AWS Livre blanc

Connectivité hybride

Connectivité hybride: AWS Livre blanc

Table of Contents

Connectivité hybride

Date de publication : 6 juillet 2023 (Révisions du document)

De nombreuses entreprises doivent connecter leurs centres de données sur site, leurs sites distants et le cloud. Un réseau hybride connecte ces différents environnements. Ce livre blanc décrit les éléments de base d'AWS et les principales exigences à prendre en compte pour choisir le modèle de connectivité hybride qui vous convient le mieux. Pour vous aider à déterminer la solution la mieux adaptée à votre activité et à vos exigences techniques, nous fournissons des arbres de décision pour vous guider tout au long du processus de sélection logique.

Introduction

Une organisation moderne utilise un large éventail de ressources informatiques. Dans le passé, il était courant d'héberger ces ressources dans un centre de données sur site ou une installation de colocation. Avec l'adoption croissante du cloud computing, les entreprises fournissent et consomment des ressources informatiques provenant de fournisseurs de services cloud via une connexion réseau. Organisations peuvent choisir de migrer une partie ou la totalité de leurs ressources informatiques existantes vers le cloud. Dans les deux cas, un réseau commun est nécessaire pour connecter les ressources sur site et dans le cloud. La coexistence de ressources sur site et dans le cloud est appelée cloud hybride, et le réseau commun qui les connecte est appelé réseau hybride. Même si votre entreprise conserve toutes ses ressources informatiques dans le cloud, elle peut tout de même avoir besoin d'une connectivité hybride vers des sites distants.

Vous avez le choix entre plusieurs modèles de connectivité. Bien que le fait de disposer d'options apporte de la flexibilité, le choix de l'option optimale nécessite une analyse des exigences commerciales et techniques, et l'élimination des options qui ne conviennent pas. Vous pouvez regrouper les exigences en fonction de considérations telles que la sécurité, le délai de déploiement, les performances, la fiabilité, le modèle de communication, l'évolutivité, etc. Une fois qu'ils ont soigneusement collecté, analysé et pris en compte les exigences, les architectes du réseau et du cloud peuvent identifier les éléments constitutifs et les solutions de réseau AWS hybride applicables. Pour identifier et sélectionner le ou les modèles optimaux, les architectes doivent comprendre les avantages et les inconvénients de chaque modèle. Il existe également des limitations techniques qui peuvent entraîner l'exclusion d'un modèle par ailleurs adapté.

Pour simplifier le processus de sélection, ce livre blanc vous guide à travers chaque élément clé dans un ordre logique. Pour chaque considération, des questions sont utilisées pour recueillir

les exigences. L'impact de chaque décision de conception est identifié, ainsi que les solutions potentielles. Le livre blanc présente des arbres de décision pour certaines considérations afin de faciliter le processus décisionnel, d'éliminer les options et de comprendre les conséquences de chaque décision. Il se termine par un scénario couvrant un cas d'utilisation hybride, en appliquant la sélection et la conception du modèle de end-to-end connectivité. Vous pouvez utiliser cet exemple pour voir comment exécuter les processus décrits dans ce livre blanc dans un exemple pratique.

Ce livre blanc a pour but de vous aider à sélectionner et à concevoir un modèle de connectivité hybride optimal. Ce livre blanc est structuré comme suit :

- Éléments de base de la connectivité hybride — Vue d'ensemble des AWS services utilisés pour la connectivité hybride.
- Considérations relatives à la sélection et à la conception de la connectivité : définition de chaque modèle de connectivité, de la manière dont chacun influe sur la décision de conception, des questions d'identification des exigences, des solutions et des arbres de décision.
- Un cas d'utilisation par un client - Un exemple de la façon d'appliquer les considérations et les arbres de décision dans la pratique.

Êtes-vous Well-Architected ?

Le AWSWell-Architected Framework vous aide à comprendre les avantages et les inconvénients des décisions que vous prenez lors de la création de systèmes dans le cloud. Les six piliers du Framework vous permettent d'apprendre les meilleures pratiques architecturales pour concevoir et exploiter des systèmes fiables, sécurisés, efficaces, rentables et durables. À l'aide du AWS Well-Architected Tool, disponible gratuitement dans le AWS Management Console, vous pouvez évaluer votre charge de travail par rapport à ces meilleures pratiques en répondant à une série de questions pour chaque pilier.

Pour obtenir des conseils d'experts supplémentaires et les meilleures pratiques relatives à votre architecture cloud (déploiements d'architecture de référence, diagrammes et livres blancs), consultez le Centre d'architecture. AWS

AWSéléments constitutifs de la connectivité hybride

Une architecture de connectivité réseau hybride repose sur trois éléments constitutifs :

- Connexions réseau hybrides : types de connexion entre les services de AWS connectivité et les dispositifs de passerelle client sur site.
- AWSservices de connectivité hybrides : les AWS services qui fournissent la connectivité et le routage entre l'infrastructure du client etAWS.
- Dispositif de passerelle client sur site : appareil du réseau existant du client qui est le point de terminaison local pour la connexion réseau hybride. Les différents types de connexion ont des exigences techniques différentes pour ces appareils, qui sont abordées dans les sections suivantes.

Connexions réseau hybrides

Vous pouvez vous connecter à une machine sur site de différentes façons. AWS Ce livre blanc se concentre sur la manière dont ces différentes méthodes peuvent être combinées dans des architectures globales. Toutefois, un bref aperçu des différentes options (AWS Direct Connectréseau privé virtuel de site à site et Transit Gateway Connect) est fourni.

AWS Direct Connect

AWS Direct Connectest un service qui établit une connexion réseau dédiée entre vos locaux etAWS. Consultez AWS Direct Connect pour plus de détails.

Il existe deux types de AWS Direct Connect connexions : dédiées et hébergées. Une connexion dédiée est un lien direct entre un AWS appareil et votre appareil sur site, tandis qu'une connexion hébergée est prise en charge par un AWS partenaire qui peut gérer les détails de connexion pour vous. Consultez la section AWS Direct ConnectConnexions pour plus d'informations.

Une connexion Direct Connect utilise des interfaces virtuelles (VIF) pour isoler les différents flux de trafic. Plusieurs VIF peuvent utiliser le même lien Direct Connect, séparé par des balises VLAN (802.1q). Il existe trois types de VIF qui fournissent une connectivité au AWS réseau. Voir interfaces AWS Direct Connect virtuelles pour plus de détails. Les trois types sont les suivants :

- VIF privé : un VIF privé est une connexion privée entre votre appareil et les ressources qu'il contientAWS. Elles se terminent à l'intérieur soit directement AWS sur une passerelle privée

virtuelle (VGW) (qui prend en charge un seul VPC), soit via une passerelle Direct Connect qui se connecte ensuite à plusieurs VGW.

- VIF public : un VIF public permet la connectivité à toutes les AWS ressources publiques, telles que S3, DynamoDB et les plages d'adresses IP EC2 publiques. Bien qu'un VIF public ne dispose pas d'un accès direct à Internet, n'importe quelle ressource publique Amazon peut y accéder (y compris les instances EC2 publiques d'autres clients), ce que les clients doivent prendre en compte lors de la planification de la sécurité.
- VIF de transit : un VIF de transit est une connexion privée entre votre appareil et une AWS Transit Gateway passerelle Direct Connect. Les VIF de transit sont désormais pris en charge sur les liaisons dont les vitesses sont inférieures à 1 Gbit/s. Consultez l'annonce de lancement pour plus de détails.

> **Note**
>
> L'interface virtuelle hébergée (VIF hébergée) est un type de VIF privé dans lequel le VIF est attribué à une personne différente de Compte AWS celle Compte AWS qui possède la AWS Direct Connect connexion (qui peut inclure un AWS Direct Connect partenaire). AWSne permet plus à de nouveaux partenaires de proposer ce modèle. Vous pouvez vous connecter à une interface virtuelle hébergée pour plus d'informations.

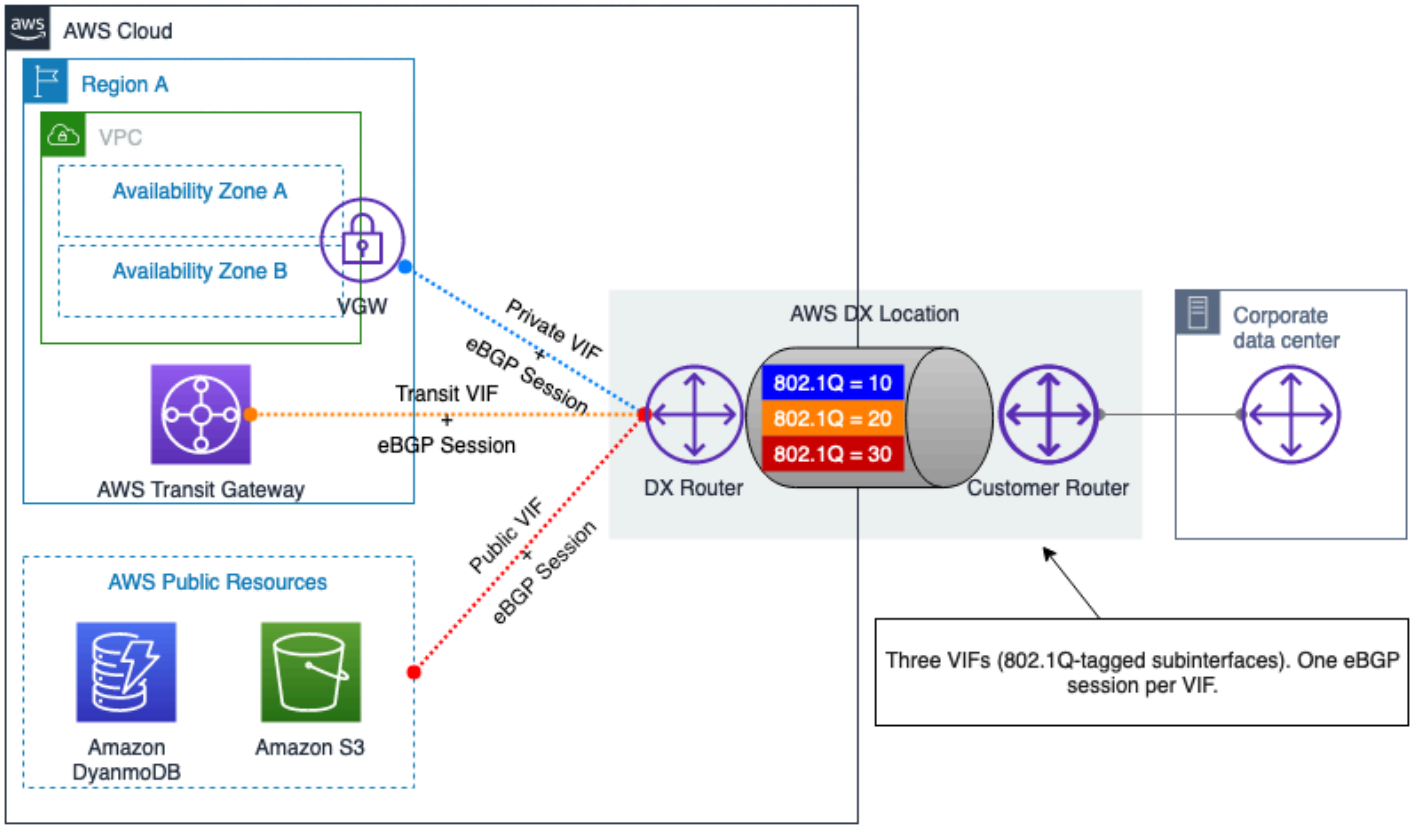

Figure 1 — AWS Direct Connect VIF privés et publics

Réseau privé virtuel (VPN) site à site

Un site-to-site VPN permet à deux réseaux de communiquer en toute sécurité et peut être utilisé sur un moyen de transport non fiable, tel qu'Internet. Les clients peuvent établir des connexions VPN entre des sites sur site et Amazon Virtual Private Clouds (Amazon VPC) via deux options :

- AWSVPN géré de site à site (VPN AWS S2S) : il s'agit d'un service VPN entièrement géré et hautement disponible, utilisant IPsec. Voir Qu'est-ce que c'est AWS Site-to-Site VPN pour plus d'informations. Vous pouvez activer l'accélération pour votre connexion Site-to-Site VPN. Vous pouvez vous connecter à une connexion VPN de site à site de façon accélérée pour plus d'informations. Le VPN S2S peut également utiliser les VIF de transit Direct Connect pour éviter que le trafic ne transite par Internet, ce qui réduit les coûts et permet l'utilisation d'adresses IP privées. Pour plus de détails, consultez la section VPN IP privé avec AWS Direct Connect.
- VPN de site à site logiciel (VPN géré par le client) : avec cette option de connectivité VPN, vous êtes responsable du provisionnement et de la gestion de l'ensemble de la solution VPN,

généralement en exécutant le logiciel VPN sur une instance EC2. Pour plus d'informations, consultez Software Site-to-Site VPN.

Les deux options nécessitent une assistance sur le dispositif de passerelle client pour mettre fin à l'extrémité locale des tunnels VPN. Vous pouvez vous connecter à une instance physique ou à une appliance logicielle. Pour plus d'informations sur les périphériques réseau testés parAWS, reportez-vous à la liste des périphériques de passerelle client testés.

Transit Gateway Connect (TGW Connect)

Transit Gateway Connect utilise des tunnels GRE entre un périphérique de passerelle AWS Transit Gateway et un périphérique de passerelle sur site. Le protocole BGP est utilisé en plus de TGW Connect pour activer le routage dynamique. Notez que TGW Connect n'est pas crypté. Vous pouvez vous connecter à Transit Gateway Connect pour plus d'informations.

AWSservices de connectivité hybrides

AWSles services de connectivité hybrides fournissent des composants réseau hautement évolutifs et hautement disponibles. Ils jouent un rôle essentiel dans la création de solutions réseau hybrides. Au moment de la rédaction de ce livre blanc, il existait trois principaux points de terminaison de service :

- AWSLa passerelle privée virtuelle (VGW) est un service régional hautement redondant qui fournit le routage et le transfert IP au niveau du VPC, faisant office de passerelle permettant au VPC de communiquer avec les dispositifs de passerelle de vos clients. VGW peut mettre fin aux connexions VPN AWS S2S et aux VIF privées. AWS Direct Connect
- AWS Transit Gateway(TGW) est un service régional, hautement disponible et évolutif qui vous permet de connecter plusieurs VPC entre eux, ainsi qu'à vos réseaux locaux via un VPN Site-to-Site et/ou Direct Connect à l'aide d'une seule passerelle centralisée. Conceptuellement, un AWS Transit Gateway agit comme un routeur cloud virtuel hautement disponible et redondant. AWS Transit Gatewayprend en charge le routage ECMP (Equal Cost Multipath) sur plusieurs connexions Direct Connect, tunnels VPN ou homologues TGW Connect. Les passerelles de transit peuvent être reliées entre elles, à la fois dans la même région et entre régions, ce qui permet à leurs ressources connectées de communiquer via les liaisons d'appairage. Vous pouvez vous connecter à une section sur les AWS Transit Gatewayscénarios.
- AWS CloudLe WAN fournit un tableau de bord central pour établir des connexions entre vos succursales, vos centres de données et les VPC Amazon, afin de créer un réseau mondial en quelques clics seulement. Vous utilisez des politiques réseau pour automatiser les tâches de

gestion et de sécurité du réseau en un seul endroit. Vous pouvez vous connecter à une connexion AWS CloudWAN de différentes façons.

- Direct Connect Gateway (DXGW) est un service disponible dans le monde entier qui distribue les informations de routage sur ses connexions, en se comportant de la même manière que les réflecteurs de route BGP d'un réseau traditionnel. Les données ne transitent pas par un DXGW, il ne gère que les informations de routage. Vous pouvez créer un DXGW dans n'importe quel endroit Région AWS et y accéder depuis tous les autres. Régions AWS Vous pouvez connecter des VIF Direct Connect à un DXGW, puis associer le DXGW à des VGW (en utilisant des VIF privés) ou à un (en utilisant des VIF de transit). AWS Transit Gateway Voir Passerelles Direct Connect pour plus d'informations. Il n'est pas nécessaire de créer plusieurs DXGW à des fins de redondance, car il s'agit d'un service disponible à l'échelle mondiale. Cependant, vous pouvez choisir d'utiliser plusieurs DXGW pour séparer les domaines de routage, par exemple un réseau de production et un réseau de test que vous souhaitez garder complètement isolés.

Considérations relatives au type de connectivité hybride et à la conception

Cette section du livre blanc couvre les considérations qui influent sur vos choix lors de la sélection d'un réseau hybride auquel connecter vos environnements sur site. AWS Il suit un processus de réflexion logique pour vous aider à sélectionner une solution de connectivité hybride optimale. Les considérations affectant votre conception sont classées en considérations qui ont un impact sur votre type de connectivité et en considérations qui affectent votre conception de connectivité. Les considérations relatives au type de connectivité vous aideront à choisir entre un VPN basé sur Internet ou Direct Connect. Les considérations relatives à la conception de la connectivité vous aideront à décider comment configurer les connexions.

Les considérations suivantes qui ont un impact sur votre type de connectivité sont abordées : délai de déploiement, sécurité, SLA, performances et coût. Après avoir examiné ces considérations et leur incidence sur vos choix de conception, vous serez en mesure de décider si l'utilisation d'une connexion Internet ou de Direct Connect est recommandée pour répondre à vos besoins.

Les considérations suivantes qui ont une incidence sur la conception de votre connectivité sont abordées : évolutivité, modèle de communication, fiabilité et intégration du SD-WAN tiers. Après avoir examiné ces considérations et leur incidence sur vos choix de conception, vous serez en mesure de décider de la conception logique optimale recommandée pour répondre à vos exigences.

La structure suivante est utilisée pour discuter et analyser chacune des considérations relatives à la sélection et à la conception :

- Définition - Brève définition de ce qu'est la considération.
- Questions clés - Fournit un ensemble de questions pour vous permettre de recueillir les exigences associées à la prise en compte.
- Capacités à prendre en compte - Solutions pour répondre aux exigences associées à la prise en compte.
- Arbre de décision - Pour certaines considérations ou un groupe de considérations, un arbre de décision est fourni pour vous aider à sélectionner la solution de réseau hybride optimale.

Les considérations affectant la conception de votre réseau hybride sont traitées dans un ordre où le résultat d'une considération fait partie de l'entrée pour la prise en compte suivante. Comme l'illustre la

figure 2, la première étape consiste à choisir le type de connectivité, puis à l'affiner en tenant compte des considérations relatives à la sélection du design.

La figure 2 montre les deux catégories de considérations, les considérations individuelles et l'ordre logique dans lequel les considérations sont abordées dans les sous-sections suivantes. Telles sont les considérations essentielles à prendre en compte lors de la prise de décision de conception d'un réseau hybride. Si la conception ciblée ne nécessite pas toutes ces considérations, vous pouvez vous concentrer sur les considérations qui s'appliquent à vos besoins.

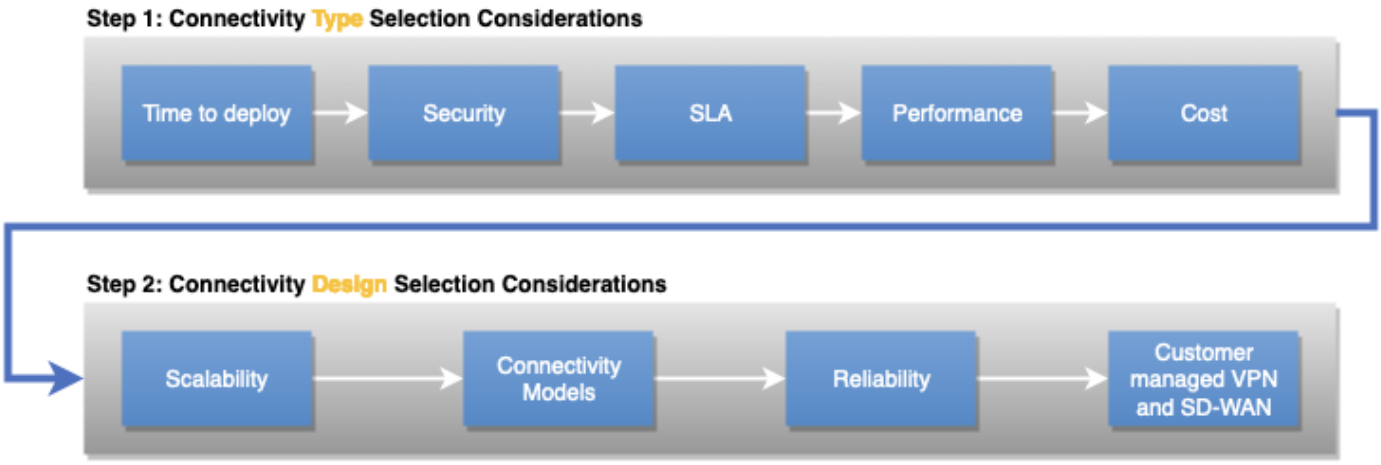

Figure 2 — Catégories de considérations, considérations individuelles et ordre logique entre elles

Sélection du type de connectivité

Cette section couvre les considérations qui affectent le type de connectivité que vous sélectionnez pour votre charge de travail. Cela inclut le délai de déploiement, la sécurité, le SLA, les performances et les coûts.

Considérations

- Il est temps de déployer
- Sécurité
- Contrat de niveau de service (SLA)
- Performances
- Coût

Il est temps de déployer

Définition

Le temps de déploiement peut être un facteur important dans le choix d'un type de connectivité adapté à une charge de travail. Selon le type de connectivité et les emplacements sur site, la connectivité peut être établie en quelques heures, mais cela peut prendre des semaines, voire des mois, si des circuits supplémentaires doivent être installés. Cela influencera votre décision d'utiliser une connexion Internet, une connexion dédiée privée ou une connexion hébergée privée fournie en tant que service géré par un AWS Direct Connect partenaire.

Questions clés

- Quel est le calendrier requis pour le déploiement : heures, jours, semaines ou mois ?
- Pendant combien de temps la connexion sera-t-elle nécessaire ? S'agira-t-il d'un projet éphémère ou d'une infrastructure permanente ?

Capacités à prendre en compte

Lorsque vous avez besoin d'une AWS connectivité en quelques heures ou quelques jours, vous devrez probablement utiliser une connexion réseau existante. Cela implique souvent d'établir une connexion VPN AWS via l'Internet public. Si un partenaire AWS DX existant vous fournit une AWS connectivité privée, une nouvelle connexion hébergée peut être mise en place en quelques heures.

Lorsque vous avez des jours, voire des semaines, vous pouvez travailler avec un AWS Direct Connect partenaire pour établir une connectivité privée avecAWS. AWS Direct Connect Les partenaires vous aident à établir une connectivité réseau entre les AWS Direct Connect sites et votre environnement de centre de données, de bureau ou de colocation. Certains AWS Direct Connectpartenaires sont autorisés à proposer des connexions hébergées Direct Connect. Les connexions hébergées peuvent souvent être mises en service plus rapidement que les connexions dédiées. AWS Direct Connect Le partenaire fournira chaque connexion hébergée en utilisant son infrastructure existante connectée au AWS backbone.

Lorsque vous disposez de plusieurs semaines, voire de plusieurs mois, vous pouvez envisager d'établir une connexion privée dédiée avecAWS. Les fournisseurs de services et AWS Direct Connect les partenaires facilitent les connexions AWS Direct Connect dédiées. Il est courant que les fournisseurs de services installent des équipements réseau dans les locaux du client afin de faciliter

une connexion dédiée Direct Connect. En fonction du fournisseur de services, de l'emplacement de votre site et d'autres facteurs physiques, l'installation d'une connexion dédiée Direct Connect peut prendre de plusieurs semaines à quelques mois.

Si votre équipement réseau est déjà installé dans la même installation de colocation où le site existe, vous pouvez rapidement établir une connexion AWS Direct Connect dédiée via une interconnexion sur le AWS Direct Connect site de colocation. Une fois que vous avez demandé la connexion, AWS vous avez mis à votre disposition une lettre d'autorisation et d'affectation des installations de connexion (LOA-CFA) à télécharger, ou vous avez envoyé un e-mail pour vous demander plus d'informations. Le LOA-CFA est l'autorisation de connexion àAWS, et est exigé par votre fournisseur de réseau pour commander une connexion croisée pour vous.

Tableau 1 — Comparaison du rapport coût-efficacité

	Connectivité basée sur Internet	Connexion dédiée DX (équipement existant sur le site DX)	Connexion dédiée DX (net-new)	Connexion hébergée DX (port existant avec DX Partner)	Connexion hébergée DX (net-new)
Délai d'approvisionnement	Des heures à des jours	Jours	Plusieurs semaines, voire plusieurs mois	Des heures à des jours	Plusieurs jours, semaines, voire mois

> **Note**
>
> Les directives relatives aux délais de mise à disposition fournies sont basées sur des observations du monde réel et ne servent qu'à titre d'illustration. Si l'on tient compte de l'emplacement de votre site, de la proximité des sites de connexion directe et de l'infrastructure préexistante, tout cela aura un impact sur le temps de provisionnement. Votre AWS Direct Connect partenaire vous indiquera le délai d'approvisionnement précis.

Sécurité

Définition

Les exigences de sécurité influenceront votre type de connectivité hybride. Ces considérations incluent :

- Type de transport : connexion Internet ou réseau privé
- Exigences en matière de chiffrement

Questions clés

- Vos exigences et politiques de sécurité autorisent-elles l'utilisation de connexions chiffrées sur Internet pour vous connecterAWS, ou imposent-elles l'utilisation de connexions réseau privées ?
- Lorsque vous utilisez des connexions réseau privées, la couche réseau doit-elle fournir un chiffrement en transit ?

Solutions techniques

Vos exigences et politiques de sécurité peuvent autoriser l'utilisation d'Internet ou exiger l'utilisation d'une connexion réseau privée entre le réseau de votre entreprise AWS et le réseau de votre entreprise. Ils influent également sur la décision de savoir si le réseau doit fournir un chiffrement en transit ou si le chiffrement au niveau de la couche application est acceptable.

Si vous pouvez tirer parti d'Internet, vous AWS Site-to-Site VPN pouvez l'utiliser pour créer des tunnels cryptés entre votre réseau et vos Amazon VPC ou AWS Transit Gateway vos Amazon sur Internet. L'extension de votre solution SD-WAN à Internet est également une option si vous utilisez une connexion Internet. AWS La section VPN et SD-WAN gérés par le client plus loin dans ce livre blanc couvre les considérations spécifiques relatives au SD-WAN.

Si vous avez besoin d'une connexion réseau privée entre le réseau AWS de votre entreprise, il est AWS recommandé d'utiliser des connexions AWS Direct Connect dédiées ou des connexions hébergées. Si le chiffrement en transit est requis sur une connexion réseau privée, vous devez établir un VPN via Direct Connect (via un VIF public ou un VIF de transit), ou envisager d'utiliser MacSec sur une connexion dédiée 10 Gbit/s ou 100 Gbit/s.

Tableau 2 — Exemple d'exigences relatives au type de connectivité d'Automotive Corp

	Site-to-Site VPN	Direct Connect
Transport	Internet	Connexion réseau privée
Chiffrement en transit	Oui	Nécessite un VPN S2S sur DX, un VPN S2S sur un VIF de transit ou MacSec sur une connexion dédiée de 10 Gbit/s ou 100 Gbit/s

Contrat de niveau de service (SLA)

Définition

Les entreprises ont souvent besoin d'un fournisseur de services pour respecter un SLA pour chaque service consommé par l'organisation. L'organisation développe à son tour ses propres services sur le dessus et peut proposer un SLA à ses propres consommateurs. Le SLA est important car il décrit la manière dont le service est fourni et géré, et il inclut souvent des caractéristiques mesurables spécifiques, telles que la disponibilité. Si le service enfreint le SLA défini, un fournisseur de services propose généralement une compensation financière spécifiée dans le contrat. Un SLA définit le type de mesure, l'exigence et la période de mesure. À titre d'exemple, reportez-vous à la définition de l'objectif de disponibilité dans le cadre du AWS Direct ConnectSLA.

Questions clés

- Un SLA de connexion à connectivité hybride assorti de crédits de service est-il requis ?
- L'ensemble du réseau hybride doit-il respecter un objectif de disponibilité ?

Capacités à prendre en compte

Type de connectivité : La connectivité Internet peut être imprévisible. Tout en AWS faisant très attention à la mise en place de multiples liens avec un ensemble diversifié de fournisseurs de services Internet, l'administration d'Internet se situe simplement en dehors du AWS domaine administratif d'un seul fournisseur. L'ingénierie des itinéraires et l'influence du trafic qu'un fournisseur de cloud peut exercer une fois que le trafic a quitté la frontière de son réseau sont limitées. Cela dit, il existe un AWS Site-to-Site VPNSLA qui fournit des objectifs de disponibilité pour les AWS Site-to-Site VPN terminaux.

AWSDirect Connect propose un accord de niveau de service officiel avec des crédits de service calculés en pourcentage du total des frais d'heure de AWS Direct Connect port que vous avez payés pour les connexions applicables en cas d'indisponibilité pendant le cycle de facturation mensuel au cours duquel le SLA n'a pas été respecté. Il s'agit du transport recommandé si un SLA est requis. AWS Direct Connectrépertorie les exigences de configuration minimales spécifiques pour chaque objectif de disponibilité, telles que le nombre d'AWS Direct Connectemplacements, de connexions et d'autres détails de configuration. Le non-respect des exigences signifie que les crédits de service ne peuvent pas être offerts en cas de rupture des SLA définis par le service.

Il est important de noter que même si le service sélectionné pour fournir une connectivité hybride est configuré pour répondre aux exigences du SLA, le reste du réseau peut ne pas fournir le même niveau de SLA. La AWS responsabilité s'arrête sur le AWS Direct Connect site du AWS Direct Connect port. Une AWS fois que le trafic est transféré au réseau de votre entreprise, il n'est plus de la responsabilité deAWS. Si vous utilisez un fournisseur de services entre AWS et votre réseau local, la connectivité est soumise au SLA entre vous et le fournisseur de services, le cas échéant. N'oubliez pas que l'ensemble du réseau hybride est aussi performant que sa partie la plus faible lorsque vous concevez une connectivité hybride.

AWS Direct Connectles partenaires offrent de AWS Direct Connect la connectivité. Le partenaire peut proposer un SLA avec des crédits de service basés sur son offre de produits jusqu'au point de démarcation avec. AWS L'option doit être évaluée et étudiée plus avant directement avec les partenaires APN. AWSpublie une liste de partenaires de livraison validés.

Conception logique : outre le type de connectivité, vous devez également prendre en compte d'autres éléments de base dans le cadre de votre conception globale. Par exemple, AWS Transit Gatewaypossède son propre SLA, tout comme le VPN AWSS2S. AWS Transit GatewayPour des raisons de sécurité, vous utilisez peut-être le VPN AWS S2S pour des raisons de sécurité, mais vous devez concevoir les deux de manière cohérente avec chaque SLA pour être éligible à des crédits de service pour chaque service concerné.

Passez en revue les recommandations AWS Direct Connect en matière de résilience et la boîte à outils de résilience.

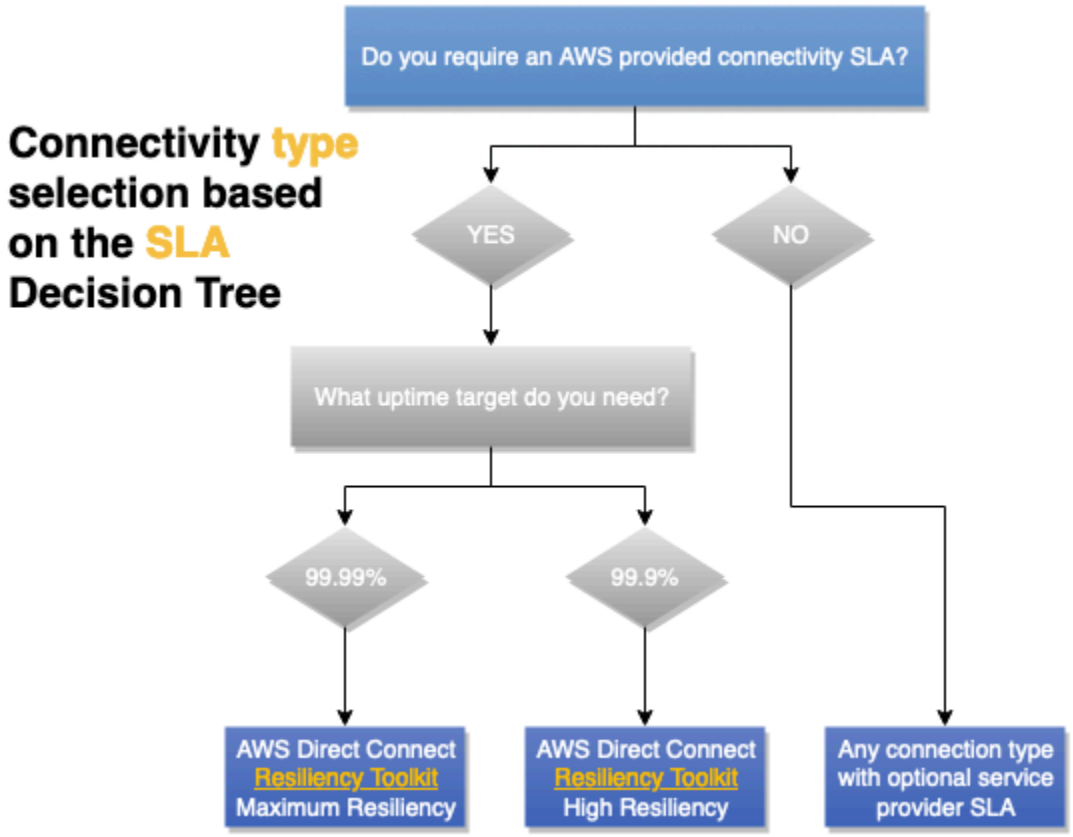

Figure 3 — Arbre décisionnel relatif à la prise en compte des accords de niveau de service

Performances

Définition

De nombreux facteurs influencent les performances du réseau, tels que la latence, la perte de paquets, l'instabilité et la bande passante. En fonction des exigences de l'application, l'importance de chacun de ces facteurs peut varier.

Questions clés

En fonction des exigences de votre application, vous devez identifier et hiérarchiser les facteurs de performance réseau qui ont un impact sur le comportement de votre application et sur l'expérience utilisateur.

Bande passante

La bande passante fait référence au taux de transfert de données d'une connexion et est généralement mesurée en bits par seconde (bps). Les mégabits par seconde (Mbits/s) et les gigabits

par seconde (Gbit/s) sont courants et correspondent à la base 10 (1 000 000 bits par seconde = 1 Mbits/s), par opposition à la base 2 (2^10) observée ailleurs.

Lorsque vous évaluez les besoins en bande passante des applications, gardez à l'esprit que les besoins en bande passante peuvent changer au fil du temps. Le déploiement initial dans le cloud, les opérations normales, les nouvelles charges de travail et les scénarios de basculement peuvent tous avoir des exigences de bande passante différentes.

Les applications peuvent avoir leurs propres considérations relatives à la bande passante. Certaines applications peuvent nécessiter des performances déterministes sur une connexion à bande passante élevée, tandis que d'autres peuvent nécessiter à la fois des performances déterministes et une bande passante élevée. Une application peut avoir besoin d'une configuration spéciale pour utiliser plusieurs flux de trafic (parfois appelés flux ou sockets) en parallèle si elle atteint les limites de bande passante par flux de trafic, ce qui lui permet d'utiliser une plus grande partie de la bande passante de la connexion. Les VPN peuvent limiter le débit en raison des surcharges liées au tunneling, des limites de MTU inférieures ou des limites de bande passante matérielle.

Latence

La latence est le temps nécessaire pour qu'un paquet passe de la source à la destination via une connexion réseau. Elle est généralement mesurée en millisecondes (ms), les exigences de faible latence étant parfois exprimées en microsecondes (µs). La latence est fonction de la vitesse de la lumière, elle augmente donc avec la distance.

Les exigences de latence des applications peuvent prendre différentes formes. Une application hautement interactive, telle qu'un bureau virtuel, peut avoir une cible de latence mesurée entre le moment où l'utilisateur effectue une saisie et celui où il voit le bureau virtuel réagir à cette entrée. Les applications de voix sur IP (VoIP) peuvent avoir des exigences similaires. Un deuxième type de charge de travail à prendre en compte est celui qui est hautement transactionnel et qui nécessite une réponse du serveur avant de pouvoir continuer. Les bases de données ou d'autres formes de stockages de clés/valeurs peuvent être fortement impactées par l'augmentation de la latence du réseau.

Jitter (Instabilité)

La gigue mesure la constance de la latence du réseau et, comme la latence, elle est généralement mesurée en millisecondes (ms).

Les exigences liées à l'instabilité des applications se retrouvent généralement dans les applications de streaming en temps réel, y compris la diffusion vidéo et vocale. Ces applications ont tendance

à exiger que leur flux de données soit à un débit et à un délai constants, avec de petites zones tampons pour corriger les petites instabilités.

Perte de paquets

La perte de paquets est la mesure du pourcentage de trafic réseau qui n'est pas délivré. Tous les réseaux présentent parfois un certain degré de perte de paquets en raison de fortes rafales de trafic, de réductions de capacité, de pannes d'équipement réseau, etc. Ainsi, les applications doivent avoir une certaine tolérance à l'égard de la perte de paquets, mais leur tolérance peut varier d'une application à l'autre.

Les applications qui utilisent le protocole TCP pour transporter leur trafic ont la capacité de corriger la perte de paquets par retransmission. Les applications qui utilisent le protocole UDP ou leurs propres protocoles en plus de l'IP doivent mettre en œuvre leurs propres moyens de gestion des pertes de paquets, et peuvent y être très sensibles. Une application de voix sur IP peut simplement insérer du silence dans la partie de l'appel où le paquet a été perdu, au lieu de tenter une retransmission. Certaines solutions VPN incluent leurs propres mécanismes de restauration en cas de perte de paquets sur le réseau qu'elles utilisent pour transporter le trafic.

Capacités à prendre en compte

Lorsqu'une latence et un débit prévisibles sont nécessaires, AWS Direct Connect c'est le choix recommandé, car il fournit des performances déterministes. La bande passante peut être sélectionnée en fonction des exigences de débit. AWSrecommande de l'utiliser AWS Direct Connect lorsque vous avez besoin d'une expérience réseau plus cohérente que celle que peuvent fournir les connexions Internet. Les VIF privés et les VIF de transit prennent en charge les trames jumbo, ce qui peut réduire le nombre de paquets sur le réseau et améliorer le débit grâce à une réduction des frais généraux. AWS Direct Connect SiteLinkpermet d'utiliser le AWS backbone pour assurer la connectivité entre vos sites et peut être activé à la demande. La bande passante utilisée SiteLink doit être prise en compte lors de la sélection de la bande passante Direct Connect.

L'utilisation d'un VPN AWS Direct Connect ajoute du chiffrement. Cependant, cela réduit la taille de la MTU, ce qui peut réduire le débit. AWSles fonctionnalités VPN gérées de site à site (S2S) sont disponibles dans la documentation. AWS Site-to-Site VPN De nombreux emplacements de connexion directe prennent en charge MacSec si le chiffrement de votre connexion est la principale exigence de chiffrement. MacSec ne présente pas les mêmes considérations relatives à la MTU ou au débit potentiel que les connexions VPN de site à site. AWS Transit Gatewaypermet aux clients d'augmenter horizontalement le nombre de connexions VPN et d'augmenter le débit en conséquence

grâce au routage multichemin à coût égal (ECMP). AWSle VPN Site-to-site géré prend en charge l'utilisation des VIF de transit Direct Connect pour une connectivité privée. Consultez le VPN IP privé pour plus de détails. AWS Direct Connect

Une autre option consiste à utiliser un VPN Site-to-Site AWS géré sur Internet. Il peut être une option intéressante en raison de son faible coût et est largement disponible. Cependant, gardez à l'esprit que les performances sur Internet constituent le meilleur effort. Les événements météorologiques sur Internet, la congestion et les périodes de latence accrues peuvent être imprévisibles. AWSpropose une solution avec le VPN S2S AWS accéléré, qui peut atténuer certains des inconvénients liés à l'utilisation d'un chemin Internet. Le VPN S2S accéléré utilise AWS Global Accelerator, qui permet au trafic VPN d'entrer dans le AWS réseau le plus tôt possible et le plus près possible du dispositif de passerelle client. Cela optimise le chemin d'accès réseau en utilisant le réseau AWS mondial sans congestion pour acheminer le trafic vers le point de terminaison offrant les meilleures performances. Vous pouvez utiliser des connexions VPN accélérées pour éviter les perturbations réseau susceptibles de se produire lorsque le trafic est acheminé via Internet public.

Coût

Définition

Dans le cloud, le coût de la connectivité hybride inclut le coût des ressources provisionnées et de leur utilisation. Le coût des ressources allouées est mesuré en unités de temps, généralement toutes les heures. L'utilisation concerne le transfert et le traitement de données généralement mesurés en gigaoctets (Go). Les autres coûts incluent le coût de la connectivité au point de présence du AWS réseau. Si votre réseau se trouve au sein de la même installation de colocation, le coût d'une connexion croisée peut être aussi faible que le coût d'une connexion croisée. Si votre réseau se trouve à un autre endroit, cela impliquera des frais pour un fournisseur de services ou un partenaire APN Direct Connect.

Questions clés

- Quelle quantité de données prévoyez-vous d'envoyer AWS par mois depuis votre établissement et depuis Internet ?
- Quelle quantité de données prévoyez-vous d'envoyer AWS par mois à vos installations et à Internet ?
- À quelle fréquence ces montants changeront-ils ?
- Quels sont les changements dans un scénario de défaillance ?

Capacités à prendre en compte

Si vous souhaitez exécuter des charges de travail gourmandes en bande passanteAWS, vous AWS Direct Connect pouvez réduire les coûts de votre réseau de AWS deux manières. Tout d'abord, en transférant des données AWS directement depuis et vers, vous pouvez réduire les coûts de bande passante que vous payez à votre fournisseur de services Internet. Ensuite, toutes les données transférées via votre connexion dédiée sont facturées au taux de transfert de AWS Direct Connect données réduit, plutôt qu'au tarif de transfert de données Internet. Consultez la page de tarification de Direct Connect pour plus de détails.

AWS Direct Connectpermet d'interconnecter vos sites AWS Direct Connect SiteLink à l'aide du AWS backbone. Consultez le blog de SiteLink lancement pour plus d'informations. L'exploitation de cette fonctionnalité entraîne des coûts de transfert de données Direct Connect normaux, et une facturation par heure SiteLink est activée. Vous pouvez activer et désactiver SiteLink à la demande, et cela peut être une bonne option pour les scénarios de défaillance impliquant Internet ou une connectivité à un réseau privé.

Si vous faites appel à un fournisseur de services réseau pour la connectivité entre un site sur site et un site Direct Connect, votre capacité et le temps nécessaire pour modifier vos engagements en matière de bande passante dépendent de votre contrat avec le fournisseur de services.

Le AWS backbone peut acheminer votre trafic vers n'importe quel point de présence du AWS réseau, Région AWS sauf en Chine. Cette fonctionnalité présente de nombreux avantages techniques par rapport à l'utilisation d'Internet pour accéder à distanceRégions AWS, mais elle a un coût. Consultez la page de tarification du transfert de données EC2 pour plus de détails. S'il y en a un AWS Transit Gatewaydans le trajet du trafic, cela augmente le coût de traitement des données par Go. Toutefois, si vous utilisez le peering interrégional entre deux passerelles de transit, le traitement des données de transit ne vous sera facturé qu'une seule fois.

La conception optimale des applications permet de limiter le traitement des données AWS et de minimiser les frais de sortie de données inutiles. L'entrée de données AWS est gratuite.

> **Note**
>
> Dans le cadre de la solution de connectivité globale, outre le coût de la AWS connexion, vous devez également prendre en compte le coût de la end-to-end connectivité, y compris le coût du fournisseur de services, les connexions croisées, les racks et l'équipement sur un site DX (si nécessaire).

Si vous ne savez pas si vous devez utiliser Internet ou une connexion privée, calculez un seuil de rentabilité où AWS Direct Connect cela devient moins coûteux que l'utilisation d'Internet. Si le volume de données signifie que cela AWS Direct Connect coûte moins cher et que vous avez besoin d'une connectivité permanente, AWS Direct Connect c'est le meilleur choix de connectivité.

Si la connectivité est temporaire et qu'Internet répond à d'autres exigences, il peut être moins coûteux d'utiliser le VPN AWS S2S sur Internet en raison de l'élasticité d'Internet. Notez que cela nécessite que vous disposiez d'une connectivité Internet suffisante depuis votre réseau local.

Si vous vous trouvez dans un établissement qui en dispose AWS Direct Connect (la liste est disponible sur le site Web de Direct Connect), vous pouvez établir une connexion croisée avec. AWS Cela signifie utiliser des connexions dédiées à 1,10 ou 100 Gbit/s. AWS Direct Connectles partenaires proposent davantage d'options de bande passante et des capacités plus petites, ce qui peut optimiser vos coûts de connectivité. Par exemple, vous pouvez commencer par une connexion hébergée de 50 Mbits/s par rapport à une connexion dédiée de 1 Gbit/s.

AvecAWS Transit Gateway, vous pouvez partager vos connexions VPN et Direct Connect avec de nombreux VPC. Bien que vous soyez facturé en fonction du nombre de connexions que vous établissez AWS Transit Gateway par heure et de la quantité de trafic qui y circuleAWS Transit Gateway, cela simplifie la gestion et réduit le nombre de connexions VPN et de VIF nécessaires. Les avantages et les économies de coûts liés à la réduction des frais d'exploitation peuvent facilement compenser les coûts supplémentaires liés au traitement des données. Vous pouvez éventuellement envisager une conception où se AWS Transit Gateway trouve le chemin du trafic vers la plupart des VPC, mais pas vers tous. Cette approche permet d'éviter les frais de traitement des AWS Transit Gateway données pour les cas d'utilisation dans lesquels vous devez transférer de grandes quantités de donnéesAWS. Reportez-vous à la section Modèles de connectivité pour plus de détails sur cette conception. Une autre approche consiste à AWS Direct Connect le combiner comme chemin principal avec le VPN AWS S2S sur Internet comme chemin de sauvegarde/basculement. Bien que techniquement faisable et très rentable, cette solution présente des inconvénients techniques (décrits dans la section Fiabilité de ce livre blanc) et peut être plus difficile à gérer. AWSne le recommande pas pour les charges de travail très critiques ou critiques.

L'approche finale est un VPN ou un SD-WAN géré par le client et déployé dans une ou plusieurs instances Amazon EC2. Cela peut être moins cher à grande échelle s'il y a des dizaines, voire des centaines de sites, par rapport au VPN AWS S2S. Cependant, il faut tenir compte des frais de gestion, des coûts de licence et du coût des ressources EC2 pour chaque appliance virtuelle.

Matrice de décision

Tableau 3 — Example Corp. Entrées de conception de connectivité automobile

Catégorie	VPN ou SD-WAN géré par le client	AWSVPN S2S	AWSVPN S2S accéléré	AWS Direct ConnectConnexion hébergée	AWS Direct ConnectConnexion dédiée
Nécessite une connexion Internet	Oui	Oui	Oui	Non	Non
Coût des ressources provisionnées	Octroi de licences pour les instances et les logiciels EC2	AWSVPN S2S	AWSVPN S2S et accélérateur mondial AWS	Tranche de capacité applicable du coût du port	Coût d'un port dédié
Coût de transfert de données	Tarif Internet	Tarif Internet ou tarif Direct Connect	Internet avec transfert de données premium	Tarif Direct Connect	Tarif Direct Connect
Passerelle de transit	Facultatif	Facultatif	Obligatoire	Facultatif	Facultatif
AWSCoûts de traitement des données	N/A	Uniquement avec AWS Transit Gateway	Oui	Uniquement avec AWS Transit Gateway	Uniquement avec AWS Transit Gateway
Peut être réutilisé AWS Direct Connect ?	Oui	Oui	Non	N/A	N/A

Sélection du design de connectivité

Cette section du livre blanc couvre les considérations qui influent sur le choix de votre conception de connectivité. La conception de la connectivité inclut les aspects logiques ainsi que la manière de concevoir et d'optimiser la fiabilité de votre connectivité hybride.

Les considérations suivantes seront abordées : évolutivité, modèles de connectivité, fiabilité, VPN et SD-WAN gérés par le client.

Considérations

- Evolutivité
- Modèles de connectivité
- Fiabilité
- VPN et SD-WAN gérés par le client

Evolutivité

Définition

L'évolutivité fait référence à la capacité de votre solution de connectivité à croître et à évoluer au fil du temps en fonction de l'évolution de vos besoins.

Lorsque vous concevez une solution, vous devez tenir compte de la taille actuelle ainsi que de la croissance prévue. Cette croissance peut être une croissance organique ou être liée à une expansion rapide, comme dans les scénarios de fusion et d'acquisition.

Remarque : en fonction de l'architecture de solution ciblée, il est possible que tous les éléments précédents ne soient pas nécessairement pris en compte. Cependant, ils peuvent servir d'éléments de base pour identifier les exigences d'évolutivité des solutions de réseau hybrides les plus courantes. Ce livre blanc se concentre sur la sélection et la conception de la connectivité hybride. Il est recommandé de prendre également en compte l'échelle de la connectivité hybride par rapport à l'architecture réseau VPC. Pour plus d'informations, consultez le livre blanc sur la création d'une infrastructure AWS réseau multi-VPC évolutive et sécurisée.

Questions clés

- Quel est le nombre actuel et prévu de VPC nécessitant une connectivité à un ou plusieurs sites sur site ?

- Les VPC sont-ils déployés dans une Région AWS ou plusieurs régions ?
- À combien de sites locaux doit-on se connecter ? AWS
- Combien de dispositifs de passerelle client (généralement des routeurs ou des pare-feux) possédez-vous par site auxquels vous devez vous connecter ? AWS
- Combien de routes devraient être annoncées sur les Amazon VPC et quel est le nombre d'itinéraires attendus depuis le site ? AWS
- Est-il nécessaire d'augmenter la bande passante au AWS fil du temps ?

Capacités à prendre en compte

L'échelle est un facteur important dans la conception de la connectivité hybride. À ce stade, la section suivante intégrera l'échelle dans le cadre de la conception du modèle de connectivité ciblé.

Les meilleures pratiques recommandées pour minimiser la complexité d'échelle de la conception de la connectivité réseau hybride sont les suivantes :

- Le résumé des itinéraires doit être utilisé pour réduire le nombre d'itinéraires annoncés et reçus de. AWS Ainsi, le schéma d'adressage IP doit être conçu pour maximiser l'utilisation de la synthèse des routes. L'ingénierie du trafic est une considération globale essentielle. Pour plus d'informations sur l'ingénierie du trafic, reportez-vous à la sous-section Ingénierie du trafic dans la section Fiabilité.
- Réduisez le nombre de sessions de peering BGP en utilisant DXGW avec VGW ou AWS Transit Gateway, lorsqu'une seule session BGP peut fournir une connectivité à plusieurs VPC.
- Envisagez le Cloud WAN lorsque plusieurs Régions AWS sites locaux doivent être connectés ensemble.

Modèles de connectivité

Définition

Le modèle de connectivité fait référence au modèle de communication entre le ou les réseaux locaux et les ressources du cloud dans AWS. Vous pouvez déployer des ressources cloud au sein d'un Amazon VPC au sein d'un Région AWS ou de plusieurs VPC répartis dans plusieurs régions, ainsi que des AWS services dotés d'un point de terminaison public dans une ou plusieurs régions Régions AWS, tels qu'Amazon S3 et DynamoDB.

Questions clés

- Existe-t-il une exigence de communication entre les VPC au sein d'une région et entre les régions ?
- Est-il nécessaire d'accéder aux points de terminaison AWS publics directement depuis les locaux ?
- Est-il nécessaire d'accéder aux AWS services à l'aide de points de terminaison VPC sur site ?

Capacités à prendre en compte

Voici quelques-uns des scénarios de modèles de connectivité les plus courants. Chaque modèle de connectivité couvre les exigences, les attributs et les considérations.

Remarque : comme indiqué précédemment, ce livre blanc se concentre sur la connectivité hybride entre les réseaux sur site et. AWS Pour plus de détails sur la conception de l'interconnexion des VPC, consultez le livre blanc sur la création d'une infrastructure réseau multi-VPC AWS évolutive et sécurisée.

Modèles

- AWS VPN de site à site accéléré —, unique AWS Transit GatewayRégion AWS
- AWS DX — DXGW avec VGW, région unique
- AWS DX — DXGW avec VGW, multi-régions et peering public AWS
- AWS DX — DXGW avec AWS Transit Gateway, multi-régions et peering public AWS
- AWS DX — DXGW avec AWS Transit Gateway plusieurs régions (plus de 3)

AWS VPN de site à site accéléré —, unique AWS Transit GatewayRégion AWS

Ce modèle est construit à partir de :

- Unique Région AWS.
- AWS Connexion VPN de site à site gérée avec. AWS Transit Gateway
- VPN accéléré activé.

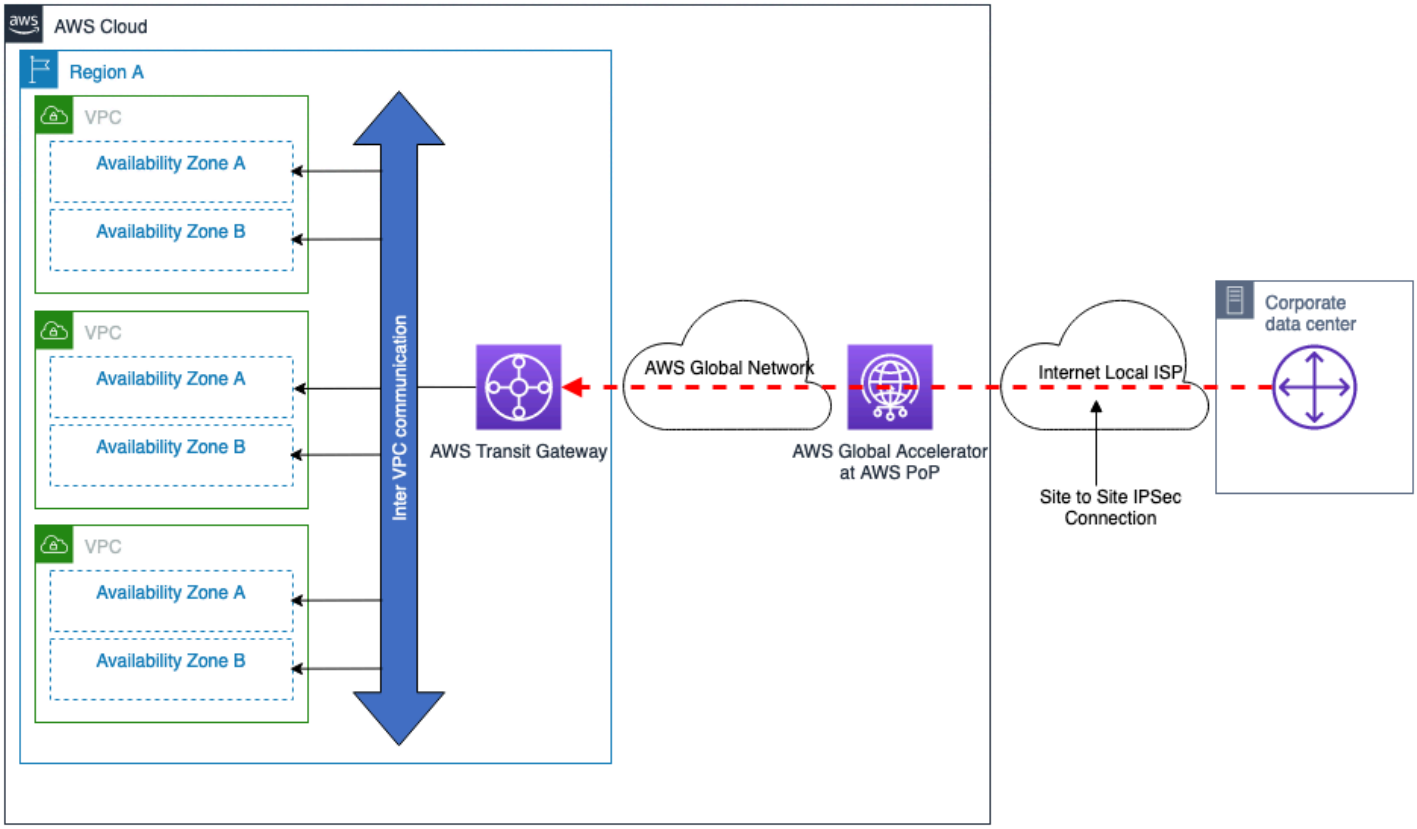

Figure 4 — VPN AWS géré — AWS Transit Gateway, unique Région AWS

Attributs du modèle de connectivité :

- Offrez la possibilité d'établir des connexions VPN optimisées sur l'Internet public en utilisant des connexions VPN AWS accélérées de site à site.
- Offrez la possibilité d'augmenter la bande passante de connexion VPN en configurant plusieurs tunnels VPN avec ECMP.
- Peut être utilisé pour la connexion à partir de plusieurs sites distants.
- Permet un basculement automatique avec routage dynamique (BGP).
- Lorsqu' AWS Transit Gateway ils sont connectés à des VPC, tous les VPC connectés peuvent utiliser les mêmes connexions VPN. Vous pouvez également contrôler le modèle de communication souhaité entre les VPC. Pour plus d'informations, reportez-vous à Comment fonctionnent les passerelles de transport en commun.
- Offre des options de conception flexibles pour intégrer des dispositifs de sécurité tiers et virtuels SD-WAN à. AWS Transit Gateway Voir Sécurité réseau centralisée pour le trafic VPC à VPC et sur site vers VPC.

Considérations relatives à l'échelle :

- Jusqu'à 50 Gbit/s de bande passante avec plusieurs tunnels IPsec et ECMP configurés (chaque flux de trafic sera limité à la bande passante maximale par tunnel VPN).
- Des milliers de VPC peuvent être connectés par. AWS Transit Gateway
- Reportez-vous aux quotas VPN de site à site pour connaître les autres limites d'échelle, telles que le nombre de routes.

Autres considérations :

- Les coûts AWS Transit Gateway de traitement supplémentaires liés au transfert de données entre le centre de données sur site et AWS.
- Les groupes de sécurité d'un VPC distant ne peuvent pas être référencés. Cela est AWS Transit Gateway toutefois pris en charge par le peering VPC.

AWS DX — DXGW avec VGW, région unique

Ce modèle est construit à partir de :

- Unique Région AWS.
- Deux AWS Direct Connect connexions vers des sites DX indépendants.
- AWS DXGW directement connecté aux VPC à l'aide de VGW.
- Utilisation facultative de AWS Transit Gateway pour la communication inter-VPC.

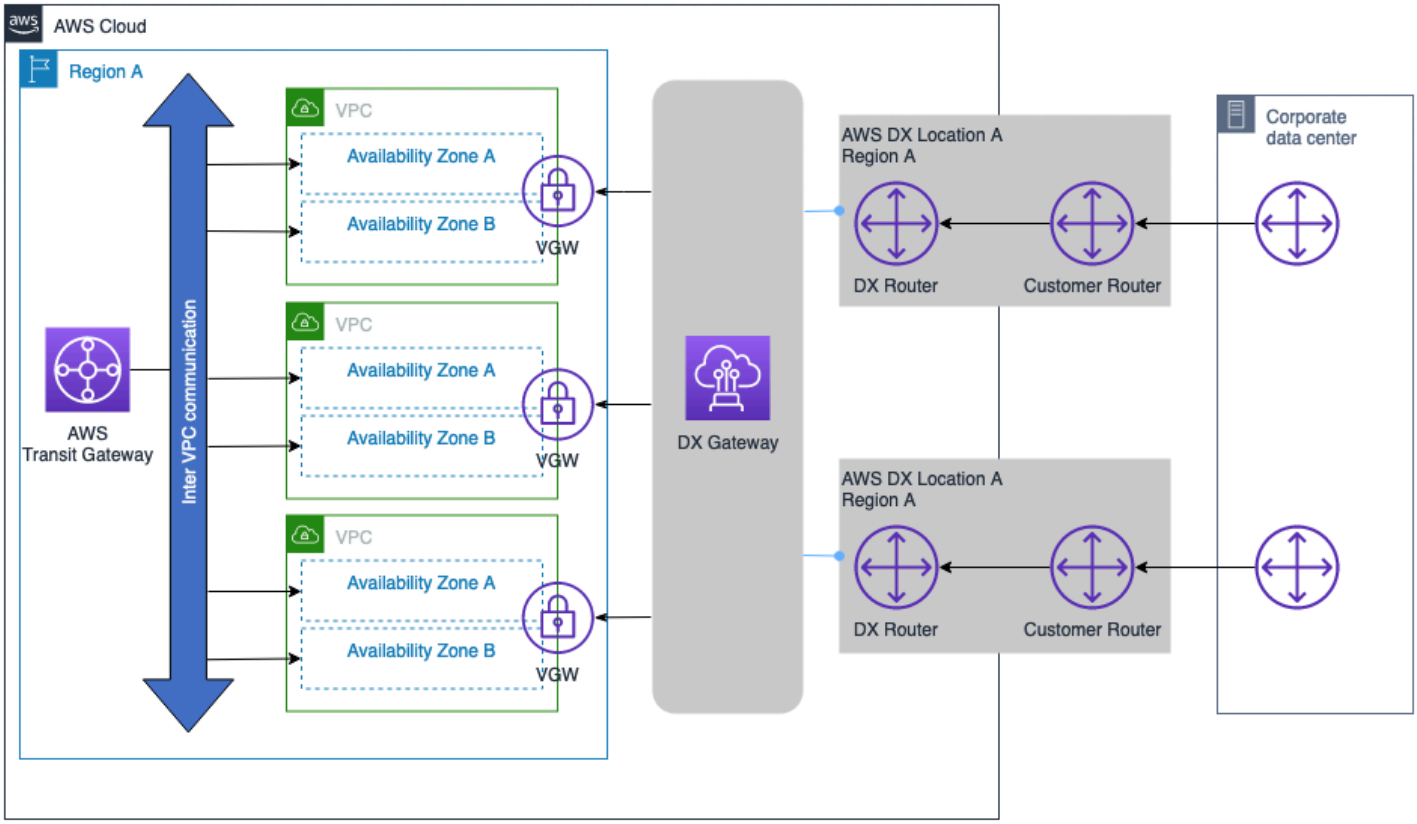

Figure 5 — AWS DX — DXGW avec VGW, simple Région AWS

Attributs du modèle de connectivité :

- Permet de se connecter à des VPC et à des connexions DX dans d'autres régions à l'avenir.
- Permet un basculement automatique avec routage dynamique (BGP).
- AWS Transit Gateway Vous pouvez ainsi contrôler le modèle de communication souhaité entre les VPC. Pour plus d'informations, reportez-vous à la section Fonctionnement des passerelles de transport en commun.

Considérations relatives à l'échelle :

AWS Direct Connect Référez-vous aux quotas pour plus d'informations sur les autres limites d'échelle, telles que le nombre de préfixes pris en charge, le nombre de VIF par type de connexion DX (dédiée, hébergée). Voici quelques points essentiels à prendre en compte :

- La session BGP pour un VIF privé peut annoncer jusqu'à 100 routes chacune pour IPv4 et IPv6.

- Jusqu'à 20 VPC peuvent être connectés par DXGW au cours d'une seule session BGP. Si plus de 20 VPC sont nécessaires, des DXGW supplémentaires peuvent être ajoutés pour faciliter la connectivité à grande échelle, ou envisager d'utiliser l'intégration de Transit Gateway.
- Des AWS Direct Connect s supplémentaires peuvent être ajoutés comme vous le souhaitez.

Autres considérations :

- Aucun coût de traitement AWS Transit Gateway associé au transfert de données entre les réseaux locaux AWS et entre eux.
- Les groupes de sécurité d'un VPC distant ne peuvent pas être référencés AWS Transit Gateway (nécessite un peering VPC).
- Le peering VPC peut être utilisé plutôt que AWS Transit Gateway pour faciliter la communication entre les VPC, mais cela ajoute de la complexité opérationnelle à la création et à la gestion d'un grand nombre de VPC peering à grande échelle. point-to-point
- Si la communication entre VPC n'est pas requise, ni l'appairage AWS Transit Gateway VPC ne sont nécessaires dans ce modèle de connectivité.

AWS DX — DXGW avec VGW, multi-régions et peering public AWS

Ce modèle est construit à partir de :

- Plusieurs centres de données sur site avec double connexion à AWS.
- Deux AWS Direct Connect connexions vers des sites DX indépendants.
- AWS DXGW directement connecté à plus de 10 VPC via VGW, jusqu'à 20 VPC utilisant VGW.
- Utilisation facultative de AWS Transit Gateway pour les communications inter-VPC et inter-régions.

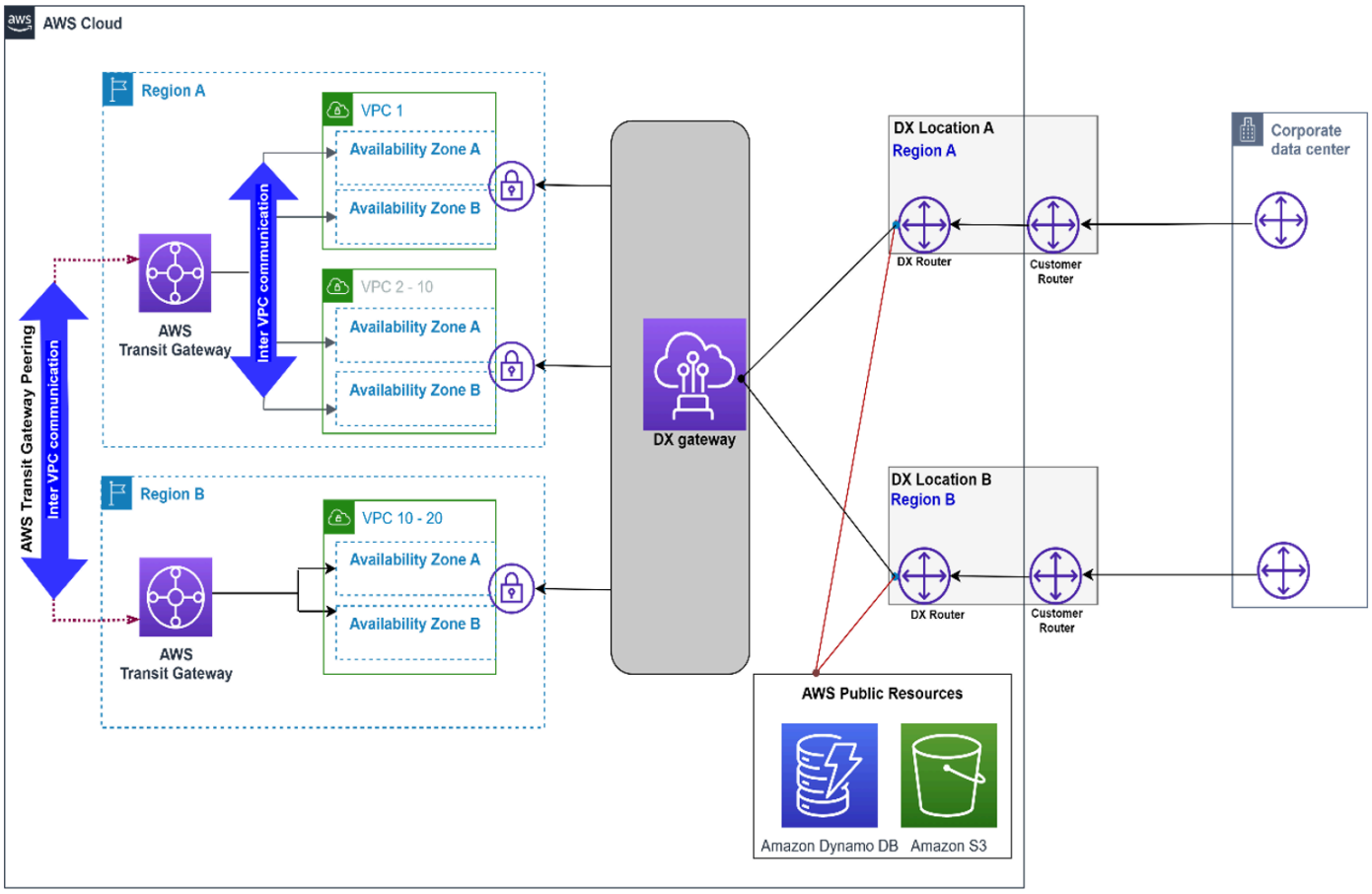

Figure 6 — AWS DX — DXGW avec VGW, multi-régions et VIF public

Attributs du modèle de connectivité :

- AWS DXGW directement connecté à plus de 10 VPC utilisant VGW, jusqu'à 20 VPC utilisant VGW.
- AWS Le VIF public DX est utilisé pour accéder aux services AWS publics, tels qu'Amazon S3, directement via les connexions AWS DX.
- Offrez la possibilité de vous connecter à des VPC et à des connexions DX dans d'autres régions à l'avenir.
- Communication VPC entre VPC et entre régions facilitée par le peering AWS Transit Gateway Transit Gateway.

Considérations relatives à l'échelle :

AWS Direct Connect Référez-vous aux quotas pour plus d'informations sur les autres limites d'échelle, telles que le nombre de préfixes pris en charge, le nombre de VIF par type de connexion DX (dédiée, hébergée). Voici quelques points essentiels à prendre en compte :

- La session BGP pour un VIF privé peut annoncer jusqu'à 100 routes chacune pour IPv4 et IPv6.
- Jusqu'à 20 VPC peuvent être connectés par DXGW au cours d'une seule session BGP sur chaque VIF privé, jusqu'à 30 VIF privés par DXGW.
- Des AWS Direct Connect s supplémentaires peuvent être ajoutés comme vous le souhaitez.

Autres considérations :

- Aucun coût de traitement AWS Transit Gateway associé au transfert de données entre les réseaux locaux AWS et entre eux.
- Les groupes de sécurité d'un VPC distant ne peuvent pas être référencés AWS Transit Gateway (nécessite un peering VPC).
- Le peering VPC peut être utilisé plutôt que AWS Transit Gateway pour faciliter la communication entre les VPC, mais cela ajoutera de la complexité opérationnelle pour créer et gérer un grand nombre de VPC peering à grande échelle. point-to-point
- Si la communication entre VPC n'est pas requise, ni l'appairage AWS Transit Gateway VPC ne sont nécessaires dans ce modèle de connectivité.

AWS DX — DXGW avec AWS Transit Gateway, multi-régions et peering public AWS

Ce modèle est construit à partir de :

- Multiple Régions AWS.
- Deux AWS Direct Connect connexions vers des sites DX indépendants.
- Un seul centre de données sur site avec deux connexions à AWS.
- AWS DXGW avec. AWS Transit Gateway
- Nombre élevé de VPC par région.

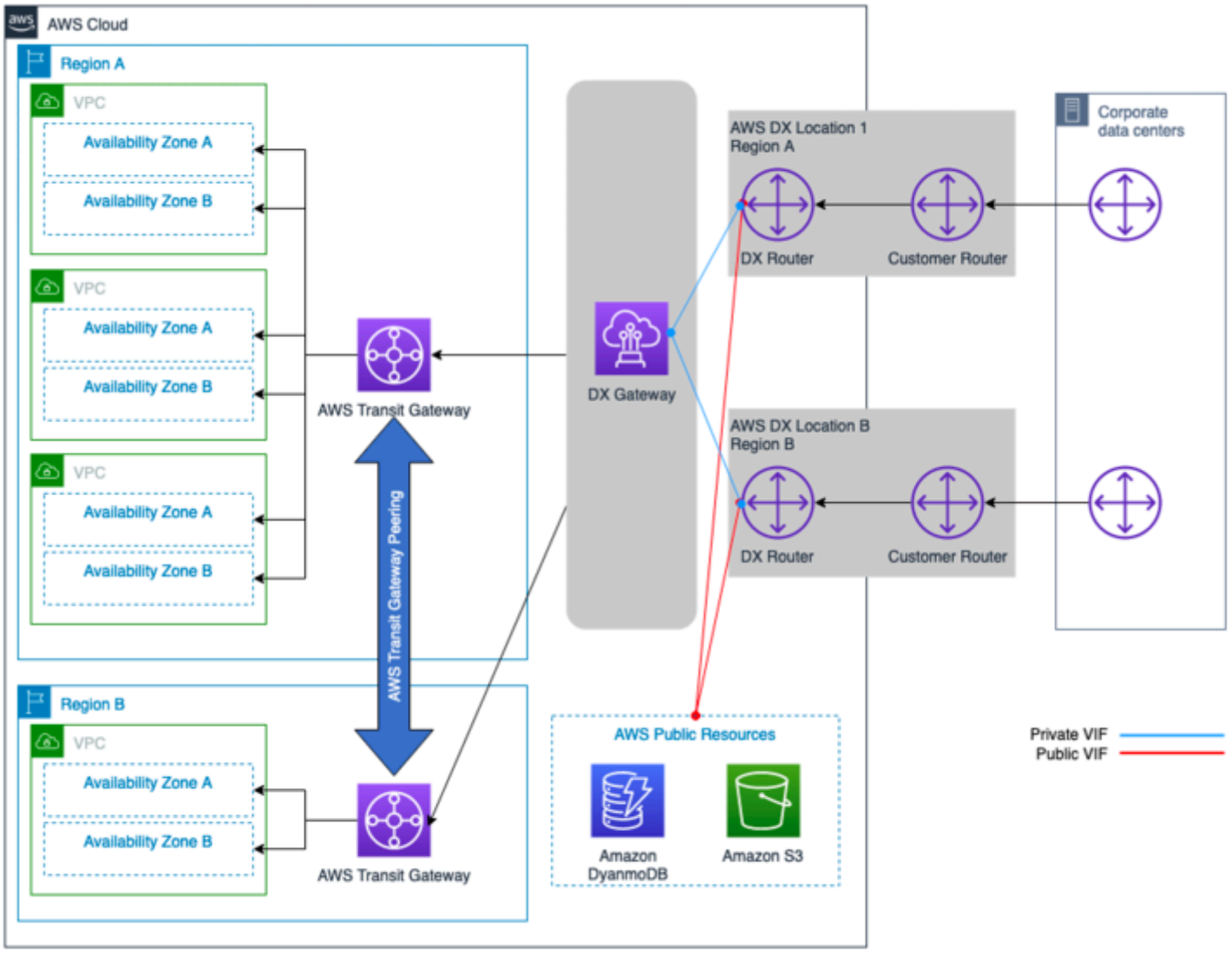

Figure 7 — AWS DX — DXGW avec AWS Transit Gateway, multi-régions et VIF public AWS

Attributs du modèle de connectivité :

- AWS Le VIF public DX est utilisé pour accéder à des ressources AWS publiques telles que S3 directement via les connexions AWS DX.
- Offrez la possibilité de vous connecter à des VPC et/ou à des connexions DX dans d'autres régions à l'avenir.
- Une AWS Transit Gateway fois connecté aux VPC, une connectivité maillée complète ou partielle peut être obtenue entre les VPC.
- Communication entre VPC et VPC inter-régions facilitée par le peering. AWS Transit Gateway

- Offre des options de conception flexibles pour intégrer des dispositifs de sécurité tiers et virtuels SD-WAN. AWS Transit Gateway Voir : Sécurité réseau centralisée pour le trafic VPC à VPC et sur site vers VPC.

Considérations relatives à l'échelle :

- Le nombre d'itinéraires à destination et en provenance AWS Transit Gateway est limité au nombre maximum d'itinéraires pris en charge via un Transit VIF (les nombres entrants et sortants varient). Reportez-vous aux AWS Direct Connect quotas pour plus d'informations sur les limites d'échelle et le nombre de routes et de VIF pris en charge.
- Passez à des milliers de VPC par AWS Transit Gateway session BGP.
- Un seul Transit VIF par AWS DX.
- Des connexions AWS DX supplémentaires peuvent être ajoutées selon les besoins.

Autres considérations :

- Encourt des coûts de AWS Transit Gateway traitement supplémentaires pour le transfert de données entre le site AWS et le site sur site.
- Les groupes de sécurité d'un VPC distant ne peuvent pas être référencés AWS Transit Gateway (nécessite un peering VPC).
- Le peering VPC peut être utilisé plutôt que AWS Transit Gateway pour faciliter la communication entre les VPC, mais cela ajoutera de la complexité opérationnelle pour créer et gérer un grand nombre de VPC peering à grande échelle. point-to-point
- Si plus de trois AWS Transit Gateway s sont nécessaires, du DXGW supplémentaire peut être ajouté. Reportez-vous au mode de connectivité suivant.

AWS DX — DXGW avec AWS Transit Gateway plusieurs régions (plus de 3)

Ce modèle est construit à partir de :

- Multiple Régions AWS (plus de 3).
- Deux centres de données sur site.
- Deux AWS Direct Connect connexions vers des sites DX indépendants par région.
- AWS DXGW avec. AWS Transit Gateway
- Nombre élevé de VPC par région.

- Maille complète de peering entre AWS Transit Gateway nous.

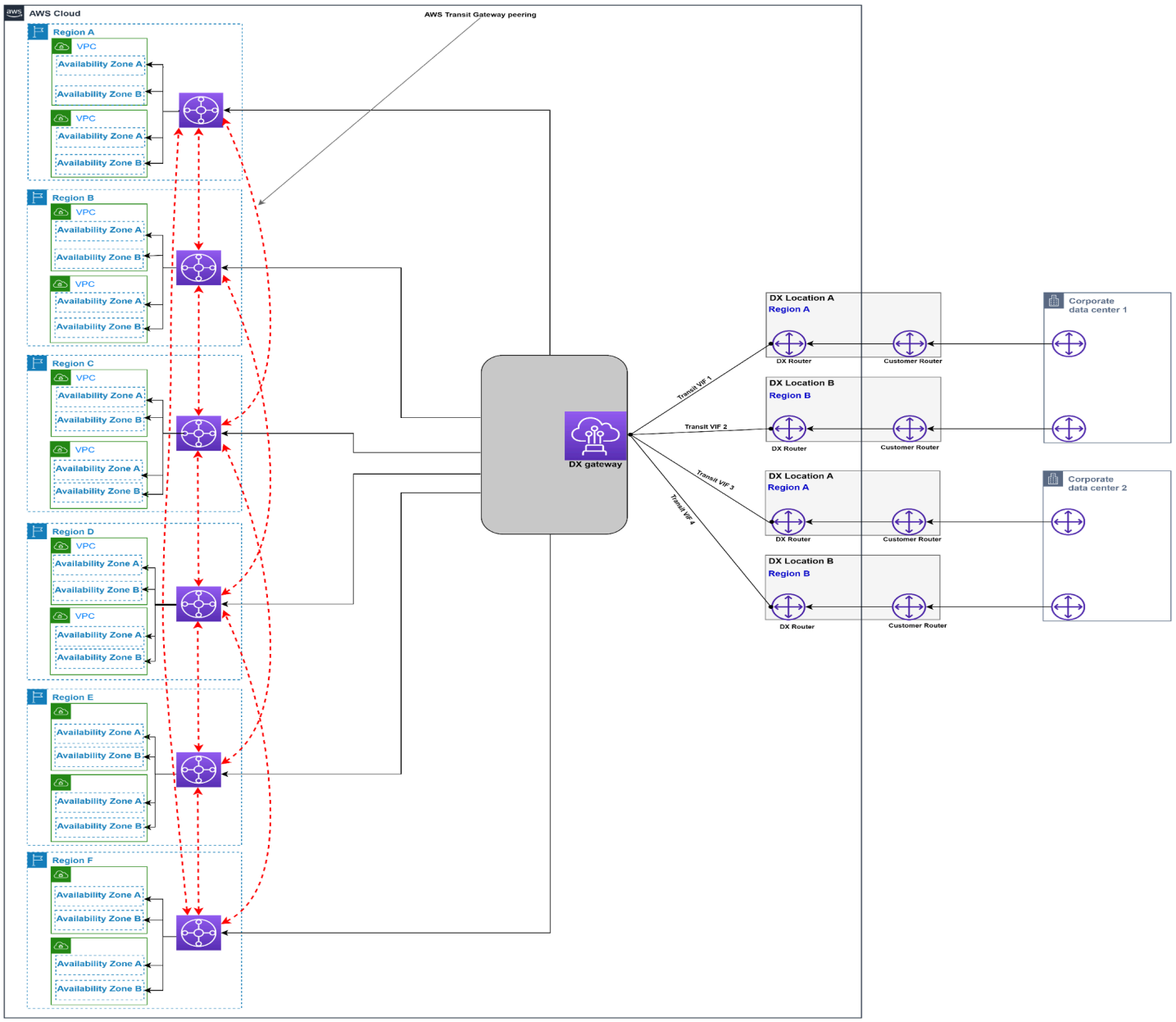

Figure 8 — AWS DX — DXGW avec AWS Transit Gateway plusieurs régions (plus de trois)

Attributs du modèle de connectivité :

- Frais d'exploitation les plus faibles.
- AWS Le VIF public DX est utilisé pour accéder aux ressources AWS publiques, telles que S3, directement via les connexions AWS DX.

- Offrez la possibilité de vous connecter à des VPC et à des connexions DX dans d'autres régions à l'avenir.
- Une AWS Transit Gateway fois connecté aux VPC, une connectivité maillée complète ou partielle peut être obtenue entre les VPC.
- La communication VPC interrégionale est facilitée par AWS Transit Gateway le peering.
- Offre des options de conception flexibles pour intégrer des dispositifs de sécurité tiers et virtuels SD-WAN. AWS Transit Gateway Voir : Sécurité réseau centralisée pour le trafic VPC à VPC et sur site vers VPC.

Considérations relatives à l'échelle :

- Le nombre d'itinéraires à destination et en provenance AWS Transit Gateway est limité au nombre maximum d'itinéraires pris en charge via un Transit VIF (les nombres entrants et sortants varient). Reportez-vous aux AWS Direct Connect quotas pour plus d'informations sur les limites d'échelle. Envisagez de résumer les itinéraires si nécessaire pour réduire le nombre d'itinéraires.
- Passez à des milliers de VPC par AWS Transit Gateway session BGP unique par DXGW (en supposant que les performances fournies par les connexions AWS DX provisionnées soient suffisantes).
- Jusqu'à six AWS Transit Gateway s peuvent être connectés par DXGW.
- Si plus de trois régions doivent être connectées AWS Transit Gateway, des DXGW supplémentaires sont nécessaires.
- Un seul Transit VIF par AWS DX.
- Des connexions AWS DX supplémentaires peuvent être ajoutées selon les besoins.

Autres considérations :

- Encourt des coûts AWS Transit Gateway de traitement supplémentaires pour le transfert de données entre le site sur site et. AWS
- Les groupes de sécurité d'un VPC distant ne peuvent pas être référencés AWS Transit Gateway (nécessite un peering VPC).
- Le peering VPC peut être utilisé plutôt que AWS Transit Gateway pour faciliter la communication entre les VPC, mais cela ajoutera de la complexité opérationnelle pour créer et gérer un grand nombre de VPC peering à grande échelle. point-to-point

L'arbre de décision suivant couvre les considérations relatives à l'évolutivité et au modèle de communication :

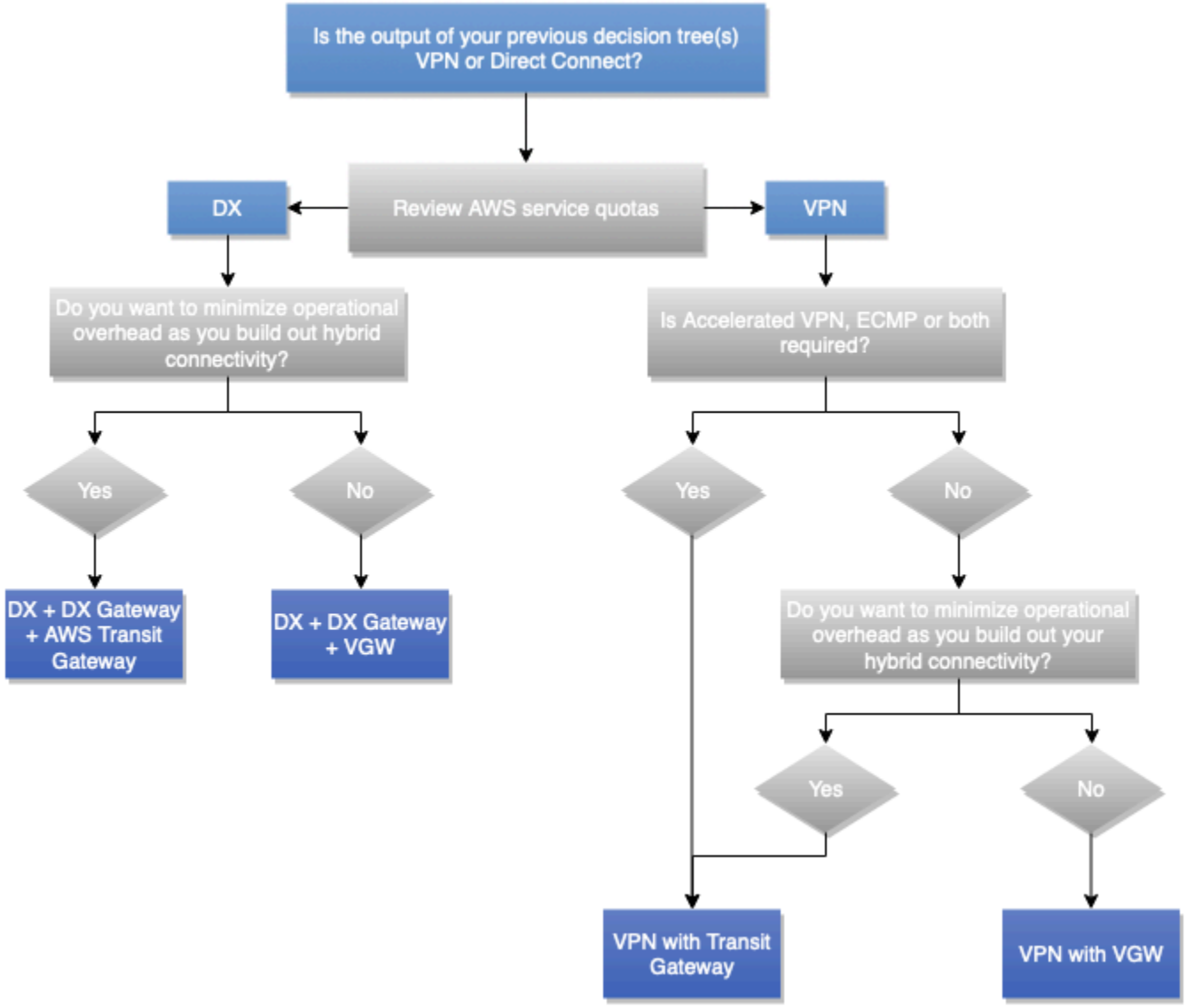

Figure 9 — Arbre décisionnel du modèle d'évolutivité et de communication

> **Note**
>
> Si le type de connexion sélectionné est VPN, généralement pour des raisons de performance, il convient de décider si le point de terminaison du VPN est une connexion VPN AWS VGW ou AWS Transit Gateway AWS S2S. Si ce n'est pas encore fait, vous pouvez prendre en compte le modèle de communication requis entre le VPC ainsi que le nombre de VPC à connecter à la ou aux connexions VPN pour vous aider à prendre une décision.

Fiabilité

Définition

La fiabilité fait référence à la capacité d'un service ou d'un système à exécuter la fonction attendue lorsque cela est nécessaire. La fiabilité d'un système peut être mesurée par le niveau de sa qualité opérationnelle dans un laps de temps donné. Comparez cela à la résilience, qui fait référence à la capacité d'un système à se remettre d'une infrastructure ou d'une interruption de service de manière dynamique et fiable.

Pour plus de détails sur la manière dont la disponibilité et la résilience sont utilisées pour mesurer la fiabilité, reportez-vous au pilier de fiabilité du AWS Well-Architected Framework.

Questions clés

Disponibilité

La disponibilité est le pourcentage de temps pendant lequel une charge de travail est disponible pour être utilisée. Les objectifs les plus courants sont les suivants : 99 % (3,65 jours d'indisponibilité autorisés par an), 99,9 % (8,77 heures) et 99,99 % (52,6 minutes), avec une réduction du nombre de neuf dans le pourcentage (« deux neuf » pour 99 %, « trois neuf » pour 99,9 %, etc.). La disponibilité de la solution réseau entre AWS et le centre de données sur site peut être différente de la disponibilité globale de la solution ou de l'application.

Les principales questions relatives à la disponibilité d'une solution réseau sont les suivantes :

- Mes AWS ressources peuvent-elles continuer à fonctionner si elles ne peuvent pas communiquer avec mes ressources sur site ? Et vice versa ?
- Dois-je considérer les interruptions programmées pour la maintenance planifiée comme incluses ou exclues de la métrique de disponibilité ?
- Comment vais-je mesurer la disponibilité de la couche réseau, indépendamment de l'état général de l'application ?

La section Disponibilité du pilier de fiabilité du Well-Architected Framework contient des suggestions et des formules pour la disponibilité des calculs.

Résilience

La résilience est la capacité d'une charge de travail à se rétablir après une interruption d'infrastructure ou de service, à acquérir dynamiquement des ressources informatiques pour répondre à la demande

et à atténuer les perturbations, telles que les mauvaises configurations ou les problèmes de réseau transitoires. Si un composant réseau redondant (lien, périphériques réseau, etc.) n'est pas suffisamment disponible pour fournir seul la fonction attendue, il présente une faible résilience aux pannes. Il en résulte une expérience utilisateur médiocre et dégradée.

Les principales questions relatives à la résilience d'une solution réseau sont les suivantes :

- Combien de défaillances discrètes et simultanées dois-je prévoir ?
- Comment puis-je réduire les points de défaillance uniques à la fois grâce aux solutions de connectivité et à mon réseau interne ?
- Quelle est ma vulnérabilité face aux événements de déni de service distribué (DDoS) ?

Solution technique

Tout d'abord, il est important de noter que toutes les solutions de connectivité réseau hybride ne nécessitent pas un haut niveau de fiabilité, et que l'augmentation des niveaux de fiabilité entraîne une augmentation correspondante des coûts. Dans certains scénarios, un site principal peut nécessiter des connexions fiables (redondantes et résilientes) car les interruptions de service ont un impact plus important sur l'activité, tandis que les sites régionaux peuvent ne pas exiger le même niveau de fiabilité en raison de l'impact moindre sur l'entreprise en cas de panne. Il est recommandé de se référer aux recommandations de AWS Direct Connect résilience car elles expliquent les AWS meilleures pratiques pour garantir une résilience élevée lors de la conception. AWS Direct Connect

Pour obtenir une solution de connectivité réseau hybride fiable dans un contexte de résilience, la conception doit prendre en compte les aspects suivants :

- Redondance : visez à éliminer tout point de défaillance unique sur le chemin de connectivité réseau hybride, y compris, mais sans s'y limiter, les connexions réseau, les périphériques réseau, la redondance entre les zones de disponibilité et les emplacements DX Régions AWS, ainsi que les sources d'alimentation des appareils, les chemins de fibre optique et les systèmes d'exploitation. Aux fins et dans le cadre de ce livre blanc, la redondance se concentre sur les connexions réseau, les appareils périphériques (par exemple, les dispositifs de passerelle client), la localisation AWS DX et Régions AWS (pour les architectures multirégionales).
- Composants de basculement fiables : dans certains scénarios, un système peut être fonctionnel, mais ne pas exécuter ses fonctions au niveau requis. Une telle situation est courante lors d'une panne unique lorsqu'il est découvert que les composants redondants prévus fonctionnaient de

manière non redondante. Leur charge réseau n'a aucune autre destination en raison de leur utilisation, ce qui se traduit par une capacité insuffisante pour l'ensemble de la solution.

- Temps de basculement : le temps de basculement est le temps nécessaire à un composant secondaire pour assumer pleinement le rôle du composant principal. Le temps de basculement dépend de plusieurs facteurs : le temps nécessaire pour détecter la panne, le temps nécessaire pour activer la connectivité secondaire et le temps nécessaire pour informer le reste du réseau de la modification. La détection des défaillances peut être améliorée à l'aide de la détection des pairs morts (DDP) pour les liaisons VPN et de la détection du transfert bidirectionnel (BFD) pour les liaisons. AWS Direct Connect Le délai d'activation de la connectivité secondaire peut être très court (si ces connexions sont toujours actives), court (si une connexion VPN préconfigurée doit être activée) ou plus long (si des ressources physiques doivent être déplacées ou de nouvelles ressources configurées). La notification du reste du réseau se fait généralement par le biais de protocoles de routage internes au réseau du client, chacun d'entre eux ayant des temps de convergence et des options de configuration différents. La configuration de ces protocoles n'entre pas dans le cadre de ce livre blanc.
- Ingénierie du trafic : L'ingénierie du trafic dans le contexte d'une conception de connectivité réseau hybride résiliente vise à déterminer comment le trafic doit circuler sur plusieurs connexions disponibles dans des scénarios normaux et de panne. Il est recommandé de suivre le concept de conception en cas de défaillance, selon lequel vous devez déterminer comment la solution fonctionnera dans différents scénarios de défaillance et si elle sera acceptable ou non par l'entreprise. Cette section décrit certains des cas d'utilisation courants de l'ingénierie du trafic qui visent à améliorer le niveau de résilience global de la solution de connectivité réseau hybride. La AWS Direct Connect section sur le routage et le BGP traite de plusieurs options d'ingénierie du trafic pour influencer le flux de trafic (communautés, préférence locale BGP, longueur du chemin AS). Pour concevoir une solution d'ingénierie du trafic efficace, vous devez bien comprendre comment chacun des composants du AWS réseau gère le routage IP en termes d'évaluation et de sélection des itinéraires, ainsi que les mécanismes possibles pour influencer le choix des itinéraires. Les détails à ce sujet n'entrent pas dans le cadre de ce document. Pour plus d'informations, consultez la documentation Transit Gateway Route Evaluation Order, Site-to-Site VPN Route Priority et Direct Connect Routing et BGP selon les besoins.

> **Note**
>
> Dans la table de routage VPC, vous pouvez faire référence à une liste de préfixes contenant des règles de sélection d'itinéraires supplémentaires. Pour plus d'informations sur ce cas d'utilisation, reportez-vous à la section Priorité des itinéraires pour les listes de préfixes. AWS

Transit Gateway les tables de routage prennent également en charge les listes de préfixes, mais une fois appliquées, elles sont étendues à des entrées de route spécifiques.

Exemple de double connexion VPN de site à site avec des itinéraires plus spécifiques

Ce scénario est basé sur un petit site sur site se connectant à un seul Région AWS via des connexions VPN redondantes via Internet à. AWS Transit Gateway La conception de l'ingénierie du trafic illustrée à la Figure 10 montre qu'avec l'ingénierie du trafic, vous pouvez influencer le choix du chemin afin d'accroître la fiabilité de la solution de connectivité hybride en :

- Connectivité hybride résiliente : les connexions VPN redondantes fournissent chacune la même capacité de performance, prennent en charge le basculement automatique en utilisant le protocole de routage dynamique (BGP) et accélèrent la détection des défaillances de connexion grâce à la détection des pairs morts du VPN.
- Efficacité des performances : configurer l'ECMP sur les deux connexions VPN afin de AWS Transit Gateway maximiser la bande passante globale de la connexion VPN. Alternativement, en annonçant des itinéraires différents, plus spécifiques, en plus de l'itinéraire récapitulatif du site, la charge peut être gérée indépendamment entre les deux connexions VPN

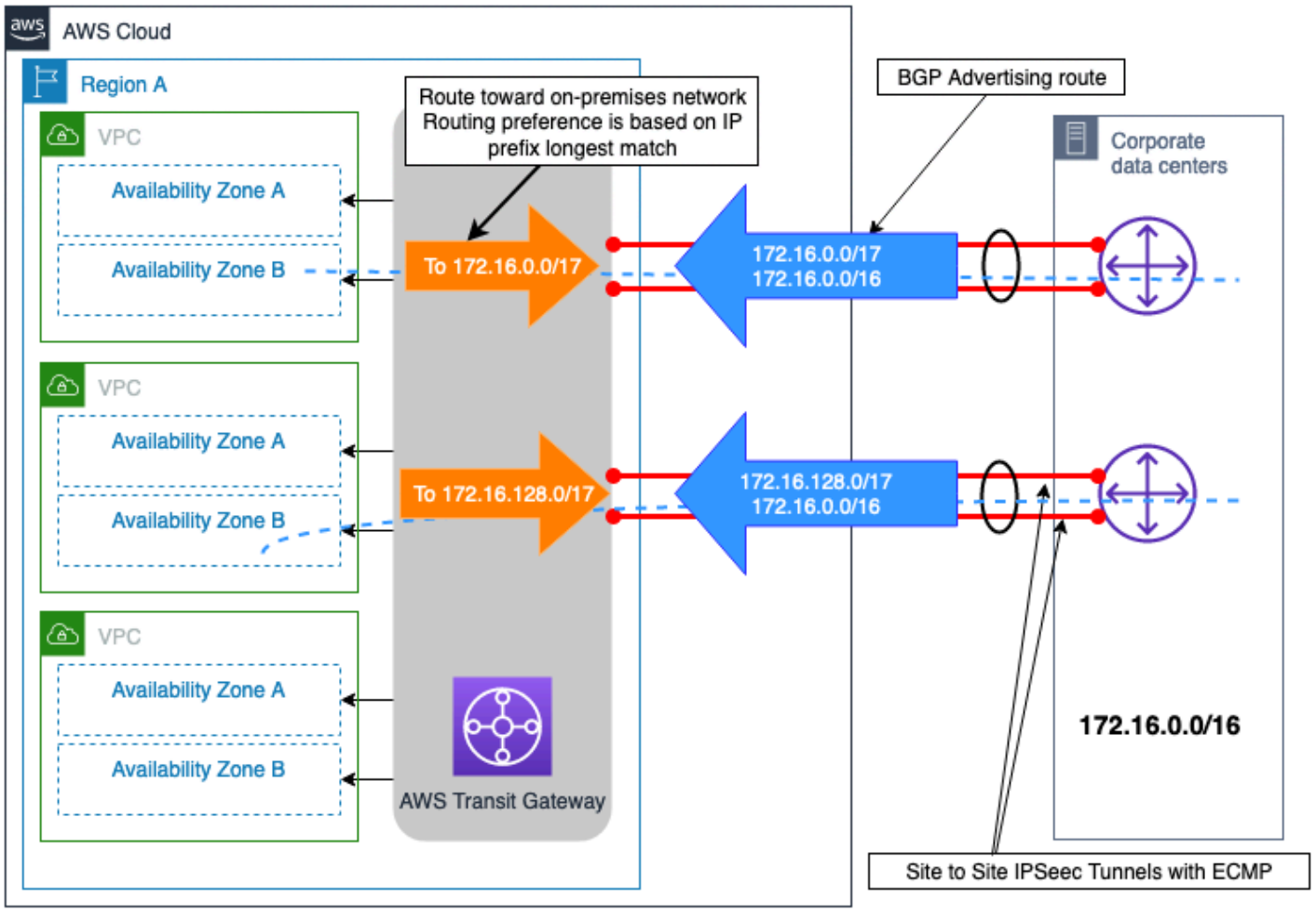

Figure 10 — Exemple de double connexion VPN de site à site avec des itinéraires plus spécifiques

Exemple de deux sites sur site avec plusieurs connexions DX

Le scénario illustré à la Figure 11 montre deux sites de centres de données sur site situés dans différentes régions géographiques et connectés à AWS l'aide du modèle de connectivité Maximum Resiliency (décrit dans les recommandations de AWS Direct Connect résilience) utilisant DXGW et AWS Direct Connect VGW. Ces deux sites sur site sont interconnectés via une liaison d'interconnexion de centres de données (DCI). Les préfixes IP locaux (192.168.0.0/16) qui appartiennent aux sites de succursales distants sont annoncés à partir des deux sites de centres de données locaux. Le chemin principal pour ce préfixe doit être le centre de données 1. Le trafic à destination et en provenance des sites distants basculera vers le centre de données 2 en cas de panne du centre de données 1 ou des deux sites DX. Il existe également un préfixe IP spécifique au site pour chaque centre de données. Ces préfixes doivent être accessibles directement et via l'autre site du centre de données en cas de défaillance des deux sites DX.

En associant les attributs de la communauté BGP aux routes annoncées à AWS DXGW, vous pouvez influencer la sélection du chemin de sortie du côté de DXGW. AWS Ces attributs de communauté contrôlent AWS l'attribut de préférence locale BGP attribué à l'itinéraire annoncé. Pour plus d'informations, reportez-vous aux politiques de routage AWS DX et aux communautés BGP.

Pour optimiser la fiabilité de la connectivité au Région AWS niveau, chaque paire de connexions AWS DX configure ECMP afin que les deux puissent être utilisées simultanément pour le transfert de données entre chaque site sur site et. AWS

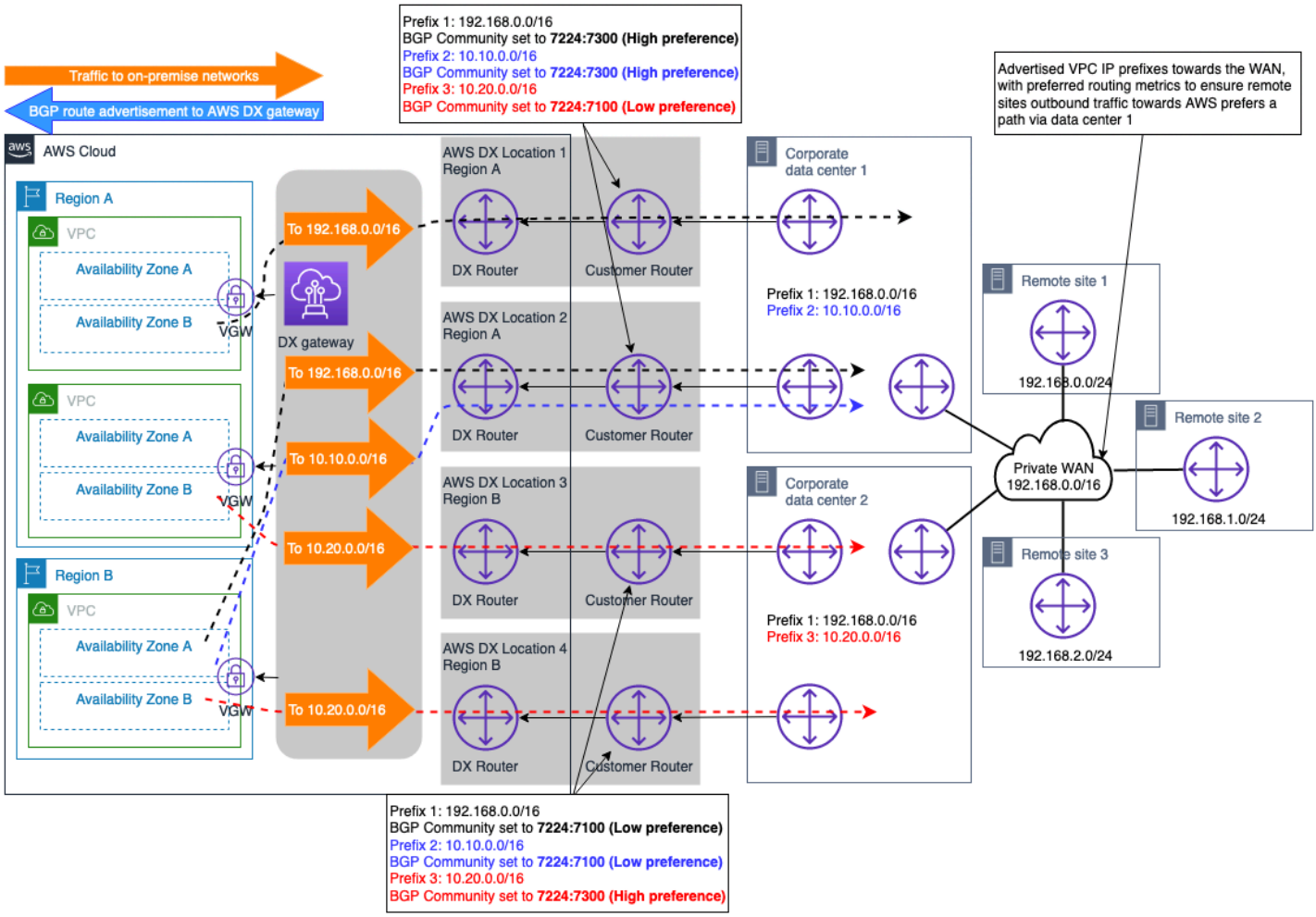

Figure 11 — Exemple de deux sites sur site avec plusieurs connexions DX

Avec cette conception, les flux de trafic destinés aux réseaux sur site (avec la même longueur de préfixe annoncée et la même communauté BGP) seront répartis sur les deux connexions DX par site à l'aide d'ECMP. Toutefois, si l'ECMP n'est pas requis sur la connexion DX, le même concept discuté

précédemment et décrit dans la documentation des politiques de routage et des communautés BGP peut être utilisé pour affiner la sélection du chemin au niveau de la connexion DX.

Remarque : Si des dispositifs de sécurité se trouvent sur le chemin des centres de données locaux, ils doivent être configurés pour autoriser les flux de trafic sortant par une liaison DX et provenant d'une autre liaison DX (les deux liaisons étant utilisées avec ECMP) au sein du même site de centre de données.

Exemple de connexion VPN en tant que sauvegarde d'une connexion AWS DX

Le VPN peut être sélectionné pour fournir une connexion réseau de secours à une AWS Direct Connect connexion. Ce type de modèle de connectivité est généralement dicté par le coût, car il réduit le niveau de fiabilité de la solution de connectivité hybride globale en raison de performances indéterministes sur Internet, et aucun SLA ne peut être obtenu pour une connexion via l'Internet public. Il s'agit d'un modèle de connectivité valide et rentable, qui doit être utilisé lorsque le coût est la priorité absolue et que le budget est limité, ou éventuellement comme solution provisoire jusqu'à ce qu'un DX secondaire puisse être fourni. La figure 12 illustre la conception de ce modèle de connectivité. L'un des principaux aspects de cette conception, où les connexions VPN et DX se terminent au AWS Transit Gateway, est que la connexion VPN peut annoncer un plus grand nombre de routes que celles qui peuvent être annoncées via une connexion DX connectée à. AWS Transit Gateway Cela peut entraîner une situation de routage sous-optimale. Une option pour résoudre ce problème consiste à configurer le filtrage des itinéraires sur le dispositif de passerelle client (CGW) pour les itinéraires reçus de la connexion VPN, en autorisant uniquement les itinéraires récapitulatifs à accepter.

Remarque : Pour créer l'itinéraire récapitulatif sur le AWS Transit Gateway, vous devez spécifier un itinéraire statique vers une pièce jointe arbitraire dans la table de AWS Transit Gateway routage afin que le résumé soit envoyé le long de l'itinéraire le plus spécifique.

Du point de vue de la table de AWS Transit Gateway routage, les routes pour le préfixe local sont reçues à la fois de la connexion AWS DX (via DXGW) et du VPN, avec la même longueur de préfixe. Selon la logique de priorité des itinéraires de AWS Transit Gateway, les itinéraires reçus via Direct Connect ont une préférence plus élevée que ceux reçus via le VPN Site-to-Site, et le chemin qui les traverse AWS Direct Connect sera donc le chemin préféré pour atteindre le ou les réseaux locaux.

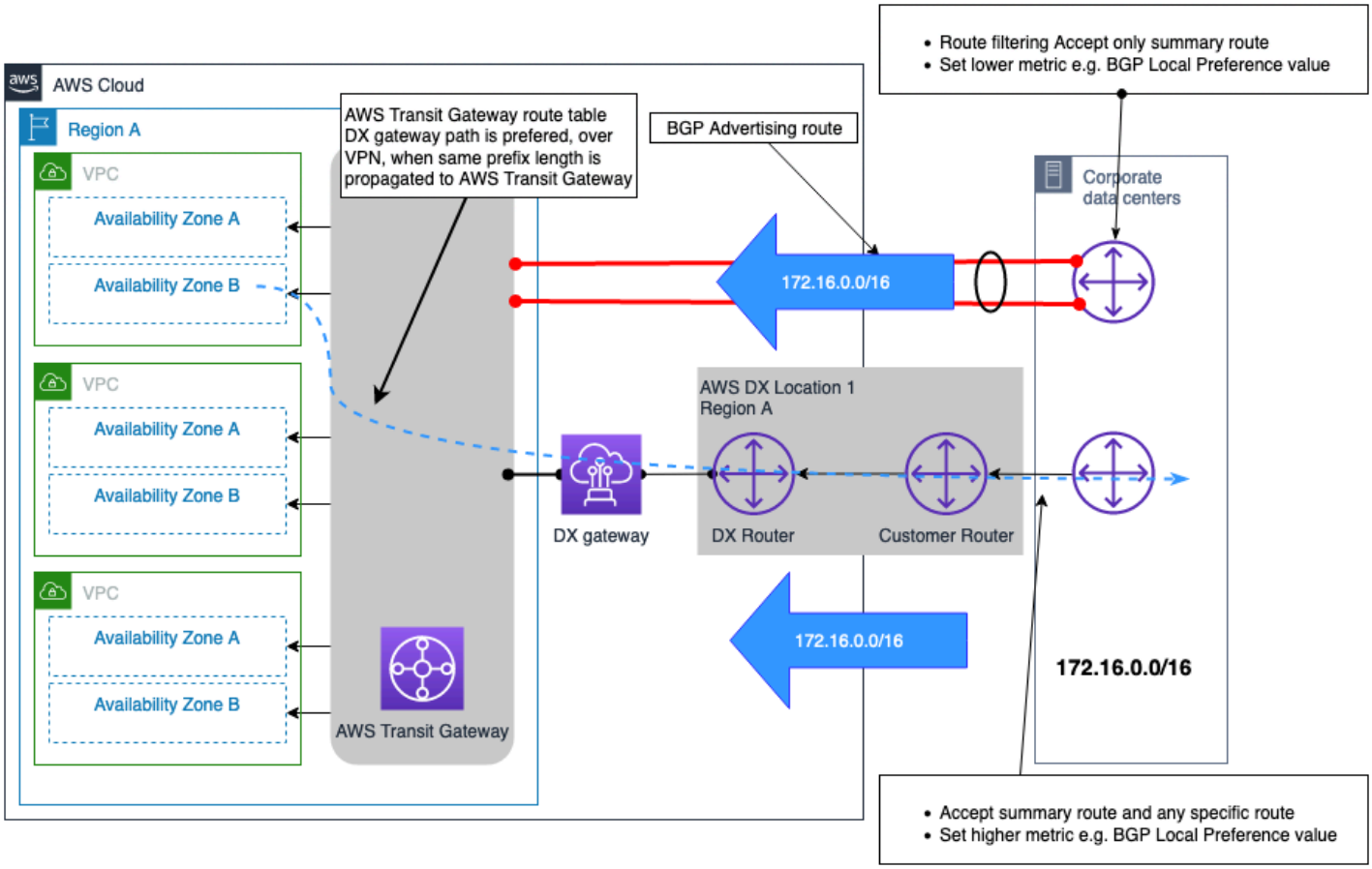

Figure 12 — Exemple de connexion VPN en tant que sauvegarde d'une connexion AWS DX

L'arbre de décision suivant vous guide dans la prise de décision souhaitée pour parvenir à une connectivité réseau hybride résiliente (qui se traduira par une connectivité réseau hybride fiable). Pour plus d'informations, reportez-vous à AWS Direct Connect Resiliency Toolkit.

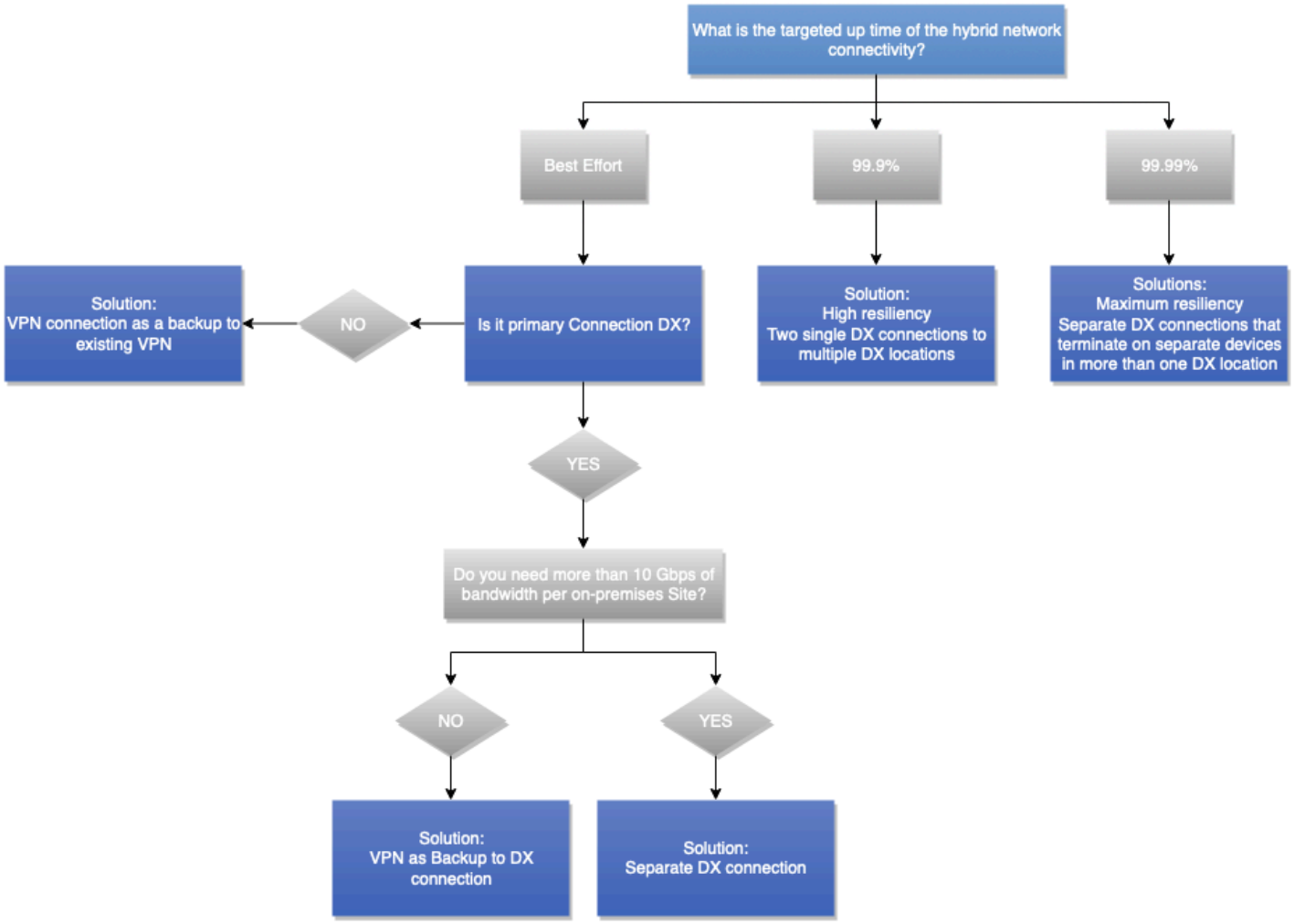

Figure 13 — Arbre décisionnel en matière de fiabilité

VPN et SD-WAN gérés par le client

Définition

La connectivité à Internet est une marchandise et la bande passante disponible continue d'augmenter chaque année. Certains clients choisissent de créer un WAN virtuel sur Internet plutôt que de créer et d'exploiter un réseau WAN privé. Un réseau étendu défini par logiciel (SD-WAN) permet aux entreprises de fournir et de gérer rapidement et de manière centralisée ce WAN virtuel grâce à une utilisation intelligente de logiciels. D'autres clients choisissent d'adopter les VPN autogérés traditionnels de site à site.

Impact sur les décisions de conception

Le SD-WAN et les VPN gérés par le client peuvent fonctionner via Internet ou. AWS Direct Connect Le SD-WAN (ou toute autre superposition de VPN logiciel) est aussi fiable que le transport réseau sous-jacent. Par conséquent, les considérations relatives à la fiabilité et aux SLA abordées précédemment dans ce livre blanc s'appliquent ici. Par exemple, la création d'une superposition SD-WAN sur Internet n'offrira pas la même fiabilité que si elle est construite sur un. AWS Direct Connect

Définition des exigences

- Utilisez-vous le SD-WAN dans votre réseau sur site ?
- Avez-vous besoin de fonctionnalités spécifiques qui ne sont disponibles que sur certains appareils virtuels utilisés pour la terminaison d'un VPN ?

Solutions techniques

AWS recommande d'intégrer le SD-WAN au AWS Transit Gateway SD-WAN et publie une liste des fournisseurs qui prennent en charge AWS Transit Gateway l'intégration. AWS peut servir de hub pour les sites SD-WAN ou de site satellite. Le AWS backbone peut être utilisé pour connecter différents hubs SD-WAN déployés AWS à un réseau hautement fiable et performant. Les solutions SD-WAN prennent en charge le basculement automatique via tous les chemins disponibles, ainsi que des fonctionnalités de surveillance et d'observabilité supplémentaires dans un seul volet de gestion. L'utilisation intensive de la configuration automatique et de l'automatisation permet un provisionnement et une visibilité rapides par rapport aux réseaux WAN traditionnels. Toutefois, l'utilisation de tunnels et de surcoûts de chiffrement n'est pas comparable à celle des liaisons fibre optique haut débit dédiées utilisées dans le cadre de la connectivité privée.

Dans certains cas, vous pouvez choisir d'utiliser un appareil virtuel doté d'une fonctionnalité VPN. Les raisons du choix d'une appliance virtuelle autogérée incluent les fonctionnalités techniques et la compatibilité avec le reste de votre réseau. Lorsque vous sélectionnez un VPN autogéré ou une solution SD-WAN qui utilise une appliance virtuelle déployée dans une instance EC2, vous êtes responsable de la gestion de cette appliance. Vous êtes également responsable de la haute disponibilité et du basculement entre les dispositifs virtuels. Une telle conception accroît votre responsabilité opérationnelle, mais elle pourrait vous apporter plus de flexibilité. Les fonctionnalités et capacités de la solution dépendent de l'appliance virtuelle que vous sélectionnez.

AWS Marketplace contient de nombreux dispositifs virtuels VPN que les clients peuvent déployer sur Amazon EC2. AWS recommande de commencer par un VPN S2S AWS géré et d'envisager d'autres

options s'il ne répond pas à vos besoins. Les frais de gestion des appareils virtuels sont à la charge du client.

Exemple de cas d'utilisation automobile chez Example Corp.

Cette section du livre blanc explique comment les considérations, les questions de définition des exigences et les arbres de décision sont utilisés pour vous aider à choisir la conception optimale du réseau hybride. Il est important d'identifier et de saisir les exigences, car elles sont utilisées comme entrée dans les arbres de décision. La saisie des exigences dès le départ permet d'éviter de nouvelles itérations de conception. L'interruption complète d'un projet si la conception doit être revue et la mise en attente de ressources précieuses peuvent être minimisées et, idéalement, évitées lorsque les exigences sont comprises dès le départ.

Example Corp. Automotive sera utilisé tout au long de cette section en tant que client indicatif. Ils cherchent à déployer dans un premier temps leur premier projet d'analyse surAWS. Le projet d'analyse est axé sur l'analyse des données des voitures fabriquées par l'entreprise et d'autres ensembles de données qui existent déjà dans les centres de données de l'entreprise. Dans un premier temps, le groupe d'architecture de l'entreprise pense avoir besoin d'un Compte AWS Amazon VPC et de quelques sous-réseaux pour héberger les environnements de production et de développement. L'équipe du projet est impatiente de commencer et a demandé l'accès à l'environnement de développement dès que possible. Leur objectif est d'entrer en production dans trois mois.

Example Corp. Automotive prévoit également de l'utiliser AWS pour plusieurs autres projets, tels que la migration de ses systèmes ERP, de son infrastructure de bureau virtuel (VDI) et de 20 autres applications depuis ses installations sur site au AWS cours des 6 prochains mois. Certaines exigences relatives à des projets supplémentaires sont encore en cours de définition, mais il est clair que leur AWS Cloud utilisation va augmenter.

L'équipe d'architecture a décidé de tirer parti de l'approche décrite dans ce livre blanc. Ils ont utilisé les questions de définition des exigences décrites sous chaque considération pour saisir les entrées nécessaires à la prise de décisions de conception.

Ils commencent par les exigences liées au type de connectivité, qui sont résumées dans le tableau suivant.

Tableau 4 — Exemples d'entrées de fiabilité d'Automotive Corp

Considérations relatives au choix du type de connectivité	Questions relatives à la définition des exigences	Réponses
Il est temps de déployer	Quel est le calendrier requis pour le déploiement ? Des heures, des jours, des semaines ou des mois ?	• Développement/Test : 1 mois • Production : 3 mois
Sécurité	Vos exigences et politiques de sécurité autorisent-elles l'utilisation de connexions chiffrées sur Internet pour vous connecter AWS ou imposent-elles l'utilisation de connexions à un réseau privé ?	• Développement/Test : VPN de site à site acceptable • Production : réseau privé requis
	Lorsque vous utilisez des connexions réseau privées, la couche réseau doit-elle fournir un chiffrement en transit ?	Non, le chiffrement de la couche application sera utilisé.
SLA	Un contrat de niveau de service de connectivité hybride assorti de crédits de service est-il requis ?	• Développement/Test : Non • Production : Oui
	Quel est l'objectif de disponibilité ?	• Développement/Test : N/A • Production : 99,99 %
	L'ensemble du réseau hybride respecte-t-il l'objectif de disponibilité ?	• Développement/Test : N/A • Production : Oui
Performances	Quel est le débit requis ?	• Développement/Test : 100 Mbits/s

Considérations relatives au choix du type de connectivité	Questions relatives à la définition des exigences	Réponses
		• Production : 500 Mbits/s, passant à 2 Gbit/s
	Quelle est la latence maximale acceptable entre un réseau local AWS et un réseau local ?	• Développement/Test : aucune exigence stricte • Production : moins de 30 ms
	Quelle est la gigue maximale acceptable sur le réseau ?	• Développement/Test : aucune exigence stricte • Production : instabilité minimale requise
Coût	À quelle quantité de données enverriez-vous AWS par mois ?	• Développement/Test : 2 To • Production : 20 To, passant à 50 To
	À partir de quelle quantité de données enverriez-vous AWS par mois ?	• Développement/Test : 1 To • Production : 10 To, passant à 25 To
	Cette connectivité est-elle permanente ?	Oui

Sur la base des exigences reçues, l'équipe d'architecture a suivi l'arbre de décision relatif au type de connectivité illustré à la figure 9. Cela a permis à l'équipe d'architecture de décider du type de connectivité pour les environnements de développement, de test et de production. En ce qui concerne l'environnement de production, ils ont pris en compte les exigences immédiates et à venir. Pour le développement et les tests, Example Corp. Automotive établira un site-to-site VPN sur Internet. Pour la production, ils travailleront avec un fournisseur de services auquel ils connecteront leur réseau d'entrepriseAWS Direct Connect. Example Corp. Automotive a initialement envisagé d'utiliser une connexion hébergée Direct Connect, mais en raison des exigences d'un SLA AWS fourni, elle a sélectionné Direct Connect Dedicated Connections.

Après avoir choisi le type de connectivité, l'étape suivante consiste à identifier les exigences qui ont une incidence sur le choix de la conception de connectivité. Cela est lié à la conception logique, notamment à la manière dont les connexions sont configurées et AWS aux services à utiliser pour répondre aux exigences commerciales et techniques.

Pour saisir les exigences en matière d'évolutivité et de modèle de communication, l'équipe d'architecture a utilisé les questions de définition des exigences figurant dans les sections associées de ce livre blanc. Les exigences liées à ces deux considérations sont résumées dans le tableau suivant.

Tableau 5 — Questions relatives à la définition des exigences

Considérations relatives au choix du design de connectivité	Questions relatives à la définition des exigences	Réponses
Scalabilité	Quel est le nombre actuel ou prévu de VPC nécessitant une connectivité à des sites sur site ?	2 au départ, passant à 30 en 6 mois
	Ces VPC sont-ils déployés dans une Région AWS ou plusieurs régions ?	Région unique
	À combien de sites locaux faut-il se connecter ? AWS	2 centres de données
	Combien de dispositifs de passerelle client avez-vous, par site, auxquels vous devez vous connecter AWS ?	2 routeurs par centre de données
	Combien de routes devraient être annoncées aux AWS VPC ainsi que le nombre de routes attendues depuis le côté ? AWS	• Itinéraires vers lesquels la publicité sera faite AWS : 20 itinéraires

Considérations relatives au choix du design de connectivité	Questions relatives à la définition des exigences	Réponses
		• Itinéraires à partir desquels vous souhaitez recevoir AWS : 1 /16 itinéraire
	Est-il prévu d'envisager une augmentation de la bande passante de la connexion AWS dans un futur proche ?	• Développement/Test : 100 Mbits/s • Production : 500 Mbps, passant à 2 Gbit/s.
Modèles de conception de connectivité	L'activation de la communication entre VPC est-elle obligatoire (au sein d'une région et/ou entre régions) ?	Oui, dans un Région AWS
	Est-il obligatoire d'accéder aux services de points de terminaison AWS publics directement depuis les locaux ?	Oui
	Est-il nécessaire d'accéder aux AWS services à l'aide de points de terminaison VPC sur site ?	Non

Sur la base des contributions, l'équipe d'architecture a suivi l'arbre de décision de la section Conception de la connectivité. Après avoir prévu que le nombre de VPC passerait de 2 à 30 au cours des 6 prochains mois, l'équipe d'architecture a décidé de les utiliser AWS Transit Gateway comme passerelle de terminaison pour la connexion et pour le routage inter-VPC. Independent AWS Transit Gateway s mettra fin à la connexion VPN utilisée pour le développement et les tests, ainsi que pour la connectivité de production avecAWS Direct Connect. L'utilisation de AWS Transit Gateway s séparés simplifie la gestion des modifications et fournit une démarcation claire entre les environnements de développement/test et de production. Pour la production, une AWS Direct Connect passerelle est

requise en raison deAWS Transit Gateway. Un VIF public sera utilisé pour accéder aux services de point de terminaison AWS publics. La figure 14 illustre le chemin emprunté dans l'arbre de décision en fonction des exigences collectées.

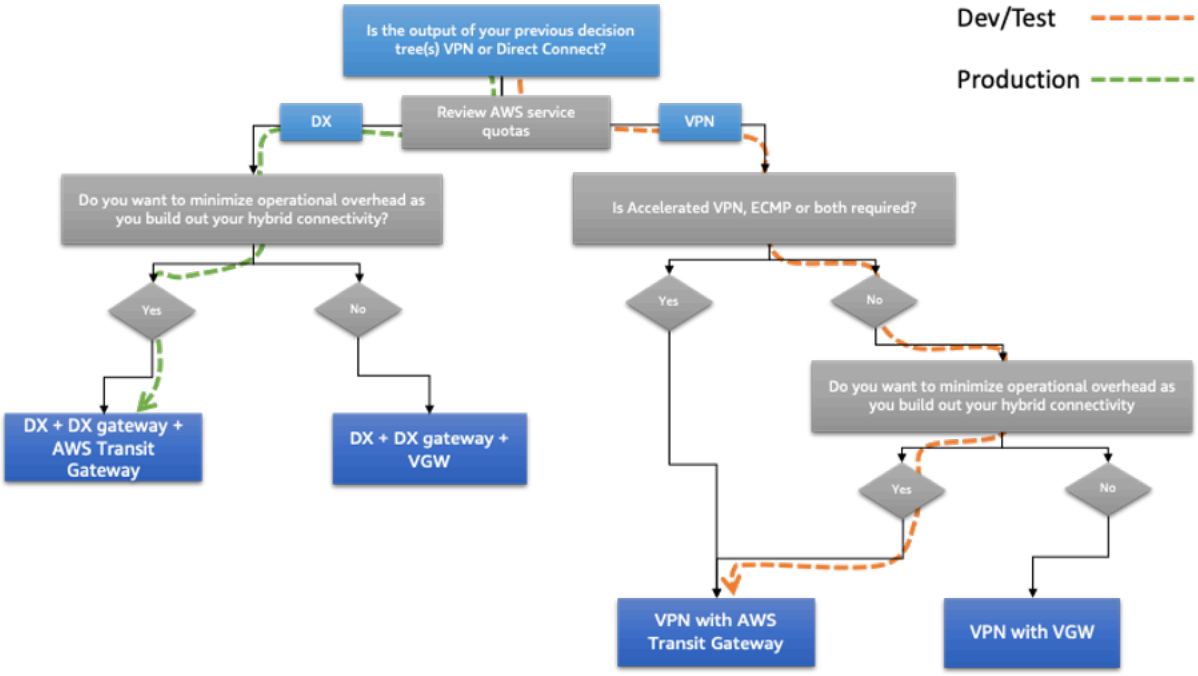

Figure 14 — Arbre décisionnel relatif à la conception des connexions automobiles de Example Corp.

Après avoir choisi la solution répondant aux exigences d'évolutivité et de modèle de communication, l'étape suivante consiste à identifier les exigences associées à la fiabilité. Cela est lié au niveau de disponibilité et de résilience requis.

Pour définir les exigences de fiabilité, l'équipe d'architecture a utilisé les questions de définition des exigences figurant dans la section associée de ce livre blanc. Les exigences sont résumées dans le tableau suivant.

Tableau 6 — Questions relatives aux exigences de fiabilité

Considérations relatives au choix du design de connectivité	Questions relatives à la définition des exigences	Réponses
Fiabilité	Quelle est l'ampleur de l'impact sur l'entreprise en	• Développement/Test : faible • Production : élevée

Considérations relatives au choix du design de connectivité	Questions relatives à la définition des exigences	Réponses
	cas de panne de connectivité AWS ?	
	D'un point de vue commercial, le coût lié à une panne de connectivité est-il supérieur au AWS coût du déploiement d'un modèle de connectivité hautement fiable pour ? AWS	• Développement/Test : Non • Production : Oui

Sur la base des contributions reçues, l'équipe chargée de l'architecture a suivi l'arbre décisionnel décrit dans les sections sur les considérations de fiabilité abordées précédemment dans ce livre blanc. Après avoir pris en compte l'objectif de disponibilité de 99,99 % pour la connectivité de production et l'impact commercial élevé en cas d'interruption de service, l'équipe d'architecture a décidé d'utiliser 2 sites Direct Connect et de disposer de 2 liens entre chaque centre de données sur site et chaque site Direct Connect (4 liens au total). La connectivité VPN utilisée pour le développement et les tests utilisera également deux connexions VPN pour une redondance supplémentaire. À l'aide des techniques d'ingénierie des routes décrites dans la section sur la fiabilité, la connectivité sera configurée comme suit :

- Pour le développement et les tests, le trafic sera équilibré à l'aide de l'ECMP sur les 2 tunnels destinés au centre de données principal. Cela permet un débit plus élevé. Les tunnels destinés au centre de données secondaire seront utilisés en cas de défaillance des tunnels principaux.
- Pour la production, la latence entre les sites sur site et AWS sur l'un ou l'autre des sites Direct Connect est très similaire. Dans ce cas, il a été décidé d'équilibrer la charge du trafic entre AWS et sur site sur les deux connexions destinées au centre de données principal pour les systèmes sur site déployés dans le centre de données principal. De même, pour les systèmes sur site exécutés dans le centre de données secondaire, le trafic sera équilibré entre les deux connexions au centre de données secondaire. En cas d'échec des connexions, le BGP facilitera un basculement automatique.

La figure 15 illustre le chemin emprunté dans l'arbre de décision en fonction des exigences collectées.

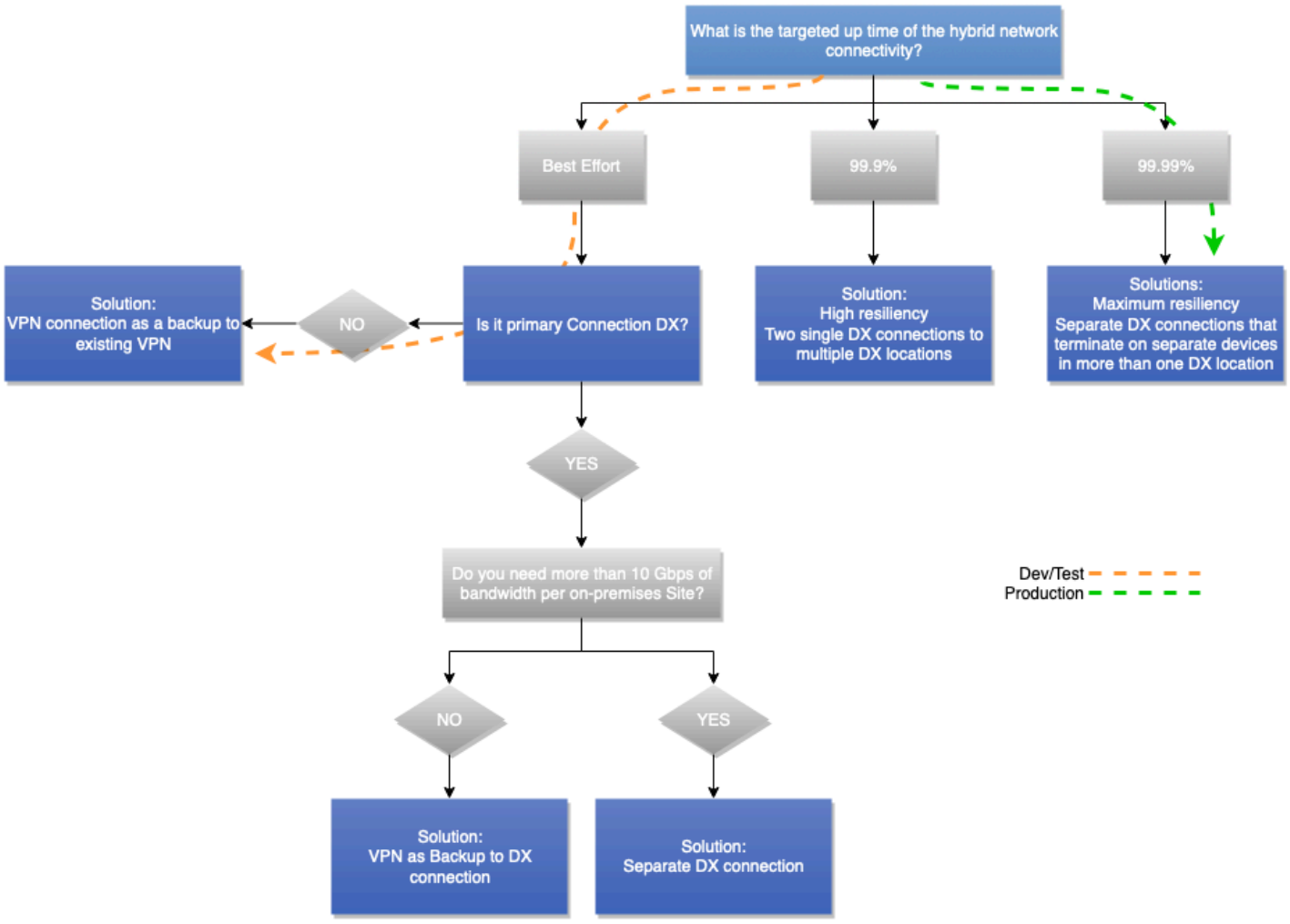

Figure 15 — Arbre décisionnel relatif à la fiabilité du secteur automobile d'Example Corp.

Architecture sélectionnée par Example Corp. Automotive

Le schéma suivant illustre l'architecture sélectionnée par Example Corp. Automotive après avoir collecté les exigences et parcouru les arbres de décision décrits dans les sections précédentes de ce livre blanc.

Il utilise le VPN AWS S2S sur Internet et se termine AWS Transit Gateway pour le développement et les tests. Il utilise ensuite AWS Direct Connect la passerelle Direct Connect et une seconde AWS Transit Gateway pour le trafic de production. AWS Transit Gatewayest utilisé pour le routage inter-VPC. Du point de vue du chemin de données, les tunnels VPN du centre de données principal sont

utilisés comme chemins principaux pour le développement et les tests, tandis que les tunnels menant au centre de données secondaire sont utilisés comme chemins de basculement. Pour le trafic de production, toutes les connexions sont utilisées simultanément. Le trafic en provenance AWS préfère la connexion réseau la plus optionnelle en fonction du centre de données dans lequel se trouve le système sur site. Example Corp. Automotive utilise des techniques d'ingénierie d'itinéraires similaires pour préférer le chemin approprié lorsque le trafic est envoyé, afin de AWS garantir l'utilisation de trajectoires de trafic symétriques afin de minimiser l'utilisation du réseau d'entreprise entre les centres de données principaux et secondaires sur site.

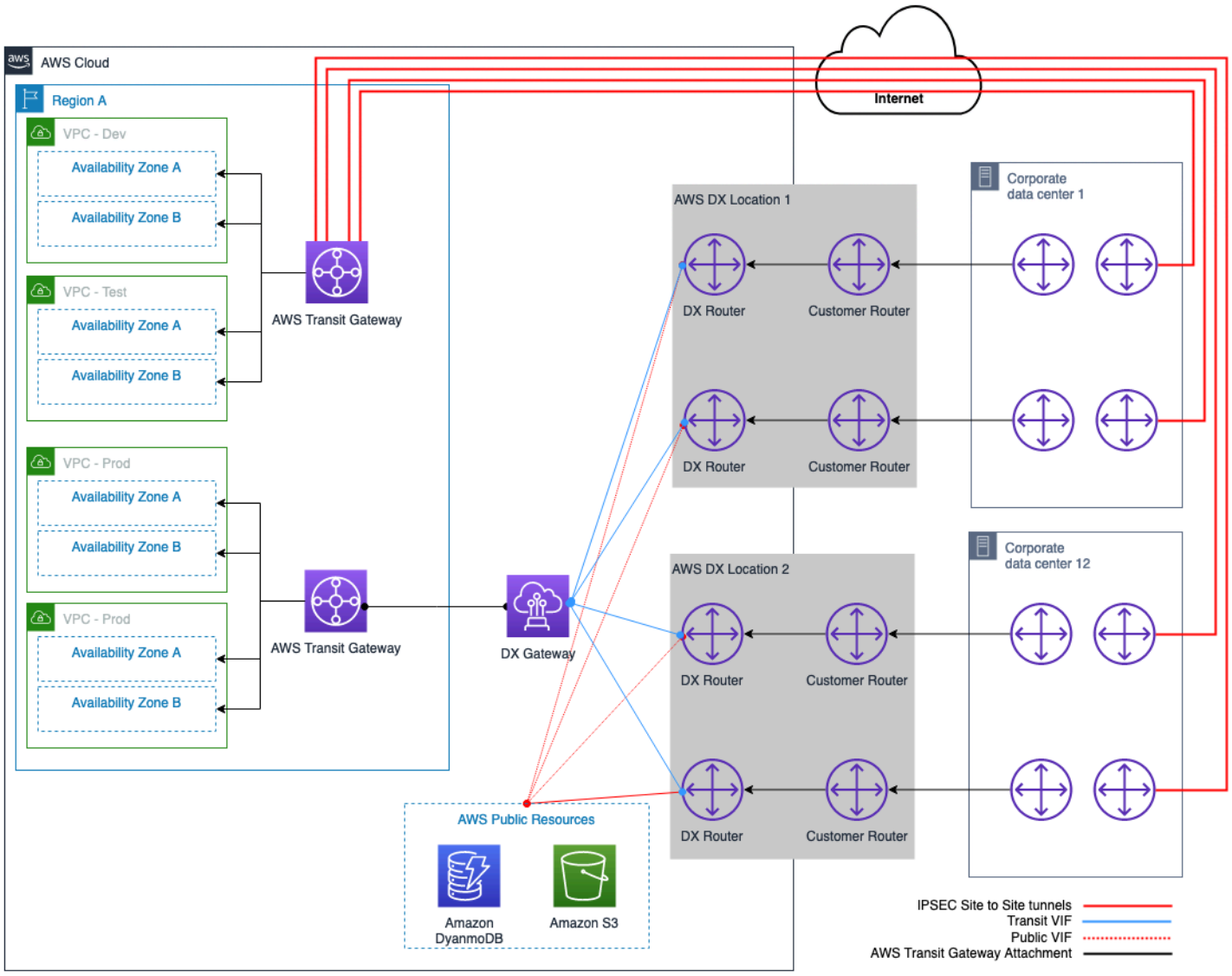

Figure 16 — Example Corp. Automotive a sélectionné le modèle de connectivité hybride

Conclusion

Un modèle de connectivité hybride est l'un des points de départ fondamentaux pour l'adoption du cloud computing. Un réseau hybride peut être construit avec une architecture optimale en suivant le processus de sélection du modèle de connectivité décrit dans ce livre blanc.

Le processus consiste en des considérations classées dans un ordre logique. L'ordre ressemble beaucoup à un modèle mental suivi par un réseau chevronné et des architectes cloud. Au sein de chaque groupe de considérations, les arbres de décision permettent de sélectionner rapidement un modèle de connectivité, même avec des exigences d'entrée limitées. Vous constaterez peut-être que certaines considérations et les impacts correspondants pointent vers des solutions différentes. Dans ces cas, en tant que décideur, vous devrez peut-être faire des compromis sur certaines exigences et sélectionner la solution la plus optimale qui répond à vos exigences commerciales et techniques.

Collaborateurs

Les contributeurs à ce document incluent :

- James Devine, architecte de solutions principal, Amazon Web Services
- Andrew Gray, architecte de solutions principal, réseau, Amazon Web Services
- Maks Khomutskyi, architecte de solutions senior, Amazon Web Services
- Marwan Al Shawi, architecte de solutions, Amazon Web Services
- Santiago Freitas, responsable de la technologie, Amazon Web Services
- Evgeny Vaganov, architecte de solutions spécialisé dans les réseaux, Amazon Web Services
- Tom Adamski, architecte de solutions spécialisé dans les réseaux, Amazon Web Services
- Armstrong Onaiwu, architecte de solutions, Amazon Web Services

Suggestions de lecture

- Création d'une infrastructure réseau AWS multi-VPC évolutive et sécurisée
- Options DNS dans le cloud hybride pour Amazon VPC
- Amazon Virtual Private Cloud Connectivity Options
- Amazon Virtual Private Cloud Documentation
- Documentation AWS Direct Connect
- Quelle est la différence entre une interface virtuelle hébergée (VIF) et une connexion hébergée ?

Révisions du document

Pour recevoir les notifications des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

Modification	Description	Date
Mise à jour mineure	Mis à jour pour refléter l'augmentation de la limite de quota DX.	10 juillet 2023
Mise à jour majeure	Mis à jour pour intégrer les meilleures pratiques, services et fonctionnalités les plus récents.	6 juillet 2023
Mise à jour mineure	Diagrammes d'architecture de référence mis à jour pour refléter les modifications du quota DX.	27 juin 2023
Mise à jour mineure	Corrige les liens brisés.	22 mars 2022
Publication initiale	Livre blanc publié pour la première fois	22 septembre 2020

Avis

Les clients sont tenus de réaliser leur propre évaluation indépendante des informations contenues dans ce document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWSles produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.