Guide de l’utilisateur

AWS Direct Connect

AWS Direct Connect: Guide de l’utilisateur

Table of Contents

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

Direct Connect relie votre réseau interne à un 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 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 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.

- Pour obtenir la liste des points de vente Direct Connect auxquels vous pouvez vous connecter, consultez la section Points de vente AWS Direct Connect.
- Pour obtenir des réponses aux questions concernant Direct Connect, consultez la FAQ Direct Connect.

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

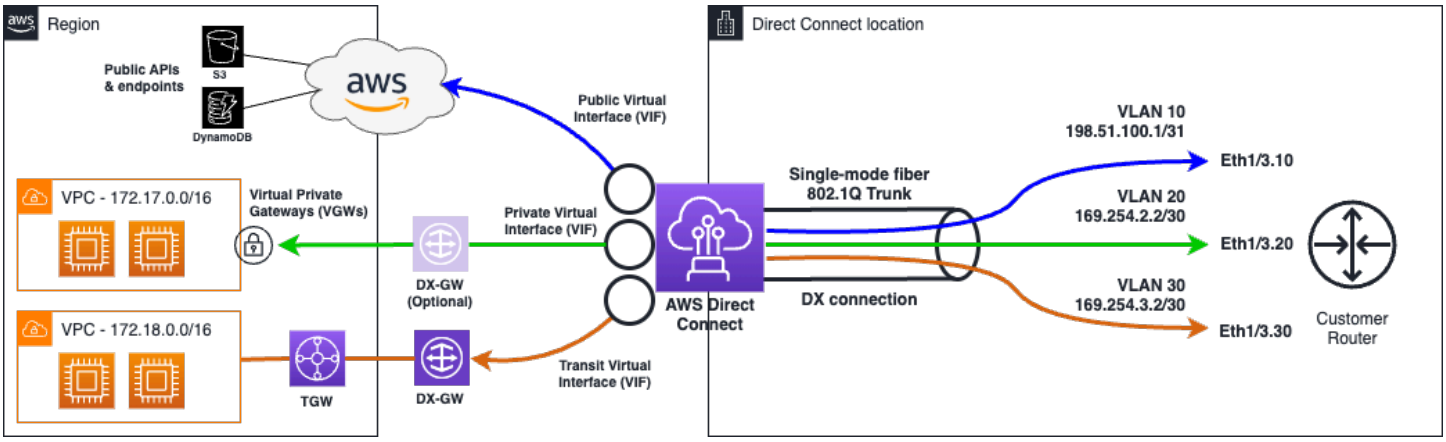


Table des matières

- Direct Connect politiques de routage et communautés BGP

Direct Connect composants

Les principaux composants que vous utilisez pour Direct Connect sont les suivants :

Connexions

Créez une connexion dans un Direct Connect lieu pour établir une connexion réseau entre vos locaux et une AWS région. Pour de plus amples informations, veuillez consulter Direct Connect connexions dédiées et hébergées.

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. Les types d'interfaces pris en charge sont décrits ci-dessous dansthe section called "Types d'interfaces virtuelles Direct Connect pris en charge". Pour plus de détails sur les interfaces prises en charge, reportez-vous Direct Connect interfaces virtuelles et interfaces virtuelles hébergées aux sections etConditions préalables pour les interfaces virtuelles.

Exigences réseau

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

- Votre réseau est colocalisé avec un emplacement existant Direct Connect . Pour plus d'informations sur les Direct Connect emplacements disponibles, consultez la section Détails du produit AWS Direct Connect.
- Vous travaillez avec un 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 Direct Connect.

Votre réseau doit également répondre aux conditions suivantes :

- Votre réseau doit utiliser une fibre monomode avec un émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, un émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits, un émetteur-récepteur 100GBASE- pour 100 gigabit Ethernet ou un 400GBASE- LR4 pour Ethernet 400 Gbit/s. LR4
- Selon le point de terminaison AWS Direct Connect servant votre connexion, la négociation automatique des appareils sur site devra peut-être être activée ou désactivée pour toute connexion dédiée. Si une interface virtuelle reste inactive alors qu'une connexion Direct Connect est établie, voirRésoudre les problèmes liés à la couche 2 (liaison de données).
- L'encapsulation VLAN 802.1Q doit être prise en charge sur l'ensemble de la connexion, y compris les périphériques intermédiaires.
- Votre appareil doit prendre en charge le protocole BGP (Border Gateway Protocol) et l'authentification BGP MD5 .
- (Facultatif) Vous pouvez configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau. Le BFD asynchrone est automatiquement activé pour chaque 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.

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

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 de plus amples informations, veuillez consulter MTUs pour les interfaces virtuelles privées ou les interfaces virtuelles de transit.

Types d'interfaces virtuelles Direct Connect pris en charge

AWS Direct Connect prend en charge les trois types d'interface virtuelle (VIF) suivants :

- Interface virtuelle privée

  Ce type d'interface est utilisé pour accéder à un Amazon Virtual Private Cloud (VPC) à l'aide d'adresses IP privées. Avec une interface virtuelle privée, vous pouvez

  - Connectez-vous directement à un seul VPC par interface virtuelle privée pour accéder à ces ressources en mode privé IPs dans la même région.
  - Connectez une interface virtuelle privée à une passerelle Direct Connect pour accéder à plusieurs passerelles privées virtuelles sur tous les comptes et toutes les AWS régions (à l'exception des régions de AWS Chine).
- Interface virtuelle publique

  Ce type d'interface virtuelle est utilisé pour accéder à tous les services AWS publics à l'aide d'adresses IP publiques. Grâce à une interface virtuelle publique, vous pouvez vous connecter à toutes les adresses IP AWS publiques et à tous les services dans le monde entier.
- Interface virtuelle Transit

  Ce type d'interface est utilisé pour accéder à une ou plusieurs passerelles Amazon VPC Transit associées aux passerelles Direct Connect. Une interface virtuelle de transit vous permet de connecter plusieurs passerelles Amazon VPC Transit sur plusieurs comptes et Régions AWS (à l'exception des régions de AWS Chine).

> **Note**
>
> Le nombre de différents types d'associations entre une passerelle Direct Connect et une interface virtuelle est limité. Pour plus d'informations sur les limites spécifiques, consultez la Quotas Direct Connect page.

Pour plus d'informations sur les interfaces virtuelles, consultezInterfaces virtuelles et interfaces virtuelles hébergées.

Tarification de 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 EC2 instances classiques ou le EC2 trafic 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 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. Direct Connect

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

Accès aux Direct Connect régions éloignées

Direct Connect des sites situés dans des régions publiques ou AWS GovCloud (US) peuvent accéder aux services publics de toute autre région publique (à l'exception de la Chine (Pékin et Ningxia)). En outre, Direct Connect les connexions dans les régions publiques AWS GovCloud (US) peuvent être configurées pour accéder à un VPC de votre compte dans n'importe quelle autre région publique (à l'exception de la Chine (Pékin et Ningxia). Par conséquent, vous pouvez utiliser une même connexion Direct Connect pour créer des services sur plusieurs régions. Tout le trafic réseau reste sur le backbone du réseau AWS mondial, que vous accédiez à des AWS services 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 Direct Connect , consultez Stratégies de routage et communautés BGP (Border Gateway Protocol).

Accès aux services publics dans une région isolée

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 Interfaces virtuelles et interfaces virtuelles hébergées.

Après avoir créé une interface virtuelle publique et établi une session BGP, votre routeur apprend les itinéraires des autres AWS régions publiques. Pour plus d'informations sur les préfixes actuellement proposés par AWS, consultez la section Plages d'adresses AWS IP dans le. Référence générale d'Amazon Web Services

Accès VPCs dans une région éloignée

Vous pouvez créer une Passerelle Direct Connect dans toutes les régions publiques. Utilisez-le pour connecter votre Direct Connect connexion via une interface virtuelle privée VPCs à votre compte situé dans différentes régions ou à une passerelle de transit. Pour de plus amples informations, veuillez consulter Direct Connect passerelles.

Vous pouvez également créer une interface virtuelle publique pour votre Direct Connect connexion, puis établir une connexion VPN avec votre VPC dans la région distante. 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.

Network-to-Amazon Options de connectivité VPC

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

- Amazon Virtual Private Cloud Connectivity Options

Direct Connect politiques de routage et communautés BGP

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. 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 d'accéder Direct Connect à AWS des services publics, vous devez spécifier les préfixes publics ou IPv6 les IPv4 préfixes à utiliser 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.

- 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 Direct Connect si le même préfixe est annoncé à la fois sur Internet et sur une interface virtuelle publique.
- 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 de AWS Chine ne sont annoncés que dans les régions de Chine. 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.

- Direct Connect annonce des préfixes avec une longueur de chemin minimale de 3.
- 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 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 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.
- 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 Direct Connect clients
  - Des réseaux homologues au réseau AWS mondial
  - Des fournisseurs de transit d'Amazon
- Lorsque vous utilisez une interface publique, vous pouvez utiliser un ASN public ou privé. Cependant, il y a des considérations importantes à prendre en compte :
  - Public ASNs : vous devez être propriétaire de l'ASN et avoir le droit de l'annoncer. AWS vérifiera que vous êtes bien propriétaire de l'ASN. Le format ASNs (1-2147483647) et le format long (1-4294967295) sont pris en ASNs charge.
  - Privé ASNs : vous pouvez utiliser le mode ASNs privé dans les plages suivantes :
    - privé ASNs : 64512-65534
    - long privé ASNs : 4200000000-4294967294

    Toutefois, Direct Connect vous remplacerez l'ASN privé par l' AWS ASN (7224) lors de la publicité de vos préfixes AWS auprès d'autres clients ou sur Internet.
  - ASN préfixant :
    - Avec un ASN public (ASN et ASN long), le préattachement fonctionnera comme prévu, et votre ASN préétabli sera visible sur les autres réseaux.
    - Avec un ASN privé (ASN et ASN long), tout préfixe que vous ferez sera supprimé lorsque votre ASN privé sera AWS remplacé par 7224. Cela signifie que la préfixation de l'ASN n'est pas efficace pour influencer les décisions de routage en dehors de AWS l'utilisation d'un ASN privé sur une interface virtuelle publique.
- Lorsque vous établissez une session d'appairage BGP AWS via une interface virtuelle publique, utilisez 7224 pour les numéros de système autonomes (ASN) afin d'établir la session BGP sur le côté. AWS L'ASN de votre routeur ou de votre passerelle client doit être différent de cet ASN. L'ASN de votre client peut être soit un ASN (1-2147483647, hors plages réservées), soit un ASN long (1-4294967295, hors plages réservées).

Communautés BGP d'interface virtuelle publique

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 Direct Connect.

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

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

Direct Connect fournit également des tags communautaires BGP sur les itinéraires Amazon annoncés. Si vous avez l' 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 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 IPv6 préfixes IPv4 ou 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 active/passive des connexions. 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 active/passive connexions 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 utilise le routage ECMP (Equal-Cost Multipath) sur plusieurs interfaces virtuelles privées ou de transit lorsque les préfixes ont la même longueur AS_PATH et les mêmes attributs BGP. Il n'est pas nécessaire que le préfixe ASNs dans le AS_PATH corresponde.

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 Région AWS de transit Direct Connect, l'emplacement Direct Connect associé influence la capacité à utiliser l'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 ayant la même longueur AS_PATH et la 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 Active/Active ou Active/Passive Direct Connect AWS depuis 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 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 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).

Support ASN prolongé dans Direct Connect

Support pour les longs ASNs (4 octets) vous permet de configurer de longs numéros de système autonomes (ASNs) dans le cadre des paramètres de la session BGP établie entre le périphérique AWS réseau et votre périphérique réseau. Cette fonctionnalité est activée ou désactivée pour chaque compte.

Vous pouvez définir une plage ASN ou ASN longue sur la console ou via le. APIs

- Lorsque vous utilisez la console, le champ ASN prend en charge ASNs les deux options. ASNs Vous pouvez ajouter n'importe quelle plage comprise entre 1 et 4294967294.
- Lorsque vous utilisez le APIs pour créer une interface virtuelle, vous pouvez spécifier un ASN (`asn`) ou un ASN long (`asnLong`), mais pas les deux. Pour plus d'informations sur l'utilisation de l'ASN ou de l'ASN long, consultez ce qui suit APIs dans la référence de l'Direct Connect API :
  - `BGPPeer`
  - `DeleteBGPPeerRequest`
  - `NewBGPPeer`
  - `NewPrivateVirtualInterface`
  - `NewPrivateVirtualInterfaceAllocation`
  - `NewPublicVirtualInterface`
  - `NewPublicVirtualInterfaceAllocation`
  - `NewTransitVirtualInterface`
  - `NewTransitVirtualInterfaceAllocation`
  - `VirtualInterface`

Considérations

Lorsque vous choisissez d'utiliser un ASN ou un ASN long, tenez compte des points suivants :

- Rétrocompatibilité : Direct Connect gère automatiquement les sessions BGP avec des routeurs ASN et de longs routeurs compatibles avec l'ASN. Si votre routeur ne supporte pas le format long ASNs, la session BGP fonctionnera en mode ASN.
- Format ASN : vous pouvez spécifier 4 octets ASNs au format asplain, par exemple, `4200000000` ou au format asdot, par exemple,. `64086.59904` Direct Connect accepte les deux formats mais s'affiche ASNs au format asplain
- Plages ASN privées : lorsque vous utilisez private long ASNs (`4200000000-4294967294`), le même comportement de remplacement s'applique qu'avec private ASNs. Direct Connect remplacera votre ASN privé par `7224` lorsque vous ferez de la publicité sur d'autres réseaux.
- Tags communautaires BGP : tous les tags communautaires BGP existants (`7224:xxxx`) fonctionnent avec Long. ASNs Le format du tag communautaire reste inchangé.

- Surveillance et résolution des problèmes : CloudWatch les métriques, les journaux de sessions BGP et les outils de résolution des problèmes s'affichent ASNs en texte intégral pour des raisons de cohérence.

Disponibilité et prix

Notez les points suivants pour le support ASN prolongé avec Direct Connect :

- Disponibilité : L'ASN long est disponible dans toutes les AWS régions où il Direct Connect est pris en charge.
- Tarification : aucun frais supplémentaire n'est facturé pour le support ASN prolongé au-delà de la Direct Connect tarification standard.

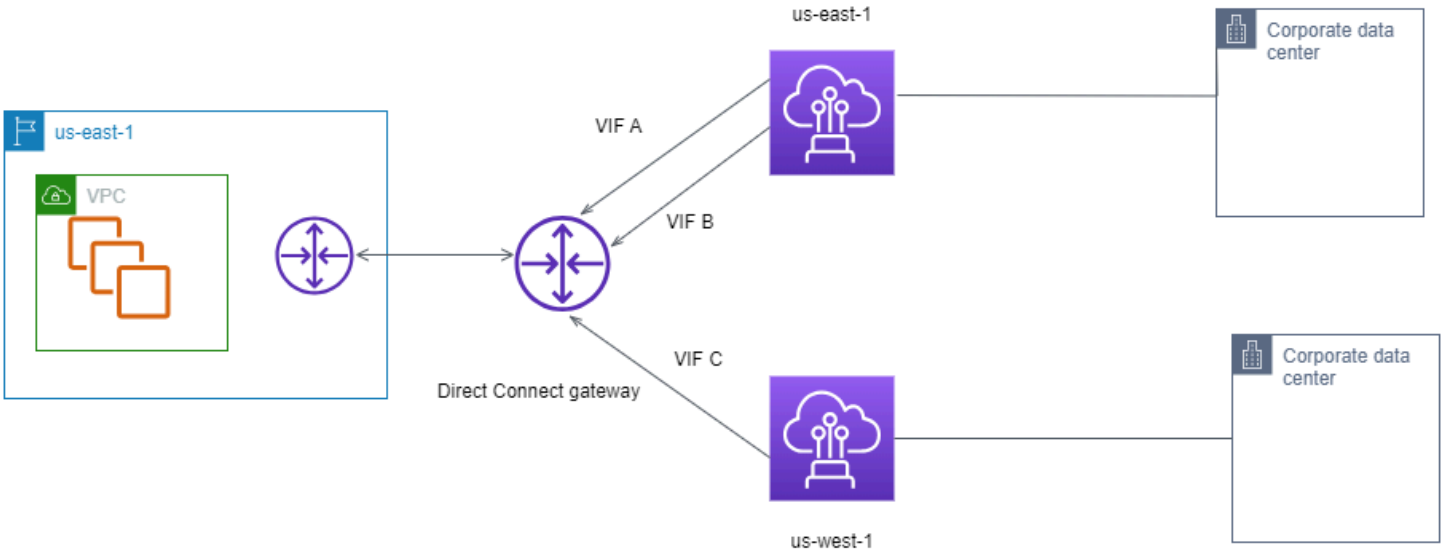
> **Note**
>
> L'activation longue durée de l'ASN s'applique à l'ensemble AWS de votre compte. Vous ne pouvez pas activer le support ASN prolongé pour des interfaces virtuelles individuelles ou des homologues BGP.

Direct Connect exemple de routage d'interface virtuelle privée

Considérez la configuration dans laquelle la région d'origine de l' Direct Connect emplacement 1 est identique à la région d'origine du VPC. Il existe un Direct Connect emplacement redondant dans une région différente. Il en existe deux privés VIFs (VIF A et VIF B) entre l' Direct Connect emplacement 1 (us-east-1) et la passerelle Direct Connect. Un VIF privé (VIF C) relie l' 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.

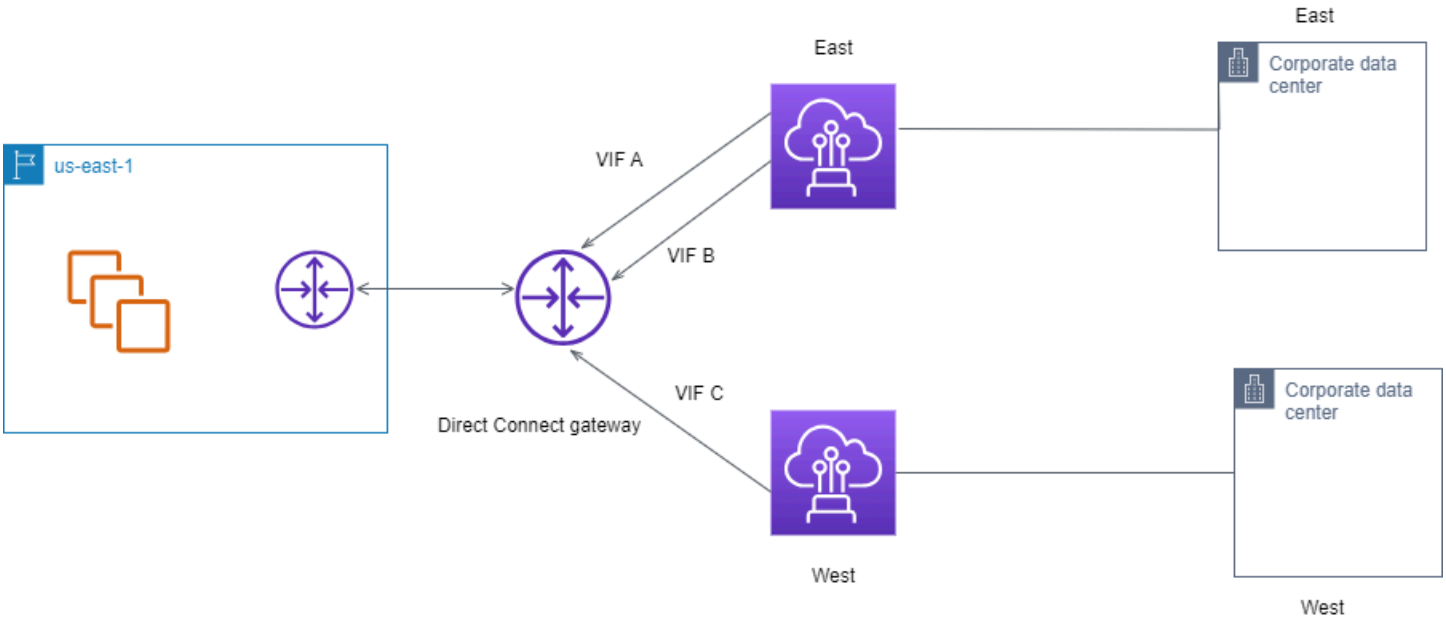
Ils VIFs ont les configurations suivantes :

- 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 il possède la plus longue longueur de préfixe.

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



Direct Connect options de connexion

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.

Les options de connexion suivantes sont disponibles pour Direct Connect.

- Résilience maximale : ce modèle est disponible dans le AWS Direct Connect Resiliency Toolkit et 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 Direct Connect. Pour de plus amples informations, veuillez consulter AWS Direct Connect Boîte à outils de résilience.
- Haute résilience : ce modèle est disponible dans le AWS Direct Connect Resiliency Toolkit et 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 Direct Connect. Pour de plus amples informations, veuillez consulter AWS Direct Connect Boîte à outils de résilience.
- Développement et test : ce modèle est disponible dans le AWS Direct Connect Resiliency Toolkit et vous permet de développer et de tester la résilience pour les charges de travail non critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts au même endroit. Pour de plus amples informations, veuillez consulter AWS Direct Connect Boîte à outils de résilience.
- Classique : une connexion classique crée une connexion sans avoir besoin du AWS Direct Connect Resiliency Toolkit. Il est destiné aux utilisateurs disposant de connexions existantes et souhaitant ajouter des connexions supplémentaires sans utiliser le kit d'outils. Ce modèle dispose d'un SLA de 95 % mais ne fournit ni résilience ni redondance. Pour de plus amples informations, veuillez consulter Connexion classique.

Rubriques

Conditions préalables à la connexion

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, un émetteur-récepteur 100GBASE- pour 100 gigabit Ethernet ou un 400GBASE- LR4 pour Ethernet 400 Gbit/s. LR4

Vous pouvez configurer une Direct Connect connexion à l'aide du AWS Direct Connect Resiliency Toolkit ou d'une connexion classique de l'une des manières suivantes :

Modèle	Bande passante	Method
Connexion dédiée	1 Gbit/s, 10 Gbit/s, 100 Gbit/s et 400 Gbit/s	Travaillez avec un 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 Direct Connect emplacement. Le fournisseur de réseau n'a pas besoin d'être un AWS Direct Connect partenaire pour vous connecter à une connexion dédiée. Direct Connect les connexions dédiées prennent en charge ces vitesses de port sur fibre monomode : 1 Gbit/s : 1000BASE-LX (1310 nm), 10 Gbit/s : 10GBASE-LR (1310 nm), 100 Gbit/s : 100GBASE- ou 400GBASE-

Modèle	Bande passante	Method
		pour 400 Gbit/s Ethernet. LR4 LR4
Connexion hébergée	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.	Travaillez avec un AWS Direct Connect partenaire du programme de partenari at pour connecter un routeur de votre centre de données, de votre bureau ou de votre environnement de colocation à un Direct Connect emplaceme nt. Seuls certains partenaires offrent des connexions de capacité plus élevée.

Pour les connexions 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 monomode avec un émetteur-récepteur 1000BASE-LX (1310 nm) pour 1 gigabit Ethernet, un émetteur-récepteur 10GBASE-LR (1310 nm) pour 10 gigabits, un émetteur-récepteur 100GBASE- pour 100 gigabit Ethernet ou un 400GBASE- LR4 pour 400 Gbit/s Ethernet. LR4
- Selon le point de terminaison AWS Direct Connect servant votre connexion, la négociation automatique des appareils sur site devra peut-être être activée ou désactivée pour toute connexion dédiée. Si une interface virtuelle reste inactive alors qu'une connexion Direct Connect est établie, voirRésoudre les problèmes liés à la couche 2 (liaison de données).
- L'encapsulation VLAN 802.1Q doit être prise en charge sur l'ensemble de la connexion, y compris les périphériques intermédiaires.
- Votre appareil doit prendre en charge le protocole BGP (Border Gateway Protocol) et l'authentification BGP MD5 .
- (Facultatif) Vous pouvez configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau. Le BFD asynchrone est automatiquement activé pour chaque 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 si vous ne créez pas de connexion classique. Pour les options de connexion au AWS Direct Connect Resiliency Toolkit, consultez leAWS Direct Connect Boîte à outils de résilience.
- La vitesse, l'emplacement et le partenaire pour toutes vos connexions.

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

AWS Direct Connect Boîte à outils de résilience

AWS offre aux clients la possibilité 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 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.
- Crée des groupes d'agrégation de liens (LAGs) et ajoute le nombre approprié de connexions dédiées LAGs lorsque vous choisissez une vitesse autre que 1 Gbit/s, 10 Gbit/s, 100 Gbit/s ou 400 Gbit/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 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 de plus amples informations, veuillez consulter the section called “Test de basculement avec Direct Connect”.
- Fournit des CloudWatch métriques Amazon pour les connexions et les interfaces virtuelles. Pour de plus amples informations, veuillez consulter Surveillez les ressources Direct Connect.

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

Modèles de résilience disponibles

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

- 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 Direct Connect.

- 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 Direct Connect.
- Développement et test : ce modèle vous permet de développer et de tester la résilience pour les charges de travail non critiques, en utilisant des connexions distinctes qui se terminent sur des appareils distincts situés au même endroit.

La meilleure pratique consiste à utiliser l'assistant de connexion du AWS Direct Connect Resiliency Toolkit pour atteindre votre objectif de SLA.

> **Note**
>
> Si vous ne souhaitez pas créer de modèle de résilience à l'aide du AWS Direct Connect Resiliency Toolkit, vous pouvez créer une connexion classique. Pour plus d'informations sur les connexions classiques, consultezConnexion classique.

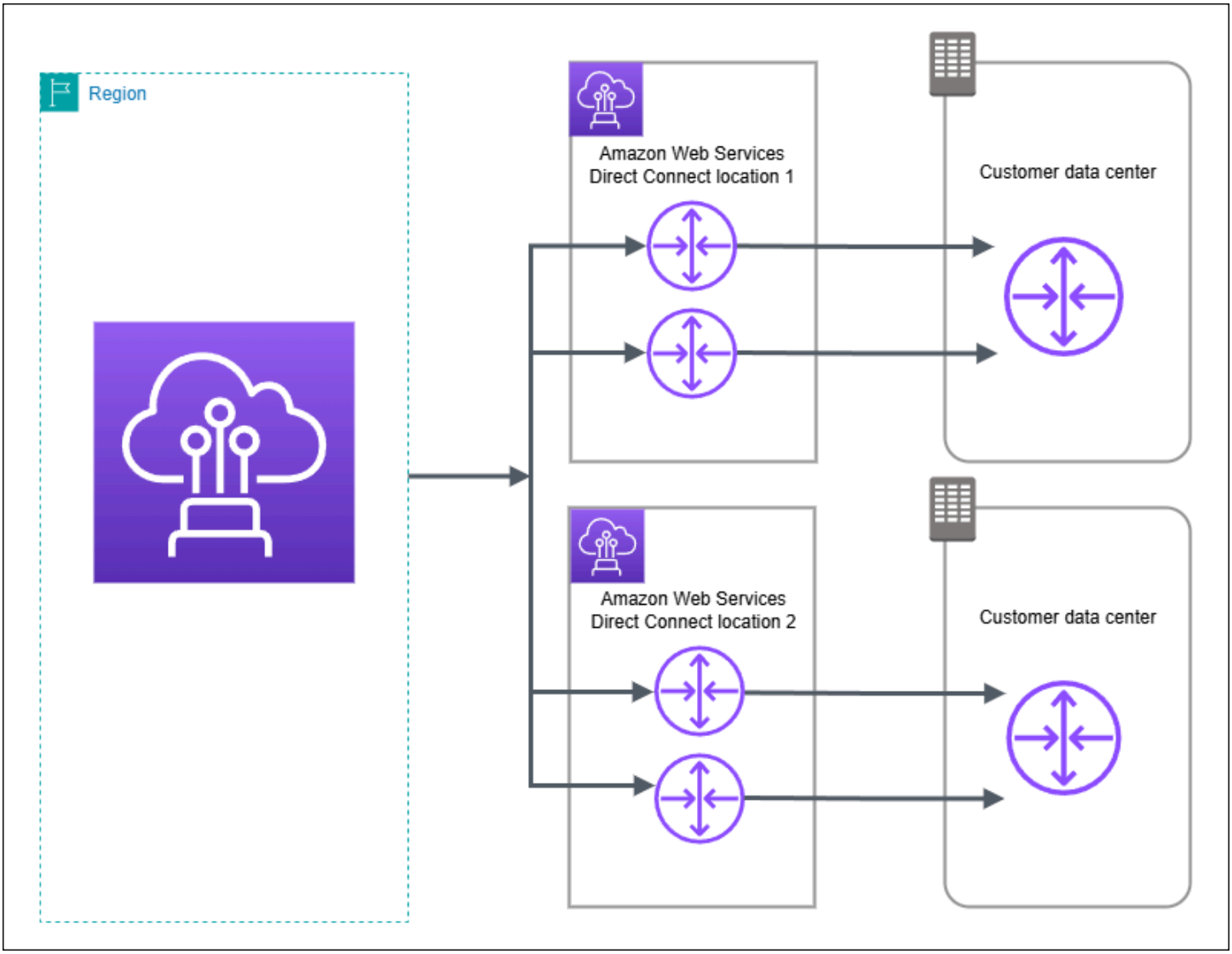
AWS Direct Connect Conditions préalables du Resiliency Toolkit

Notez les informations suivantes avant de commencer votre configuration :

- Familiarisez-vous avec leConditions préalables à la connexion.
- Le modèle de résilience disponible que vous souhaitez utiliser.

Résilience maximale

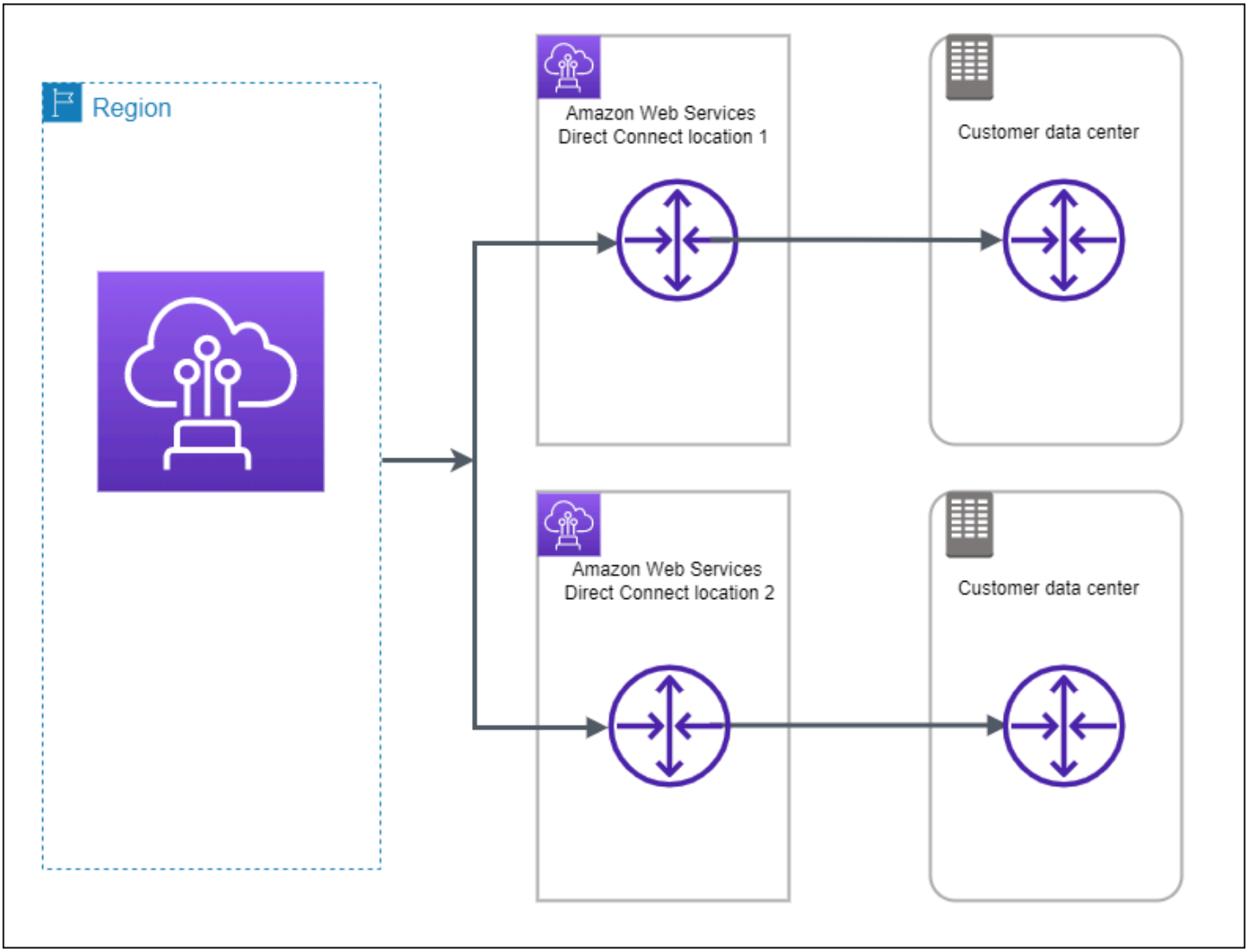
Vous pouvez obtenir une résilience maximale pour les charges de travail critiques en utilisant des connexions distinctes qui se terminent sur des appareils distincts dans plusieurs emplacements (comme illustré dans la figure suivante). Ce modèle offre une résilience contre les défaillances de l'appareil,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



Pour la procédure d'utilisation du AWS Direct Connect Resiliency Toolkit afin de configurer un modèle de résilience maximale, voir. Configurer une résilience maximale

Haute résilience

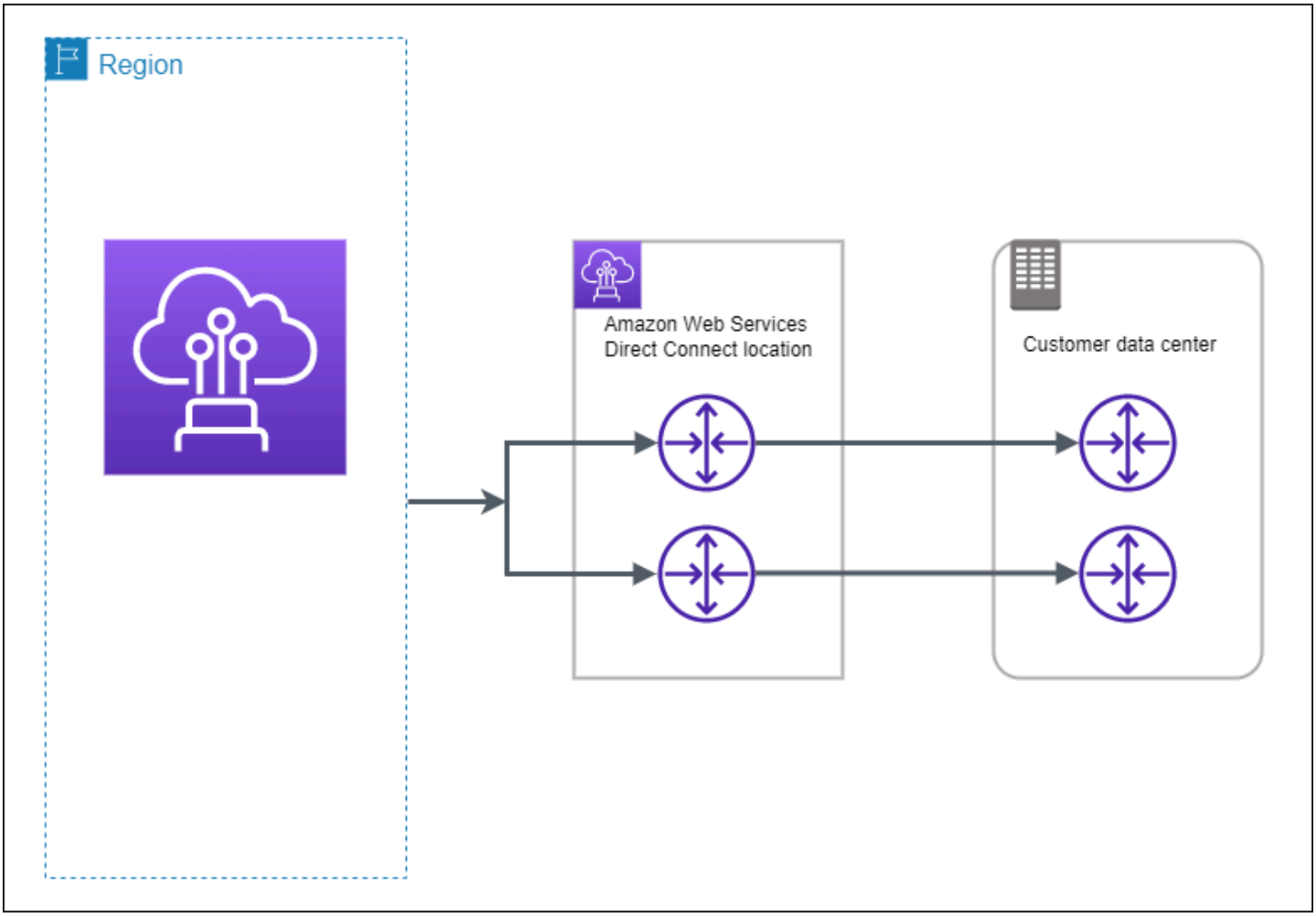
Vous pouvez obtenir une haute résilience pour les charges de travail critiques en utilisant deux connexions simples à plusieurs emplacements (comme illustré dans la figure suivante). Ce modèle offre une résilience contre les défaillances de connectivité provoquées par une coupure de fibre ou une défaillance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



Pour la procédure d'utilisation du AWS Direct Connect Resiliency Toolkit afin de configurer un modèle de haute résilience, voir. Configuration d'une résilience élevée

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.



Pour la procédure d'utilisation du AWS Direct Connect Resiliency Toolkit afin de configurer un modèle de résilience maximale, voir. Configuration du développement et de la résilience des tests

AWS Direct Connect FailoverTest

Utilisez le AWS Direct Connect Resiliency Toolkit pour vérifier les itinéraires de trafic et vérifier que ces itinéraires répondent à vos exigences de résilience.

Pour les procédures d'utilisation du AWS Direct Connect Resiliency Toolkit pour effectuer des tests de basculement, voir. Test de basculement avec Direct Connect

Configurez Direct Connect pour une résilience maximale avec le Resiliency AWS Direct Connect Toolkit

Dans cet exemple, le Direct Connect Resiliency Toolkit est utilisé pour configurer un modèle de résilience maximale

Tâches

- Étape 1 : Inscrivez-vous à AWS
- Étape 2 : Configurer le modèle de résilience
- Étape 3 : Créer vos interfaces virtuelles
- Étape 4 : Vérifier la configuration de résilience de votre interface virtuelle
- Étape 5 : Vérifier la connectivité de vos interfaces virtuelles

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

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

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape 2 : Configurer le modèle de résilience

Pour configurer un modèle de résilience maximale

1. Ouvrez la Direct Connectconsole sur 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' 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'établissement dispose de salles de réunion (MMRs) réparties 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' 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'établissement dispose de salles de réunion (MMRs) réparties 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 vous LOAs êtes prêt, vous pouvez choisir Télécharger le LOA, puis cliquer sur Continuer.

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures ouvrables. 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 d'entre elles VPCs.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La 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 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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.

Ressource	Informations obligatoires
	• IPv4: • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques dont vous êtes propriétaire. La valeur peut être l'une des suivantes : • Un CIDR appartenant au client IPv4 Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais 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 `/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 le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande) **Note** Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé CIDRs pour l'interface de votre routeur et pour l'interfa ce 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

Ressource	Informations obligatoires
	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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.
Famille d'adresses	Si la session de peering BGP sera terminée 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 32 bits, la valeur doit être comprise entre 1 et 4294967294. 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Ils CIDRs viennent 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.
	• Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6
	• 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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'appliquent uniquement aux itinéraires propagés à partir de. 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 Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ASNs appartiennent à un fournisseur de services Internet ou à un opérateur de réseau, nous vous demandons des informations supplémentaires. Il peut s'agir d'un document utilisant le papier à en-tête officiel de l'entreprise ou d'un e-mail provenant du nom de domaine de l'entreprise confirmant que vous prefix/ASN pouvez utiliser le réseau.

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

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

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

6. Sous Paramètres supplémentaires, procédez comme suit :

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

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

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

   c. Pour publier des préfixes sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, dans le champ IP homologue de votre routeur, entrez l'adresse IPv4 CIDR de destination vers laquelle Amazon doit envoyer le trafic.

- Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IPv4 CIDR à utiliser pour envoyer AWS le trafic.

  > **Important**
  >
  > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
  >
  > - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour de plus amples informations, veuillez consulter the section called “Test de basculement avec Direct Connect”.

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' 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 Amazon Linux AMIs sont disponibles dans l'onglet Quick Start 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. Envoyez un ping à IPv4 l'adresse privée et obtenez une réponse.

Configurez Direct Connect pour une résilience élevée avec le Resiliency AWS Direct Connect Toolkit

Dans cet exemple, le Direct Connect Resiliency Toolkit est utilisé pour configurer un modèle à haute résilience

Tâches

- Étape 1 : Inscrivez-vous à AWS
- Étape 2 : Configurer le modèle de résilience
- Étape 3 : Créer vos interfaces virtuelles
- Étape 4 : Vérifier la configuration de résilience de votre interface virtuelle
- Étape 5 : Vérifier la connectivité de vos interfaces virtuelles

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

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

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape 2 : Configurer le modèle de résilience

Pour configurer un modèle de haute résilience

1. Ouvrez la Direct Connectconsole sur 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' 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'établissement dispose de salles de réunion (MMRs) réparties 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' 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'établissement dispose de salles de réunion (MMRs) réparties 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 vous LOAs êtes prêt, vous pouvez choisir Télécharger le LOA, puis cliquer sur Continuer.

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures ouvrables. 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 VPCs.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La 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 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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.

Ressource	Informations obligatoires
	• IPv4: • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques que vous possédez. La valeur peut être l'une des suivantes : • Un CIDR appartenant au client IPv4 Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais 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 `/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 le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande) **Note** Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé CIDRs 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

Ressource	Informations obligatoires
	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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.
Famille d'adresses	Si la session de peering BGP sera terminée 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 32 bits, la valeur doit être comprise entre 1 et 4294967294. 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Ils CIDRs viennent 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.
	• Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6
	• 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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'appliquent uniquement aux itinéraires propagés à partir de. 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 Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ou si vous ASNs appartenez à un fournisseur de services Internet ou à un opérateur de réseau, vous AWS demande des informations supplémentaires. Il peut s'agir d'un document utilisant le papier à en-tête officiel de l'entreprise ou d'un e-mail provenant du nom de domaine de l'entreprise confirmant que vous prefix/ASN pouvez utiliser le réseau.

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

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

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

6. Sous Paramètres supplémentaires, procédez comme suit :

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

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

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

   c. Pour publier des préfixes sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, dans le champ IP homologue de votre routeur, entrez l'adresse IPv4 CIDR de destination vers laquelle Amazon doit envoyer le trafic.

- Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IPv4 CIDR à utiliser pour envoyer AWS le trafic.

  > **Important**
  >
  > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
  >
  > - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour de plus amples informations, veuillez consulter the section called "Test de basculement avec Direct Connect".

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' 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 Amazon Linux AMIs sont disponibles dans l'onglet Quick Start 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. Envoyez un ping à IPv4 l'adresse privée et obtenez une réponse.

Configurez AWS Direct Connect pour le développement et testez la résilience avec le Resiliency AWS Direct Connect Toolkit

Dans cet exemple, le Direct Connect Resiliency Toolkit est utilisé pour configurer un modèle de résilience de développement et de test

Tâches

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

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

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape 2 : Configurer le modèle de résilience

Pour configurer le modèle de résilience

1. Ouvrez la Direct Connectconsole sur 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' 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'établissement dispose de salles de réunion (MMRs) réparties 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 vous LOAs êtes prêt, vous pouvez choisir Télécharger le LOA, puis cliquer sur Continuer.

   L'examen de votre demande et la mise en place AWS d'un port pour votre connexion peuvent prendre jusqu'à 72 heures ouvrables. 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 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 d'entre elles VPCs.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La 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.

Ressource	Informations obligatoires
(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 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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.
	
	• IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR appartenant au client IPv4
	
	  Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais 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 `/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 le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande)

Ressource	Informations obligatoires
	Note Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé uniquement CIDRs pour l'interface de votre routeur et pour l'interface AWS Direct Connect. 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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.
Famille d'adresses	Si la session de peering BGP sera terminée 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 32 bits, la valeur doit être comprise entre 1 et 4294967294. 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Ils CIDRs viennent 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.
	• Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6
	• 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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'appliquent uniquement aux itinéraires propagés à partir de. 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 Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Si vos préfixes publics ASNs appartiennent à un fournisseur de services Internet ou à un opérateur de réseau, nous vous demandons des informations supplémentaires. Il peut s'agir d'un document utilisant le papier à en-tête officiel de l'entreprise ou d'un e-mail provenant du nom de domaine de l'entreprise confirmant que vous prefix/ASN pouvez utiliser le réseau.

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

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

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

6. Sous Paramètres supplémentaires, procédez comme suit :

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

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

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

   c. Pour publier des préfixes sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

      - Pour spécifier vous-même ces adresses IP, dans le champ IP homologue de votre routeur, entrez l'adresse IPv4 CIDR de destination vers laquelle Amazon doit envoyer le trafic.

- Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IPv4 CIDR à utiliser pour envoyer AWS le trafic.

  > **Important**
  >
  > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
  >
  > - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 Amazon VPC, effectuez un test de basculement de l'interface virtuelle pour vérifier que votre configuration répond à vos exigences de résilience. Pour de plus amples informations, veuillez consulter the section called “Test de basculement avec Direct Connect”.

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' 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 Amazon Linux AMIs sont disponibles dans l'onglet Quick Start 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. Envoyez un ping à IPv4 l'adresse privée et obtenez une réponse.

Direct Connect Test de basculement

Les modèles de AWS Direct Connect résilience du Resiliency Toolkit sont conçus pour garantir que vous disposez du nombre approprié de connexions d'interface virtuelle sur plusieurs sites. Après avoir terminé l'assistant, utilisez le test de basculement du AWS Direct Connect Resiliency Toolkit

pour arrêter la session de peering 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 de peering BGP et la durée du test. AWS place la session d'appairage BGP de l'interface virtuelle sélectionnée dans l'état inactif. 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 l'arrêtez manuellement, la session BGP est AWS rétablie. Une fois le test terminé, vous pouvez utiliser le AWS Direct Connect Resiliency Toolkit 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 au bout de 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 de plus amples informations, veuillez consulter the section called “Afficher l'historique des tests de basculement d'une 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 titulaire du compte reçoit une indication indiquant AWS CloudTrail qu'un test a été effectué sur une interface virtuelle.

Rubriques

- Lancer un test de basculement de l'interface virtuelle du AWS Direct Connect Resiliency Toolkit
- Afficher l'historique des tests de basculement de l'interface virtuelle AWS Direct Connect Resiliency Toolkit
- Arrêter un test de basculement de l'interface virtuelle du AWS Direct Connect Resiliency Toolkit

Lancer un test de basculement de l'interface virtuelle du AWS Direct Connect Resiliency Toolkit

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

Pour démarrer le test de basculement de l'interface virtuelle depuis la console Direct Connect

1. Ouvrez la Direct Connectconsole sur 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 que les peerings soient réduits en test, choisissez par exemple les sessions de peering à tester. IPv4

   b. Pour Durée maximale du test, saisissez la durée du test en minutes.

      La valeur maximale est de 4 320 minutes (72 heures ouvrables).

      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 du AWS CLI

Utilisez StartBgpFailoverTest.

Afficher l'historique des tests de basculement de l'interface virtuelle AWS Direct Connect Resiliency Toolkit

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

Pour consulter l'historique des tests de basculement de l'interface virtuelle depuis la console Direct Connect

1. Ouvrez la Direct Connectconsole sur 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 consulter l'historique des tests de basculement de l'interface virtuelle à l'aide du AWS CLI

Utilisez ListVirtualInterfaceTestHistory.

Arrêter un test de basculement de l'interface virtuelle du AWS Direct Connect Resiliency Toolkit

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

Pour arrêter le test de basculement de l'interface virtuelle depuis la console Direct Connect

1. Ouvrez la Direct Connectconsole sur 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 de peering BGP. L'historique des tests affiche « annulé » pour le test.

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

Utilisez StopBgpFailoverTest.

Direct Connect Connexion classique

Une connexion classique offre une approche simple pour établir une connectivité réseau dédiée entre votre infrastructure sur site et AWS. Ce type de connexion est idéal pour les entreprises qui préfèrent gérer leurs propres configurations réseau et disposer d'une infrastructure Direct Connect existante. La connexion classique ne repose pas sur le AWS Direct Connect Resiliency Toolkit.

Sélectionnez Classique lorsque vous avez des connexions existantes et que vous souhaitez ajouter des connexions supplémentaires. Une connexion classique est assortie d'un SLA de 95 %. Cependant, il ne fournit ni résilience ni redondance, qui ne se trouvent que dans le AWS Direct Connect Resiliency Toolkit lors de la création d'une connexion.

> **Note**
>
> Avant de configurer une connexion classique, familiarisez-vous avec leConditions préalables à la connexion.

Tâches

- Configuration d'une connexion Direct Connect classique

Configuration d'une connexion Direct Connect classique

Configurez une connexion classique lorsque vous disposez de connexions Direct Connect existantes.

Étape 1 : Inscrivez-vous à AWS

Pour l'utiliser 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

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

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape 2 : demander une connexion Direct Connect dédiée

Pour les connexions dédiées, vous pouvez soumettre une demande de connexion à l'aide de la 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.
- Direct Connect Emplacement auquel la connexion doit être interrompue.

> **Note**
>
> Vous ne pouvez pas utiliser la 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 Direct Connect connexion

1. Ouvrez la Direct Connectconsole sur 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 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'établissement dispose de salles de réunion (MMRs) réparties sur 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 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 ouvrables. 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 de plus amples informations, veuillez consulter Direct Connect connexions dédiées et hébergées.

Accepter votre connexion hébergée

Vous devez accepter la connexion hébergée dans la 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 Direct Connectconsole sur 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 Direct Connectconsole sur 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. S'il n'est toujours pas disponible ou si vous n'avez pas reçu d'e-mail après 72 heures ouvrables, contactez le AWS Support.

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. 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 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.

Direct Connect les sites répertoriés comme plusieurs sites (par exemple, Equinix DC1 - DC6 & DC1 0-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 Direct Connect lieu unique. Pour bénéficier de la haute disponibilité, configurez des connexions vers différents emplacements Direct Connect .

Si vous ou votre fournisseur de réseau rencontrez des problèmes pour établir une connexion physique, consultez Résoudre les problèmes (physiques) liés à la couche 1.

Étape 4 : Créer une interface virtuelle

Pour commencer à utiliser votre 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 d'entre elles VPCs.

Avant de commencer, veillez à disposer des informations suivantes :

Ressource	Informations obligatoires
Connection	La 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

Ressource	Informations obligatoires
	conforme à la norme Ethernet 802.1Q. Cette balise est obligatoire pour tout trafic traversant la connexion 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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.
	
	• IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques que vous possédez. La valeur peut être l'une des suivantes :
	  • Un CIDR appartenant au client IPv4
	
	  Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais 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 `/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 le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande)

Ressource	Informations obligatoires
	Note Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé uniquement CIDRs pour l'interface de votre routeur et pour l'interface AWS Direct Connect. 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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.
Famille d'adresses	Si la session de peering BGP sera terminée 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 32 bits, la valeur doit être comprise entre 1 et 4294967294. 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Ils CIDRs viennent 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.
	• Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6
	• 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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'appliquent uniquement aux itinéraires propagés à partir de. 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 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 ASNs appartiennent à un fournisseur de services Internet ou à un opérateur de réseau. Il peut s'agir d'un document utilisant un en-tête officiel de l'entreprise ou d'un e-mail provenant du nom de domaine de l'entreprise confirmant que vous pouvez utiliser le réseau prefix/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. Le MTU d'une interface virtuelle privée peut être de 1500 ou 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 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 ouvrables.

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

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.
6. Sous Paramètres supplémentaires, procédez comme suit :

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

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

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

c. Pour publier des préfixes sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

   [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

   > **Important**
   >
   > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
   >
   > - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 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 Direct Connectconsole sur 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 Direct Connect:

Pour plus d'informations sur la configuration manuelle de votre routeur, consultezTélécharger le fichier 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' Direct Connect appareil, consultezRésoudre les problèmes liés à la couche 2 (liaison de données). Si vous pouvez pinger l'adresse IP d'appairage, consultez Résoudre les problèmes liés à la couche 3/4 (réseau/transport). Si la session d'appairage BGP est établie, mais que vous ne parvenez pas à acheminer le trafic, consultez Résoudre les 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

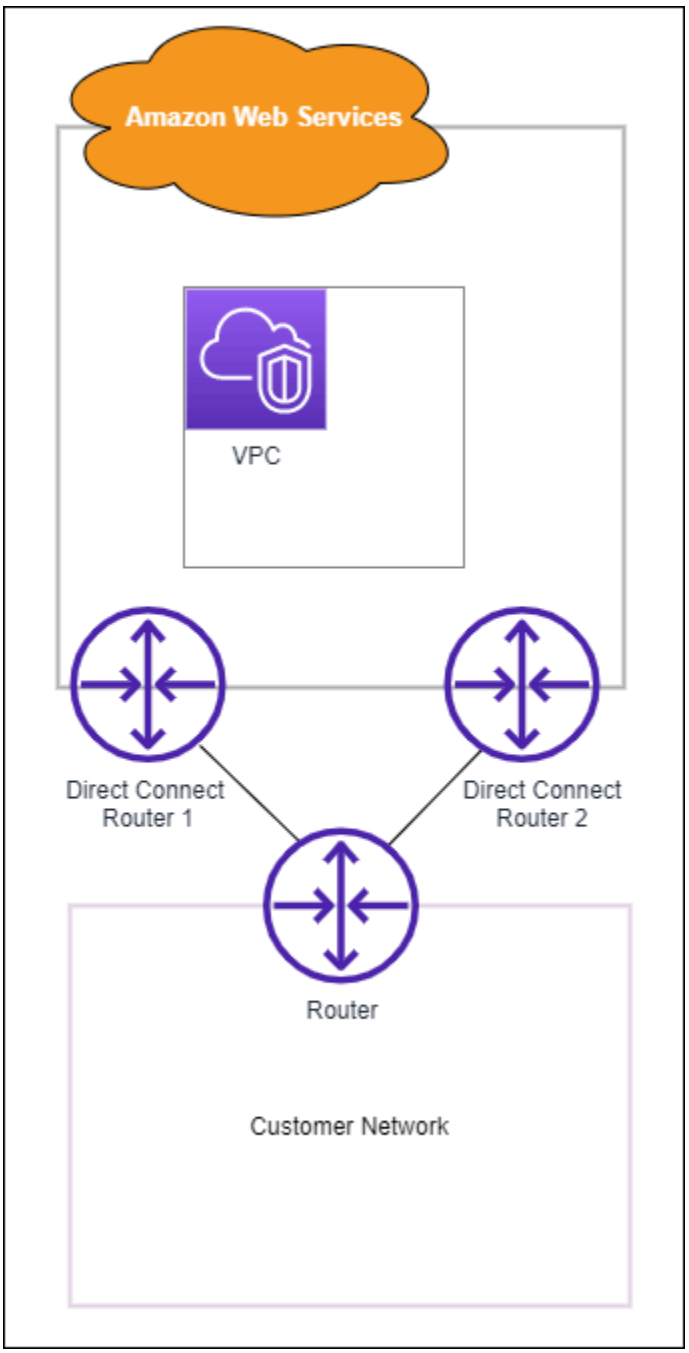
- Exécutez `traceroute` et vérifiez que l' Direct Connect identifiant figure dans la trace réseau.

Pour vérifier votre connexion d'interface virtuelle et d'interface à Amazon VPC

1. À l'aide d'une AMI pingable, telle qu'une AMI Amazon Linux, lancez une EC2 instance dans le VPC connecté à votre passerelle privée virtuelle. Les Amazon Linux AMIs sont disponibles dans l'onglet Quick Start lorsque vous utilisez l'assistant de lancement d'instance dans la EC2 console Amazon. Pour plus d'informations, consultez la section Lancer une instance dans le guide de EC2 l'utilisateur Amazon. Vérifiez que le groupe de sécurité associé à l'instance inclut une règle autorisant le trafic ICMP entrant (pour la requête ping).
2. Une fois l'instance en cours d'exécution, obtenez son IPv4 adresse privée (par exemple, 10.0.0.4). La EC2 console Amazon affiche l'adresse dans le cadre des détails de l'instance.
3. Envoyez un ping à IPv4 l'adresse privée 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. 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 Direct Connect sites.

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

Direct Connect entretien

Direct Connect s'engage à garantir la sécurité, la disponibilité et l'évolutivité des services. Pour maintenir ces normes, une maintenance périodique est requise sur les périphériques réseau matériels. La maintenance Direct Connect est divisée en deux types : planifiée et d'urgence.

Ces événements de maintenance consistent notamment à corriger les vulnérabilités de sécurité, les problèmes matériels, à effectuer des migrations d'appareils pour se conformer aux normes, à corriger les défauts et à proposer de nouvelles fonctionnalités. En suivant les pratiques décrites dansPréparation des événements de maintenance, vous pouvez mieux préparer votre environnement Direct Connect afin d'éviter les interruptions lors d'événements de maintenance. Si vous disposez d'une configuration réseau non résiliente ou d'une connexion unique, vous subirez une interruption de la connectivité entre votre réseau local et AWS les ressources.

Direct Connect envoie des notifications par e-mail concernant les événements de maintenance planifiés et d'urgence à l'adresse e-mail associée au AWS compte propriétaire de la connexion Direct Connect ou de la ressource d'interface virtuelle. Si vous utilisez une connexion hébergée Direct Connect avec l'un des partenaires de livraison Direct Connect, des notifications par e-mail sont envoyées à vous et au compte du partenaire concernant l'événement de maintenance. Vous pouvez également ajouter des adresses e-mail ou des listes de distribution supplémentaires pour recevoir des notifications. Voir Mettre à jour les contacts alternatifs associés à votre AWS compte pour plus d'informations.

Événements de maintenance

- Maintenance planifiée Direct Connect
- Maintenance d'urgence Direct Connect
- Maintenance par des tiers
- Préparation des événements de maintenance
- Demandes de report ou d'annulation d'un événement de maintenance

Maintenance planifiée Direct Connect

Les événements de maintenance planifiés impliquent des mises à niveau du réseau, telles que l'application de correctifs au système d'exploitation et des mises à jour de configuration sur les terminaux matériels, nécessaires pour améliorer la disponibilité et fournir de nouvelles fonctionnalités.

Ces événements de maintenance sont planifiés 14 jours à l'avance et se produisent généralement pendant une période de quatre heures, pendant les heures de faible trafic, sur le site Direct Connect où se trouve le point de terminaison de l'appareil. Les activités de maintenance se terminent généralement avant l'expiration du délai complet de quatre heures et vous recevrez une notification une fois les travaux terminés. Dans de rares cas où des circonstances imprévues nécessitent une prolongation de la période de maintenance, nous enverrons une notification séparée avec l'estimation d'achèvement révisée.

Selon le calendrier suivant, les notifications initiales et les notifications de rappel sont envoyées au AWS compte propriétaire de la ressource :

- 14 jours civils avant l'événement de maintenance prévu,
- 7 jours civils avant l'événement de maintenance prévu, et
- 1 jour avant l'événement de maintenance prévu.

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

En outre,

- Recevez des notifications dans votre système de surveillance ou de billetterie en intégrant à AWS Health. Pour l'intégrer AWS Health, consultez la section Surveillance des événements AWS Health avec Amazon EventBridge dans le guide de AWS Health l'utilisateur.
- Consultez les calendriers de maintenance planifiés sur votre Tableau de bord Health.

Dans de rares circonstances, un événement de maintenance planifié ne peut pas se produire comme prévu. Dans ce cas, nous enverrons une notification d'annulation et reprogrammerons l'événement dans le futur en suivant le même processus que ci-dessus.

Maintenance d'urgence Direct Connect

Les événements de maintenance d'urgence sont déclenchés de manière critique afin de prévenir les événements imminents ayant un impact sur le service ou de résoudre les défaillances qui ont déjà entraîné une interruption de la connectivité. Dans de tels cas, il est nécessaire de prendre des mesures immédiates pour rétablir l'état sain du terminal concerné.

Bien que nous nous efforcions de fournir un préavis dans la mesure du possible, certaines situations peuvent nécessiter un démarrage immédiat de la maintenance. Vous recevrez des notifications lorsque la maintenance d'urgence est planifiée ou en cours, et de nouveau lorsqu'elle sera terminée.

Ces événements se produisent généralement pendant une fenêtre de deux heures sur le site Direct Connect où se trouve le point de terminaison de l'appareil. Les activités de maintenance se terminent généralement dans cette fenêtre. Dans les cas où des circonstances imprévues nécessitent une prolongation de la période de maintenance, comme le remplacement du matériel, nous enverrons une notification séparée avec l'estimation d'achèvement révisée.

Maintenance par des tiers

Au-delà des événements de maintenance AWS déclenchés, votre partenaire de livraison Direct Connect ou votre fournisseur de services réseau qui fournit une connectivité réseau entre votre site et le site Direct Connect peut effectuer des activités de maintenance. Les partenaires de livraison Direct Connect reçoivent des notifications d'événements de AWS maintenance qui leur permettent de planifier leurs propres programmes de maintenance afin d'éviter les chevauchements. AWS n'a aucune visibilité sur les activités de maintenance d'un partenaire. Vous devrez donc vérifier auprès de celui-ci son processus de planification, ses méthodes de notification et ses meilleures pratiques.

Préparation des événements de maintenance

Pour garantir que les charges de travail de production continuent de fonctionner pendant un événement de maintenance, Direct Connect vous recommande d'utiliser le kit de résilience AWS Direct Connect pour configurer vos connexions réseau afin d'obtenir une résilience maximale. Pour un exemple de modèle de résilience maximale, voirRésilience maximale.

Grâce à une résilience maximale, les connexions sont réparties sur au moins deux sites Direct Connect, avec une terminaison sur deux points de terminaison uniques au sein de chaque site Direct Connect. Cela fournit plusieurs niveaux de redondance, ce qui réduit le risque de défaillance d'un seul terminal et aide à maintenir la connectivité pendant les événements de maintenance. Direct Connect ne planifiera jamais un événement de maintenance planifié qui interromprait simultanément vos connexions redondantes. Pour connaître les étapes d'utilisation du AWS Direct Connect Resiliency Toolkit afin de configurer une résilience maximale, voir. Configurer une résilience maximale

Lors d'un événement de maintenance planifié, Direct Connect draine le trafic vers et depuis le point de terminaison de connexion en cours de maintenance et oblige le trafic à utiliser vos connexions

redondantes. Cela permet un réacheminement plus fluide du trafic réseau sans intervention manuelle si la résilience maximale n'est pas configurée. Vous pouvez également choisir de contrôler le réacheminement du trafic entre les connexions redondantes pendant les fenêtres de maintenance en utilisant les communautés BGP (Border Gateway Protocol) locales privilégiées. Pour plus d'informations sur les communautés BGP, consultezStratégies de routage et communautés BGP (Border Gateway Protocol).

La configuration de votre environnement Direct Connect avec le modèle de résilience maximale permet de garantir que votre activité ne soit pas affectée lors d'événements de maintenance ou de défaillances d'infrastructure. Lorsqu'ils sont correctement mis en œuvre et testés, vous n'avez généralement pas besoin de prendre de mesures pour ces événements de maintenance.

Validation de la résilience

Si vous avez configuré votre environnement Direct Connect de manière à ce qu'il soit résilient, vérifiez régulièrement que votre trafic passe par d'autres connexions redondantes lorsqu'une connexion l'estout-of-service. Des tests proactifs réguliers peuvent aider à identifier et à résoudre les problèmes potentiels avant qu'ils n'affectent les charges de travail de production lors d'un événement de maintenance réel ou d'un scénario de défaillance. Cela garantira une plus grande confiance dans la fiabilité de votre réseau lors d'un événement de maintenance. Utilisez le test Direct Connect Failover pour valider la résilience de vos connexions redondantes. Pour connaître les étapes à suivre pour utiliser le test Direct Connect Failover, reportez-vous Test de basculement avec Direct Connect à la section.

Vous pouvez également tirer parti d'Amazon CloudWatch Network Monitor pour surveiller activement vos connexions Direct Connect. Pour plus d'informations, consultez Surveiller la connectivité hybride avec Amazon CloudWatch Network Synthetic Monitor.

Demandes de report ou d'annulation d'un événement de maintenance

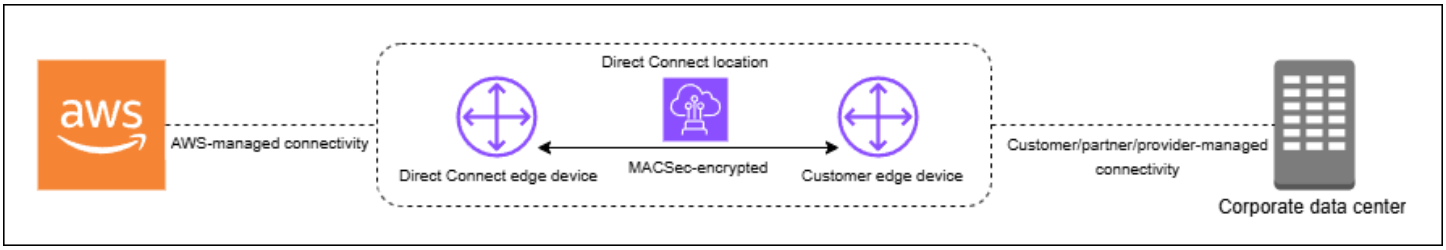
Les appareils Direct Connect sont partagés entre plusieurs clients. Par conséquent, nous ne répondons pas aux demandes spécifiques de reprogrammation ou d'annulation de maintenance. Les demandes de report ou d'annulation d'un client peuvent avoir un impact négatif sur les autres clients utilisant ce point de terminaison. Cela peut également présenter un risque pour atténuer les problèmes de disponibilité ou de sécurité en temps opportun.

Sécurité MAC dans Direct Connect

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, fonctionnant entre deux routeurs de couche 3. Tout en MACsec sécurisant la connexion entre votre routeur et l'emplacement Direct Connect au niveau de la couche 2, il AWS fournit une sécurité supplémentaire en chiffrant toutes les données au niveau de la couche physique lorsqu'elles circulent sur le réseau entre les Direct Connect sites et AWS les régions. Cela crée une approche de sécurité à plusieurs niveaux dans laquelle votre trafic est protégé à la fois lors de l'entrée initiale dans le AWS réseau AWS et pendant son transit sur celui-ci.

Dans le schéma suivant, l' Direct Connect interconnexion doit être connectée à une interface MACsec compatible sur le périphérique périphérique du client. MACsec over Direct Connect fournit un chiffrement de couche 2 pour le point-to-point trafic entre le périphérique Direct Connect et le périphérique périphérique du client. Ce chiffrement a lieu une fois que les clés de sécurité ont été échangées et vérifiées entre les interfaces situées aux deux extrémités de la connexion croisée.

> **Note**
>
> MACsec assure point-to-point la sécurité des liaisons Ethernet ; par conséquent, il ne fournit pas de end-to-end chiffrement sur plusieurs segments de réseau Ethernet séquentiels ou sur d'autres segments de réseau.



MACsec concepts

Les concepts clés suivants sont les suivants MACsec :

- Sécurité MAC (MACsec) : norme IEEE 802.1 de couche 2 garantissant la confidentialité, l'intégrité des données et l'authenticité de l'origine des données. Pour plus d'informations sur le protocole, consultez 802.1AE : MAC Security () MACsec.

- Clé d'association sécurisée (SAK) : clé de session qui établit la MACsec connectivité entre le routeur local du client et le port de connexion sur le site Direct Connect. Le SAK n'est pas partagé au préalable, mais il est automatiquement dérivé de la CKN/CAK paire par le biais d'un processus de génération de clé cryptographique. Cette dérivation se produit aux deux extrémités de la connexion une fois que vous avez fourni et provisionné la CKN/CAK paire. Le SAK est régénéré périodiquement pour des raisons de sécurité et chaque fois qu'une MACsec session est établie.
- Nom de clé d'association de connectivité (CKN) et clé d'association de connectivité (CAK) : les valeurs de cette paire sont utilisées pour générer la MACsec clé. Vous générez les valeurs de paire, vous les associez à une Direct Connect connexion, puis vous les configurez sur votre appareil Edge à la fin de la Direct Connect connexion. Direct Connect prend uniquement en charge le mode CAK statique, mais pas le mode CAK dynamique. Étant donné que seul le mode CAK statique est pris en charge, il est recommandé de suivre vos propres politiques de gestion des clés pour la génération, la distribution et la rotation des clés.
- Format de clé — Le format de clé doit utiliser des caractères hexadécimaux, d'une longueur d'exactement 64 caractères. Direct Connect prend uniquement en charge les clés AES (Advanced Encryption Standard) 256 bits pour les connexions dédiées, ce qui correspond à une chaîne hexadécimale de 64 caractères.
- Modes de chiffrement — Direct Connect prend en charge deux modes de MACsec chiffrement :
  - must_encrypt — Dans ce mode, la connexion nécessite le MACsec chiffrement de l'ensemble du trafic. Si MACsec la négociation échoue ou si le chiffrement ne peut pas être établi, la connexion ne transmettra aucun trafic. Ce mode fournit la meilleure garantie de sécurité, mais peut avoir un impact sur la disponibilité en cas MACsec de problème connexe.
  - should_encrypt — Dans ce mode, la connexion tente d'établir le MACsec chiffrement mais revient à une communication non chiffrée en cas d'échec de la négociation. MACsec Ce mode offre une plus grande flexibilité et une meilleure disponibilité, mais peut autoriser le trafic non chiffré dans certains scénarios de défaillance.

  Le mode de chiffrement peut être défini lors de la configuration de la connexion et peut être modifié ultérieurement. Par défaut, les nouvelles connexions MACsec activées sont définies sur le mode « should_encrypt » afin d'éviter d'éventuels problèmes de connectivité lors de la configuration initiale.

MACsec rotation des touches

- Rotation CNN/CAK (manuelle)

Direct Connect MACsec prend en charge MACsec les porte-clés pouvant contenir jusqu'à trois CKN/CAK paires. Cela vous permet de faire pivoter manuellement ces touches à long terme sans interruption de connexion. Lorsque vous associez une nouvelle CKN/CAK paire à l'aide de la `associate-mac-sec-key` commande, vous devez configurer la même paire sur votre appareil. L'appareil Direct Connect tente d'utiliser la dernière clé ajoutée. Si cette clé ne correspond pas à celle de votre appareil, elle revient à la touche active précédente, garantissant ainsi la stabilité de la connexion pendant la rotation.

Pour plus d'informations sur l'utilisation`associate-mac-sec-key`, voir associate-mac-sec-key.

- Rotation de la clé d'association sécurisée (SAK) (automatique)

  Le SAK, qui est dérivé de la CKN/CAK paire active, est soumis à une rotation automatique basée sur les éléments suivants :

  - intervalles de temps
  - volume de trafic crypté
  - MACsec établissement de session

  Cette rotation est gérée automatiquement par le protocole, s'effectue de manière transparente sans perturber la connexion et ne nécessite aucune intervention manuelle. Le SAK n'est jamais stocké de manière persistante et est régénéré grâce à un processus de dérivation de clé sécurisé conforme à la norme IEEE 802.1X.

Connexions prises en charge

MACsec est disponible sur les connexions Direct Connect dédiées et les groupes d'agrégation de liens :

MACsec Connexions prises en charge

- Connexions dédiées
- LAGs
- Interconnexions entre partenaires

> **Note**
>
> Les partenaires utilisant des appareils compatibles peuvent chiffrer la connexion de couche 2 entre leur appareil réseau périphérique et l'appareil Direct Connect. MACsec Les partenaires qui activent cette fonctionnalité peuvent chiffrer tout le trafic passant par le lien sécurisé. MACsec le chiffrement fonctionne entre les deux appareils spécifiques de la couche 2 et n'est pas pris en charge sur les connexions hébergées.

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

Connexions dédiées

Les informations suivantes vous aideront à vous familiariser avec MACsec les connexions Direct Connect dédiées. Il n'y a pas de frais supplémentaires pour l'utilisation MACsec. Les étapes de configuration MACsec sur une connexion dédiée se trouvent dansCommencez avec MACsec une connexion dédiée.

Les opérations d'interconnexion des partenaires suivent les mêmes procédures que les connexions dédiées. Lorsque vous exécutez des commandes CLI ou SDK pour les interconnexions entre partenaires, les réponses incluent des informations MACsec connexes, le cas échéant.

MACsec prérequis pour les connexions dédiées

Notez les exigences suivantes pour MACsec les connexions non dédiées :

- MACsec est pris en charge sur les connexions Direct Connect dédiées à 10 Gbit/s, 100 Gbit/s et 400 Gbit/s à des points de présence sélectionnés. Pour ces connexions, les suites de MACsec chiffrement 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 et 400 Gbit/s, GCM-AES-XPN -256.
- Seules les MACsec clés 256 bits sont prises en charge.
- La numérotation étendue des paquets (XPN) est requise pour les connexions 100 Gbit/s et 400 Gbit/s. Pour les connexions 10 Gbit/s, Direct Connect prend en charge les protocoles GCM-AES-256 et -256. GCM-AES-XPN Les connexions haut débit, telles que les connexions dédiées de 100 Gbit/s et 400 Gbit/s, peuvent rapidement épuiser l'espace MACsec de numérotation des

paquets 32 bits d'origine, 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, l'amendement IEEE Std 802.1 AEbw -2013 a introduit la numérotation étendue des paquets, augmentant l'espace de numérotation à 64 bits, allégeant ainsi l'exigence 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 norme IEEE 802.1Q (point q/VLAN) tag offset/dot 1) n'q-in-clear est pas prise en charge pour déplacer une balise VLAN en dehors d'une charge utile chiffrée.

En outre, vous devez effectuer les tâches suivantes avant de procéder à MACsec la configuration sur une connexion dédiée.

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

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

LAGs

Les exigences suivantes vous aideront à vous familiariser avec MACsec les groupes d'agrégation de liens Direct Connect (LAGs) :

- LAGs doit être composé de connexions dédiées MACsec compatibles avec le chiffrement MACsec
- Toutes les connexions au sein d'un LAG doivent avoir la même bande passante et le même support MACsec
- MACsec la configuration s'applique uniformément à toutes les connexions du LAG
- Activation de la création de LAG et MACsec possibilité de le faire simultanément
- Une seule MACsec clé peut être utilisée à tout moment sur tous les liens LAG. La possibilité de prendre en charge plusieurs MACsec touches est uniquement destinée à la rotation des clés.

Interconnexions entre partenaires

Le compte partenaire propriétaire de l'interconnexion peut être utilisé MACsec sur cette connexion physique ou ce LAG. Les opérations sont les mêmes que pour les connexions dédiées, mais elles sont effectuées à l'aide des appels spécifiques au partenaire API/SDK .

Rôles liés à un service

Direct Connect utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. Direct Connect Les rôles liés au service sont prédéfinis par 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 Direct Connect car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Direct Connect définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Direct Connect peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM. Pour de plus amples informations, veuillez consulter the section called "Rôles liés à un service".

MACsec considérations CKN/CAK clés pré-partagées

AWS Direct Connect les utilisations AWS gérées CMKs pour les clés pré-partagées que vous associez aux connexions ou LAGs. Secrets Manager stocke vos paires CKN et CAK pré-partagées sous forme de secret chiffré par la clé racine du Secrets Manager. Pour plus d'informations, consultez la section « AWS géré » CMKs dans le guide du AWS Key Management Service développeur.

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.

Commencez à l'utiliser MACsec sur une Direct Connect connexion dédiée

La tâche suivante vous permet de commencer MACsec à configurer pour une utilisation sur une connexion dédiée Direct Connect

Étape 1 : Créer une connexion

Pour commencer à l'utiliser MACsec, vous devez activer la fonctionnalité lorsque vous créez une connexion dédiée.

(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 qui prend en charge. MACsec Pour plus d'informations, reportez-vous MACsec considérations à la section Création d'un LAG.

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

Après avoir créé la connexion ou le LAG qui prend en charge MACsec, vous devez CKN/CAK associer un à la connexion. Pour plus d'informations, consultez :

- Associer un MACsec CKN/CAK à une connexion
- Associer un MACsec CKN/CAK à un LAG

Étape 4 : configurer votre routeur sur site

Mettez à jour votre routeur local avec la clé MACsec secrète. La clé MACsec secrète du routeur local et celle de l' Direct Connect emplacement doivent correspondre. Pour de plus amples informations, veuillez consulter Télécharger le fichier de configuration du routeur.

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

Vous pouvez éventuellement supprimer l'association entre le CKN/CAK et la connexion ou le LAG. Si vous devez supprimer l'association, consultez l'une des rubriques suivantes :

- Supprimer l'association entre une clé MACsec secrète et une connexion
- Supprimer l'association entre une clé MACsec secrète et un LAG

Direct Connect connexions dédiées et hébergées

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

Il existe deux types de connexions :

- Connexion dédiée : connexion Ethernet physique associée à un seul client. Les clients peuvent demander une connexion dédiée via la Direct Connect console, la CLI ou l'API. Pour de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter Connexions hébergées.

Rubriques

Direct Connect Connexions dédiées

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

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 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 Direct Connect.

Vitesse du port

Les valeurs possibles sont 1 Gbit/s, 10 Gbit/s, 100 Gbit/s et 400 Gbit/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.

Une fois que vous avez demandé la connexion, nous mettons à votre disposition une lettre d'autorisation et d'attribution des installations de connexion (LOA-CFA) que vous pouvez télécharger ou vous envoyer par e-mail pour vous demander plus d'informations. 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 Direct Connect place, vous ne pouvez pas y commander de connexion croisée.

Les opérations suivantes sont disponibles pour les connexions dédiées :

- Créer une connexion à l'aide de l'assistant de connexion
- Créer une connexion classique
- the section called “Affichage des informations de connexion”
- the section called “Mise à jour d'une connexion”
- Associer un MACsec CKN/CAK à une connexion
- the section called “Supprimer l'association entre une clé MACsec secrète et une connexion”
- the section called “Supprimer une connexion”

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, consultez 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 de plus amples informations, veuillez consulter Interfaces virtuelles et interfaces virtuelles hébergées.

Si vous ne disposez d'aucun équipement sur un 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 Direct Connect.

Si vous souhaitez créer une connexion utilisant MAC Security (MACsec), passez en revue les conditions préalables avant de créer la connexion. Pour de plus amples informations, veuillez consulter the section called "MACsec prérequis pour les connexions dédiées".

Lettre d'autorisation et attribution d'une installation de raccordement (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.

Le LoA téléchargé est signé numériquement et filigrané pour valider l'authenticité du LoA émis par. AWS La signature numérique et le filigrane figurant dans le LoA. Le document PDF empêche le fournisseur d'installations sur les sites Direct Connect d'agir sur un LoA modifié ou potentiellement frauduleux. La signature numérique peut être authentifiée en ouvrant le PDF et en consultant le panneau de signature. Un document valide indiquera « La signature est valide » et « Le document n'a pas été modifié depuis que la signature a été appliquée ». Le filigrane reprend le panneau de brassage et les fils assignés sur le corps du LoA en tant qu'indicateur visuel, mais non sécurisé, de l'authenticité.

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.

Pour connaître les étapes à suivre pour télécharger le Loa-CFA, consultez. Télécharger la LOA-CFA

> **Note**
>
> Pour plus d'informations sur la tarification, consultez Tarification d'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 de plus amples informations, veuillez consulter Supprimer une Direct Connect connexion.

Rubriques

Créez une connexion Direct Connect dédiée 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 Direct Connect dédiée".

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

1. Ouvrez la Direct Connectconsole sur 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 the section called "AWS Direct Connect Boîte à outils de résilience".

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 Gbit/s à 400 Gbit/s.

   b. Pour Emplacement, choisissez l' 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 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 MACsec compatible.

      MACsec n'est disponible que sur des connexions dédiées.

   e. (Facultatif) Choisissez Ajouter une balise pour ajouter des key/value paires 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 "Lettre d'autorisation et attribution d'une installation de raccordement (LOA-CFA)".

Utilisez l'une des commandes suivantes.

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

Création d'une connexion Direct Connect classique

Pour les connexions dédiées, vous pouvez soumettre une demande de connexion à l'aide de la 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.
- Direct Connect Emplacement auquel la connexion doit être interrompue.

> **Note**
>
> Vous ne pouvez pas utiliser la 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 Direct Connect connexion

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Sur l'écran 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 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'établissement dispose de salles de réunion (MMRs) réparties sur 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 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 key/value paires 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 ouvrables. 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 de plus amples informations, veuillez consulter Connexions dédiées et hébergées.

Téléchargez le Direct Connect LOA-CFA

Vous pouvez télécharger le LOA-CFA à l'aide de la Direct Connect console ou de la ligne de commande. Une fois que vous avez téléchargé le LOA-CFA et que vous l'avez fourni à votre fournisseur de réseau ou de colocation, celui-ci peut commander la connexion croisée pour vous.

Pour télécharger la LOA-CFA

1. Ouvrez la Direct Connectconsole sur 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 de plus amples informations, veuillez consulter Demande de connexions croisées sur Direct Connect des sites.

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

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

Associer un MACsec CKN/CAK à une connexion Direct Connect

Après avoir créé la connexion qui prend en charge MACsec, vous pouvez CKN/CAK associer un à la connexion. Vous pouvez créer l'association à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

> **Note**
>
> Vous ne pouvez pas modifier une clé MACsec secrète 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 Supprimer l'association entre une clé MACsec secrète et une connexion.

Pour associer une MACsec clé à une connexion

1. Ouvrez la Direct Connectconsole sur 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. Entrez la MACsec clé.

   [Utiliser la CAK/CKN paire] Choisissez Key Pair, 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 MACsec secrète.
6. Choisissez Associer une clé.

Pour associer une MACsec clé à une connexion à l'aide de la ligne de commande ou de l'API

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

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

Vous pouvez supprimer l'association entre la connexion et la MACsec clé à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer une association entre une connexion et une MACsec clé

1. Ouvrez la Direct Connectconsole sur 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 MACsec secret à supprimer, puis choisissez Dissocier la clé.

6. Dans la boîte de dialogue de confirmation, saisissez dissocier, puis choisissez Dissocier.

Pour supprimer une association entre une connexion et une MACsec clé à l'aide de la ligne de commande ou de l'API

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

Direct Connect Connexions hébergées

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

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 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 Direct Connect.

> **Note**
>
> Vous ne pouvez pas demander une connexion hébergée via la 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 de plus amples informations, veuillez consulter 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 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 partenaire AWS Direct Connect. Vérifiez auprès de votre partenaire AWS Direct Connect s'il prend en charge la mise à niveau ou le déclassement d'une connexion existante. Si votre partenaire prend en charge la mise à niveau/la rétrogradation de votre connexion, 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.
- 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 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 :

- Supprimer une connexion
- Mise à jour d'une connexion
- Affichage des informations de connexion

Après avoir accepté une connexion, créez une interface virtuelle pour vous connecter à des ressources AWS publiques et privées. Pour de plus amples informations, veuillez consulter Interfaces virtuelles et interfaces virtuelles hébergées.

Accepter une connexion Direct Connect 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 Direct Connect .

Avant de pouvoir commencer à utiliser une connexion hébergée, vous devez accepter la connexion. Vous pouvez accepter une connexion hébergée à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

1. Ouvrez la Direct Connectconsole sur 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.

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

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

Supprimer une Direct Connect connexion

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). 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 une interface virtuelle.

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 Lettre d'autorisation et attribution d'une installation de raccordement (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.

Vous pouvez supprimer une connexion à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer une connexion

1. Ouvrez la Direct Connectconsole sur 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.

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

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

Mettre à jour une Direct Connect connexion

Vous pouvez mettre à jour l'attribut de connexion suivant à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

- Nom de la connexion.
- Mode de MACsec cryptage de la connexion.

> **Note**
>
> Bien que vous ne puissiez pas modifier directement les MACSec propriétés des connexions hébergées, les partenaires peuvent MACSec les activer sur leurs propres interconnexions afin de fournir des connexions hébergées sécurisées à leurs clients.

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`

Pour mettre à jour une connexion

1. Ouvrez la Direct Connectconsole sur 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.

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(Direct Connect API)

Afficher les détails Direct Connect de la connexion

Vous pouvez consulter l'état actuel de votre connexion à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. 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 Surveillez les ressources Direct Connect.

Pour afficher les informations sur une connexion

1. Ouvrez la Direct Connectconsole sur 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.

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

- describe-connections (AWS CLI)
- DescribeConnections(Direct Connect API)

Demande de connexions croisées sur 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 Direct Connect site, contactez le fournisseur approprié pour effectuer le raccordement croisé. Pour obtenir des instructions spécifiques à chaque fournisseur, consultez les tableaux ci-dessous. Les partenaires et leurs coordonnées sont organisés par région. Pour obtenir des tarifs spécifiques pour les connexions croisées, vous devez contacter directement le partenaire Direct Connect. Une fois la connexion croisée établie, vous pouvez créer les interfaces virtuelles à l'aide de la Direct Connect console.

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

Si vous ne possédez pas encore d'équipement sur un 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 Direct Connect . Pour plus d'informations, consultez la section Support des partenaires APN. Direct Connect Vous devez communiquer la LOA-CFA au fournisseur que vous avez sélectionné afin de simplifier votre demande de connexion transversale.

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

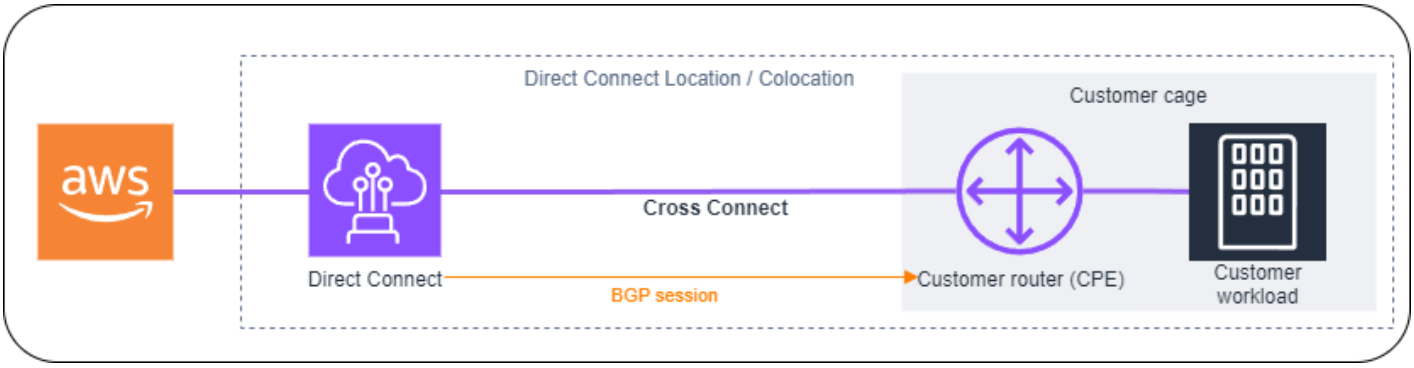
> **Note**
>
> Si la connexion transversale n'est pas terminée dans un délai de 90 jours, l'autorisation accordée par la LOA-CFA expire. Pour renouveler une LOA-CFA expirée, vous pouvez la télécharger à nouveau à partir de la console Direct Connect . Pour de plus amples informations, veuillez consulter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

Options de connectivité

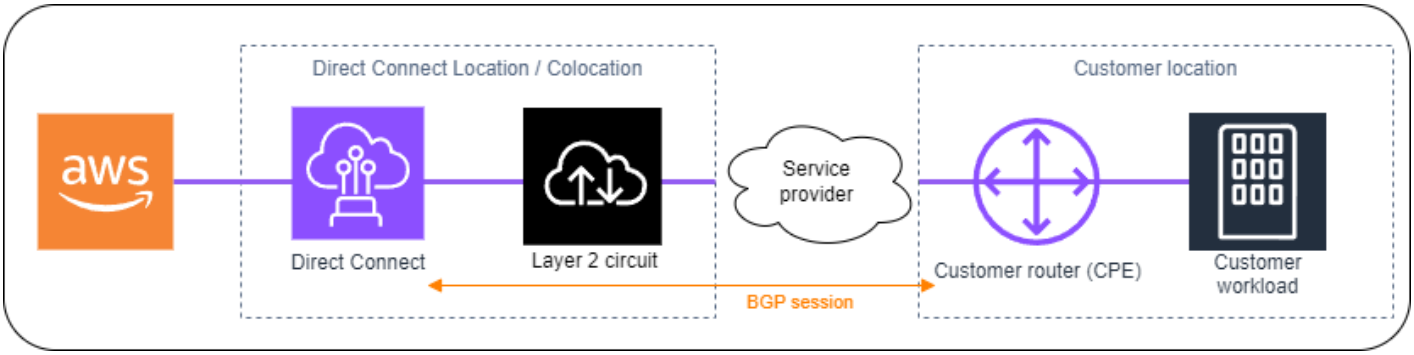
Les options disponibles pour se connecter à un point de vente Direct Connect peuvent varier en fonction du partenaire et de AWS la région. Vous pouvez travailler avec l'un des partenaires du

réseau de AWS partenaires (APN) qui peut fournir une ou plusieurs des options de connectivité suivantes :

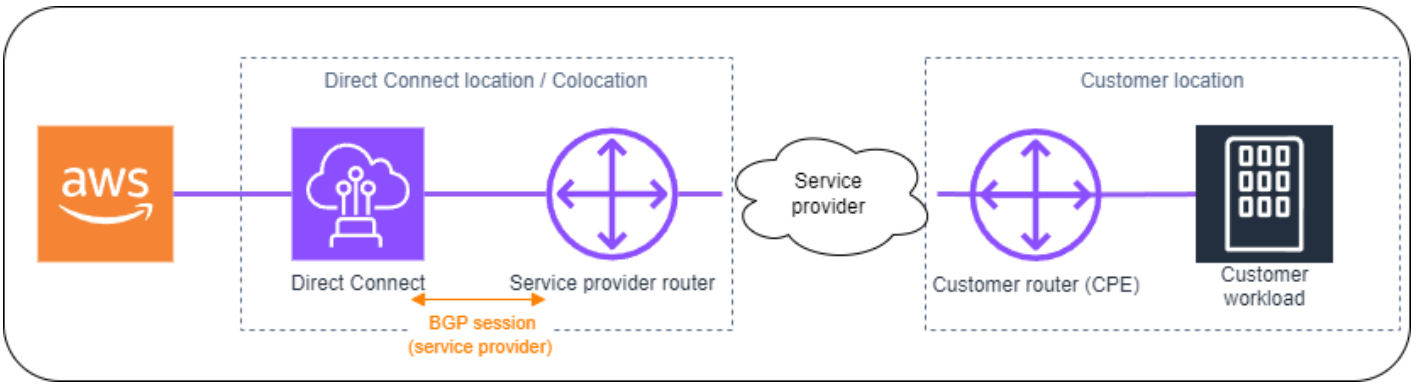
- Si des ressources sont déployées dans le même center/colocation centre de données que le site Direct Connect, le site peut fournir une interconnexion entre l' Direct Connect équipement et vos ressources. Pour cela, vous devez d'abord fournir un LOA-CFA à l'établissement. Pour plus d'informations, consultez Lettre d'autorisation et attribution d'une installation de raccordement (LOA-CFA). Voici un exemple de cette option de connectivité Direct Connect :



- Étendez la connexion Direct Connect au niveau de la couche 2 (couche de liaison de données) via un « circuit » entre le site Direct Connect et le site du client en travaillant avec les partenaires Direct Connect. Le routeur installé sur le site du client formera directement une session BGP avec l' AWS équipement. Par exemple, les technologies qui peuvent être utilisées sont Metro Ethernet, Dark Fibre ou Wavelength. Voici un exemple de cette option de connectivité Direct Connect.



- Étendez la connexion Direct Connect au niveau de la couche 3 (couche réseau) de l'emplacement Direct Connect à votre emplacement en travaillant avec les partenaires Direct Connect. Pour cette option de connectivité, le partenaire Direct Connect fournit un routeur au sein de l'emplacement Direct Connect qui forme une session BGP (Border Gateway Protocol) avec l' AWS équipement. Le partenaire Direct Connect a ensuite établi un autre BGP avec vous, par exemple via le protocole MPLS (Multiprotocol Label Switching). Voici un exemple de cette option de connectivité Direct Connect.



USA Est (Ohio)

Emplacement	Comment demander une connexion
Colomb, Cologix COL2	Contactez Cologix à l'adresse sales@cologix.com.
Cologix, Minneapolis MIN3	Contactez Cologix à l'adresse sales@cologix.com.
CyrusOne West III, Houston	Soumettez une demande à l'aide du formulaire de contact client.
Equinix, Chicago CH2	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.

Emplacement	Comment demander une connexion
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.
Digital Realty ATL1 &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 DC1 0-D12, Ashburn	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix DAA1 - DC3 et DC6, Dallas	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Miami MI1	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Seacaucus NY5	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 ATL1, 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 pouvez envoyer vos questions à l'adresse cloudaccess@edgeconnex.com.
Equinix LA3, El Segundo	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix SV1 & 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.

Emplacement	Comment demander une connexion
Digital Realty SEA1 0, Westin Building, 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, Seattle SE2	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 Indonésie à l'adresse awsdx@dci-indonesia.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@netmagic solutions.com.
Sify Rabale, Mumbai	Contactez Sify à l'adresse aws.directconnect@sifycorp.com.
STT Delhi DC2, New Delhi	Contactez STT sur demande. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Contactez STT sur demande. AWSDX@sttelemediagdc .in.
STT Hyderabad, Hyderabad DC1	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.

Emplacement	Comment demander une connexion
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., Région administrative spéciale de Hong Kong	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Singapour SG2	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.
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, Melbourne ME2	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Sydney SY3	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, Osaka OS1	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Tōkyō TY2	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Emplacement	Comment demander une connexion
NEC Inzai, Inzaï	Contactez NEC Inzai à l'adresse connection_support@ices.jp.nec.com.

Canada (Centre)

Emplacement	Comment demander une connexion
Telehouse, 250 Front Street W, Toronto	Contactez product@ca.telehouse.com.
Cologix, Montréal MTL3	Contactez Cologix à l'adresse sales@cologix.com.
Cologix, Vancouver VAN2	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.
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, Francfort FR5	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Helsinki HE6	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Munich MU1	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix, Varsovie WA1	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Interxion AMS7, Amsterdam	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion CPH2, Copenhague	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion FRA6, Francfort	Contactez Interxion à l'adresse customer.services@interxion.com.

Emplacement	Comment demander une connexion
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, Zürich	Contactez Interxion à l'adresse customer.services@interxion.com.
IPB, Berlin	Contactez IPB à l'adresse kontakt@ipb.de.
Equinix, Madrid ITConic MD2	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 datacentre@eirevo.ie.
Equinix, Dublin DX1	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Equinix LD5, Londres (Slough)	Contactez Equinix à l'adresse awsdealreg@equinix.com.
Interxion DUB2, Dublin	Contactez Interxion à l'adresse customer.services@interxion.com.
Interxion MRS1, Marsella	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, Milan ML2, 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, Manchester MA3	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, Paris PA3	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 DC53Bahreïn, Manama	Pour finaliser la connexion, vous pouvez collaborer avec l'un de nos partenaires fournisseurs de réseau dans l'emplacement 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.

Emplacement	Comment demander une connexion
AWS DC52Bahreïn, Manama	Pour finaliser la connexion, vous pouvez collaborer avec l'un de nos partenaires fournisseurs de réseau dans l'emplacement 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, Dubaï, 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
Cirion BNARAGMS, Buenos Aires	Contactez Cirion à l'adresse cloud.connect@ciriontechnologies.com.
Equinix RJ2, Rio de Janeiro	Contactez Equinix à l'adresse awsdealreg@equinix.com.
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 José	Contactez Equinix à l'adresse awsdealreg@equinix.com.

Direct Connect interfaces virtuelles et interfaces virtuelles hébergées

Vous devez créer l'une des interfaces virtuelles suivantes (VIFs) pour commencer à utiliser votre 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 Direct Connect dédiée ou hébergée, quelle que soit la vitesse. Pour plus d'informations sur les configurations de passerelle Direct Connect, veuillez consulter Passerelles Direct Connect.

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

Règles publicitaires de préfixe d'interface virtuelle publique

Nous vous communiquons les préfixes Amazon appropriés afin que vous puissiez accéder aux adresses IP publiques des charges de travail de vos services VPCs et des autres AWS services. Vous pouvez accéder à tous les AWS préfixes via cette connexion ; par exemple, les adresses IP publiques utilisées par les instances Amazon EC2, Amazon S3, les points de terminaison d'API AWS pour les services et Amazon.com. Vous n'avez pas accès aux préfixes autres qu'Amazon. Pour obtenir la liste actuelle des préfixes utilisés par AWS, consultez les plages d'adresses AWS IP dans le guide de l'utilisateur Amazon VPC. Sur cette page, vous pouvez télécharger un `.json` fichier des plages d' AWS adresses IP actuellement publiées. Notez que pour les plages d'adresses IP publiées :

- Les préfixes annoncés via BGP via une interface virtuelle publique peuvent être agrégés ou désagrégés par rapport à ce qui est répertorié dans la liste des plages d'adresses AWS IP.

- Les plages d'adresses IP auxquelles vous accédez AWS via vos propres adresses IP (BYOIP) ne sont pas incluses dans le `.json` fichier, mais elles sont AWS tout de même publiées via une interface virtuelle publique.
- AWS ne republie pas les préfixes clients reçus via les interfaces virtuelles publiques Direct Connect sur des réseaux extérieurs à. AWS Les préfixes annoncés sur une interface virtuelle publique seront visibles par tous les clients sur. AWS

> **Note**
>
> Nous vous recommandons d'utiliser un filtre pare-feu (basé sur l' source/destination adresse des paquets) pour contrôler le trafic en provenance et à destination de certains préfixes.

Pour plus d'informations sur les interfaces virtuelles publiques et les stratégies de routage, consultezthe section called “Stratégies de routage d'interface virtuelle publique”.

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 virtuelles privées 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 Direct Connect SiteLink.

> **Note**
>
> - SiteLink n'est pas disponible dans AWS GovCloud (US) et dans les régions de Chine.
> - SiteLink ne fonctionne pas si un routeur local annonce le même itinéraire AWS sur plusieurs interfaces virtuelles.

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 de plus amples informations, veuillez consulter MTUs pour les interfaces virtuelles privées ou les interfaces virtuelles de transit.

Conditions préalables pour les interfaces virtuelles

Avant de créer une interface virtuelle, procédez comme suit :

- Créez une connexion. Pour de plus amples informations, veuillez consulter 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, consultez Associer une connexion à un LAG.

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

Ressource	Informations obligatoires
Connection	La 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
	Note • Vous ne pouvez pas utiliser le même ASN pour la passerelle client et la passerelle gateway/Direct Connect virtuelle sur l'interface virtuelle. • Vous pouvez utiliser le même ASN de passerelle client pour plusieurs interfaces virtuelles. • Plusieurs interfaces virtuelles peuvent avoir le même ASN de passerelle virtuelle/passerelle Direct Connect et le même ASN de passerelle client, à condition qu'elles fassent partie de connexions Direct Connect différentes. Par exemple : Passerelle virtuelle (ASN 64 496) <---Interface virtuelle 1 (connexion Direct Connect 1) ---> Passerelle client (ASN 64 511) Passerelle virtuelle (ASN 64 496) <---Interface virtuelle 2 (connexion Direct Connect 2) ---> Passerelle client (ASN 64 511)
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 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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. • IPv4: • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques que vous possédez. Note • Le peering IPs pour les interfaces virtuelles privées et de transit peut être effectué à partir de n'importe quelle plage d'adresses IP valide. Cela peut également inclure les adresses IP publiques appartenant au client, à condition qu'elles ne soient utilisées que pour créer la session de peering BGP et qu'elles ne soient pas annoncées via l'interface virtuelle ou utilisées pour le NAT. • Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. La valeur peut être l'une des suivantes : • Un CIDR appartenant au client IPv4 Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais le même masque de sous-réseau doit être utilisé à la

Ressource	Informations obligatoires
	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. • Et un CIDR /31 AWS fourni. Contactez le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande) • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé CIDRs 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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.

Ressource	Informations obligatoires
Famille d'adresses	Si la session de peering BGP sera terminée 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum. • IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie : • Ils CIDRs viennent 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. • Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6 • 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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 configuré es 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 Direct Connect console et recherche z 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 le privé VIFs et le transit VIFs, le compte s'applique à l'interface virtuelle et à la destination de la passerelle privée virtuelle gateway/Direct Connect.
- Pour le public VIFs, le compte est utilisé pour la facturation par interface virtuelle. L'utilisation du transfert de données sortant (DTO) est mesurée en fonction du propriétaire de la ressource au taux de transfert de Direct Connect données.

> **Note**
>
> Les préfixes 31 bits sont pris en charge sur tous les types d'interfaces virtuelles Direct Connect. Voir RFC 3021 : Utilisation de préfixes 31 bits sur les IPv4 Point-to-Point liens pour plus d'informations.

MTUs pour les interfaces virtuelles privées ou les interfaces virtuelles de transit

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. Le MTU d'une interface virtuelle privée peut être de 1500 ou 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 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 le même itinéraire mais utilisent des valeurs de MTU différentes, ou si vous avez un Site-to-Site VPN qui annonce le même itinéraire, 1500 MTU sont utilisés.

Important

Les cadres Jumbo s'appliqueront uniquement aux itinéraires propagés 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 des instances 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 les étapes de définition du MTU pour une interface virtuelle privée, voirDéfinissez le MTU d'une interface virtuelle privée.

Direct Connect interfaces virtuelles

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.

Consultez ce qui suit pour créer une interface virtuelle :

- Créer une interface virtuelle publique
- Créer une interface virtuelle privée
- Créer une interface de transit virtuelle vers la passerelle Direct Connect

Prérequis

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

Conditions préalables pour le transfert d'interfaces virtuelles vers une passerelle Direct Connect

Pour connecter votre 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. Le MTU d'une interface

virtuelle privée peut être de 1500 ou 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 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.

Création d'une interface virtuelle Direct Connect publique

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

Pour mettre en service une interface virtuelle publique

1. Ouvrez la Direct Connectconsole sur 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 l'ASN BGP, entrez le numéro de système autonome (ASN) du Border Gateway Protocol Autonomous System Number (ASN) de votre routeur homologue local pour la nouvelle interface virtuelle.

   Les valeurs valides sont comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

   > **Note**
   >
   > Lorsque vous établissez une session d'appairage BGP AWS via une interface virtuelle publique, utilisez-la 7224 comme ASN pour établir la session BGP sur le côté. AWS L'ASN de votre routeur ou de votre passerelle client doit être différent de cet ASN.

6. Sous Paramètres supplémentaires, procédez comme suit :

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

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

      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 sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 de plus amples informations, veuillez consulter 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(Direct Connect API)

Création d'une interface virtuelle Direct Connect privée

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

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. Le MTU d'une interface virtuelle privée peut être de 1500 ou 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 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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.
6. Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :

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

[IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

> **Important**
>
> Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
>
> - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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.
8. Téléchargez la configuration de routeur pour votre périphérique. Pour de plus amples informations, veuillez consulter 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(Direct Connect API)

Création d'une interface virtuelle de transit vers la Direct Connect passerelle

Avant de connecter une interface virtuelle de transport en commun à la passerelle Direct Connect, familiarisez-vous avec le texte.

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

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

[IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

> **Important**
>
> Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
>
> - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 de plus amples informations, veuillez consulter 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(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(Direct Connect API)

Téléchargez le fichier de configuration du Direct Connect 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 MACsec activées, 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

Pour télécharger le fichier de configuration du routeur

1. Ouvrez la Direct Connectconsole sur 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 Direct Connect:
7. 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

Paramètre	Description
Suite de chiffrement à clé	16
Compensation de confident ialité	0
Indicateur ICV	Non
Heure du changement de clé SAK	Substitution de PN>

Interfaces Direct Connect virtuelles hébergées

Pour utiliser votre 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 Direct Connect connexion ou le groupe d'agrégation de liens (LAG) pour lequel vous créez l'interface virtuelle.
Nom de l'interfa ce 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 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 l'une des deux (double pile). N'utilisez pas Elastic IPs (EIPs) 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.
	
	• IPv4:
	  • (Interface virtuelle publique uniquement) Vous devez spécifier les IPv4 adresses publiques uniques dont vous êtes le propriétaire. La valeur peut être l'une des suivantes :
	  • Un CIDR appartenant au client IPv4
	
	  Ils peuvent être publics IPs (appartenant au client ou fournis par AWS), mais 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 `/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 le AWS Support pour demander un IPv4 CIDR public (et fournissez un cas d'utilisation dans votre demande)

Ressource	Informations obligatoires
	Note Nous ne pouvons garantir que nous serons en mesure de répondre à toutes les demandes d' IPv4 adresses publiques AWS fournies. • (Interface virtuelle privée uniquement) Amazon peut générer des IPv4 adresses privées pour vous. Si vous spécifiez le vôtre, assurez-vous de spécifier privé uniquement CIDRs pour l'interface de votre routeur et pour l'interface AWS Direct Connect. 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 attribue automatiquement un IPv6 /125 CIDR. Vous ne pouvez pas spécifier vos propres IPv6 adresses de pairs.
Famille d'adresses	Si la session de peering BGP sera terminée 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 32 bits, la valeur doit être comprise entre 1 et 4294967294. 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	IPv4 Routes publiques ou IPv6 routes pour faire de la publicité sur BGP. Vous devez publier au moins un préfixe à l'aide de BGP, jusqu'à 1 000 préfixes maximum.
	• IPv4: Le IPv4 CIDR peut se chevaucher avec un autre IPv4 CIDR public annoncé Direct Connect lorsque l'une des conditions suivantes est vraie :
	  • Ils CIDRs viennent 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.
	• Sur une interface virtuelle publique Direct Connect, vous pouvez spécifier n'importe quelle longueur de préfixe comprise entre /1 et /32 pour IPv4 et entre /1 et /64 pour. IPv6
	• 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.

Ressource	Informations obligatoires
(Interfaces virtuelles privées et de transit uniquement) Cadres Jumbo	Unité de transmission maximale (MTU) de paquets dépassés 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'appliquent uniquement aux itinéraires propagés à partir de. 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 Direct Connect console et recherchez les trames jumbo compatibles sur la page de configuration générale de l'interface virtuelle.

Créez une interface virtuelle privée hébergée dans Direct Connect

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

Pour créer une interface virtuelle privée hébergée

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

      > **Important**
      >
      > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
      >
      > - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 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 l'interface virtuelle hébergée acceptée par le propriétaire de l'autre AWS compte, vous pouvez télécharger le fichier de configuration. Pour de plus amples informations, veuillez consulter 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(Direct Connect API)

Créez une interface virtuelle publique hébergée dans Direct Connect

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

Pour créer une interface virtuelle publique hébergée

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

6. Pour configurer un IPv4 BGP ou un IPv6 homologue, procédez comme suit :

   [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

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

7. Pour publier des préfixes sur Amazon, pour les préfixes que vous souhaitez publier, entrez les adresses de destination IPv4 CIDR (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 l'interface virtuelle hébergée acceptée par le propriétaire de l'autre AWS compte, vous pouvez télécharger le fichier de configuration. Pour de plus amples informations, veuillez consulter 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(Direct Connect API)

Création d'une interface virtuelle de transport en commun Direct Connect 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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

      [IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

      > **Important**
      >
      > Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle

client comme adresse source ou de destination plutôt que les connexions. point-to-point

- 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 l'interface virtuelle hébergée acceptée par le propriétaire de l'autre AWS compte, vous pouvez télécharger le fichier de configuration du routeur pour votre appareil. Pour de plus amples informations, veuillez consulter 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(Direct Connect API)

Afficher les détails de l'interface Direct Connect virtuelle

Vous pouvez consulter l'état actuel de votre interface virtuelle à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. 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 Direct Connectconsole sur 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(Direct Connect API)

Ajouter un pair BGP à une interface Direct Connect virtuelle

Ajoutez ou supprimez une IPv4 session de peering IPv6 BGP à votre interface virtuelle à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Une interface virtuelle peut prendre en charge une seule session d'appairage IPv4 BGP et une seule session d'appairage IPv6 BGP. Vous ne pouvez pas spécifier vos propres IPv6 adresses d'homologues pour une session de peering IPv6 BGP. Amazon vous attribue automatiquement un IPv6 /125 CIDR.

Le protocole BGP multiprotocole 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.

Utilisez la procédure suivante pour ajouter un appairage BGP.

Pour ajouter un appairage BGP

1. Ouvrez la Direct Connectconsole sur 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 homologues IPv4 BGP, procédez comme suit :
   - Sélectionnez IPv4.
   - Pour spécifier vous-même ces adresses IP, dans le champ IP homologue de votre routeur, entrez l'adresse IPv4 CIDR de destination vers laquelle Amazon doit envoyer le trafic. Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IPv4 CIDR à utiliser pour envoyer AWS le trafic.
6. (Interface virtuelle publique) Pour ajouter des homologues IPv4 BGP, procédez comme suit :
   - Pour l'adresse IP homologue de votre routeur, entrez l'adresse de destination IPv4 CIDR à laquelle le trafic doit être envoyé.
   - Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IPv4 CIDR à utiliser pour envoyer AWS le trafic.

> **Important**
>
> Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
>
> - 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 .

7. (Interface virtuelle privée ou publique) Pour ajouter des homologues IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon ; vous ne pouvez pas spécifier d' IPv6 adresses 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483646) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

   Notez que si vous n'entrez pas de valeur, nous en attribuons une automatiquement.
9. Pour fournir votre propre clé BGP, entrez votre clé BGP dans le champ Clé d'authentification 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)
- Créer BGPPeer (Direct Connect API)

Supprimer un homologue BGP d'interface Direct Connect virtuelle

Si votre interface virtuelle possède à la fois une session d'appairage IPv6 BGP IPv4 et une session d'appairage BGP, vous pouvez supprimer l'une des sessions d'appairage BGP (mais pas les deux). Vous pouvez supprimer un homologue BGP d'interface virtuelle à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer un appairage BGP

1. Ouvrez la Direct Connectconsole sur 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)
- Supprimer BGPPeer (Direct Connect API)

Définir le MTU d'une interface virtuelle Direct Connect privée

Si votre interface virtuelle possède à la fois une session d'appairage IPv6 BGP IPv4 et une session d'appairage BGP, vous pouvez supprimer l'une des sessions d'appairage BGP (mais pas les deux). Pour plus d'informations sur MTUs les interfaces virtuelles privées, reportez-vous à la section MTUs relative aux interfaces virtuelles privées ou aux interfaces virtuelles de transit.

Vous pouvez définir le MTU d'une interface virtuelle privée à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour définir la MTU d'une interface virtuelle privée

1. Ouvrez la Direct Connectconsole sur 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 MTU (taille MTU 8500), sélectionnez Activé.
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(Direct Connect API)

Ajouter ou supprimer des balises d'interface Direct Connect virtuelle

Les balises permettent d'identifier l'interface virtuelle. Vous pouvez ajouter ou supprimer une balise à l'aide de la Direct Connect console, de la ligne de commande ou de l'API si vous êtes le propriétaire du compte pour l'interface virtuelle.

Pour ajouter ou supprimer une balise de l'interface virtuelle

1. Ouvrez la Direct Connectconsole sur 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 une interface Direct Connect virtuelle

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 Direct Connect les frais de transfert de données associés à l'interface virtuelle.

Vous pouvez supprimer une interface virtuelle à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer une interface virtuelle

1. Ouvrez la Direct Connectconsole sur 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(Direct Connect API)

Accepter une interface Direct Connect 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.

Vous pouvez accepter une interface virtuelle hébergée à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour accepter une interface virtuelle hébergée

1. Ouvrez la Direct Connectconsole sur 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 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(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(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(Direct Connect API)

Migrer une interface Direct Connect 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 VLAN IDs sont uniques ; par conséquent, migrer un VIF de cette manière signifierait qu'ils VLANs 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 Direct Connectconsole sur 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

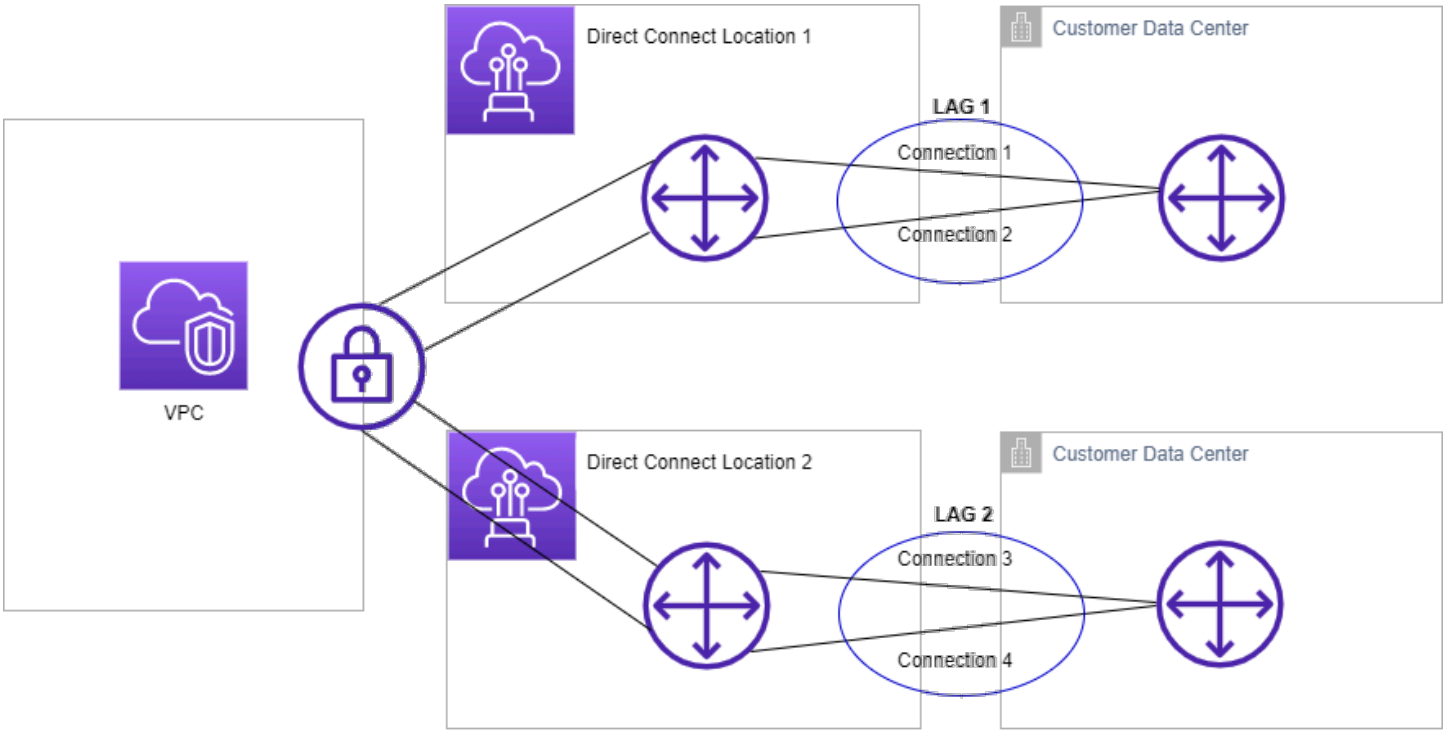
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(Direct Connect API)

Direct Connect groupes d'agrégation de liens (LAGs)

Vous pouvez utiliser plusieurs connexions pour augmenter la bande passante disponible. Un groupe d'agrégation de liens (LAG) est une interface logique qui utilise le protocole LACP (Link Aggrégation Control Protocol) pour agréger plusieurs connexions sur un seul Direct Connect point de terminaison, ce qui vous permet de les traiter comme une seule connexion gérée. LAGs rationalisez 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 connexions LAGs au lieu des quatre 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 Gbit/s, 10 Gbit/s, 100 Gbit/s ou 400 Gbit/s.
- Toutes les connexions du LAG doivent utiliser la même bande passante.
- Vous pouvez avoir un maximum de deux connexions 100 Gbit/s ou 400 Gbit/s, ou quatre connexions avec un débit de port inférieur à 100 Gbit/s dans un LAG. Chaque connexion du LAG est comptabilisée dans la limite de connexion globale pour la région.
- Toutes les connexions du LAG doivent se terminer au même Direct Connect point de terminaison.
- LAGs 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 et d'attribution des installations de connexion (LOA-CFA) pour une nouvelle connexion physique individuellement à partir de la console. Direct Connect Pour de plus amples informations, veuillez consulter Lettre d'autorisation et attribution d'une installation de raccordement (LOA-CFA).

Tous LAGs ont un attribut qui détermine le nombre minimum de connexions dans le LAG qui doit être opérationnel pour que le LAG lui-même soit opérationnel. Par défaut, cet attribut est défini sur 0 pour les nouveaux LAGs utilisateurs. 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 Active/Active mode.

> **Note**
>
> Lorsque vous créez un LAG ou que vous associez plusieurs connexions au LAG, il se peut que nous ne soyons pas en mesure de garantir un nombre suffisant de ports disponibles sur un point de Direct Connect terminaison donné.

Rubriques

- MACsec considérations pour Direct Connect
- Création d'un LAG sur un point de Direct Connect terminaison
- Afficher les détails du LAG sur un Direct Connect terminal

- Mettre à jour un LAG sur un Direct Connect terminal
- Associer une connexion à un LAG sur un Direct Connect point de terminaison
- Dissocier une connexion d'un LAG au niveau d'un point de terminaison Direct Connect
- Associer un MACsec CKN/CAK à un LAG de point de terminaison Direct Connect
- Supprimer l'association entre une clé MACsec secrète et un LAG de point de Direct Connect terminaison
- Supprimer un LAG de point de Direct Connect terminaison

MACsec considérations pour Direct Connect

Tenez compte des points suivants lorsque vous souhaitez effectuer une configuration MACsec sur LAGs :

- Lorsque vous créez un LAG à partir de connexions existantes, nous dissocions toutes les MACsec clés des connexions. Ensuite, nous ajoutons les connexions au LAG et associons la MACsec clé LAG aux connexions.
- Lorsque vous associez une connexion existante à un LAG, les MACsec clés actuellement associées au LAG sont associées à la connexion. Par conséquent, nous dissocions les MACsec clés de la connexion, ajoutons la connexion au LAG, puis associons la MACsec clé LAG à la connexion.
- Une seule MACsec clé peut être utilisée à tout moment sur tous les liens LAG. La possibilité de prendre en charge plusieurs MACsec touches est uniquement destinée à la rotation des clés.

Création d'un LAG sur un point de Direct Connect terminaison

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, les connexions doivent se trouver sur le même AWS appareil (se terminer au même Direct Connect point de terminaison). 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 AWS est interrompue lors de la création du LAG.

Pour créer un LAG avec de nouvelles connexions

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
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 1 Go ou 10 Go, ou deux lorsque la vitesse du port est de 100 Gbit/s ou 400 Gbit/s.
   - (Facultatif) Configurez la sécurité MAC (MACsec) pour la connexion. Sous Paramètres supplémentaires, sélectionnez Demander un port MACsec compatible.

     MACsec n'est disponible que sur des 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.

Pour créer un LAG à partir des connexions existantes

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.

2. Dans le panneau de navigation, sélectionnez LAGs.
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 1 Go ou 10 Go, ou deux lorsque la vitesse du port est de 100 Gbit/s ou 400 Gbit/s.
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.

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

- create-lag (AWS CLI)
- CreateLag(Direct Connect API)

Pour décrire votre LAGs utilisation de la ligne de commande ou de l'API

- describe-lags (AWS CLI)
- DescribeLags(Direct Connect API)

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

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

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 du LAG sur un Direct Connect terminal

Après avoir créé un LAG, vous pouvez consulter ses détails à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour afficher des informations sur votre LAG :

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Vous pouvez consulter des informations sur le LAG, notamment son identifiant et le Direct Connect point de terminaison sur lequel les connexions se terminent.

Pour obtenir des informations sur votre LAG à l'aide de la ligne de commande ou de l'API

- describe-lags (AWS CLI)
- DescribeLags(Direct Connect API)

Mettre à jour un LAG sur un Direct Connect terminal

Vous pouvez mettre à jour les attributs du groupe d'agrégation de liens (LAG) suivants à l'aide de la Direct Connect console, de la ligne de commande ou de l'API :

- Le nom du LAG.
- La valeur du nombre minimum de connexions opérationnelles pour que le LAG soit opérationnel.
- Le mode de MACsec chiffrement du LAG.

  MACsec n'est disponible que sur des 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.

Pour mettre à jour un LAG

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
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.

Pour mettre à jour un LAG à l'aide de la ligne de commande ou de l'API

- update-lag (AWS CLI)
- UpdateLag (API Direct Connect)

Associer une connexion à un LAG sur un Direct Connect point de terminaison

Vous pouvez associer une connexion existante à un LAG à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. La connexion peut être autonome ou faire partie d'un autre LAG. La connexion doit se faire sur le même AWS appareil et 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 AWS via la connexion est interrompue pendant l'association.

Pour associer une connexion à un LAG

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
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.

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

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(Direct Connect API)

Dissocier une connexion d'un LAG au niveau d'un point de terminaison Direct Connect

Convertissez une connexion en connexion autonome en la dissociant d'un LAG à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. 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 lors de la dissociation.

Pour dissocier une connexion d'un LAG

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le volet de gauche, choisissez LAGs.
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).

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

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag(Direct Connect API)

Associer un MACsec CKN/CAK à un LAG de point de terminaison Direct Connect

Après avoir créé le LAG qui prend en charge MACsec, vous pouvez associer un CKN/CAK à la connexion à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

> **Note**
>
> Vous ne pouvez pas modifier une clé MACsec secrète 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 une clé MACsec secrète et un LAG”.

Pour associer une MACsec clé à un LAG

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Choisissez Associer une clé.
5. Entrez la MACsec clé.

   [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 MACsec secrète.
6. Choisissez Associer une clé.

Pour associer une MACsec clé à un LAG à l'aide de la ligne de commande ou de l'API

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

Supprimer l'association entre une clé MACsec secrète et un LAG de point de Direct Connect terminaison

Vous pouvez supprimer l'association entre le LAG et la MACsec clé à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer une association entre un LAG et une MACsec clé

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
3. Sélectionnez le LAG et choisissez View details (Afficher les détails).
4. Sélectionnez le MACsec secret à supprimer, puis choisissez Dissocier la clé.
5. Dans la boîte de dialogue de confirmation, saisissez dissocier, puis choisissez Dissocier.

Pour supprimer une association entre un LAG et une MACsec clé à l'aide de la ligne de commande ou de l'API

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

Supprimer un LAG de point de Direct Connect terminaison

Si vous n'en avez plus besoin LAGs, 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 de plus amples informations, veuillez consulter Supprimer une connexion.

Vous pouvez supprimer un LAG à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer un LAG

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Dans le panneau de navigation, sélectionnez LAGs.
3. Sélectionnez le LAGs, puis choisissez Supprimer.
4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

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

- delete-lag (AWS CLI)
- DeleteLag (API Direct Connect)

Direct Connect passerelles

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

- Passerelles Direct Connect

  À l'aide d'une passerelle Direct Connect, vous pouvez associer la passerelle Direct Connect à une passerelle de transit à plusieurs VPCs, à une passerelle privée virtuelle ou, si vous utilisez AWS le Cloud WAN, à un réseau central Cloud WAN.
- Associations de la passerelle privée virtuelle

  À l'aide d'une passerelle privée virtuelle, vous pouvez associer la passerelle Direct Connect via une interface virtuelle privée à un ou plusieurs comptes situés VPCs dans la même région ou dans des régions différentes.
- Associations de la passerelle de transit

  Utilisez une passerelle Direct Connect pour connecter votre connexion Direct Connect via une interface virtuelle de transport à la passerelle de transport VPCs ou à celles VPNs qui sont attachées à votre passerelle de transport en commun.
- Associations du réseau central Cloud WAN

  Utilisez une passerelle Direct Connect pour associer une passerelle Direct Connect à un réseau AWS Network Manager central.
- Interactions des préfixes autorisés

  Utilisez les préfixes autorisés pour interagir avec les passerelles de transport en commun et les passerelles privées virtuelles.

Rubriques

Direct Connect passerelles

Utilisez Direct Connect la passerelle pour connecter votre VPCs. Vous associez une Direct Connect passerelle à l'un des éléments suivants :

- Une passerelle de transit lorsque vous en avez plusieurs VPCs dans la même région
- Passerelle privée virtuelle
- Un réseau central AWS Cloud WAN

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. Une passerelle Direct Connect est un composant virtuel de Direct Connect conçu pour agir comme un ensemble distribué de réflecteurs de route BGP. Comme il fonctionne en dehors du chemin du trafic de données, il évite de créer un point de défaillance unique ou d'introduire des dépendances spécifiques Régions AWS. La haute disponibilité est intrinsèquement intégrée à sa conception, ce qui élimine le besoin de plusieurs passerelles Direct Connect.

Les clients utilisant Direct Connect avec VPCs qui contournent actuellement une zone de disponibilité parent ne seront pas en mesure de 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 annoncé sur deux ou plusieurs VPCs passerelles privées virtuelles associées (VGWs) associées à la même passerelle Direct Connect et sur la même interface virtuelle. Dans ce cas, ils VPCs peuvent communiquer entre eux via le point de

terminaison Direct Connect. Par exemple, si vous annoncez un superréseau (par exemple, 10.0.0.0/8 ou 0.0.0.0/0) qui chevauche le réseau connecté VPCs à une passerelle Direct Connect (par exemple, 10.0.0.0/24 et 10.0.1.0/24), et sur la même interface virtuelle, ils peuvent communiquer entre eux à partir de votre réseau local. VPCs

Si vous souhaitez bloquer les VPC-to-VPC communications 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 elles VPCs, en les utilisant également dans le cadre du groupe de sécurité par défaut du VPC.
2. Évitez de faire de la publicité pour un superréseau provenant de votre réseau local qui chevauche votre réseau. VPCs Au lieu de cela, vous pouvez annoncer des itinéraires plus spécifiques à partir de votre réseau local qui ne se chevauchent pas avec votre VPCs.
3. Provisionnez une seule passerelle Direct Connect pour chaque VPC que vous souhaitez connecter à votre réseau local au lieu d'utiliser la même passerelle Direct Connect pour plusieurs VPC. VPCs Par exemple, au lieu d'utiliser une seule passerelle Direct Connect pour votre développement et votre production VPCs, utilisez des passerelles Direct Connect distinctes pour chacune d'entre elles VPCs.

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 passerelles VPCs connectées à des passerelles de transit associées à la même passerelle Direct Connect, elles VPCs peuvent communiquer. Pour les VPCs empêcher de communiquer, associez une table de routage aux pièces jointes VPC pour lesquelles l'option Blackhole est définie.

Rubriques

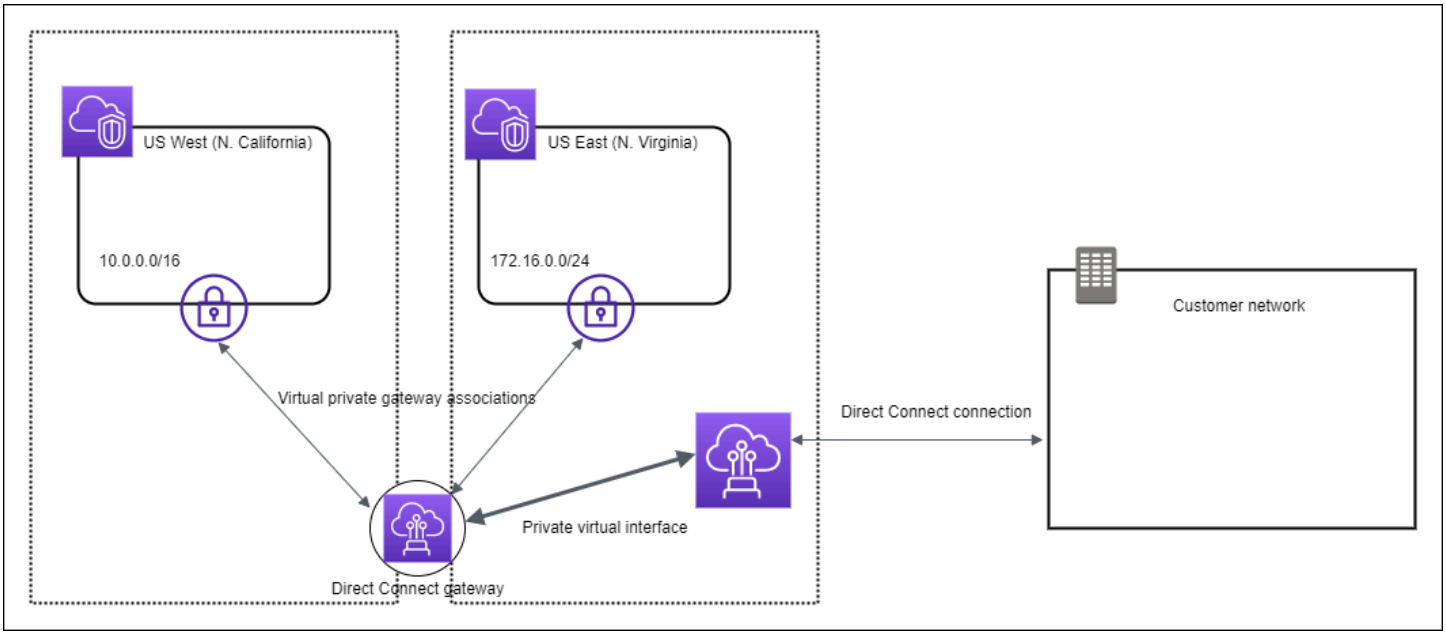
Scénarios

Les paragraphes suivants décrivent quelques scénarios d'utilisation des passerelles Direct Connect.

Scénario : associations de passerelles privées virtuelles

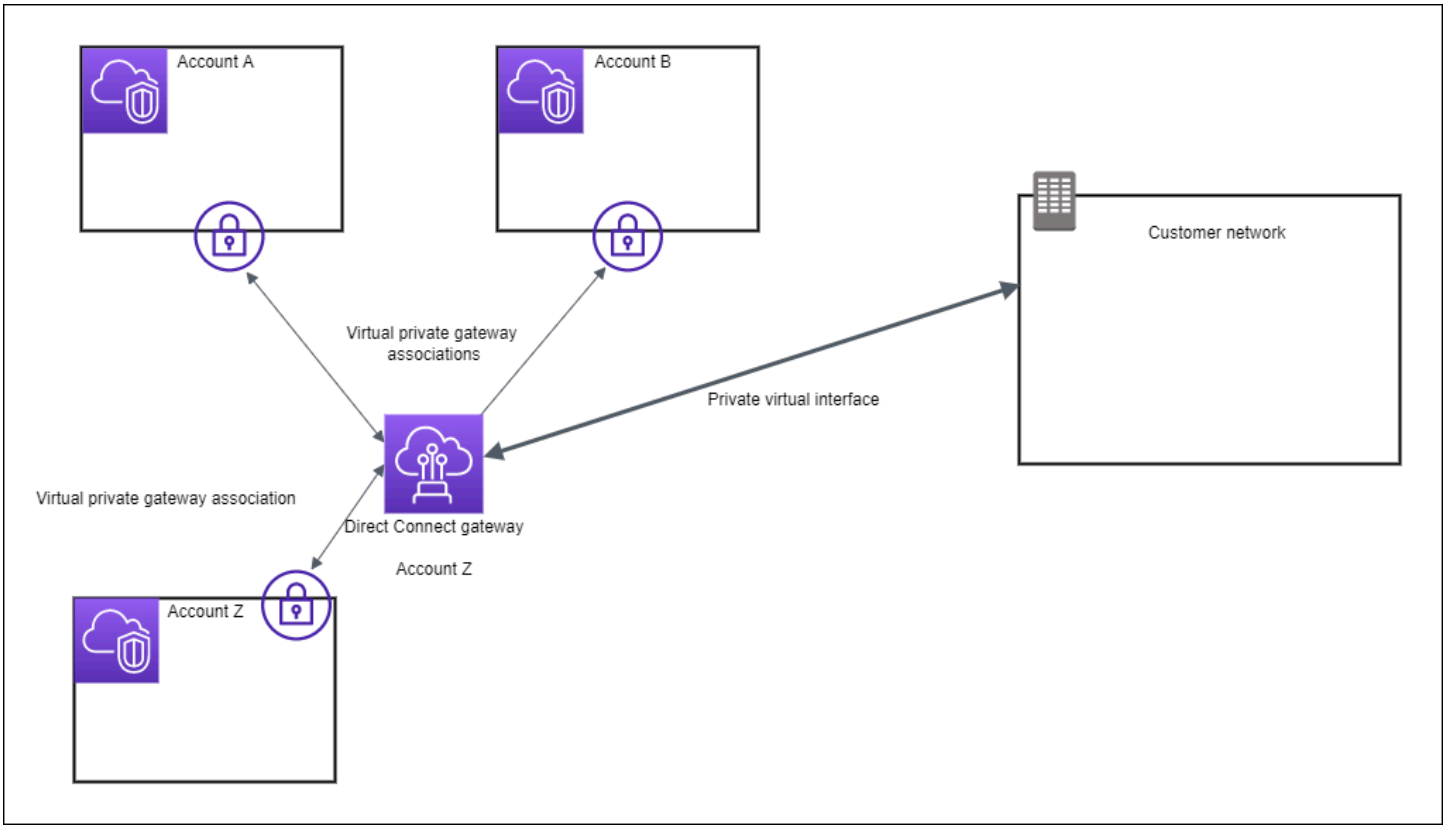
Dans le schéma suivant, la passerelle Direct Connect vous permet d'utiliser votre Direct Connect connexion dans la région USA Est (Virginie du Nord) pour accéder VPCs à votre compte dans les régions USA Est (Virginie du Nord) et USA Ouest (Californie du Nord).

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' Direct Connect emplacement. Il existe une connexion Direct Connect entre l'emplacement et le centre de données du client.



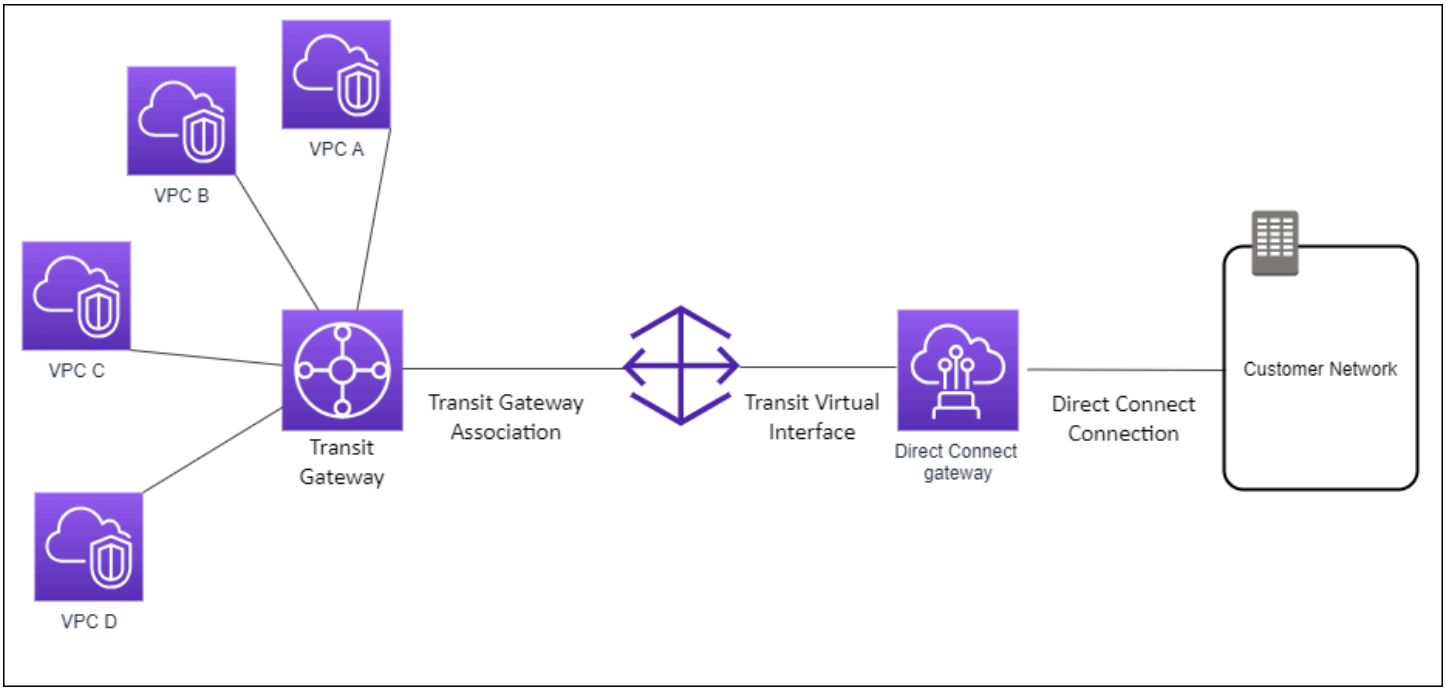
Scénario : associations de passerelles privées virtuelles entre les comptes

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.



Scénario : associations de passerelles de transit

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



La solution implique les éléments suivants :

- Une passerelle de transit 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.

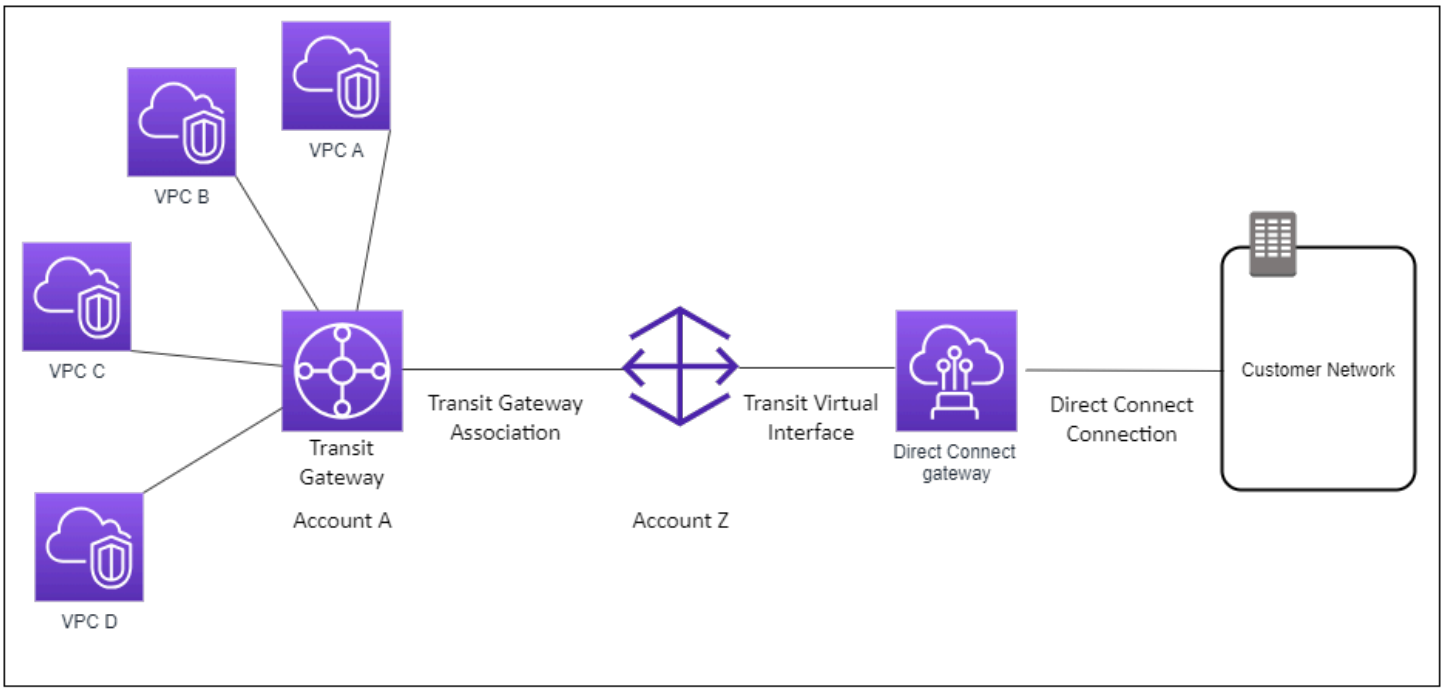
Cette configuration offre les avantages suivants. Vous pouvez effectuer les actions suivantes :

- Gérez une seule connexion pour plusieurs VPCs ou pour celles VPNs 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.

Scénario : associations de passerelles de transit entre les 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, le VPCs rattaché à la passerelle de transit peut acheminer le trafic de 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.



Création d'une Direct Connect passerelle

Vous pouvez créer une passerelle Direct Connect dans n'importe quelle région prise en charge à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour créer une passerelle Direct Connect

1. Ouvrez la Direct Connectconsole sur 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.

> **Note**
>
> Si vous souhaitez créer une passerelle Direct Connect à utiliser avec un réseau central AWS Cloud WAN. L'ASN ne doit pas être dans la même plage que l'ASN du réseau central.

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(Direct Connect API)

Migrer d'une passerelle privée virtuelle vers une Direct Connect passerelle

Vous pouvez migrer une passerelle privée virtuelle attachée à une interface virtuelle vers une passerelle Direct Connect.

Si vous utilisez Direct Connect en VPCs contournant actuellement une zone de disponibilité parent, vous ne pourrez pas migrer vos connexions Direct Connect ou vos interfaces virtuelles.

Les étapes suivantes décrivent les étapes à suivre pour migrer une passerelle privée virtuelle vers une passerelle Direct Connect.

Pour migrer vers une passerelle Direct Connect

1. Créez une passerelle Direct Connect.

   Si la passerelle Direct Connect n'existe pas encore, vous devez la créer. Pour connaître les étapes de création d'une passerelle Direct Connect, consultezCréation d'une passerelle Direct Connect.
2. Créez une interface virtuelle pour la passerelle Direct Connect.

   Une interface virtuelle est requise pour la migration. Si l'interface n'existe pas, vous devez la créer. Pour les étapes de création de l'interface virtuelle, reportez-vous àInterfaces virtuelles.
3. Associez la passerelle privée virtuelle à la passerelle Direct Connect.

   La passerelle Direct Connect et une passerelle privée virtuelle doivent être associées. Pour connaître les étapes de création de l'association, voirAssocier ou dissocier des passerelles privées virtuelles.
4. Supprimez l'interface virtuelle associée à la passerelle privée virtuelle. Pour de plus amples informations, veuillez consulter Supprimer une interface virtuelle.

Supprimer une Direct Connect passerelle

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. Une fois que vous avez dissocié toutes les passerelles privées virtuelles associées et supprimé toutes les interfaces virtuelles privées associées, vous pouvez supprimer la passerelle Direct Connect à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

- Pour connaître les étapes à suivre pour dissocier une passerelle privée virtuelle, consultez. Associer ou dissocier des passerelles privées virtuelles
- Pour connaître les étapes de suppression d'une interface virtuelle, consultezSupprimer une interface virtuelle.

Pour supprimer une passerelle Direct Connect

1. Ouvrez la Direct Connectconsole sur 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(Direct Connect API)

Direct Connect associations de passerelles privées virtuelles

Vous pouvez associer une passerelle privée virtuelle à une passerelle Direct Connect pour permettre la connectivité entre votre Direct Connect connexion et entre VPCs différents comptes et régions. Chaque VPC nécessite une passerelle privée virtuelle que vous associez à la passerelle Direct Connect. Une fois ces associations établies, vous créez des interfaces virtuelles privées sur votre connexion Direct Connect à la passerelle Direct Connect, permettant VPCs à plusieurs utilisateurs de partager la même connexion Direct Connect par le biais de leurs associations de passerelle privée virtuelle respectives.

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 de plus amples informations, veuillez consulter Quotas Direct Connect.
- 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 VPCs blocs CIDR auxquels vous vous connectez via une passerelle Direct Connect ne peuvent pas se chevaucher. Si vous ajoutez un bloc d' IPv4 adresse CIDR à un VPC associé à une passerelle Direct Connect, assurez-vous que le bloc d'adresse CIDR ne chevauche pas un bloc d'adresse CIDR existant pour un autre VPC associé. Pour plus d'informations, consultez la section Ajouter des blocs IPv4 CIDR 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 ceux VPCs qui sont associés à une seule passerelle Direct Connect. 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.
- 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 annonce toutes les connexions VPCs via l'ASN qui lui est attribué.

Pour connecter votre 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 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 de plus amples informations, veuillez consulter Interfaces virtuelles et interfaces virtuelles hébergées.

Rubriques

- Création d'une passerelle privée Direct Connect virtuelle
- Associer ou dissocier des Direct Connect passerelles privées virtuelles
- Création d'une interface virtuelle privée vers la Direct Connect passerelle
- Associer une passerelle privée Direct Connect virtuelle entre les comptes

Création d'une passerelle privée Direct Connect virtuelle

La passerelle réseau privé virtuel doit être attachée au VPC auquel vous souhaitez vous connecter. Vous pouvez créer une passerelle privée virtuelle et l'associer à un VPC à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

> **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 annonce toutes les connexions VPCs via l'ASN qui lui est attribué.

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 Direct Connectconsole sur 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 Amazon EC2 Query)
- 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 Amazon EC2 Query)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Associer ou dissocier des Direct Connect passerelles privées virtuelles

Vous pouvez associer ou dissocier une passerelle privée virtuelle et une passerelle Direct Connect à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. Le propriétaire du compte de la passerelle privée virtuelle effectue ces opérations.

Pour associer une passerelle privée virtuelle

1. Ouvrez la Direct Connectconsole sur 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 Direct Connectconsole sur 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(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(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(Direct Connect API)

Création d'une interface virtuelle privée vers la Direct Connect passerelle

Pour connecter votre 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. Vous pouvez créer une interface virtuelle privée à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

> **Note**
>
> Si vous acceptez une interface virtuelle privée hébergée, vous pouvez l'associer à une passerelle Direct Connect dans votre compte. Pour de plus amples informations, veuillez consulter Accepter une interface virtuelle hébergée.

Pour mettre en service une interface virtuelle privée vers une passerelle Direct Connect

1. Ouvrez la Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

[IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

> **Important**
>
> Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
>
> - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 de plus amples informations, veuillez consulter 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 (API Direct Connect)

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(Direct Connect API)

Associer une passerelle privée Direct Connect virtuelle entre les 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 CIDRs des informations identiques ou inférieures CIDRs sur 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 Interactions des préfixes autorisés.

Direct Connect passerelles et associations de passerelles de transit

Vous pouvez utiliser une Direct Connect passerelle pour connecter votre connexion Direct Connect via une interface virtuelle de transport à la passerelle de transport VPCs ou à VPNs celles qui sont attachées 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 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 de plus amples informations, veuillez consulter Quotas Direct Connect.
- 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 situées dans différentes régions, utilisez une passerelle unique ASNs pour chaque passerelle de transit.
- Toute adresse de point-to-point connectivité utilisant une `/30` plage, par exemple, `192.168.0.0/30` ne se propage pas vers une passerelle de transit.

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 le site AWS vers la passerelle de transit, même si les personnes VPCs rattachées à la passerelle de transit n'ont pas été attribuées CIDRs. 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 la passerelle de transit et les passerelles privées virtuelles, consultez. Interactions des préfixes autorisés

Rubriques

- Associer ou dissocier Direct Connect une passerelle de transit
- Création d'une interface virtuelle de transit vers la Direct Connect passerelle

- Créer une passerelle de transit et une proposition Direct Connect d'association
- Accepter ou rejeter une passerelle de transit et une proposition Direct Connect d'association
- Mettre à jour les préfixes autorisés pour une passerelle de transit et Direct Connect une association
- Supprimer une passerelle de transit et une proposition Direct Connect d'association

Associer ou dissocier Direct Connect une passerelle de transit

Associez ou dissociez une passerelle de transit à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour associer une passerelle de transit

1. Ouvrez la Direct Connectconsole sur 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 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 Direct Connectconsole sur 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 Direct Connectconsole sur 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 pour laquelle vous souhaitez modifier les préfixes autorisés, 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 au CIDRs VPC Amazon pour toutes les passerelles privées virtuelles. Pour en savoir plus sur les préfixes autorisés, consultez 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. 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(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(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(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(Direct Connect API)

Création d'une interface virtuelle de transit vers la Direct Connect passerelle

Pour connecter votre 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. Vous pouvez utiliser la Direct Connect console, la ligne de commande ou l'API.

> **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 Direct Connectconsole sur 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 comprises entre 1 et 4294967294. Cela inclut la prise en charge à la fois ASNs (1-2147483647) et longue (1-4294967294). ASNs Pour plus d'informations ASNs et pour une longue période, ASNs voirSupport ASN prolongé dans Direct Connect.

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

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

[IPv4] Pour configurer un pair IPv4 BGP, choisissez IPv4et effectuez l'une des opérations suivantes :

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

> **Important**
>
> Lorsque vous configurez les interfaces virtuelles AWS Direct Connect, vous pouvez spécifier vos propres adresses IP à l'aide de la RFC 1918, utiliser d'autres schémas d'adressage ou opter pour des adresses CIDR IPv4 /29 AWS attribuées à partir de la plage Link-Local de la RFC 3927 IPv4 169.254.0.0/16 pour la connectivité. point-to-point Ces point-to-point connexions doivent être utilisées exclusivement pour le peering eBGP entre le routeur de votre passerelle client et le point de terminaison Direct Connect. À des fins de trafic VPC ou de tunneling, comme le VPN IP AWS Site-to-Site privé ou Transit Gateway Connect, il est AWS recommandé d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que les connexions. point-to-point
>
> - 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 pair IPv6 BGP, choisissez IPv6. Les IPv6 adresses homologues sont automatiquement attribuées à partir du pool d' IPv6 adresses d'Amazon. Vous ne pouvez pas spécifier d' IPv6 adresses 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 de plus amples informations, veuillez consulter 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 (API Direct Connect)

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(Direct Connect API)

Créer une passerelle de transit et une proposition Direct Connect d'association

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 Direct Connect. Vous pouvez créer une proposition d'association à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour créer une proposition d'association

1. Ouvrez la Direct Connectconsole sur 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(Direct Connect API)

Accepter ou rejeter une passerelle de transit et une proposition Direct Connect d'association

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. Vous pouvez accepter ou rejeter la proposition d'association à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour accepter une proposition d'association

1. Ouvrez la Direct Connectconsole sur 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 Direct Connectconsole sur 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(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(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(Direct Connect API)

Mettre à jour les préfixes autorisés pour une passerelle de transit et Direct Connect une association

Vous pouvez mettre à jour les préfixes autorisés depuis la passerelle de transit via la passerelle Direct Connect à l'aide de la Direct Connect console, de la ligne de commande ou de l'API. Pour mettre à jour les préfixes autorisés pour une passerelle de transit et une association Direct Connect à l'aide de la Direct Connect console,

- Si vous êtes le propriétaire de la passerelle de transit, vous devez créer une nouvelle proposition d'association pour cette passerelle Direct Connect, en spécifiant les préfixes à autoriser. Pour les étapes de création d'une nouvelle proposition d'association, voirCréer une proposition d'association pour les passerelles de transit.
- Si vous êtes propriétaire de la passerelle Direct Connect, vous pouvez mettre à jour les préfixes autorisés lorsque vous acceptez la proposition d'association ou si vous mettez à jour les préfixes autorisés pour une association existante. Pour connaître les étapes de mise à jour des préfixes autorisés lorsque vous acceptez l'association, consultezAccepter ou rejeter une proposition d'association de passerelle de transit.

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(Direct Connect API)

Supprimer une passerelle de transit et une proposition Direct Connect d'association

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 de plus amples informations, veuillez consulter Créer une proposition d'association pour les passerelles de transit.

Vous pouvez supprimer une passerelle de transit et une proposition d'association Direct Connect à l'aide de la Direct Connect console, de la ligne de commande ou de l'API.

Pour supprimer une proposition d'association

1. Ouvrez la Direct Connectconsole sur 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(Direct Connect API)

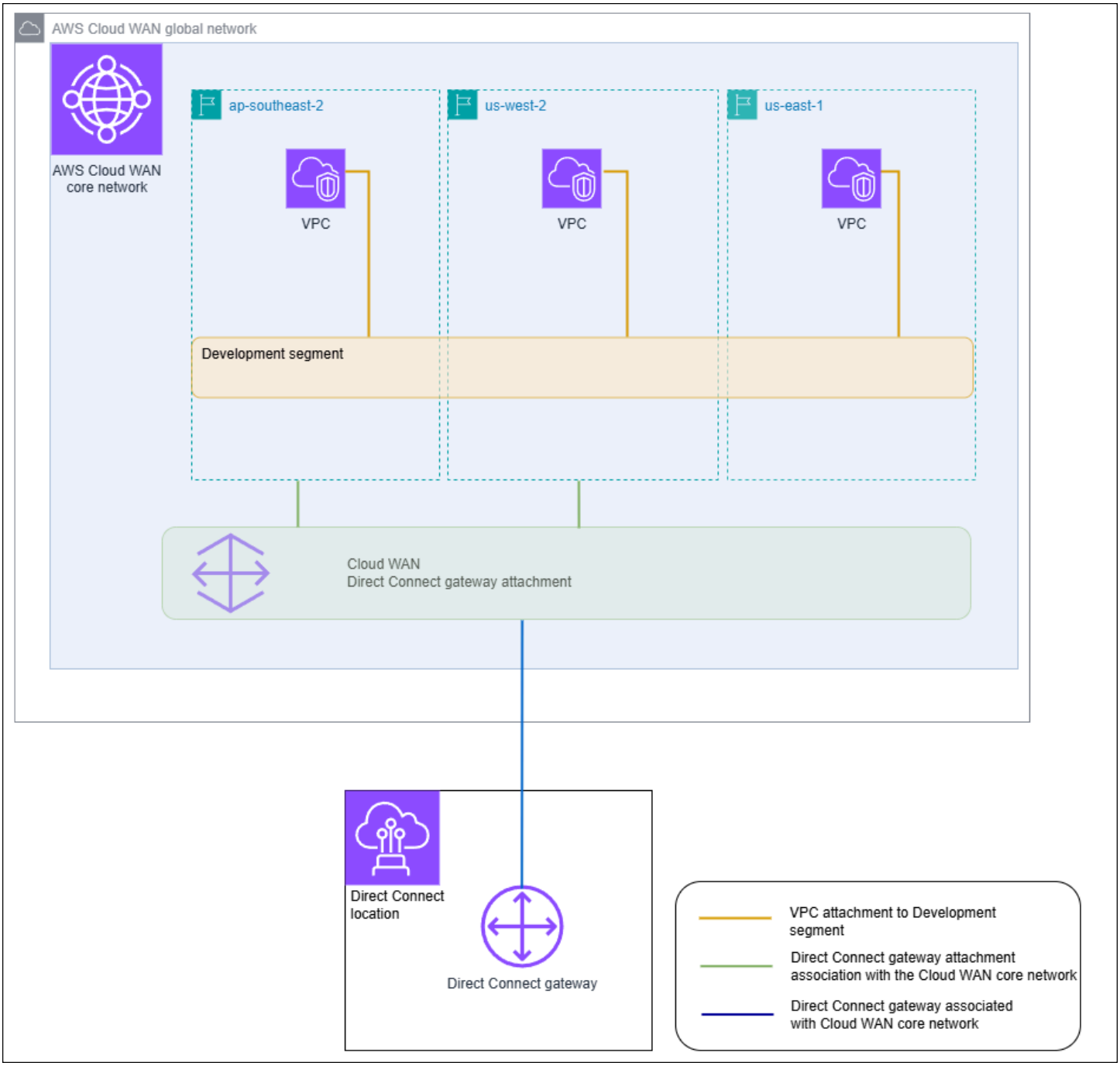
Direct Connect associations de passerelle et de réseau central AWS Cloud WAN

Associez une Direct Connect passerelle à un réseau central AWS Cloud WAN à l'aide d'un type de pièce jointe Direct Connect dans Cloud WAN. Cette association directe achemine le trafic entre les emplacements périphériques sélectionnés par votre réseau principal et vos connexions Direct Connect en utilisant le chemin le plus court disponible

Le type de pièce jointe de passerelle Direct Connect prend en charge le protocole BGP (Border Gateway) pour la propagation automatique des informations de routage entre votre réseau principal et les sites locaux. La pièce jointe Direct Connect prend également en charge les fonctionnalités standard du Cloud WAN, telles que la gestion centralisée basée sur des règles, l'automatisation des pièces jointes basée sur des balises et la segmentation pour les configurations de sécurité avancées.

> **Note**
>
> L'association entre un réseau central et une passerelle Direct Connect est créée, supprimée et gérée depuis la console Cloud WAN dans Network Manager. Lorsque vous utilisez une passerelle Direct Connect avec Cloud WAN, la console Direct Connect et la CLI APIs et refléteront l'association, mais ne peuvent pas être utilisées pour la modifier. Vous pouvez toutefois utiliser l'API Direct Connect ou la ligne de commande pour vérifier si une association a été créée.

L'exemple suivant montre un réseau mondial Cloud WAN composé de trois régions au sein du réseau central Cloud WAN. Chaque région possède son propre VPC connecté à un segment de développement du réseau central partagé entre ces trois régions. À l'aide de Cloud WAN, une pièce jointe à une passerelle Direct Connect est créée dans Cloud WAN à l'aide d'une passerelle Direct Connect créée à l'aide de Direct Connect. La pièce jointe est associée à deux des trois régions, ap-southeast-2 et us-west-2, et est autorisée à accéder au segment Développement. Même si us-east-1 partage le même segment de développement, la pièce jointe à la passerelle Direct Connect n'est pas partagée avec cette région et n'est donc pas disponible.



Rubriques

- Conditions préalables
- Considérations
- Associations de passerelles Direct Connect à un réseau central Cloud WAN
- Vérifier l'association d'une Direct Connect passerelle à un réseau central AWS Cloud WAN

Conditions préalables

L'association d'une passerelle Direct Connect à un réseau central Cloud WAN nécessite les éléments suivants :

- Une passerelle Direct Connect existante. Pour connaître les étapes de création d'une passerelle Direct Connect, consultezCréation d'une passerelle Direct Connect.
- Un réseau central AWS Cloud WAN. Pour plus d'informations sur le Cloud WAN, consultez le Guide de l'utilisateur du AWS Cloud WAN.

Considérations

Les limites suivantes s'appliquent aux associations de passerelles Direct Connect avec un réseau central Cloud WAN :

- Une passerelle Direct Connect peut être associée à un seul réseau central Cloud WAN et à un seul segment de ce réseau central. Une fois qu'une association est créée, cette passerelle ne peut pas être associée à d'autres ressources dans AWS les régions. Si vous dissociez la passerelle du réseau principal, vous pouvez ensuite utiliser cette passerelle pour d'autres types d'association.
- La pièce jointe à la passerelle Cloud WAN Direct Connect utilise le type d'interface virtuelle de transit pour la connectivité.
- La pièce jointe Cloud WAN ne prend pas en charge les listes de préfixes autorisés. Tous les préfixes d'un segment de réseau principal seront publiés sur la passerelle Direct Connect associée à ce segment.
- Le quota pour le nombre maximum de préfixes pouvant être annoncés sur site ou AWS via une interface virtuelle de transit est différent du quota pour les préfixes annoncés depuis un réseau central Cloud WAN vers un réseau local. Les quotas pour les autres ressources Direct Connect utilisées avec une association Cloud WAN sont également applicables. Consultez Quotas Direct Connect.
- L'attribut BGP AS-PATH sera conservé sur le réseau principal, la passerelle Direct Connect et l'interface virtuelle.
- L'ASN d'une passerelle Direct Connect doit être en dehors de la plage ASN configurée pour le réseau principal Cloud WAN. Par exemple, si vous avez une plage ASN comprise entre 64512 et 65534 pour le réseau principal, l'ASN de la passerelle Direct Connect doit utiliser un ASN en dehors de cette plage.

- Il est possible que le Cloud WAN ne prenne pas en charge des types de pièces jointes spécifiques utilisant le type de pièce jointe Direct Connect pour le transport. Pour plus d'informations sur les connexions de passerelle Direct Connect à un réseau central Cloud WAN, consultez la section Pièces jointes de passerelle Direct Connect dans le AWS Cloud WAN dans le Guide de l'utilisateur du AWS Cloud WAN.
- CloudWatch Network Monitor prend en charge les métriques de latence et de perte de paquets lorsqu'il est utilisé avec un type de connexion de passerelle Cloud WAN Direct Connect. La fonctionnalité Network Health Indicator n'est pas prise en charge. Pour plus d'informations, consultez la section Utilisation Amazon CloudWatch du moniteur réseau dans le guide de Amazon CloudWatch l'utilisateur.

Associations de passerelles Direct Connect à un réseau central Cloud WAN

L'association d'une passerelle Direct Connect à un réseau central AWS Cloud WAN s'effectue à l'aide de la console AWS Cloud WAN, du Cloud WAN APIs ou de la ligne de commande.

Pour associer une passerelle Direct Connect existante à un réseau central Cloud WAN, créez une nouvelle pièce jointe Direct Connect dans la console Cloud WAN. Une fois la pièce jointe Direct Connect créée, l'association est établie. Par défaut, lors de la création de l'association, vous pouvez choisir la valeur par défaut pour inclure tous les emplacements périphériques du réseau central dans le segment de réseau central choisi. Vous pouvez également spécifier des emplacements de bord individuels.

Pour plus d'informations sur les connexions de passerelle Direct Connect à un réseau central Cloud WAN, consultez la section Pièces jointes de passerelle Direct Connect dans le AWS Cloud WAN dans le Guide de l'utilisateur du AWS Cloud WAN.

Vérifier l'association d'une Direct Connect passerelle à un réseau central AWS Cloud WAN

Vous pouvez vérifier l'association d'une passerelle Direct Connect à un réseau central Cloud WAN à l'aide de la console Direct Connect, de l'API Direct Connect ou de la ligne de commande.

Pour vérifier l'association d'une passerelle Direct Connect à un réseau central Cloud WAN à l'aide de la console

1. Ouvrez la Direct Connectconsole sur https://console.aws.amazon.com/directconnect/v2/home.
2. Choisissez les passerelles Direct Connect dans le volet de navigation.

3. Choisissez la pièce jointe de passerelle Direct Connect dont vous souhaitez afficher l'association.
4. Choisissez l'onglet Associations de passerelles.
   - La colonne ID affiche l'identifiant du réseau principal auquel la passerelle Direct Connect est associée.
   - La colonne État affiche les informations associées.
   - La colonne Type d'association affiche le réseau central Cloud WAN.

Pour vérifier l'association d'une passerelle Direct Connect à un réseau central Cloud WAN à l'aide de la ligne de commande ou de l'API

- DescribeDirectConnectGatewayAssociations(Direct Connect API)
- describe-direct-connect-gateway-association ()AWS CLI

Interactions de préfixes autorisées pour les passerelles Direct Connect

Découvrez la façon dont les préfixes autorisés interagissent avec les passerelles de transit et les passerelle privées virtuelles. Pour de plus amples informations, veuillez consulter 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 le même CIDRs nombre ou une plus petite plage CIDRs de préfixes sur 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 peut retarder ou supprimer uniquement 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 local vers ou depuis une passerelle Direct Connect vers la passerelle de transit, même lorsque les personnes VPCs rattachées à la passerelle de transit n'ont pas d'attribution CIDRs. 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 préfixes identiques ou inférieurs. CIDRs

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.

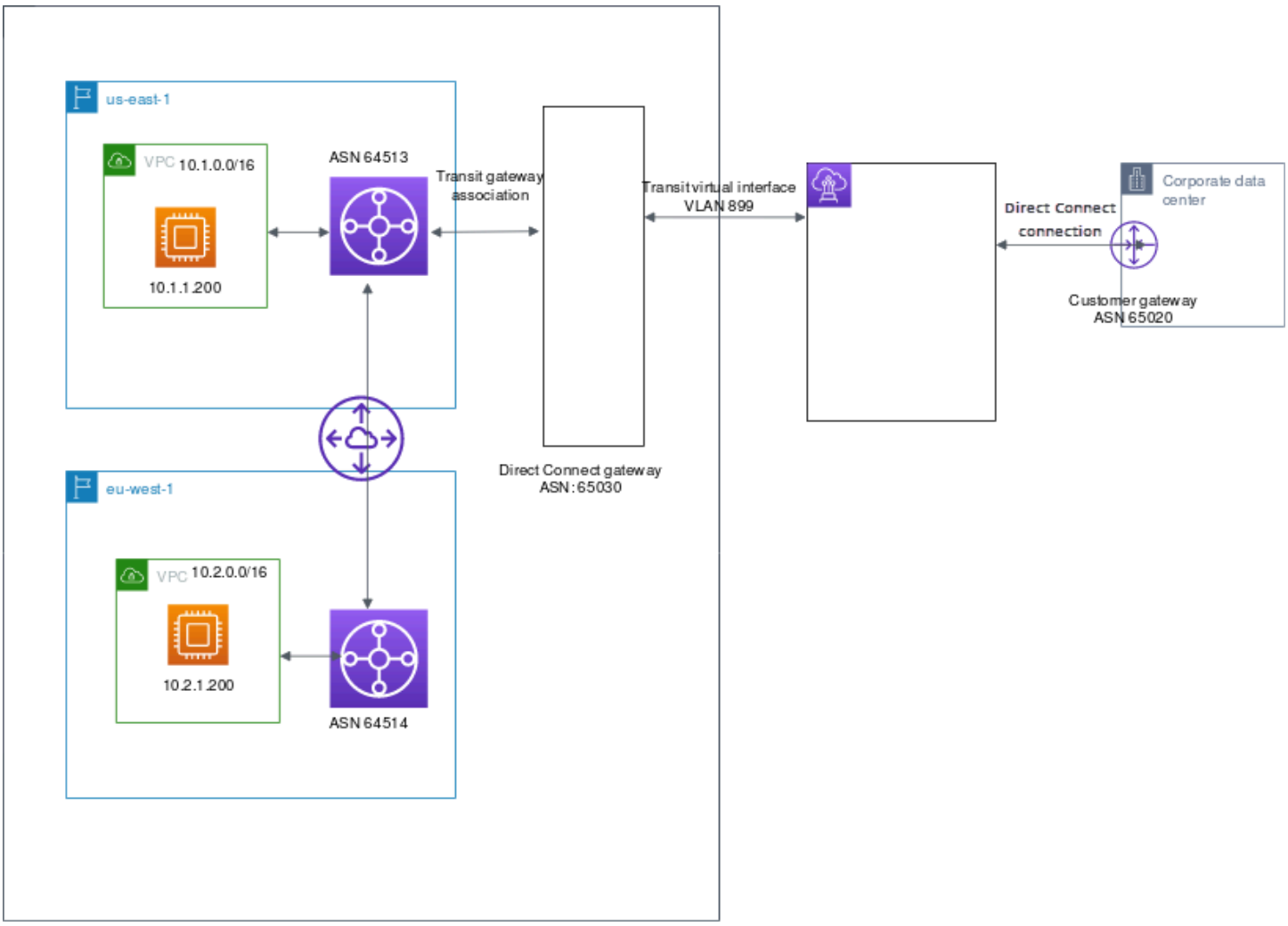
Les chevauchements de préfixes autorisés ne sont pas autorisés lorsque plusieurs passerelles de transit sont associées à une passerelle Direct Connect. Par exemple, si vous avez une passerelle de transit avec une liste de préfixes autorisés qui inclut 10.1.0.0/16 et une deuxième passerelle de transit 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 IPv4 réseaux, 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 peut retarder ou supprimer uniquement le trafic qui utilise ce préfixe.

Exemple : autorisé aux préfixes dans une configuration de passerelle de transit

Pensez à la configuration dans laquelle vous avez des instances dans deux AWS régions 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 Direct Connect .



Configurez les options suivantes pour les ressources :

- Passerelle Direct Connect : définissez l'ASN sur 65030. Pour de plus amples informations, veuillez consulter Création d'une passerelle Direct Connect.
- Interface virtuelle de transit : définissez le VLAN sur 899 et l'ASN de l'homologue du routeur client sur 65020. Pour de plus amples informations, veuillez consulter Créer une interface de transit virtuelle vers la passerelle Direct Connect.
- Association de la passerelle Direct Connect à la passerelle de transit : définissez les préfixes autorisés sur 10.0.0.0/8.

  Ce bloc d'adresse CIDR englobe les deux blocs d'adresse CIDR VPC (10.0.0.0/16 et 10.2.0.0/16). Pour de plus amples informations, veuillez consulter Associez ou dissociez une passerelle de transit à Direct Connect..

- Route VPC : pour acheminer le trafic depuis le VPC 10.2.0.0/16, créez une route dans la table de routage VPC avec une destination 0.0.0.0/0 et l'ID de passerelle de transit comme cible. Cela permet au trafic provenant du VPC d'atteindre la passerelle Direct Connect. Pour plus d'informations sur le routage vers une passerelle de transit, consultez la section Routage d'une passerelle de transit dans le guide de l'utilisateur Amazon VPC.

AWS Direct Connect Ressources de balises

Une balise est une étiquette que le propriétaire d'une ressource attribue à ses Direct Connect ressources. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises permettent au propriétaire de la ressource de classer vos Direct Connect ressources 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.

Par exemple, vous avez deux Direct Connect connexions dans une région, chacune située à 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 aucune signification sémantique 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, ses balises sont également supprimées.

Vous pouvez baliser les Direct Connect ressources suivantes à l'aide de la Direct Connect console, de l' Direct Connect API AWS CLI AWS Tools for Windows PowerShell, du SDK ou d'un AWS SDK. Lorsque vous utilisez ces outils pour gérer les balises, vous devez spécifier l'Amazon Resource Name (ARN) pour la ressource. Pour plus d'informations sur ARNs, consultez Amazon Resource Names (ARNs) 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	Oui	Oui	Oui	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 d'étiquette sont sensibles à la casse.

- Le `aws:` préfixe est réservé à l' AWS usage. 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 ne sont prises en charge que pour les connexions, les interconnexions et LAGs. Pour plus d'informations sur l'utilisation des balises dans le cadre de la gestion des coûts, consultez la section Utilisation des balises de répartition des coûts dans le guide de AWS Billing and Cost Management l'utilisateur.

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	« Hello, World! »	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

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des 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 conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Direct Connect, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service 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 son utilisation Direct Connect. Les rubriques suivantes expliquent comment procéder à la configuration Direct Connect pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos Direct Connect ressources.

Rubriques

Protection des données dans AWS Direct Connect

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans Direct Connect. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. 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 plus d'informations 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 AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (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 le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent 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 par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

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 Nom. Cela inclut lorsque vous travaillez avec Direct Connect ou d'autres Services

AWS utilisateurs de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez 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 interréseau dans AWS Direct Connect

Trafic entre les clients de service et sur site et les applications

Vous avez 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 Sécurité de l'infrastructure.
- Une association pour VPCs. Pour plus d'informations, consultez Associations de la passerelle privée virtuelle et Associations de la passerelle de transit.

Trafic entre les AWS ressources d'une 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 Sécurité de l'infrastructure.
- Une association pour VPCs. Pour plus d'informations, consultez Associations de la passerelle privée virtuelle et Associations de la passerelle de transit.

Chiffrement dans 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 IPsec connexion privée cryptée 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 les options de connectivité Amazon VPC-to-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 Direct Connect des connexions compatibles MACsec pour chiffrer vos données depuis le centre de données de votre entreprise jusqu'à l' Direct Connect emplacement. Pour de plus amples informations, veuillez consulter Sécurité MAC (MACsec).

Gestion des identités et des accès pour Direct Connect

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. 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 outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution de problèmes d'identité et d'accès dans Direct Connect)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Direct Connect fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques basées sur une identité pour Direct Connect)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session 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 savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des 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

Fonctionnalité 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
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble du fonctionnement de Direct Connect et des autres AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Direct Connect

Prend en charge les politiques basées sur l'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 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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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. 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. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM 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 AWS JSON 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. 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": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Ressources relatives aux politiques pour Direct Connect

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Direct Connect et leurs caractéristiques ARNs, consultez la section Ressources définies par Direct Connect dans le Guide de référence des AWS Direct Connect API. 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

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales 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.

ACLs dans Direct Connect

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette 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 ABAC, consultez Définition d'autorisations avec l'autorisation 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

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations de principals entre services pour Direct Connect

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour Direct Connect

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de 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 apparaissent dans votre Compte AWS répertoire et appartiennent au 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 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. 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.

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 IAM (console) 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 ARNs format de chaque type de ressource, voir Actions, ressources et clés de condition pour Direct Connect dans la référence d'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 Direct Connect
- Accès complet à 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 :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON 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. 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 politique suivant accorde un accès en lecture à Direct Connect.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

L'exemple de politique suivant accorde un accès complet à Direct Connect.

JSON

```
{
    "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 AWS JSON 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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Direct Connect utilise les méthodes suivantes ARNs :

Ressource de connexion directe ARNs

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 de ARNs, consultez Amazon Resource Names (ARNs) et AWS Service Namespaces.

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 consulter la liste des types de ressources Direct Connect et de leurs caractéristiques ARNs, reportez-vous à la section Types de ressources définis par Direct Connect dans le guide de l'utilisateur IAM. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Direct Connect.

Si un ARN de ressource ou un modèle d'ARN de ressource autre `*` que celui spécifié dans le `Resource` champ de la déclaration de politique IAM pour DescribeConnections, DescribeVirtualInterfaces, DescribeDirectConnectGateways, ou DescribeInterconnects DescribeLags, le modèle spécifié `Effect` ne se produira que si l'ID de ressource correspondant est également transmis dans l'appel d'API. Toutefois, si vous fournissez `*` en tant que ressource au lieu d'un ID de ressource spécifique dans la déclaration de politique IAM, l'identifiant spécifié `Effect` fonctionnera.

Dans l'exemple suivant, aucune des deux options spécifiées ne `Effect` réussira si l'`DescribeConnectionsaction` est appelée sans que la demande ne `connectionId` soit transmise.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
```

```
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

Toutefois, dans l'exemple suivant, l'`DescribeConnections`action fournie pour le `Resource` champ de la déclaration de politique IAM `"Effect": "Allow"` aboutira, qu'elle `connectionId` ait été spécifiée ou non dans la demande. *

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

Clés de condition

Les administrateurs peuvent utiliser les politiques AWS JSON 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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales 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 voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Vous pouvez utiliser les clés de condition avec la ressource de balise. Pour plus d'informations, consultez 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 Actions définies par Direct Connect.

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 d'afficher les informations relatives aux ressources Direct Connect de votre AWS compte. 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 peuvent toujours utiliser la console Direct Connect, associez également la politique AWS gérée suivante aux entités. Pour en savoir plus, consultez Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

```
directconnect
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. 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 permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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 Direct Connect

L'exemple de politique suivant accorde un accès en lecture à Direct Connect.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
```

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

Accès complet à Direct Connect

L'exemple de politique suivant accorde un accès complet à Direct Connect.

JSON

```
{
    "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.

JSON

```
 {
"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 les paires clé-valeur de balise qui peuvent être transmises dans une demande qui balise une ressource. AWS L'exemple suivant montre comment créer une politique qui permet d'utiliser l' 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.

JSON

```
{
    "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.

JSON

```
 {
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "environment"
```

```
            ]
          }
        }
      }
    }
```

Rôles liés à un service pour Direct Connect

AWS Direct Connect utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. Direct Connect Les rôles liés au service sont prédéfinis par 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 Direct Connect car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Direct Connect définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Direct Connect peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance 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. Cela protège vos Direct Connect ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès 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 avec un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Direct Connect

Direct Connect utilise un rôle lié à un service nommé. `AWSServiceRoleForDirectConnect` Cela permet Direct Connect de récupérer le MACSec secret stocké 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 Direct Connect doit disposer des autorisations requises. Pour accorder les autorisations requises, associez la stratégie suivante à l'identité IAM.

JSON

```
{
    "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 Direct Connect

Il n'est pas nécessaire de créer manuellement un rôle lié à un service. AWS Direct Connect crée pour vous le rôle lié au service. Lorsque vous exécutez la `associate-mac-sec-key` commande, AWS

crée un rôle lié à un service qui permet Direct Connect de récupérer les MACsec secrets stockés en votre AWS Secrets Manager nom dans l'API AWS Management Console AWS CLI, le ou l' AWS API.

> **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, puis que vous devez le créer à nouveau, vous pouvez utiliser le même processus pour recréer le rôle dans votre compte. Direct Connect crée à nouveau le rôle lié au 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'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `directconnect.amazonaws.com` service. Pour plus d'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 Direct Connect

Direct Connect ne vous permet pas de modifier le rôle `AWSServiceRoleForDirectConnect` lié au service. 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 plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour 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 AWS Secrets Manager Web. L' AWS Management Console AWS API Direct Connect nettoie les ressources et supprime le rôle lié au service pour vous. AWS CLI

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 Direct Connect service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, attendez quelques minutes, puis réessayez l'opération.

Pour supprimer Direct Connect les ressources utilisées par **`AWSServiceRoleForDirectConnect`**

1. Supprimez l'association entre toutes les MACsec clés et connexions. Pour de plus amples informations, consultez the section called "Supprimer l'association entre une clé MACsec secrète et une connexion".
2. Supprimez l'association entre toutes les MACsec clés et LAGs. Pour de plus amples informations, consultez the section called "Supprimer l'association entre une clé MACsec secrète et un LAG".

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForDirectConnect` service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles Direct Connect liés à un service

Direct Connect prend en charge l'utilisation de rôles liés à un service dans tous les Régions AWS endroits où la fonctionnalité de sécurité MAC est disponible. Pour plus d'informations, consultez Emplacements AWS Direct Connect.

AWS politiques gérées pour AWS Direct Connect

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

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

AWS politique gérée : AWSDirect ConnectFullAccess

Vous pouvez associer la politique `AWSDirectConnectFullAccess` à vos identités IAM. Cette politique accorde des autorisations permettant un accès complet à Direct Connect.

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectFullAccess dans AWS Management Console.

AWS politique gérée : AWSDirect ConnectReadOnlyAccess

Vous pouvez associer la politique `AWSDirectConnectReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations permettant un accès en lecture seule à. Direct Connect

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectReadOnlyAccess dans AWS Management Console.

AWS politique gérée : AWSDirect ConnectServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé AWSServiceRoleForDirectConnectpour permettre de récupérer les secrets Direct Connect de sécurité MAC en votre nom. Pour de plus amples informations, veuillez consulter the section called "Rôles liés à un service".

Pour consulter les autorisations relatives à cette politique, consultez AWSDirectConnectServiceRolePolicy dans AWS Management Console.

Direct Connect mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées Direct Connect depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du Direct Connect document.

Modification	Description	Date
AWSDirectConnectServiceRolePolicy : nouvelle politique	Pour prendre en charge la sécurité MAC, le rôle AWSServiceRoleForDirectConnectlié au service a été ajouté.	31 mars 2021
Direct Connect a commencé à suivre les modifications	Direct Connect a commencé à suivre les modifications apportées à ses politiques AWS gérées.	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
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Direct Connect

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 besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification 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 vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez 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 un rôle de service. Mary n'est pas autorisée à transmettre 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 besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures Compte AWS à moi 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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Direct Connect prend en charge ces fonctions, consultez Comment Direct Connect fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Connexion et surveillance AWS Direct Connect

Vous pouvez utiliser les outils de surveillance automatique pour surveiller Direct Connect et signaler en cas de 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 de plus amples informations, veuillez consulter Surveillez 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 Enregistrez les appels Direct Connect d'API en utilisant AWS CloudTrail la section Utilisation des fichiers CloudTrail journaux dans le Guide de AWS CloudTrail l'utilisateur.

Pour de plus amples informations, veuillez consulter Surveillez les ressources Direct Connect.

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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans AWS Direct Connect

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, 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 AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, Direct Connect propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Pour plus d'informations sur l'utilisation d'un VPN avec AWS Direct Connect, consultez AWS Direct Connect Plus VPN.

Basculement

Le AWS Direct Connect Resiliency Toolkit fournit un assistant de connexion doté de plusieurs modèles de résilience qui vous aident à commander des connexions dédiées pour atteindre votre objectif de SLA. 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.

- 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 the section called “AWS Direct Connect Boîte à outils de résilience”.

Sécurité de l'infrastructure dans Direct Connect

En tant que service géré, AWS Direct Connect il est protégé par les procédures de sécurité du réseau AWS mondial. Vous utilisez des appels d'API AWS publiés pour accéder 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 depuis n'importe quel emplacement réseau, mais vous pouvez prendre Direct Connect en charge les politiques d'accès basées sur les ressources, qui

peuvent inclure des restrictions basées sur l'adresse IP source. Vous pouvez également utiliser des Direct Connect politiques pour contrôler l'accès depuis des points de terminaison Amazon Virtual Private Cloud (Amazon VPC) spécifiques ou spécifiques. VPCs En fait, cela isole l'accès réseau à une Direct Connect ressource donnée uniquement du VPC spécifique au sein AWS du réseau. Pour obtenir un exemple, consultez the section called "Exemples de politiques basées sur une identité pour Direct Connect".

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 protéger votre réseau de manière plus sécurisée contre le piratage BGP, consultez Comment contribue à sécuriser AWS le routage Internet.

Utiliser la Direct Connect CLI

Vous pouvez utiliser le AWS CLI pour créer et utiliser des Direct Connect ressources.

L'exemple suivant utilise les AWS CLI commandes pour créer une Direct Connect connexion. 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 Guide de l'utilisateur AWS Command Line Interface.

Table des matières

Étape 1 : Créer une connexion

La première étape consiste à envoyer une demande de connexion. Assurez-vous de connaître la vitesse du port dont vous avez besoin et son Direct Connect emplacement. Pour de plus amples informations, veuillez consulter Connexions dédiées et hébergées.

Pour créer une demande de connexion

1. Décrivez les Direct Connect emplacements de 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, la sortie est extraite dans 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 Direct Connect connexion, vous devez créer une interface virtuelle pour commencer à l'utiliser. 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 AWS des services qui ne figurent pas dans un VPC. Vous pouvez créer une interface virtuelle qui prend en charge IPv4 IPv6 le trafic.

Avant de commencer, veillez à prendre connaissance des conditions préalables dans the section called “Conditions préalables pour les interfaces virtuelles”.

Lorsque vous créez une interface virtuelle à l'aide de AWS CLI, la sortie inclut des informations de configuration génériques du routeur. Pour créer une configuration de routeur spécifique à votre appareil, utilisez la Direct Connect console. 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 IPv4 le trafic, vous avez besoin d' IPv4 adresses privées pour chaque fin de session de peering BGP. Vous pouvez spécifier vos propres IPv4 adresses ou laisser Amazon les générer pour vous. Dans l'exemple suivant, les IPv4 adresses 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 qui prend en charge le IPv6 trafic, utilisez la même commande que ci-dessus et spécifiez `ipv6` le `addressFamily` paramètre. Vous ne pouvez pas spécifier vos propres IPv6 adresses pour la session de peering 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 IPv4 le trafic, vous devez également spécifier des IPv4 adresses publiques pour chaque fin de session de peering BGP, ainsi que IPv4 les itinéraires publics que vous allez annoncer via BGP. L'exemple suivant crée une interface virtuelle publique pour le IPv4 trafic.

```
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 qui prend en charge IPv6 le trafic, vous pouvez spécifier IPv6 les itinéraires que vous allez annoncer via BGP. Vous ne pouvez pas spécifier d' IPv6 adresses pour la session de peering ; Amazon vous attribue des IPv6 adresses. L'exemple suivant crée une interface virtuelle publique pour le IPv6 trafic.

```
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>
```

Enregistrez les appels Direct Connect d'API en utilisant AWS CloudTrail

Direct Connect est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Direct Connect. CloudTrail capture tous les appels d'API Direct Connect sous forme d'événements. Les appels capturés incluent des appels provenant de la Direct Connect console et des appels de code vers les opérations de l' Direct Connect API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour Direct Connect. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite Direct Connect, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Direct Connect informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Direct Connect, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS . Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Direct Connect, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge

- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les Direct Connect actions sont enregistrées CloudTrail et documentées dans la référence de l'Direct Connect API. Par exemple, les appels aux `CreatePrivateVirtualInterface` actions `CreateConnection` et génèrent des entrées dans les fichiers CloudTrail journaux.

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 les éléments suivants :

- Si la demande a été faite avec les informations d'identification root ou Gestion des identités et des accès AWS (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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément `userIdentity` CloudTrail.

Comprendre les entrées du fichier Direct Connect journal

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

Voici des exemples d'enregistrements de CloudTrail journal pour 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
    },
    ...
  ]
}
```

Surveiller Direct Connect les ressources

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 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 Surveillez 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 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 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 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.

Surveillez avec Amazon CloudWatch

Vous pouvez surveiller les 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. Les données métriques de chaque intervalle sont une agrégation d'au moins deux échantillons collectés pendant cet intervalle.

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

Direct Connect métriques et dimensions

Des métriques sont disponibles pour les connexions Direct Connect physiques et les interfaces virtuelles.

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.

Métrique	Description
	Cette métrique est disponible pour les connexions dédiées et hébergées. **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 : aucune unité n'a été renvoyée pour cette métrique.
`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

Métrique	Description
`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
`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

Métrique	Description
`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`	Le nombre total d'erreurs pour tous les types d'erreurs de niveau MAC enregistrées par le AWS périphérique. Le total comprend les erreurs de contrôle de redondance cyclique (CRC). La cause première de ces erreurs peut être du côté du client ou du AWS côté du client. 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 de toutes les erreurs pour l'intervalle sélectionné en CloudWatch 5 minutes, par exemple, appliquez la statistique « somme ». 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
`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 Dimensions disponibles avec Direct Connect. Unités : dBm

Métrique	Description
`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 Dimensions disponibles avec Direct Connect. 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.
`ConnectionDiscardsPpsEgress`	Taux de rejet de paquets pour les données sortantes du AWS côté de la connexion. Cette métrique suit les paquets abandonnés en raison de débordements de mémoire tampon, de congestion de l'interface ou d'autres conditions du réseau. 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. Unités : paquets par seconde

Direct Connect métriques de l'interface virtuelle

Les métriques suivantes sont disponibles à partir des interfaces 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

Direct Connect dimensions disponibles

Vous pouvez filtrer les 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'interface virtuelle Direct Connect et filtre les données en fonction de l'interface virtuelle.

Rubriques

- Afficher les Direct Connect CloudWatch métriques
- Créez des CloudWatch alarmes Amazon pour surveiller Direct Connect les connexions

Afficher les Direct Connect CloudWatch métriques

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**
>
> Lorsque vous surveillez Direct Connect via Direct Connect CloudWatch, vous pouvez demander des mesures à intervalles d'une minute. Cependant, la fréquence de mise à jour réelle est contrôlée par CloudWatch. Comme il CloudWatch contrôle l'intervalle, Direct Connect ne peut pas toujours garantir des intervalles inférieurs à cinq minutes.

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 Direct Connect console

1. Ouvrez la Direct Connectconsole sur 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"
```

Créez des CloudWatch alarmes Amazon pour surveiller 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 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 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.

Direct Connect quotas

Le tableau suivant répertorie les quotas associés à Direct Connect.

Composant	Quota	Commentaires
Interfaces virtuelles privées ou publiques par connexion Direct Connect dédiée	50	Cette limite ne peut pas être augmentée.
Interfaces virtuelles de transit par connexion Direct Connect dédiée. Les interfaces virtuelles Transit peuvent être utilisées pour se connecter à un réseau central Transit Gateway ou AWS Cloud WAN. Pour de plus amples informations, veuillez consulter Passerelles.	4	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Interfaces virtuelles privées ou publiques par connexion Direct Connect dédiée et interfaces virtuelles de transit par connexion 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 Direct Connect hébergée	1	Cette limite ne peut pas être augmentée.

Composant	Quota	Commentaires
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 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'interfa ces virtuelles de transit autorisées est désormais de quatre (4) et est compté par rapport au maximum de 51 interface s 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 annoncez plus de 100 routes chacune pour IPv4 et IPv6 via la session BGP, la session BGP passera en état d'inactivité et la session BGP sera interrompue.	100 pour IPv4 et IPv6	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
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 liens (LAGs) 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.
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 Direct Connect passerelle	20	Cette limite ne peut pas être augmentée.
Passerelles de transit par Direct Connect passerelle	6	Cette limite ne peut pas être augmentée.

Composant	Quota	Commentaires
Nombre maximum de préfixes de route annoncés entre une passerelle Direct Connect du réseau central AWS Cloud WAN connectée à une connexion sur site. **Note** Toutes les interfaces virtuelle s de transit connectées à cette passerelle Direct Connect recevront tous les préfixes de route annoncés par le réseau central.	5 000	Contactez votre architecte de solutions (SA, Solutions Architect) ou votre responsable de compte technique (TAM, Technical Account Manager) pour obtenir une aide supplémentaire.
Interfaces virtuelles (privées ou de transit) par 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	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 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.

Composant	Quota	Commentaires
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.

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), 100 Gbit/s : 100GBASE- et 400 Gbit/s : 400GBASE-. LR4 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

Limites ASN

Les limites suivantes s'appliquent aux numéros de système autonomes (ASNs) utilisés avec Direct Connect :

- Plage ASN côté client : 1 à 4 294 967 294

  - ASNs: 1 à 2147483647
  - Longtemps ASNs : 1 à 4294967294
- ASN côté Amazon : valeurs fixes attribuées par AWS (généralement 7224 pour les interfaces virtuelles publiques)
- Gammes ASN privées :
  - privé ASNs : 64 512 à 65 534
  - long privé ASNs : 4 200 000 000 à 4 294 967 294

> **Note**
>
> Pour les interfaces virtuelles publiques, votre ASN doit être un ASN privé ou déjà enregistré et autorisé à être utilisé avec l'interface virtuelle.

Considérations relatives à l'équilibrage de charge

Si vous souhaitez utiliser l'équilibrage de charge avec plusieurs publics VIFs, ceux-ci VIFs doivent tous se trouver dans la même région.

Résoudre les problèmes Direct Connect

Les informations de dépannage suivantes peuvent vous aider à diagnostiquer et à résoudre les problèmes liés à votre connexion Direct Connect .

Table des matières

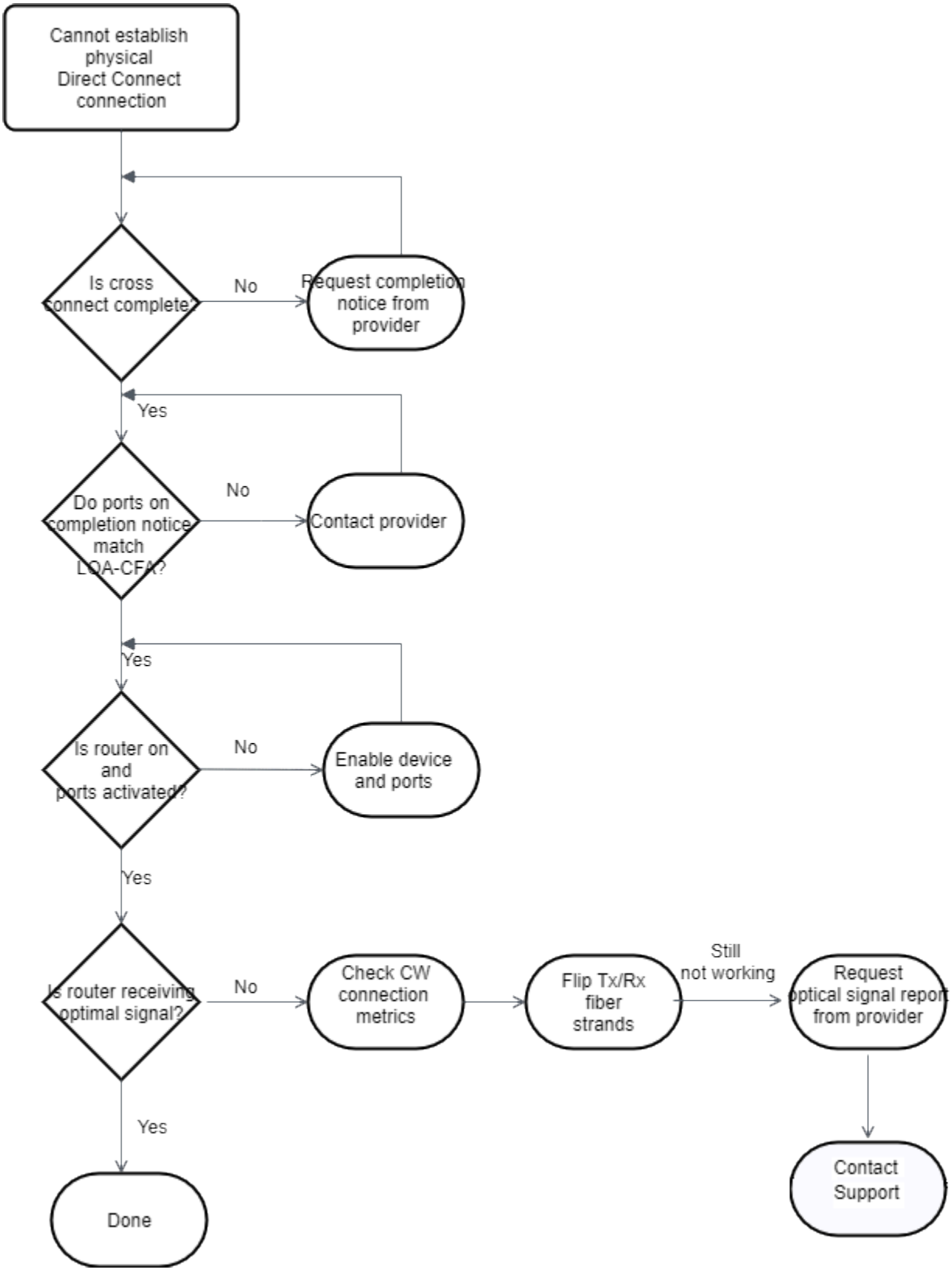
Résoudre les problèmes (physiques) liés à la couche 1

Si vous ou votre fournisseur de réseau rencontrez des difficultés pour établir une connectivité physique avec un 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 Résoudre les problèmes liés à la couche 2 (liaison de données). Selon le point de terminaison Direct Connect qui dessert votre connexion, la négociation automatique devra peut-être être activée ou désactivée en conséquence.
4. Vérifiez que le routeur reçoit un signal optique acceptable sur la connexion transversale.
5. Essayez de retourner (également connu sous le nom de laminage) les fils Tx/Rx de fibres.

6. Consultez les CloudWatch statistiques Amazon pour Direct Connect. Vous pouvez vérifier les valeurs Tx/Rx optiques de l' Direct Connect appareil (1 Gbit/s et 10 Gbit/s), le nombre d'erreurs physiques et l'état de fonctionnement de l'appareil. 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.

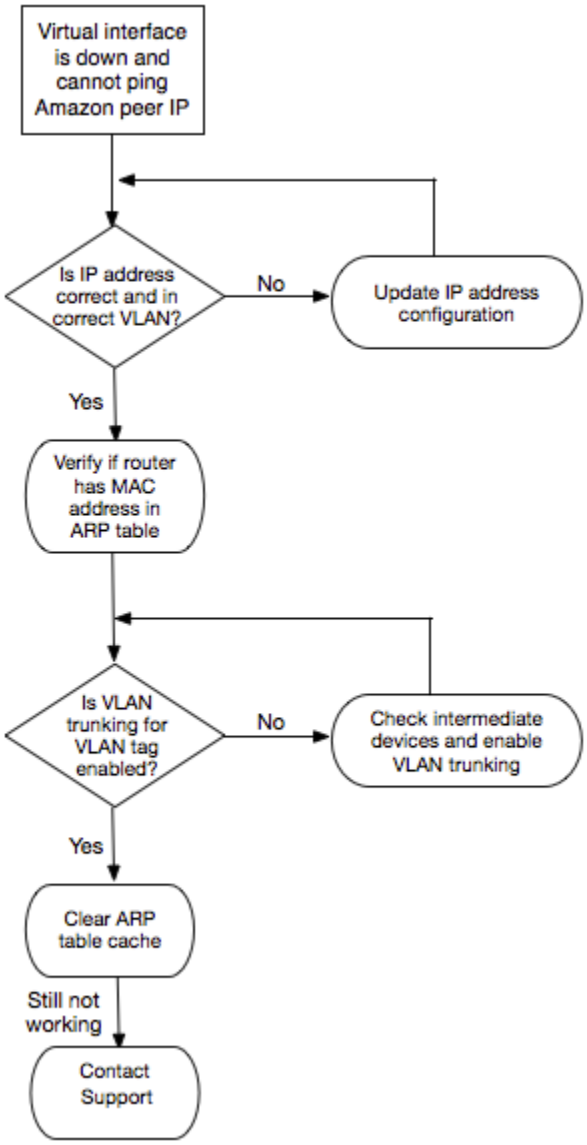

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Résoudre les problèmes liés à la couche 2 (liaison de données)

Si votre connexion 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.



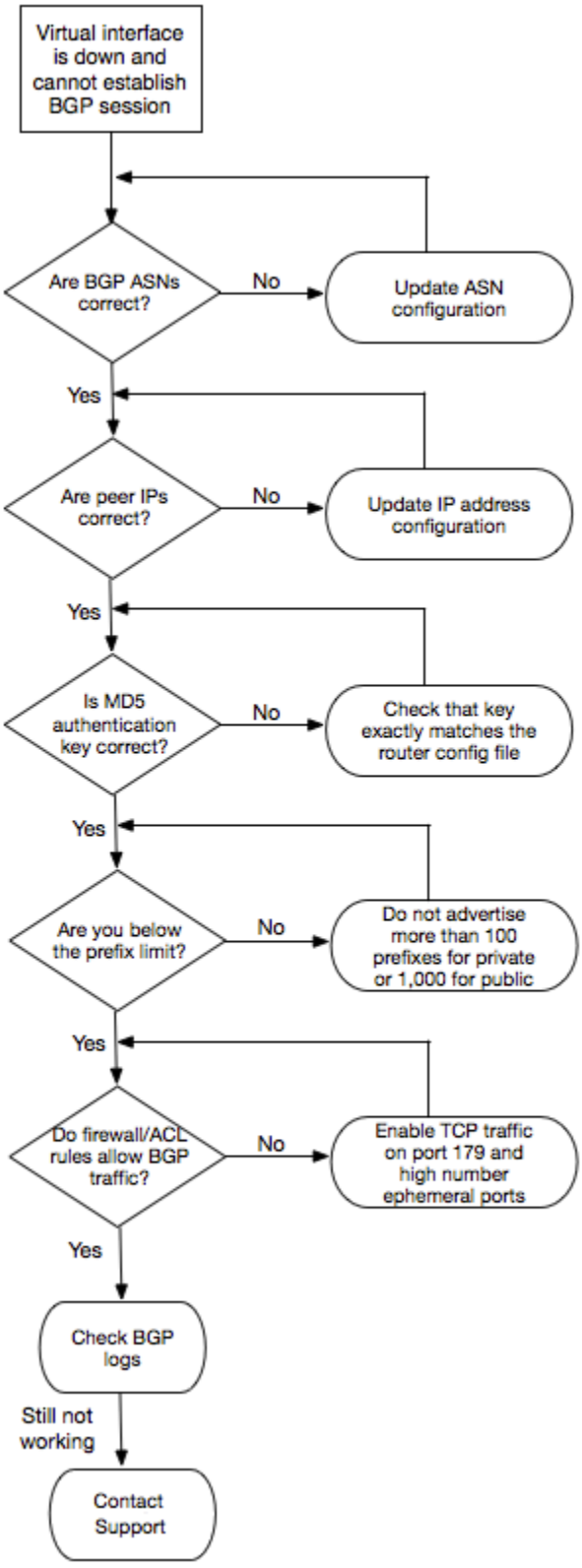
Si la session BGP n'est toujours pas établie après la vérification de ces étapes, consultez Résoudre les problèmes liés à la couche 3/4 (réseau/transport). Si la session BGP est établie, mais que vous rencontrez des problèmes de routage, consultez Résoudre les problèmes de routage.

Résoudre les problèmes liés à la couche 3/4 (réseau/transport)

Imaginons une situation dans laquelle votre connexion Direct Connect physique est active et où vous pouvez envoyer un ping à l'adresse IP du pair Amazon. Si votre interface virtuelle est active et que la session d'appairage BGP ne peut pas être établie, suivez 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 homologues IPs des deux côtés de la session d'appairage BGP sont correctement configurés.
3. Assurez-vous que votre clé MD5 d'authentification est configurée et qu'elle correspond exactement à la clé figurant 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 Résoudre les problèmes de routage.

Résoudre les problèmes liés à l'ASN de longue durée

Si vous rencontrez des problèmes avec de longues configurations ASN, suivez les étapes ci-dessous pour les résoudre :

La session BGP échoue avec un ASN long

Symptômes : la session BGP ne peut pas être établie après avoir configuré un long ASN

Cause : le routeur local peut ne pas prendre en charge la fonctionnalité ASN prolongée

Résolution :

- Vérifiez que votre routeur est compatible avec la norme RFC 6793
- Vérifiez la configuration BGP pour un format ASN cohérent
- Consultez les journaux BGP pour détecter les erreurs de négociation des capacités

Les réponses de l'API indiquent l'ASN comme 0

Symptômes : les réponses de l'API affichent `asn` le champ sous la forme 0

Cause : Ce comportement est attendu lorsque l'ASN réel dépasse 2 147 483 647

Résolution : utilisez le `asnLong` champ dans les réponses de l'API pour obtenir la valeur ASN correcte

Migration de l'ASN vers des problèmes ASN de longue durée

Symptômes : perte de connectivité lors de la migration ASN

Cause : le rétablissement de la session BGP est requis pour les modifications de l'ASN

Résolution :

- Planifier la migration pendant les fenêtres de maintenance
- Mettre à jour une interface virtuelle à la fois
- Surveiller l'état de la session BGP lors des modifications
- Vérifier la convergence des tables de routage après la migration

Si vous continuez à rencontrer des problèmes liés aux longues configurations ASN après avoir suivi ces étapes de dépannage, contactez le AWS Support en fournissant les informations suivantes :

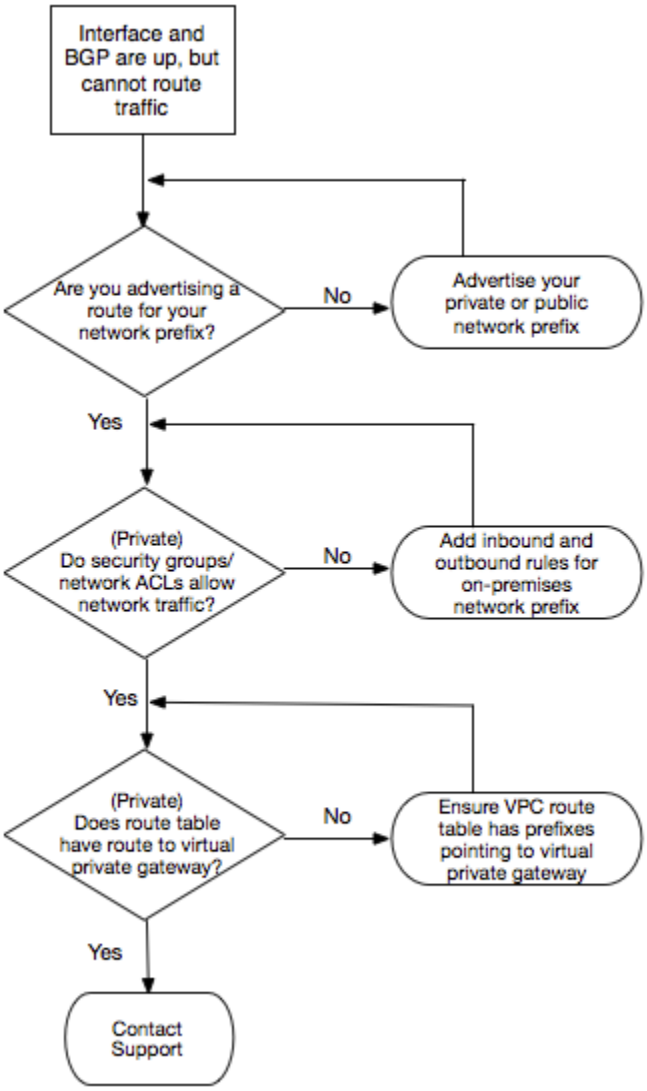
- ID d'interface virtuelle ou ID d'homologue BGP
- Valeurs ASN configurées (ASN et ASN long)
- Modèle de routeur et version logicielle
- Configuration BGP et journaux
- Messages d'erreur ou symptômes observés

Résoudre les 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 votre réseau ACLs autorisent le trafic entrant et sortant pour votre préfixe réseau local. Pour plus d'informations, consultez la section Groupes de sécurité et réseau ACLs dans le guide de l'utilisateur 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 les versions de AWS Direct Connect. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Support pour un ASN long	Vous pouvez désormais utiliser des valeurs ASN longues pour les sessions BGP avec des interfaces Direct Connect virtuelles.	24 juillet 2025
Création d'une association entre la passerelle Direct Connect et un réseau AWS Network Manager central	Vous pouvez désormais créer une association de passerelle Direct Connect directement entre Direct Connect et un réseau central AWS Cloud WAN.	25 novembre 2024
Support pour 400G	Rubriques mises à jour pour inclure la prise en charge des connexions 400G.	18 juillet 2024
Ajout d'une limite SiteLink de préfixes	Un préfixe limite pour SiteLink a été ajouté à la rubrique Quotas et limites.	15 juin 2023
Support pour SiteLink	Vous pouvez créer une interface virtuelle privée qui permet la connectivité entre deux points de présence Direct Connect (PoPs) dans la même AWS région.	1er décembre 2021
Support de sécurité MAC	Vous pouvez utiliser Direct Connect des connexions compatibles MACsec pour	31 mars 2021

	chiffrer vos données depuis le centre de données de votre entreprise jusqu'à l' Direct Connect emplacement.	
Support pour 100G	Rubriques mises à jour pour inclure la prise en charge des connexions dédiées de 100G.	12 février 2021
Nouveau site en Italie	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement en Italie.	22 janvier 2021
Nouveau site en Israël	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement en Israël.	7 juillet 2020
Support pour les tests de basculement du Resiliency Toolkit	Utilisez la fonctionnalité de test de basculement du Resiliency Toolkit pour tester la résilience de vos connexions.	3 juin 2020
CloudWatch Support métrique VIF	Vous pouvez surveiller les Direct Connect connexion s physiques et les interface s virtuelles à l'aide de CloudWatch.	11 mai 2020
AWS Direct Connect Boîte à outils de résilience	Le AWS Direct Connect Resiliency Toolkit fournit un assistant de connexion doté de plusieurs modèles de résilience qui vous aident à commander des connexions dédiées pour atteindre votre objectif de SLA.	7 octobre 2019

Support régional supplémentaire pour le support pour AWS Transit Gateway tous les comptes	Support régional supplémentaire pour AWS Transit Gateway tous les comptes.	30 septembre 2019
AWS Direct Connect support pour AWS Transit Gateway	Vous pouvez utiliser une Direct Connect passerelle pour connecter votre Direct Connect connexion via une interface virtuelle de transit à la passerelle de transit VPCs ou VPNs attachée à celle-ci. Vous associez une passerelle Direct Connect à la passerelle de transit. Créez ensuite une interface virtuelle de transit pour votre Direct Connect connexion à la passerelle Direct Connect.	27 mars 2019
Support pour cadres Jumbo	Vous pouvez envoyer des images jumbo (9001 MTU). Direct Connect	11 octobre 2018
Communautés BGP à 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.	6 février 2018
Direct Connect passerelle	Vous pouvez utiliser une passerelle Direct Connect pour connecter votre Direct Connect connexion VPCs à des régions éloignées.	1er novembre 2017

CloudWatch Métriques Amazon	Vous pouvez consulter CloudWatch les statistiques de vos Direct Connect connexion s.	29 juin 2017
Groupes d'agrégation de liens	Vous pouvez créer un groupe d'agrégation de liens (LAG) pour agréger plusieurs Direct Connect connexions.	13 février 2017
IPv6 soutien	Votre interface virtuelle peut désormais prendre en charge une session de peering IPv6 BGP.	1er décembre 2016
Support de balisage	Vous pouvez désormais étiqueter vos Direct Connect ressources.	4 novembre 2016
LOA-CFA en libre-service	Vous pouvez désormais télécharger votre lettre d'autorisation et votre attributi on d'installation de connexion (LOA-CFA) à l'aide de la Direct Connect console ou de l'API.	22 juin 2016
Nouveau site 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).	3 juin 2016
Nouveau site à Amsterdam	Rubrique mise à jour pour inclure l'ajout du nouvel emplacement à Amsterdam dans la région Europe (Francfort).	19 mai 2016

Nouveaux sites à Portland, en 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).	27 avril 2016
Nouveau site 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).	le 9 décembre 2015
Nouveaux sites 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)).	27 novembre 2015
Nouveau site dans la région de Chine (Pékin)	Rubriques mises à jour pour inclure l'ajout du nouvel emplacement à Beijing dans la région Chine (Beijing).	14 avril 2015
Nouveau site de Las Vegas dans la région de l'ouest des États-Unis (Oregon)	Rubriques mises à jour pour inclure l'ajout du nouveau site de Direct Connect Las Vegas dans la région de l'ouest des États-Unis (Oregon).	10 novembre 2014

Nouvelle région de l'UE (Francfort)	Sujets mis à jour pour inclure l'ajout de nouveaux Direct Connect sites desservant la région de l'UE (Francfort).	23 octobre 2014
Nouveaux sites dans la région Asie-Pacifique (Sydney)	Rubriques mises à jour pour inclure l'ajout de nouveaux Direct Connect sites desservant la région Asie-Paci fique (Sydney).	14 juillet 2014
Support pour AWS CloudTrail	Ajout d'une nouvelle rubrique expliquant comment vous pouvez l'utiliser CloudTrail pour enregistrer l'activité Direct Connect.	4 avril 2014
Support pour accéder aux AWS régions éloignées	Ajout d'une nouvelle rubrique pour expliquer comment accéder aux ressources publiques d'une région à distance.	19 décembre 2013
Support pour les connexions hébergées	Rubriques mises à jour pour inclure la prise en charge des connexions hébergées.	22 octobre 2013
Nouveau site dans la région UE (Irlande)	Sujets mis à jour pour inclure l'ajout du nouveau Direct Connect site desservant la région UE (Irlande).	24 juin 2013
Nouveau site de Seattle dans la région de l'ouest des États-Unis (Oregon)	Rubriques mises à jour pour inclure l'ajout du nouveau Direct Connect site de Seattle desservant la région de l'ouest des États-Unis (Oregon).	8 mai 2013

Support pour l'utilisation d'IAM avec Direct Connect	Ajout d'une rubrique sur l'utilisation Gestion des identités et des accès AWS avec Direct Connect.	21 décembre 2012
Nouvelle région Asie-Pacifique (Sydney)	Rubriques mises à jour pour inclure l'ajout du nouveau Direct Connect site desservant la région Asie-Pacifique (Sydney).	14 décembre 2012
Nouvelle AWS Direct Connect console et régions des États-Unis (Virginie du Nord) et de l'Amérique du Sud (Sao Paulo)	Le guide de Direct Connect démarrage a été remplacé par le guide de Direct Connect l'utilisateur. Ajout de nouvelles rubriques pour couvrir la nouvelle Direct Connect console, ajout d'une rubrique sur la facturation, ajout d'informations sur la configuration du routeur et mise à jour de rubriques pour inclure l'ajout de deux nouveaux Direct Connect sites desservant les régions des États-Unis de l'Est (Virginie du Nord) et de l'Amérique du Sud (Sao Paulo).	13 août 2012

Support aux régions de l'UE (Irlande), de l'Asie-Pacifique (Singapour) et de l'Asie-Pacifique (Tokyo)	Ajout d'une nouvelle section de résolution des problèmes et de rubriques mises à jour pour inclure l'ajout de quatre nouveaux Direct Connect sites desservant les régions de l'ouest des États-Unis (Californie du Nord), de l'UE (Irlande), de l'Asie-Pacifique (Singapour) et de l'Asie-Pacifique (Tokyo).	10 janvier 2012
Support pour la région de l'ouest des États-Unis (Californie du Nord)	Rubriques mises à jour pour inclure l'ajout de la région USA Ouest (Californie du Nord).	8 septembre 2011
Publication publique	La première version de Direct Connect.	3 août 2011

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.