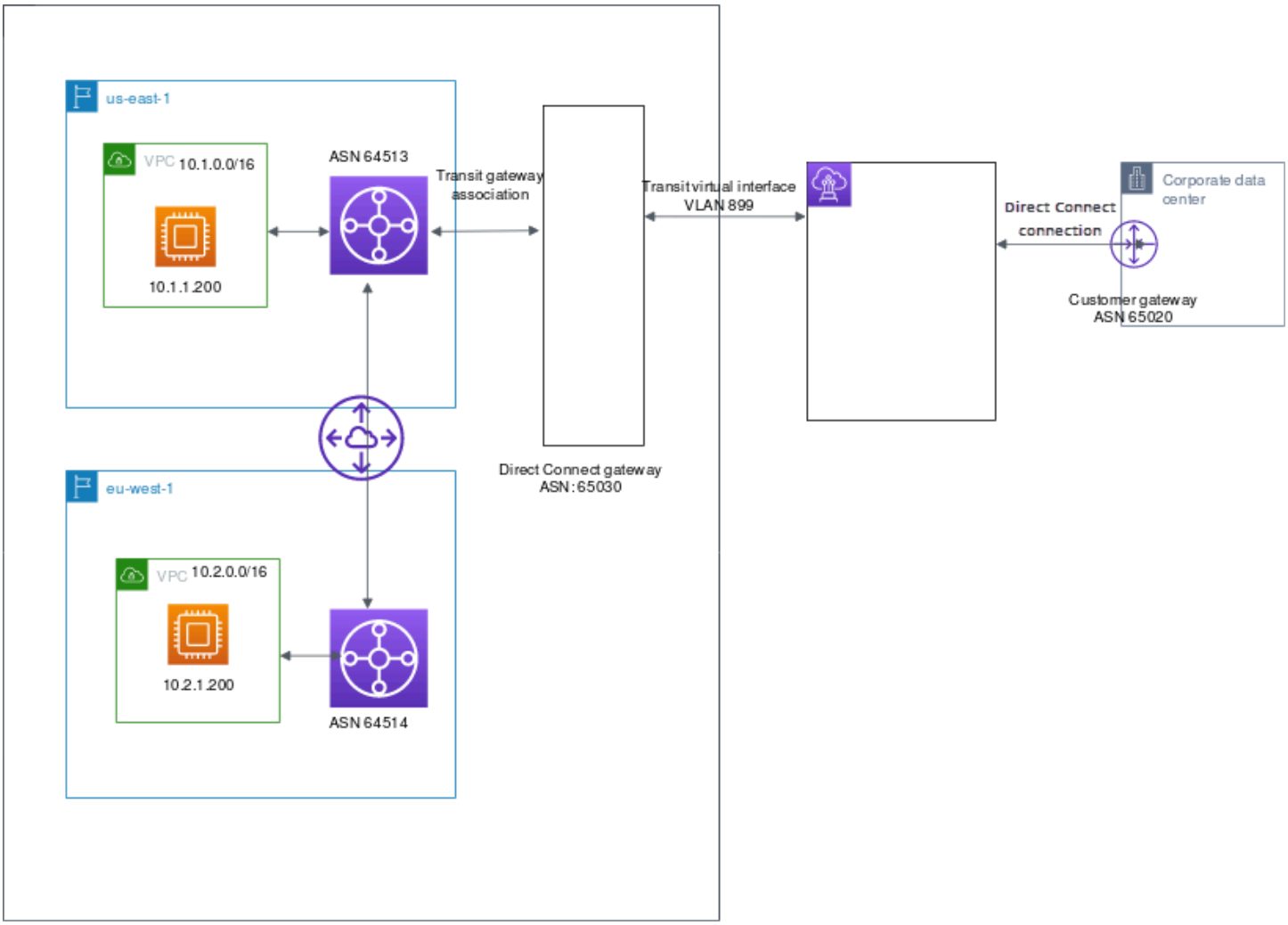
Lorsque vous supprimez ou ajoutez un préfixe autorisé, le trafic qui n'utilise pas ce préfixe n'est pas impacté. Pendant les mises à jour, l'état passe de `associated` à `updating`. La modification d'un préfixe existant ne peut retarder que le trafic qui utilise ce préfixe.

Exemple : autorisé aux préfixes dans une configuration de passerelle de transit

Tenez compte de la configuration dans laquelle vous avez des instances dans deux régions AWS différentes qui ont besoin d'accéder au centre de données de l'entreprise. Vous pouvez utiliser les ressources suivantes pour cette configuration :

- Une passerelle de transit dans chaque région.
- Une connexion d'appairage de passerelle de transit.
- Une passerelle Direct Connect.
- Une association de passerelles de transit entre l'une des passerelles de transit (celle de us-east-1) et la passerelle Direct Connect.

- Une interface virtuelle de transit entre l'emplacement sur site et l'emplacement AWS Direct Connect.



Configurez les options suivantes pour les ressources.

- Passerelle Direct Connect : définissez l'ASN sur 65030. Pour en savoir plus, consultez the section called “Création d'une passerelle Direct Connect”.
- Interface virtuelle de transit : définissez le VLAN sur 899 et l'ASN sur 65020. Pour en savoir plus, consultez the section called “Créer une interface de transit virtuelle vers la passerelle Direct Connect”.
- Association de la passerelles Direct Connect avec la passerelle de transit : définissez les préfixes autorisés sur 10.0.0.0/8.

Ce bloc d'adresse CIDR couvre les deux blocs d'adresse CIDR VPC. Pour en savoir plus, consultez the section called "Association et dissociation de passerelles de transit".

- Route VPC : pour acheminer le trafic depuis le VPC 10.2.0.0, créez une route dans le table de routage VPC dont la destination est 0.0.0.0/0 et l'ID de passerelle de transit comme cible. Pour plus d'informations sur le routage vers une passerelle de transit, veuillez consulter Routage pour une passerelle de transit dans le Guide de l'utilisateur d'Amazon VPC.

Balisage de ressources AWS Direct Connect

Une balise est une étiquette que le propriétaire d'une ressource attribue à ses ressources AWS Direct Connect. Chaque étiquette est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises permettent au propriétaire de ressources de classer ses ressources AWS Direct Connect de différentes manières, par exemple, par objectif ou par environnement. Cela s'avère utile quand il existe un grand nombre de ressources du même type : vous pouvez identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées.

Supposons par exemple que vous avez deux connexions AWS Direct Connect dans une région, chacune dans des emplacements différents. La connexion `dxcon-11aa22bb` traite le trafic de production et est associée à l'interface virtuelle `dxvif-33cc44dd`. La connexion `dxcon-abcabcab` est une connexion redondante (sauvegarde) et est associée à l'interface virtuelle `dxvif-12312312`. Vous pouvez choisir de baliser vos connexions et interfaces virtuelles comme suit, pour les différencier :

ID de ressource	Clé de balise	Valeur de balise
`dxcon-11aa22bb`	Objectif	Production
	Emplacement	Amsterdam
`dxvif-33cc44dd`	Objectif	Production
`dxcon-abcabcab`	Objectif	Sauvegarde
	Emplacement	Francfort
`dxvif-12312312`	Objectif	Sauvegarde

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Les balises n'ont pas de signification sémantique pour AWS Direct Connect et sont interprétées strictement comme des chaînes de caractères. De plus, les étiquettes ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur

null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, les balises associées à celle-ci seront également supprimées.

Vous pouvez baliser les ressources AWS Direct Connect suivantes à l'aide de la console AWS Direct Connect, de l'API AWS Direct Connect, de la AWS CLI, du AWS Tools for Windows PowerShell ou d'un SDK AWS. Lorsque vous utilisez ces outils pour gérer les balises, vous devez spécifier l'Amazon Resource Name (ARN) pour la ressource. Pour de plus amples informations sur l'utilisation des ARN, veuillez consulter Amazon Resource Names (ARN) dans le Référence générale d'Amazon Web Services.

Ressource	Prend en charge les étiquettes	Prend en charge les balises lors de la création	Prend en charge les balises contrôlant l'accès et l'allocation des ressources	Prend en charge la répartition des coûts
Connexions	Oui	Oui	Oui	Oui
Interfaces virtuelles	Oui	Oui	Oui	Non
Groupes d'agrégation de liaisons (LAG)	Oui	Oui	Oui	Oui
Interconnexions	Oui	Oui	Oui	Oui
Passerelles Direct Connect	Non	Non	Non	Non

Restrictions liées aux étiquettes

Les règles et restrictions suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 128 caractères Unicode
- Longueur de valeur maximale : 265 caractères Unicode

- Les clés et valeurs de balise sont sensibles à la casse.
- Le préfixe `aws:` est réservé à l'utilisation d'AWS. Vous ne pouvez pas modifier ou supprimer la clé ou la valeur d'une balise lorsque la balise possède une clé de balise avec le préfixe `aws:`. Les balises avec le préfixe `aws:` ne sont pas comptabilisées comme vos balises pour la limite de ressources.
- Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : / @.
- Seul le propriétaire de la ressource peut ajouter ou supprimer des balises. Par exemple, dans le cas d'une connexion hébergée, le partenaire ne sera pas en mesure d'ajouter, de supprimer ou d'afficher les balises.
- Les balises de répartition des coûts sont uniquement prises en charge pour les connexions, les interconnexions et les groupes d'agrégation de liaisons (LAG). Pour de plus amples informations sur la façon d'utiliser des balises avec la gestion des coûts, veuillez consulter Utilisation des balises de répartition des coûts dans le Guide de l'utilisateur AWS Billing and Cost Management.

Gestion des balises à l'aide de la CLI ou de l'API

Utilisez les commandes suivantes pour ajouter, mettre à jour, répertorier et supprimer les étiquettes pour vos ressources.

Tâche	API	INTERFACE DE LIGNE DE COMMANDE (CLI)
Ajouter ou remplacer une ou plusieurs étiquettes.	TagResource	tag-resource
Supprimer une ou plusieurs étiquettes.	UntagResource	untag-resource
Décrire une ou plusieurs balises.	DescribeTags	describe-tags

Exemples

Utilisez la commande tag-resource pour baliser la connexion `dxcon-11aa22bb`.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Utilisez la commande describe-tags pour décrire les balises de la connexion `dxcon-11aa22bb`.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Utilisez la commande untag-resource pour supprimer une balise d'une connexion `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Sécurité dans AWS Direct Connect

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Direct Connect, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud – Votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Direct Connect. Les rubriques suivantes expliquent comment configurer AWS Direct Connect pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources AWS Direct Connect.

Rubriques

Protection des données dans AWS Direct Connect

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Direct Connect. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que

le champ Name (Nom). Cela est également valable lorsque vous utilisez AWS Direct Connect ou d'autres Services AWS à l'aide de la console, de l'API, d'AWS CLI ou des kits SDK AWS. Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Pour en savoir plus sur la protection des données, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD sur le Blog sur la sécurité d'AWS.

Rubriques

Confidentialité du trafic inter-réseaux dans AWS Direct Connect

Trafic entre les clients de service et sur site et les applications

Vous disposez de deux options de connectivité entre votre réseau privé et AWS:

- Association à un AWS Site-to-Site VPN. Pour de plus amples informations, veuillez consulter the section called "Sécurité de l'infrastructure".
- Association aux VPC. Pour plus d'informations, consultez the section called "Associations de la passerelle privée virtuelle" et the section called "Associations de la passerelle de transit".

Trafic entre des ressources AWS dans la même Région

Deux options de connectivité s'offrent à vous :

- Association à un AWS Site-to-Site VPN. Pour de plus amples informations, veuillez consulter the section called "Sécurité de l'infrastructure".
- Association aux VPC. Pour plus d'informations, consultez the section called "Associations de la passerelle privée virtuelle" et the section called "Associations de la passerelle de transit".

Chiffrement en transit AWS Direct Connect

AWS Direct Connect ne chiffre pas votre trafic en transit par défaut. Pour chiffrer les données en transit qui transitent AWS Direct Connect, vous devez utiliser les options de chiffrement du transit pour ce service. Pour en savoir plus sur le chiffrement du trafic des instances EC2, consultez la section Chiffrement en transit du guide de l'utilisateur Amazon EC2.

Avec AWS Direct Connect et AWS Site-to-Site VPN, vous pouvez combiner une ou plusieurs connexions réseau AWS Direct Connect dédiées avec le VPN Amazon VPC. Cette combinaison fournit une connexion privée à chiffrement IPsec qui réduit également les coûts du réseau, augmente le débit de bande passante et fournit une expérience réseau plus cohérente que les connexions VPN basées sur Internet. Pour plus d'informations, consultez Options de connectivité Amazon VPC vers Amazon VPC.

MAC Security (MACsec) est une norme IEEE qui garantit la confidentialité, l'intégrité des données et l'authenticité de l'origine des données. Vous pouvez utiliser AWS Direct Connect des connexions compatibles MacSec pour chiffrer vos données depuis le centre de données de votre entreprise jusqu'à l' AWS Direct Connect emplacement. Pour plus d'informations, voir Sécurité MAC.

Gestion des identités et des accès pour Direct Connect

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Des administrateurs IAM contrôlent les personnes peuvent être authentifiées (connectées) et autorisées (dotées d'autorisations) à utiliser des ressources Direct Connect. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

Votre utilisation d'AWS Identity and Access Management (IAM) diffère selon la tâche que vous accomplissez dans Direct Connect.

Utilisateur du service – Si vous utilisez le service Direct Connect pour accomplir votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utilisez de fonctions Direct Connect pour accomplir votre travail, plus vous risquez d'avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonction dans Direct Connect, consultez Résolution de problèmes d'identité et d'accès dans Direct Connect.

Administrateur du service – Si vous êtes le responsable des ressources Direct Connect dans votre entreprise, vous bénéficiez probablement d'un accès total à Direct Connect. Votre responsabilité est de déterminer à quelles fonctionnalités et ressources Direct Connect les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Direct Connect, consultez Comment Direct Connect fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez probablement en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à Direct Connect. Pour voir des exemples de politiques basées sur une identité pour Direct Connect que vous pouvez utiliser dans IAM, consultez Exemples de politiques basées sur une identité pour Direct Connect.

Authentification par des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail d'accès AWS. Pour plus d'informations sur la connexion à AWS, consultez Connexion à votre Compte AWSdans le Guide de l'utilisateurConnexion à AWS.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des demandes d'API AWS dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Utilisateur root Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, l'AWS Directory Service, l'annuaire Identity Centerou tout utilisateur qui accède à Services AWS en utilisant des informations d'identification fournies via une source d'identité. Quand

des identités fédérées accèdent à Comptes AWS, elles endossent des rôles, ces derniers fournissant des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications et de vos Comptes AWS. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou

AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center.
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès interservices : certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.
  - Transmission de séances d'accès (FAS) – Lorsque vous vous servez d'un utilisateur ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées à Service AWS qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer

d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section séances d'accès transmises.

- Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié au service – Un rôle lié au service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou séance de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées par. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez attacher à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent les politiques gérées par AWS et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courantes. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- politiques de contrôle des services (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans

les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.

- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, veuillez consulter Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Comment Direct Connect fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Direct Connect, découvrez les fonctions IAM que vous pouvez utiliser avec Direct Connect.

Fonctions IAM que vous pouvez utiliser avec Direct Connect

Fonction IAM	Support Direct Connect
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non

Fonction IAM	Support Direct Connect
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Direct Connect et d'autres services AWS fonctionnent avec IAM, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Direct Connect

Prend en charge les politiques basées sur une identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un Groupes d'utilisateurs IAM ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, veuillez consulter Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur une identité pour Direct Connect

Pour voir des exemples de politiques basées sur une identité pour Direct Connect, consultez Exemples de politiques basées sur une identité pour Direct Connect.

Politiques basées sur une ressource dans Direct Connect

Prend en charge les politiques basées sur une ressource	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le principal et la ressource se trouvent dans des Comptes AWS différents, un administrateur IAM dans le compte approuvé doit également accorder à l'entité principal (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions de politique pour Direct Connect

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de politique possèdent généralement le même nom

que l'opération d'API AWS associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Direct Connect, voir Actions définies par Direct Connect dans la référence d'autorisation de service.

Les actions de politique dans Direct Connect utilisent le préfixe suivant avant l'action :

```
Direct Connect
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Ressources relatives aux politiques pour Direct Connect

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour afficher la liste des types de ressource Direct Connect et leurs ARN, veuillez consulter Ressources définies par Direct Connect dans la Référence de l'API AWS Direct Connect. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Direct Connect.

Pour voir des exemples de politiques basées sur une identité pour Direct Connect, consultez Exemples de politiques basées sur une identité pour Direct Connect.

Pour voir des exemples de politiques basées sur les ressources Direct Connect, consultez Exemples de politique basée sur l'identité Direct Connect utilisant des conditions basées sur des balises.

Clés de condition de politique pour Direct Connect

Prise en charge des clés de condition de stratégie spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Pour afficher une liste des clés de condition Direct Connect, consultez la section Clés de condition pour Direct Connect dans la Référence de l'API AWS Direct Connect. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions, ressources et clés de condition pour Direct Connect dans la référence d'autorisation de service.

Pour voir des exemples de politiques basées sur une identité pour Direct Connect, consultez Exemples de politiques basées sur une identité pour Direct Connect.

ACL dans Direct Connect

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Direct Connect

Prend en charge ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés étiquettes. Vous pouvez attacher des étiquettes à des entités IAM (utilisateurs ou rôles), ainsi qu'à de nombreuses ressources AWS. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balise dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Direct Connect

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les Services AWS qui fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires quand vous vous connectez à la AWS Management Console en utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide d'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations de principals entre services pour Direct Connect

Prend en charge les transmissions de sessions d'accès (FAS)	Oui

Lorsque vous vous servez d'un utilisateur IAM ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées à Service AWS qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section séances d'accès transmises.

Rôles de service pour Direct Connect

Prend en charge les fonctions du service	Oui

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'un rôle de service peut altérer la fonctionnalité de Direct Connect. Ne modifiez des rôles de service que quand Direct Connect vous le conseille.

Rôles liés à un service pour Direct Connect

Prend en charge les rôles liés à un service.	Non

Un rôle lié à un service est un type de rôle de service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Service-linked role (Rôle lié à un service). Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur une identité pour Direct Connect

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ni à modifier des ressources Direct Connect. Ils ne peuvent pas non plus exécuter des tâches à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Direct Connect, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Direct Connect dans la Référence de l'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Actions, ressources et clés de conditions Direct Connect
- Utilisation de la console Direct Connect
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès en lecture seule à AWS Direct Connect
- Accès complet à AWS Direct Connect
- Exemples de politique basée sur l'identité Direct Connect utilisant des conditions basées sur des balises

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Direct Connect dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Démarrer avec AWS gérées et évoluez vers les autorisations de moindre privilège - Pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées AWS qui accordent des autorisations dans de nombreux cas d'utilisation courants. Elles sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques AWS gérées par le client qui sont spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées via un Service AWS spécifique, comme AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Authentification multifactorielle (MFA) nécessaire : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans votre Compte AWS, activez l'authentification

multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Actions, ressources et clés de conditions Direct Connect

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Direct Connect prend en charge des actions, ressources et clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, veuillez consulter Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de politique possèdent généralement le même nom que l'opération d'API AWS associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique dans Direct Connect utilisent le préfixe suivant avant l'action : `directconnect:`. Par exemple, pour accorder à une personne l'autorisation d'exécuter une instance Amazon EC2 avec l'opération d'API `DescribeVpnGateways` Amazon EC2, vous incluez l'action `ec2:DescribeVpnGateways` dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Direct Connect définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

L'exemple de stratégie suivant accorde l'accès en lecture à AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

L'exemple de stratégie suivant accorde l'accès complet à AWS Direct Connect.

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

Pour consulter une liste des actions Direct Connect, consultez la section Actions définies par Direct Connect dans le Guide de l'utilisateur IAM.

Ressources

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions

qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Direct Connect utilise les ARN suivants :

ARN de ressource Direct Connect

Type de ressource	ARN
dxconn	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Pour plus d'informations sur le format des ARN, consultez Amazon Resource Names (ARNs) et Espaces de noms du service AWS.

Par exemple, pour spécifier l'interface `dxcon-11aa22bb` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Pour spécifier toues les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Certaines actions Direct Connect, telles que la création de ressources, ne peuvent pas être exécutées sur une ressource précise. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour afficher la liste des types de ressources Direct Connect et leurs ARN, veuillez consulter Types de ressources définis par AWS Direct Connect dans le Guide de l'utilisateur IAM. Pour en savoir plus sur les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez SERVICE-ACTIONS-URL ;.

Clés de condition

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Direct Connect définit son propre ensemble de clés de condition et prend également en charge l'utilisation des clés de condition globales. Pour afficher toutes les clés de condition globales AWS, veuillez consulter la rubrique Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Vous pouvez utiliser les clés de condition avec la ressource de balise. Pour de plus amples informations, veuillez consulter Exemple : Restriction de l'accès à une région spécifique.

Pour afficher une liste des clés de condition Direct Connect, consultez la section Clés de condition pour Direct Connect dans le Guide de l'utilisateur IAM. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez SERVICE-ACTIONS-URL ;.

Utilisation de la console Direct Connect

Pour accéder à la console Direct Connect, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Direct Connect de votre compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (ou rôles) tributaires de cette stratégie.

Pour garantir que ces entités pourront continuer à utiliser la console Direct Connect, attachez également aux entités la stratégie suivante gérée par AWS. Pour en savoir plus, consultez Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

```
directconnect
```

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à l'interface AWS CLI ou API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API AWS.

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

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès en lecture seule à AWS Direct Connect

L'exemple de stratégie suivant accorde l'accès en lecture à AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
```

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

Accès complet à AWS Direct Connect

L'exemple de stratégie suivant accorde l'accès complet à AWS Direct Connect.

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

Exemples de politique basée sur l'identité Direct Connect utilisant des conditions basées sur des balises

Vous pouvez contrôler l'accès aux ressources et aux demandes en utilisant des conditions de clé de balise. Vous pouvez également utiliser une condition dans votre stratégies IAM pour contrôler si des clés de balise spécifiques peuvent être utilisées sur une ressource ou dans une demande.

Pour plus d'informations sur la façon d'utiliser des balises avec les politiques IAM, veuillez consulter Contrôle de l'accès à l'aide de balises dans le Guide de l'utilisateur IAM.

Association d'interfaces virtuelles Direct Connect basées sur des balises

L'exemple suivant montre comment créer une stratégie autorisant l'association d'une interface virtuelle uniquement si la balise contient la clé d'environnement et les valeurs preprod ou production.

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

```
        {
          "Effect": "Allow",
          "Action": [
            "directconnect:AssociateVirtualInterface"
          ],
          "Resource": "arn:aws:directconnect:*:*:dxvif/*",
          "Condition": {
            "StringEquals": {
              "aws:ResourceTag/environment": [
                "preprod",
                "production"
              ]
            }
          }
        },
        {
          "Effect": "Allow",
          "Action": "directconnect:DescribeVirtualInterfaces",
          "Resource": "*"
        }
      ]
    }
```

Contrôle de l'accès aux demandes en fonction des balises

Vous pouvez utiliser des conditions dans vos politiques IAM pour contrôler quelles paires clé-valeur de balise peuvent être transmises dans une demande qui balise une ressource AWS. L'exemple suivant montre comment créer une politique qui permet d'utiliser l'AWS Direct Connect TagResource action pour attacher des balises à une interface virtuelle uniquement si la balise contient la clé d'environnement et les valeurs de préproduction ou de production. En tant que bonne pratique, utilisez le modificateur `ForAllValues` avec la clé de condition `aws:TagKeys` pour indiquer que seule la clé environment est autorisée dans la demande.

```
    {
        "Version": "2012-10-17",
        "Statement": {
            "Effect": "Allow",
            "Action": "directconnect:TagResource",
            "Resource": "arn:aws:directconnect:*:*:dxvif/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": [
```

```
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

Contrôle des clés de balise

Vous pouvez utiliser une condition dans vos politiques IAM pour contrôler si des clés de balise spécifiques peuvent être utilisées sur une ressource ou dans une demande.

L'exemple suivant montre comment créer une stratégie vous permettant de baliser des ressources, mais uniquement celles contenant la clé de balise environment.

```
 {
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "environment"
        ]
      }
    }
  }
}
```

Rôles liés à un service pour AWS Direct Connect

AWS Direct Connect utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Direct Connect. Les rôles liés à un service sont prédéfinis par AWS Direct Connect et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service permet d'utiliser AWS Direct Connect plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS Direct Connect définit les

autorisations de ses rôles liés à un service et, sauf définition contraire, seul AWS Direct Connect peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources AWS Direct Connect sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS Direct Connect

AWS Direct Connect utilise le rôle lié à un service nommé `AWSServiceRoleForDirectConnect`. Cela permet à AWS Direct Connect de récupérer les secrets MACsec stockés dans AWS Secrets Manager en votre nom.

Le rôle lié à un service `AWSServiceRoleForDirectConnect` approuve les services suivants pour endosser le rôle :

- `directconnect.amazonaws.com`

Le rôle lié à un service `AWSServiceRoleForDirectConnect` utilise la stratégie gérée par `AWSDirectConnectServiceRolePolicy`.

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 que la création du rôle lié au service `AWSServiceRoleForDirectConnect` réussisse, l'identité IAM avec laquelle vous utilisez AWS Direct Connect doit disposer des autorisations requises. Pour accorder les autorisations requises, associez la stratégie suivante à l'identité IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Direct Connect

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. AWS Direct Connect crée pour vous le rôle lié à un service pour vous. Lorsque vous exécutez la commande `associate-mac-sec-key`, AWS crée un rôle lié à un service qui permet à AWS Direct Connect de récupérer les secrets MACsec stockés dans AWS Secrets Manager en votre nom dans la AWS Management Console, l'AWS CLI ou l'APIAWS.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous devez ensuite le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. AWS Direct Connect crée à nouveau le rôle lié à un service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation AWS Direct Connect. Dans l'interface AWS CLI ou l'API AWS, créez un rôle lié à un service avec le nom de service `directconnect.amazonaws.com`. Pour de plus amples informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous

supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Direct Connect

AWS Direct Connect ne vous permet pas de modifier le rôle lié à un service `AWSServiceRoleForDirectConnect`. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Direct Connect

Vous n'avez pas besoin de supprimer manuellement le rôle `AWSServiceRoleForDirectConnect`. Lorsque vous supprimez votre rôle lié à un service, vous devez supprimer toutes les ressources associées stockées dans le service web AWS Secrets Manager. La AWS Management Console, l'AWS CLI ou l'API AWS, AWS Direct Connect nettoie les ressources et supprime le rôle lié à un service à votre place.

Vous pouvez également utiliser la console IAM pour supprimer le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle.

> **Note**
>
> Si le service AWS Direct Connect utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, attendez quelques minutes, puis réessayez l'opération.

Pour supprimer les ressources AWS Direct Connect utilisées par le service **`AWSServiceRoleForDirectConnect`**

1. Supprimer l'association entre toutes les clés MACsec et les connexions. Pour plus d'informations, consultez the section called "Supprimer l'association entre une connexion et une clé secrète MACsec".
2. Supprimer l'association entre toutes les clés MACsec et les LAG. Pour plus d'informations, consultez the section called "Supprimer l'association entre un LAG et une clé secrète MACsec".

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service `AWSServiceRoleForDirectConnect`. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Direct Connect

AWS Direct Connect prend en charge l'utilisation des rôles liés à un service dans toutes les Régions AWS où la fonctionnalité de sécurité MAC est disponible. Pour plus d'informations, consultez Emplacements AWS Direct Connect.

Politiques AWS gérées pour AWS Direct Connect

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou lorsque de nouvelles opérations API deviennent accessibles pour les services existants.

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

AWSpolitique gérée : AWSDirectConnectFullAccess

Vous pouvez associer la politique `AWSDirectConnectFullAccess` à vos identités IAM. Cette stratégie accorde des autorisations qui permettent un accès complet à AWS Direct Connect.

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectFullAccess dans AWS Management Console.

AWSpolitique gérée : AWSDirectConnectReadOnlyAccess

Vous pouvez associer la politique `AWSDirectConnectReadOnlyAccess` à vos identités IAM. Cette stratégie accorde des autorisations qui permettent d'accéder en lecture seule à AWS Direct Connect.

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectReadOnlyAccess dans AWS Management Console.

AWSpolitique gérée : AWSDirectConnectServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé AWSServiceRoleForDirectConnectpour permettre de récupérer les secrets AWS Direct Connect de sécurité MAC en votre nom. Pour en savoir plus, consultez the section called “Rôles liés à un service”.

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectServiceRolePolicy dans AWS Management Console.

Mises à jour AWS Direct Connect vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS Direct Connect depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document AWS Direct Connect.

Modification	Description	Date
AWSDirectConnectServiceRolePolicy : nouvelle politique	Pour prendre en charge la sécurité MAC, le rôle AWSServiceRoleForDirectConnectlié au service a été ajouté.	31 mars 2021
AWS Direct Connect a démarré le suivi des modifications	AWS Direct Connect a commencé à suivre les modifications pour ses stratégies gérées par AWS.	31 mars 2021

Résolution de problèmes d'identité et d'accès dans Direct Connect

Pour identifier et résoudre des problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Direct Connect et IAM, utilisez les informations ci-après.

Rubriques

Je ne suis pas autorisé à effectuer une action dans Direct Connect

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `directconnect:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `directconnect:`*`GetWidget`*.

Si vous avez encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur selon lequel vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos stratégies doivent être mises à jour pour vous permettre de transmettre un rôle à Direct Connect.

Certains Services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer une nouvelle fonction du service ou rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'erreur suivante se produit quand un utilisateur IAM nommé `marymajor` tente d'utiliser la console pour exécuter une action dans Direct Connect. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

Je veux autoriser des personnes extérieures à mon Compte AWS à accéder à mes ressources Direct Connect

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Direct Connect prend en charge ces fonctions, consultez Comment Direct Connect fonctionne avec IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, consultez la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des tiers Comptes AWS, consultez Fournir l'accès aux Comptes AWS appartenant à des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Journalisation et surveillance dans AWS Direct Connect

Vous pouvez utiliser les outils de surveillance automatique pour surveiller AWS Direct Connect et signaler en cas de problème :

- Alarmes Amazon CloudWatch – Surveillez une métrique unique sur une période donnée que vous spécifiez. Réalise une ou plusieurs actions en fonction de la valeur de la métrique, par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS. Les alarmes CloudWatch n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier : l'état doit avoir changé et été maintenu pendant un certain nombre de périodes. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon CloudWatch.
- Surveillance des journaux AWS CloudTrail – Partagez des fichiers journaux entre les comptes et surveillez les fichiers journaux CloudTrail en temps réel en les envoyant aux journaux CloudWatch. Vous pouvez également écrire des applications de traitement des journaux en Java et vous assurer que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour en savoir plus, veuillez consulter Journalisation des appels d'API AWS Direct Connect avec AWS CloudTrail et Utilisation des fichiers journaux CloudTrail dans le Guide de l'utilisateur AWS CloudTrail.

Pour de plus amples informations, veuillez consulter Surveillance.

Validation de conformité pour AWS Direct Connect

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Direct Connect

L'infrastructure mondiale d'AWS repose sur les Régions AWS et les zones de disponibilité AWS. Les Régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez AWS Infrastructure mondiale.

Outre l'infrastructure globale AWS, AWS Direct Connect propose plusieurs fonctionnalités qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

Pour plus d'informations sur l'utilisation d'un VPN avec AWS Direct Connect, consultez AWS Direct Connect Plus VPN.

Basculement

La Boîte à outils de résilience AWS Direct Connect fournit un assistant de connexion avec plusieurs modèles de résilience qui vous aide à commander des connexions dédiées pour atteindre votre objectif en matière de SLA. Vous sélectionnez un modèle de résilience, puis la Boîte à outils de résilience AWS Direct Connect vous guide lors du processus de commande de connexion dédiée. Les modèles de résilience sont conçus pour vous assurer de disposer du nombre approprié de connexions dédiées dans plusieurs emplacements.

- Résilience maximale : vous pouvez obtenir une résilience maximale pour les charges de travail critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans plusieurs emplacements. Ce modèle offre une résilience contre les défaillances de l'appareil, de la connectivité et de l'emplacement complet.
- Haute résilience: vous pouvez obtenir une haute résilience pour les charges de travail critiques en utilisant deux connexions simples à plusieurs emplacements. Ce modèle offre une résilience contre les défaillances de connectivité provoquées par une coupure de fibre ou une défaillance d'appareil. Cela permet également d'éviter une défaillance complète de l'emplacement.

- Développement et test : vous pouvez obtenir une résilience de développement et de test pour les charges de travail non critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans un seul emplacement. Ce modèle offre une résilience contre les défaillances de l'appareil, mais n'assure pas la résilience contre les défaillances de l'emplacement.

Pour de plus amples informations, veuillez consulter Utiliser le AWS Direct Connect Resiliency Toolkit pour démarrer.

Sécurité de l'infrastructure dans AWS Direct Connect

En tant que service géré, AWS Direct Connect est protégé par les procédures de sécurité du réseau mondial AWS. Vous utilisez les appels d'API publiés AWS pour accéder à AWS Direct Connect via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Nous recommandons TLS 1.3. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Vous pouvez appeler ces opérations d'API à partir de n'importe quel emplacement sur le réseau, mais AWS Direct Connect prend en charge les stratégies d'accès basées sur les ressources, ce qui peut inclure des restrictions en fonction de l'adresse IP source. Vous pouvez également utiliser des politiques AWS Direct Connect pour contrôler l'accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou de VPC spécifiques. En effet, cela permet d'isoler l'accès réseau vers une ressource AWS Direct Connect donnée depuis le VPC spécifique uniquement au sein du réseau AWS. Pour obtenir un exemple, consultez the section called “Exemples de politiques basées sur l’identité”.

Sécurité protocole de passerelle frontière (BGP)

L'Internet s'appuie en grande partie sur le protocole BGP pour acheminer les informations entre les systèmes du réseau. Le routage BGP peut parfois être exposé à des attaques malveillantes ou à un détournement BGP. Pour comprendre comment AWS protége votre réseau de manière plus

sécurisée contre le détournement BGP, consultez Comment AWS contribue à sécuriser le routage Internet.

Utilisation de AWS CLI

Vous pouvez utiliser AWS CLI pour créer et travailler avec des ressources AWS Direct Connect.

L'exemple suivant utilise les commandes de l'AWS CLI pour créer une connexion AWS Direct Connect. Vous pouvez également télécharger la Lettre d'autorisation - Affectation d'installation de connexion (LOA-CFA) et mettre en service une interface virtuelle privée ou publique.

Avant de commencer, veillez à avoir installer et configurer l'AWS CLI. Pour plus d'informations, consultez le AWS Command Line InterfaceGuide de l'utilisateur .

Table des matières

Étape 1 : Créer une connexion

La première étape consiste à envoyer une demande de connexion. Veillez à connaître la vitesse du port requise et l'emplacement AWS Direct Connect. Pour de plus amples informations, veuillez consulter AWS Direct Connect connexions.

Pour créer une demande de connexion

1. Décrivez les emplacements AWS Direct Connect pour votre région actuelle. Dans le résultat renvoyé, notez le code de l'emplacement pour l'emplacement dans lequel vous souhaitez établir la connexion.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
```

```
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
    ]
}
```

2. Créez la connexion et indiquez le nom, la vitesse du port et le code de l'emplacement. Dans le résultat renvoyé, notez l'ID de connexion. Vous avez besoin de l'ID pour récupérer la LOA-CFA dans l'étape suivante.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Étape 2 : Télécharger la LOA-CFA

Une fois la demande de connexion effectuée, vous pouvez récupérer la LOA-CFA à l'aide de la commande `describe-loa`. Le résultat est codé en base64. Vous devez extraire le contenu LOA pertinent, le décoder et créer un fichier PDF.

Pour récupérer la LOA-CFA à l'aide de Linux ou de macOS

Dans cet exemple, la dernière partie de la commande décode le contenu à l'aide de l'utilitaire en base64 et envoie le résultat vers un fichier PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Pour récupérer la LOA-CFA à l'aide de Windows

Dans cet exemple, le résultat est extrait vers un fichier appelé myLoaCfa.base64. La deuxième commande utilise l'utilitaire `certutil` pour décoder le fichier et envoyer le résultat vers un fichier PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Une fois la LOA-CFA téléchargée, envoyez-la à votre fournisseur de réseau ou de colocalisation.

Étape 3 : Créer une interface virtuelle et récupérer la configuration du routeur

Après avoir commandé une connexion AWS Direct Connect, vous devez créer une interface virtuelle pour pouvoir l'utiliser. Vous pouvez créer une interface virtuelle privée pour vous connecter à votre VPC. Ou vous pouvez créer une interface virtuelle publique pour vous connecter aux services AWS extérieurs au VPC. Vous pouvez créer une interface virtuelle qui prend en charge le trafic IPv4 ou IPv6.

Avant de commencer, veillez à prendre connaissance des conditions préalables dans Conditions préalables pour les interfaces virtuelles.

Lorsque vous créez une interface virtuelle à l'aide d'AWS CLI, le résultat inclut des informations générique sur la configuration du routeur. Pour créer une configuration du routeur propre à votre appareil, utilisez la console AWS Direct Connect. Pour de plus amples informations, veuillez consulter Télécharger le fichier de configuration du routeur.

Pour créer une interface virtuelle privée

1. Récupérez l'ID de la passerelle réseau privé virtuel (vgw-xxxxxxxx) attachée à votre VPC. Vous avez besoin de l'ID pour créer l'interface virtuelle dans l'étape suivante.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
   ```

```
            "State": "available",
            "Tags": [
                {
                    "Value": "DX_VGW",
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Créez une interface virtuelle privée. Vous devez spécifier un nom, un ID VLAN et un numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol).

   Pour le trafic IPv4, vous avez besoin d'adresses IPv4 privées pour chaque fin de la session d'appairage BGP. Vous pouvez spécifier vos propres adresses IPv4 ou laisser Amazon les générer pour vous. Dans l'exemple suivant, les adresses IPv4 sont générées pour vous.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
```

```
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

Pour créer une interface virtuelle privée prenant en charge le trafic IPv6, utilisez la même commande ci-dessus et spécifiez `ipv6` pour le paramètre `addressFamily`. Vous ne pouvez pas spécifier vos propres adresses IPv6 pour la session d'appairage BGP ; Amazon vous attribue des adresses IPv6.

3. Pour afficher les informations de configuration du routeur au format XML, décrivez l'interface virtuelle que vous avez créée. Utilisez le paramètre `--query` pour extraire les informations `customerRouterConfig` et le paramètre `--output` pour organiser le texte en lignes délimitées par des tabulations.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
```

```
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

Pour créer une interface virtuelle publique

1. Pour créer une interface virtuelle publique, vous devez spécifier un nom, un ID VLAN et un numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol).

   Pour le trafic IPv4, vous devez également spécifier des adresses IPv4 publiques pour chaque fin de la session d'appairage BGP et des routes IPv4 publiques que vous publiez sur BGP. L'exemple suivant crée une interface virtuelle publique pour le trafic IPv4.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
```

```
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Pour créer une interface virtuelle publique prenant en charge le trafic IPv6, vous pouvez spécifier les routes IPv6 que vous publierez sur BGP. Vous ne pouvez pas spécifier d'adresses IPv6 pour la session d'appairage ; Amazon vous les attribue. L'exemple suivant crée une interface virtuelle publique pour le trafic IPv6.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. Pour afficher les informations de configuration du routeur au format XML, décrivez l'interface virtuelle que vous avez créée. Utilisez le paramètre `--query` pour extraire les informations `customerRouterConfig` et le paramètre `--output` pour organiser le texte en lignes délimitées par des tabulations.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Journalisation des appels d'API AWS Direct Connect avec AWS CloudTrail

AWS Direct Connect est intégré avec ,AWS CloudTrail un service qui fournit un registre des actions prises par un utilisateur, un rôle ou un service AWS dans AWS Direct Connect. CloudTrail capture les appels d'API vers AWS Direct Connect en tant qu'événements. Les appels capturés incluent des appels de la console AWS Direct Connect et les appels de code vers les opérations d'API AWS Direct Connect. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour AWS Direct Connect. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). En utilisant les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS Direct Connect, l'adresse IP, l'auteur et la date de la demande, ainsi que d'autres détails.

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

AWS Direct Connect Informations dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de sa création. Lorsqu'une activité a lieu dans AWS Direct Connect, cette activité est enregistrée dans un événement CloudTrail avec d'autres AWS événements de service dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS Direct Connect, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Amazon S3 bucket. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail

- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception des fichiers journaux CloudTrail de plusieurs régions et Réception des fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions AWS Direct Connect sont consignées par CloudTrail et documentées dans la Référence des API AWS Direct Connect. À titre d'exemple, les appels vers les actions `CreateConnection` et `CreatePrivateVirtualInterface` génèrent des entrées dans les fichiers journaux CloudTrail.

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 les informations d'identification utilisateur racine ou AWS Identity and Access Management (utilisateur 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.

Pour en savoir plus, consultez l'élément CloudTrail `userIdentity`.

Présentation des AWS Direct Connect entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer les événements dans des fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

Voici des exemples d'enregistrements de journal CloudTrail pour AWS Direct Connect.

Example Exemple : CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
```

```
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Exemple : CreatePrivateVirtualInterface

```
{
    "Records": [
    {
```

```
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
```

```
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example Exemple : DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example Exemple : DescribeVirtualInterfaces


```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

AWS Direct Connect Ressources de surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos ressources Direct Connect. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Avant de commencer à surveiller Direct Connect, vous devez toutefois créer un plan de surveillance comprenant des réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles ressources doivent être surveillées ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de surveillance ?
- Qui doit être informé en cas de problème ?

L'étape suivante consiste à établir une base de référence pour les performances normales de Direct Connect dans votre environnement, en mesurant les performances à différents moments et dans différentes conditions de charge. Lorsque vous surveillez Direct Connect, stockez les données de surveillance historiques. Vous pouvez ainsi les comparer avec les données de performances actuelles, identifier des modèles de performances normales et des anomalies de performances, ainsi que concevoir des méthodes pour les résoudre.

Pour établir une base de référence, vous devez surveiller l'utilisation, l'état et l'état de vos connexions physiques Direct Connect.

Table des matières

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller une AWS Direct Connect connexion. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique suivants pour surveiller Direct Connect et signaler tout problème :

- Amazon CloudWatch Alarms — Surveillez une seule métrique sur une période que vous spécifiez. Réalise une ou plusieurs actions en fonction de la valeur de la métrique, par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour plus d'informations sur les métriques et les dimensions disponibles, consultez Surveillance avec Amazon CloudWatch.
- AWS CloudTrail Surveillance des journaux : partagez les fichiers journaux entre les comptes et surveillez les fichiers CloudTrail journaux en temps réel en les envoyant à CloudWatch Logs. Vous pouvez également écrire des applications de traitement des journaux en Java et vous assurer que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour plus d'informations, reportez-vous à Journalisation des appels d'API AWS Direct Connect avec AWS CloudTrail la section Utilisation des fichiers CloudTrail journaux dans le Guide de AWS CloudTrail l'utilisateur.

Outils de surveillance manuelle

Un autre élément important de la surveillance d'une AWS Direct Connect connexion consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes. Le Direct Connect et les tableaux de bord de CloudWatch la console fournissent une at-a-glance vue d'ensemble de l'état de votre AWS environnement.

- La AWS Direct Connect console affiche :
  - L'état de la connexion (voir la colonne État)
  - L'état de l'interface virtuelle (voir la colonne État)
- La page d' CloudWatch accueil indique :
  - Alarmes et statuts en cours
  - Graphiques des alarmes et des ressources
  - Statut d'intégrité du service

  En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :
  - Créer des tableaux de bord personnalisés pour surveiller les services de votre choix

- Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
- Recherchez et parcourez tous les indicateurs de vos AWS ressources.
- Créer et Modifier des alarmes pour être informé des problèmes.

Surveillance avec Amazon CloudWatch

Vous pouvez surveiller les AWS Direct Connect connexions physiques et les interfaces virtuelles à l'aide de CloudWatch. CloudWatch collecte des données brutes à partir de Direct Connect et les transforme en indicateurs lisibles. Par défaut, CloudWatch fournit les données métriques Direct Connect à intervalles de 5 minutes.

Pour obtenir des informations détaillées à ce sujet CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon. Vous pouvez également surveiller vos services CloudWatch pour voir ceux qui utilisent des ressources. Pour plus d'informations, consultez la section AWS Services qui publient CloudWatch des métriques.

Table des matières

AWS Direct Connect métriques et dimensions

Des métriques sont disponibles pour les connexions AWS Direct Connect physiques et les interfaces virtuelles.

AWS Direct Connect Métriques de connexion

Les mesures suivantes sont disponibles à partir des connexions dédiées Direct Connect.

Métrique	Description
`ConnectionState`	État de la connexion. 1 signifie active et 0 signifie inactive. Cette métrique est disponible pour les connexions dédiées et hébergées.

Métrique	Description
	Note Cette métrique est également disponible dans les comptes du propriétaire de l'interface virtuelle hébergée en plus des comptes du propriétaire de la connexion. Unités : booléennes
`ConnectionBpsEgress`	Débit pour les données sortantes du AWS côté de la connexion. Le nombre communiqué représente l'agrégation (moyenne) sur la période de temps spécifiée (5 minutes par défaut, 1 minute au minimum). Vous pouvez modifier l'agrégation par défaut. Cette métrique peut être indisponible pour une nouvelle connexion ou lors du redémarrage d'un périphérique. La métrique se déclenche lorsque la connexion est utilisée pour envoyer ou recevoir du trafic. Unités : bits par seconde
`ConnectionBpsIngress`	Débit pour les données entrantes du AWS côté de la connexion. Cette métrique peut être indisponible pour une nouvelle connexion ou lors du redémarrage d'un périphérique. La métrique se déclenche lorsque la connexion est utilisée pour envoyer ou recevoir du trafic. Unités : bits par seconde

Métrique	Description
`ConnectionPpsEgress`	Débit de paquets pour les données sortantes du AWS côté de la connexion. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut, 1 minute au minimum). Vous pouvez modifier l'agrégation par défaut. Cette métrique peut être indisponible pour une nouvelle connexion ou lors du redémarrage d'un périphérique. La métrique se déclenche lorsque la connexion est utilisée pour envoyer ou recevoir du trafic. Unités : paquets par seconde
`ConnectionPpsIngress`	Débit de paquets pour les données entrantes du AWS côté de la connexion. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut, 1 minute au minimum). Vous pouvez modifier l'agrégation par défaut. Cette métrique peut être indisponible pour une nouvelle connexion ou lors du redémarrage d'un périphérique. La métrique se déclenche lorsque la connexion est utilisée pour envoyer ou recevoir du trafic. Unités : paquets par seconde
`ConnectionCRCErrorCount`	Ce nombre n'est plus utilisé. Utilisez `ConnectionErrorCount` à la place.

Métrique	Description
`ConnectionErrorCount`	Nombre total d'erreurs pour tous les types d'erreur de niveau MAC sur le périphérique AWS . Le total comprend les erreurs de contrôle de redondance cyclique (CRC). Cette métrique est le nombre d'erreurs survenues depuis le dernier point de données signalé. En cas d'erreur sur l'interface, la métrique indique des valeurs différentes de zéro. Pour obtenir le nombre total d'erreurs pour l'intervalle sélectionné en 5 minutes CloudWatch, par exemple, appliquez la statistique « somme ». Pour plus d'informations sur l'obtention des statistiques de somme, consultez Getting Statistics for a Metric dans le guide de l' CloudWatch utilisateur Amazon. La valeur de la métrique est définie sur 0 lorsque les erreurs sur l'interface cessent. **Note** Cette métrique remplace `ConnectionCRCErrorCount` , qui n'est plus utilisé. Unités : nombre

Métrique	Description
`ConnectionLightLevelTx`	Indique l'état de la connexion par fibre optique pour le trafic sortant (de sortie) provenant du AWS côté de la connexion. Il existe deux dimensions pour cette métrique. Pour de plus amples informations, veuillez consulter the section called "AWS Direct Connect dimensions disponibles". Unités : dBm
`ConnectionLightLevelRx`	Indique l'état de la connexion par fibre optique pour le trafic entrant (entrant) du AWS côté de la connexion. Il existe deux dimensions pour cette métrique. Pour de plus amples informations, veuillez consulter the section called "AWS Direct Connect dimensions disponibles". Unités : dBm
`ConnectionEncryptionState`	Indique l'état du chiffrement de la connexion. 1 indique que le chiffrement de la connexion est `up` et 0 indique que le chiffrement de la connexion est `down`. Lorsque cette métrique est appliquée à un LAG, 1 indique que toutes les connexions du LAG sont chiffrées `up`. 0 indique qu'au moins une connexion LAG est chiffrée `down`.

AWS Direct Connect métriques d'interface virtuelle

Les métriques suivantes sont disponibles à partir des interfaces AWS Direct Connect virtuelles.

Métrique	Description
`VirtualInterfaceBpsEgress`	Débit pour les données sortantes depuis le AWS côté de l'interface virtuelle. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut). Unités : bits par seconde
`VirtualInterfaceBpsIngress`	Débit pour les données entrantes sur le AWS côté de l'interface virtuelle. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut). Unités : bits par seconde
`VirtualInterfacePpsEgress`	Débit de paquets pour les données sortantes depuis le AWS côté de l'interface virtuelle. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut). Unités : paquets par seconde
`VirtualInterfacePpsIngress`	Débit de paquets pour les données entrantes sur le AWS côté de l'interface virtuelle. Le nombre communiqué représente l'agrégat ion (moyenne) sur la période de temps spécifiée (5 minutes par défaut). Unités : paquets par seconde

AWS Direct Connect dimensions disponibles

Vous pouvez filtrer les AWS Direct Connect données à l'aide des dimensions suivantes.

Dimension	Description
`ConnectionId`	Cette dimension est disponible dans les métriques relatives à la connexion Direct Connect et à l'interface virtuelle. Cette dimension filtre les données en fonction de la connexion.
`OpticalLaneNumber`	Cette dimension filtre les `ConnectionLightLevelTx` données et les `ConnectionLightLevelRx` données, et filtre les données en fonction du numéro de voie optique de la connexion Direct Connect.
`VirtualInterfaceId`	Cette dimension est disponible dans les métriques de l'interfa ce virtuelle Direct Connect et filtre les données en fonction de l'interface virtuelle.

Afficher AWS Direct Connect CloudWatch les métriques

AWS Direct Connect envoie les statistiques suivantes concernant vos connexions Direct Connect. Amazon agrège CloudWatch ensuite ces points de données à intervalles de 1 minute ou 5 minutes. Par défaut, les données métriques Direct Connect sont écrites toutes CloudWatch les 5 minutes.

> **Note**
>
> Si vous définissez un intervalle d'une minute, Direct Connect s'efforcera d'écrire les mesures nécessaires pour CloudWatch utiliser cet intervalle, mais cela ne peut pas toujours être garanti.

Vous pouvez utiliser les procédures suivantes pour consulter les mesures relatives aux connexions Direct Connect.

Pour afficher les métriques à l'aide de la CloudWatch console

Les métriques sont d'abord regroupées par espace de noms de service, puis par les différentes combinaisons de dimension au sein de chaque espace de noms. Pour plus d'informations sur l'utilisation Amazon CloudWatch des métriques Direct Connect, notamment sur l'ajout de fonctions mathématiques ou de requêtes prédéfinies, consultez la section Utilisation Amazon CloudWatch des métriques dans le guide de l' CloudWatch utilisateur Amazon.

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Metrics (Métriques), puis choisissez All metrics (Toutes les métriques).
3. Dans la section Métriques, choisissez DX.
4. Choisissez un nom ConnectionIdou un nom de métrique, puis choisissez l'une des options suivantes pour définir davantage la métrique :

   - Ajouter à la recherche : ajoute cette métrique aux résultats de recherche.
   - Rechercher uniquement ceci : recherche uniquement cette métrique.
   - Supprimer de la graphique : supprime cette métrique de la graphique.
   - Représenter graphiquement cette métrique uniquement : représente graphiquement uniquement cette métrique.
   - Représenter graphiquement tous les résultats de recherche : représente graphiquement toutes les métriques.
   - Représenter graphiquement avec requête SQL : ouvre le générateur de requêtes Metric Insights, qui vous permet de choisir ce que vous souhaitez représenter graphiquement en créant une requête SQL. Pour plus d'informations sur l'utilisation de Metric Insights, consultez la section Interrogez vos CloudWatch métriques avec Metrics Insights dans le guide de CloudWatch l'utilisateur Amazon.

Pour afficher les métriques à l'aide de la AWS Direct Connect console

1. Ouvrez la AWS Direct Connectconsole à l'adresse https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de navigation, choisissez Connections (Connexions).
3. Sélectionnez votre connexion.
4. Choisissez l'onglet Surveillance pour afficher les métriques pour votre connexion.

Pour consulter les statistiques à l'aide du AWS CLI

À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Création d' CloudWatch alarmes pour surveiller AWS Direct Connect les connexions

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Elle envoie une notification à une rubrique Amazon SNS en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes.

Vous pouvez par exemple créer une alarme qui surveille l'état d'une connexion AWS Direct Connect . Une notification est envoyée lorsque l'état de la connexion est down (inactive) pendant 5 périodes consécutives de 1 minute. Pour en savoir plus sur ce qu'il faut savoir pour créer une alarme et pour plus d'informations sur la création d'une alarme, consultez la section Utilisation d'Amazon CloudWatch Alarms dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une CloudWatch alarme.

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Alarms (alertes), puis All alarms (Toutes les alertes).
3. Sélectionnez Create Alarm (Créer une alerte).
4. Choisissez Sélectionner une métrique, puis choisissez DX.
5. Choisissez la métrique Métriques de connexion.
6. Sélectionnez la AWS Direct Connect connexion, puis sélectionnez la métrique Select.
7. Sur la page Spécifier la métrique et les conditions, configurez les paramètres de l'alarme. Pour plus de précisions sur les métriques et les conditions, consultez la section Utilisation d'Amazon CloudWatch Alarms dans le guide de CloudWatch l'utilisateur Amazon.
8. Choisissez Suivant.
9. Configurez les actions d'alarme sur la page Configurer les actions. Pour plus d'informations sur la configuration des actions d'alarme, consultez la section Actions d'alarme dans le guide de CloudWatch l'utilisateur Amazon.
10. Choisissez Suivant.

11. Sur le page Ajouter un nom et une description, saisissez un Nom et une Description de l'alarme facultative, puis choisissez Suivant.
12. Vérifiez l'alarme proposée sur la page Prévisualiser et créer.
13. Si nécessaire, choisissez Modifier pour modifier les informations, puis choisissez Créer une alarme.

    La page Alarmes affiche une nouvelle ligne contenant des informations sur la nouvelle alarme. L'état Actions indique les Actions activées, indiquant que l'alarme est active.

AWS Direct Connect quotas

Le tableau suivant répertorie les quotas associés à AWS Direct Connect.

Composant	Quota	Commentaires
Interfaces virtuelles privées ou publiques par connexion AWS Direct Connect dédiée	50	Cette limite ne peut pas être augmentée.
Interfaces virtuelles de transit par connexion AWS Direct Connect dédiée	4	Cette limite ne peut pas être augmentée.
Interfaces virtuelles privées ou publiques par connexion AWS Direct Connect dédiée et interfaces virtuelles de transit par connexion AWS Direct Connect dédiée	51	Lorsque le AWS Direct Connect support pour Amazon VPC Transit Gateway a été lancé, un quota d'une (1) interface virtuelle de transit a été ajouté au quota de 50 interfaces virtuelles privées ou publiques par connexion dédiée. Le nombre d'interfaces virtuelles de transit autorisées est désormais de quatre (4) et est compté par rapport au maximum de 51 interfaces virtuelles par connexion dédiée. Cette limite ne peut pas être augmentée.
Interfaces virtuelles privées, publiques ou de transit par connexion AWS Direct Connect hébergée	1	Cette limite ne peut pas être augmentée.
AWS Direct Connect Connexions actives par site Direct Connect, par région et par compte	10	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Nombre d'interfaces virtuelles par groupe d'agrégation de liaisons (LAG)	51	Lorsque le AWS Direct Connect support pour Amazon VPC Transit Gateway a

Composant	Quota	Commentaires
		été lancé, un quota d'une (1) interface virtuelle de transit a été ajouté au quota de 50 interfaces virtuelles privées ou publiques par LAG. Le nombre d'interfaces virtuelles de transit autorisées est désormais de quatre (4) et est compté par rapport au maximum de 51 interfaces virtuelles par LAG. Cette limite ne peut pas être augmentée.
Route par session BGP (Border Gateway Protocol) sur une interface virtuelle privée ou transite l'interface virtuelle d'un site vers. AWS Si vous assurez la promotion de plus de 100 routes chacune pour IPv4 et IPv6 par le biais de la session BGP, cette dernière passera en état inactif avec la session BGP DOWN.	100, chacune pour l'IPv4 et l'IPv6	Cette limite ne peut pas être augmentée.
Routes par session BGP (Border Gateway Protocol) sur une interface virtuelle publique	1 000	Cette limite ne peut pas être augmentée.

Composant	Quota	Commentaires
Connexions dédiées par groupe d'agrégation de liaisons (LAG)	4 lorsque la vitesse du port est inférieure à 100G 2 lorsque la vitesse du port est de 100G	
Groupes d'agrégation de liaisons (LAG) par région	10	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
AWS Direct Connect passerelles par compte	200	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Passerelles privées virtuelles par AWS Direct Connect passerelle	20	Cette limite ne peut pas être augmentée.
Passerelles de transit par AWS Direct Connect passerelle	6	Cette limite ne peut pas être augmentée.

Composant	Quota	Commentaires
Interfaces virtuelles (privées ou de transit) par AWS Direct Connect passerelle	30	Cette limite ne peut pas être augmentée.
Nombre de préfixes par AWS Transit Gateway trajet AWS vers le local sur une interface virtuelle de transit	200 au total combiné pour IPv4 et IPv6	Cette limite ne peut pas être augmentée.
Nombre d'interfaces virtuelles par passerelle privée virtuelle	Il n'y a pas de limite.	
Nombre de passerelles Direct Connect associées à une passerelle de transit	20	Cette limite ne peut pas être augmentée.
SiteLink limite de préfixes	100	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.

AWS Direct Connect prend en charge ces vitesses de port sur fibre monomode : 1 Gbit/s : 1000BASE-LX (1310 nm), 10 Gbit/s : 10GBASE-LR (1310 nm) et 100 Gbit/s : 100GBASE-LR4.

Quotas BGP

Les quotas BGP sont les suivants. Les minuteries BGP négocient jusqu'à la valeur la plus basse entre les routeurs. Les intervalles BFD sont définis par l'appareil le plus lent.

- Minuterie de maintien par défaut : 90 secondes
- Minuterie minimale de maintien : 3 secondes

  Une valeur de maintien de 0 n'est pas prise en charge.

- Minuterie KeepAlive par défaut : 30 secondes
- Minuterie minimale keepalive : 1 seconde
- Minuterie de redémarrage progresif : 120 secondes

  Nous vous recommandons de ne pas configurer le redémarrage progressif et le BFD en même temps.
- Intervalle minimum de détection de la vivacité de la BFD : 300 ms
- Multiplicateur minimum de la BFD : 3

Considérations relatives à l'équilibrage de charge

Si vous souhaitez utiliser l'équilibrage de charge avec plusieurs VIF publiques, toutes les VIF doivent se trouver dans la même région.

Résolution des problèmes AWS Direct Connect

Les informations de dépannage suivantes peuvent vous aider à diagnostiquer et à résoudre les problèmes liés à votre connexion AWS Direct Connect .

Table des matières

Dépannage de problèmes (physiques) de niveau 1

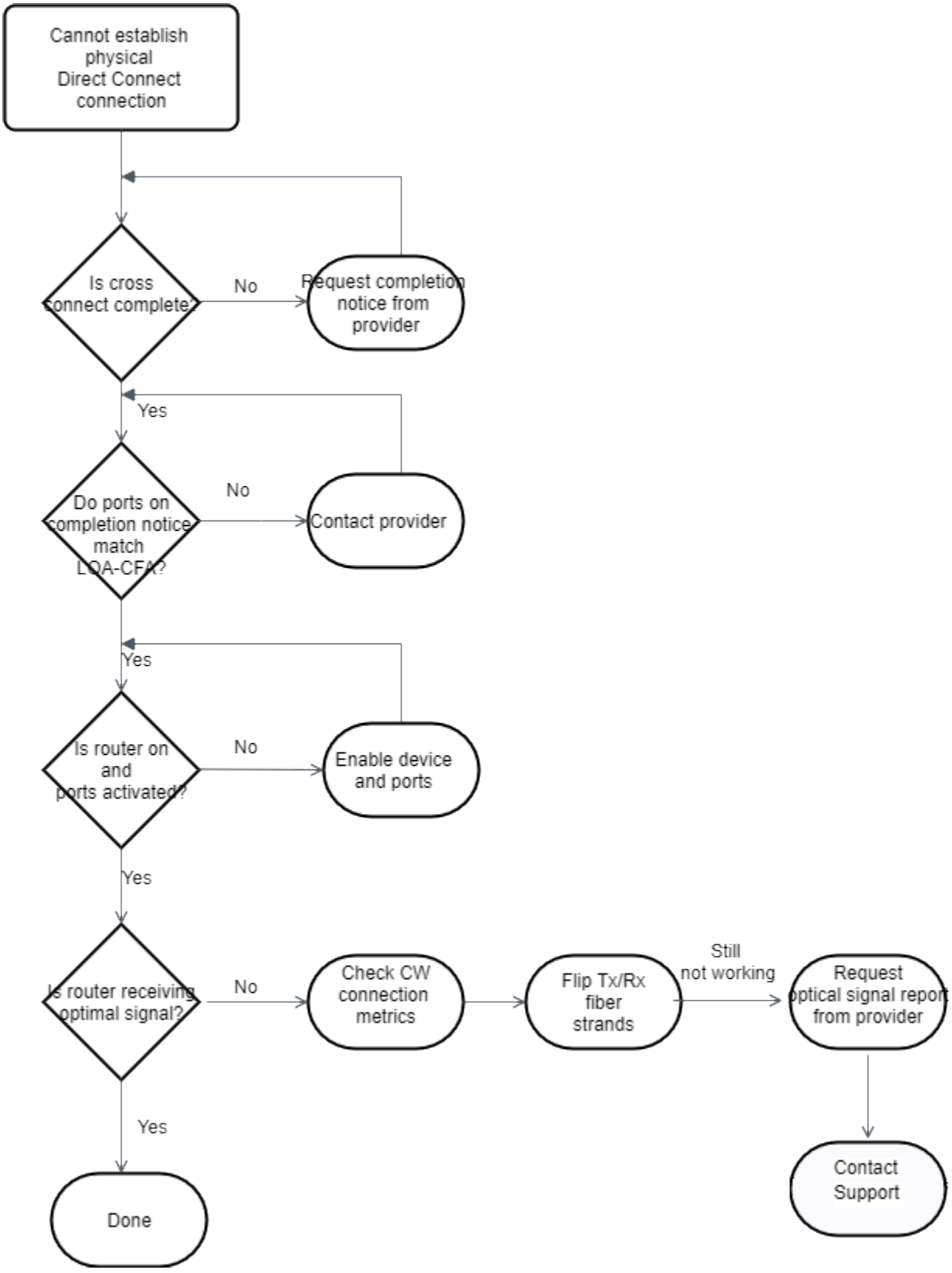
Si vous ou votre fournisseur de réseau rencontrez des difficultés pour établir une connectivité physique avec un AWS Direct Connect appareil, suivez les étapes ci-dessous pour résoudre le problème.

1. Vérifiez auprès du fournisseur de colocalisation que la connexion transversale est terminée. Demandez-lui ou demandez à votre fournisseur de réseau de vous fournir un avis d'achèvement de connexion transversale et comparez les ports avec ceux répertoriés sur votre LOA-CFA.
2. Vérifiez que votre routeur ou que le routeur de votre fournisseur est sous tension et que les ports sont activés.
3. Assurez-vous que les routeurs utilisent le bon émetteur-récepteur optique. La négociation automatique du port doit être désactivée si vous disposez d'une connexion dont la vitesse de port est supérieure à 1 Gb/s. Toutefois, selon le point de terminaison AWS Direct Connect qui dessert votre connexion, il peut être nécessaire d'activer ou de désactiver la négociation automatique pour les connexions à 1 Gbit/s. Si la négociation automatique doit être désactivée pour vos connexions, la vitesse du port et le mode duplex intégral doivent être configurés manuellement. Si votre interface virtuelle reste inactive, consultez Dépannage de problèmes (de liaison de données) de niveau 2.
4. Vérifiez que le routeur reçoit un signal optique acceptable sur la connexion transversale.
5. Essayez la distribution (également connue sous le nom de propagation) des câbles de fibre Tx/Rx.
6. Consultez les CloudWatch statistiques Amazon pour AWS Direct Connect. Vous pouvez vérifier les valeurs optiques Tx/Rx de l' AWS Direct Connect appareil (1 Gbit/s et 10 Gbit/s), le nombre

d'erreurs physiques et l'état de fonctionnement. Pour plus d'informations, consultez la section Surveillance avec Amazon CloudWatch.

7. Contactez le fournisseur de colocalisation et demandez un rapport écrit du signal optique Tx/Rx sur la connexion transversale.
8. Si les étapes précédentes ne permettent pas de résoudre les problèmes de connectivité physique, contactez AWS Support et fournissez l'avis d'achèvement de la connexion transversale et le rapport du signal optique du fournisseur de colocalisation.

Le diagramme suivant comprend les étapes permettant de diagnostiquer les problèmes liés à la connexion physique.

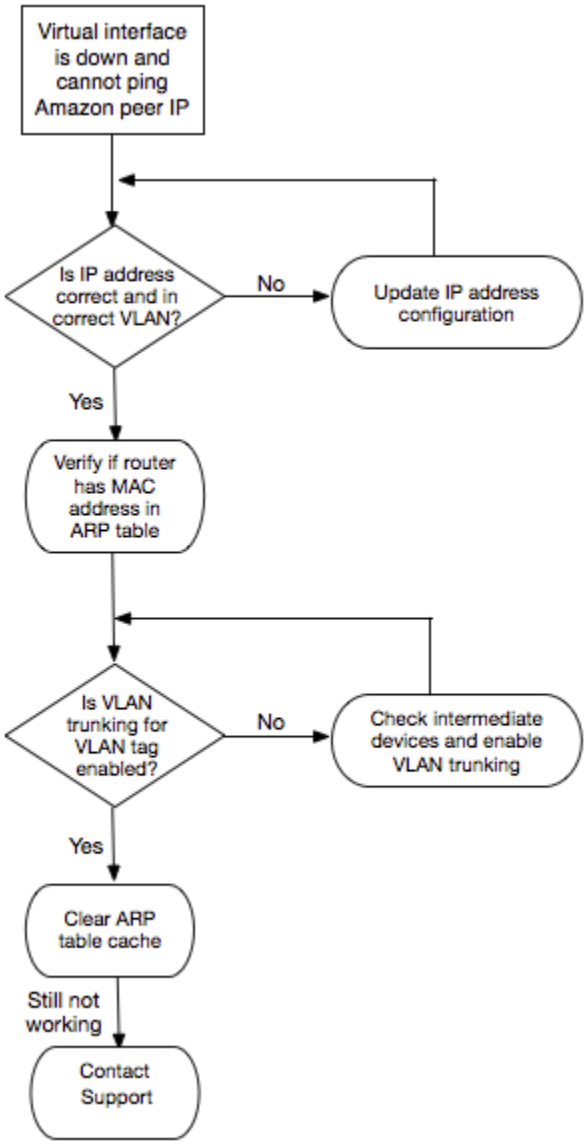

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Dépannage de problèmes (de liaison de données) de niveau 2

Si votre connexion AWS Direct Connect physique est active mais que votre interface virtuelle est hors service, suivez les étapes ci-dessous pour résoudre le problème.

1. Si vous ne pouvez pas pinger l'adresse IP d'appairage Amazon, vérifiez que votre adresse IP de pair est correctement configurée et dans le bon VLAN. Assurez-vous que l'adresse IP est configurée dans la sous-interface VLAN et non dans l'interface physique (par exemple, GigabitEthernet 0/0.123 au lieu de 0/0). GigabitEthernet
2. Vérifiez si le routeur possède une entrée d'adresse MAC provenant du AWS point de terminaison dans votre table de protocole de résolution d'adresses (ARP).
3. Assurez-vous que la jonction VLAN de tous les périphériques intermédiaires entre les points de terminaison est activée pour votre balise VLAN 802.1Q. L'ARP ne peut pas être établi sur le AWS côté tant qu'il n'a pas AWS reçu de trafic étiqueté.
4. Effacez le cache de votre tableau d'ARP (ou du tableau de votre fournisseur).
5. Si les étapes ci-dessus ne permettent pas d'établir l'ARP ou si vous ne parvenez toujours pas à envoyer un ping à l'adresse IP de l'homologue Amazon, contactez le AWS Support.

Le diagramme suivant montre les étapes permettant de diagnostiquer les problèmes liés à la liaison de données.



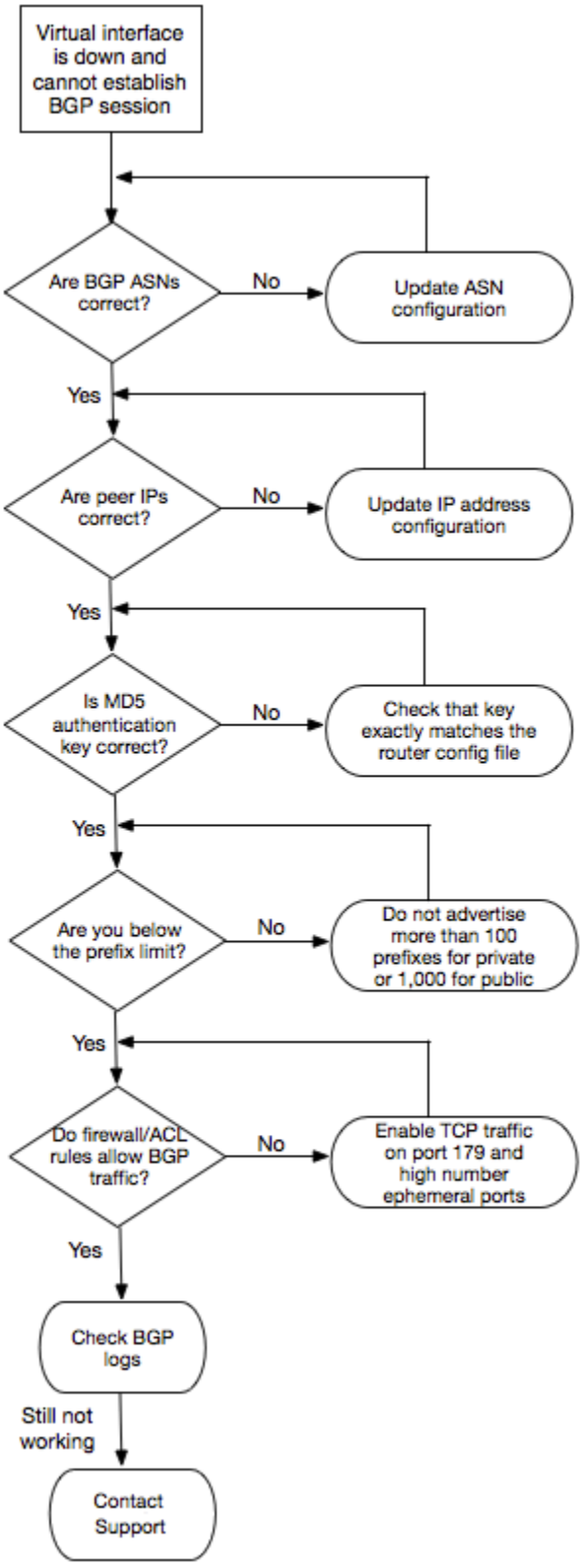
Si la session BGP n'est toujours pas établie après la vérification de ces étapes, consultez Dépannage des problèmes (de réseau/transport) de niveau 3/4. Si la session BGP est établie, mais que vous rencontrez des problèmes de routage, consultez Dépannage des problèmes de routage.

Dépannage des problèmes (de réseau/transport) de niveau 3/4

Imaginons une situation dans laquelle votre connexion AWS Direct Connect physique est active et où vous pouvez envoyer un ping à l'adresse IP du pair Amazon. Si votre interface virtuelle ne fonctionne pas et que la session d'appairage BGP ne peut pas être établie, utilisez les étapes suivantes pour résoudre le problème :

1. Assurez-vous que votre numéro d'ASN (Autonomous System Number) local de BGP et le numéro ASN d'Amazon sont correctement configurés.
2. Assurez-vous que les IP de pair pour les deux côtés de la session d'appairage BGP sont configurés correctement.
3. Assurez-vous que votre clé d'authentification MD5 est configurée et qu'elle correspond exactement à la clé indiquée dans le fichier de configuration du routeur téléchargé. Vérifiez qu'il n'y ait pas d'espaces ou de caractères supplémentaires.
4. Vérifiez que vous ou votre fournisseur ne publiez pas plus de 100 préfixes pour interfaces virtuelles privées ou 1 000 préfixes pour interfaces virtuelles publiques. Ces limites strictes ne doivent pas être dépassées.
5. Assurez-vous qu'aucun pare-feu ni règle ACL ne bloque le port TCP 179 ni aucun autre port éphémère avec un numéro élevé. Ces ports sont nécessaires à BGP pour établir une connexion TCP entre les pairs.
6. Vérifiez vos journaux BGP pour tout erreur ou message d'avertissement.
7. Si les étapes ci-dessus n'établissent pas la session de peering BGP, contactez le Support AWS.

Le diagramme suivant présente les étapes permettant de diagnostiquer les problèmes liés à la session d'appairage BGP.



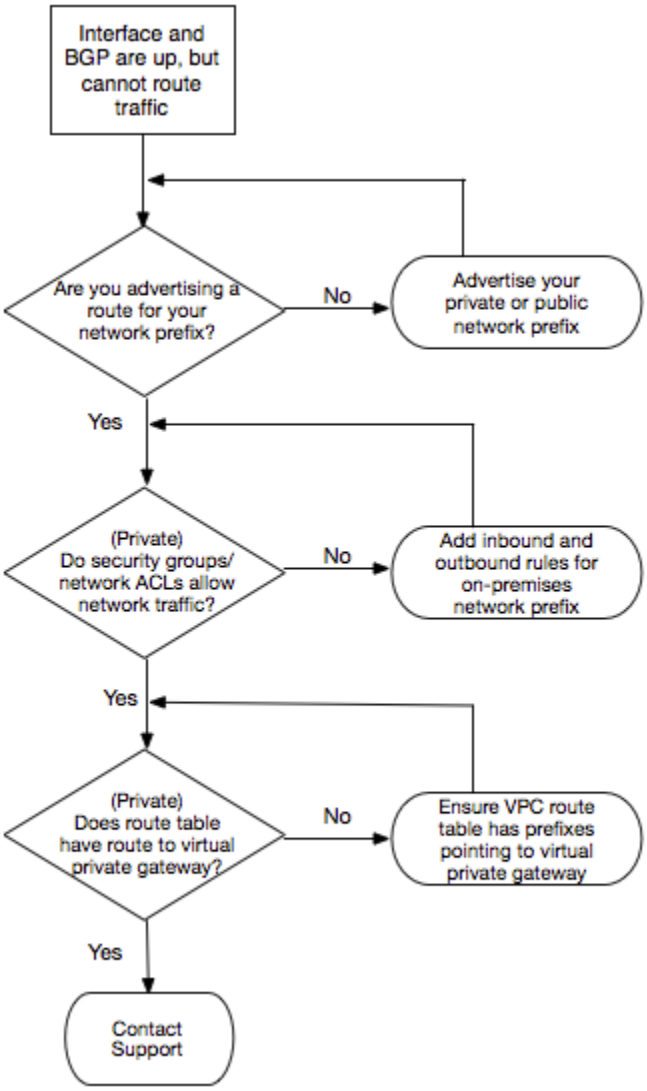
Si la session d'appairage BGP est établie, mais que vous rencontrez des problèmes de routage, consultez Dépannage des problèmes de routage.

Dépannage des problèmes de routage

Prenons l'exemple d'une situation où votre interface virtuelle fonctionne et que vous avez établi une session d'appairage BGP. Si vous ne parvenez pas à acheminer le trafic via l'interface virtuelle, utilisez les étapes suivantes pour résoudre le problème :

1. Assurez-vous de publier une route pour le préfixe de votre réseau local au cours de la session BGP. Pour une interface virtuelle privée, cela peut être un préfixe réseau privé ou public. Pour une interface virtuelle publique, cela doit être un préfixe réseau publiquement routable.
2. Pour une interface virtuelle privée, assurez-vous que vos groupes de sécurité VPC et vos ACL réseaux permettent un trafic entrant et sortant pour le préfixe de votre réseau local. Pour plus d'informations, consultez les rubriques Groupes de sécurité et ACL réseau dans le Guide de l'utilisateur d'Amazon VPC.
3. Pour une interface virtuelle privée, assurez-vous que les préfixes de vos tables de routage VPC pointent vers la passerelle réseau privé virtuel à laquelle votre interface réseau privé virtuel est connectée. Par exemple, si vous préférez que l'ensemble de votre trafic soit acheminé par défaut vers votre réseau local, vous pouvez ajouter la route par défaut (0.0.0.0/0 et/ou ::/0) avec la passerelle réseau privé virtuel comme cible dans vos tables de routage VPC.
   - Vous pouvez également activer la propagation de route pour mettre à jour automatiquement des routes dans vos tables de routage selon votre publicité de routage BGP dynamique. Vous pouvez avoir jusqu'à 100 itinéraires propagés par table de routage. Cette limite ne peut pas être augmentée. Pour plus d'informations, consultez Activation et désactivation de la propagation de route dans le Guide de l'utilisateur d'Amazon VPC.
4. Si les étapes ci-dessus ne résolvent pas vos problèmes de routage, contactez le AWS Support.

Le diagramme suivant montre les étapes permettant de diagnostiquer les problèmes liés au routage.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Historique du document

Le tableau suivant décrit toutes les versions des AWS Direct Connect.

Fonctionnalité	Description	Date
Support pour SiteLink	Vous pouvez créer une interface privée virtuelle qui permet la connectivité entre deux points de présence Direct Connect (PoPs) dans la même AWS région. Pour de plus amples informations, veuillez consulter Interfaces virtuelles hébergées.	2021-12-01
Prise en charge MAC Security	Vous pouvez utiliser des connexions AWS Direct Connect qui prennent en charge MACsec pour chiffrer vos données depuis le centre de données de votre entreprise jusqu'à l'emplacement AWS Direct Connect. Pour en savoir plus, consultez Sécurité MAC.	31/03/2021
Prise en charge de 100G	Rubriques mises à jour pour inclure la prise en charge des connexions dédiées de 100G.	12/02/2021
Nouvel emplacement en Italie	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement en Italie. Pour en savoir plus, consultez the section called "Europe (Milan)".	2021-01-22
Nouvel emplacement en Israël	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement en Israël. Pour en savoir plus, consultez the section called "Israël (Tel Aviv)".	2020-07-07
Prise en charge des tests de basculement de la boîte à outils de résilience	Utilisez la fonctionnalité de test de basculement de la boîte à outils de résilience pour tester la résilience de vos connexions. Pour en savoir plus, consultez the section called "AWS Direct Connect Test de basculement".	03/06/2020

Fonctionnalité	Description	Date
CloudWatch Support métrique VIF	Vous pouvez surveiller les AWS Direct Connect connexions physiques et les interfaces virtuelles à l'aide de CloudWatch. Pour en savoir plus, consultez the section called “Surveillance avec Amazon CloudWatch”.	2020-05-11
Boîte à outils de résilience AWS Direct Connect	La Boîte à outils de résilience AWS Direct Connect fournit un assistant de connexion avec plusieurs modèles de résilience qui vous aide à commander des connexions dédiées pour atteindre votre objectif en matière de SLA. Pour en savoir plus, consultez Utiliser le AWS Direct Connect Resiliency Toolkit pour démarrer.	07-10-2019
Prise en charge de régions supplémentaires pour prendre en charge AWS Transit Gateway entre comptes	Pour plus d'informations, consultez the section called “Associations de la passerelle de transit”.	30-09-2019
Prise en charge AWS Direct Connect pour AWS Transit Gateway	Vous pouvez utiliser une AWS Direct Connectpasserelle pour connecter votre connexion AWS Direct Connect via une interface de transit virtuelle aux VPC ou VPN attachés à votre passerelle de transit. Vous associez une passerelle Direct Connect à la passerelle de transit. Ensuite, vous créez une interface de transit virtuelle pour votre connexion AWS Direct Connect à la passerelle Direct Connect. Pour plus d'informations, consultez the section called “Associations de la passerelle de transit”.	27/03/2019

Fonctionnalité	Description	Date
Prise en charge des trames jumbo	Vous pouvez envoyer les trames jumbo (MTU de 9001) via AWS Direct Connect. Pour en savoir plus, consultez Définir la MTU du réseau pour les interfaces virtuelles privées ou les interfaces de transit virtuelles.	2018-10-11
Communautés BGP de préférence locale	Vous pouvez utiliser les balises de la communauté BGP de préférence locale pour équilibrer la charge et définir les préférences de routage du trafic entrant vers votre réseau. Pour en savoir plus, consultez Communautés BGP de préférence locale.	06-02-2018
AWS Direct ConnectPasserelle	Vous pouvez utiliser une passerelle Direct Connect pour associer votre connexion AWS Direct Connect à des VPC dans des régions distantes. Pour en savoir plus, consultez Utilisation des passerelles Direct Connect.	01-11-2017
CloudWatch Métriques Amazon	Vous pouvez consulter CloudWatch les statistiques de vos AWS Direct Connect connexions. Pour en savoir plus, consultez Surveillance avec Amazon CloudWatch.	29/06/2017
Groupes d'agrégation de liaisons (LAG)	Vous pouvez créer un groupe d'agrégation de liaisons (LAG) pour regrouper plusieurs connexions AWS Direct Connect. Pour en savoir plus, consultez Groupes d'agrégation de liaisons (LAG).	2017-02-13
Prise en charge d'IPv6	Votre interface virtuelle peut désormais prendre en charge une session d'appairage BGP IPv6. Pour en savoir plus, consultez Ajouter ou supprimer un homologue BGP.	2016-12-01
Prise en charge du balisage	Vous pouvez maintenant baliser vos ressources AWS Direct Connect. Pour en savoir plus, consultez Balisage de ressources AWS Direct Connect.	2016-11-04

Fonctionnalité	Description	Date
LOA-CFA en libre-service	Vous pouvez désormais télécharger votre Lettre d'autorisation - Affectation d'installation de connexion (LOA-CFA) à l'aide de la console ou de l'API AWS Direct Connect.	2016-06-22
Nouvel emplacement dans la Silicon Valley	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement dans la Silicon Valley dans la région USA Ouest (Californie du Nord).	2016-06-03
Nouvel emplacement à Amsterdam	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement à Amsterdam dans la région Europe (Francfort).	2016-05-19
Nouveaux emplacements à Portland, dans l'Oregon, et à Singapour	Rubrique mise à jour pour inclure l'ajout de nouveaux emplacements à Portland, dans l'Oregon, et à Singapour dans les régions USA Ouest (Oregon) et Asie Pacifique (Singapour).	2016-04-27
Nouvel emplacement à Sao Paulo, Brésil	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement à São Paulo, dans la région Amérique du Sud (São Paulo).	2015-12-09
Nouveaux emplacements à Dallas, Londres, Silicon Valley et Mumbai	Sujets mis à jour pour inclure l'ajout de nouveaux sites à Dallas (région de l'Est des États-Unis (Virginie du Nord)), à Londres (région Europe (Irlande)), dans la Silicon Valley AWS GovCloud (région de l'ouest des États-Unis) et à Mumbai (région Asie-Pacifique (Singapour)).	2015-11-27

Fonctionnalité	Description	Date
Nouvel emplacement dans la région Chine (Beijing)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement à Beijing dans la région Chine (Beijing).	2015-04-14
Nouvel emplacement à Las Vegas dans la région USA Ouest (Oregon)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement AWS Direct Connect à Las Vegas, dans la région USA Ouest (Oregon).	2014-11-10
Nouvelle région UE (Francfort)	Rubriques mises à jour pour inclure l'ajout des nouveaux emplacements AWS Direct Connect desservant la région UE (Francfort).	2014-10-23
Nouveaux emplacements dans la région Asie-Pacifique (Sydney)	Rubriques mises à jour pour inclure l'ajout des nouveaux emplacements AWS Direct Connect desservant la région Asie-Pacifique (Sydney).	2014-07-14
Prise en charge de AWS CloudTrail	Ajout d'une nouvelle rubrique expliquant comment vous pouvez l'utiliser CloudTrail pour enregistrer l'activitéAWS Direct Connect. Pour en savoir plus, consultez Journalisation des appels d'API AWS Direct Connect avec AWS CloudTrail.	2014-04-04
Prise en charge de l'accès des régions AWS à distance	Ajout d'une nouvelle rubrique pour expliquer comment accéder aux ressources publiques d'une région à distance. Pour en savoir plus, consultez Accès à une région AWS à distance.	2013-12-19

Fonctionnalité	Description	Date
Prise en charge des connexions hébergées	Rubriques mises à jour pour inclure la prise en charge des connexions hébergées.	2013-10-22
Nouvel emplacement dans la région UE (Irlande)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement AWS Direct Connect desservant la région UE (Irlande).	2013-06-24
Nouvel emplacement à Seattle dans la région USA Ouest (Oregon)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement AWS Direct Connect à Seattle, desservant la région USA Ouest (Oregon).	2013-05-08
Prise en charge de l'utilisation d'IAM avec AWS Direct Connect	Ajout d'une rubrique sur l'utilisation d'AWS Identity and Access Management avec AWS Direct Connect. Pour en savoir plus, consultez the section called “Gestion des identités et des accès”.	2012-12-21
Nouvelle région Asie-Pacifique (Sydney)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement AWS Direct Connect desservant la région Asie-Pacifique (Sydney).	2012-12-14

Fonctionnalité	Description	Date
Nouvelle console AWS Direct Connect et nouvelles régions USA Est (Virginie du Nord) et Amérique du Sud (São Paulo)	Remplacement du Manuel de mise en route d'AWS Direct Connect par le Guide de l'utilisateur AWS Direct Connect. Ajout de nouvelles rubriques pour couvrir la nouvelle console AWS Direct Connect, ajout d'une rubrique sur la facturation, ajout d'informations de configuration du routeur et rubriques mises à jour pour inclure l'ajout de deux nouveaux emplacements AWS Direct Connect desservant les régions USA Est (Virginie du Nord) et Amérique du Sud (Sao Paulo).	2012-08-13
Prise en charge des régions UE (Irlande), Asie-Pacifique (Singapour) et Asie-Pacifique (Tokyo)	Ajout d'une nouvelle section de résolution des problèmes et rubriques mises à jour pour inclure l'ajout de quatre nouveaux emplacement AWS Direct Connect desservant les régions USA Ouest (Californie du Nord), UE (Irlande), Asie-Pacifique (Singapour) et Asie-Pacifique (Tokyo).	2012-01-10
Prise en charge de la région USA Ouest (Californie du Nord)	Rubriques mises à jour pour inclure l'ajout de la région USA Ouest (Californie du Nord).	2011-09-08
Publication	Première version d'AWS Direct Connect.	2011-08-03

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.