Connexion à Salesforce Hyperforce à l'aide de Megaport AWS Direct Connect

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Connexion à Salesforce Hyperforce à l'aide de Megaport AWS Direct Connect

Table of Contents

Connexion à Salesforce Hyperforce à l'aide de Megaport AWS Direct Connect

Bennett Borofka et Kranthi Pullagurla (AWS), Abhiram Gajjala (Salesforce), Kevin Dresser (Megaport)

Août 2024 (historique du document)

De nombreux AWS utilisateurs ont des charges de travail hybrides qui s'étendent sur le cloud et sur site. Pour fournir de manière adéquate une connectivité réseau privée et fiable entre ces environnements, vous pouvez choisir parmi une variété d'options afin de garantir la valeur commerciale et l'optimisation des coûts. Les utilisateurs disposant de succursales, de centres de données d'entreprise et d'un personnel connecté à un VPN ont des exigences uniques pour permettre l'accès à Salesforce Hyperforce sous forme d'exécution. AWS Ce guide décrit des cas d'utilisation pour aider Salesforce Hyperforce et AWS les utilisateurs à configurer une connectivité privée Direct Connect et fiable à Hyperforce en utilisant la plate-forme de réseau défini par logiciel (SDN) Megaport.

Salesforce Hyperforce est une architecture d'infrastructure Salesforce de nouvelle génération conçue pour fonctionner sur des fournisseurs de cloud tels que. AWS Vous pouvez utiliser Hyperforce pour bénéficier de sa conformité, de sa sécurité, de son agilité, de son évolutivité et de sa confidentialité améliorées. Hyperforce propose plusieurs options pour établir une connectivité réseau privée et fiable avec Hyperforce à partir de votre site sur site, d'autres fournisseurs de cloud ou d'autres Comptes AWS fournisseurs de cloud.

Direct Connectest un service cloud qui contourne Internet pour relier les succursales et les centres de données à AWS. Il offre le chemin le plus court entre votre position et Hyperforce, où le trafic réseau reste sur le réseau AWS principal et ne traverse jamais l'Internet public.

Megaport est une plateforme et un partenaire SDN. Direct Connect Megaport propose une variété d'options de connectivité réseau aux utilisateurs qui souhaitent une connectivité rapide AWS et fiable avec d'autres fournisseurs de cloud.

Ce guide s'adresse aux praticiens, aux architectes, aux administrateurs et aux opérateurs des réseaux, de l'infrastructure cloud et de Salesforce Hyperforce.

Composants de la solution

Direct Connect vous oblige à créer votre propre connexion dédiée ou à AWS travailler avec un Direct Connect partenaire pour créer une connexion hébergée. Cet article fournit des conseils sur l'utilisation de Megaport en tant que Direct Connect partenaire afin de faciliter les cas d'utilisation hybrides et multiples pour la connexion à Salesforce Hyperforce.

Direct Connect

Direct Connect établit une connexion réseau privée et dédiée entre les centres de données sur site et AWS. Ce lien direct aide les organisations à contourner l'Internet public et fournit une communication fiable et privée avec AWS les ressources.

Bien qu'Hyperforce fonctionne sur une AWS infrastructure, son utilisation Direct Connect pour y accéder nécessite de gérer, de Compte AWS facturer et de configurer la connexion. L'utilisation Direct Connect pour se connecter à l' Compte AWS Hyperforce géré par Salesforce n'est pas prise en charge.

Connexion hébergée

Une connexion hébergée est une connexion Ethernet physique qu'un Direct Connect partenaire fournit au nom d'un utilisateur. Les cas d'utilisation et les architectures décrits dans ce guide utilisent une connexion hébergée avec le Direct Connect partenaire Megaport. Les connexions hébergées offrent des plages de bande passante comprises entre 50 Mbits/s et 25 Gbit/s par incréments multiples, tandis que les connexions dédiées sont fournies dans des capacités de 1 Gbit/s, 10 Gbit/s et 100 Gbit/s. Pour plus d'informations sur la Direct Connect bande passante et les coûts, consultez la section Direct Connect tarification.

Interface virtuelle publique

L'architecture Hyperforce nécessite l'accès à l'espace d'adresses IP public des AWS ressources à partir d'emplacements sur site et multicloud. Une interface virtuelle publique (VIF) est utilisée pour connecter votre site distant au public Services AWS et au public IPs déployé sur AWS. L'utilisation d'un VIF privé pour accéder à Hyperforce n'est pas prise en charge.

Remarques

- L'utilisation d'un VIF public nécessite l'utilisation d' IPv4 adresses publiques uniques. Vous devrez fournir votre propre IPv4 CIDR ou demander un /31 CIDR au Support AWS . Pour plus d'informations, consultez les conditions requises pour les interfaces virtuelles dans la Direct Connect documentation.
- L'utilisation d'un VIF public pour vous connecter AWS depuis votre environnement sur site ou multicloud modifie la façon dont le trafic est acheminé des préfixes AWS publics vers vos utilisateurs. Nous vous recommandons d'utiliser un filtre de préfixes (feuille de route) pour vous assurer que les préfixes Amazon acceptés sont limités à l'infrastructure Hyperforce et à toutes les autres ressources nécessaires. AWS Pour plus d'informations, consultez les règles relatives à la publicité relative au préfixe de l'interface virtuelle publique dans la Direct Connect documentation.
- Les préfixes annoncés par ne Direct Connect doivent pas être annoncés au-delà des limites du réseau de votre connexion. Par exemple, ces préfixes ne doivent pas être inclus dans les tables de routage Internet public. Pour plus d'informations, consultez les politiques de routage des interfaces virtuelles publiques dans la Direct Connect documentation.

Salesforce

Salesforce est une plateforme de gestion de la relation client (CRM) conçue pour vous aider à vendre, à servir, à commercialiser, à analyser et à communiquer avec vos clients.

Hyperforce

Salesforce Hyperforce est une architecture d'infrastructure Salesforce de nouvelle génération conçue pour le cloud public. Il offre une évolutivité, une flexibilité et une agilité améliorées grâce à l'utilisation de l' AWS infrastructure. C'est le moyen le plus rapide et le plus simple d'exécuter Salesforce sur une infrastructure de cloud public.

Salesforce Express Connect (SEC)

Salesforce Express Connect (SEC) permet une connectivité privée et fiable entre les utilisateurs et les centres de données gérés par Salesforce. Garantir une connectivité privée à Hyperforce nécessite actuellement une connexion SEC en conjonction avec. Direct Connect

Remarques

- Un nombre limité de services Salesforce sont toujours exécutés dans l'infrastructure gérée par Salesforce. Pour maintenir la connectivité à tous les services de l'infrastructure gérée par Salesforce et d'Hyperforce, les utilisateurs qui ont besoin d'un accès réseau privé à Salesforce doivent continuer à utiliser SEC en même temps. Direct Connect
- Salesforce et AWS ne vendez pas SEC. Si vous avez besoin d'une connectivité réseau privée à une infrastructure gérée par Salesforce, vous aurez besoin d'une connexion SEC. Cet article décrit l'établissement d'une nouvelle connexion SEC à Salesforce à l'aide de Megaport.
- La SEC n'est utilisée pour aucune migration de données entre l'infrastructure gérée par Salesforce et Hyperforce. Si vous migrez vers Hyperforce, Salesforce facilite les migrations de données au sein de votre organisation sur un backbone privé. La SEC est nécessaire pour que les utilisateurs puissent se connecter de manière continue et privée à Salesforce.

Mégaport

Megaport simplifie et accélère la connectivité au cloud hybride de Régions AWS manière évolutive, privée et à la demande. Megaport agit en tant que facilitateur dans cet écosystème de connectivité et propose des solutions SDN pour simplifier et optimiser le processus de connexion aux services cloud, y compris le. AWS Cloud Les connexions Megaport sont appelées connexions croisées virtuelles (VXCs), qui sont des circuits Ethernet de couche 2 qui fournissent une connectivité privée, flexible et à la demande entre tous les emplacements du réseau Megaport. Pour accéder au réseau Megaport, vous devez d'abord créer un port, Megaport Virtual Edge (MVE) ou Megaport Cloud Router (MCR), qui sont abordés dans les sections suivantes.

Port Megaport

Le port Megaport est une interface Ethernet haut débit qui crée une network-to-network interface (NNI) entre votre réseau et le réseau Megaport. Il est configuré comme un tronc de réseau local virtuel (VLAN) 802.1Q pouvant en prendre en charge jusqu'à 100 VXCs, chacun étant présenté comme un VLAN unique. Le processus de provisionnement du port active l'interface Megaport et génère une lettre d'autorisation (LOA) contenant des instructions permettant à l'opérateur du centre de données d'établir la connexion croisée physique entre votre équipement et le nouveau port.

> **Note**
>
> Votre périphérique réseau nécessite des interfaces 10 ou 100 Gbit/s avec des émetteurs-récepteurs optiques 10GBASE-LR (duplex sur fibre optique monomode [SMOF]) ou 100G-LR4 (duplex sur SMOF).

Mégaport virtuel (MVE)

Megaport Virtual Edge (MVE) est une plateforme de virtualisation des fonctions réseau (NFV) qui fournit une infrastructure virtuelle pour les services réseau à la périphérie du SDN mondial de Megaport. Vous pouvez utiliser MVE pour déployer une pile réseau virtuelle (ou point de présence) sans présence physique ni matériel dans un centre de données. Le MVE est disponible dans 27 régions métropolitaines du monde entier et est étroitement lié aux sites de Direct Connect peering ()NNIs. MVE prend en charge les appliances VNF tierces de fournisseurs tels qu'Aruba, Cisco, Fortinet, Palo Alto Networks, Versa Networks et. VMware

> **Note**
>
> Megaport ne vend pas de licences tierces et exige que vous utilisiez un modèle de licence BYOL (Bring Your Own License).

Routeur cloud Megaport (MCR)

Megaport Cloud Router (MCR) est un service de routeur virtuel géré qui permet une mise en réseau directe de couche 2 et de couche 3 entre les points de terminaison du réseau Megaport, y compris les autres fournisseurs de cloud. Le MCR peut être déployé en tant que service autonome pour acheminer le trafic entre différents environnements cloud sans que vous ayez à être physiquement présent dans ce centre de données. Il peut également être connecté à votre port pour rediriger le trafic pertinent vers un emplacement physique. Le MCR est géré via le portail Megaport pour configurer les fonctions de routage statiques et dynamiques du Border Gateway Protocol (BGP), notamment la détection du transfert bidirectionnel (BFD), le discriminateur à sorties multiples (MED), le numéro de système autonome (ASN) et le NAT. Pour plus d'informations, consultez la section Configuration des paramètres avancés du BGP dans la documentation de Megaport.

Cas d’utilisation

Les cas d'utilisation présentés dans les sections suivantes fournissent des exemples de la manière dont vous pouvez permettre à vos utilisateurs de bénéficier d'une connectivité privée et fiable à Hyperforce.

- Succursales
- VPN-connected main d'œuvre
- Infrastructure de bureau virtuel multicloud

Considérations clés

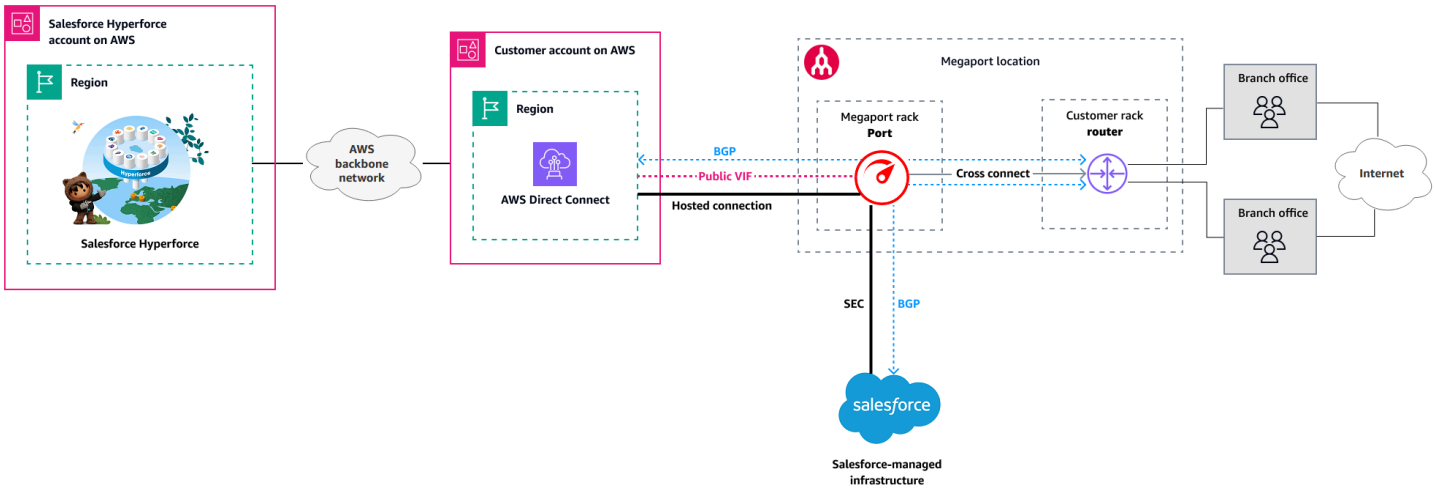
- Hyperforce peut être utilisé à la fois pour la connectivité privée et publique.
- Vous pouvez utiliser n'importe quelle combinaison des cas d'utilisation décrits.
- Les nouveaux utilisateurs de Salesforce et les utilisateurs qui migrent depuis l'infrastructure du centre de Salesforce-managed données peuvent utiliser Hyperforce. Les cas d'utilisation couvrent les deux scénarios.
- La migration des données d'une instance de centre de Salesforce-managed données vers Hyperforce est gérée par Salesforce en arrière-plan et n'utilise pas l'architecture réseau décrite dans ces cas d'utilisation.
- Certains aspects de la connexion des applications utilisateur à Hyperforce nécessitent toujours une connectivité réseau avec les centres de Salesforce-managed données. Pour cette raison, si vous avez besoin d'une connectivité entièrement privée, vous devez utiliser SEC avec Direct Connect.

Cas d'utilisation : succursales

Ce cas d'utilisation couvre un scénario dans lequel vous avez un routeur physique dans un emplacement Megaport et vous l'utilisez comme rampe d'accès. Direct Connect Dans ce scénario, vous avez également une ou plusieurs succursales connectées à cet emplacement via des circuits privés.

L'utilisation de Megaport Port Direct Connect offre à vos utilisateurs travaillant dans des succursales une connectivité privée à Salesforce Hyperforce. Les succursales se composent d'un bureau unique ou d'un groupe de bureaux interconnectés via un réseau métropolitain (MAN). Les bureaux sont

accessibles Direct Connect en utilisant un emplacement Megaport. Le schéma suivant montre l'architecture de ce cas d'utilisation.



Exigences

- Vos utilisateurs accèdent à Salesforce via des connexions réseau privées.
- Vos utilisateurs travaillent principalement à partir de succursales disposant d'une connectivité privée avec un Megaport-enabled emplacement.
- Vous êtes propriétaire d'un Compte AWS serveur pour gérer la connexion Direct Connect hébergée avec Megaport.
- Vous disposez d'un routeur physique déployé sur un site Megaport qui facilite une connexion croisée avec le routeur de Megaport.

Configuration du port Megaport avec VXC

Le port Megaport est configuré avec un VXC et fournit le segment de réseau privé de couche 2 à. AWS La Direct Connect connexion est configurée en tant que connexion hébergée et attachée à un VIF public. Pour obtenir des instructions étape par étape, consultez la documentation Megaport suivante :

- Création d'un port
- Configuration et maintenance des connexions AWS hébergées

Configuration de vos appareils réseau

Les périphériques réseau déployés sur le site Megaport de votre rack sont configurés pour prendre en charge la connectivité aux instances Hyperforce via. Direct Connect Ces appareils peuvent inclure un routeur, un commutateur, un pare-feu ou une pile réseau combinée de plusieurs appareils. Les types de fournisseur et de modèle sont facultatifs, en fonction de vos besoins. Nous vous recommandons de contacter votre administrateur réseau pour configurer ces appareils.

Le périphérique utilisé pour établir la connexion croisée physique avec le rack Megaport doit prendre en charge le balisage VLAN 802.1Q pour établir la contiguïté de couche 2. Une contiguïté de couche 3 est ensuite établie entre votre routeur et le VIF AWS public à l'aide du protocole BGP.

> **Remarques**
>
> - Les préfixes BGP annoncés par votre routeur AWS sont configurés Console de gestion AWS lorsque vous créez le VIF public.
> - Les préfixes annoncés par ne Direct Connect doivent pas être annoncés au-delà des limites du réseau de votre connexion. Par exemple, ces préfixes ne doivent pas être inclus dans les tables de routage Internet public. Pour plus d'informations, consultez la section Politiques de routage de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration Direct Connect

Accepter une connexion hébergée

Dans votre Compte AWS, acceptez le VXC créé précédemment en tant que connexion hébergée. Pour obtenir des instructions, consultez la Direct Connect documentation.

Création d'un VIF public

Dans votre compte, fournissez un VIF public dans le cadre de la connexion que vous avez acceptée de Megaport. Avant de créer ce VIF, vous devez obtenir les informations suivantes :

- Le BGP ASN du routeur déployé sur le site Megaport.
- Adresses IPv4 publiques pour le peering (généralement /31 CIDR). Vous pouvez les posséder ou en faire la demande auprès de AWS Support. Pour plus d'informations, consultez la section

Adresses IP homologues dans la section Conditions requises pour les interfaces virtuelles de la Direct Connect documentation.

Pour créer un VIF public, suivez les étapes décrites dans la Direct Connect documentation.

Après avoir créé le VIF public, vous devez vous assurer que la clé d'authentification BGP correspond aux deux extrémités de l'homologue BGP pour que l'état de peering soit disponible.

> **Note**
>
> L'utilisation d'un VIF public pour vous connecter AWS depuis votre environnement sur site modifie la façon dont le trafic est acheminé des préfixes AWS publics vers vos utilisateurs. Nous vous recommandons d'utiliser un filtre de préfixes (feuille de route) pour vous assurer que les préfixes Amazon acceptés sont limités à l'infrastructure Hyperforce et à toutes les autres ressources nécessaires. AWS Pour plus d'informations, consultez la section Règles relatives à la publicité relative au préfixe de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration du port Megaport avec SEC

Vous pouvez également équiper le port Megaport d'un VXC SEC, qui fournit les éléments réseau de couche 2 pour la connexion privée aux Salesforce-managed centres de données. SEC vous permet d'accéder aux applications et aux services Salesforce directement via une connexion privée dédiée. Le SEC est fourni sous la forme d'un service routé de couche 3. Vous accédez aux services Salesforce en utilisant des adresses IP publiques et vous devez exécuter le BGP pour recevoir les itinéraires Salesforce. Megaport alloue une plage d'adresses IP `/31` publiques pour chaque peering Salesforce.

> **Note**
>
> La SEC propose deux options d'adressage IP :
>
> - Source NAT votre trafic LAN pour utiliser l'espace IP `/31` public fourni par Megaport.
> - Faites la promotion de votre propre espace d'adresse IP public auprès de Salesforce. (Salesforce n'acceptera pas les blocs d'espace d'adressage IP RFC1918.)

Pour obtenir des instructions détaillées, consultez la section Connexion à Salesforce Express Connect dans la documentation de Megaport.

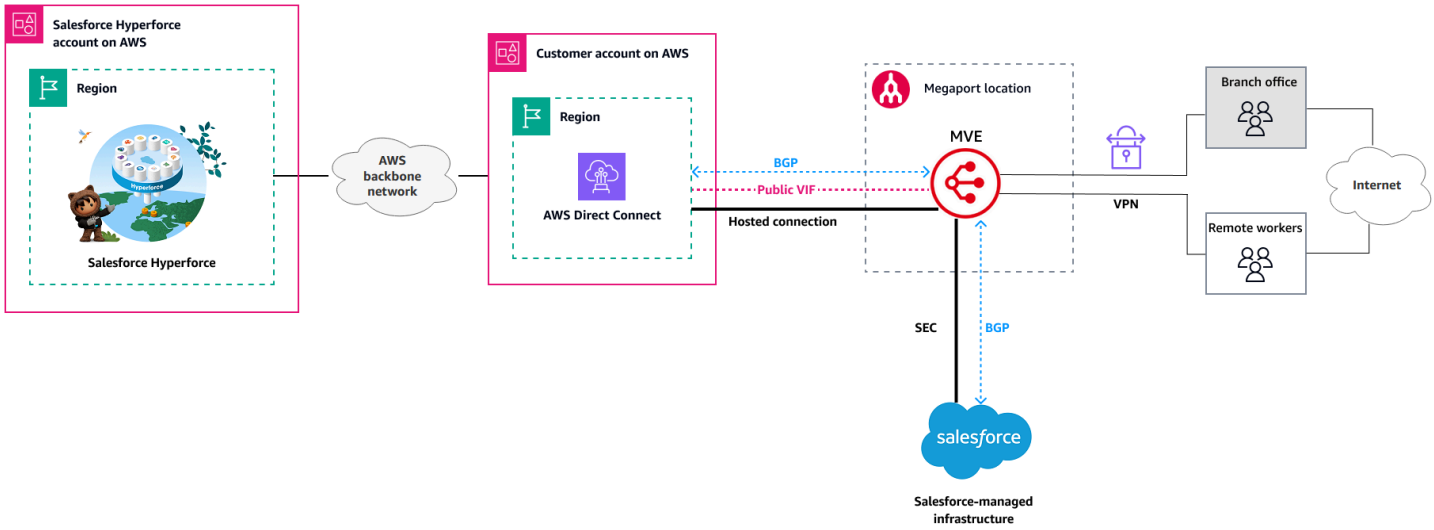
Configuration de Salesforce Hyperforce

Pour activer les connexions entrantes de votre réseau d'entreprise vers Salesforce, vous devez configurer l'accès entrant à Hyperforce par mesure de sécurité. Pour autoriser les domaines requis, suivez les instructions de la section Autoriser les domaines pour une console Salesforce dans Salesforce Classic dans la documentation Salesforce. N'utilisez pas d'adresses IP.

Cas d'utilisation : VPN-connected main d'œuvre

Ce cas d'utilisation couvre un scénario dans lequel vous utilisez un concentrateur VPN virtuel sur un site Megaport comme passerelle d'accès. Direct Connect Dans ce scénario, vous avez des succursales ou des employés distants dotés de VPN de site à site qui se connectent au concentrateur VPN.

Utilisez Megaport MVE avec un pare-feu virtuel tiers pour offrir à vos télétravailleurs Direct Connect une connectivité privée à Salesforce Hyperforce. Les télétravailleurs se connectent au concentrateur VPN depuis un routeur connecté à Internet dans une succursale ou depuis un client VPN exécuté sur leur appareil. Les télétravailleurs se rendent ensuite Direct Connect en utilisant un emplacement Megaport.



Exigences

- Vos télétravailleurs accèdent à Salesforce via des connexions réseau privées.

- Vos télétravailleurs ou les utilisateurs de vos succursales disposent d'une connectivité VPN de site à site avec un Megaport-enabled emplacement sur Internet.
- Vous êtes propriétaire d'un Compte AWS serveur pour gérer la connexion Direct Connect hébergée avec Megaport.

Configuration de Megaport MVE avec VXC

Le Megaport MVE configuré avec un VXC fournit le segment de réseau privé de couche 2 à. AWS Le MVE est une solution virtuelle qui ne nécessite pas de port. Toutefois, vous devez spécifier le dispositif de réseau virtuel tiers à déployer. Le processus et les fonctionnalités de déploiement de VXC sont les mêmes, que vous utilisiez un port, un MVE ou un MCR. Direct Connect doit être provisionnée en tant que connexion hébergée et attachée à un VIF public.

Pour un aperçu et des instructions étape par étape, consultez la documentation Megaport suivante :

- Présentation de MVE
- Configuration et maintenance des connexions AWS hébergées

Configuration des applications VNF

MVE prend en charge les appliances VNF (Virtual Network Function) tierces de fournisseurs tels qu'Aruba, Cisco, Fortinet, Palo Alto Networks, Versa Networks et VMware. Vous pouvez choisir un fournisseur pour gérer le routage, la sécurité et les fonctions VPN SSL du MVE. Pour obtenir la liste complète des partenaires d'intégration MVE, consultez la documentation de Megaport.

Par exemple, ce cas d'utilisation décrit une architecture de haut niveau dans laquelle Megaport MVE prend en charge les VPN/SD-WAN connexions provenant de succursales régionales et d'utilisateurs distants disposant d'une connexion VPN SSL. Ce MVE correspond à ces connexions AWS et les achemine en privé vers Hyperforce via. Direct Connect

Les principaux éléments de cette architecture sont les suivants :

- Filtres d'itinéraire pour limiter les AWS préfixes pour les instances Hyperforce pertinentes
- Politiques VPN SSL basées sur le nom de domaine complet (FQDN) Hyperforce et les plages d'adresses IP
- Politique NAT pour les utilisateurs d'Hyperforce qui utilisent une adresse IP publique unique qui fait face AWS

Configuration des filtres d'itinéraire

Lorsque le VNF a établi le peering BGP avec le VIF AWS public, la table de routage doit être remplie de préfixes pour tous les services publics et Hyperforce. AWS Vous pouvez appliquer le filtrage des itinéraires à l'aide de listes d'adresses IP ou de balises communautaires BGP. Nous vous recommandons de configurer une feuille de route contenant des préfixes incluant une série d'instances Hyperforce dans un. Région AWS

Remarques :

- Les préfixes BGP annoncés par votre routeur AWS sont configurés Console de gestion AWS lorsque vous créez le VIF public.
- Les préfixes annoncés par ne Direct Connect doivent pas être annoncés au-delà des limites du réseau de votre connexion. Par exemple, ces préfixes ne doivent pas être inclus dans les tables de routage Internet public. Pour plus d'informations, consultez la section Politiques de routage de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration Direct Connect

Accepter une connexion hébergée

Dans votre Compte AWS, acceptez le VXC créé précédemment en tant que connexion hébergée. Pour obtenir des instructions, consultez la Direct Connect documentation.

Création d'un VIF public

Dans votre compte, fournissez un VIF public dans le cadre de la connexion que vous avez acceptée de Megaport. Avant de créer ce VIF, vous devez obtenir les informations suivantes :

- Le BGP ASN de l'appliance VNF.
- Adresses IPv4 publiques pour le peering (généralement `/31` CIDR). Vous pouvez les posséder ou en faire la demande auprès de Support. Pour plus d'informations, consultez la section Adresses IP homologues dans la section Conditions requises pour les interfaces virtuelles de la Direct Connect documentation.

Pour créer un VIF public, suivez les étapes décrites dans la Direct Connect documentation.

Après avoir créé le VIF public, vous devez vous assurer que la clé d'authentification BGP correspond aux deux extrémités de l'homologue BGP pour que l'état de peering soit disponible.

> **Note**
>
> L'utilisation d'un VIF public pour vous connecter AWS depuis votre environnement local modifie la façon dont le trafic est acheminé vers votre site sur site. AWS Nous vous recommandons d'utiliser un filtre de préfixes (feuille de route) pour vous assurer que les préfixes Amazon acceptés sont limités à l'infrastructure Hyperforce et à toutes les autres ressources nécessaires. AWS Pour plus d'informations, consultez la section Règles relatives à la publicité relative au préfixe de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration de Megaport MVE avec SEC

Dans certains cas, les demandes de connexion Hyperforce sont redirigées vers les centres de Salesforce-managed données. Pour conserver ce trafic sur un réseau privé, vous pouvez ajouter un Megaport VXC à Salesforce à l'aide de SEC. Vous pouvez configurer vos politiques de sécurité VNF avec des règles à l'aide du FQDN de connexion Salesforce. Cette Direct Connect architecture est similaire à celle décrite plus haut dans ce guide.

Pour obtenir des instructions détaillées, consultez la section Connexion à Salesforce Express Connect dans la documentation de Megaport.

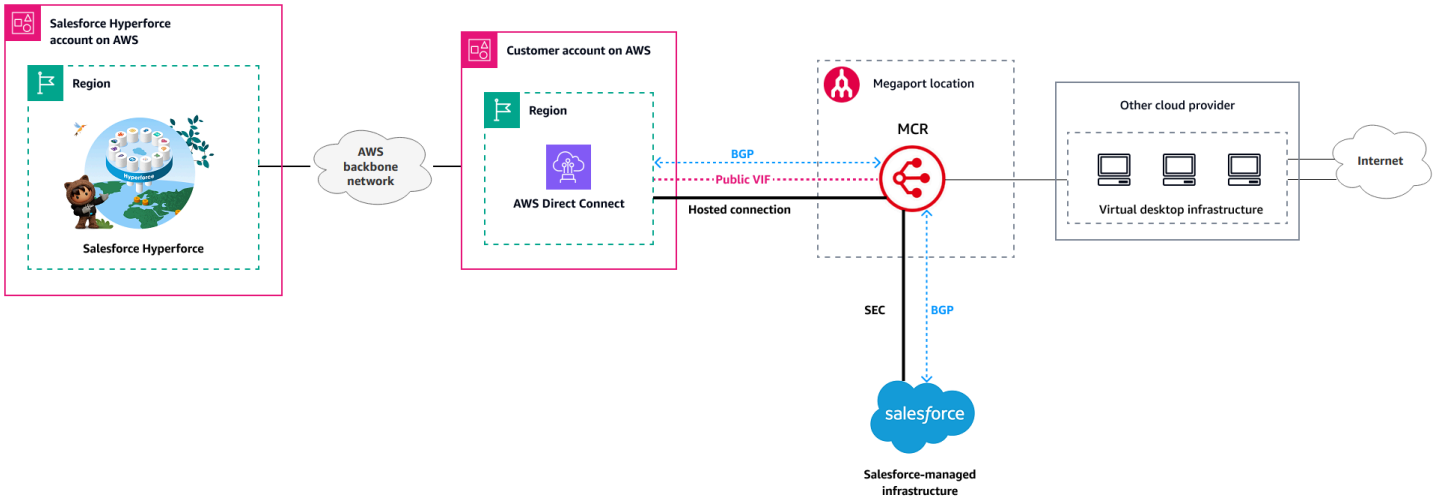
Configuration de Salesforce Hyperforce

Pour activer les connexions entrantes de votre réseau d'entreprise vers Salesforce, vous devez configurer l'accès entrant à Hyperforce par mesure de sécurité. Pour autoriser les domaines requis, suivez les instructions de la section Autoriser les domaines pour une console Salesforce dans Salesforce Classic dans la documentation Salesforce. N'utilisez pas d'adresses IP.

Cas d'utilisation : infrastructure de bureau virtuel multicloud

Ce cas d'utilisation couvre un scénario dans lequel vous disposez d'une infrastructure de bureau virtuel (VDI) exécutée par un autre fournisseur de cloud disposant d'une connexion privée à Megaport et utilisée comme passerelle d'accès pour Direct Connect

L'utilisation de Megaport MCR Direct Connect offre à vos utilisateurs VDI une connectivité privée à Salesforce Hyperforce. Les utilisateurs du VDI utilisent leur ordinateur de bureau pour leur travail quotidien, et le VDI fournit une passerelle d'accès en Direct Connect utilisant un emplacement Megaport.



Exigences

- Les utilisateurs accèdent à Salesforce via des connexions réseau privées.
- Les utilisateurs utilisent un VDI.
- Le VDI fonctionne chez un autre fournisseur de cloud et dispose d'une connexion privée établie avec Megaport.
- Vous êtes propriétaire d'un Compte AWS serveur pour gérer la connexion Direct Connect hébergée avec Megaport.

Configuration de Megaport MCR avec VXC

Pour obtenir des instructions étape par étape, consultez la documentation Megaport suivante :

- Création d'un MCR
- Création de connexions MCR à AWS

Remarques

- Les préfixes BGP annoncés par votre routeur AWS sont configurés Console de gestion AWS lorsque vous créez le VIF public.
- Les préfixes annoncés par ne Direct Connect doivent pas être annoncés au-delà des limites du réseau de votre connexion. Par exemple, ces préfixes ne doivent pas être inclus dans les tables de routage Internet public. Pour plus d'informations, consultez la section Politiques de routage de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration Direct Connect

Accepter une connexion hébergée

Dans votre Compte AWS, acceptez le VXC créé précédemment en tant que connexion hébergée. Pour obtenir des instructions, consultez la Direct Connect documentation.

Création d'un VIF public

Dans votre compte, fournissez un VIF public dans le cadre de la connexion que vous avez acceptée de Megaport. Avant de créer ce VIF, vous devez obtenir les informations suivantes :

- Le BGP ASN du MCR.
- Adresses IPv4 publiques pour le peering (généralement `/31` CIDR). Vous pouvez les posséder ou en faire la demande auprès de Support. Pour plus d'informations, consultez la section Adresses IP homologues dans la section Conditions requises pour les interfaces virtuelles de la Direct Connect documentation.

Pour créer un VIF public, suivez les étapes décrites dans la Direct Connect documentation.

Après avoir créé le VIF public, vous devez vous assurer que la clé d'authentification BGP correspond aux deux extrémités de l'homologue BGP pour que l'état de peering soit disponible.

Note

L'utilisation d'un VIF public pour vous connecter AWS depuis votre environnement sur site ou multicloud modifie la façon dont le trafic est acheminé des préfixes AWS publics vers vos

utilisateurs. Nous vous recommandons d'utiliser un filtre de préfixes (feuille de route) pour vous assurer que les préfixes Amazon acceptés sont limités à l'infrastructure Hyperforce et à toutes les autres ressources nécessaires. AWS Pour plus d'informations, consultez la section Règles relatives à la publicité relative au préfixe de l'interface virtuelle publique dans la Direct Connect documentation.

Configuration de Megaport MCR avec SEC

Pour obtenir des instructions détaillées, consultez la section Création de connexions MCR à Salesforce Express Connect dans la documentation de Megaport.

Configuration de Salesforce Hyperforce

Pour activer les connexions entrantes de votre réseau d'entreprise vers Salesforce, vous devez configurer l'accès entrant à Hyperforce par mesure de sécurité. Pour autoriser les domaines requis, suivez les instructions de la section Autoriser les domaines pour une console Salesforce dans Salesforce Classic dans la documentation Salesforce. N'utilisez pas d'adresses IP.

Tarification

Les considérations financières relatives aux solutions décrites dans ce guide dépendent de divers facteurs, tels que l'échelle, la bande passante consommée, les produits sélectionnés et les remises des fournisseurs. Lorsque vous fixez le prix des différents composants, tenez compte des points suivants :

- Direct Connect — Le prix varie en fonction de la région, du type de port, de la capacité et des données transférées. Utilisez le Calculateur de tarification AWSpour estimer vos coûts.
- Connexion hébergée Megaport à AWS — Le prix varie en fonction de l'utilisation et de la capacité du produit. Megaport PortMVE, et MCR sont disponibles directement auprès de Megaport ou peuvent être achetés via. AWS Marketplace
- Megaport SEC — Ceci est disponible directement via Megaport.
- Salesforce Hyperforce : il est disponible directement via Salesforce.

Ressources

Documentation AWS

- Direct Connect
- Direct Connect Guide de l'utilisateur

Documentation Megaport

- Création d'un port
- Configuration et maintenance des connexions AWS hébergées
- Vue d'ensemble des connexions
- Vue d'ensemble du MCR
- Présentation de MVE
- Connexion à Salesforce Express Connect

Documentation Salesforce

- Présentation d'Hyperforce — Informations générales et FAQ
- Autoriser les domaines pour une console Salesforce dans Salesforce Classic
- Autoriser les domaines requis

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un RSSfil RSS.

Modification	Description	Date
Publication initiale	—	30 août 2024

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.