Livre blanc AWS

Création d'une infrastructure réseau AWS à plusieurs VPC évolutive et sécurisée

Création d'une infrastructure réseau AWS à plusieurs VPC évolutive et sécurisée: Livre blanc AWS

Table of Contents

Création d'une infrastructure réseau AWS à plusieurs VPC évolutive et sécurisée

Date de publication : 10 juin 2020 (Historique du document)

Résumé

Les clients AWS comptent souvent sur des centaines de comptes et de VPC pour segmenter leurs charges de travail et étendre leur couverture. L'étendue de la couverture entraîne souvent des défis en matière de partage des ressources, de connectivité inter-VPC et de connectivité pour le trafic sur site vers VPC.

Ce livre blanc décrit les bonnes pratiques pour créer des architectures réseau évolutives et sécurisées dans un grand réseau à l'aide de services AWS tels qu'Amazon VPC, AWS Transit Gateway, AWS PrivateLink et AWS Direct Connect Gateway. Il présente des solutions pour gérer une infrastructure croissante en garantissant la capacité de mise à l'échelle, la haute disponibilité et la sécurité tout en maintenant les coûts à un niveau bas.

Introduction

Les clients AWS commencent par créer des ressources dans un seul compte AWS représentant une limite de gestion qui segmente les autorisations, les coûts et les services. Cependant, au fur et à mesure que l'organisation du client se développe, une plus grande segmentation des services devient nécessaire pour surveiller les coûts, contrôler l'accès et faciliter la gestion de l'environnement. Une solution multi-comptes résout ces problèmes en fournissant des comptes spécifiques pour les services informatiques et les utilisateurs au sein d'une organisation. AWS fournit plusieurs outils pour gérer et configurer cette infrastructure, notamment AWS Landing Zone et AWS Control Tower.

Figure 1 – Structure du compte Landing Zone

AWS Landing Zone et AWS Control Tower automatisent la configuration et l'intégration de plusieurs services AWS afin de fournir un environnement multi-comptes de base hautement contrôlé avec Identity and Access Management (IAM), gouvernance, sécurité des données, conception du réseau et journalisation.

La solution AWS Landing Zone de la Figure 1 comprend quatre comptes : le compte AWS Organizations (utilisé pour gérer la configuration et l'accès aux comptes gérés AWS Landing Zone), le compte de services partagés (utilisé pour créer des services partagés d'infrastructure tels que les services d'annuaire), le compte d'archivage des journaux (connexion centralisée dans des compartiments S3) et le compte de sécurité (utilisé par l'équipe de sécurité et de conformité d'une entreprise pour auditer ou effectuer des opérations de sécurité d'urgence en cas d'incident dans les comptes en étoile).

Ce livre blanc présente un compte de services réseau détenu par l'équipe réseau qui gère votre infrastructure AWS. Les services réseau et l'infrastructure réseau du compte sont partagés par l'ensemble des comptes et des VPC de manière centralisée (similaire à un réseau en étoile). Cette conception permet une meilleure gestion de votre zone de destination et contribue à réduire les coûts, car il n'est pas nécessaire de dupliquer les services réseau dans chaque VPC en étoile et dans chaque compte.

> **Note**
>
> Dans ce livre blanc, « zone de destination » est un terme générique désignant la configuration multi-comptes/multi-VPC évolutive, sécurisée et performante dans laquelle vous

déployez vos charges de travail. Cette configuration peut être créée à l'aide de n'importe quel outil.

La plupart des clients commencent par déployer leur infrastructure avec quelques VPC seulement. Le nombre de VPC qu'un client possède est généralement lié au nombre de comptes, d'utilisateurs et d'environnements intermédiaires (production, développement, test, etc.). À mesure que l'utilisation du cloud augmente, le nombre d'utilisateurs, d'unités commerciales, d'applications et de régions avec lesquels un client interagit se multiplie, ce qui entraîne la création de nouveaux VPC.

À mesure que le nombre de VPC augmente, la gestion entre VPC devient essentielle au fonctionnement du réseau cloud du client. Ce livre blanc aborde les bonnes pratiques dans trois domaines spécifiques de la connectivité hybride et entre VPC :

- Connectivité réseau : interconnexion de VPC et de réseaux sur site à grande échelle.
- Sécurité du réseau : création de points de sortie centralisés pour accéder à Internet et aux points de terminaison tels que la passerelle NAT, les points de terminaison VPC et AWS PrivateLink.
- Gestion du DNS : résolution du DNS dans la zone de destination et du DNS hybride.

Connectivité VPC à VPC

Les clients peuvent utiliser deux modèles de flux VPC différents pour configurer des environnements à plusieurs VPC : plusieurs-à-plusieurs ou en étoile. Dans l'approche plusieurs-à-plusieurs, le trafic entre chaque VPC est géré individuellement entre chaque VPC. Dans le modèle en étoile, l'ensemble du trafic entre les VPC passe par une ressource centrale, qui achemine le trafic selon des règles établies.

Rubriques

Appairage de VPC

Le moyen le plus simple de connecter deux VPC consiste à utiliser l'appairage de VPC. Dans cette configuration, une connexion permet une connectivité bidirectionnelle complète entre les VPC. Cette connexion d'appairage est utilisée pour acheminer le trafic entre les VPC. Les VPC entre différents comptes et régions AWS peuvent également être appairés ensemble. L'appairage de VPC n'entraîne que des coûts pour le trafic transitant par la connexion (il n'y a pas de frais d'infrastructure horaires).

L'appairage de VPC est une connectivité point à point et ne prend pas en charge le routage transitif. Par exemple, si vous avez une connexion d'appairage de VPC entre le VPC A et le VPC B, et entre le VPC A et le VPC C, une instance du VPC B ne peut pas transiter par le VPC A pour atteindre le VPC C. Pour acheminer des paquets entre le VPC B et le VPC C, vous devez créer une connexion directe d'appairage de VPC.

À grande échelle, lorsque vous avez de 10 à 100 VPC, leur interconnexion avec l'appairage entraîne un maillage de 100 à 1 000 connexions d'appairage, qui sont difficiles à gérer et à mettre à l'échelle. Il existe une limite maximale de 125 connexions d'appairage par VPC.

Figure 2 – Configuration réseau à l'aide de l'appairage de VPC

Si vous utilisez l'appairage de VPC, une connectivité sur site (VPN et/ou Direct Connect) doit être établie sur chaque VPC. Les ressources d'un VPC ne peuvent pas atteindre celles sur site à l'aide de la connectivité hybride d'un VPC appairé (Figure 2).

Il est préférable d'utiliser l'appairage de VPC lorsque les ressources d'un VPC doivent communiquer avec les ressources d'un autre VPC, que l'environnement des deux VPC est contrôlé et sécurisé et que le nombre de VPC à connecter est inférieur à 10 (pour permettre la gestion individuelle de chaque connexion). L'appairage de VPC offre le coût global le plus faible par rapport aux autres options de connectivité entre VPC.

Solution VPC de transit

Les VPC de transit peuvent résoudre certaines des lacunes de l'appairage de VPC en introduisant une conception en étoile pour la connectivité entre VPC. Dans un réseau VPC de transit, un VPC central (le VPC hub) se connecte à tous les autres VPC (VPC en étoile) via une connexion VPN utilisant généralement le BGP sur IPsec. Le VPC central contient des instances EC2 exécutant des appliances logicielles qui acheminent le trafic entrant vers leurs destinations à l'aide de la superposition VPN (Figure 3). L'appairage de VPC de transit présente les avantages suivants :

- Le routage transitif est activé à l'aide du réseau VPN superposé, ce qui permet une conception en étoile plus simple.
- Lors de l'utilisation d'un logiciel fournisseur tiers sur l'instance EC2 dans le VPC de transit hub, les fonctionnalités du fournisseur relatives à la sécurité avancée (pare-feu de couche 7/IPS/IDS) peuvent être exploitées. Si les clients utilisent le même logiciel sur site, ils bénéficient d'une expérience opérationnelle et de surveillance unifiée.

Figure 3 – VPC de transit avec CSR Cisco

Le VPC de transit présente ses propres défis, tels que des coûts d'exécution plus élevés pour les appliances virtuelles, un débit limité par VPC (jusqu'à 1,25 Gbit/s par tunnel VPN) et des frais de configuration et de gestion supplémentaires (les clients doivent gérer la disponibilité et la redondance des instances EC2).

Passerelle de transit

AWS Transit Gateway fournit une conception en étoile pour connecter des VPC et des réseaux sur site en tant que service entièrement géré sans que vous ayez à allouer des appliances virtuelles tels que les CSR Cisco. Aucune superposition VPN n'est requise, et AWS gère la haute disponibilité et la capacité de mise à l'échelle.

Transit Gateway permet aux clients de connecter des milliers de VPC. Vous pouvez attacher l'ensemble de votre connectivité hybride (connexions VPN et Direct Connect) à une seule passerelle Transit Gateway. Vous consolidez et contrôlez ainsi l'ensemble de la configuration de routage AWS de votre organisation en un seul endroit (Figure 4). Transit Gateway contrôle la façon dont le trafic est acheminé entre tous les réseaux en étoile connectés à l'aide de tables de routage. Ce modèle en étoile simplifie la gestion et réduit les coûts opérationnels, car les VPC ne se connectent qu'à la passerelle Transit Gateway pour accéder aux réseaux connectés.

Figure 4 – Conception en étoile avec AWS Transit Gateway

Transit Gateway est une ressource régionale qui peut connecter des milliers de VPC au sein d'une même région AWS. Vous pouvez créer plusieurs passerelles de transit par région, mais les passerelles Transit Gateway au sein d'une région AWS ne peuvent pas être appairées, et vous pouvez vous connecter à un maximum de trois passerelles de transit sur une seule connexion Direct Connect pour une connectivité hybride. Pour ces raisons, vous devez limiter votre architecture à une seule passerelle Transit Gateway connectant tous vos VPC dans une région donnée, et utiliser des tables de routage Transit Gateway pour les isoler là où cela s'avère nécessaire. Il existe un cas pour lequel il est nécessaire de créer plusieurs passerelles Transit Gateway uniquement pour limiter le rayon d'impact d'une mauvaise configuration.

Placez la passerelle Transit Gateway de votre organisation dans son compte de services réseau. Elle peut ainsi être gérée de manière centralisée par les ingénieurs réseau qui gèrent le compte de services réseau. Utilisez AWS Resource Access Manager (RAM) pour partager une passerelle Transit Gateway afin de connecter des VPC sur plusieurs comptes de votre organisation AWS au sein de la même région. AWS RAM vous permet de partager facilement et en toute sécurité des ressources AWS avec n'importe quel compte AWS ou au sein de votre organisation AWS. Pour de plus amples informations, veuillez consulter le billet de blog Automating AWS Transit Gateway attachments to a transit gateway in a central account.

Rubriques

Transit Gateway et VPC de transit

Transit Gateway offre de nombreux avantages par rapport à une solution VPC de transit :

- Transit Gateway élimine la complexité de la maintenance des connexions VPN avec des centaines de VPC.
- Transit Gateway supprime la nécessité de gérer et de mettre à l'échelle des appliances logicielles basées sur EC2. AWS est responsable de la gestion de toutes les ressources nécessaires pour acheminer le trafic.
- Transit Gateway supprime la nécessité de gérer la haute disponibilité en fournissant une infrastructure multi-AZ hautement disponible et redondante.
- Transit Gateway améliore la bande passante pour les communications inter-VPC à des vitesses de rafale de 50 Gbit/s par zone de disponibilité.
- Transit Gateway rationalise les coûts d'utilisation selon un modèle simple par heure et par Go transféré.
- Transit Gateway réduit la latence en supprimant les proxys EC2 et le besoin d'encapsulation VPN.

Transit Gateway et appairage de VPC

Transit Gateway résout la complexité liée à la création et à la gestion de plusieurs connexions d'appairage de VPC à grande échelle. Ces avantages font de Transit Gateway un bon choix par défaut pour la plupart des architectures réseau. Cependant, l'appairage de VPC reste un choix pertinent, car il offre les avantages suivants, contrairement à Transit Gateway :

- Faible coût : avec l'appairage de VPC, vous ne payez que les frais de transfert de données. Transit Gateway facture des frais horaires par attachement en plus des frais de transfert de données.
- Aucune limite de bande passante : avec Transit Gateway, la bande passante maximale (rafale) par connexion VPC est de 50 Gbit/s. L'appairage de VPC ne comporte aucune bande passante globale. Les limites de performances du réseau d'instance individuelle et les limites de débit (10 Gbit/s au sein d'un groupe de placement et 5 Gbit/s dans les autres cas) s'appliquent aux deux options. Seul l'appairage de VPC prend en charge les groupes de placement.

- Latence : contrairement à l'appairage de VPC, Transit Gateway est un saut supplémentaire entre les VPC.
- Compatibilité des groupes de sécurité : le référencement des groupes de sécurité fonctionne avec l'appairage de VPC au sein d'une région. Actuellement cela ne fonctionne pas avec Transit Gateway.

Dans la configuration de votre zone de destination, l'appairage de VPC peut être utilisé en combinaison avec le modèle en étoile activé par Transit Gateway.

AWS PrivateLink

Les clients peuvent souhaiter exposer en privé un service/une application résidant dans un VPC (fournisseur de services) à d'autres VPC consommateurs au sein d'une région AWS de telle sorte que seuls les VPC consommateurs initient des connexions au VPC du fournisseur de services. La capacité de vos applications privées à accéder aux API des fournisseurs de services en est un exemple.

Pour utiliser AWS PrivateLink, créez un équilibreur Network Load Balancer pour votre application dans votre VPC et créez une configuration de service de point de terminaison d'un VPC pointant vers cet équilibreur de charge. Un consommateur de service crée ensuite un point de terminaison d'interface pour votre service. Une interface réseau Elastic est ainsi créée dans votre sous-réseau avec une adresse IP privée qui sert de point d'entrée au trafic destiné au service. Le consommateur et le service ne doivent pas obligatoirement se trouver dans le même VPC. Si le VPC est différent, les VPC du consommateur et du fournisseur de services peuvent avoir des plages d'adresses IP qui se chevauchent. Outre la création du point de terminaison d'un VPC d'interface pour accéder aux services d'autres VPC, vous pouvez créer des points de terminaison d'un VPC d'interface pour accéder en privé aux services AWS pris en charge via AWS PrivateLink (Figure 5).

Figure 5 – AWS PrivateLink

Le choix entre Transit Gateway, l'appairage de VPC et AWS PrivateLink dépend de la connectivité.

AWS PrivateLink : utilisez AWS PrivateLink lorsque vous avez configuré un client/serveur dans lequel vous souhaitez autoriser un ou plusieurs VPC consommateurs à accéder de manière unidirectionnelle à un service spécifique ou à un ensemble d'instances spécifique dans le VPC du fournisseur de services. Seuls les clients du VPC consommateur peuvent initier une connexion

au service dans le VPC du fournisseur de services. Cette solution constitue également une option appropriée lorsque le client et les serveurs des deux VPC ont des adresses IP qui se chevauchent, car AWS PrivateLink tire parti des ENI au sein du VPC client de telle sorte qu'il n'y ait aucun conflit d'adresses IP avec le fournisseur de services. Vous pouvez accéder aux points de terminaison AWS PrivateLink via l'appairage de VPC, le VPN et AWS Direct Connect.

Appairage de VPC et Transit Gateway : utilisez l'appairage de VPC et Transit Gateway lorsque vous souhaitez activer la connectivité IP de couche 3 entre les VPC.

Votre architecture contiendra un mélange de ces technologies afin de répondre à différents cas d'utilisation. Tous ces services peuvent être combinés et fonctionner les uns avec les autres. Par exemple, AWS PrivateLink pour gérer la connectivité client-serveur de style API, l'appairage de VPC pour gérer les exigences de connectivité directe lorsque des groupes de placement peuvent être nécessaires dans la région ou lorsque la connectivité inter-région est nécessaire, et Transit Gateway pour simplifier la connectivité des VPC à grande échelle ainsi que la consolidation en périphérie pour une connectivité hybride.

Partage de VPC Amazon

Le partage de VPC est utile lorsque l'isolation réseau entre les équipes n'a pas besoin d'être strictement gérée par le propriétaire du VPC, mais que les utilisateurs et les autorisations au niveau du compte doivent l'être. Avec un VPC partagé, plusieurs comptes AWS créent leurs ressources d'application (telles que des instances Amazon EC2) dans des VPC Amazon partagés et gérés de manière centralisée. Dans ce modèle, le compte qui détient le VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants). Une fois un sous-réseau partagé, les participants peuvent afficher, créer, modifier et supprimer leurs ressources d'application contenues dans les sous-réseaux partagés avec eux. Ils ne peuvent toutefois pas afficher, modifier ou supprimer des ressources appartenant à d'autres participants ou au propriétaire du VPC. La sécurité entre les ressources des VPC partagés est gérée à l'aide de groupes de sécurité et d'ACL réseau de sous-réseau.

Avantages du partage de VPC :

- Conception simplifiée : aucune complexité liée à la connectivité inter-VPC
- Nombre de VPC gérés moins important
- Séparation des tâches entre les équipes réseau et les propriétaires d'applications
- Meilleure utilisation des adresses IPv4

- Faibles coûts : aucun frais de transfert de données entre les instances appartenant à différents comptes au sein de la même zone de disponibilité

Remarque : Lorsque vous partagez un sous-réseau avec plusieurs comptes, vos participants doivent bénéficier d'un certain niveau de coopération puisqu'ils partagent l'espace IP et les ressources réseau. Si nécessaire, vous pouvez choisir de partager un sous-réseau différent pour chaque compte de participant. Un sous-réseau par participant permet à l'ACL réseau de fournir une isolation réseau en plus des groupes de sécurité.

La plupart des architectures client contiendront plusieurs VPC, dont beaucoup seront partagés avec plusieurs comptes. Transit Gateway et l'appairage de VPC peuvent être utilisés pour connecter les VPC partagés. Supposons, par exemple, que vous ayez 10 applications. Chaque application nécessite son propre compte AWS. Les applications peuvent être classées en deux portefeuilles d'applications (les applications d'un même portefeuille ont des exigences réseau similaires, par exemple les applications 1 à 5 dans le portefeuille « Marketing » et les applications 6 à 10 dans le portefeuille « Ventes »).

Vous pouvez avoir un VPC par portefeuille d'applications (deux VPC au total), et le VPC est partagé avec les différents comptes de propriétaires d'applications au sein de ce portefeuille. Les propriétaires d'applications déploient des applications dans leur VPC partagé respectif (dans ce cas, dans les différents sous-réseaux pour la segmentation et l'isolation des routes réseau à l'aide de listes de contrôle d'accès réseau (NACL). Les deux VPC partagés sont connectés via la passerelle Transit Gateway. Avec cette configuration, vous pourriez passer de 10 VPC à seulement 2 VPC (Figure 6).

Figure 6 – Exemple de configuration – VPC partagé

> **Note**
>
> Les participants au partage de VPC ne peuvent pas créer toutes les ressources AWS d'un sous-réseau partagé. Pour de plus amples informations, veuillez consulter Limitations Amazon VPC.

Connectivité hybride

Cette section est consacrée à la connexion sécurisée de vos ressources cloud à vos centres de données sur site. Il existe deux approches pour activer la connectivité hybride :

1. Connectivité individuelle : dans cette configuration, une connexion VPN et/ou une interface virtuelle privée Direct Connect est créée pour chaque VPC. Pour cela, il convient de tirer parti de la passerelle réseau privé virtuel. Cette option est idéale lorsque le nombre de VPC est restreint, mais à mesure qu'un client met à l'échelle ses VPC, la gestion de la connectivité hybride par VPC peut devenir difficile.
2. Consolidation Edge : dans cette configuration, les clients consolident la connectivité informatique hybride pour plusieurs VPC sur un seul point de terminaison. Tous les VPC partagent ces connexions hybrides. Pour cela, il convient de tirer parti d'AWS Transit Gateway et de Direct Connect Gateway.

Rubriques

- VPN
- Direct Connect

VPN

Figure 7 – Options de terminaison AWS VPN

Il existe trois façons de configurer un VPN sur AWS :

1. Consolider la connectivité VPN sur Transit Gateway : cette option tire parti du réseaux VPN de transit par passerelle sur Transit Gateway. Transit Gateway prend en charge la terminaison IPsec pour le Site-to-Site VPN. Les clients peuvent créer des tunnels VPN vers Transit Gateway et peuvent accéder aux VPC qui y sont attachés. Transit Gateway prend en charge les connexions VPN statiques et dynamiques basées sur BGP. Transit Gateway prend également en charge ECMP (routage multi-chemin à coût égal) sur les attachements VPN. Chaque connexion VPN a un débit maximal de 1,25 Gbit/s, et l'activation d'ECMP vous permet d'agréger le débit des différentes connexions VPN. Dans cette option, vous payez le tarif de Transit Gateway et celui de AWS VPN. Nous vous recommandons d'utiliser cette option pour la connectivité VPN. Pour de plus amples informations, veuillez consulter la Présentation AWS VPN.

2. Résilier le VPN sur une instance EC2 : cette option est utilisée par les clients dans les cas sensibles lorsqu'ils souhaitent un ensemble de fonctionnalités logicielles d'un fournisseur particulier (comme Cisco DMVPN ou GRE), ou lorsqu'ils souhaitent une cohérence opérationnelle entre les différents déploiements VPN. Vous pouvez tirer parti de la conception du VPC de transit pour la consolidation Edge, mais il est important de se rappeler que toutes les considérations clés de la section sur la connectivité VPC à VPC pour le VPC de transit s'appliquent à la connectivité VPN hybride. Vous êtes responsable de la gestion de la haute disponibilité et vous payez les coûts liés aux instances EC2 ainsi que les licences logicielles des fournisseurs.
3. Résilier le VPN sur une passerelle réseau privé virtuel : cette option permet une conception de connectivité individuelle dans laquelle vous créez une connexion VPN (composée d'une paire de tunnels VPN redondants) pour chaque VPC. Cet option constitue un excellent moyen de commencer à utiliser la connectivité VPN dans AWS. Cependant, à mesure que vous augmentez le nombre de VPC, la conception de la consolidation Edge utilisant Transit Gateway devrait finalement s'avérer être une meilleure option. Le débit VPN vers un VPC est limité à 1,25 Gbit/s et la répartition de charge ECMP n'est pas prise en charge. Du point de vue de la tarification, vous ne payez que pour AWS VPN. Aucuns frais ne s'appliquent à l'exploitation d'une passerelle réseau privé virtuel. Pour de plus amples informations, veuillez consulter Tarification AWS VPN et AWS VPN sur une passerelle réseau privé virtuel.

Direct Connect

Bien que le VPN sur Internet soit une excellente option dans un premier temps, la connectivité Internet peut ne pas être fiable pour le trafic de production. En raison de ce manque de fiabilité, de nombreux clients choisissent AWS Direct Connect, qui permet une connexion par fibre dédiée cohérente, à faible latence et à bande passante élevée entre les centres de données des clients et AWS. Il existe quatre manières de tirer parti de AWS Direct Connect pour se connecter à des VPC :

Figure 8 – Quatre façons de connecter vos centres de données sur site à la zone de destination

- Créer une interface virtuelle privée pour une passerelle réseau privé virtuel connectée à un VPC : vous pouvez créer 50 interfaces virtuelles privées par connexion Direct Connect, ce qui vous permet de vous connecter à un maximum de 50 VPC (une interface virtuelle privée fournit la connectivité à un VPC). Il existe un appairage BGP par VPC. Dans cette configuration, la connectivité est limitée à la région AWS dans laquelle l'emplacement Direct Connect est hébergé. Pour accéder aux VPC dans la zone de destination, cette méthode est rarement préférée, car le mappage de l'interface virtuelle au VPC est individuel et il n'y a pas d'accès global.

- Créer un interface virtuelle privée vers une passerelle Direct Connect associée à plusieurs passerelles réseau privé virtuel (chaque passerelle réseau privé virtuel est attachée à un VPC) : une passerelle Direct Connect peut se connecter à un maximum de 10 passerelles réseau privé virtuel dans le monde (à l'exception de la Chine) sur n'importe quel compte AWS. C'est une excellente option si une zone de destination se compose d'un petit nombre de VPC (dix VPC maximum) et/ou si vous avez besoin d'un accès global. Il existe un appairage BGP par passerelle Direct Connect par connexion Direct Connect. La passerelle Direct Connect est uniquement destinée au flux de trafic nord/sud et n'autorise pas la connectivité VPC à VPC.
- Créer une interface virtuelle de transit vers une passerelle Direct Connect associée à Transit Gateway : vous pouvez associer une passerelle Transit Gateway à une passerelle Direct Connect via une connexion Direct Connect dédiée ou hébergée s'exécutant à 1 Gbit/s ou plus. Cette option vous permet de connecter votre centre de données sur site à un maximum de trois passerelles Transit Gateway (qui peuvent se connecter à des milliers de VPC) sur différentes régions AWS et comptes AWS via une interface virtuelle et un appairage BGP. Il s'agit de la configuration la plus simple parmi les quatre options permettant de connecter plusieurs VPC à grande échelle, mais vous devez tenir compte des limites de Transit Gateway. L'une des principales limites est que vous ne pouvez publier que 20 plages d'adresses CIDR d'une passerelle Transit Gateway vers un routeur sur site via l'interface virtuelle de transit. Avec les options 1 et 2, vous payez le prix Direct Connect. Pour l'option 3, vous payez également les frais d'attachement et les frais de transfert de données Transit Gateway. Pour de plus amples informations, veuillez consulter la documentation Associations Transit Gateway sur Direct Connect.
- Créer une connexion VPN vers Transit Gateway via une passerelle virtuelle publique Direct Connect : une interface virtuelle publique vous permet d'accéder à tous les services publics et points de terminaison AWS à l'aide des adresses IP publiques. Lorsque vous créez un attachement VPN sur une passerelle Transit Gateway, vous obtenez deux adresses IP publiques pour la terminaison du VPN côté AWS. Ces adresses IP publiques sont accessibles via l'interface virtuelle publique. Vous pouvez créer autant de connexions VPN vers autant de passerelles Transit Gateway que vous le souhaitez via une interface virtuelle publique. Lorsque vous créez un appairage BGP via l'interface virtuelle publique, AWS annonce la totalité de la plage d'adresses IP publiques AWS à votre routeur. Il est conseillé d'utiliser un pare-feu sur site afin de garantir que vous n'autorisez qu'un certain trafic (par exemple, vous autorisez uniquement le trafic vers les points de terminaison VPN). Cette option peut être utilisée pour chiffrer votre passerelle Direct Connect au niveau de la couche réseau.

La troisième option (interface virtuelle de transit vers passerelle Direct Connect) peut sembler être la meilleure car elle vous permet de consolider l'ensemble de votre connectivité sur site pour

une région AWS donnée en un seul point (Transit Gateway) à l'aide d'une seule session BGP par connexion Direct Connect. Cependant, compte tenu de certaines des limites et considérations relatives à l'option 3, nous prévoyons que les clients tireront parti à la fois de l'option 2 et de l'option 3 pour répondre aux exigences de connectivité de leur zone de destination. La Figure 9 illustre un exemple de configuration dans lequel l'interface virtuelle de transit est utilisée comme méthode par défaut pour la connexion à des VPC, et une interface virtuelle privée est utilisée pour un cas d'utilisation sensible dans lequel une énorme quantité de données doit être transférée d'un contrôleur de domaine sur site vers le VPC multimédia. L'interface virtuelle privée est utilisée pour éviter les frais de transfert de données Transit Gateway. Il est recommandé d'avoir au moins deux connexions à deux emplacements Direct Connect différents pour profiter d'une redondance maximale, soit quatre connexions au total. Vous créez une interface virtuelle par connexion pour un total de quatre interfaces virtuelles privées et quatre interfaces virtuelles de transit. Vous créez également un VPN en tant que connectivité de secours aux connexions AWS Direct Connect.

Figure 9 – Exemple d'architecture de référence pour la connectivité hybride

Utilisez le compte de services réseau pour créer des ressources Direct Connect permettant la démarcation des limites administratives du réseau. La connexion Direct Connect, la passerelle Direct Connect et la passerelle Transit Gateway peuvent toutes résider dans un compte de services réseau. Pour partager la connectivité AWS Direct Connect avec votre zone de destination, partagez simplement la passerelle Transit Gateway via la RAM avec d'autres comptes.

Sortie centralisée vers Internet

Lorsque vous déployez des applications dans votre zone de destination, de nombreuses applications nécessitent un accès Internet sortant uniquement (par exemple, le téléchargement de bibliothèques/ de correctifs/de mises à jour du système d'exploitation). Pour cela, il est préférable d'utiliser une passerelle de traduction d'adresses réseau (NAT) ou une instance EC2 (configurée avec un NAT source (SNAT)) comme prochain saut pour tous les accès Internet de sortie. Les applications internes résident dans des sous-réseaux privés, tandis que la passerelle NAT/les instances NAT EC2 résident dans un sous-réseau public.

Utilisation de la passerelle NAT

Le déploiement d'une passerelle NAT dans chaque VPC en étoile peut devenir coûteux, car vous payez des frais horaires pour chaque passerelle NAT que vous déployez (veuillez consulter Tarification Amazon VPC). La centraliser représente donc une option viable. Pour centraliser, nous créons un VPC de sortie dans le compte de services réseau et acheminons l'ensemble du trafic sortant des VPC en étoile via une passerelle NAT située dans ce VPC tirant parti de Transit Gateway, comme illustré Figure 10.

Remarque : Lorsque vous centralisez la passerelle NAT à l'aide de Transit Gateway, vous payez des frais de traitement des données Transit Gateway supplémentaires, ce qui n'est pas le cas dans l'approche décentralisée consistant à exécuter une passerelle NAT dans chaque VPC. Dans certains cas sensibles, lorsque vous envoyez d'énormes quantités de données via la passerelle NAT à partir d'un VPC, il peut s'avérer plus rentable de conserver le NAT local dans le VPC pour éviter les frais de traitement des données Transit Gateway.

Figure 10 – Passerelle NAT centralisée utilisant Transit Gateway (vue d'ensemble)

Figure 11 – Passerelle NAT centralisée utilisant Transit Gateway (conception de table de routage)

Dans cette configuration, les attachements du VPC en étoile sont associés à la table de routage 1 (RT1) et sont propagés à la table de routage 2 (RT2). Nous avons explicitement ajouté un routage Blackhole pour empêcher les deux VPC de communiquer entre eux. Si vous souhaitez autoriser la communication entre VPC, vous pouvez supprimer l'entrée de routage 10.0.0.0/8 -> Blackhole de RT1. Cela leur permet de communiquer via la passerelle NAT. Vous pouvez également propager les attachements du VPC en étoile vers RT1 (ou vous pouvez également utiliser une table de routage

et associer/propager tout cela), ce qui active un flux de trafic direct entre les VPC à l'aide de Transit Gateway.

Nous ajoutons un routage statique dans RT1 qui pointe l'ensemble du trafic vers le VPC de sortie. En raison de ce routage statique, Transit Gateway envoie l'ensemble du trafic Internet via ses ENI dans le VPC de sortie. Une fois dans le VPC de sortie, le trafic suit les règles définies dans la table de routage du sous-réseau où se trouvent ces ENI Transit Gateway. Nous ajoutons un routage dans cette table de routage de sous-réseau pointant l'ensemble du trafic vers la passerelle NAT. Le saut suivant de la table de routage du sous-réseau de la passerelle NAT est une passerelle Internet (IGW). Pour que le trafic de retour soit renvoyé, vous devez ajouter une entrée de table de routage statique dans la table de routage du sous-réseau de passerelle NAT pointant l'ensemble du trafic lié au VPC en étoile vers Transit Gateway en tant que saut suivant.

Haute disponibilité

Pour obtenir une haute disponibilité, vous devez utiliser deux passerelles NAT (une dans chaque zone de disponibilité). Au sein d'une zone de disponibilité, la disponibilité SLA de la passerelle NAT est de 99,9 %. La redondance en cas d'échec de composants au sein d'une zone de disponibilité est gérée par AWS dans le cadre du contrat SLA. Le trafic est abandonné pendant la période de 0,1 % pendant laquelle la passerelle NAT peut être indisponible dans une zone de disponibilité. Si une zone de disponibilité échoue complètement, le point de terminaison Transit Gateway et la passerelle NAT de cette zone de disponibilité échouer, et l'ensemble du trafic circule via les points de terminaison Transit Gateway et NAT de l'autre zone de disponibilité.

Sécurité

Vous vous fiez aux groupes de sécurité sur les instances source, aux routages Blackhole dans les tables de routage Transit Gateway et à l'ACL réseau du sous-réseau dans lequel se trouve la passerelle NAT.

Capacité de mise à l'échelle

Une passerelle NAT peut prendre en charge jusqu'à 55 000 connexions simultanées pour chaque destination unique. Pour ce qui est du débit, vous êtes limité par les limites de performances de la passerelle NAT. Transit Gateway n'est pas un équilibreur de charge et ne distribue pas votre trafic uniformément sur la passerelle NAT dans les différentes zones de disponibilité. Si possible, le trafic sur la passerelle Transit Gateway reste dans une zone de disponibilité. Si l'instance EC2 à l'origine du trafic se trouve dans la zone de disponibilité 1, le trafic sort de l'interface réseau Elastic Transit Gateway dans la zone de disponibilité 1 du VPC de sortie et est acheminé vers le saut suivant en

fonction de la table de routage de sous-réseau dans laquelle réside l'interface réseau Elastic. Pour obtenir la liste complète des règles, veuillez consulter Règles et limites des passerelles NAT.

Pour de plus amples informations, veuillez consulter le billet de blog Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway.

Utilisation d'une instance EC2 pour obtenir un trafic sortant centralisé

L'utilisation d'un dispositif de pare-feu logiciel (sur EC2) à partir de AWS Marketplace en tant que point de sortie est similaire à la configuration de la passerelle NAT. Cette option peut être utilisée si vous souhaitez tirer parti des fonctionnalités du système pare-feu de couche 7/système de prévention et de détection des intrusions (IPS/IDS) des différentes offres de fournisseurs.

Dans la Figure 12, nous remplaçons la passerelle NAT par une instance EC2 (avec SNAT activé sur l'instance EC2). Cette option comporte quelques considérations clés :

Haute disponibilité

Dans cette configuration, vous êtes responsable de la surveillance de l'instance EC2, de la détection des échecs et du remplacement de l'instance EC2 par une instance de sauvegarde/de secours. La plupart des fournisseurs AWS disposent d'une automatisation prédéfinie pour leurs logiciels déployés dans cette configuration. Cette automatisation peut contrôler les éléments suivants :

- Détecter l'échec de l'instance EC2-1 principale.
- Modifier la table de routage « Table de routage Egx 1 » pour pointer l'ensemble du trafic vers l'instance EC2-2 de sauvegarde en cas d'échec de l'instance principale. Cette opération est également nécessaire pour les sous-réseaux de la zone de disponibilité 2.

Figure 12 – NAT centralisée utilisant des instances EC2 et Transit Gateway

Capacité de mise à l'échelle

Transit Gateway n'est pas un équilibreur de charge et ne distribue pas votre trafic uniformément entre les instances des deux zones de disponibilité. Si possible, le trafic sur la passerelle Transit Gateway reste dans une zone de disponibilité. Vous êtes limité par les capacités de bande passante d'une seule instance EC2. Vous pouvez mettre à l'échelle verticalement cette instance EC2 à mesure que l'utilisation augmente.

Si le fournisseur que vous choisissez pour l'inspection du trafic sortant ne prend pas en charge l'automatisation pour la détection des échecs, ou si vous avez besoin d'une mise à l'échelle horizontale, vous pouvez utiliser une autre conception. Dans cette conception (Figure 13), nous ne créons pas d'attachement de VPC sur la passerelle de transit pour le VPC de sortie, mais nous créons un attachement VPN IPsec et un VPN IPsec de Transit Gateway vers les instances EC2 en utilisant le protocole BGP pour changer les routages.

Avantages

- Détection des échecs et réacheminement du trafic géré par le protocole BGP. Aucune automatisation de la table de routage de sous-réseau VPC n'est requise.
- Le BGP ECMP peut être utilisé pour équilibrer la charge du trafic sur plusieurs instances EC2. Il est possible d'opérer une mise à l'échelle horizontale.

Figure 13 – NAT centralisée utilisant des instances EC2 et le VPN Transit Gateway

Facteurs clés à prendre en compte

- Surcharge de gestion VPN sur les instances EC2
- La bande passante au niveau de Transit Gateway est limitée à 1,25 Gbit/s par tunnel VPN. Avec ECMP, Transit Gateway peut prendre en charge jusqu'à 50 Gbps de bande passante VPN totale. Les capacités de traitement de paquets et de VPN de l'appliance du fournisseur peuvent être un facteur limitant.
- Cette conception suppose que l'instance EC2 FW fonctionne avec la même interface réseau Elastic pour le trafic entrant et sortant.
- Si vous activez la répartition de charge ECMP du trafic sur plusieurs instances EC2, vous devez activer SNAT pour le trafic sur l'instance EC2 afin de garantir la symétrie du flux de retour, ce qui signifie que la destination ne connaîtra pas la véritable source.

Sécurité réseau centralisée pour le trafic VPC vers VPC et pour le trafic sur site vers VPC

AWS fournit des groupes de sécurité et des listes de contrôle d'accès réseau (NACL) de sous-réseau pour implémenter la sécurité du réseau au sein de votre zone de destination. Il s'agit de pare-feux de couche 4. Imaginons le cas d'un client qui souhaite implémenter un pare-feu de couche 7/ système IPS/IDS dans sa zone de destination afin d'inspecter le trafic qui circule entre des VPC ou entre un centre de données sur site et un VPC. Cette opération peut être réalisée à l'aide de Transit Gateway et d'appliances logicielles tierces exécutées sur des instances EC2. À l'aide de l'architecture de la Figure 14, nous pouvons permettre au trafic VPC vers VPC et au trafic sur site vers VPC de circuler via les instances EC2. La configuration est similaire à celle dont nous avons déjà parlé dans la Figure 12, mais nous supprimons le routage Blackhole dans la table de routage 1 afin de permettre la circulation du trafic VPC interne et nous attachons l'attachement VPN et/ou l'attachement Direct Connect GW à la table de routage 1 pour permettre le flux de trafic hybride. Cela permet à l'ensemble du trafic provenant des étoiles de circuler vers le VPC de sortie avant d'être envoyé vers la destination. Vous avez besoin de routages statiques dans la table de routage du sous-réseau du VPC de sortie (où résident les dispositifs EC2 du pare-feu) pour envoyer le trafic destiné aux VPC en étoile et l'adresse CIDR sur site via Transit Gateway après inspection du trafic.

> **Note**
>
> Les informations de routage ne sont pas propagées dynamiquement depuis Transit Gateway vers la table de routage du sous-réseau et doivent être entrées de manière statique. Il existe une limite flexible de 50 routages statiques sur une table de routage de sous-réseau.

Figure 14 – Contrôle du trafic VPC vers VPC et VPC sur site

Facteurs clés à prendre en compte lors de l'envoi de trafic vers des instances EC2 pour inspection en ligne :

- Frais supplémentaires de traitement des données de Transit Gateway
- Le trafic doit passer par deux sauts supplémentaires (instance EC2 et Transit Gateway)
- Possibilité de goulots d'étranglement en termes de bande passante et de performance

- Complexité supplémentaire liée à la maintenance, à la gestion et à la mise à l'échelle des instances EC2 :
  - Détection des échecs et basculement en mode veille
  - Suivi de l'utilisation et mise à l'échelle horizontale/verticale
  - Configuration du pare-feu, gestion des correctifs
  - Traduction d'adresses réseau source (SNAT) du trafic lors de la répartition de charge pour garantir un flux symétrique

Vous devez être sélectif quant au trafic qui passe par ces instances EC2. L'un des moyens d'y parvenir consiste à définir des zones de sécurité et à inspecter le trafic entre les zones non fiables. Une zone non fiable peut être un site distant géré par un tiers, un VPC fournisseur que vous ne contrôlez pas ou auquel vous ne faites pas confiance, ou un VPC d'environnement de test (sandbox)/de développement, dont le cadre de sécurité est plus souple par rapport au reste de votre environnement. La Figure 15 permet un flux de trafic direct entre des réseaux approuvés tout en inspectant le flux de trafic vers/depuis des réseaux non approuvés à l'aide d'instances EC2 en ligne. Nous avons créé trois zones dans cet exemple :

- Zone non fiable : il s'agit de tout trafic provenant du « VPN vers un site non fiable distant » ou du VPC du fournisseur tiers.
- Zone de production : contient le trafic provenant du VPC de production et du contrôleur de domaine du client sur site.
- Zone de développement : contient le trafic provenant des deux VPC de développement.

Voici des exemples de règles que nous définissons pour la communication entre les zones :

1. Zone non fiable Zone de production - Communication non autorisée
2. Zone de production Zone de développement : communication autorisée via les appliances FW EC2 dans le VPC de sortie
3. Zone non fiable Zone de développement : communication autorisée via les appliances FW EC2 dans le VPC de sortie
4. Zone de production Zone de production et Zone de développement Zone de développement – Communication directe via Transit Gateway

Il s'agit d'une configuration comportant trois zones de sécurité, mais il peut y en avoir plus. Vous pouvez utiliser plusieurs tables de routage et des routages Blackhole pour obtenir une isolation de sécurité et un flux de trafic optimal. Le choix des zones appropriées dépend de votre stratégie globale de conception des zones de destination (structure du compte, conception du VPC). Des zones peuvent permettre l'isolation entre l'unité commerciale, les applications, les environnements, etc.

Dans cet exemple, nous résilions le VPN distant non fiable sur Transit Gateway et envoyons l'ensemble du trafic vers les appliances logicielles FW sur EC2 à des fins d'inspection. Vous pouvez également résilier ces VPN directement sur les instances EC2 au lieu de Transit Gateway. Avec cette approche, le trafic VPN non fiable n'interagit jamais directement avec Transit Gateway. Le nombre de sauts dans le flux de trafic diminue de 1 et vous économisez sur les coûts AWS VPN. Pour activer les échanges de routages dynamiques (pour que Transit Gateway apprenne le CIDR du VPN distant via BGP), les instances de pare-feu doivent être connectées à Transit Gateway via un VPN. Dans le modèle d'attachement TGW natif, vous devez ajouter des routes statiques dans la table de routage TGW pour le CIDE VPN avec le saut suivant comme VPC de sortie/sécurité. Dans notre configuration (Figure 15), nous avons une route par défaut pour sortir le VPC pour l'ensemble du trafic. Nous n'avons pas besoin d'ajouter explicitement de routages statiques spécifiques. Avec cette approche, vous passez d'un point de terminaison VPN Transit Gateway entièrement géré à une instance EC2 autogérée, en ajoutant une surcharge de gestion VPN ainsi qu'une charge supplémentaire sur l'instance EC2 en termes de calcul et de mémoire.

Figure 15 – Isolation du trafic avec Transit Gateway et définition de zones de sécurité

DNS

Lorsque vous lancez une instance dans un VPC personnalisé, AWS fournit un nom d'hôte DNS privé à l'instance (il peut s'agir d'un nom d'hôte DNS public) en fonction des attributs DNS que vous spécifiez pour le VPC et si votre instance dispose d'une adresse IPv4 publique. Lorsque l'attribut enableDnsSupport est défini sur true, vous obtenez une résolution DNS au sein du VPC à partir du résolveur Route 53 (décalage IP+2 par rapport au CIDR du VPC). Par défaut, le résolveur Route 53 répond aux requêtes DNS pour les noms de domaine du VPC, comme les noms de domaine des instances EC2 ou des équilibreurs de charge Elastic Load Balancing. Avec l'appairage de VPC, les hôtes d'un VPC peuvent résoudre les noms d'hôte DNS publics en adresses IP privées pour les instances de VPC appairés, à condition que cette option soit activée. Il en va de même pour les VPC connectés via AWS Transit Gateway. Pour de plus amples informations, veuillez consulter Activation de la prise en charge de la résolution DNS pour une connexion d'appairage de VPC.

Si vous souhaitez mapper vos instances à un nom de domaine personnalisé, vous pouvez utiliser Amazon Route 53 pour créer un enregistrement de mappage DNS vers IP personnalisé. Une zone hébergée Amazon Route 53 est un conteneur qui comporte des informations sur la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines. Les zones hébergées publiques contiennent des informations DNS qui peuvent être résolues sur l'Internet public, tandis que les zones hébergées privées sont une implémentation spécifique qui ne présente des informations qu'aux VPC qui ont été attachés à la zone hébergée privée spécifique. Dans une configuration de zone de destination dans laquelle vous avez plusieurs VPC/comptes, vous pouvez associer une seule zone hébergée privée à plusieurs VPC sur des comptes AWS et des régions. Les hôtes finaux des VPC utilisent leur adresse IP de résolveur Route 53 respective (décalage IP+2 par rapport au CIDR du VPC) comme serveur de noms pour les requêtes DNS. Le résolveur Route 53 dans un VPC accepte les requêtes DNS provenant uniquement des ressources d'un VPC.

DNS hybride

La coordination de la résolution DNS entre la configuration de la zone de destination AWS et les ressources sur site constitue l'un des éléments les plus critiques d'un réseau hybride. Les clients qui implémentent des environnements hybrides disposent généralement d'un système de résolution DNS déjà en place et souhaitent une solution DNS qui fonctionne en tandem avec leur système actuel. Lorsque vous intégrez un DNS pour les VPC dans une région AWS avec un DNS pour votre réseau, vous avez besoin d'un point de terminaison entrant du résolveur Route 53 (pour les requêtes

DNS que vous transférez vers vos VPC) et d'un point de terminaison sortant du résolveur Route 53 (pour les requêtes que vous transférez à partir de vos VPC vers votre réseau). Comme le montre la Figure 16, vous pouvez configurer les points de terminaison sortants du résolveur pour transférer les requêtes qu'il reçoit des instances EC2 de vos VPC vers les serveurs DNS de votre réseau. Pour réacheminer les requêtes sélectionnées, d'un VPC vers un système sur site, créez des règles de résolveur Route 53 qui spécifient les noms de domaine pour les requêtes DNS que vous souhaitez réacheminer (par exemple, example.com) et les adresses IP des résolveurs DNS de votre réseau vers lesquels vous voulez réacheminer les requêtes. Pour les requêtes entrantes provenant de systèmes sur site vers des zones hébergées Route 53, les serveurs DNS de votre réseau peuvent transférer les requêtes aux points de terminaison entrants du résolveur dans un VPC spécifié.

Figure 16 – Résolution DNS hybride à l'aide du résolveur Route 53

Cela permet à vos résolveurs DNS sur site de résoudre facilement les noms de domaine des ressources AWS telles que les instances EC2 ou les enregistrements dans une zone hébergée privée Route 53 associée à ce VPC.

Il n'est pas recommandé de créer des points de terminaison du résolveur Route 53 dans chaque VPC de la zone de destination. Centralisez-les dans un VPC de sortie central (dans le compte de services réseau). Cette approche permet une meilleure gestion tout en maintenant les coûts bas (des frais horaires vous sont facturés pour chaque point de terminaison d'entrée/de sortie que vous créez). Vous partagez le point de terminaison d'entrée et de sortie centralisé avec le reste de la zone de destination.

Résolution sortante : utilisez le compte de services réseau pour écrire des règles de résolution (en fonction des requêtes DNS qui seront transmises aux serveurs DNS sur site). À l'aide de Resource Access Manager (RAM), partagez ces règles du résolveur Route 53 avec plusieurs comptes (et associez-les aux VPC dans les comptes). Les instances EC2 des VPC en étoile peuvent envoyer des requêtes DNS au résolveur Route 53 et le service du résolveur Route 53 transmettra ces requêtes au serveur DNS sur site via les points de terminaison du résolveur Route 53 de sortie dans le VPC de sortie. Vous n'avez pas besoin d'appairer des VPC en étoile au VPC de sortie ni de les connecter via Transit Gateway. N'utilisez pas l'adresse IP du point de terminaison du résolveur de sortie en tant que DNS principal dans les VPC en étoile. Les VPC en étoile doivent utiliser le résolveur Route 53 (pour décaler le CIDR du VPC) dans leur VPC.

Figure 17 – Centralisation des points de terminaison du résolveur Route 53 dans le VPC de sortie

Résolution DNS d'entrée : créez des points de terminaison de sortie du résolveur Route 53 dans un VPC centralisé et associez toutes les zones hébergées privées de votre zone de destination à ce VPC centralisé. Pour de plus amples informations, veuillez consulter Association de plusieurs VPC à une zone hébergée privée. Plusieurs zones hébergées privées associées à un VPC ne peuvent pas se chevaucher. Comme le montre la Figure 17, cette association de zones hébergées privées au VPC centralisé permettra aux serveurs sur site de résoudre le DNS pour toute entrée dans n'importe quelle zone hébergée privée (associée au VPC central) à l'aide du point de terminaison d'entrée dans le VPC centralisé. Pour de plus amples informations sur les configurations DNS hybrides, veuillez consulter Gestion DNS centralisée du cloud hybride avec Amazon Route 53 et AWS Transit Gateway et Options DNS de cloud hybride pour Amazon VPC.

Accès centralisé aux points de terminaison privés d'un VPC

Un point de terminaison d'un VPC vous permet de connecter de façon privée votre VPC aux services AWS pris en charge sans avoir besoin d'une passerelle Internet ou d'un appareil NAT. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les points de terminaison de services AWS avec ce point de terminaison d'interface. Le trafic entre votre VPC et d'autres services ne quitte pas le backbone du réseau AWS. Deux types de points de terminaison peuvent actuellement être configurés : les points de terminaison d'interface (basés sur AWS PrivateLink) et les points de terminaison de passerelle. Les points de terminaison de passerelle sont alloués gratuitement, et la centralisation ne fait pas l'objet d'un cas d'utilisation fort.

Points de terminaison d'un VPC d'interface

Un point de terminaison d'interface est une interface réseau Elastic avec une adresse IP privée qui sert de point d'entrée au trafic destiné à un service AWS pris en charge. Lorsque vous allouez un point de terminaison d'interface, les utilisateurs sont facturés pour chaque heure d'exécution du point de terminaison. Par défaut, vous créez un point de terminaison d'interface dans chaque VPC à partir duquel vous souhaitez accéder au service AWS. Cela peut s'avérer coûteux et difficile à gérer dans la configuration de la zone de destination lorsqu'un client souhaite interagir avec un service AWS spécifique sur plusieurs VPC. Pour éviter cela, vous pouvez héberger les points de terminaison d'interface dans un VPC centralisé. Tous les VPC en étoile utiliseront ces points de terminaison centralisés.

Lorsque vous créez un point de terminaison d'un VPC pour un service AWS, vous pouvez activer un DNS privé. Lorsqu'il est activé, le paramètre crée une zone hébergée privée Route 53 gérée par AWS qui permet de résoudre le point de terminaison du service AWS public à l'adresse IP privée du point de terminaison d'interface. La zone hébergée privée gérée fonctionne uniquement au sein du VPC avec le point de terminaison de l'interface. Dans notre configuration, lorsque nous voulons que les VPC en étoile puissent résoudre le DNS du point de terminaison d'un VPC hébergé dans un VPC centralisé, la zone hébergée privée gérée ne fonctionnera pas. Pour résoudre ce problème, désactivez l'option qui crée automatiquement le DNS privé lorsqu'un point de terminaison d'interface est créé. Vous pouvez également créer manuellement une zone hébergée privée Route 53 et ajouter un enregistrement d'alias avec le nom complet du point de terminaison du service AWS pointant vers le point de terminaison de l'interface, comme indiqué dans la Figure 18.

Figure 18 – Zone hébergée privée créée manuellement

Nous associons cette zone hébergée privée à d'autres VPC au sein de la zone de destination. Cette configuration permet aux VPC en étoile de résoudre les noms de point de terminaison à service complet pour les points de terminaison d'interface dans le VPC centralisé.

> **Note**
>
> Pour accéder à la zone hébergée privée partagée, les hôtes des VPC en étoile doivent utiliser l'adresse IP du résolveur Route 53 de leur VPC. Les points de terminaison d'interface sont également accessibles à partir de réseaux sur site sur VPN et via Direct Connect. Utilisez des règles de transfert conditionnel pour envoyer l'ensemble du trafic DNS pour les noms de point de terminaison à service complet aux points de terminaison entrants du résolveur Route 53, qui résoudront les demandes DNS en fonction de la zone hébergée privée.

Dans la Figure 19, Transit Gateway active le flux de trafic des VPC en étoile vers les points de terminaison de l'interface centralisée. Créez des points de terminaison d'un VPC et la zone hébergée privée associée dans le compte de services réseau et partagez-la avec les VPC en étoile des comptes en étoile. Pour de plus amples informations sur le partage des informations de point de terminaison avec d'autres VPC, veuillez consulter le billet de blog Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver.

Remarque : Une approche de point de terminaison d'un VPC distribué, c'est-à-dire un point de terminaison par VPC, vous permet d'appliquer des politiques de moindre privilège sur les points de terminaison d'un VPC. Dans une approche centralisée, vous appliquerez et gérerez des politiques pour tous les accès au VPC en étoile sur un seul point de terminaison. Le nombre croissant de VPC risque d'accroître la complexité du maintien du moindre privilège avec un document de politique unique. Un document de politique unique entraîne également un rayon d'impact plus important. Vous êtes également limité au niveau de la taille du document de politique (20 480 caractères).

Figure 19 – Centralisation des points de terminaison d'un VPC d'interface

Conclusion

À mesure que vous mettez à l'échelle votre utilisation d'AWS et que vous déployez des applications dans la zone de destination AWS, le nombre de VPC et de composants réseau augmente. Dans ce livre blanc, vous avez appris à gérer cette infrastructure croissante en garantissant la capacité de mise à l'échelle, la haute disponibilité et la sécurité, tout en maintenant les coûts à un niveau bas. Il est essentiel de prendre les bonnes décisions de conception lorsque vous tirez parti de services tels que Transit Gateway, de AWS Direct Connect, de points de terminaison VPC et d'appliances logicielles tierces. Il est important de comprendre les facteurs clés à prendre en compte pour chaque approche, de concevoir la solution en fonction de vos exigences et d'analyser l'option ou la combinaison d'options qui vous convient le mieux.

Participants

Les personnes suivantes ont participé à l'élaboration de ce document :

- Sidhartha Chauhan, Architecte de solutions, Amazon Web Services
- Amir Abu-Akeel, Architecte en infrastructure cloud, Amazon Web Services
- Sohaib Tahir, Architecte de solutions, Amazon Web Services

Historique du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

update-history-change	update-history-description	update-history-date
Mise à jour mineure	Mise à jour de la section Transit Gateway et appairage de VPC.	2 avril 2021
Livre blanc mis à jour	Texte corrigé pour correspon dre aux options illustrées dans la Figure 7.	10 juin 2020
Mise à jour mineure	Texte corrigé pour correspon dre aux options illustrées dans la Figure 7.	10 juin 2020
Publication initiale	Livre blanc publié.	15 novembre 2019

Mentions légales

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d'AWS et de ses affiliés, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l'état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.