AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

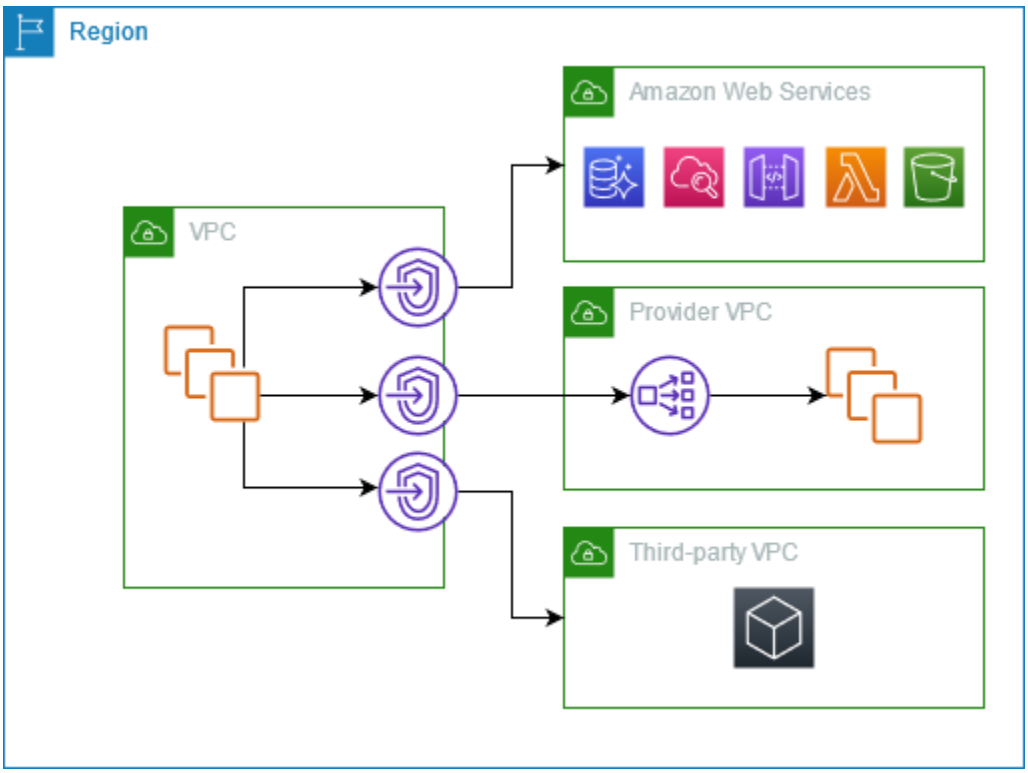
Qu'est-ce que c'est AWS PrivateLink ?

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

Cas d’utilisation

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

Dans le schéma suivant, le VPC de gauche possède plusieurs instances EC2 dans un sous-réseau privé et trois points de terminaison d’un VPC d'interface. Le point de terminaison VPC supérieur se connecte à un. Service AWS Le point de terminaison VPC intermédiaire se connecte à un service hébergé par un autre Compte AWS (un service de point de terminaison VPC). Le point de terminaison VPC inférieur se connecte à un service AWS Marketplace partenaire.



En savoir plus

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

Utiliser des points de terminaison d'un VPC

Vous pouvez créer, accéder et gérer des points de terminaison d’un VPC 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 console Amazon VPC 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
  - Notification AWS : :EC2 : :VPC EndpointConnection
  - AWS::EC2::VPCEndpointService
  - Autorisations AWS : :EC2 : :VPC EndpointService
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDK — Fournissez des API spécifiques au langage. Les kits de développement (SDK) prennent en charge la plupart des détails de connexion, notamment le calcul des signatures, le traitement des nouvelles tentatives de demande et le traitement des erreurs. Pour plus d'informations, consultez la section Outils sur lesquels vous pouvez vous appuyer AWS.
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à Amazon VPC. 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 les AWS PrivateLink actions dans la Référence API d'Amazon EC2.

Tarification

Pour en savoir plus sur la tarification des points de terminaison d’un VPC, voir Tarification AWS PrivateLink.

AWS PrivateLink concepts

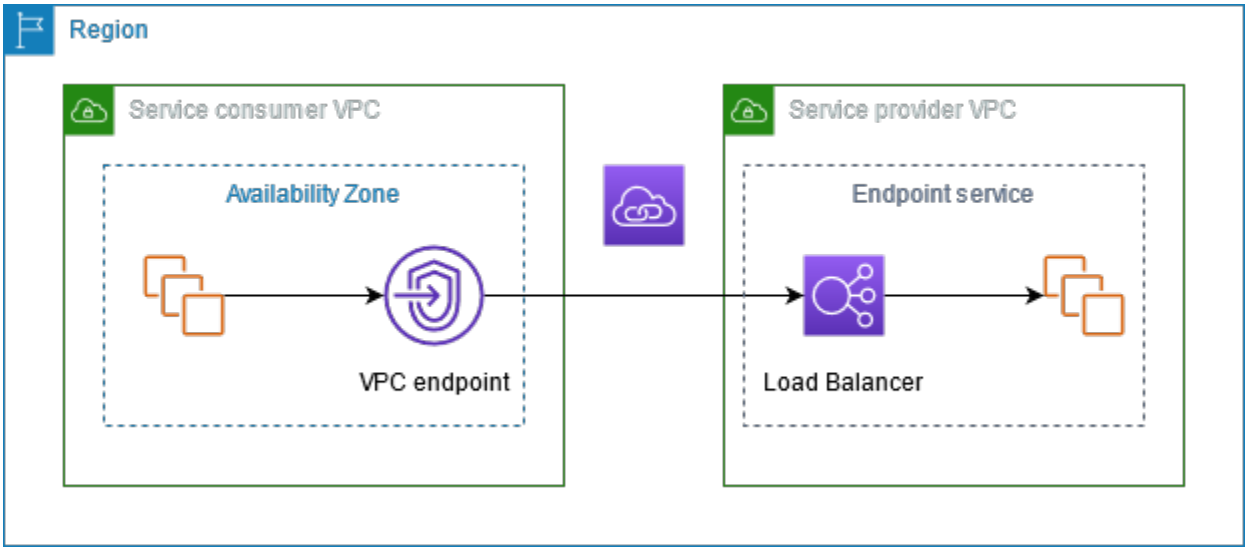
Vous pouvez utiliser Amazon VPC pour définir un cloud privé virtuel (VPC, Virtual Private Cloud), qui est un réseau virtuel logiquement isolé. Vous pouvez lancer AWS des ressources dans votre VPC. Vous pouvez autoriser les ressources de votre VPC à se connecter à des ressources extérieures à ce VPC. Par exemple, ajoutez une passerelle Internet au VPC pour permettre l'accès à Internet, ou ajoutez une connexion VPN pour permettre l'accès à votre réseau sur site. Vous pouvez également utiliser AWS PrivateLink cette option pour autoriser les ressources de votre VPC à se connecter aux services d'autres VPC à l'aide d'adresses IP privées, comme si ces services étaient hébergés directement dans votre VPC.

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 du service créent des points de terminaison d'un VPC d'interface pour se connecter aux services de point de terminaison qui sont hébergés par les fournisseurs du service.



Fournisseurs du service

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 des instances EC2, ou à l'aide de serveurs sur site.

Concepts

- Services de point de terminaison

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. Le consommateur du service doit spécifier le nom du service lors de la création d'un point de terminaison d’un VPC. 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.

Consommateurs du service

L'utilisateur d'un service est un consommateur du service. Les consommateurs de services peuvent accéder aux services des terminaux depuis AWS des ressources, telles que des instances EC2, ou depuis des serveurs sur site.

Concepts

- Points de terminaison d’un VPC
- Interfaces réseau de point de terminaison
- Politiques de point de terminaison
- États de point de terminaison

Points de terminaison d’un VPC

Le consommateur du services crée un point de terminaison d’un VPC pour connecter son VPC à un service de point de terminaison. Le consommateur du service doit spécifier le nom du service de point de terminaison lors de la création d'un point de terminaison d’un VPC. Il existe plusieurs types de points de terminaison d’un VPC. Vous devez créer le type de point de terminaison d’un VPC requis par le service de point de terminaison.

- `Interface` : créez un point de terminaison d'interface pour envoyer le trafic TCP à un service de point de terminaison. Le trafic destiné au service de point de terminaison est résolu à l'aide du DNS.
- `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 VPC vers le point de terminaison d'équilibreur de charge de passerelle 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.

Il existe un autre type de point de terminaison d'un VPC, `Gateway`, qui crée un point de terminaison de passerelle pour envoyer le trafic vers Amazon S3 ou DynamoDB. Les points de terminaison de passerelle ne sont pas utilisés AWS PrivateLink, contrairement aux autres types de points de terminaison VPC. Pour plus d’informations, consultez the section called “Points de terminaison de passerelle”.

Interfaces réseau de point de terminaison

L'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 de point de terminaison. Pour chaque sous-réseau que vous spécifiez lorsque vous créez un point de terminaison de VPC, nous créons une interface réseau de point de terminaison dans le sous-réseau.

Si le point de terminaison d'un VPC prend en charge le protocole IPv4, ses interfaces réseau du point de terminaison possèdent des adresses IPv4. Si le point de terminaison d'un VPC prend en charge le protocole IPv6, ses interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de terminaison est inaccessible depuis Internet. Lorsque vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, notez que `denyAllIgwTraffic` est activé.

Les adresses IP d'une interface réseau de point de terminaison ne changeront pas pendant la durée de vie de son point de terminaison d'un VPC.

Politiques de point de terminaison

La politique de point de terminaison de VPC est une politique de ressources IAM qui est jointe à un point de terminaison d'un VPC. Elle détermine quels principaux peuvent utiliser le point de terminaison d'un VPC pour accéder au service de point de terminaison. La politique par défaut de point de terminaison d'un VPC autorise toutes les actions de tous les principaux sur toutes les ressources via le point de terminaison d'un VPC.

États de point de terminaison

Quand vous créez un point de terminaison d'un VPC, le service de point de terminaison reçoit une demande de connexion. Le fournisseur du service peut accepter ou refuser la demande. Si le fournisseur du service accepte la demande, le consommateur du service peut utiliser le point de terminaison d'un VPC après que ce dernier soit passé à l'état `Available`.

Les états possibles pour un point de terminaison d'un VPC 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 point de terminaison d'un VPC revient à cet état si le consommateur du service modifie le point de terminaison d'un VPC.
- `Available` – Le point de terminaison d'un VPC est disponible pour utilisation.
- `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 point de terminaison d'un VPC n'a pas pu être rendu disponible.

- `Deleting` – Le consommateur du service a supprimé le point de terminaison d'un VPC et la suppression est en cours.
- `Deleted` – Le point de terminaison d'un VPC est supprimé.

AWS PrivateLink connexions

Le trafic provenant de votre VPC est envoyé à un service de point de terminaison via une connexion entre le point de terminaison d'un VPC et le service de point de terminaison. Le trafic entre un point de terminaison VPC et un service 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.

Avec un point de terminaison d'un VPC, les utilisateurs peuvent utiliser des politiques de point de terminaison pour contrôler quels principaux IAM peuvent utiliser le point de terminaison d'un VPC pour accéder au service de point de terminaison.

Zones hébergées privées

La zone hébergée est un conteneur pour les enregistrements DNS qui définissent comment acheminer le trafic pour un domaine ou un sous-domaine. Avec une zone hébergée publique, les enregistrements précisent comment acheminer le trafic sur Internet. Avec une zone hébergée privée, les enregistrements précisent comment acheminer le trafic dans vos VPC.

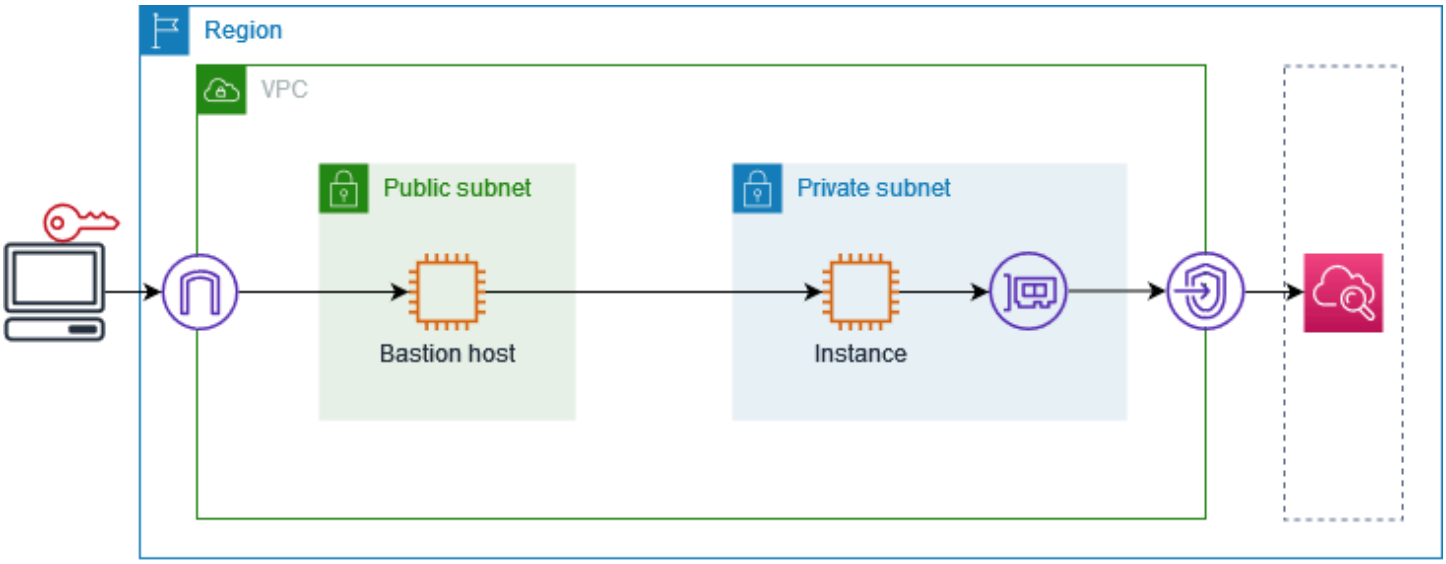
Vous pouvez configurer Amazon Route 53 pour acheminer le trafic du domaine vers un point de terminaison de VPC. Pour plus d'informations, voir Acheminement du trafic vers un point de terminaison de VPC en utilisant votre nom de domaine.

Vous pouvez utiliser Route 53 pour configurer le DNS à horizon partagé, dans lequel vous utilisez le même nom de domaine pour un site Web public et un service de point de terminaison alimenté par. AWS PrivateLink Les requêtes DNS pour le nom d'hôte public provenant du VPC du consommateur sont résolues en adresses IP privées des interfaces réseau de point de terminaison, mais les requêtes provenant de l'extérieur du VPC continuent à être résolues en points de terminaison publics. Pour plus d'informations, voir Mécanismes DNS pour l'acheminement du trafic et l'activation du basculement pour les déploiements AWS PrivateLink.

Commencez avec AWS PrivateLink

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

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 fichier `.pem` de la clé privée se trouve sur votre ordinateur et non sur l'hôte bastion, vous utiliserez le transfert de clé SSH. 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 point de terminaison VPC pour CloudWatch, le trafic provenant de l'instance à laquelle il CloudWatch est destiné est résolu vers l'interface réseau du point de terminaison, puis envoyé à l' CloudWatch aide du point de terminaison VPC.



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

Étape 1 : Créer un VPC et 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 console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
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 Create VPC (Créer un VPC).

Étape 2 : Lancer les instances

À l'aide du VPC 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 trafic SSH entrant à partir du bloc CIDR de votre ordinateur.

- Créez un groupe de sécurité pour l'instance qui autorise le trafic SSH entrant depuis le groupe de sécurité pour l'hôte bastion.
- Créez un profil d'instance IAM et associez la politique CloudWatchReadOnlyd'accès.

Pour lancer l'hôte bastion

1. Ouvrez la console Amazon EC2 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 votre VPC.
    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 console Amazon EC2 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 votre VPC.
    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). Pour IAM instance profile (Profil d'instance IAM), choisissez votre nom de profil d'instance IAM.
8. Choisissez Launch 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'agent SSH à l'aide de la commande suivante, où *key.pem* est 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'option `--region`, spécifiez la région dans laquelle vous avez créé le VPC.

```
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 configuration VPC actuelle.

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

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

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

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

Prérequis

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

Pour créer un point de terminaison VPC pour CloudWatch

1. Ouvrez la console Amazon VPC 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***.monitoring.
7. Pour VPC, sélectionnez votre VPC.
8. Pour Subnets (Sous-réseaux), sélectionnez la zone de disponibilité puis le sous-réseau privé.
9. Pour Security group (Groupe de sécurité), sélectionnez le groupe de sécurité du point de terminaison d'un VPC.
10. Pour Policy (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison d'un VPC.
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 : Test du point de terminaison d'un VPC

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

Pour tester le point de terminaison d'un VPC

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

```
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 rôle IAM 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'option `--region` indique la région dans laquelle vous avez créé le point de terminaison d'un VPC.

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 console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez 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 d'un point de terminaison d’un VPC, vous pouvez le supprimer.

Pour supprimer le point de terminaison d’un VPC

1. Ouvrez la console Amazon VPC 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’un VPC.
4. Choisissez Actions, Delete VPC endpoints (Supprimer le point de terminaison d’un VPC).
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 VPC afin que le trafic puisse passer du VPC vers Service AWS. Si cette configuration ne répond pas aux exigences de sécurité de votre réseau, vous pouvez AWS PrivateLink connecter votre VPC Services AWS comme s'il se trouvait dans votre VPC, sans passer par une passerelle Internet.

Vous pouvez accéder en privé à ceux Services AWS qui s'intègrent à l' AWS PrivateLink aide de points de terminaison VPC. 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 le point de terminaison VPC de votre interface est provisionné dans chaque zone de disponibilité. Vous êtes également facturé par Go de données traitées. Pour plus d’informations, consultez Tarification d’AWS PrivateLink.

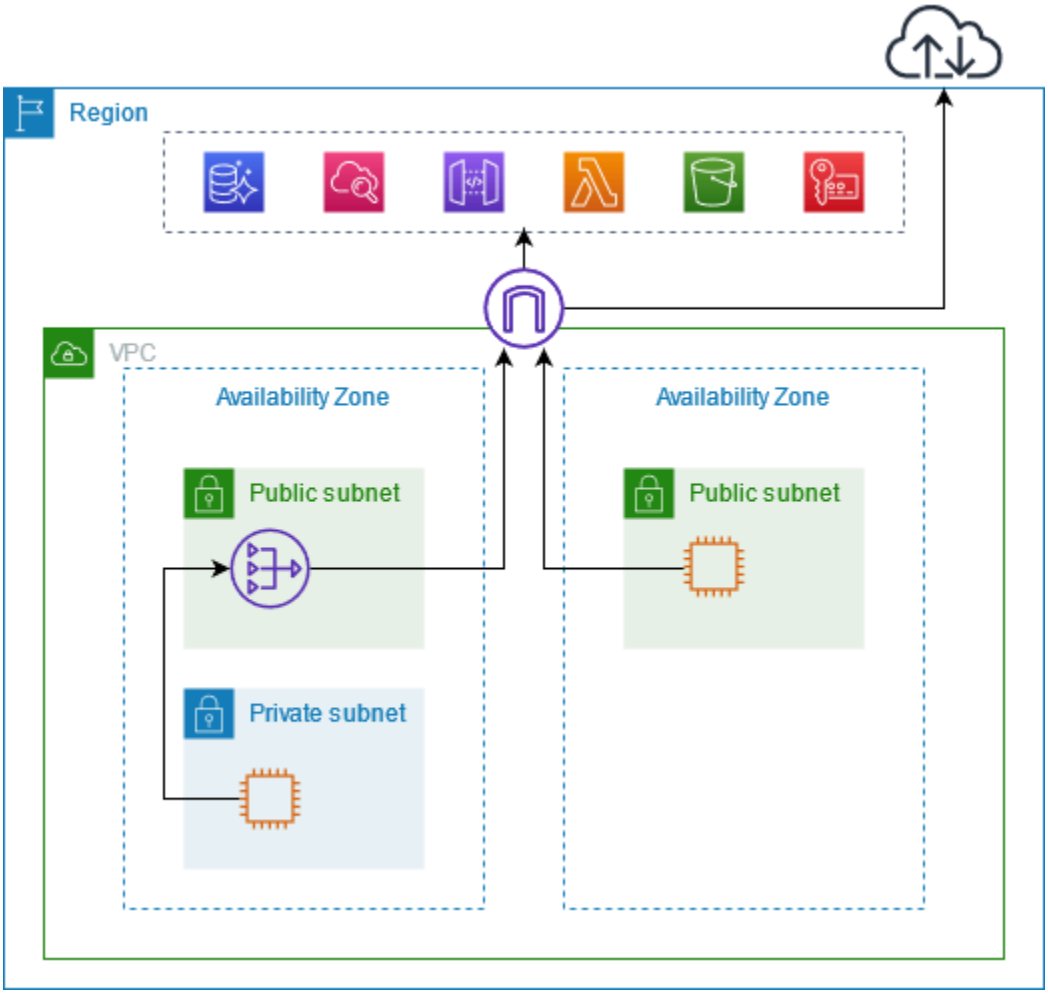
Table des matières

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.

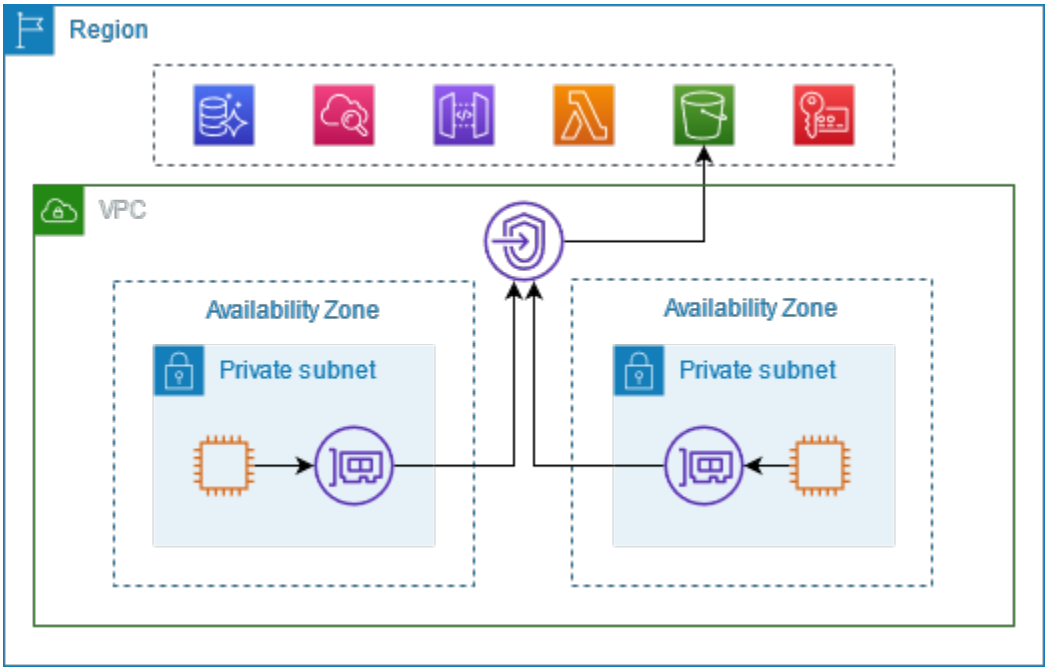
Accès via des points de terminaison de service public

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 du VPC, puis vers le. Service AWS Le trafic vers un Service AWS à partir d'une instance d'un sous-réseau privé est acheminé vers une passerelle NAT, puis vers la passerelle Internet pour le VPC, 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 terminaison VPC d'interface, qui établit des connexions entre les sous-réseaux de votre VPC et une interface réseau d'utilisation. Service AWS Le trafic destiné au Service AWS est résolu vers les adresses IP privées des interfaces réseau du point de terminaison à l'aide du DNS, puis envoyé au Service AWS moyen de la connexion entre le point de terminaison VPC et le. Service AWS



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

Noms d'hôte DNS

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 terminaison VPC d'interface, nous créons des noms DNS régionaux et zonaux que vous pouvez utiliser pour communiquer avec eux depuis Service AWS votre VPC.

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

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

Les noms DNS zonaux ont la syntaxe suivante :

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

Lorsque vous créez un point de terminaison VPC d'interface pour un Service AWS, vous pouvez activer le DNS privé. Avec le DNS privé, vous pouvez continuer à effectuer des demandes à un service en utilisant le nom DNS de son point de terminaison public, tout en tirant parti de la connectivité privée via le point de terminaison d'un VPC de l'interface. Pour plus d'informations, consultez the section called "Résolution DNS".

La commande describe-vpc-endpoints suivante affiche les entrées DNS 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 des noms DNS 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"
        }
    ]
]
```

Résolution DNS

Les enregistrements DNS que nous créons pour votre point de terminaison de VPC d'interface sont publics. Par conséquent, ces noms DNS peuvent être résolus publiquement. Cependant, les requêtes DNS provenant de l'extérieur du VPC renvoient toujours les adresses IP privées des interfaces réseau du point de terminaison, de sorte que ces adresses IP ne peuvent pas être utilisées pour accéder au service de point de terminaison, sauf si vous avez accès au VPC.

DNS privé

Si vous activez le DNS privé pour le point de terminaison VPC de votre interface et que les noms d'hôte DNS et la résolution DNS sont activés sur votre VPC, nous créons pour vous une zone AWS hébergée privée masquée et gérée. La zone hébergée contient un ensemble d'enregistrements pour le nom DNS par défaut du service qui se résout en adresses IP privées des interfaces réseau du point de terminaison de votre VPC. 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 noms DNS privés pour vos points de terminaison VPC 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 point de terminaison VPC.

Amazon fournit un serveur DNS pour votre VPC, appelé Route 53 Resolver. Route 53 Resolver résout automatiquement les noms de domaine VPC locaux et enregistre dans des zones hébergées privées. Toutefois, vous ne pouvez pas utiliser Route 53 Resolver en dehors de votre VPC. Si vous souhaitez accéder à votre point de terminaison d'un VPC depuis votre réseau sur site, vous pouvez utiliser les points de terminaison Route 53 Resolver et les règles Resolver. Pour plus d'informations, consultez la section Intégration AWS Transit Gateway avec AWS PrivateLink et Amazon Route 53 Resolver.

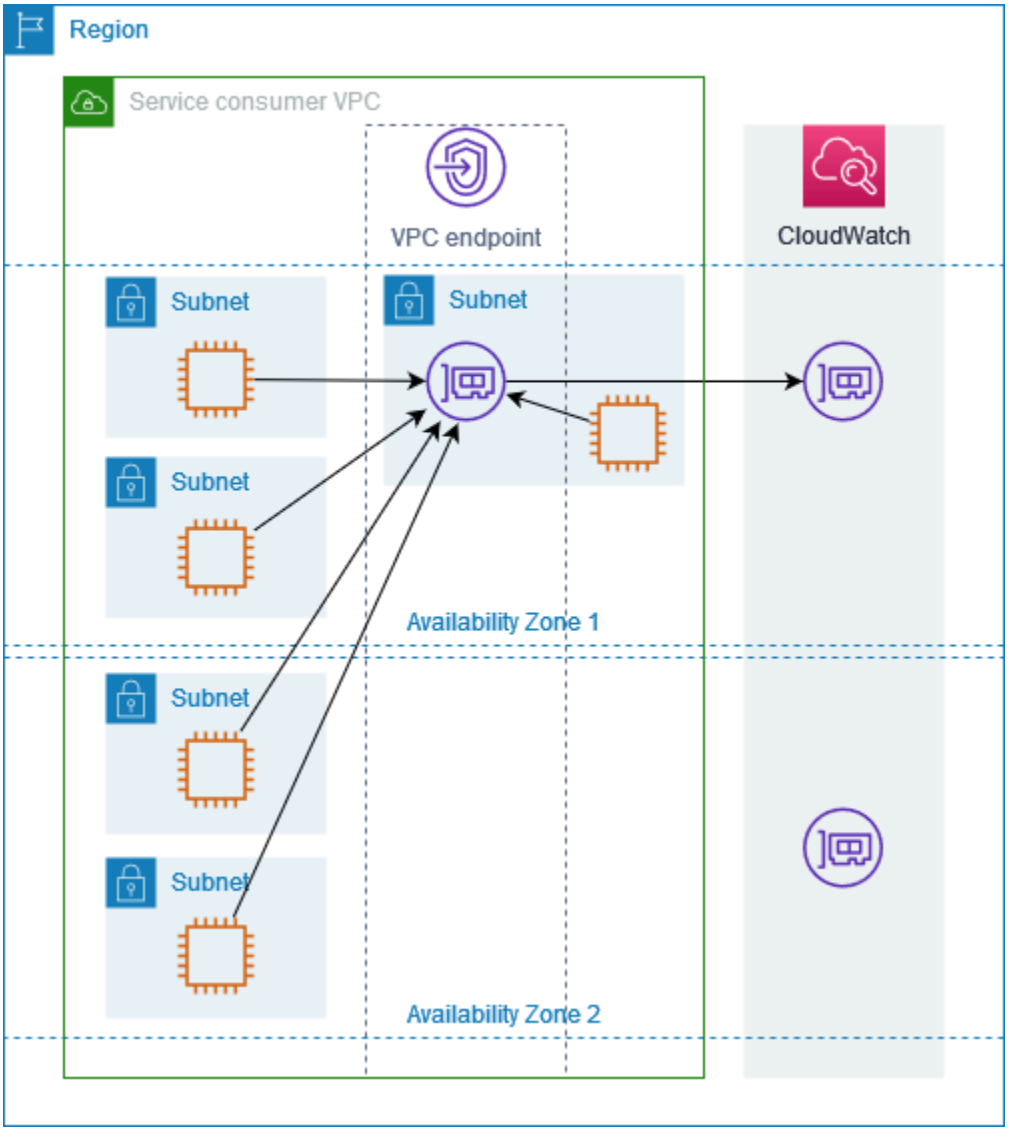
Sous-réseaux et zones de disponibilité

Vous pouvez configurer votre point de terminaison d'un VPC avec un sous-réseau par zone de disponibilité. Nous créons une interface réseau pour le point de terminaison d'un VPC dans 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 terminaison d'un VPC. Les adresses IP d'une interface réseau de point de terminaison ne changeront pas pendant la durée de vie de son point de terminaison d'un VPC.

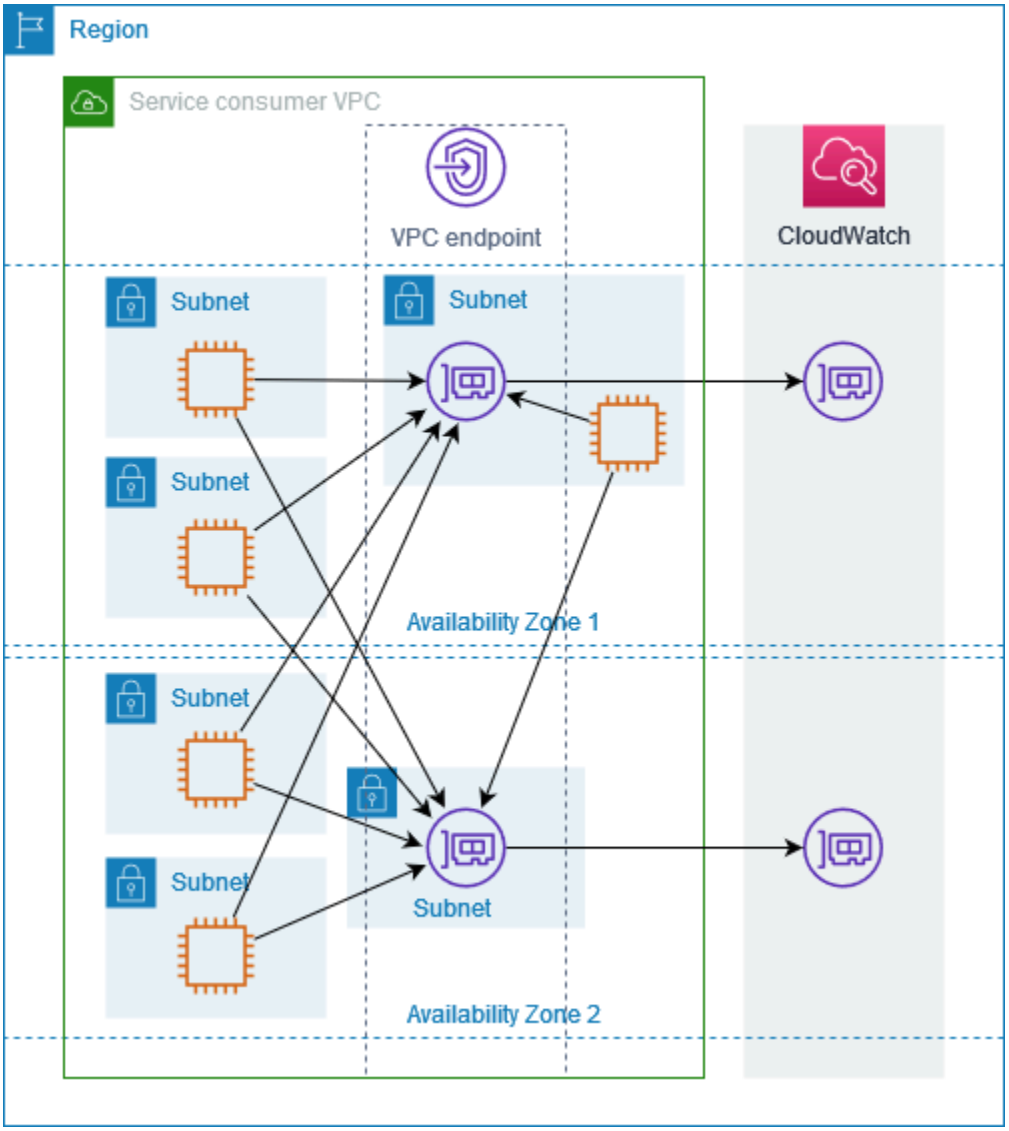
Dans un environnement de production, pour assurer une disponibilité et une résilience élevées, nous recommandons ce qui suit :

- Configurez au moins deux zones de disponibilité par point de terminaison VPC et déployez les AWS Service AWS ressources qui doivent y accéder.
- configurez les noms DNS privés pour le point de terminaison d'un VPC.
- Accédez au Service AWS en utilisant son nom DNS régional, également connu sous le nom de point de terminaison public.

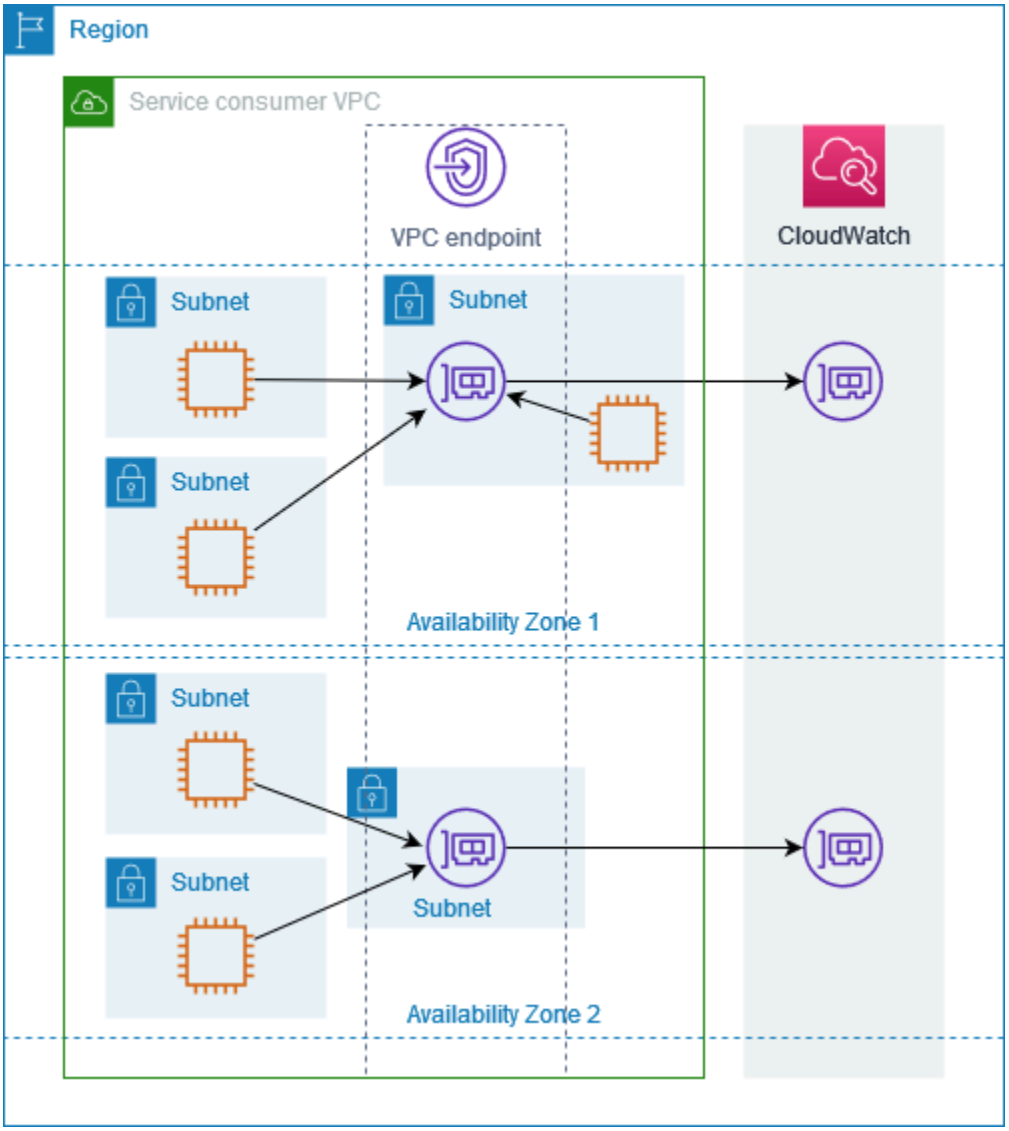
Le schéma suivant montre un point de terminaison VPC pour Amazon CloudWatch avec une interface réseau de point de terminaison dans une seule zone de disponibilité. Lorsqu'une ressource d'un sous-réseau du VPC accède à CloudWatch Amazon via son point de terminaison public, nous résolvons le trafic vers 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 point de terminaison VPC pour Amazon CloudWatch avec des interfaces réseau de points de terminaison dans deux zones de disponibilité. Lorsqu'une ressource d'un sous-réseau du VPC accède à CloudWatch Amazon 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 prendre en charge l'IPv6 via leurs points de terminaison privés même s'ils ne prennent pas en charge l'IPv6 via leurs points de terminaison publics. Les points de terminaison qui prennent en charge IPv6 peuvent répondre aux requêtes DNS avec des enregistrements AAAA.

Exigences pour activer IPv6 pour un point de terminaison d'interface

- Le Service AWS doit rendre ses points de terminaison de service disponibles via IPv6. Pour plus d'informations, consultez the section called “Afficher la prise charge d'IPv6”.
- 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 des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4.
- IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
- Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.

Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv4, les interfaces réseau du point de terminaison possèdent des adresses IPv4. Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv6, les interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de terminaison est inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, remarquez que `denyAllIgwTraffic` est activé.

Services AWS qui s'intègrent à AWS PrivateLink

Les éléments suivants Services AWS s'intègrent à AWS PrivateLink. Vous pouvez créer un point de terminaison de VPC pour vous connecter à ces services de manière privée, comme s'ils étaient exécutés dans votre propre VPC.

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 terminaison VPC 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-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig

Service AWS	Nom du service
	com.amazonaws.*region*.appconfigdata
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 Auto Scaling	com.amazonaws.*region*.application-autoscaling
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*.athena
AWS Audit Manager	com.amazonaws.*region*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS Échange de données B2B	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*region*.bedrock
	com.amazonaws. *région .bedrock-agent*

Service AWS	Nom du service
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-runtime
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.brakett
AWS Clean Rooms	com.amazonaws.*region*.cleanrooms
AWS Clean Rooms ML	com.amazonaws. *région .cleanrooms-ml*
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
AWS CloudHSM	com.amazonaws.*region*.cloudhsmv2
AWS Cloud Map	com.amazonaws.*region*.servicediscovery
	com.amazonaws.*region*.servicediscovery-fips
	com.amazonaws.*region*.data-servicediscovery
	com.amazonaws.*region*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*.cloudtrail
Amazon CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum

Service AWS	Nom du service
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
Amazon CloudWatch Network Monitor	com.amazonaws. *region* *.networkmonitor*
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws.*region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws. *région* *.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*.codeguru-profiler
CodeGuru Réviseur Amazon	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*region*.codewhisperer

Service AWS	Nom du service
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Config	com.amazonaws.*region*.config
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws. *région*.cases
	com.amazonaws.*region*.connect-campaigns
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
AWS Catalogue de contrôle	com.amazonaws. *region .controlcatalog*
AWS Data Exchange	com.amazonaws.*region*.dataexchange
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*.datasync
Amazon DataZone	com.amazonaws.*region*.datazone
AWS Deadline Cloud	com.amazonaws. *région .deadline* .management
	com.amazonaws. *région .deadline.scheduling*
Amazon DevOps Guru	com.amazonaws.*region*.devops-guru

Service AWS	Nom du service
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws. *région .dynamodb*
API directes Amazon EBS	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
EC2 Image Builder	com.amazonaws.*region*.imagebuilder
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-telemetry
Amazon EKS	com.amazonaws.*region*.eks
	com.amazonaws.*region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws.*region*.elasticbeanstalk
	com.amazonaws.*region*.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.*region*.drs
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing

Service AWS	Nom du service
Amazon ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*region*.elasticfilesystem-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR on EKS	com.amazonaws.*region*.emr-containers
Amazon EMR sans serveur	com.amazonaws.*region*.emr-serverless
Amazon EMR WAL	com.amazonaws. *région .emrwal.prod*
Résolution des entités AWS	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws. *région .pipes-data*
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips

Service AWS	Nom du service
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Amazon Managed Grafana	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana
AWS Ground Station	com.amazonaws.*region*.groundstation
Amazon GuardDuty	com.amazonaws.*region*.guardduty-data
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws. *région .dicom-medical-imaging*
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
AWS HealthOmics	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.storage-omics
IAM Identity Center	com.amazonaws.*region*.identitystore
Rôles Anywhere IAM	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data

Service AWS	Nom du service
	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*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws.*region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws.*region*.greengrass
AWS IoT RoboRunner	com.amazonaws.*region*.iotroborunner
AWS IoT SiteWise	com.amazonaws.*region*.iotsitewise.api
	com.amazonaws.*region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws.*region*.iottwinmaker.api
	com.amazonaws.*region*.iottwinmaker.data
Amazon Kendra	com.amazonaws.*region*.kendra
	aws.api.*region*.kendra-ranking
AWS Key Management Service	com.amazonaws.*region*.kms
	com.amazonaws.*region*.kms-fips
Amazon Keyspaces (pour Apache Cassandra)	com.amazonaws.*region*.cassandra
	com.amazonaws.*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams

Service AWS	Nom du service
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api

Service AWS	Nom du service
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB for Redis	com.amazonaws.*region*.memory-db
	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 Neptune Analytics	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
Amazon OpenSearch Service	Ces points de terminaison sont gérés par des services
AWS Organizations	com.amazonaws. *région* .organisations
	com.amazonaws. *région .organizations-fips*
AWS Outposts	com.amazonaws. *région .avant-postes*
AWS Panorama	com.amazonaws.*region*.panorama
AWS Cryptographie des paiements	com.amazonaws.*region*.payment-cryptography.controlplane
	com.amazonaws.*region*.payment-cryptography.dataplane

Service AWS	Nom du service
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime
AWS Supply Chain	com.amazonaws. *région .scn*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS 5G privée	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api. *région .qbusiness*
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws. *région .quicksight-website*
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS Data API	com.amazonaws.*region*.rds-data
AWS Re:Post Private	com.amazonaws. *région .repostspace*
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
API de données Amazon Redshift	com.amazonaws.*region*.redshift-data

Service AWS	Nom du service
	com.amazonaws. *région* .redshift-data-fips
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Amazon S3 Multi-Region Access Points	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts

Service AWS	Nom du service
Service Catalog	com.amazonaws.*region*.servicecatalog
	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*.states
	com.amazonaws.*region*.sync-states
AWS Storage Gateway	com.amazonaws.*region*.storagegateway
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS Générateur de réseaux de télécommunications	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips

Service AWS	Nom du service
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
Amazon Timestream pour InfluxDB	com.amazonaws. *région* .*timestream-influxdb*
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Thin Client	com.amazonaws. *région* .*thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

Voir les noms Service AWS disponibles

Vous pouvez utiliser la commande describe-vpc-endpoint-services pour afficher les noms de service qui prennent en charge les points de terminaison d'un VPC.

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 commande describe-vpc-endpoint-services 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 stratégies de point de terminaison, appelez la commande describe-vpc-endpoint-services 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",
    "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.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "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.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
```

```
    "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 la prise charge d'IPv6

Vous pouvez utiliser la commande describe-vpc-endpoint-services suivante pour afficher les informations Services AWS auxquelles vous pouvez accéder via 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.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

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

Vous pouvez créer un point de terminaison VPC 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 votre VPC, 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 de 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 y accéderont Service AWS dans votre VPC.
- Pour utiliser le système DNS privé, vous devez activer les noms d'hôte DNS et la résolution DNS pour votre VPC. Pour plus d'informations, voir Affichage et mise à jour des attributs DNS dans le Guide de l'utilisateur Amazon VPC.
- Pour activer IPv6 pour un point de terminaison d'interface, celui-ci Service AWS doit prendre en charge l'accès via IPv6. Pour plus d’informations, consultez 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 votre VPC. Par exemple, pour s'assurer qu'il AWS CLI peut envoyer des requêtes HTTPS au Service AWS, le groupe de sécurité doit autoriser le trafic HTTPS entrant.

- Si vos ressources se trouvent dans un sous-réseau doté d'une ACL réseau, vérifiez que l'ACL réseau autorise le trafic entre les ressources de votre VPC et les interfaces réseau des points de terminaison.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour plus d'informations, consultez AWS PrivateLink quotas.

Création d'un point de terminaison de VPC

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

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

1. Ouvrez la console Amazon VPC 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 Service name (Nom du service), sélectionnez le service. Pour plus d'informations, consultez the section called "Services qui s'intègrent".
6. Pour VPC, sélectionnez le VPC à partir duquel vous allez accéder au Service AWS.
7. Si, à l'étape 5, vous avez sélectionné le nom de service pour Amazon S3 et si vous souhaitez configurer la prise en charge du DNS privé, sélectionnez Paramètres supplémentaires, Activer le nom DNS. Lorsque vous effectuez cette sélection, elle sélectionne également automatiquement Activer le DNS privé uniquement pour un point de terminaison entrant. Vous pouvez configurer un DNS privé avec un point de terminaison Resolver 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 DNS privé uniquement pour le point de terminaison entrant, vous recevrez un message d'erreur lorsque vous tenterez la dernière étape 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 le nom DNS 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 point de terminaison VPC.

8. Pour Subnets (Sous-réseaux), sélectionnez un seul sous-réseau par zone de disponibilité à partir duquel vous accéderez au Service AWS. Il n'est pas possible de sélectionner plusieurs sous-réseaux dans la même zone de disponibilité. Pour plus d'informations, consultez the section called “Sous-réseaux et zones de disponibilité”.

   Nous créons une interface réseau du point de terminaison dans chaque sous-réseau que vous sélectionnez. 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 Designate IP addresses et entrez une adresse IPv4 à partir de la plage d'adresses de sous-réseau. Si le service de point de terminaison prend en charge le protocole IPv6, vous pouvez également saisir une adresse IPv6 à partir de la plage d'adresses de sous-réseau. Notez que les quatre premières adresses IP et la dernière adresse IP d'un bloc CIDR 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 des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et que le service accepte les requêtes IPv4.
   - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 et que le service accepte les requêtes IPv6.
   - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6 et que le service accepte les requêtes IPv4 et IPv6.

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

11. Pour Policy (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, sélectionnez Custom (Personnalisé) pour joindre une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC. Cette option n'est disponible que si le service

prend en charge les politiques de points de terminaison de VPC. Pour plus d'informations, consultez 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 points de terminaison d'un VPC dans des sous-réseaux qui sont partagés avec vous. Toutefois, vous pouvez utiliser les points de terminaison d'un VPC dans les sous-réseaux qui sont partagés avec vous.

Configuration d'un point de terminaison d'interface

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

Tâches

- Ajouter ou supprimer des sous-réseaux
- Association de groupes de sécurité
- Pour modifier la politique de point de terminaison de VPC
- Activation de noms DNS 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 plus d'informations, consultez the section called "Sous-réseaux et zones de disponibilité".

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

1. Ouvrez la console Amazon VPC 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 Designate IP addresses et entrez une adresse IPv4 à partir de la plage d'adresses de sous-réseau. Si le service de point de terminaison prend en charge le protocole IPv6, vous pouvez également saisir une adresse IPv6 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 terminaison d'un VPC, nous remplaçons l'interface réseau de point de terminaison par une nouvelle. Ce processus déconnecte temporairement le sous-réseau et le point de terminaison d'un 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 de point de terminaison à partir des ressources de votre VPC.

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

1. Ouvrez la console Amazon VPC 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)

Pour modifier la politique de point de terminaison de VPC

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 plus d'informations, consultez Politiques de point de terminaison.

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

1. Ouvrez la console Amazon VPC 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 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)

Activation de noms DNS privés

Nous vous recommandons d'activer les noms DNS privés pour vos points de terminaison VPC 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 point de terminaison VPC.

Pour utiliser des noms DNS privés, vous devez activer à la fois les noms d'hôte DNS et la résolution DNS pour votre VPC. Après avoir activé les noms DNS privés, quelques minutes peuvent s'écouler avant que les adresses IP privées ne soient disponibles. Les enregistrements DNS que nous créons lorsque vous activez les noms DNS privés sont privés. Le nom DNS privé n'est donc pas résoluble publiquement.

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

1. Ouvrez la console Amazon VPC 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, Modify private DNS name (Modifier le nom DNS 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, si vous avez sélectionné Activer pour ce point de terminaison à l'étape précédente, sélectionnez également Activer le DNS privé uniquement pour un point de terminaison entrant. Si vous préférez la fonctionnalité DNS privée standard, désactivez l'option Activer le DNS privé uniquement pour un 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 DNS privé uniquement pour un point de terminaison entrant, vous recevrez un message d'erreur lorsque vous enregistrerez les modifications à l'étape suivante. Pour plus d’informations, consultez the section called “DNS privé”.
7. Choisissez Enregistrer les modifications.

Pour modifier l'option des noms DNS 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 console Amazon VPC 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 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 notification SNS
- Ajout d'une stratégie d'accès
- Ajout d'une stratégie de clé

Création d'une notification SNS

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

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

1. Ouvrez la console Amazon VPC 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 (ARN de notification), choisissez l'ARN de la rubrique SNS que vous avez créée.
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 rubrique Amazon SNS qui permet de AWS PrivateLink publier des notifications en votre nom, comme la suivante. Pour plus d'informations, voir Comment modifier la stratégie d'accès à ma rubrique Amazon SNS ? 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 rubriques SNS chiffrées, la politique de ressources de la clé KMS doit être fiable AWS PrivateLink pour appeler des opérations d' AWS KMS API. 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 avec un point de terminaison de VPC, 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 console Amazon VPC 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, Delete VPC endpoints (Supprimer le point de terminaison de VPC).
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

Les points de terminaison d'un VPC de passerelle fournissent une connectivité fiable à Amazon S3 et DynamoDB sans nécessiter de passerelle Internet ou d'appareil NAT pour votre VPC. Les points de terminaison de passerelle ne sont pas utilisés AWS PrivateLink, contrairement aux autres types de points de terminaison VPC.

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

Tarification

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

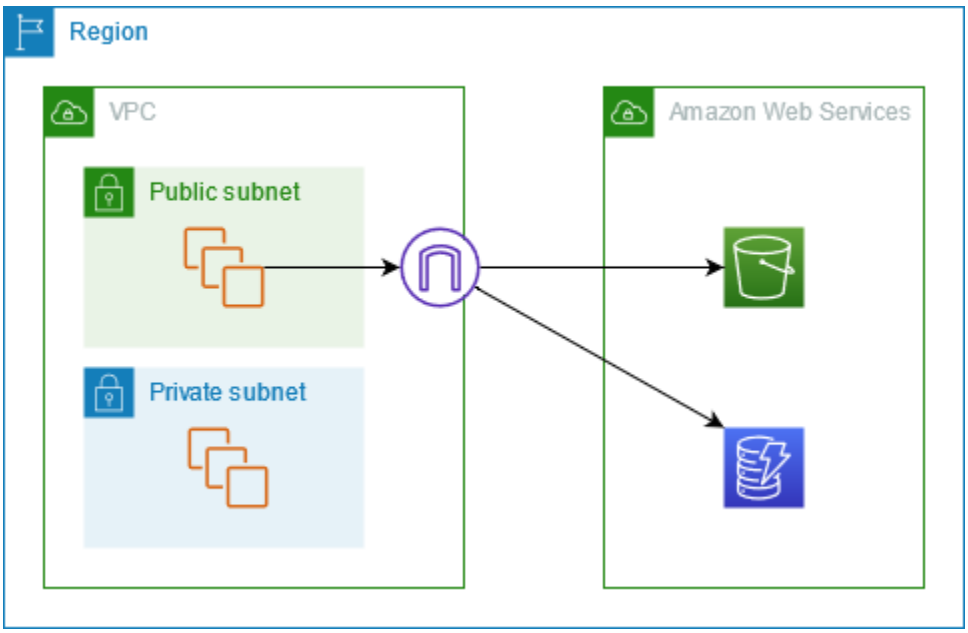
Table des matières

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.

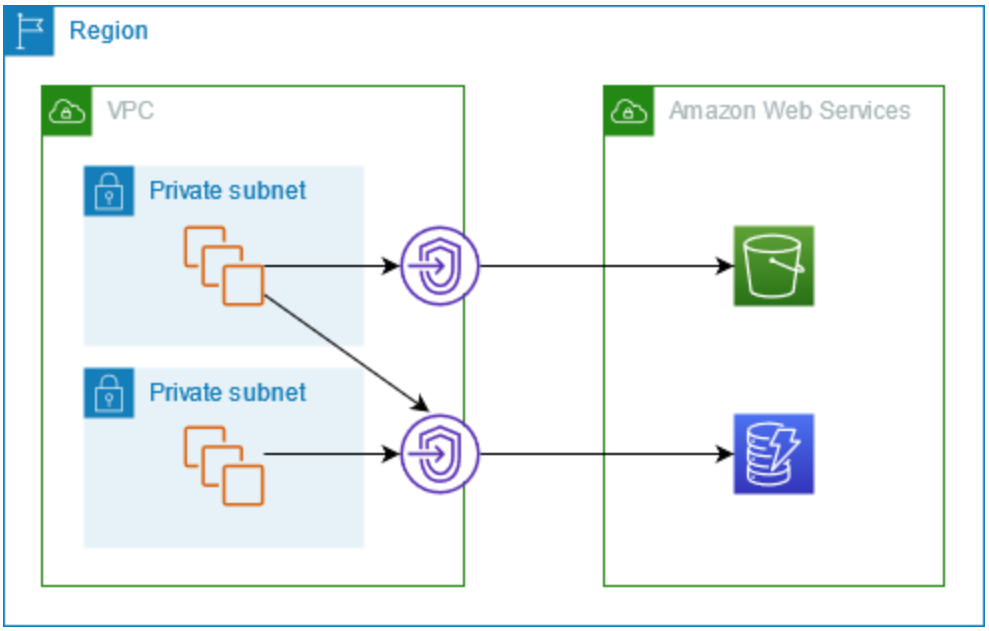
Accès via une passerelle Internet

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 à partir d'une instance d'un sous-réseau public est acheminé vers la passerelle Internet du VPC, puis vers 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 un appareil NAT 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 VPC vers Amazon S3 ou DynamoDB est acheminé vers le point de terminaison de 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 préfixes gérés par AWS dans le Guide de l'utilisateur Amazon VPC.



Routage

Lorsque vous créez un point de terminaison de passerelle, vous sélectionnez les tables de routage VPC des 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

Les ACL réseau pour les sous-réseaux de ces instances doivent également autoriser le trafic à destination et en provenance du service. Voici un exemple de règle sortante. Vous ne pouvez pas référencer les listes de préfixes dans les règles ACL 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 votre VPC en utilisant les points de terminaison de VPC de passerelle. Après avoir créé le point de terminaison de passerelle, vous pouvez l'ajouter comme cible dans votre table de routage pour le trafic destiné à Amazon S3 depuis votre VPC.

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 d'une passerelle, vous pouvez accéder à Amazon S3 à partir de votre VPC sans avoir besoin d'une passerelle Internet ou d'un périphérique NAT pour votre VPC et sans frais supplémentaires. Toutefois, les points de terminaison de passerelle n'autorisent pas l'accès depuis des réseaux locaux, depuis des VPC homologues 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 de plus amples informations, veuillez consulter Types de points de terminaison d'un VPC pour Amazon S3 dans le Guide de l'utilisateur 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 serveurs DNS d'Amazon, vous devez activer à la fois les noms d'hôte DNS et la résolution DNS pour votre VPC. Si vous utilisez votre propre serveur DNS, assurez-vous que les requêtes vers Amazon S3 se résolvent correctement en 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.
- L'ACL réseau du sous-réseau pour vos 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 ne pouvez pas référencer les listes de préfixes dans les règles ACL réseau, mais vous pouvez obtenir les plages d'adresses IP pour Amazon S3 à partir de la liste de préfixes pour Amazon S3.

- Vérifiez si vous utilisez un système Service AWS qui nécessite l'accès à un compartiment S3. Par exemple, un service peut avoir besoin d'accéder à des compartiments contenant des fichiers journaux ou vous demander de télécharger des pilotes ou des agents sur vos instances EC2. 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 la condition `aws:SourceIp` dans une stratégie d'identité ou une stratégie de compartiment pour les demandes adressées à Amazon S3 qui traversent un point de terminaison d'un VPC. Utilisez à la place la condition `aws:VpcSourceIp`. Vous pouvez également utiliser des tables de routage pour contrôler quelles instances EC2 peuvent accéder à Amazon S3 via le point de terminaison d'un VPC.
- Les points de terminaison de passerelle ne prennent en charge que le trafic IPv4.
- Les adresses IPv4 source des instances de vos sous-réseaux concernés, telles que reçues par Amazon S3, vont passer du statut d’adresses IPv4 publiques à celui d’adresses IPv4 privées dans votre VPC. Un point de terminaison change de routes réseau et déconnecte les connexions TCP ouvertes. Les connexions précédentes qui utilisaient des adresses IPv4 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 de point de terminaison ne peuvent être étendues à l'extérieur d'un VPC. Les ressources situées de l'autre côté d'une connexion VPN, d'une connexion d'appairage VPC, d'une passerelle de transit ou d'une AWS Direct Connect connexion dans votre 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 y a également une limite de 255 points de terminaison de passerelle par VPC.

DNS privé

Vous pouvez configurer un DNS privé afin d'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.

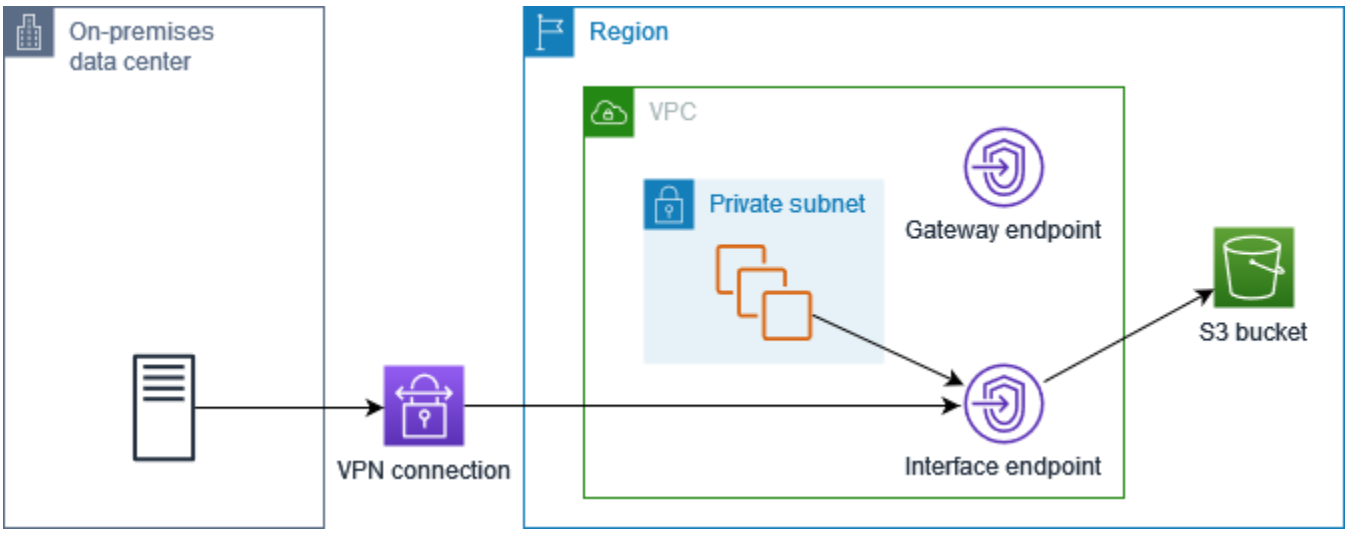
Route 53 Resolver

Amazon fournit un serveur DNS pour votre VPC, appelé Route 53 Resolver. Route 53 Resolver résout automatiquement les noms de domaine VPC locaux et enregistre dans des zones hébergées privées. Toutefois, vous ne pouvez pas utiliser Route 53 Resolver en dehors de votre VPC. Route 53 fournit des points de terminaison Resolver et des règles Resolver afin que vous puissiez utiliser Route 53 Resolver en dehors de votre VPC. Un point de terminaison Resolver entrant réachemine des requêtes DNS à partir du réseau sur site vers Route 53 Resolver. Un point de terminaison Resolver sortant réachemine des requêtes DNS à partir de Route 53 Resolver vers le réseau sur site.

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

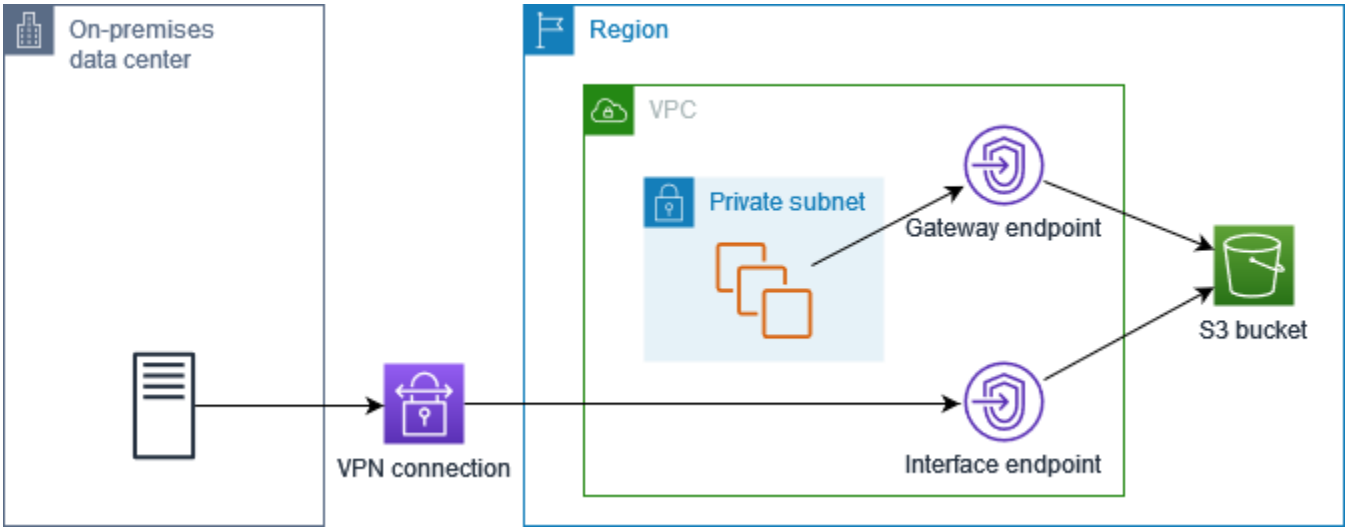
DNS privé

Si vous configurez un DNS privé pour votre point de terminaison d'interface pour Amazon S3 mais que vous ne configurez pas un DNS privé uniquement pour le point de terminaison Resolver entrant, les demandes provenant de votre réseau sur site et de votre VPC utilisent le point de terminaison d'interface pour accéder à Amazon S3. Par conséquent, vous payez pour utiliser le point de terminaison d'interface pour le trafic provenant du VPC au lieu d'utiliser le point de terminaison de passerelle sans frais supplémentaires.



DNS privé uniquement pour le point de terminaison Resolver entrant

Si vous configurez un DNS privé uniquement pour le point de terminaison Resolver entrant, les demandes provenant de votre réseau sur site utilisent le point de terminaison d'interface pour accéder à Amazon S3 et les demandes de votre 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 un DNS privé

Vous pouvez configurer un DNS privé 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 de VPC” (configurer pendant la création) ou the section called “Activation de noms DNS 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 console Amazon VPC 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. *région* s.3.

6. Pour VPC, sélectionnez le VPC dans lequel 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 (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, sélectionnez Custom (Personnalisé) pour joindre une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC.
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, de VPC, 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 en utilisant la clé de condition aws:sourceVpce. 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 : restriction de l'accès à un VPC spécifique

Vous pouvez créer une politique de compartiment qui restreint l'accès à des VPC spécifiques en utilisant la clé de condition aws:sourceVpc. Ceci est utile si vous avez plusieurs points de terminaison configurés dans le même VPC. La politique suivante refuse l'accès au compartiment spécifié à l'aide des actions spécifiées à moins que la demande ne provienne du VPC spécifié. 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 condition aws : VpcSource Ip. 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 console Amazon VPC 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)

Pour modifier la politique de point de terminaison de VPC

Vous pouvez modifier la politique de point de terminaison pour un point de terminaison de passerelle, qui contrôle l'accès à Amazon S3 depuis le VPC via le point de terminaison. La politique par défaut permet un accès complet. Pour plus d'informations, consultez Politiques de point de terminaison.

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

1. Ouvrez la console Amazon VPC 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 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. Cela est utile si d'autres compartiments Services AWS de votre VPC 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 : restriction de l'accès à un rôle IAM spécifique

Vous pouvez créer une politique qui restreint l'accès à un rôle IAM 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 DNS privé est activé.

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

1. Ouvrez la console Amazon VPC 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, Delete VPC endpoints (Supprimer le point de terminaison de VPC).
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 à partir de votre VPC à l'aide de points de terminaison de VPC de passerelle. Après avoir créé le point de terminaison de passerelle, vous pouvez l'ajouter comme cible dans votre table de routage pour le trafic destiné à DynamoDB depuis votre VPC.

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 de passerelle, vous pouvez accéder à DynamoDB depuis votre VPC, sans avoir besoin d'une passerelle Internet ou d'un périphérique NAT pour votre VPC, et sans frais supplémentaires. Toutefois, les points de terminaison de passerelle

n'autorisent pas l'accès depuis des réseaux locaux, depuis des VPC homologues 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 points de terminaison VPC 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 serveurs DNS d'Amazon, vous devez activer à la fois les noms d'hôte DNS et la résolution DNS pour votre VPC. Si vous utilisez votre propre serveur DNS, assurez-vous que les requêtes vers DynamoDB se résolvent correctement en 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.
- L'ACL réseau du sous-réseau pour vos instances qui accèdent à DynamoDB par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination de DynamoDB. Vous ne pouvez pas référencer les listes de préfixes dans les règles ACL réseau, mais vous pouvez obtenir les plages d'adresses IP pour DynamoDB à partir de la liste de préfixes pour DynamoDB.
- Si vous enregistrez les AWS CloudTrail opérations DynamoDB, les fichiers journaux contiennent les adresses IP privées des instances EC2 du VPC du consommateur de services et l'ID du point de terminaison de la passerelle pour toutes les demandes effectuées via le point de terminaison.

- Les points de terminaison de passerelle ne prennent en charge que le trafic IPv4.
- Les adresses IPv4 source des instances de vos sous-réseaux concernés passent d'adresses IPv4 publiques à adresses IPv4 privées de votre VPC. Un point de terminaison change de routes réseau et déconnecte les connexions TCP ouvertes. Les connexions précédentes qui utilisaient des adresses IPv4 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 de point de terminaison ne peuvent être étendues à l'extérieur d'un VPC. Les ressources situées de l'autre côté d'une connexion VPN, d'une connexion d'appairage VPC, d'une passerelle de transit ou d'une connexion au sein de votre VPC ne peuvent pas utiliser un point de terminaison de passerelle pour communiquer AWS Direct Connect avec DynamoDB.
- Votre compte dispose d'un quota par défaut de 20 points de terminaison de passerelle par Région, qui est réglable. Il y a 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 console Amazon VPC 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. *région* .dynamodb.
6. Pour VPC, sélectionnez le VPC dans lequel 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 (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, sélectionnez Custom (Personnalisé) pour joindre une politique de point de terminaison de

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

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 IAM

Vous pouvez créer des politiques IAM pour contrôler les principaux IAM qui peuvent accéder aux tables DynamoDB en utilisant un point de terminaison de VPC spécifique.

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 terminaison de VPC spécifique en utilisant la clé de condition aws:sourceVpce. La politique suivante refuse l'accès aux tables DynamoDB du compte, sauf si le point de terminaison de 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",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
```

```
}
```

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

Vous pouvez créer une politique qui autorise l'accès à un rôle IAM spécifique. La politique suivante donne accès au rôle IAM 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 console Amazon VPC 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)

Pour modifier la politique de point de terminaison de VPC

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

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

1. Ouvrez la console Amazon VPC 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 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 console Amazon VPC 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, Delete VPC endpoints (Supprimer le point de terminaison de VPC).
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 dans votre propre VPC.

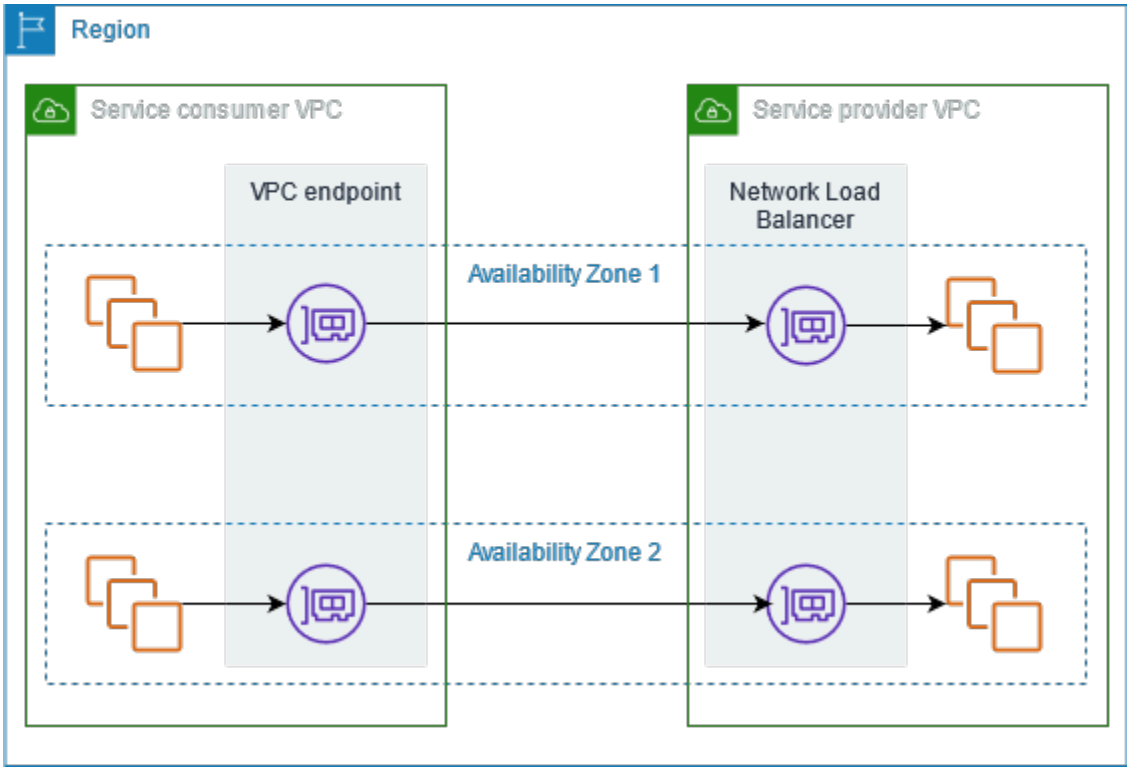
Table des matières

Présentation

Vous pouvez découvrir, acheter et fournir des produits SaaS optimisés par le AWS PrivateLink biais de AWS Marketplace. Pour plus d'informations, voir AWS Marketplace: - PrivateLink.

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 utiliser des points de terminaison de VPC pour vous connecter à des 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 du service, vous créez un point de terminaison de VPC d'interface, qui établit des connexions entre un ou plusieurs sous-réseaux de votre VPC et le service de point de terminaison.



Création d'un point de terminaison d'interface

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

Exigence

Abonnez-vous au service.

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

1. Ouvrez la console Amazon VPC 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. Pour Service category (Catégorie de service), choisissez Services AWS Marketplace .
   b. Saisissez le nom du service.
5. Si vous êtes abonné à un service portant la désignation AWS Service Ready, procédez comme suit :

   a. Pour la catégorie de service, sélectionnez PrivateLink Ready partner services.
   b. Saisissez le nom du service et choisissez Verify service (Vérifier le service).
6. Pour VPC, sélectionnez le VPC à partir duquel vous allez accéder au produit.
7. Pour Subnets (Sous-réseaux), sélectionnez un seul sous-réseau par zone de disponibilité à partir duquel vous accéderez au produit.
8. Pour Groupe 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 du VPC et les interfaces réseau 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 l'équilibreur de charge de passerelle lorsque vous créez un service de point de terminaison d'un VPC. 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 Tarification d'AWS PrivateLink.

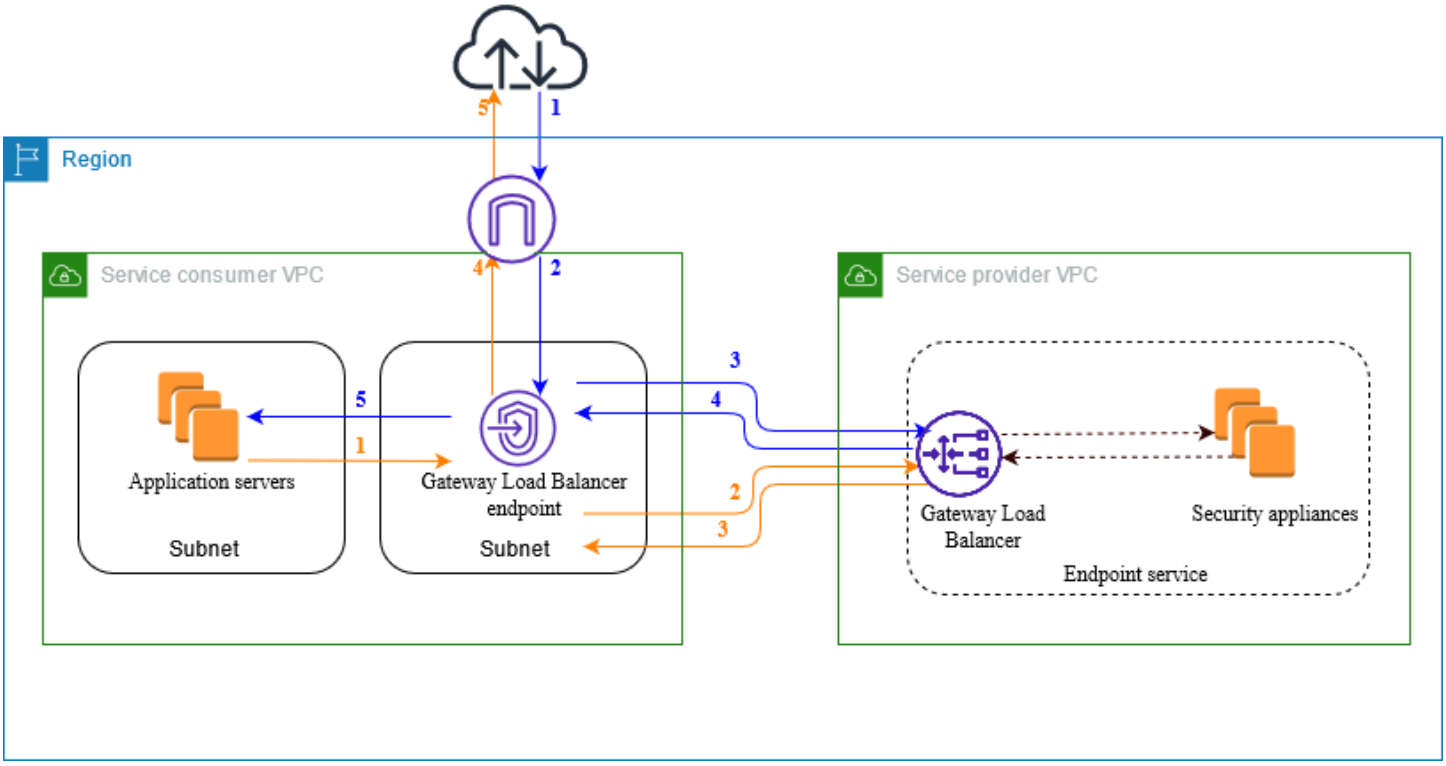
Table des matières

Pour plus d'informations, consultez Gateway Load Balancers.

Présentation

Le schéma suivant montre comment les serveurs d'applications accèdent aux dispositifs de sécurité via AWS PrivateLink. Les serveurs d'applications s'exécutent dans un sous-réseau du VPC du consommateur du service. Vous créez un point de terminaison d'équilibreur de charge de passerelle dans un autre sous-réseau du même VPC. Tout le trafic entrant dans le VPC du consommateur du service par la passerelle Internet est d'abord acheminé vers le point de terminaison d'équilibreur de charge de passerelle 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 VPC du consommateur du service 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 du service peuvent mettre leurs points de terminaison à la disposition des consommateurs du service sur IPv4, IPv6 ou IPv4 et IPv6, même si leurs appareils de sécurité ne prennent en charge qu'IPv4. Si vous activez le support dualstack, les consommateurs existants peuvent continuer à utiliser le protocole IPv4 pour accéder à votre service et les nouveaux consommateurs peuvent choisir d'utiliser le protocole IPv6 pour accéder à votre service.

Si le point de terminaison équilibreur de charge de Passerelle prend en charge le protocole IPv4, les interfaces réseau du point de terminaison possèdent des adresses IPv4. Si le point de terminaison équilibreur de charge de Passerelle prend en charge le protocole IPv6, les interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de terminaison est inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, remarquez que `denyAllIgwTraffic` est activé.

Exigences pour activer IPv6 pour un service de point de terminaison

- Le VPC et les sous-réseaux du service de point de terminaison doivent être associés à des blocs CIDR IPv6.
- 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 le trafic IPv6.

Exigences pour activer IPv6 pour un point de terminaison Gateway Load Balancer

- Le service de point de terminaison doit avoir un type d'adresse IP prenant en charge le protocole IPv6.

- 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 des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4.
  - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
  - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.
- Les tables de routage des sous-réseaux du VPC consommateur de services doivent acheminer le trafic IPv6 et les ACL réseau de ces sous-réseaux doivent autoriser le trafic IPv6.

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 les routages IPv6 sont inclus pour une configuration dualstack.

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	Cible
CIDR IPv4 VPC	Local
CIDR IPv6 VPC	Local
Sous-réseau d'application CIDR IPv4	*vpc-endpoint-id*

Destination	Cible
Sous-réseau d'application CIDR IPv6	*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	Cible
CIDR IPv4 VPC	Local
CIDR IPv6 VPC	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	Cible
CIDR IPv4 VPC	Local
CIDR IPv6 VPC	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 les identifiants AZ pour identifier de manière cohérente les zones de disponibilité de votre service. Pour plus d'informations, consultez la section AZ IDs dans le guide de l'utilisateur Amazon EC2.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour plus d’informations, consultez AWS PrivateLink quotas.

Prérequis

- Créez un VPC de fournisseur du service 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 équilibreur de charge de passerelle dans le VPC de votre fournisseur du service. Si vous envisagez d'activer la prise en charge d'IPv6 sur votre service de point de terminaison, vous devez activer la prise en charge de la technologie dualstack sur votre équilibreur de charge de passerelle. Pour plus d'informations, veuillez consulter Mise en route des équilibreurs de charge de passerelle.
- Lancez les dispositifs de sécurité dans le VPC du fournisseur du service et enregistrez-les dans 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 console Amazon VPC 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 :

   - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.

- Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
- Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.

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.

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 plus d'informations, consultez 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 plus d'informations, consultez 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 votre VPC, 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 de 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

Considérations

- Vous ne pouvez choisir qu'une seule zone de disponibilité dans le VPC du consommateur du service. 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 les identifiants AZ pour identifier de manière cohérente les

zones de disponibilité de votre service. Pour plus d'informations, consultez la section AZ IDs dans le guide de l'utilisateur Amazon EC2.

- Pour pouvoir utiliser le service de point de terminaison, le fournisseur du service doit accepter les demandes de connexion. Le service ne peut pas lancer de requêtes vers les ressources de votre VPC via le point de terminaison de VPC. Le point de terminaison ne renvoie que les réponses au trafic initié par les ressources de votre VPC.
- 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 d'équilibreur de charge de passerelle, même si la cible se trouve dans le même VPC que le Network Load Balancer.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour plus d'informations, consultez AWS PrivateLink quotas.

Prérequis

- Créez un VPC de consommateur du service avec au moins deux sous-réseaux dans la zone de disponibilité à partir de laquelle vous accéderez 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 les zones de disponibilité 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 commande describe-vpc-endpoint-services.
- Si vos ressources se trouvent dans un sous-réseau doté d'une liste de contrôle d'accès (ACL, Access Control List) réseau, vérifiez que cette dernière autorise le trafic entre les interfaces réseau du point de terminaison et les ressources du VPC.

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 console Amazon VPC 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 Other endpoint services (Autres services de point de terminaison).
5. Pour Service Name (Nom du service), saisissez le nom du service et choisissez Verify service (Vérifier le service).
6. Pour VPC, sélectionnez le VPC dans lequel créer le point de terminaison.
7. Pour Subnets (Sous-réseau), sélectionnez le sous-réseau dans lequel créer le point de terminaison.
8. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
   - IPv4 – Attribuez des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4.
   - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
   - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.
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 VPC du consommateur du service. Cela permet aux dispositifs de sécurité d'effectuer une inspection de sécurité du trafic entrant destiné aux serveurs d'applications. Pour plus d'informations, consultez the section called “Routage”.

Pour configurer le routage à l'aide de la console

1. Ouvrez la console Amazon VPC 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 compatible avec IPv4, choisissez Add route (Ajouter un itinéraire). Pour Destination, entrez le bloc CIDR IPv4 du sous-réseau pour les serveurs d'applications. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
   c. Si vous prenez en charge IPv6, choisissez Add route (Ajouter un itinéraire). Pour Destination, entrez le bloc CIDR IPv6 du sous-réseau pour les serveurs d'applications. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
   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 prenez en charge IPv4, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez **`0.0.0.0/0`**. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
   c. Si vous prenez en charge IPv6, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez **`::/0`**. Pour Target (Cible), sélectionnez le point de terminaison de VPC.
   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 prenez en charge IPv4, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez **`0.0.0.0/0`**. Pour Target (Cible), sélectionnez la passerelle Internet.

   c. Si vous prenez en charge IPv6, choisissez Add route (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 console Amazon VPC 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 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 console Amazon VPC 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)

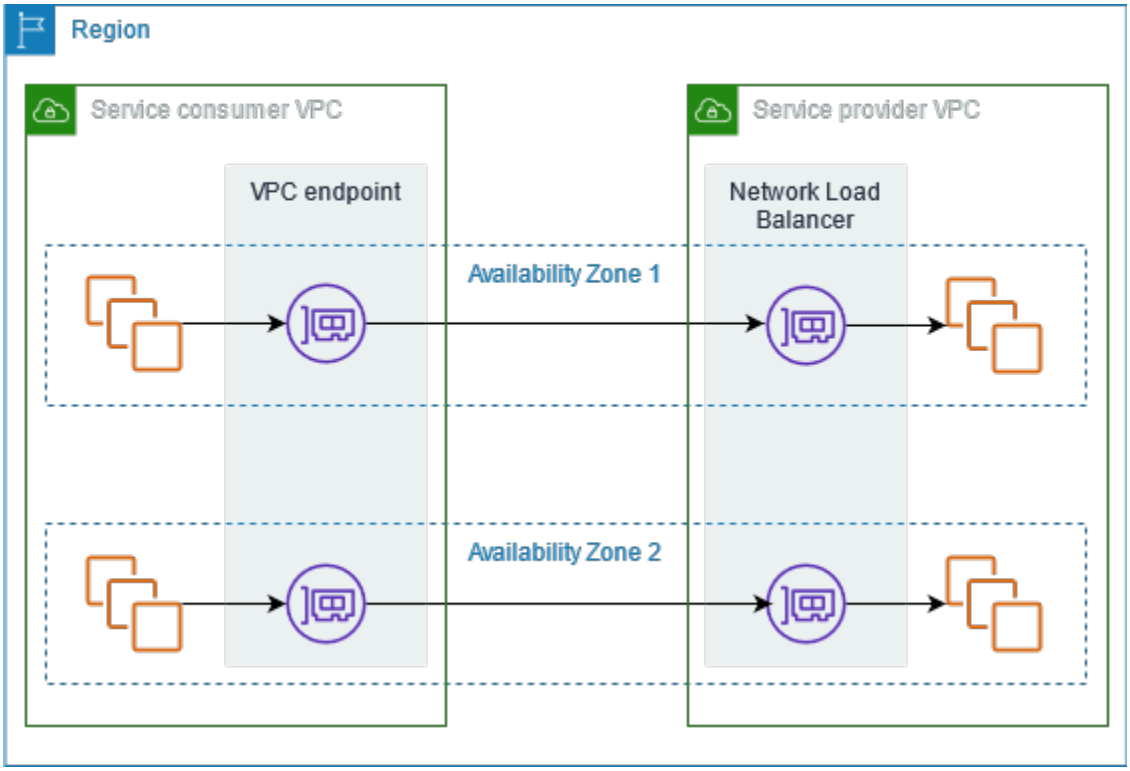
Partagez vos services via AWS PrivateLink

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 du service, vous créez un Network Load Balancer (équilibreur de charge de réseau) dans votre VPC comme frontal du service. Vous sélectionnez ensuite cet équilibreur de charge lorsque vous configurez le service de point de terminaison d'un VPC. Vous accordez l'autorisation à des principaux AWS spécifiques afin qu'ils puissent se connecter à votre service. En tant que consommateur du service, le client crée un point de terminaison d'un VPC d'interface, qui établit des connexions entre les sous-réseaux qu'il sélectionne dans son VPC et 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.

Noms d'hôte DNS

Lorsqu'un fournisseur de services crée un service de point de terminaison VPC, il AWS génère un nom d'hôte DNS 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 nom d'hôte DNS pour un service de point de terminaison d'un VPC dans la Région us-east-2 :

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

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

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

Les noms zonaux ont la syntaxe suivante :

```
endpoint_id-zone.endpoint_service_id.region.vpce.amazonaws.com
```

DNS privé

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

Types d'adresses IP

Les fournisseurs du service peuvent mettre leurs points de terminaison à la disposition des consommateurs du service sur IPv4, IPv6 ou IPv4 et IPv6, même si leurs serveurs backend ne prennent en charge qu'IPv4. Si vous activez le support dualstack, les consommateurs existants peuvent continuer à utiliser le protocole IPv4 pour accéder à votre service et les nouveaux consommateurs peuvent choisir d'utiliser le protocole IPv6 pour accéder à votre service.

Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv4, les interfaces réseau du point de terminaison possèdent des adresses IPv4. Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv6, les interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de terminaison est inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, remarquez que `denyAllIgwTraffic` est activé.

Exigences pour activer IPv6 pour un service de point de terminaison

- Le VPC et les sous-réseaux du service de point de terminaison doivent être associés à des blocs CIDR IPv6.

- 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 le trafic IPv6. Si le service traite les adresses IP sources à partir de l'en-tête du protocole proxy version 2, il doit traiter les adresses IPv6.

Exigences pour activer IPv6 pour un point de terminaison d'interface

- Le service de point de terminaison doit prendre en charge les requêtes IPv6.
- 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 des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4.
  - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
  - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.

Type d'adresse IP d'enregistrement DNS pour un point de terminaison d'interface

Le type d'adresse IP d'enregistrement DNS pris en charge par un point de terminaison d'interface détermine les enregistrements DNS que nous créons. Le type d'adresse IP de l'enregistrement DNS 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 noms DNS privés, régionaux et zonaux. Le type d'adresse IP doit être IPv4 ou Dualstack.
- IPv6 – Créez des enregistrements AAAA pour les noms DNS privés, régionaux et zonaux. Le type d'adresse IP doit être IPv6 ou Dualstack.
- Dualstack – Créez des enregistrements A et AAAA pour les noms DNS privés, régionaux et 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. Vous pouvez accéder au service de point de terminaison à partir d'autres Régions en utilisant l'appairage VPC.
- Le service de point de terminaison ne prend en charge que le trafic sur TCP.
- 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 les identifiants AZ pour identifier de manière cohérente les zones de disponibilité de votre service. Pour plus d'informations, consultez la section AZ IDs dans le guide de l'utilisateur Amazon EC2.
- 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 du service et les ID des points de terminaison d'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.

- 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 plus d'informations, consultez AWS PrivateLink quotas.

Prérequis

- Créez un VPC pour votre service de point de terminaison avec au moins un sous-réseau dans chaque zone de disponibilité dans laquelle le service doit être disponible.
- Pour permettre aux consommateurs du service de créer des points de terminaison de VPC d'interface IPv6 pour votre service de terminaison, le VPC et les sous-réseaux doivent être associés à des blocs CIDR IPv6.
- Créez un équilibreur de charge de réseau 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 requêtes IPv6, ses équilibreurs de charge de réseau Network Load Balancer doivent utiliser le type d'adresse IP

dualstack. Les cibles n'ont pas besoin de prendre en charge le trafic IPv6. 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 les adresses IP sources à partir de l'en-tête du protocole de proxy version 2, vérifiez que vous pouvez traiter les adresses IPv6.

- 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 prendre en charge les consommateurs du service qui utilisent des noms d'hôte DNS 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 console Amazon VPC 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. Les zones de disponibilité incluses répertorient les zones de disponibilité activées pour les équilibreurs de charge réseau sélectionnés. Votre service de point de terminaison sera disponible dans ces zones de disponibilité.
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, ces requêtes sont acceptées automatiquement.
7. Pour Enable private DNS name (Activer le nom DNS privé), sélectionnez Associate a private DNS name with the service (Associer un nom DNS privé au service) pour associer un nom DNS

privé que les consommateurs du service peuvent utiliser pour accéder à votre service, puis saisissez le nom DNS privé. Dans le cas contraire, les consommateurs de services peuvent utiliser le nom DNS spécifique au point de terminaison fourni par. AWS Le fournisseur du service doit vérifier qu'il est le propriétaire du domaine de nom DNS privé pour que les consommateurs puissent utiliser le nom DNS privé. Pour plus d'informations, consultez Gestion des noms DNS.

8. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :

   - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.
   - Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
   - Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.

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.

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 terminaison VPC 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 plus d'informations, consultez 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, voir la procédure suivante.
- Acceptez la demande de connexion au point de terminaison de la part du consommateur du service. Pour plus d'informations, consultez 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 console Amazon VPC 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 Other endpoint services (Autres services de point de terminaison).
5. Pour Service name (Nom du service), saisissez le nom du service (par exemple, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) et choisissez Verify service (Vérifier le service).
6. Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
7. Pour Subnets (Sous-réseaux), sélectionnez les sous-réseaux (Zones de disponibilité) à partir desquels vous allez accéder au service de point de terminaison.
8. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :

    - IPv4 – Attribuez des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et que le service de point de terminaison accepte les requêtes IPv4.
    - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 et que le service de point de terminaison accepte les requêtes IPv6.
    - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option est prise en charge uniquement si tous les sous-réseaux

sélectionnés possèdent des plages d'adresses IPv4 et IPv6 et que le service de point de terminaison accepte les requêtes IPv4 et IPv6.

9. Dans DNS record IP type (Type d'IP d'enregistrement DNS), choisissez l'une des options suivantes :

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

10. Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
11. 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
- Association d'un nom DNS privé
- 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 permettent à des AWS principaux spécifiques de créer un point de terminaison VPC d'interface pour se connecter à votre service de point de terminaison. Pour ajouter des autorisations à un AWS principal, vous avez besoin de son Amazon Resource Name (ARN). La liste suivante inclut des exemples d’ARN pour les AWS principaux prises en charge.

ARN pour les directeurs AWS

Compte AWS (inclut tous les principaux du compte)

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

Rôle

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

Utilisateur

arn:aws:iam::*account_id*:user/*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 console Amazon VPC 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). Pour Principals to add (Principaux à ajouter), saisissez l'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-permissions (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.

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

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 rejetez une demande déjà acceptée, cela n'affecte pas la connexion entre le point de terminaison et le service.

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

1. Ouvrez la console Amazon VPC 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 console Amazon VPC 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-connections ou 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 depuis cette zone de disponibilité aux points de terminaison VPC 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 console Amazon VPC 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.

Association d'un nom DNS privé

Vous pouvez associer un nom DNS privé à votre service de point de terminaison. Après avoir associé un nom DNS privé, vous devez mettre à jour l'entrée pour le domaine sur votre serveur DNS. Le fournisseur du service doit vérifier qu'il est le propriétaire du domaine de nom DNS privé pour que les consommateurs puissent utiliser le nom DNS privé. Pour plus d'informations, consultez Gestion des noms DNS.

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

1. Ouvrez la console Amazon VPC 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, Modify private DNS name (Modifier le nom DNS privé).
5. Sélectionnez Associate a private DNS name with the service (Associer un nom DNS privé au service) et saisissez le nom DNS privé.

   - 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 nom DNS privé est prêt à être utilisé par les consommateurs du service lorsque l'état de vérification est verified (vérifié). Si l'état de vérification change, les nouvelles demandes de connexion sont refusées, mais les connexions existantes ne sont pas affectées.

Pour modifier un nom DNS 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 console Amazon VPC 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, Verify domain ownership for private DNS name (Vérifier la propriété du domaine pour le nom DNS 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)

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 requêtes IPv6, ses équilibreurs de charge de réseau Network Load Balancer doivent utiliser le type d'adresse IP dualstack. Les cibles n'ont pas besoin de prendre en charge le trafic IPv6. 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 console Amazon VPC 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 de VPC.
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 :
   - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.
   - Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
   - Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.
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 console Amazon VPC 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 de VPC.

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 Enregistrer.

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

1. Ouvrez la console Amazon VPC 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 d'un VPC, puis choisissez l'onglet Connexions au 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 Enregistrer.

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

1. Ouvrez la console Amazon VPC 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 d'un VPC, 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 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)

Gestion des noms DNS privés pour les services de point de terminaison de VPC

Les fournisseurs du service peuvent configurer des noms DNS privés pour leurs services de point de terminaison. Lorsqu'un fournisseur du service utilise un nom DNS public existant comme nom DNS privé pour son service de point de terminaison, les consommateurs du service n'ont pas besoin de modifier les applications qui utilisent le nom DNS public existant. Avant de pouvoir configurer un nom DNS privé pour votre service de point de terminaison, vous devez prouver que vous êtes propriétaire du domaine en procédant à une vérification de la propriété du domaine.

Considérations

- Un service de point de terminaison ne peut avoir qu'un seul nom DNS privé.
- Vous ne devez pas créer d'enregistrement A pour le nom DNS privé, afin que seuls les serveurs du VPC du consommateur du service puissent résoudre le nom DNS privé.
- Les noms DNS privés ne sont pas pris en charge pour les points de terminaison d'équilibreur de charge de passerelle.
- Pour vérifier un domaine, vous devez avoir un nom d'hôte public ou un fournisseur DNS public.
- Vous pouvez vérifier le domaine d'un sous-domaine. Par exemple, vous pouvez vérifier example.com, au lieu de a.example.com. Chaque étiquette DNS 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 maintenant b.example.com en tant que nom DNS privé. Vous devez vérifier example.com ou b.example.com pour que les consommateurs du service puissent utiliser le nom.

Vérification de la propriété du domaine

Votre domaine est associé à un ensemble d'enregistrements de service de nom de domaine (DNS) que vous gérez par l'intermédiaire de votre fournisseur DNS. Un enregistrement TXT est un type d'enregistrement DNS 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 enregistrement TXT au serveur DNS pour votre domaine public.

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

Après avoir ajouté un enregistrement, vous pouvez vérifier l'état du processus de vérification du domaine à l'aide de la console Amazon VPC. 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, Verify domain ownership for private DNS name (Vérifier la propriété du domaine pour le nom DNS privé).

Le nom DNS privé est prêt à être utilisé par les consommateurs du service lorsque l'état de vérification est verified (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 l'enregistrement TXT. 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 nom DNS 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 créez l'enregistrement TXT.

```
[
    {
        "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'enregistrement TXT.

Nom	Type	Valeur
_6e86v84tqgqubxbwi i1m.example.com	TXT	VPCE RxlTt : L6P0E 45JEVFwOCP

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 fournisseur DNS ne permet pas aux noms d'enregistrement DNS de contenir des traits de soulignement, vous pouvez omettre le « _6e86v84tqgqubxbwii1m » et utiliser simplement « 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 »).

Ajout d'un enregistrement TXT au serveur DNS de votre domaine

La procédure d'ajout d'enregistrements TXT au serveur DNS de votre domaine dépend de l'entité qui fournit votre service DNS. Votre fournisseur DNS 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 :

- Sous Record type (Type d'enregistrement), choisissez TXT.

- Pour TTL (seconds) (TTL [secondes]), saisissez **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 fournisseur DNS et connectez-vous à votre compte. Recherchez la page permettant de mettre à jour les enregistrements DNS de votre domaine. Ajoutez un enregistrement TXT avec le nom et la valeur que nous avons fournis. La mise à jour d'un enregistrement DNS peut prendre jusqu'à 48 heures, mais elle est souvent effective bien plus tôt.

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

Fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	Ajout d'un enregistrement TXT
Dreamhost	Ajout d'enregistrements DNS personnalisés
Cloudflare	Gestion des enregistrements DNS
HostGator	Gérer les enregistrements DNS avec HostGator /eNom
Namecheap	Comment ajouter des enregistrements TXT/SPF/DKIM/DMARC pour mon domaine ?
Names.co.uk	Modification des paramètres DNS du domaine
Wix	Ajout ou mise à jour des enregistrements TXT dans le compte Wix

Vérification de la publication de l'enregistrement TXT

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

Vous allez interroger les serveurs DNS qui desservent votre domaine, car ce sont eux qui contiennent le plus up-to-date d'informations sur votre domaine. La propagation des informations de votre domaine aux autres serveurs DNS prend du temps.

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

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'enregistrement TXT est correctement publié en utilisant la commande suivante, où *name_server* est l'un des serveurs de noms que vous avez trouvé 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 valeur TXT.

   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 fournisseur DNS autorise les traits de soulignement dans les noms d'enregistrements TXT. Si votre fournisseur DNS n'autorise pas les traits de soulignement, vous

pouvez omettre le nom de vérification du domaine (par exemple, « _6e86v84tqgqubxbwii1m ») dans l'enregistrement TXT.

- Vérifiez si votre fournisseur DNS a ajouté le nom de domaine à la fin de l'enregistrement TXT. Certains fournisseurs DNS ajoutent automatiquement le nom de votre domaine au nom d'attribut de l'enregistrement TXT. Pour éviter cette duplication du nom de domaine, ajoutez un point à la fin du nom de domaine lorsque vous créez l'enregistrement TXT. Cela indique à votre fournisseur DNS qu'il n'est pas nécessaire d'ajouter le nom de domaine à l'enregistrement TXT.
- Vérifiez si votre fournisseur DNS a modifié la valeur de l'enregistrement DNS 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 fournisseur DNS a modifié les valeurs de votre enregistrement TXT 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 fournisseur DNS ne vous permet pas d'avoir plus d'un enregistrement TXT avec le même nom d'attribut, vérifiez si votre fournisseur DNS vous permet d'attribuer plusieurs valeurs d'attribut au même enregistrement TXT. Par exemple, si votre DNS est géré par Amazon Route 53, vous pouvez utiliser la procédure suivante.

  1. Dans la console Route 53, choisissez l'enregistrement TXT 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 fournisseur DNS ne vous permet pas d'attribuer plusieurs valeurs au même enregistrement TXT, vous pouvez vérifier le domaine une fois avec la valeur dans le nom de l'attribut de l'enregistrement TXT, et une autre fois avec la valeur supprimée du nom de l'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 notification SNS
- Ajout d'une stratégie d'accès
- Ajout d'une stratégie de clé

Création d'une notification SNS

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

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

1. Ouvrez la console Amazon VPC 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 (ARN de notification), choisissez l'ARN de la rubrique SNS que vous avez créée.
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 rubrique SNS qui permet AWS PrivateLink de publier des notifications en votre nom, comme la suivante. Pour plus d'informations, voir Comment modifier la stratégie d'accès à ma rubrique Amazon SNS ? 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 rubriques SNS chiffrées, la politique de ressources de la clé KMS doit être fiable AWS PrivateLink pour appeler des opérations d' AWS KMS API. 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 console Amazon VPC 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)

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. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS PrivateLink les ressources. IAM est 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.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d’écrire 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 qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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 (IAM Identity 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 avec une 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 la section 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 section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

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, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

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 vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

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 obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité 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 utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

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 Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

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 obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (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 en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- 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 direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - 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 rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

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 documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

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

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

Les politiques 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 appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l’identité

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

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 découvrir comment choisir entre

une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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 les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes 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.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder

à une entité IAM (utilisateur ou rôle IAM). 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 remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON 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 les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- 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 plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

Comment AWS PrivateLink fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS PrivateLink, découvrez les fonctionnalités IAM disponibles. AWS PrivateLink

Fonctionnalités IAM que vous pouvez utiliser avec AWS PrivateLink

Fonction 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
ACL	Non
ABAC (étiquettes 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 IAM AWS PrivateLink et des autres Services AWS fonctionnalités, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

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 des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. 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 découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. 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 administrateur IAM du compte sécurisé 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, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

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 plus d'informations, consultez 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 les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

AWS PrivateLink partage son espace de noms d'API avec Amazon EC2. Les actions de politique en AWS PrivateLink cours utilisent le préfixe suivant avant l'action :

```
ec2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

```
]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "ec2:Describe*"
```

Pour consulter la liste des AWS PrivateLink actions, consultez les AWS PrivateLink actions dans le manuel Amazon EC2 API Reference. Pour plus d'informations, consultez Actions Defined by Amazon EC2 (Actions définies par Amazon EC2) dans Service Authorization Reference (Référence de l'autorisation de service).

Ressources politiques pour AWS PrivateLink

Prend en charge les ressources de politique	Oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de 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 les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (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 Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

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 de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Les clés de condition suivantes sont spécifiques à AWS PrivateLink :

- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, veuillez consulter Actions définies par Amazon EC2.

ACL dans AWS PrivateLink

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AWS PrivateLink

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas 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'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec 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 d'IAM dans le guide de l'utilisateur d'IAM.

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, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. 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 Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour AWS PrivateLink

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS 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 une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour AWS PrivateLink

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

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 à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS PrivateLink, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans le Service Authorization Reference.

Exemples

Contrôler l'utilisation de points de terminaison d'un VPC

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 avec des points de terminaison de VPC, consultez the section called "Politiques de point de terminaison".

Contrôler la création de points de terminaison d'un VPC en fonction du propriétaire du service

Vous pouvez utiliser la clé de condition `ec2:VpceServiceOwner` pour contrôler le point de terminaison d'un VPC qui peut être créé en fonction du propriétaire du service (`amazon`, `aws-marketplace` ou ID de compte). L'exemple suivant accorde l'autorisation de créer des points de terminaison VPC avec le propriétaire de 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"
                    ]
                }
            }
        }
    ]
}
```

Contrôle des noms DNS privés pouvant être spécifiés pour les services de point de terminaison d'un VPC

Vous pouvez utiliser la clé de condition `ec2:VpceServicePrivateDnsName` pour contrôler quel service de point de terminaison d'un VPC peut être modifié ou créé en fonction du nom DNS privé associé au service de point de terminaison VPC. L'exemple suivant accorde l'autorisation de créer un service de point de terminaison d'un VPC avec le nom DNS privé spécifié. Pour utiliser cet exemple, remplacez la région, l'ID de compte et le nom DNS 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"
                    ]
                }
            }
        }
    ]
}
```

Contrôle des noms de services pouvant être spécifiés pour les services de point de terminaison d'un VPC

Vous pouvez utiliser la clé de condition `ec2:VpceServiceName` pour contrôler quel point de terminaison d'un VPC peut être créé en fonction du nom du service de point de terminaison d'un VPC. L'exemple suivant accorde l'autorisation de créer un point de terminaison d'un VPC 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"
                    ]
                }
            }
        }
    ]
}
```

Utilisation des stratégies de point de terminaison pour contrôler l'accès à des points de terminaison d’un VPC

Une politique de point de terminaison est une politique basée sur les ressources que vous attachez à un point de terminaison VPC 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 de compartiment Amazon S3 pour contrôler l'accès aux compartiments depuis des points de terminaison ou des VPC spécifiques.

Table des matières

Considérations

- Une politique de point de terminaison est un document de politique JSON qui utilise le langage de politique IAM. 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 plus d'informations, consultez the section called "Afficher la prise en charge de stratégie de point de terminaison".
- Lorsque vous créez un point de terminaison d'un VPC pour un service de point de terminaison autre qu'un Service AWS, nous autorisons un accès complet au point de terminaison.

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

Mise à jour d'une politique de point de terminaison d’un VPC

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 console Amazon VPC 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’un VPC.
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 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)

Métriques CloudWatch pour AWS PrivateLink

AWS PrivateLink publie des points de données vers 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 relatives à ces points de données sous la forme d'un ensemble classé de données en 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 alarme CloudWatch pour surveiller une métrique spécifiée et initier une action (par exemple, l'envoi d'une notification à une adresse e-mail) si la métrique sort de 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 des métriques à CloudWatch à intervalles d'une minute, sans coût supplémentaire.

Pour plus d'informations, consultez le Guide de l'utilisateur Amazon CloudWatch.

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 dont l'état est SYN_SENT et ESTABLISHED.

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 paquets RST 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 un point de terminaison d'un VPC.
`VPC Id`	Filtre les données 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. Statistics : 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. Statistics : 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`	Le nombre de paquets RST 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 un point de terminaison d'un VPC.

Affichage des métriques CloudWatch

Vous pouvez afficher ces métriques CloudWatch à l'aide de la console Amazon VPC, de la console CloudWatch ou de l'AWS CLI comme suit.

Pour afficher les métriques à l'aide de la console Amazon VPC

1. Ouvrez la console Amazon VPC 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 des métriques à l'aide de la console CloudWatch

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Sélectionnez l'espace de noms AWS/PrivateLinkEndpoints.
4. Sélectionnez l'espace de noms AWS/PrivateLinkServices.

Pour afficher les métriques à l'aide de la 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 Contributor Insights pour vos services de points de terminaison afin de vous aider à trouver les points de terminaison qui contribuent le plus à chaque métrique prise en charge. Pour plus d'informations, consultez Contributor Insights dans le Guide de l'utilisateur d'Amazon CloudWatch.

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 paquets RST 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 de plus amples informations sur les frais associés au Contributor Insights, consultez Tarification Amazon CloudWatch.

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 pour AWS PrivateLink à l'aide soit de la AWS Management Console ou de la AWS CLI.

Pour activer les règles Contributor Insights pour AWS PrivateLink à l'aide de la console

1. Ouvrez la console Amazon VPC 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 Contributor Insights pour AWS PrivateLink à l'aide de la AWS CLI

1. Utilisez la commande list-managed-insight-rules comme suit pour énumérer les règles disponibles. Pour l'option `--resource-arn`, spécifiez l'ARN de votre service de 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 commande put-managed-insight-rules comme suit pour activer la règle. Vous devez spécifier le nom du modèle et l'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 pour 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 Contributor Insights pour AWS PrivateLink à l'aide de la console

1. Ouvrez la console Amazon VPC 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 Contributor Insights pour AWS PrivateLink à l'aide de la AWS CLI

Utilisez la commande disable-insight-rules pour désactiver une règle.

Supprimer les règles Contributor Insights

Utilisez les procédures suivantes pour supprimer les règles intégrées pour AWS PrivateLink à l'aide soit de la AWS Management Console ou de la 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 Contributor Insights pour AWS PrivateLink à l'aide de la console

1. Ouvrez la console CloudWatch 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 Contributor Insights pour AWS PrivateLink à l'aide de la AWS CLI

Utilisez la commande delete-insight-rules pour supprimer une règle.

AWS PrivateLink quotas

Les tableaux suivants indiquent les quotas, auparavant appelés limites, pour les ressources AWS PrivateLink par région pour votre compte. Sauf indication contraire, vous pouvez demander une augmentation pour ces quotas. Pour plus d'informations, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Si vous demandez d'augmenter un quota s'appliquant par ressource, nous l'augmentons pour toutes les ressources de la région.

Nom	Par défaut	Ajustable	Commentaires
Points de terminaison d'équilibreur de charge 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
Points de terminaison d'un VPC de passerelle par région	20	Oui	Vous pouvez créer jusqu'à 255 points de terminaison de passerelle par VPC
Caractères par politique de point de terminaison d'un VPC	20 480	Non	La taille maximale d'une politique de point de terminaison d'un VPC inclut des espaces blancs

Les considérations suivantes s'appliquent au trafic qui passe par un point de terminaison d'un VPC :

- Par défaut, chaque point de terminaison d'un VPC peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et augmente automatiquement jusqu'à 100 Gb/s. La bande passante maximale pour un point de terminaison VPC, lors de la répartition de la charge entre toutes les zones de disponibilité, correspond au nombre de zones de disponibilité multiplié par 100 Gb/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 gros paquet autorisé qui peut passer par un point de terminaison d'un VPC. Plus la MTU est grande, plus la quantité de données pouvant être transmises dans un seul paquet est importante.

Un point de terminaison d’un VPC prend en charge une MTU de 8 500 octets. Les paquets d'une taille supérieure à 8 500 octets arrivant au point de terminaison d’un VPC sont supprimés.

- La détection de la MTU du chemin (PMTUD) n'est pas prise en charge. Les points de terminaison d’un VPC ne génèrent pas le message ICMP suivant : `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Type 3, Code 4).
- Les points de terminaison d’un VPC appliquent la taille maximale du segment (MSS) pour tous les paquets. Pour de plus amples informations, veuillez consulter RFC879.

Historique du document pour AWS PrivateLink

Le tableau suivant décrit les versions de AWS PrivateLink.

Modification	Description	Date
Adresses IP désignées	Vous pouvez spécifier les adresses IP pour les interfaces réseau de vos points de terminaison lorsque vous créez ou modifiez votre point de terminaison d'un VPC.	17 août 2023
Prise en charge d'IPv6	Vous pouvez configurer vos services de point de terminaison Équilibreur de charge de Passerelle et vos points de terminaison Équilibreur de charge de Passerelle pour qu'ils prennent en charge à la fois les adresses IPv4 et IPv6 ou uniquement les adresses IPv6.	le 12 décembre 2022
Contributor Insights	Vous pouvez utiliser les règles intégrées de Contributor Insights pour identifier les points de terminaison spécifiques qui contribuent le plus aux CloudWatch statistiques pour AWS PrivateLink.	18 août 2022
Prise en charge d'IPv6	Les fournisseurs du service peuvent permettre à leur service de point de terminaison d'accepter les requêtes IPv6, même si leurs services	11 mai 2022

	backend ne prennent en charge que l'IPv4. Si un service de point de terminais on accepte les requêtes IPv6, les consommateurs du service peuvent activer la prise en charge d'IPv6 pour leurs points de terminaison d'interface afin de pouvoir accéder au service de point de terminaison via IPv6.	
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 d'équilibreur de charge de passerelle dans votre VPC pour acheminer le trafic vers un service de point de terminaison d'un VPC que vous avez configuré à l'aide d'un équilibreur de charge de passerelle.	10 novembre 2020
Stratégies de point de terminaison d'un VPC	Vous pouvez attacher une politique IAM à un point de terminaison d'un VPC d'interfa ce pour un AWS service afin de contrôler l'accès au service.	23 mars 2020

Clés de condition pour les points de terminaison d'un VPC et les services de point de terminaison	Vous pouvez utiliser des clés de condition EC2 pour contrôler l'accès aux points de terminaison d'un VPC et aux services de point de terminaison.	6 mars 2020
Identification des points de terminaison d'un VPC et des services de point de terminaison lors de la création	Vous pouvez ajouter des identifications lorsque vous créez des points de terminaison d'un VPC et des services de points de terminaison.	5 février 2020
Noms DNS privés	Vous pouvez accéder aux services AWS PrivateLink basés depuis votre VPC à l'aide de noms DNS privés.	6 janvier 2020
Services de points de terminaison d'un VPC	Vous pouvez créer vos propres services de points de terminaison et permettre à d'autres comptes Comptes AWS et utilisateurs de se connecter à votre service via un point de terminaison d'un VPC d'interface. Vous pouvez proposer vos services de point de terminaison à l'abonnement sur AWS Marketplace.	28 novembre 2017

Points de terminaison VPC d'interface pour Services AWS	Vous pouvez créer un point de terminaison d'interface auquel vous connecter à Services AWS cette intégration AWS PrivateLink sans utiliser de passerelle Internet ou de périphérique NAT.	8 novembre 2017
Points de terminaison d’un VPC pour DynamoDB	Vous pouvez créer un point de terminaison d'un VPC de passerelle pour accéder à Amazon DynamoDB depuis votre VPC sans utiliser de passerelle Internet ou de dispositif NAT.	le 16 août 2017
Points de terminaison d'un VPC pour Amazon S3	Vous pouvez créer un point de terminaison d'un VPC de passerelle pour accéder à Amazon S3 depuis votre VPC sans utiliser de passerelle Internet ou de dispositif NAT.	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.