AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

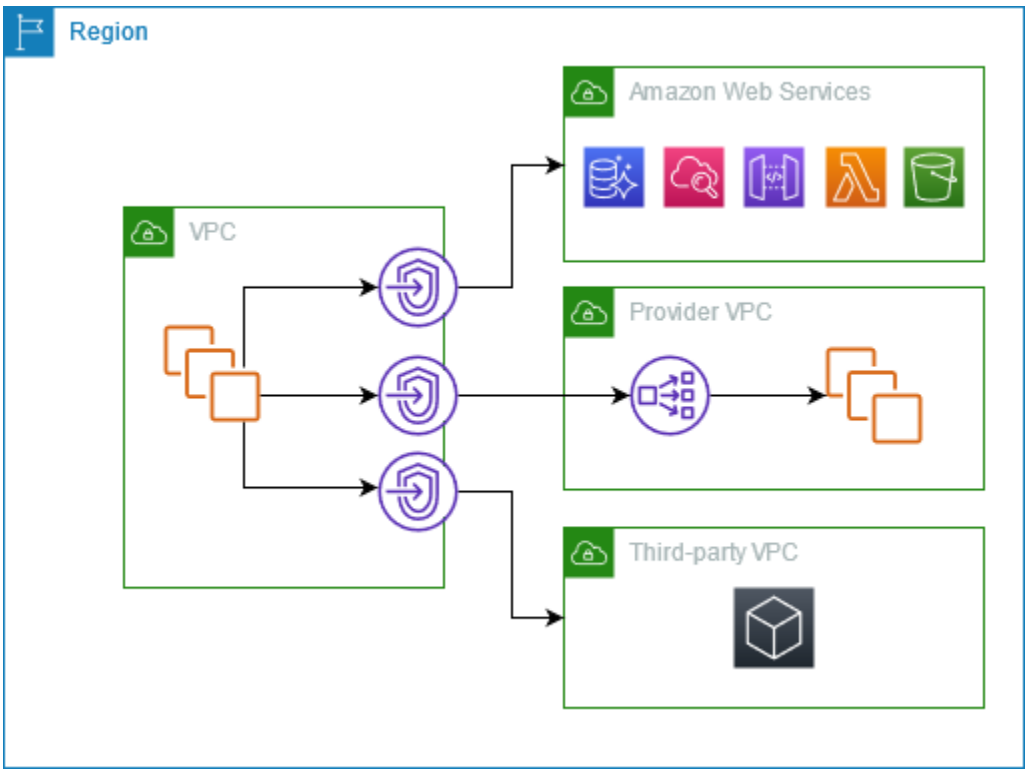
Qu'est-ce que c'est AWS PrivateLink ?

AWS PrivateLink est une technologie hautement disponible et évolutive que vous pouvez utiliser pour vous connecter en privé à des services et VPC à des ressources comme s'ils se trouvaient dans votre environnementVPC. Il n'est pas nécessaire d'utiliser une passerelle Internet, un NAT appareil, une adresse IP publique, une AWS Direct Connect connexion ou une AWS Site-to-Site VPN connexion pour autoriser la communication avec le service ou la ressource depuis vos sous-réseaux privés. Par conséquent, vous contrôlez les API points de terminaison, les sites, les services et les ressources spécifiques accessibles depuis votreVPC.

Cas d’utilisation

Vous pouvez créer des VPC points de terminaison pour connecter les clients de votre entreprise VPC à des services et à des ressources qui s'intègrent à AWS PrivateLink. Vous pouvez créer votre propre service de VPC point de terminaison et le mettre à la disposition d'autres AWS clients. Pour de plus amples informations, veuillez consulter the section called “Concepts”.

Dans le schéma suivant, VPC sur la gauche, vous trouverez plusieurs EC2 instances Amazon dans un sous-réseau privé et cinq points de terminaison : trois VPC points de terminaison d'interface, un point de VPC terminaison de ressource et un point de VPC terminaison de réseau de services. VPC Le premier point de VPC terminaison de l'interface se connecte à un AWS service. Le point de VPC terminaison de la deuxième interface se connecte à un service hébergé par un autre AWS compte (un service de VPC point de terminaison). Le point de VPC terminaison de la troisième interface se connecte à un service partenaire AWS Marketplace. Le point de VPC terminaison de la ressource se connecte à une base de données. Le point de VPC terminaison du réseau de service se connecte à un réseau de service.



En savoir plus

- the section called “Concepts”
- Accès Services AWS
- Accès aux produits SaaS
- Accès à des dispositifs virtuels
- Partage des services

Travailler avec des VPC endpoints

Vous pouvez créer, accéder et gérer des VPC points de terminaison à l'aide de l'une des méthodes suivantes :

- AWS Management Console— Fournit une interface Web que vous pouvez utiliser pour accéder à vos AWS PrivateLink ressources. Ouvrez la VPC console Amazon et choisissez Endpoints ou Endpoint services.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de Services AWS, y compris AWS PrivateLink. Pour plus d'informations sur les commandes pour AWS PrivateLink, consultez ec2 dans la référence des AWS CLI commandes.

- AWS CloudFormation - Créez des modèles qui décrivent vos AWS ressources. Vous utilisez les modèles pour provisionner et gérer ces ressources comme une seule unité. Pour plus d'informations, consultez les AWS PrivateLink ressources suivantes :
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS: : ElasticLoadBalancing V2 : : LoadBalancer
- AWS SDKs— Fournissez des informations spécifiques à la langueAPIs. Ils SDKs prennent en charge de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour de plus amples informations, veuillez consulter Outils pour créer sur AWS.
- Requête API — Fournit des API actions de bas niveau que vous appelez à l'aide de HTTPS requêtes. L'utilisation de la requête API est le moyen le plus direct d'accéder à AmazonVPC. Toutefois, il faut alors que votre application gère les détails de bas niveau, notamment la génération du hachage pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez AWS PrivateLink les actions dans le Amazon EC2 API Reference.

Tarification

Pour plus d'informations sur la tarification des VPC terminaux, consultez la section AWS PrivateLink Tarification.

AWS PrivateLink concepts

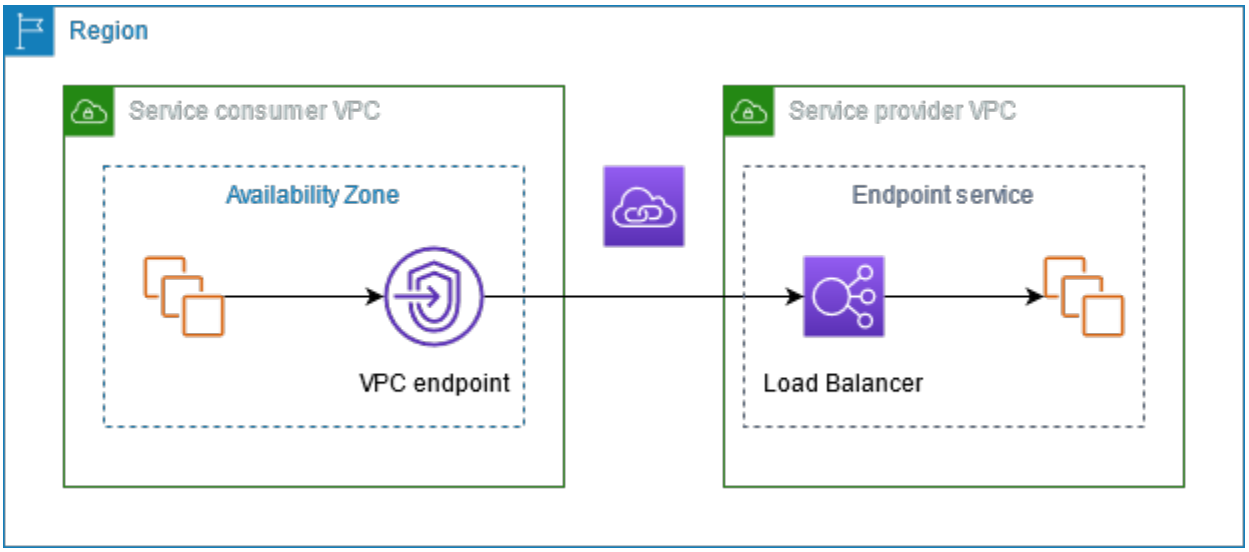
Vous pouvez utiliser Amazon VPC pour définir un cloud privé virtuel (VPC), qui est un réseau virtuel isolé de manière logique. Vous pouvez autoriser vos clients VPC à se connecter à d'autres destinationsVPC. Par exemple, ajoutez une passerelle Internet au VPC pour autoriser l'accès à Internet, ou ajoutez une VPN connexion pour autoriser l'accès à votre réseau local. Vous pouvez également l'utiliser AWS PrivateLink pour permettre aux clients de vous connecter VPC à des services et à des ressources dans d'autres VPCs pays en utilisant des adresses IP privées, comme si ces services et ressources étaient hébergés directement dans votreVPC.

Les concepts suivants sont importants à comprendre lorsque vous commencez à utiliser AWS PrivateLink.

Table des matières

Diagramme d'architecture

Le schéma suivant fournit une vue d'ensemble détaillée du AWS PrivateLink fonctionnement. Les consommateurs créent des VPC points de terminaison pour se connecter aux services et ressources des terminaux hébergés par les fournisseurs.



Fournisseurs

Comprenez les concepts liés à un fournisseur.

Prestataire de services

Le propriétaire d'un service est le fournisseur du service. Les fournisseurs de services incluent AWS AWS les partenaires et autres Comptes AWS. Les fournisseurs de services peuvent héberger leurs services à l'aide de AWS ressources, telles que EC2 des instances, ou de serveurs sur site.

Fournisseur de ressources

Le propriétaire d'une ressource, par exemple une base de données, un cluster de nœuds ou une instance, est le fournisseur de ressources. Les fournisseurs de ressources incluent AWS les services, AWS les partenaires et les autres AWS comptes. Les fournisseurs de ressources peuvent héberger leurs ressources sur site VPCs ou sur site.

Concepts

- Services de point de terminaison
- Noms de service
- États de service
- Configuration des ressources
- Passerelle de ressources

Services de point de terminaison

Le fournisseur du service crée un service de point de terminaison pour rendre son service disponible dans une Région. Le fournisseur du service doit spécifier un équilibreur de charge lorsqu'il crée un service de point de terminaison. L'équilibreur de charge reçoit des requêtes des consommateurs du service et les achemine vers votre service.

Par défaut, votre service de point de terminaison n'est pas disponible pour les consommateurs du service. Vous devez ajouter des autorisations permettant à des entités spécifiques de AWS se connecter à votre service de point de terminaison.

Noms de service

Chaque service de point de terminaison est identifié par un nom de service. Un consommateur de services doit spécifier le nom du service lors de la création d'un VPC point de terminaison. Les consommateurs de services peuvent demander les noms des services pour Services AWS. Les fournisseurs du service doivent communiquer le nom de leurs services aux consommateurs du service.

États de service

Les états possibles pour un service de point de terminaison sont les suivants :

- `Pending` – Le service de point de terminaison est en cours de création.

- `Available` – Le service de point de terminaison est disponible.
- `Failed` – Le service de point de terminaison n'a pas pu être créé.
- `Deleting` – Le fournisseur du service a supprimé le service de point de terminaison et la suppression est en cours.
- `Deleted` – Le service de point de terminaison est supprimé.

Configuration des ressources

Le fournisseur de ressources crée une configuration de ressource pour partager une ressource. Une configuration de ressources est un objet logique qui représente soit une ressource unique telle qu'une base de données, soit un groupe de ressources tel qu'un cluster de nœuds. Une ressource peut être une adresse IP, un nom de domaine cible ou une base de données AmazonRDS.

Lors du partage avec d'autres comptes, le fournisseur de ressources doit partager la ressource via un partage de AWS RAM ressources pour permettre AWS aux principaux spécifiques de l'autre compte de se connecter à la ressource via un point de VPC terminaison de ressource.

Les configurations de ressources peuvent être associées à un réseau de service auquel les principaux se connectent via un point de terminaison du réseau de services. VPC

Passerelle de ressources

Une passerelle de ressources est un point d'entrée vers un point VPC d'où une ressource est partagée. Le fournisseur crée une passerelle de ressources pour partager les ressources à partir duVPC.

Consommateurs de services ou de ressources

L'utilisateur d'un service ou d'une ressource est un consommateur. Les consommateurs peuvent accéder aux services et aux ressources des terminaux depuis leur site VPCs ou depuis leur site.

Concepts

- Points de terminaison VPC
- Interfaces réseau de point de terminaison
- Politiques de point de terminaison
- États de point de terminaison

Points de terminaison VPC

Un consommateur crée un VPCpoint de terminaison pour le connecter à un service ou VPC à une ressource de point de terminaison. Un consommateur doit spécifier le service, la ressource ou le réseau de services du point de terminaison lors de la création d'un VPC point de terminaison. Il existe plusieurs types de VPC points de terminaison. Vous devez créer le type de VPC point de terminaison dont vous avez besoin.

- `Interface`- Créez un point de terminaison d'interface à envoyer TCP ou à envoyer UDP du trafic vers un service de point de terminaison. Le trafic destiné au service de point de terminaison est résolu à l'aide deDNS.
- `GatewayLoadBalancer` – Créer un Point de terminaison d'équilibreur de charge de passerelle pour envoyer le trafic vers une flotte de dispositifs virtuels en utilisant des adresses IP privées. Vous acheminez le trafic de votre point de terminaison Gateway Load Balancer VPC à l'aide de tables de routage. L'équilibreur de charge de passerelle distribue le trafic vers les dispositifs virtuels et peut s'adapter à la demande.
- `Resource`- Créez un point de terminaison de ressource pour accéder à une ressource qui a été partagée avec vous et qui réside dans une autreVPC. Un point de terminaison de ressources vous permet d'accéder de manière privée et sécurisée à des ressources telles qu'une base de données, un cluster de nœuds, une instance, un point de terminaison d'application, une cible de nom de domaine ou une adresse IP qui peut se trouver dans un sous-réseau privé dans un autre environnement VPC ou dans un environnement sur site. Les points de terminaison des ressources ne nécessitent pas d'équilibreur de charge et vous permettent d'accéder directement à la ressource.
- `Service network`- Créez un point de terminaison de réseau de services pour accéder à un réseau de services que vous avez créé ou qui a été partagé avec vous. Vous pouvez utiliser un seul point de terminaison de réseau de services pour accéder de manière privée et sécurisée à plusieurs ressources et services associés à un réseau de services.

Il existe un autre type de VPC point de terminaison`Gateway`, qui crée un point de terminaison passerelle pour envoyer du trafic vers Amazon S3 ou DynamoDB. Les points de terminaison de la passerelle ne l'utilisent pas AWS PrivateLink, contrairement aux autres types de points de VPC terminaison. Pour de plus amples informations, veuillez consulter the section called “Points de terminaison de passerelle”.

Interfaces réseau de point de terminaison

Une interface réseau de point de terminaison est une interface réseau gérée par le demandeur qui sert de point d'entrée pour le trafic destiné à un service, une ressource ou un réseau de services de point de terminaison. Pour chaque sous-réseau que vous spécifiez lorsque vous créez un VPC point de terminaison, nous créons une interface réseau de point de terminaison dans le sous-réseau.

Si un VPC point de terminaison est compatibleIPv4, ses interfaces réseau de points de terminaison possèdent IPv4 des adresses. Si un VPC point de terminaison est compatibleIPv6, ses interfaces réseau de points de terminaison possèdent IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison n'est pas accessible depuis Internet. Lorsque vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Politiques de point de terminaison

Une politique de VPC point de terminaison est une politique de IAM ressources que vous attachez à un VPC point de terminaison. Il détermine quels principaux peuvent utiliser le VPC point de terminaison pour accéder au service de point de terminaison. La politique de VPC point de terminaison par défaut autorise toutes les actions de tous les principaux sur toutes les ressources du VPC point de terminaison.

États de point de terminaison

Lorsque vous créez un point de VPC terminaison d'interface, le service de point de terminaison reçoit une demande de connexion. Le fournisseur du service peut accepter ou refuser la demande. Si le fournisseur de services accepte la demande, le consommateur de services peut utiliser le VPC point de terminaison une fois que celui-ci est entré dans l'`Available`état.

Les états possibles d'un point de VPC terminaison sont les suivants :

- `PendingAcceptance` – La demande de connexion est en attente. Il s'agit de l'état initial si les demandes sont acceptées manuellement.
- `Pending` – Le fournisseur du service a accepté la demande de connexion. Il s'agit de l'état initial si les demandes sont acceptées automatiquement. Le VPC point de terminaison revient à cet état si le client du service le VPC modifie.
- `Available`- Le VPC terminal est prêt à être utilisé.
- `Rejected` – Le fournisseur du service a refusé la demande de connexion. Le fournisseur du service peut également refuser une connexion lorsqu'elle est disponible pour utilisation.

- `Expired` – La demande de connexion a expiré.
- `Failed`- Le VPC point de terminaison n'a pas pu être mis à disposition.
- `Deleting`- Le client du service a supprimé le VPC terminal et la suppression est en cours.
- `Deleted`- Le VPC point de terminaison est supprimé.

AWS PrivateLink connexions

Le trafic provenant de vous VPC est envoyé vers un service ou une ressource de point de terminaison via une connexion entre le VPC point de terminaison et le service ou la ressource de point de terminaison. Le trafic entre un VPC point de terminaison et un service ou une ressource de point de terminaison reste au sein du AWS réseau, sans passer par l'Internet public.

Un fournisseur de services ajoute des autorisations afin que les consommateurs puissent accéder au service de point de terminaison. Les consommateurs de services initient la connexion et le fournisseur de services accepte ou rejette les demandes de connexion. Un propriétaire de ressource ou un propriétaire de réseau de services partage une configuration de ressources ou un réseau de services avec les consommateurs AWS Resource Access Manager afin que les consommateurs puissent accéder au réseau de ressources ou de services.

Avec les VPC points de terminaison d'interface, les consommateurs peuvent utiliser des politiques relatives aux terminaux pour contrôler quels IAM principaux peuvent utiliser un VPC point de terminaison pour accéder à un service ou à une ressource de point de terminaison.

Zones hébergées privées

Une zone hébergée est un conteneur d'DNSenregistrements qui définit le mode d'acheminement du trafic pour un domaine ou un sous-domaine. Avec une zone hébergée publique, les enregistrements précisent comment acheminer le trafic sur Internet. Dans le cas d'une zone hébergée privée, les enregistrements indiquent comment acheminer le trafic dans votreVPCs.

Vous pouvez configurer Amazon Route 53 pour acheminer le trafic du domaine vers un VPC point de terminaison. Pour plus d'informations, consultez la section Routage du trafic vers un VPC point de terminaison à l'aide de votre nom de domaine.

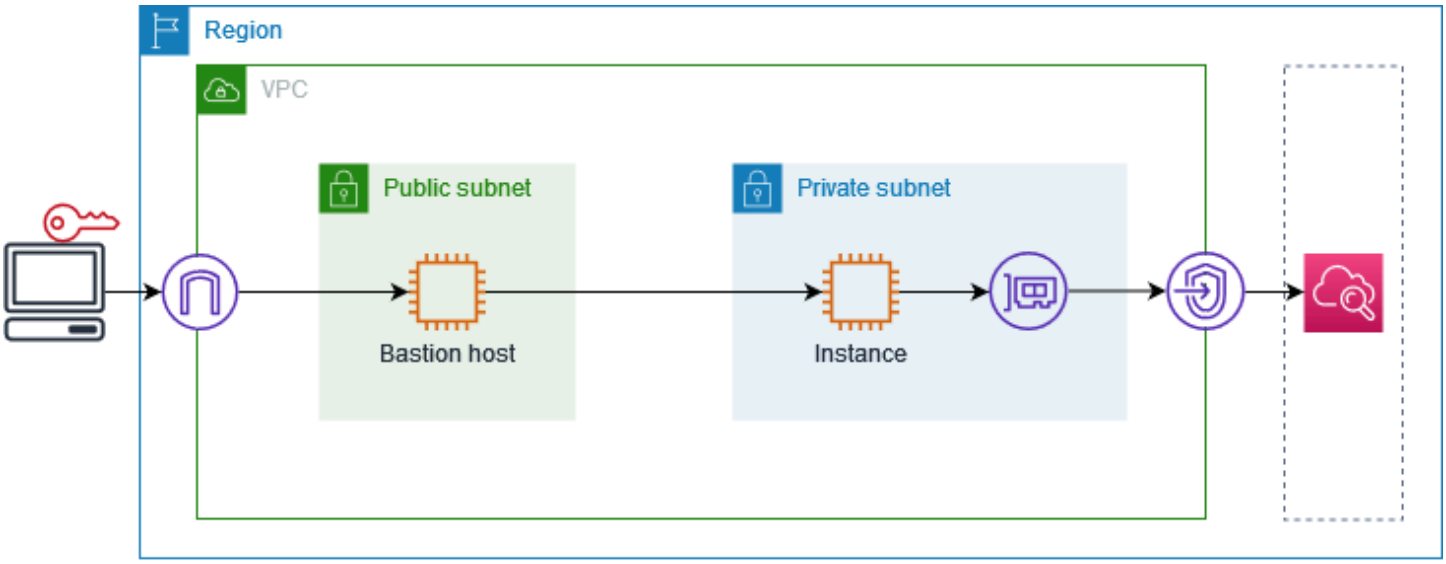
Vous pouvez utiliser Route 53 pour configurer Split-HorizonDNS, en utilisant le même nom de domaine pour un site Web public et un service de point de terminaison alimenté par. AWS PrivateLink DNSles demandes de nom d'hôte public émanant du consommateur sont VPC résolues vers les adresses IP privées des interfaces réseau des terminaux, mais les demandes provenant

de l'extérieur VPC continuent d'être résolues vers les points de terminaison publics. Pour plus d'informations, consultez DNSMécanismes de routage du trafic et activation du basculement pour les AWS PrivateLink déploiements.

Commencez avec AWS PrivateLink

Ce didacticiel explique comment envoyer une demande depuis une EC2 instance d'un sous-réseau privé à Amazon à CloudWatch l'aide AWS PrivateLink de.

Le schéma suivant fournit un aperçu de ce scénario. Pour vous connecter depuis votre ordinateur à l'instance dans le sous-réseau privé, vous devez d'abord vous connecter à un hôte bastion dans un sous-réseau public. L'hôte bastion et l'instance doivent utiliser la même paire de clés. Comme le `.pem` fichier de la clé privée se trouve sur votre ordinateur, et non sur l'hôte de Bastion, vous allez utiliser le transfert de SSH clé. Vous pouvez ensuite vous connecter à l'instance depuis l'hôte bastion sans spécifier le fichier `.pem` dans la commande ssh. Une fois que vous avez configuré un VPC point de terminaison pour CloudWatch, le trafic provenant de l'instance à laquelle il est destiné CloudWatch est résolu vers l'interface réseau du point de terminaison, puis envoyé à CloudWatch l'aide du VPC point de terminaison.



À des fins de test, vous pouvez utiliser une zone de disponibilité unique. En production, nous vous recommandons d'utiliser au moins deux zones de disponibilité pour une faible latence et une haute disponibilité.

Tâches

- Étape 1 : créer un VPC avec des sous-réseaux
- Étape 2 : Lancer les instances
- Étape 3 : Tester CloudWatch l'accès
- Étape 4 : créer un VPC point de terminaison auquel accéder CloudWatch

Étape 1 : créer un VPC avec des sous-réseaux

Utilisez la procédure suivante pour créer un VPC avec un sous-réseau public et un sous-réseau privé.

Pour créer le VPC

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez CreateVPC (Créer).
3. Pour que Resources crée, choisissez VPCet plus encore.
4. Pour la génération automatique du tag Name, entrez un nom pour leVPC.
5. Pour configurer les sous-réseaux, procédez comme suit :
    a. Pour Number of Availability Zones (Nombre de zones de disponibilité), choisissez 1 ou 2, selon vos besoins.
    b. Pour Number of public subnets (Nombre de sous-réseaux publics), assurez-vous de disposer d'un sous-réseau public par zone de disponibilité.
    c. Pour Number of private subnets (Nombre de sous-réseaux privés), assurez-vous de disposer d'un sous-réseau privé par zone de disponibilité.
6. Sélectionnez CreateVPC (Créer).

Étape 2 : Lancer les instances

À l'aide de VPC celui que vous avez créé à l'étape précédente, lancez l'hôte bastion dans le sous-réseau public et l'instance dans le sous-réseau privé.

Prérequis

- Créez une paire de clés à l'aide du format .pem. Vous devez choisir cette paire de clés lorsque vous lancez à la fois l'hôte bastion et l'instance.
- Créez un groupe de sécurité pour l'hôte Bastion qui autorise le SSH trafic entrant depuis le CIDR bloc de votre ordinateur.

- Créez un groupe de sécurité pour l'instance qui autorise le SSH trafic entrant depuis le groupe de sécurité pour l'hôte Bastion.
- Créez un profil d'IAMinstance et associez la CloudWatchReadOnlyAccesspolitique.

Pour lancer l'hôte bastion

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Launch Instance.
3. Dans Name (Nom), saisissez un nom pour votre hôte bastion.
4. Conservez l'image et le type d'instance par défaut.
5. Pour Key pair (Paire de clés), choisissez votre paire de clés.
6. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
    a. Pour VPC, choisissez votreVPC.
    b. Pour Subnet (Sous-réseau), sélectionnez votre sous-réseau public.
    c. Pour Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).
    d. Pour Firewall (Pare-feu), choisissez Select existing security group (Sélectionner un groupe de sécurité existant), puis choisissez le groupe de sécurité pour l'hôte bastion.
7. Choisissez Launch Instance.

Pour lancer l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Launch Instance.
3. Pour Name (Nom), saisissez un nom pour votre instance.
4. Conservez l'image et le type d'instance par défaut.
5. Pour Key pair (Paire de clés), choisissez votre paire de clés.
6. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
    a. Pour VPC, choisissez votreVPC.
    b. Pour Subnet (Sous-réseau), choisissez private subnet (Sous-réseau privé).
    c. Pour Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Disable (Désactiver).

   d. Pour Firewall (Pare-feu), choisissez Select existing security group (Sélectionner un groupe de sécurité existant), puis choisissez le groupe de sécurité pour l'instance.

7. Développez Advanced Details (Détails avancés). IAMPar profil d'instance, choisissez votre profil d'IAMinstance.
8. Choisissez Launch instance (Lancer une instance).

Étape 3 : Tester CloudWatch l'accès

Utilisez la procédure suivante pour vérifier que l'instance ne peut pas y accéder CloudWatch. Pour ce faire, utilisez une AWS CLI commande en lecture seule pour. CloudWatch

Pour tester CloudWatch l'accès

1. Depuis votre ordinateur, ajoutez la paire de clés à l'SSHagent à l'aide de la commande suivante, où se *key.pem* trouve le nom de votre fichier .pem.

   ```
   ssh-add ./key.pem
   ```

   Si vous recevez un message d'erreur indiquant que les autorisations pour votre paire de clés sont trop ouvertes, exécutez la commande suivante, puis réessayez la commande précédente.

   ```
   chmod 400 ./key.pem
   ```

2. Connexion à l'hôte bastion depuis votre ordinateur. Vous devez spécifier l'option `-A`, le nom d'utilisateur de l'instance (par exemple `ec2-user`) et l'adresse IP publique de l'hôte bastion.

   ```
   ssh -A ec2-user@bastion-public-ip-address
   ```

3. Connexion à l'instance depuis l'hôte bastion. Vous devez spécifier le nom d'utilisateur de l'instance (par exemple `ec2-user`) et l'adresse IP privée de l'instance.

   ```
   ssh ec2-user@instance-private-ip-address
   ```

4. Exécutez la commande CloudWatch list-metrics sur l'instance comme suit. Pour l'`--region`option, spécifiez la région dans laquelle vous avez créé leVPC.

   ```
   aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
   ```

5. Après quelques minutes, la commande expire. Cela montre que vous ne pouvez pas y accéder CloudWatch depuis l'instance avec la VPC configuration actuelle.

```
Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
```

6. Restez connecté à votre instance. Après avoir créé le VPC point de terminaison, vous allez réessayer cette list-metrics commande.

Étape 4 : créer un VPC point de terminaison auquel accéder CloudWatch

Utilisez la procédure suivante pour créer un VPC point de terminaison qui se connecte à CloudWatch.

Prérequis

Créez un groupe de sécurité pour le VPC point de terminaison qui autorise le trafic à CloudWatch. Par exemple, ajoutez une règle qui autorise le HTTPS trafic provenant du VPC CIDR bloc.

Pour créer un VPC point de terminaison pour CloudWatch

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Sous Name (Nom), saisissez un nom pour le point de terminaison.
5. Pour Service category (Catégorie de service), choisissez Services AWS.
6. Pour Service, sélectionnez com.amazonaws. ***region***.surveillance.
7. Pour VPC, sélectionnez votreVPC.
8. Pour Subnets (Sous-réseaux), sélectionnez la zone de disponibilité puis le sous-réseau privé.
9. Pour Groupe de sécurité, sélectionnez le groupe de sécurité pour le VPC point de terminaison.
10. Pour Policy, sélectionnez Accès complet pour autoriser toutes les opérations effectuées par tous les principaux sur toutes les ressources du VPC point de terminaison.
11. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.

12. Choisissez Créer un point de terminaison. Le statut initial est Pending (En attente). Avant de passer à l'étape suivante, attendez que le statut soit Disponible. Cette opération peut prendre quelques minutes.

Étape 5 : tester le VPC point de terminaison

Vérifiez que le VPC point de terminaison envoie des demandes depuis votre instance à CloudWatch.

Pour tester le VPC point de terminaison

Exécutez la commande suivante sur votre instance. Pour l'`--region`option, spécifiez la région dans laquelle vous avez créé le VPC point de terminaison.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

Si vous obtenez une réponse, même une réponse avec des résultats vides, vous êtes connecté à CloudWatch l'utilisation de AWS PrivateLink.

Si un `UnauthorizedOperation` message d'erreur s'affiche, assurez-vous que l'instance possède un IAM rôle autorisant l'accès à CloudWatch.

Si le délai de la demande expire, vérifiez les points suivants :

- Le groupe de sécurité du point de terminaison autorise le trafic à CloudWatch.
- L'`--region`option indique la région dans laquelle vous avez créé le VPC point de terminaison.

Étape 6 : Nettoyage

Si vous n'avez plus besoin de l'hôte bastion et de l'instance que vous avez créés pour ce didacticiel, vous pouvez y mettre fin.

Pour résilier les instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez les deux instances de test, choisissez Instance state) (État de l'instance, Terminate instance (Résilier l'instance).
4. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Si vous n'avez plus besoin du VPC point de terminaison, vous pouvez le supprimer.

Pour supprimer le point de VPC terminaison

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le VPC point de terminaison.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Accès Services AWS via AWS PrivateLink

Vous accédez à un point de terminaison et vous Service AWS l'utilisez. Les points de terminaison de service par défaut sont des interfaces publiques. Vous devez donc ajouter une passerelle Internet à votre interface VPC afin que le trafic puisse passer du VPC au Service AWS. Si cette configuration ne répond pas aux exigences de sécurité de votre réseau, vous pouvez l'utiliser AWS PrivateLink pour vous VPC connecter Services AWS comme si elles se trouvaient dans le vôtreVPC, sans passer par une passerelle Internet.

Vous pouvez accéder en privé à ceux Services AWS qui s'intègrent à l' AWS PrivateLink utilisation des VPC points de terminaison. Vous pouvez créer et gérer toutes les couches de votre pile d'applications sans utiliser de passerelle Internet.

Tarification

Vous êtes facturé pour chaque heure pendant laquelle votre point de VPC terminaison d'interface est mis en service dans chaque zone de disponibilité. Vous êtes également facturé par Go de données traitées. Pour plus d'informations, consultez AWS PrivateLink Pricing (Tarification CTlong).

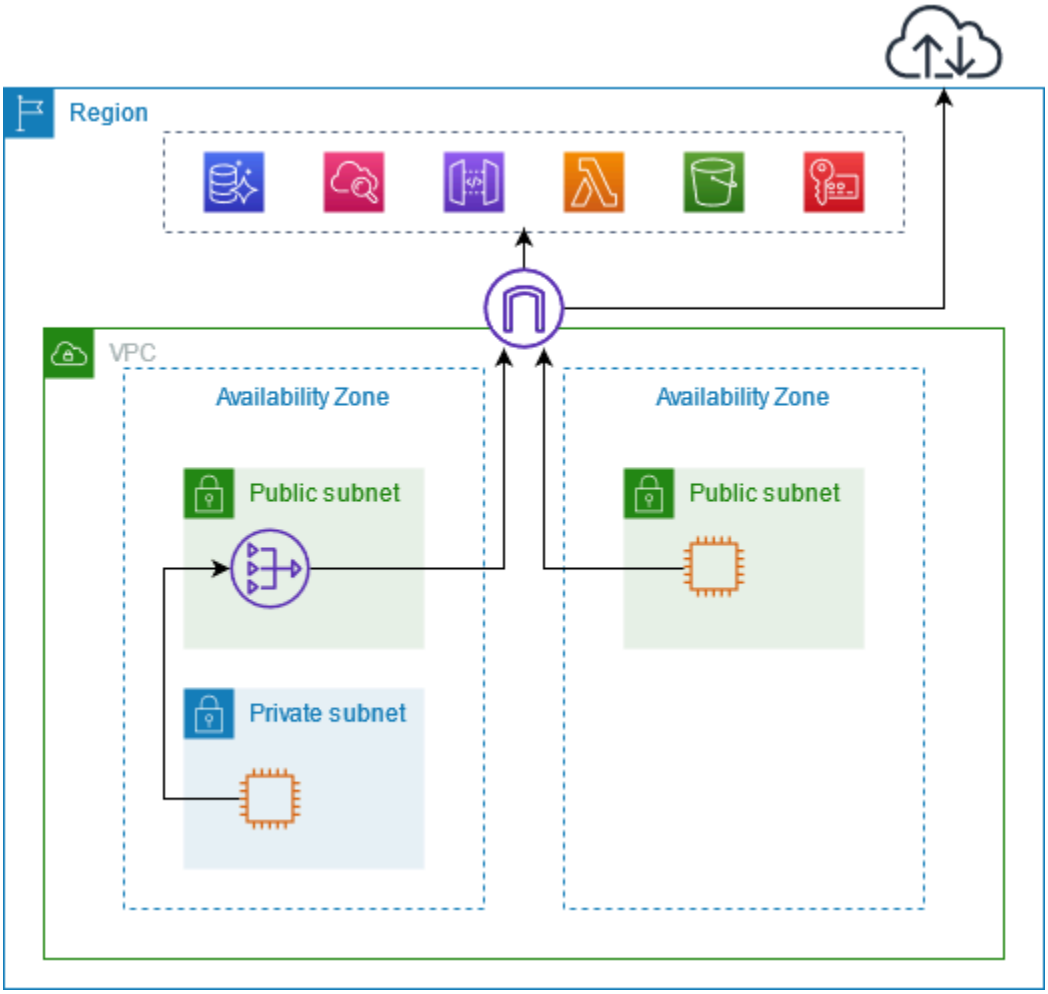
Table des matières

Présentation

Vous pouvez y accéder Services AWS via leurs points de terminaison de service public ou vous connecter à une Services AWS utilisation AWS PrivateLink prise en charge. Cette vue d'ensemble compare ces méthodes.

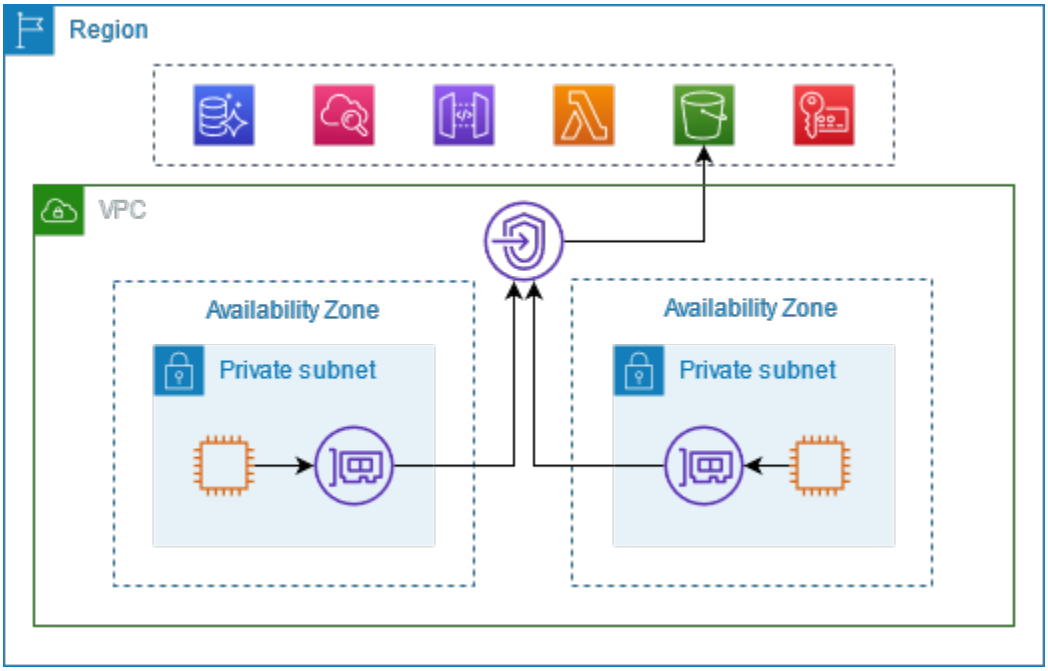
Accès via des points de terminaison de service public

Le schéma suivant montre comment les instances accèdent Services AWS via les points de terminaison du service public. Le trafic à destination et en Service AWS provenance d'une instance d'un sous-réseau public est acheminé vers la passerelle Internet pour le, VPC puis vers le. Service AWS Le trafic à destination et en Service AWS provenance d'une instance d'un sous-réseau privé est acheminé vers une NAT passerelle, puis vers la passerelle Internet duVPC, puis vers le. Service AWS Lorsque ce trafic traverse la passerelle Internet, il ne quitte pas le AWS réseau.



Connect via AWS PrivateLink

Le schéma suivant montre comment les instances y Services AWS accèdent AWS PrivateLink. Tout d'abord, vous créez un point de VPC terminaison d'interface, qui établit des connexions entre les sous-réseaux de votre interface réseau VPC et ceux de vos interfaces réseau d' Service AWS utilisation. Le trafic destiné au Service AWS est résolu vers les adresses IP privées des interfaces réseau du point de terminaison à l'aide deDNS, puis envoyé à l' Service AWS aide de la connexion entre le VPC point de terminaison et le Service AWS.



Services AWS accepte automatiquement les demandes de connexion. Le service ne peut pas lancer de demandes de ressources via le VPC point de terminaison.

DNSnoms d'hôtes

La plupart Services AWS proposent des points de terminaison régionaux publics, dont la syntaxe est la suivante.

```
protocol://service_code.region_code.amazonaws.com
```

Par exemple, le point de terminaison public pour Amazon CloudWatch dans us-east-2 est le suivant.

```
https://monitoring.us-east-2.amazonaws.com
```

Avec AWS PrivateLink, vous envoyez du trafic vers le service à l'aide de points de terminaison privés. Lorsque vous créez un point de VPC terminaison d'interface, nous créons des DNS noms régionaux et zonaux que vous pouvez utiliser pour communiquer avec le Service AWS depuis votreVPC.

Le DNS nom régional du point de VPC terminaison de votre interface a la syntaxe suivante :

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

La syntaxe des DNS noms de zone est la suivante :

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

Lorsque vous créez un point de VPC terminaison d'interface pour un Service AWS, vous pouvez activer le mode privé DNS. Avec le mode privéDNS, vous pouvez continuer à envoyer des demandes à un service en utilisant le DNS nom de son point de terminaison public, tout en tirant parti de la connectivité privée via le point de VPC terminaison de l'interface. Pour de plus amples informations, veuillez consulter the section called “DNSrésolution”.

La describe-vpc-endpointscommande suivante affiche les DNS entrées d'un point de terminaison d'interface.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

Voici un exemple de sortie pour un point de terminaison d'interface pour Amazon CloudWatch avec DNS les noms privés activés. La première entrée est le point de terminaison régional privé. Les trois entrées suivantes sont les points de terminaison zonaux privés. La dernière entrée provient de la zone hébergée privée cachée, qui résout les requêtes adressées au point de terminaison public en adresses IP privées des interfaces réseau du point de terminaison.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
```

```
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

DNSrésolution

Les DNS enregistrements que nous créons pour le point de VPC terminaison de votre interface sont publics. Par conséquent, ces DNS noms peuvent être résolus publiquement. Cependant, les DNS demandes provenant de l'extérieur renvoient VPC toujours les adresses IP privées des interfaces réseau des terminaux, de sorte que ces adresses IP ne peuvent pas être utilisées pour accéder au service des points de terminaison à moins que vous n'ayez accès auVPC.

Privé DNS

Si vous activez le mode privé DNS pour le point de VPC terminaison de votre VPC interface et que vous avez activé à la fois les DNSnoms d'hôte et la DNS résolution, nous créons pour vous une zone hébergée privée masquée et AWS gérée. La zone hébergée contient un ensemble d'enregistrements pour le DNS nom par défaut du service qui le résout en adresses IP privées des interfaces réseau des terminaux de votreVPC. Par conséquent, si vous avez des applications existantes qui envoient des demandes à l' Service AWS aide d'un point de terminaison régional public, ces demandes passent désormais par les interfaces réseau du point de terminaison, sans que vous ayez à apporter de modifications à ces applications.

Nous vous recommandons d'activer les DNS noms privés pour vos VPC points de terminaison pour Services AWS. Cela garantit que les demandes qui utilisent les points de terminaison du service

public, telles que les demandes effectuées via un AWS SDK, sont résolues vers votre VPC point de terminaison.

Amazon met à votre VPC disposition un DNS serveur appelé Route 53 Resolver. Le résolveur Route 53 résout automatiquement les noms de VPC domaine locaux et les enregistre dans des zones hébergées privées. Cependant, vous ne pouvez pas utiliser le résolveur Route 53 depuis l'extérieur de votreVPC. Si vous souhaitez accéder à votre VPC point de terminaison depuis votre réseau local, vous pouvez utiliser les points de terminaison Route 53 Resolver et les règles du résolveur. Pour plus d'informations, consultez la section Intégration AWS Transit Gateway avec AWS PrivateLink et Amazon Route 53 Resolver.

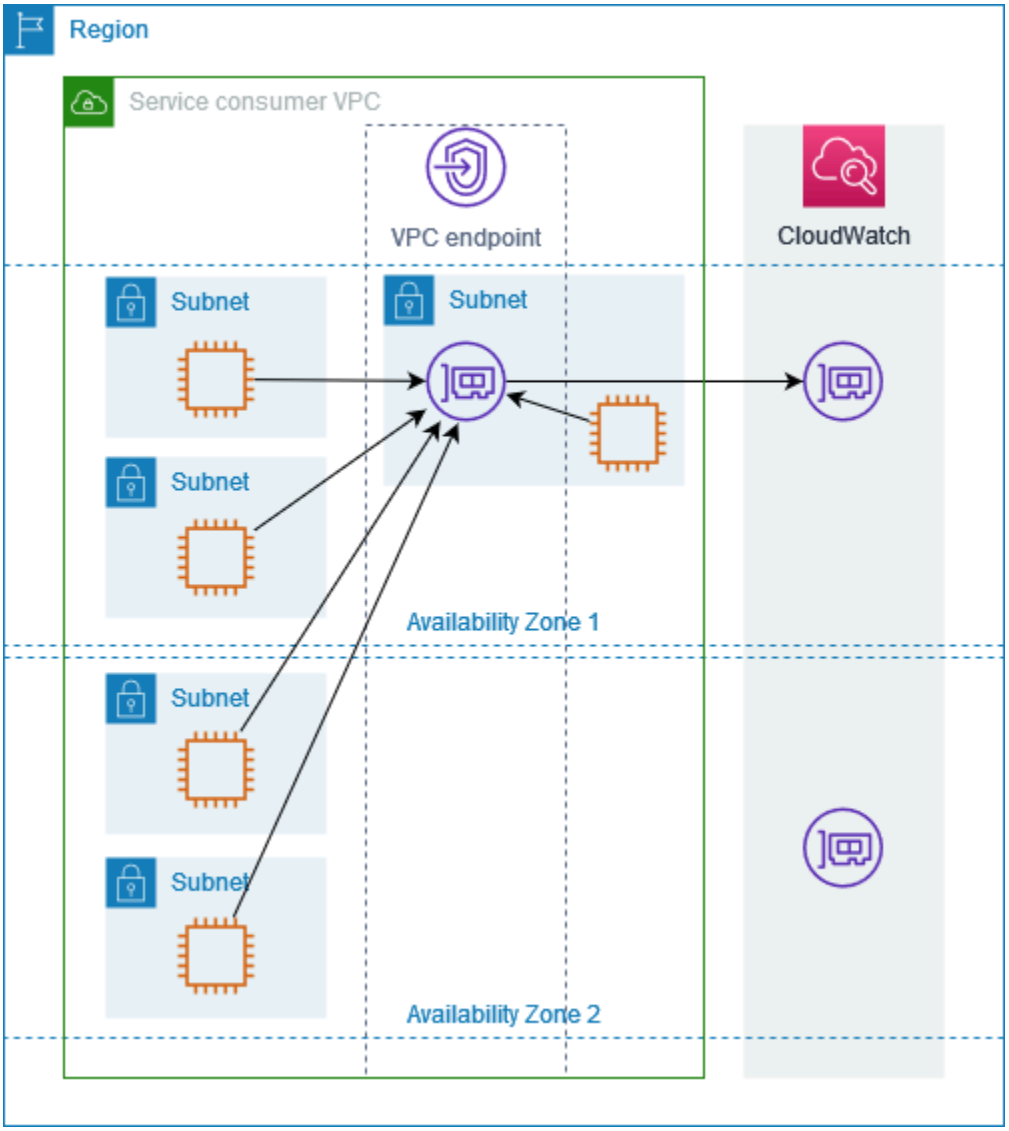
Sous-réseaux et zones de disponibilité

Vous pouvez configurer votre VPC point de terminaison avec un sous-réseau par zone de disponibilité. Nous créons une interface réseau pour le point de VPC terminaison de votre sous-réseau. Nous attribuons des adresses IP à chaque interface réseau de point de terminaison à partir de son sous-réseau, en fonction du type d'adresse IP du point de VPC terminaison. Les adresses IP d'une interface réseau de point de terminaison ne changeront pas pendant la durée de vie de son VPC point de terminaison.

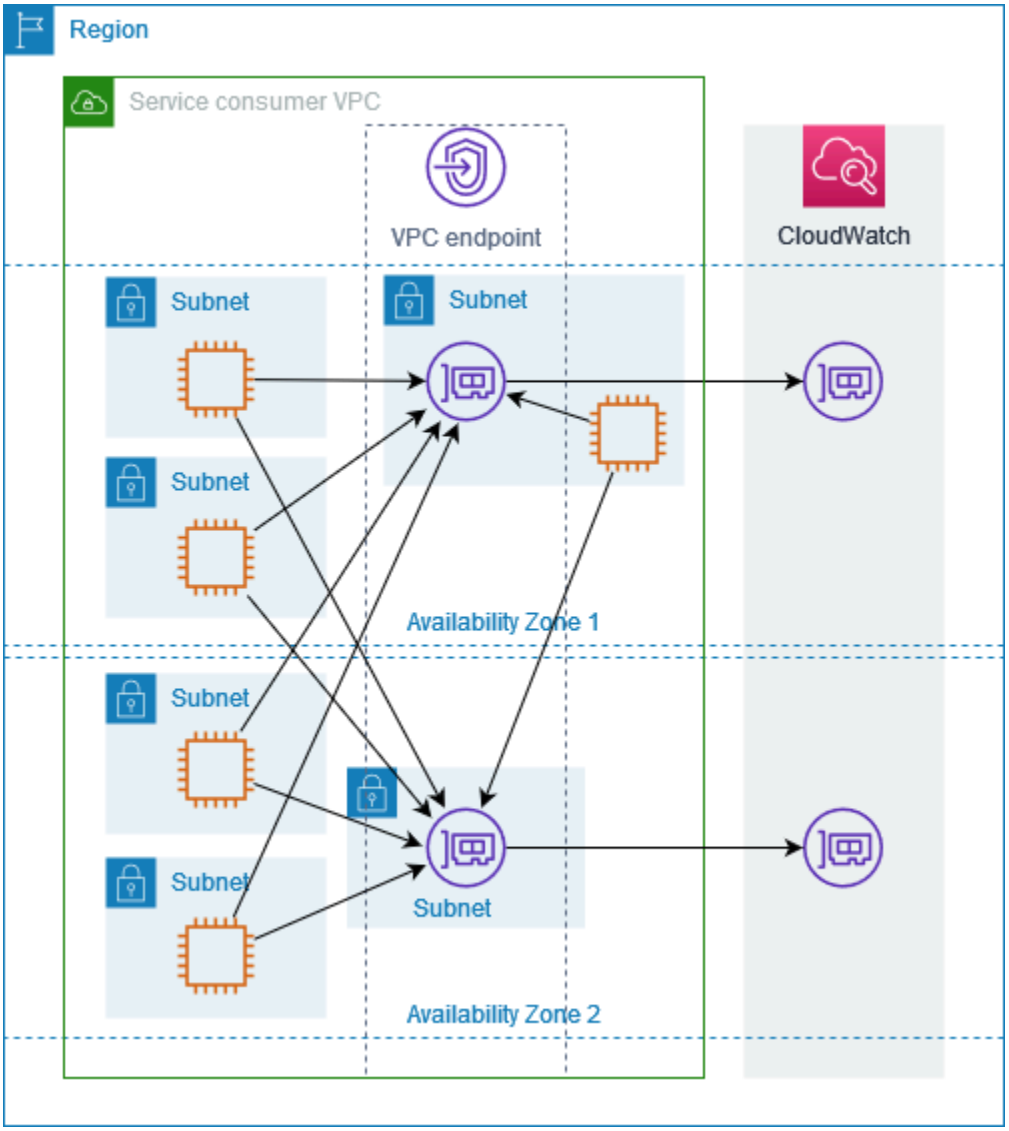
Dans un environnement de production, pour assurer une disponibilité et une résilience élevées, nous recommandons ce qui suit :

- Configurez au moins deux zones de disponibilité par VPC point de terminaison et déployez Service AWS les AWS ressources qui doivent y accéder.
- Configurez DNS les noms privés du VPC point de terminaison.
- Accédez au Service AWS en utilisant son DNS nom régional, également appelé point de terminaison public.

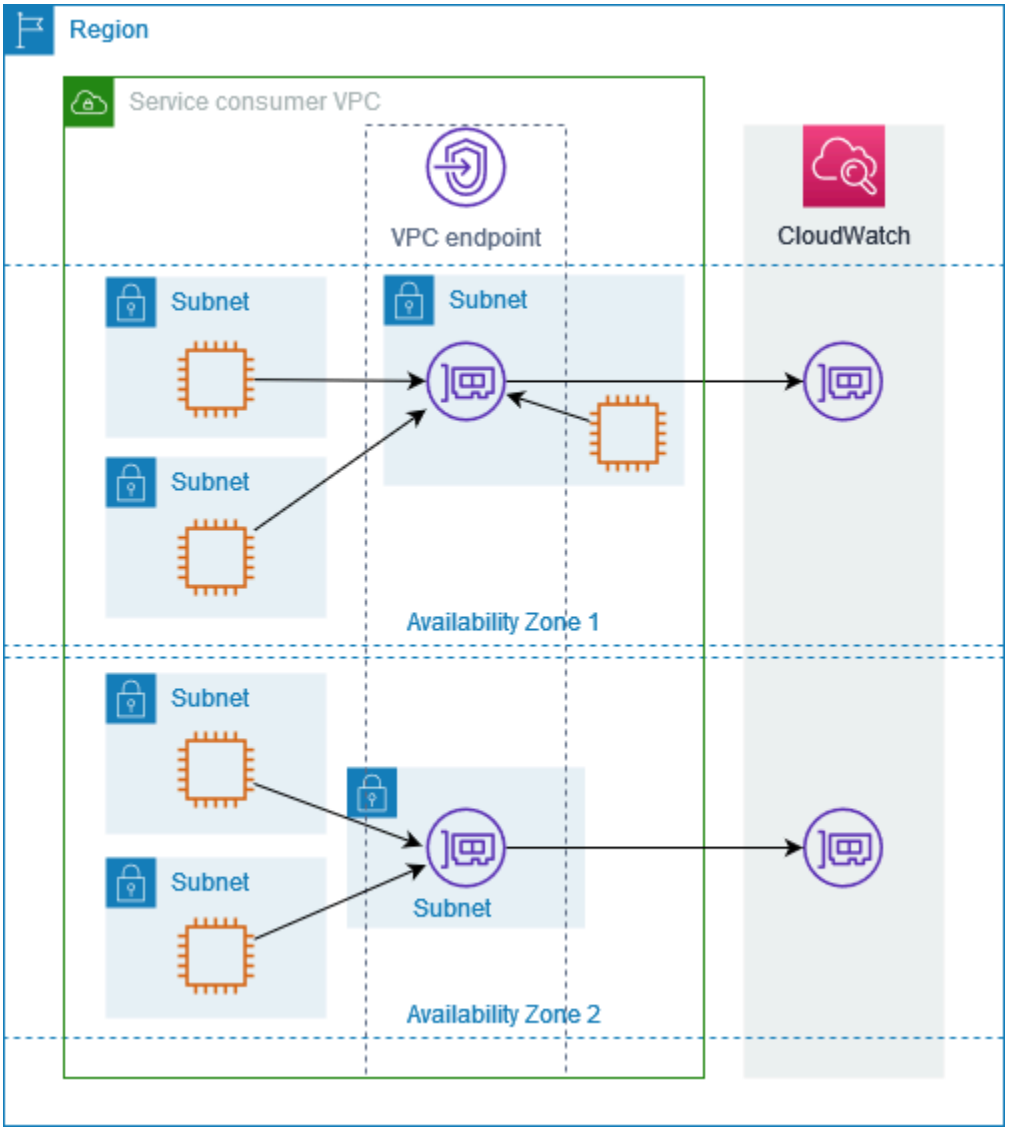
Le schéma suivant montre un VPC point de terminaison pour Amazon CloudWatch doté d'une interface réseau de point de terminaison dans une seule zone de disponibilité. Lorsqu'une ressource d'un sous-réseau VPC accède à Amazon CloudWatch via son point de terminaison public, nous résolvons le trafic vers l'adresse IP de l'interface réseau du point de terminaison. Cela inclut le trafic provenant de sous-réseaux situés dans d'autres zones de disponibilité. Toutefois, si la zone de disponibilité 1 est altérée, les ressources de la zone de disponibilité 2 perdent l'accès à Amazon CloudWatch.



Le schéma suivant montre un VPC point de terminaison pour Amazon CloudWatch avec des interfaces réseau de points de terminaison dans deux zones de disponibilité. Lorsqu'une ressource d'un sous-réseau VPC accède à Amazon CloudWatch via son point de terminaison public, nous sélectionnons une interface réseau de point de terminaison saine, en utilisant l'algorithme Round Robin pour alterner entre les deux. Nous résolvons ensuite le trafic vers l'adresse IP de l'interface réseau du point de terminaison sélectionné.



Si cela convient mieux à votre cas d'utilisation, vous pouvez envoyer le trafic depuis vos ressources vers le Service AWS en utilisant l'interface réseau du point de terminaison dans la même zone de disponibilité. Pour ce faire, utilisez le point de terminaison de la zone privée ou l'adresse IP de l'interface réseau du point de terminaison.



Types d'adresses IP

Services AWS peuvent être pris en charge IPv6 via leurs points de terminaison privés même s'ils ne le font pas IPv6 via leurs points de terminaison publics. Les points de terminaison compatibles IPv6 peuvent répondre aux DNS requêtes avec des AAAA enregistrements.

Exigences relatives à l'activation IPv6 d'un point de terminaison d'interface

- Service AWS Il doit rendre ses points de terminaison de service disponibles sur. IPv6 Pour de plus amples informations, veuillez consulter the section called “Afficher le IPv6 support”.
- Le type d'adresse IP d'un point de terminaison d'interface doit être compatible avec les sous-réseaux du point de terminaison d'interface, comme décrit ici :

- IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
- IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
- Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

Si un point de VPC terminaison d'interface est compatibleIPv4, les interfaces réseau du point de terminaison ont IPv4 des adresses. Si un point de VPC terminaison d'interface est compatibleIPv6, les interfaces réseau du point de terminaison ont IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison n'est pas accessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Services AWS qui s'intègrent à AWS PrivateLink

Les éléments suivants Services AWS s'intègrent à AWS PrivateLink. Vous pouvez créer un VPC point de terminaison pour vous connecter à ces services en privé, comme s'ils s'exécutaient vous-mêmeVPC.

Cliquez sur le lien dans la Service AWScolonne pour consulter la documentation des services intégrés à AWS PrivateLink. La colonne Nom du service contient le nom du service que vous spécifiez lorsque vous créez le point de VPC terminaison de l'interface, ou elle indique que le service gère le point de terminaison.

Service AWS	Nom du service
Analyseur d'accès	com.amazonaws. *region*.access-analyseur
AWS Account Management	com.amazonaws. *region*.compte
APIPasserelle Amazon	com.amazonaws. *region*.execute-api
AWS AppConfig	com.amazonaws. *region*.app config

Service AWS	Nom du service
	com.amazonaws. *region*données de configuration .app
AWS App Mesh	com.amazonaws. *region*.appmesh
	com.amazonaws. *region*. appmesh-envoy-management
AWS App Runner	com.amazonaws. *region*.apprunner
Services AWS App Runner	com.amazonaws. *region*.apprunner.requests
Application Autoscaling	com.amazonaws. *region*.mise à l'échelle automatique de l'application
AWS Application Discovery Service	com.amazonaws. *region*.découverte
	com.amazonaws. *region*.arsenal-discovery
AWS Service de migration d'applications	com.amazonaws. *region*.mgn
Amazon AppStream 2.0	com.amazonaws. *region*.appstream .api
	com.amazonaws. *region*.appstream. streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.athéna
AWS Audit Manager	com.amazonaws. *region*.responsable de l'audit
Amazon Aurora	com.amazonaws. *region*.rds
AWS Auto Scaling	com.amazonaws. *region*.plans de mise à l'échelle automatique
AWS Échange de données B2B	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.sauvegarde

Service AWS	Nom du service
	com.amazonaws. *region*.backup-gateway
AWS Batch	com.amazonaws. *region*.batch
Amazon Bedrock	com.amazonaws. *region*.socle
	com.amazonaws. *region*.bedrock-agent
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*.bedrock-runtime
AWS Billing and Cost Management	com.amazonaws. *region*.facturation
	com.amazonaws. *region*.freetier
	com.amazonaws. *region*.taxe
AWS Billing Conductor	com.amazonaws. *region*. responsable de la facturation
Amazon Braket	com.amazonaws. *region*.support
AWS Clean Rooms	com.amazonaws. *region*. salles propres
AWS Clean Rooms ML	com.amazonaws. *region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws. *region*.cloudcontrol api
	com.amazonaws. *region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws. *region*répertoire .cloud
AWS CloudFormation	com.amazonaws. *region*.cloud formation
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.service discovery
	com.amazonaws. *region*.servicediscovery-fips

Service AWS	Nom du service
	com.amazonaws. *region*.data-servicediscovery
	com.amazonaws. *region*. data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.cloud trail
Amazon CloudWatch	com.amazonaws. *region*.signaux d'application
	com.amazonaws. *region*. informations sur les applicati ons
	com.amazonaws. *region*.évidemment
	com.amazonaws. *region*.evidently-dataplane
	com.amazonaws. *region*.moniteur Internet
	com.amazonaws. *region*.internetmonitor-fips
	com.amazonaws. *region*.surveillance
	com.amazonaws. *region*.moniteur de débit réseau
	com.amazonaws. *region*. rapports du moniteur de flux réseau
	com.amazonaws. *region*.moniteur réseau
	com.amazonaws. *region*.observabilityadmin
	com.amazonaws. *region*.rhum
	com.amazonaws. *region*.rum-dataplane
	com.amazonaws. *region*.synthétiques
	com.amazonaws. *region*.synthetics-fips
Amazon CloudWatch Logs	com.amazonaws. *region*.journaux

Service AWS	Nom du service
AWS CodeArtifact	com.amazonaws. *region*.codeartefact.api
	com.amazonaws. *region*référentiels .codeartifact.
AWS CodeBuild	com.amazonaws. *region*.codebuild
	com.amazonaws. *region*.codebuild-fips
AWS CodeCommit	com.amazonaws. *region*.code commit
	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*. git-codecommit-fips
AWS CodeConnections	com.amazonaws. *region*.codeconnections.api
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*. codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws. *region*profileur .codeguru
CodeGuru Réviseur Amazon	com.amazonaws. *region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws. *region*.code pipeline
Amazon Comprehend	com.amazonaws. *region*.comprendre
Amazon Comprehend Medical	com.amazonaws. *region*. comprendre la médecine
AWS Compute Optimizer	com.amazonaws. *region*.compute-optimizer
AWS Config	com.amazonaws. *region*.config
Amazon Connect	com.amazonaws. *region*intégrations .app

Service AWS	Nom du service
	com.amazonaws. *region*.étuis
	com.amazonaws. *region*campagnes .connect
	com.amazonaws. *region*.profil
	com.amazonaws. *region*.voiceid
	com.amazonaws. *region*.sagesse
AWS Connector Service	com.amazonaws. *region*connecteur .aws
AWS Control Catalog	com.amazonaws. *region*.controlcatalog
AWS Cost Explorer	com.amazonaws. *region*.ce
Hub d'optimisation des coûts	com.amazonaws. *region*. cost-optimization-hub
AWS Data Exchange	com.amazonaws. *region*.échange de données
Exportations de données AWS	com.amazonaws. *region*. bcm-data-exports
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.synchronisation des données
Amazon DataZone	com.amazonaws. *region*.zone de données
AWS Deadline Cloud	com.amazonaws. *region*.deadline. Gestion
	com.amazonaws. *region*.deadline. planification
Amazon DevOps Guru	com.amazonaws. *region*.devops guru
AWS Directory Service	com.amazonaws. *region*.ds

Service AWS	Nom du service
	com.amazonaws. *region*.ds-data
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
Amazon EBS direct APIs	com.amazonaws. *region*.ebs
Amazon EC2	com.amazonaws. *region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws. *region*.mise à l'échelle automatique
EC2 Image Builder	com.amazonaws. *region*.générateur d'images
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr .dkr
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws. *region*.ecs-agent
	com.amazonaws. *region*.ecs-télémétrie
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws. *region*. tige de haricot élastique
	com.amazonaws. *region*. elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Amazon Elastic File System	com.amazonaws. *region*système de fichiers .elastic
	com.amazonaws. *region*.elasticfilesystem-fips

Service AWS	Nom du service
Elastic Load Balancing	com.amazonaws. *region*. équilibrage de charge élastique
Amazon ElastiCache	com.amazonaws. *region*.cache élastique
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
Amazon EMR sur EKS	com.amazonaws. *region*Conteneurs .emr
Amazon EMR sans serveur	com.amazonaws. *region*.emr-serverless
	com.amazonaws. *region*. emr-serverless-services.livy
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Messagerie sociale destinée aux utilisateurs finaux	com.amazonaws. *region*.messagerie sociale
Résolution des entités AWS	com.amazonaws. *region*. résolution de l'entité
Amazon EventBridge	com.amazonaws. *region*.événements
	com.amazonaws. *region*.tuyaux
	com.amazonaws. *region*.pipes-data
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.schémas
AWS Fault Injection Service	com.amazonaws. *region*.fis
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api

Service AWS	Nom du service
Amazon Forecast	com.amazonaws. *region*.prévision
	com.amazonaws. *region*requête .forecast
	com.amazonaws. *region*.forecast-fips
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*. détecteur de fraude
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
AWS Glue	com.amazonaws. *region*.colle
	com.amazonaws. *region*.glue.tableau de bord
AWS Glue DataBrew	com.amazonaws. *region*.databrew
Amazon Managed Grafana	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana-workspace
AWS Ground Station	com.amazonaws. *region*. station au sol
Amazon GuardDuty	com.amazonaws. *region*. devoir de garde
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*. guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*. dicom-medical-imaging
	com.amazonaws. *region*.imagerie médicale
	com.amazonaws. *region*. runtime-medical-imaging

Service AWS	Nom du service
AWS HealthLake	com.amazonaws. *region*.healthlake
AWS HealthOmics	com.amazonaws. *region*.analytics-omics
	com.amazonaws. *region*. control-storage-omics
	com.amazonaws. *region*.storage-omics
	com.amazonaws. *region*.tags-omics
	com.amazonaws. *region*.workflows-omics
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAMCentre d'identité	com.amazonaws. *region*.boutique d'identité
IAM Roles Anywhere	com.amazonaws. *region*. rôles n'importe où
Amazon Inspector	com.amazonaws. *region*.inspecteur 2
	com.amazonaws. *region*.inspector-scan
AWS IoT Core	com.amazonaws. *region*.iot.data
	com.amazonaws. *region*.iot .credentials
	com.amazonaws. *region*.iot .fleethub.api
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
AWS IoT Core for LoRaWAN	com.amazonaws. *region*.iotwireless.api
	com.amazonaws. *region*tasses .lorawan
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.iot par flotte
AWS IoT Greengrass	com.amazonaws. *region*. herbe verte

Service AWS	Nom du service
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iot sur le site .api
	com.amazonaws. *region*.iot par site
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*classement .kendra
AWS Key Management Service	com.amazonaws. *region*.km
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (pour Apache Cassandra)	com.amazonaws. *region*.cassandre
	com.amazonaws. *region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
	com.amazonaws. *region*. kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*. formation lacustre
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws. *region*.launchwizard
Amazon Lex	com.amazonaws. *region*.models-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.gestionnaire de licences
	com.amazonaws. *region*. license-manager-fips

Service AWS	Nom du service
	com.amazonaws. *region*. license-manager-linux-subscriptions
	com.amazonaws. *region*. license-manager-linux-subscriptions-pourboires
	com.amazonaws. *region*. license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws. *region*. équipement de surveillance
Amazon Lookout for Metrics	com.amazonaws. *region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws. *region*. lookoutvision
Amazon Macie	com.amazonaws. *region*.macie 2
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*.m2
Amazon Managed Blockchain	com.amazonaws. *region*.requête de chaîne de blocs gérée
	com.amazonaws. *region*.chaîne de blocs gérée.bitcoin.mainnet
	com.amazonaws. *region*.chaîne de blocs gérée.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*espaces de travail .aps
Streaming géré par Amazon pour Apache Kafka	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips

Service AWS	Nom du service
Amazon Managed Workflows for Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow .env-fips
	com.amazonaws. *region*.airflow.ops
AWS Management Console	com.amazonaws. *region*.console
	com.amazonaws. *region*.connexion
Amazon MemoryDB	com.amazonaws. *region*.base de données de mémoire
	com.amazonaws. *region*.memorydb-fips
Orchestrateur de l'AWS Migration Hub	com.amazonaws. *region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.refactor-spaces
Migration Hub Strategy Recommendations	com.amazonaws. *region*.migrationhub-strategy
Amazon MQ	com.amazonaws. *region*.mq
Amazon Neptune Analytics	com.amazonaws. *region*.neptune-graph
	com.amazonaws. *region*. neptune-graph-data
	com.amazonaws. *region*. neptune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.firewall réseau
	com.amazonaws. *region*. network-firewall-fips
Amazon OpenSearch Service	Ces points de terminaison sont gérés par des services

Service AWS	Nom du service
AWS Organizations	com.amazonaws. *region*.organisations
	com.amazonaws. *region*.organisations-fips
AWS Outposts	com.amazonaws. *region*.avant-postes
AWS Panorama	com.amazonaws. *region*.panorama
AWS Cryptographie des paiements	com.amazonaws. *region*.payment-cryptography.controlplane
	com.amazonaws. *region*.cryptographie de paiement. plan de données
AWS PCS	com.amazonaws. *region*.pièces
	com.amazonaws. *region*.pcs-fips
Amazon Personalize	com.amazonaws. *region*.personnaliser
	com.amazonaws. *region*.personnalisez les événements
	com.amazonaws. *region*.personalize-runtime
Amazon Pinpoint	com.amazonaws. *region*.épingler
	com.amazonaws. *region*. pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*.polly
AWS Price List	com.amazonaws. *region*.pricing.api
AWS 5G privée	com.amazonaws. *region*.réseaux privés
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. pca-connector-ad
	com.amazonaws. *region*. pca-connector-scep

Service AWS	Nom du service
AWS Proton	com.amazonaws. *region*.proton
Amazon Q Business	aws.api. *region*.qbusiness
Amazon Q Developer	com.amazonaws. *region*.codewhisperer
	com.amazonaws. *region*.q
	com.amazonaws. *region*.applications
Abonnements d'utilisateurs Amazon Q	com.amazonaws. *region*abonnements utilisate ur .service
Amazon QLDB	com.amazonaws. *region*session .qldb
Amazon QuickSight	com.amazonaws. *region*.quicksight - site
Amazon RDS	com.amazonaws. *region*.rds
RDSDonnées Amazon API	com.amazonaws. *region*.rds-data
Amazon RDS Performance Insights	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS Re:Post Private	com.amazonaws. *region*.espace de republication
Corbeille	com.amazonaws. *region*.rbin
Amazon Redshift	com.amazonaws. *region*.redshift
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift-serverless
	com.amazonaws. *region*. redshift-serverless-fips
Données Amazon Redshift API	com.amazonaws. *region*.redshift data
	com.amazonaws. *region*. redshift-data-fips

Service AWS	Nom du service
Amazon Rekognition	com.amazonaws. *region*.reconnaissance
	com.amazonaws. *region*.rekognition-fips
	com.amazonaws. *region*.reconnaissance du streaming
	com.amazonaws. *region*. streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws. *region*.ram
AWS Resource Groups	com.amazonaws. *region*.groupes de ressources
	com.amazonaws. *region*. resource-groups-fips
AWS RoboMaker	com.amazonaws. *region*.robomaker
Amazon S3	com.amazonaws. *region*.s3
	com.amazonaws. *region*tableaux .s3
Amazon S3 Multi-Region Access Points	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws. *region*.s3-avant-postes
Amazon SageMaker AI	aws.sagemaker. *region*.expériences
	aws.sagemaker. *region*.carnet
	aws.sagemaker. *region*.partner-app
	aws.sagemaker. *region*.studio
	com.amazonaws. *region*. sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips

Service AWS	Nom du service
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws. *region*.plans d'épargne
AWS Secrets Manager	com.amazonaws. *region*.secretsmanager
AWS Security Hub	com.amazonaws. *region*.securityhub
AWS Security Token Service	com.amazonaws. *region*.sts
AWS Serverless Application Repository	com.amazonaws. *region*.serverlessrepo
Service Catalog	com.amazonaws. *region*.catalogue de services
	com.amazonaws. *region*.servicecatalog-appregistry
Amazon SES	com.amazonaws. *region*.email-smtp
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snow Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.états

Service AWS	Nom du service
	com.amazonaws. *region*.sync-states
AWS Storage Gateway	com.amazonaws. *region*. passerelle de stockage
AWS Supply Chain	com.amazonaws. *region*.scn
AWS Systems Manager	com.amazonaws. *region*messages .ec2
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-contacts
	com.amazonaws. *region*.ssm-incidents
	com.amazonaws. *region*.ssm-quicksetup
	com.amazonaws. *region*Messages .sms
AWS Générateur de réseaux de télécommunications	com.amazonaws. *region*.tnb
Amazon Textract	com.amazonaws. *region*extrait .t
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream pour InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*. timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transcrire
	com.amazonaws. *region*. transcrire le streaming
Amazon Transcribe Medical	com.amazonaws. *region*.transcrire
	com.amazonaws. *region*. transcrire le streaming

Service AWS	Nom du service
AWS Transfer for SFTP	com.amazonaws. *region*.transfert
	com.amazonaws. *region*.transfer.server
Amazon Translate	com.amazonaws. *region*.traduire
AWS Trusted Advisor	com.amazonaws. *region*. conseiller de confiance
Amazon Verified Permissions	com.amazonaws. *region*. autorisations vérifiées
Amazon VPC Lattice	com.amazonaws. *region*.vpc en treillis
AWS Well-Architected Tool	com.amazonaws. *region*. bien architecturé
Amazon WorkMail	com.amazonaws. *region*.workmail
Amazon WorkSpaces	com.amazonaws. *region*.espaces de travail
Navigateur sécurisé Amazon Workspaces	com.amazonaws. *region*.espaces de travail-web
	com.amazonaws. *region*. workspaces-web-fips
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.xray

Voir les noms Service AWS disponibles

Vous pouvez utiliser la describe-vpc-endpoint-servicescommande pour afficher les noms des services qui prennent en charge les VPC points de terminaison.

L'exemple suivant montre les points de terminaison d'interface Services AWS qui prennent en charge dans la région spécifiée. L'option `--query` limite la sortie aux noms de services.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

Voici un exemple de sortie :

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

Afficher les informations sur un service

Une fois que vous avez le nom du service, vous pouvez utiliser la describe-vpc-endpoint-servicescommande pour afficher des informations détaillées sur chaque service de point de terminaison.

L'exemple suivant affiche des informations sur le point de terminaison de CloudWatch l'interface Amazon dans la région spécifiée.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

Voici un exemple de sortie. `VpcEndpointPolicySupported` indique si les stratégies de point de terminaison sont prises en charge. `SupportedIpAddressTypes` indique quels types d'adresses IP sont pris en charge.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
```

```
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

Afficher la prise en charge de stratégie de point de terminaison

Pour vérifier si un service prend en charge les politiques relatives aux terminaux, appelez la describe-vpc-endpoint-servicescommande et vérifiez la valeur de`VpcEndpointPolicySupported`. Les valeurs possibles sont `true` et `false`.

L'exemple suivant vérifie si le service spécifié prend en charge les politiques relatives aux points de terminaison dans la région spécifiée. L'option `--query` limite la sortie à la valeur de `VpcEndpointPolicySupported`.

```
aws ec2 describe-vpc-endpoint-services \
```

```
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

Voici un exemple de sortie.

```
True
```

L'exemple suivant répertorie les politiques de point de terminaison Services AWS qui prennent en charge les politiques de point de terminaison dans la région spécifiée. L'option `--query` limite la sortie aux noms de services. Pour exécuter cette commande à l'aide de l'invite de commande Windows, supprimez les guillemets simples autour de la chaîne de requête et remplacez le caractère de continuation de ligne de \ à ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

Voici un exemple de sortie.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

L'exemple suivant répertorie ceux Services AWS qui ne prennent pas en charge les politiques de point de terminaison dans la région spécifiée. L'option `--query` limite la sortie aux noms de services. Pour exécuter cette commande à l'aide de l'invite de commande Windows, supprimez les guillemets simples autour de la chaîne de requête et remplacez le caractère de continuation de ligne de \ à ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
```

```
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

Voici un exemple de sortie.

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

Afficher le IPv6 support

Vous pouvez utiliser la describe-vpc-endpoint-servicescommande suivante pour afficher les Services AWS informations auxquelles vous pouvez accéder IPv6 dans la région spécifiée. L'option `--query` limite la sortie aux noms de services.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

Voici un exemple de sortie :

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
```

```
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
    "com.amazonaws.us-east-1.iotfleetwise",
    "com.amazonaws.us-east-1.kinesis-firehose",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.m2".
    "com.amazonaws.us-east-1.macie2".
    "com.amazonaws.us-east-1.networkflowmonitor".
    "com.amazonaws.us-east-1.networkflowmonitorreports".
    "com.amazonaws.us-east-1.pca-connector-scep",
    "com.amazonaws.us-east-1.pcs",
    "com.amazonaws.us-east-1.pcs-fips",
    "com.amazonaws.us-east-1.pi",
    "com.amazonaws.us-east-1.pi-fips",
    "com.amazonaws.us-east-1.polly",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.rbin",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.sagemaker.api",
    "com.amazonaws.us-east-1.securityhub",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.synthetics".
    "com.amazonaws.us-east-1.synthetics-fips".
    "com.amazonaws.us-east-1.textract",
    "com.amazonaws.us-east-1.textract-fips",
    "com.amazonaws.us-east-1.timestream-influxdb",
    "com.amazonaws.us-east-1.timestream-influxdb-fips",
    "com.amazonaws.us-east-1.trustedadvisor",
    "com.amazonaws.us-east-1.workmail",
    "com.amazonaws.us-east-1.xray"
]
```

Accès et Service AWS utilisation d'un point de VPC terminaison d'interface

Vous pouvez créer un point de VPC terminaison d'interface pour vous connecter à des services alimentés par AWS PrivateLink, y compris de nombreux services Services AWS. Pour un aperçu, consultez the section called “Concepts” et Accès Services AWS.

Pour chaque sous-réseau que vous spécifiez à partir de votreVPC, nous créons une interface réseau de point de terminaison dans le sous-réseau et lui attribuons une adresse IP privée à partir de la plage d'adresses du sous-réseau. Une interface réseau de point de terminaison est une interface réseau gérée par le demandeur ; vous pouvez la visualiser dans votre Compte AWS, mais vous ne pouvez pas la gérer vous-même.

Des frais s'appliquent à l'utilisation horaire et au traitement de données. Pour plus d'informations, veuillez consulter Tarification des points de terminaison d'interface.

Table des matières

Prérequis

- Déployez les ressources qui accèderont Service AWS à votreVPC.
- Pour utiliser le mode privéDNS, vous devez activer les DNS noms d'hôte et DNS la résolution pour votreVPC. Pour plus d'informations, consultez Afficher et mettre à jour DNS les attributs dans le guide de VPC l'utilisateur Amazon.
- IPv6Pour activer un point de terminaison d'interface, celui-ci Service AWS doit prendre en charge l'accèsIPv6. Pour de plus amples informations, veuillez consulter the section called “Types d'adresses IP”.
- Créez un groupe de sécurité pour l'interface réseau du point de terminaison qui autorise le trafic attendu provenant des ressources de votreVPC. Par exemple, pour s'assurer qu'il AWS CLI peut envoyer des HTTPS demandes au Service AWS, le groupe de sécurité doit autoriser le HTTPS trafic entrant.

- Si vos ressources se trouvent dans un sous-réseau doté d'un réseauACL, vérifiez que le réseau ACL autorise le trafic entre les ressources de votre interface réseau VPC et celles du point de terminaison.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour de plus amples informations, veuillez consulter AWS PrivateLink quotas.

Création d'un point de terminaison VPC

Utilisez la procédure suivante pour créer un point de VPC terminaison d'interface qui se connecte à un Service AWS.

Pour créer un point de terminaison d'interface pour un Service AWS

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Dans Type, sélectionnez AWS services.
5. Pour Service name (Nom du service), sélectionnez le service. Pour de plus amples informations, veuillez consulter the section called “Services qui s'intègrent”.
6. Pour VPC, sélectionnez le VPC depuis lequel vous allez accéder au Service AWS.
7. Si, à l'étape 5, vous avez sélectionné le nom du service pour Amazon S3, et si vous souhaitez configurer le DNSsupport privé, sélectionnez Paramètres supplémentaires, Activer DNS le nom. Lorsque vous effectuez cette sélection, elle sélectionne également automatiquement Activer le mode privé DNS uniquement pour le point de terminaison entrant. Vous pouvez configurer le mode privé DNS avec un point de terminaison de résolution entrant uniquement pour les points de terminaison d'interface pour Amazon S3. Si vous ne disposez pas d'un point de terminaison de passerelle pour Amazon S3 et que vous sélectionnez Activer le mode privé DNS uniquement pour le point de terminaison entrant, vous recevrez un message d'erreur lorsque vous tenterez de passer à l'étape finale de cette procédure.

   Si, à l'étape 5, vous avez sélectionné le nom du service pour un service autre qu'Amazon S3, l'option Paramètres supplémentaires, Activer DNS le nom est déjà sélectionnée. Nous vous recommandons de conserver la valeur par défaut. Cela garantit que les demandes qui utilisent les points de terminaison du service public, telles que les demandes effectuées via un AWS SDK, sont résolues vers votre VPC point de terminaison.

8. Pour les sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer les interfaces réseau des points de terminaison. Vous pouvez sélectionner un sous-réseau par zone de disponibilité. Il n'est pas possible de sélectionner plusieurs sous-réseaux dans la même zone de disponibilité. Pour de plus amples informations, veuillez consulter the section called “Sous-réseaux et zones de disponibilité”.

   Par défaut, nous sélectionnons les adresses IP dans les plages d'adresses IP des sous-réseaux et les attribuons aux interfaces réseau des points de terminaison. Pour choisir vous-même les adresses IP, sélectionnez Désigner les adresses IP. Notez que les quatre premières adresses IP et la dernière adresse IP d'un CIDR bloc de sous-réseau sont réservées à un usage interne. Vous ne pouvez donc pas les spécifier pour les interfaces réseau de vos terminaux.

9. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :

   - IPv4— Attribuez IPv4 des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses et si le service accepte les IPv4 demandes.
   - IPv6— Attribuez IPv6 des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux et que le service accepte IPv6 les demandes.
   - Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et si le service accepte à la fois les IPv6 demandes IPv4 et les demandes.

10. Pour Security groups (Groupes de sécurité), sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison. Par défaut, nous associons le groupe de sécurité par défaut auVPC.

11. Pour Policy, pour autoriser toutes les opérations effectuées par tous les principaux sur toutes les ressources via le point de terminaison de l'interface, sélectionnez Accès complet. Pour restreindre l'accès, sélectionnez Personnalisé et entrez une politique. Cette option n'est disponible que si le service prend en charge les politiques relatives aux VPC terminaux. Pour de plus amples informations, veuillez consulter Politiques de point de terminaison.

12. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.

13. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison d'interface à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer des VPC points de terminaison dans des sous-réseaux partagés avec vous. Toutefois, vous pouvez utiliser les VPC points de terminaison dans les sous-réseaux partagés avec vous.

ICMP

Les points de terminaison de l'interface ne répondent pas aux ping demandes. Vous pouvez utiliser les nmap commandes nc ou à la place.

Configuration d'un point de terminaison d'interface

Après avoir créé un point de VPC terminaison d'interface, vous pouvez mettre à jour sa configuration.

Tâches

- Ajouter ou supprimer des sous-réseaux
- Association de groupes de sécurité
- Modifier la politique du VPC point de terminaison
- Activer les DNS noms privés
- Gérer les balises

Ajouter ou supprimer des sous-réseaux

Vous pouvez choisir un sous-réseau par zone de disponibilité pour votre point de terminaison d'interface. Si vous ajoutez un sous-réseau, nous créons une interface réseau de point de terminaison dans le sous-réseau et lui attribuons une adresse IP privée à partir de la plage d'adresses IP du sous-réseau. Si vous supprimez un sous-réseau, nous supprimons son interface réseau de point de terminaison. Pour de plus amples informations, veuillez consulter the section called “Sous-réseaux et zones de disponibilité”.

Pour modifier les sous-réseaux à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Manage subnets (Gérer les sous-réseaux).
5. Sélectionnez ou désélectionnez les zones de disponibilité selon vos besoins. Pour chaque zone de disponibilité, sélectionnez un sous-réseau. Par défaut, nous sélectionnons les adresses IP dans les plages d'adresses IP des sous-réseaux et les attribuons aux interfaces réseau des points de terminaison. Pour choisir les adresses IP d'une interface réseau de point de terminaison, sélectionnez Désigner les adresses IP et entrez une IPv4 adresse dans la plage d'adresses de sous-réseau. Si le service de point de terminaison le prend en chargeIPv6, vous pouvez également saisir une IPv6 adresse à partir de la plage d'adresses de sous-réseau.

   Si vous spécifiez une adresse IP pour un sous-réseau qui possède déjà une interface réseau de point de terminaison pour ce point de VPC terminaison, nous remplaçons l'interface réseau de point de terminaison par une nouvelle. Ce processus déconnecte temporairement le sous-réseau et le point de terminaison. VPC
6. Choisissez Modify subnets (Modifier les sous-réseaux).

Pour modifier les sous-réseaux à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Association de groupes de sécurité

Vous pouvez modifier les groupes de sécurité qui sont associés aux interfaces réseau pour votre point de terminaison d'interface. Les règles du groupe de sécurité contrôlent le trafic autorisé vers l'interface réseau du point de terminaison à partir des ressources de votreVPC.

Pour modifier les groupes de sécurité à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.

4. Choisissez Actions, Gérer les groupes de sécurité.
5. Activez ou désactivez des groupes de sécurité si nécessaire.
6. Choisissez Modify security groups (Modifier les groupes de sécurité).

Pour modifier les groupes de sécurité à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Modifier la politique du VPC point de terminaison

S'il Service AWS prend en charge les politiques de point de terminaison, vous pouvez modifier la politique de point de terminaison pour le point de terminaison. Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet. Pour de plus amples informations, veuillez consulter Politiques de point de terminaison.

Pour modifier la politique de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Manage policy (Gérer la politique).
5. Choisissez Full Access (Accès complet) pour autoriser un accès complet au service, ou choisissez Custom (Personnalisé) et joignez une politique personnalisée.
6. Choisissez Save (Enregistrer).

Pour modifier la politique de point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Activer les DNS noms privés

Nous vous recommandons d'activer les DNS noms privés pour vos VPC points de terminaison pour Services AWS. Cela garantit que les demandes qui utilisent les points de terminaison du service

public, telles que les demandes effectuées via un AWS SDK, sont résolues vers votre VPC point de terminaison.

Pour utiliser des DNS noms privés, vous devez activer à la fois les DNSnoms d'hôte et DNS la résolution pour votreVPC. Après avoir activé DNS les noms privés, la disponibilité des adresses IP privées peut prendre quelques minutes. Les DNS enregistrements que nous créons lorsque vous activez les DNS noms privés sont privés. Par conséquent, le DNS nom privé ne peut pas être résolu publiquement.

Pour modifier l'option des DNS noms privés à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Modifier le DNS nom privé.
5. Sélectionnez ou désélectionnez Enable for this endpoint (Activer pour ce point de terminaison) selon les besoins.
6. Si le service est Amazon S3, la sélection d'Activer pour ce point de terminaison à l'étape précédente permet également de sélectionner Activer le mode privé DNS uniquement pour le point de terminaison entrant. Si vous préférez la DNS fonctionnalité privée standard, désactivez Activer le privé DNS uniquement pour le point de terminaison entrant. Si vous ne disposez pas d'un point de terminaison de passerelle pour Amazon S3 en plus d'un point de terminaison d'interface pour Amazon S3, et que vous sélectionnez Activer le mode privé DNS uniquement pour le point de terminaison entrant, vous recevrez un message d'erreur lorsque vous enregistrerez les modifications à l'étape suivante. Pour de plus amples informations, veuillez consulter the section called “Privé DNS”.
7. Sélectionnez Save Changes (Enregistrer les modifications).

Pour modifier l'option des DNS noms privés à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Gérer les balises

Vous pouvez marquer votre point de terminaison d'interface pour vous aider à l'identifier ou à le catégoriser en fonction des besoins de votre organisation.

Pour gérer les balises à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Manage tags (Gérer les balises).
5. Pour chaque balise à ajouter, choisissez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Save (Enregistrer).

Pour gérer les balises à l'aide de la ligne de commande

- create-tags et delete-tags (AWS CLI)
- New-EC2Taget Remove-EC2Tag(Outils pour Windows PowerShell)

Réception d'alertes pour les événements relatifs aux points de terminaison d'interface

Vous pouvez créer une notification afin de recevoir des alertes pour des événements spécifiques liés au point de terminaison de votre interface. Par exemple, vous pouvez recevoir un e-mail quand une demande de connexion est acceptée ou refusée.

Tâches

- Création d'une SNS notification
- Ajout d'une stratégie d'accès
- Ajout d'une stratégie de clé

Création d'une SNS notification

Utilisez la procédure suivante pour créer une SNS rubrique Amazon pour les notifications et vous abonner à la rubrique.

Pour créer une notification pour un point de terminaison d'interface à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Dans l'onglet Notifications, choisissez Create notification (Créer une notification).
5. Pour Notification ARN, choisissez ARN le SNS sujet que vous avez créé.
6. Pour vous abonner à un événement, sélectionnez-le dans Events (Événements).
   - Connect (Connexion) – Le consommateur du service a créé le point de terminaison d'interface. Cela envoie une demande de connexion au fournisseur du service.
   - Accept (Acceptation) – Le fournisseur du service a accepté la demande de connexion.
   - Reject (Refus) – Le fournisseur du service a refusé la demande de connexion.
   - Delete (Suppression) – Le consommateur du service a supprimé le point de terminaison d'interface.
7. Choisissez Create notification (Créer une notification).

Pour créer une notification pour un point de terminaison d'interface à l'aide de la ligne de commande

- create-vpc-endpoint-connection-notification ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Outils pour Windows PowerShell)

Ajout d'une stratégie d'accès

Ajoutez une politique d'accès à la SNS rubrique Amazon qui AWS PrivateLink permet de publier des notifications en votre nom, comme la suivante. Pour plus d'informations, consultez Comment modifier la politique d'accès de mon SNS sujet Amazon ? Utilisez les clés de condition globale `aws:SourceArn` et `aws:SourceAccount` pour vous protéger contre le problème du député confus.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Ajout d'une stratégie de clé

Si vous utilisez des SNS sujets chiffrés, la politique de ressources associée à la KMS clé doit faire confiance AWS PrivateLink aux AWS KMS API opérations d'appel. Voici un exemple de stratégie de clé.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
```

```
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Suppression d'un point de terminaison d'interface

Lorsque vous avez terminé d'utiliser un VPC point de terminaison, vous pouvez le supprimer. La suppression d'un point de terminaison d'interface supprime également les interfaces réseau de ce point de terminaison.

Pour supprimer un point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer un point de terminaison à l'aide de la ligne de commande

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Outils pour Windows PowerShell)

Points de terminaison de passerelle

VPCLes points de terminaison Gateway fournissent une connectivité fiable à Amazon S3 et DynamoDB sans avoir besoin d'une passerelle Internet ou NAT d'un appareil pour votre. VPC Les points de terminaison de la passerelle ne l'utilisent pas AWS PrivateLink, contrairement aux autres types de points de VPC terminaison.

Amazon S3 et DynamoDB prennent en charge à la fois les points de terminaison de passerelle et les points de terminaison d'interface. Pour une comparaison des options, consultez les rubriques suivantes :

- Types de VPC points de terminaison pour Amazon S3
- Types de VPC points de terminaison pour Amazon DynamoDB

Tarification

Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle.

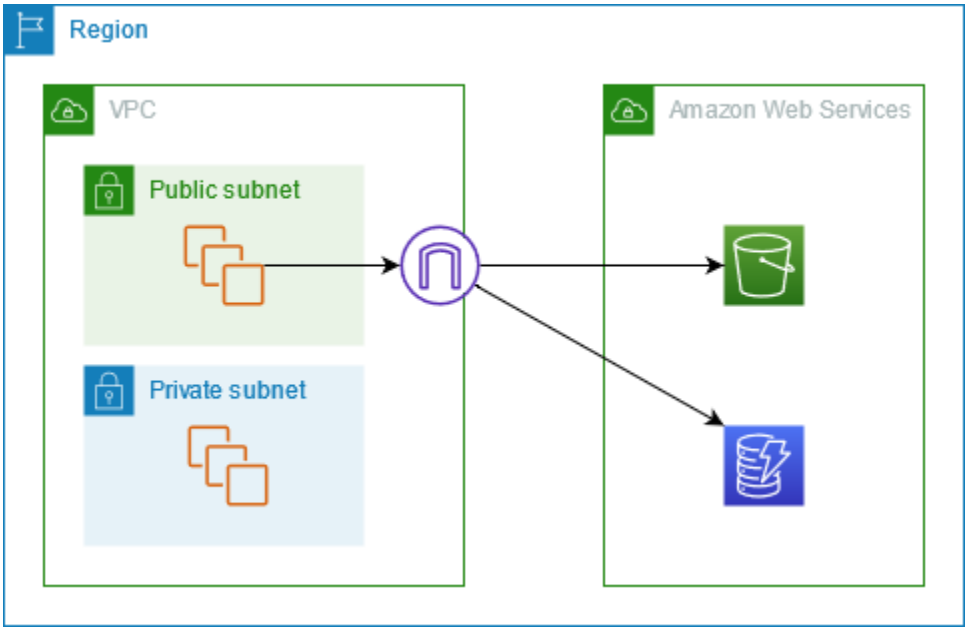
Table des matières

Présentation

Vous pouvez accéder à Amazon S3 et DynamoDB via leurs points de terminaison de service public ou via des points de terminaison de passerelle. Cette vue d'ensemble compare ces méthodes.

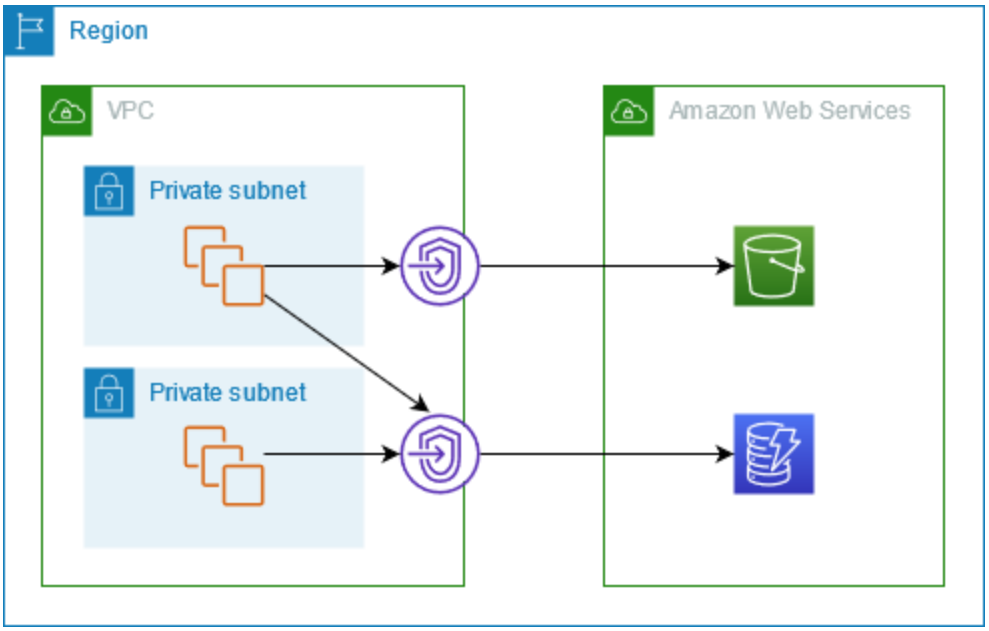
Accès via une passerelle Internet

Le schéma suivant montre comment les instances accèdent à Amazon S3 et DynamoDB via leurs points de terminaison de service public. Le trafic vers Amazon S3 ou DynamoDB depuis une instance d'un sous-réseau public est acheminé vers la passerelle Internet pour le, puis vers VPC le service. Les instances d'un sous-réseau privé ne peuvent pas envoyer de trafic vers Amazon S3 ou DynamoDB, car par définition les sous-réseaux privés ne disposent pas d'itinéraires vers une passerelle Internet. Pour permettre aux instances du sous-réseau privé d'envoyer du trafic vers Amazon S3 ou DynamoDB, vous devez ajouter NAT un appareil au sous-réseau public et acheminer le trafic du sous-réseau privé vers l'appareil. NAT Lorsque le trafic vers Amazon S3 ou DynamoDB passe par la passerelle Internet, il ne quitte pas le réseau. AWS



Accès via un point de terminaison de passerelle

Le schéma suivant montre comment les instances accèdent à Amazon S3 et DynamoDB via un point de terminaison de passerelle. Le trafic de votre part VPC vers Amazon S3 ou DynamoDB est acheminé vers le point de terminaison de la passerelle. Chaque table de routage de sous-réseau doit avoir un itinéraire qui envoie le trafic destiné au service vers le point de terminaison de passerelle en utilisant la liste de préfixes du service. Pour plus d'informations, consultez les listes de AWS préfixes gérées par -dans le guide de VPCl'utilisateur Amazon.



Routage

Lorsque vous créez un point de terminaison de passerelle, vous sélectionnez les tables de VPC routage pour les sous-réseaux que vous activez. L'itinéraire suivant est automatiquement ajouté à chaque table de routage que vous sélectionnez. La destination est une liste de préfixes pour le service détenu par AWS et la cible est le point de terminaison de la passerelle.

Destination	Cible
prefix_list_id	*gateway_endpoint_id*

Considérations

- Vous pouvez consulter les itinéraires de point de terminaison que nous ajoutons à votre table de routage, mais vous ne pouvez pas les modifier ni les supprimer. Pour ajouter un itinéraire de point de terminaison à une table de routage, associez-le au point de terminaison de passerelle. Nous supprimons l'itinéraire du point de terminaison lorsque vous dissociez la table de routage du point de terminaison de passerelle ou lorsque vous supprimez le point de terminaison de passerelle.
- Toutes les instances des sous-réseaux associés à une table de routage associée à un point de terminaison de passerelle utilisent automatiquement le point de terminaison de passerelle pour accéder au service. Les instances des sous-réseaux qui ne sont pas associées à ces tables de routage utilisent le point de terminaison du service public, et non le point de terminaison de la passerelle.
- Une table de routage peut avoir à la fois un itinéraire de point de terminaison vers Amazon S3 et un itinéraire de point de terminaison vers DynamoDB. Vous pouvez avoir des itinéraires de points de terminaison vers le même service (Amazon S3 ou DynamoDB) dans plusieurs tables de routage. Vous ne pouvez pas avoir plusieurs itinéraires de point de terminaison vers le même service (Amazon S3 ou DynamoDB) dans une seule table de routage.
- Nous utilisons la route la plus spécifique qui correspond au trafic afin de déterminer comment router le trafic (correspondance de préfixe le plus long). Pour les tables de routage avec un itinéraire de point de terminaison, cela signifie ce qui suit :
  - S'il existe un itinéraire qui envoie tout le trafic Internet (0.0.0.0/0) vers une passerelle Internet, l'itinéraire du point de terminaison est prioritaire sur le trafic destiné au service (Amazon S3 ou DynamoDB) dans la Région actuelle. Le trafic destiné à un autre Service AWS utilise la passerelle Internet.

- Le trafic destiné au service (Amazon S3 ou DynamoDB) dans une autre région est dirigé vers la passerelle Internet, car les listes de préfixes sont spécifiques à une Région.
- S'il existe un itinéraire qui spécifie la plage d'adresses IP exacte du service (Amazon S3 ou DynamoDB) dans la même Région, cet itinéraire a la priorité sur l'itinéraire du point de terminaison.

Sécurité

Lorsque vos instances accèdent à Amazon S3 ou DynamoDB via un point de terminaison de passerelle, elles accèdent au service en utilisant son point de terminaison de passerelle. Les groupes de sécurité de ces instances doivent autoriser le trafic en provenance ou à destination du service. Voici un exemple de règle sortante. Elle fait référence à l'ID de la liste de préfixes du service.

Destination	Protocole	Plage de ports
prefix_list_id	TCP	443

Le réseau ACLs des sous-réseaux de ces instances doit également autoriser le trafic à destination et en provenance du service. Voici un exemple de règle sortante. Vous ne pouvez pas faire référence à des listes de préfixes dans ACL les règles réseau, mais vous pouvez obtenir les plages d'adresses IP du service à partir de sa liste de préfixes.

Destination	Protocole	Plage de ports
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Points de terminaison de passerelle pour Amazon S3

Vous pouvez accéder à Amazon S3 à partir de vos VPC VPC points de terminaison de passerelle. Après avoir créé le point de terminaison de la passerelle, vous pouvez l'ajouter en tant que cible dans votre table de routage pour le trafic destiné VPC à Amazon S3.

Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle.

Amazon S3 prend en charge les points de terminaison de passerelle et les points de terminaison d'interface. Avec un point de terminaison de passerelle, vous pouvez accéder à Amazon S3 depuis votre ordinateurVPC, sans avoir besoin d'une passerelle Internet ou d'un NAT appareilVPC, et sans frais supplémentaires. Toutefois, les points de terminaison de la passerelle n'autorisent pas l'accès depuis des réseaux locaux, depuis des réseaux homologues VPCs dans d'autres AWS régions ou via une passerelle de transit. Pour ces scénarios, vous devez utiliser un point de terminaison d'interface qui est disponible moyennant des frais supplémentaires. Pour plus d'informations, consultez la section Types de VPC points de terminaison pour Amazon S3 dans le guide de l'utilisateur d'Amazon S3.

Table des matières

Considérations

- Le point de terminaison de passerelle est disponible uniquement dans la Région où vous l'avez créé. Veillez à créer votre point de terminaison de passerelle dans la même Région que vos compartiments S3.
- Si vous utilisez les DNS serveurs Amazon, vous devez activer à la fois les DNSnoms d'hôte et DNS la résolution pour votreVPC. Si vous utilisez votre propre DNS serveur, assurez-vous que les demandes adressées à Amazon S3 sont correctement résolues vers les adresses IP gérées par AWS.
- Les règles des groupes de sécurité pour les instances qui accèdent à Amazon S3 par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination d'Amazon S3. Vous pouvez faire référence à l'ID de la liste de préfixes pour Amazon S3 dans les règles du groupe de sécurité.

- Le réseau du sous-réseau ACL de vos instances qui accèdent à Amazon S3 via un point de terminaison de passerelle doit autoriser le trafic à destination et en provenance d'Amazon S3. Vous ne pouvez pas faire référence à des listes de préfixes dans ACL les règles du réseau, mais vous pouvez obtenir la plage d'adresses IP d'Amazon S3 à partir de la liste de préfixes d'Amazon S3.
- Vérifiez si vous utilisez un système Service AWS qui nécessite l'accès à un compartiment S3. Par exemple, un service peut nécessiter l'accès à des compartiments contenant des fichiers journaux ou vous obliger à télécharger des pilotes ou des agents sur vos EC2 instances. Si tel est le cas, assurez-vous que votre politique de point de terminaison autorise la ressource Service AWS or à accéder à ces compartiments à l'aide de l'`s3:GetObject`action.
- Vous ne pouvez pas utiliser `aws:SourceIp` cette condition dans une politique d'identité ou une politique de compartiment pour les demandes adressées à Amazon S3 qui transitent par un point de VPC terminaison. Utilisez à la place la condition `aws:VpcSourceIp`. Vous pouvez également utiliser des tables de routage pour contrôler quelles EC2 instances peuvent accéder à Amazon S3 via le VPC point de terminaison.
- Les points de terminaison de la passerelle prennent en charge uniquement IPv4 le trafic.
- Les IPv4 adresses source des instances de vos sous-réseaux concernés telles que reçues par Amazon S3 passent d'IPv4adresses publiques à des IPv4 adresses privées dans votreVPC. Un point de terminaison change de route réseau et déconnecte TCP les connexions ouvertes. Les connexions précédentes qui utilisaient des IPv4 adresses publiques ne sont pas reprises. Nous vous recommandons de ne pas avoir de tâches importantes en cours d'exécution lorsque vous créez ou modifiez un point de terminaison ou de réaliser un test pour vous assurer que votre logiciel puisse automatiquement se reconnecter à Amazon S3 ; après l'interruption de la connexion.
- Les connexions aux points de terminaison ne peuvent pas être étendues à partir d'unVPC. Les ressources situées de l'autre côté d'une VPN connexion, d'une connexion d'VPCappairage, d'une passerelle de transit ou d'une AWS Direct Connect connexion de votre part VPC ne peuvent pas utiliser un point de terminaison de passerelle pour communiquer avec Amazon S3.
- Votre compte dispose d'un quota par défaut de 20 points de terminaison de passerelle par Région, qui est réglable. Il existe également une limite de 255 points de terminaison de passerelle par. VPC

Privé DNS

Vous pouvez configurer le mode privé DNS pour optimiser les coûts lorsque vous créez à la fois un point de terminaison de passerelle et un point de terminaison d'interface pour Amazon S3.

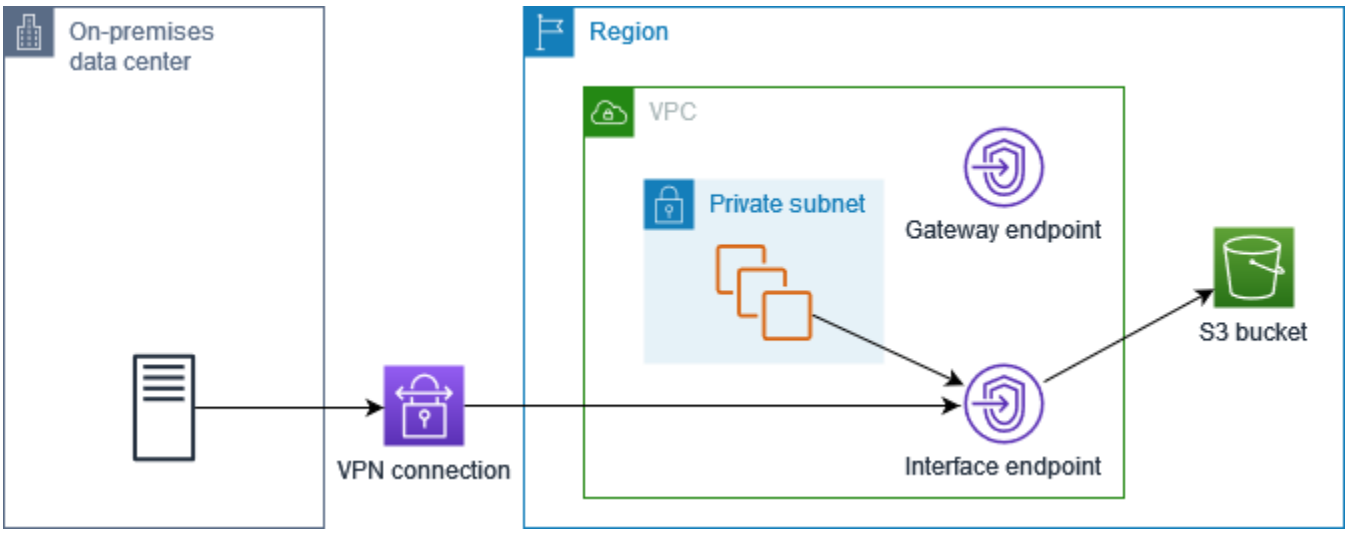
Route 53 Resolver

Amazon fournit un DNS serveur, appelé Route 53 Resolver, pour votreVPC. Le résolveur Route 53 résout automatiquement les noms de VPC domaine locaux et les enregistrements dans les zones hébergées privées. Cependant, vous ne pouvez pas utiliser le résolveur Route 53 depuis l'extérieur de votreVPC. Route 53 fournit des points de terminaison et des règles de résolution afin que vous puissiez utiliser le résolveur Route 53 depuis l'extérieur de votre. VPC Un point de terminaison de résolution entrant transmet les DNS requêtes du réseau local à Route 53 Resolver. Un point de terminaison sortant transmet les DNS requêtes du résolveur Route 53 au réseau local.

Lorsque vous configurez le point de terminaison de votre interface pour qu'Amazon S3 utilise le mode privé DNS uniquement pour le point de terminaison de résolution entrant, nous créons un point de terminaison de résolution entrant. Le point de terminaison du résolveur entrant résout les DNS requêtes adressées à Amazon S3 depuis le site vers les adresses IP privées du point de terminaison de l'interface. Nous ajoutons également ALIAS des enregistrements pour le résolveur Route 53 à la zone hébergée publique d'Amazon S3, afin que les DNS requêtes provenant de votre VPC résolution soient envoyées aux adresses IP publiques Amazon S3, qui acheminent le trafic vers le point de terminaison de la passerelle.

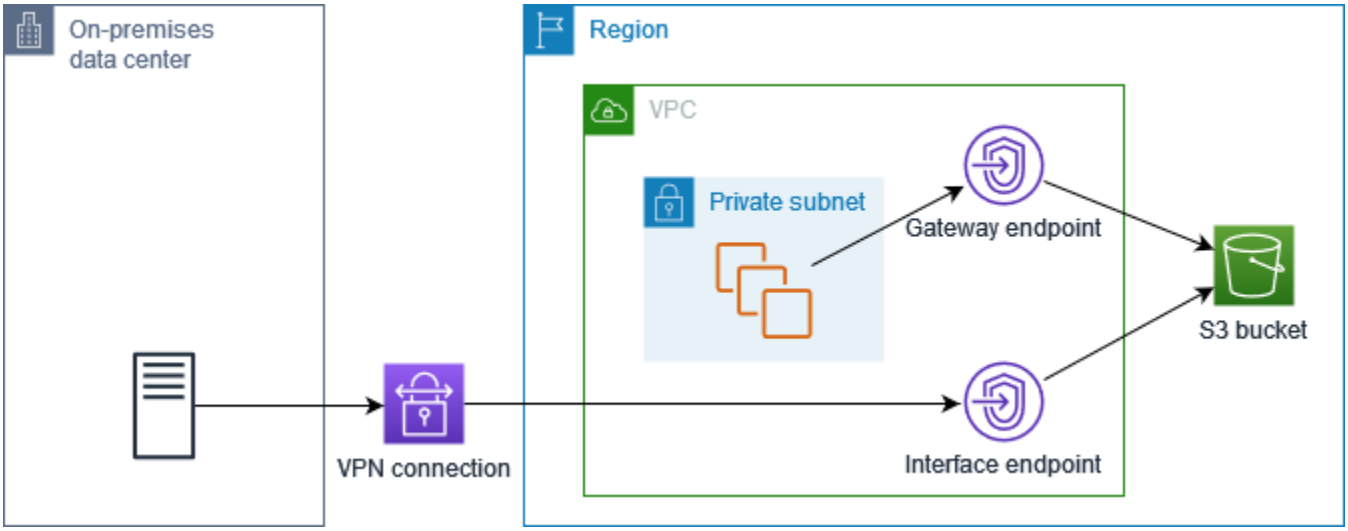
Privé DNS

Si vous configurez le mode privé DNS pour le point de terminaison de votre interface pour Amazon S3, mais que vous ne configurez pas le mode privé DNS uniquement pour le point de terminaison entrant du résolveur, les demandes provenant de votre réseau local et de vous-même VPC utilisent le point de terminaison d'interface pour accéder à Amazon S3. Par conséquent, vous payez pour utiliser le point de terminaison de l'interface pour le trafic provenant duVPC, au lieu d'utiliser le point de terminaison de la passerelle sans frais supplémentaires.



Privé DNS uniquement pour le point de terminaison entrant du résolveur

Si vous configurez le mode privé DNS uniquement pour le point de terminaison entrant du résolveur, les demandes provenant de votre réseau local utilisent le point de terminaison de l'interface pour accéder à Amazon S3, et les demandes provenant de vous VPC utilisent le point de terminaison de passerelle pour accéder à Amazon S3. Par conséquent, vous optimisez vos coûts, car vous payez pour utiliser le point de terminaison d'interface uniquement pour le trafic qui ne peut pas utiliser le point de terminaison de passerelle.



Configurer le mode privé DNS

Vous pouvez configurer le mode privé DNS pour un point de terminaison d'interface pour Amazon S3 lorsque vous le créez ou après l'avoir créé. Pour plus d'informations, veuillez consulter the section called “Création d'un point de terminaison VPC” (configurer pendant la création) ou the section called “Activer les DNS noms privés” (configurer après la création).

Créer un point de terminaison de passerelle

Utilisez la procédure suivante pour créer un point de terminaison de passerelle qui se connecte à Amazon S3.

Pour créer un point de terminaison de passerelle à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Services AWS.
5. Pour les services, ajoutez le filtre Type = Gateway et sélectionnez com.amazonaws. *region*.s3.

6. Pour VPC, sélectionnez le point de terminaison VPC dans lequel vous souhaitez créer le point de terminaison.
7. Pour Configure route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau de point de terminaison.
8. Pour Policy, sélectionnez Accès complet pour autoriser toutes les opérations effectuées par tous les principaux sur toutes les ressources du VPC point de terminaison. Sinon, sélectionnez Personnalisé pour associer une politique de point de VPC terminaison qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le VPC point de terminaison.
9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison de passerelle à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Contrôle de l'accès à l'aide de politiques de compartiment

Vous pouvez utiliser des politiques de compartiment pour contrôler l'accès aux compartiments à partir de points de terminaison spécifiquesVPCs, de plages d'adresses IP et. Comptes AWS Ces exemples supposent qu'il existe également des déclarations de politique générale qui autorisent l'accès requis pour vos cas d'utilisation.

Example Exemple : restriction de l'accès à un point de terminaison spécifique

Vous pouvez créer une politique de compartiment qui restreint l'accès à un point de terminaison spécifique à l'aide de la clé de sourceVpce condition aws :. La politique suivante refuse l'accès au compartiment spécifié à l'aide des actions spécifiées à moins que le point de terminaison de passerelle spécifié ne soit utilisé. Notez que cette politique bloque l'accès au compartiment spécifié à l'aide des actions spécifiées via la AWS Management Console.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Exemple : Restreindre l'accès à un VPC

Vous pouvez créer une politique de compartiment qui restreint l'accès à des informations spécifiques à l'aide VPCs de la clé de sourceVpc condition aws :. Cela est utile si plusieurs points de terminaison sont configurés simultanémentVPC. La politique suivante refuse l'accès au compartiment spécifié en utilisant les actions spécifiées, sauf si la demande provient du compartiment spécifiéVPC. Notez que cette politique bloque l'accès au compartiment spécifié à l'aide des actions spécifiées via la AWS Management Console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
```

```
}
```

Example Exemple : restriction de l'accès à une plage d'adresses IP spécifique

Vous pouvez créer une politique qui restreint l'accès à des plages d'adresses IP spécifiques à l'aide de la clé de VpcSourceIp condition aws :. La politique suivante refuse l'accès au compartiment spécifié à l'aide des actions spécifiées à moins que la demande ne provienne de l'adresse IP spécifiée. Notez que cette politique bloque l'accès au compartiment spécifié à l'aide des actions spécifiées via la AWS Management Console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Exemple : Restreindre l'accès aux compartiments d'un domaine spécifique Compte AWS

Vous pouvez créer une politique qui restreint l'accès aux compartiments S3 dans un Compte AWS spécifique en utilisant la clé de condition `s3:ResourceAccount`. La politique suivante refuse l'accès aux compartiments S3 à l'aide des actions spécifiées à moins qu'ils ne proviennent du Compte AWS spécifié.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
```

```
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Association de tables de routage

Vous pouvez modifier les tables de routage qui sont associées au point de terminaison de passerelle. Lorsque vous associez une table de routage, nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau du point de terminaison. Lorsque vous dissociez une table de routage, nous supprimons automatiquement le point de terminaison de la table de routage.

Pour associer des tables de routage à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, Gérer les tables de routage.
5. Sélectionnez ou désélectionnez les tables de routage si nécessaire.
6. Choisissez Modify route tables (Modifier les tables de routage).

Pour associer des tables de routage à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Modifier la politique du VPC point de terminaison

Vous pouvez modifier la politique de point de terminaison d'un point de terminaison de passerelle, qui contrôle l'accès à Amazon S3 depuis le VPC point de terminaison. La politique par défaut permet

un accès complet. Pour de plus amples informations, veuillez consulter Politiques de point de terminaison.

Pour modifier la politique de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, Manage policy (Gérer la politique).
5. Choisissez Full Access (Accès complet) pour autoriser un accès complet au service, ou choisissez Custom (Personnalisé) et joignez une politique personnalisée.
6. Choisissez Save (Enregistrer).

Voici des exemples de stratégies point de terminaison pour accéder à Amazon S3.

Example Exemple : restriction de l'accès à un compartiment spécifique

Vous pouvez créer une stratégie qui restreint l'accès uniquement à des compartiments S3 spécifiques. Ceci est utile si vous Services AWS en avez d'autres VPC qui utilisent des compartiments S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example Exemple : restreindre l'accès à un IAM rôle spécifique

Vous pouvez créer une politique qui restreint l'accès à un IAM rôle spécifique. Vous devez utiliser `aws:PrincipalArn` pour accorder l'accès à un principal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example Exemple : restriction de l'accès aux utilisateurs dans un compte spécifique

Vous pouvez créer une politique qui restreint l'accès à un compte spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
```

```
}
```

Suppression d'un point de terminaison de passerelle

Lorsque vous avez terminé avec un point de terminaison de passerelle, vous pouvez le supprimer. Lorsque vous supprimez un point de terminaison de passerelle, nous supprimons l'itinéraire du point de terminaison des tables de routage du sous-réseau.

Vous ne pouvez pas supprimer un point de terminaison de passerelle si le mode privé DNS est activé.

Pour supprimer un point de terminaison de passerelle à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer un point de terminaison de passerelle à l'aide de la ligne de commande

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Outils pour Windows PowerShell)

Points de terminaison de passerelle pour Amazon DynamoDB

Vous pouvez accéder à Amazon DynamoDB depuis VPC vos points de terminaison de passerelle d'utilisation. VPC Après avoir créé le point de terminaison de la passerelle, vous pouvez l'ajouter en tant que cible dans votre table de routage pour le trafic destiné VPC à DynamoDB.

Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle.

DynamoDB prend en charge à la fois les points de terminaison de passerelle et les points de terminaison d'interface. Avec un point de terminaison passerelle, vous pouvez accéder à DynamoDB depuis VPC votre ordinateur, sans avoir besoin d'une passerelle Internet NAT ou d'VPCun appareil, et sans frais supplémentaires. Toutefois, les points de terminaison de la passerelle n'autorisent pas l'accès depuis des réseaux locaux, depuis des réseaux homologues VPCs dans d'autres

AWS régions ou via une passerelle de transit. Pour ces scénarios, vous devez utiliser un point de terminaison d'interface qui est disponible moyennant des frais supplémentaires. Pour plus d'informations, consultez la section Types de VPC points de terminaison pour DynamoDB dans le manuel du développeur Amazon DynamoDB.

Table des matières

Considérations

- Le point de terminaison de passerelle est disponible uniquement dans la Région où vous l'avez créé. Veillez à créer votre point de terminaison de passerelle dans la même Région que vos tables DynamoDB.
- Si vous utilisez les DNS serveurs Amazon, vous devez activer à la fois les DNSnoms d'hôte et DNS la résolution pour votreVPC. Si vous utilisez votre propre DNS serveur, assurez-vous que les demandes adressées à DynamoDB sont correctement résolues vers les adresses IP gérées par. AWS
- Les règles des groupes de sécurité pour les instances qui accèdent à DynamoDB par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination de DynamoDB. Vous pouvez faire référence à l'ID de la liste de préfixes pour DynamoDB dans les règles du groupe de sécurité.
- Le réseau ACL du sous-réseau de vos instances qui accèdent à DynamoDB via un point de terminaison de passerelle doit autoriser le trafic à destination et en provenance de DynamoDB. Vous ne pouvez pas faire référence à des listes de préfixes dans ACL les règles réseau, mais vous pouvez obtenir la plage d'adresses IP de DynamoDB à partir de la liste de préfixes de DynamoDB.
- Si vous enregistrez AWS CloudTrail les opérations DynamoDB, les fichiers journaux contiennent les adresses IP privées des instances du VPC consommateur de services et l'ID EC2 du point de terminaison de la passerelle pour toutes les demandes effectuées via le point de terminaison.
- Les points de terminaison de la passerelle prennent en charge uniquement IPv4 le trafic.

- Les IPv4 adresses source des instances de vos sous-réseaux concernés passent des IPv4 adresses publiques aux IPv4 adresses privées de votreVPC. Un point de terminaison change de route réseau et déconnecte TCP les connexions ouvertes. Les connexions précédentes qui utilisaient des IPv4 adresses publiques ne sont pas reprises. Nous vous recommandons de ne pas exécuter de tâches importantes lorsque vous créez ou modifiez un point de terminaison de passerelle. Vous pouvez également vérifier que votre logiciel peut se reconnecter automatiquement à DynamoDB en cas de rupture de connexion.
- Les connexions aux points de terminaison ne peuvent pas être étendues à partir d'unVPC. Les ressources situées de l'autre côté d'une connexion, d'une VPN connexion d'VPCappairage, d'une passerelle de transit ou d'une AWS Direct Connect connexion dans votre établissement VPC ne peuvent pas utiliser un point de terminaison de passerelle pour communiquer avec DynamoDB.
- Votre compte dispose d'un quota par défaut de 20 points de terminaison de passerelle par Région, qui est réglable. Il existe également une limite de 255 points de terminaison de passerelle par. VPC

Créer un point de terminaison de passerelle

Utilisez la procédure suivante pour créer un point de terminaison de passerelle qui se connecte à DynamoDB.

Pour créer un point de terminaison de passerelle à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Services AWS.
5. Pour les services, ajoutez le filtre Type = Gateway et sélectionnez com.amazonaws.*region*.dynamodb.
6. Pour VPC, sélectionnez le point de terminaison VPC dans lequel vous souhaitez créer le point de terminaison.
7. Pour Configure route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau de point de terminaison.
8. Pour Policy, sélectionnez Accès complet pour autoriser toutes les opérations effectuées par tous les principaux sur toutes les ressources du VPC point de terminaison. Sinon, sélectionnez Personnalisé pour associer une politique de point de VPC terminaison qui contrôle les

autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le VPC point de terminaison.

9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison de passerelle à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Contrôlez l'accès à l'aide IAM de politiques

Vous pouvez créer des IAM politiques pour contrôler les IAM principaux autorisés à accéder aux tables DynamoDB à l'aide d'un point de terminaison spécifique. VPC

Example Exemple : restriction de l'accès à un point de terminaison spécifique

Vous pouvez créer une politique qui restreint l'accès à un point de VPC terminaison spécifique à l'aide de la clé de sourceVpce condition aws :. La politique suivante refuse l'accès aux tables DynamoDB du compte, sauf si le point de terminaison VPC spécifié est utilisé. Cet exemple suppose qu'il existe également une déclaration de politique qui autorise l'accès requis pour vos cas d'utilisation.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
```

```
   ]
}
```

Example Exemple : autoriser l'accès à partir d'un IAM rôle spécifique

Vous pouvez créer une politique qui autorise l'accès à l'aide d'un IAM rôle spécifique. La politique suivante accorde l'accès au IAM rôle spécifié.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
      }
   ]
}
```

Example Exemple : autorisation d'accès à partir d'un compte spécifique

Vous pouvez créer une politique qui n'autorise l'accès qu'à partir d'un compte spécifique. La politique suivante accorde l'accès aux utilisateurs du compte spécifié.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
```

```
            }
         }
      }
   ]
}
```

Association de tables de routage

Vous pouvez modifier les tables de routage qui sont associées au point de terminaison de passerelle. Lorsque vous associez une table de routage, nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau du point de terminaison. Lorsque vous dissociez une table de routage, nous supprimons automatiquement le point de terminaison de la table de routage.

Pour associer des tables de routage à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, Gérer les tables de routage.
5. Sélectionnez ou désélectionnez les tables de routage si nécessaire.
6. Choisissez Modify route tables (Modifier les tables de routage).

Pour associer des tables de routage à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Modifier la politique du VPC point de terminaison

Vous pouvez modifier la politique de point de terminaison d'un point de terminaison de passerelle, qui contrôle l'accès à DynamoDB depuis VPC le point de terminaison. La politique par défaut permet un accès complet. Pour de plus amples informations, veuillez consulter Politiques de point de terminaison.

Pour modifier la politique de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, Manage policy (Gérer la politique).
5. Choisissez Full Access (Accès complet) pour autoriser un accès complet au service, ou choisissez Custom (Personnalisé) et joignez une politique personnalisée.
6. Choisissez Save (Enregistrer).

Pour modifier un point de terminaison de passerelle à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Voici des exemples de stratégies de point de terminaison pour accéder à DynamoDB.

Example Exemple : autorisation d'accès en lecture seule

Vous pouvez créer une politique qui restreint l'accès en lecture seule. La politique suivante accorde l'autorisation de lister et de décrire les tables DynamoDB.

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Exemple : restreindre l'accès à une table spécifique

Vous pouvez créer une stratégie qui restreint l'accès à une table DynamoDB spécifique. La politique suivante autorise l'accès à la table DynamoDB spécifiée.

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

Suppression d'un point de terminaison de passerelle

Lorsque vous avez terminé avec un point de terminaison de passerelle, vous pouvez le supprimer. Lorsque vous supprimez un point de terminaison de passerelle, nous supprimons l'itinéraire du point de terminaison des tables de routage du sous-réseau.

Pour supprimer un point de terminaison de passerelle à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer un point de terminaison de passerelle à l'aide de la ligne de commande

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Outils pour Windows PowerShell)

Accédez aux produits SaaS via AWS PrivateLink

En utilisant AWS PrivateLink, vous pouvez accéder aux produits SaaS en privé, comme s'ils s'exécutaient vous-mêmeVPC.

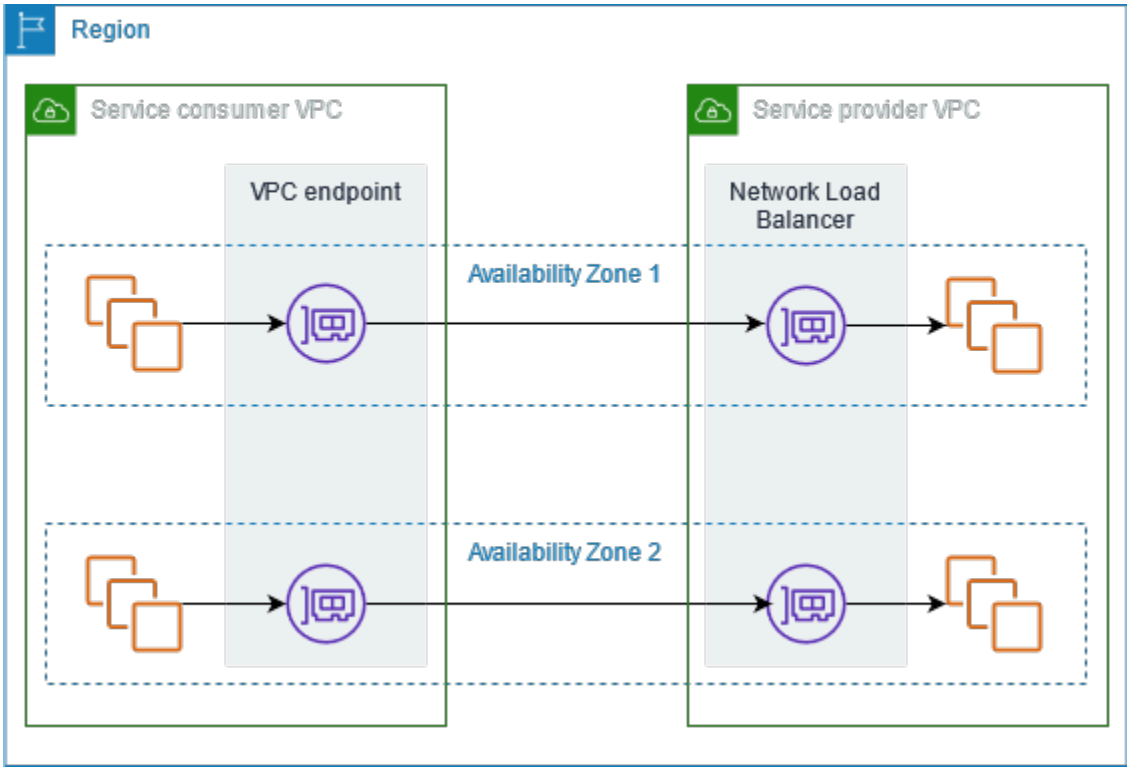
Table des matières

Présentation

Vous pouvez découvrir, acheter et fournir des produits SaaS optimisés par le AWS PrivateLink biais de AWS Marketplace. Pour plus d'informations, consultez Accéder aux applications SaaS de manière sécurisée et privée à l'aide AWS PrivateLink de

Vous pouvez également trouver des produits SaaS développés par AWS PrivateLink des AWS partenaires. Pour plus d'informations, voir Partenaires AWS PrivateLink.

Le schéma suivant montre comment vous utilisez les VPC points de terminaison pour vous connecter aux produits SaaS. Le fournisseur du service crée un service de point de terminaison et autorise ses clients à accéder au service de point de terminaison. En tant que consommateur de services, vous créez un point de VPC terminaison d'interface, qui établit des connexions entre un ou plusieurs sous-réseaux de votre service VPC et du service de point de terminaison.



Création d'un point de terminaison d'interface

Utilisez la procédure suivante pour créer un point de VPC terminaison d'interface qui se connecte au produit SaaS.

Exigence

Abonnez-vous au service.

Pour créer un point de terminaison d'interface vers un service partenaire

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Si vous avez acheté le service auprès de AWS Marketplace, procédez comme suit :
    a. Dans Type, sélectionnez AWS Marketplace services.
    b. Sélectionnez le service.
5. Si vous êtes abonné à un service portant la désignation AWS Service Ready, procédez comme suit :

   a. Pour Type, choisissez PrivateLink Ready partner services.
   b. Entrez le nom du service, puis choisissez Vérifier le service.
6. Pour VPC, sélectionnez celui VPC à partir duquel vous allez accéder au produit.
7. Pour les sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer les interfaces réseau des points de terminaison.
8. Pour Security groups (Groupes de sécurité), sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison. Les règles du groupe de sécurité doivent autoriser le trafic entre les ressources des interfaces réseau VPC et celles du point de terminaison.
9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison.

Pour configurer un point de terminaison d'interface

Pour plus d'informations sur la configuration du point de terminaison de votre interface, voir the section called “Configuration d'un point de terminaison d'interface”.

Accédez aux appliances virtuelles via AWS PrivateLink

Vous pouvez utiliser un équilibreur de charge de passerelle pour distribuer le trafic à un parc d'appliances virtuelles réseau. Les appliances peuvent être utilisées pour l'inspection de sécurité, la conformité, les contrôles de stratégie et d'autres services de mise en réseau. Vous spécifiez le Gateway Load Balancer lorsque vous créez un service de point de VPC terminaison. D'autres principaux AWS accèdent au service de point de terminaison en créant un point de terminaison d'équilibreur de charge de passerelle.

Tarification

Vous êtes facturé pour chaque heure pendant laquelle votre point de terminaison Gateway Load Balancer est approvisionné dans chaque zone de disponibilité. Vous êtes également facturé par Go de données traitées. Pour plus d'informations, consultez AWS PrivateLink Pricing (Tarification CTlong).

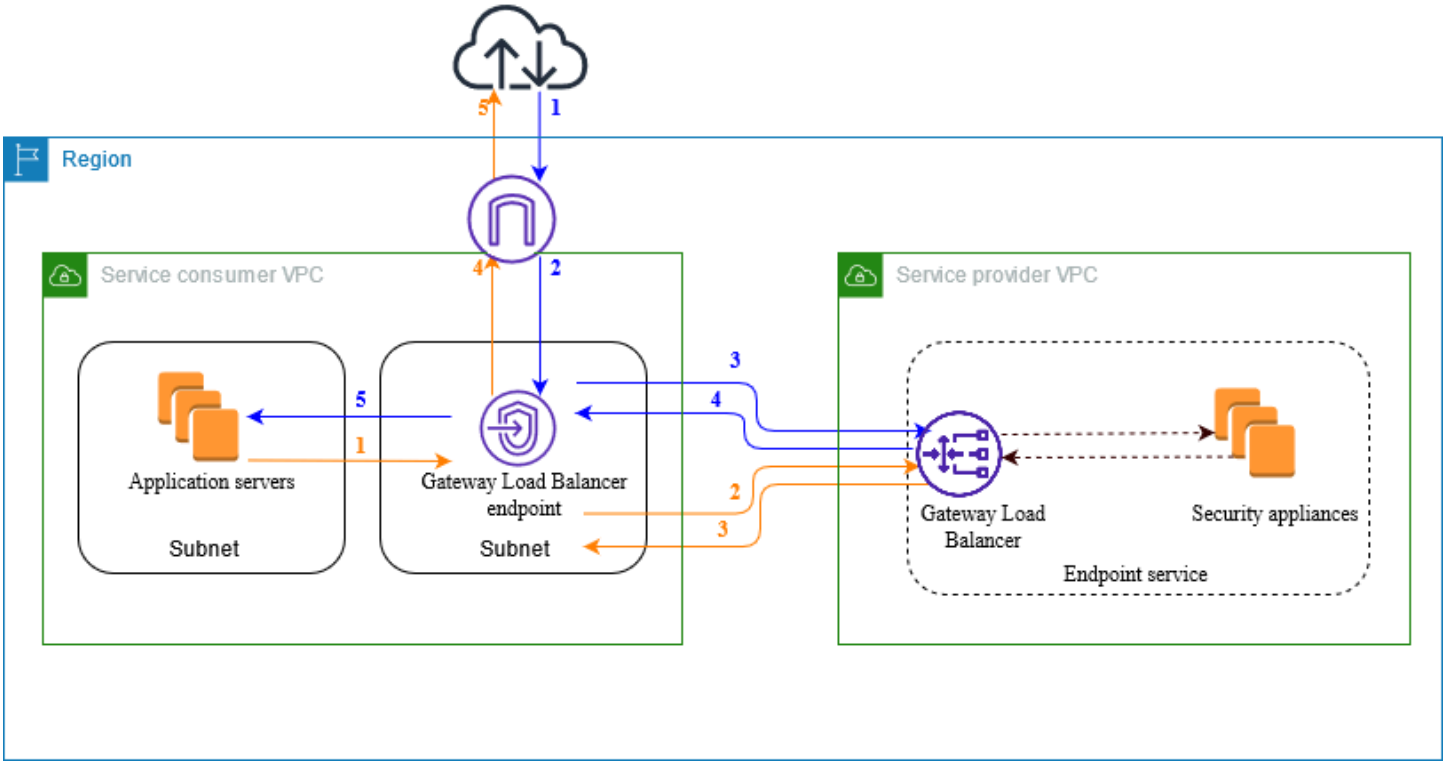
Table des matières

Pour plus d'informations, consultez Gateway Load Balancers.

Présentation

Le schéma suivant montre comment les serveurs d'applications accèdent aux dispositifs de sécurité AWS PrivateLink. Les serveurs d'applications s'exécutent dans un sous-réseau du consommateur VPC de services. Vous créez un point de terminaison Gateway Load Balancer dans un autre sous-réseau du même. VPC Tout le trafic entrant dans le consommateur de services VPC via la passerelle Internet est d'abord acheminé vers le point de terminaison Gateway Load Balancer pour inspection, puis acheminé vers le sous-réseau de destination. De même, tout le trafic quittant les serveurs

d'applications est acheminé vers le point de terminaison d'équilibreur de charge de passerelle pour être inspecté avant d'être réacheminé par la passerelle Internet.



Trafic depuis Internet vers les serveurs d'applications (flèches bleues) :

1. Le trafic entre dans le consommateur de services VPC via la passerelle Internet.
2. Le trafic est envoyé au point de terminaison d'équilibreur de charge de passerelle, en fonction de la configuration de la table de routage.
3. Le trafic est envoyé à l'équilibreur de charge de passerelle pour être inspecté par le dispositif de sécurité.
4. Le trafic est renvoyé au point de terminaison d'équilibreur de charge de passerelle après inspection.
5. Le trafic est envoyé aux serveurs d'applications, en fonction de la configuration de la table de routage.

Trafic des serveurs d'application vers Internet (flèches oranges) :

1. Le trafic est envoyé au point de terminaison d'équilibreur de charge de passerelle, en fonction de la configuration de la table de routage.

2. Le trafic est envoyé à l'équilibreur de charge de passerelle pour être inspecté par le dispositif de sécurité.
3. Le trafic est renvoyé au point de terminaison d'équilibreur de charge de passerelle après inspection.
4. Le trafic est envoyé à la passerelle Internet en fonction de la configuration de la table de routage.
5. Le trafic est redirigé vers Internet.

Types d'adresses IP

Les fournisseurs de services peuvent mettre leurs points de terminaison de service à la disposition des consommateurs de services IPv4IPv6, ou IPv4 les deuxIPv6, même si leurs dispositifs de sécurité sont uniquement IPv4 compatibles. Si vous activez le support dualstack, les clients existants peuvent continuer IPv4 à utiliser votre service et les nouveaux consommateurs peuvent choisir de l'utiliser pour accéder IPv6 à votre service.

Si un point de terminaison Gateway Load Balancer est compatibleIPv4, les interfaces réseau du point de terminaison ont IPv4 des adresses. Si un point de terminaison Gateway Load Balancer est compatibleIPv6, les interfaces réseau du point de terminaison ont IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison est inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Conditions requises IPv6 pour activer un service de point de terminaison

- Les sous-réseaux VPC et du service de point de terminaison doivent être associés à des IPv6 CIDR blocs.
- L’équilibreur de charge de la Passerelle du service du point de terminaison doit utiliser le type d'adresse IP dualstack. Les dispositifs de sécurité n'ont pas besoin de prendre en charge IPv6 le trafic.

Conditions requises IPv6 pour activer un point de terminaison Gateway Load Balancer

- Le service de point de terminaison doit avoir un type d'adresse IP qui inclut IPv6 le support.
- Le type d'adresse IP d'un point de terminaison d'interface équilibreur de charge de la Passerelle doit être compatible avec le sous-réseau du point de terminaison équilibreur de charge de la Passerelle, comme décrit ici :

- IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
- IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
- Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

- Les tables de routage des sous-réseaux du consommateur de services VPC doivent acheminer le IPv6 trafic et le réseau ACLs de ces sous-réseaux doit autoriser IPv6 le trafic.

Routage

Pour acheminer le trafic vers le service de point de terminaison, spécifiez le point de terminaison d'équilibreur de charge de passerelle comme cible dans vos tables de routage, à l'aide de son ID. Pour le schéma ci-dessus, ajoutez des itinéraires aux tables de routage comme suit. Notez que IPv6 les routes sont incluses pour une configuration à double pile.

Table de routage pour la passerelle Internet

Cette table de routage doit comporter un itinéraire qui envoie le trafic destiné aux serveurs d'applications vers le point de terminaison d'équilibreur de charge de passerelle.

Destination	Target
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

Table de routage pour le sous-réseau avec les serveurs d'applications

Cette table de routage doit comporter un itinéraire qui envoie le trafic destiné aux serveurs d'applications vers le point de terminaison d'équilibreur de charge de passerelle.

Destination	Target
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Locale
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Table de routage pour le sous-réseau avec le point de terminaison d' équilibreur de charge de passerelle

Cette table de routage doit envoyer le trafic renvoyé par l'inspection vers sa destination finale. Pour le trafic provenant d'Internet, l'itinéraire local envoie le trafic vers les serveurs d'applications. Pour le trafic provenant des serveurs d'applications, ajoutez un itinéraire qui envoie tout le trafic à la passerelle Internet.

Destination	Target
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Locale
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Création d'un système d'inspection en tant que service de point de terminaison d'équilibreur de charge de passerelle

Vous pouvez créer votre propre service alimenté par AWS PrivateLink, connu sous le nom de service de point de terminaison. Vous êtes le fournisseur de services, et les AWS principaux responsables qui créent des connexions avec votre service sont les consommateurs de services.

Les services de point de terminaison nécessitent un Network Load Balancer (équilibreur de charge de réseau) ou un Gateway Load Balancer (équilibreur de charge de passerelle). Dans ce cas, vous

allez créer un service de point de terminaison à l'aide de l'équilibreur de charge de passerelle. Pour plus d'informations sur la création d'un service de point de terminaison à l'aide d'un Network Load Balancer (équilibreur de charge de réseau), voir Création d'un service de point de terminaison.

Table des matières

Considérations

- Le service de point de terminaison n'est disponible que dans la Région où vous l'avez créé.
- Lorsque les consommateurs du service extraient des informations sur un service de point de terminaison, ils ne peuvent voir que les zones de disponibilité qu'ils ont en commun avec le fournisseur du service. Lorsque le fournisseur du service et le consommateur du service se trouvent dans des comptes différents, un nom de zone de disponibilité, tel que `us-east-1a`, peut être mappé à une zone de disponibilité physique différente dans chaque Compte AWS. Vous pouvez utiliser AZ IDs pour identifier systématiquement les zones de disponibilité de votre service. Pour plus d'informations, consultez la section AZ IDs dans le guide de EC2 l'utilisateur Amazon.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour de plus amples informations, veuillez consulter AWS PrivateLink quotas.

Prérequis

- Créez un fournisseur de services VPC avec au moins deux sous-réseaux dans la zone de disponibilité dans laquelle le service doit être disponible. Un sous-réseau est destiné aux instances du dispositif de sécurité et l'autre est destiné à l'équilibreur de charge de passerelle.
- Créez un Gateway Load Balancer chez votre fournisseur de services. VPC Si vous envisagez d'activer le IPv6 support sur votre service de point de terminaison, vous devez activer le support dualstack sur votre Gateway Load Balancer. Pour plus d'informations, veuillez consulter Mise en route des équilibreurs de charge de passerelle.
- Lancez des dispositifs de sécurité chez le fournisseur de services VPC et enregistrez-les auprès d'un groupe cible d'équilibreurs de charge.

Création du service de point de terminaison

Utilisez la procédure suivante pour créer un service de point de terminaison à l'aide d'un équilibreur de charge de passerelle.

Pour créer un service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Choisissez Create endpoint service (Créer un service de point de terminaison).
4. Pour Load balancer type (Type d'équilibreur de charge), choisissez Gateway (Passerelle).
5. Pour Available load balancers (Équilibreurs de charge disponibles), sélectionnez l'équilibreur de charge de passerelle.
6. Dans la section Require acceptance for endpoint (Acceptation requise pour le point de terminaison), sélectionnez Acceptance required (Acceptation requise) pour exiger que les demandes de connexion à votre service de point de terminaison soient acceptées manuellement. Sinon, ils sont acceptés automatiquement.
7. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
   - Sélectionner IPv4— Activez le service de point de terminaison pour qu'il accepte les IPv4 demandes.
   - Sélectionner IPv6— Activez le service de point de terminaison pour qu'il accepte les IPv6 demandes.
   - Sélectionnez IPv4et IPv6— Activez le service de point de terminaison pour qu'il accepte à la fois les IPv6 demandes IPv4 et.
8. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
9. Sélectionnez Create (Créer).

Pour créer un service de point de terminaison à l'aide de la ligne de commande

- create-vpc-endpoint-service-configuration ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Assurer la disponibilité de votre service de point de terminaison

Les fournisseurs du service doivent faire ce qui suit pour mettre leurs services à la disposition des consommateurs du service.

- Ajoutez des autorisations qui permettent à chaque utilisateur de se connecter à votre service de point de terminaison. Pour de plus amples informations, veuillez consulter the section called “Gestion des autorisations”.
- Fournissez au consommateur du service le nom de votre service et les zones de disponibilité prises en charge afin qu'il puisse créer un point de terminaison d'interface pour se connecter à votre service. Pour plus d'informations, consultez la procédure ci-dessous.
- Acceptez la demande de connexion au point de terminaison de la part du consommateur du service. Pour plus d'informations, voir the section called “Acceptation ou refus des demandes de connexion”.

AWS les principaux peuvent se connecter à votre service de point de terminaison en privé en créant un point de terminaison Gateway Load Balancer. Pour de plus amples informations, veuillez consulter Créer un point de terminaison d'équilibreur de charge de passerelle.

Accès à un système d'inspection à l'aide d'un point de terminaison d'équilibreur de charge de passerelle

Vous pouvez créer un point de terminaison d'équilibreur de charge de passerelle pour vous connecter aux services de points de terminaison développés par AWS PrivateLink.

Pour chaque sous-réseau que vous spécifiez à partir de votreVPC, nous créons une interface réseau de point de terminaison dans le sous-réseau et lui attribuons une adresse IP privée à partir de la plage d'adresses du sous-réseau. Une interface réseau de point de terminaison est une interface réseau gérée par le demandeur ; vous pouvez la visualiser dans votre Compte AWS, mais vous ne pouvez pas la gérer vous-même.

Des frais s'appliquent à l'utilisation horaire et au traitement de données. Pour plus d'informations, veuillez consulter Tarification des points de terminaison de équilibreur de charge de passerelle.

Table des matières

- Prérequis
- Créer le point de terminaison
- Configurer le routage
- Gérer les balises
- Suppression d'un point de terminaison d'équilibreur de charge de passerelle

Considérations

- Vous ne pouvez choisir qu'une seule zone de disponibilité dans le client du serviceVPC. Vous ne pourrez plus changer ce sous-réseau par la suite. Pour utiliser un point de terminaison d'équilibreur de charge de passerelle dans un sous-réseau différent, vous devez créer un point de terminaison d'équilibreur de charge de passerelle.
- Vous pouvez créer un seul point de terminaison d'équilibreur de charge de passerelle par zone de disponibilité et par service, et vous devez sélectionner la zone de disponibilité que l'équilibreur de charge de passerelle prend en charge. Lorsque le fournisseur du service et le consommateur du service se trouvent dans des comptes différents, un nom de zone de disponibilité, tel que `us-east-1a`, peut être mappé à une zone de disponibilité physique différente dans chaque Compte AWS. Vous pouvez utiliser AZ IDs pour identifier systématiquement les zones de disponibilité de votre service. Pour plus d'informations, consultez la section AZ IDs dans le guide de EC2 l'utilisateur Amazon.
- Pour pouvoir utiliser le service de point de terminaison, le fournisseur du service doit accepter les demandes de connexion. Le service ne peut pas envoyer de demandes aux ressources de votre ordinateur VPC via le VPC point de terminaison. Le point de terminaison renvoie uniquement des réponses au trafic initié par les ressources de votreVPC.
- Chaque point de terminaison de l’équilibreur de charge Passerelle peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et augmente automatiquement jusqu'à 100 Gbit/s.
- Si un service de point de terminaison est associé à plusieurs équilibreurs de charge de passerelle, un point de terminaison d'équilibreur de charge de passerelle établit une connexion avec un seul équilibreur de charge par zone de disponibilité.
- Pour que le trafic reste dans la même zone de disponibilité, nous vous recommandons de créer un point de terminaison d'équilibreur de charge de passerelle dans chaque zone de disponibilité vers laquelle vous enverrez du trafic.

- La préservation de l'adresse IP du client Network Load Balancer n'est pas prise en charge lorsque le trafic est acheminé via un point de terminaison Gateway Load Balancer, même si la cible se trouve dans le même emplacement que le Network VPC Load Balancer.
- Si les serveurs d'applications et le point de terminaison Gateway Load Balancer se trouvent dans le même sous-réseau, les NACL règles sont évaluées pour le trafic entre les serveurs d'applications et le point de terminaison Gateway Load Balancer.
- Si vous utilisez un Gateway Load Balancer avec une passerelle Internet de sortie uniquement, le trafic est supprimé. IPv6 Utilisez plutôt une passerelle Internet et des règles de pare-feu entrant.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour de plus amples informations, veuillez consulter AWS PrivateLink quotas.

Prérequis

- Créez un consommateur de services VPC avec au moins deux sous-réseaux dans la zone de disponibilité à partir de laquelle vous allez accéder au service. Un sous-réseau est destiné aux serveurs d'applications et l'autre au point de terminaison d'équilibreur de charge de passerelle.
- Pour vérifier quelles zones de disponibilité sont prises en charge par le service de point de terminaison, décrivez le service de point de terminaison à l'aide de la console ou de la describe-vpc-endpoint-servicescommande.
- Si vos ressources se trouvent dans un sous-réseau doté d'un réseauACL, vérifiez que le réseau ACL autorise le trafic entre les interfaces réseau du point de terminaison et les ressources duVPC.

Créer le point de terminaison

Utilisez la procédure suivante pour créer un point de terminaison d'équilibreur de charge de passerelle qui se connecte au service de point de terminaison pour le système d'inspection.

Pour créer un point de terminaison d'équilibreur de charge de passerelle à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Type, choisissez les services Endpoint qui utilisent NLBs et GWLBs.
5. Pour Service Name (Nom du service), saisissez le nom du service et choisissez Verify service (Vérifier le service).

6. Pour VPC, sélectionnez celui VPC à partir duquel vous allez accéder au service de point de terminaison.
7. Pour les sous-réseaux, sélectionnez un sous-réseau dans lequel créer une interface réseau de point de terminaison.
8. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
   - IPv4— Attribuez IPv4 des adresses à l'interface réseau du terminal. Cette option n'est prise en charge que si le sous-réseau sélectionné possède une plage d'IPv4adresses.
   - IPv6— Attribuez IPv6 des adresses à l'interface réseau du terminal. Cette option n'est prise en charge que si le sous-réseau sélectionné est un sous-réseau IPv6 unique.
   - Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses à l'interface réseau du point de terminaison. Cette option n'est prise en charge que si le sous-réseau sélectionné possède à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.
9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison. L'état initial est `pending acceptance`.

Pour créer un point de terminaison d'équilibreur de charge de passerelle à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Configurer le routage

Utilisez la procédure suivante pour configurer les tables de routage pour le client du serviceVPC. Cela permet aux dispositifs de sécurité d'effectuer une inspection de sécurité du trafic entrant destiné aux serveurs d'applications. Pour de plus amples informations, veuillez consulter the section called "Routage".

Pour configurer le routage à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Tables de routage.
3. Sélectionnez la table de routage pour la passerelle Internet et procédez comme suit :

a. Choisissez Actions, Modifier les routes.

b. Si vous êtes d'IPv4accord, choisissez Ajouter un itinéraire. Pour Destination, entrez le IPv4 CIDR bloc du sous-réseau pour les serveurs d'applications. Pour Target, sélectionnez le VPC point de terminaison.

c. Si vous êtes d'IPv6accord, choisissez Ajouter un itinéraire. Pour Destination, entrez le IPv6 CIDR bloc du sous-réseau pour les serveurs d'applications. Pour Target, sélectionnez le VPC point de terminaison.

d. Sélectionnez Enregistrer les modifications.

4. Sélectionnez la table de routage pour le sous-réseau avec les serveurs d'applications et procédez comme suit :

   a. Choisissez Actions, Modifier les routes.

   b. Si vous êtes d'IPv4accord, choisissez Ajouter un itinéraire. En regard de Destination, entrez **`0.0.0.0/0`**. Pour Target, sélectionnez le VPC point de terminaison.

   c. Si vous êtes d'IPv6accord, choisissez Ajouter un itinéraire. En regard de Destination, entrez **`::/0`**. Pour Target, sélectionnez le VPC point de terminaison.

   d. Sélectionnez Enregistrer les modifications.

5. Sélectionnez la table de routage pour le sous-réseau avec le point de terminaison d'équilibreur de charge de passerelle, puis procédez comme suit :

   a. Choisissez Actions, Modifier les routes.

   b. Si vous êtes d'IPv4accord, choisissez Ajouter un itinéraire. En regard de Destination, entrez **`0.0.0.0/0`**. Pour Target (Cible), sélectionnez la passerelle Internet.

   c. Si vous êtes d'IPv6accord, choisissez Ajouter un itinéraire. En regard de Destination, entrez **`::/0`**. Pour Target (Cible), sélectionnez la passerelle Internet.

   d. Sélectionnez Enregistrer les modifications.

Pour configurer le routage à l'aide de la ligne de commande

- create-route (AWS CLI)
- New-EC2Route(Outils pour Windows PowerShell)

Gérer les balises

Vous pouvez baliser votre point de terminaison d'équilibreur de charge de passerelle pour vous aider à l'identifier ou à le catégoriser en fonction des besoins de votre organisation.

Pour gérer les balises à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Manage tags (Gérer les balises).
5. Pour chaque balise à ajouter, choisissez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Save (Enregistrer).

Pour gérer les balises à l'aide de la ligne de commande

- create-tags et delete-tags (AWS CLI)
- New-EC2Taget Remove-EC2Tag(Outils pour Windows PowerShell)

Suppression d'un point de terminaison d'équilibreur de charge de passerelle

Lorsque vous avez terminé avec un point de terminaison, vous pouvez le supprimer. La suppression d'un point de terminaison d'équilibreur de charge de passerelle supprime également les interfaces réseau du point de terminaison. Vous ne pouvez pas supprimer un point de terminaison d'un équilibreur de charge de passerelle s'il existe des itinéraires dans vos tables de routage qui pointent vers ce point de terminaison.

Pour supprimer un point de terminaison d'équilibreur de charge de passerelle

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Points de terminaison, puis sélectionnez votre point de terminaison.
3. Choisissez Actions, Supprimer le point de terminaison.

4. Dans le message de confirmation, sélectionnez Oui, supprimer.

Pour supprimer un point de terminaison d'équilibreur de charge de passerelle

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

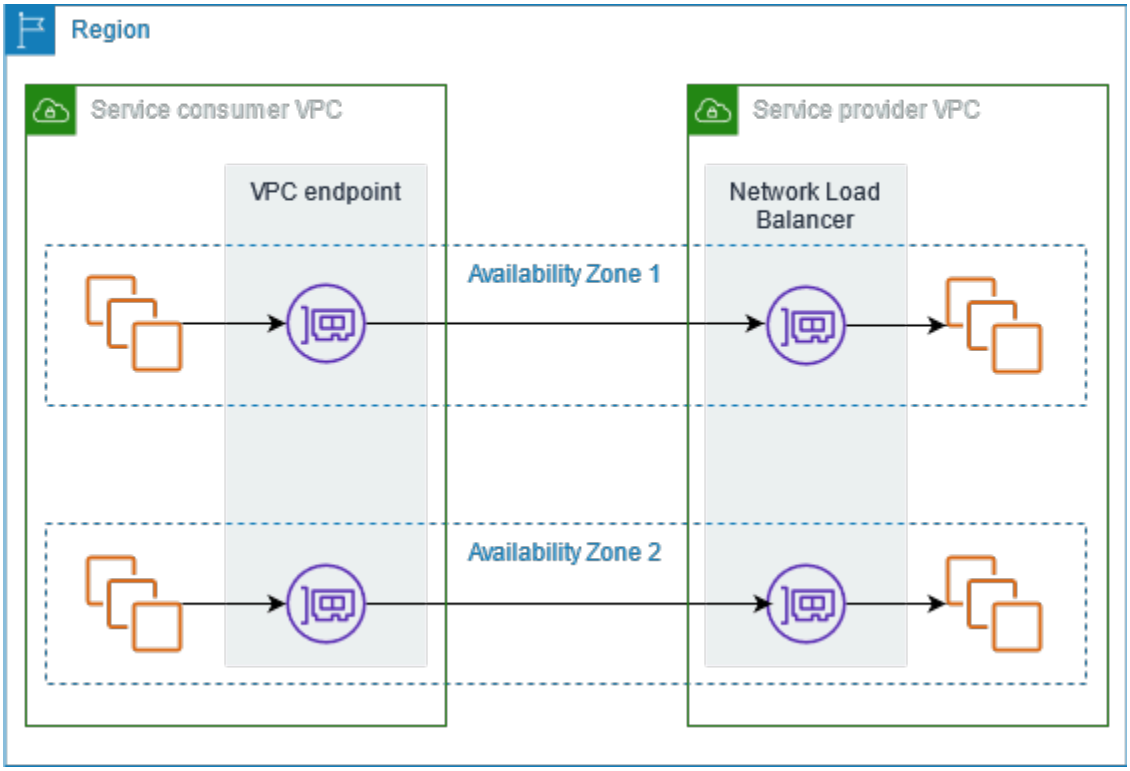
Partagez vos services via AWS PrivateLink

Vous pouvez héberger votre propre service AWS PrivateLink optimisé, appelé service de point de terminaison, et le partager avec d'autres AWS clients.

Table des matières

Présentation

Le schéma suivant montre comment vous partagez votre service hébergé AWS avec d'autres AWS clients, et comment ces clients se connectent à votre service. En tant que fournisseur de services, vous créez un Network Load Balancer dans votre interface en VPC tant que service. Vous sélectionnez ensuite cet équilibreur de charge lorsque vous créez la configuration du service de VPC point de terminaison. Vous accordez l'autorisation à des principaux AWS spécifiques afin qu'ils puissent se connecter à votre service. En tant que consommateur de services, le client crée un point de VPC terminaison d'interface, qui établit des connexions entre les sous-réseaux qu'il sélectionne auprès de son service de point de terminaison VPC et celui de votre service de point de terminaison. L'équilibreur de charge reçoit les demandes du consommateur du service et les achemine vers les cibles hébergeant votre service.



Pour une faible latence et une haute disponibilité, nous vous recommandons de rendre votre service disponible dans au moins deux zones de disponibilité.

DNSnoms d'hôtes

Lorsqu'un fournisseur de services crée un service de point de VPC terminaison, il AWS génère un DNS nom d'hôte spécifique au point de terminaison pour le service. Les noms ont la syntaxe suivante :

```
endpoint_service_id.region.vpce.amazonaws.com
```

Voici un exemple de DNS nom d'hôte pour un service de point de VPC terminaison dans la région us-east-2 :

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

Lorsqu'un client de services crée un point de VPC terminaison d'interface, nous créons des DNS noms régionaux et zonaux que le consommateur de services peut utiliser pour communiquer avec le service de point de terminaison. Les noms régionaux ont la syntaxe suivante :

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

Les noms zonaux ont la syntaxe suivante :

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

Privé DNS

Un fournisseur de services peut également associer un DNS nom privé à son service de point de terminaison, afin que les consommateurs du service puissent continuer à accéder au service en utilisant son DNS nom existant. Si un fournisseur de services associe un DNS nom privé à son service de point de terminaison, les consommateurs de services peuvent activer des DNS noms privés pour les points de terminaison de leur interface. Si un fournisseur de services n'active pas le mode privéDNS, les consommateurs de services devront peut-être mettre à jour leurs applications pour utiliser le DNS nom public du service de point de VPC terminaison. Pour de plus amples informations, veuillez consulter Gérer les DNS noms.

Accès interrégional

Un fournisseur de services peut héberger un service dans une région et le rendre disponible dans un ensemble de régions prises en charge. Un consommateur de services sélectionne une région de service lors de la création d'un point de terminaison.

Autorisations

- Par défaut, IAM les entités ne sont pas autorisées à rendre un service de point de terminaison disponible dans plusieurs régions ou à accéder à un service de point de terminaison dans plusieurs régions. Pour accorder les autorisations requises pour l'accès entre régions, un IAM administrateur peut créer des IAM politiques qui autorisent l'action avec `vpce:AllowMultiRegion` autorisation uniquement.
- Pour contrôler les régions qu'une IAM entité peut spécifier comme région prise en charge lors de la création d'un service de point de terminaison, utilisez la clé de `ec2:VpceSupportedRegion` condition.
- Pour contrôler les régions qu'une IAM entité peut spécifier en tant que région de service lors de la création d'un VPC point de terminaison, utilisez la clé de `ec2:VpceServiceRegion` condition.

Considérations

- Un fournisseur de services doit choisir une région optionnelle avant de l'ajouter en tant que région prise en charge pour un service de point de terminaison.
- Votre service de point de terminaison doit être accessible depuis sa région hôte. Vous ne pouvez pas supprimer la région hôte de l'ensemble des régions prises en charge. À des fins de redondance, vous pouvez déployer votre service de point de terminaison dans plusieurs régions et activer l'accès entre régions pour chaque service de point de terminaison.
- Un consommateur de services doit choisir une région optionnelle avant de la sélectionner comme région de service pour un terminal. Dans la mesure du possible, nous recommandons aux consommateurs d'accéder à un service en utilisant la connectivité intra-régionale plutôt que la connectivité interrégionale. La connectivité intra-régionale permet de réduire la latence et les coûts.
- Si un fournisseur de services supprime une région de l'ensemble des régions prises en charge, les consommateurs de services ne peuvent pas sélectionner cette région comme région de service lorsqu'ils créent de nouveaux points de terminaison. Notez que cela n'affecte pas l'accès au service de point de terminaison à partir de points de terminaison existants qui utilisent cette région comme région de service.
- Pour une haute disponibilité, les fournisseurs et les consommateurs doivent utiliser au moins deux zones de disponibilité. Notez que l'accès interrégional ne nécessite pas que les fournisseurs et les consommateurs utilisent les mêmes zones de disponibilité.
- Avec un accès interrégional, AWS PrivateLink gère le basculement entre les zones de disponibilité. Il ne gère pas le basculement entre les régions.
- L'accès interrégional n'est pas pris en charge pour les AWS Marketplace services dont le DNS nom est convivial.
- L'accès entre régions n'est pas pris en charge pour les équilibreurs de charge réseau dont une valeur personnalisée est configurée pour le délai d'TCPinactivité.
- L'accès entre régions n'est pas pris en charge en cas de UDP fragmentation.

Types d'adresses IP

Les fournisseurs de services peuvent mettre leurs points de terminaison de service à la disposition des consommateurs de services IPv4IPv6, ou IPv4 les deuxIPv6, même si leurs serveurs principaux sont uniquement compatibles. IPv4 Si vous activez le support dualstack, les clients existants peuvent continuer IPv4 à utiliser votre service et les nouveaux consommateurs peuvent choisir de l'utiliser pour accéder IPv6 à votre service.

Si un point de VPC terminaison d'interface est compatibleIPv4, les interfaces réseau du point de terminaison ont IPv4 des adresses. Si un point de VPC terminaison d'interface est compatibleIPv6, les interfaces réseau du point de terminaison ont IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison n'est pas accessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Conditions requises IPv6 pour activer un service de point de terminaison

- Les sous-réseaux VPC et du service de point de terminaison doivent être associés à des IPv6 CIDR blocs.
- Tous les équilibreurs de charge de réseau Network Load Balancers du service de point de terminaison doivent utiliser le type d'adresse IP dualstack. Les cibles n'ont pas besoin de prendre en charge IPv6 le trafic. Si le service traite les adresses IP sources à partir de l'en-tête du protocole proxy version 2, il doit traiter IPv6 les adresses.

Exigences relatives à l'activation IPv6 d'un point de terminaison d'interface

- Le service de point de terminaison doit prendre en charge IPv6 les demandes.
- Le type d'adresse IP d'un point de terminaison d'interface doit être compatible avec les sous-réseaux du point de terminaison d'interface, comme décrit ici :
  - IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
  - IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
  - Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

DNStype d'adresse IP d'enregistrement pour un point de terminaison d'interface

Le type d'adresse IP d'DNSenregistrement pris en charge par un point de terminaison d'interface détermine les DNS enregistrements que nous créons. Le type d'adresse IP d'DNSenregistrement d'un point de terminaison d'interface doit être compatible avec le type d'adresse IP du point de terminaison d'interface, comme décrit ici :

- IPv4— Créez des enregistrements A pour les DNS noms privés, régionaux et zonaux. Le type d'adresse IP doit être IPv4ou Dualstack.
- IPv6— Créez AAAA des enregistrements pour les DNS noms privés, régionaux et zonaux. Le type d'adresse IP doit être IPv6ou Dualstack.
- Dualstack — Créez A et AAAA enregistrez les noms privés, régionaux et DNS zonaux. Le type d'adresse IP doit être Dualstack.

Créez un service propulsé par AWS PrivateLink

Vous pouvez créer votre propre service alimenté par AWS PrivateLink, connu sous le nom de service de point de terminaison. Vous êtes le fournisseur du service et les principaux AWS qui créent des connexions à votre service sont les consommateurs du service.

Les services de point de terminaison nécessitent un Network Load Balancer (équilibreur de charge de réseau) ou un Gateway Load Balancer (équilibreur de charge de passerelle). L'équilibreur de charge reçoit des requêtes des consommateurs du service et les achemine vers votre service. Dans ce cas, vous allez créer un service de point de terminaison à l'aide d'un équilibreur de charge réseau Network Load Balancer. Pour plus d'informations sur la création d'un service de point de terminaison à l'aide d'un équilibreur de charge de passerelle Gateway Load Balancer, voir Accès à des dispositifs virtuels.

Table des matières

Considérations

- Le service de point de terminaison n'est disponible que dans la Région où vous l'avez créé. Les consommateurs peuvent accéder à votre service depuis d'autres régions si vous activez l'accès interrégional, ou s'ils utilisent le VPC peering ou une passerelle de transit.
- Lorsque les consommateurs du service extraient des informations sur un service de point de terminaison, ils ne peuvent voir que les zones de disponibilité qu'ils ont en commun avec le

fournisseur du service. Lorsque le fournisseur du service et le consommateur du service se trouvent dans des comptes différents, un nom de zone de disponibilité, tel que `us-east-1a`, peut être mappé à une zone de disponibilité physique différente dans chaque Compte AWS. Vous pouvez utiliser AZ IDs pour identifier de manière cohérente les zones de disponibilité de votre service. Pour plus d'informations, consultez AZ IDs dans le guide de EC2 l'utilisateur Amazon.

- Lorsque les consommateurs du service envoient du trafic vers un service via un point de terminaison d'interface, les adresses IP sources fournies à l'application sont les adresses IP privées des nœuds de l'équilibreur de charge, et non les adresses IP des consommateurs du service. Si vous activez le protocole proxy sur l'équilibreur de charge, vous pouvez obtenir les adresses des consommateurs de services et les points de terminaison IDs de l'interface à partir de l'en-tête du protocole proxy. Pour de plus amples informations, veuillez consulter le protocole proxy dans le Guide de l'utilisateur des Network Load Balancers.
- Un Network Load Balancer peut être associé à un seul service de point de terminaison, mais un service de point de terminaison peut être associé à plusieurs Network Load Balancers.
- Si un service de point de terminaison est associé à plusieurs Network Load Balancers, chaque interface réseau de point de terminaison à un équilibreur de charge. Lorsque la première connexion à partir d'une interface réseau de point de terminaison est lancée, nous sélectionnons au hasard l'un des Network Load Balancers situés dans la même zone de disponibilité que l'interface réseau du point de terminaison. Toutes les demandes de connexion suivantes à partir de cette interface réseau de point de terminaison utilisent l'équilibreur de charge sélectionné. Nous vous recommandons d'utiliser la même configuration d'écouteur et de groupe cible pour tous les équilibreurs de charge d'un service de point de terminaison, afin que les utilisateurs puissent le service quel que soit l'équilibreur de charge choisi.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour de plus amples informations, veuillez consulter AWS PrivateLink quotas.

Prérequis

- Créez un service VPC pour votre terminal avec au moins un sous-réseau dans chaque zone de disponibilité dans laquelle le service doit être disponible.
- Pour permettre aux consommateurs de services de créer des VPC points de terminaison d'IPv6interface pour votre service de point de terminaison, les sous-réseaux VPC et doivent être associés à IPv6 CIDR des blocs.
- Créez un Network Load Balancer dans votre. VPC Sélectionnez un sous-réseau par zone de disponibilité dans lequel le service doit être disponible pour les consommateurs. Pour une faible

latence et tolérance aux pannes, nous vous recommandons de rendre votre service disponible dans toutes les zones de disponibilité de la région.

- Si votre Network Load Balancer possède un groupe de sécurité, il doit autoriser le trafic entrant provenant des adresses IP des clients. Vous pouvez également désactiver l'évaluation des règles des groupes de sécurité entrants pour le trafic entrant. AWS PrivateLink Pour plus d'informations, consultez la section Groupes de sécurité dans le Guide de l'utilisateur pour les équilibreurs de charge réseau.
- Pour permettre à votre service de point de terminaison d'accepter les IPv6 demandes, ses équilibreurs de charge réseau doivent utiliser le type d'adresse IP à double pile. Les cibles n'ont pas besoin de prendre en charge IPv6 le trafic. Pour plus d'informations, consultez la section Type d'adresse IP du Guide de l'utilisateur des équilibreurs de charge de réseau Network Load Balancer.

  Si vous traitez des adresses IP sources à partir de l'en-tête du protocole proxy version 2, vérifiez que vous pouvez traiter IPv6 les adresses.
- Lancez des instances dans chaque zone de disponibilité dans laquelle le service doit être disponible et enregistrez-les dans un groupe cible d'équilibreurs de charge. Si vous ne lancez pas d'instances dans toutes les zones de disponibilité activées, vous pouvez activer l'équilibrage de charge entre zones pour aider les utilisateurs du service qui utilisent des DNS noms d'hôte zonaux pour accéder au service. Des frais de transfert régional de données s'appliquent lorsque vous activez l'équilibrage de charge entre zones. Pour plus d'informations, consultez la section Équilibrage de charge entre zones dans le Guide de l'utilisateur pour les équilibreurs de charge réseau.

Création d'un service de point de terminaison

Utilisez la procédure suivante pour créer un service de point de terminaison à l'aide d'un équilibreur de charge de réseau Network Load Balancer.

Pour créer un service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Choisissez Create endpoint service (Créer un service de point de terminaison).
4. Pour Load balancer type (Type d'équilibreur de charge), choisissez Network (Réseau).
5. Pour Équilibreurs de charge disponibles, sélectionnez les Network Load Balancers à associer au service du point de terminaison. Pour voir les zones de disponibilité activées pour l'équilibreur de

charge que vous avez sélectionné, voir Détails des équilibreurs de charge sélectionnés, Zones de disponibilité incluses. Votre service de point de terminaison sera disponible dans ces zones de disponibilité.

6. (Facultatif) Pour rendre votre service de point de terminaison disponible depuis des régions autres que la région où il est hébergé, sélectionnez les régions dans les régions de service. Pour de plus amples informations, veuillez consulter the section called “Accès interrégional”.
7. Dans la section Require acceptance for endpoint (Acceptation requise pour le point de terminaison), sélectionnez Acceptance required (Acceptation requise) pour exiger que les demandes de connexion à votre service de point de terminaison soient acceptées manuellement. Sinon, ces requêtes sont acceptées automatiquement.
8. Pour Activer le DNS nom privé, sélectionnez Associer un DNS nom privé au service pour associer un DNS nom privé que les clients du service peuvent utiliser pour accéder à votre service, puis entrez le DNS nom privé. Dans le cas contraire, les consommateurs de services peuvent utiliser le DNS nom spécifique au point de terminaison fourni par. AWS Avant que les consommateurs de services puissent utiliser le DNS nom privé, le fournisseur de services doit vérifier qu'ils sont propriétaires du domaine. Pour de plus amples informations, veuillez consulter Gérer les DNS noms.
9. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :

   - Sélectionner IPv4— Activez le service de point de terminaison pour qu'il accepte les IPv4 demandes.
   - Sélectionner IPv6— Activez le service de point de terminaison pour qu'il accepte les IPv6 demandes.
   - Sélectionnez IPv4et IPv6— Activez le service de point de terminaison pour qu'il accepte à la fois les IPv6 demandes IPv4 et.
10. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
11. Sélectionnez Create (Créer).

Pour créer un service de point de terminaison à l'aide de la ligne de commande

- create-vpc-endpoint-service-configuration ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Mettre le service de point de terminaison à la disposition des consommateurs du service

AWS les principaux peuvent se connecter à votre service de point de terminaison en privé en créant un point de VPC terminaison d'interface. Les fournisseurs du service doivent faire ce qui suit pour mettre leurs services à la disposition des consommateurs du service.

- Ajoutez des autorisations qui permettent à chaque utilisateur de se connecter à votre service de point de terminaison. Pour de plus amples informations, veuillez consulter the section called “Gestion des autorisations”.
- Fournissez au consommateur du service le nom de votre service et les zones de disponibilité prises en charge afin qu'il puisse créer un point de terminaison d'interface pour se connecter à votre service. Pour de plus amples informations, veuillez consulter the section called “Connexion à un service de point de terminaison en tant que consommateur du service”.
- Acceptez la demande de connexion au point de terminaison de la part du consommateur du service. Pour de plus amples informations, veuillez consulter the section called “Acceptation ou refus des demandes de connexion”.

Connexion à un service de point de terminaison en tant que consommateur du service

Un consommateur du service utilise la procédure suivante pour créer un point de terminaison d'interface afin de se connecter à votre service de terminaison.

Pour créer un point de terminaison d'interface à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Type, choisissez les services Endpoint qui utilisent NLBs et GWLBs.
5. Dans Nom du service, entrez le nom du service (par exemple,`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), puis choisissez Vérifier le service.
6. (Facultatif) Pour vous connecter à un service de point de terminaison disponible dans une région autre que la région du point de terminaison, sélectionnez Région de service, Activer le point de

terminaison interrégional, puis sélectionnez la région. Pour de plus amples informations, veuillez consulter the section called “Accès interrégional”.

7. Pour VPC, sélectionnez celui VPC à partir duquel vous allez accéder au service de point de terminaison.
8. Pour les sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer les interfaces réseau des points de terminaison.
9. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :

   - IPv4— Attribuez IPv4 des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés ont des plages d'IPv4adresses et si le service de point de terminaison accepte les IPv4 demandes.
   - IPv6— Attribuez IPv6 des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux et que le service de point de terminaison accepte IPv6 les demandes.
   - Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau des terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et si le service de point de terminaison accepte à la fois les IPv6 demandes IPv4 et les demandes.

10. Pour le type d'IP d'DNSenregistrement, choisissez l'une des options suivantes :

    - IPv4— Créez des enregistrements A pour les DNS noms privés, régionaux et zonaux. Le type d'adresse IP doit être IPv4ou Dualstack.
    - IPv6— Créez AAAA des enregistrements pour les DNS noms privés, régionaux et zonaux. Le type d'adresse IP doit être IPv6ou Dualstack.
    - Dualstack — Créez A et AAAA enregistrez les noms privés, régionaux et DNS zonaux. Le type d'adresse IP doit être Dualstack.
    - Service défini — Créez des enregistrements A pour les noms privés, régionaux et zonaux et DNS des AAAA enregistrements pour les noms régionaux et zonauxDNS. Le type d'adresse IP doit être Dualstack.

11. Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
12. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison d'interface à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Configuration d'un service de point de terminaison

Après avoir créé un service de point de terminaison, vous pouvez mettre à jour sa configuration.

Tâches

- Gestion des autorisations
- Acceptation ou refus des demandes de connexion
- Gérez les équilibreurs de charge
- Associer un DNS nom privé
- Modifier les régions prises en charge
- Modification des types d'adresses IP pris en charge
- Gérer les balises

Gestion des autorisations

La combinaison des autorisations et des paramètres d'acceptation vous permet de contrôler les consommateurs de services (AWS principaux) autorisés à accéder à votre service de point de terminaison. Par exemple, vous pouvez accorder des autorisations à des principaux spécifiques en qui vous avez confiance et accepter automatiquement toutes les demandes de connexion, ou vous pouvez accorder des autorisations à un groupe plus large de principaux et accepter manuellement des demandes de connexion spécifiques en qui vous avez confiance.

Par défaut, votre service de point de terminaison n'est pas disponible pour les consommateurs du service. Vous devez ajouter des autorisations qui autorisent des AWS principaux spécifiques à créer un point de VPC terminaison d'interface pour se connecter à votre service de point de terminaison. Pour ajouter des autorisations à un AWS directeur, vous avez besoin de son Amazon Resource Name (ARN). La liste suivante inclut des exemples ARNs de AWS principes pris en charge.

ARNspour les AWS directeurs

Compte AWS (inclut tous les principaux du compte)

arn:aws:iam : ::root *account_id*

Rôle

arn:aws:iam : :role/ *account_id role_name*

Utilisateur

arn:aws:iam : ::user/ *account_id user_name*

Tous les principes en tout Comptes AWS

*

Considérations

- Si vous accordez à tout le monde l'autorisation d'accéder au service de point de terminaison et configurez le service de point de terminaison pour qu'il accepte toutes les requêtes, votre équilibreur de charge sera public même s'il n'a pas d'adresse IP publique.
- Si vous supprimez des autorisations, cela n'affecte pas les connexions existantes entre le point de terminaison et le service qui ont été précédemment acceptées.

Pour gérer des autorisations pour votre service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison et choisissez l'onglet Allow principals (Autoriser les principaux).
4. Pour ajouter des autorisations, choisissez Allow principals (Autoriser les principaux). Dans le champ Principaux à ajouter, entrez le nom ARN du principal. Pour ajouter un autre mandataire, choisissez Add principal (Ajouter un mandataire). Lorsque vous avez terminé d'ajouter des principaux, choisissez Allow principal (Autoriser les principaux).
5. Pour supprimer des autorisations, sélectionnez le principal et choisissez Actions (Actions) puis Delete (Supprimer). Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour ajouter des autorisations pour votre service de point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint-service-autorisations ()AWS CLI
- Edit-EC2EndpointServicePermission(Outils pour Windows PowerShell)

Acceptation ou refus des demandes de connexion

La combinaison des autorisations et des paramètres d'acceptation vous permet de contrôler les consommateurs de services (AWS principaux) autorisés à accéder à votre service de point de terminaison. Par exemple, vous pouvez accorder des autorisations à des principaux spécifiques en qui vous avez confiance et accepter automatiquement toutes les demandes de connexion, ou vous pouvez accorder des autorisations à un groupe plus large de principaux et accepter manuellement des demandes de connexion spécifiques en qui vous avez confiance.

Vous pouvez configurer votre service de point de terminaison pour qu'il accepte automatiquement les demandes de connexion. Sinon, vous devez les accepter ou les refuser manuellement. Si vous n'acceptez pas une demande de connexion, le consommateur du service ne peut pas accéder à votre service de point de terminaison.

Si vous accordez à tout le monde l'autorisation d'accéder au service de point de terminaison et configurez le service de point de terminaison pour qu'il accepte toutes les requêtes, votre équilibreur de charge sera public même s'il n'a pas d'adresse IP publique.

Vous pouvez recevoir une notification lorsqu'une demande de connexion est acceptée ou refusée. Pour de plus amples informations, veuillez consulter the section called “Réception d'alertes pour les événements relatifs au service de point de terminaison”.

Pour modifier le paramètre d'acceptation à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, Modifier le paramètre d'acceptation du point de terminaison.
5. Sélectionnez ou désélectionnez Acceptance required (Acceptation requise).
6. Choisissez Enregistrer les modifications

Pour modifier le paramètre d'acceptation à l'aide de la ligne de commande

- modify-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Pour accepter ou refuser une demande de connexion à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Dans l'onglet Endpoint connections (Connexions de point de terminaison), sélectionnez la connexion de point de terminaison.
5. Pour accepter la demande de connexion, choisissez Actions, Accept endpoint connection request (Accepter la demande de connexion de point de terminaison). À l'invite de confirmation, saisissez **`accept`**, puis choisissez Accept (Accepter).
6. Pour rejeter la demande de connexion, choisissezActions (Actions),Reject endpoint connection request (Rejeter la demande de connexion de point de terminaison). À l'invite de confirmation, saisissez **`reject`**, puis choisissez Reject (Refuser).

Pour accepter ou refuser une demande de connexion à l'aide de la ligne de commande

- accept-vpc-endpoint-connectionsou reject-vpc-endpoint-connections(AWS CLI)
- Approve-EC2EndpointConnectionou Deny-EC2EndpointConnection(Outils pour Windows PowerShell)

Gérez les équilibreurs de charge

Vous pouvez gérer les équilibreurs de charge associés à votre service de point de terminaison. Vous ne pouvez pas dissocier un équilibreur de charge si des points de terminaison sont connectés à votre service de point de terminaison.

Si vous activez une autre zone de disponibilité pour un Network Load Balancer, vous pouvez également activer la zone de disponibilité pour votre service de point de terminaison. Après avoir activé une zone de disponibilité pour le service de point de terminaison, les clients du service peuvent ajouter un sous-réseau de cette zone de disponibilité aux points de VPC terminaison de leur interface.

Pour gérer les équilibreurs de charge de votre service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, Associate or disassociate load balancers (Associer des équilibreurs de charge).
5. Modifiez la configuration du service de point de terminaison selon vos besoins. Par exemple :
   - Cochez la case correspondant à un équilibreur de charge pour l'associer au service de point de terminaison.
   - Décochez la case correspondant à un équilibreur de charge afin de le dissocier du service de point de terminaison. Vous devez conserver au moins un équilibreur de charge sélectionné.
   - Si vous avez récemment activé une autre zone de disponibilité pour votre équilibreur de charge, celle-ci apparaît sous Zones de disponibilité incluses. Si vous enregistrez les modifications à l'étape suivante, cela active le service de point de terminaison pour la nouvelle zone de disponibilité.
6. Choisissez Enregistrer les modifications

Pour gérer les équilibreurs de charge de votre service de point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Pour activer le service de point de terminaison dans une zone de disponibilité récemment activée pour l'équilibreur de charge, il suffit d'appeler la commande avec l'ID du service de point de terminaison.

Associer un DNS nom privé

Vous pouvez associer un DNS nom privé à votre service de point de terminaison. Après avoir associé un DNS nom privé, vous devez mettre à jour l'entrée du domaine sur votre DNS serveur. Avant que les consommateurs de services puissent utiliser le DNS nom privé, le fournisseur de services doit

vérifier qu'ils sont propriétaires du domaine. Pour de plus amples informations, veuillez consulter Gérer les DNS noms.

Pour modifier le DNS nom privé d'un service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, Modifier le DNS nom privé.
5. Sélectionnez Associer un DNS nom privé au service et DNS saisissez-le.
   - Les noms de domaine doivent être en minuscules.
   - Vous pouvez utiliser des caractères de remplacement dans les noms de domaine (par exemple, **`*.myexampleservice.com`**).
6. Sélectionnez Enregistrer les modifications.
7. Le DNS nom privé est prêt à être utilisé par les consommateurs de services lorsque le statut de vérification est vérifié. Si l'état de vérification change, les nouvelles demandes de connexion sont refusées, mais les connexions existantes ne sont pas affectées.

Pour modifier le DNS nom privé d'un service de point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Pour lancer le processus de vérification du domaine à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, Vérifier la propriété du domaine pour le DNS nom privé.
5. Lorsque vous êtes invité à confirmer, saisissez **`verify`**, puis choisissez Delete (Supprimer).

Pour lancer le processus de vérification du domaine à l'aide de la ligne de commande

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification(Outils pour Windows PowerShell)

Modifier les régions prises en charge

Vous pouvez modifier l'ensemble des régions prises en charge pour votre service de point de terminaison. Avant de pouvoir ajouter une région opt-in, vous devez vous y inscrire. Vous ne pouvez pas supprimer la région qui héberge votre service de point de terminaison.

Une fois que vous avez supprimé une région, les consommateurs de services ne peuvent pas créer de nouveaux points de terminaison la spécifiant comme région de service. La suppression d'une région n'affecte pas les points de terminaison existants qui la spécifient comme région de service. Lorsque vous supprimez une région, nous vous recommandons de rejeter toutes les connexions de point de terminaison existantes depuis cette région.

Pour modifier les régions prises en charge pour votre service de point de terminaison

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, puis Modifier les régions prises en charge.
5. Sélectionnez et désélectionnez Régions selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

Modification des types d'adresses IP pris en charge

Vous pouvez modifier les types d'adresses IP pris en charge par votre service de point de terminaison.

Considération

Pour permettre à votre service de point de terminaison d'accepter les IPv6 demandes, ses équilibreurs de charge réseau doivent utiliser le type d'adresse IP à double pile. Les cibles n'ont pas besoin de prendre en charge IPv6 le trafic. Pour plus d'informations, consultez la section Type d'adresse IP du Guide de l'utilisateur des équilibreurs de charge de réseau Network Load Balancer.

Pour modifier les types d'adresses IP pris en charge à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de VPC point de terminaison.
4. Choisissez Actions, Modify supported IP address types (Modifier les types d'adresses IP pris en charge).
5. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
   - Sélectionner IPv4— Activez le service de point de terminaison pour qu'il accepte les IPv4 demandes.
   - Sélectionner IPv6— Activez le service de point de terminaison pour qu'il accepte les IPv6 demandes.
   - Sélectionnez IPv4et IPv6— Activez le service de point de terminaison pour qu'il accepte à la fois les IPv6 demandes IPv4 et.
6. Sélectionnez Enregistrer les modifications.

Pour modifier les types d'adresse IP pris en charge à l'aide de la ligne de commande

- modify-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Outils pour Windows PowerShell)

Gérer les balises

Vous pouvez baliser vos ressources pour vous aider à les identifier ou à les catégoriser en fonction des besoins de votre organisation.

Pour gérer des balises pour votre service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de VPC point de terminaison.
4. Choisissez Actions, Manage tags (Gérer les balises).

5. Pour chaque balise à ajouter, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Save (Enregistrer).

Pour gérer les balises pour les connexions de votre point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de VPC point de terminaison, puis choisissez l'onglet Connexions de point de terminaison.
4. Sélectionnez la connexion au point de terminaison, puis choisissez Actions (Actions), Manage tags (Gérer les balises).
5. Pour chaque balise à ajouter, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Save (Enregistrer).

Pour gérer des balises pour les autorisations de votre service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de VPC point de terminaison, puis choisissez l'onglet Autoriser les principaux.
4. Sélectionnez le principal puis choisissez Actions (Actions), Gérer les balises.
5. Pour chaque balise à ajouter, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Save (Enregistrer).

Pour ajouter et supprimer des balises à l'aide de la ligne de commande

- create-tags et delete-tags (AWS CLI)
- New-EC2Taget Remove-EC2Tag(Outils pour Windows PowerShell)

Gérer les DNS noms des services de VPC point de terminaison

Les fournisseurs de services peuvent configurer DNS des noms privés pour leurs services de point de terminaison. Supposons qu'un fournisseur de services mette son service à disposition via un point de terminaison public et en tant que service de point de terminaison. Si le fournisseur de services utilise le DNS nom du point de terminaison public comme DNS nom privé du service de point de terminaison, les consommateurs du service peuvent accéder au point de terminaison public ou au service de point de terminaison en utilisant la même application client, sans modification. Si une demande provient du consommateur de servicesVPC, les DNS serveurs privés résolvent le DNS nom en adresses IP des interfaces réseau des terminaux. Dans le cas contraire, les DNS serveurs publics attribuent le DNS nom au point de terminaison public.

Avant de configurer un DNS nom privé pour votre service de point de terminaison, vous devez prouver que vous êtes le propriétaire du domaine en effectuant une vérification de propriété du domaine.

Considérations

- Un service de point de terminaison ne peut avoir qu'un seul DNS nom privé.
- Lorsque le consommateur crée un point de terminaison d'interface pour se connecter à votre service, nous créons une zone hébergée privée et l'associons au client du serviceVPC. Nous créons un CNAME enregistrement dans la zone hébergée privée qui associe le DNS nom privé du service de point de terminaison au DNS nom régional du point de VPC terminaison. Lorsqu'un consommateur envoie une demande au DNS nom public du service, les DNS serveurs privés résolvent la demande aux adresses IP des interfaces réseau des terminaux.
- Pour vérifier un domaine, vous devez disposer d'un nom d'hôte public ou d'un DNS fournisseur public.
- Vous pouvez vérifier le domaine d'un sous-domaine. Par exemple, vous pouvez vérifier example.com, au lieu de a.example.com. Chaque DNS étiquette peut comporter jusqu'à 63 caractères et la longueur totale du nom de domaine ne doit pas dépasser 255 caractères.

Si vous ajoutez un sous-domaine supplémentaire, vous devez vérifier le sous-domaine ou le domaine. Imaginons par exemple que vous aviez un a.example.com et vérifié un example.com. Vous ajoutez désormais b.example.com en tant que nom privéDNS. Vous devez vérifier example.com ou b.example.com pour que les consommateurs du service puissent utiliser le nom.

- Les DNS noms privés ne sont pas pris en charge pour les points de terminaison Gateway Load Balancer.

Vérification de la propriété du domaine

Votre domaine est associé à un ensemble d'enregistrements de service de noms de domaine (DNS) que vous gérez par l'intermédiaire de votre DNS fournisseur. Un TXT enregistrement est un type d'DNSenregistrement qui fournit des informations supplémentaires sur votre domaine. Il se compose d'un nom et d'une valeur. Dans le cadre du processus de vérification, vous devez ajouter un TXT enregistrement sur le DNS serveur pour votre domaine public.

La vérification de la propriété du domaine est terminée lorsque nous détectons l'existence de l'TXTenregistrement dans DNS les paramètres de votre domaine.

Après avoir ajouté un enregistrement, vous pouvez vérifier l'état du processus de vérification du domaine à l'aide de la VPC console Amazon. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison). Sélectionnez le service de point de terminaison et vérifiez la valeur de l'état de vérification du domaine dans l'onglet Details (Détails). Si la vérification du domaine est en cours, attendez quelques minutes et rafraîchissez l'écran. Si nécessaire, vous pouvez lancer le processus de vérification manuellement. Choisissez Actions, Vérifier la propriété du domaine pour le DNS nom privé.

Le DNS nom privé est prêt à être utilisé par les consommateurs de services lorsque le statut de vérification est vérifié. Si l'état de vérification change, les nouvelles demandes de connexion sont refusées, mais les connexions existantes ne sont pas affectées.

Si l'état de vérification est failed (échoué), voir the section called “Résolution des problèmes de vérification de domaine”.

Obtention du nom et de la valeur

Nous vous fournissons le nom et la valeur que vous utilisez dans le TXT dossier. Par exemple, les informations sont disponibles dans la AWS Management Console. Sélectionnez le service de point

de terminaison et consultez Domain verification name (Nom de vérification du domaine) et Domain verification value (Valeur de vérification du domaine) dans l'onglet Details (Détails) pour le service de point de terminaison. Vous pouvez également utiliser la AWS CLI commande describe-vpc-endpoint-service-configurations suivante pour récupérer des informations sur la configuration du DNS nom privé pour le service de point de terminaison spécifié.

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

Voici un exemple de sortie. Vous utiliserez `Value` et `Name` lorsque vous créerez l'TXTenregistrement.

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

Par exemple, supposons que votre nom de domaine est example.com et que `Value` et `Name` sont comme indiqué dans l'exemple de sortie précédent. Le tableau suivant est un exemple des paramètres d'TXTenregistrement.

Nom	Type	Valeur
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce : l6p0 ERxlTt45jevFwOCp

Nous vous suggérons d'utiliser `Name` comme sous-domaine d'enregistrement, car il se peut que le nom de domaine de base soit déjà utilisé. Toutefois, si votre DNS fournisseur n'autorise pas les noms d'DNSenregistrement à contenir des traits de soulignement, vous pouvez omettre le « _6e86v84tqgqubxbwii1m » et simplement utiliser « exemple.com » dans l'enregistrement. TXT

Après avoir vérifié « _6e86v84tqgqubxbwii1m.example.com », les consommateurs du service peuvent utiliser « example.com » ou un sous-domaine (par exemple, « service.example.com » ou « my.service.example.com »).

Ajoutez un TXT enregistrement au DNS serveur de votre domaine

La procédure d'ajout d'TXTenregistrements au DNS serveur de votre domaine dépend de la personne qui fournit votre DNS service. Votre DNS fournisseur peut être Amazon Route 53 ou un autre bureau d'enregistrement de noms de domaine.

Amazon Route 53

Créez un enregistrement pour votre zone hébergée publique. Utilisez les valeurs suivantes :

- Dans Type d'enregistrement, sélectionnez TXT.
- Pendant TTL(secondes), entrez**1800**.
- Pour Routing policy (Stratégie de routage), sélectionnez Simple routing (Routage simple).
- Pour Record name (Nom d'enregistrement), saisissez le domaine ou le sous-domaine.
- Pour Value/Route traffic to (Valeur/Acheminer le trafic vers), saisissez la valeur de vérification de domaine.

Pour plus d'informations, voir Création d'enregistrements à l'aide de la console du Guide du développeur Amazon Route 53.

Procédure générale

Accédez au site Web de votre DNS fournisseur et connectez-vous à votre compte. Trouvez la page permettant de mettre à jour les DNS enregistrements de votre domaine. Ajoutez un TXT enregistrement avec le nom et la valeur que nous avons fournis. Les mises à jour des DNS enregistrements peuvent prendre jusqu'à 48 heures pour prendre effet, mais elles prennent souvent effet beaucoup plus tôt.

Pour des instructions plus spécifiques, consultez la documentation de votre DNS fournisseur. Le tableau suivant fournit des liens vers la documentation de plusieurs DNS fournisseurs courants. Cette liste ne prétend pas être exhaustive et ne constitue pas une recommandation des produits ou services fournis par ces entreprises.

DNS/Fournisseur d'héberge ment	Lien vers la documentation
GoDaddy	Ajouter un TXT enregistrement

DNS/Fournisseur d'héberge ment	Lien vers la documentation
Dreamhost	Ajouter des DNS enregistrements personnalisés
Cloudflare	Gérez les DNS enregistrements
HostGator	Gérez DNS les enregistrements avec HostGator/eNom
Namecheap	Comment ajouter TXT/SPF/DKIM/DMARC des enregistrements pour mon domaine ?
Names.co.uk	Modifier les DNS paramètres de votre domaine
Wix	Ajouter ou mettre à jour TXT des enregistrements dans votre compte Wix

Vérifiez si l'TXTenregistrement est publié

Vous pouvez vérifier que l'TXTenregistrement de vérification de la propriété de votre domaine de DNS nom privé est correctement publié sur votre DNS serveur en suivant les étapes suivantes. Vous allez exécuter la nslookup commande, qui est disponible pour Windows et Linux.

Vous allez interroger les DNS serveurs qui desservent votre domaine, car ce sont eux qui contiennent le plus up-to-date d'informations sur votre domaine. Les informations de votre domaine mettent du temps à se propager vers d'autres DNS serveurs.

Pour vérifier que votre TXT enregistrement est publié sur votre DNS serveur

1. Trouvez les serveurs de noms pour votre domaine en utilisant la commande suivante.

   ```
   nslookup -type=NS example.com
   ```

   Le résultat liste les serveurs de noms qui desservent votre domaine. Vous interrogerez l'un de ces serveurs à l'étape suivante.
2. Vérifiez que l'TXTenregistrement est correctement publié à l'aide de la commande suivante, où se *name_server* trouve l'un des serveurs de noms que vous avez trouvés à l'étape précédente.

```
nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
```

3. Dans le résultat de l'étape précédente, vérifiez que la chaîne qui suit `text =` correspond à la TXT valeur.

   Dans notre exemple, si l'enregistrement est correctement publié, le résultat inclut les éléments suivants.

```
_6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
```

Résolution des problèmes de vérification de domaine

Si le processus de vérification de domaine échoue, les informations suivantes peuvent vous aider à résoudre les problèmes.

- Vérifiez si votre DNS fournisseur autorise les traits de soulignement dans les noms des TXT enregistrements. Si votre DNS fournisseur n'autorise pas les traits de soulignement, vous pouvez omettre le nom de vérification du domaine (par exemple, « _6e86v84tqgqubxbwii1m ») de l'enregistrement. TXT
- Vérifiez si votre DNS fournisseur a ajouté le nom de domaine à la fin de l'TXTenregistrement. Certains DNS fournisseurs ajoutent automatiquement le nom de votre domaine au nom d'attribut de l'TXTenregistrement. Pour éviter cette duplication du nom de domaine, ajoutez un point à la fin du nom de domaine lorsque vous créez l'TXTenregistrement. Cela indique à votre DNS fournisseur qu'il n'est pas nécessaire d'ajouter le nom de domaine à l'TXTenregistrement.
- Vérifiez si votre DNS fournisseur a modifié la valeur d'DNSenregistrement pour n'utiliser que des lettres minuscules. Nous vérifions votre domaine uniquement lorsqu'il existe un enregistrement de vérification dont la valeur d'attribut correspond exactement à la valeur que nous avons fournie. Si le DNS fournisseur a modifié vos valeurs d'TXTenregistrement pour n'utiliser que des lettres minuscules, contactez-le pour obtenir de l'aide.
- Vous devrez peut-être vérifier votre domaine plus d'une fois parce que vous prenez en charge plusieurs Régions ou plusieurs Comptes AWS. Si votre DNS fournisseur ne vous autorise pas à avoir plusieurs TXT enregistrements portant le même nom d'attribut, vérifiez s'il vous DNS autorise à attribuer plusieurs valeurs d'attribut au même TXT enregistrement. Par exemple, si votre DNS compte est géré par Amazon Route 53, vous pouvez utiliser la procédure suivante.

1. Dans la console Route 53, choisissez l'TXTenregistrement que vous avez créé lorsque vous avez vérifié votre domaine dans la première région.
2. Pour Value (Valeur), allez jusqu'à la fin de la valeur de l'attribut existant, puis appuyez sur Entrée.
3. Ajoutez la valeur d'attribut de la région supplémentaire, puis enregistrez le jeu d'enregistrements.

Si votre DNS fournisseur ne vous autorise pas à attribuer plusieurs valeurs au même TXT enregistrement, vous pouvez vérifier le domaine une fois avec la valeur dans le nom d'attribut de l'TXTenregistrement, et une autre fois avec la valeur supprimée du nom d'attribut. Toutefois, vous ne pouvez vérifier le même domaine que deux fois.

Réception d'alertes pour les événements relatifs au service de point de terminaison

Vous pouvez créer une notification pour recevoir des alertes sur des événements spécifiques liés à votre service de point de terminaison. Par exemple, vous pouvez recevoir un e-mail quand une demande de connexion est acceptée ou refusée.

Tâches

- Création d'une SNS notification
- Ajout d'une stratégie d'accès
- Ajout d'une stratégie de clé

Création d'une SNS notification

Utilisez la procédure suivante pour créer une SNS rubrique Amazon pour les notifications et vous abonner à la rubrique.

Pour créer une notification pour un service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Dans l'onglet Notifications, choisissez Create notification (Créer une notification).

5. Pour Notification ARN, choisissez ARN le SNS sujet que vous avez créé.
6. Pour vous abonner à un événement, sélectionnez-le dans Events (Événements).
   - Connect (Connexion) – Le consommateur du service a créé le point de terminaison d'interface. Cela envoie une demande de connexion au fournisseur du service.
   - Accept (Acceptation) – Le fournisseur du service a accepté la demande de connexion.
   - Reject (Refus) – Le fournisseur du service a refusé la demande de connexion.
   - Delete (Suppression) – Le consommateur du service a supprimé le point de terminaison d'interface.
7. Choisissez Create notification (Créer une notification).

Pour créer une notification pour un service de point de terminaison à l'aide de la ligne de commande

- create-vpc-endpoint-connection-notification ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Outils pour Windows PowerShell)

Ajout d'une stratégie d'accès

Ajoutez une politique d'accès à la SNS rubrique qui permet AWS PrivateLink de publier des notifications en votre nom, telle que la suivante. Pour plus d'informations, consultez Comment modifier la politique d'accès de mon SNS sujet Amazon ? Utilisez les clés de condition globale `aws:SourceArn` et `aws:SourceAccount` pour vous protéger contre le problème du député confus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint-service/service-id"
        },
```

```
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Ajout d'une stratégie de clé

Si vous utilisez des SNS sujets chiffrés, la politique de ressources associée à la KMS clé doit faire confiance AWS PrivateLink aux AWS KMS API opérations d'appel. Voici un exemple de stratégie de clé.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint-service/service-
id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Suppression d'un service de point de terminaison

Lorsque vous avez terminé avec un service de point de terminaison, vous pouvez le supprimer. Vous ne pouvez pas supprimer un service de point de terminaison s'il y a des points de terminaison connectés au service de point de terminaison qui sont dans l'état `available` ou `pending-acceptance`.

La suppression d'un service de point de terminaison ne supprime pas l'équilibreur de charge associé et n'affecte pas les serveurs d'applications enregistrés dans les groupes cibles de l'équilibreur de charge.

Pour supprimer un service de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions (Actions), Delete endpoint services (Supprimer les services de point de terminaison).
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer un service de point de terminaison à l'aide de la ligne de commande

- delete-vpc-endpoint-service-configurations ()AWS CLI
- Remove-EC2EndpointServiceConfiguration(Outils pour Windows PowerShell)

Accédez aux VPC ressources via AWS PrivateLink

Vous pouvez accéder en privé à une VPC ressource d'une autre à VPC l'aide d'un point de VPC terminaison de ressource (point de terminaison de ressource). Un point de terminaison de ressources vous permet d'accéder de manière privée et sécurisée à des VPC ressources telles qu'une base de données, un cluster de nœuds, une instance, un point de terminaison d'application, une cible de nom de domaine ou une adresse IP qui peut se trouver dans un sous-réseau privé dans un autre environnement VPC ou dans un environnement sur site. Sans points de terminaison de ressources, vous devez soit ajouter une passerelle Internet à votre ressource, VPC soit accéder à la ressource à l'aide d'un point de terminaison d' AWS PrivateLink interface et d'un Network Load Balancer. Les points de terminaison des ressources ne nécessitent pas d'équilibreur de charge, vous pouvez donc accéder directement à la VPC ressource. Une VPC ressource est représentée par une configuration de ressources. Une configuration de ressources est liée à une passerelle de ressources.

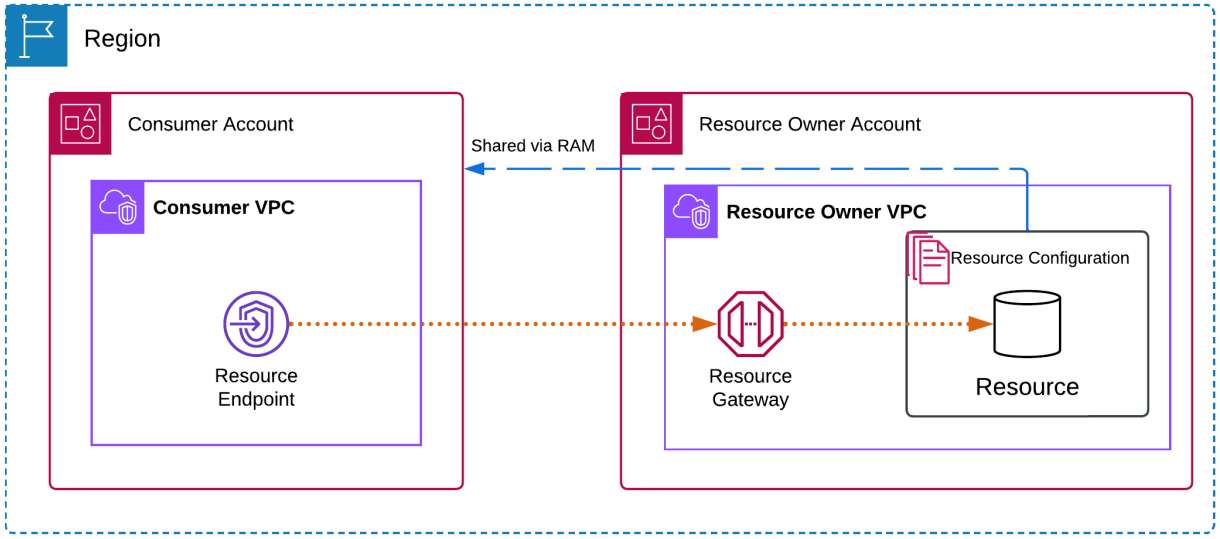
Tarification

Lorsque vous accédez à des ressources à l'aide de points de terminaison de ressources, vous êtes facturée pour chaque heure pendant laquelle votre point de VPC terminaison de ressources est provisionné. Vous êtes également facturé par Go de données traitées lorsque vous accédez aux ressources. Pour en savoir plus, consultez Pricing AWS PrivateLink (Tarification). Lorsque vous autorisez l'accès à vos ressources à l'aide de configurations de ressources et de passerelles de ressources, vous êtes facturé par Go de données traitées par vos passerelles de ressources. Pour en savoir plus, consultez Pricing Amazon VPC Lattice (Tarification).

Table des matières

Présentation

Vous pouvez accéder aux ressources de votre compte ou à celles qui ont été partagées avec vous depuis un autre compte. Pour accéder à une ressource, vous créez un point de VPC terminaison de ressource, qui établit des connexions entre les sous-réseaux de votre ressource VPC et ceux de la ressource à l'aide d'interfaces réseau. Le trafic destiné à la ressource est résolu vers les adresses IP privées des interfaces réseau du point de terminaison de la ressource à l'aide de la connexion entre le VPC point de terminaison et la ressource via la passerelle de ressources. DNS



Considérations

- TCPle trafic est pris en charge. UDPle trafic n'est pas pris en charge.
- Les connexions réseau doivent être initiées à partir du point de terminaison VPC qui contient la ressource, et non à partir de VPC celui qui possède la ressource. La ressource ne VPC peut pas établir de connexions réseau avec le point de terminaisonVPC.
- Les seules ressources prises ARN en charge sont les RDS ressources Amazon.

DNSnoms d'hôtes

Avec AWS PrivateLink, vous envoyez du trafic vers des ressources à l'aide de points de terminaison privés. Lorsque vous créez un point de VPC terminaison de ressource, nous créons DNS des noms régionaux (appelés DNS nom par défaut) que vous pouvez utiliser pour communiquer avec la

ressource depuis votre site VPC et depuis votre site. Le DNS nom par défaut de votre point de VPC terminaison de ressource possède la syntaxe suivante :

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Lorsque vous créez un point de VPC terminaison de ressource pour certaines configurations de ressources que vous utilisezARNs, vous pouvez activer le mode privé DNS. Avec le mode privéDNS, vous pouvez continuer à envoyer des demandes à la ressource en utilisant le DNS nom fourni pour la ressource par le AWS service, tout en tirant parti de la connectivité privée via le point de VPC terminaison de la ressource. Pour de plus amples informations, veuillez consulter the section called "DNSrésolution".

La describe-vpc-endpoint-associationscommande suivante affiche les DNS entrées d'un point de terminaison de ressource.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].DnsEntry'
```

Voici un exemple de sortie pour un point de terminaison de ressource pour une RDS base de données Amazon avec DNS des noms privés activés. La première entrée est le DNS nom par défaut. La deuxième entrée provient de la zone hébergée privée cachée, qui résout les demandes adressées au point de terminaison public vers les adresses IP privées des interfaces réseau du point de terminaison.

```
"DnsEntry": {
                "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
                "HostedZoneId": "ABCDEFGH123456789000"
            },
"PrivateDnsEntry": {
                "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
                "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
            }
```

DNSrésolution

Les DNS enregistrements que nous créons pour le point de VPC terminaison de votre ressource sont publics. Par conséquent, ces DNS noms peuvent être résolus publiquement. Cependant, les DNS demandes provenant de l'extérieur renvoient VPC toujours les adresses IP privées des interfaces réseau du point de terminaison de la ressource. Vous pouvez utiliser ces DNS noms pour accéder à la ressource sur site, à condition d'avoir accès au point de terminaison dans lequel se trouve le VPC point de terminaison de la ressource, via VPN ou à Direct Connect.

Privé DNS

Si vous activez le mode privé DNS pour le point de VPC terminaison de votre VPC ressource et que les DNSnoms d'hôte et la DNS résolution sont activés, nous créons des zones hébergées privées masquées et AWS gérées pour les configurations de ressources avec un nom personnaliséDNS. La zone hébergée contient un ensemble d'enregistrements pour le DNS nom par défaut de la ressource qui la résout en adresses IP privées des interfaces réseau du point de terminaison de la ressource dans votreVPC.

Amazon met à votre VPC disposition un DNS serveur appelé Route 53 Resolver. Le résolveur Route 53 résout automatiquement les noms de VPC domaine locaux et les enregistre dans des zones hébergées privées. Cependant, vous ne pouvez pas utiliser le résolveur Route 53 depuis l'extérieur de votreVPC. Si vous souhaitez accéder à votre VPC point de terminaison depuis votre réseau local, vous pouvez utiliser les DNS noms par défaut ou utiliser les points de terminaison Route 53 Resolver et les règles du résolveur. Pour plus d'informations, consultez la section Intégration AWS Transit Gateway avec AWS PrivateLink et Amazon Route 53 Resolver.

Sous-réseaux et zones de disponibilité

Vous pouvez configurer votre VPC point de terminaison avec un sous-réseau par zone de disponibilité. Nous créons une interface réseau pour le point de VPC terminaison de votre sous-réseau. Nous attribuons des adresses IP à chaque interface réseau de point de terminaison à partir de son sous-réseau, en fonction du type d'adresse IP du point de VPC terminaison. Le nombre d'adresses IP attribuées dans chaque sous-réseau dépend du nombre de configurations de ressources. Dans un environnement de production, pour une disponibilité et une résilience élevées, nous recommandons de configurer au moins deux zones de disponibilité pour chaque VPC point de terminaison.

Types d'adresses IP

Les points de terminaison des ressources peuvent prendre en charge IPv4 des IPv6 adresses ou des adresses à double pile. Les points de terminaison compatibles IPv6 peuvent répondre aux DNS requêtes avec des AAAA enregistrements. Le type d'adresse IP d'un point de terminaison de ressource doit être compatible avec les sous-réseaux du point de terminaison de ressource, comme décrit ici :

- IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
- IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
- Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

Si un point de VPC terminaison de ressource est compatibleIPv4, les interfaces réseau du point de terminaison ont IPv4 des adresses. Si un point de VPC terminaison de ressource est compatibleIPv6, les interfaces réseau du point de terminaison ont IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison n'est pas accessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Accès à une ressource via un point de VPC terminaison de ressource

Vous pouvez accéder à une VPC ressource telle qu'un nom de domaine, une adresse IP ou une RDS base de données Amazon à l'aide d'un point de terminaison de ressource. Un point de terminaison de ressource fournit un accès privé à une ressource. Lorsque vous créez le point de terminaison de ressource, vous spécifiez une configuration de ressource de type unique, de groupe ouARN. Un point de terminaison de ressource ne peut être associé qu'à une seule configuration de ressource. La configuration des ressources peut représenter une ressource unique ou un groupe de ressources.

Prérequis

Pour créer un point de terminaison de ressource, vous devez remplir les conditions préalables suivantes.

- Vous devez disposer d'une configuration de ressources créée par vous ou partagée avec vous depuis un autre compte AWS RAM.
- Si une configuration de ressources est partagée avec vous depuis un autre compte, vous devez vérifier et accepter le partage de ressources qui contient la configuration des ressources. Pour plus d'informations, consultez Acceptation et refus des invitations dans le Guide de l'utilisateur AWS RAM .

Création d'un point de terminaison de VPC ressource

Utilisez la procédure suivante pour créer un point de terminaison de VPC ressource.

Pour créer un point de terminaison VPC de ressource

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Vous pouvez spécifier un nom pour faciliter la recherche et la gestion du point de terminaison.
5. Dans Type, sélectionnez Ressources.
6. Pour les configurations des ressources, sélectionnez la configuration des ressources qui a été partagée avec vous.
7. Pour les paramètres réseau, sélectionnez celui VPC à partir duquel vous allez accéder à la ressource.
8. Si vous souhaitez configurer le DNS support privé, sélectionnez Paramètres supplémentaires, puis Activer DNS le nom. Pour utiliser cette fonctionnalité, assurez-vous que les attributs Enable DNS hostnames et Enable DNS support sont activés pour votreVPC.
9. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison de ressource à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)

- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Gérer les points de terminaison des ressources

Après avoir créé un point de terminaison de ressource, vous pouvez mettre à jour sa configuration.

Tâches

- Supprimer un point de terminaison
- Mettre à jour un point de terminaison

Supprimer un point de terminaison

Lorsque vous avez terminé d'utiliser un VPC point de terminaison, vous pouvez le supprimer.

Pour supprimer un point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer un point de terminaison à l'aide de la ligne de commande

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Outils pour Windows PowerShell)

Mettre à jour un point de terminaison

Vous pouvez mettre à jour un VPC point de terminaison.

Pour mettre à jour un point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, puis l'option appropriée.
5. Suivez les étapes de la console pour envoyer la mise à jour.

Pour mettre à jour un point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Configuration des ressources pour les VPC ressources

Une configuration de ressources représente une ressource ou un groupe de ressources que vous souhaitez rendre accessible aux clients dans VPCs d'autres comptes. En définissant une configuration de ressources, vous pouvez autoriser une connectivité réseau privée, sécurisée et unidirectionnelle aux ressources VPC de votre compte depuis les clients VPCs des autres comptes. Une configuration de ressources est liée à une passerelle de ressources par laquelle elle reçoit le trafic.

Table des matières

Types de configurations de ressources

Une configuration de ressources peut être de plusieurs types. Les différents types permettent de représenter différents types de ressources. Les types sont les suivants :

- Configuration de ressource unique : adresse IP ou nom de domaine. Il peut être partagé indépendamment.
- Configuration des ressources de groupe : collection de configurations de ressources enfants représentant un cluster de nœuds. Il peut être partagé indépendamment.
- Configuration de ressources enfant : membre d'une configuration de ressources de groupe. Il représente une adresse IP ou un nom de domaine. Il ne peut pas être partagé indépendamment ; il ne peut être partagé que dans le cadre d'un groupe. Il peut être ajouté et retiré d'un groupe en toute simplicité. Une fois ajouté, il est automatiquement accessible à ceux qui peuvent accéder au groupe.
- ARNconfiguration des ressources : représente un type de ressource pris en charge fourni par un service. AWS Les configurations des ressources pour enfants sont automatiquement gérées par AWS.

Passerelle de ressources

Une configuration de ressources est liée à une passerelle de ressources. Une passerelle de ressources est un ensemble ENIs qui sert de point d'entrée dans le lieu VPC dans lequel se trouve la ressource. Plusieurs configurations de ressources peuvent être liées à la même passerelle de ressources. Lorsque des clients VPCs d'autres comptes accèdent à une ressource de votre compteVPC, la ressource y voit le trafic provenant localement de la passerelle de ressourcesVPC.

Définition de la ressource

Dans la configuration de la ressource, identifiez la ressource de l'une des manières suivantes :

- Par un nom de ressource Amazon (ARN) : les types de ressources pris en charge fournis par les AWS services peuvent être identifiés par leur. ARN Par exemple, une RDS base de données Amazon.
- Par une cible de nom de domaine : tout nom de domaine pouvant être résolu publiquement.
- Par une adresse IP : Pour IPv4 etIPv6, uniquement IPs dans le VPC sont pris en charge.

Protocole

Lorsque vous créez une configuration de ressource, vous pouvez définir les protocoles que la ressource prendra en charge. Actuellement, seul le TCP protocole est pris en charge.

Gammes de ports

Lorsque vous créez une configuration de ressources, vous pouvez définir les ports sur lesquels elle acceptera les demandes. L'accès des clients sur les autres ports ne sera pas autorisé.

Accès aux ressources

Les consommateurs peuvent accéder aux configurations des ressources directement à VPC partir d'un VPC point de terminaison ou via un réseau de services. En tant que consommateur, vous pouvez autoriser l'accès depuis votre compte VPC à une configuration de ressources qui se trouve dans votre compte ou qui a été partagée avec vous depuis un autre compte via AWS RAM.

- Accès direct à une configuration de ressources

  Vous pouvez créer un AWS PrivateLink VPC point de terminaison de type ressource (point de terminaison de ressource) dans votre VPC pour accéder à une configuration de ressource en privé depuis votreVPC. Pour plus d'informations sur la création d'un point de terminaison de ressource, consultez la section Accès aux VPC ressources dans le guide de AWS PrivateLink l'utilisateur.
- Accès à une configuration de ressources via un réseau de service

  Vous pouvez associer une configuration de ressources à un réseau de service et vous connecter VPC au réseau de service. Vous pouvez vous connecter VPC au réseau de service via une association ou à l'aide d'un point de terminaison du AWS PrivateLink réseau de servicesVPC.

  Pour plus d'informations sur les associations de réseaux de service, voir Gérer les associations pour un réseau de services VPC Lattice.

  Pour plus d'informations sur les VPC points de terminaison des réseaux de service, consultez la section Accès aux réseaux de services dans le guide de AWS PrivateLink l'utilisateur.

Association avec le type de réseau de service

Lorsque vous partagez une configuration de ressources avec un compte client, par exemple, Account-B AWS RAM, via Account-B peut accéder à la configuration des ressources soit directement via un point de VPC terminaison de ressource, soit via un réseau de services.

Pour accéder à une configuration de ressources via un réseau de service, le compte B doit associer la configuration de ressources à un réseau de service. Les réseaux de services peuvent être partagés entre les comptes. Ainsi, le compte B peut partager son réseau de service (auquel la configuration des ressources est associée) avec le compte C, ce qui rend votre ressource accessible depuis le compte C.

Afin d'empêcher un tel partage transitif, vous pouvez spécifier que votre configuration de ressources ne peut pas être ajoutée aux réseaux de services partageables entre comptes. Si vous le spécifiez, le compte B ne pourra pas ajouter votre configuration de ressources aux réseaux de service partagés ou susceptibles d'être partagés avec un autre compte à l'avenir.

Types de réseaux de services

Lorsque vous partagez une configuration de ressource avec un autre compte, par exemple Account-B AWS RAM, via Account-B peut accéder à la ressource de l'une des trois manières suivantes :

- Utilisation d'un VPC point de terminaison de type ressource (point de VPC terminaison de ressource).
- Utilisation d'un VPC point de terminaison de type réseau de services (point de VPC terminaison de réseau de services).
- Utilisation d'une VPC association de réseau de services.

Pour l'VPCassociation du point de VPC terminaison du réseau de service et du réseau de service, la configuration des ressources devrait être placée dans un réseau de service dans le compte B. Les réseaux de services peuvent être partagés entre les comptes. Ainsi, le compte B peut partager son réseau de service (qui contient la configuration des ressources) avec le compte C, ce qui rend votre ressource accessible depuis le compte C. Afin d'empêcher un tel partage transitif, vous pouvez interdire l'ajout de votre configuration de ressources aux réseaux de services partageables entre comptes. Si vous l'interdisez, le compte B ne pourra pas ajouter votre configuration de ressources à un réseau de service partagé ou pouvant être partagé avec un autre compte.

Partage de configurations de ressources via AWS RAM

Les configurations de ressources sont intégrées à AWS Resource Access Manager. Vous pouvez partager la configuration de vos ressources avec un autre compte via AWS RAM. Lorsque vous partagez une configuration de ressource avec un AWS compte, les clients de ce compte peuvent accéder à la ressource en privé. Vous pouvez partager une configuration de ressources à l'aide d'un partage de ressources AWS RAM.

Utilisez la AWS RAM console pour afficher les partages de ressources auxquels vous avez été ajouté, les ressources partagées auxquelles vous pouvez accéder et les AWS comptes qui ont partagé des ressources avec vous. Pour plus d'informations, consultez la section Ressources partagées avec vous dans le Guide de AWS RAM l'utilisateur.

Pour accéder à une ressource depuis une autre VPC ressource du même compte que la configuration de la ressource, il n'est pas nécessaire de partager la configuration de la ressource via AWS RAM.

Surveillance

Vous pouvez activer les journaux de surveillance sur la configuration de vos ressources. Vous pouvez choisir la destination à laquelle envoyer les journaux.

Création d'une configuration de ressources dans VPC Lattice

Utilisez la console pour créer une configuration de ressources.

Pour créer une configuration de ressources à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Lattice PrivateLink et Lattice, choisissez Resource configurations.
3. Choisissez Créer une configuration de ressources.
4. Entrez un nom unique au sein de votre AWS compte. Vous ne pouvez pas modifier ce nom une fois la configuration des ressources créée.
5. Pour Type de configuration, choisissez Ressource pour une ressource unique ou enfant ou Groupe de ressources pour un groupe de ressources enfants.
6. Choisissez une passerelle de ressources que vous avez créée précédemment ou créez-en une maintenant.

7. Choisissez l'identifiant de la ressource que vous souhaitez que cette configuration de ressource représente.
8. Choisissez les plages de ports par lesquelles vous souhaitez partager la ressource.
9. Pour les paramètres d'association, spécifiez si cette configuration de ressources peut être associée à des réseaux de services partageables.
10. Pour Partager la configuration des ressources, choisissez les partages de ressources qui identifient les principaux autorisés à accéder à cette ressource.
11. (Facultatif) Pour la surveillance, activez les journaux d'accès aux ressources et la destination de livraison si vous souhaitez surveiller les demandes et les réponses depuis et vers la configuration des ressources.
12. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
13. Choisissez Créer une configuration de ressources.

Pour créer une configuration de ressources à l'aide du AWS CLI

Utilisez la commande create-resource-configuration.

Gérer les associations pour une configuration de ressources VPC Lattice

Les comptes clients avec lesquels vous partagez une configuration de ressources et les clients de votre compte peuvent accéder à la configuration des ressources soit directement via un point de terminaison de ressource, soit via un point de VPC terminaison de réseau de services. Par conséquent, votre configuration de ressources comportera des associations de points de terminaison et des associations de réseaux de services.

Gérer les associations de réseaux de services

Créez ou supprimez une association de réseau de service.

Pour gérer une association service-réseau à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Lattice PrivateLink et Lattice, choisissez Resource configurations.
3. Sélectionnez le nom de la configuration des ressources pour ouvrir sa page de détails.

4. Sélectionnez l'onglet Associations de réseaux de services.
5. Choisissez Créer des associations.
6. Sélectionnez un réseau de service dans les réseaux de service VPC Lattice. Pour créer un réseau de service, choisissez Create a VPC Lattice network.
7. (Facultatif) Pour ajouter une balise, développez les balises d'association de services, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
8. Sélectionnez Enregistrer les modifications.
9. Pour supprimer une association, cochez la case correspondante, puis choisissez Actions, Supprimer. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour créer une association de réseau de service à l'aide du AWS CLI

Utilisez la commande create-service-network-resource-association.

Pour supprimer une association de réseau de service à l'aide du AWS CLI

Utilisez la commande delete-service-network-resource-association.

Gérer les associations de VPC terminaux

Gérez une association de VPC terminaux.

Pour gérer une association de VPC terminaux à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Lattice PrivateLink et Lattice, choisissez Resource configurations.
3. Sélectionnez le nom de la configuration des ressources pour ouvrir sa page de détails.
4. Choisissez l'onglet Endpoint associations.
5. Sélectionnez l'ID de l'association pour ouvrir sa page de détails. À partir de là, vous pouvez modifier ou supprimer l'association.
6. Pour créer une nouvelle association de points de terminaison, accédez à PrivateLink et Lattice dans le volet de navigation de gauche et choisissez Endpoints.
7. Choisissez Create endpoints.

8. Sélectionnez la configuration des ressources pour vous connecter à votreVPC.
9. Sélectionnez les VPC sous-réseaux et les groupes de sécurité.
10. (Facultatif) Pour étiqueter votre VPC point de terminaison, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
11. Choisissez Créer un point de terminaison.

Pour créer une association de point de VPC terminaison à l'aide du AWS CLI

Utilisez la commande create-vpc-endpoint.

Pour supprimer une association de point de VPC terminaison à l'aide du AWS CLI

Utilisez la commande delete-vpc-endpoint.

Passerelle de ressources dans VPC Lattice

Une passerelle de ressources est un point d'entrée dans l'VPCendroit où réside une ressource. Il couvre plusieurs zones de disponibilité. Pour que votre ressource soit accessible depuis toutes les zones de disponibilité, vous devez créer vos passerelles de ressources de manière à couvrir autant de zones de disponibilité que possible.

Une passerelle de ressources est VPC indispensable si vous prévoyez de rendre les ressources du site VPC accessibles depuis d'autres comptes VPCs ou comptes. Chaque ressource que vous partagez est liée à une passerelle de ressources. Lorsque des clients VPCs d'autres comptes accèdent à une ressource de votre compteVPC, la ressource y voit le trafic provenant localement de la passerelle de ressourcesVPC. L'adresse IP source du trafic est l'adresse IP de la passerelle de ressources. Vous pouvez attribuer plusieurs adresses IP à une passerelle de ressources pour permettre un plus grand nombre de connexions réseau avec la ressource. Plusieurs ressources d'un VPC peuvent être liées à la même passerelle de ressources.

Une passerelle de ressources ne fournit pas de fonctionnalités d'équilibrage de charge.

Table des matières

- Supprimer une passerelle de ressources dans VPC Lattice

Groupes de sécurité

Vous pouvez associer des groupes de sécurité à une passerelle de ressources. Les règles de groupe de sécurité pour les passerelles de ressources contrôlent le trafic sortant de la passerelle de ressources vers les ressources.

Règles sortantes recommandées pour le trafic circulant d'une passerelle de ressources vers une ressource de base de données

Pour que le trafic circule d'une passerelle de ressources vers une ressource, vous devez créer des règles de sortie pour les protocoles d'écoute et les plages de ports acceptés par la ressource.

Destination	Protocole	Plage de ports	Comment
CIDR range for resource	TCP	3306	Autorise le trafic entre la passerelle de ressources et les bases de données.

Types d'adresses IP

Une passerelle de ressources peut avoir des IPv4 adresses IPv6 ou des adresses à double pile. Le type d'adresse IP d'une passerelle de ressources doit être compatible avec les sous-réseaux de la passerelle de ressources et le type d'adresse IP de la ressource, comme décrit ici :

- IPv4— Attribuez IPv4 des adresses aux interfaces réseau de votre passerelle. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses et si la ressource possède également une IPv4 adresse.
- IPv6— Attribuez IPv6 des adresses aux interfaces réseau de votre passerelle. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux et que la ressource possède également une IPv6 adresse.
- Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de votre passerelle. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et si la ressource possède une IPv6 adresse IPv4 ou.

Le type d'adresse IP de la passerelle de ressources est indépendant du type d'adresse IP du client ou du VPC point de terminaison via lequel la ressource est accessible.

Créer une passerelle de ressources dans VPC Lattice

Utilisez la console pour créer une passerelle de ressources.

Pour créer une passerelle de ressources à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Lattice PrivateLink et Lattice, sélectionnez Resource gateways.
3. Choisissez Créer une passerelle de ressources.
4. Entrez un nom unique au sein de votre AWS compte.
5. Choisissez le type d'IP pour la passerelle de ressources.
6. Choisissez le dans VPC lequel se trouve la ressource.
7. Choisissez jusqu'à cinq groupes de sécurité pour contrôler le trafic entrant depuis le réseau VPC de service.
8. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
9. Choisissez Créer une passerelle de ressources.

Pour créer une passerelle de ressources à l'aide du AWS CLI

Utilisez la commande create-resource-gateway.

Supprimer une passerelle de ressources dans VPC Lattice

Utilisez la console pour supprimer une passerelle de ressources.

Pour supprimer une passerelle de ressources à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Lattice PrivateLink et Lattice, sélectionnez Resource gateways.
3. Cochez la case correspondant à la passerelle de ressources que vous souhaitez supprimer et choisissez Actions, Supprimer. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour supprimer une passerelle de ressources à l'aide du AWS CLI

Utilisez la commande delete-resource-gateway.

Accédez aux réseaux de services via AWS PrivateLink

Vous pouvez vous connecter en privé à un réseau de service à partir d'un point de terminaison du réseau de service (VPCpoint de terminaison du réseau de services). VPC Un point de terminaison de réseau de services vous permet d'accéder de manière privée et sécurisée aux ressources et aux services associés au réseau de services. De cette façon, vous pouvez accéder en privé à plusieurs ressources et services via un seul VPC point de terminaison.

Un réseau de services est un ensemble logique de configurations de ressources et de services VPC Lattice. À l'aide d'un point de terminaison de réseau de services, vous pouvez connecter un réseau de services à votre réseau de services et accéder à ces ressources et services de manière privéeVPC, depuis votre site VPC ou depuis votre site. Un point de terminaison de réseau de services vous permet de vous connecter à un réseau de service. Pour vous connecter à plusieurs réseaux de service depuis votreVPC, vous pouvez créer plusieurs points de terminaison de réseau de services, chacun pointant vers un réseau de service différent.

Les réseaux de service sont intégrés à AWS Resource Access Manager (AWS RAM). Vous pouvez partager votre réseau de service avec un autre compte via AWS RAM. Lorsque vous partagez un réseau de service avec un autre AWS compte, ce compte peut créer un point de terminaison de réseau de services pour se connecter au réseau de services. Vous pouvez partager un réseau de service à l'aide d'un partage de ressources AWS RAM.

Utilisez la AWS RAM console pour afficher les partages de ressources auxquels vous avez été ajouté, les réseaux de services partagés auxquels vous pouvez accéder et les AWS comptes qui ont partagé les ressources avec vous. Pour plus d'informations, consultez la section Ressources partagées avec vous dans le Guide de AWS RAM l'utilisateur.

Tarification

Les configurations de ressources associées à votre réseau de services vous sont facturées à l'heure. Vous êtes également facturé par Go de données traitées lorsque vous accédez aux ressources via le point de VPC terminaison du réseau de services. Le point de terminaison du réseau de services lui-même ne vous est pas facturé à VPC l'heure. Pour en savoir plus, consultez Pricing Amazon VPC Lattice (Tarification).

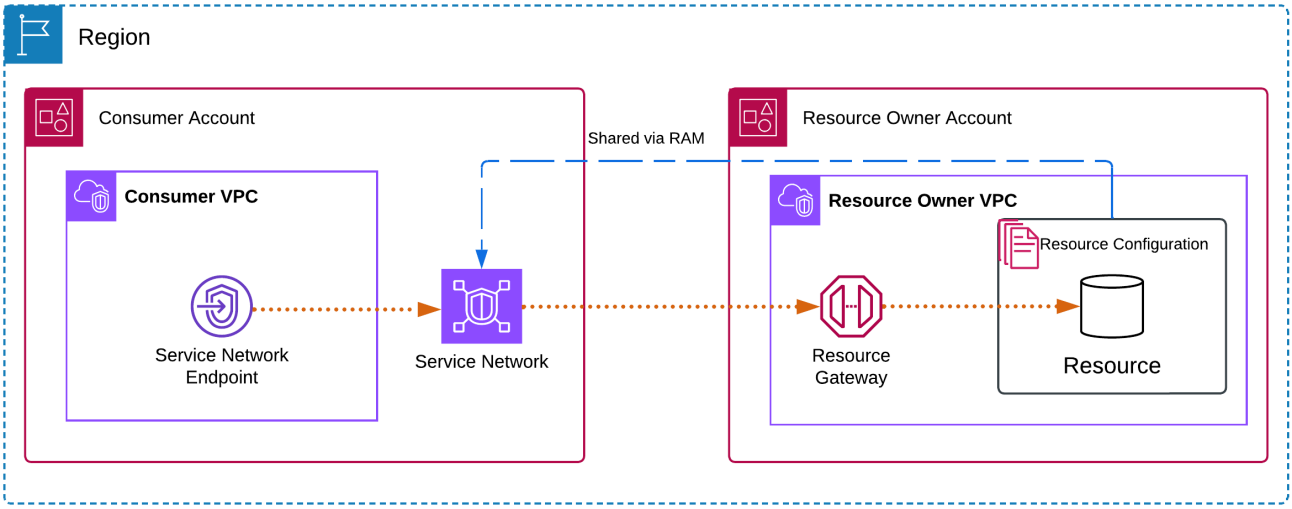
Table des matières

- DNSnoms d'hôtes
- DNSrésolution
- Privé DNS
- Sous-réseaux et zones de disponibilité
- Types d'adresses IP
- Accédez à un réseau de services via un point de terminaison du réseau de services
- Gestion des points de terminaison du réseau de services

Présentation

Vous pouvez soit créer votre propre réseau de service, soit partager un réseau de service avec vous à partir d'un autre compte. Dans tous les cas, vous pouvez créer un point de terminaison de réseau de services pour vous y connecter depuis votre. VPC Pour plus d'informations sur la création d'un réseau de services et l'association de configurations de ressources à celui-ci, consultez le guide de l'utilisateur Amazon VPC Lattice.

Le schéma suivant montre comment un point de terminaison d'un réseau de services de votre choix VPC accède à un réseau de services.



Les connexions réseau ne peuvent être initiées VPC qu'à partir du point de terminaison du réseau de services vers les ressources et les services du réseau de services. VPCAvec les ressources et les services, il n'est pas possible d'établir des connexions réseau avec le point de terminaisonVPC.

DNSnoms d'hôtes

Avec AWS PrivateLink, vous envoyez du trafic vers des réseaux de service à l'aide de points de terminaison privés. Lorsque vous créez un point de VPC terminaison de réseau de services, nous créons DNS des noms régionaux (appelés DNS nom par défaut) pour chaque ressource et service que vous pouvez utiliser pour communiquer avec la ressource et le service depuis votre site VPC et depuis votre site.

Le DNS nom par défaut d'une ressource du réseau de service possède la syntaxe suivante :

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Le DNS nom par défaut d'un service Lattice dans le réseau de services possède la syntaxe suivante :

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

Lorsque votre réseau de service utilise des configurations de ressourcesARNs, vous pouvez activer le mode privé DNS. Avec le mode privéDNS, vous pouvez continuer à envoyer des demandes à la ressource en utilisant le DNS nom fourni pour la ressource par le AWS service, tout en tirant parti de la connectivité privée via le point de terminaison du réseau de services. VPC Pour de plus amples informations, veuillez consulter the section called “DNSrésolution”.

DNSrésolution

Lorsque vous créez un point de terminaison de réseau de services, nous créons des DNS noms pour chaque configuration de ressources et chaque service Lattice associés au réseau de services. Ces DNS dossiers sont publics. Par conséquent, ces DNS noms peuvent être résolus publiquement. Cependant, les DNS demandes provenant de l'extérieur renvoient VPC toujours les adresses IP privées des interfaces réseau du point de terminaison du réseau de service. Vous pouvez utiliser ces DNS noms pour accéder aux ressources et aux services sur site, à condition d'avoir accès au point de terminaison du réseau de services dans VPC lequel se trouve, via VPN ou à Direct Connect.

Privé DNS

Si vous activez le mode privé DNS pour le point de VPC terminaison de votre réseau de services et que vous avez activé à la fois les DNSnoms d'hôte et la DNS résolution, nous créons des zones

hébergées privées masquées et AWS gérées pour les configurations de ressources portant des noms personnalisés. VPC DNS La zone hébergée contient un ensemble d'enregistrements pour le DNS nom par défaut de la ressource qui la résout en adresses IP privées des interfaces réseau du point de terminaison du réseau de services dans votre. VPC

Amazon met à votre VPC disposition un DNS serveur appelé Route 53 Resolver. Le résolveur Route 53 résout automatiquement les noms de VPC domaine locaux et les enregistre dans des zones hébergées privées. Cependant, vous ne pouvez pas utiliser le résolveur Route 53 depuis l'extérieur de votreVPC. Si vous souhaitez accéder à votre VPC point de terminaison depuis votre réseau local, vous pouvez utiliser les DNS noms par défaut ou utiliser les points de terminaison Route 53 Resolver et les règles du résolveur. Pour plus d'informations, consultez la section Intégration AWS Transit Gateway avec AWS PrivateLink et Amazon Route 53 Resolver.

Sous-réseaux et zones de disponibilité

Vous pouvez configurer votre VPC point de terminaison avec un sous-réseau par zone de disponibilité. Nous créons une interface réseau pour le point de VPC terminaison de votre sous-réseau. Nous attribuons des adresses IP à chaque interface réseau de point de terminaison à partir de son sous-réseau, en fonction du type d'adresse IP du point de VPC terminaison. Dans un environnement de production, pour une disponibilité et une résilience élevées, nous recommandons de configurer au moins deux zones de disponibilité pour chaque VPC point de terminaison.

Types d'adresses IP

Les points de terminaison du réseau de services peuvent prendre en charge des adresses ou IPv4 des adresses à IPv6 double pile. Les points de terminaison compatibles IPv6 peuvent répondre aux DNS requêtes avec des AAAA enregistrements. Le type d'adresse IP d'un point de terminaison de réseau de services doit être compatible avec les sous-réseaux du point de terminaison de ressource, comme décrit ici :

- IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
- IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
- Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

Si un point de VPC terminaison d'un réseau de services est compatibleIPv4, les interfaces réseau du point de terminaison ont IPv4 des adresses. Si un point de VPC terminaison d'un réseau de services est compatibleIPv6, les interfaces réseau du point de terminaison ont IPv6 des adresses. L'IPv6adresse d'une interface réseau de point de terminaison n'est pas accessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une IPv6 adresse, notez qu'elle `denyAllIgwTraffic` est activée.

Accédez à un réseau de services via un point de terminaison du réseau de services

Vous pouvez accéder à un réseau de services à l'aide d'un point de terminaison de réseau de services. Un point de terminaison de réseau de services fournit un accès privé aux configurations de ressources et aux services du réseau de services.

Prérequis

Pour créer un point de terminaison de réseau de services, vous devez remplir les conditions préalables suivantes.

- Vous devez disposer d'un réseau de service créé par vous ou partagé avec vous depuis un autre compte via AWS RAM.
- Si un réseau de service est partagé avec vous depuis un autre compte, vous devez vérifier et accepter le partage de ressources qui contient le réseau de service. Pour plus d'informations, consultez Acceptation et refus des invitations dans le Guide de l'utilisateur AWS RAM .

Création d'un point de terminaison de réseau de services

Créez un point de terminaison de réseau de services pour accéder au réseau de service qui a été partagé avec vous.

Pour créer un point de terminaison de réseau de services

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Vous pouvez spécifier un nom pour faciliter la recherche et la gestion du point de terminaison.

5. Dans Type, sélectionnez Réseaux de services.
6. Pour les réseaux de service, sélectionnez le réseau de service qui a été partagé avec vous.
7. Pour les paramètres réseau, sélectionnez celui VPC à partir duquel vous allez accéder au réseau de service.
8. Si vous souhaitez configurer le DNS support privé, sélectionnez Paramètres supplémentaires, puis Activer DNS le nom. Pour utiliser cette fonctionnalité, assurez-vous que les attributs Enable DNS hostnames et Enable DNS support sont activés pour votreVPC.
9. Choisissez Créer un point de terminaison.

Pour créer un point de terminaison de réseau de services à l'aide de la ligne de commande

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Outils pour Windows PowerShell)

Gestion des points de terminaison du réseau de services

Après avoir créé un point de terminaison de réseau de services, vous pouvez mettre à jour sa configuration.

Tâches

- Supprimer un point de terminaison
- Mettre à jour un point de terminaison d'un réseau de services

Supprimer un point de terminaison

Lorsque vous avez terminé d'utiliser un VPC point de terminaison, vous pouvez le supprimer.

Pour supprimer un point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison du réseau de services.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.

6. Sélectionnez Delete (Supprimer).

Pour supprimer un point de terminaison à l'aide de la ligne de commande

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Outils pour Windows PowerShell)

Mettre à jour un point de terminaison d'un réseau de services

Vous pouvez mettre à jour un VPC point de terminaison.

Pour mettre à jour un point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, puis l'option appropriée.
5. Suivez les étapes de la console pour envoyer la mise à jour.

Pour mettre à jour un point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

Gestion des identités et des accès pour AWS PrivateLink

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les AWS PrivateLink ressources. IAMest un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez AWS PrivateLink.

Utilisateur du service : si vous utilisez le AWS PrivateLink service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS PrivateLink fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur.

Administrateur du service — Si vous êtes responsable des AWS PrivateLink ressources de votre entreprise, vous avez probablement un accès complet à AWS PrivateLink. C'est à vous de déterminer les AWS PrivateLink fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS PrivateLink.

Authentification par des identités

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

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la version 4 de AWS Signature pour les API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, voir Authentification multifactorielle dans le guide de l'AWS IAM Identity Center utilisateur et Authentification AWS multifactorielle IAM dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations

d’identification d’utilisateur racine et utilisez-les pour effectuer les tâches que seul l’utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d’utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un groupe IAM est une identité qui spécifie un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour

de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Cas d'utilisation pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

Rôles IAM

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais un rôle n'est pas associé à une personne en particulier. Pour assumer temporairement un IAM rôle dans le AWS Management Console, vous pouvez passer d'un utilisateur à un IAM rôle (console). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, voir Méthodes pour assumer un rôle dans le Guide de IAM l'utilisateur.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Créer un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (un principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources

pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche ensuite une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir de IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un Service AWS dans le guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utiliser un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Les stratégies IAM définissent les autorisations d'une action quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d’une politique qui autorise l’action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l’identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

Les politiques basées sur l’identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les

politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre les politiques gérées et les politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, voir Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.

- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les OrganizationsSCPs, voir Politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs JSON politiques que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les IAM politiques associées à chaque ressource que vous possédez. Cela RCP limite les autorisations pour les ressources dans les comptes des membres et peut avoir un impact sur les autorisations effectives pour les identités Utilisateur racine d'un compte AWS, y compris, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les OrganizationsRCPs, y compris une liste de ces Services AWS supportsRCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour en savoir plus, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment AWS PrivateLink fonctionne avec IAM

Avant IAM de gérer l'accès à AWS PrivateLink, découvrez quelles IAM fonctionnalités sont disponibles AWS PrivateLink.

Fonctionnalité IAM	AWS PrivateLink soutien
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACLs	Non
ABAC(balises dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble du fonctionnement de la plupart des fonctionnalités AWS PrivateLink et des autres Services AWS IAM fonctionnalités, consultez les AWS services compatibles IAM dans le guide de IAM l'utilisateur.

Politiques basées sur l'identité pour AWS PrivateLink

Prend en charge les politiques basées sur l’identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces

politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

Avec les stratégies IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour AWS PrivateLink

Pour consulter des exemples de politiques AWS PrivateLink basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS PrivateLink

Politiques basées sur les ressources au sein de AWS PrivateLink

Prend en charge les politiques basées sur les ressources : Oui

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès entre comptes, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que mandataire dans une stratégie basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est

requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

AWS PrivateLink le service prend en charge un type de politique basée sur les ressources, connue sous le nom de stratégie de point de terminaison. Une politique de contrôle de point de terminaison que les principaux AWS peuvent utiliser le point de terminaison pour accéder au service de point de terminaison. Pour de plus amples informations, veuillez consulter the section called “Politiques de point de terminaison”.

Actions politiques pour AWS PrivateLink

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Actions dans l'espace de noms ec2

Certaines actions pour AWS PrivateLink font partie d'Amazon EC2API. Ces actions de politique utilisent le `ec2` préfixe. Pour plus d'informations, consultez AWS PrivateLink les actions dans la EC2APIréférence Amazon.

Actions dans l'espace de noms vpce

AWS PrivateLink fournit également l'action basée `AllowMultiRegion` uniquement sur les autorisations. Cette action de politique utilise le `vpce` préfixe.

Ressources politiques pour AWS PrivateLink

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Clés de conditions de politique pour AWS PrivateLink

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

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM . Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Les clés de condition suivantes sont spécifiques à AWS PrivateLink :

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Pour plus d'informations, consultez la section Clés de condition pour Amazon EC2.

ACLsdans AWS PrivateLink

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec AWS PrivateLink

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Définir des autorisations avec ABAC autorisation dans le Guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec AWS PrivateLink

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, voir Passer d'un utilisateur à un IAM rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour AWS PrivateLink

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche ensuite une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d’autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour AWS PrivateLink

Prend en charge les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir de IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un Service AWS dans le guide de IAM l'utilisateur.

Rôles liés à un service pour AWS PrivateLink

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d’effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Exemples de politiques basées sur l'identité pour AWS PrivateLink

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS PrivateLink . Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Créer des IAM politiques (console) dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AWS PrivateLink, y compris le format de ARNs pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans le Service Authorization Reference.

Exemples

- Contrôlez l'utilisation des points de VPC terminaison
- Contrôlez la création VPC de points de terminaison en fonction du propriétaire du service
- Contrôlez les DNS noms privés qui peuvent être spécifiés pour les services de point de VPC terminaison
- Contrôlez les noms de service qui peuvent être spécifiés pour les services de point de VPC terminaison

Contrôlez l'utilisation des points de VPC terminaison

Par défaut, les utilisateurs ne sont pas autorisés à utiliser des points de terminaison. Vous pouvez créer une stratégie basée sur l’identité qui autorise les utilisateurs à créer, modifier, décrire et supprimer des points de terminaison. Voici un exemple.

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

Pour plus d'informations sur le contrôle de l'accès aux services à l'aide de VPC points de terminaison, consultezthe section called “Politiques de point de terminaison”.

Contrôlez la création VPC de points de terminaison en fonction du propriétaire du service

Vous pouvez utiliser la clé de `ec2:VpceServiceOwner` condition pour contrôler quel VPC point de terminaison peut être créé en fonction du propriétaire du service (`amazon`,`aws-marketplace`, ou de l'ID du compte). L'exemple suivant accorde l'autorisation de créer des VPC points de terminaison avec le propriétaire du service spécifié. Pour utiliser cet exemple, remplacez la région, l'ID de compte et le propriétaire de service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

Contrôlez les DNS noms privés qui peuvent être spécifiés pour les services de point de VPC terminaison

Vous pouvez utiliser la clé de `ec2:VpceServicePrivateDnsName` condition pour contrôler quel service de point de VPC terminaison peut être modifié ou créé en fonction du DNS nom privé associé au service de point de VPC terminaison. L'exemple suivant accorde l'autorisation de créer un service de VPC point de terminaison avec le DNS nom privé spécifié. Pour utiliser cet exemple, remplacez la région, l'ID du compte et le DNS nom privé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

Contrôlez les noms de service qui peuvent être spécifiés pour les services de point de VPC terminaison

Vous pouvez utiliser la clé de `ec2:VpceServiceName` condition pour contrôler quel VPC point de terminaison peut être créé en fonction du nom du service du VPC point de terminaison. L'exemple suivant accorde l'autorisation de créer un VPC point de terminaison avec le nom de service spécifié. Pour utiliser cet exemple, remplacez la région, l'ID de compte et le nom de service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.s3"
                    ]
                }
            }
        }
    ]
}
```

Contrôlez l'accès aux VPC terminaux à l'aide des politiques relatives aux terminaux

Une politique de point de terminaison est une politique basée sur les ressources que vous attachez à un VPC point de terminaison pour contrôler quels AWS principaux peuvent utiliser le point de terminaison pour accéder à un. Service AWS

Une stratégie de point de terminaison n’annule ni ne remplace les politiques basées sur l'identité ni sur les ressources. Par exemple, si vous utilisez un point de terminaison d'interface pour vous connecter à Amazon S3, vous pouvez également utiliser les politiques relatives aux compartiments

Amazon S3 pour contrôler l'accès aux compartiments à partir de points de terminaison spécifiques ou spécifiques. VPCs

Table des matières

Considérations

- Une politique de point de terminaison est un document de JSON politique qui utilise le langage IAM de politique. Elle doit contenir un élément Principal. La taille d'une politique de point de terminaison ne peut excéder 20 480 caractères, espaces blancs compris.
- Lorsque vous créez une interface ou un point de terminaison de passerelle pour un Service AWS, vous pouvez associer une politique de point de terminaison unique au point de terminaison. Vous pouvez mettre à jour la politique de point de terminaison à tout moment. Si vous n'associez pas une politique de point de terminaison, nous associons la politique de point de terminaison par défaut.
- Toutes ne sont pas Services AWS compatibles avec les politiques relatives aux terminaux. Si an Service AWS ne prend pas en charge les politiques relatives aux terminaux, nous autorisons l'accès complet à n'importe quel point de terminaison pour le service. Pour de plus amples informations, veuillez consulter the section called “Afficher la prise en charge de stratégie de point de terminaison”.
- Lorsque vous créez un VPC point de terminaison pour un service de point de terminaison autre qu'un Service AWS, nous autorisons un accès complet au point de terminaison.
- Vous ne pouvez pas utiliser de caractères génériques (* ou ?) ou des opérateurs de condition numériques avec des clés de contexte globales qui font référence à des identifiants générés par le système (par exemple, ou). `aws:PrincipalAccount` `aws:SourceVpc`
- Lorsque vous utilisez un opérateur de condition de chaîne, vous devez utiliser au moins six caractères consécutifs avant ou après chaque caractère générique.
- Lorsque vous spécifiez un élément ARN dans une ressource ou une condition, la partie du compte ARN peut inclure un identifiant de compte ou un caractère générique, mais pas les deux.

Politique de point de terminaison par défaut

La politique de point de terminaison par défaut accorde un accès total au point de terminaison.

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

Politiques relatives aux points de terminaison d'interface

Par exemple, les politiques relatives aux terminaux pour Services AWS, voirthe section called “Services qui s'intègrent”. La première colonne du tableau contient des liens vers la AWS PrivateLink documentation de chacun d'entre eux Service AWS. Si un Service AWS prend en charge les politiques relatives aux terminaux, sa documentation inclut des exemples de politiques relatives aux points de terminaison.

Principaux pour les points de terminaison de passerelle

Pour * les points de terminaison de passerelle, l'`Principal`élément doit être défini sur. Pour spécifier un principal, utilisez la clé de `aws:PrincipalArn` condition.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Si vous spécifiez le principal dans le format suivant, l'accès n'est accordé Utilisateur racine d'un compte AWS qu'aux seuls utilisateurs et rôles du compte, et non à tous.

```
"AWS": "account_id"
```

Pour obtenir des exemples de politiques de point de terminaison relatives aux points de terminaison de la passerelle, veuillez consulter ce qui suit :

- Points de terminaison pour Amazon S3
- Points de terminaison pour DynamoDB

Mettre à jour une politique relative aux VPC terminaux

Utilisez la procédure suivante pour mettre à jour une politique de point de terminaison relative à un Service AWS. Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet.

Pour mettre à jour une politique de point de terminaison à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le VPC point de terminaison.
4. Choisissez Actions, Manage policy (Gérer la politique).
5. Choisissez Full Access (Accès complet) pour autoriser un accès complet au service, ou choisissez Custom (Personnalisé) et joignez une politique personnalisée.
6. Choisissez Save (Enregistrer).

Pour mettre à jour une politique de point de terminaison à l'aide de la ligne de commande

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Outils pour Windows PowerShell)

AWS politiques gérées pour AWS PrivateLink

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

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients.

Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

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

Pour plus d'informations, consultez la rubrique AWS Politiques gérées dans le IAMGuide de l'utilisateur.

AWS PrivateLink mises à jour des politiques AWS gérées

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

Modification	Description	Date
AWS PrivateLink a commencé à suivre les modifications	AWS PrivateLink a commencé à suivre les modifications apportées AWS à ses politiques gérées.	1er mars 2021

CloudWatch métriques pour AWS PrivateLink

AWS PrivateLink publie des points de données sur Amazon CloudWatch pour vos points de terminaison d'interface, vos points de terminaison Gateway Load Balancer et vos services de point de terminaison. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller une métrique spécifiée et lancer une action (telle que l'envoi d'une notification à une adresse e-mail) si la métrique dépasse ce que vous considérez comme une plage acceptable.

Les métriques sont publiées pour tous les points de terminaison d'interface, les points de terminaison Gateway Load Balancer et les services de point de terminaison. Elles ne sont pas publiées pour les points de terminaison de passerelle. Par défaut, AWS PrivateLink envoie les métriques CloudWatch à des intervalles d'une minute, sans frais supplémentaires.

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Métriques et dimensions des points de terminaison

L'espace de noms `AWS/PrivateLinkEndpoints` inclut les métriques suivantes pour les points de terminaison d'interface et les points de terminaison Gateway Load Balancer.

Métrique	Description
`ActiveConnections`	Le nombre de connexions actives simultanées. Cela inclut les connexions dans les ESTABLISHED états SYN _ SENT et.

Métrique	Description
	Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	Le nombre d'octets échangés entre les points de terminaison et les services de terminaison, agrégés dans les deux sens. Il s'agit du nombre d'octets facturés au propriétaire du point de terminaison. La facture affiche cette valeur en Go. Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute. Statistiques : les statistiques les plus utiles sont `Average`, `Sum`, `Maximum`, et `Minimum`. Dimensions • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Métrique	Description
`NewConnections`	Le nombre de nouvelles connexions établies par le point de terminaison. Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute. Statistiques : les statistiques les plus utiles sont `Average`, `Sum`, `Maximum`, et `Minimum`. Dimensions • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	Le nombre de paquets abandonnés par le point de terminaison. Cette métrique pourrait ne pas capturer tous les abandons de paquets. Des valeurs croissantes pourraient indiquer que le point de terminaison ou le service de point de terminaison n'est pas sain. Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Sum` et `Maximum`. Dimensions • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Métrique	Description
`RstPacketsReceived`	Le nombre de RST paquets reçus par le point de terminaison. Des valeurs croissantes peuvent indiquer que le service de point de terminaison n'est pas sain. Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Sum` et `Maximum`. Dimensions • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Pour filtrer ces métriques, utilisez les dimensions suivantes.

Dimension	Description
`Endpoint Type`	Filtre les données métriques par type de point de terminaison (`Interface` | `GatewayLoadBalancer`).
`Service Name`	Filtre les données métriques par nom de service.
`Subnet Id`	Filtre les données métriques par sous-réseau.
`VPC Endpoint Id`	Filtre les données métriques par VPC point de terminaison.
`VPC Id`	Filtre les données des métriques par VPC.

Métriques et dimensions de point de terminaison de service

L'espace de noms `AWS/PrivateLinkServices` inclut les métriques suivantes pour les services de points de terminaison.

Métrique	Description
`ActiveConnections`	Le nombre maximum de connexions actives des clients aux cibles via les points de terminaison. Des valeurs croissantes pourraient indiquer la nécessité d'ajouter des cibles à l'équilibreur de charge. Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute. Statistiques : les statistiques les plus utiles sont `Average` et `Maximum`. Dimensions • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	Le nombre d'octets échangés entre les services de point de terminaison et les points de terminaison, dans les deux sens. Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Sum` et `Maximum`. Dimensions • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	Le nombre de points de terminaison connectés au service de point de terminaison.

Métrique	Description
	Critères de rapport : il y a une valeur non nulle pendant la période de cinq minutes. Statistiques : les statistiques les plus utiles sont `Average` et `Maximum`. Dimensions • `Service Id`
`NewConnections`	Le nombre de nouvelles connexions établies entre les clients et les cibles via les points de terminaison. Des valeurs croissantes pourraient indiquer la nécessité d'ajouter des cibles à l'équilibreur de charge. Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Sum` et `Maximum`. Dimensions • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Métrique	Description
`RstPacketsSent`	Nombre de RST paquets envoyés aux points de terminaison par le service de point de terminaison. Des valeurs croissantes pourraient indiquer la présence de cibles non saines. Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute. Statistics : les statistiques les plus utiles sont `Average`, `Sum` et `Maximum`. Dimensions • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Pour filtrer ces métriques, utilisez les dimensions suivantes.

Dimension	Description
`Az`	Filtrer les données métriques par Zone de disponibilité.
`Load Balancer Arn`	Filtre les données métriques en fonction de l'équilibreur de charge.
`Service Id`	Filtre les données métriques par service de point de terminaison.
`VPC Endpoint Id`	Filtre les données métriques par VPC point de terminaison.

Afficher les CloudWatch indicateurs

Vous pouvez consulter ces CloudWatch statistiques à l'aide de la VPC console Amazon, de la CloudWatch console ou de la manière AWS CLI suivante.

Pour consulter les métriques à l'aide de la VPC console Amazon

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison. Sélectionnez le point de terminaison, puis choisissez l'onglet Monitoring (Surveillance).
3. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison). Sélectionnez le service de votre point de terminaison, puis choisissez l'onglet Monitoring (Surveillance).

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de PrivateLinkEndpoints noms AWS/.
4. Sélectionnez l'espace de PrivateLinkServices noms AWS/.

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles pour les points de terminaison d'interface et les points de terminaison de Gateway Load Balancer :

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles pour les services de points de terminaison :

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Utilisation des règles intégrées de Contributor Insights

AWS PrivateLink fournit des règles intégrées d'analyse des contributeurs pour vos services de point de terminaison afin de vous aider à déterminer quels points de terminaison contribuent le plus à chaque métrique prise en charge. Pour plus d'informations, consultez Contributor Insights dans le guide de CloudWatch l'utilisateur Amazon.

AWS PrivateLink fournit les règles suivantes :

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` : classe les points de terminaison en fonction du nombre de connexions actives.
- `VpcEndpointService-BytesByEndpointId-v1` : classe les points de terminaison en fonction du nombre d'octets traités.
- `VpcEndpointService-NewConnectionsByEndpointId-v1` : classe les points de terminaison en fonction du nombre de nouvelles connexions.
- `VpcEndpointService-RstPacketsByEndpointId-v1`— Classe les points de terminaison en fonction du nombre de RST paquets envoyés aux points de terminaison.

Avant de pouvoir utiliser une règle intégrée, vous devez l'activer. Une fois que vous avez activé une règle, elle commence à collecter les données des contributeurs. Pour plus d'informations sur les frais associés à Contributor Insights, consultez Amazon CloudWatch Pricing.

Vous devez disposer des autorisations suivantes pour utiliser Contributor Insights :

- `cloudwatch:DeleteInsightRules` – Pour supprimer les règles Contributor Insights.
- `cloudwatch:DisableInsightRules` – Pour désactiver les règles Contributor Insights.
- `cloudwatch:GetInsightRuleReport` – Pour obtenir les données.
- `cloudwatch:ListManagedInsightRules` – Pour répertorier les règles Contributor Insights disponibles.
- `cloudwatch:PutManagedInsightRules` – Pour activer les règles Contributor Insights.

Tâches

- Activez les règles Contributor Insights
- Désactivez les règles Contributor Insights
- Supprimer les règles Contributor Insights

Activez les règles Contributor Insights

Utilisez les procédures suivantes pour activer les règles intégrées permettant AWS PrivateLink d'utiliser le AWS Management Console ou le AWS CLI.

Pour activer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison.
4. Sur l'onglet Contributor Insights, choisissez Enable (Activer).
5. (Facultatif) Par défaut, toutes les règles sont activées. Pour activer uniquement des règles spécifiques, sélectionnez les règles qui ne doivent pas être activées, puis choisissez Actions (Actions), Désactiver la règle. Lorsque vous êtes invité à confirmer l'opération, choisissez Désactiver .

Pour activer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation du AWS CLI

1. Utilisez la list-managed-insight-rulescommande suivante pour énumérer les règles disponibles. Pour l'`--resource-arn`option, spécifiez le service ARN de votre point de terminaison.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Dans la sortie de la commande `list-managed-insight-rules`, copiez le nom du modèle depuis le champ `TemplateName`. Voici un exemple de ce champ.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Utilisez la put-managed-insight-rulescommande suivante pour activer la règle. Vous devez spécifier le nom du modèle et celui ARN de votre service de point de terminaison.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Désactivez les règles Contributor Insights

Vous pouvez désactiver les règles intégrées AWS PrivateLink à tout moment. Une fois que vous avez désactivé une règle, elle arrête de collecter les données des contributeurs, mais les données de contributeurs existantes sont conservées jusqu'à ce qu'elles aient 15 jours. Après avoir désactivé une règle, vous pouvez l'activer à nouveau pour reprendre la collecte de données des contributeurs.

Pour désactiver les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison.
4. Sur l'onglet Contributor Insights, choisissez Désactiver tout pour désactiver toutes les règles. Sinon, développez le panneau Règles, sélectionnez les règles à désactiver, puis choisissez Actions, Désactiver la règle
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Désactiver .

Pour désactiver les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation du AWS CLI

Utilisez la disable-insight-rulescommande pour désactiver une règle.

Supprimer les règles Contributor Insights

Utilisez les procédures suivantes pour supprimer les règles intégrées relatives AWS PrivateLink à l'utilisation du AWS Management Console ou du AWS CLI. Une fois que vous supprimez une règle, elle cesse de collecter les données des contributeurs et nous supprimons les données de contributeurs existantes.

Pour supprimer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Insights, puis choisissez Contributor Insights.
3. Développez le panneau Règles et sélectionnez les règles.
4. Choisissez Actions, puis Supprimer la règle.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer les règles relatives à l' AWS PrivateLink utilisation de Contributor Insights AWS CLI

Utilisez la delete-insight-rulescommande pour supprimer une règle.

AWS PrivateLink quotas

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés. Si vous demandez d'augmenter un quota s'appliquant par ressource, nous l'augmentons pour toutes les ressources de la région.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Limitation des demandes

Les API actions pour AWS PrivateLink font partie d'Amazon EC2API. Amazon EC2 limite ses API demandes au niveau supérieur. Compte AWS Pour plus d'informations, consultez la section Régulation des demandes dans le manuel Amazon EC2 Developer Guide. En outre, les API demandes sont également limitées au niveau de l'organisation pour améliorer les performances de. AWS PrivateLink Si vous utilisez AWS Organizations et que vous recevez un code `RequestLimitExceeded` d'erreur alors que vous respectez toujours les API limites de votre compte, consultez Comment identifier les AWS comptes qui passent un grand nombre d'APIappels. Si vous avez besoin d'aide, contactez l'équipe chargée de votre compte ou ouvrez un dossier de support technique en utilisant le VPCservice et la catégorie VPCEndpoints. N'oubliez pas de joindre une image du code `RequestLimitExceeded` d'erreur.

VPCquotas de terminaux

Votre AWS compte possède les quotas suivants relatifs aux VPC points de terminaison.

Nom	Par défaut	Ajustable	Commentaires
Points de terminaison Load Balancer d'interface et de passerelle par VPC	50	Oui	Il s'agit d'un quota combiné pour les points de terminaison d'interface et les points de terminaison d'équilibreur de charge de passerelle
VPCPoints de terminaison de passerelle par région	20	Oui	Vous pouvez créer jusqu'à 255 points de terminaison de passerelle par VPC

Nom	Par défaut	Ajustable	Commentaires
Politique relative aux caractères par VPC point de terminaison	20 480	Non	Taille maximale d'une politique de point de VPC terminaison, espaces blancs compris

Les considérations suivantes s'appliquent au trafic qui passe par un VPC point de terminaison :

- Par défaut, chaque VPC point de terminaison peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et évolue automatiquement jusqu'à 100 Gbit/s. La bande passante maximale pour un VPC point de terminaison, lors de la répartition de la charge entre toutes les zones de disponibilité, est le nombre de zones de disponibilité multiplié par 100 Gbit/s. Si votre application nécessite un débit plus élevé, contactez le support AWS .
- L'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus grand paquet autorisé pouvant être transmis par un VPC point de terminaison. Plus le volume est importantMTU, plus le volume de données pouvant être transmis dans un seul paquet est important. Un VPC point de terminaison prend en charge un MTU de 8 500 octets. Les paquets d'une taille supérieure à 8 500 octets qui arrivent au VPC point de terminaison sont supprimés.
- Path MTU Discovery (PMTUD) n'est pas pris en charge. VPCles points de terminaison ne génèrent pas le ICMP message suivant : `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Type 3, Code 4).
- VPCles points de terminaison appliquent le blocage de la taille maximale du segment (MSS) pour tous les paquets. Pour plus d'informations, consultez RFC879.

Historique du document pour AWS PrivateLink

Le tableau suivant décrit les versions de AWS PrivateLink.

Modification	Description	Date
Ressources d'accès et réseaux de services	AWS PrivateLink prend en charge l'accès aux ressource s et aux réseaux de services au-delà VPC des limites des comptes.	1er décembre 2024
Accès interrégional	Un fournisseur de services peut héberger un service dans une région et le rendre disponible dans un ensemble de AWS régions. Un consommateur de services sélectionne une région de service lors de la création d'un point de terminaison.	26 novembre 2024
Adresses IP désignées	Vous pouvez spécifier les adresses IP des interface s réseau de votre point de terminaison lorsque vous créez ou modifiez votre VPC point de terminaison.	17 août 2023
IPv6 Prise en charge de	Vous pouvez configurer vos services de point de terminais on Gateway Load Balancer et vos points de terminaison Gateway Load Balancer pour qu'ils prennent en charge à la IPv4 fois les adresses IPv6 et	le 12 décembre 2022

	les adresses ou uniquement les adresses. IPv6	
Contributor Insights	Vous pouvez utiliser les règles intégrées de Contributor Insights pour identifier les points de terminaison spécifiqu es qui contribuent le plus aux CloudWatch statistiques pour AWS PrivateLink.	18 août 2022
IPv6 Prise en charge de	Les fournisseurs de services peuvent autoriser leur service de point de terminaison à accepter les IPv6 demandes, même si leurs services principaux ne prennent en charge que IPv4 le support. Si un service de point de terminaison accepte les IPv6 demandes, les consommat eurs du service peuvent activer le IPv6 support pour les points de terminaison de leur interface afin qu'ils puissent accéder au service de point de terminaison via IPv6 le biais du service de point de terminaison.	11 mai 2022
CloudWatch métriques	AWS PrivateLink publie des CloudWatch métriques pour les points de terminaison de votre interface, les points de terminaison Gateway Load Balancer et les services de point de terminaison.	27 janvier 2022

Points de terminaison de l'équilibreur de charge de passerelle	Vous pouvez créer un point de terminaison Gateway Load Balancer dans votre terminal VPC pour acheminer le trafic vers un service de point de VPC terminaison que vous avez configuré à l'aide d'un Gateway Load Balancer.	10 novembre 2020
VPCpolitiques relatives aux terminaux	Vous pouvez associer une IAM politique à un point de VPC terminaison d'interface pour un AWS service afin de contrôler l'accès au service.	23 mars 2020
Clés de condition pour les VPC terminaux et les services des terminaux	Vous pouvez utiliser des clés de EC2 condition pour contrôler l'accès aux points de VPC terminaison et aux services des points de terminaison.	6 mars 2020
Étiquetez les VPC terminaux et les services de point de terminaison lors de leur création	Vous pouvez ajouter des balises lorsque vous créez des VPC points de terminais on et des services de point de terminaison.	5 février 2020
DNSNoms privés	Vous pouvez accéder aux services AWS PrivateLink basés depuis votre propre compte VPC en utilisant DNS des noms privés.	6 janvier 2020

VPCservices de terminaux	Vous pouvez créer vos propres services de point de terminaison et permettre à d'autres Comptes AWS utili sateurs de se connecter à votre service via un point de VPC terminaison d'interfa ce. Vous pouvez proposer vos services de point de terminaison à l'abonnement sur AWS Marketplace.	28 novembre 2017
VPCPoints de terminaison d'interface pour Services AWS	Vous pouvez créer un point de terminaison d'interface Services AWS auquel vous connecter à cette intégrati on AWS PrivateLink sans utiliser de passerelle Internet ou d'NATappareil.	8 novembre 2017
VPCpoints de terminaison pour DynamoDB	Vous pouvez créer un point de VPC terminaison de passerell e pour accéder à Amazon DynamoDB depuis VPC votre ordinateur sans passer par une passerelle Internet ou un appareil. NAT	le 16 août 2017
VPCpoints de terminaison pour Amazon S3	Vous pouvez créer un point de VPC terminaison de passerell e pour accéder à Amazon S3 depuis votre VPC ordinateur sans passer par une passerell e Internet ou un NAT appareil.	le 11 mai 2015

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.